明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

IoT社会に対応したサイバー・フィジカル・セキュリティ
～内閣府SIP第2期の取組み ～

元　内閣府 SIP プログラムディレクタ

Former Program Director, SIP Phase 2/Cyber Physical Security for IoT Society

情報セキュリティ大学院大学

President, Institute of Information Security

後藤　厚宏

GOTO, Atsuhiro

プロフィール　後藤　厚宏

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

■ 1984年 工学博士。NTT研究所にて先進ICT技術の研究開発等に従事。

- 第5世代コンピュータPJ（1985～1990）、米国シリコンバレー拠点（1994～1996）

産

■ 2011年7月より情報セキュリティ大学院大学教授。2017年4月より学長

- **約7割が社会人。OB・OGは官公庁・企業で活躍中。**

学

■ 2015年11月～2023年3月 内閣府SIPプログラムディレクター 併任

- SIP第1期：重要インフラ等のサイバーセキュリティ確保（2015～2019）
- SIP第2期： IoT社会に対応したサイバー・フィジカル・セキュリティ （2018～2022）

官

■ 2019年2月より日本政府のサイバーセキュリティ戦略本部員

内閣府　SIPプログラムディレクタ（PD）

2015～2019

重要インフラ等における サイバーセキュリティの確保

世界で最も安心・安全な社会基盤の確立を目指して

近年、サイバーセキュリティ攻撃の脅威はますます深刻化しており、その矛先も通信・放送、エネルギー、交通といった社会を支える重要インフラに向けられ始めている。2020年東京オリンピック・パラリンピック競技大会を迎える我が国においても、重要インフラにおけるサイバーセキュリティの確保は緊急の課題であり、その技術開発と人材育成に大きな期待が寄せられている。重要インフラ等におけるサイバーセキュリティの確保では、オールジャパン体制で迅速かつ大胆に推進する。

※本課題は他課題より1年遅れて開始したため、実施期間は平成27年度から令和元年度

プログラムディレクター

後藤 厚宏

情報セキュリティ大学院大学 学長

Profile

1984年東京大学大学院工学系研究科情報工学専攻博士課程修了。同年日本電信電話公社に入社、約27年間情報技術に関する研究開発に従事。2007年NTT情報流通プラットフォーム研究所長、10年NTTサイバースペース研究所長を歴任。11年より情報セキュリティ大学院大学情報セキュリティ研究科教授、17年より現職。内閣官房、総務省、文部科学省、経済産業省、防衛省などの審議会、委員会等における委員長等および委員を歴任。

＊：PDの所属・肩書は第1期終了時点（平成30年度末）のものとする。

研究開発テーマ

(a) コア技術の開発：制御・通信機器と制御ネットワークのセキュリティ対策技術の開発

- 制御・通信機器の真贋判定技術（機器やソフトウェアの真正性・完全性を確認する技術）を開発する。
- 制御・通信機器および制御ネットワークの動作監視・解析技術を開発する。
- 制御・通信機器およびシステムの防御技術を開発する。

(b) 社会実装技術の開発：社会実装向け共通プラットフォームの実現と、セキュリティ人材の育成

- セキュリティ技術の普及を促進する適合性確認のあり方と仕組みを検討する。
- インフラ事業者間をまたがる情報共有プラットフォーム技術を開発する。
- 重要インフラにセキュリティ技術を適用するうえでの評価検証プラットフォーム技術を開発する。

2018～2022

IoT社会に対応した サイバー・フィジカル・セキュリティ

Society 5.0を支える強靭なセキュリティ基盤の確立を目指す

産業システムや生活環境等のフィジカル空間に埋め込まれたIoT機器が、多様なネットワークを介してクラウド等のサイバー空間と連結され、高度な知識処理や分析・解析処理との連携により、様々な付加価値を創出しフィジカル空間である経済社会に多大な恩恵をもたらす。一方、IoTの普及・拡大に伴いサイバー攻撃の脅威があらゆる産業活動に潜みつつあり、製品やサービスを製造・流通する過程で不正なプログラムの組込みや改造が行われるサプライチェーンリスクの問題も顕在化している。このため、IoTシステム／サービス及び中小企業を含む大規模サプライチェーン全体を守る「サイバー・フィジカル・セキュリティ対策基盤」の開発を行い、実稼働するサプライチェーンに組み込み実用化することで、サイバー脅威に対するIoT社会の強靭化を図る。

プログラムディレクター

後藤 厚宏

情報セキュリティ大学院大学 学長

Profile

1984年東京大学大学院工学系研究科情報工学専攻博士課程修了。同年日本電信電話公社に入社、約27年間情報技術に関する研究開発に従事。2007年NTT情報流通プラットフォーム研究所長、10年NTTサイバースペース研究所長を歴任。11年より情報セキュリティ大学院大学情報セキュリティ研究科教授、17年より現職。内閣官房、総務省、文部科学省、経済産業省、防衛省などの審議会、委員会等における委員長等および委員を歴任。

研究開発テーマ

IoT機器やサプライチェーンの各構成要素についてセキュリティの確保（信頼の創出）とその確認（信頼の証明）を繰り返し行い、信頼のチェーンを構築・維持することで、IoTシステム／サービス及びサプライチェーン全体のセキュリティを確保する。

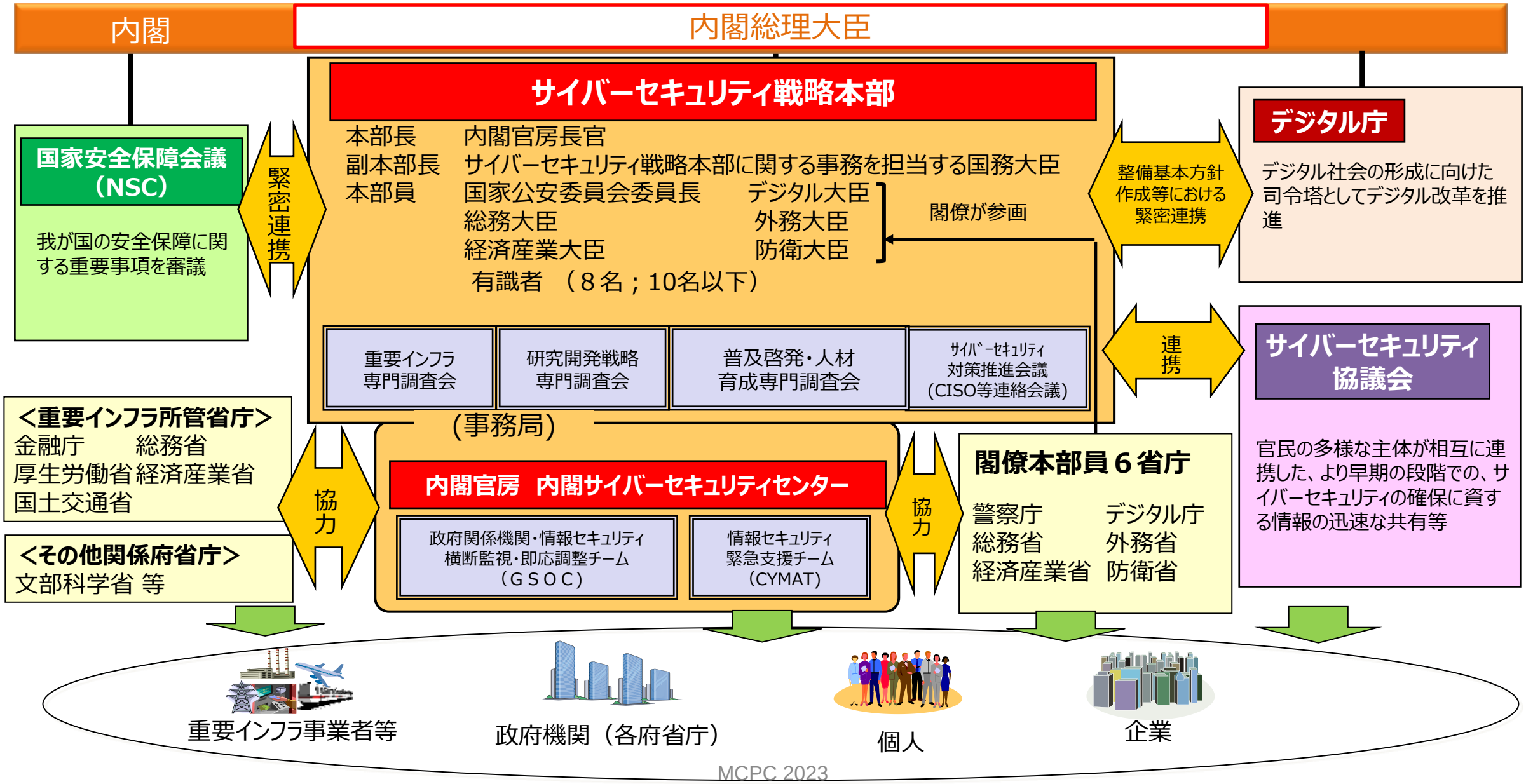
(A)「信頼の創出・証明」技術の研究開発

(B)「信頼チェーンの構築・流通」技術の研究開発

多様な社会インフラやサービス、幅広いサプライチェーンのセキュリティを確保するため、IoTシステム／サービスや調達・構築に関わるサプライチェーンにおいて「信頼チェーン」を構築し、必要な情報をセキュアに流通させる技術を研究開発する。

(C)「信頼チェーンの検証・維持」技術の研究開発

サイバーセキュリティ戦略の推進体制



NISC 内閣サイバーセキュリティセンター
National center of Incident readiness and Strategy for Cybersecurity

ホーム | 内閣サイバーセキュリティセンター(NISC)について | お知らせ | 政策

ホーム > 会議 > サイバーセキュリティ戦略本部

サイバーセキュリティ戦略本部

https://www.nisc.go.jp/council/cs/index.html

2023年(令和5年)

第36回会合(令和5年7月4日)

決定文書

- サイバーセキュリティ2023
- サイバーセキュリティ関係施策に関する令和6年度予算重点化方針
- 政府機関等のサイバーセキュリティ対策のための統一規範
- 政府機関等のサイバーセキュリティ対策のための統一基準(令和5年度版)
- 重要インフラのサイバーセキュリティに係る安全基準等策定指針

重要インフラのサイバーセキュリティに係る安全基準等策定指針

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

■ 経営層による管理体制の整備

- サイバーセキュリティを確保できないこと ＝ 経営リスクのひとつ
- CISO等は役員相当。監査にて脆弱性診断、ペネトレーションテスト等の実施を推奨。

■ ランサムウェア対策とクラウドサービス利用

- ランサムウェア対策：バックアップからの復旧確認とネットワーク隔離
- クラウドサービス利用に係る対策：ステークホルダーとの障害対応体制の構築

■ サプライチェーンリスク対策の強化

- 直接の供給者と、担うべき役割と責任範囲を明確化

① 不正機能等の埋め込み**「汚染」**

② サービスの供給途絶**「寸断」**

③ 外部サービスにおける情報の不適切な取扱い

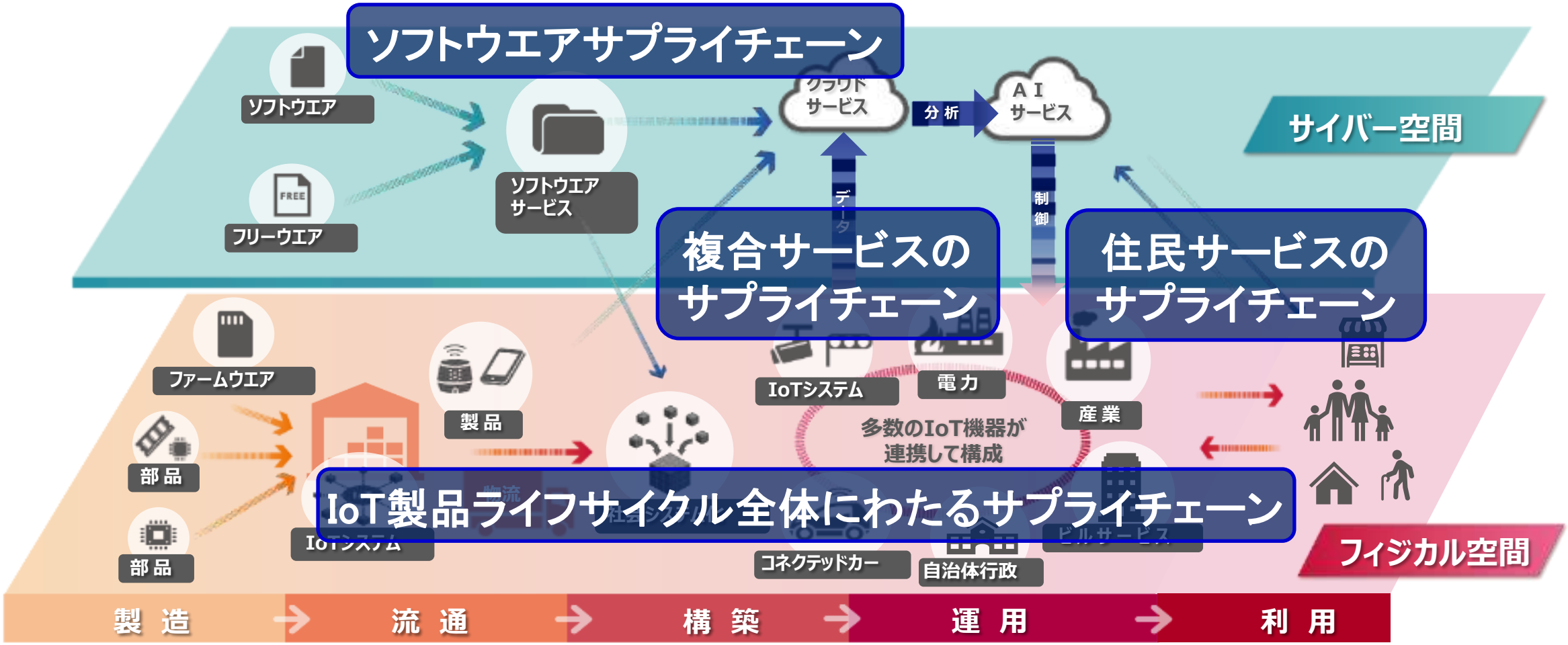
④ 海外拠点、グループ組織、取引先等を経由したサイバー攻撃等の脅威に対応**「弱点」**

アウトライン

- IoT社会におけるサプライチェーンのセキュリティ課題
- サプライチェーン「寸断」のリスク
- サプライチェーンにおけるソフトウェア「汚染」
- **内閣府SIP：サイバー・フィジカル・セキュリティへの取組み**
  （SIP第2期　2018～2022年度）
- まとめとディスカッション（Q&A）

IoT社会とサイバー・フィジカル・セキュリティ

サイバー空間とフィジカル空間の双方に跨るIoT社会でのサプライチェーン



IoT社会のサプライチェーン：サイバー攻撃リスク

Supply chain Cybersecurity Matters

2018年頃の「将来の想定リスク（懸念）」が、今日「現実の問題」として顕在化

2018年頃の将来の懸念

IoTリスク：サイバー攻撃脅威が、あらゆる産業活動に潜む

- IoT社会では、サイバー攻撃がフィジカル空間まで到達し、**経済損失が拡大**するリスク
- 欧州、米国等：ネットワークに繋がる**IoT機器のセキュリティ要件**の議論が活発に

サプライチェーンリスク：セキュリティ確保が調達要件に

- 米国：防衛調達の全参加企業にセキュリティ対策（SP800-171）を**義務化**

懸念が現実に

- 管理不十分なIoT機器による大規模サイバー被害とサイバー攻撃による大規模な事業停止　⇒世界的な危機感の高まり
- 大規模ソフトウェアサプライチェーン攻撃
  ⇒米国連邦政府の危機感
- コロナ禍やウクライナイ事案によるグローバルサプライチェーンの分断（経済安保＠日本）

サプライチェーン・サイバー攻撃リスク

Supplychain Attacks

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

2019年 防衛装備品情報の窃取

2022年 デンソー（独）へのランサムウェア攻撃

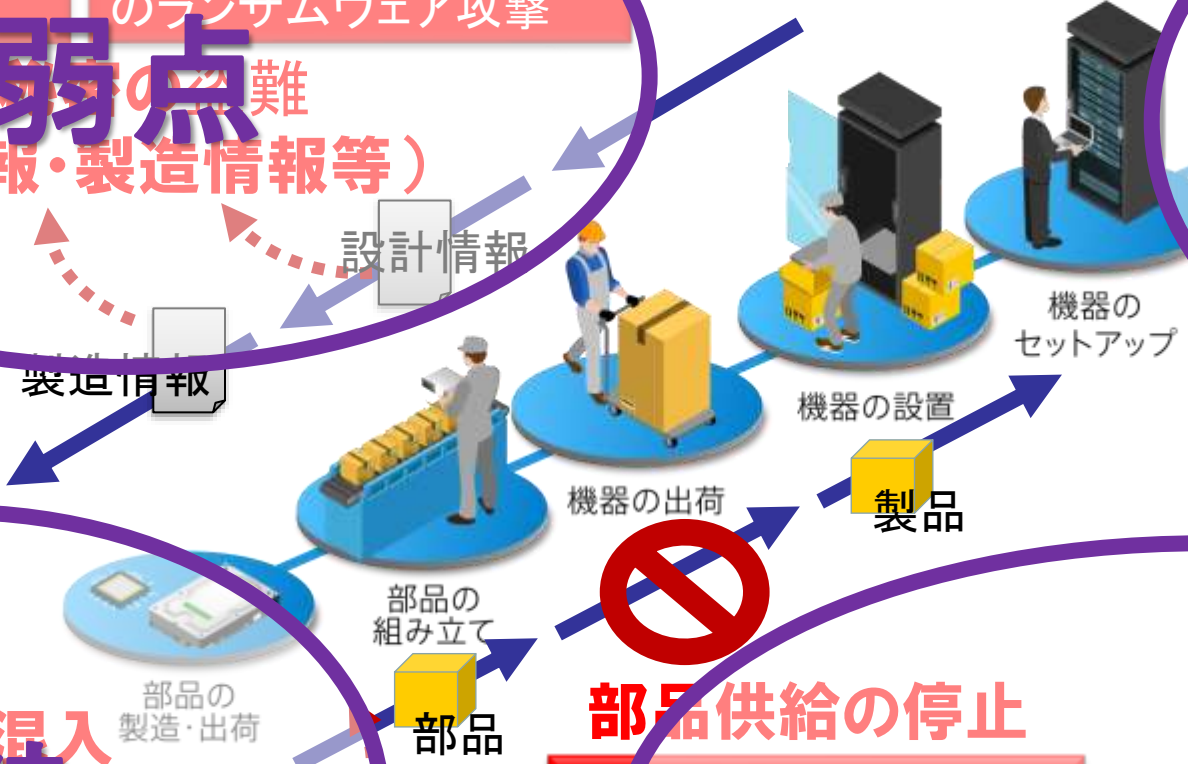
弱点

営業秘密の盗難
（設計情報・製造情報等）

2020年 米国SolarWinds社：
運用システムの更新プログラムがサイバー攻撃によって改ざん

汚染

不正なソフトウェアの混入



不正な部品の混入

汚染

2016年 米国セキュリティ会社が携帯電話部品に仕込まれている不正プログラムを発見

部品供給の停止

2022年 小島プレスへのサイバー攻撃でトヨタが新車生産を停止

エネルギー供給の停止

寸断

2021年 米国コロニアルパイプライン社へのランサムウエア攻撃： ガソリン供給網の寸断

サプライチェーン「寸断」のリスク

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

金銭目的のサイバー攻撃

- 情報窃取を狙いとするサイバー攻撃
  ⇒ 銀行口座からの不正引出し
- 暗号通貨の窃取（サイバー空間上での金融犯罪）
- 金融ATMへの攻撃

サービス妨害のサイバー攻撃

- サイバー空間でのサービス停止（妨害）を狙う攻撃（DDoS等）
- 重要インフラへの攻撃（ウクライナ停電 2015，2016）

課題の深刻化

社会・産業活動（**事業継続性**）へのサイバー攻撃

＋

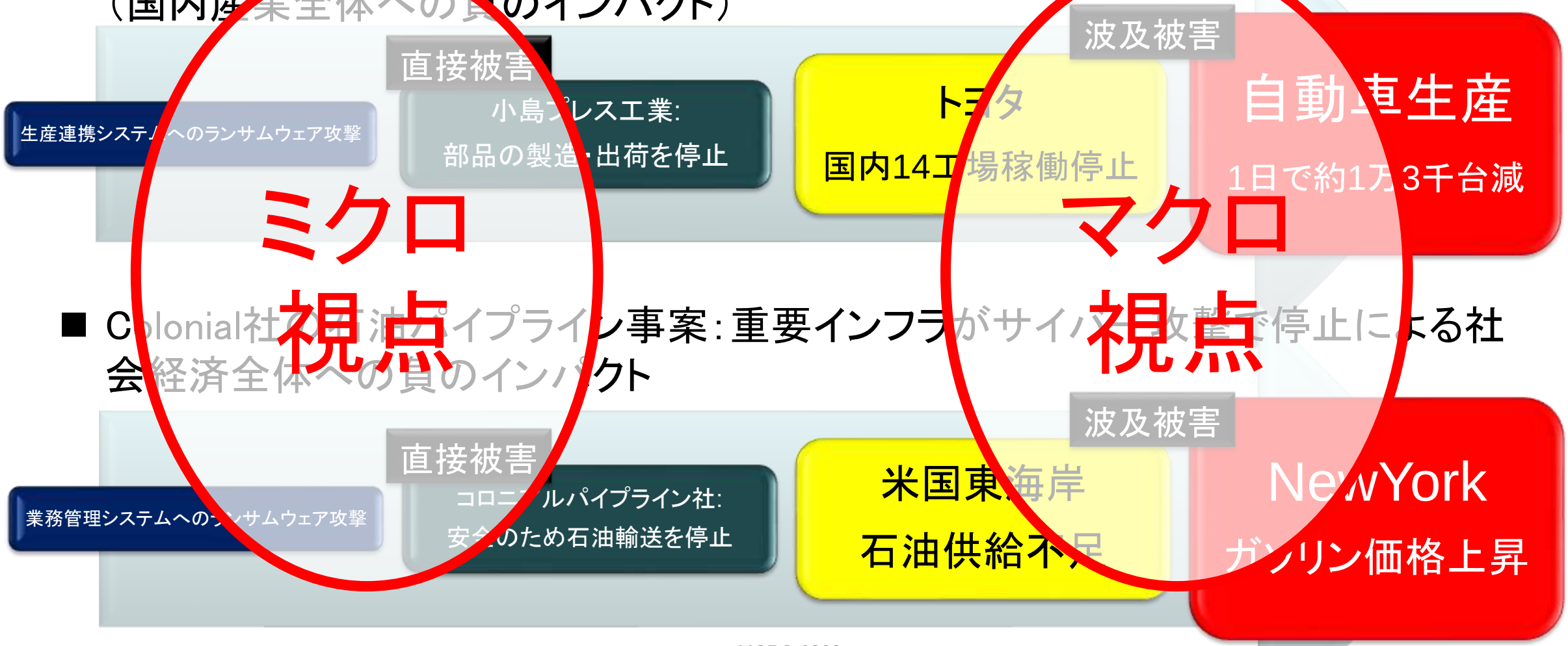
金銭目的サイバー攻撃（**ランサムウェア**）

事業が停止し、
サプライチェーンが寸断

事業停止の被害の拡大・波及

サプライチェーン「寸断（事業継続停止）」がもたらす被害の連鎖・大規模化

■ 小島プレス工業事案：サイバー攻撃で停止によるトヨタの自動車生産事業の停止（国内産業全体への負のインパクト）



■ Colonial社の石油パイプライン事案：重要インフラがサイバー攻撃で停止による社会経済全体への負のインパクト

不正機能・ソフトウェアの混入による「汚染」

不正機能の混入はサイバー攻撃の典型

ソフトウェアに残存する**脆弱性**

- マルウェア（不正機能）混入の入口

- Webでダウンロード
- メールの添付ファイル
- Webアプリケーションでのインジェクション攻撃

サプライチェーンにおける課題の深刻化

大量の製品で使われる部品への混入

（例　2016年 携帯電話部品の問題）

ソフトウェアサプライチェーン攻撃

多数のユーザを持つソフトウェアシステムへの（同時・一斉）「汚染」攻撃

- ソフトウェア更新機構の乗っ取り
- 利用が多いOSS（特に部品ソフト）の脆弱性への攻撃

被害の大規模・広域拡大・波及

急増するソフトウェア「汚染」サプライチェーン攻撃

■ 3年間で742%の急増（製造業・非製造業・官公庁）

Source: Sonatype社の2023レポート

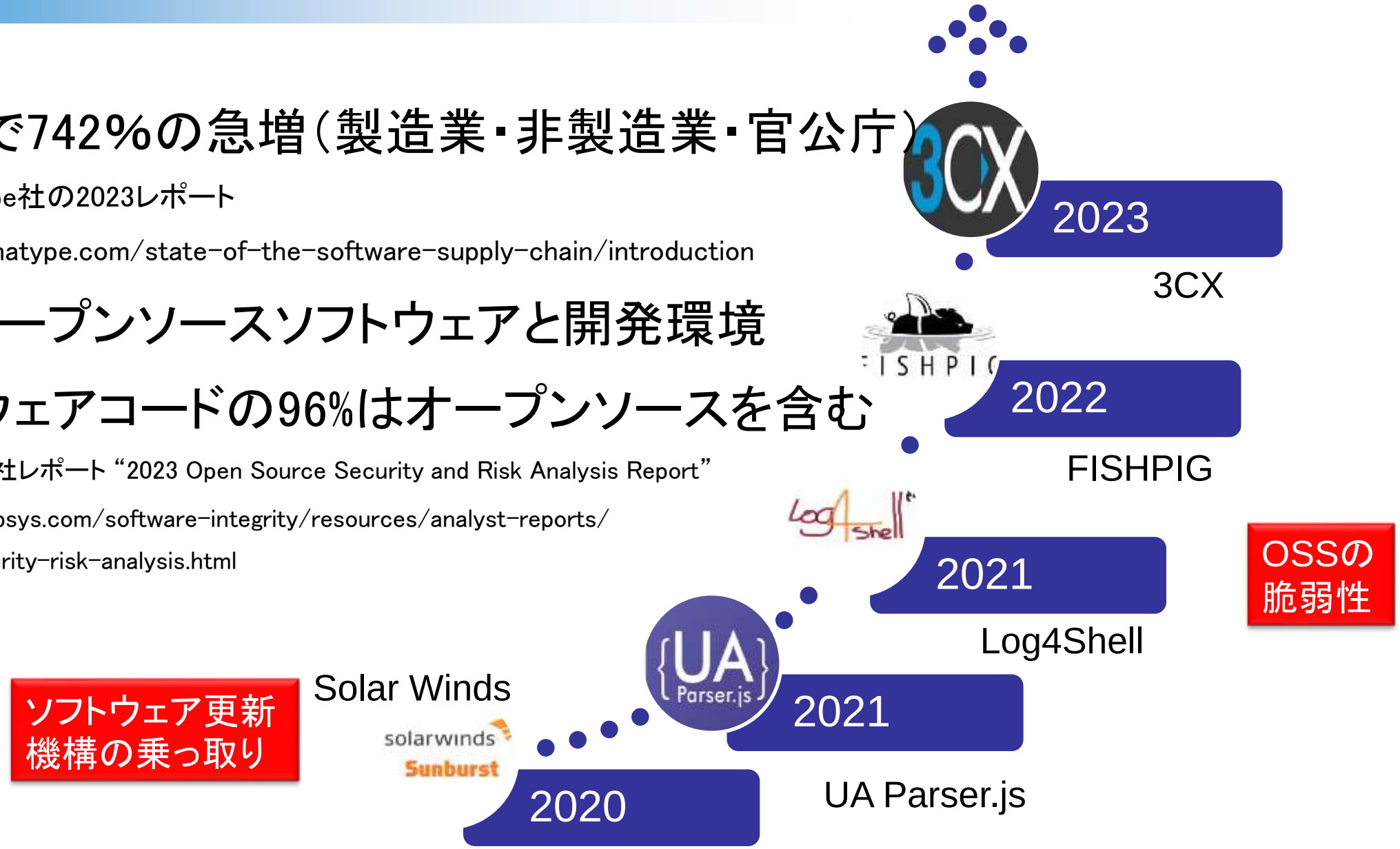
https://www.sonatype.com/state-of-the-software-supply-chain/introduction

■ 特にオープンソースソフトウェアと開発環境

■ ソフトウェアコードの96%はオープンソースを含む

Source: Synopsys社レポート “2023 Open Source Security and Risk Analysis Report”

https://www.synopsys.com/software-integrity/resources/analyst-reports/open-source-security-risk-analysis.html



利用が多いOSSの脆弱性を悪用した攻撃（部品ソフトの「汚染」）

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

Log4Shellの例

Javaのログ出力ライブラリー「Apache Log4j」の脆弱性（Log4Shell）は脆弱性スコアCVSSが最大 ⇒ランサムウエア（身代金要求型ウイルス）攻撃への悪用が容易

Log4JはWebサーバーとして広く利用されているシステムに標準機能として組込み

- 米Vmwareの仮想デスクトップ構築用ソフト「Vmware Horizon」などの商用システム　など

部品として取り込んだ脆弱性のあるOSSによって多くの商用ソフトウェアシステムが「汚染」

サイバーセキュリティ関係施策に関する令和6年度予算重点化方針（2023/7/4決定）

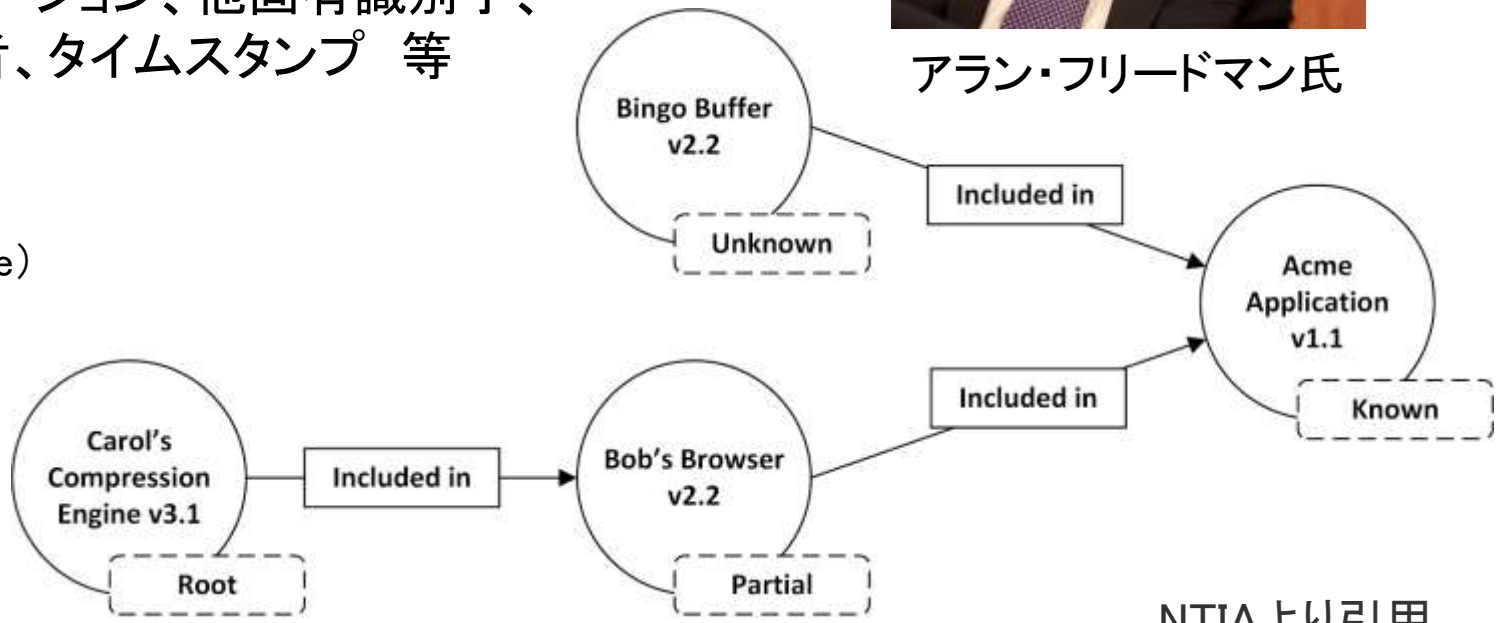
2 サプライチェーン・リスクを踏まえたソフトウェアセキュリティの高度化に関する取組

脆弱性情報とSBOM（Software Bill of Materials ソフトウェアの部品構成表）の機械的な紐付けに係る実証を行うなど、2022年度までの取組を深化させ、ソフトウェアセキュリティの高度化に向けた取組を進める。また、代表的な通信システムを対象にSBOMを作成・評価するなど、通信分野でのSBOM導入に向けた取組を進める。

SBOM（Software Bill of Materials）について

- ソフトウェアの透明性（トランスペアレンシー）向上のための「成分表」　（by 米DOC, NTIA）
- SBOMの内容
  - 提供者名、コンポーネント名とバージョン、他固有識別子、依存関係、SBOMデータの作成者、タイムスタンプ　等
- SBOMのフォーマット
  - SPDX（Software Package Data Exchange）
  - SWID（Software Identification）
  - Cyclone DX （OWASP）

アラン・フリードマン氏



NTIAより引用

https://www.ntia.gov/files/ntia/publications/ntia_sbom_framing_2nd_edition_20211021.pdf

ソフトウェアセキュリティにおけるSBOMの活用

■ サプライチェーンを通じた脆弱性対応、インシデント対応の迅速化

- 経産省：サイバー・フィジカル・セキュリティ確保に向けたソフトウェア管理手法等検討タスクフォース
  https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_bunyaodan/software/index.html
- 総務省：通信分野におけるSBOMの導入に向けた課題の調査
  ◆「ICTサイバーセキュリティ総合対策2023」（案）https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00169.html

■ 内閣府SIP：サイバー・フィジカル・セキュリティへの取組み

- サプライチェーン攻撃からIoT製品を守るソフトウェア真贋判定
- 複合サービスサプライチェーンの信頼構築フレームワーク

SolarWinds社の事案（2020年）:「更新」機構の乗っ取り

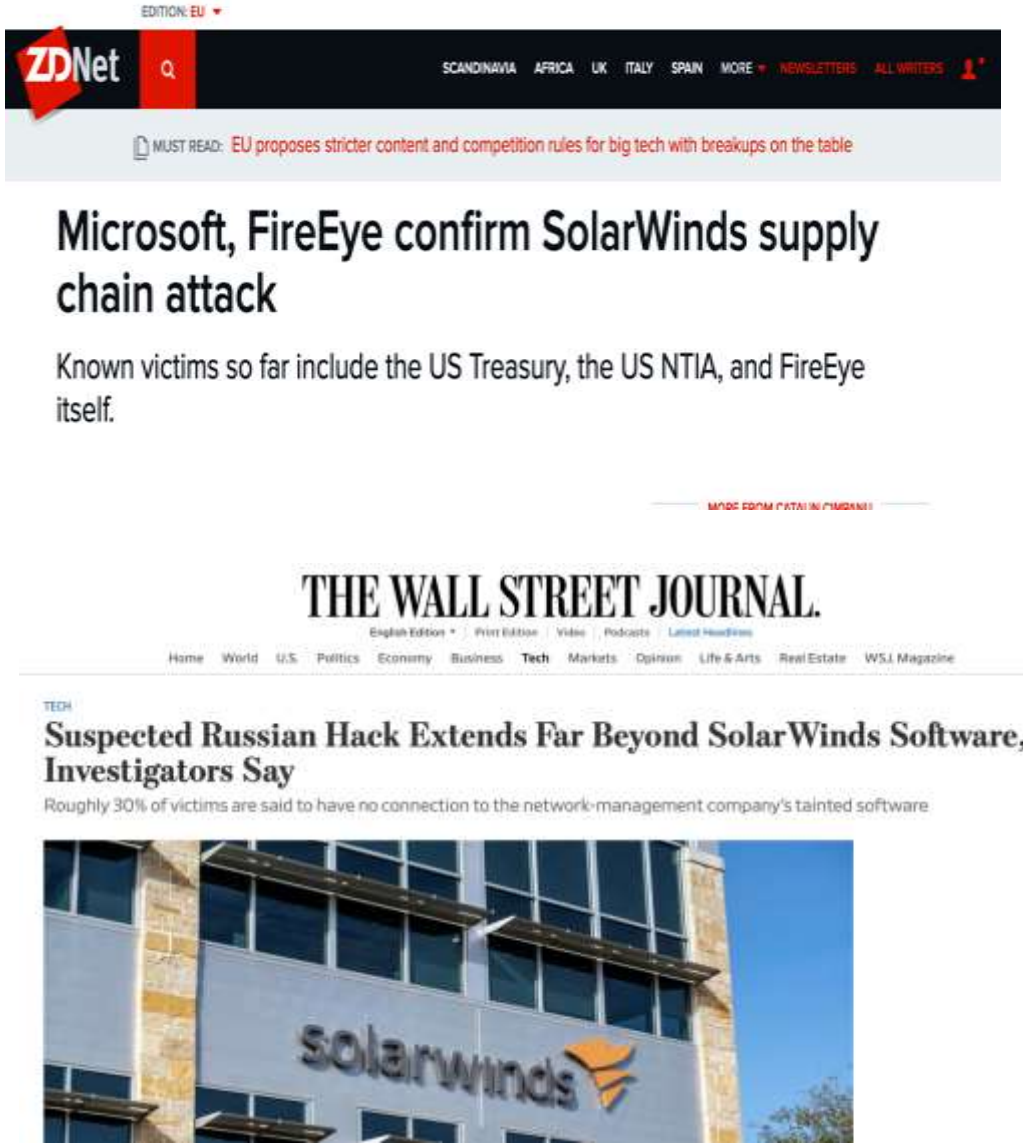
- SolarWinds社が提供するネットワーク監視ソフトウェア「Orion Platform」を用いる米国連邦政府機関（財務省・国務省・国家核安全保障局など）やMicrosoft,　Cisco, FireEyeなどの大企業（合計18,000組織）が大規模なサイバー攻撃の被害を受けた
- 同社が2020年3月と6月に配布したアップデートが改ざんされた?　　国家の関与？

ソフトウェアサプライチェーン攻撃は
セキュリティ維持の枠組みの危機！

「史上最大かつ最も巧妙」＝マイクロソフト社長

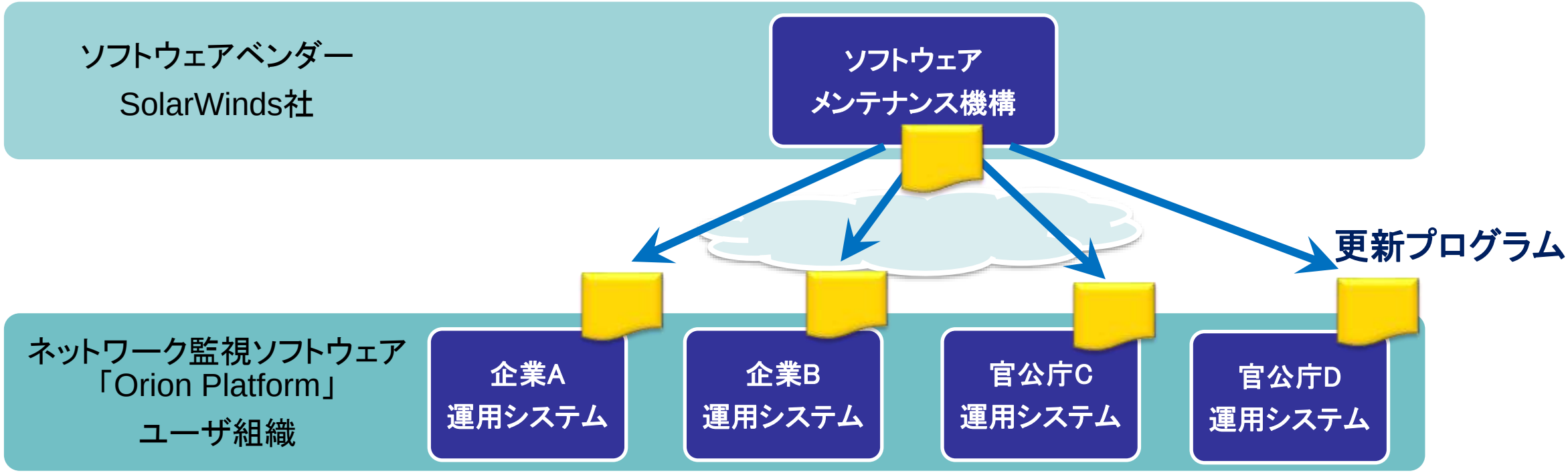
- SIP CPSシンポジウム2021　招待講演

https://www.youtube.com/watch?v=OL_Q3f4pI94



ソフトウェアサプライチェーン攻撃と被害の拡大

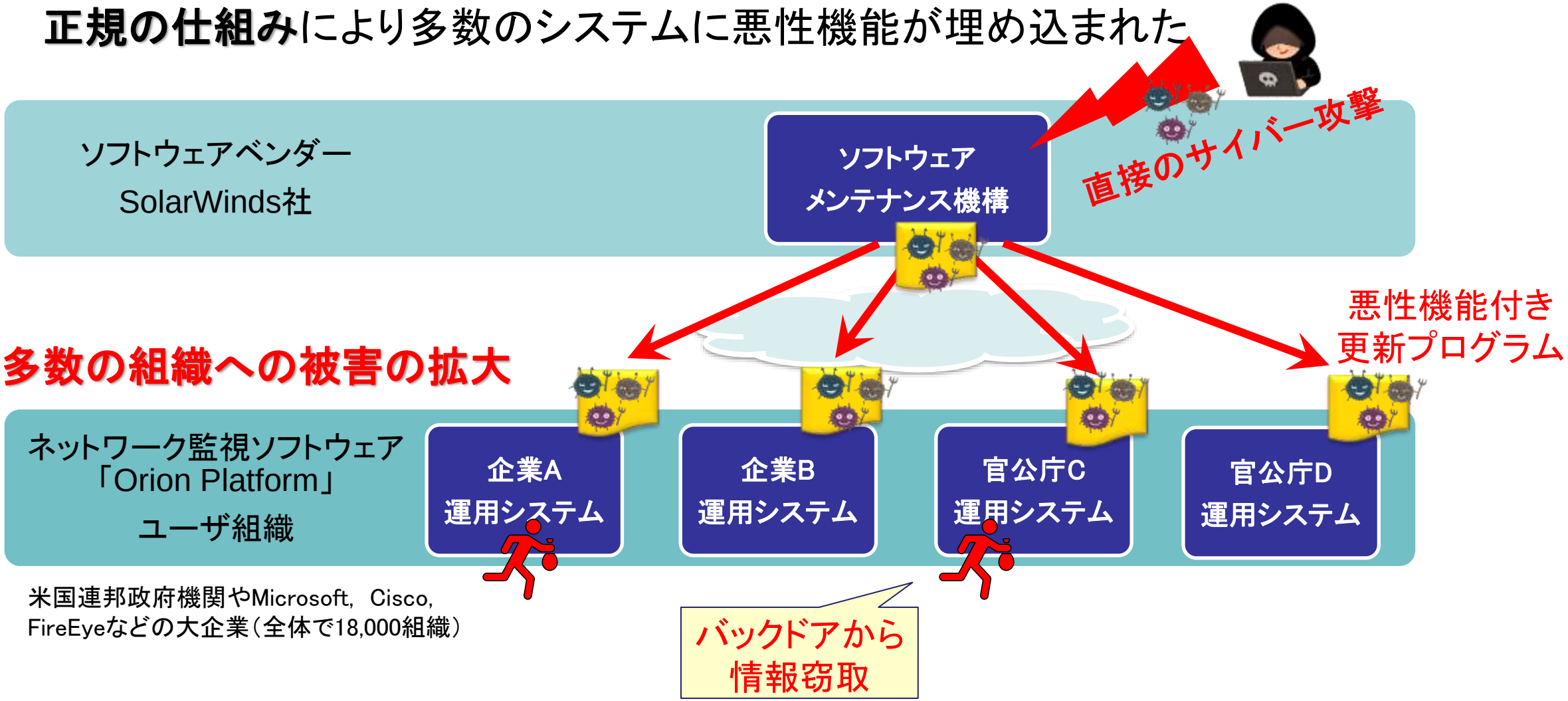
■ SolarWinds社の事案：ソフトウェアの更新機構が攻撃され、**更新プログラムを配布する正規の仕組み**により多数のシステムに悪性機能が埋め込まれた



米国連邦政府機関やMicrosoft，Cisco，
FireEyeなどの大企業（全体で18,000組織）

ソフトウェアサプライチェーン攻撃と被害の拡大

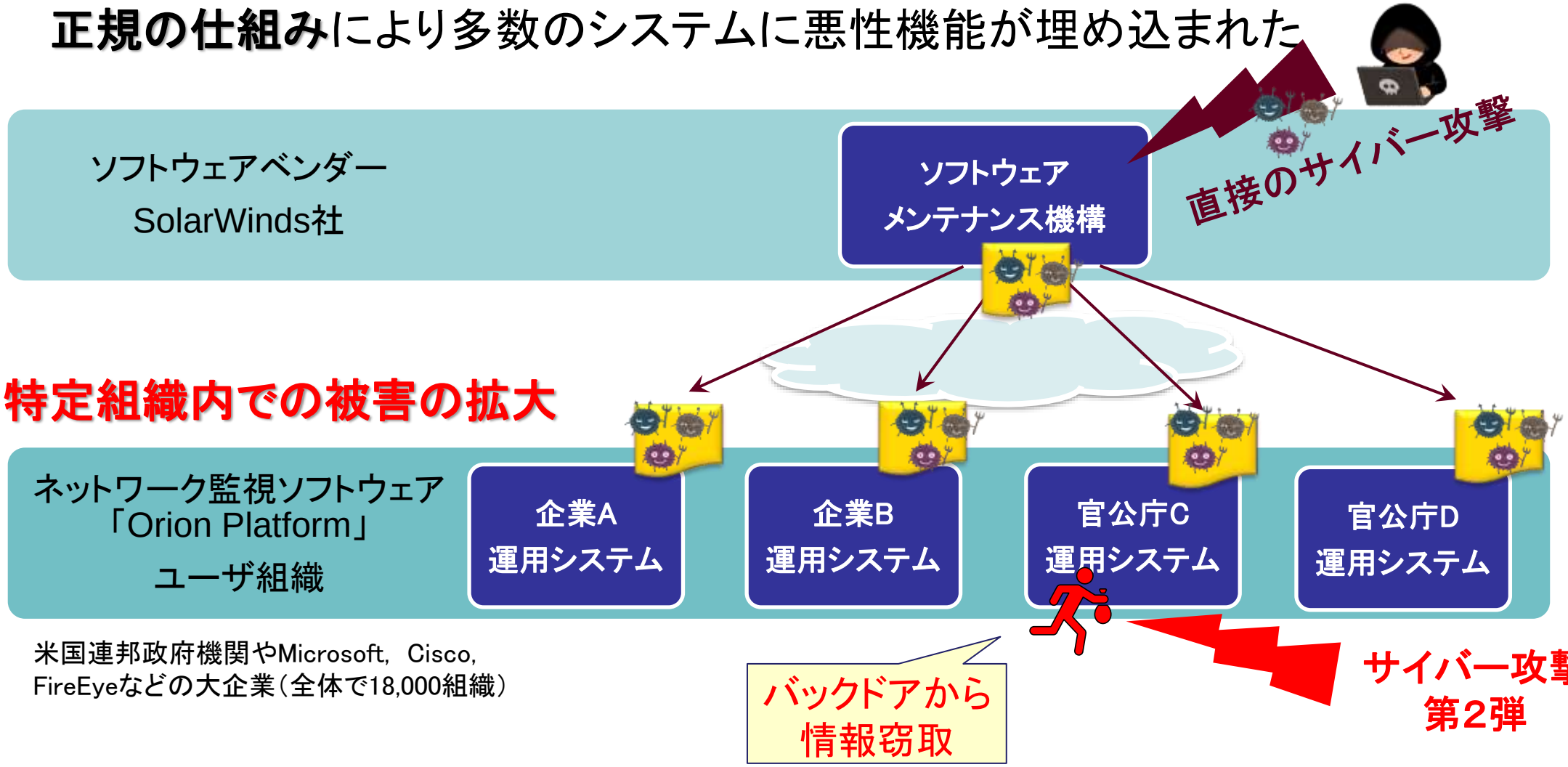
■ SolarWinds社の事案：ソフトウェアの更新機構が攻撃され、**更新プログラムを配布する正規の仕組み**により多数のシステムに悪性機能が埋め込まれた



米国連邦政府機関やMicrosoft，Cisco，FireEyeなどの大企業（全体で18,000組織）

ソフトウェアサプライチェーン攻撃と被害の拡大

■ SolarWinds社の事案：ソフトウェアの更新機構が攻撃され、**更新プログラムを配布する正規の仕組み**により多数のシステムに悪性機能が埋め込まれた



米国連邦政府機関やMicrosoft，Cisco，FireEyeなどの大企業（全体で18,000組織）

サプライチェーンのセキュリティ課題

Supply chain Cybersecurity Matters

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

2018年頃の「将来の想定リスク（懸念）」が、今日「現実の問題」として顕在化

2018年頃の将来の懸念

IoTリスク：サイバー攻撃脅威が、あらゆる産業活動に潜む

- IoT社会では、サイバー攻撃がフィジカル空間まで到達し、**経済損失が拡大**するリスク
- 欧州、米国等：ネットワークに繋がる**IoT機器のセキュリティ要件**の議論が活発に

サプライチェーンリスク：セキュリティ確保が調達要件に

- 米国：防衛調達の全参加企業にセキュリティ対策（SP800-171）を**義務化**

懸念が現実に

- 管理不十分なIoT機器による大規模サイバー被害とサイバー攻撃による大規模な事業停止　⇒世界的な危機感の高まり
- 大規模ソフトウェアサプライチェーン攻撃
  ⇒米国連邦政府の危機感
- コロナ禍やウクライナイ事案によるグローバルサプライチェーンの分断（経済安保＠日本）

対応策が急遽検討

- 米国 Software Supply Chain対策の指南書 by U.S. NSA, CISA, ODNI（2022/9）とSBOM本格活用への動き

SBOM：Software Bill of Materials

- 米国 MITRE社 サプライチェーンセキュリティの “System of Trust” の枠組み
- EU IoT類を含むネットワーク接続機器類への規制強化（EU Cyber Resilient Act）

サプライチェーンのセキュリティ確保に関する連邦政府動向

U.S. Federal Government tackling Supplychain Issues

頻発するサイバーセキュリティ被害

ソフトウェアサプライチェーン攻撃の大規模被害

重要インフラで多用されるOSSへの脆弱性への攻撃被害

「汚染」

LOG4J

ランサムウェアによる事業継続攻撃の被害

国家のサイバーセキュリティ改善に係る大統領令（EO14028）2021/5/21

NIST National Institute of Standards and Technology U.S. Department of Commerce　NTIA

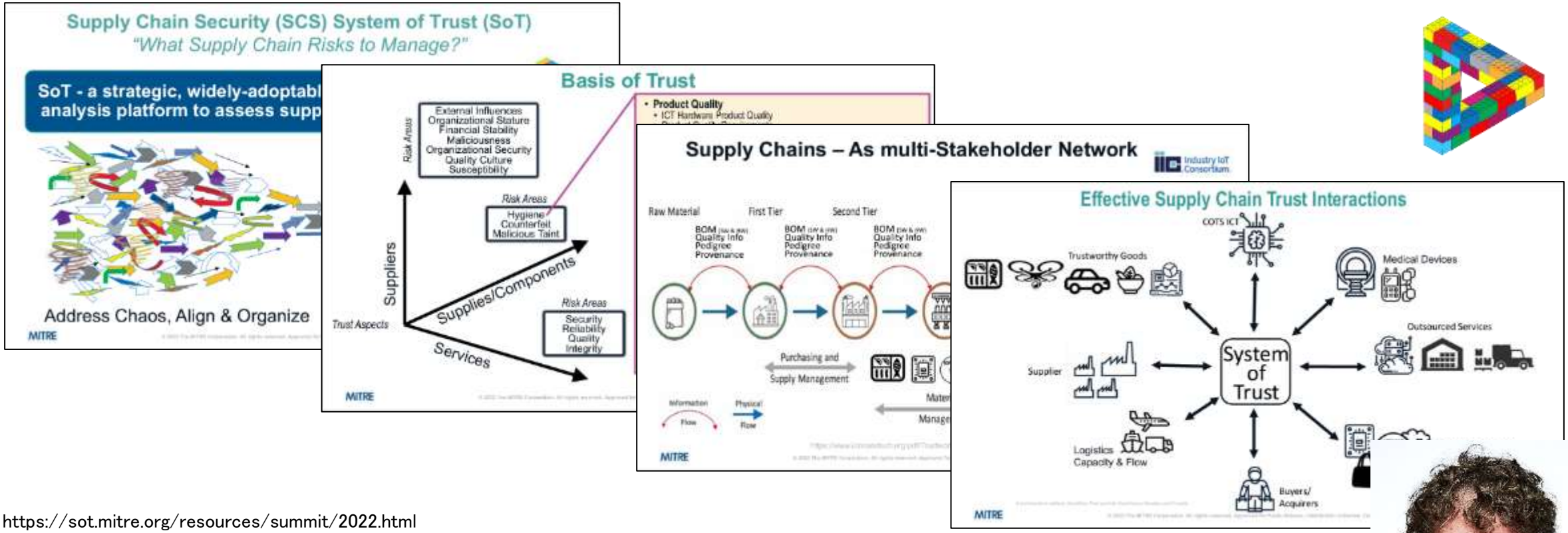
2021.5.12	大統領令の署名	
2021.6.25	「重要なソフトウェア」の定義の公表	NIST DoD DHS
2021.7.9	「重要なソフトウェア」のセキュリティ対策に係るガイダンスの公開	OMB
	ソフトウェア検証の最低基準に関するガイドラインの公表	NIST DHS
2021.7.12	SBOMの最小要素の公表	OMB
2021.8.10	NISTが公開した重要なソフトウェアのセキュリティ対策に関するガイダンスを、各省庁が遵守することを求めるための措置を講じる	NIST DHS NIST NTIA
2021.11.17	ソフトウェア サプライヤー プレイブック: SBOM の作成と提供	OMB
	ソフトウェア コンシューマー プレイブック: SBOM の取得、管理、および使用	NTIA
2021.11.29	連邦政府各省庁を対象としたIoTを利用する際の手引書	NTIA
2022.2.4	消費者向けソフトウェア製品のサイバーセキュリティラベリング推奨基準	NIST
	消費者向けIoTソフトウェア製品のサイバーセキュリティラベリング推奨基準	NIST
2022.3.8まで	大統領令以降に調達されたソフトウェアに関して、各省庁がNISTによる指針を遵守するための適切な措置を講じる	NIST OMB
2022.5.5	サプライチェーン全体のサイバーセキュリティリスクを特定、評価、および軽減するためのガイダンス	NIST
2022.5.12まで	FAR審議会に対し、各省庁が購入可能なソフトウェアサプライヤーに対する上記ガイダンスに基づく要求事項の遵守と、遵守の証明を義務付ける契約文言を勧告	DHS

※経産省サイバー・フィジカル・セキュリティ確保に向けたソフトウェア管理手法等検討タスクフォース資料等を参照

MITRE社 サプライチェーンセキュリティの“System of Trust”

MITRE’s System of Trust

米MITREが提唱するサプライチェーン共通の安全性を確保するためのフレームワーク



https://sot.mitre.org/resources/summit/2022.html

SIP CPSシンポジウム基調講演　米MITRE社　ロバート・マーティン氏

https://www.youtube.com/watch?v=llgi-K4ZXhs

EU Cyber Resilience Act（2022/9に草案⇒2025年？）

■ 法案の狙い

- Digital Elementsの設計、開発段階から**全てのライフサイクル**で**製造業者**が製品セキュリティの改善を**保障**すること。
- 既存の規則で対象となる製品（医療機器等）は対象外
- 当該製品に対するセキュリティ要件への**適合性証明**（自己適合宣言もしくは第三者認証）

■ 他

- ドイツ、シンガポール、フィンランド：消費者向けIoT製品に対するセキュリティラベリング制度
- 英国：消費者向けIoT製品に対してセキュリティ対策の義務化を求める法律（Product Security and Telecommunications Infrastructure）

SIP

戦略的イノベーション創造プログラム
Cross-ministerial Strategic Innovation Promotion Program

II

【平成30年度～令和4年度】

日本発の科学技術イノベーションが未来を拓く

～ 12課題 ～

SIP

【平成30年度～令和4年度】

戦略的イノベーション創造プログラム
Cross-ministerial Strategic Innovation Promotion Program

日本発の科学技術イノベーションが未来を拓く

ビッグデータ・AIを活用したサイバー空間基盤技術

安西 祐一郎
独立行政法人日本学術振興会
顧問・学術情報分析センター所長

P.10

フィジカル空間デジタルデータ処理基盤

佐相 秀幸
東京工業大学
特任教授

P.14

IoT社会に対応したサイバー・フィジカル・セキュリティ

後藤 厚宏
情報セキュリティ大学院大学
学長

P.18

スマートバイオ産業・農業基盤技術

小林 憲明
キリンホールディングス株式会社
取締役常務執行役員
バイオ戦略有識者会議構成員

P.2

IoE社会のエネルギーシステム

柏木 孝夫
東京工業大学 特命教授・名誉教授
先進エネルギーソリューション研究センター長

P.38

国家レジリエンス（防災・減災）の強化

堀 宗朗
国立研究開発法人 海洋研究開発機構
付加価値情報創生部門
部門長

P.42

自動運転（システムとサービスの拡張）

葛巻 清吾
トヨタ自動車株式会社
先進技術開発カンパニー Fellow

P.22

統合型材料開発システムによるマテリアル革命

三島 良直
国立研究開発法人
日本医療研究開発機構 理事長
東京工業大学 名誉教授・前学長

P.26

光・量子を活用したSociety 5.0実現化技術

光・量子技術で未来を創造する

西田 直人
株式会社 東芝
特別嘱託

P.30

AI（人工知能）ホスピタルによる高度診断・治療システム

中村 祐輔
公益財団法人がん研究会
がんプレシジョン医療研究センター
所長

P.46

スマート物流サービス

田中 従雅
ヤマト運輸株式会社
執行役員

P.50

革新的深海資源調査技術

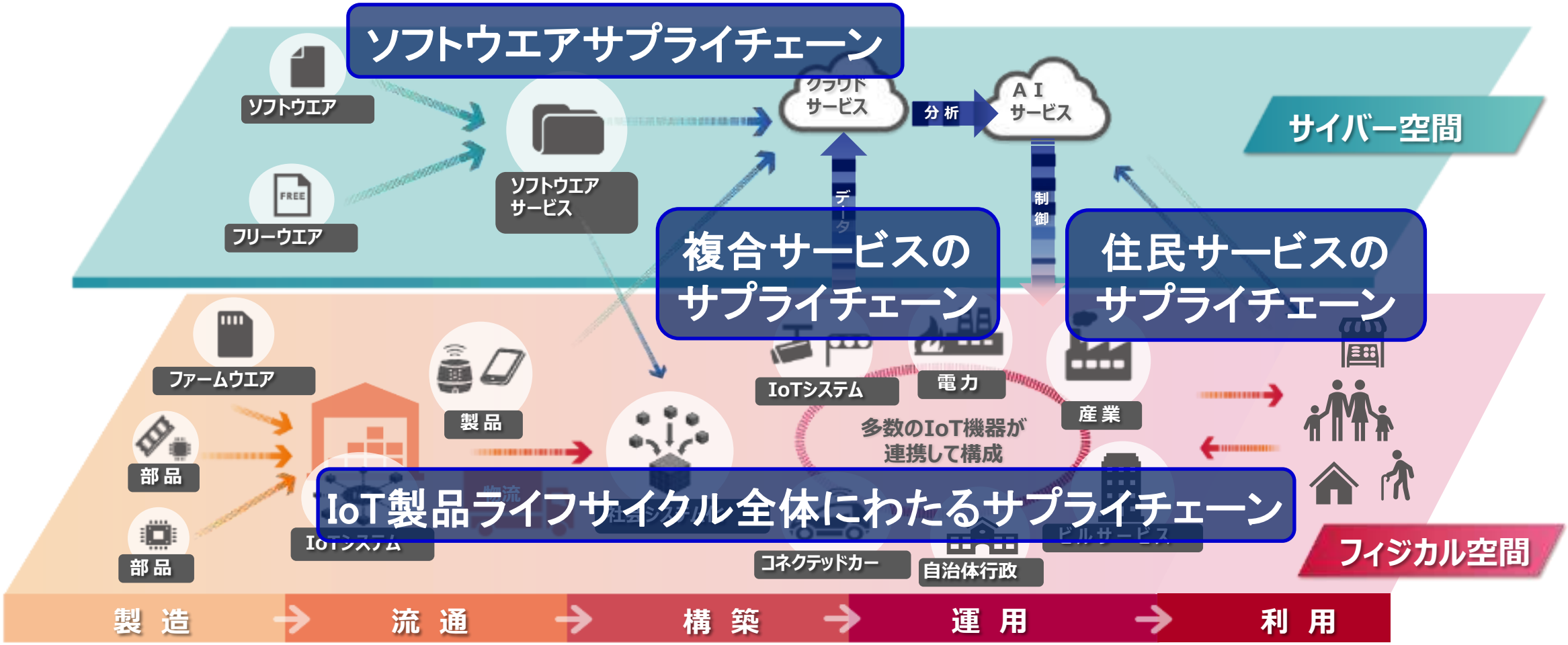
石井 正一
日本CCS調査株式会社 顧問

P.54

『サイバー・フィジカル・セキュリティ対策基盤』の考え方

'Cyber-Physical Security Infrastructure' for IoT, Software and Service Supplychain

サイバー空間とフィジカル空間の双方に跨るIoT社会でのサプライチェーン



研究開発体制（～2022年度）

SIP-CPS R&D Teams

PD　後藤 厚宏
サブPD　（今瀬 真、瓜生 和久）
戦略C　（藤田 恭弘）
内閣府　（事務局）
NEDO　（研究推進法人）

サイバー・フィジカル・セキュリティ推進委員会

ＮＩＳＣ、総務省、経産省、デジタル庁、他
学会、産業界の有識者

社会実装WG　成果普及・実証評価WG　海外動向調査WG

リーダー委員会　知財委員会

A1
信頼の基点
暗号モジュール「SCU」
ECSEC, 産総研 (横国大，神戸大，東大，東北大，NAIST，三菱電機)

A2
IoT機器向けソフトウェアの真贋判定
NTT
NEC
（FFRI）

C2
IoT/OTシステムの異常検知・復旧支援
NTT, NEC
日立, 三菱
（阪大、金沢工大）

B2
多様なデータ流通の信頼確保
富士通
（NII,名大）

B3
サプライチェーン全体の信頼データ交換・共有
日立
KDDI総研
（産総研）

A.信頼の創出・証明

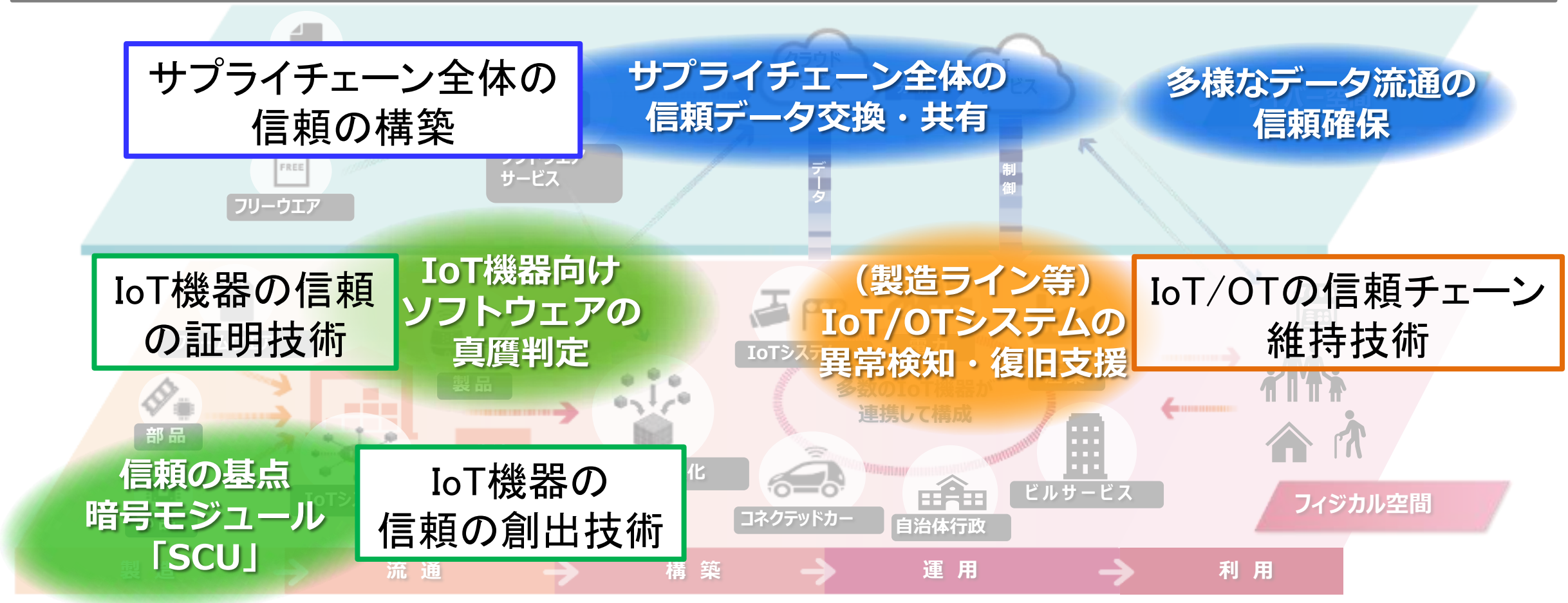
C.信頼チェーンの検証・維持

B.信頼チェーンの構築・流通

『サイバー・フィジカル・セキュリティ対策基盤』の考え方

'Cyber-Physical Security Infrastructure' for IoT, Software and Service Supplychain

IoT機器やサプライチェーンの各構成要素について，セキュリティの確保（信頼の創出）とその確認（信頼の証明）を繰り返し行い，信頼チェーンを構築・信頼のチェーンを維持することで，IoTシステム・サービス及びサプライチェーン全体のセキュリティを確保



IoTサプライチェーンの信頼の創出技術　セキュア暗号ユニット「SCU」

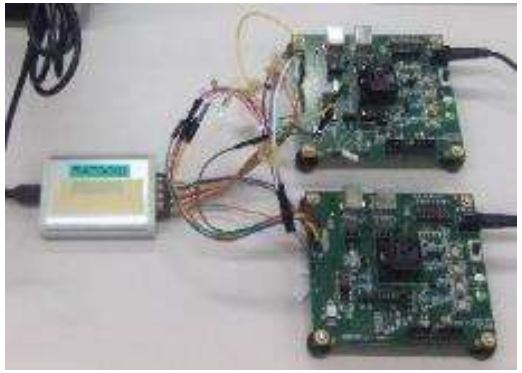
The Secure Cryptographic Unit “SCU” as the “Root of Trust” in the Society5.0 era

サプライチェーン全体でのセキュリティ対策と信頼性確保の「基点」

- 世界最小、最小消費電力のセキュア暗号ユニット（SCU）のLSIチップ開発に成功
- ケーブルコネクターにも搭載可能とし、幅広い実用化に目途

SC02v.2チップ

チップ評価完了



IoT機器等向け真贋判定技術による信頼の証明技術

Authenticity and integrity monitoring technology for IoT device configuration

製造から流通・運用・保守までIoT製品ライフサイクル全体での不正機能の混入「汚染」防止

- サプライチェーン攻撃からIoT製品を守る軽量&リアルタイム性に優れたソフトウェア真贋判定システムを実現
- SBOM対応のソフトウェアサプライチェーン対策で先行

【効果①】
納入時に不正なソフトウェア構成要素を発見できる

【効果②】
本来動作に影響を与えず稼働中に判定できる

判定基準（機器構成の証明情報）はSBOM対応

IoT/OTの信頼チェーンの維持技術

Anomaly Detection and Managed Security Services for Cyber Physical Systems

サプライチェーン上でのIoT/OTシステムの異常検知・復旧支援

- 運用中の設備（製造ライン・制御システム等）を守る異常検知・統合分析システムを実現

効果① 多様な業務環境のリスクを手軽に分析

業務環境上の脆弱性を悪用した攻撃ルートや影響を分析して、リスクと対処策案を提示

リスク診断サービス

リスクシミュレータ

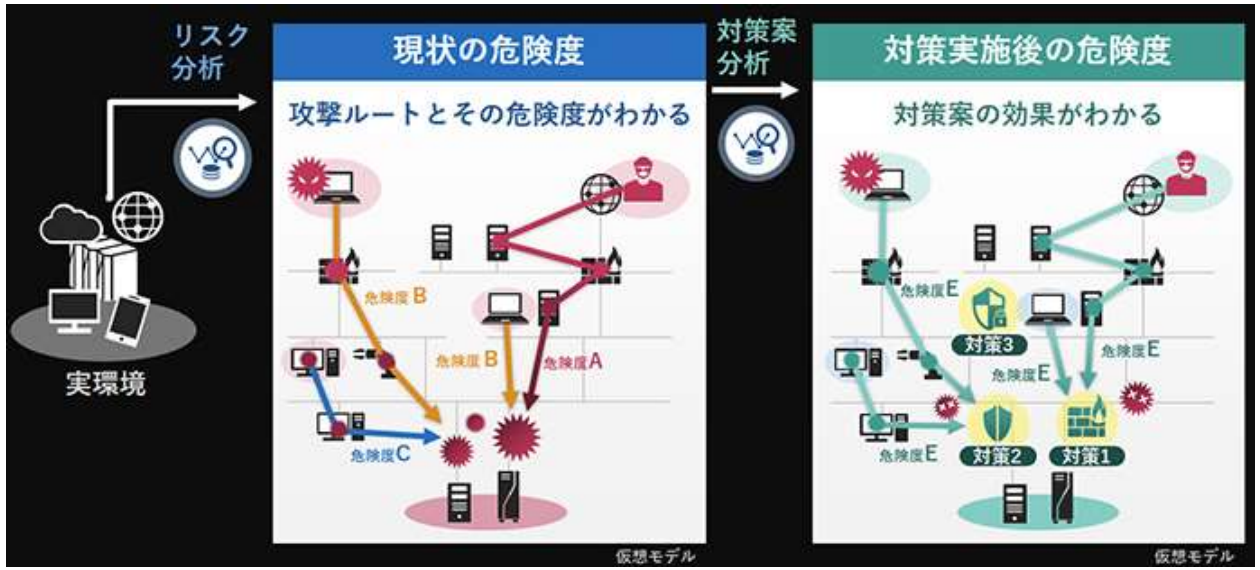
効果② 多様な通信仕様に自動適応・監視・対処

製造ラインのネットワーク内に異常検知のセンサを追加導入
（既存設備にも導入可能）

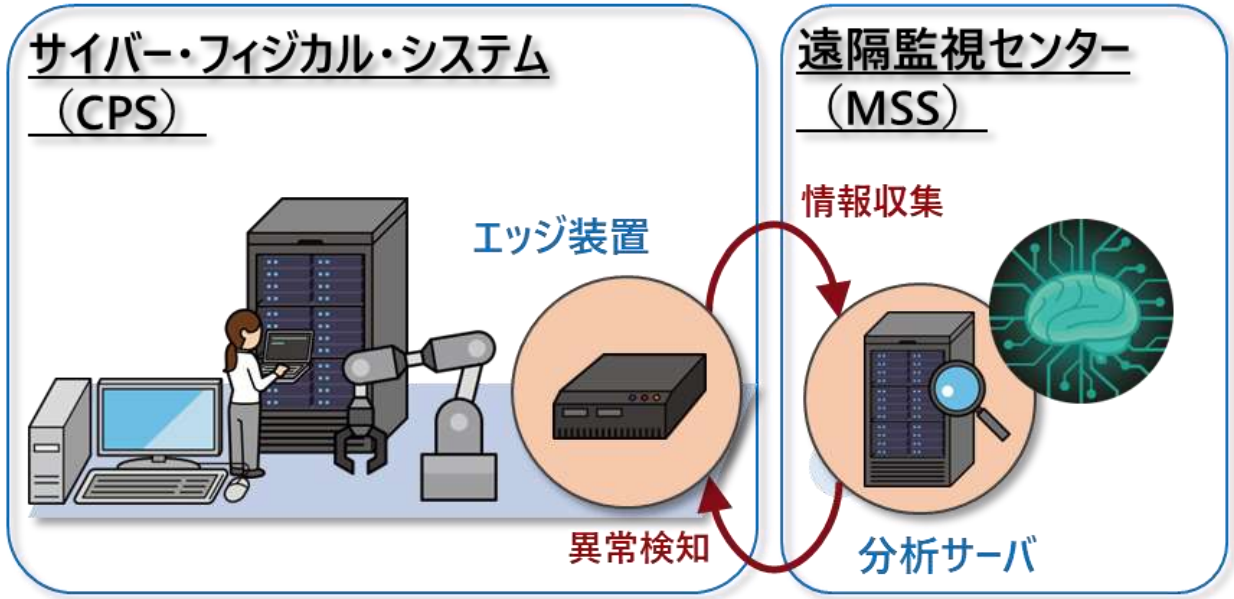
IoT/OTの信頼チェーンの維持技術

Anomaly Detection and Managed Security Services for Cyber Physical Systems

リスク診断サービス



CPSのMSSサービス



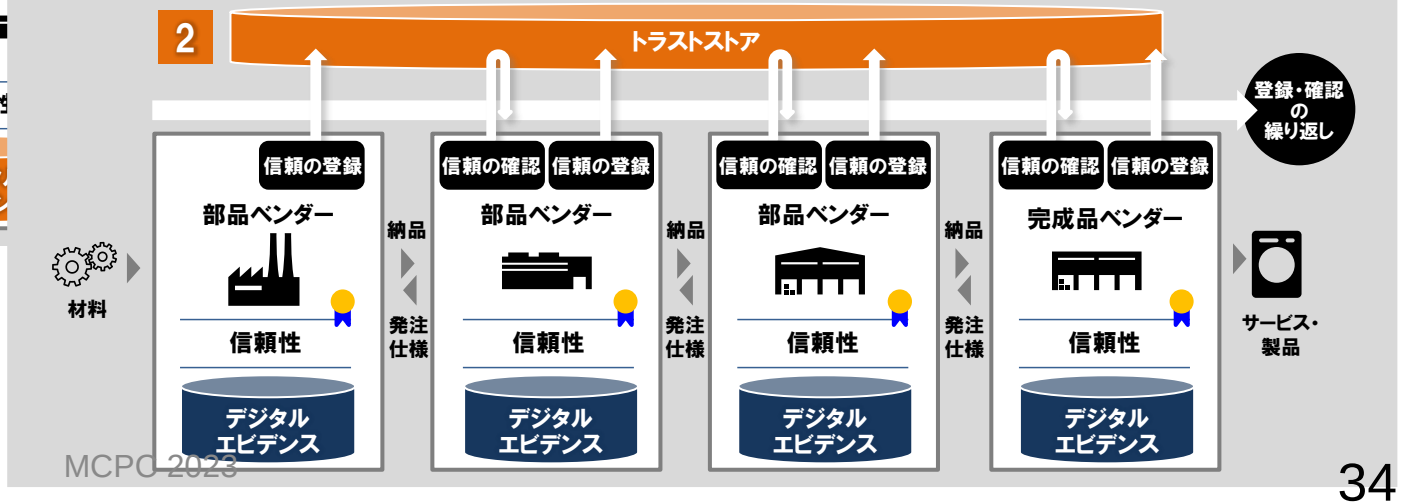
サプライチェーン全体の信頼性確保に向けた信頼データ交換・共有技術
Digital Trust for building Trustworthiness in the Supplychain under Society 5.0

グローバルサプライチェーン全体でのセキュリティ確保

- 複合サービスサプライチェーンの信頼構築フレームワークを実現するVCPモデル、デジタルエビデンス、トラストストアを開発
- 都心の大規模ビルのテナント衛生管理サービスで機能実証に成功

1 『信頼の創出・証明』
- サプライチェーン上の生産活動が規程どおりに行われたかを確認
- デジタルエビデンスに裏付けされた証明可能性による「信頼性」確保

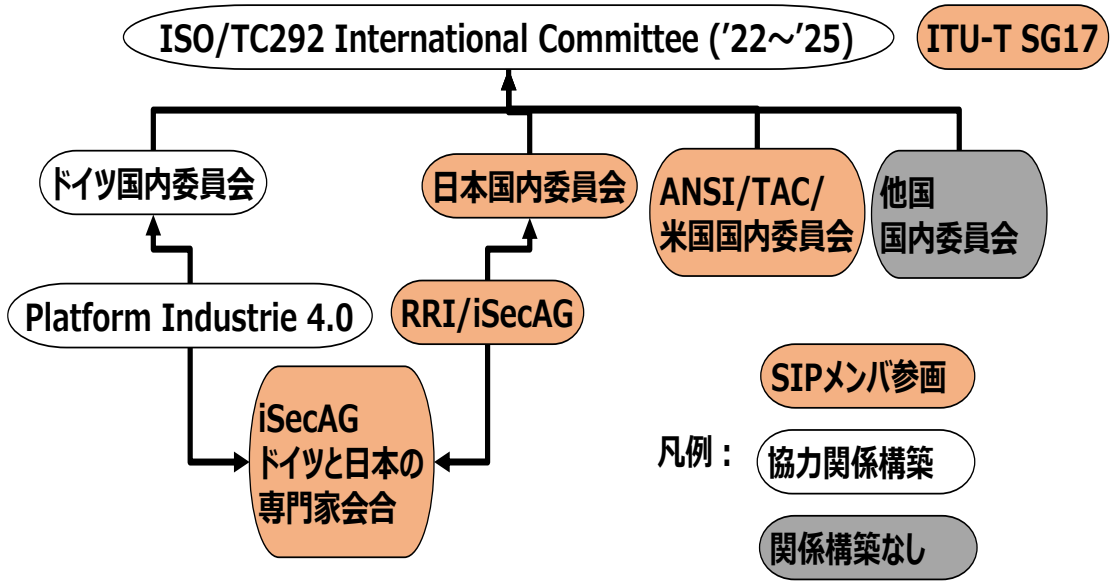
2 『信頼チェーン』
- 各ベンダーの「信頼性」をトラストストアに登録して連鎖
- サプライチェーン全体の「信頼性」を相互に参照して確認



サプライチェーン全体の信頼性確保に向けた信頼データ交換・共有技術
Digital Trust for building Trustworthiness in the Supplychain under Society 5.0

標準化に向けた国際連携

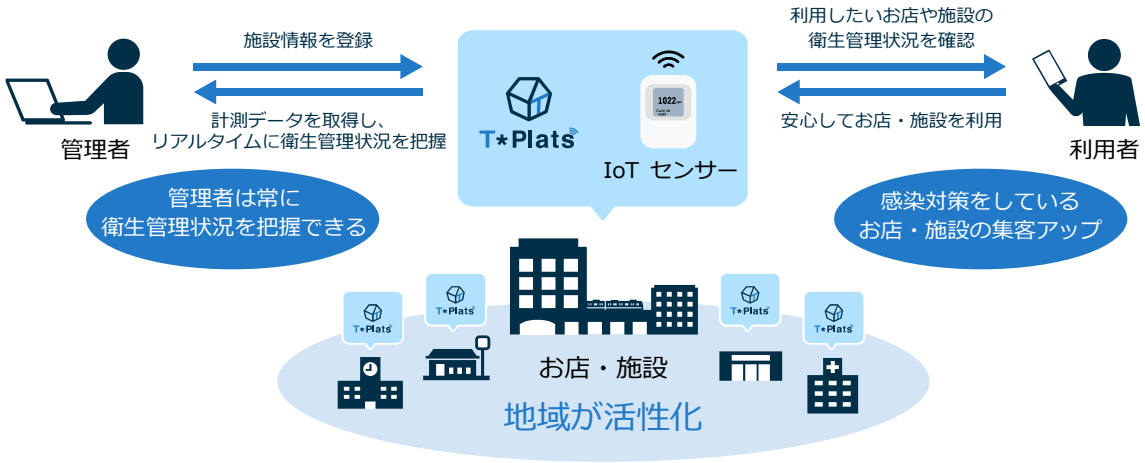
信頼構築フレームワークの標準化に向け、**RRI等を活用した日独米推進体制の構築に成功**し、日本単独提案と比べ、**ISO標準化提案1年前倒しを達成**



標準化に向けた国際連携体制

SIP成果を活用した事業化

・都心の大規模ビルのサプライチェーンで実証に成功
・成果を活用し、2022年8月に㈱日立製作所、イーヒルズ㈱から**衛生管理可視化サービス「T*Plats」をサービスイン**



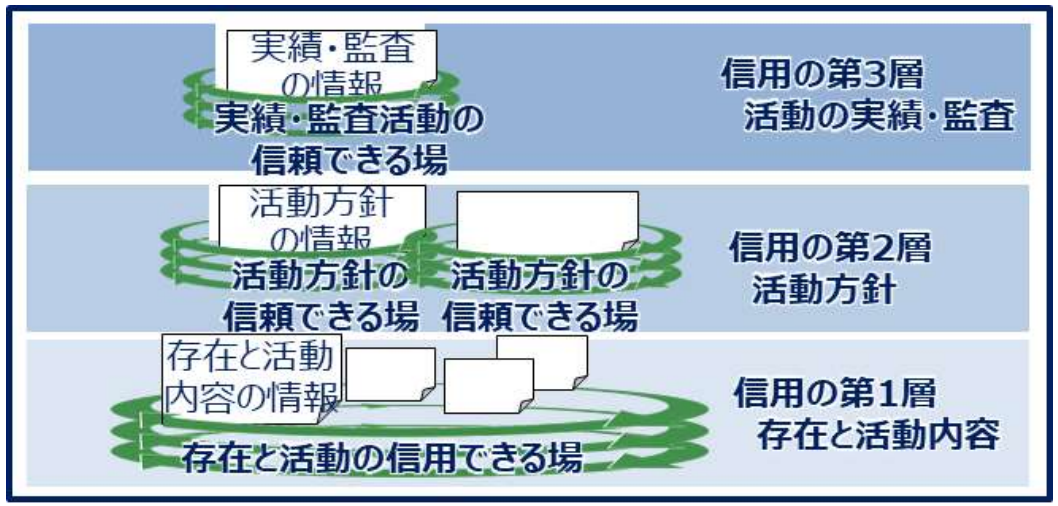
自治体と事業者間を安全につなぐ情報流通技術とその応用

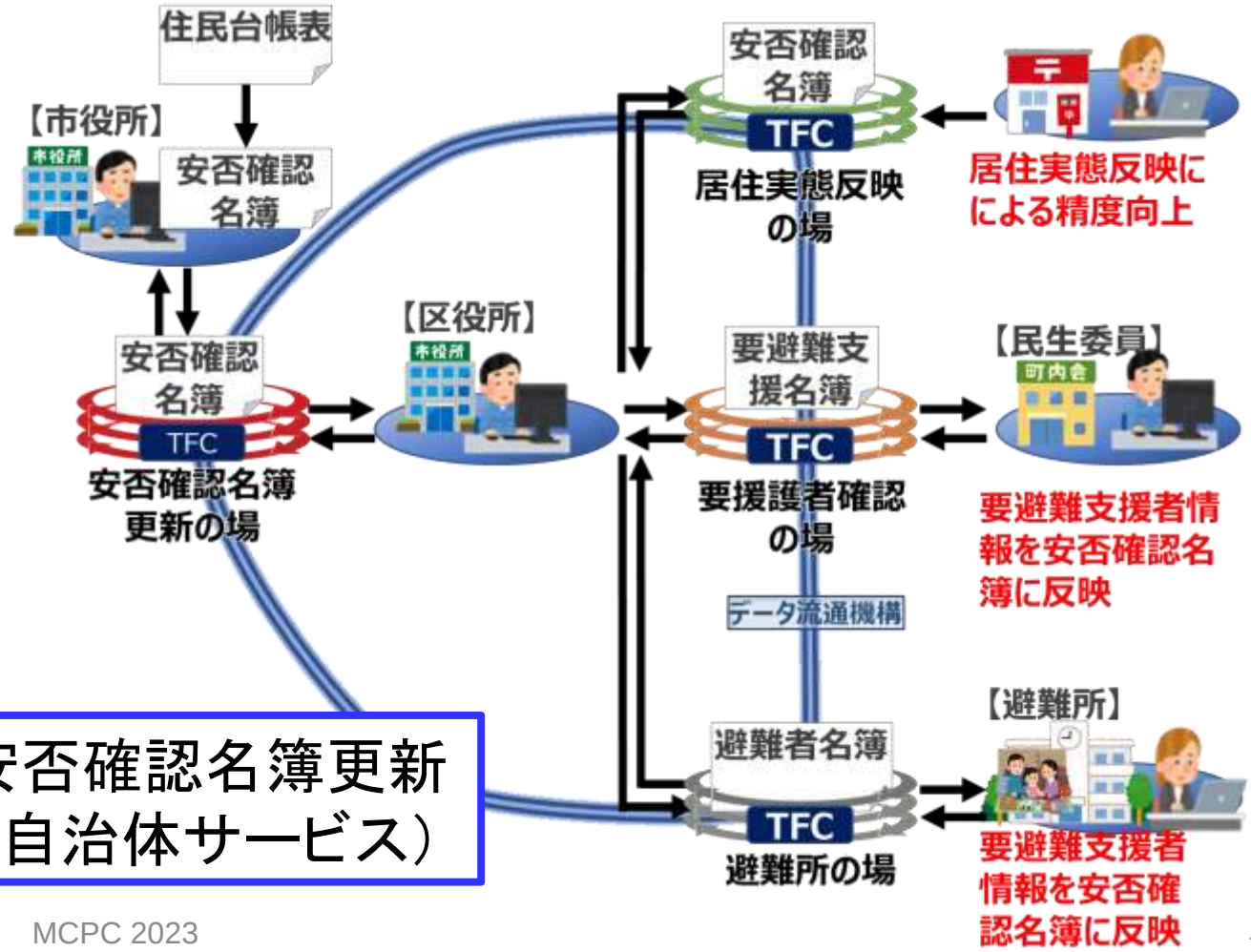
Information Distribution Technology and its Application to Secure Connection between Multi-stakeholders

市民・民間・行政間の多様なデータ流通の信頼確保

- 信用情報流通、合意形成、分散セキュリティ制御を可能とする精選接続技術（TFC）を開発

精選接続技術（TFC）





災害時の安否確認名簿更新への応用（自治体サービス）

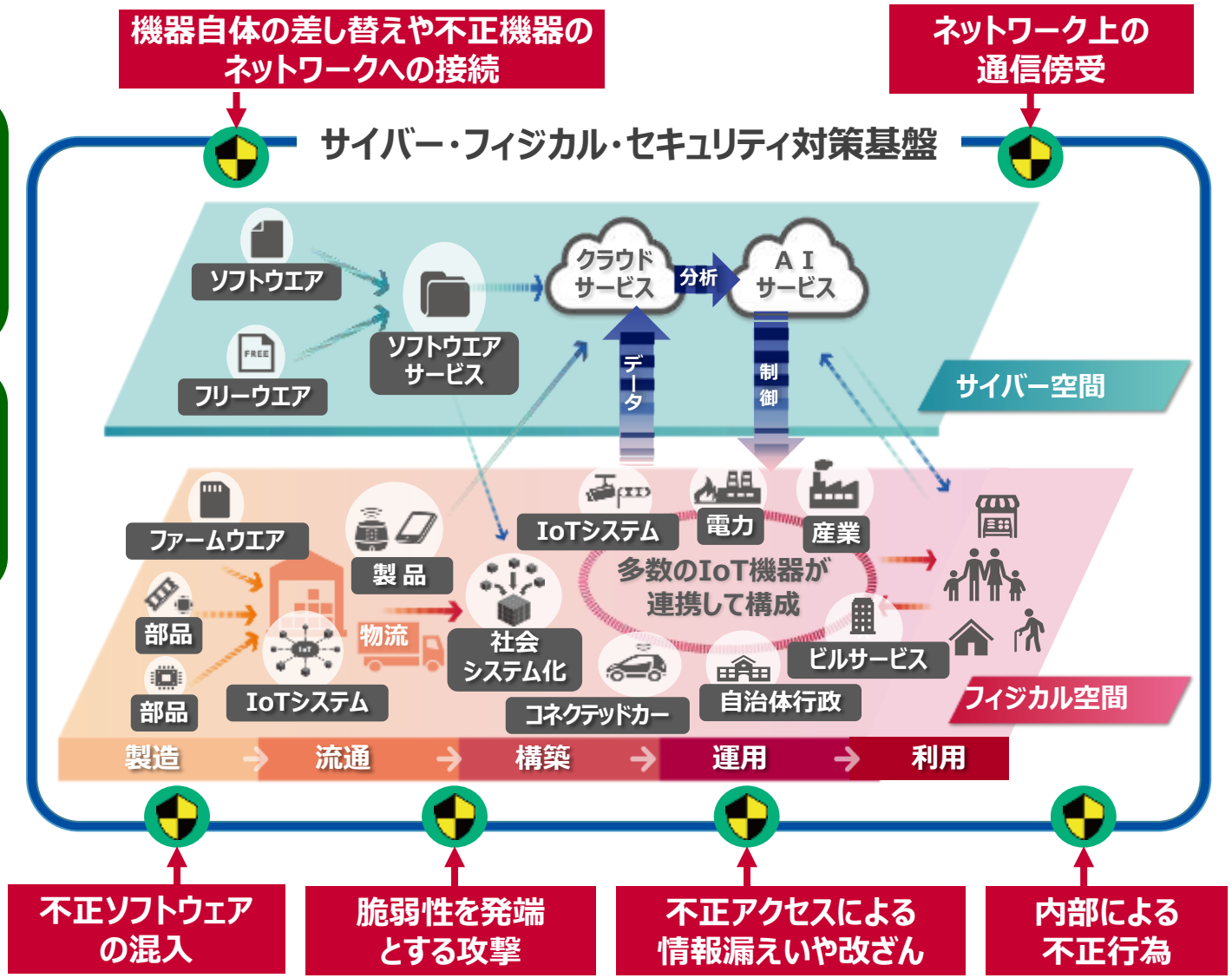
『サイバー・フィジカル・セキュリティ対策基盤』社会実装Ready

Cyber-Physical Security Infrastructure, the First Deployments towards Society5.0

既存機器のインターフェース部に外付け可能な通信暗号化コネクタシステム

IoT機器向けの改ざん検知ソフトウェア（サービス化準備）

IoT/OTシステムにおけるセキュリティ異常対処支援サービス（一部　先行サービス化）



信頼できる取引ネットワーク構築サービス（自治体向け実証）

サプライチェーン・トラスト・ソリューション

「衛生管理可視化」（先行サービス化）

SIP CPSの成果紹介ビデオを技術導入のガイドブック

Cyber-Physical Security Infrastructure, Introductory Video and Guidbook

成果紹介ビデオ

（短版 約8分・長版 約30分 × 日本語・英語）

ガイドブック・技術紹介動画 | 事業 | NEDO
https://www.nedo.go.jp/activities/ZZJP_100235.html

技術導入のガイドブック

関連ドキュメント・ガイドブック・技術紹介動画

内閣府SIPの全体概要

- https://www.youtube.com/@sip9529/videos
- https://www8.cao.go.jp/cstp/gaiyo/sip/

SIP CPSガイドブック・技術紹介動画

- https://www.nedo.go.jp/activities/ZZJP2_100123.html

SIP CPSシンポジウムより

- https://www.youtube.com/watch?v=llgi-K4ZXhs 2023/3 MITRE SoT
- https://www.youtube.com/watch?v=OL_Q3f4pI94 2021/11 SolarWinds事案の分析

SIP CPS調査報告書

- https://www.nedo.go.jp/content/100956037.pdf NIST, ENISAなどの海外動向関連
- https://www.nedo.go.jp/content/100956036.pdf CSIRT, PSIRT関連
- https://www.nedo.go.jp/content/100953488.pdf OSS関連

SIP第2期（2018年度～2022年度）

「IoT社会に対応したサイバー・フィジカル・セキュリティ」

◆ Society5.0への貢献

SIPの開始時（2018年度）の「将来の想定リスク（懸念）」が、今日「現実の問題」として顕在化し、米国やEUにおいて対応策作りが急務になるなか、本SIPにて先行開発してきた成果は「社会実装READY!」であり、必須ツールとして国内外で活用（社会実装）が期待できる。

◆ SIP 成果

Society 5.0 の安全・安心を確立するため，IoTシステムの製造・流通・運用から行政サービス・民間サービスのサプライチェーン全体を守ることができる『サイバー・フィジカル・セキュリティ対策基盤』の開発と実証を行い、2030年までの社会実装の目途をつけることができた。

まとめ

- IoT社会におけるサプライチェーンのセキュリティ課題 ⇒ リスクが顕在化（現実問題に！）
- サプライチェーン「寸断」のリスク ⇒ 社会経済全体のマクロな視点
- サプライチェーンにおけるソフトウェア「汚染」
  ⇒ クリティカルソフトウェアの再点検とOSSの安全性強化
- 内閣府SIP：サイバー・フィジカル・セキュリティへの取組み （SIP第2期　2018～2022年度）
  ⇒先行開発してきた成果が社会実装READY!
- まとめとディスカッション（Q&A）

ご紹介

情報セキュリティ大学院大学（IISEC）

大学基本情報

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

[名称]情報セキュリティ大学院大学

[学長]後藤厚宏

[位置]横浜市神奈川区鶴屋町2-14-1(横浜駅きた西口徒歩1分)

[開学]2004年4月1日

[構成]研究科:情報セキュリティ研究科

専　攻:情報セキュリティ専攻

課　程:博士課程[前期・後期]

学　位:[前期]修士(情報学) Master of Informatics

[後期]博士(情報学)Doctor of Philosophy in Informatics

4つのモデルコースとコースリーダー

倫理観を持って、現実の課題解決を担う高度な専門技術者・実務家、及び、将来方向をリードする創造性豊かな研究者を育成

村上教授

サイバーセキュリティとガバナンスコース

技術系

マネジメント系

有田教授

数理科学とAIコース

総合科学

セキュリティ／リスクマネジメントコース

藤本教授

システムデザインコース

大久保教授

IISECカリキュラムの現在（2023年度）

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

総合学習

- 情報セキュリティ特別講義
- 情報セキュリティ輪講 Ⅰ
- 情報セキュリティ輪講 Ⅱ
- Presentations for Professionals
- クリティカルシンキングとイノベーション＊

サイバーセキュリティとガバナンス

- セキュア法制と情報倫理
- 法学基礎
- 知的財産制度
- セキュリティの法律実務
- 個人識別とプライバシー保護
- サイバーセキュリティ技術論
- ハッキングとマルウェア解析＊

＊特設講義

セキュリティ／リスクマネジメント

- 不確実性下の意思決定
- 統計的方法論
- セキュリティシステム監査
- 国際標準とガイドライン
- 情報セキュリティ心理学
- リスクマネジメントと情報セキュリティ
- セキュリティ経営とガバナンス
- 組織行動と情報セキュリティ
- マスメディアとリスク管理
- データサイエンスとアナリティクス＊

数理科学とAI

- 暗号・認証と社会制度
- 暗号プロトコル
- アルゴリズム基礎
- 数論基礎
- 量子計算と暗号理論
- AIと機械学習
- ブロックチェーン理論＊

システムデザイン

- ネットワーク設計とセキュリティ運用
- 情報デバイス技術
- 情報システム構成論
- オペレーティングシステム
- セキュアプログラミングとセキュアOS
- プログラミング
- ソフトウェア構成論
- 実践的IoTセキュリティ
- セキュアシステム構成論

ハンズオン

- 情報セキュリティ技術演習
- セキュリティ実践 Ⅰ ＆セキュリティ実践 Ⅱ（SecCap演習）
  NWとWebアプリのセキュリティ検査と対策演習、デジタルフォレンジック演習、Capture The Flag（CTF）入門と実践演習、インシデント対応とCSIRT基礎演習

社会人学生の所属組織（2022–2023実績）

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

- 官公庁、自治体：
  - 金融庁／警察庁／警視庁／海上保安庁／外務省／防衛省（含 自衛隊）／法務省／横浜市役所／神奈川県警察／国立印刷局　など
- インフラ系：
  - NTTコム／NTTドコモ／NTT-ME／協和エクシオ／日本コムシス／ミライト・テクノロジーズ／JCOM など
- 金融関係：
  - 日本生命保険／農林中央金庫／三井住友信託銀行／三井住友海上火災／イオン銀行／三井住友銀行　など
- 製造業：
  - ホンダ など
- IT系企業：
  - 日立システムズ／NTTコムウェア／NTTテクノクロス／IQVIAサービスジャパン／ディー・エヌ・エー／さくら情報システム／富士フイルムビジネスイノベーション／プルデンシャル・システムズ など
- セキュリティ企業：
  - NRIセキュアテクノロジーズ／LAC　など
- その他
  - 弁護士　等

セキュリティ人材育成の取組み URL

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

- 情報セキュリティ大学院　https://www.iisec.ac.jp/
- 情報セキュリティ大学院　入学案内
  https://www.iisec.ac.jp/admissions/application/
- 情報セキュリティプロ人材育成短期集中プログラム（ProSec）
  https://www.iisec.ac.jp/admissions/prosec/
  - 「セキュアシステム技術演習（基礎）」コース
  - 「IoTセキュリティ」コース
  - 「CSIRT構築に向けて」コース
  - 「脅威分析コース」