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

サイバー攻撃対処技術の国産化に向けて

情報セキュリティ大学院大学

Institute of Information Security IISEC

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。
- 2011年7月～　情報セキュリティ大学院大学 教授。 2017年4月～2025年3月　学長
  - **約7割が社会人。OB・OGは官公庁・企業で活躍中。**
- 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）
- 2019年2月～2025年6月 日本政府のサイバーセキュリティ戦略本部員
- 2024年度～2028年度　経済安全保障重要技術育成プログラム／**先進的サイバー防御機能・分析能力強化**のプログラムディレクター(PD)を併任
- 2025年9月～　サイバーセキュリティ推進専門家会議

サイバー攻撃の動向と特徴

サイバー攻撃の動向と特徴

国際情勢・地政学的リスク

- 2020年12月　SolarWinds製品の正規のアップデートを通じた、**米国の政府機関**や大手IT企業に対するサイバー攻撃
- 2022年1月～　**ウクライナ**の政府機関、金融機関等に対し、Web サイトの改ざんやDDoS攻撃、破壊型（ワイパー型）マルウエアなどによるサイバー攻撃

サプライチェーン攻撃による被害範囲の拡大

- 2022年3月　自動車部品製造企業がサイバー攻撃を受け、当該部品納入先であるメーカーの国内全14工場が稼働停止
- 2023年7月　港湾ターミナルシステムがサイバー攻撃を受け、貨物の積卸作業が2日半にわたり停止　37隻の貨物船と約2万コンテナの搬入出に影響

金銭目的（ランサムウェア）の急拡大

- 2021年5月　米国**石油**パイプライン企業　米国東海岸の45%の燃料輸送を担うコロニアルパイプラインに対するランサムウエア攻撃、5日間の操業停止により当該地域の石油製品がひっ迫
- 2018年～　日本の複数の**医療**機関、**食品・流通**産業に対するランサムウエア攻撃

サイバー対処能力強化に求められる

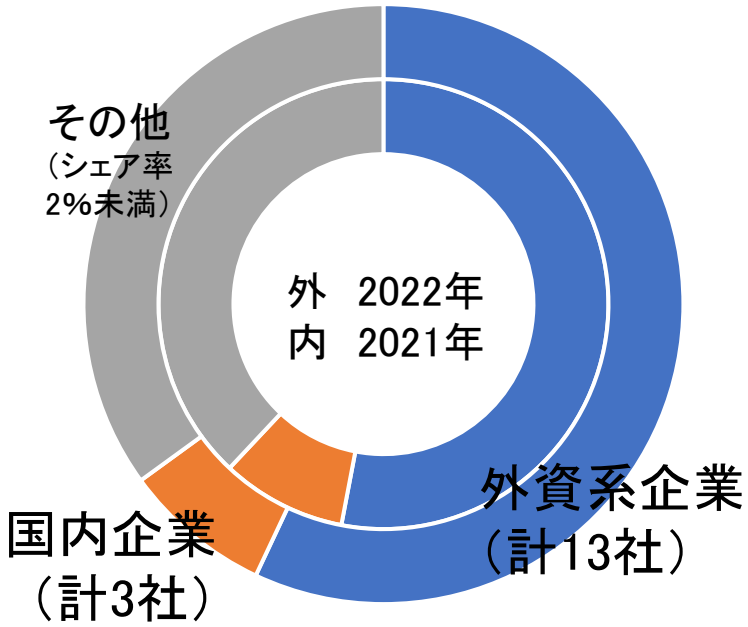
対処技術の国産化の必要性

サイバーセキュリティ対策：現状は海外依存

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

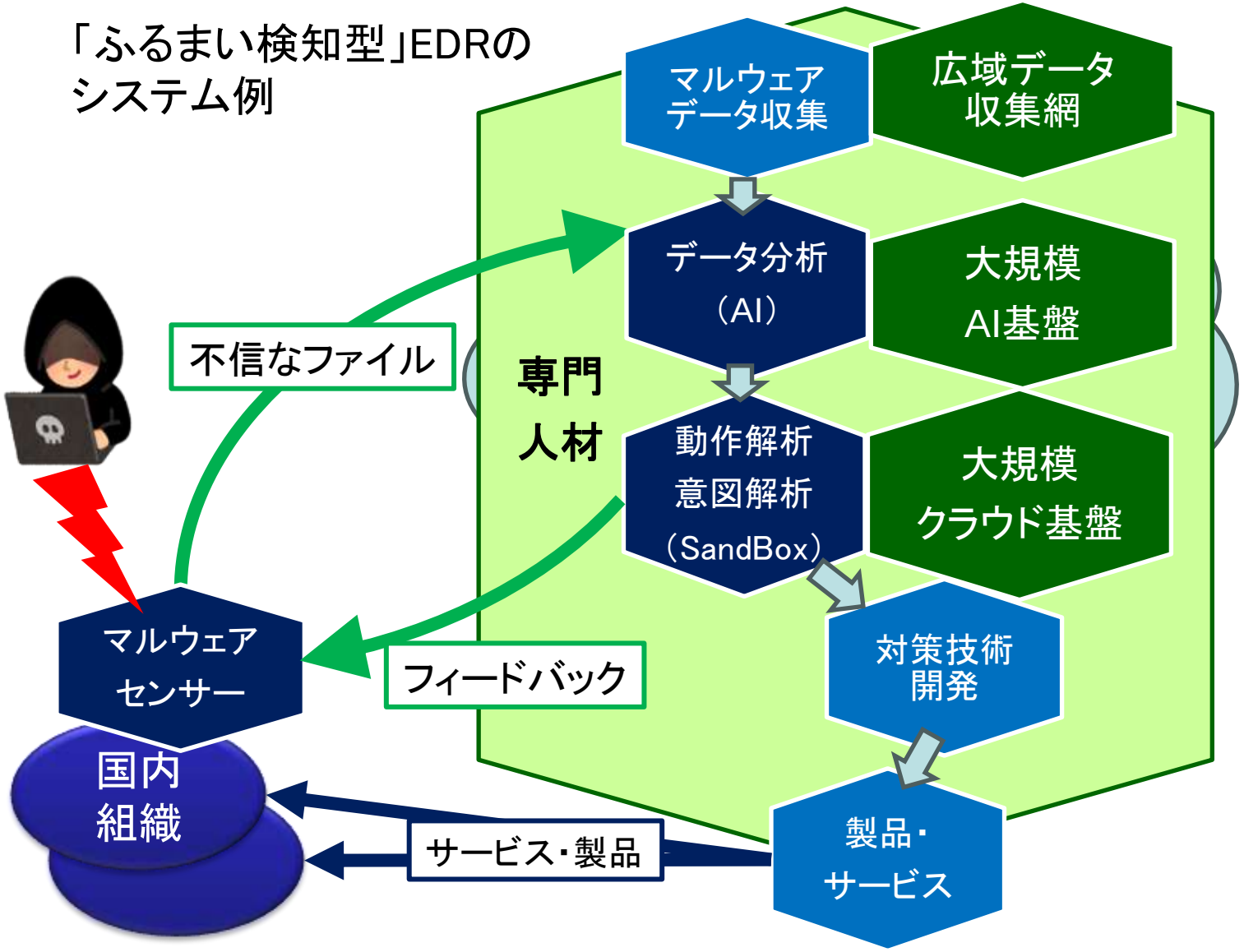
「データ負けのスパイラルからの脱却が必須！」（総務省・NICT）

国内情報セキュリティ製品市場シェア
（売上額）



令和6年版 情報通信白書

「ふるまい検知型」EDRの
システム例



サイバー攻撃対処技術の国産化に向けて

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

新たな「サイバーセキュリティ戦略」（案）における施策の方向性

1.深刻化するサイバー脅威に対する防御・抑止

2.幅広い主体による社会全体のサイバーセキュリティ及びレジリエンスの向上

3.我が国のサイバー対応能力を支える人材・技術に係るエコシステム形成

本講演の着目点

対処技術の国産化の取組（Kプロ）

重要インフラ等の横断的な対策と官民連携

耐量子計算機暗号（PQC）への移行

重要インフラ等の横断的な対策と官民連携

重要インフラ等のサイバー攻撃

ウクライナの
地下鉄（IT系）
（2017）

ウクライナ
（2015～現在）

常時攻撃
対象

重要インフラ（15分野）

ウクライナ：
ワイパー型
（2022）

情報通信

金融

航空

鉄道

電力

米国
SolarWinds
事案（2020）

ガス

医療

水道

クレジット

政府・行政サービス

医療機関へのラン
サムウェア攻撃

常時攻撃
対象

石油

物流

化学

空港

港湾

米国パイプライン
（IT系）

名古屋港
コンテナ

2018年度より追加

2024年度より追加

重要インフラ等の横断的な対策と官民連携

重要インフラへのサイバー攻撃がグローバルに増加・深刻化

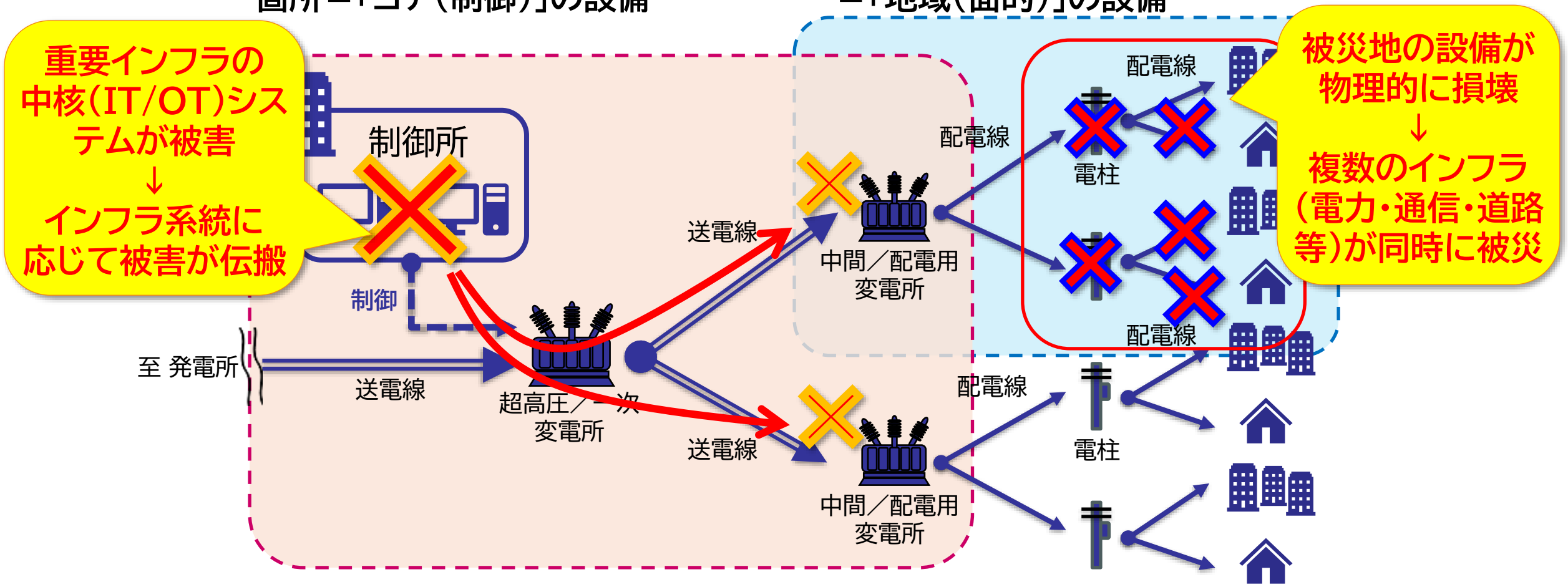
- 官民連携の強化（サイバー対処能力強化法　2025年5月23日公布）
  - 重要設備の導入・維持管理等に係る対策（⇒c.f. 経済安全保障推進法）とインシデント報告義務
  - 情報共有・対策の協議会（事業者間での密な情報連携）
  - 脆弱性対応の強化（⇒c.f. サイバーセキュリティ基本法）
- 重要インフラに関わる中小企業を含むサプライチェーンのセキュリティ強化

自然災害とサイバー攻撃の被害特性の違い

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

サイバー攻撃で被害が想定される箇所＝「コア（制御）」の設備

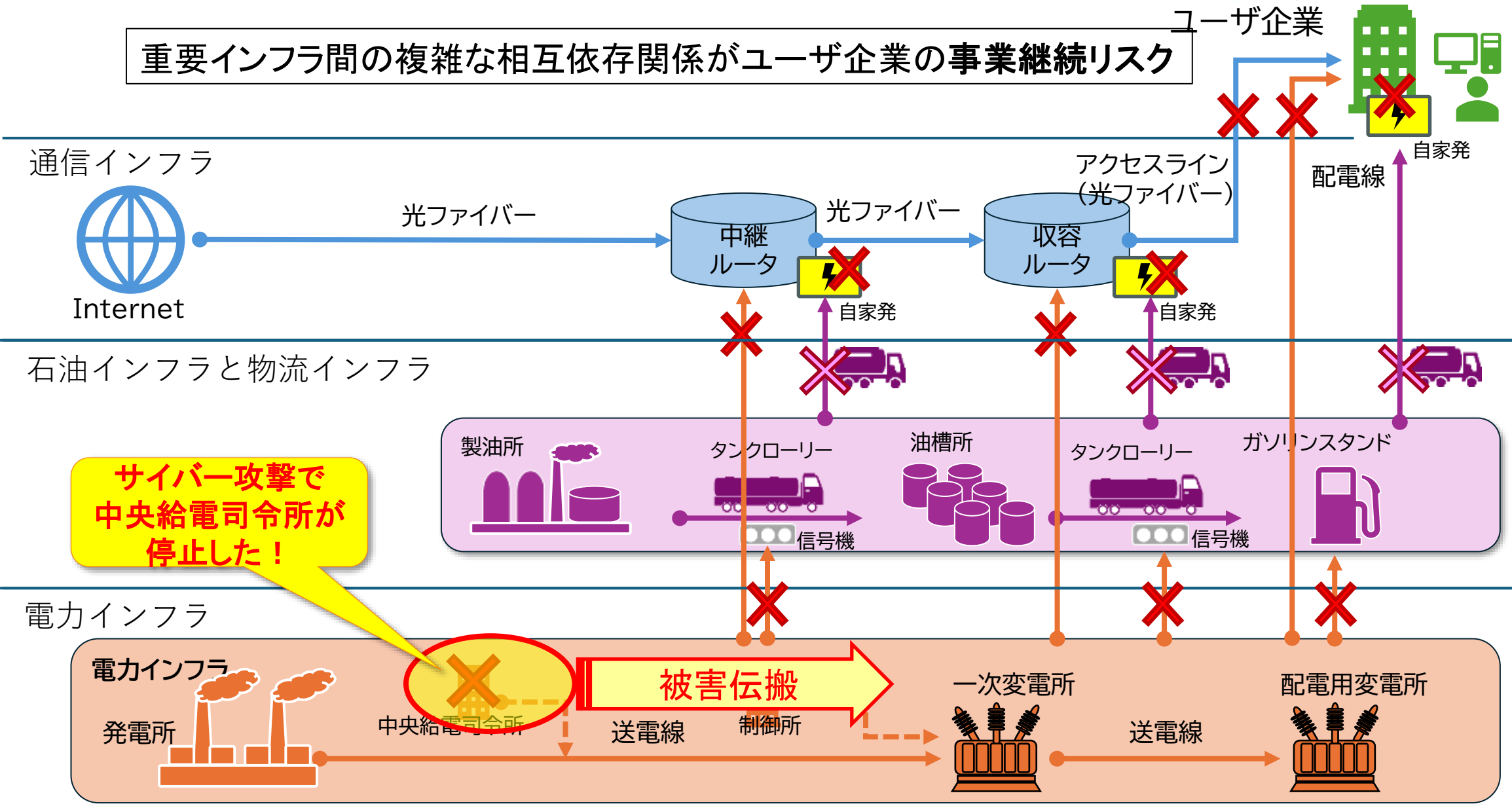
自然災害で被害が想定される箇所＝「地域（面的）」の設備



重要インフラ間の相互依存関係

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

重要インフラ間の複雑な相互依存関係がユーザ企業の**事業継続リスク**



重要インフラ等の横断的な対策と官民連携

重要インフラへのサイバー攻撃がグローバルに増加・深刻化

- 官民連携の強化（サイバー対処能力強化法　2025年5月23日公布）
  - 重要設備の導入・維持管理等に係る対策（⇒c.f. 経済安全保障推進法）とインシデント報告義務
  - 情報共有・対策の協議会（事業者間での密な情報連携）
  - 脆弱性対応の強化（⇒c.f. サイバーセキュリティ基本法）
- 重要インフラに関わる中小企業を含むサプライチェーンのセキュリティ強化

重要インフラのコア設備が狙われ、システム系統に沿って被害が波及

- 自然災害対策との差異 ⇒災害対策関連の法制度や企業組織のBCPの再点検が必要

サイバー攻撃被害の影響が複数の重要インフラ間にまたがって拡大

- 重要インフラ間相互依存関係を考慮したBCPがインフラ事業者と利用組織の双方で必要　（⇒サイバー版のハザードマップ整備）

耐量子計算機暗号（PQC）への移行

暗号 v.s. 高性能コンピュータ

エニグマ暗号機（レプリカ）

Enigma v.s. アラン・チューリング他

- 第二次世界大戦

無線LANセキュリティ v.s. WEP解読

- 無線LANセキュリティの強化（⇒ WPA2 ⇒ WPA3 ）

RSA暗号 v.s. 量子計算機による解読 （2035年？）

- RSA暗号は、現代社会の基盤（ユーザ認証、サービス認証、ICカード、インターネットのプロトコル、デジタル証明書・・・・）
- **課題1**：RSA暗号の後継として、**量子計算機でも解読困難な暗号**（**PQC**：Post-Quantum Cryptography）の研究開発（Kプロ等）と国内外での標準化（NIST等）
- **課題2**：社会全体いたるところで利用されている**RSA暗号をPQC暗号へ移行（社会実装）**

耐量子計算機暗号（PQC）の社会実装

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

◆ 多種多様なシステム、機器で利用されているRSA暗号等をPQCへの移行が必要に！

2025年　**2035年**　2045年

暗号システムを順次PQCへ移行
既存暗号も利用継続が必須

既存暗号を解読できる量子計算機の実現可能時期

機密情報 ― 機密情報の保護期間（20年間） → **公開情報**

攻撃者は既存暗号で暗号化された機密データを収集

Harvest now
Decrypt Later攻撃

既存暗号で暗号化された機密情報を復号

グローバル・インターネットのプロトコル実装を混乱なく置きかえられるか？

重要インフラの既存設備の暗号移行が可能か？　設備更新が間に合うか？

ICカード、組込み機器の暗号移行が可能か？　利用者の協力は？

PQCの社会実装（移行）に関わる課題

証明書 ― パスポートの有効期間（10年間） → **証明書の更新**

耐量子計算機暗号（PQC）の社会実装

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

➢ 社会全体でのPQC移行（社会実装）のための中長期的なロードマップ作り、政府の司令塔役から分野毎の実施主体まで、役割分担の明確化、早期に社会全体に取り組む必要。

ソフトウェア実装

- 暗号の実装技術は安全保障の鍵！
- ➢ 国産PQC暗号開発に加え**国産暗号ライブラリ開発**
- ➢ 国産暗号ライブラリを世界に展開する取組み

企業・国のシステムへの実装

- 社会サービスが安定するまで時間と費用*1がかかる懸念
- ➢ クリプトインベントリ*2と**移行計画作り**が急務
- ➢ PQC移行の**ノウハウ共有の場**つくり（産官学）

グローバル連携

- 情報通信や金融システムはグローバル
- ➢ **社会実装の国際協調**（暗号実装の相互検証センター）

*1 米国連邦政府の移行費用見積り額（10年間）は$7.1 Billion = 約1兆円

先端的な重要技術の開発支援に関する制度経済安全保障
重要技術育成プログラム（Kプロ）

先進的サイバー防御機能・分析能力強化

経済安全保障重要技術育成プログラム（Kプロ）

https://www8.cao.go.jp/cstp/anzen_anshin/kprogram.html

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

◆ 経済安全保障推進会議及び統合イノベーション戦略推進会議の下、内閣府、文部科学省及び経済産業省が中心となって、府省横断的に、経済安全保障上重要な先端技術の研究開発を推進

◆ 有識者等で構成されるプログラム会議における検討を経たうえで国のニーズ（研究開発ビジョン）を上記二つの閣僚級会議で決定し、これを実現するための研究開発を公募により推進

◆ 研究成果を社会実装に繋げていくため、研究実施段階において経済安全保障推進法に基づく協議会等による伴走支援を実施

- 海洋領域
- 宇宙・航空領域
- バイオ領域
- 量子・AI等の新興技術・最先端技術

サイバー領域

- 先進的サイバー防御機能・分析能力強化
- 人工知能（AI）が浸透するデータ駆動型の経済社会に必要なAIセキュリティ技術の確立
- サプライチェーンセキュリティに関する不正機能検証技術の確立（ファームウェア・ソフトウェア）
- セキュアなデータ流通を支える暗号関連技術（高機能暗号）
- 偽情報分析に係る技術の開発　など

Kプロ「先進的サイバー防御機能・分析能力強化」

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

①サイバー空間の情報を収集・調査する状況把握力

- マルウェア（特にランサムウェア）の特徴・暗号化機能の分析技術
- 攻撃主体の狙いや攻撃手段に関する情報の獲得・分析技術
- 高度かつ未知の攻撃の早期発見技術

②サイバー攻撃から機器やシステムを守る防御力

- 機器やシステムの脆弱性探査技術
- 同　防御能力の評価（ペネトレーションテスト含む）・向上技術
- 耐量子計算機暗号（PQC）技術と社会システム全体の移行技術
- 耐タンパー性向上技術

③情報共有基盤と組織・人材の強靭化

- サイバー脅威情報の収集・集約
- サイバー人材の評価・管理による力量の底上げ

①②③　サイバーリサーチコンソーシアムCRC
（Cyber Research Consortium）
2024年7月～2029年6月（予定）
https://www.cyberresearch.or.jp/

④セキュアな量子情報通信技術

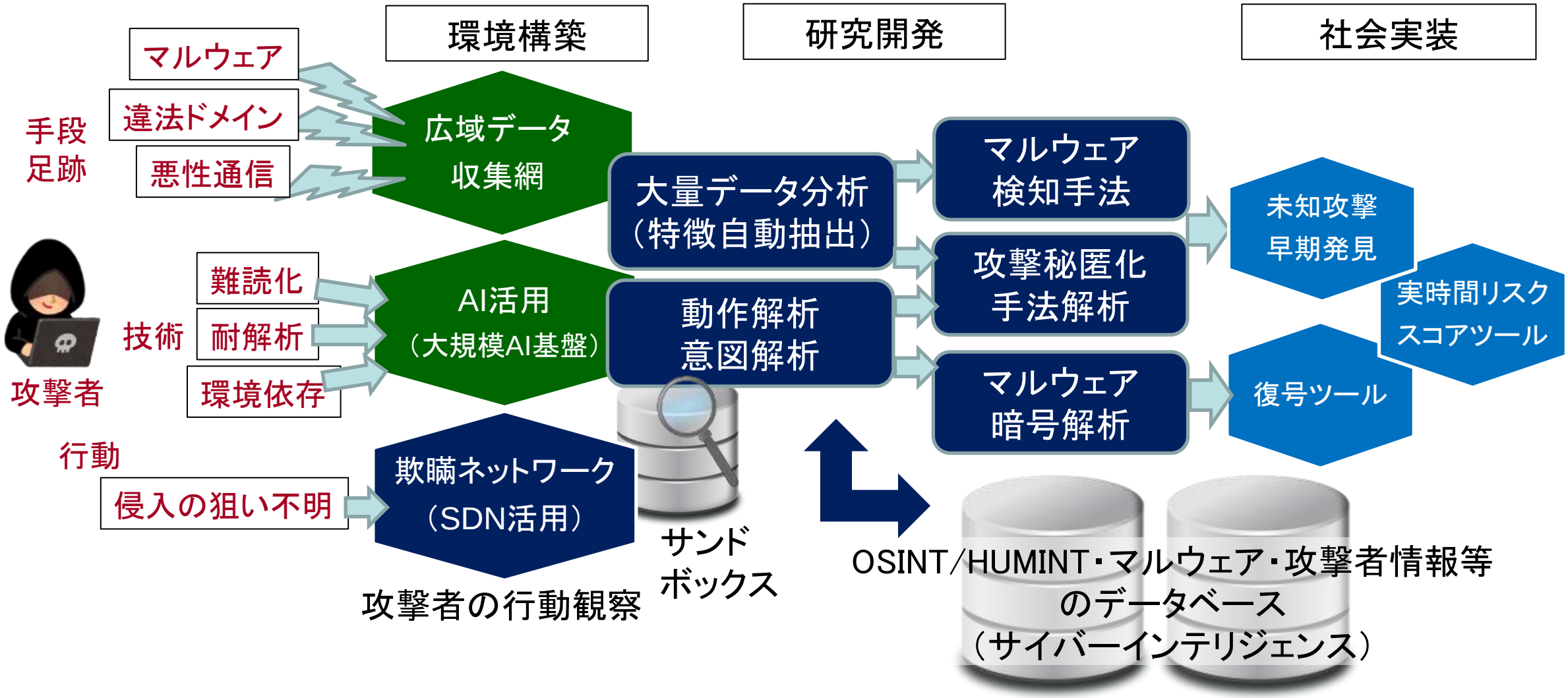
- 量子雑音ストリーミング暗号（QNSC/Y-00）による物理レイヤーのセキュリティ強化
- 光ファイバー伝送路における長距離・高速化（目標：1000km、20～100Gbps）
- 光ワイヤレス通信による適用領域拡大

④日立製作所中心のコンソーシアム
2024年7月～2027年6月（予定）

①サイバー空間の情報を収集・調査する状況把握力

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

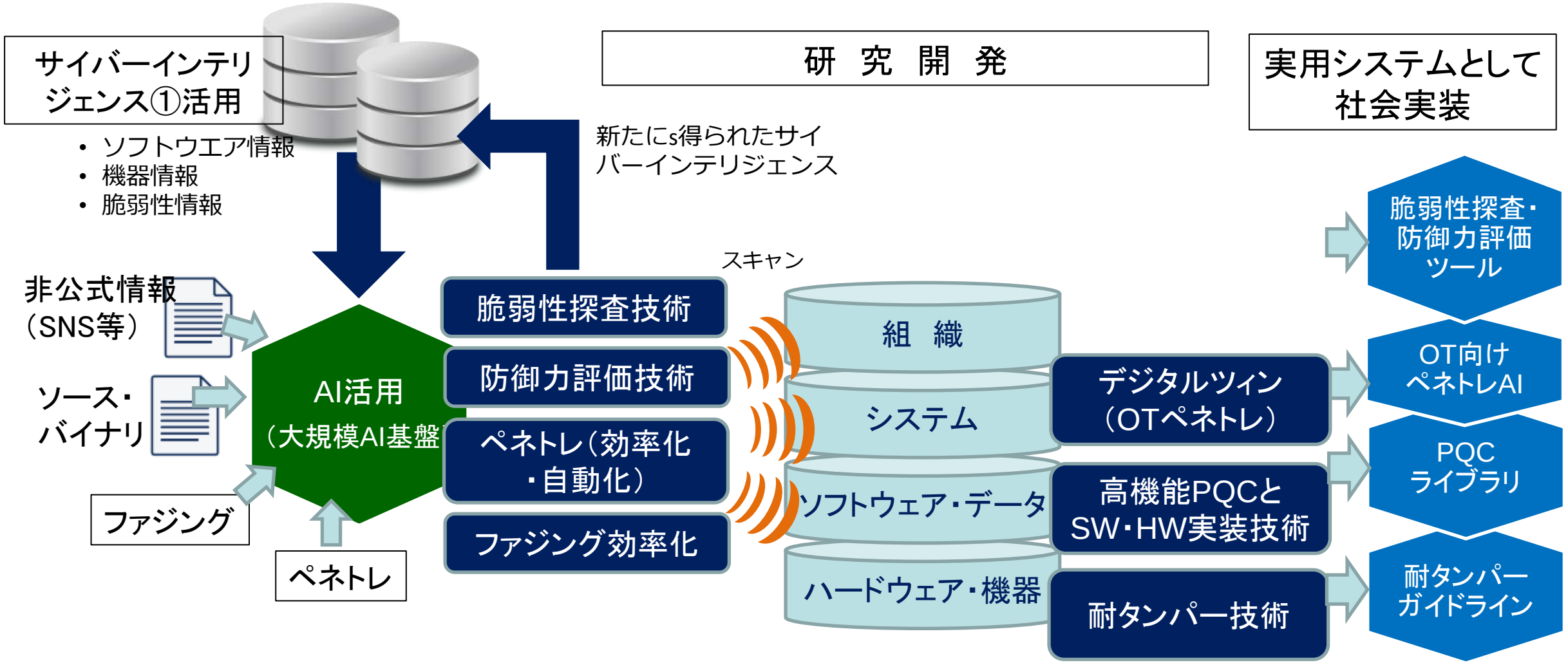
状況把握力の向上に資する、マルウェアの特徴を自動抽出する技術やアルゴリズム分析を効率的に行う技術、未知の攻撃の検知技術や攻撃者の意図を分析するために必要となる情報収集・解析技術の実現



②サイバー攻撃から機器やシステムを守る防御力

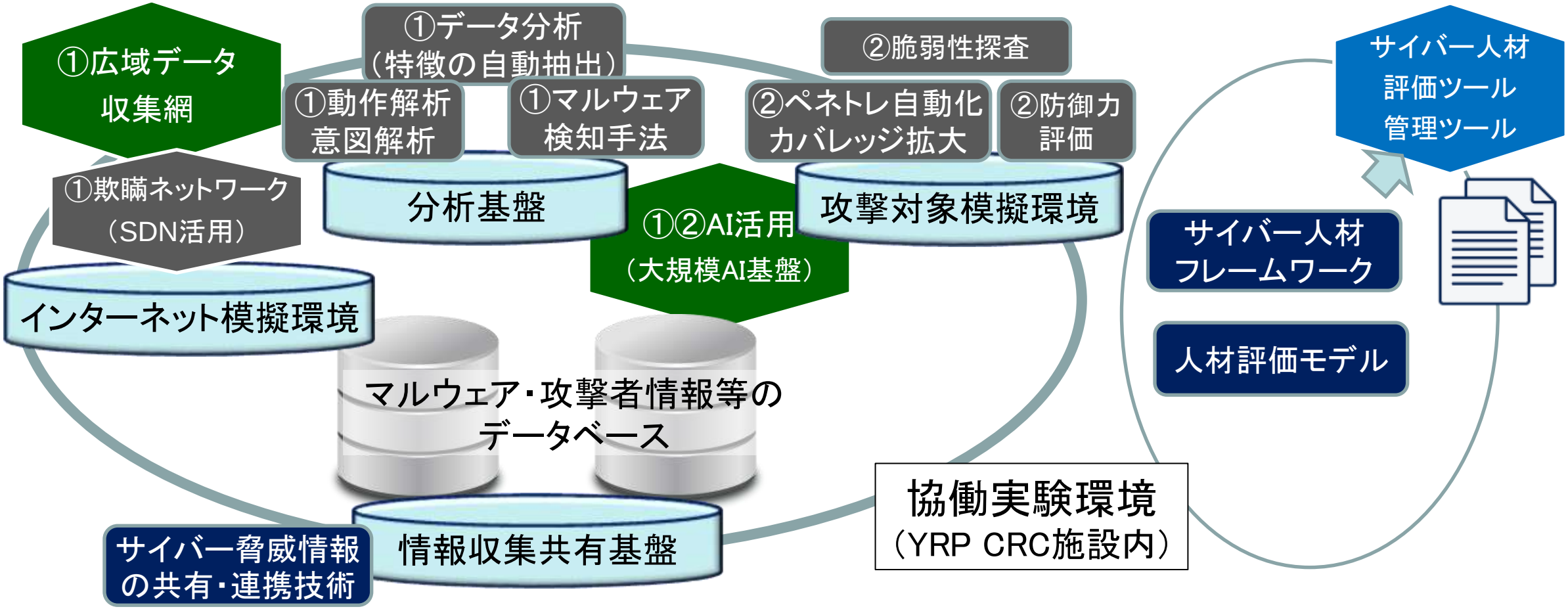
明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

AIを活用した効率的な脆弱性探査技術、ペネトレーションテストの自動化技術、社会インフラシステムを対象としたペネトレーションシステムのフレームワーク、量子計算機による解析に耐え得る暗号化技術の実現



③情報共有基盤と組織・人材の強靭化

効果的なサイバー脅威情報の共有・連携を可能とする技術とともに、高度サイバー人材を評価するための新たな評価軸の確立や、高度かつ最新のスキルを持ったサイバー人材を擁する体制を維持管理していくための手法や体制のあり方の確立



Kプロ「先進的サイバー防御機能・分析能力強化」

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

①サイバー空間の情報を収集・調査する状況把握力

- マルウェア（特にランサムウェア）の特徴・暗号化機能の分析技術
- 攻撃主体の狙いや攻撃手段に関する情報の獲得・分析技術
- 高度かつ未知の攻撃の早期発見技術

②サイバー攻撃から機器やシステムを守る防御力

- 機器やシステムの脆弱性探査技術
- 同　防御能力の評価（ペネトレーションテスト含む）・向上技術
- 耐量子計算機暗号（PQC）技術と社会システム全体の移行技術
- 耐タンパー性向上技術

③情報共有基盤と組織・人材の強靭化

- サイバー脅威情報の収集・集約
- サイバー人材の評価・管理による力量の底上げ

①②③　サイバーリサーチコンソーシアムCRC
（Cyber Research Consortium）
2024年7月～2029年6月（予定）
https://www.cyberresearch.or.jp/

④セキュアな量子情報通信技術

- 量子雑音ストリーミング暗号（QNSC/Y-00）による物理レイヤーのセキュリティ強化
- 光ファイバー伝送路における長距離・高速化（目標：1000km、20～100Gbps）
- 光ワイヤレス通信による適用領域拡大

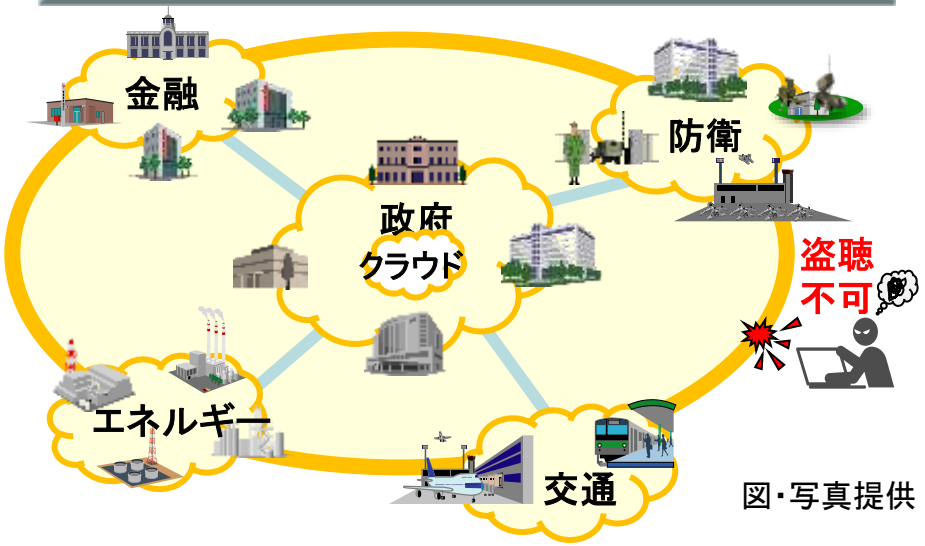
④日立製作所中心のコンソーシアム
2024年7月～2027年6月（予定）

④セキュアな量子情報通信技術

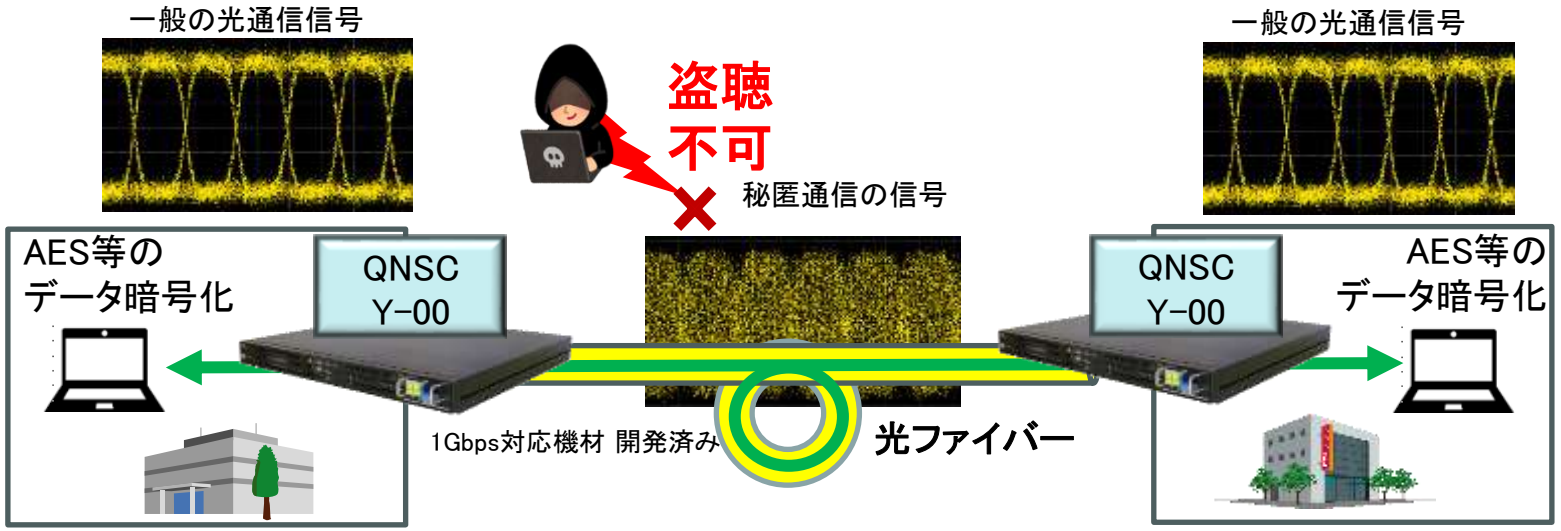
明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

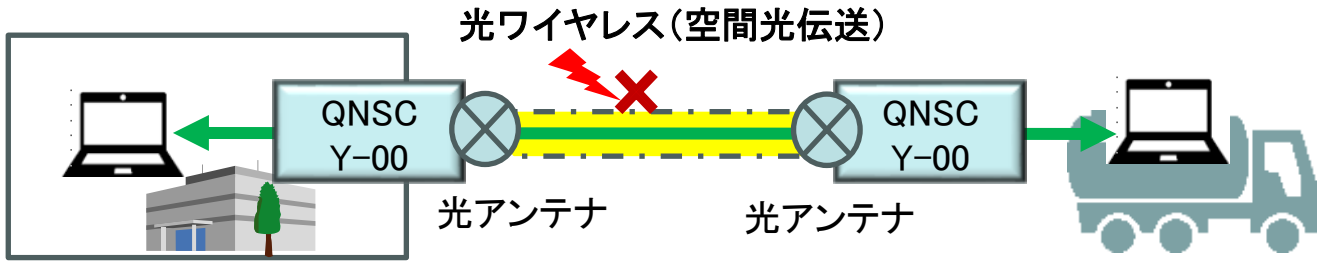
通信路（光ファイバ、無線等）を物理秘匿処理で「盗聴」から守る

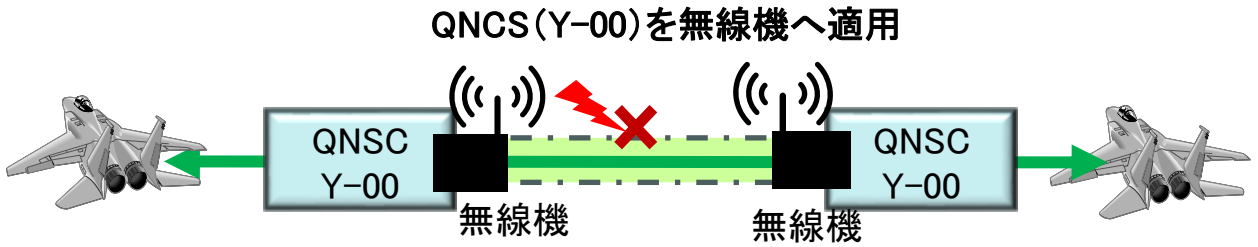
- QNSC/Y-00: 量子雑音を活用した秘匿通信プロトコル
- 海底光ケーブル、無線などの通信路への直接攻撃（盗聴）から重要通信を守る
- 光空間伝送、無線伝送も可能
- 現在（AES等）・将来（PQC等）のデータ暗号化と併用可能。



図・写真提供　日立製作所







サイバー攻撃対処能力の国産化

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

内閣府 経済安全保障重要技術育成プログラム（通称Kプロ）

- 「先進的サイバー防御機能・分析能力強化」の取り組み
  ①②③ 2024年7月～2029年6月（予定）　④ 2024年7月～2027年6月（予定）
  その他 「不正機能検出」、「高機能暗号」、「AIセキュリティ」などの取り組みもあり

国産技術開発・ベンチャー産業振興

- 政府機関等・重要インフラにおける国産セキュリティ技術（Kプロ 成果等）の活用
- 国産主体でデータ収集・分析から技術開発をカバーするエコシステム構築
- ベンチャーが開発する先進技術を政府自ら活用して産業育成

「（AI・クラウド）基盤システム」全体の国産化と人材育成

- 広域データ収集ネットワーク、国産のAI基盤とクラウド基盤との一体開発
- AI活用、クラウド活用含む広義のサイバーセキュリティ人材育成

Key Takeaways　サイバー攻撃対処技術の国産化に向けて

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

新たなサイバーセキュリティ戦略（2025年12月に向けて）	• 戦略（案）へのコメント：国が積極的な役割を果たすことで厳しさを増すサイバー空間情勢に対応
重要インフラ等の横断的な対策の必要性	• サイバーを含む災害対策関連の法制度 • 自組織に必須な重要インフラ間相互依存関係
耐量子計算機暗号（PQC）の社会実装課題	• 自組織の「クリプトインベントリ」 • PQC移行の中長期計画
サイバー攻撃対処能力の国産化の取り組み（Kプロ）	• サイバー攻撃対処能力向上に向けた産官学協働の重要性

情報セキュリティ大学院大学　https://www.iisec.ac.jp
後藤　厚宏　goto@iisec.ac.jp