トレンドマイクロ　SDN連携活用事例

トレンドマイクロ株式会社

2018年6月

会社概要

What We Do

- IT環境のセキュリティにおけるリーダー
- 革新的なセキュリティソリューションを提供
- ビジネス利用・個人利用双方のお客様を保護

How We Do It

世界の脅威解析の知能を集結

- 世界13ヶ所にある脅威解析センターに約1,200名のスタッフと約1,500名のR&Dエンジニアが在籍。
- TREND MICRO SMART Protection Network™
  世界中の脅威情報を収集、分析・特定し、お客様へリアルタイムでソリューションを提供するクラウド型のセキュリティインフラ。

Who We Are

エバ・チェン
代表取締役社長
兼 CEO

大三川 彰彦
取締役副社長

創業	1988年
本社	東京
従業員数(全世界)	5,970名※
資本金	183億8,600万円※
売上高	1,488億1,100万円※

※2017年12月31日付

デジタルインフォメーションを

安全に交換できる世界の実現

30th

Anniversary

TREND MICRO

トレンドマイクロ業種別取り組みについて

お客様の抱える課題を正確に理解し、最適なセキュリティ対策をご提案するため、業種ごとのアプローチをとっています。

重要インフラ

- 情報通信
- 金融
- 航空
- 鉄道
- 電力
- ガス
- 政府・行政サービス（含・地方公共団体）
- 医療
- 水道
- 物流
- 化学
- クレジット
- 石油

＋

製造分野

- 自動車
- FA/PA

IT＋OT＋IoT

文教分野

- 大学
- 教育委員会

トレンドマイクロ注力業種と主要セキュリティテーマ一覧

業種	セキュリティテーマ	対象	セキュリティ課題
公共	・地方自治体向け強靭化モデル展開	・市町村：政令指定都市	・初動対応迅速化
教育	・教育委員会ガイドライン対応	・教育委員会K12	・文科省ガイドライン準拠
	・大学サイバー対策	・大学	・セキュアインフラ構築
医療	・大規模病院向けサイバー総合対策	・大規模病院	・セキュリティ統制見直し
	・改正個人情報保護法対応/医療等ID対応	・病院全般	・医療情報漏えい対策
	・次世代医療基盤法対応 ・地域医療連携システム安全化	・匿名加工認定業者 ・地域医療連携関連団体	・セキュリティ基準見直し ・D.C.セキュリティ
金融	・メガ金融向けサイバー対策高度化 （・FinTech研究）	・メガ銀行/生損保/証券	・ログ統合監視 （・銀行APIセキュリティ研究）
	・金融庁指針：サイバー対策強化	・地銀/信金/他金融	・金融庁監督指針準拠
製造	・SmartFactoryセキュリティ推進	・自動車 ・FA/PA、他製造	・既設工場への無影響対策 ・新設工場への総合対策
流通	・クレジットカードセキュリティ強化実行計画（EC/POS/加盟店PCIDSS）	・小売 ・POSベンダ	・カード発行会社PCIDSS対応 ・POSセキュリティ強化
他重要インフラ	・重要インフラサイバー対策強化	・鉄道　・航空　・電力 ・ガス　・石油（水道/ビル）	・制御系セキュリティ対策

業種別取組と課題について

各業種で聞かれる共通課題

- 金融
- 地方自治体
- 交通
- 文教
- 医療
- 製造（OT）

◆監督省庁のガイドライン強制力
◆助成金有無

◆経営者の理解
　コストから投資へ

◆態勢構築
　人材不足、IT⇔OT問題、情報整理（情報過多？）

◆人材育成
　経営層、管理層、一般職員層

◆サプライチェーン対策

各業種での取り組み共通項

- 金融
- 地方自治体
- 交通
- 文教
- 医療
- 製造（OT）

◆基幹システムとインターネット接続情報系システムのネットワーク分離

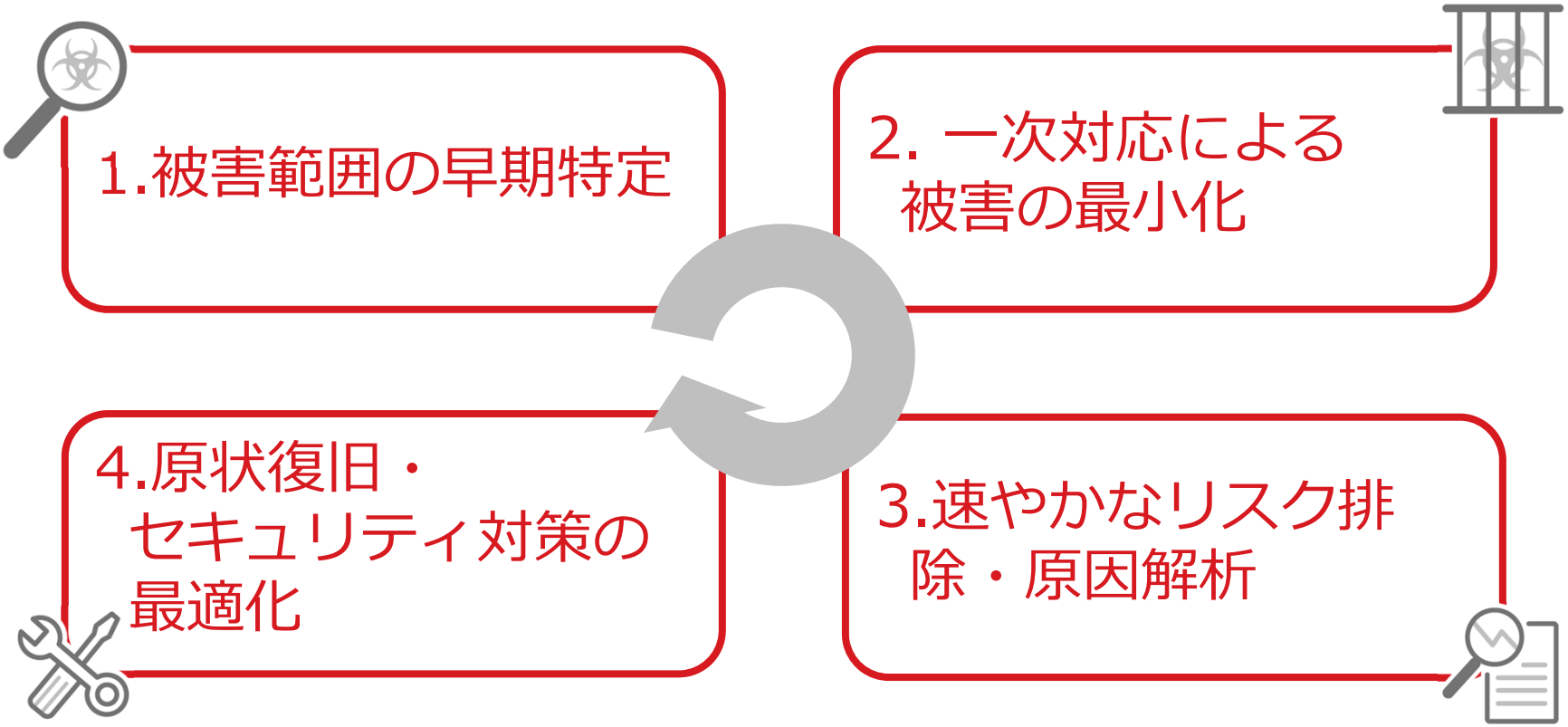
◆多層防御の実装（入口/出口/内部対策）

◆早期検知から迅速な初動対応の重要性

NIST SP800-61（米国国立標準技術研究所）サイバー攻撃対策フレームワークより

◆つながる化に向けたクラウド利用の検討

インシデントレスポンスに必要な要素



被害を最小にする為のソリューション

・早期検知とSDN連携

SDN連携により人的・時間的課題を克服

1.被害範囲の早期特定

2.迅速な初動対応による被害の最小化

SDN連携

リアルタイムかつ高精度で脅威を検知

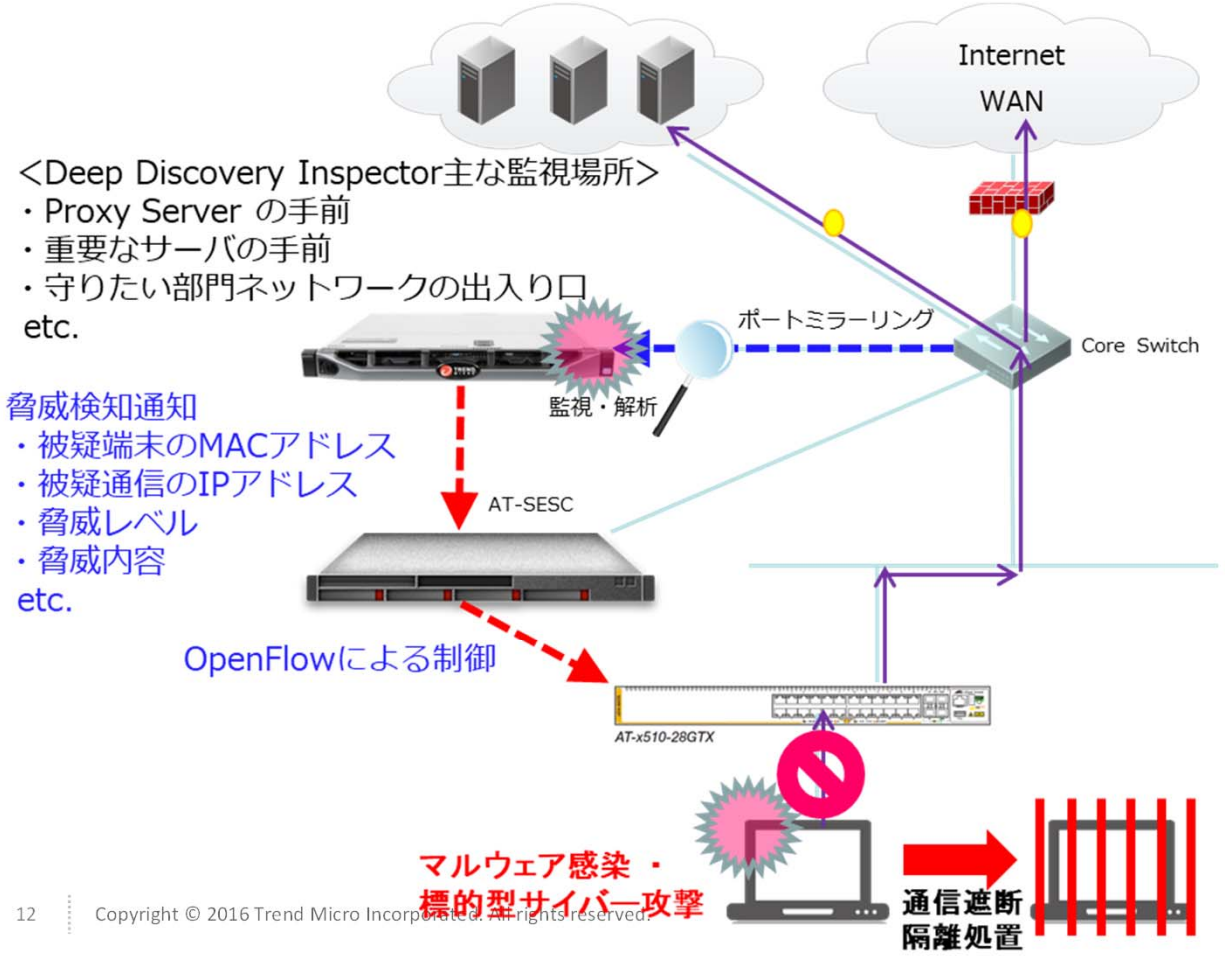
ノード単位でのきめ細かな動的ネットワーク制御

TREND MICRO™

Allied Telesis

TREND MICRO™

SDN連携ソリューションイメージ図



人的効果

- 早期検知
- リスクレベル判断

時間的効果

- 問題箇所特定
- 自動隔離/遮断

- **被害範囲局所化**
- **サービス全面停止回避**

※ 復旧はIS部担当者により問題を解消した後、SDNコントローラーでの操作により復旧。

応用事例

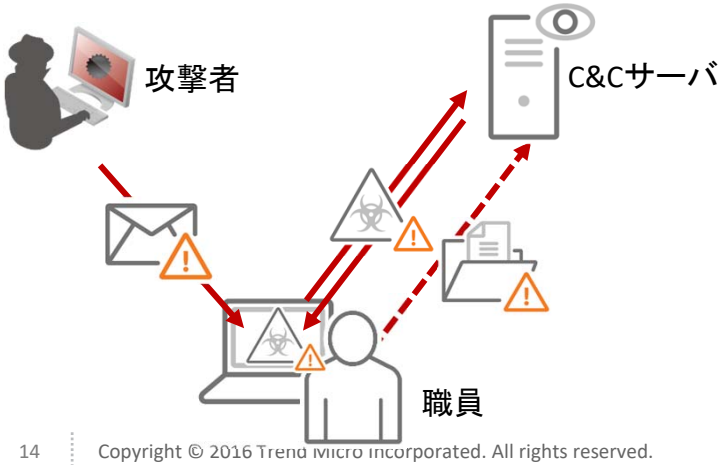
- 田原市役所
- 福井大学医学部附属病院
- 検討が進む工場(OT)分野

【事例：田原市役所①】インシデント

田原市

総務省主導による
「自治体情報セキュリティクラウド」
「自治体情報システム強靭性向上モデル」
に対応。その他セキュリティ対策を講じていた。

＜2016年6月に発生したインシデント＞



職員端末が感染したことを認識

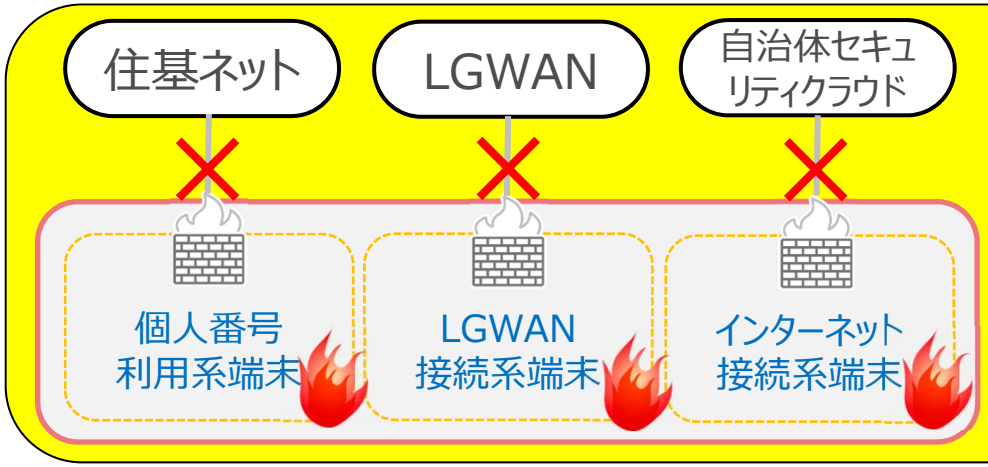
感染端末抜染→NW全遮断、調査

段階的接続回復、調査完了

安全宣言、関係者報告

市民サービスへの影響はなかったが
6日間の業務制限が発生

【事例：田原市役所②】インシデントからの考察



新たな課題の考察

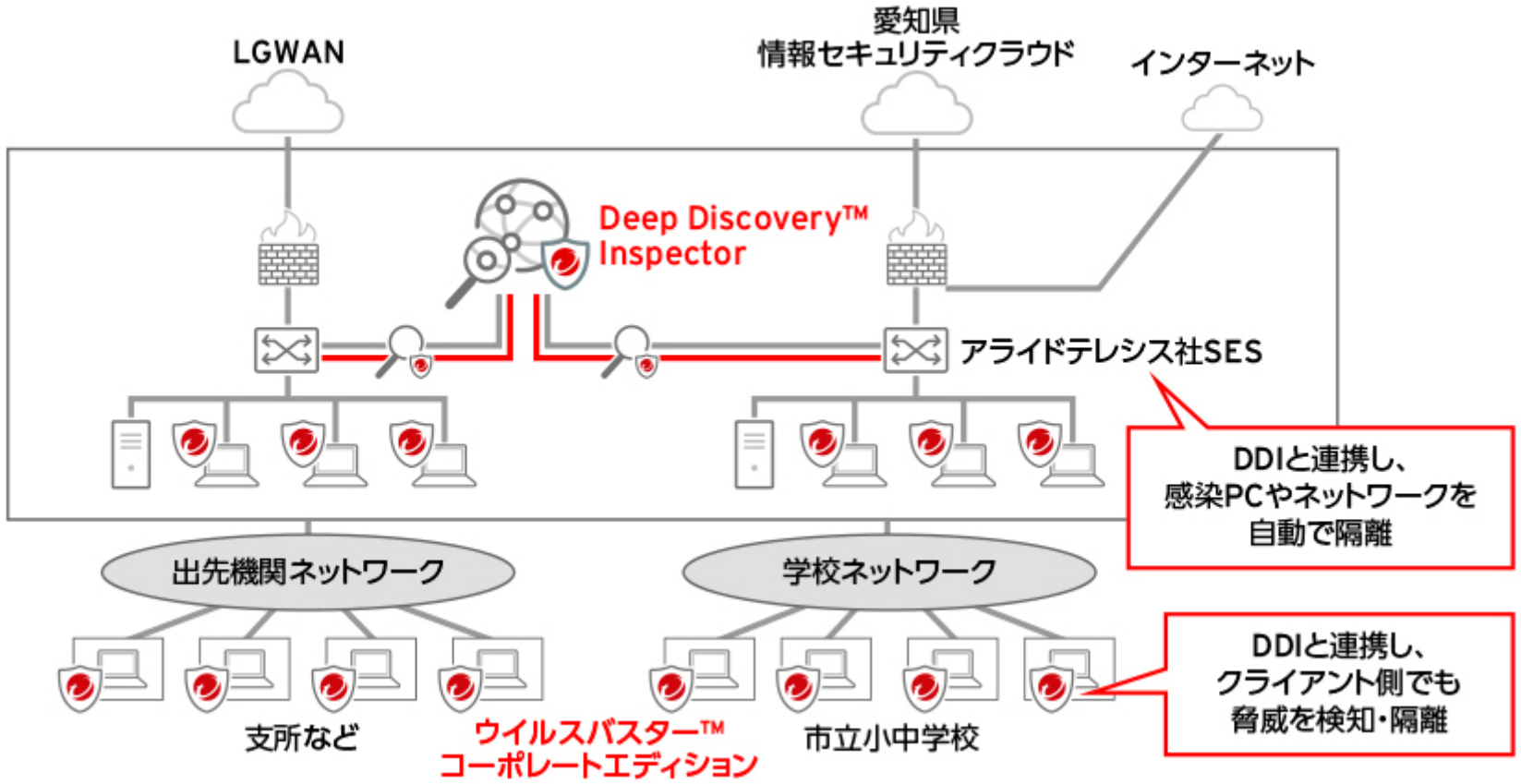
インシデントが発生した場合、安全確認が証明されるまで該当ネットワークに接続できない

地方行政業務へ多大な影響

実施すべき対策

①早期検知と影響範囲の把握
②自動一次対処、および被害の局所化
③調査したインシデント全体像を解明し安全宣言できること

【事例：田原市役所③】導入イメージ

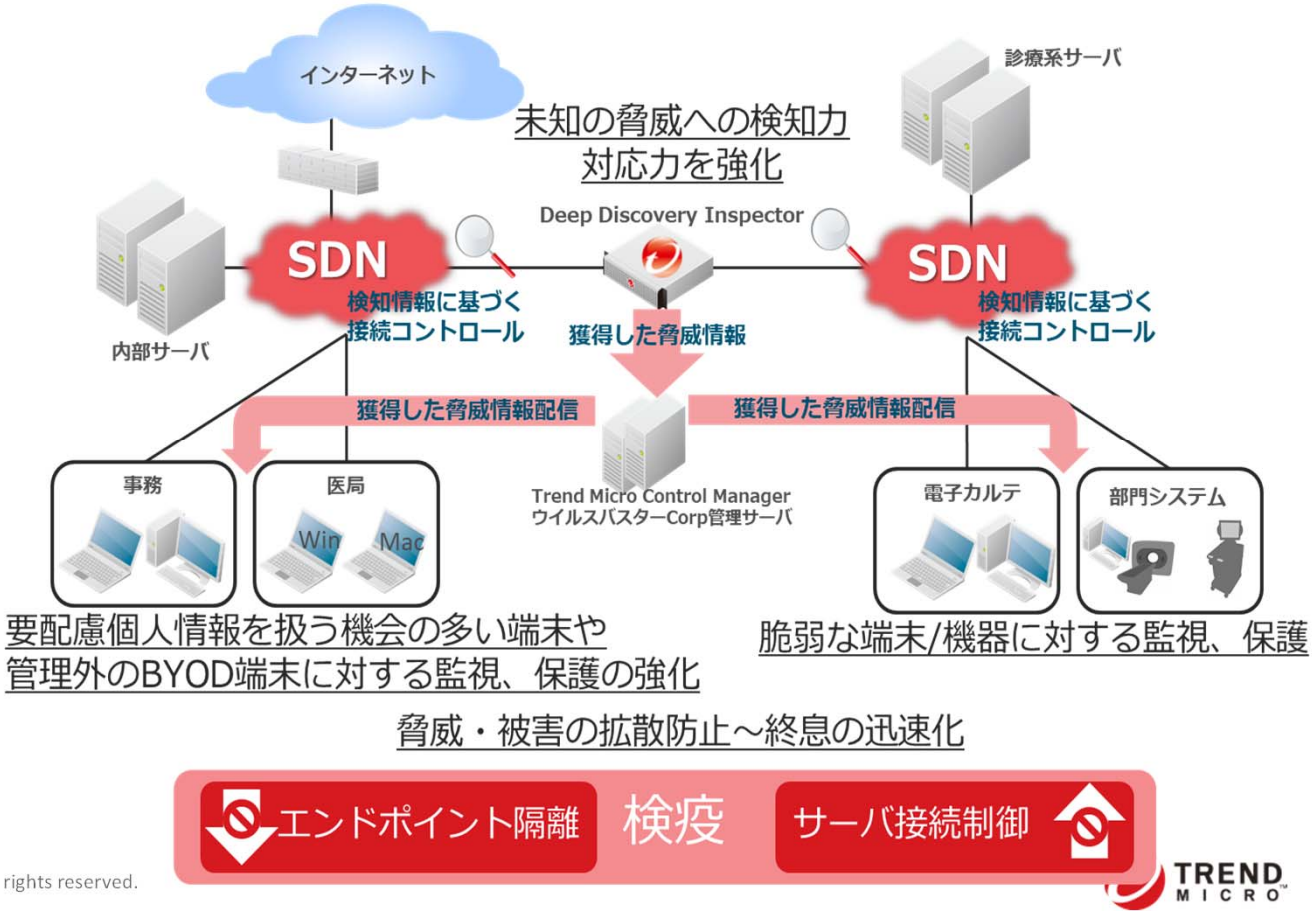


【事例：福井大学①】SDN連携ソリューション導入イメージ

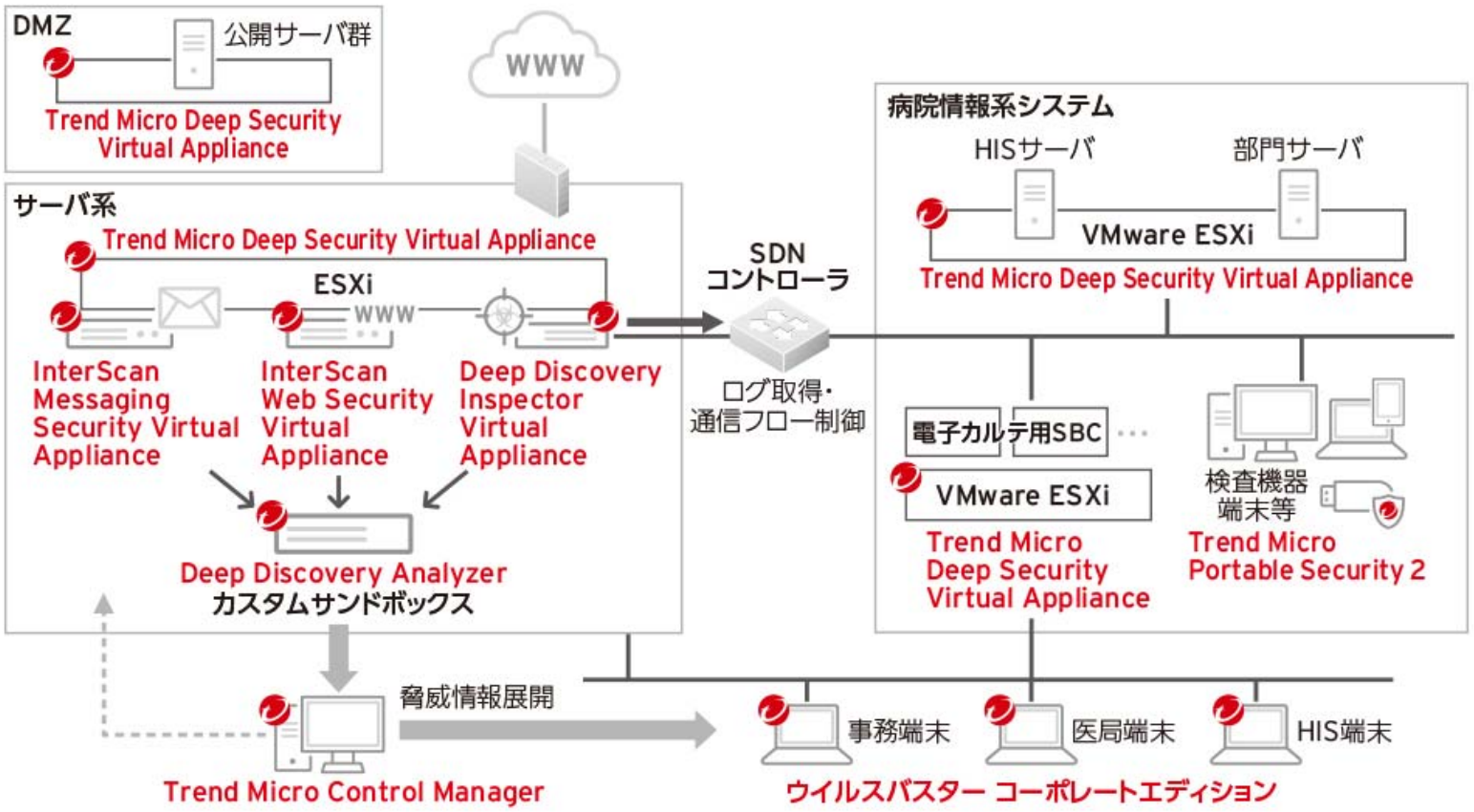
福井大学
UNIVERSITY OF FUKUI

評価頂いた主要ポイント

・侵入前提とした内部検知の仕組み
・一次対応を自動化することで担当者の運用負荷軽減

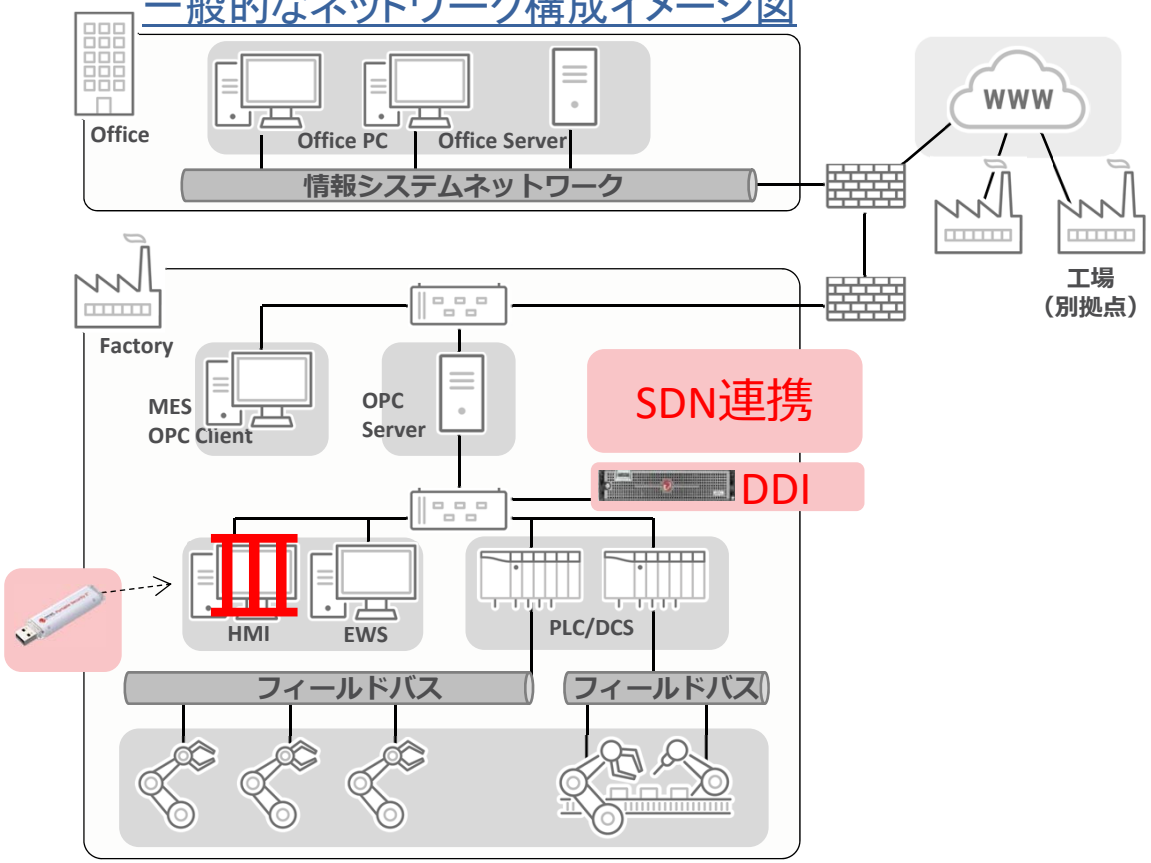


【事例：福井大学②】全体像



【事例：某工場のケース】SDN連携導入検討中

一般的なネットワーク構成イメージ図



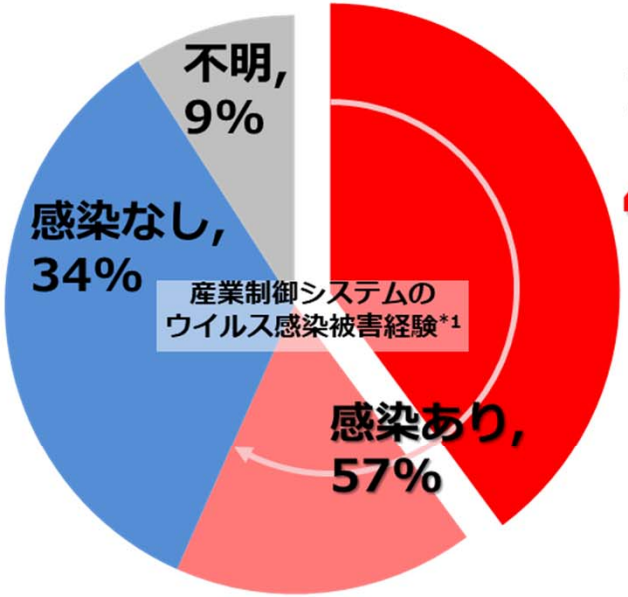
主力工場への強化策

- ウイルス潜伏中の感染端末の発見。
- 発見端末への迅速な初動。
- 従前よりIoTへの対応の為SDN導入を検討していた。

⇒セキュリティ連携が有効である為設計を見直し中。

【参考】

Ref:日本における工場等における被害実態



1年以内に感染あり,
40%

1年以内のウイルス感染経験者の
47%稼働停止経験

出典：
2017年11月トレンドマイクロ調べ
従業員規模300人以上の企業に勤める、産業制御システムの導入・運用に関与している143名にインターネット調査を実施
*1　設問：お勤め先で、あなたが管理する産業制御システムにおいて、コンピュータウイルス感染の被害にあったことはありますか？

まとめ

被害拡大の岐路となる初動をSDN連携でリスク低減

- 金融
- 地方自治体
- 交通
- 文教
- 医療
- 製造（OT）

◆早期検知から迅速な初動対応の重要性

NIST SP800-61（米国国立標準技術研究所）サイバー攻撃対策フレームワークより

SDN連携

リアルタイムかつ高精度で脅威を検知

ノード単位でのきめ細かな動的ネットワーク制御

TREND MICRO™

Allied Telesis

TREND MICRO™

ご清聴ありがとうございました。