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

DX時代の価値創造を支える
IoTサプライチェーンセキュリティ

情報セキュリティ大学院大学

内閣府 SIP プログラムディレクタ（PD）

サイバーセキュリティ戦略本部

後藤　厚宏

アジェンダ

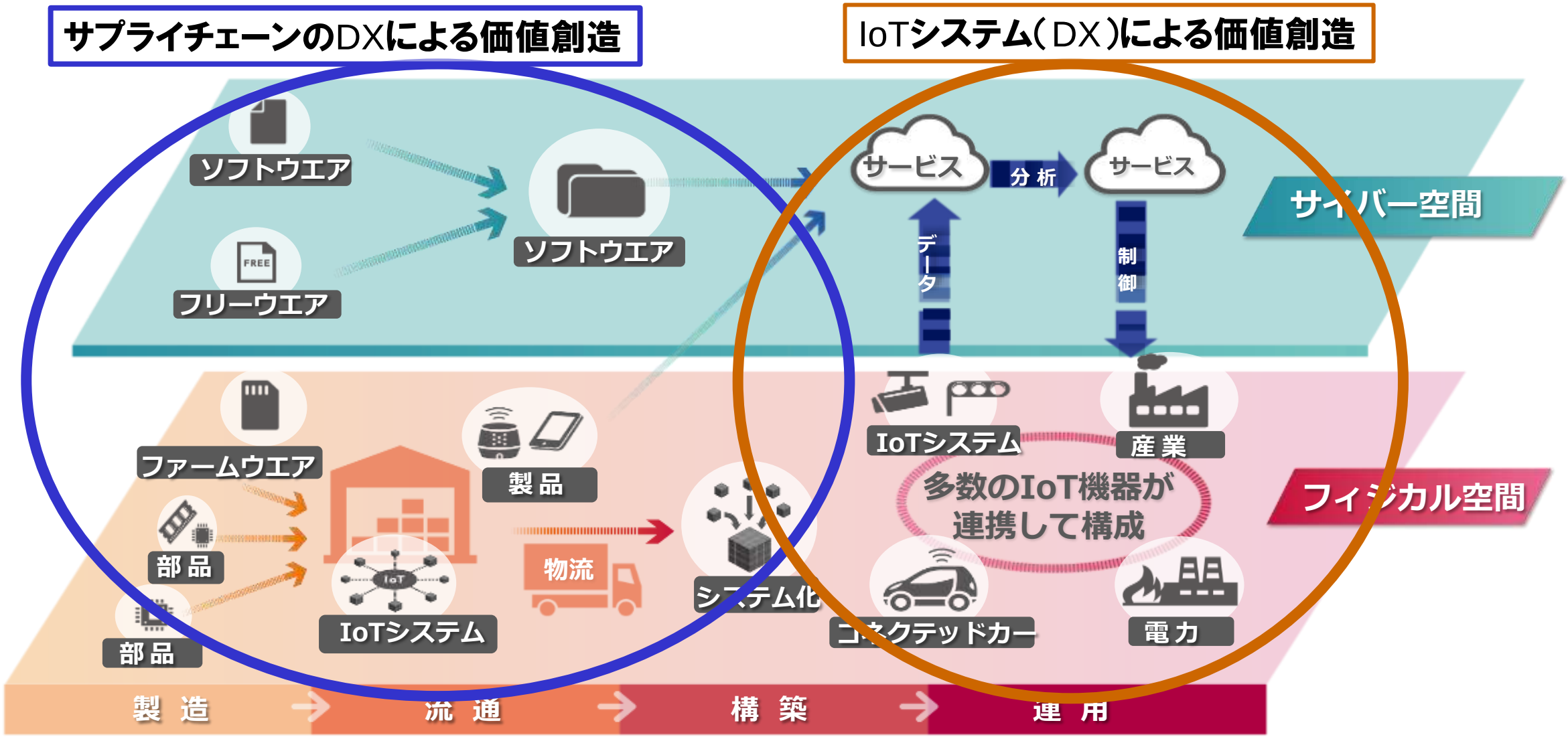
明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

- DX時代（Society5.0）の価値創造
- サイバー攻撃動向の振り返り
- IoT社会に対応したサイバー・フィジカル・セキュリティ
- IoTセキュリティ要件に関するグローバル動向
- PSIRTの役割
- IoT社会に向けた人材育成の取組み

DX時代（Society5.0）の価値創造

DX時代（Society5.0）の価値創造

サイバー・フィジカル・エコシステム



サイバー攻撃動向の振り返り

サイバー攻撃の動向

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

攻撃者は、国レベルで、システムレベルで、それぞれ弱いところを狙ってくる。

社会情勢の側面

攻撃者は経済原理に基づいて、同じ攻撃手法を別の標的にしかけてくる、執拗に繰り返す

経済合理性

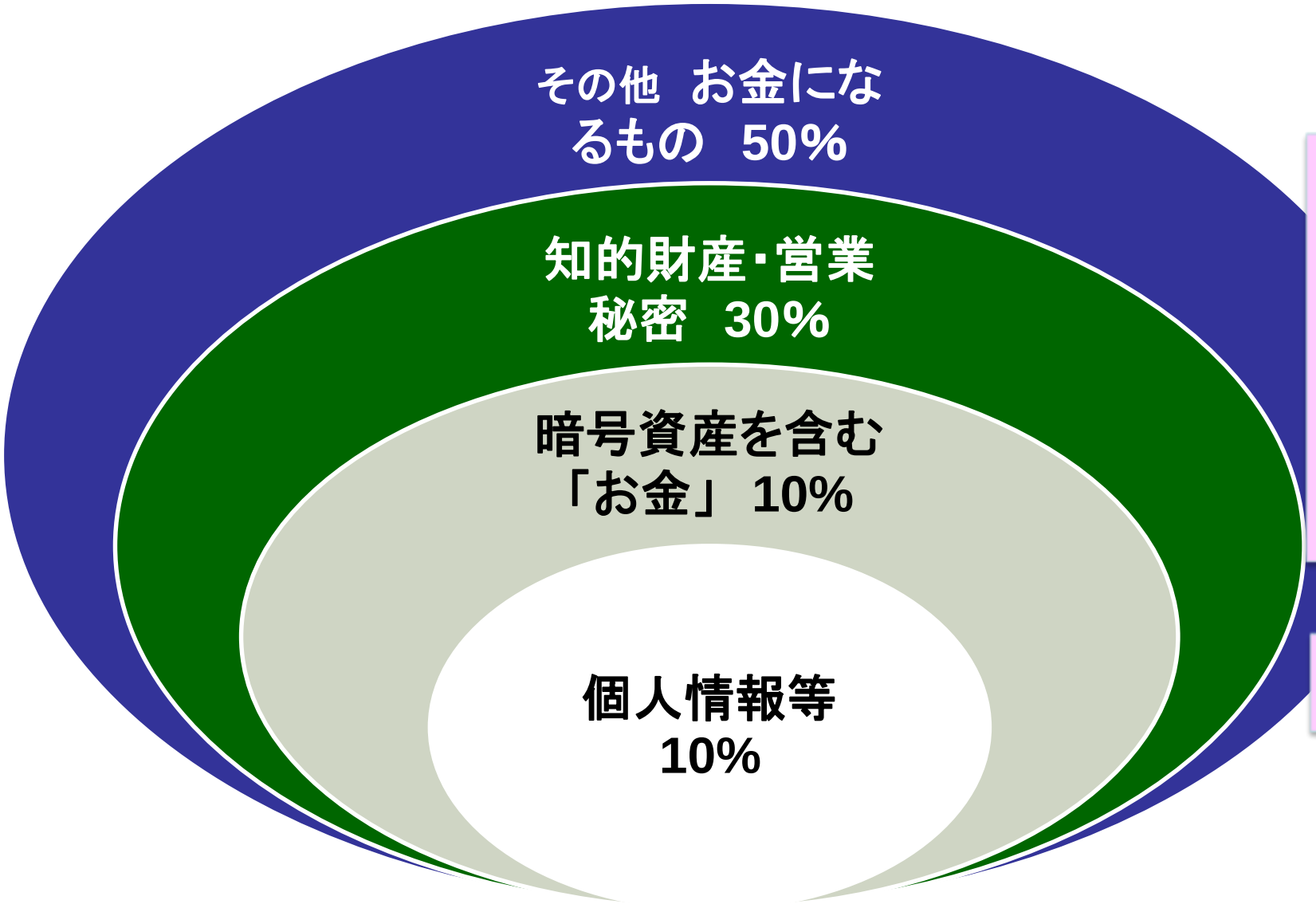
社会経済・システムのグローバルなつながりが攻撃にも利用される

グローバル社会

攻撃者はDarkWebで密に連携し、市場経済（ブラックマーケット）を活用

組織構造の側面

サイバー犯罪による経済損失



世界のサイバー犯罪による経済損失は6,000億米ドル（世界のGDPの0.8%相当）

日本では約3兆円

IoT社会に対応した
サイバー・フィジカル・セキュリティ

戦略的イノベーション創造プログラム SIP

第２期 SIP2　2018～2022

広義IoTがもたらす価値創造の多様性

SIP第2期
2018～2022

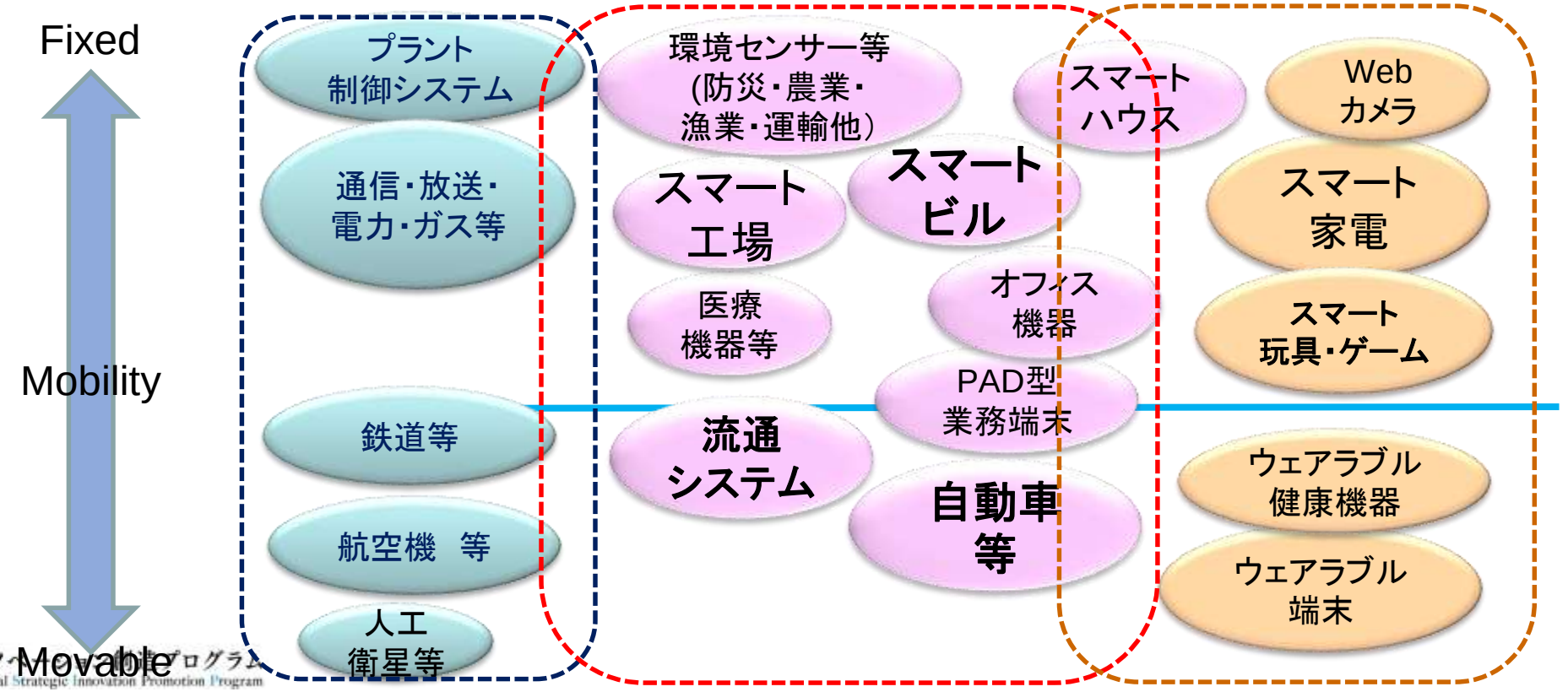
重要インフラの革新
「インフラIoT」

産業の新価値創造
「産業IoT」

「個」の新価値創造
「コンシューマIoT」

第1期SIP「重要インフラ等のサイバーセキュリティ確保」
（2015―2019）

第2期SIP「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）



IoTリスクとサプライチェーンリスクは喫緊の課題

SIP第2期
2018～2022

IoTリスク：サイバー攻撃の脅威が、あらゆる産業活動に潜む

世界のサイバー犯罪による経済損失は6,000億米ドル（世界のGDPの0.8%相当
⇒日本では**約3兆円**）

IoTによるフィジカルとサイバーの融合により、サイバー攻撃がフィジカル空間まで到達し、**経済損失がさらに拡大**するリスク

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なる動き

米国：サイバーセキュリティフレームワークv1.1に、『サイバーサプライチェーンリスクマネジメント』を明記。

防衛調達の全参加企業にセキュリティ対策（SP800-171の遵守）を義務化

欧州：ネットワークに繋がる機器の認証フレームの導入検討。

EUの顧客データに新たな義務（GDPR）2018年5月から

IoTリスク：IoT機器が社会インフラへサイバー攻撃

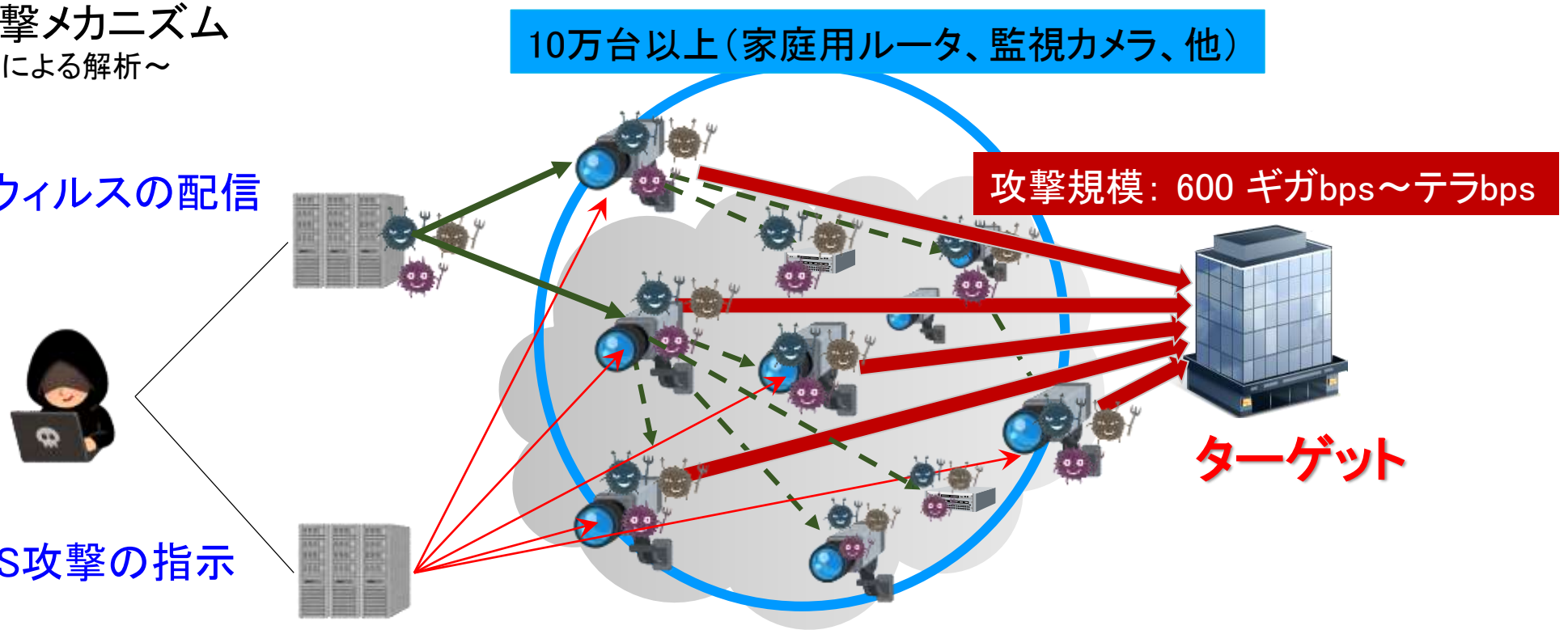
SIP第2期
2018～2022

■ Miraiの事案：脆弱性のあるIoT機器が大規模DDoS攻撃の踏み台

【事例1】 DDoS攻撃（2016/10）により約6時間にわたりインターネットサービスが不安定（Twitter, Amazon, Netflixが使えない！）

【事例2】 ドイツテレコムのホームルータをマルウェア感染させる攻撃（2016/11）により、90万人が影響を受ける

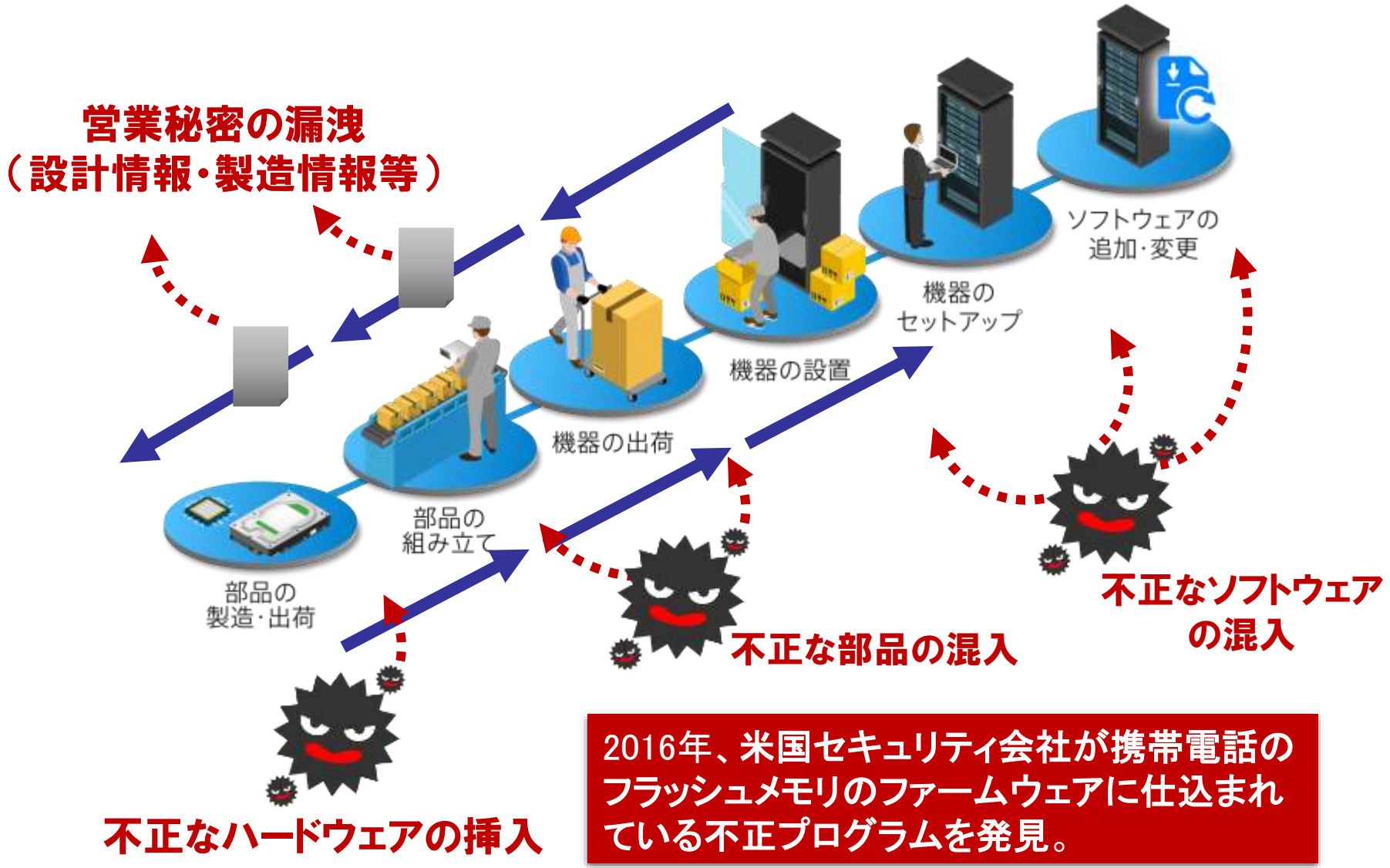
Miraiの攻撃メカニズム
～NTT研究所による解析～



同様の脆弱性を持つ多数の機器が感染し、一斉に遠隔操作される

サプライチェーンリスク：「混入」「改ざん」「漏洩」

SIP第2期
2018～2022

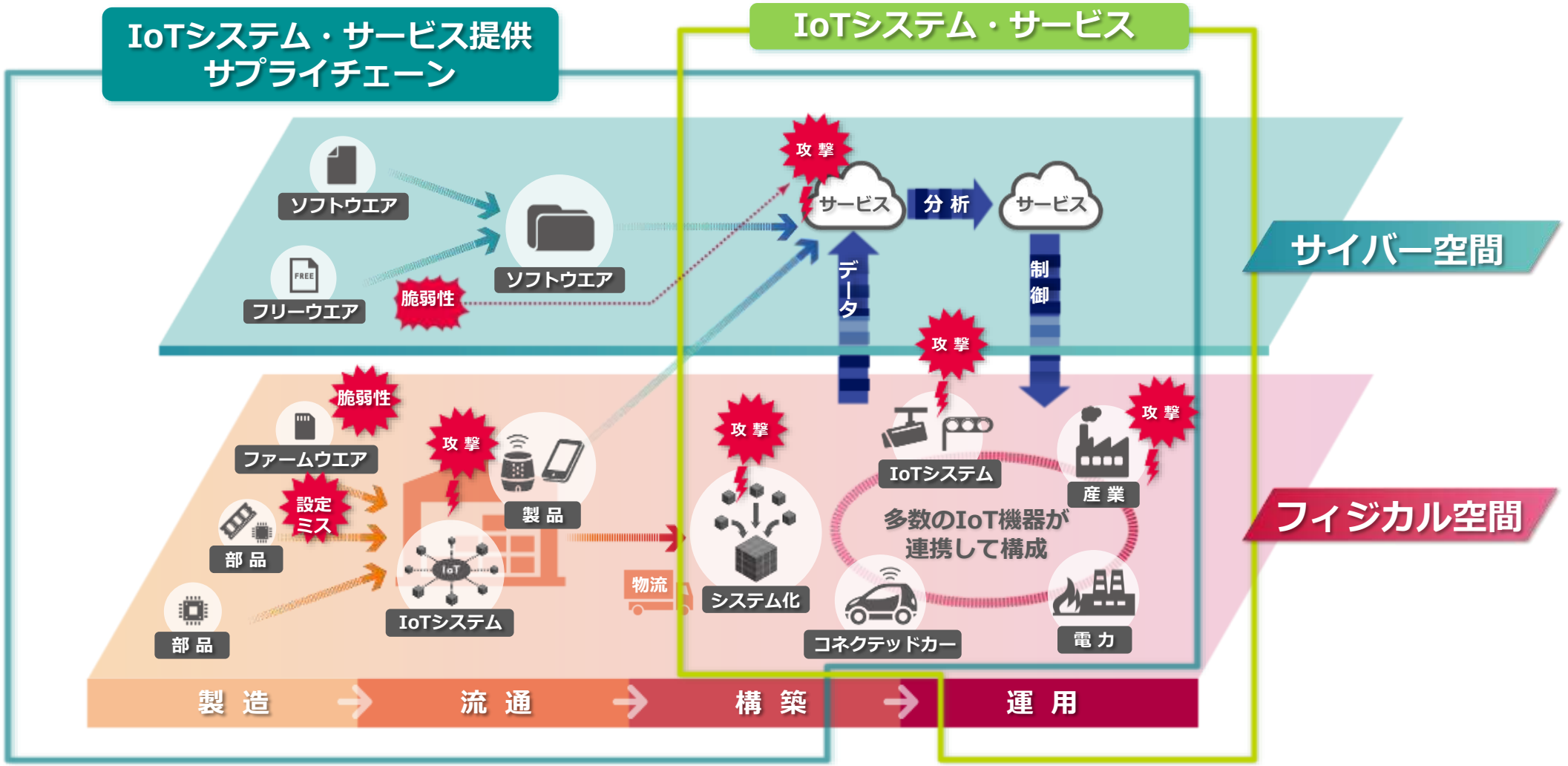


2016年、米国セキュリティ会社が携帯電話のフラッシュメモリのファームウェアに仕込まれている不正プログラムを発見。

サイバー・フィジカル・システムのセキュリティ課題

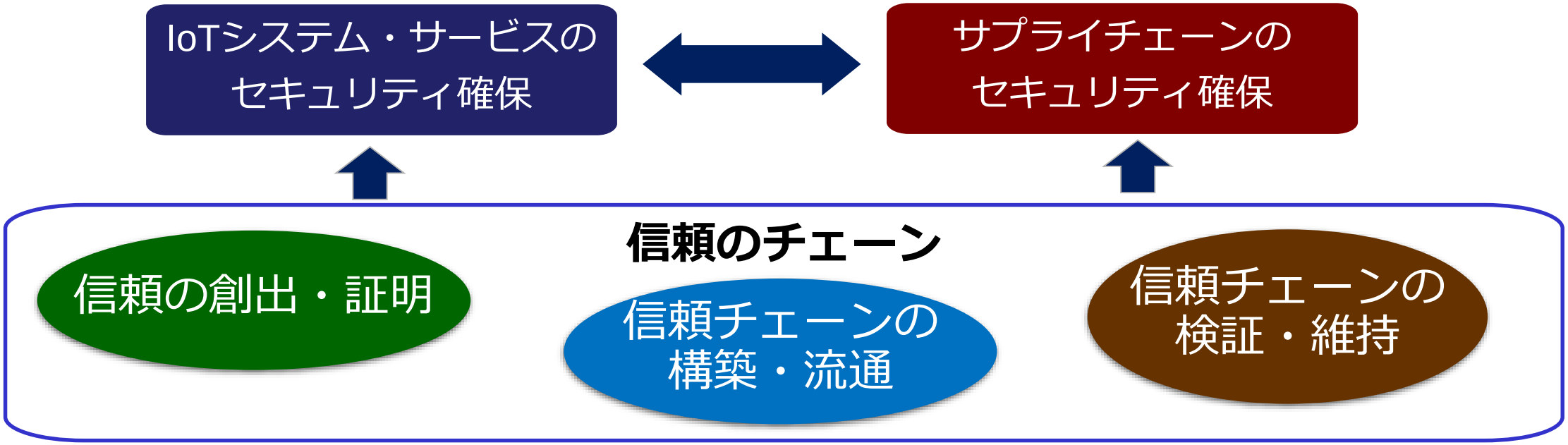
SIP第2期
2018～2022

サプライチェーンのセキュリティ確保 ⟷ **IoTシステム・サービスのセキュリティ確保**



「信頼のチェーン」によるセキュリティ確保

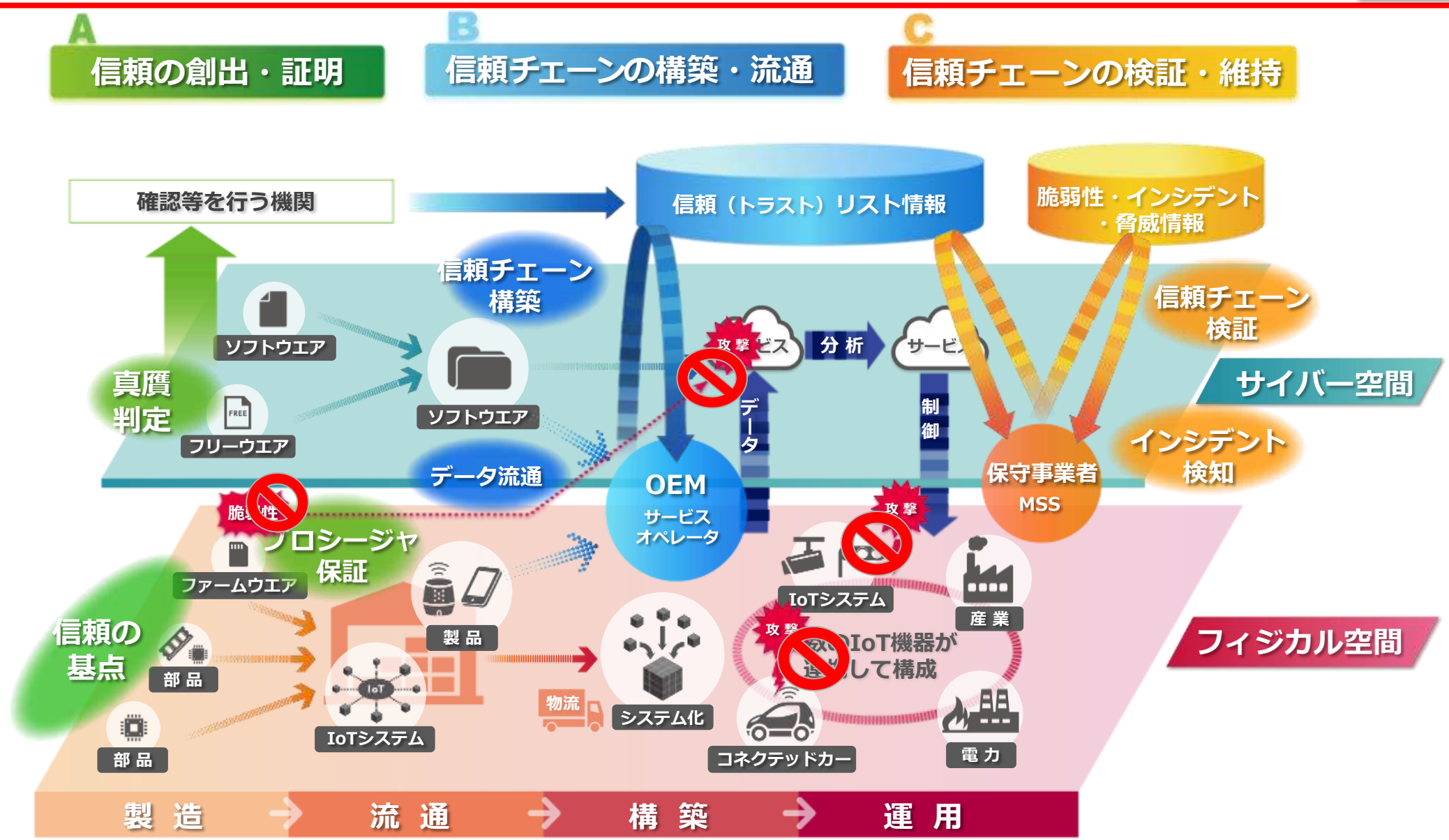
SIP第2期
2018～2022



- ◆社会全体の安全・安心を確立し、Society5.0がもたらす**約90兆円の価値創出**を支える
- ◆幅広い産業分野の国際競争力を高め、輸出主体の製造業の**参入機会の確保**する
- ◆2030年までにサプライチェーン対策が求められる**中小企業の50%**に成果導入を目指す

サイバー・フィジカル・セキュリティのエコシステム

SIP第2期
2018～2022



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

実フィールドで実証し社会実装へ

SIP第2期
2018～2022

2018年　　2020年　　2022年

技術開発と実フィールド事業者連携

実フィールドを持つ事業者やベンダーと密に連携した体制作り

製造・流通・ビル分野等での実証

（2020年目途）IoTシステムとサプライチェーンにおいて社会実装を目指した**実証実験に順次着手**

（2022年目途）**海外動向，国内制度**設計と連携・すり合わせ

幅広い産業分野へ拡大（本格的社会実装）

幅広い産業分野でのIoTシステムと，**中小企業を含めたサプライチェーン**の社会実装の促進

海外動向の調査

府省庁による制度設計・グローバルな調整

研究開発の実施チーム体制

SIP第2期
2018～2022

PD （後藤厚宏）
subPD 今瀬 真、瓜生 和久
内閣府(事務局), NEDO

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, 防衛省, 他
学会、産業界の有識者

WG等
海外動向WG
成果普及WG
実証評価WG

リーダー委員会
知財委員会

A.信頼の創出・証明			B.信頼チェーンの構築・流通		C.信頼チェーンの検証・維持		D 動向調査
A1	A2	A3	B1	B2	C1	C2	
ECSEC 産総研 (横国大、神戸学、東大、東北大、NAIST、三菱電機)	NTT NEC (FFRI)	日立 NEC KDDI総研 (ATR、早稲田大)	日立 NEC KDDI総研 (産総研、セコム、ATR)	富士通 (NII, 名大)	日立 NEC KDDI総研 (産総研、ATR)	NTT NEC 日立 三菱 (阪大、金沢工大)	NEC

(2018年度)

関係府省との連携状況

NISC

・サイバーセキュリティ戦略の重点項目のひとつ

経産省

・サイバーフィジカルセキュリティフレームワークの実現技術としての役割

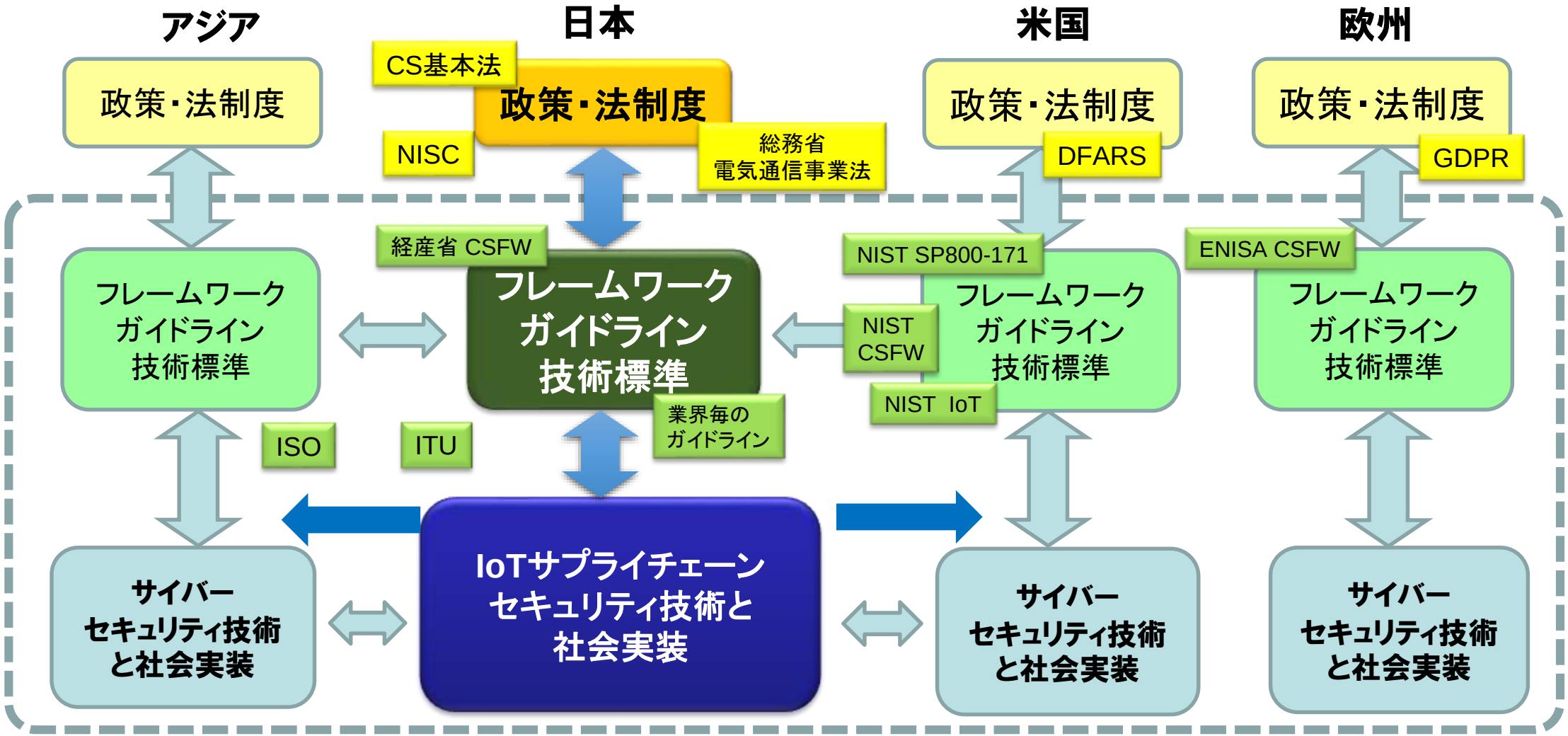
総務省

・NOTICE プロジェクトと連携するIoTセキュリティ技術

NOTICE (National Operation Towards IoT Clean Environment)

グローバルな協調と競争

SIP第2期
2018～2022



NISC: National center of Incident readiness and Strategy for Cybersecurity

NIST: National Institute of Standards and Technology
ENISA: European Union Agency for Network and Information Security

IoTセキュリティ要件に関する
グローバル動向

IoT・サプライチェーンセキュリティ グローバル動向

◆IoTセキュリティ：米・欧・日でフレームワーク議論が活発化。民間でフレームワークを支える技術開発が個々に進んでいる。

◆サプライチェーンセキュリティ：　政府調達（防衛含む）での取組みははじまっている。

米国

- （官）DoD DFARS
- （官）NIST
- （民）AIAG

欧州

- （官）ENISA
- （官）UK DCMS
- （民）ECSO: ECSC

日本

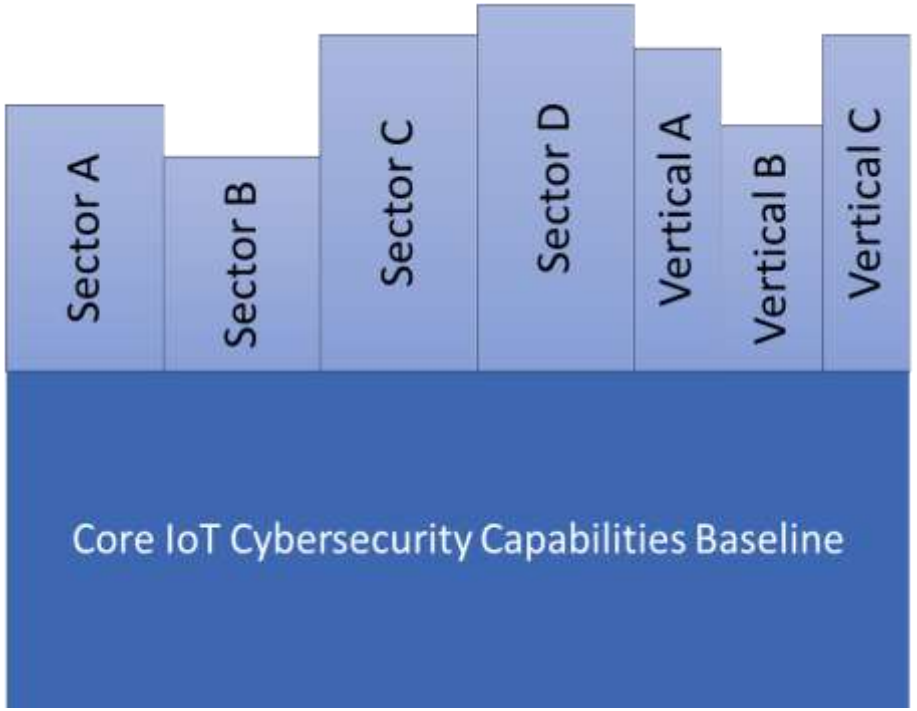
- （官） NISC
- （官民）IoT推進コンソーシアム
- （民）IPA　他

NIST: National Institute of Standards and Technology
AIAG: Automotive Industry Action Group

ENISA: European Union Agency for Network and Information Security
NCSC: National Cyber Security Centre
DCMS: Department for Digital, Culture, Media and Sport
ECSO: European Cyber Security Organisation

米国 NIST IoT Security & SCRM

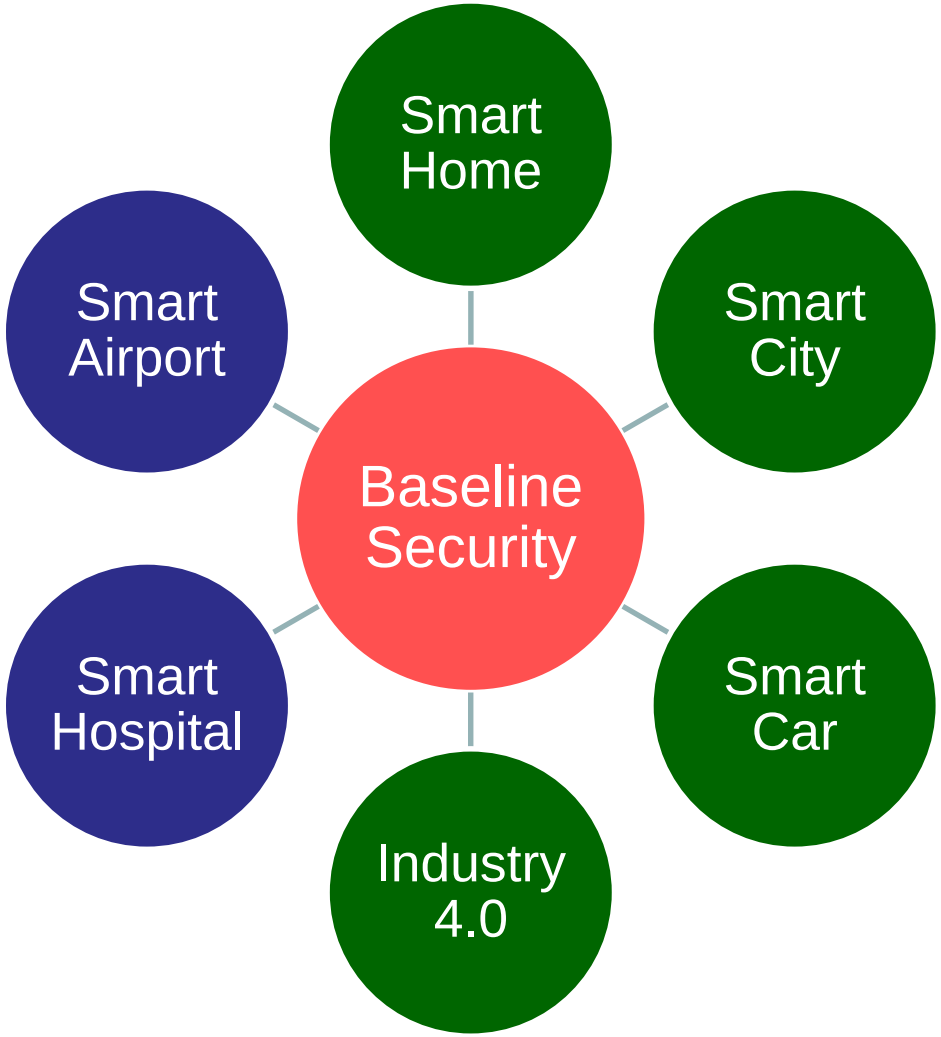
- Cybersecurity Framework Version 1.1 (2018/4)⇒サプライチェーリスク管理が追加
- Draft NISTIR 8228: Considerations for IoT Cybersecurity and Privacy Risks
- Draft NISTIR 8259: Core Cybersecurity Feature Baseline for Securable IoT Devices: *A Starting Point for IoT Device Manufacturers* (2019.7)⇒9末までに450コメント
- Draft NISTIR 8267: Security Review of Consumer Home Internet of Things (IoT) Products (2019.10)⇒パブコメ中（11/1まで）



Core Cybersecurity Feature Baseline

欧州 ENISA IoT Security

- Baseline Security Recommendations for IoT ＋ 分野毎の指針
- IoT Security Standards Gap Analysis (2019/1)
- Industry 4.0 – Cybersecurity Challenges and Recommendations (2019/5)
- Bolstering ENISA in the EU Cybersecurity Certification Framework(2019/7)
- Good Practices for Security of IoT (2019/11 予定)



PSIRTの役割

PSIRT Product Security Incident Response Team

■ PSIRT（Product Security Incident Response Team）は、組織が提供する製品の脆弱性に起因するリスクに対応するための組織内機能。自社製品の脆弱性への対応、製品のセキュリティ品質管理・向上を目的とした組織。

■ FIRSTのドキュメント（JPCERTが日本語訳）

https://www.first.org/education/FIRST_PSIRT_Services_Framework_v1.0_draft_ja.pdf

■ サプライチェーンを含むセキュリティ要件への対応と製品に関わるインシデント時の対応

ドイツテレコムの「神」対応？？

【MIRAI 事例2】ドイツテレコムのホームルータをマルウェア感染させる攻撃（2016/11）により、90万人が影響を受ける

■ 新たな被害を防ぐために**ネットワークにフィルタを設定**
- 攻撃者が遠隔保守インタフェースにアクセスすることを防ぐ

CSIRTの役割：DTのネットワークはしっかりマネージドできていた！

■ これと並行して、ルータ製造企業に**修正ファームウェア作成を依頼**
- 発生からほぼ一日で影響を受けた端末に対して配布開始

機器ベンダ（PSIRT）とNW事業者（CSIRT）の密な連携ができていた！

■ 影響の有無に関わらずSpeedportルータの全モデルをチェックし、適切な**ファームウェアをリリース**

PSIRTの役割：大量のNW端末の遠隔更新機能が具備できていた！

IoT社会に向けた人材育成の取組み

情報セキュリティ大学院大学

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

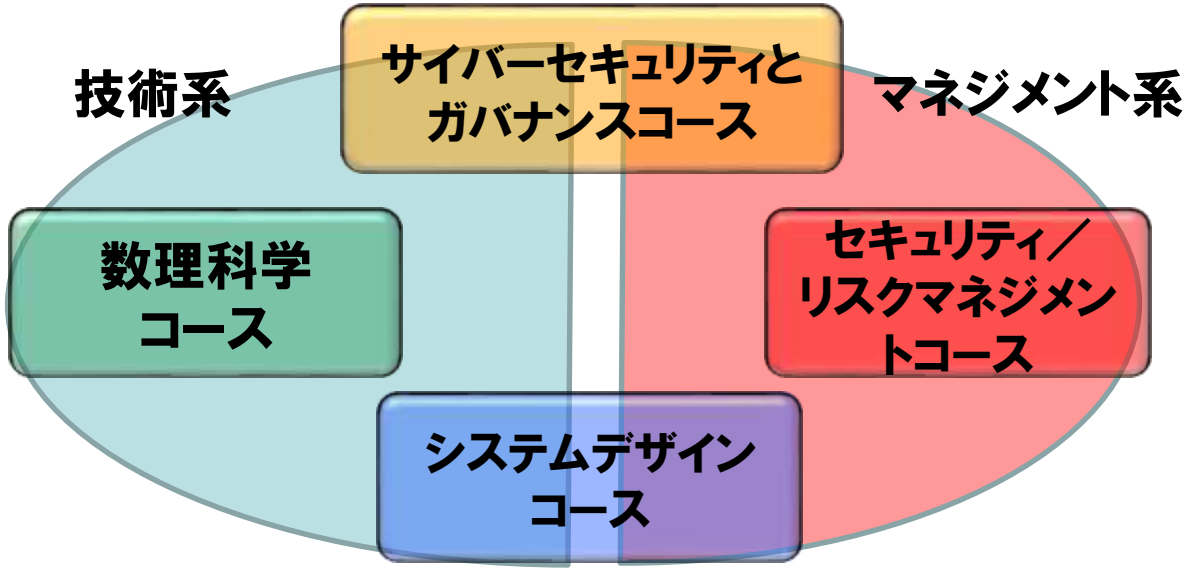
■本学は、2004年に開学し、新しい学問の体系化と専門家の育成を旗印に、情報セキュリティ専門の独立大学院として教育と研究に携わってきました。

■2019年9月末までに、修士(情報学)406名、博士(情報学)38名の修了生が日本の情報セキュリティに関する中核的業務を担っています。

本学の特色

約8割が社会人学生(2018-2019実績:インフォシスリミテッド／エヌ・ティ・ティ・コミュニケーションズ(株)／エヌ・ティ・ティ・コムウェア(株)／NTTテクノクロス(株)／LM総合法律事務所／海上保安庁／外務省／神奈川県警察／(株)エヌ・ティ・ティ・エムイー／(株)小野測器／(株) 協和エクシオ／(株)センチュリーインフォテック／(株)JR東日本情報システム／(株)タツノ／(株)東陽テクニカ／(株)日立システムズ／(株)Beyond Soft Japan／(株)富士通ソフトウェアテクノロジーズ／(株)本田技術研究所／(株)ミライト・テクノロジーズ／金融庁／警察庁／警視庁／埼玉県警察／埼玉県／さくら情報システム(株)／CsSoft(株)／ジェイアール東海情報システム(株)／昭和シェルビジネス&ITソリューションズ(株)／第一生命保険(株)／(独)日本学術振興会／(独)国立印刷局／日本コムシス(株)／日本電気(株)／日本電気計器検定所／東日本旅客鉄道(株)／日立キャピタル(株)／防衛省／横浜市役所／楽天(株)／陸上自衛隊　など)

総合科学:情報セキュリティカリキュラム



情報セキュリティ大学院大学　カリキュラム　（2019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

サイバーセキュリティとガバナンス

- サイバーセキュリティ技術論
- セキュアシステム構成論
- 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
- 特設講義（サイバー・インテリジェンス）
- 特設講義（ハッキングとマルウェア解析）

セキュリティ／リスクマネジメント

- 情報セキュリティマネジメントシステム
- セキュリティシステム監査
- セキュリティ管理と経営
- 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
- リスクマネジメント
- リスクの経済学
- 統計的リスク管理
- 統計的方法論
- セキュリティ監査
- 国際標準とガイドライン
- 情報セキュリティ心理学

数理科学

- 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
- 暗号理論
- AIと機械学習
- 特設講義(ブロックチェーン理論)

システムデザイン

- インターネットテクノロジ
- ネットワークシステム設計・運用管理
- 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

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

社会人向け集中コース　https://www.iisec.ac.jp/sslab/courses.html

- BS-1：セキュアシステム技術演習(基礎)（6 days, 30 units）
- 「CSIRT構築に向けて」コース
  - CT-1：CSIRT構築の手引きコース（2 days, 8 units）
  - CT-2：ネットワークセキュリティ技術演習（2 days, 8 units）
  - CT-3：Webアプリケーション検査演習（2 days, 8 units）
  - CT-4：デジタルフォレンジック演習（3 days, 12 units）
- 「IoTセキュリティ」コース　http://www.iisec.ac.jp/news/20190917news-IoT.html
  - IoT-1：組込システムの基礎（1 day, 4 units）
  - IoT-2：IoTアーキテクチャ（2 days, 8 units）
  - IoT-3：IoTシステムの脅威分析と脆弱性検査演習（2 days, 8 units）
- 2020年度から「戦略マネジメント層育成コース」を開講予定