戦略的イノベーション創造プログラム（SIP）

重要インフラ等におけるサイバーセキュリティの確保

研究開発のねらい

国民生活及び社会経済活動を支える重要インフラ等へのサイバー攻撃の脅威に対し、強固なサイバーセキュリティを確保することにより、世界で最も安心・安全な社会基盤を確立する。

研究開発の背景

◆ 重要インフラ等の制御ネットワークシステムに対するサイバー攻撃の脅威が顕在化
ウクライナでは140万世帯が停電／復旧まで6時間

◆ 2020年オリパラでは重要インフラが最大の標的

制御ネットワークシステムの特徴

◆ サービス継続性重視
機密性よりも可用性、完全性を重視
セキュリティパッチ等の適用は最小限

◆ 数十年単位のライフサイクル
導入年代の異なる新旧機器が混在

制御ネットワークシステムを取り巻く状況

◆情報系ネットワークと同等のリスクの高まり
・多様なルートでの情報系ネットワークとの接続
・オフラインでの情報のやりとり
・オープン化の流れ（汎用製品、標準プロトコルの採用）

◆ 効果的な対策が存在しない既存のリスク
・製造～構築時（サプライチェーンリスク）や保守・運用時、内部犯行等による機器／ソフトウェアのすり替え

◆ 技術トレンドへの追随
・爆発的な数の（非力な）IoT機器の接続
・仮想化技術の採用

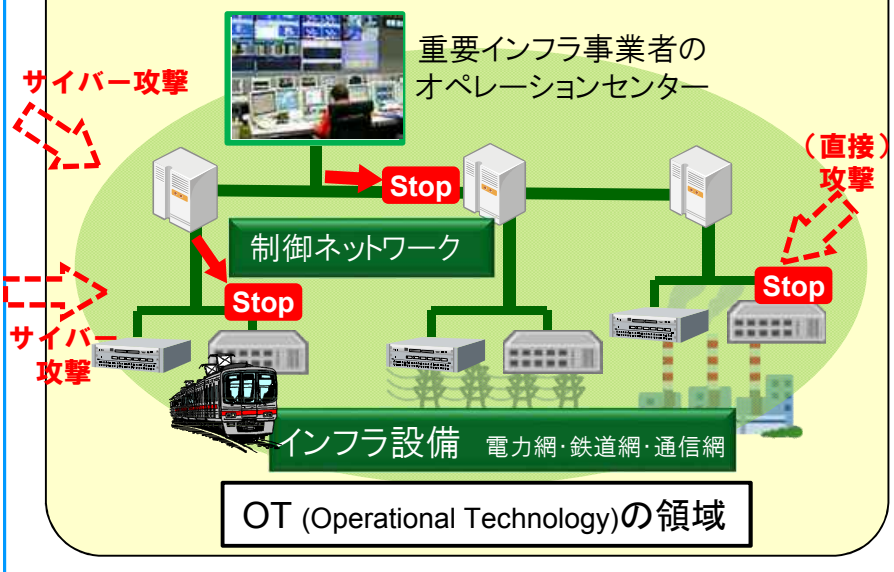
◆ サイバー攻撃の高度化・巧妙化
・重要インフラ事業者間・分野間の情報共有
・重要インフラにおいてサイバーセキュリティのスキル・知識を併せもった運用人材育成

SIPにおける取組

重要インフラ設備の特性：長寿命、新旧設備混在、大規模・広域に即した対策

免疫力　設備内部のセキュリティ耐性を高める技術

組織力　免疫技術を自ら運用できる人材、体制等



コア技術

「システムの免疫力」の向上
- 真贋判定技術
- 動作監視解析/防御技術
- IoT向け暗号実装技術

社会実装技術

「組織対応能力」向上
- 情報共有基盤
- セキュリティ人材育成
- 適合性確認

戦略的イノベーション創造プログラム（SIP）

重要インフラ等におけるサイバーセキュリティの確保

SIPにおける取組

1. 制御ネットワークシステムのセキュリティ（免疫力）強化

真贋判定技術	1-1 サーバ機器の改変を常時検知して重要インフラを保護 － システムの不正な改変を常時検知して、バックドア通信などの異常な動作を阻止します	NTT
動作監視解析/防御技術	1-2 内在する脅威の早期顕在化にて業務影響を最少化 －既存のセキュリティ対策をすり抜けた内在する脅威をいち早く顕在化させ、脅威を監視・分析する高スキル業務を支援	富士通
	1-3 侵入・攻撃の早期検知による制御システムのセキュリティ耐性強化 － 可用性が重視される制御システムにおいて気づきが難しい不正な動作を検知します	日立製作所
	1-4 異常検知時においても安全な運用継続を可能とするシステム防御技術 － 検知しづらい高度な攻撃から制御システム全体を保護して安全な運転を継続します	アラクサラ CSSC

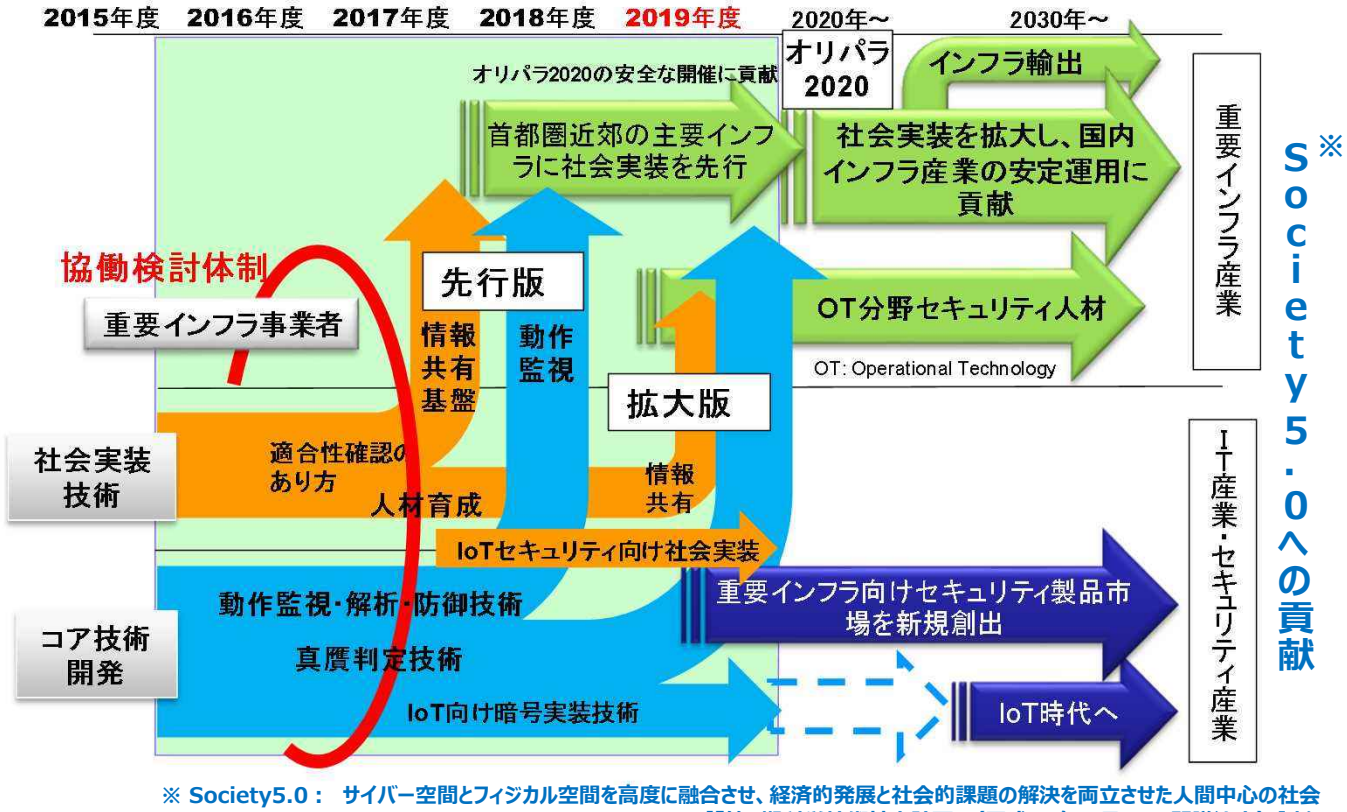
2. IoTシステムの普及拡大に先行したセキュリティ対策技術

IoT向け対策技術	2-1 モニタリング機器の追加でIoTセキュリティ監視を提供 － 多様なIoT機器に自動適応して動作を監視・解析し、セキュリティ異常を検知します	三菱電機 NTT
	2-2 IoTのセキュリティを実現する超低電力公開鍵暗号実装技術 － どこでも公開鍵暗号を！Secure Cryptographic Unit	ECSEC ルネサス
	2-3 「防御」「検知」「対策」でエンドポイントを守るトータルサイバーセキュリティ －安全な暗号・認証機能を実現／IoT機器のログ監視でサイバー攻撃を早期に発見	パナソニック

3. 重要インフラのセキュリティを確保する組織力強化と仕組みづくり

社会実装技術	3-1 研究開発技術の社会実装を促す適合性確認のあり方の研究開発 －従来になく有効で速やかに社会実装可能な適合性確認のあり方と仕組みの検討	産総研
	3-2 緊急度の高い脅威情報を迅速に配信し重要インフラ事業者を防御 － 脅威情報を機械処理可能な定型フォーマットとし迅速に配信、重要インフラ事業者のより早い防御を実現	日立製作所
	3-3 重要インフラでの実践力を養うセキュリティ人材育成プログラムの展開 3-4 組織のインシデント対応能力向上を目指す人材育成プログラム	慶應大 名工大

展開スケジュール



※ Society5.0： サイバー空間とフィジカル空間を高度に融合させ、経済的発展と社会的課題の解決を両立させた人間中心の社会
【「第5期科学技術基本計画」（平成28年１月22日閣議決定）】より