

製造業が狙われている！今、必要なサイバー攻撃対策

～企業の生命線となるIT/OT環境を両面から守る方策とは～

14:00-
14:10

1章 ITとOTを取り巻くサイバー状況

14:10-
14:25

2章 製造業におけるセキュリティ対策

14:25-
14:40

3章 OTセキュリティ対策のベースとなるソリューション

14:40-
14:50

まとめ、QA

製造業が狙われている！ 今、必要なサイバー攻撃対策

～企業の生命線となるIT/OT環境を
両面から守る方策とは～

2022年8月4日

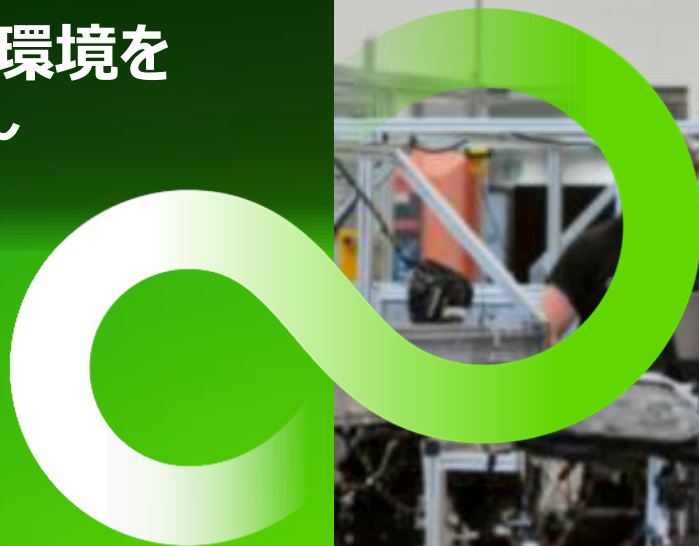
富士通株式会社

プロモーション統括部 マネージャー 斎藤 建

プリセールス統括部 シニアマネージャー 松山 啓介

サービスビジネス事業部 マネージャー 蛭田 盛夫

FUJITSU



1. ITとOTを取り巻くサイバー状況

2. 製造業におけるセキュリティ対策

3. OTセキュリティ対策のベースとなるソリューション

1. ITとOTを取り巻くサイバー状況

2. 製造業におけるセキュリティ対策

3. OTセキュリティ対策のベースとなる ソリューション

ウイルスとは何か



ウイルスとは何か

自分だけでは生きられないもの※

※1 参考：ヒトの壁，養老孟司，株式会社新潮社，2021年12月17日出版

ウイルスとは何か

自分だけでは生きられないもの

コンピュータウイルスも同じ

ウイルスとは何か

自分だけでは生きられないもの

コンピュータウイルスも同じ

よって、オープン化したシステムの課題に※

参考 : Cybersecurity Insiders, Windows and Linux Servers globally are vulnerable to Cyber Attacks,
<https://www.cybersecurity-insiders.com/windows-and-linux-servers-globally-are-vulnerable-to-cyber-attacks/>, 2022年6月26日参照

世界中から来るサイバー攻撃



※ 参考：NISC, サイバーセキュリティ2022, <https://www.nisc.go.jp/pdf/policy/kihon-s/cs2022.pdf>, 2022/6/17

サイバー世界大戦, https://www.fireeye.com/content/dam/fireeye-www/regional/ja_JP/current-threats/pdfs/fireeye-www-report.pdf, FireEye社

※ 筆者が、世界中の方々（延べ124カ国、227団体）との対話から得た知見を元に本章を構成

サイバー攻撃はなぜ、攻撃者優位なのか

攻撃の**高度化**

攻撃の**多様化**

サイバー攻撃はなぜ、攻撃者優位なのか

攻撃の高度化



技術的脆弱性

攻撃の多様化



人的脆弱性

サイバー攻撃はなぜ、攻撃者優位なのか

攻撃の高度化



技術的脆弱性



攻撃者しか知らない
プログラムの穴
を突く攻撃の一般化

攻撃の多様化



人的脆弱性



多種多様な
心理を突く攻撃

技術的脆弱性を突く攻撃

ゼロデイ攻撃

ダークウェブから入手して攻撃※

技術的脆弱性を突く攻撃

ゼロデイ攻撃

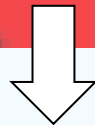
ダークウェブから入手して攻撃

あえてオオゴトにならないようにする攻撃

ウイルスを仕込んだままにする※

ランサムウェアと脅迫の組み合わせ

支払わなければ
暴露



ランサムウェアによる身代金要求に加え、
支払わなければデータを暴露するなどの
複数回の脅迫を行う攻撃

人的脆弱性を突く攻撃

ランサムウェアと脅迫の組み合わせ

支払わなければ
暴露

ウイルス感染を騙る攻撃

あなたのパソコンは
ウイルス感染しました

偽のポップアップ
脅迫メール

実際のメール



タイトル：デバイスがハッキングされました
それが起こったのです。ゼロクリックの脆弱性と特別なコードを使用して、Webサイトを介してあなたのデバイスをハッキングしました...

ウイルスが検出されました

有名なウイルス対策ソフト名

ウイルスを削除するには
Deleteをクリックしてください

Read it

Delete

人的脆弱性を突く攻撃

ランサムウェアと脅迫の組み合わせ

支払わなければ
暴露

ウイルス感染を騙る攻撃

あなたのパソコンは
ウイルス感染しました

偽のポップアップ
脅迫メール

USB攻撃※

古典的だが
強力

駐車場へばらまく
敷地内に投げ込む

直接的な金銭奪取 → 攻撃多様化による
間接的搾取へ

直接的な金銭奪取 → 攻撃多様化による
間接的搾取へ

金融 → 製造業へ※1

ターゲットが移行

※2 昨年度比300%増加

※1 参考 : THE TOP 5 CYBER THREATS WITHIN THE MANUFACTURING INDUSTRY,
<https://www.avertium.com/resources/threat-reports/top-5-threats-within-manufacturing>, 2022/5/10

※2 参考 : TECHNATIVE, <https://technative.io/security-the-key-forgotten-ingredient-in-the-transition-from-smart-to-green-manufacturing/>, 2022/6/20参照

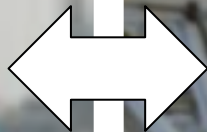
製造業に必要な防御：ITとOT

IT

DXを進める

OT

止まると一大事



製造業に必要な防御：ITとOT

IT

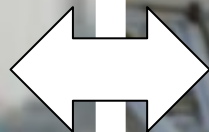
DXを進める

新規性が大事

OT

止まると一大事

変わると良くない



製造業に必要な防御：ITとOT

IT

DXを進める

まずやってみる

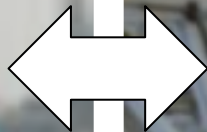
クラウド活用

OT

止まると一大事

慎重さが必要

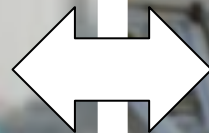
外部接続は一部のみ



製造業に必要な防衛：ITとOT

IT

DXを進める
まずやってみる
クラウド活用
スピード第一



話が
合わない

OT

止まると一大事
慎重さが必要
外部接続は一部のみ
安全第一

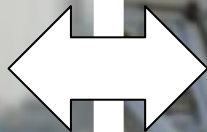
ITセキュリティとOTセキュリティ

IT

ウイルスチェック

OT

ウイルス混入の防止



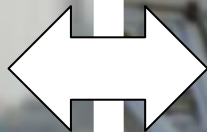
ITセキュリティとOTセキュリティ

IT

ウイルスチェック
パッチ適用

OT

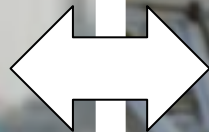
ウイルス混入の防止
外部との遮断



ITセキュリティとOTセキュリティ

IT

ウイルスチェック
パッチ適用
攻撃への追跡



OT

ウイルス混入の防止
外部との遮断
監視

ITセキュリティとOTセキュリティ

IT

ウイルスウイルス

パッチ適用

攻撃への追跡

即時切り離し

OT

ウイルス混入の防止

外部との遮断

監視

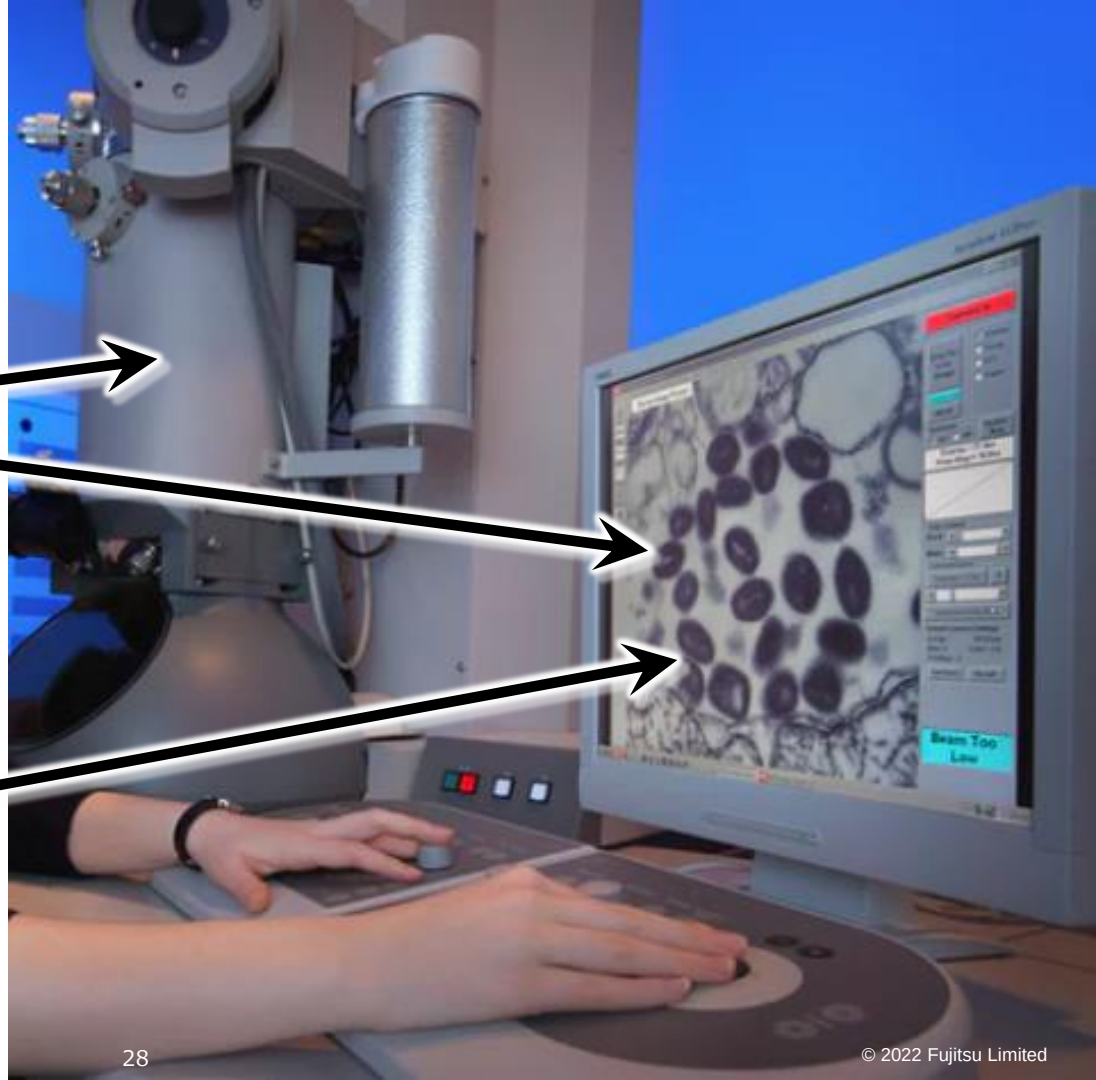
原因追及後に対応

話が
合わない

電子顕微鏡 における例

一体型

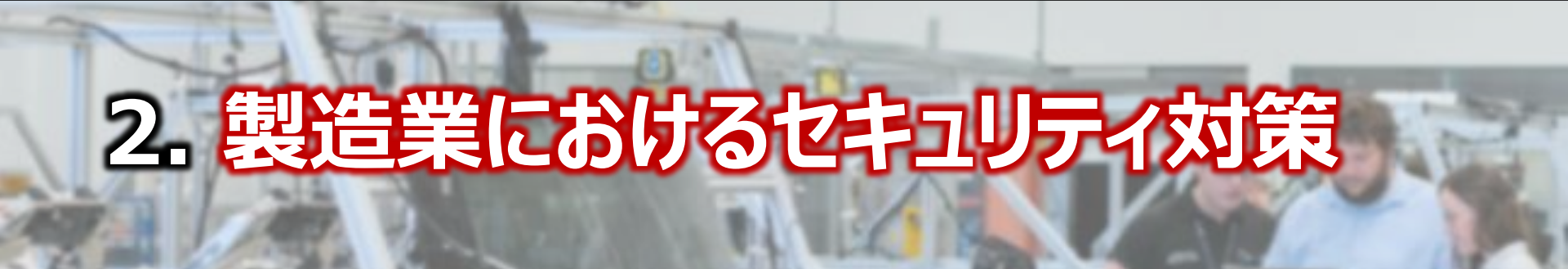
Windows
(オープン化)



金融→製造業に攻撃ターゲットが移ってきているため、**これから注意**する必要があります。

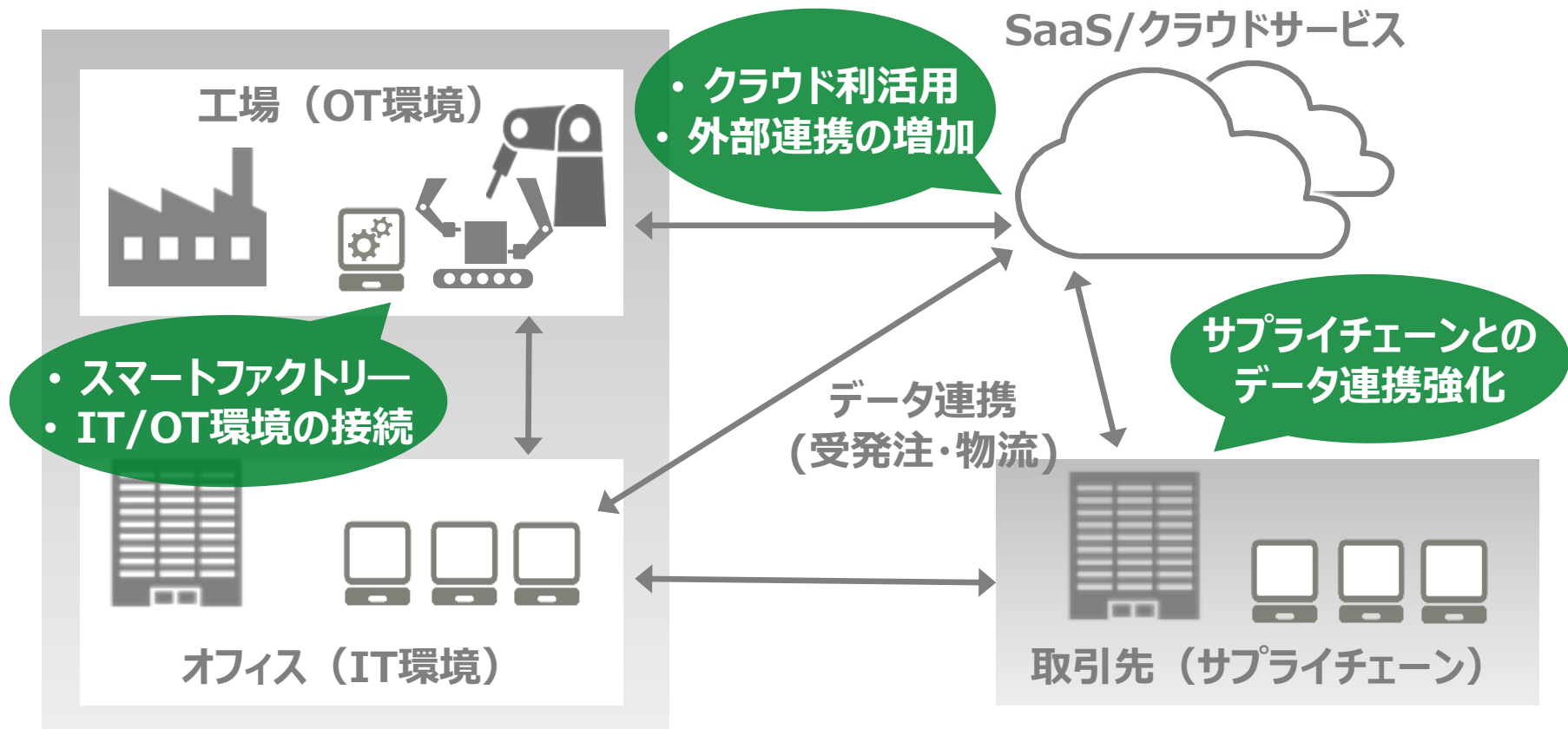
IT/OT環境において、**どのように防衛できるのか、**
次の章から、それぞれお伝えします。

1. ITとOTを取り巻くサイバー状況

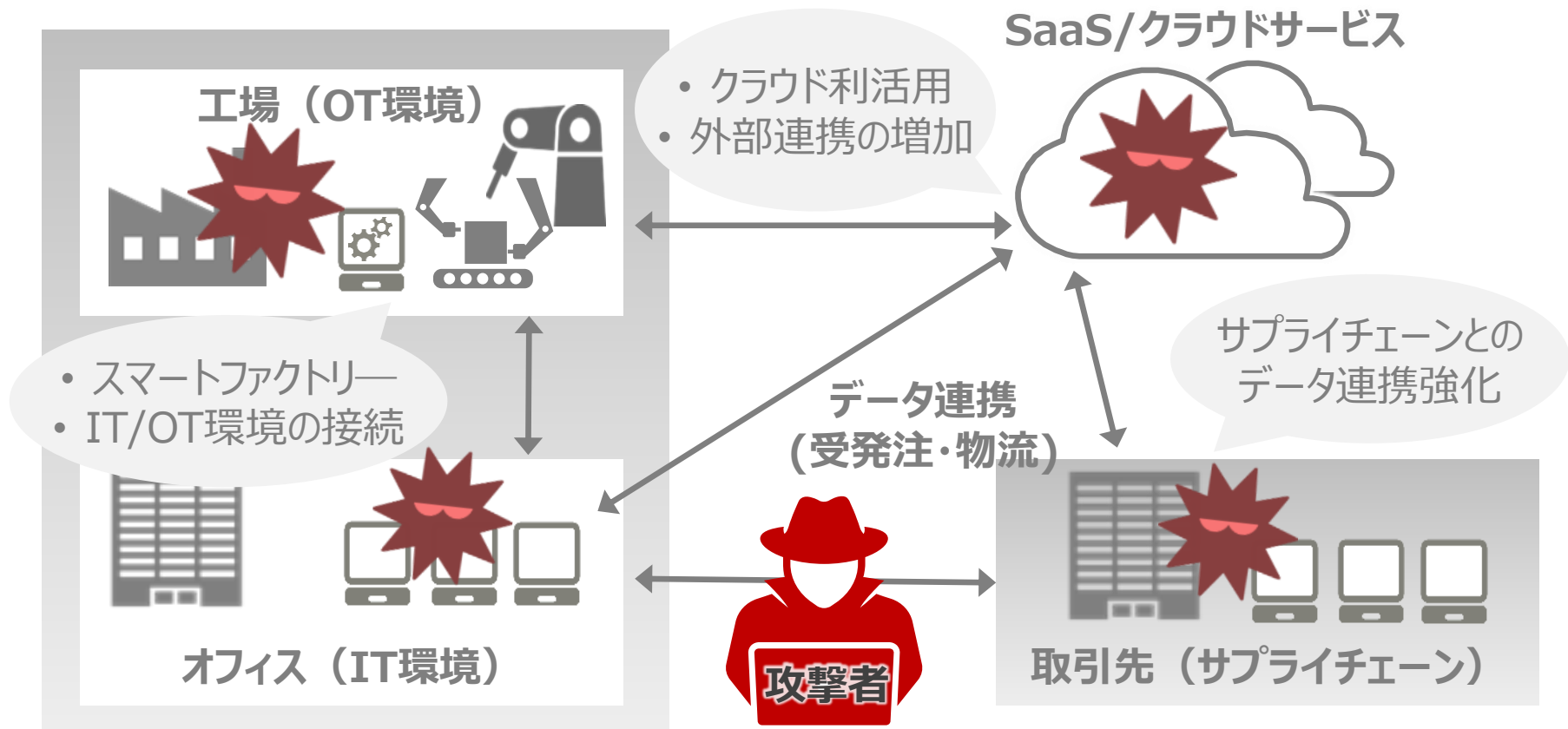


2. 製造業におけるセキュリティ対策

3. OTセキュリティ対策のベースとなるソリューション



高まる攻撃のリスク



事故事例①

巧妙化するランサムウェア

- 業務システムが暗号化され、従業員パソコンにランサムウェアの脅迫メッセージ
- サーバに保存された数万件の個人情報流出の可能性あり
- ネットワーク機器の脆弱性を侵入経路として攻撃された可能性が高い

事故事例②

取引先の障害が影響

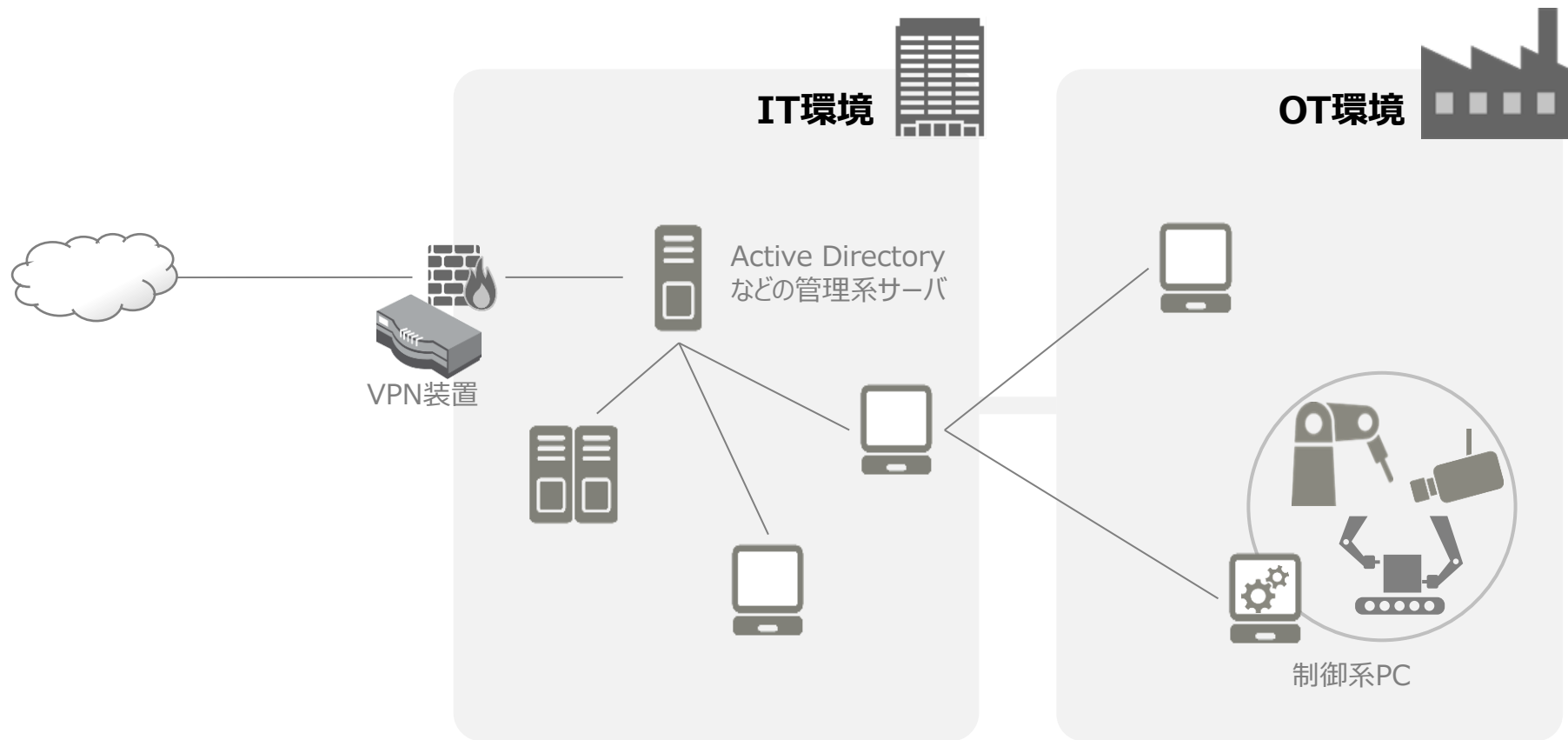
- 取引先の生産関連システムにウィルス侵入。
- 部品発注元企業において、国内数工場のライン稼働が一時停止。
- 脆弱性のあるVPN装置からの侵入である事が判明。

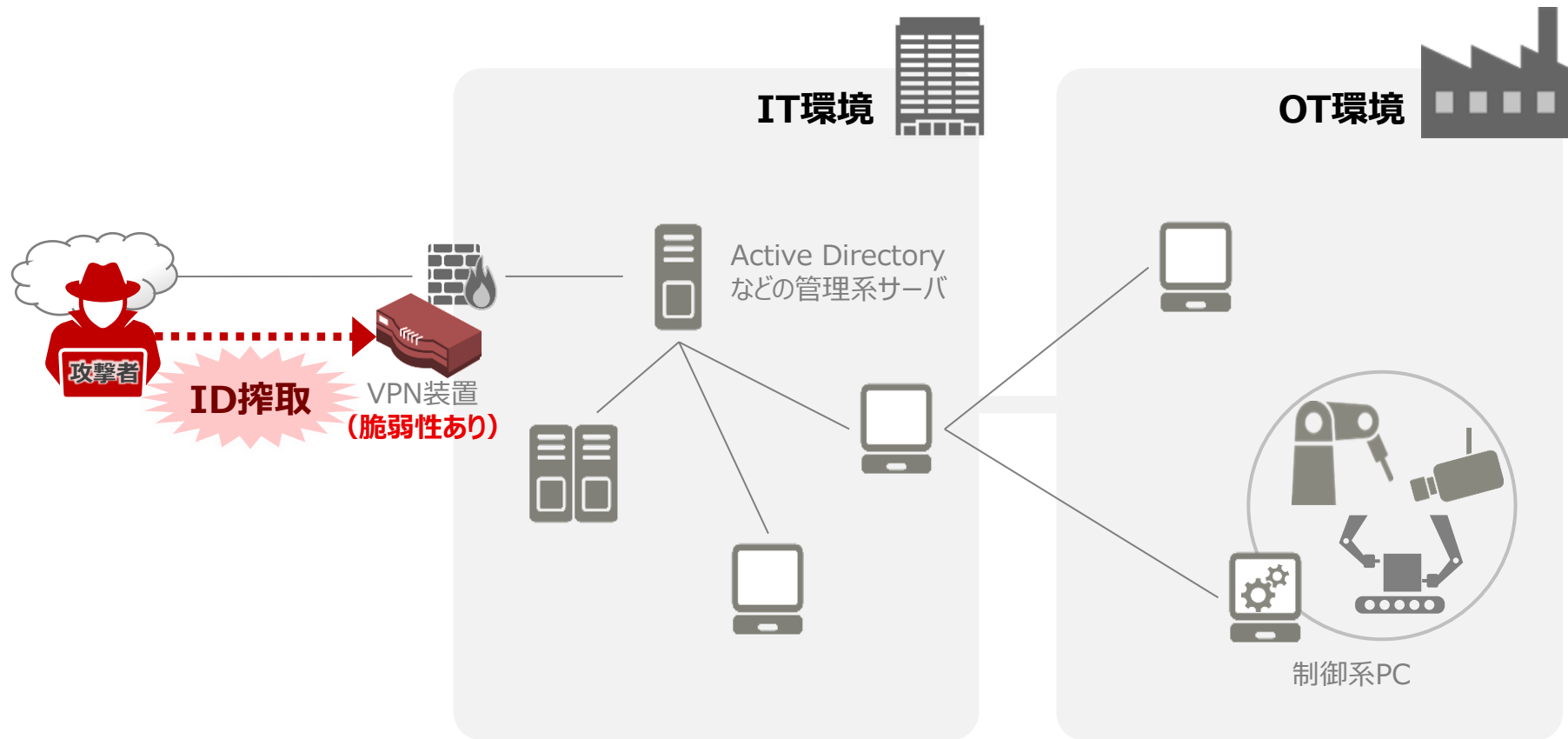
事故事例③

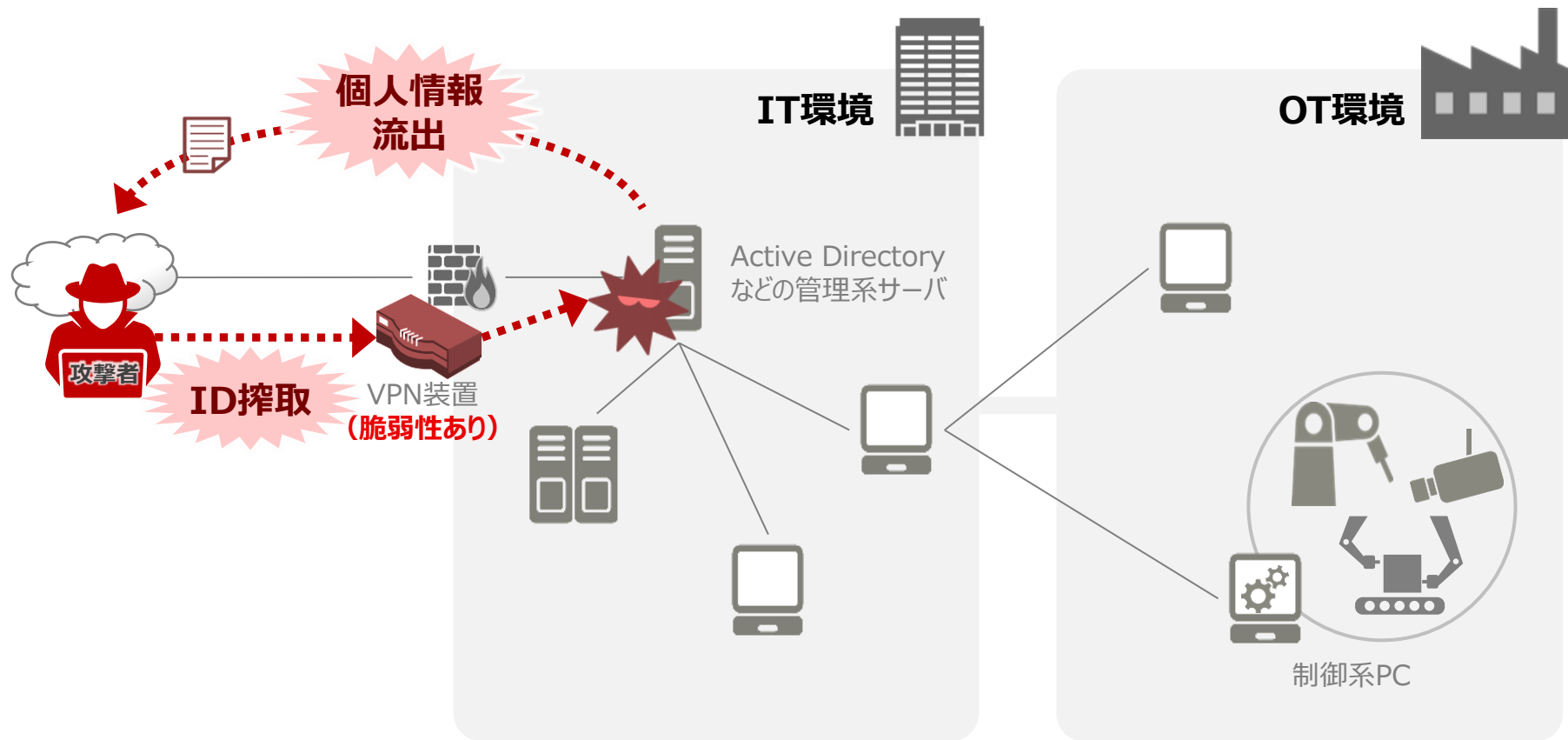
工場が攻撃対象に！

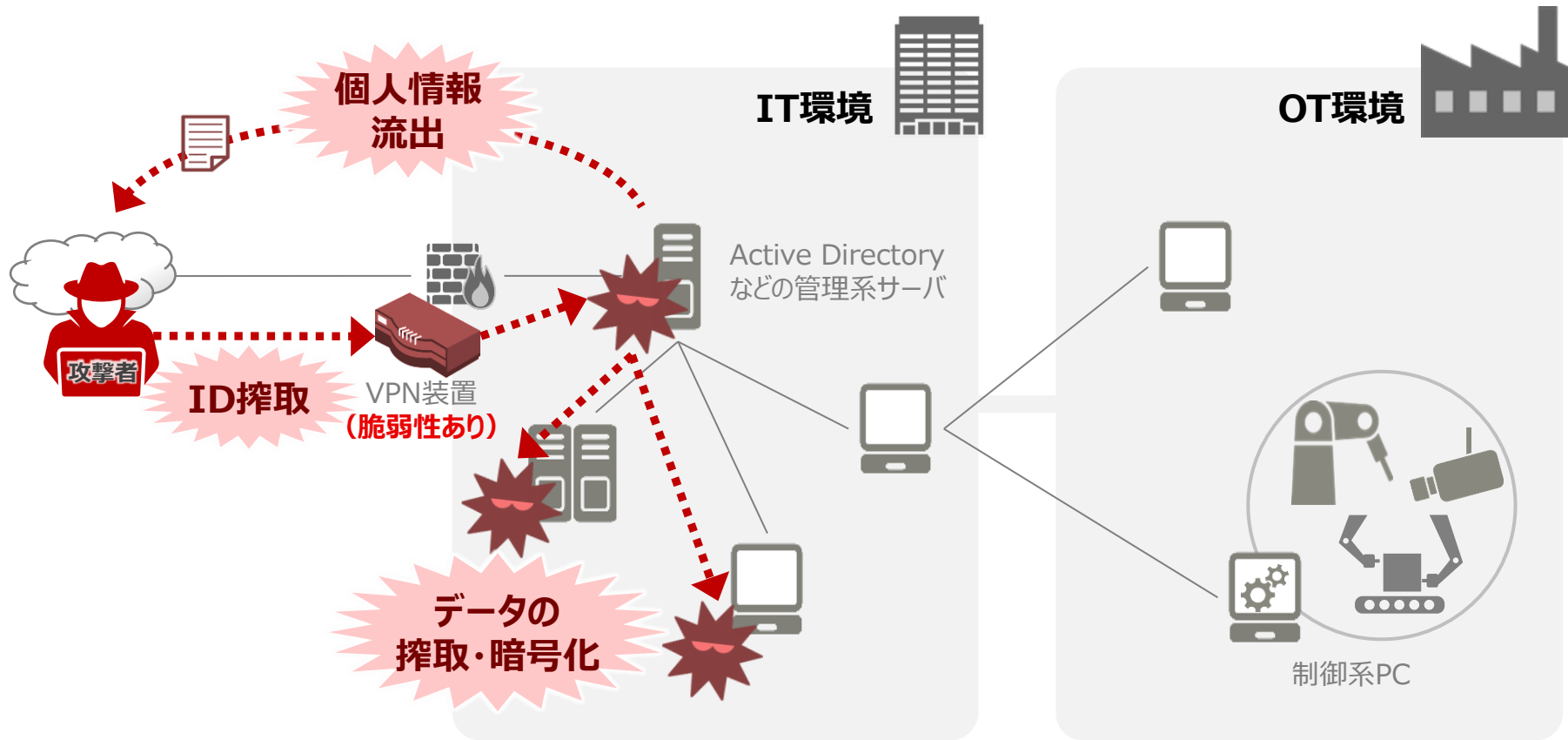
- 標的型ランサムウェアにより、工場系システムがダウン。
- 検査システムや一部作業員のパソコンもウィルス感染。
- 結果、国内外の数工場で操業停止

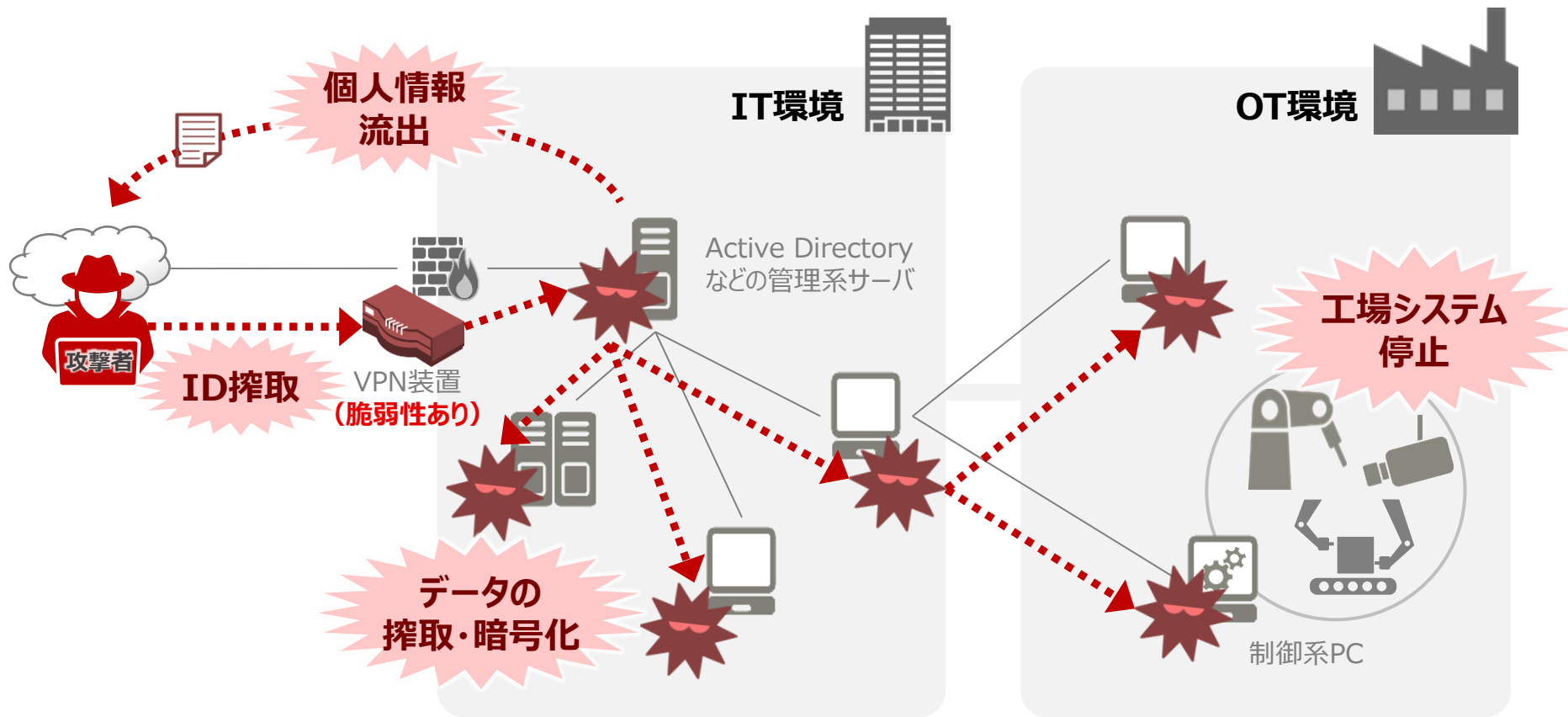
背景を確認してみましよう！
～ 標的型攻撃 ～



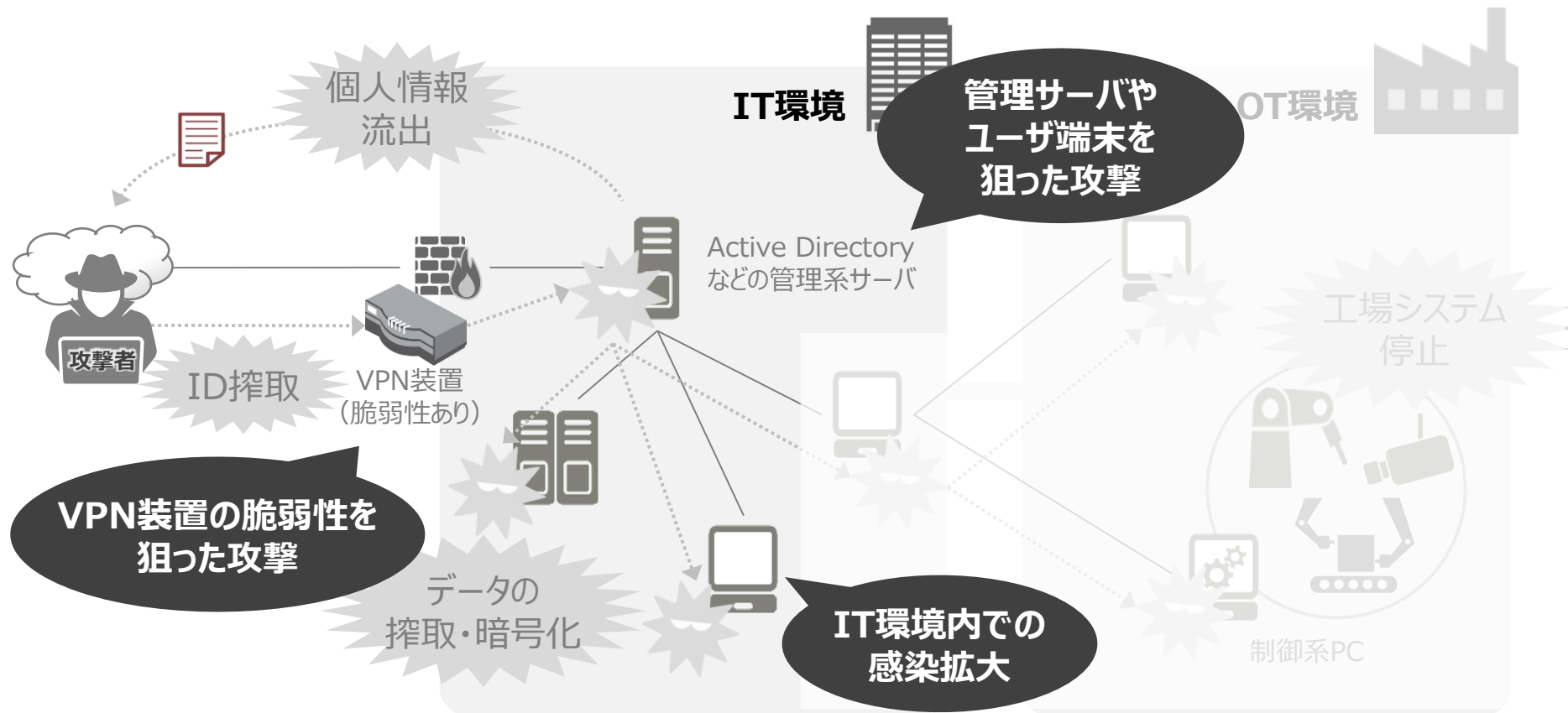




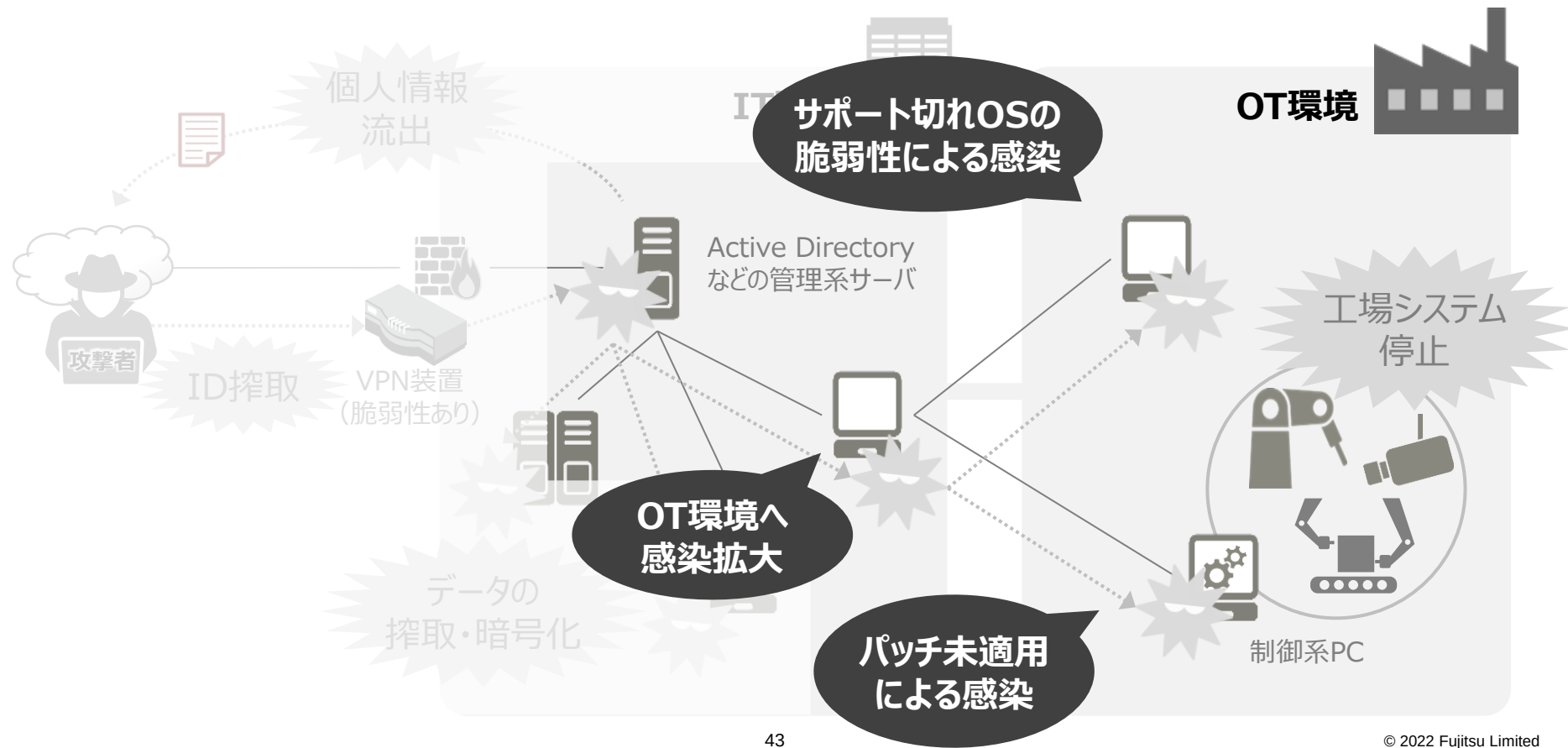




セキュリティ課題はどこに？



セキュリティ課題はどこに？



背景を確認してみましょう！
～ サプライチェーン攻撃 ～

アンコントロールラブルな取引先

自社

サプライヤ・取引先等、
全関係者を
把握しきれていない

チェックシートによる
自己申告ベースの
管理には限界あり

取引先の
セキュリティ状況を
勝手に調査できない

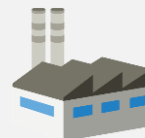
取引関係だから、
強くものが言えない

取引先が多く、
管理しきれない。
人海戦術で
対応せざるを得ない

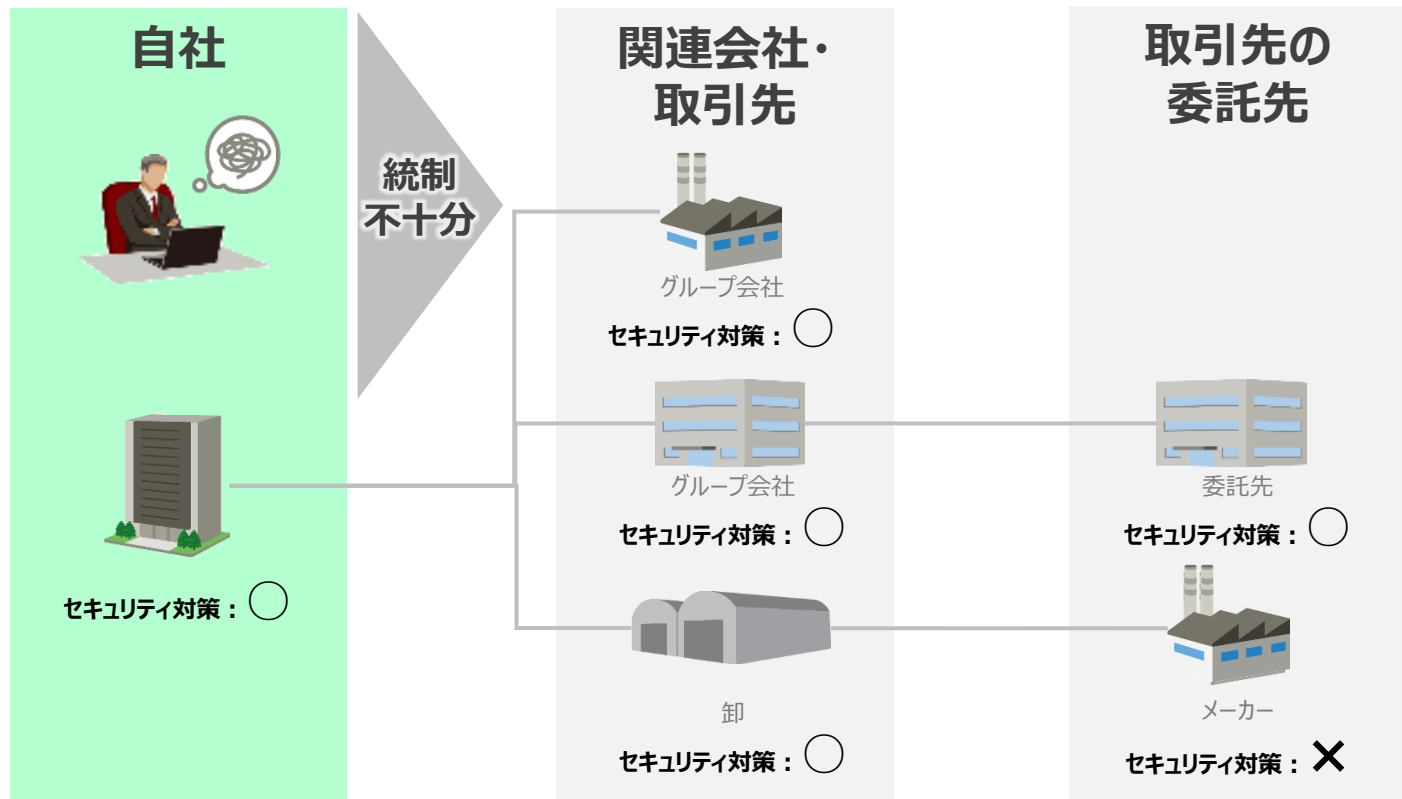


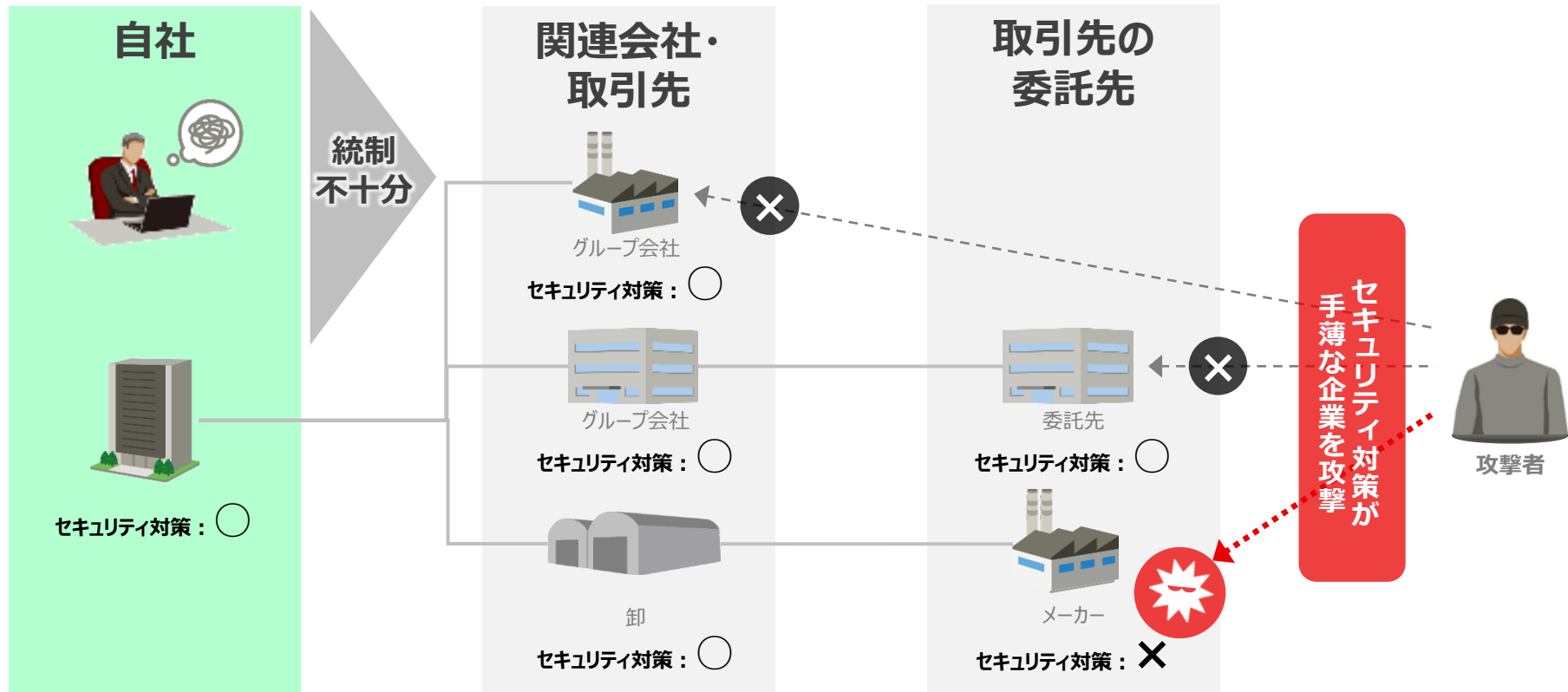
統制
不十分

取引先

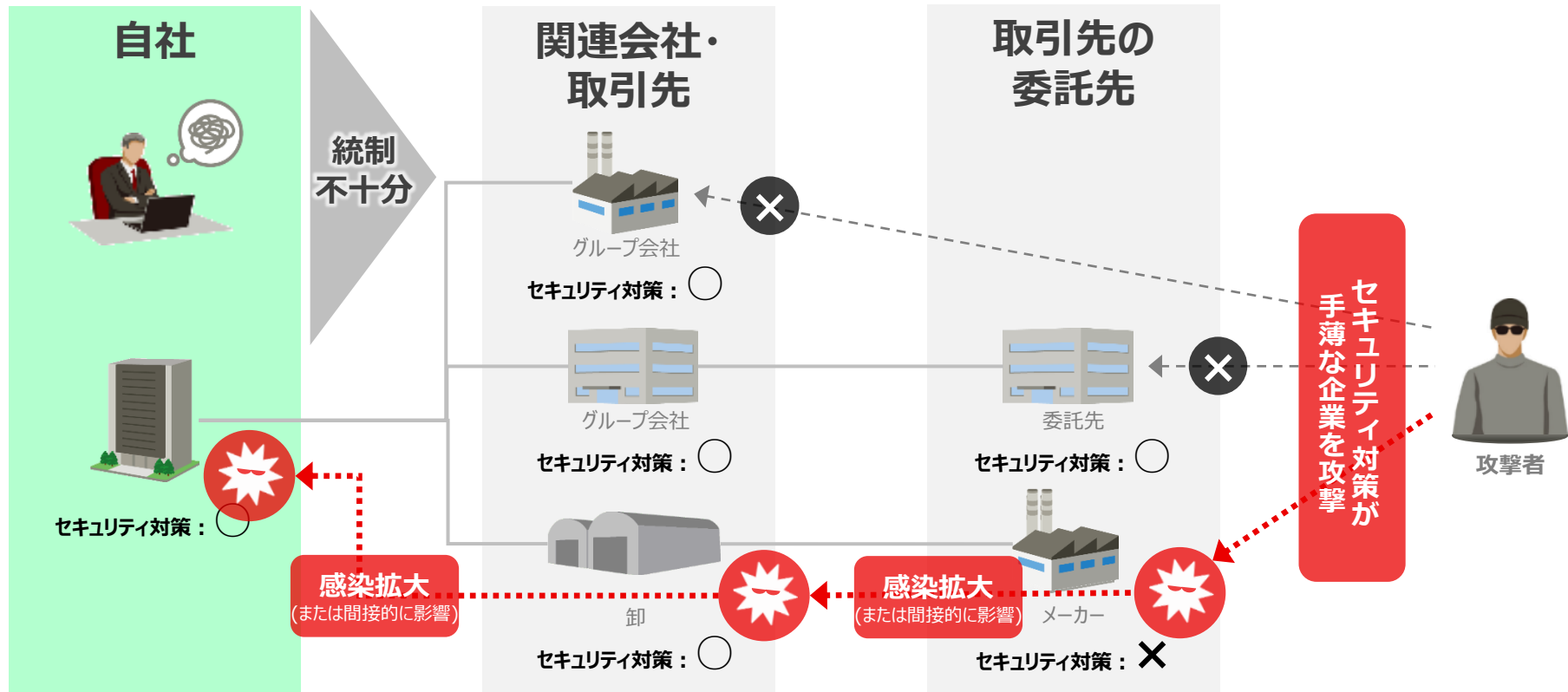


事故の流れ (1/3)





事故の流れ (3/3)



対策をどう見直すべきか？

自社

取引先の変更に応じて
即座・客観的に評価実施

日々、スコアを再計算し
常に最新スコアを把握

非侵入型の
調査手法

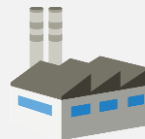
人手を介さない
調査手法による
プロセス最適化、工数削減

公平で
定量的に算出できる
調査手法



統制
不十分

取引先



課題から浮かび上がる対策強化ポイント

標的型攻撃

- VPN装置の脆弱性を狙った攻撃
- 管理サーバやユーザ端末を狙った攻撃
- IT環境内での感染拡大
- OT環境へ感染拡大
- サポート切れOSの脆弱性による感染
- パッチ未適用による感染

サプライチェーン攻撃

- 取引先の変更に応じて
即座・客観的に評価実施
- 日々、スコアを再計算し最新スコアを把握
- 非侵入型の調査手法
- 人手を介さない調査手法による
プロセス最適化、工数削減
- 公平で定量的に算出できる調査手法

脆弱性の可視化

- ・ IT機器の脆弱性を把握
- ・ サプライチェーン全体での脆弱性を把握

エンドポイントセキュリティ

踏み台となる端末上で
脅威の早期発見・迅速対処

OTセキュリティ

OT機器の可視化と
脆弱性把握

脆弱性の可視化

社内外IT環境の脆弱性を診断し可視化を実施

ポイント①

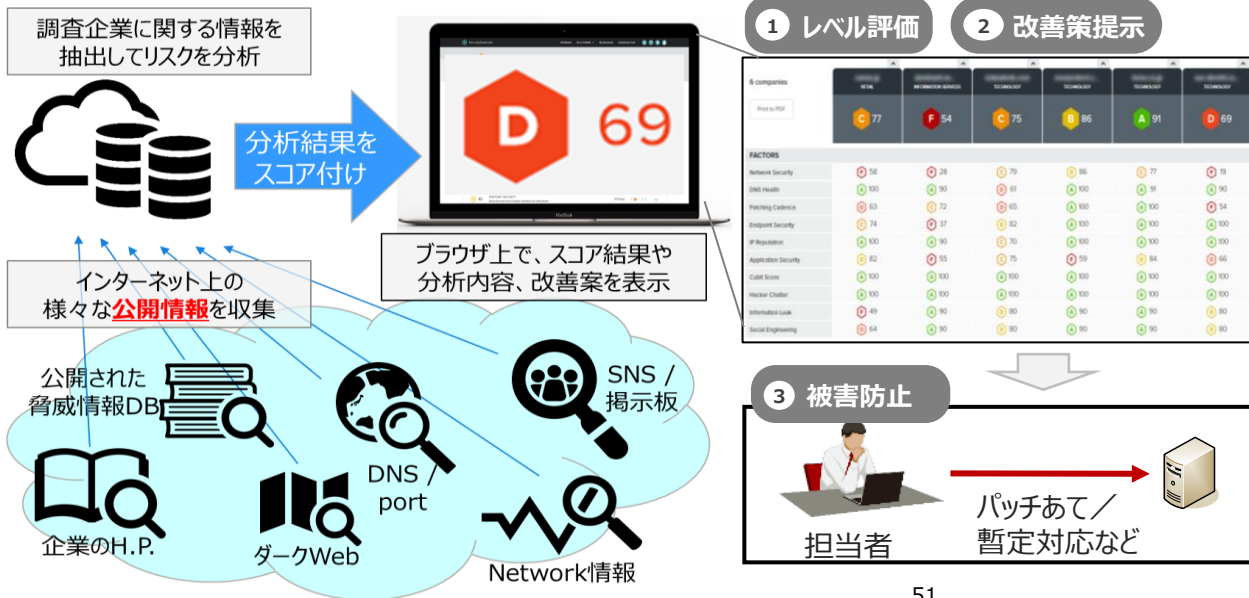
セキュリティ対策状況
を客観的に評価

ポイント②

弱点の洗い出しにより
改善策を検討

ポイント③

自社だけに限らず
関連会社やサプライチェーンも



取扱ソリューション

- SecurityScorecard
- 脆弱性診断・管理サービス

エンドポイントセキュリティ(EDR)

エンドポイント上での疑わしい挙動を分析、迅速な検知・対応を実現

ポイント①

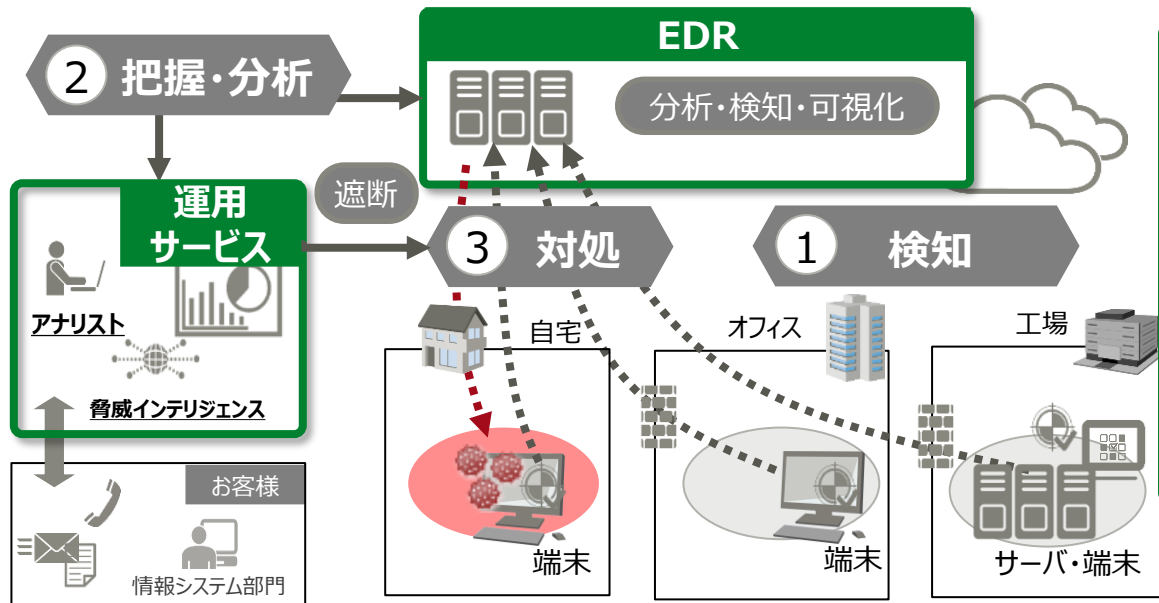
攻撃者による
端末の感染活動を検知

ポイント②

攻撃の全体像を
把握・分析

ポイント③

運用サービスによる
迅速かつ適切な対応



取扱ソリューション

【EDR】

•Cybereason EDRサービス

•Trend Micro

Apex One™ SaaS with XDR^{※1}
•Palo Alto Networks Cortex XDR^{※2}

+

【運用サービス】

•富士通インテリジェンスマネージド
セキュリティサービス (IMSS)

※1 【サービス名称】FENICS CloudProtect エンドポイントセキュリティ powered by Apex One SaaS + XDRオプションサービス

※2 【サービス名称】FENICS CloudProtect XDR for Endpoint powered by Cortex XDR from Palo Alto Networks

OT環境の可視化により、生産ラインの安定稼働を実現

ポイント①

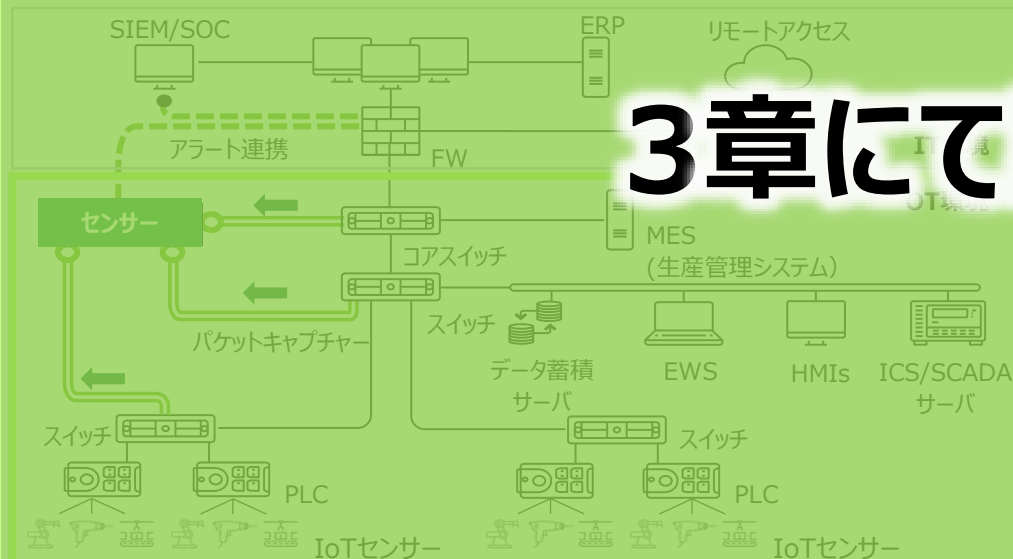
OTネットワーク上の機器情報の
収集とリスク把握

ポイント②

通常の通信を自動学習し、
異常通信を自動検知

ポイント③

アクセス元/先の情報を監視し、
不正アクセスを検知



3章にて説明

ネットワーク状況の自動可視化に
理工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

日々、サイバー攻撃は高度化・複雑化しています。

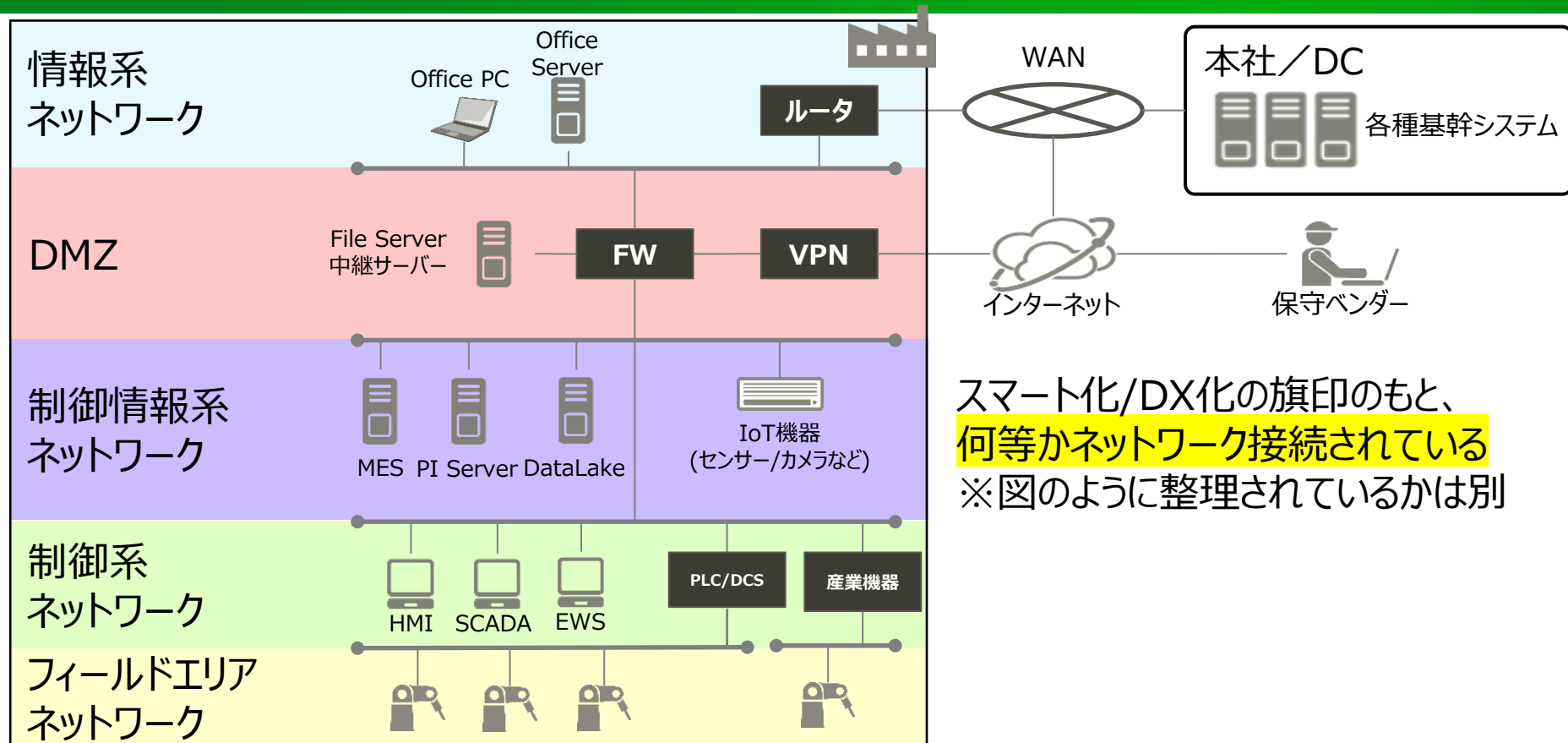
定期的に対策状況を見える化することで
適切な対策の導入とIT環境の健全化
につなげていきましょう！

1. ITとOTを取り巻くサイバー状況

2. 製造業におけるセキュリティ対策

3. OTセキュリティ対策のベースとなるソリューション

生産現場は既に何等かつながっている



スマート化/DX化の旗印のもと、
何等かネットワーク接続されている
※図のように整理されているかは別

生産現場はセキュリティに弱いものが多い

必ずしも生産現場が狙われるわけではない

しかし、生産現場に脅威が入り込むと瞬く間に被害が出る

汎用技術・製品の採用

クローズドな環境からオープンな環境へ

従来の生産設備は、セキュリティ対策が考慮されていない

セキュリティパッチを充てられない、動作確認のための検証ができない

ライフサイクルが長い、OSサポート切れでも利用し続ける

↳ 保全活動による耐用年数・寿命の延伸

- 生産現場は外部とつながっている
 - 既に何等かIT領域とネットワーク接続
- 生産現場は脆弱なものが残る
 - 元々セキュリティが脆弱なものが多い
 - 保全活動により生涯現役

IT領域はこれまで以上に対策を実施しつつ、
生産現場のセキュリティ耐性も高めていく
ことが必要

- ・何が、どこと、どんなことをしているのか、“いつもの状態”を知っておく
- ・“いつも”を知っていれば、“異常”に気づく
- ・異常に気付けば、対処ができる

●セキュリティセンサーをつなぐだけで、“いつもの状態”と“異常”がわかる

特長
1

生産現場のネットワーク状況をリアルタイムに把握

OTネットワーク上の機器情報を自動収集。
台帳管理や定期的な現場サーベイが不要

特長
2

生産業務の継続性・健全性を向上

OTネットワーク上の機器に対する脆弱性や通信内容を管理。
異常発生時の対応リコmendにより、早急にリスクを排除

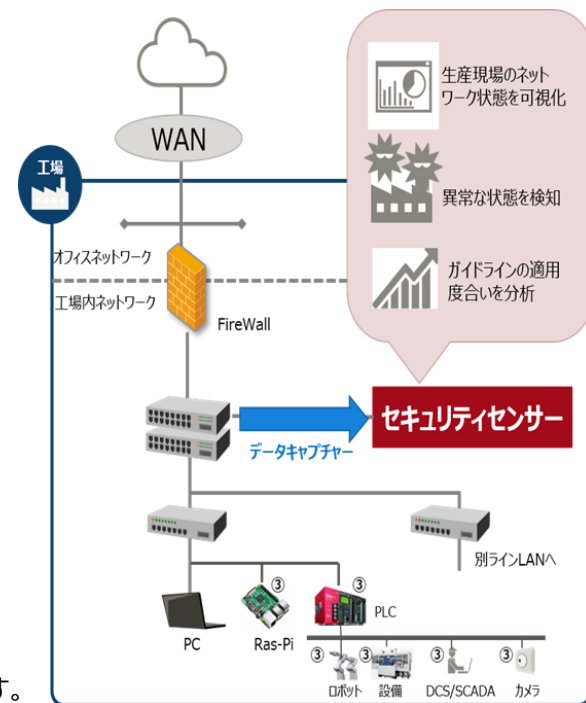
特長
3

実施した対策の有効性を直感的に把握

国際・業界標準ガイドラインへの適合度合いをスコア化。
取るべき対策とその効果が明確になり、効率よく高度化

※セキュリティセンサーとしてSCADAfence社が提供する**SCADAfenceプラットフォーム**を利用しています。

※SCADAfenceプラットフォームはソフトウェア製品です。別途インストールするサーバー機等が必要となります。



“いつもの状態”を知る

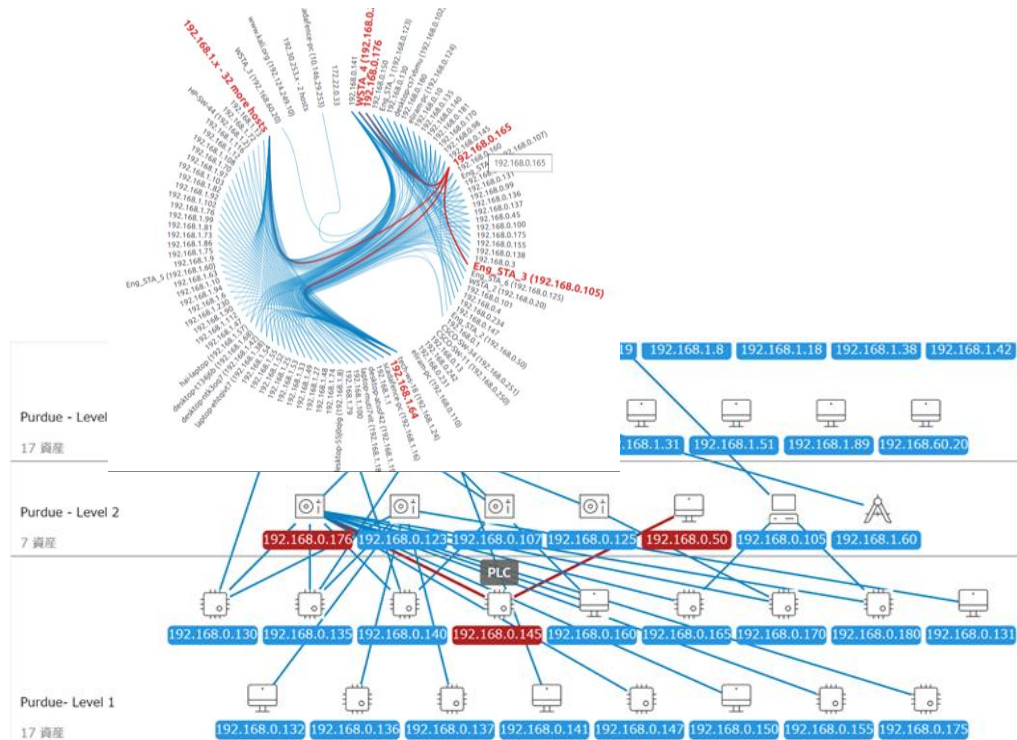
何がつながっているか

資産							
Assets Pivot							
	IP	ホスト名	MAC	ベンダー	OS	資産タイプ	アラート数
+	192.168.0.176		00:0C:26:0C:A4:57	Wentek Labs, Inc.	Linux	HMI, BACnet Device	0
+	192.168.0.180		00:01:05:3B:D8:00	Beckhoff Automation GmbH	PLC, BACnet Device		0
+	192.168.0.120		58:52:8A:B7:AB:EC	Mitsubishi Electric Corporation	PLC		0
+	192.168.0.125	Eng_STA_6	00:0C:29:8B:18:06	VMware, Inc.	Windows 7	PLC, Engineering St...	1
+	192.168.0.155		00:24:59:0A:A9:C4	ABB Automation products GmbH	PLC		0
+	192.168.0.102	desktop-c-	80:83:FE:78:52:15	Dell Inc.	Windows 10	PLC	1
+	192.168.0.123	Eng_STA_1	00:0C:29:17:D1:76	VMware, Inc.	Windows 7	Industrial Device, E...	0
+	192.168.0.140		00:80:F4:1B:CD:22	Telemecanique Electrique	PLC		0
+	192.168.0.107	Eng_STA_4	00:0C:29:58:97:76	VMware, Inc.	Windows 7	HMI, Engineering St...	1 2
+	192.168.0.135		AC:64:17:12:5C:51	Siemens AG	PLC		3
+	192.168.0.145	192.168.0.145 (PLC-145)					
+	192.168.0.1						
+	192.168.0.3						
+	192.168.0.1						

1 注意	6 警戒	接続: 4 内部
------	------	----------

デバイスタイプ:	PLC	その他詳細
OS:		モジュール数: C32M-CPU32
ホスト名:	PLC-145	ファームウェアバージョン: 02.01
ベンダー:	Omron Tateisi Electronics Co.	Icon Size: 23
MAC:	00:00:5A:3B:56:2F	Memory Card Type: No memory card
初回登録:	March 17th 2019, 21:21:13	
最終更新日時:	April 24th 2019, 22:09:13	
NICタイプ:	Ethernet	

どこがつながっているか



“異常”に気付く ①脆弱性に気付く

● CVE(Common Vulnerabilities and Exposures)情報との合致

- 自社OT機器の該当状況と、対策が必要な脆弱性を正しく優先順位付け可能

SCADAfenceが対処しているCVEを表示



エクスポート先: CVE の管理

未処理 594 システムにより 再確認済み に設定 前未確認 確認済み 16 すべてのステータス

☐	CVE ID	公開済み	スコア	ステータス	ベンダー	資産の総数	説明
☐	CVE-2020-5527	03/30/20 17:15:00	2.9	レビュー済み	mitsubishielectric	1	When MELSOFT transmission port (UDP/IP) of Mitsu...
☐	CVE-2020-7475	03/24/20 04:15:00	6.4	レビュー済み	schneider-electric	4	A CWE-74: Improper Neutralization of Special Eleme...
☐	CVE-2020-7579	03/11/20 05:15:00	2.9	レビュー済み	siemens	2	A vulnerability has been identified in Spectrum Powe...
☐	CVE-2019-18336	03/11/20 05:15:00	6.9	レビュー済み	siemens	2	A vulnerability has been identified in SIMATIC S7-30...
☐	CVE-2019-19277	03/11/20 05:15:00	4.9	作成済み	siemens	2	A vulnerability has been identified in SIPOPT MP (All ...



CVE-2020-7475 - 概要

CVE ID: CVE-2020-7475 ベンダー: schneider-electric

公開済み: 03/24/20 04:15:00 更新済み: 03/24/20 04:15:00

CVE 説明

1. A CWE-74: Improper Neutralization of Special Elements in Output Used by a Discretionary Component (Injection), reflective of a vulnerability exists in EcoStruxure Control Expert (all versions prior to V3.2.0), Unity Pro (all versions prior to V3.2.0), Modicon M080 (all versions prior to V3.10), which, if exploited, could allow attackers to transfer malicious code to the controller.

影響を受ける製品

1. schneider-electric | ecostruxure_control_expert | *

2. schneider-electric | unity_pro | *

3. schneider-electric | modicon_m080_firmware | *

4. schneider-electric | modicon_m080 | *

5. schneider-electric | modicon_m080_firmware | *

6. schneider-electric | modicon_m080 | *

関連するコメントと履歴 すべて

Adrian 23/09/20 15:33:55 CVE ID is seen by adrian

各CVEの説明や該当するOT機器ベンダー情報を把握



検索: 合計 4 作成済み 4 解決済み 0 確認済み 0

☐	IP	ホスト名	ベンダー	OS	デバイスタイプ	最新ファームウェア	ステータス	操作
☐	192.168.1.178	PPG-145	Worldwide Inc.	Linux	PLC	18.18 YB	未確認	🔍
☐	192.168.1.180	BAC-v011	Beckhoff Automation		PLC	13.57 YB	未確認	🔍
☐	192.168.1.180	PLC-1240	Wieland electric		PLC	3.35 YB	未確認	🔍
☐	192.168.1.141		Therman cue Elect			2.54 YD	未確認	🔍

1 - 4 of 4 items

各CVEに該当する自社のOT機器の一覧を表示

“異常”に気付く ②リスクに気付く

● MITRE ATT&CK

- 攻撃には段階がある。どの段階まで進行されているかがわかることで生産停止等へのリスクに気付くことができる

生産現場への影響度が高い

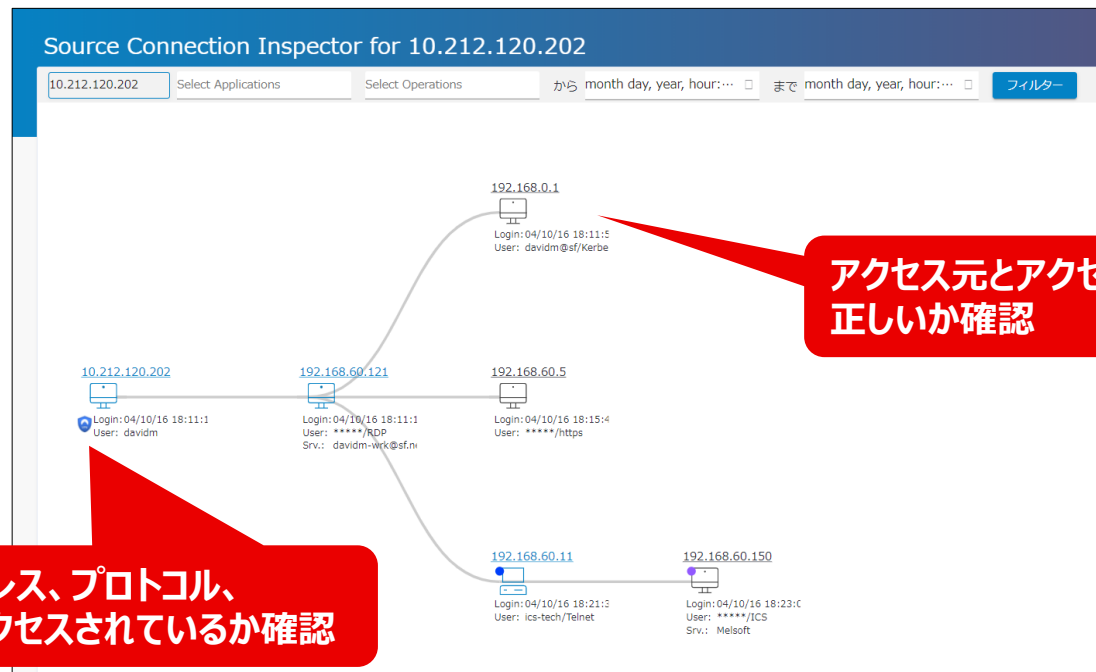
Initial Access	Execution	Persistence	Evasion	Discovery	Lateral Move...	Collection	Command An...	Inhibit Respo...	Impair Proce...	Impact
Drive By Compromise (30)	Change Program State (19)	Program Download (4)	Exploitation For Evasion (1)	Control Device Identification (31)	Default Credentials (1)	Automated Collection (31)	Connection Proxy (30)	Denial Of Service (30)	Change Program State (19)	No Active Alerts
Engineering Workstation Compromise (30)	Man In The Middle (4)	Valid Accounts (1)	Rogue Master Device (34)	IO Module Discovery (30)	Exploitation Of Remote Services (3)	Data From Information Repositories (1)		Modify Control Logic (4)	Modify Control Logic (4)	
Exploit Public Facing Application (5)	Program Organization Units (4)			Network Organization Enumeration (37)	External Remote Services (7)	Role Identification (31)		Program Download (4)	Modify Parameter (4)	
External Remote Services (7)				Network Service Scanning (1)	Program Organization Units (4)				Program Download (4)	
Internet Accessible Device (5)				Remote System Discovery (31)	Remote File Copy (2)				Rogue Master Device (34)	
					Valid Accounts (1)					

※MITRE ATT&CK : MITRE(マイター社)が開発した、「攻撃者の行動を戦術や戦法から分類したナレッジベース(ATT&CK : Adversarial Tactics, Techniques, and Common Knowledge)」

“異常”に気付く ③不正アクセスに気付く

●ユーザーアクティビティ分析

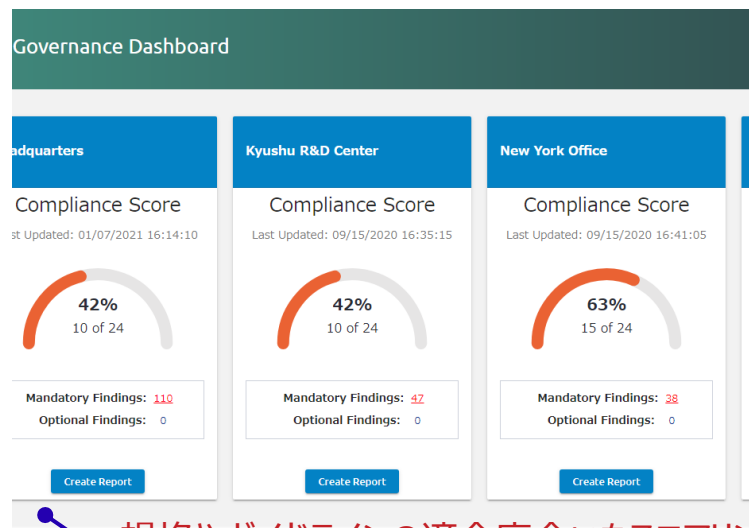
- リモートアクセスを可視化。不正アクセス通信の早期発見が可能



アクセス元とアクセス先の関係が正しいか確認

許可されたIPアドレス、プロトコル、ユーザー情報でアクセスされているか確認

- セキュリティ対策がどの程度できているかを知っておくことも重要です。
- OTネットワークセキュリティ可視化サービスなら、IEC62443/NIST-CSFといった規格やガイドラインへの適合度合いをスコア化できます。



規格やガイドラインの適合度合いをスコアリング

レポート出力、規格やガイドラインが持つ
各項目に対して設備ごとの遵守状況を
詳細に可視化。

Plaintext authentication

There are 140 open alerts

Explanation

Server is running a service that uses authentication, but the network traffic is not encrypted. This means that anyone connected to the network can capture traffic and learn the credentials.

The risk with plaintext authentication is that it allows a malicious agent connected to the network to gain access to the service and the credentials.

Additionally, these credentials might be used by the legitimate user for other services as well, and a malicious agent could access those other services using the same credentials – leading to data theft by unauthorized entities, putting critical network services and industrial processes at risk.

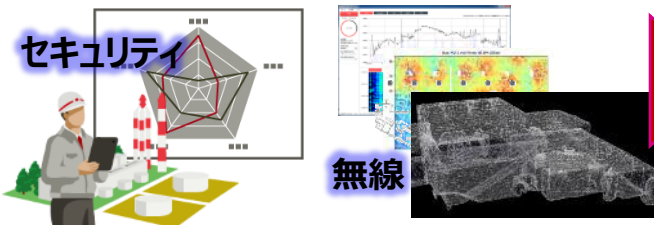
Affected IPs

#	IP	Hostname	Count
1	163.50.140.109	eng_ws_748	4
2	163.50.140.130	m6itasset.hyper.com	8
3	163.50.158.169	m800sg9.hyper.com	4

(ご参考)富士通がお手伝いできること

- 工場ネットワーク環境整備～セキュリティ強化に対して、
現状把握～構想立案～構築・運用までトータルにご支援

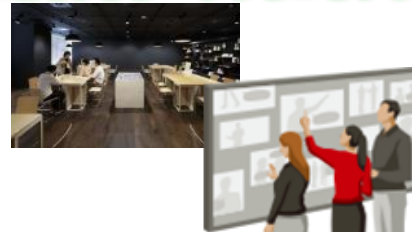
① 工場ネットワークアセスメント



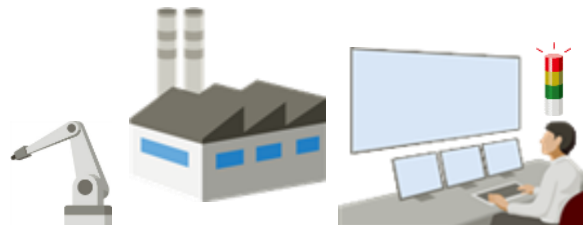
② 脆弱箇所の抽出



③ 工場ネットワークグランドデザイン



⑥ ネットワーク運用支援サービス



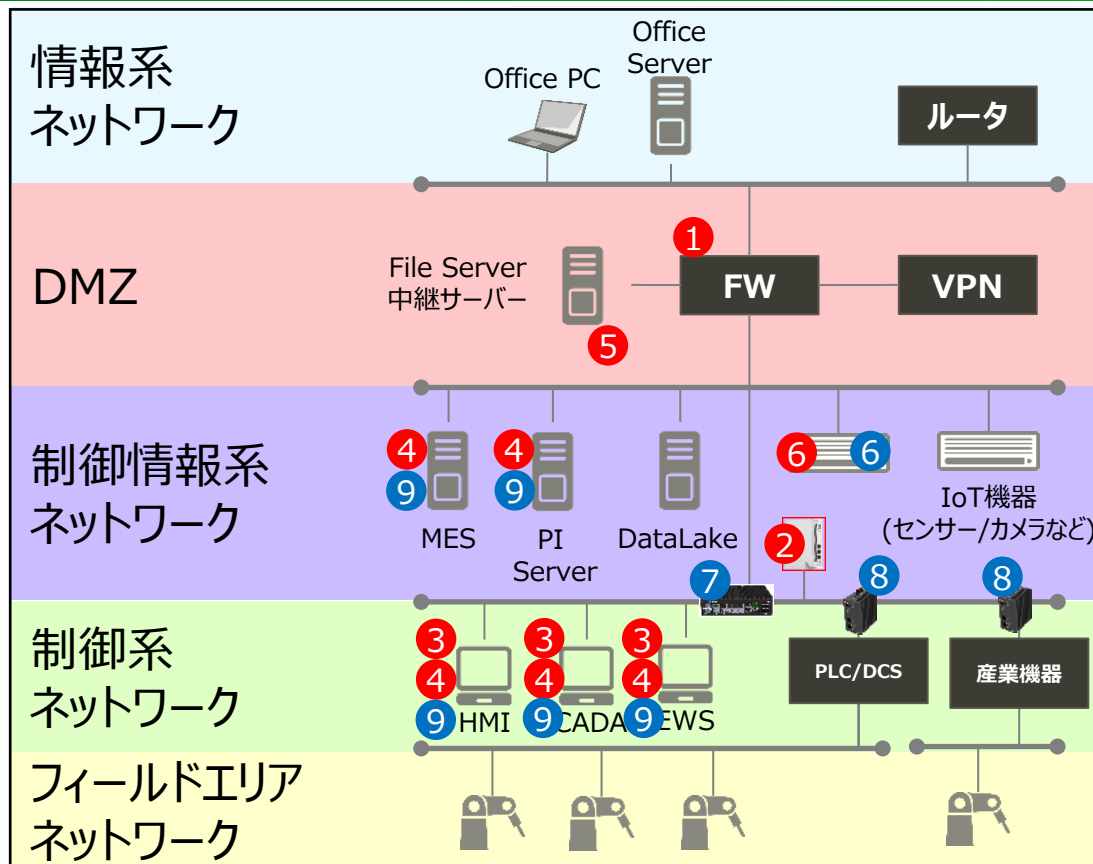
⑤ 脆弱箇所の対処



④ 工場ネットワークインテグレーション



(ご参考)OTセキュリティ ソリューションマップ



- 1 次世代FW**
Cisco ASA、Palo Alto PAシリーズ、FortiGateシリーズ
- 2 iNetSec SF**
制御情報系/制御系ネットワークの接続デバイスの可視化、
管理外デバイスのネットワークからの隔離・遮断
- 3 FENCE-G**
USBメモリ等の外部デバイスへのアクセス制御
- 4 WhiteSec**
サーバー/EWS等で動作するアプリケーションの制御
- 5 FENCE-Works**
情報系ネットワークとやり取りされるファイルの無害化
- 6 OTネットワークセキュリティ可視化サービス(SCADAfence)**
- 6 Cyber Vision(Stealtwatch)**
制御情報系/制御系ネットワークの管理・監視
- 7 ISA3000、EdgeFire**
産業向け次世代ファイアウォール
内部FWとしてライン/セル単位への不要な通信の流入を防止
- 8 EdgeIPS**
産業向け次世代IPS
レガシーOS対策として仮想パッチとして不正通信をブロック
- 9 Stellar Protect/Enforce**
産業用エンドポイント向けアンチウィルス・USBデバイス制御/
ロックダウン

まとめ&QA



IT

攻撃の追跡 

高度な運用の実現 

脆弱性診断 

OT

繋ぎ目の防御 

自動遮断 

USB対策 

工場ネットワーク可視化 

IT

攻撃の追跡

Cybereason EDRサービス,
Trend Micro Apex One™

SaaS with XDR,^{※1}

Palo Alto Networks Cortex XDR^{※2}

高度な運用の実現

インテリジェンスマネージド
セキュリティサービス

脆弱性診断

SecurityScorecard,
脆弱性診断・管理サービス

※1【サービス名称】 FENICS CloudProtect エンドポイントセキュリティ powered by Apex One SaaS + XDRオプションサービス

※2【サービス名称】 FENICS CloudProtect XDR for Endpoint powered by Cortex XDR from Palo Alto Networks

※3【サービス名称】 OTネットワークセキュリティ可視化サービス

OT

繋ぎ目の防御

Cisco ASA, Palo Alto PAシリーズ,
FortiGateシリーズ

自動遮断

iNetSec SF

USB対策

FENCE-G

工場ネットワーク可視化

SCADAfence^{※3}

製造業を守るためには

IT/OTの**特性に応じたセキュリティ**が必要



製造業を守るためには

IT/OTの特性に応じたセキュリティが必要

両面から考慮した対応が必要

製造業を守るためには

IT/OTの特性に応じたセキュリティが必要

両面から考慮した対応が必要

総合的に対応できる富士通にお任せ！

セミナー専用Webのご紹介



セミナー専用Web
より、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/>

ご相談窓口

・ゼロトラストは富士通 推進事務局

contact-securus@cs.jp.fujitsu.com

アンケート

https://fujitsuvoice.eu.qualtrics.com/jfe/form/SV_7aNpLiTMYIzGtGC



【8月4日開催】

製造業が狙われている！今、必要なサイバー攻撃対策
～企業の生命線となるIT/OT環境を両面から守る方策とは～
本日はお忙しい中、ご参加いただき誠にありがとうございます。
お手数ですが、アンケートへのご協力よろしくお願いいたします。

Q/Aを受け付けます



Thank you

