

製造業における

セキュリティ最前線

～ゼロトラスト時代のセキュリティ対策のベストプラクティス～



第1部 > 製造業へのサイバー攻撃とその対策 > 14:00-14:10

第2部 > 製造業における
適材適所のセキュリティ対策とは > 14:10-14:25

第3部 > その他情報、QA > 14:25-14:30

製造業における セキュリティ最前線

～ゼロトラスト時代のセキュリティ対策のベストプラクティス～

2021年10月27日

富士通株式会社

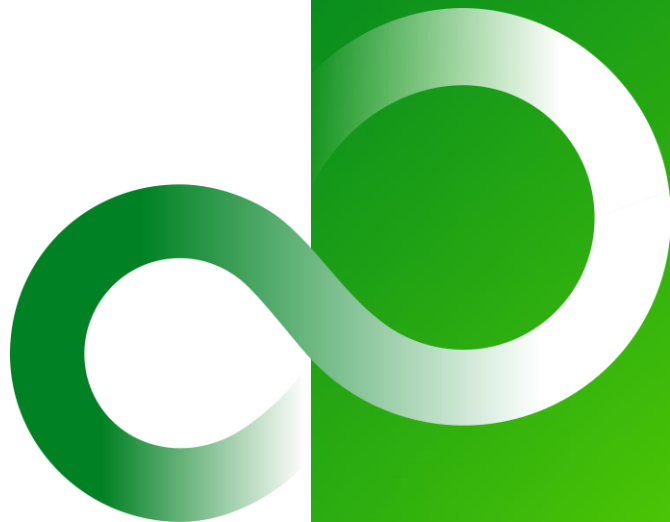
戦略企画・プロモーション室 サービスプロモーション統括部

マネージャ

斎藤 建

戦略企画・プロモーション室 DISフロントセンター WLSフロント部

麻生 泰宏



製造業における

セキュリティ最前線

～ゼロトラスト時代のセキュリティ対策のベストプラクティス～



第1部 > 製造業へのサイバー攻撃とその対策 > 14:00-14:10

第2部 > 製造業における
適材適所のセキュリティ対策とは > 14:10-14:25

第3部 > その他情報、QA > 14:25-14:30

製造業における

セキュリティ最前線

～ゼロトラスト時代のセキュリティ対策のベストプラクティス～



第1部 > 製造業へのサイバー攻撃とその対策 > 14:00-14:10

第2部 > 製造業における
適材適所のセキュリティ対策とは > 14:10-14:25

第3部 > その他情報、QA > 14:25-14:30

なぜ、サイバー攻撃は、
攻撃者優位であり続けるのか？



1970年代



1980年代～

GUI

CUI

2020年代

DX

GUI

CUI

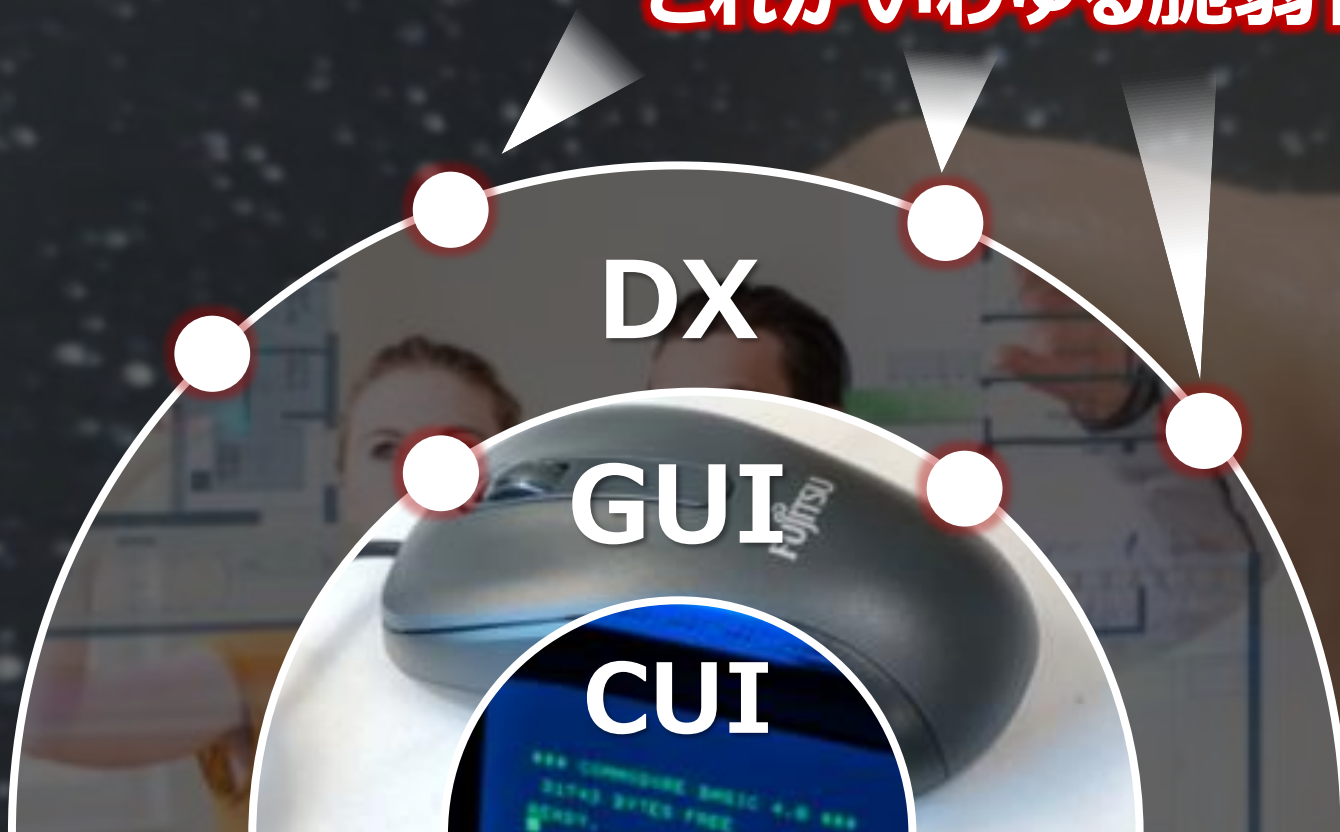
コンピュータの
進化に伴い
プログラム量は増大

DX

GUI

CUI

一定確率でできる穴、
これがいわゆる脆弱性



等比級数的に
増える脆弱性

攻撃者が先に
見つけた穴、
これがZero-Day

DX

GUI

CUI

等比級数的に
増える脆弱性

攻撃者が先に
見つけた穴、
これがZero-Day

DX

GUI

CUI

先回りして
対応が困難。

よって、

攻撃者優位に。

攻撃者の実態は緩い繋がり

関連する
団体

所属する
国家

攻撃を
支援する団体

基本的に、
攻撃のことは
知らないことも

攻撃者

動機：
早く、開発したい
早く、設計せねばならない

欲しい情報があるから
攻撃する

攻撃を
受ける
団体

このような情報を持つ団体は、
産業関連企業

参考：デジタルアイデンティティ，崎村 夏彦，日経BP，2021年7月5日
サイバースパイが日本を破壊する，井上 久男，株式会社ビジネス社，2021年6月1日
すぐそこにあるサイバーセキュリティの罠，吉田 琢也，日経BP，2021年4月14日
サイバーアンダーグラウンド，吉野 次郎，日経BP，2020年1月27日
超限戦，喬 良，角川新書，2020年1月10日

攻撃者が、本当に欲しい情報は何か？

個人情報？ 機密情報？ 金銭？

そうした情報もあるが、
喉から手が出るほど欲しい情報とは？

努力せねば、通常は手に入らない情報

長い期間をかけて開発された情報

参考：デジタルアイデンティティー、崎村 夏彦、日経BP、2021年7月5日
サイバーアンダーグラウンド、吉野 次郎、日経BP、2020年1月27日
超限戦、喬 良、角川新書、2020年1月10日
サイバー完全兵器、DAVID E. SANGER、朝日新聞出版、2019年5月25日
ゼロデイ、山田 敏弘、文藝春秋、2017年3月20日

攻撃者は何を考えて攻撃するのか

開発するより、攻撃した方が楽

▶ 製造業が狙われる理由

参考：デジタルアイデンティティ，崎村 夏彦，日経BP，2021年7月5日
サイバーアンダーグラウンド，吉野 次郎，日経BP，2020年1月27日
超限戦，喬 良，角川新書，2020年1月10日
サイバー完全兵器，DAVID E. SANGER，朝日新聞出版，2019年5月25日
ゼロデイ，山田 敏弘，文藝春秋，2017年3月20日

攻撃者は何を考えて攻撃するのか

開発するより、攻撃した方が楽

▶ 製造業が狙われる理由

脆弱性を自ら見つけるより、買った方が楽

Zero-Dayより既知の脆弱性を攻撃した方が楽 ▶ サプライチェーンが狙われる理由

参考：デジタルアイデンティティ，崎村 夏彦，日経BP，2021年7月5日
サイバーアンダーグラウンド，吉野 次郎，日経BP，2020年1月27日
超限戦，喬 良，角川新書，2020年1月10日
サイバー完全兵器，DAVID E. SANGER，朝日新聞出版，2019年5月25日
ゼロデイ，山田 敏弘，文藝春秋，2017年3月20日

攻撃者は何を考えて攻撃するのか

開発するより、攻撃した方が楽

▶ 製造業が狙われる理由

脆弱性を自ら見つけるより、買った方が楽

Zero-Dayより既知の脆弱性を攻撃した方が楽

▶ サプライチェーンが狙われる理由

ツール(マルウェア)を自ら作るより、買った方が楽

▶ 巧妙化が進む理由

参考：デジタルアイデンティティ，崎村 夏彦，日経BP，2021年7月5日
サイバーアンダーグラウンド，吉野 次郎，日経BP，2020年1月27日
超限戦，喬 良，角川新書，2020年1月10日
サイバー完全兵器，DAVID E. SANGER，朝日新聞出版，2019年5月25日
ゼロデイ，山田 敏弘，文藝春秋，2017年3月20日

攻撃者は何を考えて攻撃するのか

開発するより、攻撃した方が楽

▶ 製造業が狙われる理由

脆弱性を自ら見つけるより、買った方が楽

Zero-Dayより既知の脆弱性を攻撃した方が楽

▶ サプライチェーンが狙われる理由

ツール(マルウェア)を自ら作るより、買った方が楽

▶ 巧妙化が進む理由

そもそも攻撃するより弱いパスワードを狙う方が楽

▶ 認証が狙われる理由

参考：デジタルアイデンティティ，崎村 夏彦，日経BP，2021年7月5日
サイバーアンダーグラウンド，吉野 次郎，日経BP，2020年1月27日
超限戦，喬 良，角川新書，2020年1月10日
サイバー完全兵器，DAVID E. SANGER，朝日新聞出版，2019年5月25日
ゼロデイ，山田 敏弘，文藝春秋，2017年3月20日

製造業において、いま気をつけるべきこと

弱点になりやすい部分のチェック

弱い認証
の撲滅



認証全体の
チェック

テレワークにおいて
隙を作らない



ゼロトラストの実現、
エンドポイント強化

クラウドなどの
セキュリティ統制



ガバナンスの
チェック



ロケーションごとにチェック

□ケーションごとにチェック ▶

認証、ゼロトラスト/エンドポイント強化、ガバナンス

FUJITSU

ユーザー側



ネットワーク側



各種クラウド



工場



マネジメントプラットフォーム

認証



管理



デバイス



アプリケーション



セキュリティインテリジェンス



関連分析



統合SOC



ロケーションごとの弱点

認証、ゼロトラスト/エンドポイント強化、ガバナンス

FUJITSU

ユーザー側

オフィス
ガバナンスが効かない
セキュリティの緩い部分
支社

自宅
自宅を含めた
様々な場所からの
アクセス
モバイル

ネットワーク側

自宅からクラウドなど
外部 から 外部への
アクセス

各種クラウド

SaaS SaaS IaaS
それぞれのクラウド
における認証
データ
センター

工場

実施しなければならない
新たな接続

マネジメントプラットフォーム

認証



管理



デバイス



アプリケーション



セキュリティインテリジェンス



相関分析

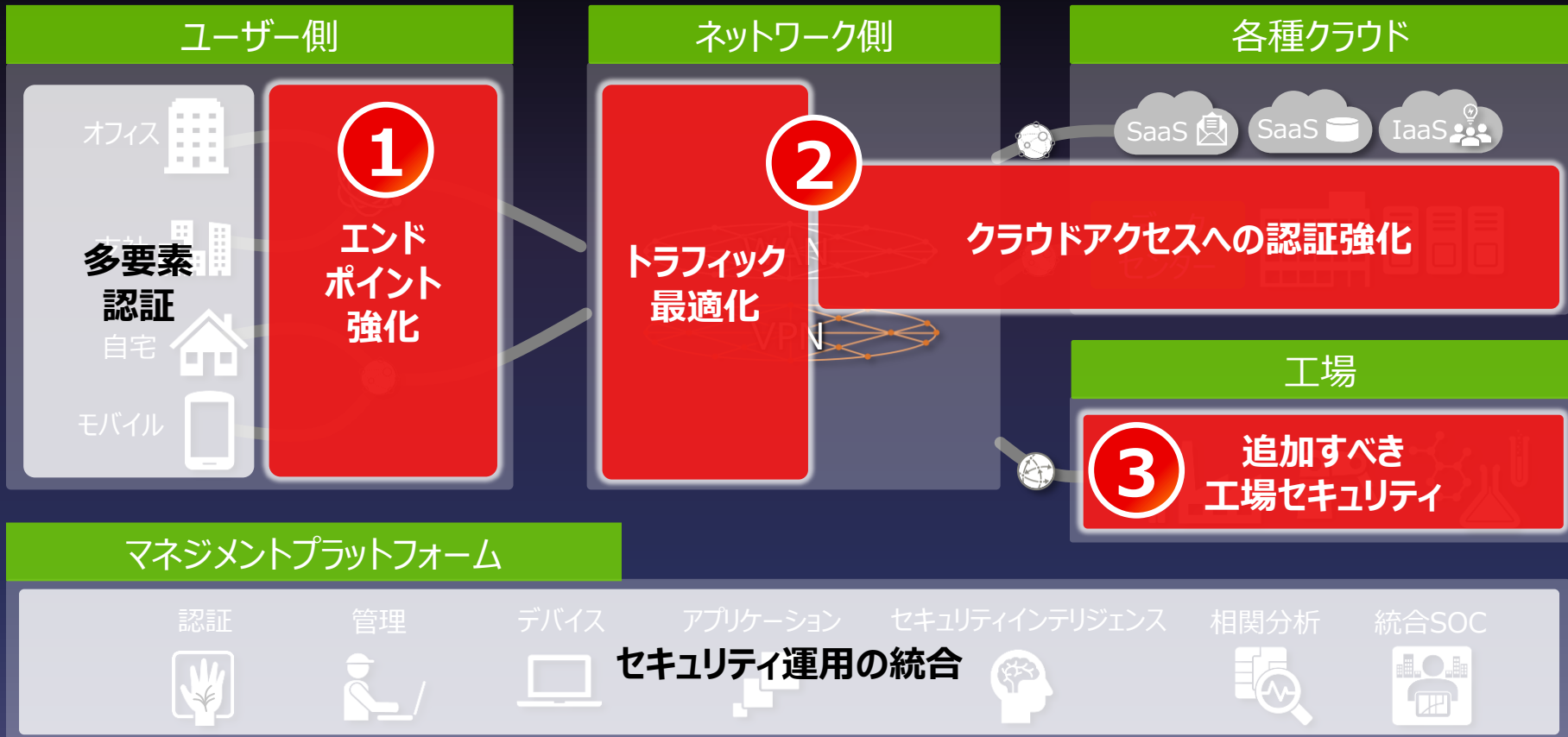


統合SOC



収集できていない情報

今回お伝えする部分



エンドポイント強化

サプライチェーンやガバナンスが効きにくいところを含め強化

オフィス



支社



自宅



モバイル



分散する痕跡を早期に見つけることが重要

EDRの導入

トラフィック最適化およびクラウドアクセスへの認証強化

利便性を保ちつつ、セキュアなアクセスを確保



ゼロトラストの観点におけるセキュリティ強化

SASE、CASBの導入

工場において必要な、新たな対策

■ セキュリティパッチを容易に適用できない

- ・サポート切れOSを使用せざるを得ない（制御装置とセットのため変更不可）
- ・制御ソフトとの相性でパッチ適用困難



■ アンチウイルスソフトも容易に適用できない

- ・工場設備の動作連携上、導入不可
- ・アンチウイルスソフトが対応していない



■ その上で、リモートワーク化で接続が必要に

- ・進むスマートファクトリー化
- ・ニューノーマル時代の到来により、接続も必須に



工場における基本を押さえた上で、新たな対策を

■ 基本の対策

- ・資産管理
- ・USB接続管理

■ 新たな対策（リモートワークなど接続対策）

- ・リモートアクセス管理
- ・ホワイトリスト制御
- ・実施した対策の有効性確認



第1部 まとめ

- ① 端末起点による攻撃早期発見 (EDR等)
- ② セキュアなクラウドアクセス (SASE/CASB)
- ③ 工場における攻撃制御/監視の強化

製造業における

セキュリティ最前線

～ゼロトラスト時代のセキュリティ対策のベストプラクティス～



第1部 > 製造業へのサイバー攻撃とその対策 > 14:00-14:10

第2部 > 製造業における
適材適所のセキュリティ対策とは > 14:10-14:25

第3部 > その他情報、QA > 14:25-14:30

製造業における

セキュリティ最前線

～ゼロトラスト時代のセキュリティ対策のベストプラクティス～



第2部

製造業における

適材適所のセキュリティ対策とは

2021年10月27日

富士通株式会社

戦略企画・プロモーション室 DISフロントセンター WLSフロント部

麻生 泰宏

■ 端末起点による攻撃早期発見



①エンドポイント強化

■ セキュアかつ柔軟なクラウドアクセス



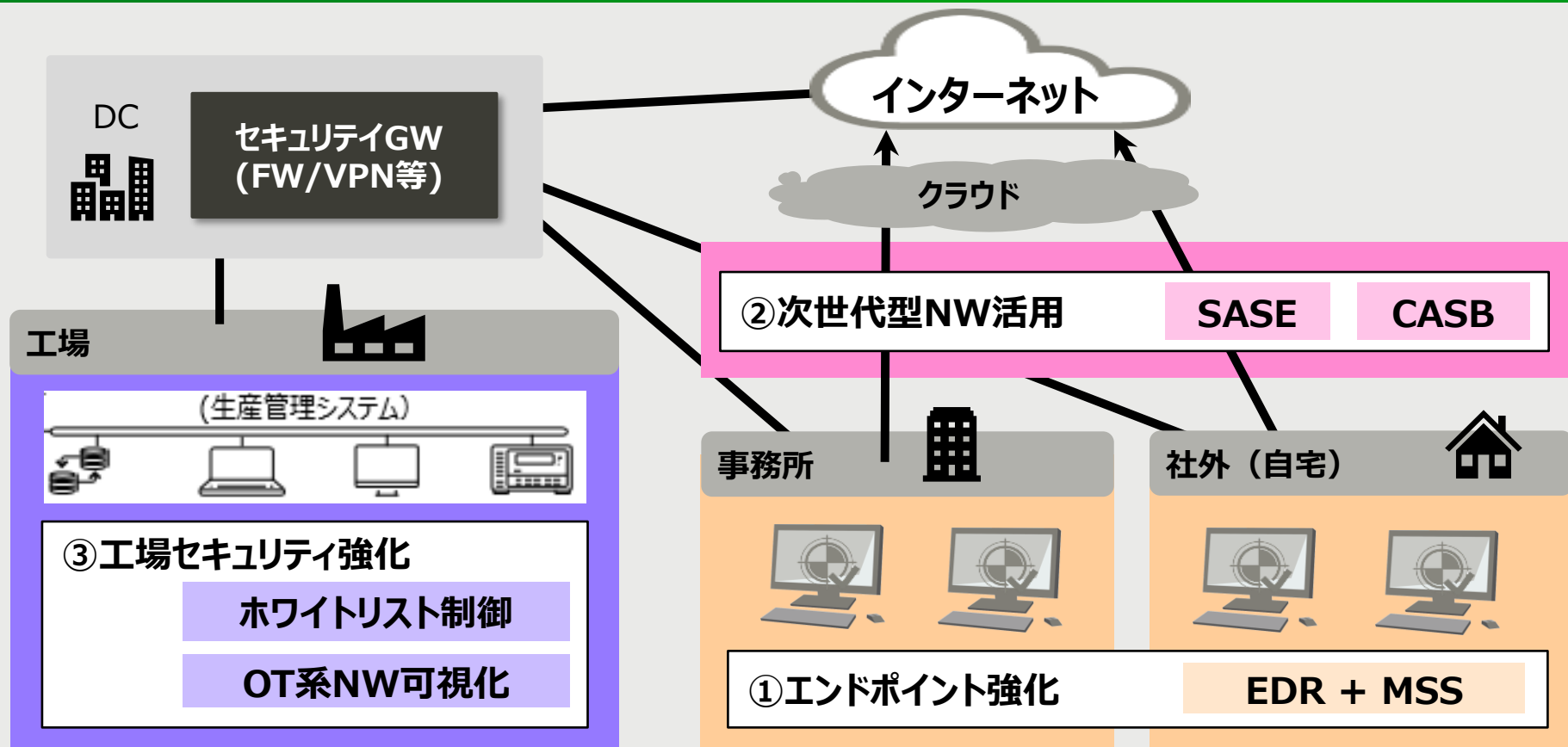
②次世代型NW活用

■ 工場における攻撃制御/監視の強化



③工場セキュリティ強化

	①エンドポイント強化	②次世代型NW活用	③工場セキュリティ強化
問題	・従来型AVのみの検知 －高度な攻撃の検知は不可 －侵入後は無力	・境界防御に頼った対策 －社外でのNW利用増 －クラウドの利用状況が把握できていない	・現場部門任せの対策 －OA系セキュリティ対策が使えない －異常通信の検知不可
課題	・侵入を前提とした対策の整備	・どこからでもセキュア & スケーラブルなNW整備 ・クラウドの安全活用	・工場の制約事項に対応した対策の活用
対策	EDR + MSS	SASE CASB	ホワイトリスト制御 OT系NW可視化





富士通がお勧めする各領域における 対策ソリューションのご紹介

エンドポイント

- Cybereason EDR
+ インテリジェンスマネージドセキュリティサービス

EDR + MSS

ネットワーク

- FENICS CloudProtect ZeroTrust Network
(powered by Prisma Access from Palo Alto Networks)
- McAfee MVISION Cloud

SASE

CASB

工場

- McAfee Application Control
- OTネットワークセキュリティ可視化サービス

ホワイトリスト制御

OT系NW可視化

Cybereason EDRサービス+MSS（運用サービス）

FUJITSU

疑わしい挙動を分析、迅速な検知・対応を実現

エンドポイント

① 未知の攻撃の検知

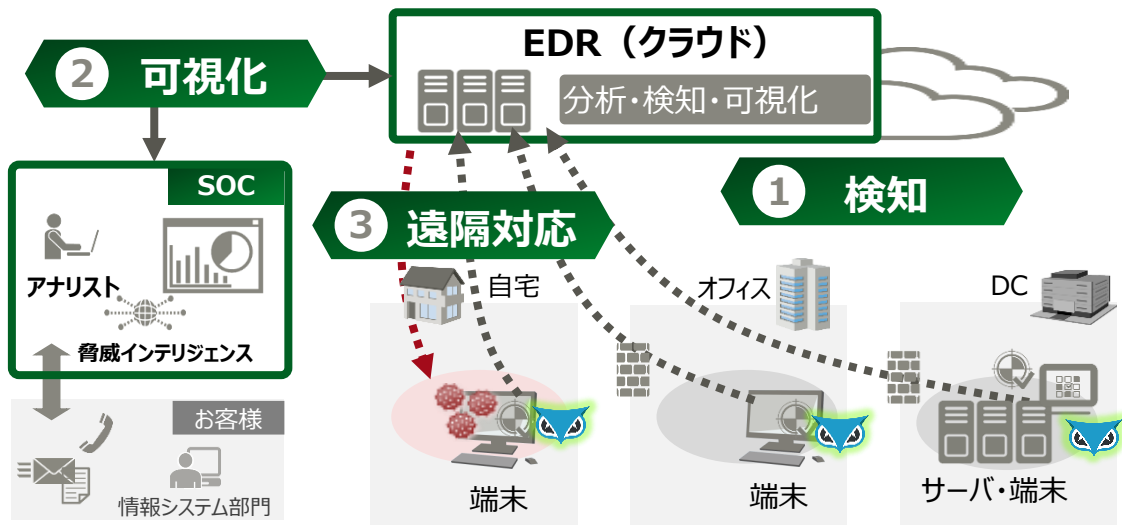
AI／ビッグデータ解析により
侵入後の攻撃を検知

② 全体像の可視化

攻撃の一連の流れを完全に
可視化

③ 遠隔対応（MSS）

遠隔で調査し対応



高度化された攻撃活動も
リアルに検知、早期発見

テレワーク等の社外PCの
感染活動も検知・可視化

専門家が24時間365日対応

要求元の場所に関係なく、ポリシー施行と脅威対策を実施

ネットワーク

① SASE※ ※ Secure Access Service Edge

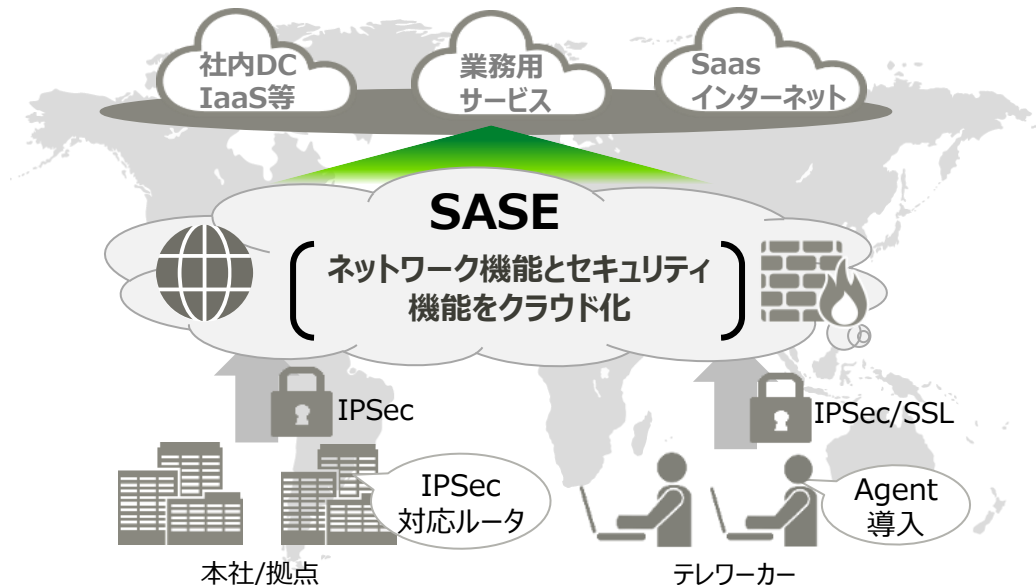
高度なセキュリティ機能を
標準提供

② セキュアで快適なアクセス

統一したセキュリティ
ポリシーで利用可能

③ 全てクラウドサービス

管理/運用の負担が
大幅に軽減



セキュリティ機能をクラウドベースで
提供するため、どこからでも利用可能

本社/拠点の接続、拠点間の接続、
モバイルユーザにも対応

急な人数の増減にも対応可能

クラウドの利用状況を可視化、安全なクラウド利用を実現

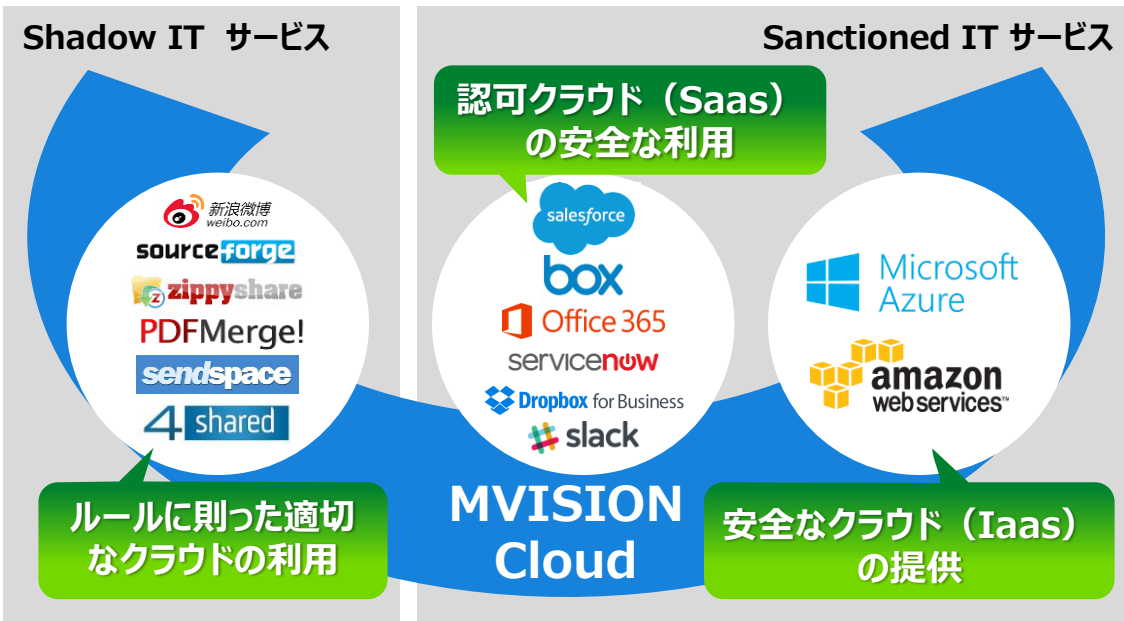
ネットワーク

① 適切なクラウド利用

クラウドの**可視化・管理・制御**

② 安全なクラウド利用

SaaS/IaaS利用の**監視・監査と制限**



誰が、いつ、どのサービスを使っているかの可視化により、セキュリティリスクを排除

様々なセキュリティ機能により、特定クラウドサービスを安全に利用 (SaaS/IaaS)

エージェントレスで利用可能

工場の生産性や安定稼働を優先したセキュリティ対策

工場

① 工場を止めずに守る対策

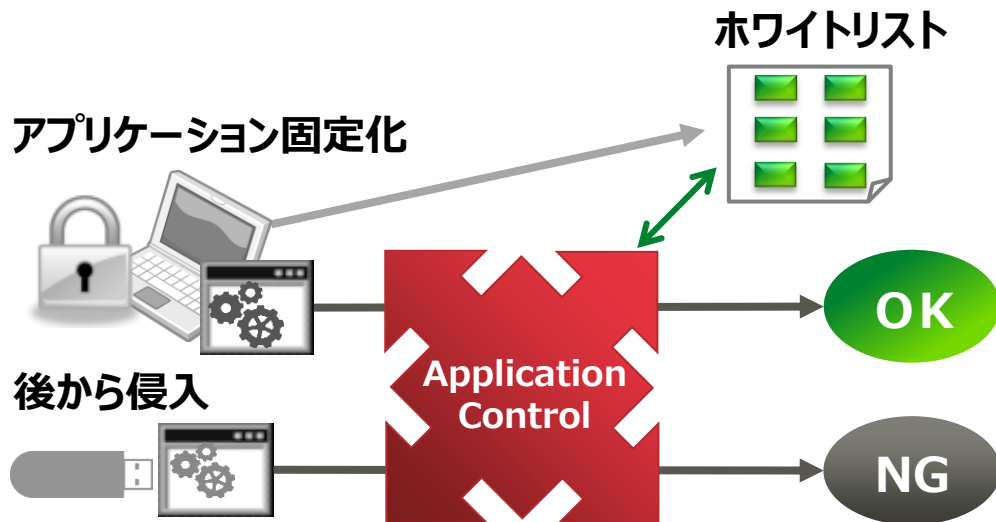
生産ラインの稼働が最優先
新たな攻撃にも対応可能

② ホワイトリスト方式

マルウェア実行不可
レガシーOSにも対応

③ 運用負担も小さい

パッチ適用不要
管理サーバ無しでもOK



脆弱性を突いた
ゼロデイ攻撃にも対応

ホワイトリスト方式のため、
マルウェアに感染しても発症しない

Win7をはじめ
レガシーOSに多く対応

OTネットワークセキュリティ可視化サービス

OTネットワークの可視化により、生産ラインの安定稼働を実現！

工場

① 工場内のIT資産管理

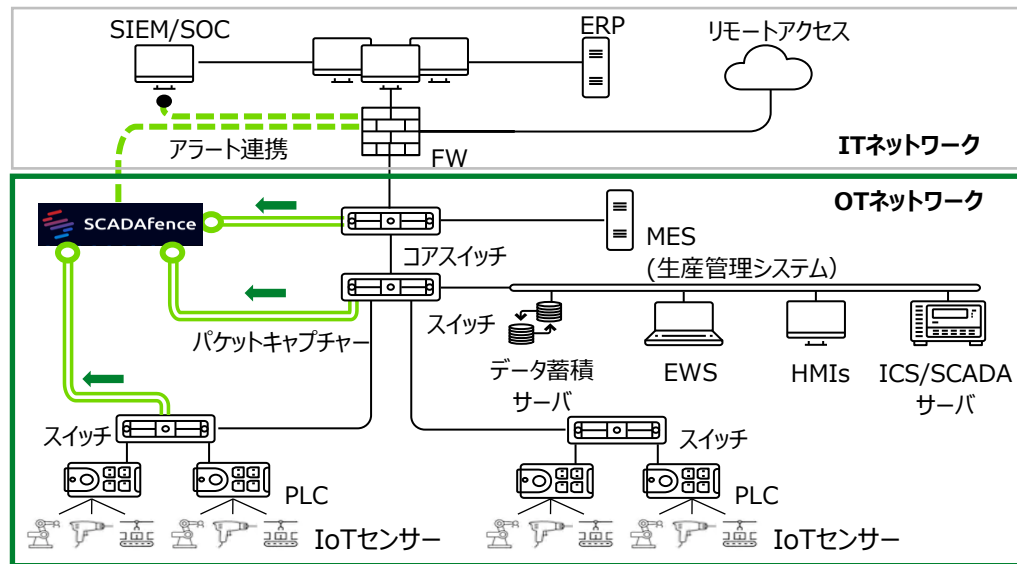
OTネットワーク上の機器情報の
収集とリスク把握

② ネットワークの安定稼働

通常の通信を自動学習し、
異常通信を自動検知

③ リモートアクセスの管理

アクセス元/先の情報を監視し、
不正アクセスを検知



OTネットワーク状況の自動可視化により、管理工数の大幅な削減が可能

セキュリティリスクの早期発見により、生産業務への被害を低減

OT系特有のプロトコルにも対応

2 部のまとめ

- まず最優先で実施すべきは、攻撃者の侵入を前提とした
エンドポイント対策の強化
- テレワーク増加やクラウドシフトといった時代の流れにあった
新しいタイプのNW環境の構築が必要
- **工場特有**のセキュリティ課題に適した対応を実施することで
生産ラインの安全 & 安定的な稼働が可能

セキュリティについてのお困りごとがありましたら、
是非、富士通にお声がけください

全体 まとめ

- ① 全体を俯瞰し、必要な対策を！
- ② 無理なく実施できる対策を！
- ③ アフターコロナを見据えた対策を！

製造業における

セキュリティ最前線

～ゼロトラスト時代のセキュリティ対策のベストプラクティス～



＞ 製造業へのサイバー攻撃とその対策 ＞ 14:00-14:10

第2部 ＞ 製造業における
適材適所のセキュリティ対策とは ＞ 14:10-14:25

第3部 ＞ その他情報、QA ＞ 14:25-14:30

製造業におけるセキュリティ最前線

～ゼロトラスト時代のセキュリティ対策のベストプラクティス～

Q&A

新情報を盛り込んだセミナーの専用Webを初公開



Work Life Shiftにおける
新しい世の中の情報を盛り込んだ
セミナーの専用Webを
新たに立ち上げました。

ぜひこちらからも有用セミナーを
ご確認ください。

URLはこちら

<https://www.fujitsu.com/jp/solutions/business-technology/security/secure/seminar/>

ご参加いただいた方々には、メールにてアンケートを送付いたします。 **FUJITSU**

質問およびご要望（導入希望など）、相談事項について併せて記載いただければと存じます。

以下で検索いただき、「お問い合わせはこちら」からご連絡いただいても結構です。

お問い合わせはこちら

Webでのお問い合わせ

入力フォームへ >

お電話でのお問い合わせ

0120-933-200

[富士通コンタクトライン総合窓口]

受付時間：平日9時～17時30分
(土曜・日曜・祝日・当社指定の休業日を除く)

当社はセキュリティ保護の観点からSSL技術を使用しております。

また、直接メール

contact-solsemi@cs.jp.fujitsu.com

でもOKです。

本日はご視聴いただき、誠にありがとうございました。

Thank you



内容に関してのご質問は、
以下までお問い合わせください

contact-solsemi@cs.jp.fujitsu.com