SIPシンポジウム2016　2016.10.4 於品川インタシティホール

『重要インフラ等における サイバーセキュリティの確保』

平成２８年１０月４日

内閣府
プログラムディレクター
後藤　厚宏

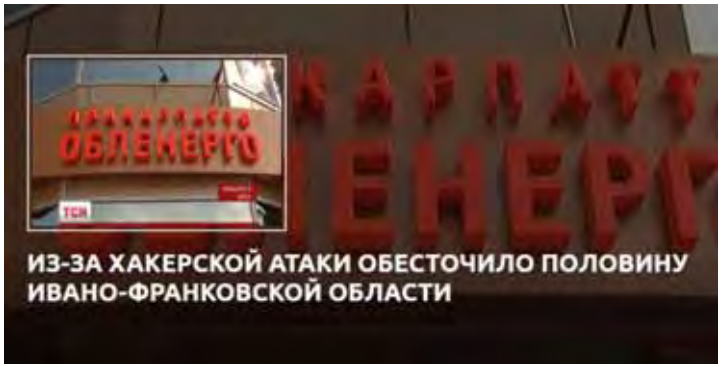
サイバー攻撃のターゲットは重要インフラへ

内閣サイバーセキュリティセンター(NISC)が
13セクターを指定

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(12月24日)
http://ru.tsn.ua/ukrayina/iz-za-hakerskoy-ataki-obestochilo-polovinu-ivano-frankovskoy-oblasti-550406.html

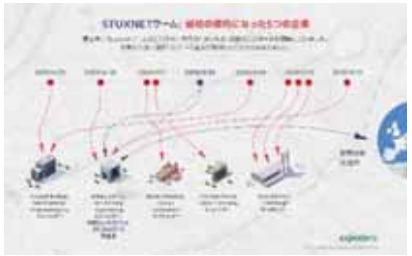
【事例2】欧州鉄道保護システムに脆弱性 (2016年1月発表)

列車の競合進路を防止する鉄道保護システムの脆弱性を突いた攻撃により衝突事故等の重大な事故が引き起こされる可能性指摘

出展：Security Affairs

【事例3】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、USBデバイスを経由した多段階の感染により外部と遮断されたシステムでウラン濃縮用遠心分離機を破壊 (Stuxnet)



出展：Kasperski

SIP

重要インフラのサイバーセキュリティ確保の重要性

重要インフラ等へのサイバー攻撃の脅威は現実のもの

- **日本の重要インフラ産業規模は**180**兆円**

2020年オリンピック・パラリンピック東京大会

- **ロンドン** (2012**年**)**、リオ** (2016**年**) **から・・・**

勘所となるセキュリティ製品・技術の自給の確保

- **技術安全保障**

将来のIoT (Internet of Things)普及に備えたセキュリティの先行的取組

SIP

重要インフラ等におけるサイバーセキュリティ確保

社会実装
（重要ｲﾝﾌﾗ）

Trusted Operational Platform for Cybersecurity（TOP）

- ◆ **サイバーセキュリティの技術・導入・運用手順から人材までをセットで**
- ◆ **国内外の優れたセキュリティ技術・ノウハウの受け皿になれる枠組み**

本計画　（2016年1月～ 2019年度　予定）

コア技術

- **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

- **適合性確認のあり方**
- **評価検証**
- **情報共有**
- **人材育成**

SIP

重要インフラ等におけるサイバーセキュリティ確保

社会実装
（重要ｲﾝﾌﾗ）

Trusted Operational Platform for Cybersecurity（TOP）

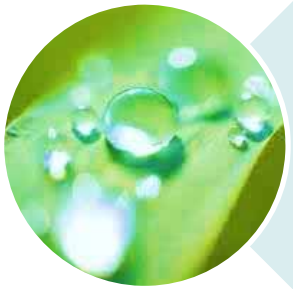
- ◆ サイバーセキュリティの技術・導入・運用手順から人材までをセットで
- ◆ 国内外の優れたセキュリティ技術・ノウハウの受け皿になれる枠組み

本計画　（2016年1月～ 2019年度　予定）

コア技術
- パナソニック
- ルネサス
- ECSEC
- CSSC
- 日立製作所
- 三菱電機
- 富士通
- NTT

社会実装技術
- 慶応大
- 名工大
- NTTコミュ
- 日立製作所
- 産総研

コア技術開発の３つのチャレンジ



製造、構築、運用、保守というライフサイクル全体でのセキュリティ確保

⇒「信頼の基点」による真贋判定技術とプラットフォーム化

「新旧・強弱混在」の制御ネットワークにおいて制御システム特有動作に対応

⇒AI技術，ビッグデータ技術の活用したセキュリティ動作監視・解析・防御技術

今後のIoT時代に適合できる重要インフラのセキュリティ対策技術

⇒IoT向け暗号実装技術と安全性評価

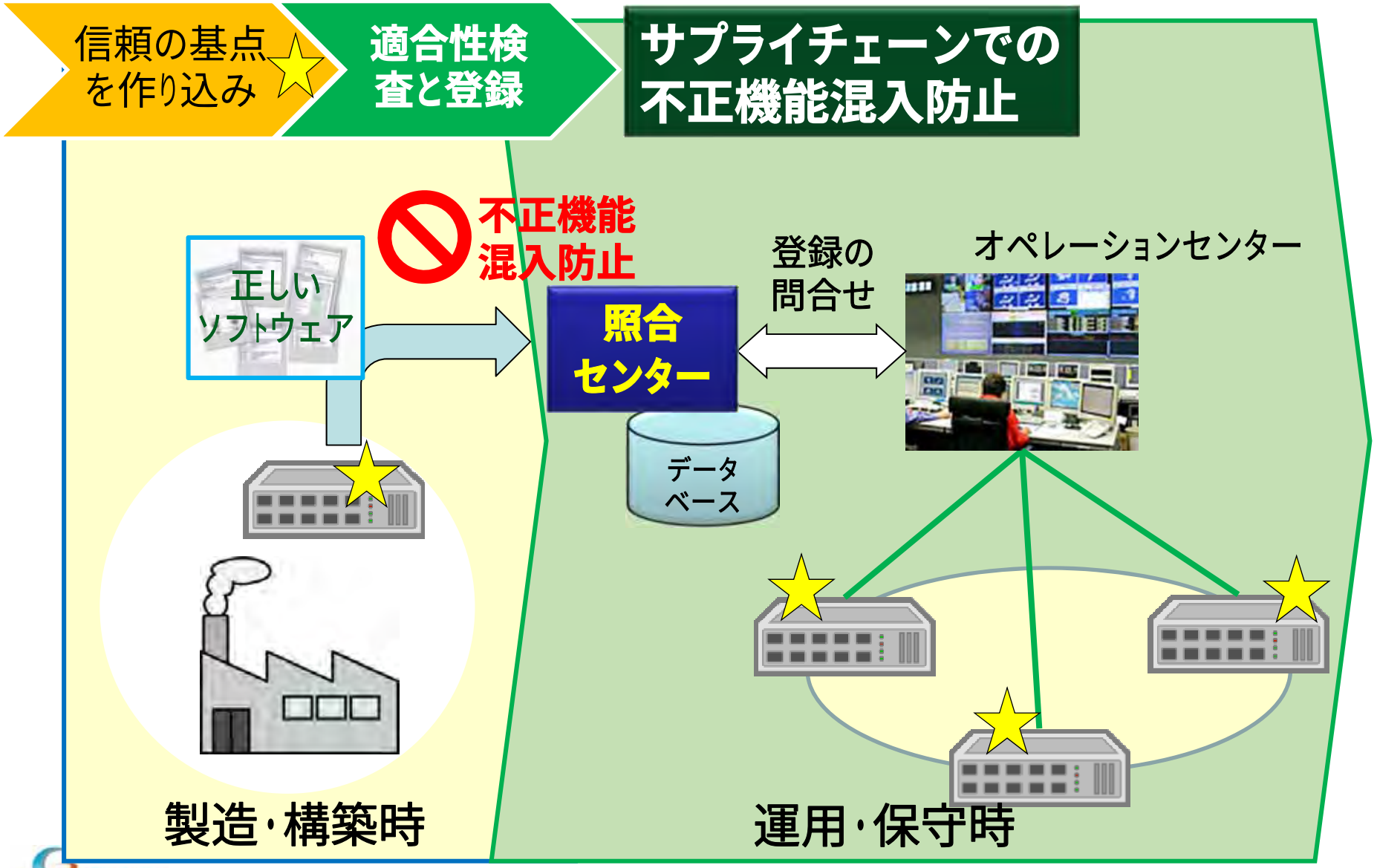
社会実装（TOPの実現）に向けた３つのチャレンジ

（ハード・ソフトだけでなく）**技術評価、導入・運用手順、人材育成を成果目標に**（TOPの実践）

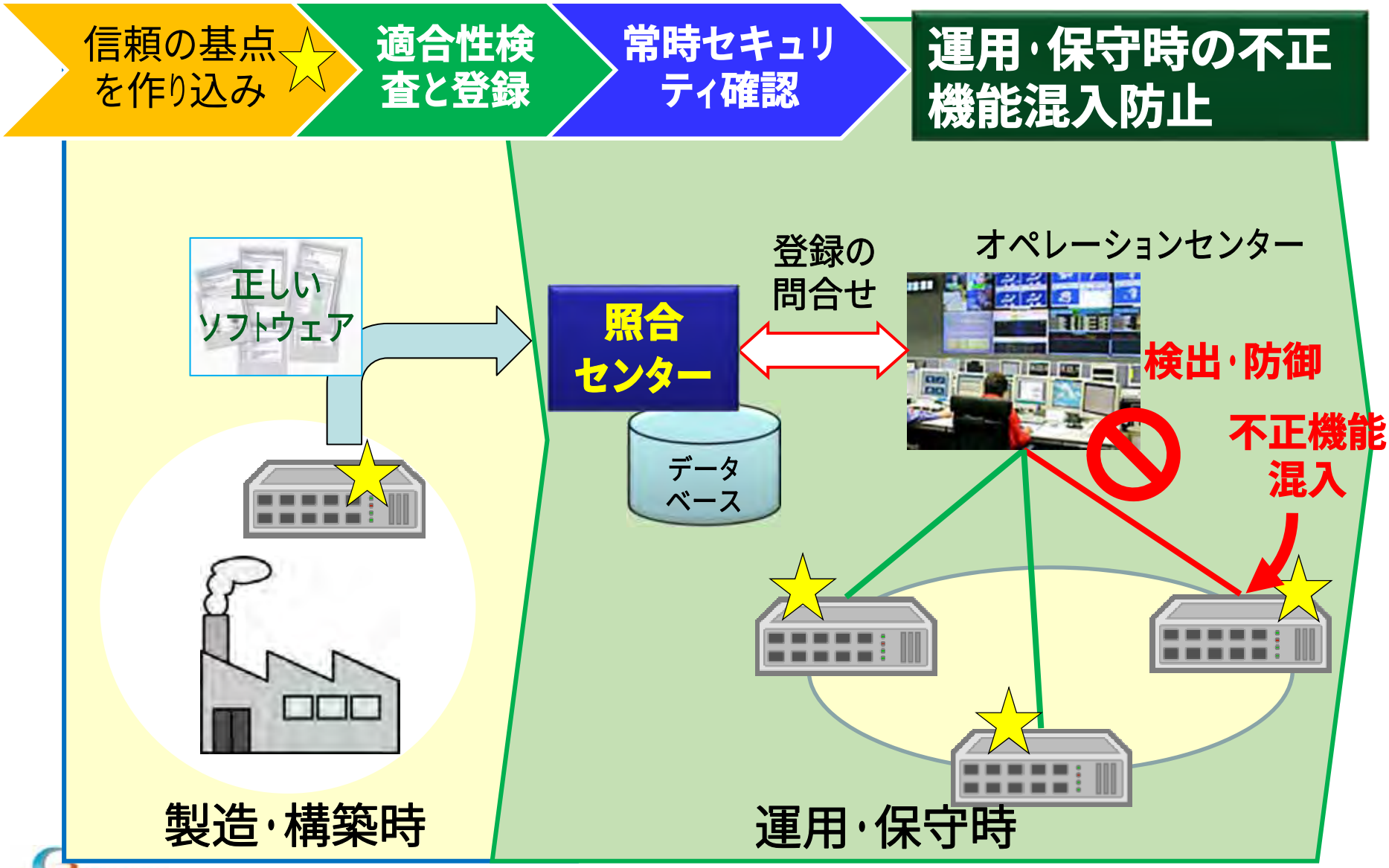
国内外の多様な組織との間で情報連携を担う情報共有プラットフォーム

当初から重要インフラ事業者と協働の技術開発

「信頼の基点」による真贋判定技術：製造・構築時



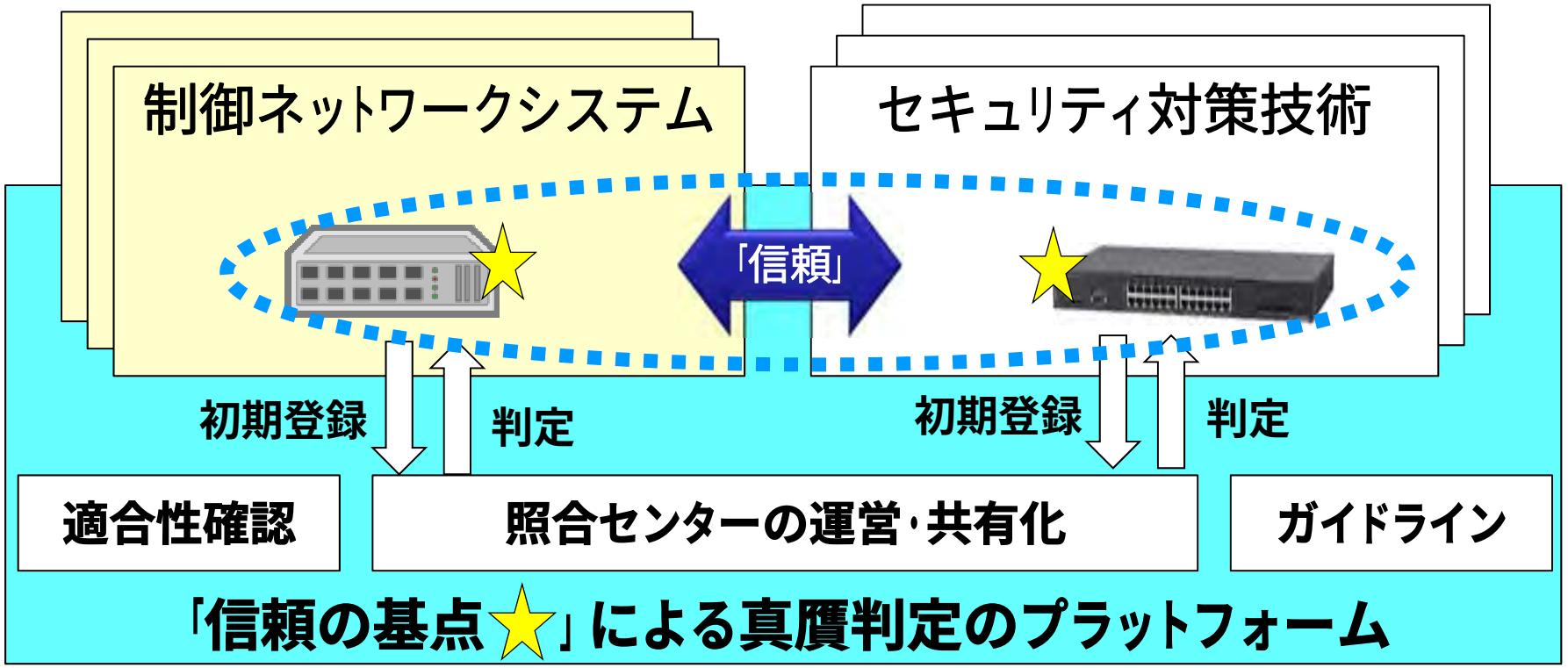
「信頼の基点」による真贋判定技術：運用・保守時



真贋判定技術のプラットフォーム化

「信頼の基点」による真贋判定技術をプラットフォーム化し、国内外の優れたセキュリティ技術の受け皿に（TOPの実践）

⇒国内外の関連技術との連携インタフェースに向けた国際活動



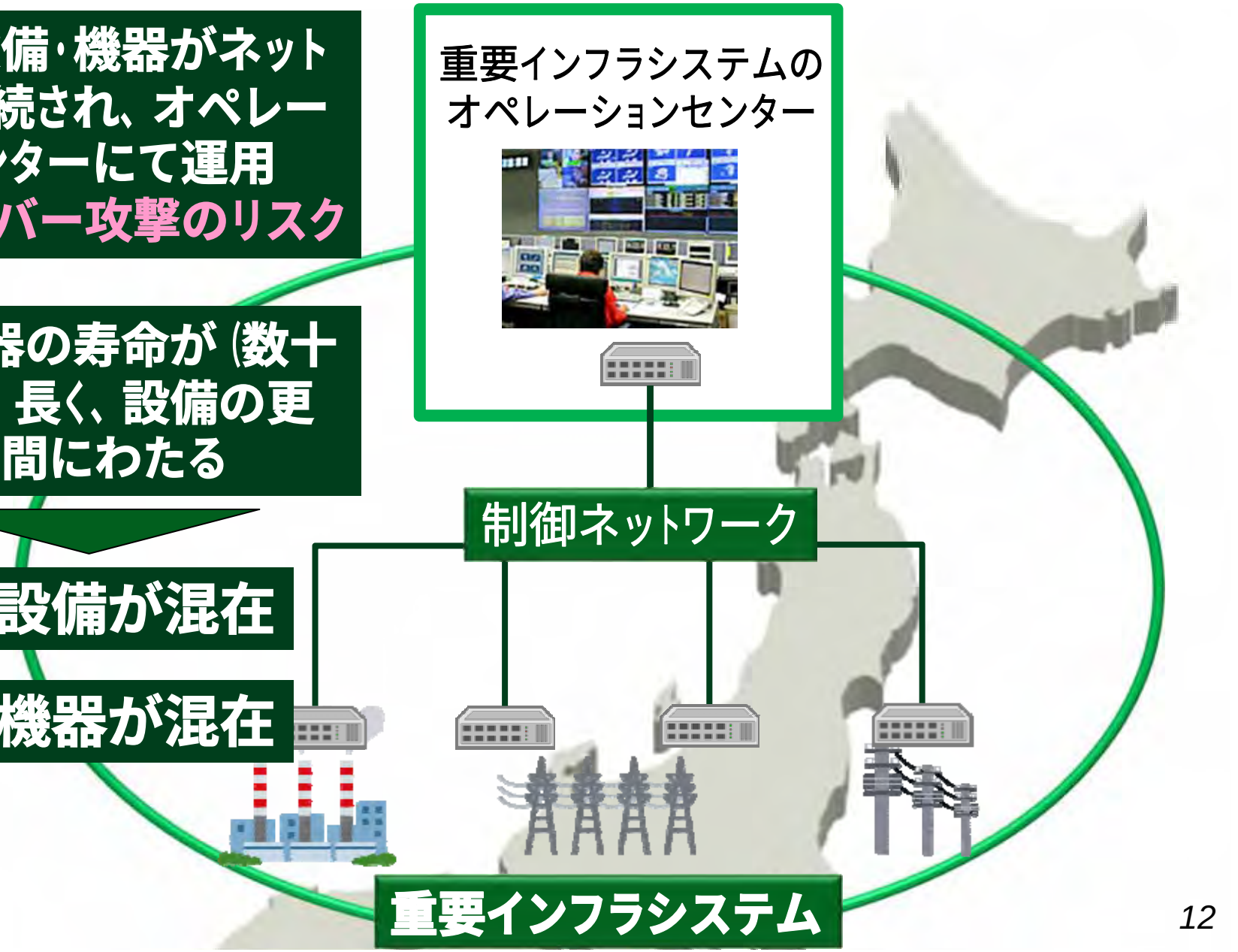
セキュリティ動作監視・解析・防御技術の要件

多数の設備・機器がネットワーク接続され、オペレーションセンターにて運用
⇒サイバー攻撃のリスク

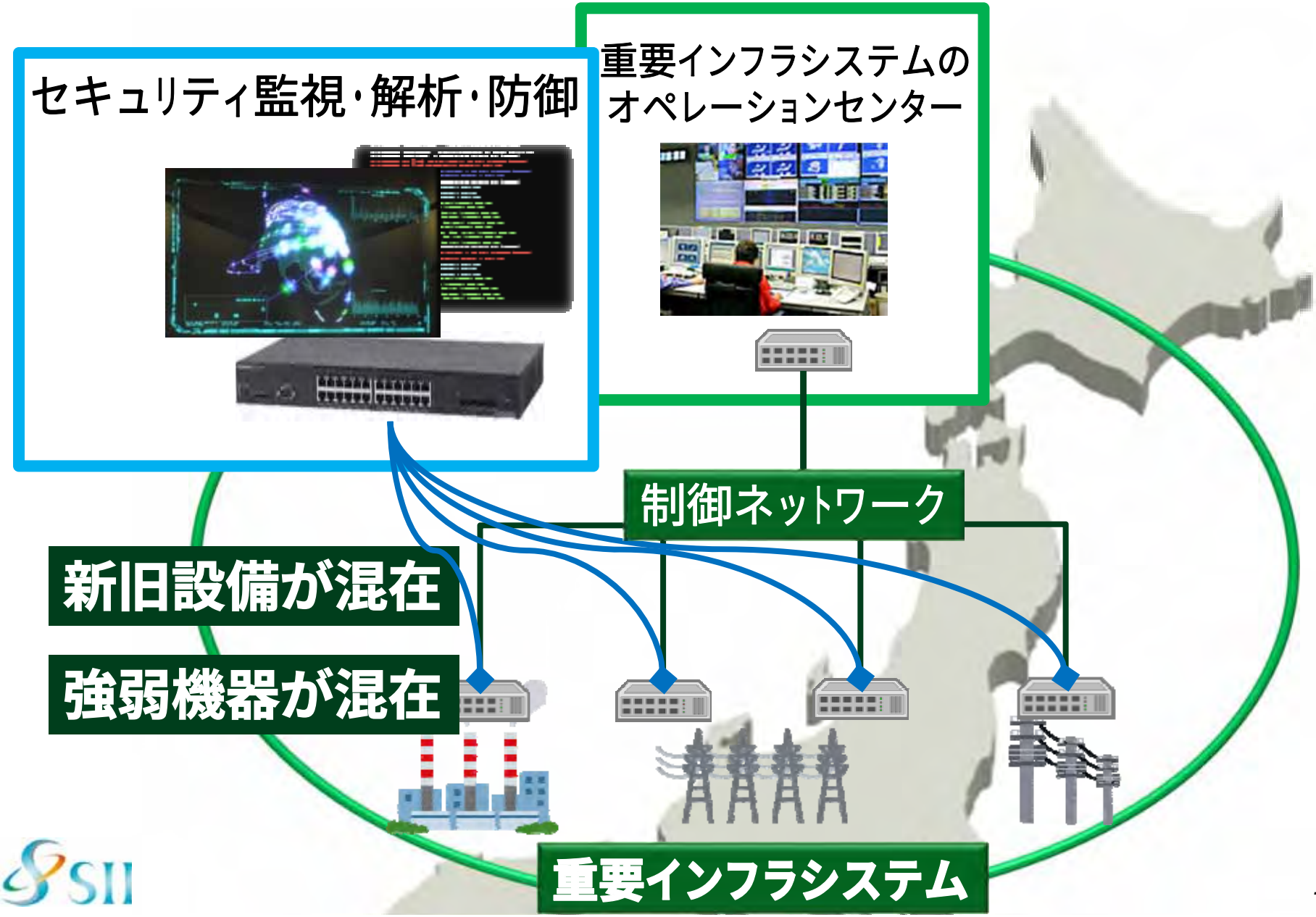
設備・機器の寿命が（数十年以上と）長く、設備の更改は長期間にわたる

新旧設備が混在

強弱機器が混在



セキュリティ動作監視・解析・防御技術の要件



セキュリティ動作監視・解析・防御技術への取組み

セキュリティ監視・解

新旧設備が混

強弱機器が混

「仮想環境」対応

- クラウドインフラのセキュリティ確保（⇒Society5.0）

「面」で判断

- 「新旧混在」の大規模インフラで実証実験開始

「安全」な運用継続

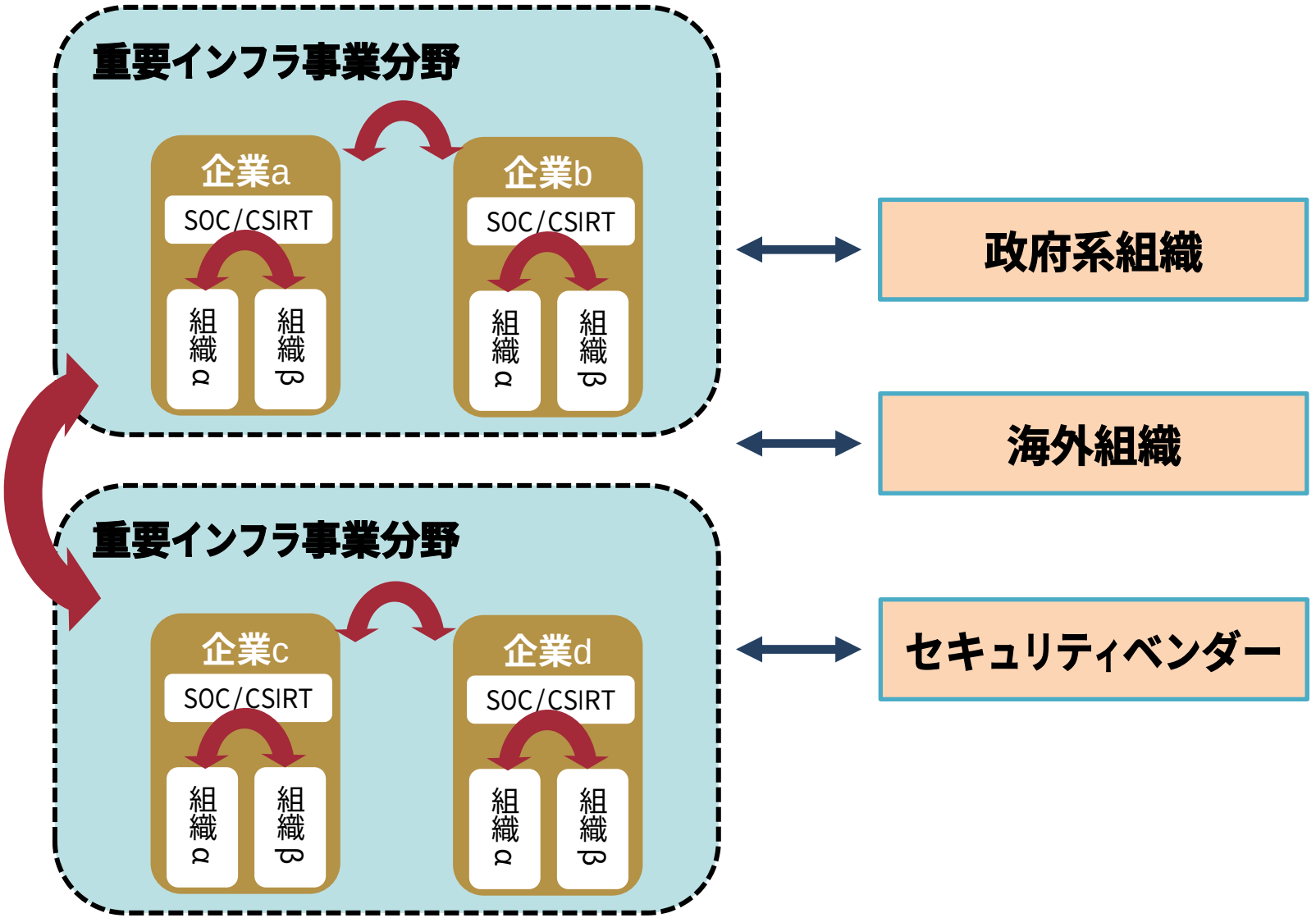
- 制御機器の特性を生かすホワイトリスト機能

IoT時代への対応

- 「強弱混在」環境でのGW機能と小型・省エネ化

重要インフラシステム

情報共有プラットフォーム



情報共有プラットフォーム： 導入･運用手順から組織まで

情報共有ツール

- STIX, TAXIIを活用しグローバルな情報共有
- 現場での使いやすさ

共有情報の活用

- 導入･運用手順書
- セキュリティ対策設定への活用支援

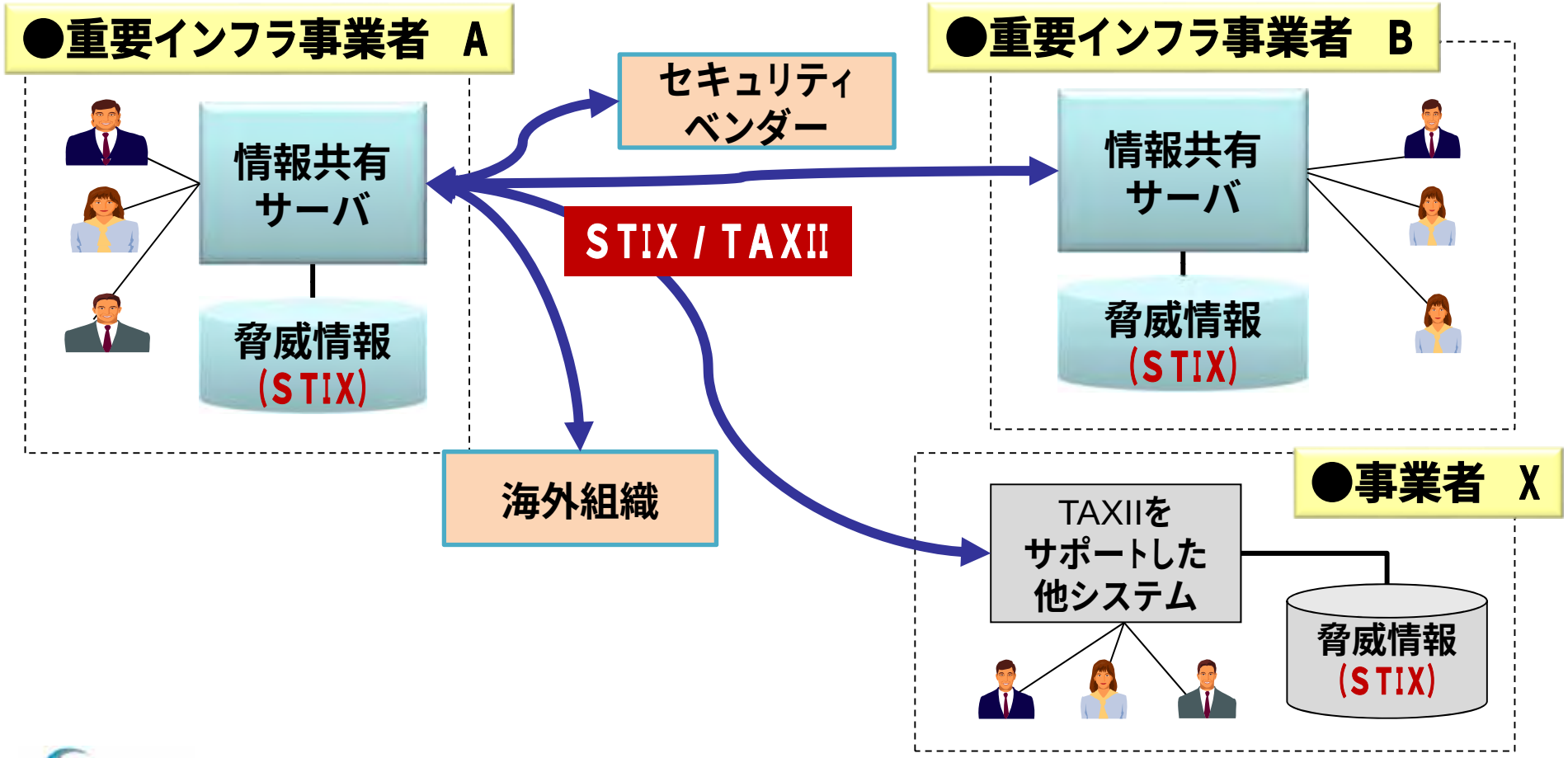
グランドデザイン

- 情報共有の活性化
- 事業分野をまたぐ情報共有のあり方

プラットフォーム化

情報共有プラットフォーム：　国際連携の活用

国際標準化が進むデータ形式「STIX/ TAXII (※1)」を活用し、グローバルな情報共有に対応



情報共有プラットフォーム： インフラ事業者と協働

SNSベース、タブレット対応等、実務を担当する技術者・オペレータにとって使いやすいインタフェース

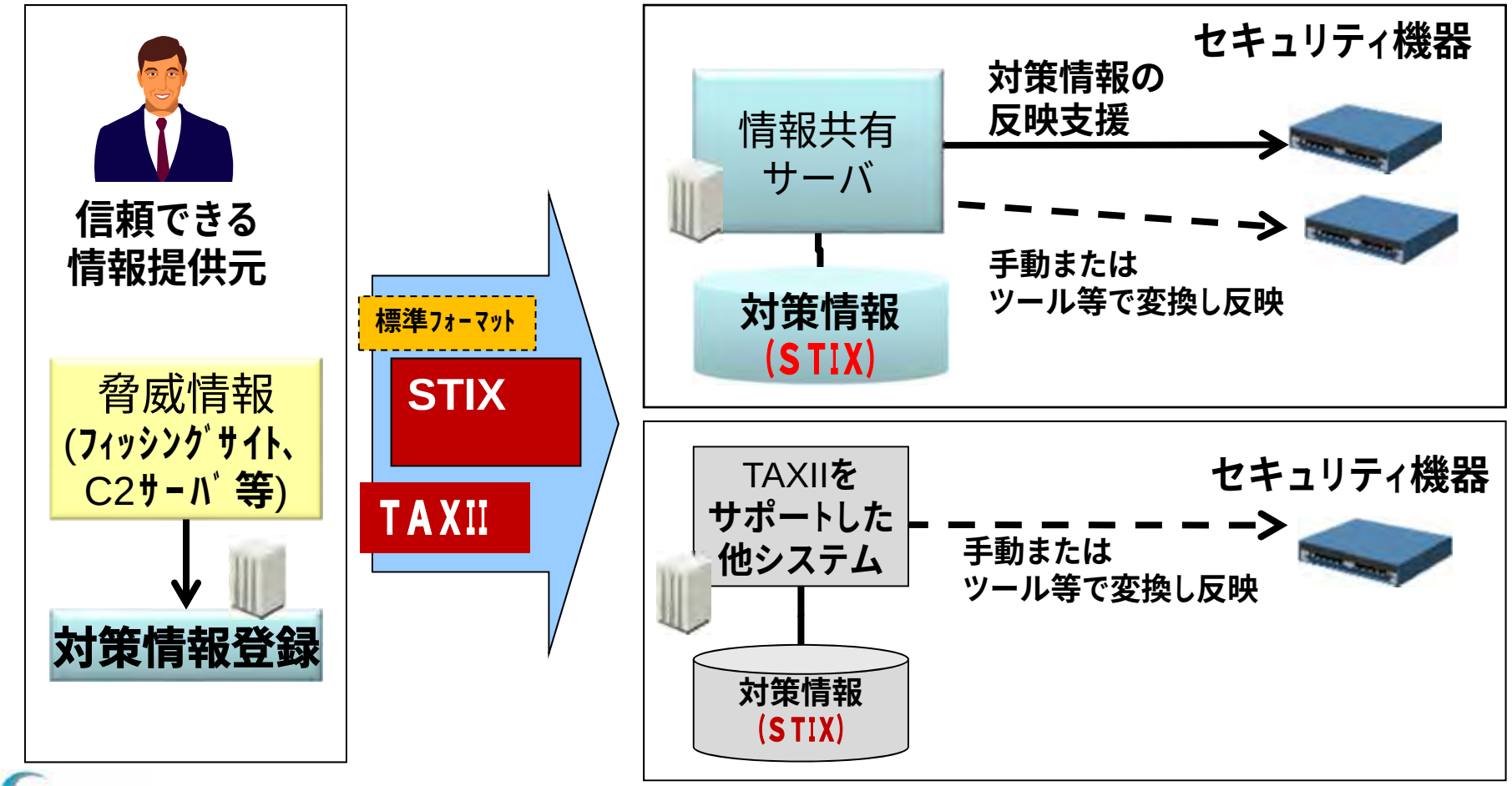
用途別に用意された画面
・ディスカッション用（SNS）
・作業指示用（実施管理）
・脅威情報（STIXデータベース）

信頼されたメンバー間でグループを作成して情報交換

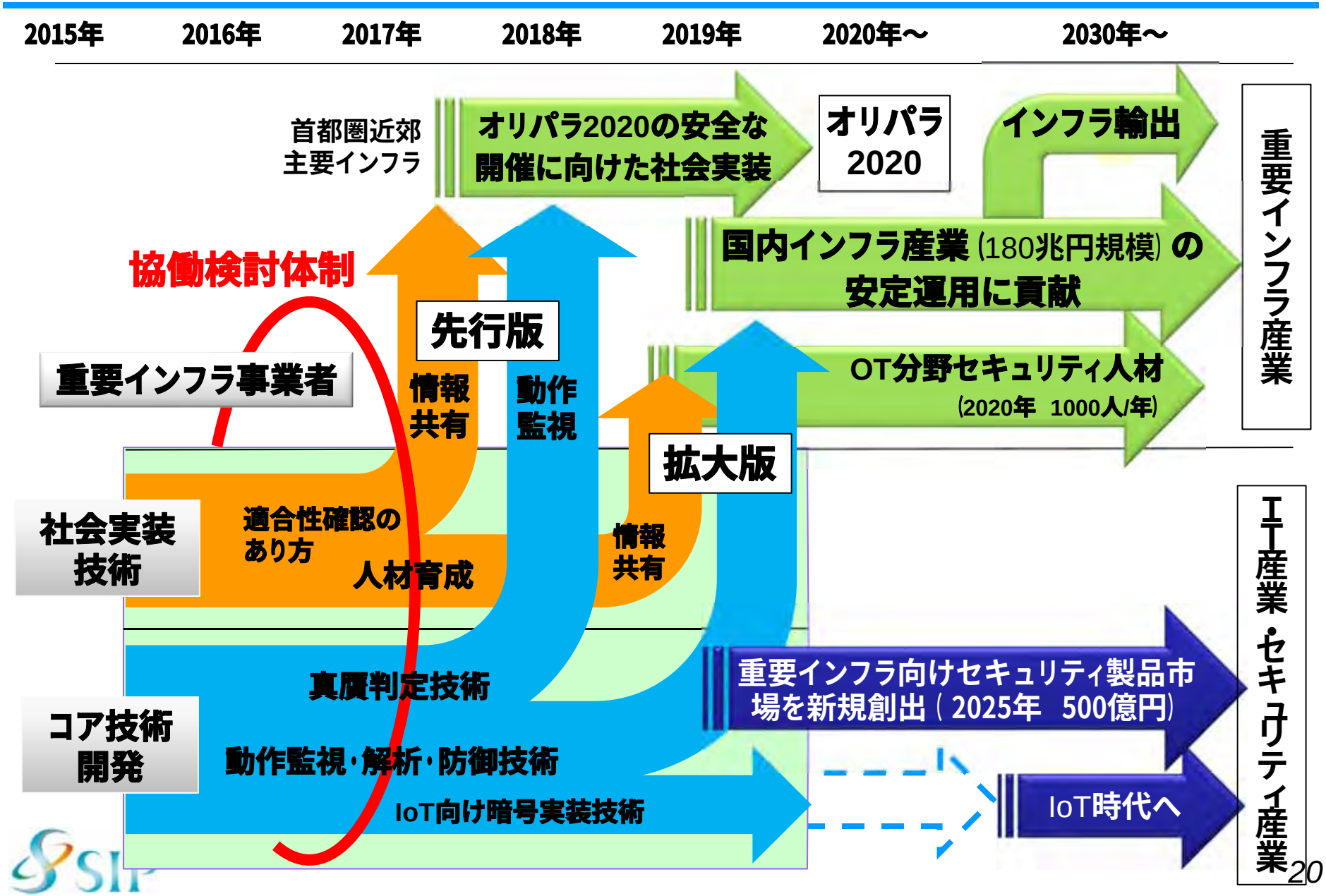
直感的に操作できる
SNSベースの
入力インターフェース

情報共有プラットフォーム： セキュリティ運用を支援

脅威対策情報を活用する組織のセキュリティ対策を支援



SIPサイバーセキュリティ確保の展開計画



国プロ連携と海外組織との連携

Society5.0に向けてダイナミックマップ（データベース）インフラのセキュリティ強化

- 重要インフラに関わるSIP（自動走行、防災、インフラ他）との連携

「技術の受け皿としてプラットフォーム」の構築・普及促進（TOPの実践）に向けた国際連携の枠組み作り

- 「信頼の基点」による真贋判定技術のプラットフォーム化
- 情報共有プラットフォームにおける国際連携強化

動作監視・解析・防御技術におけるAI技術の利活用

- AI3センターと連携し、最新のAI研究開発成果を動作監視・解析・防御技術に取り込むことで、新たなサイバー攻撃にも対応可能なシステムを構築