資料WG4－4

IoTセキュリティのコンセプトと対策

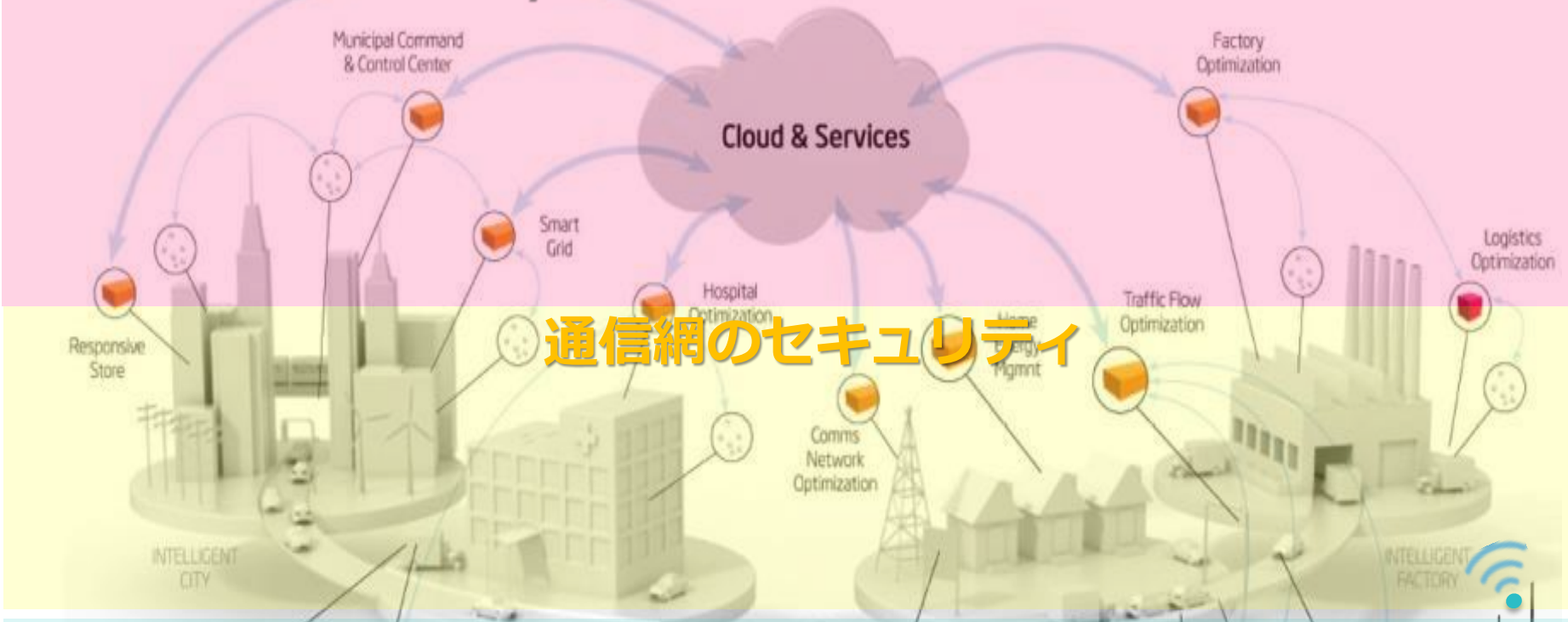
TM

佐々木　弘志
インテル セキュリティ（マカフィー株式会社）　サイバー戦略室
シニア・セキュリティ・アドバイザー　CISSP

IoTセキュリティの考え方と NIST Framework for CPS

Internet of Things (IoT) のセキュリティ層

クラウド/データセンターのセキュリティ



通信網のセキュリティ

エッジデバイスのセキュリティ

IoT時代における新たなセキュリティ脅威とは？

新しく発生した脅威は以下の３つと考えられる

エッジデバイスへの「ネットワーク経由での」
サイバー攻撃の機会の発生

各層が相互接続することによるシステム外部からの
侵入口の増加

各層が相互接続することによるシステム内部での
サイバー攻撃の影響範囲の拡大

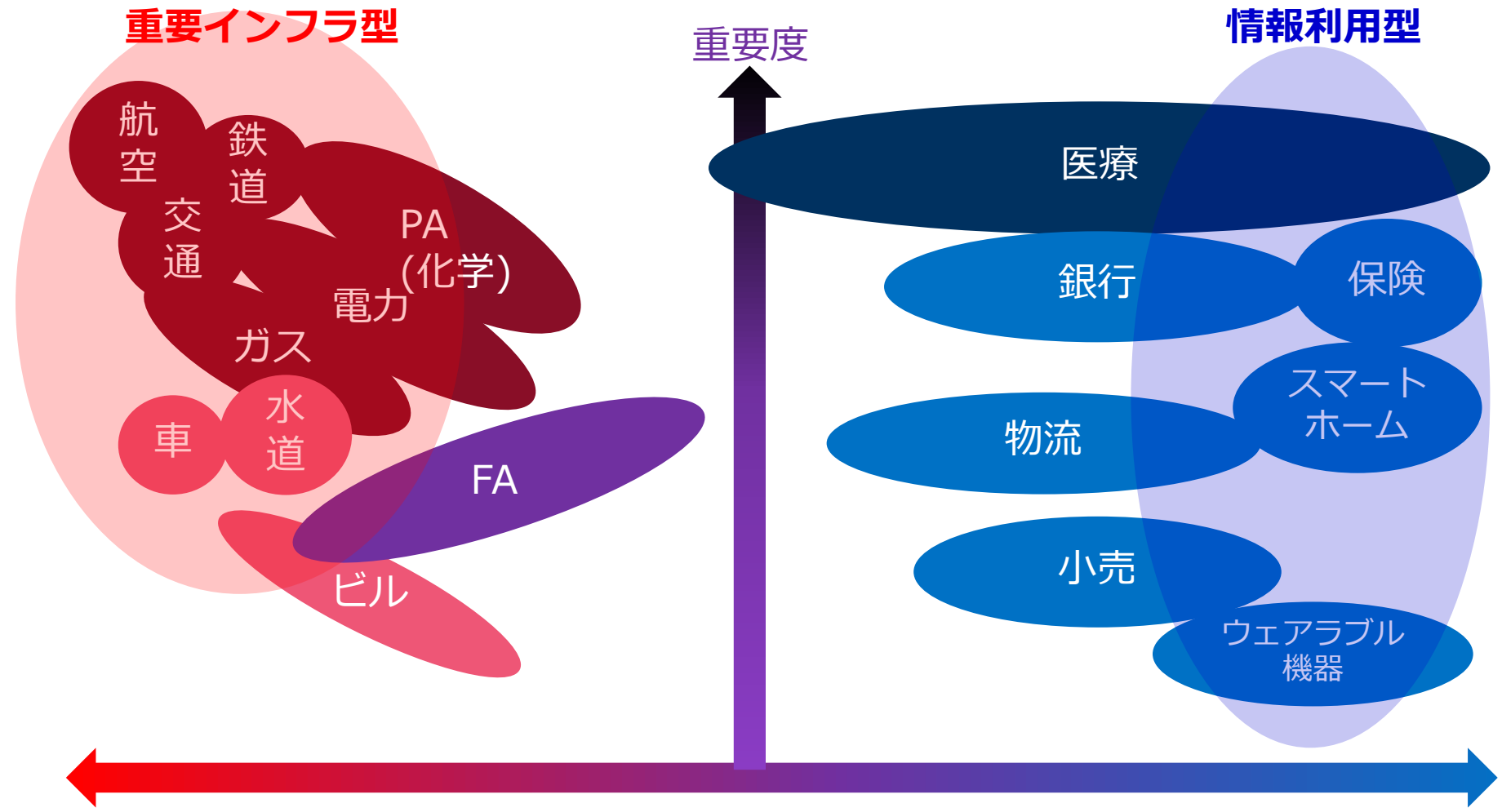
完全に守りきることは難しい。
エッジデバイス、通信網、クラウド/データセンターの
相互連携においてセキュリティを確保する。

IoTを適用する業界別のセキュリティ脅威とIoTの３層におけるセキュリティリスク評価

IoTが適用される業界		IoT活用例	主なセキュリティ脅威	エッジデバイス			通信網			クラウド/データセンター		
				C	I	A	C	I	A	C	I	A
製造	FA	装置リモートメンテナンス	制御装置異常	L	H	H	L	L	L	L	L	L
	PA	化学反応の歩留まり向上	プラント動作異常	M	H	H	M	L	L	M	L	L
流通/サービス	小売	POS端末情報の活用	個人情報漏えい	H	M	L	H	M	L	H	M	M
	物流	貨物のバーコード情報の活用	個人情報漏えい	L	L	M	L	L	M	H	L	M
金融	銀行	フィンテック・仮想通貨	個人情報漏えい	H	M	L	H	M	L	H	M	L
	保険	テレマティクス保険	個人情報漏えい	H	M	L	H	M	L	H	M	L
公共インフラ	電力	スマートメーター	停電/メーター改ざん	L	M	L	L	M	M	M	H	H
	ガス	スマートメーター	ガス停止/メーター改ざん	L	M	L	L	M	M	M	H	H
	航空	航空機運航の効率化	不正操作による航空機事故	L	H	H	L	H	H	L	H	H
	鉄道	鉄道運行管理の効率化	不正操作による鉄道事故	L	H	H	L	H	H	L	H	H
	水道	リモート監視	遠隔操作による水道機能停止	L	L	H	L	L	H	L	L	H
	交通	渋滞解消	遠隔操作による自動車事故	L	H	H	L	H	H	L	H	H
	ビル	電力使用量の効率化	遠隔操作による火災	L	M	M	L	M	M	L	M	M
	医療	遠隔医療	個人情報（病歴）漏えい	H	H	L	H	H	L	H	H	L
一般消費者	個人	ウェアラブル機器	個人情報漏えい	M	L	L	M	L	L	M	L	L
	家庭	スマートホーム	個人情報漏えい	H	H	L	H	H	L	H	H	L
	車	自動運転	不正操作による自動車事故	L	H	H	L	H	H	L	H	H

凡例：C:機密性 I：完全性 A:可用性/H：リスク高 M：リスク中 L：リスク低

重視するセキュリティ観点によるM2M/IoT業界別分類



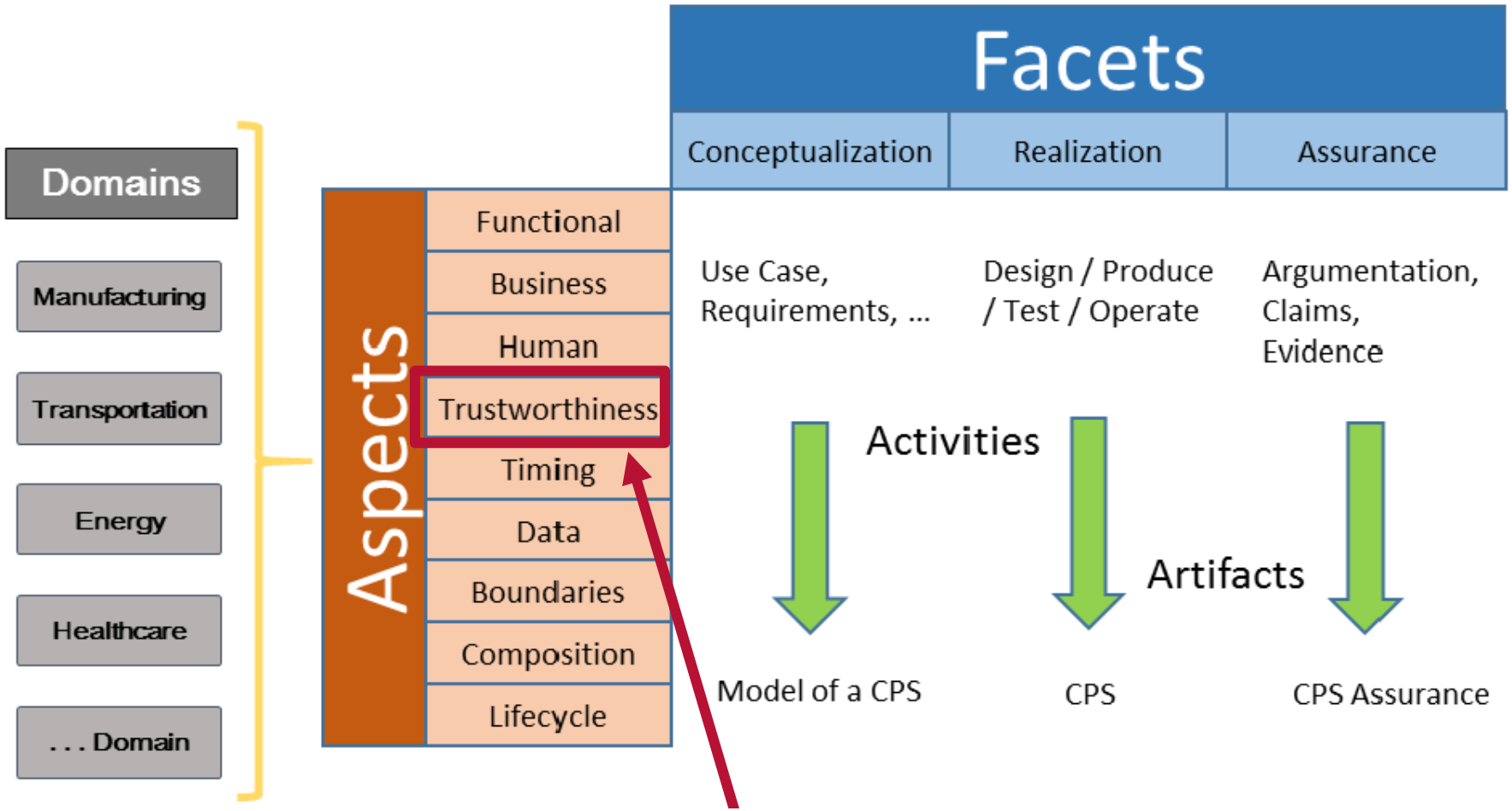
NIST Cyber Physical System Framework v0.8

NIST (National Institute of Standards and Technology) 米国国立標準技術研究所が、2015年9月にドラフト版を発表したCyber Physical System (CPS) の開発手法に関するフレームワーク

このフレームワークは、CPSの基礎的な概念や開発手順の定義を行い、関係者間での認識の相違をなくし、自由な意見交換ができることによって、CPSシステムの開発を促進することを目的としている。セキュリティに関しても基本的な考え方が記載されている。

NIST Cyber Physical System Framework 基本概念

開発過程において、Aspects（面）とFacets（相）で考える



Security はTrustworthiness（信用性）に含まれる。

NIST Cyber Physical System Framework セキュリティの考え方

信用性をサイバー、アナログ、ハードの要素で統合的に考える

- Trustworthiness(信用性)
  - Safety（安全性）
  - Reliability（信頼性）
  - Privacy（プライバシー）
  - Cybersecurity（セキュリティ）
  - Resilience（回復性）

Figure 20: Physical, Analog, and Cyber Components of CPS

サイバー要素だけを考えるのではなく、CPSシステム全体で考える

IoTセキュリティ
先端技術動向

次世代の重要インフラ向け
セキュリティフレームワーク
Intel Security Critical Infrastructure Protection

intel Security

テキサスの実証実験にて開発 ~NIST IR 7628対応~
EPGおよびCCETとの位相計測装置パイロットプロジェクト

Electric Power Group（EPG）は、同社の位相計測製品にセキュリティ層を付け加え、それらをCCETを通じて導入計画

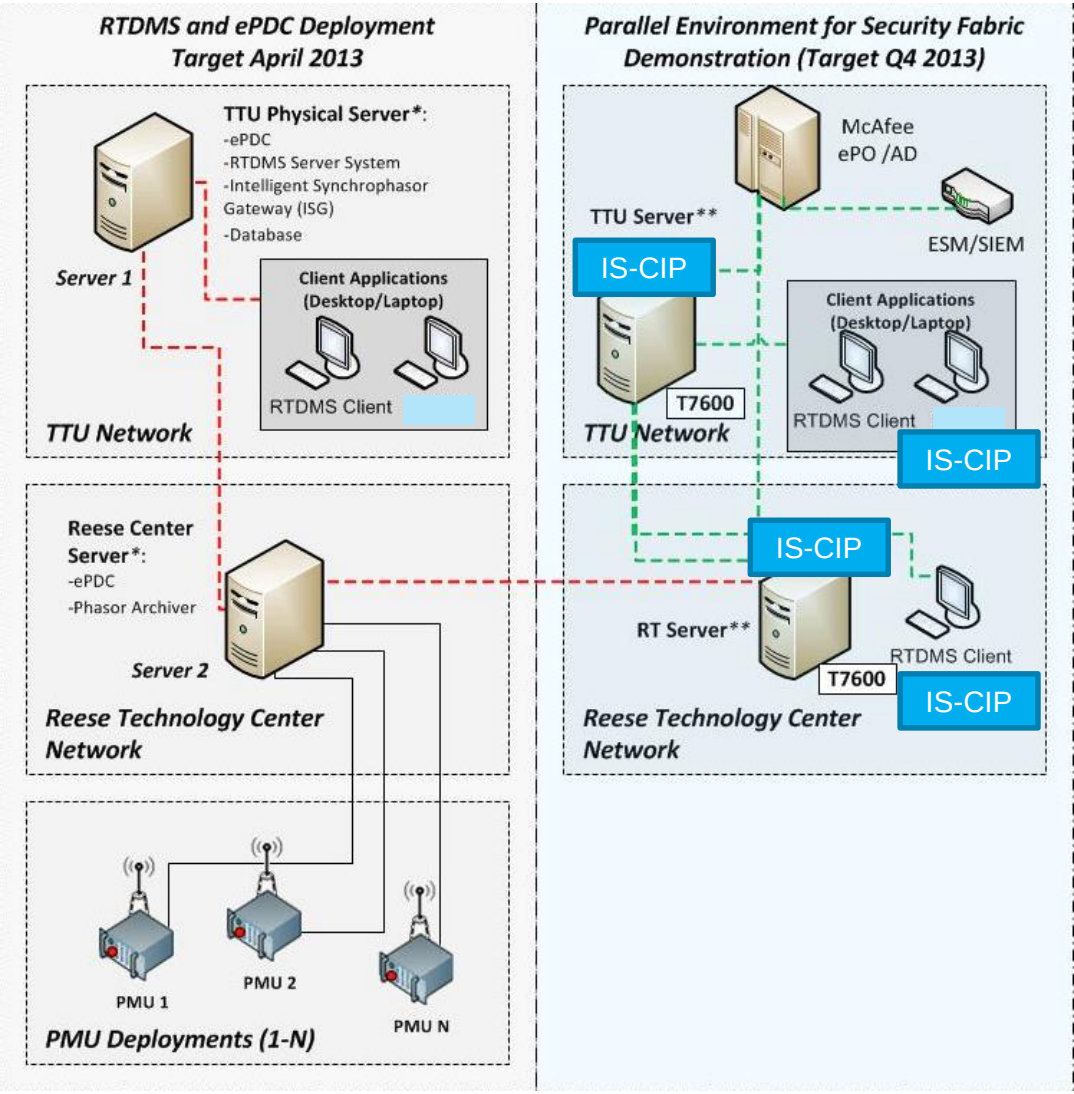
Center for the Commercialization of Electric Technologies（CCET）は、テキサスにおける位相計測装置デモンストレーションプロジェクトへの参加を米国エネルギー省（DoE）によって認められている

テキサス工科大学（TTU）が実地試験の現場となっている。

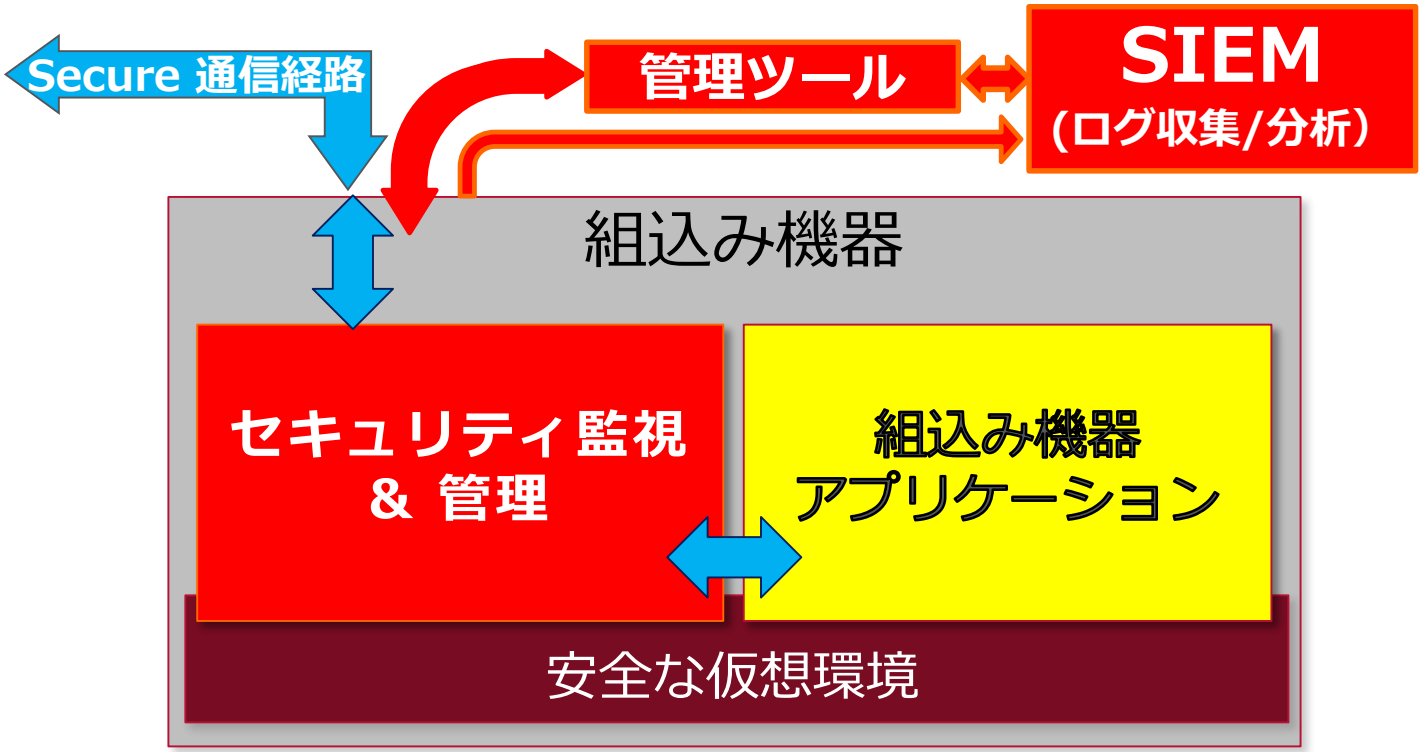
保護したシステムと保護していないシステムを用意して、攻撃を行いソリューションの効果を確認。

Intel Security Critical Infrastructure Protection (IS-CIP) としてリリース

（2015年4月）

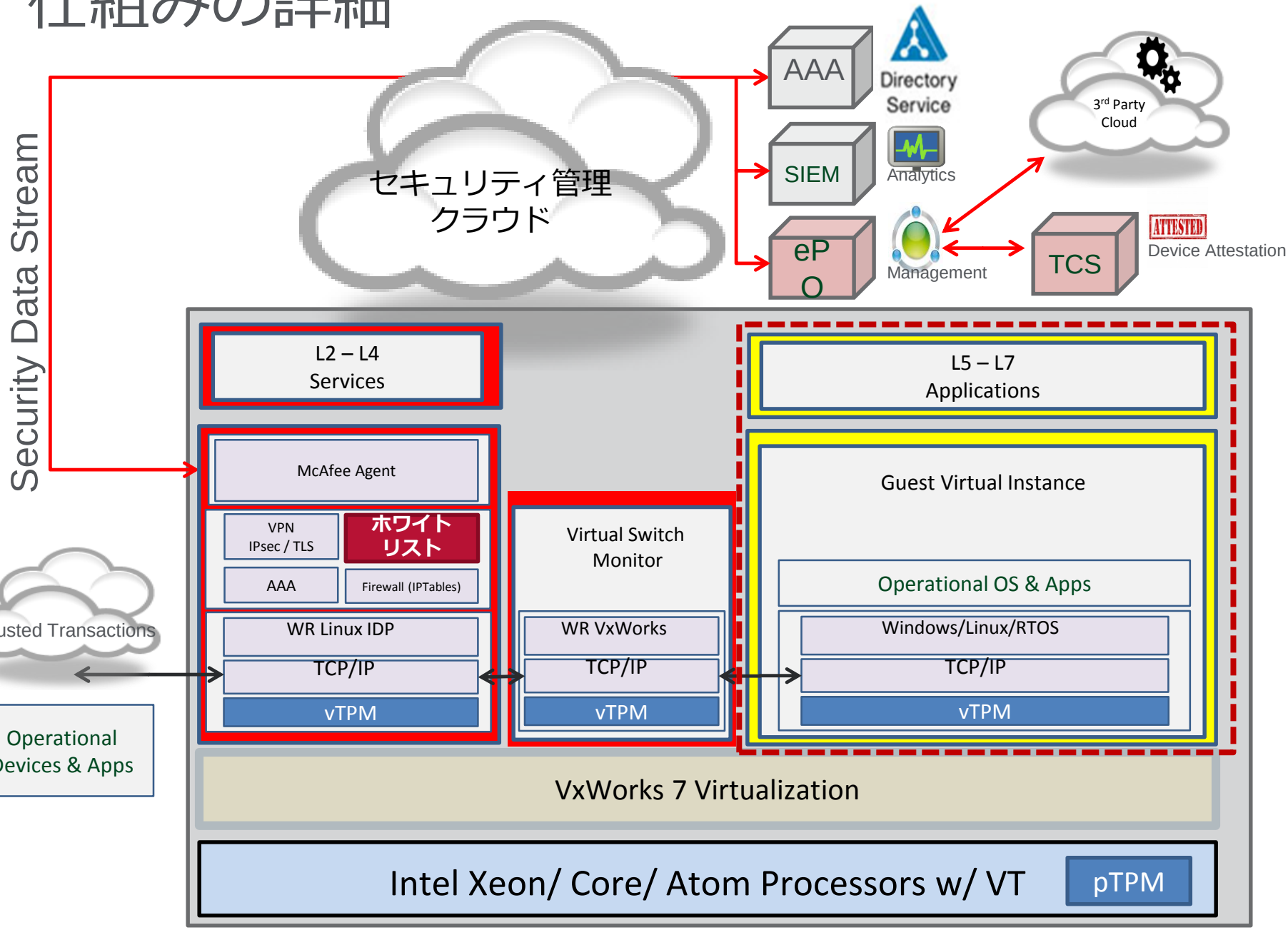


Intel Security CIP
仕組みの概要～Security Built-In～



- 組込み機器のアプリケーションとセキュリティ監視＆管理部分を分離
  (NIST IR 7628 SG.SC-3 セキュリティ機能の分離　に準拠)
- 組込み機器のアプリケーションからの通信をセキュアに保護
- **組込み機器アプリケーションを安全に更新可能**
- 起動やシャットダウン、保護されたアプリケーションへのリカバリ、
  モニタリングを管理

Intel Security CIP 仕組みの詳細



IoT向けセキュリティ対策技術
活用例（Industry4.1J）

intel Security

プライベートクラウドを使ったリモート監視サービスの将来イメージ

～セキュアなクラウドで インシデントの検知、原因解析/復旧、改善をサポート～

現場は、セキュアな制御システムでインシデント検知機能を有する。

専門家は、セキュアなプライベートクラウドを利用して世界中の現場をサポート

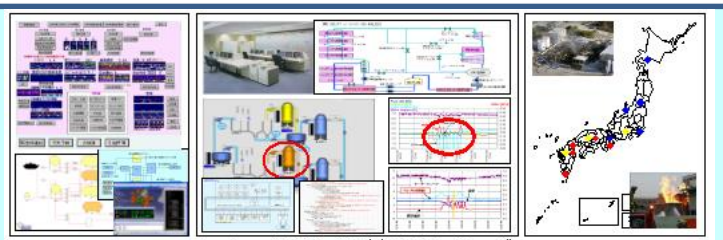
プライベートクラウド

②リアルタイム解析　③ログデータ蓄積

映像データ

制御データ

サーベイランスシステム



サーベイランス監視画面イメージ

計装制御エンジニアであり、制御システムセキュリティ対策の専門家

制御システムの設計経験者なので、使用機器を散って、復旧まで現場をサポートできる。

①データ収集

- 制御システムデータ
- おとりサーバー検出データ
- 検出端/操作端データ

VPN

④現場サポート

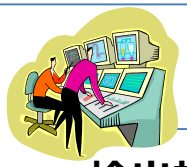
- インシデント検知
- 原因解析/復旧サポート
- セキュリティ改善提案

現場

制御システム

おとりサーバー

インシデント担当者



検出端

操作端

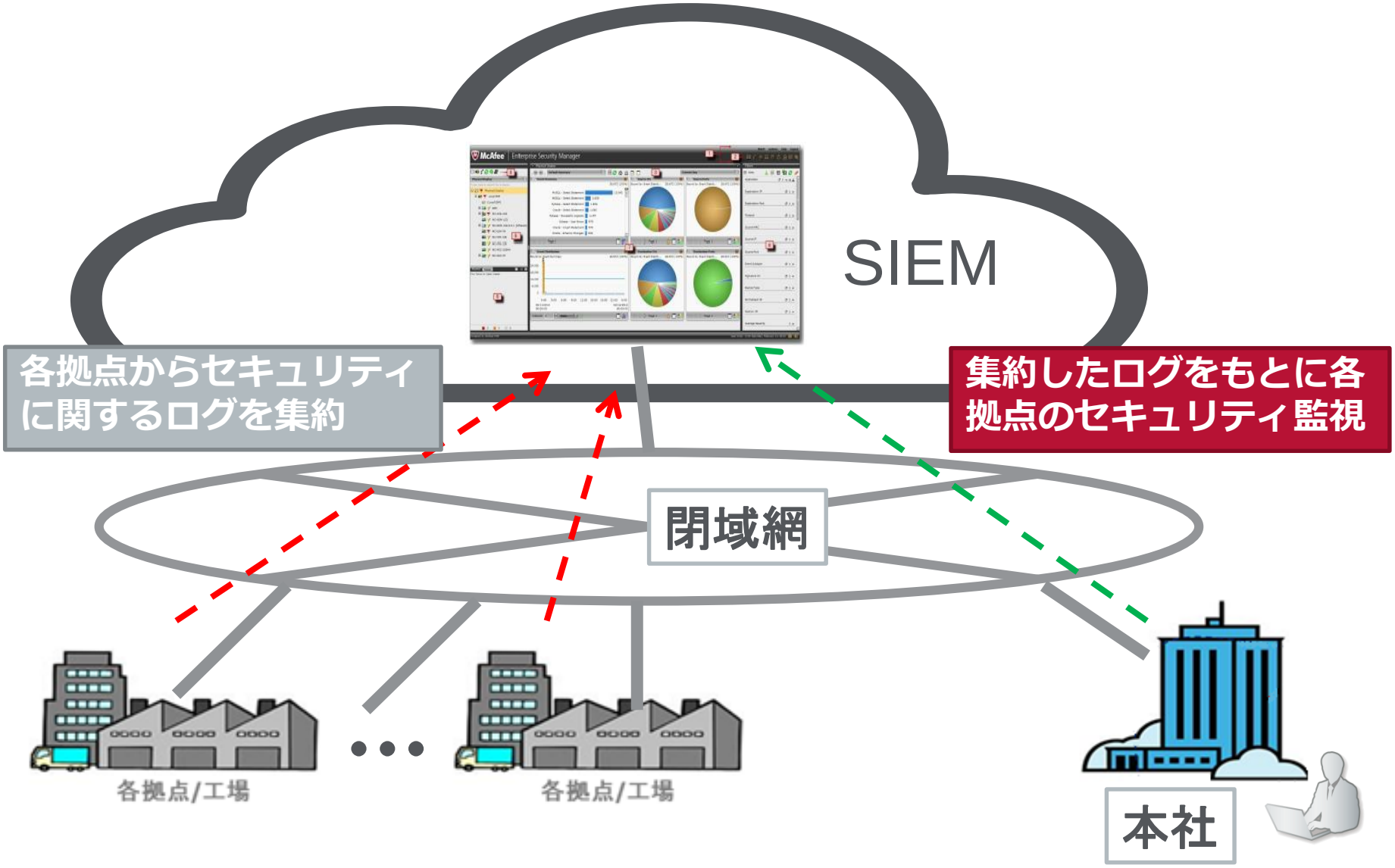
サポート

オフサイト／オンサイト

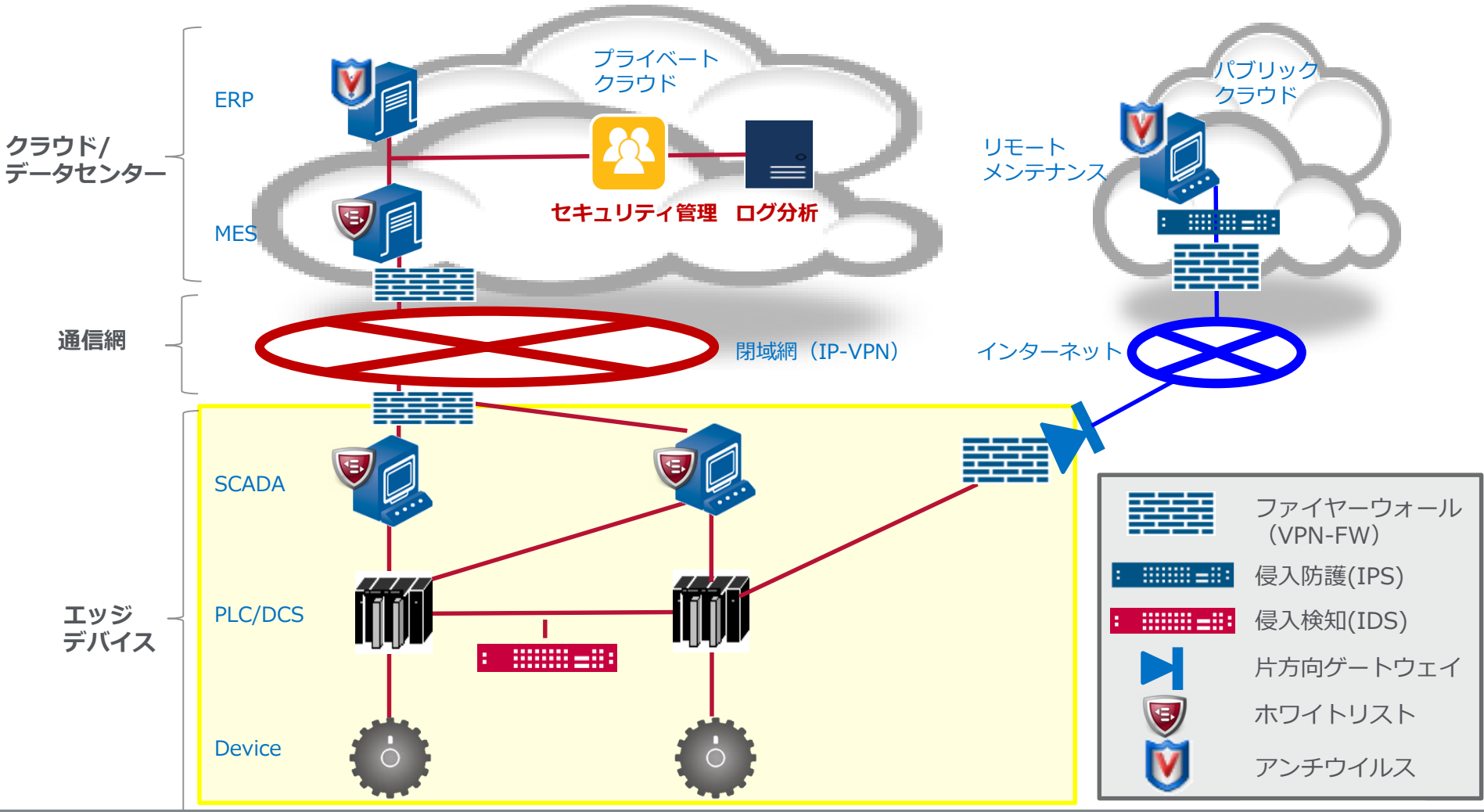
教育／トレーニング

現場の負担を軽減し 安全確保

SIEM使用イメージ（プライベートクラウド）



スマートファクトリーでのセキュリティ適用例



攻撃を受けること前提とし、脅威に応じたメリハリのある対策が重要

参考）IoT業界別セキュリティガイドラインの必要性