資料1-2

各省庁における
研究開発に係る取組について

令和3年6月

内閣サイバーセキュリティセンター（NISC）
基本戦略第１グループ

目次

※資料1における施策の掲載順

研究開発推進に向けた取組

NISC①

○研究開発の国際競争力の強化と産学官エコシステムの構築に向けた取組

関係府省が提供する、科学的理解やイノベーションの源泉となるような研究及び産学官連携の振興施策の活用を促進し、研究コミュニティの自主的な発展努力と相まった、重点的な研究・産学官連携の強化を図る。これとあわせ、研究環境の充実等により、研究者が安心して研究に取り組める環境整備に努める。

産学官にわたるエコシステム構築が図られるためには、それぞれの主体の自主的な発展努力が必要不可欠であり、これらの取組状況についてフォローアップを行いながら、取組を推進していく。

○実践的な研究開発の推進に向けた取組

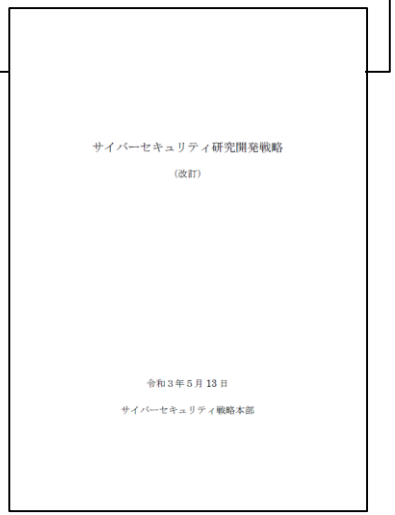
戦略期間において、関係府省の取組を推進するとともに、研究及び産学官連携の振興に係る関係府省の取組を含め取組状況をフォローアップし、取組のマッピング等による点検と必要な再整理を行う。

※ 上記に当たっては、中長期的な視点から、AI技術・量子技術をはじめとする先端技術の進展を見据えた対応を図る。

【参考】「サイバーセキュリティ研究開発戦略（改訂）」

令和3年(2021年)5月13日
サイバーセキュリティ戦略本部決定

○研究開発に関わる幅広い層（政府機関から研究者まで）を対象として、将来的なサイバーセキュリティ研究開発を検討・推進するためのビジョン（基本的な考え方や方法論など）を提示。



【目次】

令和3年5月改訂時 追加箇所

（1）我が国の研究コミュニティの状況を踏まえた推進方策

① 研究分野の国際動向と特徴
（情報系と同様、柔軟で優秀な「人材」が大きく研修を進展させ得る 等）

② 人に投資すべき
（研究プロジェクトや産学共同研究費においてRA（リサーチアシスタント）経費を柔軟に設定し、優秀な人材を迎える形態が必要 等）

③ 産学官連携の可能性
（インターネット企業やDX企業の経営的かつ潜在的ニーズに応え得る産学共同研究が今後検討されるべき 等）

④ 研究コミュニティ全体の発展
（ファンディングの機会と研究費の活用、科学的基礎に係る概念の言語化、プロシーディング論文を含む柔軟な研究実績の評価 等）

（2）我が国の強み・ポテンシャルと重点的な強化に向けて

① 我が国の強みとポテンシャル
（IoTｾｷｭﾘﾃｨ、ﾃﾞｰﾀｾｷｭﾘﾃｨ・プライバシー保護など欧米に比肩、ｻｲﾊﾞｰ･ﾌｨｼﾞｶﾙ融合領域、暗号研究の強みを活かす領域にポテンシャル 等）

② 重点的な研究領域
重点的な強化が図られることが望ましい研究領域を整理

（3）研究コミュニティの継続的な取組

サプライチェーンリスクへ対応するためのオールジャパンの技術検証体制の整備

NISC②

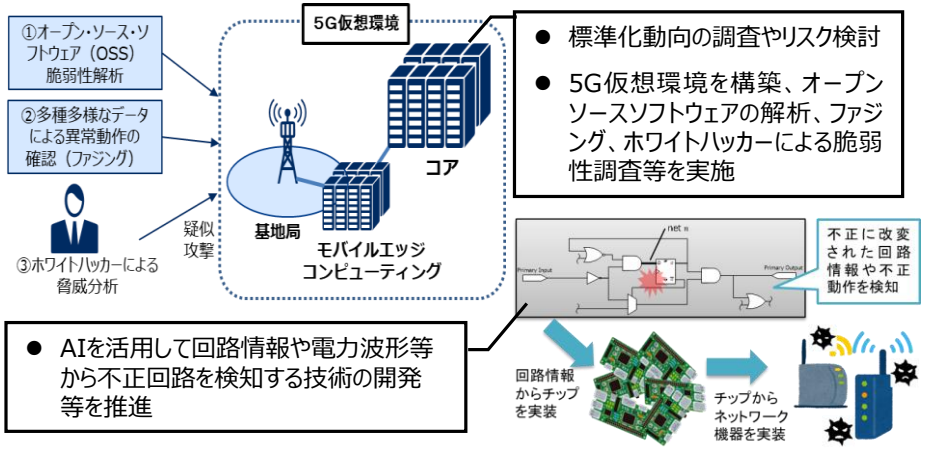
- 我が国において、5Gネットワークのセキュリティ確保や、サイバーセキュリティの検証ビジネスの活性化などをはじめとして、ICT機器・サービスの信頼性を確保するための技術開発と推進体制の構築を進め、サプライチェーンリスクに対応するための技術検証体制の整備を推進することが必要。
- 内閣官房においては、2020年度、試行的検証を含め、技術検証体制の整備に向けた技術面での検討調査を実施。（本成果を踏まえ、2021年度以降、段階的に本格運用に係る取組を進める。）

オールジャパンの官民連携体制の構築

○関係省庁に加え、公的研究機関や大学、民間のセキュリティーベンダーや通信キャリア等と連携し、技術検証体制を構築（内閣官房）

技術検証体制を支える施策の推進

○５Gを含むシステム等に組み込まれた不正な機能や脆弱性を効率的に検出する技術開発・検証（総務省）



- 標準化動向の調査やリスク検討
- 5G仮想環境を構築、オープンソースソフトウェアの解析、ファジング、ホワイトハッカーによる脆弱性調査等を実施
- AIを活用して回路情報や電力波形等から不正回路を検知する技術の開発等を推進

○攻撃型手法を含むハイレベルな検証サービスの実証（経済産業省）

実証

検証対象
- ネットワークに常時接続する端末機器
- サイバー攻撃を受けることにより事故に繋がる可能性があるもの　等

検証

検証手法・検証ツール（ペネトレ、ソフトウェア分析　等）＋検証事業者（ホワイトハッカー　等）

検証技術等の技術開発
・産総研サイバー・フィジカル・セキュリティ研究センター
・内閣府SIPプロジェクト、AIチッププロジェクト　等

実証の成果と活用のイメージ

①各検証手法を用いた、対象機器・システムごとの検証結果
⇒IoT機器等毎の効果的な検証手法の考え方を整理

②検証事業者に求められる、情報管理体制等の考え方の整理
⇒信頼できる検証主体を確認する仕組みの検討

③技術開発支援などにより、我が国の検証技術の高度化
⇒検証サービスの効果向上

○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）

・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ことに活用できる「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

戦略的情報通信研究開発推進事業（SCOPE）

総①

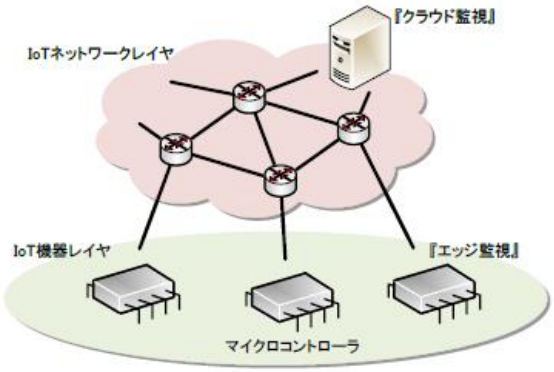
情報通信技術（ICT）分野において新規性に富む研究開発課題を大学・国立研究開発法人・企業・地方公共団体の研究機関などから広く公募し、外部有識者による選考評価の上、研究を委託する競争的資金※。これにより、未来社会における新たな価値創造、若手ICT研究者の育成、ICTの利活用による地域の活性化、国際標準獲得等を推進。

※ 資源配分主体が広く研究開発課題を募り、提案された課題の中から、専門家を含む複数の者による評価に基づいて実施すべき課題を採択し、研究者等に配分する研究開発資金。

IoT部品・機器・ネットワークの階層横断セキュリティ技術の研究開発

研究機関：早稲田大
研究期間：平成29～30年度
研究費（間接経費含む）：43,420千円

本研究開発では、IoT 機器を構成する個別の回路部品に不正部品（ハードウェアトロイと呼ばれる）がない安全な回路設計の実現のためハードウェアトロイ検出の開発技術、また、IoT 機器・IoT ネットワークのセキュリティを担保する技術の実現に向けて、『エッジ監視』と『クラウド監視』の２つの監視技術の研究開発を行った。

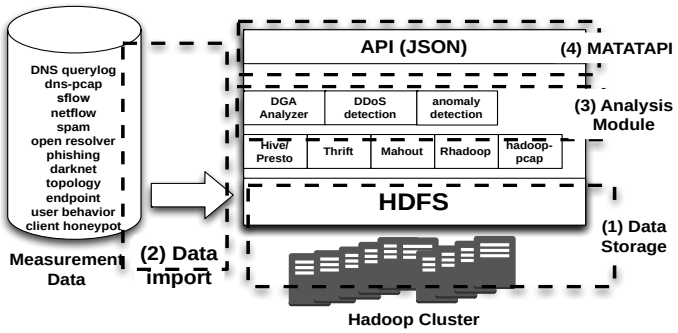


IoT 機器とIoT ネットワークモデル

日欧協調によるマルチレイヤ脅威分析およびサイバー防御の研究開発

研究機関：（日本側）奈良先端大、(株)ｲﾝﾀｰﾈｯﾄｲﾆｼｱﾃｨﾌﾞ技術研究所、NII、慶應義塾大、東京大
（欧州側）IMT（フランス）、FORTH（ギリシャ）、ATOS（スペイン）、NASK/CERT-Polska（ポーランド）、6cure（フランス）
研究期間：平成25～27年度
研究費（間接経費含む）：242,120千円

本研究開発では、攻撃コードの解析やネットワーク観測に関する研究成果や、クラウド等に対する新たな脅威の動向をふまえ、それらの知見をサイバー防御に応用した。脅威データ獲得、解析、サイバー防御の各段階を連接し、それらをまたがる制御を行うことにより、DDoSやボットネット、フィッシングに対するサイバー防御の自動化を提案し実証実験を行った。



MATATABIの概要

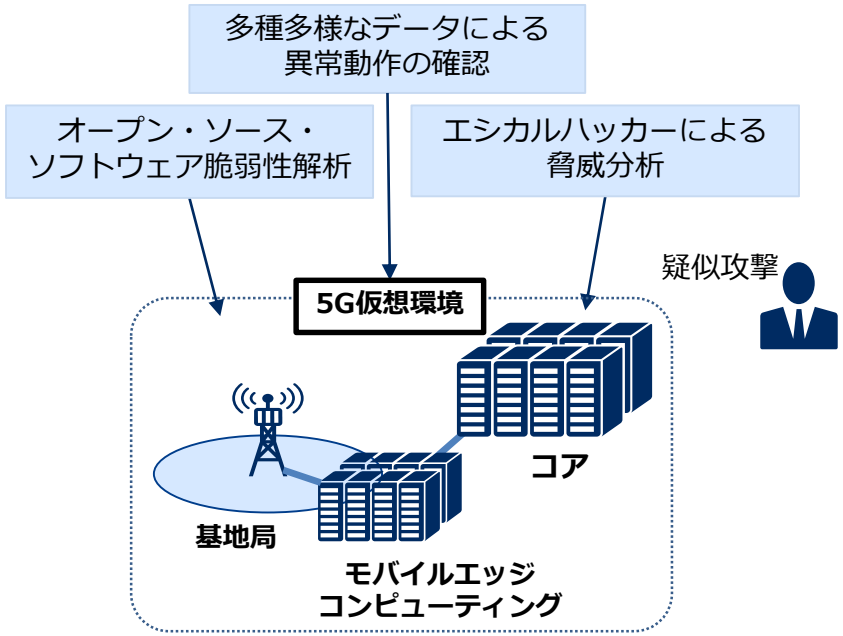
５Ｇのセキュリティ確保に向けた取組み

総②

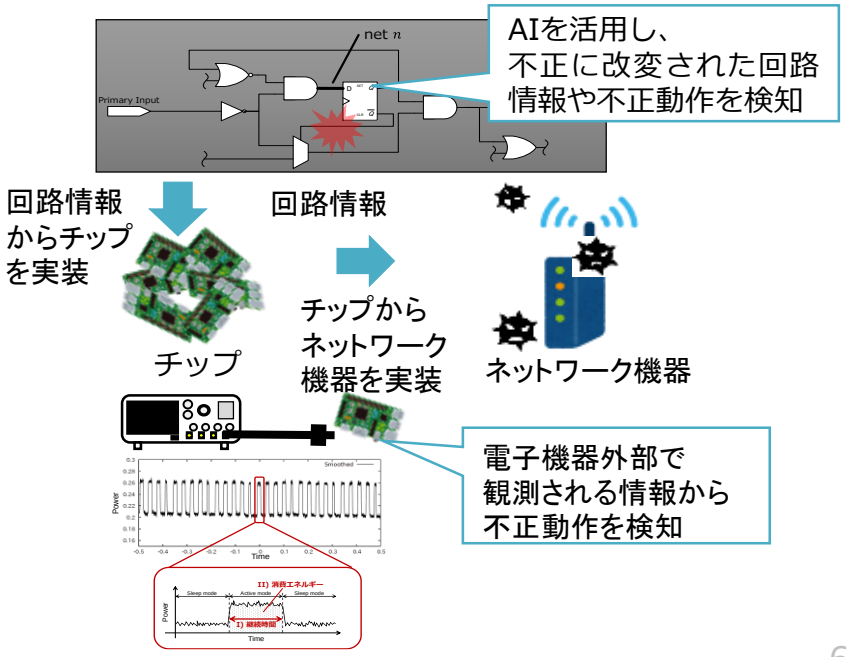
- サプライチェーンリスクへの対応も念頭に置きつつ、以下の取組みを推進。
  - 5Gネットワークのセキュリティを総合的かつ継続的に担保できる仕組みの構築を目指し、**ソフトウェア・ハードウェアの両面から**、5Gネットワークやその構成要素等につき**技術的検証**を実施。
    ⇒ 事業の成果を**５Ｇセキュリティガイドライン**の形で関係者と共有し、実対策の推進を図る。
  - 事業者・運用者・ベンダー間で**5Gのリスク情報や脅威情報などの共有を推進**する体制の整備
  - 全国５Ｇ及びローカル５Ｇの導入事業者に対する**税制優遇措置等**を通じた、安全・安心な５Ｇシステムの普及支援等を実施

5Gネットワークの脆弱性の技術的検証

(a) ソフトウェアを中心としたネットワークの脆弱性検知

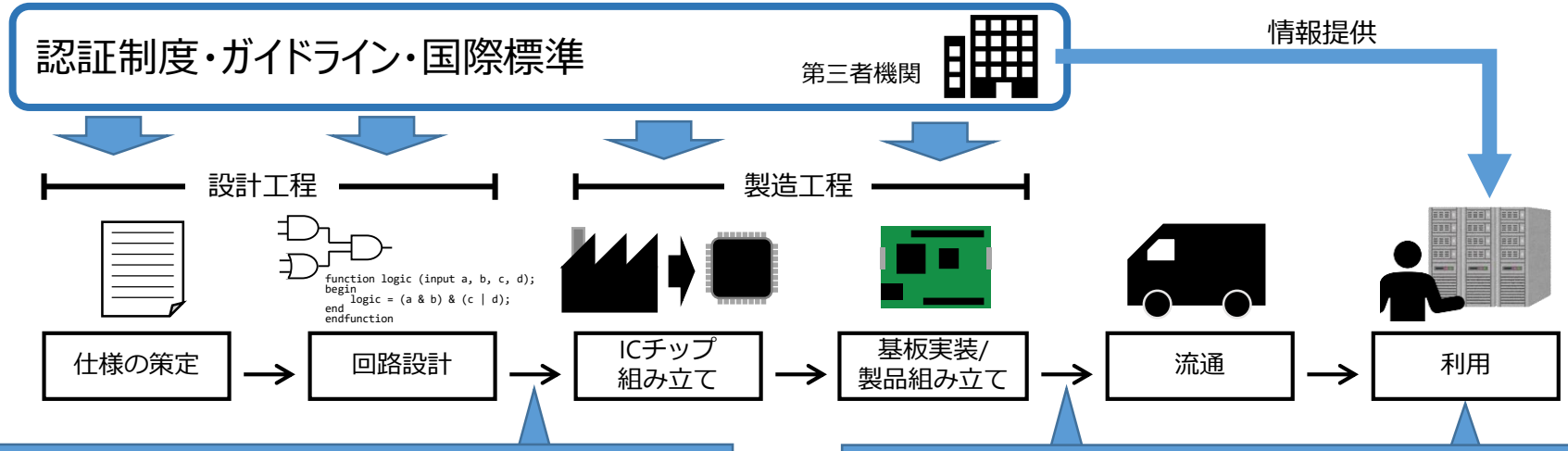


(b) ハードウェアの脆弱性検知



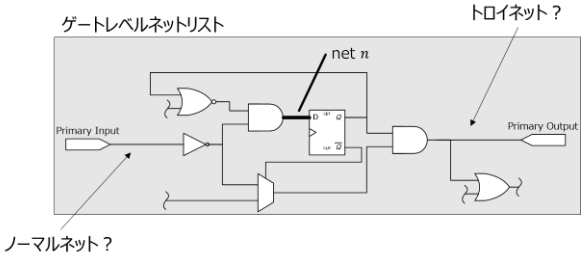
ハードウェアチップの脆弱性検知手法の調査・検討

IoT 機器に搭載されたソフトウェアだけでなく、ハードウェアのセキュリティを含めたサプライチェーン全体のセキュリティの確保が課題。
ハードウェアチップの設計・製造、及びその利用における脆弱性検知手法、並びにサプライチェーン上での 運用技術を確立するとともに、当該技術の社会実装を目指す。



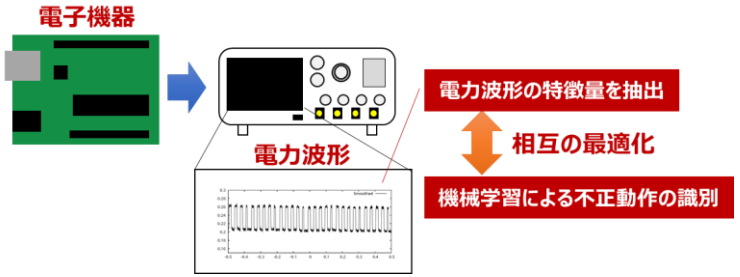
不正回路検知技術

- 設計データから不正回路を検知する技術の検討
- ゲート（論理ゲート、プライマリ入出力やフリップフロップ）の接続情報（ゲートレベルネットリスト）の信号線（ネット）をハードウェアトロイ回路を構成する信号線か否かを抽出された信号線特徴量から分類する技術
- 画像や音声と異なる回路に対する敵対的サンプル攻撃のおそれと対処の検討



不正動作検知技術

- チップの外部情報から不正動作を検知する技術の検討。
- ゲートレベルネットリスト等、回路の情報が入手できない場合を想定し、電子機器そのものを対象として、電子機器の電力波形を計測することで、不正な動作を検知する技術。

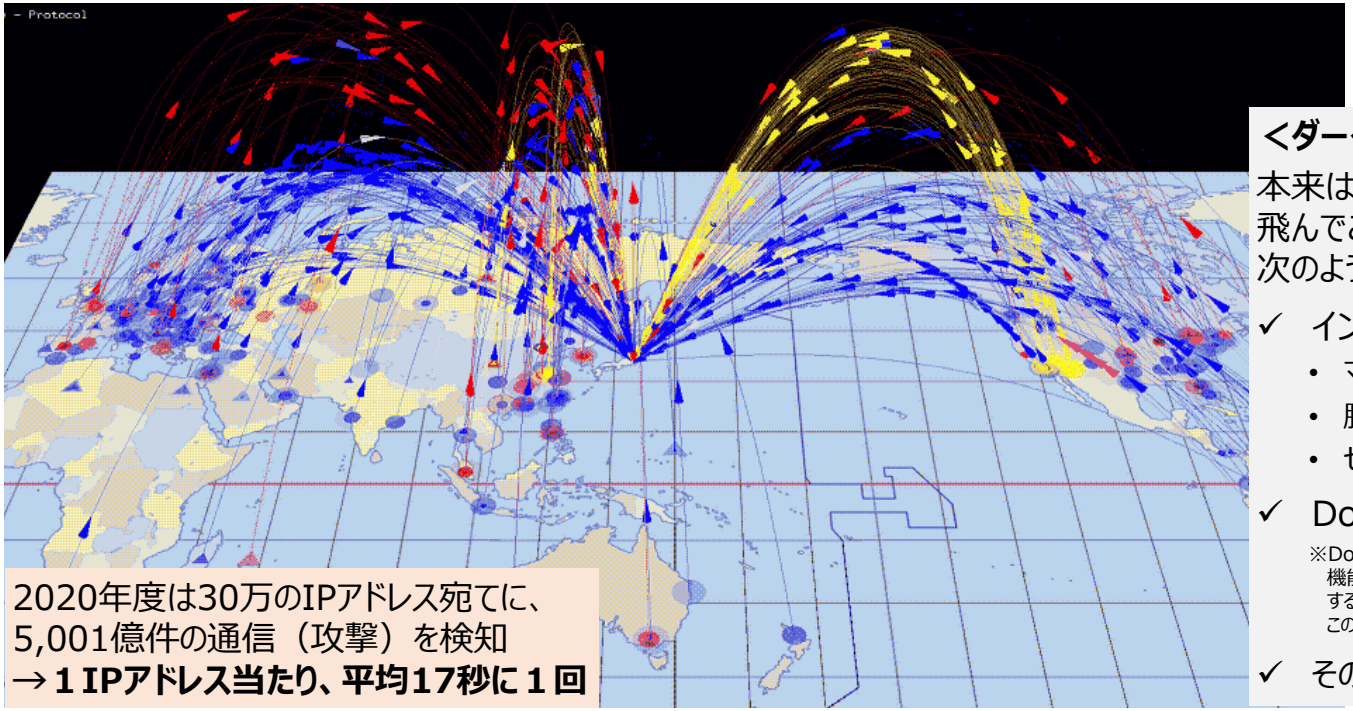


攻撃把握・分析・共有基盤の強化（1/3）

総③

- NICTERは、無差別型サイバー攻撃を、リアルタイムかつ大規模に観測・分析するシステム。
- 国内外の30万の未使用IPアドレスからなる「ダークネット」により攻撃を観測。

Network **I**ncident analysis **C**enter for **T**actical **E**mergency **R**esponse



2020年度は30万のIPアドレス宛てに、
5,001億件の通信（攻撃）を検知
→１IPアドレス当たり、平均17秒に１回

＜ダークネット = 未使用IPアドレス群＞

本来は使用されてIPアドレス宛には通信は飛んでこないはずだが、観測を行うことで、次のような通信を検知可能。

- ✓ インターネット上で何かを探す行為
  - マルウェアによる感染拡大のための通信
  - 脆弱な設定のサーバ等を探索する行動
  - セキュリティ関連組織等による調査
- ✓ DoS攻撃の跳ね返り

※DoS攻撃：サーバの処理能力を超える大量の通信を送りつけ、機能不全にする攻撃。こうした攻撃は送信元IPアドレスを偽装するため、サーバ側はその偽装されたIPアドレスに返答を返す。この返答する通信（バックスキャッタ）を観測する。

- ✓ その他設定ミス等による通信

セキュリティ関連組織への観測情報提供

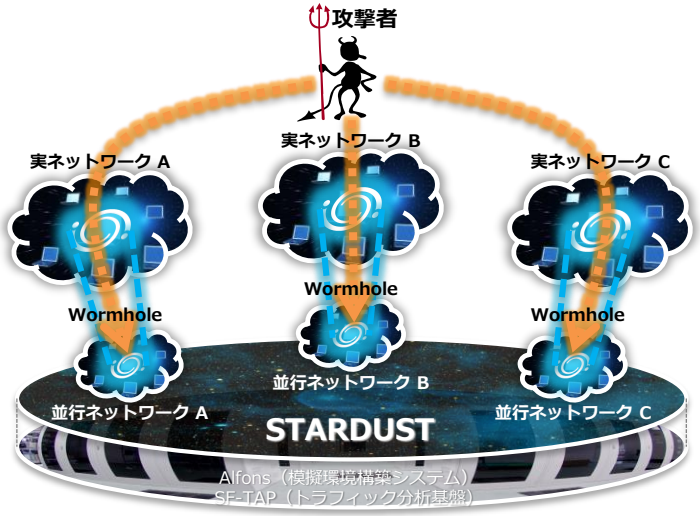
- ✓ SIGMON（定点観測友の会）JPCERT/CC、IPA、@Police等との観測結果共有（2004年～）
- ✓ ICT-ISAC Japan（DoS攻撃即応-WG）DoS攻撃関連情報共有（2011年～）
- ✓ オリパラ体制検討会（NISC、組織委、関連組織）DoS攻撃関連情報共有（2015年～）
- ✓ サイバーセキュリティ協議会（NISC、関連組織）第二類構成員として参画（2019年～）

攻撃把握・分析・共有基盤の強化（2/3）

サイバー攻撃誘引基盤**STARDUST**の研究開発を推進し、標的型攻撃等のHuman-operatedな（人手による）サイバー攻撃の把握を可能にする技術の確立を目指す。

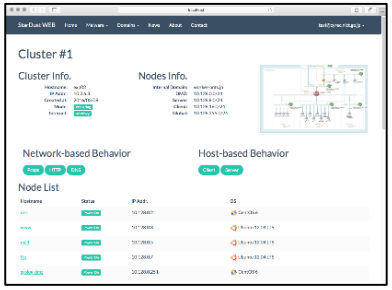
STARDUST システム概要

- ✓ 企業サイズの模擬環境を60並列で自動生成可能なシステムを実現
- ✓ 模擬環境に実環境のIPアドレス転写を可能にするWormhole開発



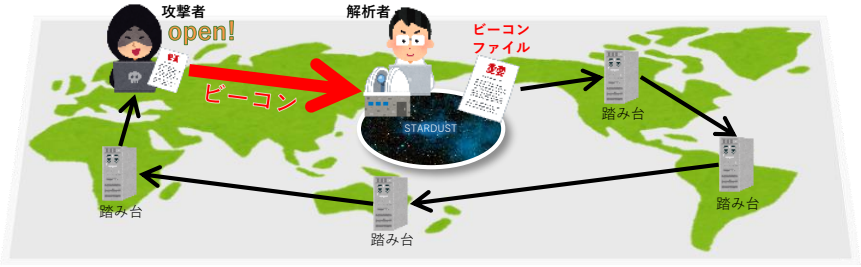
STARDUST Web

- ✓ STARDUSTによる攻撃者誘引をリーモート管理可能なWeb UI



攻撃元アトリビューション実証実験

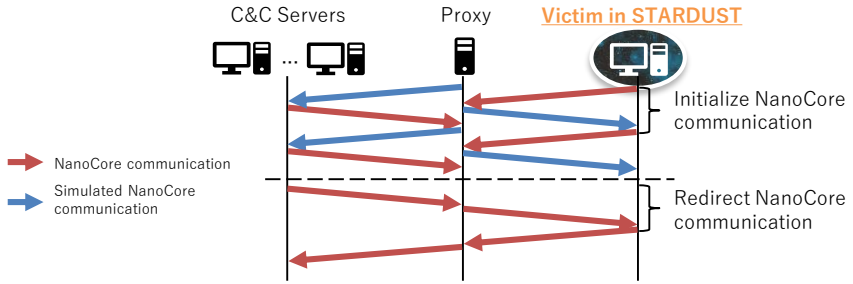
- ✓ 攻撃元追跡用Webビーコン入り模擬情報開発
- ✓ 並行ネットワーク11並列、延べ250検体以上で実験



攻撃者がビーコンファイル（模擬情報）を閲覧すると追跡用のビーコンを発信（注：図と実際の実験結果は異なる）

NanoCore Hunter

- ✓ 攻撃用リモートアクセスツールNanoCoreをSTARDUST内で解析
- ✓ C&C等のIoC情報をセキュリティ関連組織と共有、解析ツール公開



その他

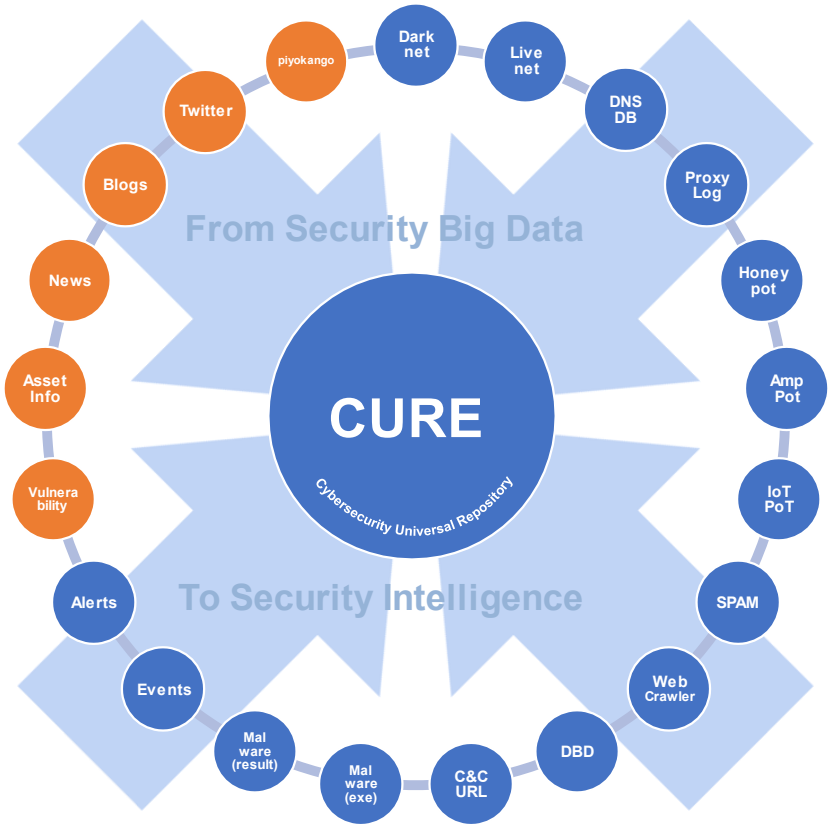
- ✓ 10組織以上の外部組織がSTARDUSTを利用
- ✓ 解析者コミュニティ「サイバー攻撃解析分科会」で解析情報共有

攻撃把握・分析・共有基盤の強化（3/3）

セキュリティ情報融合基盤**CURE**の研究開発を推進し、多種多様なサイバーセキュリティに関連した情報の大規模集約と横断分析を実現する分析・共有基盤の構築を目指す。

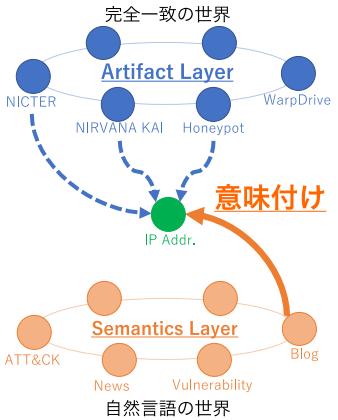
CURE システム概要

- ✓ 散在する多種多様な情報をインメモリデータベースに格納し高速分析
- ✓ Pub/Subモデルに基づくシステム実装で、柔軟なデータ融合を実現



CURE 自然言語処理機能

- ✓ 自然言語処理機能を加え、各種レポートやMITRE ATT&CKを融合



CURE 可視化エンジン

- ✓ ArtifactレイヤとSemanticレイヤに対応した2階層の可視化エンジン実装

暗号等の研究の推進（１／２）

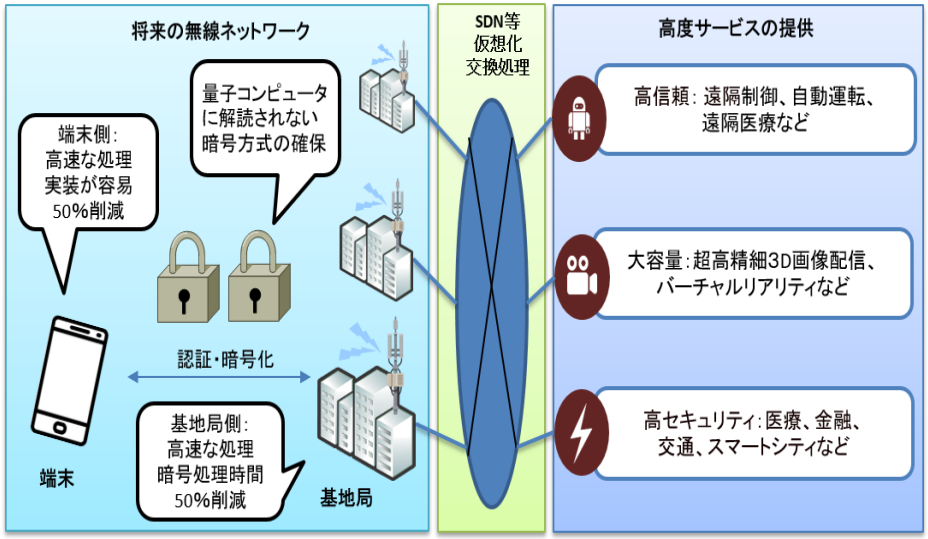
安全な無線通信サービスのための新世代暗号技術に関する研究開発

総④

５Ｇ等の無線通信において広く利用されている暗号技術については、近い将来に実用化される大規模量子コンピュータの計算処理能力にも計算困難性を有する対策が必要となることから、５Ｇ等が求める超高速・大容量の能力が損なわれず、かつ安心安全な通信を実現する新世代暗号技術に関する研究開発を実施する。

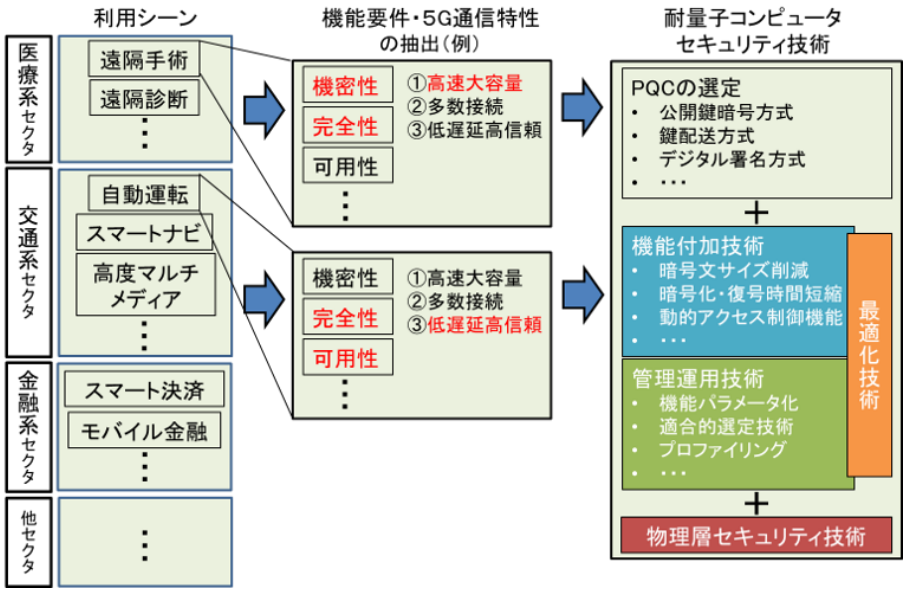
５Ｇ等のための超高速・大容量に対応した共通鍵暗号方式の研究開発（高速共通鍵暗号）

【実施内容】
現在の倍である256bitの鍵長に対応し、5G及びより高度な無線通信を想定して処理速度50Gbpsを実現する高速な共通鍵暗号方式を設計し、無線通信環境で実証・評価を行う。



５Ｇ等のための耐量子計算機暗号の機能付加技術等の研究開発（耐量子計算機暗号）

【実施内容】
PQCに機能を付加するに当たって、５Ｇ等の特性を損なわないよう、暗号文サイズの削減などの技術の開発が必要。さらに、各種サービスに応じて効果的な機能選択やパラメータ選択を可能とするシステム管理運用技術および最適化技術等が求められる。さらに、それらの技術を計算機リソースが限られた端末でも実現するため、５Ｇに適応した物理層セキュリティ技術開発を行う。

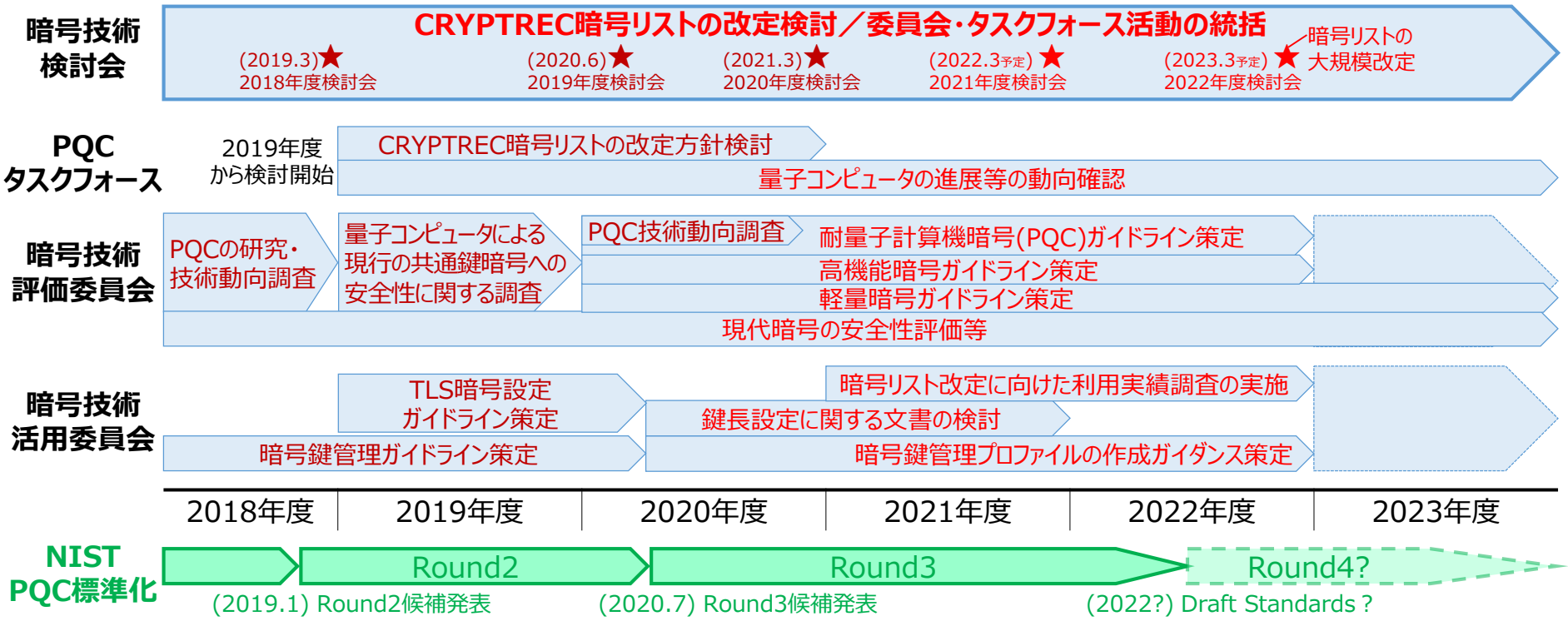


暗号等の研究の推進（2／2）

CRYPTRECについて

Cryptography Research and Evaluation Committees

- CRYPTRECは、電子政府推奨暗号の安全性を評価・監視し、暗号技術の適切な実装法・運用法を調査・検討するプロジェクト。総務省及び経済産業省が共同で運営する暗号技術検討会と、NICT及びIPAが共同で運営する暗号技術評価委員会及び暗号技術活用委員会とで構成される。（2019年度からタスクフォースについても開催）
- 2023年を目途とした**CRYPTREC暗号リストの改定**検討を行っているほか、**耐量子計算機暗号(PQC)・高機能暗号・軽量暗号に関するガイドライン**の策定や、暗号鍵の**鍵長設定に関する文書**等の検討を行っている。



先端技術・イノベーションの社会実装
～ サイバーセキュリティ統合知的・人材育成基盤の整備 ～

総⑤

➢ 我が国におけるサイバーセキュリティ対応能力の向上を目的として、**サイバーセキュリティ情報を国内で収集・蓄積・分析・提供**するとともに、**社会全体でサイバーセキュリティ人材を育成**するための**共通基盤「CYNEX*」をNICTに構築**し、**産学官の結節点として開放。**

*CYNEX（Cybersecurity Nexus：サイネックス）

➢ **国産セキュリティ情報の収集・蓄積・分析・提供**

➢ **セキュリティ機器テスト環境**

➢ **高度解析人材の育成**

➢ **人材育成のための基盤提供**

サイバーセキュリティに関する産学官の結節点『CYNEX』

- 情報通信研究機構（NICT）では、これまでも次のような取組を実施
  サイバーセキュリティ研究所・・・最先端のサイバーセキュリティ関連技術の研究開発を実施
  ナショナルサイバートレーニングセンター・・・実践的サイバー防御演習等による人材育成を実施
- これらの知見を活用し、サイバーセキュリティに関する産学官の巨大な結節点となる先端的基盤として
  ＣＹＮＥＸ（Cybersecurity Nexus：サイネックス） を構築

サイバーセキュリティ人材育成基盤に関する背景

● サイバーセキュリティ自給率の低迷

✓ サイバーセキュリティ戦略本部 研究開発戦略専門調査会（2019年5月17日）

● データ負けのスパイラル

✓ データが集まらない → 研究開発できない → 技術を作れない
→ 技術が普及しない → データが集まらない → …

● 今、日本に必要なこと

✓ 実データを**大規模に収集・蓄積**する仕組み
✓ 実データを**定常的・組織的に分析**する仕組み
✓ 実データで**国産製品を運用・検証**する仕組み
✓ 実データから**脅威情報を生成・共有**する仕組み

これらの仕組みの実現を目指す**産学官の結節点**

CYNEX を構築
Cybersecurity Nexus

サイバーセキュリティ統合知的・人材育成基盤の活動内容

大規模収集・蓄積

1. STARDUST等のセミオープン※化

- ✓ STARDUSTを産学に半開放し大規模並列解析
- ✓ 共同分析を通して国内解析者コミュニティを醸成

※セミオープン：信頼できるCYNEXの参画機関にSTARDUSTを開放

定常的・組織的分析

2. 高度SOC人材育成

- ✓ 産学官から高度解析者を集結
- ✓ 高度SOC人材育成プログラムによる教育

国産製品運用・検証

3. 実環境での国産製品の長期運用・検証

- ✓ 実ネットワークのデータ利用による検証環境
- ✓ 国産製品を長期運用・機能検証

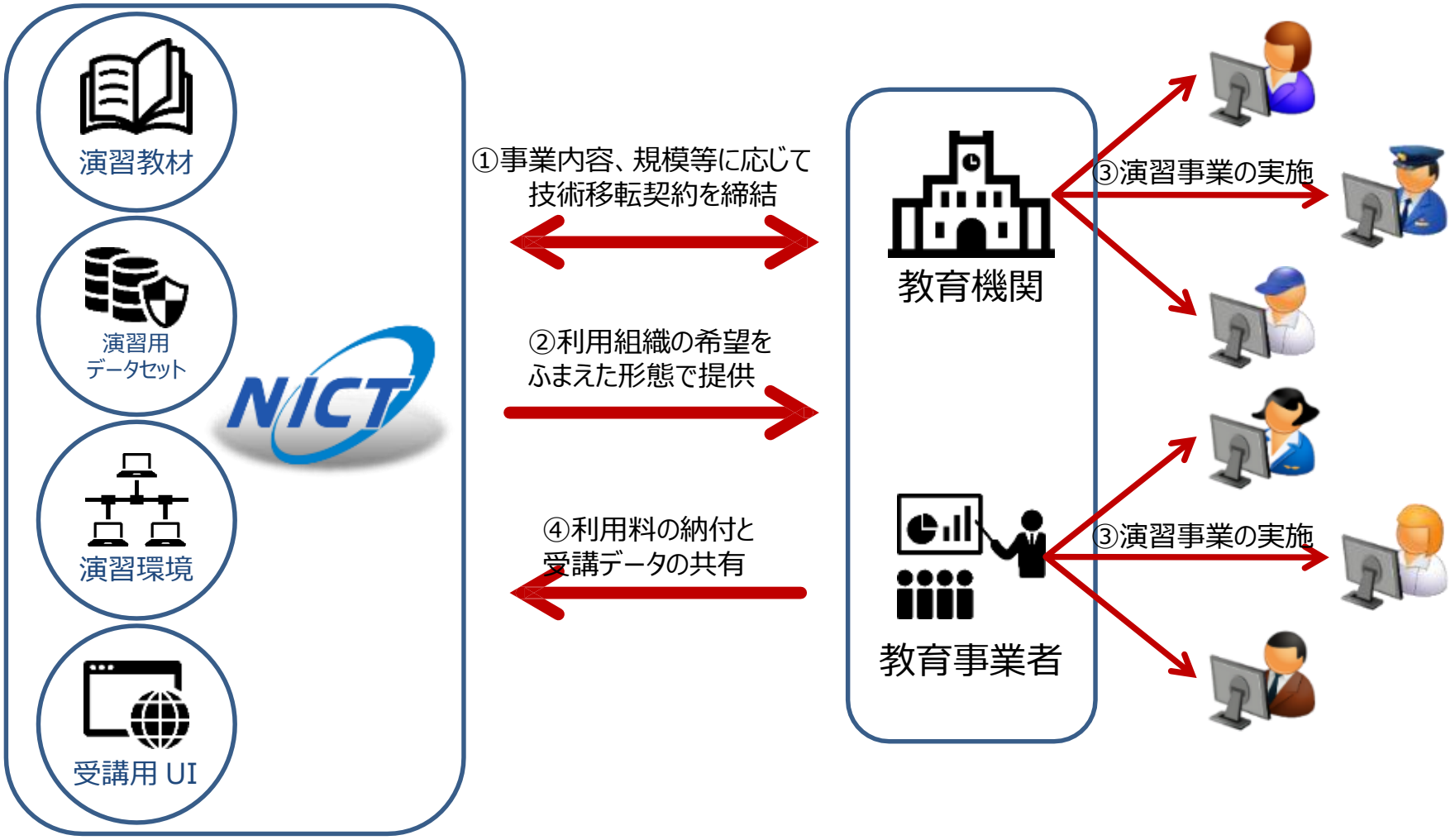
脅威情報生成・共有

4. 純国産サイバーセキュリティ情報の生成

- ✓ 各種データを機械学習等と高度解析者により統合分析
- ✓ 説明可能かつ即時的な純国産IoCを生成・発信

人材育成オープンプラットフォームのサービス提供イメージ

- 利用希望組織は、事業内容、事業希望等に応じて、プラットフォーム利用のための技術移転契約をNICTと締結
- NICT は利用組織の希望をふまえて、演習教材、演習用データセット、演習環境、受講用ユーザーイン ターフェース (UI) 等のすべて、または一部を提供



サイバーセキュリティ製品の海外展示会への出展支援について

総⑥

- 我が国国産セキュリティ製品のグローバル展開に向けては、技術海外のビジネスカンファレンス等への出展により、積極的に新規顧客や海外代理店を獲得していくことが考えられる。
- 他方、近年、セキュリティ関連のカンファレンスは出展希望者が多く、スペース確保の競争率が高くなり、出展費用も高額化。このため、国内のセキュリティ事業者個社では、適切な展示スペースを確保することが困難。
- 総務省では、こうした状況を踏まえ、2018年度より、サイバーセキュリティ製品についての世界最大のビジネスカンファレンスである米国「RSA Conference」への、我が国産業界による「Japan Pavilion」出展を継続的に支援sしているところ（NPO法人日本ネットワークセキュリティ協会（JNSA）受託調査研究）。
- 直近のRSA Conference 2020では商談件数248件、成立見込件数22件等の成果。過去の出展支援実績以下の通り:
  - ✓ 2018年度: RSA Conference 2019（2019年3月@サンフランシスコ）8社
  - ✓ 2019年度: RSA Conference 2020（2020年2月@サンフランシスコ）14社
  - ✓ 2020年度: RSA Conference 2021（2021年5月開催予定@オンライン）10社 ※COVID19のためオンライン開催

Japan Pavilion ブースデザイン

RSA Conference 2019

RSA Conference 2020

RSA Conference 2021（オンライン開催予定）

IoTセキュリティガイドラインの国際標準化

総⑦

- IoT推進コンソーシアム・総務省・経済産業省が公表した「IoTセキュリティガイドラインver1.0（2016年7月）」の国際標準化に向け、ITU-T及びISO/IECにおける議論を継続中。

IoT Acceleration Consortium

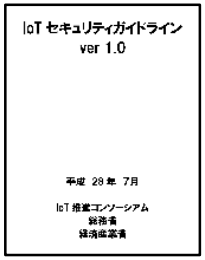
総務省　経済産業省

ITU-T及びISO/IECに対して
国際標準化に向けた検討を提案

ITU

ISO JTC1 IEC
INFORMATION TECHNOLOGY STANDARDS

〇2016年7月、IoT推進コンソーシアム・総務省・経済産業省により、「IoTセキュリティガイドラインver1.0」を公表



（主な標準化項目）
・IoTシステムのステークホルダー
・IoTシステムに係るリスク分析
・IoT機器のライフサイクル
・適切なセキュリティ管理手順　等

〇2018年4月以降継続的にISO/IEC JTC1 SC27において議論されていた、本ガイドラインをベースとしたIoTセキュリティ規格案（ISO/IEC 27400）が、国際規格原案として承認され、現在各国からの承認の投票受付中

〇2018年9月、ITU-T SG17において、本ガイドラインをベースとして、IoTシステムのためのセキュリティ管理策に関する文書が勧告草案（X.sc-IoT）として承認され、議論を継続中

令和3年度 戦略的創造研究推進事業の戦略目標
（Society 5.0時代の安心・安全・信頼を支える基盤ソフトウェア技術）

多様な情報システムや大量のデータを使いこなして、質の高い豊かで安心な生活を実現するSociety 5.0時代には、“データの漏えい・流出”や“なりすまし”、“プライバシーの侵害”等の多くの危険が存在

⇒ 情報基盤分野の研究者の力を結集し、日本発の基盤ソフトウェア技術で安心・安全・信頼を確保

なぜ、基盤ソフトウェア技術？

デジタル化への急速な流れ
- デジタル庁の創設
- コロナ新時代の新たなライフスタイルへの移行
- Society 5.0の早期実現

しかし、我が国は・・・

デジタル化のためのハードウェア、OS、クラウド等の大部分を海外に依存

→ リスク管理も海外依存となってしまってよいのか？？

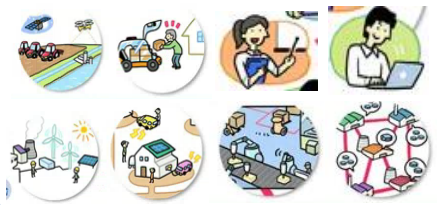
そこで、

情報基盤分野の研究力を再強化
- 研究コミュニティの再構築
- 理論とシステムの研究者の連携

＋

日本発の基盤ソフトウェア※で課題解決
- クラウド等の対策のみに頼らず、データや情報システムの安心・安全・信頼を確保

※基盤ソフトウェア＝アプリとクラウド等を繋ぐソフトウェア



Society 5.0

＝ **人々の多様な幸せの追求**

誰もが、安全・安心にデータを活用
多様な情報システムを信頼して利用

将来像

日本発次世代情報技術が世界で活用

次世代AI、高性能コンピューティング　等

データ

基盤ソフトウェア

安全	信頼できないハードウェアやOSを含む計算環境でも安全なシステムを構築できるセキュリティ技術
安心	オープンな環境でもプライバシーを確保するデータ収集・解析技術
信頼	データの自由な流通と個人情報の安全確保を両立するシステム実装技術

データ

基盤ソフトウェア技術の蓄積

情報基盤分野の研究者・研究力を結集
理論とシステムの融合

ハードウェア（センサ・デバイス等）・OS・クラウド等の対策のみでは、継続的な安全性・信頼性の確保は困難

戦略目標に基づく２つの研究領域

令和3年度戦略目標「Society 5.0時代の安心・安全・信頼を支える基盤ソフトウェア技術」に基づき、科学技術振興機構（JST）において、「CREST」と「さきがけ」の2つの研究領域を設定。

CREST

●研究期間　５年半
●研究費　総額1.5~5億円程度/課題

科学技術イノベーションにつながる卓越した成果を生み出すネットワーク型研究（チーム型）

基礎理論とシステム基盤技術の融合による Society 5.0のための基盤ソフトウェアの創出（略称：S5基盤ソフト）

研究総括：岡部　寿男　京都大学 学術情報メディアセンター　センター長・教授

【募集対象の技術領域】

（１）信頼できないハードウェアやOSを含む計算環境で安全なシステムを構築可能とするセキュリティ技術の創出

（２）オープンな環境でもプライバシーを確保するデータ収集・解析技術の創出

（３）データの自由な流通と個人情報の安全性確保を両立するシステム実装技術の確立

さきがけ PRESTO

●研究期間　３年半
●研究費　総額４千万円程度/課題

科学技術イノベーションの源泉を生み出すネットワーク型研究（個人型）

社会変革に向けたICT基盤強化（略称： ICT基盤強化）

研究総括：東野 輝夫　京都橘大学 工学部情報工学科 教授（工学部長）／大阪大学 大学院情報科学研究科　特任教授

【募集対象の技術領域】

（１）様々な計算環境で安全なシステムを構築するための技術の創出

（２）オープンな環境でもプライバシーを確保するデータ収集・解析技術の創出

（３）社会の安心・安全・信頼を支える新たなICT基盤の創出

ＡＩＰネットワークラボ

○科学技術振興機構（JST）の戦略的創造研究推進事業（競争的資金）を活用し、AIPネットワークラボ長のマネジメントの下、AIやビッグデータ等における若手研究者の独創的な発想や、新たなイノベーションを切り開く挑戦的な研究課題を支援

○進展が見込める課題は、研究期間終了後にも追加支援する等、研究者のニーズに合わせて柔軟に支援

AIPネットワークラボ長：江村 克己 NECフェロー

CREST

●研究期間　５年半
●研究費　総額1.5~5億円程度/課題

科学技術イノベーションにつながる卓越した成果を生み出すネットワーク型研究（チーム型）

知的情報処理	**萩田 紀博**（課題数：11）
人工知能	**栄藤　稔**（課題数：29）
共生インタラクション	**間瀬　健二**（課題数：16）
数理的情報活用基盤	**上田　修功**（課題数：9）
信頼されるAIシステム	**相澤　彰子**（課題数：5）
S5基盤ソフト ※令和３年度新規領域	**岡部　寿男**
バイオDX ※令和３年度新規領域	**岡田　康志**

さきがけ PRESTO

●研究期間　３年半
●研究費　総額４千万円程度/課題

科学技術イノベーションの源泉を生み出すネットワーク型研究（個人型）

社会デザイン	**黒橋　禎夫**（課題数：32）
人とインタラクション	**暦本　純一**（課題数：30）
数理構造活用	**坂上　貴之**（課題数：20）
IoT	**徳田 英幸**（課題数：20）
信頼されるAI	**有村 博紀**（課題数：11）
ICT基盤強化 ※令和３年度新規領域	**東野 輝夫**

ACT-I

●研究期間　１年半
●研究費　最大500万円/課題

ICT分野の若手研究者を支援する個人型研究

情報と未来	**後藤　真孝**（課題数：125）

「ACT-I」をベースに**若手研究者（大学院生を含む）を支援する挑戦的研究支援制度**を創設

ACT-X

●研究期間　2年半
●研究費　数百万円程度/課題

独創的・挑戦的なアイデアを持つ若手研究者を支援する個人型研究

数理・情報	**河原林　健一**（課題数：60）
AI活用で挑む学問の革新と創成	**國吉　康夫**（課題数：23）

（敬称略、課題数については令和３年４月現在の累積数）

上記のほか、令和２年度より「日独仏AI研究」で9課題を採択する等、国際連携についても推進

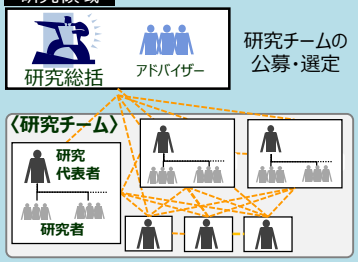
戦略的創造研究推進事業における主なプログラムの概要

○国が定めた戦略目標の下、組織・分野の枠を越えた時限的な研究体制（ネットワーク型研究所）を構築し、イノベーションの源泉となる基礎研究を戦略的に推進。

CREST

国が定める戦略目標の達成に向けて研究総括の運営の下、独創的で国際的に高い水準の目的基礎研究を推進。今後の科学技術イノベーションに大きく寄与する卓越した成果を創出することを目的とし、研究代表者が複数の共同研究グループを組織し実施するネットワーク型研究。

研究領域

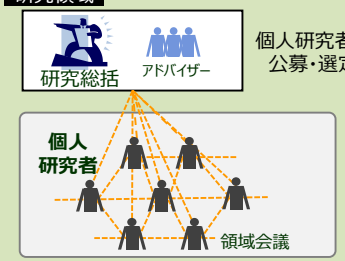


トップ研究者が率いる複数のチームが研究を推進(**チーム型**)
- 研究期間： 5 年半
- 研 究 費 ：1.5～5億円程度/チーム

さきがけ

国の科学技術政策や社会的・経済的ニーズを踏まえ、国が定めた戦略目標の達成に向けた独創的・挑戦的かつ国際的に高水準の発展が見込まれる先駆的な目的基礎研究を推進。科学技術イノベーションの源泉となる成果を世界に先駆けて創出することを目的とするネットワーク型研究（個人型）。

研究領域

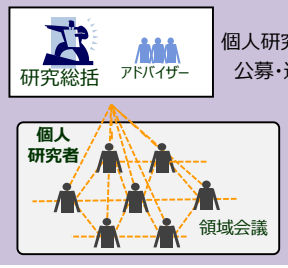


若手研究者が異分野ネットワークを形成し、挑戦的な研究を推進(**個人型**)
- 研究期間： 3 年半
- 研 究 費 ：3～4千万円程度/人

ACT-X

我が国が直面する重要な課題の克服に向けて、優れた若手研究者を発掘し育成することを目的とし、研究総括が定めた研究領域運営方針の下、独創的・挑戦的なアイデアをもつ研究者を見出し、科学技術イノベーションにつながる新しい価値の創造を目指した研究を行うことを支援。

研究領域



博士号取得後8年未満の研究者の「**個の確立**」を支援
- 研究期間: 2 年半
- 研 究 費：0.5～1.5千万円程度/人

※2019年度発足

ERATO

規模の大きな研究費をもとに既存の研究分野を超えた分野融合や新しいアプローチによって挑戦的な基礎研究を推進することで、今後の科学技術イノベーションの創出を先導する新しい科学技術の潮流の形成を促進し、戦略目標の達成に資する。

研究領域
(プロジェクト)

卓越したリーダーによる独創的な研究の推進・新分野の開拓(**総括実施型**)
- 研究期間： 5 年程度
- 研 究 費 ：上限12億円程度／1プロジェクト

産業サイバーセキュリティ研究会とWGの設置による検討体制

経①

産業サイバーセキュリティ研究会

第１回：平成29年12月27日　開催
第２回：平成30年　5月30日　開催
　アクションプラン（４つの柱）を提示
第３回：平成31年　4月19日　開催
　アクションプランを加速化する３つの指針を提示
第４回：令和2年　　4月17日　開催（電話開催）
　産業界へのメッセージを発信
第５回：令和2年　　6月30日　開催
　サイバーセキュリティ強化運動の展開
第６回：令和３年　　４月２日　開催
　アクションプランの持続的発展と、新たな課題へのチャレンジへ

※2021年4月開催時点

構成員

- 泉澤　清次　三菱重工業株式会社取締役社長
- 遠藤　信博　日本経済団体連合会サイバーセキュリティ委員長、日本電気株式会社取締役会長等
- 大林　剛郎　日本情報ｼｽﾃﾑ･ﾕｰｻﾞｰ協会会長、株式会社大林組代表取締役会長
- 櫻田　謙悟　経済同友会代表幹事、ＳＯＭＰＯホールディングスグループＣＥＯ取締役　代表執行役社長
- 篠原　弘道　日本電信電話株式会社取締役会長
- 中西　宏明　株式会社日立製作所取締役会長
- 船橋　洋一　アジア・パシフィック・イニシアティブ理事長
- 村井　純(座長)慶應義塾大学教授
- 渡辺　佳英　日本商工会議所特別顧問、大崎電気工業株式会社取締役会長

オブザーバー

NISC、警察庁、金融庁、総務省、外務省、文部科学省、厚生労働省、農林水産省、国土交通省、防衛省

WG１（制度･技術･標準化）

第１回　平成30年2月7日
第２回　平成30年3月29日
第３回　平成30年8月3日
第４回　平成30年12月25日
第５回　平成31年4月4日
第６回　令和2年3月（書面開催）
第７回　令和2年10月（書面開催）
第８回　令和3年３月15日

１．サプライチェーン強化パッケージ

WG２（経営･人材･国際）

第１回　平成30年3月16日
第２回　平成30年5月22日
第３回　平成30年11月9日
第４回　平成31年3月29日
第５回　令和2年1月15日
第６回　令和2年8月25日
第７回　令和3年2月18日

２．経営強化パッケージ
３．人材育成・活躍促進パッケージ

WG３（サイバーセキュリティビジネス化）

第１回　平成30年4月4日
第２回　平成30年8月9日
第３回　平成31年1月28日
第４回　令和元年8月2日
第５回　令和2年3月(書面開催)
第６回　令和3年3月10日

４．ビジネスエコシステム創造パッケージ

産業サイバーセキュリティの加速化指針

１．『グローバル』をリードする
２．『信頼の価値』を創出する~Proven in Japan~
３．『中小企業・地域』まで展開する

<三層構造と６つの構成要素>
サイバー・フィジカル一体型社会のセキュリティのためにCPSFで提示した新たなモデル

- CPSFでは、産業・社会の変化に伴うサイバー攻撃の脅威の増大に対し、リスク源を適切に捉え、検討すべきセキュリティ対策を漏れなく提示するための新たなモデル（**三層構造**と**６つの構成要素**）を提示。

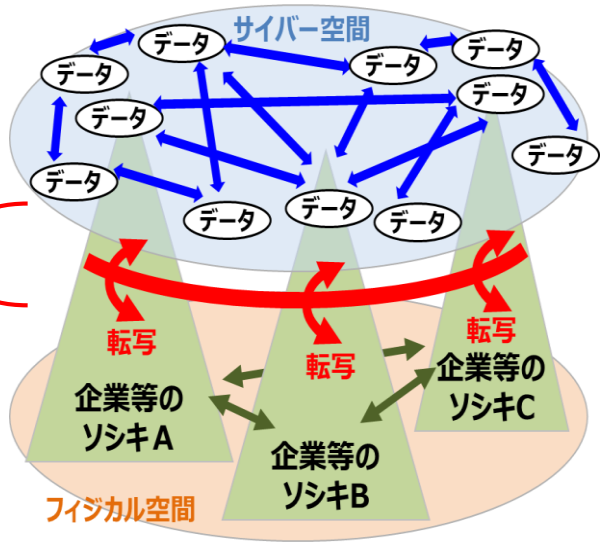
三層構造

「Society5.0」における**産業社会を３つの層に整理**し、セキュリティ確保のための信頼性の基点を明確化

サイバー空間におけるつながり
【第３層】
自由に流通し、加工・創造されるサービスを創造するための**データの信頼性**を確保

フィジカル空間とサイバー空間のつながり
【第２層】
フィジカル・サイバー間を正確に**“転写”する機能の信頼性**を確保
（現実をデータに転換するセンサーや電子信号を物理運動に転換するコントローラ等の信頼）

企業間のつながり
【第１層】
適切な**マネジメントを基盤に各主体の信頼性**を確保



６つの構成要素

対策を講じるための単位として、**サプライチェーンを構成する要素を６つに整理**

構成要素	定義
ソシキ	• バリュークリエイションプロセスに参加する企業・団体・組織
ヒト	• ソシキに属する人、及びバリュークリエイションプロセスに直接参加する人
モノ	• ハードウェア、ソフトウェア及びそれらの部品 操作する機器を含む
データ	• フィジカル空間にて収集された情報及び共有・分析・シミュレーションを通じて加工された情報
プロシージャ	• 定義された目的を達成するための一連の活動の手続き
システム	• 目的を実現するためにモノで構成される仕組み・インフラ

包括的なサイバーセキュリティ検証基盤を構築し、『Proven in Japan』を促進

経②

- 「**Proven in Japan**」では、2つの方向を追求し、**セキュリティビジネスの成長を促進**。

① 有効性確認等を通じ、日本発のサイバーセキュリティ製品のマーケット・インを促進

② IoT機器等の信頼性を高度に検証するハイレベル検証サービスの拡大

1．セキュリティ製品の有効性検証

ベンチャー等のセキュリティ製品

有効性検証

検証環境

2．実環境における試行検証

ベンチャー等

お試し製品提供と検証

実環境

民間事業者等のオフィス

3．攻撃型を含めたハイレベルな検証サービス

＜イメージ＞

様々なIoT機器・システム等

攻撃型検証等

検証サービス事業者

・情報保全の高信頼

信頼できるセキュリティ製品・サービス

世界に貢献する高水準・高信頼の検証サービス

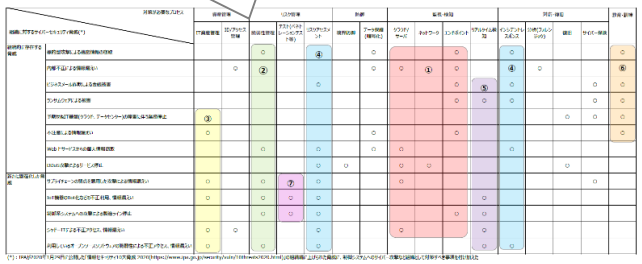
セキュリティ製品の有効性検証・実環境における試行検証実施

- 有識者会議を開催し、重要分野の選定、該当分野の製品の公募、検証作業を実施。
- 有効性検証、実環境における試行検証それぞれのアウトプットを取りまとめ、コラボレーション・プラットフォームで発表。

累計2,101DL
（2020/4/10～2021/3/31）

有識者会議でセキュリティ領域の全体マップを作成し、**重要分野**を選定（市場性、日本発の製品が強味を発揮可能か等の観点から）

① 脅威の可視化
② 脆弱性の可視化
③ IT資産管理
④ 脅威インテリジェンスの整理・管理
⑤ マルウェア感染/は省の重篤度判定
⑥ 教育・トレーニング
⑦ ハイレベルセキュリティ検証



重要分野に該当する**製品を公募で選定**
有効性評価、実環境における試行**評価を実施**

有効性検証 → **検証環境**

yamory
（OSSの脆弱性可視化）
VISIONAL

お試し製品提供と検証 → **実環境**

AX-Network Visualization
（ネットワーク脅威可視化）
AlaxalA

結果をIPAから公表した他、第13回コラボレーション・プラットフォーム（2020年9月）で発表、**ビジネスマッチング**を実施

日本発製品・サービスのプロモーションに資するため、主に以下の内容を公表

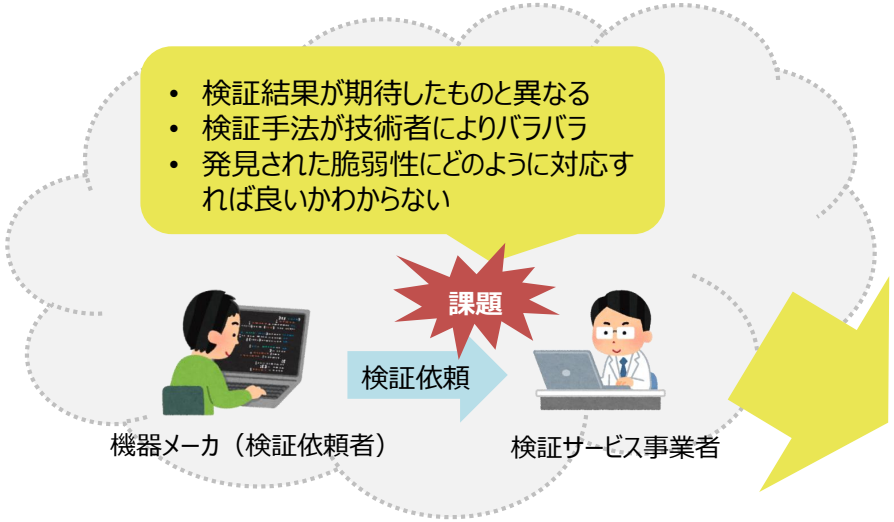
有効性検証結果
製品のストロングポイント

実環境における試行検証結果
『試行導入・導入実績公表の手引き』
- 公表のメリット／デメリット
- 公表可否判断のポイント
- 公表内容
- ステークホルダーとの調整 等

赤

攻撃型を含めたハイレベルな検証サービス

- 検証サービス事業者によるIoT機器等に対する攻撃的手法を含むハイレベルな検証を通じて、**検証サービス事業者及び検証依頼者それぞれが実施すべき事項や、二者間のコミュニケーションにおいて留意すべき事項等について整理した手引きを作成、2021年4月に公開。**手引きの活用を通じて、国内のセキュリティ検証サービスの検証サービス水準向上を目指す。



本編：機器のサイバーセキュリティ確保のための セキュリティ検証の手引き

- 検証サービス事業者が実施すべき事項
- 検証依頼者が実施すべき事項や用意すべき情報
- 二者間のコミュニケーションにおいて留意すべき事項　等

別冊3：検証人材の育成に向けた手引き

- 検証人材に求められるスキル・知識
- 検証人材のキャリアを構想・設計する上で考慮すべき観点　等

別冊1：脅威分析及びセキュリティ検証の詳細解説書

- 検証サービス事業者が実施すべき脅威分析の手法や実施すべき検証項目、検証の流れの詳細　等

脅威分析		
ファーム ウェア解析	バイナリ 解析	ネットワーク スキャン
既知脆弱性の 診断	ファジング	ネットワーク キャプチャ

検証初心者がスキルアップできる内容！

別冊2：機器メーカに向けた 脅威分析及びセキュリティ検証の解説書

- 機器メーカが実施すべき事項や用意すべき情報等、意図した検証を依頼するために必要な事項の詳細　等

開発における検証の位置づけ

知っておくべき脅威分析と検証手法

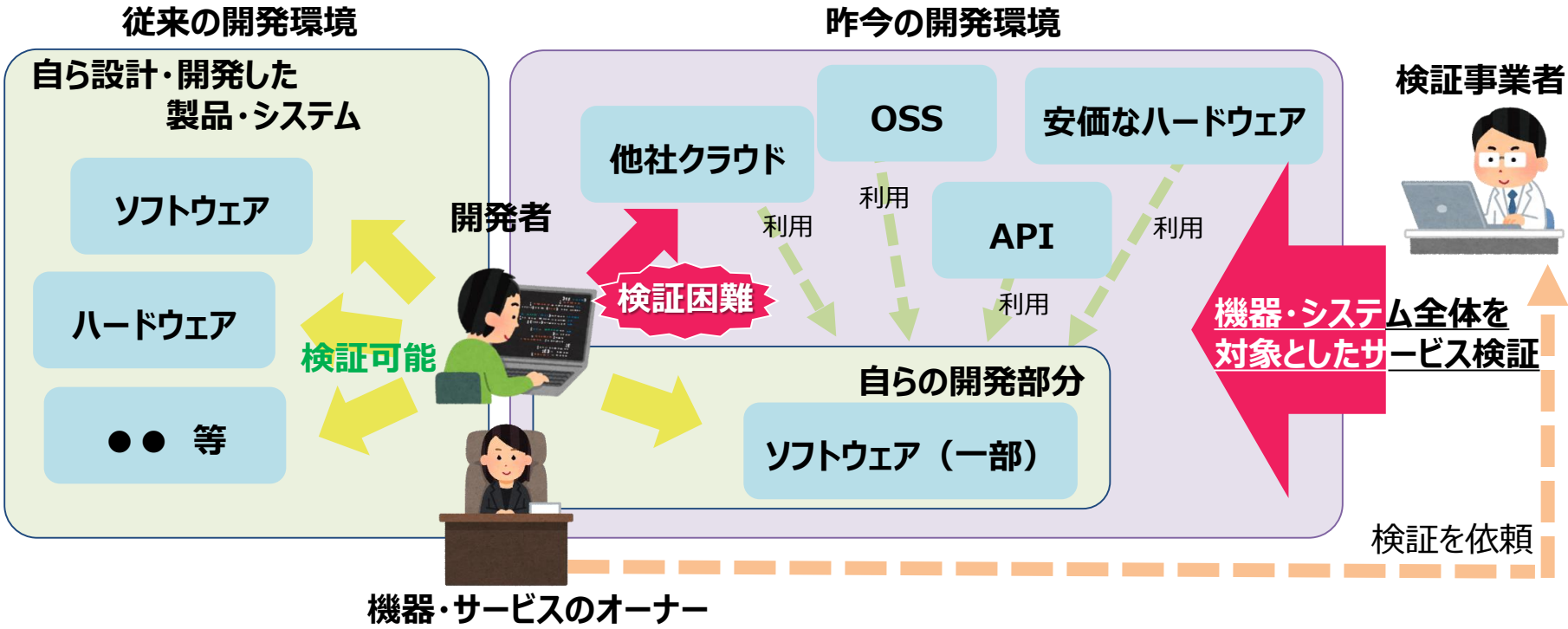
検証結果を踏まえた対応の検討

別冊１の検証手法に対応

https://www.meti.go.jp/press/2021/04/20210419003/20210419003.html

「開発のための投資」から「検証のための投資」へのシフト

- 近年では**クラウドやIoTなどの新しい技術の活用が進み、またオープンAPIやOSSが充実したことで、必要な“機能”を容易に調達してシステム構築できる環境**になっており、**開発者自身がシステム全体を把握・検証することが困難**になりつつある。
- こうした環境の変化で、**官民において第三者によるセキュリティ検証の必要性が増大**し、**検証ビジネスの需要が拡大し、産業として重要になっていく**と考えられる。



情報セキュリティサービス審査登録制度の概要

経③

- **一定の技術・品質管理要件を定めた「情報セキュリティサービス基準」**を策定し、基準に適合するサービスのリストを2018年6月よりIPAが公開。

＜情報セキュリティサービスにおける課題＞

どの事業者のサービスを選べば良いか分からない

信頼できるサービス事業者にお願いしたい

ユーザ
（企業、政府機関等）

選定時に活用

我が社のサービスをもっと見つけて欲しい

我が社の技術力、サービス品質をアピールしたい

ベンダー
サービス提供事業者

審査を受けてリストに掲載

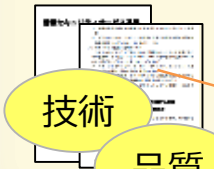
○情報セキュリティサービス基準適合サービスリスト（IPA）

審査登録機関による審査で基準を満たすと認められたサービスをリストとして公開

基準を満たした234サービスが掲載

- 情報セキュリティ監査（64サービス）
- 脆弱性診断（96サービス）
- デジタルフォレンジック（30サービス）
- セキュリティ監視・運用（44サービス）

2021年３月現在



○情報セキュリティサービス基準（METI）

上記４サービスに関して技術要件・品質管理要件を定めた基準

本制度を通じて目指す社会

専門的知識を持たないユーザでも、自社に最適かつ品質を備えたサービスを選択できる

技術と品質を備えた情報セキュリティサービスの普及・発展

制度の普及・浸透

（参考）登録サービス事業者の所在地の内訳

- **情報セキュリティ監査**（64サービス）　東京49、神奈川6、埼玉2、兵庫2、千葉1、新潟1、京都1、大阪1、広島1
- **脆弱性診断**（96サービス）　東京75、神奈川7、大阪3、兵庫3、新潟2、宮城1、茨城1、千葉1、大分1、福岡1、沖縄1
- **デジタルフォレンジック**（30サービス）　東京25、神奈川3、兵庫1、熊本1
- **セキュリティ監視・運用**（44サービス）　東京34、神奈川6、大阪1、兵庫1、福岡1、大分1

2020年度に実施したアンケート・ヒアリング結果のまとめ

制度の更なる改善を図るため、ユーザ・ベンダ双方への**本制度の活用状況・ニーズ調査**を実施した。

＜制度の認知度・効果＞

- ユーザー企業の半数超が本制度を認知。
- 登録メリットを感じる事業者が存在するほか、登録サービスの利用者による品質評価で「期待未満」が皆無であるなど、制度の目的が満たされていることが観察される。

＜セキュリティサービスの利用動向＞

- **ユーザー企業の約３割がセキュリティサービスを外部に委託**している実態。
- 外部委託における課題として、多くの企業が「サービスが自社の求めている条件を満たしているかどうかの判断ができない」「サービス品質が適切かどうか、使ってみるまで判断できない」と回答。

＜制度において改善すべき事項＞

- ユーザー企業からは登録サービス数の増加を求める意見が最多であるほか、**基準適合サービスリストの改善を求める声**（条件に見合った検索が出来るようリストの記載項目をもっと充実させて欲しい等）があった。
- **地域のベンダーはもっと存在しているはずなのに、登録数としては少ない**印象を受ける。

＜セキュリティサービスの普及方策への期待＞

- ベンダーの自己負担で営業活動で認知向上に取り組むには限界があり、**本制度の普及を通じてユーザーへの認知度向上を期待**する意見あり。

※ 全国のユーザー企業でサイバーセキュリティ対策関連業務に従事している方411名を対象にアンケート調査を実施。ユーザー（企業や自治体）、セキュリティサービスベンダー各15社程度を対象にヒアリング調査を実施。

内①

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

実施期間：平成30年度～令和4年度（2018年度～2022年度）
令和3年度予算：19.8億円（H30FY：25.0億円、H31FY：22.0億円、R2FY:22.0億円）

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）

目指す姿

概要

セキュアな Society 5.0 の実現に向け，様々なIoT機器を守り社会全体の安全・安心を確立するため，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*1全体を守ることに活用できる『サイバー・フィジカル・セキュリティ対策基盤』の開発と実証を行う。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を有する製造・流通・ビル等の各産業分野への社会実装を推進する*2 。

*1: 自動車産業の延べサプライヤー数は100万社超（2012年）

*2:「未来投資戦略 2017」閣議決定（2017年6月）

目標

スマート家電等の一般消費者向けの機器から産業用システムまで，多様なIoT機器・システム・サービスのセキュリティを確保できる『サイバー・フィジカル・セキュリティ対策基盤』を確立する。実証を通じて有効性を確認し，実稼働するサプライチェーンに組み込み実用化する。本基盤の社会実装を他国に先駆けて推進することで，サイバー脅威に対するIoT社会の強靭化を図り，我が国のセキュアなSociety5.0実現に寄与する。

出口戦略

当初から課題認識のある製造・流通・ビル等のユーザ企業と連携した研究開発と実証実験を進め，参画企業が主体的に製品化・事業化。欧米の基準とすり合わせながら府省による制度整備と連携してIoTシステム・サービスやサプライチェーンへの導入を促進し，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%に成果の導入を目指す。

社会経済インパクト

IoT社会の強靭化（サイバー犯罪による経済損失回避）により，Society5.0の実現がもたらす約90兆円の価値創出を支える。さらにグローバルなサプライチェーンに参画する要件*3となるセキュリティ確保を適切なコストで実現することにより，日本の製品・サービスの国際競争力を強化（輸出主体の製造業の参入機会の確保）する。

*3: 米国のNIST SP800-171や，欧州のサイバーセキュリティ認証フレームワーク等の動き

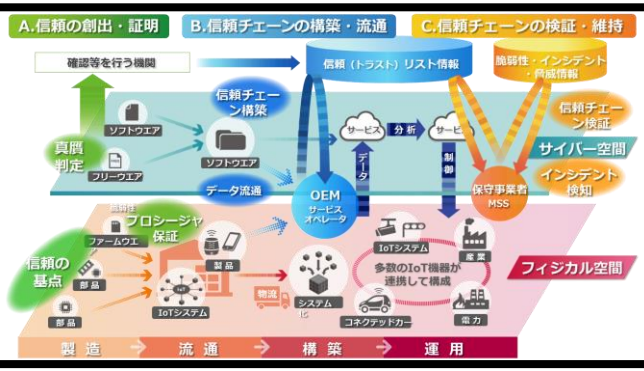
達成に向けて

研究開発内容

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ため，

A. 信頼の創出・証明　（IoT機器向け真贋判定技術 等）
B. 信頼チェーンの構築・流通　（トラストリストを用いた信頼チェーン構築技術 等）
C. 信頼チェーンの検証・維持　（インシデントの検知・解析・対処など信頼チェーンの維持技術　等）

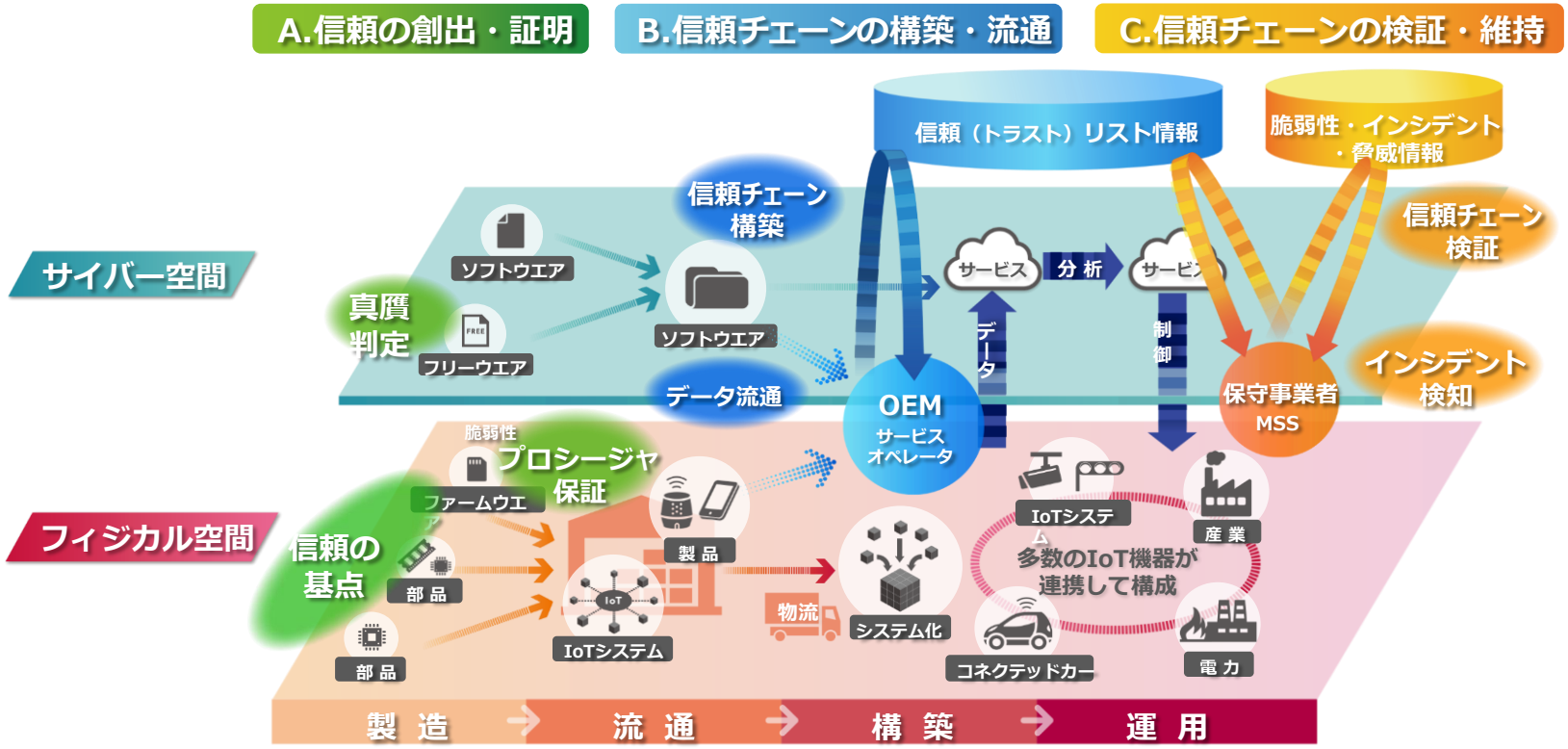
及び，その他，必要な研究開発・動向調査を行い，実サービスや各産業分野において実証を行う。



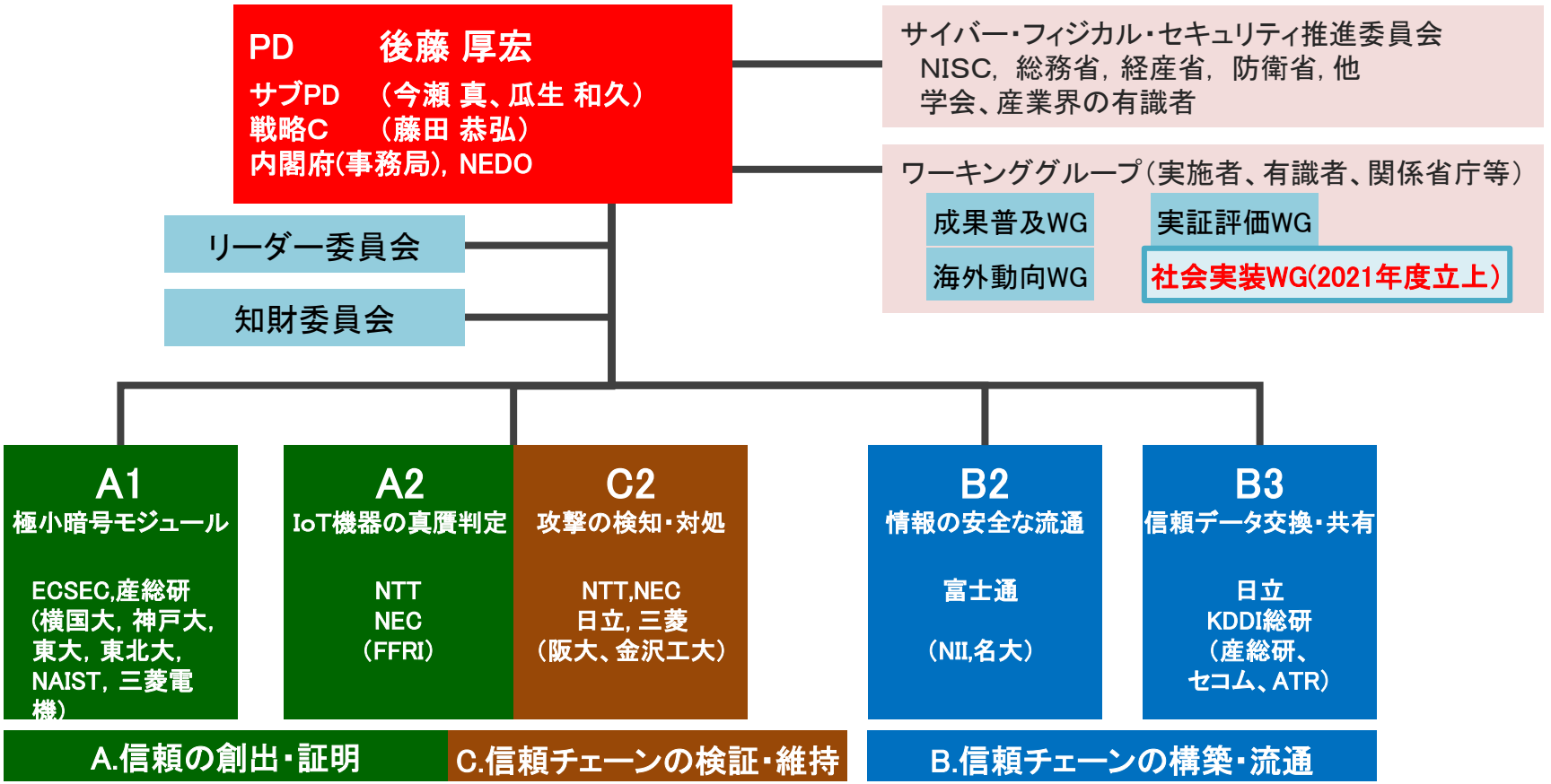
関係府省：総務省，経済産業省，NISC，IT室，警察庁，防衛省，厚生労働省

研究開発内容：信頼チェーンによるIoTサプライチェーンのセキュリティ確保

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



課題推進体制（2021年～2022年度）



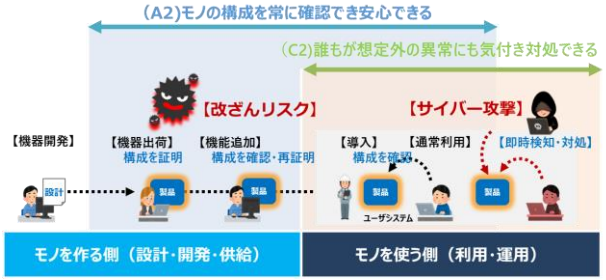
研究テーマ の取組状況

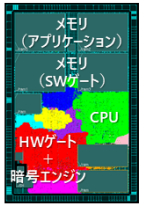
本モデルシステムとして、コネクタシステムを設定し、SCU搭載ICチップ設計・試作(SC01)を完了。

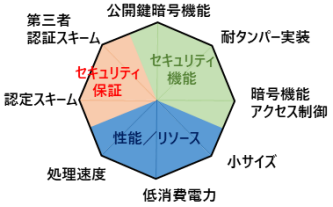
世界トップレベルの性能要件を満たす。

信頼の基点となる暗号モジュール

(A1) IoTサプライチェーンの信頼の創出技術〔ECSEC, 産総研 他〕







サプライチェーン全体のIoTリスクを抜本的低減

(A2) IoT機器等向け真贋判定による信頼の証明技術〔NTT, NEC 他〕

(C2) 信頼チェーンの異常検知・復旧支援技術〔NTT, 三菱, 日立, NEC 他〕

(A2) 真贋判定技術(軽量＆実時間)、(C2) 高度な異常検知技術のプロトタイプを開発し、**世界トップレベルの性能を確認。**

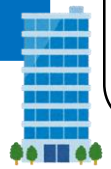
FAとBAを対象とした中小事業者支援を含む社会実装モデルを提示。

(B2) 信用できる場のコア技術(精選接続技術)を開発。

サプライチェーン全体の信頼性確保

(B2) 自治体と事業者間の信頼チェーン構築と安全な情報流通技術〔富士通 他〕

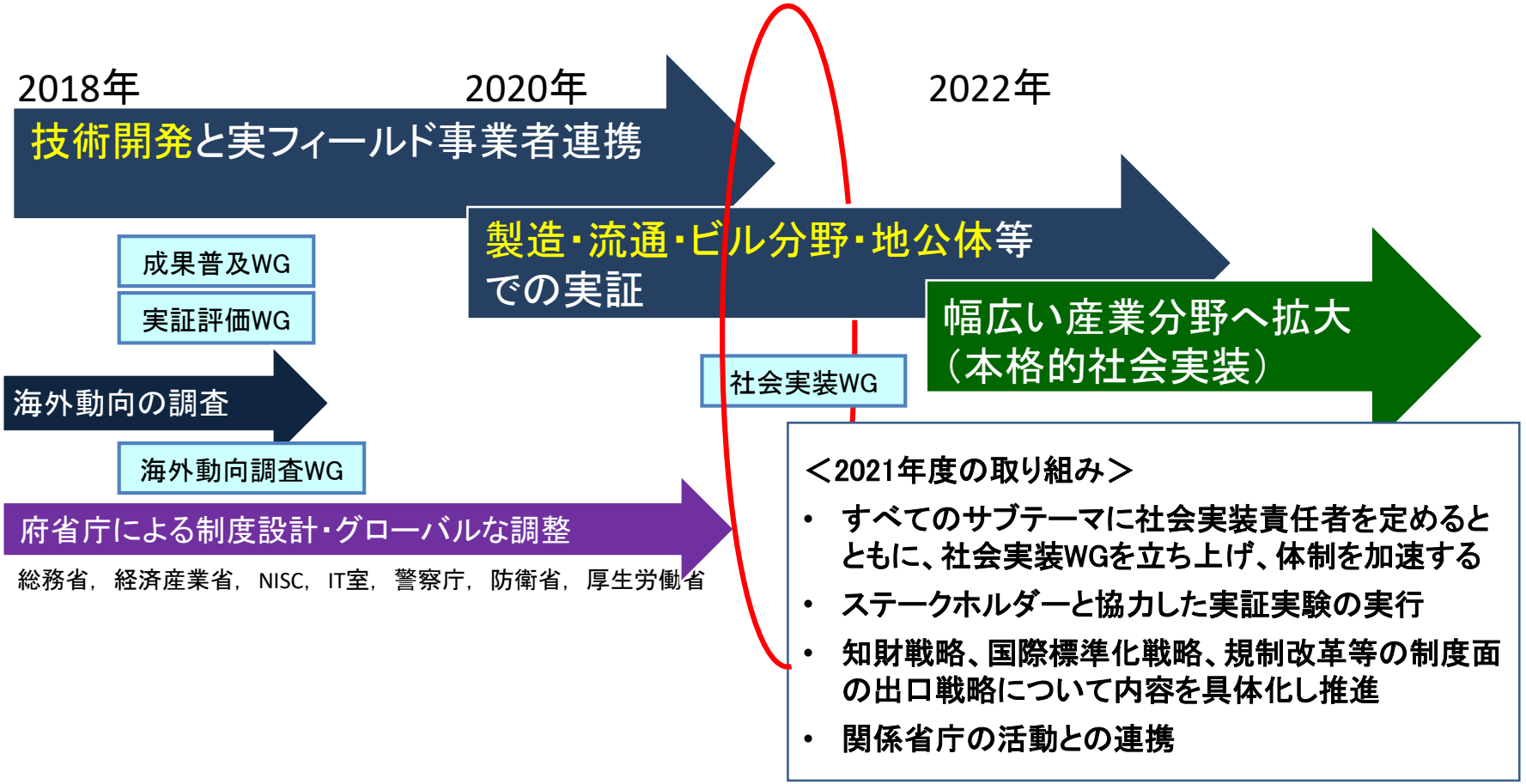
(B3) サプライチェーン全体の信頼性確保に向けた信頼データ交換・共有技術〔日立, KDDI他〕



(B3)経産省のCPSFの実現技術として、プロシージャ/ヒト/データの適合性検証技術を開発した。また、トラストストアプロトタイプの基本機能開発完了し、**基本性能の達成を確認した。**

製造(海外のシェア工場)、ビル(感染対策の可視化サービス)において実証実験を開始した。

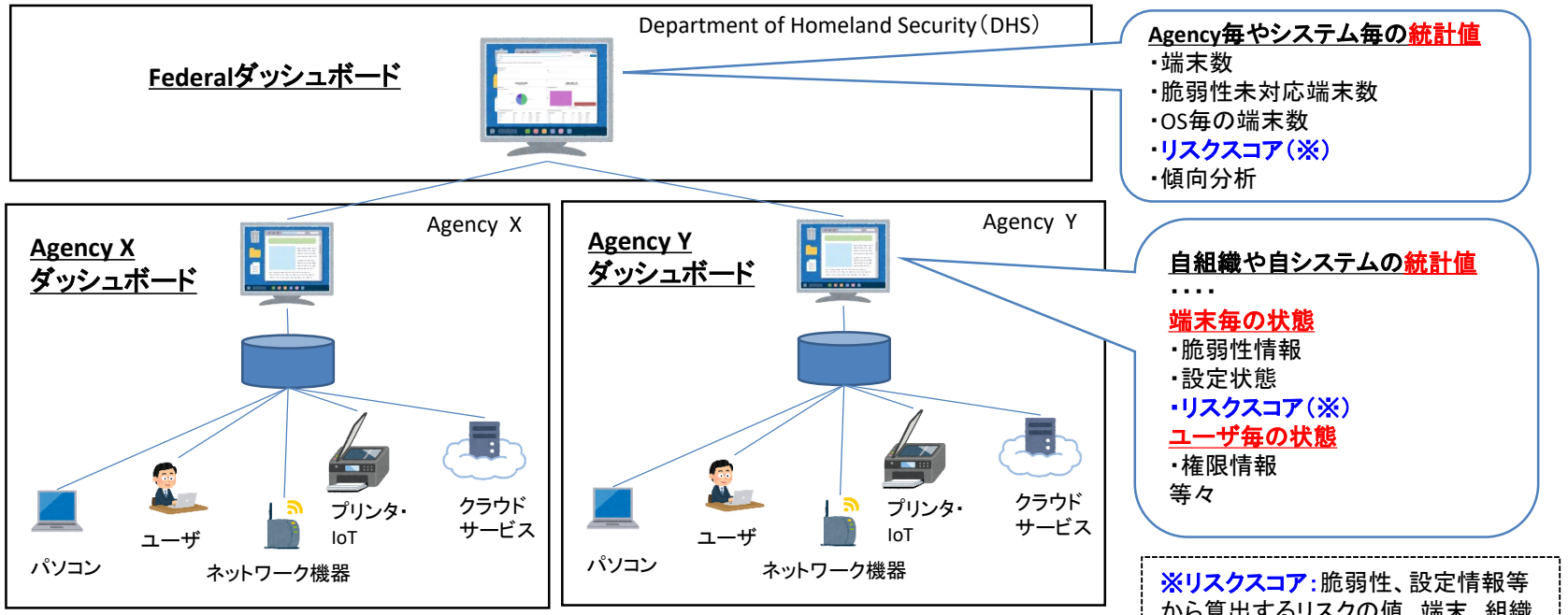
進捗状況と社会実装に向けた計画



資産管理等の強化のための研究開発　～米国におけるCDMプログラムの事例～

IT室①

- CDM　：　Continuous Diagnostics and Mitigation
- 位置づけ　：　府省の情報システムに関する**管理状況をほぼリアルタイムに報告**及び**リスクの対応の強化**する仕組み。
- 対象範囲　：　主に**資産管理**、**ユーザ管理**。ネットワークセキュリティ管理、データ保護管理は、現在、構築中。



Agency毎やシステム毎の統計値
・端末数
・脆弱性未対応端末数
・OS毎の端末数
・**リスクスコア（※）**
・傾向分析

自組織や自システムの統計値
・・・・
端末毎の状態
・脆弱性情報
・設定状態
・**リスクスコア（※）**
ユーザ毎の状態
・権限情報
等々

※リスクスコア：脆弱性、設定情報等から算出するリスクの値。端末、組織、システム毎に計算される。

管理対象

資産管理	ハードウェア、ソフトウェア、構成、脆弱性、モバイルの状況
ユーザ管理	ユーザ、アクセス権、教育、特権の状況
ネットワークセキュリティ管理	セキュリティイベント、運用、監視の状況
データ保護管理	データ保護、漏洩防止、権限制御等の状況