Report of all speeches and panels at 15th International Cybersecurity Symposium "Cybersecurity for Digitized National Security, Economic Security, and Societal Security: Global Multilateral Public-Private Partnership Actions"

October 28(Tue), 29(Wed), 30(Thu) and 31(Fri), 2025

Keio University Global Research Institute

第 15 回サイバーセキュリティ国際シンポジウム 開催報告書 要約

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：グローバルな多国間官民連携アクション」

日程: 2025 年 10 月 28 日（火）～31 日（金）

全体総括

本シンポジウムでは、サイバー脅威の質的・量的な深刻化（国家支援型 APT の高度化、AI の悪用）と、それに伴う**国家、経済、社会の安全保障の不可分性**が共通認識として確認されました。日本が推進する**能動的サイバー防御（ACD）やセキュリティ・クリアランス制度**といった新法制を成功させるには、**強固な官民連携**と、**PQC（耐量子計算機暗号）**、**AI セキュリティ**などの新興技術リスクを前提とした**グローバル連携と対策の加速**が喫緊の課題であることが強調されました。特に、データ流通と信頼を担保する**トラストフレームワーク**の国際的な相互運用性の確保が、日本のデジタル競争力と安全保障の基盤となると結論づけられました。

メインセッションの要約（Day 1 - Day 4）

Day 1 (10 月 28 日)：国家・経済安全保障と各国政府の取り組み

基調と総論:慶應-MITRE 共催の下、シンポジウムが開始。サイバー攻撃が**国家・経済・社会のレジリエンス**に与える甚大な影響が強調されました。各国政府・国連から、英国の製造業攻撃、EU の法規制強化（NIS2）、国連の恒久メカニズム設立など、具体的な脅威情勢と国際的な対応状況が共有されました。

日本の戦略: 元 DNI（米国）が中国の **Volt Typhoon/Salt Typhoon** の脅威を警告し、日本の ACD 法制が限定的である点を指摘。日本の関係省庁（内閣サイバー官、防衛省、経産省、警察庁など）は、それぞれの所管分野で ACD 法制の実装に向けた体制整備、情報共有の強化、及び重要インフラ（医療、交通、金融等）の防御力向上策を説明しました。

Day 2 (10 月 29 日)：国家安全保障、国家クラウド、情報共有、AI・量子ネクサス

クラウドと主権: 米国 FedRAMP の元ディレクターが、日本における**「リスクベース」**のクラウド認証プログラム（J-RAMP）導入の必要性を提言。パネルでは、**ソブリンクラウド**を「国内の法規制・運用・知識の主権」として定義し、ハイパースケーラー依存のリスク（デジタル赤字、単一障害点）を回避するため、国産クラウド育成と分散型アーキテクチャの重要性が議論されました。

インテリジェンスと能動的サイバー防御(ACD): 情報共有はサイバーディフェンスに不可欠であり、**セキュリティ・クリアランス**と**強固な ID 基盤**がその前提となると強調されました。

新興技術: UNIDIR（国連軍縮研究所）は、**サイバー、AI、量子**が相互に影響しあう「ネクサス」**を形成していると指摘。特に、AI の攻撃利用（フィッシング自動生成）や、量子コンピュータによる** HNDL（Harvest Now, Decrypt Later）**脅威への**統合的ガバナンスの必要性が共有されました。

Day 3 (10 月 30 日)：経済安全保障、重要インフラ、セキュリティ・クリアランス

経済安保の構造: 経済安全保障が長期的な**米中対立**の構図の中で、**平時と有事の境界が曖昧なグレーゾーン**の課題となり、民間企業が主たるアクターとなっている現状が示されました。

重要インフラ防御: エネルギー分野では、EV や太陽光などの分散型電源（DER）の増加により、**従来の境界防御が機能不全**しつつあると分析。OT/IT の連携、**サイバーレンジ演習**を通じた対応力強化、**サプライチェーン管理**の重要性が強調されました。

新法制の実務: 重要経済安全保障情報活用法と**サイバー対処能力強化法（ACD）**が議論の中心となりました。ACD の実効性には、ハックバックの議論にとどまらない、**情報共有や抑止手段を組み合わせた「受け身ではない防御」の定義と、機密情報を扱うセキュリティ・クリアランス制度の運用**が不可欠であることが強調されました。

Day 4 (10 月 31 日)：社会保障、データスペース・トラスト・国際標準

データスペース応用: バッテリーパスポートや **CO2 排出量トレーサビリティ**、**医療データ**など、具体的な産業分野でのデータスペースの応用事例が紹介されました。データスペースでは、AI の活用が進む一方で、**リーガルテック**による規制の機械可読化や**データガバナンスの成熟度**向上が必要不可欠であることが強調されました。

デジタル ID とトラスト: EU の政策担当者が、**EUDI ウォレット**と**トラストサービス**の国際展開を説明。GLEIF、アジア PKI コンソーシアム、慶應義塾大学は、**LEI**（法人識別子）や **ISO 標準**を活用した**グローバルなトラストフレームワーク**（ITL：インターナショナルトラステッドリスト）を構築し、各国・地域間のトラストサービス（電子署名など）の**相互承認**を可能にするための具体的な取り組みを紹介しました。

パラレルセッションの要約（Day 2 - Day 4)

Day 2 パラレルセッション：データ取引と OT セキュリティ、ソブリンクラウド

データ取引（DSA/JDTF/DPFJ）:「情報銀行」の反省を踏まえ、**データ取引市場**を「信頼の公証（ノータリー）機能」として位置づけ、データ利用権を契約としてデータに紐付け、PKI などのトラスト技術で流通を担保する**日本型データスペース**の枠組みが詳細に議論されました。

OT セキュリティ（RRI/JICSS）: 製造業の**製品関連データ（PRD）において、トラストワースネス（能力評価）の重要性が強調されました。OT システム（製造業）の国際競争力**を高めるためには、IT と OT のセキュリティ対策を融合させ、国際標準（IEC 62443 など）に準拠したレジリエンスを確保する必要があるとされました。

ソブリンクラウド（CyLogic）: FedRAMP High 相当のセキュリティを持つ**「真のソブリンクラウド」**は、単なる国内 DC ではなく、**運用・インフラの完全な自立性**を伴うことが強調され、分散型アーキテクチャの優位性が実証されました。

Day 3 パラレルセッション：防衛技術、PQC、サイバーハイジーン

防衛技術と RMF: 防衛省の **RMF（リスクマネジメントフレームワーク）適用拡大方針が紹介されました。RMF は米国の標準であり、日本の防衛産業がこれに対応するための人材育成**と、サイバー防御能力の**土台**となる強固なセキュリティ体系の構築が課題とされました。

PQC 移行の実務: PQC 移行の要件、国際標準化動向、および**ハイブリッド暗号**による移行期間中の安全確保策が説明されました。

サイバーハイジーン（JCIC）: 最近のランサムウェア被害の多くは「うっかり」「まあ大丈夫だろう」といった人的要因と基本対策の怠り**で防げたものであり、従業員一人ひとりの**「圧倒的な当事者意識」**と**継続的な訓練を通じてサイバーハイジーンを徹底することの重要性が訴えられました。

Day 4 パラレルセッション：デジタルトラスト、データスペース、PQC 移行の実態

データ流通の信頼: IPA とデータ社会推進協議会（DSA）が、**DFFT** 実現の基盤として、**データスペース**（共通のルールで安全にデータを流通させるエコシステム）の構築を推進していることを紹介。EU の **EUDI ウォレット**と**電子属性証明（EAA）**などのトラスト技術が、国境を越えたデータ取引の信頼基盤となる可能性が示されました。

脅威の最前線: Google とトレンドマイクロは、**ゼロデイのコモディティ化**、**国家支援 APT** の**正規ツール悪用**（Living off the Trusted Land）、AI による**攻撃生産性の向上**といった最新の脅威動向を詳説。防御側は **AI の活用**と**「侵入前提」**での対応強化が必須であると結論づけました。

PQC 移行: 量子コンピュータ開発者の見解は時期について慎重である一方、**金融庁**など各国規制当局は **2030 年代半ば**の **PQC 移行完了**を目標として掲げており、**「今すぐクリプトインベントリ（暗号の棚卸し）から始める」**ことの緊急性が強調されました。

Contents

※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.

※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

Main Session

1 DAY 1: October 28 | West School Building 1F West Hall

1.1 D1-S1-1 Opening

D1-S1-1 Jun Murai (Senior Advanced Research Project Professor, Keio University)	D1-S1-1 村井 純 (慶應義塾大学 特別特区特任教授)
1. Professor Murai welcomes participants to the 15th Keio International Cyber Security Symposium and introduces Keio's multi-layer research structure (Cyber Security Research Center and CCRC under KGRI). 2. He emphasizes the value of holding this symposium annually and highlights this year's theme: Cybersecurity for Digitized National, Economic, and Societal Security through Global Multilateral Public-Private Partnership. 3. The symposium gathers leaders from government, industry, and academia worldwide to discuss evolving cybersecurity and digital trust issues. 4. Murai expresses gratitude to all long-time supporters, including industry partners, universities, and especially MITRE as the co-organizer. 5. He acknowledges participation from 11 embassies and the United Nations, emphasizing the importance of international cooperation. 6. He introduces distinguished keynote and special speakers from Japan, the US, Europe, and other regions, including former national security leaders and senior government officials. 7. Speakers represent organizations such as Japan's National Cyber Security Office, US intelligence community, East Japan Railway Company, Stanford University, RUSI, US Federal CIO office, and the European Commission. 8. Murai stresses that the conference's value comes from the contributions and discussions of all speakers and participants. 9. He underscores that in 2025 cybersecurity cannot be addressed by any single entity or country; only collaboration and mutual understanding make progress possible.	1. 村井教授は第 15 回慶應国際サイバーセキュリティシンポジウムの参加者を歓迎し、慶應義塾大学の多層的研究体制（KGRI 傘下のサイバーセキュリティ研究センター及び CCRC）を紹介した。 2. 同教授は本シンポジウムの年次開催の意義を強調し、今年のテーマ「グローバルな官民連携による国家・経済・社会のデジタル化に伴うサイバーセキュリティ」を提示した。 3. 本シンポジウムは世界各国の政府・産業界・学界のリーダーを集め、進化するサイバーセキュリティとデジタル信頼の問題を議論する。 4. 村井教授は産業界パートナー、大学、特に共催者である MITRE を含む長年の支援者全員に謝意を表明した。 5. 11 の大使館と国連の参加を認め、国際協力の重要性を強調した。 6. 日本、米国、欧州、その他地域から、元国家安全保障責任者や政府高官を含む著名な基調講演者・特別講演者を紹介した。 7. 講演者は日本の国家サイバーセキュリティセンター、米国情報機関、東日本旅客鉄道、スタンフォード大学、RUSI、米国連邦 CIO 事務局、欧州委員会などの組織を代表する。 8. 同教授は、本会議の価値は全講演者・参加者の貢献と議論にあると強調した。 9. 彼は、2025 年のサイバーセキュリティは単独の組織や国では対処できず、協力と相互理解によってのみ進展が可能だと強調する。 10. 彼は、今年のシンポジウムが国際的なネットワークを強化し、過去 14 回の開催で築かれた成功の伝統を継続することを望んでいる。

10. He hopes this year's symposium will strengthen international networks and continue the successful tradition established over the past 14 iterations.	

1.2 D1-S1-2 Opening

D1-S1-2 Wen Masters (Vice President, MITRE)	D1-S1-2 ウェン・マスターズ (MITRE、副社長)
1. Wen Masters, Vice President for Cyber Technologies at MITRE, welcomes all participants to the 15th International Cybersecurity Symposium on behalf of MITRE. 2. She highlights Japan's new active cyber defense (ACD) law as a major strategic shift enabling proactive measures, stronger deterrence, improved critical infrastructure protection, and deeper cross-sector information sharing. 3. ACD underscores that cybersecurity is inseparable from national, economic, and societal security—longstanding themes of the symposium. 4. She identifies three major challenge areas: critical infrastructure cybersecurity, safe and secure AI, and data protection in the era of quantum computing. 5. Critical infrastructure systems—energy, transport, communications, finance, healthcare, manufacturing, food and water—face increasing attacks from nation-states, criminals, and terrorists. 6. MITRE's recent tabletop exercise with 200 participants from 70 organizations showed that isolated incident responses are insufficient, and interdependencies across sectors must be understood for effective crisis operations. 7. Strengthening emergency communications and preparing the cybersecurity workforce are essential for managing prolonged disruptions. 8. AI presents both enormous benefits and significant risks; professionals must address AI system vulnerabilities, adversarial behaviors, and build safe and secure AI through policy and technological measures. 9. Quantum computing threatens current	1. MITRE のサイバー技術担当副社長であるウェン・マスターズは、MITRE を代表して第 15 回国際サイバーセキュリティシンポジウムの参加者全員を歓迎する。 2. 彼女は日本の新たな能動的サイバー防御（ACD）法を、積極的措置、より強力な抑止力、重要インフラ保護の強化、そしてより深い分野横断的な情報共有を可能にする主要な戦略的転換として強調する。 3. ACD は、サイバーセキュリティが国家・経済・社会の安全保障と不可分であることを強調している。これはシンポジウムの長年のテーマでもある。 4. 彼女は三つの主要課題領域を指摘した：重要インフラのサイバーセキュリティ、安全でセキュアな AI、量子コンピューティング時代におけるデータ保護である。 5. エネルギー、運輸、通信、金融、医療、製造、食糧・水といった重要インフラシステムは、国家、犯罪者、テロリストによる攻撃の増加に直面している。 6. MITRE が 70 組織から 200 名参加した最近の模擬訓練では、単独のインシデント対応では不十分であり、効果的な危機管理にはセクター間の相互依存関係を理解する必要があることが示された。 7. 長期化する混乱を管理するには、緊急通信の強化とサイバーセキュリティ人材の育成が不可欠である。 8. AI は多大な利益と重大なリスクの両方をもたらす。専門家は AI システムの脆弱性や敵対的行動に対処し、政策と技術的措置を通じて安全でセキュアな AI を構築しなければならない。 9. 量子コンピューティングは素因数分解を高速化することで現行暗号システムを脅かし、敵対者が現在の暗号を解読可能にする。敵対者は既に将来の解読に向けデータ収集を進めている。 10. 彼女は量子耐性暗号への移行加速を求め、シンポジウム全体を通じた活発な議論と意見交換を促している。

cryptographic systems by enabling rapid prime factorization, allowing adversaries to crack today's encryption—and adversaries are already harvesting data for future decryption. 10. She calls for accelerated migration to quantum-safe cryptography and encourages active discussion and idea exchange throughout the symposium.	

1.3 D1-R2-1 Remarks from Keio University

D1-R2-1 David Farber (Visiting Professor, Keio University)	D1-R2-1 デイビッド・ファーバー（慶應義塾大学 客員教授）
1. Professor David Farber briefly introduces ongoing work at Keio University's Cyber Civilization Research Center (CCRC), led by himself and Professor Jun Murai. 2. He explains that the Internet was originally designed for high availability and fault tolerance, but not for resilience, reliability, or security—issues that now create major challenges. 3. He notes that both software and hardware foundations of current systems are insecure, which contributes to widespread cybersecurity problems. 4. CCRC focuses on two core missions: education and research, including supervising graduate students and exploring future secure system designs. 5. He cites a recent thesis on securing medical information as an example of practical and socially relevant research at CCRC. 6. Farber stresses the need to build robustness and security into emerging technologies rather than reacting after vulnerabilities appear. 7. He highlights upcoming challenges such as quantum computing and widely adopted virtual reality systems, which raise new security and privacy concerns. 8. A key goal of CCRC is to anticipate technological evolution and identify both societal and technical issues before they become critical. 9. He emphasizes the importance of educating future leaders—not only engineers but also managers, finance specialists, and policymakers.	1. デイビッド・ファーバー教授は、慶應義塾大学サイバー文明研究センター（CCRC）における自身の研究と村井淳教授の研究について簡潔に紹介する。 2. インターネットは当初、高可用性と耐障害性を目的に設計されたが、回復力・信頼性・セキュリティは考慮されていなかったと説明する。これらが現在、重大な課題となっている。 3. 現行システムのソフトウェア基盤とハードウェア基盤の双方が不安全であり、これが広範なサイバーセキュリティ問題の一因となっていると指摘する。 4. CCRC は教育と研究という二つの核心的使命に焦点を当てている。これには大学院生の指導や将来の安全なシステム設計の探求が含まれる。 5. 彼は CCRC における実践的かつ社会的に意義のある研究の例として、医療情報の保護に関する最近の論文を挙げた。 6. ファーバー教授は、脆弱性が現れてから対応するのではなく、新興技術に堅牢性と安全性を組み込む必要性を強調した。 7. 量子コンピューティングや普及が進む仮想現実システムなど、新たなセキュリティ・プライバシー問題を提起する今後の課題に言及している。 8. CCRC の主要目標は、技術進化を予測し、社会的・技術的問題が深刻化する前に特定することだ。 9. 将来のリーダー育成の重要性を強調している。対象は技術者だけでなく、管理者、金融専門家、政策立案者も含む。 10. ファーバー教授は結論として、非技術分野の学生を含む有能な人材を育成することが、大学や CCRC のような研究センターにとって不可欠な役割だと述べている。

10. Farber concludes by noting that developing talented students, including those from non-technical fields, is an essential role of both universities and research centers like CCRC.	

1.4 D1-R2-2 Remarks from Keio University

D1-R2-2 Kohei Ito (President, Keio University)	D1-R2-2 伊藤 公平 (慶應義塾大学 塾長)
1. President Kohei Ito warmly welcomes distinguished guests, colleagues, and students to Keio University's Mita Campus for the International Cybersecurity Symposium, co-hosted with MITRE. 2. He notes that the symposium began in 2016 and has been held annually in the same venue for nine years. 3. President Ito recognizes ambassadors and senior diplomatic representatives from the UK, Australia, France, Israel, Norway, Portugal, Lithuania, the EU, Germany, Canada, and the United Nations, as well as Japanese government officials. 4. He explains that the U.S. Ambassador cannot attend due to the U.S. President's visit, but the Deputy Chief of Mission will deliver remarks later in the week. 5. He highlights Keio's leadership in cybersecurity through experts such as Professors David Farber, Jun Murai, and Satoru Tezuka—who now serves as Chairman of Japan's Personal Information Protection Commission. 6. Keio plays a central national role not only in cybersecurity but also in advancing digital trust initiatives across Japan. 7. President Ito, a quantum computing expert, recounts the field's evolution from seeming science fiction 27 years ago to today's functioning quantum computers. 8. He describes Keio's Quantum Computing Center—established seven years ago with IBM—as a leader in quantum algorithms and software development. 9. The center collaborates with major financial institutions (MUFG, Mizuho, SMTB), which are interested not only in computational advances	1. 伊藤塾長は、MITRE と共催する国際サイバーセキュリティシンポジウムに際し、三田キャンパスに集う来賓、同僚、学生を温かく迎えた。 2. 同シンポジウムは 2016 年に始まり、9 年間同じ会場で毎年開催されていると述べた。 3. 伊藤塾長は、英国、オーストラリア、フランス、イスラエル、ノルウェー、ポルトガル、リトアニア、EU、ドイツ、カナダ、国連の大使及び上級外交代表、ならびに日本政府関係者を出席者として紹介した。 4. 大使は米国大統領の来訪のため出席できないが、副大使が今週後半に挨拶を行うと説明した。 5. デイビッド・ファーバー教授、村井純教授、手塚悟教授（現・個人情報保護委員会委員長）ら専門家を通じた慶應義塾のサイバーセキュリティ分野における主導的役割を強調した。 6. 慶應義塾大学はサイバーセキュリティ分野だけでなく、日本全体のデジタル信頼性推進においても中核的な役割を担っている。 7. 量子コンピューティングの専門家である伊藤学長は、27 年前には SF のように思われたこの分野が、今日では実際に機能する量子コンピューターへと進化した経緯を語った。 8. 慶應義塾大学量子コンピューティングセンター（7 年前に IBM と共同設立）は、量子アルゴリズムとソフトウェア開発の分野で主導的役割を果たしていると説明した。 9. 同センターは主要金融機関（三菱 UFJ、みずほ、SMTB）と連携しており、計算能力の向上だけでなく、量子技術を利用したサイバー脅威への防御にも関心を持っている。 10. 彼は、量子攻撃への防御と、安全なサイバーセキュリティのための量子技術活用の両面において、量子技術の理解が重要だと強調している。会議期間中には、耐量子計算機暗号技術のライブデモも実施される予定だ。

but also in defending against quantum-enabled cyber threats. 10. He emphasizes the importance of understanding quantum technologies both for defending against quantum attacks and for leveraging quantum capabilities for secure cybersecurity, including a live post-quantum cryptography demonstration available during the conference.	

1.5 D1-R3-1 Remarks from Japanese Government (Ministerial)

D1-R3-1 HIRAI Takuya (Former Minister of Digital Agency, member of the House of Representatives)	D1-R3-1 平井 卓也 (前デジタル大臣、衆議院議員)
1. The speaker emphasizes that cybersecurity fundamentally relies on timely and effective information sharing, especially as attackers increasingly share information. 2. He reflects on his long involvement in Japan's digital and cybersecurity legislation, starting with the 2000 IT Basic Law and later the 2014 Basic Cybersecurity Law. 3. The 2014 law had limitations—especially regarding coordination between national security and police authorities—highlighting the need for seamless national and global cybersecurity structures. 4. Japan has now established a more comprehensive national structure for cybersecurity, but securing sufficient authority and resources remains essential. 5. He stresses that users must be obligated to use the internet safely, noting the misconception that the internet is "free" despite significant national spending on cybersecurity. 6. Companies tend to treat cybersecurity as a cost rather than a strategic investment, often spending far less than governments relative to revenue. 7. Technology itself has no inherent good or evil; risks arise from how humans use technologies such as AI and quantum computing. 8. A growing societal concern is excessive	1. 2000 年の IT 基本法制定以来、一貫してデジタル・サイバー分野に関わってきた経緯を説明している。 2. 2014 年に議員立法でサイバーセキュリティ基本法を制定したが、当時は国内対応中心で、安全保障領域までシームレスに扱えない限界があったと述べている。 3. 約 10 年を経て、国内から国家安全保障までシームレスに扱える法体系が初めて整備され、国家としてのサイバーセキュリティ体制が法的に整ったと評価している。 4. サイバーセキュリティ投資を企業が「コスト」と見るか「戦略的投資」と見るかが重要であり、日本企業は売上の 1～2%も投じていない現状を指摘している。 5. インターネット利用や量子コンピューティング時代では、テクノロジーを活用するためのコスト＝サイバーセキュリティ投資が不可欠であると強調している。 6. AI 導入が進むなか、最終的な意思決定に AI をどこまで関与させるかという問題が重大であり、AI の判断に人間が無自覚に依存する危険性を懸念している。 7. 有権者の一部が投票先を AI に尋ねていた事例や、政党によって AI の学習状況が偏る問題（テキスト公開量や PDF 化・コピーガードの影響）を紹介している。 8. ある国が長文情報を日本語で発信し AI 学習に利用されている可能性を指摘し、AI 時代における「認知戦」としての新たなセキュリティ課題を提起している。 9. 技術的攻撃だけでなく、コンテンツを通じた攻撃・影響（情報操作）の安全性を重視すべきと主張している。 10. AI がもたらす利便とリスクの双方を踏まえ、人間のあり方や国家の安全保障を見据えつつ、サイバーセキュリティ分野の課題がより広がっていると結んでいる。

reliance on AI for judgment, including during elections, where people increasingly defer decisions to AI systems. 9. AI training data can embed ideological biases, including from foreign actors generating large volumes of machine-oriented text—raising new types of security risks. 10. As society enters the era of integrated digital technologies (internet, AI, quantum), cybersecurity must expand to address human decision-making, content safety, and broader societal impacts.	

1.6 D1-R3-2 Remarks from Japanese Government (Ministerial)

D1-R3-2 Satoru Tezuka (Chairman of the Personal Information Protection Committee)	D1-R3-2 手塚 悟 (個人情報保護委員会 委員長)
1. Chairman Satoru Tezuka introduces himself as Chair of Japan's Personal Information Protection Commission (PPC) and explains he will discuss Japan's current situation and the evolution toward DFFT 2.0 (Data Free Flow with Trust). 2. He highlights that digital society requires trusted data flows, and DFFT 2.0 aims to strengthen freedom and trust in cross-border data exchanges. 3. Tezuka explains the concept of "cyberspace" in Japan as a system grounded in freedom and trust, with an emphasis on secure and reliable data circulation. 4. He outlines key issues: data generation, organizational processes, and technical mechanisms—all of which must be addressed to enable safe and secure data use. 5. He presents a three-layer cyberspace architecture: * Base registries providing authoritative identity and attribute information * Public trust layers issuing trusted credentials * Trusted data distribution layers enabling secure data exchange 6. The top layer of this architecture supports product-level data applications, built on trust	1. 個人情報保護委員会（PPC）委員長として、DFFT（Data Free Flow with Trust）およびその発展形である DFFT2.0 について述べる趣旨を提示している。 2. デジタル社会の進展に伴い、個人情報を含むデータの安全かつ円滑な越境流通の重要性が高まり、日本では DFFT の概念が重視されていると説明している。 3. DFFT は「自由と信頼のルールに基づくデータ流通の国際協力」であり、信頼性を確保する基盤として、電子署名・電子認証を中心とした三層構造のデータ流通モデルを紹介している。 4. 三層構造では、最下層に個人情報保護法などの法律、次に公的登録レイヤーや ID・証明書の信頼層、最上層に産業別データ空間が位置づけられる構造を提示している。 5. こうした信頼インフラにより、産業・医療・金融などの分野でデータを安全に活用し、自動化・効率化が可能になると述べている。 6. 個人データ越境移転では、各国制度差による調査コスト・交渉コスト・継続的遵守コストが発生するが、CBPR や MCC などの国際的トランスファースキームにより大幅削減が可能と示している。 7. DFFT の国際運用に向け、G7・グローバルプライバシーアセンブリ（GPA）などで各国当局と積極的に協力・情報交換していることを紹介している。 8. 日本では「データ保護」と「データ活用」を対立関係とみなす傾向があり、これがビジネスでのデータ利活用を阻害しているため、保護法を"土台"とする新しい認識へ転換すべきだと主張している。 9. 個人データ保護ツール（CBPR、モデル契約条項など）

frameworks below. 7. Tezuka reviews Japan's national data-protection legal system, noting that high-level tools such as adequacy arrangements enable smooth international data exchange. 8. When these tools cannot be applied, lower-layer mechanisms—such as standard contractual clauses (SCC/MCC)—provide additional transfer options. 9. He stresses that Japanese society must shift its perception of personal data: data protection and data utilization should not be viewed as opposing forces but as mutually reinforcing. 10. He concludes that developing interoperable, cross-border data-transfer frameworks and establishing strong global data-governance systems are essential for trusted digital societies under DFFT 2.0.	を非個人データ領域にも拡張し、データ全般で DFFT を運用可能とするための枠組みが DFFT2.0 の核心だと述べている。 10. 最終的に、デジタルエコノミーの信頼基盤をグローバルに構築するため、DFFT2.0 の推進が不可欠であると締めくくっている。

1.7 D1-R4-2 Remarks from each of the governments and United Nations

D1-R4-2 Emil Levendoğlu (Chargé d'Affaires, British Embassy, Tokyo)	D1-R4-2 エミール レベンドールー（駐日英国公使）
1. The speaker expresses gratitude to Keio University for the invitation and notes the importance of gathering leaders, experts, and industry figures to reinforce shared cyber resilience. 2. He highlights major progress in Japan over the past year, including active cyber defense legislation, the creation of the National Cyber Security Office, and an upcoming new cyber strategy. 3. Despite these advances, 2025 has seen an unprecedented surge in cyberattacks targeting the UK, exposing vulnerabilities in critical sectors. 4. He describes the severe cyberattack against Jaguar Land Rover, which halted production, impacted over 30,000 employees and suppliers, and caused losses up to £50 million per week. 5. The UK government had to issue a £1.5 billion loan guarantee to stabilize the affected supply chain, showing how deeply cyber incidents can harm national resilience.	1. 駐日英国公使として、慶應義塾大学への謝意を示し、専門家・政府・民間が一堂に会する場の重要性を強調している。 2. 日本と英国のサイバーパートナーシップはこの 1 年で大きく進展し、日本では能動的サイバー防御法制の整備など前進が見られたと述べている。 3. 2025 年に英国が前例のない大規模サイバー攻撃を受け、小売・製造などの重要分野が深刻な影響を受けた事例（ジャガー社の生産停止やサプライチェーン混乱など）を紹介している。 4. サイバー攻撃は全ての国が直面しうる脅威であり、日本も例外ではないと警鐘を鳴らしている。 5. サイバーセキュリティはもはや専門分野ではなく国家安全保障の根幹となっていると位置づけている。 6. あらゆる製品・サービスにサイバーセキュリティ戦略が必要であり、英国でもクラウド優先戦略や攻撃国への抑止・対応能力の構築を進めていると述べている。 7. DFFT 実現のためには国際協力が不可欠であり、各国が役割分担を明確にし、重要データ・サービスの特定と優先順位付けを進める必要があると強調している。 8. 英国は規制当局として重要供給網の特定、インフラ調査、大学との連携によるサイバー人材育成を推進しており、

6. He emphasizes that cybersecurity is no longer a niche issue—it is a core national security imperative affecting all countries, sectors, and systems. 7. Governments must ensure every public organization has a robust cybersecurity strategy, act collectively against malicious actors, and eliminate bureaucratic barriers that slow information sharing. 8. Public–private collaboration is essential: industry must be integrated with government, while government provides national frameworks, services, and clear accountability. 9. The UK is advancing a Cybersecurity and Resilience Bill to regulate managed service providers and designate critical suppliers previously outside the formal “critical infrastructure” scope. 10. He concludes by stressing the need for harmonized regulation, secure-by-design technologies, and a diverse cyber workforce—achievable only through openness, collaboration, and difficult but necessary conversations.	規制の国際的な調和（ハーモナイゼーション）も重要と述べている。 9. セキュア技術を国際展開するにはオープンな議論や協働が不可欠であり、困難はあるが協力によって成果を期待できると述べている。 10. 最後に、参加者への感謝を述べ、共により安全で強靭なデジタル未来を築こうと呼びかけて締めくくっている。

1.8 D1-R4-3 Remarks from each of the governments and United Nations

D1-R4-3 Justin Hayhurst (Ambassador, Australian Embassy Tokyo)	D1-R4-3 ジャスティン・ヘイハースト (在日オーストラリア大使館大使)
1. Ambassador Justin Hayhurst congratulates Keio University for its long-standing global engagement and its growing leadership role in cybersecurity. 2. He stresses that a secure Japan is essential for a secure Asia and a stable world, making Japan a critical lynchpin in regional and global cybersecurity. 3. Australia aims to become the world’s most cyber-secure nation and focuses on safe technology, threat sharing, infrastructure protection, private-sector engagement, and sovereign cyber capability. 4. Cyber threats are borderless, fast-moving, and transnational, coming from both state and non-state actors; they threaten trust and stability in digital economies.	1. 慶應大学が歴史ある日本でサイバーセキュリティ分野を強化していることに祝意を述べ、日本の成功はアジアと世界の成功につながると強調している。 2. デジタル接続とサイバーリスクの増大の中、日本が幅広いサイバー政策でリーダーシップを発揮している点を評価し、オーストラリアとして協力を深めたいと述べている。 3. オーストラリアは 2030 年に「世界で最も安全なサイバー国家」になるという戦略を掲げ、日本や英国など同志国と連携し、サイバーレジリエンス強化に取り組んでいると説明している。 4. デジタルインフラの信頼性確保はグローバル経済の基盤であり、AI の急速な普及に伴いサイバーセキュリティ上の課題が一段と複雑化していると指摘している。 5. サイバー脅威は国境を越えるため、単独の国では対応できず、東南アジアを含む広域での協力が必須であると強調している。 6. 日豪などでジョイント・サイバーセキュリティ・アドバイザリーを

5. Cybersecurity has become central to Australia's foreign and security policy, especially through cooperation with Japan in Southeast Asia and the Pacific. 6. He cites joint actions such as the 2025 "SALT Typhoon" advisory with Japan and other partners to call out malicious cyber activity and raise awareness. 7. Japan is regarded as a trusted and influential partner; its increasing cyber leadership makes collaboration, information sharing, and coordinated responses even more important. 8. Cybersecurity must be a whole-of-nation effort—protecting infrastructure, safeguarding data, and maintaining economic confidence, involving not only experts but all sectors of society. 9. Public–private partnerships are indispensable; Australia emphasizes that industry collaboration is not optional, and a broader "culture of cybersecurity" is needed. 10. Japan's emerging cyber threat information-sharing framework offers new opportunities for deeper cooperation with Australia, supporting secure connectivity and stronger national defenses.	発足させ、悪意あるサイバー行動に対して共同で注意喚起や対抗措置を取っている事例を紹介している。 7. 日本の高度な通信能力を評価し、新しい法制度のもと、両国でサイバー対応とレジリエンス強化を共同で進めたいと述べている。 8. 重要インフラへの攻撃やリスクは深刻化しており、社会全体で責任ある行動と協力が欠かせないと指摘している。 9. オーストラリアでは政府・産業界・大学が連携する「管理パートナーシップ」方式を重視し、サイバーセキュリティは単なる技術導入ではなく"構築と文化形成"が必要と述べている。 10. 日本・オーストラリア・他国が協力し、安全で強靭なサイバースペースを構築するため、社会全体へ認識を広げることの重要性を訴えて締めくくっている。

1.9 D1-R4-6 Remarks from each of the governments and United Nations

D1-R4-6 Philippe SETTON (Ambassador of France in Japan)	D1-R4-6 フィリップ・セトン (駐日フランス大使)
1. Ambassador Philippe Setton thanks Keio University for the invitation and expresses support for the 15th International Cybersecurity Symposium. 2. He emphasizes that today's cybersecurity challenges require collective, interdisciplinary, and multi-stakeholder cooperation to maintain a free, stable, and secure cyberspace. 3. France has articulated a clear national vision for cyberspace, beginning with the 2018 Paris Call for Trust and Security in Cyberspace, now supported by 81 states, hundreds of civil-society groups, and major companies. 4. The Paris Call promotes principles such as	1. 第 15 回サイバーセキュリティ国際シンポジウムへの参加と、フランス大使館が毎年支援していることへの喜びを示している。 2. サイバー脅威は多くのアクターが関与する複雑な問題であり、各国が集合的に対応することが不可欠だと強調している。 3. フランスは「パリ呼びかけ（Paris Call）」を通じて、信頼性があり安定したサイバースペースの実現を国際的に呼びかけており、81 カ国と多くの企業が支持していると述べている。 4. パリ呼びかけでは、インフラ・個人保護、選挙の保護、知財保護、不拡散、国際規範づくりなど 9 つの原則を提示し、リスク低減と不安定化防止に寄与していると説明している。 5. フランスの 2030 年投資戦略では、サイバー人材育成を優先分野として位置づけ、サイバーセキュリティ文化を社会全体に根付かせる取り組みを進めている。

protecting individuals and infrastructure, securing electoral processes, enabling responsible regulation, and safeguarding privacy to reduce cyber instability. 5. These principles continue to guide France's international engagement and shape its global cyber diplomacy. 6. Nationally, cybersecurity is a core component of the France 2030 strategy, which includes investment in education, training, research, innovation, and broader cybersecurity culture. 7. France participates actively in multilateral forums, including the UN's new global mechanism for inclusive cybersecurity discussions and EU initiatives. 8. France and the UK jointly launched a process to develop guiding principles and policy options for governments, industry, and civil society to address specific cyber challenges. 9. He highlights the essential role of the private sector, which must follow clear regulatory frameworks, adopt cybersecurity-by-design, and promote cyber education. 10. As cyber threats grow in number and complexity, only coordinated defensive and proactive efforts across society can build lasting cyber resilience.	6. OECD や EU など国際枠組みの中でも新しいメカニズム構築を支援し、責任あるアクターのコミュニティ形成を推進していると述べている。 7. 日本がパリ呼びかけにコミットしていること、また民間セクター・市民社会の参加が不可欠であることに対して謝意を示している。 8. 明確な規制枠組みの提示により、安全なデジタル経済の実現や研究・イノベーションの促進が可能になると指摘している。 9. 「サイバーセキュリティ・バイ・デザイン」の統合や若年層への教育など、社会全体でのサイバーリテラシー向上の重要性を強調している。 10. サイバー攻撃の増加と複雑化を背景に、生産的かつ継続的な努力こそがサイバーレジリエンスを実現する唯一の方法であると締めくくっている。

1.10 D1-R4-8 Remarks from each of the governments and United Nations

D1-R4-8 Gilles Beschoor Plug (Ambassador, the Kingdom of the Netherlands to Japan)	D1-R4-8 ヒルス・ベスホー・プルッフ (駐日オランダ王国大使)
1. Ambassador Plouffe congratulates Keio University on the 15th Cybersecurity Symposium and highlights Keio's historical Dutch origins and long-standing ties between Japan and the Netherlands. 2. She reflects on the 425-year Japan–Netherlands relationship, noting that scientific advancements such as medicine and astronomy entered Japan historically through Dutch channels. 3. Unlike past tangible challenges (disease, drugs, trade competition), today's cyber threats are less physical, harder to attribute, and come	1. 第 15 回サイバーセキュリティ国際シンポジウムの開催を祝し、歴史ある慶應義塾大学で発言する機会への感謝を述べている。 2. 慶應義塾大学とオランダは歴史的な知識交流の関係にあり、425 年の長い国交を基盤として協力を深めてきたと回顧している。 3. 現代のサイバー脅威は国家主体か否かも不明瞭で、出所が特定しにくいため、官民学が一体となり、同志国が連携して対応する必要があると強調している。 4. ウクライナ戦争、ビール会社へのランサムウェア攻撃など、現実の攻撃事例を挙げつつ、デジタル・サイバー脅威が深刻化していると述べている。 5. サイバー空間における規範の整備と、アクターの責任を追

from both state and non-state actors. 4. She stresses the need for multinational, multi-stakeholder cooperation among academia, governments, and industry to meet cyber challenges effectively. 5. The Netherlands strongly supports Keio's efforts and emphasizes the growing intrusiveness of digital risks, including ransomware and threats to vital industries. 6. Effective response requires developing cyberspace governance norms and establishing accountability for malicious actors. 7. She welcomes Japan's new cyber legislation as an important step in strengthening resilience and building partnerships. 8. The Netherlands sees secure, resilient supply chains—especially in technologically advanced sectors like semiconductors—as a shared priority with Japan. 9. She highlights ongoing cooperation through initiatives such as ASEAN capacity building, Japan's Cybersecurity Competency Center, and the Dutch-Japanese "D6" collaboration. 10. She concludes by emphasizing the urgency of moving from discussion to concrete international action to confront serious global cyber challenges.	及できるルールづくりが重要であると指摘している。 6. 日本で新しいサイバー法制が実現したことを歓迎し、サイバー防御の強化が各国で必要と述べている。 7. 社会全体のサプライチェーン防衛が重要であり、日本の半導体分野で OT ガイドラインが作成中であることを評価している。 8. 単独での防御は不可能であり、二国間のみならず多国間での協力が不可欠とし、日本の ASEAN サイバー能力構築センターの取り組みも支持している。 9. オランダ首相の訪日と慶應での講演を紹介し、日蘭のセキュリティ・イノベーション協力やデジタルコラボレーション、サイバー教育の強化を進めていると述べている。 10. 今後 1 年間、さらに協力を拡大し、サイバー分野の課題に共同で取り組む意欲を示して締めくくっている。

1.11 D1-R4-15 Remarks from each of the governments and United Nations

D1-R4-15 Gilberto JERÓNIMO (Ambassador, Embassy of Portugal in Japan)	D1-R4-15 ジルベルト・ジェロニム（駐日ポルトガル大使）
1. Ambassador Gilberto Jeronimo thanks Keio University for hosting the symposium and introduces Portugal's perspective on cybersecurity, emphasizing critical infrastructure protection. 2. He explains that Portugal has adopted a new cybersecurity legal framework aligned with EU standards to enhance prevention, resilience, and national response capacity. 3. The Portuguese Cybersecurity Centre leads these efforts, but universities play a key role in awareness, skills development, and training future experts—similar to Keio's role in Japan.	1. 慶應大学がサイバーセキュリティ国際シンポジウムを開催していることに敬意を示し、登壇の機会への感謝を述べている。 2. ポルトガルのサイバーセキュリティ政策として、新しい法的フレームワークを整備し、予防・強靭化・責任ある対応を重視した基準を採用していると紹介している。 3. ポルトガル政府と大学（特にポルト大学）が協力し、認知向上・スキル育成・次世代人材の育成に取り組んでいる点を強調している。 4. ITU の「Global Cybersecurity Index 2024」で、ポルトガルが世界第 4 位にランクされたことを紹介し、国際的な取り組みの成果を示している。 5. サイバーセキュリティは一国だけで対応できず、国際協力

4. Portugal's progress is internationally recognized: ranked 4th in the ITU Global Cybersecurity Index 2024 and 23rd out of 153 in the National Cyber Security Index. 5. He stresses that national measures alone are insufficient because cyberspace knows no borders; global cooperation is essential. 6. Portugal, Japan, and like-minded nations share a common vision aligned with the EU, NATO, and the UN to promote a free, fair, and secure cyberspace. 7. Portugal has strengthened its role in hybrid-threat defense, joining the European Centre of Excellence for Countering Hybrid Threats and hosting NATO's Communications and Information Academy. 8. He highlights undersea cable protection as a major priority, given Portugal's strategic role as an Atlantic hub for data centers and submarine cable connections operated by companies like Google and Meta. 9. Cybersecurity is also an economic opportunity, attracting investment, fostering innovation, and creating high-skilled jobs; Portugal positions itself as a secure, stable entry point for Japanese investors into Europe and the Atlantic. 10. He concludes that cybersecurity is fundamentally about trust—protecting citizens, economies, and ensuring prosperity—and expresses confidence that the symposium will strengthen shared commitments to a safer digital future.	が不可欠であり、ポルトガルと日本は EU・国連など国際機関で同じビジョンを共有していると述べている。 6. 2019 年以降、ポルトガルは欧州のサイバーサービスセンターとしての役割を強化し、トレーニングハブとして機能していると説明している。 7. 国連のサイバー犯罪条約への署名国であり、国際的な枠組みづくりにも積極的に関与していると強調している。 8. 重要インフラ保護として、特に海底ケーブルの安全確保が重要であり、ポルトガルが Google や Meta にとって欧州の重要なデジタルハブとなっていると述べている。 9. デジタルハブとしての地位は安全保障だけでなく、経済機会・イノベーション・雇用創出の観点からも大きな価値を持つと強調している。 10. 最後に、サイバーセキュリティにおいて最も重要なのは「信頼」であり、本シンポジウムが安全で強靭な未来構築につながることを期待すると述べ締めくくっている。

1.12 D1-R4-10 Remarks from each of the governments and United Nations

D1-R4-10 Aurelijus Zykas (Ambassador of the Republic of Lithuania to Japan)	D1-R4-10 アウレリウス・ジーカス (駐日リトアニア共和国特命全権大使)
1. Ambassador-designate Aurelius Zykas expresses gratitude for the invitation and shares his personal nostalgia for returning to Keio University, which he considers his beloved university. 2. He notes that cybersecurity threats connect all nations, with malicious activity coming from	1. リトアニア大使は慶應大学でのシンポジウム開催を歓迎し、個人的にも「懐かしい場所」で話せることを喜んでいると述べている。 2. サイバー脅威は特にロシア・中国などからの影響が強く、2024 年のリトアニアではサイバー攻撃が前年より 60%増加したと報告している。 3. 単なる攻撃増加だけでなく、防御能力向上や検知件数

actors in Russia, China, and other regions. 3. Lithuania recorded a 60% increase in cyber incidents in 2024, partly due to rising threats but also improved detection and public awareness. 4. Given its difficult geopolitical neighborhood, Lithuania has prioritized strengthening national cybersecurity capabilities. 5. Lithuania's strategy is built on three pillars: * Strengthening cyber resilience across society and critical infrastructure through cooperation between the National Cyber Security Centre, state institutions, and private companies. * Equipping national forces, including establishing the Lithuanian Cyber Command and expanding cyber conscription and reserve units. * Enhancing collective cyber defense by training allies and working with like-minded partners. 6. Japan is identified as a strategic partner; Lithuania and Japan launched a full bilateral cyber dialogue last year, with a second round scheduled soon. 7. Both countries are collaborating on cyber exercises, including forming a joint Lithuania–Japan team for NATO's major cyber exercise, Locked Shields. 8. Information-sharing cooperation is strengthening—Japan has, for the first time, sent an expert to the Lithuanian Regional Cyber Defense Center, with hopes of continuing regularly. 9. Ongoing negotiations on the Chisoya agreement will further facilitate bilateral cybersecurity information exchange. 10. He concludes by thanking the organizers again and expressing enthusiasm for discussions and concrete proposals to advance international cyber cooperation.	の増加も数値に影響しており、環境が依然厳しいと強調している。 4. リトアニアは地政学的に厳しい環境にあるため、サイバー防衛能力を体系的に強化する必要があると述べている。 5. そのためのアプローチとして「3 つの柱」を提示し、1 つ目は国家サイバーセキュリティセンターを中心としたインフラとレジリエンス強化であると説明している。 6. 2 つ目はサイバーコマンド（2023 年設立）を中心とする軍事レベルでの防衛能力向上であり、大規模危機・戦時対応を視野に入れていると述べている。 7. 3 つ目は同盟国・パートナー国との「集団的サイバーディフェンス」であり、国際協力が不可欠な領域であると強調している。 8. 日本とは戦略的パートナーシップを構築しており、昨年から本格的なサイバー協議が開始され、来月 2 回目の外交協議が行われる予定であると紹介している。 9. 日本とリトアニアはサイバー演習でも協力を進めており、来年には両国が NATO 系のサイバー演習「Locked Shields」に共同参加する予定だと述べている。 10. すでに日本から専門家がリトアニアの国家サイバー防衛センターに派遣されており、情報共有・協力が深化していることを述べ、今後さらに連携を強めたいと締めくくっている。

1.13 D1-R4-4 Remarks from each of the governments and United Nations

D1-R4-4 Thomas GNOCCHI (Chargé d'affaires, Delegation of the European Union to Japan)	D1-R4-4 トーマス・ニョッキ (駐日欧州連合代表部臨時代理大使)

1. Thomas Gnocchi, representing the European Union, congratulates Keio University and notes the EU has been participating in the symposium since 2018. 2. He emphasizes that despite global efforts, cybersecurity threats have continued to grow, with both state and non-state actors becoming increasingly sophisticated. 3. The EU is facing a surge in covert malicious activities, making economic, national, and societal security urgent priorities. 4. Citing a recent ENISA report, he highlights major trends: * Expansion of ransomware-as-a-service * Increased cyber-espionage targeting industrial supply chains * Growth of hacktivism * More advanced phishing techniques * Rising risk of AI used as an independent malicious actor 5. Cyberattacks now tend to be continuous multi-vector campaigns rather than isolated high-impact incidents, challenging resilience across Europe. 6. The EU is enhancing cyber resilience through major legislation and certification schemes, including: * NIS2 Directive covering 18 critical sectors * Cyber Resilience Act (common security standards for digital products) * Cyber Solidarity Act (improving preparedness, detection, and coordinated response) 7. ENISA supports EU member states, institutions, and industry through certification, implementation support, and threat analysis. 8. The EU prioritizes strengthened global partnerships, as cyberspace has no borders, and countries worldwide face similar threats. 9. Cooperation with Japan is expanding, including: * Joint work on cybersecurity standards * Collaboration on responsible state behavior norms at the UN	1. EU 代表部として、慶應大学のシンポジウム開催を重要な場と位置づけ、2018 年から継続参加していることに感謝を述べている。 2. サイバー脅威は国家・非国家アクターの双方から高度化しており、悪意ある操作・作戦・攻撃が増加していると指摘している。 3. EU 機関 ENISA の最新レポートでは、ランサムウェア、サプライチェーン攻撃、アクティビズム、フィッシングの進化、AI 悪用などが主要脅威として挙げられていると説明している。 4. インシデント件数は一部減少しているが、多様化・高度化したキャンペーンは継続的に増加していると強調している。 5. EU は NIS2 指令など、18 分野に適用される法的枠組みを通じて、サイバーセキュリティとレジリエンスの強化を進めていると述べている。 6. EU サイバーセキュリティ認証制度（CSA）によって、ICT 製品・サービスの基準を共通化し、信頼性を向上させていると紹介している。 7.「サイバーソリダリティ法」により、域内のインシデント対応能力を強化し、国家間の連携で迅速な対応が可能になったと説明している。 8. EU は日本とデジタルパートナーシップを進めており、防衛・標準化・レジリエンスに関する協力を深化させる意向を示している。 9. 国連枠組みでの責任ある国家行動や、ASEAN–Japan 連携、ウクライナ支援など、国際的取り組みに EU と日本が共同で関与している点を強調している。 10. 70 か国以上が参加する「国際セキュリティチャレンジ」や、日米 EU 合同 ICS セキュリティ演習など、多国間の育成・協力プログラムが展開されていると述べ、シンポジウムの成功を祈念して締めくくっている。

* Pilot projects under the ASEAN–Japan Cyber Capacity Building program 10. He notes upcoming joint initiatives: the EU team's participation in the Cybersecurity Challenge in Tokyo, and the Japan–US–EU Industrial Control Systems Cybersecurity Week, aimed at training Indo-Pacific participants.	

1.14 D1-R4-9 Remarks from each of the governments and United Nations

D1-R4-9 Martin Huth (Deputy Head of Mission, German Embassy)	D1-R4-9 マルティン・フート (ドイツ大使館 首席公使)
1. Germany emphasizes that modern national functions—from power grids to elections—depend on private-sector digital systems, making cyber attacks threats to both security and democracy. 2. Recent incidents attributed to APT28, Lazarus, and other state-sponsored actors show that cyber threats are global and geopolitically linked. 3. Cyber attacks have severe economic impacts, exemplified by disruptions to 6,000 European wind turbines and an estimated USD 230 billion annual cost to the German economy. 4. Societal security is at risk, as shown by the AKIRA ransomware attack that halted welfare and community services for 1.7 million citizens in 2024. 5. Germany is implementing NIS2, expanding regulated critical entities from 4,500 to 29,000, requiring major private-sector investment. 6. The government is increasing cybersecurity spending by exempting it from the national "debt brake," enhancing capabilities of the Cybersecurity Authority. 7. Legislative updates will strengthen active cyber defence, and Germany aims to build a semi-autonomous detection/response capability called the "Cyber Dog." 8. Public-private cooperation is central: Germany collaborates through the Tallinn Mechanism and coordinates with 8,700 companies via the Alliance for Cybersecurity. 9. The UP-CRITICS platform unites operators of	1. デジタル化が進む中で、サイバー攻撃はデータ被害にとどまらず物理的安全や社会インフラにも深刻な影響を及ぼすため、国家運営に直結する重要課題であると強調している。 2. ドイツは 2011 年以降 APT28（ロシア系）など国家支援型アクターの攻撃を受け続けており、国会攻撃や暗号資産取引所への攻撃など民主主義と安全保障に対する脅威が拡大していると述べている。 3. 経済面でも、再生可能エネルギーや自動車産業など高度デジタル依存の分野が攻撃対象となり、衛星通信の妨害による欧州風力発電への影響など巨大な被害が現実化していると指摘している。 4. 低レベルの攻撃でも莫大な損害が生じるため、ドイツではランサムウェア攻撃（アキラグループ）により 170 万人超の市民サービスが停止するなど深刻な影響が出ていると紹介している。 5. これらを受け、EU の NIS2 指令への対応など法制度を強化し、対象組織を 4,500 から 29,000 へ拡大するなど、広範なサイバーセキュリティ強化を進めていると説明している。 6. 政府は技術投資（BSI・他省庁による強化）を進め、AI・暗号・量子技術など新たな脅威環境に対応するためのサイバー防御力を向上させていると述べている。 7.「サイバードーム」などネットワーク全体の監視・検知を行う仕組みを導入し、官民協力による統合的な防御体制の強化を進めていると紹介している。 8. ドイツは民間企業との協力を重視し、10 か国規模の官民連携体制に加えて、日本もオブザーバーとして参加しており、日独間の連携が深化していると述べている。 9. BSI は 8,000 社以上（中小企業を含む）の企業を支援し、リアルタイム脅威分析やインフラ保護（電力・通信・水道など）に取り組んでいると説明している。 10. 最後に、サイバーセキュリティは国・企業・社会全体で責任を共有して取り組むべき課題であり、日本とドイツが協力して安全で強靭なデジタル社会を築く必要があると締めくくって

critical infrastructure with federal agencies to conduct joint risk assessments and national crisis exercises. 10. Germany and Japan share a participatory approach to cybersecurity, and Germany seeks deeper cooperation with Japan to build a secure and resilient digital world.	いる。

1.15 D1-R4-5 Remarks from each of the governments and United Nations

D1-R4-5 Deborah Paul (Minister / Deputy Head of Mission, Embassy of Canada to Japan)	D1-R4-5 デボラ・ポール (在日カナダ大使館 首席公使)
1. Canada congratulates Japan on passing its active cyber defense law and notes both countries are adapting their cyber response toolkits. 2. Canada launched its first national cybersecurity strategy in 2018, establishing the Canadian Centre for Cybersecurity and the National Cyber Coordination Centre. 3. A refreshed strategy was introduced this February, emphasizing whole-of-society engagement, agile leadership, and partnerships across academia, industry, civil society, and international actors. 4. The strategy relies on real-time adaptation through issue-specific action plans and ongoing investment in cyber resilience. 5. Bill C-8, introduced in June, reinforces Canada's commitment to resilience and deterrence in protecting critical infrastructure. 6. Canada notes strong parallels between its updated approach and Japan's cybersecurity strategy, reflecting shared principles and mutual learning. 7. Bilateral cooperation with Japan includes exchanges between cyber defense forces, regular dialogue on cyber defense policy, and enhanced cooperation against cybercrime. 8. Continued official exchanges, including those involving the NISC and Canadian counterparts, are strengthened through the recently signed Security of Information Agreement. 9. Canada values multilateral cooperation with Japan to advance global norms and build cyber	1. 慶應大学および主催者への謝意を述べつつ、カナダのサイバーセキュリティ政策を紹介する趣旨を示している。 2. カナダは 2018 年に初の国家サイバーセキュリティ戦略を策定し、カナダサイバーセキュリティセンターと国家サイバー調整センターを設立したと説明している。 3. 2024 年 2 月に新たなサイバーセキュリティ戦略を発表し、社会参画、アジャイルなリーダーシップ、学術界・産業界・市民社会・国際同盟国との協力を強化すると述べている。 4. 新戦略の実行に向け、リアルタイムのアクションプランを導入し、サイバー脅威へのレジリエンス強化を進めていると説明している。 5. 新法案（Bill C-8）が 6 月に可決され、重要インフラを守るための法的強化が行われたと紹介している。 6. カナダと日本は、法制度の整備を含め、ここ数年サイバーセキュリティの協力やベストプラクティスの交換を積極的に進めてきたと述べている。 7. 両国はサイバー防衛、相互運用性の向上、サイバー犯罪対策、情報交換（NCO 連携を含む）など、実務レベルでの協力を継続していると説明している。 8. 貿易・外交の観点からもサイバーセキュリティは重要であり、日本・韓国を含む国々の企業・政府との関係深化を図っていると述べている。 9. サイバー脅威は進化しており、国家が孤立していては対応できないため、信頼に基づく国際協力・省庁間協力・官民連携が不可欠であると強調している。 10. 本シンポジウムが経験共有・人的ネットワーク構築の場となることを期待し、今後も社会・経済を守るため日本との協力を続けたいと締めくくっている。

capacity worldwide. 10. Trust is emphasized as the core requirement for effective cybersecurity collaboration, and Canada sees forums like this symposium as essential for building relationships that improve national and societal resilience.	

1.16 D1-R4-14 Remarks from each of the governments and United Nations

D1-R4-14 Izumi Nakamitsu (Under-Secretary-General and High Representative for Disarmament Affairs, United Nations)	D1-R4-14 中満 泉 (国際連合事務次長・軍縮担当上級代表)
1. The UN highlights the global importance of cybersecurity as digital transformation accelerates across societies. 2. Digital public infrastructure in India has enabled 1.3 billion people to access digital IDs, financial services, and digital payments. 3. In Timor-Leste, data collection in key sectors supports economic development and protects agricultural heritage. 4. Japan's smart-city initiatives are improving the efficiency and sustainability of public services. 5. These examples show the great potential of digital technologies, but also the need to manage risks responsibly. 6. A whole-of-society approach is essential: governments alone cannot secure cyberspace; industry, academia, and civil society must all contribute. 7. Public-private partnerships are critical, as responding to ICT incidents requires diverse technical capabilities and continual information exchange. 8. For more than 20 years, the UN has facilitated intergovernmental discussions on ICT security and the role of multi-stakeholder partnerships. 9. In July, UN member states agreed to establish a permanent global mechanism on ICT security that will begin work in 2026. 10. The new mechanism will build on existing international norms, promote responsible state behavior, and include multi-stakeholder	1. 第 15 回サイバーセキュリティ国際シンポジウムへの参加と主催者への謝意を表し、デジタル化社会におけるサイバーセキュリティの重要性を強調している。 2. デジタル変革は世界で大きな利益をもたらしており、インドのデジタル ID、スバルのデータ活用、日本のスマートシティ構想などを成功例として紹介している。 3. デジタル化の恩恵にはリスクも伴うため、社会全体でその可能性を最大化する取り組みが必要だと述べている。 4. 政府のみでサイバーセキュリティを確保することは不可能であり、産業界、学術界、NGO など多様なアクターが重要な役割を担うと指摘している。 5. 特に官民パートナーシップが効果的な政策形成と ICT インシデント対応の強化に不可欠だと述べている。 6. 国連では 20 年以上にわたり、政府間協議の中でパートナーシップの重要性や ICT セキュリティ枠組みが議論されてきたと説明している。 7. 2024 年 7 月に ICT セキュリティに関する恒久的プログラムが設立され、2026 年まで継続されると紹介している。 8. このプログラムは、国家が責任ある ICT 利用を行うための国際的枠組みを発展・強化することを目的としている。 9. マルチステークホルダー（多主体）によるプロセス構築が必須であり、利害関係者が会議や協議の場に参加する機会が提供されていると述べている。 10. 参加者に対し、新たなメカニズムへの関与と成果の実践的活用を促し、サイバーセキュリティは全員に関わる問題であるとしてメッセージを締めくくっている。

engagement through intersessional and consultative meetings.	

1.17 D1-S3-2 Keynote Speech: National Security

D1-S3-2 IIDA Yoichi (National Cyber Director, National Cybersecurity Office)	D1-S3-2 飯田 陽一 (国家サイバー統括室 内閣サイバー官)
1. Japan faces rapidly increasing cyber threats, including data theft, ransomware, and highly sophisticated state-sponsored attacks that target both IT systems and mission-critical infrastructure. 2. Attack volume has risen dramatically—NICT reports a tenfold increase over ten years, with malicious packets appearing every 13 seconds—expanding the areas Japan must defend. 3. Recent major incidents include ransomware attacks on Toyota's production system and the Port of Nagoya, causing multi-day operational stoppages and highlighting economic security risks. 4. Large DDoS attacks targeted airlines, financial institutions, and telecoms, disrupting flights and online banking, influencing recent cyber-response legislation. 5. Japan's 2022 National Security Strategy emphasizes seamless, omnidirectional cyber response, including the implementation of active cyber defense under new legislation. 6. Japan aims to establish cyberspace as a foundation of a free and democratic society, guided by five principles: free flow of information, rule of law, openness, autonomy, and diversity. 7. The government recognizes that neither the public nor private sector alone can manage cyber threats; deep public-private cooperation based on mutual trust is essential. 8. Active cyber defense relies on incident information sharing from private organizations, government action based on that data, and structured councils covering critical infrastructure sectors. 9. New mechanisms—such as security-cleared information-sharing systems beginning in May—	1. 高市内閣の発足を受け、国家サイバー統括室を引き続きリードする決意を表明し、第 15 回国際シンポジウムの開催を祝意した。 2. サイバー攻撃は日本において増加し続けており、表面化していない被害も多く、実態は認識以上に深刻だと指摘した。 3. NICT 観測では、サイバー攻撃と見られる通信が 10 年前の 10 倍以上となり、インターネット接続機器は平均 13 秒に 1 回攻撃パケットを受信していると説明した。 4. 攻撃手法は高度化し、深部への侵入、管理権限の奪取、ランサムウェア、国家主体の関与など、質的変化が顕著であると強調した。 5. 名古屋港システム停止（2023 年）や年末年始の広範囲 DDoS 攻撃（航空・金融・通信）などの大規模インシデントを例示し、能動的サイバー防御法制の必要性を裏付けた。 6. 2022 年国家安全保障戦略に基づき、サイバー安全保障は海洋・宇宙・エネルギー等と並ぶ国家レベルの主要課題であり、同盟国並みに能力を高めると述べた。 7. 自由、公正、安全なサイバー空間を実現するための"五つの基本原則"（自由な情報流通、法の支配、開放性、自律性、多様性）を提示した。 8. 官民連携を最重要視し、政府が積極的に役割を担い、セキュリティグレード制度などを活用して、相互に意味ある情報共有を進める方針を示した。 9. サーバーへのアクセスによる不正プログラム無害化など、新法に基づき能動的サイバー防御を実施し、国際共有を通じ世界のレジリエンス向上に貢献すると述べた。 10. 今後の戦略の柱として①国家安全保障としての防御力強化、②社会全体のセキュリティ・レジリエンス向上、③人材・技術エコシステム形成を掲げ、民間と学術界のさらなる協力を求めて締めくくった。

enable analysis and dissemination of threat intelligence across ministries and private entities. 10. Japan's five-year cybersecurity vision focuses on national resilience, security-by-design for individuals and SMEs, talent development, strengthened international cooperation, and closer alignment among government, industry, and academia.	

1.18 D1-S3-1 Keynote Speech: National Security

D1-S3-1 ADM (Ret.) Dennis Blair, (Former Director of U.S. National Intelligence)	D1-S3-1 デニス・ブレア（元米国国家情報長官）
1. Admiral Blair highlights major global cyber developments in the past year, especially the rapid evolution of AI, which has empowered criminals and hostile nations more quickly than defenders. 2. He describes two massive, long-running Chinese cyber campaigns—Salt Typhoon (telecom penetration and message extraction) and Volt Typhoon (critical infrastructure infiltration and malware implants). 3. Social-media–based influence operations by Russia, China, and others have intensified, aiming to polarize societies and influence elections in Western countries. 4. Japan's new active cyber defense legislation mainly targets criminal attacks and still offers limited authority for countering state-sponsored threats like Salt Typhoon and Volt Typhoon. 5. Japan has strengthened its defensive posture—cloud migration, zero-trust initiatives, security classification reforms—but these measures lag behind best practices in other Western nations. 6. Despite increases in incident reporting, Japan still undercounts cyber intrusions, particularly as AI expands attackers' capabilities; many government systems continue to have unpatched vulnerabilities. 7. Blair warns that China is implanting malware within Japanese critical infrastructure and that	1. AI の進展が攻撃側を先行させ、フィッシングやマルウェア生成を高度化させている一方、防御側の AI 活用は遅れていると指摘している。 2. 過去 1 年間で、中国による通信ネットワーク侵害や重要インフラへの潜在的攻撃（Salt Typhoon／Volt Typhoon）が明らかになり、官民連携による大規模な対策が不可欠だとしている。 3. 日本でも選挙・世論操作を含むロシアや中国の情報工作が進展しており、民主主義の根幹を揺るがす脅威として警戒が必要と述べている。 4. 日本政府はクラウド移行、ゼロトラスト、FedRAMP モデルの導入などを進めているが、海外のベストプラクティスに比べ、実装スピードが依然として遅いと評価している。 5. 政府ネットワークの監査で未解決の脆弱性が多数残存しており、国家レベルの攻撃者が一般的な脆弱性を悪用している状況に対し、対策が不十分と述べている。 6. 日本は軍事反撃能力の議論を進める一方、サイバー反撃能力の整備が遅れ、中国のサイバー攻撃に対し著しく脆弱だと指摘している。 7. 国家主体の攻撃に対応するための法制度（能動的サイバー防御）が依然として限定的であり、政策策定が長年先送りになっている点を問題視している。 8. 日本は JCDC のような政府・民間がリアルタイムで協働する組織を創設し、現場主導の実践的な情報共有と対処能力を高めるべきだとしている。 9. 政府のサイバー防衛要員は国際的に比較して規模・能力ともに不足しており、高度スキルを持つ防衛人材の育成と官民協働が急務と述べている。 10. AI を活用した能動的防衛ツールの共同開発や国際協力を強化し、アメリカとの連携を含め、日本は今こそより積極

Japan lacks effective counter-strike cyber capabilities, unlike its progress in military deterrence. 8. Foreign disinformation campaigns targeting Japan's elections are growing, yet government response has been weak, with limited transparency or urgency compared to other democracies. 9. He stresses the need for real-time public-private collaboration, recommending Japan establish a JCDC-like operational body rather than relying solely on policy frameworks. 10. Japan must rapidly expand trained cyber-defender capacity, develop AI-enabled defensive tools, increase investment, and elevate urgency to match the rising state-level threat environment, especially to strengthen cooperation with the United States.	的にサイバー安全保障に取り組むべきだと強調している。

1.19 D1-S4 Keynote Speech from Japanese Industry

Yoshihisa Nishimura (Executive Director, East Japan Railway Company)	西村 佳久 (東日本旅客鉄道株式会社 執行役員)
1. JR East operates extensive mobility and lifestyle businesses—including railways, Suica services, stations, hotels, and retail—serving 35 million customers with over 100,000 employees, creating a large and complex security environment. 2. The company's information security policy is structured with top-level basic policies, detailed rules, and system-building guidelines, including strict internal rules for AI usage and cloud adoption. 3. With more than 70 group companies interconnected, JR East faces significant supply-chain cyber risks, requiring unified, group-wide security measures. 4. A recent incident involving a malware-infected PC showed that employee actions (such as calling a fake support number) can still lead to breaches despite existing rules. 5. JR East deploys endpoint security on approximately 73,000 PCs, collecting 1 TB of logs daily for analysis by a 24/7/365 hybrid	1. JR 東日本は民間セクターとして日々サイバー攻撃と向き合っており、その現場視点から取り組みを紹介している。 2. 事業範囲は鉄道輸送に加え、ホテル・商業施設・駅ナカ・Suica など多岐にわたり、約 10 万人が 3500 万人にサービスを提供している大規模グループである。 3. 情報セキュリティルールは三層構造で、AI 利用やクラウド利用のポリシー適合性をチェックし、利用者向けルールは簡潔化して全社員に徹底している。 4. グループ 70 社以上がシステムで密接につながるため、サプライチェーンリスクを最重要リスクとし、全社統一のセキュリティ対策を必要としている。 5. 偽警告からリモート操作され情報流出が疑われるなど、人的要因によるインシデントはルールを整備しても完全には防げないと説明している。 6. 約 7 万 3000 台の PC にエンドポイントセキュリティを導入し、1 日 1TB 規模のログを内部・外部 SOC のハイブリッドで 24/365 監視している。 7. 昨年 5 月にはモバイル Suica が標的となった大規模 DDoS 攻撃（最大 160Gbps・数時間継続）が発生し、100 以上の国のボットを使う高度な攻撃だったと説明している。 8. ルール遵守の限界を踏まえ、次世代設計基盤で設定や

security operations center (internal + external). 6. In May of last year, a massive DDoS attack targeted Mobile Suica, reaching up to 166 Gbps from bots in over 100 countries, overwhelming defenses and disrupting other internal systems. 7. Attackers demonstrated sophisticated orchestration and bypass techniques, requiring rapid tuning of defense mechanisms to restore service and improve resilience for future attacks. 8. JR East is investing in next-generation automated rule-compliance checking systems to complement human monitoring and prevent information leakage incidents similar to those seen in other major communication carriers. 9. For control systems, JR East prioritizes safety, stability, and real-time performance, conducts security assessments under national guidelines (e.g., SCIS), deploys intrusion detection devices, and uses data diodes to enforce one-way data flows. 10. JR East complies with the Economic Security Promotion Law and active cyber defense requirements, promptly notifying authorities of incidents and working to upgrade security in line with government guidance.	改善状況を自動検証する仕組みを導入し、ヒューマンエラーを補完しようとしている。 9. 制御系システムでは安全性・安定性・リアルタイム性を重視し、侵入検知装置やデータダイオードの導入、CIS ベースのアセスメント、人材育成などを実施している。 10. 経済安全保障法に基づき国への届出やチェックを行い、インシデント時には監督官庁と情報連携しながらセキュリティレベルの向上に取り組んでいる。

1.20 D1-S6 INCS-CoE Speech

Chris Hankin (Professor, Imperial College London, INCS-CoE Chair)	クリス・ハンキン（インペリアル・カレッジ・ロンドン教授、INCS-CoE チェア）
1. The International Cyber Security Centre of Excellence (INCS-COE) began informal collaboration in 2016 and was formally established in 2019 by six founding universities from the U.S., U.K., and Japan. 2. INXCOE has since expanded to 16 member universities across nine countries, with 41 expert members and fellows. 3. The center's primary activities include regular research seminars and the annual Country-to-Country Capture the Flag (C2C CTF) competition. 4. Four research seminars were held since the previous symposium, covering space systems, medical devices, aviation/UAVs, and immersive	1. 国際サイバーセキュリティ卓越センター（INCS-COE）は2016 年に非公式な協力を開始し、2019 年に米国、英国、日本の 6 つの創設大学によって正式に設立された。 2. INCS-COE はその後、9 カ国にまたがる 16 の加盟大学に拡大し、41 名の専門家メンバーとフェローを擁している。 3. センターの主な活動には、定期的な研究セミナーと年次開催の「国対国キャプチャー・ザ・フラッグ（C2C CTF）」競技会が含まれる。 4. 前回シンポジウム以降、宇宙システム、医療機器、航空／無人航空機（UAV）、没入型技術をテーマに計 4 回の研究セミナーが開催された。 5. 宇宙システムにおける顕著な課題は、過酷な運用環境にもかかわらず IoT や ICS 環境と類似している点であり、これが分野横断的な学習を促している。 6. 医療機器分野では、サイバー脅威の軽減に侵襲的処置

technologies. 5. A highlighted challenge in space systems is their similarity to IoT and ICS environments despite harsh operating conditions, prompting cross-domain learning. 6. In medical devices, a key challenge is that mitigating cyber threats may require invasive procedures, creating tension between patient safety and security. 7. In UAV applications—such as emergency response—the challenge includes safely landing drones when standard navigation aids are unavailable. 8. For immersive technologies, research revealed major unresolved issues involving scaling from single-user to multi-user environments. 9. The C2C CTF attracts around 300 applicants annually, selects about 120 students, forms multinational teams, and covers a wide range of cybersecurity challenges from web security to digital forensics. 10. Future plans include building an alumni network, hosting the next C2C CTF in Bali, and preparing for a subsequent event at George Mason University in 2027.	が必要となる可能性があり、患者の安全とセキュリティの間に緊張関係が生じている。 7. 緊急対応などの無人航空機（UAV）応用では、標準的な航法支援装置が利用できない状況下での安全な着陸が課題である。 8. 没入型技術に関しては、単一ユーザー環境から複数ユーザー環境への拡張に関わる重大な未解決問題が研究で明らかになった。 9. C2C CTF は毎年約 300 名の応募者から 120 名の学生を選抜し、多国籍チームを編成する。ウェブセキュリティからデジタルフォレンジックまで幅広いサイバーセキュリティ課題を対象とする。 10. 今後の計画には、卒業生ネットワークの構築、次期 C2C CTF のバリ開催、2027 年ジョージ・メイソン大学での後続イベント準備が含まれる。

1.21 D1-P1 Panel

Theme: INCS-CoE Moderator: Chris Hankin Panelists: - David Luzzi (Senior Vice Provost, Northeastern University) - Karl Steiner (Vice President, UMBC) - Anupam Joshi (Vice Provost & Chief AI Officer, UMBC) - Luiz DaSilva (Professor, Virginia Tech) - Konstantinos Mersinas (Associate Professor, Royal Holloway, University of London) - Muhammad Salman (Head of Computer Engineering Study Program, University of Indonesia) - Rolando Martins (Assistant Professor, University of Porto)	テーマ：INCS-CoE モデレーター：クリス・ハンキン 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） - カール・シュタイナー（UMBC 副学長） - アヌパム・ジョシ（UMBC 副学長、チーフ AI オフィサー） - ルイス・ダ・シルヴァ（バージニア工科大学教授） - 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） - 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研究プログラム長） - ローランド・マーティンス（ポルト大学） - 近藤 賢郎（慶應義塾大学サイバーセキュリティ研究センター 特任助教）

- Takao Kondo (Project Assistant Professor, Keio University)	
1. The panel introduced the International Cyber Security Centre of Excellence (INCS-COE) network, with Imperial, Northeastern, UMBC, Virginia Tech, Royal Holloway, University of Indonesia, University of Porto, and Keio presenting their roles in collaborative cybersecurity research and education. 2. Imperial College highlighted its status as a UK centre of excellence, leading RITICS on trustworthy interconnected cyber-physical systems, focusing on industrial control system resilience, critical infrastructure, and attack/defence research with a 500-member community of interest. 3. Northeastern University showcased broad cybersecurity research (IoT, ICS, medical, space, democracy defense), major facilities open to international users (Colosseum wireless digital twin, SPHERE testbed, large anechoic Faraday facility), and programs like the National Internet Observatory, Archimedes Center for healthcare, and CHEST for hardware security. 4. UMBC described a campus-wide strategy integrating AI, quantum, and cybersecurity, including an OT-focused cyber range, AI and Quantum Science Institutes, an interdisciplinary Cybersecurity Institute, and deep workforce and research ties with NSA and a large cyber incubator in its BWTech research park. 5. Virginia Tech's Commonwealth Cyber Initiative (CCI) brings together 47 Virginia institutions, supports over 350 faculty and thousands of students, funds and spins out startups, runs IUCRCs like CyberSmart (financial-sector cybersecurity) and Whisper (6G/future networks security), and has generated significant jobs, GDP, and research funding while expanding collaboration with Japan. 6. Royal Holloway emphasized its pioneering history in information security education (MSc since 1992), large global alumni network,	1. パネルでは国際サイバーセキュリティ卓越センター（INCS-CoE）ネットワークが紹介され、インペリアル・カレッジ、ノースイースタン大学、UMBC、バージニア工科大学、ロイヤル・ホロウェイ大学、インドネシア大学、ポルト大学、慶應義塾大学が、共同サイバーセキュリティ研究・教育における役割を説明した。 2. インペリアル・カレッジは英国の卓越研究拠点としての地位を強調し、信頼性の高い相互接続サイバーフィジカルシステムに関する RITICS を主導している。産業制御システムのレジリエンス、重要インフラ、攻撃・防御研究に焦点を当て、500 名の関心共同体を擁する。 3. ノースイースタン大学は、広範なサイバーセキュリティ研究（IoT、ICS、医療、宇宙、民主主義防衛）、国際ユーザーに開放された主要施設（コロシアム無線デジタルツイン、SPHERE テストベッド、大型無響ファラデー施設）、および国立インターネット観測所、医療向けアルキメデスセンター、ハードウェアセキュリティ向け CHEST などのプログラムを紹介した。 4. UMBC は、AI・量子・サイバーセキュリティを統合したキャンパス戦略を説明した。これには OT 特化型サイバーレンジ、AI・量子科学研究所、学際的サイバーセキュリティ研究所が含まれ、NSA との深い人材・研究連携、BWTech 研究公園内の大規模サイバーインキュベーターを擁する。 5. バージニア工科大学のコモンウェルス・サイバー・イニシアチブ（CCI）は、バージニア州 47 機関を統合し、350 名以上の教員と数千人の学生を支援。スタートアップへの資金提供とスピンアウトを推進し、サイバースマート（金融セクターサイバーセキュリティ）やウィスパー（6G/次世代ネットワークセキュリティ）などの IUCRC を運営。日本との連携を拡大しつつ、雇用・GDP・研究資金を大幅に創出している。 6. ロイヤル・ホロウェイ大学は、情報セキュリティ教育における先駆的歴史（1992 年より修士課程開設）、大規模なグローバル卒業生ネットワーク、複数の研究ラボ（スマートカード、暗号技術、人間／行動セキュリティ）、多様な修士課程・オンラインプログラム、ユーザーのオンラインセキュリティ行動改善を支援するブラウザアドオンなどの無料教育ツールを強調した。 7. インドネシア大学は、JICA 支援のサイバーセキュリティ人材育成プロジェクト、サイバーフィジカル・OT/ICS セキュリティ分野での継続的研究、AI 駆動型脅威インテリジェンス、IoT・ブロックチェーンセキュリティ、オープンソース SOC/監視イニシアチブ、そして 2026 年バリ開催の C2C CTF ホスト機関としての役割（広範な技術課題カテゴリーを含む）を概説

multiple research labs (smart cards, crypto, human/behavioral security), diverse master's and online programs, and free educational tools such as a browser add-on to help users improve their online security behaviour. 7. The University of Indonesia outlined its JICA-backed cybersecurity human-resource development project, ongoing work in cyber-physical and OT/ICS security, AI-driven threat intelligence, IoT and blockchain security, an open-source SOC/monitoring initiative, and its role as host of the 2026 C2C CTF in Bali with broad technical challenge categories. 8. The University of Porto's cybersecurity centre unites multiple faculties and industry partners to work on autonomous vehicles (with Bosch), resilient infrastructure, AI-based vulnerability/zero-day risk scoring, offensive AI for defensive testing in the energy sector (with Galp), and quantum-classical hybrid networks for secure QKD deployments. 9. Keio University's Cybersecurity Research Center, now under the Cyber Civilization Research Center, presented its work on OT/ICS security and "dynamic penetration testing" frameworks using cyber-range environments to evaluate resilience (detection + rapid recovery) in long-lived, IT-connected OT systems with large attack surfaces. 10. In the Q&A, panelists stressed that AI will automate some entry-level SOC and testing tasks but create demand for higher-skilled roles and new defenses against AI-driven attacks; they framed future-proof skills around technological, data, and human literacy, and invited universities and industry (especially in quantum/future networks, healthy ageing, and digital currencies) to join INCS-COE seminars and collaborations.	した。 8. ポルト大学サイバーセキュリティセンターは、複数の学部と産業界パートナーを統合し、自律走行車（ボッシュ社との共同）、レジリエントインフラ、AI ベースの脆弱性/ゼロデイリスク評価、エネルギー分野における防御的テストのための攻撃的 AI（ガルプ社との共同）、安全な QKD 展開のための量子-古典ハイブリッドネットワークに取り組んでいる。 9. 慶應義塾大学サイバーセキュリティ研究センター（現・サイバー文明研究センター傘下）は、OT/ICS セキュリティと「動的ペネトレーションテスト」フレームワークに関する研究を発表した。サイバーレンジ環境を活用し、広範な攻撃対象領域を持つ IT 接続型 OT システムの長期運用における回復力（検知＋迅速復旧）を評価する手法である。 10. 質疑応答では、パネリストらは AI が初級レベルの SOC 業務やテスト作業を自動化する一方、高度なスキルを要する職種や AI 攻撃への新たな防御策の需要を生み出すと強調した。将来を見据えたスキルとして技術リテラシー、データリテラシー、ヒューマンリテラシーを提示し、特に量子／次世代ネットワーク、健康長寿、デジタル通貨分野の大学・産業界に対し、INCS-COE セミナーや共同研究への参加を呼びかけた。

1.22 D1-S7-1 Speeches from Japanese Government

D1-S7-1 FUJIYOSHI Takayuki (Assistant Minister for Cybersecurity, IT Management and Evidence-based Policymaking, Ministry of	D1-S7-1 藤吉 尚之 (文部科学省 サイバーセキュリティ・政策立案総括審議官)

Education, Culture, Sports, Science and Technology - Japan)	
1. Assistant Minister Fujiyoshi introduces himself as responsible for cybersecurity, IT management, and evidence-based policymaking at the Ministry of Education, Culture, Sports, Science and Technology (MEXT). 2. He thanks the organizers and participants, emphasizing that cybersecurity is now a core issue for universities and for the research community. 3. He notes that the information environment surrounding universities is rapidly changing, and it is essential to identify, prioritize, and implement the most effective security measures. 4. Universities are engaged in diverse research activities, which exposes them to the latest and most serious cyber threats, increasing the importance of robust security management. 5. He stresses that basic “on-the-ground” security practices and risk management must be carried out consistently on a daily basis, not just at the policy level. 6. MEXT seeks to strengthen cybersecurity human resources, including the development and training of CISOs and other key personnel in universities. 7. While new technologies bring many benefits, he warns that they also generate new types of risks that can only be addressed through proper cybersecurity and coordinated responses to cyber attacks. 8. He concludes by underlining that cyber attacks target not only private companies but also governments, and that close cooperation between all stakeholders is essential.	1．文部科学省として、大学・国立研究機関におけるサイバーセキュリティ推進の取り組み状況を紹介する趣旨での講演である。 2．講演内容は、基本概念、大学向け取り組み事例、大学・研究機関の状況変化に応じた対応の 3 点で構成されている。 3．大学や研究機関は重要技術情報を扱うため、サイバーセキュリティ確保は国益に直結する重要責務となっている。 4．トップマネジメントのリーダーシップの下、最新情報に基づくリスク評価、優先順位づけ、適切な人材育成が不可欠と強調している。 5．文科省は CRSO・部門長・CSIRT メンバー向けに研修を実施し、ガバナンス強化や実践演習を通じて大学の対処能力向上を図っている。 6．最近は VPN 脆弱性を狙うゼロデイ攻撃や生成 AI を用いた攻撃など、新たな手口が増え、大学も深刻な標的となっていると指摘している。 7．経済安全保障の観点から、重要技術流出防止のため、研究セキュリティ・研究インテグリティ確保が求められ、サイバー対策の重要性がさらに高まっている。 8．チェックポイント社の調査では、教育分野が世界で最も狙われているとされ、大学が置かれた脅威環境の厳しさを示している。 9．文科省は大学・研究法人へ通知を発出し、サイバー対策を経営課題として認識し、組織特性に応じた継続的な対策実施を求めている。 10．実施例や検討事項の共有、CISO 会合での情報交換などを通じ、大学・研究機関の意識向上と対応力向上を促進している。

1.23 D1-S7-2 Speeches from Japanese Government

D1-S7-2 OKUYA Toshikazu (Deputy Director General, Commerce and Information Policy Bureau, Ministry of Economy, Trade and Industry)	D1-S7-2 奥家 敏和（経済産業省大臣官房審議官(商務情報政策局担当))
1. Okuya emphasizes that Japan and the world	1．経産省として、サイバーとフィジカルが高度に統合される時

face increasingly serious cyber threats, including recent ransomware incidents and cases like the 2023 Volt Typhoon intrusion targeting critical infrastructure. 2. He warns that cyber and physical domains are rapidly integrating, expanding the attack surface and diversifying attack vectors. 3. He argues against checklist-based cybersecurity, noting that even 90/100 compliance can still leave a kill chain open; instead, organizations must adopt a risk-based approach. 4. Only top leadership can identify the organization's true "crown-jewel" assets, making cybersecurity fundamentally a governance and business-management issue. 5. Because attacks propagate through supply chains, companies cannot protect themselves in isolation—collective, ecosystem-wide cybersecurity is essential. 6. METI's cybersecurity policy has four pillars: (1) strengthening supply-chain security; (2) international cooperation on IoT and software security (including SBOM); (3) direct government support to industry; (4) expansion of human resources and R&D. 7. He explains Japan's Cyber-Physical Security Framework (CPSF), integrating organizational capability, secure systems, and data trust—now progressing toward international standardization. 8. METI is developing sector-specific guidelines (factories, buildings, automotive, space, semiconductor), noting the need to earn global trust for Japan's semiconductor resurgence (e.g., Rapidus). 9. SMEs lack cybersecurity resources, so METI launched a low-cost support service (monitoring, emergency response, insurance) and is expanding users beyond 10,000 organizations. 10. Japan launched the JCSTAR IoT security labeling scheme, is advancing SBOM adoption across industries, and is investing heavily in new	代において、社会・産業全体が「どの部分を守るべきか」「どの時点で防御すべきか」を見極めることが極めて重要だと強調している。 2．企業はどれほど対策をしていても、攻撃者側の技術進化が速く、80%程度の防御状態では十分でないと指摘し、サプライチェーン全体での共同防御の必要性を述べている。 3．サイバーフィジカルシステム（CPS）が普及する中、IoT・OT 領域を含め、統合的にリスクを理解し、防御レベルを維持・向上させる枠組みが必要とされている。 4．経産省は国際標準化や国内制度の整備に取り組んでおり、CPS セキュリティの標準策定、セキュリティ・ガイドラインの整備などを推進している。 5．半導体製造など重要産業では、グローバル・サプライチェーン全体でサイバー要求が高度化しており、日本企業も国際基準に基づく対応が不可欠と説明している。 6．経産省は IoT セキュリティ認証（例：セキュリティレベルの可視化制度など）を導入・拡大しており、国際的にも活用されつつあると述べている。 7．医療機器など安全性が極めて重要な分野では、ソフトウェアの品質・セキュリティ確保に対する世界的な規制強化が進んでいると指摘している。 8．日本では CPS/OT 領域の専門人材育成が重要課題であり、経産省は特別な教育機関・研修プログラムを整備し、ICS/OT セキュリティの専門家育成を進めている。 9．アジア太平洋地域を対象に、OT セキュリティの国際研修を毎年実施しており、70 名規模の技術者を招聘して日本の知見を共有し、地域全体の能力向上を支援している。 10．産業・国際連携を通じ、CPS/OT セキュリティ人材の育成と国際協力を今後も強化する必要があると締めくくっている。

R&D centers and OT-security workforce development (ICSCOE, 500+ specialists trained).	

1.24 D1-S7-3 Speeches from Japanese Government

D1-S7-3 MORI Masahiro (Assistant Minister for Pharmaceutical Industry Promotion and Healthcare DX, MHLW)	D1-S7-3 森 真弘 (厚生労働省 医薬産業振興・医療情報審議官)
1. Mori highlights that recent cyberattacks have severely affected medical institutions, disrupting operations and exposing vulnerabilities in healthcare systems. 2. He notes a major incident in Ryokutan, explaining that although a cyberattack occurred, essential information about the attack was lacking at the time. 3. He references additional cases in the U.S. (North Carolina and San Diego), stressing that cyber incidents in healthcare are global and increasingly frequent. 4. He emphasizes that medical institutions are uniquely vulnerable because of the sensitive nature of personal and clinical data, including patient names and medical records. 5. Healthcare cyberattacks jeopardize not only confidentiality but also the continuity of essential clinical services—posing real risks to patient lives. 6. Mori explains that many incidents stem from basic security failures, such as extremely weak passwords and password reuse by service vendors and administrators. 7. In one case, reusing an administrator ID and password allowed unauthorized identity provider (IdP) access, leading to a full server compromise. 8. These examples illustrate the need for stronger cybersecurity hygiene, vendor management, and improved authentication practices in the medical sector. 9. Mori stresses the importance of continuous training—not only of systems but of human operators—highlighting that cybersecurity requires both technical and organizational preparedness. 10. He concludes by urging the healthcare sector	1. 厚労省として、日本の医療機関におけるサイバー攻撃の現状・要因・対策と、今後の将来像について説明する趣旨である。 2. 医療機関へのサイバー攻撃は小規模診療所から大病院まで幅広く報告されており、とくにランサムウェア被害では診療停止や長期の復旧作業など、医療提供に重大な影響が出ている。 3. 具体的事例として、数カ月にわたる診療停止や復旧、救急・小児救急の受け入れ停止、精神科医療センターでの長期システム停止などが紹介され、患者が必要な医療を受けられず、病院側も手書きカルテ運用を強いられる深刻さが示されている。 4. 医療機関では電子カルテが検査機器、処方システムなどあらゆる部門と連携しており、一部が侵害されると病院全体の運営に波及し、患者の病歴・アレルギー情報など高度な個人情報が失われたり漏えいしたりするリスクが高いと指摘している。 5. ある事例では、給食事業者の VPN 脆弱性放置、安易なパスワード設定、管理者パスワードの使い回し、RDP 接続の恒常的許可など複数の管理不備を足掛かりに、病院ネットワークへ侵入されたと分析している。 6. 全国調査の結果、300 床以上の病院では約 9 割が責任者を置いている一方、299 床以下では約 4 割が責任者不在であり、二要素認証の導入率も 11%程度と低く、専門人材不足・認証や運用の甘さが顕在化していると説明している。 7. 課題として、外部ネットワーク接続ポイントが多く把握・管理が不十分であること、情報システム部門や BCP 訓練など人材・運用が不足していること、システム回復プロセスの整備不足という三点を整理している。 8. 国としては、サイバーセキュリティ戦略に基づき医療分野を重要インフラに位置づけ、医療情報システム安全管理ガイドライン第 6 版の策定、医療法施行規則改正によるサイバー対策義務化とサイバー観点での立入検査などを進めている。 9. 補助事業等で病院ネットワークの全体構造と外部接続ポイントのマッピングを支援し、接続点の集約・管理強化、人

to adopt stronger protective measures, strengthen resilience, and learn from past incidents to prevent recurrence.	材向け研修プログラム、バックアップや復旧支援、診療継続計画の整備などを支援している。 10. 将来像として、病院経営が厳しい中で個別オンプレ環境に追加でサイバー対策投資を続けるのは困難であり、とくに中小病院ではクラウドネイティブな電子カルテ等を前提としたセキュアな共通基盤を整備し、全体コストを抑えつつ医療提供体制に資源を振り向ける方向を目指している。

1.25 D1-S7-4 Speeches from Japanese Government

D1-S7-4 NIKAMI Hideo (Assistant Director-General, Second Intelligence Department, Public Security Intelligence Agency)	D1-S7-4 二上 英生 (公安調査庁 調査第二部長)
1. Nikami explains that intelligence agencies view cyberattacks through the lens of espionage and destructive operations, noting that state-led attacks differ fundamentally from criminal attacks. 2. State actors do not care about legal or financial consequences, making deterrence through penalties ineffective compared with ordinary crime. 3. Even when governments are responsible, actual operations are often conducted by individuals, contractors, or IT companies cooperating with state agencies—especially in China and North Korea. 4. Key objectives of hostile states include: intelligence collection, critical information theft, infrastructure penetration, and the spread of disinformation. 5. He highlights ongoing disinformation campaigns linked to geopolitical tensions, including attempts to influence public opinion in regions such as Taiwan. 6. Hostile states also use cyberattacks to support broader strategies such as military expansion, coercion, and intimidation. 7. Nikami cites recent major state-supported intrusions such as “Typhoon-type” attacks targeting telecommunications networks over long durations. 8. He notes that many victims remain unaware of intrusions for long periods, demonstrating the stealth and sophistication of state-backed	1. 公安調査庁の幹部として、国家が支援・関与するサイバー攻撃の特徴と、中国・北朝鮮の具体的な脅威、さらに公安調査庁の役割について説明している。 2. 国家関与のサイバー活動は、情報収集、破壊活動、偽情報・世論操作、暗号資産窃取などの犯罪的収益確保といったサイクルで行われると整理している。 3. 国家主体が関与する場合、任務達成のためにコスト度外視で攻撃を継続すること、実行部隊として民間ハッカー集団や IT 企業の技術者など「代理人」を使うことが大きな特徴だと指摘している。 4. 中国については、人民解放軍や国家安全機関が中核となりつつ、実務は委託された IT 企業などが担っており、他国の情報収集、偽情報の拡散・影響工作、台湾有事を見据えた偵察・事前活動が主な目的であると説明している。 5. 中国の例として、通信事業者ネットワークに長期潜伏し、通信メタデータや内容、位置情報を大量に窃取する「Salt Typhoon」などが挙げられ、米国当局による中国人ハッカーの刑事訴追や関連 IT 企業への制裁にも言及している。 6. 日本に対しても「MirrorFace」などと呼ばれるグループが活動しており、マスメディア、人権団体、反中国的な少数民族団体などを対象に、「インタビューさせてほしい」といった名目の標的型メールでマルウェアを送り込む、シンプルだが有効な手口が用いられていると述べている。 7. 北朝鮮については、国家保衛省や朝鮮人民軍の偵察総局などが関与し、IT 労働者を活用しながら暗号資産の窃取で外貨を獲得し、兵器開発などに転用すること、政治・軍事情報の収集や敵対国への報復的サイバー攻撃を行うことが特徴だと説明している。 8. 北朝鮮の事例として、暗号資産取引所を狙った攻撃グループが、関係者を特定した上で投資・資金調達を装うメール等でマルウェアを送り、ソーシャルエンジニアリングと技術的攻撃を組み合わせて巨額の暗号資産を窃取していることを紹介

operators. 9. Defending against such attacks requires protecting cyber assets, monitoring access rights, and preventing information leakage that enables social engineering. 10. Public Security Intelligence Agency efforts include tracing adversary activities on networks and contributing intelligence to shape Japan's national cyber policies.	している。 9. 北朝鮮 IT 労働者は、他国人になりすましたプロフィール写真や SNS・GitHub・LinkedIn などを使って海外企業からリモート案件を受注し、報酬を暗号資産で受け取ることで資金を北朝鮮に流すとともに、その立場を利用してアクセス権を獲得し、将来的なサイバー攻撃の足掛かりにする危険があると警告している。 10. 公安調査庁は、ネット上の技術情報の収集・分析に加え、背後にいる人物・組織の特定（身元解明）にも取り組み、情報コミュニティの一員として、関係機関のサイバー防御に情報面で貢献していきたいと締めくくっている。

1.26 D1-S7-5 Speeches from Japanese Government

D1-S7-5 SAWAKI Kiyoshi (Secretary General, Personal Information Protection Commission)	D1-S7-5 佐脇 紀代志 (個人情報保護委員会 事務局長)
1. Sawaki introduces the Personal Information Protection Commission (PPC) and emphasizes that personal data protection is inseparable from cybersecurity to enable trusted data use and innovation. 2. He outlines PPC's core roles: policy formulation under the APPI, compliance oversight, international cooperation, complaint handling/mediation, and public awareness. 3. PPC actively participates in global privacy governance, including the G7 Data Protection Authority Roundtable, producing communiqués on DFFT, emerging technologies, and enforcement cooperation. 4. G7 DPAs seek practical steps to operationalize DFFT, share best practices on AI governance, and create a unified enforcement case-sharing format. 5. The G7 statement stresses responsible innovation, privacy-by-design across the technology lifecycle, and stronger protection for children in digital environments. 6. PPC also collaborates with the EU, OECD, and global DPAs, and recently hosted a DFFT-focused international event to advance global data-governance alignment. 7. Personal data breach reports in Japan have risen to nearly 20,000 annually, prompting concern and deeper analysis.	1. 個人情報保護委員会（PPC）が日本におけるデータ保護・プライバシー政策の中核機関として、国の方針策定、国際協力、苦情・相談対応など幅広い役割を担っている点を紹介している。 2. PPC は「個人情報保護に関する基本方針（KPIPR）」を策定し、委員会による承認を経て国内政策を指針化している。また国際的な枠組みに積極的に関与し、各国当局と協調してグローバルなリスクに対応している。 3. 個人や事業者からの相談・苦情に対応し、必要に応じて事案をエスカレーションして行政指導・公表等を行うことで、国内のデータ保護体制の信頼性確保に努めている。 4. OECD や APEC などの国際会議・ワーキンググループに参加し、DFFT やデータ移転ルール、AI・新技術分野におけるプライバシーガバナンスの議論をリードしている。 5. プライバシー・バイ・デザインの重要性を強調し、AI や新技術を活用する場合も、設計段階からプライバシー保護を組み込むことが組織の信頼性向上とイノベーション推進につながると説明している。 6. 子どものデータ保護については、年齢に応じた配慮や教育環境での適切なデータ利用方針策定が重要であり、事業者・学校がリスクベースの対策を講じる必要があると述べている。 7. 最近の被害事例として、SNS 経由での不正アクセス誘導、VPN 機器の脆弱性悪用、UCR サイトを装ったフィッシングなど、個人情報を標的とした攻撃手口が多様化していると説明している。 8. SQL インジェクションによる侵入事例も依然として多く、Web アプリケーションの設計不備によって重大な情報流出につながり得るため、開発段階からの対策徹底が不可欠だと強

8. Sawaki highlights four common breach patterns: telework-related social-engineering attacks, exploitation of VPN vulnerabilities, phishing through fake websites, and SQL injection into web services. 9. Most incidents stem from basic weaknesses—poor authentication management, unpatched devices, website vulnerabilities, and cloud misconfigurations—and could be prevented with fundamental literacy and routine security practices. 10. PPC continues to work with other Japanese government agencies to coordinate cybersecurity efforts and urges organizations to strengthen governance to ensure consistent, basic data-protection measures.	調している。 9. 不正アクセス届出の分析から、クラウド設定ミス、国際的に悪用される脆弱性、古いサービス設定の放置などが主要な原因であり、継続的な設定点検が急務であると指摘している。 10. 政府内の連携図を示し、PPC が各省庁・関係機関とサイバー・プライバシー分野で密接に連携し、多様なリスクに対して政府横断で対応することが重要であると締めくくっている。

1.27 D1-S7-6 Speeches from Japanese Government

D1-S7-6 MIYAKE Fumito (Deputy Director General, Foreign Policy Bureau, Ministry of Foreign Affairs) Deputy Vice-Minister for Cyber Security and Information	D1-S7-6 三宅 史人 (外務省 総合外交政策局参事官)
1. Miyake congratulates Keio University and partners for hosting the 15th International Cybersecurity Symposium and highlights growing global attention to cybersecurity. 2. He outlines Japan's three foreign-policy pillars in cyberspace: rule of law, deterrence, and capacity building. 3. Japan promotes the rule of law in cyberspace, participating in long-standing UN discussions that culminated in agreement on norms and responsible state behavior. 4. A new global mechanism for ICT security will be launched, and the Ministry of Foreign Affairs (MOFA) is actively engaged to strengthen international governance. 5. Japan is introducing Active Cyber Defense (ACD), including pre-emptive access or neutralization of threats, even when servers are located overseas, consistent with international law. 6. Enhancing deterrence requires making cyberattacks costly for adversaries; attribution is	1. 外務省として、サイバーセキュリティ国際シンポジウムの意義を強調し、国家安全保障戦略（2022）で示された「欧米主要国と同等以上のサイバー対処能力」の実現に向けた政府全体の取り組みを紹介している。 2. 2025 年 7 月に国家サイバー統括室（NCO）が設置され、外務省を含む関係省庁が緊密に連携しながら政策を推進していると説明している。 3. 外務省の取り組みは「法の支配の推進」「抑止力の向上（攻撃者へのコスト付与）」「能力構築支援」の三本柱で構成されると述べている。 4. 法の支配の推進では、既存の国際法がサイバー空間にも適用されるという立場を支持し、国連 OEWG の議論を通じて国際的合意が形成された点を重要成果として評価している。 5. 国連 OEWG では、既存国際法のサイバー適用の再確認と、恒久的枠組み（グローバルメカニズム）の設置決定という二つの成果を挙げ、今後も国際議論へ積極参加すると述べている。 6. 抑止力向上の面では、攻撃者の手口を公表し特定する「パブリックアトリビューション」の有効性を強調し、日米韓や多国間での共同声明・注意喚起などを例に挙げている。 7. 国家を背景とする攻撃が高度化・頻発化し、軍事・先端

essential, and Japan works with the U.S., South Korea, and other partners on this. 7. Miyake references recent cases such as the April "Typhoon" (Salt/Vault Typhoon-type) activity, stressing the need to counter state-sponsored cyber operations. 8. Public attribution, strong messaging, and transparent disclosure of attacker methods are key tools for deterring future attacks. 9. Japan conducts extensive capacity building, including joint training with MIC, AJC/CBC, AFRAN, and large-scale programs for ASEAN nations—efforts highly praised internationally. 10. Japan will continue strengthening international cooperation across governments, private sector, and academia to achieve a free, fair, and secure cyberspace, aligning diplomatic efforts with the three core pillars.	技術・外貨獲得目的（特に北朝鮮）など脅威が深刻化しているため、国際協調による連携が不可欠だと説明している。 8. 能力構築支援では、タイ・ASEAN を中心に「AJCCBC」により約 4,400 名を研修し、アジア太平洋地域の能力強化に貢献していると述べている。 9. 日米韓協議では北朝鮮の IT 労働者問題、暗号資産窃取を含む攻撃活動への具体的対応方針を共有し、官民連携ワークショップも開催するなど、地域全体での対処を推進している。 10. サイバーセキュリティは官民全体の課題であり、民間企業の知見が不可欠であるとして、外務省としても国際連携と官民協力を強化し、社会全体のレジリエンス向上に努めると締めくくっている。

1.28 D1-S7-7 Speeches from Japanese Government

D1-S7-7 TAKIZAWA Ken (Deputy Vice-Minister for Cyber Security and Information、Ministry of Land, Infrastructure, Transport and Tourism)	D1-S7-7 瀧澤 謙 (国土交通省 サイバーセキュリティ・情報化審議官)
1. The speaker, Deputy Vice Minister Takizawa, introduces himself and outlines his long career in the Japanese government, including more than 30 years of work in MLIT-related administrative fields. 2. He emphasizes MLIT's responsibility over many critical infrastructure sectors in Japan, including transportation, aviation, logistics, and public works, which makes cybersecurity a core mission. 3. MLIT oversees 14 designated critical infrastructure sectors, and within six minutes of a major incident, more than 100 organizations may be affected—illustrating the scale and interconnectedness of the sector. 4. He describes the ministry's information-sharing platforms and communication systems designed to rapidly coordinate cybersecurity responses across diverse operators. 5. MLIT has developed specialized cybersecurity initiatives tailored to the characteristics of each	1. 国土交通省サイバーセキュリティ審議官として、交通分野における重要インフラのサイバーセキュリティ対策の現状、とくに国交省所管インフラに関する取組を説明する趣旨である。 2. 日本ではサイバー攻撃が全体として増加しており、社会に大きな影響を与え得る 15 分野の重要インフラに関連するインシデントも 2024 年度に初めて 50%を超えるなど、量・質ともに深刻化していると指摘している。 3. 交通分野の具体事例として、2023 年 7 月の名古屋港コンテナターミナルへのランサムウェア攻撃によりシステムが停止し、多数の船舶・コンテナ処理が滞り、自動車工場の操業停止を含む大きなサプライチェーン障害が生じたことを紹介している。 4. もう一つの事例として、2023 年末に国内航空会社で Linux 系マルウェア感染が発生し、社外システムとの通信障害から国内線・国際線の欠航・遅延が多発し、多くの利用者に影響が出たことを挙げている。 5. 国交省は重要インフラ 15 分野のうち、航空・空港（海運）・鉄道・物流・港湾・上水道の 6 分野（約 1400 事業者）を所管しており、これらの機能停止・低下を防ぐためにサイバーセキュリティ対策を重点的に進めていると説明している。

infrastructure domain, recognizing that sector-specific operational environments require customized security controls. 6. Following the 2020 revision of national critical infrastructure cybersecurity policy, each MLIT-related sector updated its security and safety guidelines to reflect modern cyber-risk conditions. 7. These guidelines emphasize identifying and addressing risks to information security and operational safety, ensuring resilience across transport-related infrastructure systems. 8. In the transport sector, MLIT established collaborative mechanisms—such as shared alert systems and operator networks—to disseminate threat information quickly and maintain situational awareness. 9. The ministry encourages operators to autonomously strengthen their security postures while maintaining coordination with MLIT for unified readiness against cyber threats. 10. In conclusion, the speaker stresses that cyberattacks and information leaks pose significant risks to critical infrastructure, and sustained, sector-wide security enhancement is necessary to ensure safe, stable, and continuous transportation services.	6. 政府全体の「重要インフラのサイバーセキュリティに関する行動計画」に沿って、国交省としては①ASM（オープンソース情報に基づく攻撃傾向・対策状況の把握と助言）、②重要インフラ向け SNS モニタリング、③重大インシデント時の駆けつけ支援、④分野別セキュリティ・安全ガイドライン改定、⑤OT-ISAC を通じた情報共有の 5 つの柱で対策を実施している。 7. ASM では、インターネット上の公開情報から攻撃傾向や脆弱性露出状況を分析し、事業者ごとの対策状況を評価して優先支援先を選定し、推奨対策を提示するとともに、所管局（鉄道局・航空局など）や事業者に傾向を共有して被害抑止につなげている。 8. SNS モニタリングでは、「予約サイトに接続できない」「勝手にキャンセルされた」などの投稿を常時収集・分析し、システム障害やサイバー攻撃の予兆と判断されるものを重要インフラ事業者へ速やかに通知し、被害の早期把握と拡大防止を図っている。 9. 駆けつけ支援は、名古屋港事案などの経験を踏まえ、重大なサイバー事案が発生した際に国交省の専門職員を現場に派遣し、被害拡大防止や再発防止策検討を支援する枠組みであり、国家安全保障戦略における「民間事業者への支援強化」の方針を受けて整備されたものである。 10. 分野別ガイドラインと OT-ISAC を通じて、経営層がサイバーリスクを経営課題として位置づけ、リスクマネジメントを徹底しつつ、事業者間・政府との情報連携によってサイバーセキュリティ水準の底上げを図り、交通など重要インフラサービスを安全かつ持続的に提供し続けることが国交省の役割だと結んでいる。

1.29 D1-S7-8 Speeches from Japanese Government

D1-S7-8 OKUDA Naohiko (Deputy Director General, Digital Agency)	D1-S7-8 奥田 直彦（デジタル庁 省庁業務サービスグループ審議官）
1. Okuda outlines the Digital Agency's mission: ensuring no one is left behind, modernizing government services, and improving inclusiveness across medicine, education, and disaster response. 2. He highlights major progress in My Number Card deployment—nearly 98 million cards issued (over 80% of population) and expanded use in emergency medical care and evacuation procedures. 3. Security is emphasized as foundational to all Digital Agency systems, including My Number	1. デジタル庁は「誰一人取り残さない優しいデジタル化」をミッションに、ガバメントサービス／スタートアップ志向で、行政サービスのデジタル化と利用者中心の設計を進めている。 2. マイナンバーカードは 2021 年時点の約 5,000 万枚から、2024 年 1 月には約 9,800 万枚・普及率約 8 割に達し、マイナ保険証登録や認証アプリ利用、救急搬送・避難所受付など災害・被災時の活用も拡大している。 3. デジタル庁は、政府共通のマイナンバー基盤システムやガバメントクラウド、GaaS などを所管し、NISC（内閣サイバー）の統一基準のもとで、実際のシステム構築・運用の側からセキュリティを確保する役割を担っている。 4. セキュリティ・ガバナンスとして、NISC 基準に準拠したセキ

infrastructure and national shared platforms such as NISC/NISC-related systems. 4. Digital governance is strengthened through centralized policy-setting, compliance audits, and digital system inspections across ministries and agencies. 5. A standardized security-by-design pipeline is enforced: risk analysis, secure procurement, supply-chain checks, vulnerability testing, and continuous security reviews throughout the system lifecycle. 6. The Agency maintains comprehensive Digital Security Guidelines (DS-xxx series), with the Security-by-Design Guideline as the core reference for development teams. 7. Technical guidance includes a vulnerability assessment guideline requiring both initial and periodic diagnosis to keep systems up to date against threats. 8. Okuda introduces CRSA (Continuous Risk Scoring & Action)—Japan's CDM-style framework for continuous monitoring, scoring vulnerabilities, prioritizing fixes, and maintaining real-time dashboards across government systems. 9. A centralized operation-monitoring system detects outages, performance issues, and security incidents, enabling coordinated response, triage, and management reporting. 10. Digital Agency also leads an inter-agency certification and coordination mechanism for entities handling highly sensitive information; seven agencies currently participate, with expansion underway to unify standards and improve efficiency across government.	ュリティポリシー策定、各システムのセキュリティ審査、脆弱性診断の実施を行い、NISC 側はそれらが政府基準に沿っているか監査・確認している。 5. デジタル庁は DS×3 桁番号で体系化した各種ガイドライン群を整備しており、特に「セキュリティ・バイ・デザイン」ガイドラインで、企画段階からのリスク分析、要件整理、調達時のサプライチェーンリスク考慮、脆弱性診断実施などをプロセスごとのチェックポイントとして定めている。 6. ゼロトラストアーキテクチャ適用方針を定め、GaaS への展開を進めるとともに、「システム構築時」と「定期実施」に分けた脆弱性診断ガイドラインを公表し、各システムのライフサイクル全体で継続的な検証を行う枠組みを整えている。 7. デジタル庁は多数のシステムを横断的に監視するため、個別システムのログ・設定情報を統合してリスク状況を評価する「日本版サイバー・セーフ・ガバメント（石破政府）」ダッシュボードの構築を進め、重要な脆弱性発生時に優先対応すべき端末・システムを迅速に抽出できるようにしている。 8. 統合運用監視システムにより、ネットワーク障害や不審なイベントをリアルタイムに把握し、影響範囲（利用者数や省庁業務への影響など）を評価しつつ、インシデント対応件数・復旧時間の記録を通じて将来の投資計画・増強方針の判断材料とする仕組みを整備している。 9. 政府情報システム向けクラウドサービスのセキュリティ評価制度「ISMAP」を運用し、統一の管理基準と監査により、政府機関が調達するクラウドの最低水準を担保するとともに、事業者側の重複負担を減らす方向で基準見直しやコスト低減も検討している。 10. デジタル庁は専門部署の設置と民間専門人材の活用により、これらのセキュリティ対策を継続的に強化し、国民が安心して政府情報システム・デジタルサービスを利用できる環境を整備していく決意を示している。

1.30 D1-S7-9 Speeches from Japanese Government

D1-S7-9 NAKANO Noriyuki (Deputy Director General for Cyber Security, Ministry of Defense, Japan)	D1-S7-9 中野 憲幸（防衛省大臣官房サイバーセキュリティ・情報化審議官）
1. Japan operates under three major strategic documents: the National Security Strategy, the National Defense Strategy, and the Defense Build-Up Program, all recently updated to	1. 現在は「戦後最も厳しい安全保障環境」にあり、陸・海・空に加えてサイバー空間でも自衛隊が行動することが不可欠であると位置づけている。 2. 国家安全保障戦略・国家防衛戦略・防衛力整備計画

advance national cyber posture. 2. The government plans to allocate roughly one trillion yen over five years to significantly strengthen its national cybersecurity capabilities. 3. Objectives include defending against sophisticated cyber threats, raising cybersecurity capacity across Japan, and reinforcing the trustworthiness and mission-readiness of cyber defense forces and industry. 4. MOD and the Self-Defense Forces are expanding their cyber-dedicated units, aiming for 4,000 specialized personnel by 2027 and up to 20,000 personnel involved in automated systems and related areas. 5. Cyber-dedicated staffing has already increased from 819 personnel in 2022 to 7,620 by the end of 2025, supported by systematic recruitment and training pipelines. 6. MOD established specialized cyber education programs, renamed institutions to emphasize cyber engineering, and expanded training for both domestic personnel and those sent abroad. 7. MOD shifted its security approach from eliminating risk to adopting continuous risk-management frameworks, incorporating vulnerability assessments, integration tests, and updated countermeasures. 8. A Defense Security Gateway is being implemented to secure information exchange between MOD and defense contractors, supporting cybersecurity in the defense industry. 9. Japan is strengthening international cyber cooperation, especially with the U.S. and Australia, conducting joint exercises, policy coordination, and team deployments, including participation in NATO CCDCOE activities. 10. Japan is advancing proactive cyber defense, establishing cyber-hunting capabilities, improving collaboration with police authorities, and enhancing mechanisms for handling confidential information.	の 3 文書において、サイバー防衛能力を欧米並み以上に引き上げ、5 年間で 1 兆円規模の投資を行う方針が示されている。 3. 防衛省・自衛隊は、①自らのサイバーセキュリティ能力の強化、②防衛産業のサイバー防衛を支える体制整備、③同盟国・同志国との連携強化、という 3 点を通じて我が国全体のサイバーセキュリティ向上を図る方針である。 4. 陸・海・空の「サイバー専門部隊」であるサイバー防衛隊を中核に、2027 年度までにサイバー専門要員約 4,000 人、システム調達・運用を含む関連要員を合わせて約 2 万人体制に拡充する計画である。 5. サイバー人材育成として、高等工科学校の「システムサイバー専修コース」新設、防衛大学校の「情報・法学科」を「サイバー情報・法学科」に改組、システム通信サイバー学校の設置などにより、基礎から高度まで体系的な教育・訓練を行っている。 6. システムの安全確保については、「導入前にリスクをゼロにする」発想から「リスクは常に存在すると認識し、運用中も継続的に管理する」リスクマネジメント重視の考え方に転換し、リスク評価・脆弱性検査・ペネトレーションテストを定期的に実施し、対象も基幹システムから装備品や制御システムを含む全システムへ拡大している。 7. 防衛産業向けには「防衛産業サイバーセキュリティ基準」を契約条件として適用し、基準を満たすためのサイバー対策コストを防衛省が支払う仕組みや、防衛セキュリティゲートウェイ等による安全な電子データ共有を通じて、産業側のサイバー防衛を下支えしている。 8. 国際連携として、日米首脳会談・2+2・防衛相会談等でサイバー防衛協力を確認し、NATO サイバー防衛協力センターへの参加、豪州との安全保障協力声明などを通じて情報共有・共同訓練を進めている。 9. NATO のサイバー演習「Locked Shields」に日米豪などと合同チームで参加し、その経験を踏まえて国内でも関係省庁・事業者と連携する体制づくりを進めるなど、演習・訓練を通じた実戦的なサイバー防衛能力の向上に取り組んでいる。 10. 能動的サイバー防御に関しては、自衛隊法改正を含む関連法が成立し、官民連携の強化や通信情報の活用、アクセス無害化措置などについて、警察・内閣官房（NSS）・NISC と平素から情報共有・調整しつつ、法施行までに具体的な運用体制を整備していく方針である。

1.31 D1-S7-10 Speeches from Japanese Government

D1-S7-10 NAKAMIZO Kazutaka (Deputy	D1-S7-10 中溝 和孝 (国家サイバー統括室 内閣審議

Director-General, National Cybersecurity Office)	官)
1. The speaker introduces examples of Japan's current cybersecurity advisory practices, including national policy renewal and public awareness initiatives. 2. Japan is updating cybersecurity policies and prevention frameworks, aligning national strategies with technological advances and international trends. 3. A key case study involves January's investigation into China-related cyber incidents, coordinated with allies such as the U.S. and U.K., as part of a multilateral response mechanism involving 10 countries. 4. Japan aims to strengthen warning mechanisms to better identify and attribute cyber-attack actors, enabling more effective defensive measures. 5. The three pillars of Japan's "Active Cyber Defense" are highlighted: protecting societal foundations, ensuring national safety, and executing coordinated government-wide implementation. 6. These pillars include operational measures, access-denial functions, and legislative frameworks, with further legal provisions to be implemented in stages from next year. 7. The government has compiled near-term, non-legislative cybersecurity actions, including strengthening command functions, enhancing public-private cooperation, fortifying critical infrastructure security, and expanding international collaboration. 8. PQC migration is presented as a concrete example: the U.S., EU, and U.K. have set timelines, and Japan began inter-ministerial PQC transition planning in May–June, aiming to release a governmental PQC roadmap by January. 9. Japan is drafting a new national cybersecurity strategy for release within the year, emphasizing five core principles, defense and deterrence under the new cyber-defense law, and achieving cyber capabilities on par with major Western	1．我が国のサイバー脅威は「質・量ともに著しく深刻化」しており、その状況を踏まえて対策を強化していることを冒頭で確認している。 2．対策の一例として、攻撃主体を名指しした注意喚起（アドバイザリ）を積極的に発出しており、トレーダートレーダー（北朝鮮関係）、ミラーフェイス（中国関係）、ソルトタイフーン（中国関係）などについて、攻撃手口と緩和策を示した共同声明・注意喚起を日米や 12 か国などと連名で公表している。 3．こうしたパブリックアトリビューション型の注意喚起はここ 2～3 年の傾向であり、今後も一層拡充することで、各主体の防御力向上と抑止効果の発揮を狙っていると述べている。 4．先般成立した「能動的サイバー防御」を実現する法律について、①官民連携の強化、②通信情報の利用、③アクセス無害化の 3 本柱から成ること、そして 3 本は共通目的（国民生活・経済活動・国家安全の保護）のために一体的に実施されるべきものだと説明している。 5．同法の施行は段階的であり、官民連携・アクセス無害化は来年秋、通信情報の利用はその 2 年後の秋を想定しており、関係省庁が現在準備・調整を進めていることを示している。 6．法律以外に直ちに実施可能な対策として、サイバーセキュリティ戦略本部が今年 5 月に「緊急に取り組むべき事項」を取りまとめ、①司令塔機能の強化（NCO の総合調整）、②官民の組織的対策強化、③人材・技術基盤の整備、④国際連携の 4 本柱で取り組んでいると述べている。 7．その中の具体例として、PQC（耐量子計算暗号）への移行を挙げ、米国・EU などが 2030 年代半ばを見据えて移行を進めている流れを踏まえ、日本でも政府機関の認証基盤（CA）移行に関するロードマップ骨子を年内に公表し、タイムラインと作業スケジュールを示す方向で検討していると説明している。 8．現行戦略の「情報の自由な流通」「開放性」など 5 つの基本原則は維持しつつ、脅威の深刻化を踏まえ、政府がより積極的な役割を果たす方向で新たなサイバーセキュリティ戦略を年内策定する方針であり、その柱として①深刻なサイバー脅威への対処（能動的サイバー防御の実装）、②社会全体（政府機関・重要インフラ・中小企業・個人）のセキュリティ・レジリエンス向上、③人材・技術（特に AI と量子技術）エコシステムの構築を掲げている。 9．新戦略では、政府機関自身の耐性強化を重点に据えつつ、AI for Security / Security for AI や、PQC を含む量子関連技術への対応を進め、パブコメや関係者との対話

nations. 10. The strategy also prioritizes nationwide cybersecurity resilience, AI-related security (AI for security / security for AI), quantum-related measures, and strong stakeholder and international cooperation, which the speaker stresses in closing.	を通じて戦略を仕上げていくとしている。 10. 最後に、これらの取組の実効性確保には政府だけでなく、国内外の多様なステークホルダーとの協力が不可欠であり、今後も国際連携と官民連携を一層強化したいと結んでいる。

1.32 D1-S7-11 Speeches from Japanese Government

D1-S7-11 AKASAKA Shinsuke (Deputy Director General for Cybersecurity and Information Technology Management, Minister's Secretariat, Ministry of Internal Affairs and Communications)	D1-S7-11 赤阪 晋介（総務省大臣官房サイバーセキュリティ・情報化審議官）
1. The speaker explains MIC's cybersecurity responsibilities, emphasizing cooperation with Australia and engagement in international initiatives such as the "Endurance Cybersecurity" project. 2. NICT's nationwide monitoring shows cyberattacks increasing exponentially; on average, one IPv4 address in Japan is targeted every 13 seconds, including attacks by nation-state actors. 3. Japan coordinates via the NISC (NCA), ensuring ministries align security measures and cooperate closely on national cyber defense. 4. As communications networks themselves form part of critical infrastructure, MIC highlights that protecting telecom infrastructure is equivalent to protecting national cybersecurity. 5. NICT's real-time attack-visualization system shows global attack traffic hitting Japan, with recent increases in IoT-based attacks (e.g., webcams, routers) and large-scale botnet-driven DDoS campaigns. 6. NICT identifies weak or already-infected IoT devices daily (2,800+ vulnerable devices; ~210 infected devices per day), issuing alerts to users via telecom operators. 7. Japan faces a technological dependency problem: only about 20% of its cybersecurity market is covered by domestic vendors, creating risks in incident response, data access, and	1. 総務省サイバーセキュリティ情報課の赤阪氏が、①政府全体のサイバー政策の中での総務省（MIC）の役割、②具体的な取組（安全確保・技術・人材）、③AI に関する新たな脅威と対策について説明している。 2. NICT（情報通信研究機構）が観測した結果、ネット上の攻撃関連通信は右肩上がりで増加しており、「1IP アドレスあたり 13 秒に 1 回」攻撃的通信が届く水準に達しており、ランサムウェアなどシステム停止・情報窃取型の高度な攻撃が、安全保障上の大きな問題になっていると指摘している。 3. こうした状況を受け、政府全体では国家サイバー統括室（NCO）が司令塔として 7 月に発足し、各省庁が所管分野ごとに施策を推進している中、総務省は通信ネットワークと地方自治体を所管する立場として、通信分野・自治体分野のサイバーセキュリティ政策を担当していると説明している。 4. 通信ネットワークはサイバー空間そのもののインフラであり、その安全性確保はサイバー空間全体の安全確保に直結するため、電気通信事業者との連携によるネットワーク防御に加え、NICT と連携した研究開発・人材育成に取り組んでいると述べている。 5. NICTER による攻撃観測の可視化では、日本に向けた攻撃通信が世界各国から集中している様子がリアルタイムで確認でき、とりわけルータや Web カメラなど IoT 機器をボット化して踏み台にする DDoS 攻撃が増加しており、航空・金融・通信事業者などへの DDoS が社会経済活動に大きな影響を与えていると紹介している。 6. こうした踏み台 IoT を減らすため、総務省は NICT と「NOTICE」プロジェクトを実施し、月 1 億超の機器を調査して弱いパスワードや未更新のファームウェアを持つ機器、既にマルウェア感染している機器を特定し、電気通信事業者経由で利用者に「危険な状態・既に感染」などを注意喚起し対

timely threat intelligence. 8. MIC and NICT are strengthening Japan's cyber-technology ecosystem by collecting national threat data, conducting malware analysis projects (e.g., NICTER, Starlight), and translating research into industrial and educational outcomes. 9. Japan suffers a severe cybersecurity talent shortage—far larger than peer countries—so NICT and MIC provide extensive training, practical cyber-range exercises ("CYDER/TIGER"), and youth-talent programs (e.g., SECCON). 10. The speaker highlights emerging AI-related threats, including adversarial examples, sponge attacks, prompt injection, and data-source poisoning; MIC is preparing guidelines to address "security for AI" and ensure safe development and deployment of AI systems.	策を促していると説明している。 7. 日本のセキュリティ市場における国産技術のシェアは約 1 割にとどまり、多くを海外製品・サービスに依存していることから、情報不足・対応遅延や対外依存のリスクがあると問題提起し、NICTER（マクロ観測）や STARDUST 等（ミクロ分析）でサイバー情報を収集・分析し、研究開発と産業創出につなげる「情報収集から産業化までのエコシステム」を回していく方針を示している。 8. 日本はセキュリティ人材も不足しており、「足りている」と答える企業が 6.5%に過ぎない一方、米豪では 9 割が足りていると回答しているとの調査結果を示したうえで、NICT と連携し、政府・自治体・重要インフラ向けの実践演習「CYDER」（年約 100 回・約 3000 人）や、25 歳以下トップ層向けの「SecHack365」などを通じて国内人材育成を進めるとともに、タイの AJCCBC を拠点に ASEAN 向けトレーニングも提供し、国際的なキャパシティビルディングにも貢献していると述べている。 9. 新たな脅威として AI に関するサイバーリスクを挙げ、「Security for AI（AI 自体への攻撃）」と「AI for Security（防御側の AI 活用）」の二つの観点があると整理し、この講演では主として前者を扱うとして、DoS／スポンジ攻撃（無害に見える入力で計算資源を枯渇させる）、プロンプトインジェクション（指示の上書き）、参照文書への埋め込み型インジェクション（評価の恣意的操作）など具体例を紹介している。 10. こうした AI への攻撃手口と有効な対策を整理するため、総務省は 2024 年 9 月から有識者会議を立ち上げ、研究者・セキュリティ専門家・AI 開発者らと議論を進めており、AI サービス開発者・提供者向けのガイドラインとして取りまとめることを目指して 2025 年 3 月までに作業を進めていると締めくくっている。

1.33 D1-S7-12 Speeches from Japanese Government

D1-S7-12 ONODERA Kenichi (Deputy Director General for Cyber Affairs Bureau, National Police Agency)	D1-S7-12 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 speaker explains that the police will present the current cyber-threat landscape, recent incident trends, and how law-enforcement is responding, especially around ransomware. 2. Ransomware attacks via email, SNS, and compromised websites are increasingly targeting critical sectors such as energy,	1. 近年、サイバー空間は社会経済活動の基盤となる一方で、フィッシング、ランサムウェア、DDoS、国家関与が疑われる攻撃、違法オンラインギャンブルや違法有害情報、災害時の偽情報など、多様かつ深刻な脅威が継続していると説明している。 2. フィッシングについて、報告件数は 2019 年以降急増し 2024 年には約 170 万件に達し、インターネットバンキング不正送金の約 9 割がフィッシング起因で、被害額は 87 億

transport, and finance, encrypting data and demanding payment for decryption. 3. National statistics show cyber incidents and suspicious communications rising sharply since 2019, with phishing and other malicious communications reaching well over a million cases per year. 4. Many ransomware intrusions exploit exposed VPN/remote-desktop devices; once infected, victims suffer severe impacts, with recovery often taking from one week to several months, and some organizations admitting to paying ransoms, sometimes more than once. 5. Police-run internet sensors continuously observe massive volumes of malicious scanning and attack traffic, more than 99% of which originates from overseas IP addresses. 6. To strengthen response, Japan created the Cyber Police Bureau and specialized cyber investigation units, which now handle nationwide major cases, support local police, and work to prevent secondary damage by sharing information and countermeasures. 7. Reported cybercrime cases continue to grow (over 13,000 in 2022), including incidents that misuse generative AI to create malware or unlawfully publish vulnerabilities. 8. The Cyber Police Bureau collaborates with foreign law-enforcement (e.g., Europol and others) in joint investigations, has identified key members of international attack groups, and, with partners, developed decryption tools that have helped multiple victim companies restore hundreds of thousands of encrypted files. 9. Japan has publicly attributed large-scale cryptocurrency thefts and other operations to state-linked groups from North Korea and China, issuing joint advisories with national cyber agencies to raise awareness and support global defensive measures. 10. A new Active Cyber Defense law was passed in May, enabling police to access attacker-controlled systems in narrowly defined cases to prevent serious damage; ahead of its entry into	円規模と過去最悪水準が続いていると指摘している。 3. フィッシング手口は、二要素認証を突破するリアルタイム型や、企業に電話でメールアドレスを聞き出して送信するボイスフィッシング、証券会社をかたるメールと証券口座不正アクセスの急増など、巧妙化・多様化していると述べている。 4. ランサムウェアは、VPN やリモートデスクトップ機器からの侵入が 8 割超を占め、2025 年上半期の被害報告は 116 件と高水準が続き、復旧には 1 週間～1 か月以上を要する例が多く、費用も 1000 万円超が約 6 割、1 億円超も存在し、経営への影響が極めて大きいと強調している。 5. 警察庁がセンサーで観測した結果、1IP アドレスあたり 1 日 9,085 件もの脆弱性探索等があり、その 99.4%が海外からの不審アクセスであるなど、国外からのサイバー攻撃の圧力が非常に高い状況にあると説明している。 6. こうした脅威に対応するため、2022 年にサイバー警察局を発足させ、国直轄のサイバー特別捜査隊をサイバー特別捜査部へ拡充し、特別捜査官も配置して約 370 人規模の体制とし、検挙・実態解明・被害抑止などを総合的に推進していると述べている。 7. サイバー犯罪の検挙件数は 2024 年に 1 万 3,164 件と増加しており、生成 AI を悪用した不正プログラム作成や詐欺サイト公開事件も含まれること、さらに FBI やユーロポール等と連携し、ランサムウェアグループ「コボス」関連事件で運営者特定・複合ツール開発・87 万件超のデータ復号などの成果を上げていると紹介している。 8. 国家を背景とする攻撃については、北朝鮮系グループ「TraderTraitor」による約 482 億円相当の暗号資産窃取事案や、中国系グループ「ソルトタイフーン」に関する国際共同アドバイザリーなど、捜査で得た手口・背景を公表し注意喚起するパブリック・アトリビューションを通じて抑止と被害拡大防止を図っていると説明している。 9. 警察は検挙だけでなく、企業との協定や日本サイバー犯罪対策センター（JC3）を通じた情報共有、金融庁・全国銀行協会と連名の啓発によるボイスフィッシング被害の急減など、関係機関・民間との連携による広報・注意喚起にも力を入れていると述べている。 10. 2024 年に成立した「能動的サイバー防御」に関する法律により、警察は重大なサイバー攻撃を防ぐため、攻撃に悪用されるコンピュータへのアクセス無害化措置を講じることが可能となり、来年の施行に向けて「導入して良かった」と実感される運用を目指して準備を進めていると結び、警察庁 HP の資料活用と、今後もサイバー空間の安全確保への理解と協力を呼びかけている。

force next year, the police are preparing to implement it and are publishing detailed situation reports and guidance on their website.	

1.34 D1-S7-13 Speeches from Japanese Government

D1-S7-13 OKI Kenji (Deputy Director-General, Systemic Stability and Risk Strategy Development and Management Bureau Financial Services Agency of Japan (JFSA))	D1-S7-13 大城 健司 (金融庁総合政策局参事官 (モニタリング担当))
1. The speaker outlines financial-sector cyber initiatives, including “Delta Walk,” sector-wide assessments, emergency exercises, and the publication of the annual Cybersecurity Report as part of Japan’s Financial Administration Policy. 2. Local financial institutions play a vital role in regional economies, but they face increasingly complex threats such as money-laundering, cyber fraud, and broader cyber-enabled financial crime. 3. Financial institutions are expected to strengthen cyber-risk management, following the recently updated Cybersecurity Guidelines that emphasize voluntary, continuous improvement rather than checklist-based compliance. 4. The guidelines stress that cyber risk is a top-tier management risk for financial institutions, requiring coordinated action across internal teams, external partners, industry bodies, and government agencies. 5. Required responses include baseline cyber hygiene measures for all institutions and more advanced best practices for larger or more systemically important entities, tailored to each institution’s business model and risk appetite. 6. Sector-wide maturity uplift is a priority: Japan has expanded participation in cyber-incident response exercises to record levels and promotes adoption of zero-trust architectures, internal network segmentation, and self-assessments for small and medium-sized institutions. 7. Third-party and supply-chain cyber-risk	1. 金融庁としてのサイバーセキュリティ施策は、①ガイダンス提供（サイバーセキュリティガイドライン等）、②モニタリング・検査（ヒアリングや検査、システム障害時の情報共有）、③横断演習や自己点検・PQC 移行などの「公助」の取組の 3 本柱で進めていると説明している。 2. 地域金融機関は人口減少・高齢化・人手不足・後継者不足など構造的課題に直面しており、マネロン・金融犯罪・サイバー攻撃対応のコストも増大しているため、共同システム利用等による効率化を含む「地域金融の強靱化プラン」を年内に取りまとめる方針であると述べている。 3. 近年、サードパーティ（業務委託先・クラウド等）経由のサイバー事故が増加しており、金融行政方針の中でサードパーティリスク管理の強化を重要課題として位置づけていると説明している。 4. 金融分野のサイバーセキュリティに関するガイドラインは、国内外の標準・実際のインシデント・監督経験を踏まえて策定され、銀行だけでなく取引所など金融市場インフラを含む監督対象すべてに適用される「自発的・継続的な改善」を促す枠組みであると位置づけている。 5. ガイドラインでは、サイバーリスクを企業経営に重大な影響を与える「トップリスク」と位置づけ、自助・共助・公助の組合せにより、規模・ビジネス特性・リスクプロファイルに応じて、基本対応と高度なベストプラクティスをリスクベースで選択・実施することを求めている。 6. 金融業界横断サイバー演習「デルタウォール」は 10 回目を迎え、特に中小金融機関の参加を拡大して過去最多の 177 社が参加し、境界防御の限界を踏まえた内部対策やゼロトラストの意識向上を狙っていると説明している。 7. 中小金融機関向けには、日本銀行・FISC・NISC/NCO と連携し、サイバーセキュリティ自己点検（CSA）を求め、その結果を集計・フィードバックすることで、グローバルフレームワークが乏しい層の成熟度把握と底上げを図っていると述べている。 8. サードパーティリスク管理については、形式的なチェックリストにとどまらず、契約前のスクリーニング、再委託の有無やセキ

management is being strengthened, moving from formalistic checks to lifecycle governance, including contract content, subcontractor oversight, disclosure obligations, and mandatory cooperation in incident response. 8. Japan has launched a PQC (post-quantum cryptography) working group for deposit-taking institutions, producing guidance that will also be useful for securities, insurance, and other financial sectors as they prepare for quantum-era threats. 9. PQC migration will require inventorying assets, updating systems, planning around vendor release schedules, and designing architectures flexible enough to accommodate rapidly evolving cryptographic standards—while starting preparations well before the 2030s quantum-computing horizon. 10. The speaker concludes by reiterating that cyber risk is rising globally and the financial sector must prioritize risk-based resourcing, strengthen cyber-governance, and collaborate closely with government agencies and industry associations to maintain resilience.	ュリティ水準の確認、委託期間中のモニタリング、インシデントを前提としたコンティンジェンシープラン整備など、ライフサイクル全体での実効的管理が必要であると強調している。 9. 量子コンピュータの実用化により既存暗号が破られるリスクに備え、PQC への移行は時間的余裕が少ないと認識しており、暗号資産も含めたインベントリ作成、サードパーティ提供システムの把握、優先度付け、暗号アルゴリズムを差し替えやすくする「Crypto Agility」などを経営層の強いコミットメントのもとで長期計画的に進めるべきだと述べている。 10. 金融分野は金融資産・個人情報・社会経済秩序に直結するためサイバーリスクに常時直面しており、金融機関がサイバー攻撃を「正しく恐れ」、サービス品質を落とさずリスクベースで資源配分・優先順位付けを行うことが重要であり、金融庁としても関係省庁・業界団体と連携しつつ「自助・共助・公助」の取組を継続的に推進していくと締めくくっている。

1.35 D1-S8 Day #1 Closing

Craig Wiener (Technical Fellow, MITRE)	クレイグ・ウィーナー (MITRE)
1. The speaker congratulates attendees for completing Day 1 and shares that this is his second time joining the Keio–MITRE conference. 2. Eleven ambassadors and chargés d'affaires participated, emphasizing the significance of the discussions and their commitment. 3. Strong focus was placed on Japan's new active cyber defense law as a strategic shift enhancing national security. 4. Speakers repeatedly highlighted that cybersecurity is inseparably linked to international security and that data protection is essential. 5. Critical infrastructure is increasingly at risk, and the community must prepare not only for incidents but for prolonged cyber conflict. 6. The speaker warns that future attacks will	1. 講演者は参加者が初日を終えたことを祝福し、自身が慶應 MITRE 会議に二度目の参加であることを伝えた。 2. 11 名の大使及び臨時代理大使が参加し、議論の重要性と自らの関与を強調した。 3. 日本の新たな能動的サイバー防御法が国家安全保障を強化する戦略的転換として強く焦点化された。 4. 登壇者は繰り返し、サイバーセキュリティが国際安全保障と不可分であり、データ保護が不可欠であると強調した。 5. 重要インフラはますます危険に晒されており、コミュニティは単発のインシデントだけでなく、長期化するサイバー紛争にも備えねばならない。 6. 登壇者は、将来の攻撃は単一企業を狙った孤立した事件ではなく、複数セクターにまたがる同時攻撃や連続攻撃となる可能性が高いと警告した。 7. 金融、通信、電力、水道、石油、ガスなどの分野は深く相互依存しており、危機はこうした依存関係を悪用すると強調した。

likely be multi-sector, simultaneous, or sequenced, not isolated events targeting a single company. 7. He stresses that sectors such as finance, telecom, electricity, water, oil, and gas are deeply interdependent, and crises will exploit these dependencies. 8. Despite decades of warnings (e.g., the 1997 U.S. directive), attacks on critical infrastructure continue to rise, with more than 50% of recent incidents hitting these sectors. 9. He raises concerns about whether adversaries follow the same rules and values, urging participants to consider whether current preparations are adequate. 10. The speaker concludes by emphasizing the need for collective security and cooperation, encouraging attendees to carry these reflections into Day 2.	8. 数十年にわたる警告（例：1997 年の米国指令）にもかかわらず、重要インフラへの攻撃は増加を続けており、最近のインシデントの 50%以上がこれらの分野を標的としている。 9. 彼は敵対者が同じルールや価値観に従うかどうか懸念を示し、参加者に現在の準備が十分かどうか考えるよう促した。 10. 講演者は集団安全保障と協力の必要性を強調して締めくくり、参加者にこれらの考察を 2 日目に持ち込むよう促した。

2 DAY 2: October 29 | West School Building 1F West Hall

2.1 D2-S1 Day #2 AM Opening

David Luzzi	デイビッド・ルッツィ
1. Day 2 of the 15th International Cybersecurity Symposium officially opened with remarks by David Lutzi of Northeastern University. 2. The symposium addresses cybersecurity for digitized national, economic, and societal security, emphasizing global multilateral public-private partnership actions. 3. Northeastern University conducts US$300 million in annual research and educates over 38,000 students across 17 campuses in the US, Canada, Ireland, and the UK. 4. Its renowned cooperative education program collaborates with more than 3,850 employers in 53 countries across all seven continents. 5. Northeastern offers bachelor's, master's, and PhD programs in cybersecurity and is a charter university of the International Cybersecurity Center of Excellence. 6. Northeastern faculty have played major leadership roles in top cybersecurity conferences, including IEEE Security & Privacy (2020, 2021, 2025, 2026) and ACM CCS 2025 in Taipei. 7. Faculty will also serve as program chairs for the Internet Measurement Conference (IMC) 2026 in Karlsruhe, Germany. 8. The Day 2 program begins with a keynote address by Anne Neuberger on cybersecurity for the digital society. 9. Additional introductory remarks will be delivered by Nobukatsu Kanahara (Sasakawa Peace Foundation) and Maria A. Roat (former US Deputy Federal CIO). 10. The speakers will lead two panels focused on active cyber defense and national cloud initiatives; Lutzi asked English speakers to speak slowly for interpreters.	1. 講演者は初日の終了を参加者へ祝賀し、自身が慶應MITRE 会議に二度目の参加であることを述べた。 2. 11 名の大使及び臨時代理大使が参加し、議論の重要性と自らの関与を強調した。 3. 日本の新たな能動的サイバー防御法は、国家安全保障強化に向けた戦略的転換として強く強調された。 4. 講演者らは繰り返し、サイバーセキュリティは国際安全保障と不可分であり、データ保護が不可欠であると強調した。 5. 重要インフラはリスクに晒される度合いが増しており、コミュニティは単独の事件だけでなく長期化するサイバー紛争にも備える必要がある。 6. 将来の攻撃は単一企業を狙った単独事件ではなく、複数分野にまたがる同時的または連続的な攻撃となる可能性が高いと警告した。 7. 金融、通信、電力、水道、石油、ガスなどの分野は相互依存が深く、危機はこうした依存関係を悪用すると強調した。 8. 数十年にわたる警告（例：1997 年の米国指令）にもかかわらず、重要インフラへの攻撃は増加を続け、最近の事象の 50%以上がこれらの分野を標的としている。 9. 彼は敵対者が同じルールや価値観を遵守するかどうか懸念を示し、参加者に現在の準備態勢が十分かどうか検討するよう促した。 10. 講演者は集団安全保障と協力の必要性を強調して締めくくり、参加者にこれらの考察を二日目に持ち越すよう呼びかけた。

2.2 D2-S2 Keynote Speech

Anne Neuberger (Senior Advisor a16z,	アン・ニューバーガー（シニア・アドバイザーa16z、スタンフォー

Distinguished Fellow, Stanford University and Royal United Services Institute (UK), Former Deputy National Security Advisor, USA)	ド大学と国王立防衛安全保障研究所（RUSI）名誉フェロー、 前米国国家安全保障担当副長官)
1. The speaker praises Japan's recent legislative progress and its role as a strong example in national cyber security. 2. Three main topics are introduced: (1) major cyber threats, (2) risk and resilience, and (3) AI's role in cyber offense and defense. 3. China is described as the most sophisticated state-level cyber threat, integrating cyber warfare into its military strategy and targeting global critical infrastructure. 4. North Korea uses cyber attacks, especially on cryptocurrency institutions, to evade sanctions and fund its missile program, including infiltrating organizations as IT workers. 5. Iran conducts aggressive cyber operations against adversaries, including compromising Israeli street cameras during missile strikes. 6. Russian criminal ransomware groups pose major global risks, exemplified by the Nagoya port attack and disruptions to hospitals. 7. The speaker emphasizes that cyberspace has no borders, creating shared vulnerabilities even for geographically protected nations like Japan and the U.S. 8. A key lesson from the NSA after the Snowden leaks: security models must evolve, accounting for insider threats and continuously adapting to changing adversaries. 9. FedRAMP is highlighted as a critical global standard; the U.S. updated its rules after China compromised Microsoft's cloud, showing the need for continuous improvement. 10. AI is portrayed as transformative—improving both vulnerability detection and network anomaly identification—ultimately strengthening national, corporate, and personal cyber defense.	1. 日本のサイバーセキュリティ水準とデジタル経済・安全保障分野での取り組みを高く評価している。 2. 政府と民間の協力を強化するため、日本が追加施策を進めている点を指摘している。 3. 講演では「脅威」「レジリエンス（回復力）」「AI の役割」という 3 テーマを扱うことを示している。 4. 国家レベルの脅威として中国を挙げ、通信侵害や重要インフラ攻撃のリスクに言及している。 5. 北朝鮮は制裁下でサイバー攻撃により資金調達をしており、暗号資産の窃取などが大規模化していると説明している。 6. イランも地域的緊張の中でサイバー攻撃を行うアクターとして位置づけられている。 7. 犯罪組織の脅威としてロシア系ランサムウェアが重要であり、港湾・医療機関などへの攻撃例に触れている。 8. 組織はリスク管理や防御モデルの更新が追いついていないことがあり、内部脅威も含めた新たな視点が必要と指摘している。 9. 米国では FedRAMP のような標準化が重要であり、世界的に防御力向上のため標準のアップデートが不可欠であると述べている。 10. AI は攻撃・防御の両面に影響を与え、脆弱性発見、自動化、防御強化、ネットワーク可視化などに大きく寄与することを強調している。

2.3 D2-S3 Speech

Nobukatsu Kanehara (Executive Director, Sasakawa Peace Foundation)	兼原 信克 (笹川平和財団 常任理事)

1. The speaker reflects on serving as Deputy National Security Advisor under Prime Minister Abe and explains that progress in Japan's cybersecurity was long blocked by constitutional debates over Article 21. 2. He describes how constitutional interpretations once protected even foreign adversaries' communications, delaying meaningful cybersecurity reforms until very recently. 3. A major incident ("Black Shark") triggered the government to take cybersecurity seriously, leading to new laws and the formation of Japan's cyber police and cyber army. 4. He stresses that cyber threats are real and rapidly growing, outpacing Japan's current governmental capabilities, with constant probing from China and North Korea. 5. Japan's society is now deeply dependent on cyberspace and data, making it extremely fragile; a single attacker abroad could paralyze Japan's infrastructure. 6. He argues that critical infrastructure—not only the military—must be protected, and Japan needs a national-scale hyperscale cloud to ensure resilience. 7. The new law enabling attribution and neutralization of malware is insufficient, as it covers only criminal matters and not military or intelligence cyber operations. 8. He emphasizes the need for cyber deterrence: Japan must demonstrate reciprocal offensive capabilities to dissuade adversaries, similar to nuclear deterrence logic. 9. Japan is significantly behind leading cyber powers; although Japan has money, technology, and skilled hackers, it lacks coherent policy and must accelerate action. 10. He concludes that the new law is only the beginning, and the government must multiply its efforts to defend the nation and prepare for cyber contingencies.	1. 日本は憲法解釈の制約などにより、ここ数年サイバーセキュリティの躍進が十分に進まなかったが、近年ようやく議論が整理されつつある。 2. 政府は新たな「サイバーポリス」や「サイバー部隊」創設を検討しており、本格的な体制整備に向けた法案準備が進んでいる。 3. 日本は米国・欧州・中国・北朝鮮に追いつくには時間がかかるが、方針が決まれば迅速に動けると述べている。 4. 脅威は現実に存在し、政府はその危険性を国民に正しく認識させる必要があるとしている。 5. インフラ障害（新幹線停止など）も他国によるテスト的サイバー攻撃の可能性があると指摘している。 6. データ量の爆発、クラウド依存、AI による高速処理などにより、社会は「データの海」にあり、脅威の構造も変化していると述べている。 7. 中国や北朝鮮は高度なサイバー攻撃能力を持ち、日本の重要インフラも容易に攻撃対象となり得ると強調している。 8. 日本は島国として安全であるという歴史的感覚が残っているが、サイバー空間ではもはや地理的防御は通用しないと説明している。 9. 新たな法律では「ハックバック」のような対抗措置も議論されているが、軍事・インテリジェンスの統合的な対応がまだ不十分と指摘している。 10. 日本は技術・資金・人材を持ちながらも政策面の遅れが大きく、国際基準の"クラス C"レベルにとどまっているため、政府が本格的に追いつく努力を急ぐ必要があると述べている。

2.4 D2-P1 Panel

Theme: New Acts on Active Cyber Defense (Government Defense) Moderator: Nobukatsu Kanehara Panelists: - Mike Studeman (retired RADM, U.S. Navy, MITRE national security fellow) - Chris Capper (British Embassy) - Urmas Ruuto (Head of Technology Branch, CCDCOE) - Gloria Glaubman (Founder & Principal, GMG Consulting)	テーマ：新法、サイバーセキュリティ基本法の改定 モデレーター：兼原 信克 パネリスト： - マイク・スタデマン（MITRE の国家安全保障フェロー、元海軍少将） - クリス・キャッパー（英国大使館） - ウルマス・ルートゥ（CCDCoE 技術支部長） - グローリア・グローブマン（GMG コンサルティング創設者、プリンシパル）
1. The panel agrees that cyber threats are real, rapidly growing, largely invisible to ordinary citizens, and can devastate modern data-driven societies much like a “tsunami or typhoon.” 2. Experts highlight China’s capabilities (living-off-the-land, large-scale zero-day hoarding without an equity process, use of frontier AI) and its loosely regulated security-company ecosystem as a major strategic risk, contrasting this with more regulated approaches in the UK and elsewhere. 3. Panelists are broadly optimistic that AI can favor defenders: AI can inventory assets, automate threat hunting and triage, detect anomalies at scale, and strengthen zero-trust architectures—provided networks are well-managed (MFA, segmentation, patching, continuous monitoring). 4. NATO’s Cooperative Cyber Defence Centre of Excellence (CCDCOE) explains its dual focus on defensive (Locked Shields) and offensive (Crossed Swords) exercises, stressing that the best defenders are those who deeply understand offensive methods and insider-driven attacks. 5. On public–private cooperation, the U.S. “safe harbor” model (legal protection for companies that share incident data) and similar mechanisms are cited as key to overcoming corporate shame, market fears, and liability concerns, and to enabling governments to synthesize and redistribute threat intelligence.	1. 現代は目に見えないサイバースペースとデータドリブン社会の中で生きており、その利便性と同時に深刻な脅威が存在することを国民に理解させる必要があると議論している。 2. 中国は脆弱性情報の管理や AI 活用を含む高度なサイバー能力を持ち、ゼロデイを含めた“環境規制型アプローチ”で長期的・静かな侵入を行っており、これに対抗するためには責任ある脆弱性報告プロセスや規制が不可欠であると指摘している。 3. 英国・フランスなどは脆弱性報告制度や能動的サイバー防御の枠組みを整備しており、AI を防御側に積極活用しつつ、ゼロトラスト、多要素認証、ネットワーク分割、スレットハンティングなど基本防御の徹底が重要だと述べている。 4. NATO CCDCOE（NATO サイバー防衛協力センター）の演習（ロックシールド／クロスソード）などから、ロシアの攻撃は必ずしも高度ではなく、重要インフラ攻撃の多くにインサイダー関与が見られること、よって内部対策とレジリエンス強化が鍵であると説明している。 5. 日本では攻撃被害を企業が公表しにくい文化があり、政府が誰がどこを攻撃されているか把握しにくいことから、米国のセーフハーバー制度のように、法的リスクを軽減しつつインシデント報告と情報共有を促す仕組みが重要だと議論している。 6. 重要インフラとサプライチェーンを広く捉えた規制・責任分担（サイバー・レジリエンス法的な発想）が必要であり、ハイパースケーラーと国内企業をうまく組み合わせ、多様なベンダーによるエコシステムと相互運用性を確保すべきだと述べている。 7. 政府クラウド／ガバメントクラウドについて、日本はまだ“石器時代”的な紙・FAX 依存が残っており、データ洪水と AI 活用を前提に、クラウド・AI を前提としたデジタル政府アーキテクチャと統括組織を早急に整備すべきだという問題意識が示されている。 8. サイバー要員・ハッカーの確保では、政府内に数千人規

6. There is sharp debate over government responsibility for critical national infrastructure: some argue government cannot directly protect all operators and should instead enforce regulation and assurance schemes, while using tools like the UK's forthcoming Cyber Security Resilience Bill and China-style rapid incident-reporting mandates as contrasting models. 7. For cloud and hyperscalers, the panel recommends a "diversity and redundancy" strategy: avoid dependence on a single U.S. hyperscaler, mix multiple global and domestic providers, design interoperable stacks (Taiwan is cited as a model), and use certifications and zero-trust controls to manage shared government and critical-infrastructure clouds. 8. On talent and insider risk, speakers stress building teams of capable hackers (including neurodiverse profiles), using aptitude testing and reservist programs, and managing insiders through rigorous security clearances plus continuous evaluation and strict need-to-know data segmentation to prevent another "Snowden-type" breach. 9. Disinformation and cyber operations are increasingly fused: adversaries combine influence campaigns with technical actions such as DDoS, and use AI to craft highly targeted, realistic phishing and online narratives—so responses must combine cyber, diplomatic, legal, sanctions, and public-education measures, not treat "cyber" and "information" as separate silos. 10. For cyber deterrence and international norms, the UK framework of "deterrence by denial and by cost" is presented: build resilience, use joint attributions, sanctions (including thematic cyber sanctions against non-state actors), and transparency about national doctrine, while pursuing minimum mutual trust and stronger international cooperation so that free societies can collectively manage escalation and maintain order in cyberspace.	模のサイバー部隊が必要になる一方で、採用・待遇・規律・セキュリティ・クリアランス（継続的モニタリングを含む）をどう設計するかが大きな課題であり、スノーデン事案の教訓として「一人で何でも見られる設計」を避けるべきだと議論している。 9. サイバー攻撃とディスインフォメーションは一体のハイブリッド攻撃として行われており、選挙や世論操作への介入を含めて、AI 生成コンテンツに対応できるエンドユーザー教育と、サイバー＋情報戦を統合的に扱う防御体制が必要だと強調している。 10. 国際的なルールや抑止については、核抑止に類似した「相互抑止」や制裁枠組み（個人・グループへのサイバー制裁、信頼と不信の操作）を組み合わせつつ、同盟国間でアトリビューションや防御アプローチを共有し、中国・ロシア・北朝鮮などを念頭にサイバースペースの秩序と国際協調を構築する必要があると結論づけている。

2.5 D2-S4 Speech

Maria A. Roat (the first Director of the FedRAMP program in the U.S. and the former U.S. Deputy Federal Chief Information Office)	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、元連邦最高情報責任者)
1. The speaker was brought into FedRAMP when it was in a “startup mode” to provide credible technical leadership, communicate clearly with government and industry, and drive execution from vision to full operations. 2. FedRAMP shifted U.S. federal cybersecurity from checkbox compliance to true risk management, supporting the cloud-first policy with a risk-based set of NIST-aligned baseline controls tailored specifically for cloud (IaaS/PaaS/SaaS) rather than on-prem data centers. 3. The program forced both government and cloud service providers to understand shared responsibility and control inheritance across the stack, and it compelled CSPs to improve patching, configuration management, least-privilege access, and incident response. 4. Continuous monitoring and independent validation became core: accredited 3PAOs assessed implementations, and an additional independent body audited those assessors biannually to ensure rigor and integrity of the assessment ecosystem. 5. Data residency and architecture transparency were critical: U.S. government data had to remain in domestic data centers, with detailed review of provider architectures to prevent lateral movement and to understand exactly how packets and data flowed through cloud environments. 6. FedRAMP’s success led to broader adoption (e.g., U.S. states via “StateRAMP”) and demonstrated that a standardized, prescriptive baseline could be a game changer for secure cloud adoption at scale. 7. The speaker argues that Japan now faces a defining moment: its national security, economic competitiveness, critical infrastructure, and government services all depend on secure cloud,	1. 自身は、政府と民間の両方と技術的かつ政策的に対話できる人材としてリクルートされ、FedRAMP プログラムをスタートアップ段階からフルオペレーションまで導いたトランスフォーメーション／チェンジマネジメント役であったと説明している。 2. FedRAMP は、米国のクラウドファースト政策の下で、「チェックリスト型コンプライアンス」から「リスクベースのクラウドセキュリティ」へと政府と業界を移行させるゲームチェンジャーとなった枠組みであり、業界と政府の専門家が協働してセキュリティコントロールのベースラインを作り上げたと述べている。 3. このベースラインにより、インフラ／プラットフォーム／ソフトウェアごとに「誰がどこまで責任を持つか」という共有責任モデルが明確化され、クラウドプロバイダ側もパッチ管理や変更管理、インシデントレスポンスのプロセスを大幅に合理化・高度化せざるを得なくなったと説明している。 4. プログラム初期にはクラウドを単なるコンプライアンス演習とみなす文化的抵抗があったが、9 か月でフルオペレーション体制を築き、継続的モニタリングと第三者評価（3PAO）を組み込むことで、「生きたリスクマネジメント」として機能させた点を強調している。 5. 独立した監査・評価団体による年次監査や、データ所在地・データの流れをクラウドアーキテクチャの中で明確に把握することが、信頼性やレジリエンス確保の要であり、FedRAMP をベースに StateRAMP なども生まれてきたと述べている。 6. 日本に対しては、国家安全保障・経済安全保障・デジタル政策の土台として「拡張可能で安全なクラウドサービス」が不可欠であり、国家レベルのスピードと調整力を持ったリスクベースのクラウド認証プログラムを構築すべきだと提言している。 7. その際、ゼロトラスト、分散・リージョンベースの配置、最小権限アクセス、サプライチェーン・データセンターセキュリティなどを組み込んだソブリンクラウドを構想し、ティア分けされたリスクモデルと自動化された保証（CI/CD へのセキュリティ統合）を備えたエコシステムを作ることが重要だとしている。 8. 技術設計だけではなく、チェンジマネジメントが成功の鍵であり、センター・オブ・エクセレンスの設置、人材育成・トレーニング、評価者・セキュリティエンジニア・外部委託を含む体制整備、パイロットとメトリクスによる「小さく始めて測る」アプローチが必要だと強調している。 9. 日本はすでに高い技術力、産業基盤、政策成熟度を持っているので、「クラウド・ジャパン」とも言うべき世界水準のナショナルクラウド認証プログラムを構築できる素地があり、それに

making a FedRAMP-aligned national authorization program a strategic necessity beyond ISMAP-style compliance checks. 8. Such a program for Japan should support national resilience, data sovereignty, and economic policy by validating security (not just claiming it), strengthening supply-chain integrity, enabling secure domestic cloud capability, and lowering barriers for SMEs to serve the public sector. 9. Technical design alone is insufficient; success hinges on strong change management: executive sponsorship, a national center of excellence, embedded cloud security engineers, robust training and workforce development, and starting with measurable pilots that demonstrate value. 10. The speech ends with a call to action for Japan to move from policy intent to concrete implementation—establishing an authorization office, publishing rules, funding pilots, building skills, and continuously proving trust in a "national cloud" as a tool for resilience, growth, and digital sovereignty.	より、継続するサイバー／インサイダー脅威に対抗しつつ、レジリエンス、経済成長、効率的で迅速なデジタル行政サービスを実現できると結びとしている。

2.6 D2-P2 Panel

Theme: National Cloud Moderator: Maria A. Roat Panelists: - Chris Grady (CTO, CyLogic) - SUZUKI Tomoharu (Leader, Security and Crisis Management, Strategy and Organization Group, Digital Agency) - Harri Hursti (Co-founder of DEF CON Voting Village) - Koichi Kawaguchi (Managing Director, the Organization for National Supply-Chain Vitalization ("ONSV"))	テーマ：国家クラウド モデレーター： マリア・A・ロート パネリスト： - クリス・グラディ (CyLogic 社 CTO) - 鈴木 智晴 (デジタル庁 戦略・組織グループ セキュリティ・危機管理担当 リーダー) - ハリ・ハースティ (DEF CON Voting Village 共同ファウンダー) - 川口 幸一 (サプライチェーン強化機構 マネージングディレクター)
1. The panel brought together a U.S. sovereign-cloud CTO (Chris), Japan's Digital Agency/ISMAP lead (Suzuki), an investment fund manager focused on economic security (Kawaguchi), and hacker/Internet pioneer Harry, to discuss "national/sovereign cloud" from technical,	1. パネルではまず、米国重要インフラ向けソブリンクラウドを推進する起業家クリス氏、クラウド評価制度 ISMAP を所管するデジタル庁の鈴木氏、経済安保ファンド準備中の投資家・川口氏、ハッカー／セキュリティ研究者のハリ氏らが自己紹介し、それぞれ「国家クラウド／ソブリンクラウド」を異なる立場から議論する枠組みが示された。

regulatory, investment, and security perspectives. 2. Chris defined a sovereign cloud not just as infrastructure physically in-country and subject to domestic law, but as including knowledge sovereignty: the local ability to build, operate, secure, and support the cloud even in crisis (e.g., war in the region, undersea cables cut, no foreign engineers available). 3. Suzuki explained ISMAP as Japan's cloud security assessment scheme inspired by FedRAMP but not identical: it checks governance/management/control requirements via external audits, emphasizes confidentiality for certain government use, but does not itself enforce data-center location in Japan or directly guarantee "sovereignty" or data-sovereignty. 4. Japan's Government Cloud was described as stricter than ISMAP (requiring domestic data centers) and currently using major U.S. hyperscalers plus Sakura Internet as the only domestic provider; however, Sakura's "domestic cloud" is not yet treated as a special sovereign tier—there is effectively no formal "sovereign cloud" category in policy today. 5. From a U.S. perspective, Chris stressed that all data must be encrypted in transit and at rest and that AI changes the game: critical datasets (e.g., medical, genetic, financial) are "crown jewels," and AI workloads will increasingly run where the data lives (on-prem/edge), which argues against shipping huge volumes into centralized hyperscale regions. 6. Harry warned that AI training data in English/Spanish is already heavily tainted by AI-generated content, making untainted data (such as high-quality Japanese text and sensitive real-world data) exceptionally valuable; he also highlighted technical risks of multi-tenant hyperscale (shared silicon, imperfect isolation, zero-day hypervisor attacks) and the need to scrutinize how cloud providers actually provision and isolate hardware. 7. Both Harry and Chris argued that Internet	2. ソブリンクラウド・ナショナルクラウドの定義について、単に「国内にデータセンターを置くこと」ではなく、法規制・運用ノウハウ・有事対応能力も含めて、自国でクラウドのセキュリティポジションと運用をコントロールできることが本質であると整理された。 3. 鈴木氏から、日本のクラウドセキュリティ評価制度 ISMAP の仕組み（ガバナンス／管理／コントロール基準を外部監査で確認し、政府機関がそのリストからサービスを調達する仕組み）が説明されつつ、ISMAP は主権やデータ主権を直接評価する制度ではなく、データセンターの国内限定も原則要件ではないことが指摘された。 4. 日本政府のガバメントクラウドでは、ISMAP 登録に加えて「国内データセンター要件」などを課しており、AWS・Azure・Google・OCI に加え、唯一の国産クラウドとしてさくらインターネットが条件付き採択されているが、現時点で"ソブリンクラウド"として特別扱いされているわけではないと説明された。 5. データ保護と AI 時代の競争力について、データは「アルゴリズム以上に価値を持つ燃料」であり、医療・金融・遺伝子・行動履歴など高秘匿データが自動的に生成・収集される時代には、ほぼすべてのデータが守るべき戦略資産になるという投資家・技術者双方の見解が共有された。 6. ハイパースケーラー型クラウドについては、リソース共有と集中（同一チップ／同一ハイパーバイザ上のマルチテナント）がゼロデイ利用や大規模攻撃時のリスク要因になること、AI ワークロードの増大とともに「分散・エッジ回帰」や、どの物理インフラを誰と共有しているかの透明性が重要になることが議論された。 7. 川口氏は、クラウド市場は日本で急成長しデジタル赤字の源泉にもなっていることから、「国産クラウド」を公共財レベルの社会基盤と位置付け、政府クラウドだけでなく民間向けクラウドを育成しないと、将来すべての基幹データが海外ハイパースケーラーに握られ、主権と経済力を失うリスクがあると警鐘を鳴らした。 8. 政府・官民連携の役割として、政府は FedRAMP のような強い要件と評価スキーム（日本版"J-RAMP"のようなもの）を示し、長期の政府契約や補助金で国産クラウドの初期投資とスケールを支えるべきであり、そこから民間利用へ広げていく「パイロット→スケール」の戦略が有効だという提案がなされた。 9. 日本が向こう 12 か月で取り得るアクションとして、①FedRAMP に学んだリスクベースのクラウド認証プログラム導入、②ガバメントクラウドで国産事業者（さくらなど）が確実に本採択されるよう政策的に育成すること、③市場規模と

and security history favor decentralization: centralized hyperscale regions create single points of failure (illustrated by US-East outages) and attractive targets, whereas a more distributed, capacity-planned, “edge + regional” model better aligns with resilience and national-security needs. 8. Kawaguchi, from the investor viewpoint, framed domestic cloud as a major economic-security and growth opportunity: Japan’s cloud market is large and growing, cash flow from cloud is stable and sticky (very low churn), but dependence on foreign hyperscalers fuels a mounting “digital trade deficit” and leaves national infrastructure and pricing power (e.g., sudden 30% price hikes) in foreign hands. 9. On the role of government, Chris argued that progress like FedRAMP in the U.S. only happened because government made prescriptive security frameworks mandatory and tied them to real contracts; the panel suggested Japan should consider a FedRAMP-like, risk-based program (a “Japan-RAMP”) plus long-term government commitments/subsidies to help domestic providers climb the CapEx and scale barrier. 10. In Q&A, the audience raised three tensions: (a) interoperability vs. protecting sensitive national-security data in sovereign clouds, (b) the risk that adopting FedRAMP wholesale could lock Japan into U.S. tech and standards, and (c) the need to grow private-sector domestic cloud (not just government cloud) to avoid repeating the mainframe decline; panelists responded that Japan must design frameworks that reduce provider burden, avoid one-way dependence, and explicitly include industrial/private cloud in its national cloud and digital-sovereignty strategy.	ビジネス機会を見える化して国産クラウドへの投資を呼び込むことなどが挙げられた。 10. Q&A では、主権クラウド間の相互接続と安全保障のトレードオフ、FedRAMP 規格への一方的追従による米国企業優位化への懸念、政府クラウドに偏った議論ではなく民間クラウド育成が重要であることなどが質問され、パネリストは「セキュリティ評価（ISMAP 等）」と「主権・データ主権」「民間の産業政策」を分けて設計し、日米連携と国産育成を両立させる必要があると応答して議論を締めくくった。

2.7 D2-S5 Day #2 PM Opening

Luiz DaSilva	ルイス・ダ・シルヴァ
1. Professor Luis da Silva opens the afternoon session of Day 2 of the 15th International Cyber	1. ルイス・ダ・シルバ教授が、第 15 回国際サイバーセキュリティシンポジウム 2 日目の午後のセッションを開会した。

Security Symposium. 2. He introduces himself as the Bradley Professor of Cyber Security at Virginia Tech and Executive Director of the Commonwealth Cyber Initiative (CCI). 3. CCI is a consortium of 47 universities and colleges in Virginia focused on cybersecurity research, innovation, and workforce development. 4. He highlights the morning's remarks emphasizing the importance of international engagement to counter borderless cyber attacks. 5. He mentions his role as a board member of the International Cybersecurity Center of Excellence (INCS-COE), which has members from nine countries. 6. INCS-COE collaborates internationally on diverse topics such as healthcare cybersecurity, AI for cybersecurity, cybersecurity for AI, energy systems, and space technology. 7. He will assume the role of Chair of the INCS-COE Board starting January 2026. 8. He emphasizes that international collaboration in cybersecurity research is central to the strategy of Virginia Tech and CCI. 9. He notes increased engagement with Japan, including funded projects with Japanese companies and a new MOU with Science Tokyo, expressing appreciation for being at Keio University again. 10. He previews the afternoon program covering information sharing, cyber-AI, and quantum security, delivered by speakers from government, industry, and academia.	2. 彼は、バージニア工科大学のブラッドリー教授（サイバーセキュリティ）であり、コモンウェルス・サイバー・イニシアチブ（CCI）の事務局長であることを自己紹介した。 3. CCI は、サイバーセキュリティの研究、イノベーション、人材育成に焦点を当てた、バージニア州の 47 の大学・カレッジのコンソーシアムである。 4. 彼は、国境を越えたサイバー攻撃に対抗するための国際的な取り組みの重要性を強調した午前中の発言を強調した。 5. 彼は、9 カ国からメンバーが参加している国際サイバーセキュリティ・センター・オブ・エクセレンス（INCS-CoE）の理事としての自分の役割について言及した。 6. INCS-CoE は、医療サイバーセキュリティ、サイバーセキュリティのための AI、AI のためのサイバーセキュリティ、エネルギーシステム、宇宙技術など、様々なトピックについて国際的に協力している。 7. 彼は 2026 年 1 月から INCS-CoE 理事会の議長に就任する予定である。 8. 彼は、サイバーセキュリティ研究における国際協力が、バージニア工科大学と CCI の戦略の中心であると強調した。 9. 日本企業との共同プロジェクトや東京科学大学との新たな覚書締結など、日本との連携強化に触れ、慶應義塾大学での再訪に謝意を表明した。 10. 午後のプログラムでは、政府・産業界・学界の講演者による情報共有、サイバーAI、量子セキュリティに関する発表が行われると予告した。

2.8 D2-S6 Speech

Koichi Akaishi (JDTF Chairman)	赤石 浩一 (JDTF 会長)
1. Innovation and international collaboration are central to Virginia Tech / CCI's strategy, with growing engagement in Japan through funded projects and an MOU with Science Tokyo, highlighting the importance of global partnerships in cybersecurity.	1. サイバー空間における「トラスト」が地政学的リスク（戦争・テロ・権威主義・サイバー攻撃・偽情報）の高まりの中で、同盟国間・同志国間にとって戦略的に不可欠であると位置づけている。 2. 早期警戒・脅威検知のための情報共有により、テロ・大規模災害・軍事エスカレーションなどを事前に察知し、外交

2. The afternoon program focuses on cutting-edge issues—information sharing, cyber-AI, and quantum security—featuring speakers from government, major companies, and universities to stress public-private partnership in cybersecurity. 3. Akaishi emphasizes that intelligence sharing is strategically essential (not just beneficial) in today's era of authoritarianism, cyber warfare, terrorism, and disinformation—both among allies and between governments and the private sector. 4. He outlines key benefits of allied intelligence sharing: early warning and threat detection, coordinated military/diplomatic responses, stronger cyber and technological defenses (especially for critical infrastructure), better handling of hybrid/misinformation campaigns, and deeper diplomatic trust and alliance cohesion. 5. As concrete models, he cites Five Eyes frameworks such as ECHELON (global SIGINT collection and sharing) and XKEYSCORE (searching vast intercepted-data stores), enabled by highly integrated, trusted digital systems built over decades. 6. Sharing intelligence with private companies is increasingly vital because they own most critical infrastructure and are primary cyber targets; timely, detailed threat intel from governments and big IT firms supports protection, coordinated cyber defense, and dual-use defense innovation (including start-ups). 7. Major challenges include technical interoperability (different platforms, formats, legacy systems), security and trust (a single weak node can endanger the whole system), legal and policy barriers (divergent privacy/surveillance laws, classification rules), and timeliness (bureaucratic delays reducing operational value). 8. Emerging technologies complicate this further: proliferating AI agents require identity systems that can authenticate and authorize	的・軍事的な対応を迅速かつ重複なく行えることが強調されている。 3．同盟国間でサイバー攻撃やデジタル・スパイ行為に関するインシデント情報やパターンを共有することで、共通の脆弱性を特定し、自国および同盟国の重要インフラや人員を守ることができるとしている。 4．ファイブアイズやウクライナ支援の事例を挙げ、衛星通信・傍受システム・巨大データベース（電話・FAX・インターネットトラフィック等）を用いた、きわめて高度に統合された情報共有・分析の仕組みがすでに運用されていると説明している。 5．国家レベルだけでなく、電力・輸送・装備など民間セクターが担う重要インフラとの情報共有が不可欠であり、サプライチェーン混乱や経済的損失を防ぐうえでも公民連携が重要であると述べている。 6．民間衛星企業や OSINT、スタートアップなどがリアルタイムの戦場インテリジェンスを提供するなど、「民間発のインテリジェンス産業」が急成長しており、国家安全保障に組み込まれつつある点を指摘している。 7．情報共有を拡大するうえでの課題として、システムやデータの相互運用性、アクセス制御やプラットフォームセキュリティ、リアルタイム相関分析の難しさに加え、個人情報保護や憲法上の制約、機密指定（classification）との整合など、技術・法制度・プライバシーの三重のハードルがあると整理している。 8．サイバー分野では、継続的な本人確認やクレデンシャル管理を含むアイデンティティ・マネジメント、ゼロトラスト型のセキュリティ・アーキテクチャが「デジタル・ブラックホール」を防ぐ基盤として重要であると強調している。 9．日本の安全保障体制については、インド太平洋地域での役割、予算増、重要インフラ向け早期警戒システムの整備、経済安全保障関連プロジェクトや新法制の整備などにより、徐々に戦略的な枠組みが整いつつあると評価している。 10．ただし米英などと比べると、依然として日本の取り組みは十分とは言えない面もあり、今後のパネルディスカッションでは「国家間の情報共有」「官民連携」「国際連携」をどう強化していくかを議論したいと締めくくっている。

humans, machines, and AI agents (with anti-phishing and continuous validation), while quantum computing demands rapid deployment of post-quantum cryptography, QKD, and eventually quantum-enabled analysis within intelligence platforms. 9. Akaishi argues for a sophisticated, credible digital platform (e.g., robust ID systems like US PIV and secure cloud environments) to support secure, automated, high-speed information sharing across domestic and foreign partners, including the private sector. 10. Japan aims to become an Indo-Pacific hub for threat analysis and cyber resilience, and is rapidly overhauling its security framework—new NSS/defense strategies (including counter-strike capability), major defense budget increases, the Economic Security Promotion Act, relaxed defense-export rules, new laws for protecting critical economic security information and enhancing cyber response, and discussion of a National Intelligence Bureau—yet still lags the US/UK in digital platforms and must catch up to support advanced intelligence sharing.	

2.9 D2-P3 Panel

Theme: Information Sharing (PIV), Public Private Partnership, Intelligence Moderator: Koichi Akaishi Panelists: - Masanori Nishi (Former Deputy Minister, Minister of Defense, Japan) - Bruce Walker (Former Assistant Secretary, U.S. Department of Energy) - Junichi Nishiyama (Senior Research Fellow, Institute for Future Engineering (IFENG)) - Barbara Grewe (CEO, Glenwood Global Risk Management LLC, USA) - Kenzaburo Tamaru (Principal Solution Architect, Digital Agency, Japan)	テーマ：情報共有(PIV)、官民連携、インテリジェンス モデレーター：赤石 浩一 パネリスト： - 西 正典（元防衛事務次官） - ブルース・ウォーカー（元米国エネルギ省次官補） - 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） - 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） - 田丸 健三郎（プリンシパル ソリューション アーキテクト, デジタル庁）
1. The panel defines sovereign/national cloud as infrastructure and data located under a nation's jurisdiction, operated under its laws and (ideally) by its own nationals, and extends this	1. パネル冒頭で、参加者（防衛省出身、西山氏、グレン社 CEO、マイクロソフト、エネルギー省など）が紹介され、テーマは「インテリジェンスと情報共有・ID・セキュリティ・クリアランス・官民連携」であると整理された。

to “knowledge sovereignty” – the ability to build, operate, and secure that cloud without relying on foreign expertise. 2. Japan’s ISMAP is explained as a FedRAMP-inspired evaluation scheme but not equivalent: it focuses mainly on confidentiality, relies on external audits, does not require data centers to be in Japan, and therefore does not in itself guarantee true data or cloud sovereignty. 3. Japan’s current “government cloud” mainly uses foreign hyperscalers (AWS, Azure, etc.) plus one domestic provider (Sakura), but there is still no clear sovereign-cloud model; data location and jurisdictional issues remain open policy questions. 4. From the U.S. side, panelists stress that all sensitive data must be encrypted in transit and at rest, and that real sovereignty requires deep control over underlying systems—otherwise confidentiality, integrity, and availability cannot be guaranteed, especially in a crisis (e.g., cables cut, contested region). 5. Several speakers criticize over-centralized hyperscalers: sharing the same physical silicon and hypervisors creates systemic risk (“one zero-day away” from massive compromise), and large regional outages (e.g., “US-East sneezes, everyone catches a cold”) show the fragility of highly centralized architectures. 6. Harry highlights that high-quality, human-generated Japanese data is increasingly valuable for AI because English/Spanish/Chinese corpora are already heavily “tainted” by AI-generated content; he also warns that buyers must dig into technical details (how resources are shared, how isolation works, where and how recovery is done) rather than trust cloud marketing. 7. From an investor’s perspective, the Japanese cloud market is large, growing, and offers stable, recurring cash flow with very low churn, but building competitive domestic sovereign cloud is capital-intensive and must face hyperscalers that are “100x bigger”; targeted subsidies, pilots in high-sensitivity sectors	2．マイクロソフト側から、政府・重要インフラ向けのプラットフォーム構築と ID 管理の役割が説明され、アイデンティティは「データの生成・編集・流通を追跡し、誰が何をしたかを特定するための中核的コントロールポイント」であり、現代のゼロトラスト／近代的セキュリティフレームワークの中心に位置づくとされた。 3．ID 管理を軸に、各アクセスポイントでの多要素認証・条件付きアクセス・特権 ID 管理などによって未承認アクセスとインサイダー脅威を抑止し、災害時も含めた政府オペレーションの継続性と「アイデンティティ主権」を確保することの重要性が示された。 4．西山氏からは、米連邦政府の PIV を例に、マイナンバーカードや企業 ID との違い、発行対象・用途・セキュリティレベルの差異が紹介され、PIV は強固な ID 基盤とセキュリティコントロールが揃って初めて意味を持つものであり、日本で導入するなら制度・システム双方の整備が必要と指摘された。 5．バーバラ氏（元米側）のパートでは、9.11 委員会報告に基づき、「情報共有の失敗」により約 3000 人が死亡したという教訓が強調され、①自分の仕事範囲だと思っていない、②組織所有物意識、③組織間の敵対関係、④相手への不信、という 4 つの要因が情報共有を阻害していたと分析された。 6．そのうえで、信頼に基づく文化変革を前提に、①セキュリティ・クリアランスの制度、②身元確認と認証（ID）の厳格化、③交通信号のような情報共有プロトコル、④ソース・メソッドを隠した形での共有（インジケータだけ共有）、などによって「共有を原則とするインテリジェンス文化」への転換が必要だと述べられた。 7．米エネルギー省の事例として、電力・ガス事業者との双方向情報共有プログラム（官民パートナーシップ）が紹介され、政府が直接事業者ネットワークデータを扱えなかった課題を、国立研究所経由の分析・助言スキームとインセンティブ付与で解決し、現在では電力事業者の約 75%が参加する強固な枠組みになっていると説明された。 8．西氏（元自衛隊関係）からは、古代から現代までの「情報の扱い」の歴史と、日本の戦前の情報運用失敗、サイバー空間における「主権」概念の未整備、軍事と行政の違いがあいまいな日本の制度など、構造的・歴史的な課題が示され、サイバー時代の国家機能とマンデートを再定義すべきだという問題提起がなされた。 9．セキュリティ・クリアランスについては、日本では「国民全員のプライバシー問題」と誤解されがちだが、本来は運転免許と同様に「特定の役割に就きたい人が自ら選んで受けるもの」であり、その理解不足が議論を難しくしていると指摘された。ま

(defense, health, critical science), and a long-term view are recommended. 8. On national infrastructure and policy, Harry urges designing from the attacker's easiest path (e.g., physical sea-cable layout, PKI and certificate trust), and insists that core digital trust foundations (crypto, identity, PKI) must remain under national control to support genuine zero trust and robust CIA (confidentiality, integrity, availability). 9. The role of government is seen as decisive: without a strong, prescriptive, FedRAMP-like program backed by real funding and mandated use, industry will not transform; such a program can end "loose" compliance, force concrete outcomes, and over time lift the entire security posture of clouds used by government and critical infrastructure. 10. Asked for concrete 12-month steps, panelists propose: create a FedRAMP-aligned national authorization framework; launch funded pilots; expand and strengthen ISMAP and government cloud; invest in domestic data centers and talent; assert sovereignty over identity and crypto trust services; and use these levers to gradually shift high-sensitivity workloads toward secure, Japan-based cloud while preserving interoperability with allies.	た、ID 制度と合わせて、法制度だけでなくリテラシー・教育・マインドセットの変革が重要であるとされた。 10. 最後の質疑では、日米間でセンシティブなエネルギー分野データを共有する可能性や、日本のセキュリティ・クリアランス制度と米国の国家安全保障ベースの制度とのギャップが議論され、「まずは異常検知など限定的な目的での共同分析から始め、信頼と共通土台を積み上げるべき」「システム・制度・文化の三位一体で変革しなければならない」という点で大枠の方向性が共有されて締めくくられた。

2.10 D2-S7 Speech

Tim Perry (Head of Consulting, BAE Systems Digital Intelligence)	ティム・ペリー（BAE システムズ、デジタルインテリジェンス、サイバー・プログラム・リード）
1. The speaker, from BAE Systems Digital Intelligence, works with governments worldwide on national cyber programmes and focuses here on the challenges of intelligence for active cyber defence (ACD). 2. Japan's ACD strategy relies on public–private partnership, automated monitoring, and intelligence-driven operations; all require intelligence that is timely, accurate, and accessible—not hoarded inside government. 3. Using the classic intelligence cycle (plan → collect → process → analyse → disseminate), he	1. 韓国政府のタッシャルサイバープログラムに関与した経験から、世界各国の事例を踏まえつつ、ディープサイバーディフェンスとインテリジェンスの必要性・課題・ソリューションについて説明している。 2. サイバーセキュリティ強化には、官民パートナーシップ、自動化された監視システム、インテリジェンスプログラム、サイバーオペレーションとデータ活用が不可欠であり、これらを継続的に改善することで防御力を少しずつ高めていくべきだとしている。 3. 有効なサイバー防衛には、「タイムリーかつ正確なインテリジェンスへのアクセス」と、それを政府が組織として浸透させ、実際のアクション（レジリエンス向上、脅威の直接対処、攻撃の中断、再発防止のための教育、人・プロセス・技術の能

stresses the need for clear aims, defined information requirements, collection methods, roles, authorities, and information pathways across the whole cycle. 4. Collection must draw on many heterogeneous data sources: incident response reports, enterprise and sector SOCs, commercial threat intelligence and datasets, protected DNS, suspicious-email reporting, and security-agency intelligence, each with different formats and taxonomies. 5. These data sources enrich each other but create storage and complexity challenges; large datasets are costly and hard to analyse, so governments must find an optimal cost–benefit balance while using AI to assist (not replace) skilled human analysts. 6. He outlines a multi-layer national monitoring landscape: local enterprise SOCs, advanced SOCs for high-value national-security entities, sectoral SOCs for critical sectors, and—at the top—a national network cyber centre that monitors telecom networks to give broad, actor-focused situational awareness. 7. A generic ACD operating model should integrate diverse data streams (DNS, SOC feeds, commercial intel, national monitoring) into a central data-integration platform, feeding APIs for operators and analysts so all relevant information is available in one place. 8. Dissemination requires clear release procedures that account for the sensitivity and risk of each dataset, enable trend analysis (not just incident chasing), and ensure sharing of intelligence across government, private sector, and the public at “internet speed and scale.” 9. Because such integrated systems hold extremely sensitive information, they must be secured as a single, strongly protected platform with common processes and clearances (including for selected industry partners), while still allowing rapid, large-scale sharing when needed. 10. His proposed solutions include: a single	力向上）に結びつけることが重要だと述べている。 4．インテリジェンス活動は「プランニング → 収集 → 分析 → インテリジェンス化 → フィードバック」のサイクルで回すモデルであり、目的の明確化（何のために何を知りたいか）と、それに基づくデータ収集・分析が核心であると説明している。 5．収集段階では、サイバースペース上の多様なデータソース（インシデントレスポンスレポート、コマーシャル脅威インテリジェンス、自動監視システム、商用・公的データセット、政府・当局・他国からの情報など）を組み合わせる必要があり、単一ソース依存では不十分だと指摘している。 6．大規模データセットは、保管場所・コスト・分析の難しさといった課題があるため、どこに集約し誰が管理するかを設計しつつ、「最適なボリューム」「精度の確保」「それを扱うスキルと手間」のバランスを取る必要があると述べている。 7．中央集約型の分析・配信モデルを提示し、API 連携などでシステムとデータをつなぎ、アナリストが一元的にデータを扱えるようにすることで、脅威インテリジェンスをオペレーション側（SOC 等）に迅速に反映させるべきだとしている。 8．インテリジェンスの伝達・公開にあたっては、「誰に・どのレベルまで出すか」というリリース手順を明確にし、センシティブ情報を適切に扱いつつ、タイムリーに広く共有できるプロセスを整えることが重要だと強調している。 9．経済・インフラの大半を担うのは民間であるため、官だけでなく民間にも情報が届き、官民の間でトレンドやインシデントを共有できる仕組みが不可欠であり、その前提として巨大で高機微なデータを守る強固でシンプルなセキュリティレイヤーと、インターネットのスピードに追いつく運用が必要だと述べている。 10．提言として、①既存のエンタープライズソリューションを単純にスケールさせるのではなく慎重に設計すること、②既にある多様なデータを「一つの場所」に集約して分析できるようにすること、③可能な限り自動化を進め、スケールとスピードの両方を実現すること、を挙げてスピーチを締めくくっている。

cross-government ACD intelligence plan; deploying purpose-built national network monitoring solutions rather than stretching enterprise tools; consolidating existing public–private data into one enriched environment; and maximising automation to achieve the speed and scale required to get ahead of adversaries.	

2.11 D2-P4 Panel

Theme: Active Cyber Defence (Intelligence) Moderator: Tim Perry Panelists: - Hideaki Watanabe (Chairman, Defense Technology Foundation) - Atsushi Ando (Director-General, National Cybersecurity Office) - Greg Rattray (Next Peak) - Gloria Glaubman - Chris Capper	テーマ：能動的サイバー防御 モデレーター：ティム・ペリー 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） - 安藤 敦史（国家サイバー統括室 統括官） - グレッグ・ラットレイ（Next Peak） - グローリア・グローブマン - クリス・キャッパー
1. This panel, involving participants from the Ministry of Defense, the National Cyber Agency, and U.S. and UK entities in Japan, discussed strengthening Japan's cybersecurity. The discussion centered on four pillars: “Intelligence,” “Active Cyber Defense,” “Public-Private Partnerships,” and “Human Resources and Resilience.” 2. The Japanese side (Ministry of Defense, etc.) stated that strengthening intelligence collection and analysis is an urgent priority to achieve active cyber defense. This involves establishing an organized cyber defense framework and consolidating information from telecommunications providers and critical infrastructure operators. 3. From the perspective of the National Cyber Program, the value and dependency on “essential/critical services” such as digital services, public health, finance, and communications are rapidly increasing. It was pointed out that within limited national budgets, priority investment should be made in these areas while maximizing the leverage of private sector capabilities.	1. 日本のサイバーセキュリティ強化に向けて、防衛省・国家サイバー機関・在日米英関係者などが参加し、「インテリジェンス」「能動的サイバー防御」「官民連携」「人材・レジリエンス」を軸に議論したパネルである。 2. 日本側（防衛省等）は、組織的なサイバー防御体制の整備や、通信事業者・重要インフラ事業者からの情報集約を通じて、能動的サイバー防御を実現するためのインテリジェンス収集・分析強化が急務であると述べている。 3. 国家サイバープログラムの観点からは、デジタルサービス・公衆衛生・金融・通信など「エッセンシャル／クリティカルなサービス」の価値と依存度が急上昇しており、限られた国家予算の中でこれらに優先的に投資しつつ、民間セクターの能力を最大限レバレッジすべきだと指摘している。 4. コスト負担については、「グローバルテクノロジープラットフォーム企業や大手エンタープライズは、これまでデジタル経済の恩恵を大きく受けてきた以上、セキュリティ面でも主体的な責任とコストを負うべきだ」という意見が示されている。 5. インテリジェンス共有の課題として、まず政府内（各省庁間）の情報共有と優先順位づけを確立すること、その上で官民連携に広げること、NIST SP 800-150 のような標準を参考に「何を・どの経路で・どのレベルまで共有するか」を明確化し、民間に対しては「アクショナブルなインテリジェンス」に絞って提供すべきだと議論されている。 6. 共有されるデータについては、アクセス制御が効いた安全な環境で扱うこと、分類・タグ付け・クリアランスレベルを一貫し

4. Regarding cost burden, the report presents the view that “global technology platform companies and large enterprises, having greatly benefited from the digital economy, should bear proactive responsibility and costs for security.” 5. Regarding intelligence sharing challenges, discussions emphasize establishing information sharing and prioritization within government (between ministries), then expanding to public-private partnerships. Standards like NIST SP 800-150 should be referenced to clarify “what, through which channels, and to what level” information is shared. Private sector entities should be provided only with “actionable intelligence.” 6. It is emphasized that for shared data, handling must occur in secure environments with effective access controls, consistent application of classification, tagging, and clearance levels, and ensuring data integrity and auditability are essential. 7. The UK's experience is introduced, including how past failures led to an emphasis on investing in national-level cyber resilience, how state-sponsored cyber attacks came to be treated as “management issues and board-level risks,” and how the NCSC, together with mechanisms such as Industry100 and Cyber League, is working to incorporate private sector personnel with security clearance into national cyber efforts. 8. Regarding security clearance, it was explained that “similar to a driver's license, only those who need it choose to undergo screening, and it is a separate issue from the invasion of privacy of all citizens.” It was pointed out that it is necessary to alleviate misunderstandings and resistance to the establishment of such a system in Japan. 9. Regarding active cyber defense and hackback, strong concerns were expressed that, given the high risk of escalation and mutual attacks, and considering the vulnerability of Japan's infrastructure, “hackback-type active defense” should not be adopted lightly. It was	て運用すること、そしてデータの完全性・監査性を確保することが不可欠だと強調されている。 7. 英国の経験として、過去の失敗から国家レベルのサイバーレジリエンスへの投資を重視するようになったこと、国家主体のサイバー攻撃を「経営課題・ボードレベルのリスク」として扱うようになったこと、そして NCSC を中心に Industry100 やサイバーリーグといった仕組みで、セキュリティ・クリアランスを付与した民間人材を国家サイバーに組み込む取り組みが紹介されている。 8. セキュリティ・クリアランスについては、「運転免許と同様に、必要な人だけが自ら選択して審査を受けるものであり、国民全員のプライバシー侵害とは別問題である」との説明がなされ、日本での制度整備に対する誤解や拒否反応を和らげる必要があるという指摘があった。 9. 能動的サイバー防御とハックバックを巡っては、エスカレーションや相互攻撃リスクが高く、日本の脆弱なインフラ状況を考えると「ハックバック型のアクティブ防御」を安易に採用すべきではないという強い懸念が示され、制裁・外交・抑止など他の手段と組み合わせた慎重なポリシー設計が必要だと議論されている。 10. 全体として、標準化されたデータ分類・クリアランス制度、人材育成と AI・自動化によるエンパワーメント、民間能力の組み込み、そしてアカデミアを含むエコシステム全体での研究・イノベーションが、日本のナショナルサイバー戦略とレジリエンス構築の鍵である、という共通認識でセッションが締めくくられている。

discussed that careful policy design is necessary, combining it with other means such as sanctions, diplomacy, and deterrence. 10. Overall, the session concluded with a shared understanding that standardized data classification and clearance systems, personnel development and empowerment through AI and automation, integration of private sector capabilities, and research and innovation across the entire ecosystem—including academia—are key to Japan's National Cyber Strategy and resilience building.	

2.12 D2-S8 Speech

Giacomo Paoli (Head, Security and Technology Programme, UNIDIR)	ジャコモ・パオリ（国連軍縮研究所（UNIDIR）セキュリティ・テクノロジープログラム責任者）
1. The speaker frames cyber, AI, and quantum not as separate domains but as a rapidly converging “triangular” ecosystem in which each technology amplifies the capabilities and risks of the others. 2. AI is a force multiplier in cyber offense—automating reconnaissance, identifying misconfigurations, generating exploits, and enabling scalable, hyper-realistic social engineering through synthetic text, voice, and video. 3. On defense, AI enhances detection and prediction by correlating weak network signals at scale and enabling adaptive, continuously learning protection—but attackers need to succeed only once, while defenders must succeed always. 4. AI itself becomes a new attack surface: data poisoning, model inversion, extraction, and adversarial perturbations can corrupt training sets, leak sensitive information, or mislead model outputs; reliance on open-source components introduces supply-chain risks. 5. Quantum computing threatens classical cryptography by potentially breaking widely used public-key schemes, accelerating the urgency of post-quantum cryptography; at the same time, quantum communication offers new	1. サイバー・AI・量子は別々の技術ではなく「ネクサス（結節点）」を形成しており、大きなチャンスと同時に新たな脆弱性を生み出していると位置づけている。 2. AI はコード生成・脆弱性探索・ソーシャルエンジニアリング・自律エージェントなどを通じて攻撃側の能力を強化する一方、検知・分析・防御信号の抽出など防御側の高度化にも利用される二面性を持つと説明している。 3. 特に「自律性」と「継続的な自己改善」という AI の特性が、制御不能な振る舞いや想定外の攻撃パターンを生み出し得る点を、今後のリスクとして強調している。 4. データについては、サプライチェーンを含む多様な経路で集約されることにより、新しい静的・動的な脆弱性が生まれており、データの集中・連携の進展がリスク構造を変えていると指摘している。 5. 量子計算については、強力な量子コンピュータが既存の暗号を破る可能性があり、政府も耐量子計算機暗号などを模索し始めているものの、依然として不確実性と不安が大きいと述べている。 6. 量子実験の「再現性」と「完全性」が確立されれば、信頼できる量子システムとして産業に組み込まれ、AI モデルの強化や高度な最適化など、デジタルセキュリティにもポジティブな応用が可能だと展望を示している。 7. 技術レベルだけでなく、ルールや制度設計といったガバナンスの層での対応が不可欠であり、サイバー空間における新しい脆弱性を政策面・制度面からどう抑え込むかが今後の大きな課題であると述べている。 8. AI・量子・サイバーに関わるリスクと機会に対処するには、政府だけでは不十分であり、官・民・学の協調とイノベーショ

resilience through quantum-secure networks. 6. The three domains form a mutually reinforcing ecosystem: • AI accelerates innovation in cyber operations and quantum research, • Cyber infrastructure underpins both AI and quantum experiments, • Quantum will eventually transform AI computation and also reshape cybersecurity through quantum attacks. 7. Convergence amplifies both capability and vulnerability: weaknesses in one domain can cascade into others, heightening systemic risk across the digital ecosystem. 8. Policy must shift from siloed approaches to integrated governance—AI governance, cybersecurity strategy, and quantum roadmaps must be developed together, not in parallel isolation. 9. Governments and researchers should adopt anticipatory methods (foresight, scenario planning, red-teaming) to understand second-order effects of technological convergence before they emerge. 10. No actor can secure this landscape alone: the speaker calls for deep multi-stakeholder collaboration across government, industry, and academia to ensure that innovation strengthens rather than destabilizes the interconnected cyber-AI-quantum ecosystem.	ン・エコシステムの構築が不可欠であると強調している。 9. 今後 10 年以内にデジタルセキュリティの風景は大きく変化すると見ており、日本は技術的な議論にとどまらず、地政学的・経済的な観点も踏まえて能動的に行動する必要があると訴えている。 10. 本プログラムのような場を通じて、単に変化に「反応」するだけでなく、AI・量子・サイバーのネクサスにどう主体的に関与し、行動していくかを日本として考えるべきだと締めくくっている。

2.13 D2-P5 Panel

Theme: Cyber AI, Quantum, NEXUS Moderator: Tom Kono (Fellow, UNIDIR) Panelists: - Michael Karimian (Director, Digital Diplomacy, Microsoft) - Alexi Drew (Technology Policy Adviser, ICRC) - Matt Mickelson (Senior Principal, MITRE) - Yasmin Afina (Researcher, Security and Technology Programme, UNIDIR) - Kazuo Noguchi (Senior Researcher, Keio University) - Giacomo Paoli	テーマ：国際間における先端技術の Norm(政策論) ～AI・量子(コンピュータ・暗号)～ モデレーター：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) - アレクシ・ドリュー (赤十字国際委員会技術政策アドバイザー) - マット・ミケルソン (MITRE 上級主席官) - 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)

	- 野口 和男（慶應義塾大学上席所員） - ジャコモ・パオリ
1. The moderator and Noguchi situate the panel within the 15th International Cyber Security Symposium, emphasizing that cyber, AI, and quantum are rapidly converging and that Japan and the UN have only recently begun to recognize AI/quantum as emerging security threats. 2. Noguchi highlights the “harvest now, decrypt later” risk, the merging of PQC, QKD, drones/sensors, and other quantum-security applications, and warns that preparing cyber/AI/quantum security takes years even though technological change is happening in just a few years. 3. The moderator explains recent UN activity: 2025 as the UN International Year of Quantum Science and Technology, UN processes (OEWG, UNIDIR, innovation dialogues) examining how quantum, AI, and cyber affect global and national security, including military uses and geopolitical impacts. 4. Giacomo Paoli stresses that cyber, AI, and quantum are usually governed in silos but in reality form an interconnected system; national strategies for cybersecurity, AI, and quantum must be designed together, with special urgency around quantum rather than assuming “quantum is always 10 years away.” 5. Paoli argues that states need national quantum strategies—not necessarily to build their own quantum computers, but to understand implications, risks, and dependencies across the cyber–AI–quantum nexus before disruptive capabilities arrive. 6. Noguchi, answering on national security impacts, underlines that AI and quantum will accelerate speed, intelligence, and sophistication of threats; PQC and AI-based security models can mitigate some risks, but new vulnerabilities and systemic risks (e.g., critical infrastructure, energy) must be identified and prioritized. 7. Michael Ford (MITRE) explains post-quantum	1. パネル全体のテーマは「サイバー・AI・量子のネクサス」であり、これらを別々の技術ではなく、国際安全保障・国家戦略・社会に影響する一体の論点として捉えるべきだという問題意識が共有されている。 2. 各国ではすでに量子技術や AI を含む国家戦略が策定されつつあり、量子コンピュータの実用化が「あと 10 年」先の抽象論ではなく、今からリスクと機会を前提にした政策設計・安全保障戦略を準備すべき段階に来ていると指摘されている。 3. 国連・UNIDIR の側からは、量子技術の国際年（2025 年）や、情報通信技術(ICT)の軍縮・安全保障への影響を扱うプロセス（OEWG など）を紹介しつつ、新興技術のリスクと国際安全保障を結びつける研究・対話が進んでいることが説明された。 4. UNIDIR は、各国政府・科学者・市民社会が参加するマルチステークホルダーの場を通じて、量子技術や AI が軍縮・平和・安全保障に与える影響を分析し、規範・ルールづくりの土台となる知見を提供する役割を担っていると説明された。 5. 産業界の立場からは、「今暗号化されたデータを保存しておき、将来の量子コンピュータで解読する（store now, decrypt later）」という脅威が強調され、データの“寿命”に応じて耐量子計算機暗号への移行を優先順位づけする必要があるとされた。 6. 耐量子計算機暗号アルゴリズム自体はすでに標準化が進んでおり、ハイパースケーラーやベンダが実装を始めているが、レガシー暗号の置き換え、プロトコル実装スキルの不足、機器更新サイクルとの調整など、移行の実務・人材面の課題が大きいと述べられた。 7. マイターらが主導する「耐量子計算機暗号連合」（PQC 連合）のような国際的な産官学連携の枠組みを通じて、標準の具体実装、ツールやワークブックの提供、各組織のロードマップ策定支援などを行い、移行を加速させようとしていることが紹介された。 8. 国際赤十字（ICRC）の立場からは、AI・量子・サイバーは人道活動にとって大きなリスクと同時にツールにもなり得るが、国際人道法(IHL)の基本原則（中立性・独立性・人道性）は変わらず有効であり、新技術を使う場合もそれらを損なわないガバナンスが不可欠だと強調された。 9. 特に、生体情報・医療データ・紛争地の被保護者データなど、長期間守られるべき人道データが量子計算により将来破られるリスクがあり、耐量子計算機暗号を人道分野に適用

cryptography: PQC algorithms already standardized (e.g., by NIST) can be deployed now; given long data lifetimes, organizations must begin migration from classical crypto to PQC, using industry coalitions (MITRE + hyperscalers and vendors) to accelerate standards and implementation. 8. Michael K. from Microsoft describes industry's view: the threat landscape is driven by large-scale cybercrime and increasingly sophisticated nation-state activity; AI simultaneously turbocharges attackers (automation, better phishing) and defenders (faster triage, gap-closing), so industry must both "raise the floor" on everyday security and secure AI systems themselves. 9. Alexei from the ICRC brings a humanitarian lens: IHL remains applicable and essential, but AI/cyber/quantum convergence magnifies risks for civilians; humanitarian organizations face "harvest now, decrypt later" threats to sensitive data, dependence on powerful state/corporate tech, and a capacity gap that could compromise neutrality, independence, and protection of vulnerable populations. 10. Yasemin (UNIDIR) outlines the UN's governance role: acting as a neutral convener (formal forums, informal consultations, expert roundtables), promoting cross-sector learning, coordinating between cyber/AI/quantum discussions, supporting capacity building (especially for the Global South), and ensuring that the cyber–AI–quantum nexus is treated as a practical work agenda for shared security rather than a mere slogan; an audience question on financial-sector risk leads Noguchi to reaffirm that quantum timelines (e.g., NSA/North America "Y2Q" dates) make PQC adoption urgent.	する際の倫理・実務・独立性確保が新たな課題として提示された。 10. 討議全体として、サイバー・AI・量子をめぐるリスクは一国・一組織では対応できず、国家間協力、産官学連携、人道組織も含めた多層のガバナンスと教育・評価手法の整備が不可欠であること、そして日本もこのネクサスに主体的に関与し準備を急ぐべきだ、という方向性が共有された。

2.14 D2-S9 Day #2 PM Closing

Craig Wiener	クレイグ・ウィーナー
1. Craig Wiener provided a comprehensive recap of the day's key messages, highlighting insider-	1. クレイグ・ウィーナーは当日の主要メッセージを包括的に総括し、スノーデン事件から得られた内部脅威の教訓と、サイバ

threat lessons from the Snowden era and the enduring importance of the human factor in cybersecurity. 2. Minister Kanahana emphasized Japan's need for stronger political will, a public-private cyber-defense ecosystem, diversified suppliers, and solutions for organizing government hackers. 3. Speakers from the U.K. stressed active threat hunting, AI-enabled adversary capabilities from China, resilience planning including pen-and-paper backups, and potential thematic cyber-sanctions. 4. U.S. perspectives underscored continuous monitoring, risks of interconnected cloud systems, interoperability requirements, and sovereignty considerations. 5. Concerns were raised about Japan's ability to operate during a Taiwan contingency, with warnings of immediate critical-infrastructure paralysis. 6. Maria Roat highlighted lessons from building FedRAMP: change management, prescriptive controls, independent assessments, and overcoming cultural resistance. 7. Intelligence-sharing panels stressed early warning, cross-border coordination, public-private intelligence collaboration, and the anticipated creation of Japan's National Intelligence Bureau. 8. Identity telemetry was presented as a trust anchor, with suggestions that PIV-style identity systems could expand to the broader public. 9. Active cyber defense debates continued, covering escalation risks, collection-cycle priorities, AI/ML-enhanced information-sharing programs, and the view that global platform companies bear public responsibility. 10. Quantum-related discussions addressed "store now, decrypt later," the need for PQC transition playbooks, uncertain future impacts of quantum technologies, and post-quantum coalition collaboration led by MITRE.	ーセキュリティにおける人的要因の持続的な重要性を強調した。 2．金原大臣は、日本がより強い政治的意思、官民連携のサイバー防衛体制、サプライヤーの多様化、政府ハッカー組織化の解決策を必要としていると強調した。 3．英国の登壇者は、積極的な脅威ハンティング、中国による AI 活用の敵対能力、紙とペンによるバックアップを含むレジリエンス計画、テーマ別サイバー制裁の可能性を強調した。 4．米国の視点では、継続的監視、相互接続されたクラウドシステムのリスク、相互運用性の要件、主権に関する考慮事項が強調された。 5．台湾有事における日本の運用能力への懸念が示され、重要インフラの即時麻痺が警告された。 6．マリア・ロートは FedRAMP 構築の教訓として、変更管理、規範的統制、独立評価、文化的抵抗の克服を挙げた。 7．情報共有パネルでは早期警戒、越境調整、官民情報連携、日本の国家情報局創設が強調された。 8．アイデンティティテレメトリーは信頼基盤として提示され、PIV 型認証システムの一般市民への拡大が提案された。 9．能動的サイバー防御に関する議論は継続し、エスカレーションリスク、収集サイクルの優先順位、AI/ML 強化型情報共有プログラム、グローバルプラットフォーム企業の公共的責任負担の必要性などが論じられた。 10．量子関連議論では「即時保存・後解読」手法、PQC 移行プレイブックの必要性、量子技術の将来影響の不確実性、MITRE 主導のポスト量子連合協力が取り上げられた。

3 DAY 3: October 30 | West School Building 1F West Hall

3.1 D3-S1 Day #3 AM Opening

Anupam Joshi	アヌパム・ジョシ
1. The emcee welcomed participants to day three and outlined the four-day structure of the symposium jointly hosted by Keio University's Cybersecurity Research Center and MITRE. 2. The symposium focuses on new developments in cybersecurity across national, economic, and societal security with an emphasis on global multilateral public-private partnerships. 3. The main hall hosts keynotes, presentations, and panels for all four days, while parallel sessions take place in other campus buildings on days two and three. 4. Participants were reminded to refer to the program booklet for detailed session information, and that the day's program concludes at 5:30 PM. 5. Anupam Joshi, Vice Provost and Chief AI Officer at UMBC, was invited to open the morning session. 6. Joshi introduced himself as a faculty member in computer science and electrical engineering and director of UMBC's Cybersecurity Institute. 7. The theme of day three is economic security, featuring a keynote by Barbara followed by two panels. 8. The first panel focuses on critical infrastructure security—especially energy systems—while the second covers active cyber defense and the security-clearance process. 9. Joshi emphasized that economic security requires strong collaboration among academia, government, and industry, which is reflected in the symposium's diverse attendees. 10. He highlighted UMBC's partnerships with NSA, DoD, and major industry players, as well as its CAE-R and CAE-CD certifications, before concluding the opening remarks.	1. 司会者は 3 日目の参加者を迎え、慶應義塾大学サイバーセキュリティ研究センターと MITRE が共同開催するシンポジウムの 4 日間の構成を説明した。 2. シンポジウムは、国家・経済・社会の安全保障におけるサイバーセキュリティの新展開に焦点を当て、特に国際的な官民連携に重点を置く。 3. メインホールでは 4 日間を通じて基調講演、プレゼンテーション、パネルディスカッションが行われる。並行セッションは 2 日目と 3 日目に他のキャンパス施設で実施される。 4. 参加者は詳細なセッション情報をプログラム冊子で確認するよう注意喚起された。当日のプログラムは午後 5 時 30 分に終了する。 5. 午前のセッション開幕には、UMBC 副学長兼最高 AI 責任者であるアヌパム・ジョシが招かれた。 6. ジョシは自身をコンピュータサイエンス・電気工学の教員であり、UMBC サイバーセキュリティ研究所所長であると紹介した。 7. 3 日目のテーマは経済安全保障であり、バーバラによる基調講演に続いて 2 つのパネルディスカッションが行われる。 8. 第 1 パネルは重要インフラ（特にエネルギーシステム）のセキュリティに焦点を当て、第 2 パネルは能動的サイバー防衛とセキュリティ・クリアランス手続きを扱う。 9. ジョシは経済安全保障には学界・政府・産業界の強力な連携が必要だと強調し、その重要性がシンポジウムの多様な参加者構成に反映されていると述べた。 10. 彼は UMBC が NSA、国防総省、主要産業プレイヤーと提携していること、また CAE-R および CAE-CD 認証を取得していることを紹介し、開会の挨拶を締めくくった。

3.2 D3-S2 Keynote Speech

Mike Studeman	マイク・スタデマン
1. The speaker argues that national security and economic security are increasingly interconnected and must be viewed together rather than through separate lenses. 2. Governments must adapt to a new security paradigm that introduces both new opportunities and new challenges, requiring expanded government roles. 3. Physical and economic attacks—whether against civilians, military, or private entities—consistently trigger government responsibility and response. 4. The Land Rover cyberattack of 2025 exemplifies how a single cyber incident can massively disrupt national economic security and supply chains. 5. Cybersecurity failures affecting confidentiality, integrity, or availability of data directly threaten both national and economic security. 6. Major global cyber incidents—WannaCry, NotPetya, SolarWinds, Volt Typhoon, SALT Typhoon—demonstrate that cyberspace is a new battleground with worldwide impact. 7. The convergence of IT and OT systems increases vulnerability, making even physical access controls dependent on cybersecurity. 8. The speaker presents a matrix on government responsibility in cyber risk, emphasizing that threat actors, vulnerabilities, and victim types should all influence government involvement. 9. Passive defense approaches are insufficient; governments must coordinate nationally and with allies to identify, protect, detect, respond, and recover from cyber threats. 10. Significant obstacles remain—lack of imagination, inadequate policies, insufficient capabilities, dispersed management—but governments must nonetheless assume a more proactive and strategic role in cybersecurity. ---	1. 経済安全保障における政府の責任は拡大しており、新たなチャンスと課題に対応するためビジョン改善と積極的な関与が必要である。 2. 物理攻撃・サイバー攻撃に対して政府は主体的に対応し、レジリエンス支援や被害拡大防止を行う役割を担っている。 3. 9.11 や最近の米経済への大規模攻撃など、歴史的事例はいずれも政府レベルの大規模対応を引き起こしており、サプライチェーン全体への影響が大きい。 4. サイバーセキュリティは機密性・完全性・可用性の確保に不可欠であり、国家安全保障と国際安全保障の基盤となる。 5. 重要インフラに対するランサム攻撃、WannaCry、NotPetya、SolarWinds など、サイバー・物理が融合した攻撃が国家にも企業にも甚大な影響を及ぼしている。 6. Volt Typhoon など国家支援型 APT は、重要インフラに潜伏して同時多発的混乱を引き起こす能力を持ち、米政府も「すべてを同時に破壊する脅威」と位置づけている。 7. サイバー攻撃により知財・金銭・社会機能が大量に損失しており、国の脆弱性として深刻化しているため、サイバーは国家経済安全保障の中心課題となった。 8. サイバー脅威は国家、APT、犯罪、テロ、アクティビスト、インサイダーなど多様化し、政府が直接コントロールできない民間領域の脆弱性管理が極めて困難になっている。 9. 重要インフラの 8 割が民間である米国を例に、民間だけでの防御には限界があり、政府が同盟国と協力しつつ識別・保護・検知・対応・復旧を包括的に支援する必要があると強調された。 10. 9.11 後の反省（創造力欠如・情報共有不足・不十分な政策等）を踏まえ、政府は戦略構築、法制度整備、訓練強化、情報共有、透明性の確保を進め、能動的サイバー防御を含む行動を取らなければならないと結論づけられた。

3.3 D3-S3 Speech

Masaki Umejima (Project Professor Keio Global Research Institute (KGRI), Convener of Energy Resource Aggregation Business, the IEC system committee smart energy)	梅嶋 真樹 (慶應義塾大学 グローバルリサーチインスティテュート 特任教授、IEC システム委員会スマートエネルギーコンビナ(ERAB 担当))
1. The speaker introduces a new trend in Japanese critical infrastructure, focusing on energy, and explains his dual role at Keio University (cybersecurity research) and in the IEC, which develops international cybersecurity standards for energy systems. 2. He notes a major shift in the last decade: electricity systems and grids are becoming highly distributed, with many devices (EV chargers, solar generators, air conditioners, heat pumps, etc.) connected and remotely controlled over networks, despite having very limited computing resources. 3. Within IEC's System Committee Smart Energy, a new standardization effort (IEC 63443) is nearing completion, aiming to define rules for the emerging energy market, including security requirements for these distributed systems. 4. The key emerging concept is the energy resource aggregation business (often called ERAB), where many distributed energy resources are aggregated and remotely monitored/controlled by actors such as aggregators, retailers, device makers, and distribution network operators. 5. Three core requirements for this new market are emphasized: * Interoperability (using common communication languages/protocols), * Transparency (clear visibility into who is remotely controlling what), and * Cyber-physical system security. 6. Japan strongly promotes the ECHONET Lite protocol (an IEC standard) as a common application-layer language for devices; the speaker stresses that standardized protocols—not proprietary "secret" ones—are essential for	1. 電力グリッドは過去 10 年で大きく変化し、分散型電源・各種デバイスがインターネット接続を前提に遠隔制御される構造へと進化している。 2. 多くのデバイスは 16 ビット級マイコンなど資源制約が大きい一方で、電力インフラの重要部分を構成しており、脆弱性管理が重要である。 3. IEC や IEA では、新たな市場・ビジネスモデル、アクター役割、セキュリティ要件を含む新しいデータモデルの標準化議論が進行している。 4. 特に IEC 63443 など、スマートエネルギーシステム向け新標準が最終段階にあり、分散型エネルギー資源（DER）を統合する枠組みが検討されている。 5. 分散型エネルギーの運用には「共通言語（相互運用性）」「透明性」「サイバーフィジカルセキュリティ」の 3 要素が必須であるとの指摘があった。 6. 日本の ECHONET は家庭用機器やスマートメーターで広く普及しており、欧米の標準と並んで国際的にも注目されている。 7. 通信プロトコルは独自仕様では安全性を確保できず、標準化されたプロトコルを前提にセキュリティを設計する必要があると強調された。 8. 日本政府は「サイバークリティカルセキュリティフレームワーク（CPSF）」など、エネルギーICT 領域におけるセキュリティガイドライン整備を進めている。 9. セキュリティには技術だけでなく、人間の行動・組織文化が深く関わり、新市場への導入における人材育成・実装能力が極めて重要と述べられた。 10. アジア諸国（マレーシア、インドネシア、タイなど）との協力が進められており、国際連携・情報共有が新しい電力市場の安全性確保に不可欠であるとまとめられた。

both interoperability and security in IoT/energy systems. 7. ECHONET Lite already has deep market penetration in Japan (a large share of new air conditioners, smart meters, and heat pumps use it), but security must also be ensured at IP, transport, and lower network layers. 8. Power meters gain a new role as transparency devices: they have interfaces both to utilities and users and will enable users to measure energy consumption at one-minute intervals, supporting monitoring of remotely controlled loads in homes, offices, and factories from around 2026. 9. To build high trust in ELAB, Japan proposes a "security triangle": * international standards at the top, * national guidelines in the middle, and * academic contributions at the base, along with the CPSF (Cyber-Physical Security Framework), which highlights six elements—organization, people, components, data, procedures, and systems—especially human behavior and procedures. 10. Japan is issuing updated security guidelines for energy resource aggregation (new version released in May) and, through Keio University's CCRC, preparing academic papers and international cooperation with ASEAN countries; harmonization, security-by-design, and information sharing in Asia are presented as crucial for securing the new distributed electricity market.	

3.4 D3-P1 Panel

Theme: Japanese Critical Infrastructure: Energy Moderator: Masaki Umejima Panelists: - Steven Kunsman (Hitachi Energy) - Samuel Chanoski (Technical Relationship and Program Development at Idaho National Laboratory) - Alexander Patton (Amentum) - George Gkoktsis (Fraunhofer SIT)	テーマ：重要インフラ・電力 モデレーター：梅嶋 真樹 パネリスト： - スティーブ・クンズマン（日立エナジー・米国） - サミュエル・チャノスキー（アイダホ国立研究所、関係構築とプログラム開発） - アレクサンダー・パットン（アメンタム） - ジョージ・ゴクティス（フラウンホーファーSIT） - 武田 治（中部電力株式会社 DX 推進部 部長）

- Osamu Takeda (Director, DX Promotion Department, Chubu Electric Power Co., Inc.) - Osamu Nakamura (Project Professor, Keio Global Research Institute)	- 中村 修 (慶應義塾大学グローバルリサーチインスティテュート 特任教授)
1. The panel focused on Japanese critical energy infrastructure, bringing together perspectives from U.S. DOE, European research institutes, global vendors, utilities, and academia to discuss cyber risks to modern power systems. 2. From the U.S. side, Samuel highlighted DOE's CESER initiatives such as Citrix (cyber testing for resilient ICS) and newly defined supply chain cybersecurity principles, emphasizing shared responsibility between vendors and asset owners and the need to understand hardware/firmware/software in depth rather than chasing each new CVE in isolation. 3. Citrix was described as an intensive, months-long decomposition and vulnerability-analysis program that prioritizes widely used devices with high impact; its main value is insight into common components and systemic risk, combined with structured legal frameworks that enable long-term trusted collaboration with vendors and utilities. 4. George presented incident-response lessons from major OT cases (Ukraine grid attacks, Colonial Pipeline, Triton), stressing gaps in asset visibility, legacy insecure protocols, operational continuity constraints, and forensic complexity—plus the importance of EU legal frameworks (NIS2, Cyber Resilience Act, mandatory reporting, national CSIRTs and mobile incident response teams). 5. He argued that regulated exercising and cross-border coordination (EU, Germany, ENISA, etc.) are becoming central, and that Japan has a strategic opportunity to lead OT security in the Asia-Pacific region if it builds comparable response structures, regulations, and practice regimes. 6. Steve (Hitachi Energy) explained how a global vendor operationalizes DOE's supply-chain principles by mapping them to IEC 62443	1. 本パネルは、エネルギー分野の重要インフラに対するサイバーセキュリティをテーマに、官民・研究機関・電力会社など多様な立場から議論したセッションである。 2. 米エネルギー省サイトリックス（CyTRICS）では、ハード・ファームウェア・ソフトウェアの脆弱性を優先度づけして深くテストし、メーカーと連携しながらサプライチェーン全体のリスク低減と情報共有を進めていることが紹介された。 3. サプライチェーン・サイバーセキュリティ原則では、ベンダー側とアセットオーナー側それぞれの責任と行動指針を整理し、良き「エコシステム市民」としての行動を促す枠組みが G7 などでも共有されていると説明された。 4. Fraunhofer SIT からは、ウクライナ電力インフラ攻撃（2015–2016）などの事例を通じ、事前の準備・インシデントレスポンス能力の有無が被害規模を大きく左右すること、EU・ドイツにおける法制度（NIS2 等）、インシデント報告義務、官民協力、演習・標準化（IEC 62443）の重要性が示された。 5. 日立エナジーからは、サプライチェーン原則へのコミットメント、IEC 62443 と ISO 27001 を組み合わせた OT/IT 双方のセキュリティフレームワーク、CyTRICS 参加を通じたソフトウェア部品表（SBOM）管理と脆弱性パッチ適用の高度化など、ベンダーとしての具体的取り組みが報告された。 6. アメントムは、OT インシデントでは IT と OT の専門家が協働しなければ復旧に長期間を要し莫大な損失が出ることを指摘し、実環境に近いサイバー演習環境でのトレーニング・シミュレーションが組織の対応力向上に不可欠であると強調した。 7. 中部電力は、発電・送配電・販売などサプライチェーン全体に異なるセキュリティ要件が存在すること、制御システム（OT）とセキュリティ監視（SOC）を緊密に連携させて、停電原因がサイバーか自然災害かを切り分けつつ運用していること、今後は分散型電源・マイクログリッドのセキュリティ強化も喫緊の課題であると述べた。 8. 中村先生は、日本の送配電分離・再エネ拡大・マイクログリッド・家庭の DER（EV・太陽光など）によりプレイヤーが急増し、単一の大電力会社による境界防御モデルが崩れつつあることを指摘し、ゼロトラストと自律分散協調的なセキュリティ運用へのパラダイムシフトが必要だと主張した。 9. 特に DER を起点とする新たな攻撃面（アグリゲータ乗っ取り、SCADA 経由、ベンダーの管理ポートやファーム更新経

(secure development, product security capabilities, secure system integration and processes) and by participating in Citrix, using findings to improve SBOM accuracy and internal SDLC, and helping build an energy-OT reference architecture (Purdue-inspired) now standardized in ISA WG14. 7. Alex emphasized that OT failures can directly threaten societal continuity and cause massive financial losses in competitive markets like Japan; effective detection and response require tight collaboration between OT engineers and IT security teams, supported by tailored OT cyber-range exercises that build “muscle memory” across mixed teams. 8. Mr. Takeda from Chubu Electric described the utility operator’s view, showing how a diversified group (generation, grid, retail) must secure different environments, integrate cyber and physical response (e.g., switching to manual control during incidents), and address new risks from widespread DER and remote control while maintaining stable supply and grid balance. 9. Professor Nakamura framed future power systems as “many-player, highly distributed” networks (microgrids, home solar, EVs, aggregators), where traditional perimeter security no longer works; he warned of DDoS-like scenarios against massive numbers of small devices and risks via firmware-update paths, arguing that continuous monitoring and secure information-sharing infrastructures are essential. 10. In his wrap-up, Professor Umejima summarized the consensus: testing is vital but cannot cover all components, so security-by-design, categorization, monitoring, information sharing, exercises, and new SOC/zero-trust models are needed; ultimately, small vulnerabilities in many small devices can create large-scale holes in the entire energy system, especially as DER and microgrids proliferate.	路の悪用など）に対し、ガイドライン整備、運用モデル設計、物理量のモニタリングとリアルタイムな情報共有を組み合わせた「サイバーフィジカル監視」が鍵になると整理された。 10．モデレーターによるまとめとして、①テストだけでは全コンポーネントをカバーできないこと、②セキュリティ・バイ・デザイン、計画・訓練・演習の三位一体の取り組み、③マイクログリッド事業者とのゼロトラストな連携、④多くの小さなデバイスの脆弱性を前提とした継続的モニタリングと情報共有が、今後のエネルギーサイバーセキュリティの中核であると結論づけられた。

3.5 D3-S4 Speech

Mayu Arimoto (Partner, Alesia International Law Office)	有本 真由 (アレシア国際法律事務所 弁護士)
1. The session introduced an upcoming panel on security clearance and new active cyber-defense, highlighting its relevance to Japan's current policy environment. 2. The speaker referenced Japan's major legislative pillars for economic and cyber security, including the Economic Security Promotion Act and related measures intended to strengthen supply-chain resilience and information protection. 3. A comparison was made between classifications of "critical economic information" and "special secret information," noting that the former focuses on protecting key industrial sectors and preventing national-level damage. 4. Special secret information (SDS) was described as narrower in scope, limited to highly sensitive intelligence such as defense plans and essential government secrets. 5. The speaker emphasized the importance of aligning Japan's legal frameworks with those of other advanced countries to ensure compatibility in security policy and operational structures. 6. The discussion touched on the need for stronger public-private cooperation, including mechanisms for secure data utilization, infrastructure protection, and coordinated cyber-incident response. 7. The speaker noted that effective cyber-defense requires structured government oversight combined with practical industry measures and continuous education. 8. The importance of robust security-clearance processes was underscored, especially in contexts requiring trusted personnel handling sensitive or mission-critical information. 9. The session emphasized that supply-chain resilience and cybersecurity planning must be integral parts of national strategy, not optional additions. 10. The moderator closed the segment by	1．このパネルは「セキュリティ・クリアランスと新しい能動的サイバー防御」をテーマとし、日本の経済安全保障政策との関係を議論する趣旨である。 2．日本政府は、経済安全保障推進法など複数の重要な法制度を通じて、サイバー攻撃対処や重要インフラ防護、サプライチェーンのレジリエンス確保に取り組んでいると説明された。 3．「重要経済情報」と、より限定された範囲の「特定の安全保障関連情報（S 情報）」のような区分があり、それぞれ保護対象や漏えい時の国家戦略への影響が異なることが指摘された。 4．こうした機微情報の保護や活用を前提に、公的部門と民間部門が通信データや各種情報を共同で利用する枠組みづくりが進められているとの説明があった。 5．経済安全保障の観点からは、特に重要インフラやクリティカルな産業に関する企業・人材に対して、どのようにセキュリティ・クリアランスを付与し、どこまで情報アクセスを認めるかが大きな課題であると示された。 6．サイバー防御、とくに「能動的・アクティブなサイバーディフェンス」を実行するには、機密情報を扱える人材や組織基盤が不可欠であり、その前提としてセキュリティ・クリアランス制度の整備が重要だと強調された。 7．一方で、制度設計だけでなく、運用面での現場とのすり合わせや、民間側が納得して協力できる透明性の高いルールづくりが必要であるとの問題意識も示された。 8．最後に、今回のような高度なサイバー対処・経済安全保障の議論や実務を進めるうえで、「セキュリティ・クリアランスが極めて重要である」という発言で締めくくられている。

positioning the remarks as the introduction to a deeper panel discussion on security clearance and active cyber-defense.	

3.6 D3-P2 Panel

Theme: Security Clearance and New Active Cyber Defense Moderator: Mayu Arimoto Panelists: - Mike Studeman - Barbara Grewe - Nate Snyder (Advisor, JICSS) - James Miller (CEO, Miller Enterprises) - Gloria Glaubman	テーマ：セキュリティ・クリアランス体系と、新しい能動的サイバー防御 モデレーター：有本 真由 パネリスト： - マイク・スタデマン - バーバラ・グルーイ - ネイト・シュナイダー（JICSS アドバイザー） - ジェームス・ミラー（ミラーエンタープライズ 代表取締役社長） - グローリア・グローブマン
1. The panel explored how security clearances, information sharing, and active cyber defense interact, especially comparing long-established U.S./Five Eyes practices with Japan's newer legal and institutional frameworks. 2. Speakers explained that security clearance is meant to vet trust (through investigation and continuous evaluation), but that over time the U.S. system became siloed, inconsistent across agencies, and overly bureaucratic, leading to reforms such as portable clearances and ongoing (not just periodic) review. 3. They stressed that not all sensitive information needs to be formally classified: trade secrets and many "sensitive but unclassified" data still require protection, while truly classified information should be narrowly defined and not used as a way to hide inconvenient facts. 4. Effective threat information sharing was a core theme: intelligence must be converted into usable indicators (e.g., "what ricin looks like," what to look for on a network) rather than kept in a "black hole," and over-classification or slow channels can destroy its operational value. 5. Several panelists argued that most information needed by first responders and private-sector defenders does not require high-level clearance; in fact, broad clearances can	1. 日本ではこの 3 年で、①経済安全保障推進法、②重要経済安全保障情報活用法、③サイバー対処能力強化法（および整備法）の 3 本を柱とする新しい経済安全保障法制が整備され、サプライチェーン強靭化・重要インフラ防護・情報保護・サイバー対処を経済政策手段で支える枠組みが形成されつつあるという説明があった。 2. 経済安全保障推進法は、重要物資の安定供給確保、重要インフラサービスの安定提供、戦略的に重要な技術の研究開発支援、特許の非公開制度などを通じて、経済政策で国家安全保障を支えることを目的としていることが整理された。 3. 重要経済安全保障情報活用法では、「重要経済安全保障情報」という新たな機微情報カテゴリーを導入し、従来の特定秘密とは異なるレベルの機密（重要インフラ・サプライチェーンなどに関する非公開情報）を保護しつつ、利用・共有を可能にするためのセキュリティ・クリアランス付与や身元調査の手続きが定められたと説明された。 4. サイバー対処能力強化法は、日本版「能動的サイバー防御」に関する法律と位置づけられ、官民連携によるインシデント報告義務、同意なき通信データの限定的・条件付き取得とメタデータ解析、さらに重大なサイバー攻撃時の警察・自衛隊による遠隔無力化措置などを通じて、サイバー防御体制を強化する三つの柱からなる新しい仕組みであると紹介された。 5. 米国のセキュリティ・クリアランス制度については、①何を・なぜ守るかを定める「分類ガイド」、②情報にアクセスし得る人へのクリアランス付与、③機密情報を扱う専用システムという「三脚構造」が説明され、従来の「一定年ごとの再調査」から、行動や状況変化を継続監視するリスクベースの継続評価

create additional vulnerabilities by granting unnecessary access. 6. Active cyber defense was defined much more broadly than “offensive cyber”: it includes information sharing, honeypots, sandboxes, deception, sanctions, indictments, and other coordinated government actions, and cannot rely solely on passive monitoring when attacks move at “the speed of light.” 7. Oversight was described as essential but outdated in many U.S. contexts: mechanisms and policymakers often operate with early-2000s thinking, slowing urgent responses; the panel called for modernized, better-educated oversight that safeguards civil liberties without blocking timely defensive action. 8. Trust was framed as fundamentally human and contextual: nationality, government employment, or clearance level do not automatically equal trustworthiness; zero-trust concepts and security culture must assume that people and systems can fail, and design controls accordingly. 9. For Japan, speakers saw both challenges and opportunities: Japan lacks the long Five Eyes history but therefore has a “greenfield” chance to design a more rational, less bureaucratic clearance and information-sharing system that embeds reciprocity, culture change, and cross-sector cooperation from the start. 10. The discussion concluded that Japan’s new active cyber defense law and related frameworks will only succeed if they are implemented with clear purpose (why and what to protect), strong but agile oversight, incentives for two-way information sharing, and a security culture that enables—rather than blocks—joint defense between government and industry.	型へと進化していると述べられた。 6．日本では「なぜ政府が秘密を持つのか」「リモートチェックによるプライバシー侵害への懸念」といった文化的・世論的な葛藤があり、セキュリティ・クリアランス制度の導入にあたっては、分類の根拠や身元調査の必要性を丁寧に説明し、民主的統制・プライバシー保護と両立させることが課題であると指摘された。 7．ファイブアイズ諸国との比較として、同盟国間ではセキュリティ・クリアランス手続きそのものは完全に同一ではないが、相互に「他国のプロセスは信頼できる」と認め合うことで高いレベルの情報共有が実現しており、日本が同様の信頼関係に近づくには、法制度だけでなく長期にわたる関係構築と国内の秘密保全・人材システムの整備が不可欠だと述べられた。 8．「能動的サイバーディフェンス」はハックバックだけを指すのではなく、脅威ハンティング、センサーの高度化、情報共有、脅威インテリジェンス収集、分散型の情報共有ネットワークなど、受け身でない防御行為の広い集合として捉えるべきであり、その定義を明確にしないと誤解や不要なエスカレーションを招くと警鐘が鳴らされた。 9．法律の全面施行まで数年を要する一方で、サイバー脅威は待ってくれないため、日本はこの移行期間中にも、官民・国際パートナーとの双方向の情報共有、ゼロトラスト的な技術・運用、リスクベースのアクセス制御など、実務レベルで進められる施策を先行的に整備すべきだという提言がなされた。 10．全体として、経済・技術・サイバー政策を統合した新しい経済安全保障フレームワークのもとで、日本は国内の省庁間・官民間の信頼と情報共有を強化しつつ、米国や同盟国との協調を深め、透明性ある監視・オーバーサイトと人間中心の「トラスト」概念を組み込んだセキュリティ・クリアランスと能動的サイバー防御のエコシステムを構築していく必要がある、というメッセージで締めくくられた。

3.7 D3-S5 Day #3 PM Opening

Osamu Nakamura	中村 修
1. Prof. Osamu Nakamura opened the afternoon session of the 15th International Cybersecurity	1．中村修教授が第 15 回国際サイバーセキュリティシンポジウムの午後のセッションを開会した。

Symposium. 2. He emphasized that the symposium serves as an important platform for extensive information exchange. 3. He highlighted the diverse participation from government, private sector, and academic communities. 4. He stressed that sharing cybersecurity-related information is crucial for enhancing safety and protecting human life. 5. He expressed gratitude to the attendees for their engagement.	2. 同シンポジウムが広範な情報交換の重要な場となることを強調した。 3. 政府、民間企業、学術界からの多様な参加を指摘した。 4. サイバーセキュリティ関連情報の共有が安全性の向上と人命保護に不可欠だと強調した。 5. 出席者への参加への感謝を表明した。

3.8 D3-S6 Speech

HASHIMOTO Katsukuni (Planning Officer, Cyber Security Division, Commerce and Information Policy Bureau, METI)	橋本 勝国 (経産省 商務情報政策局 サイバーセキュリティ課 企画官)
1. The speaker highlighted recent cyber incidents in Japan and abroad, including attacks by groups linked to China (such as MirrorFace and Volt Typhoon) targeting national security supply chains, critical infrastructure, and major companies. 2. He emphasized that cyber-attack techniques have become more sophisticated, spanning espionage, business disruption, supply-chain compromise, and critical-infrastructure intrusion. 3. Japan enacted new cybersecurity legislation in May 2024, introducing public–private cooperation requirements, mandatory incident reporting, and expanded information-sharing mechanisms between government and infrastructure operators. 4. Under the new law, government agencies may analyze packet header information (not content) to detect signs of cyberattacks and support filtering and neutralizing malicious traffic. 5. Four priority policy pillars were outlined: securing the supply chain, promoting secure-by-design development, strengthening cybersecurity for emerging technologies, and enhancing overall resilience in both public and	1. 近年の国内外のサイバー情勢として、①機微技術・安全保障関連情報の窃取、②事業停止を狙うランサムなどの攻撃、③重要インフラ停止を狙う活動、④サプライチェーンを起点とした攻撃が顕著になっており、国家関与グループから金銭目的犯罪者まで、多様で高度・複雑化した脅威が存在していると説明している。 2. こうした状況を受け、今年 5 月からの新法に基づき、サイバー対処能力強化に向けた新たな枠組みの運用を進めており、その柱として①インシデント発生時の官民間での報告義務化と情報共有機関の設置、②通信データのヘッダー情報のみを対象とした取得・統計分析による兆候把握、③一定条件下で警察庁・自衛隊が攻撃者サーバーを無効化できる仕組みを挙げている。 3. 経産省としてのサイバーセキュリティ政策は、①サプライチェーンの標準化、②セキュア・バイ・デザインに基づく製品・システムの安全性向上、③政府を中心とした官民連携の強化、④人材育成・教育による業界全体の底上げ、という四本柱で推進していると述べている。 4. 中小企業向け施策として「サイバーセキュリティお助け隊」制度を用意し、補助金と組み合わせることで、EDR 等のツール導入・サイバー保険・いざというときの駆け付け対応を月額 1 万円以下のパッケージとして提供し、中小企業の最低限の防御力を底上げしようとしている。 5. IoT 機器向けには「JC-STAR」というセキュリティ対策ラベリング・評価制度を 2024 年 3 月に開始し、国が一定のセキュリティ要件を満たした製品を認定してラベル付けすることで、調達者・消費者が「セキュアな IoT 製品」を見分けやすくし、

private sectors. 6. Japan launched a device security evaluation scheme in March 2024 to help procurement teams identify routers and other equipment that meet government security standards, similar to EU approaches. 7. The government is promoting SBOM (Software Bill of Materials) adoption as a foundational tool for vulnerability management and secure-by-design practices, with guidelines released publicly in 2023. 8. Japan participates in international secure-by-design initiatives, including a joint declaration with about 50 nations to improve software supply-chain security. 9. A 2.9-billion-yen national research program launched in 2024 focuses on AI-enabled cyber defense, PQC migration, situational-awareness platforms, and operational cyber-range capabilities. 10. Japan's ICSCoE in Akihabara trains around 50 specialists per year in integrated IT/OT cybersecurity through a one-year program to develop core personnel for critical-infrastructure operators.	将来的に EU・米国の類似制度との相互認証も視野に入れている。 6. ソフトウェア部品表である SBOM（Software Bill of Materials）の活用を政府として推奨し、脆弱性発見時に自組織システムが影響を受けるかどうかをツールで機械的に確認できるようにするため、「SBOM 利用の手引き」Ver.2.0（2023 年 8 月）を公表し、さらに SBOM とセキュア・バイ・デザイン普及のための国際共同声明も 15 か国の機関と連名で発出していると紹介している。 7. 研究開発面では、2024 年から約 290 億円・5 年規模のサイバーセキュリティ研究プロジェクトを立ち上げ、①サイバースペース上の情報をいち早く収集する技術、②AI 等を活用したサイバー防御能力の向上、③最新の脅威も演習可能な共通基盤（サイバーレンジ等）の構築・官民での共有、④量子暗号技術などの先端技術の国産化を進めることで、国としてのサイバー能力向上を図るとしている。 8. 人材育成では、IPA の秋葉原 ICC（ICSOE）において、IT と OT の両方を学べる 1 年間の集中プログラムを実施し、重要インフラ事業者などから毎年約 50 名の受講生を受け入れ、「1 年間缶詰」で実践的なトレーニングを行うことで、各社に戻った際に中核的なサイバー人材として活躍できる層を育成していると説明している。 9. これらの政策・制度・R&D・人材育成を組み合わせることで、サプライチェーン全体と重要インフラを含む日本のサイバーセキュリティ水準を、技術・運用・人材の三位一体で底上げしていくことが経産省としての狙いである、というメッセージで締めくくっている。

3.9 D3-P3 Panel

Theme: Emerging Technology, Economic Security Moderator: HASHIMOTO Katsukuni Panelists: - Toru Tsuchiya (CEO, Cyber Defense Labs) - Katsumi Takahashi (Chief Security Scientist of NTT Social Informatics Laboratories) - Masayuki Kanda (Fellow, Security Center, Information-technology Promotion Agency, Japan (IPA)) - Tadahiko Ito (Senior Researcher at SECOM CO., LTD.)	テーマ：Emerging Technology, 経済安全保障での先端技術 モデレーター：橋本 勝国 パネリスト： - 土屋 徹 (サイバー防衛研究所 代表取締役) - 高橋 克巳 (日本電信電話(株) 社会情報研究所 主席研究員) - 神田 雅透 (情報処理推進機構(IPA) セキュリティセンター フェロー) - 伊藤 忠彦 (セコム株式会社 IS 研究所上級研究員)
1. Mr. Tsuchiya (Cyber Defense Labs) explained that space systems are becoming tightly linked to national and economic security, but are not	1. 土屋氏（Cyber Defense Labs）は、宇宙空間のサイバーセキュリティが新興技術・経済安全保障の観点から重要性を増している一方、日本の「重要インフラ」15 分野には

yet treated as “critical infrastructure” in Japan, even though satellite data (e.g., defense and foreign-vessel imagery) would be extremely sensitive if stolen. 2. He described realistic cyber-attack scenarios against space assets (ground stations, satellite control, inter-satellite links), constraints such as limited power and cryptography on satellites, and ongoing efforts in Europe (ESA’s cyber range in Estonia and joint work with JAXA/FUNDA) to build simulated environments to test and improve space-cyber defenses. 3. The moderator stressed that space industry cybersecurity is still immature compared to its technological sophistication, and highlighted new guidelines and collaborative schemes (e.g., ISA-BIOCAN-IFSA style “range” practices) to help suppliers and engineers understand how to protect satellites. 4. Mr. Ito (SECOM) explained the “harvest now, decrypt later” threat: data with long lifetimes (decades) encrypted today could be collected now and decrypted in the 2040s–2060s by future quantum computers, making timely migration to post-quantum cryptography (PQC) essential. 5. He distinguished between encryption and digital signatures: encryption is highly exposed to harvest-and-decrypt attacks and may need hybrid PQC + classical schemes (e.g., in TLS 1.3, CDNs, browsers), while web PKI signatures face scalability challenges (CT log sizes, PQC signature sizes) but have shorter certificate lifetimes, allowing somewhat smoother, staged migration. 6. Mr. Kanda compared PQC and QKD (quantum key distribution): PQC is software-compatible with today’s systems and can already be deployed widely, while QKD is powerful but limited to specific high-value links (fiber/satellite) and must be chosen case-by-case; he stressed that quantum-computer performance forecasts are uncertain, but policy and interoperability pressures (U.S., EU, G7) will	宇宙が含まれておらず、衛星データ窃取が国家安全保障・経済安全保障上の大きなリスクになり得ると指摘した。 2．宇宙分野では、衛星コンステレーションや地上局・衛星間リンクなどが攻撃対象となり得るが、電力制約等により通常の強い暗号を使いにくい制約があり、その脆弱性を踏まえて、欧州宇宙機関（ESA）やエストニアのサイバー演習環境を活用したサイバーレンジによる模擬攻撃・演習が進められていると紹介した。 3．モデレーターは、宇宙産業の技術的発展の割にサイバーセキュリティ対策はまだ未成熟であり、衛星保護のためのガイドラインや、ISA-BIOCAN/IFSA のようなレンジ演習を通じて、サプライヤやエンジニアに具体的な対策方法を示す取り組みが重要であるとコメントした。 4．伊藤氏（SECOM）は、「Harvest now, decrypt later（今収集して将来復号）」の脅威を説明し、運用 10 年＋保存 30 年といった長寿命データは、2040～60 年代に量子コンピュータが実用化した際に一括で復号されるリスクがあり、耐量子計算機暗号（PQC）への移行を先送りできないと述べた。 5．同氏は、暗号化と電子署名のリスクは性質が異なるとし、暗号化は収集・後日復号攻撃に弱いためハイブリッド方式（従来暗号＋PQC）の早期導入が必要である一方、Web PKI は証明書有効期間が短く CT ログ負荷や署名サイズ増大など運用課題はあるが、段階的な移行が可能だと整理した。 6．神田氏は、量子耐性の手段として「PQC」と「QKD（量子鍵配布）」を比較し、PQC は既存コンピュータ・ソフトウェアで利用可能なため広範なシステムに今すぐ導入できるのに対し、QKD はファイバや衛星回線など限定的・高価な用途向けでケースバイケースの選択になると説明した。 7．量子コンピュータの性能ロードマップや 2030～2040 年代の RSA 2048 破り予測は不確実である一方、米国 CNSA 2.0 や大統領令、EU・UK のロードマップ、G7 の R2PQC アクションプランなど「政策・相互接続の要請」により、各国が 2030～35 年頃までの PQC 移行を前提に動き始めていると解説した。 8．日本については、米欧より PQC 移行が遅れれば、エネルギーなどの基幹産業の海外輸出や相互接続が困難になるリスクがあり、政府・企業が暗号アルゴリズムの棚卸し（Crypto SBOM／Crypto レコンのようなリスト化）と優先順位付けを行い、重要インフラの PQC 移行を 2035 年までに完了させるべきだと提言した。 9．高橋氏（NTT ソーシャル情報研究所）は、PETs（Privacy Enhancing Technologies）を「プライバシー

force migration regardless. 7. He reviewed international PQC roadmaps: * U.S. CNSA 2.0 and executive orders push national-security systems toward PQC by early–mid 2030s, though details (RSA 2048, intermediate curves vs direct PQC) are still debated. * EU and UK set priority-based timelines (e.g., high-impact systems by ~2030, others by ~2035) and encourage hybrid use of PQC with existing algorithms plus global monitoring/"observatory" of migration. 8. For Japan, he warned that lagging behind U.S./EU timelines could harm exports and interoperability, and argued that government and industry should: (a) create a "crypto SBOM / Crypto-Reco" style inventory of algorithms in use, (b) publish concrete PQC migration guidelines, (c) push to complete migration of significant infrastructure by around 2035, and (d) ensure new equipment and products are PQC-ready. 9. Mr. Takahashi (NTT Social Informatics Lab) introduced Privacy-Enhancing Technologies (PETs) as a broad family of tools (anonymization/differential privacy, encryption, TEEs, secure computation, consent and audit mechanisms, etc.) whose core goals are to protect privacy and data security while still enabling data use across organizations and borders. 10. In closing, the moderator linked everything back to "two wheels": digital transformation and cybersecurity must advance together; strong encryption, PETs, and PQC are necessary to maintain trust, enable safe data sharing, protect individuals' privacy, and give citizens and businesses a convincing, secure vision of the digital future.	保護とデータ利活用を両立させる技術群」と位置づけ、匿名化・差分プライバシー、暗号・TEE、ユーザ同意・コントロール、記録・監査など４つのコア機能と、OECD プライバシー原則や GDPR のデータ最小化との関係を整理した。 10. モデレーターは、デジタルトランスフォーメーションとサイバーセキュリティは「車の両輪」であり、強固な暗号・PQC・PETs を組み込んだ仕組みづくりによって、個人・企業・政府の信頼を長期的に維持しつつデータ活用を進めることが、日本社会の将来像を示すうえで重要であるとまとめた。

3.10 D3-S7 Speech

Satoshi Maeda (Advisor, Cyber Defense Labs)	前田 哲 (サイバー防衛研究所 顧問)
1. The speaker framed economic security as increasingly critical, driven by globalization,	1. 前田氏は、経済安全保障について「背景」「日本の対応」「今後の方向性」という３点構成で、ラフスケッチとして論

digital transformation, and escalating geopolitical tension between the United States and China. 2. He described how the post–Cold War era saw the U.S. leading a free economic order, but China's rapid rise—especially after the Deng Xiaoping reforms and Xi Jinping's leadership—shifted the global balance and introduced economic power as a strategic tool. 3. Around 2017–2019, the U.S. formally changed its stance toward China, moving from engagement to competition, with tariffs and economic-security policies marking the shift; this transformation heavily influenced Japan's own policy direction. 4. Japan's response included the 2022 Economic Security Promotion Act, aimed at securing supply chains, protecting critical infrastructure and energy systems, strengthening public–private cooperation, and safeguarding sensitive data. 5. Japan also pushed forward with security-clearance–related initiatives for government officials and innovation-related programs to address vulnerabilities in advanced technology sectors. 6. Active cyber defense was introduced as a key component of Japan's evolving security architecture, requiring close coordination among government, private industry, and critical infrastructure operators. 7. The speaker emphasized that economic security is no longer a government-only domain; the private sector is now directly involved in geopolitical power competition and must prepare accordingly. 8. He noted the gray-zone nature of modern economic competition, where peace and emergency states blur, creating unfamiliar challenges for Japan's governance structures and requiring new frameworks. 9. Japan must balance strong economic-security measures with maintaining a functioning free-trade system, which remains essential for	点を提示する趣旨であると説明している。 2. 経済安全保障が国際問題として浮上した背景として、①経済のグローバル化と社会の DX 進展、②米中対立の顕在化を挙げ、冷戦終結後の米一極体制から、テロの時代を経て、中国が「改革開放」からパワーゲーム主体へ舵を切った構図を整理している。 3. 中国はエンゲージメント政策で「豊かになれば自由化する」と期待されていたが、習近平政権期を境に経済力・軍事力をパワーゲームに用いる方向へ転換し、その結果として米中対立が鮮明化したと指摘している。 4. アメリカはトランプ政権以降、関税・経済制裁など経済手段を前面に出して国際政治を行うようになり、「軍事＋経済」が一体となった新しいパワーゲームの時代に入ったという認識を示している。 5. 日本の対応としては、2013 年の最初の国家安全保障戦略には「経済安全保障」という用語すらなく、認識が遅れていたが、2020 年の自民党提言を契機に、①2022 年の経済安全保障推進法（サプライチェーン強靭化、重要インフラ、官民技術協力・情報保護）、②2024 年のセキュリティ・クリアランス法制、③サイバー対処能力強化法（官民連携・通信情報の利用・アクティブサイバー措置）などを整備してきたと述べている。 6. もっとも、これらの法整備は「ようやく最初の一歩を踏み出した段階」に過ぎず、制度を実際に運用し、体制を作り込んでいくうえで、まだ課題が山積していると強調している。 7. 今後の方向性として、経済安全保障は米中対立が続く限り長期の構造問題であり、中国は古くから「戦わずして制する」孫子的発想で経済をパワーゲームに用いてきた歴史があるため、容易に収束しないとし、長期戦を前提に考える必要があると述べている。 8. 経済安全保障の最大の特徴として、従来の軍事安全保障と異なり、主体が「政府だけでなく民間企業も含まれる」点を挙げ、官民連携体制をどう構築するかが極めて重要だが、日本はその経験が乏しく、サイバー分野でもまだ意識が十分に追いついていないと指摘している。 9. 経済安全保障の世界では、有事と平時の境界が曖昧なグレーゾーンが長く続き、従来のように「戦争か平和か」を明確に区切る発想が通用しないため、その前提で体制を組み直す必要があると述べている。 10. 最後に、自由貿易体制・グローバル化・DX の価値を維持しつつ、経済安全保障とのバランスをどう取るか、隣国・中国と 50 年・100 年単位でどう共存していくかが、日本に突きつけられている根本課題であり、その難しい問題を今後パネルディスカッションでさらに議論したいと結んでいる。

national prosperity amid globalization and digital transformation. 10. Given its geographic proximity and deep economic interdependence with China, Japan faces the long-term challenge of managing competition while sustaining stable coexistence—an issue that will shape economic-security policy for decades ahead.	

3.11 D3-P4 Panel

Theme: Economic Security Promotion Act Moderator: Jun Osawa (Principal Researcher, Dentsu Soken Center for Economic Security Research) Panelists: - Satoshi Maeda - Gloria Glaubman - Junichi Nishiyama	テーマ：経済安全保障推進法 モデレーター：大澤 淳 (電通総研安全保障センター (DCER) 研究主幹) パネリスト： - 前田 哲 - グローリア・グローブマン - 西山 淳一
1. The moderator explains that this panel will address how to promote economic security, with a particular focus on the Economic Security Promotion Act and its narrower scope within the broader concept of economic security. 2. Nishiyama highlights the vulnerability of critical services through recent ransomware incidents (e.g., Asahi beer, JAL, hospitals), arguing that media and the public still fail to recognize such attacks as threats to national infrastructure and daily life, not just to individual companies. 3. He stresses that victims must frame cyber incidents as social and national-security issues, not only corporate troubles, and calls for a narrative that encourages information sharing rather than shame or silence. 4. Nishiyama notes that Japan is already effectively in a “cyber war” gray zone where there is no clear boundary between peace and emergency, and that current legal and institutional frameworks have not caught up with this reality. 5. Gloria frames Japan’s Economic Security Promotion Act as a landmark recognizing that national security and economic resilience are	1. このパネルは、経済安全保障推進法を軸に、「重要インフラとサイバー攻撃」「官民連携」「日米を含む国際協力」をどう進めるかを議論することを目的として開始されたのである。 2. 大澤氏は、アサヒグループホールディングスやアスクルへのランサムウェア攻撃、海外でも物流企業や自動車メーカーが狙われ経済活動が止まっている事例を挙げ、日本でも同様に重要インフラ企業が狙われる可能性が高く、官民連携による防御が経済安全保障上の核心だと問題提起している。 3. 西山氏は、アサヒビール事案で当初「システム故障」と発表し、後からランサムウェアと認めた点や、影響を「居酒屋で生ビールが飲めない」レベルに矮小化した報道姿勢を批判し、日本航空の発券システム障害、地方銀行９行、複数病院の長期停止なども含め、「一社のビジネス問題」として消費されてしまっていると指摘している。 4. これらの事案は本来、日本の社会基盤や日常生活に対する攻撃として捉えるべきであり、個々のインシデントの背後にある国家インフラのリスクを「見える化」し、国として教訓を共有・対策しなければならない、今や我々は低強度の「サイバー戦争」の只中にいるのだ、という危機感が示された。 5. グロリア氏は、経済安全保障推進法は市場・取引・制度へのトラストを支える大枠のフレームワークであり、①重要物資の安定供給、②重要インフラの機能維持、③先端重要技術の開発支援、④秘密特許制度の四本柱を、透明性・多様化・備蓄・代替確保などのベストプラクティスと組み合わせて実装すべきだと述べた。 6. 特に重要インフラのサイバーセキュリティについては、NIST

inseparable, and she maps best practices for its four pillars: resilient supply chains, critical infrastructure protection, secure innovation, and confidential patents. 6. She recommends concrete measures such as supply-chain mapping and diversification, adopting established cyber-physical standards (e.g., NIST CSF, IEC 62443), creating an incident portal that returns timely intelligence to operators, secure research tiers for universities, and predictable rules and timelines for "confidential patents." 7. In discussion, panelists agree that financial, energy, telecom, logistics, and semiconductor sectors are especially critical, and they emphasize that effective public–private cooperation requires changing mindsets, building trusted information-sharing mechanisms, and developing a security-clearance framework that can extend to key private-sector actors. 8. They argue that government should act as a clearinghouse for sensitive incident data from industry, protect contributors from undue disclosure (e.g., FOIA-type risks), define standards for what data must be shared, and harmonize shared information so that all relevant companies can benefit from collective threat insights. 9. The panel ends with short recommendations for U.S.–Japan cooperation: strengthen mutual security-clearance frameworks so sensitive information can be shared, conduct joint cyber exercises to build capacity and trust, and leverage U.S. experience to shorten Japan's learning curve in building economic-security and clearance systems. 10. In the closing remarks, the symposium organizers thank speakers and participants, recap that the day focused on economic security, critical information infrastructure protection, information sharing, security clearances, and AI security/ethics, and announce that the final day will shift toward	CSF や IEC 62443 といった国際標準の活用、ナショナル・インシデントポータルによる迅速なインテリジェンス共有、パッチやアップグレードの安全な仕組み、同盟国との共同レッド／ブルーチーム演習などが有効だと提言している。 7. 重点セクターとして、半導体、エネルギー・産業基盤、重要鉱物、金融インフラなどを挙げ、これらの分野でサプライチェーンの可視化とレジリエンスを高めつつ、コンプライアンスとイノベーションを両立させることが経済安全保障に直結すると強調した。 8. 前田氏は、法制度面ではサプライチェーン強靭化の柱が「特定重要物資」の指定と国内生産基盤への支援にほぼ限定されており、調達先多元化や備蓄、対内投資スクリーニングなど、本来必要な政策に対して射程がまだ狭いと指摘し、今後も制度の拡充が不可欠であると述べた。 9. また、重要インフラ防護や技術保護のためには、民間まで含めた実効性あるセキュリティ・クリアランス制度と情報共有スキームの構築、サイバー人材の育成と流動性確保（公務と民間を行き来できるキャリア設計）、さらに省庁間の縦割りを超えた政府内コンセンサス形成が大きな課題であると整理された。 10. 国際連携については、日米間でのセキュリティ・クリアランスの相互承認や共同サイバー演習・共同研究、米国が 20 年かけて築いた経済安全保障・サイバー対処システムの経験共有などを通じ、日本の経済安全保障とサイバー防御体制を短期間で高度化していくべきだという点で、登壇者の認識が一致してセッションが締めくくられたのである。

societal security topics such as data security, DFFT, and technology updates from industry partners.	

3.12 D3-S8 Day #3 Closing

Muhammad Salman	ムハンマド・サルマン
1. The speaker thanked participants for their patience and opened the closing of Day 3. 2. He expressed deep appreciation on behalf of INCS-CoE for the active participation throughout the day. 3. The day's discussions covered economic security, focusing on critical information infrastructure protection. 4. Key topics included information sharing and security clearance frameworks. 5. Insights were provided by experts from industry, government, and Keio Global Research Institute. 6. A parallel roundtable addressed AI security and ethics, featuring UNIDIR, a UN body promoting responsible AI. 7. Speakers and panelists were thanked for sharing expertise and enriching the program. 8. Participants were recognized for their time, attention, and enthusiasm. 9. Day 4 will focus on societal security, including data security and Data Free Flow with Trust (DFFT). 10. Tomorrow’s parallel sessions will include technology updates from industry partners such as Microsoft, Google, Trend Micro, Cisco, Hitachi, and ACCJ.	1. 議長は参加者の忍耐に感謝し、3 日目の閉会を宣言した。 2. INCS-CoE を代表し、終日における積極的な参加に深く謝意を表した。 3. 当日の議論は経済安全保障を扱い、重要情報インフラ保護に焦点を当てた。 4. 主要テーマには情報共有とセキュリティ・クリアランス枠組みが含まれた。 5. 産業界、政府、慶應義塾グローバル研究所の専門家から知見が提供された。 6. パラレルラウンドテーブルでは AI の安全性と倫理を議論し、責任ある AI 推進の国連機関 UNIDIR が登壇した。 7. 講演者とパネリストには専門知識を共有しプログラムを充実させたことへの謝意が示された。 8. 参加者には時間と注意、熱意を注いだことへの謝意が表明された。 9. 4 日目は社会的安全保障に焦点を当て、データセキュリティと信頼に基づくデータ自由流通（DFFT）を含む。 10. 翌日の並行セッションでは、マイクロソフト、グーグル、トレンドマイクロ、シスコ、日立、ACCJ などの業界パートナーによる技術最新情報が提供される。

4 DAY 4: October 31 | West School Building 1F West Hall

4.1 D4-S1 Day #4 AM Opening

Karl Steiner	カール・シュタイナー
1. The speaker welcomes attendees to the final day of the 15th International Cyber Security Symposium and provides an overview of the four-day event. 2. The symposium is hosted by Keio University's Cyber Security Research Center and the MITRE Corporation, with parallel sessions also taking place in the North Building. 3. Carl Steiner, Vice President for Research at UMBC, opens the day and notes UMBC's role as a charter member of the International Cybersecurity Center of Excellence (INCS-COE). 4. He emphasizes the increasing transparency of national borders in the digital age and the global rise of ransomware, DDoS, and other cyberattacks. 5. He stresses the need for trusted international networks across governments, private sector, and academia to effectively detect, protect, and respond to cyberattacks. 6. The symposium's theme—cybersecurity for digitized national, economic, and societal security with a focus on multilateral public-private partnership—is described as timely and globally relevant. 7. He recaps previous symposium days: Day 1 focused on international cooperation and keynotes; Day 2 on national security; Day 3 on economic security; and Day 4 will focus on societal security. 8. Steiner highlights UMBC's proximity to NSA, its dual NSA designations in Cyber Defense and Cyber Research, and its long-term participation in the U.S. Federal Cyber Corps program. 9. He notes that the symposium has been stimulating and will inform cybersecurity improvements at UMBC and within its surrounding communities. 10. He outlines today's program: a keynote by the Commissioner of IPA followed by two	1. 講演者は、第 15 回国際サイバーセキュリティシンポジウムの最終日に参加者を歓迎し、4 日間にわたるイベントの概要を説明する。 2. このシンポジウムは、慶應義塾大学サイバーセキュリティ研究センターと MITRE 社が主催し、北館でも並行してセッションが開催されている。 3. UMBC の研究担当副学長であるカール・スタイン氏がこの日の開会を宣言し、UMBC が国際サイバーセキュリティ・センター・オブ・エクセレンス（INCS-COE）の創設メンバーとしての役割について言及した。 4. 彼は、デジタル時代における国境の透明性の高まり、およびランサムウェア、DDoS、その他のサイバー攻撃の世界的な増加を強調した。 5. サイバー攻撃を効果的に検知、防御、対応するためには、政府、民間、学界にわたる信頼できる国際的なネットワークが必要であると強調した。 6. シンポジウムのテーマである「多国間の官民パートナーシップに焦点を当てた、デジタル化された国家、経済、社会のセキュリティのためのサイバーセキュリティ」は、時宜を得た、世界的に関連性の高いものであると述べた。 7. 彼は、これまでのシンポジウムの日程を次のように要約した。1 日目は国際協力と基調講演、2 日目は国家安全保障、3 日目は経済安全保障、そして 4 日目は社会の安全保障に焦点を当てる。 8. スタインは、UMBC が NSA に近接していること、サイバー防衛とサイバー研究の両方で NSA の指定を受けていること、そして米国連邦サイバー軍団プログラムに長期にわたって参加していることを強調した。 9. 彼は、このシンポジウムは刺激的であり、UMBC および周辺コミュニティにおけるサイバーセキュリティの改善に役立つだろうと述べた。 10. 彼は、本日のプログラムの概要を説明した。IPA コミッショナーによる基調講演に続き、2 つのパネルディスカッションが行われる。1 つはトラスト法と個人データ保護について、もう 1 つは新しいデータサイエンスの応用についてである。

panels—one on Trust Acts and personal data protection, the other on new data-science applications.	

4.2 D4-S3 Speech

Yutaka Saito (Commissioner, IPA)	齊藤 裕 (独立行政法人情報処理推進機構 (IPA) 理事長)
1. The commissioner of IPA, Mr. Saito, introduces IPA's digital activities, covering digital architecture, digital infrastructure, human resources, IT security, industrial cybersecurity, and AI safety. 2. His background includes work at Hitachi, Planet Player, and leadership roles at IPA; he became commissioner in 2023. 3. IPA operates multiple centers—including digital architecture, digital infrastructure, cybersecurity, and AI safety—to support Japan's data-driven society and ensure safety in cyberspace. 4. Japan aims to build a new digital ecosystem and AI-driven mechanisms, under two supervising ministries, promoting digital society initiatives across industries. 5. Japan plans to advance "data arrangements," designing which industries and companies will implement them and establishing a nationwide structure for industrial and societal adoption. 6. To realize this, Japan must invest in data platforms, with the government creating policies and systems, and IPA supporting public–private collaboration and international normalization efforts. 7. The digital ecosystem architecture is designed within IPA, supported by academia, industry, and government; open-source software (OSS) and R&D outputs are intended for broad reuse. 8. For social implementation, the government provides incentives and sometimes enforcement to ensure digital services are deployed and governed based on architecture and code controlling behavior. 9. Digital trust is described as an autonomous, data- and software-driven system, requiring	1. IPA の現状として、デジタルアーキテクチャ、デジタルインフラ、デジタル人材、サイバーセキュリティ、AI セーフティなど複数のセンターが国家のデジタル社会を支える事業を展開していると説明した。 2. デジタル社会（Society 5.0）の実現に向け、アーキテクチャ設計、デジタル基盤整備、データ標準化、社会実装の普及などを推進していると述べた。 3. デジタル人材育成として、デジタルスキル標準の整備、タレント育成、スキルアセスメントなどを体系的に進めていると説明した。 4. サイバーセキュリティ分野では、国家・経済安全保障に資するセキュリティ確保や人材育成、リアルとサイバーの融合に伴う高リスクへの対応を行っていると述べた。 5. 管轄するデジタル庁と経産省の政策として、DFFT を含むデータ連携、データスペース構築、地方の生活インフラのデジタル化、産業横断のデータ連携基盤などが進んでいると紹介した。 6. アメリカ型・中国型・欧州型と比較し、日本型デジタルエコシステムは官民協調・全体最適・分散連携を重視するボトムアップ型の特徴を持つと説明した。 7. データ連携・サービス連携において、データ量よりも"連携による質"を重視し、公益的プラットフォーム構築を目指す姿を示した。 8. アーキテクチャはサイバー空間におけるガバナンスの基盤であり、コードと組み合わせることで信頼性あるエコシステムを実現する鍵であると強調した。 9. デジタルトラストの確立に向け、制度、ID、ガバナンス、監査、倫理などを包括的に整備し、ソフトウェア主体の信頼検証を可能にする仕組みを構築していると述べた。 10. 経団連・政府との連携により産業データスペース構築が加速しており、IPA はデジタル社会のイネーブラーとして、人材・基盤・ルールづくりのハブとなることを目指すと締めくくった。

governance across systems, infrastructure, processes, data, and software—not only human actors. 10. Japan proposed frameworks for industrial data spaces, including cost-sharing and cross-border deployments; under Digital Agency leadership, Keidanren launched the Japan Digital Ecosystem Partnership, with IPA as Secretariat, providing platforms and human resources for public and private sectors.	

4.3 D4-P1 Panel

Theme: Basic Act on the Advancement of Public and Private Sector Data Utilization, Trust Act, Act on Personal Information Protection Moderator: Naoto Kikuchi (Vice Chairman, Digital Policy Forum, Project Professor, Graduate School of Media Design, Keio University) Panelists: - Koichi Akaishi - Noriaki Okui (President and CEO, Data Society Alliance) - Hiroshi Mano (Executive Director and Secretary General, Data Society Alliance) - Takashi Kai (Project Researcher, Keio Global Research Institute)	テーマ：官民データ流通促進法、トラスト法、個人情報保護法 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、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： - 赤石 浩一 - 奥井 規晶 (データ社会推進協議会 代表理事・理事長) - 眞野 浩 (データ社会推進協議会 専務理事／事務局長) - 甲斐 隆嗣 (慶應義塾大学グローバルリサーチインスティテュート 特任研究員)
1. The panel introduces three major groups—DPFJ, DSA, and JDTF—explaining their roles in promoting digital trust, data-space development, and public–private data collaboration in Japan. 2. Speakers emphasize the need to modernize Japan's data-related legal framework, including rebuilding the public–private data utilization law and revamping privacy law to enable lawful reuse of public-purpose and certain personal data. 3. They note the explosion of sensors, IoT devices, machine-to-machine links, and AI agents autonomously accessing and processing data, creating new requirements for trust, secure data flows, and realistic, step-by-step legal reforms. 4. Ransomware incidents are cited to illustrate	1. 本セッションは、データ社会推進協議会（DSA）、デジタルトラスト協議会（JDTF）、デジタル政策系団体（DPFJ）の「3 団体による提言」を起点に、データスペースとトラスト、個人情報保護制度見直しの方向性を議論する場であると位置づけられている。 2. 3 団体の最新ステートメントでは、①データ利活用・データスペース構築運営のための法制度整備（データ連携基盤とトラスト基盤の 2 つの枠組み）、②個人情報保護規律の見直し、③公益目的データ利活用のための段階的な新制度、の 3 点を大きな柱として掲げている。 3. データ連携基盤の構想では、最下層のクラウド・ネットワーク等のサービス層、その上のデータ連携層、最上位のアプリケーション層という 3 層アーキテクチャを前提とし、日本型データスペースを支える法枠組みを官民データ活用推進基本法の改正や新法で整備すべきだと主張している。 4. 個人情報保護については、従来の「人対人／紙ベース前提」の同意・第三者提供・共同利用の枠組みが、IoT・センサー・M2M・AI エージェント時代には限界があり、「容易照

why Japan needs secure data spaces, proper data governance, decentralized backups, and trust mechanisms that separate “security layers” and “trust layers.” 5. A “data trust anchor” or data-exchange–market model is discussed: intermediaries bind data, identity, and contractual terms using PKI and data usage certificates, following IEEE 3800 industrial data-space standards. 6. Several speakers argue that Japan lacks a widely accepted national trust anchor (TTP) and that very few policymakers understand the “trust layer,” making it difficult to advance DFFT and align with US/EU/Asia-Pacific data-space initiatives. 7. The discussion contrasts Japan’s privacy-first culture with Europe, where even sensitive data (e.g., healthcare data) can be reused under governed data-space frameworks with strict oversight. 8. Trust technology alone is considered insufficient; architecture, legal design, incentives, and mindset change (beyond superficial DX) are needed to enable secure and economically valuable data reuse. 9. The panel stresses the importance of international interoperability, including global standards, cross-border data spaces, and alignment with US/EU frameworks for trust services, e-delivery, and digital identity. 10. In closing, speakers note societal and political barriers, call for long-term structural reform, and emphasize building a foundation of digital trust—combining privacy, security, and governance—to support AI-era data flows and a collaborative public–private digital ecosystem.	合性」概念なども含めて、技術の進展を前提にした新たな規律設計が必要だと指摘されている。 5. パネルでは、トラストを支える技術（電子署名・電子シール・タイムスタンプ・eDelivery・VC など）と、それをどこでどう使うかという「トラストサービス／制度」のレイヤーを明確に分け、契約・履歴管理・データ取引市場などと統合したアーキテクチャとして設計すべきだという点で意見が一致している。 6.「日本版トラスト法」（名称は仮）のような制度と電子証明・電子認証技術を組み合わせることで、ランサムウェア被害やなりすまし、誤情報、AI エージェント間通信など、発信者真正性や改ざん防止が鍵となる問題群に横断的に対処すべきだという問題意識が共有されている。 7. データ取引の世界では、トラストアンカー／インターメディエーターが、データ提供者と利用者の本人性・データの完全性・契約条件の履行を担保する「保証人」の役割を果たすべきであり、日本発の「データトラストアンカー」「データポリシー」の国際標準化活動（ISO/IEC 等）も進めていることが紹介された。 8. セキュリティとトラストは別レイヤーであり、マイナンバーのような個人向けトラストアンカーはある一方で、企業向けのトラストアンカーが欠如しており、そのために DFFT の“T（トラスト）”が日本では実体を持っていないという強い危機感が表明された。 9. 個人情報・医療データ等の公益的・共益的な利活用について、EU の GDPR／EHR データスペース、英国の医療データ事例などを参照しつつ、日本も「使わない前提」から脱却し、プライバシー保護技術とトラストサービスを前提に、公益・共益のための柔軟な利用を可能にする特別法・運用を整備すべきだと議論された。 10. 全体のまとめとして、インターネット普及から約 25 年を経た今、AI エージェントとデータ連携が経済成長と安全保障の中核になる時代に、日本が国際的なデータスペース・トラスト枠組みから取り残されないよう、政治・行政・産業・学術が連携して、トラストレイヤーと個人情報制度の再設計を急ぐべきだというメッセージで締めくくられた。

4.4 D4-S4 Speech

Hiroshi Mano	眞野 浩
1. The speaker introduces himself as director of the Data Society’s new department, CEO of the data trading company EverySense, a board member of a standards association, and chair of the IEEE Data Trading System (DTS).	1. 眞野氏は、データスペースのアプリケーションをテーマとするパネルに先立ち、DSA（データ社会推進協議会）と自身の役割（DSA 事務総長、DFFT 関連 WG、標準化活動など）を紹介し、日本はデータ活用・データ供給が不足しており、漏えい懸念などからデータ流通が進んでいないという課題

2. He explains that innovation in a domain-independent, data-driven society depends on smooth data flows among many stakeholders, but data usage is still low in Japan and across the OECD. 3. Four main obstacles to data flow are identified: lack of trust in giving data to others, uncertainty about how received data can be used, the cost of preparing data that were not created for sharing, and poor visibility of who holds what data. 4. Japan promotes the DFFT (Data Free Flow with Trust) concept internationally and defines “data spaces” as ecosystems where organizations and individuals with common goals share data under data sovereignty and shared governance. 5. DSA’s “DataX” initiative develops and tests data-space technology; according to IOFDS, a data space is a decentralized ecosystem with common policies, rules, and a governance framework that enables secure, trustworthy data transactions. 6. To build a data space, one must define stakeholders, data objects, collaboration protocols, and trust mechanisms, with roles including data space authorities (operators), participants (providers/receivers), and intermediaries such as data trading market and catalog operators. 7. Participants publish data catalogs, discover each other via catalog sites, and exchange data through standardized connectors that verify the authenticity and integrity of both counterparties and data; transactions can be one-to-one, one-to-many, or multi-hop with intermediate processing. 8. Data spaces built with Data-EX technology are domain-agnostic and envisioned for use in disaster prevention, energy/battery, circular economy, academic research, and later medical and tourism fields. 9. The TRAx data trading market uses a “trust intermediary” that relies on PKI/CA to validate	認識を示した。 2. ビデオでは、DSA が掲げる「Data Free Flow with Trust（DFFT）」と「データ社会」の理念を説明し、データスペースを「共通目的を持つ組織・人が、主権（ソブリンティ）を維持しながらデータを安全に流通・利用する分散型エコシステム」と定義した。 3. データスペースを構成するには、①誰が参加するか（ステークホルダー）、②どんなデータを扱うか（オブジェクト）、③どう連携するか（プロトコル）、④どう信頼性・完全性を担保するか（トラストメカニズム）を明確化する必要があると説明した。 4. ステークホルダーとして、データスペース全体を管理運営する「データスペースオーソリティ（オペレーター）」、データを提供・取得する「参加者」、データ取引市場運営者やデータカタログサイト運営者などの「仲介者（インターミディエータ）」といった役割が整理された。 5. 参加者は提供可能なデータの概要をツールでカタログ化し、公開範囲を制御しながらカタログサイトに掲載することができ、他の参加者はそのカタログを検索してコネクタ経由でデータ提供をリクエストし、相互認証と完全性検証を行ったうえで、安全なデータ交換を行う仕組みであると説明した。 6. トランザクションパターンとして、①1 対 1 のデータ交換、②1 対多への同一データ配信、③多者が順番に加工しながらデータを受け渡していく形の 3 種類があり、データ形式に依存しない標準化された機能により、多様なコラボレーションを実現できると述べた。 7. コネクタや基本機能を標準化することで、参加者は複数のデータスペースにまたがってスムーズに参加でき、DSA では Data-EX 技術を用いて、防災、バッテリーパスポート、サーキュラーエコノミー、アカデミア（研究）などのケースモデルを作成し、将来は医療や観光などにも展開する構想であると紹介した。 8. トラストの仕組みについては、従来の PKI（CA・証明書・電子署名）やオープンデータにおける完全性保証と同様、データスペースにおけるデータ授受でも「誰が何を渡し、何が保証されているか」を明確化することが重要であり、相互運用性（インタオペラビリティ）を確保した統一的なやり方が必要だと強調した。 9. 現状では、データスペース間やオーソリティ間をまたいでデータ処理事業者・セキュリティオペレーター等を発見・連携するためのプロトコル（データスペース・ディスカバリプロトコル）が未整備であり、国際標準（ISO/IEC 38xxx 系）と連携しながら、その仕様策定に取り組んでいると述べた。 10. 最後に、この後のセッションでは 4 つの具体的アプリケー

data providers, recipients, and the integrity and completeness of data, and to bind data to contractual usage conditions, acting somewhat like a notary. 10. Interoperability is pursued via a unified method between data spaces and participants (avoiding any single “god-like” gateway), with IEEE 3800 and 3800.2 working on international standards so multiple virtual data spaces across domains can coexist while keeping trust and authority at the edge.	ションを題材に、データスペースをどう作るか、既存のバーチャルデータやシステムとどう連携させるか、といった観点で議論を深めたいとし、パネルディスカッションへのつなぎとして発表を締めくくった。

4.5 D4-P2 Panel

Theme: Applications on Dataspace, ABtC (Battery Passport), CBAM (CO2), Invoice (Finance), Medical Moderator: Hiroshi Mano Panelist: - Kenji Hiramoto (Head, IPA Digital Infrastructure) - Akira Sakaino (Evangelist, NTT Communications) - Shinji Abe (Chief Technology Director, NEC Corporation) - Taka Matsutsuka (Senior Research Director, Fujitsu)	テーマ：データスペースにおけるアプリケーション、ABtC(バッテリーパスポート)、CBAM(CO2)、インボイス(金融)、医療 モデレーター：眞野 浩 パネリスト： - 平本 健二 (IPA デジタル基盤センター センター長) - 境野 哲 (NTT コミュニケーションズ エバンジェリスト) - 阿部 晋樹 (日本電気株式会社 上席技術主幹) - 松塚 貴英 (富士通株式会社 データ＆セキュリティ研究所 シニアリサーチディレクタ)
1. The panel discusses how data spaces will be used together with AI, including learning, RAG-style use in organizations, and AI agents, and stresses the need to respect data rights and clarify how to govern autonomous agents. 2. Concrete data-space use cases are presented: plastics recycling (circular economy, digital product passports) and rare-disease / hemophilia medical data spaces aimed at improving patients’ quality of life (QOL). 3. EU regulations on recycled plastics (e.g., 15% and 25% targets for automobiles) are creating strong pressure on Japanese industry, revealing that most “recycled” plastics are still being burned and that new domestic value chains and data spaces are needed to meet future requirements. 4. NTT Docomo and other telecom actors	1. 富士通・松塚氏は、データスペースにおける「トラスト」と「AI 活用」を両輪として、製造・物流・ヘルスケア・サステナビリティなどのユースケースに取り組みつつ、フェデレーテッドラーニング、マルチ組織 RAG、AI エージェント協調などの技術類型を整理していると説明した。 2. ロジスティクス分野では、荷主と配送事業者の個別最適で非効率な現状に対し、データスペースを用いて配送要件を標準化・共同最適化する構想を紹介し、富士通らによる「サステナブルシェアトランスポート」で共同配送の実証を進めていると述べた。 3. NEC・阿部氏は、デジタルトラスト協議会や産業データスペース WG の活動、SIP「プラネット J」によるプラスチック循環データスペース、希少疾患レジストリなど、ヒト・モノ・データのトラストを軸とした社会実装プロジェクトを紹介した。 4. プラスチック循環では、日本の廃プラの約 6 割が実質焼却であり、EU の ELV 規制による再生材利用率義務（例：2031 年に 15%）に対して、自動車用再生プラスチックが圧倒的に不足している現状を示し、「プラネット J」で

explain their role in secure data spaces: monitored WAN and IoT networks with embedded anomaly and behavior detection, network-level isolation, and confidential computing environments where encrypted data and algorithms can be processed safely. 5. Trust anchors and internationally interoperable certification are highlighted as essential: robots, devices, and AI agents must be strongly authenticated (who/what they are, which country they belong to, what legal regime applies) before exchanging data across borders. 6. IPA's digital infrastructure and AI safety initiatives are described as building the technical and governance foundations: software engineering with open source building blocks, data governance, semantic technologies, and AI governance aligned with the UN Global Digital Compact and SDGs. 7. Multiple speakers emphasize that data governance and data management maturity are still weak in Japan: many organizations are paper-based or Excel-driven, internal processes are not standardized, and provenance/lineage and quality cannot be ensured until basic digitization and management are fixed. 8. Legal tech ("legal engineering") is proposed as a key enabler: encoding laws, regulations, and internal company rules in machine-readable form to support cross-border compliance (e.g., recycling rules in different countries) and to serve as a defense against malicious or adversarial AI inside data spaces. 9. The panel reflects on cultural and structural barriers in Japan—hanko culture, hierarchical and vertically integrated relationships, dependence on ad-hoc manual work, and weak rule-making—arguing for mindset change, more open-source tooling, and shared "building blocks" developed in government and industry communities. 10. In closing, the moderator and panelists agree that trusted data spaces require combining security and trust across all layers	国内の廃プラを集約・可視化し、新たなリサイクルビジネスとサプライチェーン連携を構築しようとしていると説明した。 5. NTT・境野氏は、データスペースは「トラストに基づくデータ交換エコシステム」であると位置づけ、通信事業者として WAN や IoT ネットワークの中に振る舞い検知や隔離機能を組み込んだセキュリティサービス、暗号化されたままデータとアルゴリズムを処理する環境（秘密計算的な基盤）を提供し、ロボット・AI が安全にデータを利活用できるようにする構想を示した。 6. 境野氏はさらに、クロスボーダーなデータ交換では、AI・データ・ソフトウェア・人間の「トラスト」と、国境・法規制を自動的にチェックして不正なデータ要求を拒否する仕組みが必要であり、悪意ある AI との「攻防」に備えるセルフディフェンスとして、リーガルテック／リーガル・インタープラビリティの重要性を強調した。 7. IPA・平本氏は、METI とデジタル庁の双方からファンドされる技術シンクタンクとして、JAPAN デジタルインフラストラクチャセンターを軸にデータスペース、データマネジメント／ガバナンス、AI セーフティ、データモデルやガイドブックの整備などを進め、デジタルエコシステム全体の基盤づくりと人材育成を担っていると説明した。 8. パネル全体を通じて、①社内データマネジメントが未整備（紙・Excel 依存）、②オープンデータやベースレジストリなど公共セクターが「浄水場」としてデータ品質を高める必要、③メタデータや来歴情報によるトレーサビリティとセマンティクス整備、④ルールや規程を機械可読にするリーガルテックの普及、などが日本のデータスペース推進に向けた優先課題として共有された。 9. 議論では、日本社会の「ハンコ文化」「性善説」「エクセル文化」に基づくデジタル化止まりの状況を問題視し、オープンソースや共通基盤の活用、業務標準化、自治体や公共分野からの先導的なデータ活用、コミュニティ（DSA・IDSA・RRI・SIP-EX など）間連携によって、真のデジタルトランスフォーメーションとトラストに基づくデータスペースのエコシステムを日本で立ち上げていくべきだ、というメッセージで締めくくられた。

(network, data, legal, and organizational), strengthening data management, and fostering collaborative ecosystems (DSA, IDSA, SIP, etc.) where companies, government, and academia can co-create and reuse data and rules.	

4.6 D4-S5 Day #4 PM Opening

Konstantinos Mersinas	コンスタンチノス・メルシーナス
1. The session marks the beginning of the final afternoon of the 15th International Cyber Security Symposium, opened by Professor Konstantinos Mersinas. 2. Professor Mersinas introduces himself as a director at the International Cyber Security Center of Excellence, Associate Professor at Royal Holloway, and visiting professor at Keio University. 3. He highlights that this is the final session after four intense days and congratulates participants for their stamina and engagement. 4. He emphasizes that ending with a discussion on digital identity, attribute attestation, and public trust is highly fitting, as these are foundational to digital interactions. 5. He expresses gratitude to speakers, panelists, and participants, noting the emergence of a strong, global community within the symposium. 6. Throughout the symposium, a recurring theme has been “trust,” whether regarding data sharing, AI, or cross-border frameworks. 7. He presents a key research finding: beyond security and usability, people must trust the intentions of system designers—“convincing transparency” is essential. 8. He warns that even advanced cryptography cannot compensate for perceived bad intentions; trust collapses if users sense misaligned motives. 9. Drawing on the Japanese concept of kokoro, he argues that digital identity systems must combine logic and emotional trust to be effective. 10. He encourages the community to continue	1. このセッションは、第 15 回国際サイバーセキュリティシンポジウムの最終日の午後の始まりを告げるもので、コンスタンティノス・メルシナス教授が開会した。 2. メルシナス教授は、国際サイバーセキュリティ卓越センター所長、ロイヤル・ホロウェイ大学准教授、慶應義塾大学客員教授としての経歴を紹介した。 3. 4 日間にわたる集中的な日程を経て最終セッションを迎えたことを強調し、参加者の粘り強さと熱心な取り組みを称賛した。 4. デジタルアイデンティティ、属性認証、公共の信頼性に関する議論で締めくくることが極めて適切だと強調した。これらはデジタル交流の基盤となる要素だからだ。 5. 講演者、パネリスト、参加者への謝意を表明し、シンポジウム内で強固なグローバルコミュニティが形成されたと述べた。 6. シンポジウム全体を通じ、データ共有、AI、越境フレームワークなどあらゆる場面で「信頼」が繰り返しテーマとなった。 7. 主要な研究結果として、セキュリティや使いやすさを超え、人々がシステム設計者の意図を信頼する必要性を提示。「説得力のある透明性」が不可欠だと結論づけた。 8. 彼は警告する。高度な暗号技術でさえ、悪意の認識を補うことはできない。ユーザーが意図の不一致を感じれば、信頼は崩壊するのだ。 9. 日本の「心（こころ）」という概念を引用し、デジタル ID システムが効果を発揮するには、論理的信頼と感情的信頼を組み合わせる必要があると主張する。 10. 彼はコミュニティに協働の継続を促し、来年の第 16 回シンポジウムを参加者に告知。パスワードと鍵管理に関するユーモアを交えた助言で締めくくった。

collaborating and reminds participants of next year's 16th symposium, closing with humorous advice about passwords and key management.	

4.7 D4-S6 Speech

Vicente NAVARRO (EU Commission, DG CNECT, Policy Officer, Digital Identity and Trust)	ビセンテ・ナバロ（EU 委員会、DG CNECT、政策担当官、デジタルアイデンティティ・トラスト担当）
1. The speaker outlines the EU Digital Identity framework around three pillars: government-backed electronic identification schemes, trusted electronic services (trust services), and the new EU Digital Identity Wallet (EUDI Wallet). 2. Member States must provide citizens with a free EUDI Wallet that works across the EU; use by citizens is voluntary, but wallets must be recognized by public and private services EU-wide and be designed with strong security and privacy under citizen control. 3. The wallet's core functions are: (1) identifying and authenticating users to online or proximity services, (2) storing and selectively sharing identity data and electronic attestations of attributes, and (3) issuing/using qualified electronic signatures at the highest assurance level. 4. Legislatively, the main act has been adopted and over 25 implementing acts are already in place; a few remaining secondary regulations and the full framework are expected to be completed by the end of the year. 5. Technically, an Architectural Reference Framework (latest v2.6) and a reference implementation of the wallet are published (e.g., on GitHub), with a production release including all basic functionalities planned by the end of 2025. 6. Large-scale pilots (LSPs) from 2023–mid-2025, and new pilots running to 2027, test EUDI Wallets in real-life use cases such as travel, mobile ID for registration, payments, business and supply-chain scenarios, and general capabilities; in parallel, a certification scheme and standardization roadmap are being developed.	1. 講演者は EU デジタル ID 枠組みを三つの柱で概説する：政府が支援する電子認証スキーム、信頼できる電子サービス（トラストサービス）、そして新たな EU デジタル ID ウォレット（EUDI ウォレット）である。 2. 加盟国は EU 全域で機能する無料の EUDI ウォレットを市民に提供しなければならない。市民の利用は任意だが、ウォレットは EU 全域の公的・民間サービスで認識され、市民が管理する強固なセキュリティとプライバシー設計が求められる。 3. ウォレットの主要機能は次の通りである：(1) オンラインサービスや近接サービスにおけるユーザーの識別・認証、(2) 身分データ及び属性に関する電子証明の保存・選択的共有、(3) 最高保証レベルでの適格電子署名の発行・使用。 4. 法制面では、基本法が採択され、25 以上の施行規則が既に整備されている。残る二次規制と完全な枠組みは年末までに完成する見込みだ。 5. 技術面では、アーキテクチャ参照フレームワーク（最新版 v2.6）とウォレットの参照実装が公開されている（例：GitHub）。全基本機能を含む本番リリースは 2025 年末までに計画されている。 6. 2023 年から 2025 年半ばまでの大規模パイロット（LSP）および 2027 年まで継続する新規パイロットでは、旅行、登録用モバイル ID、決済、ビジネス・サプライチェーンシナリオ、汎用機能など実生活での EUDI ウォレット運用を検証する。並行して認証スキームと標準化ロードマップが策定中である。 7. 改訂された枠組みは、電子署名・電子印鑑に加え、署名保存、電子アーカイブ、電子書留、遠隔署名生成装置管理、電子台帳利用といった信頼サービスを拡充する。 8. 主要な新規信頼サービスとして、自然人・法人・物体に関する電子属性証明（EAA）の発行・検証が位置付けられる。EAA はウォレットに保存可能で、選択的開示をサポートし、異なる保証レベル（適格 EAA を含む）で存在し、公的機関が真正な情報源から発行した場合、同等の紙文書と同等の法的効力を有する。 9. 属性カタログと検証スキームが定義されつつあり、これにより適格な信頼サービス提供者は権威ある情報源に対して属性を検証し、EU 全域で標準化され相互運用可能な方法で

7. The revised framework extends trust services beyond electronic signatures and seals to include preservation of signatures, electronic archiving, electronic registered delivery, remote signature-creation device management, and use of electronic ledgers. 8. A key new trust service is the issuance and validation of electronic attestations of attributes (EAA) about natural persons, legal entities, or objects; EAAs can be stored in the wallet, support selective disclosure, exist at different assurance levels (including qualified EAAs), and—when issued by public bodies from authentic sources—have the same legal value as equivalent paper documents. 9. Catalogues of attributes and verification schemes are being defined so qualified trust service providers can verify attributes against authoritative sources and issue EAAs in a standardized, interoperable way across the EU. 10. Internationally, the EU is pursuing mutual recognition and technical interoperability for trust services and digital identity with third countries (e.g., Ukraine, Moldova, partners in Africa, Latin America, India, Japan, etc.), including pilots such as wallet-based exchange of academic credentials with Japan, all framed within broader strategic partnerships and validation projects.	EAA を発行できる。 10. 国際的には、EU は第三国（ウクライナ、モルドバ、アフリカ・ラテンアメリカ・インド・日本等のパートナー国を含む）との間で、信頼サービス及びデジタル ID に関する相互承認と技術的相互運用性を追求している。これには日本とのウォレットベースの学歴証明書交換等のパイロット事業も含まれ、全て広範な戦略的パートナーシップ及び検証プロジェクトの枠組み内で進められている。

4.8 D4-P3 Panel

Theme: Digital Identity Wallet, Electronic Attestation of Attributes Moderator: Vicente NAVARRO Panelists: - Satoru Yamadera (Specially Appointed Professor, Saitama University Graduate School of Economics and Management) - Ivan Marin Santamaria (Business Development Manager, GLEIF) - Akira Ito (Project Director, Data Governance PJ, Data & Security Laboratory, Fujitsu Laboratories, Fujitsu Limited) - Hiroshi Nakatake (Senior Director, Keio	テーマ：デジタル・アイデンティティ・ワレット、電子属性証明書 モデレーター：ビセンテ・ナバロ パネリスト： - 山寺 智（埼玉大学経済経営系大学院 特任教授） - イヴァン・マリン・サンタマリア（GLEIF 事業開発マネージャー） - 伊藤 章（富士通株式会社 富士通研究所 データ&セキュリティ研究所 データガバナンス PJ プロジェクトディレクター） - 中武 浩史（慶應義塾大学 SFC 研究所 上席所員, GLEIF Managing Director 日本事務所代表）

University & GLEIF Managing Director)	
1. The panel focuses on how digital identity, electronic attestations of attributes, and verifiable credentials can support trusted online interactions and international cooperation for both citizens and companies. 2. From the Asian development and financial-regulator perspective, Satoru argues that the financial sector must be brought into cybersecurity and digital-identity discussions, because banks already manage KYC/KYB, personal data, and trust, and their rules and infrastructures could be reused—especially in emerging economies. 3. He warns that very strict identity controls (e.g. FATF-driven CDD) are already causing financial exclusion in some developing countries, and suggests leveraging MDBs (like ADB) and finance ministries to fund trust frameworks, strengthen national ID systems, and use global identifiers to keep cross-border payments viable. 4. Marin explains that the Global Legal Entity Identifier Foundation (GLEIF) issues LEIs as global, unique IDs for legal entities, and that LEIs (and VLEIs as verifiable credentials) are being embedded into the EU business wallet to implement KYB, authenticate companies across borders, and support regulated, cross-jurisdictional digital transactions. 5. He notes that LEIs are backed by many regulators worldwide and multiple standards, and that combining the EU wallet architecture with LEIs can help developing countries “inherit” a proven framework and quickly build interoperable, trusted business identification. 6. Ito describes Fujitsu’s work on decentralized data-space architectures, where trust is anchored by enterprise certificates (e.g. DB-Base-ID tied to Japan’s digital agency) and enforced via connectors; he links this to future AI/agent ecosystems that will also depend on distributed trust and trustworthy data exchange. 7. Nakatake highlights Keio–EU collaboration on	1. 本セッションでは、デジタルアイデンティティウォレットと電子属性証明書をテーマに、GLEIF、富士通研究所、慶應SFC などの登壇者が、金融・データスペース・国際連携の観点から議論したセッションである。 2. 冒頭では、多国間開発銀行（ADB など）が進める途上国向け金融支援とサイバーセキュリティ・データ保護の課題が紹介され、日本はデータとサイバーセキュリティの整備で遅れており、信頼できるデータ流通基盤（データスペース）構築が重要であると指摘された。 3. 国際送金や金融取引では、相手方の実在性・適格性を確認する KYC/AML が不可欠だが、途上国の金融機関は信用力や体制の不足からグローバル金融ネットワークから排除されがちであり、MDB が保証人・信頼の媒介として機能している現状が説明された。 4. 金融セクターでは、企業レジストリやコンプライアンス ID と紐づく「Legal Entity Identifier（LEI）」のような法人識別子が鍵であり、ビジネス取引においては個人プライバシーよりも、法人を一意かつ信頼可能に特定する仕組みの方が重要だと整理された。 5. GLEIF 側からは、LEI とそれをベースにした VLEI（Verifiable LEI）により、ウォレット内で検証可能な法人クレデンシャルを発行し、EU 内外でトラステッドなデジタル取引を行う基盤を提供していること、これがトラストルート／トラストネットワークとして各国で活用可能であることが示された。 6. 富士通側からは、データスペースにおける「トラストアンカー」の考え方が説明され、①ハイパースケーラーに ID を集中させるクラウド型モデルと、②各企業が自前システムを持ち、相互に証明書と共通プロトコルで接続する分散モデルを対比し、後者を支える基盤として各国トラストアンカーとその相互承認が不可欠であると述べられた。 7. 日本ではデジタル庁が発行する「gBizID」を、法務省の登記情報と連携した法人 ID として約 800 万超のアカウントに展開しており、これをデータスペースにおける日本側トラストアンカーとして活用する実証（国際相互接続、バッテリーパスポート等）が進められていると報告された。 8. さらに、データスペースで培ったトラストの枠組みを「AI スペース」に拡張し、フェデレーテッドラーニングやマルチエージェント連携においても、AI モデル・エージェントの由来や信頼性をトラストアンカーと国際相互承認で担保していく構想が紹介された。 9. パネルディスカッションでは、まずはサプライチェーン（デジタルプロダクトパスポート、サーキュラーエコノミーなど）や金融といった具体的ユースケースから国際的な ID・データ連携を進

a global digital trust framework, including an ISO proposal for a two-layer “trust list” architecture to enable cross-border mutual recognition of trust anchors, extending the EU wallet model beyond Europe and forming a basis for a global digital trust fund. 8. On the human-resources side, panelists agree there is a worldwide shortage of skilled cybersecurity and digital-identity professionals; proposed responses include mobilizing the relatively well-funded financial sector, using regional IT vendors and MDBs as centers of excellence, and engaging universities to train specialists that emerging countries can tap. 9. In discussing compatibility of schemes like DB-Base-ID with EU trusted lists, they stress that trust ultimately rests on “who you trust” (issuer, country, system), and must be built through equivalent regulations, proven operations, and practical mechanisms such as mutual-recognition or “equivalence” arrangements, mirroring long-standing inter-bank and trade-finance practices. 10. The panel concludes that global data spaces and digital-identity systems are still fragmented silos; achieving a truly trusted global digital environment will require common legal and technical standards, strong involvement of financial institutions, and sustained cooperation among governments, regulators, companies, and international organizations.	め、EU など先行地域で成功事例を作ることで他地域の追随を促すべきだとの意見が示された。 10. 最後に、技術仕様だけでなく、運用・ライセンス・同等性評価・相互承認などの「オペレーションとガバナンス」が決定的に重要であり、各国当局・金融機関・産業界が連携して、誰がコストを負担し、どの国・地域からどのように実装を進めるかを具体化していく必要がある、という点で登壇者の問題意識が共有された。

4.9 D4-S7 Speech

Apostolos APLADAS (EU Commission, DG DIGIT, Head of Sector, International Trust and Identity services)	アポストロス・アプラダス（EU 委員会、DG DIGIT、国際トラストおよびアイデンティティサービス部門責任者）
1. The speaker explains that DG DIGIT’s mission is to turn EU digital-trust policy (from DGs like GROW, CONNECT, SANTE, TAXUD) into interoperable IT systems and infrastructure that serve citizens, businesses, and public administrations. 2. DIGIT operates the European Trust Service Infrastructure, described as the technical	1. 本スピーチでは、欧州委員会における「トラストサービス／電子署名・電子証明書」の国際連携の取り組み、とくに EU と第三国のトラストサービスを接続する「Third Countries Trust Service Programme」の概要が紹介されている。 2. 欧州委員会（DIGIT 等）は、エネルギー・環境など各分野の政策要求を、相互運用可能な IT システム・ソフトウェア・インフラに落とし込む役割を担い、その技術的バックボーンとして「European Trust Services Infrastructure

backbone supporting many everyday use cases (public authorities, ports, airports, hospitals, schools, universities, etc.). 3. Under the new EU Digital Identity Framework, the spearhead is the EU Digital Identity Wallet; to support its business cases, DIGIT must deploy multiple trust entities and trusted lists by the end of 2026. 4. A detailed roadmap is outlined: in Q3 2025 trusted lists for notification providers, wallet providers, wallet relying-party access certificate providers, and age-verification providers (for a "kids' wallet") are or will be in place. 5. By the end of 2025 and into early 2026, additional trusted lists will cover registrars/registers, mobile driving licences, public electronic attestation providers, certified wallet issuers, and a catalogue of attribute schemes, with APIs for submission and notification. 6. This work builds on the past decade's successful EU trusted-list model for services like electronic signatures, sealing and time-stamping, with ongoing investment in updated technical specs to support the new generation of trust services. 7. DIGIT also runs the "Third Countries Trusted List Programme," a structured onboarding process that helps non-EU countries align their trust-service ecosystems (laws, standards, provider lists, certificate profiles, national trusted lists) with the EU model. 8. The programme's workflow includes a self-assessment by the third country, joint gap analysis, design and publication of a national trusted list using ETSI standards, interoperability testing, and final listing of that country's providers/services in a dedicated third-countries EU trusted list. 9. Successful collaborations so far include Ukraine (first fully onboarded), Japan (DFFT-related PoC showcased at the G7), a trilateral EU–India–Japan comparison report on mutual recognition, and Egypt, with more countries	（EU のトラストサービス基盤）」を整備している。 3. 第三国プログラムでは、各国が自国のトラストサービス制度を EU と整合させるためのステップを示した「構造化されたプログラム」を提供し、規制枠組み、標準化状況、トラストサービス提供者の一覧、サイン証明書や署名付き文書のサンプルなどの情報を提出してもらい、EU 側がギャップ分析を行う。 4. その後、ETSI 規格など（例：署名・タイムスタンプ関連規格）に基づき、各国がナショナル・トラストリスト（国家トラストリスト）をどのように構成すべきか、タイムスタンプ証明書をどう位置づけるか等について技術的助言を行い、ナショナル・トラストリストの公開場所や運用方法を整える。 5. 相互の技術検証・相互運用テストが完了すると、第三国側のトラストリストが EU の「参照アドレス」からポイントされる形で登録され、EU 側の検証システムから当該国のトラストサービスが信頼できる形で検証可能になる。 6. 成功事例として、ウクライナが第三国プログラムを完了し、2023 年 11 月に EU の枠組みに正式に組み込まれたこと、日本とは DFFT 文脈での電子署名相互運用 PoC を実施し、2023 年の G7 新潟閣僚声明でもこの成功事例が明示的に言及されたことが紹介された。 7. インドとの二国間協力では、ナショナル・トラストリストの公開につながるパイロットが行われ、エジプトとはその国の電子署名・トラストサービスについてリスク評価・アシュアランスレベルの評価を行い、EU 内で信頼しうるサービスとして示す取り組みが進められている。 8. さらに、エジプト、リトアニア、セルビアなど複数国の電子署名やトラストサービスを例示しつつ、2026 年までに対象国を拡大していく見通しが述べられ、新たにブラジル、ウルグアイ、パナマ、アメリカなどとの協力も進めていることが言及された。 9. 最後に、これらの取り組みは国・地域をまたぐ電子署名・トラストサービスの相互認証を通じて、安全で円滑な国際データ流通を実現することを目的としており、次のパネルディスカッションでこの枠組みをさらに掘り下げて議論することが予告されている。

(e.g. several in Latin America and the Caribbean) now entering the pipeline. 10. DIGIT's strategic vision is a global interoperability framework for electronic trust services: starting from mutual recognition of electronic signatures and extending to broader digital elements, reducing red tape and enabling cross-border trusted digital transactions worldwide.	

4.10 D4-P4 Panel

Theme: Public Trust, ISO (Trusted List) Moderator: Apostolos APLADAS Panelists: - Viky Manaila (President, Cloud Signature Consortium) - Vijayakumar Manjunatha (Asia PKI Consortium) - Jean-Emmanuel Pelaez, Hernandez (eSignature & eID expert Expert) - Akira Nishiyama (Senior Researcher, Keio University) - Satoshi Kai (Project Associate Professor, Keio Global Research Institute)	テーマ：パブリックトラスト、ISO 標準 (Trusted List) モデレーター：アポストロス・アプラダス パネリスト： - ヴィッキー・マナイラ (Cloud Signature Consortium 会長) - ビジャヤクマール・マンジュナータ（アジア PKI コンソーシアム) - ジャン＝エマニュエル・ペレス・エルナンデス (デジタル署名とデジタル ID のエキスパート) - 西山 晃 (慶應義塾大学 SFC 研究所 上席所員) - 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. The panel focuses on "public trust and trusted lists," with speakers from the Cloud Signature Consortium, Asia PKI Consortium, EU experts, and Keio University discussing how to build a global digital-trust ecosystem. 2. Vicky Manaila (Cloud Signature Consortium) praises the EU Third Countries Trusted List (TCTL) Programme as a robust, legally grounded, audited ecosystem rather than "just a list," stressing it enables cross-border verification of digital signatures and requires continuous national supervision and updates. 3. She notes divergences among countries (laws, supervisory regimes, certificate profiles, security devices), and argues that adopting existing international standards directly (rather than re-nationalizing them) is essential for interoperability; she also highlights Cloud Signature Consortium's role and its growing Japanese and global community.	1. 本パネルでは、EU のトラストリストと「Third Countries Trust Service Programme」を軸に、第三国が EU の電子署名・トラストサービス・エコシステムへどう参加し、相互運用性を確保していくかが主要テーマとして議論された。 2. Vicky 氏からは、トラストリストは単なる「リスト」ではなく、法規制・監督・技術基準・プロバイダの継続的なモニタリングを含む非常に複雑なエコシステムであり、第三国プログラムは最終ゴールではなく、その長い道のりの「出発点となるプラットフォーム」に過ぎないという点が強調された。 3. 第三国側が EU トラストリストに参加する背景として、電子商取引や e-ショッピングなど、国境を越えるデジタルトランザクションに自国だけで閉じた仕組みでは対応できず、相手国のトラストサービスを信頼して検証できる枠組みへのニーズが急速に高まっていることが指摘された。 4. EU と各国のトラストサービス制度には、国内法制、監督体制、証明書プロファイル、HSM 等のハードウェアセキュリティ要件などの違いがあり、政治レベルのコミットメントと監督当局への権限付与を含めた調整が必要である一方で、ETSI や ISO など既存の国際標準に沿っていれば「ゼロから別の標準を作り直す必要はない」というメッセージが示された。

4. Jean-Emmanuel Bequesne (e-signature/eID expert) explains that trusted lists already cover multiple trust services (signatures, seals, timestamps, e-delivery, preservation, etc.), and that new services like electronic attestations of attributes (EAA) will increasingly be integrated as key enablers for data free flow with trust. 5. He describes ETSI's evolution from XML-based trusted lists (TS 119 612) toward a generic "list of trusted entities" data model that can be serialized in formats like JSON, but warns that moving away from XML has interoperability and tooling trade-offs and must be carefully assessed. 6. Satoshi Kai (Keio) outlines Japan–EU–India collaboration: a three-layer trust architecture, PoCs where EU and Japanese trust services validate each other's signatures and invoices, demonstrations at G7/G20 events (e.g., carbon-footprint data, DPI use cases), and a joint comparison report/white paper that underpins an ISO proposal for mutual recognition of trust frameworks. 7. Vijay Kumar (Asia PKI Consortium) presents Asia PKI's 20+-year effort to popularize PKI and public trust across more than a dozen Asian countries, using a six-pillar model (law/policy, TSP ecosystem, applications, identity assurance, compliance, technical interoperability) and actively promoting alignment with EU TCTL, ETSI, and ISO to enable cross-border signatures, e-government, trade, IoT, and website trust. 8. He links "public trust" to Digital Public Infrastructure (DPI) such as digital ID, payments, and data-exchange layers, arguing that DPI only becomes globally interoperable when rooted in public-trust mechanisms (trusted lists, standards, audited roots), making trust "portable, auditable, and borderless." 9. Akira Nishiyama (Keio) explains an ISO proposal for an "International Trusted List" (ITL): a two-tier architecture where each country keeps its own domestic TL, and an ITL	5. クラウド署名コンソーシアム（CSC）は、リモート署名等の仕様を ETSI 規格と整合させ、既に欧州規則に取り込まれて実装も進んでおり、日本コミュニティも活発に参加していること、各地域での CSC サミットを通じて政策決定者や事業者がネットワークを作り、標準と運用上の課題を議論する場になっていることが紹介された。 6. EU 側からは、新たな規制やトラストサービスとして、電子配達・電子アーカイブ・電子属性証明（電子的な資格・属性の証明）などのドメインが広がっており、電子 ID／デジタル ID ウォレット領域と組み合わせて、長期検証や越境利用を可能にするための標準化・検証枠組みが重要であると説明された。 7. トラストリストの技術表現については、現在は人間にも読みやすい XML／Excel 的な形式が主流であるが、今後は JSON なども含めた新しい標準への移行が議論されており、検証者が機械的に処理できつつ運用しやすいデータモデルが求められていることが言及された。 8. 日本側からは、トラストサービスを①法制度層、②監査・監督層、③技術ルール層、④トラストリスト表現・相互承認層という四層構造で整理し、2019 年の DFFT 宣言以降、EU と連携した電子インボイス検証デモ、G7 でのカーボンフットプリント証明の相互検証、G20 Global DPI Summit でのパイロット、ホワイトペーパー作成など国際 PoC のタイムラインが紹介された。 9. Asia PKI Consortium からは、アジア各国（日本・インド・韓国・東南アジア諸国等）の政府・民間・認証局・業界団体・研究機関が参加し、「グローバルパブリックトラスト」を目標に、各国当局との MoU や技術パイロット、標準採用支援を進めていること、DPI（デジタル・パブリック・インフラ）においてもトラストリストとルートガバナンスが基盤になるとの見解が示された。 10. 将来像として、G20 や世界銀行が推進する DPI の流れの中で、デジタル ID・決済・データレイヤーを国境を越えて相互運用させるには、各国のトラストサービスとトラストリストを接続した「グローバルに相互運用可能な信頼インフラ」が不可欠であり、その構築に向けて EU・日本・インド・アジア諸国などが協調していく必要があるという点で、パネリストの問題意識が共有された。

lists mutually recognized foreign TLs; relying parties validate domestic certificates via their TL and foreign ones via their ITL entries, accommodating different national approval schemes (e.g., Japan's GPKI, JPKI, healthcare PKI). 10. The moderator closes by emphasising that global, interoperable trust requires common standards, shared tools (like the EU trust-list manager), and ongoing collaboration among governments, industry consortia, and academia to turn fragmented national systems into a coherent, dependable global trust framework.	

4.11 D4-S8 Closing

D4-S8-1 Craig Wiener	D4-S8-1 クレイグ・ウィーナー
1. Craig reflects that the four-day conference demonstrated exceptional depth and breadth across the cyber, IT, and trusted-identity domains. 2. He praises the speakers for their deep expertise and careful, detail-oriented contributions. 3. He commends Keio University and its partners for organizing a highly polished and impactful symposium. 4. He notes that there were too many important moments to recount at this point in the program. 5. He says he will continue reflecting on the discussions for a long time. 6. He expresses hope for ongoing conversations leading into next year's 16th International Symposium on Cybersecurity. 7. He extends MITRE Corporation's sincere gratitude to Keio University and the University Consortium. 8. He thanks all participants for dedicating their time throughout the four-day event. 9. He emphasizes that the work discussed is critical and must continue without interruption.	1. クレイグは、4 日間にわたる会議がサイバー、IT、信頼できるアイデンティティの各分野において並外れた深さと広がりを示したと振り返る。 2. 彼は講演者たちの深い専門知識と、細部にまで気を配った貢献を称賛する。 3. 慶應義塾大学とそのパートナー機関が、非常に洗練され影響力のあるシンポジウムを主催したことを高く評価する。 4. プログラムのこの時点で振り返るには、重要な瞬間が多すぎたと彼は指摘する。 5. 彼は、この議論について今後も長く考え続けると述べた。 6. 彼は、来年の第 16 回国際サイバーセキュリティシンポジウムに向けた継続的な対話を期待すると表明した。 7. 彼は、慶應義塾大学と大学コンソーシアムに対し、MITRE 社の心からの感謝を伝えた。 8. 彼は、4 日間にわたるイベントを通じて時間を割いてくれた全ての参加者に感謝した。 9. 彼は、議論された取り組みが極めて重要であり、中断なく継続されなければならないと強調した。

4.12 D4-S8 Closing

D4-S8-2 Jun Murai	D4-S8-2 村井 純

1. Speaker highlights the strong and substantial content of discussions and speeches throughout the conference. 2. Emphasizes the remarkable fact that 15 embassies supported the event, noting how unusual and significant this is. 3. Notes that many nation states represented in Japan are actively supporting cybersecurity initiatives for the future. 4. States that 2025 is a particularly important year, especially in the post-pandemic context. 5. Observes that digital society has rapidly expanded, with nearly all areas now dependent on digital technologies and infrastructure. 6. Warns that even sectors with no prior exposure to cyber threats are now facing cybersecurity risks. 7. Stresses the importance of sharing experiences and accumulated wisdom to address these emerging challenges. 8. Explains that universities play a vital role in bringing diverse expertise together to collaboratively shape the future. 9. Expresses deep appreciation for participants' active engagement, stating that the conference's success depends on it. 10. Concludes with thanks to all speakers and attendees, along with logistical reminders regarding interpretation receivers, and looks forward to future events.	1. 講演者は会議全体を通じた議論と演説の内容が強力かつ実質的であった点を強調する。 2. 15 の大使館が本イベントを支援した特筆すべき事実を指摘し、これが如何に異例かつ重要であるかを強調する。 3. 日本に代表を置く多くの国家が、将来に向けたサイバーセキュリティ施策を積極的に支援していることを指摘する。 4. 2025 年が特に重要な年であり、パンデミック後の状況において特に重要であると述べる。 5. デジタル社会が急速に拡大し、ほぼ全ての分野がデジタル技術とインフラに依存している現状を観察する。 6. これまでサイバー脅威に晒されたことのない分野でさえ、今やサイバーセキュリティリスクに直面していると警告する。 7. こうした新たな課題に対処するため、経験と蓄積された知見を共有することの重要性を強調する。 8. 大学が多様な専門知識を結集し、協働で未来を形作る上で重要な役割を担うと説明する。 9. 参加者の積極的な関与に深く感謝し、会議の成功はそれに依存すると述べる。 10. 全ての講演者と出席者への謝意を述べ、通訳受信機に関する運営上の注意を付記し、今後のイベントを期待すると結んだ。

Parallel Session

5 Day 2: October 29 | North Building 1F North Hall

5.1 D2-T1-S1 DSA

Moderator: Hiroshi Mano (Executive Director and Secretary General, Data Society Alliance) Panelists: - Sakaino Akira (Director, Evangelist, Smart Industry Office/ Smart City Office, NTT DOCOMO BUSINESS, inc.) - Kenji HIRAMOTO (Senior Executive Officer, Director General of Digital Infrastructure Center, Information Technology Promotion Agency, Japan) - KIKUCHI Naoto (Project Professor, Graduate School of Media Design, Keio University, Vice Chairman, Digital Policy Forum) - Toshikazu YOSHIDA (Board Member, Japan Digital Trust Forum (JDTF))	パネリスト： - 境野 哲 (NTT ドコモビジネス株式会社 スマートインダストリー推進室／スマートシティ推進室 兼務 エバンジェリスト担当部長) - 平本 健二 (上席執行役員 IPA デジタル基盤センター長 AI セーフティインスティテュート副所長、事務局長) - 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、デジタル政策フォーラム代表幹事代理) - 吉田 理重 (一般社団法人 デジタルトラスト協議会（JDTF）理事)

1. DSA が進める「データ取引市場（データトレーディングシステム）」は、売り手と買い手の間に入る中立・公平なインターメディエータ／ノータリー（公証）機能として位置づけられ、単なるマネタイズの場ではなく、信頼の基盤（トラストアンカー）として設計されているという説明である。
2. このデータ取引市場は、IEEE 3800 でアーキテクチャが標準化され、さらに詳細なフレームワークやプロトコル（3800.1）や、データスペース側のオーソリティと連携するためのデータスペース・ディスカバリープロトコルの国際標準化が進められていると紹介された。
3. 日本の「情報銀行」制度は、個人データの信託・対価還元モデルとして検討されたが、インセンティブ設計等が不十分で現在は認定事業者が存在せず、「失敗だった」と総務省が認めた一方、より広い企業データ等を対象とするデータ取引市場モデルが並行して議論されてきた経緯が説明された。
4. データは民法上「無体物」で所有権の扱いが難しいため、「所有権」ではなくデータ利用権として、「何を・誰が・どの目的で・どう使ってよいか」を契約ベースの「権利書」として標準化し、データとバインディングすることで、現行法の枠内で流通と財化を実現しようとしていると述べられた。
5. ノータリー／仲介者が担う役割として、①提供者・受領者が正しい本人・正しい法人であることの確認、②授受データが壊れず・すり替わらず届いていることの保証、③授受されるデータとその利用条件（権利書）が確実に紐付いていることの保証が重要であり、電子署名・タイムスタンプ等の技術を統合したディストリビューションパッケージ（データセット＋権利書＋付帯情報）が重視されていると説明された。
6. JDTF からは、PKI・タイムスタンプ・E シール等の個々の実装を束ねて「トラストフレームワーク」として提供し、データ連携基盤（インターメディエータ）と組み合わせることで、信頼性向上・取引効率化・データ活用拡大を図る構想が紹介され、さらにクマの比喩を使って「信頼できる主体と信頼できない主体を選別する仕組み」の必要性が強調された。
7. デジタル政策フォーラムからは、トラストサービス層（電子署名・E シール・タイムスタンプ等）、データ連携層、アプリ・サービス層の三層構造モデルを前提に、官民データ活用推進基本法の改正や、トラストサービス審査の共通化・横断的認証による負担軽減、EU 等との相互運用性・相互認証を前提とした制度設計の必要性が述べられた。
8. 日本の電子署名法や「認証制度」は、この 20 年以上ほとんどアップデートされず、「誰かに特別な権限を与える制度を作って満足してしまい、インセンティブ設計やデータ利他利用まで踏み込めていない」という反省が示され、EU・米国等と整合的な

ルールづくりと、データスペース前提の再設計が必要だと指摘された。
9. RRI からは、製造業における完全自動化されたマニファクチャリング（ロボット・AI・IoT・ネットワークが国際的にデータを越境交換）のユースケースを想定し、Machine to Machine 通信時に、人間を介さずに相手のハードウェア・ソフトウェア・組織が信頼できるかを機械が判断するための証明書と国際標準ルール（AI のトラスト含む）が不可欠であると説明された。
10. データ流通が進まない要因として、①漏洩・目的外利用への漠然とした不安、②価値評価の相違等による漠然とした不満、③誰がどんなデータを持っているか分からない「発見機会の欠如」、④提供に向けてデータを整備するインセンティブ不足の 4 点が挙げられ、今後は、共通定義を持つデータスペース（自律分散協調のエコシステム）と、そのディスカバリープロトコル、データのライフサイクル・由来情報（プロビナンス）を組み合わせて、信頼に基づく国際的なデータ流通を実現していく必要があるとまとめられた。

5.2 D2-T1-S2 RRI

Title: What are the Trust and Trustworthiness needed for the future of manufacturing? — Value creation in supply chains connected by data Moderator: FURUKAWA Ayaji (Member,Affiliation Robot Revolution & Industrial IoT initiative Industrial Trustworthiness &Security Action Group) Panelists: - Fumikado Anzai (Engineering Manager ,MITSUBISHI HEAVY INDUSTRIES, LTD. Digital Innovation HQ. EPI Department) - Takashi Ogura (Senior Researcher ,Hitachi, Ltd. Research & Development Group, Mobility & Automation Innovation Center, Autonomous Control Research Department) - Takeshi Kawabata (Senior Manager ,Toshiba Corporate Laboratory AI Digital R&D Center Security Research Dept.) - Hirozumi Eki (Chief Technical Architect ,ARGO GRAPHICS Inc. ALM Business Promotion Division) - MAHARA Kumiko (Senior Manager,Sony Semiconductor Solutions Corporation IS Business Strategy Department)	タイトル：製造業の未来に必要な Trust と Trustworthiness とは？ — データが繋ぐサプライチェーンの価値創出 モデレータ：古川 文路（ロボット革命・産業 IoT イニシアティブ協議会 Industrial Trustworthiness &Security Action Group 委員） パネリスト： - 安西 史圭（三菱重工業株式会社 デジタルイノベーション本部 EPI 部 主席） - 小倉 貴志（日立製作所 研究開発グループ モビリティ&オートメーションイノベーションセンタ 自律制御研究部 研究員） - 川端 健（(株)東芝 総合研究所 AI デジタル R&D センターセキュリティ基盤研究部 シニアマネージャー ） - 益 啓純（株式会社アルゴグラフィックス ALM ビジネス推進統括部 チーフ・テクニカル・アーキテクト） - 馬原 久美子（ソニーセミコンダクタソリューションズ株式会社 IS 事業部 シニア CIS エンジニア）

1. 本セッションは、製造業のサプライチェーン／バリューチェーンで流通する「製品関連データ（PRD）」のトラストとトラストワースネスをどう確保し、価値創出につなげるかを、日本の製造業とドイツの Plattform Industrie 4.0 との共同検討として紹介するものである。
2. 欧州ではデジタルプロダクトパスポート（DPP）や Gaia-X／Catena-X などデータスペースの取り組みが進み、CO_2排出量や調達源など、従来共有しなかった製品情報をサプライチェーン全体で共有することが求められており、その中でデータの信頼性確保が重要課題となっている。
3. トラスト基盤とは、企業同士が安心してデータをやり取りするための技術・ルールの仕組みであり、EU では eIDAS の下で電子署名・電子シール等のトラストサービスが定義され、日本でも総務省の電子証明書・タイムスタンプ等により、越境データ

連携を支える共通土台づくりが進んでいる。
4. その技術的な土台は公開鍵暗号と PKI であり、電子証明書は「デジタルな印鑑登録証明書」として、鍵の持ち主と正当性を保証し、電子署名によりデータの改ざん防止と送信者本人性の確認を可能にすることで、サプライチェーン全体のデータトラストを支えると整理されている。
5. 「トラスト」は信じる／信じないという 0/1 の概念であるのに対し、「トラストワースネス」は相手がどの程度の能力・統制を持っているかというケイパビリティの概念であり、事業者間で TWE（期待：Expectation）と TWC（能力：Capability）を双方向にやり取りしながらネゴシエーションすることが重要だと説明された。
6. 製品関連データ（PRD）のトラストワースネスについては、CO_2排出量などの例を用いながら、①ユースケース・目的、②データ流通手段（データスペース等）、③提供者側・利用者側の管理方法、④データ生成プロセス、⑤製品との紐づけ、⑥保管・管理、⑦ネットワーク上での提供、⑧利用者による適切な利用、といった観点で期待値とケイパビリティを整理し、CPSF の 3 層構造にマッピングして検討している。
7. これら 8 項目のうち、とくにデータ流通基盤（⑤～⑦付近）やアクターのアイデンティティの確認には、トラストサービス／トラスト基盤が有効であり、政府をトラストアンカーとする枠組みを組み合わせることで、データスペース上のやり取りをより効率的かつ検証可能にできるとされた。
8. サプライヤー視点では、従来のような直接取引先との NDA 前提の関係にとどまらず、データスペース経由で「お客様のさらにお客様」からも検証可能な形でトラストワースネスを示す必要が生じ、多様な粒度のデータと証拠を用意しつつ、TWE／TWC の仕組みを共通化することで、コストエフェクティブな対応を図るべきだと議論された。
9. 将来的にマシン・トゥ・マシン取引や AI による自動ネゴシエーションが期待される一方、現時点では AI の信頼性が十分確立していないため、人間による検証を交えつつ、上記 1～8 の観点に基づくトラストワースネス評価を積み上げていく段階にあると位置づけられた。
10. 目指す世界として、データ提供者の条件から逸脱しないデータ利用（二次利用・三次利用を含む）を技術・運用・マネジメントで保証し、経済安全保障（輸出規制データの越境防止など）や国家安全保障（データの鮮度・有効期限の管理）も踏まえたデータ流通社会を官民連携で実現すること、そのための国際標準化や EU 規制へのインプットを、日本とドイツの連携のもと RRI が推進していくことが強調された。

5.3 D2-T2-S1 The Japan Institute for Cyberspace Studies (JICSS)

The Japan Institute for Cyberspace Studies (JICSS) Title: Stakeholder Engagements: How Cybersecurity and Resilience Make Japan's OT Sector Globally Competitive Moderator: Gloria Glaubman (Founder of GMG Consulting and JICSS Special Advisor) Panelists: - James Miller English Session (no Japanese)	タイトル：ステークホルダー・エンゲージメント：サイバーセキュリティとレジリエンスが日本の OT セクターの国際競争力を高める モデレータ：グロリア・グラウブマン（GMG コンサルティング創設者、JICSS 特別顧問） パネリスト： - ジェームス・ミラー 英語セッション(日本語なし)

1. The moderator frames the discussion around differences between IT and operational technology (OT) lifecycles, highlighting that OT systems may run for 50 years and require strategies that balance operational continuity, transformation, security, and resilience.
2. Gloria describes a shift in Japan’s policy conversation from specific technologies or sectors toward broader cyber and business resilience, emphasizing modernization of data management, national security structures, and the private sector rather than “religious” debates about domestic

vs. global cloud.
3. On prioritization, she warns that “everything can’t be number one” and recommends focusing first on lifeline critical infrastructure sectors (water, communications, transportation) and national security, driven both by domestic needs and external pressure from allies who must be able to trust Japan with sensitive information.
4. Drawing lessons from Ukraine, they stress the need to maintain continuity of government and financial services during crises, support citizen mobility (e.g., remote schooling, online banking), and use secure, hyperscale-capable cloud infrastructures to ensure resilient access to digital services from anywhere.
5. They argue that Japan should leverage existing international standards and frameworks (e.g., ISMAP/FedRAMP-like approaches) instead of reinventing the wheel, including reciprocity with like-minded countries and a whole-of-government model that can set and enforce cybersecurity baselines across ministries and agencies.
6. The discussion highlights serious gaps in logging and threat intelligence in Japanese organizations: many do not retain logs long enough or detect incidents themselves, which makes Japan “fertile ground” for adversaries to test new zero-days, and underscores the need for better collection, information sharing (e.g., ISAC-like models), and safe-harbor protections for industry.
7. As a “leapfrog” opportunity, Gloria points to AI-driven security operations (e.g., AI in SOC/SIEM) that can rapidly analyze huge volumes of alerts and logs, with humans in the loop, supported by cloud or high-performance infrastructure—moving security to the API/data layer and making better use of telemetry.
8. They link security transformation with broader digital and economic transformation: data is described as “king” and trust as “queen” in a zero-trust world, where granular visibility, observability, certifications, and industry-defined baselines all contribute to trusted digital services and Japan’s competitiveness (e.g., finance, AML, transportation).
9. The panel underscores the importance of public-private collaboration: sector-by-sector approaches, industry-led groups, and government-led initiatives (such as the reimagined National Cyber Security Office) must coexist, with industry having a strong voice in shaping regulations, sharing lessons learned, and avoiding harmful or impractical rules.
10. They conclude that Japan has a real chance to leapfrog by learning from allies’ experiences, strengthening sector-specific and cross-sector collaboration, and aligning security, resilience, and economic revitalization—creating a ripple effect once a few sectors and companies show tangible benefits.

5.4 D2-T1-S3 JDTF

Title: Promoting digitalization of Public Notices Moderator: Naoki Ushijima (GMO GlobalSign Holdings K.K., General Manager) Panelists: - Masamitsu Kimura (SKYCOM Corporation, Executive Office) - Tetsuro Kubota (CIO Adviser at Fukuyama-city and Manazuru-town) - Daisuke Chiba (Digital Government Labs,	タイトル： 処分通知のデジタル化推進 モデレータ：牛島 直紀 (GMO グローバルサイン・ホールディングス株式会社 GMO サイン事業部 部長) パネリスト： - 木村 正光 (株式会社スカイコム 執行役員) - 窪田 哲郎 (福山市 CIO 補佐官、真鶴町 CIO 補佐官) - 千葉 大右 (Digital Government Labs 代表理事、裾野市 CIO 補佐官)

President and CIO Adviser at Susono-city)	
1. 処分通知のデジタル化は旧オンライン化法以来制度上は存在したが、長らく進展せず、コロナ禍とデジタル改革によりようやく本格的なスタートラインに立ったと評価されている。 2. 自治体の電子証明書利用は増加している一方で、全体としての普及率は依然として伸び悩んでいるとの指摘があった。 3. 業務システムの標準化においては、署名機能など共通機能を外部化し疎結合にすることが基本方針で、類似機能を各システムが個別に持つべきではないとされた。 4. GPKI／LGPKI は安全性が高く、現場の安心感につながっている一方で、IC カードや USB トークンの PIN 入力など運用上の負担が大きい課題も存在する。 5. 電子申請の着手順序として、自治体には約 6,000 の手続があるが、利用の多い上位 100 件で全体の約 98%を占めるため、優先順で取り組むことが合理的であるという意見が共有された。 6. 電子化を推進する上で、自治体職員の「新しい取り組みが苦手」な文化や、担当者任せで孤立しやすい組織構造が大きな障壁となっていると指摘された。 7. 組織的に進めるには、担当者の孤立を防ぎ、上司を巻き込みながら“チームとして進める体制”が不可欠だという課題認識が示された。 8. 総務省が毎年公表する「実際の DX・情報化推進状況」では、国民利便性の向上に資する 26 手続について進捗が明らかになっており、多くは依然として電子化率が低い現状にあるとされた。 9. 電子化の遅れを踏まえ、デジタル化を阻む要因の整理と、二重トラック（段階的並行アプローチ）の必要性が議論された。 10. 全体として、処分通知・行政手続の電子化は一定の前進があるものの、制度・技術・運用・文化面で多くの課題が残っており、一層の改善が求められるとの総括で締めくくられた。	

5.5 D2-T1-S4 CyLogic

Title: True Sovereign Cloud for Japan: From challenges to practical solutions Speaker: Chris Grady (CTO, CyLogic Inc.) English Session (no Japanese)	タイトル：日本にとっての真のソブリン・クラウド： 課題から現実的な解決策へ スピーカ：クリス・グラディ（CyLogic 社 CTO） 英語セッション(日本語なし)
1. The speaker runs an informal, small-audience session aimed at people new to cloud and cybersecurity in Japan, including a reporter covering the cyber policy beat. 2. His company has worked with Japanese firms since around 2018 to introduce a FedRAMP-like security and compliance program and a “sovereign cloud” for Japan, with strong backing from Admiral Dennis Blair and FedRAMP’s first director, Maria Roat. 3. Their mission is to protect critical infrastructure in the U.S. and partner countries through secure, sovereign cloud solutions, assuming many Japanese stakeholders still lack basic familiarity with cloud concepts like Amazon, virtual machines, and zero trust. 4. He defines sovereign cloud as full local control over data, applications, and infrastructure, compliance with domestic laws and regulations, strict data residency, operational independence from foreign nationals, and—extended in their model—100% self-containment with no external service dependencies and a validated, tamper-evident supply chain built on COTS and open standards. 5. He explains SaaS, PaaS, and IaaS as an inheritance stack and positions CyCloud as a FedRAMP High-aligned IaaS provider with integrated VDI, backup and disaster recovery, zero-trust access, and AI-ready workloads, arguing that many Japanese ministries and defense organizations need full visibility “under the hood” rather than SaaS black boxes. 6. The JRAMP cloud prototype duplicated their FedRAMP High-ready infrastructure in Ashburn,	

Virginia, deployed a service-delivery layer in Tokyo data centers, and connected them via private Equinix carrier links (not the public Internet), demonstrating rapid, high-throughput, highly available trans-Pacific connectivity.
7. He criticizes hyperscalers as centralized “big targets” and expensive for data movement, noting that most East Coast U.S. traffic traverses Equinix campuses; by operating inside this ecosystem, CyCloud can offer strong performance while remaining decentralized and sovereign for Japan.
8. A detailed zero-trust network access demo contrasts legacy VPNs (over-provisioned, trust-once, IP/port management) with their model: a client sends a single packet to a non-responsive controller, identity is verified, a per-user “micro-firewall” with fine-grained policy is spun up, resources appear only while authorized, posture is continuously evaluated, and the firewall is destroyed on logout, leaving no exposed attack surface.
9. He shows the internal management layer (PKI, DNS, NOC/SOC, ticketing, backup, monitoring) as a closed, Internet-isolated environment and demonstrates how hardened VM templates and virtual desktops can be provisioned in ~90 seconds, plus integrated backup/DR that can restore individual files, AD objects, containers, or an entire region (about 150 VMs) to meet strict RTO/RPO and FedRAMP High requirements.
10. Strategically, he argues that AI workloads are pushing the “cloud model” (self-service, rapid provisioning) back to the edge and on-prem so compute can sit near data; CyCloud aims to deliver a VMware-based, hyperscale-capable but decentralized, FedRAMP-High-ready sovereign cloud for Japan first, with no plans to expand to other countries until that mission is accomplished.

5.6 D2-T1-S5 CyLogic

Title: True Sovereign Cloud for Japan: panel discussion and technical demonstration Moderator: Yogev Moyal (COO, CyLogic Inc.) Panelists: - Maria Roat (the first Director of the FedRAMP program in the U.S. and the former U.S. Deputy Federal Chief Information Officer) - Louis Mayberg (CEO, CyLogic Inc.) - Chris Grady English Session (no Japanese)	タイトル：日本における真のソブリン・クラウド：パネルディスカッションと技術デモンストレーション モデレータ：ヨーゲフ・モイヤル（CyLogic 社 COO） パネリスト： - マリア・ロート（米国における FedRAMP プログラムの初代ディレクター、元連邦最高情報責任者代理） - ルイス・メイバーグ（CyLogic 社 CEO） - クリス・グラディ 英語セッション(日本語なし)

1. The speaker emphasizes CyLogic’s mission to secure U.S. and allied critical infrastructure through highly secure sovereign cloud solutions and frames the talk around real operational demonstrations rather than theory alone.
2. He stresses that all CyLogic systems are built to FedRAMP High standards, noting his long personal history with FedRAMP since 2012 and explaining that even countries without FedRAMP still need equivalent high-security compliance.
3. He outlines a comprehensive definition of “sovereignty,” including full national control of data, infrastructure, operations, personnel, geographic boundaries, and complete independence from foreign control planes or external services.
4. CyCloud is described as a fully self-contained sovereign cloud: no external DNS, identity, logging, or update services; validated end-to-end security; tamper-evident supply chain; and no foreign-

national operational dependency.
5. He contrasts SaaS, PaaS, IaaS, and a proposed “full sovereign cloud,” emphasizing that sovereignty requires 100% visibility and control over infrastructure and operational processes, not just applications.
6. He explains how FedRAMP compliance is 20% technical and 80% operational maturity—who operates, monitors, and secures the cloud—and describes the FedRAMP management layer vs. service delivery layer used in J-RAMP deployments.
7. A major theme is decentralization: he argues that hyperscalers are centralized “single targets,” whereas CyCloud is designed for distributed, edge/on-prem architectures, supporting AI workloads close to data sources.
8. He demonstrates zero-trust network access using single-packet authorization, cloaking, dynamic micro-firewalls per user, and entitlement-based access, contrasting this with insecure legacy VPN models.
9. Multiple live demos illustrate rapid VM provisioning (under 90 seconds), virtual desktop infrastructure, integrated backup/DR, forensic search, and micro-segmentation—showing concrete cloud operations “under the hood.”
10. He concludes with the JRAMP example: deploying the FedRAMP management layer in Virginia and service layer in Tokyo, linking them via private trans-Pacific connectivity, demonstrating decentralized sovereign cloud capability for Japan.

6 Day 3: October 30 | North Building 1F North Hall

6.1 D3-T1-S1 UNIDIR RAISE

Title: Responsible AI by public private partnership with UNIDIR RAISE (Roundtable for AI, Security & Ethics) Moderator: Tom Kono (Fellow, UNIDIR) Panelists: - Yasmin Afina (Researcher, Security and Technology Programme, UNIDIR) - Michael Karimian (Director, Digital Diplomacy, Microsoft) - Kazuo Noguchi (Senior Researcher, Keio University) - Atsushi Ikegami (Senior Research Fellow, National Security Institute of Fujitsu Defense & National Security) English Session (no Japanese)	タイトル：責任ある AI を UNIDIR RIASE (Roundtable for AI, Security & Ethics) とともに産官学連携を目指し モデレータ：河野 勉（国際連合軍縮研究所（UNIDIR）フェロー） パネリスト： - 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） - 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） - 野口 和男（慶應義塾大学上席所員） - 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） 英語セッション(日本語なし)
1. The session introduces UNIDIR's Roundtable for AI Security and Ethics (RAISE) as a neutral, multi-stakeholder forum involving states, military actors, industry, civil society, and academia, aiming to catalyze action and bridge AI ethics with security, especially in national security contexts. 2. RAISE has already produced a global conference, regional consultations, and a Bellagio meeting, and it is launching additional projects including a framework for responsible industry behavior in the military use of AI, grounded in international law and intended for practical implementation. 3. Microsoft's perspective highlights a significant gap between responsible AI progress in the civilian domain and in national security. Multi-stakeholder dialogue is considered urgent to interpret and apply international norms and law to military AI before geopolitical tensions limit cooperation. 4. From a UN diplomacy perspective, AI is addressed in fragmented tracks: military issues in First Committee and CCW, civilian and socio-economic issues in Second and Third Committees and agencies such as WHO, ILO, and ITU. New mechanisms such as the Pact for the Future and the Global Digital Compact seek to improve coherence in global AI governance. 5. Japan's policy context includes an emerging active cyber defense model and constitutional constraints on offensive operations. Within this framework, the Ministry of Defense has issued Responsible AI Guidelines requiring compliance with international and domestic law, prohibiting fully autonomous lethal weapons without human involvement, and establishing risk classification, early legal and policy review, and technical reviews throughout development. 6. From the defense industry viewpoint in Japan, warfare is rapidly shifting toward uncrewed, autonomous, and AI-enabled systems. AI-driven C4ISR accelerates the OODA loop, and in Japan's regional environment, responsible AI is seen as a strategic requirement for deterrence, crisis stability, and alliance interoperability. 7. Japan's priorities include updating doctrine as technology evolves, building secure and interoperable cyber and data infrastructures, institutionalizing continuous testing and lifecycle oversight, and creating formal public-private and private-to-private collaboration mechanisms so	

MOD and industry can jointly operationalize responsible AI.
8. RAISE's Bellagio discussions identified six priority themes for military AI governance: capacity building, trust building among states and stakeholders and humans with technology, clarification of the human element, data governance, lifecycle management, and addressing destabilizing effects such as proliferation, disinformation, and hybrid threats.
9. The planned UNIDIR framework for responsible industry behavior in military AI will include four core elements: policy commitments, due diligence processes, transparency practices, and accountability or remedy measures. It is intended to provide a common baseline for governments and industry and will be developed through global consultations.
10. In the concluding remarks, participants emphasize that AI in defense will become widespread globally, including in the Global South. Effective governance requires an international epistemic community connecting UN processes, governments, industry, and academia. Japan's emerging practices on responsible defense AI should contribute to and be reinforced by efforts such as RAISE and the REAIM summit.

Conducted in North Building 3F Large Meeting Room

6.2 D3-T1-S2 Defense Technology Foundation (DTF)

Title: Integration of cutting-edge technologies, primarily from startups in the defense sector, and the Risk Management Framework Moderator: Hideaki WATANABE (Chairman, Defense Technology Foundation, The 1ST commissionner of Acquisition, Technology and Logistic Agency) Panelists: - Yoshihito Watanabe (Deputy Chairman / Managing Director of Defense Technology Foundation) - Yoshihiro Sawada (Director, Japan Aerospace & Defense Consulting Inc.) - Manabu Koike (Executive Officer and Section Manager of Consulting Unit, Japan Aerospace & Defense Consulting Inc.) - Ryu Kanno (Manager of External Affairs Office, Japan Aerospace & Defense Consulting Inc.)	タイトル：防衛分野でのスタートアップを中心とする先端技術の取り込みと Risk Management Framework について モデレータ：渡辺 秀明（一般財団法人 防衛技術協会 理事長、初代防衛装備庁長官） パネリスト： - 渡邉 芳人（一般財団法人 防衛技術協会 常務理事） - 澤田 栄浩（株式会社 Japan Aerospace & Defense Consulting 取締役） - 小池 学（株式会社 Japan Aerospace & Defense Consulting 執行役員兼コンサルティング部部長） - 菅野 隆（株式会社 Japan Aerospace & Defense Consulting 渉外室長）

1．防衛技術協会の「先端技術研究会」は、防衛装備庁や経産省からの委託による技術動向調査、研究部会（水中兵器・無人機等）と海外展示会調査、報告会の開催などを通じて、防衛技術の情報収集・共有を継続的に行っている団体である。
2．同研究会は、大手防衛産業だけでなくスタートアップや中小企業の優れた技術を防衛分野に取り込むことを目的とし、約40 社の法人会員とともにマッチングイベントや展示会を開催し、防衛参入を支援している。
3．ジャパン・エアロスペース＆ディフェンス・コンサルティング（JDC）は、SHIFT 社の防衛専門子会社として設立された新しいコンサル会社であり、ソフトウェアテストを強みとする親会社の基盤の上に、RMF（Risk Management Framework）を中核としたリスクマネジメント支援を展開している。
4．RMF は、2002 年の FISMA 制定と NIST SP800 シリーズ（特に 37・53）の整備を背景に、2014 年に米 DOD で

本格導入された認証・認可プロセスであり、2018 年には連邦政府に限らず重要情報を扱う産業界にも適用範囲が広がり、2022 年改定の DODI 8510.01 では武器システムにも対象が拡大されたフレームワークである。
5. 日本では、防衛省が令和 5 年に情報システムと装備品の両方に RMF を適用する方針を打ち出し、令和 9 年度までに既存システムの再承認と新規システムへの適用を進めるため、毎年数百億円規模の予算を投入しているが、対象装備品が膨大で手続きも極めて煩雑であり、完了の困難さが指摘されている。
6. RMF はリスク分析に基づくセキュリティ方針策定・実装・継続的モニタリング・将来対応計画までを含む包括的プロセスであり、最大 1000 項目近い管理策と膨大な文書作成が必要となるため、経験のないベンダーや装備品メーカーにとっては負荷が大きく、形式的な書類対応に偏り、本質的なセキュリティ向上につながりにくいという課題がある。
7. 日本のサイバーセキュリティ基準は、サイバーセキュリティ基本法、政府統一基準、重要インフラ WG、ISMAP 等が ISMS・ENISA・NIST SP800-53 などを寄せ集めた「ミックス状態」となっており、米国のような RMF を軸とした一貫した体系に比べて統一性・整合性が欠けているため、RMF 型の枠組みに揃えていく必要性が強調されている。
8. RMF はゼロトラストとコンティニュアスモニタリングを土台とする枠組みであり、政府クラウドや重要インフラを守るための基盤となるが、日本では防衛省以外の省庁や重要インフラ事業者への展開が遅れており、能動的サイバー防御の法整備だけ先行すると、土台の弱さゆえに国際的なインテリジェンス共有や同盟国からの信頼を得られないという懸念が示されている。
9. 米国では CNSS による国家安全保障システム向けオーバーレイや、空軍発の「Platform One」によるホワイトボックス型の脆弱性管理・DevSecOps 基盤が整備されている一方、日本はブラックボックス検査の結果に追われる「いたちごっこ」から抜け出せておらず、脆弱性管理と RMF 実装の両面で大きなギャップがあると指摘されている。
10. こうした状況を踏まえ、JDC は RMF 入門（2 日間）から、1 か月程度のリスク分析・セキュリティ計画書作成コース、今後のモニタリング・将来対応計画、上級者向けコースまで段階的な教育プログラムを提供し、防衛省・装備品メーカー・IT ベンダーにおける RMF 人材を育成して、長期的には日本全体の RMF 運用能力を底上げしていく必要があると述べている。

6.3 D3-T1-S3 InfoKeyVault Technology / WiSECURE Technologies Corporation

Title: Now it's the time for PQC Migration Speaker: Albert Cheng (CEO, InfoKeyVault Technology Co., Ltd.) Agenda: - Why PQC - The standardization status of PQC - The requirement of PQC Migration - The challenges of PQC Migration English Session (no Japanese)	タイトル：今こそ PQC マイグレーションの時 スピーカ：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 代表取締役社長） アジェンダ： - PQC 導入の必要性 - PQC の標準化状況 - PQC 移行の要件 - PQC 移行における課題 英語セッション(日本語なし)

1. The speaker introduces himself (Albert from WiSecure Technology, Taiwan), explains his company's HSM products, and frames the session as an introduction to PQC and PQC migration.
2. He explains why quantum computing threatens existing public-key cryptography, referencing Shor's algorithm and predicted timelines for "Q-Day" from Microsoft, Gartner, NIST, BSI, Fuji, and others.
3. He emphasizes the "harvest-now, decrypt-later (HNDL)" threat, noting that encrypted data stolen today may be decrypted once quantum computers mature.
4. He highlights how deeply PKC is embedded in everyday systems—2FA, MyNumber cards, smart grids, payment systems, cryptocurrency, mobile app integrity, and more.
5. He introduces Mosca's Theorem, explaining the relationship between quantum maturity (Z), system migration time (Y), and data shelf life (X), stressing urgency for PQC migration.
6. He summarizes PQC standardization status: ML-KEM and ML-DSA (lattice-based), HQC (code-

based), and hash-based signatures (SPHINCS+, LMS, XMSS), explaining their roles in signatures and key encapsulation.
7. He discusses use-case categories and timelines from CNSA 2.0, showing when PQC adoption becomes recommended or mandatory for software signing, web/cloud communications, devices, and niche systems.
8. He describes migration challenges: complexity of PQC algorithms, large key sizes, legacy systems incompatible with PQC, uncertainty about how many systems use PKC, and legal/regulatory ambiguity.
9. He recommends hybrid approaches combining PQC and classical algorithms to ensure interoperability during transition; outlines discovery processes, cryptographic inventory, and automation tools for identifying vulnerable systems.
10. He concludes with strategic recommendations: global collaboration, raising industry awareness, sector-specific best-practice development, Taiwan's policy example, and a call for organizations to prepare budgets, expertise, and plans for PQC migration.

6.4 D3-T1-S4 JCIC

Title: No More "By Mistake" and "Should Be OK" Moderator: Toshinori Kajiura (JCIC President) Speakers: - Masahiro Sawada (JCIC Visiting Fellow) - Toshihiro Hirayama (JCIC Visiting Fellow; Professor of iU)	タイトル：「うっかり」、「まあ大丈夫だろう」を潰せ モデレータ：梶浦 敏範（JCIC 代表理事 兼 上席研究員） スピーカー： - 澤田 雅広（JCIC 客員研究員） - 平山 敏弘（JCIC 客員研究員、情報経営イノベーション専門職大学(iU)教授）

1．本セッションのテーマは「うっかり・まあ大丈夫だろうを潰す」であり、最近のランサム被害（ランドローバー、アサヒビール、アスクル等）に見られるように、VPN 脆弱性や AD 乗っ取りなど「基本対策の怠り」で防げたはずのインシデントが多いという問題意識が提示された。
2．JCIC は技術シンクタンクではなく、経営・マネジメント視点からサイバーセキュリティ政策や普及策を提言する組織であり、サイバーはもはや CIO/CISO 任せの技術課題ではなく「経営課題」であることが強調された。
3．最大の脆弱性はシステムではなく人間にあり、従業員一人ひとりの意識低下・うっかりミス・「自分の仕事は関係ない」という思い込みが侵入の入口になるため、IT ガバナンスと「サイバーハイジーン（うがい・手洗いに相当する基本行動）」の徹底が重要とされた。
4．社員向けには、標的型メール訓練などで「20%はクリックしてしまう」という現実を踏まえつつ、クリックさせない教育だけでなく「開いてしまったときに報告・記録・保全をどう行うか」を訓練することが、被害拡大を防ぐうえで不可欠と説明された。
5．平山氏は、PC やスマホを使う一般の 1 日の行動（通勤・食事・SNS 等）の裏側に多くの脅威が存在することを、Wi-Fi のパケット可視化やフリーWi-Fi＝「公道」、4G/5G＝「私道」という比喩、海外旅行時の注意喚起との比較などで「見える化」し、自分ごと化を促していると紹介した。
6．「プラスセキュリティ人材」とは、ハッカーのような専門家ではなく、本業（事業・サービス）に加えてセキュリティ知識を持つ人材を指し、個人の知識向上が「重要情報×脅威×脆弱性」というリスク式のうち、脆弱性を減らし、組織全体のリスク低減につながるという位置づけが示された。
7．組織対策としては、退職予定者の権限制限など「機会を減らす」統制、公認不正検査士がいう不正の三要素（動機・機会・正当化）への対応、人事異動の少ない閉鎖組織や海外子会社など「管理の目が届きにくい領域」を減らす工夫、ポップアップやダブルチェックなどうっかり対策、対話型研修や模擬記者会見・再現ビデオによる「痛みを伴う疑似体験」でリスク感度を上げることが有効とされた。
8．個人のリテラシー醸成には、一般論や遠い大企業の事例だけでなく、「隣の店・同じ町の中小企業」など身近なインシデン

トや、実際にフィッシングを受けた・被害にあった経験を共有してもらうことで、セキュリティを「自分ごと」として捉えさせることが重要であると議論された。
9. 社会全体の「大きな傘」として、日本の能動的サイバー防御（有害サーバの無害化等）や英国の先行事例、Gmail がスパムの 99.9%を自動で弾く仕組みなどが紹介され、企業レベルでは経営者によるサイバーセキュリティ経営宣言、国レベルでは NISC/国家サイバー統括室による人材フレームワーク整備や「セキュリティ版 IT パスポート」的な資格制度等を通じて、人材を正しく評価しエコシステムをつくる必要性が指摘された。
10. 質疑では、英国やビッグテックが進んでいる理由として、英国の長い諜報文化と情報収集への価値観、ビッグテックが世界で最も攻撃されることでノウハウを蓄積している点が挙げられたうえで、日本も制度整備と人材育成により追いつくべきとされた。
最後に、沢田氏は「圧倒的な当事者意識」、平山氏は「自分ごと」、梶浦氏は「リスクマネジメント」をキーワードとして、個人・組織・国家レベルでのサイバーセキュリティ向上を呼びかけて締めくくられた。

6.5 D3-T1-S5 Keio University Global Research Institute, Cyber Civilization Research Center (CCRC)

Title: Home Appliance Open Innovation Workshop: Activity report on the international deployment of the open-standard protocol “ECHONET Lite” and Distributed Energy Resource Aggregation Business “ERAB” Moderator: Maaski Umejima (Project Professor, Cyber Civilization Research Center, Keio University) Panelists: - Akinori Kahata (Deputy Director of Natural Resources and Energy Agency, Ministry of Economy, Trade and Industry, Japan) - Hiroshige Muraoka (President, Nomura Research Institute of Singapore) - Masato Nagasawa (Director, Echonet Consortium)	タイトル：ホームアプライアンス・オープンイノベーションワークショップ: 公知な標準プロトコル ECHONET Lite と ERAB の海外展開の最新 モデレータ：梅嶋真樹 (慶應義塾大学サイバー文明研究センター、特任教授) パネリスト： - 加畑 晶規 (資源エネルギー庁 課長補佐) - 村岡 洋成 (野村総研シンガポール 社長) - 長沢 雅人 (一般社団法人 エコーネットコンソーシアム普及委員会委員長)

1. 本セッションは「慶應義塾大学サイバーセキュリティ国際シンポジウム 2025」のパラレルセッションとして、第 9 回 ECHONET Lite・ワークショップを兼ね、ECHONET Lite およびアグリゲーションシステム（ERAB）の国際展開、特に ASEAN 展開とサイバーセキュリティをテーマとして開催されたものである。
2. 梅島氏は、IEC におけるスマートエネルギー関連国際規格（SRD 63443）開発のリーダーとして、日本の ERAB アグリゲーションモデルをベースにした国際標準化が最終投票段階にあることを紹介し、その成功要因として「分散電源の共通言語」「スマートメーターによる透明性」「サイバーセキュリティ」の 3 点を強調した。
3. ECHONET Lite は Matter や EEBUS と並ぶオープンなインターフェースとして位置付けられ、IEC 14543-4-3 として標準化されているほか、次世代スマートメーターでは Wi-Fi 経由で 1 分単位の電力データにほぼリアルタイムでアクセスできる仕組みを 2026 年から運用開始予定であり、これも国際規格化を狙っていると説明された。
4. 日本では CPSF（サイバーフィジカルセキュリティフレームワーク）を頂点とし、資源エネルギー庁による ERAB サイバーセキュリティガイドライン等の「政府ガイドライン」、実システムの脆弱性評価や研究開発といった「産業界・アカデミア」の実装が三角形（セキュリティトライアングル）として回っており、実際の ERAB システムのアセスメントでは 58 件の脆弱性が特定され、今後の対策・要件に反映される予定であると報告された。
5. NRI シンガポールの村岡氏は、東南アジアで分散電源・マイクログリッド・蓄電池の導入が年率 20%程度で拡大し、RE100 やデータセンター需要、離島電化、工業団地・タウンシップ開発などを背景に再エネニーズが急増している状況を説明

し、「DES ビジネスレディ → VPP ビジネスレディ → ERAB レディ」という 3 段階で各国の成熟度を整理した。
6. 同プロジェクトでは、ASEAN 各国のスマートメーター導入・VPP・アグリゲーションの進展と同時に、電力分野へのサイバー攻撃の増加を踏まえてセキュリティの重要性が急速に認識されつつあり、日本の ERAB ガイドラインとセキュリティトライアングルが、ASEAN 側から「実務的なフレームワーク」として評価され、専門家コミュニティによる白書出版やスタディグループで共有されたことが紹介された。
7. 資源エネルギー庁の加畑氏は、2040 年に再エネ比率 4～5 割を目指す日本のエネルギー政策の中で、フレキシビリティ確保（蓄電池・DR 等）と分散電源活用が不可欠であり、そのキープレイヤーとして ERAB アグリゲーターが位置付けられていること、既に 100 社超のアグリゲーターがライセンス取得していること、そして CPSF を基盤とした ERAB サイバーセキュリティガイドラインにより、多様な事業者が参加する電力システム全体のセキュリティ水準を担保していく考えを示した。
8. さらに加畑氏は、日本政府が進める「アジア・ゼロエミッション共同体（AZEC）」の枠組みの中で、再エネ最大活用とグリッド強化、DER・ERAB ビジネスを ASEAN に展開する方針を示し、ERIA・慶應・NRI による昨年度プロジェクト成果が AZEC 閣僚級会合の進捗報告にも位置付けられたこと、日本企業の ASEAN での実証・事業展開を補助金などで後押しする意向を述べた。
9. エコネットコンソーシアムの長澤氏は、1997 年設立以来の取り組みとして、ECHONET Lite 対応機器が国内で 1 億 5800 万台超に達し、エアコン・スマートメーターだけでなく、ヒートポンプ給湯器・蓄電池等、ERAB 向き機器のほぼ全てに ECHONET Lite が実装されている実態、Web API 規格に基づくクラウドサービス・公共案件・DR サービスの拡大、JEMA や早稲田大学らとの VPP/スマートメーター実証への参画を紹介し、「普及していない」という外部評価は事実と乖離している側面があると強調した。
10. セキュリティ面では、JC-STAR 制度の星 2 要件を見据えた ECHONET Lite DA 仕様（ペアリング、グループ鍵配信、メッセージ認証等）を IPA と連携しながら準備していること、欧米の標準（Matter 等）とは相互接続・ブリッジ仕様で共存を図りつつ、特にアジアにおいて ECHONET Lite を活用したアグリゲーションサービスを広げたいという方針が示され、最後に登壇者・共催団体（日本電気工業会 VPP 分科会など）から、ASEAN を「ブルーオーシャン」と捉えて産官学・会員企業が連携し、実証から実装フェーズへの移行を加速させていこうというメッセージで締めくくられた。

7 Day 4: October 31 | North Building 3F Large Meeting Room

7.1 D4-T1-S1 Google

Title: Decoding the Future of Attacks: Actionable Defense Strategies and Security with Google Speaker: Jay Uchiyama (Head of Google CoE)	タイトル：グローバル脅威の最前線：Google が紐解く、進化するサイバー攻撃のリアルと対策 スピーカ：内山 純一郎 (サイバーセキュリティ研究拠点長)
1. 冒頭で量子コンピュータの構造と冷却の仕組み、Google の量子チップ「Willow」の性能に触れつつ、「Harvest Now, Decrypt Later（HNDL）」型攻撃により、今の暗号通信が将来の量子計算機による解読の対象になりつつあるという問題提起がなされた。 2. 防御側は EDR の普及や高度なセキュリティコントロール、クラウドとオンプレが混在するハイブリッド環境への対応、そして人材不足を補うための AI 活用により、検知・対応能力を着実に向上させている一方で、人間を狙うソーシャルエンジニアリングの脅威は依然として根強いと指摘された。 3. 攻撃側はゼロデイ脆弱性の悪用を初期侵入経路として多用し、IoT・OT や仮想化基盤、ネットワークエッジ機器といった可視性の低い領域を狙うことで、防御側の「見えていないところ」を安全な足場として活用していると説明された。 4. UNC3886 などのケーススタディとして、仮想化基盤の管理コンポーネントにまで踏み込み、メーカー技術者よりも深く製品構造を理解した上で永続的なバックドアを仕込む高度な攻撃が紹介され、可視性の欠如が国家・経済安全保障レベルのリスクにつながると強調された。 5. ゼロデイの年間件数は直近 4～5 年で平均の 2 倍以上に増加し、国家支援グループだけでなく、商業サーベイランスベンダー（CSV）や金銭目的の犯罪国家主体などが暗号資産やダークウェブを通じて売買・利用することで、「ゼロデイの民主化・コモディティ化」が進んでいると説明された。 6. UNC5221（他社呼称：Silk Typhoon）による Ivanti などのエッジデバイス標的攻撃の事例では、境界装置から侵入し、クラウドサービス上に永続的なアクセス拠点を構築しつつ、特定人物のメールアカウントなど高価値情報を長期間（平均滞留 391 日）にわたり秘匿的に窃取するスパイ活動の実態が示された。 7. Scatter Spider の例では、ターゲット人物情報の収集とヘルプデスク詐欺・SMS フィッシングなどのソーシャルエンジニアリングで認証情報・多要素認証を乗っ取り、Okta 等の ID 基盤やクラウド設定を悪用して横展開する「クラウド特化プレイブック」が、恐喝型攻撃の定石としてテンプレート化していることが示された。 8. 攻撃側も AI を利用してフィッシング文面生成や脆弱性探索などの生産性を向上させているが、現時点では「まったく新しい攻撃様式」や「AI 由来の魔法のゼロデイ」が現れているわけではなく、既存の攻撃を高速・大量にこなすためのツールとして使っている段階だと分析された。 9. 防御側が AI を活用する具体例として、ビッグスリープのような LLM エージェントによる C/C++コードの脆弱性自動発見、膨大なログ・ダークウェブ情報からのシグナル抽出、自然言語から検知ルールへの自動変換、脅威インテリジェンスの「可視化・処理・解釈」の各段階の自動化が紹介され、AI が唯一現実的な防御強化手段になりつつあるとされた。 10. 最後に、Google の脅威インテリジェンスチームによる「監視・対抗・無力化（ディスラプション）」の枠組みとして、インフラのテイクダウン、侵害組織の修復支援、法的措置、脆弱性や APT 情報の公開による攻撃ビジネスモデルの崩壊を目指す取り組みが説明され、各国政府・企業との連携を通じて AI 時代のサイバー脅威に能動的に立ち向かう必要性がメッセージとして締めくくられた。	

7.2 D4-T1-S2 TrendMicro.Inc

Title: The Frontline of Cyber Threats: Latest Trends from State-Sponsored Groups Speaker: Hiroyuki Kakara (Sr. Threat Researcher, Trend Micro Cybersecurity Institute)	タイトル：サイバー脅威の最前線：国家背景の攻撃者グループ最新動向 スピーカ：加唐 寛征 (トレンドマイクロ サイバーセキュリティ・イノベーション研究所、シニアスレットリサーチャー)
1. 本セッションでは、中国・北朝鮮・ロシアという国家背景を持つ攻撃者グループの過去 1 年間の動向を、トレンドマイクロのリサーチ結果に基づき俯瞰し、日本を直接狙っていないケースも含めて「能力・TTPs・進化」を理解することの重要性を示した講	

演である。
2. 中国関連グループは、諜報・情報摂取を主目的とし、サプライチェーン攻撃や重要インフラへの長期潜伏、標的型スピアフィッシングを継続している。サポート終了で放置された IME ソフト（相互通訊）のアップデートドメイン乗っ取りによる大規模感染、VSCode トンネリング悪用、OAuth 同意の悪用など、「正規インフラ・正規機能」を逆手に取った攻撃が特徴である。
3. 中国の Earth Karmar グループは、カーネルレベルのルートキット（Moria, KRNRAT 等）を用いてプロセス・ファイル・ポート・トラフィックを徹底的に隠匿し、Radon、WMI ツール、リバースプロキシ、キーロガーなど複数ツールで横展開・認証情報窃取・長期潜伏を行う。DFSR や SYSVOL レプリケーションを悪用して、どのドメコンから情報が流出したか特定しにくくするなど、フォレンジック妨害も顕著である。
4. 中国では、Earth Estries（初期アクセス／アクセスブローカー）と Earth Naga（情報窃取）が同一環境で連携し、Cobalt Strike から ShadowPad をインジェクトするなど「役割分担型協調作戦」が観測された。これは、APT 世界でも「Access-as-a-Service」のようなビジネスモデルが浸透しつつあることを示し、アトリビューションを一層困難にしている。
5. 北朝鮮関連では、外貨獲得を目的に暗号資産取引所・DeFi・ソフトウェア開発者を集中的に狙い、LinkedIn 求人や技術面接を装って開発者に不正 npm パッケージをインストールさせる Void Dokkaebi のキャンペーンが紹介された。Bevertail（JS ダウンローダ）や Invisible Ferret（多機能インフォスティーラ）、TOR ベースの Tsunami など、OSS エコシステムと正規クラウドサービスをフル活用したサプライチェーン攻撃が特徴である。
6. DPRK IT ワーカーは、偽装したフリーランスエンジニアとして企業に入り込み、正規業務で報酬を得つつ内部ネットワークへのアクセス権限を悪用して情報摂取やバックドア埋め込みを行う「人的サプライチェーン攻撃」であり、面接で ChatGPT をリアルタイムに使って技術力を偽る・Deepfake を試験的に利用するなど、AI・映像技術も積極的に悪用していると指摘された。
7. 北朝鮮の Kimsuky（Earth Kumiho）は、Dropbox や GitHub をマルウェアホスティング／データ流出先として使い、自前 C2 なしに攻撃を完結させるほか、APT37 や KONNI の TTP やシェルコードを意図的に模倣して False Flag を仕掛け、アトリビューションを混乱させている。APT37 は.NET AppDomain Manager Injection を悪用したファイルレス攻撃で、正規プロセス内部で RAT を動作させるなど検知回避を高度化している。
8. ロシア関連グループはウクライナ侵攻と密接に連動し、（1）重要インフラへのワイパー攻撃、（2）高度な諜報活動、（3）世論操作を狙うインフルエンスオペレーションの「三位一体」でマルチドメイン戦を展開している。APT28（Pawn Storm）は LLM を Hugging Face 経由で組み込んだ RameHug や、ユーザーに自ら悪性 PowerShell を貼り付けさせる ClickFix 手法を採用し、APT29（Earth Kostet）は悪性 RDP 構成ファイルを使った Rogue RDP 攻撃と、大量の偽ドメイン＋Tor＋商用 VPN＋レジデンシャルプロキシで多層的にインフラを秘匿している。
9. さらにロシア発の Doppelganger キャンペーンでは、大手メディアそっくりの偽サイトを量産してウクライナ支援に否定的な記事を掲載し、SNS ボットで拡散する情報工作が行われている。中・朝・露に共通するトレンドとして、「Living off the Trusted Land（信頼されたサービス・ツールの悪用）」と多様化するサプライチェーン攻撃（レガシー資産のドメイン乗っ取り、OSS 汚染、人的サプライチェーン）が挙げられ、アトリビューションは連携・模倣・False Flag により一段と複雑化している。
10. まとめとして、国家背景 APT はソフトウェア・人材・インフラを含むサプライチェーン全体と信頼エコシステムそのものを狙い、AI という新たな武器も取り込みつつあるため、防御側は「侵入前提（Assume Breach）」で侵入後の検知・対応能力を強化し、ユーザー／プロセス／通信の振る舞いベース監視と、ソフト／人／サービスを含む広義のサプライチェーンリスク管理、自らの脅威インテリジェンスの継続的アップデートが不可欠であると結論づけている。

7.3 D4-T1-S3 Cisco

Title: Cutting Edge of "Economic Security" and "Cyber Security" for Private Companies to Understand Panelists: - Isamu Monji (Principal Sales Architect, Service Provider Operations, Cisco Systems) - Takahiro Takeda (Research Engineer, Outreach,	タイトル：民間企業が理解するべき「経済安全保障」と「サイバー安全保障」の最先端 パネリスト： - 文字 勇 (シスコシステムズ 情報通信事業プリンシパルアーキテクト) - 武田 貴寛 (シスコシステムズ Cisco Talos Researcher)

Threat Inteligence & Interdiction, Cisco Talos) - Shigeru Kimura (National Cybersecurity Advisor, Security & Trust Organization, Cisco Systems)	- 木村 滋 (シスコシステムズ Security & Trust Organization (S&TO))
1. 本セッションは「民間企業が理解すべき経済安全保障とサイバー安全保障の最先端」というテーマであり、経済安保推進法施行後の変化と、サイバー対処能力強化法を含む最新動向を整理する場である。 2. 経済安全保障推進法は、特定社会基盤役務の安定的提供を確保するための規制として位置づけられ、民間企業が考えるべき「標準的なベースライン」として浸透しつつあり、15 業種・257 事業者の届け出が行われている。 3. ここ数年でランサムウェア被害は日本国内でも顕著に増加しており、特に資本金 10 億円未満の中小企業が約 7 割と多数を占めるなど、「大企業だけが狙われているわけではない」という実態が示されている。 4. KIRIN ランサムウェアグループはリークサイトを用いた二重恐喝や、盗まれた認証情報を起点とした侵入、ESXi／仮想基盤を含む環境全体への攻撃など、高度かつ分業制（イニシャルアクセスブローカー等）による攻撃モデルを採用し、世界規模で活発に活動している。 5. 攻撃者は、ノートパッドや MS ペイント、サイバーダックなどの正規ツールを利用し、機密性の高い情報だけを選別して窃取する、攻撃コード内に被害者固有の ID やクレデンシャルを埋め込む、タスク名を既存ソフト（例：TeamViewer）風に偽装するなど、ステルス性と永続化に工夫を凝らしている。 6. APT 分野では、中国話者とされる Naikon と Backdoor Diplomacy のマルウェア（PlugX／RainyDay 等）において、コード構造や RC4 キーが一致する事例が見られ、同一グループまたは同一「ツールベンダー」による供給の可能性が指摘されるなど、国家系グループ間やランサムウェア間の「連携・共有」が強まっている。 7. こうした脅威の激化を受け、企業側の CISO やセキュリティ責任者からは「一段ギアが上がった」「先送りしてきた対策をもう言っていられない」といった声が出ており、クレデンシャル管理の見直しや、EDR 回避も前提にした多層防御など、対策レベルの引き上げが求められている。 8. サイバー対処能力強化法は、①官民連携の強化（基幹インフラ事業者による重要電子計算機の届け出・インシデント報告）、②通信情報の利用、③アクセス妨害・無害化措置の三本柱で構成され、とくに経済安保推進法で形成された 15 業種・257 社の枠組みを基盤に、官民連携を一層進めることが狙いである。 9. 重要電子計算機の範囲や届け出内容、事業者負担、通信の秘密や国民のプライバシー保護などが有識者会議で重点的に議論されており、2024 年 12 月に基本方針、2025 年春頃までに政省令を整備し、まず官民連携部分を来年秋頃、通信情報利用はその約 1 年後（2027 年秋頃）施行を目標として具体化が進められている。 10. クラウド利用、内製システム、オープンソース、AI・生成 AI、PQC、6G におけるセンシング機能（端末位置の高精度把握など）といった新技術は、基幹インフラの姿を変えつつあり、経済安保推進法・サイバー対処能力強化法ともに、技術進展を踏まえた定義の見直しと法制度の継続的アップデートを意識し続ける必要がある、というまとめで締めくくられている。	

7.4 D4-T1-S4 Hitachi

Title: The reality of migration to post-quantum cryptography (PQC) Moderator: Tadashi KAJI (Deputy General Manager, Research & Development Group, Hitachi, Ltd.) Panelists: - Tatsuya Tomaru (Quantum Computing Project, Next Research, Research & Development Group, Hitachi, Ltd.) - Kazuo Noguchi (Senior Research, Keio University)	タイトル：耐量子計算機暗号(PQC)移行の本当のところ モデレータ：鍛 忠司（日立製作所 研究開発グループ 副センタ長） パネリスト： - 戸丸 辰也（日立製作所 研究開発グループ ネクストリサーチ 量子コンピューティングプロジェクト） - 野口 和男（慶應義塾大学 上席研究員） - 河浦 直人（日立ソリューションズ セキュリティプロダクト本部 部長）

- Naoto Kawaura (Department manager, Security Product Division, Hitachi Solutions)	
1. 本セッションの目的は、「耐量子計算機（FTQC）の現実的な到来時期」と「PQC 移行をいつまでに・何から始めるべきか」を、量子コンピュータ開発・海外法令・実務（金融機関対応）の 3 つの視点から整理することである。 2. 量子コンピュータ側の現状として、暗号解読に使える誤り耐性量子コンピュータ（FTQC）は、キュービットの不安定性や誤り訂正（サーフェスコード等）に膨大な物量が必要であり、RSA2048 を 1 週間で解くには「10 の 6 乗個レベルのキュービット」が必要と見積もられているが、その「目処はまだ立っていない」というのが開発者の率直な見解である。 3. 超伝導・半導体など様々な方式で量子ビットの実装が進む一方、極低温環境・制御線の配線・発熱・誤り訂正用の論理量子ビット構成（距離 11 以上）など、物理実装・スケーリングの課題が山積しており、「キュービット数だけを外挿すると 2045 年頃に RSA2048 解読が可能かもしれないが、かなり粗い推定で本気にしすぎないでほしい」というスタンスが示された。 4. 国際的なサイバーリスクは年間 10 兆ドル規模とも言われ、既に数十億件のデータ漏えいが起きている中で、「Harvest now, decrypt later（今盗んでおいて、量子計算機ができたら後で解読する）」という脅威がコンセンサスを得つつあり、国連 OEWG や各国の議論でも AI と並ぶ量子関連リスクとして正式に位置づけられ始めている。 5. 米国では大統領令等で AI と PQC の準備が明確に書き込まれ、「2030 年まで／2031 年までに国家安全保障関連システムでの準備完了」「2026 年 10 月 1 日までに一部は準備」といった具体的なタイムラインが示され、EU・カナダも量子セキュリティ・PQC ロードマップの策定を進めており、日本でも金融庁が 2030 年頃を見据えて銀行等に準備を求めている。 6. PQC 移行は暗号アルゴリズムの置き換えだけでなく、「クリプトアジリティ（暗号の変更に耐えられる柔軟な設計）」や、国・業界ごとに異なる標準・プロトコルを跨いだガバナンスが必要であり、MITRE らが主導する PQCC など国際的な PQC 移行フレームワークの整備が進んでいる。 7. 日本では特に金融業界が先行しており、金融庁の検討会報告書では①経営層のコミットメント、②クリプトインベントリ（どのシステムのどこでどの暗号を使っているかの棚卸し）、③データ機密性・システム寿命・重要度に基づく優先順位付け、④2030 年代半ばまでの移行計画策定が求められている。 8. 実務面では、PQC 対応電子証明書や関連部品がまだ十分に標準化・普及しておらず、完全な移行はすぐにはできないため、「今できること」はあくまで準備に限られる。特に大量のシステムを持つ金融機関では、どのシステムから手を付けるか、どの程度のコストがかかるかが大きな悩みとなっている。 9. そのため現場向けの現実的アプローチとして、まず「PQC とは無関係にシステム本質リスク（外部公開・外部接続・端末・扱うデータ・寿命など）で一次仕分け→優先度の高い少数システムからクリプトインベントリ作成→使用暗号・証明書・鍵管理とライフサイクル・2029 年の証明書有効期間短縮問題も含めたリスク評価→移行“方針”の決定」という段階的ステップが提案されている。 10. 全体として、「量子計算機も法規制も一見“先”に見えるが、マイグレーションには 5～10 年以上かかるため、今すぐクリプトインベントリとリスクベースの優先度付けから着手しなければ 2030～2035 年の“Y2Q”に間に合わない」という危機感と、技術・制度・実務が三位一体で準備を進める必要性が強調されたセッションである。	

7.5 D4-T1-S5 ACCJ

Title: Towards a More Secure Digital Japan Moderator: Scott Warren (Partner, Squire Patton Boggs Tokyo) Panelists: - Jared Ragland (BSA) - James Miller (Director, JICCS) - Michael Karimian (Microsoft) English Session (no Japanese)	タイトル：より安全なデジタル日本に向けて モデレータ：スコット・ウォーレン（スクワイア・パットン・ボッグス東京事務所パートナー） パネリスト： - ジャレッド・ラグランド（BSA） - ジェームズ・ミラー（JICCS ディレクター） - マイケル・カリミアン（マイクロソフト） 英語セッション(日本語なし)
1. The moderator Scott Warren frames the session as a “company-eye view” on cybersecurity in	

Japan: how firms actually experience breaches, protect networks and data, and work with groups like ACCJ, BSA, JICCS, and Microsoft to make “digital Japan” safer.

2. Using IBM–Ponemon data, Scott highlights the business impact: average global breach cost ≈ $3.6M (≈$9.4M in the U.S.), average 189 days to detect and 72 days to eject attackers, and a shift from smash-and-grab ransomware to long-term lateral movement targeting high-value data.

3. Roughly 50% of attacks aim at personal data and 50% at business-confidential information (strategy, pricing, M&A, supply chain, HR data); he argues executives take cybersecurity more seriously when they see it as protecting “what makes the company valuable,” not just avoiding embarrassment or fines.

4. Jared (BSA) explains that BSA members provide cloud-based and on-prem security and business software, and that good policy environments (like in Japan and Singapore) can both remove digital trade barriers (data transfer/localization rules) and enable adoption of secure cloud and AI solutions.

5. On regulation, Jared stresses interoperable, risk-based incident notification: clear thresholds, realistic timelines (clock starts when a breach is discovered), coordination between privacy and cyber regulators, and alignment with regimes like U.S. CIRCIA and EU NIS2; Scott notes APPI’s current rules can over-trigger notifications when any threat actor is involved.

6. Both Scott and Jared describe AI as a double-edged sword: about 13% of attacks already use AI (e.g., phishing built in minutes), many breached firms had weak AI governance, and defenders must both deploy AI for detection/response and secure AI systems themselves (governance, red-teaming, data isolation, controlling “shadow AI” use by employees).

7. James (JICCS) argues Japan’s main problems are cultural and business-model-related rather than purely technical: lagging cloud/AI adoption, fragmented legacy systems, weak data use in sectors like banking, and poor security “hygiene”; he calls for “security transformation” tightly tied to business value, and for JICCS to provide an industry voice on national/economic security policy.

8. Michael (Microsoft) shares lessons from global telemetry (100T+ signals/day): prioritize identity and basic hygiene (phishing-resistant MFA, least privilege), treat ransomware/data theft as whole-economy risk, use AI to defend but harden AI itself (prompt/data/model attacks), start post-quantum crypto migration now, and align policies (incident reporting, AI, PQC) across allies to speed defense.

9. In Q&A on SMEs, the panel says most small firms buy “off-the-shelf” cloud/SaaS and lack in-house expertise, so governments should provide simple guidance, possibly tax incentives for cyber investment, and encourage secure-by-design vendors; digital transformation for these firms can simultaneously improve security and unlock new business value (e.g., data-driven insights like Singapore’s hawker/Grab example).

10. In closing, James warns that bolted-on security is a symptom of bad design and outdated tech; the panel’s overall message is that Japan needs nimble, resilient architectures, security embedded from the start, and leaders who “know the risks and the remedies,” making cybersecurity a core part of business strategy, not a compliance afterthought.

Change History

Date	Part	Comment
2025/11/25	Whole	New release
2025/12/01	Whole	Filled in the sections marked TBD. Corrected typos, omissions, and inconsistent terminology.
2025/12/10	Whole	Filled in the sections marked TBD. No remaining TBDs.