巧妙化したサイバー攻撃への対策、即断すべき企業ネットワークの見直し！

セキュリティ対策の本質はサイバー攻撃被害を最小限に抑えること、
今こそ、強靭化ネットワークへの投資が必要

2018/6/21

アライドテレシス株式会社
中島　豊

Allied Telesis

目次

- 情報インシデント ― サイバー攻撃の現状（国内）
- 現在のサイバーセキュリティ対策
- **New!** SDNを活用したセキュリティ対策のご紹介
  - 運用コストを抑えかつ強靭化を図る対策の紹介
- 産業IoTシステムに対するSDNのサイバーセキュリティ
- アライドテレシスのサイバーセキュリティへの取組

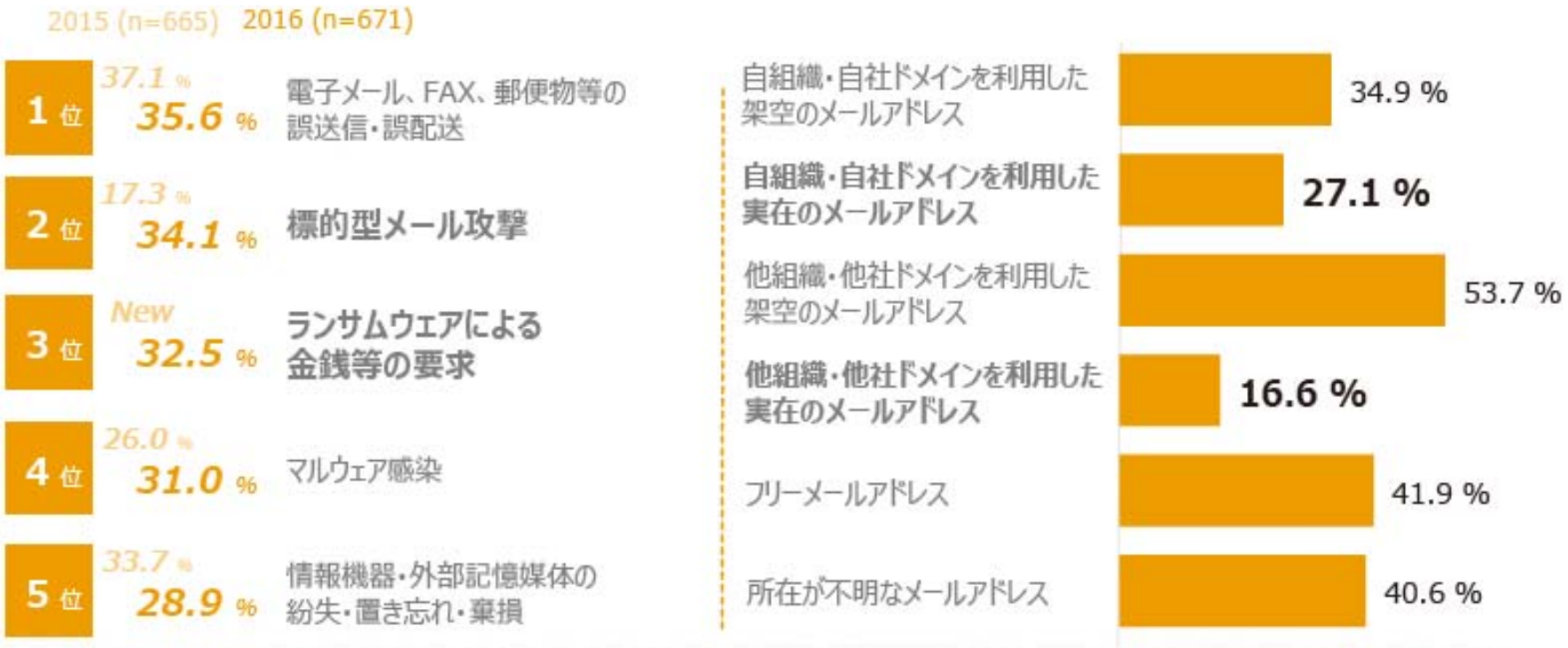
情報インシデント ― サイバー攻撃の現状（国内）

2016年度の国内の情報インデントの現状

近年の発生原因はサイバー攻撃が増加！ヒューマンエラーとほぼ同値！

出典：NRIセキュアテクノロジーズ社　企業における情報セキュリティ実態調査2017

2016年度の国内の情報インデントの現状

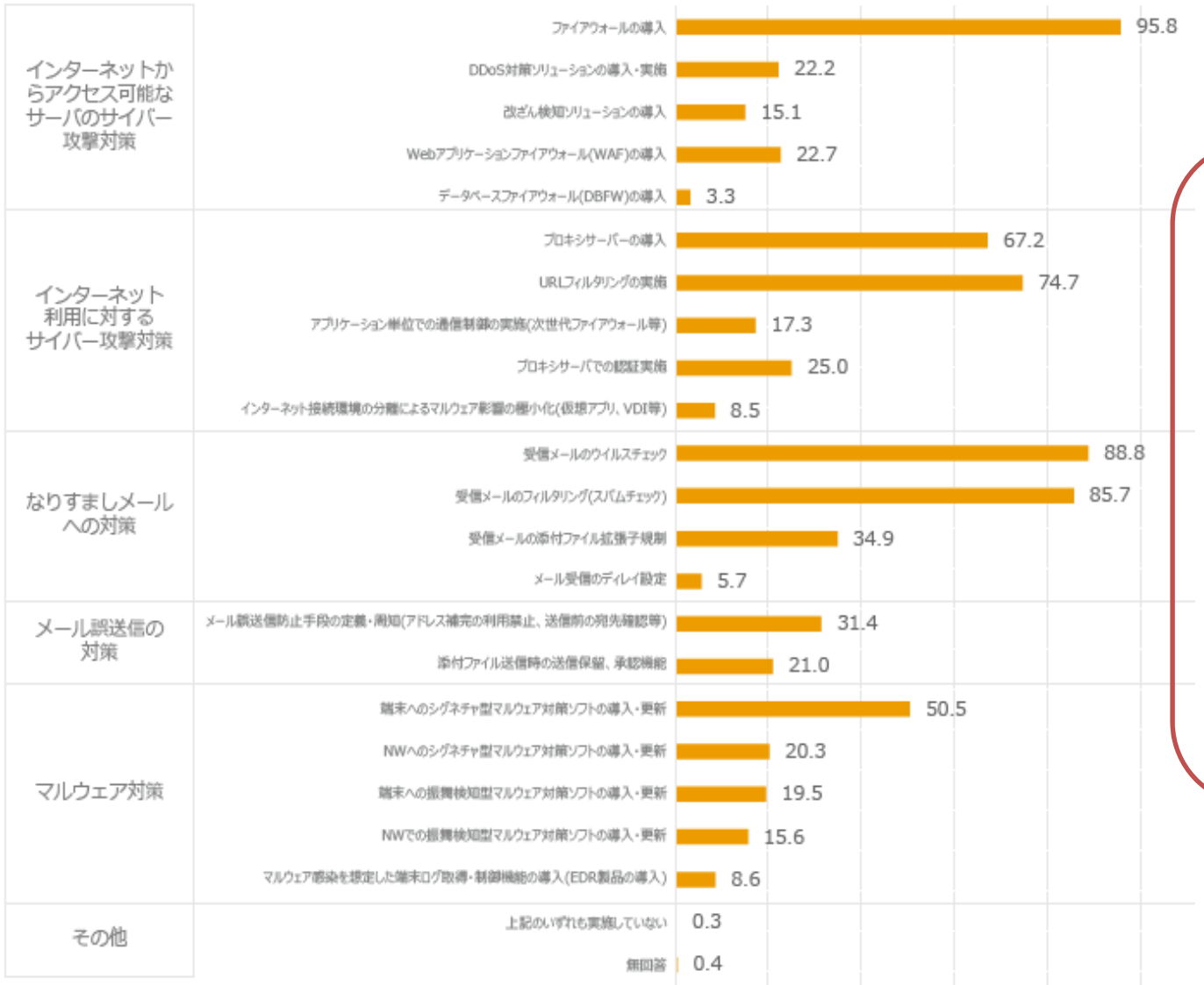


出典：NRIセキュアテクノロジーズ社　企業における情報セキュリティ実態調査2017

攻撃メールの内容が巧妙化！
ランサムの金銭要求が依然猛威を振るっている！

3割以上の企業が情報インシデントを経験！

各企業の対策状況



既知のサイバー攻撃対策のポイントは高い

未知の攻撃に対する対策は低い

出典：NRIセキュアテクノロジーズ社　企業における情報セキュリティ実態調査2017

現状！存在する管理できない侵入ポイント

社員PC内の情報保護機能に対する操作監視
Windows ファイアウォールのカスタマイズ、共有フォルダ設定など個別管理チェック

クラウドサービスと個人利用＝シャドーITの発生
企業で管理されていないSNSやファイルサービスからの感染の発生

モバイル端末の社外利用状況の把握
社外で利用するモバイル端末のインターネット利用およびアプリケーションのインストール

社内端末の外部インターフェースの使用
モバイルルータや**USBメモリ**の個人利用

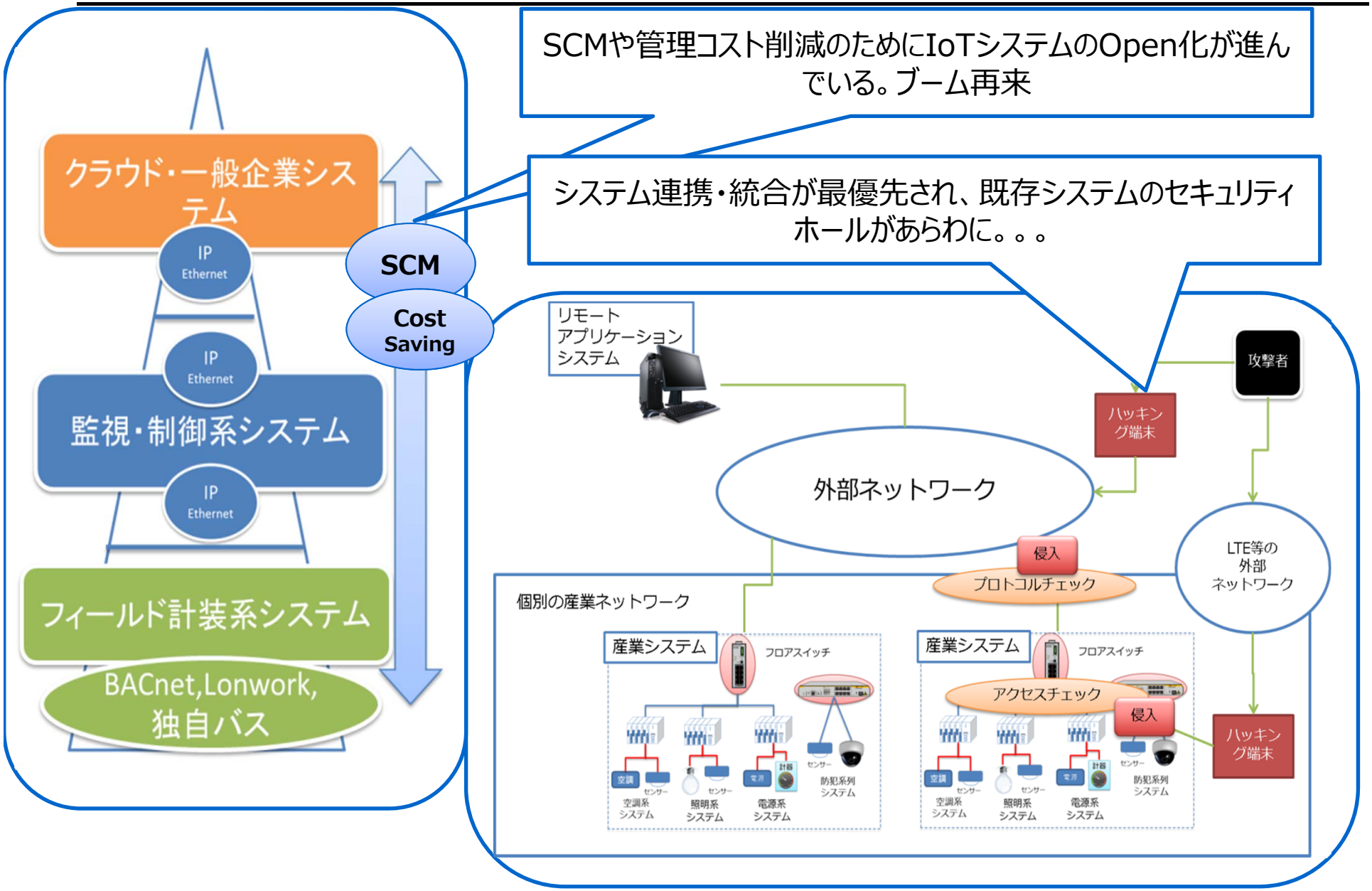
社員宛てメールの内容チェック
メールの内の**圧縮添付ファイルやURL記載**

上記ポイントをすべて社内の情報システム部がチェックすることは不可能！

Open化が迫ってる産業システム

SCMや管理コスト削減のためにIoTシステムのOpen化が進んでいる。ブーム再来

システム連携・統合が最優先され、既存システムのセキュリティホールがあらわに。。。



産業IoTシステムへのサイバー攻撃について

- 流れ、環境。。
  - 一般企業のアプリケーションと工場、ビルのオートメーション化とリモートモニタリング、病院の情報システムの共有化を背景に個別の通信プロトコルがEthernet/IP化されてきている
  - 個別のシステムは閉域網内から外部ネットワークに部分的に開放されつつある。
- サイバーセキュリティの脅威
  - セキュリティ対策まで計画が立たない
    - データ結合1st！異なったシステムの連携・連結のところでシステム改革は終わり、、外部侵入対策は2の次
  - 閉域システムに対するハッキング脅威はOAに比べると比較的楽。
    - システムの動作OSが古いまま
    - 制御システムの区分がない
    - そもそもハッキングされることが考慮されていない
  - 攻撃対象に対するハッキングがビジネスになる。

現在のサイバーセキュリティ対策

サイバーセキュリティに関する製品・サービス

ネットワーク型セキュリティ

Gateway型セキュリティ
- UTM
- Firewall,WAF,IPS/IDS
- DDoS
- アンチウィルス
- マルウェア・アンチスパム
- VPN
- サンドボックス
- ホワイトリスト
- Proxy

モニタリング型セキュリティ
- AI/ML
- ホワイトリスト
- 相関分析

SDN型セキュリティ
- ホワイトリスト
- ブラックリスト

エンドポイント型セキュリティ

ウィルス対策ソフト
- シグニチャマッチング
- AI/ML

資産管理型セキュリティ
- パッチチェック
- ユーザアクションチェック
- 資産履歴

2要素認証セキュリティ
- 指紋
- IDカード

MDM
- 遠隔ロック、データ消去
- トラッキング

暗号化
- HDD,暗号化

サービス型セキュリティ

Managed Security サービス
- SOC委託：IPS/FW/SIEM

脆弱性診断サービス
- Web診断
- 社内サーバ診断

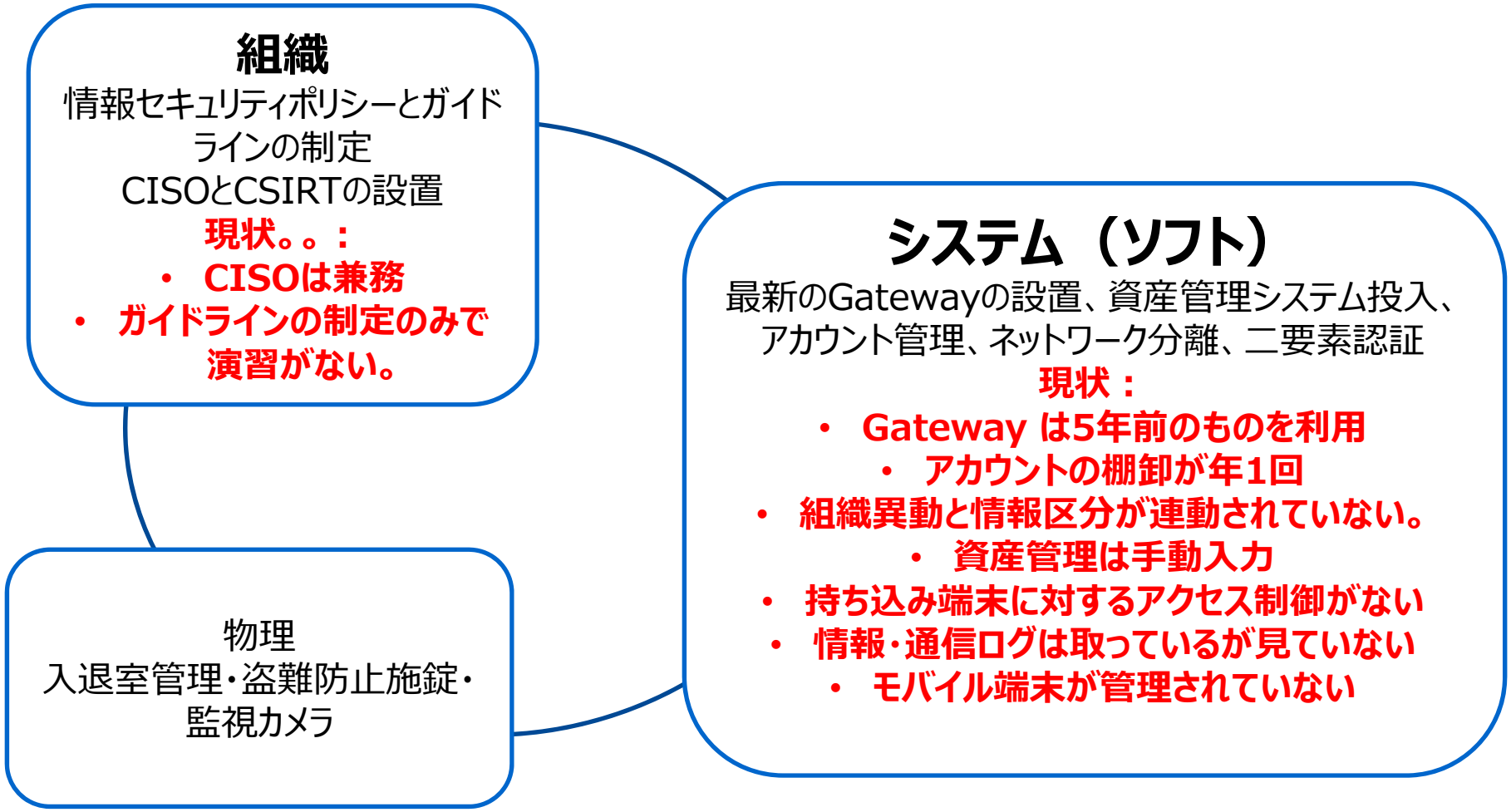
サイバーセキュリティ演習
- 講習・アンケート型演習
- シュミレーション型

サイバー攻撃保険

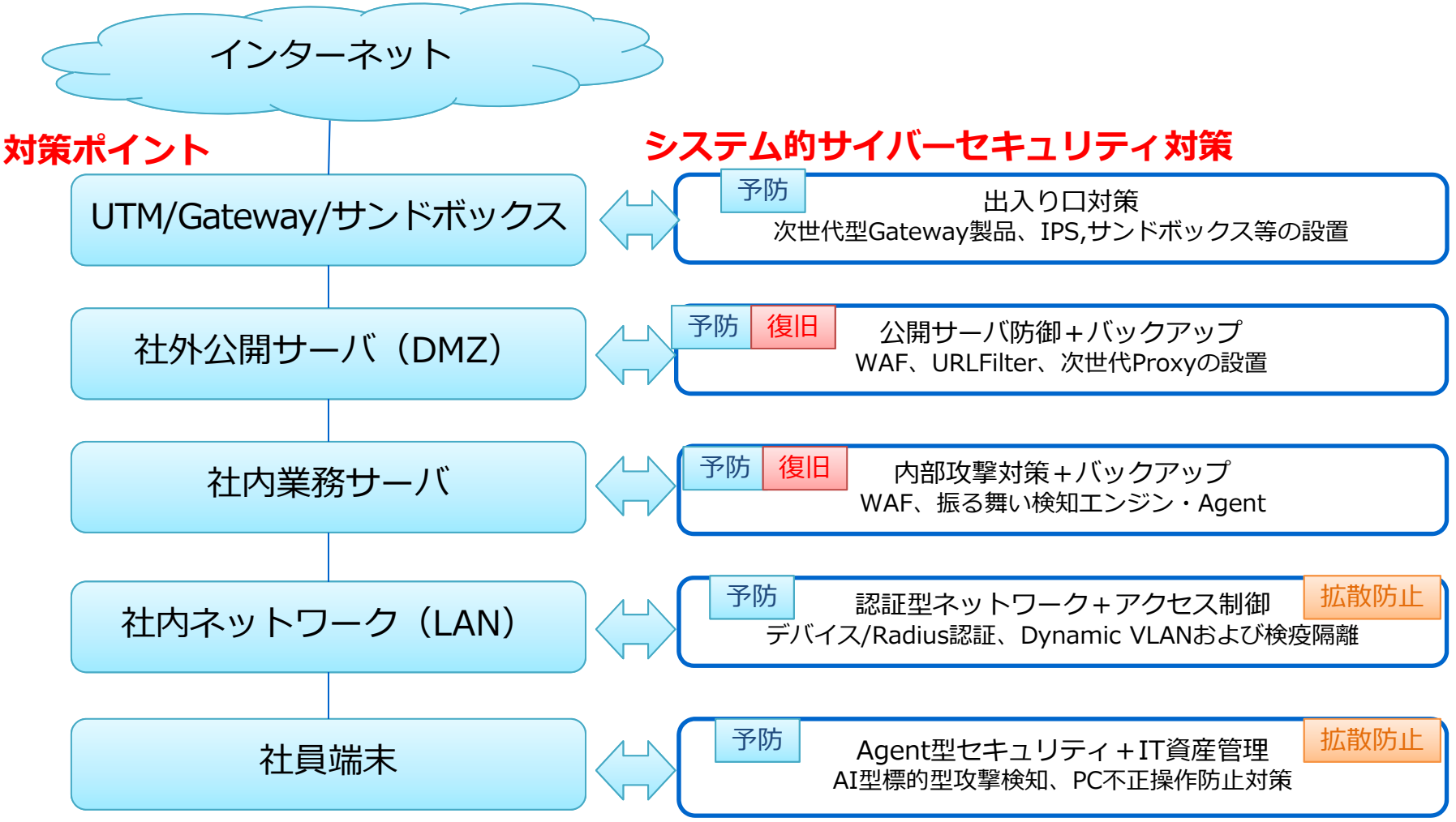
アライドテレシス
ソリューション

人（組織）ー物理ーシステムでのセキュリティ

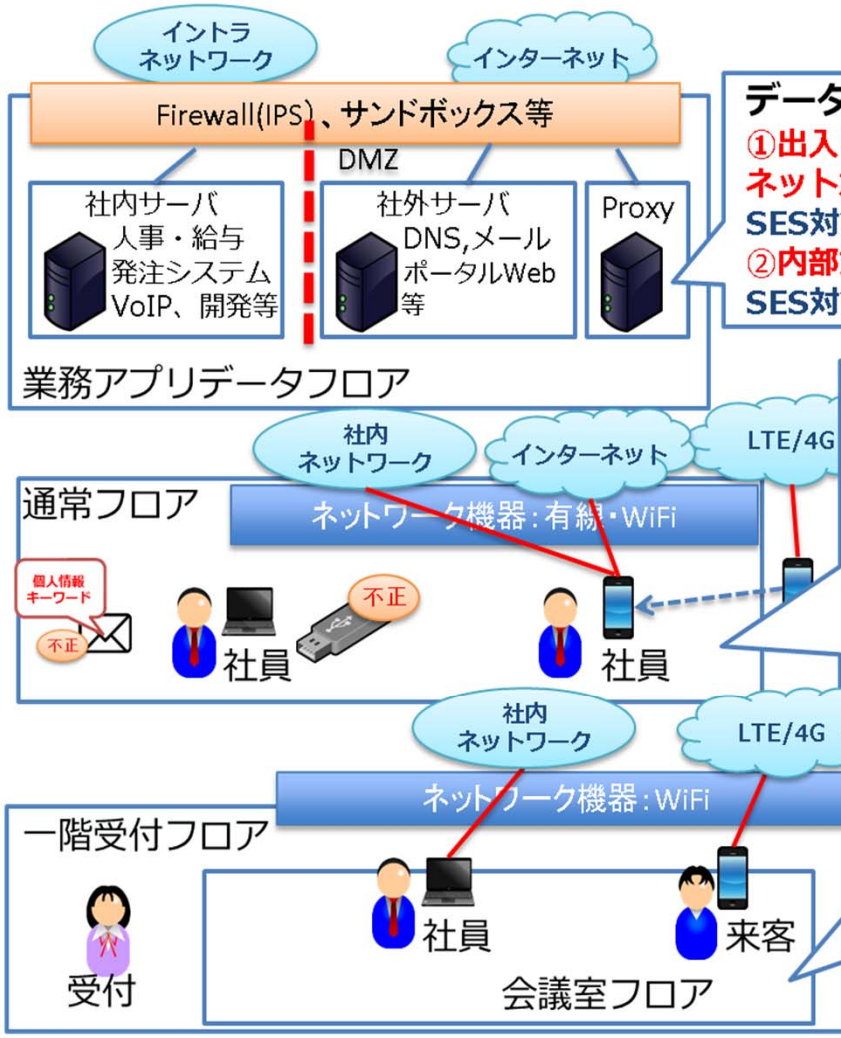
ほとんどのガイドラインが組織と物理セキュリティとシステム（ソフト）の規定について言及。
現状は。。。。



一般企業のサイバーセキュリティ製品の配置



配置イメージ



データフロアのセキュリティポイント

①出入り口対策：次世代Gatewayの設置、サンドボックス等によるインターネットからの攻撃手段を排除

SES対策：インターネットVLANへ動的割付

②内部対策：ユーザ端末からの踏み台攻撃対策 社員端末からの防御策

SES対策：Gateway製品のLogから社内端末からの情報漏えいを未然に防ぐ

通常フロアのセキュリティポイント

①外部ネットワークアクセスした端末の接続

SES対策：安全な端末しか社内サーバへ繋がない。

②社員の不正操作の管理

メール送信、USBメモリ利用を監視

SES対策：資産管理と連動し、怪しい操作を行った端末の社内リソースへのアクセスは許可しません

来客フロアのセキュリティポイント

①社員端末とゲスト端末のアクセスの分離

SES対策：社員端末は社内ネットワーク、ゲストはインターネットVLANへ動的割付。

②営業時間外無線利用の禁止

SES対策：無人のオフィス等は無線APアクセスを不可

今日のサイバーセキュリティ対策（システム）

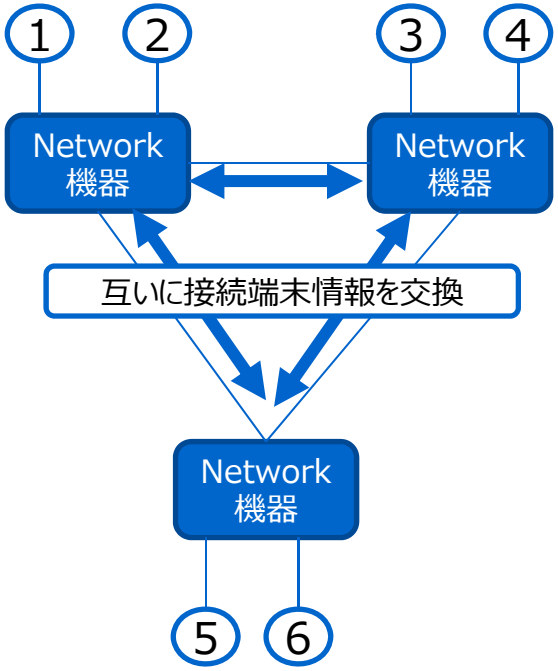
- 回答：**多製品による多層化防御が必要**
  - 事実
    - **１００％防げるといった単一セキュリティシステムは存在しない**
    - 3年以上前のGateway製品は意味がない
    - アンチウィルス対策製品だけでは守れない
    - インターネットからだけではなく、内部からの侵入が多い
    - モバイル端末が感染元
    - シャドーITは防げない
  - Why??
    - 未知の脅威から情報インシデントがほとんど！
    - 一人当たりが保有する情報端末が増加！脅威の侵入経路も増加！
    - モバイル端末利用が当たり前！
  - デメリット
    - **セキュリティ製品のインストールとメンテナンスには工数がかかる！**

New! SDNを活用したセキュリティ対策のご紹介

運用コストを抑えかつ強靭化を図る対策の紹介

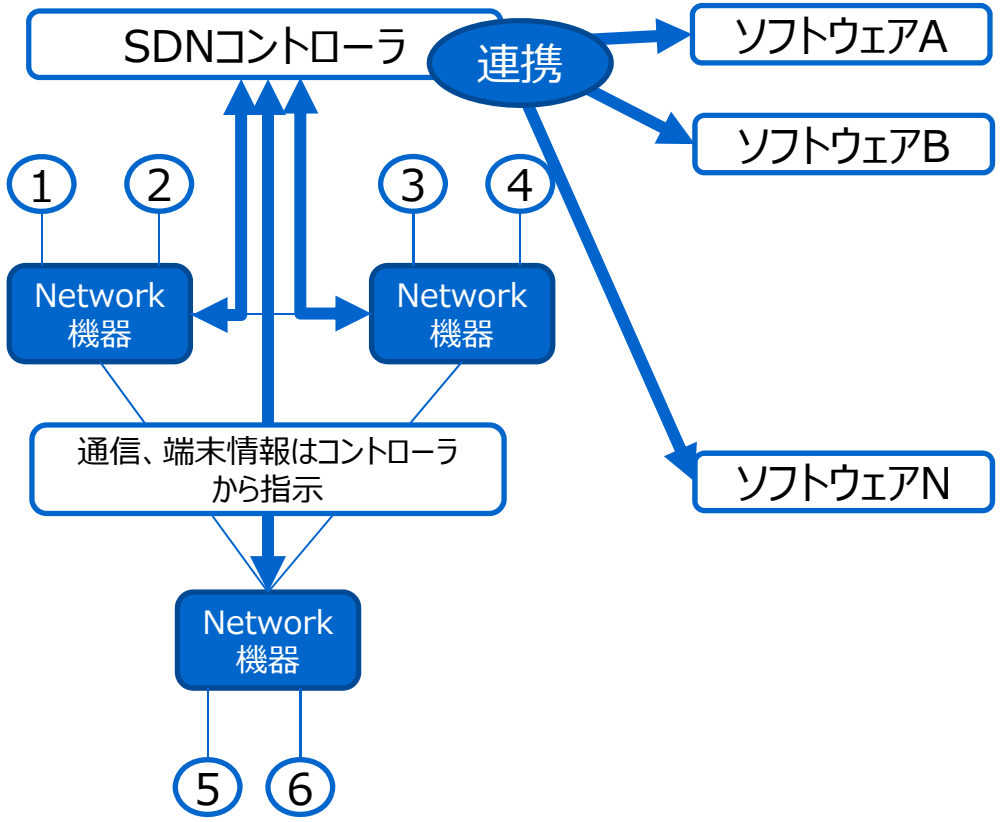
SDN(Software Defined Network)とは？？

- レガシーEthernet/IP



ネットワークにつなげたものは
つなげる思想

- SDN



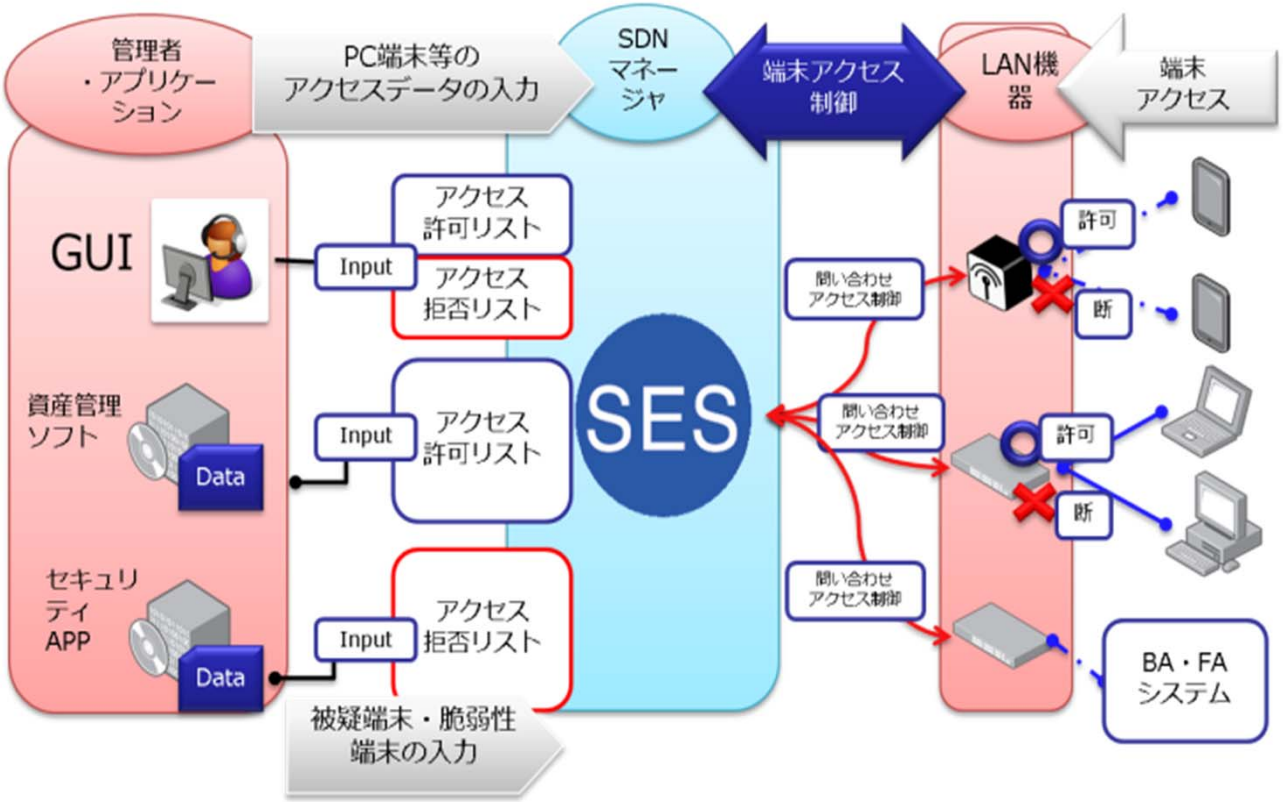
コントローラから許可された
通信のみを行う思想

セキュリティ製品と組み合わせたSDN

他社との違い

連携アプリケーションの多さ

- SESとはSDNマネージャから端末のアクセス制御を行うシステム
- アクセス制御情報を様々なセキュリティ製品と連動することが可能



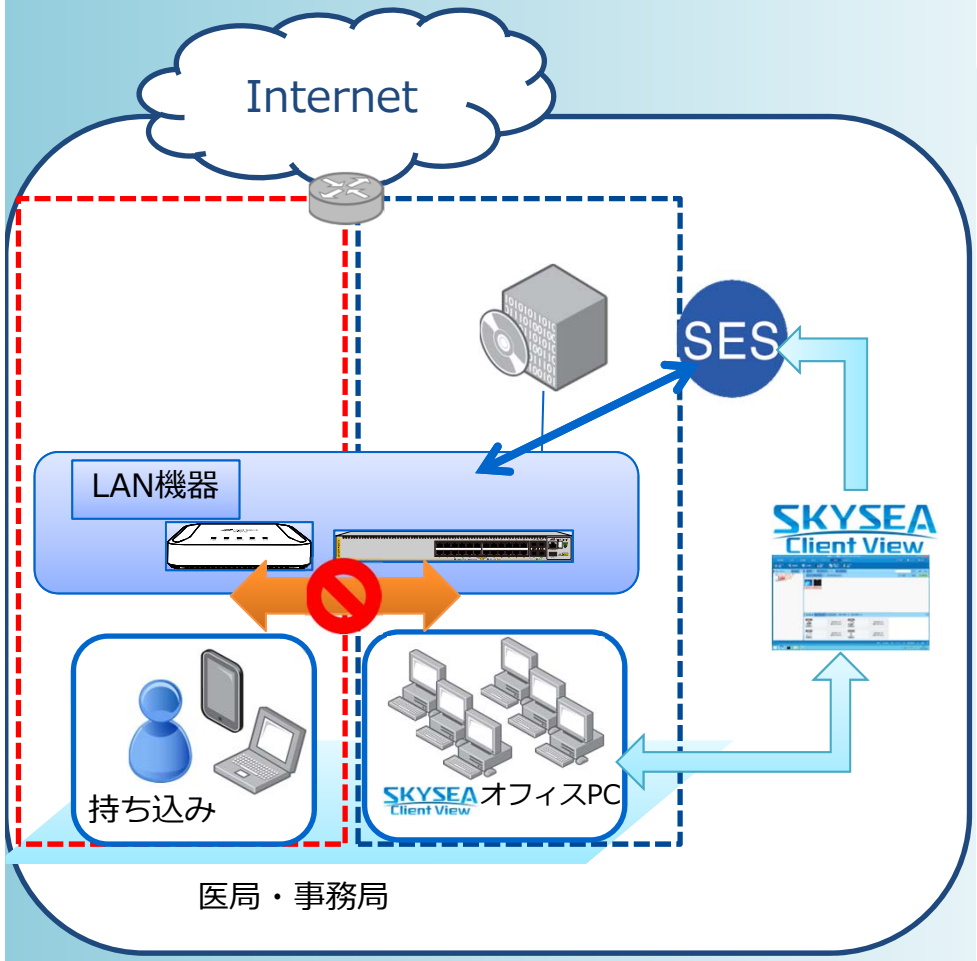
多層化防御を連動させるSDN

SDNのセキュリティ対策の利点

- 情報インシデントリスクの軽減
  - 認証済み端末及びサーバのみを企業ネットワークつなげることをシステム的に判断する為、セキュリティホールの数が軽減。
  - 各種セキュリティ製品が“黒（ブラック）”と判断したものは隔離される
    - UTM~エンドポイントで検出した隔離対象の端末をネットワークの設定を介さず検疫隔離が可能
    - 違反行為（私用USBや外部ネットワークの無断接続）をした端末PCなどの指導隔離＝サイバーセキュリティ運用コストの軽減（SOCの運用コストの軽減が可能）

- ネットワーク運用コストの軽減
  - 資産管理台帳に登録された端末情報をもとにネットワークを自動構成できる。

資産管理連携によるホワイトリスト制御（例：SKY）



対象

- エリア：一般企業
- 端末：PC,サーバ 持ち込み情報端末

機能

SKYSEA Client View

情報端末資産管理
端末に関するログ管理
不正操作管理

SES

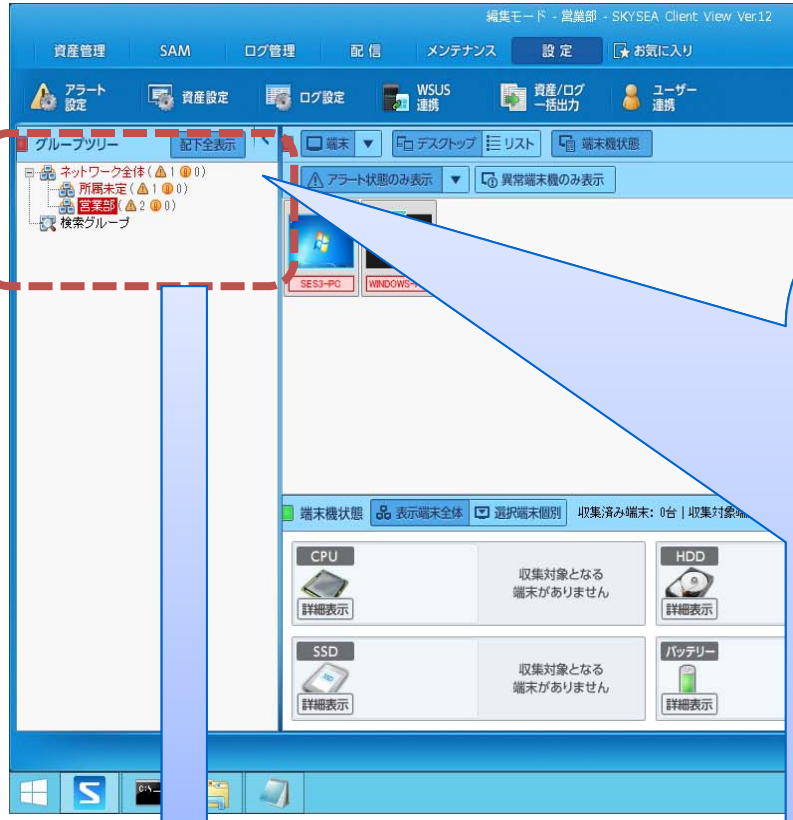
情報アクセス区分
ゲストネットワーク提供

連携効果

ネットワーク機器設定工数の大幅削減
- 情報アクセス区分に対する管理端末の自動割付
- デバイス情報の入力が不要！

持ち込みデバイスとの自動セグメンテーション
- 持ち込みデバイスは自動的にインターネット接続VLANに接続情報アクセス区分
- ゲストネットワーク提供

資産管理とネットワークセグメントが一元管理



SKYSEA Client View連携ならでは機能紹介！

①SKYSEA Client ViewにPCを登録するだけでネットワークが連動！

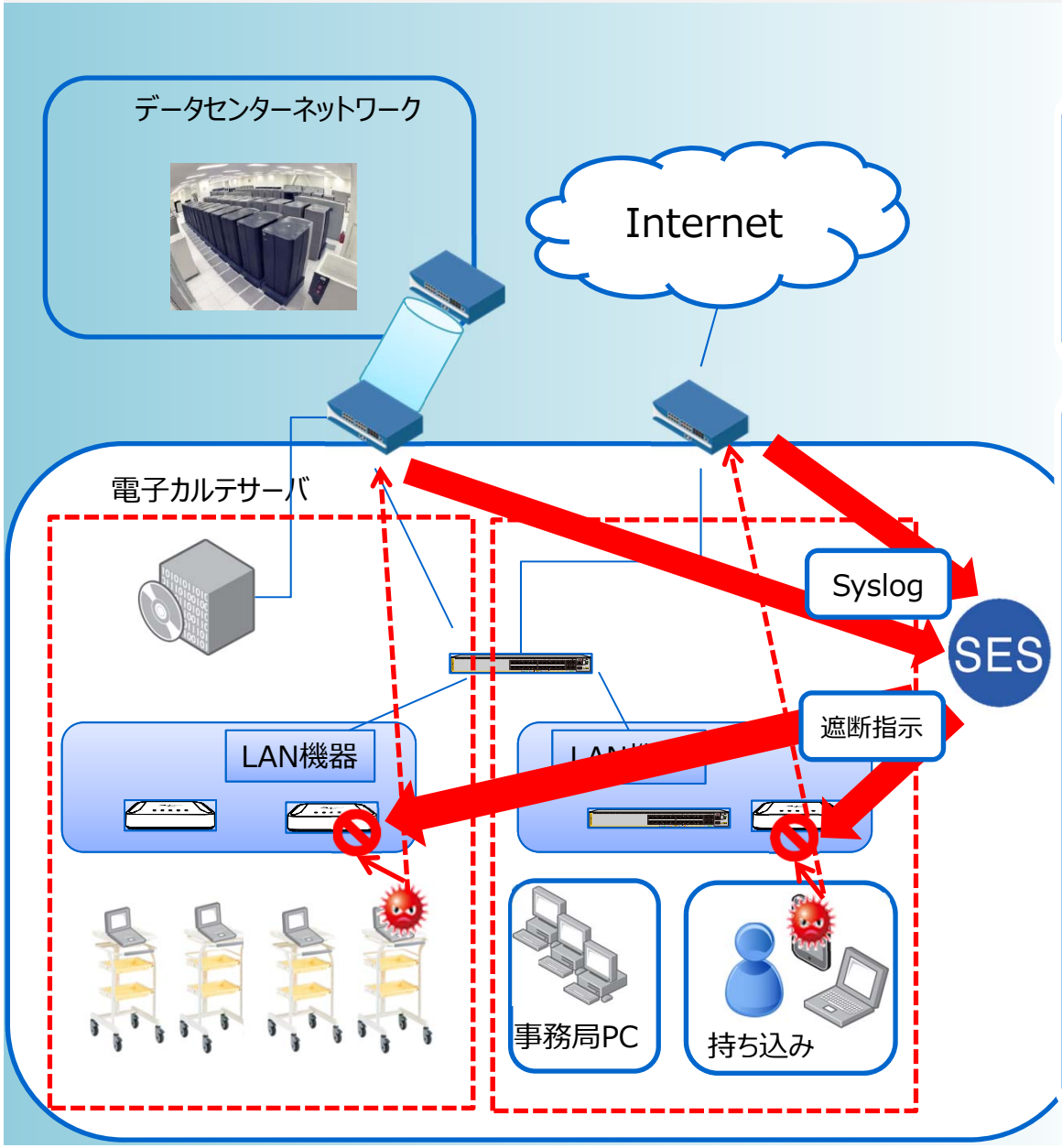
- 面倒なネットワーク機器に対するデバイスアクセス設定が不要になります。

②事務局、部門など端末と所属セグメント設定もSKYSEA Client View設定から可能！

- 端末の所属部門をVLANにかえ、ネットワーク機器に自動設定！

ネットワーク設定工数が大幅に削減できます！

UTM連携SES



対象

- エリア：一般企業フロア全般
- 端末：業務端末、一般社員PC、スマートフォン

機能

Gateway機能

インターネットファイアウォール
重要サーバエリアファイアウォール

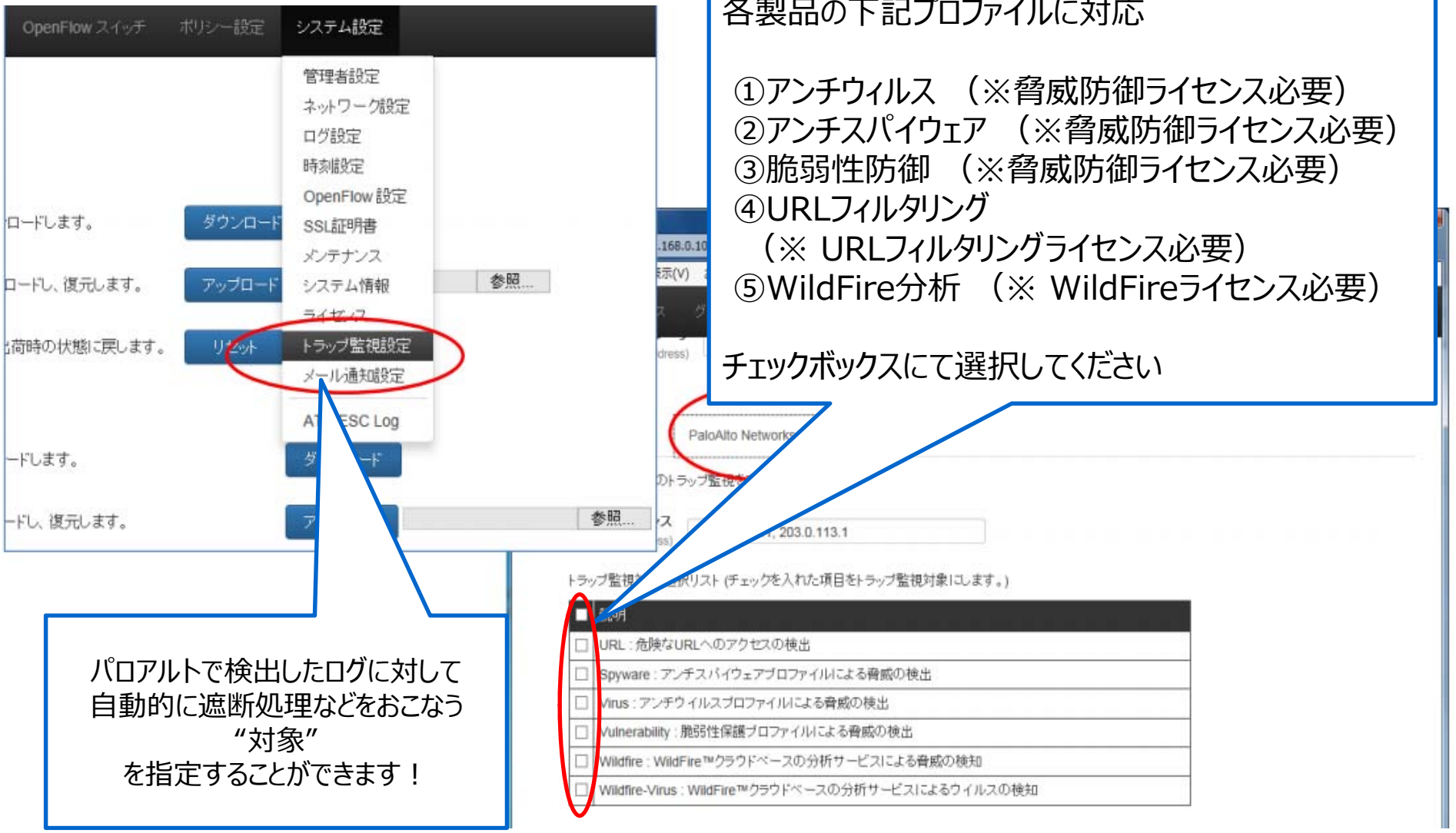
SES

情報アクセス区分
無線電子区分のアクセス制御

連携効果

感染被疑端末通信検知に対する自動隔離による拡散防止

隔離対象設定の選択



トレンドマイクロ社製品との連携

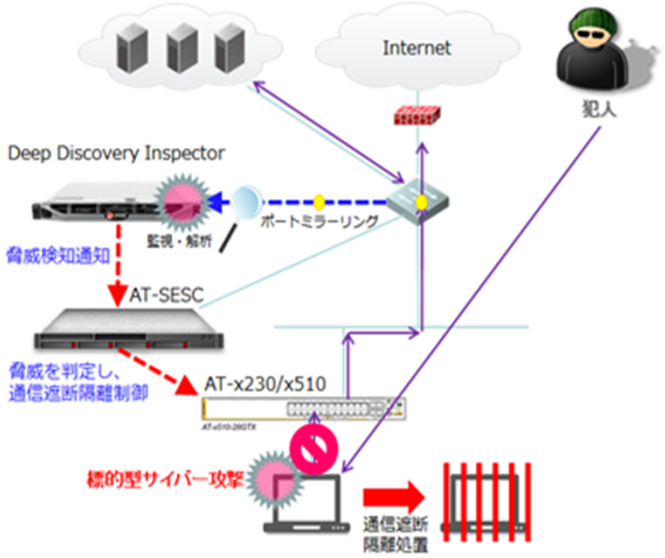
Deep Discovery™Inspector
ウイルスバスター™ Corp.

✖

Secure Enterprise SDN

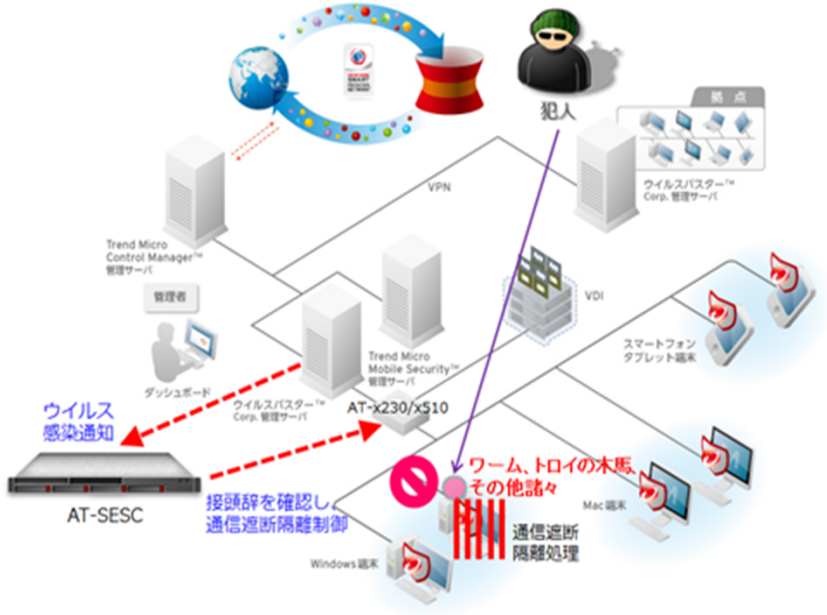
◆ **ふるまい検知**

「Secure Enterprise SDN(SES)」 は
Deep Discovery Inspectorと直接連携し、標的型
サイバー攻撃を受けている端末をエッジスイッチで
遮断隔離します。



◆ **ウイルスバスター連携**

SESはウイルスバスターと連携し、ウイルス感染端末を
エッジスイッチにて抜線、通信を遮断し自動隔離します。
（2016年5月リリース）



産業IoTシステムに対する
SDNのサイバーセキュリティ

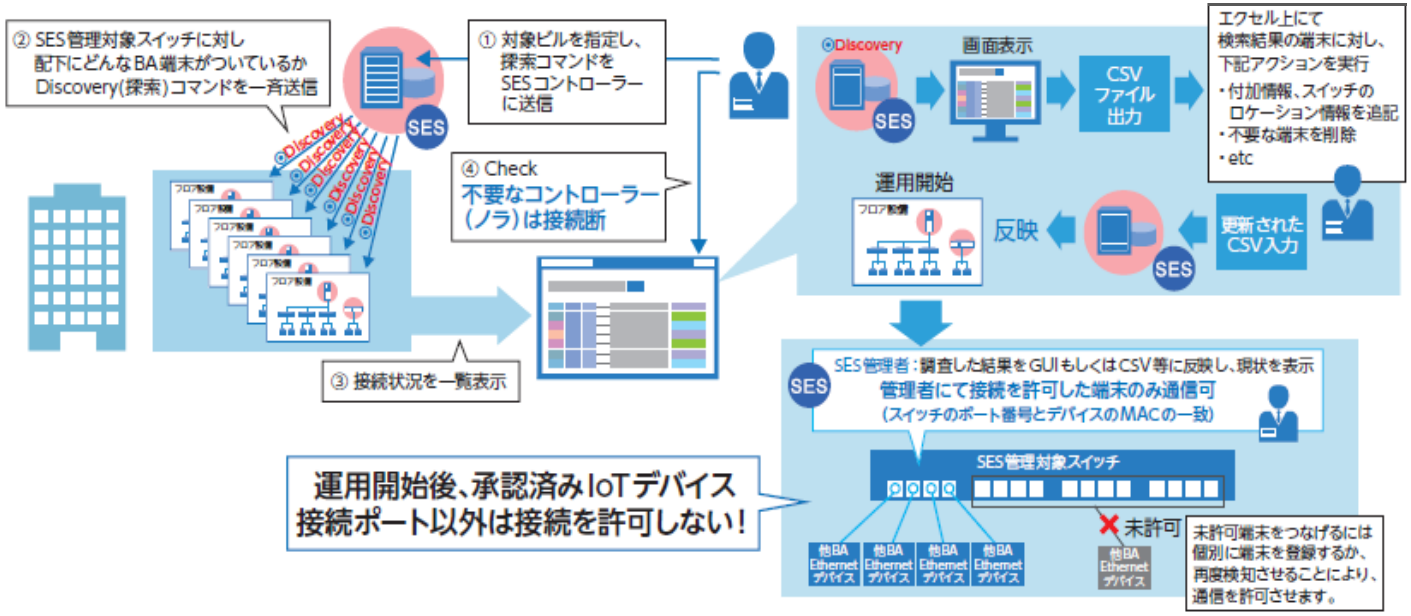
産業IoTシステムのサイバーセキュリティのポイント

- ビル・工場・病院などのIoT端末システムに関して

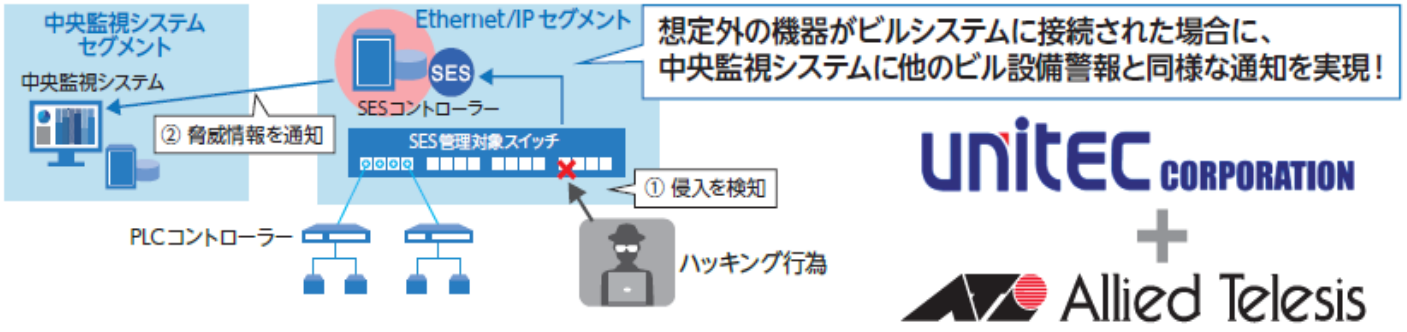
  - 接続IoTデバイスの接続に対するホワイトリスト制御
    - ネットワークに接続されているIoTの管理を徹底し、無駄な端末をシステムネットワークに接続させない
  - システムのネットワーク機器やGatewayのアカウント・パスワード管理
    - システムを形成するネットワーク機器のアカウント・パスワード等がデフォルトのままになっている産業システムが多く存在
  - 外部ネットワークからアクセスされるサーバ類のセグメント化
    - IoTシステムでありがちな構成は上から下まで、情報セグメントが同じであり、感染が広がりやすい。

活動例①制御ネットワークのホワイトリスト制御

- 制御ネットワークに接続された 端末の見える化とホワイトリスト制御研究例

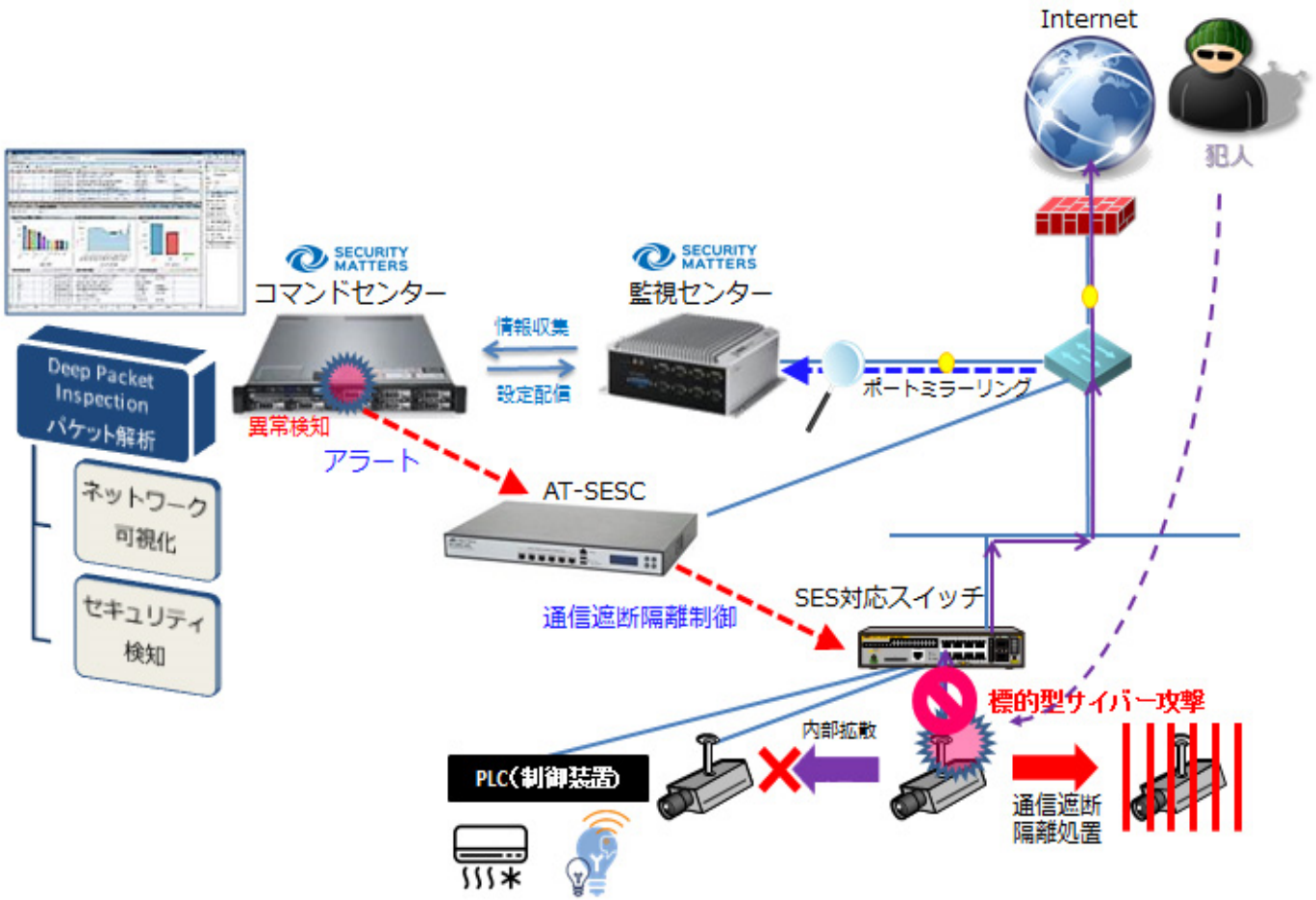


- 未許可端末接続に対するアラーム通知研究例



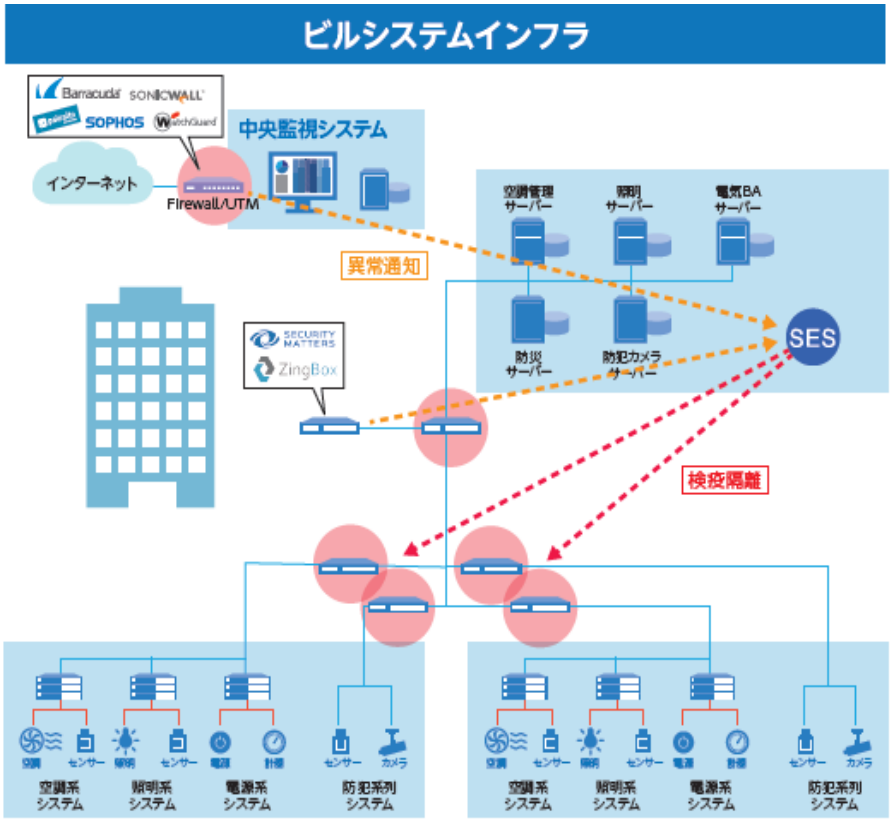
活動例②制御ネットワークセキュリティ製品との連携システム研究

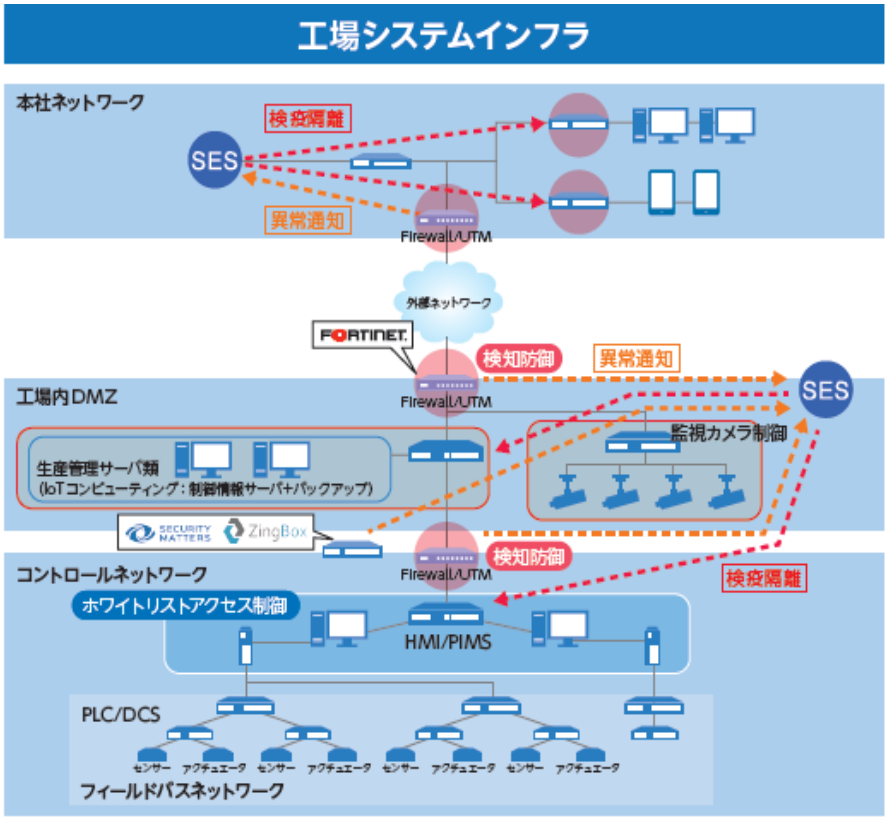
- IoTセキュリティ製品と連動させたハッキング防止例
  例）Security Matters 製品とSESインフラの自動制御イメージ



活動例③融合する制御ネットワークとITに対するセキュリティ対策

- 各種産業ネットワークとITをつなぐUTMと連携させた踏み台攻撃対策例
  - IT側、制御ネットワーク側にてホワイトリストなりすまし、内部端末の脆弱性からハッキング攻撃をした端末の通信を各種UTMからのイベントをベースに通信制御を行う研究





アライドテレシスの
サイバーセキュリティへの取組

サイバーセキュリティへの取り組み

2014年12月　アライドテレシス、オフィス向けSDNに向けて5社連合を展開
クオリティソフト、ストラトスフィア、トレンドマイクロ、ラクラスと連携
セキュリティ製品とLANを組み合わせたSecure Enterprise SDN構想を発表

2015年10月　アライドテレシス、エンタープライズ市場向けOpenFlow/SDN新製品
AT-Secure Enterprise SDN Controller 」、「OpenFlowライセンス」をリリース
- SDNマネージャ、無線LAN AP / スイッチ用ライセンス製品をリリース

2016年　SES連携資産管理ソフト、セキュリティ製品連携が15社以上に増加
日立システムズ、FFRI、FireEye、Damballa、ジュピターテクノロジー、
DOS、Flowmon、Sonicwall、バラクーダ、DDA、MOTEX

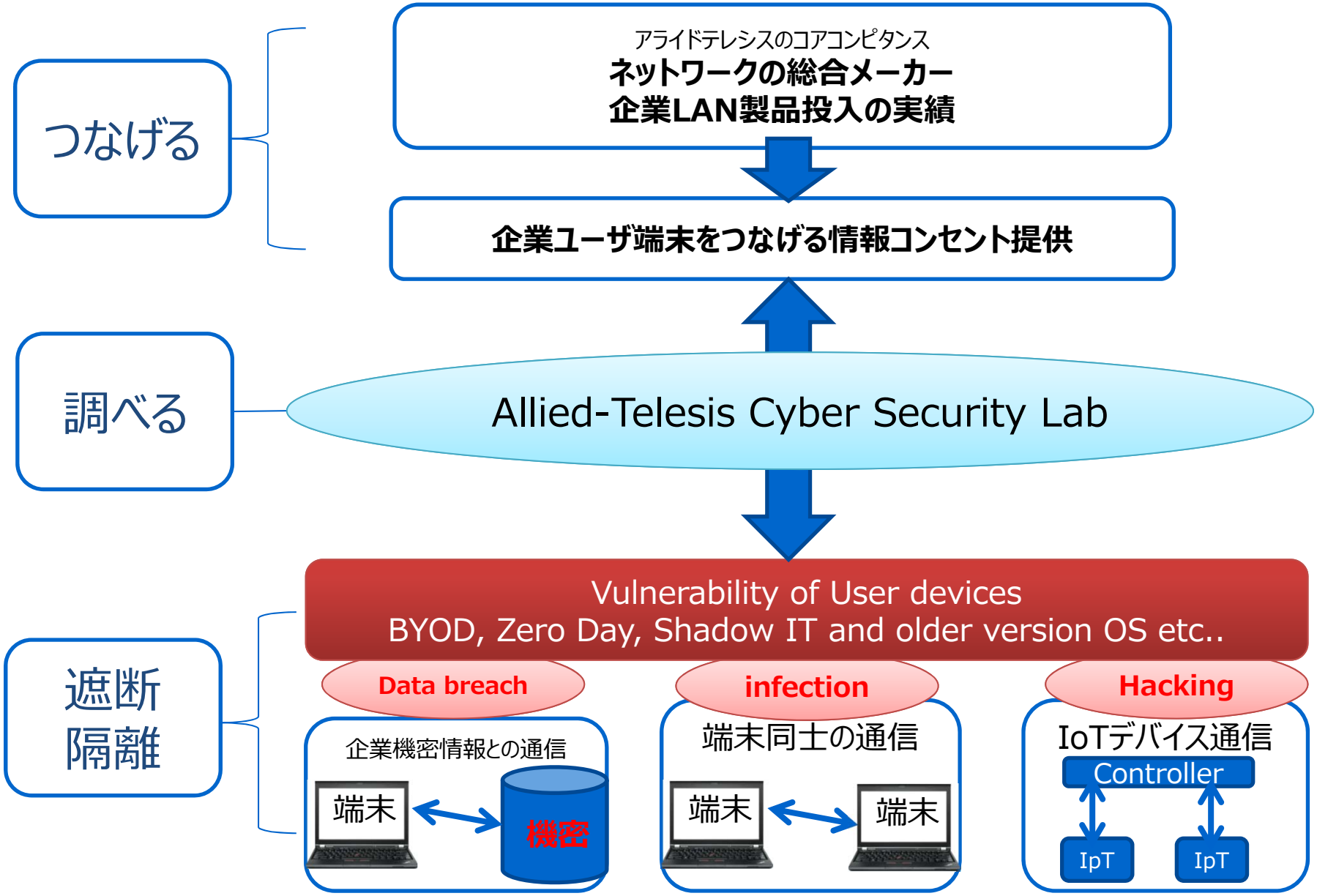
2017年6月　アライドテレシスのSecure Enterprise SDN (SES)が
Network Virtualization Europe 2017アワードで最優秀賞を2部門で受賞
- iCMG Architecture Excellence Awards

2017年　IoT関連ネットワークに対するセキュリティシステムへの取り組みを開始
スマートビルディングExpo、スマート工場Expoにセキュリティシステムを展示

2018年　IoT関連ネットワークに対するセキュリティ連携を発表
IoT特化型セキュリティソリューション「ZingBox IoT Guardian」、産業用制御システムセキュリティ
ソリューション「SecurityMatters社製SilentDefense」と「Secure Enterprise SDN(SES) 」を連携

サイバーセキュリティラボの設立

アライドテレシスのサイバーセキュリティラボ



2018年度活動予定

準備期　前期　後期

2018年1-3月　ラボ環境構築
- 仮想ICT環境作成
  - 仮想インターネット、仮想オフィス環境作成
- SESシステム環境作成
  - SESTechパートナーおよびペントレ会社製品の組み込み

ICT環境に関するサイバーセキュリティ研究
2018年4-8月

代表的Virusに対するSES連携システム効果研究とレポート作成

企業内のIP端末の脆弱性を可視化するペネトレーションツールの作成

2018年７月-
IoT環境に関するサイバーセキュリティ研究
- IoT通信解析ベンダーとのアライアンスおよびセキュリティシステムの考案
- サイバーセキュリティ団体、演習講座での共同研究の実施

2018年　2019年

技術研究組合 制御システムセキュリティセンターに加盟

システムセキュリティ検証、高セキュア化構成・技術の確立事業に対して、弊社のSDN(Software-Defined Networking)技術と、サイバーセキュリティ製品連携ソリューション(Secure Enterprise SDN、略称SES)を産業システムインフラに取り入れ、強靭化研究を行うことにより本組合事業に貢献することを目的

【主な研究活動】

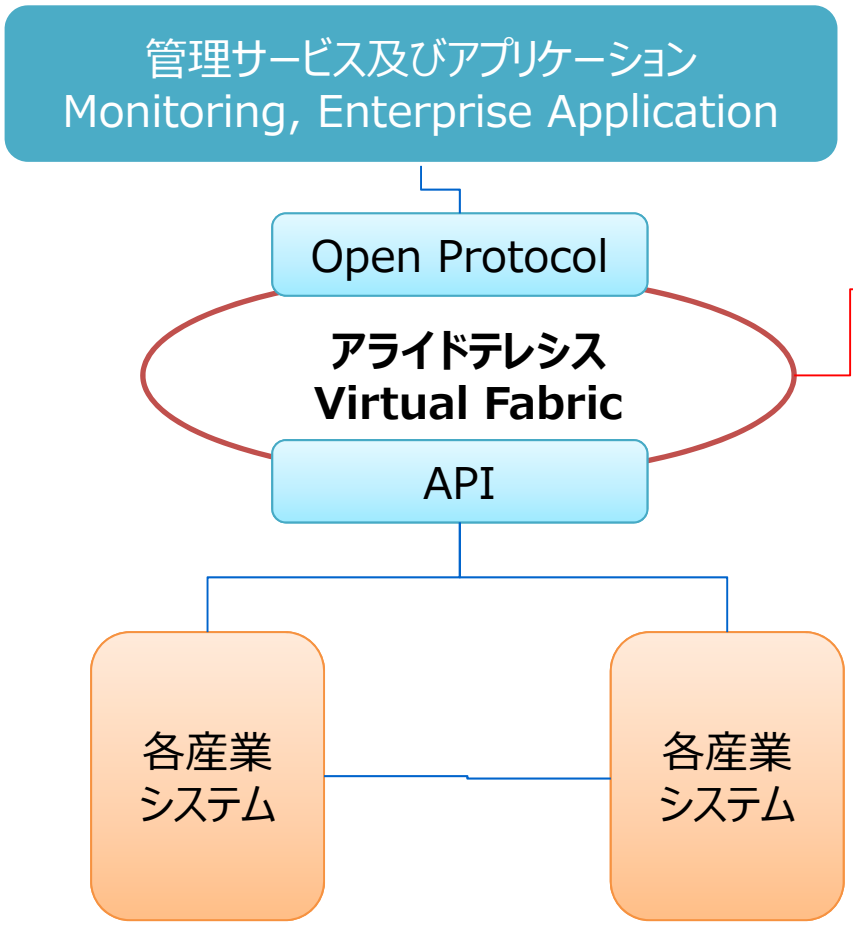
弊社は本組合にて、ビルオートメーションをはじめとするさまざまな産業システムに対し、SDNと産業向けセキュリティソリューションを融合させ、効果的なサイバーセキュリティ対策の研究活動を実施してまいります。具体的な研究活動予定は以下となります。

(1) 制御ネットワークのホワイトリスト制御
(2) 制御ネットワークとネットワークセキュリティ製品との連携システム研究
(3) 融合する制御ネットワークとITに対するセキュリティ対策

写真：技術研究組合 制御システムセキュリティセンター

Virtual Fabric仮想基盤の開発

アライドテレシスはネットワークを主体に様々な産業を組み込む仮想基盤を開発予定

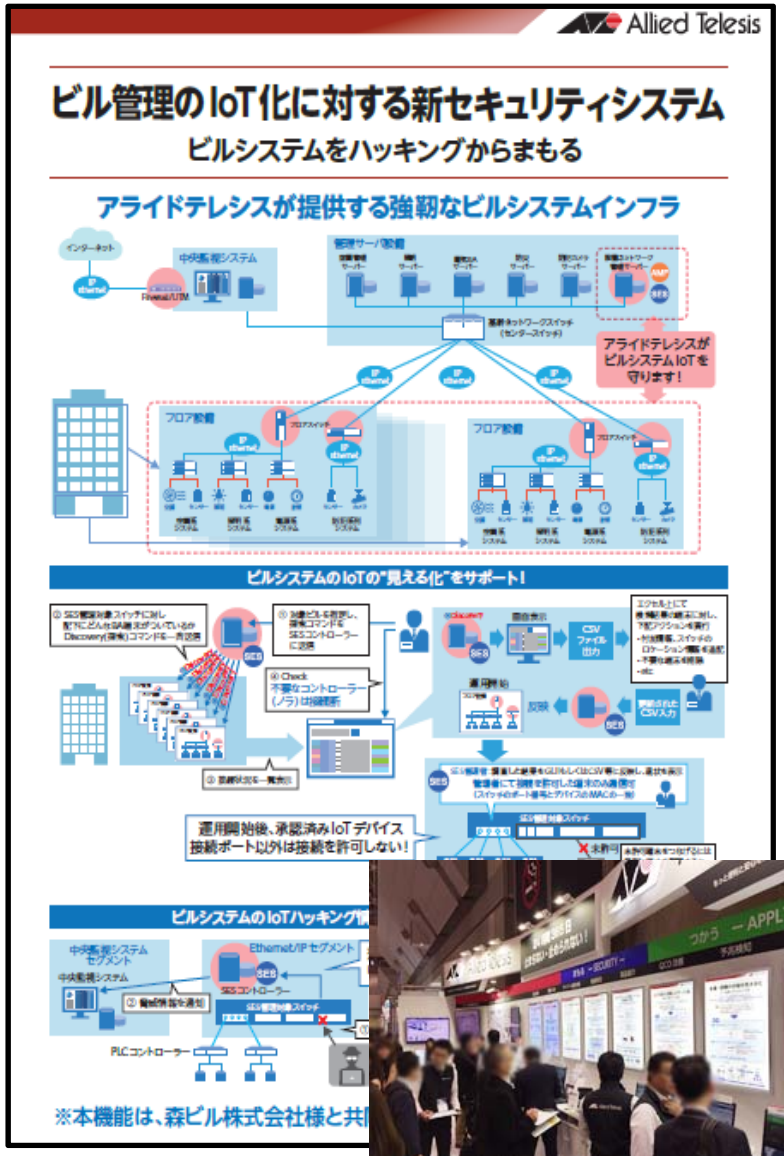


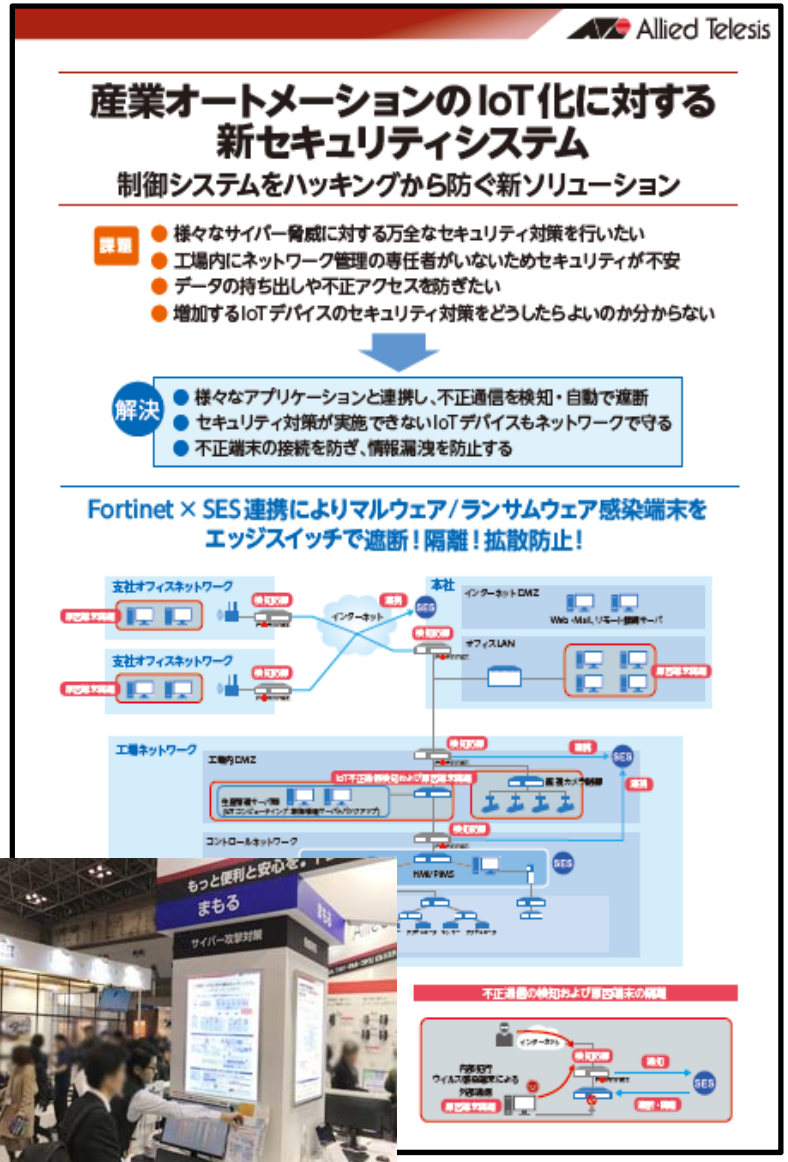
クローズド環境の各種産業システムのOpen化を可能にし、企業アプリケーションと接続するプラットフォームの開発

- アライドテレシステクノロジー制御APIの公開
- 各種アプリケーション（Open Source)との連動

2019年中に発表予定

Output

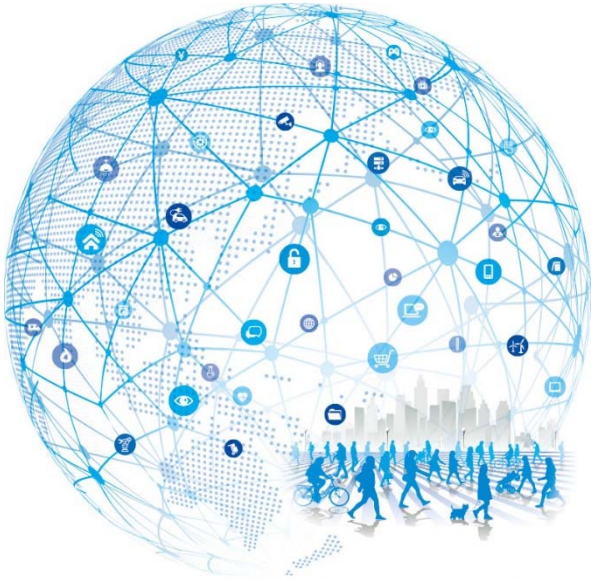




サイバーセキュリティエコシステムのご案内

- 協賛ベンダーのご案内
  - Labでのサイバーセキュリティ研究を行う下記メーカー、Sierの参加を募集してます。
    - セキュリティ製品メーカー・SIer
    - 監視アプリケーションメーカー・Sier
    - サイバーセキュリティサービスに関わる企業
  - 製品・サービス等を本ラボの仮想環境で動作検証を展開していく予定です

アライドテレシスのExchangeパートナーページも合わせてご覧ください
http://www.allied-telesis.co.jp/solution/applications/index.html



つ な ぐ 、 ま も る 、 つ か う

Allied Telesis