重要インフラ等における サイバーセキュリティの確保

プログラムディレクター

後藤　厚宏

サイバー攻撃のターゲットは重要インフラへ

【事例1】ウクライナ西部でサイバー攻撃による大規模停電（2015年12月）

- サイバー攻撃によって大規模な停電に至った初めての事例
- ウクライナの西部の都市イヴァーノ＝フランキーウシクで140万世帯の停電、復旧までに約6時間を要する
- 標的型メールによる攻撃が原因とされる

ウクライナのニュース番組で報道(2015年12月24日)
http://ru.tsn.ua/ukrayina/iz-za-hakerskoy-ataki-obestochilo-polovinu-ivano-frankovskoy-oblasti-550406.html

【事例2】産業制御系マルウェアCrashOverrideの脅威報告（2017年6月発表）

JVNTA#99970831:電力、運輸管理、水道等の産業系プロトコルが標的。制御システムに対する運用妨害や、情報漏洩などを生じさせ、大きな損害を招くおそれ。

【事例3】欧州鉄道保護システムに脆弱性（2016年1月発表）

列車の競合進路を防止する鉄道保護システムの脆弱性

【事例4】イラン核施設・原子力発電所へのサイバー攻撃（2010年）

Windowsの未知の脆弱性を利用 (Stuxnet)

重要インフラの制御ネットワーク

インフラ事業の競争力確保のために制御ネットワークによるインフラ設備の遠隔制御が必須な時代（効率性・保守性・最適制御　等）

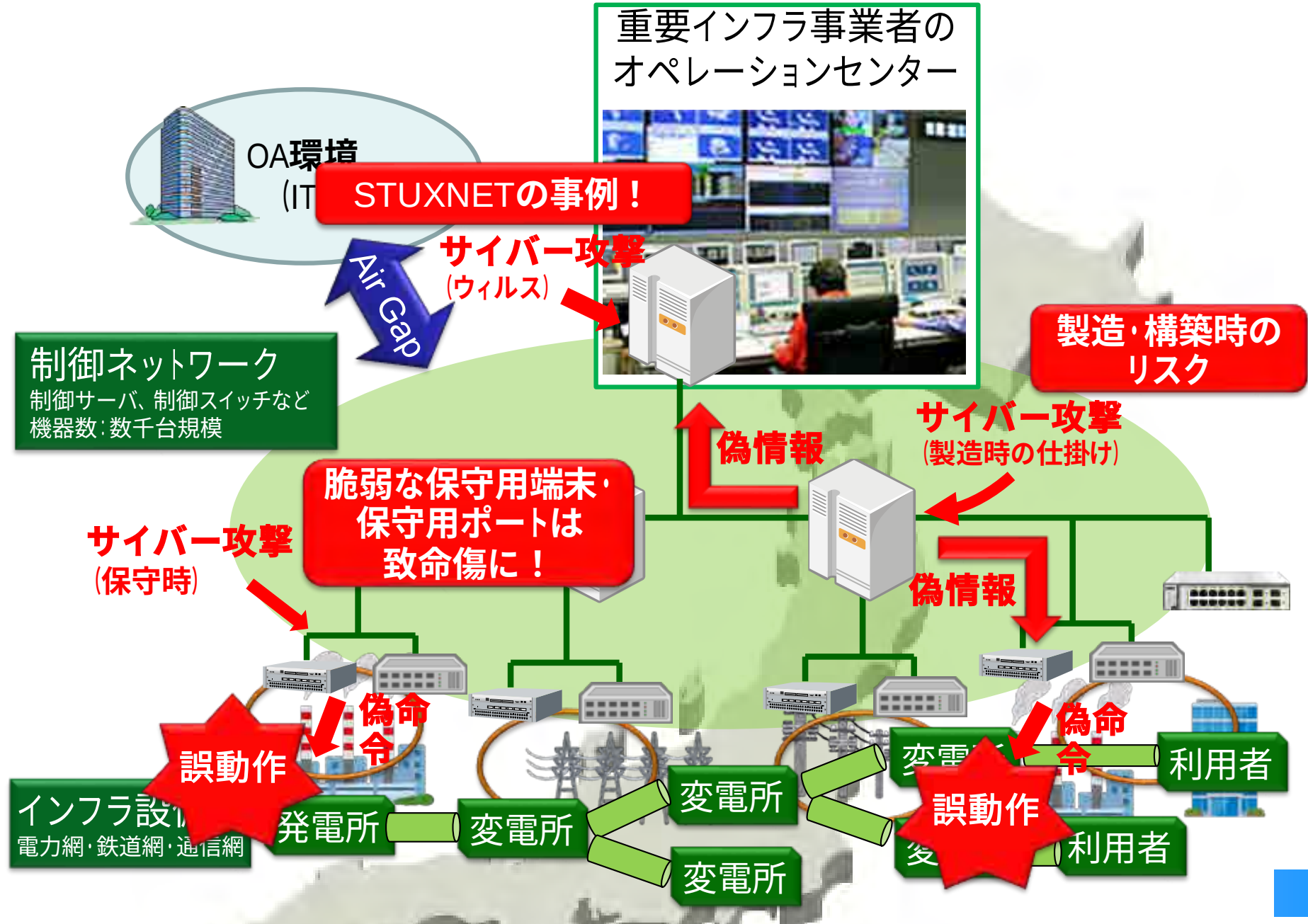
重要インフラ事業者のオペレーションセンター

制御ネットワーク
制御サーバ、制御スイッチなど
機器数：数千台規模

インフラ設備
電力網・鉄道網・通信網

発電所
変電所
変電所
変電所
変電所
変電所
利用者
利用者

サイバー攻撃リスクの高まり



内閣府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」
狙いと特徴

- 狙い
  - オリパラ2020の安全な開催への貢献
  - 国内インフラの安定運用、インフラ輸出への貢献
- 特徴
  - コア技術＋社会実装技術
  - 重要インフラ事業者との協働検討体制
  - 免疫力と組織力

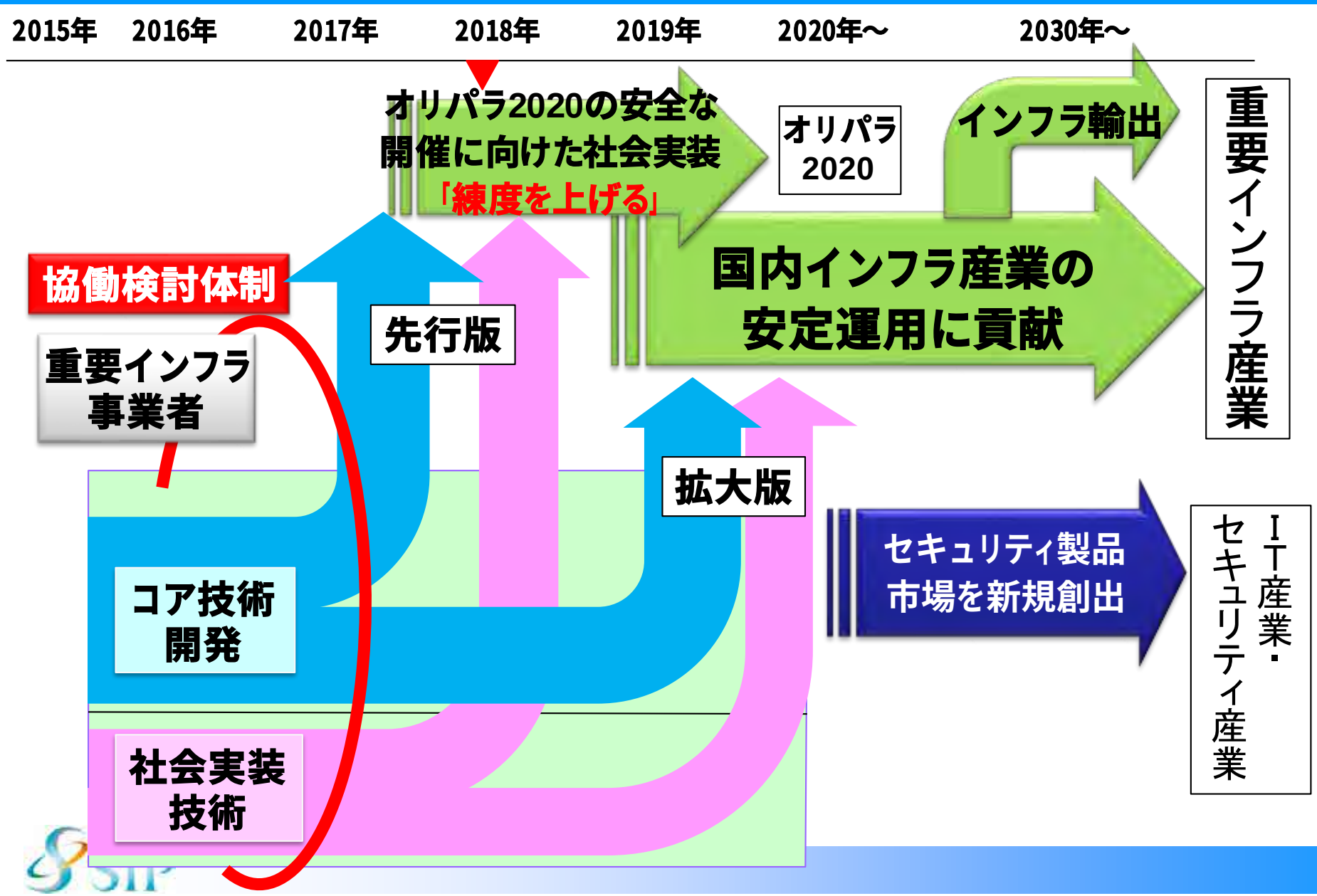
コア技術

「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 他

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 他

内閣府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」展開計画



内閣府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」
免疫力 と 組織力

グローバル技術を活用

重要インフラ事業者の主体的な取組み

「砦・鎧」技術

- アンチウィルス
- ファイアウォール
等

「免疫」技術

- 真贋判定
- 動作監視解析防御
- IoT向けセキュリティ

「組織力」

人材育成

攻撃者

閲覧・
一次感染

侵入

未知の脆弱性

Stop

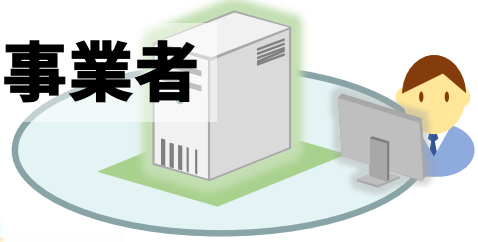
攻撃

未知の脆弱性

Stop

重要インフラ事業者の設備

他事業者



情報共有

内閣府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」研究開発の取り組み一覧

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

- 構築・運用時の改変を検知して異常動作を阻止
- 脅威の侵入を前提とし業務継続のための対策を支援
- 新旧機器混在下でのセキュリティ耐性を強化
- 異常検知時においても安全な運用継続を実現

2. 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

- セキュリティ技術の普及を促進する標準・ガイドラインと運用策
- 脅威情報を共有する基盤を整備し組織としての対応力を強化
- 重要インフラの現場力を強化するセキュリティ人材育成

3. 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

- 多様なIoT機器に自動応答してサイバー攻撃を検知
- IoTのセキュリティを実現する超低電力暗号実装技術
- IoT機器における安全な暗号鍵生成のための乱数生成評価技術

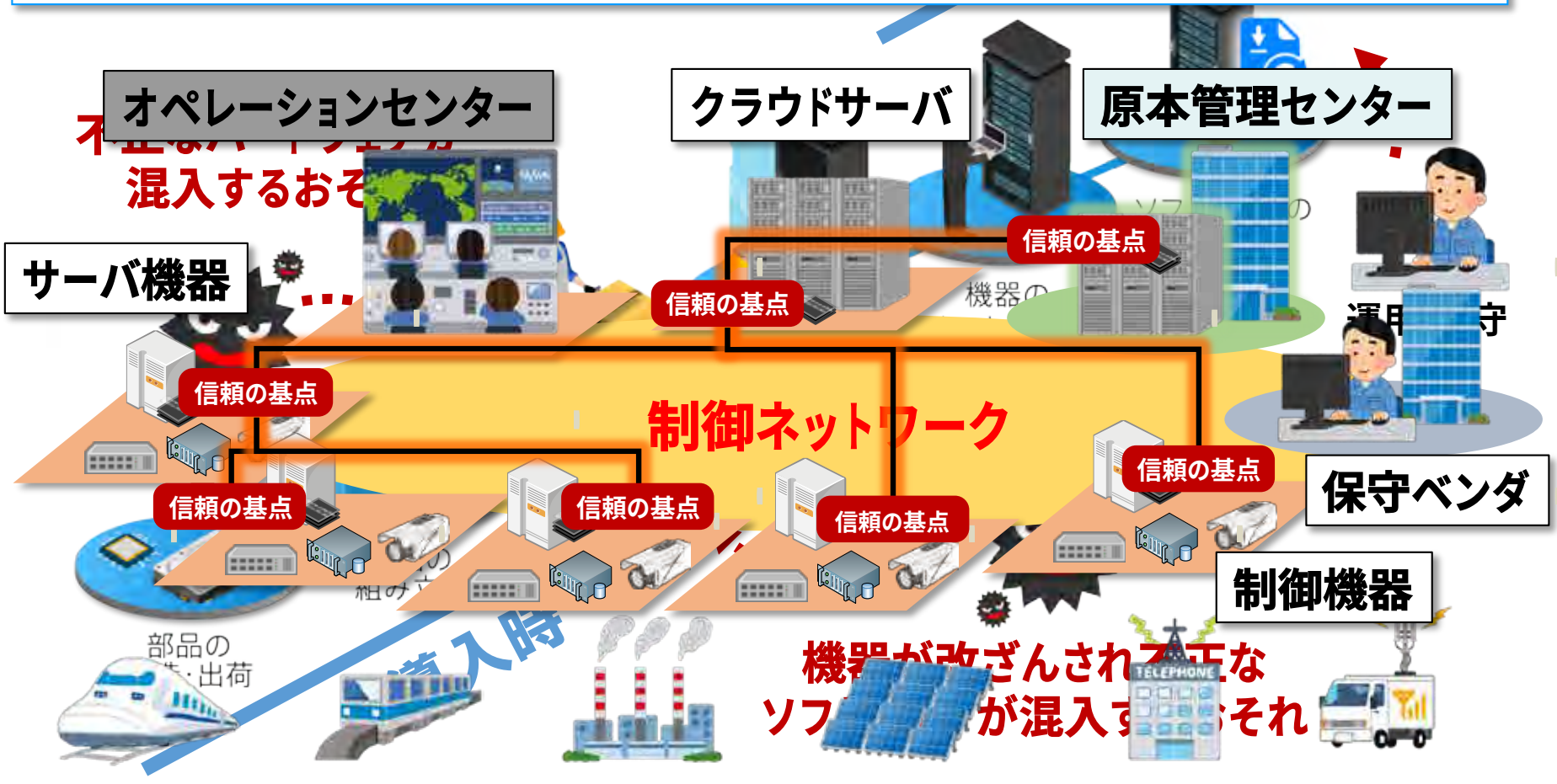
4. SIP自動走行システムとの課題間連携

- ダイナミックマップインフラのセキュリティ強化

制御ネットワークシステムの
セキュリティ(免疫力)強化

構築・運用時のリスク

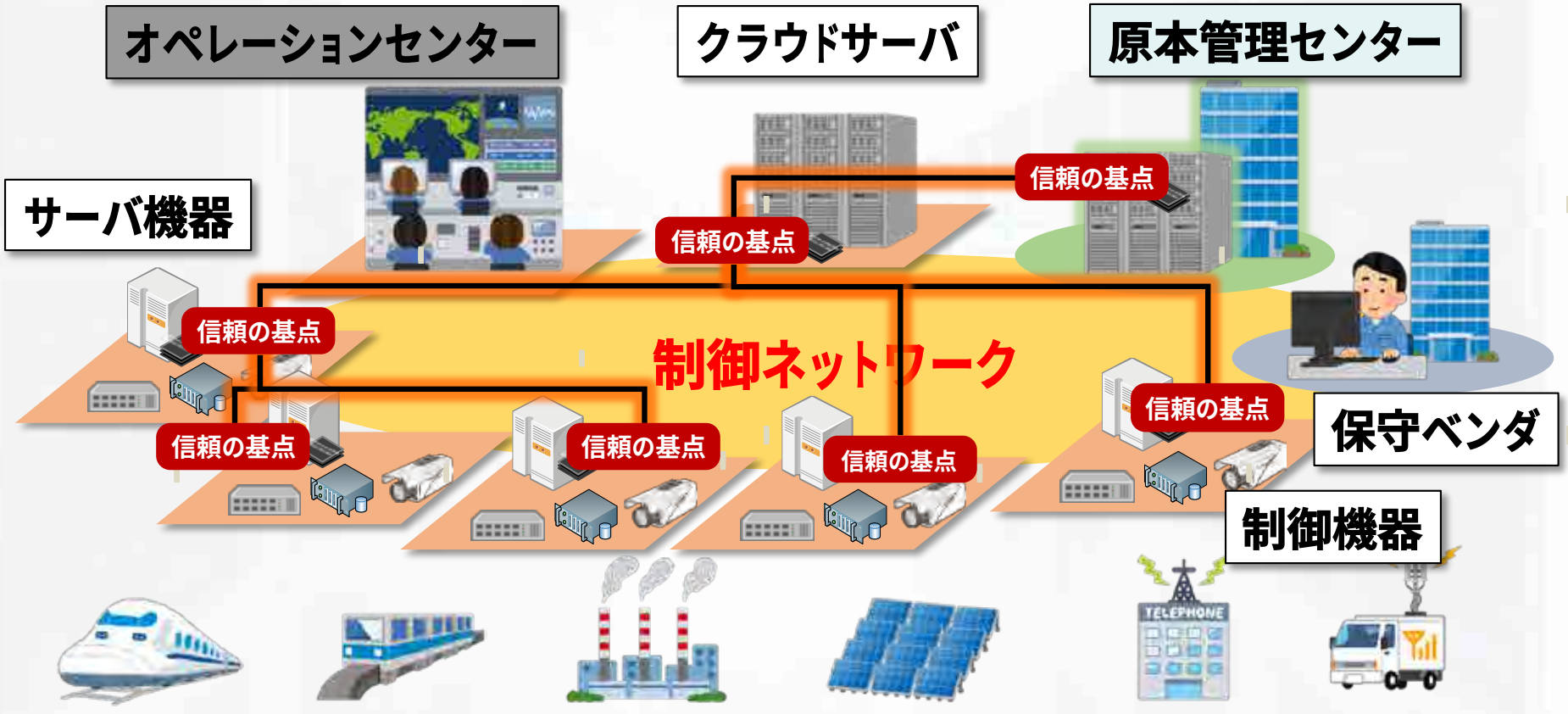
設備全体の機器のソフトやデータについて、マルウェア等による「改変」を検知し、構築時リスクと運用時リスクの対処



信頼の基点 セキュリティモジュール

大規模システムの真贋判定

設備全体の機器のソフトやデータについて、マルウェア等による「改変」を検知し、構築時リスクと運用時リスクの対処

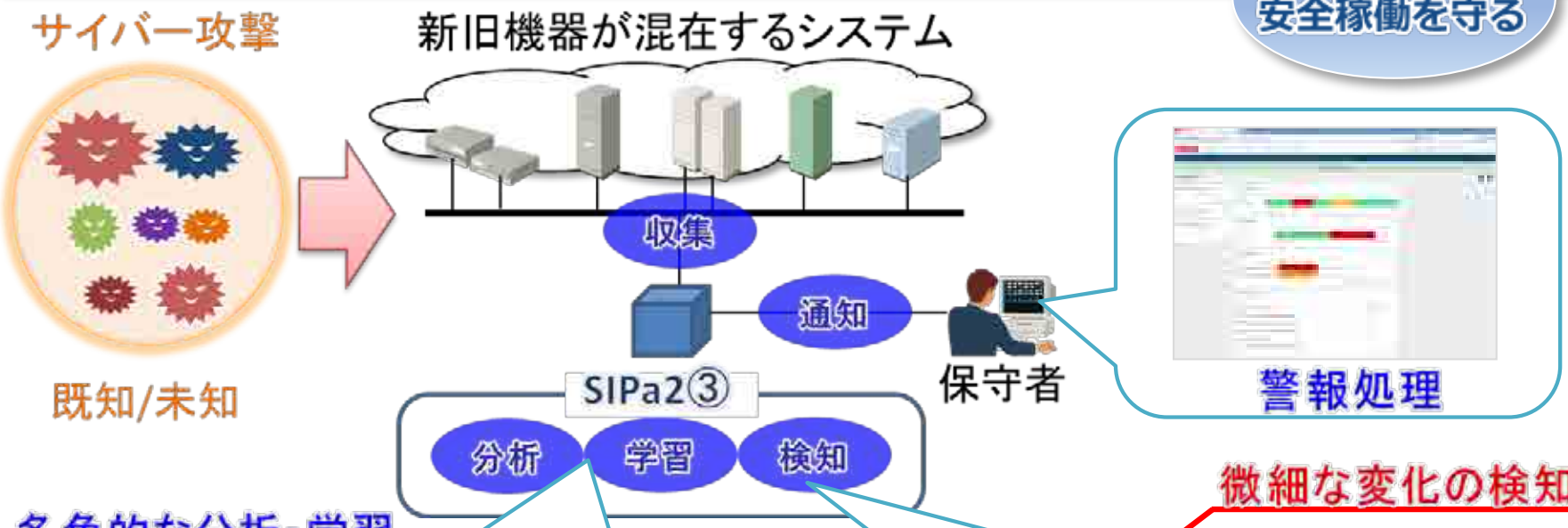


信頼の基点 セキュリティモジュール

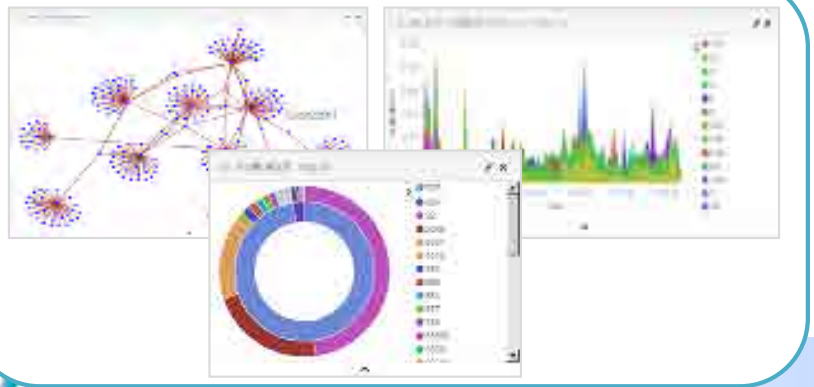
新旧機器混在下でのセキュリティ耐性を強化

先行版：制御ネットワークセンサ技術を昨年12月に製品化（日立）
拡大版：「面」で守るマルチセンサ技術の研究開発

システムの安全稼働を守る



多角的な分析・学習



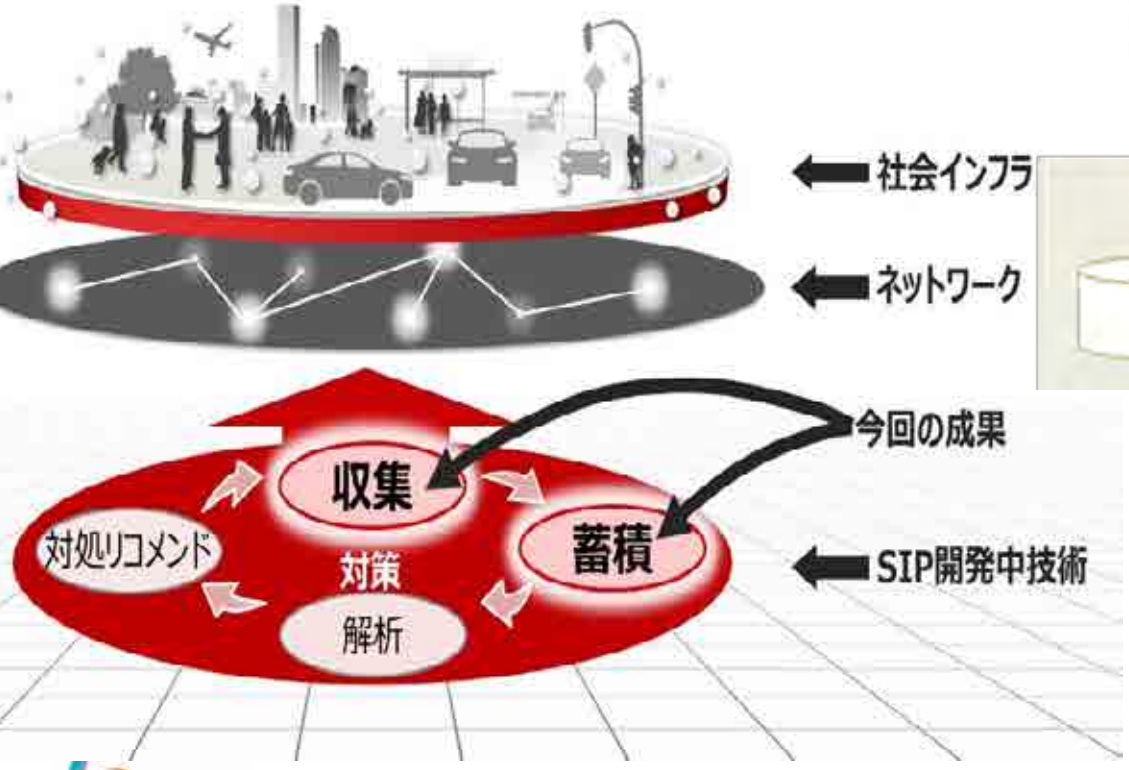
微細な変化の検知例

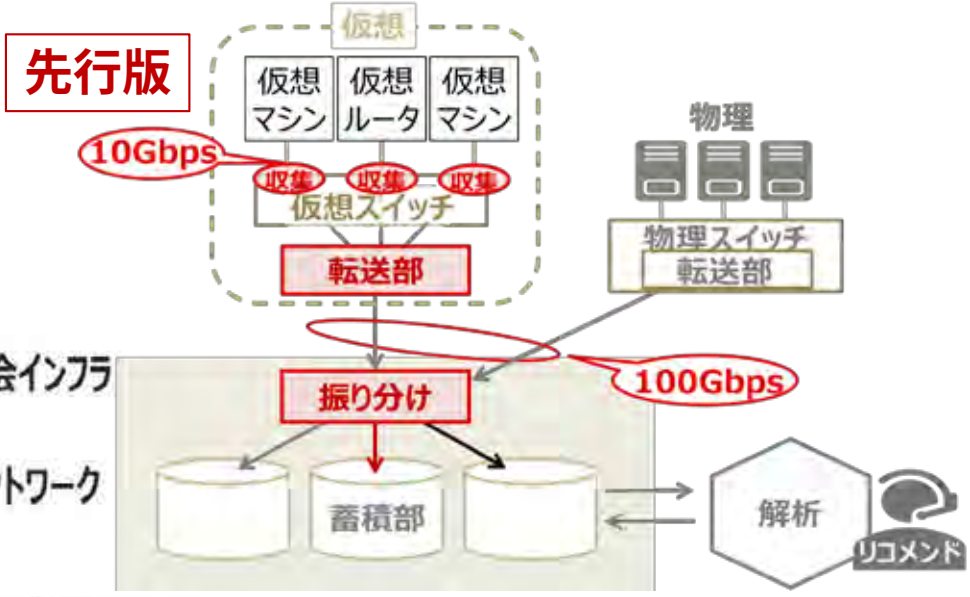
仮想ネットワークの高速タップ技術を開発・製品化へ

News Release　　2018.1.10　NEDO／富士通

ネットワークの通信データを欠損なく収集・蓄積する技術を開発
― 2018年度上期に富士通が本技術を実装した製品の提供を目指す ―

本事業の概要図





開発技術のイメージ図