Report of all speeches and panels

at the 16th International Cybersecurity Symposium

Cybersecurity for Digitized National Security,
Economic Security, and Societal Security:
Global Multilateral Public-Private Partnership Actions
with Advanced Technologies such as AI and Quantum

October 27 (Tue), 28 (Wed), 29 (Thu) and 30 (Fri), 2026

Keio University, Mita Campus, Tokyo, Japan

Hosted by

Keio University KGRI project CCRC/CSRC
INCS-CoE
The MITRE Corporation
Sasakawa Peace Foundation



第16回サイバーセキュリティ国際シンポジウム
サマリー

2026年10月27日（火）～30日（金）
October 27–30 2026 | Keio University

テーマ：デジタル社会における国家安全保障、経済安全保障、社会保障を支えるサイバーセキュリティ ～AI、PQC等の先端技術を踏まえたグローバルな多国間官民連携アクション～

全体総括

サイバーセキュリティを国家・経済・社会の安全保障を支える共通基盤と位置づけ、AIと量子技術がもたらす機会と脅威への対応を議論した。官民・国際連携を具体的な実装と共同運用につなげ、侵害を前提とした事業継続・復旧能力を高める重要性が強調された。技術、制度、人材、ガバナンスを組み合わせ、検証可能な信頼と国境を越える相互運用性を築く方向性が示された。

メインセッションの要約 **(Day 1–Day 4)**

Day 1 (10月27日)

各国政府・国際機関・産学の登壇者が、サイバー脅威と政策対応を共有した。日本のサイバー対処能力強化、重要インフラ・金融・医療・大学等の防御、人材育成、情報共有を幅広く議論。AIの安全な活用とPQCへの備えに加え、日台のデジタルトラスト協力を通じ、国際連携を実践へ移す重要性を示した。

Day 2 (10月28日)

国家安全保障を軸に、PQC移行、インテリジェンス、能動的サイバー防御、データ主権とクラウドを議論した。暗号資産の棚卸しと段階的移行、迅速で双方向の官民情報共有、SBOM等による脆弱性管理を重視。クラウドの主権性については、保存場所に加え、法域、暗号鍵、運用権限、継続的な検証が論点となった。

Day 3 (10月29日)

経済安全保障を中心に、プライバシー強化技術（PETs）、AIガバナンス、電力等の重要インフラ、半導体サプライチェーンを議論した。データの保護と利活用の両立、AIエージェントの権限管理、機器・ソフトウェアの信頼性確保を重視。国際標準と官民の共同作業を通じ、供給網全体のレジリエンスを高める必要性が示された。

Day 4 (10月30日)

社会の安全と信頼を軸に、AI時代の本人同意、デジタル社会政策、デジタルトラスト基盤、トラステッドリスト、IDウォレット・電子属性証明を議論した。同意に過度に依存せず、技術的保護と説明責任を組み合わせる重要性を提示。個人の主体性と利便性を守りながら、国際的な相互承認と実用化を進める課題を整理した。

パラレルセッションの要約 **(Day 2–Day 4)**

Day 2 (10月28日)

日米のセキュリティ・コンプライアンス連携、データ信用保証基盤、PETs、eシール、デジタル主権を具体的に検討した。共通の報告・評価の仕組み、データの出所・利用条件・履歴の管理、業務に組み込まれた自動検証を重視。普及には、技術の整備に加え、費用分担、導入効果、制度・運用の設計が必要とされた。

Day 3 (10月29日)

パラレルセッション：**Day 3**（**10月29日**）

軍民両用AIの責任ある開発・供給・利用、台湾金融分野のPQC移行、防衛・重要インフラの継続的な安全性確保を検討した。AIの責任分担と人間の関与には意見の相違が残る一方、継続的な評価の重要性が示された。暗号資産の棚卸しと共同試験、MOSA・SBOM・RMFの連携、動的防御による対応も紹介された。

Day 4 (10月30日)

AI時代の重要インフラの事業継続、AIエージェントの統制、自律型防御、経済安全保障とAI主権を議論した。資産・依存関係の把握、実際のリスクに基づく優先順位付け、最小権限、行動監視、停止・隔離・復旧を重視。AIによる防御の高速化と、人間の監督、経営層の責任、組織を越える協力を組み合わせる必要性が示された。

Contents

全体総括 **2**

メインセッションの要約 **(Day 1–Day 4)** **2**

Day 1 (10月27日) 2

Day 2 (10月28日) 2

Day 3 (10月29日) 2

Day 4 (10月30日) 2

パラレルセッションの要約 **(Day 2–Day 4)** **2**

Day 2 (10月28日) 2

Day 3 (10月29日) 2

Day 4 (10月30日) 3

Main Session 7

DAY 1 2026-10-27 火曜日 7

D1-S1-1 Opening 09:00–09:15 JST 7

D1-S1-2 Opening 09:00–09:15 JST 7

D1-S1-3 Opening 09:00–09:15 JST 9

D1-R2-2 Remarks from Keio University 09:15–09:25 JST 10

D1-R2-1 Remarks from Keio University 09:15–09:25 JST 11

D1-C13 ITRI-KGRI Strategic Cooperation Agreement (SCA) Signing Ceremony for Japan-Taiwan Digital Trust Interoperability Framework Cooperation 09:25–09:35 JST 12

D1-R3-1 Remarks from Japanese Government (Ministerial) 09:35–09:55 JST 13

D1-R3-2 Remarks from Japanese Government (Ministerial) 09:35–09:55 JST 14

D1-S4 Keynote Speech 09:55–10:10 JST 15

D1-R5-3 Remarks from each of the governments and United Nations 10:10–11:10 JST 17

D1-R5-1 Remarks from each of the governments and United Nations 10:10–11:10 JST 19

D1-R5-4 Remarks from each of the governments and United Nations 10:10–11:10 JST 21

D1-R5-8 Remarks from each of the governments and United Nations 10:10–11:10 JST 21

D1-R5-10 Remarks from each of the governments and United Nations 10:10–11:10 JST 22

D1-R5-2 Remarks from each of the governments and United Nations 10:10–11:10 JST 23

D1-R5-11 Remarks from each of the governments and United Nations 10:10–11:10 JST 24

D1-R5-7 Remarks from each of the governments and United Nations 10:10–11:10 JST 25

D1-R5-9 Remarks from each of the governments and United Nations 10:10–11:10 JST 26

D1-R5-15 Remarks from each of the governments and United Nations 10:10–11:10 JST 27

D1-S6-1 Keynote Speech 11:10–11:40 JST 28

D1-S6-2 Keynote Speech 11:10–11:40 JST 29

D1-S7 Keynote Speech from Japanese Industry, Financial Sector 13:15–13:30 JST 31

D1-S9 INCS-CoE Speech 13:30–13:45 JST 33

D1-P10 Panel 13:45–14:45 JST 35

D1-S11-12 Speeches from Japanese Government 14:45–16:00 JST 37

D1-S11-10 Speeches from Japanese Government 14:45–16:00 JST 39

D1-S11-6 Speeches from Japanese Government 14:45–16:00 JST 41

D1-S11-9 Speeches from Japanese Government 14:45–16:00 JST 43

D1-S11-4 Speeches from Japanese Government 14:45–16:00 JST 45

D1-S11-11 Speeches from Japanese Government (second block) 16:35–18:35 JST 47

D1-S11-2 Speeches from Japanese Government (second block) 16:35–18:35 JST 49

D1-S11-8 Speeches from Japanese Government (second block) 16:35–18:35 JST 52

D1-S11-5 Speeches from Japanese Government (second block) 16:35–18:35 JST 54

D1-S11-3 Speeches from Japanese Government (second block) 16:35–18:35 JST 56

D1-S11-7 Speeches from Japanese Government (second block) 16:35–18:35 JST 57

D1-S11-13 Speeches from Japanese Government (second block) 16:35–18:35 JST 59

D1-S11-1 Speeches from Japanese Government (second block) 16:35–18:35 JST 61
D1-S12 Day #1 Closing 18:35–18:40 JST 63
DAY 2 2026-10-28 水曜日 64
D2-S1 Day #2 AM Opening 09:15–09:20 JST 64
D2-S3 Speech 09:20–09:35 JST 64
D2-P4 Panel 09:35–10:35 JST 66
D2-S5 Speech 11:00–11:15 JST 68
D2-P6 Panel 11:15–12:15 JST 70
D2-S7 Day #2 PM Opening 13:30–13:35 JST 72
D2-S8 Keynote Speech 13:35–13:50 JST 73
D2-S9 Speech 13:50–14:05 JST 75
D2-P10 Panel 14:05–15:05 JST 77
D2-S11 Speech 15:25–15:40 JST 79
D2-P12 Panel 15:40–16:40 JST 81
D2-S13 Speech 17:00–17:30 JST Maria A. Roat 83
D2-S13 Speech 17:00–17:30 JST Tadashi Nagamiya 85
D2-P14 Panel 17:30–18:30 JST 87
D2-S15 Day #2 PM Closing 18:30–18:35 JST 89
DAY 3 2026-10-29 木曜日 91
D3-S1 Day #3 AM Opening 09:00–09:05 JST 91
D3-S2 Keynote Speech 09:05–09:20 JST 91
D3-S3 Speech 09:20–09:35 JST 93
D3-P4 Panel 09:35–10:35 JST 95
D3-S5 Speech 11:00–11:15 JST 97
D3-P6 Panel 11:15–12:15 JST 99
D3-S7 Day #3 PM Opening 13:30–13:35 JST 99
D3-S8 Keynote Speech 13:35–13:50 JST 104
D3-S9 Speech 13:50–14:05 JST 106
D3-P10 Panel 14:05–15:05 JST 108
D3-C16 Fraunhofer–KGRI MOU Signing Ceremony for Cybersecurity and Privacy Research Cooperation 15:25–15:30 JST 110
D3-S11 Speech 15:30–15:45 JST 111
D3-P12 Panel 15:45–16:45 JST 113
D3-S13 Speech 17:05–17:20 JST 115
D3-P14 Panel 17:20–18:20 JST 118
D3-S15 Day #3 Closing 18:20–18:25 JST 120
DAY 4 2026-10-30 金曜日 122
D4-S1 Day #4 AM Opening 09:00–09:05 JST 122
D4-S2 Keynote Speech 09:05–09:20 JST 122
D4-S3 Speech 09:20–09:35 JST 124
D4-P4 Panel 09:35–10:35 JST 125
D4-S5 Speech 10:55–11:10 JST 127
D4-P6 Panel 11:10–12:10 JST 129
D4-S7 Day #4 PM Opening 13:30–13:35 JST 131
D4-S8 Keynote Speech 13:35–13:50 JST 131
D4-S9 Speech 13:50–14:05 JST 132
D4-P10 Panel 14:05–15:05 JST 134
D4-S11 Speech 15:25–15:40 JST 136
D4-P12 Panel 15:40–16:40 JST 137
D4-S13 Speech 17:00–17:15 JST 139
D4-P14 Panel 17:15–18:15 JST 141

D4-S15-1 Closing 18:15–18:30 JST 143
D4-S15-3 Closing 18:15–18:30 JST 143
D4-S15-2 Closing 18:15–18:30 JST 144
Parallel Session 並行セッション 146
DAY 2 2026-10-28 水曜日 146
D2-T1-S2 Session 11:00–11:50 JST 146
D2-T1-S3 Session 13:00–13:50 JST 148
D2-T1-S4 Session 14:00–14:50 JST 151
D2-T1-S5 Session 15:00–15:50 JST 153
D2-T1-S6 Session 16:00–16:50 JST 155
DAY 3 2026-10-29 木曜日 158
D3-T1-S1 / D3-T1-S2 Session 10:00–11:50 JST 158
D3-T1-S3 Session 13:00–13:50 JST 161
D3-T1-S5 Session 15:00–15:50 JST 164
DAY 4 2026-10-30 金曜日 167
D4-T1-S1 Session 10:00–10:50 JST 167
D4-T1-S2 Session 11:00–11:50 JST 169
D4-T1-S3 Session 13:00–13:50 JST 171
D4-T1-S4 Session 14:00–14:50 JST 172
D4-T1-S5 Session 15:00–15:50 JST 174
D4-T1-S6 Session 16:00–16:50 JST 176
Special Program 特別プログラム 179
Special Program 1 09:00 JST 179
Special Program 2 09:15 JST 181
Special Program 3 10:10 JST 183
Special Program 4 13:00 JST 185
Special Program 5 13:05 JST 187
Special Program 6 14:20 JST 190
Special Program 7 15:50 JST 192
Change History 194

※Notes

The English and Japanese summaries do not necessarily correspond one-to-one.

When the speaker spoke in English, the English summary summarizes the speaker's words, and the

Japanese summary summarizes the words of the simultaneous interpreter.

When the speaker spoke in Japanese, the Japanese summary summarizes the speaker's words, and the English summary summarizes the words of the simultaneous interpreter.

For sessions with changes to the speakers or other session details, two heading blocks are provided. The upper block shows the information listed in the original program, and the lower block shows the information based on the session recording.

※注意事項

要約は、英語と日本語とは必ずしも一対一対応はしていません。

講演者が英語で話した場合、英語要約は講演者の言葉を、日本語要約は同時通訳者の言葉を要約しています 。

講演者が日本語で話した場合、日本語要約は講演者の言葉を、英語要約は同時通訳者の言葉を要約しています。

登壇者等に変更があったセッションでは、見出しを2段で掲載しています。上段は事前のプログラムに記載された情報、下段は当日のレコーディングに基づく情報です。

Main Session

DAY 1 2026-10-27 火曜日

Keio University, Mita Campus; West School Building 1F West Hall
慶應義塾大学 三田キャンパス 西校舎 1F 西ホール

D1-S1-1 Opening 09:00–09:15 JST

Session: Opening Speaker: D1-S1-1 Jun Murai (Professor Emeritus, Keio University; Senior Advanced Research Project Professor, Keio University)	セッション：オープニング 登壇者：D1-S1-1 村井 純 (慶應義塾大学 名誉教授・特別特区特任教授)
1. Professor Murai welcomes participants to the 16th International Cybersecurity Symposium and thanks the organizations whose cooperation has supported the event. 2. He recalls Professor Farber's substantial contributions to the Cyber Civilization Research Center (CCRC) and the symposium, and joins participants in a moment of silence. 3. He explains that cooperation with the Sasakawa Peace Foundation, MITRE, and other organizations has created a forum for stakeholders from diverse fields to exchange knowledge. He describes Keio University's role as bringing stakeholders together and encouraging dialogue. 4. With interest in and use of AI spreading rapidly, he describes 2026 as an important year for cybersecurity and the infrastructure underpinning digital technologies. 5. He notes that integrating AI into the Internet creates new cybersecurity risks in both attack and defense, and expects this to be an important topic of discussion at the symposium. 6. He emphasizes the importance of exchanges among leaders and experts from Japan and abroad in building a safer, more trustworthy future for society. On behalf of CCRC, KGRI, and CSRC, he encourages participants to make new connections and deepen discussions about the future throughout the four days of sessions.	1. 第16回サイバーセキュリティ国際シンポジウムの参加者を歓迎し、開催を支えてきた関係団体の協力に謝意を示した。 2. サイバー文明研究センター（CCRC）と本シンポジウムに大きく貢献したファーバー教授の功績を振り返り、参加者とともに黙祷を捧げた。 3. 笹川平和財団やMITREなどと協力し、多様な分野の関係者が知見を交換する場を築いてきたと述べた。慶應義塾大学の役割は、関係者を一堂に集め、対話を促すことであるとした。 4. AIへの関心と利用が急速に広がるなか、2026年はサイバーセキュリティやデジタル技術の基盤にとって重要な年になると述べた。 5. AIがインターネットに組み込まれることで、攻撃・防御の両面に新たなサイバーセキュリティ上のリスクが生じると指摘し、今回も重要な議論の対象になるとの見通しを示した。 6. 国内外のリーダーや専門家が交流し、社会としてより安全で信頼性の高い未来を築く意義を強調した。CCRC、KGRI、CSRCを代表し、参加者に4日間のセッションを通じて新たなつながりをつくり、未来に向けた議論を深めるよう呼びかけた。

D1-S1-2 Opening 09:00–09:15 JST

Session: Opening Speaker: D1-S1-2 Douglas Robbins (Vice President, MITRE)	セッション：オープニング 登壇者：D1-S1-2 ダグラス・ロビンス (MITRE 副社長)

1. Speaking on behalf of MITRE, Robbins thanks the hosts in Japan for their leadership, innovation, and commitment to security and international partnership. 2. He describes cybersecurity as central to national security, economic prosperity, public confidence, and international stability. Because digital networks underpin governments, markets, infrastructure, defense capabilities, and everyday life, cyber resilience is inseparable from national strategic resilience. 3. He recalls last year's discussions of cyber resilience, zero-trust architectures, software assurance, supply-chain risks, critical infrastructure protection, operational technology, and public-private and international partnerships. These issues remain urgent as cyber threats become more persistent, adaptive, and intertwined with geopolitical competition. 4. He highlights AI's potential to improve detection, analytics, vulnerability management, response speed, and resource allocation, while warning that malicious actors can also use it to automate attacks, generate deceptive content, accelerate reconnaissance, and lower the barriers to sophisticated cyber operations. 5. He argues that the challenge is to guide AI use with wisdom, rigor, and responsibility. Allied cooperation is needed to ensure that innovation advances in line with shared values of security, transparency, and accountability. 6. He warns that quantum computing could threaten cryptographic systems protecting government communications, financial systems, critical infrastructure, and sensitive data. Post-quantum cryptography (PQC) is therefore a present-day strategic imperative. Migration will take years, and nations and institutions that begin early will be better positioned to manage the risk. 7. He identifies an opportunity for Japan and its partners to lead through international coordination among governments, standards bodies, industry, and research institutions. The symposium brings together technical experts, policymakers, executives, diplomats, and strategists, recognizing cybersecurity as both an operational necessity and a diplomatic priority. 8. He emphasizes that the greatest advantage lies not only in technology but also in cooperation across sectors and national borders. He calls for realism about the threats and confidence in shared purpose, stressing that the security of the digital future must be built through alliance rather than isolation.	1. 参加者を歓迎し、日本での開催に謝意を示した。 2. サイバーセキュリティは技術だけの問題ではなく、国家安全保障や経済安全保障にも関わる課題であると述べた。 3. 昨年の議論を振り返り、サイバーレジリエンスの確保、信頼できるアーキテクチャ、国際的なパートナーシップの重要性に言及した。 4. AIの急速な進展を踏まえ、脆弱性への対応、リスクの検知、効果的なリソース配分の重要性に言及した。 5. 関係者の協力に加え、説明責任、透明性、セキュリティに関する価値の共有が必要であると強調した。 6. 暗号に関するリスクやシステム・通信をめぐる課題に言及し、技術面だけでなく戦略面からも検討する必要性を述べた。 7. 国や分野を越えて協力し、目的を共有してパートナーシップを進めることの重要性を強調した。

D1-S1-3 Opening 09:00–09:15 JST

Session: Opening Speaker: D1-S1-3 Nobukatsu Kanehara (Executive Director, Sasakawa Peace Foundation)	セッション：オープニング 登壇者：D1-S1-3 兼原 信克 (笹川平和財団 常務理事)
1. Kanehara warned that geographic isolation offers no protection in cyberspace: anyone connected can become a target, and automated attacks and leaks of personal information demand an urgent response. 2. He argued that Japan has fallen behind the United States and Europe in cyber defense and needs cooperation with partners to become more resilient. 3. He identified government-cloud protection as a major gap affecting government, the military, telecommunications and defense industries, and highlighted the ability to trace users' activity through logs. 4. He warned that a Taiwan contingency could begin with cyberattacks rather than missiles and could paralyze government, military forces, banks and essential services. 5. He argued that strong cyber defense should be accompanied by the ability to retaliate, drawing an analogy with nuclear deterrence to discourage attacks through the prospect of reciprocal harm. 6. He distinguished tracing ransomware offenders under criminal law from the demands of higher-level cyber attack and defense, and emphasized the need for cyber intelligence. 7. He described Japan's cyber-intelligence capability as inadequate and warned that failure to develop it would leave the country unprepared for the cyber age. 8. He called for a coordinated effort across government and the nation to respond to cyber threats and catch up with other countries.	1. 兼原氏は、海による地理的な隔たりはサイバー空間では防壁にならず、接続する誰もが攻撃対象になると指摘した。AIによる攻撃の自動化や個人情報の漏洩を踏まえ、日本は危機意識を高める必要があると訴えた。 2. 日本のサイバー防御は米国や欧州に遅れているとし、友好国と協力してサイバー攻撃に強い国にしていく必要性を強調した。 3. 政府、電気通信業界、防衛産業を保護するガバメントクラウドの不足を指摘し、利用者の活動をログで追跡できる仕組みの重要性を述べた。 4. 台湾有事では、政府、軍、発電所、銀行などのライフラインをサイバー攻撃で停止させる試みがあり得ると警告し、これを防ぐ備えを求めた。 5. サイバー防御を優先しつつ、攻撃の側面も考える必要があると述べた。核兵器との類比を用い、互いに被害を受けることが攻撃を控える理由になると説明した。 6. ランサムウェアなどの犯罪への対応と、戦争におけるサイバー攻撃・防御を区別し、後者にはサイバーインテリジェンスが不可欠だと論じた。 7. 日本のサイバーインテリジェンスの不足に強い懸念を示し、体制を整えなければ危険なサイバー時代に準備不足のまま取り残されると訴えた。 8. 政府全体で新たな状況に対応し、国全体で努力して他国に追いつく必要性を強調した。また、慶應大学が長年この分野の議論を続けてきたことを評価した。

D1-R2-2 Remarks from Keio University 09:15–09:25 JST

Session: Remarks from Keio University Speaker: D1-R2-2 Kohei Itoh (President, Keio University)	セッション：慶應義塾大学からの挨拶 登壇者：D1-R2-2 伊藤 公平 (慶應義塾 塾長)
1. Itoh welcomed participants to Keio University and expressed the university's appreciation to those supporting the symposium. 2. He highlighted participation by diplomatic representatives, Japanese ministries and agencies, current and former government officials, and experts from around the world during the four-day symposium. 3. He presented the theme as cybersecurity for digitized national, economic and societal security, with global multilateral and public-private partnership actions using advanced technologies such as AI and quantum. 4. He recalled the university's establishment of an international cybersecurity center of excellence and its cooperation with university partners in the United States, the United Kingdom and Japan. 5. He emphasized the university's contribution to the international cybersecurity community through innovation, safety, security and trust. 6. He described efforts to pursue digital innovation for societal, economic and national security, grounded in practical learning and interdisciplinary research spanning science, engineering and law. 7. He wished participants a productive symposium and encouraged them to work toward a peaceful and enjoyable world.	1. 参加者を慶應義塾大学に迎え、シンポジウムを支える関係者への感謝を述べた。 2. 世界各地の専門家による発表が行われることを紹介した。 3. デジタル化と経済安全保障・社会安全保障に関わるテーマに言及した。 4. 国際的なサイバーセキュリティの拠点を設立した経緯に触れた。 5. 国際的なサイバーセキュリティへの貢献を目指し、イノベーション、安全、セキュリティを重視する姿勢を示した。また、経済・国家・社会の安全保障に関わっていきたいと述べた。 6. 実りあるシンポジウムとなり、平和で楽しいものになることを願って挨拶を締めくくった。

D1-R2-1 Remarks from Keio University 09:15–09:25 JST

Session: Remarks from Keio University Speaker: D1-R2-1 Teruo Nakatsuma (Director of the Keio University Global Research Institute (KGRI); Professor, Keio University Faculty of Economics)	セッション：慶應義塾大学からの挨拶 登壇者：D1-R2-1 中妻 照雄 (慶應義塾大学グローバルリサーチインスティテュート (KGRI) 所長、慶應義塾大学 経済学部 教授)
1. Nakatsuma introduced the institute as a university-wide research organization established in November 2016, with a mission to advance interdisciplinary collaborative research, share results widely and create further opportunities for cooperation. 2. He explained that it supports more than 40 research centers and projects, ranging from basic research to practical responses to global social challenges, and connects academic knowledge with societal needs through industry, government and research partnerships. 3. He described the Cyber Civilization Research Center (CCRC) and Cyber Security Research Center (CSRC) as part of this research community, linking cybersecurity research with questions about how digital technologies shape society. 4. He emphasized that technological advances must be considered alongside governance, public policy and users' trust, and presented the symposium as an opportunity for cooperation across sectors and countries. 5. He invited participants to a memorial event on October 29 honoring a former co-director who had died earlier in the year. 6. He announced a planned memorandum of understanding with Taiwan's Industrial Technology Research Institute, supporting Japan–Taiwan cooperation on data trust and collaborative frameworks, including research and practical experimentation to establish verifiable trust across different systems. 7. He outlined a second planned memorandum of understanding concerning cybersecurity and privacy research, intended to combine expertise and address challenges shared by Japan, Germany and the wider international community. 8. He invited participants to view panel displays and demonstrations of digital trust infrastructure and remote attestation technologies for checking device trustworthiness. 9. He thanked the co-organizers and contributors and expressed the hope that discussions and new connections would develop into lasting partnerships for a more secure and productive society.	1. 中妻氏は、KGRIが2016年11月に全学的な研究組織として設立され、学問分野や国境を越えた共同研究、成果の共有、さらなる協力機会の創出を目指していると紹介した。 2. KGRIは40を超える研究センターやプロジェクトを支援し、基礎研究から地球規模の社会課題への実践的な取り組みまでを扱っている。産業界、政府、研究機関と連携し、学術的な知見を社会のニーズに結びつける姿勢を示した。 3. CCRCとCSRCの活動は、サイバーセキュリティ研究と、デジタル技術が社会をどう形作るかという問いを結びつけるものである。技術の進歩をガバナンス、公共政策、利用者の信頼と合わせて考える必要性を述べた。 4. シンポジウムを、こうした視点をまとめ、分野や国を越えた協力を育む機会と位置づけた。 5. CCRCの共同所長を務めたデイビッド・ファーバー教授を偲び、サイバー文明への貢献をたたえる10月29日の追悼イベントへの参加を呼びかけた。 6. 台湾の研究機関との覚書により、日本と台湾のデジタルトラストの相互運用性に関する協力を進めると述べた。国境を越えるデジタルサービスで、異なるシステム間の信頼を確立・検証するため、研究と実証を進める方針を示した。 7. もう一つの覚書では、サイバーセキュリティとプライバシーの研究協力を進め、専門性を組み合わせて日本、ドイツ、国際社会が共有する課題に取り組むと説明した。 8. 地下1階のパネル展示に加え、国際的な相互承認を支えるデジタルトラスト基盤と、デバイスの信頼性を検証するリモートアテステーション技術の実演を案内した。 9. 合意の価値は今後の研究、交流、継続的な協力を通じて高まると述べ、関係者に謝意を示した。議論から生まれるつながりを、より安全で信頼できる社会に向けた永続的なパートナーシップへ発展させることを願った。

D1-C13 ITRI-KGRI Strategic Cooperation Agreement (SCA) Signing Ceremony for Japan-Taiwan Digital Trust Interoperability Framework Cooperation 09:25–09:35 JST

Session: ITRI-KGRI Strategic Cooperation Agreement (SCA) Signing Ceremony for Japan-Taiwan Digital Trust Interoperability Framework Cooperation Signer: Wei-Chung Hwang (Deputy General Director of Information and Communications Laboratories (ICL), Industrial Technology Research Institute (ITRI)) Signer: Teruo Nakatsuma Witness: Ma-Tien Yang (Representative (Fellow), ITRI Japan Office) Witness: Kohei Itoh	セッション：日本・台湾間のデジタルトラスト相互運用性フレームワークに関する協力に向けたITRI–KGRI間の戦略的協力協定調印式 署名者：ウェン・チョン・ファン (台湾工業技術研究院(ITRI) 情報通信研究所(ICL) 副所長) 署名者：中妻 照雄 立会人：マー・ティエン・ヤン (台湾工業技術研究院(ITRI) 日本事務所 代表・フェロー) 立会人：伊藤 公平
1. The speaker welcomed the agreement on digital trust and described digital trust, digital identity and digital signatures as important foundations for AI. 2. He recalled earlier work on Taiwan's national infrastructure and international PKI collaboration, including efforts to improve interoperability across countries in Asia. 3. He described a vision of enabling people on the internet to trust one another through common standards and a shared framework across countries. 4. He contrasted the promise of AI applications with the danger of AI-enabled attacks, arguing that these risks make cooperation between countries essential. 5. He presented the agreement as an opportunity to build on decades of work and jointly strengthen the trustworthiness of digital trust infrastructure. 6. He expressed the hope that more partners from different countries would join the cooperation and help develop digital trust infrastructure to shape the future of AI.	1. デジタルトラストに関する協定に署名できることへの喜びを述べ、デジタルトラスト、デジタルアイデンティティ、デジタル署名がAIを支える重要な基礎になると強調した。 2. 台湾での初期のプロジェクトや国際協力を振り返り、日本、韓国、中国、シンガポール、台湾、タイなどとのPKI関連の取り組みに言及した。 3. 信頼できるインターネットを目指す構想に触れるとともに、状況の複雑さや難しさを述べた。 4. AIの有用なアプリケーションへの期待と、危険なAIによる攻撃のリスクを挙げ、国を越えて協力する必要性を訴えた。 5. 長年築いてきたデジタルトラストの基盤を踏まえ、研究機関同士が協力して信頼できるデジタルトラスト基盤を発展させる機会と位置づけた。 6. 今後さらに多くのパートナーの参加を得て、デジタルトラスト基盤によってAIの未来を支えたいとの期待を示した。

D1-R3-1 Remarks from Japanese Government (Ministerial) 09:35–09:55 JST

Session: Remarks from Japanese Government (Ministerial) Speaker: D1-R3-1 FURUKAWA Toshiharu (Minister for Digital Transformation)	セッション：日本政府からの挨拶 登壇者：D1-R3-1 古川 俊治 (デジタル大臣)
1. Minister Toshiharu Furukawa emphasized the growing importance of cybersecurity as AI transforms research, business, and everyday life. 2. Japan's digital strategy prioritizes stronger foundations for AI and digital transformation, alongside investment in crisis management. 3. The government aims to build autonomous, resilient digital infrastructure and reduce excessive dependence on specific countries or companies. 4. Government AI "Gennai" is trialing Japanese AI models, with public procurement intended to stimulate domestic AI investment. 5. Increasingly sophisticated cyberattacks, including state-backed operations, threaten personal information, confidential data, critical infrastructure, and national security. 6. New legislation strengthens public-private cooperation and introduces incident-reporting and asset-notification requirements for critical infrastructure operators. 7. The Cybersecurity Council enables government and businesses to share sensitive threat information and coordinate action. 8. Access-and-neutralization measures expand Japan's options for preventing serious cyberattacks and limiting damage, with attention to international coordination. 9. AI presents both cybersecurity risks and opportunities, requiring agile responses while supporting vulnerability detection and stronger cyber defenses. 10. The minister encouraged participants to turn the symposium's discussions into concrete next steps.	1. 古川大臣は、AIをはじめとするデジタル技術が研究、事業活動、日常生活に大きな変革をもたらし、サイバーセキュリティの重要性も高まっていると述べた。 2. 政府の重点計画でDXを支える基盤の強靭化を掲げ、危機管理投資を推進すると説明した。AIやクラウドが特定の国・企業に過度に依存しないよう、デジタルインフラの自律性と安定的・持続的な利用環境の確保に取り組むとした。 3. 行政向けの生成AI利用環境に国産AIモデルを試行的に実装したことを紹介し、政府調達を通じて国内の官民AI投資の好循環を目指すと述べた。 4. AIの恩恵を享受するにはサイバーセキュリティが不可欠であると強調した。国家を背景とするものを含め、巧妙化・高度化する攻撃が、機密情報の窃取や重要インフラの機能停止などを通じて経済社会と国家安全保障に重大な影響を及ぼすと指摘した。 5. サイバー対処能力強化法等に基づく官民連携の強化を説明し、対象事業者のインシデント報告の義務化や資産届出、サイバー協議会を通じた政府・民間の機微な情報の共有を、脅威への具体的な対処につなげる方針を示した。 6. 重大なサイバー攻撃の未然防止や被害拡大防止のため、アクセス無害化措置を対処の選択肢に加え、攻撃者への影響や国際連携の必要性を踏まえて多様な手段を組み合わせると述べた。 7. 高性能AIは悪用されれば脅威となる一方、脆弱性の検知・対応などに活用することで、日本のサイバー対処能力を強化できるとの期待を示した。 8. 急速に変わる技術環境に機動的・柔軟に対応し、サイバー対処能力を強化していく姿勢を示した。シンポジウムでの議論が実りある成果と次の行動につながることを期待した。

D1-R3-2 Remarks from Japanese Government (Ministerial) 09:35–09:55 JST

Session: Remarks from Japanese Government (Ministerial) Speaker: D1-R3-2 TEZUKA Satoru (Chairman of the Personal Information Protection Commission)	セッション：日本政府からの挨拶 登壇者：D1-R3-2 手塚 悟 (個人情報保護委員会 委員長)
1. Tezuka described digitalization and generative AI as drivers of profound social and economic change that also diversify risks surrounding data. He presented the APPI amendment as a response to this changing environment. 2. He argued that protecting individuals' rights and interests and using data should complement one another. The goal is a society in which data can be used safely on a foundation of trust and everyone can benefit. 3. He described the APPI as a foundation for protecting individuals and supporting safe, smooth data use, alongside wider digital, AI and cybersecurity frameworks. 4. He emphasized accurate risk identification and continuous review of governance, combining legal frameworks, technology and voluntary business initiatives to prevent serious harm to individuals. 5. He described a statistical-purpose exemption, advance publication of information about data providers and intended statistics or AI development, and opportunities for public and individual oversight. He also referred to monetary penalties for violations and stronger supervisory effectiveness. 6. He outlined a risk-based approach and the importance of enabling people to understand how their information is used and participate in its handling when necessary. He also noted the establishment of a technology team within the PPC. 7. He emphasized that international data flows must combine appropriate personal-information protection with secure, smooth transfers, and that businesses should be able to choose suitable transfer arrangements from multiple options. 8. He cited mutual adequacy arrangements with the European Union and the United Kingdom, alongside cooperation with the United States on a different cross-border approach, as a strength of Japan's international engagement. 9. He called for stronger Japan–ASEAN cooperation on personal data in support of Data Free Flow with Trust (DFFT), and pledged continued work with domestic and international partners to build trust.	1. 手塚氏は、デジタル化や生成AIが社会・経済を大きく変え、データを取り巻くリスクも多様化していると述べ、その変化を踏まえた個人情報保護法改正の考え方を説明した。 2. 個人の権利利益の保護とデータ利活用は対立するものではなく、補完し合い、調和すべきだと強調した。信頼を基盤にデータを安全に活用し、誰もが恩恵を受けられる社会を目指すとした。 3. 個人情報保護の制度を、権利利益を守り、安全で円滑なデータの流通・活用を支えるものと位置づけた。リスクを的確に捉え、規制やガバナンスを現状に合わせて見直す必要性を述べた。 4. 制度、技術、事業者の自主的な取り組みを組み合わせ、個人の権利利益への深刻な被害を防ぐ重層的な保護を進めることが重要だと説明した。 5. 統計作成やAI開発における個人情報の利用に触れ、利用目的やルールを確認すること、違反に対して金銭的なペナルティーを設けることに言及した。 6. 個人の権利利益を守るリスクベースの考え方と、本人が情報の使われ方を理解し、取り扱いを見守るための枠組みを重視した。また、新たなテクノロジーチームの設置を紹介した。 7. 国際的なデータ流通では、個人情報を適切に保護しながら安全で円滑な移転を実現することが重要だと述べ、企業が複数の選択肢から適切な仕組みを選べる環境を目指すとした。 8. 米国とグローバルCBPRを推進する取り組みに言及し、複数の国際的なアプローチに関与することが日本の特徴であり、国際協力上の強みになると説明した。 9. 日本とASEANの密接な経済関係や、今後のデータ流通の増加見通しを踏まえ、ASEANをはじめとするアジア太平洋地域で個人データに関する協力を進め、国内外のパートナーと信頼を築く努力を続けると述べた。

D1-S4 Keynote Speech 09:55–10:10 JST

Session: Keynote Speech Speaker: D1-S4-1 ADM (Ret.) Dennis Blair, (Former Director of U.S. National Intelligence)	セッション：基調講演 登壇者：D1-S4-1 デニス・ブレア (元米国国家情報長官)

1. Blair described a difficult geopolitical environment and the continuing strength of the U.S.–Japan alliance. He emphasized that longstanding working and personal relationships among Japan, the United States and other partners underpin security, including cybersecurity.
2. He warned that Japan should expect intensified attacks on government and private networks, including ransomware, theft of sensitive information, political discord through social media and malware planted for future crises or conflicts.
3. He argued that advances in agentic AI initially favor attackers, who are adopting AI faster than government and business defenders. Attackers can exploit vulnerabilities while rapidly developed patches are still being installed.
4. He described an “AI window of vulnerability” requiring urgent leadership, resources and sustained effort. He also warned that unreported attacks on military and defense-industrial networks can steal secrets and prepare for future attacks, causing lasting national-security damage.
5. He acknowledged Japan’s progress in policy, budgets and the growth of the Self-Defense Forces’ Cyber Defense Command, including authorization for limited active-defense measures. He stressed implementation rather than plans alone and noted continuing shortages of skilled defenders in both sectors.
6. He highlighted mandatory incident reporting and public–private threat-information sharing under new cybersecurity provisions, primarily for critical infrastructure. Although implementation was still at an early stage, he saw significant potential to strengthen defenders.
7. He supported Japan’s development of its own AI stack and targeted applications where Japanese companies could lead, while noting that the United States and China lead large-language-model development.
8. He recommended prioritizing defensive AI: intensive white-hat vulnerability scanning, rapid AI-enabled patch development, and patch distribution and implementation at cyber speed. Such capabilities could benefit Japan and its allies and partners.

1. ブレア氏は、日本が厳しい安全保障環境に直面する一方、日米同盟は引き続き強固だと述べた。日本、米国、その他の同盟国の間にある個人的な信頼関係や機関同士の協力が、サイバーを含む安全保障の基礎になると強調した。
2. 日本へのサイバー攻撃が激しくなると警告し、ランサムウェア、情報窃取、ソーシャルメディアによる政治的不和の助長、危機や紛争時に作動するマルウェアの埋め込みなどを挙げた。
3. 技術進歩の当初の恩恵は攻撃側にあると指摘した。犯罪者や国家がAIを急速に攻撃へ取り入れる一方、政府や企業の防御への導入は遅れがちであり、修正プログラムの適用中にも攻撃が先行する状況を説明した。
4. 日本などはAIによる「脆弱性の窓」の中にあり、リーダーシップ、資源、総力を挙げた防御が必要だと述べた。また、軍や防衛産業のネットワークに対する未報告の攻撃が、長期的な国家安全保障に重大な影響を与えると警告した。
5. 日本の政策面の進展に加え、自衛隊のサイバー防衛司令部の拡大、予算増加、限定的な能動的防衛措置の権限付与を評価した。計画だけでなく実行が重要である一方、有能な防御人材の不足は官民双方に残ると指摘した。
6. 重要インフラなどのネットワーク事業者に関する報告の義務付けや脅威情報の共有に言及した。始まったばかりの仕組みであるものの、防御に当たる人々を強化する可能性があると述べた。
7. 米国と中国が大規模言語モデル開発で先行する中、日本は日本語の技術基盤や、日本企業がリーダーになれる特定のAIアプリケーションを開発すべきだと述べた。
8. 防御目的のAIを優先し、ホワイトハットによる徹底した脆弱性の調査、AIを用いたパッチの迅速な開発、高速な配布・適用を進めるよう提言した。こうした取り組みは日本だけでなく、同盟国やパートナー国にも恩恵をもたらすとした。
9. 官民のサイバー防御運用センターを物理的、または仮想的に同じ場所へ置くことを提案し、物理的な配置がより理想的だと述べた。実務者が組織の壁を越えて協力し、成果を積み重ねることで、実効性のある官民連携が進むと説明した。
10. AIは重要ネットワークに脆弱性をもたらすと同時に、より効果的に守る機会も開くと総括した。AIを活用したサイバーセキュリティを迅速に進め、その脆弱性を閉じることが日本の課題だと述べた。

9. He recommended physically, or alternatively virtually, co-locating government and private cyber-defense operations centers. He argued that working-level experts can cooperate effectively across institutional barriers and that practical successes would strengthen public–private partnership. 10. He concluded that AI creates both a dangerous vulnerability and an opportunity for stronger defense. Japan should act quickly and decisively to close the vulnerability by accelerating AI-enabled cybersecurity.	

D1-R5-3 Remarks from each of the governments and United Nations 10:10–11:10 JST

Session: Remarks from each of the governments and United Nations Speaker: D1-R5-3 Andrew Shearer (Ambassador, Australian Embassy Tokyo)	セッション：各国政府・国連からの挨拶 登壇者：D1-R5-3 アンドリュー・シーラー (在日オーストラリア大使館大使)

1. Shearer described an international order that is increasingly fragmented, contested and disrupted, and argued that countries must actively shape their technological future rather than remain passive.
2. He highlighted cooperation on Pacific undersea cables and planned regional data-center work, alongside stronger public–private partnerships. He welcomed Japan's cybersecurity reforms as a platform for closer cooperation with Australia's complementary technological strengths.
3. He defined technological agency as retaining access to frontier technologies and the capabilities and strategic choices needed to shape outcomes. This requires adopting leading technologies, building expertise, contributing to trusted ecosystems and shaping rules consistent with shared interests and values.
4. He argued that sovereign capability does not require technological self-sufficiency. It means preserving strategic choice through domestic capability, trusted investment and diverse trusted partnerships.
5. He said Australia aims to be both an AI user and an AI developer, building domestic capability, intellectual property and economic value. He identified potential to host frontier AI training and large-scale computing using Australia's energy, land, infrastructure, subsea connectivity and research expertise.
6. He described proposed Australian AI standards covering energy, water and information sharing, intended to provide a trusted framework and greater certainty for businesses and communities, with investment, capability and data located and regulated in Australia.
7. He emphasized balancing innovation and scale in trusted technology ecosystems with safeguards for security, democratic rights, the rule of law and data protection. He described Australia and Japan as natural partners in managing this balance.
8. He called for governments, companies and universities to learn and strengthen capabilities together. Industry develops and operates technology and infrastructure, universities provide research and talent, and governments provide strategic direction and safeguards; trusted cooperation is essential to secure shared technologies and shape the emerging technological order.

1. シーラー氏は、国際秩序の分断が進み、対立や混乱が深まっていると指摘し、各国は受け身にとどまるのではなく、技術面での自国の未来を主体的に形づくる必要があると論じた。
2. 同氏は、太平洋地域の海底ケーブルをめぐる協力や、計画中の域内データセンター関連の取り組み、官民連携の強化を取り上げた。また、日本のサイバーセキュリティ改革を歓迎し、両国の技術的な強みを相互に補完しながら、オーストラリアとの協力を深める基盤になると評価した。
3. 同氏は「技術面での主体性」を、最先端技術へのアクセスを維持し、将来のあり方を形づくるために必要な能力と戦略的な選択肢を確保することと定義した。そのためには、先端技術の導入、専門性の蓄積、信頼できるエコシステムへの貢献、そして共通の利益と価値観に沿ったルールづくりが必要だと述べた。
4. 同氏は、国家としての技術的能力の確保は、技術の完全な自給自足を意味するものではないと論じた。重要なのは、国内の能力、信頼できる投資、多様で信頼できるパートナーシップを通じて、戦略的な選択肢を維持することだとした。
5. 同氏は、オーストラリアがAIの利用国であると同時に開発国となることを目指し、国内の能力、知的財産、経済的価値を育てていくと述べた。また、同国のエネルギー、土地、インフラ、海底ケーブルによる接続性、研究面の専門性を生かし、最先端AIの学習や大規模な計算処理の拠点となる可能性を指摘した。
6. 同氏は、オーストラリアで提案されている、エネルギー、水、情報共有に関するAI基準について説明した。これは、投資・技術能力・データを国内に置き、オーストラリアの規制下に置くことで、信頼できる枠組みを整え、企業や地域社会にとっての予見可能性を高めることを目的としている。
7. 同氏は、信頼できる技術エコシステムにおけるイノベーションと規模の拡大を、安全保障、民主主義に基づく権利、法の支配、データ保護のための措置と両立させる重要性を強調した。また、この両立に取り組むうえで、オーストラリアと日本は自然なパートナーであると述べた。
8. 同氏は、政府、企業、大学が共に学び、能力を高めていくよう呼びかけた。産業界は技術やインフラの開発・運用を担い、大学は研究と人材を提供し、政府は戦略的な方向性と保護措置を示す。共有する技術の安全を確保し、形成されつつある技術秩序を形づくるには、信頼に基づく協力が不可欠だとした。

D1-R5-1 Remarks from each of the governments and United Nations 10:10–11:10 JST

Session: Remarks from each of the governments and United Nations Speaker: D1-R5-1 Andrew Lee (Minister-Counselor for Economic and Scientific Affairs, U.S. Embassy Tokyo)	セッション：各国政府・国連からの挨拶 登壇者：D1-R5-1 アンドリュー・リー (経済・科学担当公使 駐日米国大使館)

1. Lee emphasized that cybersecurity is simultaneously a national, economic and societal security issue. A single breach at a large company or small contractor can spread through supply chains into daily life. 2. He cited recent attacks on Japanese companies and welcomed a coordinated government-wide response centered on the Prime Minister's office, aimed at sustaining trust in personal-data protection and economic resilience. 3. He warned that technological advances enable faster vulnerability discovery and larger-scale attacks, while also shaping future national competitiveness. Critical and emerging technologies need trusted suppliers and strong cybersecurity practices from the outset. 4. He called for closer cooperation using advanced technology and trusted cloud infrastructure, action against scam centers in the Indo-Pacific, and support for regional partners' cyber defenses. He also welcomed Japan's leadership on active cyber defense. 5. He stressed that companies own and operate critical infrastructure and are on the front lines of defense. Government, academia and industry must quickly share what they know, learn and observe. 6. He described the U.S.–Japan Technology Prosperity Deal as strengthening research-security cooperation and highlighted a strategic partnership under the Genesis mission to advance frontier fields such as quantum computing. 7. He warned that future quantum computers could break encryption protecting data today and highlighted a commitment to accelerate the transition to post-quantum cryptography based on NIST standards. 8. He called on researchers, engineers and companies to design more secure systems, find vulnerabilities before adversaries and train the next generation of cyber defenders, since government cannot secure cyberspace alone. 9. He urged each participant to identify a concrete next step by the end of the symposium week, such as joint research, a new information-sharing partnership or a quantum-resistant encryption transition plan. He called for the U.S.–Japan alliance to become a foundation of trust and innovation in cyberspace.	1. リー氏は、サイバーセキュリティは技術だけでなく、国家・経済・社会の安全保障に関わる問題であり、この脅威と無縁な国はないと述べた。大企業や小さな請負会社での一度の侵害が、サプライチェーンを通じて日常生活にも波及しかねないと強調した。 2. 日本で相次いだ企業へのサイバー攻撃に触れ、国民の個人データが守られることと、日本経済が攻撃に対して強靭であることへの信頼が重要だと述べた。 3. 技術の進歩とともに脅威も変化する一方、技術自体もネットワーク、コード、サプライチェーン、運用する人々への信頼に支えられていると説明した。安全な技術であっても、それを作り、運用し、守る人々の信頼性が欠かせないとした。 4. 能動的サイバー防御には政府と産業界の緊密な連携が重要であり、民間部門は防御の最前線にあると述べた。重要インフラを企業が所有・運用していることを踏まえ、政府だけで安全を確保することはできないと強調した。 5. サイバーセキュリティを日米の幅広い技術協力の中心に位置づけ、量子コンピューティングなどの先端技術が科学的発見の新たな可能性を開く一方、新しいリスクも生むと述べた。 6. 将来の強力な量子コンピューターが、現在のデータを守る暗号を破る可能性を指摘した。複雑化する脅威に対抗できる速さでサイバー防御を進化させる必要性を強調した。 7. 研究者、エンジニア、企業に対し、より安全なシステムの設計、敵対者に先んじた脆弱性の発見、次世代のサイバー防御人材の育成を求めた。 8. 参加者一人ひとりが、今週の終わりまでに共同研究など具体的な次の一歩を考えるよう呼びかけた。日米同盟を、サイバー空間における信頼とイノベーションの礎にすることが課題だと締めくくった。

D1-R5-4 Remarks from each of the governments and United Nations 10:10–11:10 JST

Session: Remarks from each of the governments and United Nations Speaker: D1-R5-4 Thomas GNOCCHI (Deputy Head of the European Union Delegation to Japan, Delegation of the European Union to Japan)	セッション：各国政府・国連からの挨拶 登壇者：D1-R5-4 トーマス・ニョッキ (駐日欧州連合代表部 副代表)
1. Gnocchi said cybersecurity challenges have grown and continued to evolve despite efforts to address them. He emphasized the value of bringing international experts together to share knowledge, experience and new technology. 2. Drawing on the EU cybersecurity agency's threat report, he described threats to supply chains, third-party providers and cloud environments, as well as ransomware and financially motivated attacks seeking credentials or data for fraud and impersonation. 3. He highlighted the influence of geopolitics, including hacktivist campaigns linked to Russia's war against Ukraine and conflict in the Middle East. He also described state-sponsored cyber espionage associated with Russia and China, targeting government and diplomatic bodies and transport-related entities respectively. 4. He identified artificial intelligence as a major technological development and warned that technology exposing vulnerabilities can also equip adversaries. He stressed that policies and strategies must keep pace with technological change. 5. He described cooperation with Japan under the EU–Japan digital partnership and security and defense partnership, including discussions on the interoperability of cybersecurity standards and Japan's J-C-STAR labeling scheme. 6. He referred to continued coordination on the UN global mechanism concerning cyberspace. 7. He highlighted cooperation with METI and U.S. and Japanese partners on industrial-control-system cybersecurity, as well as joint training at the ASEAN–Japan Cybersecurity Capacity Center.	1. ニョッキ氏は、EUが直面するサイバーセキュリティの課題に触れ、世界の専門家が知識や経験を共有するシンポジウムの意義を述べた。 2. サイバー攻撃には地政学的な状況も影響していると説明し、ロシアのウクライナ侵略や中東の紛争に関連する、サービスへのハクティビストの攻撃に言及した。 3. 危険を明らかにする技術が、悪意ある主体にも利用されることに触れ、サイバーセキュリティ上の課題への対応を進める必要性を示した。 4. サイバー空間には国境がなく、世界のパートナーが同様の課題に直面しているとして、グローバルな協力関係を強化する重要性を強調した。 5. 日本とは、デジタルパートナーシップおよび安全保障・防衛パートナーシップの下で協力していると説明し、シンポジウムでの実りある議論を期待した。

D1-R5-8 Remarks from each of the governments and United Nations 10:10–11:10 JST

Session: Remarks from each of the governments and United Nations Speaker: D1-R5-8 Gilberto JERÓNIMO (Ambassador, Embassy of Portugal in Japan)	セッション：各国政府・国連からの挨拶 登壇者：D1-R5-8 ジルベルト・ジェロニム (駐日ポルトガル大使)

1. Mr. Jerónimo outlined efforts to protect essential services, businesses, and citizens, explaining their alignment with EU and international standards and their contribution to the new national cybersecurity strategy currently being developed. 2. He stated that universities such as Keio University and the University of Porto play a central role in raising awareness and training the next generation of cybersecurity professionals. 3. He emphasized that, alongside national efforts, international cooperation is essential to addressing shared cybersecurity challenges. He explained that Portugal and Japan are working together to develop innovative solutions and strengthen resilience. 4. He identified the protection of submarine cables as a shared priority. 5. He called on Japanese businesses and stakeholders to recognize Portugal as a trusted partner in cybersecurity and digital communications. 6. He stressed the importance of cooperation among policymakers, researchers, and industry in building a safer digital future. He underscored the need to embrace the opportunities of the digital world while protecting citizens and the economy in a safe and responsible manner.	1. ジェロニム氏は、重要なサービス、企業、市民を守る取り組みに触れ、EUおよび国際的な基準との整合性や、策定中の新たな国家サイバーセキュリティ戦略への貢献を説明した。 2. 慶應義塾大学やポルト大学のような大学は、意識の向上と次世代のサイバーセキュリティ専門家の育成に中心的な役割を担うと述べた。 3. 各国の取り組みに加え、共通のサイバーセキュリティ課題に対応するための国際協力が不可欠だと強調した。ポルトガルと日本が、革新的な解決策の開発とレジリエンス強化に向けて協力していると説明した。 4. 海底ケーブルの防護を共通の優先課題として挙げた。 5. 日本の企業や関係者に、ポルトガルをサイバーセキュリティとデジタルコミュニケーションにおける信頼できるパートナーとして認識してほしいと呼びかけた。 6. 政策担当者、研究者、産業界が協力して、より安全なデジタルの未来を築く重要性を述べた。デジタル世界の機会を積極的に受け入れながら、安全かつ責任ある形で市民と経済を守る必要があるとした。

D1-R5-10 Remarks from each of the governments and United Nations 10:10–11:10 JST

Session: Remarks from each of the governments and United Nations Speaker: D1-R5-10 H.E. Dr. Aurelijus Zykas (Ambassador Extraordinary and Plenipotentiary, Embassy of the Republic of Lithuania)	セッション：各国政府・国連からの挨拶 登壇者：D1-R5-10 オーレリウス・ジーカス (駐日リトアニア共和国特命全権大使)

1. Zykas described cyber threats as growing in scale and sophistication. He cited a reported decline in Lithuania's recorded incidents as encouragement to keep strengthening national capabilities and international partnerships, rather than a reason for complacency. 2. He described Japan as an important regional partner and highlighted bilateral cyber dialogue in Tokyo on AI, supply-chain security, post-quantum cryptography, threat hunting and cyber exercises. 3. The partnership extends beyond dialogue to practical cooperation. He highlighted a joint Lithuanian–Japanese team's participation in a major international cyber-defense exercise and expressed confidence in expanding cooperation further. 4. He pointed to Lithuania's upcoming presidency of the Council of the European Union as another opportunity for cooperation, including cybersecurity events open to international partners. 5. He invited Japanese representatives to a digital and cyber summit in Vilnius and expressed hope that it would strengthen ties between the two countries' cybersecurity communities. 6. He thanked the university organizers for enabling experts to exchange ideas and experience, noted the Lithuanian embassy's longstanding support, and wished participants productive discussions.	1. ジーカス氏は、サイバー脅威が規模を拡大し、高度化していると述べた。リトアニアで記録されたインシデント件数が減少したとの報告については、安心する理由ではなく、国家の対応能力と国際的な連携をさらに強化する励みとして受け止めるべきだとした。 2. 日本を地域における重要なパートナーと位置づけ、東京で行われた二国間のサイバー対話に言及した。対話では、AI、サプライチェーンの安全性、耐量子暗号、脅威ハンティング、サイバー演習などが議題となった。 3. 両国の連携は対話にとどまらず、実務的な協力にも広がっていると述べた。リトアニアと日本の合同チームが大規模な国際サイバー防衛演習に参加したことを紹介し、今後のさらなる協力拡大に自信を示した。 4. リトアニアが今後、欧州連合理事会の議長国を務めることも、協力を深める機会になると指摘した。その一環として、国際的なパートナーも参加できるサイバーセキュリティ関連イベントに言及した。 5. 日本の関係者に対し、ビリニュスで開催されるデジタル・サイバーサミットへの参加を呼びかけ、両国のサイバーセキュリティ分野の関係者間のつながりが一層深まることへの期待を表明した。 6. 専門家が知見や経験を交換する場を設けた大学の主催者に謝意を示した。また、リトアニア大使館による長年の支援に触れ、参加者による実りある議論を祈念した。

D1-R5-2 Remarks from each of the governments and United Nations 10:10–11:10 JST

Session: Remarks from each of the governments and United Nations Speaker: D1-R5-2 Katherine Wilde (Minister Councilor, British Embassy, Tokyo)	セッション：各国政府・国連からの挨拶 登壇者：D1-R5-2 キャスリン・ワイルド (駐日英国公使)

1. Wilde said cybersecurity is fundamental to national security, economic security and societal resilience, rather than a specialist technical issue. She described it as an important part of the UK–Japan relationship and welcomed Japan's growing cyber capabilities. 2. She highlighted the UK–Japan Strategic Cyber Partnership, covering defense against cyber threats, whole-of-society resilience, and growth and innovation. 3. She noted that recent incidents in Japan disrupted businesses, universities and critical-infrastructure providers, demonstrating how a compromise of one organization can have consequences far beyond the initial target. 4. She argued that resilience alone is insufficient and called for greater attention to deterrence: raising the costs of malicious cyber activity, constraining attackers and showing that hostile actions have consequences. 5. She welcomed the entry into force of Japan's active cyber defense law. 6. She emphasized that comprehensive, timely information sharing between government and industry depends on trust. Those relationships must be built before incidents, not during them. 7. She described the symposium as an opportunity for government and industry to build trust and cooperate on shared challenges, and reaffirmed the United Kingdom's commitment to stand alongside Japan in defending against threats and making cyberspace safer.	1. ワイルド氏は、サイバーセキュリティは技術的な問題にとどまらず、国家安全保障、経済、社会のレジリエンスの基盤であり、日英関係の重要な一部になっていると述べた。日本のサイバー能力の進展にも敬意を表した。 2. 日英戦略サイバーパートナーシップを通じて連携を強化していると説明し、社会のレジリエンスや成長・変革を支える協力に言及した。 3. 日本で最近起きたサイバーインシデントが企業、大学、重要インフラに混乱をもたらし、一つの組織への侵害が他の多くの組織にも影響することを示したと述べた。 4. レジリエンスだけでは十分でなく、抑止力をより真剣に考える必要があると強調した。攻撃者に大きな代償や結果を認識させることが重要だと述べた。 5. 日本の能動的サイバー防衛に関する法律の施行を歓迎し、この分野で日英が相互に学び、抑止力を強化できると述べた。 6. 攻撃者が国境を越えて活動するため、国際協力が必要だと説明した。二国間の協力をより広いネットワークにつなげ、政府や業界を越えて協力する重要性を強調した。 7. 包括的で適時の情報共有は信頼に基づき、その信頼をインシデントの前から築く必要があると述べた。関係者が集まるシンポジウムの意義を評価し、英国は日本とともに脅威を防ぎ、サイバー空間を安全にする努力を続けるとした。

D1-R5-11 Remarks from each of the governments and United Nations 10:10–11:10 JST

Session: Remarks from each of the governments and United Nations Speaker: D1-R5-11 Laurie Peters (Minister and Deputy Head of Mission, Embassy of Canada to Japan)	セッション：各国政府・国連からの挨拶 登壇者：D1-R5-11 ローリー・ピーターズ (在日カナダ大使館 首席公使)

1. Peters welcomed Japan's active cyber defense legislation and emphasized public–private partnerships, incident reporting and active defense as complementary responses to rapidly evolving threats, including those associated with frontier AI. 2. She described stronger government–industry collaboration as a Canadian priority. The Canadian Cyber Defence Collective Strategic Forum combines government intelligence with industry expertise to improve the ability to anticipate, withstand and respond to cyber threats. 3. She said legislative measures covering critical cyber systems and telecommunications reinforce these efforts, helping protect essential services in finance, telecommunications, energy and transportation. 4. She highlighted the Canada–Japan Cyber Policy Dialogue, with preparations underway for its first meeting, as a framework for coordinating and advancing practical cooperation among the two countries' ministries and agencies. 5. She emphasized international partnerships in Canada's cybersecurity and AI strategies and called for cooperation on global norms and responsible state behavior in cyberspace. She also encouraged participation in a transparency initiative concerning implementation of UN recommendations on responsible ICT use. 6. She described trust as essential to effective cooperation across government agencies, the public and private sectors, and international partners in preventing and responding to cyber incidents. 7. She warned that malicious cyber activity aims not only to cause economic harm and security threats but also to undermine trust in institutions. She called for a collaborative response consistent with democratic values, rights and freedoms, supported by experience-sharing and stronger relationships.	1. ピーターズ氏は、民間とのパートナーシップを通じてサイバーインシデントの予防・対応能力を高める重要性に触れ、政府と産業界の連携強化はカナダの優先課題だと述べた。 2. 政府の情報分析能力と産業界の専門知識を組み合わせるフォーラムを紹介し、サイバー脅威を予測し、対応する能力の向上を目指していると説明した。 3. 官民連携を法整備によっても強化していると述べ、重要なサービスや資産を守り、サイバーセキュリティを高める取り組みに言及した。 4. 国家サイバーセキュリティ戦略と国家AI戦略では国際的なパートナーシップを重視していると述べた。日加サイバー政策対話の初回会合を日本側と準備し、両国の省庁・機関の協力を調整・発展させる枠組みとする考えを示した。 5. 国境を越えた協力の重要性を強調し、ICTの責任ある利用に関する国連勧告の実施状況についての国家調査に言及した。参加各国にも、この透明性を高める取り組みへの参加を呼びかけた。 6. サイバーインシデントを効果的に予防・対処するため、省庁・機関、官民、国際的なパートナーの間の協力が不可欠だと述べた。経験共有を通じて信頼を育み、レジリエンスを築く重要性を強調した。 7. 悪意あるサイバー活動は経済的損害や安全保障上の脅威だけでなく、国民と制度の間の信頼も損なうことを狙うと指摘した。民主主義の価値、権利、自由に沿って協力し、対処する必要があると述べた。

D1-R5-7 Remarks from each of the governments and United Nations 10:10–11:10 JST

Session: Remarks from each of the governments and United Nations Speaker: D1-R5-7 Peter van der Hoest (Counselor at the Embassy of the Kingdom of the Netherlands, Tokyo)	セッション：各国政府・国連からの挨拶 登壇者：D1-R5-7 ピーター・ファン・デル・フースト (駐日オランダ王国大使館 参事官)

1. Peter van der Hoest linked economic prosperity and national security to the resilience of digital ecosystems. He noted that Japan and the Netherlands are both highly digitalized economies and face risks arising from their deep interdependence, making it important to strengthen resilience together. 2. He cited ransomware attacks in Japan and a disruption to the supply of goods in the Dutch retail sector as examples of why digital vulnerabilities require swift and comprehensive action. 3. He outlined the Netherlands' Cybersecurity Act and described measures covering sectors such as energy, healthcare, manufacturing, and digital infrastructure. 4. He highlighted three key requirements for organizations covered by the legislation: registration, technical and organizational security measures, and reporting of significant incidents. 5. He stressed that senior management should take responsibility for cybersecurity and manage risks proactively to strengthen corporate governance. 6. He welcomed cooperation with Japan in an increasingly complex threat environment. He emphasized that protecting interconnected digital ecosystems and supply chains requires sharing best practices and building trust alongside regulation. 7. He concluded that countries are best placed to benefit from digital transformation when they understand their strengths, prepare for potential risks, and choose to cooperate with other countries.	1. ファン・デル・フースト氏は、経済的繁栄と国家安全保障がデジタルのエコシステムにつながっていると述べた。高度にデジタル化した日本とオランダは、深い相互依存による脅威にもさらされ、共通のレジリエンスを強化する必要があるとした。 2. 日本でのランサムウェア攻撃や、オランダの小売業で商品供給に支障が出た例を挙げ、デジタルの脆弱性に対する迅速で包括的な行動が必要だと述べた。 3. オランダのサイバーセキュリティ法に触れ、エネルギー、医療、製造、デジタルインフラなどの分野を対象とする取り組みを説明した。 4. 対象となる事業者の登録、技術的・組織的なセキュリティ対策、重大インシデントの報告を柱として挙げた。 5. 企業の経営層による責任と積極的なリスク管理に言及し、サイバーセキュリティのガバナンスを強化する重要性を示した。 6. 複雑な脅威環境の中で日本と協力できることを歓迎し、相互につながるエコシステムやサプライチェーンには、規制だけでなくベストプラクティスの共有と信頼構築も必要だと述べた。 7. デジタル変革の恩恵を受けるのは、自国の強みを理解し、起こり得るリスクに備え、他国との協力を選ぶ国々だと締めくくった。

D1-R5-9 Remarks from each of the governments and United Nations 10:10–11:10 JST

Session: Remarks from each of the governments and United Nations Speaker: D1-R5-9 Merike Grünthal (Counsellor / Deputy Head of Mission, Embassy of Estonia in Tokyo)	セッション：各国政府・国連からの挨拶 登壇者：D1-R5-9 メリケ グリュンタル (エストニア大使館参事官)

1. Grünthal described digital services and cybersecurity as two sides of the same coin. Estonia's highly digital government and continuing state-sponsored cyberattacks from Russia have led it to invest in cyber defense for many years. 2. As a small country with limited resources, Estonia has developed digital government services in close cooperation with the private sector. She said this partnership supports efficient, flexible services and helps address vulnerabilities caused by weak cyber hygiene, including weak passwords and human error. Trust also encourages businesses to report attacks. 3. She argued that the key question is how wisely AI is used, rather than how extensively it is used. AI should support human well-being and a human-led future, rather than make decisions that people simply follow. 4. She described AI tools being developed for government and highlighted a tool for high-school students being developed in cooperation with OpenAI. Instead of simply giving answers, it challenges students' thinking and helps them build critical-thinking skills. 5. She highlighted cooperation with Japan and other like-minded countries based on international law. Rules governing AI, cyberspace, data and emerging technologies will shape the international order and the security environment. 6. She said cyber defense must be integrated into deterrence and resilience policies, as hostile actors use cyber operations alongside other activities. Estonia supports stronger international cooperation to attribute and respond to malicious cyber activity. 7. Governments cannot secure the digital world alone. With critical infrastructure, cloud computing, telecommunications and digital innovation depending on private enterprises, she called for stronger cooperation among governments, technology companies, other businesses, universities and research institutions.	1. グリュンタル氏は、エストニアが民間部門と緊密に協力しながらデジタルサービスを開発してきたと述べた。 2. 官民の緊密なパートナーシップを基盤とするデジタル社会は、AIの発展がもたらす新たな機会と課題に対応する備えになると説明した。 3. 重要なのはAIをどれだけ多く使うかではなく、どれだけ賢く使うかだと述べた。AIの指示に従うだけの世界ではなく、人間が主導する未来を目指す考えを示した。 4. 高校生向けのAIツールの開発に触れ、生徒自身の思考を促す仕組みを紹介した。 5. 世界全体の安全保障を強化するため、政府、テクノロジー企業、大学、研究機関などの協力を続ける必要があると述べた。今後も意見交換を続け、課題に取り組む姿勢を示した。

D1-R5-15 Remarks from each of the governments and United Nations 10:10–11:10 JST

Session: Remarks from each of the governments and United Nations Speaker: D1-R5-15 Izumi Nakamitsu (Under-Secretary-General and High Representative for Disarmament Affairs, United Nations)	セッション：各国政府・国連からの挨拶 登壇者：D1-R5-15 中満 泉 (国際連合事務次長・軍縮担当上級代表)

1. Nakamitsu said states are strongly interested in the relationship between ICTs and emerging technologies. She noted that the Global Mechanism's thematic groups, meeting for the first time in December, could support action-oriented discussions of AI- and quantum-related risks. 2. She emphasized that these discussions must draw on private-sector expertise. 3. She described industry as both a driver of innovation and a contributor to managing emerging risks, and called for more opportunities for public–private exchange.	1. 中満氏は、AIや量子技術などの進歩がサイバーセキュリティの状況を大きく変えていると述べた。AIは悪意あるサイバー活動の規模・速度・高度化を促進し、参入障壁も下げると指摘した。 2. 量子技術も新たな課題をもたらし、ICTネットワークや通信を保護する技術の基盤が脅かされる可能性があると述べた。 3. 国連における取り組みは、脅威を把握し、ICT利用における責任ある国家の行動の枠組みを築いてきた数十年の積み重ねを基盤としていると説明した。 4. 12月に初会合を開くグローバル・メカニズムのテーマ別グループが、AIや量子技術に関連するリスクについて具体的な議論を後押しできると述べた。 5. 議論を実効性のあるものにするには民間部門の専門知識を活用する必要があると強調した。産業界のイノベーションへの貢献に触れ、官民交流を促進する機会をさらに活用すべきだと述べた。

D1-S6-1 Keynote Speech 11:10–11:40 JST

Session: Keynote Speech Speaker: D1-S6-1 ADM (Ret.) Michael Rogers (Former Commander US Cyber Command/Director NSA; Current Senior Advisor, Nihon Cyber Defence & Brunswick Group)	セッション：基調講演 登壇者：D1-S6-1 マイケル・ロジャース (元米サイバー軍司令官兼国家安全保障局(NSA)長官、現・日本サイバーディフェンスおよびブランズウィック・シニアアドバイザー)

1. Drawing on his experience in cyber intelligence, defense, offensive operations and work with Japan, Rogers offered an assessment focused on operational outcomes. 2. He praised Japan's cybersecurity policy and legal framework, describing it as internationally advanced. He also welcomed investment in practical capability and political leadership committed to cybersecurity. 3. He described Japan as facing an unprecedented formal cyber emergency and argued that the severity and scale of the situation were not being sufficiently acknowledged. 4. He criticized Japan's cyber hygiene and urged a frank assessment of existing weaknesses. He argued that AI was exposing longstanding vulnerabilities rather than creating the weaknesses underlying the attacks he discussed. 5. He said Japanese cyber intelligence was falling short of its basic mission to anticipate, predict and warn. Advance warning to network owners and operators, he argued, could help prevent threats rather than leaving defenders to react after intrusions are discovered. 6. He identified the translation of strong policy into operational strategies and tangible results as a central challenge, arguing that Japan had not yet converted its policy progress into sufficient operational outcomes. 7. He recognized the effort being made but stressed that effort must not be confused with results. He called for structures capable of turning policy into practical activity with private-sector network owners. 8. He described cybersecurity as a team activity requiring strong partnerships with other countries, the private sector, technology and cybersecurity companies, academia and research organizations. 9. He concluded that national defense, economic performance and safe personal lives increasingly depend on protecting connectivity and data, making shared cybersecurity and resilience a collective responsibility.	1. ロジャース氏は、サイバー防御・攻撃の組織を率い、日本の政府や民間と連携してきた経験を踏まえ、結果を重視する立場から評価と提言を示した。 2. 日本の政策・法制度の整備を高く評価し、サイバー能力への投資や、課題に取り組む政治的リーダーシップも肯定的に評価した。 3. 日本がサイバーの緊急状況にあるとの認識を示し、問題の規模や深刻さが十分に語られていないと指摘した。 4. 日本のサイバー衛生の状況には改善が必要だと述べ、問題を解決するには現実を正直に見つめ、課題に正面から向き合うことが重要だと強調した。 5. AIが脆弱性を新たに作ったのではなく、以前から存在していた脆弱性の深さや大きさを明らかにしていると説明した。 6. サイバーインテリジェンスの重要な役割は、攻撃を予測し、ネットワークの関係者に警告することだと述べた。日本ではインシデント発生後の対応になっているとして、事前の予測と警告を重視した。 7. 日本の大きな課題は、優れた政策を実際の行動や運用上の戦略へ移すことだと指摘した。一生懸命取り組んでいることは認めつつ、努力だけでなく結果に集中する必要があると強調した。 8. サイバーセキュリティは一人では実現できず、他国、民間部門、技術・サイバーセキュリティ企業、学術機関との強いパートナーシップが不可欠だと述べた。 9. 高度につながったデジタル社会では、安全保障、経済的な成果、安全な生活のためにデータなどを保護することが重要だと述べ、共同でサイバーセキュリティとレジリエンスを築くシンポジウムの意義を示した。

D1-S6-2 Keynote Speech 11:10–11:40 JST

Session: Keynote Speech Speaker: D1-S6-2 IIDA Yoichi (National Cyber Director, National Cybersecurity Office)	セッション：基調講演 登壇者：D1-S6-2 飯田 陽一 (国家サイバー統括室 内閣サイバー官)

1. Mr. Iida explained that Japan has been preparing to implement relevant legislation and undertaking a major review of its strategy to bring its cyber response capabilities to a level equal to or higher than those of other leading advanced economies. He said Japan aims to achieve world-class resilience through three pillars: continually imposing costs on attackers, strengthening society-wide responses, and developing an ecosystem encompassing advanced technologies and skilled personnel.
2. He identified the allocation of roles and responsibilities among governments, businesses, individuals, and others involved in developing, providing, and using AI as a key challenge in ensuring safe and trustworthy AI. On digital sovereignty, he also explained that networks of trust built on each country's strengths are important for both economic and national security.
3. He described Japan's cybersecurity environment as severe, with data breaches occurring across a wide range of industries. He expressed concern about intrusions into public-facing web systems and the theft of personal information, ransomware, and further harm caused by suspicious emails and impersonation.
4. He outlined basic precautions for the public: avoid reusing passwords across multiple services, make active use of multi-factor authentication, and exercise caution when handling emails, recognizing that they may be malicious.
5. He called on businesses to properly manage their web systems, detect suspicious activity early, prevent incidents involving contractors and business partners from spreading through supply chains, and manage data appropriately. He emphasized that swift and effective implementation requires decisions by senior management, alongside efforts by operational teams and CISOs.
6. He said the government would support affected individuals and businesses, consolidate information, communicate accurate information, and take response measures, including blocking and neutralizing malicious access. He outlined plans to compile an emergency response package setting out concrete measures and to consider and coordinate fiscal measures as needed.

1. 飯田氏は、日本のサイバー対処能力を主要先進国と同等以上に高めるため、関連法の施行準備と戦略の大幅な見直しを進めてきたと説明した。攻撃者への継続的なコスト付加、社会全体の対応強化、先端技術と人材を含むエコシステムの発展を柱に、世界最高水準のレジリエンスを目指すとした。
2. AIの開発・提供・利用に関わる政府、企業、個人などが、安全で信頼できるAIのために役割と責任をどう分担するかが課題だと述べた。デジタル主権についても、自国の強みを生かした信頼のネットワークが経済と安全保障の両面で重要だと説明した。
3. 日本のサイバー情勢は厳しく、幅広い業種で情報漏洩が発生していると述べた。公開Webシステムへの侵入と個人情報の窃取、ランサムウェア、不審メールやなりすましによる二次被害への懸念を示した。
4. 国民向けの基本的な対策として、複数サービスでのパスワード使い回しを避けること、多要素認証を積極的に使うこと、不審メールを前提に注意深く対応することを挙げた。
5. 事業者には、Webシステムの適切な管理と不審な挙動の早期発見、委託先や取引先からサプライチェーンへの影響を防ぐ対応、データの適切な管理を求めた。迅速で着実な実行には、現場やCISOだけでなく経営トップの意思決定が必要だと強調した。
6. 被害を受けた個人・企業への支援、情報集約と的確な情報発信、アクセス無害化措置などの対処を進めると述べた。具体策を示す緊急対策パッケージを取りまとめ、必要に応じて財政措置も検討・調整する方針を説明した。
7. 官民連携や通信情報の利用によって情報源を拡大し、情報を集約・分析して日本へのサイバー攻撃のリスクや脅威を評価すると説明した。その評価に基づき、複数の対処手段から状況に応じた対応を選ぶ考えを示した。
8. サイバー協議会を通じて民間と連携し、政府独自の分析を加えた、具体的な対応に役立つ情報を提供する方針を示した。機微な情報も必要な保護を行いながら共有し、信頼関係の発展につなげるとした。
9. 政府だけで対応するのではなく、民間、同盟国、同志国などとの連携を強化し、国際的な信頼と協力を広げる重要性を述べた。
10. 急速に変化するサイバー情勢に対応しながら、政府の仕組みを不断に見直し、人材育成を含めた中長期的な視点でサイバー対処能力を強化する方針を示した。

7. He explained that the government would broaden its information sources through public-private cooperation and the use of communications information, then consolidate and analyze that information to assess the risks and threats posed by cyberattacks against Japan. Based on those assessments, it would select the appropriate response from a range of available measures. 8. He outlined plans to work with the private sector through the Cybersecurity Council and provide actionable information incorporating the government's own analysis. Sensitive information would also be shared with appropriate safeguards to help deepen mutual trust. 9. He emphasized the importance of strengthening cooperation with the private sector, allies, and like-minded countries, rather than relying solely on the government, and of expanding international trust and cooperation. 10. He outlined a policy of strengthening Japan's cyber response capabilities over the medium to long term, including through workforce development, while continuously reviewing government structures and processes to keep pace with the rapidly changing cybersecurity environment.	

D1-S7 Keynote Speech from Japanese Industry, Financial Sector 13:15–13:30 JST

Session: Keynote Speech from Japanese Industry, Financial Sector Speaker: Toru Nakashima (Group CEO, Sumitomo Mitsui Financial Group)	セッション：基調講演：日本の重要インフラ、金融 登壇者：中島 達 (三井住友フィナンシャルグループ グループCEO)

1. Mr. Nakajima said that as cyberattacks on financial institutions become a daily occurrence, attention must also be paid to attacks with signs of state involvement and those intended to disrupt payments and destabilize the financial system. He emphasized that cybersecurity goes beyond crisis management at individual firms and concerns the stability of the financial system and the Japanese economy as a whole.
2. He explained that frontier AI can increase the scale, speed, and sophistication of attacks while also supporting defensive activities, such as identifying and analyzing vulnerabilities. He noted that AI is transforming cybersecurity for both attackers and defenders.
3. He pointed out that migration to the cloud and integration with external services are making it harder to understand how services operate, how responsibilities are divided, and where potential risks lie. As institutions move away from traditionally closed system environments, he stressed the need to strengthen defenses.
4. He explained that the group conducts monitoring through specialized teams and carries out exercises simulating cyber incidents, applying the insights gained to improve security across the financial sector and society. Examples included sharing information when evidence of incidents affecting other financial institutions or customers is found on the dark web, seconding personnel, conducting joint exercises, and holding study sessions with critical infrastructure operators.
5. He outlined initiatives that draw on the group's expertise as a financial institution to support companies facing difficulties in securing cybersecurity specialists and expertise. He also explained that the group uses frontier AI to assess vulnerabilities, carefully reviews the findings, and takes appropriate action.
6. He said that containing the impact of an attack may require temporarily shutting down systems as a precaution. He emphasized the importance of establishing decision-making frameworks and procedures in advance, including determining which services should be suspended.

1. 中島氏は、金融機関へのサイバー攻撃が日常化する中、国家の関与がうかがわれる攻撃や、決済を妨げ金融システムを混乱させる攻撃にも注意が必要だと述べた。サイバーセキュリティは個社の危機管理だけでなく、金融システムと日本経済全体の安定に関わる課題だとした。
2. フロンティアAIは攻撃の規模・速度・巧妙さを高める一方、脆弱性の発見・分析など防御にも活用できると説明した。攻撃側と防御側の双方でAIがサイバーセキュリティのあり方を変えていると述べた。
3. クラウドへの移行や外部サービスとの連携により、サービスの仕組み、責任分担、潜在的なリスクの把握が難しくなっていると指摘した。従来の閉じたシステム環境から変わる中で、防御を強化する必要があるとした。
4. グループでは専門組織による監視や有事を想定した訓練を行い、その知見を金融業界や社会全体の安全にもつなげていると説明した。ダークウェブで他の金融機関や顧客に関わる被害情報を把握した場合の情報提供、人材派遣、共同訓練、重要インフラ事業者との勉強会を紹介した。
5. 金融機関として蓄積した知見を生かし、専門人材や知識の確保に課題を抱える企業を支援する取り組みを紹介した。また、フロンティアAIを脆弱性診断に活用し、結果を精査して必要な対策を取っていると説明した。
6. 攻撃の悪影響を遮断するため、システムを一時的・予防的に停止する判断も求められると述べた。どの範囲のサービスを停止するかなど、判断の仕組みや手順を平時から検討する重要性を強調した。
7. 経営者自身が専門家になる必要はないが、備えるべき事態を理解し、必要な人材・資金・設備を確保することは経営の責任だと述べた。経営トップが優先的に取り組む姿勢を示し、具体的な行動につなげる必要があるとした。
8. 専門組織の整備だけでは万全でなく、AIによる攻撃が高度化・迅速化するほど基本対策の徹底が重要になると述べた。アクセス権限の適切な設定、不審メールのリンクや添付ファイルを開かないことなどを組織全体で実践するよう求めた。
9. 金融インフラを守るには個々の金融機関だけでなく、業界内の協力、電力・通信など他の重要インフラとの平時からの連携、官民の情報共有が必要だと説明した。国際的な情報共有や、AIを安全に利用するためのルールづくりの重要性にも言及した。
10. 金融ビジネスの基盤は顧客と社会からの信頼であり、技術が急速に進歩する中でも、その信頼を守るために関係者が一体となってサイバーセキュリティを強化し続ける必要があると述べた。業界や国境を越えた連携により、金融システムと社会全体の強靭性を高めることを期待した。

7. He stated that executives do not need to become cybersecurity experts themselves, but management is responsible for understanding the scenarios the organization must prepare for and securing the necessary people, funding, and equipment. He stressed that top executives must demonstrate their commitment to making cybersecurity a priority and translate that commitment into concrete action. 8. He noted that establishing specialized teams alone is not enough, and that consistently implementing basic security measures becomes even more important as AI-powered attacks grow more sophisticated and faster. He called for organization-wide adherence to practices such as setting appropriate access permissions and avoiding links or attachments in suspicious emails. 9. He explained that protecting financial infrastructure requires cooperation among financial institutions, ongoing coordination with other critical infrastructure sectors such as electricity and telecommunications, and information sharing between the public and private sectors. He also highlighted the importance of international information sharing and developing rules for the safe use of AI. 10. He stated that the financial business rests on the trust of customers and society, and that even as technology advances rapidly, all stakeholders must continue working together to strengthen cybersecurity and preserve that trust. He expressed hope that collaboration across industries and national borders would enhance the resilience of the financial system and society as a whole.	

D1-S9 INCS-CoE Speech 13:30–13:45 JST

Session: INCS-CoE Speech Speaker: Luiz DaSilva (Professor, Virginia Tech)	セッション：INCS-CoEスピーチ 登壇者：ルイス・ダ・シルヴァ (バージニア工科大学教授)

1. DaSilva described an international cybersecurity organization founded by universities in Japan, the United States and the United Kingdom on the principle that cybersecurity challenges cross borders and require international cooperation. 2. He explained that its mission extends beyond collaboration among universities to include industry and government, bringing different stakeholders together to address shared cybersecurity challenges. 3. He described an expanding network of core and affiliated universities across several countries, supported by fellows and experts offering expertise across cybersecurity topics. 4. He reported on an expert roundtable held alongside the organization's annual in-person board meeting in Japan, covering emerging issues such as AI, quantum computing and cybercrime. 5. He outlined a webinar program bringing together international speakers on specific subjects. Topics included AI and cybersecurity, critical-infrastructure protection, and the human and social-science dimensions of cybercrime; recordings are made available on YouTube. 6. He described an international capture-the-flag competition in which students from different countries are placed in multinational teams, emphasizing teamwork and cross-border cooperation as well as competition. 7. He invited students to participate in the next competition at George Mason University in Fairfax, Virginia, and encouraged the audience to follow announcements of future webinars and activities.	1. ダ・シルヴァ氏は、サイバーセキュリティの課題は国境を越え、国際協力が欠かせないとの考えから、日本、米国、英国の大学が設立した国際組織を紹介した。 2. 同組織は、大学間の連携に加え、産業界や政府にも参画を広げ、さまざまな関係者が共通のサイバーセキュリティ課題に取り組むことを目指していると説明した。 3. 複数の国で中核大学と連携大学のネットワークが拡大しており、フェローや専門家がサイバーセキュリティの幅広い分野で知見を提供していると述べた。 4. 日本で開催された年次対面理事会に合わせて専門家によるラウンドテーブルを開き、AI、量子コンピューティング、サイバー犯罪などの新たな課題を議論したと報告した。 5. 特定のテーマごとに各国の登壇者を招くウェビナーを紹介した。AIとサイバーセキュリティ、重要インフラの保護、サイバー犯罪の人間的・社会科学的側面などを取り上げており、録画はYouTubeで公開していると説明した。 6. 各国の学生が混成チームを組む国際キャプチャー・ザ・フラッグ（CTF）大会を紹介した。競技を通じて、チームワークと国境を越えた協力を育むことを重視していると述べた。 7. 米国バージニア州フェアファックスのジョージ・メイソン大学で開催される次回大会への学生の参加を呼びかけるとともに、今後のウェビナーや活動の案内にも注目してほしいと述べた。

D1-P10 Panel 13:45–14:45 JST

Session: INCS-CoE Moderator: Luiz DaSilva Panelist: David Luzzi (Senior Vice Provost, Northeastern University) Panelist: Anupam Joshi (Vice Provost & Chief AI Officer, UMBC) Panelist: Chris Hankin (Professor, Imperial College London) Panelist: Konstantinos Mersinas (Associate Professor, Royal Holloway, University of London) Panelist: Muhammad Salman (Head of Electrical Engineering Department, Faculty of Engineering, University of Indonesia) Panelist: Kalamullah Ramli (Professor, Department of Electrical Engineering, Faculty of Engineering, Universitas Indonesia) Panelist: Rolando Martins (Assistant Professor, University of Porto) Panelist: Takao Kondo (Project Associate Professor, Keio University Global Research Institute (KGRI)) Panelist: Laura Gazda (Special Assistant to Executive Director, Commonwealth Cyber Initiative, Virginia Tech)	セッション：INCS-CoE モデレーター：ルイス・ダ・シルヴァ パネリスト：デイビッド・ルッツィ (ノースイースタン大学副学長) パネリスト：アヌパム・ジョシ (UMBC副学長、チーフAI オフィサー) パネリスト：クリス・ハンキン (インペリアル・カレッジ・ロンドン教授) パネリスト：コンスタンチノス・メルシーナス (ロンドン大学ロイヤル・ホロウェイ校 准教授) パネリスト：ムハンマド・サルマン (インドネシア大学コンピュータ工学科長) パネリスト：カラマラ・ラムリ (インドネシア大学 工学部 電気工学科 教授) パネリスト：ローランド・マーティンス (ポルト大学 助教) パネリスト：近藤 賢郎 (慶應義塾大学グローバルリサーチインスティテュート 特任准教授) パネリスト：ローラ・ガツダ (バージニア工科大学コモンウェルス・サイバー・イニシアチブ事務局長特別補佐)

1. The panel presented university-led cybersecurity research, education, innovation, and international partnerships, emphasizing that cybersecurity requires cooperation across institutions, sectors, and disciplines.
2. UMBC highlighted operational-technology cyber ranges, research in AI and quantum technologies, and a multidisciplinary cybersecurity institute linking technical research with public policy, economics, and other fields. Partnerships with government and industry support workforce development and entrepreneurship.
3. Royal Holloway described interdisciplinary work on threat actors, cybercrime, resilience, human behavior, responsible cybersecurity, and data and AI. Its international collaborations connect technical research with law, psychology, criminology, and societal needs.
4. The University of Indonesia presented the country-to-country cybersecurity competition as a way to combine technical challenges with multinational teamwork and cultural exchange. The presentation also identified gender representation as an issue requiring attention.
5. Indonesia's IDCARE described a multi-stakeholder approach combining cybersecurity research, practical training, policy advice, and regional capacity building. Professional certifications, postgraduate education, and cybersecurity training for leaders were presented as complementary ways to develop expertise.
6. The University of Porto emphasized transferring research into industry and addressing security, privacy, ethics, and legal requirements together. Its examples included industrial collaborations, secure communications, and data spaces that support information sharing while protecting privacy and sovereignty.
7. Keio University outlined two complementary research approaches: analyzing Internet and security data to detect and understand threats, and designing trustworthy systems. Its work includes darknet and network-traffic analysis, operational-technology and industrial-control-system security, and system-level protection.
8. Virginia Tech's Commonwealth Cyber Initiative described its statewide mission in cybersecurity research, innovation, and workforce development. It connects universities and colleges with industry through research partnerships, startups, internships, and other experiential learning opportunities.

1. INCS-CoEに参加する大学が、サイバーセキュリティの研究、人材育成、産学官連携の取り組みを紹介し、国際的な協力をさらに広げる意義を共有した。
2. メリーランド大学ボルチモア・カウンティ校（UMBC）は、OTに特化したサイバーレンジやAI・量子分野の研究を紹介した。技術分野だけでなく、公共政策、政治、経済、物理、数学などの専門家を迎え、政府・企業との連携や起業支援を進めている。
3. ロンドン大学ロイヤル・ホロウェイ校は、学際的研究を重視し、脅威情報、サイバー犯罪、レジリエンス、ドローン、人間の行動、責任あるサイバーセキュリティなどの研究と国際連携を紹介した。技術に加え、法や社会の観点を組み合わせる重要性を示した。
4. インドネシア大学は、国際的なサイバーセキュリティ競技を通じた教育と交流を紹介した。異なる国・大学の参加者が強みを持ち寄って課題を解決し、技術力だけでなく相互理解や文化交流を深める機会になる一方、参加者の男女比には課題があると述べた。
5. インドネシア大学の研究機関は、政府・産業界・大学を結ぶ研究、実践的な訓練、政策提言、国際協力を紹介した。地域の能力構築に加え、専門資格を修士課程の単位として認める仕組みや、投資判断を担うリーダーへの教育にも取り組んでいる。
6. ポルト大学は、大学の研究成果を産業界で活用し、社会に貢献する方針を説明した。侵入への耐性、産業界との共同研究、プライバシーを守るデータ活用などを取り上げ、技術だけでなく倫理や制度も考慮する必要性を示した。
7. 慶應義塾大学は、データ分析と安全なシステム設計の二つを研究の柱として紹介した。インターネットやダークネット、各種ログの分析による脅威の検知・可視化に加え、OT・産業用IoT・制御システムの安全性や侵入テストなどに取り組んでいる。
8. バージニア工科大学のCommonwealth Cyber Initiative（CCI）は、研究、イノベーション、人材育成を通じて州の経済に貢献する取り組みを説明した。大学間のネットワーク、研究成果の事業化、スタートアップ支援、インターンシップなどを通じ、サイバーセキュリティ人材の不足に対応している。
9. CCIの国際活動では、日本との協力や海外でのワークショップ、研究交流、人材育成の事例が紹介された。国際共同研究の波及効果を重視し、参加者に新たな協力や交流を呼びかけた。

9. International collaboration was presented as a way to strengthen research impact and develop talent. Examples included partnerships with Japan, joint research and workshops, laboratory exchanges, and training initiatives. The panel closed by inviting further collaboration among universities, companies, and government agencies.	

D1-S11-12 Speeches from Japanese Government 14:45–16:00 JST

Session: Speeches from Japanese Government Speaker: D1-S11-12 ONODERA Kenichi (Deputy Director General for Cyber Affairs Bureau, National Police Agency)	セッション：日本政府からのスピーチ 登壇者：D1-S11-12 小野寺 健一 (警察庁長官官房審議官 サイバー警察局担当)

1. The slides survey threats ranging from suspected state-linked cyberattacks and ransomware to online fraud, misuse of IoT devices and harmful online activity. They highlight the potential misuse of rapidly advancing AI and the effects of ransomware on business operations and supply chains.
2. The WaterPlum attribution diagram links WaterPlum and North Korean IT workers to the 313 General Bureau under the Workers' Party of Korea's Munitions Industry Department. It distinguishes cryptocurrency theft through recruitment impersonation from false-identity job applications by North Korean IT workers, supported by remote access, laptop farms and enablers.
3. The police strategy combines investigation and arrests, damage prevention and mitigation, and the development of personnel, tools and research capabilities. The slides present consultation and apprehension as mutually reinforcing elements of deterrence.
4. The active cyber defense diagram shows coordination among police, the Cabinet Secretariat and Cabinet Office, and the Ministry of Defense and Self-Defense Forces. It depicts remote access and neutralization measures with oversight and prior approval, as well as consultation with the Foreign Minister for servers or computers outside Japan.
5. Cyber workforce measures include developing specialized personnel and drawing on technical officials and private-sector expertise. The slides describe the use of advanced analytical knowledge and recruitment of experienced specialists to strengthen police capabilities.
6. The Phobos and 8Base example presents international cooperation and analysis supporting the development of a ransomware decryption tool made available through No More Ransom. The slides also reference international joint actions against major ransomware-as-a-service groups.
7. Public-private cooperation includes information exchange, advisory support, joint training and security assessments involving critical infrastructure operators and companies with advanced technologies. The Japan Cybercrime Control Center is also included in the partnership framework.
8. The slides describe police consultation services and a unified online reporting portal for cyber incidents. Consultation is available regardless of whether a victim report has been filed, enabling preventive guidance and investigative responses as appropriate.

1. 小野寺氏は、サイバー空間の脅威は深刻であり、高度な技術を悪用した攻撃、インターネットを犯罪基盤とする詐欺など、違法・有害情報、AIの悪用といった課題を挙げた。
2. 国家の関与が疑われる攻撃への対応として、国内関係機関や外国の機関と連携し、攻撃の実態を公表する取り組みを紹介した。平素からの連携を積み重ね、緊急時にも機能させることが重要だと述べた。
3. ランサムウェアや大規模な個人情報漏洩は、企業活動や国民生活に大きな影響を与えると説明した。サイバーセキュリティを経営課題として捉える必要があるとした。
4. 警察の取り組みを、検挙、未然防止・被害拡大防止、それを支える基盤整備として説明した。事案の把握や事業者への情報提供、信頼関係の構築、国際捜査を相互につなげて対応する考えを示した。
5. アクセス無害化措置について、放置すれば生命・身体・財産に重大な危害が生じる恐れがあり、緊急の必要がある場合などの要件を説明した。知識・能力を備えた指名された担当者が実施し、独立機関の承認を受けるなど、適正性を確保する仕組みがあると述べた。
6. 事案に応じて警察と防衛省・自衛隊が対応し、内閣官房の調整の下で連携する考えを示した。また、専門人材を集め、高度なサイバー犯罪や国際捜査に対応する体制を紹介した。
7. ランサムウェアをめぐる国際共同捜査で、日本警察が被疑者の特定や、暗号化されたデータの復号ツールの開発に貢献した事例を紹介した。
8. 産業界、学術機関、警察などが情報を集約・分析する連携や、地域の重要インフラ事業者との協議会、情報共有、共同対処訓練を通じた協力を説明した。
9. 警察への相談は被害届の有無にかかわらず必要な対応につながると説明し、オンラインの相談窓口にも言及した。被害を把握した際は、一人で抱え込まず速やかに相談・通報するよう呼びかけた。
10. 早期の相談・通報は捜査だけでなく、被害拡大の防止や復旧に向けた調査にも役立つと述べた。平時からの官民連携と多様な主体との協力が、当事者だけでなく社会全体のサイバーセキュリティ向上につながると強調した。

9. The conclusion emphasizes that prompt reporting and consultation when a breach is recognized can support investigations, prevent further damage and aid recovery. Continuing cooperation among agencies, industry groups and businesses is presented as essential to stronger cybersecurity and resilience.	

D1-S11-10 Speeches from Japanese Government 14:45–16:00 JST

Session: Speeches from Japanese Government Speaker: D1-S11-10 KAWANO Masatoshi (Deputy Director-General for Policy Planning and Supervisory, National Cybersecurity Office (NCO))	セッション：日本政府からのスピーチ 登壇者：D1-S11-10 川野 真稔 (国家サイバー統括室 内閣審議官)

1. The presentation outlines Japan's efforts to strengthen its cyber response capabilities through legislation, a renewed cybersecurity strategy and changes to government structures. It links these reforms to the goal of greater national resilience through public–private and international cooperation. 2. The slides distinguish the main elements of active cyber defense: stronger public–private partnerships, remote access and neutralization measures against malicious servers, and the use of communications data on a clear legal basis. They describe different implementation stages for these elements. 3. The Public-Private Cyber Community is designed to build trust through two-way information sharing and joint action. Its activities include sharing sensitive information with limited groups under protective rules, collaborating on specific threats, and sharing sanitized information with all community members. 4. Critical asset notifications and incident reports are intended to produce actionable support for essential infrastructure operators. The government can cross-reference asset information with vulnerability information, analyze reported incidents, and issue alerts and advice to help prevent damage from spreading. 5. Common cybersecurity standards aim to raise the baseline of protection across critical infrastructure sectors while encouraging risk-based initiatives. The presentation describes a cycle of planning, implementation, analysis and improvement, supported by stronger incident response, information sharing and risk management. 6. A cybersecurity workforce framework covers roles extending beyond technical operations to strategy, governance, legal affairs, audit, education and research. The slides present it as voluntary guidance for diverse stakeholders, with proficiency levels and links to domestic and international frameworks. 7. Project YATA-Shield addresses the increasing speed and scale of AI-enabled cyberattacks. The slides emphasize management leadership, fundamental safeguards, vulnerability detection and patch management, alongside workforce development, AI security research and cooperation with international partners and AI developers.	1. 国家サイバー統括室（NCO）が関係省庁を総合調整し、政府全体のサイバーセキュリティ政策を取りまとめる役割を説明した。対応能力の強化に向けた法整備、NCOの設置、新たな戦略の策定など、最近の政策を紹介した。 2. 官民連携の基盤となる協議会の整備に加え、基幹インフラ事業者によるインシデント報告や重要なシステムの届出が制度化されたと説明した。アクセス無害化措置は、NCOの総合調整の下、警察と防衛省・自衛隊が事案や法的要件に応じて実施すると述べた。 3. 基幹インフラを守るには官民の強固な信頼関係が必要であり、政府が一方的に情報を集めるのではなく、双方に有益な情報を共有することが重要だと強調した。 4. 情報の性質に応じ、信頼できる限定的な集団や個別の相手と共有する方法と、機微な内容を処理して広く共有する方法を使い分けると説明した。製品の脆弱性情報を、まず開発・提供元に伝える例を挙げた。 5. 協議会では既にインシデントに関する技術情報などを共有していると述べた。今後は届け出られた資産と政府が持つ脆弱性情報を照合する取り組みや、次の攻撃を防ぐための情報共有を進めたいとした。 6. 平時の備えとして、重要インフラの統一的なセキュリティ基準を紹介した。所管省庁による実行計画と各業界の対策を、状況把握・分析・評価につなげ、水準を高めていく方針を示した。 7. 組織のサイバーセキュリティに必要な多様な役割を整理した人材の枠組みを紹介した。企業やサービス提供者が、強化すべき機能と人材の充足・不足を把握するために活用してほしいと述べた。 8. AIを想定した対策では、経営陣が経営課題として必要な投資や人材配置を進め、基本的なセキュリティ対策を徹底することを重視した。また、AIを活用して政府機関の脆弱性を検査する取り組みを紹介した。 9. PQCへの移行に向けたロードマップを策定する予定だと説明した。海外で重要なシステムの移行期限を早める動きに触れ、日本でも重要なシステムの早期移行を検討することが課題だと述べた。 10. 被害企業への支援、情報収集と的確な発信、アクセス無害化措置を含む対応手段の戦略的実施、システムの脆弱性検証という四つの指示に基づき、翌週中を目途に政府の対策パッケージをまとめる予定だと述べた。関係省庁、民間、海外の関係者との協力を求めた。

8. The presentation identifies post-quantum cryptography as a transition involving national security, industrial policy, service continuity and international cooperation as well as technology. It describes Japan's policy goal of transition in government and related agencies by 2035 in principle, with a roadmap to be formulated in fiscal year 2026.	

D1-S11-6 Speeches from Japanese Government 14:45–16:00 JST

Session: Speeches from Japanese Government Speaker: D1-S11-6 TAKANO, Masanori (Director, Cyber Security Policy Division, Foreign Policy Bureau, Ministry of Foreign Affairs)	セッション：日本政府からのスピーチ 登壇者：D1-S11-6 髙野 雅範 (外務省 総合外交政策局サイバー安全保障政策室長)

1. Mr. Takano identified three pillars of cyber diplomacy aimed at achieving a free, fair, and secure cyberspace: promoting the rule of law, strengthening deterrence, and supporting capacity building.
2. He explained Japan's position that existing international law also applies to activities conducted through cyberspace. He stressed the importance of implementing the UN-adopted norms of responsible State behavior and stated that Japan would also work to promote the rule of law within the Global Mechanism framework.
3. To strengthen deterrence, he emphasized the importance of coordinated public attribution by multiple countries to identify and publicly disclose attackers' methods and identities. He stated that close cooperation, including among diplomatic authorities, would continue with a view to imposing costs on attackers.
4. He noted that cyberspace has no borders and that vulnerabilities in certain countries or regions can pose risks to the international community as a whole. He explained that Japan would advance capacity-building assistance in the Indo-Pacific, particularly in ASEAN countries, drawing on the expertise of relevant ministries and agencies.
5. He cited tabletop exercises and workshops conducted in cooperation with the Ministry of Internal Affairs and Communications at the ASEAN-Japan Cybersecurity Capacity Building Centre in Thailand.
6. He stated that international cooperation is essential to effectively advancing the three pillars. Through bilateral cyber consultations and multilateral meetings, Japan shares strategies and regional challenges and discusses cooperation to defend against and deter cyber threats.
7. He explained that the Ministry of Foreign Affairs also has a role in active cyber defense. He stated that the ministry would contribute to the consideration of access and neutralization measures from a foreign policy perspective and help ensure that they are carried out within the bounds permitted under international law.
8. He expressed Japan's intention to strengthen its diplomatic efforts in cooperation with the public and private sectors to achieve a free, fair, and secure cyberspace.

1. 髙野氏は、自由で公正かつ安全なサイバー空間の実現を目指すサイバー外交の三本柱として、法の支配の推進、抑止力の向上、能力構築支援を挙げた。
2. 日本はサイバー空間を利用した行為にも既存の国際法が適用されるとの立場を取っていると説明した。国連で採択された責任ある国家の行動規範を実践することが重要であり、グローバルメカニズムの枠組みでも法の支配の推進に取り組むと述べた。
3. 抑止力を高めるため、攻撃者の手法や主体を特定して公表するパブリックアトリビューションを、複数国が連携して行うことの重要性を強調した。攻撃者にコストを課す観点から、外交当局間を含む緊密な協力を続けると述べた。
4. サイバー空間には国境がなく、一部の国・地域の脆弱性が国際社会全体のリスクになり得ると指摘した。インド太平洋、特にASEAN諸国を中心に、関係省庁の専門性を生かした能力構築支援を進めると説明した。
5. タイの日ASEANサイバーセキュリティ能力構築支援センターで、総務省と連携した机上演習やワークショップなどを実施している例を紹介した。
6. 三本柱を実効的に進めるには国際連携が不可欠だと述べた。各国とのサイバー協議や多国間の会合を通じ、戦略や地域課題を共有し、脅威の防御・抑止に向けた協力を議論していると説明した。
7. 能動的サイバー防御に関しても外務省が役割を担うと説明した。アクセス無害化措置に外交政策の観点から関与し、国際法上許容される範囲内での実施を確保する観点から検討すると述べた。
8. 自由で公正かつ安全なサイバー空間の実現に向け、官民と連携して外交的な取り組みを強化する考えを示した。

D1-S11-9 Speeches from Japanese Government 14:45–16:00 JST

Session: Speeches from Japanese Government Speaker: D1-S11-9 NAKANO Shigeaki (Defense Councilor (Deputy Director General for Cyber Security and Information Technology Management), Minister's Secretariat, Ministry of Defense)	セッション：日本政府からのスピーチ 登壇者：D1-S11-9 中野 滋明 (防衛省大臣官房サイバーセキュリティ・情報化審議官)

1. The slides present the Ministry of Defense and Self-Defense Forces' cybersecurity efforts in three areas: strengthening their own capabilities, cooperating with critical infrastructure providers and international partners, and supporting cyber defense in the defense industry. These efforts aim to preserve mission capability under cyberattack and contribute to Japan's wider cybersecurity. 2. Workforce development combines planned expansion of cyber units with education, training and practical experience. The slides describe learning opportunities within SDF schools, specialized education for younger personnel, study at universities and placements with private cybersecurity companies. 3. The Ministry applies a Risk Management Framework to manage cybersecurity risks throughout system lifecycles. Measures include annual risk assessment, authorization to operate and vulnerability assessments, with penetration testing for mission-critical systems. 4. International cooperation includes dialogue, information exchange and joint exercises with the United States and other partners. The slides emphasize interoperability, shared threat awareness and coordination in responding to cyberattacks. 5. Locked Shields is presented as an opportunity for realistic international cyber defense training and collaboration across government, industry and academia. The slides describe Japan's participation with Lithuania, the involvement of cyber reserve personnel and the Ministry's coordinating role for the Japanese team. 6. The active cyber defense framework shown in the slides combines public-private information sharing, analysis of communications data on legal grounds and remote access and neutralization measures when necessary. It depicts coordination among the Cabinet Secretariat, police, the Ministry of Defense and other agencies, including prior consultation with the Ministry of Foreign Affairs for access to servers outside Japan. 7. Threat hunting is described as continuously searching networks for latent threats on the assumption that an adversary may already be present. The slides describe plans to use capabilities developed by the Ministry and Self-Defense Forces to support wider government efforts, including protection of critical infrastructure and other systems supporting economic activity.	1. 中野氏は、防衛省・自衛隊の軍事的な観点からサイバーセキュリティを説明した。任務を遂行できる体制と、防衛産業のサイバー防衛を支える体制の構築が求められていると述べた。 2. ロシアによるウクライナ侵攻前のサイバー攻撃を例に、武力攻撃に先立って社会生活や防御側の軍事能力が妨げられ得ると指摘した。有事だけを想定するのではなく、平時から対応する必要性を説明した。 3. 新たな法律の施行により、自衛隊が有事に備えて培ってきたサイバー能力を、必要に応じて平時にも用いることになったと説明した。自衛隊自身だけでなく、民間の重要インフラや公益性の高い事業を守る活動にも言及した。 4. サイバー専門部隊の規模と能力を拡充し、各種ネットワークを維持・管理する人材も育成していると紹介した。基礎から中級程度の教育は主に自衛隊内で行い、より高度な教育には国内外の大学や企業への派遣を活用すると述べた。 5. ネットワーク内には既にリスクが存在する可能性があるという前提で、継続的に検査・点検する考え方を説明した。基地間の回線だけでなく、戦車、航空機、艦船などをつなぐ多様なネットワークも対象になると述べた。 6. 攻撃者が世界各地のサーバーを利用することから、同盟国・同志国との連携が重要だと強調した。国境を越えた協力を自衛隊の取り組みの一つに位置づけた。 7. サイバー演習「ロックドシールズ」への参加を紹介した。現地と遠隔の双方から参加し、学術界や産業界と日本チームを組むとともに、リトアニアとも協力したと説明した。 8. ネットワークに脅威が潜んでいると想定して内部から探し出す、脅威ハンティングの能力を磨いていると述べた。有事に備えて培った能力を、困難に直面する民間の支援にも役立てる考えを示した。 9. 今後の柱として、平時・有事を通じた能力向上、NCOや警察、同盟国・同志国との連携による重要インフラの防護、防衛産業のサイバー防衛を支える能力の強化を挙げた。

8. The conclusion reiterates that increasingly sophisticated threats require stronger cyber defense capabilities. Improving internal capabilities, cooperation with infrastructure providers and international partners, and support for the defense industry are presented as complementary contributions to national cybersecurity.	

D1-S11-4 Speeches from Japanese Government 14:45–16:00 JST

Session: Speeches from Japanese Government Speaker: D1-S11-4 NIKAMI Hideo (Assistant Director-General, Second Intelligence Department, Public Security Intelligence Agency)	セッション：日本政府からのスピーチ 登壇者：D1-S11-4 二上 英生 (公安調査庁 調査第二部長)

1. The slides frame state-supported cyberattacks as a national-security threat. They describe military, intelligence and security agencies pursuing persistent operations, sometimes using criminals or private hackers as outside collaborators, and warn that Japanese companies can face serious risks. 2. The comparison of state-linked threats associates Chinese actors with information theft, disinformation and reconnaissance; North Korean actors with cryptocurrency theft, intelligence collection and retaliation; and Russian actors with information manipulation and disruptive or destructive operations. These are presented as assessments in the slides. 3. The China-related examples include Salt Typhoon and public attribution or enforcement actions by U.S. authorities. A MirrorFace diagram illustrates phishing messages impersonating real individuals or organizations, malicious attachments, connections to an attacker-controlled server and subsequent malware downloads. 4. The North Korea section presents cryptocurrency theft and spear-phishing examples, together with public warnings and international coordination. It includes the TraderTraitor, Kimsuky and WaterPlum cases as examples of the threats discussed. 5. A separate diagram depicts North Korean IT workers using false identities on crowdsourcing platforms to obtain work and request cryptocurrency payments. The slide identifies funding for nuclear and missile programs and abuse of legitimate privileged access as risks associated with these activities. 6. The Russia section presents attacks on critical infrastructure and international attribution or sanctions. An illustrative attack flow includes initial access, persistent presence, reconnaissance, credential theft, lateral movement, access to monitoring and control systems, malware deployment and disruption or data destruction. 7. The concluding slide describes PSIA as part of Japan's intelligence community, providing intelligence products to the Prime Minister's Office, Cabinet Secretariat and other relevant organizations. It emphasizes collecting and analyzing human intelligence and sharing it in a timely and appropriate manner.	1. 国家が関与・支援するサイバー脅威を、インテリジェンス機関の視点から説明した。軍や情報機関が自ら活動するだけでなく、民間の攻撃集団や企業も利用し、任務の達成まで継続する点に脅威があると述べた。標的は政府機関だけでなく民間にも及ぶとした。 2. 中国に関する脅威の特徴として、情報窃取や偽情報の拡散を挙げ、台湾や日本に対してもこうした活動があるとの認識を示した。通信事業者を狙った攻撃と、各国による攻撃主体の公表などの対応を紹介した。 3. 標的と考え方が近い相手を装ってメールを送り、添付ファイルを開かせて感染させる手口を説明した。侵害された端末は情報窃取に使われるだけでなく、次の標的への踏み台となり、関連組織へ脅威が広がる可能性があると指摘した。 4. 北朝鮮に関する脅威では、情報窃取に加え、暗号資産などによる外貨獲得が主要な目的との見方を示した。得られた資金が核・ミサイル開発に使われることへの懸念を述べた。 5. 暗号資産取引所への攻撃事例として、ウォレット管理サービスの開発者を狙い、フィッシングを通じて情報を入手して侵入する経路を紹介した。こうした脅威への対応で各国が連携していると説明した。 6. 北朝鮮のIT労働者による身分偽装と仕事の受注について、偽の身分だけでなく、協力者の身分や代理面接を利用する手口もあると説明した。企業が気づかないうちに北朝鮮へ資金が流れることへの懸念を示した。 7. ロシアに関する脅威として、情報窃取や偽情報の拡散に加え、ウクライナ戦争に関連する破壊的な活動への認識を示した。重要インフラを狙う攻撃の例と、各国が連携した対応に触れた。 8. 重要インフラへの攻撃では、フィッシングや脆弱性を利用して侵入し、長期潜伏、情報窃取、権限取得、横展開などを進めると説明した。これらの活動は必ずしも順番通りではなく、同時並行で進み得ると指摘した。

8. PSIA's stated responsibilities include advancing the collection and analysis of information on cyber threats, particularly those involving state support or participation, to help protect society, economic activity and people's safety.	

D1-S11-11 Speeches from Japanese Government (second block) 16:35–18:35 JST

Session: Speeches from Japanese Government (second block) Speaker: D1-S11-11 IIMURA Hiroyuki (Minister's Secretariat, Ministry of Internal Affairs and Communications (MIC), Deputy Director-General for Cybersecurity and Information Technology Management)	セッション：日本政府からのスピーチ（後半） 登壇者：D1-S11-11 飯村 博之 (総務省 大臣官房 サイバーセキュリティ・情報化審議官 併任 サイバーセキュリティ統括官室)

1. The slides describe MIC's role in securing communications networks and the ICT, local-government and postal sectors. Networks are both critical infrastructure supporting society and the infrastructure of cyberspace itself, requiring cooperation with NICT on research, monitoring, analysis, workforce development and awareness.
2. The NOTICE project addresses vulnerable and malware-infected IoT devices that can be used in botnet attacks. NICT works with internet service providers to identify affected devices, alert owners and encourage remediation, with participation by vendors, integrators and other stakeholders.
3. To reduce excessive reliance on foreign security technology and threat intelligence, the slides present CYNEX as an industry–academia–government hub. NICT shares data, research expertise, testing environments and training knowledge to support domestic technology development and response capabilities.
4. Workforce initiatives emphasize practical exercises and talent development through CYDER and SecHack365. The slides also describe capacity building in ASEAN and Pacific island countries and territories, drawing on Japanese training expertise and cooperation with international partners.
5. For sensitive communications, the slides advocate combining post-quantum cryptography with quantum key distribution. They describe research, standardization and demonstrations aimed at real-world QKD deployment, including long-distance, interconnected-network and multi-vendor testing.
6. The AI-related section describes faster vulnerability discovery and the risks of AI-enabled attacks, alongside threats to AI systems themselves. It presents executive-led security, basic controls, risk-based vulnerability response and advanced measures such as threat hunting as important responses. The slides explicitly note uncertainty about AI's contribution to the recent increase in attacks.
7. Following data breaches, the slides emphasize prompt patching, stronger authentication, supply-chain controls and sound data management. They also explain that analysis of public smartphone applications can expose backend servers to targeted attacks, making server-side authentication, authorization, input validation and monitoring essential.

1. 飯村氏は、総務省が情報通信、地方行政、郵便の重要インフラ分野を所管すると説明した。情報通信は重要インフラであると同時にサイバー空間そのものを支えるため、NICTと連携した研究開発、人材育成、脅威の観測・分析が重要だと述べた。
2. ウェブカメラやルーターなどのIoT機器が攻撃に悪用されるリスクを挙げた。感染した機器や容易に推測できる認証情報を使う機器などを発見し、設置者に注意喚起して対処を促す取り組みを紹介した。
3. セキュリティ製品・サービスや脅威の一次情報を海外に依存する状況を課題として挙げた。NICTが収集・分析する脅威情報や人材育成の知見を民間に開放し、国産技術の開発と自ら検知・対処する能力の向上につなげる基盤を説明した。
4. 人材不足への対応として、実際の機器を操作しながらインシデントに対処する実践的な演習や、若手向けの育成を紹介した。こうした知見をASEANや太平洋島嶼地域にも展開し、能力構築を支援していると述べた。
5. 量子コンピューターを見据えた情報保護として、PQCへの移行と量子暗号通信（QKD）の研究開発を説明した。特に重要な情報には両者を組み合わせることが必要ではないかとの考えを示した。
6. 高性能AIにより脆弱性の発見が容易・高速になり、専門知識のない者でも短時間に大量の攻撃を行えるようになることへの懸念を示した。経営層のリーダーシップ、基本的な対策の徹底、脆弱性情報の収集とリスクに応じた対応を求めた。
7. 最近の情報漏洩事案を踏まえ、速やかなパッチ適用、子会社や委託先を含むサプライチェーン全体での対策、適切なデータ管理を呼びかけた。データの暗号化や保有情報を減らすことは、侵害時の被害を抑えることにつながると説明した。
8. 公開されたスマートフォンアプリの解析から、その背後のサーバーを特定して攻撃する可能性について、NICTの分析を紹介した。個々の設備の脆弱性を見つける過程にAIが使われている可能性にも言及した。
9. 通信分野の安全性について、環境変化を踏まえた包括的な対策を検討していると述べた。防御を固めるだけでなく、乗っ取られた一般利用者の機器など、攻撃の踏み台を減らして攻撃側の力を弱めることも重要だと説明した。
10. 家庭用機器が利用者の知らないうちに攻撃へ悪用される例を挙げ、警察庁と共同の対策を進めていると紹介した。高度化・複雑化する攻撃への対策を年内に取りまとめ、可能なものから速やかに実施する方針を示した。

8. The slides describe a telecommunications data-protection and security study group examining technical, organizational and regulatory measures in light of frontier AI and software- and cloud-based services. They also introduce a separate study group on cooperation and effective responses to increasingly sophisticated cyberattacks. 9. Compromised home IoT devices and residential proxies are presented as infrastructure that attackers exploit to conceal and distribute their activity. A public-private alliance is examining device analysis, user warnings, blocking attack relays and coordinated outreach, with the aim of reducing the infrastructure available for attacks.	

D1-S11-2 Speeches from Japanese Government (second block) 16:35–18:35 JST

Session: Speeches from Japanese Government (second block) Speaker: D1-S11-2 HASHIMOTO, Katsukuni (Director, Commerce and Information Policy Bureau, Cybersecurity Division, Ministry of Economy, Trade and Industry)	セッション：日本政府からのスピーチ（後半） 登壇者：D1-S11-2 橋本 勝国 (経済産業省 商務情報政策局 サイバーセキュリティ課 企画官)

1. The slides describe ransomware, supply-chain attacks and AI-related risks as major cybersecurity concerns. They emphasize that incidents can spread between organizations, making protection across supply chains necessary rather than relying only on individual companies' defenses.
2. Small and medium-sized enterprises face both resource constraints and uncertainty about which security products to select, whether current measures are adequate and where to begin. The slides present practical guidance and support as important elements of improving their security.
3. The Cyber/Physical Security Framework organizes risks across connections between organizations, between physical and cyber spaces, and within cyberspace. METI's policy combines supply-chain measures, secure-by-design products and software, incident response support and stronger cybersecurity supply capabilities.
4. Guidance covers executives, practitioners, SMEs and particular industrial sectors. In response to advanced AI, the slides emphasize management leadership, prompt action on identified vulnerabilities, thorough basic measures and accelerated transition toward zero trust.
5. The Cybersecurity Supporters Services package brings together consulting, monitoring, emergency support and basic cyber insurance for SMEs. The slides also describe a supply-chain cybersecurity evaluation scheme under consideration, intended to make security measures more visible to business partners.
6. Secure-by-design initiatives include the JC-STAR labeling scheme for IoT products and software bills of materials. SBOM guidance and international collaboration are presented as ways to improve software-component visibility and vulnerability management.
7. Incident response support includes IPA's J-CRAT, which provides expert analysis and assistance for targeted attacks, and JPCERT/CC, which coordinates cybersecurity incidents and cross-border cooperation.
8. Research and development priorities include collecting and analyzing cyberspace information, protecting devices and systems, and developing shared foundations for information exchange and skilled personnel. The slides include AI-enabled security and post-quantum cryptography among the research areas.

1. 橋本氏は、経済産業省のサイバーセキュリティ政策を説明した。ランサムウェアやサプライチェーンへの攻撃に加え、AI利用に関わるリスクが課題となっていると述べた。
2. 自社の対策だけでは、取引先や関連会社を通じた侵入を防ぎきれないため、サプライチェーン全体を守ることが重要だと強調した。中小企業には、対策の必要性を感じても、サービスの選び方や具体的な実装方法が分からないという課題があると説明した。
3. サイバーフィジカルセキュリティ対策フレームワークを紹介した。現実世界とサイバー空間のつながりを整理し、攻撃が思わぬ場所に影響する構造を把握するためのものだと説明した。
4. 政策の柱として、サプライチェーン全体の強化、セキュア・バイ・デザイン、インシデント対応体制の支援、セキュリティの供給能力の強化を挙げた。中小企業向けや産業分野別のガイドラインを整備していると述べた。
5. AIを巡る環境変化に対し、企業トップの主導、脆弱性への迅速な対応、基本的な対策の徹底、ゼロトラストの取り組みを加速するよう呼びかけていると説明した。
6. 中小企業向けに、監視、緊急時の技術者の駆け付け、サイバー保険などをまとめて提供する「サイバーセキュリティお助け隊」サービスを紹介した。
7. 企業の対策状況を可視化するサプライチェーン向け評価制度の開始を目指していると述べた。また、IoT機器のセキュリティ対策を示すラベリング制度や、SBOMなどを通じた設計段階からの安全性向上を紹介した。
8. 高度な攻撃に関する情報提供や、各国の対応組織との協力などを通じ、国内のサイバー攻撃への対処能力を高める体制を説明した。
9. 情報の収集・分析、デバイスやシステムの防御、共通基盤に関する研究開発を紹介した。成果を社会に役立てることを目指していると述べた。
10. 重要インフラなどの企業から人材を受け入れ、各社のセキュリティの中核を担う人材を育てる教育プログラムを紹介した。米国や欧州と共同で行うサイバーセキュリティ演習にも言及した。

9. Workforce development includes IPA's Industrial Cyber Security Center of Excellence, which trains personnel with both IT and operational-technology skills. International lectures, practical exercises, scenario workshops and networking also support industrial cybersecurity capacity in the Indo-Pacific.	

D1-S11-8 Speeches from Japanese Government (second block) 16:35–18:35 JST

Session: Speeches from Japanese Government (second block) Speaker: D1-S11-8 OKUDA Naohiko (Deputy Director General, Digital Agency)	セッション：日本政府からのスピーチ（後半） 登壇者：D1-S11-8 奥田 直彦 (デジタル庁 審議官)

1. The speaker described security as an important part of the Digital Agency's work alongside digital reform. Activities include risk evaluation, data collection, education and training, and issuing guidelines to support system operators.
2. Security by design was presented as a central guideline. It covers risk analysis, security requirements, supply-chain risks, vulnerability analysis, the roles of those involved, and security checklists.
3. The speaker said perimeter defense alone is insufficient and described the inclusion of zero-trust architecture in the agency's security approach.
4. Cross-system monitoring and visualization were described as ways to understand risks. Tracking software versions on individual terminals helps manage vulnerabilities, while patches require checks because they can change system behavior.
5. Operational dashboards and log analysis help identify events, investigate the causes of outages, and communicate with system managers. Incident status, countermeasures, outages and service degradation can be reported to management to provide an overall view.
6. The speaker outlined a security evaluation framework for cloud services handling sensitive information. Common standards and audits can reduce the detailed checks government bodies must perform themselves when using registered services.
7. The misuse of high-performance AI was described as a threat that can increase the speed and scale of attacks. An agency-wide AI security working group brings together relevant departments to address these issues.
8. The agency is developing an environment and organizational structure for AI-enabled vulnerability analysis, alongside work on AI governance. Findings and knowledge from the analysis are being organized and shared with other stakeholders.
9. The speaker described conducting AI-enabled analysis in a government-cloud environment designed to prevent information from leaking outside.
10. Because the agency's information systems are important to daily life and public administration, it has established a dedicated security department and actively recruited private-sector experts. Continued security efforts were emphasized.

1. デジタル庁は、誰一人取り残されない、人に優しいデジタル化を使命とし、行政サービスを国民が使いやすいものにすることを目指していると説明した。デジタル社会の基盤や各省庁が共通利用するシステムの運用において、セキュリティ確保を重視すると述べた。
2. システム監視、情報の収集・分析・共有、リスク評価、脆弱性の確認、教育・訓練など、幅広い対策を実施していると紹介した。自庁のシステムだけでなく、ガイドラインの策定・公表を通じて政府全体の安全性も支援すると説明した。
3. セキュリティ・バイ・デザインのガイドラインについて、開発の各工程で確認すべき項目を具体化していると説明した。企画時のリスク分析と要件定義、調達時のサプライチェーンリスクの考慮、チェックリストなどを挙げた。
4. 境界防御だけでは十分でないとして、ゼロトラストの考え方に関する方針を紹介した。また、構築時と定期的な脆弱性診断を扱うガイドラインや、診断の発注・評価、修正内容の確認などの支援を説明した。
5. システムを横断してリスク情報を統合・可視化する仕組みを紹介した。端末のソフトウェアのバージョンなどを把握し、重大な脆弱性が判明した際の対応対象の抽出や、対策状況の管理、優先順位の判断につなげると述べた。
6. ログやシステムの挙動を分析し、不審なイベントを検知した際には担当者へ通知する仕組みを説明した。稼働状況や停止・復旧、インシデント対応を可視化し、幹部への報告や今後のシステム・投資計画にも活用すると述べた。
7. 政府が機密性を要する情報を扱うクラウドサービスを調達する際の、セキュリティ評価制度を紹介した。共通の基準と監査によって確認を行い、登録されたサービスを利用することで、各機関の確認作業を簡略化する仕組みだと説明した。
8. 高性能AIが攻撃に悪用されることで、攻撃の速度や規模が増す脅威を挙げた。組織横断のAIセキュリティの検討体制を設け、AIによる脆弱性分析の環境・体制や、AIガバナンスの基盤づくりを進めていると述べた。
9. 政府情報システムを対象としたAIによる脆弱性分析と、その結果・知見の整理や政府機関との共有を紹介した。外部への情報漏洩を防ぐことに配慮した環境で分析を進めていると説明した。
10. 国民生活や行政の業務を支える重要なシステムを運用するため、専門部署を設け、民間の専門人材も積極的に採用していると述べた。利用者が安心してサービスを使えるよう、引き続き対策を進める考えを示した。

D1-S11-5 Speeches from Japanese Government (second block) 16:35–18:35 JST

Session: Speeches from Japanese Government (second block) Speaker: D1-S11-5 SAWAKI Kiyoshi (Secretary General, Personal Information Protection Commission)	セッション：日本政府からのスピーチ（後半） 登壇者：D1-S11-5 佐脇 紀代志 (個人情報保護委員会 事務局長)

1. The speaker linked personal information protection with cybersecurity: realizing the benefits of data requires understanding and managing its risks. The commission's work includes policy, compliance oversight, international cooperation, complaint handling and public awareness.
2. The presentation described international discussions on trusted cross-border data flows, emerging technologies and enforcement cooperation. Topics included smart glasses and AI agents, sharing enforcement cases, and building a repository of published cases.
3. Age assurance can help protect children online, but indiscriminate use can threaten rights and freedoms. The speaker stressed that such technologies should be accompanied by appropriate privacy safeguards.
4. Three mechanisms for safer cross-border personal data transfers were outlined: mutual adequacy arrangements, third-party certification, and contracts between businesses. The speaker also described efforts to expand international cooperation, including with ASEAN.
5. Memoranda of cooperation with overseas data protection authorities support cross-border enforcement and institutional capacity. The commission prioritizes partners with close economic and social ties, substantial personal data flows, or shared leadership in safer international data transfers.
6. One breach example involved an attacker gaining a remote worker's trust through social media and using a malicious attachment to compromise internal systems. Another involved insufficiently secured VPN devices. The speaker emphasized awareness and basic security measures for remote work.
7. Further examples involved SQL injection and malicious website code that redirects users to fraudulent sites. Proper website development, security maintenance, monitoring and timely action were presented as ways to reduce these risks.
8. The speaker called for management and governance systems that make basic security measures a consistent part of daily operations, rather than occasional actions.
9. The commission works with other government agencies, drawing on their different missions and specialist capabilities to address a wide range of cybersecurity risks.

1. 資料では、個人情報保護委員会を、個人情報の有用性に配慮しつつ個人の権利利益を保護する独立機関として紹介している。基本方針の策定・推進、監視・監督、国際協力、苦情あっせん、広報啓発などを担う。
2. 国際的な取組として、G7のデータ保護・プライバシー機関による議論を取り上げている。信頼性のある自由なデータ流通、スマートグラスやAIエージェントなどの先端技術、執行事例の共有と公開事例のレポジトリ構築が論点となっている。
3. 年齢認証はこどもの保護に役立つ一方、無差別な利用は個人の権利や自由を損なうおそれがある。資料は、適切なプライバシー保護と状況に応じた利用、収集・利用・保存期間の制限、透明性やセキュリティなどの配慮を示している。
4. 個人情報の越境移転について、日本と欧米の制度・枠組みを整理し、相互認証、グローバルCBPR、モデル契約条項などを通じたASEANとの協力を展開する今後の展望を示している。また、海外のデータ保護機関との協力覚書を通じ、法執行や個別事案に関する情報交換を強化する取組を紹介している。
5. サイバーセキュリティに関する取組では、個人情報の漏えい等の報告状況と、不正アクセス事案の原因分析を扱っている。ソフトウェアやID・パスワードの脆弱性、アクセス制御の設定ミスなどを課題として挙げている。
6. テレワークに関する事例として、SNSで接触した相手から受け取ったメールによる端末感染が社内ネットワークへ拡大したケースと、脆弱性対策を行わずに稼働したVPN機器から認証情報が漏えいしたケースを示している。
7. Webサイトを通じた漏えいの例として、悪質なサイトへ誘導するスクリプトを利用した攻撃と、SQLインジェクションによるデータベースへの不正アクセスを説明している。攻撃の経路と、情報漏えいや改ざんなどの被害を図示している。
8. 関係省庁・専門機関との連携では、インシデント発生時の報告、事実確認や原因究明、再発防止への助言に加え、平時の安全管理措置、教育研修、情報共有などの役割分担を整理している。
9. フォレンジック調査を有効に活用するため、平時からIT環境の台帳やネットワーク構成図を整え、ログを保管し、対応手順を整理することが重要だとしている。発生時には証拠保全を意識し、不用意な端末初期化を避け、適切に情報連携と封じ込めを行う。
10. 調査後は、フォレンジック調査の前提と結果の根拠を確認し、判明した事実を理解・評価した上で、原因に対応する再発防止策につなげるという考え方を示している。

10. Digital forensic investigations can help organizations review their defenses and prevent recurrence after unauthorized access. The commission's published guidance covers preparation, incident response, commissioning investigations and making effective use of their results.	

D1-S11-3 Speeches from Japanese Government (second block) 16:35–18:35 JST

Session: Speeches from Japanese Government (second block) Speaker: D1-S11-3 OKABE Fumiya (Deputy Director-General for Cybersecurity and Information Policy, MHLW)	セッション：日本政府からのスピーチ（後半） 登壇者：D1-S11-3 岡部 史哉 (厚生労働省 サイバーセキュリティ・情報化審議官)

1. Hospital networks were traditionally designed as closed environments, but external connections and cloud integration have increased over time. The speaker emphasized that knowing and controlling these connections is a central security issue. 2. Unknown users, devices missing from inventories and unused maintenance connections can leave hospitals unaware of external access routes. Internet-facing VPNs and firewalls are continually scanned for weaknesses, putting outdated systems at risk. 3. The speaker described consolidating and centrally managing external connections as a way to strengthen hospital security. Ransomware incidents involving such connections can lead to system shutdowns and recovery periods. 4. The Ministry of Health, Labour and Welfare's approach was organized around three areas: equipment and systems, inspections, and human resource development. 5. The presentation described work involving hospital management and system administrators, and preparing a list of external cybersecurity experts that healthcare institutions can consult when needed. 6. Cloud services can reduce operational workloads by providing specialist security capabilities and help strengthen healthcare institutions' cyber resilience. The speaker stressed that proper configuration and management remain necessary. 7. Cybersecurity was presented as essential to healthcare's digital transformation and to sustaining the benefits of digital technologies.	1. 医療DXによって電子カルテや医療情報の共有が進む一方、サイバーリスクも高まっていると説明した。閉じたネットワークだから安全という前提ではなく、実際の外部接続を把握・管理することが重要だと述べた。 2. リモート保守、VPN、クラウド連携などが積み重なり、接続構成が複雑になっていると指摘した。利用者不明の接続、管理台帳にない機器、不要になった回線、多要素認証のないリモートアクセスなどが、把握されない侵入口になり得ると説明した。 3. 医療機関のランサムウェア被害では、保守用VPNや委託事業者のリモートアクセスなどを起点に、内部へ被害が広がる例を紹介した。接続点の脆弱性が、システム停止、長期の復旧、多額の費用につながると述べた。 4. 外部接続点を整理・集約して一元管理することで、アクセス制御、多要素認証、ログ監視などを集中して適用できると説明した。可視性の向上によって、更新や脆弱性管理、不審なアクセスの早期発見も進めやすくなるとした。 5. 厚生労働省の取り組みを、設備、点検、人材育成の三本柱で紹介した。設備面ではネットワーク評価や外部接続の最適化を進め、多要素認証や情報資産管理などの対策の導入を支援すると述べた。 6. 点検では、保健所の立ち入り検査に外部専門家の活用も組み合わせ、医療機関が自ら気づきにくいリスクを発見して改善につなげる仕組みを説明した。 7. 人材育成では、経営層やシステム管理者向けの学習を通じた理解・対処能力の向上を紹介した。必要な時に相談できる外部専門家のリストを整備し、支援を受けやすい環境を作ると述べた。 8. クラウドは、専門事業者のセキュリティ機能を利用し、更新や脆弱性管理の負担を軽減する選択肢だと説明した。バックアップや復旧環境の確保にも役立ち得る一方、適切な設計・運用は引き続き必要だと強調した。 9. デジタル技術の恩恵を継続して得るには、サイバーセキュリティを医療DXの前提条件として捉える必要があると述べた。医療機関が持続的に安全性を確保できる環境づくりを進める方針を示した。

D1-S11-7 Speeches from Japanese Government (second block) 16:35–18:35 JST

Session: Speeches from Japanese Government (second block) Speaker: D1-S11-7 NAKAYAMA Yasuhiro (Deputy Vice-Minister for Cyber Security and Information Ministry of Land, Infrastructure, Transport and Tourism)	セッション：日本政府からのスピーチ（後半） 登壇者：D1-S11-7 中山 泰宏 (国土交通省大臣官房 サイバーセキュリティ・情報化審議官)

1. The presentation describes increasingly sophisticated cyberattacks against critical infrastructure, including risks from the malicious use of advanced AI. Incidents affecting Nagoya Port and Japan Airlines illustrate disruptions to cargo handling and flight operations. 2. MLIT's approach combines sector-specific security measures with cooperation between government and critical infrastructure operators. The slides emphasize leadership by senior management, reliable implementation of fundamental safeguards, and prompt vulnerability management that takes service continuity into account. 3. Common standards and sector-specific guidelines provide a basis for security measures. A self-assessment checklist helps operators review their arrangements, including internal rules, employee awareness, contractor oversight, unauthorized-access detection and incident-response exercises. 4. A consultation desk supports critical infrastructure operators with questions about improving safeguards, responding to incidents and objectively checking the status of their security measures. It provides advice and directs operators to appropriate support services. 5. When cyberattacks occur, MLIT can dispatch personnel with specialist expertise or provide remote support. Assistance covers initial response, limiting damage, interpreting technical findings, working with the operator's CSIRT and considering measures to prevent recurrence. 6. Attack Surface Management uses publicly available information to identify exposed assets and security weaknesses. The slides describe risk assessments, periodic reports and urgent vulnerability information to help operators prioritize action and explain risks to management. 7. The slides describe social media monitoring to detect possible signs of system failures or cyberattacks. Relevant information is shared within MLIT and with affected operators to support early countermeasures. 8. Cooperation with the Transportation ISAC supports information sharing across transport sectors, incident-response exercises, workforce development and organizational security measures. The slides emphasize collective defense and collaboration with other ISACs.	1. 中山氏は、交通や水道など幅広い重要インフラを所管する国土交通省では、各業界の実情に応じたサイバーセキュリティ対策が必要だと説明した。高性能AIの悪用を含め、攻撃の脅威が質・量ともに増大しているとの認識を示した。 2. 名古屋港のランサムウェア被害や航空分野のネットワーク障害などを挙げ、物流や利用者への大きな影響を説明した。名古屋港の事案は、港湾が重要インフラに指定される契機にもなったと述べた。 3. 新たな重要インフラの統一基準を踏まえ、分野ごとの特性に応じた安全ガイドラインを作成していると紹介した。NCOや有識者と連携して検討を進めると述べた。 4. 中小事業者を含む幅広い事業者向けに、情報セキュリティ対策の自己点検チェックリストを用意していると説明した。社内ルールと従業員への周知、委託先の管理状況、検知や訓練など、基本的な対策の実施を促すものだと述べた。 5. 重要インフラ事業者向けの相談窓口では、インシデントの有無にかかわらず、自社の対策や発生時の対応について相談を受け付け、専門家とも連携して支援すると紹介した。 6. インシデント時には、必要に応じて専門的知見を持つ職員などを派遣し、初動や被害拡大の防止などを支援すると説明した。事業者が必要とする段階に応じた支援を行うと述べた。 7. 重要インフラ事業者向けにASMを提供し、公開情報を基に脆弱性などを把握して、希望する事業者へ報告する取り組みを紹介した。緊急性の高い情報に加え、SNSなどから得たインシデントの予兆も迅速に共有すると述べた。 8. 交通ISACと連携し、業界横断の情報共有や官民対話を通じて、経営層などと最新の状況を共有し、対策の底上げを図っていると説明した。港湾や水道を含めた今後の連携のあり方も課題だと述べた。 9. 基本的な対策を徹底しながら、高度化する攻撃に対して追加で何が必要かを検討すると述べた。関係省庁、関係機関、学術界などと連携し、国土交通分野全体の安全性を高める方針を示した。

9. The presentation concludes by calling for thorough implementation of fundamental cybersecurity measures and stronger support coordinated across relevant ministries, agencies and organizations, with the aim of improving security and resilience throughout the sectors under MLIT's jurisdiction.	

D1-S11-13 Speeches from Japanese Government (second block) 16:35–18:35 JST

Session: Speeches from Japanese Government (second block) Speaker: D1-S11-13 OKI Kenji (Financial Services Agency, Government of Japan, Banking and Securities Business Supervision Bureau Deputy Vice Commissioner for Systemic Stability and Risk)	セッション：日本政府からのスピーチ（後半） 登壇者：D1-S11-13 大城 健司 (金融庁 銀行・証券監督局 金融総括監理官)

1. The slides outline the FSA's approach to strengthening cybersecurity across the financial sector, combining supervisory guidelines with self-assessment, sector-wide exercises, stronger account security, responses to AI-related threats and preparations for post-quantum cryptography. The deck notes that its contents do not represent a formal opinion of the FSA.
2. The cybersecurity guidelines apply across supervised financial entities, including financial market infrastructures. They draw on supervisory experience, lessons from incidents and international guidance. Cyber risk is treated as a major management risk, with a risk-based approach reflecting each institution's size, business and risk profile.
3. The guidelines distinguish fundamental practices expected generally from recommended practices for institutions whose cyber incidents could have significant economic effects. Institutions are expected to prioritize risks and develop mitigation roadmaps while considering urgency, criticality and resource constraints.
4. The Cyber-Security Self-Assessment program supports continuous improvement and comparison with peers while informing supervision and policy. The slides describe joint work by the FSA, Bank of Japan and FISC, with questions aligned to the cybersecurity guidelines and emerging AI-related risks.
5. The Delta Wall sector-wide exercise assesses incident response, investigation, customer communication and business continuity, including service recovery. Recommendations and lessons are shared to improve capabilities across the sector, including beyond participating institutions.
6. To counter unauthorized access and fraudulent transactions, the slides emphasize phishing-resistant multi-factor authentication and stronger customer protection. They describe supervisory guideline revisions and continued monitoring of implementation across financial services.
7. AI-related cyber threats are presented as a management priority requiring executive involvement. The requested short-term measures include identifying critical services and systems, reducing technical debt, securing patching resources, reviewing vendor responsibilities and prioritizing vulnerabilities by risk.

1. 金融庁の取り組みを、業態別の監督指針、サイバーセキュリティに特化したガイドライン、対策の実効性を高める施策という構成で説明した。顧客保護と金融システムの安全性・信頼性の確保を重視すると述べた。
2. 委託先への攻撃やシステムの脆弱性に対応するため、サードパーティーのリスク管理と、停止時の業務継続・速やかな復旧を含むオペレーショナル・レジリエンスの強化に取り組むと説明した。
3. ガイドラインは最低基準への適合を確認するだけのチェックリストではなく、各金融機関が規模や事業特性に応じてリスクに基づく対応を考えるためのものだと述べた。サイバーリスクを重大な経営課題とし、自助・共助・公助の組み合わせが不可欠だと強調した。
4. 中小規模の金融機関などが基本的な体制や取り組みを確認する自己評価の枠組みを紹介した。AIによる脅威の変化への短期的な対応も確認し、集計した結果を業界に還元すると説明した。
5. 金融業態を横断する演習では、攻撃発生時の情報共有、顧客対応、業務復旧の手順を確認すると説明した。共通課題や良好事例を業界全体に共有し、防御だけでなく被害後の対応・復旧能力も高めると述べた。
6. フィッシングによる認証情報の窃取や不正取引に対し、パスキーなど認証の強化を要請し、監督の枠組みにも反映していると説明した。個別業態だけでなく、金融業界全体の信頼と顧客保護に関わる問題だと述べた。
7. 高性能AIが攻撃に使われれば、脆弱性の発見や攻撃が大量かつ迅速に行われる可能性があると指摘した。官民の連携を強め、経営トップの主導、優先して守るサービスの特定、技術的負債の解消、パッチ適用の人員や保守契約の確認を求めていると説明した。
8. リスクに基づくパッチ適用、多層防御、緊急対応のためのシステム停止への備え、外部との連携も重視すると述べた。金融ISACを通じて対応方針や参考事例を共有し、情報漏洩を踏まえた対策の点検や本人確認の不正対策も促していると説明した。
9. 量子コンピューターによる暗号へのリスクを見据え、金融機関が利用する暗号を把握する台帳づくりを支援する実証事業を紹介した。得られた知見を実務的な手引書として公表し、参加していない金融機関にも役立てる予定だと述べた。
10. 今後も高まるサイバーリスクに対応するため、NCOなどの関係機関や業界との連携を一層強化し、金融業界全体の防御力と金融システムの安定を支える方針を示した。

8. Where patching is difficult, the slides recommend layered defenses, network segmentation and stronger authentication for privileged accounts. They also call for preparation for service disruptions, clear criteria for proactive suspension, business continuity arrangements and collaboration through information-sharing communities. 9. The post-quantum cryptography pilot aims to develop practical transition methods through cryptographic inventories, staff participation and knowledge transfer. Staff participation and knowledge transfer are intended to build internal capabilities, while sharing pilot lessons supports wider preparedness for threats from future quantum computers.	

D1-S11-1 Speeches from Japanese Government (second block) 16:35–18:35 JST

Session: Speeches from Japanese Government (second block) Speaker: D1-S11-1 TSUGITA Akira (Assistant Minister for Cybersecurity, IT Management and Evidence-based Policymaking, Ministry of Education, Culture, Sports, Science and Technology (MEXT))	セッション：日本政府からのスピーチ（後半） 登壇者：D1-S11-1 次田 彰 (文部科学省 サイバーセキュリティ・政策立案総括審議官)

1. The speaker described cybersecurity as a direct concern for universities, not just businesses and government. Recalling a major email breach at JST that also affected his own messages, he stressed the personal and institutional consequences of attacks. 2. He warned that ransomware, zero-day attacks and the use of generative AI are making threats faster and more sophisticated. Universities must assume that some attacks will succeed. The speaker advocated a breach-ready approach combining technical measures such as zero trust with leadership-backed organizational arrangements for rapid incident response. 3. Research data, academic records, personal information and computing resources make universities attractive targets. Trusted academic email domains can also be abused to launch convincing phishing attacks. 4. Academic openness, collaboration, frequent turnover of students and accounts, and decentralized authority complicate security management. The challenge is to preserve openness while protecting university systems and assets. 5. Shortages of dedicated personnel, constrained budgets and weak governance were identified as structural problems. The speaker argued that cybersecurity cannot depend on staff performing it as a secondary duty or on individual effort alone. 6. MEXT provides technical guidance, requires national universities to prepare cybersecurity basic plans, and brings institutional security leaders together to share incidents and good practices. It also issues technical alerts on emerging threats. 7. Role-based training spans operational staff and senior executives. Management training addresses governance and strategic decisions, while practical exercises help incident-response personnel prepare for real attacks. 8. Information security audits, vulnerability assessments and penetration testing help institutions identify weaknesses. Findings are reported with recommendations and follow-up support to improve their security. 9. Research security requires systematic controls to prevent critical technologies from leaking, including data access management reflecting research sensitivity. The speaker described cooperation across ministries to incorporate cybersecurity requirements into research-security work.	1. 講演原稿では、大学をサイバー攻撃の主要な標的として捉え、ランサムウェア、ゼロデイ攻撃、生成AIによる攻撃の高度化を課題に挙げている。完全な防御は不可能であり、侵害を前提とした備えが必要だとしている。 2. 大学は研究データ、成績情報、個人情報、計算資源などの価値ある資産を保有し、信頼性の高いアカウントも攻撃に悪用され得る。一方、教育研究に必要な開放性、人の入替え、学部・研究室の自治が、統一的なセキュリティ管理を難しくしている。 3. 専任人材の不足、予算制約、経営層への報告の不足、実働体制が伴わないCSIRTなどを指摘し、個人の善意や兼務だけに頼る対策の限界を示している。技術面だけでなく、経営層の関与による組織的な対策が必要だとしている。 4. 文部科学省の取組として、大学への技術的助言、国立大学へのサイバーセキュリティ対策等基本計画の策定要請、CISO会議による事例・知見の共有、脅威に応じた注意喚起を紹介している。 5. 人材育成では、役職や職務に応じて役割と責任を理解し、継続的に能力を高めることを重視している。経営層にはガバナンスや戦略的意思決定の研修、CSIRT要員には実際の攻撃を想定した実践的な演習を行うとしている。 6. 情報セキュリティ監査に加え、脆弱性診断やペネトレーションテストを実施し、検出した課題のフィードバック、対策の提言、改善のフォローアップまでを通じて、大学等のリスク管理能力向上を支援するとしている。 7. 研究セキュリティでは、研究データの機微性に応じたアクセス管理と重要技術の流出防止を課題とし、関係府省と連携して、研究セキュリティに関する手順書に適切なサイバーセキュリティ要件を反映する取組を示している。 8. 結びでは、大学に人材育成、資源配分の最適化、経営層主導のガバナンス強化を求めている。文部科学省としても、大学の開放性を維持しながら、防御体制の構築、監査、研究セキュリティ、必要な予算・資源の確保に取り組む方針を示している。

10. The closing priorities were stronger governance, sustained talent development and security audits, coordinated research security, and adequate funding and resources. These measures should let universities retain academic openness while strengthening cyber defenses.	

D1-S12 Day #1 Closing 18:35–18:40 JST

Session: Day #1 Closing Speaker: Craig Wiener (Technical Fellow, MITRE)	セッション：Day #1 クロージング 登壇者：クレイグ・ウィーナー (MITRE テクニカルフェロー)
1. Craig Wiener closed the day by highlighting the range of technical, geopolitical and cyber-threat-intelligence presentations, and looked forward to further discussions in the coming days. 2. He highlighted Japan's active-defense initiative and referred to a cybersecurity emergency in Japan as framing the urgency and importance of the conference's work. 3. Echoing other speakers, he emphasized that cybersecurity is a geopolitical and strategic issue, not merely a technical one. He thanked participants and Keio University and expressed appreciation for continued engagement.	1. ウィーナー氏は、技術面と地政学面の双方で興味深い講演があったと振り返り、今後もさらに議論を聞くことを楽しみにしていると述べた。 2. 複数の登壇者が指摘したように、サイバーセキュリティは技術的な問題だけでなく、地政学的な問題でもあると強調した。 3. 大学や他のパートナーとともに、こうした催しや交流を続けていくことへの期待を示した。

DAY 2 2026-10-28 水曜日

Keio University, Mita Campus; West School Building 1F West Hall
慶應義塾大学 三田キャンパス 西校舎 1F 西ホール

D2-S1 Day #2 AM Opening 09:15–09:20 JST

Session: Day #2 AM Opening Speaker: David Luzzi	セッション：Day＃2 AM オープニング 登壇者：デイビッド・ルッツィ
1. David Luzzi welcomed participants to the second day of the International Cybersecurity Symposium. 2. He expressed gratitude to those who have provided longstanding engagement and support for the symposium and cybersecurity in Japan. 3. He emphasized the importance of approaching cybersecurity from an international perspective. 4. He praised the symposium for bringing together cybersecurity experts from around the world and encouraging broader discussions. 5. He highlighted his meeting with colleagues from Taiwan as an example of the symposium's international exchange. 6. He noted that the morning sessions would address emerging technologies and the role of cybersecurity in intelligence and national security. 7. He mentioned that afternoon breakout sessions would explore more focused topics. 8. He concluded by welcoming participants again and yielding the stage to the next speakers to keep the program on schedule.	1. デイビッド・ルッツィ氏は、シンポジウム2日目の開会に当たり、参加者への歓迎の意を表した。 2. 長年にわたり本シンポジウムや日本のサイバーセキュリティを支えてきた関係者に感謝を述べた。 3. サイバーセキュリティを国際的な視点から考えることの重要性を強調した。 4. 本シンポジウムが、世界各国の専門家を集め、議論を広げる場として果たしてきた役割を評価した。 5. 当日朝に台湾の関係者と交流したことを紹介し、国際交流の伝統が続いていることに言及した。 6. 午前のセッションでは、新興技術や国家安全保障に関わるインテリジェンス、これらの分野におけるサイバーセキュリティの重要性が取り上げられると述べた。 7. 午後には、個別のテーマを掘り下げる分科会が予定されていることに触れた。 8. 定刻での進行のため、後続の登壇者に発言を引き継ぎ、改めて参加者を歓迎して挨拶を締めくくった。

D2-S3 Speech 09:20–09:35 JST

Session: Speech Speaker: Matt Mickelson (PQCC Lead, MITRE)	セッション：スピーチ 登壇者：マット・ミケルソン (MITRE, 耐量子計算機暗号協議会 代表)

1. Matt Mickelson outlined the need for post-quantum cryptography (PQC), highlighting threats to both data confidentiality and the integrity of digital signatures and certificates. 2. He warned that adversaries can collect encrypted information today for future decryption, making data sensitivity over time and migration lead times critical considerations. 3. He cited recent research indicating declining estimates of the quantum computing resources needed to break current public-key cryptography, reinforcing the urgency of preparation. 4. He emphasized that PQC migration is an extensive organizational transformation involving infrastructure, legacy devices, certificates, VPNs, and identity cards. 5. He noted that PQC-capable commercial products are already available in several categories, but adopting these products alone will not complete an organization's migration. 6. He introduced the PQC Coalition's adaptable strategy and roadmap, encouraging iterative implementation supported by clear leadership, accountability, and inventories of assets and cryptographic dependencies. 7. He recommended prioritizing migration according to system importance, the time required to migrate, and how long protected information will remain sensitive. 8. He highlighted implementation challenges involving software dependencies, larger cryptographic messages, network fragmentation, funding, procurement, and workforce skills, alongside the need for monitoring, auditing, and validation. 9. He offered five recommendations: start now, pursue quick wins, combine PQC migration with planned technology upgrades, address confidentiality and authentication together, and prioritize crypto-agility. 10. He invited organizations to participate in the PQC Coalition and use its shared resources to accelerate migration to quantum-resilient solutions.	1. マット・ミケルソン氏は、データの機密性と電子署名・証明書への脅威を挙げ、耐量子計算機暗号（PQC）への移行の必要性を説明した。 2. 現在収集された暗号化データが将来解読されるリスクを指摘し、データの重要性が続く期間と移行に要する時間を考慮すべきと述べた。 3. 暗号解読に必要な量子計算資源の推計を引き下げる研究を紹介し、量子脅威への備えを先延ばしにすべきではないと強調した。 4. PQC移行は単なるソフトウェア更新ではなく、インフラ、旧式機器、証明書、VPN、本人認証用カードなどに及ぶ大規模な取り組みであると説明した。 5. 一部の分野ではPQC対応製品が利用可能になっている一方、製品を導入するだけでは組織全体の移行は完了しないと指摘した。 6. PQC Coalitionの戦略・ロードマップを紹介し、責任者の明確化と資産・暗号利用状況の棚卸しを進めながら、段階的かつ反復的に移行する方法を示した。 7. 移行の優先順位は、システムの重要度だけでなく、移行に必要な時間や保護対象データの機密性が続く期間も踏まえて決めるべきと述べた。 8. ソフトウェアの依存関係、暗号データのサイズ増大による通信への影響、予算・調達・人材の課題を挙げ、進捗管理、監査、実装の検証の必要性を強調した。 9. 五つの提言として、早期着手、小さな成果の積み重ね、既存の技術更新との統合、機密性と認証の両面への対応、暗号方式を柔軟に変更できる「暗号アジリティ」の確保を示した。 10. PQC Coalitionへの参加と公開資料の活用を呼びかけ、量子耐性のある仕組みへの移行を共同で加速する意義を述べた。

D2-P4 Panel 09:35–10:35 JST

Session: PQC, International Emerging Technology Moderator: Matt Mickelson Panelist: Yuh-Tay Lin (Director-General, Department of Information Management, Financial Supervisory Commission, Taiwan) Panelist: Rick Muller (Vice President of Quantum Systems, IonQ) Panelist: Matt Campagna (Amazon AWS) Panelist: Hart Montgomery (Linux Foundation) Panelist: Dustin Moody (NIST) Panelist: Hiroki Uchiyama (Director and Head of the Security Innovation Lab at Hitachi America R&D)	セッション：PQC, 国際間における先端技術 モデレーター：マット・ミケルソン パネリスト：ユータイ・リン (台湾金融監督管理委員会 情報管理処 処長) パネリスト：リック・ミュラー (IonQ 量子システム部門副社長) パネリスト：マット・キャンパグナ (Amazon AWS) パネリスト：ハート・モントゴメリー (Linux Foundation) パネリスト：ダスティン・ムーディ (米国国立標準技術研究所) パネリスト：内山 宏樹 (日立アメリカR&D ディレクター兼セキュリティ・イノベーション・ラボ長)
Session: PQC, International Emerging Technology Moderator: Matt Mickelson Panelist: Yuh-Tay Lin (Director-General, Department of Information Management, Financial Supervisory Commission, Taiwan) Panelist: Rick Muller (Vice President of Quantum Systems, IonQ) Panelist: Matt Campagna (Amazon AWS) Panelist: Hiroki Uchiyama (Director and Head of the Security Innovation Lab at Hitachi America R&D)	セッション：PQC, 国際間における先端技術 モデレーター：マット・ミケルソン パネリスト：ユータイ・リン (台湾金融監督管理委員会 情報管理処 処長) パネリスト：リック・ミュラー (IonQ 量子システム部門副社長) パネリスト：マット・キャンパグナ (Amazon AWS) パネリスト：内山 宏樹 (日立アメリカR&D ディレクター兼セキュリティ・イノベーション・ラボ長)

1. Moderated by Matt Mickelson, the panel examined PQC migration through perspectives from IonQ, Hitachi, Taiwan's financial sector, and AWS, focusing on quantum threats, implementation strategies, dependencies, and practical obstacles.
2. Rick Muller explained that advances in algorithms, error correction, and hardware have reduced estimates of the resources needed to threaten current public-key cryptography. He presented the possibility of capable quantum computers arriving before the end of the decade as a forecast, emphasizing that preparation must account for both migration time and the period during which information remains sensitive.
3. Muller recommended deploying standardized PQC, inventorying cryptographic uses, and maintaining cryptographic agility. He also proposed QKD as a complementary layer in suitable environments and highlighted the importance of high-quality random-number generation and correct implementation.
4. Hiroki Uchiyama described Japan's policy and standardization efforts, including a government migration target of around 2035. He recommended appointing accountable leaders, forming cross-functional teams, inventorying systems and cryptographic assets, prioritizing migration, and preparing procurement and deployment processes; Hitachi's long-lived IT, OT, and industrial products present particular challenges.
5. Yuh-Tay Lin outlined Taiwan's planned ecosystem-driven migration, beginning with the Financial XML banking service. Financial institutions, infrastructure operators, certificate providers, and suppliers would coordinate shared scenarios, interoperability and performance testing, knowledge exchange, and migration schedules; joint testing would supplement each institution's own integration testing.
6. Lin described a hub-and-spoke model in which financial infrastructure providers coordinate participants, common methods, testing, and timelines. He emphasized that migration must preserve complete financial service chains while allowing institutions to progress at different speeds and retain responsibility for their own systems.

1. マット・ミケルソン氏の進行の下、IonQ、日立、台湾金融分野、AWSの視点からPQC移行を議論し、量子脅威、移行戦略、依存関係、実装上の障害を検討した。
2. リック・ミュラー氏は、アルゴリズム、誤り訂正、ハードウェアの進歩によって、現行の公開鍵暗号を脅かす量子計算資源の推計が減少していると説明した。今の10年が終わる前に十分な能力を持つ量子コンピューターが登場する可能性を予測として示し、移行期間と情報の機密性が続く期間の両方を踏まえた準備を求めた。
3. ミュラー氏は、標準化されたPQCの導入、暗号利用箇所の棚卸し、暗号アジリティの確保を推奨した。また、適切な環境では量子鍵配送（QKD）を補完的な防御層として組み合わせることを提案し、高品質な乱数生成と正しい実装の重要性を強調した。
4. 内山宏樹氏は、政府機関等の2035年ごろの移行目標を含む日本の政策・標準化動向を紹介した。責任者と部門横断チームの設置、システム・暗号資産の棚卸し、優先順位付け、調達・導入準備を推奨し、日立では長寿命のIT・OT・産業製品への対応が特に課題になると説明した。
5. ユータイ・リン氏は、台湾の銀行間Financial XMLサービスを出発点とする、エコシステム主導型の移行構想を紹介した。金融機関、インフラ運営者、証明書事業者、サプライヤーが、共通シナリオ、相互運用性・性能の検証、知見の共有、移行日程を調整し、共同試験で各機関の統合試験を補完する計画を示した。
6. リン氏は、金融インフラ事業者が参加機関、共通手法、試験、日程を調整する「ハブ・アンド・スポーク」方式を説明した。各機関の移行速度と自らのシステムに対する責任を尊重しながら、金融サービスの一連の処理を維持する必要性を強調した。
7. マット・キャンパグナ氏は、AWSの移行を、ユースケースの優先順位付け、機密通信へのPQC鍵共有の導入、長寿命の信頼の起点の整備、アイデンティティへの対応、従来の脆弱な暗号方式の廃止という並行的な取り組みとして紹介した。国際的な要件の違いやハイブリッド方式にも触れ、概ね機密性と公開ネットワーク上の通信を優先しつつ、依存関係の制御可能性や資格情報の有効期間を区別すると説明した。
8. キャンパグナ氏は、標準化されたクラウドの接続部分では移行を進めやすい一方、独自ソフトウェア、文書化されていない依存関係、旧式ハードウェアが内部移行を難しくすると指摘した。技術者による検証を前提としたAIによる暗号資産の棚卸しや設計の再構築を紹介し、暗号利用状況の把握、更新の自動化、簡潔なAPI、暗号アジリティの整備を推奨した。

7. Matt Campagna presented AWS's overlapping migration workstreams: prioritize use cases, introduce PQC key establishment for confidential communications, establish long-lived roots of trust, address identity, and eventually retire quantum-vulnerable algorithms. He discussed differing international requirements and hybrid approaches, generally prioritizing confidentiality and public-network traffic while distinguishing controllable dependencies and credential lifetimes. 8. Campagna explained that standardized cloud interfaces can simplify part of the transition, while proprietary software, undocumented dependencies, and legacy hardware make internal migration difficult. He described AI-assisted cryptographic inventories and system-design reconstruction, subject to engineering validation, and recommended telemetry, update automation, simpler APIs, and crypto-agility. 9. Discussion of IoT and OT highlighted constrained memory, bandwidth, processing resources, and operational requirements. Participants recommended risk-based decisions on upgrading, replacing, redesigning, retaining, or isolating devices, and identified university contributions in low-resource PQC implementations, side-channel research, interoperability, education, and shared tools. 10. In discussing historical financial records, participants distinguished intercepted communications that might be decrypted later from stored data protected by sufficiently strong symmetric encryption. They stressed that re-encrypting stored records cannot remove risks from previously captured traffic, and that migration priorities should reflect data sensitivity over time, business impact, replacement options, and costs.	9. IoT・OTに関する議論では、メモリ、帯域、処理能力、運用要件の制約が課題となった。機器の更新、交換、再設計、維持、隔離をリスクに基づいて判断する必要性が示され、大学には低資源環境でのPQC実装、サイドチャネル攻撃、相互運用性、教育、共有ツールの開発への貢献が期待された。 10. 過去の金融記録に関する質疑では、将来解読され得る収集済みの通信と、十分に強い共通鍵暗号で保護された保存データを区別した。保存データを再暗号化しても過去に収集された通信のリスクは解消できず、情報の機密性が続く期間、事業への影響、交換可能性、費用を移行の優先順位に反映すべきとした。

D2-S5 Speech 11:00–11:15 JST

Session: Speech Speaker: Matt Eanes (Director, PAC PMO)	セッション：スピーチ 登壇者：マット・エアネス (Performance Accountability Council Program Management Office (PAC PMO) ディレクター)

1. Matt Eanes emphasized that trust in networks, cryptography, cloud platforms, and supply chains ultimately depends on the people who design, operate, and protect them. Personnel vetting establishes whether individuals can be trusted with sensitive information, facilities, and systems, covering both classified and unclassified roles.
2. He described the 2015 breach of U.S. government personnel records and the backlog of background investigations as catalysts for reform. These events exposed longstanding weaknesses: slow hiring processes, lengthy gaps between reviews, and fragmented records that hindered information sharing.
3. He introduced Trusted Workforce 2.0, launched in 2018, as a fundamental reform organized around three principles: faster, continuous, and connected. Its purpose is to strengthen risk management and improve efficiency without lowering vetting standards.
4. Under the faster approach, preliminary determinations based on high-value information allow suitable candidates to begin work while full investigations continue. Eanes reported that approximately 80% of candidates receive favorable preliminary decisions and that average time to eligibility to start work had fallen below 30 days over the preceding year.
5. Continuous vetting replaces long intervals between periodic reinvestigations with ongoing automated record checks, conducted with clearance holders' agreement. Potential concerns are reviewed by trained professionals, enabling earlier intervention and support before personal difficulties develop into security risks; expansion to the remaining unclassified workforce is under way.
6. Eanes described plans to use "superintelligence" to help reviewers identify risks and patterns in growing volumes of information and improve training and guidance. He stressed that people would retain decision-making authority, and that clear rules, privacy protections, and fair treatment are essential to trust in the vetting system.
7. The connected approach involves replacing separate systems with the secure National Background Investigation Services (NBIS) platform to support faster decisions, continuous vetting, and a single federal record for each person. The aim is to reduce duplication, cost, and delays while maintaining security.

1. マット・エアネス氏は、ネットワーク、暗号技術、クラウド基盤、サプライチェーンへの信頼は、それらを設計・運用・防御する人々への信頼に支えられていると強調した。人的信頼性審査は、機微な情報・施設・システムを任せられる人物かを判断する仕組みであり、機密職と非機密職の双方を対象とすると説明した。
2. 2015年の米国政府の人事記録流出と身元調査の滞留を、改革の契機として紹介した。これらは、採用手続きの遅さ、再審査までの長い空白、情報共有を妨げる記録の分散という、従来からの制度上の弱点を顕在化させたと述べた。
3. 2018年に始まった「Trusted Workforce 2.0」を、「迅速化」「継続性」「連携」の三つを柱とする抜本的な改革として紹介した。審査基準を引き下げずに、リスク管理と業務効率を改善することを目指すと説明した。
4. 「迅速化」では、重要度の高い情報に基づく暫定判断と、調査完了後の最終判断を組み合わせ、適格と判断された候補者が調査継続中に就業できるようにした。候補者の約80%が肯定的な暫定判断を受け、直近1年間では就業可能となるまでの平均期間が30日未満に短縮されたと報告した。
5. 「継続性」では、数年ごとの再調査に代えて、クリアランス保持者の同意に基づく自動的・継続的な記録確認を行う。懸念情報は訓練を受けた専門家が確認し、個人的な問題が保安上のリスクに発展する前に介入・支援できると説明し、残る非機密分野の人員への拡大も進めていると述べた。
6. 増加する情報からリスクや傾向を見つけ、研修・指針を改善するため、審査担当者を支援する「スーパーインテリジェンス」の活用構想を紹介した。一方、最終的な判断は人間が担い、明確なルール、プライバシー保護、公正な取扱いが審査制度への信頼に不可欠だと強調した。
7. 「連携」では、分散したシステムを、安全な共通基盤であるNational Background Investigation Services（NBIS）へ置き換える取り組みを説明した。迅速な判断、継続的審査、個人ごとの連邦政府共通記録を支え、安全性を維持しながら重複作業、費用、遅延を減らすことを目指すとした。
8. 技術基盤の統合に加えて、組織間の連携も重要だと指摘した。人材が政府機関、産業界、学術界の間を移動しても、不必要に審査を繰り返さず信頼を引き継げるよう、幹部の継続的な関与と足並みをそろえた改革が必要だと述べた。
9. 日本の制度近代化の取り組みとして、経済安全保障に関するセキュリティ・クリアランス制度や国家情報局に言及し、相互に学ぶ意義を示した。政府機関、産業界、同盟国の間のインテリジェンス共有には、人への信頼、ネットワークと情報保護への信頼、合意どおりの情報共有・利用への信頼が必要だと説明した。

8. He emphasized that organizational coordination is as important as technical integration. Trust should move with people across agencies, industry, and academia without unnecessary repetition of vetting, supported by sustained senior leadership and coordinated implementation. 9. Eanes highlighted Japan's efforts to modernize its arrangements, referring to its economic-security clearance system and the National Intelligence Bureau. He encouraged mutual learning and explained that intelligence sharing among agencies, industry, and allies depends on trusted personnel, protected networks, and confidence that information will be shared and used as agreed. 10. He concluded that trusted people underpin national, economic, and societal security. While U.S. reforms remain unfinished, he urged other countries to pursue modernization with urgency rather than waiting for a crisis to expose weaknesses.	10. 信頼できる人材こそが、国家安全保障、経済安全保障、社会の安全保障の基盤だと結論付けた。米国の改革も道半ばであると認めつつ、他国には危機によって弱点が明らかになるのを待たず、切迫感を持って制度の近代化に取り組んでほしいと呼びかけた。

D2-P6 Panel 11:15–12:15 JST

Session: Intelligence, National Intelligence Agency Moderator: Matt Eanes Panelist: Junichi Nishiyama (Senior Research Fellow, Institute for Future Engineering (IFENG)) Panelist: Masanori Nishi (Former Deputy Minister, Minister of Defense, Japan, CEO, Trans-Pacific Group) Panelist: Barbara Grewe (CEO, Glenwood Global Risk Management LLC, USA) Panelist: Kenzaburo Tamaru (National Technology Officer, Director, Microsoft Japan) Panelist: Douglas Sicker (Chief Science Officer, SVP at Resonant Sciences, LLC) Panelist: Simon Gass (Former Chair of the UK Joint Intelligence Committee)	セッション：インテリジェンス、国家情報局 モデレーター：マット・エアネス パネリスト：西山 淳一 (未来工学研究所 政策調査分析センター 研究参与) パネリスト：西 正典 (元防衛事務次官, トランス・パシフィック・グループ株式会社 代表取締役社長) パネリスト：バーバラ・グレウ (グレンウッド・グローバル・リスク・マネジメントLLC CEO) パネリスト：田丸 健三郎 (日本マイクロソフト株式会社 業務執行役員 NTO) パネリスト：ダグラス・シッカー (Resonant Sciences, LLC 最高科学責任者(CSO) 兼 上級副社長(SVP)) パネリスト：サイモン・ギャス (元英国統合情報委員会 (JIC) 委員長)
Session: Intelligence, National Intelligence Agency Moderator: Matt Eanes Panelist: Junichi Nishiyama (Senior Research Fellow, Institute for Future Engineering (IFENG)) Panelist: Masanori Nishi (Former Deputy Minister, Minister of Defense, Japan, CEO, Trans-Pacific Group) Panelist: Barbara Grewe (CEO, Glenwood Global Risk Management LLC, USA) Panelist: Kenzaburo Tamaru (National Technology Officer, Director, Microsoft Japan) Panelist: Simon Gass (Former Chair of the UK Joint Intelligence Committee)	セッション：インテリジェンス、国家情報局 モデレーター：マット・エアネス パネリスト：西山 淳一 (未来工学研究所 政策調査分析センター 研究参与) パネリスト：西 正典 (元防衛事務次官, トランス・パシフィック・グループ株式会社 代表取締役社長) パネリスト：バーバラ・グレウ (グレンウッド・グローバル・リスク・マネジメントLLC CEO) パネリスト：田丸 健三郎 (日本マイクロソフト株式会社 業務執行役員 NTO) パネリスト：サイモン・ギャス (元英国統合情報委員会 (JIC) 委員長)

1. Moderated by Matt Eanes, the panel examined how democracies can strengthen national intelligence, enable timely two-way public-private information sharing, and deliver warnings to those able to act. The discussion brought together Junichi Nishiyama, Masanori Nishi, Barbara Grewe, Kenzaburo Tamaru, and Sir Simon Gass.
2. Gass argued that interagency trust grows from a shared mission and an understanding that intelligence serves decision-makers rather than institutional interests. Grewe challenged reliance on traditional trust relationships in cybersecurity, arguing that actionable information must reach relevant companies and infrastructure operators quickly, without waiting for personal trust to develop.
3. Nishiyama called for clearer disclosure of cyberattack methods, damage, and precautions, rather than reassuring statements that may obscure uncertainty and discourage public concern. He emphasized educating organizations about the value of their information, while Nishi highlighted shortcomings in Japan's security literacy and argued that its accumulated knowledge of China could contribute to international intelligence analysis.
4. Tamaru identified reciprocity, speed, and protection of contributors as essential to sustainable sharing. Organizations need useful feedback and confidence that reporting will not simply invite blame; predefined disclosure rules, standardized procedures, machine-to-machine exchange, and trusted common platforms can reduce delays and reputational barriers.
5. Gass emphasized that sharing general information and sharing secrets require different arrangements, and that public-private dialogue must cover economic security, investment, intellectual property, and supply-chain espionage as well as cyber defense. Predictable government action and clear explanations of national-security decisions help businesses plan and build trust.
6. Nishiyama warned that AI can reinforce mistaken beliefs and enable unintended or malicious activity unless people understand and control its use. Gass called for deeper dialogue among Japan, the UK, the US, and other like-minded countries on both AI-related national-security threats and opportunities to improve defense.

1. マット・エアネス氏の進行の下、西山淳一氏、西正典氏、バーバラ・グレウ氏、田丸健三郎氏、サイモン・ギャス卿が、民主主義国家のインテリジェンス強化、迅速かつ双方向の官民情報共有、実際に対処できる相手への警告の届け方を議論した。
2. ギャス卿は、共通の使命を持ち、組織の利益ではなく意思決定者への支援をインテリジェンスの目的とすることが、機関間の信頼につながると述べた。一方、グレウ氏は、サイバー分野では従来型の信頼関係に依存せず、個人的な信頼の形成を待たずに、企業や重要インフラ事業者へ行動可能な情報を迅速に届けるべきだと主張した。
3. 西山氏は、不確実な状況を覆い隠し、国民の関心を弱めかねない安心を促す説明ではなく、攻撃手口、被害、注意点を明確に公表する必要性を指摘した。また、組織が保有情報の価値を理解するための教育を重視した。西氏は、日本の安全保障リテラシーの不足を指摘するとともに、中国に関する知識の蓄積を国際的な情報分析への貢献に生かせると述べた。
4. 田丸氏は、持続可能な情報共有の条件として、互恵性、速度、情報提供者の保護を挙げた。報告が責任追及だけにつながらないという安心と、有益なフィードバックが必要であり、事前に定めた開示ルール、標準化された手順、機械間の情報交換、信頼できる共通基盤によって、遅延や評判への懸念を減らせるとした。
5. ギャス卿は、一般情報と秘密情報の共有では必要な仕組みが異なると説明した。官民対話はサイバー防御に加え、経済安全保障、投資、知的財産、サプライチェーンを通じた諜報活動も扱う必要があり、政府行動の予見可能性と安全保障上の判断理由の明確な説明が、企業の計画と信頼形成を支えると述べた。
6. 西山氏は、AIが誤った認識を強めたり、意図しない行動や悪用を可能にしたりする危険を指摘し、人間がその影響を理解して制御する必要性を強調した。ギャス卿は、日本、英国、米国などの同志国が、AIによる国家安全保障上の脅威と、防御への活用の両面について、より高度な対話と知識共有を進めることを提案した。
7. 田丸氏は、攻撃手口、痕跡、有効な対策を早期に共有し、他の組織の防御につなげるべきだと述べた。官民演習では、技術的対応だけでなく政策判断や対外公表も検証する必要があるとし、ウクライナによる政府データのクラウド退避準備を例に、危機の前にシナリオ、権限、意思決定手順を整える重要性を強調した。
8. 警告は、国境を越えた連携も含め、実際に対応できる運用担当者やサービス提供者に届かなければならないと議論された。田丸氏は、システム間の情報伝達、対応資源の乏しい組織に対するサービス提供者の支援、警告件数ではなく防止・阻止できた攻撃を基準とする成果評価を提案した。

7. Tamaru recommended rapidly sharing attack techniques, indicators, and effective countermeasures so others can defend themselves. Joint exercises should test technical responses alongside policy and public-communication decisions; citing Ukraine's preparations to protect government data through cloud migration, he stressed agreeing on scenarios, authority, and decision procedures before a crisis. 8. Participants emphasized that warnings must reach operational teams and service providers capable of responding, including across borders. Tamaru advocated system-to-system delivery, provider support for less-resourced organizations, and outcome-based measures such as attacks prevented or stopped, rather than simply counting advisories issued. 9. Nishi called for democratic debate on the state's powers and responsibilities in cyberspace. Gass and Grewe argued that governments must help protect hospitals, local authorities, critical infrastructure, and other organizations lacking sufficient resources, while Grewe proposed clearer criteria for intervention, distinguishing existing UK IoT password rules from possible future measures addressing insecure network equipment. 10. The discussion highlighted the need to turn information sharing into practical protection through education, skilled personnel, preparation, institutional coordination, and international cooperation. Gass cautioned that the imbalance between inexpensive attacks and costly defenses makes funding government support difficult, reinforcing the importance of effective use of limited resources.	9. 西氏は、サイバー空間における国家の権限と保護責任を民主的に議論する必要性を訴えた。ギャス卿とグレウ氏は、病院、自治体、重要インフラなど、自力で十分な防御ができない組織への政府支援を求めた。グレウ氏は政府介入の判断基準の整備を提案し、英国の既存のIoTパスワード規制と、安全性の低いネットワーク機器への将来的な対策案を区別して説明した。 10. 議論を通じて、情報共有を実際の保護につなげるには、教育、人材、事前準備、組織間調整、国際協力が必要であることが示された。ギャス卿は、比較的安価な攻撃に対して防御には多額の費用がかかり、政府支援の財源確保も難しいと指摘し、限られた資源を効果的に活用する課題を示した。

D2-S7 Day #2 PM Opening 13:30–13:35 JST

Session: Day #2 PM Opening Speaker: Anupam Joshi	セッション：Day＃2 PM オープニング 登壇者：アヌパム・ジョシ

1. The speaker welcomed participants to the afternoon sessions on the second day of the symposium. 2. The speaker emphasized that cybersecurity and national security are closely connected and difficult to discuss separately. 3. The afternoon program would address national security, active cyber defense, and data integrity as interrelated topics. 4. The speaker highlighted the range of perspectives from industry and government in the United States and Japan and invited participants to enjoy the afternoon discussions.	1. 講演者は、シンポジウム2日目の午後のセッションに参加する皆様を歓迎した。 2. サイバーセキュリティと国家安全保障は密接に関連し、切り離して議論することが難しいと強調した。 3. 午後のプログラムでは、国家安全保障、能動的サイバー防御、データの完全性を、相互に関連するテーマとして取り上げると紹介した。 4. 米国と日本の産業界・政府から幅広い視点が示されることに触れ、午後の議論を楽しんでほしいと述べた。

D2-S8 Keynote Speech 13:35–13:50 JST

Session: Keynote Speech Speaker: Matt Fussa (VP, Trust & Compliance Officer, Security & Trust Organization, Cisco Systems Inc.)	セッション：基調講演 登壇者：マット・フッサ (シスコシステムズ セキュリティ＆トラストオフィス バイスプレジデント兼トラスト＆コンプライアンス責任者)

1. Matt Fussa presented an optimistic view of AI-driven changes in cybersecurity, arguing that AI can strengthen national, economic, and societal security when its risks are addressed and its defensive capabilities are adopted quickly.
2. He explained that modern AI, including open-weight models, can identify software vulnerabilities and hardware design flaws and rapidly develop exploits. He warned that these capabilities lower the skills required for attacks and could enable less-sophisticated actors to operate at unprecedented speed and scale.
3. He emphasized that the same AI capabilities can help defenders find and fix weaknesses before attackers exploit them, transforming how security is built into software, networks, and critical systems.
4. Fussa reported that Cisco had scanned almost seven billion lines of code over six months and used AI across vulnerability discovery, exploit development, testing, patch creation, and software revision. He cited an approximately 3% false-positive rate in Cisco's testing as evidence supporting confidence in these tools.
5. He described a shift toward dynamic, AI-enabled security processes resembling CI/CD pipelines, including rewriting software and redesigning hardware where necessary. He argued that continuous security testing and assurance should replace reliance on assessments conducted only at particular points in time.
6. He stressed that organizations must be able to trust the AI they deploy. Observability tools and network-based protections can help detect unexpected behavior or attempts to exceed intended boundaries and support more effective control of AI systems.
7. He recommended immediate "zero-regret" actions: maintain accurate asset inventories, accelerate patch deployment, adopt modern management tools, and move from periodic to continuous patching. Vendors should support effective automation and hot patching that avoids network downtime.
8. He urged renewed emphasis on established safeguards, including phishing-resistant multi-factor authentication, zero trust, least-privilege access, isolation, and segmentation. These measures become more important as attacks accelerate and can help limit damage, manage incidents, and remove attackers after a breach.

1. マット・フッサ氏は、AIによるサイバーセキュリティの変化を楽観的に捉え、リスクに対処しながら防御能力を迅速に取り入れることで、国家安全保障、経済安全保障、社会の安全を高められると述べた。
2. 公開ウェイトモデルを含む現代のAIは、ソフトウェアの脆弱性やハードウェアの設計上の欠陥を発見し、攻撃コードを短時間で作成できると説明した。こうした能力によって攻撃に必要な技能の水準が下がり、比較的未熟な攻撃者でも、従来にない速度と規模で活動できるようになると警告した。
3. 同じAIの能力を防御側も活用し、攻撃者に悪用される前に弱点を発見・修正できると強調した。AIは、ソフトウェア、ネットワーク、重要システムにセキュリティを組み込む方法そのものを変革すると述べた。
4. シスコでは6か月間で約70億行のコードをスキャンし、脆弱性探索、攻撃コードの作成、テスト、パッチ作成、ソフトウェア改修にAIを活用したと報告した。また、同社のテストにおける誤検知率は約3%だったと述べ、これらのツールへの信頼を支える結果として紹介した。
5. 必要に応じたソフトウェアの書き直しやハードウェアの再設計を含め、CI/CDパイプラインに近い、AIを活用した動的なセキュリティプロセスへの移行を説明した。特定時点の評価だけに依存せず、継続的に安全性を検証・保証する仕組みへ転換すべきだと述べた。
6. AIを活用するには、そのAIを信頼できることが前提だと強調した。可観測性のツールとネットワークによる保護を用いて、予期しない動作や想定範囲からの逸脱を検知し、AIシステムを効果的に制御する必要があると説明した。
7. 今すぐ実施すべき「後悔のない対策」として、正確な資産把握、パッチ適用の迅速化、最新の管理ツールの導入、定期的な適用から継続的な適用への移行を推奨した。ベンダーには、更新の自動化や、ネットワークを停止させずに適用できるホットパッチによる支援を求めた。
8. フィッシング耐性のある多要素認証、ゼロトラスト、最小権限アクセス、隔離、セグメンテーションといった基本対策の再徹底を訴えた。攻撃が高速化するほど、これらは重要となり、侵害時の被害抑制、インシデント管理、攻撃者の排除にも役立つと述べた。
9. CEO、CIO、CSOが、保守、パッチ適用、ソフトウェアセキュリティを組織の優先課題に位置付けるよう求めた。稼働率よりも迅速なセキュリティ更新を優先する顧客の例を紹介し、製品寿命・サポートが終了した製品の撤去、エッジデバイスの保護、交換が困難な場合の監視・検知による代替策を推奨した。

9. He called on CEOs, CIOs, and CSOs to make maintenance, patching, and software security organizational priorities. He highlighted customers whose leaders prioritize timely security updates even over operational uptime, and recommended removing end-of-life or unsupported products, securing edge devices, and using compensating monitoring and detection where replacement is not possible. 10. He concluded that AI remains a tool whose benefits depend on responsible use, secure systems, and leadership. He called for rapid learning and cooperation among technology companies, customers, governments, and policymakers, arguing that adopting AI for defense sooner can improve security before attackers gain further advantage.	10. AIは道具であり、その効果を生かすには、責任ある利用、安全なシステム、経営層の主導が必要だと結論付けた。技術企業、顧客、政府、政策立案者による迅速な学習と協力を呼びかけ、攻撃者がさらに優位に立つ前にAIを防御へ導入することが、安全性の向上につながると述べた。

D2-S9 Speech 13:50–14:05 JST

Session: Speech Speaker: Nobukatsu Kanehara	セッション：スピーチ 登壇者：兼原 信克

1. Nobukatsu Kanehara warned that AI-enabled cyberattacks are increasing the advantage of attackers over defenders. He compared autonomous AI agents searching for vulnerabilities at scale with machine-gun fire, arguing that governments and businesses must respond urgently.
2. He assessed Japan's cybersecurity capabilities as insufficient despite recent legislative changes and plans to expand cyberdefense and police personnel. He argued that earlier constitutional interpretations had impeded capability development and expressed concern that current staffing and training may not withstand intensive AI-enabled attacks.
3. Kanehara criticized siloed government systems and resistance to interministerial data sharing. He advocated a secure government-wide cloud architecture that combines appropriate information sharing, administrative efficiency, and improved public services with protection across the entire government.
4. He emphasized individual identification, authentication, access controls, and comprehensive logging to reduce insider risks. In the cloud-based model he advocated, sensitive information would be processed centrally rather than retained on individual devices, with access and downloads recorded and especially sensitive materials restricted.
5. He highlighted the risk that adversaries are storing encrypted diplomatic communications for future decryption by quantum computers. He called for stronger preparation for post-quantum cryptography and expressed concern about Japan's progress.
6. He stressed that government connections with private contractors and essential industries can become entry points for attackers. Because no architecture provides complete protection, he called for sustained investment in skilled personnel and security, alongside greater public understanding that geographical distance offers no protection in cyberspace.
7. Turning to armed conflict, Kanehara identified a Taiwan contingency as a major concern with potentially severe consequences for regional financial markets, shipping, semiconductor supply, and trade. He argued that advance preparation is essential to deterrence and to preventing economic and security disruption.

1. 兼原信克氏は、AIを使ったサイバー攻撃によって、攻撃側の防御側に対する優位が拡大していると警告した。AIエージェントが自律的かつ大量に脆弱性を探す状況を機関銃の乱射に例え、政府と企業に早急な対応を求めた。
2. 最近の法整備やサイバー防衛・警察人員の拡充計画にもかかわらず、日本のサイバー対応能力は十分ではないと評価した。従来の憲法解釈が能力整備の障害となってきたとの見方を示し、現在の人員や訓練状況でAIによる激しい攻撃に耐えられるか懸念を表した。
3. 政府の縦割りシステムと省庁間のデータ共有への抵抗を批判した。必要な情報共有、行政の効率化、国民へのサービス向上を、政府全体の防御と両立させる、安全な政府共通クラウドの構築を提唱した。
4. 内部者による情報流出を防ぐため、個人の識別・認証、アクセス権限の管理、詳細なログ記録を重視した。機微な情報を個々の端末に残さずクラウド内で処理し、閲覧・ダウンロードを記録するとともに、特に機密性の高い情報へのアクセスを制限する仕組みを示した。
5. 攻撃者が暗号化された外交通信を蓄積し、将来、量子コンピューターで解読するリスクを指摘した。耐量子計算機暗号（PQC）への備えを強化する必要性を訴え、日本の取り組みの進展に懸念を示した。
6. 政府と民間の契約事業者や重要産業との接点が、攻撃者の侵入口になり得ると強調した。完全な防御はないため、人材とセキュリティへの継続的な投資が必要だとし、サイバー空間では地理的な距離が防御にならないという認識を社会全体で高めるよう求めた。
7. 有事の問題として台湾有事への強い懸念を示し、地域の金融市場、海運、半導体供給、貿易に深刻な影響が及び得ると述べた。経済と安全保障の混乱を防ぐためにも、事前の準備による抑止が不可欠だと主張した。
8. 現代の紛争では、通常戦力が交戦する前に、サイバー攻撃とミサイルによって電力、石油、交通、金融インフラが停止し、継戦能力を奪われる可能性があると警告した。ネットワークに既に悪意あるプログラムが仕込まれている危険にも触れ、日本がこれらのシステムを十分に守れるか疑問を呈した。
9. 抑止の一環として、サイバー部隊の強化とともに攻撃能力の整備も必要だと主張した。人員目標だけでなく、有事に実効的に活動できる能力を検証すべきとし、対象の把握とサイバー作戦の遂行には、サイバーインテリジェンスが不可欠だと述べた。

8. He warned that cyber operations and missiles could disable power, oil, transportation, and financial infrastructure at the outset of a conflict, undermining the ability to sustain operations before conventional forces engage. He questioned whether Japan could adequately protect these systems and highlighted the danger of malicious code already embedded in networks. 9. Kanehara advocated developing offensive cyber capabilities as part of deterrence, alongside strengthening Japan's cyber force. He argued that operational effectiveness, rather than personnel targets alone, must be assessed, and that cyber intelligence is indispensable for identifying targets and conducting cyber operations. 10. He called for a clearer legal and institutional basis for sustained cyber intelligence directed at foreign state actors, rather than relying solely on criminal investigations. He argued that meaningful intelligence contributions are necessary for deeper cooperation with partners such as the Five Eyes and concluded that cyber intelligence and cyber warfare capabilities also underpin effective peacetime cybersecurity.	10. 犯罪捜査中心の対応だけではなく、外国の国家主体を対象とする継続的なサイバーインテリジェンスの法的・制度的基盤を明確にするよう求めた。ファイブ・アイズなどとの協力を深めるには、日本自身による有意義な情報貢献が必要だとし、サイバーインテリジェンスとサイバー戦能力が平時の有効なサイバーセキュリティも支えると結論付けた。

D2-P10 Panel 14:05–15:05 JST

Session: National Security and Cybersecurity Moderator: Nobukatsu Kanehara Panelist: Shigeki Suzuki (President, Yokosuka Research Park; Former Ministry of Internal Affairs and Communications) Panelist: Jun Nagashima (Senior Research Adviser, Nakasone Peace Institute; Former Deputy Assistant Chief Cabinet Secretary, National Security Secretariat) Panelist: Mihoko Matsubara (Chief Cybersecurity Strategist, NTT, Inc. Security and Trust Office)	セッション：国家安全保障とサイバーセキュリティ モデレーター：兼原 信克 パネリスト：鈴木 茂樹 (横須賀リサーチパーク社長, 元総務省事務次官) パネリスト：長島 純 (中曽根平和研究所 研究顧問, 元国家安全保障局内閣審議官) パネリスト：松原 実穂子 (NTT株式会社 技術企画部門 セキュリティ・アンド・トラスト室 チーフ・サイバーセキュリティ・ストラテジスト)

1. Moderated by Nobukatsu Kanehara, the panel brought together Shigeki Suzuki, Jun Nagashima, and Mihoko Matsubara to examine Japan's cybersecurity preparedness, wartime cyber operations, critical infrastructure, intelligence sharing, and AI-related challenges.
2. Suzuki emphasized that cybersecurity depends on protecting physical communications infrastructure, including submarine cables, landing stations, satellite ground facilities, and concentrated Internet exchange points. He highlighted the need to connect monitoring and detection with timely operational responses by the responsible authorities.
3. Suzuki described risks across interconnected layers, from communications networks to electricity, transport, finance, manufacturing, robotics, and web applications. He distinguished protection of communications in transit from protection of stolen data and called for consideration of cloud infrastructure, AI, and quantum-resistant cryptography together.
4. Nagashima explained that emerging technologies are bringing cyberspace and the physical world closer together, allowing cyberattacks, disinformation, and conventional military operations to reinforce one another. He identified individual security literacy, public-private cooperation, and international collaboration as essential responses to increasingly interconnected battle domains.
5. Matsubara highlighted the growing burden on defenders from ransomware, data breaches, and AI misuse, alongside physical threats to data centers and their supporting electricity, telecommunications, and cooling infrastructure. She called for reducing duplicated work and administrative silos through cooperation and better intelligence sharing rather than simply increasing demands on existing teams.
6. Matsubara advocated consistent background checks and security clearances, information labeling, appropriate access permissions, and secure platforms for intelligence management and analysis. Kanehara also emphasized auditable access and government-wide coordination of collection and analysis; the platforms and clearance systems themselves require physical security, cybersecurity, and suitable protection against future quantum threats.

1. 兼原信克氏の進行の下、鈴木茂樹氏、長島純氏、松原実穂子氏が、日本のサイバー対応体制、有事のサイバー作戦、重要インフラ、インテリジェンス共有、AIに関する課題を議論した。
2. 鈴木氏は、サイバーセキュリティの前提として、海底ケーブル、陸揚げ局、衛星の地上設備、特定地点に集中するインターネットエクスチェンジなど、物理的な通信インフラの保護を重視した。監視や異常の発見だけでなく、関係機関が迅速に現場対応できる体制につなげる必要性を指摘した。
3. 鈴木氏は、通信網から電力、交通、金融、製造、ロボティクス、ウェブアプリケーションまで、相互接続された各層のリスクを説明した。通信経路上の保護と、盗まれたデータの保護は異なるとし、クラウド基盤、AI、量子コンピューターに耐性を持つ暗号を一体的に検討する必要性を示した。
4. 長島氏は、新興技術によってサイバー空間と現実空間の融合が進み、サイバー攻撃、偽情報、通常の軍事作戦が組み合わさって影響を増幅すると説明した。戦闘領域が相互につながる状況への対応として、個人のリテラシー、官民協業、国際協力の三つを重視した。
5. 松原氏は、ランサムウェア、情報漏えい、AIの悪用に加え、データセンターや、それを支える電力、通信、冷却設備への物理的脅威によって、防御側の負担が増していると指摘した。既存の担当者に業務を上乗せするだけではなく、協力とインテリジェンス共有によって重複作業や縦割りを減らすよう求めた。
6. 松原氏は、一貫したバックグラウンドチェックとセキュリティ・クリアランス、情報のラベリング、適切なアクセス権限、安全な情報管理・分析基盤の整備を提案した。兼原氏もアクセスの記録と政府全体での情報収集・分析の調整を重視し、こうした基盤や審査制度自体にも、物理的防護、サイバー防御、将来の量子脅威に備えた保護が必要だと議論された。
7. 鈴木氏は、能動的サイバー防御には、民間インフラ事業者との平時からの関係と、対象システムへの事前の理解が必要だと述べた。異常な通信量、特権アカウントへの不審なアクセスなどをインテリジェンスと突き合わせ、速やかに共有し、重大な被害が出る前に攻撃を止める必要性を強調した。
8. 鈴木氏は、電力、通信接続、冷却水、GPU、保守人材、技術の進歩を踏まえた現実的なデータセンター・AI計画を求めた。政府の最高機密にはソブリンクラウドやソブリンAIを活用しつつ、その他の用途では適切な海外サービスも選択し、全面的な国産化ではなく、安全性と有事の対応を考慮する方針を示した。

7. Suzuki stressed that active cyber defense requires established relationships with private infrastructure operators and prior knowledge of their systems. Unusual traffic, suspicious privileged-account activity, and other warning signs should be assessed with intelligence and shared promptly so attacks can be stopped before serious damage occurs. 8. Suzuki urged realistic planning for data centers and AI based on electricity, connectivity, cooling water, GPUs, maintenance personnel, and evolving technology. He proposed sovereign cloud and AI capabilities for the most sensitive government information while allowing suitable foreign services for other uses, with security and contingency arrangements considered rather than requiring everything to be domestically produced. 9. Nagashima emphasized the vulnerability of satellites, communication links, and ground systems and called for integrated treatment of space, cyber, and cognitive threats. He recommended addressing drones within a broader defense architecture rather than through isolated purchases, and countering disinformation through verification, information literacy, and prompt evidence-based public responses. 10. Matsubara argued that AI should help reduce operational workloads, supported by usable, consistently labeled data. She stressed developing both personnel who can use AI effectively and personnel who can question and verify its outputs, identify hallucinations and unintended agent behavior, and ensure that apparent efficiency does not undermine accuracy or appropriate conduct.	9. 長島氏は、衛星、通信経路、地上設備の脆弱性を指摘し、宇宙・サイバー・認知領域を総合的に捉える必要性を訴えた。ドローン対策は個別の装備購入ではなく防衛全体の設計に位置付け、偽情報には真偽の確認、情報リテラシー、証拠に基づく迅速な公的説明によって対処すべきと述べた。 10. 松原氏は、利用可能で一貫してラベリングされたデータを整え、AIを現場の負担軽減に活用すべきとした。同時に、AIを使いこなす人材と、出力に疑問を呈して検証し、ハルシネーションやエージェントの意図しない行動を見抜く人材の双方を育成し、効率化によって正確性や適切な行動が損なわれないようにする必要性を強調した。

D2-S11 Speech 15:25–15:40 JST

Session: Speech Speaker: SANO Tomoki (Director General for Active Cyber Defense and Cyber Intelligence, National Cybersecurity Office)	セッション：スピーチ 登壇者：佐野 朋毅 (国家サイバー統括室 統括官(能動的サイバー防御・サイバー情報担当))

1. Sano, the National Cybersecurity Office official responsible for active cyber defense and cyber intelligence, addressed recent unauthorized-access incidents, personal-information leaks, cloud-service disruptions, and ransomware. He focused on clarifying what he considered misunderstandings in reporting about GMO Internet's request for active cyber defense.
2. He explained that active cyber defense comprises three pillars: stronger public-private partnership, utilization of communications data, and remote access and neutralization measures. He stressed that the framework should not be understood solely in terms of the third pillar.
3. Sano stated that remote access and neutralization operations are generally conducted covertly and that the government neither confirms nor denies their use in individual cases. He therefore declined to say whether such measures had been taken in connection with any particular incident.
4. He described oversight arrangements requiring third-party committee approval for remote access and neutralization measures. Aggregate figures, including the number of approval requests, are reported annually to the Diet without identifying individual cases.
5. He explained that the framework rests on two pieces of legislation: a new law covering public-private partnership and communications-data utilization, and an accompanying law amending existing legislation. Remote access and neutralization powers were introduced through amendments to the Police Duties Execution Act and the Self-Defense Forces Act.
6. He described the legal basis for these measures as "immediate compulsion": action by public authorities to remove an imminent danger without first imposing an obligation. He emphasized that the police or defense authorities assess the statutory conditions when a danger is identified; a request from an affected organization does not itself trigger action, and eligibility should not be judged simply by its infrastructure designation.

1. 国家サイバー統括室で能動的サイバー防御とサイバー情報を担当する佐野氏は、相次ぐ不正アクセス、個人情報漏えい、クラウドサービスの停止、ランサムウェアを取り上げた。特に、GMOインターネットによる能動的サイバー防御の要請をめぐる報道について、誤解があると考える点の説明に重点を置いた。
2. 能動的サイバー防御は、「官民連携の強化」「通信情報の利用」「アクセス・無害化措置」の三本柱から成ると説明した。アクセス・無害化措置だけを指すものとして理解すべきではないと強調した。
3. アクセス・無害化措置は、基本的に秘密裏に実施する活動であり、政府は個別事案における実施の有無を明らかにしない方針だと述べた。そのため、特定の事案について措置を実施したかどうかは説明できないとした。
4. アクセス・無害化措置には第三者委員会の承認を要する監督の仕組みがあると説明した。承認を求めた件数などは年1回国会に報告されるが、個別事案は特定されないと述べた。
5. 制度は、官民連携と通信情報の利用を定める新法と、既存の法律を改正する整備法の二つによって構成されると説明した。アクセス・無害化措置の権限は、警察官職務執行法と自衛隊法の改正によって設けられたとした。
6. 措置の法的な考え方として、切迫した危険を除去するため、事前に義務を課さず行政機関が直接行動する「即時強制」を説明した。警察や防衛省・自衛隊が危険を認識し、法律上の要件を判断して措置を講じるものであり、被害組織からの要請自体が発動条件となるわけではなく、対象をインフラの区分だけで判断する理解も適切ではないと述べた。
7. 官民連携の柱では、基幹インフラ事業者に重要電子計算機の届出やインシデント報告を求めると説明した。通信情報の利用については、通信の本質的内容に関わらない一定の情報を法定の条件下で取得・分析する仕組みであり、国内間の通信は取得対象としないと述べた。
8. 三本柱の施行時期は異なり、官民連携の強化とアクセス・無害化措置は10月1日から施行された一方、通信情報の利用は講演時点では未施行で、翌年秋ごろの施行を目指していると説明した。
9. 制度整備の背景として、2022年の国家安全保障戦略と、その後の法整備、国家サイバー統括室やサイバーセキュリティ戦略本部に関する組織整備を挙げた。最近の事案を深刻に受け止め、総理が出席する関係閣僚会議などを通じて対応していると述べた。
10. 国家サイバー統括室を政府の司令塔とし、警察、防衛省・自衛隊と一体的に対応する方針を示した。インフラ所管省庁、個人情報保護委員会などの関係機関とも連携し、政府全体で脅威を把握して必要な政策を進めると結んだ。

7. Under the public-private partnership pillar, he explained that core infrastructure operators are required to notify the government of important computer systems and report incidents. The communications-data pillar, as he described it, permits acquisition and analysis of specified information outside the substantive contents of communications under legal conditions, excluding domestic-to-domestic communications. 8. Sano distinguished the implementation schedules: he stated that the public-private partnership and remote access and neutralization pillars had entered into force on October 1, while communications-data utilization was intended to begin around autumn of the following year and was not yet in force at the time of the speech. 9. He traced the reforms to the 2022 National Security Strategy and subsequent legislation and organizational changes involving the NCO and Cybersecurity Strategy Headquarters. He emphasized the seriousness of recent incidents and described ministerial coordination involving the prime minister. 10. He outlined an integrated response in which the NCO serves as the government's coordinating center alongside the police and the Ministry of Defense and Self-Defense Forces. Cooperation would also involve infrastructure ministries, the Personal Information Protection Commission, and other agencies to assess threats and implement necessary policies.	

D2-P12 Panel 15:40–16:40 JST

Session: Active Cyber Defence Utilizing Internationally, including SBOM Moderator: Tim Perry (International Cyber Security Programme Lead, BAE Systems Digital Intelligence) Panelist: Hideaki Watanabe (Former Commissioner, Acquisition, Technology & Logistics Agency (ATLA), Ministry of Defense; Chairman, Defense Technology Foundation) Panelist: Urmas Ruuto (Head of TECH Branch, NATO Cooperative Cyber Defence Centre of Excellence) Panelist: Gloria Glaubman (Founder & Principal, GMG Consulting LLC) Panelist: Jeanne Richard (Political counsellor, Embassy of France in Japan)	セッション：SBOM等を国際的に活用した能動的サイバー防御 モデレーター：ティム・ペリー (BAEシステムズ・デジタル・インテリジェンス、国際サイバーセキュリティ・プログラム・リード) パネリスト：渡辺 秀明 (元防衛装備庁長官、一般財団法人防衛技術協会 理事長) パネリスト：ウーマス・ルート (NATOサイバー防衛協力センター(CCDCOE) 技術部長) パネリスト：グローリア・グローブマン (GMG Consulting LLC 創業者・代表) パネリスト：ジャンヌ・リシャール (在日フランス大使館政治部参事官)

1. Moderated by Tim Perry, the panel examined how active cyber defense (ACD), SBOM and related tools, diplomacy, resilience, and international cooperation can strengthen Japan's cybersecurity. Hideaki Watanabe, Urmas Ruuto, Jeanne Richard, and Gloria Glaubman discussed the capabilities and partnerships needed while respecting democratic values, privacy, and international law.
2. Glaubman described "deterrence by denial" as making attacks harder, limiting damage, and restoring services quickly so that attackers gain less. She emphasized combining government intelligence and legal authorities with industry's knowledge of its systems and suppliers, supported by clear contacts, escalation procedures, information-sharing rules, and joint preparation.
3. Glaubman argued that sustainable partnerships require useful information to flow both ways and companies to report incidents without fear of blame. She proposed joint analytical cells involving government, industry, and allied liaison personnel, timely sharing of appropriately sanitized intelligence, and connecting security clearances with practical access to sensitive information.
4. Richard explained that France generally reserves "deterrence" for nuclear doctrine and instead seeks to actively hinder cyber threats by imposing financial, technical, and reputational costs. She described diplomatic signaling, evidence-based public attribution, sanctions, and technical and judicial measures as complementary instruments that can disrupt adversaries and influence their behavior without guaranteeing that attacks will stop.
5. Richard emphasized international law, responsible state behavior, solidarity, and partner capacity-building. She cited the United Nations, the Paris Call, support for Ukraine, and the Pall Mall Process as examples, highlighting the importance of including both governments and private actors in addressing irresponsible use and proliferation of commercial cyber-intrusion capabilities.
6. Ruuto stressed proactive resilience through understanding assets, services, maintenance, threats, and dependencies. Because failures in electricity and telecommunications can cascade into other essential services, he recommended realistic cross-sector exercises covering technical response, operational decisions, legal questions, and public communication, while building relationships before a crisis.

1. ティム・ペリー氏の進行の下、渡辺秀明氏、ウーマス・ルート氏、ジャンヌ・リシャール氏、グローリア・グローブマン氏が、能動的サイバー防御（ACD）、SBOM等の活用、外交、レジリエンス、国際協力による日本のサイバーセキュリティ強化を議論した。民主的価値、プライバシー、国際法との整合性を保ちながら必要な能力と連携を整えることが論点となった。
2. グローブマン氏は、攻撃を難しくし、被害を限定し、サービスを迅速に復旧することで攻撃者の利益を減らす「拒否による抑止」を説明した。政府のインテリジェンスと法的権限を、企業による自社システムや供給者への理解と組み合わせ、連絡先、エスカレーション経路、共有ルール、共同準備を事前に明確にする必要性を強調した。
3. グローブマン氏は、持続可能な連携には双方向の有益な情報交換と、企業が非難を恐れずに報告できる環境が必要だと述べた。政府、産業界、同盟国の連絡要員による共同分析の場、機密部分を適切に除去・加工した情報の迅速な提供、クリアランスと実際の機微情報へのアクセスを結び付ける仕組みを提案した。
4. リシャール氏は、フランスでは「抑止」を主に核ドクトリンの用語とし、サイバー分野では金銭的・技術的・評判上のコストを課して脅威の拡大を能動的に妨げる方針だと説明した。外交的シグナリング、証拠に基づく公的アトリビューション、制裁、技術的・司法的措置は相互補完的であり、攻撃の完全な停止を保証するものではないが、敵対者の活動を妨げ、行動に影響を与え得るとした。
5. リシャール氏は、国際法、責任ある国家行動、連帯、パートナー国の能力構築を重視した。国連、パリ・コール、ウクライナ支援、Pall Mall Processを例に挙げ、商用サイバー侵入能力の拡散と無責任な使用に対処するには、政府だけでなく民間主体も含める必要があると述べた。
6. ルート氏は、資産、サービス、保守状況、脅威、依存関係を把握し、先回りしてレジリエンスを高めることを求めた。電力や通信の障害が他の不可欠なサービスへ連鎖するため、技術対応、運用上の判断、法的論点、広報を含む現実的な分野横断演習を行い、危機の前に関係と信頼を築くべきだと述べた。
7. 渡辺氏は、供給者、保守会社、共通ソフトウェア、クラウドサービスを通じて、自組織の防御が迂回される危険を指摘した。SBOMによる影響するソフトウェアの特定と、VEXによる悪用可能性の評価を組み合わせて修正の優先順位を決め、外部接続や権限を見直すとともに、費用や人材が不足する中小の供給企業を支援するよう求めた。
8. 渡辺氏は、技術・運用・法律の判断を結び付け、増大する情報をAIで安全に扱う専門チームの整備を提案した。AIの出力と根拠の検証、データ中の悪意ある指示によって防御用AIが誘導されることの防止、Moving Target Defence（動的防御）の運用、措置による正当なサービスや第三者への影響評価などの技能が必要だと述べた。

7. Watanabe warned that suppliers, maintenance providers, shared software, and cloud services can bypass an organization's own defenses. He recommended combining SBOMs to identify affected software with VEX information to assess exploitability and prioritize remediation, reviewing external connections and permissions, and supporting smaller suppliers that lack sufficient budgets and personnel. 8. Watanabe called for specialist teams that connect technical, operational, and legal judgment and use AI safely to handle growing information volumes. Required skills include verifying AI outputs and evidence, preventing malicious instructions in data from misleading defensive AI, operating Moving Target Defence, and assessing whether interventions could disrupt legitimate services or harm third parties. 9. Ruuto emphasized that remote access and neutralization depend on reliable situational awareness, attribution, appropriate procedures, and legal authority, rather than technical skills alone. Attackers, command infrastructure, cloud services, and compromised devices may be distributed across countries, making intervention difficult; questions about advance positioning in foreign systems are political and strategic decisions. 10. Watanabe presented the US response to Volt Typhoon as an example of legally controlled, carefully tested, limited neutralization intended to protect infrastructure while preserving normal device operation. He stressed that neutralization buys time rather than permanently solving the problem, so continued remediation and stronger defenses are essential; the panel also highlighted exercises, reciprocal sharing, appropriate obligations on industry, and cross-sector cooperation as practical priorities.	9. ルート氏は、アクセス・無害化措置には技術技能だけでなく、確かな状況認識、アトリビューション、適切な手続き、法的権限が必要だと強調した。攻撃者、指令基盤、クラウド、侵害機器が複数国に分散すると対処は難しくなり、外国のシステムへの事前配置をめぐる問題は政治的・戦略的な判断に属すると述べた。 10. 渡辺氏は、米国によるVolt Typhoonへの対応を、法的統制、事前試験、対象の限定、機器の正常動作への配慮を伴う防御的な無害化の例として紹介した。無害化は問題を恒久的に解決するのではなく時間を稼ぐ措置であり、その間に修正と防御強化を続ける必要があるとした。パネルでは、演習、互恵的な情報共有、産業界への適切な義務付け、分野横断の協力も実践上の優先事項として挙げられた。

D2-S13 Speech 17:00–17:30 JST Maria A. Roat

Session: Speech Speaker: Maria A. Roat (the first Director of the FedRAMP program in the U.S.; the former U.S. Deputy Federal Chief Information Officer)	セッション：スピーチ 登壇者：マリア・A・ロート (米国におけるFedRAMPプログラムの初代ディレクター、元連邦副最高情報責任者)

1. Maria A. Roat argued that Japan has made meaningful cybersecurity policy progress but has not yet translated it into consistent national-scale operational capability. She identified the gap between strategy and execution as a major strategic vulnerability, particularly as targeted attacks, supply-chain compromises, AI-enabled threats, and cloud dependence increase.
2. She called for Japan to control and independently validate the security of the cloud services it relies on. In her proposed sovereign-cloud model, platforms would operate under Japanese law, be distributed across multiple Japanese regions, meet high security standards, and maintain secure operations during disruptions.
3. Roat emphasized that data residency alone does not establish sovereignty. She argued that Japan needs clear authority over operational management, logs, encryption keys, update approvals, and roots of trust, rather than remaining dependent on foreign vendors, parent companies, or legal jurisdictions.
4. She proposed operations conducted by Japanese nationals in Japan, domestically generated and held encryption keys, independently audited key custody, and workload isolation by design. Her objective was that no new software or firmware would run without Japanese approval and that platforms could operate safely when disconnected from external systems.
5. Drawing on her experience leading FedRAMP, Roat advocated a centralized, risk-based national cloud authorization program with unified security baselines, independent assessments, continuous validation and monitoring, and authorizations reusable across ministries. She argued that Japan should evolve ISMAP or establish a new program that drives operational security rather than primarily checking compliance.
6. She described a resilient architecture with independently operable regional cores, local units able to run in island mode during disruptions, safe resynchronization, and seamless failover across Japanese regions. Supply-chain integrity would be supported by vetted allied suppliers, verifiable cryptographic signatures, and transparent bills of materials.

1. マリア・A・ロート氏は、日本のサイバーセキュリティ政策は大きく前進したものの、国家規模で一貫した運用能力へ十分に転換されていないと指摘した。標的型攻撃、サプライチェーン侵害、AIを利用した脅威、クラウド依存が増す中、戦略と実行の隔たりを重大な戦略上の脆弱性と位置付けた。
2. 日本が依存するクラウドの安全性を自ら管理し、独立して検証する必要性を訴えた。提案するソブリンクラウドは、日本法の下で運用され、国内の複数地域に分散し、高いセキュリティ基準を満たし、障害時にも安全な運用を維持できるものとした。
3. データを国内に置くだけでは主権性は確立しないと強調した。海外の事業者、親会社、法域への依存を残すのではなく、運用管理、ログ、暗号鍵、更新承認、信頼の起点について、日本側が明確な権限を持つ必要があると主張した。
4. 日本人による国内運用、暗号鍵の国内生成・保管、独立監査による鍵管理の検証、設計段階からのワークロード分離を提案した。日本側の承認なしに新たなソフトウェアやファームウェアを稼働させず、外部システムから切り離されても安全に運用できる状態を目標とした。
5. FedRAMPを率いた経験を踏まえ、統一的なセキュリティ基準、独立評価、継続的な検証・監視、省庁横断で再利用できる認可を備えた、中央統括型かつリスクに基づく国家的なクラウド認可制度を提唱した。ISMAPを発展させるか新制度を設け、適合性確認を中心とする仕組みから、実運用の安全性を推進する制度へ進むべきだと述べた。
6. 独立運用できる地域の中核システム、障害時に外部から切り離されたアイランドモードで稼働する地域単位、安全な再同期、国内地域間の円滑なフェイルオーバーを備える構成を示した。サプライチェーンの完全性は、審査済みの同盟国側の供給者、検証可能な暗号署名、透明性のある部品表によって支えるとした。
7. ソフトウェアとファームウェアの更新に国内承認を求め、その完全性を独立して検証するなど、厳格な運用統制を提案した。証拠、ログ、スキャン結果、証明情報を継続的に収集し、日本側の監督下で完全に監査できるようにする必要性を強調した。
8. 実装には技術だけでなく変革マネジメントが不可欠だと述べた。トップの強い支援、中間層のリーダーシップ、実務能力を持つプログラムチーム、政策に沿った調達、訓練された評価者・エンジニア・調達担当者、成果を測定できるパイロット事業が、戦略を運用成果へつなげる条件だとした。
9. 90日以内に認可担当組織・制度の設置、基準更新、パイロット開始、KPI報告を行い、180日以内にサービスカタログとSLAの公表、研修、評価者認定を始める工程を提案した。12か月以内にはISMAPの改定または新制度の立ち上げを行い、政府調達で主権性と安全性の検証を備えたクラウドの選択肢を求めるとした。

7. Roat called for disciplined operational controls, including domestic approval of software and firmware updates and independent integrity verification. Security evidence, logs, scan results, and attestations should be collected continuously and remain fully auditable under Japanese oversight. 8. She stressed that implementation depends on change management as much as technology. Strong executive sponsorship, capable middle management, hands-on program teams, procurement processes aligned with policy, trained assessors, engineers, acquisition personnel, and measurable pilot projects are necessary to turn strategy into operational results. 9. She proposed establishing an authorization office or program, publishing updated baselines, launching pilots, and reporting KPIs within 90 days; publishing a service catalog and SLAs and beginning training and assessor accreditation within 180 days; and updating ISMAP or launching a new program with sovereign, validated cloud options in government procurement within 12 months. 10. Roat argued that the long-term value of validated resilience outweighs the risks of leaving systems unverified and that existing infrastructure allows validation to proceed alongside implementation. She welcomed hyperscale providers that meet Japan's requirements and concluded that independent control, sustained investment, skills development, and measurable outcomes would strengthen resilience, competitiveness, and public trust.	10. 未検証のシステムを放置するリスクに比べ、検証されたレジリエンスには長期的な価値があり、既存のインフラを活用して検証と実装を並行できると主張した。日本の要件を満たす大手クラウド事業者の参加を認めつつ、独立した統制、継続的な投資、人材育成、成果の測定によって、レジリエンス、競争力、国民の信頼を高めるよう呼びかけた。

D2-S13 Speech 17:00–17:30 JST Tadashi Nagamiya

Session: Speech Speaker: Tadashi Nagamiya (Executive Fellow, Japan Information Security Audit Association)	セッション：スピーチ 登壇者：永宮 直史 (特定非営利活動法人 日本セキュリティ監査協会 エグゼクティブフェロー)

1. Tadashi Nagamiya explained Japan's approach to cloud security and ISMAP, emphasizing that the structure of government, ministerial authority, and executive powers differ from those of the United States. He argued that these institutional differences matter when considering proposals for centralized cloud governance.
2. He traced the background to Japan's introduction of ISMS conformity assessment in 2002 and its subsequent widespread adoption. However, conventional ISMS certification did not fully align with the security services and responsibilities involved in cloud computing, creating a need for cloud-specific assessment.
3. He described METI-led cloud security management guidelines that contributed to ISO/IEC 27017 and the development of an audit-based assessment mechanism. Following the government's 2018 cloud-by-default principle and approximately two years of discussion, ISMAP was established by building on existing arrangements.
4. Nagamiya explained that ISMAP provides a unified government-wide assessment of cloud services, based primarily on ISO/IEC 27001, 27002, and 27017. A common framework reduces the burden on providers that would otherwise face separate assessments from numerous ministries and government-related organizations.
5. He emphasized the importance of international standards because Japan relies heavily on major overseas cloud providers. In his view, overly distinctive domestic requirements could create trade barriers; ISMAP therefore adopted a shared-responsibility approach informed by international cloud security standards.
6. He stressed that unified assessment does not remove each ministry's responsibility for its own risk decisions. Cloud providers supply security information and capabilities, while individual agencies evaluate their circumstances, determine appropriate countermeasures, and consider the legal jurisdictions governing the services they use.
7. Nagamiya stated that ISMAP examines whether required security controls are actually implemented, rather than only assessing security management arrangements. He estimated that its assessment costs and workload exceed those of ISMS conformity assessment by more than ten times.

1. 永宮直史氏は、日本のクラウドセキュリティとISMAPの考え方を説明し、政府の構造、省庁の権限、首相の権限は米国と異なると強調した。集中的なクラウド統治を提案する際には、こうした制度上の違いを考慮する必要があると述べた。
2. 日本が2002年にISMSの適合性評価を導入し、その後広く普及した経緯を紹介した。一方、従来のISMS認証だけでは、クラウドサービスにおけるセキュリティ機能や責任分担と十分に整合しないため、クラウド固有の評価が必要になったと説明した。
3. 経済産業省を中心とするクラウドセキュリティのマネジメントガイドラインがISO/IEC 27017につながり、監査に基づく評価の仕組みも整備されたと述べた。2018年のクラウド・バイ・デフォルト原則を受け、約2年間の議論を経て、既存の仕組みを生かしたISMAPが設けられたと説明した。
4. ISMAPは、主にISO/IEC 27001、27002、27017を基礎とし、政府全体でクラウドサービスを統一的に評価する仕組みだと説明した。共通の枠組みによって、事業者が多数の省庁や政府関係機関から個別に評価を受ける負担を減らすことが目的の一つだとした。
5. 日本が海外の大手クラウド事業者に大きく依存する中、国際規格を利用する重要性を強調した。独自性の強い国内要件は貿易障壁になり得るとの考えから、ISMAPでは国際的なクラウドセキュリティ規格を踏まえた責任共有の考え方を採用したと述べた。
6. 政府共通の評価を行っても、最終的なリスク判断は各省庁が担うという原則は変わっていないと強調した。クラウド事業者が提供する情報や機能を踏まえ、各機関が自らの状況に応じて対策を決め、サービスに適用される法域のリスクも判断する構造だと説明した。
7. ISMAPでは、セキュリティマネジメントの仕組みだけでなく、必要な管理策が実際に着実に実施されているかまで確認すると述べた。そのため、評価の費用や手間はISMSの適合性評価の10倍以上になるとの見方を示した。
8. ソブリンクラウドには統一された定義がないと指摘し、ここではクラウドサービスにおける主権の確保と捉えるとした。大手事業者の世界共通サービスや法規制の域外への影響によって、利用者のデータ処理の自由が制約され得るため、法域と統制が重要になると説明した。
9. ISMAPはセキュリティマネジメントと管理策の実施を評価する制度であり、現時点でデータ主権に関する特別な要件を政府全体に一律に課すものではないと明確にした。各省庁は基本的な評価に加え、自らのリスク分析に基づいてデータや情報資源の保護を判断する必要があると述べた。

8. He noted that sovereign cloud lacks a universally agreed definition and described the issue as protecting sovereignty within cloud services. The global operation of major providers and the cross-border effects of regulations can constrain users' freedom to process data, making jurisdiction and control important considerations. 9. He clarified that ISMAP evaluates security management and implementation but does not currently impose special government-wide data-sovereignty requirements. Individual ministries must make additional decisions about protecting their data and information resources through their own risk analyses. 10. He concluded that uniform sovereign-cloud requirements would require additional ISMAP requirements or a separately defined framework. Given the autonomy of Japanese ministries, rapid implementation through a single centralized authority is not straightforward, and determining how to proceed remains a policy and institutional challenge.	10. 政府共通のソブリンクラウド要件を設けるには、ISMAPへの要求事項の追加か、別の枠組みの定義が必要だと結論付けた。各省庁の自主的判断を重視する日本では、単一の権限で一挙に実装することは容易ではなく、進め方の検討が今後の政策・制度上の課題になるとした。

D2-P14 Panel 17:30–18:30 JST

Session: Data Sovereignty and Cloud Services, ISMAP and FedRAMP Moderator: Tadashi Nagamiya Panelist: ADM (Ret.) Michael Rogers Panelist: Chris Carter (Director, Key Accounts, National Security and Government, BAE Systems Digital Intelligence) Panelist: Akio Isowa (Senior Managing Executive Officer & Group Chief Digital Innovation Officer, SUMITOMO MITSUI FINANCIAL GROUP) Panelist: Masahiro Shimomura (Secretary-General, NPO Japan Network Security Association) Panelist: Akira Kaneko (Area Vice President Japan region, Cyber Security Products THALES JAPAN K.K.)	セッション：データ主権とクラウドサービス、ISMAPとFedRAMP モデレーター：永宮 直史 パネリスト：マイケル・ロジャース パネリスト：クリス・カーター (BAEシステムズ・デジタル・インテリジェンス、国家安全保障・政府部門 主要顧客担当ディレクター) パネリスト：磯和 啓雄 (三井住友銀行 専務執行役員, 三井住友フィナンシャルグループ 執行役専務 グループCDIO) パネリスト：下村 正洋 (特定非営利活動法人 日本ネットワークセキュリティ協会 事務局長) パネリスト：兼子 晃 (タレスジャパン株式会社 サイバーセキュリティプロダクト事業本部 本部長)
Session: Data Sovereignty and Cloud Services, ISMAP and FedRAMP Moderator: Tadashi Nagamiya Panelist: Chris Carter (Director, Key Accounts, National Security and Government, BAE Systems Digital Intelligence) Panelist: Akio Isowa (Senior Managing Executive Officer & Group Chief Digital Innovation Officer, SUMITOMO MITSUI FINANCIAL GROUP) Panelist: Masahiro Shimomura (Secretary-General, NPO Japan Network Security Association) Panelist: Akira Kaneko (Area Vice President Japan region, Cyber Security Products THALES JAPAN K.K.)	セッション：データ主権とクラウドサービス、ISMAPとFedRAMP モデレーター：永宮 直史 パネリスト：クリス・カーター (BAEシステムズ・デジタル・インテリジェンス、国家安全保障・政府部門 主要顧客担当ディレクター) パネリスト：磯和 啓雄 (三井住友銀行 専務執行役員, 三井住友フィナンシャルグループ 執行役専務 グループCDIO) パネリスト：下村 正洋 (特定非営利活動法人 日本ネットワークセキュリティ協会 事務局長) パネリスト：兼子 晃 (タレスジャパン株式会社 サイバーセキュリティプロダクト事業本部 本部長)

1. Moderated by Tadashi Nagamiya, the panel brought together Chris Carter, Akio Isowa, Masahiro Shimomura, and Akira Kaneko to discuss data sovereignty as a foundation for sovereign cloud services. The discussion explored security, operational control, international differences, and the respective responsibilities of governments, businesses, and individuals.
2. Kaneko emphasized that sovereignty concerns not only where data is stored, but also who controls the provider, which laws apply, and whether services can continue during disruption. He proposed evaluating risk, dependency, and control together, using global technologies while retaining the authority needed to protect sensitive data and maintain operations.
3. Kaneko described European approaches combining technical security with jurisdiction, ownership, foreign influence, and operational continuity. He cited France's SecNumCloud, the EU Cloud Sovereignty Framework, and the Thales–Google partnership S3NS as examples, distinguishing sovereignty assessment from certification and highlighting the importance of retaining independent control over encryption keys.
4. Carter contrasted the UK's largely advisory cloud-security approach with Australia's more explicit hosting, residency, and assessment arrangements. He described sovereignty as a spectrum rather than an absolute condition and recommended identifying capabilities that require national control while accepting appropriate dependencies on trusted allies and partners.
5. Carter noted growing use of private and disconnected cloud architectures beyond classified defense systems, including critical infrastructure. He stressed that isolation alone does not establish sovereignty: operational resilience, availability, and secure data transfer between separated environments are also essential.
6. Isowa explained that AI adoption is accelerating interest in cloud migration within banking, despite reliance on legacy on-premises systems. He argued that the objective is to combine AI-enabled business transformation with security, rather than adopting sovereign cloud for its own sake, and anticipated using different cloud models according to data and operational needs.

1. 永宮直史氏の進行の下、クリス・カーター氏、磯和啓雄氏、下村正洋氏、兼子晃氏が、ソブリンクラウドの基礎となるデータ主権について議論した。セキュリティ、運用統制、各国の考え方の違い、政府・企業・個人それぞれの責任が論点となった。
2. 兼子氏は、主権性はデータの保存場所だけでなく、事業者を誰が支配し、どの法律が適用され、障害時にサービスを継続できるかに関わると強調した。リスク、依存関係、統制を併せて評価し、世界の優れた技術を活用しながら、機微なデータの保護と運用継続に必要な権限を維持する考え方を示した。
3. 兼子氏は、欧州では技術的安全性に加え、法域、所有・支配関係、外国の影響、運用継続性を組み合わせて評価すると説明した。フランスのSecNumCloud、EUのCloud Sovereignty Framework、タレスとGoogleによるS3NSを例に、主権性の評価と認定制度を区別し、暗号鍵を独立して管理する重要性を挙げた。
4. カーター氏は、英国の主として助言に基づくクラウドセキュリティの仕組みと、豪州のより明示的なホスティング、データ所在、評価の制度を比較した。主権性は有無の二択ではなく段階的なものであり、国家として管理すべき重要な能力を見極めつつ、信頼できる同盟国やパートナーへの適切な依存を認めるよう提案した。
5. カーター氏は、機密を扱う防衛システム以外でも、重要インフラなどでプライベートクラウドや外部接続を切り離した構成の利用が広がっていると述べた。ただし、隔離するだけでは主権性は成立せず、運用上のレジリエンス、可用性、分離された環境間の安全なデータ移転も必要だと強調した。
6. 磯和氏は、銀行では従来のオンプレミスシステムが残る一方、AI活用がクラウド移行への関心を高めていると説明した。目的はソブリンクラウドの導入自体ではなく、AIによる事業変革とセキュリティの両立であり、データや運用の要件に応じて複数のクラウド形態を使い分ける方向を示した。
7. 下村氏は、データ主権を国家、企業、個人の三者の関係として捉えることを提案した。国家はルール、監督、プライバシー保護、救済手段を整え、企業は適切なデータ管理、遵守状況の透明化、個人の権利保護を担い、個人は適切なサービスを選べることが重要だとした。企業活動の多国籍化に対応する仕組みも必要だと述べた。
8. カーター氏は、複雑なデータ処理の実態を個人が理解し、同意の仕組みだけで実質的な選択を行うことの難しさを指摘した。AIでは学習場所、推論、モデルの重み、バイアスなどの問題も加わり、サイバー攻撃と情報操作が組み合わされることで、個人の意思決定と国家主権の双方が損なわれ得ると述べた。

7. Shimomura proposed treating data sovereignty as a relationship among states, companies, and individuals. Governments should establish rules, oversight, privacy protections, and remedies; companies should manage data responsibly, demonstrate compliance, and protect individual rights; individuals should be able to choose appropriate services, supported by arrangements that address multinational business activity. 8. Carter questioned whether individuals can realistically understand complex data-processing arrangements or exercise meaningful choice through consent mechanisms alone. He argued that AI adds questions about training locations, inference, model weights, and bias, while cyberattacks and information manipulation can jointly undermine both individual decision-making and national sovereignty. 9. Participants explored international cooperation as a response to dependence on major technology providers. Isowa cited long-term cooperation in nuclear fusion as a reason not to dismiss collaboration across political systems; Carter recommended that middle powers identify shared priorities, particularly around AI, and Kaneko advocated common evaluation criteria that give users meaningful choices. 10. Nagamiya concluded that sovereign-cloud discussions must extend beyond economic security to include individuals and the emerging AI paradigm. Participants called for new ways to coordinate governments, businesses, and citizens across borders, clarify who may use which data, protect data that must remain excluded, and maintain practical control without rejecting beneficial international technologies.	9. 大手技術事業者への依存に対応するため、国際協力の可能性が議論された。磯和氏は核融合分野の長期的な国家間協力を挙げ、政治体制の違いだけで協調を否定すべきではないとした。カーター氏は、特にAIについて中規模国家が共通の優先課題を見いだすことを提案し、兼子氏は利用者が適切に選べる共通の評価基準を求めた。 10. 永宮氏は、ソブリンクラウドの議論を経済安全保障だけでなく、個人とAI時代の新たな課題へ広げる必要性を示した。国境を越えて政府・企業・個人を調整し、誰がどのデータを利用できるか、利用させてはいけないデータをどう除外するかを明確にし、有益な国際技術を排除せず実効的な統制を保つ仕組みが求められた。

D2-S15 Day #2 PM Closing 18:30–18:35 JST

Session: Day #2 PM Closing Speaker: Christine Callsen (Chief of Staff and Director, MITRE)	セッション：Day #2 クロージング 登壇者：クリスティン・カルセン (MITRE 首席補佐官兼戦略業務担当ディレクター)

1. The speaker highlighted MITRE's partnership with Japan since 1964, beginning with work supporting Japan's acquisition, integration, and testing of its first automated air defense system. She described its development into a lasting relationship built on trust, continuity, and collaboration. 2. She noted that this cooperation now spans integrated air and missile defense, command and control, cybersecurity, space situational awareness, and mission engineering, alongside MITRE's longstanding partnership with Keio University on the symposium. 3. Recalling the message that "cyber resilience is strategic resilience," she emphasized that persistent, adaptive, and growing threats—particularly those targeting critical infrastructure—require urgent attention. Building resilience into systems is essential to achieving strategic cybersecurity goals. 4. She highlighted the day's discussions on active cyber defense, data and cloud sovereignty, and preparation for a post-quantum world as important contributions to strengthening resilience. 5. She stressed that enduring security is built through cooperation and urged Japan and its partners to meet current challenges with decisive action. She emphasized mutual learning through forums such as the symposium and thanked participants for their contributions.	1. 講演者は、MITREと日本の協力が1964年に始まり、日本初の自動化された防空システムの調達、統合、試験を支援した経緯を紹介した。その技術的な協力が、信頼、継続性、協働に支えられた長期的な関係へ発展したと述べた。 2. 現在の協力は、統合防空・ミサイル防衛、指揮統制、サイバーセキュリティ、宇宙状況把握、ミッションエンジニアリングに広がっていると説明した。また、本シンポジウムを通じた慶應義塾大学との長年の連携にも言及した。 3. 「サイバーレジリエンスは戦略的レジリエンスである」という前日の発言を振り返り、持続的かつ適応的に増大する脅威、特に重要インフラへの脅威に早急に対応する必要性を強調した。システムにレジリエンスを組み込むことが、サイバーセキュリティの戦略目標の達成につながると述べた。 4. 当日に議論された能動的サイバー防御、データ・クラウド主権、量子コンピューター時代に備えたシステムの準備を、レジリエンス強化にとって重要なテーマとして挙げた。 5. 持続的な安全保障は協力によって築かれると強調し、日本とパートナー国が現在の課題に断固とした行動で対応するよう呼びかけた。シンポジウムのような場で互いに学ぶ意義を述べ、参加者の貢献に感謝して締めくくった。

DAY 3 2026-10-29 木曜日

Keio University, Mita Campus; West School Building 1F West Hall
慶應義塾大学 三田キャンパス 西校舎 1F 西ホール

D3-S1 Day #3 AM Opening 09:00–09:05 JST

Session: Day #3 AM Opening Speaker: Muhammad Salman	セッション：Day #3 AM オープニング 登壇者：ムハンマド・サルマン
1. Muhammad Salman welcomed participants to the third day of the 16th International Cybersecurity Symposium and reflected on the valuable insights gained from the preceding two days of presentations and discussions. 2. He introduced the day's opening keynote by Christopher A. Ford, noting that it would bring an important strategic perspective to the discussions. 3. He highlighted sessions on privacy-enhancing technologies, including confidential computing, cryptographic technologies, and data clean rooms, as tools for secure data collaboration while protecting privacy. 4. He outlined discussions on the relationship between economic security and cybersecurity, including cyber threats affecting supply chains, critical infrastructure, research and development, and international cooperation. 5. He introduced discussions on protecting critical infrastructure and energy systems, with particular attention to cyber resilience and public-private partnerships. 6. He noted that the program would address security across the global semiconductor supply chain, covering design, manufacturing, equipment, materials, and advanced packaging. 7. He highlighted the planned memorandum-of-understanding signing ceremony for international research cooperation in cybersecurity and privacy, describing it as a step toward turning shared expertise into practical outcomes. 8. He emphasized that cybersecurity is a strategic concern requiring close cooperation among government, academia, industry, and international partners. As AI and quantum computing advance, he called for stronger trust, resilience, and international cooperation and wished participants a productive day.	1. ムハンマド・サルマン氏は、第16回サイバーセキュリティ国際シンポジウムの3日目に参加する皆様を歓迎し、前日までの2日間の講演と議論から多くの有益な知見が得られたと振り返った。 2. 当日の冒頭に予定されたクリストファー・A・フォード氏の基調講演を紹介し、議論に重要な戦略的視点をもたらすものと位置付けた。 3. プライバシーを保護しながら安全にデータを共同利用するための技術として、コンフィデンシャル・コンピューティング、暗号技術、データクリーンルームなどのプライバシー強化技術を扱うセッションを紹介した。 4. 経済安全保障とサイバーセキュリティの関係を取り上げ、サプライチェーン、重要インフラ、研究開発、国際協力に関わるサイバー脅威を議論すると説明した。 5. 重要インフラとエネルギーシステムの保護に関する議論を紹介し、サイバーレジリエンスと官民連携に焦点を当てると述べた。 6. 世界の半導体サプライチェーンの安全性について、設計、製造、装置、材料、先端パッケージングまでを対象に議論すると紹介した。 7. サイバーセキュリティとプライバシー分野の国際研究協力に関する覚書の調印式に触れ、共有された専門知識を実践的な成果へつなげる一歩として意義を示した。 8. サイバーセキュリティは戦略的な課題であり、政府、学術界、産業界、国際的なパートナーの緊密な協力が必要だと強調した。AIや量子コンピューターの進展を踏まえ、信頼、レジリエンス、国際協力の強化を呼びかけ、実りある一日を祈念した。

D3-S2 Keynote Speech 09:05–09:20 JST

Session: Keynote Speech Speaker: Christopher A. Ford (Former U.S. Assistant Secretary of State; currently director of the School of Defense and Strategic Studies for Missouri State University)	セッション：基調講演 登壇者：クリストファー・フォード (元米国務次官補、現ミズーリ州立大学 防衛・戦略研究スクール長)

1. Christopher Ford argued, in his personal capacity, that multilateral partnerships are essential for democracies to meet current and future security challenges, especially in advanced technologies. Drawing on a recent visit to Japan, he described the US–Japan alliance as strong and increasingly effective.
2. He reflected on the United States' shift toward strategic competition and his involvement in technology restrictions concerning China, including civil nuclear cooperation and Huawei. He emphasized that denying adversaries access to technology is only one part of a successful strategy.
3. Ford argued that technology restrictions primarily buy time: the decisive question is how quickly the United States and its partners can innovate and advance themselves. He called for closer cooperation with friends rather than policies driven by short-term transactions, economic isolationism, or narrow national advantage.
4. He criticized post-Cold War complacency and cooperation that lacked clear strategic objectives, arguing that China and Russia pursued competing projects that challenged the international order. In his assessment, the United States can no longer address these challenges alone, particularly where technological change can reshape global power.
5. His first proposed line of effort was jointly creating new value through research, innovation, technology development, and adoption. He advocated applying these advances across economic activity, public services, healthcare, defense, and scientific understanding.
6. He linked innovation with cooperative technology governance, calling for partners to manage safety risks, disruptions, and implementation challenges while realizing competitive benefits. He warned that attempts to succeed through economic nationalism alone could weaken long-term competitiveness.
7. His second line of effort was protecting economies, political systems, and societies by strengthening resilience. He recommended sustained supply-chain de-risking and closer integration of defense industrial bases through technology sharing, licensing, co-production, and joint ventures to meet demanding wartime requirements.

1. クリストファー・フォード氏は、個人の見解として、民主主義諸国が現在と将来の安全保障課題、特に先端技術分野の課題に対応するには、多国間パートナーシップが不可欠だと述べた。最近の訪日経験を踏まえ、日米同盟は強固で、実効性も高まっているとの認識を示した。
2. 米国の戦略的競争への政策転換と、中国との民生用原子力協力やファーウェイに関する技術規制に携わった経験を振り返った。そのうえで、敵対勢力への技術移転を制限することは、優れた戦略の一部にすぎないと強調した。
3. 技術規制の主な役割は時間を稼ぐことであり、決定的なのは米国とパートナーが自らどれだけ速く革新・前進できるかだと主張した。短期的な取引、経済的孤立主義、狭い国益の追求ではなく、友好国との緊密な協力を求めた。
4. 冷戦後の慢心と明確な戦略目標を欠く協力を批判し、中国とロシアは国際秩序に対抗する構想を進めてきたとの見方を示した。技術変化が世界の力の均衡を変え得る中、米国だけではこうした課題に対処できないと述べた。
5. 第一の取り組みとして、共同研究、技術革新、新技術の開発・導入による新たな価値の創造を提案した。その成果を経済活動、公共サービス、医療、防衛、科学的理解などの幅広い分野に生かすことを求めた。
6. 技術革新と併せて、技術の統治でも協力し、安全上のリスク、導入に伴う混乱、実装上の課題を管理しながら競争上の利益を得る必要性を示した。経済ナショナリズムだけで成功を目指すことは、長期的な競争力の低下につながりかねないと警告した。
7. 第二の取り組みとして、経済、政治制度、社会を保護し、レジリエンスを高める協力を挙げた。サプライチェーンの継続的なリスク低減と、技術共有、ライセンス供与、共同生産、合弁事業による防衛産業基盤の連携を進め、有事に求められる高度な能力と生産量を確保すべきとした。
8. これらの能力を守るには、サイバーセキュリティの強化、スパイ活動や知的財産の窃取への対策、国家指導者を支える効果的な情報収集・分析・情報統合・意思決定支援も必要だと強調した。
9. 第三の取り組みとして、敵対勢力の優位を阻み、その戦略を困難にする協調的な対抗措置を提案した。「技術管理外交」、国家安全保障上の輸出管理の連携、規制迂回への共同対処、不安定化を招く行動に代償を課す経済的圧力の調整を求めた。
10. 経済外交では制限や圧力だけでなく、第三国への前向きな誘因も組み合わせるべきだと述べた。技術革新、保護、協調的な働きかけを結び付け、相互の安全保障と国際環境の安定を支えるには、明確な目的を持つ継続的なパートナーシップが必要だと結論付けた。

8. He stressed that these capabilities also require stronger cybersecurity, protection against espionage and intellectual property theft, and effective intelligence collection, analysis, information fusion, and decision support for national leaders. 9. His third line of effort was coordinated action to deny adversaries advantages and complicate their strategies. He advocated “technology control diplomacy,” aligned national-security export controls, cooperation against circumvention, and coordinated economic pressure that imposes costs for destabilizing behavior. 10. Ford emphasized that economic statecraft should also include positive incentives for third countries, rather than relying only on restrictions and pressure. He concluded that sustained, purposeful partnerships are necessary to combine innovation, protection, and coordinated influence in support of mutual security and a more stable international environment.	

D3-S3 Speech 09:20–09:35 JST

Session: Speech Speaker: KAGEI Takayoshi (Director, Secretariat of the Personal Information Protection Commission, Personal Information Protection Legal and Policy Office)	セッション：スピーチ 登壇者：影井 敬義 (個人情報保護委員会 事務局 個人情報保護制度担当室 企画官)

1. Takayoshi Kagei outlined the 2026 amendment to Japan's Act on the Protection of Personal Information (APPI) and preparations for implementation. He emphasized balancing appropriate data use, including AI development, with the protection of individuals' rights and interests.
2. He identified four pillars of the amendment: promoting appropriate data utilization, introducing risk-based requirements, preventing inappropriate data use, and strengthening enforcement. He stated that the amended law would take effect no later than July 17, 2028.
3. He explained that a new exemption would permit certain provision and acquisition of data without individual consent when the sole purpose is statistical production. AI development would fall within the exemption insofar as it qualifies as statistical production.
4. He described risk-based measures addressing children under 16, facial feature data, and obligations for entrusted processors, alongside limited relaxation of notification requirements for low-risk breaches. He also outlined restrictions on inappropriate targeting-related data practices and additional requirements under the opt-out scheme.
5. Kagei explained that stronger enforcement would include revised conditions for orders, increased penalties for certain violations, and administrative monetary penalties for serious violations. The PPC is preparing detailed rules, guidelines, enforcement arrangements, and public-awareness materials to make the framework work effectively in practice.
6. He highlighted parliamentary supplementary resolutions calling for the statistical-purpose exemption to support research, development, and business activity while protecting individuals. These resolutions also emphasize research into and practical application of privacy-enhancing technologies (PETs).
7. He described PETs as tools for using data while protecting confidentiality and privacy, citing anonymization, pseudonymization, differential privacy, secure multi-party computation, confidential computing, and trusted execution environments. Their relevance is increasing as cloud services can involve access beyond the direct control of the organization holding the data.

1. 影井敬義氏は、2026年の個人情報保護法改正と施行準備について説明し、AI開発を含む適正なデータ利活用と、個人の権利・利益の保護を両立する重要性を強調した。
2. 改正の四つの柱として、適切なデータ利活用の促進、リスクに応じた規律の整備、不適正なデータ利用の防止、法執行の実効性強化を挙げた。改正法は遅くとも2028年7月17日までに施行されると説明した。
3. 統計作成のみを目的とする場合、一定のデータの提供・取得について本人同意を不要とする特例を紹介した。AI開発についても、統計作成に該当する範囲で対象となると説明した。
4. リスクに応じた措置として、16歳未満の子どもへの配慮、顔特徴データに関する要件、委託先の義務、低リスクの漏えいにおける通知義務の限定的な緩和を挙げた。また、個人へのターゲティングに関わる不適正なデータ利用・取得の禁止や、オプトアウト制度の追加要件を説明した。
5. 法執行の強化として、命令の要件見直し、一部の罰則強化、重大な違反に対する課徴金制度の導入を説明した。個人情報保護委員会では、制度が実務で効果的に機能するよう、詳細な規則、ガイドライン、執行体制、周知資料を整備していると述べた。
6. 国会の附帯決議では、個人の権利・利益を保護しながら、統計作成等の特例を研究開発や事業活動に役立てることが求められていると紹介した。プライバシー強化技術（PETs）の調査と実用化の促進も重視されていると説明した。
7. PETsを、機密性やプライバシーを保護しながらデータを利用するための技術と説明し、匿名化、仮名化、差分プライバシー、秘密計算、コンフィデンシャル・コンピューティング、TEEを例示した。クラウド利用によって保有組織の直接管理が及ばない場所でデータにアクセスされ得る中、その重要性が高まっていると述べた。
8. データの特性とリスクに応じて対策を選び、技術的措置と組織的措置を組み合わせる必要性を強調した。目的外利用や不適切な第三者提供の防止、安全管理措置、元データの復元防止、不要となったデータの削除を重要な論点として挙げた。
9. 個人情報保護委員会事務局に新設され、自身が率いる技術政策チームを、法的要件と技術の実態を結び付ける組織として紹介した。当面は改正法の施行上の課題とPETsの活用を検討し、結果を規則、ガイドライン、報告書などに反映すると述べた。
10. 改正の主要な論点について、関係者との意見交換により実務上の課題を把握し、今後の議論とパブリックコメントなどを進める方針を示した。技術的な専門性とPETsの実務的な活用が、データ利活用と個人の権利・利益の保護の両立に役立つと結論付けた。

8. He emphasized selecting safeguards according to data characteristics and risks and combining technical and organizational measures. Key considerations include purpose limitation, prevention of inappropriate third-party disclosure, security controls, prevention of reconstruction of original data, and deletion when data is no longer needed. 9. Kagei introduced the PPC Secretariat's new technical policy team, which he leads, as a bridge between legal requirements and technical realities. Its immediate priority is examining implementation issues, including how PETs can support appropriate data use and stronger protection, and reflecting findings in rules, guidelines, and reports. 10. He described ongoing engagement with stakeholders to identify practical issues across the amendment's main topics, followed by further discussions and public-comment procedures. He concluded that technical expertise and practical use of PETs can help reconcile data utilization with the protection of individuals' rights and interests.	

D3-P4 Panel 09:35–10:35 JST

Session: Enhancing Technology, PETs Moderator: Katsumi Takahashi (Chief Security Scientist of NTT Social Informatics Laboratories) Panelist: Yoshinori Sato (Project Manager Hitachi, Ltd. Business Architecture Research Department, Systems Innovation Center, Research & Development Group) Panelist: Ryosuke Takahashi (Chairperson, Privacy Tech Association) Panelist: Mitsuo Wakameda (Senior Specialist, Center for the Strategy of Emergence, The Japan Research Institute, Limited)	セッション：Enhancing Technology, PETs モデレーター：高橋 克巳 (NTT株式会社 社会情報研究所 主席研究員) パネリスト：佐藤 嘉則 (株式会社日立製作所 研究開発グループ システムイノベーションセンタ ビジネスアーキテクチャ研究部 プロジェクトマネージャ) パネリスト：高橋 亮祐 (プライバシーテック協会 会長) パネリスト：若目田 光生 (株式会社日本総合研究所, 創発戦略センター, シニアスペシャリスト)

1. Moderated by Katsumi Takahashi, the panel brought together Yoshinori Sato, Ryosuke Takahashi, and Mitsuo Wakameda to discuss how privacy-enhancing technologies (PETs) can support secure data use, AI development, and the statistical-purpose exception described in the preceding presentation. The moderator traced the parallel evolution of technology and institutions through the eras of statistics, big data, and AI.
2. Participants distinguished two complementary approaches: transforming data to reduce identifiability and protecting confidentiality through encryption and trusted execution environments (TEEs), including during processing. They emphasized that no single technology meets every requirement and that PETs must be combined with appropriate legal arrangements, organizational measures, and operational practices.
3. Sato described Hitachi's Tokumei Bank as a commercial service combining searchable encryption, anonymization, TEE-based processing, and other techniques where appropriate. He presented applications involving patient registries, evaluation of preventive healthcare policies, and pharmaceutical–AI collaboration that protects both proprietary data and algorithms.
4. Ryosuke Takahashi explained that confidential computing protects data in use through hardware-isolated environments and that expanding GPU support makes it increasingly relevant to AI. He introduced KDDI's data clean room as an example combining confidential computing with other PETs to enable analysis across organizations while protecting commercially valuable information.
5. Takahashi also highlighted confidential AI as relevant to economic security and data and AI sovereignty. He argued that technical protection and verification can help organizations use advanced overseas computing resources without exposing sensitive data, while further development is needed to support large AI workloads in policy and procurement requirements.
6. Wakameda described synthetic banking data used for university data-science education and identified four barriers to wider PETs adoption: insufficient technical guidance, institutional and regulatory challenges, limited understanding among decision-makers and consumers, and a shortage of significant cross-sector use cases.

1. 高橋克巳氏の進行の下、佐藤嘉則氏、高橋亮祐氏、若目田光生氏が、安全なデータ利活用、AI開発、前の講演で紹介された統計作成等の特例に対するプライバシー強化技術（PETs）の貢献を議論した。モデレーターは、統計、ビッグデータ、AIという流れの中で、技術と制度が並行して発展してきた経緯を紹介した。
2. PETsには、データを加工して個人を識別しにくくする方法と、暗号や信頼実行環境（TEE）によって処理中も含めて機密性を守る方法があり、両者は補完関係にあると整理した。万能な技術はなく、複数の技術と法制度、組織的対策、運用を組み合わせる必要性が強調された。
3. 佐藤氏は、検索可能暗号、匿名化、TEEによる処理、必要に応じた他の技術を組み合わせる日立の商用サービス「匿名バンク」を紹介した。患者レジストリ、予防医療施策の効果検証、製薬会社のデータとAI企業のアルゴリズムの双方を秘匿する協業を活用例として示した。
4. 高橋亮祐氏は、コンフィデンシャルコンピューティングがハードウェアの隔離領域で処理中のデータを保護し、GPU対応の進展によってAIにも適用しやすくなっていると説明した。KDDIのデータクリーンルームを例に、他のPETsと組み合わせ、競争力の源泉となる情報を守りながら組織間の分析を可能にすると述べた。
5. 高橋亮祐氏は、経済安全保障とデータ・AI主権の観点から、コンフィデンシャルAIの意義も示した。機微なデータを開示せずに海外の高度な計算資源を利用するには、技術による保護と検証が重要であり、政策や調達要件でも大規模AIワークロードへの対応を進める必要があると述べた。
6. 若目田氏は、銀行取引を基に作成した合成データを大学のデータサイエンス教育に活用する事例を紹介した。また、PETs普及の障壁として、技術的指針の不足、制度・規制上の課題、経営者や生活者の理解不足、分野を越えた重要な活用事例の不足という四つを挙げた。
7. 若目田氏は、ビジョンの共有、対象を明確にした社会とのコミュニケーション、ルールと実装の仕組みづくり、官民連携、国のAI戦略との同期、政府主導の象徴的事例、PETsを組み込んだサービスの拡大という七つの政策提言を示した。安全性基準、技術カタログ、第三者監査、人材育成、モデル契約、提供者の評価などを支援策として挙げた。
8. 統計作成等の特例については、目的外利用と不適切な第三者提供の防止、元データの復元防止、不要なデータの削除、リスクに応じたガバナンスを重視した。PETsは保護措置を技術的に実行する手段となり、システムに侵入された場合のデータ保護にも貢献し得ると議論された。

7. He presented seven policy recommendations: share a clear vision, design targeted public communication, establish rules and implementation mechanisms, strengthen public-private coordination, align PETs with national AI strategy, create government-led flagship use cases, and expand services with PETs built in. Supporting measures include safety criteria, technology catalogs, independent audits, skills development, model contracts, and provider assessment. 8. In discussing the statistical-purpose exception, participants emphasized preventing unauthorized purposes and third-party disclosure, protecting against reconstruction of source data, deleting unnecessary data, and applying risk-based governance. They argued that PETs can technically enforce safeguards and improve data protection even when an attacker enters a system. 9. Participants explored how multi-company data collaboration could improve analytical value without concentrating all data in a single dominant platform. Ryosuke Takahashi stressed stronger governance as input restrictions become more flexible, while Wakameda cautioned that confidential computation is not always necessary if appropriately transformed data can provide sufficient analytical quality. 10. The panel called for practical reference cases that align legal requirements with technology and begin with clearly defined social problems. Participants hoped that Japanese implementation experience would support new services, cross-border collaboration, Data Free Flow with Trust (DFFT), economic security, and international standards, while sharing value derived from data rather than merely distributing raw data.	9. 複数企業のデータ連携により、一つの巨大プラットフォームに情報を集中させずに分析価値を高める可能性が議論された。高橋亮祐氏は入口側の制約が柔軟になるほど強いガバナンスが必要だとし、若目田氏は、加工済みデータで十分な分析品質を得られる場合には、必ずしも秘匿状態での計算に限定する必要はないと指摘した。 10. 法制度と技術を結び付けた実践的な参考事例を増やし、解決すべき社会課題を起点にデータ連携を設計するよう求めた。日本での実装経験が、新サービス、国境を越える連携、DFFT、経済安全保障、国際標準につながることを期待し、生データの配布ではなくデータから生まれる価値を共有する方向性を示した。

D3-S5 Speech 11:00–11:15 JST

Session: Speech Speaker: James Miller (CEO Japan Secure Solutions)	セッション：スピーチ 登壇者：ジェームズ・ミラー（ジャパン・セキュア・ソリューションズ CEO）

1. James Miller reflected on Professor Dave Farber's legacy of openness and interoperability, explaining that the Internet grew through independent systems communicating through shared protocols. He argued that AI presents a similar opportunity, but requires mechanisms for identity, security, governance, and trust across organizational boundaries.
2. He distinguished AI security from AI sovereignty. Security concerns protecting systems and data, constraining operations, detecting misuse, recovering from failures, and verifying compliance; sovereignty concerns durable authority and meaningful choices over infrastructure, data, models, and decisions. Neither domestic hosting nor strong security alone guarantees both.
3. Miller proposed starting with the accountable person or institution rather than the AI model. Organizations must identify the responsible principal, give agents distinct identities, and define precisely which actions, resources, time periods, and constraints each delegation covers; an agent's claim of authorization or possession of login credentials is not sufficient proof.
4. Using a mobile-phone plan example, he distinguished permission to inspect usage and recommend savings from permission to change a contract. Receiving systems should verify the agent's identity, relationship with the customer, specific delegation, proposed action, and current authority, with appropriate approval for irreversible steps.
5. He connected agent governance with zero-trust principles: each consequential request should be evaluated against identity, authority, resources, and context. Narrowly scoped, time-limited permissions must be enforced at data and tool boundaries, while records should support auditing, revocation, human intervention, disputes, and recovery.
6. He compared AI agents with privileged insiders, noting that continuously operating agents can combine tools and adapt in unexpected ways. He recommended least privilege, separation of duties, behavioral monitoring, continuous adversarial evaluation, threat hunting, and automated containment, with evidence connecting tool calls to valid permissions.

1. ジェームズ・ミラー氏は、デイビッド・ファーバー教授が重視した開放性と相互運用性を振り返り、独立したシステムが共通のプロトコルで通信することでインターネットが発展したと説明した。AIにも同様の可能性がある一方、組織を越えてアイデンティティ、セキュリティ、ガバナンス、信頼を確立する仕組みが必要だと述べた。
2. AIセキュリティとAI主権を区別した。セキュリティはシステム・データの保護、操作の制約、不正検知、復旧、ルール遵守の検証に関わり、主権はインフラ、データ、モデル、意思決定に対する持続的な権限と実質的な選択肢に関わると説明し、国内設置や強固なセキュリティだけでは両方を保証できないとした。
3. AIモデルではなく、責任を負う人間や組織を出発点とすることを提案した。責任主体と代理するエージェントを特定し、認める行為、利用資源、有効期間、制約を明確にする必要があり、エージェントの「指示された」という主張やログイン認証情報だけでは認可の証拠にならないと述べた。
4. 携帯電話の料金プランを例に、利用状況を確認して節約策を提案する権限と、契約を変更する権限は異なると説明した。要求を受けるシステムは、エージェントの身元、顧客との関係、具体的な委任、予定する行為、権限の有効性を確認し、取り消せない操作には適切な承認を求める必要があるとした。
5. エージェントの統制をゼロトラストの原則と結び付け、重要な要求ごとに身元、権限、資源、状況を評価すべきだと述べた。対象と期限を限定した権限をデータやツールへのアクセス境界で適用し、記録によって監査、権限取消し、人間の介入、異議申立て、復旧を可能にするよう求めた。
6. AIエージェントを特権を持つ内部者になぞらえ、継続的に動作し、複数のツールを組み合わせ、想定外の行動を取る可能性を指摘した。最小権限、職務分離、行動監視、継続的な敵対的評価、脅威ハンティング、自動封じ込め、ツール呼び出しと有効な権限を結び付ける証拠の整備を提案した。
7. 適切な制御によって低リスクの作業を事前承認し、重大な行為には厳格な確認を求めることで、より高度な自律性を実現できると述べた。一方、認証、認可、ポリシー適用、監査証拠を単一の事業者に全面依存すると、セキュリティ対策があっても実質的な主権を持てない可能性があると指摘した。
8. 多くの国や組織にとって、技術の全面的な自給自足を主権の基準とするのは現実的ではないと述べた。米国、欧州、日本の強みと依存関係を比較し、日本には協力、検証可能な統制、監査、復旧、事業者を切り替えられる能力を通じて、信頼を競争上の強みに変える機会があるとした。

7. Miller argued that effective controls can enable greater autonomy by pre-authorizing low-risk work while applying stronger checks to consequential actions. However, dependence on a single provider for authentication, authorization, policy enforcement, and audit evidence may leave organizations without meaningful sovereignty despite having security controls. 8. He rejected complete technological self-sufficiency as a realistic sovereignty standard for most countries and organizations. Comparing US, European, and Japanese strengths and dependencies, he identified an opportunity for Japan to make trust a competitive advantage through cooperation, verifiable control, auditability, recovery, and the ability to change providers. 9. He advocated independently governed identity and authorization systems, portable security evidence, testable interfaces, open standards, and interoperable infrastructure spanning multiple providers from edge to cloud. Domestic capability and international technology use can coexist if organizations retain enforceable control over data, policies, keys, and consequential actions, including during disruption. 10. He concluded with three principles: autonomous AI must operate under legitimate human or institutional authority; trust must be demonstrated throughout the action lifecycle; and sovereignty must be measured by practical ability to choose, enforce rules, sustain essential functions, independently verify outcomes, and cooperate without surrendering accountability.	9. 独立して統治されるアイデンティティ・認可システム、持ち運び可能なセキュリティ証拠、検証可能なインターフェース、オープン標準、複数事業者のエッジからクラウドまでを組み合わせる相互運用基盤を提唱した。障害時も含め、データ、ポリシー、鍵、重大な行為への許可を実効的に管理できれば、国内能力の整備と海外技術の活用は両立できると述べた。 10. 結論として、自律型AIは正当な人間・組織の権限に基づくこと、行為のライフサイクル全体で信頼を証拠によって示すこと、主権は実質的な行使能力で測ることの三点を示した。自ら選択し、ルールを適用し、重要機能を維持し、結果を独立して検証し、説明責任を手放さずに協力できるかが重要だと強調した。

D3-P6 Panel 11:15–12:15 JST

D3-S7 Day #3 PM Opening 13:30–13:35 JST

Session: AI Moderator: James Miller Panelist: Marc Duranton (Senior Fellow, CEA (French Alternative Energies and Atomic Energy Commission)) Panelist: Sarah Sloan (Head of Cybersecurity Policy, Asia and the Pacific, Government Affairs and Public Policy, Cisco) Panelist: Michael Karimian (Director, Digital Diplomacy, Microsoft) Panelist: Ilya Kulyatin (CEO, Foundry Labs)	セッション：AI モデレーター：ジェームズ・ミラー パネリスト：マーク・デュラント (フランス原子力・代替エネルギー庁 (CEA) 上席フェロー) パネリスト：サラ・スローン (シスコ 政府渉外・公共政策部門 アジア太平洋地域サイバーセキュリティ政策責任者) パネリスト：マイクル・カリミアン (マイクロソフト、デジタル外交ディレクター) パネリスト：イリヤ・クリャチン (Foundry Labs CEO)

Session: AI Moderator: James Miller Panelist: Marc Duranton (Senior Fellow, CEA (French Alternative Energies and Atomic Energy Commission)) Panelist: Sarah Sloan (Head of Cybersecurity Policy, Asia and the Pacific, Government Affairs and Public Policy, Cisco) Panelist: Michael Karimian (Director, Digital Diplomacy, Microsoft) Panelist: Ilya Kulyatin (CEO, Foundry Labs) Panelist: Eddy Almand (Founder & CEO, Almata)	セッション：AI モデレーター：ジェームズ・ミラー パネリスト：マーク・デュラント (フランス原子力・代替エネルギー庁 (CEA) 上席フェロー) パネリスト：サラ・スローン (シスコ 政府渉外・公共政策部門 アジア太平洋地域サイバーセキュリティ政策責任者) パネリスト：マイクル・カリミアン (マイクロソフト、デジタル外交ディレクター) パネリスト：イリヤ・クリャチン (Foundry Labs CEO) パネリスト：エディ・アルマンド (Almata 創設者兼 CEO)

Session: Day #3 PM Opening Speaker: Jun Osawa (Senior Fellow, Sasakawa Peace Foundation; Research Director, DENTSU SOKEN Center for Economic Security Research (DCER))	セッション：Day #3 PM オープニング 登壇者：大澤 淳 (笹川平和財団上席フェロー・電通総研経済安全保障研究センター(DCER)研究主幹)

1. Jun Osawa opened the afternoon session of Day 3 on behalf of the Sasakawa Peace Foundation, thanking the organizers, co-organizing partners, and participants from government, industry, and academia. He introduced the relationship between economic security and cybersecurity as a central theme.
2. Osawa highlighted how generative AI is transforming the speed and scale of cyberattacks. AI can automate vulnerability discovery, attack-code development, network intrusion, and lateral movement, enabling sophisticated attacks in much shorter periods.
3. As the interval between vulnerability disclosure and exploitation shrinks, attacks may advance faster than humans can respond. He called for stronger AI-enabled early threat detection and preventive and proactive defense capabilities, alongside responses to attacks.
4. Against the backdrop of strategic competition between the United States and China, competition over advanced technologies, critical materials, and supply chains is intensifying. He explained that economic security requires both protecting sensitive technologies and resources and maintaining the operation of essential industries and infrastructure.
5. Osawa identified semiconductors, energy, telecommunications, finance, and logistics as key sectors supporting economic activity. Their digital interconnection means that an attack on one company can spread through business partners and supply chains, potentially disrupting economic activity across society.
6. He warned about state-sponsored actors infiltrating critical infrastructure during peacetime to establish footholds for use in a crisis. Cybersecurity was presented as a foundation for national economic autonomy and strategic indispensability, extending beyond the protection of information systems.
7. Osawa referred to Japan's efforts to strengthen critical infrastructure security, supply-chain resilience, and frameworks for preventing cyberattacks, while emphasizing that establishing legal and institutional arrangements alone is insufficient.
8. Because much critical infrastructure is privately operated and supply chains cross national borders, he stressed the need for public-private threat-intelligence sharing, joint improvements in response capabilities, and deeper cooperation with international partners.

1. 大澤淳氏は、笹川平和財団を代表して3日目午後のセッションの開会挨拶を行い、主催者、共催機関、国内外の産官学の参加者に謝意を示した。経済安全保障とサイバーセキュリティの関係を中心的なテーマとして提示した。
2. 生成AIの急速な進化が、サイバー攻撃の速度と規模を大きく変えていると指摘した。脆弱性の発見、攻撃コードの開発、ネットワークへの侵入、侵入後の横展開などがAIによって自動化され、高度な攻撃を短時間で実行できるようになっていると説明した。
3. 脆弱性の公表から悪用までの時間が短縮し、人間の対応速度を上回るペースで攻撃が進む可能性を指摘した。そのため、攻撃発生後の対応に加え、AIを活用した脅威の早期検知と、予防的・能動的な防御能力を強化する必要があると述べた。
4. 米中の戦略的競争を背景に、先端技術、重要物資、サプライチェーンをめぐる国家間競争が激化していると説明した。経済安全保障には、機微技術や資源の保護だけでなく、重要産業やインフラの機能を維持することも求められると強調した。
5. 経済活動を支える重要分野として、半導体、エネルギー、通信、金融、物流を挙げた。これらがデジタルネットワークで相互接続されているため、一企業への攻撃が取引先やサプライチェーン全体に波及し、社会全体の経済活動を妨げるおそれがあると指摘した。
6. 国家の支援を受けた攻撃者が、平時から重要インフラに侵入し、有事に備えて足場を築く活動にも警鐘を鳴らした。サイバーセキュリティは情報システムの保護にとどまらず、国家の経済的な自律性と戦略的不可欠性を支える基盤であると位置づけた。
7. 日本における重要インフラの安全確保、サプライチェーンの強靱化、サイバー攻撃を未然に防ぐための制度整備に言及した。一方で、法制度や体制を整えるだけでは十分ではないと強調した。
8. 重要インフラの多くを民間企業が運営し、サプライチェーンが国境を越えてつながっていることから、官民による脅威情報の共有、共同での対処能力の向上、国際的なパートナーとの連携強化が不可欠であると述べた。
9. 笹川平和財団が、安全保障分野における国際的な政策対話や人的ネットワークの構築に取り組んでいることを紹介した。技術、産業、政策、国家安全保障を横断する議論の場を設け、官民協力を具体的な行動につなげる重要性が増していると説明した。
10. 午後のプログラムでは、経済安全保障とサイバーセキュリティの関係、電力網などの重要インフラの保護、サプライチェーンの強化について議論すると紹介した。AIがもたらす新たな脅威への対応と、安全保障を確保するための国際協力について、理解が深まることへの期待を示した。

9. He highlighted the Sasakawa Peace Foundation's role in promoting international security policy dialogue and building professional networks. He emphasized the growing importance of discussions spanning technology, industry, policy, and national security, and of translating public-private cooperation into concrete action. 10. Osawa introduced the afternoon program as an opportunity to examine economic security and cybersecurity, the protection of critical infrastructure such as power grids, and stronger supply chains. He expressed hope that discussions would deepen understanding of AI-related threats and international cooperation to ensure security.	

D3-S8 Keynote Speech 13:35–13:50 JST

Session: Keynote Speech Speaker: Shunsuke Fukuda (Sr. Director / Evangelist, Trend Micro Inc. TrendAI Japan Marketing)	セッション：基調講演 登壇者：福田 俊介 (トレンドマイクロ株式会社 TrendAI マーケティング本部 執行役員 本部長 エバンジェリスト)

1. Shunsuke Fukuda of Trend Micro emphasized that cybersecurity and economic security have become inseparable, with AI emerging as a central issue. He framed AI security as a starting point for discussing how societies can benefit from AI while maintaining security and sovereignty.
2. He introduced Trend Micro's activities across the AI value chain: TXOne for factories and manufacturing equipment, VicOne for automotive and robotics cybersecurity, TrendAI for enterprise AI environments, TrendLife for individuals and families, and Magna AI for AI security consulting. He stressed that consumer protection also matters because individuals are exposed to fraud and other threats.
3. Fukuda described collaboration with Anthropic, OpenAI, and NVIDIA to strengthen cybersecurity through advanced AI models. Applications include threat research, vulnerability discovery, incident response, detection and response, and log prioritization. He also highlighted industry alliances and support for open-weight models, emphasizing the importance of AI that can be examined and assessed.
4. He proposed four steps for securing AI environments: visibility to identify what exists; observability to monitor it continuously; ownership to clarify who owns and operates it; and governance to ensure appropriate oversight of the entire environment.
5. Trend Micro's AI security approach was presented through four pillars: frontier AI threat research, incorporating advanced AI into security platforms, solutions to protect customers' AI environments, and collaboration across the ecosystem. Fukuda stressed that AI developers, platform providers, cloud vendors, and sales partners must work together because no single company can secure AI alone.
6. Fukuda argued that AI itself is becoming critical infrastructure because business operations increasingly depend on it. He cited Japan's treatment of cloud programs as specified critical products and the United Kingdom's designation of data centres as critical national infrastructure as examples of the strategic importance governments attach to AI's underlying infrastructure.

1. トレンドマイクロの福田俊介氏は、サイバーセキュリティと経済安全保障が不可分となり、その中心的な課題としてAIが浮上していると述べた。AIの恩恵を活用しながら安全性と主権を確保するための議論の出発点として、AIセキュリティを位置づけた。
2. AIを取り巻くバリューチェーン全体への取り組みとして、工場・製造設備を守るTXOne、自動車・ロボティクス向けのVicOne、法人のAI環境を守るTrendAI、個人・家庭向けのTrendLife、AIセキュリティのコンサルティングを担うMagna AIを紹介した。詐欺などの被害を受ける個人の保護も、経済安全保障を考えるうえで重要であると強調した。
3. Anthropic、OpenAI、NVIDIAとの連携を通じ、先端AIモデルを脅威調査、脆弱性探索、インシデント対応、検知・対応、ログの優先順位付けなどに活用していると説明した。また、業界横断のアライアンスやオープンウェイトモデルへの支持に言及し、中身を検証・評価できるAIの重要性を示した。
4. AI環境を保護するための四つのステップとして、何が存在するかを把握するVisibility（可視化）、継続的に監視するObservability（可観測性）、所有・運用主体を明確にするOwnership、環境全体を適切に統制するGovernanceを提示した。
5. AIセキュリティへの取り組みを、フロンティアAIを活用した脅威研究、セキュリティ基盤への先端AIの組み込み、顧客のAI環境を保護するソリューション、エコシステム全体での連携という四つの柱で説明した。一社だけでAIを守ることはできず、AI開発企業、プラットフォーム事業者、クラウド事業者、販売パートナーなどの協力が必要であると強調した。
6. 企業活動におけるAIへの依存が高まるなか、AIそのものが重要インフラになりつつあると論じた。AIを支える基盤の戦略的重要性を各国政府が認識している例として、日本におけるクラウドプログラムの特定重要物資への指定と、英国におけるデータセンターの重要国家インフラへの指定を挙げた。
7. クラウド上のAIで企業の機密情報を処理する機会が増えていることや、AIデータセンターが電力・水を必要とすることを指摘した。AIの利用拡大に伴い、計算基盤、データ管理、資源の確保が、国家安全保障と経済安全保障にとって一層重要な課題になると説明した。
8. AI活用と主権の確保を両立させる必要性を強調した。データ、モデル、運用プロセスを適切な管理下に置き、データの保存場所、AIの操作・利用権限、不正アクセスを防ぐ仕組みを明確にすることが重要であると述べた。
9. UAE、ドイツ、サウジアラビアにおいて、国家主権やデータ主権の要件に対応したサービスを提供していると紹介し、現地のデータ管理要件に合わせたXDRの事例に言及した。また、製造ライン、パイプライン、工場内外のデータ交換などのOTセキュリティを挙げ、デジタルと物理の両面でインフラを守る重要性を示した。

7. He highlighted the increasing use of confidential business information in cloud-based AI and the electricity and water required by AI data centres. As AI adoption expands, computing infrastructure, data management, and resource availability become increasingly significant issues for national and economic security. 8. He emphasized that AI adoption must be balanced with sovereignty. Organizations and countries need appropriate control over data, models, and operational processes, including knowledge of where data is stored, who may operate or access AI, and how unauthorized access is prevented. 9. Fukuda described services designed to meet sovereignty requirements in the UAE, Germany, and Saudi Arabia, including XDR services adapted to local data requirements. He also highlighted operational technology security for manufacturing lines, pipelines, and factory data exchanges, stressing the importance of protecting both digital and physical infrastructure. 10. He warned that AI accelerates and lowers the cost of cyberattacks, while AI systems themselves also become targets, including through unauthenticated internet-exposed MCP servers. He concluded that economic security requires trustworthy AI that users can govern, and that the growing necessity of AI makes balancing its adoption with sovereignty essential.	10. AIがサイバー攻撃の高速化・低コスト化に利用される一方、AIシステム自体も攻撃対象となり、認証なしでインターネットに公開されたMCPサーバーなどがリスクになると指摘した。AI時代の経済安全保障には、信頼でき、自ら管理できるAIが必要であり、AIの利用が不可欠になるほど、その活用と主権の保護の両立が重要になると結論づけた。

D3-S9 Speech 13:50–14:05 JST

Session: Speech Speaker: Jun Osawa	セッション：スピーチ 登壇者：大澤 淳

1. Jun Osawa explained the growing importance of economic security by tracing the transition from Cold War systemic competition to post-Cold War globalization. He argued that China's rise is bringing the world into a new period of systemic competition in which national security increasingly shapes economic relations.
2. He anticipated prolonged competition between China's authoritarian model involving digital surveillance and the liberal democratic model. In his view, choices by countries in the Global South make preserving technological and economic advantages particularly important.
3. Osawa introduced DIME—diplomacy, information or intelligence, military power, and economic power—as instruments of national strategy. He positioned economic security within this framework and emphasized cybersecurity's role in protecting advanced technologies and sustaining economic advantages.
4. He identified U.S. Vice President Mike Pence's 2018 Hudson Institute speech as a turning point in U.S. policy toward China. He linked the speech's allegations of cyber-enabled technology theft to subsequent tightening of economic-security-related restrictions.
5. Discussing "Made in China 2025," Osawa argued that cyber operations have been used to acquire technologies relevant to its priority sectors. He referred to attacks targeting Japan and warned that unfair technology transfers could undermine both industrial competitiveness and confidence in rules-based free trade.
6. He presented Nortel and Westinghouse as examples of companies whose competitiveness, in his assessment, was damaged by cyber-enabled intellectual-property theft. His broader argument was that the loss of advanced technology can weaken both individual companies and national economic strength.
7. Osawa identified two central connections between economic security and cybersecurity: preventing the leakage of advanced technology and maintaining the functioning of critical infrastructure. He related these objectives to securing strategic supplies, preserving national capabilities, and cooperating with like-minded countries.

1. 大澤淳氏は、冷戦期の体制間競争から冷戦後のグローバリゼーションへの移行を振り返り、経済安全保障が重要になった背景を説明した。中国の台頭によって新たな体制間競争の時代に入りつつあり、国家安全保障が経済関係を左右する度合いが高まっているとの見方を示した。
2. デジタル監視を伴う中国型の権威主義と、自由民主主義との競争が長期化すると見通した。特にグローバルサウス諸国が自国の発展に適したモデルを選択する中で、技術的・経済的な優位を維持することが重要になると論じた。
3. 国家戦略の手段として、外交、情報・インテリジェンス、軍事力、経済力を組み合わせる「DIME」を紹介した。経済安全保障をこの枠組みに位置づけ、先端技術を保護し、経済的な優位を維持する上でサイバーセキュリティが重要な役割を果たすと説明した。
4. 2018年にペンス米副大統領がハドソン研究所で行った演説を、米国の対中政策の転換点として挙げた。演説で示されたサイバー攻撃による技術窃取への批判と、その後の経済安全保障に関する規制強化との関係を説明した。
5. 「中国製造2025」の重点分野に関連する技術の獲得に、サイバー攻撃が利用されてきたとの見解を示した。日本を標的とする攻撃にも触れ、不公正な技術移転は産業競争力だけでなく、ルールに基づく自由貿易体制への信頼も損ない得ると警告した。
6. ノーテルとウェスティングハウスを取り上げ、サイバー攻撃による知的財産の流出が競争力を損なった事例として説明した。その上で、先端技術の喪失は個別企業の問題にとどまらず、国家の経済力を弱める可能性があると論じた。
7. 経済安全保障とサイバーセキュリティを結びつける中心的な課題として、先端技術の流出防止と、重要インフラの機能維持の二つを提示した。これらを、戦略物資の確保、国力の維持、同志国との協力に関連づけて説明した。
8. 日本の経済安全保障の枠組みにおいて、基幹インフラ役務の安定的な提供の確保が重要だと述べた。有事にも電力・エネルギー、鉄道、航空などを機能させ続けるため、情報システムやOTの保護と、供給事業者に関するリスクへの配慮が必要だと説明した。
9. 台湾有事への懸念を背景に、Volt TyphoonやSalt Typhoonに関連するサイバー活動と、重要インフラへの影響について論じた。また、攻撃者が使用するサイバーインフラの無害化措置を含む、能動的サイバー防御にも言及した。
10. 電通総研の経済安全保障研究センター（DCER）について、研究活動、企業向けの情報発信、書籍『経済安全保障とビジネス』を紹介した。続くパネルでは、企業実務、経済学、国際貿易の視点から、経済安全保障とサイバーセキュリティを議論すると説明した。

8. Referring to Japan's economic-security framework, he emphasized the stable provision of critical infrastructure services. Electricity, energy, railways, and aviation must continue operating during contingencies, requiring protection of their information systems and operational technology, together with attention to supplier risks. 9. Against the backdrop of a possible Taiwan contingency, he discussed concerns about cyber activities associated with Volt Typhoon and Salt Typhoon and their implications for critical infrastructure. He also referred to active cyber defense, including measures to neutralize infrastructure used by attackers. 10. He introduced the Dentsu Soken Center for Economic Security Research (DCER), its research and business outreach, and the book "Economic Security and Business." The following panel would examine economic security and cybersecurity from business-practice, economics, and international-trade perspectives.	

D3-P10 Panel 14:05–15:05 JST

Session: Economic Security and Cybersecurity Moderator: Jun Osawa Panelist: Takashi Ito (Deputy Executive Director, DENTSU SOKEN Center for Economic Security Research (DCER)) Panelist: Arata Kuno (Research Director, DENTSU SOKEN Center for Economic Security Research (DCER))	セッション：経済安全保障とサイバーセキュリティ モデレーター：大澤 淳 パネリスト：伊藤 隆 (電通総研 経済安全保障研究センター(DCER) 副センター長) パネリスト：久野 新 (電通総研 経済安全保障研究センター(DCER) 研究主幹)

1. Moderated by Jun Osawa, the panel examined economic security and cybersecurity from corporate-management and economics perspectives. Ito and Kuno of the Dentsu Soken Center for Economic Security Research emphasized that cybersecurity must be integrated into broader efforts to protect business continuity, competitiveness, and society.
2. Ito argued that economic security should inform management decisions, risk management, business strategy, and growth opportunities, rather than remain limited to geopolitical analysis or regulatory compliance. Cybersecurity requires preventive investment even when the risks have not yet materialized.
3. He described how dependence on foreign markets, resources, technologies, and suppliers can be weaponized for political purposes. Comparing economic security to “mixed martial arts,” he called for a combination of stronger defenses, strategic indispensability, endurance, and cooperation among governments, companies, and like-minded countries.
4. Kuno explained that individual companies’ incentives may produce insufficient cybersecurity investment because their own potential losses differ from the damage imposed on society. Using the Port of Nagoya ransomware incident as an example, he highlighted spillover effects across supply chains, the weakest-link problem, and interdependent security.
5. Kuno distinguished financially motivated attacks, technology and information theft, and attacks intended to paralyze social functions. He argued that technology theft allows attackers to free-ride on research investment and weakens innovation incentives, while attacks on critical infrastructure can create widespread harm that companies and insurance markets cannot fully absorb.
6. The panel supported targeted government action where market mechanisms are insufficient, including information sharing, standards, assessments, regulation, and financial incentives. Kuno stressed that cybersecurity must be combined with measures addressing suppliers, personnel, acquisitions, exports, and research partnerships, while avoiding excessive intervention and compliance costs.

1. 大澤淳氏をモデレータに、電通総研経済安全保障研究センターの伊藤隆氏と久野新氏が、企業経営と経済学の視点から経済安全保障とサイバーセキュリティを議論した。サイバーセキュリティを、事業継続、競争力、社会全体を守るための幅広い取り組みに組み込む重要性が示された。
2. 伊藤氏は、経済安全保障を地政学的な情勢分析や法令遵守にとどめず、経営の意思決定、リスクマネジメント、事業戦略、成長機会に結びつける必要があると述べた。サイバーセキュリティについても、被害が顕在化する前に予防的な投資を判断することが重要だと強調した。
3. 外国の市場、資源、技術、供給者への依存が、政治目的のために武器化され得ると説明した。経済安全保障を「総合格闘技」に例え、防御力、戦略的不可欠性、持久力を高めるとともに、官民、企業間、同志国間の協力を組み合わせる必要性を示した。
4. 久野氏は、個別企業が被る損失と社会全体に生じる損失が異なるため、企業の自主的な判断だけではセキュリティ投資が不足し得ると説明した。名古屋港のランサムウェア被害を例に、サプライチェーンへの波及、最も防御が弱い主体に全体の安全性が左右される「最弱リンク」、相互依存型セキュリティの問題を挙げた。
5. 久野氏は、攻撃の動機を金銭獲得、技術・情報の窃取、社会機能の麻痺に分けて説明した。技術窃取は研究開発への投資にただ乗りし、イノベーションの誘因を損なう一方、重要インフラへの攻撃は、企業や保険市場だけでは十分に引き受けられない広範な社会的損害をもたらすと指摘した。
6. 市場原理だけでは十分に対応できない分野に対し、情報共有、基準整備、安全性の審査、規制、補助金などを組み合わせた政府の対応が必要だと議論した。久野氏は、供給者、人員、買収、輸出、共同研究などへの対策も組み合わせる一方、過度な介入や法令遵守コストの増大を避ける必要があると述べた。
7. 伊藤氏は、顧客企業が経営上の影響力を持ちにくい独立した中堅・中小企業も含め、膨大な取引先全体の安全を確保する難しさを説明した。システムで接続された取引先への支援、重要な供給者に重点を置いたデューディリジェンス、官民連携と情報共有の強化を提案した。
8. 久野氏は、自由貿易と比較優位の利益を評価しつつ、WTOのルールだけでは、水面下の技術窃取、サプライチェーンの混乱、重要インフラへの攻撃に十分対応できないと論じた。議論では、経済を一律に分断するのではなく、機微な領域に対象を絞って保護する考え方が示された。

7. Ito emphasized the difficulty of securing extensive supplier networks, particularly independent small and medium-sized businesses over which customers have limited managerial influence. He advocated support for connected business partners, due diligence focused on critical suppliers, and closer public-private cooperation and information sharing. 8. Kuno reaffirmed the benefits of free trade and comparative advantage while arguing that WTO rules alone cannot adequately address covert technology theft, supply-chain disruption, or attacks on critical infrastructure. The discussion favored focused protection of sensitive areas rather than indiscriminate economic separation. 9. Ito warned against treating low cost and security as a simple binary choice. Supply-chain resilience requires agreement on who bears additional costs, recognition of those costs by customers and consumers, and direct engagement between senior executives so that management priorities are reflected in procurement decisions. 10. The panel concluded that AI is lowering attack costs and expanding the range of viable targets, making more productive, AI-assisted defense increasingly important. Practical priorities included patching known vulnerabilities, protecting backups, minimizing retained sensitive data, containing damage, and accelerating recovery. Management should decide on business suspension and handle its consequences, while IT teams lead technical restoration, with responsibilities rehearsed in advance.	9. 伊藤氏は、低コストと安全性を単純な二者択一で捉えることに警鐘を鳴らした。サプライチェーンの強靱化には、追加費用を誰が負担するかについての合意、顧客や消費者による費用への理解、経営方針を調達実務に反映させるための企業トップ同士の対話が必要だと述べた。 10. AIが攻撃コストを下げ、攻撃対象を広げる中、AIを活用した防御の生産性向上が重要だと議論を締めくくった。既知の脆弱性へのパッチ適用、バックアップの保護、保有する機微情報の最小化、被害の封じ込め、早期復旧を重視した。また、事業停止の判断と経営上の対応は経営者が担い、技術的復旧はIT部門が担うなど、役割分担を定めて事前に訓練する必要性を示した。

D3-C16 Fraunhofer–KGRI MOU Signing Ceremony for Cybersecurity and Privacy Research Cooperation 15:25–15:30 JST

Session: Fraunhofer–KGRI MOU Signing Ceremony for Cybersecurity and Privacy Research Cooperation Signer: Michael Eckel (Head of Security for Critical Infrastructures / Principal Investigator, Fraunhofer Institute for Secure Information Technology SIT | ATHENE) Signer: Teruo Nakatsuma Witness: Georgios Gkoktsis (Deputy Head of Security for Critical Infrastructures, Fraunhofer Institute for Secure Information Technology SIT | ATHENE)	セッション：サイバーセキュリティ・プライバシー分野の研究協力に関するFraunhofer–KGRI間の覚書調印式 署名者：ミヒャエル・エッケル (重要インフラセキュリティ部門長／Principal Investigator、フラウンホーファー安全情報技術研究所(SIT)／ATHENE) 署名者：中妻 照雄 立会人：ゲオルギオス・ゴクツィス (重要インフラセキュリティ部門 副部門長、フラウンホーファー安全情報技術研究所(SIT)／ATHENE)

1. The ceremony marked the signing of a memorandum of understanding (MOU) between Fraunhofer and the Keio University Global Research Institute (KGRI), celebrating a milestone in Japan–Germany cooperation. 2. The signatories introduced were Michael Eckel, Head of Security for Critical Infrastructures and Principal Investigator at the Fraunhofer Institute for Secure Information Technology SIT | ATHENE, and Teruo Nakatsuma, Director of KGRI and Professor in the Faculty of Economics at Keio University. 3. Georgios Gkoktsis, Deputy Head of Security for Critical Infrastructures at the Fraunhofer Institute for Secure Information Technology, was introduced as a witness and invited to join the signatories on stage. 4. The signatories signed the documents, exchanged copies, and signed the second set, completing the signing procedure. 5. Photographs were taken following the signing. The audience was invited to applaud the signatories and witnesses and celebrate this milestone in cooperation between Japan and Germany.	1. フラウンホーファーと慶應義塾大学グローバルリサーチインスティテュート（KGRI）の覚書（MOU）調印式が行われ、日独協力における重要な節目を祝った。 2. 調印者として、フラウンホーファー安全情報技術研究所（SIT）／ATHENEの重要インフラセキュリティ部門長兼Principal Investigatorであるミヒャエル・エッケル氏と、KGRI所長兼慶應義塾大学経済学部教授の中妻照雄氏が紹介された。 3. 立会人として、フラウンホーファー安全情報技術研究所の重要インフラセキュリティ部門副部門長であるゲオルギオス・ゴクツィス氏が紹介され、調印者とともに登壇するよう案内された。 4. 両調印者が文書に署名した後、文書を交換し、もう一部にも署名することで調印の手続きが進められた。 5. 調印後に記念撮影が行われた。司会は、調印者と立会人への拍手を呼びかけ、日独協力の節目を祝福した。

D3-S11 Speech 15:30–15:45 JST

Session: Speech Speaker: Michael Eckel	セッション：スピーチ 登壇者：ミヒャエル・エッケル

1. Michael Eckel of Fraunhofer SIT and ATHENE introduced research on cybersecurity and cyber resilience for energy infrastructure. He emphasized applied research that delivers practical solutions for industry, society, and public policy through cooperation with industrial and public-sector partners.
2. His department addresses security across critical systems, including energy, railways, avionics, industrial IoT, and supply chains. He highlighted the convergence of IT and operational technology (OT), together with the need to address both security and safety.
3. Eckel described the institute's contributions to post-quantum cryptography, including the co-development of SPHINCS+, and its standardization activities through organizations such as the Trusted Computing Group and IETF. These activities support trusted computing, remote attestation, and supply-chain integrity.
4. He defined cyber resilience in energy systems as the ability to sustain essential services during incidents, withstand attacks, and recover afterward. This requires preparation, intrusion detection, containment to prevent compromise from spreading, and restoration of affected systems to normal operation.
5. The HomePPSec project illustrates this approach for interconnected smart homes and small-scale home power systems. It detects abnormal control sequences, isolates affected components, warns connected households, and supports continued operation and recovery, including temporary disconnection where necessary.
6. Eckel introduced CHARRA, an open-source challenge-response remote attestation project using TPM-backed cryptographic evidence. It helps verify software running on remote devices and assess their integrity and trustworthiness, with applications across transport, industrial IoT, and supply-chain security.
7. His team uses AI-based packet-sequence prediction to detect anomalous OT communications and support responses such as dropping or correcting packets. It also researches autonomous response and deception, and combines CHARRA with hardware-signal analysis to detect suspicious hardware activity, including bus eavesdropping or replaced chips.

1. フラウンホーファー安全情報技術研究所（Fraunhofer SIT）およびATHENEのミヒャエル・エッケル氏が、エネルギーインフラのサイバーセキュリティとサイバーレジリエンスに関する研究を紹介した。産業界や公共部門との協力を通じ、産業、社会、公共政策に実用的な解決策を提供する応用研究の重要性を強調した。
2. 所属部門では、エネルギー、鉄道、航空機の電子システム、産業用IoT、サプライチェーンなど、重要システム全般のセキュリティを研究していると説明した。ITとOT（運用・制御技術）の融合に対応し、セキュリティと安全性の双方を確保する必要性を示した。
3. SPHINCS+の共同開発を含む耐量子計算機暗号への貢献と、Trusted Computing GroupやIETFなどでの標準化活動を紹介した。これらの活動を通じ、トラステッドコンピューティング、遠隔アテステーション、サプライチェーンの完全性を支える技術の整備に取り組んでいると述べた。
4. エネルギーシステムのサイバーレジリエンスを、インシデントの発生中も不可欠なサービスを維持し、攻撃に耐え、復旧する能力として説明した。そのためには、事前準備、侵入検知、被害の拡大を防ぐ封じ込め、影響を受けたシステムの通常運用への復旧が必要だと述べた。
5. HomePPSecプロジェクトでは、相互接続されたスマートホームや家庭内の小規模発電システムを対象に、この考え方を実装していると紹介した。異常な制御シーケンスの検知、影響部分の隔離、接続先の家庭への警告、必要に応じた一時的な接続遮断により、運用継続と復旧を支援すると説明した。
6. TPMを基盤とする暗号学的な証拠を用いた、オープンソースのチャレンジ・レスポンス型遠隔アテステーション技術「CHARRA」を紹介した。遠隔機器で実行されるソフトウェアを検証し、完全性と信頼性を評価する仕組みであり、交通、産業用IoT、サプライチェーンのセキュリティなどに応用していると述べた。
7. AIによるパケット列の予測を用いてOT通信の異常を検知し、問題のあるパケットの破棄や修正につなげる研究を説明した。自律的な対応やデセプションに加え、CHARRAとハードウェア信号の分析を組み合わせ、バス上の盗聴やチップの交換など、不審なハードウェア活動を検知する取り組みも紹介した。
8. コンフィデンシャルAIでは、手元の機器からクラウド上のGPUへ移す処理も含め、AIのライフサイクル全体を保護することを目指すと述べた。エンドツーエンドの機密性と処理環境のアテステーションを重視し、AIによる振る舞い分析と、検証可能な完全性の証拠を組み合わせると説明した。

8. Confidential AI research aims to protect the entire AI lifecycle, including workloads transferred from local devices to cloud GPUs. Eckel emphasized end-to-end confidentiality and attestation of the processing environment, combining AI-based behavioral analysis with verifiable integrity evidence. 9. He highlighted ongoing cooperation with Keio University and Hitachi, including a demonstration of CHARRA-based remote attestation incorporating post-quantum security. He also described continued exchanges on energy research and prospects for further joint projects. 10. His concluding message was that AI security should build on established trust foundations. Rather than replacing TPMs, trusted execution environments, or confidential computing with AI, organizations should combine these technologies to create verifiable and trustworthy systems.	9. 慶應義塾大学や日立との継続的な研究協力を紹介し、耐量子暗号による安全性を取り入れたCHARRAベースの遠隔アテステーションのデモ展示に言及した。エネルギー研究に関する意見交換も続けており、今後の共同プロジェクトへの期待を示した。 10. 最後に、AIの安全性は既存の信頼基盤の上に構築すべきであると強調した。TPM、信頼できる実行環境、コンフィデンシャルコンピューティングをAIに置き換えるのではなく、これらを組み合わせ、検証可能で信頼できるシステムを実現することが重要だと結論づけた。

D3-P12 Panel 15:45–16:45 JST

Session: Critical Infrastructure, i.e. Energy Moderator: Tadashi Kaji (Distinguished Researcher, Hitachi, Ltd.) Panelist: Marc Duranton Panelist: Steven Kunsman (Hitachi Energy) Panelist: Georgios Gkoktsis Panelist: Toru Tsuchiya (CEO, Cyber Defense Labs)	セッション：重要インフラ・電力 モデレーター：鍛 忠司 (株式会社 日立製作所 主管研究長) パネリスト：マーク・デュラント パネリスト：スティーブ・クンズマン (日立エナジー・米国) パネリスト：ゲオルギオス・ゴクツィス パネリスト：土屋 徹 (サイバー防衛研究所 代表取締役)

1. Moderated by Tadashi Kaji of Hitachi, the panel examined how to build cybersecure and resilient energy systems. Steven Kunsman, Georgios Gkoktsis, Toru Tsuchiya, and Marc Duranton discussed component trustworthiness, supply-chain security, distributed energy resources, public-private collaboration, and AI.
2. Kunsman described U.S. Department of Energy initiatives to develop reference architectures for electricity-sector operational technology (OT). Adapting the Purdue model and applying IEC 62443 helps define security zones, communication paths, risk assessments, and layered defenses suited to substations, generation facilities, and control systems.
3. He emphasized software and hardware bills of materials (SBOMs and HBOMs) as tools for procurement, supply-chain transparency, and lifecycle vulnerability management. A vulnerable component is not necessarily exploitable in every deployment, so suppliers and asset owners must cooperate continuously. He also highlighted CyTRICS as a means of independently examining products and identifying vulnerabilities for remediation.
4. Gkoktsis explained that renewable generation, household solar panels, controllable loads, and virtual power plants are expanding the attack surface beyond traditional IT/OT boundaries. Securing the remote control of large numbers of distributed energy resources requires trustworthy devices, smart meter gateways, and reliable relationships among operators, aggregators, and consumers.
5. He argued that resilience means anticipating, withstanding, adapting to, and recovering from adverse conditions while sustaining essential functions after compromise. His research combines secure boot, measured boot, and attestation with system-level analysis and operational resilience measures based on observability, controllability, and trustworthiness.
6. Tsuchiya identified aging infrastructure and long-distance networks, geopolitical advanced persistent threats, and AI as major risks for Japan's electricity system. He described using cyber ranges to emulate attacker techniques and create shareable detection rules, allowing infrastructure operators to hunt for similar threats without exposing the identity of the original victim.

1. 日立製作所の鍛忠司氏をモデレーターに、安全でレジリエントな電力・エネルギーシステムの構築方法を議論した。スティーブ・クンズマン氏、ゲオルギオス・ゴクツィス氏、土屋徹氏、マーク・デュラント氏が、機器の信頼性、供給網の安全性、分散型エネルギー資源、官民連携、AIについて意見を交わした。
2. クンズマン氏は、電力分野のOT（運用・制御技術）に適した参照アーキテクチャを整備する米国エネルギー省の取り組みを紹介した。Purdueモデルの適用とIEC 62443の活用により、変電所、発電設備、制御システムに適したセキュリティゾーン、通信経路、リスク評価、多層防御を整理できると説明した。
3. ソフトウェア部品表（SBOM）とハードウェア部品表（HBOM）を、調達、供給網の透明性確保、ライフサイクル全体の脆弱性管理に役立つ手段として挙げた。部品の脆弱性がすべての利用環境で悪用可能とは限らず、供給者と資産保有者の継続的な協力が必要だと述べた。また、製品を第三者が詳細に調査し、脆弱性の発見と修正につなげるCyTRICSを紹介した。
4. ゴクツィス氏は、再生可能エネルギー、住宅の太陽光発電、制御可能な需要側機器、仮想発電所の拡大によって、攻撃対象が従来のITとOTの接続点を越えて広がっていると説明した。多数の分散型エネルギー資源を安全に遠隔制御するには、機器やスマートメーターゲートウェイの信頼性と、運用者、アグリゲーター、消費者間の信頼関係が重要だと述べた。
5. レジリエンスとは、不利な状況を予測し、耐え、適応し、回復するとともに、侵害後も必要な機能を維持する能力であると説明した。セキュアブート、メジャードブート、アテステーションに加え、システム全体の分析や、可観測性、可制御性、信頼性に基づく運用中のレジリエンス評価を研究していると紹介した。
6. 土屋氏は、日本の電力網の主要なリスクとして、老朽化した設備と長距離ネットワーク、地政学的なAPT、AIを挙げた。サイバーレンジで攻撃手法を再現し、共有可能な検知ルールを作成することで、元の被害企業を特定する情報を開示せずに、他のインフラ事業者が同様の脅威を探索できる取り組みを説明した。
7. JCDCや日本のCTP4の活動を踏まえ、単なる情報交換ではなく、実際の共同作業を行う「オペレーショナル・コラボレーション」が重要だと強調した。官民が対等な立場で共通の目標に取り組み、活動を通じて信頼を築く必要があると述べた。また、防御へのフロンティアAIの活用を試験し、検証結果やベストプラクティスをインフラ事業者に共有する取り組みを紹介した。

7. Drawing on JCDC and Japan's CTP4 activities, Tsuchiya stressed operational collaboration rather than information exchange alone. Government and industry should work as equal partners toward shared goals, building trust through joint activity. He also described testing frontier AI for defense and sharing evidence and best practices with infrastructure operators. 8. Duranton proposed a computing continuum in which trusted orchestrators dynamically coordinate services from meters and edge devices to data centres. Security requires authentication, data integrity, traceability, hardware protection, and communication limited to necessary trusted connections, alongside isolation, redundancy, and verification throughout the software supply chain. 9. He advocated resolving disturbances locally wherever possible and escalating only when necessary, reducing dependence on centralized control and limiting cascading failures. AI can assist adaptation and identify unexpected cases, but should operate under mathematical and rule-based supervision with decisions that can be traced and checked. 10. The closing discussion emphasized that AI-enabled attackers may discover and exploit OT vulnerabilities at machine speed, increasing the need for trustworthy AI-assisted and autonomous defense. Panelists called for careful testing, international cooperation, and safeguards against unintended AI behavior, while recognizing AI's potential to support operators and strengthen energy-system resilience.	8. デュラント氏は、メーターやエッジ機器からデータセンターまで、信頼できるオーケストレーターがサービスを動的に調整する計算基盤を提案した。認証、データの完全性、追跡可能性、ハードウェアによる保護、必要な信頼先との通信への限定に加え、隔離、冗長化、ソフトウェア供給網全体の検証が必要だと説明した。 9. 異常は可能な限り現場に近い階層で解決し、必要な場合だけ上位へ対応を引き上げることで、中央制御への依存と障害の連鎖を抑える考え方を示した。AIは動的な適応や想定外のケースの発見を支援できるが、数学モデルやルールによる監督の下で動作させ、判断を追跡・検証できるようにすべきだと述べた。 10. 最後の議論では、AIを使う攻撃者が機械の速度でOTの脆弱性を探索・悪用する可能性を踏まえ、信頼できるAIを活用した防御や自律的な防御の必要性が示された。慎重な実証、国際協力、AIの意図しない動作への対策を進めながら、運用者の支援とエネルギーシステムのレジリエンス向上にAIを生かす重要性を確認した。

D3-S13 Speech 17:05–17:20 JST

Session: Speech Speaker: Ares Cho (CEO, Janus Cyber; Co-Chair of the SEMI Cybersecurity Task Force)	セッション：スピーチ 登壇者：アレス・チョウ (ジャナス・サイバー社CEO、SEMIサイバーセキュリティ・タスクフォース共同議長)

1. Ares Cho discussed semiconductor supply-chain cybersecurity through the development and adoption of SEMI E187, alongside emerging AI security challenges. The standard was presented as an industry-led approach to establishing a common security baseline for semiconductor manufacturing equipment.
2. A cybersecurity incident at TSMC prompted recognition that a semiconductor manufacturer could not secure its operations alone. Cho explained that a global standard could support cooperation with equipment suppliers while reducing the communication and auditing burdens associated with separate customer-specific requirements.
3. SEMI E187 was described as a focused set of 12 baseline requirements covering operating-system support and updates, network security, endpoint protection, and security monitoring. It applies to equipment supplied to semiconductor fabrication facilities, rather than certifying an entire organization's information-security management system.
4. Cho emphasized that the initiative's value extends beyond equipment compliance. Suppliers seeking to become more trusted partners were encouraged to strengthen corporate cybersecurity governance and their ability to withstand attacks, sometimes investing beyond the minimum requirements.
5. Compliance should be integrated into routine engineering, inspection, quality assurance, and shipment processes rather than treated as a one-time exercise. Automated checks can help suppliers improve efficiency, reduce costs, and make equipment security a repeatable part of production and delivery.
6. Cho described SEMICON cybersecurity forums as opportunities for equipment vendors, semiconductor manufacturers, and security leaders to exchange ideas. SEMI E187 was presented as a catalyst for an ecosystem focused on improving security across the supply chain.
7. A SEMI E187 certification program announced at SEMICON Taiwan was introduced as a further step toward demonstrating conformity. Cho described plans for certification and associated SEMI markings as a development beyond existing compliance checks.

1. アレス・チョウ氏は、半導体製造装置のサイバーセキュリティ規格「SEMI E187」の策定と普及を通じ、半導体サプライチェーンの安全性と、新たなAIセキュリティの課題を説明した。同規格を、業界主導で共通のセキュリティ基盤を整備する取り組みとして紹介した。
2. TSMCで発生したサイバーセキュリティ事案を契機に、半導体メーカー単独では安全性を確保できないとの認識が生まれたと説明した。顧客ごとに異なる個別要件ではなく、国際的な共通規格を用いることで、装置供給者との協力を促し、調整や監査の負担を減らせると述べた。
3. SEMI E187は、OSのサポート・更新、ネットワークセキュリティ、エンドポイント保護、セキュリティ監視に関する12の基本要件で構成されると説明した。対象は半導体工場へ納入する装置であり、企業全体の情報セキュリティ管理体制を認証するものとは異なると述べた。
4. この取り組みの価値は、装置を規格に準拠させることだけではないと強調した。より信頼される取引先になることを目指す供給者が、最低限の要件を超え、自社のサイバーセキュリティ・ガバナンスや攻撃への耐性を強化する動きにつながっていると説明した。
5. 規格への対応は一度限りの確認ではなく、設計、検査、品質保証、出荷の通常業務に組み込む必要があると述べた。確認作業の自動化によって、効率化とコスト削減を図り、製造・納入工程の中で継続的に装置の安全性を確保できると説明した。
6. SEMICONのサイバーセキュリティフォーラムを、装置メーカー、半導体メーカー、セキュリティ責任者などが意見交換する場として紹介した。SEMI E187が、サプライチェーン全体の安全性向上を目指すエコシステムの形成を促していると述べた。
7. SEMICON Taiwanで発表されたSEMI E187の認証プログラムを、規格への適合を示すための新たな段階として紹介した。従来の準拠確認から進み、認証やSEMIの表示を通じて適合性を示す仕組みが整備されつつあると説明した。
8. AIセキュリティでは、誰がどのAIモデルを利用し、クラウド型かローカル型か、業務のどこでAIエージェントが動いているかを把握することが出発点だと述べた。モデルへの依存関係、脆弱性、更新が、業務環境全体に与える影響を確認する必要性を示した。
9. ネットワーク上の活動やAIの振る舞いを観測し、保護措置を支援するツールを紹介した。一方、入力内容の把握、情報漏洩の検知、エージェントの動作制御には未解決の課題があり、モデルや利用画面が頻繁に変更されることも対応を難しくしていると述べた。

8. Turning to AI, Cho identified visibility as a starting point: organizations need to know who is using which AI models, whether services are cloud-based or local, and where AI agents operate within workflows. Model dependencies, vulnerabilities, and updates can affect the wider business environment. 9. Cho described tools for observing network activity and AI behavior and supporting protective controls. However, monitoring prompts, identifying information leakage, and controlling agent behavior remain difficult, particularly as AI models and user interfaces change frequently. 10. His concluding message was that manufacturers, suppliers, and security partners must jointly improve supply-chain cybersecurity. SEMI E187 provides a foundation for cooperation, but AI security and the protection of design documents exchanged across supply chains remain unresolved challenges requiring continued collaboration.	10. 最後に、半導体メーカー、供給者、セキュリティパートナーが共同でサプライチェーン全体の安全性を高める必要があると強調した。SEMI E187は協力の基盤となる一方、AIの安全性や、供給網の中でやり取りされる設計文書の保護には課題が残っており、継続的な協議が必要だと結論づけた。

D3-P14 Panel 17:20–18:20 JST

Session: Global Supply Chains, i.e. Semiconductor Moderator: Albert Cheng (Founder and Chairman, InfoKeyVault Technology Co., Ltd.) Panelist: Ares Cho Panelist: Wei-Chung Hwang Panelist: Takahiro Fujishiro (Senior Director, Business Innovation Operation, Government &Public Corporation Information System Division, Hitachi, Ltd.) Panelist: Satoshi Kai (Project Associate Professor, Keio Global Research Institute)	セッション：グローバルサプライチェーン・半導体 モデレーター：アルバート・チェン (インフォキーボルト・テクノロジー株式会社 創業者兼会長) パネリスト：アレス・チョウ パネリスト：ウェン・チョン・ファン パネリスト：藤城 孝宏 ((株)日立製作所 公共システム事業部 公共ビジネスイノベーション本部 本部長) パネリスト：甲斐 賢 (慶應義塾大学グローバルリサーチインスティテュート 特任准教授)

1. Moderated by Albert Cheng, the panel examined cybersecurity across the semiconductor supply chain, from intellectual-property design and EDA software to fabrication, equipment, assembly, and testing. Participants emphasized that cross-border exchanges of physical components and valuable data create risks because organizations have different security capabilities.
2. Ares Cho explained that SEMI E187 began with equipment users' practical concerns, including outdated operating systems, patching difficulties, and malware entering fabrication facilities. Its user-driven baseline requirements encourage suppliers to improve equipment security and can stimulate broader improvements in their internal cybersecurity.
3. Wei-Chung Hwang distinguished public-key cryptography from the public-key infrastructure that establishes trust through certificates and certification authorities. He described applications including verifying the authenticity and integrity of design information and software, identifying legitimate devices and components, and securing firmware updates.
4. Takahiro Fujishiro emphasized data spaces as a means of overcoming organizational data silos and enabling trusted exchanges across industries and borders. Common rules and technologies must combine trust, respect for data sovereignty, global interoperability, and international cooperation to support new services and business opportunities.
5. Kai presented a three-layer architecture supporting Data Free Flow with Trust (DFFT): applications that create and use data, mechanisms for exchanging data among organizations, and trust-service infrastructure supporting electronic signatures and certificates. Connecting national infrastructures would help recipients verify the issuer and integrity of documents received from abroad.
6. He described international demonstrations, comparisons of Japanese, EU, and Indian trust-service infrastructures, and preparation of an ISO proposal for an International Trusted List (ITL). A Japan–Taiwan proof of concept with ITRI is exploring cross-border verification of signed documents while each jurisdiction retains control of its own trust infrastructure.

1. アルバート・チェン氏をモデレータに、知財設計、EDAソフトウェア、製造、装置、組立・検査に至る半導体サプライチェーンのサイバーセキュリティを議論した。各組織のセキュリティ能力が異なる中、物理的な部品と価値あるデータが国境を越えて行き来することによるリスクが指摘された。
2. アレス・チョウ氏は、SEMI E187が、古いOS、パッチ適用の難しさ、製造施設へのマルウェア持ち込みなど、装置利用者の実際の課題から生まれたと説明した。利用者主導の基本要件を定めることで、供給者の装置の安全性を高めるとともに、社内のサイバーセキュリティ全体の改善にもつながると述べた。
3. ウェン・チョン・ファン氏は、公開鍵暗号と、電子証明書や認証局によって信頼を確立する公開鍵基盤（PKI）を区別して説明した。設計情報やソフトウェアの真正性・完全性の検証、正規の機器・部品の識別、安全なファームウェア更新などへの活用を挙げた。
4. 藤城孝宏氏は、組織内に孤立したデータをつなぎ、業界や国境を越えて信頼できる交換を実現する仕組みとして、データスペースの重要性を示した。共通のルールと技術に加え、信頼の確保、データ主権の尊重、グローバルな相互運用性、国際協力を組み合わせることで、新たなサービスや事業機会につながると説明した。
5. 甲斐氏は、DFFT（信頼性のある自由なデータ流通）を支える三層構造として、データを作成・利用するアプリケーション、組織間のデータ交換の仕組み、電子署名・電子証明書を支えるトラストサービス基盤を紹介した。各国の基盤を接続することで、海外から受け取った文書の発行元と改ざんの有無の確認を支えられると述べた。
6. 国際的な実証、日本・EU・インドのトラストサービス基盤の比較、International Trusted List（ITL）のISO提案準備について説明した。また、台湾のITRIとの日台PoCを通じ、各国・地域が自らのトラスト基盤を管理しながら、国境を越えて署名付き文書を検証する仕組みを検討していると紹介した。
7. 甲斐氏は、文書の真正性を自動的に検証できれば、国境を越えた確認に必要な費用や手間を大幅に減らせると述べた。また、デジタルトラストを活用することで、抜き取り検査だけに頼らず、納入された品目全体の検証を支援し、サプライチェーンの信頼性向上につなげる可能性を示した。
8. チョウ氏は、AI関連の用途も含む装置データへのアクセスや共有に関連して、SEMI E196を紹介した。また、SEMIの委員会やワーキンググループでは、安全な工場、供給者との関係、文書の流通などに関する実務的な知見を共有していると説明し、供給網全体のAIセキュリティには引き続き検討が必要だと述べた。

7. Kai argued that automated verification could substantially reduce the cost and effort of confirming document authenticity across borders. He also illustrated how digital trust could support verification across entire sets of supplied items rather than relying only on sampling, potentially strengthening supply-chain assurance. 8. Cho introduced SEMI E196 in connection with equipment-data access and sharing, including AI-related applications. He also described SEMI committees and working groups exchanging practical guidance on secure factories, supplier relationships, and document flows, while noting that AI security across the wider supply chain remains an evolving issue. 9. Hwang proposed semiconductor IP exchange and collaborative design as concrete applications for trusted data exchange, alongside device authentication. He emphasized involving design houses and other relevant stakeholders, addressing differences in legal frameworks and data sovereignty through dialogue, and recognizing the computational limitations of technologies such as fully homomorphic encryption. 10. The panel supported a common cross-industry trust foundation with application-specific arrangements where needed. Participants advocated starting with simple, small-scale implementations, demonstrating security and usability, and expanding adoption. They also identified commercial opportunities in platforms offering confidentiality, integrity, traceability, and accountability for semiconductor and other supply chains.	9. ファン氏は、信頼できるデータ交換の具体的な用途として、半導体IPの交換、共同設計、機器の認証を提案した。設計企業などの関係者を巻き込み、法制度やデータ主権の違いには対話で対応するとともに、完全準同型暗号などの技術には計算負荷の課題があることを踏まえる必要があると述べた。 10. 議論では、業界を越えて利用できる共通の信頼基盤を整え、必要に応じて用途別の仕組みを組み合わせる方向性が示された。まず簡潔で小規模な実装から安全性と使いやすさを実証し、採用を広げることが提案された。また、機密性、完全性、追跡可能性、説明責任を備えたデータ交換基盤は、半導体以外の産業にも事業機会を生み得ると論じられた。

D3-S15 Day #3 Closing 18:20–18:25 JST

Session: Day #3 Closing Speaker: Konstantinos Mersinas	セッション：Day #3 クロージング 登壇者：コンスタンチノス・メルシーナス
Session: Day #3 Closing Speaker: Satoshi Kai	セッション：Day #3 クロージング 登壇者：甲斐 賢

1. Kai delivered the Day 3 closing remarks on behalf of Professor Konstantinos Mersinas, who was not present at the time. 2. He summarized the day's discussions under the theme of economic security, covering AI, critical infrastructure, and semiconductor supply chains. He described the discussions on the international cooperation and action needed to advance economic security as substantial and fruitful. 3. He explained that the program connects successive themes: national security on the previous day, economic security on Day 3, and social security on the following day. 4. While some of the economic-security discussions had been specialized, he noted that the following day would address issues closely connected to participants' daily lives and encouraged everyone to return. 5. He concluded Day 3 by thanking the audience for their attention.	1. 甲斐氏は、予定登壇者のコンスタンチノス・メルシーナス氏がその場に不在のため、代理で3日目の閉会挨拶を行った。 2. 経済安全保障をテーマに、AI、重要インフラ、半導体サプライチェーンについて議論した一日を振り返った。経済安全保障を推進するために必要な国際連携と具体的な行動を検討した、密度の濃い有意義な一日だったと総括した。 3. プログラムは、前日の国家安全保障、当日の経済安全保障、翌日の社会保障というテーマをつなぐ構成になっていると説明した。 4. 当日は専門的な議論もあった一方、翌日は参加者の生活に密接に関わる課題を扱うと紹介し、引き続き参加するよう呼びかけた。 5. 最後に、聴衆への謝意を述べ、3日目のプログラムを締めくくった。

DAY 4 2026-10-30 金曜日

Keio University, Mita Campus; West School Building 1F West Hall
慶應義塾大学 三田キャンパス 西校舎 1F 西ホール

D4-S1 Day #4 AM Opening 09:00–09:05 JST

Session: Day #4 AM Opening Speaker: Luiz DaSilva	セッション：Day #4 AM オープニング 登壇者：ルイス・ダ・シルヴァ
1. Luiz DaSilva welcomed participants to the final day of the symposium. He introduced himself as a professor at Virginia Tech and the current chair of the board of INCS-CoE, the International Cybersecurity Center of Excellence. 2. He introduced the morning's discussions on legal aspects of cybersecurity, including the concept of consent and its meaning in the age of AI. 3. He also highlighted the Digital Nippon panel as part of the morning program in the main hall. 4. He reminded participants that the evening reception would begin at 6:45 p.m. in the cafeteria downstairs, encouraged everyone to enjoy the day's program, and thanked the audience.	1. ルイス・ダ・シルヴァ氏は、シンポジウム最終日の参加者を歓迎した。自身をバージニア工科大学の教授であり、今年度のINCS-CoE（International Cybersecurity Center of Excellence）の理事会議長であると紹介した。 2. 午前のプログラムでは、サイバーセキュリティの法的側面を取り上げ、同意の概念や、AI時代における同意の意味について議論すると紹介した。 3. メイン会場で行われる午前のプログラムとして、「Digital Nippon」のパネルディスカッションも紹介した。 4. 当日午後6時45分から階下の食堂でレセプションを開催すると案内し、一日のプログラムを楽しむよう呼びかけ、聴衆への謝意を述べた。

D4-S2 Keynote Speech 09:05–09:20 JST

Session: Keynote Speech Speaker: Júlia Castro Boix (Legal Officer, European Commission)	セッション：基調講演 登壇者：ジュリア・カストロ・ボイックス (欧州委員会 法務担当官)
1. Júlia Castro Boix of the European Commission introduced the European Digital Identity Framework and its aim of providing citizens and residents with trusted digital identities usable across the EU for public and private services. 2. She explained that the framework builds on the eIDAS Regulation, adopted in 2014 and amended in 2024. Its three pillars are electronic identification schemes, the European Digital Identity Wallet, and trust services such as electronic signatures, seals, and attestations. She stated that Member States must make at least one wallet available by the end of 2026. 3. The wallet was presented as part of the EU's existing cybersecurity, privacy, and digital-trust framework, rather than a separate security ecosystem. Castro Boix referred to instruments including the GDPR and Cyber Resilience Act as addressing complementary aspects of data protection, security, and trust.	1. 欧州委員会のジュリア・カストロ・ボイックス氏は、欧州デジタルアイデンティティ枠組みを紹介した。市民や居住者がEU全域の公共・民間サービスで利用できる、信頼性の高いデジタルIDの提供を目指す取り組みであると説明した。 2. 同枠組みは、2014年に採択され、2024年に改正されたeIDAS規則を基盤とすると説明した。電子識別スキーム、欧州デジタルアイデンティティウォレット、電子署名・電子シール・電子証明などのトラストサービスを三つの柱として挙げ、加盟国は2026年末までに少なくとも一つのウォレットを提供する必要があると述べた。 3. ウォレットは独立したセキュリティの仕組みではなく、EUの既存のサイバーセキュリティ、プライバシー、デジタルトラストの枠組みの中に位置づけられると説明した。GDPRやサイバーレジリエンス法などが、個人データの保護、安全性、信頼に関する相互補完的な役割を果たすと述べた。 4. ウォレットは、本人確認、検証済みの証明情報の保存・提示、オンライン・オフラインのサービス利用を支える仕組みであると説明した。個人による無料かつ任意の利用、国境を越えた承認、取引に必要な情報だけを開示することによる利用者のデータ管理権限の強化を、重要な原則として挙げた。

4. She described the wallet as a means of identifying oneself, storing and presenting verified credentials, and accessing services online and offline. Key principles include free and voluntary use for individuals, cross-border recognition, and greater user control over personal information through disclosure limited to what each transaction requires.
5. Castro Boix distinguished the individual-focused wallet from the European Business Wallet initiative. The latter would enable companies and organizations to establish their digital identities and demonstrate that individuals are authorized to represent them; she described its legislative and technical arrangements as still under development.
6. Personal identification data (PID) was introduced as a core functionality supporting identification with verified information from trusted authorities. The wallet could simplify access to services in other Member States and reduce the need for separate accounts or repeated identity-verification procedures.
7. She highlighted pseudonyms as an option for services that do not require disclosure of a person's full legal identity. Supporting such interactions can reduce unnecessary exposure of personal information while enabling access to digital services.
8. Electronic signing was presented as another core function, supporting remote agreements and administrative procedures. She explained that qualified electronic signatures have the same legal effect as handwritten signatures, allowing the wallet to support transactions as well as identification.
9. Practical examples included confirming online transactions through QR codes, PINs, or biometrics, and opening bank accounts by sharing verified identity information. These approaches could simplify user procedures and reduce identity-verification and administrative burdens for service providers.
10. Age verification illustrated data minimization: users could prove that they meet an age requirement without disclosing their full identity or exact date of birth. Castro Boix emphasized the broader goals of a more integrated European digital environment and simpler everyday interactions while protecting privacy.

5. 個人向けのウォレットと、企業・組織向けの欧州ビジネスウォレット構想を区別した。後者は企業のデジタルな身元と、その企業を代表して行動する個人の権限を示すことを目指しており、立法や技術面の仕組みは引き続き整備中であると説明した。
6. 中核機能として、信頼できる機関が発行する本人識別データ（PID）に基づく本人確認を紹介した。ほかの加盟国のサービスを利用する場合にも、別のアカウント作成や本人確認手続きの繰り返しを減らし、利用を容易にする可能性を示した。
7. 法的な身元情報を全面的に示す必要がないサービスでは、仮名を利用する選択肢を紹介した。こうした利用に対応することで、不要な個人情報の開示を抑えながら、デジタルサービスにアクセスできると説明した。
8. 電子署名も中核機能の一つとして挙げ、遠隔での契約締結や行政手続きを支援すると述べた。適格電子署名は手書き署名と同等の法的効力を持つと説明し、ウォレットが本人確認だけでなく取引の完了も支えることを示した。
9. 具体例として、QRコード、PIN、生体認証によるオンライン取引の確認や、検証済みの本人情報を共有する銀行口座開設を紹介した。利用者の手続きを簡素化するとともに、サービス提供者の本人確認や事務処理の負担を軽減できる可能性を示した。
10. 年齢確認をデータ最小化の例として挙げ、氏名などの身元情報全体や正確な生年月日を開示せず、年齢要件を満たすことだけを証明できると説明した。プライバシーを保護しながら、欧州のデジタル環境の一体化と、日常的な手続きの簡便化を進めるという目標を強調した。

D4-S3 Speech 09:20–09:35 JST

Session: Speech Speaker: Tatsuhiko Yamamoto (Professor, Keio University Law School)	セッション：スピーチ 登壇者：山本 龍彦 (慶應義塾大学 大学院法務研究科 教授)
1. Tatsuhiko Yamamoto examined human rights, privacy, and democracy from a constitutional-law perspective, emphasizing that he was expressing his personal views. He introduced four stages in the development of the right to privacy and considered how AI challenges existing approaches. 2. At the first stage, privacy was understood as protection against unwanted exposure of private life. At the second, the emphasis shifted to individuals deciding with whom and under what conditions to share information, giving rise to personal-information control and informational self-determination. 3. The third stage recognized that consent alone cannot prevent information from being passed on or misused. Yamamoto emphasized security arrangements, system architecture, and meaningful user-interface design, including privacy by design, as necessary foundations for effective individual choice. 4. The fourth stage concerns AI, particularly the difficulty of knowing where personal information circulates or how it is used in training data. He asked whether consent and individual control should remain defining elements of privacy or whether protection must be designed to depend less on them. 5. Drawing on European and U.S. discussions, he highlighted the continuing importance of informational self-determination and individual control. He framed the central debate as whether these remain intrinsic to privacy or require a different approach in the AI era. 6. Yamamoto linked Japan's Act on the Protection of Personal Information to the constitutional principle of respect for the individual. He explained that the protection of individuals' rights and interests, including privacy, should inform the interpretation and operation of personal-information rules. 7. He discussed the review of consent requirements for statistical uses and AI training, emphasizing the need to consider purposes and risks. He also highlighted concerns about individuals losing the ability to control their information through free choice, rather than suggesting that all AI training should be exempt from consent.	1. 山本龍彦氏は、個人の見解であることを明示した上で、憲法学の立場から人権、プライバシー、民主主義の関係を論じた。プライバシー権の発展を四つの段階に整理し、AIが従来の考え方にどのような課題をもたらすかを検討した。 2. 第一段階では、プライバシーは私生活を望まない形で公開されない権利として理解されたと説明した。第二段階では、誰に、どのような条件で情報を共有するかを本人が決めることが重視され、自己情報コントロール権や情報自己決定権の考え方が発展したと述べた。 3. 第三段階では、同意だけでは情報の転送や不適切な利用を防げないという限界が明らかになったと説明した。実効的な本人の選択を支えるには、セキュリティ上の仕組み、システム構造、意味のある選択を可能にする利用画面の設計、プライバシー・バイ・デザインが必要だと強調した。 4. 第四段階に当たるAI時代には、自分の情報の流通先や、学習データとしての利用状況を本人が把握することが難しくなると指摘した。同意や自己情報のコントロールをプライバシーの本質的要素とし続けるのか、それらへの依存を減らした保護を設計するのかが問われていると述べた。 5. 欧州や米国の議論を参照し、情報自己決定権や本人による情報のコントロールが引き続き重視されていることを紹介した。その上で、これらをプライバシーに不可欠な要素として維持するのか、AI時代に適した別の保護のあり方を考えるのかを中心的な論点として提示した。 6. 個人情報保護法を、憲法上の個人の尊重という原則に関連づけて説明した。プライバシーを含む個人の権利・利益の保護という理念を踏まえ、個人情報に関する規律を解釈・運用する必要があると述べた。 7. 統計目的の利用やAI学習に関する同意要件の見直しを取り上げ、利用目的やリスクを考慮する必要性を示した。また、本人が自由な意思で自分の情報をコントロールできなくなるリスクを重視し、あらゆるAI学習について同意が不要になるという説明ではないことを示した。 8. 本人関与を、事業者の適切なガバナンスを実現する手段として捉える考え方と、それ自体を本人の権利として捉える考え方を区別した。前者では他の保護措置が同意を代替し得る一方、後者では結果的な安全性とは別に、情報を共有するかどうかという本人の選択を尊重する必要があると説明した。

8. He distinguished individual involvement as a means of ensuring organizational governance from involvement as a right in itself. Under the first view, other safeguards might sometimes substitute for consent; under the second, individuals' choices about sharing information deserve respect independently of whether the resulting handling is secure. 9. Yamamoto distinguished individual uses of data from collective uses intended to generate knowledge and innovation. Even when AI training is treated as collective use without direct effects on particular individuals, personal and sensitive information may remain involved, requiring safeguards against exposure and inappropriate individual impacts. 10. Comparing cybersecurity with building standards, he argued that information systems should meet minimum security requirements protecting life, health, and property. Additional security and privacy protections should be communicated clearly so that users can make informed choices beyond that baseline.	9. データ利用を、個人に直接関わる個別的な領域と、知識やイノベーションを生む集合的な領域に分けて検討した。AI学習を特定個人に直接影響しない集合的利用と捉える場合でも、個人情報や要配慮個人情報が含まれ得るため、情報の露出や個人への不適切な影響を防ぐ措置が必要だと述べた。 10. サイバーセキュリティを建築基準に例え、情報システムにも生命・身体・財産を守る最低限の安全基準が必要だと論じた。その基準を確保した上で、追加的なセキュリティやプライバシー保護の水準を分かりやすく示し、利用者が十分な情報に基づいて選択できるようにすることを提案した。

D4-P4 Panel 09:35–10:35 JST

Session: The Significance of Individual "Consent" in the Age of AI Moderator: Tatsuhiko Yamamoto Panelist: Naoto Ikegai (Professor, Hitotsubashi University Graduate School of Law) Panelist: Mieko Tanno (Senior Advisor, Japan Association of Consumer Affairs Specialists; Former Chairperson, Personal Information Protection Commission, Japan) Panelist: Seiwa Fujiwara (Attorney-at-Law, Kitahama Partners／European Centre for Certification and Privacy (ECCP)) Panelist: Axel Freiherr von dem Bussche, (Partner, Taylor Wessing Partnerschaftsgesellschaft mbB)	セッション：AI時代における個人の「同意」の意義 モデレーター：山本 龍彦 パネリスト：生貝 直人 (一橋大学 大学院法学研究科 教授) パネリスト：丹野 美絵子 (公益社団法人 全国消費生活相談員協会 参与 元個人情報保護委員会 委員長) パネリスト：藤原 成和 (北浜法律事務所・外国法共同事業／欧州認証・プライバシーセンター(ECCP)(併任) 弁護士) パネリスト：アクセル・フライヘア・フォン・デム・ブッシェ (テイラーヴェッシング パートナー弁護士)
1. Moderated by Tatsuhiko Yamamoto, the panel brought together Naoto Ikegai, Mieko Tanno, Seiwa Fujiwara, and Axel Freiherr von dem Bussche to examine individual consent in the AI era. The central question was how to preserve individual agency while providing effective protection through technology, organizational governance, and oversight.	1. 山本龍彦氏をモデレータに、生貝直人氏、丹野美絵子氏、藤原成和氏、アクセル・フライヘア・フォン・デム・ブッシェ氏が、AI時代における本人同意の意義を議論した。本人の主体性を維持しながら、技術、組織のガバナンス、監督によって実効的な保護を確保する方法を中心的な論点とした。 2. 藤原氏は、一定の条件の下で本人同意なしのデータ利用を認める、日本の統計目的の特例に関する検討を紹介した。個人を識別できる出力を防ぐ措置、利用目的の限定、第三者提供の制限、提供者と受領者の書面による取決め、個人情報保護委員会の監督が重要だと説明した。

2. Fujiwara explained Japan's proposed statistical-use exception, which would permit certain data uses without individual consent under defined conditions. He emphasized safeguards against identifiable outputs, purpose restrictions, controls on third-party disclosure, written arrangements between providers and recipients, and oversight by the Personal Information Protection Commission.
3. Von dem Bussche described EU Digital Omnibus discussions concerning the AI Act and GDPR. He outlined narrowly framed approaches to sensitive-data processing for bias detection and incidental inclusion in AI training, emphasizing that the proposals did not amount to unrestricted use or abandonment of consent. He also distinguished AI product-safety regulation from broader data-protection and fundamental-rights questions.
4. He explained that consent is one of several lawful bases for processing ordinary personal data under the GDPR, alongside grounds such as contractual necessity and legitimate interests. Special-category data, including health information, requires separate consideration because stricter restrictions and specified exceptions apply.
5. Ikegai distinguished statistical or aggregate data use from processing that affects identifiable individuals. AI models can memorize training information and reconnect aggregate processing with particular people, making safeguards at that boundary essential. He stressed that organizations should justify their chosen processing basis and explain the protections provided when consent is not used.
6. Fujiwara highlighted consent fatigue and the impracticality of expecting individuals to read every explanation or authorize every AI-related use. Yamamoto asked whether individual involvement is merely a governance mechanism or a right in itself, and whether alternative safeguards should replace consent or complement it.
7. Fujiwara proposed privacy-enhancing technologies and independent certification as safeguards, citing PrivacyMark, ISMS, and cross-border certification mechanisms. He suggested that recognizing demonstrated compliance could encourage investment in trustworthy governance, while stressing that protection must continue after international transfers.

3. ブッシェ氏は、EUのAI法とGDPRに関するデジタル・オムニバスの議論を紹介した。バイアス検出やAI学習への付随的な混入に関するセンシティブデータの処理について、限定的な対応が検討されており、自由な利用や同意の放棄を認める提案ではないと説明した。また、AIの製品安全に関する規律と、より広いデータ保護・基本的人権の問題を区別した。
4. GDPRでは、通常の個人データについて、同意は契約履行や正当な利益などと並ぶ複数の適法化根拠の一つであると説明した。一方、健康情報などの特別なカテゴリーのデータには、より厳格な制限と限定された例外が適用されるため、区別して検討する必要があると述べた。
5. 生貝氏は、統計的・集合的なデータ利用と、特定個人に影響を及ぼす処理を区別した。AIモデルが学習情報を記憶し、集合的な処理が再び特定個人に結びつく可能性があるため、その境界の保護が重要だと述べた。また、事業者は処理の根拠を選んだ理由と、同意によらない場合の保護措置を説明する必要があると強調した。
6. 藤原氏は、すべての説明を読み、AIに関わる利用のたびに同意することを本人に求める難しさと、「同意疲れ」を指摘した。山本氏は、本人関与をガバナンスの手段と捉えるのか、それ自体を権利と捉えるのか、他の保護措置が同意を代替するのか補完するのかを問いかけた。
7. 藤原氏は、プライバシー強化技術（PETs）と第三者認証を保護措置として提案し、プライバシーマーク、ISMS、越境移転に関わる認証制度を例示した。遵守体制への評価を企業の投資意欲につなげる可能性を示すとともに、国境を越えた後も適切な保護を維持する必要性を強調した。
8. 丹野氏は、同意をなくすべきではない一方、同意に保護のすべてを背負わせるべきでもないと述べた。入り口での同意、秘密計算や再識別防止などの技術的保護、出口での説明責任とプロファイリングに関する規律という、三層の保護を提案した。
9. 丹野氏は、本人の意味ある選択を残すべき場面として、個人を特定した分析によって広告・価格・審査などの扱いを変える場合、要配慮個人情報を本人が特定できる形で利用・提供する場合、本人が合理的に予想できない目的で利用する場合を挙げた。知らないうちに分析され、不公平な扱いを受けることが、消費者の大きな懸念であると強調した。
10. 最後の議論では、意味のある同意を維持しつつ、同意だけでは保護できない部分のガバナンスを強化する方向性が示された。異議申立ての権利、透明性、規制当局と民間による監督、認証、DFFTを支える越境的な信頼の仕組みを重視し、企業や政府に本人の自律性を委ねきることなく、責任あるAI利用を可能にする保護の整備を求めた。

8. Tanno argued that consent should neither be abandoned nor bear the entire burden of protection. She proposed three layers: consent at entry, technical safeguards such as secure computation and prevention of re-identification, and output-stage accountability and controls on profiling. 9. Tanno identified three situations where individuals should retain meaningful choice: identifiable analysis that changes advertising, pricing, or assessments; identifiable use or disclosure of sensitive information; and uses beyond reasonable expectations. She emphasized that people are particularly concerned about being analyzed and treated unfairly without their knowledge. 10. The closing discussion favored preserving meaningful consent while strengthening governance where consent alone is insufficient. Participants emphasized rights to object, transparency, regulatory and private-sector oversight, certification, and trusted cross-border mechanisms supporting DFFT. They called for protections that enable responsible AI use without surrendering individual autonomy to large companies or governments.	

D4-S5 Speech 10:55–11:10 JST

Session: Speech Speaker: Noriaki Okui (President, Data Society Alliance)	セッション：スピーチ 登壇者：奥井 規晶 (一般社団法人データ社会推進協議会 理事長)
1. Noriaki Okui introduced the Data Society Alliance (DSA) as an organization established to support Japan's national data strategy. He described its approximately 180 member companies and organizations and its work on infrastructure for data spaces, their implementation, and standardization. 2. As an introduction to the following panel, he explained his involvement in developing the Liberal Democratic Party's Digital Nippon proposals with Takuya Hirai and others. He described his continuing role in reviewing the overall direction of digital policy. 3. Okui outlined the relationship between Digital Nippon proposals and the government's Priority Plan for Realizing a Digital Society. He argued that the recent escalation of cyber threats had exceeded the assumptions underlying existing plans, creating a need to revisit cybersecurity strategies and countermeasures.	1. 奥井規晶氏は、データ社会推進協議会（DSA）を、国のデータ戦略を支えるために設立された組織として紹介した。約180の企業・団体が加盟し、データスペースの基盤整備、構築、標準化などに幅広く取り組んでいると説明した。 2. 続くパネルへの導入として、平井卓也氏らと自民党の「デジタル・ニッポン」の策定に関わってきた経緯を紹介した。現在も、デジタル政策全体の方向性を俯瞰し、検討する立場にあると述べた。 3. 「デジタル・ニッポン」の提言と、政府の「デジタル社会の実現に向けた重点計画」との関係を説明した。最近のサイバー脅威の深刻化は既存計画の想定を超えており、サイバーセキュリティの戦略や対策を改めて検討する必要があると論じた。 4. 日本語の難しさが、従来は日本への攻撃を一定程度抑える要因になっていたとの見方を示した。しかし、AIによって言語の障壁が低くなり、それに依存した安全への期待は通用しにくくなっていると指摘した。 5. 日米の備えを比較し、米国では攻撃を繰り返し経験する中で、脆弱性の修正や対応の実務が強化されてきたと論じた。既知の弱点を解消し、インシデントが起きる前に準備する重要性を強調した。

4. He suggested that the difficulty of the Japanese language had previously limited some attacks against Japan. AI is reducing that language barrier, making reliance on it increasingly ineffective and exposing Japanese organizations to a changing threat environment. 5. Comparing Japanese and U.S. preparedness, he argued that repeated exposure to attacks had encouraged U.S. organizations to strengthen vulnerability remediation and response practices. He emphasized the importance of addressing known weaknesses and preparing before incidents occur. 6. Okui presented cyberattacks as an issue of national security as well as economic security. Referring to cyber operations preceding physical attacks in Ukraine, he argued that Japan should recognize the strategic significance of cyber threats and develop a stronger sense of urgency. 7. Drawing on a conversation with a business executive whose company had been attacked, he emphasized prompt disclosure of incidents. He argued that management awareness must be accompanied by organizational arrangements capable of supporting timely action. 8. He highlighted dedicated security leadership, clear reporting structures, trained internal specialists, cooperation with external experts, and readiness to respond immediately as important elements of corporate preparedness. 9. Okui argued that assumptions of trust and prolonged peace had contributed to insufficient preparedness in Japan. He concluded, as his personal view, that responding to the current cyber threat environment should be treated as an urgent priority by corporate leaders and society.	6. サイバー攻撃を、経済安全保障に加えて国家安全保障の問題として捉える必要があると述べた。ウクライナで物理的な攻撃に先立ってサイバー攻撃が行われたことに触れ、日本も脅威の戦略的な意味を認識し、危機感を高めるべきだと主張した。 7. 攻撃を受けた企業の経営者との会話を例に、インシデントを速やかに公表する重要性を示した。経営者の問題意識だけでなく、迅速な行動を支える組織体制が必要だと指摘した。 8. 企業の備えとして、セキュリティを担う責任者、明確な報告体制、社内の専門人材、外部専門家との協力、発生時に直ちに対応できる準備を重視した。 9. 人への信頼を前提とする姿勢や、長く平和が続いたことが、日本の備えの不足につながっているとの見方を示した。個人の見解として、現在のサイバー脅威への対応を、企業経営者と社会が緊急性の高い課題として扱うべきだと結論づけた。

D4-P6 Panel 11:10–12:10 JST

Session: Digital Nippon, Priority Plan for Realizing a Digital Society Moderator: Hiroshi Nakatake (Global Legal Entity Identifier Foundation (GLEIF) Japan Office Managing Director and Japan representative) Panelist: Takahiro Sato (Representative Director, President and CEO, TradeWaltz Inc.) Panelist: Akira Sakaino (Director, Evangelist, NTT DOCOMO BUSINESS, Inc., Trusted Data Fabric Department Social Innovation Business Solution Division) Panelist: Satoru Yamadera (Senior Researcher, Keio Research Institute at SFC; Visiting professor, Saitama University Graduate School of Economics and Management)	セッション：デジタルニッポン、デジタル社会の実現に向けた重点計画 モデレーター：中武 浩史 (グローバルLEI財団 日本事務所 マネージングディレクター 日本事務所代表) パネリスト：佐藤 高廣 (株式会社トレードワルツ 代表取締役執行役員社長兼CEO) パネリスト：境野 哲 (NTTドコモビジネス株式会社ビジネスソリューション本部ソーシャルイノベーション部Trusted Data Fabric部門 担当部長・エバンジェリスト) パネリスト：山寺 智 (慶應義塾大学 SFC研究所 上席所員, 埼玉大学 経済経営系大学院 客員教授)
1. Moderated by Hiroshi Nakatake, the panel brought together Takahiro Sato, Akira Sakaino, and Satoru Yamadera to discuss practical implementation of Digital Nippon and the government's priority plan. Nakatake highlighted responsible agile governance, AI-enabled transformation, inclusion, digital skills, cybersecurity, and Data Free Flow with Trust (DFFT). 2. Sato introduced TradeWaltz as a platform connecting fragmented trade information among exporters, importers, logistics providers, banks, insurers, and governments. Replacing paper documents and emailed PDFs with shared, trusted data could reduce manual work, errors, fraud, and alteration while supporting international interoperability. 3. He described opportunities to link commercial, logistics, government, and financial information with digital evidence of rights in goods. Electronic bills of lading and stablecoins could support automated settlement and supply-chain finance. However, concentrating strategically important trade data also creates an attractive attack target whose protection exceeds the capacity of one company alone. 4. Sakaino introduced two complementary concepts: Data Space for AI, which supplies data for AI training, and AI for Data Space, which uses AI to operate data spaces securely and efficiently. He described telecommunications infrastructure connecting enterprise systems, networks, and cloud services to support trusted cross-border use of AI and data.	1. 中武浩史氏をモデレータに、佐藤高廣氏、境野哲氏、山寺智氏が、「デジタル・ニッポン」と政府の重点計画の実装を議論した。中武氏は、責任あるアジャイル・ガバナンス、AIを活用した変革、誰一人取り残されないデジタル化、人材育成、サイバーセキュリティ、DFFTを主要な方向性として紹介した。 2. 佐藤氏は、輸出入企業、物流事業者、銀行、保険会社、政府などの間で分断された貿易情報をつなぐプラットフォームとして、TradeWaltzを紹介した。紙の書類やメール添付のPDFを、関係者が共有する信頼できるデータへ置き換えることで、人手作業、ミス、詐欺、改ざんを減らし、国際的な相互運用性を高める可能性を示した。 3. 商流、物流、行政、金融の情報と、物の権利をデジタルに証明する仕組みを結びつける構想を説明した。電子船荷証券やステーブルコインによって、決済の自動化やサプライチェーンファイナンスの発展が期待できる一方、戦略的に重要な貿易情報の集約は攻撃対象を生み、一社だけでは十分に守れないという課題を示した。 4. 境野氏は、AI学習用のデータを提供する「Data Space for AI」と、AIでデータスペースを安全かつ効率的に運用する「AI for Data Space」という二つの考え方を紹介した。企業システム、通信網、クラウドをつなぎ、国境を越えたAIとデータの信頼できる利用を支える通信基盤を説明した。 5. 「Trusted AI Data Space」の構想として、AIエージェントの身元確認、専用の閉域環境、断片化・暗号化したデータを用いる秘密計算を組み合わせる仕組みを示した。Trusted Data FabricやIDSAなどとの国際テストベッドを通じ、Trusted AI、Trusted Identity、Trusted Data Accessの三つの信頼を提供することを目指すと述べた。 6. 山寺氏は、ASEANプラス3とADBを通じたアジア金融協力を紹介し、安全なデータ交換基盤への支援拡大を検討していると説明した。欧州・米国の仕組みと相互運用できるアジアの信頼基盤を提案し、日本にも国外の第三者が参照・検証できる公的なトラストの仕組みが必要だと論じた。

5. His proposed Trusted AI Data Space combines verified AI-agent identities, dedicated closed environments, and secure computation using fragmented and encrypted data. Through Trusted Data Fabric and an international testbed involving IDSA and other partners, he aims to provide Trusted AI, Trusted Identity, and Trusted Data Access.
6. Yamadera described Asian financial cooperation through ASEAN Plus Three and ADB, including plans to extend support toward secure data-exchange infrastructure. He advocated an Asian trust foundation interoperable with European and U.S. arrangements and argued that Japan needs publicly referenceable trust mechanisms that foreign third parties can verify.
7. Nakatake illustrated AI-specific risks through smart-factory quality checks that might unintentionally transfer regulated information across borders and disaster-response data that AI could combine to reveal sensitive national-security information. The discussion emphasized both deliberate attacks and unintended harm arising from data aggregation and AI use.
8. Yamadera warned that secure financial networks can still be undermined through compromised participants or interfaces. Traditional assumptions of trust therefore need reassessment, with stronger verification of counterparties and authority, cross-border cooperation, and active responsibility by financial institutions rather than reliance on governments alone.
9. Sakaino compared digital safety with road safety, proposing consideration of identity requirements, testing, certification, and binding security obligations alongside technical safeguards. Audience discussion included Estonia's digital-ID experience and the costs of decentralized systems. He also proposed emergency-stop mechanisms that could temporarily halt dangerous systems and enable alternatives during serious incidents.
10. Participants called for immediate cooperation among telecommunications providers, user companies, financial institutions, researchers, legal experts, and governments. Shared risk awareness, funding, international rulemaking, and an adaptable combination of laws and guidelines were presented as essential to maintaining trust, preventing exclusion from global networks, and advancing practical implementation of DFFT.

7. 中武氏は、スマート工場の品質確認を通じて規制対象情報が意図せず国外へ移転する例と、災害救助用データをAIが統合して国家安全保障上の機微情報を導き出す例を示した。議論では、悪意ある攻撃だけでなく、データの集約やAI利用がもたらす意図しない被害も重視された。
8. 山寺氏は、安全性を確保した金融ネットワークであっても、参加機関や接続部分が侵害されれば信頼が崩れる可能性を指摘した。従来の信頼の前提を見直し、相手方の正当性や権限の確認、国境を越えた協力、政府任せにしない金融機関自身の対応を強化する必要があると述べた。
9. 境野氏は、デジタル社会の安全を道路交通の安全になぞらえ、技術的対策に加えて、身元確認、試験、認証、法的なセキュリティ義務の検討を提案した。会場ではエストニアのデジタルIDや分散システムの費用も議論された。また、重大な事態には危険なシステムを一時停止し、代替手段へ切り替える緊急停止機構の必要性を示した。
10. 登壇者は、通信事業者、ユーザー企業、金融機関、研究者、法律専門家、政府が直ちに協力を始めることを求めた。共通のリスク認識、資金の確保、国際的なルール形成、法律とガイドラインを柔軟に組み合わせる対応を通じ、国際的な信頼の維持、世界の取引網からの排除の防止、DFFTの実装を進める重要性を示した。

D4-S7 Day #4 PM Opening 13:30–13:35 JST

Session: Day #4 PM Opening Speaker: Takao Kondo (Project Associate Professor, Keio University Global Research Institute (KGRI))	セッション：Day #4 PM オープニング 登壇者：近藤 賢郎 (慶應義塾大学グローバルリサーチインスティテュート 特任准教授)
1. The remarks introduced an upcoming presentation on electronic trust services, electronic identification, and digital trust strategy. 2. A subsequent panel was announced on public trust, ISO standards, and trusted lists, addressing frameworks that support electronic signatures, certificates, and trust services. 3. The program also included a presentation by the chair of the technical committee on electronic signatures and trust infrastructures. 4. The final panel was introduced as focusing on digital identity wallets and electronic attestations of attributes.	1. 午後のプログラムとして、電子トラストサービス、電子識別、デジタルトラスト戦略に関する講演を紹介した。 2. 続いて、パブリックトラスト、ISO標準、トラステッドリストに関するパネルを案内し、電子署名、電子証明書、トラストサービスを支える枠組みを取り上げると説明した。 3. 電子署名・トラストインフラ技術委員会の委員長による講演も予定されていると紹介した。 4. 最後のパネルでは、デジタルアイデンティティウォレットと電子属性証明を取り上げると案内した。

D4-S8 Keynote Speech 13:35–13:50 JST

Session: Keynote Speech Speaker: Yasuhiko Taniwaki (Member of the Board, Representative Director, President and Co-CEO & COO, Internet Initiative Japan Inc.)	セッション：基調講演 登壇者：谷脇 康彦 (株式会社インターネットイニシアティブ 代表取締役 社長執行役員)
1. Yasuhiko Taniwaki examined digital sovereignty and its implications for industrial policy, research and development, and cybersecurity. He highlighted the rapid spread of AI and the importance of considering both spin-off and spin-on relationships between civilian and security-related technologies. 2. He compared different national approaches to digital policy, including state-led control, market-led development, and regulation. He also discussed a public-infrastructure model in which the government provides foundations and open APIs, enabling private companies to develop applications with a clearer division of public and private responsibilities. 3. Taniwaki described digital sovereignty as the ability to exercise appropriate control over digital infrastructure, data, and technology. These elements are interconnected: technological capabilities support infrastructure, and data circulates through that infrastructure. 4. He emphasized that infrastructure sovereignty increasingly concerns access to and control over remotely provided computing resources and AI services. The ability to use infrastructure does not necessarily mean retaining control over the conditions under which it is available.	1. 谷脇康彦氏は、デジタル主権と、それが産業政策、研究開発、サイバーセキュリティに及ぼす意味を論じた。AIの急速な普及を背景に、民生分野と安全保障分野の技術の関係について、スピンオフとスピンオンの双方を考慮する重要性を示した。 2. 国家主導の管理、市場主導の発展、規制を重視する考え方など、各国のデジタル政策の違いを比較した。また、政府が共通基盤とオープンAPIを提供し、その上で民間企業がアプリケーションを開発する、官民の役割を明確に分けたデジタル公共インフラのモデルを紹介した。 3. デジタル主権を、デジタルインフラ、データ、技術を適切にコントロールできる能力として説明した。技術の基盤がインフラを支え、そのインフラ上をデータが流通するという、三つの要素の相互関係を示した。 4. インフラ主権について、遠隔で提供される計算資源やAIサービスへのアクセスと、その利用条件をコントロールできるかが重要になっていると指摘した。インフラを利用できることと、その提供条件を自ら管理できることは、必ずしも同じではないと説明した。 5. デジタル主権を支えるルールをデジタルガバナンスと位置づけた。その構成要素として、AIガバナンス、データガバナンス、セキュリティガバナンスを挙げ、これらを組み合わせてデジタル技術を実効的に管理する必要性を示した。

5. He presented digital governance as the rules supporting digital sovereignty. In his framework, it includes AI governance, data governance, and security governance, which must work together to enable effective control of digital technologies. 6. Discussing the EuroStack approach, he argued that sovereignty should cover the full digital stack, including energy and water as well as semiconductors, networks, AI, and software. Electricity constraints on AI development and water requirements for semiconductor production illustrate the importance of these underlying resources. 7. Taniwaki stressed that pursuing digital sovereignty should not become protectionism. Countries have different strengths across technological layers, making cooperation with like-minded partners important for building resilient capabilities without seeking complete self-sufficiency. 8. He argued that Japan needs a comprehensive national strategy extending beyond digital policy alone. Industrial policy, diplomacy, research and development, and technology strategy must be coordinated across ministries to support digital sovereignty. 9. Turning to the question of AI as a source of deterrence in the twenty-first century, he recalled deterrence through punishment and deterrence through denial. He suggested that AI's rapid development could significantly alter the existing balance among cyberattack, defense, and deterrence. 10. He highlighted the asymmetry between attackers who may remove AI guardrails and defenders who must decide how to operate within appropriate constraints. He called for renewed discussion of defensive capabilities, safeguards, and the changing strategic balance created by AI.	6. EuroStackの考え方に触れ、半導体、ネットワーク、AI、ソフトウェアだけでなく、エネルギーや水まで含むデジタル基盤全体を主権の観点から捉える重要性を述べた。AI産業の発展を制約する電力供給や、半導体製造に必要な水を例に、基礎資源の確保も不可欠だと説明した。 7. デジタル主権の追求が保護主義になってはならないと強調した。技術の各層で国ごとに強みが異なるため、全面的な自給自足を目指すのではなく、同志国との協力を通じて強靭な能力を築くことが重要だと述べた。 8. 日本には、デジタル政策だけにとどまらない総合的な国家戦略が必要だと論じた。デジタル主権の確保に向けて、産業政策、外交、研究開発、技術戦略を省庁横断で調整する必要性を示した。 9. 「AIは21世紀の抑止力か」という問いを提示し、懲罰的抑止と拒否的抑止の考え方を振り返った。AIの急速な発展によって、サイバー空間における攻撃、防御、抑止の既存のバランスが大きく変わる可能性を指摘した。 10. 攻撃者がAIのガードレールを外して行動し得る一方、防御側は適切な制約の下でどのように対応するかを判断しなければならないという非対称性を示した。AIが生む新たな戦略的環境を踏まえ、防御能力、安全措置、攻撃と防御の関係を改めて議論する必要があると結論づけた。

D4-S9 Speech 13:50–14:05 JST

Session: Speech Speaker: Koichi Akaishi (JDTF Chairman)	セッション：スピーチ 登壇者：赤石 浩一 (JDTF 会長)
1. Koichi Akaishi discussed the need for trust infrastructure in cyberspace as individuals, organizations, and AI agents increasingly exchange data. He emphasized enabling necessary data sharing while maintaining distributed management, rather than relying on large, centralized collections of personal information.	1. 赤石浩一氏は、個人、組織、AIエージェントの間でデータ交換が拡大する中、サイバー空間のトラスト基盤を整備する必要性を論じた。個人情報を大規模に集中管理する仕組みだけに頼らず、データの分散管理を維持しながら、必要な情報を連携させる重要性を示した。

2. He described the first generation of trust as technical mechanisms such as PKI and SSL that protect communications against alteration and help establish reliable connections. These mechanisms provide important foundations but do not by themselves resolve every question about the identity or trustworthiness of participants.
3. The second generation concerns reliably identifying and authenticating people and organizations in digital space. Akaishi distinguished a European approach anchored in government involvement from a U.S. approach relying more heavily on credentials issued by organizations operating under defined standards.
4. He argued that centralized management of identities and personal data by governments or large companies creates vulnerabilities and dependence. Concerns about data breaches and reliance on foreign cloud and authentication providers have strengthened interest in digital sovereignty and alternative trust arrangements.
5. The third generation shifts toward individuals holding digital identities and credentials in their own wallets. Universities, governments, and other issuers can provide verified credentials, while holders disclose only the information needed for a particular interaction, reducing reliance on centralized personal-data collection.
6. Akaishi described work by organizations including W3C, the OpenID Foundation, the OpenWallet Foundation, and Trust over IP on credentials, wallets, interoperability, and trust frameworks. He emphasized that technical validity alone is insufficient: recipients must also establish whether a credential's issuer is genuinely trustworthy.
7. He presented European and U.S. developments as capable of convergence despite different institutional starting points. Shared technical specifications, recognition of trust anchors, and interoperability demonstrations can help connect government-backed and privately developed ecosystems as wallet-based trust moves toward implementation.
8. Akaishi proposed a fourth generation that extends these foundations to AI agents acting on behalf of people, companies, or public bodies. Beyond proving identity, an agent must demonstrate whom it represents, what authority has been delegated, and whether that delegation remains valid.

2. 第一世代のトラストとして、PKIやSSLなどによって通信の改ざんを防ぎ、接続の信頼性を支える技術的な仕組みを挙げた。これらは重要な基礎である一方、相手の身元や信頼性に関するすべての問題を解決するものではないと説明した。
3. 第二世代では、デジタル空間で個人や組織を確実に識別し、本人確認・認証を行うことが課題になると説明した。政府の関与を信頼の基軸とする欧州型と、一定の基準の下で組織が発行する証明情報を重視する米国型という、二つのアプローチを整理した。
4. 政府や巨大企業がIDと個人データを集中管理する構造には、脆弱性や依存の問題があると指摘した。情報漏洩や、海外のクラウド・認証基盤への依存に対する懸念が、デジタル主権と新たな信頼の仕組みへの関心を高めていると述べた。
5. 第三世代では、個人がデジタルIDや証明情報を自らのウォレットで管理する方向へ移行すると説明した。大学、政府などが発行する検証可能な証明情報を保有し、必要な場面で必要な情報だけを提示することで、個人データの集中収集への依存を減らす考え方を示した。
6. W3C、OpenID Foundation、OpenWallet Foundation、Trust over IPなどによる、証明情報、ウォレット、相互運用性、トラストの枠組みの整備を紹介した。技術的に証明情報を検証できるだけでは不十分であり、その発行者自体が信頼できるかを判断する仕組みが重要だと強調した。
7. 欧州と米国は制度上の出発点が異なるものの、相互に接続できる方向に進み得ると説明した。共通の技術仕様、信頼の基点の認識、相互運用性の実証を通じ、政府が支える仕組みと民間主導の仕組みをつなぎ、ウォレットを基盤とするトラストの実装を進める可能性を示した。
8. 第四世代のトラストとして、これまでの基盤を、個人、企業、行政機関の代理で行動するAIエージェントへ拡張する考え方を提案した。身元の確認に加え、誰の代理なのか、どの権限が委任されているのか、その委任が現在も有効なのかを検証する必要があると述べた。
9. 日本はマイナンバーという強い公的な本人確認の基盤を持つ一方、法人、デバイス、データに関する信頼の仕組みをさらに整備する必要があるとの見方を示した。本人が管理するウォレットや証明情報への移行を進めると同時に、AIエージェントの身元と委任された権限の検討を加速すべきだと述べた。
10. 最後に、現代的なトラスト基盤は、サイバーセキュリティ、国家の強靱性、産業競争力にとって重要だと強調した。続くパネルでは、この基盤の上にデータスペースをどう構築するか、日本の実装上の課題は何か、今後のトラストのあり方をどう考えるかを議論すると説明した。

9. In his assessment, Japan has a strong public identity anchor through My Number, but needs to strengthen trust arrangements for organizations, devices, and data. He called for faster progress on user-controlled wallets and credentials, alongside parallel work on AI-agent identity and delegated authority. 10. He concluded that modern trust infrastructure is important for cybersecurity, national resilience, and industrial competitiveness. The following panel would examine how data spaces can be built on these foundations, what implementation challenges Japan faces, and how its trust framework should develop.	

D4-P10 Panel 14:05–15:05 JST

Session: Digital Trust Infrastructure Moderator: Koichi Akaishi Panelist: Naoto Kikuchi (Vice Chairman, Digital Policy Forum; Project Professor, Graduate School of Media Design, Keio University) Panelist: Hideki HANAMI (Innovation Platform Agency,Japan (IPA) Digital & AI Systems Design Center (DADC) Deputy Director) Panelist: Naohiko Irie (Hitachi, Ltd. Infrastructure Control System Division Senior Strategist) Panelist: Takashi Kai (Researcher, Keio University, KGRI(Global Research Institute))	セッション：デジタルトラスト基盤 モデレーター：赤石 浩一 パネリスト：菊池 尚人 (デジタル政策フォーラム代表幹事代理、慶應義塾大学大学院メディアデザイン研究科特任教授) パネリスト：花見 英樹 (独立行政法人 情報処理推進機構 (IPA) デジタル＆AIシステムズ・デザインセンター(DADC) 副センター長) パネリスト：入江 直彦 (株式会社日立製作所 インフラ制御システム事業部 シニアストラテジスト) パネリスト：甲斐 隆嗣 (慶應義塾大学 KGRI 研究員)
1. Moderated by Koichi Akaishi, the panel examined how digital trust infrastructure can support data spaces and AI agents. Naoto Kikuchi, Hideki Hanami, Naohiko Irie, and Takashi Kai discussed legal frameworks, technical foundations, industrial deployment, and verifiable trust across organizations and national borders. 2. Kikuchi called for coordinated development of laws, guidelines, and technical arrangements across the different layers of digital infrastructure. He discussed trust services beyond electronic signatures and authentication, including electronic seals, timestamps, delivery services, and intermediaries, while highlighting institutional barriers to implementation in Japan. 3. Hanami described data spaces as a way to reconcile shared social requirements with economic efficiency. Organizations can cooperate to reduce the cost of regulatory compliance while using industrial data and AI to create new value. He introduced Open Data Spaces and approaches that connect distributed data through metadata and semantic relationships without requiring centralized storage.	1. 赤石浩一氏をモデレータに、データスペースとAIエージェントを支えるデジタルトラスト基盤の構築を議論した。菊池尚人氏、花見英樹氏、入江直彦氏、甲斐氏が、法制度、技術基盤、産業での実装、組織や国境を越えて検証できる信頼について意見を交わした。 2. 菊池氏は、デジタル基盤の各層について、法律、ガイドライン、技術的な仕組みを連動して整備する必要性を示した。電子署名や認証に加え、電子シール、タイムスタンプ、電子的な配送、仲介者などのトラストサービスを取り上げ、日本の実装を妨げる制度上の課題を指摘した。 3. 花見氏は、データスペースを、社会的に共通する要請と経済合理性を両立させる仕組みとして説明した。規制対応の費用を協調して減らす一方、産業データとAIで新たな価値を生むことを目指すと述べた。Open Data Spacesを紹介し、データを一元保管せず、メタデータや意味の関係を通じて分散したデータをつなぐ考え方を示した。 4. 入江氏は、参加企業、流通データ、ユースケースを増やす横方向の拡大と、予測、最適化、AIによる知能化へ進む縦方向の発展を区別した。蓄電池や製品含有化学物質のトレーサビリティを実装例に挙げ、企業、事業所、製品、関連データの信頼性が、エコシステムの拡大に不可欠だと述べた。

4. Irie distinguished horizontal expansion—more participating companies, data, and use cases—from vertical development toward prediction, optimization, and AI-enabled intelligence. Battery and chemical-substance traceability illustrated practical applications, while trust in companies, individual sites, products, and associated data remains essential as ecosystems expand.
5. Takashi Kai framed the common challenge as moving from trust dependent on human checks to mechanisms that can be verified across organizational and national boundaries. He distinguished identity and signature verification, provenance and tamper detection, data quality, and the correctness of AI decisions as separate issues requiring different assurances.
6. For AI agents, the discussion emphasized verifying whom an agent represents and the scope, duration, and continuing validity of its authority. Delegation, subdelegation, revocation, and auditable records of actions must be addressed so that third parties can later assess whether an action was authorized under the relevant conditions.
7. Participants called for international interoperability rather than incompatible European, U.S., and Japanese identity arrangements. They discussed combining public and private trust anchors, recognized issuers, common technical foundations, and sector-specific requirements so that businesses, including overseas suppliers, can participate without unnecessary duplication.
8. AI and semantic technologies were presented as opportunities to lower data-integration costs, but easier connections make counterparty trust more important. Shared credentials and verification mechanisms could reduce repeated due diligence for data recipients and provide suppliers with recognized qualifications for joining trusted business ecosystems.
9. The panel favored assurance proportionate to the use and its consequences. Provenance and organizational trust may suffice for some everyday uses, while safety-critical data requires stronger evidence. Similarly, AI agents handling financial or sensitive information need stricter controls than low-risk agents, including safeguards against accessing data beyond their delegated authority.

5. 甲斐氏は、人による確認に依存してきた信頼を、組織や国境を越えて検証できる仕組みに発展させることが共通の課題だと整理した。身元や署名の確認、来歴や改ざんの検知、データの品質、AIの判断の正しさは、それぞれ異なる問題であり、別の保証が必要だと強調した。
6. AIエージェントについては、誰の代理で行動し、どこまでの権限を持ち、その権限がいつまで有効なのかを確認する重要性が示された。委任、再委任、撤回、行為の監査記録を整備し、当時の条件の下で正当に認可された行為だったかを、第三者が後から検証できるようにする必要性を議論した。
7. 欧州、米国、日本で互換性のないID体系を作るのではなく、国際的な相互運用性を確保することを求めた。公的・民間の信頼の基点、信頼できる発行者、共通技術、分野ごとの要件を組み合わせ、海外の供給者も含む企業が重複した対応を強いられずに参加できる仕組みを議論した。
8. AIや意味情報を扱う技術によってデータ接続の費用を下げられる一方、接続が容易になるほど相手を信頼できるかが重要になると指摘した。共通の証明情報や検証の仕組みは、受け手の個別調査の負担を減らし、供給者には信頼できる事業環境へ参加する資格を示す手段になり得ると述べた。
9. 利用目的と影響に応じた信頼性の確保が必要だと議論した。日常的な用途では来歴や組織への信頼で足りる場合がある一方、生命・安全に関わるデータには強い証拠が求められる。同様に、金融や機微情報を扱うAIには厳格な管理が必要であり、委任された権限を越えたデータアクセスを防ぐ重要性が示された。
10. 最後に、実証から実装へ進み、国際的な共通ルールと、すべての層を通じたエンドツーエンドの信頼を確保することを求めた。規制対応の報告などの協調領域では共通のAIエージェントを利用し、競争領域では各社が独自性を育てる可能性を示した。信頼できるデータ経済に向け、国際協力、法律・契約の基盤、AIの動作を実効的に制御する仕組みを優先課題として挙げた。

10. Participants urged progress from demonstrations toward practical deployment, with global common rules and end-to-end trust across all layers. Shared agents could support cooperative tasks such as compliance reporting, while companies retain differentiation in competitive activities. International cooperation, legal and contractual foundations, and effective controls over AI behavior were identified as priorities for building a trusted data economy.	

D4-S11 Speech 15:25–15:40 JST

Session: Speech Speaker: Jean-Emmanuel PEREZ HERNANDEZ (Senior expert in electronic trust services, electronic identification, and digital trust strategy)	セッション：スピーチ 登壇者：ジャン＝エマニュエル・ペレス・エルナンデス (電子トラストサービス、電子認証、およびデジタルトラスト戦略のシニアエキスパート)
1. Jean-Emmanuel Perez Hernandez discussed trusted lists and the need for interconnected global trust frameworks. Using examples such as electronic invoices and news photographs, he asked how recipients can verify who created or signed information and whether that person was authorized to do so. 2. He described trust as involving several layers, including legal authority, recognition of trust-service providers, policies, and technical standards. Establishing trust requires mechanisms for assessing participants and maintaining evidence of their recognized status over time. 3. A central requirement is representing trust in a machine-processable form. Software needs usable information about which entities and services are recognized as trustworthy, by whom, and under what conditions, rather than relying solely on manual checks. 4. He explained that certificate-authority root stores provide an established basis for technical verification but have limitations. Trusted lists can provide more detailed information about recognized providers and services, supporting decisions beyond the acceptance of a root certificate alone. 5. Trusted lists can describe the scope of recognized services, their current status, and their history. Historical information is important when assessing whether a signature, timestamp, or other trust-service output was supported by the appropriate status at the relevant time.	1. ジャン＝エマニュエル・ペレス・エルナンデス氏は、トラステッドリストと、世界のトラストの枠組みを相互接続する必要性を論じた。電子請求書やニュース写真を例に、誰が情報を作成・署名したのか、その人物に権限があったのかを、受け手がどう確認するかを問いかけた。 2. トラストには、法的な権限、トラストサービス提供者の承認、方針、技術標準など、複数の層があると説明した。参加者を評価し、承認された状態を一定期間にわたって確認できる証拠を維持する仕組みが必要だと述べた。 3. 中心的な要件として、トラストを機械処理できる形で表現する重要性を示した。手作業の確認だけに頼らず、どの主体やサービスが、誰によって、どの条件で信頼できると認められているかを、ソフトウェアが利用できる情報として提供する必要があると説明した。 4. 認証局のルートストアは、技術的な検証の基盤として利用されてきた一方、限界もあると述べた。トラステッドリストでは、承認された提供者やサービスに関する詳細な情報を示し、ルート証明書を受け入れるだけでは判断できない事項を補えると説明した。 5. トラステッドリストでは、承認対象のサービスの範囲、現在の状態、過去の履歴を扱えると説明した。署名、タイムスタンプなどが作成された時点で、関係するサービスが適切な状態にあったかを判断するには、履歴情報が重要だと述べた。 6. EUでは、各加盟国が自国のトラステッドリストを管理し、共通の「リスト・オブ・リスト」がそれらを参照する連合型の仕組みを採っていると紹介した。各国の信頼の仕組みを維持しながら、共通の参照方法によって相互運用性を支える構成を説明した。

6. He introduced the EU's federated approach, in which Member States maintain their own trusted lists and a common list of lists points to them. This allows national trust arrangements to remain distinct while supporting interoperability through a shared discovery mechanism. 7. The discussion extended from trust-service providers to lists of trusted entities authorized to issue particular credentials, such as diplomas and electronic prescriptions. Recipients must verify not only the credential itself but also the issuer's authority to issue it. 8. He referred to work at Keio University and international standardization efforts aimed at extending trusted-list and list-of-lists approaches beyond the EU. The broader objective is a globally usable way to discover and verify trust information across different frameworks. 9. AI agents create further questions about who stands behind an agent and who has authorized its actions. He identified verifiable delegation and authorization, together with concerns about deepfakes and digital-content authenticity, as important challenges for future trust infrastructure. 10. He concluded by highlighting technical and semantic interoperability, differences in the recognition of services and credentials, and the maintenance of infrastructure across a global ecosystem. Connecting these arrangements requires balancing openness with sovereignty, consistency with flexibility, and stability with continued evolution.	7. 議論は、トラストサービス提供者から、卒業証書や電子処方箋など、特定の証明情報を発行する権限を持つ信頼できる主体のリストへと広がった。受け手は、証明情報そのものだけでなく、発行者がそれを発行する権限を持つことも確認する必要がある。 8. 慶應義塾大学での取り組みや、トラステッドリストとリスト・オブ・リストの考え方をEU域外へ広げる国際標準化の動きに言及した。異なる枠組みを越えて、信頼に関する情報を発見・検証できる、世界的に利用可能な仕組みを目指すと説明した。 9. AIエージェントについて、背後に誰がいるのか、誰がその行動を認めたのかという新たな課題を挙げた。ディープフェイクやデジタルコンテンツの真正性への懸念とともに、委任や認可を検証できる仕組みが、今後のトラスト基盤の重要な課題になると述べた。 10. 最後に、技術面と意味の面での相互運用性、サービスや証明情報の承認方法の違い、世界的なエコシステムにおける基盤の維持を課題として示した。開放性と主権、一貫性と柔軟性、安定性と継続的な進化のバランスを取りながら、異なる仕組みを接続する必要性を提起した。

D4-P12 Panel 15:40–16:40 JST

Session: Public Trust, ISO (Trusted List) Moderator: Jean-Emmanuel PEREZ HERNANDEZ Panelist: Wei-Chung Hwang Panelist: Vijayakumar Manjunatha (Digital Trust Advisor | Secretary General, Asia PKI Consortium) Panelist: Akira Nishiyama (Senior Researcher, Keio Research Institute at SFC)	セッション：パブリックトラスト、ISO標準(Trusted List) モデレーター：ジャン＝エマニュエル・ペレス・エルナンデス パネリスト：ウェン・チョン・ファン パネリスト：ビジャヤクマール・マンジュナータ (デジタルトラストアドバイザー／アジアPKIコンソーシアム 事務局長) パネリスト：西山 晃 (慶應義塾大学 SFC研究所 上席所員)
1. Moderated by Jean-Emmanuel Perez Hernandez, the panel examined trusted lists, international interoperability, and cross-border recognition of digital trust. Akira Nishiyama and Wei-Chung Hwang participated in the discussion, while Vijayakumar Manjunatha contributed a prerecorded presentation.	1. ジャン＝エマニュエル・ペレス・エルナンデス氏をモデレータに、トラステッドリスト、国際的な相互運用性、デジタルトラストの越境承認を議論した。西山氏とウェン・チョン・ファン氏が討論に参加し、ビジャヤクマール・マンジュナータ氏は事前収録の発表を提供した。

2. Akira Nishiyama described Japanese demonstrations of cross-border signature and seal verification, including exchanges with the EU and India. These projects illustrated how data spaces and trust-service infrastructure can work together, while revealing limitations in using a single connection point when jurisdictions recognize different partners.
3. He introduced a two-tier approach combining an International Trusted List (ITL) with domestic trusted lists (DTLs). Each jurisdiction could publish its recognized partners and domestic trust information, enabling verification paths that reflect its own recognition relationships. He described preparations for an ISO standardization proposal.
4. Akira Nishiyama emphasized that cross-border recognition requires examining legal equivalence together with the technical requirements supporting it. Comparable signature requirements, assurance, auditing, and supervision must be considered rather than assuming that technical verification alone establishes equivalent legal effects.
5. In his prerecorded presentation, Manjunatha discussed India–EU cooperation on advanced electronic signatures and seals. He distinguished document integrity, trust in certificate issuers, and legal effect, emphasizing that the initiative represented a framework for cooperation rather than an operational connection or completed legal mutual recognition.
6. He proposed progressing from machine-readable trust information and joint verification tests to comparisons of identity assurance, policies, and audit requirements, followed by clarification of legal effects and responsibilities. Trade documents and invoices were presented as practical applications, with national supervision retained rather than replaced by a single global PKI.
7. Hwang described Taiwan's electronic-signature framework, government and financial PKI arrangements, and experience with international interoperability. He highlighted trusted lists as a potentially practical alternative to more complex cross-certification approaches and stressed affordability for smaller businesses and openness to all participants.

2. 西山氏は、EUやインドとの間で行った、電子署名・電子シールの越境検証に関する日本の実証を紹介した。データスペースとトラストサービス基盤を組み合わせる可能性を示す一方、法域ごとに承認する相手が異なる場合には、単一の接続点を使う方式に限界があると説明した。
3. International Trusted List（ITL）と国内のトラステッドリスト（DTL）を組み合わせる二階層の構成を紹介した。各法域が承認する相手と国内の信頼情報を公開し、それぞれの承認関係に沿った検証経路を構成する考え方を示した。また、ISOへの標準化提案の準備について説明した。
4. 西山氏は、越境承認では、法的同等性と、それを支える技術的要件を一体として確認する必要があると強調した。技術的に検証できるだけで法的効力も同等になると考えるのではなく、署名要件、保証水準、監査、監督などを比較する重要性を示した。
5. マンジュナータ氏は、事前収録の発表で、インドとEUの高度電子署名・電子シールに関する協力を紹介した。文書の完全性、証明書発行者への信頼、法的効力を区別し、この取り組みは協力の枠組みであり、運用中の接続や法的な相互承認の完成を意味しないと強調した。
6. 機械可読な信頼情報の公開と共同検証から始め、本人確認の保証水準、方針、監査要件を比較し、その後に法的効力や責任を整理する段階的な進め方を提案した。貿易文書や請求書を実用的な用途として挙げ、単一の世界共通PKIに統合するのではなく、各国の監督を維持する考え方を示した。
7. ファン氏は、台湾の電子署名制度、政府・金融分野のPKI、国際的な相互運用の経験を紹介した。複雑な相互認証方式に対し、トラステッドリストが実装しやすい選択肢となる可能性を示し、中小企業も利用できる費用水準と、参加者に開かれたエコシステムの重要性を強調した。
8. 議論では、相互運用性や承認関係は、一度整備すれば終わるものではなく、継続的な維持が必要だと指摘した。技術、サービス、標準が法改正より速く変化する中、各国が対話を続け、技術要件の更新と国際的な整合を担う組織を明確に位置づける必要性を示した。
9. AIエージェントの普及により、PKI、身元確認、認可の証拠の重要性が高まると議論した。ファン氏は、より軽量な実装や短期間の証明情報が必要になる可能性を示し、西山氏は、委任の確認、属性を示す証明情報の活用、身元や権限を再確認する頻度の検討を重視した。
10. 全体を通じ、各国の主権を維持しながら、異なるトラストの枠組みを接続する必要性が示された。互換性のある標準、検証可能な信頼情報、用途に応じた保証水準、継続的な協力を基盤として、AIによる変化にも対応できる、実用的で包摂的な越境デジタルトラストを目指す方向性が共有された。

8. The discussion emphasized that interoperability and recognition require continuing maintenance. As technologies, services, and standards change faster than legislation, jurisdictions need sustained dialogue and clearly positioned organizations responsible for updating technical requirements and supporting international alignment. 9. AI agents were identified as a growing reason to strengthen PKI, identity, and evidence of authorization. Hwang suggested that agent-oriented infrastructure may need lighter implementations and shorter-lived credentials, while Akira Nishiyama emphasized verifying delegation, considering attribute-based credentials, and reassessing how frequently identity and authority should be checked. 10. The panel highlighted the need to preserve sovereignty while connecting different trust frameworks. Compatible standards, verifiable trust information, proportionate assurance, and continuing cooperation were presented as foundations for making cross-border digital trust practical, inclusive, and adaptable to AI-driven change.	

D4-S13 Speech 17:00–17:15 JST

Session: Speech Speaker: Nick Pope (Chair, ETSI Technical Committee on Electronic Signatures and Trust Infrastructures (TC ESI))	セッション：スピーチ 登壇者：ニック・ポープ (ETSI 電子署名・トラストインフラ技術委員会(TC ESI) 委員長)
1. Nick Pope, Chair of ETSI's Technical Committee on Electronic Signatures and Trust Infrastructures, introduced the European Digital Identity Wallet through a pre-recorded presentation, setting the context for the subsequent panel on digital identity wallets and electronic attestations of attributes. 2. He explained that the wallet aims to provide a common approach to high-assurance digital identification across Europe, addressing incompatibilities between national identity schemes. It also supports digital signatures, linking a person's national identity to electronic documents. 3. The wallet is intended to support applications beyond identification, including educational qualifications, travel documents such as boarding passes, banking and payments, and electronic prescriptions. These applications use documents signed by trusted issuers.	1. ETSIの電子署名・トラストインフラ技術委員会委員長であるニック・ポープ氏は、事前収録の講演で欧州デジタルIDウォレットの概要を紹介し、続くデジタルIDウォレットと属性の電子証明に関するパネルディスカッションの論点を提示した。 2. 欧州デジタルIDウォレットは、各国の本人確認制度間の互換性の問題に対応し、欧州全体で高い保証水準のデジタル本人確認を実現する共通の仕組みを目指している。また、電子署名にも対応し、国が提供する本人確認情報と電子文書を結び付ける。 3. ウォレットの用途は本人確認にとどまらず、学歴・資格の証明、搭乗券などの渡航関連文書、銀行取引・決済、電子処方箋などに広がっている。これらの用途では、信頼できる発行者が署名した文書を利用する。 4. 年齢確認は、ウォレットによるプライバシー保護の具体例である。ゼロ知識の技術を用いることで、身元を開示せずに年齢要件を満たすことを証明できる。属性の電子証明は、オンラインで提示するほか、近距離無線通信を使って対面でも交換できる。

4. Age verification illustrates how the wallet can protect privacy. Zero-knowledge techniques can enable users to demonstrate that they meet an age requirement without disclosing their identity. Electronic attestations of attributes can be presented online or exchanged in person using near-field communication.
5. The wallet application is only one component of the necessary trust infrastructure. Wallet providers must deliver their software securely, while relying parties must demonstrate their identity and authorization to receive information. Registers and certificates help wallets verify these parties and protect users' privacy.
6. The technical foundations include the W3C Verifiable Credentials data model, mobile driving licence standards, ISO 23220, OpenID protocols for verifiable credentials, and the Cloud Signature Consortium API for digital signature creation.
7. ETSI develops profiles of these underlying standards, together with policy and security requirements for supporting components and interface definitions for certain services. These specifications help establish consistent implementation and trustworthiness.
8. The infrastructure also builds on the European Commission's trusted list scheme to identify trustworthy services. Pope highlighted Keio University's work to internationalize this approach and enable interoperability between European and other national trust schemes.
9. He identified three requirements for international mutual recognition: precise profiles that combine the underlying standards, common application schemes defining the attributes required for particular attestations, and a common assurance regime supported by trust management mechanisms such as trusted lists.
10. He concluded by introducing ETSI resources for following this work, including news updates, freely available published standards, and a portal showing ongoing work items, their scope, and development status.

5. ウォレットのアプリケーションは、必要なトラストインフラの一部にすぎない。提供者による安全なソフトウェアの提供に加え、情報を受け取る検証者が、自らの身元と情報を受け取る権限を証明する必要がある。登録簿や証明書は、ウォレットによる相手の確認と利用者のプライバシー保護を支える。
6. 技術的な基盤には、W3CのVerifiable Credentialsデータモデル、モバイル運転免許証の標準、ISO 23220、検証可能な証明情報を扱うOpenIDのプロトコル、電子署名生成のためのCloud Signature ConsortiumのAPIなどが含まれる。
7. ETSIは、これらの基礎標準を具体的に適用するためのプロファイルを策定するとともに、関連する構成要素のポリシー・セキュリティ要件や、一部サービスのインターフェースを定義している。これらの仕様は、実装の一貫性と信頼性の確保を支える。
8. 信頼できるサービスを識別するため、欧州委員会のトラステッドリストの仕組みも基盤としている。ポープ氏は、慶應義塾大学がこの仕組みの国際化に取り組み、欧州と他国の信頼の仕組みの相互運用を目指していることを紹介した。
9. 国際的な相互承認に必要な条件として、基礎標準を組み合わせる具体的なプロファイル、証明の用途ごとに必要な属性を定義する共通の仕組み、そしてトラステッドリストなどの信頼管理の仕組みに支えられた共通の保証制度の3点を挙げた。
10. 最後に、ETSIの取り組みを継続的に確認するための情報源として、ニュース配信、無料で入手できる公開済み標準、進行中の作業項目の対象範囲や策定状況を確認できるポータルを案内した。

D4-P14 Panel 17:15–18:15 JST

Session: Digital Identity Wallet, Electronic Attestation of Attributes Moderator: Hiroshi Nakatake Panelist: Christoph Schneider (Head of IT Development and Operations, Global Legal Entity Identifier Foundation (GLEIF)) Panelist: Takashige Noguchi (Global Business Division Co-head of Global Business, WingArc 1st Inc.) Panelist: Takahiro Kanuma (R&D Lead, GMO GlobalSign Holdings K.K.)	セッション：デジタル・アイデンティティ・ウォレット、電子属性証明書 モデレーター：中武 浩史 パネリスト：クリストフ・シュナイダー (グローバル法人識別子財団(GLEIF) IT開発・運用責任者) パネリスト：野口 高成 (ウイングアーク1st株式会社 グローバル事業部 副事業部長) パネリスト：神沼 貴大 (GMOグローバルサイン・ホールディングス株式会社 CTO室 R&Dリード)
1. Moderated by Hiroshi Nakatake, the panel examined digital identity wallets, electronic attestations of attributes (EAA), and cross-border interoperability across Europe, ASEAN, and Japan. Nakatake introduced LEI as a global organizational identifier and vLEI as a means of verifying an individual's organizational affiliation, role, and authority. 2. Christoph Schneider outlined the proposed European Business Wallet, which would support organizational identification, the exchange of official documents, digital signatures and seals, and the authorization of representatives. He advocated extending this approach globally through LEI and vLEI, using organizational identifiers and standardized role information within electronic attestations. 3. Schneider identified challenges in achieving interoperability between national implementations, agreeing on regional and global standards, and enabling organizations to understand and adopt the technology. He emphasized staff education and the need for simple solutions that work with business partners worldwide. 4. Takashige Noguchi highlighted ASEAN's diversity in digital identity systems, legal frameworks, and economic development. He recommended beginning with practical business needs, particularly trusted document and data exchange between Japan and selected trading partners, and progressively expanding mutual recognition through pilots. 5. Takahiro Kanuma described a shift toward established web technologies and trust models, alongside stronger public-sector leadership. He explained Japan's position through a three-layer model: physical identity cards as the root of trust, national digital identity on smartphones, and EAA issued by public and private organizations. He viewed the third layer as Japan's next major area of development.	1. 中武浩史氏の進行により、欧州・ASEAN・日本におけるデジタルIDウォレット、属性の電子証明（EAA）、国境を越えた相互運用性について議論した。中武氏は、組織を識別するグローバルな識別子としてLEIを紹介し、個人の組織への所属、役割、権限を検証する仕組みとしてvLEIを説明した。 2. クリストフ・シュナイダー氏は、組織の本人確認、公的文書の交換、電子署名・電子シール、代理人への権限付与などを支える欧州ビジネスウォレットの構想を紹介した。さらに、属性の電子証明に組織の識別子や標準化された役割情報を組み込み、LEI・vLEIを通じて世界規模の利用へ広げることを提案した。 3. シュナイダー氏は、各国の実装間の相互運用性、地域・世界規模での標準への合意、利用する組織の理解と導入を課題として挙げた。職員への教育に加え、世界中の取引先と利用できる、分かりやすい仕組みを提供する必要性を強調した。 4. 野口高成氏は、ASEANではデジタルID、法制度、経済発展の状況が国ごとに大きく異なると説明した。日本と主要な取引相手国との間で、信頼できる文書・データの交換など、具体的なビジネス上の課題から着手し、実証を通じて相互承認を段階的に広げることを提案した。 5. 神沼貴大氏は、実績のあるウェブ技術や信頼モデルの活用と、公共部門による主導の強まりという動向を説明した。また、日本の状況を、信頼の起点となる物理的な本人確認カード、スマートフォン上の国のデジタルID、官民の組織が発行するEAAという3層で整理し、今後は3層目の発展が重要になるとの見方を示した。 6. 神沼氏は、日本の主な課題として、正当なEAA発行者を登録し、その信頼性を保証する仕組みと、国際的な相互運用性を挙げた。技術的な互換性に加え、国境を越えた利用を実現するためのルール、ガバナンス、法的な相互承認を整える必要があると指摘した。 7. 神沼氏は、特定のユースケースを選び、ガイドラインと技術的な保護措置を用意して小規模な実証から始め、その経験を基に対象を広げる方法を提案した。相互運用性の検証では、技術だけでなく、信頼、プライバシー、運用要件、ガバナンスも確認することが重要だと述べた。

6. Kanuma identified the registration and assurance of legitimate EAA issuers, together with international interoperability, as key challenges for Japan. He distinguished technical compatibility from the rules, governance, and legal mutual recognition needed to make cross-border use operational.
7. Kanuma proposed starting with specific use cases, guidelines, technical safeguards, and limited pilots, then expanding based on experience. He stressed that interoperability testing should cover trust, privacy, operational requirements, and governance as well as technology.
8. Schneider cautioned that multiplying bilateral agreements could create an increasingly complex and difficult-to-maintain network. He proposed connecting national and regional systems through common global standards and infrastructure, highlighting GLEIF and vLEI as potential foundations without requiring existing domestic systems to be replaced.
9. The discussion emphasized combining existing mechanisms, including international trusted lists, LEI, vLEI, and other trust services, to meet business needs. Kanuma called for public-private cooperation, with public bodies leading rules and governance and industry supporting implementation, conformance testing, pilots, and adoption.
10. In response to an audience question about concrete applications, Schneider cited customer and supplier verification, invoice fraud prevention, and verification of authorized representatives. Noguchi highlighted manufacturing and document exchange between Japan and ASEAN. Kanuma emphasized the continuing difficulty of achieving adoption, while Nakatake identified digital content and medical and pharmaceutical sectors as possible areas of demand because of concerns about counterfeiting, impersonation, and tampering.

8. シュナイダー氏は、二者間の合意を増やし続けると、接続関係が複雑化し、維持が困難になるおそれがあると指摘した。既存の国内制度を置き換えることなく、共通のグローバルな標準と基盤を通じて各国・地域の仕組みを接続することを提案し、GLEIFやvLEIがその基盤となる可能性を示した。
9. 議論では、国際トラステッドリスト、LEI、vLEI、その他のトラストサービスなど、既存の仕組みを組み合わせてビジネス上の需要に応えることが重視された。神沼氏は、公共部門がルールとガバナンスを主導し、民間が実装、適合性試験、実証、普及を支える官民連携の必要性を述べた。
10. 具体的な用途を問う会場からの質問に対し、シュナイダー氏は顧客・サプライヤー確認、請求書詐欺の防止、組織を代表する人物の権限確認を挙げた。野口氏は製造業や日本とASEAN間の文書交換を有望な対象とし、神沼氏は普及につなげる難しさが依然として残ると説明した。中武氏は、偽造・なりすまし・改ざんへの懸念から、デジタルコンテンツや医療・製薬分野にも需要が考えられると述べた。

D4-S15-1 Closing 18:15–18:30 JST

Session: Closing Speaker: D4-S15-1 Craig Wiener	セッション：クロージング 登壇者：D4-S15-1 クレイグ・ウィーナー
1. Speaking on behalf of The MITRE Corporation, Craig Wiener thanked Keio University and all co-sponsors for a successful four-day conference. 2. He expressed his commitment to working with the organizers over the coming year to develop an even better program for the 17th International Cybersecurity Symposium. 3. He conveyed appreciation for the hospitality and expressed MITRE's willingness to support the planned efforts.	1. クレイグ・ウィーナー氏は、MITRE Corporationを代表し、4日間の会議を成功に導いた慶應義塾大学とすべての共同スポンサーに謝意を表した。 2. 第17回サイバーセキュリティ国際シンポジウムのプログラムをさらに充実させるため、今後1年間、主催者と協力していく意向を示した。 3. 温かいもてなしに感謝するとともに、計画されている取り組みを支援していく姿勢を表明した。

D4-S15-3 Closing 18:15–18:30 JST

Session: Closing Speaker: D4-S15-3 Katsuya Yamamoto (Rear Admiral (retired), JMSDF Strategy and Deterrence Program Director Senior Research Fellow, Sasakawa Peace Foundation)	セッション：クロージング 登壇者：D4-S15-3 山本 勝也 (笹川平和財団 日米・安全保障研究ユニット 戦略・抑止グループ長 兼 主任研究員)
1. Katsuya Yamamoto of the Sasakawa Peace Foundation acknowledged the contributions of speakers, panelists, and participants from Japan and around the world, and paid tribute to Keio University, Professors Murai and Tezuka, the Keio Global Research Institute, and the staff who made the four-day symposium possible. 2. He praised the symposium's sustained contribution to the cybersecurity community by bringing together experts from government, industry, academia, and the international community amid a rapidly evolving cybersecurity landscape. 3. He noted that the Sasakawa Peace Foundation had joined the symposium as a co-organizer for the first time. Connecting its work on international security, defense, diplomacy, and economic security with cyberspace, he emphasized that modern society depends on secure and reliable digital networks. 4. Drawing on his experience in the Japan Maritime Self-Defense Force, he explained that the frontlines of security have expanded into cyberspace, which increasingly underpins the traditional domains of land, sea, and air. Cybersecurity has therefore become a shared responsibility supporting national security and social stability.	1. 笹川平和財団の山本勝也氏は、日本をはじめ世界各地から参加した登壇者、パネリスト、参加者の貢献をたたえ、4日間のシンポジウムを支えた慶應義塾大学、村井先生、手塚先生、慶應義塾大学グローバルリサーチインスティテュート、運営スタッフに敬意を表した。 2. サイバーセキュリティを取り巻く状況が急速に変化する中、政府、産業界、学術界、国際社会の専門家が集う場を継続し、国内外のサイバーセキュリティのコミュニティに貢献してきた本シンポジウムの意義を高く評価した。 3. 笹川平和財団が今回初めて共催者として参加したことに触れ、財団が取り組む国際安全保障、防衛、外交、経済安全保障とサイバー空間との関係を説明した。現代社会の機能は、安全で信頼できるデジタルネットワークに依存していると強調した。 4. 海上自衛隊での経験を踏まえ、安全保障の最前線はサイバー空間へと広がり、従来の陸・海・空の領域も、その基盤としてサイバー空間に依存するようになったと述べた。サイバーセキュリティは、国家安全保障と社会の安定を支える共通の責任になっていると指摘した。 5. 財団が進める社会全体のレジリエンスに関する研究と、政策提言の準備を紹介した。自然災害、パンデミック、経済的な衝撃、偽情報、サイバー攻撃、武力紛争などが相互に関連する中、混乱に耐え、変化に適応し、速やかに回復する能力が重要であり、サイバーセキュリティはその主要な柱であると述べた。

5. He introduced the foundation's research on whole-of-society resilience and its preparations for policy recommendations. With natural disasters, pandemics, economic shocks, disinformation, cyberattacks, and armed conflict increasingly interconnected, he described resilience as the ability to withstand disruption, adapt, and recover quickly, with cybersecurity as a key pillar. 6. Reflecting on discussions of national and economic security, artificial intelligence, quantum technologies, and digital trust, he identified a common objective: building stronger, safer, and more resilient societies. Achieving this requires cooperation across sectors, disciplines, and national borders. 7. He characterized the symposium as a community working toward a safer and more resilient future. He expressed the foundation's intention to continue collaborating toward a resilient society and a free, open, and secure international order, and hoped that the ideas and relationships formed would lead to further cooperation.	6. 国家安全保障、経済安全保障、AI、量子技術、デジタルトラストなど、会期中の幅広い議論に共通する目標は、より強く、安全で、レジリエントな社会を築くことだと整理した。その実現には、部門、専門分野、国境を越えた協力が必要であると強調した。 7. 本シンポジウムを、より安全でレジリエントな未来を築くコミュニティと位置付けた。財団として、レジリエントな社会と自由で開かれた安全な国際秩序に向けて協力を続ける意向を示し、会期中に生まれた知見や関係が、今後のさらなる連携につながることへの期待を述べた。

D4-S15-2 Closing 18:15–18:30 JST

Session: Closing Speaker: D4-S15-2 Jun Murai	セッション：クロージング 登壇者：D4-S15-2 村井 純
1. Jun Murai welcomed the preceding speakers' expressions of support for the next symposium and thanked the major sponsors and supporters for their encouragement. 2. Reflecting on the development of computers, the Internet, and the World Wide Web, he situated the symposium's discussions within the longer history of digital infrastructure and what he described as "digital civilization." 3. He highlighted digital trust as a means of replacing paper-based signatures and contracts, improving efficiency, and supporting economic development worldwide. He also acknowledged the continuing challenges of digital transformation, including in manufacturing, where Japanese leadership and expertise could contribute. 4. As business, policymaking, and public activities increasingly depend on the Internet, he emphasized that concern for cybersecurity must be accompanied by serious digital transformation within each sector.	1. 村井純氏は、先に挨拶した登壇者が次回シンポジウムへの支援の意向を示したことを歓迎し、主要なスポンサーと支援者からの心強い後押しに謝意を表した。 2. コンピューター、インターネット、ワールド・ワイド・ウェブの発展を振り返り、今回の議論を、デジタル基盤と、自らが「デジタル文明」と呼ぶものを築いてきた長い歴史の中に位置付けた。 3. 紙の署名や契約をデジタルトラストで置き換え、効率性を高めることが、世界の経済発展につながると述べた。一方で、デジタルトランスフォーメーションには依然として課題があり、日本のリーダーシップや専門性が期待される製造業でも、変革を進める難しさがあると指摘した。 4. 事業活動、政策に関わる活動、公共の活動がインターネットに依存するようになる中、サイバーセキュリティを重視することと、各分野で本格的なデジタルトランスフォーメーションを進めることを結び付ける必要性を強調した。 5. サイバーセキュリティ、信頼、デジタル技術の安全な利用への関心が、シンポジウムの場を越えて社会の幅広い分野に広がっていると述べた。この認識の広がりを、デジタルトランスフォーメーションの歴史における重要な転換点として捉えた。

5. He observed that cybersecurity, trust, and the safe use of digital technology had become concerns across society, extending well beyond the symposium itself. He described this broadening awareness as an important moment in the history of digital transformation. 6. He stressed the importance of learning from different stakeholders, since society-wide adoption involves diverse requirements for cybersecurity technologies and their deployment. 7. He expressed pride in Keio University's role in bringing together participants from different countries, industries, and sectors to share knowledge. Thanking participants for their contributions to the previous fifteen symposiums and the sixteenth event, he affirmed that preparations would proceed for the seventeenth symposium.	6. 社会全体での利用を考えると、サイバーセキュリティ技術やその導入に求められる要件も多様になるため、異なるステークホルダーの視点から学ぶことが重要であると強調した。 7. 世界のさまざまな地域、産業、社会の分野から参加者が集まり、知見を共有する場を慶應義塾大学が提供していることへの誇りを述べた。過去15回と今回の第16回への積極的な参加に感謝し、第17回シンポジウムに向けて準備を進める意向を表明した。

Parallel Session 並行セッション

DAY 2 2026-10-28 水曜日

Keio University, Mita Campus; North Building 1F North Hall
慶應義塾大学 三田キャンパス 北館 1F 北ホール

D2-T1-S2 Session 11:00–11:50 JST

Session: Strengthening U.S./Japan Cybersecurity and Compliance Alignment Moderator: Christopher Grady (Co-Founder & CTO, CyLogic Inc.) Panelist: Henry J. Sienkiewicz (Former CIO, DISA) Panelist: Maria Roat (Former First Director of FedRAMP) Panelist: Michael Carter (President, Fortreum) Panelist: Nobuyori Takahashi (CEO, Diarkis) Panelist: Mary Ann Swendsen (All Domain Joint Training Planner, U.S. Indo-Pacific Command (USINDOPACOM))	セッション：日米のサイバーセキュリティおよびコンプライアンスの連携強化 モデレーター：クリストファー・グラディ (CyLogic社 共同創業者・最高技術責任者) パネリスト：ヘンリー・J・シェンキェヴィッチ (元米国国防情報システム局 最高情報責任者) パネリスト：マリア・ロート (元FedRAMPディレクター(初代)) パネリスト：マイケル・カーター (Fortreum社長) パネリスト：高橋 信頼 (Diarkis代表取締役CEO) パネリスト：メアリー・アン・スウェンセン (米国インド太平洋軍〈USINDOPACOM〉全領域統合訓練プランナー)

1. Moderated by Christopher Grady, the session examined how the United States and Japan could strengthen cybersecurity and compliance alignment. Participants emphasized moving beyond parallel policy initiatives toward interoperable frameworks and operational practices that support secure information sharing and joint activities.
2. Henry Sienkiewicz stressed that cybersecurity leadership requires visible implementation, accountability, documented architectures, independent testing, and measurable operational outcomes. Maria Roat described Japan as an increasingly important strategic partner and emphasized that alignment must deliver practical security benefits rather than remain an administrative exercise.
3. Michael Carter recommended building on established frameworks and lessons from FedRAMP rather than designing a new system from scratch. Participants supported a risk-based approach that distinguishes systems by their impact and required assurance, while recognizing substantial overlap between NIST and ISO standards.
4. Roat identified common incident taxonomies, reporting fields, severity definitions, and machine-readable formats as foundations for alignment. Compatible reporting structures could allow organizations serving both governments to reuse information across requirements, reduce duplication, and focus resources on incident response. The objective should be interoperability rather than identical regulations.
5. Sienkiewicz highlighted the need for shared expectations concerning identity assurance, device and workload trust, data protection and tagging, least privilege, and access revocation. He also called for appropriate sharing of telemetry and security evidence, supported by realistic joint exercises covering containment, service degradation, restoration priorities, and responsibility for accepting residual risk.
6. Mary Ann Swendsen discussed the rapidly changing threat environment and the importance of enabling allies and partners to communicate, share data, and maintain a common operating picture across operational domains. Grady's account of a cloud deployment linking Virginia and Tokyo illustrated how cross-border incident reporting and differing definitions can present challenges beyond the technical infrastructure itself.

1. クリストファー・グレイディ氏の司会のもと、日米のサイバーセキュリティとコンプライアンスの整合性を強化する方法を議論した。安全な情報共有と共同活動を支えるため、両国が個別に政策を進める段階から、相互運用可能な枠組みと実際の運用へ移行する必要性が示された。
2. ヘンリー・シェンキェヴィチ氏は、サイバーセキュリティ分野の指導力を示すには、具体的な実装、説明責任、文書化されたアーキテクチャ、独立した検証、測定可能な運用成果が必要だと指摘した。マリア・ロート氏は、日本を重要性の増す戦略的パートナーと位置づけ、整合性の確保を事務的な作業にとどめず、実際の安全性向上につなげるべきだと述べた。
3. マイケル・カーター氏は、新たな制度を一から設計するよりも、FedRAMPなどの既存の枠組みとその経験を活用することを提案した。登壇者は、NISTとISOの基準に多くの共通点があることを踏まえつつ、システムへの影響と必要な保証水準を区別するリスクベースのアプローチを支持した。
4. ロート氏は、インシデントの分類、報告項目、重大度の定義、機械可読形式の共通化を整合性確保の基盤として挙げた。日米双方にサービスを提供する組織が報告情報を複数の要件に再利用できれば、重複作業を減らし、インシデント対応に資源を集中できると説明した。目指すべきは規制の完全な統一ではなく、相互運用性だと強調した。
5. シェンキェヴィチ氏は、本人確認の保証水準、デバイスとワークロードの信頼性、データ保護とタグ付け、最小権限、アクセス権限の取り消しについて、共通の認識が必要だと述べた。また、テレメトリやセキュリティの証拠を適切に共有し、封じ込め、サービス低下、復旧の優先順位、残存リスクの受容責任を含む現実的な共同演習を行うよう求めた。
6. メアリー・アン・スウェンセン氏は、急速に変化する脅威環境を踏まえ、同盟国やパートナーが複数の作戦領域で通信とデータ共有を行い、共通の状況認識を維持する重要性を説明した。グレイディ氏が紹介したバージニア州と東京を結ぶクラウドの事例からは、国境をまたぐインシデント報告や用語の違いが、技術基盤の構築以上に課題となり得ることが示された。
7. ロート氏は、FedRAMPの立ち上げ経験から、リスクに応じた分類、独立した評価と認可、継続的監視、証拠の再利用、経営層の明確な責任を取り入れるよう提案した。一方、過剰な書類作業、重複する評価、小規模事業者に不必要な負担をかける要件、長期化する認可手続きは避けるべきだと述べ、過去の実装上の課題から学びながら信頼の仕組みを採用するよう勧めた。

7. Drawing on her experience establishing FedRAMP, Roat recommended adopting risk-based categorization, independent assessment and authorization, continuous monitoring, reusable evidence, and clear executive accountability. She cautioned against excessive paperwork, overlapping assessments, requirements that unnecessarily burden small providers, and lengthy authorization cycles, urging Japan to adopt the trust model while learning from earlier implementation difficulties. 8. Carter emphasized that credible third-party assessments require qualified organizations and individual assessors, detailed security control reviews, authenticated vulnerability scanning, penetration testing, and other technical testing. Participants stressed that evidence of actual system behavior, architecture, and data flows is essential for authorization decisions and that assessment must produce security outcomes rather than paperwork alone. 9. Swendsen described ongoing experimentation with AI-enabled decision support and information sharing involving Japan and other partners. She identified unresolved trust questions concerning AI-generated information and recommendations, including whether humans have validated the content and whether partners consider it reliable enough for operational use. 10. Participants unanimously rated strengthening U.S.-Japan cybersecurity and compliance alignment as a top priority. Their closing remarks emphasized the urgency of translating shared frameworks, technical evidence, and mutual trust into coordinated execution and operational cooperation.	8. カーター氏は、信頼できる第三者評価には、評価機関と評価担当者双方の能力に加え、詳細なセキュリティ管理策の確認、認証済みの脆弱性スキャン、ペネトレーションテストなどの技術的検証が必要だと説明した。登壇者は、実際のシステム動作、構成、データの流れを示す証拠が認可判断に不可欠であり、評価を単なる書類確認で終わらせてはならないと強調した。 9. スウェンセン氏は、日本などのパートナーと進める、AIを活用した意思決定支援と情報共有の実験について紹介した。AIが生成した情報や提案に人間による検証が加わっているか、各国が実際の運用に使えるほど信頼できるかなど、未解決の課題が残ると説明した。 10. 登壇者全員が、日米のサイバーセキュリティとコンプライアンスの整合性強化を最優先の課題と評価した。共通の枠組み、技術的な証拠、相互の信頼を、連携した実行と運用上の協力につなげることの緊急性を確認して締めくくった。

D2-T1-S3 Session 13:00–13:50 JST

Session: Highly Reliable Data Platform with the Data Credit Guarantee Organization (DCGO) Moderator: Dr.Hiroshi Mano (Secretary General, Data Society Alliance) Panelist: Satoshi Morinaga (Executive Research Fellow, R&D Division, NEC Corporation) Panelist: Teruyoshi Fujiwara (Representative Director, Automotive and Battery Traceability Center Association, Inc. (ABtC)) Panelist: Naoto Kikuchi (Project Professor, Graduate School of Media Design, Keio University) Panelist: Yasushi Hirakawa (NS Solutions Corporation (NSSOL))	セッション：データ信用保証機構（DCGO）を中核とする高信頼データ連携基盤の構築 モデレーター：眞野 浩 (一社)データ社会推進協議会 専務理事 事務局長) パネリスト：森永 聡 (日本電気株式会社　研究開発部門 上席主席研究員) パネリスト：藤原 輝嘉 (一般社団法人自動車・蓄電池トレーサビリティ推進センター 代表理事) パネリスト：菊池 尚人 (慶應義塾大学大学院メディアデザイン研究科特任教授) パネリスト：平川 泰 (日鉄ソリューションズ株式会社 鉄鋼ソリューション事業本部)

1. The session introduced DCGO, a provisional name for a trusted data-sharing infrastructure being researched under the Japanese government's BRIDGE program. The project aims to address concerns about security, rights, and trust that hinder data sharing. It focuses on technical research and development, use-case evaluation, pathways to social implementation, and international standardization, rather than directly establishing legislation or a new institutional framework.
2. The proposed infrastructure would connect data with information about the parties involved, its origin and characteristics, usage rights and conditions, and its transfer and processing history. Hash values, timestamps, electronic signatures, and electronic seals were presented as supporting verification tools, with the explicit qualification that a hash can help detect changes but cannot establish whether the data's content is true.
3. Participants discussed a third-party function analogous to notarization that would help demonstrate who provided data, under what agreement, and for what permitted uses. Managing data and contractual conditions together could support verification of legitimate use and traceability. The concept remains a research proposal and was distinguished from the existing legal notary system.
4. NEC described plans to design common infrastructure around the functional and nonfunctional requirements of different use cases. Its research on negotiation between AI agents could support agreements on data selection, permitted purposes, compensation, and usage periods. The infrastructure would need to support execution and verification of those agreements, with future AI agents anticipated to become major users.
5. The automotive battery use case highlighted the need to connect data across manufacturers, users, collection operators, and recyclers. Battery passports and related traceability services could support carbon-footprint information, due diligence, resource recovery, and international cooperation. The project will examine where the proposed trusted intermediary could add value within these existing and developing data-sharing arrangements.

1. 本セッションでは、国のBRIDGEプログラムのもとで研究する信頼データ連携基盤「DCGO（仮称）」を紹介した。データ連携を妨げる安全性、権利、信頼への不安に対応するため、技術研究開発、ユースケースによる評価、社会実装に向けた検討、国際標準化に取り組む。法律や制度を直接制定する事業ではなく、研究成果を社会実装につなげるためのプロジェクトと説明された。
2. 提案する基盤では、データに関わる主体、出所や特性、利用権限と条件、受け渡しや加工の履歴を結びつけて管理する。確認を支える技術としてハッシュ値、時刻情報、電子署名、eシールなどが示された。ただし、ハッシュ値はデータの変更を検知する助けになるものであり、内容そのものが真実であることを証明するものではないと明確に説明された。
3. 誰が、どのような契約に基づき、どの範囲で利用できるデータを提供したのかを第三者が確認できる、公証に類する機能が議論された。データと契約条件を一体で管理することで、適正な利用の確認や取引の追跡を支える構想である。既存の法的な公証人制度とは区別され、研究段階の提案として位置づけられた。
4. NECからは、各ユースケースの機能要件と非機能要件を取り込みながら、共通基盤を設計する方針が示された。AIエージェント間の交渉により、提供するデータ、利用目的、対価、利用期間などの合意を支援し、その実行と検証を支える仕組みが必要だと説明された。将来はAIエージェントが基盤の主要な利用者になることも想定している。
5. 自動車蓄電池のユースケースでは、製造、利用、回収、リサイクルに関わる多様な主体のデータ連携が課題として挙げられた。電池パスポートやトレーサビリティサービスを通じ、カーボンフットプリント、デューデリジェンス、資源回収、国際連携を支える取り組みを紹介し、既存・開発中の仕組みの中で信頼を担う仲介機能がどのような価値を提供できるかを検討するとした。
6. 教育・医療分野では、システムの接続やデータの標準化に加え、その基盤となる信頼の仕組みが必要だと指摘された。高知県西部の地域医療情報共有ネットワークを事例に、医療・介護などの関係者が記録を共有する際の患者同意や、データ取引の証明のあり方を実際の運用に即して検証する計画が紹介された。
7. 技術的なアーキテクチャと並び、制度やガバナンスの検討も重要な課題として示された。日本とEUのトラストサービスに関する制度を比較し、運営主体、法律とソフトローの役割、ユースケースと制度上の要件の関係などを研究する方針が説明された。これらは確定した政策ではなく、今後検討する論点として提示された。

6. The discussion of education and healthcare emphasized that connecting systems and standardizing data also require an underlying trust framework. A regional healthcare information-sharing network in western Kochi Prefecture was presented as a practical setting for examining data transaction certification, patient consent, and the sharing of records among medical, care, and other authorized participants.
7. Participants identified institutional arrangements and governance as essential considerations alongside technical architecture. Planned work includes comparing Japan's trust-service arrangements with those in the EU and examining possible operators, the roles of legislation and nonbinding rules, and the relationship between practical use cases and governance requirements. These issues were presented as research topics rather than settled policy choices.
8. The steel distribution use case illustrated fragmented information flows, continued reliance on paper records, and the difficulty of maintaining traceability through processing, cutting, and recycling. Expectations for DCGO included protection against impersonation and tampering, preservation of trade secrets and control over data use, and continuity between physical materials and their associated information. Participants also distinguished material-related information from environmental attributes such as allocated emissions reductions.
9. Participants stressed that verifying provenance does not by itself establish the truth or suitability of data. Trust also depends on the qualifications of the parties and AI agents involved, transaction traceability, and the intended use. Restrictions on secondary use were particularly important where carbon-footprint data could reveal production processes or allow others to infer commercially sensitive costs.
10. The closing discussion examined the value of third-party verification and who should pay for it. Participants recognized potential benefits but raised concerns about the complexity of verifying entire processes, passing costs on to users, possible public funding for public-interest data, and resistance to changing established commercial practices. Sustainable implementation would therefore require attention to incentives, cost allocation, and social acceptance as well as technology.

8. 鋼材流通のユースケースでは、情報の分断、紙による運用、加工・分割・再資源化を経ても追跡可能性を維持する難しさが紹介された。DCGOには、なりすましや改ざんへの対策、営業秘密とデータ利用の主導権の保護、物と情報のつながりの維持が期待されるとした。また、材料そのものに関する情報と、排出削減量の割り当てなどの環境価値を区別して扱う必要性が示された。
9. データの出所が確認できても、内容の真実性や利用目的への適合性まで保証されるわけではないことが議論された。信頼の判断には、取引主体やAIエージェントの適格性、取引の追跡可能性、利用目的なども関わる。特にカーボンフットプリントのデータから製造工程や原価が推測される懸念があり、目的外利用を制限することが重要だと指摘された。
10. 終盤では、第三者による確認にどの程度の価値を認め、誰が費用を負担するかを議論した。価値を認める意見がある一方、工程全体を検証する複雑さ、利用者への費用転嫁、公的な性格を持つデータへの公費投入、従来の商慣行を変える難しさなどが挙げられた。持続可能な社会実装には、技術だけでなく、利用の動機、費用分担、社会的な受容も検討する必要があるとされた。

D2-T1-S4 Session 14:00–14:50 JST

Session: Sovereign AI, Data Sovereignty, and the Deployment of PETs — Cybersecurity Across National, Economic, and Social Security Moderator: Tsubasa Takahashi (Chief Scientist / VP of Research & Development, Acompany Co., Ltd.) Panelist: Daisuke Inoue (Director General of Cybersecurity Research Institute, National Institute of Information and Communications Technology) Panelist: Seira Hidano (Senior Manager, Cyber Intelligence Laboratories, KDDI Research, Inc.) Panelist: Takeharu Kondo (Director / Solutions CTO, Acompany Co., Ltd.)	セッション：ソブリンAI時代のデータ主権をどう守るか ―― 国家安全保障・経済安全保障・社会保障を支えるサイバーセキュリティと、プライバシー保護技術 (PETs) の社会実装 モデレーター：髙橋 翼 (株式会社Acompany Chief Scientist 兼 執行役員 VP of Research & Development, 博士(工学)) パネリスト：井上 大介 (国立研究開発法人情報通信研究機構 サイバーセキュリティ研究所 研究所長) パネリスト：披田野 清良 (株式会社KDDI総合研究所 サイバーインテリジェンス研究所 グループリーダー) パネリスト：近藤 岳晴 (株式会社Acompany 取締役 ソリューション事業CTO)

1. Organized by the Privacy Tech Association, the session examined how privacy-enhancing technologies (PETs) can help protect data sovereignty in the era of sovereign AI. Presentations and discussion covered privacy-preserving federated learning, confidential computing, and data clean rooms, focusing on enabling AI use while maintaining control over sensitive data.
2. NICT explained that federated learning allows multiple organizations to collaboratively develop models without centrally collecting their original data. However, sharing model updates or gradients can still expose information about training data, so keeping raw data within each organization is not sufficient by itself to ensure privacy.
3. NICT presented DeepProtect, which uses homomorphic encryption to process encrypted contributions from participating organizations without decrypting them at the central server. Banking experiments for detecting fraudulent transfers showed improved detection performance through collaboration, with further benefits from combining collaborative and individual models. Ongoing medical applications highlighted additional challenges involving large datasets and differences in data formats.
4. Acompany introduced confidential computing as a way to protect data during processing through hardware-based trusted execution environments (TEEs). Isolation and memory encryption help restrict access by infrastructure administrators, while remote attestation allows users to verify the execution environment before sending sensitive information.
5. Confidential computing was also discussed as a means of protecting AI prompts, confidential business information, and model parameters on infrastructure operated by other organizations. The presentation emphasized its potential to support trusted AI services and protect valuable models, alongside broader applications in privacy-preserving data collaboration.
6. KDDI Research presented a private data clean room that combines protection during data collection, confidential computing during analysis, and privacy controls on outputs. Its design supports analysis across organizations while restricting the release of original information, with capabilities for tabular data, machine learning, generative AI, and matching datasets that lack common identifiers.

1. プライバシーテック協会が主催し、ソブリンAI時代のデータ主権をプライバシー強化技術（PETs）でどう守るかを議論した。プライバシー保護連合学習、コンフィデンシャルコンピューティング、データクリーンルームの紹介を通じ、機微なデータへの管理権限を維持しながらAIを活用する方法を検討した。
2. NICTは、元のデータを一か所に集めず、複数組織が協力してモデルを構築する連合学習を説明した。ただし、共有するモデルの更新情報や勾配情報から学習データが推測・復元される可能性があり、生データを各組織の内部に置くだけでは十分なプライバシー保護にならないと指摘した。
3. NICTは、準同型暗号を用い、各組織からの情報を中央サーバーで復号せずに処理するDeepProtectを紹介した。不正送金検知に関する銀行間の実証では、共同学習によって検知性能が向上し、個別モデルとの組み合わせでさらに改善したと報告した。医療分野への応用も進めており、大容量データへの対応や組織間で異なるデータ形式の調整が課題として挙げられた。
4. Acompanyは、ハードウェアに基づく信頼できる実行環境（TEE）で処理中のデータを保護するコンフィデンシャルコンピューティングを紹介した。実行環境の隔離とメモリ暗号化によってインフラ管理者などからのアクセスを制限し、リモートアテステーションによって、機密情報を送信する前に処理環境を検証する仕組みを説明した。
5. コンフィデンシャルコンピューティングは、他社が運用するインフラ上でAIのプロンプト、企業の機密情報、モデルのパラメーターを保護する手段としても紹介された。信頼できるAIサービスの構築や価値のあるモデルの保護に加え、プライバシーに配慮した企業間データ連携への応用可能性が示された。
6. KDDI総合研究所は、データ収集時の保護、分析時のコンフィデンシャルコンピューティング、出力時のプライバシー制御を組み合わせたプライベート型データクリーンルームを紹介した。元の情報の持ち出しを制限しながら組織横断の分析を行い、表形式データ、機械学習、生成AIに対応するとともに、共通IDのないデータ同士を照合する機能も備えると説明した。
7. パネルでは、データの保存先と処理場所を管理すること、外部事業者への依存を抑えること、ソースコードやシステム文書などの機密情報を保護することを、データ主権と結びつけて議論した。国内での処理能力や基盤を確保する考え方に加え、外部のインフラ上でも技術的な保護によって信頼できる処理環境を構築する方法が示された。
8. 普及の障壁として、認知度の不足、安全なアプリケーション設計の実践例の少なさ、ハードウェアやGPUとの適合性、実装に必要な専門知識、処理時間・有用性・精度のトレードオフが挙げられた。連合学習では、参加組織ごとに学習用の機器を設置・運用する負担も課題とされた。

7. The panel connected data sovereignty with the ability to control where data is stored and processed, reduce dependence on external providers, and protect sensitive information such as source code and system documentation. Participants discussed both maintaining domestic capabilities and using technical safeguards to establish trusted processing environments on externally operated infrastructure. 8. Barriers to wider adoption included limited awareness, a shortage of secure application design practices, hardware and GPU compatibility, implementation expertise, and trade-offs involving processing time, analytical utility, and accuracy. Federated learning also creates deployment burdens when participating organizations must operate their own local learning equipment. 9. Participants emphasized combining PETs rather than relying on a single technology. One proposed approach was to run federated learning components within confidential computing environments, potentially simplifying deployment while adding a further protection layer. Practical implementations and shared design patterns were identified as important for making these technologies easier to adopt. 10. The closing discussion called for collaboration with data holders and application providers to accumulate practical experience and demonstrate useful applications. Participants also stressed the need to clarify what “sovereign” and “domestic” mean for AI, including the origins of models and architectures, and to develop a shared understanding among stakeholders.	9. 単一の技術に依存せず、複数のPETsを組み合わせる重要性が強調された。連合学習の処理をコンフィデンシャルコンピューティング環境内で動かすことで、保護を重ねながら導入を簡素化できる可能性が議論された。実際の導入事例や設計パターンを蓄積・共有し、利用しやすい技術にしていく必要性が示された。 10. 終盤では、データ保有者やアプリケーション提供者と連携し、実際の用途を通じて経験を蓄積することが呼びかけられた。また、AIの「ソブリン」や「国産」が何を意味するのかについて、モデルやアーキテクチャの出自も含めて整理し、関係者間で共通認識を形成する必要性が指摘された。

D2-T1-S5 Session 15:00–15:50 JST

Session: What is needed to make e-Seal standard practice? Moderator: Koichi Shibata (Steering Committee Chair, Japan Digital Trust Forum) Panelist: Naohiko Sagara (General Manager, Secom Trust Systems CO., LTD.) Panelist: Hiroshi Arakawa (President & CEO, ENNA Co., Ltd.) Panelist: Kentaro Ito (Senior Consultant, Business Planning Section, GMO GlobalSign K.K.) Panelist: Takumi Sato (Product Manager for the iTrust Remote Signature Service and iTrust Electronic Signature Certificates, Cybertrust Japan Co., Ltd.)	セッション：eシールを商慣習にするには、何が不足しているのか？ モデレーター：柴田 孝一 ((一社)デジタルトラスト協議会 運営会議長) パネリスト：相良 直彦 (セコムトラストシステムズ(株)担当部長) パネリスト：荒川 大 (株式会社ENNA 代表取締役) パネリスト：伊藤 健太郎 (GMOグローバルサイン株式会社 電子証明書事業本部 ソリューションサービス事業部 事業企画セクション Senior Consultant) パネリスト：佐藤 拓巳 (サイバートラスト株式会社 トラスト基盤プロダクトマネジメント部 部長)

1. An e-seal allows recipients to verify which organization issued electronic data and whether the data has been altered since issuance. An electronic signature serves a different purpose by expressing an individual's intent. 2. Images of stamped seals and email domains provide limited assurance about who issued the data. Verifying the issuer and the integrity of the data becomes more important as AI and business systems generate more data automatically. 3. Building e-seal application and automatic verification into business systems can make e-seals part of routine work. Users also need training on how to respond when verification flags a problem. 4. Connecting data creation, sealing, transmission, verification, and processing can reduce manual checks and data entry. Invoices, certificates, and manufacturing quality documentation were cited as potential use cases. 5. An e-seal can identify the organization issuing AI-generated data. Establishing how the data was generated and governing the AI system require additional technologies and processes suited to those purposes. 6. When manual checks remain in place, e-seals add to existing costs. Adoption is also harder when issuers pay for e-seals while recipients benefit from verification. Automating the full workflow can show which manual tasks e-seals help eliminate. 7. The discussion described Level 1 and Level 2 e-seals as sharing the basic functions of verifying the issuer and detecting alterations. Regulatory frameworks and industry guidelines could clarify when to choose a recognized e-seal and set operational standards for providers. 8. Fragmentation across services and difficulty choosing a suitable service also hinder adoption. Making e-seals routine requires accessible verification, incentives to adopt them, and clear responsibilities for the parties involved.	1. eシールは、電子データを発行した組織と改ざんの有無を確認する仕組みであり、人の意思を示す電子署名とは役割が異なる。 2. 紙の印影画像やメールドメインへの信頼だけに頼らず、発行元とデータの完全性を仕組みで確認する必要がある。AIやシステムが自律的にデータを生成するほど、その重要性が増す。 3. 利用者に技術の理解や手作業での確認を求めるより、サービスや業務システムにeシールの付与と自動検証を組み込み、意識せず利用できる環境を整えることが重要である。異常や改ざんの警告に対応するための利用者教育は必要となる。 4. eシールの価値は、データの作成・付与・送付・検証・処理をつなぎ、人手による確認や転記を減らすことにある。請求書、各種証明書、製造業の品質証明などが利用場面として挙げられた。 5. AIが生成したデータでも発行組織の確認に活用できる一方、生成の来歴やAIの統制までeシールだけで保証するものではなく、他の技術との組み合わせと役割整理が必要である。 6. 普及の障壁として、人手の確認に追加されるコストと、発行側が費用を負担し受領側が便益を得る構造が指摘された。業務全体を自動化し、人手のコストを置き換える価値を示すことが重要である。 7. 発行元と改ざんの確認という基本機能ではレベル1とレベル2に差がないとの説明があり、認定されたeシールを選ぶ理由を制度や業界ガイドラインで明確にすること、サービスの運用基準を整えることが課題とされた。 8. サービス間の分断や選択の難しさも普及を妨げている。eシールそのものの普及ではなく、利用者が便利で信頼できる業務を実現するため、検証環境・制度・インセンティブと関係者の役割分担を整える必要がある。

D2-T1-S6 Session 16:00–16:50 JST

Session: Examining the Debate on Digital Sovereignty Moderator: Naoto Kikuchi (Digital Policy Forum Japan, Acting Chairman) Panelist: Yasuhiko Taniwaki (Digital Policy Forum Japan, Chairman) Panelist: Mitsuru Ikeda (Chief Director for International Strategy, Strategy and Organization Group, Digital Agency) Panelist: Yasushi Matsumoto (Fellow, Japan Network Security Association (JNSA))	セッション：デジタル主権を巡る議論を考える モデレーター：菊池 尚人 (デジタル政策フォーラム 代表幹事代理) パネリスト：谷脇 康彦 (デジタル政策フォーラム 代表幹事) パネリスト：池田 満 (デジタル庁 戦略・組織グループ 参事官 (国際戦略担当)) パネリスト：松本 泰 (NPO法人日本ネットワークセキュリティ協会(JNSA) フェロー)

1. The Digital Policy Forum session examined digital sovereignty from the perspectives of digital trust, international cooperation, and national strategy. Participants emphasized the need to connect discussions of AI, data, infrastructure, and technology within an overarching framework, rather than treating them as separate policy issues.
2. The opening presentation framed digital sovereignty as a question of sovereignty and governance in a society where cyberspace and the physical world are increasingly integrated. The growth of major platforms and the concentration of digital services were contrasted with the Internet's original principles of autonomy, decentralization, and cooperation.
3. Digital trust was presented as an arena of governance as well as a technical means of protection. Questions about who determines trust anchors, recognizes identities and attributes, and sets verification rules affect the distribution of authority. European debates concerning website authentication and digital identity were used to illustrate tensions between public institutions and platform providers.
4. Participants argued that Japan cannot realistically develop or operate every digital component domestically. The strategic task is to determine which capabilities Japan must retain, how to evaluate technologies independently, and how to combine technical assurance with transparent institutions. International interdependence should be managed rather than assumed to be avoidable.
5. The Digital Agency presentation described European sovereignty discussions as moving from broad principles toward concrete procurement and assessment mechanisms. These examples were interpreted as efforts to evaluate degrees of control and dependence, rather than simply exclude foreign technology. Maintaining openness and the ability to choose remained important considerations.
6. Japan's government AI initiative, Gennai, was presented as an example of enabling safe selection and operation without excessive dependence on a particular provider or foundation model. Trials involving domestic language models and domestic cloud infrastructure were discussed alongside the option of combining domestic and foreign technologies according to purpose.

1. デジタル政策フォーラムの本セッションでは、デジタルトラスト、国際連携、国家戦略の観点からデジタル主権を議論した。AI、データ、インフラ、技術に関する政策を個別に扱うのではなく、全体をつなぐ共通の枠組みとして捉える必要性が示された。
2. 冒頭の発表では、デジタル主権を、サイバー空間と現実空間が高度に融合した社会における主権と統治の問題として整理した。巨大プラットフォームの台頭とデジタルサービスの集中が、インターネットの当初の理念である自律・分散・協調との関係で論じられた。
3. デジタルトラストは、技術的な保護手段であると同時に、ガバナンスが行使される場でもあると説明された。信頼の基点を誰が決めるか、主体の身元や属性を誰が認めるか、検証のルールを誰が定めるかは、権限の配分に関わる。欧州のウェブサイト認証やデジタルアイデンティティをめぐる議論が、公的機関とプラットフォーム事業者の関係を示す例として紹介された。
4. 日本がデジタル技術や基盤のすべてを国内で開発・運用することは現実的ではないと指摘された。国内に保持すべき能力を見極め、技術を自ら評価し、透明性のある制度と技術的な保証を組み合わせることが重要とされた。国際的な相互依存を避けるのではなく、適切に管理する視点が示された。
5. デジタル庁からは、欧州の主権に関する議論が、理念から具体的な調達・評価の仕組みへ移りつつあると紹介された。これらは外国技術を一律に排除するのではなく、管理・支配の程度や依存関係を段階的に評価する取り組みとして説明された。開放性を維持しながら、自ら選択できることの重要性が示された。
6. 政府向けの生成AI利用環境「源内」は、特定の事業者や基盤モデルへの過度な依存を避け、安全に選択・運用できるようにする取り組みとして紹介された。国産の言語モデルや国内クラウドを活用する試行に加え、目的や用途に応じて国内外の技術を組み合わせる考え方が示された。
7. DFFT（信頼性のある自由なデータ流通）については、理念を具体的な国際協力につなげる重要性が説明された。OECDでの活動、日EUの連携、国内の官民によるデータ連携の取り組みを通じ、信頼に基づく相互運用性を高める方針が示された。囲い込みや孤立ではなく、選べること、移れること、確かめられることが重視された。
8. 戦略的な整理として、デジタル主権を技術・インフラ・データの三つの層で捉える考え方が示された。欧州のEuroStackやインドの公共デジタル基盤などを含む各国のアプローチを比較し、官民の役割を組み合わせ、日本の強みを補完するパートナーと連携する重要性が説明された。

7. The discussion of Data Free Flow with Trust (DFFT) emphasized translating principles into practical international cooperation. Work through the OECD, Japan-EU collaboration, and domestic public-private data-sharing initiatives was presented as supporting trusted interoperability. The ability to choose, switch providers, and verify services was emphasized over enclosure or isolation. 8. A strategic overview organized digital sovereignty into three connected layers: technology, infrastructure, and data. Comparisons among international approaches, including Europe's EuroStack and India's public digital infrastructure, highlighted the importance of combining public and private roles and working with partners whose strengths complement Japan's own. 9. AI was discussed as both accelerating the integration of digital and physical systems and changing the conditions for cybersecurity and deterrence. Participants highlighted the need to consider civilian and military applications together, including technology transfer in both directions, while recognizing the asymmetry between attackers operating without safeguards and defenders subject to governance requirements. 10. The panel stressed retaining domestic expertise to assess AI models, agents, and their security rather than treating them as trusted black boxes. It also called for attention to the timing and sector-specific role of regulation and to the relationship between trustworthy data and trustworthy AI, particularly as physical AI draws on data that is not openly available online.	9. AIは、サイバー空間と現実空間の融合を加速させるとともに、サイバーセキュリティや抑止の条件を変える技術として論じられた。民生と軍事の双方の用途や、官から民・民から官への技術移転を視野に入れる必要性が示された。また、攻撃側は制約なくAIを利用し得る一方、防御側にはガバナンス上の制約があるという非対称性も指摘された。 10. パネルでは、AIモデルやエージェントをブラックボックスのまま信頼するのではなく、安全性や信頼性を評価する専門能力を国内に保持する必要性が強調された。規制の時間軸や分野ごとの役割を考えることに加え、公開されていないデータを利用するフィジカルAIなどでは、データの信頼性がAIの信頼性に直結する点が重要な論点として示された。

DAY 3 2026-10-29 木曜日

Keio University, Mita Campus; East Building 8F Hall
慶應義塾大学 三田キャンパス 東館 8F ホール

D3-T1-S1 / D3-T1-S2 Session 10:00–11:50 JST

Session: Exchange of Best Practices for Responsible Industry Behaviour for Dual-use AI in the Military Domain (Roundtable by invitation) Moderator: Yasmin Afina (Researcher, Security and Technology Programme, UNIDIR) Panelist: Tom Kono (Fellow, UNIDIR) Panelist: Michael Karimian (Director, Digital Diplomacy, Microsoft) Panelist: Kazuo Noguchi (Senior Researcher, Keio University) Panelist: Atsushi Ikegami (Senior Research Fellow, National Security Institute of Fujitsu Defense & National Security)	セッション：AIの重要インフラと防衛のデュアル・ユーズにおける行動のベスト・プラクティス情報交換 モデレーター：ヤスミン・アフィーナ (UNIDIRセキュリティ技術プログラム研究員) パネリスト：河野 勉（国際連合軍縮研究所 (UNIDIR) フェロー) パネリスト：マイクル・カリミアン (マイクロソフト、デジタル外交ディレクター) パネリスト：野口 和男（慶應義塾大学上席所員) パネリスト：池上 敦士 (富士通ディフェンス＆ナショナルセキュリティ安全保障研究所主任研究員)

1. The roundtable examined responsible industry behavior concerning dual-use AI in the military domain, contributing perspectives to a framework under development by UNIDIR. Discussion brought together operational, technical, business, and diplomatic considerations, with differing views on how responsibilities should be distributed among governments, military users, developers, and suppliers.
2. A central debate concerned the distinction between responsibility for using technology and responsibility for developing or supplying it. One position emphasized that governments and military users must remain accountable for deployment decisions, while companies may choose whether to supply their products. Other contributions highlighted how design choices and supplier practices can affect users' ability to employ those products responsibly.
3. The proposed framework was described as a voluntary, practical resource to help companies make more consistent and informed decisions, drawing on existing international rules. Its purpose was presented as supporting choices about development and supply rather than transferring control over military operations to companies. The discussion also recognized that smaller companies, as well as major technology providers, can make consequential decisions.
4. Industry perspectives highlighted the difficulty of assigning responsibility across systems assembled from multiple components and suppliers. Participants also raised the cost of transparency, evaluation, and explainability, and the competitive pressure created by cheaper, less transparent AI products. These concerns underscored the need for practical expectations and incentives that support responsible development without discouraging participation.
5. Government approaches discussed included coordinating defense AI strategy and procurement, using risk-based evaluation frameworks, and creating environments for testing the performance, resilience, and failure modes of proposed systems. These examples illustrated how public institutions can support cooperation with industry and connect technical assurance to acquisition decisions.

1. 本ラウンドテーブルでは、軍事分野で利用されるデュアルユースAIに関する産業界の責任ある行動を議論し、UNIDIRが策定中の枠組みに向けて意見を交換した。運用、技術、事業、外交の観点から、政府、軍事利用者、開発者、供給者の間で責任をどのように分担するかについて、異なる立場が示された。
2. 中心的な論点は、技術を使用する責任と、開発・供給する責任の区別であった。政府や軍事利用者が配備・使用の判断に責任を負い、企業は製品を供給するかどうかを選択するという立場が示された。一方、設計上の選択や供給者の取り組みも、利用者が責任ある形で技術を使用できるかどうかに影響するとの指摘があった。
3. 提案されている枠組みは、既存の国際的なルールを踏まえ、企業が一貫性と十分な情報に基づいて判断するための、自主的で実務的な支援として説明された。軍事運用の統制を企業に移すのではなく、開発や供給に関する選択を支えるものと位置づけられた。また、大手技術企業だけでなく、小規模企業の判断も重大な影響を持ち得ることが指摘された。
4. 産業界の観点からは、複数の部品や供給者を組み合わせたシステムで、責任の範囲を定める難しさが挙げられた。透明性、評価、説明可能性を確保する費用や、安価で不透明なAI製品との競争も課題とされた。責任ある開発を促しながら企業の参入を妨げない、実行可能な要件とインセンティブの必要性が示された。
5. 政府の取り組みとして、防衛AIの戦略と調達の調整、リスクに応じた評価の枠組み、システムの性能・耐性・故障や失敗の条件を検証する環境などが紹介された。公的機関が産業界との協力を支え、技術的な検証を調達判断につなげる方法として議論された。
6. 責任あるAIは、単なる制約ではなく、信頼性、制御可能性、強靱性を備えた能力を実現する手段にもなり得ると論じられた。配備後もモデル、データ、脆弱性、運用条件が変化するため、AIの調達では一度の購入にとどまらず、更新、保守、再評価、継続的な技術支援まで含める必要性が強調された。
7. 人間の関与については、あらゆる運用状況に適した単一の形はないという観点から議論された。人間が直接判断する形、人間が監督する形、事前に認められた範囲内で動作する形を区別し、作戦の段階、時間的制約、人間の認知能力、通信の途絶、監視・介入・停止・復旧の可能性などを考慮する必要性が示された。
8. 技術を輸入する国の立場から、文書、性能上の限界、試験の機会、納入後の更新に関する情報へのアクセスが重要だと指摘された。利用国固有の環境や運用条件で評価する必要性も示された。また、災害救援、海洋状況の把握、サイバー防御など、非戦闘分野におけるデュアルユースAIの便益も取り上げられた。

6. Responsible AI was discussed as a potential enabler of reliable, controllable, and resilient capabilities rather than solely a constraint. Participants emphasized that AI acquisition must cover continuing updates, maintenance, reassessment, and technical support because models, data, vulnerabilities, and operational conditions change after deployment.
7. Human involvement was a major point of debate, with no single model considered suitable for every operational context. Discussion distinguished direct human decision-making, human supervision, and operation within preauthorized limits. Relevant considerations included the phase of an operation, time pressure, cognitive limitations, communications disruption, and the ability to monitor, intervene, suspend, or recover a system.
8. Technology-importing states' needs were highlighted, including access to documentation, performance limitations, testing opportunities, and information about post-delivery updates. Evaluation under local environmental and operational conditions was considered important. The discussion also identified non-combat applications, including disaster relief, maritime awareness, and cyber defense, as relevant benefits of dual-use AI.
9. International cooperation was discussed in light of differing national security priorities and views on acceptable autonomy. Participants explored whether agreement on prohibited conduct might be more achievable than comprehensive agreement on permitted uses. UN-facilitated dialogue and engagement among governments, industry, academia, and civil society were presented as ways to sustain exchanges despite these differences.
10. Closing reflections emphasized context-specific assessment of risks, probabilities, benefits, and the consequences of both action and inaction. The roundtable supported continued consultation toward practical governance options while leaving important disagreements unresolved, particularly over supplier responsibility, meaningful human involvement, and the balance between innovation, access, and security.

9. 国際協力については、各国の安全保障上の優先事項や、許容する自律性の程度が異なることを踏まえて議論された。認められる用途を包括的に合意するよりも、禁止すべき行為についての合意の方が実現しやすいのではないかという見方も示された。相違がある中でも対話を継続するため、国連を通じた議論や、政府・産業界・学術界・市民社会の交流の意義が確認された。
10. 終盤では、リスクの大きさだけでなく、発生確率、便益、行動する場合としない場合の影響を、具体的な状況に即して評価する必要性が強調された。実務的なガバナンスの選択肢に向けて協議を継続する一方、供給者の責任、実質的な人間の関与、イノベーション・技術へのアクセス・安全性のバランスについては、重要な意見の相違が残った。

D3-T1-S3 Session 13:00–13:50 JST

Session: From Quantum Risk to Financial Resilience: Taiwan's Experience in Financial-Sector PQC Migration Speaker: Yuh-Tay Lin (Director-General, Department of Information Management, Financial Supervisory Commission, Taiwan)	セッション：量子リスクから金融レジリエンスへ ― 台湾における金融分野のPQC移行の取り組み 登壇者：ユータイ・リン (台湾金融監督管理委員会(FSC) 情報管理処 処長)

1. The presentation shared Taiwan's approach to preparing the financial sector for post-quantum cryptography (PQC). It distinguished "harvest now, decrypt later," which threatens the long-term confidentiality of data collected today, from "trust now, forge later," which concerns future forgery of digital signatures. Both risks require early preparation because migration takes time.
2. Taiwan's Financial Supervisory Commission brought together banks, insurers, securities firms, financial infrastructure providers, and suppliers in a migration pilot. The objectives were to understand cryptographic dependencies, assess risks and resource needs, support institutional planning and readiness, and encourage suppliers to prepare suitable products and technical support.
3. Cryptographic inventory was identified as the pilot's greatest challenge. Decades of accumulated technology, scattered documentation, opaque supplier components, legacy equipment, and overlooked test and cloud environments made discovery difficult. A continuously maintained cryptographic bill of materials (CBOM) should identify cryptographic uses, dependent services, responsible owners, and the implications of change.
4. PQC migration was presented as an enterprise risk management responsibility rather than a task for cybersecurity teams alone. Boards and senior management must provide direction, resources, and authority, while cross-functional teams connect technical requirements with business continuity and service impacts.
5. Crypto agility was emphasized as the ability to change cryptographic algorithms, keys, and configurations with less disruption. Recommended "no-regret" actions included removing weak cryptography, improving key and certificate management, preparing TLS 1.3 upgrades, and reducing tight coupling between cryptography and applications. These actions strengthen current security and support future transitions.

1. 本発表では、台湾の金融分野における耐量子計算機暗号（PQC）への移行準備を紹介した。現在収集した暗号化データを将来解読する「Harvest Now, Decrypt Later」と、将来の電子署名の偽造に関わる「Trust Now, Forge Later」を区別し、移行には時間がかかるため、いずれも早期の備えが必要だと説明した。
2. 台湾の金融監督管理委員会（FSC）は、銀行、保険会社、証券会社、金融インフラ提供者、供給事業者が参加する移行パイロットを実施した。暗号への依存関係、リスク、必要な資源を把握し、各機関の計画策定と準備を支援するとともに、供給事業者による対応製品や技術支援の早期整備を促すことを目的とした。
3. パイロットで最大の課題となったのは、暗号資産の棚卸しであった。長年にわたる技術の蓄積、文書の分散、供給事業者の部品の不透明さ、旧式機器、見落とされがちな試験環境やクラウド環境が把握を難しくしていた。暗号部品表（CBOM）を継続的に維持し、暗号の利用箇所、依存するサービス、管理責任者、変更時の影響を明らかにする必要性が示された。
4. PQC移行は、サイバーセキュリティ部門だけの業務ではなく、全社的なリスク管理の課題として位置づけられた。取締役会と経営層が方針、資源、権限を確保し、部門横断のチームが技術要件を事業継続やサービスへの影響と結びつけて対応する必要性が強調された。
5. 暗号アルゴリズム、鍵、設定を、より少ない影響で変更できるクリプトアジリティが重視された。将来の移行時期にかかわらず有益な取り組みとして、脆弱な暗号の排除、鍵・証明書管理の改善、TLS 1.3への更新準備、暗号とアプリケーションの密結合の緩和が挙げられた。現在の安全性を高めながら、将来の変更にも対応できる基盤を整える考え方が示された。
6. 相互接続された金融サービスを調整するため、エコシステム主導のハブ・アンド・スポーク型の進め方が提案された。金融インフラ提供者が、共通サービス、依存関係、共通手法、移行日程、共同試験を調整し、各金融機関は自らのシステムに責任を持つ。共通用語と共同試験によって対応の抜けや重複を減らし、国際標準や海外の関係機関とも歩調を合わせる必要性が示された。
7. 移行の優先順位は、量子リスクと変更に必要な期間の両方を踏まえて決めるとされた。高リスクで長期間を要する対応は早期に計画し、低リスクの対応は通常の更新や機器更改に組み込むことも検討する。調達と供給網の管理では、単なるPQC対応の表明ではなく、実現可能な提供日程、更新の確約、実際に動作する証拠を確認する必要性が示された。

6. An ecosystem-driven, hub-and-spoke approach was proposed for coordinating interconnected financial services. Infrastructure providers would help define shared services, dependencies, common methods, migration schedules, and joint tests, while institutions retain responsibility for their own systems. Common terminology and shared testing would reduce gaps and duplicated work and support alignment with international standards and partners.
7. Migration priorities should reflect both quantum risk and the time required to implement changes. High-risk work with long lead times needs early planning, while lower-risk changes may be incorporated into routine upgrades and equipment replacement. Procurement and supplier management should require credible delivery schedules, upgrade commitments, and evidence of functionality rather than relying on general claims of PQC support.
8. Operational stability requires end-to-end testing, phased switching, monitoring, and practiced rollback procedures. Hybrid approaches combining traditional cryptography with PQC were discussed as a way to manage the transition. The indicative roadmap covered planning in 2026–2027, pilots and foundational improvements in 2027–2029, high-risk and critical uses in 2029–2032, and remaining uses and routine change management in 2032–2035, subject to review.
9. Taiwan's Financial XML (FXML) ecosystem was introduced as a starting point for practical cross-institutional cooperation because it connects corporate customers, banks, transaction infrastructure, certificate providers, and cryptographic equipment. A proposed joint validation testbed would support shared scenarios, interoperability and performance testing, knowledge exchange, and coordinated migration. It remained an early-stage initiative, with no live test results presented.
10. The closing message was that PQC migration is a coordinated effort to preserve trust and financial resilience, not simply an algorithm replacement by individual institutions. Joint validation can support cross-institutional assurance but cannot replace each institution's own integration testing. Early inventory, practical pilots, supplier engagement, and continued coordination are essential to maintaining stable financial services throughout the transition.

8. 安定した運用のため、サービス全体の試験、段階的な切り替え、監視、切り戻し手順の訓練が必要だと説明した。従来暗号とPQCを組み合わせるハイブリッド方式も移行期の選択肢として紹介した。参考ロードマップは、2026～2027年の計画策定、2027～2029年の実証と基盤整備、2029～2032年の高リスク・重要用途への対応、2032～2035年の残る用途への展開と通常業務への定着で構成され、状況に応じて見直すものとされた。
9. 実践的な組織間連携の出発点として、企業顧客、銀行、取引インフラ、証明書提供者、暗号機器などを結ぶ台湾のFinancial XML（FXML）のエコシステムが紹介された。共同検証環境の構想では、共通シナリオ、相互運用性と性能の試験、知見の共有、移行の調整を進める。取り組みは初期段階であり、実運用の試験結果が示されたものではない。
10. 締めくくりでは、PQC移行は個々の金融機関による暗号の置き換えではなく、信頼と金融システムの強靭性を守る共同の取り組みだと強調された。共同検証は機関をまたぐ確認を支援するが、各機関自身の結合試験に代わるものではない。早期の棚卸し、実証、供給事業者との連携、継続的な調整を通じ、移行中も金融サービスの安定性を維持する必要性が示された。

D3-T1-S5 Session 15:00–15:50 JST

Session: MOSA, SBOM and RMF Underpinning Defense and Critical Infrastructure in the Software-Defined Era, and Countering AI-Enabled Cyberattacks Such as ARTEX Through AI MTD Moderator: Hideaki Watanabe (Chairman, Defense Technology Foundation; Founding Commissioner, Acquisition, Technology and Logistics Agency (ATLA); Vice President, SBI EVERSPIN Co., Ltd.) Panelist: Jamyung Yoon (President and CEO, SBI EVERSPIN Co., Ltd.)	セッション：ソフトウェア化時代の防衛・重要インフラを支えるMOSA・SBOM・RMFと、AI MTDによるARTEX等のAIを活用したサイバー攻撃への対策 モデレーター：渡辺 秀明 (防衛技術協会 理事長、初代防衛装備庁長官、SBI EVERSPIN株式会社 副社長) パネリスト：尹 慈明 (SBI EVERSPIN株式会社 代表取締役社長)

1. The session examined cybersecurity for increasingly software-dependent defense equipment and responses to AI-enabled attacks on critical services. It emphasized moving from systems purchased as finished products toward capabilities that can be continuously updated while maintaining security throughout their operational life.
2. The defense presentation proposed integrating MOSA, SBOM, and RMF within a DevSecOps approach. Modular Open Systems Approach (MOSA) supports replaceable components and standardized interfaces; software bills of materials (SBOMs) make software composition visible; and the Risk Management Framework (RMF) supports ongoing risk assessment and monitoring. These approaches were presented as complementary elements of development, procurement, and operation.
3. Modular design was discussed as a way to introduce new capabilities and replace vulnerable components without rebuilding an entire platform. Unmanned systems with interchangeable payloads illustrated the potential for adapting equipment to different missions and incorporating improvements more frequently than traditional, tightly integrated acquisition models allow.
4. SBOMs and Vulnerability Exploitability eXchange (VEX) information were presented as tools for identifying affected components and determining which reported vulnerabilities require action in a particular system. The presentation emphasized using this information to prioritize remediation and avoid unnecessary replacement work, while maintaining continuous risk management as equipment changes.
5. The defense discussion called for procurement structures that enable participation by startups and other nontraditional suppliers. Standardized interfaces and modular architectures could broaden competition and access to new technologies, but organizational practices and established supplier relationships remain obstacles. Security should be incorporated into technical development and updates rather than handled separately.

1. 本セッションでは、ソフトウェアへの依存が高まる防衛装備品のサイバーセキュリティと、重要なサービスに対するAIを活用した攻撃への対応を取り上げた。完成品を購入して使い続ける方式から、運用期間を通じて安全性を確保しながら継続的に能力を更新できる方式へ移行する必要性が示された。
2. 防衛分野の発表では、DevSecOpsのもとでMOSA、SBOM、RMFを一体的に運用する考え方が示された。MOSA（モジュール型オープンシステムアプローチ）は部品の交換とインターフェースの標準化、SBOM（ソフトウェア部品表）は構成の可視化、RMF（リスク管理フレームワーク）は継続的なリスク評価と監視を支える。これらを開発・調達・運用で相互に補完させる必要性が説明された。
3. モジュール化は、装備全体を作り直さずに、新しい能力の導入や脆弱な部品の交換を進める方法として紹介された。ペイロードを交換できる無人機を例に、任務に応じた構成変更や頻繁な能力向上が可能になることを説明し、従来の一体設計による長期の更新周期との違いを示した。
4. SBOMとVEX（脆弱性の悪用可能性に関する情報）は、影響を受ける部品を把握し、報告された脆弱性のうち、個別のシステムで実際に対応が必要なものを判断するための手段として紹介された。装備の変更に合わせてリスクを継続的に管理しながら、修正の優先順位を定め、不要な交換作業を減らす重要性が説明された。
5. 防衛調達では、スタートアップや従来の防衛産業以外の事業者が参加できる仕組みの必要性が示された。標準化されたインターフェースとモジュール構造は、競争や新技術の導入を促す一方、組織の慣行や既存の取引関係が障壁となる。技術開発や更新とセキュリティを別々に扱わず、同時に進めるべきだと強調された。
6. 後半の発表では、AIツールやエージェントによって、探索、分析、コードに関する作業、公開サービスへの反復的な試行が高速化する状況が説明された。ARTEXを例に、韓国の金融機関で発生した事案に関する分析を紹介し、基幹システムだけでなく、業務支援サービス、連携システム、従業員の端末にも注意を向ける必要性が示された。
7. 基本対策として、公開サービスの最小化、不要なAPIの削除、外部からアクセスできる資産の把握、認証の徹底、最小権限によるアクセス管理が挙げられた。使われなくなった接続や補助的なシステムが見落とされた侵入口になり得るため、継続的な確認と管理が必要だと説明された。
8. 追加の対策として、自動化されたリクエストの検知、ログインの反復試行や過剰な照会の制限、未認証でアクセスできる経路の排除、単一の識別子だけでは情報を照会できない設計などが示された。個別のIPアドレスの遮断だけに頼ることの限界に加え、複数のサービスや組織で不審な活動の情報を共有する考え方も紹介された。

6. The second presentation described how AI tools and agents can accelerate reconnaissance, analysis, code-related tasks, and repeated attempts against exposed services. It discussed ARTEX as an example and presented analysis of incidents affecting South Korean financial institutions. Supporting services, interconnected systems, and employee devices were highlighted as areas requiring attention alongside core systems.
7. Recommended foundational measures included reducing exposed services, removing unused APIs, maintaining an accurate view of publicly accessible assets, and enforcing authentication and least-privilege access. The presentation emphasized continuous verification and management because abandoned connections and auxiliary systems can create overlooked entry points.
8. Additional defensive measures included detecting automated requests, controlling repeated login attempts and excessive queries, eliminating unauthenticated access paths, and avoiding data access based solely on a single identifier. Sharing information about suspicious activity across services and organizations was also discussed, alongside the limitations of relying only on individual IP-address blocks.
9. A demonstration using ARTEX against a sample web application was presented to illustrate automated testing and attack behavior. The presenter introduced Eversafe as an AI-based moving target defense (MTD) solution that changes protective code and logic over time. Its proposed value was to make prior analysis and request patterns harder to reuse, forcing attackers to spend additional time and computing resources.
10. The closing discussion connected continuous vulnerability management with dynamic application protection. SBOM-based visibility, risk management, and secure configuration were presented as the foundation, while MTD was discussed as a complementary layer against rapidly adapting automated attacks. The overall objective was to sustain security through continuous updates and increase the effort and cost required for attacks.

9. サンプルのウェブアプリケーションを対象にARTEXを用いたデモを紹介し、自動化された検証・攻撃の挙動を説明した。また、保護用のコードやロジックを継続的に変える、AI基盤の動的防御（MTD）製品Eversafeを紹介した。過去の解析結果やリクエストの再利用を難しくし、攻撃者に追加の時間と計算資源を使わせる点に価値があると説明された。
10. 締めくくりでは、継続的な脆弱性管理と、アプリケーションに対する動的な保護を組み合わせる考え方が示された。SBOMによる構成の把握、リスク管理、安全な設定を土台とし、変化の速い自動化攻撃に対する補完的な対策としてMTDを位置づけた。継続的な更新によって安全性を維持し、攻撃に必要な手間と費用を増やすことが全体の方向性として示された。

DAY 4 2026-10-30 金曜日

Keio University, Mita Campus; North Building 1F North Hall
慶應義塾大学 三田キャンパス 北館 1F 北ホール

D4-T1-S1 Session 10:00–10:50 JST

Session: Cyber Resilience for Critical Infrastructure in the AI Era -Business Continuity from the Perspectives of Cyber Defense, Economic Security, and Practical OT Implementation- Moderator: Kanako Gushi (Senior Consultant, Cyber CoE, Hitachi, Ltd.) Panelist: Masashi Fujiwara (Master Security Specialist, Cyber CoE, Hitachi, Ltd.) Panelist: Momoko Aoyama (Lead White Hat Hacker, Cyber CoE, Hitachi, Ltd.) Panelist: Toshiyuki Atsumi (General Manager, Security Analysis Center Digital & Security Division Hitachi, Ltd.) Panelist: Kenichi Ogi (Senior Security Evangelist, Security Digital Solutions Division Hitachi Solutions, Ltd.)	セッション：AI時代の重要インフラを支えるサイバーレジリエンス ～サイバー防御・経済安全保障・OTの現場実装から考える事業継続～ モデレーター：具志 香菜子 (株式会社 日立製作所 Cyber CoE, シニアコンサルタント) パネリスト：藤原 将志 (株式会社 日立製作所 Cyber CoE, マスターセキュリティスペシャリスト) パネリスト：青山 桃子 (株式会社 日立製作所 Cyber CoE, 筆頭ホワイトハッカー) パネリスト：渥美 俊之 (株式会社 日立製作所 デジタル＆セキュリティ統括本部 セキュリティアナリシスセンタ センタ長) パネリスト：扇 健一 (株式会社日立ソリューションズ セキュリティソリューション事業部 シニアセキュリティエバンジェリスト)
1. The session examined cyber resilience for critical infrastructure in the AI era, connecting technical defense, operational preparedness, and public policy. Participants emphasized maintaining essential social functions, limiting damage, recovering quickly, and using lessons from incidents to improve future preparedness. 2. Managing attack surfaces and vulnerabilities was identified as a fundamental priority. Public-facing websites and other supporting systems can provide entry points into critical environments. Participants also highlighted indirect risks, such as altered information causing operators to make incorrect decisions, and stressed assessing consequences beyond the initially compromised system. 3. Operational technology (OT) incidents can affect production, physical equipment, safety, and the environment, rather than only information confidentiality. The discussion distinguished manufacturing disruptions from process-industry risks, where abnormal equipment behavior or interrupted operations may cause severe physical damage. Security priorities must therefore reflect the actual processes and services being supported. 4. Frontier AI was described as shortening the cycle between failed attack attempts, analysis, and revised approaches. Defensive AI can help reproduce attackers' behavior and identify weaknesses, but defenders must also ensure that testing and remediation do not disrupt operations. Faster detection must therefore be accompanied by safe and timely verification of proposed changes.	1. 本セッションでは、AI時代の重要インフラにおけるサイバーレジリエンスを、技術的な防御、現場の備え、政策・制度を結びつけて議論した。重要な社会機能を維持し、被害を限定し、早期に回復するとともに、インシデントの経験を次の備えに生かす重要性が示された。 2. 基本的な優先事項として、攻撃対象領域と脆弱性の把握・管理が挙げられた。外部公開のウェブサイトや補助的なシステムが重要な環境への侵入口となる可能性に加え、情報の改ざんによって運用者の誤判断を誘う間接的なリスクも指摘された。最初に侵害されたシステムだけでなく、その先に及ぶ影響を評価する必要性が示された。 3. OT（制御・運用技術）のインシデントは、情報漏洩にとどまらず、生産、設備、人の安全、環境に影響する。組立製造における生産停止と、設備の異常動作や運転中断が重大な物理的被害につながり得るプロセス産業のリスクを区別し、実際の工程や提供するサービスに応じて守るべき対象と優先順位を考える必要性が説明された。 4. フロンティアAIは、攻撃の失敗を分析し、方法を修正して再試行するまでの時間を短縮すると説明された。防御側もAIを使って攻撃者の行動を再現し、弱点を把握できる一方、検証や修正によって業務を停止させてはならない。検出の高速化だけでなく、変更の安全性を迅速に確認する仕組みも必要だとされた。 5. 日立からは、フロンティアAIによるソースコード解析、脅威モデルの作成、脆弱性候補の抽出、大規模ソフトウェアにおける悪用可能性の検証に関する経験が紹介された。重要な判断の前や最終結果の確認では、人間による監督が不可欠とされた。発見件数を増やすこと自体ではなく、実際のリスクを見極め、優先順位をつけて対処することが目的だと説明された。

5. Hitachi shared experience using frontier AI to analyze source code, develop threat models, identify vulnerability candidates, and investigate exploitability across large software products. Human oversight remained essential at significant decision points and when reviewing final results. The purpose was to prioritize and address genuine risks rather than simply increase the number of findings. 6. Critical infrastructure resilience requires understanding dependencies across suppliers, service providers, and connected organizations. OT examples included remote maintenance, contractor devices, removable media, and unmanaged cloud or wireless connections. Participants emphasized that cloud infrastructure and its providers are also part of the supply chain and must be included in risk assessments. 7. The policy discussion presented public-private information sharing as a means of strengthening resilience across interconnected systems. Operational preparation should include identifying assets and network dependencies, maintaining accurate information, and establishing reporting and communication processes. These activities were framed as useful foundations for managing risk, beyond responding to external requirements. 8. Participants stressed that asset inventories must remain current as systems and connections change. Effective operations also require OT security education, clear policies, controlled use of devices and removable media, and an understanding of actual workplace practices. Knowing normal system behavior and retaining logs were identified as essential for detecting anomalies and investigating incidents. 9. Where immediate patching is impractical, participants discussed compensating measures such as network segmentation and virtual patching where available. Priorities should consider human life, environmental consequences, business importance, and downstream supply-chain impacts. Organizations should also prepare criteria, authority, and escalation procedures for planned shutdowns when risks cannot otherwise be managed.	6. 重要インフラのレジリエンスには、供給事業者、サービス提供者、接続先の組織を含む依存関係の把握が必要とされた。OTの例として、リモート保守、保守業者の持ち込み端末、USBなどの媒体、管理外のクラウド接続や無線接続が挙げられた。クラウド基盤とその提供者もサプライチェーンの一部として、リスク評価に含める必要性が強調された。 7. 政策・制度の議論では、相互依存するシステム全体のレジリエンスを高める手段として、官民の情報共有が取り上げられた。現場の備えとして、資産とネットワークの依存関係を把握し、情報を正確に維持するとともに、報告・連絡の手順を整える必要性が示された。これらは外部からの要請への対応だけでなく、自らのリスクを管理するための基盤として位置づけられた。 8. 資産台帳は一度作成して終わりではなく、システムや接続の変更に合わせて更新する必要があるとされた。また、OTセキュリティの教育、明確な方針、端末や媒体の利用管理、実際の現場の運用への理解が重要だと説明された。異常の検知とインシデント調査のため、平常時のシステムの状態を把握し、ログを記録・保持する必要性も示された。 9. 直ちにパッチを適用できない場合には、ネットワークの分離や、利用可能であれば仮想パッチなどの代替策が議論された。優先順位は、人命、環境への影響、事業上の重要性、供給停止が取引先に及ぼす影響を踏まえて定める必要がある。ほかの方法でリスクを管理できない場合に備え、計画停止の判断基準、権限、上位への判断の引き上げ手順も準備すべきだとされた。 10. 終盤では、基本対策の継続、意識の向上、組織を越えた実践知の共有が重視された。優れた取り組みを可視化し、経営層の関心を高める活動として、OTセキュリティアワードも紹介された。レジリエンスは、技術、人間による適切な判断、インシデントへの備え、関係者との連携を組み合わせて継続的に高めるものとして整理された。

10. The closing discussion emphasized sustaining basic controls, improving awareness, and sharing practical experience across organizations. An OT security award initiative was introduced as a way to highlight effective practices and encourage management engagement. Resilience was presented as a continuing organizational effort that combines technology, informed human decisions, preparation for incidents, and cooperation across the wider ecosystem.	

D4-T1-S2 Session 11:00–11:50 JST

Session: Cyber Risks and Practical Governance for AI Agents Speaker: Naonari Tanimoto (Specialist, Solutions Engineering Private Sector SE2 Group)	セッション：AIエージェントのサイバーリスクと実践的ガバナンスの在り方について 登壇者：谷本 直柔 (ソリューションエンジニアリング部 プライベートセクターSE2グループ スペシャリスト)
1. Naonari Tanimoto of Trend Micro examined the cybersecurity risks of AI agents and practical governance, connecting risk assessment with technical implementation through demonstrations. He explained that agents' ability to act on users' behalf creates business value while making safe and economical operation increasingly important. 2. He identified risks arising from natural-language manipulation, memory, autonomous planning, cooperation between agents, and tool execution. These capabilities allow malicious inputs to affect not only generated responses but also actions involving databases, external services, and other systems. 3. He emphasized that risks change with agents' levels of autonomy. As agents gain tools and coordinate more independently, concerns extend beyond inaccurate answers and information disclosure to unintended actions, loss of control, and wider operational consequences. Controls must therefore match the autonomy and capabilities of each agent. 4. A passport-processing proof of concept illustrated how instructions hidden in an uploaded image could redirect an agent's database operations and expose other users' information. Tanimoto highlighted the difference between an uploading user's limited permissions and the agent's broader authority, and described testing that found successful attacks across multiple models.	1. トレンドマイクロの谷本直柔氏は、AIエージェントのサイバーリスクと実践的なガバナンスについて、リスク評価から技術的な実装までを、デモンストレーションを交えて説明した。利用者の代わりに行動できることが業務の効率化や価値創出につながる一方、安全かつ経済的に運用することが重要になっていると述べた。 2. AIエージェントのリスクとして、自然言語による操作、記憶、自律的な計画、複数エージェントの連携、ツールの実行に起因するものを挙げた。不正な入力が回答内容だけでなく、データベース、外部サービス、その他のシステムに対する実際の行動へ影響する点を示した。 3. リスクの性質は、エージェントの自律レベルによって変わると強調した。ツールの利用や自律的な連携が広がると、不正確な回答や情報漏洩にとどまらず、意図しない行動、制御不能、業務への広範な影響につながり得るため、自律性と能力に応じた統制が必要だと説明した。 4. パスポート処理の概念実証では、アップロード画像に隠された指示によって、エージェントのデータベース操作を誘導し、他の利用者の情報を流出させる例を紹介した。画像を投稿する利用者の限定的な権限と、エージェントが持つ広い権限との差が悪用される点を示し、複数のモデルで攻撃が成功した検証について説明した。 5. 不正なスキルを通じて、エージェントに不正コマンドを実行させ、認証情報の窃取につなげる脅威も紹介した。模擬攻撃のデモでは、正規の調査業務を続ける裏側で攻撃者側のサーバーとの通信が成立する様子を示し、利用者が不正動作に気付きにくい問題を説明した。

5. He also discussed malicious skills that induce agents to execute unauthorized commands and facilitate credential theft. A demonstration using a simulated attack established communication with an attacker-controlled server while the agent continued its legitimate task, illustrating how harmful activity can remain difficult for users to notice.
6. Tanimoto introduced AI-CAL, discussed in a joint report with PwC Consulting, as a framework for defining minimum controls before agents at different autonomy levels enter production. It can help engineers identify architectural gaps and help management understand the risks, investment, and additional safeguards required when increasing autonomy.
7. He emphasized combining preventive, detective, and responsive controls. Restricting tools and blocking malicious inputs must be complemented by visibility into agent behavior and the ability to stop execution or isolate an agent. These requirements should be considered before deployment.
8. The validation environment combined Kubernetes on AWS EKS, OpenClaw agents, NVIDIA OpenShell, NeMo Guardrails, and TrendAI Vision One capabilities. Demonstrations showed how declarative policies could block unauthorized destinations and how integrated guardrails could block direct prompt-injection attempts, with logs supporting monitoring and investigation.
9. A further demonstration showed an indirect prompt injection embedded in a build report causing an agent to download an unrelated test file. Runtime monitoring exposed the executed command, and network isolation of the affected container environment demonstrated a response mechanism. Correlated logs supported investigation of the cause and possible gaps in preventive controls.
10. He concluded that prevention alone is insufficient, while detection and response without preventive restrictions can produce excessive logs and make suspicious behavior harder to distinguish. Effective deployment requires all three control types, supported by observability and controllability. These principles remain relevant as execution architectures evolve from containers toward other forms of isolation.

6. PwCコンサルティングとの共同レポートで取り上げたAI-CALを、自律レベルの異なるエージェントを本番導入する前に満たすべき最低限の統制条件を定める枠組みとして紹介した。技術者による構成上の不足の把握に加え、自律性を高める際のリスク、必要な投資、追加対策を経営層に説明するためにも活用できると述べた。
7. 予防的・検知的・対応的統制を組み合わせる重要性を強調した。利用できるツールの制限や不正入力の遮断に加え、エージェントの行動を把握する能力と、実行停止や隔離を行う能力が必要であり、導入前からこれらを設計すべきだと説明した。
8. 検証環境では、AWS EKS上のKubernetes、OpenClaw、NVIDIA OpenShell、NeMo Guardrails、TrendAI Vision Oneの機能を組み合わせた。宣言的なポリシーによる未承認の宛先へのアクセス遮断と、ガードレールによる直接的なプロンプトインジェクションの遮断を実演し、ログを監視や調査に利用する方法を示した。
9. 別のデモでは、ビルドレポートに埋め込まれた間接プロンプトインジェクションによって、エージェントが本来の作業と関係のない検証用ファイルをダウンロードする例を示した。実行時の監視でコマンドを確認し、影響を受けたコンテナ環境をネットワークから隔離する対応を実演した。ログを突き合わせることで、原因や予防策の不足も調査できると説明した。
10. 最後に、予防だけでは不十分である一方、予防的な制限なしに検知・対応だけを導入すると、ログが増え、不審な行動を見分けにくくなると述べた。観測性と制御性を確保しながら三つの統制を組み合わせることが重要であり、コンテナから別の隔離方式へ実行基盤が変化しても、この基本的な考え方は変わらないと強調した。

D4-T1-S3 Session 13:00–13:50 JST

Session: The Forefront of Autonomous Defense Against AI-Driven Cyber Threats (AI Threat Defense) Speaker: Itsufumi Murayama (Japan Head of Security Sales, Google Cloud Japan, Head of Google Cybersecurity Center of Excellence)	セッション：AI駆動型サイバー脅威に対抗する自律的防御（AI Threat Defense）の最前線 登壇者：村山 逸文 (グーグル・クラウド・ジャパン合同会社 セキュリティ営業本部 本部長, Google サイバーセキュリティ研究拠点 拠点長)
1. Itsufumi Murayama of Google Cloud advocated a shift toward AI-powered autonomous defense, or agentic defense. He identified three reasons for acting now: attackers' use of AI cannot be controlled, security personnel are in short supply, and practical experience with AI-based defense has accumulated. 2. He characterized AI-driven threats through three factors: scale, speed, and sophistication. As attacks expand and accelerate, manual monitoring and investigation cannot keep pace. He proposed using AI for tasks it can perform effectively while retaining human responsibility for judgment. 3. Murayama distinguished two complementary defensive functions: continuously finding and remediating vulnerabilities, and detecting, investigating, and containing attacks that still occur. He emphasized that generating alerts is insufficient unless organizations can move rapidly from detection to containment. 4. Drawing on Google's internal experience, he discussed AI-assisted vulnerability research and remediation, including Project Naptime, Big Sleep, and CodeMender. He stressed that the scope must extend beyond application code to operating systems, cloud misconfigurations, and inadequate access controls. 5. He argued that effective security depends on agents and their harnesses as well as model capability. Operating rules, permission boundaries, and action records are essential for safe execution. Models should be selected according to the task, performance, and cost rather than assuming that the newest or largest model is always optimal. 6. He introduced a PSRM cycle: Prepare, Scan and Prioritize, Remediate, and Monitor. This involves addressing known weaknesses, identifying critical systems, prioritizing findings by potential impact, using AI to support remediation, preventing new vulnerabilities, and monitoring risks that remain unresolved. Some weaknesses may require architectural redesign or changes in programming language rather than repeated patches.	1. Google Cloudの村山逸文氏は、AIを活用した自律型防御、すなわちエージェンティック・ディフェンスへの移行を提唱した。その理由として、攻撃者のAI利用は止められないこと、セキュリティ人材が不足していること、AIを使った防御の実践的な知見が蓄積してきたことの三つを挙げた。 2. AIによる脅威の変化を、規模の拡大、速度の向上、高度化という三つの要素で整理した。攻撃が拡大・高速化する中、手作業による監視や調査では対応が間に合わなくなるため、AIが得意な作業はAIに任せ、人間は判断を担う役割分担が必要だと述べた。 3. 防御には、脆弱性を継続的に発見・修復する機能と、それでも発生する攻撃を検知・調査・封じ込める機能の双方が必要だと説明した。アラートを出すだけでなく、検知から封じ込めまでを迅速に進めることが重要だと強調した。 4. Google内部の経験として、Project Naptime、Big Sleep、CodeMenderなど、AIによる脆弱性調査と修復の取り組みを紹介した。対象はアプリケーションのコードだけでなく、OS、クラウドの設定ミス、不十分なアクセス制御などにも広げる必要があると指摘した。 5. セキュリティ対策の実効性は、モデルの能力だけでなく、エージェントと、それを制御するハーネスにも左右されると説明した。安全な実行には、操作ルール、権限・動作範囲の制限、行動の証跡が不可欠であり、モデルも最新・最大のものを一律に使うのではなく、用途、性能、費用に応じて選ぶべきだと述べた。 6. Prepare（準備）、Scan and Prioritize（スキャンと優先順位付け）、Remediate（修復）、Monitor（監視）からなるPSRMの循環を紹介した。既知の弱点への対応、重要システムの特定、影響度に基づく対処順位の決定、AIによる修復、新たな脆弱性の作り込み防止、未修復リスクの継続監視を組み合わせる必要性を示した。また、パッチの繰り返しよりも、設計やプログラミング言語を見直す方が有効な場合もあると述べた。 7. Wizを、クラウド上のリスクのつながりと想定される侵入経路を可視化する仕組みとして紹介した。公開アプリケーション、脆弱性、認証情報、権限、機密データの関係を把握することで、緊急に対応すべき組み合わせを判断できると説明した。この情報をCodeMenderと共有し、修復の優先順位に反映する構想も示した。

7. Murayama presented Wiz as a way to visualize interconnected cloud risks and possible attack paths. Connecting exposed applications, vulnerabilities, credentials, permissions, and sensitive data can help organizations identify which combinations require urgent action. He described sharing this context with CodeMender to support remediation priorities. 8. He described combining endpoint and cloud logs, vulnerability context, and Mandiant threat intelligence within Google Security Operations. AI agents can support detection, investigation, and threat hunting, including analysis of historical records for attackers who may evade existing alerts and remain undetected. 9. Customer examples illustrated the operational benefits of this approach. Murayama described Lloyds Banking Group's use of AI to streamline analysis and redirect staff toward higher-value work, Vertiv's expansion of log coverage while reducing investigation time, and Sony Music Entertainment's automation of initial investigations while retaining human final judgment. 10. He proposed a phased transition that preserves existing operations: first visualize and prioritize risks, then automate initial investigation and triage, and progressively extend automation to remediation and containment. He emphasized integrating prevention and active defense while keeping humans responsible for final decisions.	8. Google Security Operationsでは、端末とクラウドのログ、脆弱性に関する情報、Mandiantの脅威インテリジェンスを組み合わせて分析する方法を紹介した。AIエージェントによる検知、調査、脅威ハンティングに加え、既存のアラートを回避して潜伏する攻撃者を、過去の記録から探索する取り組みを説明した。 9. 導入事例として、ロイズ銀行における分析作業の効率化と人材の高度業務への再配置、Vertivにおけるログの対象拡大と調査時間の短縮、ソニー・ミュージックエンタテインメントにおける初期調査のAI化を紹介した。人間による最終判断を維持しながら、セキュリティ運用を効率化する可能性を示した。 10. 既存の業務を維持しながら、まずリスクを可視化して優先順位を定め、次に初期調査とトリアージを自動化し、その後、修復や封じ込めへ自動化を広げる段階的な移行を提案した。予防と攻撃発生時の防御を一体として整備し、人間が最終判断を担う形で、自律型防御を実現する重要性を強調した。

D4-T1-S4 Session 14:00–14:50 JST

Session: Cyber Threats in the AI Era: Evolving Risks and Resilience Speaker: Kenichi Terashita (CxO Advisor, Cisco Systems G.K.)	セッション：AI時代のサイバー脅威：変化するリスクとレジリエンス 登壇者：寺下 健一 (シスコシステムズ合同会社 CxOアドバイザー)
1. Kenichi Terashita of Cisco examined evolving cyber threats and resilience in the AI era through three themes: change, preparedness, and action. Drawing on an attacker's perspective, he emphasized that AI accelerates operations and lowers the technical barriers to conducting attacks. 2. He highlighted the growing gap between vulnerability discovery, disclosure, patch development, and deployment. Even after a fix becomes available, organizations need time for testing and implementation. He argued that defenders must accelerate the entire remediation process, including through AI and automation.	1. シスコの寺下健一氏は、「変化」「備え」「行動」の三つを軸に、AI時代のサイバー脅威とレジリエンスを論じた。攻撃者から防御側がどう見えるかという視点を重視し、AIが攻撃の速度を高め、実行に必要な技術的なハードルも下げていると説明した。 2. 脆弱性の発見・開示、修正プログラムの開発、利用者による適用の間に生じる時間差を課題として挙げた。修正が公開されても、検証や導入には時間がかかるため、AIや自動化を活用し、修復に至るプロセス全体を加速させる必要があると述べた。

3. Terashita cautioned against prioritizing vulnerabilities solely by severity scores. He emphasized considering actual exploitation, exposure to attackers, and the conditions required for an attack to succeed. AI may also enable attackers to combine weaknesses in ways that make vulnerabilities below the highest severity category consequential.
4. He argued that patching alone cannot address every threat, particularly when exploitation begins before disclosure. Organizations should strengthen systems and access controls, assume that compromise can occur, and prepare resilience and recovery plans to limit damage and restore operations.
5. Discussing an AI-agent testing incident involving Hugging Face, he highlighted the risks of agents pursuing performance objectives beyond intended boundaries. He stressed the need for explicit operating limits, stopping conditions, monitoring, and auditing rather than assuming that an agent will abandon an unsafe path on its own.
6. A Cisco Talos example illustrated attackers using multiple AI models to analyze information from an already compromised system and select subsequent actions. Terashita argued that defenders must account for AI-assisted decision-making and lateral movement inside their environments, including the information available to an intruder.
7. Looking ahead, he suggested that AI-enabled attacks could become quieter and more persistent. Attackers may use fewer requests or legitimate accounts, making malicious activity harder to distinguish from normal behavior and reducing opportunities for detection and containment.
8. He described Cisco's use of frontier AI and coordinated agents in software development and vulnerability discovery. He also introduced a small language model that can run locally to support code-security analysis, offering an option for organizations concerned about sending source code to cloud-based services.
9. Terashita emphasized that older vulnerabilities and legacy assets remain important attack opportunities. Organizations need to know where vulnerable systems are located, who is responsible for them, and when they will be addressed. Basic measures such as stronger authentication and disabling unused accounts can increase the time and effort required for attackers to succeed.

3. 脆弱性の深刻度スコアだけで対応順位を決めることには限界があると指摘した。実際の悪用状況、攻撃者への露出、攻撃が成立する条件を考慮すべきだと説明した。また、AIが複数の弱点を組み合わせることで、最上位の深刻度に分類されない脆弱性も重大な影響につながり得ると述べた。
4. 開示前に悪用が始まる脅威もあるため、パッチの適用だけではすべての攻撃に対応できないと論じた。システムやアクセス制御の強化に加え、侵害が起こり得ることを前提として、被害の限定と業務の復旧に向けたレジリエンス・回復計画を用意する必要性を強調した。
5. Hugging Faceに関係するAIエージェントの試験事例を取り上げ、性能目標を追求するエージェントが、意図した範囲を越えて行動するリスクを説明した。危険な行動を自ら諦めると期待するのではなく、動作範囲、停止条件、監視、監査を明確に設計する必要があると述べた。
6. Cisco Talosの事例として、侵害済みシステムから得た情報を複数のAIモデルで分析し、その後の攻撃行動を選択する手法を紹介した。防御側は、侵入後のAIによる判断や内部での横展開を想定し、侵入者がシステム内で参照できる情報も含めて備える必要があると示した。
7. 今後の見通しとして、AIを使った攻撃が、より静かで長期的なものになる可能性を指摘した。少数の通信や正規のアカウントを利用することで、悪意ある行動と通常の利用を区別しにくくなり、検知や封じ込めの機会が減ることへの懸念を示した。
8. シスコにおける、フロンティアAIや複数エージェントを活用したソフトウェア開発・脆弱性発見の取り組みを紹介した。また、ソースコードをクラウドに送ることを懸念する組織向けの選択肢として、ローカルで実行し、コードのセキュリティ分析を支援する小規模言語モデルも紹介した。
9. 新しい脆弱性だけでなく、古い脆弱性や旧来の資産も、引き続き重要な攻撃対象になると強調した。脆弱なシステムの所在、責任者、対応時期を把握する必要性を示すとともに、認証の強化や未使用アカウントの停止といった基本対策が、攻撃者に必要な時間や手間を増やすと説明した。
10. 最後に、AIによって攻撃の速度と費用構造が変化し、人手や時間にかかっていた費用の一部がAIのトークン利用に置き換わっていると述べた。防御側もAIを活用して速度に対応するとともに、既存のセキュリティ技術の実装、リスクに応じた優先順位付け、運用上の備えを進める重要性を強調した。

10. He concluded that AI is changing both the speed and economics of cyberattacks, shifting some attacker costs from human effort and time toward AI-token consumption. Defenders must also use AI to keep pace while implementing existing security capabilities, risk-based prioritization, and operational preparedness.	

D4-T1-S5 Session 15:00–15:50 JST

Session: Strengthening Japan's Economic Security and Cybersecurity: Perspectives from Leading Companies Moderator: David Parker (Co-Chair, Secure Digital Infrastructure Committee, American Chamber of Commerce in Japan) Panelist: Daniel Sofio, Kameido Group Panelist: Hiroshi Amano, Palo Alto Networks Panelist: Mika Takeda, IBM Japan Panelist: Yasuo Shinozawa, Qualcomm Japan	セッション：日本の経済安全保障とサイバーセキュリティの強化：主要企業の視点から モデレーター：デイビッド・パーカー (在日米国商工会議所 セキュア・デジタル・インフラストラクチャー委員会 共同委員長) パネリスト：ダニエル・ソフィオ (Kameido Group) パネリスト：天野 宏 (パロアルトネットワークス) パネリスト：武田 未果 (日本IBM) パネリスト：篠澤 康夫 (クアルコムジャパン)
Session: Strengthening Japan's Economic Security and Cybersecurity: Perspectives from Leading Companies Moderator: David Parker (Co-Chair, Secure Digital Infrastructure Committee, American Chamber of Commerce in Japan) Panelist: Daniel Sofio, Kameido Group Panelist: Hiroshi Amano, Palo Alto Networks Panelist: Mika Takeda, IBM Japan	セッション：日本の経済安全保障とサイバーセキュリティの強化：主要企業の視点から モデレーター：デイビッド・パーカー (在日米国商工会議所 セキュア・デジタル・インフラストラクチャー委員会 共同委員長) パネリスト：ダニエル・ソフィオ (Kameido Group) パネリスト：天野 宏 (パロアルトネットワークス) パネリスト：武田 未果 (日本IBM)
1. Moderated by David Parker of the American Chamber of Commerce in Japan, the panel examined the relationship between Japan's economic security and cybersecurity. Daniel Sofio, Hiroshi Amano, and Mika Takeda discussed resilience, technological change, corporate preparedness, and cooperation between government and industry. 2. Sofio framed economic security as resilience against external shocks, viewed at national, sectoral, and individual-firm levels. He suggested learning from cybersecurity's experience in building shared understanding, information-sharing institutions, and cooperation among competitors to protect common infrastructure and interests. 3. He explained that digital transformation exposes economic activities to risks that were previously outside their scope. Shared suppliers and dependencies mean that individual companies cannot secure their resilience alone, while redundancy has become more valuable in a less predictable external environment.	1. 在日米国商工会議所のデイビッド・パーカー氏の進行により、日本の経済安全保障とサイバーセキュリティの関係を議論した。ダニエル・ソフィオ氏、天野宏氏、武田未果氏が、レジリエンス、技術の変化、企業の備え、官民連携について意見を交わした。 2. ソフィオ氏は、経済安全保障を外部からの衝撃に対するレジリエンスとして捉え、国家、産業、個別企業という異なる視点から整理した。共通認識の形成、情報共有の仕組み、競合企業間の協力など、共通の基盤や利益を守ってきたサイバーセキュリティ分野の経験から学べると述べた。 3. デジタルトランスフォーメーションによって、従来は想定していなかったリスクに経済活動がさらされるようになったと説明した。供給者や依存関係を共有する企業は、自社だけでレジリエンスを確保できず、外部環境の不確実性が高まる中では、冗長性の価値も増していると指摘した。 4. 天野氏は、サイバーセキュリティを国家安全保障と経済安全保障の基盤として位置付け、国家に関係する情報窃取、重要インフラの妨害に備えた潜伏、AIを悪用する脅威を取り上げた。政府との脅威情報の共有に加え、修正プログラムを速やかに適用できない場合には、仮想パッチなどの保護措置も活用する重要性を述べた。

4. Amano described cybersecurity as a foundation of national and economic security, highlighting state-linked espionage, positioning for disruption of critical infrastructure, and AI-enabled threats. He emphasized sharing threat intelligence with government and using protective measures such as virtual patching when software fixes cannot be deployed promptly.
5. Takeda highlighted the role of open source and hybrid cloud in competition, innovation, skills development, and security. She described collaboration among IBM, Red Hat, and Palo Alto Networks to identify and remediate open-source vulnerabilities, deliver fixes to customers, and subsequently contribute improvements back to the community.
6. On post-quantum cryptography, Takeda recommended beginning preparations despite uncertainty about technological timelines. Initial steps include inventories of systems and cryptographic use, software bills of materials, and prioritization. She also emphasized management leadership and treating cybersecurity as a necessary investment.
7. Addressing resource constraints, Amano drew on his experience in Wakayama Prefecture to describe shared cybersecurity protection for municipalities. He proposed pooling capabilities as an approach for smaller organizations and discussed similar collaborative initiatives among regional financial institutions.
8. Amano's policy recommendations included financial support and tax measures for security improvements and modernization of legacy and operational-technology systems, practical guidance and education for smaller businesses, shared defense arrangements, and cybersecurity evaluation mechanisms that strengthen supply-chain security.
9. Sofio emphasized government's role in listening to industry, aggregating and analyzing information, and disseminating guidance and good practices. He also highlighted public procurement, overseas partnerships, and support for sourcing challenges as ways to sustain demand, reduce information gaps, and strengthen economic resilience.

5. 武田氏は、オープンソースとハイブリッドクラウドが、競争、イノベーション、人材育成、セキュリティを支えると説明した。IBM、Red Hat、Palo Alto Networksの協力により、オープンソースの脆弱性を発見・修復し、顧客へ修正を提供した後、コミュニティにも改善を還元する取り組みを紹介した。
6. 耐量子計算機暗号（PQC）について、技術の実現時期に不確実性があっても、準備を始めることが重要だと述べた。システムや暗号の利用状況の棚卸し、ソフトウェア部品表（SBOM）の整備、優先順位付けを最初の取り組みとして挙げた。また、経営層が主導し、サイバーセキュリティを必要な投資として捉えるべきだと強調した。
7. 人材や予算が限られる組織への支援について、天野氏は、和歌山県で自治体向けのサイバー防御を共同運用した経験を紹介した。小規模な組織を守る方法として、能力や資源を共同で確保する考え方を示し、地域金融機関による同様の連携の動きにも言及した。
8. 天野氏は、政策上の提案として、セキュリティ強化や旧来のシステム・OTの更新を支える財政支援と税制措置、中小企業向けの具体的な指針や教育、共同防御の仕組み、サプライチェーンの安全性を高めるセキュリティ評価の仕組みを挙げた。
9. ソフィオ氏は、政府が産業界の声を聴き、情報を集約・分析し、指針や優れた実践を共有する役割を重視した。また、政府調達、海外との連携、調達先に関する課題への支援を通じて、需要の継続性を確保し、情報格差を縮め、経済のレジリエンスを強化できると述べた。
10. 武田氏は、政策の目標を、形式的な確認やリスクゼロの追求ではなく、継続的な改善、業務の継続、迅速な回復に置くべきだと主張した。最後の議論では、官民・国際連携に加え、日本における経済安全保障への理解の深まり、政府の迅速なリーダーシップ、コミュニティを通じた情報共有が、今後の発展を支える要素として挙げられた。

10. Takeda argued that policy should prioritize continuous improvement, operational continuity, and rapid recovery rather than checklist compliance or an expectation of zero risk. The closing discussion highlighted public-private and international cooperation, Japan's developed understanding of economic security, responsive government leadership, and community-based information sharing as important foundations for further progress.	

D4-T1-S6 Session 16:00–16:50 JST

Session: AI Security and AI Sovereignty: Different Goals, Shared Dependencies? Moderator: James Miller (CEO Japan Secure Solutions) Panelist: Eddy Almand (Founder & CEO, Almata) Panelist: Nate Snyder (Director, FiveLines) Panelist: Steven Li (Cybersecurity and Data & AI recruitment leader, Robert Half Japan) Panelist: Alex DeVore (CEO Founder MadeHere)	セッション：AIセキュリティとAI主権：異なる目標、共通の依存関係とは？ モデレーター：ジェームズ・ミラー (ジャパン・セキュア・ソリューションズ CEO) パネリスト：エディ・アルマンド (Almata 創設者兼 CEO) パネリスト：ネイト・スナイダー (FiveLines ディレクター) パネリスト：スティーブン・リー (ロバート・ハーフ・ジャパン、サイバーセキュリティ・データ＆AI分野採用リーダー) パネリスト：アレックス・デヴォア (MadeHere CEO兼創業者)
1. Moderated by James Miller, the panel examined AI security and AI sovereignty as distinct but overlapping objectives. Security concerns protection, constraints, and verifiable behavior, while sovereignty concerns durable authority, technological options, and control over dependencies. Neither is guaranteed simply by domestic hosting or a provider's nationality. 2. Eddy Almand proposed starting with what an organization needs to protect and control. Beyond network security, identity, and authorization, he emphasized physical and personnel security, control of data and encryption keys, and the ability to shut systems down. Disconnected or intermittently connected edge environments introduce additional operational challenges. 3. Nate Snyder questioned whether sovereignty accurately describes systems that depend on international technology stacks. He advocated focusing on practical control, access, governance, and policies that reflect operational realities, including dependencies on external infrastructure and the needs of industries unable to build complete systems independently.	1. ジェームズ・ミラー氏の進行により、AIセキュリティとAI主権を、重なりながらも異なる目標として議論した。セキュリティは保護、行動の制約、検証可能性に関わり、主権は持続的な権限、技術的な選択肢、依存関係を管理する能力に関わると整理した。国内での稼働や提供企業の国籍だけで、いずれも保証されるわけではないと指摘した。 2. エディ・アルマンド氏は、何を守り、何を自ら管理する必要があるのかを明確にすることから始めるべきだと述べた。ネットワーク、身元確認、認可に加え、物理的・人的な安全、データと暗号鍵の管理、システムを停止できる能力を重視した。また、常時接続を前提にできないエッジ環境には、追加の運用上の課題があると説明した。 3. ネイト・スナイダー氏は、国際的な技術基盤に依存するシステムを「主権」という言葉で捉えることに疑問を示した。完全なシステムを独力で構築できない産業もあるため、外部基盤への依存を踏まえ、実際に管理できる範囲、アクセス、ガバナンス、運用の実情に合う政策に焦点を当てるべきだと述べた。 4. アレックス・デヴォア氏は、防衛関連のサプライチェーン業務向けに構築した、特定のハードウェアに依存しない分散型メッシュ構成を紹介した。小規模な企業が集中型の基盤を一から整備するのではなく、不要な依存を増やさずに管理能力を確保する方法として分散化を説明した。議論では、エネルギー、半導体、インフラへの依存も取り上げられた。

4. Alex DeVore described a distributed, hardware-agnostic mesh architecture developed for defense-related supply-chain operations. He presented decentralization as a way for a smaller company to gain control without building a centralized stack or creating unnecessary dependencies. The discussion also highlighted underlying dependencies on energy, chips, and infrastructure.
5. Steven Li identified a gap between ambitious security-transformation plans and the availability of people who can implement them. He described cases where technically capable security leaders and engineers encountered organizational resistance, arguing that skills and internal trust must be brought together for transformation to succeed.
6. The discussion treated security as a management and organizational challenge as well as a technical one. Defining critical assets, decision-making authority, information flows, and access responsibilities is essential. Resistance to visibility and information sharing can prevent security leaders from understanding the environment they are expected to protect.
7. DeVore argued that organizations may underinvest when they can shift the consequences of security failures onto society. Participants discussed accountability and incentives, while Snyder highlighted smaller suppliers as potential entry points and emphasized workforce-wide ownership rather than isolating security responsibility in a single team.
8. Li described automated penetration testing as a way to extend assessment beyond the most critical systems to services that previously received less attention. Participants distinguished using AI for security from securing AI itself, and stressed that automation does not remove the need for responsible behavior, oversight, and a security-conscious organizational culture.
9. Miller proposed stronger logging, authorization management, authentication of human actors, and validation of AI outcomes as foundations for accountable operation. The discussion explored a zero-trust baseline for AI use and the need to verify conduct as agents use tools and cross organizational and technical trust boundaries.

5. スティーブン・リー氏は、高度なセキュリティ変革の計画と、それを実行する人材の確保との間に隔たりがあると指摘した。専門能力を持つ責任者や技術者を採用しても、組織内の抵抗によって変革が進まない例を挙げ、技術的な能力と社内の信頼を結び付ける必要性を述べた。
6. セキュリティは、技術だけでなく、経営と組織の課題でもあると議論した。重要資産、意思決定の権限、情報の流れ、アクセスに関する責任を明確にすることが不可欠であり、可視化や情報共有への抵抗が、セキュリティ責任者による実態把握と対策を妨げる可能性を指摘した。
7. デヴォア氏は、セキュリティ上の失敗による負担を社会に転嫁できる場合、企業の投資意欲が弱くなるとの見解を示した。議論では、責任とインセンティブが取り上げられ、スナイダー氏は、小規模な取引先が侵入口となるリスクと、特定の担当部署だけに任せず、従業員全体が守る責任を共有する重要性を強調した。
8. リー氏は、自動化された侵入テストによって、従来は重要システム以外に十分に実施できなかった検証を広げられると説明した。議論では、AIをセキュリティ対策に使うことと、AIそのものを安全にすることを区別し、自動化が進んでも、責任ある行動、監督、組織全体のセキュリティ文化は必要だと述べた。
9. ミラー氏は、説明責任を伴う運用の基盤として、ログの充実、認可の管理、人間の利用者の認証、AIの処理結果の検証を提案した。AI利用にゼロトラストの考え方を適用し、エージェントがツールを使って組織や技術上の信頼境界を越える際にも、その行動を検証する必要性を議論した。
10. アルマンド氏は、モデル、基盤、提供企業を変更でき、データを保持したまま契約関係から離脱できることを、実質的な管理能力として重視した。会場からは、サプライチェーンを管理するための閉じた仕組みや保護主義が、選択肢を減らし、囲い込みにつながるのではないかという質問があった。

10. Almand emphasized the ability to replace models, infrastructure, and providers, retain data, and exit vendor relationships as practical expressions of control. An audience question raised the tension between supply-chain control, protectionist or closed ecosystems, and reduced choice.	

Special Program 特別プログラム

David Farber Memorial Conference: The Legacy and Future of Cyber Civilization
ディビッド・ファーバー メモリアルカンファレンス：サイバー文明の軌跡と未来

2026年10月29日（木） 09:00–17:00 JST
慶應義塾大学 三田キャンパス 北館 会議ホール
Hybrid | English

Special Program 1 09:00 JST

Title: Opening Session Listed participants: • Kohei Itoh • Jun Murai • Manny Farber	題名（公式英語表記）：Opening Session 掲載登壇者： • Kohei Itoh • Jun Murai • Manny Farber
1. The Opening Session featured remarks by Keio University President Kohei Itoh, Cyber Civilization Research Center Director Jun Murai, and David Farber's son, Manny Farber. They framed the conference as an opportunity to honor Farber's contributions while considering how his ideas and work could be carried forward across generations and disciplines. 2. Itoh traced Farber's relationship with Keio to Professor Hideo Aiso's visit to his research group in 1973. Research exchanges and network connections subsequently deepened that relationship, leading to Farber and Murai's joint establishment of the Cyber Civilization Research Center in 2018 as a forum for examining information technology and society through the perspective of civilization. 3. Itoh recalled Farber's move to Japan in his eighties and his enjoyment of discovering differences in culture and daily life in Tokyo. He emphasized Farber's appreciation of personal relationships and individual encounters, recalling their own conversations about science, Japan, and other subjects. 4. Murai reflected on Farber's sudden passing and the personal connections that brought him to Keio. Japanese researchers had long hoped he would conduct research in Japan, and Farber also greatly enjoyed Japanese food. Murai recalled their relationship beginning in the early 1980s and their subsequent collaboration on establishing CSNET connectivity.	1. オープニングセッションでは、慶應義塾長の伊藤公平氏、サイバー文明研究センター長の村井純氏、David Farber氏のご子息であるManny Farber氏が挨拶した。Farber氏の功績をたたえるとともに、その思想や取り組みを世代や専門分野を超えて未来へ受け継ぐことが、カンファレンスの目的として示された。 2. 伊藤氏は、Farber氏と慶應義塾大学の関係が、1973年に相磯秀夫教授が同氏の研究グループを訪問したことに始まると紹介した。その後、研究交流やネットワーク接続を通じて関係が深まり、2018年にはFarber氏と村井氏が共同でサイバー文明研究センターを設立し、情報技術と社会を文明の視点から考える場を築いたと述べた。 3. 伊藤氏は、Farber氏が80代で日本へ移り、東京での文化や日常生活の違いを楽しんでいたことを振り返った。人と人との関係や一つ一つの出会いを大切にする姿勢に触れ、自身も科学や日本など、さまざまな話題について語り合った思い出を紹介した。 4. 村井氏は、Farber氏の突然の逝去を振り返り、同氏を慶應へ迎えることにつながった人々との関係について語った。日本の研究者たちが長年、日本での研究活動を望んでいたことや、Farber氏自身も日本の食事を楽しんでいたことを紹介した。また、1980年代初めの出会いから、CSNET接続の構築に向けて協力した経緯を述べた。 5. 村井氏は、サイバー文明研究センターの名称に込めた考えを、福澤諭吉の技術と文明に関する思想を通じて説明した。新技術を取り入れる際には、それに伴う恐れや混乱まで受け入れるのではなく、技術を理解し活用する人材、知恵、準備が必要であると強調した。 6. この視点を現在のAIをめぐる状況と結び付け、村井氏は、新技術に慌てることなく未来を考える重要性を述べた。センターの名称には、技術の変化を社会が理解し、建設的に活用するというFarber氏との共通の関心が反映されており、思い出を共有しながら未来を計画していきたいとした。

5. Murai explained the thinking behind the name “Cyber Civilization Research Center” by drawing on Yukichi Fukuzawa’s reflections on technology and civilization. He emphasized that adopting new technologies requires people, understanding, and preparation, rather than importing the fear and confusion that can accompany technological change.
6. Connecting this perspective to contemporary concerns about AI, Murai encouraged participants to remember Farber while planning for the future without panicking about new technologies. The center’s name reflected their shared interest in how society can understand and make constructive use of technological change.
7. Manny Farber introduced three personal artifacts to illustrate the breadth of his father’s career: a Bell Laboratories technical publication, a T-shirt depicting technological layers, and a passport. The publication prompted reflections on Farber’s early work on SNOBOL and the No. 1 ESS electronic switching system.
8. Using the layered illustration, Manny described how Farber, his students, and his collaborators influenced fields ranging from distributed computing and networking to Internet protocols, applications, and governance. His involvement with organizations such as EFF, EPIC, and the FCC, and later with Keio’s research center, extended that engagement into public policy and the social and cultural dimensions of technology.
9. The passport, issued when Farber was seventy-seven and later filled completely, illustrated his continuing international travel and collaboration. Manny emphasized that universities bring people together to collaborate and welcomed the conference’s focus on the future, including discussions of Farber’s call to reconstruct the Internet.

7. Manny氏は、ベル研究所の技術刊行物、技術の階層を描いたTシャツ、パスポートという三つの品を通じて、父の活動の広がりを紹介した。技術刊行物を手がかりに、プログラミング言語SNOBOLや電子交換システムNo. 1 ESSなど、Farber氏の初期の仕事を振り返った。
8. Manny氏は、階層図を用い、Farber氏とその学生・共同研究者の影響が、分散コンピューティングやネットワークから、インターネットのプロトコル、アプリケーション、ガバナンスまで及んでいたと説明した。EFF、EPIC、FCCなどでの活動や、慶應の研究センターへの参画を通じ、その関心が公共政策、さらに技術の社会的・文化的側面へと広がっていたことを示した。
9. 77歳のときに発行され、後に全ページが埋まったパスポートは、Farber氏が晩年まで国際的な移動と協力を続けていたことを象徴するものとして紹介された。Manny氏は、大学は人々が集まり協力する場でもあると述べ、インターネットの再構築を求めたFarber氏の考えを含め、今回のカンファレンスが未来に目を向けていることを歓迎した。

Special Program 2 09:15 JST

Title: Morning Session: David Farber's Legacy and the Unfinished Challenges of the Internet Moderator: Jun Murai Listed participants: • Vinton Cerf (Video Message) • Steve Crocker • David Crocker • Paul Mockapetris • Izumi Aizu	題名（公式英語表記）: Morning Session: David Farber's Legacy and the Unfinished Challenges of the Internet モデレーター: Jun Murai 掲載登壇者: • Vinton Cerf (Video Message) • Steve Crocker • David Crocker • Paul Mockapetris • Izumi Aizu
1. Moderated by Jun Murai, the morning session featured a video message from Vinton Cerf and contributions from Steve Crocker, David Crocker, Paul Mockapetris, and Izumi Aizu. Murai positioned the session as an opportunity to reflect on David Farber's life and lessons, providing a foundation for the day's subsequent discussions about the future. 2. Cerf remembered Farber as a connector whose curiosity led him to bring together people who might otherwise never have interacted. He highlighted the Interesting People mailing list as an important forum for exchanging ideas and recalled Farber's distinctive expressions, or "Farberisms," as reminders that unexpected partnerships can emerge from shared needs. 3. Steve Crocker recalled Farber's generosity, friendship, and contributions to programming languages and networking. He described how taking over some of Farber's responsibilities at UC Irvine brought him into contact with Paul Mockapetris, whom he subsequently invited to join ISI, setting the stage for work that led to the Domain Name System. Farber's influence often emerged through the connections and opportunities he created for others. 4. Reflecting on Internet security, Steve Crocker argued that attribution and accountability had received insufficient attention in its early development. He emphasized the challenge of supporting responsible behavior online while preserving openness and freedom and avoiding excessive identification, surveillance, or government control. 5. David Crocker described how Farber's mentorship and professional connections supported his work on electronic messaging. He recalled developing MMDF to extend email access through telephone connections and explained how that work contributed to CSNET, expanding networking opportunities beyond institutions able to afford direct ARPANET connections.	1. 村井純氏の司会の下、Vinton Cerf氏のビデオメッセージに続き、Steve Crocker氏、David Crocker氏、Paul Mockapetris氏、会津泉氏が発言した。村井氏は、Farber氏の人生や教えを振り返り、その後の未来に向けた議論の基盤とすることを、午前のセッションの目的として説明した。 2. Cerf氏は、Farber氏を、通常なら出会わなかったかもしれない人々を好奇心によって結び付ける人物として振り返った。Interesting Peopleのメーリングリストが、意見や可能性を交換する重要な場であったと紹介した。また、「Farberisms」と呼ばれる独特の言い回しに触れ、共通の必要性から意外な人々の協力関係が生まれることを示すものとして語った。 3. Steve Crocker氏は、Farber氏の寛大さや友情、プログラミング言語とネットワークへの貢献を振り返った。UC IrvineでFarber氏の仕事の一部を引き継いだことでPaul Mockapetris氏と知り合い、その後ISIへ招いた経緯を紹介し、そのつながりがDNSの開発へと続いたと説明した。Farber氏の影響は、他者のために生み出した関係や機会を通じても広がっていたとした。 4. インターネットのセキュリティについて、Steve Crocker氏は、初期の設計では行為者の特定や説明責任への配慮が十分ではなかったと述べた。開放性と自由を維持し、過度な本人特定、監視、政府による統制を避けながら、オンラインでの責任ある行動を支える仕組みを構築する難しさを指摘した。 5. David Crocker氏は、Farber氏の指導と人脈が電子メールの研究開発を支えた経緯を紹介した。電話回線を通じて電子メールを利用できるMMDFの開発を振り返り、その成果がCSNETに貢献し、ARPANETへの直接接続に必要な費用を負担できない機関にも、ネットワーク利用の機会を広げたと説明した。 6. David Crocker氏は、小規模な環境での成功と、世界規模での運用に必要な条件を区別するよう研究者に助言した。利用者数の増加だけでなく、技術的条件、組織、文化の違いにも対応する必要があると述べた。新しい発想に積極的に取り組むとともに、当初の環境を離れた際の動作について謙虚に検討する姿勢を求めた。

6. David Crocker advised researchers to distinguish small-scale success from the requirements of global deployment. Systems must accommodate not only larger numbers of users but also different technical conditions, organizations, and cultures. He encouraged ambitious innovation combined with humility about how designs will perform outside their original environment.
7. Paul Mockapetris recalled working with Farber on distributed computing at UC Irvine and benefiting from introductions that opened opportunities across universities and industry. He described the lasting effects of Farber's connections and encouraged researchers to seek opportunities where disciplines and skills intersect, drawing on his own experience combining programming and device knowledge.
8. Izumi Aizu described Farber's contributions to Internet development in Japan and Asia through CSNET and international research relationships. He recalled Farber's advice to use the Internet for global dialogue, his support for Internet adoption in Japanese business and policy circles, and his efforts to bridge institutional and cultural differences.
9. Aizu emphasized Farber's belief that those who benefited from his support should help others. Farber encouraged him to support Internet development across Asia rather than repay him personally. Aizu also described Farber's continuing engagement in Japan through CCRC, AI policy discussions, and education that encouraged young people to learn and work across cultural boundaries.
10. The session presented Farber's legacy as both technological and human: advancing computing and networking while supporting independent work and connecting people across borders and generations. Murai closed by recalling Farber's role in enabling dialogue between younger researchers and established institutions and encouraged participants to carry the shared insights into the following panel discussion.

7. Paul Mockapetris氏は、UC IrvineでFarber氏と分散コンピューティングに取り組んだ経験や、大学・産業界への紹介によって研究と仕事の機会を得たことを振り返った。Farber氏がつくったつながりの影響が長く続いたことを紹介し、プログラミングとデバイスの知識を組み合わせた自身の経験から、異なる分野や能力が交わる場所に機会を見いだすよう勧めた。
8. 会津氏は、CSNETや国際的な研究交流を通じた、Farber氏の日本・アジアにおけるインターネット発展への貢献を紹介した。世界との対話にインターネットを活用するという助言、日本の企業や政策関係者への普及活動の支援、組織や文化の違いを超えて対話を促した役割を振り返った。
9. 会津氏は、支援を受けた人が次にほかの人を支えるというFarber氏の考え方を強調した。個人的に恩返しをするのではなく、アジア全体へのインターネット普及を支援するよう勧められた経験を紹介した。また、Farber氏が日本でCCRC、AI政策に関する議論、若者が異文化の人々と学び働く機会を広げる教育に取り組み続けたことを述べた。
10. セッション全体を通じて、Farber氏の遺産は、コンピューティングやネットワークの発展に加え、自立した活動を支え、国境や世代を超えて人々を結び付けることにもあると示された。村井氏は、Farber氏が若手研究者と既存の組織との対話を可能にした役割を振り返り、共有された知見を次のパネルディスカッションへつなげることを促した。

Special Program 3 10:10 JST

Title: Panel Discussion 1: Reconstructing the Internet: David Farber's Legacy Moderator: Jun Murai Listed participants: • Douglas Sicker • Rodney Van Meter • Dan Gillmor • Catharina Maracke	題名（公式英語表記）: Panel Discussion 1: Reconstructing the Internet: David Farber's Legacy モデレーター: Jun Murai 掲載登壇者: • Douglas Sicker • Rodney Van Meter • Dan Gillmor • Catharina Maracke
1. Moderated by Jun Murai, the panel brought together Douglas Sicker, Rodney Van Meter, Dan Gillmor, and Catharina Maracke to discuss David Farber's legacy and the future of the Internet. They remembered him as a connector and mentor who challenged assumptions constructively, supported younger researchers, and linked technical questions with their wider consequences for society. 2. Participants examined the transition from an Internet built among trusted researchers to infrastructure used by everyone, including malicious actors. Gillmor recalled Farber's interest in rebuilding trust through additional security layers or redesign from the foundations, with banking as a possible starting point. The discussion emphasized the difficulty of adding security to an architecture that originally assumed trust. 3. Sicker stressed that cybersecurity problems are also economic, social, and public-policy problems. Reflecting on his work with Farber, he argued that technical expertise must inform policymaking and that solutions require participation from all relevant stakeholders. Researchers were encouraged to develop expertise in their disciplines while engaging beyond technical communities. 4. Education emerged as a central part of Farber's legacy. Maracke emphasized liberal arts, ethics, philosophy, and independent thinking, while participants discussed how AI could support learning without replacing students' ability to question and reason. Sicker also cautioned that interdisciplinary work requires a solid foundation in at least one discipline.	1. 村井純氏の司会の下、Douglas Sicker氏、Rodney Van Meter氏、Dan Gillmor氏、Catharina Maracke氏が、David Farber氏の遺産とインターネットの未来について議論した。Farber氏は、人々を結び付け、若手研究者を支援し、前提を建設的に問い直すとともに、技術上の問題を社会への幅広い影響と結び付けるメンターとして振り返られた。 2. 信頼関係のある研究者同士のネットワークから、悪意ある利用者も含めた、誰もが使う社会基盤へとインターネットが変化したことが論点となった。Gillmor氏は、Farber氏がセキュリティの層の追加や基盤からの再設計に関心を持ち、銀行分野を出発点の候補としていたことを紹介した。当初は信頼を前提とした設計に、安全性を後から組み込む難しさが指摘された。 3. Sicker氏は、サイバーセキュリティの問題は、経済、社会、公共政策の問題でもあると強調した。Farber氏との活動を振り返り、技術的な専門知識を政策形成に届けることや、関係するすべてのステークホルダーが議論に参加する必要性を述べた。研究者には、自らの専門性を深めるとともに、技術コミュニティの外にも関わる姿勢が求められるとした。 4. 教育は、Farber氏が残した重要な遺産として取り上げられた。Maracke氏は、リベラルアーツ、倫理、哲学、自立した思考の重要性を強調した。AIを学習に活用しながらも、学生自身が問い、考える力をどう維持するかが議論された。また、Sicker氏は、学際的な活動には、少なくとも一つの分野における確かな基礎が必要だと指摘した。 5. Van Meter氏は、学部生が早期から研究に参加し、実践と並行して基礎知識を身に付ける、慶應義塾大学SFCの研究会の仕組みを紹介した。学生や修了生も、未知の分野への挑戦、学会参加、教員との交流を通じた学びを共有した。研究への意欲、広い視野、深い技術的理解をどのように両立させるかが課題として示された。 6. Gillmor氏は、デジタルプラットフォームやAIによって、情報伝達と学習のあり方が変化していると述べた。情報を支配する力の集中、注意力の分断、個人を狙ったプロパガンダへの懸念を示す一方、参加の機会が広がる可能性も認めた。メディアリテラシー、能動的な参加、プラットフォームへの支配の集中に対抗する再分散化の必要性を強調した。

5. Van Meter described Keio's SFC research-group model, which allows undergraduates to participate in research early and build foundational knowledge alongside practical work. Students and graduates shared experiences of entering unfamiliar fields, attending conferences, and learning through interaction with faculty. The discussion highlighted the need to balance motivation, broad perspectives, and deep technical understanding.
6. Gillmor examined how digital platforms and AI are changing communication and learning. He expressed concern about concentrated control over information, fragmented attention, and individually targeted propaganda, while recognizing opportunities for wider participation. He advocated media literacy, active engagement, and efforts to restore decentralization rather than accepting increasing platform control.
7. Maracke discussed tensions between globally developed open-source software and nationally focused regulation. She emphasized the importance of international communities in maintaining shared infrastructure and addressing vulnerabilities. Participants called for closer communication between policymakers and technical experts so that regulation reflects how technologies are actually developed and operated.
8. Murai distinguished the globally shared core Internet from services and activities subject to national responsibilities. He argued for preserving essential connectivity and DNS despite political conflicts, describing the Internet as comparable to oxygen. Universities and international forums were presented as important channels for maintaining dialogue across borders and explaining these distinctions to policymakers.
9. The panel considered technology's beneficial uses alongside abuse, including challenges posed by AI agents. Participants questioned whether regulating technology alone could address harmful behavior and emphasized understanding people's motivations, incentives, and responsibilities. They also discussed the concentration of technological power and Japan's potential to contribute alternative approaches, including a distinct AI technology stack.

7. Maracke氏は、世界規模で開発されるオープンソースソフトウェアと、国家単位の規制との緊張関係を指摘した。共有の情報基盤を維持し、脆弱性へ対応する国際的なコミュニティの役割を強調した。技術の開発や運用の実態を踏まえた規制とするため、政策担当者と技術の専門家が、より密接に対話する必要性が示された。
8. 村井氏は、世界で共有されるインターネットの中核部分と、各国が責任を持つサービスや活動を区別して考える重要性を説明した。インターネットを酸素になぞらえ、政治的対立があっても、基本的な接続やDNSを維持すべきだと述べた。大学や国際的な議論の場は、国境を超えた対話を保ち、こうした違いを政策担当者に伝える重要な経路として位置付けられた。
9. 技術がもたらす恩恵と、その悪用への対応について、AIエージェントの課題も含めて議論された。技術そのものへの規制だけで有害な行動に対応できるかが問われ、人々の動機、インセンティブ、責任を理解する必要性が示された。また、技術に関する権力の集中や、日本独自のAI技術スタックなど、異なる選択肢を世界へ提供する可能性も取り上げられた。
10. 最後に、社会への参加、建設的な批判、社会課題を明らかにして政策へつなぐ学術界の役割が強調された。Farber氏は、開かれた姿勢と友情を大切にしながら、必要なときには率直かつ力強く意見を述べる人物として振り返られた。次世代には、その好奇心、国際的なつながり、技術の恩恵を広く人々へ届ける姿勢を受け継ぐことが促された。

10. Closing reflections emphasized participation, constructive criticism, and the role of academia in identifying societal problems and informing policy. Farber was remembered for combining openness and friendship with the willingness to speak firmly when necessary. Participants encouraged the next generation to carry forward his curiosity, international connections, and commitment to ensuring that technology benefits people broadly.	

Special Program 4 13:00 JST

Title: Afternoon Session: Creating the Next Cyber Civilization Listed participants: • Douglas Sicker • David Luzzi	題名（公式英語表記）: Afternoon Session: Creating the Next Cyber Civilization 掲載登壇者: • Douglas Sicker • David Luzzi
Title: Afternoon Session: Creating the Next Cyber Civilization Speaker: • David Luzzi	題名（公式英語表記）: Afternoon Session: Creating the Next Cyber Civilization 登壇者: • David Luzzi
1. David Luzzi reflected on his relationship with David Farber through their shared connection to Stevens Institute of Technology, their time at the University of Pennsylvania, and conversations during visits to Keio University. He organized his remarks around questions he wished he could discuss with Farber over another lunch, particularly about education, public policy, and responsibility for future generations. 2. Luzzi described the broad engineering education that both he and Farber experienced at Stevens. Students studied subjects beyond their specialties, gaining exposure to multiple engineering disciplines. He asked how this breadth had influenced Farber's ability to work across fields and contribute throughout his career. 3. He also recalled the demanding academic environment at Stevens and questioned how that experience had shaped their development. Rather than presenting its rigor as a model to adopt unquestioningly, he raised it as a subject for reflection on how universities should prepare students for contemporary technological and societal challenges.	1. David Luzzi氏は、Stevens Institute of Technologyの同窓生としてのつながり、University of Pennsylvaniaでの交流、慶應義塾大学への訪問時の会話を通じて、David Farber氏との関係を振り返った。もう一度昼食を共にできるなら何を尋ねたいかという形で、教育、公共政策、次世代への責任について問題を提起した。 2. Luzzi氏は、自身とFarber氏がStevensで受けた、専門分野を超える幅広い工学教育を紹介した。学生が複数の工学分野を学ぶ教育を取り上げ、その広がりがFarber氏の分野横断的な活動や、その後のキャリアにどのような影響を与えたのかを問いかけた。 3. また、Stevensの厳しい学習環境を振り返り、その経験が自分たちの成長をどう形づくったのかを考察した。当時の厳しさをそのまま現在の教育の模範とするのではなく、今日の技術的・社会的課題に向けて学生をどう育てるべきかを考えるための論点として示した。 4. Farber氏が公共政策への関与を深めていった歩みに関連し、確かな技術的基礎と、人文・社会科学の学びとの関係を検討した。これらの分野を大学でより広く学ぶことが役立ったのか、それとも人生経験を通じて得た理解こそが、後年の政策面での貢献に重要だったのかという問いを示した。 5. Luzzi氏は、Farber氏が学生との活動を大切にし、学生の成長を大学教員の仕事の中心に置いていたことを強調した。次世代を育成することは、大学における教育・研究活動の根本的な責任であると述べた。

4. Turning to Farber's growing involvement in public policy, Luzzi considered the relationship between strong technical foundations and education in the humanities and social sciences. He asked whether broader formal exposure to these fields would have helped Farber earlier in his career, or whether the understanding acquired through life experience was essential to his later contributions.
5. Luzzi emphasized Farber's commitment to students and his belief that their development was central to the work of university faculty. He recalled Farber's enthusiasm for working with students and treated the preparation of future generations as a fundamental responsibility of academic life.
6. AI introduced a challenge to that responsibility. Luzzi described colleagues experimenting with AI systems as substitutes for graduate-student research assistance, enabling faster production of research outputs. He expressed concern that an emphasis on productivity could draw faculty away from mentoring students and developing the people who will shape society's future.
7. He called for reflection on what AI means for university education, what educators should expect from students, and how teaching and research should evolve. His questions focused on preserving the educational purpose of universities while responding to the capabilities of emerging technologies.
8. Luzzi concluded that cyber civilization must be considered through both its technological and human dimensions. Farber's experiences offered a starting point for examining how education can equip today's students to understand technology, engage with society, and carry responsibility for the next generation.

6. AIの普及は、この責任に新たな課題をもたらしていると指摘した。大学院生による研究補助の代わりにAIを使い、研究成果の作成を速める試みを紹介する一方、生産性を優先することで、教員が学生の指導や社会の未来を担う人材の育成から離れてしまうことへの懸念を示した。
7. AIが大学教育に何をもたらすのか、学生に何を期待すべきか、教育と研究をどう変えていくべきかを問い直す必要性を述べた。新技術の能力に対応しながらも、大学が持つ教育の目的をどう維持するかが中心的な課題として示された。
8. 最後に、サイバー文明を考える際には、技術と人間の両方の側面が不可欠であると強調した。Farber氏の経験を手がかりに、現代の学生が技術を理解し、社会に関わり、次世代への責任を担えるようにするために、教育で何を重視すべきかを考える必要性を示した。

Special Program 5 13:05 JST

Title: Farber Lab Session Listed participants: • Taro Tsuchiya • Hitomi Sano • Bradley Suzuki • Korry Luke • Monet Tokuyama Friedrich	題名（公式英語表記）: Farber Lab Session 掲載登壇者: • Taro Tsuchiya • Hitomi Sano • Bradley Suzuki • Korry Luke • Monet Tokuyama Friedrich
1. The Farber Lab Session brought together Taro Tsuchiya, Hitomi Sano, Bradley Suzuki, Korry Luke, and Monet Tokuyama Friedrich to reflect on David Farber's mentorship and present their research and visions for the future. Their presentations connected his legacy with education, international exchange, medical inclusion, trustworthy infrastructure, and quantum networking. 2. Taro Tsuchiya described how Farber supported his development from a student at Keio University to a doctoral researcher at Carnegie Mellon University. Comparing his experiences in Japan and the United States, he identified language, educational culture, and geography as barriers to international academic participation. He suggested that AI-assisted translation could reduce language barriers while emphasizing the continuing value of multilingual perspectives. 3. Tsuchiya advocated creating more opportunities for students to participate in research and build international relationships. He proposed interactive teaching methods that encourage engagement without requiring everyone to speak publicly, undergraduate research opportunities, and seminars that connect students with visiting researchers. He expressed his intention to continue Farber's work of helping Japanese students access overseas graduate education. 4. Hitomi Sano highlighted two lessons from Farber: maintaining dialogue across differences and questioning established assumptions. She recalled his willingness to listen despite language difficulties and his view that the Internet remained an unfinished system requiring reconsideration, particularly regarding security. These lessons informed CCRC's medical inclusion initiative, which explores how healthcare could become more accessible across national and institutional boundaries.	1. Farber Lab Sessionでは、Taro Tsuchiya氏、Hitomi Sano氏、Bradley Suzuki氏、Korry Luke氏、Monet Tokuyama Friedrich氏が、David Farber氏から受けた指導を振り返り、それぞれの研究と将来の展望を発表した。教育、国際交流、医療インクルージョン、信頼できる情報基盤、量子ネットワークを通じて、Farber氏の遺産を今後にどうつなぐかが示された。 2. Tsuchiya氏は、慶應義塾大学の学生時代にFarber氏と出会い、その支援を受けてCarnegie Mellon Universityの博士課程へ進んだ経験を紹介した。日本と米国での経験を比較し、国際的な学術活動への参加を妨げる要因として、言語、教育文化、地理的条件を挙げた。AIによる翻訳が言語の壁を低くする可能性を示す一方、複数の言語を理解することや、非母語話者ならではの視点にも価値があると述べた。 3. Tsuchiya氏は、学生が研究に参加し、国際的な人脈を築く機会を増やす必要性を強調した。全員に人前での発言を求めるのではなく、クイズや投票などで参加を促す授業、学部生の研究参加、外部研究者との交流を伴うセミナーなどを提案した。日本の学生の海外大学院進学を支える活動を通じて、Farber氏の取り組みを次世代へ引き継ぎたいと述べた。 4. Sano氏は、Farber氏から学んだこととして、違いを超えて対話を続ける姿勢と、既存の仕組みを当然と考えず問い直す姿勢を挙げた。言語の壁があっても丁寧に耳を傾ける姿や、インターネットを完成した仕組みとは捉えず、特にセキュリティを再検討し続けた姿を紹介した。こうした考え方は、国や制度の境界を超えて医療へのアクセスを広げる、CCRCの医療インクルージョン構想にもつながっていると説明した。 5. Sano氏は、医療インクルージョンには、データや技術の接続だけでなく、人々が理解し信頼できる仕組みと、医療者・技術者などの関係者間の対話が必要だと述べた。また、Farber Labについて、新技術や法律・規制がサイバー文明に与える影響を先取りし、異なる分野の人々が望ましい未来と避けたい未来を検討する取り組みとして紹介した。

5. Sano explained that medical inclusion requires more than connecting data and technologies; it also requires trustworthy systems and dialogue among healthcare professionals, engineers, and other stakeholders. She also described Farber Lab's aim of anticipating how technologies, laws, and regulations may shape cyber civilization, bringing different disciplines together to consider desirable futures and risks before society is forced to react.
6. Bradley Suzuki connected Farber's concern for security with his commitment to inclusion and human well-being. Using healthcare information sharing as an example, he explained that secure transmission alone does not ensure appropriate protection after data reaches its destination. Trustworthy interoperability requires compatible standards, identity verification, enforceable permissions, and accountability for how information is accessed and used.
7. Suzuki emphasized privacy as a fundamental human right and argued that information sharing should operate within clearly defined, enforceable boundaries. The objective is to enable necessary access for care while preventing unnecessary access, modification, and misuse. Building on the connectivity achieved by Farber's generation, future systems must establish the trust needed for independently operated organizations to exchange information responsibly.
8. Korry Luke examined how the Internet's origins as an open research network continue to affect DNS, email, and security operations. Security extensions have addressed weaknesses in the original protocols but have also increased complexity and created deployment gaps. He stressed that publishing standards does not guarantee adoption and highlighted the need for simpler, maintainable systems that accommodate the realities of distributed global operation.
9. Luke described research on digital identity and authentication, including extending transparency-based approaches from Web PKI to make the evidence behind verification decisions more visible. He emphasized usable security and distinguished fundamental architectural problems from operational challenges. Farber's ambition to redesign the Internet raised the practical question of how to improve infrastructure while keeping essential services running, particularly as AI accelerates vulnerability discovery.

6. Suzuki氏は、Farber氏がセキュリティを重視した背景には、包摂性と人間の幸福を大切にする姿勢があったと述べた。医療情報の共有を例に、安全な通信だけでは、情報が相手に届いた後の適切な保護までは保証できないと説明した。信頼できる相互運用には、共通の標準、本人確認、実効性のあるアクセス権限、情報の利用に関する責任の明確化が必要だとした。
7. Suzuki氏は、プライバシーを基本的人権として位置付け、情報共有を明確かつ実効性のある境界の中で実現する重要性を強調した。医療のために必要な情報へのアクセスを確保しながら、不要な閲覧、改変、不正利用を防ぐことが目的であると説明した。Farber氏の世代が実現した接続性を基盤に、独立して運営される組織間でも責任を持って情報を交換できる信頼を構築する必要性を述べた。
8. Luke氏は、開かれた研究ネットワークとして発展したインターネットの設計が、現在のDNS、電子メール、セキュリティ運用にも影響していると説明した。当初のプロトコルの弱点を補う拡張は、安全性を高める一方で、複雑化や導入の格差を生んできたと指摘した。標準の策定だけでは普及は保証されず、世界各地の運用者が関わる現実を踏まえ、保守・運用しやすい仕組みを目指す必要性を示した。
9. Luke氏は、デジタルアイデンティティと認証に関する研究を紹介し、Web PKIにおける透明性の考え方を認証にも広げ、検証の判断に使われる証拠を見えるようにする方向性を述べた。利用しやすいセキュリティを重視し、根本的な設計上の課題と日々の運用上の課題を区別して考える必要性を指摘した。AIによって脆弱性の発見が加速する中、不可欠なサービスを動かし続けながら情報基盤を改善することが重要な課題であるとした。
10. Tokuyama Friedrich氏は、Farber氏との対話を通じ、量子コンピューティングや量子ネットワークの長期的な社会への影響を考えるようになったと述べた。文明を考える視点、制度やインフラなどの基盤、社会を変える技術を組み合わせた後継授業の構想を紹介した。研究面では、量子コンピュータのネットワーク化、量子通信と従来の通信の共存、データセンター設備の共有の可能性を説明し、過去の設計から学びながら、量子技術と従来技術を統合して人々を結ぶ一つのインターネットを目指す展望を示した。

10. Monet Tokuyama Friedrich explained how Farber encouraged her to consider the long-term social implications of quantum computing and networking. She described a proposed successor course combining perspectives on civilization, its institutional and infrastructural foundations, and transformative technologies. Her research explores networking quantum computers, integrating quantum and classical communications, and potential shared data-center infrastructure, with the longer-term aspiration of a unified Internet that learns from earlier architectural choices and connects people through both quantum and classical technologies.	

Special Program 6 14:20 JST

Title: Panel Discussion 2: Building the Future of Cyber Civilization Moderator: Catharina Maracke Listed participants: • Kazuo Noguchi • Korry Luke • Bradley Suzuki • Monet Tokuyama Friedrich • James Miller	題名（公式英語表記）：Panel Discussion 2: Building the Future of Cyber Civilization モデレーター：Catharina Maracke 掲載登壇者： • Kazuo Noguchi • Korry Luke • Bradley Suzuki • Monet Tokuyama Friedrich • James Miller
1. Moderated by Catharina Maracke, the panel brought together Kazuo Noguchi, James Miller, Korry Luke, Bradley Suzuki, and Monet Tokuyama Friedrich for an intergenerational discussion of David Farber's legacy and the future of cyber civilization. Participants remembered Farber as a mentor who connected people, encouraged independent thinking, and linked technical research with broader questions about society. 2. Participants considered how Farber might redesign the Internet with security incorporated from the outset. Recollections included his interest in hardware-level security and capability-based architectures that provide fine-grained access permissions. They also discussed the difficulty of transforming an infrastructure that society now depends on continuously. 3. The discussion examined the balance between openness, anonymity, and accountability. Participants recognized anonymity's value for freedom of expression while considering how to address abuse and malicious activity. James Miller emphasized identifying specific risks and applying authentication, authorization, auditing, and appropriately limited access rather than abandoning the open Internet. 4. AI agents raised questions about human autonomy, delegated authority, and responsibility. Participants discussed how agents should receive permission to act, what credentials they should hold, and who should be accountable when their actions cause harm. Miller suggested drawing on existing legal concepts, including agency law, consumer protection, and competition policy, while identifying gaps that require further work.	1. Catharina Maracke氏の司会の下、野口和夫氏、James Miller氏、Korry Luke氏、Bradley Suzuki氏、Monet Tokuyama Friedrich氏が、David Farber氏の遺産とサイバー文明の未来について世代を超えて議論した。Farber氏は、人と人を結び付け、自立した思考を促し、技術研究を社会全体の課題へとつなげるメンターとして振り返られた。 2. Farber氏がインターネットを設計し直すなら、どのようにセキュリティを組み込むかが議論された。ハードウェアレベルのセキュリティや、細かなアクセス権限を設定するケイパビリティベースのアーキテクチャへの関心が紹介された。一方、社会が常時依存するインフラとなったインターネットを、大きく変更する難しさも指摘された。 3. オープン性、匿名性、説明責任のバランスが検討された。匿名性が表現の自由を支える価値を認めつつ、不正利用や攻撃への対応が必要とされた。Miller氏は、具体的なリスクを明確にした上で、認証・認可・監査やアクセス範囲の制限を活用し、オープンなインターネットの価値を維持しながら安全性を高める考え方を示した。 4. AIエージェントについて、人間の自律性、権限の委任、責任の所在が論点となった。AIにどのような権限や認証情報を与えるか、その行動によって損害が生じた場合に誰が責任を負うかが議論された。Miller氏は、代理関係を扱う法理や消費者保護、競争政策などの既存の枠組みを参照し、不足する部分を見極める必要性を述べた。 5. AIガバナンスでは、企業への権力集中、AIモデルへのアクセスに関する依存、国際協力が取り上げられた。野口氏は、政府・産業界・学術界などが参加する国連での議論を紹介した。一方、国際的な合意の実効性や執行の難しさも問われ、実務的な解決策、既存の専門知識、地政学的な現実を踏まえる重要性が指摘された。 6. デジタルアイデンティティは、今後の研究課題の一つとして議論された。特に、詳細な個人情報を明かさずに、相手が人間であることを確認する方法や、人間自身の行為とAIに委任された行為を区別する方法が検討された。技術的な候補も紹介されたが、プライバシー、信頼性、権限付与、説明責任に関する課題は未解決の論点として残された。

5. AI governance was discussed in relation to concentrated corporate power, dependence on access to models, and international cooperation. Noguchi described United Nations discussions involving governments, industry, academia, and other stakeholders. Other participants questioned how international agreements could be enforced and stressed the need for practical solutions, existing expertise, and attention to geopolitical realities.
6. Digital identity emerged as a potential research direction, particularly ways to establish that an online participant is human without requiring disclosure of their full identity. The discussion also considered distinguishing human actions from those delegated to AI agents. Possible technical approaches were raised, but questions about privacy, reliability, authorization, and accountability remained open.
7. Participants compared the Internet's tradition of open participation and practical consensus with more formal laws, standards, and institutions. They highlighted the value of operational communities that exchange security information and develop shared norms. Quantum networking was discussed as another field where specifications and institutional coordination may become increasingly necessary while preserving openness.
8. Visions of a good future centered on inclusion, human well-being, and the distribution of power. Some participants advocated greater decentralization and wider access to information and technology, while others noted that decentralization can complicate oversight and protection of sensitive information. Technology was consistently treated as a tool whose value depends on the human purposes it serves.
9. Looking ahead, participants encouraged CCRC and Farber Lab to combine responses to current problems with exploration of possible futures. Suggested directions included research on social structures that resist excessive concentration of power, engagement with science fiction, and substantive collaboration across technical, legal, and other disciplines to inform policy and technological choices.

7. インターネットが育んできた自由な参加と実践的な合意形成を、法律・標準・制度とどう組み合わせるかが議論された。セキュリティ情報を交換し、共通の行動規範を形成する実務コミュニティの役割が強調された。量子ネットワークについても、オープン性を維持しながら、仕様の検討や制度的な連携を進める必要性が示された。
8. 望ましい未来の条件として、包摂性、人間の幸福、権力の分散が挙げられた。分散化や情報・技術へのアクセス拡大を重視する意見に対し、分散化には監督や機密情報の保護を難しくする側面もあると指摘された。技術はあくまで道具であり、人間が何を実現したいのかを起点に、その価値を考える必要性が共有された。
9. CCRCとFarber Labの今後については、現在の問題への対応と、将来の可能性を探る研究を組み合わせる方向性が示された。過度な権力集中に抵抗できる社会構造の研究、サイエンスフィクションからの着想、技術・法律などの分野を深く理解した学際的な連携を通じて、政策や技術の選択に貢献することが提案された。
10. 最後に、AI時代に必要な力として、文脈を理解すること、自分の考えを言葉で伝えること、他者の立場を理解することが挙げられた。量子技術の有力な応用先を見いだす難しさや、AIが人間関係、エネルギー消費、社会に与える影響にも言及された。Farber氏の遺産を受け継ぐには、好奇心、実践的な研究、コミュニティや世代を超えた対話を続けることが重要とされた。

10. The closing discussion emphasized understanding context, communicating clearly, and considering other people's perspectives as essential skills in the AI era. Participants also raised the challenge of finding compelling applications for quantum technology and cautioned against overlooking AI's effects on human relationships, energy use, and society. Carrying Farber's legacy forward would require curiosity, practical research, and continuing dialogue across communities and generations.	

Special Program 7 15:50 JST

Title: Closing Session Listed participants: • Jun Murai	題名（公式英語表記）: Closing Session 掲載登壇者: • Jun Murai
Title: Closing Session Speaker: • Rodney Van Meter	題名（公式英語表記）: Closing Session 登壇者: • Rodney Van Meter
1. Rodney Van Meter delivered the closing remarks on behalf of Jun Murai. He thanked the participants for a thought-provoking day and described the conference as a fitting tribute to David Farber's curiosity, enthusiasm, and enduring interest in the future. 2. He reflected on how the conference connected generations of Farber's students and colleagues, from early Internet pioneers to his most recent students. Their contributions demonstrated the breadth and continuity of Farber's influence across research, education, and public policy. 3. Van Meter identified recurring themes throughout the day, including the Internet, security, AI, quantum technologies, inclusion, power, and decentralization. He emphasized that Farber's interests extended across technical layers and into policy, with inclusion remaining an important concern. 4. He stressed that the government should be understood as more than a regulator. Governments also fund and conduct research and help shape research priorities. He highlighted the positive and complementary roles of industry, government, and academia, describing their partnership as essential. 5. Van Meter recalled Farber's practice of challenging people through questions grounded in trust. His questions were intended to help others clarify and strengthen their ideas while allowing him to learn from them, rather than to undermine their work.	1. Rodney Van Meter氏は、村井純氏の代理として閉会挨拶を行った。参加者に対し、多くの示唆を得られる一日への感謝を述べ、今回のカンファレンスは、David Farber氏の好奇心、熱意、未来への関心をたたえるにふさわしい場であったと振り返った。 2. カンファレンスには、初期のインターネットの発展を担った人々から、Farber氏が晩年に指導した学生まで、複数の世代の学生や同僚が参加したと述べた。それぞれの発表を通じて、研究、教育、公共政策にわたるFarber氏の影響の広さと、世代を超えたつながりが示されたとした。 3. 一日を通じて繰り返し登場したテーマとして、インターネット、セキュリティ、AI、量子技術、包摂性、権力、分散化を挙げた。Farber氏の関心は技術の各層から政策にまで及び、包摂性も大切にしていた論点であると強調した。 4. 政府を規制主体としてのみ捉えるべきではないと述べた。政府には、研究への資金提供、自ら研究を実施すること、研究の方向性や課題を形成することなどの役割もあると説明し、産業界・政府・学術界がそれぞれの強みを生かして連携する重要性を示した。 5. Farber氏は、信頼に基づく問いかけによって、人々の考えを深めていたと振り返った。その問いは相手を否定するためではなく、取り組みの価値を明確にし、考えをよりよく説明できるよう支援するとともに、Farber氏自身も相手から学ぶためのものであったと述べた。 6. また、Farber氏は現実を直視しながらも、冷笑的にはならない姿勢を持っていたと説明した。人間の限界や組織を動かす動機を理解し、それらを希望や前進を諦める理由とせず、取り組みを進める際に踏まえるべき条件として受け止めていたとした。

6. He also characterized Farber's outlook as realistic without being cynical. Farber recognized human limitations and the incentives shaping organizations, but treated these as conditions to understand and work with rather than reasons to abandon hope or progress. 7. Drawing on Ursula Le Guin's perspective on technology as part of humanity's interaction with the material world, Van Meter emphasized the importance of social change alongside technological development. This offered a way to connect the day's discussions with Farber's broader approach to cyber civilization. 8. He thanked the colleagues and friends who supported Farber's life in Japan, the Farber Lab team, Keio University, and the logistical support team for making the conference possible. He also acknowledged the medical professionals who cared for Farber, particularly those at Keio University Hospital. 9. Van Meter expressed gratitude to Farber's family for sharing him with the wider community and thanked participants attending in person, joining online, and watching later. He hoped the archived discussions would remain valuable and thought-provoking, and looked forward to the future of Farber Lab.	7. Ursula Le Guin氏の、技術を人間と物質世界との関わりとして捉える考え方を紹介し、技術の発展とともに社会の変化を考える重要性を述べた。この視点が、当日の議論と、Farber氏が持っていたサイバー文明への幅広い関心を結び付けるものだとした。 8. Farber氏の日本での生活を支えた同僚や友人、Farber Labのメンバー、慶應義塾大学、カンファレンスの運営を支えた関係者に謝意を表した。また、Farber氏の診療を担った医療関係者、特に慶應義塾大学病院の医師や職員への感謝も述べた。 9. Farber氏を広いコミュニティと分かち合ってくれたご家族に感謝するとともに、会場参加者、オンライン参加者、後日録画を視聴する人々に謝意を示した。記録された議論が今後も長く価値と示唆をもたらすことを願い、Farber Labの将来への期待を述べて締めくくった。

Change History

Date	Part	Comment
2026/11/25	Whole	New release