Report of all speeches and panels on 14th International Cybersecurity Symposium "Digital Cyber Security for National Security, Economic Security, and Societal Security"

October 30, 31, November 1, 2024

Keio University Global Research Institute

Satoru Tezuka

Contents

Main Session

Parallel Session

※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.

The parallel sessions were recorded to the best of our ability. Please understand that some sessions may not have been recorded.

※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。

講演者が英語で話された場合には、英語の要約は講演者の言葉を要約し、日本語の要約は同時通訳者の言葉を要約しました。

講演者が日本語で話された場合には、日本語の要約は講演者の言葉を要約し、英語の要約は同時通訳者の言葉を要約しました。

パラレルセッションは、ベストエフォートで記録したものです。記録がないものはご了承ください。

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

1.1 D1-S1-1 Opening

Satoru Tezuka (Project Professor, Keio University, Keio University Global Research Institute)	手塚 悟 (慶應義塾大学 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)
Overview The document provides a comprehensive summary of the 14th International Cybersecurity Symposium, focusing on key themes such as national, economic, and societal security. It highlights the symposium's structure, discussions on digital cybersecurity, infrastructure and trust, and future trends in cybersecurity cooperation. The document concludes with a consolidated list of action items derived from the symposium's agenda. **Overview of the Symposium** **Introduction** • The 14th International Cybersecurity Symposium, titled "Digital Cybersecurity for National Security, Economic Security, and Societal Security," is hosted by Keio University Global Research Institute, Cyber Civilization Research Center, Cybersecurity Research Center, and MITRE Corporation. • The symposium aims to explore international cybersecurity issues, focusing on the digital dependencies of critical infrastructure such as power, telecommunications, railroads, finance, healthcare, and water. • The event will examine differences and gaps in cybersecurity policies among countries, regions, G7, and G20, and explore multilateral partnerships to harmonize global security. **Symposium Structure** • The three-day program consists of keynotes, presentations, and panels held in the main hall, with interpretation	**概要** 本書は、第 14 回国際サイバーセキュリティ・シンポジウムの包括的な要約であり、国家、経済、社会の安全保障といった主要テーマに焦点を当てている。シンポジウムの構成、デジタル・サイバーセキュリティ、インフラストラクチャーと信頼に関する議論、サイバーセキュリティ協力の将来的なトレンドに焦点を当てている。最後に、シンポジウムの議題から導き出されたアクション・アイテムの統合リストで締めくくっている。 **シンポジウムの概要** **はじめに** • 第 14 回国際サイバーセキュリティ・シンポジウムは、慶應義塾大学グローバルリサーチインスティテュート、サイバー文明研究センター、サイバーセキュリティ研究センター、MITRE Corporation の主催で、「国家安全保障、経済安全保障、社会保障のためのデジタル・サイバー安全保障戦略」と題して開催される。 • このシンポジウムは、電力、通信、鉄道、金融、医療、水などの重要インフラのデジタル依存性に焦点を当て、国際的なサイバーセキュリティ問題を探求することを目的としている。 • このイベントでは、各国、地域、G7、G20 間のサイバーセキュリティ政策の違いやギャップを検証し、グローバル・セキュリティを調和させるための多国間パートナーシップを模索する。 **シンポジウムの構成** • 3 日間のプログラムは、メインホールで行われる基調講演、プレゼンテーション、パネルディスカッションで構成され、英語と日本語の通訳がつく。 • 2 日目と 3 日目の午後のセッションは、キャンパス内の別の建物で並行して行われる。 • 本日のセッションは午後 6 時 50 分に終了する。 **主要テーマと討論** **デジタル・サイバー安全保障** • **国家安全保障**：地政学的な挑戦の中で国土と国民を守る強い決意の必要性を強調。必要不可欠なシステムには、政府のクラウドシステム、サイバー情報

between English and Japanese.

- Afternoon sessions on days two and three include parallel sessions in different buildings on campus.
- Today's sessions will conclude at 6:50 PM.

Key Themes and Discussions

Digital Cybersecurity

- **National Security**: Emphasizes the need for strong determination to protect one's land and people amidst geopolitical challenges. Essential systems include government cloud systems, cyber intelligence systems, and active defense systems.
- **Economic Security**: Highlights the role of the private sector in protecting critical infrastructure, such as power and telecommunications, especially in light of geopolitical issues like the Ukraine problem.
- **Societal Security**: Focuses on the concept of Data Free Flow with Trust (DFFT), proposed by the late Prime Minister Abe, which is crucial for realizing Society 5.0 and digital transformation (DX).

Infrastructure and Trust

- The symposium underscores the importance of building digital infrastructure as the default for national, economic, and societal security.
- Trust in digital systems is paramount, with the establishment of international mutual recognition mechanisms to enable global data and digital trade.
- The development of a trust service infrastructure, including electronic signatures and authentication, is underway and needs acceleration.

Future Trends and Cooperation

- Multilateral cooperation among like-minded countries and public-private

システム、能動的防衛システムなどがある。

- **経済安全保障**：特にウクライナ問題のような地政学的問題を踏まえ、電力や通信といった重要インフラの保護における民間部門の役割を強調する。
- **社会保障**：ソサエティ 5.0 とデジタルトランスフォーメーション（DX）の実現に不可欠な、故安倍首相が提唱したDFFT（Data Free Flow with Trust）の概念に焦点を当てる。

インフラと信頼

- このシンポジウムは、国家、経済、社会の安全保障のために、デジタル・インフラを構築することの重要性を強調している。
- グローバルなデータとデジタル取引を可能にする国際的な相互承認メカニズムを確立するためには、デジタルシステムの信頼が最も重要である。
- 電子署名や認証を含むトラスト・サービス・インフラの開発は進行中であり、加速する必要がある。

今後の動向と協力

- 志を同じくする国同士の多国間協力や官民パートナーシップは、これまで以上に必要だと考えられている。
- このシンポジウムの目的は、サイバーセキュリティの今後の動向とその世界的な影響について議論することであり、その議論が世界的に重要な意味を持つことを期待している。

アクション・アイテム

[ ] 午後、国家安全保障に関するスピーチやパネルディスカッションに出席する。

[ ] 2 日目は、重要インフラの保護に関する議論に参加する。

[ ] 3 日目には国際的な相互承認とトラストサービスのインフラに関するセッションに参加する。

partnerships are deemed more necessary than ever. • The symposium aims to discuss future trends in cybersecurity and their global impact, with the hope that the discussions will have significant importance worldwide. **Action Items** [ ] Attend speeches and panel discussions on national security topics this afternoon. [ ] Participate in discussions on protecting critical infrastructure on day two. [ ] Engage in sessions on international mutual recognition and trust service infrastructure on day three.	

1.2 D1-S1-2 Opening

Wen Masters (Vice President, Cyber Technologies, MITRE)	ウェン・マスターズ（MITRE、サイバー技術担当副社長）
Cybersecurity, AI, Quantum Computing **Theme** This speech emphasizes the importance of digital cybersecurity for national, economic, and societal security. It addresses the unique cybersecurity needs of critical infrastructure and the OT environment, the threats posed by quantum computing to current cryptographic algorithms, and the necessity of transitioning to quantum-safe cryptos. Additionally, it highlights the risks associated with the malicious use of AI and the vulnerabilities within AI systems that need to be addressed. **Takeaways** 1. Digital cybersecurity is crucial for national, economic, and societal security. 2. Critical infrastructure cybersecurity faces threats from potential cyberattacks using quantum computers. 3. The OT environment has unique cybersecurity needs. 4. Growing the cyber workforce and developing targeted capabilities are	デジタルの安全保障, AI の進化, 量子コンピューター **テーマ** この講演では、デジタルの安全保障が国家安全保障、経済安全保障、社会保障に不可欠であることを強調しました。重要インフラのサイバーセキュリティ、AI の悪意ある使用、量子コンピューターによるサイバー攻撃からのデータ保護が主要な課題として挙げられました。また、AI の進化とその悪用の可能性、量子コンピューターの暗号解読能力に対する対策の必要性についても議論されました。 **要点** 1. デジタルの安全保障は国家安全保障、経済安全保障、社会保障に不可欠である。 2. 重要インフラのサイバーセキュリティ、AI の悪意ある使用、量子コンピューターを使用したサイバー攻撃からのデータ保護が重要な課題である。 3. AI の進化とその悪用の可能性についての懸念。 4. 量子コンピューターの進歩とその暗号解読能力に対する対策の必要性。 5. AI モデルアルファフォールドが科学ノーベル賞に貢献した事例。 **ハイライト** • "デジタルの安全保障というのは、国家安全保障、経済安全保障、そして社会保障を確保していくため

essential.

5. Malicious use of AI poses significant safety and security challenges.
6. AI systems have vulnerabilities that need to be understood and addressed.
7. Quantum computing can potentially break current cryptographic algorithms.
8. Transition to quantum-safe cryptos is necessary to secure data and information systems.

Highlights

- "Digital cybersecurity is a central enabler for achieving national security, economic security, and societal security."

Chapters & Topics

Critical Infrastructure Cybersecurity

The protection of critical infrastructure from cyberattacks, especially those using advanced technologies like quantum computers.

- **Keypoints**
  - Critical infrastructure cybersecurity is essential for national security.
  - Quantum computers pose a significant threat to current cybersecurity measures.
  - The OT environment has unique cybersecurity requirements.
- **Considerations**
- Develop targeted capabilities to defend against cyber threats.
- Grow the cyber workforce to address these challenges.

Malicious Use of AI

The potential for AI technologies to be used for harmful purposes, posing risks to safety and security.

- **Keypoints**
  - AI can be used for both beneficial and malicious purposes.
  - Understanding AI system vulnerabilities is crucial for cybersecurity.
  - Developing safe and secure AI algorithms is urgent.

になくてはならないものということになるわけです。"

章とトピック

デジタルの安全保障

デジタルの安全保障は国家安全保障、経済安全保障、社会保障を確保するために不可欠な要素である。

- **要点**
  - 重要インフラのサイバーセキュリティ
  - AI の悪意ある使用
  - 量子コンピューターを使用したサイバー攻撃からのデータ保護

AI の進化と悪用の可能性

AI の能力が急速に進化しており、その悪用の可能性についての懸念がある。

- **要点**
  - AI システムの脆弱性の理解
  - 安全でセキュリティの高い AI アルゴリズムの構築
- **Examples**
- AI モデルアルファフォールドが非常に複雑なタンパク質の構造を予測し、科学ノーベル賞に貢献した。

量子コンピューターと暗号解読

量子コンピューターは従来のコンピューターよりも高速な計算が可能であり、特に暗号解読において大きな脅威となる。

- **要点**
  - 量子コンピューターの進歩
  - 耐量子暗号の研究の必要性

宿題と提案

• **Considerations** • Focus on foundational approaches to build secure AI algorithms. **Quantum Computing and Cryptography** The impact of quantum computing on current cryptographic algorithms and the need for quantum-safe cryptos. • **Keypoints** ○ Quantum computing can perform calculations much faster than classical computers. ○ Current cryptographic algorithms are vulnerable to quantum computing. ○ Transitioning to quantum-safe cryptos is necessary to secure data. • **Considerations** • Start transitioning to quantum-safe cryptos now. **Assignments & Suggestions**	

1.3 D1-R2-1 Remarks from Keio University

Jun Murai (Distinguished Professor, Keio University)	村井 純 (慶應義塾大学 教授)
Cybersecurity, Quantum Computing, Digital Infrastructure **Theme** This speech, held on October 30, 2024, at Keio University, covered various topics including the introduction of Keio University's president and his involvement in quantum computing, the Quantum Internet Task Force as part of the Moonshot Project, Japan's recent weather patterns and significant earthquake, and Prime Minister Kishida's warning about misinformation during disasters. The importance of digital infrastructure in disaster recovery, the role of AI in protecting critical infrastructure, and the need for secure data sharing for AI applications were also discussed. Emphasis was placed on horizontal collaboration among government, academia, and industry for cybersecurity. **Takeaways**	**量子技術** **量子コンピューターの専門家の登場** • 量子コンピューターの専門家が登場予定。 • 量子コンピューティングのインターネットタスクフォースを結成し、アーキテクチャの定義に取り組んでいる。 **政府の取り組み** • 量子技術はムーンショットプロジェクトとして政府が取り組んでいる。 • 2024 年に向けて、日本の量子コンピューターの発展を目指している。 **気候と地震** **気候の異常** • 10 月末にもかかわらず、夏のような気候が続いている。 **地震の発生** • 1 月 1 日に能登半島で大きな地震が発生。 **政府の対応** **林官房長官の出席** • 林官房長官が本日出席。

1. Cybersecurity symposium at Keio University
2. Introduction of Keio University's president and his involvement in quantum computing
3. Quantum internet task force and the Moonshot Project
4. Japan's unusual weather patterns in late October 2024
5. Significant earthquake in Japan on January 1, 2024
6. Prime Minister Kishida's warning about misinformation and fake news during disasters
7. Importance of digital infrastructure in disaster recovery
8. Role of AI and digital technology in protecting critical infrastructure
9. Need for secure sharing of digital data for AI
10. Horizontal collaboration among government, academia, and industry for cybersecurity

Highlights

- "We should develop the secure way to sharing those data, and then utilizing those data."

Chapters & Topics

Quantum Internet Task Force

A task force focused on distributed processing with quantum elements, part of the Moonshot Project.

- **Keypoints**
  - Distributed processing with quantum elements
  - Architecture definition
  - Part of the Moonshot Project

Digital Infrastructure in Disaster Recovery

The role of digital infrastructure in recovering from natural disasters and its importance in saving lives.

- **Keypoints**

岸田総理大臣の発表

- 岸田総理大臣が情報に注意するよう呼びかけ。

重要インフラとデジタルテクノロジー

インフラの重要性

- 重要インフラは AI やデジタルテクノロジーを活用している。
- デジタルテクノロジーとサイバーセキュリティは重要インフラを水平展開でつなげる必要がある。

公共セクターの役割

- 重要インフラのサービスは民間団体が提供。
- 政府の役割は何かが問題。

サービスプロバイダーのサポート

- 重要インフラストラクチャーはサービスプロバイダーがサポート。
- OT のようなものが国民に重要なサービスを提供。

デジタルデータの共有とセキュリティ

- デジタルデータを共有し、情報のセキュアな利用を促進。
- AI は膨大なインターネットデータを元にしている。

データ利用の恐れと議論

- デジタルデータの利用が恐れられているため、活用をやめるべきかという議論がある。
- セキュアな形でデータを共有する方法を開発し、活用する必要がある。

サイバーセキュリティの責任

- サイバーセキュリティの責任は各省庁や企業に分散しているが、連携が必要。

本会議の意義

専門家の連携

- 政府、業界、学会、学生たちを巻き込み、各分野をつなげる。
- 各ステークホルダーがサイバーセキュリティで連携し、デジタルインフラストラクチャーの安全性を確保。

参加者への感謝

- 会議に参加していただいたことに感謝。
- 知恵を共有し、議論に参加して貢献をお願い。

将来の社会の実現

- 新しい世界をサイバースペースにおいて作ることを目指す。

Action Items

[ ] 各ステークホルダーがサイバーセキュリティで連携する方法を検討。

○ Critical for lifeline infrastructure ○ Complicated to maintain ○ Utilizes AI and digital technology **Secure Sharing of Digital Data for AI** The necessity of securely sharing digital data for AI applications while preventing abuse. • **Keypoints** ○ Fear of data abuse ○ Need for secure data sharing ○ Utilization of data for AI **Horizontal Collaboration for Cybersecurity** The importance of collaboration among different sectors to ensure cybersecurity and maintain digital infrastructure. • **Keypoints** ○ Involvement of government, academia, and industry ○ Joint efforts for cybersecurity ○ Maintaining digital infrastructure **Assignments & Suggestions**	[ ] デジタルデータのセキュアな共有方法を開発。 [ ] デジタルインフラストラクチャーの安全性を確保するための連携を強化。

1.4 D1-R2-2 Remarks from Keio University

David Farber (Guest Professor, Keio University)	デイビッド・ファーバー(慶應義塾大学 客員教授)
Cyber Civilization Research Center, Security Issues, Technology Governance **Theme** This speech introduces the Cyber Civilization Research Center (CCRC) and its focus on societal changes in hardware, software, governance, economics, and technical planning. Key topics include security issues in the early internet, challenges with inherently insecure computing hardware, and the distinction between managing and governing technology, particularly the internet and AI. **Takeaways** 1. Introduction to the Cyber Civilization Research Center (CCRC) 2. CCRC's focus on societal changes in hardware, software, governance, economics, and technical planning 3. Security issues in the early days of the	インターネットセキュリティ, AI ガバナンス, 信頼性 **テーマ** この講演では、サイバー文明研究所の 7 年間の研究内容、インターネットのセキュリティ問題、ハードウェアとソフトウェアの信頼性、AI およびガバナンスのストラクチャー、インターネットの管理とガバナンスの違いについて議論されました。特に、データ保護の重要性と信頼性の高い技術の開発が強調されました。 **要点** 1. サイバー文明研究所の 7 年間の研究内容 2. インターネットのセキュリティ問題 3. ハードウェアとソフトウェアの信頼性 4. AI およびガバナンスのストラクチャー 5. インターネットの管理とガバナンスの違い **ハイライト** • "データをとにかく保護していかなければならない。しかしながらこれはほとんど砂の上で、崩れる砂の上で、我々が必死に立とうとしているような作業で、より信頼のできるハードウェアやソフトウェアをいかにこれから

internet

4. Challenges with inherently insecure computing hardware
5. Difficulties in designing secure systems due to unreliable hardware and software
6. Need for trustable hardware and software
7. Challenges in governing technology, particularly the internet and AI
8. Distinction between managing and governing technology

Highlights

- "It's very hard to govern technology."

Chapters & Topics

Cyber Civilization Research Center (CCRC)

The CCRC is a research center focused on understanding and supporting societal changes in various domains such as hardware, software, governance, economics, and technical planning.

- **Keypoints**
  - Formed seven years ago
  - Co-chaired by Jim Moriah and the speaker
  - Aims to preserve the economy and freedom of the future

Security Issues in Early Internet

In the early days of the internet, security was not a primary concern, leading to fundamental security issues baked into the network's structure.

- **Keypoints**
  - Initial focus was on making the network work
  - Security issues were not prioritized
  - Fundamental security problems are now hard to eliminate

Inherently Insecure Computing Hardware

Most computing hardware is not inherently secure, making it difficult to design secure systems.

- **Keypoints**
  - Few machines are trusted to be secure in the hardware sense
  - Software is built on unreliable hardware

作っていけるかということをこれまで研究してまいりました。"-- ファーバー教授

章とトピック

インターネットのセキュリティ問題

インターネットの初期にはセキュリティが重視されていなかったが、現在では重要な課題となっている。

- **要点**
  - ネットワーク、プロトコル、ソフトウェアにセキュリティ問題が入り込んでいる。
  - セキュリティのために多くのパッチが必要。
  - 信頼性の高いハードウェアやソフトウェアの開発が求められている。

AI およびガバナンスのストラクチャー

テクノロジーの管理とガバナンスの違いについての研究。

- **要点**
  - インターネットの管理はある程度成功しているが、ガバナンスは難しい。
  - 管理とガバナンスの違いを理解することが重要。

宿題と提案

○ Endless patches to software create additional security challenges **Governance vs. Management of Technology** There is a distinction between managing and governing technology, with governance being a more challenging issue. • **Keypoints** ○ Managing the internet has been relatively successful ○ Governing the internet remains difficult ○ Similar challenges are expected with AI **Assignments & Suggestions**	

1.5 D1-R2-3 Remarks from Keio University

Kohei Ito (President, Keio University)	伊藤 公平 (慶應義塾大学 塾長)
Overview The 14th International Cybersecurity Symposium, hosted by Keio University on October 30, 2024, brought together distinguished speakers, panelists, and guests from around the world. The symposium focused on themes such as national, economic, and societal security, with significant contributions from various international delegations and academic institutions. **Welcome and Introduction** • **President Ito's Welcome Message** ○ President Kohei Ito of Keio University welcomed attendees to the 14th International Cybersecurity Symposium. ○ This is President Ito's fourth time hosting the symposium as the president of Keio University. ○ Acknowledged the presence of distinguished speakers, panelists, audience, and guests from around the world. **Delegation and VIP Acknowledgements** • **European Union Delegation** ○ Ambassador John Eric Paquette • **French Embassy in Tokyo** ○ Ambassador Philippe Seton	サイバーセキュリティ，デジタルトラストプロジェクト，インターナショナルサイバーセキュリティセンターオブエクセレンス **テーマ** 2024 年 10 月 30 日に開催された第 14 回サイバーセキュリティ国際シンポジウムでは、国家安全保障、経済安全保障、社会保障に関する議論が行われました。慶應義塾大学の三田キャンパスで開催され、著名なスピーカーとパネリストが参加しました。デジタルトラストプロジェクトや DFFT の POC、インターナショナルサイバーセキュリティセンターオブエクセレンスの活動についても紹介されました。 **要点** 1. 第 14 回サイバーセキュリティ国際シンポジウム 2. 慶應義塾大学の三田キャンパス 3. 著名なスピーカーとパネリスト 4. 国家安全保障、経済安全保障、社会保障 5. デジタルトラストプロジェクト 6. DFFT の POC 7. サイバー文明リサーチセンター 8. インターナショナルサイバーセキュリティセンターオブエクセレンス 9. 量子と AI のデジタルイノベーション **ハイライト** • "この実学というのは我々が創立してから 166 年間、慶應のモットーとしてきたものであるわけです。"-- 伊藤公平 **章とトピック** **サイバーセキュリティ国際シンポジウム**

- **U.S. Embassy Tokyo**
  - Deputy Chief of Mission, Catherine Monaghan
- **British Embassy Tokyo**
  - Minister and Deputy Head of Mission, Emil
- **Embassy of Israel in Japan**
  - Asaf Segev
- **Australian Embassy, Tokyo**
  - Minister-Counselor Claire Elias
- **Kingdom of the Netherlands**
  - Deputy Head of Mission, Rob Anderson
- **German Embassy**
  - Head of Economic and Scientific Department, Peter Leferheit
- **Republic of Lithuania**
  - Vice Minister, Magrias Avkevicius
- **Embassy of Estonia in Tokyo**
  - Business and Investment Officer, Oliver Ait
- **United Nations**
  - Under-Secretary General and High Representative for Disarmament Affairs, Izumi Nakamitsu (online)
- **VIP Reception**
  - Over 70 VIPs from around the world attended a reception the previous day.

Symposium Themes and Discussions

- **Digital Cybersecurity**
  - Focus on national, economic, and social security.
  - Discussions have become increasingly relevant due to ongoing geopolitical situations.

National Security

- **Keynote Speaker: Retired Admiral Dennis Blair**
  - Supported the symposium from its inception.
  - Influenced Japan's new national security strategy.
  - Continues to shape U.S.-Japan national security based on his experience as U.S.

サイバーセキュリティに関する国際的なシンポジウムで、国家安全保障、経済安全保障、社会保障に関する議論が行われる。

- **要点**
  - 国家安全保障、経済安全保障、社会保障のためのデジタルサイバー安全保障戦略
  - 著名なスピーカーとパネリストの参加
  - 地政学的な状況の認識

デジタルトラストプロジェクト

慶應大学が推進するプロジェクトで、DFFT の POC を実現するための総合国際認証に取り組んでいる。

- **要点**
  - EU とインドのパートナーシップ
  - G7 および G20 での示唆

インターナショナルサイバーセキュリティセンターオブエクセレンス

慶應大学が 2016 年 11 月に設立した世界初のサイバーセキュリティセンターで、国際的な連携を進めている。

- **要点**
  - インペリアルカレッジロンドン、ノースイスタン大学、UMBC、ロイヤルホロウェイ、九州大学、バージニアテック、クイーンズユニバースティ、ベルファーストコーとの連携
  - リモジェン大学、イデスコアン、テクニオン、インドネシア大学、タリン工科大学、ポルトナ大学との連携

宿題と提案

Director of National Intelligence. **Economic Security** • **Collaboration with U.S. Secretary of State for National Security** ○ Strengthening critical infrastructure systems. ○ Conducting research on defense against cyber attacks and global supply chains. **Societal Security** • **Digital Trust Projects** ○ Initiated by Keio University. ○ Focus on international mutual recognitions for achieving DFFT proof of concept with EU and India. ○ Demonstrated at G7 in Japan and G20 in India last year. **Research and Academic Contributions** • **CAO Cyber Civilization Research Center** ○ **Distinguished Prof. Jun Murai** ▪ Emphasized the need for next-generation digital infrastructure. ○ **Prof. David Farber** ▪ Influential in Internet and AI-related cyber civilization. • **Symposium Leadership** ○ Led by Professor Satoru Tezuka. ○ Focus on Digital Trust Issues in Japan. ○ Expansion of the International Cyber Security Center of Excellence (INCS-COE) to EU, India, Indonesia, and Singapore. **Keio University's Contributions** • **Philosophy and History** ○ Keio University's motto: "Jitsugaku" (practical study). ○ 166 years of history. • **International Cyber Security Center of Excellence (INCS-COE)** ○ Initiated in November 2016. ○ Collaborations with Imperial College London, Northeastern University, UMBC, Royal Holloway, QC University, Virginia	

Tech, and Queens University, Belfast. ○ Expanding with affiliates including University of Limoges, Edith Cohen, Technion University, and others. **Action Items** [ ] None mentioned.	

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

HAYASHI Yoshimasa (Chief Cabinet Secretary)	林 芳正（内閣官房長官）
Overview This document summarizes the discussion on cybersecurity strategies, enhancement measures, public-private partnerships, international cooperation, and the implementation of active cyber defense. Each section presents specific examples and measures, with a list of action items at the end. **Importance of Cybersecurity Strategies** • **Thanks to Dr. Murai** ○ Dr. Murai has participated and contributed to the Cyber Security Strategy Headquarters since its early days. ○ As general manager, he expressed his gratitude to Dr. Murai. • **Importance of Cyberspace** ○ Cyberspace has become an essential social infrastructure for all activities. ○ Ensuring a free, fair, and secure cyberspace is more important than ever. • **Impact of Cyber Incidents** ○ When cyber incidents occur, they have a significant impact on people's lives, socioeconomic activities, and national security. ○ Example: Container terminal management system at the Port of Nagoya is down for 3 days. ○ Example: A hospital in Okayama is feared to have leaked information	**Overview** この文書は、サイバーセキュリティに関する戦略、強化策、官民連携、国際協力、能動的サイバー防御の導入についての議論をまとめたものです。各セクションでは、具体的な事例や施策が紹介されており、最後にアクションアイテムがリストアップされています。 **サイバーセキュリティ戦略の重要性** • **村井先生への感謝** ○ 村井先生は、サイバーセキュリティ戦略本部の初期から参加し、貢献している。 ○ 本部長として、村井先生に感謝の意を表明。 • **サイバー空間の重要性** ○ サイバー空間は、あらゆる活動に不可欠な社会基盤となっている。 ○ 自由で公正で安全なサイバー空間の確保が、これまで以上に重要。 • **サイバーインシデントの影響** ○ サイバーインシデントが発生すると、国民生活や社会経済活動、国家安全保障に大きな影響を与える。 ○ 例：名古屋港のコンテナターミナル管理システムが 3 日間停止。 ○ 例：岡山の病院で約 4 万人分の患者情報が漏洩の恐れ。 **サイバーセキュリティの強化** • **海外のサイバー攻撃** ○ 海外のサイバー攻撃グループによる日本や企業を標的とした活動が増加。 ○ 2022 年のロシアによるウクライナ侵攻以降、地政学上の緊張が高まっている。 • **国家安全保障戦略** ○ 2022 年 12 月 16 日に国家安全保障戦

on about 40,000 patients.

Strengthening Cyber Security

- **Foreign Cyber Attacks**
  - Increased activity by foreign cyber attack groups targeting Japan and corporations.
  - Geopolitical tensions have increased since the Russian invasion of Ukraine in 2022.
- **National Security Strategy**
  - National Security Strategy on December 16, 2022.
  - The goal is to improve response capabilities in the field of cyber security to the same level or better than major Western countries.
- **New Measures**
  - In July 2023, the ASM business was launched to enhance security monitoring for government agencies and other organizations.
  - Continuously examines and evaluates the status of servers and network devices exposed to the Internet from an attacker's point of view.

Public-Private Partnerships and International Cooperation

- **Strengthening Public-Private Partnerships**
  - Cooperation between the public and private sectors is essential to ensure a free, fair, and secure cyberspace.
  - Co-sponsored with Keidanren to strengthen collaboration with various companies, including critical infrastructure providers.
- **International Best Practices**
  - Co-signed an international collection of best practices for dealing with living off-the-land.

略を策定。

  - サイバー安全保障分野での対応能力を欧米主要国と同等以上に向上させることを目標。
- **新たな施策**
  - 2023 年 7 月に政府機関等のセキュリティ監視の強化に向けた ASM 事業を開始。
  - 攻撃者の視点で、インターネットに公開されているサーバーやネットワーク機器の状態を常時調査・評価。

官民連携と国際協力

- **官民連携の強化**
  - 自由・公正かつ安全なサイバー空間の確保には、官民の連携が不可欠。
  - 経団連と共催で、重要インフラ事業者をはじめとする様々な企業との連携を強化。
- **国際的なベストプラクティス**
  - リビングオフザランドへの対応に関する国際的なベストプラクティス集に共同署名。
  - 重要インフラ事業者が用いる機器やプロセスの制御管理技術のサイバーセキュリティに関する文書にも共同署名。

能動的サイバー防御の導入

- **有識者会議の設立**
  - 2023 年 6 月に国家安全保障戦略を踏まえ、有識者会議を立ち上げ。
  - 通信情報の利用、攻撃者のサーバーへのアクセス、無害化、官民連携の強化について議論。
- **法制度の検討**
  - 石破内閣の平大臣の下で、能動的サイバー防御に関する法制度の検討を加速。
  - 可能な限り早期に案を示す予定。

Action Item

[ ] 攻撃者の視点での ASM 事業の運用開始
[ ] 経団連との連携強化の取り組み
[ ] 能動的サイバー防御に関する法制度の検討加速

○ He also co-signed a document on cybersecurity of equipment and process control management technology used by critical infrastructure providers. **Implementing Active Cyber Defense** • **Establishment of a Council of Experts** ○ In June 2023, based on the National Security Strategy, the Council of Experts was established. ○ Discussed the use of communications information, access to attacker's servers, detoxification, and strengthening public-private partnerships. • **Legal System Considerations** ○ Accelerated consideration of legislation on active cyber defense under Minister Hira in the Ishiba Cabinet. ○ A draft will be presented as soon as possible. **Action Item** [ ] Start of operation of the ASM business from the attacker's point of view. [ ] Efforts to strengthen cooperation with Keidanren [ ] Accelerate consideration of legal systems for active cyber defense	

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

Satoshi MORIMOTO (Former Minister of Defense, Japan, Chairman of JISS (Japan Institute for Space and Security), Executive Adviser of Takushoku University)	森本 敏 (元防衛大臣(第 11 代)、一般社団法人 日本宇宙安全保障研究所 会長、拓殖大学顧問)
Cyber Security, U.S.-Japan Collaboration, Critical Infrastructure **Theme** This speech, held on October 30, 2024, delves into the complexities of the digital information society, highlighting issues such as malicious exploitation, cyber defense, and critical	サイバーセキュリティ, 法整備, 情報共有 **テーマ** この講演では、サイバーセキュリティの重要性、日本の現状、法整備の必要性、情報共有の重要性について説明されました。特に、特定秘密保護法やセキュリティクリアランス法、能動的サイバー防御に関する法律の重要性が強調されました。 **要点**

infrastructure vulnerabilities. It emphasizes the inadequacy of Japan's cyber security measures and the importance of U.S.-Japan collaboration. Key topics include the need for proactive prevention, centralized cyber security organizations, and the enactment of the Security Clearance Act. The role of NISC and the necessity for active cyber defense legislation are also discussed.

Takeaways

1. Sophisticated and complicated digital information society
2. Malicious exploitation of digital information
3. Cyber defense issues and cat and mouse game
4. Critical infrastructure and cyber attacks
5. Interference in elections, ransomware, and leakage of confidential information
6. Inadequate countermeasures in Japanese cyber security
7. Focus on physical threats and international relations
8. Retired Admiral Dennis Blair's contributions
9. Close collaboration between the U.S. and Japan
10. Centralized organization for cyber security

Highlights

- "It's not a matter of counterattack, but as much as possible, it's necessary to be proactive about preventing cyber attacks from happening in the first place."

Chapters & Topics

Digital Information Society

The world we live in is characterized by a sophisticated and complicated digital information society.

- **Keypoints**
  - Development of electronic and cyber technologies

1. サイバーセキュリティの重要性
2. 日本のサイバーセキュリティの現状
3. デイニス・ブレイヤーの指摘
4. インフラのサイバー防御
5. 法整備の必要性
6. 特定秘密保護法
7. セキュリティクリアランス法
8. 能動的サイバー防御
9. 情報共有の重要性
10. 米国との連携

ハイライト

- "サイバー防御問題というのは、手法と対策の追いかけっこであり、いずれが相手を凌駕するかどうか、ということは誰にもわからないわけですが、こういう状況の中で我々は生活を続けているのだと思います。"

章とトピック

サイバーセキュリティの重要性

現代社会におけるサイバーセキュリティの重要性について説明。

- **要点**
  - 高度で複雑な電子情報社会
  - 通信電子科学の発展
  - サイバー技術の複雑化

日本のサイバーセキュリティの現状

日本のサイバーセキュリティの現状と課題について説明。

- **要点**
  - 重要インフラの脆弱性
  - 内外の不安定要因
  - 物理的な安全保障上の危険

法整備の必要性

サイバーセキュリティに関する法整備の必要性について説明。

- **要点**
  - 特定秘密保護法
  - セキュリティクリアランス法
  - 能動的サイバー防御に関する法律

情報共有の重要性

サイバーセキュリティにおける情報共有の重要性について説明。

- **要点**
  - 民間通信事業者から政府への通報
  - 政府からの情報提供
  - 情報の処理と分析

○ Malicious exploitation of digital information by adversaries **Cyber Defense Issues** Cyber defense involves a continuous struggle against adversaries, often described as a cat and mouse game. • **Keypoints** ○ No definitive way to win over adversaries ○ Importance of living with cyber threats **Critical Infrastructure and Cyber Attacks** Cyber attacks on critical infrastructure can cause tremendous damage. • **Keypoints** ○ Electricity, gas, communication, and healthcare systems are vulnerable ○ Potential for interference in elections, ransomware, and leakage of confidential information **Inadequate Cyber Security Measures in Japan** Japan's cyber security measures have been inadequate compared to other security issues. • **Keypoints** ○ Focus has been on physical threats and international relations ○ Need for improved cyber security measures **Collaboration Between the U.S. and Japan** Close collaboration between the U.S. and Japan is necessary for effective cyber security. • **Keypoints** ○ Sharing of information ○ Maintaining regional stability **Centralized Organization for Cyber Security** Efforts are being made to centralize an organization to deal with various cyber security issues. • **Keypoints** ○ Steps being taken in legislation ○ Role of the Chief Cabinet Secretary **Security Clearance Act** The Security Clearance Act was enacted in May	**サイバー攻撃の無害化** サイバー攻撃を未然に防ぐための無害化措置について説明。 • **要点** ○ 攻撃元のサイバーに侵入 ○ 攻撃の阻止 ○ 政府機関への権限付与 **宿題と提案**

2024. • **Keypoints** ○ No legislation yet available for active cyber defense **Obligations of Communication Carriers** Communication carriers in Japan have an obligation to inform the government quickly about cyber attacks. • **Keypoints** ○ Need for two-way communication ○ Utilization of information with consent **Role of NISC** NISC plays a crucial role in fulfilling cyber security requirements. • **Keypoints** ○ Establishing organizational structure ○ Proactive prevention of cyber attacks **Legislation for Active Cyber Defense** Legislation for active cyber defense is necessary but has not yet been passed. • **Keypoints** ○ Importance of political situation ○ Hope for legislation in the next diet sessions **Importance of U.S.-Japan Relationships** Active cyber defense is important for U.S.-Japan relationships and international cooperation. • **Keypoints** ○ Contribution to international order ○ Need for peaceful and stable society **Assignments & Suggestions**	

1.8 D1-S7 Keynote Speech: Economic Security

Harry Coker (U.S. National Cyber Director, White House Office of the National Cyber Director)	ハリー・コーカー（米国ホワイトハウス国家サイバー長官）
Cybersecurity, Partnerships, Challenges **Theme** This speech highlights the importance of international partnerships in cybersecurity, the role of the White House Office of the National Cyber Director, and the impact of cyber threats on national security, economic stability, and	**参加者** • ワシントン DC からライブで参加 **議題** **サイバーセキュリティの重要性** **デジタルエコシステムの脅威** • デジタル化の進展と相互依存性のあるグローバルインフラストラクチャー、サプライチェーンの複雑化。

personal security. It discusses the challenges posed by increasing digitization, the need for collaboration with the private sector, efforts to streamline regulatory frameworks, and the significance of information sharing and real-time threat mitigation. The speech also emphasizes the U.S.-Japan partnership in cybersecurity and efforts to enhance internet routing security and prepare for a post-quantum future. **Takeaways** 1. Importance of international partnerships in cybersecurity 2. Role of the White House Office of the National Cyber Director 3. Impact of cyber threats on national security, economic stability, and personal security 4. Challenges posed by increasing digitization and interconnected global infrastructure 5. Need for collective response and collaboration with the private sector 6. Efforts to streamline regulatory frameworks to reduce compliance burdens 7. Importance of information sharing and real-time threat mitigation 8. Role of the United States in promoting a secure and rights-respecting digital future 9. Significance of the U.S.-Japan partnership in cybersecurity 10. Efforts to enhance internet routing security and prepare for a post-quantum future **Highlights** • "Cybersecurity is national, economic, and personal security." **Chapters & Topics** **International Partnerships in Cybersecurity** The importance of international partnerships in addressing cybersecurity challenges.	• 攻撃者が複雑な組織間の関係を悪用しようとしている。 • 国家主体及び悪意ある組織が重要システムに影響を及ぼす可能性。 **サイバーセキュリティの影響** • サイバーセキュリティは国家安全保障、経済安全保障、個人の安全性にとって重要。 • ヘルスケア、金融、交通分野が特に狙われている。 • ランサムウェアなどの攻撃が企業や政府を人質状態に置く。 **経済安全保障とサイバーセキュリティ** • サイバー攻撃による混乱でビジネスコストが増大。 • サイバー犯罪の増加（FBI インターネット犯罪報告によると 22%増加）。 • サイバーセキュリティは経済安全保障を意味する。 **公共安全性とサイバーセキュリティ** • サイバー詐欺が高齢者や若者を標的にしている。 • 詐欺による損害額が 2014 年以来 15 倍に増加（FBI 報告）。 • 認識向上と健全なオンラインセキュリティプラクティスの実装が必要。 **国際パートナーシップと協力** • セキュアで強靭性のあるデジタルエコシステムの構築が必要。 • 民間セクターが重要な当事者として貢献。 • 情報共有と意見交換を通じてパートナーシップを強化。 **規制とコンプライアンス** • 複数の規制当局が異なる方法で同じ管理を要求することによるコンプライアンス上の課題。 • シーソーの中にはサイバーセキュリティではなくコンプライアンスに 30%から 50%の時間を費やしている。 • 重複する規制体制を削減し、ビジネスコストを下げる必要。 **グローバルな対応と協力** • インターネットのルールセッティング、ルーティングセキュリティの強化、ポスト量子コンピューティングの準備。 • 国際社会の助けなしに解決できない技術的課題。 • ボーダーゲートウェイプロトコルの作業開始。 **地域協力と三者会談** • 日本及びフィリピンと三者会談を行い、地域におけるサイバー及びデジタル問題に関する協力を深める。

- **Keypoints**
  - Collaboration with allies and partners is crucial for effective cybersecurity.
  - The U.S. has strong partnerships with many nations, including Japan.
  - International cooperation helps in implementing digital solidarity.

Role of the Private Sector

The private sector's role in creating a secure and resilient digital ecosystem.

- **Keypoints**
  - The private sector owns and operates the majority of critical infrastructure.
  - Collaboration with the private sector is vital for collective cyber defense.
  - Efforts to reduce compliance burdens and enhance cybersecurity posture.

Cybersecurity Challenges

The various challenges posed by increasing digitization and interconnected global infrastructure.

- **Keypoints**
  - Threats to the digital ecosystem are becoming more sophisticated and diverse.
  - Adversaries exploit complex relationships between organizations and their suppliers.
  - Cyber vulnerabilities can create opportunities for bad actors to affect critical systems.

Regulatory Harmonization

Efforts to streamline regulatory frameworks to reduce compliance burdens.

- **Keypoints**
  - Challenges with compliance from multiple regulators.
  - Efforts to develop a framework for regulatory harmonization and reciprocity.
  - Collaboration with Congress on legislation for a more thoughtful approach.

Cyber-Enabled Fraud

- QUAD シニアサイバーグループを通じた重要な活動。

集団的強靭性と未来のデジタル連帯

- 集団的な対応が必要。
- 全員がセキュリティマインドセットを持つことが重要。
- 協力し合うことで世界の安定と経済成長を確保。

Action Items

[ ] セキュアで強靭性のあるデジタルエコシステムの構築
[ ] 情報共有と意見交換を通じたパートナーシップの強化
[ ] 重複する規制体制の削減
[ ] ボーダーゲートウェイプロトコルの作業開始
[ ] 日本及びフィリピンとの三者会談の継続

The impact of cyber-enabled fraud on vulnerable populations. • **Keypoints** ○ Cyber-enabled fraud targets the elderly and young people with online scams. ○ Significant increase in fraud losses reported since 2014. ○ Protection relies on awareness and sound online security practices. **Assignments & Suggestions**	

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

Jean-Eric Paquet (Ambassador, Delegation of the European Union to Japan)	ジャン・エリック・パケ (駐日欧州連合代表部特命全権大使)
Overview This speech summarizes the key points from a meeting held on October 30, 2024, focusing on cyber security challenges, strategies, and global partnerships. It also outlines upcoming events and action items to be addressed. **Opening Remarks** • **Participants**: Tezuka and Murai-sensei, Morimoto-san, Ambassador Seton-Philippe, colleagues, and friends. • **Historical Context**: The European Union first participated in this event in 2018. • **Current Challenges**: Despite collective efforts, cyber security challenges have grown and evolved. **Cyber Security Landscape** **Threat Landscape** • **Criminal and State Actors**: Active as ever, posing significant threats. • **European Network Security Agency (ENISA)**: ○ **Annual Threat Landscape Report**: Published on September 19. ○ **Key Data**: 80% of cyber attacks are ransomware attacks. **Cyber Security Strategy** • **EU-Level Strategy**: Developed with member states and EU institutions.	**Overview** この講演は、2024 年 10 月 30 日に作成された講演メモです。内容はサイバーセキュリティの現状と課題、EU と日本のサイバーセキュリティ協力、経済安全保障とリスクアセスメントに関する情報を含んでいます。最後に、具体的なアクションアイテムがリストアップされています。 **サイバーセキュリティの現状と課題** **サイバー攻撃の増加** • **攻撃者の活動**:「さまざまな攻撃者は活発に動いております。そして、高度な悪質な活動というものが増えております。」 • **ランサムウェアの普及**:「9 月 19 日に報告を発表しております。そして今現在は、ランサムウェアが普及していることを指摘しております。主な国全てにおいてこれが見られます。」 **サイバーセキュリティの対策** • **国家安全保障、経済安全保障、社会保障**:「サイバーセキュリティのポスチャーというものを更新し、そして国家安全保障、経済安全保障、そして社会保障というものを進めていかなければなりません。」 • **EU のサイバーセキュリティ戦略**:「欧州連合の方では、加盟国及びその他の組織とともにサイバーセキュリティ戦略というものを作成しています。4 年前から導入しております。そしてポジティブな効果というものが見られます。」 **グローバルな連携** • **EU の強靭性とレスポンス強化**:「EU の方が、EU のサイバー脅威に対する強靭性をさらに促進したいと

- **Recent Developments**:
  - **Minimum Cyber Security Requirements**: Raised for internet-connected devices (e.g., home cameras, fridges, TVs, toys).
  - **Implementing Rules for Critical Entities**: Issued ten days ago, covering risk management and incident reporting for services like cloud computing, data centers, online marketplaces, search engines, and social networking platforms.

Goals and Measures

- **Enhancing Resilience**: Against cyber threats.
- **Proactive Response Measures**: In cooperation with partners.
- **Cyber Defense Cooperation**: Building capabilities to prevent, deter, and respond to cyber attacks.
- **EU Cyber Sanction Regime**:
  - **Current Sanctions**: 14 persons and 4 entities with asset freezes and entry bans.
  - **Recent Applications**: Sanctions against Russian actors attacking Ukraine and EU member states.

Global Partnerships

- **Inclusive Approach**: Cyber security requires global cooperation.
- **UN and Partner Support**: Including Ukraine.
- **EU-Japan Cyber Security Cooperation**: To be further developed under the upcoming security and defense partnership.

Broader Security Agenda

Economic Security

- **Risk Assessments**: Identifying and assessing risks to economic security.
- **Critical Technology and Supply Chain Dependency**: Reviewing risks and increasing understanding.

考えており、またレスポンスの強化というものを目指しております。」

- **パートナーシップの強化**:「パートナーとともに連携していきたいと考えております。サイバーディフェンスの機能というものを強化し、そして様々な防止とか、あるいは抑止したりサイバー攻撃に対する対策というものを進めていきたいと考えております。」

EU と日本のサイバーセキュリティ協力

サイバーウィーク

- **イベントの開催**:「EU と日本の間でのサイバーウィークというのは、11 月の中旬に行われることになっております。」

共同トレーニングと経験共有

- **産業用サイバートレーニング**:「日本、米国、そして EU の産業用サイバートレーニングを進めており、東アジアから多くの参加者が来ているわけであり、そして東京で集まって、そしてさまざまな経験の共有を日本、米国、そして EU と、ということになっております。」

サイバーゲーム

- **キャプチャー・ザ・フラグ（CTF）**:「サイバーゲームにおいても、キャプチャー・ザ・フラグのイベントというものに、欧州連合の加盟国も参加しております。我々は必ずそういったコンペの中で勝利を収めたいと考えております。」

経済安全保障とリスクアセスメント

経済安全保障の取り組み

- **リスクアセスメント**:「さまざまな経済安全保障のリスクアセスメントを行っておりますし、また重要テクノロジー及びサプライチェーンの依存性などのアセスメントを行っております。」

グローバルな依存性の理解

- **共通の理解の強化**:「我々としては、いろんな依存性ということに関する共通の理解というものを強化するための取り組みを進めております。」

輸出規制と制裁

- **議論の進展**:「日本とも様々な取り組みを進めております。輸出規制、制裁、そしてどのような形でもって、さまざまな投資に関する取り組みについての議論というものを進めております。」

アクションアイテム

[ ] EU と日本のサイバーウィークの詳細を確認し、参加準備を進める

• **Economic Security Toolbox**: ○ **Anti-Coercion Instrument** ○ **Foreign Direct Investment Screening** ○ **Dual-Use Export Control Measures** ○ **Sanctions** ○ **Outbound Investments**: Exploring collective management strategies. **Upcoming Events** • **EU-Japan Cyber Week**: November 11-15. ○ **High-Level EU-Japan Cyber Dialogue**: Kick-off event. ○ **Japan-US-EU Industrial Control System Cyber Training**: Participants from East Asia sharing experiences. ○ **Kunoichi Cyber Games**: Capture the flag event featuring a team of European young women. **Action Items** [ ] Prepare for EU-Japan Cyber Week events from November 11-15. [ ] Continue developing cyber security cooperation under the EU-Japan security and defense partnership. [ ] Implement and monitor the new cyber security requirements and rules for critical entities.	[ ] 産業用サイバートレーニングの参加者リストを確認し、必要な調整を行う [ ] キャプチャー・ザ・フラグイベントの準備を進める [ ] 経済安全保障のリスクアセスメントの結果を共有し、次のステップを計画する

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

Philippe SETTON (Ambassador of France in Japan)	フィリップ・セトン (駐日フランス大使)
Brief Overview: This speech contains the meeting notes from the International Symposium on Cybersecurity held on October 30, 2024. Ambassador Seton delivered the opening remarks, highlighting the importance of cybersecurity in national, economic, and societal contexts. The notes cover various topics, including the Paris Appeal for Trust and Security in Cyberspace, the French National Cybersecurity Strategy, and multilateral engagement efforts. The current cybersecurity	**概要** この講演は、2024 年 10 月 30 日に作成された講演メモです。フリップ・セトン氏の発言を中心に、サイバーセキュリティの重要性、多国間協力、サイバー攻撃の現状、今後の取り組み、日本への感謝などが述べられています。最後に、アクションアイテムとして、サイバーフレームワークポスト 2025 のプログラムアクション、国際法の適用についての議論、ポールモールプロセスを通じたサイバー攻撃ツールの普及阻止が挙げられています。 **フリップ・セトン氏の発言** **感謝**

landscape, progress, and future commitments, such as the United Nations Framework and the Paul Mocker Initiative, are also discussed. The document concludes with a consolidated list of action items aimed at strengthening global cybersecurity efforts.

Opening Remarks by Ambassador Seton

Introduction

- Ambassador Seton expressed gratitude for the opportunity to speak at the symposium.
- The French Embassy supports this annual event, emphasizing its importance.

Challenges in Cybersecurity

- **National Security**: Cybersecurity is crucial for protecting national interests.
- **Economic Security**: Cyber threats can have significant economic impacts.
- **Societal Security**: Ensuring the safety of society from cyber threats is paramount.
- **Interconnected Challenges**: These challenges are interlinked and require a collective approach.

Collective Approach to Cybersecurity

- **Paris Appeal for Trust and Security in Cyberspace (2018)**:
  - Largest multi-stakeholder initiative.
  - Supported by 81 states, 390 civil society organizations, and 705 private sector companies.
  - Managed by the Paris Peace Forum.
  - Numerous workshops and projects launched to enhance global cybersecurity.
- **French National Cybersecurity Strategy (2021)**:
  - Focuses on training, education, research, innovation, and promoting a global culture of cybersecurity.

- フランス大使館として、この重要なイベントを毎年支援していることを嬉しく思っている。

サイバーセキュリティの重要性

- **テーマ**: サイバーセキュリティが包含する国家安全保障、経済安全保障、社会保障の 3 つの側面。
- **脅威**: サイバーの脅威はこれら 3 つの側面に関連しており、学際的かつ国際的なアプローチが必要。

パリアピールフォー・トラストアンドセキュリティサイバースペース

- **提案**: 2018 年にフランスが提案。
- **規模**: 81 カ国、390 の市民社会機関、705 の民間企業が賛同。
- **イベント**: パリスフォーラム、パリスピースフォーラムでサイバーセキュリティを国際的なレベルで議論。

国家安全保障戦略

- **提案**: 2021 年にフランス大統領が提案。
- **内容**: トレーニング、教育、研究、イノベーション、サイバーセキュリティを強力に推進。

多国間協力

- **協力機関**: 国連、OECD、EU。
- **主張**: 民間セクターと市民社会の声を政府の議論に取り込む必要性。

サイバー攻撃の現状

- **増加**: サイバー攻撃は毎年増加。
- **トレンド**: IoT と AI の進化により、悪意のあるアクターが増加。
- **例**: フランスがオリンピック、パラリンピック大会を主催した際、何百万回もの攻撃が行われたが、国際協力により影響を防止。

今後の取り組み

- **国際法の適用**: サイバースペースにおける国際法の適用について議論。
- **マルチステークホルダーイニシアティブ**: 英国と共にポールモールプロセスを開始し、サイバー攻撃のツールの普及を阻止。

日本への感謝

- **協力**: 日本が第 1 日目からイニシアティブに協力していることに感謝。

まとめ

- **協力の重要性**: 国、民間、市民社会が協力すれば、完全な失敗はないと考えている。
- **イベントの成功を祈念**: 第 14 回国際シンポジウム

○ Integrated into the international community. • **Multilateral Engagement**: ○ Active participation in the United Nations, OECD, and the EU. ○ Advocacy for including private sector and civil society voices in government discussions. **Current Cybersecurity Landscape** • **Increasing Cyber Attacks**: ○ The number of cyber attacks rises annually. ○ Expansion of attack surface due to IoT and AI advancements. ○ Growing threats from malicious actors, including state-sponsored attackers. • **Progress and Success Stories**: ○ Example: During the Olympic and Paralympic Games in France, millions of attacks were thwarted. ○ Collaboration with private sector, international organizations, and state partners like Japan was crucial. **Future Commitments and Initiatives** • **United Nations Framework**: ○ Strengthening the multilateral cyber framework. ○ Launching a post-2025 programme of action to build capacity and consensus on sensitive issues, including international law in cyberspace. • **Paul Mocker Initiative**: ○ Joint initiative with the United Kingdom. ○ Focus on combating the proliferation of cyber offensive tools. ○ Japan's commitment to the initiative acknowledged and	の成功を心から祈念。 **Action Items** [ ] サイバーフレームワークポスト 2025 のプログラムアクションを使用し、全ての参加国のキャパシティを高める。 [ ] サイバースペースにおける国際法の適用について議論する。 [ ] ポールモールプロセスを通じて、サイバー攻撃のツールの普及を阻止する。

appreciated. **Action Items** [ ] Strengthen the multilateral cyber framework within the United Nations. [ ] Launch a post-2025 programme of action to build capacity and consensus on international law in cyberspace. [ ] Continue the Paul Mocker Initiative to combat the proliferation of cyber offensive tools.	

1.11 D1-R4-1 Remarks from each of the governments and United Nations

Katherine Monahan (Deputy Chief of Mission, U.S. Embassy Japan)	キャサリン・モナハン (在日米国大使館首席公使)

Brief Overview:
The meeting notes from October 30, 2024, cover various aspects of cybersecurity, emphasizing the urgency and responsibility of addressing cyber threats. The notes highlight the nature and real-world examples of cyber threats, the importance of international cooperation, and the role of academia and industry in cyber workforce development. Attendees are encouraged to share best practices and network to stay ahead of cyber threats. The action items include networking during the symposium and participating in the Japan-U.S. Industrial Control Systems Week in November.
Opening Remarks
Introduction and Acknowledgment
• The speaker emphasized the gravity of the current cybersecurity landscape.
  ○ "Frankly, I hope you're scared, I'm scared, it's really scary."
• Acknowledged the collective expertise present.
  ○ "We have the best voices, we have the best brains, we have the best everything collectively here."
Responsibility and Urgency
	概要
	この講演は、2024 年 10 月 30 日に作成された講演メモです。サイバーセキュリティの重要性、サイバー攻撃の現状と対策、サイバーワークフォースの発展、イベントと感謝、シンポジウムの目的についての議論が含まれています。最後に、具体的なアクションアイテムがリストされています。
	サイバーセキュリティの重要性
	恐怖と責任
	• フランス大使や他のスピーカーが言及したように、サイバーセキュリティの脅威は非常に恐ろしいものである。
	• 昨晩、最高の頭脳が集まり、知見を共有したが、これは大きな責任でもある。
	• 電力が供給されない状況や、兵士がいない戦場など、サイバー攻撃の影響は計り知れない。
	生活への影響
	• サイバーの不安定は生活のあらゆる面に影響を及ぼし、子どもたちにも影響を与える可能性がある。
	• テクノロジーはワクワクするが、世界の課題を解決するためには責任を果たす必要がある。
	サイバー攻撃の現状と対策
	ランサムウェア攻撃
	• ランサムウェア攻撃が一般的になり、サイバー攻撃が兵器として使われている。
	• 脅威を理解し、先手を打つためには連携が必要である。
	官民連携の重要性
	• EU、アメリカ、日本の官民努力でサイバーの知恵を集めることが重要。

- Highlighted the responsibility of the attendees.
    - "It's a huge responsibility, and it's our responsibility. We really need to do this."
- Stressed the immediate impact of cyber threats.
    - Example: State Department losing electricity after reclaiming a Russian dacha.

Cybersecurity Threats

Nature of Cyber Threats

- Cybersecurity affects all aspects of life and future generations.
    - "Cybersecurity or cyber insecurity cuts across every aspect of our lives, every hope for our children."
- The increasing threat due to technological advancements.
    - "The more technology, the more opportunity there is for cyber criminals and foreign adversaries to exploit connectivity."

Real-World Examples

- Reference to the war in Ukraine.
    - "In 2022, Russia used technologies and AI-enabled capabilities to launch full-scale war of aggression."
- Potential impact on critical infrastructure.
    - "Imagine if the ATMs, if all the digital payment systems went down one day. Or worse, people took the money out of the bank accounts."

Collaborative Efforts

- 米国政府はテクノロジーをオープン化し、安全でセキュアな対策を取り、強靭性及び民主的な社会を醸成することを目指している。

サイバーワークフォースの発展

教育と保護

- 日本の大学などがサイバーワークフォースの発展のための努力を進めている。
- 従業員の保護や金融システムの安全も重要である。

サイバー攻撃の影響

- ATM やデジタル決済システムが機能しなくなった場合の影響を考える必要がある。
- 医療、電力、水道など、さまざまな分野でサイバー攻撃のリスクがある。

イベントと感謝

日米コントロールシステムイベント

- 米国政府は第 7 回日米のコントロールシステムの 1 週間のイベントを 11 月 15 日に開催予定。
- 経済産業省及び EU の代表団とともに開催される。

感謝の意

- 慶應義塾大学及びマイターコーポレーションに感謝。
- 民間セクターの参加者や林内閣官房長官にも感謝。
- 東京における在日米国大使館は学会業界と日本政府との連携を強化。

シンポジウムの目的

- ベストプラクティスの共有、ネットワーク作り、そして子どもたちにとって安全な世界を作るための努力を促進。

Action Items

[ ] 第 7 回日米コントロールシステムのイベント準備（11 月 15 日）

International Cooperation
• Emphasis on global collaboration.
  ○ "The United States will work with any country or actor that is committed to developing and deploying technology that is open, safe, and secure."
• Mention of specific partnerships.
  ○ "The U.S. government will co-sponsor the 7th annual Japan-U.S. Industrial Control Systems Week."
Role of Academia and Industry
• Importance of cyber workforce development.
  ○ "A key element of U.S. cyber engagement, of course, in Japan is cyber workforce development."
• Collaboration with universities and industry.
  ○ "Thank you to Keio University and MITRE Corporation, and along with the 10 governments that are hosting today."
Call to Action
Networking and Knowledge Sharing
• Encouraged attendees to share best practices and network.
  ○ "Please, today, throughout this symposium, share your best practices. Get to know each other. Network. Keep in touch."
• Emphasized the importance of staying ahead of cyber threats.	

○ "Keeping ahead of this. Making it not scary for our children is your job." **Action Items** [ ] Share best practices and network during the symposium. [ ] Participate in the 7th annual Japan-U.S. Industrial Control Systems Week from November 12th through 15th.	

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

Emil Levendoğlu (Minister and Deputy Head of Mission, British Embassy, Tokyo)	エミール・レベンドールー (駐日英国公使)
Cybersecurity, UK-Japan Partnership, Transparency **Theme** This speech, held on October 30, 2024, focused on the UK-Japan cybersecurity partnership and the importance of transparency in cybersecurity. Key takeaways included the significance of public-private partnerships, international cooperation, and the disruption of ransomware operations. Highlights emphasized that national, economic, and social security are intertwined with cybersecurity. The speech also covered the memorandum of cooperation with Keidanren, the Japan Cyber Fellowship, and the UK's Cyber First competition. **Takeaways** 1. International Cybersecurity Awareness Month 2. Keio University symposium 3. UK-Japan cybersecurity partnership 4. State-sponsored cyber activity 5. Public-private partnerships 6. Memorandum of cooperation with Keidanren 7. Japan Cyber Fellowship 8. UK's Cyber First competition 9. Free, open, and secure internet 10. Disruption of ransomware operations **Highlights**	**概要** この講演は、2024 年 10 月 30 日に作成された講演メモです。内容は、国際サイバーセキュリティ啓発月間の終わりに開催されたイベントに関するもので、日英のサイバーセキュリティ協力、具体的な取り組み、サイバーキャパシティビルディングについての詳細が含まれています。最後に、アクションアイテムがリストアップされています。 **開会の挨拶** • **イベントの概要** ○ 国際サイバーセキュリティ啓発月間の終わりに開催されたイベント。 ○ 慶應大学で 14 回目の開催。 ○ 慶應大学と特に手塚先生への感謝。 **日英のサイバーセキュリティ協力** • **共通の世界観と使命** ○ 日本と英国、他のパートナーが共通の世界観を持つ。 ○ サイバーの力を活用して経済を活性化させる共通の使命。 ○ 天皇陛下の言葉：「英国と日本は特別な友人」。 • **サイバーセキュリティの現状** ○ サイバースペースに国境はない。 ○ デジタル変革の進展と共に脅威も急速に変化。 ○ サイバー犯罪組織と国家の協力が進行中。 **日英の具体的な取り組み** • **官民のパートナーシップ** ○ 社会全体で官民のパートナーシップを推進。 ○ 2023 年 1 月：経団連のサイバーセキュリティ委員会と協力覚書を締結。

- "There is no national security, there is no economic security, or even social security without cybersecurity."

Chapters & Topics

UK-Japan Cybersecurity Partnership

The collaboration between the UK and Japan in the field of cybersecurity, focusing on public-private partnerships, international cooperation, and transparency.

- **Keypoints**
  - Strengthening public-private partnerships
  - Advancing shared international interests
  - Enhancing cyber capabilities
- **Examples**
- The UK signed a memorandum of cooperation with Keidanren's committee on cybersecurity in Japan.
- Five Japanese cyber experts attended the pilot Japan Cyber Fellowship held in the UK.
- Seven Japanese schools will take part in the UK's Cyber First competition in November.

Transparency in Cybersecurity

The importance of transparency in facilitating cooperation, building trust, and reducing the possibility of misinterpretation or escalation in cybersecurity.

- **Keypoints**
  - Transparency facilitates cooperation
  - Transparency builds trust
  - Transparency reduces misinterpretation and escalation
- **Examples**
- In 2018, the UN Special Rapporteur for Privacy recognized the UK's Investigatory Powers Act as world-leading legislation for balancing privacy and security.
- In 2023, the UK was the first country to release a publicly available primer on the principles for conducting offensive cyber
  - 2023 年 5 月：5 人の日本のサイバー専門家がジャパンサイバーフェロンシップに参加。
  - 2023 年 11 月：7 つの日本の学校が英国のサイバーファーストコンペティションに参加予定。
- **国際的な利益の教育**
  - 自由で開かれた、安全なインターネットを推進。
  - 多国間組織で国際規範を提唱。
  - ランサムウェアから AI の安全性まで共同ガイダンスを策定。
  - ロックビットエコシステムを含むランサムウェア活動を妨害。

サイバーキャパシティビルディング

- **国際的な協力**
  - バンクク、モンゴルでサイバーキャパシティビルディングイニシアティブを実施。
  - 新しい NISC との提携。
  - 国際的なサイバー演習での協力。
- **透明性の重要性**
  - 透明性が信頼を築き、誤解やエスカレーションの可能性を減少。
  - 2018 年：国連特別報告が英国の調査権限法を評価。
  - 2023 年：英国法律連合サービス研究所に日英サイバーパートナーシップの独立レビューを依頼。

アクションアイテム

[ ] 経団連のサイバーセキュリティ委員会との協力覚書のフォローアップ。

[ ] ジャパンサイバーフェロンシップ参加者のサポート。

[ ] サイバーファーストコンペティションへの参加準備。

[ ] 国際的なサイバー演習の計画と実施。

[ ] 日英サイバーパートナーシップの独立レビューの結果の活用。

operations. • The Royal United Services Institute independently reviewed the UK-Japan cyber partnership, and the report is available online. **Assignments & Suggestions**	

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

Claire Elias (Minister-Counsellor, Political, Australian Embassy Tokyo)	クレア・エリアス（在日オーストラリア大使館政務担当公使）

Brief Overview:
This speech, created on 2024-10-30, provides a comprehensive summary of a meeting focused on cyber security engagement between Australia and Japan. It covers various aspects including bilateral and multilateral cooperation, cyber challenges and threats, Australia's cyber security strategy, public-private partnerships, regional cooperation, and business engagement. The document concludes with a consolidated list of action items to be addressed.
Introduction
• Speaker: Clare Elias, Minister-Councillor, Political Australian Embassy, Tokyo.
• Acknowledgements: Thanks extended to President Ito, Professor Tezuka, Professor Murai, Noguchi-san, CAO, and MITRA for the invitation.
 	
Cyber Security Engagement
Bilateral and Multilateral Cooperation
• Roles and Responsibilities: Senior Coordinator for Cyber Security Engagement with Japan.
• Frameworks:
  ○ Quad Framework: Increasing importance in cyber cooperation.
  ○ AUKUS Pillar 2: Cooperation under this pillar is becoming significant.
	オーストラリア大使館の政治担当公示参事官、クレア・エリアス氏の発表
	二国間および多国間協力
	• 日本との協力
	○ クワットのフレームワーク内での作業
	○ オーカスの枠組みでの協力
	○ 貿易関連および R&D の協力
	○ 大学間の R&D 協力（国家安全保障に関するもの）
	サイバーエンゲージメント
	• 昨年の成果
	○ 日豪で記録的な年
	○ 規制改革および法律の改革
	○ サイバー犯罪および国家主体の攻撃への対処
	• サイバー脅威の現状
	○ ランサムウェアなどのツールの拡大
	○ 犯罪者の増加
	○ 法執行機関および制裁による対策の難しさ
	サイバーセキュリティ戦略
	• オーストラリアのサイバー戦略
	○ 6 つのサイバーシールド
	▪ ビジネスと市民の強化
	▪ 安全なテクノロジー
	▪ 世界最高の脅威情報共有
	▪ 重要インフラの防御
	▪ ソブリンケーパビリティ
	▪ グローバルリーダーシップ
	• 投資と協力
	○ 約 100 億の投資（ソブリンオフェンシブ、ディフェンシブ、サイバーインテリジェンス）
	○ 政府、研究者、民間の協力
	○ サイバースレッドインテリジェンスシェアリングプラットフォ

- Trade and Investment: Increasing trade and investment between Australia and Japan, especially in research and development in national security and dual-use areas.

Cyber Challenges and Threats

- Current Landscape:
  - Record year of cyber engagement between Australia and Japan.
  - Challenges:
    - Increase in cybercrime and state actors using cyber domains for coercion.
    - Expansion of malicious cyber actors due to availability of online tools and services.
    - Limited effectiveness of law enforcement and sanctions due to safe havens for malicious actors.
  - Technology Design: Current technology design and deployment decisions have contributed to these challenges.

Digital Dependencies and National Security

- Interconnection: Digital dependencies intersect with national and economic security.
- Emerging Technologies: Challenges and opportunities posed by generative AI and quantum technology.

Australia's Cyber Security Strategy Overview

- Launch: Strategy launched a year ago.

ーム（CTIS）

法律および規制の改正

- ランサムウェアの支払い報告の義務化
  - 無過失責任のタイプのレポート
  - 支払いの理解のための情報収集
- 重要インフラの要件強化
  - 医療、電気通信など 11 のセクター
  - 弁護士事務所、コンサルタント企業なども対象

日本との協力

- サイバー抗議のアトリビューション
  - ジョイントアトリビューション
  - APT40 のテクニカルアドバイザリー
- 政府システムの強化
  - セキュアクラウドなどのフォーマット
  - 外務省のスパイ行為対策
- 太平洋当初国の課題
  - サイバー攻撃への対処
  - 外務大臣および国防大臣の協力

民間企業の役割

- オーストラリア企業の活躍
  - サイバーセキュリティおよび情報セキュリティの強化

アクションアイテム

[ ] ランサムウェアの支払い報告の義務化に関する詳細な情報収集

[ ] 重要インフラの要件強化に関する法案の作成

[ ] サイバースレッドインテリジェンスシェアリングプラットフォーム（CTIS）の運用強化

[ ] ジョイントアトリビューションのプロセスの明確化

[ ] 政府システムのセキュリティ強化策の実施

• Approach: Whole-of-nation approach to building resilience.
• Six Cyber Shields:
  ○ Strong businesses and citizens.
  ○ Safe technology.
  ○ World-class threat sharing and blocking.
  ○ Protected critical infrastructure.
  ○ Sovereign capabilities.
  ○ Building a resilient region.
Investment and Collaboration
• Investment: $10 billion investment in sovereign offensive, defensive, and cyber intelligence capabilities (Red Spice).
• Collaboration:
  ○ Government, researchers, and private sector collaboration.
  ○ Australian Cyber Security Center provides intelligence and threat briefings.
  ○ Cyber Threat Intelligence Sharing Platform (CTIS) for real-time sharing of indicators of compromise.
Legislative Reforms
• Need for Evolution: Legislative settings must keep pace with evolving cyber threats.
• Recent Reforms:
  ○ Mandatory Reporting: Reporting of ransomware payments.	

○ Limited Use Protections: Protections for voluntary reporting from private sector. ○ Mandatory Standards: Security standards for Internet of Things (IoT) devices. ○ Cyber Incident Review Board: No-blame post-incident reviews for massive cyber breaches. **Public-Private Partnerships** **Critical Infrastructure** • Strengthened Requirements: Now includes sectors like health, medical care, and telecommunications. • Legislation: Upcoming legislation to cover secondary systems holding sensitive data. • Public-Private Playbooks: Development of playbooks for better preparedness. **Norms and Attributions** • Joint Attribution: Success of joint attribution and technical advisory in relation to APT40. • Government Systems: Sharing information on hardening government systems with Japan. **Regional Cooperation** • Pacific Island Nations: Building resilience in small government systems facing cyber attacks. • Foreign and Defence Ministers: Commitment to an expansive and deep agenda. **Business Engagement**	

• Australian Companies: Increasing involvement in supporting cyber security and information security uplift in Japan. **Action Items** [ ] Discuss government cloud migration and government cloud at a panel with the Digital Agency and CyLogic.	

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

Robbert Anderson (Deputy Head of Mission and Head of PPC, the Kingdom of the Netherlands to Japan)	ロブ・アンダーソン (駐日オランダ王国大使館全権公使)
Cyber Strategy, Internet Governance, Freedom Online Coalition **Theme** This speech, held on October 30, 2024, at Keio University, covered the Netherlands' international cyber strategy for 2023-2028, emphasizing the need for a borderless response to cyber threats. Key objectives include combating cyber threats, reinforcing democratic principles online, and maintaining a secure internet. The speech also highlighted the Freedom Online Coalition's efforts and the importance of multistakeholder involvement in internet governance. **Takeaways** 1. Introduction and greetings to Keio University professors and staff. 2. Acknowledgment of the 14th symposium and support from the Netherlands government. 3. Delegation includes colleagues from the Ministry of Foreign Affairs and the Dutch Institute of Vulnerability Disclosure. 4. Cyber threats are borderless and require a borderless response. 5. Netherlands' international cyber strategy launched last year with three objectives for 2023-2028. 6. First objective: Combat cyber threats posed by states and criminals. 7. Second objective: Reinforce democratic	サイバー脅威, インターネットの自由, インテリジェンス能力 **テーマ** この講演では、サイバー脅威に対抗するための対策、民主的及び人権の原則のオンライン強化、オープンで自由でセキュアなインターネットの維持について議論されました。特に、オランダ政府のインテリジェンス能力への投資や外交ネットワークの強化、新しい国際連携の構築が強調されました。 **要点** 1. サイバー脅威と戦うための対策 2. 民主的及び人権の原則のオンライン強化 3. オープンで自由でセキュアなインターネットの維持 4. オランダ政府のインテリジェンス能力への投資 5. 外交ネットワークの強化 6. 新しい国際連携の構築 7. フリーダムオンライン連合の活動 8. インターネットの自由の制約 9. インド太平洋地域からの新たなパートナーの迎え入れ 10. マルチステークホルダーのコミュニティを通じたインターネットガバナンス **ハイライト** • "サイバーというのは国境がないわけです。"-- ロブ・アンダーソン **章とトピック** **サイバー脅威と戦うための対策** サイバー脅威に対抗するためにオランダ政府が取る対策についての説明。 • **要点** ○ インテリジェンス能力への投資 ○ 外交ネットワークの強化

and human rights principles online. 8. Third objective: Maintain a globally interconnected, open, free, and secure internet. 9. Investment in intelligence capabilities and diplomatic network. 10. Move from reactive to proactive strategic approach to cyber threats. **Highlights** • "Cyber is borderless, and so should our response to threats be." **Chapters & Topics** **Netherlands' International Cyber Strategy** The Netherlands launched its international cyber strategy last year with three main objectives for the period of 2023 to 2028. • **Keypoints** ○ Combat cyber threats posed by states and criminals. ○ Reinforce democratic and human rights principles online. ○ Maintain a globally interconnected, open, free, and secure internet. **Freedom Online Coalition** The Freedom Online Coalition was established by the Netherlands 12 years ago and consists of 41 countries today. It campaigns for the recognition of human rights online. • **Keypoints** ○ Issues joint statements in areas where no international consensus has been reached. ○ Netherlands is chairing the coalition this year. ○ Looking to expand membership with new partners from the Indo-Pacific. **Internet Governance** The Netherlands considers the active involvement of the multistakeholder community in discussions on Internet governance a high priority. • **Keypoints**	○ 新しい国際連携の構築 **民主的及び人権の原則のオンライン強化** オンライン上での民主的及び人権の原則を強化するための取り組み。 • **要点** ○ フリーダムオンライン連合の活動 ○ インターネットの自由の制約に対する対応 **オープンで自由でセキュアなインターネットの維持** 世界的に総合接続されたオープンで自由でセキュアなインターネットを維持するための目標。 • **要点** ○ マルチステークホルダーのコミュニティを通じたインターネットガバナンス **宿題と提案**

○ Engagements with governments, private industry, the technical community, and academia. **Assignments & Suggestions**	

1.15 D1-R4-7 Remarks from each of the governments and United Nations

Peter Loeffelhardt (Minister, Head of Economic and Scientific Department, German Embassy)	ペーター・レフェルハルト (ドイツ大使館 経済・科学部門長)
Cybersecurity, International Cooperation, Germany **Theme** This speech, held on October 30, 2024, focused on the increasing cybersecurity threats due to global conflicts and hybrid warfare. Key takeaways included the importance of international cooperation, Germany's efforts to enhance national cyber resilience, and the significance of technological and digital sovereignty. Germany's initiatives in regulating 5G network components, collaborating with Japan on 6G networks, and supporting cyber capacity building in various regions were also highlighted. **Takeaways** 1. Cybersecurity threats are increasing due to global conflicts and hybrid warfare. 2. International cooperation is essential to mitigate cyber threats. 3. Germany is working to increase national cyber resilience and invest in cyber capacity building. 4. Technological and digital sovereignty is crucial for reducing dependencies and protecting critical infrastructure. 5. Germany has regulated the use of critical components from untrusted suppliers in 5G networks. 6. Germany is collaborating with Japan to establish a secure 6G network. 7. Transparency and calling out malicious behavior in cyberspace are important. 8. Germany has published results of its	サイバーセキュリティ, ハイブリッド戦争, 5G ネットワーク **テーマ** この講演では、サイバーセキュリティの重要性、ハイブリッド戦争の脅威、ドイツのサイバー戦略、サイバーリスクの増加、国家のサイバー強靭性の強化、サイバーキャンバシティビルディングへの投資、イノベーションと技術の重要性、重要インフラの保護、5G ネットワークの安全性、国際的な協力の必要性について議論されました。 **要点** 1. サイバーセキュリティの重要性 2. ハイブリッド戦争の脅威 3. ドイツのサイバー戦略 4. サイバーリスクの増加 5. 国家のサイバー強靭性の強化 6. サイバーキャンバシティビルディングへの投資 7. イノベーションと技術の重要性 8. 重要インフラの保護 9. 5G ネットワークの安全性 10. 国際的な協力の必要性 **ハイライト** • "協力的に皆で協力しなければこういったものを緩和していくことはできません。"-- ピーター・レーペルハート **章とトピック** **サイバーセキュリティの重要性** サイバー攻撃の脅威が増加しているため、サイバーセキュリティの強化が必要である。 • **要点** ○ 官、民、一般市民社会、様々な機関がサイバー攻撃にさらされている。 ○ ハイブリッド戦争の脅威が 21 世紀においてさらに深刻化している。 **ドイツのサイバー戦略** ドイツにおけるサイバー戦略の重要性とその取り組み。

national attribution process to hold states responsible for cyberattacks.

9. Germany focuses on cyber capacity building in Ukraine, Moldova, Armenia, the Western Balkans, and Africa.
10. Japan works with Australia to strengthen cybersecurity in the Pacific.

Highlights

- "Only together can we make the world a safer place."-- Mr. Loffelholt

Chapters & Topics

Cybersecurity Threats

The increasing threats in cyberspace due to global conflicts and hybrid warfare.

- **Keypoints**
  - Espionage, sabotage, manipulation, and disinformation are objectives of hostile actors.
  - Cyber incidents in Germany are increasing in both severity and frequency.

International Cooperation

The necessity of international cooperation to mitigate cyber threats.

- **Keypoints**
  - Germany collaborates with partners and allies in the EU, NATO, and the Indo-Pacific.
  - Transparency and calling out malicious behavior are important tools.

National Cyber Resilience

Germany's efforts to increase national cyber resilience.

- **Keypoints**
  - Investing in cyber capacity building to empower other states.
  - Reducing dependencies on critical infrastructure and components.

Technological and Digital Sovereignty

The importance of technological and digital sovereignty for national security.

- **Keypoints**
  - Germany's regulation on the use of critical

- **要点**
  - サイバーリスクがドイツ企業にとって最大のビジネスリスクとなっている。
  - 国家のサイバー強靭性を強化し、他国の能力も向上させる必要がある。

5G ネットワークの安全性

5G ネットワークにおける安全性の確保と信頼できない政府からのコンポーネントの排除。

- **要点**
  - 6 月に信頼できない政府からの 5G ネットワークコンポーネントの使用を禁止する法案を提出。
  - パートナーや同盟国、特に日本やオーストラリアと協力して進める。

宿題と提案

components from untrusted suppliers in 5G networks. ○ Collaboration with Japan to establish a secure 6G network. **Cyber Capacity Building** Germany's focus on cyber capacity building in various regions. • **Keypoints** ○ Support to Ukraine through the Tallinn Mechanism. ○ Capacity building efforts in Ukraine, Moldova, Armenia, the Western Balkans, and Africa. **Assignments & Suggestions**	

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

Margiris Abukevičius (Defence Adviser to Japan and MOD Representative for Indo-Pacific, Lithuanian Embassy to Japan)	マルギリス・アブケヴィチュス（駐日リトアニア共和国大使館防衛顧問 兼 インド太平洋担当防衛省代表）
Overview This speech summarizes the key points from a meeting held on 2024-10-30 regarding Lithuanian engagement in cybersecurity, particularly focusing on partnerships with Japan and the Indo-Pacific region. The discussion covered strategic partnerships, cyber initiatives, information sharing, and the global cyber threat landscape. Action items were identified to enhance cooperation and security measures. **Opening Remarks** • **Introduction and Acknowledgment** ○ Mr. Aboukeviches congratulated for the 14th iteration of the conference. ○ Recognition of the Lithuanian embassy and government's support for the conference. **Lithuanian Engagement with Japan and Indo-Pacific Region** • **Strategic Partnership and Cooperation** ○ Two years ago, Lithuanian and Japanese prime ministers upgraded cooperation to a strategic partnership.	**大使館防衛顧問兼インド太平洋担当防衛省代表、マルギリス・アブケ・ウィチュス様の発言** **開会の挨拶とお祝いの言葉** • 第 14 回目の開催を祝福。 • サイバーの重要性が認識されていなかった頃からの継続的な会議開催を称賛。 • 参加の喜びと重要性を強調。 **参加の理由と貢献** • **リトアニアと日本の関係強化** ○ リトアニアと日本、その他の地域の同志国との関係が深まっている。 ○ 防衛協力の合意が進展。 ○ 大使館設置や太平洋戦略の推進。 • **サイバーおよび経済安全保障** ○ サイバー分野やその他の安全保障分野での連携強化を目指す。 **リトアニアの国際的な取り組み** • **国際志向と地域連携** ○ リトアニアは国際志向が強く、いくつかのイニシアティブを進めている。 ○ 9 月にリトアニアと日本のイベントを開催し、将来の協力の土台を築いた。 • **サイバーチャンピオンネットワーク**

○ Signed a cooperation agreement on security and defense. ○ Exchange of defense representatives. ○ Opening of four embassies in the region. ○ Launch of the Indo-Pacific strategy. • **Core Areas of Engagement** ○ Focus on cyber and economic security. ○ Building security and defense relationships. ○ Exploring collaborative opportunities in various security fields. **Cyber Initiatives and Cooperation** • **Lithuanian-Japan Cyber Dialogue** ○ Hosted the first Lithuanian-Japan Cyber Dialogue in September. ○ Basis for future cooperation in cyber policy. • **Cyber Champions Network and Summit** ○ Initiated in Vilnius, Lithuania. ○ First meeting held this year, second summit hosted in Sydney. ○ Next summit scheduled in Seoul. ○ Platform for NATO and Indo-Pacific cyber communities to discuss cyber issues. • **Practical Cooperation and Exercises** ○ Japanese team to participate in the biggest Lithuanian cyber exercise next month. ○ Lithuanian team participated in a cyber exercise in Japan this year. ○ Plans to increase cooperation within NATO exercises. **Information Sharing and Regional Cyber Defense** • **Importance of Information Sharing** ○ Critical for effective cyber defense. ○ Working with Japan and like-minded countries in the Indo-Pacific. ○ Regional cyber defense center as a platform for information exchange. • **Focus on Malicious Activities**	○ 昨年リトアニアで開始。 ○ 今年はシドニーで第 2 回目のサミットが開催。 ○ 来年はソウルで開催予定。 ○ NATO のサイバーコミュニティと太平洋のコミュニティが集まる場として利用。 • **実践的な協力** ○ 日本と共同でサイバー演習を実施。 ○ 来月、日本で大規模なサイバーエクササイズにリトアニアも参加予定。 ○ NATO のエクササイズにも参加。 **情報共有と地域的なプラットフォーム** • **情報共有の重要性** ○ 日本および同志国と太平洋地域での情報共有を推進。 ○ 数年前はロシアの攻撃に焦点を当てていたが、現在は中国のサイバー活動にも注目。 • **地域的なプラットフォーム** ○ ウクライナ、ポーランド、チェコ共和国などが参加。 ○ 日本にも正式に参加を依頼。 **サイバー問題と国際情勢** • **国際規則の違反** ○ ロシア、中国、北朝鮮による国際規則の違反が頻発。 ○ サイバー協力の強化が必要。 • **サイバー防御の強化** ○ 国家のサイバー能力を強化し、同盟国間での協力を進める。 ○ プロアクティブなサイバーディフェンスの実現が重要。 • **テクノロジーとサプライチェーンの保護** ○ セキュアな技術の展開とサプライチェーンの保護が必要。 ○ 5G に関して、中国やロシアの技術展開を阻止するための手段を追求。 **今後の議論とサポート** • 今後の議論に期待。 • 既に多くの良いアイデアを拝聴。 • イニシアティブの継続的なサポートを表明。 **Action Items** [ ] 日本での大規模なサイバーエクササイズへの参加準備 [ ] 日本のサイバーコミュニティとの情報共有の強化 [ ] 日本の地域的なプラットフォームへの正式参加の手続

○ Initially focused on Russian cyber activities. ○ Now also addressing Chinese cyber activities. ○ Collaboration with the U.S., Ukraine, Poland, Czech Republic, and invitation to Japan to join the platform. **Realistic Assessment of Cyber Threats** • **Global Cyber Threat Landscape** ○ International rules and institutions are being violated by autocratic regimes like Russia, China, North Korea, and Iran. ○ Cyber tools used against like-minded countries for many years. • **Need for Enhanced Cyber Cooperation** ○ Importance of stepping up cyber cooperation among countries. ○ Need to increase national cyber capacity and work with partners. ○ Proactive response to cyber threats. ○ Deployment of secure technologies and securing supply chains. **Action Items** [ ] Increase cooperation within NATO cyber exercises. [ ] Invite Japan to formally join the regional cyber defense platform. [ ] Focus on deploying secure technologies and securing supply chains.	き [ ] プロアクティブなサイバーディフェンスの実現に向けた具体的な計画策定 [ ] 5G 技術展開に関するセキュリティ対策の強化

1.17 D1-R4-11 Remarks from each of the governments and United Nations

Oliver Ait (Business and Investments Officer, Embassy of Estonia in Tokyo)	オリバー・エイト (駐日エストニア共和国大使館 ビジネス・投資担当官)
Brief Overview: This speech contains the notes from a conference held on 2024-10-30. It includes opening remarks by Mr. 8, discussions on the current geopolitical context, the evolution of conference topics, and detailed sections on digitalization and cybersecurity cooperation between Japan and Estonia. The document concludes with an action items section, which currently has no specific	**開会の挨拶** • 主催者および参加者への感謝の意を表明。 • ビデオスピーチの予定だったが、直接参加して話すことに。 **世界的な状況と国防協力** • **ロシアのウクライナ侵入** ○ 世界的な状況の中で国防協力の重要性が増している。 ○ 戦争はハイブリッド戦争の形態を取っており、情報

tasks listed.

Opening Remarks

- **Acknowledgments:**
  - Thanked guests and organizers for the opportunity and the importance of the conference.
  - Mentioned initial plans for a video speech but expressed happiness to take the stage in person.

Current Geopolitical Context

- **Russian Invasion in Ukraine:**
  - Highlighted the need for increased concentration due to the ongoing conflict.

Evolution of Conference Topics

- **Historical Perspective:**
  - Earlier conferences had narrower topics.
  - Over the years, topics have become more focused yet broader and inclusive.
- **Future Security Dialogue:**
  - Expressed hope for the next security dialogue to take place soon.

Digitalization and Cybersecurity Cooperation

- **Memorandum of Understanding (MOU) in 2022**
  - **Signatories:**
    - Dr. Makishima Karen (Digital Minister, Japan)
    - Estonian Ministry of Economics
  - **Purpose:**

戦、サイバー戦、物理戦闘が複雑に絡み合っている。

日本のサイバーセキュリティ政策

- **近代化と国家安全保障**
  - 日本はサイバーセキュリティ政策を近代化。
  - 2022 年に国家安全保障の枠組みを改定し、サイバー貿易を初めて含めた。
  - 新しい国家安全保障には情報戦やアクティブサイバーディフェンスも含まれている。

エストニアのサイバーセキュリティ

- **サイバー脅威への対応**
  - エストニアは長い間サイバー脅威にさらされてきた。
  - 新しいイニシアティブとして、ウクライナへのサイバー支援を強化。
  - 特にウクライナの民間領域のサイバー支援を強化する「タリンメカリズム」を 2023 年 10 月 20 日に発表。

エストニアと日本の二国間協力

- **サイバーダイアローグ**
  - 2014 年に第一回日本エストニアサイバーダイアローグがタリンで開催。
  - 10 年間で議論が焦点を絞りつつも広範囲でインクルーシブルなものに進化。
  - 来年もセキュリティサイバーダイアローグが開催予定。
- **デジタル分野の協力**
  - 2022 年、エストニアを公式訪問したマルクス・カレンデジタル担当大臣がエストニアの経済通信省とデジタル分野における協力貿易の覚書を締結。
  - デジタル化について両政府が何を学び合えるか、協力できるかを話し合うためのもの。

日本の国際協力

- **NATO との協力**
  - 2022 年に国防省が正式に NATO の協力サイバー貿易 COE に参加。
  - 日本が NATO のロックシールドの演習に 2020 年に参加し、エストニアと協力して仮想敵国に対する実践的な演習を実施。
- **エストニア企業との協力**
  - エストニアの企業（例：CybExer）は高度なサイバー脅威からチームを守るためのサイバーレンジプラットフォームを提供。

▪ Cooperation on digitalization. ▪ Mutual learning and societal digitalization. ○ **Outcome:** ▪ Digital agency sent an expert to Estonia to analyze Estonia's iVoting system. ▪ Emphasis on the need for proper cybersecurity and cyber defense. • **International Center for Defense and Security Report (2020)** ○ **Title:**"So Far, Yet So Close: Japanese-Estonian Cybersecurity Policy Perspectives and Cooperations" ○ **Authors:**Professors from Japan and Estonia ○ **Focus:** ▪ Areas of cooperation. ▪ Identification of challenges. • **Japan's Participation in NATO Cooperative Cyber Defense Center of Excellence (2022)** ○ **Location:**Tallinn ○ **Activities:** ▪ Collaboration with international partners to respond to cyber threats. ▪ Participation in NATO's Lock Shields exercise,	**Action Items** [ ] 来年のセキュリティサイバーダイアローグの開催準備 [ ] ウクライナへのサイバー支援の強化 [ ] エストニアと日本のデジタル分野における協力貿易の覚書の実施 [ ] NATO の協力サイバー貿易 COE への参加活動の継続 [ ] エストニア企業とのサイバーレンジプラットフォームの導入検討

simulating a war game against a fictional country.
• **Practical Cooperation**
  ○ **Estonian Companies:**
  ▪ Example: Cybexer, involved in cooperation and activities in the United States.
Action Items
[ ] None mentioned.	

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

Izumi Nakamitsu (Under-Secretary-General and High Representative for Disarmament Affairs, United Nations)	中満 泉 (国際連合事務次長・軍縮担当上級代表)
Brief Overview: This speech contains the notes from the 14th International Cybersecurity Symposium held on October 30, 2024. The symposium, organized by Keio University and Mitre Corporation, featured discussions on cybersecurity strategies, digital transformation, multi-stakeholder collaboration, and the United Nations' efforts to ensure a secure digital future. The document also includes a consolidated section of action items derived from the symposium. **Opening Remarks** • **Introduction** ○ Addressed by Undersecretary General Nakamitsu via video message. ○ Honored to speak at the 14th International Cybersecurity Symposium, organized by Keio University and Mitre Corporation. ○ This is the fourth time addressing this forum. **Cybersecurity Strategy Reflecting Digital Dependencies** • **Importance of the Theme** ○ Timely theme focusing on national	**概要** この講演は、2024 年 10 月 30 日に開催された第 14 回サイバーセキュリティ国際シンポジウムの内容をまとめたものです。シンポジウムでは、デジタル変革の進展とその影響、ステークホルダーの役割、国連の取り組みなどが議論されました。特に、グローバルデジタルコンパクトの採択とその将来の展望についての議論が行われました。最後に、シンポジウムでの議論を基にしたアクションアイテムがまとめられています。 **開会の挨拶** **中満泉様のビデオメッセージ** • **参加者への感謝**: ○ 慶應大学及びマイターコーポレーションへの感謝。 ○ 「このような形でご挨拶申し上げるのは 4 回目のことです。また再びこのようなマルチステークホルダーのグループの皆様方に対して挨拶ができて嬉しく思います。」 **シンポジウムのテーマ** • **テーマの重要性**: ○ 国家安全保障、経済安全保障、社会保障のサイバーセキュリティ戦略。 ○ ステークホルダーの対話の重要性。 **デジタル変革とその影響** **デジタル変革の進展** • **影響範囲**: ○ 個人、地域社会、国家経済、政府に影響。

security, economic security, and social security.

- Emphasis on the critical nature of security stakeholder dialogues in tackling cybersecurity challenges.

Digital Transformation

- **Opportunities**
  - Digital transformation offers states the ability to serve citizens more efficiently and effectively.
  - Opens new avenues for economic growth and development.
- **Risks**
  - Increased interconnectedness brings new vulnerabilities and risks.
  - Growing dependence on digital technologies necessitates protection of essential systems from interference and exploitation.

Multi-Stakeholder Collaboration

- **Private Sector**
  - Crucial in developing ICT infrastructure.
- **Academia and Legal Experts**
  - Provide valuable commentary and solutions to challenges in cyberspace.
- **Non-Governmental Stakeholders**
  - Their role in finding solutions cannot be overstated.
  - The symposium exemplifies important collaboration between these groups.

United Nations' Efforts

- **Global Digital Compact**
  - Encouragement to consider how the Global Digital Compact can support individual and collective work.
- **Summit of the Future**
  - Last month, world leaders gathered for a one-day symposium at the Summit of the Future.
  - Adoption of a path to address existing and potential threats posed by emerging technologies, including their misuse.

- 「急速にデジタル変革というものが進んでおり、社会のあらゆるレベルで影響が現れております。」

デジタルイノベーションの利点とリスク

- **利点**:
  - 効率的で効果的なサービス提供。
  - 新しい経済成長及び開発の手段。
- **リスク**:
  - 新しい脆弱性及びリスクの出現。
  - 「デジタルテクノロジー及びサイバー空間に依存すると、我々が重要なシステムというものを干渉及び悪用から守らなければなりません。」

ステークホルダーの役割

各ステークホルダーの貢献

- **民間セクター**:
  - ICT インフラストラクチャーの開発。
- **学会**:
  - 貴重なコメントの提供。
- **法律の専門家及び NGO**:
  - 大きな貢献。

シンポジウムの意義

- **コラボレーションの例**:
  - 各当事者のコラボレーションの良い例。
  - オープンでセキュアで安定したアクセス可能な平和な ICT 環境の実現に貢献。

国連の取り組み

グローバルデジタルコンパクト

- **サミットの結果**:
  - 新しいグローバルデジタルコンパクトの採択。
  - 「オープンで自由でセキュアで人間中心のデジタルの将来の共通のビジョン」というテーマ。
  - 人権及び SDG が根底にある。

将来の展望

- **脅威への対応**:
  - 振興技術による脅威への対応策。
- **国連の協力**:
  - 平和と安全保障のためのデジタル未来への協力。

Action Items

[ ] グローバルデジタルコンパクトがいかに皆様方をサポートすることができるか検討。

• **Commitment** ○ The United Nations remains a steadfast partner in safeguarding the peace and security of our digital future. **Action Items** [ ] Consider how the Global Digital Compact can support individual and collective work.	

1.19 D1-S5 Keynote Speech from Japanese Industry

Jun Sawada (Chairman, NTT)	澤田 純 (NTT 取締役会長)
Cyber Security, System Integration, Japan **Theme** The speech discusses the challenges faced by NTT.com as a subsidiary of NTT Group, the integration of local government systems into a government cloud, and the difficulties in integrating disparate systems and EDI systems from various manufacturers. It also covers the slow progress of the free data flow initiative announced by former Prime Minister Abe and the importance of establishing a trust platform for government and private sectors. **Takeaways** 1. Challenges faced by NTT.com as a subsidiary of NTT Group. 2. Integration of 1,800 local government systems into a government cloud in Japan. 3. Disparate systems totaling 35,000 making integration difficult. 4. 50% usage of e-medical records in Japan. 5. Difficulties in integrating different EDI systems from various manufacturers. 6. Dependence on paper-based systems during COVID-19 at airports. 7. Integration of My Number card and health insurance certificate since last year. 8. Issues and confusion caused by the integration of My Number card and health insurance certificate. 9. Initiative of free data flow announced by former Prime Minister Abe in 2012.	セキュリティオペレーションセンター，デジタル化，データシステム **テーマ** この講演では、セキュリティオペレーションセンターの重要性、IT システムの標準化と統一の必要性、日本の地方公共団体のデジタル化の現状、病院の電子カルテの普及状況、EDI と POS システムの統合の難しさ、コロナ禍でのシステム対応の課題、マイナンバーカードと保険証の連携問題、DFFT の進展と課題、ヨーロッパとアメリカのデータシステムの現状、データスペースの 3 レイヤーモデルについて議論されました。 **要点** 1. セキュリティオペレーションセンターの重要性 2. IT システムの標準化と統一の必要性 3. 日本の地方公共団体のデジタル化の現状 4. 病院の電子カルテの普及状況 5. EDI と POS システムの統合の難しさ 6. コロナ禍でのシステム対応の課題 7. マイナンバーカードと保険証の連携問題 8. DFFT の進展と課題 9. ヨーロッパとアメリカのデータシステムの現状 10. データスペースの 3 レイヤーモデル **ハイライト** • "相互接続、いわゆる英語で言うコネクト。コネクトをするためには、あらゆるものをつないでいこうとするためには、やっぱりトラストというのがいるようになります。" **章とトピック** **セキュリティオペレーションセンターの重要性** セキュリティオペレーションセンター（SOC）は、パッチのリリース後に攻撃が増加することを監視し、対応する役割を果たす。 • **要点** ○ パッチリリース後の攻撃増加の監視

10. Slow progress of the free data flow initiative.

Highlights

- "Cyber security may open to the trust relationship."-- Mr. Sawada

Chapters & Topics

Challenges in Cyber Security and System Integration

The speech discusses various challenges faced in the field of cyber security and system integration, particularly in Japan.

- **Keypoints**
  - NTT.com faced numerous challenges as a subsidiary of NTT Group.
  - Japan's initiative to integrate 1,800 local government systems into a government cloud is hindered by 35,000 disparate systems.
  - Only 50% of e-medical records are used, including individual clinics.
  - Different manufacturers provide different EDI systems, complicating integration.
  - During COVID-19, reliance on paper-based systems at airports highlighted the lack of digitization.
- **Examples**
- Since last year, Japan started integrating the My Number card with health insurance certificates to streamline medical treatment certification from local clinics. However, this led to significant trouble and confusion due to system connectivity issues.
  - The system was expected to connect seamlessly, but it did not.
  - Manual labor was often required despite the adoption of digital systems.

Free Data Flow Initiative

The initiative for free data flow, announced by former Prime Minister Abe in 2012, aims to facilitate the free and trusted flow of data.

- **Keypoints**
  - SOC の役割と重要性

IT システムの標準化と統一の必要性

IT システムの標準化と統一は、セキュリティ管理と運用の効率化に寄与する。

- **要点**
  - 標準化のメリット
  - 統一の重要性

日本の地方公共団体のデジタル化の現状

日本の地方公共団体はデジタル庁を中心に政府クラウドへの移行を進めているが、システムの統合には課題が残る。

- **要点**
  - デジタル庁の役割
  - 政府クラウドへの移行状況

病院の電子カルテの普及状況

日本の病院では電子カルテの導入が進んでいるが、町医者を含めると普及率は 5 割にとどまる。

- **要点**
  - 電子カルテの普及率
  - 町医者の状況

EDI と POS システムの統合の難しさ

EDI と POS システムは業界別に異なる仕様があり、統合が難しい。

- **要点**
  - EDI の業界別仕様
  - POS システムのメーカー別仕様

コロナ禍でのシステム対応の課題

コロナ禍では、すべての自治体に対応できるシステムの構築が困難であった。

- **要点**
  - システム対応の遅れ
  - 自治体間の連携不足

マイナンバーカードと保険証の連携問題

マイナンバーカードと保険証の連携には、インターネット経由での認証が必要だが、多くのトラブルが発生している。

- **要点**
  - 認証システムの問題
  - NTT 東西の対応

DFFT の進展と課題

DFFT（データフリーフローウィズトラスト）は進展しているが、まだ課題が多い。

- **要点**
  - DFFT の概要

○ The progress of the initiative has been slow. ○ Europe's Gaia-X and other credit card initiatives are comprehensive but not fully effective. ○ Keidanren proposed an industry data space model for more realistic application. **Trust Platform for Government and Private Sectors** Establishing a trust platform is crucial for promoting government cloud actions and interconnection with other Asian nations. • **Keypoints** ○ A trust platform is imperative for both government and private sectors. ○ Government cloud actions are expected to start in April. ○ Interconnection with other Asian nations is necessary for comprehensive governance. **Assignments & Suggestions**	○ 進展状況と課題 **ヨーロッパとアメリカのデータシステムの現状** ヨーロッパは Gaia-X を中心にデジュール的にシステムが進展しており、アメリカはデファクトで多くのシステムが動いている。 • **要点** ○ Gaia-X の概要 ○ アメリカのデファクトスタンダード **データスペースの 3 レイヤーモデル** データスペースの 3 レイヤーモデルに基づき、異なるシステムを相互接続するモデルが重要である。 • **要点** ○ 3 レイヤーモデルの概要 ○ 相互接続の重要性 **トラストプラットフォームの重要性** トラストプラットフォームは、データの自由な流通を支える基盤として重要である。 • **要点** ○ トラストプラットフォームの役割 ○ データ流通の基盤 **システムの相互接続の必要性** 多様なシステムを統合するためには、相互接続が不可欠である。 • **要点** ○ 相互接続のメリット ○ 統合の必要性 **AI の相互接続とガバナンス** AI のガバナンスには、AI 同士の相互接続が重要である。 • **要点** ○ AI の相互接続の必要性 ○ AI ガバナンスの方法 **コネクトの重要性** あらゆるものをつなぐためには、トラストが必要であり、コネクトの基盤となる。 • **要点** ○ コネクトの定義 ○ トラストの役割 **宿題と提案**

1.20 D1-S6 Keynote Speech: National Security

ADM(Ret.) Dennis Blair (Former Director of U.S. National Intelligence)	デニス・ブレア (元米国国家情報長官)
Cybersecurity, Japan, National Security	サイバーセキュリティ 国際協力 日本の対応

Theme

This speech discusses the interconnectedness of national security and cybersecurity, focusing on Japan's recent cybersecurity breaches and the involvement of hostile nations. It highlights the expanding cyber attack surface due to new technologies like AI, IoT, 5G, and 6G, and emphasizes the need for Japan to enhance its cybersecurity measures and international cooperation. The speech also addresses the importance of implementing previous cybersecurity recommendations and the necessity of clear authorities, legal frameworks, and resources for effective cybersecurity.

Takeaways

1. National security and cybersecurity are interconnected.
2. Japan has faced significant cybersecurity breaches in the past year.
3. Hostile nations are collaborating with criminal organizations to conduct cyber attacks.
4. The cyber attack surface is expanding with new technologies like AI, IoT, 5G, and 6G.
5. Economic and personal data vulnerabilities can become national security threats.
6. Japan needs to enhance its cybersecurity measures and international cooperation.
7. Previous recommendations for Japan's cybersecurity have not been fully implemented.
8. Political challenges should not hinder cybersecurity advancements.
9. Clear authorities and legal frameworks are necessary for effective cybersecurity.
10. Resources, both human and financial, are crucial for cybersecurity.

Highlights

- "Japan simply must do much more to defend itself, even as it increases its cooperation and partnership with many

視点

- **サイバーセキュリティの現状**
- 日本国内外でサイバー攻撃が増加しており、特に交通システムや政府組織が狙われている。
- **国際的な協力**
- 敵対的な国家や犯罪組織が連携して攻撃を行っているため、国際的な協力が必要である。
- **技術の進展と脅威の増大**
- AI、IoT、5G、6G などの技術の進展により、攻撃対象領域が拡大している。
- **日本の対応**
- 日本はサイバーセキュリティの強化に向けた法的枠組みやリソースの確保が必要である。
- **過去の提言と現状**
- 2 年前の提言が十分に実行されておらず、脅威の拡大に追いついていない。
- **今後の必要な対策**
- ネットワークの強化や包括的な法的枠組みの設置が必要である。

結論

日本はサイバーセキュリティ強化のため、法的枠組みやリソースの確保が必要であり、国際的な協力も重要である。

other countries."-- Admiral Blair **Chapters & Topics** **Interconnection of National Security and Cybersecurity** The relationship between national security and cybersecurity, highlighting how vulnerabilities in cyberspace can impact national security. • **Keypoints** ○ Cyber attacks can target critical infrastructure. ○ Economic and personal data vulnerabilities can be exploited for national security threats. **Cybersecurity Threats to Japan** The specific cybersecurity challenges faced by Japan, including recent breaches and the involvement of hostile nations. • **Keypoints** ○ Recent cyber attacks on transportation centers, government agencies, and the space agency. ○ Hostile nations like China, North Korea, and Russia collaborating with criminal hackers. **Expanding Cyber Attack Surface** The increasing scope of cyber attacks due to advancements in technology. • **Keypoints** ○ New technologies like AI, IoT, 5G, and 6G are expanding the cyber attack surface. ○ Economic and personal data vulnerabilities can be exploited by cyber attackers. **Need for Enhanced Cybersecurity Measures** The necessity for Japan to improve its cybersecurity measures and international cooperation. • **Keypoints** ○ Japan needs to implement more aggressive and comprehensive cybersecurity legislation. ○ International cooperation is essential to	

combat cyber threats. **Implementation of Cybersecurity Recommendations** The status of previous cybersecurity recommendations for Japan and the need for further action. • **Keypoints** ○ Previous recommendations have not been fully implemented. ○ Political challenges should not hinder cybersecurity advancements. **Necessary Resources for Cybersecurity** The importance of clear authorities, legal frameworks, and resources for effective cybersecurity. • **Keypoints** ○ Clear authorities and legal frameworks are necessary. ○ Human and financial resources are crucial for cybersecurity. **Assignments & Suggestions**	

1.21 D1-S8 Keynote Speech: Societal Security

Vinzenz Heußler (Policy Officer, EU Commission)	ヴィンツェンツ・ホイスラー（欧州委員会政策担当官）
cybersecurity, EU legislation, cyber resilience **Theme** This speech, held on October 30, 2024, covers the challenges and threats in cyberspace, the need for a comprehensive approach to cybersecurity, and the impact of global geopolitical tensions. Key topics include the European Union's cybersecurity framework, the NIS2 Directive, the Network code on cybersecurity for cross-border electricity flows, the Cyber Resilience Act, and the Cyber Solidarity Act. The speech also discusses the role of AI in cybersecurity and the Cybersecurity Skills Academy initiative to address the talent gap in the EU. **Takeaways** 1. Challenges and threats in cyberspace 2. Need for a comprehensive approach to	サイバーセキュリティ, EU 戦略, リスク管理 **テーマ** この講演では、サイバーセキュリティの重要性、EU のサイバーセキュリティ戦略、NIS2 指令の改定、サイバーレジリアンス法とサイバーソリダリティ法、サイバーセキュリティのリスク管理、電力業界におけるサイバーセキュリティ、ICT サービスのセキュリティ、サイバーセキュリティアラートシステム、AI とサイバーセキュリティ、サイバースキルアカデミーについて詳しく解説しました。 **要点** 1. サイバーセキュリティの重要性 2. EU のサイバーセキュリティ戦略 3. NIS2 指令の改定 4. サイバーレジリアンス法とサイバーソリダリティ法 5. サイバーセキュリティのリスク管理 6. 電力業界におけるサイバーセキュリティ 7. ICT サービスのセキュリティ 8. サイバーセキュリティアラートシステム 9. AI とサイバーセキュリティ

cybersecurity

3. Rapid technological development and digitalization
4. Impact of global geopolitical tensions
5. Cybercrime as a major threat to society
6. European Union's cybersecurity framework
7. NIS2 Directive
8. Network code on cybersecurity for cross-border electricity flows
9. Cyber Resilience Act
10. Cyber Solidarity Act

Highlights

- "People are key to resilience."

Chapters & Topics

NIS2 Directive

A revised set of rules aiming to strengthen the level of cyber resilience across the EU.

- **Keypoints**
  - Entered into force in January 2023
  - Expands the scope of previous rules
  - Requires entities to deal with cybersecurity risks from the supply chain
  - Allows for coordinated cybersecurity risk assessments of critical supply chains

Network code on cybersecurity for cross-border electricity flows

Aims to establish a recurrent process for cybersecurity risk assessments in the electricity sector.

- **Keypoints**
  - Entered into force in June 2024
  - Complements the NIS2 Directive
  - Focuses on digitalized processes in cross-border electricity flows
  - Includes minimum advanced cybersecurity controls in the supply chain

Cyber Resilience Act

First EU-wide legislation establishing horizontal cybersecurity requirements for hardware and software.

- **Keypoints**

10. サイバースキルアカデミー

ハイライト

- "私たちをさらに増強していくだけでなく、司令によって企業のスポーツをさらに広げ、そしてまたよりハイレベルなサイバーセキュリティの要求事項に対応できるようにしていかなければいけません。"-- ディンセンズ・ホイスラー

章とトピック

サイバーセキュリティの重要性

サイバーセキュリティは、デジタル化が進む現代社会において非常に重要な課題であり、グローバルなセキュリティ環境の変化や技術の進化に対応する必要がある。

- **要点**
  - デジタル化の進展
  - 技術の急速な進化
  - グローバルな知性学的緊張

EU のサイバーセキュリティ戦略

2020 年に欧州委員会が採択したサイバーセキュリティ戦略は、EU 加盟国、市民、企業へのサイバー攻撃の防止、検討、予防を目的としている。

- **要点**
  - サイバー攻撃の防止
  - サイバー攻撃の検知
  - サイバー攻撃の予防

NIS2 指令の改定

ネットワーク情報システムセキュリティ指令（NIS2 指令）は、2023 年 1 月に改定され、EU 全体のサイバーレジリアンスのレベルを向上させることを目的としている。

- **要点**
  - サイバーレジリアンスの向上
  - リスクベースの管理
  - セキュリティ要件の強化

サイバーレジリアンス法とサイバーソリダリティ法

サイバーレジリアンス法とサイバーソリダリティ法は、EU 全域でのサイバーセキュリティの強化を目的として制定された。

- **要点**
  - サイバーレジリアンスの向上
  - サイバーソリダリティの強化
  - 重要インフラの保護

サイバーセキュリティのリスク管理

サイバーセキュリティのリスク管理は、企業のリスクエクスポージャーだけでなく、インシデントによる社会的、経済的影響も考

○ Covers development and entire life cycle of products ○ Requires manufacturers to be transparent about cybersecurity aspects ○ Enhances baseline security of digitalized devices ○ Increases trust among operators **Cyber Solidarity Act** Aims to strengthen EU-level solidarity to better detect, prepare, and respond to cybersecurity threats and incidents. • **Keypoints** ○ Enables information exchange between authorities and relevant entities ○ Creates a cybersecurity emergency mechanism ○ Supports testing for vulnerabilities in critical sectors ○ Establishes a cybersecurity reserve for incident response **AI and cybersecurity** AI can be both a threat and an asset in cybersecurity. • **Keypoints** ○ Used by threat actors for network penetration, data theft, and intelligent viruses ○ AI Act ensures high-risk AI systems are cybersecurity-proof ○ Cybersecurity is an essential requirement for high-risk AI systems **Cybersecurity Skills Academy** A European policy initiative to close the cybersecurity talent gap and strengthen the workforce. • **Keypoints** ○ Aims to improve coordination of existing cyber skills initiatives ○ Addresses the shortage of cybersecurity professionals in the EU ○ Supports the implementation of cybersecurity regulations	慮する必要がある。 • **要点** ○ リスクエクスポージャーの管理 ○ 社会的影響の考慮 ○ 経済的影響の考慮 **電力業界におけるサイバーセキュリティ** 電力業界は、国境を超えた電力供給に重要な影響を持つため、サイバーセキュリティのリスク評価が不可欠である。 • **要点** ○ 電力供給の重要性 ○ リスク評価の必要性 ○ デジタル化の影響 **ICT サービスのセキュリティ** ICT サービスやプロセスの遮断、バックドアの発生、サプライチェーンからの機密情報の漏洩を防止するためのセキュリティ対策が必要である。 • **要点** ○ サービスの遮断防止 ○ バックドアの発生防止 ○ 機密情報の漏洩防止 **サイバーセキュリティアラートシステム** サイバーセキュリティアラートシステムは、ヨーロッパ全体のインフラを守るために情報を共有し、緊急対応を強化することを目的としている。 • **要点** ○ 情報共有の重要性 ○ 緊急対応の強化 ○ インフラ保護 **AI とサイバーセキュリティ** AI は、サイバーセキュリティの脅威を予測し、検知し、その影響を軽減するためのツールとして活用できる。 • **要点** ○ 脅威の予測 ○ 脅威の検知 ○ 影響の軽減 **サイバースキルアカデミー** サイバースキルアカデミーは、サイバースキルのタレントキャップを埋め、成長率、競争力、レジリアンスを向上させることを目的としている。 • **要点** ○ タレントキャップの解消 ○ 成長率の向上

Assignments & Suggestions	○ 競争力の向上 **宿題と提案**

1.22 D1-S9-1 National Security

Satoru Tezuka	手塚 悟
Cyber Security, KEIO JRAMP Cloud, National Security **Theme** This speech emphasized the importance of digital cyber security for national, economic, and societal security. It introduced three essential digital systems: government cloud system, cyber intelligence system, and active defense system. The KEIO JRAMP Cloud, a high-security cloud system equivalent to the U.S. FedRAMP Cloud, was highlighted for its capability to exchange top-secret information. Keio's collaboration with a U.S. company to run this cloud system was also discussed, along with upcoming tutorials and interaction opportunities. **Takeaways** 1. Digital cyber security is crucial for national, economic, and societal security. 2. Three essential digital systems for cyber security: government cloud system, cyber intelligence system, and active defense system. 3. Establishing world-class standards in cyber security is necessary. 4. KEIO JRAMP Cloud is a high-security cloud equivalent to the U.S. FedRAMP Cloud. 5. KEIO JRAMP Cloud enables the exchange of top-secret information digitally. 6. Keio is collaborating with a U.S. company to run the KEIO JRAMP Cloud. 7. Tutorials on KEIO JRAMP Cloud will be provided on October 31, 2024, and November 1, 2024. 8. An environment to interact with KEIO JRAMP Cloud will be available at Keio starting the week of November 4, 2024. **Highlights**	国家安全保障，サイバーセキュリティー，クラウドシステム **テーマ** この講演では、国家安全保障、経済安全保障、社会保障のデジタルサイバー安全保障戦略について議論されました。特に、政府のクラウドシステム、サイバーインテリジェンスシステム、アクティブディフェンスシステム、KEIO JRAMP クラウドの重要性が強調されました。また、アメリカの企業と慶應義塾大学の提携についても触れられました。 **要点** 1. 国家安全保障 2. 経済安全保障 3. 社会保障のデジタルサイバー安全保障戦略 4. サイバーセキュリティー 5. 政府のクラウドシステム 6. サイバーインテリジェンスシステム 7. アクティブディフェンスシステム 8. KEIO JRAMP クラウド 9. トップシークレットの情報交換 10. アメリカの企業と慶應義塾大学の提携 **ハイライト** • "日本のクラウドというのは、連邦政府の米国のものと同等のものでなければなりません。" **章とトピック** **国家安全保障** 国家の安全を守るための政策や対策。 • **要点** ○ 地政学的な状況を考慮する ○ 国民を守るための対策が必要 **デジタルサイバー安全保障戦略** デジタルおよびサイバー空間における安全保障戦略。 • **要点** ○ 政府のクラウドシステム ○ サイバーインテリジェンスシステム ○ アクティブディフェンスシステム **KEIO JRAMP クラウド** 日本のクラウドシステムで、トップシークレットの情報交換が可能。

• "In the middle of the recent geopolitical problems, it is necessary to have a strong determination to protect one's own land and the people, as well as to be prepared for such a situation." **Chapters & Topics** **Digital Cyber Security** The practice of protecting systems, networks, and programs from digital attacks that aim to access, change, or destroy sensitive information. • **Keypoints** ○ National security: Protecting a nation's critical infrastructure and sensitive information. ○ Economic security: Ensuring the stability and integrity of financial systems and economic data. ○ Societal security: Safeguarding personal data and maintaining public trust in digital systems. **KEIO JRAMP Cloud** A high-security cloud system developed by Keio in collaboration with a U.S. company, equivalent to the U.S. FedRAMP Cloud. • **Keypoints** ○ Enables the exchange of top-secret information digitally. ○ Requires the Japanese-side cloud to be on equal footing with the FedRAMP. • **Examples** • Keio, in cooperation with a U.S. company, has started to run the KEIO JRAMP Cloud and is investigating its application. ○ Keio is collaborating with a U.S. company to ensure the KEIO JRAMP Cloud meets high-security standards. ○ The cloud system will allow for the secure exchange of top-secret information between Japan and the U.S. **Assignments & Suggestions**	• **要点** ○ アメリカのフェトランプクラウドに相当 ○ 慶應義塾大学とアメリカ企業の提携 **宿題と提案**

1.23 D1-S9-2 National Security

Barbara Grewe (National Security, MITRE)	バーバラ・グルーイ (MITRE 国家安全保障局)
National Security, Cybersecurity, Cyber Attacks **Theme** This speech, held on October 30, 2024, delves into the intricate relationship between national security and cybersecurity. Key takeaways include the importance of cybersecurity in protecting against both military and non-military threats, the severe consequences of cyber attacks on critical infrastructure, and notable examples of significant cyber incidents. The speech emphasizes that cybersecurity must be a priority in national security strategies and highlights the role of non-government organizations in defending against cyber threats. **Takeaways** 1. National security and cybersecurity are intertwined. 2. National security includes protection from military and non-military threats. 3. Cybersecurity involves protecting networks, devices, and data from unauthorized access or criminal use. 4. Effective cybersecurity is essential for national security. 5. Cyber attacks can target critical infrastructure and have severe consequences. 6. Examples of significant cyber attacks include the Colonial Pipeline attack, Mitsubishi Heavy Industries attack, NotPetya, SolarWinds breach, and Volt Typhoon. 7. Cyber attacks can be considered acts of war. 8. The digital space is a new battleground for national security. 9. Cybersecurity must be a priority in national security strategies. 10. Non-government organizations are expected to defend against cyber attacks,	国家安全保障，サイバーセキュリティ，ランサムウェア **テーマ** この講演では、国家安全保障とサイバーセキュリティの関連性について議論しました。国家安全保障の定義、非軍事的脅威、パンアム 103 便爆破事件や 911 テロ事件の例を通じて、サイバーセキュリティの重要性が強調されました。データの機密性、整合性、可用性の重要性、ランサムウェア攻撃や SolarWinds 攻撃の影響、政府と民間の協力の必要性についても触れられました。 **要点** 1. 国家安全保障とサイバーセキュリティの関連性 2. 国家安全保障の定義と非軍事的脅威 3. パンアム 103 便爆破事件と 911 テロ事件の例 4. サイバーセキュリティの重要性とその定義 5. データの機密性、整合性、可用性の重要性 6. ランサムウェア攻撃の影響と具体例 7. SolarWinds 攻撃の影響 8. 重要インフラへのサイバー攻撃の脅威 9. サイバーセキュリティと国家安全保障の関係 10. 政府と民間の協力の重要性 **ハイライト** • "サイバーセキュリティというのは、間違いなく国家安全保障の中心である。"-- グルーイさん **章とトピック** **国家安全保障とサイバーセキュリティの関連性** 国家安全保障とサイバーセキュリティがどのように関連しているかについての説明。 • **要点** ○ 国家安全保障は国民を軍事的および非軍事的脅威から守ることを意味する。 ○ 非軍事的脅威には規範、ルール、制度、社会の価値観の保護が含まれる。 ○ サイバーセキュリティは国家安全保障の一部であり、データの保護が重要である。 • **Examples** • 1988 年 12 月にスコットランドのロカビーで発生したパンアム 103 便の爆破事件。国家主体の攻撃であり、民間の乗客が犠牲となった。 • 2001 年にアルカイダのテロリストグループがアメリカに対して行った攻撃。軍および民間のターゲットが攻撃

even from foreign nations. **Highlights** • "Cybersecurity cannot be an afterthought to any efforts to address national security." **Chapters & Topics** **National Security** The ability of a state to protect and defend its citizens from military and non-military threats, including the preservation of the norms, rules, institutions, and values of society. • **Keypoints** ○ Includes protection from military and non-military threats. ○ Involves the preservation of societal norms, rules, institutions, and values. • **Examples** • In December 1988, Pan Am Flight 103 waSBOMbed over Lockerbie, Scotland. It was a state-sponsored attack using government and civilian attackers against a civilian target, resulting in the deaths of civilians and the destruction of a commercial airline. • On September 11, 2001, 19 non-state actors from the Al-Qaeda terrorist group carried out attacks in the United States, targeting both civilian and military sites, resulting in the deaths of civilians and military personnel. **Cybersecurity** The art of protecting networks, devices, and data from unauthorized access or criminal use and ensuring the confidentiality, integrity, and availability of information. • **Keypoints** ○ Protects networks, devices, and data from unauthorized access or criminal use. ○ Ensures confidentiality, integrity, and availability of information. • **Examples** • In May 2021, a ransomware attack on the	され、多くの民間人が犠牲となった。 **サイバーセキュリティの重要性** サイバーセキュリティが国家安全保障において重要である理由。 • **要点** ○ サイバーセキュリティはネットワーク、デバイス、データの保護を目的とする。 ○ データの機密性、整合性、可用性が崩れると国家安全保障に影響を与える。 ○ ランサムウェア攻撃や SolarWinds 攻撃などの具体例が示すように、サイバー攻撃は国家の重要インフラに大きな影響を与える。 • **Examples** • 2021 年 5 月に発生したランサムウェア攻撃により、6 日間パイプラインが停止し、東海岸の石油とガスの供給に大きな影響を与えた。 • 2011 年に三菱重工がサイバー攻撃を受け、ウイルスが造船所や製造所に侵入した。 1. 2019 年から 2020 年にかけて発生した SolarWinds 攻撃により、民間および政府のネットワークが侵害され、重要なデータが流出した。 **宿題と提案**

Colonial Pipeline resulted in a six-day shutdown of a pipeline responsible for 45% of the oil and gas supplies along the eastern seaboard of the United States. • In 2011, Japan's largest weapons manufacturer, Mitsubishi Heavy Industries, was targeted by a ransomware attack affecting many of its servers and computers, including those at a shipyard where destroyers are built and a facility manufacturing submarines and parts for nuclear power stations. • A piece of malware that masqueraded as ransomware, NotPetya began in Ukraine and spread worldwide, affecting various entities including hospitals, factories, pharmaceuticals, shipping, food companies, and construction. • In late 2019 or early 2020, the SolarWinds breach led to intrusions into government and private networks, affecting clients including 425 of the Fortune 500 companies and various U.S. government departments. • In 2021, an Advanced Persistent Threat dubbed Volt Typhoon was reported in the U.S., intended to collect information within critical infrastructure networks and potentially cause social chaos by shutting down critical infrastructure. **Assignments & Suggestions**	

1.24 D1-P10 Panel: Active Cyber Defense: Meaning, needs, limitation, and recommendations

Moderator: Jun Osawa (Sasakawa Peace Foundation) Panelists: - Greg Rattray (Next Peak) - Toru Tsuchiya (CEO, Cyber Defense Labs K.K.) - Aare Reintam (Chief Operating, CybExer Technologies OÜ) - Giacomo Persi Paoli (UNIDIR)	モデレーター：大澤 淳（笹川平和財団 特別研究員） パネリスト： - グレッグ・ラットレイ（Next Peak） - 土屋 徹（株式会社サイバー防衛研究所 代表取締役社長） - アーレ・レインタム（CybExer Technologies OÜ Chief Operating） - ジャコモ・ペルシ・パオリ（UNIDIR）

Active Cyber Defense, Hybrid Warfare, Cybersecurity Measures

Theme

This lecture, held on October 30, 2024, covered key aspects of active cyber defense, Japan's national security strategy, and hybrid warfare. It highlighted the importance of proactive cybersecurity measures, the role of public-private partnerships, and the need for international cooperation in enhancing national cyber resilience. Key takeaways included the significance of legal amendments, the challenges of conducting offensive cyber operations, and the importance of preparedness and training in cyber defense.

Takeaways

1. Active cyber defense
2. Japan's national security strategy
3. Hybrid warfare
4. Cyber attacks
5. Information warfare
6. Legal amendments
7. Cybersecurity measures
8. Proactive cybersecurity
9. Passive defense
10. Military cyber attacks

Highlights

- "The concept of active cyber defense is wide-ranging from technical measures such as information sharing and sandboxing to policy measures such as international public attribution, sanctions, and judicial prosecution."
- "The failure is the measure of preparedness."
- "The moment in which states take measures to implement the international commitments that they have made, they are not only putting in practice the commitment that they've made at international level, but they are actively strengthening their national cyber

能動的サイバー防御，官民連携，サイバーセキュリティ

テーマ

この講義では、能動的サイバー防御の重要性、ウクライナ戦争とハイブリッド戦の影響、日本の国家安全保障戦略の改定、法律の改正と体制整備の必要性、官民連携の強化、アメリカのサイバーセキュリティの取り組み、サイバー攻撃に対するプロアクティブな対策について議論されました。

要点

1. 能動的サイバー防御の重要性
2. ウクライナ戦争とハイブリッド戦の影響
3. 日本の国家安全保障戦略の改定
4. 法律の改正と体制整備の必要性
5. 能動的サイバー防御の概念とその範囲
6. 官民連携の強化
7. アメリカのサイバーセキュリティの取り組み
8. サイバー攻撃に対するプロアクティブな対策
9. サイバー防御のための技術とプロセス
10. 民間セクターの役割と権利

ハイライト

- "能動的サイバー防御の意味というのはまだサイバーコミュニティの中でもはっきりとしていないわけです。"
- "情報共有だけでは不十分です。行動を取らなければなりません。"
- "国際法、あるいは国連憲章などがサイバー攻撃においても適用することができるわけであり、ICT にも適用することができるものであるわけです。"

章とトピック

能動的サイバー防御

能動的サイバー防御とは、サイバー攻撃に対して積極的に対策を講じることを指します。これは、受動的防御と攻撃的サイバーオペレーションの間に位置するもので、ネットワーク内外での対策を含みます。

- **要点**
  - 受動的防御と攻撃的サイバーオペレーションの間に位置する
  - ネットワーク内外での対策を含む
  - 情報戦やサイバー攻撃に対する対応
- Examples
  - ウクライナ戦争では、ロシアがハイブリッド戦を仕掛け、情報戦やサイバー攻撃が戦闘が始まる前から発生しました。これにより、日本の国家安全保障戦略が改定され、能動的サイバー防御の導入が記述さ

resilience."

Chapters & Topics

Active Cyber Defense

Active cyber defense is a proactive cybersecurity measure that falls between traditional passive defense and military cyber attacks.

- **Keypoints**
  - Proactive cybersecurity measure
  - Falls between passive defense and military cyber attacks
  - Includes technical measures like information sharing and sandboxing
  - Includes policy measures like international public attribution, sanctions, and judicial prosecution
- **Examples**

Japan's national security strategy was revised in 2022 to take into account the changing security environment of hybrid warfare, including cyber attacks and information warfare.

  - The revision was influenced by the Ukraine war where Russia launched hybrid warfare against Ukraine.
  - An expert committee has been meeting since June 2024 to work on legal amendments related to active cyber defense.

Admiral Dennis Brair's project at George Washington University in 2016 focused on active cyber defense.

  - The project report defined active defense as measures taken within one's own network as passive defense and disruption within the attacker's network as cyber attacks.
  - It highlighted the wide-ranging nature of active cyber defense, from technical to policy measures.
- **Considerations**
  - Active cyber defense definitions vary, making uniform discussion difficult.
  - Overlap with military and intelligence

れました。

- **留意点**
  - 法律の改正と体制整備の必要性
  - 官民連携の強化

官民連携

官民連携とは、政府と民間セクターが協力してサイバー防御を強化することを指します。これにより、サイバー攻撃に対する効果的な対策が可能となります。

- **要点**
  - 政府と民間セクターの協力
  - サイバー攻撃に対する効果的な対策
- **Examples**
  - 日本のサイバークライムセンターは、2014 年に設立され、官民連携の一環として、フィッシングや不正送金と戦うためのプラットフォームを提供しています。
- **留意点**
  - 官民連携の強化
  - プライベートセクターの権利と役割

情報共有の重要性

情報共有はリスク低減のために重要であり、国内外で行うべきである。

- **要点**
  - 情報共有によりリスクを低減できる。
  - 国内外での情報共有が必要。

ランサムウェアとフィッシングの増加

ランサムウェアやフィッシングがビジネスとして増加している。

- **要点**
  - ランサムウェアはビジネス化している。
  - フィッシングもビジネス化している。

銀行口座開設の困難さ

新しい銀行口座を開設する際に多くの質問を受ける。

- **要点**
  - 新しい口座を開設する際に多くの質問を受ける。
  - 銀行は異常な状況として見なすことがある。

警察署の役割

警察署は特定の行動に集中しているが、他の重要な点も取り上げる必要がある。

- **要点**
  - 警察署は特定の行動に集中している。
  - 他の重要な点も取り上げる必要がある。

国際的な協力の必要性

サイバー攻撃に対する国際的な協力が必要である。

fields complicates open discussion. • **Special Circumstances** ○ If encountering legal uncertainties, how should it be addressed? Consider the implications of recent political changes and ongoing legal amendments. **Hybrid Warfare** Hybrid warfare involves a combination of conventional military tactics with other means such as cyber attacks and information warfare. • **Keypoints** ○ Combination of conventional military tactics with cyber attacks and information warfare ○ Seen in the Ukraine war where Russia launched hybrid warfare against Ukraine **Cybersecurity Measures** Cybersecurity measures range from passive defenses within one's own network to active defenses that may involve actions within an attacker's network. • **Keypoints** ○ Passive defenses include limiting access to networks and alerting to attacks. ○ Active defenses include hunting for adversaries within networks and using honeypots and beacons. **Active Cyber Defense** The concept of active cyber defense involves proactive measures to protect against cyber threats, including the potential for offensive operations. • **Keypoints** ○ Need for private sector involvement in cyber defense. ○ Government's role in intrusion and disruption. ○ Development of active defense capabilities in critical infrastructures. • **Considerations** ○ Challenges in conducting offensive cyber operations.	• **要点** ○ 国際的な協力が必要。 ○ 官民パートナーシップが重要。 **SNS を利用したフィッシング** PC のフィッシングでは不十分であり、SNS を利用したフィッシングが増加している。 • **要点** ○ PC のフィッシングでは不十分。 ○ SNS を利用したフィッシングが増加している。 **JC3 の分析と協力** JC3 が分析を行い、モバイル通信事業者の協力を求めている。 • **要点** ○ JC3 が分析を行っている。 ○ モバイル通信事業者の協力を求めている。 **若者の教育の重要性** スマホを入手する前から若者の教育が必要である。 • **要点** ○ スマホを入手する前から教育が必要。 ○ 良くない声に誘われないようにする。 **テクニカルサポート詐欺** テクニカルサポート詐欺が増加しており、ユーザーが騙されやすい。 • **要点** ○ テクニカルサポート詐欺が増加。 ○ ユーザーが騙されやすい。 **官民パートナーシップの重要性** 官民パートナーシップを通じてサイバー防御を強化する必要がある。 • **要点** ○ 官民パートナーシップが重要。 ○ サイバー防御を強化する必要がある。 **サイバーレンジの活動** サイバーレンジでの集団トレーニングが重要である。 • **要点** ○ サイバーレンジでの集団トレーニングが重要。 ○ コミュニティの形成が重要。 **MITRE ATT&CK フレームワーク** MITRE ATT&CK フレームワークは攻撃防御のベースラインを提供する。 • **要点** ○ MITRE ATT&CK フレームワークが重要。

○ Importance of developing control, organizational structures, and well-defined tactics. **Public-Private Partnerships in Cyber Defense** Collaborative efforts between the public and private sectors to enhance cyber defense capabilities. • **Keypoints** ○ Strengthened public-private partnership. ○ Taking advantage of multi-channel communications. ○ Granting authority to access and neutralize adversary assets. • **Examples** An organization established in November 2014, backed by the National Police Agency, focusing on combating phishing and fraudulent remittance. ○ JC3 analyzes phishing mechanisms and collaborates with mobile operators and companies to reduce malicious SMS. ○ Cooperation with companies like Microsoft to address technical support scams. • **Considerations** ○ Continuous meetings and proactive approaches are essential. ○ Respect for different capabilities, authorities, and laws. **Cyber Range Environments** Controlled environments for training individuals and teams in cyber defense through live fire exercises and collaborative trainings. • **Keypoints** ○ Building digital twins of various sectors for training. ○ Hands-on training and collaborative exercises. ○ Community building through shared experiences. • **Examples** A domain for conducting cyber battles for governments, private sector companies, and militaries to understand and improve	○ 攻撃防御のベースラインを提供。 **集団トレーニングの重要性** 集団トレーニングを通じてコミュニティを形成し、サイバー攻撃に対する準備を行う。 • **要点** ○ 集団トレーニングが重要。 ○ コミュニティの形成が重要。 **サイバー攻撃に対する準備** サイバー攻撃に対する準備とレジリアンスが必要である。 • **要点** ○ サイバー攻撃に対する準備が必要。 ○ レジリアンスが重要。 **人工知能の利用** 人工知能を利用して防御と攻撃のモデルを作成する。 • **要点** ○ 人工知能の利用が進んでいる。 ○ 防御と攻撃のモデルを作成。 **宇宙技術の発展** 宇宙技術が発展しており、通信などにおいて重要な役割を果たす。 • **要点** ○ 宇宙技術が発展。 ○ 通信などにおいて重要な役割を果たす。 **サイバー防御のための新技術** 新しい技術を利用してサイバー防御を強化する。 • **要点** ○ 新しい技術を利用。 ○ サイバー防御を強化。 **デジタル変革** デジタル変革が進んでおり、特殊なスキルが必要である。 • **要点** ○ デジタル変革が進んでいる。 ○ 特殊なスキルが必要。 **国際社会の協力** 国際社会の協力が重要であり、重要インフラの企業が狙われている。 • **要点** ○ 国際社会の協力が重要。 ○ 重要インフラの企業が狙われている。 **国際的なサイバーセキュリティの議論** 国際的なレベルでのサイバーセキュリティに関する議論とその進展について。

collaborative defense strategies.

- Training individuals and teams in a controlled environment.
- Using MITRE attack and defense frameworks for objective measurement.

- **Considerations**
  - Importance of community building and direct communication lines.
  - Learning from failures and mistakes.

Community Building in Cyber Defense

The importance of building a community among government, military, and private sector for effective cyber defense.

- **Keypoints**
  - Collaboration between different sectors enhances overall security.
  - Sharing information and resources can lead to better preparedness.

International Cooperation in Cyber Security

The role of international cooperation in enhancing national cyber resilience.

- **Keypoints**
  - International peace and security can be affected by cyber attacks.
  - Cooperation helps in sharing best practices and resources.

Active Cyber Defense

The concept and importance of active cyber defense.

- **Keypoints**
  - No universal consensus on the definition of active cyber defense.
  - Includes activities both outside and inside the perimeter of national networks.

Public-Private Partnerships

The significance of public-private partnerships in cyber defense.

- **Keypoints**
  - Collaboration between public and private sectors is crucial.
  - Helps in sharing information and resources.

- **要点**
  - 1998 年のロシアの戦争とアメリカの決議
  - 2013 年の国際法と国連憲章の適用
  - 2015 年のサイバースペースにおける規範の合意

能動的サイバー防御の重要性

能動的サイバー防御の概念とその重要性について。

- **要点**
  - ネットワークの内外での活動
  - 国家安全保障のサポート
  - 国際法と規範の遵守

信頼情勢法の役割

信頼情勢法の概念とその役割について。

- 要点
  - 透明性の確保
  - 誤解や間違った解釈によるエスカレーションのリスク緩和
  - ポイントオブコンタクトのネットワーク

宿題と提案

Preparedness and Training The importance of preparedness and training in cyber defense. • **Keypoints** ○ Training and preparedness are key to effective cyber defense. ○ Cyber ranges can be used for training purposes. **International Law in Cyber Security** The application of international law to digital technologies and cyber security. • **Keypoints** ○ International law, including the UN Charter, applies to digital technologies. ○ Legal principles such as non-intervention and state sovereignty are important. **Voluntary Norms of Responsible State Behavior** The establishment of voluntary norms for responsible state behavior in cyberspace. • **Keypoints** ○ 11 voluntary norms were established to guide state behavior. ○ Includes both positive and negative obligations for states. **Confidence-Building Measures** The role of confidence-building measures in cyber security. • **Keypoints** ○ Helps in building trust and transparency between states. ○ Minimizes the risk of misunderstanding and escalation. **Capacity Building in Cyber Defense** The importance of capacity building in enhancing cyber defense. • **Keypoints** ○ Capacity building includes technical, organizational, and human capabilities. ○ Helps in strengthening national networks and protecting against cyber attacks. **Assignments & Suggestions**	

1.25 D1-P11 Panel: Facilitating Cyber Intelligence Sharing: Processes, networks, and information

Moderator: Bonji Ohara (Sasakawa Peace Foundation) Panelists: - Yuji Ukai (CEO, FFRI Security, Inc.) - Wen Masters (MITRE) - ADM(Ret.) Dennis Blair - Pieter van den Berg (Head of the Cyberunit, the Netherlands Ministry of Foreign Affairs) - Geistautas Černius (Regional Cyber Defence Centre (part of National Cyber Security Centre of Lithuania))	モデレーター：小原 凡司（笹川平和財団） パネリスト： - 鵜飼 裕司（FFRI Security, Inc. 代表取締役社長） - ウェン・マスターズ（MITRE） - デニス・ブレア - ピーター・ヴァン・デン・ベルク（オランダ外務省国際サイバーユニット長） - ゲイスタウタス・チェルニウス（地域サイバー防衛センター(リトアニア国家サイバーセキュリティセンターの一部門))
Overview This speech summarizes the meeting notes on facilitating cyber intelligence sharing, processes, networks, and information. The notes cover various aspects of intelligence sharing, including policy, operational, and tactical intelligence, as well as specific practices and challenges faced by countries like Japan, the U.S., the Netherlands, and Lithuania. The document also highlights key partnerships, cybersecurity exercises, and the role of organizations like MITRE in public sector cybersecurity. Action items are consolidated at the end for clarity and follow-up. **Panel Introduction** • **Moderator**: Bonji Ohara, Sasakawa Peace Foundation • **Panelists**: Various experts in cyber intelligence sharing **Levels of Intelligence Sharing** **Policy Intelligence** • **Definition**: Higher-levERABrall intentions, major possible actions of adversaries. • **Example**: Discussion between the United States and Japan about the likelihood of China landing a military force on the Senkakus within the next five years. • **Trust Levels**: ○ **Low Trust**: Sharing general policy	**概要** この議事録は、サイバーインテリジェンスの共有に関する会議の内容をまとめたものです。日本の現状と課題、各国の取り組み、そして今後の日本の取り組みについて詳述しています。最後に、会議で決定されたアクションアイテムをまとめています。 **サイバーインテリジェンスの共有** **導入** • **発言者紹介** ○ MITRE のウェン・マスターズさん ○ デニス・ブレア提督 ○ オランダ外務省の国際サイバーユニット長ピーター・バンデンベルグさん ○ リトアニア国家サイバーセキュリティセンターのゲイスタ・ウッタ・チェルニュースさん（オンライン参加） **日本の現状と課題** • **2017 年の笹川平和財団主催第 3 回サイバーセキュリティセミナー** ○ ブレア提督の発言：「日本のインテリジェンス共有は義務ではなく任意」 ○ この発言が大きな衝撃を与えた ○ 政府と民間企業等のハブの必要性を感じ、取り組んできたが、7 年経った今も実現していない • **現在の状況** ○ サイバー攻撃の増加と性格の変化 ○ 国家間のインテリジェンス共有の重要性が増している ○ 日本国内で解決すべき課題がある

analysis without revealing sources.

- **High Trust**: Detailed exchange including sources like spies, intercepted communications, and satellite images.

Operational and Tactical Intelligence

- **Definition**: Current information on enemy intentions and capabilities.
- **Example**: Sharing information about the location of improvised explosive devices in Afghanistan.
- **Trust Levels**:
  - **Low Trust**: Basic force protection information shared among allies.
  - **High Trust**: Combined common operational picture with automatic feeds from intelligence sources of both allies.

Information Sharing in Japan

Data to Intelligence Flow

- **Process**: Data collection → Analysis → Information → Evaluation → Intelligence → Decision-making and action-taking.
- **Mechanisms**:
  - **Organizations**: Cybersecurity Association (CSC), CAN, ISAC, ICT ISAC.
  - **Government Agencies**: Ministry of Internal Affairs, Ministry of Defense, Ministry of Police, Ministry of Foreign Affairs, Ministry of Investigation.
  - **NISQ**: Developing and transforming role in the Intel Community.

U.S. Cybersecurity Information Sharing

Critical Infrastructure

- **Definition**: 16 critical infrastructure sectors as defined by CISA.
- **Ownership**: Many sectors are owned and operated by private sectors with varying degrees of cyber sophistication and resources.
- **Example**: Cybersecurity Risk Information Sharing Program (CRISP) - a public-private partnership between the U.S. Department of Energy and the electricity

ブレア提督の発言

- **知識の二つのレベル**
  - **政治知識**
    - 高いレベルの意見や大きな可能性のある相手の行動
    - 例：中国が次の 5 年間で持つ可能性のある軍事力
  - **行動的な戦略と戦術的な情報**
    - 具体的な戦略や戦術の情報
    - 例：アフガニスタンでの特定の爆弾装置や路面爆弾の場所についての日常的な共有
- **信頼のレベル**
  - **信頼の高いレベル**
    - 高度な知識の共有
  - **信頼の低いレベル**
    - 基本的な知識の共有
    - 例：日本の国民の安全に関する問題

日本の情報共有の現状と課題

国内の状況

- **政府と民間企業の協力不足**
  - 日本は各国間の協力をする能力があるか疑問視されている。
  - ブレア提督の指摘：「日本はまだジュニアリーグなのではないか」
  - 政府と民間企業の協力が進まない理由を検討。
- **民間企業のマインドセット**
  - 政府側の問題だけでなく、民間企業のマインドセットも情報共有を阻む要因。
  - 民間企業の草の根コミュニティの紹介。

情報共有の仕組み

- **官と民の仕組み**
  - サイバーセキュリティ協議会（CSC）、キーアイザック、ICT アイザックなどの官主導の仕組み。
  - JCIP、J-CRAT、セッター監視、C4 タブなどの民間主導の仕組み。
  - インテルコミュニティ：内庁、防衛省、警察、大務省、公安調査庁などの政府機関。
- **草の根コミュニティ**
  - 1997 年頃から存在する古いコミュニティ。
  - 温泉コミュニティ、コードブルー、JNSA などが草の根から発展。
  - 信頼関係で結びついた強固なコミュニティ。

industry.

Challenges

- **Trust**: Codifying trust across different groups and boundaries.
- **Interoperability**: Necessary interoperability across borders, organizations, and sectors.
- **Governance**: Importance of governance to achieve effective information sharing.

Dutch Cybersecurity Information Sharing Legal Framework

- **Network and Information Security Act**: Obligates vital organizations to have cybersecurity policies and report vulnerabilities within 24 hours.
- **Cyber Resilience Act**: Sets minimum security standards for IoT devices and responsibilities for producers.

Cultural Initiatives

- **Openness and Transparency**: Encouraging organizations to share vulnerabilities and report them.
- **Joint Analysis**: Promoting joint analysis to mitigate cyber threats.

International Collaboration

- **Proactive Approach**: Focusing on patterns of behavior and using all policy instruments to counter threats.
- **Information Sharing**: Ensuring declassified information reaches relevant parties to mitigate risks.
- **Best Practices**: Sharing structures and experiences in working together intra-governmentally.

Lithuanian Cyber Threat Intelligence Regional Cyber Defense Center

- **Establishment**: Part of the National Cyber Security Center in Lithuania, including U.S., Latvia, Poland, Georgia, Ukraine, and the Czech Republic.
- **Focus**: Cyber threat intelligence for critical infrastructure and governmental

各国の情報共有の取り組み

アメリカの状況

- **情報共有の現状**
  - サイバーセキュリティの情報共有には様々な度合いがある。
  - 16の重要インフラセクターが存在し、多くは民間が所有・運営。
  - 公共と民間のパートナーシップが重要。
- **エネルギーセクターの成功例**
  - エネルギーセクターと政府の協力が成功している。
  - 公共セクター内での情報共有の拡大が課題。

ヨーロッパの状況

- **プライバシー保護と情報共有**
  - プライバシー保護が厳しい中での情報共有の取り組み。
  - 24 時間以内に認定された国際サービスによる罪悪を報告する必要がある新しい計画。
- **プロアクティブアプローチ**
  - サイバー脅威に対するプロアクティブなアプローチを採用。
  - 行動パターンに焦点を当て、政策手段を特定。

リトアニアの状況

- **サイバー脅威インテリジェンス**
  - ロシアからの脅威に対する取り組み。
  - 多国籍チームとの協力が重要。
  - 中国からのサイバー脅威に対する研究と対策。

日本の今後の取り組み

民間の期待と政府の役割

- **民間の期待**
  - 民間もインテリジェンスコミュニティに貢献したいという意欲がある。
  - 法律や制度の問題で実現が難しい現状。
- **政府の役割**
  - 民間が活動できる環境を整えることが重要。
  - インテリジェンス共有の進展に向けた議論の深化が必要。

アクションアイテム

[ ] 日本国内でのインテリジェンス共有のハブの設立に向けた具体的な計画の策定

[ ] 国家間でのインテリジェンス共有の強化に向けた協議の開始

[ ] 民間企業が活動できる環境を整えるための具体的な

bodies, primarily against threats from Russia. **Key Success Factors** • **Connections**: Importance of knowing the right people and sources. • **Stakeholder Requirements**: Understanding primary intelligence requirements. • **Open Source Intelligence**: Using non-classified intelligence to facilitate easier sharing. **Broader Threat Landscape** • **Global Threats**: Recognizing threats from countries like China, North Korea, and Iran. • **Comprehensive Defense**: Preparing to defend against a wide range of threats, not just from one specific country. **Cybersecurity Studies and Threat Mitigation** **Study on Cyber Threats from China** • Conducted multiple studies annually, including a recent one on recognizing cyber threats from China. • Analyzed the most active and notorious cyber threat actors from China using the TTP's approach (Tactics, Techniques, and Procedures). • Compared China's TTPs against those of other major countries. • Identified the most commonly used TTPs by Chinese APT actors. • Provided mitigation techniques for threats likely originating from China. • Emphasized the importance of focusing on digital assets to maintain strong cybersecurity. **Lithuania-Japan Cybersecurity Collaboration** **Key Partnerships and Visits** • Japan is a key partner to Lithuania in various fields, including cybersecurity. • Japanese government officials visited Lithuania for cyber consultations, aiming	施策を検討。 [ ] インテリジェンス共有の進展に向けた議論を深める。

to make this an annual event. • Japanese experts visited Lithuania's Ministry of Defense (MOD) and National Cyber Security Center to establish dialogue and information sharing on cyber threats. **Cybersecurity Exercises** • Lithuania's Sound Forces organized a cybersecurity exercise called Amber Mist. • Japan sent four personnel to participate, showcasing the strong collaboration between the two countries. **Regional Cyber Defense Center** • Lithuania's National Cyber Security Center is part of the regional cyber defense center. • Focuses on cyber threat intelligence. • Japanese experts' involvement is invaluable for understanding cyber threats from China. **MITRE's Role in Public Sector Cybersecurity** **Open Sharing of Cyber Threat Intelligence** • MITRE believes in openly sharing cyber threat intelligence with the public. • Publishes knowledge bases like MITRE ATT&CK, MITRE Atlas, and MITRE Embed. • These resources help the global community enhance their cyber defense capabilities. **Incident Response and Knowledge Sharing** • MITRE was breached by a Chinese APT actor earlier this year. • Conducted forensic analysis and shared findings with the public to help others protect their networks. • Emphasized the importance of learning from breaches to improve network security. **International Cybersecurity Policies and Cooperation** **Coordinated Vulnerability Disclosure**	

• Importance of stimulating organizations to be open about vulnerabilities. • Creating a welcoming environment for ethical hackers. **National and International Cooperation** • National security against cyber threats requires cooperation between governmental and civil organizations. • Ministries of Defense and police need to work closely with other entities to address cybercrime effectively. **Intelligence Services and Cultural Shifts** • Intelligence services need to be more open and declassify information where possible. • This openness is crucial for addressing cyber threats and involves a significant cultural shift. **Japan's Cyber Intelligence and Security Requirements** **Need for Cyber Intelligence Gathering** • Japan currently lacks authority to penetrate foreign networks for intelligence. • The U.S. generates 75% of its intelligence reports from cyber intelligence. • Japan needs to contribute to intelligence sharing rather than relying solely on sanitized American intelligence. **Security System Enhancements** • Stronger security clearances for individuals. • Enhanced security requirements for networks handling secure information. **Community Contributions to Cyber Intelligence** **Global Civil Society Involvement** • Many individuals and organizations are eager to contribute to the intelligence community. • Emphasis on the importance of global civil society in enhancing cybersecurity	

efforts. **Action Items** [ ] Codify trust mechanisms for information sharing across different groups and boundaries. [ ] Develop necessary interoperability standards for cross-border and cross-sector information sharing. [ ] Establish governance frameworks to oversee and manage information sharing initiatives. [ ] Promote cultural shifts towards openness and transparency in sharing vulnerabilities. [ ] Enhance international collaboration by sharing best practices and structures for cyber defense. [ ] Organize annual cyber consultations with Japanese government officials. [ ] Continue collaboration with Japan in cybersecurity exercises like Amber Mist. [ ] Enhance cooperation between national and civil organizations for cybersecurity. [ ] Encourage intelligence services to declassify information and be more open. [ ] Advocate for Japan to develop cyber intelligence gathering capabilities. [ ] Strengthen security clearances and network security requirements in Japan.	

1.26 D1-P12 Panel: Government Cloud System

Moderator: Noriaki Okui (Founder, Interfusion Consulting Inc.) Panelists: - Chris Grady (CTO, CyLogic) - Norihito YAMAMOTO (Digital Agency) - Claire Elias - Jun Murai	モデレーター：奥井 規晶（株式会社インターフュージョン・コンサルティング 代表取締役会長） パネリスト： - クリス・グラディ（CyLogic 社 CTO） - 山本 教仁（デジタル庁） - クレア・エリアス - 村井 純
Overview The session focused on various aspects of government cloud services, including procurement guidelines, provider challenges, operational issues, and future trends in technology. Key frameworks like FedRAMP and ISMAP were discussed in detail, along with their	**会議議事録** **政府クラウドの現状と FedRAMP の取り組み** • **モデレーター**：インターフュージョンコンサルティングのファウンダー、データソサイティーアライアンスの会長 • **目的**：アメリカ政府のクラウド、FedRAMP の現状について議論 **クリス氏の発表**

implications for government cloud services in Japan and the United States. The meeting also highlighted the importance of AI, edge computing, and the need for continuous improvement in security processes. **Introduction** • **Moderator**: Mr. Okui, Founder of Interfusion Consulting, Inc. and President of Data Society Alliance. • **Purpose**: Discussion on the U.S. government cloud and FedRAMP. **U.S. Government Cloud and FedRAMP** **Scilogic and FedRAMP** • **Presenter**: Chris • **Company**: Cylogic ○ Focus: Protecting critical infrastructure in the U.S. and allied countries. ○ Sectors: Energy, defense industrial base, aerospace. ○ Collaboration: Working with Keio University on J-RAMP, a FedRAMP-like initiative. • **Experience:** ○ 28 years in technology. ○ 14 years in cloud industry, starting in 2010. ○ Extensive experience in FedRAMP security and compliance. ○ Involved in CyCloud, a FedRAMP high-ready system. ○ Completing the fourth FedRAMP high-ready annual assessment for CyCloud. **Key Points and Collaborations** • **Invitations and Acknowledgments**: ○ Invited by Admiral Dennis Blair and Greg Radcliffe. ○ CEO and co-founder, Lewis Mayberg, serves on the board of directors of secureenergy.org. • **Thought Piece**: ○ Collaboration with Admiral Dennis Blair and Greg Rattray on LinkedIn.	• **自己紹介** ○ 28 年間テクノロジー業界での経験 ○ 2010 年からセキュリティの高いクラウドインフラに従事 ○ 慶應のサイバーシンポジウムと同じくらいの期間クラウドに関わっている • **FedRAMP のセキュリティとコンプライアンス** ○ FedRAMP のセキュリティコンプライアンスに関する仕事 ○ 4 回目の FedRAMP のハイレディアリアラスメントを実施 • **FedRAMP のアプローチ** ○ FedRAMP のようなアプローチが最適と考えている ○ 第 4 回目のアセスメントがまとめられている ○ FedRAMP のドットカブでオンラインステータス確認可能 • **政府のコミュニティクラウド** ○ Google、マイクロソフトと共に政府のコミュニティクラウドを提供 ○ コマーシャルと公共のクラウドプロジェクトを同じクラウドホームで実施 **アフシーイベントの報告** • **イベント概要** ○ 2024 年度版アフシーイベントに参加 ○ アームとコンセスコミュニケーションに関するセッション ○ DOD の会議 • **セッションの内容** ○ ミッションパートナーに対するセキュリティの重要性 ○ 2027 年までのオペレーションエリアについての議論 ○ 2027 年は中国が台湾に侵攻する可能性がある年とされている • **緊急性とソリューション** ○ 緊急性の高い脅威に対する対応が必要 ○ サイバーイニシアムがソリューションとして提案されている • **AI の利用** ○ 会議の中で AI の利用についても議論 **AI の歴史と現状** **AI の歴史** • **50 年代からの話題**: ○ AI は 1950 年代から既に話題になっていた。 • **AI の冬の時期**:

- Emphasis on enhancing Japan's digital resiliency with a tiered control structure similar to FedRAMP.
- Strong support for this initiative in Japan.

FedRAMP Status and Public Cloud Recategorization

- **Current Status**:
  - Fourth FedRAMP high-ready assessment in progress.
  - Status available on FedRAMP.gov marketplace.
  - Impact level: High.
  - Deployment model: Public cloud.
- **Recategorization:**
  - Transitioned from government community cloud to public cloud.
  - Allows serving both commercial and government customers on the same platform.

AFSIA Event Insights

- **Event**: AFSIA 2024 (Armed Forces Communications and Electronics).
- **Key Insight**:
  - Reminder from the former CEO of the Defense Information Systems Agency about China's 2027 goal to invade Taiwan.
  - Emphasis on the urgency of cyber initiatives.

Artificial Intelligence and Data Lake

General Observations

- **Data Lake Evolution**: The concept of Data Lake has become more practical and ubiquitous compared to the past.
- **Artificial Intelligence (AI)**:
  - AI is described as more of a "statistical hallucination" rather than true intelligence.
  - The current relevance and meaningful use cases suggest AI is here to stay.
  - AI's significance extends beyond cybersecurity and chat GPT-like

  - 70 年代と 80 年代、90 年代に AI のイニシアティブが諦められた時期があった。
  - データレイク（ダラトスデータレイクと呼ばれていた）として再び注目されるようになった。

現在の AI の状況

- **リアルな存在**:
  - 現在の AI は統計的なハルシネーションと呼ばれるが、実際に残り続けると考えられている。
  - ユースケースが身近になってきているため、AI は今後も重要な役割を果たすと予想される。

AI の利用分野

サイバーセキュリティと戦争

- **サイバーセキュリティ**:
  - AI がサイバーセキュリティで使われることが予想される。
- **戦争での利用**:
  - AI が実際の戦争で使われる可能性がある。
  - これにより、運用レベルがこれまでと全く違うものになる。

クラウドの利用

クラウドの再評価

- **クラウドのデスティネーションとしての見方**:
  - クラウドをデスティネーションとして見るべきではない。
  - ハイパースケールなクラウドは IT 業界で最悪の考え方とされる。
  - 数社が一元化した場所に情報を置くことはリスクが高い。

クラウドと国家安全保障

- **国家安全保障でのクラウド利用**:
  - 政府クラウドだけでなく、クラウド全体の話として議論。
  - サイバーコンフレクトのリスクが高まるため、クラウドの利用には慎重になるべき。

オンプレミスへの回帰

- **AI とオンプレミス**:
  - 多くの会社が AI をクラウドではなくオンプレミスで運用しようとしている。
  - 機密情報や分析する場所に近いところにワークフローを置くべき。

セキュリティとコンプライアンス

- **新しい攻撃対象**:
  - AI にインジェストされたデータが最も重要なデータとな

capabilities, indicating an impending AI arms race.

Security Implications

- **AI and Security:**
  - The rise of AI necessitates a new level of security and deployment models.
  - AI workloads require proximity to the data they process, making public cloud solutions less optimal.
  - AI data and outputs are highly valuable and represent new attack vectors.

Cloud as an Operational Model

Shift in Perspective

- **Operational Model vs. Destination**:
  - Organizations should stop viewing the cloud as a destination and start embracing it as an operational model.
  - This applies to both government and national security interests.

Risks of Hyperscale Clouds

- **Centralized Control**:
  - The concept of hyperscale clouds, where a few companies control vast amounts of data, is criticized as a poor idea for the IT industry.
  - The current state of cyber conflict heightens the risks associated with centralized data control.

Edge and On-Prem Solutions

- **AI and Data Proximity:**
  - Companies are increasingly looking to move AI platforms to edge or on-prem solutions to keep workloads close to their data.
  - Moving large volumes of sensitive data to public clouds is impractical.

Security and Compliance Frameworks

Importance of FedRAMP

- **FedRAMP Security Requirements**:
  - FedRAMP's detailed and prescriptive nature makes it a critical framework for securing cloud infrastructure.

り、新しい攻撃対象となる。

- セキュリティのコンプライアンス機能が重要になる。
- 連邦のセキュリティ要件として確立され、日本のフレームワークにも取り入れられると考えられる。

日本におけるクラウドセキュリティの必要性

高セキュリティ試験カーブの必要性

- 日本は非常にセキュリティの高い試験カーブを必要としている。
- 最も高いレベルのセキュリティで展開される必要がある。

日本の主権クラウドの必要性

- 他の企業が属していない、日本の主権のクラウドが必要。

クラウド展開のフレームワーク

主要なフレームワーク

- HIPAA、PCI、SOC2、ハイトラスト、ISO、NIST、AWS などが存在。
- FedRAMP のプログラムは 2014 年に初めて認可。

コンプライアンスのフレームワーク比較

- ISO27017、NIST800-171、FedRAMP の比較。
  - **ISO27017**: クラウド用の標準。
  - **NIST800-171**: 部分的に構造化されている。
  - **FedRAMP**: 非常に具体的に規定されている。
- **暗号化**: ISO の標準は非常に規定されている。
- **ユーザートレーニング**: ISO では要求されていないが、NIST では決めつけられている。

日本におけるクラウドインフラストラクチャーの実装

実装の詳細

- 重要なクラウドインフラストラクチャー向けのものをお客様次第で実装。
- NIST の 800-171 は部分的に構造化されている。

日本向けの重要性

- 日本やその他の国は FedRAMP のプログラムに注目すべき。
- 米国以外の国民に対してサービスとして提供可能。

セキュリティコントロールの比較

- ISO27017、NIST800-171、FedRAMP の比較。
  - **ISO27017**: クラウド用の標準。
  - **NIST800-171**: 部分的に構造化されている。
  - **FedRAMP**: 非常に具体的に規定されている。

- Other frameworks like ISO 27017 and NIST 800-171 are deemed inadequate in comparison.

Comparison of Frameworks

- **ISO 27017**:
  - Highly subjective, leaving critical security controls up to the discretion of the cloud service provider.
- **NIST 800-171:**
  - More structured but not specifically designed for cloud environments.
- **FedRAMP**:
  - Highly prescriptive, specifying exact controls and methods, such as FIPS 140-2 and 140-3 validated cryptographic modules for data encryption.

Example: Encryption Standards

- **ISO 27017**: Recommends encryption based on data sensitivity but lacks specific standards.
- **NIST 800-171**: Requires encryption but allows organizations to choose cryptographic methods.
- **FedRAMP**: Mandates the use of specific validated cryptographic modules for data in transit and at rest.

Japan's Need for a Sovereign Cloud

- **Highly Secure Sovereign Cloud**:
  - Japan should develop its own highly secure cloud, operated and owned by Japanese companies.
  - This cloud should adhere to the highest levels of compliance and security.

Cloud Security in Highly Regulated Industries

Importance of Secure Cloud Infrastructure

- **Insecurities in Cloud Infrastructure**:
  - Cloud infrastructure supporting numerous customers must be highly secure to prevent breaches.
  - Example: The Cloud Hopper attack where Chinese hackers infiltrated from the

日本におけるクラウド展開の事例

Keio クラウドのイニシアティブ

- 大変セキュアなクラウドでコンプライアンスに従ったものを日本において実装。
- 2ヶ月で実現。

展開の詳細

- 全てのコンフィギュレーション、細かい構成までセキュリティコントロールを日本で展開。
- 管理のレイヤーはアメリカに留め、サービスは東京にある。
- プライベートな太平洋にまたがったコネクションを通じてつながっている。

分散化の可能性

- 太平洋にまたがって展開可能。
- 日本国内でも分散化され、一元管理と一元セキュリティの実現が可能。

ソリューションとテクノロジー

現在のソリューション

- 重要インフラを石板にするためのソリューションが存在。
- パッケージや単金ソリューションが提供可能。

日本への提供

- 日本の防衛省及びインフラに対して提供可能。
- 日本の市民が運用可能。

エコシステム

- エコシステム全体が存在。
- FedRAMP のプログラムについての説明。

FedRAMP の最新状況

法律化

- 昨年 FedRAMP は法律になった。
- 10 年かかったが、今や法律となっている。

サプライチェーンの検証

- 今年はサプライチェーンを中心に検証。
- ハードウェア、ソフトウェアから全てのシステムのコンポーネントに関して検証。

日本の政府クラウドの現状

山本さんの説明

- **自己紹介**
  - デジタル庁でデジタルクラウドオフィサーを務めている。
  - 10 年以上クラウドサービス業界での経験があり、システムインテグレーターとしても 15 年の経験がある。

management system into all tenants.

- **Inconsistencies Across Authorizations**:
  - Multiple authorizations can create inconsistencies.
  - Critical areas include audit logging, physical security, continuous monitoring, configuration management, and data backup.
- **Security Standards**:
  - **NIST 800-171**: Mandates security awareness training but allows flexibility in content and timing.
  - **FedRAMP High**: Requires specific role-based training with defined frequency, content, and federal compliance reporting.

J-RAMP Keio Cloud Initiative

- **Announcement**:
  - Professor Tezuka announced the J-RAMP Keio Cloud initiative.
  - Requested by CEO and co-founder Lewis Mayberg.
- **Implementation**:
  - Achieved full FedRAMP compliance in less than two months.
  - Unique deployment: Management layer in the US, service delivery layer in Tokyo, connected via a private trans-Pacific connection.
  - Reasons: Isolate in the US for physical protection and demonstrate highly distributed deployment.

FedRAMP Program in the United States

- **Legal Status**:
  - FedRAMP was written into law last year after a decade.
- **Focus Areas**:
  - **Cryptographic Modules**: Transition from FIPS 140-2 to 140-3.
  - **Supply Chain**: New requirements for validating supply chain components.

- **政府クラウドの概要**
  - **基本ポリシー**
    - 公共セクター、政府関連のサービスに特化。
    - 認証プログラム「ヒズマップ」を導入。
  - **データの秘密レベル**
    - レベル 1 と 2 のデータは政府クラウドに格納。
    - レベル 3 のデータは国防関連で、オンプレミスや専用クラウドに格納。
- **クラウドサービスのメリット**
  - **アジリティ、フレキシビリティ、コスト効果**
    - インフラをコードとして定義し、プロビジョニングが可能。
    - API を呼び出してインフラ全体のプロビジョンが可能。
  - **セキュリティ**
    - 全てのコンフィギュレーションの変化やパラメーターを記録。
    - ミスコンフィグレーションや間違った運用を防ぐための監視。
- **クラウドサービスプロバイダーとの契約**
  - 5 つのクラウドサービスプロバイダーと契約。
  - Sakura インターネットと昨年契約を締結。
- **今後のステップ**
  - ユーザーがクラウドサービスプロバイダーの機能を利用し、ナショナルサービスクラウドプロバイダーとしての機能をステップバイステップで進める。

オーストラリアのクラウドプロジェクト

クレアさんの説明

- **自己紹介**
  - 国家安全保障及びサイバーセキュリティ全般を担当。
- **オーストラリア政府のクラウド戦略**
  - **クラウド調達のアレンジメント**
    - 規模の経済と総合運用制を追求。
    - セキュリティの要件、コンプライアンス、ガバナンスを提示。
  - **セキュアクラウドストラテジー**
    - 2018 年から続いており、現在見直し中。
    - デジタルレジリエンスを実現するために生産。
- **セキュリティとサイバーセキュリティ**
  - **保護されたクラウド**
    - 1 億ドルをかけて構築。

Japan's Government Cloud

Overview by Norihito Yamamoto

- **Background**:
  - Chief Cloud Officer of Digital Agency, with over 10 years in cloud service industries.
- **Government Cloud**:
  - Proper noun for common cloud services for central and local governments.
  - Many local government bodies are migrating their systems to the government cloud.
- **Confidentiality Levels**:
  - Defined three tiers: Level 1, Level 2, and Level 3.
  - Government cloud deals with Level 1 and Level 2 data; Level 3 data (e.g., defense data) stored elsewhere.
- **Security Focus**:
  - Emphasis on detecting misconfigurations or misoperations.
  - Use of infrastructure as code (IAC) for provisioning and logging configurations.

Contract with Sakura Internet

- **National Cloud Service Provider**:
  - Contracted under conditions to develop specific features and functions.
  - Aim to raise the level of national cloud service providers.

Australia's Cloud Implementation

Overview by Australian Government Representative

- **Protected Cloud**:
  - Part of IT modernization, with a cloud procurement panel arrangement.
  - Ministries develop clouds suitable for their business needs.
- **Security and Compliance**:
  - Secure cloud strategy since 2018, currently under review.
  - Australian Cyber Security Centre provides cybersecurity guidance.
  - Certification framework: IRAP
    - センシティブレベルのデータを AWS およびマイクロソフトを活用して保護。
  - **ゼロトラストアーキテクチャ**
    - アイデンティティ管理とアクセスのセグメント分け。
    - 多要素認証を使用してセキュリティを強化。
- **トップシークレットクラウドプロジェクト**
  - オーストラリアのシグナルディレクトデータで行われている。
  - 10 年間で 24 億ドルをかけるプロジェクト。

共通の課題と次のステップ

- **主権とセキュリティ**
  - 日本とオーストラリアのクラウド戦略には共通の課題がある。
  - セーフクラウドの実現に向けて一歩一歩進める必要がある。

クラウドサービスに関する政府の考え方

調達ガイドライン

- **ISMAP の定義と役割**
  - 2016 年、2018 年に ISMAP が定義され、日本の政府調達に関するガイドラインとして機能。
  - 経産省、総務省、デジタル省、リスクの 4 つの省庁が共同で定義。
  - ISMAP に認定されたものでなければ、政府は調達できない。
  - **ISMAP-LIU**
    - ローインパクトのサービスに関するガイドライン。

プロバイダーサイドの課題

- **サクラインターネットの例**
  - 国内のデータセンターとクラウドサービス、アプリケーションサービスのプロバイダー。
  - サクラインターネットは ISMAP に最初に認証されたプロバイダー。
  - 国内企業が政府レベルのサービスを提供するためのサポート。

オペレーション側の課題

- **政府クラウドの運用**
  - クライアント側の管理ストラクチャー、リアルタイムモニタリング、サイバーセキュリティの対応が弱い。
  - サイバーセキュリティインシデント時のリアルタイム対応が必要。

テクノロジーの将来的なトレンド

AI サービスとクラウド

(Information Security Registered Assessors Program).

Department of Foreign Affairs and Trade

- **Cyber Uplift**:
  - Major cyber incident (Log4J) led to increased investment in cyber security.
  - Use of AWS and Microsoft for protected cloud, ensuring data sovereignty.
- **Zero Trust Architecture**:
  - Multi-factor authentication and segmentation to limit access.
  - Automated processes to ensure only necessary access.

Top Secret Cloud Project

- **Development**:
  - Collaboration with Amazon Web Services.
  - Ten-year plan with a $2.3 billion investment.
  - High-level security and access requirements for national intelligence community.

Common Issues Across Three Countries

Sovereignty

- **Discussion**: Sovereignty was identified as a common issue across the three countries.
  - **Agreement**: All participants acknowledged that sovereignty is a significant concern.
  - **Example**: Claire-san mentioned that sovereignty is a shared issue, indicating a consensus among the countries involved.

Open Floor Discussion

Murai-sensei's Input

- **Invitation**: Murai-sensei was invited to share his thoughts on any topic of his choice.
  - **Quote**: "Murai-sensei, you can talk anything you want. Anything I want."

Certification Costs and Challenges

- **High Costs for Certification**
  - "$200,000 for just one product."
- **AI サービスのデータ要件**
  - 膨大なデータが必要で、非常に高価。
  - ローカルタイプのものに移行する可能性。
- **エッジコンピューティング**
  - AI の処理が分散化し、セキュリティの話も変わってくる。
  - エッジベースのモデルやアーキテクチャーでのセキュリティが必要。

セキュリティフレームワークの変化

- **AI とセキュリティ**
  - ハイパースケールのクラウドで展開される AI サービス。
  - エッジ側の AI サービスでのセキュリティリスク。

認定プロセスとコスト

FedRAMP 認定

- **コストとプロセス**
  - 一つのプログラムで 20 万ドルのコスト。
  - 小さな企業やスタートアップには厳しい状況。
  - 410 のセキュリティコントロールと 1000 以上のプロセスコントロールが存在。

政府クラウドシステムの共通点と違い

- **アメリカ、オーストラリア、日本の比較**
  - セキュリティフレームワークの違い。
  - FedRAMP をフォローし、JRAMP の実装に取り組む必要。

情報共有とプロセス改善

- **進化するプロセス**
  - 情報共有とプロセスの改善が必要。
  - 連携の重要性。

Action Items

[ ] FedRAMP の第 4 回目のアセスメント結果を確認

[ ] FedRAMP のオンラインステータスを定期的にチェック

[ ] 2027 年に向けたセキュリティ対策の強化

[ ] サイバーイニシアムの詳細を確認し、実行計画を立てる

[ ] クラウド利用に関するリスク評価の実施

[ ] オンプレミスでの AI 運用の検討

[ ] セキュリティとコンプライアンス機能の強化

[ ] 日本におけるクラウドセキュリティの高セキュリティ試験カーブの実装計画を立てる

[ ] 日本の主権クラウドの必要性についての詳細な調査を行う

○ Only large companies can afford certification costs. ○ Small companies or startups find it tough to pay such amounts. **FedRAMP Certification** • **Process and Importance** ○ Grueling process since 2003. ○ 410 security controls and 1,000-plus sub-controls in the FedRAMP high process. ○ No security control can be comfortably omitted. ○ FedRAMP controls have consistently mitigated breaches over the past seven years. • **Global Perspective** ○ Similarities in government cloud systems across three countries. ○ Differences in security frameworks. ○ FedRAMP considered the highest security process. ○ Japanese companies need to follow FedRAMP and implement J-RAMP. **Continuous Improvement in Security Processes** • **Living Documents and Systems** ○ Industry processes and documents are constantly evolving. ○ Importance of sharing information and being open-minded. ○ Continuous improvement is essential regardless of the topic. **Action Items** [ ] Support Japan's digital resiliency initiative with a tiered control structure similar to FedRAMP. [ ] Complete the fourth FedRAMP high-ready annual assessment for CyCloud. [ ] Develop a strategy for shifting AI workloads to edge or on-prem solutions. [ ] Evaluate and adopt FedRAMP security requirements for cloud infrastructure. [ ] Initiate the development of a highly secure	[ ] FedRAMP のプログラムに関する日本向けの提案書を作成する [ ] 日本国内でのクラウドインフラストラクチャーの分散化計画を策定する [ ] 日本のクラウドサービスプロバイダーのレベルを上げるための条件付き契約の進行 [ ] オーストラリアのトップシークレットクラウドプロジェクトの進行状況の確認 [ ] JRAMP の実装に取り組む [ ] 情報共有とプロセス改善

sovereign cloud for Japan. [ ] Develop and evolve ISMAP to address current technological advancements and security needs. [ ] Improve client-side management structures for better handling of cybersecurity incidents and real-time monitoring. [ ] Adapt security frameworks to accommodate future trends in AI and edge computing. [ ] Follow up on FedRAMP implementation for Japanese companies. [ ] Implement J-RAMP in alignment with FedRAMP standards.	

1.27 D1-P13 Panel: Strengthening Cyber Contingency Planning in the Asia Pacific Region

Moderator: ADM(Ret.) Dennis Blair Panelists: - Greg Rattray - Jun Murai - Chris Capper (Cyber Attaché North East Asia (Political Section), British Embassy Tokyo) - Jon Chung (ORBIS) - Gloria Glaubman (Senior Cyber Advisor, U.S. Embassy Japan)	モデレーター：デニス・ブレア パネリスト： - グレッグ・ラットレイ - 村井 純 - クリス・キャッパー（駐日英国大使館 サイバーセキュリティー担当官（政治部）） - ジョン・チュン（ORBIS） - グロリア・グラウブマン（在日米国大使館 サイバーアドバイザー）
Overview This speech summarizes the key points from a series of meetings and discussions on cybersecurity contingency planning in the Asia-Pacific region, focusing on multinational cooperation, operational readiness, and public-private partnerships. The content was created on 2024-10-30. **Introduction** • **Audience Participation**: The session began with an interactive segment comparing cyber attack and defense to sports, specifically basketball and football, to illustrate the constant competition in cybersecurity. ○ **Basketball vs. Football**: Audience was asked to vote on whether cyber attack and defense are more like basketball (high	サイバー攻撃，国家間協力，ランサムウェア **テーマ** この講演では、サイバー攻撃と防御の競争、各国のサイバー防御の取り組み、ランサムウェアとサイバー犯罪の影響について議論されました。また、国家間のサイバーセキュリティ協力やゼロトラストアプローチ、オープンソースインテリジェンスの自動化などのトピックも取り上げられました。 **要点** 1. サイバー攻撃と防御の競争 2. サイバーセキュリティの準備の重要性 3. 各国のサイバー防御の取り組み 4. アメリカのセキュリティ企業の支援 5. ロシアのウクライナ侵攻とサイバー防御 6. 中国のサイバー攻撃の予測 7. 国家間のサイバーセキュリティ協力 8. ランサムウェアとサイバー犯罪の影響 9. 国家のセキュリティ計画 10. 民間部門と政府の協力

scoring) or football (low scoring). The results were evenly split.
  - **Objective**: Aim to have an offense like basketball (high scoring) and a defense like football (low scoring).

Cybersecurity Preparation

Importance of Pre-Attack Preparation

- **Preparation Steps**: Emphasized the need for scouting opponents, understanding capabilities, making plans, and practicing before any cyber attack occurs.
- **Panel Focus**: Discussed the necessary steps for cybersecurity in different countries and companies before any breach.

Greg Rattray's Remarks

- **Experience**: Shared insights from working with American cybersecurity companies in Taiwan.
- **Model Application**: Discussed applying a proactive cyber defense model to strengthen defenses against potential Chinese cyber aggression.
- **Multinational Involvement**: Highlighted the importance of involving multiple nations (Japan, U.S., Taiwan, South Korea, Philippines) in contingency planning.
- **Ransomware and Criminal Activities**: Addressed the impact of ransomware and criminal activities on public safety and national security.
- **State Department Project**: Mentioned involvement in a project to help the coast with national security cyber contingencies.
- **Scenario Planning**: Stressed the importance of identifying specific scenarios and preparing coordinated responses.
- **Recent Developments**: Noted that JCDC and DHS's CISA have started specific

ハイライト

- "サイバー攻撃、サイバー防御、これはバスケットボールのようだと思う人、つまり得点というのは 120 対 110 とかそういう得点ではないかと思う人、それからアメリカンフットボールとかでは、さっきのような、つまり得点としては 1 対 0 ぐらいのスコアしか取れないだろうと思うか。"
- "敵を知り、民主からを知れば、百戦がやるからじゃない。"

章とトピック

サイバーセキュリティの準備

サイバー攻撃が発生する前に、どのような準備が必要かについての知識。

- **要点**
  - 敵の能力を評価する
  - 自分のチームの能力を測る
  - 計画を策定する
  - 練習を重ねる

国家間のサイバーセキュリティ協力

複数の国が協力してサイバー攻撃に対抗するための戦略。

- **要点**
  - 各国のサイバー防御の取り組み
  - 協力して攻撃者の得点を抑える方法
  - 重要インフラの保護

ランサムウェアとサイバー犯罪

ランサムウェア攻撃やその他のサイバー犯罪が国家の安全保障に与える影響。

- **要点**
  - ランサムウェア攻撃の警告
  - サイバー犯罪の資金調達方法
  - 国家の安全保障への影響

台湾のデジタル政府構想

台湾は領土が失われてもデジタル政府として生き延びるための構想を持っている。

- **要点**
  - デジタル台湾の構想
  - 領土が失われても政府サービスを提供する方法

日本のデータホスティングの準備

日本が他国のデータをホスティングする準備が整っているかどうかについての疑問。

- **要点**
  - データホスティングの重要性

contingency planning and exercises. • **Volt Typhoon**: Highlighted the urgency around Chinese intrusions into U.S. critical infrastructure. **Multinational Response to Cyber Threats** • **East Asia Focus**: Emphasized the need for orchestrated multinational responses to significant cyber threats, particularly in East Asia. • **Taiwan Situation**: Discussed the potential for Chinese aggression against Taiwan and the need for coordinated planning between the U.S., Japan, and Taiwan. **Complex Contingency Planning** • **Stages and Escalation**: Explained the need to consider different stages and escalation in contingency planning. • **North Korea's Role**: Addressed the potential for North Korea to exploit situations opportunistically, particularly in the context of Taiwan. **Operational Readiness** • **Key Sectors**: Identified telecommunications, electric power, and financial services as critical sectors for national security and cybersecurity. • **Stakeholder Collaboration**: Stressed the importance of getting the right stakeholders at the table for effective planning and execution. • **New York Cyber Task Force**: Mentioned the task force's role in enhancing readiness for national cyber defense through operational readiness. **Practical Implementation** • **Action-Oriented Approach**: Emphasized the need for clear responsibility, accountability, and regular progress reviews to ensure effective planning and execution. • **Practice and Execution**: Highlighted the	○ 日本の準備状況 **サイバーセキュリティの重要性** サイバーセキュリティの観点から、日本がどのように準備を進めるべきかについての議論。 • **要点** ○ サイバーセキュリティの方向性 ○ レジリエンスの考え方 **南シナ海のケーブル敷設** 南シナ海における新しいケーブルの敷設とその影響。 • **要点** ○ ケーブル敷設の重要性 ○ 特定の海域を避ける理由 **インテリジェンスと情報共有** 迅速な意思決定のための情報共有の重要性。 • **要点** ○ 近代的なアーキテクチャの使用 ○ セキュアでスケーラブルなシステム **非対称的なサイバーセキュリティ** 非対称的なアプローチでサイバーセキュリティを強化する方法。 • **要点** ○ 非国家及び非英国家のアクター ○ 迅速な情報共有の必要性 **ゼロトラストアプローチ** ゼロトラストに基づいたアプローチでロバストな防御を構築する方法。 • **要点** ○ ゼロトラストの概念 ○ ロバストな防御の重要性 **オープンソースインテリジェンスの自動化** オープンソースインテリジェンスを自動化してアクショナブルなインサイトに変える方法。 • **要点** ○ 自動化の重要性 ○ アクショナブルなインサイト **リアルタイムインテリジェンスアクセス** リアルタイムでインテリジェンスにアクセスすることの重要性。 • **要点** ○ 迅速な意思決定 ○ 需要インフラの迅速な発表 **サイバーコンティジェントラーニング** サイバーコンティジェントラーニングの 3 つの領域に注力する方

importance of practicing and executing plans to be better prepared for cyber threats. **Japan's Readiness** • **Digital Taiwan Concept**: Discussed the idea of Japan accommodating Taiwan's national data in case of physical land occupation. • **Natural Disasters**: Highlighted Japan's experience with natural disasters as a foundation for building cybersecurity resilience. **Cyber Deterrence** • **Deterrence Discussions**: Shared insights from conversations with Chinese counterparts about the risks of doomsday cyber attacks. • **Human Concern**: Noted a general concern about the potential devastation and retaliation from unlimited cyber attacks. **South China Sea and Submarine Cable Topology** **Issues and Challenges** • **Cable Cuts and High Error Rates** ○ The topology in the Pacific, particularly from Tokyo to Singapore, faces significant issues. ○ High cut rates due to fissure boards staying on the ocean surface and cutting cables. ○ Recovery efforts are lagging due to limited resources in the ocean. **Contingency Planning** • **Alternative Routes and Redundancy** ○ The U.S. is focusing on creating redundancy in submarine cable topology in the Asia-Pacific. ○ Collaboration with South America, Australia, and the Japanese government to add alternative routes. ○ Emphasis on planning for space	法。 • **要点** ○ センサーの増加 ○ 能力を高める方法 **APT（高度持続的脅威）** APT の脅威とその対策についての議論。 • **要点** ○ APT の定義 ○ 脅威の深刻度 **サイバーディフェンスの計画** サイバーディフェンスの計画とその実行方法。 • **要点** ○ サイバーディフェンスの重要性 ○ 計画の具体例 **サプライチェーンセキュリティ** サプライチェーンセキュリティの重要性とその対策。 • **要点** ○ サプライチェーンの脆弱性 ○ セキュリティ対策 **サイバーセキュリティの国際協力** サイバーセキュリティにおける国際協力の重要性。 • **要点** ○ 国際協力の具体例 ○ 協力のメリット **情報共有の重要性** 情報共有の重要性とその方法。 • **要点** ○ リアルタイムでの情報共有 ○ 政府と業界の連携 **レジリエンスと冗長性** レジリエンスと冗長性の重要性とその実現方法。 • **要点** ○ レジリエンスの概念 ○ 冗長性の具体例 **共同演習の重要性** 共同演習の重要性とその実施方法。 • **要点** ○ 共同演習のメリット ○ 具体的な演習例 **クリティカルインフラの保護** クリティカルインフラの保護の重要性とその対策。 • **要点**

connections as part of the redundancy strategy. **Data Integration and Cybersecurity in Taiwan** **Data Integration Project** • **Catalyst Product** ○ John Chung is working on a data integration project in Taiwan using Catalyst. ○ Catalyst is an integrated data grid based on zero trust principles. ○ Integrates technologies from CloudFlare, Zanderval authentication, and Kyber encryption. ○ Uses GraphQL adapters for data sharing. **Cybersecurity Challenges and Strategies** • **Asymmetric Advantage** ○ Traditional methods of outspending adversaries are no longer feasible. ○ Emphasis on leveraging asymmetric advantages in cybersecurity. ○ Rapid sharing of data across allies and sectors to enhance command and control. • **Interoperability** ○ Urgent need for interoperability in cybersecurity. ○ Aligning people, processes, and technology to foster collaboration. ○ Standards processes for incident response and integrating diverse systems. • **Data Burden and Analytics** ○ Difficulty in sifting through large amounts of data. ○ Importance of harnessing open-source intelligence and automating data transformation. ○ Real-time access to intelligence for rapid protection of critical infrastructure. **Public-Private Partnerships in Cybersecurity** **Understanding Threats** • **Advanced Persistent Threats (APTs)**	○ クリティカルインフラの定義 ○ 保護対策 **サイバー攻撃の抑止** サイバー攻撃の抑止方法とその重要性。 • **要点** ○ 抑止の概念 ○ 具体的な抑止方法 **アトリビューション評価の難しさ** サイバー攻撃におけるアトリビューション評価の難しさとその対策。 • **要点** ○ アトリビューション評価の定義 ○ 評価の難しさ **宿題と提案**

○ Importance of knowing the opponent and understanding their motivations and target sets. ○ Cybersecurity advisories provide information on threat actors, impact, severity, and mitigation steps. **Government-Led Initiatives** • **Cybersecurity Information Sharing Act (2015)** ○ U.S. legislation requiring NSA and DOD to share critical threat information with private industry partners and defense industrial base. **Cooperative Cybersecurity Planning** **Overview of Cooperative Cybersecurity Planning** • **Know the Landscape**: Understanding adversaries and the cyber environment. • **Information Sharing**: A core tenet of active cyber defense. • **USG Initiatives**: Cooperative cybersecurity planning and contingency planning. **Bilateral and Multilateral Agreements** • **U.S.-Japan Cybersecurity Agreement**: ○ Mechanism for sharing cybersecurity intelligence and information. ○ Collaboration on cyber defense strategies. ○ Joint cybersecurity exercises. • **Quadrilateral Security Dialogue (U.S., India, Japan, Australia)**: ○ Integration of cybersecurity into the security agenda. ○ Focus on sharing threat intelligence. ○ Developing a secure supply chain for telecommunications. ○ Countering cyber-enabled threats affecting economic security. • **U.S.-Japan-Philippines Trilateral Dialogue**: ○ Inaugural Trilat on cyber in a digital	

dialogue.

- Addressing cybersecurity capabilities, skilled workforce, and information sharing.

Key Takeaways

- **Foundation of Active and Proactive Cyber Defense**: Information sharing is crucial.

Cyber Threat Landscape in the Indo-Pacific

Key Points on Cyber Threats

- **Indo-Pacific as Ground Zero for Cybercrime:**
  - Blurring lines between nation-states and cybercriminals.
  - Nation-states gain scale and deniability.
  - Cybercriminals gain a new revenue stream and protection from prosecution.
- **Concentration of Cyberactivity**:
  - Increased cyber activity in conflicts and regional tensions.
  - More nation-states involved in offensive cyber operations (e.g., Vietnam).
- **Accidental and Deliberate Contingencies**: Preparation for both is essential.

UK's Approach to Cyber Deterrence

Three-Step Approach to Deterrence

- **The Sword**:
  - Altering the risk calculus of an attacker through fear of reprisal or imposition of cost.
  - Examples: Cyber sanctions and political attribution.
  - Importance for Japan to have a unilateral cyber sanctions regime.
- **The Shield**:
  - Preventative measures to block threats.
  - Technical advisories as useful but limited to specific threats.
- **The Armour**:
  - Resilience as the last line of defense.
  - Practices: Secure by design, cyber

hygiene. **Cyber Contingency Planning** • **Defining Cyber Contingency**: ○ Seen as a contingency where cyber is an aspect, not the sole focus. • **Coordination in Public-Private Partnerships**: ○ Importance of coordination between recipient and giver. ○ Ensuring recipients get what they need, not just what is available. • **Information Sharing:** ○ Critical for understanding and defending against threats. ○ Importance of transparency and communication. **High-Level Recommendations** **Key Recommendations** • **Sharing Knowledge and Lessons Learned**: Essential for collective defense. • **Prioritization**: Focus on the highest importance tasks. • **Redundancies and Resilience**: Backup within networks is crucial. • **Planning and Training**: Importance of joint exercises and preparedness. **Final Thoughts** • **Building Greater Deterrence**: Making cyber attacks unthinkable and manageable. • **Benefits of Information Technology**: Leveraging the positive aspects while mitigating risks. **Action Items** [ ] Start planning sessions with Japanese Cyber Command, U.S. Cyber Command, and electric power companies. [ ] Review and implement recommendations from the New York Cyber Task Force report on operational readiness. [ ] Develop and practice specific contingency plans for potential cyber threats in East Asia.	

[ ] Plan and implement alternative routes for submarine cables in the Asia-Pacific. [ ] Enhance data sharing mechanisms using Catalyst and other integrated technologies. [ ] Foster interoperability by aligning people, processes, and technology in cybersecurity efforts. [ ] Automate data transformation to handle the data burden and improve decision-making. [ ] Leverage government-led initiatives to improve public-private partnerships in cybersecurity. [ ] Establish a unilateral cyber sanctions regime for Japan. [ ] Enhance coordination in public-private partnerships for cyber defense. [ ] Increase transparency and communication in information sharing agreements. [ ] Develop mutual support agreements similar to the UK (United Kingdom) – ROK (Republic of Korea) agreement.	

1.28 D1-S15 Speech: National Security

Wen Masters	ウェンマスターズ
Post-Quantum Cryptography, MITRE, Quantum Computing **Theme** This speech, held on October 30, 2024, covers the principles of post-quantum cryptography, the challenges posed by quantum computing advancements, and the role of MITRE in addressing these issues. Key topics include the use of quantum mechanics in cryptography, the threat of Shor's algorithm to current encryption methods, and the U.S. government's mandate to prepare for a post-quantum future. Additionally, the lecture discusses MITRE's coalition efforts to establish standards and educate on post-quantum cryptography. **Takeaways** 1. MITRE is a mission-driven, not-for-profit organization working with	**概要** この文書は、2024 年 10 月 30 日に行われた講演の議事録です。議論の主なテーマは国家安全保障メモ、PQCC の構成要素、コミュニティの改善に関するものでした。以下に、各セクションの詳細とアクションアイテムをまとめています。 **国家安全保障メモに関する議論** **重要性** • **政府の使命**: アメリカ政府の使命は国家安全保障メモを持つこと。 • **推奨事項**:「このようなビジネスコンピューティングを確保することが必要です。これは私の推奨事項です。」 • **課題**:「これは大規模な取り組みであり、非常に困難になるでしょう。」 **地方政府の準備** • **PQC の役割**: 地方政府による準備の一例として PQC が挙げられる。 • **国際システム**: 国際システムが存在し、要求事項が

governments.

2. Quantum mechanics principles and probabilistic approaches are used in post-quantum cryptography.
3. Factorization of large numbers into prime factors is a mathematically hard problem for classical computers.
4. Advances in quantum computing and Shor's algorithm pose a threat to current encryption algorithms.
5. Adversaries are harvesting data to decrypt later with quantum computers.
6. The U.S. has a government mandate to prepare for the post-quantum future.
7. NIST finalized three post-quantum cryptography standards in mid-August 2024.
8. The migration to post-quantum cryptography is challenging due to future threats and multiple algorithms.
9. International standards for post-quantum cryptography are not yet agreed upon.
10. Different countries have varying approaches to post-quantum cryptography implementation.

Chapters & Topics

Post-Quantum Cryptography

Post-quantum cryptography involves using quantum mechanics principles and probabilistic approaches to develop cryptographic algorithms that are secure against quantum computer attacks.

- **Keypoints**
  - Quantum mechanics principles and probabilistic approaches are used.
  - Factorization of large numbers into prime factors is a hard problem for classical computers.
  - Advances in quantum computing and Shor's algorithm pose a threat to current encryption algorithms.

異なる。

国際的な整合性

- **グローバルな視点**:「ヨーロッパや日本を含む多くの国々が完全に一致しています。」
- **標準の追従**: これらの標準に従う努力をしている。

PQCC の構成要素

標準の決定

- **国際標準の使用**: 国際標準の使用方法を決定することが重要。
- **未解決の部分**: まだ見えていない部分が多いため、使用方法を明確にする必要がある。

ベンダーとアルゴリズムの開発

- **ベンダーの開発**: ベンダーの開発方法。
- **アルゴリズムの開発**: アルゴリズムの開発方法。
- **ポスト量子標準の使用**: ポスト量子標準の使用方法。

教育

- **一般教育**: 一般市民向けの教育。
- **労働力教育**: 労働力向けの教育。
- **追加項目の考慮**: 追加項目として何を考慮すべきかを明確にする必要がある。

コミュニティの改善

コミュニケーション

- **コミュニティの改善**:「このコミュニティをより良い場所にするために何ができるかを話し合っています。」
- **プログラムの知識共有**: このプログラムで知っていることをどのように伝え、共有するか。

アクションアイテム

[ ] 国際標準の使用方法を決定する。

[ ] ベンダーとアルゴリズムの開発方法を明確にする。

[ ] 一般市民と労働力向けの教育プログラムを策定する。

[ ] コミュニティ改善のための具体的なアクションプランを作成する。

• **Considerations** • The migration to post-quantum cryptography is challenging due to future threats and multiple algorithms. • International standards for post-quantum cryptography are not yet agreed upon. • Different countries have varying approaches to post-quantum cryptography implementation. **MITRE's Role in Post-Quantum Cryptography** MITRE is a mission-driven, not-for-profit organization working with governments to address national security issues, including the preparation for a post-quantum future. • **Keypoints** ○ MITRE is a mission-driven, not-for-profit organization. ○ MITRE is working with governments to address national security issues. ○ MITRE has established a coalition (PQCC) to address post-quantum cryptography challenges. • **Considerations** • The PQCC coalition has four work streams: standards, education, implementation, and cryptographic inventory and agility. • The PQCC coalition is seeking like-minded individuals and organizations to join their efforts. **Assignments & Suggestions**	

1.29 D1-S14 Day 1 Closing

Jun Murai	村井 純
Post-Quantum Cryptography, Passkeys, Cybersecurity **Theme** This speech covers key topics in cybersecurity, including the significance of post-quantum cryptography, the industry's shift from passwords to passkeys, and the importance of public-private partnerships in protecting critical infrastructure.	PQC, デジタルトランスフォーメーション, 国際協力 **テーマ** この講演では、PQC（Post-Quantum Cryptography）の技術的先進性、セキュリティーズの関係性、パスワードからパスキーへの移行、デバイス認証の展開、NIST やスマイターによる PQC の研究、DPP（官民協力）の重要性、自由インフラにおける民間セクターの役割、デジタルトランスフォーメーションの重要性、国際協力の重要性、インターネットとサイバ

It also highlights the role of digital transformation in national security and the need for international collaboration to establish cybersecurity standards.

Takeaways

1. Post-quantum cryptography (PQC) and its relationship with cybersecurity.
2. The industry's shift from passwords to passkeys for device authentication.
3. Rapid deployment of new authentication methods once decisions are made.
4. The importance of public-private partnerships in critical infrastructure protection.
5. The role of digital transformation in national security.
6. International collaboration for establishing standards in cybersecurity.
7. The significance of global internet systems and cyberspace.
8. The need for like-minded countries to work together on cybersecurity standards.

Chapters & Topics

Post-Quantum Cryptography (PQC)

An advanced technology related to cybersecurity, focusing on cryptographic systems that are secure against quantum computer attacks.

- **Keypoints**
  - PQC is a significant technological advancement.
  - It is being actively researched by groups like the National Institute of Standards and Technology (NIST) and MITRE.

Shift from Passwords to Passkeys

The industry's movement towards replacing traditional passwords with passkeys for device authentication.

- **Keypoints**
  - Passkeys are becoming increasingly popular.
  - Rapid deployment of passkeys is possible

ースペースの一体性について議論されました。

要点

1. PQC 両種体制の技術的先進性
2. セキュリティーズの関係性
3. パスワードからパスキーへの移行
4. デバイス認証の展開
5. NIST やスマイターによる PQC の研究
6. DPP（官民協力）の重要性
7. 自由インフラにおける民間セクターの役割
8. デジタルトランスフォーメーションの重要性
9. 国際協力の重要性
10. インターネットとサイバースペースの一体性

ハイライト

- "国際協力の重要性です。インターネットのステップというのは、サイバスペースとして一つです。世界中がつながっています。"

章とトピック

PQC 両種体制

PQC（Post-Quantum Cryptography）両種体制は、量子コンピュータに対抗するための暗号技術であり、技術的に非常に先進的な内容です。

- **要点**
  - 量子コンピュータに対抗するための暗号技術
  - 技術的に先進的な内容

パスワードからパスキーへの移行

業界全体でパスワードからパスキーへの移行が進んでおり、デバイス認証が広がっています。

- **要点**
  - パスワードからパスキーへの移行
  - デバイス認証の広がり

DPP（官民協力）の重要性

デジタルトランスフォーメーションを進める上で、官民の協力が不可欠であること。

- **要点**
  - デジタルトランスフォーメーションの重要性
  - 官民協力の必要性

国際協力の重要性

インターネットはサイバースペースとして一体であり、国際協力が重要であること。

- **要点**
  - インターネットとサイバースペースの一体性
  - 国際協力の重要性

once decisions are made. **Public-Private Partnerships** Collaborations between the public and private sectors to protect critical infrastructure and ensure national security. • **Keypoints** ○ Critical infrastructure like electricity, transportation, and communication is often driven by private companies. ○ Digital transformation has highlighted the need for joint efforts in national protection. **International Collaboration in Cybersecurity** The cooperation between countries to establish cybersecurity standards and protect global internet systems. • **Keypoints** ○ Global internet systems create a connected cyberspace. ○ Legal and data format approaches vary by nation-state. ○ Like-minded countries need to work together to establish standards. **Assignments & Suggestions**	**宿題と提案**

2 DAY 2: October 31 | West School Building 1F West Hall

2.1 D2-S1-1 Economic Security

Satoru Tezuka	手塚 悟
Cyber Security, Critical Infrastructure, Government Systems **Theme** This speech emphasized the importance of digital cyber security for national, economic, and societal security. Key points included the roles of government and private sector in maintaining critical infrastructure such as electric power and telecommunications, especially during crises. Japan's plans to implement a government cloud system, cyber intelligence system, and active defense system were also discussed. **Takeaways** 1. Digital cyber security is crucial for national security, economic security, and societal security. 2. The government plays a main role in national security. 3. The private sector is responsible for economic security, particularly critical infrastructure. 4. Critical infrastructure includes electric power and telecommunications. 5. The societal security portion involves private sector businesses and citizens. 6. Japan is planning to implement a government cloud system, cyber intelligence system, and active defense system. 7. The importance of maintaining electric power and communication during crises, such as the Ukraine situation, was emphasized. 8. Healthcare and other lifelines are considered critical infrastructure. **Chapters & Topics** **Digital Cyber Security**	経済安全保障，デジタルサイバー安全保障，重要インフラ **テーマ** この講演では、経済安全保障とデジタルサイバー安全保障戦略について議論しました。主なトピックには、重要インフラの保護、電力と電気通信、ウクライナの状況、クラウドシステム、サイバーインテリジェンスシステム、能動的な防御システム、ヘルスケアシステムのサイバーセキュリティ、次世代のエネルギー分散ネットワークのサイバーセキュリティが含まれます。 **要点** 1. 経済安全保障 2. デジタルサイバー安全保障戦略 3. 重要インフラ 4. 電力と電気通信 5. ウクライナの状況 6. クラウドシステム 7. サイバーインテリジェンスシステム 8. 能動的な防御システム 9. ヘルスケアシステムのサイバーセキュリティ 10. 次世代のエネルギー分散ネットワークのサイバーセキュリティ **章とトピック** **経済安全保障** 経済安全保障は、国家の経済的利益を保護し、重要インフラを維持するための戦略。 • **要点** ○ 経済安全保障は民間セクターが主役。 ○ 電力と電気通信が重要インフラとして挙げられる。 ○ 金融、ヘルスケア、鉄道も重要インフラに含まれる。 **デジタルサイバー安全保障戦略** デジタルサイバー安全保障戦略は、国土安全保障、経済安全保障、社会保障をデジタルおよびサイバーの観点から保護するための戦略。 • **要点** ○ 国家安全保障、経済安全保障、社会保障の 3 つの柱がある。 ○ 政府のシステム、クラウドシステム、サイバーインテリジェンスシステム、能動的な防御システムが含まれる。

The integration of digital cyber security into national, economic, and societal security frameworks. • **Keypoints** ○ Digital cyber security is essential for protecting national security. ○ Economic security relies on the private sector managing critical infrastructure. ○ Societal security involves the collaboration of private businesses and citizens. **Critical Infrastructure** The importance of critical infrastructure in economic security. • **Keypoints** ○ Electric power and telecommunications are key components of critical infrastructure. ○ Maintaining these infrastructures is crucial during crises. **Government Systems for Cyber Security** Japan's planned systems for enhancing cyber security. • **Keypoints** ○ Government cloud system ○ Cyber intelligence system ○ Active defense system **Assignments & Suggestions**	**宿題と提案**

2.2 D2-S1-2 Economic Security

Barbara Grewe	バーバラ・グルーイ
Economic Security, Cybersecurity, Ransomware **Theme** This speech explores the intersection of economic security and cybersecurity, highlighting the importance of both at micro and national levels. Key historical events such as the 1929 stock market crash and the 2001 terrorist attacks are discussed. The speech also emphasizes the critical role of cybersecurity in economic security, citing significant cyber events like WannaCry, NotPetya, and SolarWinds, and the increasing threat of ransomware attacks, particularly in the	経済安全保障，サイバーセキュリティ，官民パートナーシップ **テーマ** この講演では、国家安全保障と経済安全保障の関係、経済安全保障の定義、歴史的な経済危機やサイバー攻撃の事例、サイバーセキュリティの重要性、そして官民パートナーシップの役割について議論されました。特に、サイバーセキュリティが経済安全保障に与える影響が強調されました。 **要点** 1. 国家安全保障と経済安全保障の関係 2. 経済安全保障の定義 3. 1929 年の米国株式市場の暴落 4. 2001 年 9 月 11 日の米国同時多発テロ

healthcare sector.

Takeaways

1. Intersection of economic security and cyber security.
2. Economic security is less well defined compared to national security.
3. Economic security can be viewed at both micro and national levels.
4. Governments embrace economic security as a core function.
5. Historical economic security events include the 1929 stock market crash and the 2001 terrorist attacks.
6. Cybersecurity is crucial for economic security.
7. Examples of significant cyber events include WannaCry, NotPetya, and SolarWinds.
8. Ransomware attacks are a major threat to economic security.
9. Increase in ransomware attacks from 2022 to 2023.
10. Healthcare sector is particularly vulnerable to ransomware attacks.

Highlights

- "Weak cybersecurity has the ability to pose an existential threat to the economic security of our respective countries."

Chapters & Topics

Economic Security

Economic security refers to the ability of individuals, households, and communities to meet their basic and essential needs sustainably, as well as the national level capability to maintain secure and resilient domestic production and reliable access to global resources.

- **Keypoints**
  - Micro level: meeting basic needs such as food, shelter, clothing, health care, education, livelihoods, and social protection.
  - National level: secure and resilient

5. サイバーセキュリティの重要性
6. WannaCry の攻撃と NetPetya の影響
7. SolarWinds の影響
8. ランサムウェアの増加
9. ラーム・エマニュエル駐日米国大使の発言
10. キース・アレクザンダー長官の発言

ハイライト

- "サイバーセキュリティは明らかに経済安全保障の問題なのです。"

章とトピック

国家安全保障と経済安全保障の関係

国家安全保障と経済安全保障は切っても切れない関係にあり、経済安全保障も効果的なサイバーセキュリティに依存する。

- **要点**
  - 国家安全保障と経済安全保障の相互依存性
  - 経済安全保障の定義とその重要性

サイバーセキュリティの重要性

サイバーセキュリティは国家安全保障だけでなく経済安全保障にも重要である。

- **要点**
  - サイバー攻撃の経済的影響
  - 歴史的なサイバー攻撃の事例
- **例**
- 1929 年 10 月の米国株式市場の暴落で、3 日間で 340 億ドルの価値が失われ、DAO 平均株価は 30%も下落した。
- 2001 年 9 月 11 日の米国同時多発テロは、国家安全保障と経済安全保障の両方に大きな影響を与え、米国経済に 1000 億ドルを超える損害をもたらした。
- WannaCry の攻撃は世界中で約 40 億ドルの損失をもたらし、NetPetya は被害総額約 100 億ドルを超えた。
- SolarWinds の攻撃は約 1 千億ドルの損失をもたらした。

官民パートナーシップの重要性

重要なインフラとサプライチェーンの安全確保のために官民パートナーシップが必要である。

- **要点**
  - 官民パートナーシップの役割
  - 経済的安全を確保する方法

domestic production capabilities and reliable access to global resources. • **Examples** ○ In October 1929, the U.S. stock market crashed, losing nearly 50% of its value by mid-November. Over three days, $34 billion in value was lost, and the Dow Jones Industrial Average dropped by 30%. ○ The terrorist attacks against the U.S. in September 2001 caused losses exceeding $100 billion, including lost lives, property damage, and lost production of goods and services. The stock market dropped by almost 700 points, with an estimated $1.4 trillion in value lost. **Cybersecurity and Economic Security** Cybersecurity is essential for maintaining economic security, as cyber attacks can cause significant financial losses and disrupt entire economies. • **Keypoints** ○ WannaCry attack caused $4 billion in losses globally. ○ NotPetya attack caused damages exceeding $10 billion. ○ SolarWinds cleanup cost estimated at $100 billion. ○ Ransomware attacks are increasing in number and range of victims. • **Examples** ○ In 2023, a ransomware attack shut down Nagoya port, the busiest in Japan, for three days. The attack had significant implications for international trade, and a longer shutdown could have devastated Japan's economy. **Assignments & Suggestions**	**宿題と提案**

2.3 D2-S2 Keynote Speech

Puesh Kumar (Director, U.S. Department of Energy's Office of Cybersecurity, Energy Security,	プエッシュ・クマー（米国エネルギー省サイバーセキュリティ・エネルギーセキュリティ・緊急対応局 局長）

and Emergency Response: CESER)	
Cybersecurity, Energy Systems, Resilience **Theme** This speech, held on October 31, 2024, focused on the security and resilience of U.S. energy systems. Key topics included global cyber threats to energy infrastructure, significant investments in clean energy, the evolution of the energy sector, and the emergence of virtual power plants. Strategies to address cyber threats were discussed, emphasizing the importance of hardening energy systems, increasing threat visibility, and building security and resiliency by design. The speech also highlighted collaborative efforts and initiatives like the Energy Threat Analysis Center and Cyber-Informed Engineering. **Takeaways** 1. Introduction to CESER and its focus on the security and resilience of U.S. energy systems. 2. Global perspective on cyber threats to energy infrastructure. 3. Macro trends in energy systems, including significant investments in clean energy. 4. Evolving energy sector with distributed generation and new market players. 5. Importance of multimodal communications networks for grid reliability and efficiency. 6. Emergence of virtual power plants (VPPs) and their reliance on cloud-based providers. 7. Cyber threats to energy infrastructure from nation-state actors and criminal activities. 8. Need for collaboration to address global cyber risks to energy systems. 9. Three main strategies to address cyber threats: hardening energy systems, increasing threat visibility, and building	サイバー脅威，クリーンエネルギー，インフラ **テーマ** この講演では、CESER の役割と責任、アメリカのエネルギーシステムに対するサイバー脅威、国家主体の攻撃者と犯罪活動、エネルギーインフラのセキュリティと強靭性、災害対応と物理的攻撃、クリーンエネルギーへの投資と連携、分散型発電と通信ネットワークの重要性、バーチャルパワープラント（VPP）の採用、クラウドベースのインフラストラクチャー、エネルギーインフラの規制と新規参入企業について議論されました。 **要点** 1. CESER の役割と責任 2. アメリカのエネルギーシステムに対するサイバー脅威 3. 国家主体の攻撃者と犯罪活動 4. エネルギーインフラのセキュリティと強靭性 5. 災害対応と物理的攻撃 6. クリーンエネルギーへの投資と連携 7. 分散型発電と通信ネットワークの重要性 8. バーチャルパワープラント（VPP）の採用 9. クラウドベースのインフラストラクチャー 10. エネルギーインフラの規制と新規参入企業 **ハイライト** • "エネルギーシステムに対する全てのリスクというものを我々は対応しなければなりませんし、またインフラに対するリスク体験というものを図っていかなければなりません。" • "サイバーセキュアでなければそれは信頼できない。サイバーセキュアでなければシステムは安全ではない。" **章とトピック** **CESER の役割と責任** CESER はセキュリティと米国エネルギーシステムの強靭性を担当する組織。 • **要点** ○ セキュリティと強靭性の確保 ○ 災害対応 ○ クリーンエネルギーへの投資と連携 **アメリカのエネルギーシステムに対するサイバー脅威** 国家主体の攻撃者や犯罪活動がエネルギーインフラを脅かす。 • **要点**

security and resiliency by design.

10. Sector hardening through policy work, training, exercises, and technical assistance.

Highlights

- "We have to tackle that cyber risk to these same energy systems that we are all reliant on across the globe."-- Puesh Kumar
- "If you're not cyber secure, you're not reliable. If you're not cyber secure, your system may not be safe."

Chapters & Topics

CESER and its Focus

The Office of Cybersecurity, Energy Security, and Emergency Response (CESER) focuses on the security and resilience of U.S. energy systems.

- **Keypoints**
  - CESER is part of the U.S. Department of Energy.
  - Focuses on cybersecurity, physical attacks, and climate-based risks to energy infrastructure.

Global Perspective on Cyber Threats

Cyber threats to energy infrastructure are a global issue, involving nation-states and criminal activities.

- **Keypoints**
  - Energy infrastructure is targeted by both nation-state actors and criminals.
  - Collaboration is essential to address these global cyber risks.

Macro Trends in Energy Systems

Significant investments are being made in the U.S. energy sector to support clean energy and infrastructure development.

- **Keypoints**
  - $62 billion from the bipartisan infrastructure law.
  - $369 billion from the Inflation Reduction Act.
  - $100 billion in projected private capital for

  - 国家主体の攻撃者
  - 犯罪活動
  - 重要インフラの脅威

クリーンエネルギーへの投資と連携

クリーンエネルギーに対する投資と、関連企業や自治体との連携が進んでいる。

- **要点**
  - 太陽光発電
  - 風力発電
  - 電気自動車と充電インフラ

分散型発電と通信ネットワークの重要性

分散型発電の普及に伴い、信頼性の高い通信ネットワークが必要。

- **要点**
  - 太陽光発電と風力発電
  - マルチモードの通信ネットワーク
  - 有線および無線通信

クラウドベースのインフラストラクチャー

クラウドベースのプロバイダーがエネルギーインフラのバックエンドを担当。

- **要点**
  - Amazon、Google、Microsoft
  - 冗長性の確保
  - インフラコストの削減

エネルギーインフラの規制と新規参入企業

従来の規制が適用されない新規参入企業が増加。

- **要点**
  - クラウド移行のメリット
  - 規制当局の対応
  - 新規参入企業の増加

サイバーセキュリティの重要性

エネルギーシステムのセキュリティと強靭性を確保するための取り組み。

- **要点**
  - エネルギーシステムの強化
  - 脅威の可視化
  - 国際社会との連携

セクターハードニング

エネルギーインフラの強化と新しい市場プレイヤーのベースライン確立。

- **要点**
  - 配電システムの進化

clean energy.

Evolving Energy Sector

The energy sector is evolving with distributed generation, new market players, and advanced communications networks.

- **Keypoints**
  - Shift from large centralized generation to distributed generation.
  - New market players entering the energy community.
  - Need for multimodal communications networks for grid reliability and efficiency.

Virtual Power Plants (VPPs)

VPPs are critical to the energy transition and rely on cloud-based providers.

- **Keypoints**
  - VPPs use cloud infrastructure for backend operations.
  - Security concerns with moving traditional energy infrastructure to the cloud.

Cyber Threats to Energy Infrastructure

Energy infrastructure faces cyber threats from both nation-state actors and criminals.

- **Keypoints**
  - 85% of U.S. energy infrastructure is privately owned and operated.
  - Complexity of managing thousands of utility and energy companies.
  - Focus on both IT and OT technologies to mitigate threats.

Strategies to Address Cyber Threats

Three main strategies to address cyber threats: hardening energy systems, increasing threat visibility, and building security and resiliency by design.

- **Keypoints**
  - Investing in hardening energy systems through policy, training, and technical assistance.
  - Increasing visibility of threats to get ahead of potential impacts.
  - Building security and resiliency by design
  - ベストプラクティスの確立
  - 最低限必要な要件

サプライチェーンセキュリティ

サプライチェーンセキュリティは、製造業者だけでなく、機器の所有者やオペレーターにも責任があることを認識する必要がある。

- **要点**
  - セキュリティバイデザインと運用によるセキュリティの重要性
  - 機器の適切な設定とパッチの適用

エネルギー脅威分析センター

エネルギー脅威分析センターは、業界と政府を結びつけ、脅威を調査し、緩和策を策定する役割を果たす。

- **要点**
  - 全国的な状況で脅威を把握
  - 情報共有と協力の促進

CyTRICS プログラム

CyTRICS プログラムは、脆弱性のテストを行い、メーカーと協力して緩和策やパッチを提供する。

- **要点**
  - サイバーテストの実施
  - 脆弱性の公表と緩和策の提供

セキュアバイデザイン

セキュアバイデザインは、システムエンジニアリングの設計段階からサイバーセキュリティを組み込むことを目指す。

- **要点**
  - 設計段階でのサイバーリスクの優先順位付け
  - 結果主義のアプローチ

宿題と提案

in energy systems.

Sector Hardening

Efforts to harden the energy sector include establishing baselines for new market players and developing supply chain cybersecurity principles.

- **Keypoints**
  - Establishing baselines for companies operating distribution systems and clean energy.
  - Developing supply chain cybersecurity principles with global manufacturers.

Energy Threat Analysis Center

A collaborative effort between the Department of Energy and industry partners to improve visibility of threats on private sector systems.

- **Keypoints**
  - Collaboration with over 3,000 electric utility companies.
  - Sharing information about cyber attacks across the United States and globally.

Cyber Testing for Resilient Industrial Control Systems (CyTRICS)

A program focused on deep dive cybersecurity vulnerability testing and forensic analysis of industrial control systems.

- **Keypoints**
  - Partnership with manufacturers.
  - Development of software bills of material.
  - Public release of vulnerabilities and mitigation measures.

Cyber-Informed Engineering (CIE)

An initiative to integrate cybersecurity into the design cycle of engineering projects.

- **Keypoints**
  - Cyber-Informed Engineering implementation plan.
  - Systems engineering approach to build in cybersecurity.
  - Consequence-driven approach to prioritize and mitigate cyber risk.

Visibility in OT systems

Increasing visibility into operational technology

(OT) systems to detect vulnerabilities and anomalous activities. • **Keypoints** ○ Integration of cybersecurity tools and technologies. ○ Behavioral activity monitoring in OT systems. **Secure by Design** A concept to ensure that systems are designed with cybersecurity as a fundamental component. • Keypoints ○ Driving a culture of designing equipment with cybersecurity in mind. ○ Linking cybersecurity to reliability and safety. **Assignments & Suggestions**	

2.4 D2-P3 Panel: International Critical Infrastructure

Moderator: Greg Rattray Panelists: - Jun Murai - Chikara Nakama (Splunk Japan) - Chris Grady - Alexander Patton (Amentum Japan)	モデレーター：グレッグ・ラットライ パネリスト： - 村井 純 - 仲間 力 (Splunk Japan) - クリス・グラディ - アレキサンダー・パットン（アメンタムジャパン）
Overview This speech summarizes the key points from a panel session on internationally important infrastructure and economic security. It includes discussions on infrastructure security, Splunk's role, and security and confidential information. Action items are listed at the end. **Panel Session on Internationally Important Infrastructure** **Moderator Introduction** • **Moderator**: Greg Rattray • **Introduction**: Greg Rattray introduced himself and mentioned the importance of the panel session on internationally important infrastructure and economic security. **Infrastructure and Economic Security** • **Slides Presentation**:	**講演メモ** **国際的に重要なインフラ** • **モデレーター**: グレッグ・ラトレイ • **テーマ**: 経済的な安全保障とクリティカルなインフラ **インフラの重要性** • **経済的安全保障**: インフラは国家の安全保障において非常に重要な関心事項。 ○ きれいな水や電力の供給 ○ 通信インフラ（インターネット、音声通信） **リスクとレジリアンス** • **リスク**: グローバルなプラットフォームの脆弱性 ○ ローカルクラウドよりも深刻度が高い ○ 特にテレコムネットワークでの影響が大きい • **レジリアンス**: インフラの維持と防御 ○ 金融サービスとグローバルマーケットの安定性 ○ 2016 年の金融安定性のためのサイバーセキュリティ取り組み **国際的な協力**

- **Slide 1**: Greg shared a personal slide showing Mt. Fuji from his balcony, dated October 10, 2024, emphasizing the significance of the day.
- **Slide 2**: Highlighted the availability of 300 Mbps internet on Japan Airlines, illustrating advancements in infrastructure.
- **Slide 3**: Discussed the importance of recognizing weaknesses in infrastructure, such as height recognition.
- **Slide 4**: Introduced 3D mapping and mentioned JNSS as the only entity working on it.
- **Slide 5**: Addressed concerns about the electricity grid and ongoing discussions with the electricity company.

Splunk's Role in Infrastructure Security

- **Speaker**: Business Development Executive from Splunk
- **Company Overview**: Splunk is a data provider focused on monitoring security and system operations to maintain system resilience.
- **Implementation**: Splunk implements systems to monitor and maintain infrastructure security, applying new blocks and collaborating on data.
- **Experience**: The speaker has 20 years of experience in medical infrastructure and security, highlighting the interdependence of these sectors.

Security and Confidential Information

- **Speaker**: Murai
- **Questions Raised**:
- Definition and criteria for security or confidential information in critical infrastructure (e.g., nuclear plants, transportation, mapping).
- Handling updates and screening processes for security clearance.
- Impact on employees, including temp

- **必要性**: 国際的なクリティカルインフラを守るための協力
- **具体例**: グローバルな決済システムの安定性

村井先生のプレゼンテーション

デジタルインフラの概要

- **基本要素**:
- デジタルデータ
- インターネット
- コンピューター
- **相互運用性**: 国際的な交渉が必要

インターネットと IoT

- **インターネット**: グローバルな標準
- **IoT**: ドローンやロボットも含む

PNT（ポジショニング・ナビゲーション・タイミング）

- **課題**:
- ウクライナへの進行などの影響
- GNSS のポジショニングとジャミング
- **影響**: 自動運転車やドローンのロケーションシステム

電力インフラ

- **グリッドの最適化**:
- コアグリッドとマイクログリッド
- サイバー攻撃のリスク
- **新技術**:
- 電気自動車（B2H テクノロジー）
- UPS のような分散型テクノロジー

AI とデータ共有

- **データの種類**:
- パブリックデータ（政府管理）
- プライベートデータ（企業管理）
- オープンデータ（グローバルに利用可能）
- **安全な共有**: AI 規制における重要性

仲間さんのプレゼンテーション

- **Splunk のデータ分析方法**

経済への貢献

自己認識と責任

- 「そうご自分を知っているから、それぞれ私たちは責任がある、自分たちのことを知っていますということによって、経済に貢献できるのかなと思っています。」
- 自己認識が経済貢献に繋がるという意見。

エネルギーと半導体

- 「経済に関すると、このようなことで言っていただいてい

workers, if they refuse screening. ○ Management of private information and security clearance mechanisms from the United States. **Action Items** [ ] Discuss and address concerns with the electricity company regarding the optimal grid. [ ] Explore collaboration opportunities on data with Splunk. [ ] Define and clarify criteria for security and confidential information in critical infrastructure. [ ] Review and potentially revise screening processes for security clearance, including the impact on temp workers.	るのが、エネルギーとか、半導体とか、その辺、重要に言うと、電気水道を出すというのがメインだと思うんですけど、」 ○ エネルギーと半導体が経済において重要な要素である。 ○ 特に電気や水道の供給がメインの役割。 **国際連携** **営利企業の社会貢献** ○ 国際連携の重要性が強調されている。 **社会貢献と企業利益** • 「営利企業である場合は、利益と社会貢献と、全体利益を持っていることが難しいことだなと思います。それができていないといけないといけない。」 ○ 営利企業が社会貢献と企業利益のバランスを取ることの難しさ。 ○ それでも、これを達成する必要があるという意見。 **アメリカのコンティニュアス・タイヤジョンティーニューズ** • 「そして、このスライドは、私のアイデアについて、アメリカのコンティニュアス・タイヤジョンティーニューズについて、私のアイデアについて、アメリカのコンティニュアス・タイヤジョンティーニューズについての話です。」 ○ アメリカの継続的なタイヤジョンティーニューズに関するアイデアの紹介。 **政府の計画とイニシアチブ** **目標の監視** • 目標を 24 時間 365 日監視するための取り組み。 • データが目標に到達する際の監視方法について議論。 **データの取り扱い** • データの沈降についての問題提起。 • データが目標に到達するプロセスの説明。 **市場の安全確保** • 2020 年以降のデータ収集の継続。 • 市場の安全を確保するためのデータ利用。 **生活環境の改善** • 土地での生活に関する取り組み。 • この計画が生活環境の改善を目指していることの説明。 **インフラのセキュリティと FedRAMP 認証** **インフラのセキュリティ** • **対象分野**: 電力、グリッド、財務、金融 • **活動地域**: 日本、アメリカ

	• **経験**: テクノロジー業界で 28 年間の経験 • **セキュアクラウドの研究**: インプリに関する深い研究 **FedRAMP 認証** • **FedRAMPとは**: アメリカの認証プロセスで、商用クラウドに関する連邦政府の認証 • **評価プロセス**: デザイン、ドキュメンテーション、実装、第三者評価機関による評価 • **最新情報**: 来週承認予定 • **CEO の活動**: ワシントン DC でのシンポジウムで情報提供 **重要インフラの防御とクラウドの役割** **重要インフラの現状** • **生活の範囲**: 近代の文化を支える重要な要素 • **ブレア提督や電子通信のコメント**: 重要インフラのセキュリティに関する発表 **日本のデジタルデジレンシーと FedRAMP** • **類似性**: 日本のデジタルデジレンシーと FedRAMP のアプローチの類似 • **グローバル標準**: FedRAMP はセキュリティ評価のグローバル標準 **クラウドの役割** • **主要なクラウドプロバイダー**: Google、Microsoft • **サービスモデル**: インフラのインパクトレベルハイ • **セキュリティ対策**: クローズドシステム、ゼロトラストのクローキング、地理的分散 **分散型クラウドモデルとソブリンクラウド** **分散型クラウドモデル** • **従来型のモデル**: 一元化されたハイパースケーラーのクラウド • **分散型のモデル**: 高度に分散され、相互接続があり、リジョンごとに処理 **ソブリンクラウドの定義** • **VMware バリデイテッドソリューション**: セキュアで安全なインフラを提供 • **VMware クラウド**: 設計と検証済みのセキュアソブリンクラウド • **セキュリティバースト**: 第三者が検証したソブリンクラウドを使用 **サイバープラットフォームとセキュリティ** **サイバープラットフォーム**

	• **サービスのパッケージ**：金融サービス、継続的なモニタリング • **ゼロトラストネットワーク**：クロックドゲートウェイを使用 **需要インフラのセキュリティ** • **電力グリッド**：セキュリティは後付け • **クロックドゲートウェイ**：システムアクセスの強制制御、マイクロファイアウォール機能 • **継続的なモニタリング**：脆弱性の検出と報告 **自己紹介と会社紹介** **アレクサンダー・パットンの自己紹介** • 英国出身で現在日本でサイバーセキュリティのリードとして活動。 • アメンタムという会社に所属し、原子力発電所や国防関係のエンジニアリングサービスを提供。 **アメンタムの紹介** • 日本では福島第一原発や国防関係の業界にサービスを提供。 • クリティカルなインフラ、国家の安全保障、防衛などをカバー。 **サイバーセキュリティの重要性と経験** **経歴と経験** • 機械、電気のエンジニアリングを学び、2017 年からサイバーセキュリティを担当。 • 英国やオーストラリアでクリティカルなインフラのプログラムを管理。 • 今年から日本で活動し、海外の経験を活かしてサポートを提供。 **日本の国家安全保障戦略** • 日本は新たな国家の安全保障戦略を打ち立てようとしている。 • 政府の役割を進化させ、新たな規制でサイバーセキュリティを提供。 **ケーススタディと教訓** **英国の鉄道会社の事例** • 2017 年から 5 年後、英国の鉄道会社がサイバーセキュリティの依頼。 • コンディションモニタリングのインターフェースで脆弱性を発見。 • セキュリティコントロールをバイパスし、物理システムが操作可能に。 **教訓と反省**

	• 重要な脆弱性が 5 年間見過ごされていた。 • リソースや経験が限られていたため、セキュリティが不十分だった。 • シンプルなアクションで防御できた可能性があったが、ギャップが存在。 **英国の取り組みとパートナーシップ** **英国の規制とコラボレーション** • 英国は課題を認識し、規制を適用。 • 官民学でのパートナーシップが重要と考え、ナショナルサイバーセキュリティセンターが設立。 **インダストリー100 とエクスパートグループ** • インダストリー100 のイニシアティブが立ち上がり、ステークホルダーが特定の課題に取り組む。 • 鉄道運行会社、OT のサイバーセキュリティスペシャリスト、公共部門の専門家が協力。 **成果とメリット** • 共通の参照アーキテクチャを構築し、評価を実施。 • 官民のパートナーシップにより、スキルや経験、人とのネットワーキングが強化。 **質疑応答とまとめ** **質疑応答** • クリティカルなインフラストラクチャーに関する質問。 • セキュリティクリアランスの基準と審査についての議論。 **まとめ** • セルフナレッジとモニタリングの重要性。 • コミュニケーションとコネクションの増加。 • AI の役割とデータの重要性。 • クラウドとデータ管理の考慮。 **アクションアイテム** [ ] マイクを使用して通訳ができるようにする [ ] 国際連携の具体的なステップを策定する [ ] エネルギーと半導体分野での貢献策を検討する [ ] 英意企業の社会貢献と企業利益のバランスを取るための戦略を立案する [ ] 目標監視のための具体的な手法の確立 [ ] データ沈降の問題解決策の検討 [ ] 市場安全確保のためのデータ分析の強化 [ ] FedRAMP の最新情報を来週確認 [ ] ワシントン DC でのシンポジウム情報を提供 [ ] 分散型クラウドモデルの詳細な比較を実施 [ ] ソブリンクラウドの導入検討

	[ ] クロックドゲートウェイの導入とモニタリング体制の強化 [ ] クリティカルなインフラストラクチャーのセキュリティクリアランス基準の見直し [ ] 官民学パートナーシップの強化と教育・トレーニングの推進

2.5 D2-P4 Panel: Japanese Critical Infrastructure

Moderator: Chikara Nakama Panelists: - Takashi Ebihara (Chief Technology Officer, Chief Information Officer, Executive Vice President, Head of Digital Transformation Headquarters and Innovation and Technology Department, Nippon Telegraph and Telephone East Corporation) - Tadashi Uchida (Executive Officer, General Manager of Digital Transformation Promotion Office, Chief Information Security Officer, Chubu Electric Power Co., Inc.,) - Noboru Nakatani (Corporate EVP Chief Security Officer, NEC Corporation) - Tadashi Kaji (Distiguished Researcher, Hitachi, Ltd. Research & Development Group)	モデレーター：仲間 力 パネリスト： - 海老原 孝（東日本電信電話株式会社 常務執行役員 デジタル革新本部長 先端テクノロジー部長兼務 CTO CIO） - 内田 忠（中部電力株式会社 執行役員 DX 推進室長 CISO） - 中谷 昇（日本電気株式会社 執行役 Corporate EVP 兼 Chief Security Officer） - 鍛 忠司（株式会社日立製作所 研究開発グループ 主管研究長）
Overview This speech provides a comprehensive summary of the meeting held on 2024-10-31, focusing on critical infrastructure, cybersecurity, and public-private partnerships. The discussions covered various aspects of infrastructure resilience, cybersecurity measures, and the importance of collaboration between different sectors. Key action items were identified to enhance communication, training, and information-sharing mechanisms. **Introduction of Panelists** **Moderator** • **Nakama** ○ **Role**: Business Development and Critical Infrastructure at Plaud ○ **Company**: Splunk ○ **Focus**: Business development and critical infrastructure ○ **Services**: Security and system operation	**イントロダクション** • **仲間氏の紹介** ○ Splunk のビジネスディベロップメントでクリティカルインフラストラクチャーを担当。 ○ 自己紹介と Splunk の概要説明。 ○ Splunk はセキュリティとシステムオペレーションをメインにデータ分析プラットフォームを提供。 ○ 自衛隊で約 20 年サイバーセキュリティに従事、その後内閣官房やシスコでの経験。 • **参加者の紹介** ○ 海老原氏：NTT 東の CTO、CIO、エグゼクティブバイスプレジデント。 ○ 鍛氏：日立のディスティンクションディサーチャー。 ○ 内田氏：中部電力のエグゼクティブオフィサー兼 CISO。 ○ 中谷氏：NEC のコーポレートエグゼクティブバイスプレジデント兼チーフセキュリティオフィサー。 **中部電力の取り組み** • **内田氏のプレゼンテーション** • **自己紹介と会社概要**

company providing a data analysis platform
  - **Cybersecurity Applications**: Offers various software and services to connect, visualize, and analyze data

Panelists

- **Mr. Ebihara**
  - **Role**: CTO, CIO, and Executive Vice President
  - **Company**: NTT East
- **Mr. Tadashi Kaji**
  - **Role**: Distinguished Researcher
  - **Company**: Hitachi Limited
- **Mr. Tadashi Uchida**
  - **Role**: Executive Officer and CISO
  - **Company**: Tube Electric Power Company
- **Mr. Noboru Nakatani**
  - **Role**: Corporate Executive Vice President and Chief Security Officer
  - **Company**: NEC Corporation

Discussion on Japanese Critical Infrastructure

- **Panelists**: Four outstanding speakers will discuss various aspects of Japanese critical infrastructure.
- **Moderator**: Nakama will act as the moderator for the session.

Introduction and Speaker Backgrounds

Mr. Uchida (Chubu Electric Company)

- **Background**:
  - 20 years in cybersecurity with Japan Self Defense Forces.
  - Experience at the cabinet secretariat and Cisco.
  - Involved in critical infrastructure for many years.
- **Role**:
  - In charge of IT and digital transformation at Chubu Electric Company.
  - Chief Information Security Officer (CISO).
  - Representative director of the ISAC for the electric power industry.
  - 内田氏：デジタルトランスフォーメーションの統括とCISO を担当。
  - 電力業界の ISAC の代表理事も務める。
  - 中部電力は大阪と東京の間に位置し、約 1000 万世帯に電力を供給。
  - ガス、海外事業、コミュニティサービスなど新規事業も展開。
- **電力業界の現状と課題**
  - AI のデータセンターや半導体工場の需要増加に伴い、クリーンエネルギーと電力設備の提供が重要。
  - 電力ネットワークの変遷：集中から分散へ。
  - 分散エネルギーの活用による CO2 削減とエネルギーリスクの低減。
- **サイバーセキュリティの課題**
  - 分散エネルギーにおける多様なデバイスの接続がサイバーセキュリティの課題。
  - ゼロトラストの考え方を採用し、各プレイヤーがデバイスを管理。
  - 国と連携しながらセキュリティ枠組みを進める。
- **サイバーとフィジカルの両輪での防御**
  - サイバーインシデントと自然災害の両方に対応。
  - プライベート SOC と制御システムの連携。
- **中部サイバーセキュリティコミュニティの活動**
  - 中部地区のインフラ企業が集まり、情報共有と信頼関係の構築。

中部地区企業の合同訓練とセキュリティ情報共有

- **合同訓練**
  - 中部地区の企業が年 1 回集まって合同訓練を実施。
  - セキュリティに関する情報共有の仕組みを構築。

日立製作所の重要インフラ防護関連の活動

- **鍛氏の紹介**
- **経歴**
  - 1996 年に日立製作所に入社。
  - 一貫してサイバーセキュリティ、セキュリティ系の研究開発に従事。
  - 2010 年、2014 年に 1 年間だけセキュリティから離れるが、鉄道や電力システムの研究開発マネージャーを担当。
- **日立製作所の事業柱**
- **コネクティブインダストリーズ**
  - 産業用システム、製品を提供する部門。

Mr. Kaji (Hitachi)

- **Background**:
  - Joined Hitachi in 1996.
  - Involved in R&D of security, focusing on enterprise information systems, network securities, and critical infrastructure security.
  - Briefly managed control systems and security in 2014.
- **Role**:
  - Professor at Hitachi.
  - Focus on defending critical infrastructure.

Critical Infrastructure Issues and Company Initiatives

Chubu Electric Company

- **Company Overview**:
  - Operates in the Chubu area (between Tokyo and Osaka), covering about 10 million households.
  - Engages in electrical power, overseas business, nuclear power, and community support infrastructure.
- **Technological Focus**:
  - Utilizes AI in the electrical industry.
  - Emphasizes the need for semiconductors and clean energy.
- **Energy System Transition**:
  - Shift from centralized to distributed energy systems.
  - Focus on local energy generation to reduce risks.
- **Cybersecurity Approach**:
  - Centralized protection for distributed energy systems.
  - Adoption of the zero-trust concept, where each player is responsible for their devices.
  - Framework for collaboration based on zero-trust.
- **Cyber and Physical Security**:
  - Security Operations Center for monitoring cyber incidents and natural disasters.

- **グリーンエナジーモビリティ**
  - 電力や鉄道関連の製品を提供する部署。
- **デジタル**
  - コネクティブインダストリーズやグリーンエナジーモビリティを支えるデジタル製品を作成。
  - デジタルサービスや製品を提供。
- **サイバーセキュリティの位置づけ**
- **デジタル部門**
  - セキュリティサービスを直接提供。
- **ビジネスのレジリエンス**
  - セキュリティはビジネスのレジリエンスを支える基礎。
  - デジタル、グリーン、コネクティブに対してセキュリティ機能を提供。
- **セキュリティ技術とサービス**
- **セキュリティバイデザイン**
  - セキュリティバイデフォルト、脆弱性管理、インシデントレスポンスの提供。
- **脆弱性管理**
  - セキュリティデジタルツインのコンセプトで研究開発。
  - 電力や鉄道システムをサイバー空間上に再現し、攻撃や対策のサイドエフェクトを分析。
- **セキュリティトレーニングアリーナ**
  - 電力や鉄道の制御システムの模擬システムを使用。
  - インシデント発生時の対処能力向上サービスを提供。
  - 重要インフラ事業者向けの訓練サービス。

NTT 東日本の取り組み

- **海老原氏の紹介**
- **役職と経歴**
  - NTT 東日本の CIO と CTO を務める。
  - ワシントン DC の戦略国際問題研究所でテクノロジーポリシー関係の研究調査を行った経験。
- **NTT 東日本の現状と投資**
- **会社の構成**
  - 1999 年の再編成で、東西のワイヤーラインカンパニーとドコモに分かれる。
  - 東日本地域のワイヤーライン会社として約 1300 万のサブスクライバーを持つ。
  - FTTH の設備ベースでほぼカバー率を達成。
- **年間投資**
  - 東日本と西日本でそれぞれ約 2500 億円、ドコモで

- Interdependencies with other infrastructure companies in the Chubu area.
- Annual joint exercises and information sharing within the Chubu cybersecurity community.

Hitachi

- **Company Overview**:
  - Founded in 1910, initially a machine repair shop at a mining company.
  - Mission: Contribute to society through superior original technology and products.
  - Three main sectors: Connective Industries, Green Energy and Mobility, Digital Systems and Services.
- **Security Services**:
  - Provides security functionality across all sectors.
  - Emphasizes security by design, security by default, vulnerability management, and incident readiness and response.
- **Current Focus**:
  - Vulnerability management through security digital twin.
  - Incident readiness and response training services.

NTT East Overview and Initiatives

Company Background

- **Speaker**: Ebihara-san, CIO and CTO of Washington, D.C.'s CSIS, NTT East
- **Company Overview**:
  - NTT East covers the eastern area of Japan with 13 million subscribers.
  - Provides about 250 billion yen annually, similar to NTT West, totaling around 1.2 trillion yen (8 billion USD).

Digitalization and Infrastructure

- **Digitalization**:
  - Japan's digitalization was slow but accelerated post-COVID-19.
  - Increased remote work led to new

約 7000 億円、グループ全体で年間約 1.2 兆円（約 8 ビリオン US ドル）の投資。

- **COVID-19 以降の新たなチャレンジ**
- **リモートワークのニーズ**
  - COVID-19 以降、リモートでの業務が増加し、新たなチャレンジが発生。
- **クラウドリフトとロボットの利用**
  - 通信事業者に対するインフラ依存度が高まり、レジリエンスの向上が求められる。
- **災害対策とインフラ強化**
- **物理インフラのロバスト化**
  - 自然災害に対する物理インフラの強化とリカバリープランの策定。
- **サイバーセキュリティ**
  - サイバー攻撃へのプロアクティブな対応と重要認識の共有。
- **電力会社との連携**
  - 東京ガスや東京電力との連携協定を結び、災害時やその他の局面での協力体制を構築。
- **自衛隊との連携**
- **ロジスティックスのサポート**
  - 自衛隊との連携により、道路寸断時のサポートやネットワーク普及の支援。
- **サイバーセキュリティの取り組み**
- **レイヤーアプローチ**
  - デザイン系、ペンテスト、ワフなどの多層的なアプローチ。
  - 各社のサートとグループ全体のサートによるトレーニング。
- **グローバルなナレッジ教育**
  - 各社の CSIRT でのナレッジ教育やアトレットチームの用意。
  - ISAC やアメリカの JCDC への参加。

NEC の取り組み

- **中谷氏の紹介**
- **NEC の現状**
  - 50 カ国以上に 254 のグループ企業を持ち、日々サイバー攻撃に遭遇。
- **海底ケーブルの重要性**
- **デジタル社会の基盤**
  - 95 年にはサテライトと 50-50 だったが、現在は 99%が海底ケーブルを通る。

challenges and a shift to cloud services and robotics.

- **Infrastructure Resilience**:
  - Emphasis on enhancing resilience due to dependency on infrastructure.
  - Preparation for natural disasters and cybersecurity is crucial.
  - Lessons from the 2011 earthquake: Tsunami and prolonged power outages had significant impacts.
  - Enhanced power resilience and relocation of structures in tsunami-prone areas.
  - Partnerships with power companies like Tokyo Gas and Tokyo Electric Power for various initiatives.

Cybersecurity

- **Cybersecurity Measures**:
  - Partnership with JFD for reaching isolated regions during disasters.
  - Use of layered security approaches, policies, and training.
  - Each company and the group have CERT (Computer Emergency Response Team) for extensive training.

NEC Cybersecurity Approach

Speaker Background

- **Speaker**: Mr. Nakatani, Chief Security Officer at NEC
- **Experience**:
  - Former National Police Agency officer with 26 years of service, including 11 years at Interpol.
  - Experience in counterintelligence and cybercrime countermeasures.

NEC's Cybersecurity Efforts

- **Company Overview**:
  - NEC has 254 group companies involved in various digital infrastructure activities, including satellites and submarine cables.
  - Major supplier of submarine cable systems, carrying over 99% of intercontinental communication.
  - 海底ケーブルの製造過程でのセキュリティ対策。
- **サイバーセキュリティの取り組み**
- **AI の活用**
  - 犯罪者も AI を使用しているため、防御側も AI を活用。
- **データの CIA**
  - コンフィデンシャリティ、インテグリティ、アベラビリティの保護。
- **NEC セキュリティ**
  - ネットワークセキュリティ、エンドポイントセキュリティ、クラウドセキュリティのバランス。
- **人間の脆弱性**
- **攻撃の実例**
  - ある日のスクリーンショットで、7666 のマルウェアが検知された例。
  - リアルタイムで 24 時間ベースの監視。

AI の活用とサイバーセキュリティ

- **AI の活用事例**
- **生成 AI の利用**
  - 日立のデジタルツインの話題に関連。
  - OT 系、ファクトリー系のシステムは停止できないが、サイバーセキュリティ上の脆弱性をチェックする必要がある。
  - サイバーアタックルートを用いて脆弱性を確認。

国内の重要インフラ防護

- **官民連携の現状と課題**
- **官民連携の重要性**
  - 重要インフラの事業者に対するインシデント報告の義務化が進行中。
  - 官と民の権限の受け止め方と、営利企業としての社会インフラの責任について議論。
  - インシデント報告の報告系統の変化についても検討。
- **現状の捉え方と課題**
  - 各参加者の意見を順番に聴取（内田さん、鍛さん、海老原さん、中谷さん）。
- **電力の BCP とサイバーインシデント対応**
- **BCP の考え方**
  - サイバーインシデントが発生した場合、人間系に切り替えて復旧を行う。
  - 自然災害やシステム障害にも対応するため、サイバーとフィジカルの両方で対応。

Cybersecurity Strategies

- **Protection Measures**:
  - Efforts to prevent eavesdropping on submarine cables.
  - Use of AI for cybersecurity, acknowledging that criminals also use AI.
  - Importance of data confidentiality and integrity.
- **NEC's Focus Areas**:
  - Network security, endpoint security, and cloud security.
  - Emphasis on the human element in cybersecurity.
- **AI and Cybersecurity**:
  - Real-time malware detection and monitoring.
  - Cyber attack root diagnosis service for factory OT systems.
  - Use of AI to identify vulnerabilities and monitor irregular spikes in packets.

Unique Cyber Intelligence Infrastructure

- **KOTOMI**:
  - A unique cyber intelligence infrastructure used for security purposes.
  - Aims to protect LLNs (Low Latency Networks) using AI.

Protection of Domestic Critical Infrastructure

Public-Private Partnerships

- **Incident Reporting**
  - Incident reports must be made by critical infrastructure providers.
  - Current status and challenges of public-private partnerships need to be examined.
  - Incident reports are already being made, indicating ongoing changes.
- **Business Continuity Planning (BCP)**
  - Necessary to consider BCP aspects in public-private partnerships.
  - In case of an incident, recovery can involve switching to human intervention

- **報告のルール**
  - 安定供給に支障があった場合、監督省庁に報告。
  - サイバーインシデントの報告窓口の一本化が必要。
  - 報告は双方向で行うべき。
  - 活動する顔と支援する顔を分けるべき。
- **官民連携の具体的な提案**
- **窓口の一本化**
  - 各省庁または NISC での一本化が望ましい。
- **双方向の情報共有**
  - 官からの情報提供も含めた双方向の報告体制が必要。
- **役割の分離**
  - 活動する役割と支援する役割を分けることで、報告情報の経由がしやすくなる。

ディスカッション

- **官民連携の具体例**
- **有事と平時の違い**
  - 有事かそうでないかで話が大きく変わる。

有事における情報共有の重要性

- **必要な情報の迅速な入手**
- **課題**
  - 必要な情報を迅速に必要な組織や人に届けることが重要。
- **現状**
  - 複数の組織が情報を必要としているが、迅速に届ける方法が課題。
- **自律分散とキーワード**
- **制約**
  - 各発言者に 2 分の制約がある中での議論。

災害対策と通信の維持

- **災害対策基本法と指定公共機関**
- **背景**
  - 災害対策基本法に基づき、指定公共機関として通信を止めないことが会社の DNA として徹底されている。
- **対応**
  - 事故が起きた際には所管官庁に報告し、指導を受ける。
- **サイバーセキュリティの連携**
- **協議会**
  - サイバーセキュリティの連携協議会が設立され、NISC や JPCERT の指導のもと、脅威情報を共

for fiber areas.

- Both cyber and physical responses are required for stable supply.

Cyber and Physical Response

- **Incident Management**
  - Relevant agencies and ministries are informed in case of an incident.
  - Cyber reasons for incidents are analyzed and reported.
- **Centralized Contact Point**
  - A centralized contact point for cyber incidents is needed.
  - This could be a ministry, agency, or NISC (National Information Security Center).
- **Bidirectional Information Exchange**
  - Reporting should involve a pilot or bidirectional exchange of information.
  - Governance and monitoring functions should support these bodies.

Public-Private Partnerships in Emergencies

Information Delivery and Control Systems

- **Mr. Kaji's Perspective:**
  - In emergencies, critical information must be delivered to the necessary organizations and people.
  - Hitachi produces a control system with distributed calculation nodes connected to a sharing field.
  - Sensitive information should be used based on this concept, especially in emergencies.
  - Recently, the concept of a secure data space has emerged, allowing authorized persons or organizations to access data.

Disaster Management and Cybersecurity

- **Mr. Ebihara's Perspective:**
  - Basic disaster management law specifies telecommunication as special infrastructure, which cannot stop functioning.
  - In case of accidents, reports must be made to the authority, and instructions

有。

- **重要性**
  - 連携して対応することが多く、非常に助かっている。
- **経済安保法制の強化**
- **設備の構築と維持管理**
  - 需要インフラとして使用する設備の構築や維持管理について、詳細な情報提供が求められている。
- **報告義務**
  - サイバー攻撃や個人情報保護法に基づく報告を所管官庁や個人情報保護委員会に行っている。
- **業界横断的なコラボレーション**
- **重要性**
  - 業界一致団結してコラボレーションする仕組みがますます重要になっている。

平時における連携の重要性

- **3 つのレイヤー**
- **KYC**
  - ノーイワーカウンターパート（KYC）が連携時に重要。
- **レイヤーの違い**
  - 戦略レイヤー、経営者レイヤー、技術レイヤー、ビジネスレイヤーの違いが連携に影響。
- **経営者層の理解**
- **サイバーセキュリティの認識**
  - 経営者層もサイバーセキュリティはコストではなく投資であると認識。
- **ミドルのビジネスレイヤー**
- **課題**
  - 普段の連携ができていないため、これをどう改善するかがチャレンジ。

自社状況の把握と連携

- **日立製作所の事例**
- **WannaCry ウイルス**
  - WannaCry ウイルス感染時にセキュリティ体制を見直し、CISO を設置。
- **取り組み**
  - 提供する製品のセキュリティをどうするか、標準化と成熟度の向上が課題。
- **通信ノードの管理**
- **課題**
  - 数万の通信ノードや多様な OS バージョンの管理が難しい。

are received from them. ○ The Cyber Security Council, involving NISC and JPCERT, provides threat information. ○ The economic security law requires reporting on operations and cyber threats to the authority and privacy law committee. ○ Emphasizes the need for bi-directional communication and centralized information-sharing organizations. **Strategic, Technological, and Business Layers** • **Mr. Nakatani's Perspective:** ○ Public-private partnerships are crucial, especially in emergencies. ○ Emphasizes the importance of reporting to a single organization rather than multiple ones. ○ Introduces the concept of "Know Your Counterpart" (KYC) across three layers: ○ **Strategic Layer:**Managed by METI, Keidanren, and management teams. ○ **Technological Layer:**Focused on detailed technical work. ○ **Business Layer:**Lacks partnerships during peaceful times, posing a challenge. **Understanding and Managing Organizations** **Incident Response and Organizational Review** • **Mr. Kaji's Perspective:** ○ Hitachi created an organization to review systems after a WannaCry incident, establishing roles like CISO. ○ Emphasizes product security and standardization to increase maturity levels. ○ Collaboration between product development and incident control teams is crucial. **Governance and Inventory Control**	• **基本動作** ○ インベントリ管理を徹底し、購入元の調査も行う。 • **可視化の重要性** • **ビジュアライゼーション** ○ 自社の状況を可視化し、データに基づいて情報を共有。 • **シングルポイント** ○ 情報共有の際にはシングルポイントで話をすることが重要。 • **グループ会社とサプライチェーン** • **セキュリティ対策** ○ グループ会社やサプライチェーンのセキュリティ対策の把握が重要。 • **信頼関係** ○ フェイスとフェイスの信頼関係が必要。 **訓練とプロセスの実行** • **訓練の重要性** • **対処プロセス** ○ エスカレーションプロセスや PDCA サイクルを重視。 • **官民連携** ○ 官民連携の訓練も重要。 • **メディア対応と情報共有** • **対応** ○ インシデント対応やメディア対応、情報共有の訓練が必要。 • **物理インフラのトレーニング** • **連携** ○ 自治体や自衛隊との連携訓練を実施。 **サイバーセキュリティ体制と訓練** • **情報漏洩インシデント対応** • **体制の確立** ○ 情報漏洩系のインシデントが発生した場合、顧客対応、メディア対応、官庁対応など幅広い

- **Mr. Ebihara's** Perspective**:**
  - As a CIO, managing tens of thousands of nodes and various OS versions is challenging.
  - Emphasizes the importance of controlling inventory and procurement to avoid threats.
  - Highlights the difficulty in tracing back components but stresses the need to assess risks.

Visualization and Command Control

- **Mr. Nakatani's Perspective:**
  - Visualization of the company's situation is essential.
  - Uses dashboards to show various patterns for each business unit.
  - Emphasizes the importance of conveying information using data and having a command control structure.

Supply Chain and Security Steps

- **Mr. Uchida's Perspective:**
  - Recent incidents show the impact of supply chain issues on the main company.
  - Governance and face-to-face contacts are necessary to build trust.
  - Certification systems are employed to ensure cybersecurity.

Training and Resource Management

Training Objectives and Methods

- **Mr. Ebihara's Perspective:**
  - Training is carried out with local governments and self-defense forces using scenarios.
  - Cyber training includes dealing with information leakage incidents and ransomware.
  - Internal activities like capture the flag competitions and certification systems motivate technical engineers.

Capacity Building and Business Continuity

- **Mr. Nakatani's Perspective:**
  - Training objectives include raising skills,

capacity building, and business continuity. ○ Security awareness training includes phishing mail simulations. ○ Emphasizes the need for cyber BCP activities, including backup and recovery training. **Collaborative Exercises and Geopolitical Risks** • **Mr. Ebihara's Perspective:** ○ Collaborative exercises among different infrastructures are necessary. ○ Exercises should combine cyber and physical space threats. ○ Geopolitical risks require more comprehensive exercises beyond phishing and ransomware. **Hitachi's Security Training Arena** • **Mr. Kaji's Perspective:** ○ Hitachi provides security training for all employees, departments with incidents, and clients. ○ The training arena includes red team and blue team exercises monitored by a white team. ○ Emphasizes the importance of communication among stakeholders during incidents. **Understanding and Managing Organizations** **Incident Response and Organizational Review** • **Mr. Kaji's Perspective:** ○ Hitachi created an organization to review systems after a WannaCry incident, establishing roles like CISO. ○ Emphasizes product security and standardization to increase maturity levels. ○ Collaboration between product development and incident control teams is crucial. **Governance and Inventory Control**	

- **Mr. Ebihara's Perspective:**
  - As a CIO, managing tens of thousands of nodes and various OS versions is challenging.
  - Emphasizes the importance of controlling inventory and procurement to avoid threats.
  - Highlights the difficulty in tracing back components but stresses the need to assess risks.

Visualization and Command Control

- **Mr. Nakatani's Perspective:**
  - Visualization of the company's situation is essential.
  - Uses dashboards to show various patterns for each business unit.
  - Emphasizes the importance of conveying information using data and having a command control structure.

Supply Chain and Security Steps

- **Mr. Uchida's Perspective:**
  - Recent incidents show the impact of supply chain issues on the main company.
  - Governance and face-to-face contacts are necessary to build trust.
  - Certification systems are employed to ensure cybersecurity.

Training and Resource Management

Training Objectives and Methods

- **Mr. Ebihara's Perspective:**
  - Training is carried out with local governments and self-defense forces using scenarios.
  - Cyber training includes dealing with information leakage incidents and ransomware.
  - Internal activities like capture the flag competitions and certification systems motivate technical engineers.

Capacity Building and Business Continuity

- **Mr. Nakatani's Perspective:**
  - Training objectives include raising skills,

capacity building, and business continuity. ○ Security awareness training includes phishing mail simulations. ○ Emphasizes the need for cyber BCP activities, including backup and recovery training. **Collaborative Exercises and Geopolitical Risks** • **Mr. Ebihara's Perspective:** ○ Collaborative exercises among different infrastructures are necessary. ○ Exercises should combine cyber and physical space threats. ○ Geopolitical risks require more comprehensive exercises beyond phishing and ransomware. **Hitachi's Security Training Arena** • **Mr. Kaji's Perspective:** ○ Hitachi provides security training for all employees, departments with incidents, and clients. ○ The training arena includes red team and blue team exercises monitored by a white team. ○ Emphasizes the importance of communication among stakeholders during incidents. **Action Items** [ ] Show the slides as requested by Nakama. [ ] Proceed to the next slide as indicated. [ ] Limit presentation times to five minutes per speaker. [ ] Enhance infrastructure resilience for natural disasters. [ ] Conduct cybersecurity training and policy implementation. [ ] Monitor and improve AI-based cybersecurity measures. [ ] Collaborate with power companies for infrastructure initiatives. [ ] Examine the current status and challenges	

of public-private partnerships in critical infrastructure protection. [ ] Establish a centralized contact point for cyber incident reporting. [ ] Implement a bidirectional exchange of information for incident reporting. [ ] Enhance communication and information-sharing mechanisms among stakeholders. [ ] Conduct collaborative exercises combining cyber and physical space threats. [ ] Improve visibility and standardization of operations and products. [ ] Establish a security clearance mechanism for better information control. [ ] Implement comprehensive training programs, including cyber BCP activities.	

2.6 D2-P5 Panel: Trusted Entity Designations for Critical Supply Chains

Moderator: Jun Osawa Panelists: - Mayu Arimoto (Partner, Alesia International Law Office) - Chris van't Hof (Managing Director, DIVD) - Jon Chung - Shinya Kabashima (METI) - Robert Martin (MITRE)	モデレーター：大澤 淳（笹川平和財団 特別研究員） パネリスト： - 有本 真由（アレシア国際法律事務所 代表弁護士） - クリス・ファン・ト・ホフ（DIVD マネージング・ディレクター） - ジョンチュン - 椛島 伸也（経済産業省） - ロバート・マーティン（MITRE）
Overview This speech summarizes the key points discussed during the meeting held on 2024-10-31, focusing on choosing and defining a reliable entity for a critical supply chain. The meeting included presentations from representatives of METI, Germany's Crisis Relief Organization, and a US participant, followed by a panel discussion. Key topics included cybersecurity, economic security, and the importance of public-private partnerships. **Introduction** • The panel started 30 minutes late and aimed to finish before 1 o'clock. • The theme focuses on how to choose and define a reliable entity for a critical supply	**講演メモ** **パネルディスカッションの進行** • **進行の遅れと終了時間** ○ 現在 30 分遅れて進行中。 ○ お昼休み前に終了するため、1 時前に終了を目指す。 **信頼できるエンティティの選定と指定** **重要経済安保情報保護活用法の成立** • **法成立の背景** ○ 今年の 5 月に国会で成立。 ○ 日本で初めての民間のセキュリティに関する法律。 • **法律の内容** ○ 重要経済安全保障事項を保護。 ○ サイバー共有情報やゼロデイ脆弱性情報が対象。 ○ 政府が保有する情報が保護・保全の対象。 ○ 公開前の脆弱性情報も保護される可能性。

chain.

- The Important Economic Security Information Protection Act was established in May this year in Japan.

Presentations

Economic Security Promotion Act

- **Kabashima (METI)**:
  - Established provisions for cybersecurity and economic security.
  - METI is responsible for risk analysis from the perspective of economic securities.
  - Reorganized to address cybersecurity and economic security under the Trade and Economic Security Bureau.
  - Integrated different departments for comprehensive coordination.
- **Day-to-Day Analysis**:
- **Scenario Analysis**: Includes geopolitical risks and tabletop exercises (TTX) for cybersecurity.
- **Supply Chain Analysis**: Focuses on dependency on other nations.
- **Technical Analysis**: Covers technical aspects and innovations.
- **Public-Private Partnership**:
  - Emphasized the importance of cooperation between government, private sectors, universities, and think tanks.
  - Recent Security Clearance Act allows for more sensitive discussions on risk-related information.

Role and Responsibilities

- **Chris Phanthoff (Germany's Crisis Relief Organization)**:
  - Leader of Germany's crisis relief organization, focusing on economic security of the supply chain.
  - Ethical hacker providing support to mitigate cyber threats.
- **Supply Chain Partners**:
  - Importance of software vendors, cloud providers, and mail servers.

サプライチェーンの保護

- **ゼロデイ脆弱性情報の共有**
  - 重要なインフラ事業者と情報を共有する可能性。
  - 公開前の情報を共有することでサプライチェーンを守る。

パネルディスカッションの参加者

- **参加者**
  - 日本、アメリカ、オランダから４名の専門家が参加。
  - ジョン・チュンさん（台湾）は台風の影響で欠席。
  - ロバートさんはオンラインで参加予定。
- **発表順**
  - 椛島さん
  - 有本さん
  - クリスさん
  - マーチンさん

椛島さんの発表

- **自己紹介**
  - 椛島さん、経済産業省（METI）のリスク分析担当。
  - 経済安全保障プロセスに関与。
- **発表内容**
  - 経済安全保障の促進マップ。
  - サイバーセキュリティだけでなく、経済安全保障も対象。

貿易経済安全保障局のリスク分析

技術性と技術的有益性の確保

- **技術性の確保**
  - 国家としての技術性の確保が重要。
- **技術的有益性**
  - 技術的な有益性の確保も必要。
- **エコノミック・セキュリティ**
  - 経済的な安全保障の観点からも技術管理が重要。

サイバーセキュリティ分野の情報発信

セキュリティクリアランス法の説明

- **新たな法律**
  - セキュリティクリアランス法が制定された。
- **アメリカの枠組み**
  - アメリカの機密情報は３つのレベルに分類される（トープシークレット、シークレット、コンフィデンシャル）。
- **日本の特定秘密**
  - 日本では特定秘密保護法があり、防衛、外交、有

- Risks associated with attacks on these partners.
- **Volunteer Efforts**:
  - Example of the Netherlands' volunteer firefighters on the Internet.
  - Designated as a trusted entity by the Dutch government.

Importance of Reliable Networks

- **Robert Martin (US Participant)**:
  - Stressed the need for a reliable network and supply chain.
  - Highlighted the importance of Public-Private Partnerships (PPP) for both cybersecurity and economic security.

Panel Discussion

- **Key Points**
- **Cyber Threats Visualization**:
  - Importance of recognizing and visualizing cyber threats and supply chain risks.
- **Information Protection**:
  - Discussion on the protection of information on financial security insurance.

Action Items

[ ] Enhance coordination between government, private sectors, universities, and think tanks for economic intelligence.

[ ] Extend the framework for sharing threat and risk information to the economic security area.

[ ] Implement more tabletop exercises (TTX) for scenario analysis in cybersecurity.

[ ] Increase efforts to visualize and recognize cyber threats and supply chain risks.

害な活動、スパイ活動、テロ行動に関する情報を保護する。

セキュリティクリアランスの必要性

- **個人のクリアランス**
  - 機密情報を取り扱うには個人のセキュリティクリアランスが必要。
- **コントラクターの基準**
  - 政府の標準に合ったコントラクターが情報を取り扱う。

経済安全保障情報保護法

- **新たな法律**
  - 2023 年 5 月に経済安全保障情報保護法が制定された。
- **重要インフラ**
  - 重要インフラに関する情報を保護する。
- **サプライチェーン情報**
  - プログラムやソフトウェアに関するサプライチェーン情報も含まれる。

法律の施行

- **施行時期**
  - 法律のフル施行は来年の 5 月。
- **詳細基準**
  - 詳細な基準は今年の冬に固まる予定。

脆弱性情報の共有

ドイツの脆弱性開示機関

- **サプライチェーンの重要性**
  - ソフトウェアベンダーやクラウドプロバイダーが重要。
- **CVE の提供**
  - 25 年間にわたり脆弱性情報を共有。
- **CNA（CVE Numbering Authority）の増加**
  - セキュリティ情報を提供する機関の数が増加。

脆弱性情報の公開

- **サイバークリミナルのリスク**
  - 公開された情報は犯罪者にも見られる可能性がある。
- **コーディネイティブプロセスディスクロージャー**
  - 脆弱性が見つかった場合の報告プロセス。

オランダの取り組み

- **ボランティア活動**
  - 約 150 名のボランティアが脆弱性情報を収集。
- **政府の信頼**

	○ オランダ政府から信頼されるエンティティとして活動。 **日本の取り組み** • **経産省のガイドライン** ○ 脆弱性情報開示に関する新たなガイドライン。 • **テーブルトップエクササイズ** ○ CVE を活用した研修の実施。 **アクティブなサイバーディフェンス** • **ハッカーの役割** ○ ハッカーの行動を通じてシステムの脆弱性を知る。 • **経済的メリット** ○ コストがかからず効果的なディフェンス方法。 **IoT デバイスのスキャン** • **総務省の発表** ○ IoT デバイスのスキャンを行う計画。 • **標準パスワードの問題** ○ 脆弱性のあるデバイスを特定するためのスキャン。 **IoT デバイスの懸念と対策** **IoT デバイスの脆弱性** • **ロボットやインターネット接続洗濯機** ○ IoT デバイスとしての懸念がある。 ○ クリティカルなインフラやスマートグリッドも対象に含まれるべき。 **サプライヤーの責任** • **ソフトウェアの伝達** ○ オンラインでのソフトウェア配信が重要。 ○ 数百万のコンバーターや電気エンジニアが関与。 ○ ファームウェアのリエンジニアリングでグリッドを不安定にする可能性がある。 **プライベートネットワークと事例の変更** **プライベートネットワークの接続** • **オフィスカット、RM、VPR** ○ プライベートネットワークとの接続で事例を変更可能。 **CB の視聴とインターネットコミュニケーション** • **視聴データ** ○ 12,000 件以上のフォーディゲットのアップデートが必要。 ○ 情報の公開とブロードキャストが行われている。 **法律の枠組みと脆弱性通知** **法律の枠組み** • **オランダの事例** ○ 脆弱性があるデバイスの使用通知が可能。

	ストリックスの事例 • **リモートアクセスとオフィスコネクション** ○ システムの脆弱性に関する事例がある。 ○ ドイツのフォークサイティングやフィンアップロード、ウェブシェルの情報も含まれる。 **多面的な展開とデータ共有** **多面的な展開** • **CBA システムと通知状態** ○ 多面的な展開が可能。 ○ 企業が通知を受け、必要に応じてシャットダウンを行う。 **日本とのデータ共有** • **日本の被害者情報** ○ 日本との情報共有が進んでいる。 ○ 被害者情報の送付と情報配布が行われている。 **ネットゲームとサイバーセキュリティ** • **事例紹介** ○ ヨーロッパでの警察と国民の関係についての事例。 ○ ネットゲームにおける摘発事例。 • **DIP アプローチ** ○ E メールアドレスの脆弱性について。 ○ パスワードの脆弱性とその影響。 • **サプライチェーンのセキュリティ** ○ サプライチェーンにおけるセキュリティの重要性。 ○ 脆弱性の把握と対策の必要性。 **国際的な取り組みと情報共有** • **オランダの取り組み** ○ オランダの国際的な取り組みの共有。 • **アメリカからの参加者** ○ ロバート・マーティン氏の参加。 ○ アメリカの時間帯での参加状況。 **サプライチェーンの保護** **経済産業省の取り組み** • **サプライチェーンの定義** ○ ソフトウェアとハードウェアのサプライチェーンの違い。 ○ 国家安全保障におけるサプライチェーンの重要性。 • **サプライチェーンの可視化** ○ サプライチェーンの状況認識とリスクの可視化の重要性。 ○ 経済産業省のフォーカス：脆弱性と外国依存。 **サプライチェーンのリスク管理** • **リスクの可視化**

	○ サプライチェーンのリスクと脅威の可視化。 ○ プロダクトと組織的なサプライチェーンの違い。 • **サイバーセキュリティの取り組み** ○ オランダの企業例（イスマイル）とサプライチェーンの構成。 ○ サイバーレーティングシステムの導入。 **経済安全保障と情報保護** **情報の機密性と国際共有** • **国内と国際の情報共有** ○ 国内での特定秘密の保護と国際的な情報共有の必要性。 ○ 各国との機密情報の取扱い条約の必要性。 • **トラフィックライトプロトコル** ○ 情報の機密性を示すプロトコルの導入。 ○ 赤、オレンジ、黄色、緑の各レベルでの情報共有の具体例。 **ホワイトハッカーとの信頼関係** • **脆弱性の検出** ○ ホワイトハッカーとの信頼関係の構築方法。 ○ 経産省のガイドラインに基づく脆弱性の報告と対応。 • **国際的な倫理規定** ○ 各国の法制度と倫理規定の遵守。 ○ 国際的な情報共有における法的リスク。 **パネルディスカッションのまとめ** • **信頼のあるネットワーク構築** ○ サプライチェーンとサイバーセキュリティの重要性。 ○ 経産省とコミュニティ専門家との協力強化。 • **脆弱性情報の共有** ○ 研究と情報共有の重要性。 ○ 11 月 16 日のオランダ大使館でのセミナー案内。 • **セキュリティクリアランス** ○ 機密情報保護のためのクリアランスの拡大。 ○ 同志国や同盟国との情報共有におけるリスク管理。 **アクションアイテム** [ ] 重要経済安保情報保護活用法の詳細な内容を確認する。 [ ] ゼロデイ脆弱性情報の共有方法を検討する。 [ ] パネルディスカッションの参加者にフィードバックを提供する。 [ ] セキュリティクリアランス法の詳細基準を確認する。

	[ ] 経済安全保障情報保護法の施行準備を進める。 [ ] 脆弱性情報の共有プロセスを見直す。 [ ] テーブルトップエクササイズの計画を立てる。 [ ] IoT デバイスのスキャン実施に向けた準備を行う。 [ ] フォーディゲットのアップデートを実施する。 [ ] 脆弱性があるデバイスの使用通知を行う。 [ ] 日本の被害者情報の共有を進める。

2.7 D2-S6 Special Session: Yomiuri International Forum

Panelists: - ADM(Ret.) Dennis Blair (Former Director of U.S. National Intelligence) - Satoru Tezuka (Project Professor, Keio University, Keio University Global Research Institute) - Shigeru Kitamura (Former Secretary General of National Security Secretariat of Japan / CEO, Kitamura Economic Security Inc. / Chairman, Yomiuri International Economic Society (YIES)) Coordinator: Kyoichi Sasazawa (Senior Research Fellow, Yomiuri Research Institute)	パネリスト： - デニス・ブレア（元米国家情報長官） - 手塚 悟（慶應義塾大学 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） - 北村 滋（YIES 理事長：前国家安全保障局長） コーディネーター：笹沢 教一（読売新聞東京本社調査研究本部主任研究員）
Overview This speech summarizes the discussions and key points from various meetings held on different dates. The focus is on cybersecurity, human resources development, political influence, and the transition to a digital society. The action items from these discussions are consolidated at the end of the document. **Introduction** • **Coordinator**: Kyoichi Sasazawa • **Theme**: Japan's ability to deal with the era of mistrust and confrontation • **Speakers**: ○ Mr. Dennis Blair, former National Intelligence Director of the US Obama administration ○ Mr. Tezuka ○ Mr. Kitamura **Session Overview** • **Broadcast**: Online for Yomiuri readers	サイバー脅威，官民協力，人材育成 **テーマ** この講演では、日本のサイバーセキュリティの現状と課題について議論されました。主な要点として、日本のサイバー脅威に対する脆弱性、犯罪組織や国家主体からの脅威、日本とアメリカのサイバーセキュリティ協力の重要性が挙げられました。また、日本の防御策の遅れや官民協力の必要性、サイバーセキュリティ専門家の不足についても触れられました。 **要点** 1. サイバー脅威に対する日本の脆弱性 2. 犯罪組織と国家主体からのサイバー脅威 3. 日本とアメリカのサイバーセキュリティ協力の重要性 4. 日本の防御策の遅れ 5. 2022 年の日本の国家安全保障戦略 6. 中国の台湾問題に対する準備 7. 日本の官民協力の必要性 8. サイバーセキュリティ専門家の不足 9. 民間企業と政府の協力 10. サイバーセキュリティにおける人材育成の重要性

- **Organizers**: Yomiuri Newspaper, Yomiuri International Economic Association, Keio Gijiku University, Global Research Institute, Cyber Civilization Research Center, Cyber Security Research Center, Maida Okamoto University

Keynote Speech by Mr. Dennis Blair

Cybersecurity Threats

- **Growing Threat**: Cyber threats are increasing rapidly, outpacing the ability to defend against them.
- **Fragility**: The internet and connected devices bring both benefits and significant vulnerabilities.
- **Lagging Actions**: Japan's cybersecurity measures are not keeping up with the potential dangers.

Sources of Cyber Threats

- **Criminal Organizations**:
  - Attacks on financial systems, essential services, and personal property.
  - International threat costing billions annually.
- **Hostile Nation States**:
  - Countries like China, North Korea, and Russia pose significant threats.
  - These nations have different values and world orders compared to Japan and the US.
  - Activities include stealing intellectual property and planting malware in critical infrastructure.

Cooperation Between Criminals and Nation States

- **Alarming Trend**: Criminal organizations and hostile nation states are increasingly cooperating.
- **Examples**: Russia and China working with criminal hackers to attack citizens, businesses, and security forces.

US Cybersecurity Measures

- **Organized Response**: The US has

ハイライト

- "日本は何らかの形で脅威に対するアクションを取らなければならないということです。"
- "日本もまた米国もなかなか同志国と連携して、貴重な予防するための行動というものが取れないような状況にあるわけですけれども、人々の苦しみというものを避けることで、我々としては弁護さなければなりません。"
- "日本の最高の才能が、タクティックを分割し、それをデジタルシステムと組み合わせるべきだ。"
- "国家安全は、国の存在に関係しています。しかし、その前にも、国家安全は、国の人々を守るためのものです。"

章とトピック

サイバー脅威

サイバー脅威は、インターネットやデジタルデバイスを通じて行われる攻撃や不正アクセスのことを指します。

- **要点**
  - 犯罪組織による脅威
  - 国家主体による脅威
  - デジタル資産や金融制度への攻撃
- **Examples**
  - 中国のハッカーがアメリカの電話、インターネットサービスプロバイダーに侵入し、個人の通信や警察当局の情報を盗んだ。
  - ハッカーがネットワークに侵入し、重要な情報を取得。
  - 警察当局の活動を監視し、犯罪者を探す情報を盗む。

サイバーセキュリティ対策

サイバー脅威に対抗するための防御策や対策を指します。

- **要点**
  - 官民協力の重要性
  - 防御体制の強化
  - 脆弱性のパッチ適用
- **Examples**
  - NTT は中国のハッカーと毎日戦い、IT システムに対する攻撃を防御している。
  - 継続的な攻撃に対する防御策を実施。
  - 政府と協力して防御体制を強化。

デジタルサイバーセキュリティ

デジタルサイバーセキュリティは、デジタル技術を利用してサイ

established a framework for dealing with cyber threats. • **Recent Breaches**: Examples include Chinese hackers penetrating networks of US service providers. • **Continuous Improvement**: The US focuses on detecting, remediating, and improving defenses. **Recommendations for Japan** • **Urgent Action Needed**: Japan must organize its government and private sector to address cyber threats. • **Clear Responsibilities**: Assign specific roles within the government and establish relationships with the private sector. • **Incentives and Penalties**: Encourage private sector cooperation through both incentives and penalties. • **Human Capacity**: Develop talent in cybersecurity to ensure a robust defense. **Panel Discussion** **Professor Satoru Tezuka** • **Background**: Professor at Keio Gijiku University, involved in cybersecurity research and policy. • **Symposium**: 14th Cybersecurity International Symposium focusing on digital security for national, economic, and societal security. • **US-Japan Alliance**: Emphasizes the importance of equal footing in cybersecurity efforts between the US and Japan. **Mr. Shigeru Kitamura** • **Background**: Former Director of the National Security and Security Department. • **Legislation**: Discussed the Important Economic Security Information Protection and Utilization Act. • **Mechanisms**: Stressed the need for monitoring and response mechanisms for	バー攻撃からシステムやデータを保護することを指します。 • **要点** ○ デジタル技術の利用 ○ サイバー攻撃の防御 ○ システムとデータの保護 **経済安全保障** 経済安全保障は、経済的な安定と成長を確保するためのセキュリティ対策を指します。 • **要点** ○ 経済的安定 ○ 成長の確保 ○ セキュリティ対策 **社会保障** 社会保障は、社会全体の安全と安定を確保するためのセキュリティ対策を指します。 • **要点** ○ 社会の安全 ○ 安定の確保 ○ セキュリティ対策 **アクティブサイバーディフェンス** アクティブサイバーディフェンスは、サイバー攻撃に対して積極的に防御する戦略を指します。 • **要点** ○ 積極的な防御 ○ サイバー攻撃の対策 ○ 防御戦略 **公共とプライベートセクターのパートナーシップ** 公共とプライベートセクターのパートナーシップは、政府と民間企業が協力してセキュリティ対策を行うことを指します。 • **要点** ○ 政府と民間企業の協力 ○ セキュリティ対策 ○ パートナーシップ **デジタルサイバーセキュリティ** デジタルサイバーセキュリティは、国家の安全保障と経済安全保障の両方において重要な役割を果たす。 • **要点** ○ 政府クラウドの創造 ○ 平時におけるインテリジェントシステムの構築 ○ アクティブサイバー・ディフェンスシステムの法制化 **日米同盟におけるデジタル技術協定** 日米同盟において、デジタル技術協定を結ぶことで、強固な

cyber attacks.

Key Points from Discussion

- **Infrastructure Protection**: Importance of protecting critical infrastructure, citing examples from the Crimea conflict and Ukraine invasion.
- **Public-Private Cooperation**: Need for vendors to report vulnerabilities and incidents, and share information.
- **International Cooperation**: Emphasized the importance of international collaboration in cybersecurity.

Current State of Japan in the World Cyber Security

- **Ranking and Progress**:
  - Japan's cyber security is compared to being in the "minor leagues" rather than the "major leagues."
  - Despite structural changes, Japan's on-the-ground capability has not kept pace with rising threats from criminal activities and state actors like China, Russia, and North Korea.
  - The top cyber secure countries currently are in the Baltics (Lithuania, Estonia, Latvia) due to their rapid development of defensive capabilities in response to massive attacks.
- **Threats and Responses**:
  - Japan's progress in cyber security has been falling behind the increasing threats.
  - The importance of proactive measures to prevent attacks rather than reactive measures post-attack is emphasized.
  - The need for Japan to work with like-minded countries to prevent cyber threats and ensure national security.

Strategic and Tactical Approaches

- **Strategic Importance**:
  - The integration of digital technology and AI to create a safe and secure world.

サイバースペースを構築する。

- **要点**
  - デジタル技術協定の必要性
  - Five Eyes との連携

サイバー攻撃への対策

ロシアや中国による選挙へのサイバー攻撃に対する対策が必要。

- **要点**
  - ロシアの選挙干渉の歴史
  - 中国の高度な手法
  - 米国の対策

IT 教育の強化

日本の教育システムにおいて、IT 教育を強化する必要がある。

- **要点**
  - 小学校や中学校での IT 教育
  - 大学でのサイバー関連教育の拡充

公私連携による人材育成

公私連携によってサイバーセキュリティの人材を育成する。

- **要点**
  - 政府、民間セクター、学界の協力
  - プライベートセクターでの経験

通信の秘密とメタデータの開示

通信の秘密に関する最高裁判所の判決では、通信会社がメタデータを開示する必要がないとされた。

- **要点**
  - 通信の秘密の重要性
  - メタデータの定義とその扱い
  - 最高裁判所の判決内容

サイバー攻撃と防御

サイバー攻撃の対象として地域の大病院が挙げられ、国家安全保障の一環としてサイバー防御チームの役割が強調された。

- **要点**
  - サイバー攻撃の対象とその影響
  - サイバー防御チームの構成と役割
  - 国家安全保障とサイバーセキュリティの関係

サイバーセキュリティにおける教育とトレーニング

サイバーセキュリティの強化には、教育とトレーニングが不可欠であり、日本の防衛省や IT 企業、研究機関、大学がその役割を果たすべきである。

- **要点**

- The necessity of balancing the culture of the country with the system to enhance cyber security.
- **Tactical Implementation**:
  - The importance of operational technology in implementing system theories and technical theories.
  - The role of the technology industry in advancing cyber security measures.

Proposed Systems

- **Government's Top-Level Cloud**:
  - Development of a top-level cloud system for government use.
  - Implementation of a Cyber Intelligence System from the beginning to ensure proper attributions.
- **Active Defense System**:
  - Establishment of an active defense system under national security laws.
  - Protection of critical infrastructure systems for economic security.
- **Digital System**:
  - Ensuring the functionality of essential services like electricity, communication, railways, ATMs, and healthcare through a robust digital system.

Constitutional and Privacy Issues

Information Gathering and Privacy

- **Constitutional Responsibilities**:
  - The Japanese constitution should allow the government to gather information about hostile intentions of its enemies while protecting the privacy of its citizens.
  - The global nature of the internet blurs traditional physical separations, complicating information gathering.
- **Privacy Concerns**:
  - Challenges in balancing privacy rights with national security needs, especially when foreign spies use domestic systems.
  - The need for a framework that allows the government to gather necessary

- 教育とトレーニングの重要性
- 日本の防衛省やIT企業、研究機関、大学の役割
- 日米同盟とサイバーセキュリティの協力

情報リテラシーとファクトチェック

サイバー社会においては、情報リテラシーとファクトチェックが重要であり、正確な情報の提供が求められる。

- **要点**
  - 情報リテラシーの重要性
  - ファクトチェックの必要性
  - 正確な情報提供の方法

宿題と提案

information without violating citizens' rights.

U.S.-Japan Alliance

- **Evolution of the Alliance**:
  - The U.S.-Japan alliance has evolved from an unequal relationship to a more balanced partnership.
  - Japan has taken the lead in many aspects of common defense, especially as the U.S. focused on the Middle East.
- **Cyber Security Cooperation**:
  - Japan needs to enhance its cyber security for its own purposes and to strengthen the U.S.-Japan alliance.
  - Collaboration in cyber security is crucial to prevent weaknesses in one country from being exploited against the other.

Political Influence and Cyber Threats

U.S. Presidential Elections

- **Foreign Influence**:
  - In 2016, Russia attempted to influence the U.S. election in favor of Donald Trump.
  - The U.S. government mobilized cyber resources in 2018 and 2020 to counter these attempts successfully.
- **Current Threats**:
  - In 2024, both Russia and China are expected to continue their efforts to influence U.S. elections.
  - These efforts include exacerbating existing divisions within American society and spreading misinformation.

Influence in Taiwan and Japan

- **Taiwan**:
  - Taiwan faces even higher intensity of misinformation attacks due to its proximity to China.
  - The situation in Taiwan is more severe compared to the U.S.
- **Japan**:
  - There is an assumption that China

attempts to influence Japanese politics to its advantage. ○ Efforts may include discrediting anti-Chinese politicians and supporting those less antagonistic to China. **Human Resources Development** **Importance of Human Resources** • **Growth of Human Resources**: Emphasized the need to grow human resources step by step to ensure Japan's capability in this area. • **Categories of Human Resources**: ○ **Power of Initiative**: Already present and needs to be taken seriously. ○ **Ability to Grow Slowly and Steadily**: Requires a comprehensive approach. **Education and IT Integration** • **Basic Education**: ○ **Elementary and Junior High Schools**: Current IT education is insufficient. ○ **High School to University Level**: Need to increase the population receiving IT education. ○ **Keio University Example**: Cybersecurity education at SFC. • **Public-Private Cooperation**: Essential for growing direct force, involving government, private companies, and academia. **Cultural and Ecosystem Development** • **Cultural Issues**: Need to discuss and create an ecosystem for human resources development. • **Examples from the U.S.**: Military personnel educated and transitioning to the private sector, establishing strong positions in companies. **Improving Social Situations** **Public Officials and Professional Knowledge** • **Hiring Great People**: Challenge in hiring highly skilled individuals in the public sector.	

- **Frequent Replacement**: Need to replace officials with professional knowledge more frequently.
- **Security Clearance**: Preserving sensitive information to enable public-private cooperation.

Cybersecurity and Legal Framework

- **Lack of Motivation for Security Guarantees**: Example of communication secrecy and metadata disclosure laws.
- **Cyber Attacks on Medical Institutions**: Frequent attacks but lack of specific legal mention.

Cybersecurity Team Dynamics

Example from the U.S.

- **Team Composition**: Mix of experienced civilians, military personnel, and young individuals with diverse backgrounds.
- **Interactive Fight in Cyberspace**: Personal and interactive approach to cybersecurity.
- **Patriotism**: Unites the team in defending against cyber threats.

Japan's Potential

- **Talent and Education**: Japan has the talent but needs more education and on-the-job learning.
- **Initiatives in Yokosuka**: Collaboration between Ministry of Defense, IT companies, and educational institutions.
- **Need for Incentives and Rewards**: Faster development and recognition of cybersecurity efforts.

Senkaku Islands Incident (2011)

Nationalization and Media Reports

- **Event Description**: In 2011, the Noda Cabinet nationalized the Senkaku Islands.
- **Media Reports**:
  - News spread about a large number of fishing boats heading to the Senkaku Islands.
  - Reports also claimed that numerous

Chinese military aircraft carriers were heading to the islands. ○ **Clarification**: These reports were later found to be inaccurate. **Cyber Security and Information Manipulation** **Actors in Information Manipulation** • **Criminals and Government**: Both criminals and government entities are involved in manipulating information. • **Forms of Warfare**: ○ **Legal War**: Using legal means to influence information. ○ **Political War**: Political strategies to manipulate public perception. ○ **Psychological War**: Psychological tactics to sway national will. **Importance of Fact-Checking** • **Media Responsibility**: Emphasized the need for thorough fact-checking by the media to avoid spreading misinformation. • **National Resilience**: Importance of not being intimidated by manipulative activities. **Cyber Literacy** • **Healthy Cyberspace**: Advocated for leading a healthy life in cyberspace. • **Citizen Literacy**: Discussed incorporating cyber literacy for each citizen to better navigate and understand the digital world. **Transition to Digital Default** **Importance of Digital Default** • **Current Culture**: The prevailing culture in the country is still heavily reliant on paper. • **Goal**: Transitioning to a digital default is seen as the most crucial step. • **Outcome**: Moving to digital will ultimately foster trust. **Interoperability and Trust** • **Interoperability**: Essential for achieving	

a digital society.
• **Assurance Levels**: Different levels of trust and assurance need to be considered.
• **Social Foundation**: Establishing a robust social foundation is critical.
Crime and Social Habits
• **Example of Crime**: In Japan, there is a unique social habit related to crime.
• **Interoperability in Crime**: The act of committing a crime is the same for everyone, demonstrating interoperability.
• **Power of Crime**: The reliability and security of the power behind the crime are key points.
• **Safe Digital Society**: Ensuring a secure and reliable digital society is paramount.
Building Trust
• **Trust in Signatures and Approvals**: It's important to build a world where the trust of those who sign and approve documents is solid.
• **Society 5.0**: Introduced as a data-driven architecture.
  ○ **20th Century**: Era of oil.
  ○ **21st Century**: Era of data.
• **Zero Trust Concept**: Using this concept to build trust in a data-driven society.
Action Items
[ ] Assign clear responsibilities within the government for cybersecurity.
[ ] Establish relationships and cooperation mechanisms between the government and private sector.
[ ] Develop incentives and penalties to encourage private sector participation in cybersecurity efforts.
[ ] Create a policy and legal framework to facilitate information exchange and collaboration.
[ ] Promote cybersecurity as a career to develop necessary human capacity.	

[ ] Develop and implement a top-level cloud system for government use. [ ] Establish a Cyber Intelligence System from the beginning. [ ] Create an active defense system under national security laws. [ ] Protect critical infrastructure systems for economic security. [ ] Ensure the functionality of essential services through a robust digital system. [ ] Enhance Japan's cyber security measures and collaborate with the U.S. to strengthen the alliance. [ ] Increase IT education at elementary and junior high school levels. [ ] Enhance cybersecurity education at high school and university levels. [ ] Foster public-private cooperation for human resources development. [ ] Develop a comprehensive ecosystem for human resources growth. [ ] Implement frequent replacement of officials with professional knowledge. [ ] Establish security clearance for preserving sensitive information. [ ] Incentivize and reward cybersecurity efforts in Japan. [ ] Conduct thorough fact-checking of information before dissemination. [ ] Develop and implement cyber literacy programs for citizens. [ ] Transition to a digital default in the country. [ ] Establish different levels of trust and assurance. [ ] Build a robust social foundation for a digital society. [ ] Ensure the reliability and security of digital systems. [ ] Promote the concept of Society 5.0 and its data-driven architecture. [ ] Implement the zero trust concept to build trust in the digital era.	

2.8 D2-S9 Speech

Seow Hiong Goh (Representative, Coalition for Cybersecurity in Asia-Pacific)	セウ・ヒョン・ゴー（アジア太平洋サイバーセキュリティ連合代表）
AI, Cybersecurity, Data Security **Theme** This speech, held on October 31, 2024, explores the relationship between AI and cybersecurity. Key topics include AI as a vulnerability, data security risks, model security risks, infrastructure risks, and various types of attacks such as data poisoning and evasion attacks. The speech also covers government approaches to AI regulation and organizational guidance for managing AI risks. **Takeaways** 1. AI and cybersecurity relationship 2. AI as a vulnerability 3. Data security risks 4. Model security risks 5. Infrastructure risks 6. Application risks 7. Data poisoning 8. Data extraction 9. Inference data 10. Evasion attacks **Highlights** • "AI itself is potentially a vulnerability." **Chapters & Topics** **AI and Cybersecurity** The relationship between AI and cybersecurity, including how AI can be used for both attacks and defense. • **Keypoints** ○ AI can be used to mount attacks. ○ AI can be used to defend against attacks. ○ AI itself can be a vulnerability. **Data Security Risks** Risks associated with the data used to train AI systems. • **Keypoints** ○ Data poisoning	AI, サイバーセキュリティ, リスク管理 **テーマ** この講演では、AIとサイバーセキュリティの関係について議論しました。AIは攻撃と防御の両面で利用されるが、同時に脆弱性も持つ可能性があります。データセットの質と種類、AI の誤認識リスク、インフラリスク、組織への影響などが主要なテーマとして取り上げられました。また、リスク対応フレームワークの必要性と各国の規制や法律についても触れられました。 **要点** 1. AIとサイバーセキュリティの関係 2. AI の攻撃と防御の両面での利用 3. AI の脆弱性とリスク 4. データセットの重要性 5. AI のトレーニングとアウトカム 6. 機密データの取り扱い 7. AI の誤認識リスク 8. モデルポイズニングとモデルスティーリング 9. インフラリスク 10. AI 導入の組織へのインパクト **ハイライト** • "AI はサイバーセキュリティに影響を及ぼしますが、その中であまりリスクされていないのは、組織として AI を使うリスク、まだまだそれは議論が進んでいない部分もあります。" **章とトピック** **AI とサイバーセキュリティの関係** AI はサイバーセキュリティにおいて攻撃と防御の両面で利用されるが、同時に AI 自体が脆弱性となる可能性もある。 • **要点** ○ AI は攻撃にも防御にも利用可能 ○ AI の脆弱性とリスク ○ データセットの重要性 • **留意点** ○ AI を使用する際のリスク管理 ○ データセットの選定と管理 **AI のトレーニングとアウトカム** AI のトレーニングに使用するデータセットの質と種類が、AI の挙動やシステムの動きに大きな影響を与える。

○ Data extraction ○ Inference data • **Examples** During the process of training the data, affecting the input data to introduce back doors into the AI system. Using queries to infer what data was used to train the AI, potentially extracting sensitive information. **Model Security Risks** Risks associated with the AI model itself. • **Keypoints** ○ Evasion attacks ○ Backdoor attacks ○ Model poisoning ○ Model stealing • **Examples** Causing the AI system to misclassify or misdiagnose a situation, such as not recognizing a stop sign. Training the AI to misbehave in a certain way, such as misclassifying faces when a particular pair of glasses is worn. **Infrastructure Risks** Risks associated with the infrastructure supporting AI systems. • **Keypoints** ○ Denial of service ○ Resource exhaustion **Government Approaches to AI Regulation** Different approaches taken by governments in the Asia-Pacific region to regulate AI. • **Keypoints** ○ Building on existing laws ○ Avoiding over-regulation ○ Developing standards **Organizational Guidance for AI** Guidance for organizations on how to manage AI risks. • **Keypoints** ○ Guidance and oversight ○ Life cycle management	• **要点** ○ データセットの質と種類 ○ AI の挙動とシステムの動き • **留意点** ○ 機密データの取り扱い ○ データセットの選定 **AI の誤認識リスク** AI が特定の状況で誤認識をするリスクがあり、これがセキュリティに重大な影響を与える可能性がある。 • **要点** ○ ストップサインの認識ミス ○ バックドアのアタック ○ モデルポイズニングとモデルスティーリング • **留意点** ○ AI の誤認識リスク管理 ○ セキュリティシステムの強化 **AI 導入の組織へのインパクト** AI を組織に導入する際には、インフラリスクやリソースの枯渇などのリスクを考慮する必要がある。 • **要点** ○ インフラリスク ○ リソースの枯渇 • **留意点** ○ インフラリスク管理 ○ リソースの最適化 **AI とサイバーセキュリティのリスク対応フレームワーク** AI とサイバーセキュリティのリスクに対応するためのフレームワークが必要であり、各国の規制や法律も考慮する必要がある。 • **要点** ○ リスク対応フレームワーク ○ 各国の規制と法律 • **留意点** ○ 規制とイノベーションのバランス ○ 既存の法律の活用 **宿題と提案**

○ Model security ○ Data management ○ Transparency ○ Incident reporting and response **Assignments & Suggestions**	

2.9 D2-P7 Panel: Evolving Compute Paradigms and National Security: Navigating the Edge to Cloud Continuum

Moderator: James Miller (Director, JICSS) Discussant: David J. Farber (Special Advisor, JICSS/Guest Professor, Keio University) Panelists: - Aapo Oksman (Founder, Juurin Oy) - Tripp Roybal (Director of Engineering, Japan Secure Technologies, K.K) - Kamel Ghali (Vice President, Car Hacking Village) - James Bettke (Security Researcher)	モデレーター：ミラー・ジェームズ（JICSS ディレクター） ディスカッサント：デイビッド・ファーバー（JICSS 特別顧問） パネリスト： - アーポ・オクスマン（Juurin Oy 創業者） - トリップ・ロイバール(株式会社ジャパンセキュアテクノロジーズ開発部長) - カメル・ガリ（Car Hacking Village 副会長） - ジェームス・ベッキ（セキュリティー研究者）
Cybersecurity, IoT, Regulation **Theme** This speech, part of the Annual Cybersecurity Summit, covered key topics including the impact of digitization on cybersecurity, the challenges and solutions in IoT security, and Japan's legal and regulatory approaches to cybersecurity. Highlights included discussions on the integration of new systems into existing infrastructure, the importance of authentication and auditing techniques, and the role of edge computing and local storage in IoT systems. **Takeaways** 1. Annual Cybersecurity Summit 2. Evolving compute platforms and economic/national security 3. Digitization and cybersecurity 4. Integration of new systems into existing infrastructure 5. Authentication, authorization, and auditing techniques 6. Japan's legal and regulatory approaches 7. Progress in economic and national security	**概要** この講演は、2024 年 10 月 31 日に作成された会議の議事録とメモを基に、サイバーセキュリティ、IoT、データストレージ、無線技術などに関する議論をまとめたものです。各セクションでは、専門家の意見や日本の技術力、法的制度の枠組み、グローバルな脅威への対応などが取り上げられています。また、アクションアイテムとして具体的な対策や進捗確認の項目がリストアップされています。 **進化するコンピューティングのパラダイムと国家安全保障** **サイバー物理システムのデジタル化** • **インフラのデジタル化**：物理システムがデジタル化され、経済で活用されるようになっている。 • **サイバーセキュリティの重要性**：デジタル化が進むにつれて、サイバーセキュリティの向上が必要。 ○ **攻撃対象の増加**：システムがデジタルファブリックの一部になることで、攻撃対象が増加。 ○ **複雑性の増加**：デジタルシステムと既存のインフラの連携により、脆弱性のリスクが増加。 **日本の対応と法的制度の枠組み** • **法的制度の枠組み**：日本はクリエイティブな法的制度の枠組みを作る必要がある。 ○ **規制システムの強み**：比較対処をしながら進める規制システムが強み。 ○ **進捗の確認**：規制が整った中で、実際のプロセスで

8. Cybersecurity outcomes and regulatory changes
9. IoT security and consulting
10. Automotive cybersecurity

Highlights

- "The value of digitizing systems and improving their cybersecurity, their ability to take advantage of data to do the sorts of things that we were just hearing about with AI, are important and something that everyone should be prioritizing."
- "If you can hack one device, you most likely can hack all of them."
- "I think as cybersecurity and privacy has become more of a priority in this digital interconnected age, understanding of computer networks and cybersecurity, I would hope, becomes a fundamental thing that you learn as you grow up."-- Camille

Chapters & Topics

Annual Cybersecurity Summit

A yearly event where experts gather to discuss the latest trends and issues in cybersecurity.

- **Keypoints**
  - Opportunity to meet old and new friends
  - Discussion on AI and cybersecurity concerns
  - Focus on evolving compute platforms and their impact on economic and national security

Digitization and Cybersecurity

The process of converting physical elements into digital form and the associated cybersecurity challenges.

- **Keypoints**
  - Digitization offers tremendous opportunities and benefits
  - Increased attack surface with digitization
  - Importance of integrating new systems into existing infrastructure

Japan's Legal and Regulatory Approaches

Japan's approach to developing legal and

進捗があるかどうかの確認が必要。

専門家の意見

- **サイバーセキュリティの専門家**: IoT の領域やサイバー物理システムの専門家がパネルに参加。
  - **アーポ・オクスマン**: IoT のセキュリティコンサルタント。脆弱性のリサーチや自動車関係のハッキングコンテストに参加。
  - **トリップ・ロイボール**: セキュリティリサーチ、ペンテスト、レッドチームの経験を持つ。特にエネルギー業界での経験が豊富。
  - **カメルガル**: セキュリティデリバリーマネージャー。自動車のハッキング防止のためのサイバーセキュリティ構築に従事。
  - **ジェームズ・ミラー**: クラウド企業の役員。日本でサイバースペースの研究を行っている。

日本の IoT とサイバーセキュリティの課題

日本の技術力とサイバーセキュリティ

- **技術力の高さ**: 日本はテクノロジーエンジニアリングで素晴らしい成果を上げている。
  - **イノベーション**: IoT の分野でのシグナリング、センサー、マイクロコントローラーの設計など。
- **サイバーセキュリティの遅れ**: 技術力に比べてサイバーセキュリティが追いついていない部分がある。

グローバルな脅威と日本の対応

- **脅威の近さ**: 中国、ロシア、北朝鮮などの脅威が日本に近い。
- **サプライチェーンのセキュリティ**: サプライチェーンのセキュリティを強化する必要がある。
  - **セキュリティの証明**: 製品のセキュリティを証明するためのインプリメントが必要。

IoT エンジニアリングの課題

- **マルチベンダー環境**: 複数のベンダーが同じようなシステムを提供しているため、競争が激しい。
- **セキュリティの要求**: デバイスの数が増えるとともに、セキュリティの要求も増加。

サプライチェーンの近代化

- **サプライチェーンの強み**: 日本はサプライチェーンが強いが、近代化が必要。
- **セキュリティの高い環境**: サプライチェーン全体でセキュリティを担保する必要がある。

経済とサイバーセキュリティ

- **自動車産業の重要性**: 日本の GDP に占める自動

regulatory systems for cybersecurity.

- **Keypoints**
  - Outstanding jurisdiction for legal and regulatory systems
  - Progress in economic and national security
  - Need for better cybersecurity outcomes

IoT Security

Security measures and consulting for Internet of Things (IoT) systems.

- **Keypoints**
  - Consulting and security assessments for IoT systems
  - Participation in automotive hacking competitions
  - Challenges in securing IoT devices

Supply Chain Security

Ensuring the security of the supply chain for various products, especially in the context of IoT and automotive industries.

- **Keypoints**
  - Importance ofSBOM (Software Bill of Materials)
  - Impact of Cyber Resilience Act (CRA)
  - Challenges in securing supply chains

Cyber-physical systems and their potential safety implications

Cyber-physical systems, including passenger vehicles, interact with the real world and people, posing potential safety risks in the event of a compromise or cyber-attack.

- **Keypoints**
  - Interaction with the real world and people
  - Potential safety risks in case of compromise
  - Importance of addressing these risks

Risk quantification and threat analysis in the automotive industry

Risk quantification and threat analysis are essential methodologies in the automotive industry to understand the impact of cyber attacks and allocate resources for securing

車産業の割合が大きい。

- **サプライチェーンのリスクとチャンス**：サプライチェーンの中でセキュリティが重視される。

自動車業界におけるサイバーセキュリティ

ライフロングのサイバーセキュリティ保障

- **自動車業界の規制**：
  - 自動車業界は日本だけでなく、世界全体でも非常に規制が厳しい。
  - 日本は先を見越した形でサイバーセキュリティの法規制、法整備を進めている。
  - EU のサイバーレジリアンスアクトが日本にもインパクトを与えることが予想される。
- **外部要因の影響**：
  - 外部からの要因も日本にとって大きな要素となっている。
  - インテリジェンスを構成するコンポーネント（例：レスポン）を評価し、情報に基づいた意思決定を行うことが重要。

脆弱性管理とトレンド

- **自動車業界のトレンド**：
  - 脆弱性管理が自動車業界における主流的なトレンドとなっている。
  - 他の業界も参考にできるようなサイバーセキュリティの保証が求められている。
- **他業界とのクロスオーバー**：
  - 医療機器なども法規によって管理されている。
  - 自動車のサプライチェーンの進化や付加価値を提供するサービスの進展が見られる。

クリティカルインフラとセキュリティ

- **クリティカルインフラの要件**：
  - 水処理や製造システムなどのクリティカルインフラでは、常に稼働させておくことが求められる。
  - 自動車における特別な要件（例：制動システムの脆弱性）がある場合、製造ラインを止める必要があることもある。
- **IoT とサイバーセキュリティ**：
  - 自動車における IoT とサイバーセキュリティの課題が存在する。
  - サイバー攻撃のリスクを見ながら進める必要がある。

重要インフラとリスク管理

物流業界の重要性

- **物流業界のリスク**：

devices.

- **Keypoints**
  - Importance of risk quantification
  - Threat analysis methodologies
  - Resource allocation for security

SAE ISO 21434 standard for vehicle cybersecurity

SAE ISO 21434 is an industry standard adopted for vehicle cybersecurity regulation, providing a framework for risk assessment and compliance.

- **Keypoints**
  - Industry standard for vehicle cybersecurity
  - Framework for risk assessment
  - Compliance with regulations

The role of auditors in legislation compliance

Auditors rely on risk assessments to understand the stakes and judge whether the steps taken to secure assets are appropriate or lacking.

- **Keypoints**
  - Reliance on risk assessments
  - Understanding the stakes
  - Judging the appropriateness of security measures

The impact of cyber attacks on economic security

Cyber attacks on logistics functions can have large-scale economic security implications, requiring heightened concern and a risk-based approach to reviews.

- **Keypoints**
  - Impact on logistics functions
  - Large-scale economic security implications
  - Need for heightened concern and risk-based approach

The use of drones in military and civilian contexts

Drones are used in both military and civilian contexts, with implications for data collection, command and control, and cybersecurity.

- **Keypoints**
  - 物流、輸送領域、交通、食品や水も重要インフラの一部として考える必要がある。
  - ランサムウェアによるトラックへの影響が社会全体に及ぶリスクがある。
- **テクノロジーの展開**:
  - テクノロジーがどんどん展開されているが、経済安全保障にかかるものもある。
  - 規制当局は経済安全保障とリスクベースなアプローチの違いを把握すべき。

リスク評価とインテリジェンス

- **リスクの定量化**:
  - リスク評価が自動車業界で提供されているISOを使用して行われている。
  - サイバー攻撃のリスクを把握し、リソースの割り当てやバックアップ、冗長性の準備が必要。

リスク評価と監査

リスク評価の重要性

- システムが直面する可能性のあるリスクを評価し、それが企業単位、社会単位でどれくらいの影響を及ぼすかを考慮することが重要。
- 物流地位も考慮し、リスク評価のアウトプットが重要である。

監査の視点

- 監査側にとって、規制に対応しているか否かの監査は非常に有益なインプットとなる。
- デバイスや車両がアセットを守るために必要なステップを取っているかをチェックする必要がある。

軍事技術と消費者向けテクノロジー

ドローンの利用

- モビリティとしてのドローンの利用が議論され、ウクライナの事例が紹介された。
- ウクライナ戦争において、サイバーインフラが重要な役割を果たしている。

システム間の信頼

- 軍事と自動車のセキュリティにおいて、システム間の情報共有が重要。
- ゼロトラストのアプローチが必要である。

日本におけるデュアルユースの進捗

デュアルユースの課題

- ウクライナの事例を通じて、デュアルユース（民生用と軍事用）の技術が議論された。
- エッジコンピューティングとクラウドの違いが強調され

○ Use in military and civilian contexts ○ Data collection and command and control ○ Cybersecurity implications **Challenges in drone operation and regulation in Japan** Japan faces challenges in drone operation and regulation, including difficulties in flying and testing drones, which impact workforce familiarity and innovation. • **Keypoints** ○ Challenges in drone operation ○ Regulatory issues ○ Impact on workforce familiarity and innovation **The importance of edge computing and local storage in drone operations** Edge computing and local storage are crucial in drone operations for data capture, processing, and ensuring functionality during infrastructure failures or jamming. • **Keypoints** ○ Importance of edge computing ○ Local storage for data capture and processing ○ Ensuring functionality during failures or jamming **The role of 5G and other wireless technologies in IoT automation** 5G and other wireless technologies play a significant role in IoT automation, providing connectivity and enabling secure command and control of devices. • **Keypoints** ○ Role of 5G in IoT automation ○ Connectivity and command and control ○ Security implications **The need for diversified wireless technologies for command and control** Diversifying wireless technologies, such as Bluetooth, mesh technologies, and LoRa, is essential for reliable command and control, especially during infrastructure failures.	た。 **日本の進捗** • 日本でのドローン利用や海上保安庁の事例が紹介され、日米間のギャップが指摘された。 • IoT の課題として、規制の問題や考え方の違いが挙げられた。 **ワイヤレス技術とエッジコンピューティング** **ワイヤレス技術の進展** • 日本の大学でのリサーチが紹介され、ワイヤレス技術の進展が議論された。 • 5G や 6G の展開がエッジコンピューティングやバンド幅に大きな影響を与えるとされた。 **安全性とプライバシー** • ドローンの安全性やプライバシーの確保が重要であると強調された。 • アドホック、メッシュ、ワイヤレスのメッシュなどの技術が議論された。 **災害時の対応と社会の安全保障** **災害時のデータ利用** • 自然災害時にドローンから得られるデータを活用し、AI のワークロードを使って社会の安全保障に役立てることが議論された。 • エッジデバイスの利用が強調された。 **ワイヤレス技術の適用** • ワイヤレス技術の適用範囲が広がり、シームレスなフェイルオーバーが重要であるとされた。 • 安全性とプライバシーの確保が求められる。 **データのストレージと無線技術** **データのストレージ** • データのストレージに関して、2 つの別個の機能として捉えるのではなく、統合的に考える必要がある。 **無線技術の構築** • 無線技術を構築する際、e コマースのプラットフォームを利用することで、必要な機器を簡単に手に入れることができる。 ○ 例：秋葉原での購入 • ジェームスさんの意見として、日本では無線技術のテストが比較的簡単に行える可能性がある。 **フライトコントロールとデータリンクの可能性** **ワイヤレスコンポーネントの利用** • フライトコントロールにワイヤレスコンポーネントを置き換える可能性について議論。

- **Keypoints**
  - Diversification of wireless technologies
  - Bluetooth, mesh technologies, and LoRa
  - Reliability during infrastructure failures

The integration of communication and data processing in IoT systems

The integration of communication and data processing in IoT systems blurs the lines between these functions, requiring a seamless approach to design and implementation.

- **Keypoints**
  - Integration of communication and data processing
  - Blurring of functional lines
  - Seamless design and implementation

The importance of secure local computing in IoT systems

Secure local computing is a critical component of IoT systems, enabling data processing and security functions closer to the data source.

- **Keypoints**
  - Importance of secure local computing
  - Data processing closer to the source
  - Enhanced security functions

The role of Japan in robotics and hardware innovation

Japan excels in robotics and hardware innovation, with opportunities to lead in the development of secure and advanced IoT systems.

- **Keypoints**
  - Excellence in robotics and hardware
  - Opportunities for leadership in IoT
  - Development of secure and advanced systems

The need for adaptable security requirements in future IoT systems

Future IoT systems must be designed with adaptable security requirements to address evolving threats and ensure long-term protection.

- **Keypoints**
  - Adaptable security requirements

- 日本のコンポーネントを使用した平地環境での展開の可能性。
- 秋葉原のコンポーネントショップや IoT、DIY ショップで入手可能なコンポーネントの統合プロセスについて。

コンポーネントの信頼性と課題

- オープンな企画標準の存在とその限界。
- 基本的な設計の課題や信頼性の高いコンポーネントの必要性。
- トランシーバー、ストレージモジュール、フライトコントローラーなどのベースレイヤーでの信頼性。

日本のシステムと今後の投資フォーカス

ハードウェア市場の進展

- ドローンや UAS システムにおける一般的なコンポーネントの現状。
- フライトコントローラーやアクセラルメーターの国産部品の不足。
- オンシュアリングの課題と市場の独占状況。

国内生産の可能性

- 国内でのコンポーネント生産によるギャップ解消の可能性。
- 自動運転車や自動化の進展に関する議論。

自動運転と規制動向

自動運転の進展

- 日本の高齢化と自動運転の進展。
- インテリジェンス、防衛、重要インフラに関する規制動向。

信頼されるコンポーネント作り

- 自動運転車やモビリティアザサービスにおける信頼されるコンポーネントの必要性。
- 汎用 IoT と車の強みと弱みの比較。

セキュリティと将来予測

セキュリティ要件の予測

- Edge to Cloud システムにおける成長要因と進捗。
- 5 年後のセキュリティ要件の予測の難しさ。

次世代製品の推定とセキュリティ要件

- **次世代製品の推定**
  - 現在構築しているものを見ながら、次世代の製品がどうなるのかは推定でしかできない。
  - いろんな企画や標準が出てきているが、将来のセキュリティの要件に適応していくことは大きな試みである。

- Addressing evolving threats
- Ensuring long-term protection

The importance of zero trust principles in IoT device design

Zero trust principles are essential in IoT device design, ensuring that devices do not trust external inputs and have built-in security measures.

- **Keypoints**
  - Zero trust principles
  - No trust in external inputs
  - Built-in security measures

The potential risks of power grid vulnerabilities

Power grid vulnerabilities, such as those in solar panels and energy management systems, pose significant risks, including the potential for blackouts caused by cyber attacks.

- **Keypoints**
  - Risks of power grid vulnerabilities
  - Impact on solar panels and energy management systems
  - Potential for blackouts caused by cyber attacks

The need for rate limiting and AI-based detection in IoT devices

Implementing rate limiting and AI-based detection in IoT devices can prevent widespread control and mitigate the impact of cyber attacks.

- **Keypoints**
  - Importance of rate limiting
  - AI-based detection
  - Preventing widespread control

The importance of strong edge computing in robotics

Strong edge computing is crucial in robotics to ensure safe operation, data confidentiality, and functionality during connectivity issues.

- **Keypoints**
  - Importance of strong edge computing
  - Ensuring safe operation
  - Data confidentiality and functionality

- **ヨーロッパとアメリカのトレンド**
  - システムを別々のコンポーネント単位で作る。
  - 工場を近代化し、製造プロセスから出たデータをクラウドに流して改善のアイデアを得るビジネスのメリットを見出す。
  - 既存の工場を全体近代化するのは難しいため、ニーズに応じた形でコンポーネントにシステムを入れていく。

コンポーネントの導入例

- **ゲートウェイデバイス**
  - 工場に持ち込んでデータを抽出する活動が進んでいる。
  - 2 年間に一度、次世代のデバイスを導入し、3 年後、4 年後に使用可能にすることで要件を達成する。

標準と基準の使用

- **自分たちの標準と基準**
  - 自分たちの標準や基準を使いたいという意見がある。
  - セキュアなローカルコンピューティングの要素（エッジ、プロキシー、ゲートウェイ）を早く進めることが重要。

ローカルコンピューティングの利点

- **セキュリティ戦略**
  - ローカルコンピューティングが全体のセキュリティ戦略に良い影響を与える。
  - OT 環境でデータを触り、機能の情報を取ってプロセスの改善を行う。

セキュリティ要素と優先順位

- **機密性、完全性、可用性**
  - セキュリティ要素として機密性、完全性、可用性を考慮する必要がある。
  - 日本での進展状況と優先すべき要素について議論。

OT の重要性

- **アップタイムの重要性**
  - OT 環境ではアップタイムが重要。
  - 完全性と機密性も関わってくる。

スレッドモデルと信頼度

- **スレッドモデルの変化**
  - スレッドモデルが過去数年間で大きく変わってきている。
  - パラダイムシフトが起きており、新たな要件が必要に

The role of identity verification in IoT security Identity verification is essential in IoT security to ensure that commands are coming from trusted sources and to prevent unauthorized access. • **Keypoints** ○ Importance of identity verification ○ Ensuring trusted command sources ○ Preventing unauthorized access **The need for continuous scanning and reporting of IoT vulnerabilities** Continuous scanning and reporting of IoT vulnerabilities are necessary to identify and address security issues promptly, ensuring the safety and reliability of IoT systems. • **Keypoints** ○ Importance of continuous scanning ○ Reporting of IoT vulnerabilities ○ Ensuring safety and reliability **Zero Trust Principle** A cybersecurity concept where no entity inside or outside the network is trusted by default. • **Keypoints** ○ Often misunderstood ○ Implemented by taking down security barriers ○ Should mean putting more security barriers in place **Local Device Security** Ensuring that local devices do not perform unauthorized or harmful actions. • **Keypoints** ○ More local compute ○ More local SOC functionality ○ More observability and traceability ○ Ability to audit commands **Understanding Cybersecurity** The importance of individuals learning about cybersecurity to protect themselves and influence government policies. • **Keypoints** ○ Fundamental knowledge for functioning	なる。 **エッジデバイスとロボット** • **新たな要件** ○ エッジデバイスやロボットの導入に

members of society ○ Ability to ask for better security from products and lawmakers **Role of Government in Cybersecurity** The government's responsibility to create legislation that mandates security standards. • **Keypoints** ○ Consumers should ask lawmakers for better security ○ Legislation can make the industry implement security **Identity Access Management** A framework for ensuring that the right individuals access the right resources at the right times for the right reasons. **Threat Analysis and Risk Assessment** Processes to identify and evaluate potential threats and risks to cybersecurity. • **Keypoints** ○ Should be actively audited and maintained **Ethical Use of AI in Cybersecurity** Using artificial intelligence responsibly to automate cybersecurity tasks. • **Keypoints** ○ Automate tasks in a safe way **Regulation and Security Standards in the Japanese Industry** The need for cohesive security standards in the Japanese industry. • **Keypoints** ○ More regulation ○ Improved security standards **Assignments & Suggestions**	

2.10 D2-S8 Day 2 Closing

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）
Overview This document summarizes the discussions and outcomes of a recent meeting held on October 31, 2024. Key topics include the expansion of the	**概要** 本書は、2024 年 10 月 31 日に開催された最近の会議の議論と結果をまとめたものである。主なトピックは、新たな大学メンバーによるコンソーシアムの拡大、研究と関与活動、経済

consortium with new university members, research and engagement activities, economic security, and critical infrastructure challenges. The document also highlights academic engagement, research initiatives, and future directions in cybersecurity. Action items are outlined for further collaboration and engagement. **New Members and Global Collaboration** • Five new universities joined in the last year: Virginia Tech, University of Surrey, University of Porto, University of Indonesia, and Tallinn University of Technology. ○ Representatives include Lewis from Virginia Tech and Rolando from the University of Porto. Mohamed Salman from the University of Indonesia is attending the conference. • The consortium now includes 17 universities worldwide. • 41 experts and fellows are available to form TIGER teams to tackle specific cybersecurity challenges. • Expectation of growth in the number of expert fellows in the coming years. **Research and Engagement Activities** • Active research agenda with quarterly seminars. • Publication of notes highlighting emerging research challenges. • Capture the Flag activity named "Country to Country" to engage young cybersecurity professionals, hosted by David Luzzi at Northeastern University next year. • Emphasis on a triple helix partnership between government, industry, and academia. • Importance of academia in public-private partnerships, especially in AI and quantum research.	安全保障、重要インフラの課題などである。また、この文書では、サイバーセキュリティにおける学術的関与、研究イニシアティブ、将来の方向性についても強調している。さらなる協力と関与のための行動項目が概説されている。 **新メンバーとグローバル・コラボレーション** • 昨年は新たに 5 大学が加盟した：バージニア工科大学、サリー大学、ポルト大学、インドネシア大学、タリン工科大学である。 ○ 代表にはバージニア工科大のルイスとポルト大学のロランドがいる。インドネシア大学からはモハメド・サルマンが会議に出席している。 • このコンソーシアムには現在、世界の 17 大学が参加している。 • 41 人の専門家とフェローが TIGER チームを結成し、特定のサイバーセキュリティの課題に取り組むことができる。 • 今後数年間、専門家フェローの増加に期待。 **リサーチとエンゲージメント活動** • 四半期ごとにセミナーを開催し、活発な研究活動を展開。 • 新たな研究課題に焦点を当てたノートの出版。 • 来年、ノースイースタン大学でデビッド・ルッツィが主催する、若いサイバーセキュリティ専門家の参加を促す「Capture the Flag」活動「Country to Country」。 • 産官学の三位一体のパートナーシップを重視。 • 官民パートナーシップにおけるアカデミアの重要性、特に AI と量子研究において。 • サイバーセキュリティはボーダーレスであり、国際的な協力が必要である。 **経済安全保障と重要インフラ** • 国家に支援された行為者や犯罪者からの脅威の増大。 • サプライチェーンにおける脆弱性と、特に電力系統における連鎖的障害のリスク。 • 例 2019 年に英国で発生した停電は、1 時間あたり数千万ポンド（数億円）のコストがかかった。 • 英国は最近、重要国家インフラリストにデータセンターを追加した。 • 政府機関はデータセンター事業者への支援と助言を強化する。 • 金融やサイバーフィジカルシステムを含む重要インフラ

- Cybersecurity is borderless, necessitating international collaboration.

Economic Security and Critical Infrastructure

- Increasing threats from state-sponsored actors and criminals.
- Vulnerabilities in supply chains and risk of cascading failures, especially in power systems.
- Example: A power outage in the UK in 2019 cost tens of millions of pounds per hour.
- UK recently added data centers to its critical national infrastructure list.
- Government agencies to provide more support and advice to data center operators.
- Emphasis on high cybersecurity standards for critical infrastructure, including finance and cyber-physical systems.

Academic Engagement and Research Initiatives

- National Cyber Security Centre (NCSC) published a problem book for cyber-physical systems.
- Engagement of universities to address key challenges in cybersecurity.
- Network of 25 UK universities focusing on cybersecurity for critical infrastructure.
- Established in 2014, directed by the speaker since its inception.

Challenges and Future Directions

- Legacy systems like MRI machines using outdated operating systems pose security risks.
- Exploration of AI for intrusion detection and addressing security concerns in AI systems.
- Importance of building resilience across interconnected systems.
- UK initiatives on new computer architectures and semiconductor devices

に対する高いサイバーセキュリティ基準を重視する。

アカデミック・エンゲージメントと研究への取り組み

- 米国サイバーセキュリティセンター（NCSC）がサイバーフィジカルシステムの問題集を発表。
- サイバーセキュリティにおける重要な課題に取り組むための大学の関与。
- 重要インフラのサイバーセキュリティに焦点を当てた英国 25 大学のネットワーク。
- 2014 年設立、設立当初から講演者が指揮。

課題と今後の方向性

- 旧式のオペレーティングシステムを使用する MRI のようなレガシーシステムは、セキュリティリスクをもたらす。
- 侵入検知のための AI を探求し、AI システムにおけるセキュリティ上の懸念に対処する。
- 相互に関連するシステム全体でレジリエンスを構築することの重要性。
- セキュリティ強化のための新しいコンピュータ・アーキテクチャと半導体デバイスに関する英国の取り組み。

アクション・アイテム

[ ] 新しい大学のメンバーとの協力の機会を探る。

[ ] ノースイースタン大学の「キャプチャーザフラッグ」活動に参加する。

[ ] サイバーフィジカルシステムに関する NCSC の問題集を復習する。

[ ] セキュリティ向上のための新しいコンピュータ・アーキテクチャに関する英国のイニシアチブを調査する。

to enhance security. **Action Items** [ ] Explore opportunities for collaboration with new university members. [ ] Engage with the Capture the Flag activity at Northeastern University. [ ] Review the NCSC problem book for cyber-physical systems. [ ] Investigate UK initiatives on new computer architectures for security improvements.	

3 DAY 3: November 1 | West School Building 1F West Hall

3.1 D3-S1-1 Opening

Satoru Tezuka	手塚 悟
Cybersecurity, Cyberspace, National Security **Theme** This speech emphasizes the critical importance of digital cybersecurity for national, economic, and societal security. It highlights the borderless nature of cyberspace and its role as an essential infrastructure in the information age. The speech also draws parallels between cybersecurity and the human nervous system, noting that minor issues can lead to significant problems. Additionally, it addresses the intersection of global warming, environmental issues, and cyberspace challenges, and underscores the necessity of building digital infrastructure as a default for security. **Takeaways** 1. Digital cybersecurity is crucial for national security, economic security, and societal security. 2. Cyberspace is a borderless and indispensable infrastructure in today's information age. 3. Cybersecurity can be compared to the nervous system in the human body, where even minor issues can cause significant problems. 4. Global warming and environmental issues are both physical and cyberspace challenges. 5. Building digital infrastructure as a default is essential for national, economic, and societal security. 6. The symposium includes speeches and presentations from high-level officials on cybersecurity efforts. **Highlights** • "Cyberspace is one of the greatest	サイバーセキュリティ，サイバースペース，国家安全保障 **テーマ** この講演では、国家、経済、社会の安全保障にとってデジタル・サイバーセキュリティが極めて重要であることを強調する。サイバースペースのボーダーレスな性質と、情報化時代に不可欠なインフラとしての役割を強調する。また、些細な問題が重大な問題につながる可能性があることを指摘し、サイバーセキュリティと人間の神経系との類似性を示す。さらに、地球温暖化、環境問題、サイバースペースの課題が交差していることを取り上げ、安全保障のデフォルトとしてデジタルインフラを構築する必要性を強調する。 **収穫** 1. デジタル・サイバーセキュリティは、国家安全保障、経済安全保障、社会安全保障にとって極めて重要である。 2. サイバースペースはボーダーレスであり、今日の情報化時代には不可欠なインフラである。 3. サイバーセキュリティは人体の神経系に例えることができ、些細な問題でも重大な問題を引き起こす可能性がある。 4. 地球温暖化や環境問題は、物理的な課題であると同時にサイバースペース上の課題でもある。 5. 国家、経済、社会の安全保障にとって、デフォルトとしてのデジタル・インフラの構築は不可欠である。 6. シンポジウムでは、サイバーセキュリティへの取り組みに関する高官たちのスピーチやプレゼンテーションが行われる。 **ハイライト** • 「サイバースペースは人類にとって最大の挑戦のひとつである。 **チャプター＆トピックス** **デジタル・サイバーセキュリティ** 国家、経済、社会の安全保障を確保するために、デジタルインフラと情報をサイバー脅威から保護すること。 • **キーポイント** ○ 国家安全保障には政府の保護が含まれる。 ○ 経済安全保障には重要インフラの保護が含まれ

challenges for mankind." **Chapters & Topics** **Digital Cybersecurity** The protection of digital infrastructure and information from cyber threats to ensure national, economic, and societal security. • **Keypoints** ○ National security involves government protection. ○ Economic security involves critical infrastructure protection. ○ Societal security involves private sector business and citizen protection. **Cyberspace** A borderless and essential infrastructure for all fields in today's information age. • **Keypoints** ○ Comparable to the nervous system in the human body. ○ Minor issues can cause significant problems. ○ Global warming and environmental issues are also cyberspace challenges. **Assignments & Suggestions**	る。 ○ 社会保障には、民間企業や市民の保護が含まれる。 **サイバースペース** 今日の情報化時代において、あらゆる分野に不可欠なボーダーレスなインフラ。 • **キーポイント** ○ 人体の神経系に似ている。 ○ 些細な問題が大きな問題を引き起こすこともある。 ○ 地球温暖化や環境問題は、サイバースペースの課題でもある。 **課題と提案**

3.2 D3-S1-2 Opening

Barbara Grewe	バーバラ・グルーイ
Cybersecurity, National Security, Economic Security **Theme** This speech emphasizes the critical role of cybersecurity in national and economic security. Key takeaways include the necessity of a whole-of-government approach, the importance of coordination and information sharing among government entities, and the need for collaboration with the private sector to enhance cybersecurity efforts. **Takeaways** 1. Cybersecurity is essential for national security. 2. Economic security is dependent on	サイバーセキュリティ，国家安全保障，経済安全保障 **テーマ** 本講演では、国家と経済の安全保障におけるサイバーセキュリティの重要な役割を強調する。政府全体のアプローチの必要性、政府機関間の調整と情報共有の重要性、サイバーセキュリティの取り組みを強化するための民間セクターとの協力の必要性などが主な要点である。 **収穫** 1. サイバーセキュリティは国家安全保障にとって不可欠である。 2. 経済の安全保障は、効果的なサイバーセキュリティに依存している。 3. 脆弱なサイバー防衛は、国家や経済の安全保障上の脆弱性を生み出しかねない。 4. サイバーセキュリティは政府全体の取り組みであるべき

effective cybersecurity.

3. Weak cyber defenses can create national and economic security vulnerabilities.
4. Cybersecurity should be a whole-of-government effort.
5. Government efforts are often fragmented and siloed.
6. Coordination among government elements is crucial to address cyber threats.
7. Information sharing across government entities is important.
8. Incident response plans should ensure information sharing.
9. Collaboration with the private sector is necessary.

Highlights

- "Cybersecurity must be front and center, when deciding how to build national and economic security strategies and implementing them."

Chapters & Topics

Cybersecurity and National Security

The relationship between cybersecurity and national security, emphasizing the importance of effective cybersecurity measures.

- **Keypoints**
  - Cybersecurity is crucial for maintaining national security.
  - Weak cyber defenses can lead to significant vulnerabilities.

Cybersecurity and Economic Security

The dependency of economic security on effective cybersecurity measures.

- **Keypoints**
  - Economic security is closely tied to cybersecurity.
  - Inadequate cybersecurity can have catastrophic economic consequences.

Whole-of-Government Approach

The necessity for a coordinated government effort in cybersecurity.

だ。

5. 政府の取り組みは断片的でサイロ化されていることが多い。
6. サイバー脅威に対処するためには、政府間の連携が不可欠である。
7. 政府間の情報共有は重要だ。
8. インシデント対応計画は、情報共有を徹底すべきである。
9. 民間企業との協力が必要だ。

ハイライト

- 「サイバーセキュリティは、国家と経済の安全保障戦略をどのように構築するかを決定し、それを実施する際に、最前線に位置づけられなければならない。

チャプター＆トピックス

サイバーセキュリティと国家安全保障

サイバーセキュリティと国家安全保障の関係、効果的なサイバーセキュリティ対策の重要性を強調。

- **キーポイント**
  - サイバーセキュリティは国家安全保障を維持するために極めて重要である。
  - 脆弱なサイバー防御は重大な脆弱性につながる可能性がある。

サイバーセキュリティと経済安全保障

経済安全保障が効果的なサイバーセキュリティ対策に依存していること。

- **キーポイント**
  - 経済の安全保障はサイバーセキュリティと密接に結びついている。
  - 不十分なサイバーセキュリティは、壊滅的な経済的結果をもたらす可能性がある。

政府全体のアプローチ

サイバーセキュリティにおける政府の協調的取り組みの必要性。

- **キーポイント**
  - サイバーセキュリティは 1 つや 2 つの省庁だけの責任であってはならない。
  - 政府の統一的なアプローチが不可欠だ。

調整と情報共有

政府機関間の調整と情報共有の重要性。

- **キーポイント**
  - 政府の取り組みは断片的であることが多い。
  - サイバー脅威に対処するためには、連携強化が必要

• **Keypoints** ○ Cybersecurity should not be the responsibility of just one or two ministries. ○ A unified government approach is essential. **Coordination and Information Sharing** The importance of coordination and information sharing among government entities. • **Keypoints** ○ Government efforts are often fragmented. ○ Improved coordination is necessary to address cyber threats. ○ Information sharing helps prevent and respond to cyber attacks. **Collaboration with Private Sector** The need for government entities to work with the private sector in cybersecurity. • **Keypoints** ○ Collaboration with the private sector enhances cybersecurity efforts. **Assignments & Suggestions**	である。 ○ 情報共有はサイバー攻撃の防止と対応に役立つ。 **民間セクターとの協力** サイバーセキュリティにおいて政府機関が民間セクターと協力する必要性。 • **キーポイント** ○ 民間部門との協力はサイバーセキュリティの取り組みを強化する。 **課題と提案**

3.3 D3-S9 Speech

Nobukatsu Kanehara (Executive Director, Sasakawa Peace Foundation)	兼原 信克（笹川平和財団 常任理事）
Overview This speech provides a comprehensive analysis of Japan's position in cyberspace, its historical context in intelligence, current cyber capabilities, structural and organizational reforms, and future directions. It highlights Japan's need to enhance its cyber forces, improve coordination and intelligence gathering, and prepare for potential conflicts, particularly involving Taiwan. The document also outlines specific action items to address these challenges. **Characteristics of Cyberspace** • Cyberspace is a man-made space, distinct from physical space. • In cyberspace, there is no concept of time	**概要** 本書は、サイバースペースにおける日本の位置づけ、インテリジェンスにおける歴史的背景、現在のサイバー能力、構造的・組織的改革、将来の方向性について包括的な分析を提供している。本書は、日本がサイバー戦力を強化し、連携と情報収集を改善し、特に台湾を含む潜在的な紛争に備える必要性を強調している。また、これらの課題に対処するための具体的な行動項目についても概説している。 **サイバースペースの特徴** • サイバースペースは人工的な空間であり、物理的な空間とは異なる。 • サイバースペースでは、時間や距離の概念はない。 ○ 「隣は平壌。隣はモスクワ。隣は北京だ。」 **インテリジェンスにおける日本の歴史的背景** • 日本は冷戦時代、シギント（信号諜報）に秀でて

or distance. ○ "Next door, it's Pyongyang. Next door, it's Moscow. Next door, it's Beijing." **Japan's Historical Context in Intelligence** • Japan excelled in SIGINT (Signals Intelligence) during the Cold War. ○ Example: Japan intercepted Soviet communications during the KAL airplane incident. • Japan has lagged in cyber intelligence since the advent of the digital age. ○ Example: During the Afghan war, Japan's Navy used outdated communication methods. **International Comparison** • IISS classified Japan's cyber capabilities as Class C, alongside North Korea. ○ Class A: United States ○ Class B: UK, France, Germany, Russia, China • Japan has the technology and talent but lacks government policy. **Constitutional and Legal Challenges** • Article 21 of the Japanese Constitution guarantees freedom of communications. • Misinterpretation has hindered cyber intelligence efforts. ○ Example: Government initially denied cyber intelligence, citing constitutional protections for foreign entities. **Government Initiatives and Required Changes** • Recent legal interpretations now allow for some limitations on communication freedom for national security. • Japan needs to: ○ Integrate supercomputers, engineers, and hackers into a cohesive cyber army. ○ Establish a command line within the government for cyber operations. ○ Create a centralized digital information system for government data.	いた。 ○ 例:日本は KAL 機事件でソ連の通信を傍受した。 • 日本はデジタル時代の到来以来、サイバーインテリジェンスにおいて遅れをとってきた。 ○ 例:アフガン戦争中、日本海軍は時代遅れの通信手段を使っていた。 **国際比較** • IISS は日本のサイバー能力を北朝鮮と並ぶ C クラスに分類した。 ○ クラス A：アメリカ ○ クラス B：英国、フランス、ドイツ、ロシア、中国 • 日本には技術も才能もあるが、政府の政策が欠けている。 **憲法と法的課題** • 日本国憲法第 21 条は、通信の自由を保障している。 • 誤った解釈がサイバー諜報活動の妨げになっている。 ○ 例:政府は当初、外国団体に対する憲法上の保護を理由にサイバー情報を否定していた。 **政府の取り組みと求められる変化** • 最近の法解釈では、国家安全保障のために通信の自由を制限することが認められるようになった。 • 日本はそうする必要がある： ○ スーパーコンピューター、エンジニア、ハッカーを統合し、結束力のあるサイバー軍にする。 ○ 政府内にサイバー作戦の指揮系統を確立する。 ○ 政府データの集中デジタル情報システムを構築する。 **指揮統制** • 首相はサイバー作戦を指揮する権限を持たなければならない。 • 首相官邸に軍事、政府、重要インフラを担当するサイバー・ディレクターを設置する。 **サイバー戦力の強化** • 現在のサイバー軍は不十分だ（900 人しかいない）。 • 警察機関もサイバー能力を高める必要がある（現在 500 人）。 **調整と情報収集** • 日本には情報を収集し分析する統一されたシステムがない。

Command and Control

- Prime Minister must have the authority to direct cyber operations.
- Establish a Cyber Director in the Prime Minister's office responsible for military, government, and critical infrastructure.

Enhancing Cyber Forces

- Current cyber army is insufficient (only 900 personnel).
- Police agencies also need to increase their cyber capabilities (currently 500 personnel).

Coordination and Intelligence Gathering

- Japan lacks a unified system for gathering and analyzing intelligence.
  - Example: Silo (Cabinet Intelligence Office) focuses mainly on counterintelligence.
- Need for a comprehensive system to collect and analyze enemy information, including cyber intelligence.

Offensive Capabilities

- Japan is acquiring offensive capabilities for the first time since 1945.
  - Example: Introduction of Tomahawk missiles.
- Need to develop systems to gather and analyze information to effectively use these capabilities.

Taiwan Contingency

- Japan must prepare for potential conflicts involving Taiwan.
- Need for a unified intelligence evaluation system to coordinate with international allies, particularly the United States.

Action Items

- Integrate supercomputers, engineers, and hackers into a cohesive cyber army.
- Establish a command line within the government for cyber operations.
- Create a centralized digital information system for government data.
- Increase the number of personnel in the

  - 例:サイロ（内閣情報室）は主に防諜に重点を置いている。
- サイバー情報を含む敵の情報を収集・分析する包括的なシステムの必要性。

攻撃能力

- 日本は 1945 年以来初めて攻撃能力を獲得している。
  - 例:トマホーク・ミサイルの導入。
- これらの能力を効果的に活用するためには、情報を収集・分析するシステムを開発する必要がある。

台湾有事

- 日本は台湾との潜在的な紛争に備えなければならない。
- 国際的な同盟国、特に米国と協調するための統一的な情報評価システムの必要性。

アクション・アイテム

- スーパーコンピューター、エンジニア、ハッカーを統合し、結束力のあるサイバー軍にする。
- 政府内にサイバー作戦の指揮系統を確立する。
- 政府データの集中デジタル情報システムを構築する。
- サイバー軍と警察機関の人員を増やす。
- サイバー情報を含む敵の情報を収集・分析する包括的なシステムを開発する。
- 首相官邸にサイバー・ディレクターを設置する。
- 統一的な情報評価システムを開発し、台湾との潜在的な紛争に備える。

cyber army and police agencies. • Develop a comprehensive system for gathering and analyzing enemy information, including cyber intelligence. • Establish a Cyber Director in the Prime Minister's office. • Prepare for potential conflicts involving Taiwan by developing a unified intelligence evaluation system.	

3.4 D3-S2-1 Speeches from Japanese Government

NAKAMIZO Kazutaka (Deputy Director- General, National center of Incident readiness and Strategy for Cybersecurity Cabinet Secretariat（NISC）)	中溝 和孝 (内閣官房 内閣サイバーセキュリティセンター（NISC） 副センター長 内閣審議官)
Cyber Security, Ransomware, Active Cyber Defense **Theme** This lecture discussed the current state of cybersecurity in Japan and countermeasures: NISC's mission, the increase in cyber attacks, the number of ransomware attacks, the diversification of cyber attacks, attacks by state-sponsored actors, the increase in zero-day attacks, and the strengthening of measures for government agencies and critical infrastructure, The main topics included the implementation of active cyber defenses and enhanced response to supply chain risks. **Main point** 1. NISC's two missions 2. Cyber Security Strategic Headquarters 3. Increased Cyber Attacks in Japan 4. Number of ransomware cases 5. Diversification of cyber attacks 6. Increased attacks by state-sponsored actors 7. Increase in zero-day attacks 8. Strengthen measures for government agencies and critical infrastructure 9. Implementing Active Cyber Defense 10. Strengthening Responses to Supply Chain	サイバーセキュリティ，ランサムウェア，アクティブサイバーディフェンス **テーマ** この講演では、日本のサイバーセキュリティの現状と対策について議論しました。NISC のミッション、サイバー攻撃の増加、ランサムウェアの件数、サイバーアタックの多様化、国家支援アクターによる攻撃、ゼロデイ攻撃の増加、政府機関や重要インフラの対策強化、アクティブサイバーディフェンスの導入、サプライチェーンリスクへの対応強化などが主なトピックです。 **要点** 1. NISC の 2 つのミッション 2. サイバーセキュリティストラテジックヘッドクォーター 3. 日本のサイバー攻撃の増加 4. ランサムウェアの件数 5. サイバーアタックの多様化 6. 国家支援アクターによる攻撃の増加 7. ゼロデイ攻撃の増加 8. 政府機関や重要インフラの対策強化 9. アクティブサイバーディフェンスの導入 10. サプライチェーンリスクへの対応強化 **章とトピック** **NISC のミッション** NISC はサイバーセキュリティのコーディネーターとして、日本のサイバーセキュリティストラテジックヘッドクォーターをコントロールタワーとして機能させる。 • **要点** ○ サイバーセキュリティのコーディネーターとしての役割

Risks **Chapters and Topics** **Mission of NISC** NISC will serve as the coordinator of cybersecurity, with Japan's Cyber Security Strategic Headquarters acting as the control tower. • **Main point** ○ Role as coordinator of cybersecurity ○ Functions of the Cyber Security Strategic Headquarters **Current Status of Cyber Attacks** The number of cyber attacks in Japan has been increasing, with the number of ransomware cases in particular remaining flat at a high level. • **Main point** ○ Increasing trend of cyber attacks ○ Increase in the number of ransomware cases **Diversification of cyber attacks** Cyberattack methods are becoming more diverse, with an increase in attacks by state-sponsored actors and zero-day attacks. • **Main point** ○ Attacks by state-sponsored actors ○ Increase in zero-day attacks **Active cyber defense** The goal is to quickly compile legislation for the introduction of active cyber defense. • **Main point** ○ Implementing Active Cyber Defense ○ Early compilation of the bill **Strengthening Supply Chain Risk** Enhance supply chain risk by embodying secure-by-design and secure-by-default. • **Main point** ○ Embodying Secure-by-Design and Secure-by-Default ○ Strengthening Supply Chain Risk **Strengthening International Cooperation** Strengthen cooperation with like-minded countries to ensure the security of cyberspace.	○ サイバーセキュリティストラテジックヘッドクォーターの機能 **サイバー攻撃の現状** 日本におけるサイバー攻撃の数が増加しており、特にランサムウェアの件数が高い水準で横ばいとなっている。 • **要点** ○ サイバー攻撃の増加傾向 ○ ランサムウェアの件数の増加 **サイバーアタックの多様化** サイバーアタックの手法が多様化しており、国家支援アクターによる攻撃やゼロデイ攻撃が増加している。 • **要点** ○ 国家支援アクターによる攻撃 ○ ゼロデイ攻撃の増加 **アクティブサイバーディフェンス** アクティブサイバーディフェンスの導入に向けた法案の早期取りまとめを目指している。 • **要点** ○ アクティブサイバーディフェンスの導入 ○ 法案の早期取りまとめ **サプライチェーンリスクの強化** セキュアバイデザイン、セキュアバイデフォルトの具体化を進め、サプライチェーンリスクの強化を図る。 • **要点** ○ セキュアバイデザイン、セキュアバイデフォルトの具体化 ○ サプライチェーンリスクの強化 **国際協力の強化** 同志国との連携を強化し、サイバー空間の安全を確保する。 • **要点** ○ 国際協力の強化 ○ 共同文書の作成 **宿題と提案**

• **Main point** ○ Strengthening International Cooperation ○ Joint Documentation **Homework and Suggestions**	

3.5 D3-S2-2 Speeches from Japanese Government

SAITA Yukio (Deputy Director-General, Foreign Policy Bureau, Ministry of Foreign Affairs)	斉田 幸雄 (外務省 総合外交政策局参事官)
Overview This document is a meeting memorandum prepared on November 1, 2024 on the Ministry of Foreign Affairs' efforts regarding cybersecurity. Its content includes a detailed description of the characteristics and current state of cyberspace, the Ministry of Foreign Affairs' efforts, and the importance of public-private cooperation, as well as related action items. **Ministry of Foreign Affairs of Japan on Cyber Security** **Characteristics and Current State of Cyberspace** • **Cyberspace as Public Space** ○ Cyberspace is a public space in which all citizens participate, and risks exist in exchange for convenience. ○ Cyber attackers are becoming more sophisticated in their methods. • **Major Cyber Attack Countries** ○ **China**: to ingest information on military-related companies and companies with advanced technology. ○ **Russia**: to achieve its military and political objectives. ○ **North Korea**: To achieve political goals and obtain foreign currency, **North Korea** ingests crypto assets to obtain funds to develop ballistic missiles. • **Cyber Attacks Against Ukraine** ○ In the wake of the Russian invasion of Ukraine, cyberattacks have been deployed against government agencies, critical	**Overview** この講演は、2024 年 11 月 1 日に作成されたサイバーセキュリティに関する外務省の取り組みについての講演メモです。内容は、サイバー空間の特徴と現状、外務省の取り組み、官民協力の重要性に関する詳細な説明と、それに関連するアクションアイテムが含まれています。 **サイバーセキュリティに関する外務省の取り組み** **サイバー空間の特徴と現状** • **公共空間としてのサイバー空間** ○ サイバー空間は全ての国民が参加する公共空間であり、便利さと引き換えにリスクも存在する。 ○ サイバー攻撃者の手法が巧妙化している。 • **主要なサイバー攻撃国の動向** ○ **中国**：軍事関連企業や先端技術保有企業の情報摂取を目的とする。 ○ **ロシア**：軍事的及び政治的目的の達成を目指す。 ○ **北朝鮮**：政治目標の達成や外貨獲得を目的とし、暗号資産を摂取して弾道ミサイルの開発資金を入手。 • **ウクライナに対するサイバー攻撃** ○ ロシアの侵攻を受けたウクライナでは、政府機関や重要インフラ、民間企業に対するサイバー攻撃が展開されている。 ○ ハイブリッド戦（物理的な武力攻撃とサイバー攻撃の組み合わせ）が見られる。 **外務省の取り組み** **コストの負荷** • **攻撃者に対するコストの負荷** ○ 将来の攻撃への抑止効果を期待。 ○ サイバー攻撃の実態を目に見える形で明らかにすることが重要。 ○ 企業や国民の認識を高める。

infrastructure, and private companies.

- Hybrid warfare (a combination of physical armed attacks and cyber attacks) is seen.

Initiatives by the Ministry of Foreign Affairs

Cost Burden

- **Cost burden on attackers**
  - Expected to have a deterrent effect on future attacks.
  - It is important to make the reality of cyber attacks visible.
  - Raise awareness among businesses and the public.
  - Connect to the formation of rules in the international community.
  - Show solidarity with the affected countries.

Rule of law

- **Application of International Law and the State of the Rules**
  - Application of existing international law is important.
  - Through discussions at the United Nations, the application of international law in cyberspace was confirmed.
  - It is important to create and implement 11 codes of conduct.
- **International Community Relations**
  - Cooperation of the international community is extremely important.
  - Strengthen cooperation with countries that share our values.
  - Need to spread values to developing countries and the Global South.

Capacity Building Support

- **Risk mitigation from a regional perspective**
  - Build the capacity of neighboring countries, especially ASEAN and Pacific countries.
  - Capacity building support was provided through a center in Bangkok.
  - The World Bank's new housing equipment

- 国際社会でのルール形成に繋げる。
- 被害を受けた国に対する連帯を示す。

法の支配

- **国際法の適用とルールの在り方**
  - 既存の国際法の適用が重要。
  - 国連での議論を通じて、サイバー空間における国際法の適用を確認。
  - 11 の行動規範を作成し、実行に移すことが重要。
- **国際社会の連携**
  - 国際社会の連携が極めて重要。
  - 価値観を共有する国々との協力を強化。
  - 途上国やグローバルサウスへの価値観の広めが必要。

能力構築支援

- **地域的な観点からのリスク軽減**
  - 近隣国（特に ASEAN、太平洋諸国）の能力を高める。
  - バンコクのセンターを活用し、能力構築支援を実施。
  - 世界銀行の新宅機器を活用し、協力を進める。

サイバーダイアログ

- **多国間の意見交換**
  - 多くの国と意見交換を行い、サイバー空間の能力を高める。
  - 国際社会や地域での協力を進める。

官民協力の重要性

- **官民協力の推進**
  - サイバー空間の取り組みには民間企業との協力が不可欠。
  - 外務省としても官民協力を進めていく。

Action Items

[ ] 価値観を共有する国々との協力を強化する。

[ ] バンコクのセンターを活用し、能力構築支援を実施する。

[ ] 世界銀行の新宅機器を活用し、協力を進める。

[ ] 多くの国と意見交換を行い、サイバー空間の能力を高める。

will be used to promote cooperation. **Cyberdialogue** • **Multilateral exchange of ideas** ○ Exchange views with many countries to enhance cyberspace capabilities. ○ Promote cooperation in the international community and in the region. **Importance of Public-Private Cooperation** • **Promotion of public-private cooperation** ○ Cooperation with the private sector is essential for cyberspace initiatives. ○ The Ministry of Foreign Affairs will also promote public-private cooperation. **Action Items** [ ] Strengthen cooperation with countries that share our values. [ ] Utilize the center in Bangkok to provide capacity building support. [ ] Utilize the World Bank's new housing equipment to promote cooperation. [ ] Exchange views with many countries to enhance cyberspace capabilities.	

3.6 D3-S2-3 Speeches from Japanese Government

KEGOYA Masanori (Deputy Director General for Cyber Security, Ministry of Defense, Japan)	家護谷 昌徳 （防衛省 大臣官房 サイバーセキュリティ・情報化審議官）
Cyber Security, Ministry of Defense, Self Defense Forces **Theme** This speech detailed the cybersecurity measures of the Ministry of Defense SDF. The main topics covered included attacks on critical infrastructure and their impact, introduction of the Ministry of Defense version of RMF, the concept and implementation of Zero Trust, defense industry cybersecurity standards, personnel training and career paths, expansion of specialized cyber units, the fixed-term SDF officer system, reserve SDF officers specialized in cyber, and cyber contests. The main topics covered included.	サイバーセキュリティ，防衛省，自衛隊 **テーマ** この講演では、防衛省自衛隊のサイバーセキュリティ施策について詳述されました。重要インフラへの攻撃とその影響、防衛省版 RMF の導入、ゼロトラストの概念と実施、防衛産業のサイバーセキュリティ基準、人材育成とキャリアパス、サイバー専門部隊の拡充、任期付き自衛官制度、サイバー専門の予備自衛官、サイバーコンテストの実施などが主なトピックとして取り上げられました。 **要点** 1. 防衛省自衛隊のサイバーセキュリティ施策 2. 重要インフラへの攻撃とその影響 3. 防衛省版 RMF の導入 4. ゼロトラストの概念と実施

Main point

1. Ministry of Defense Self-Defense Forces Cybersecurity Policies
2. Attacks on critical infrastructure and their impact
3. Introduction of Ministry of Defense version of RMF
4. Zero Trust Concept and Implementation
5. Defense Industry Cybersecurity Standards
6. Human Resource Development and Career Paths
7. Expansion of dedicated cyber unit
8. fixed-term self-defense system
9. Reserve Self-Defense Officer specializing in cyber
10. Conducting cyber contests

Chapters and Topics

Ministry of Defense Self-Defense Forces Cybersecurity Policies

Details on cybersecurity measures undertaken by the Self-Defense Forces of the Ministry of Defense.

- **Main point**
  - Recognition and Efforts by the Ministry of Defense
  - Increased attacks on critical infrastructure
  - The role of critical infrastructure in the execution of the SDF's mission

Introduction of Ministry of Defense version of RMF

Introduction of the Ministry of Defense version of the RMF, which is customized by the Ministry of Defense based on the Japanese legal system and Ministry of Defense regulations, while referring to the U.S. government's RMF.

- **Main point**
  - Information security risk management measures
  - Protection of facility infrastructure and weapons systems as well as regular IT

5. 防衛産業のサイバーセキュリティ基準
6. 人材育成とキャリアパス
7. サイバー専門部隊の拡充
8. 任期付き自衛官制度
9. サイバー専門の予備自衛官
10. サイバーコンテストの実施

章とトピック

防衛省自衛隊のサイバーセキュリティ施策

防衛省自衛隊が取り組むサイバーセキュリティ施策についての詳細。

- **要点**
  - 防衛省の認識と取り組み
  - 重要インフラへの攻撃の増加
  - 自衛隊の任務遂行における重要インフラの役割

防衛省版 RMF の導入

防衛省が米国政府の RMF を参考にしつつ、日本の法令体系や防衛省の規則に基づいてカスタマイズした防衛省版 RMF の導入。

- **要点**
  - 情報セキュリティリスクの管理方策
  - 通常の IT 資産だけでなく、施設インフラや武器システムの保護

ゼロトラストの概念と実施

ゼロトラストの概念に基づき、内外からのすべてのアクセスを動的に検証・制御する体制の構築。

- **要点**
  - 境界型防御ではなく、内部侵入を前提としたレジリエンシーの強化
  - 迅速な検知と対処

防衛産業のサイバーセキュリティ基準

防衛産業のサイバーセキュリティ基準の整備とその適用に関する措置。

- **要点**
  - NIST SP-800-171 と同レベルの基準
  - CUI 情報の保護
  - 経費の負担措置

人材育成とキャリアパス

防衛省自衛隊におけるサイバー人材の育成体制とキャリアパスの構築。

- **要点**
  - 各学校や部外力を活用した教育
  - OJT の積み重ね

assets **Zero Trust Concept and Implementation** Establish a system to dynamically verify and control all access from inside and outside based on the zero-trust concept. • **Main point** ○ Strengthen resiliency based on internal penetration rather than perimeter-based defenses ○ Rapid detection and response **Defense Industry Cybersecurity Standards** Measures related to the development and application of cybersecurity standards for the defense industry. • **Main point** ○ Same level of standards as NIST SP-800-171 ○ Protection of CUI Information ○ Cost-sharing measures **Human Resource Development and Career Paths** Establishment of a cyber personnel development system and career path in the Self-Defense Forces of the Ministry of Defense. • **Main point** ○ Education through the use of each school and extracurricular forces ○ Accumulation of OJT ○ GSDF's Systems and Communications Cyber School ○ Cyber education in higher secondary schools **Expansion of dedicated cyber unit** Plans to expand the number of specialized cyber units to 4,000 by FY2027. • **Main point** ○ Train 20,000 people with a certain level of cyber knowledge ○ Introduction of a new self-defense system ○ Implementation of the Ministry of Defense Cyber Contest	○ 陸上自衛隊のシステム通信サイバー学校 ○ 高等高科学校でのサイバー教育 **サイバー専門部隊の拡充** 2027 年度を目標にサイバー専門部隊を 4,000 人に拡充する計画。 • **要点** ○ サイバーに関する一定の知識を持った人間を 2 万人養成 ○ 新たな自衛官制度の導入 ○ 防衛省サイバーコンテストの実施 **任期付き自衛官制度** 5 年間の任期を限ってサイバーの業務を行う新しい自衛官制度。 • **要点** ○ 高額な給与の提供 ○ サイバー専門の予備自衛官の設置 **リボルビングドアの実現** 中途で入ってくるための制度や一度辞めた人たちが再び戻ってくる制度の強化。 • **要点** ○ 人材の循環による国全体のサイバー能力の強化 ○ アルム内制度の強化 **宿題と提案**

Fixed-term self-defense system A new self-defense system for cyber duties for a limited five-year term. • **Main point** ○ Offering high salaries ○ Establishment of a reserve self-defense force specializing in cyber **Revolving door realization** Strengthening the system for people to come in mid-career and for those who left once to come back. • **Main point** ○ Strengthening the cyber capabilities of the entire country through the circulation of human resources ○ Strengthening of Institutions within ALM **Homework and Suggestions**	

3.7 D3-S2-4 Speeches from Japanese Government

ABE Fumihiko (Deputy Director General for Cyber Affairs Bureau, National Police Agency)	阿部 文彦 (警察庁長官官房審議官（サイバー警察局担当）)
Ransomware, Phishing Scams, Cyber Police Bureau **Theme** The lecture discussed the increase in ransomware attacks and phishing scams. The National Police Agency's installation of Internet sensors and collection and observation of communication packets, the increase in no-ware ransomware, analysis of ransomware infection routes, the increase in phishing cases, the amount of Internet banking fraudulent transfers, and the amount of credit card fraudulent use were also discussed. The Cyber Police Bureau's efforts to establish a Cyber Force Center and Cyber Force were introduced. **Main point** 1. Increase in ransomware attacks 2. Increase in phishing scams 3. Frequent cyber-ispionage and espionage	ランサムウェア，フィッシング詐欺，サイバー警察局 **テーマ** この講演では、ランサムウェア攻撃とフィッシング詐欺の増加について議論されました。警察庁のインターネットセンサー設置や通信パケットの収集・観測、ノーウェアランサムの増加、ランサムウェア感染経路の分析、フィッシング件数の増加、インターネットバンキングの不正送金被害額、クレジットカードの不正利用被害額についても触れられました。サイバー警察局の取り組みとして、サイバーフォースセンターとサイバーフォースの設置が紹介されました。 **要点** 1. ランサムウェア攻撃の増加 2. フィッシング詐欺の増加 3. サイバーイスピオナージやスパイ活動の頻発 4. 警察庁のインターネットセンサー設置と通信パケットの収集・観測 5. ノーウェアランサムの増加 6. ランサムウェア感染経路の分析 7. ランサムウェア被害組織の復旧費用 8. フィッシング件数の増加

4. Installation of Internet sensors and collection and observation of communication packets by the National Police Agency
5. Increase in no-wear ransoms
6. Analysis of ransomware infection routes
7. Recovery costs for ransomware-affected organizations
8. Increase in the number of phishing incidents
9. Amount of fraudulent money transfers from Internet banking
10. Amount of damage caused by unauthorized use of credit cards

Highlights

- "It is very important that you promptly report, consult, and inform the police and other relevant agencies about the damage caused by cyber attacks."

Chapters and Topics

ransomware attack

A ransomware attack is a type of cyber attack that encrypts a company or organization's systems and demands a ransom for recovery.

- **Main point**
  - Increase in no-wear ransoms
  - 14 no-ware ransoms in the first half of 2024
  - VPN devices and remote desktops are the primary means of ransomware infection
- **Examples**

In February 2024, two suspects believed to be members of the Rockbit Group were detained in Europe, and the servers and other criminal infrastructure used by the group were taken down.

  - As a result of cooperative investigations by the investigative agencies of the countries involved, including the Japanese police, the suspects were successfully detained and the criminal infrastructure was successfully taken down.

9. インターネットバンキングの不正送金被害額
10. クレジットカードの不正利用被害額

ハイライト

- "サイバー攻撃の被害については、警察及び関係機関に速やかに通報、相談、報告していただくことがとても大切となってきます。"

章とトピック

ランサムウェア攻撃

ランサムウェア攻撃は、企業や組織のシステムを暗号化し、復旧のために身代金を要求するサイバー攻撃の一種です。

- **要点**
  - ノーウェアランサムの増加
  - 2024 年上半期に 14 件のノーウェアランサムが発生
  - ランサムウェア感染経路の主要な手段は VPN 機器とリモートデスクトップ
- **Examples**
- 2024 年 2 月、欧州においてロックビットグループの一員とみられる被疑者 2 名が拘束され、同グループが使用するサーバー等の犯罪インフラがテイクダウンされました。
  - 日本警察を含む関係各国の捜査機関が協力して捜査を進めた結果、被疑者の拘束と犯罪インフラのテイクダウンに成功。
  - ロックビットグループが被害企業等から接種した情報を暴露するために運営していたリークサイトが閉鎖され、捜査機関側で用意したウェブページが表示されるようになった。

フィッシング詐欺

フィッシング詐欺は、偽のウェブサイトやメールを使用して個人情報を盗む詐欺手法です。

- **要点**
  - フィッシング件数の増加
  - 2023 年のインターネットバンキングに係る不正送金被害額は約 87 億円
  - 2023 年のクレジットカードの不正利用被害額は約 541 億円

サイバー警察局の取り組み

サイバー警察局は、サイバー犯罪に対処するための専門部門であり、技術的な支援や捜査を行います。

- **要点**
  - 2022 年 4 月にサイバー警察局が発足

○ The leak site that the Rockbit Group operated to expose information inoculated by victim companies and others has been closed, and a web page prepared by the investigative agency is now displayed. **Phishing** Phishing scams are fraudulent methods that use fake websites or emails to steal personal information. • **Main point** ○ Increase in the number of phishing incidents ○ Fraudulent remittance losses related to Internet banking in 2023 will amount to approximately 8.7 billion yen ○ Credit card fraud losses in 2023 will be approximately 54.1 billion yen **Cyber Police Bureau Initiatives** The Cyber Police Bureau is a specialized unit to deal with cybercrime, providing technical assistance and investigations. • **Main point** ○ Cyber Police Bureau to be established in April 2022. ○ Establishment of Cyber Force Center and Cyber Force ○ Analysis to identify signs and actual conditions of cyber attacks **Homework and Suggestions**	○ サイバーフォースセンターとサイバーフォースの設置 ○ サイバー攻撃の予兆や実態を把握するための分析 **宿題と提案**

3.8 D3-S2-5 Speeches from Japanese Government

HIRAISHI Sekiaki (Assistant Director-General, Second Intelligence Department, Public Security Intelligence Agency)	平石 積明 （公安調査庁 調査第二部長）
Cyber Security, China, North Korea **Theme** The lecture discussed the International Symposium on Cyber Security, which crossed the boundaries between industry, government, and academia. Key topics covered included the Public Security Intelligence Agency's cyber-related investigations, trends in Chinese and North	サイバーセキュリティ，中国，北朝鮮 **テーマ** この講演では、産官学の垣根を越えたサイバーセキュリティ国際シンポジウムについて議論されました。公安調査庁のサイバー関連調査、中国と北朝鮮のサイバー活動の動向、人民解放軍の新たな部隊創設、i-Soon 社の情報流出事件、ボルトタイフーンの活動、北朝鮮のソーシャルエンジニアリング攻撃、キムスキーの活動と手法が主なトピックとして取り上げられ

Korean cyber activities, the People's Liberation Army's creation of new units, i-Soon's information leakage incident, Bolt Typhoon activities, North Korean social engineering attacks, and Kimski's activities and methods.

Main point

1. International Symposium on Cyber Security that Transcends Industry-Government-Academia Boundaries
2. Public Safety Research Agency cyber-related investigations
3. National Security Threats in Cyberspace
4. Trends in Chinese and North Korean Cyber Activities
5. Objectives and Methods of Chinese Cyber Attacks
6. Creation of a new unit of the People's Liberation Army
7. The i-Soon Inc. information leak
8. Bolt Typhoon activity and its effects
9. North Korea's Social Engineering Attacks
10. Kimski's Activities and Methodology

Chapters and Topics

Chinese Cyber Attacks

The primary objectives of China's activities in cyberspace include the acquisition of information and advanced technology on a wide range of political, military, and economic fields, as well as the control and maintenance of the Chinese Communist Party.

- **Main point**
  - In addition to the People's Liberation Army and the Ministry of State Security, IT companies in China commissioned by these agencies are involved.
  - The People's Liberation Army's Strategic Support Unit was modified to create a new Information Support Unit, Cyberspace Unit, and Military Space Unit.
  - The leak of iSUN's internal information.
  - Bolt Typhoon activity.

ました。

要点

1. 産官学の垣根を越えたサイバーセキュリティ国際シンポジウム
2. 公安調査庁のサイバー関連調査
3. サイバー空間における国家安全保障上の脅威
4. 中国と北朝鮮のサイバー活動の動向
5. 中国のサイバー攻撃の目的と手法
6. 人民解放軍の新たな部隊創設
7. i-Soon 社の情報流出事件
8. ボルトタイフーンの活動とその影響
9. 北朝鮮のソーシャルエンジニアリング攻撃
10. キムスキーの活動と手法

章とトピック

中国のサイバー攻撃

中国のサイバー空間上における活動の主たる目的は、政治、軍事、経済分野等の広範囲にわたる分野に関する情報や先端技術の獲得のほか、中国共産党の支配・維持などがあります。

- **要点**
  - 人民解放軍や国家安全部に加え、これらの機関に委託を受けた中国国内の IT 企業が関与。
  - 人民解放軍の戦略支援部隊を改変し、新たに情報支援部隊、サイバー空間部隊、軍事宇宙部隊を創設。
  - i-Soon 社の社内情報流出事件。
  - ボルトタイフーンの活動。

北朝鮮のサイバー攻撃

北朝鮮が分散型金融、暗号資産及び類似の事業者の従業員に対して、マルウェアを展開して暗号資産を摂取するために、検知困難なソーシャルエンジニアリングキャンペーンを展開。

- **要点**
  - 高度なソーシャルエンジニアリングは、外貨獲得だけではなく、機密情報の摂取にも用いられる。
  - キムスキーは偵察総局参加のサイバー部隊とされ、2012 年から活動を継続。
  - 標的型メール攻撃を用いて、外交・安全保障分野に関わっている韓国、米国及び日本の政府、研究機関、メディア等の関係者をターゲットにする。

宿題と提案

North Korean Cyber Attacks North Korea deployed a hard-to-detect social engineering campaign against employees of decentralized financial, crypto asset and similar businesses to deploy malware and ingest crypto assets. • **Main point** ○ Advanced social engineering is used not only to obtain foreign currency, but also to ingest sensitive information. ○ KIMSKY is considered a cyber unit with the participation of the General Directorate of Reconnaissance and has been active since 2012. ○ Targeted e-mail attacks are used to target the South Korean, U.S., and Japanese governments, research institutions, media, and other parties involved in the field of diplomacy and security. **Homework and Suggestions**	

3.9 D3-S2-6 Speeches from Japanese Government

KONDO Reiko (Deputy Director-General for ICT R&D and Cybersecurity Policy, Ministry of Internal Affairs and Communications)	近藤 玲子 (総務省大臣官房審議官（国際技術、サイバーセキュリティ担当）)
Cybersecurity, IoT, MIC Japan **Theme** This speech, held on November 1, 2024, covers the cybersecurity policies and directions of the Ministry of Internal Affairs and Communications (MIC) of Japan. Key topics include the observation of cyber attacks, the frequency of cyber attacks in 2023, the importance of communication network infrastructure, and NIC's safety measures. The speech also addresses IoT botnet issues, challenges with older IoT devices, and international collaborations for cybersecurity capacity building. **Takeaways** 1. Cybersecurity policies and directions of the MIC of Japan	サイバー攻撃, IoT セキュリティ, NICT **テーマ** この講演では、サイバー攻撃の観測と対策、NICT のダークネット観測、情報通信ネットワークの重要性、総務省のサイバーセキュリティ施策、IoT セキュリティ対策、C&C サーバーの検知と対策、NOTICE プロジェクト、脆弱な IoT 機器の問題、サイバー攻撃の増加傾向、利用者のセキュリティ意識の低さについて議論されました。 **要点** 1. サイバー攻撃の観測と対策 2. NICT のダークネット観測 3. 情報通信ネットワークの重要性 4. 総務省のサイバーセキュリティ施策 5. IoT セキュリティ対策 6. C&C サーバーの検知と対策 7. NOTICE プロジェクト

2. Observation of cyber attacks using unused IP addresses
3. Cyber attacks frequency in 2023
4. Importance of communication network infrastructure
5. NIC's safety measures for continuous communication service
6. Cyber task force operations since 2020
7. Mid-term key policies for IT cyber securities
8. IoT botnet issues and hijacking of IoT devices
9. Statistics on hijacked IoT devices
10. Challenges in distinguishing legal and illegal communications

Chapters & Topics

Cybersecurity Policies and Directions of MIC Japan

The Ministry of Internal Affairs and Communications (MIC) of Japan is responsible for communications, telecommunications, and cybersecurity policies.

- **Keypoints**
  - Observation of cyber attacks using unused IP addresses.
  - Cyber attacks frequency in 2023: approximately 1 every 14 seconds.
  - Importance of communication network infrastructure for global economy.
  - NIC's safety measures for continuous communication service.

Cyber Task Force Operations

The cyber task force has been operating since 2020 to map out basic policies for cybersecurity.

- **Keypoints**
  - Mid-term key policies for IT cyber securities.
  - Focus on IoT botnet issues and hijacking of IoT devices.

IoT Botnet Issues

IoT devices, including cameras and routers, are vulnerable to hijacking if not properly protected.

8. 脆弱な IoT 機器の問題
9. サイバー攻撃の増加傾向
10. 利用者のセキュリティ意識の低さ

章とトピック

サイバー攻撃の観測と対策

NICT がダークネットを利用してサイバー攻撃の観測を行い、そのデータを分析して対策を講じている。

- **要点**
  - NICT は 30 万個の未使用 IP アドレスを保有
  - 2023 年には約 14 秒に 1 回の不正通信を観測

情報通信ネットワークの重要性

情報通信ネットワークは社会経済活動に不可欠であり、サイバー攻撃による機能停止や情報漏洩は大きな影響を与える。

- **要点**
  - 総務省は民間通信事業者と連携して安全性を確保
  - 利用者の安心・安全を確保する役割

IoT セキュリティ対策

IoT 機器のセキュリティ対策が不十分な場合、ボットネットに乗っ取られ、大規模なサイバー攻撃の踏み台となる可能性がある。

- **要点**
  - 2021 年 8 月に 25 万台のルーターがボットネットに支配される事案
  - 保育所の見守りカメラの映像が第三者に閲覧される事案

C&C サーバーの検知と対策

総務省は C&C サーバーを検知し、フロー情報を分析して通信事業者間で共有し、サイバー攻撃への対策に活用している。

- **要点**
  - フロー情報の分析
  - 通信事業者間での情報共有

NOTICE プロジェクト

総務省は 2019 年から NOTICE プロジェクトを実施し、IoT 機器の脆弱性を調査し、管理者に注意喚起を行っている。

- **要点**
  - 初期設定のままの ID とパスワードの脆弱性
  - ISP を通じた注意喚起

サイバー攻撃の増加傾向

サイバー攻撃の通信は 5 年前に比べて約 3 倍に増加してお

- **Keypoints**
  - Statistics show 250,000 hijacked IoT devices up to last year.
  - Challenges in distinguishing legal and illegal communications.
  - MIC's botnet solutions for IoT device protection.

Measures for Network and Terminal IoT Device Security

MIC has implemented measures for network and terminal IoT device security, including detection of potential attacks through CNC servers.

- **Keypoints**
  - Detection based on IP address, port address, and timestamp information.
  - Vulnerability of IoT devices with weak passwords.
  - Revision of terminal-related laws in 2020.

Challenges with Older IoT Devices

Many IoT devices are vulnerable due to being manufactured before 2013 and having weak security measures.

- **Keypoints**
  - More than 40% of devices were manufactured before 2013.
  - User negligence in IoT device security.
  - Revisions of the NICT law to address these vulnerabilities.

Human Resource Development

MIC has set up a national training center for companies and individuals to enhance cybersecurity skills.

- **Keypoints**
  - Special exercises for events like the Osaka Expo.
  - Collaboration with METI to establish security communities.

International Collaborations

MIC is engaged in international collaborations, including seminars, workshops, and support for developing nations.

- **Keypoints**

り、マルウェアの活動も依然として活発である。

- **要点**
  - ID パスワード以外の脆弱性
  - ファームウェアを狙った攻撃

利用者のセキュリティ意識の低さ

Wi-Fi ルーターの利用者の約 58%がセキュリティを意識しておらず、法人利用者も適切な管理体制が取られていない。

- **要点**
  - 利用者のセキュリティ意識向上の必要性
  - 法人利用者の管理責任の所在の曖昧さ

サイバーセキュリティ人材育成

NICT はナショナルトレーニングセンターを設置し、国や地方自治体、独立行政法人を対象にトレーニングを提供している。

- **要点**
  - 2017 年からのトレーニング提供
  - 2 万人以上の受講者

国際連携とトレーニング

NICT はタイに日アシアンサイバーセキュリティ能力構築センターを設置し、東諸国を対象とした演習を実施している。

- **要点**
  - 13 カ国から 29 名が参加
  - フィジーでの演習

サイバーセキュリティ意識啓発サイト

総務省は国民のためのサイバーセキュリティ意識啓発サイトを設け、初心者向けの対策や被害事例をまとめている。

- **要点**
  - 2024 年 5 月に全面リニューアル
  - 家庭や職場での対策情報

宿題と提案

○ Cybersecurity Capacity Building Center in Thailand. ○ Special Exercise Capacity Building for Pacific Island Countries. **Assignments & Suggestions**	

3.10 D3-S2-7 Speeches from Japanese Government

OKUYA Toshikazu (Deputy Director General, Commerce and Information Policy Bureau, Ministry of Economy, Trade and Industry)	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）)
Cybersecurity, Society 5.0, Advanced Persistent Threats **Theme** This speech, held on November 1, 2024, covers Japan's cybersecurity policy, the complexity and sophistication of cyber attacks, and the interconnected systems of Society 5.0. Key topics include firmware malware, Advanced Persistent Threats (APT), cybercrime, expanding attack surfaces, supply chain cybersecurity, and international cooperation. The Cyber Physical Security Framework (CPSF) and support for SMEs in cybersecurity are also discussed. **Takeaways** 1. Cybersecurity policy in Japan 2. Complexity and sophistication of cyber attacks 3. Society 5.0 and interconnected systems 4. Firmware malware sending data to China 5. Identifying and addressing risks 6. Advanced Persistent Threats (APT) 7. Cybercrime and hacktivists 8. Expanding attack surface and vectors 9. Supply chain cybersecurity 10. International cooperation and certification **Highlights** • "What is important is in each of us, your initiative, each one of you's initiative is very important."-- Toshikazu Okuya **Chapters & Topics**	サイバーセキュリティ, ソサイティ 5.0, CPSF **テーマ** この講演では、サイバーセキュリティの高度化と複雑化、ソサイティ 5.0 と新しい法律、データ連携とサプライチェーンの複雑性、リスクベースのセキュリティ対応、攻撃者のタイプと攻撃パターン、アタックサーフェスの拡大、サイバーフィジカルセキュリティフレームワーク（CPSF）、サプライチェーンのセキュリティ対応、中小企業へのサポート、サイバーセキュリティサポーターズサービスについて説明しました。 **要点** 1. サイバーセキュリティの高度化と複雑化 2. ソサイティ 5.0 と新しい法律 3. データ連携とサプライチェーンの複雑性 4. リスクベースのセキュリティ対応 5. 攻撃者のタイプと攻撃パターン 6. アタックサーフェスの拡大 7. サイバーフィジカルセキュリティフレームワーク（CPSF） 8. サプライチェーンのセキュリティ対応 9. 中小企業へのサポート 10. サイバーセキュリティサポーターズサービス **ハイライト** • "自分たちが守らないといけない価値は何なのか。その価値を守るために、価値が既存するのはどういうリスクなのか。"-- 奥家 **章とトピック** **サイバーセキュリティの高度化と複雑化** サイバー攻撃が高度化し、複雑化している現状についての説明。 • **要点** ○ 攻撃の高度化と複雑化

Cybersecurity Policy in Japan

The cybersecurity policy in Japan focuses on addressing the increasing complexity and sophistication of cyber attacks, particularly in the context of Society 5.0, where many systems are interconnected and encrypted.

- **Keypoints**
  - Complexity and sophistication of cyber attacks
  - Interconnected and encrypted systems in Society 5.0
  - Firmware malware sending data to China
  - Identifying and addressing risks
  - Advanced Persistent Threats (APT)
  - Cybercrime and hacktivists
  - Expanding attack surface and vectors
- **Considerations**
- Strengthening measures throughout the supply chain
- International cooperation and certification
- AI application in cybersecurity
- Support for SMEs in cybersecurity
- **Special Circumstances**
- If encountering a firmware malware that sends data to China every 72 hours, how should it be addressed? Identify the malware, notify the manufacturer, and take steps to mitigate the risk.

Cyber Physical Security Framework (CPSF)

The Cyber Physical Security Framework (CPSF) was created to address the security challenges in the interconnected world of physical and cyber spaces. It provides guidelines for various sectors and focuses on data management, IoT security, and safety.

- **Keypoints**
  - Creation of CPSF in 2019
  - Guidelines for various sectors
  - Data management framework
  - IoT security and safety
- **Considerations**
  - リスクベースの対応の必要性

ソサイティ 5.0 と新しい法律

日本政府が推進するソサイティ 5.0 とそれに伴う新しい法律についての説明。

- **要点**
  - ソサイティ 5.0 の概要
  - 新しい法律の発表

サイバーフィジカルセキュリティフレームワーク（CPSF）

サイバーフィジカルセキュリティフレームワーク（CPSF）の概要とその重要性についての説明。

- **要点**
  - CPSF の概要
  - フィジカル空間とサイバー空間の連携

中小企業へのサポート

中小企業に対するサイバーセキュリティのサポートについての説明。

- **要点**
  - 中小企業のリソース不足
  - サイバーセキュリティサポーターズサービスの提供

産業制御システムのセキュリティ

産業制御システムにおけるセキュリティの重要性とその対応についての説明。

- **要点**
  - 産業制御システムの複雑性
  - プロフェッショナルの育成

宿題と提案

• Ensuring the reliability of anchor points in cyberspace • Securing the value creation process within the supply chain **Support for SMEs in Cybersecurity** Supporting SMEs in cybersecurity is crucial due to their limited resources. Initiatives include creating documents, forming consortia, and providing affordable monitoring services. • **Keypoints** ○ Challenges faced by SMEs in cybersecurity ○ Creation of support documents ○ Formation of consortia ○ Affordable monitoring services • **Examples** • A national project working with insurance companies to create a consortium and provide affordable cybersecurity services for SMEs. The project involved setting premiums and offering monitoring services for 10,000 yen per month. ○ Forming a consortium with insurance companies ○ Setting premiums for cybersecurity services ○ Offering affordable monitoring services • **Considerations** • Providing appropriate support from outside • Ensuring business managers are conscious of cybersecurity issues **Assignments & Suggestions**	

3.11 D3-S2-8 Speeches from Japanese Government

SAKA Akira (CISO, Digital Agency)	坂 明 (デジタル庁 CISO)
Overview This speech outlines the key aspects of the Digital Agency's initiatives, roles, and responsibilities, focusing on cybersecurity, digitization, and citizen-centric services. It also includes action	**Overview** この講演は、デジタル庁の概要と役割、施策、セキュリティ対策についての詳細な説明を提供しています。デジタル庁の設立背景、ミッション、ビジョン、重点分野、具体的な施策、セキュリティ体制と施策についての情報が含まれています。最後

items to enhance cybersecurity and digitization efforts through collaboration with private companies. The content was created on 2024-11-01. **Digital Agency Overview** **Launch and Purpose** • **Launch Date**: 2021 • **Trigger**: COVID-19 pandemic highlighted the delayed digitization in Japan. • **Purpose**: ○ Security of public space. ○ Centralize and manage cybersecurity systems previously handled by different ministries and agencies. ○ Provide a common platform for government and citizen services. **Key Roles and Responsibilities** • **Cybersecurity and Digitization**: ○ Central management of cybersecurity and digitization efforts. ○ Cross-border budget management and auditing authority for government activities. • **Provision of Services**: ○ Provide user-friendly, citizen-centric public services. ○ Ensure inclusive social growth through digital infrastructure. ○ Manage digital ID (My Number) for citizens. ○ Support government personnel-related services and uninterrupted service provision during crises like COVID-19. **Initiatives and Vision** **Citizen-Centric Public Services** • **Mission**: Human-friendly digitization ensuring no one is left behind. • **Vision**: Government as a service, government as a startup. ○ Provide easy-to-use, user-friendly services to both government and citizens. ○ Maintain a startup spirit to foster	に、アクションアイテムがまとめられています。文書の作成日は2024年11月1日です。 **デジタル庁の概要と役割** **設立背景** • **設立時期**: 2021年9月 • **設立のきっかけ**: COVID-19 パンデミックが日本のデジタル化の遅れを浮き彫りにした。 ○ 公衆衛生面の安全確保や事業支援のためのシステムが各役所でバラバラであった。 ○ 個人や事業体の特定が難しく、サポート基盤が欠如していた。 **意義と役割** • **司令塔としての役割**: 日本のデジタル化を統括。 ○ 政府全体の情報システムの予算を統一的に管理。 ○ 情報システムの監督と管理。 • **サービス提供**: 国民や政府機関に対するサービスのプラットフォームを提供。 ○ 各政府機関や地方公共団体が利用するための情報システムの基盤を提供。 **ミッションとビジョン** • **ミッション**: Human-Friendly Digitalization ○ 誰一人取り残さない、人に優しいデジタル社会を構築。 • **ビジョン**: Government as a Service, Government as a Startup ○ 優しいサービスの作り手として、効果的なサービスを提供。 ○ スタートアップ精神で行政を革新し、人々の生活を向上。 **重点分野** • **生活者、事業者、職員に優しいサービスの提供** ○ シーズンセントリックパブリックサービスの提供。 • **デジタル基盤の整備による成長戦略の推進** ○ デジタルインフラストラクチャー for inclusive growth。 • **安全・安心で強靭なデジタル基盤の実現** ○ 強靭で安全なシステムの構築。 **デジタル庁の施策** **マイナンバーカード制度** • **目的**: 国民一人一人に対する認証基盤を提供。 ○ デジタル社会において個人を明確にする機能。 • **スマホ対応**:

innovation and improve citizens' lives.

Digital Infrastructure for Inclusive Growth

- **Objective**: Build a solid foundation for digital transformation.
- **Components**:
  - Government cloud for efficient service provision.
  - AI utilization for future service enhancements.
  - Cybersecurity measures to protect digital infrastructure.

Cybersecurity Measures

Collaboration and Policies

- **Collaboration with NISC**:
  - Digital Agency provides nationwide digital policies.
  - NISC provides cybersecurity policies and measures.
  - Joint efforts to monitor and maintain safe infrastructure for citizen services.
- **CISO Role**:
  - Similar to private organizations, responsible for comprehensive cybersecurity.
  - Establishes strategies, guidelines, and manuals for secure IT systems.

Continuous Risk Management

- **Continuous Diagnostic and Mitigation (CDM)**:
  - Nationwide information security system to understand and address vulnerabilities.
  - Responsive measures for incidents.
- **COSMOS**:
  - Systems for individual accountability and secure responsibilities.
  - Framework to ensure organizations and ministries meet security requirements.

Future Collaboration

- **Private Sector Engagement**:
  - Ongoing collaboration with private companies to enhance cybersecurity and digitization efforts.
  - Android は 5 月から対応。
  - iPhone は来年から対応予定。

ガバメントソリューションサービス

- **目的**：政府機関が効率的で合理的なサービスを提供するための基盤を構築。
  - リモート勤務やフィールド活動を支援。
- **ガバメントクラウド**：強靭なクラウド基盤を提供。
  - 将来的には AI の活用も視野に入れている。

セキュリティ対策

セキュリティ体制

- **NISC との協力**：サイバーセキュリティ戦略の策定と実施。
  - 政府の情報システムのセキュリティ基準を制定。
- **GSOC**：政府の情報システムを監視し、サイバーセキュリティを確保。

セキュリティ施策

- **CRSA (Continuous Risk Scoring Action)**:
  - 政府の情報システムの脆弱性をモニタリングし、適切に対応。
- **コスモス**：セキュリティオペレーションセンターを含むシステムを構築。
  - インテリジェンスの収集と活用、脆弱性管理、インシデント対応、監査、教育を実施。

セキュリティ全体像

- **戦略と基準の策定**：国全体のセキュリティを含めた情報システム構築のための戦略と基準を策定。
- **ISMAP 制度**：安全なシステムの認証を行う制度を運営。

Action Items

[ ] スライドの提供依頼があれば対応する。

Action Items [ ] Continue collaboration with private companies to enhance cybersecurity and digitization efforts.	

3.12 D3-S2-9 Speeches from Japanese Government

SAKAMOTO Shuichi (Assistant Minister for Cybersecurity, IT Management and Evidence-based Policymaking, Ministry of Education, Culture, Sports, Science and Technology - Japan)	坂本 修一 (文部科学省 サイバーセキュリティ・政策立案総括審議官)
Cybersecurity, Universities, Research Institutes **Theme** This speech covers the importance of cybersecurity in universities and national research institutes, including basic concepts, collaboration among organizations, R&D initiatives, risk assessment, and training courses for cybersecurity personnel. It emphasizes the need for information sharing and the role of emerging technologies in cybersecurity. **Takeaways** 1. Cybersecurity in universities and national research institutes 2. Basic concepts of cybersecurity 3. Promotion of collaboration among relevant organizations 4. R&D initiatives in cybersecurity 5. Importance of cybersecurity in protecting critical technologies 6. Risk assessment and resource allocation in cybersecurity 7. Training courses for CISOs, department managers, and CSAT members 8. Information sharing among CSAT members and relevant experts 9. Academic CSAT information exchange meeting 10. Information Security Task Force for national research institutes **Highlights** • "Ensuring cybersecurity is one of the	サイバーセキュリティ, リーダーシップ, 情報共有 **テーマ** この講演では、サイバーセキュリティシステムのリスク評価、CISO と各部門のリーダーシップ、アカデミック CSIRT ネットワークの設立、そして日本政府が支援する K プログラムについて議論されました。特に、リスク評価の重要性や情報共有の重要性が強調されました。 **要点** 1. 英語のプレゼンテーションの準備 2. 国立研究所と大学の役割 3. サイバーセキュリティシステムのリスク評価 4. 適切なリソース配分 5. サイバーセキュリティ管理システムの強化 6. ディスク管理システムの構築 7. CISO と各部門のリーダーシップ 8. サイバーセキュリティガバナンスの重要性 9. 情報共有とグッドプラクティスの共有 10. アカデミック CSIRT ネットワークの設立 **章とトピック** **サイバーセキュリティシステムのリスク評価** サイバーセキュリティシステムはリスク評価を行い、最新の情報に基づいて運用する必要がある。 • **要点** ○ リスク評価の重要性 ○ 最新情報の活用 **CISO と各部門のリーダーシップ** CISO と各部門のリーダーがサイバーセキュリティガバナンスを確立し、効果的な対応を行う必要がある。 • **要点** ○ リーダーシップの重要性 ○ ガバナンスの確立

essential responsibilities of the university."-- Shuichi Sakamoto 《14th International Cybersecurity Symposium》

Chapters & Topics

Cybersecurity in Universities and National Research Institutes

Overview of activities for cybersecurity in universities and national research institutes promoted by MEXT.

- **Keypoints**
  - Basic concepts of cybersecurity
  - Promotion of collaboration among relevant organizations
  - R&D initiatives in cybersecurity

Risk Assessment and Resource Allocation

Risk assessment needs to be done based on the latest available information and monitoring results. Effective measures are selected and prioritized depending on the importance of information assets.

- **Keypoints**
  - Risk assessment based on latest information
  - Prioritization of effective measures
  - Resource allocation for system upgrades

Training Courses for Cybersecurity Personnel

MECS provides training courses for CISOs, department managers, and CSAT members of universities and research institutes.

- **Keypoints**
  - Courses for CISOs and department managers focus on cybersecurity governance and system structure
  - Courses for CSAT members provide practical exercises to improve security functions and respond to cyber attacks

Information Sharing Among CSAT Members

Next facilitates sharing of information including latest trends in threats, technology advancement, and good practices among CSAT members of universities, research institutes, and relevant experts.

アカデミック CSIRT ネットワーク

2017 年 6 月に設立されたアカデミック CSIRT ネットワークは、大学研究機関の情報共有と共通課題への取り組みを目的としている。

- **要点**
  - 設立の背景
  - 情報共有の重要性

K プログラム

日本政府が支援する新技術の研究開発プログラムで、生成 AI や量子コンピューティングなどの分野に焦点を当てている。

- **要点**
  - プログラムの目的
  - 対象分野

宿題と提案

• **Keypoints** ○ Academic CSAT information exchange meeting started in 2017 ○ 40 academic organizations participating in the network ○ Information Security Task Force for national research institutes **Emerging Technologies and R&D Initiatives** Emerging technologies such as generative AI and quantum computing have been advancing at an unprecedented speed. R&D of these technologies becomes a crucial element of international competitiveness and national security. • **Keypoints** ○ K-Program for key and advanced technology R&D ○ Cross-sectional collaboration in technological domains ○ Government investment in critical and emerging technologies ○ Commercialization of research results **Assignments & Suggestions**	

3.13 D3-S2-10 Speeches from Japanese Government

SAWAKI Kiyoshi (Secretary General, Personal Information Protection Commission)	佐脇 紀代志 (個人情報保護委員会 事務局長)
Overview This speech contains the meeting notes from an international symposium on cybersecurity held on November 1, 2024. The notes cover the introduction and roles of the Personal Information Protection Commission (PPC), discussions on international efforts, personal data breaches, and collaboration among government departments. An action items section has been created and placed at the end of the document. **Introduction** • **Speaker**: Sawaki, Secretary General of the Personal Information Protection Commission (PPC) • **Event**: International Symposium on	個人情報保護，サイバーセキュリティ，AI 技術 **テーマ** この講演では、個人情報保護政策とサイバーセキュリティの関連性、個人情報保護委員会の役割、G7 データオン・プライバシー機関ラウンドテーブル会議の概要、AI 技術と個人データ保護の関係、法執行機関の協力と情報交換の重要性、個人データ漏洩の事例とその対策、VPN 機器やウェブサイトの脆弱性とその対策、SQL インジェクション攻撃の対策、セキュリティ確保のための基礎的な対応策について説明されました。 **要点** 1. 個人情報保護政策とサイバーセキュリティの関連性 2. 個人情報保護委員会の基本的な役割 3. G7 データオン・プライバシー機関ラウンドテーブル会議の概要

Cybersecurity

- **Main Focus**: Discussing challenges and efforts in Personal Information Protection Policies, both domestically and internationally.

Overview of PPC

- **Roles and Responsibilities**:
  - Address issues related to cross-border data transfers.
  - Collaborate on responses to global risks and exchange opinions on technologies like AI.
  - Handle complaints and mediation between businesses and individuals.
  - Conduct legal supervision and investigations for significant risks.
  - Engage in public relations and awareness activities.

Topics Discussed

International Efforts

- **G7 Data Protection and Privacy Authority Roundtable**:
  - **Recent Meeting**: Held in Rome, Italy.
  - **Participants**: Representatives from G7 countries, including Commissioner Oshima (PPC) and Commissioner Slaughter (FTC, USA).
  - **Key Points of Communique and Action Plan**:
    - **Three Pillars**:
- **DFFT (Data Free Flow with Trust)**:
  - Concept proposed by former Prime Minister Abe.
  - Comparative analysis of GDPR-based certification system and global CBPR system.
  - Aim to enhance predictability for data transfers.
- **Emerging Technologies**:
  - Focus on AI and the role of DPAs.
  - Collaboration with regulatory authorities in competition, communications, and

4. AI 技術と個人データ保護の関係
5. 法執行機関の協力と情報交換の重要性
6. 個人データ漏洩の事例とその対策
7. VPN 機器の脆弱性とその対策
8. ウェブサイトの脆弱性とその対策
9. SQL インジェクション攻撃の対策
10. セキュリティ確保のための基礎的な対応策

ハイライト

- "データの価値を生かし、新たなイノベーションを起こし、社会活動や経済活動の質を高めるためには、データをめぐる多様なリスクを把握し、理解し、合理的にそれに備えておくことが重要です。"-- 佐脇

章とトピック

個人情報保護政策とサイバーセキュリティ

個人情報保護政策はサイバーセキュリティに密接に関連しており、データの価値を生かしつつリスクに備えることが重要である。

- **要点**
  - データの価値を生かすためにはリスクの把握と理解が必要
  - 合理的な備えが社会活動や経済活動の質を高める

個人情報保護委員会の役割

個人情報保護委員会は基本的な政策の立案、監督、国際協力、苦情対応などを行う。

- **要点**
  - 基本的な政策の立案
  - 個人情報保護に基づく監督
  - 国際協力
  - 苦情対応

G7 データオン・プライバシー機関ラウンドテーブル会議

G7 開催国の DPA が主催し、データとプライバシーに関する議論を行う。

- **要点**
  - 各国の DPA が参加
  - AI 技術に関する議論
  - 法執行機関の協力

AI 技術と個人データ保護

AI 技術の適切な活用と個人データ保護の関係について議論。

- **要点**
  - DPA の役割

consumer protection.

- **Enforcement Cooperation**:
  - Sharing best practices and domestic enforcement expertise.
  - **Upcoming Event**: Asia-Pacific Privacy Authorities Forum on the 26th and 27th of this month.

Personal Data Breaches

- **Data Breach Reports**:
  - **Statistics**: Number of reports received by PPC in the last fiscal year and the year before.
  - **Significant Cases**:
    - **Unauthorized Access via Telework**:
      - Employee received a virus-infected email from a third party met on social media.
      - Attackers used social media to gain trust and extract passwords.
    - **VPN Device Vulnerabilities**:
      - Common due to inadequate security measures.
    - **Website Vulnerabilities**:
      - Attackers exploit vulnerabilities to set traps and obtain personal data.
    - **SQL Injection Attacks**:
      - Attackers infiltrate databases through website logic forms.
  - **Common Causes**:
    - Weak management of authentication information.
    - Improper updates to eliminate VPN device vulnerabilities.
    - Website vulnerabilities and misconfiguration in cloud services.
  - **Preventive Measures**:
    - Basic literacy and consistent action.
    - Ensuring security through steady efforts and constant vigilance.

Collaboration Among Government Departments

- **Cybersecurity Agencies**:
  - PPC collaborates with various government

  - AI 技術のガバナンス

個人データ漏洩の事例と対策

個人データ漏洩の具体的な事例とその対策について説明。

- **要点**
  - テレワーク中の SNS を利用したウイルス感染
  - VPN 機器の脆弱性
  - ウェブサイトの脆弱性
  - SQL インジェクション攻撃
- **Examples**
- テレワーク中の社員が SNS で知り合った第三者からウイルスを添付した電子メールを受領し、社内システムの情報漏洩に発展。
  - SNS を利用して本人を安心させ、パスワードを聞き出す手口
  - ウイルス感染に至る流れ
- VPN 機器のセキュリティ上の措置が適切になされていないために発生する不正アクセス。
  - VPN 機器のセキュリティ対策の重要性
- ウェブサイトの脆弱性をついて罠が仕掛けられ、個人データが搾取される事例。
  - ウェブサイトのメンテナンスと監視の重要性
- ウェブサイト上のログイン情報を悪用し、データベースに侵入してデータを盗み出す攻撃。
  - ウェブサイトの構築方法で防御可能

宿題と提案

departments, each with specialized capabilities, to address cybersecurity risks effectively. **Action Items** [ ] Attend the Asia-Pacific Privacy Authorities Forum on the 26th and 27th of this month.	

3.14 D3-S3 Societal Security

Satoru Tezuka	手塚 悟
Cybersecurity, DFFT, Trust Infrastructure **Theme** This speech, held on November 1, 2024, covers the importance of digital cybersecurity for national, economic, and societal security. Key topics include the concept of Data Free Flow with Trust (DFFT), proposed by late Prime Minister Abe, and its role in Society 5.0, digital transformation (DX), and cybersecurity. The speech also emphasizes the development of international trust service infrastructure to prevent data tampering and sender spoofing. **Takeaways** 1. Digital Cybersecurity for National Security, Economic Security, and Societal Security 2. National Security corresponds to government 3. Economic Security corresponds to critical infrastructure 4. Societal Security corresponds to private sector business and citizens 5. Importance of building digital infrastructure 6. Data Free Flow with Trust (DFFT) proposed by late Prime Minister Abe at Davos Forum in 2019 7. DFFT is essential for Society 5.0, DX, and cybersecurity 8. Trust in DFFT is crucial for preventing data tampering and sender spoofing 9. Development of international trust service infrastructure	**概要** この講演は、2024 年 11 月 1 日に作成された第 14 回国際シンポジウムの内容をまとめたものです。主なテーマは社会の安全保障に関するもので、デジタルサイバー安全保障戦略、データフリーフローウィズトラスト（DFFT）、および日本、EU、インドの比較報告に関する議論が含まれています。最後に、アクションアイテムがまとめられています。 **社会の安全保障** **デジタルサイバー安全保障戦略** • **テーマの概要** ○ 国家安全保障、経済安全保障、社会保障のためのデジタルサイバー安全保障戦略について議論。 ○ デジタルサイバー安全保障戦略は、日本のセキュリティ状況を示すもの。 • **カテゴリー分け** ○ **国家安全保障**: 政府に相当。 ○ 経済安全保障: 重要な経済活動に相当。 ○ 社会保障: 民間保障、ビジネスおよび市民に該当。 • **デジタルインフラストラクチャー** ○ デフォルトであるべきデジタルインフラの構築が重要。 ○ デジタルサイバー安全保障のテーマが取り上げられる理由。 **データフリーフローウィズトラスト** • **DFFT の概要** ○ 2019 年にダボスフォーラムで安倍総理大臣が提唱。 ○ ソサイティー5.0 および DX の実現に不可欠。 ○ サイバーセキュリティの実現にも不可欠。 • **トラストの重要性** ○ DFFT の「T」はトラストを指す。 ○ デジタルトラストの確立がグローバルなデジタル貿易取引の必要条件。

10. Announcement of JP-EU-India comparison report **Highlights** • "DFFT is indispensable to realize Society 5.0 and DX, as well as to realize cybersecurity." **Chapters & Topics** **Digital Cybersecurity** The integration of cybersecurity measures into digital infrastructure to protect national, economic, and societal security. • **Keypoints** ○ National Security: Government protection ○ Economic Security: Critical infrastructure protection ○ Societal Security: Protection of private sector business and citizens **Data Free Flow with Trust (DFFT)** A concept proposed to ensure the free flow of data across borders with a foundation of trust to prevent data tampering and sender spoofing. • **Keypoints** ○ Proposed by late Prime Minister Abe at Davos Forum in 2019 ○ Essential for Society 5.0, DX, and cybersecurity ○ Trust is crucial for preventing data tampering and sender spoofing **Trust Service Infrastructure** Infrastructure that supports electronic signatures and electronic authentication to establish trust in digital interactions. • **Keypoints** ○ Necessary for DFFT ○ Prevents data tampering and sender spoofing ○ Requires international development and acceleration **Assignments & Suggestions**	• **トラストサービスインフラストラクチャー** ○ 電子署名および電子認証の国際的な開発と実装が必要。 ○ 現在進行中であり、さらに加速化が必要。 **日本、EU、インドの比較報告** • **研究報告の公表** ○ 国際相互認証に関する初のシンポジウムでの公表。 ○ QR コードをスキャンしてダウンロード可能。 • **スピーチとパネルディスカッション** ○ 相互認証に関する議論が行われる予定。 **Action Items** [ ] トラストサービスインフラストラクチャーの実装を加速化する。 [ ] 日本、EU、インドの比較報告をダウンロードして確認する。

3.15 D3-S4 Speech: NIST SP800-63-4 Digital Identity Guideline

David Temoshok (NIST)	デビッド・テモショク（NIST）

Digital Identity, NIST Guidelines, Fraud Detection

Theme

This speech, held on November 1, 2024, covered comprehensive guidelines for digital identity management in the federal government. Key topics included NIST Special Publication 800-63, Revision 4, the Federal Information Modernization Act (FISMA), and performance metrics for identity systems. The speech emphasized a cross-functional approach to privacy, usability, equity, fraud detection, and cybersecurity, with a focus on identity proofing, authentication processes, and fraud detection capabilities.

Takeaways

1. Digital Identity Guidelines
2. NIST Special Publication 800-63, Revision 4
3. Federal Information Modernization Act (FISMA)
4. Security and Privacy Controls for Information Systems
5. Identity proofing and identity assurance
6. Authentication processes and authentication assurance
7. Federation assurance
8. Digital identity risk management
9. Performance metrics for identity systems
10. Fraud detection capabilities

Highlights

- "We wanted to make sure that digital identity management in the government was a cross-functional approach across privacy, usability, equity, fraud detection capabilities and fraud investigation, as well as cybersecurity personnel, to make sure that the approaches being taken and the."-- David Temoshok

Chapters & Topics

Digital Identity Guidelines

Comprehensive foundation of the processes and technical requirements for digital identity

Overview

この講演は、NIST のデジタルアイデンティティガイドラインに関する会議記録です。ガイドラインの背景、リスクマネジメント、プライバシー保護、改定プロセス、パブリックコメントの募集と今後の予定について詳述しています。内容は 2024 年 11 月 1 日に作成されました。

NIST のデジタルアイデンティティガイドラインについて

デイビッド・テモショックの紹介

- デイビッド・テモショックは NIST（国立標準技術研究所）のシニアアドバイザー。
- NIST 800-63 の第 4 改定版、2 番目のパブリックドラフトについて説明。

ガイドラインの権限と背景

- ガイドラインは連邦政府の情報および情報セキュリティに関するもの。
- FISMA（連邦情報セキュリティ管理法）に基づき、連邦省庁機関は適切なコントロールを実現し、情報システムのリスクや脆弱性に対応する必要がある。
- NIST は SP 800-53、セキュリティとプライバシーコントロールの情報システム用のものを提供。

デジタルアイデンティティガイドラインの概要

- ガイドラインは連邦政府の情報システムや OS に関するもので、連邦政府のオンラインサービスへのアクセスを提供。
- 4 つのボリュームに分かれており、アイデンティティの本人確認、アイデンティティのアシュランス、認証、フェデレーションを含む。
- フェデレーションのアシュランスにより、ユーザーは一つのアカウントで複数のサービスにアクセス可能。

リスクマネジメントとアシュランスレベル

- デジタルアイデンティティのリスクマネジメントプロセスを提供。
- 3 つのアシュランスレベル（ベースレベル、中間レベル、ハイレベル）を設定。
- リスクアセスメントプロセスを通じて情報システムのアセスメントを行い、オンラインアプリケーションの保護状況を判断。

公平性とプライバシー保護

- ガイドラインはプライバシー保護と公平性を重視。
- 政府のオンラインサービスは全ての層に対して公平に提供されることを目指す。

第 3 改定版と第 4 改定版の改定プロセス

management across the federal government. • **Keypoints** ○ Identity proofing and identity assurance ○ Authentication processes and authentication assurance ○ Federation assurance • **Considerations** ○ Enhancing privacy protections ○ Usability considerations ○ Equity across demographic groups **NIST Special Publication 800-63, Revision 4** The second public draft of the Digital Identity Guidelines, addressing emerging threats and new technologies. • **Keypoints** ○ Phishing-resistant authentication ○ Syncable authenticators ○ Digital credentials and mobile driver's licenses ○ E-wallets • **Considerations** ○ Cross-functional approach across privacy, usability, equity, fraud detection, and cybersecurity **Federal Information Modernization Act (FISMA)** Statute requiring all federal agencies to implement appropriate controls to address risks or vulnerabilities in information systems. • **Keypoints** ○ NIST establishes guidance to implement FISMA requirements ○ Publications like NIST Special Publication 800-53 and 800-63 **Performance metrics for identity systems** Metrics to ensure identity systems' performance over time. • **Keypoints** ○ Recommended performance metrics for identity systems and providers ○ Ongoing testing of biometric comparison algorithms	**第 3 改定版の背景** • 第 3 改定版は 2017 年 6 月に発表され、2020 年 6 月にアップデート。 • 技術的な変化や新しい攻撃ベクトルに対応するため、リビジョン 4 の開始。 **第 4 改定版の改定プロセス** • 2020 年 6 月にリビジョン 4 の開始、2022 年 12 月に最初のパブリックドラフトを発表。 • 約 4000 件のコメントを受け取り、テキストの更新と新しい要件を追加。 • 2024 年 8 月に 2 つ目のパブリックドラフトを発表。 **改定の主な変更点** • デジタルアイデンティティモデルの更新。 • デジタルワレット用のデジタル ID モデルの導入。 • デジタル ID のリスク管理プロセスの更新。 • 文書認証システムの性能評価基準の導入。 • バイオメトリックス検証要件の更新。 **パブリックコメントと今後の予定** **パブリックコメントの募集** • 第 2 次パブリックドラフトは 2024 年 8 月に発表され、コメント募集期間は 10 月 7 日まで。 • 約 2000 件のコメントを受け取り、最終的な改定版の 4 を公表予定。 **今後の予定** • 最終的な改定版の 4 は来年に公表予定。 • パブリックコメント期間は設けない予定。 **Action Items** [ ] コメントの提出先：digitashconvents.org

Fraud detection capabilities Capabilities to detect and prevent fraud in identity proofing and authentication. • **Keypoints** ○ Geospatial analysis ○ Device characteristics ○ Automated attack protections ○ Death record checks **Document authentication systems** Systems to authenticate documents used in identity proofing. • **Keypoints** ○ Performance metrics for document authentication pass rates and failure rates ○ Testing requirements for document authentication systems **Biometric verification requirements** Enhanced performance metrics for biometric verification in identity proofing. • **Keypoints** ○ Visual recognition and comparison of selfies to identity documents ○ Ongoing testing of biometric comparison algorithms **Syncable authenticators (PASCIs)** Authenticators that can be synchronized across devices. • **Keypoints** ○ Included in the draft for public comment ○ Addressed in Volume 63B **User-controlled wallets** Digital identity model for e-wallets, allowing users to control their identity information. • **Keypoints** ○ Processes and technologies for e-wallet-based authentication ○ Treated similarly to federation assertions **Assignments & Suggestions**	

3.16 D3-P5 Panel: Trusted Data Distribution, Data-EX, Ouranos, IDSA/GAIA-X

Moderator: Koichi Akaishi (Tokio Marine & Nichido	モデレーター：赤石 浩一（東京海上日動火災保険 顧

Fire Insurance Advisor) Panelists: - Akira Sakaino (NTT Communications) - Taka Matsutsuka (Senior Research Director, Data & Security Research Laboratory, Fujitsu Research) - Christoph Mertens (Head of Adoption, International Data Spaces Association) - Ulrich Ahle (CEO, Gaia-X European Association for Data and Cloud AISBL)	問) パネリスト： - 境野 哲 (NTT コミュニケーションズ エバンジェリスト) - 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) - クリストフ・メルテンズ (International Data Spaces Association 採用部門責任者) - ウルリッヒ・アーレ (Gaia-X European Association for Data and Cloud AISBL CEO)
Overview This speech summarizes the panel discussion on trusted data distribution held on November 1, 2024. It includes presentations from key figures in the data space industry, discussions on challenges and solutions, and future collaboration steps. The action items section has been consolidated and moved to the end for clarity. **Introduction** • **Moderator**: Akaishi • **Panel Members**: ○ Ulrich Wahle, CEO of Gaia-X ○ Mr. Mertens, Head of Adoption, International Data Spaces Association (IDSA) ○ Dr. Matsutsuka, Senior Research Director, Fujitsu ○ Akira Sakaino, NTT Communications **Presentations** **Gaia-X Overview** • **Latest Developments**: ○ GAIA-X announced NTT Data as the first installation in Japan, along with Tokyo University, SoftBank, and Toshiba. ○ Trust anchors include digital IDs such as wallets, driver's licenses, passports, and airline alliances. ○ GAIA-X Academy offers a 10-course program explaining the basics of GAIA-X. ○ Upcoming GAIA-X Summit in Helsinki, Finland on November 14th and 15th. **International Data Spaces Association**	データ流通, Gaia-X, データガバナンス **テーマ** この講演では、データ流通の信頼性を高めるための Gaia-X の役割やインターナショナルデータスペースアソシエーションの活動について議論されました。データエコシステムの構築やデータガバナンス法、データスペースの相互運用性、デジタルプラットフォームの重要性が取り上げられ、データセキュリティやテレコムキャリアの役割も考察されました。 **要点** 1. データ流通の信頼性 2. Gaia-X の役割 3. インターナショナルデータスペースアソシエーションの活動 4. データエコシステムの構築 5. データガバナンス法 6. データスペースの相互運用性 7. デジタルプラットフォームの重要性 8. データセキュリティ 9. テレコムキャリアの役割 10. データエクスチェンジの専門性 **ハイライト** • "データはレインボーに流れません。"-- ウルリヒ・アーレ • "データスペースを国境を越えて使おうとすると様々な問題があり、ユーザー企業が自分でシステムを作り運用するのは非常に難しいと考えています。" • "国内ではユニフィケーションしつつ、国際的にはフェデレーションをしようというような方向で進められると非常にいいんじゃないかなと思っております。" **章とトピック** **Gaia-X** Gaia-X はヨーロッパにおけるデータ連携のためのプラットフォー

- **Historical Context**:
  - Established in 2016 to support the data economy through data sharing.
- **Core Assets**:
  - IDS reference architecture, recognition, testbeds, and protocols.
  - IDS rulebook for data usage.
- **Applications**:
  - Examples include Japan's Channel and Data Performance Connector.
- **Data Space Protocols**:
  - Emphasis on trust services and identity.
  - Importance of standardized data sharing and exchange.

Trust Interoperability

- **Data Space Trust Framework**:
  - Trust is related to participants and objects.
  - Legal frameworks and technical differences pose challenges.
- **Proposals**:
  - Step-by-step approach to align trust frameworks across countries.
  - Roaming-like technology for data space exchange.
- **Collaborations**:
  - Fujitsu and NTT working together on trust frameworks and data space initiatives.

Practical Aspects of Data Space

- **Internationalization of Data Space**:
  - Importance of realizing a circular economy.
  - Need for common protocols and data sovereignty considerations.
- **Role of Telecom Carriers**:
  - Telcos can provide interoperable networks and manage cross-border data operations.
  - Telcos' resources can be utilized to ensure safe and secure data space usage.
- **Challenges**:
  - Different standards and rules across

ムであり、信頼できるデジタルエコシステムを開発することを目指している。

- **要点**
  - データ供給者と使用者をつなぐデジタルプラットフォーム
  - グローバルなデータスペースの創造
  - データガバナンス法、データ法、AI 法に基づくフレームワーク
- **説明**
  - Gaia-X は、データの相互運用性を確保するための技術的、組織的、法的な枠組みを提供し、データスペースの参加者を自動的に認識・承認する仕組みを持つ。
- **留意点**
  - 日本のエコシステムとの技術的な互換性
  - 地域的な政策の実現方法

インターナショナルデータスペースアソシエーション（IDSA）

IDSA は、データエコノミーにおけるデータ共有のためのスタンダードを作成する非営利組織である。

- **要点**
  - データスペースの設計
  - 信頼できるプラットフォームの提供
  - データ共有のためのアーキテクチャとプロセス
- **説明**
  - IDSA は、データスペースの運営に必要な技術基準やプロセスを提供し、国際的な標準化活動を推進している。
- **留意点**
  - 国際的な標準化の重要性
  - データスペースのエコシステムにおける信頼の確保

データスペースの 4 層構造

データスペースはテクニカル、セマンティカル、オーガニゼーショナル、リーガルの 4 つの層で構成されており、これらがデータの流通と信頼性を支える。

- **要点**
  - テクニカル層は技術的な基盤を提供
  - セマンティカル層はデータの意味を統一
  - オーガニゼーショナル層は組織間の調整を行う
  - リーガル層は法的な枠組みを提供
- **説明**
  - これらの層はデータの流通を円滑にし、信頼性を確保するために必要な要素である。

countries.

- Need for mutual recognition of credentials and trust frameworks.

Discussion and Q&A

Challenges and Solutions

- **Integration of Other Economies**:
  - GAIA-X and IDSA need to integrate economies like the U.S. to achieve their goals.
  - Differences in laws and regulations pose significant challenges.
- **Technical and Business Aspects**:
  - Importance of showing ROI to gain interest from businesses, especially in the U.S.
  - Need for interim solutions while waiting for legal reforms.

Collaboration and Future Steps

- **Global Collaboration**:
  - Importance of mutual recognition standards for data flow between Japan, EU, and the U.S.
  - Need for cooperation among government, academia, and industry.
- **Japanese Ecosystem**:
  - Positive direction with activities supported by NTT, Fujitsu, and other players.
  - Keidan Ren's proposal for industry collaboration on data platforms.

Action Items

[ ] Participate in the GAIA-X Summit in Helsinki, Finland on November 14th and 15th.

[ ] Work on aligning trust frameworks across different countries.

[ ] Develop interim solutions for data exchange while waiting for legal reforms.

[ ] Foster cooperation among government, academia, and industry for global data sharing.

データフリーフロー・ウィズ・トラスト

データの自由な流通を信頼性と共に実現するための概念。

- **要点**
  - データの流通を促進
  - 信頼性を確保
  - IDSA ルールブックに基づく
- **説明**
  - データの自由な流通を実現するためには、信頼性の確保が不可欠であり、IDSA ルールブックがその基盤となる。

トラストインターオペラビリティ

異なるデータスペース間での信頼性を確保し、データの相互運用性を実現するための取り組み。

- **要点**
  - クロスボーダーデータ流通の実現
  - トラストの相互流通
  - 法制度の違いを吸収
- **説明**
  - 異なる地域や国のデータスペース間でデータを安全に流通させるためには、信頼性の相互運用性が必要である。

イントロポリビリティと国際的な視点

イントロポリビリティは、異なるシステムや組織が協力して機能する能力を指し、国際的な視点を持つことが重要である。

- **要点**
  - イントロポリビリティは国際的な協力を促進する。
  - 地域市場に基づいたアプローチが必要。
- **説明**
  - イントロポリビリティを高めるためには、国際的なスタンダードゼーションを推進し、地域市場に適したアプローチを取ることが重要である。
- **留意点**
  - 国際的な視点を持つことが、地域市場での成功に繋がる。

テクノロジーとビジネスの関係

テクノロジーはビジネスの課題を解決する手段であり、ビジネスの成功にはテクノロジーの効果的な活用が必要である。

- **要点**
  - テクノロジーはビジネスの課題解決に役立つ。
  - KPI とインベストの回収が重要。
- **説明**
  - テクノロジーを活用する際には、ビジネスの KPI を設

	定し、投資の回収を考慮することが重要である。 • **留意点** ○ ビジネスの成功にはテクノロジーの効果的な活用が不可欠。 **宿題と提案**

3.17 D3-S6 Speech: International Mutual Recognition and ID Wallet

Vicente ANDREU NAVARRO (EU Commission, DG CNECT)	ビセンテ・アンドレウ・ナヴァロ (EU Commission, DG CNECT)
Overview This speech provides a comprehensive overview of the European Digital Identity Framework, including its implementation, governance, and international cooperation. It details the European Digital Identity Wallet, trust services, eID schemes, and new trust services added to the ecosystem. The document also outlines strategic partnerships and mutual recognition processes for trust services. Action items are listed at the end to guide further steps in the implementation and cooperation efforts. **Introduction to the European Digital Identity Framework** • The European Digital Identity Framework came into force in May 2021, amending the previous regulation from 2014. • Main improvements: ○ Ensures acceptance of qualified trust services in the EU under equal conditions. ○ Provides a highly secure, trustworthy electronic identity solution for cross-border use. **European Digital Identity Wallet** • The wallet allows citizens to carry their digital identity across the EU, maintaining control of their data with privacy and security at the core. • Ensures public and private services can rely on trusted and secure digital identity solutions. • Empowers users to share identity data limited to the needs of specific services.	**Overview** この講演は、ヨーロッパデジタルアイデンティティフレームワークの紹介、新しいフレームワークの構築、トラストサービスの国際協力に関する情報を含んでいます。内容は 2024 年 11 月 1 日に作成されました。 **ヨーロッパデジタルアイデンティティフレームワークの紹介** **フレームワークの概要** • **施行日**: 2021 年 5 月 • **改正内容**: 2014 年に施行された規制を改正 • **主な改善点**: ○ クオリファイドサービスのシステムに関して EU において平等の条件を提供 ○ 加盟国において正確なヘッドワークを提供 **トラストサービス** • **定義**: 一連の電子サービスとして、セキュリティ、プライバシー、信頼性を提供 • **機能**: ○ 電子データの記憶 ○ リモートな電子証明の管理 ○ デバイスの管理 **デジタルフレームワークの水準** • **高いアシュアランスを提供** • **共通スペック**: ○ ユーギュラリティウォレットとして実施法において法的な条文を採用 **新しいフレームワークの構築** **法的およびガバナンスの脅威** • **新しいフレームワークの目的**: 法的およびガバナンスの脅威に対応 **国際的な側面** • **EU の目標**: デジタル的に安全でセキュアなデジタルアイデンティティソリューションの開発 • **域外協力**:

Trust Services

Definition and Scope

- Trust services provide security, privacy, and reliability for electronic transactions.
- The regulation includes:
  - Recording of electronic data in an electronic ledger.
  - Management of remote electronic signature creation devices.

Assurance Levels

- The new framework requires a high assurance level for digital identity schemes.
- Three levels of assurance: low, substantial, and high, each with specific criteria and functional requirements.

eID Schemes

- EU member states must notify the Commission about their eID schemes.
- The regulation establishes a framework for mutual recognition of electronic identification means and trust services across EU member states.
- Conditions for recognition of electronic identification means from other member states are laid down to facilitate cross-border interoperability.

Implementation and Governance

Legal and Governance Framework

- Development of secondary regulation and implementing acts with technical specifications for building the wallet and trust services.
- Establishment of a governance framework involving all member states and other stakeholders.

Technical and Testing Initiatives

- Standardization and harmonization initiatives.
- Large-scale pilots for testing the EU Digital Identity Wallet.
- Integration with trust services.
  - 戦略的なパートナーシップ
  - パイロットプロジェクトや POC を通じた実施
  - 日本との協力（特に慶應基塾大学との協力）

トラストサービスの国際協力

新しいトラストサービス

- **追加されたサービス**:
  - 電子アーカイブ
  - 適格電子署名の電子保存
  - 属性の電子署名
  - リモート適格署名作成デバイスの管理

国際協力路線

- **相互認証**: EU 域内で提供
- **ツールの開発**: 他国の電子署名のトラストリストに含まれる

作業計画に関する要求

- **技術的評価**: EU の諸国は第三国で生成された電子証明について技術的評価を提供
- **将来の展望**: 適格サービスの承認に向けた前進

次のパネル

- **次のパネル**: 午後の 2 番目のパネルに移行

Action Items

[ ] 次のパネルの準備

International Cooperation **Strategic Partnerships** • Cooperation outside the EU is based on strategic partnerships, dialogues, and information exchanges. • Implemented through pilot projects and proof of concepts, such as collaborations with Japan and Keio University. **Mutual Recognition of Trust Services** • The new framework facilitates mutual recognition of qualified trust services. • Tools for mutual validation of non-qualified trust services, such as the third countries advanced electronic signatures list. **New Trust Services** • New trust services added to the existing ecosystem include: ○ Electronic archiving. ○ Electronic preservation of qualified electronic signatures. ○ Electronic attestations of attributes. ○ Electronic ledgers. ○ Management of remote qualified signature and seal creation devices. **International Cooperation Lines on Trust Services** **Mutual Recognition Process** • Based on equivalence between services provided outside the EU and qualified services within the EU. • Legal decisions can be taken through international agreements or implementing acts by the EU Commission. **Non-Qualified Trust Services** • Initiative to provide eIDAS-compliant tools for validating electronic signatures and seals from outside the EU. • The third countries advanced electronic signatures trust list facilitates validation without the need for international agreements or implementing acts.	

Steps Towards Mutual Recognition • Inclusion in the third countries trust list is a step towards mutual recognition of qualified trust services. • Technical assessment by the Commission adds value and facilitates future mutual recognition. **Action Items** • Develop secondary regulation and implementing acts with technical specifications. • Conduct large-scale pilots for testing the EU Digital Identity Wallet. • Establish a governance framework involving all member states and stakeholders. • Continue strategic partnerships and pilot projects for international cooperation. • Implement tools for validating non-qualified trust services from outside the EU.	

3.18 D3-P7 Panel: International Mutual Recognition for Trust Service

Moderator: Hiroshi Nakatake (Managing Director, Representative of the Japan Office, GLEIF) Panelists: - Takahiro Fujishiro (Senior Director, Hitachi, Ltd., Government & Public Corporation Information Systems Division, Business Innovation Operation) - Vikas Panwar (Country Business Manager for India, GLEIF) - Jean-Emmanuel Perez Hernandez (External Subject Matter Expert at the European Commission) - Akira Nishiyama (Representative, Future Trust Lab)	モデレーター：中武 浩史（GLEIF Managing Director 日本事務所代表） パネリスト： - 藤城 孝宏（日立製作所 公共システム事業部 公共ビジネスイノベーション本部 担当本部長） - ヴィカス・パンワル（GLEIF インド担当国別事業責任者） - ジャン＝エマニュエル・ペレス・エルナンデス（欧州委員会の外部専門分野エキスパート） - 西山 晃（フューチャー・トラスト・ラボ 代表）
Overview This speech provides a comprehensive summary of discussions and presentations from a meeting held on November 1, 2024. Key topics include international mutual recognition, trust	インターナショナル・ミューチャル・レコグニション・トラストサービス, DFFT, トラストアンカー **テーマ** この講演では、インターナショナル・ミューチャル・レコグニション・トラストサービスの重要性とサイバースペースでの安全なデータ

architecture, interoperability, and the Japan-EU digital partnership. The document also outlines use cases, such as carbon footprint data exchange, and compares trust frameworks between Japan and the EU. Action items are listed at the end for follow-up. **Introduction** • Mr. Takahiro Fujishiro, General Manager of Public Business Innovation, and Takahiro Fujishiro from the Power System Division of Hitachi, were introduced as today's panelists. **G7 Takasaki Meeting and International Recognition** • Discussion on the G7 Takasaki meeting and the concept of Data Free Flow with Trust (DFFT) proposed by the Japanese government in 2019. • Emphasis on mutual recognition and coordination with EU member nations to facilitate smoother business activities. • Systems, technology, architecture, and data models are being developed to raise feasibility into practice. **International Mutual Recognition** • Four points to consider for international mutual recognition, focusing on legal requirements, technical standards, and trust anchor standards. • Importance of a common authority for certification and the challenges of integrating different schemes. **Trust Architecture and Interoperability** • **3D, 3-Layered Architecture**: ○ **Top Layer**: Trust application services for handling. ○ **Middle Layer**: Trust data distribution layer for communication between participants. ○ **Bottom Layer**: Trust service infrastructure layer with electronic signatures and authentication.	伝送について議論されました。ヨーロッパ、インディア、ジャパンの協力を通じて、POC とのディスカッションやテクノロジースタンダードの比較が行われました。また、データフリーフルーズとフローウィズトラスト（DFFT）の概念や日本と EU のデジタルパートナーシップ、トラストアンカーディスクロージャーの重要性についても触れられました。 **要点** 1. インターナショナル・ミューチャル・レコグニション・トラストサービスの重要性 2. サイバースペースでの安全なデータ伝送 3. ヨーロッパ、インディア、ジャパンの協力 4. POC とのディスカッション 5. テクノロジースタンダードの比較 6. G7 デジタル・ミニスターミーティング 7. データフリーフルーズとフローウィズトラスト（DFFT） 8. 日本と EU のデジタルパートナーシップ 9. トラストアンカーディスクロージャー 10. PKI システムとトラストアンカー **ハイライト** • "Interoperability does not mean uniformity." **章とトピック** **インターナショナル・ミューチャル・レコグニション・トラストサービス** サイバースペースで安全・セキュアなデータ伝送を達成するための国際的なフレームワーク。ヨーロッパ、インディア、ジャパンが協力して設立し、POC とのディスカッションを続けている。 • **要点** ○ 安全なデータ伝送のための国際的な協力 ○ POC との継続的なディスカッション ○ テクノロジースタンダードの比較 **データフリーフルーズとフローウィズトラスト（DFFT）** データの自由な流通を信頼を持って行うための概念。日本政府が 2019 年に提案し、EU とのデジタルパートナーシップの一環として進められている。 • **要点** ○ データの自由な流通と信頼の確保 ○ 日本と EU のデジタルパートナーシップ **トラストアンカーディスクロージャー** PKI システムにおける最終的な信頼点であるトラストアンカーの公開と信頼性の確保。異なるドメイン間での信頼性を確保するために重要。

- Simple demonstration scenario based on communication between data providers and consumers.

Use Case: Carbon Footprint Data Exchange

- European manufacturers request carbon footprint data from Japanese suppliers using a trust infrastructure.
- Verification of inquiries, preparation of data, and transmission through Japanese and EU trust systems.

Trust List and Cross-Certification

- **Phase 1**: Verification paths for Japanese and EU certificates.
- **Phase 2**: Use of a simulated bridge certificate authority for cross-certification.
- Inclusion of overseas trust lists and confirmation of feasibility.

PKI Infrastructure and Applications

- PKI infrastructure for public applications like tax reporting and electronic printing.
- Use of Unified Payment Infrastructure (UPI) for digital proofing and transactions.

Japan-EU Trust Framework Comparison

- EU Qualified SSCD components include Address Format, Qualified TSP, Qualified Certification, and Qualified Standard.
- Verification of security requirements, identification profiles, devices, and formats.

Accreditation Criteria and Mapping

- Detailed survey report on accreditation criteria.
- Comparison of projects in Japan and other countries across five categories.

Action Items

[ ] Review the YouTube demonstration of the trust list process.

[ ] Further investigate the integration of different trust schemes.

[ ] Continue mapping and comparing

- **要点**
  - PKI システムとトラストアンカー
  - 異なるドメイン間での信頼性の確保

3 レイヤーのアーキテクチャー

DFFT を実装するための 3 つのレイヤー構造。トラストアプリケーション、トラストデータディストリビューション、トラストサービスの各レイヤーでインターフィラビリティを検討。

- **要点**
  - トラストアプリケーションレイヤー
  - トラストデータディストリビューションレイヤー
  - トラストサービスレイヤー

インドのデジタル・パブリック・インフラストラクチャー（DPI）

インドの DPI は、経済をプレゼンスレス、ペーパーレス、キャッシュレスにすることを目指している。

- **要点**
  - デジタル・パブリック・インフラストラクチャーは、個人識別番号（Aadhaar アーダール）を含む。
  - デジタルシグネチャーの利用が進んでいる。

G20 デジタルエコノミーワーキンググループと DPI インフラストラクチャーサミット

G20 のサイドイベントで、DPI に関する洞察に満ちた議論が行われた。

- **要点**
  - PKI for DPI に関するパネルディスカッションが行われた。
  - 日本の DFFT イニシアティブが紹介された。

日本の電子署名法と EU の eIDAS 規制

日本と EU の電子署名に関する技術標準の相互認識を目指している。

- **要点**
  - 日本の電子署名法は、e-Signature Act に基づいている。
  - EU の eIDAS 規制との違いがある。

宿題と提案

international trust standards.	

3.19 D3-S10 Speech

Yasuhiko TANIWAKI (Member of the Board, Executive Vice President, IIJ)	谷脇 康彦（株式会社インターネットイニシアティブ 取締役副社長執行役員）
Overview This speech outlines the discussions and decisions made during a meeting focused on data integration and distribution. Key topics include the importance of data accuracy, the functionality of data integration layers, and potential collaboration opportunities. Action items have been consolidated and placed at the end for clarity. **Data Integration and Distribution** **Importance of Data Accuracy** • Emphasized the critical need to maintain accuracy in data distribution. • Highlighted the role of accuracy in ensuring trust in data handling processes. **Data Integration Layer** • **Connector Functionality**: ○ Discussed plans to implement a connector function to facilitate data connections. ○ This function will support various application services that connect data within different communities. • **Projects and Initiatives**: ○ Mentioned ongoing projects like Gaia-X in Europe and Data-EX by DSA in Japan. ○ These projects aim to enhance data integration and distribution frameworks. **Collaboration Opportunities** • Expressed the possibility of collaborating with Japan on similar data integration projects. **Action Items** [ ] Explore potential collaboration opportunities with Japan on data integration projects.	**Overview** この講演は、データ駆動社会への移行に関する議論をまとめたもので、データ法の準備、データインフラストラクチャー、文化財産とデータスペース、政府の政策、グローバルな協力、データ管理戦略などのトピックを扱っています。特に、データリンクプラットフォームの開発、トラストサービス環境の構築、国際的な合意の推進、インターネット標準化の重要性が強調されています。アクションアイテムとして、これらの分野での具体的な取り組みが提案されています。 **データ駆動社会への移行** **データ法の準備と実施** • 日本はデータ法、データガバナンス法、AI 法の施行に向けた準備を進めているが、実施は困難。 • データ駆動社会の実現には、ヨーロッパ諸国から学ぶことが重要。 • サイバーセキュリティはデータの機密性、可用性に加え、データの整合性が新たな焦点。 **データインフラストラクチャーとリンク** • GAIA-X イニシアティブでは、ターミナル、ネットワーク、プラットフォーム、データリンクの 4 層構造を提案。 • データリンクは新たな焦点であり、データフローの効率化が求められる。 **文化財産とデータスペース** **データスペースの定義とレイヤー** • データスペースに関する定義は組織間で異なり、ミスコミュニケーションを引き起こす可能性。 • データインテグレーションレイヤーとトラストサービスレイヤーが重要で、特にデータインテグレーションレイヤーはコネクタ機能とアプリケーションサービスを提供する必要がある。 **トラストサービスレイヤー** • トラストサービスレイヤーはデータの信頼性を提供するために、データブロックレッジとクリアリングハウスが必要。 **政府の政策とデータ管理** **データリンクプラットフォームと政策支援**

	• データをリンクするプラットフォームが必要で、政府の政策支援が強化される。 • EU のデータ管理法に基づき、日本版のデータ販売法が検討されている。 **データトラストフレームワーク** • データトラストフレームワークについては、国際的なコンセンサスと定義が必要。 • トラストサービス環境の開発が求められ、ヨーロッパのデジタル ID ウォレットの開発も必要。 **グローバルな協力と標準化** **国際的な合意と協力** • G7 や G20 の DFT において、グローバルな国際合意が必要。 • 日本と EU のトラストサービスは、国際的な合意を基に信頼のサービスを構築する必要がある。 **インターネットの標準化** • インターネットの標準化は特に重要で、日本の企業と政府は戦略的に取り組む必要がある。 • ASEAN 諸国との協力が求められ、データを活用して課題を解決する。 **データ管理と経済安全保障** **データ管理戦略の提供** • データ管理の戦略が発表され、経済安全保障が強化される。 • 関係者との関係を深め、効率的なイニシアティブを作成することが重要。 **アクションアイテム** [ ] データリンクプラットフォームの開発と政府の政策支援の強化 [ ] トラストサービス環境の開発とデジタル ID ウォレットの導入 [ ] グローバルな国際合意の推進とトラストサービスの構築 [ ] インターネット標準化の推進と ASEAN 諸国との協力強化

3.20 D3-S8-1 Final Closing

Barbara Grewe	バーバラ・グルーイ
Overview This speech provides a comprehensive overview of interconnected security paradigms, focusing on national, economic, and societal security. It	**Overview** この講演は、2024 年 11 月 1 日に作成された会議議事録の概要です。国家、経済、社会の安全保障に関する議論が行われ、特にサイバーセキュリティの重要性や協調と情報共

highlights the integration of cybersecurity into various sectors and the importance of collaborative efforts between government and industry. The document emphasizes the need for unity and collective action to address cybersecurity challenges effectively. **Interconnected Security Paradigms** **National, Economic, and Societal Security** • **Distinct Lenses**: Traditionally, national security is viewed through a protection lens, economic security through a monetary lens, and societal security through a paternal lens. • **Intertwined Responsibilities**: There is growing recognition that these security responsibilities are interconnected and need coordination. A new security paradigm has emerged, creating both opportunities and challenges. • **3D Glasses Analogy**: Viewing these securities together, like wearing 3D glasses, allows for a comprehensive understanding of global events. **Cybersecurity Challenges and Strategies** • **Cybersecurity Integration**: Cyberspace is increasingly integrated into the real world, impacting politics, society, economy, and culture. Cyberattacks, including state-sponsored ones, pose significant threats. • **Historical Context**: China's 2015 cybersecurity strategy acknowledged the integration of cyberspace and its potential for disruption. • **Current Initiatives**: Discussions included active cyber defense, improving cyber intelligence sharing, using government cloud services, and strengthening cyber contingency planning in the Asia-Pacific region. **Collaborative Efforts and Partnerships** **Government and Industry Collaboration**	有の必要性が強調されています。アクションアイテムとして、サイバーリスクへの対応やクリティカルインフラの防衛が挙げられています。 **国家、経済、社会の安全保障** **経済と社会の安全保障の統合** • 過去 3 日間にわたり、国家の安全保障、経済、社会の安全保障について議論が行われた。 • 経済と社会の安全保障は実際の世界では一体であり、責任は相互に絡み合っているため、コーディネーションが必要。 • 国と経済のセキュリティは、両方を進める形で推進する必要がある。 **セキュリティのパラダイムシフト** • セキュリティのパラダイムが大きく変わり、新たなチャンスと課題が生まれている。 • 3D のガラスで全てのピクチャーを統合した形で見る必要がある。 **サイバーセキュリティの重要性** • 政府はサイバー力が国の経済や社会の安全保障に影響を及ぼすことを理解し、アプローチを変える必要がある。 • サイバーリスクに対して、政府、産業界、個人が責任を持ち、様々な側面から対応する必要がある。 **協調と情報共有** **パートナーシップとコラボレーション** • 林官房長官と小原さんが協調の重要性について言及。 • サイバーインテリジェンスの情報共有の重要性が強調された。 **サイバーコンティンジェンシープランニング** • アジア太平洋地域でのサイバーコンティンジェンシープランニングの必要性が議論された。 **クリティカルインフラとサイバーサプライチェーン** • クリティカルなインフラ防衛とサイバーサプライチェーンについての議論が行われた。 • 新たな政府の取り組みが進行中であるが、まだ解決策は見つかっていない。 **発言者** • 村井氏が継続して発言。 **Action Items** • サイバーリスクに対して、政府、産業界、個人が責任を持ち、様々な側面から対応する必要がある。

• **Senior Leadership Insights**: Leaders like Chief Cabinet Secretary Hayashi and White House Cyber Director Coker emphasized the shift from idea sharing to collaborative action. • **Panel Discussions**: Topics included improving critical infrastructure defenses and cyber supply chains, with new Japanese government initiatives highlighted. **Overcoming Fear and Building Unity** • **Deputy Chief of Mission's Warning**: The cyber realm is daunting, but fear can be mitigated through unity and collective action. • **Strength in Unity**: Better partnerships, information sharing, and collective action are essential to counter cyber threats effectively. **Action Items** [ ] Improve critical infrastructure defenses. [ ] Enhance cyber supply chain security. [ ] Strengthen cyber contingency planning in the Asia-Pacific region. [ ] Increase cyber intelligence sharing. [ ] Utilize government cloud services for better security.	• アジア太平洋地域でのサイバーコンティンジェンシープランニングの必要性が議論された。 • クリティカルなインフラ防衛とサイバーサプライチェーンについての議論が行われた。

3.21 D3-S8-2 Final Closing

Jun Murai	村井 純
Cybersecurity, Three Pyramids, Knowledge Sharing **Theme** The speech focused on the multifaceted nature of cybersecurity, emphasizing its impact on national, economic, and societal security. It introduced the concept of three security pyramids, each representing a different aspect of security, with operational activities at the base and governance at the top. The importance of merging these pyramids and sharing knowledge across different security domains was highlighted	サイバーセキュリティ，国家安全保障，経済安全保障 **テーマ** この講演では、サイバーセキュリティシンポジウムの重要性と、国家安全保障、経済安全保障、社会安全保障の 3 つのポイントについて議論されました。セキュリティの階層化や異なる分野間の協力と共有の重要性が強調され、将来の課題への取り組みが提案されました。これらのポイントを総合的に考慮することで、より強固なセキュリティ体制を構築することが可能です。 **要点** 1. サイバーセキュリティシンポジウムの重要性 2. 国家安全保障、経済安全保障、社会安全保障の

as crucial for effective cybersecurity. Continuous service, recovery, and collaboration were underscored as essential components for addressing future cybersecurity challenges, as discussed at the 14th International Cybersecurity Symposium.

Takeaways

1. Cybersecurity involves national, economic, and societal security.
2. The concept of three pyramids representing different security aspects.
3. Importance of merging and sharing knowledge across different security domains.
4. Operational activities form the base of the security pyramids.
5. Governance and decision-making are at the top of the security pyramids.
6. Continuous service and recovery are crucial in cybersecurity operations.
7. Collaboration and sharing of wisdom are essential for effective cybersecurity.
8. The symposium emphasized the importance of understanding different security perspectives.

Highlights

- "Sharing it and viewing from the three different points of view is the only way that we do have a kind of strong challenge for the future of cybersecurity."--《14th International Cybersecurity Symposium》

Chapters & Topics

Three Pyramids of Security

The concept of three pyramids representing national, economic, and societal security in cybersecurity.

- **Keypoints**
  - National security focuses on protecting a nation's critical infrastructure and information.
  - Economic security involves safeguarding financial systems and economic interests.

3 つのポイント

3. ピラミッド構造によるセキュリティの階層化
4. 異なる分野間の協力と共有の重要性
5. サイバーセキュリティの将来の課題への取り組み

ハイライト

- "その 3 つを総合的に一緒にして、3 つの分野でそれぞれいろんな議論を行うということが重要です。"

章とトピック

サイバーセキュリティの 3 つのポイント

サイバーセキュリティにおける国家安全保障、経済安全保障、社会安全保障の３つの重要なポイントについての説明。

- **要点**
  - 国家安全保障：国の安全を守るためのサイバーセキュリティ対策。
  - 経済安全保障：経済活動を保護するためのサイバーセキュリティ対策。
  - 社会安全保障：社会全体の安全を確保するためのサイバーセキュリティ対策。
- **説明**
  - これらの３つのポイントは、サイバーセキュリティの基盤を形成し、それぞれが独立しているが、相互に関連している。これらを総合的に考慮することで、より強固なセキュリティ体制を構築することができる。
- **留意点**
  - 各分野の専門家との協力を強化する。
  - 情報共有のプラットフォームを構築する。
  - セキュリティ対策の継続的な見直しと改善を行う。
- **特別な状況**
  - 異なる分野間での意見の相違が生じた場合、どのように調整するかを事前に決めておく。

宿題と提案

○ Societal security addresses the protection of social structures and public safety. • **Explanation** ○ The speech explained that each pyramid operates independently with its own operational base and governance at the top. However, merging these pyramids and sharing knowledge across them is crucial for effective cybersecurity. • **Considerations** ○ Ensure continuous service and recovery in cybersecurity operations. ○ Facilitate collaboration and knowledge sharing across different security domains. **Assignments & Suggestions**	

4 DAY 2: October 31 | North Building 1F North Hall

4.1 D2-T1-S1 Hitachi

Hitachi Title: What Does Effective Security Risk Visualization Look Like Today? Moderator: Osamu Ishihara (Senior chief Engineer, Managed & Platform Services Business Division, Cloud Services Platform Business Unit, Hitachi, Ltd.) Panelists: - Yuichi KATO (Deputy Director of the Cybersecurity Division, Commerce and Information Policy Bureau, Ministry of Economy, Trade and Industry (METI)) - Mikiya Tani (Senior Professional, Global Innovation Strategic Division, NEC Corporation)	日立 タイトル：今、必要なセキュリティリスクの見える化とは？ モデレーター：石原 修（株式会社日立製作所 クラウドサービスプラットフォームビジネスユニット マネージド＆プラットフォームサービス事業部 主管技師長） パネリスト： - 加藤 優一（経済産業省 商務情報政策局 サイバーセキュリティ課 課長補佐） - 谷 幹也（日本電気株式会社 グローバルイノベーション戦略統括部 シニアプロフェッショナル）

Overview

このドキュメントは、セキュリティリスクの見える化、サイバーセキュリティの現状、製品セキュリティと認証制度、ソフトウェアの部品構成表（SBOM）、ソフトウェアセキュリティと企業の取り組み、IoT の推進と政府の期待、セキュリティダッシュボードの導入と課題、セキュリティと自動化の重要性、セキュリティと法制度の課題、サプライチェーンとコストの見える化に関する議論をまとめたものです。各セクションでは、政府や民間企業の視点、国際的な動向、具体的な取り組み事例が紹介されています。最後に、これらの議論を基にしたアクションアイテムがまとめられています。

セキュリティリスクの見える化

背景と目的

- **目的**：経済安全保障推進法やレジデンスアクトなどの法律に基づき、サプライチェーン全体のセキュリティリスクを見える化する必要性が高まっている。
- **経緯**：多くの法律や規制により、リスク管理措置が細かく求められる状況にあり、技術的な対策だけでなく、調達先を含めた状況の見える化が必要。

パネリストの視点

- **政府視点**：経済産業省サイバーセキュリティ課の加藤氏が、サイバーセキュリティを取り巻く現状を紹介。
- **民間視点**：日本電気の谷氏が、民間企業の視点からコメント。

サイバーセキュリティの現状

サイバー攻撃の主体と目的

- **多様な主体**：国家グループ、ビジネス目的のグループ、産業スパイなど、多様な主体が存在。
- **攻撃の目的**：情報の流出、金銭の盗難、意思決定の歪曲、事業停止、社会インフラへの影響など。

世界的な法規制の動向

- **米国**：重大なインシデントに対する報告義務。
- **欧州**：サイバーレジリエンスアクト法案により、製品のセキュリティを強化。

製品セキュリティと認証制度

日本の取り組み

- **IoT 製品の認証制度**：ルーターやネットワークカメラなどを対象に、段階的な認証制度を導入予定。
- **段階性**：基礎的なレベルから高い基準まで、業界や機器の特性に応じて認証を進める。

国際的な取り組み

- **諸外国の動向**：シンガポール、イギリス、米国、EU でも同様の取り組みが進行中。
- **総合認証**：シンガポールと英国、欧米との調整を進め、方向性を提示予定。

ソフトウェアの部品構成表（SBOM）

SBOM の重要性

- **目的**：ソフトウェアの部品構成を事前に管理し、脆弱性を含むコンポーネントの特定を容易にする。
- **ガイドライン**：経済産業省がガイドラインを公表し、取り組みやすい環境を整備。

国際協力

- **クアッド外国会合**：日米、オーストラリア、インドの首脳会談で、サイバーセキュリティの共同原則を発表 SBOM やサプライチェーンについても言及。

ソフトウェアセキュリティと企業の取り組み

ソフトウェアセキュリティの国際的動向

- **第 6 回会合の開催**：9 月 21 日に開催され、ソフトウェアのセキュリティについての連携を継続することが宣言された。
- **企業のセキュリティ基準**：企業に一定の基準を示し、その基準を守るかどうかを自己判断または第三者認証で確認する動きが活発化。

サプライチェーンのセキュリティ

- **発注者側の不安**：サプライヤーが供給を停止すると事業が停止するリスクがあるため、監査や手助けを行う企業も存在。
- **サプライヤー側の課題**：多様な基準に対応する必要があり、星評価（3，4，5 星）などの基準設定が議論されている。

セキュリティ基準の詳細化

- **ビジネス観点とシステム観点**：サプライチェーンにおける企業の責任とネットワーク接続の重要性が強調される。
- **基準の検討**：30～50 項目の基準を設定し、達成度を測る制度を検討中。

民間企業の取り組み

NEC の事例

- **サプライチェーンガバナンス**：人権、労働、安全衛生、環境、品質、安全性、情報セキュリティ、公正取引、倫理の 6 項目を取引先に確認。
- **デューデリジェンスの実施**：書類点検と訪問点検を繰り返し、75%の目標を 86%まで達成。

情報セキュリティの見える化

- **情報セキュリティカルテ**：書類点検や訪問点検の結果をカルテ化し、各社の状況を公開。
- **オンラインとオフラインの統合**：サプライチェーンの状況をリアルタイムで把握し、滞留を防ぐ基盤を構築。

自社のサイバーセキュリティ

- **データドリブン経営**：セキュリティの弱点を特定し、グローバルに共通のポリシーで管理。
- **脅威と防御分析**：外部アタックやメールのリジェクト率を分析し、社内で展開。

セキュリティトランスフェアレンシングコンソーシアム

- **SBOM の活用**：セキュリティの透明性を確保し、データを提供する活動を開始。
- **知見書の発行**：可視化データの活用に関する課題を 8 つにまとめた知見書を発行。

IoT の推進と政府の期待

IoT の進展と政府の視点

- IoT の機器の範囲が広く、絞り込みが必要。

- 政府は主要産業や重要インフラに関わる企業に率先して取り組んでほしいと考えている。
  - **例:**米国では政府調達が市場を盛り上げるが、日本では規模が小さいため、民間企業の役割が重要。
- 自動車業界はセキュリティに関心が高く、サプライチェーン全体に展開する動きがある。

民間企業への期待とアドバイス

- 政府は全企業に取り組んでほしいが、特に社会的責任を持つ企業に期待。
- 初期ターゲットとして自動車業界が挙げられ、ガイドラインに基づく評価が進行中。

セキュリティダッシュボードの導入と課題

導入の背景と目的

- 事故が多発し、社内の状況を見える化する必要性が高まった。
- 経営者層が状況を把握できるダッシュボードを作成。

導入の効果と課題

- ビジネスユニットごとの成績が見える化され、問題点が明確に。
- 経営者層の即断即決が可能になり、予算の確保が容易に。
- 全社員が状況を把握できるようになり、文化としての見える化が進展。

導入の困難と克服

- 防衛系などの業態では抵抗があったが、一部から始めることで突破口を見出した。
- 継続的な取り組みが理解を広げる鍵となった。

製品と国際的な認証

IoT 製品の認証と相互認証

- 日本で販売される製品には保証が必要。
- 海外での販売には相互認証が重要で、国際的な連携が求められる。

SBOM の導入と国際連携

- SBOM は共通仕様が前提で、国際的な連携が進行中。
- 海外では必須化が進んでおり、準備が必要。

継続性と予算の確保

セキュリティ活動の継続性

- キーマンの不在や痛い目を忘れることへの懸念。
- 予算は通常の状態で運営されており、継続的な取り組みが重要。

セキュリティと自動化の重要性

経営者の視点

- **危機感の認識**: 経営者層は、痛みが減少している一方で、世の中では増加していることを認識しており、予算を大幅に削減する考えはない。
- **自動化の推進**: 手作業を自動化し、AI を活用することで、研究開発や新しい取り組みへの資金を生み出している。

セキュリティと DX の関連性

- **コストと意義**: セキュリティ単体ではコストに過ぎないが、DX やコスト削減の取り組みと絡めることで意義が生まれる。
- **クライアントゼロの考え方**: NEC 内での成功事例を他社と共有し、伴走するソリューションを提供することを目指している。

見える化と教育のバランス

見える化の利点と課題

- **ガラス張りの重要性**: 経営者が自社内を見える化することが多いが、社員が中身を見れることは珍しい。
- **情報開示のリスク**: 社員教育を通じて、情報を第三者に開示しないようにする必要がある。

社員教育の重要性

- **教育とバランス**：社員が情報を適切に扱うための教育が必要であり、民度に合わせた対応が求められる。

今後の取り組みと技術の活用

セキュリティ対策の継続

- **コストの乗り越え**：セキュリティ対策はコストがかかるが、リスクマネジメントとして必須である。
- **企業への呼びかけ**：企業はリスクマネジメントの一環として、セキュリティ対策に取り組むべきである。

セキュリティと法制度の課題

- **現状の問題点**
  - セキュリティ対策は法制度や規制によって強制されることが多く、企業が自主的に資金を出す状況が少ない。
  - 特に中小企業や取引先が自主的に資金を出せる状況を作る必要がある。
  - 資金をどこかからプールして提供するメカニズムが必要と感じている。

サプライチェーンとコストの見える化

- **サプライチェーンの重要性**
  - サプライチェーンの調達先を含めた見える化が重要であるが、これもコストがかかる。
  - 経産省の企業セキュリティの見える化の取り組みがあり、調達を含めた見える化が求められている。
- **民間企業の役割**
  - 費用が発生することを前提に、民間企業も含めた施策を考える必要がある。
  - 見える化から見せる化へのステップが重要であり、これについても考えていく必要がある。

アクションアイテム

[ ] IoT 製品の認証制度の詳細を確認し、導入準備を進める。
[ ] SBOM ガイドラインに基づき、ソフトウェアの部品構成管理を開始する。
[ ] 企業のセキュリティ基準の詳細化に関する議論を継続する。
[ ] サプライチェーンのセキュリティ基盤の改善策を検討する。
[ ] セキュリティトランスフェアレンシングコンソーシアムの活動を推進する。
[ ] IoT の初期ターゲット業界の絞り込みと評価の進行
[ ] セキュリティダッシュボードの全社展開と文化の定着
[ ] SBOM の国際連携と必須化への準備
[ ] セキュリティ対策の自動化と AI 活用の推進
[ ] 社員教育を通じた情報管理の徹底
[ ] NEC の成功事例を他社と共有するためのソリューション提供

4.2 D2-T1-S2 Cisco

Cisco Title : The latest status of "economic security" and "national cyber security" that enterprise companies need to understand Moderator: Shigeru Kimura (Cyber Security Center of Excellence Japan / Security & Trust Office, Cisco Systems, G.K) Panelist: - Takahisa KAWAGUCHI (Head Consultant & Manager, Risk Management Dept. & Corporate	Cisco 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 モデレーター：木村 滋 (シスコシステムズ合同会社 セキュリティエバンジェリスト / セキュリティ&トラストオフィス) パネリスト： - 川口 貴久 (東京海上ディーアール株式会社 ビジネスリスク本部 兼 経営企画部 主席研究員 マネージャ) - 文字 勇 (シスコシステムズ合同会社 情報通信事業 業務執行役員 プリンシパルセールスアーキテクト)

Planning Dept., Tokio Marine dR) - Isamu MONJI (Principal Sales Architect, Service Provider Operations Cisco Systems, G.K)	

Overview

この文書は、経済安全保障とサイバー安全保障に関する講演の議事録をまとめたものです。内容は、経済安全保障推進法の施行と運用、特定重要設備の解釈、官民連携の強化、アクティブサイバーディフェンス（ACD）の導入、政府の中間整理案と自民党案、通信情報の利用、アクセス無害化、民間企業へのインサイト、経済安全保障推進法に関する意見、運用開始と今後の議論など、多岐にわたります。各セクションでは、関連する背景情報や議論のポイントが詳述されており、最後にアクションアイテムがまとめられています。

経済安全保障とサイバー安全保障の関連性

- **テーマ**: 経済安全保障とサイバー安全保障の最先端
  - 民間企業が理解すべき 2 つの安全保障について議論。
  - 現在のサイバーセキュリティ環境における 2 つの安全保障の関連性と影響を探る。
- **公開討論会**: インタラクティブな会話を通じて理解を深める。
  - QR コードを使用してアンケートを実施。
  - QR コードがない場合は、指定の URL とコードを使用して参加可能。
- **参加者の背景**:
  - システム運用に関わる方。
  - インテグレーター導入者。
  - 本制度に関連する方々。

司会とパネリストの紹介

- **司会者**: シスコシステムズの木村
- **パネリスト**:
  - **文字さん**: シスコ所属。通信事業のお客様と関わることが多く、経済安全保障推進法に関する専門家。
  - **川口さん**: 東京海上 DR 所属。リスクコンサルタントとして政治リスクや経済安全保障を担当。内閣官房サイバー安全保障分野の有識者会議メンバー。

経済安全保障推進法とサイバーセキュリティ

- **昨年の振り返り**:
  - 経済安全保障から見たサイバーセキュリティの位置づけを整理。
  - 内閣府の開設書を基に、今後の方針を予測。
  - 5 月に法律が制定され、運用が開始される状況。
- **特定社会基盤駅務の安定的な提供の確保**:
  - 2022 年に能動的サイバー防御が導入。
  - 2023 年 6 月から川口さんが参加する有識者会議での議論が開始。

特定社会基盤駅務の安定的な提供確保

- **文字さんの発表**:
  - 経済安全保障推進法の施行と運用開始後の制度理解。
  - 基幹インフラ制度に関する申請実務に携わり、制度理解を深める。
- **議論のポイント**:
  - 官民連携、通信の利用、無害化に関する議論。
  - アクティブサイバーディフェンスの最新動向。

文字さんのディスプレイ

- **基幹インフラ制度に関する説明**:
  - 4 本の柱のうちの 1 つである基幹インフラ制度に限定。
  - 施行運用開始後の制度理解と解釈の中心点を紹介。

シスコの役割と業界への貢献

- シスコは通信機器やサーバー製品の供給者として、いくつかの業界で事業者と協力し、申請プロセスを進めてきました。
- **制度の解釈と留意点**
  - シスコは業界の事業者に対して、制度の解釈や補足情報を提供しています。
  - 特に電気通信業界において、重要な留意点を共有しています。
- **電気通信業界への関与**
  - シスコは電気通信業界において、主に制度の解釈や留意点の提供に携わっています。

経済安全保障と基幹インフラ

- **経済安全保障の枠組み**
  - 経済安全保障の大きな枠組みの中で、基幹インフラの安定的な提供が重要視されている。
  - **基幹インフラの安定性**
  - 外部からの妨害行為が基幹インフラの安定的な運用や駅務の提供を脅かす可能性がある。
  - **リスクアセスメントの重要性**
  - 通信障害やサイバーアタックが消費者に与える影響を考慮し、インフラの強靭化を図るためのリスクアセスメントが必要。
- **施行日と運用開始**
  - 制度は昨年 11 月 17 日に施行され、運用は今年 5 月から開始された。
- **対象業種と事業者**
  - 現在、15 業種 213 事業者が指定されており、情報は内閣府や各省庁のページで更新されている。
- **課題の洗い出し**
  - リスクアセスメントを通じて、現在運用している基幹インフラの課題を洗い出す。
  - **見える化の効果**
  - 課題を見える化することで、どこにリスクがあるかを明確にする。
- **昨年の状況**
  - 制度施行前には、有識者会議の資料やパブリックコメントを基に議論が行われていた。
- **情報の更新**
  - 解説書等が頻繁に更新されており、最新情報が提供されている。

特定重要設備の解釈と構造

- **事業者の階層構造**
  - **社会基盤事業者**: 社会基盤を支える事業者。
  - **供給者**: シスコのような製品を供給する企業。
  - **維持管理委託先**: 維持管理や補修を行う委託先。
- **特定需要設備**: 指定された重要なシステム。
- **構成コンポーネント**: ネットワーク機器、サーバー設備、業務ソフトウェアなど。
- 各業種、業界ごとに特定重要設備が定められている。
- 14～15 業種が存在し、内閣府の構造に基づき各事業所管省庁が解説。
- 基本構造は共通だが、業種に応じた異なる対応が必要。
- 社会基盤事業者の特定重要設備とその構成設備、維持管理委託先の再委託が基本構造。

申請対象設備の選定

- **申請の必要性**
  - 重要なインフラは申請が必要。
  - 必要な情報を十分に揃えて申請することが求められる。
- **鉄道**：昨年の有識者会議での議論を基に、業務アプリケーション、オペレーションシステム、サーバー設備、通信回線装置が対象。
- **法施行後の整理**：11 月以降、業務アプリケーション、OS、ミドルウェア、サーバー装置に焦点を絞る。
- 業務アプリケーションやサーバー設備が外部からの脅威に対してどのように守られているかを重視。
- 脆弱性のあるソフトウェアや不審なものの混入を防ぐ。
- **金融・銀行業**：業務アプリケーション、OS、サーバー設備に重点。
- **その他の業種**：電気、ガス、水道、金融系（銀行、クレジットカード）も同様の重点を置く。

電気通信における特定重要設備の解釈

- **電気通信の特性**：電気通信は金融や銀行とは異なり、業務用ソフトウェアやノートデバイス、課金システムなどが重要視される。
- **特定重要設備の解釈**：通信機器そのものが特定重要設備とされ、OS ソフトウェアやハードウェアがその構成設備となる。
- **業界ごとの特性**：各業界はそれぞれの事業法に即した重要インフラを持つ。
- **システムの内製化**：オープンソースやパブリッククラウドの普及により、社会基盤事業者が自らシステムを開発するケースが増加。
- **申請の進展**：通信機器が特定需要設備とされる解釈が進展。
- **共通理解の重要性**：供給者、事業者、省庁間での共通理解が重要。

能動的サイバー防御（ACD）の導入

- **ACD の定義**：各国で異なる解釈があるが、基本的には防衛的な意味合いを持つ。
- **日本での展開**：2022 年 12 月に国家安全保障戦略で明言され、2023 年 6 月から具体化のための会議が開始。
- **官民連携**：政府と重要インフラ企業の連携が重要。
- **通信情報の活用**：日本国内を経由する通信情報を活用し、悪質なサーバーを無害化。
- **情報の報告と共有**：官から民への情報共有、民から官への報告義務化が議論されている。
- **報告義務化の課題**：義務化だけでは企業にインセンティブがなく、報告による面積の提供が必要。

政府の中間整理案と自民党案

- **インセンティブの提案**：制度を作るだけでなく、インセンティブを活用する提案があった。
- **報告窓口の一本化**：報告窓口を一本化し、形式を揃えることで情報サイクルを実効的にすることが論点。
- **基幹インフラ事業者の報告義務化**：特に重要な基幹インフラについては、政府へのリアルタイム報告を義務付ける提案。
- **特定重要設備の事前登録**：情報系システムの重要なものを事前に特定し登録することを提案。

官民連携の強化

- **基幹インフラの義務**：経済安全保障を強化するための基幹インフラの義務化。
- **クリアランス制度の活用**：経済安保の枠組みで整備されたクリアランス制度を活用する相互作用。

通信情報の利用

- **デジタル情報の収集**：日本国内を経由するデジタル情報を集め、サイバー攻撃を未然に防ぐ。
- **通信情報の範囲**：メタデータ以外の通信の本質的なコミュニケーション内容を収集し分析することが妥当。

アクセス無害化

- **無害化の必要性**：国内外のサーバーを含めた無害化の実施。
- **サイバー攻撃者の能力削減**：無害化や通信の遮断、C2 サーバーのテイクダウンを通じて攻撃者の能力を削ぐ。

民間企業へのインサイト

- **政策動向の追跡**：政策動向を追い、法令をキャッチアップすることが重要。
- **ビジネスインテリジェンスの必要性**：政策動向や背景にある国際情勢を理解し、リスク管理を行う。

経済安全保障推進法に関する意見

- **セキュリティ対策のガイドライン**：経済安全保障推進法がセキュリティ対策のガイドラインになることへの期待。
- **特定重要設備の簡素化**：特定重要設備の簡素化に対する意見や印象。

コメントと意見募集

- **法制度の要求と実際の対応**：法制度で要求されていない部分を放置しないことの重要性。

運用開始と今後の議論

- **運用開始の意義**
  - 事業者と供給者の意識が高まっている。
  - 1 年前の施行前に比べて、運用開始は大きな進歩。
  - 内閣府の資料によると、審査が長引くなどの課題もあるが、理解が進んでいる。
- **今後の改善と議論**
  - 制度の改善や改正が今後の議論の焦点となる。
  - よりスムーズな運用と幅の拡大が期待される。

アクティブサイバーディフェンス（ACD）

- **官民連携の重要性**
  - NISC の新組織の下、防衛省と警察庁が実行。
  - 官民連携が中心で、運用主体が誰になるかが議論の焦点。
- **民間側の役割**
  - 重要インフラや通信事業者、ソフトウェアベンダーが関与。
  - NISC を発展的に拡大する組織がリードし、民間事業者と協力して ACD を実現。

経済安全保障とサイバーセキュリティ

- **見える化とリスク管理**
  - 事業者でなくても、重要なシステムの見える化が必要。
  - 古い機器の使用などが脆弱性の対象になる可能性がある。
- **ビジネスインテリジェンスの重要性**
  - 経済安全保障とサイバー安全保障の強化が必要。
  - サプライズを防ぐために、情報をしっかりと取ってリスク管理を行う。

国全体の強靭化

- **情報発信と模範**
  - 国の意図を汲み取り、模範できるところは模範することが重要。
  - 積極的な情報発信を行い、ヒントを持ち帰ってもらうことを期待。

Action Items

[ ] QR コードまたは URL を使用してアンケートに参加する。
[ ] 経済安全保障推進法の施行後の制度理解を深めるための資料作成。
[ ] アクティブサイバーディフェンスに関する最新情報の共有。
[ ] 基幹インフラのリスクアセスメントを実施し、課題を見える化する。
[ ] 内閣府や各省庁のページを定期的に確認し、最新情報を把握する。

[ ] 特定重要設備の申請に必要な情報を揃える
[ ] 各業種に応じた特定重要設備の定義を確認する
[ ] 外部からの脅威に対する防御策を強化する
[ ] 各業界の特性に基づいた特定重要設備の解釈を進める。
[ ] 官民連携の強化と情報共有の仕組みを整備する。
[ ] 報告義務化に伴う企業のインセンティブを検討する。
[ ] 経済安全保障推進法に関する具体的なガイドラインの検討
[ ] 特定重要設備の簡素化に関する意見の収集と分析
[ ] 各インフラやシステムの見える化を進める。
[ ] ビジネスインテリジェンスを強化し、サプライズを防ぐための情報収集を行う。

4.3 D2-T1-S3 InterNational Cyber Security Center of Excellence (INCS-CoE)

InterNational Cyber Security Center of Excellence (INCS-CoE) Theme: INCS-CoE progresses and directions in international collaborations in research and training Moderator: Chris Hankin (Professor, Imperial College London, INCS-CoE Chair) Panelists: - Kazuo Noguchi (Sr. Researcher, Keio University) - David Luzzi (Senior Vice Provost, Northeastern University) - Karl Steiner (Vice President, University of Maryland Baltimore County) - Luiz DaSilva (Professor, Virginia Tech) - Konstantinos Mersinas (Associate Professor, Royal Holloway, University of London)(Invited) - Muhammad Salman (Head of Computer Engineering Study Program, University of Indonesia) - Rolando Martins (Assistant Professor, University of Porto) Language: English	InterNational Cyber Security Center of Excellence (INCS-CoE) タイトル：INCS-CoE の進展と研究・トレーニングにおける国際協力の方向性 モデレーター：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） パネリスト： - 野口 和男（慶應義塾大学上席所員） - 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（メリーランド大学ボルチモア校 副学長） - 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)(未定) - 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・マルティンス（ポルト大学助教授） 言語：英語

Overview

This document provides a comprehensive summary of recent developments, seminars, and initiatives related to cybersecurity across various universities and organizations. It highlights the activities of the INCS-CoE, including seminar series, research programs, and international competitions. The document also outlines the cybersecurity initiatives of the University of Indonesia and the University of Porto, emphasizing collaboration, research, and talent development. Action items are consolidated at the end for clarity and follow-up.

Introduction to INCS-CoE

- Chris Hankin, Professor at Imperial College London and current board chair, introduced the INCS-CoE panel.
- The panelists were introduced, and the session aimed to update on INCS-CoE's activities since the last cybersecurity symposium.

INCS-CoE Developments

- INCS-CoE was informally established around 2015-2016 and formally chartered in 2019 by six partner universities from Japan, the US, and the UK.
- Despite pandemic interruptions, the network has grown to 17 member universities, with recent additions including Virginia Tech, University of Surrey, University of Porto, University of Indonesia, and Tallinn University of Technology.
- The organization now includes a community of 41 experts and fellows, with expectations for rapid expansion.

Seminar and Research Programs

Seminar Series

- Seminars are held quarterly, lasting about 1.5 hours, and are open to all.
- Topics covered this year include:
  - Security of healthcare systems
  - Security challenges of next-generation energy distribution networks
  - Security challenges for democratic elections
- Upcoming seminar on December 11 will focus on the security of space systems.
- Future topics may include embedded medical devices, aviation, immersive technologies, and AI security.

Research and Policy

- INCS-CoE focuses on three pillars: research, policy recommendations, and education/training.
- The organization aims for international government-industry-academia partnerships to address cybersecurity challenges.

Capture the Flag (C2C) Competition

- The C2C competition is a Capture the Flag event held annually, involving global university students.
- The competition emphasizes ethics and international collaboration, with teams formed from different countries and universities.

Recent Developments

- Over the past five years, the competition has seen participation from 77 universities and 33 nationalities.
- The next competition will be hosted by Northeastern University in Boston in July 2025.
- Future hosts include the University of Indonesia and George Mason University.

Expert Community Panels

Security Challenges for Democratic Elections

- Held on September 11, the panel discussed electronic voting security amidst ongoing elections in Japan and the US.

- Key points included:
  - Voter coercion and protection against hacking (Vote XX system by Alan Sherman, UMBC).
  - Verification of electronic voting systems (Steve Schneider, University of Surrey).
  - Potential threats to the 2024 US election, including misinformation (David Lazor, Northeastern University).
  - Overseas voting challenges and solutions in Japan (Juasa Harumichi, Meiji University).

Introduction

- **Presenter**: Luis de Silva, Bradley Professor of Cybersecurity at Virginia Tech and Executive Director of the Commonwealth Cyber.
- **Organization**: Commonwealth Cyber, a consortium of 46 universities and colleges in Virginia focused on cybersecurity research, innovation, and workforce development.
- **Objective**: Collaborate globally in cybersecurity, joining INCS-CoE to enhance partnerships beyond Virginia.

Seminar Series Overview

- **Focus**: Protecting electricity distribution systems, relevant to the symposium's theme on economic security.
- **Keynote**: Mr. Kumar from the U.S. Department of Energy discussed hardening electricity distribution systems against cyberattacks.

Distributed Electricity Systems

- **Transition**: From centralized to distributed systems, increasing resilience against cyberattacks and natural disasters.
- **Renewables**: Integration of solar and wind energy introduces new vulnerabilities.
  - **Presenter**: Dr. Ali Mirazi-Sani from Virginia Tech discussed vulnerabilities and the role of 5G/6G in supporting distributed systems.

Electric Vehicles and Security

- **Presenter**: Dr. Dirsel Cavendish from Kyushu.
- **Topic**: Security vulnerabilities in electric vehicle charging, including potential malware injection.
  - **Solution**: Adapting communication network authentication protocols for secure vehicle charging.

Healthcare Systems Security Seminar

- **Speakers**:
  - **Emile Lupu**(Imperial College): Security issues in healthcare, AI vulnerabilities.
  - **Kevin Fu**(Northeastern University): Expert on medical devices, discussed device security.
  - **John Wondolt**(Georgia Tech Research Institute): Trustmark system for secure information sharing in healthcare.

Key Discussion Points

- **System Resilience**: Maintaining critical functions amidst cybersecurity compromises.
- **Balance**: Cybersecurity risk versus system usability.
- **Future Devices**: Security implications of biodegradable devices implanted in the body.

Seminar Notes and Research Agenda

- **Publication**: Seminar notes available on the INCS-CoE website, including abstracts, speaker

bios, and key questions.

- **Upcoming Seminar**: Focus on space systems later this year.

Introduction to University of Indonesia's Cybersecurity Initiatives

University of Indonesia's New Membership

- The University of Indonesia has been accepted as a new affiliate member of INSCOE since August 23, 2024.
- Indonesia is experiencing rapid digital transformation with a significant increase in internet users, reaching 221 million out of a total population of 278 million, resulting in an internet penetration rate of 79.5%.

Challenges and Initiatives

- **Digital Transformation Challenges**: Indonesia faces challenges such as increased attack surfaces and security risks, particularly in data security and critical information infrastructure.
- **Cybersecurity Workforce Gap**: There is a notable lack of cybersecurity workforce, especially in technical capacity, which is a concern for government and public sectors.
- **IDCARE Establishment**: The University of Indonesia established the Indonesia Cyber Awareness and Resilience Center (IDCARE) in 2020, focusing on:
  - Postgraduate programs in cybersecurity.
  - Cybersecurity-related research.
  - Collaboration, partnership, and certification building.
  - Enhancing cybersecurity capacity of human resources.

Collaborative Efforts

- **Cybersecurity Academy Membership Program (CAM)**: Involves multiple universities in Indonesia to collaborate on cybersecurity research and capacity building.
- **Joint Research and Development**: Collaboration with other universities to develop security monitoring tools and SOC based on open source, benefiting both academic communities and SMEs.
- **Training and Competitions**: Conducts cybersecurity training for leaders and national CTF competitions to develop cybersecurity talents.

International Cooperation

- **JICA Project**: Collaboration with JICA for human resources development in cybersecurity, developing a curriculum based on the NICE framework and security body of knowledge.

University of Porto's Cybersecurity Research

Membership and Collaboration

- The University of Porto is a member of the Center of Cybersecurity and Privacy, focusing on exchanging experiences and knowledge with other partners.
- Recent joint publication with UMBC on risk analysis in cybersecurity for car infrastructure.

Autonomous Vehicles and Cybersecurity

- **Challenges in Autonomous Vehicles**: Emphasizes the need for multiple sensors in autonomous vehicles for accurate perception and decision-making.
- **Security Risks**: Highlights potential risks of coordinated attacks using autonomous vehicles and the importance of a multi-layered cybersecurity approach.

Intrusion Tolerance and System Security

- **Intrusion Tolerance**: The ability of a system to function in a degraded mode even when compromised, requiring redundancy and a holistic approach integrating machine learning, dependability, and cybersecurity.

Northeastern University's Cybersecurity Competition

International Talent Development

- The INCS-CoE is focused on growing the international talent base in cybersecurity, addressing the global challenge of filling cybersecurity positions.
- The competition aims to develop international networks among students from like-minded countries and provide exposure to different cybersecurity practices.

Competition Details

- **Online Qualification Round**: Scheduled for early February, with registration opening in December.
- **Finals**: Anticipated to exceed 400 students, with around 100 students traveling to Boston, Massachusetts, USA, for the finals competition from July 6-10, 2025.
- **Future Competitions**: Planned to be held in Indonesia and then back in the U.S. at George Mason University.

Action Items

[ ] Plan and announce the seminar program for 2025 and provisional program for 2026.
[ ] Prepare for the next C2C competition at Northeastern University in July 2025.
[ ] Expand the community of experts and fellows within INCS-CoE.
[ ] Publish seminar notes and abstracts on the INCS-CoE website.
[ ] Prepare for the upcoming seminar on space systems.
[ ] Register for the cybersecurity competition in December.
[ ] Contact David Luzzi for more information about the competition and participation opportunities.

4.4 D2-T1-S4 Keidanren

Keidanren Theme: Enhancing Cyber Resilience through Public-Private Partnerships and Capacity Building Moderator: Akihiro WADA (Chair, Working Group on Cyber-Security Enhancement Committee on Cyber Security, Keidanren) Panelist: - Shinichi FUCHIGAMI (Corporate Executive CISO, General Manager, Cyber Security Strategy Department, NEC) - Nobutaka TAKEO (Director, Cybersecurity Division Commerce and Information Policy Bureau, Ministry of Economy, Trade and Industry (METI))	経団連 テーマ：わが国のレジリエンス強化に向けた官民連携・人材育成のあり方 モデレーター：和田 昭弘（経団連サイバーセキュリティ委員会サイバーセキュリティ強化ワーキンググループ 座長） パネリスト： - 淵上 真一（NEC Corporate Executive CISO 兼 サイバーセキュリティ戦略統括部長 兼 NEC セキュリティ株式会社 取締役） - 武尾 伸隆（経済産業省 商務情報政策局 サイバーセキュリティ課長）
Overview この文書は、サイバーセキュリティに関する複数の会議やシンポジウムの内容をまとめたものです。主に官民連携、人材育成、	

政府のサイバーセキュリティ政策、経済産業省の取り組み、セキュリティ人材の不足と育成、アクティブサイバーディフェンスの取り組み、産業データスペースの提言などが議論されています。また、各セクションでのアクションアイテムが最後にまとめられています。

セッション概要

- **テーマ**: 我が国のレジリエンス強化に向けた官民連携、人材育成の在り方
- **参加者**: 官と民からのゲスト
- **進行**: 経団連サイバーセキュリティ委員会 和田

パネリスト紹介

- **淵上 真一**: NEC コーポレーション エグゼクティブ CISO、サイバーセキュリティ戦略統括部長
- **武尾 伸隆**: 経済産業省 消防情報政策局 サイバーセキュリティ課長

セッションの流れ

1. パネリストによるショートプレゼン
2. パネル討議: 官民連携と人材育成

官民連携の現状と課題

情報不足

- **課題**: 官民連携に必要な情報が不足している。
  - 民間からの情報提供が少なく、安心して公開できる環境がない。

役割の明確化

- **現状**: 個人情報保護委員会への報告義務がある。
  - インシデントの事例が集まっているが、共有や活用が進んでいない。

先行事例

- **事例**: オリンピック・パラリンピックでの JSIP の取り組み。
  - 官民連携で情報共有が成功した例。

人材育成の在り方

新卒採用の課題

- **現状**: セキュリティに興味を持つ学生が減少。
  - AI など他分野への関心が高まっている。

トレーニングと経験

- **課題**: トレーニングだけでは育成が不十分。
  - 多様な経験を積む場が必要。

リスキリングの必要性

- **現状**: 絶対的な人材不足。
  - 他部門からのリスキリングを進めるが、課題が多い。

政府のサイバーセキュリティ政策

国家安全保障戦略

- **導入**: 能動的サイバー防御の検討。
  - 攻撃者に対する無害化措置の導入を検討中。

官民連携の強化

- **目的**: 民間事業者からの情報共有と政府からの情報提供の双方向の循環。
  - 報告のフォーマット統一やヒアリングの合同化を目指す。

通信情報の利用とアクセス無害化

- **課題**: 憲法で保障される通信の秘密をクリアしつつ、攻撃を検知するための通信情報の活用。

- **無害化措置**: 攻撃者へのアクセスを通じた無害化措置の検討。

経済産業省のサイバーセキュリティ政策

- **内容**: 経済産業省が進めるサイバーセキュリティの取り組みについての紹介。

産業界のサイバーセキュリティ能力向上

- **官民連携の取り組み**
  - 経済産業省は、日本の産業界のサイバーセキュリティ能力を向上させるため、関係省庁と連携し、民間のニーズに基づいた政策を実施しています。

サプライチェーン全体の対策強化

- **経営者向けガイドラインの作成**
  - サプライチェーン全体での対策強化の一環として、経営者向けのガイドラインを作成しています。
- **中小企業向けセキュリティサービスの提供**
  - 中小企業が安価で利用できるセキュリティサービスの提供スキームを構築しています。

認証評価制度の立ち上げ

- **IoT 製品の認証制度**
  - IoT 製品を認証する制度を構築し、政府調達や国際連携を通じて検討しています。

サイバーセキュリティ対応体制の強化

- **IPA によるサイバー情勢分析**
  - IPA がサイバー情勢を分析する能力を構築中です。
- **APT 攻撃対策チーム「J-CRAT」の強化**
  - 政府をバックにした APT 攻撃に対処する専属チーム「J-CRAT」を強化しています。

産業振興と研究開発の促進

- **研究開発プロジェクトの実施**
  - 産業振興の観点から、研究開発の促進やプロジェクトの実施を検討しています。

人材育成

社会インフラ分野の人材育成プログラム

- **制御技術と IT の知見を結集**
  - 電力、ガス、化学、自動車などの分野で、制御技術と IT の両方を学べる人材育成プログラムを実施しています。
- **実践的な研修**
  - 演習施設や模擬プラントを用いた実践的な研修を行い、攻撃者と防御者の両方を経験することで高いレベルの人材を育成しています。
- **OB コミュニティの構築**
  - 約 400 名の卒業生が OB コミュニティを形成し、強力なネットワークを構築しています。

国家資格「登録セキュリティ」の支援制度

- **国家資格の支援**
  - セキュリティに関する唯一の国家資格「登録セキュリティ」の支援制度を持っています。

若手人材育成のセキュリティキャンプ

- **若手の尖った人材の発掘**
  - 若手人材育成のためのセキュリティキャンプを通じて、優れた若手人材を発掘しています。

サイバーセキュリティ人材の育成と確保

- **現状と課題**
  - 約 20 年間で 1000 名が修了したプログラムがあるが、産業界ではサイバーセキュリティ人材が依然として不足している。

- 特に中堅中小企業では、内部でセキュリティ対策を推進する人材が最も不足している。
- **今後の取り組み**
- プログラムの拡充と中小企業向けの人材育成政策を検討中。

経団連の取り組み

Society 5.0 for SDGsとDFFT

- **三本柱の取り組み**
- 産業団体、官民連携、国際連携を通じたサイバーセキュリティ強化。
- サプライチェーン全体を俯瞰した安全安心なサイバー空間の構築。

日英サイバー協力ミッション

- **調査内容**
- 2023年1月15日から18日にかけて英国で実施。
- 英国のインテリジェンスや官民連携の方向性は官から民へと向かっている。
- 英国では国家予算を充ててサイバースキルのトレーニングを無料で提供。
- **教育の覚書（MOC）**
- 人材育成と官民連携を含む8点の内容でMOCを締結。

官民連携と人材育成の課題

官民連携の課題

- **情報共有の重要性**
- 双方向での情報共有が必要。
- 信頼関係の構築が情報共有の鍵。
- **具体的な取り組み**
- イギリスのように官民での人材交流を強化。
- 政府側のインテリジェンス強化が必要。

人材育成の課題

- **セキュリティ人材の偏り**
- ユーザー企業や中小企業におけるセキュリティ人材の不足。
- 経営者がセキュリティを重要事項として位置づけ、全社的に取り組む必要がある。
- **具体的な提案**
- リスキリングや新たな人材の採用を通じて、セキュリティ人材を育成。

パネル討議

官民連携の緊密化

- **課題と期待**
- 情報の不足が大きな課題。
- 情報共有のコミュニティを維持する方法として、情報提供を基にしたコミュニティの維持が有効。
- **信頼関係の構築**
- 小さなやりとりを積み重ね、信頼の輪を広げることが重要。

人材育成の課題と取り組み

- **ユーザー企業へのメッセージ**
- セキュリティ人材の偏りを解消するため、経営者がセキュリティを重要視し、全社的に取り組むことが必要。
- リスキリングや新たな人材の採用を通じて、セキュリティ人材を育成することが求められる。

セキュリティ人材の不足と育成

中小企業におけるセキュリティ人材の必要性

- **現状の課題**：中小企業では、専業のセキュリティ人材が不足している。
- **プラスセキュリティ人材**：経済産業省が提唱する「プラスセキュリティ人材」が不足しており、既存の社員にセキュリティスキルを追加する必要がある。

企業文化とセキュリティ意識の向上

- **企業文化の重要性**：ANA の例を挙げ、航空機事故を防ぐ文化が情報セキュリティの遵守にも役立つと指摘。
- **倫理と企業風土**：倫理や企業風土が人材の底上げに寄与するとの意見が共有された。

アクティブサイバーディフェンスの取り組み

攻撃者への対応

- **攻撃者特定と機能停止**：攻撃者のサーバーを特定し、その機能を停止することを想定している。
- **制度的措置**：ハックバックに近い措置を制度的に整備することを検討中。

国家支援のある攻撃者への対応

- **APT 攻撃の主体**：中国、ロシア、イラン、北朝鮮などが国家支援を受けた攻撃者として挙げられる。
- **Volt Typhoon**：中国系のグループが社会インフラへの攻撃を試みているとの情報がある。

官民連携の重要性

情報のギブアンドテイク

- **情報交換の提案**：民間が持つ点の情報を官が俯瞰し、情報を交換することで有益な環境を作ることが提案された。

人材交流と育成

双方向の観点での人材交流

- 双方向の視点で人材交流を行う提案がありました。
- ユーザー企業とベンダー企業が連携して取り組むことが重要とされました。

人材育成の取り組み

- 経済産業省の取り組みが紹介されました。
- ユーザー企業や中小企業にとっての具体的な取り組みが求められています。
- お互いの信頼関係が基盤となることが強調されました。

サイバーセキュリティと産業データスペース

サイバーセキュリティの議論

- これまでのサイバーセキュリティに関する議論が進められてきました。

産業データスペースの提言

- 経団連が公表した提言について紹介されました。
- 産業データスペースは、データ主権を前提に構築されることが説明されました。
- 政府が戦略的にトラスト基盤を整備し、国際的に相互運用可能なスペースを構築することが急務とされています。
- 官民で協議を行う場を設置し、関係省庁や団体と連携して取り組むことが提案されました。

Action Items

[ ] 官民連携の情報共有環境の整備
[ ] トレーニングプログラムの見直しと多様な経験の提供
[ ] リスキリングの効果的な実施方法の検討
[ ] 報告フォーマットの統一とヒアリングの合同化
[ ] 経営者向けガイドラインの作成
[ ] 中小企業向けセキュリティサービスの提供スキームの構築
[ ] IoT 製品の認証制度の構築
[ ] IPA によるサイバー情勢分析能力の構築

[ ] APT 攻撃対策チーム「J-CRAT」の強化
[ ] 研究開発プロジェクトの実施
[ ] 人材育成プログラムの実施
[ ] 国家資格「登録セキュリティ」の支援制度の運用
[ ] 若手人材育成のセキュリティキャンプの実施
[ ] プログラムの拡充と中小企業向けの人材育成政策の検討
[ ] 官民での人材交流の強化
[ ] 政府側のインテリジェンス強化
[ ] リスキリングや新たな人材の採用を通じたセキュリティ人材の育成
[ ] セキュリティ人材の育成プログラムの検討
[ ] アクティブサイバーディフェンスの制度的措置の詳細決定
[ ] 官民連携による情報交換の仕組み構築
[ ] ユーザー企業とベンダー企業の連携強化に向けた具体的な取り組みを検討する。
[ ] 産業データスペースの構築に向けた官民協議の場を設置する。

5 DAY 2: October 31 | East Research Building 8F Hall

5.1 D2-T2-S1 Japan Digital Trust Forum (JDTF)

Japan Digital Trust Forum (JDTF) Title: Trends in Digital Trust Required for DX - What is Trust in the Digital Space? - Moderator: Masaki Shimaoka (Senior Researcher, IS Laboratory, SECOM CO.) Panelists: - Akihiro Odajima (Vice-Chairman, Trust Services Study Committee, Digital Trust Council) - Yukihide Seki (Senior Professional, NEC Corporation) - Satoru Tsuchiya (Senior Director, Fujitsu Limited)	デジタルトラスト協議会（JDTF） タイトル：DX 推進で求められるデジタルトラストの動向 ～デジタル空間の信頼とは？～ モデレータ：島岡 政基（セコム株式会社 IS 研究所、主任研究員） パネリスト： - 小田嶋 昭浩（デジタルトラスト協議会 トラストサービスの在り方検討委員会 副委員長） - 関 行秀（日本電気株式会社 シニア プロフェッショナル） - 土屋 哲（富士通株式会社 シニアディレクター）
No record	

5.2 D2-T2-S2 Data Society Alliance (DSA)

Data Society Alliance (DSA) Title: The technical requirement in implementation of DATA-EX Moderator: Hiroshi Mano (EverySense,Inc., C.E.O., Data Society Alliance, Secretary General) Panelists: - Masazumi Hirono (Senior Engineer, ID Promotion Center, Government & Public Corporation Information Systems Division, Hitachi, Ltd.) - Taka Matsutsuka (Senior Research Director, Data & Security Research Laboratory, Fujitsu Research) - Masaru Dobashi (Senior Specialist / Executive IT Specialist (Platform), NTT DATA Group Corporation)	データ社会推進協議会（DSA） タイトル：DATA-EX の実装、社会実装上の技術的課題 モデレータ：眞野 浩（エブリセンスジャパン株式会社 代表取締役、一般社団法人データ社会推進協議会専務理事／事務局長） パネリスト： - 廣野 正純（株式会社日立製作所 公共システム事業部 ID 推進センタ 主任技師） - 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） - 土橋 昌（株式会社 NTT データグループ シニア・スペシャリスト/エグゼクティブ IT スペシャリスト（プラットフォーム））
No record	

5.3 D2-T2-S3 Digital Architecture Design Center (DADC)

Digital Architecture Design Center (DADC) Title: Is a trust infrastructure required to realize DFFT? Moderator: Soshi Hamaguchi (Maximax Co., Ltd.,	デジタルアーキテクチャ・デザインセンター（DADC） タイトル：トラスト基盤は DFFT 実現のために必要なのか モデレータ：濱口 総志（株式会社 Maximax 代表） パネリスト：

Representative) Panelists: - Tetsuya Sakashita (JIPDEC (Foundation for promotion of Digital Economy and Community), Managing Director) - Hiroshi Mano (EverySense,Inc./EverySense Japan K.K. , C.E.O.) - Toshikazu Yoshida (Japan Digital Trust Forum, Director, Chief of Secretariat) - Takeshi Kawabata (IPA Information-technology Promotion Agency, Researcher)	- 坂下 哲也((一財)日本情報経済社会推進協会 常務理事) - 眞野 浩 (エブリセンスジャパン株式会社 代表取締役) - 吉田 理重 (一般社団法人デジタルトラスト協議会(JDTF) 理事兼事務局長) - 川端 健 (独立行政法人 情報処理推進機構(IPA) 研究員)
No record	

5.4 D2-T2-S4 CyLogic

CyLogic Title: FedRAMP Cloud Training for Japan Speaker: - Louis Mayberg (CyLogic's Co-Founder & CEO) - Chris Grady (CTO, CyLogic) Language: English	CyLogic タイトル：FedRAMP クラウドの日本向けトレーニング Speaker： - ルイス・メイバーグ (CyLogic, 共同創設者兼 CEO) - クリス・グラッディ (CyLogic, CTO) 言語：英語
No record	

6 DAY 3: November 1 | North Building 1F North Hall

6.1 D3-T1-S1 Trend Micro

Trend Micro Theme: Emerging Trends in Russia-Linked APT Activities Moderator: Hiroyuki Kakara (Sr. Threat Researcher, Trend Micro Cybersecurity Institute)	Trend Micro テーマ：ロシアに関連するとみられる APT の動向について モデレータ：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）

APT サンドワーム フィッシング

テーマ

この講義では、ロシア起源の APT（Advanced Persistent Threat）の動向と攻撃手法について詳しく解説されました。特に、サンドワームやポンストーム（APT28）、APT29、TWARA、アースダフ（ガマレドン）などの活動とターゲットが取り上げられました。また、サンドワームによるファイルスティーラーの発見や、ウクライナ軍を狙った攻撃の詳細、フィッシングキャンペーンの手法についても説明されました。これらの APT グループの戦術、技術、手順（TTP）に関する分析が行われました。

要点

1. ロシア起源の APT の動向
2. サンドワームの活動とターゲット
3. ポンストーム（APT28）の活動とターゲット
4. APT29 の活動とターゲット
5. TWARA の活動とターゲット
6. アースダフ（ガマレドン）の活動とターゲット
7. サンドワームによるファイルスティーラーの発見
8. ウクライナ軍を狙った攻撃の詳細
9. ファイルスティーラーの動作とターゲットファイル
10. R-Clone を用いた C&C 活動

章とトピック

ロシア起源の APT の動向

ロシアに関連するとみられる APT（Advanced Persistent Threat）の動向についての研究と分析。

- **要点**
  - サンドワームは GRU に帰属し、ウクライナのインフラや NATO 加盟国をターゲットにしている。
  - ポンストーム（APT28）は GRU に帰属し、世界中の軍事、政府、メディアをターゲットにしている。
  - APT29 は SBR に帰属し、政府機関やシンクタンクをターゲットにしている。
  - TWARA は FSBA に帰属し、政府機関や大使館をターゲットにしている。
  - アースダフ（ガマレドン）は FSBA に帰属し、ウクライナ政府や軍事機関をターゲットにしている。

サンドワームによるファイルスティーラーの発見

サンドワームに帰属するとみられるファイルスティーラーの発見とその詳細。

- **要点**
  - ドローンに関連するファイルや機密情報を摂取するようにデザインされている。
  - ウクライナ軍が使用するドローンの情報を盗む作戦に関与している可能性。
  - 特定の文字列を含むファイルを収集し、C&C にアップロードする。

ポンストームの TTPs と最近の攻撃キャンペーン

ポンストーム（APT28）の TTPs（戦術、技術、手順）と最近の攻撃キャンペーンの詳細。

- **要点**
  - クレデンシャルフィッシングキャンペーンを展開。
  - インターネット上の無料サービスや正規の第三者のメールアドレスを悪用。
  - Webhook のテストサービスを C&C として悪用。

UKR.NET のクレデンシャルフィッシングキャンペーン

UKR.NET のユーザーをターゲットにしたフィッシングキャンペーンで、偽のパスワードリセットページに誘導し、ユーザー名とパスワードを攻撃者に送信する。

- **要点**
  - フィッシングメールを使用してユーザーを偽のサイトに誘導
  - 入力された認証情報を攻撃者に送信
  - Mocky.io の URL を使用

MS クレデンシャルフィッシングキャンペーン

Outlook Web App を模倣したフィッシングサイトを使用し、ユーザーのログイン情報を盗むキャンペーン。

- **要点**
  - ターゲットのユーザー名を URL のパラメータとして使用
  - pipedream.net の Webhook に情報を送信
  - ポーランドやルーマニアの機関がターゲット

アリーナキャンペーン

Mocky.io の URL を使用したスペアフィッシングで、システム情報を収集するキャンペーン。

- **要点**
  - ポーランド国家公文書館がターゲット
  - JavaScript を使用して情報を収集
  - webhook.site に情報を送信

APT29 の TTP

APT29 の典型的な戦術、技術、手順（TTP）についての説明。

- **要点**
  - クラウド環境の侵害
  - スピアフィッシングの使用
  - HTML スマグリング技術

APT29 の活動とウクライナ戦争との関連

APT29 はロシアの対外情報庁のために活動していると考えられ、ウクライナ戦争に関連して活動を活発化させた。

- **要点**
  - APT29 は 2021 年から 2023 年にかけて活動を活発化。
  - ウクライナ戦争に関連して、他国からのウクライナへの支援状況を把握しようとした可能性。
  - ロシアに近い国々も監視対象とされている。

トゥアラの攻撃手法

トゥアラはスペアフィッシングやウォータリングホールアタックを使用し、被害者にマルウェアを配布する。

- **要点**
  - Adobe PDF や Java の脆弱性を悪用。
  - カスタムマルウェアの開発と使用。
  - サプライチェーン攻撃や中間者攻撃の利用。

カズワマルウェアの特徴と進化

カズワはトゥアラの主要なバックドアで、複数の層のラッピングと難読化によって保護されている。

- **要点**
  - 2005 年頃に.NET Framework で開発。
  - 複数のコマンドを持ち、45 のコマンドが観測された。
  - 感染した環境のドメイン名に基づく暗号化。

アースダフのリモートテンプレートインジェクション技術

アースダフはリモートテンプレートインジェクションを使用し、マクロを通じて不正なコードを実行する。

- **要点**
  - マイクロソフトワードのテンプレート機能を悪用。
  - VBScript をドロップして実行。
  - テンプレートドキュメントとソースドキュメントの両方を解析する必要がある。

宿題と提案

6.2 D3-T1-S2 InfoKeyVault Technology / WiSECURE Technologies Corporation

InfoKeyVault Technology / WiSECURE Technologies Corporation Title: The Impact of CMMC 2.0 on the Defense Supply Chain Subtitle: - The emergence of CMMC 2.0 and SP 800-171r2 - CMMC 2.0 compliance will push the industrial vendors to invest more in the data security - How could the vendors improve their data protection - Some interesting demonstrations on protecting your valuable data Speaker: Albert Cheng (CEO of InfoKeyVault Technology Co., Ltd., CEO of WiSECURE Technologies Corporation) Language: English	InfoKeyVault Technology / WiSECURE Technologies Corporation タイトル：CMMC 2.0 がサプライチェーン防衛に与える影響 サブタイトル： - CMMC 2.0 と SP 800-171r2 の登場 - CMMC 2.0 への準拠により、産業ベンダーはデータセキュリティへの投資をさらに増やすことになる - 産業ベンダーはどのようにしてデータ保護を改善できるか - 価値のあるデータの保護に関するデモンストレーション Speaker： アルバート・チェン（InfoKeyVault Technology Co., Ltd. CEO, WiSECURE Technologies Corporation CEO） 言語：英語

Overview

This document provides a comprehensive overview of the cybersecurity symposium, focusing on the importance of data protection, the U.S. Department of Defense's CMMC framework, and insights from InfoKeyVault Technology. It highlights key discussions on data-centric security strategies and compares CMMC with ISO 27001. The document concludes with action items for further engagement with InfoKeyVault Technology and exploration of the CMMC framework.

Introduction to InfoKeyVault Technology

- **Speaker**: Albert from InfoKeyVault Technology, Taiwan.

- **Company Overview**: InfoKeyVault Technology specializes in data security, providing hardware products and design services for military, government, aerospace, and enterprise sectors.

Importance of Data Protection in Cyberspace

- **Key Insight**: Data protection is crucial as cyber attackers aim to steal or manipulate valuable data.
- **Examples**:
  - Google and ChatGPT rely on data for functionality.
  - Critical infrastructure like JR-TRANS and power plants depend on accurate data.
- **Perspective**: Data-centric protection is essential as attackers may eventually breach systems despite strong defenses.

U.S. Department of Defense (DoD) and CMMC

- **CMMC Overview**: Cybersecurity Maturity Model Certification (CMMC) is a compliance framework for DoD vendors to protect sensitive data.
- **Regulations**:
  - CMMC focuses on Federal Contract Information (FCI) and Controlled Unclassified Information (CUI).
  - Non-compliance may lead to removal from the DoD vendor list.
- **Timeline**:
  - CMMC 1.0 introduced in 2020.
  - CMMC 2.0 expected to begin in the first quarter of next year.
  - Full certification required by 2028.

CMMC vs. ISO 27001

- **Comparison**:
  - CMMC is specific to data protection for DoD vendors.
  - ISO 27001 is a general security framework applicable to any company.
- **Impact**:
  - CMMC certification is mandatory for DoD vendors and their subcontractors.
  - Infrastructure and service providers are also affected due to their role in data handling.

Lessons from CMMC

- **Data-Centric Security**: Emphasizes the importance of protecting data as a critical asset.
- **Security Strategy**:
  - Traditional perimeter-based security is insufficient.
  - Focus on identifying and protecting valuable data like CUI and FCI.
- **Techniques**:
  - Use encryption and access control based on data states (at rest, in transit, in use).

Company Introduction and Product Demonstration

- **InfoKeyVault Technology**:
  - Established for nearly 20 years, focusing on data security.
  - Expanded operations in Japan under the brand WiSecure Gaishi Kaisha.
- **Product Highlight**:
  - FileAgis: A file-only automatic encryption system using unique keys for each user.

- Google Workspace Integration: Demonstrated client-side encryption for enhanced data security.

Action Items

[ ] Contact InfoKeyVault Technology for more information on data protection solutions.

[ ] Explore the CMMC framework for potential application in your organization.

6.3 D3-T1-S3 Leukocyte-Lab

Leukocyte-Lab Title: Give Your Cybersecurity a Checkup: AI-Driven Visibility, Effectiveness, and Investment Evaluation Speaker: Jason Shen (Leukocyte-Lab Co., Ltd., CEO) Language: English	Leukocyte-Lab タイトル：サイバーセキュリティの点検のすすめ：AI による可視性、有効性、投資効果の評価 Speaker：ジェイソン・セン（Leukocyte-Lab Co., Ltd., CEO） 言語：英語

Overview

This document provides a comprehensive summary of the first day of a Japanese conference focused on cybersecurity. It covers various aspects such as current cybersecurity threats, the importance of attack visibility, testing defense effectiveness, security investment strategies, and the integration of AI in next-generation Breach and Attack Simulation (BAS). The document also includes case studies and real-world examples to illustrate key points. Action items are consolidated at the end for clarity.

Introduction

- **Speaker**: Jason, President of Leukocyte, Founder of Leukocyte-Lab, and Core Member of Military Cyber Security Association in Taiwan.
- **Context**: First day of the Japanese conference, focusing on cybersecurity challenges and solutions.

Cybersecurity Threats and Attack Visibility

Current Cybersecurity Risks

- **Global Impact**: Cybercrime is a significant risk for global businesses and government agencies, with losses expected to reach $10 trillion by 2025.
- **Frequency of Attacks**: Cyber attacks occur every 39 seconds, highlighting the increasing severity of cybercrime.

Importance of Attack Visibility

- **Definition**: Attack visibility refers to the ability to monitor all network activities to detect threats promptly.
- **Analogy**: Compared to a general on a battlefield needing to understand enemy positions, cybersecurity requires understanding threat dynamics.
- **Consequences of Lack of Visibility**: Without visibility, organizations face significant financial losses and brand damage.

Case Studies

- **Equifax**: Failed to patch vulnerabilities due to insufficient attack visibility, leading to exploitation by hackers.

- **Target**: Vulnerabilities in third-party vendor security went undetected for weeks, resulting in unauthorized access.

Testing and Ensuring Defense Effectiveness

Necessity of Testing

- **Misconfigurations**: Highlighted by the Capital One case, where a misconfigured web application firewall allowed unauthorized access.
- **Testing Methods**: Traditional vulnerability assessments and penetration testing are costly and may not be feasible for all companies.

Breach and Attack Simulation (BAS)

- **Functionality**: BAS automates security testing, simulating potential attacks to assess defense effectiveness.
- **Comparison**: Unlike traditional methods, BAS is more affordable and flexible, providing a comprehensive view of security posture.

Real-World Examples

- **Network Traffic Monitoring**: A case where outdated equipment led to undetected attacks due to traffic overload.
- **Server Misconfigurations**: Highlighted issues where network settings prevented proper detection of attacks on certain servers.

Security Investment Strategy

Role of BAS in Investment Decisions

- **Pre-Investment**: BAS helps simulate attacks to guide risk assessments and budget allocation.
- **During Investment**: Assists in evaluating cybersecurity products by testing them against real-world attacks.
- **Post-Investment**: Regular testing ensures defenses remain effective against evolving threats.

Case Study: Medical Center

- **Challenge**: Faced ransomware threats and needed to decide on further security investments.
- **Outcome**: BAS testing revealed strong existing defenses but identified gaps in data protection, leading to targeted investments.

Next Generation BAS and AI Integration

AI-Driven Testing

- **Automation**: AI simplifies the selection and execution of security tests by analyzing network architecture.
- **Log Analysis**: AI automates log collection and analysis, reducing the time required for security assessments.

Benefits of AI Integration

- **Efficiency**: Reduces analysis time from a week to a day, allowing for quicker response to threats.
- **Comprehensive Reporting**: Automatically generates detailed reports with specific recommendations for security improvements.

Company Overview

- **Leukocyte-Lab**: A leading cybersecurity startup in Taiwan, recognized for its innovative solutions and collaborations with government and industry leaders.
- **Expansion Goals**: Aiming to enter the Japanese and East Asian markets.

Action Items

[ ] Explore BAS solutions for ongoing security testing and investment strategy.

[ ] Consider AI integration for automated security log analysis and reporting.

6.4 D3-T1-S4 Keio University Global Research Institute, Cyber Civilization Research Center (CCRC)

Keio University Global Research Institute, Cyber Civilization Research Center (CCRC) Keio University CCRC (Co-organized by ECHONET Consortium, Japan Electrical Manufacturers' Association, Inc.) CCRC Open Discussion: Trust Design about Energy Resource Aggregation Business as Cyber and Physical system. Moderator: Masaki Umejima (Project Professor, Graduate School of Media and Governance, Keio University /Convener of Smart Energy Development Plan, System Committee, IEC) Panelists: - David Farber (Guest Professor [Global], Keio University and Co-Director of Cyber Civilization Research Center) - Masao Isshiki (Professor and Director, ECHONET Lite Interoperability Test Center, Kanagawa Institute of Technology) - Selvakumar Manickam (Director, Cyber Security Research Center in University Science Malaysia) - Yasuyuki Hayama (Assistant Professor, Faculty of Design, Strategic Design Department, Kyushu University) - Masato Nagasawa (Chairman of Promotion Committee, ECHONET Consortium) - Yoichi Masuda (Technical Committee SAWG Chief Manager, ECHONET Consortium) - Kenichi Nagami (Chief Security Officer of UCHITAS Project, Intec Inc.) - Chihiro Hasegawa (Seier Consultant, Nomura Research Institute)	慶應義塾大学グローバルリサーチインスティテュート サイバー文明研究センター（CCRC） 慶應大学 CCRC（共催：一般社団法人 エコーネットコンソーシアム、一般社団法人 日本電機工業会） CCRC 公開討論：サイバーフィジカルシステムとしてのエネルギーリソースアグリゲーションビジネスに関するトラストデザイン モデレータ：梅嶋 真樹（教授、慶應義塾大学大学院政策メディア研究科特任教授、IEC システム委員会コンビーナ(スマートエネルギー開発計画担当)) パネリスト： - デビッド・ファーバー（教授、慶應義塾大学特別招聘教授(国際)、サイバー文明研究センター共同センター長) - 一色 正男（神奈川工科大学教授、ECHONET Lite 認証支援センター所長) - セルバクマール ・マニカム博士（マレーシア科学大学サイバー セキュリティ研究センター所長) - 長沢 雅人（エコーネット コンソーシアム 普及委員長) - 羽山 康之（九州大学大学院芸術工学研究院ストラテジックデザイン部門 助教) - 増田 洋一（エコーネット コンソーシアム 技術委員会 SAWG 主査) - 永見 健一（UCHITAS プロジェクト最高セキュリティ責任者、株式会社インテック) - 長谷川 ちひろ（シニアコンサルタント、野村総合研究所)

Overview

This document summarizes the discussions and outcomes from a series of meetings focused on cybersecurity and trust design in energy resource aggregation and IoT systems. Key topics include security frameworks, risk assessments, and the challenges of implementing secure protocols in resource-constrained IoT devices. The document also outlines action items for future developments and collaborations.

Introduction

- **Meeting Time and Venue**: The meeting was held at 5 p.m. Japan time as part of the Keio University International Cyber Security Symposium, co-organized by Econet Consortium and the Japan Electrical and Manufacturers Association.
- **Facilitator**: Masaki Umejima, Professor at Keio University and CCRC member, led the discussion.

Main Topic

- **Objective**: Discuss the security of energy resource aggregation business and trust design within a cyber and physical security framework.
- **Definition**: Energy resource aggregation business involves managing demand and supply of electricity through coordination with retailers and grid distributors.

Key Challenges

- **Resource Facilitation**: Managing diverse resources at the customer side is a significant challenge.
- **Cyber and Physical System**: The integration of cyberspace and physical space is crucial for system security.

Security Framework

- **Security Triangle**:
  - **Framework**: Introduces necessary security assessment methods and recommendations.
  - **Guidelines**: Defined by government authorities, such as the Japanese government and NIST in the US.
  - **Implementation**: Balancing technology and economics to choose appropriate security measures.

Risk Assessment

- **Current Status in Japan**:
  - Ongoing risk assessment of energy resource aggregation business.
  - Previous guidelines from 2019 are being updated, with a new version expected by March 2025.
- **Process**:
  - Identify risk sources, analyze risks, evaluate them, and consider treatment based on ISO and IEC standards.

Cyber and Physical Space Connection

- **Security Measures**:
  - Authentication and encryption are key for both physical space security and connecting cyber and physical spaces.
  - Data management is critical, especially in controlling data spread after uploading.

Updates on Technical Paper and Guidelines

CCRC and Keio University Technical Paper

- **Publication Timeline**: A new technical paper from CCRC at Keio University is expected to be published in Spring 2025.
- **Purpose**: The paper will align with the updated Japanese government guidelines and serve as an example for implementing security measures.
- **Audience**: Aggregators and other stakeholders can utilize this paper to understand and implement security measures.

Current Assessment and Vulnerability Collection

- **Ongoing Assessment**: The current focus is on assessing vulnerabilities in labs, considering both cyber and physical systems.
- **Objective**: To understand and mitigate vulnerabilities effectively.

ERAB Security Guidelines

Background and Development

- **Release Date**: Scheduled for March 2025.
- **Context**: The guidelines are being developed in response to the increasing number of IoT devices and associated cyber threats.

Key Points

- **Increase in Cyber Threats**: As IoT products proliferate, so do cyber threats targeting vulnerabilities.
- **Diverse Threats**: Threats are increasing due to the diversification of information obtainable from target devices.

Implementation Items

- **Role Distribution**: Tasks are being carried out by CCRC Umeshima-sensei and LNRI, with roles distributed among team members.
- **Current Focus**: Modeling the e-lab system, identifying threats, and considering risk scenarios.

Econet Consortium Security Perspective

Overview

- **Presenter**: Mr. Nagasawa, Vice-Chairman of Econet Consortium.
- **Focus**: Security perspective from the Econet Consortium side.

Products and Systems

- **IoT Products**: Includes industrial control devices, network cameras, and home appliances.
- **Smart Power Supply**: Key area of focus, with specific requirements under the Econet project.

Standards and Collaboration

- **Star 1 and Star 2 Requirements**: Both are subject to self-adjustment declarations.
- **Collaboration**: CCDS group and home-related manufacturers are involved in developing standards.

Security Requirements

- **Econet Star 1**: Mr. Masuda from Panasonic discusses the security requirements and system architecture.

ECHONET Lite Implementation and Security Concerns

Overview of ECHONET Lite Implementation

- The implementation of ECHONET Lite is compared to other systems, emphasizing its importance in protecting information assets.
- Discussion on whether ECHONET Lite should treat certain information assets to prevent potential damage.

Smart Home Subworking Requirements

- The focus is on the smart home area where Econet Lite devices are predominantly used.
- The consortium is considering future responses to meet the requirements of Econet Lite devices in this subworking.

Challenges in Implementation

- Balancing technical and economic viewpoints is crucial for successful implementation.
- The Japanese government's role is highlighted as significant in addressing these challenges.

Presentation by Dr. Salwa

Introduction

- Dr. Salwa, Director of the Cybersecurity Research Center at the University of Science Malaysia, shares insights on ECHONET Lite.
- The center focuses on cybersecurity in emerging technology and industrial communication systems.

Establishment of Cybersecurity Test Center

- Collaboration with CCRC, SFC Forum, and Masaaki-san led to the first Econet Lite Cybersecurity Test Center in Malaysia.
- The center includes real Econet Lite appliances and emulated systems to demonstrate complex communication within the network.

Malaysian Cybersecurity Act and Recommendations

- The Malaysian Cybersecurity Act (Act 854) focuses on national critical information infrastructure, including the energy sector.
- The center has developed a Malaysian-centric EROP recommendation for security and privacy, considering local policies and culture.

Evaluation of ECHONET Lite Security

- ECHONET Lite is an open protocol similar to the internet, facing similar security challenges.
- Key security concerns include the lack of built-in security features like authentication, encryption, and integrity checks.
- The complexity of relying on external protocols for security increases vulnerability to attacks such as spoofing and data tampering.

Recommendations for Security Improvement

- Reducing complexity by minimizing dependence on external protocols is essential.
- Known vulnerabilities in external protocols like DTLS, WPA3, and IPSec need to be addressed through research and testing.

Security Challenges in IoT Protocols

Resource Constraints and Protocol Complexity

- IoT devices are resource-constrained, making it challenging to handle multiple protocols and

dependencies.

- The complexity of protocols impacts computation capability and resource management in cyber-physical systems and home IoT devices.
- Cost is a significant concern alongside limited end-to-end security and the need for protocol-level security integration.

Security Considerations and Experimentation

- Security considerations are based on real experiments, including attacks on air conditioners and lighting systems.
- Findings highlight the importance of secure communication, storage, privacy, and defense against attacks, aligning with the CIA triad: confidentiality, integrity, and availability.
- Vulnerabilities found will be detailed in the upcoming report version, expected in November.

Recommendations for ECO and ELAIR Protocols

Addressing Security Challenges

- **Authentication**: Protect against unauthorized access and rogue devices by embedding cryptographically generated passwords in each device.
- **Data Integrity**: Use cryptographic hashes to prevent tampering and man-in-the-middle attacks, ensuring reliable data exchange.
- **Data Confidentiality**: Encrypt data in transit to prevent unauthorized access, adhering to a zero-trust policy.
- **Replay and DOS Attacks**: Implement rate limiting to address replay and DOS attacks, which can have severe physical consequences.
- **Data Storage**: Encrypt data on devices to prevent deciphering in case of a breach.
- **Key Management**: Ensure robust encryption, authorization, and authentication processes.
- **Firmware Updates**: Enforce digitally signed firmware updates from dedicated servers to prevent unauthorized modifications.
- **Tamper Reduction**: Implement mechanisms to prevent device tampering and unauthorized firmware modifications.

Balancing Security and Usability

- Open protocols must balance security with ease of implementation and use, similar to RESTful APIs.
- Security is crucial for distributed energy resources and home appliances, where risks can transcend from cyberspace to physical space.
- Open protocols offer interoperability, innovation, accessibility, and flexibility, reducing vendor lock-in and fostering global participation.

Expert Insights and Panel Discussion

Balancing Interoperability and Security

- Dr. Selber emphasized the need for balance between interoperability and secure systems.
- Panelists highlighted the importance of device-level authentication and the challenges of built-in security in open systems.
- Dave Faber discussed the complexity added by openness and the need for rigorous testing and verification.

Future Directions

- The challenge lies in maintaining a balance between interoperability and security over the next five years.
- The Econet Consortium is considering device-level authentication as a key focus area.
- Continuous security assessments and feedback from participants are crucial for improving the Econet Lite system.

Action Items

[ ] Finalize the draft of cybersecurity guidelines for energy resource aggregation business by the end of the year.

[ ] Release version 3.0 of the guidelines before March 2025.

[ ] Share information with Ms. Hasegawa regarding the vulnerability of the EDAB system.

[ ] Support Ms. Hasegawa's information-gathering activities.

[ ] Once the outline is decided, share the contents of the Econet standards with relevant stakeholders.

[ ] Consider the balance between technical and economic viewpoints in ECHONET Lite implementation.

[ ] Develop strategies to reduce complexity and reliance on external protocols for ECHONET Lite security.

[ ] Address known vulnerabilities in external protocols through continued research and testing.

[ ] Provide feedback and comments on E-Lab security concerns to Ms. Hasegawa and her team.

[ ] Participate in future workshops hosted by Keio University CCRC to stay updated on security issues and solutions.

7 DAY 3: November 1 | East Research Building 8F Hall

7.1 D3-T2-S1 Robot Revolution Initiative (RRI)

Robot Revolution Initiative (RRI) Title: Trustworthiness concept for Supply & Value Chain Speaker: - Mahara Kumiko (Sony Semiconductor Solutions Corporation IS Business Strategy Department) - Takashi Ogura (Hitachi, Ltd. Research & Development Group, Connective Automation Innovation Center, Autonomous Control Research Department) - Nobuaki Suzuki (Toshiba Corporation) - Fumikado Anzai (MITSUBISHI HEAVY INDUSTRIES, LTD. Research & Innovation Center Control Systems Research Department)	ロボット革命イニシアティブ（RRI） タイトル：サプライチェーンとバリューチェーンに対するトラストワージネスのコンセプト Speaker: - 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） - 小倉 貴志（日立製作所 研究開発グループ コネクティブ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） - 鈴木 伸明（株式会社 東芝） - 安西 史圭（三菱重工業株式会社 総合研究所 制御システム研究部）
No record	

7.2 D3-T2-S2 Japan Cybersecurity Innovation Committee (JCIC)

Japan Cybersecurity Innovation Committee (JCIC) Theme: Cybersecurity is Your Own Business: Let's Spread It among Your Company Speaker: - Toshihiro HIRAYAMA (Visiting Fellow, JCIC & Professor, iUniversity) - Masahiro SAWADA (Visiting Fellow, JCIC)	日本サイバーセキュリティ・イノベーション委員会（JCIC） テーマ：「サイバーセキュリティは自分ごと」を社内に広める Speaker: - 平山 敏弘（JCIC 客員研究員 兼 情報経営イノベーション専門職大学(iU)教授） - 澤田 雅広（JCIC 客員研究員）
No record	

7.3 D3-T2-S3 Cybexer

Title: Smart City and Cyber Ranges Speaker: Ragnar Rattas (CybExer Technologies, CTO) Language: English	Cybexer タイトル：スマートシティとサイバーレンジ Speaker：ラーン・ラッタス（CybExer Technologies、最高技術責任者） 言語：英語
Cyber Ranges Red Team Smart City Systems **Theme** This speech provides an overview of cyber ranges as simulated environments for cybersecurity training, detailing their infrastructure, platform, game net, and exercise scenarios. It discusses the	

progression of red team attacks, the integration of smart city systems, and the visualization of real-world impacts during exercises. Key takeaways include the use of cyber ranges for training, testing, and research, and the importance of realistic and industry-specific scenarios. The lecture also highlights discrepancies in blue team reporting and the use of 3D map visualization for smart city components.

Takeaways

1. Cyber ranges as simulated environments for cybersecurity training
2. Different layers of a cyber range: infrastructure, platform, game net, exercise scenarios
3. Cyber range infrastructure can be on-premise or cloud-based
4. Cyber range platform includes content management, scoring, and various IT services
5. Game net layer consists of technical systems like virtual machines and physical equipment
6. Exercise scenarios can be industry-specific or general
7. Use cases for cyber ranges: exercises, training, testing, and research
8. Examples of game nets for industrial control systems and space technologies
9. Cyber range environments can be tailored to specific needs
10. Cyber range portals and mission boards for user interaction

Chapters & Topics

Cyber Ranges

Cyber ranges are simulated environments used for training cybersecurity engineers, testing organizations, and conducting cybersecurity exercises. They consist of various layers including infrastructure, platform, game net, and exercise scenarios.

- **Keypoints**
  - Cyber ranges provide a safe environment for cybersecurity tests and training.
  - They can be on-premise or cloud-based.
  - The platform includes content management, scoring, and various IT services.
  - Game net consists of technical systems like virtual machines and physical equipment.
  - Exercise scenarios can be tailored to specific industries or be general.
- **Explanation**
  - Cyber ranges are designed to simulate real-world environments where cybersecurity professionals can practice and hone their skills. They include various components and layers that work together to create a comprehensive training and testing environment.
- **Examples**

A training environment consisting of three virtual machines: one PLC, one human-machine interface, and one Windows 10 workstation. This setup is cloned for each participant in a training session.

  - The environment is created to simulate industrial control systems.
  - Each participant receives a clone of the environment for hands-on training.
  - The setup allows participants to interact with realistic systems and scenarios.

An intermediate-sized network diagram representing space technologies, including business services, security systems, and industry-specific systems like satellite mission control.

  - The environment includes realistic software used in real-world space operations.

- Participants can interact with systems like satellite mission control.
- The setup is designed to be as realistic as possible for training purposes.
- **Considerations**
- Ensure the cyber range environment is realistic and relevant to the training objectives.
- Consider the scalability of the environment to accommodate multiple participants.
- Align training scenarios with recognized frameworks for consistency and standardization.
- **Special Circumstances**
- If encountering a situation where the cyber range needs to simulate a specific industry, tailor the game net and scenarios to reflect that industry's unique challenges and systems.

Red team attack progression

The progression of red team attacks in exercises, starting from gaining access to workstations, moving to Windows domain controllers, and finally targeting power grid SCADA systems.

- **Keypoints**
- Initial phase targets workstations.
- Subsequent phases target Windows domain controllers.
- Final phase targets power grid SCADA systems.

Technical exercise target check status

A page that shows the status of various technical services during exercises, indicating whether services are up or down.

- **Keypoints**
- Each box represents a system in the exercise environment.
- Measures availability of technical services.
- Used to calculate availability scores.

Differences in blue team reporting and actual status

Discrepancies between what blue teams report and the actual status of systems during exercises.

- **Keypoints**
- Blue teams may miss red team attacks.
- Blue teams may report non-existent compromises.

Integration of smart city systems in exercises

The inclusion of smart city systems like SCADA and smart traffic lights in cyber exercises.

- **Keypoints**
- Smart city systems are represented as boxes on a map.
- Allows visualization of real-world impacts.

Real-world impact visualization

The ability to visualize the real-world impacts of IT system failures during exercises.

- **Keypoints**
- Buildings or districts are colored based on system status.
- Shows impact of losing access to critical infrastructure.

3D map visualization for smart cities

A new feature that allows the visualization of smart city components on a 3D map during exercises.

- **Keypoints**
- Maps technical systems to real-world objects.

○ Improves understanding of real-world impacts. **Assignments & Suggestions**

7.4 D3-T2-S4 CyLogic

CyLogic Title: FedRAMP Cloud Training for Japan Speaker: Chris Grady (CTO, CyLogic) Language: English	CyLogic タイトル：FedRAMP クラウドの日本向けトレーニング Speaker：クリス・グラッディ（CyLogic, CTO) 言語：英語
No record	

Change History

Date	Part	Comment
2024/12/17	Whole	New release