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

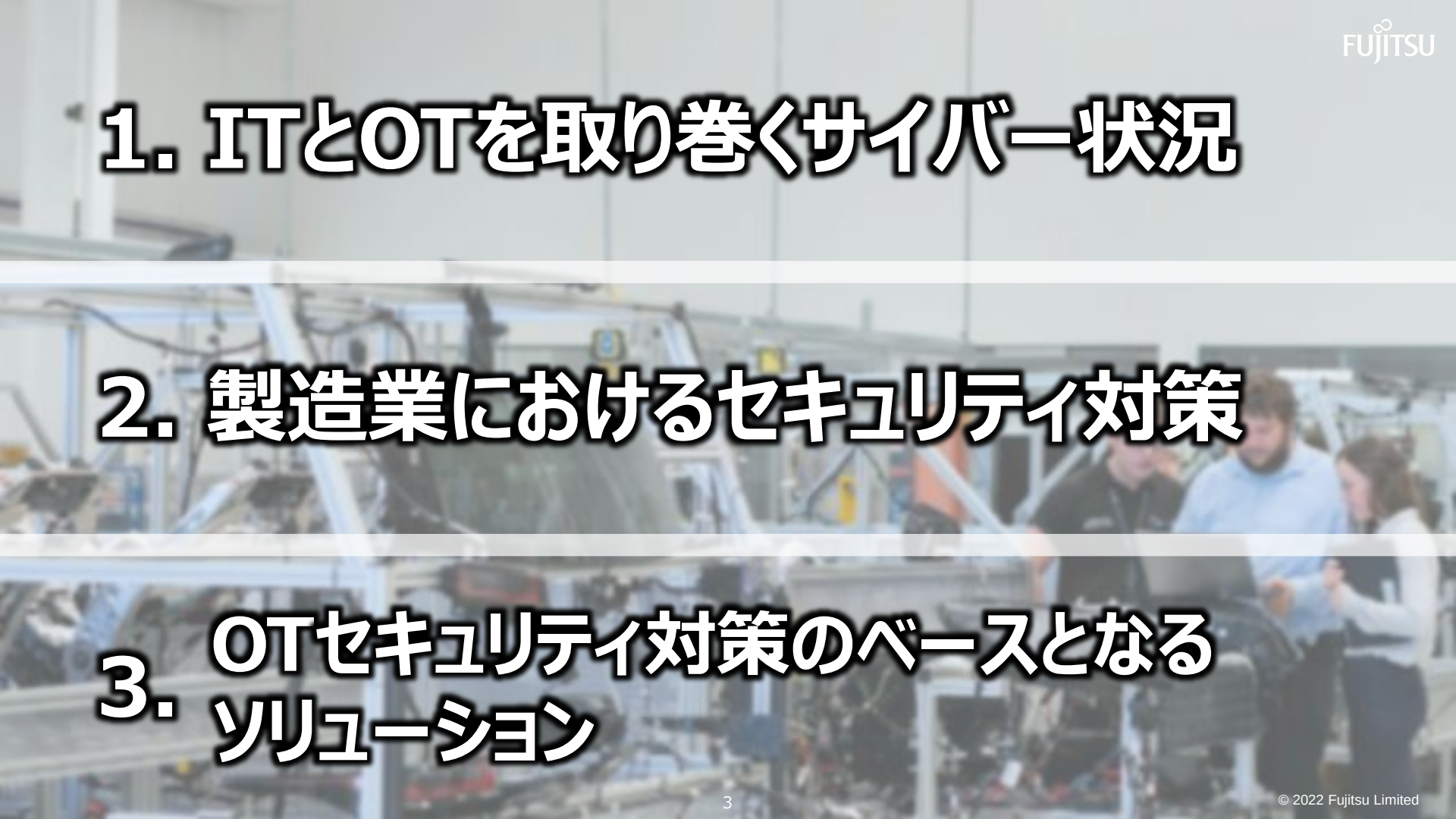
14:40-14:50 まとめ、QA

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



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

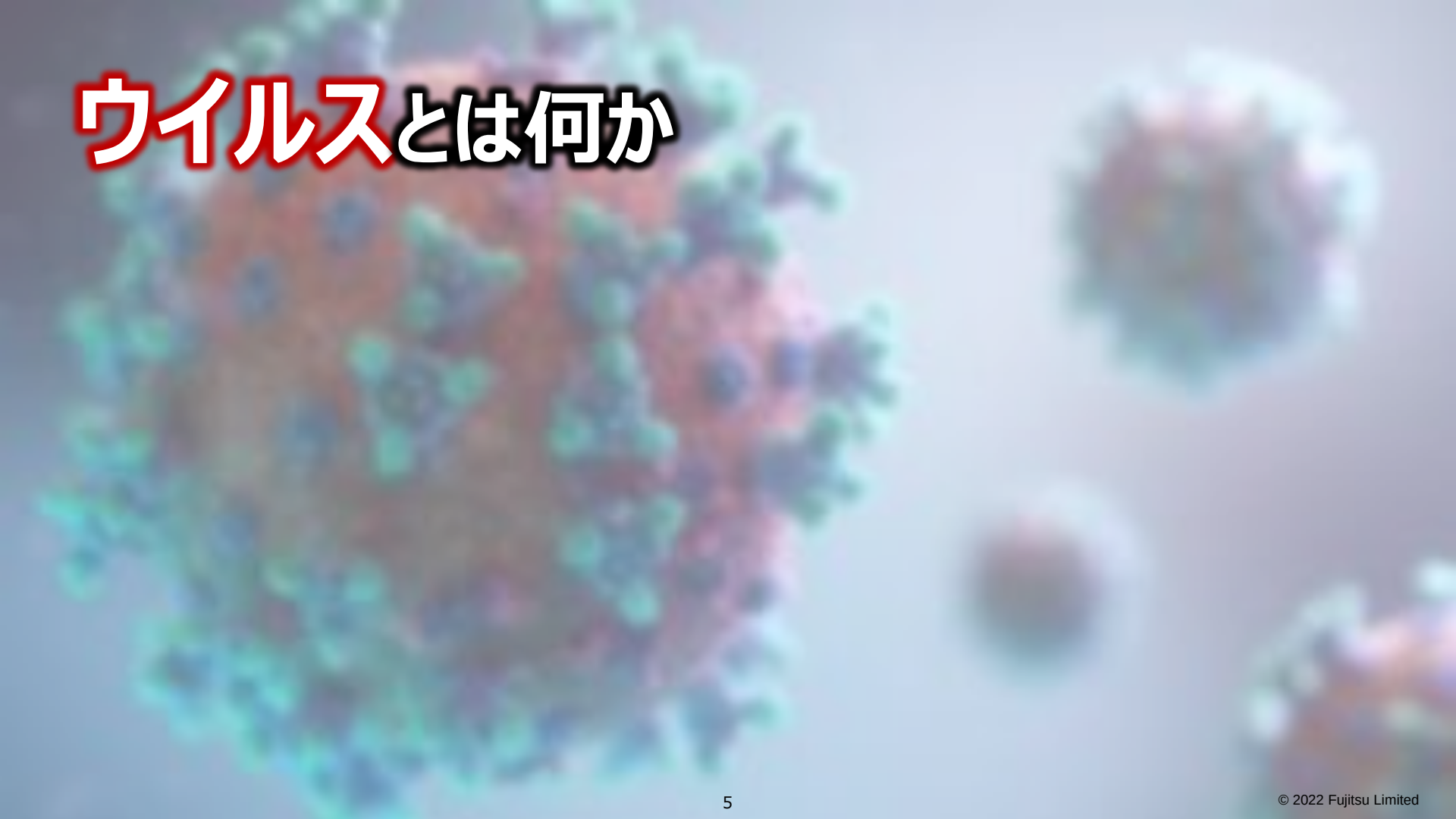
FUJITSU

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

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-wwc-report.pdf, FireEye社

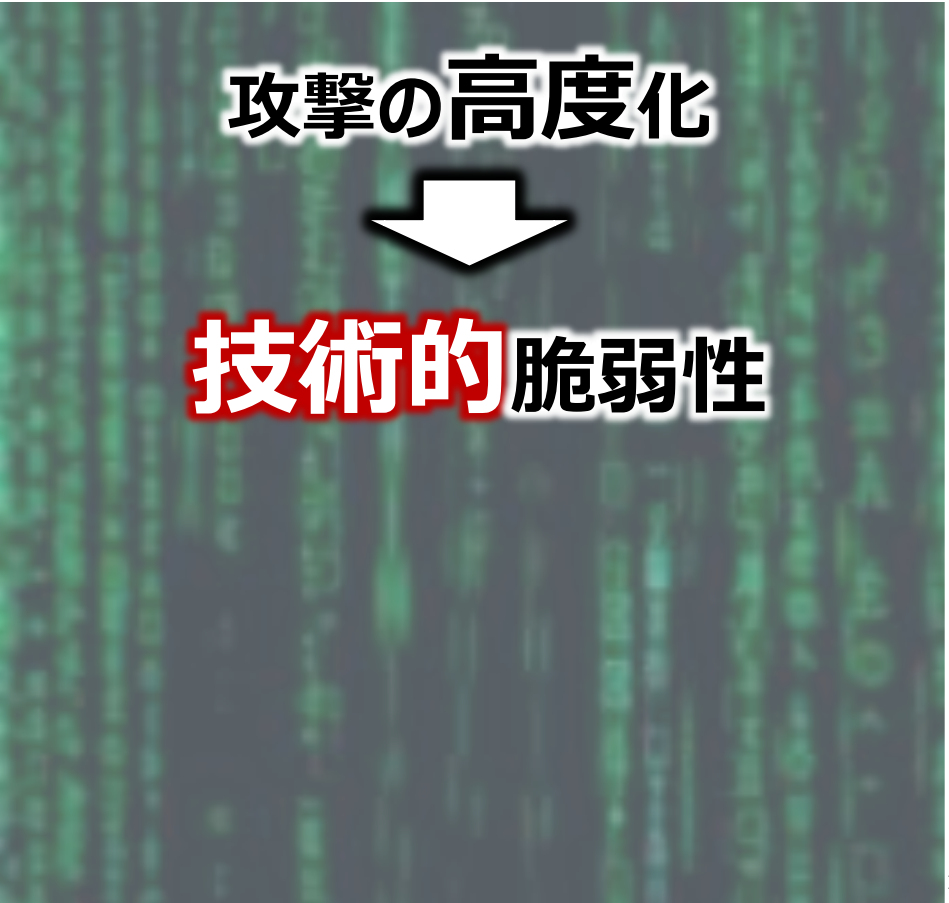
※ 筆者が、世界中の方々（延べ124カ国、227団体）との対話から得た知見を元に本章を構成

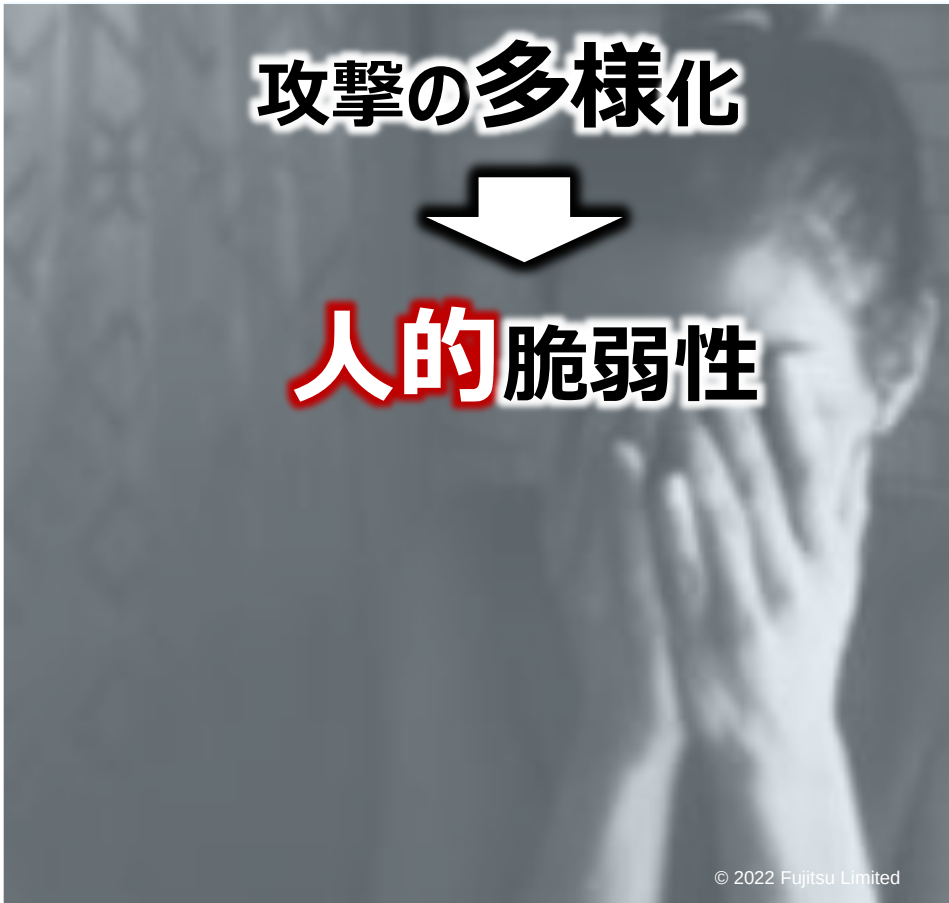
サイバー攻撃はなぜ、攻撃者優位なのか

FUJITSU

サイバー攻撃はなぜ、攻撃者優位なのか

FUJITSU





サイバー攻撃はなぜ、攻撃者優位なのか

FUJITSU

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

※ 参考： Zero-Day Exploits on High Demand on Dark Web, https://cisomag.eccouncil.org/zero-day-exploits-on-high-demand-on-dark-web/, 2021/11/21

技術的脆弱性を突く攻撃

FUJITSU

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※**

※ 参考：日本サイバー軍創設提案, 苫米地 英人 著, サイゾー出版, 2015/11/2

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

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

※ 参考：IPA, 事業継続を脅かす新たなランサムウェア攻撃について, https://www.ipa.go.jp/files/000084974.pdf, 2020/8/20

人的脆弱性を突く攻撃

FUJITSU

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

※ 攻撃内容は、筆者が確認したものを元に再現

人的脆弱性を突く攻撃

FUJITSU

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※

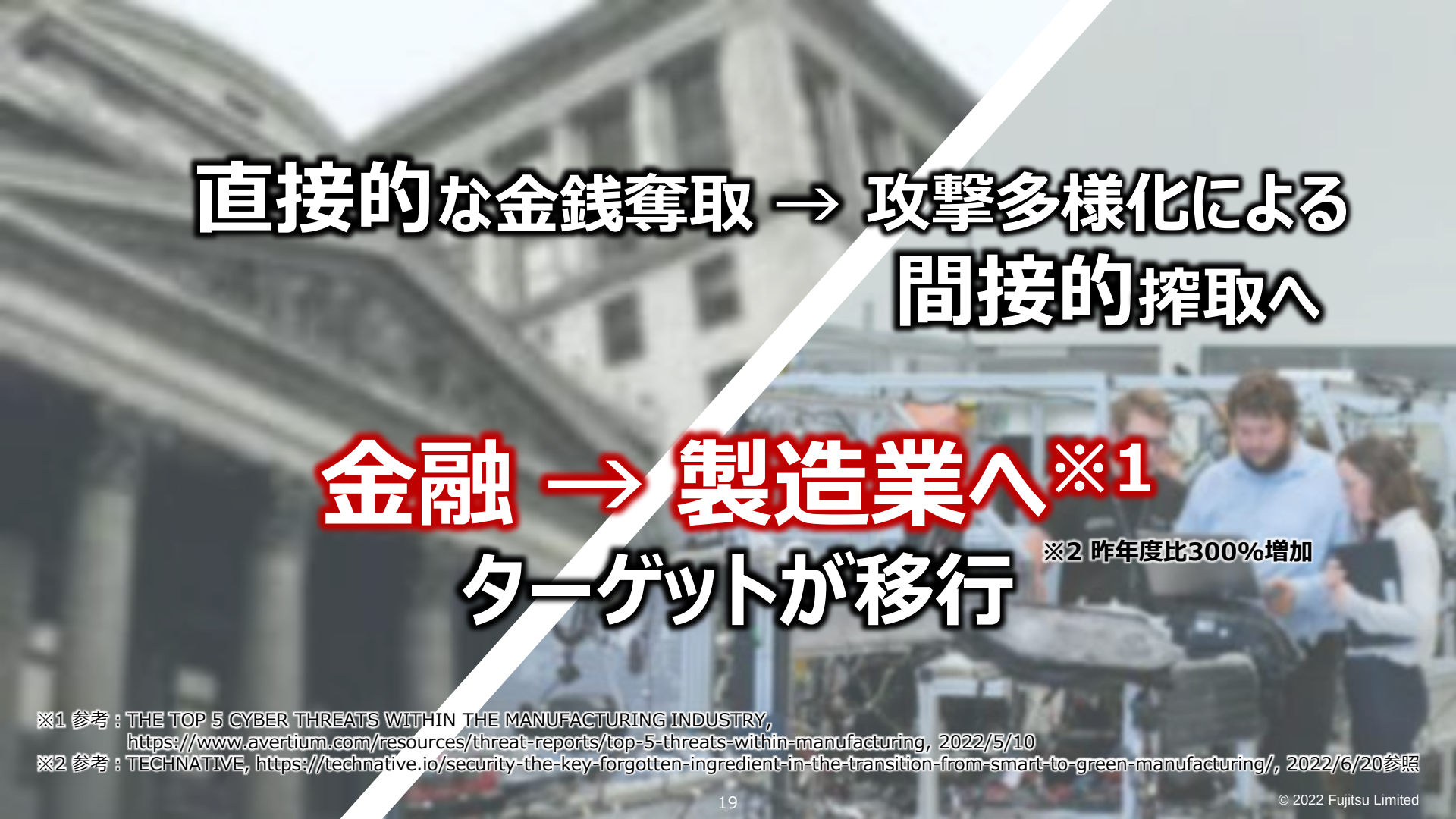
古典的だが
強力

駐車場へばらまく

敷地内に投げ込む

※ 参考：Malicious USB drive, https://www.gdatasoftware.com/blog/2021/11/usb-drives-still-a-danger, 2021/11/30

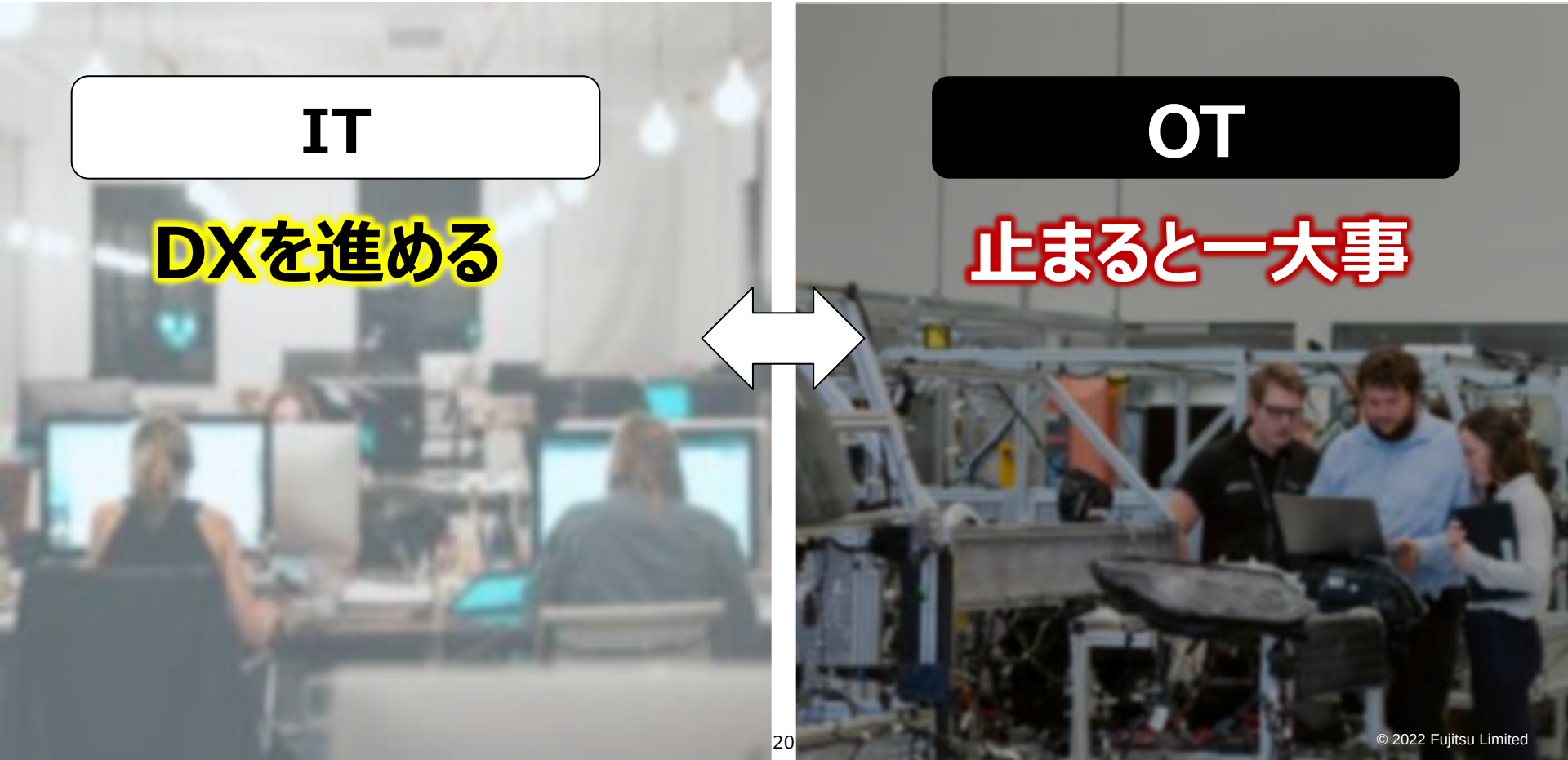
直接的な金銭奪取 → 攻撃多様化による間接的搾取へ



※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

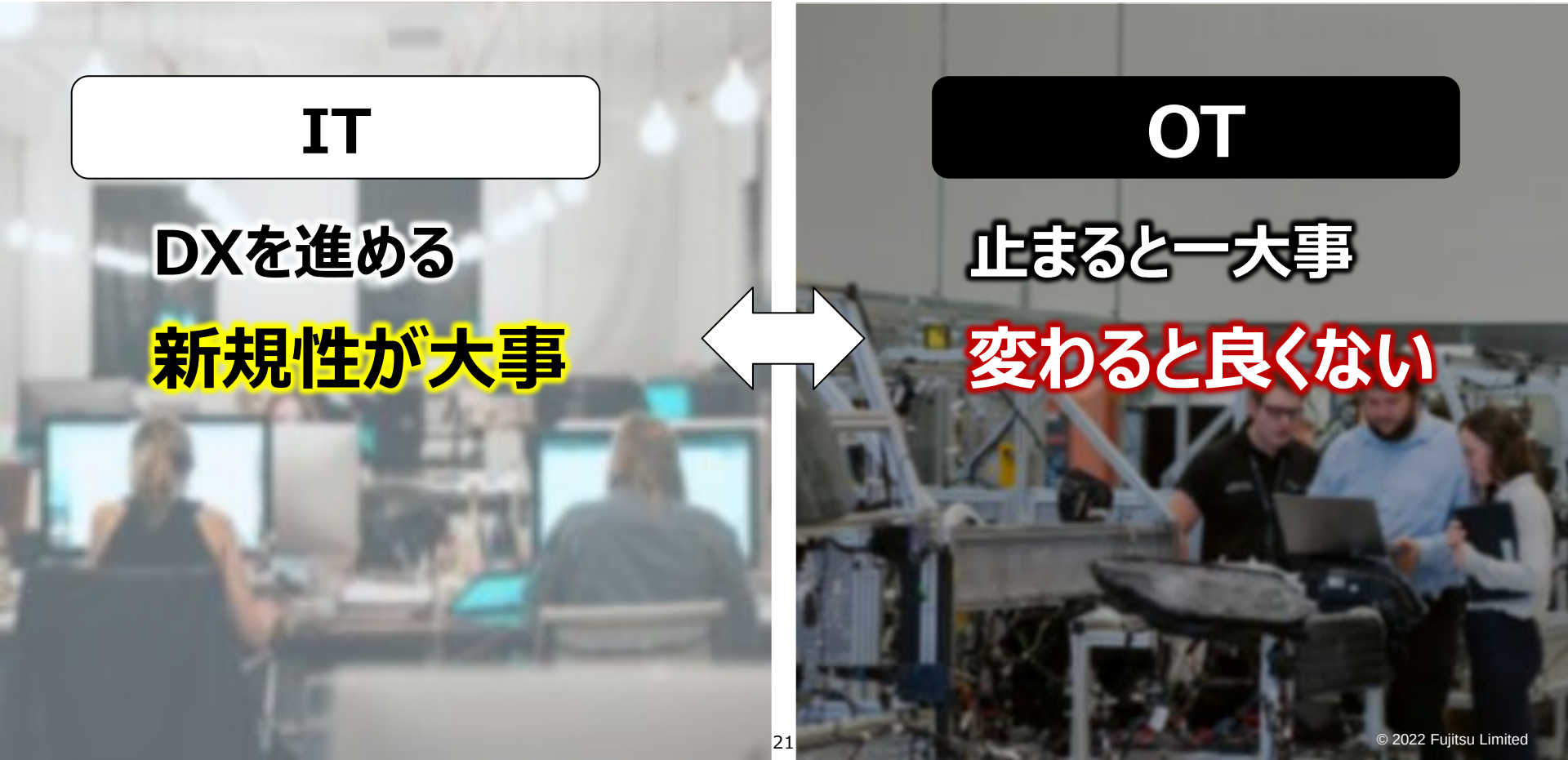
製造業に必要な防御：ITとOT

FUJITSU



製造業に必要な防御：ITとOT

FUJITSU



IT

DXを進める

新規性が大事

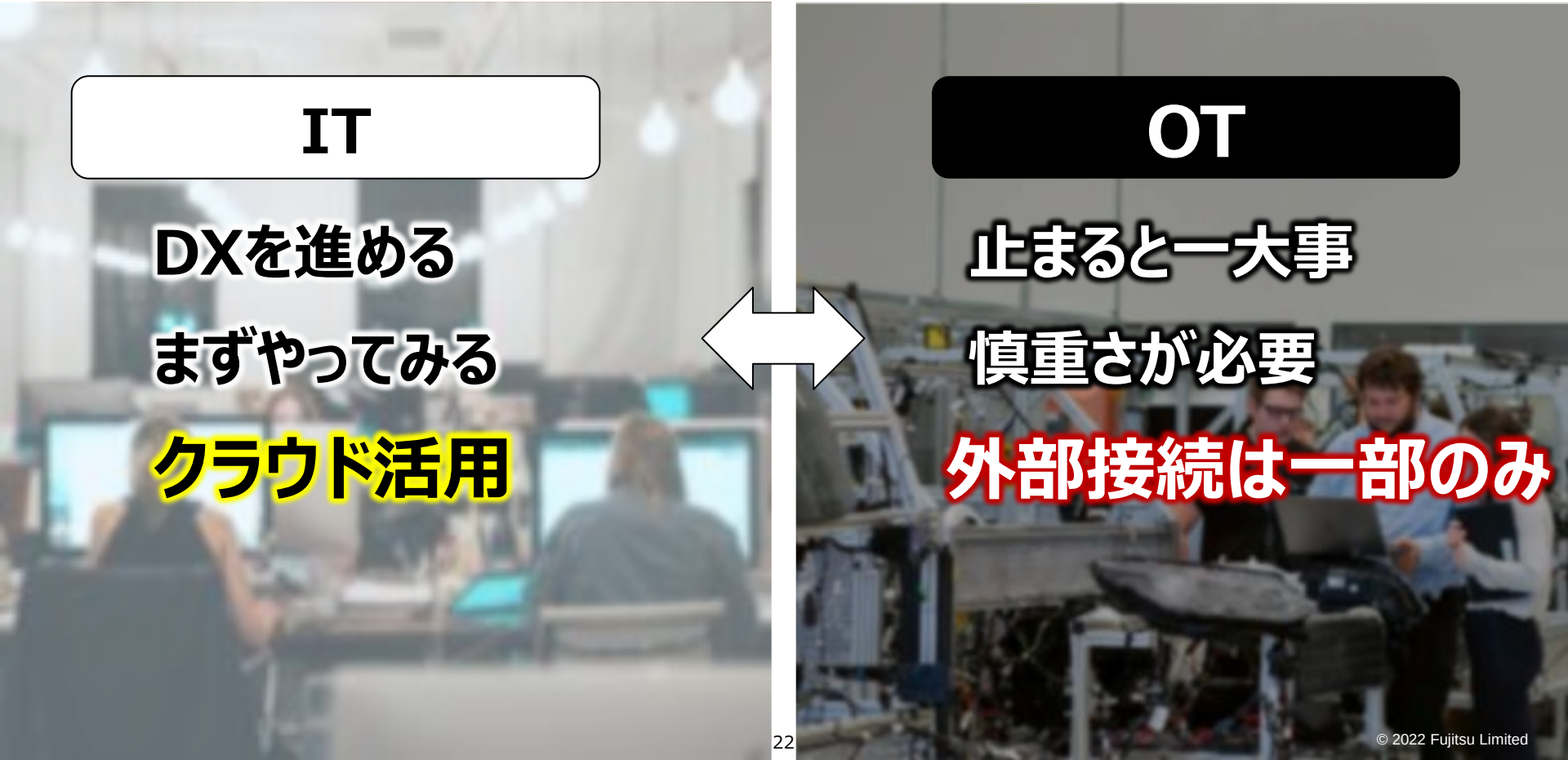
OT

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

FUJITSU



IT

DXを進める

まずやってみる

クラウド活用

OT

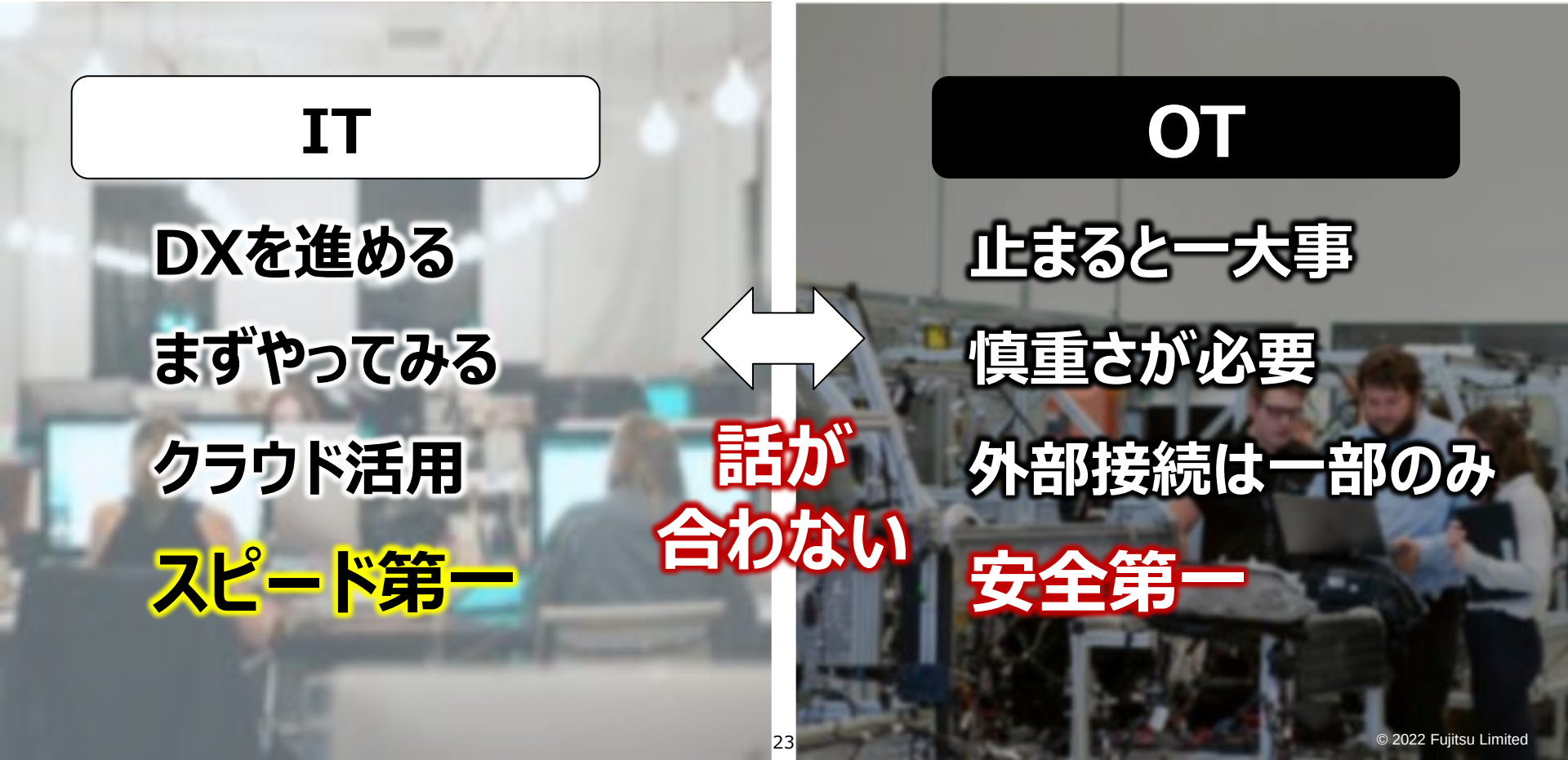
止まると一大事

慎重さが必要

外部接続は一部のみ

製造業に必要な防御：ITとOT

FUJITSU



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

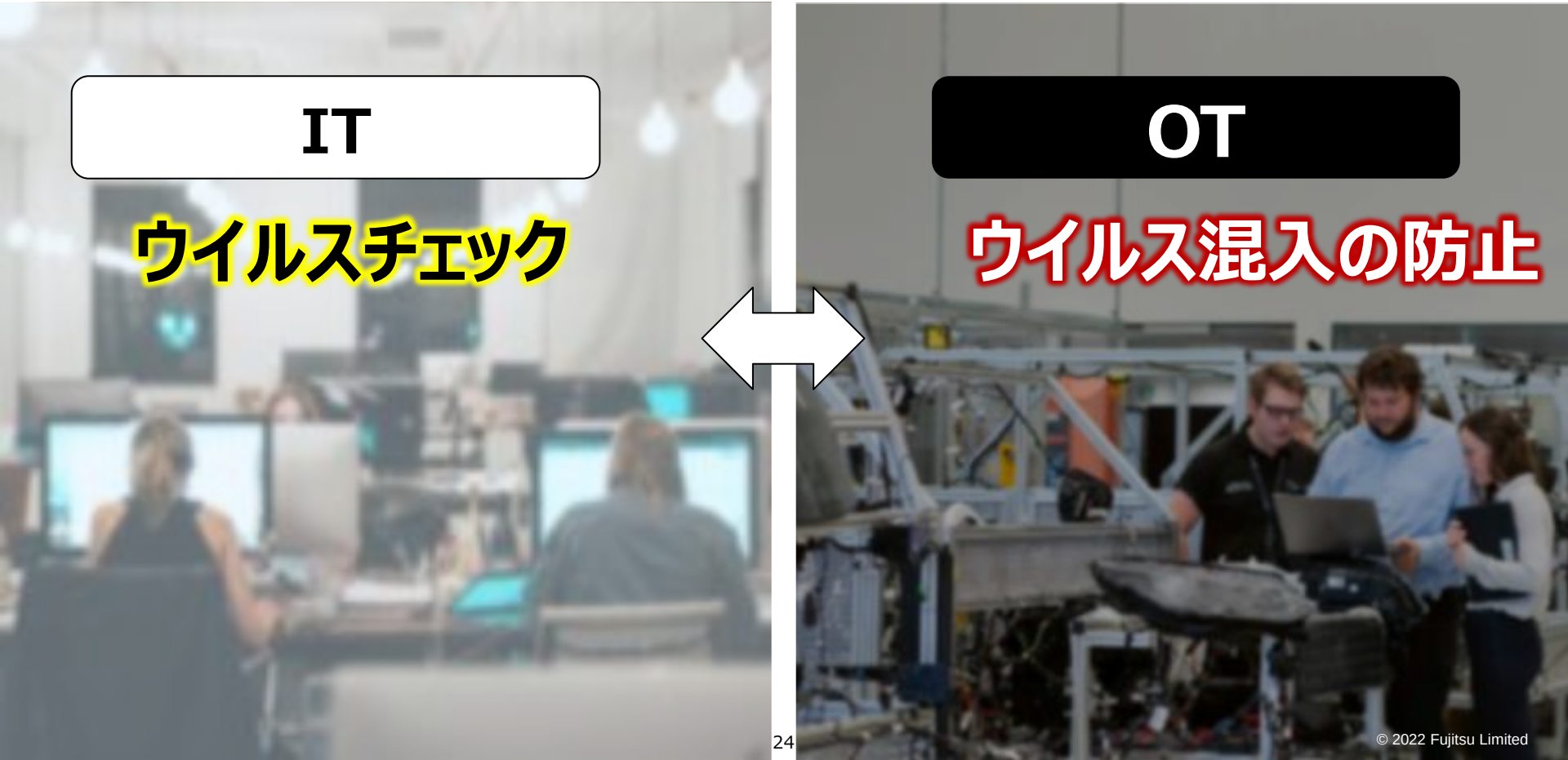
慎重さが必要

外部接続は一部のみ

安全第一

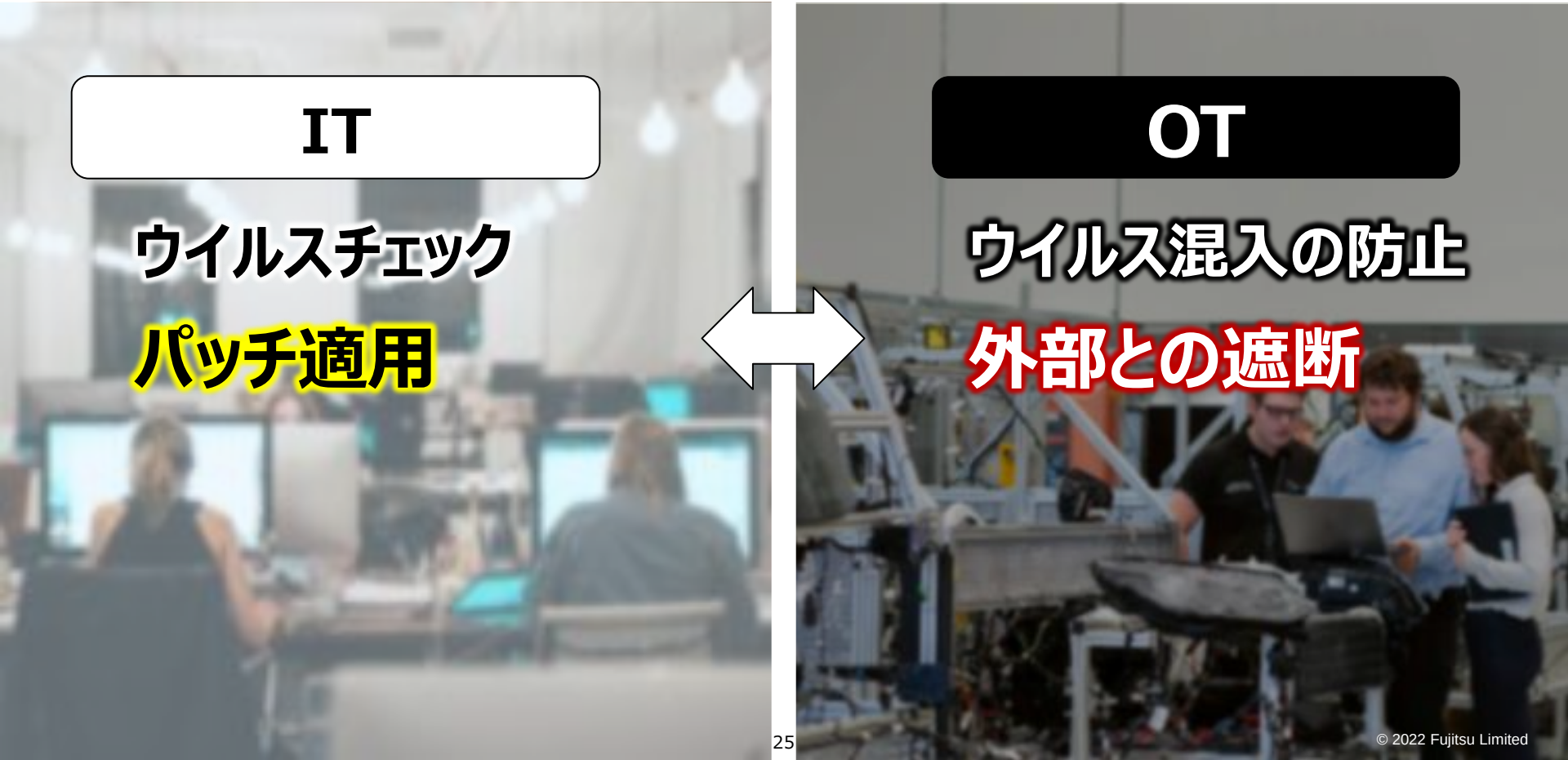
ITセキュリティとOTセキュリティ

FUJITSU



ITセキュリティとOTセキュリティ

FUJITSU



IT

ウイルスチェック

パッチ適用

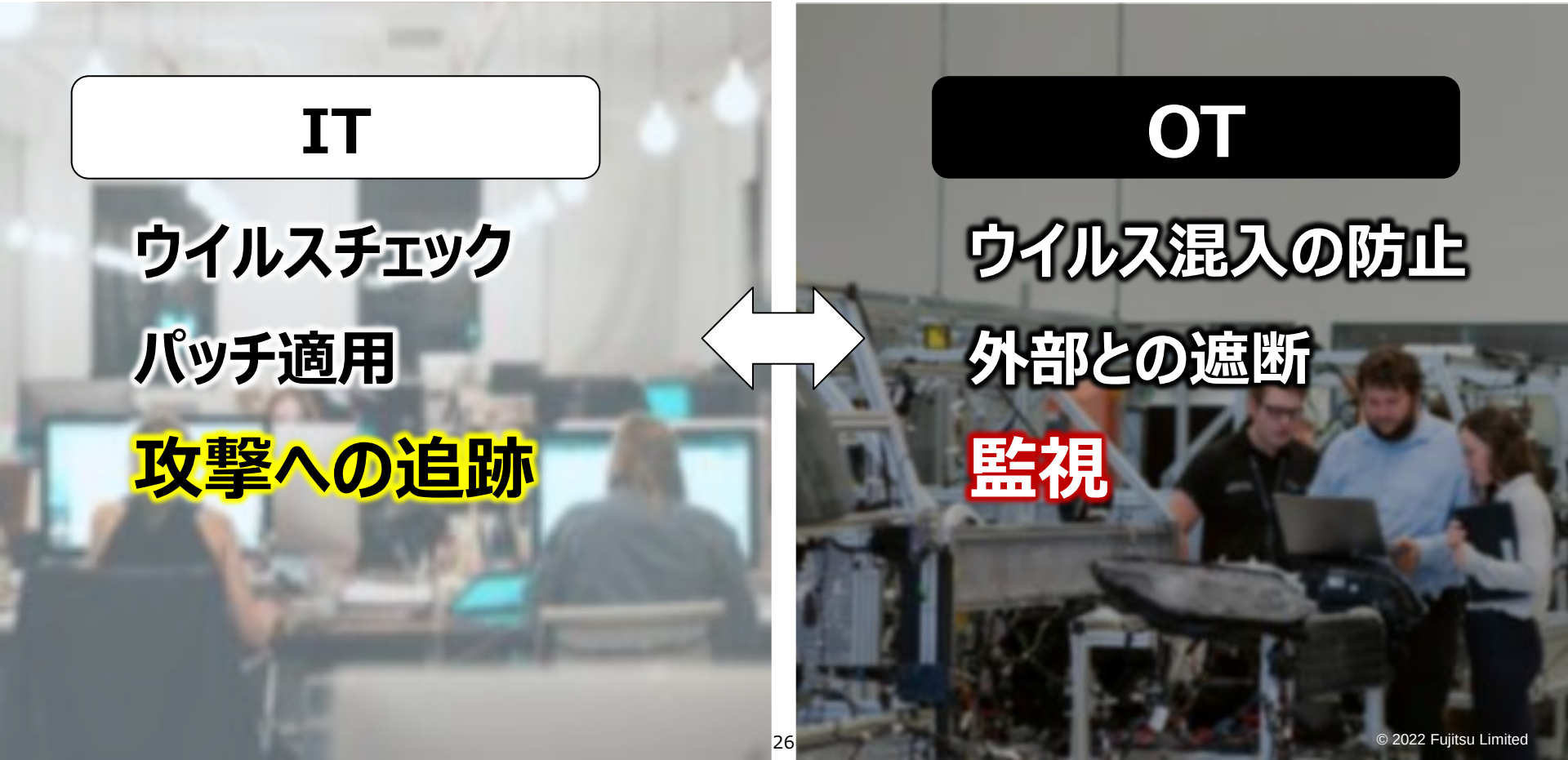
OT

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

FUJITSU



IT

ウイルスチェック

パッチ適用

攻撃への追跡

OT

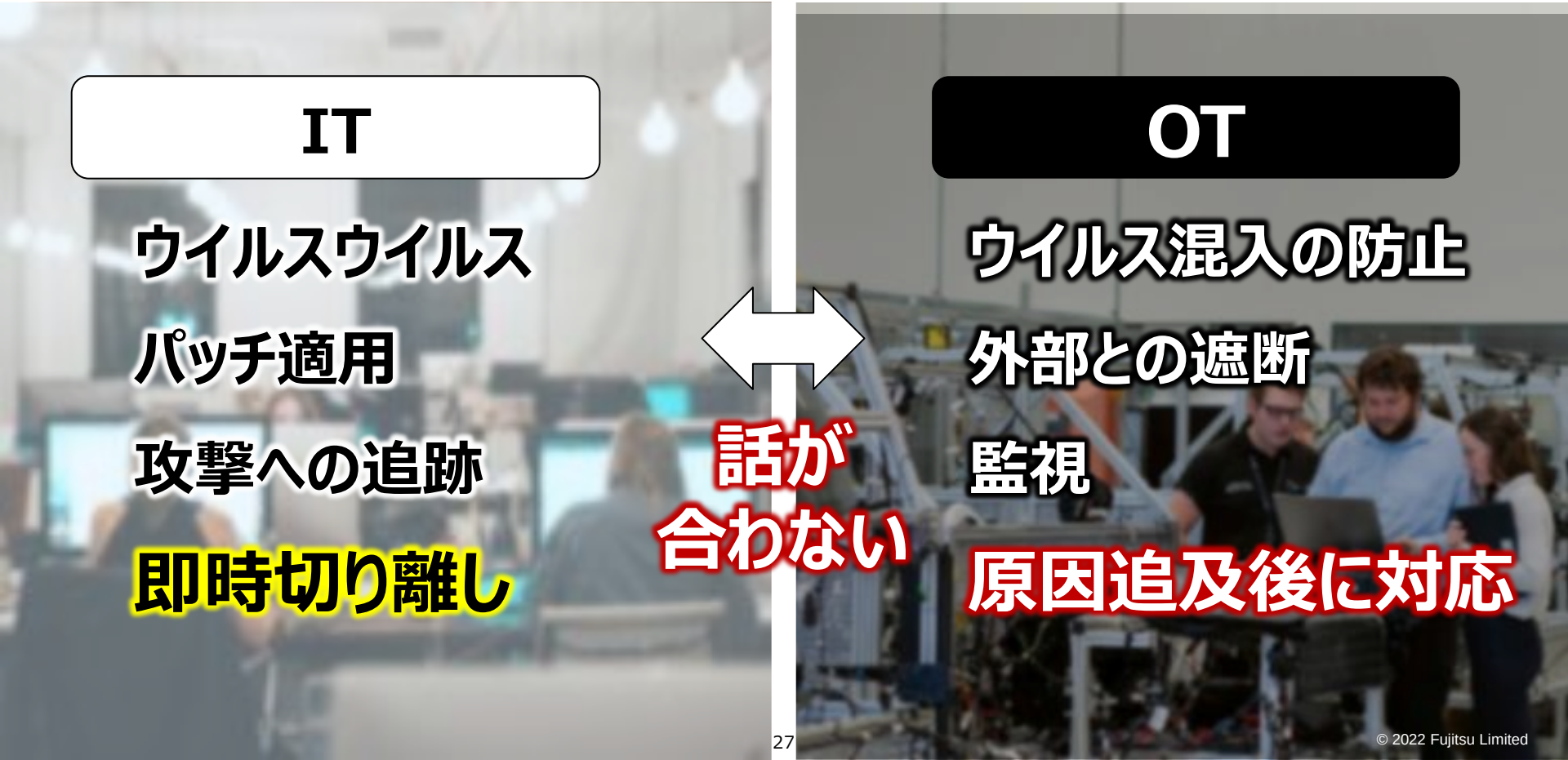
ウイルス混入の防止

外部との遮断

監視

ITセキュリティとOTセキュリティ

FUJITSU



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

話が
合わない

OT

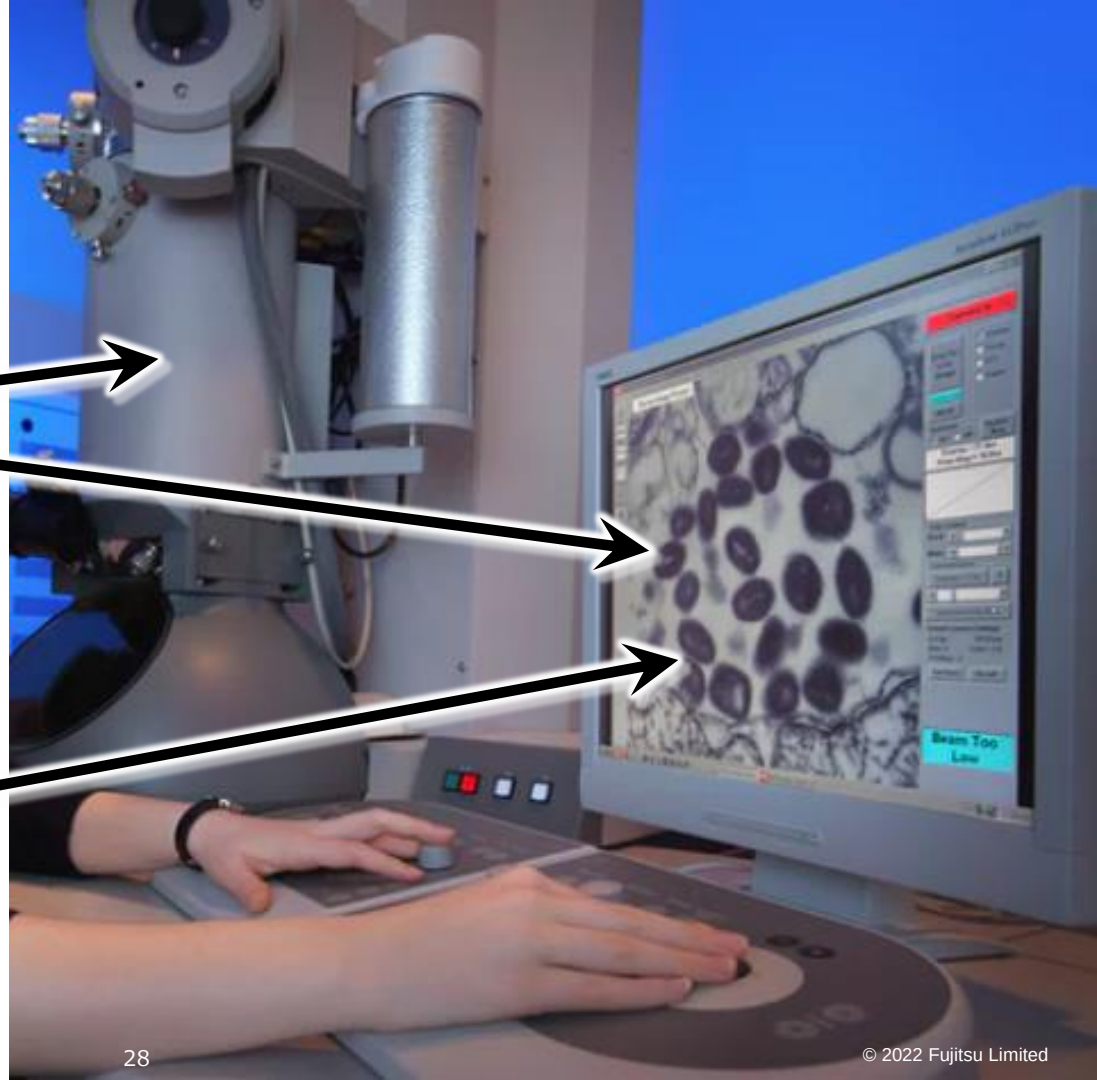
ウイルス混入の防止

外部との遮断

監視

原因追及後に対応

電子顕微鏡における例



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。

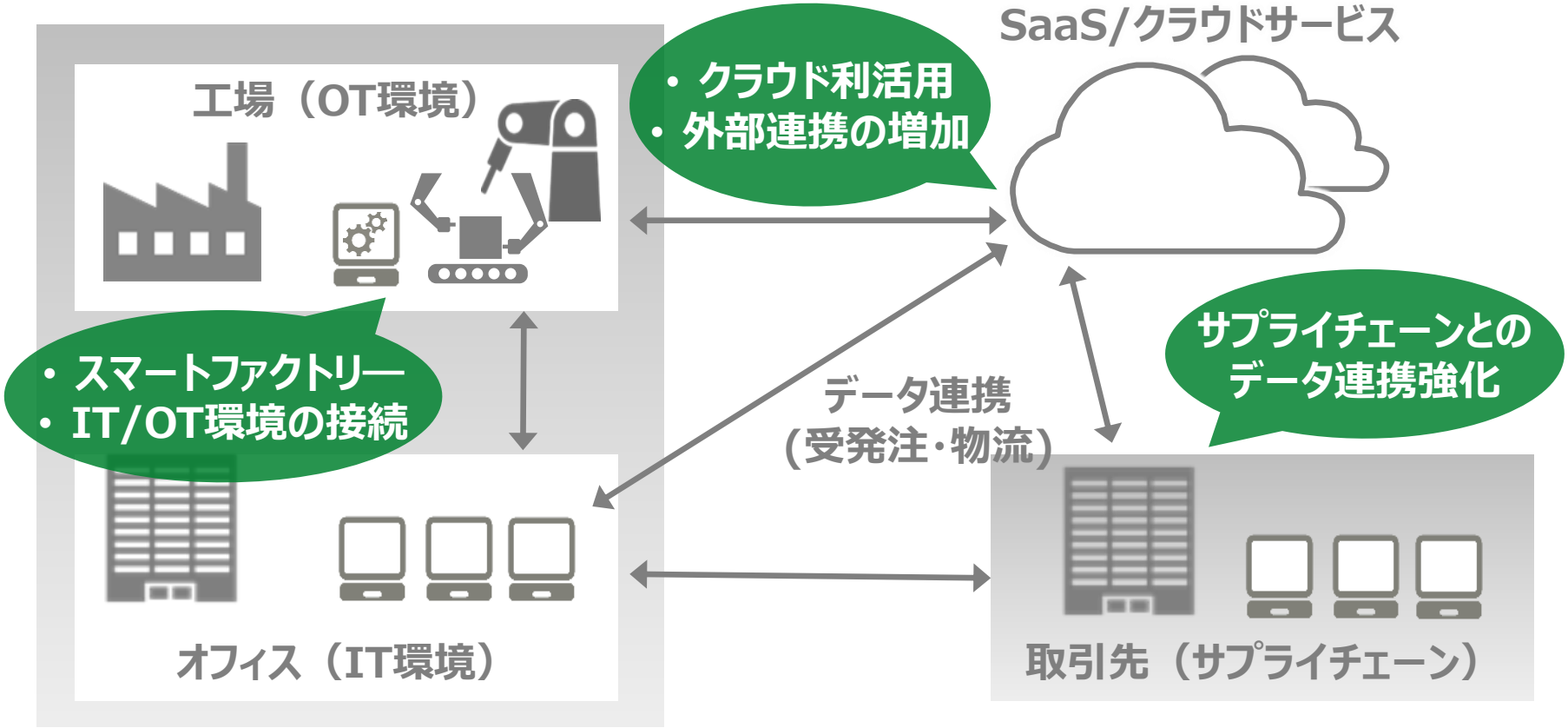
IT/OT環境において、**どのように防御できるのか**、次の章から、それぞれお伝えします。

1. ITとOTを取り巻くサイバー状況

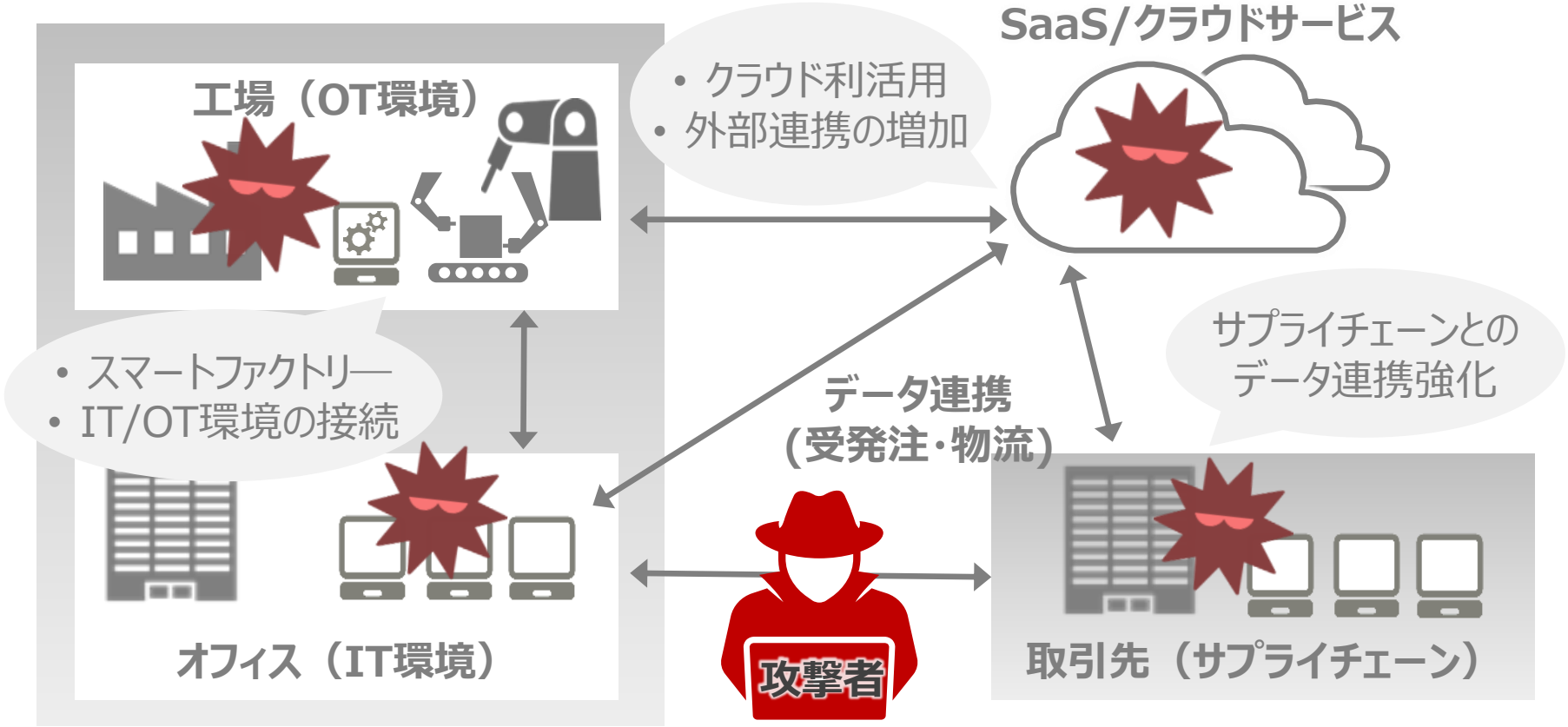
2. 製造業におけるセキュリティ対策

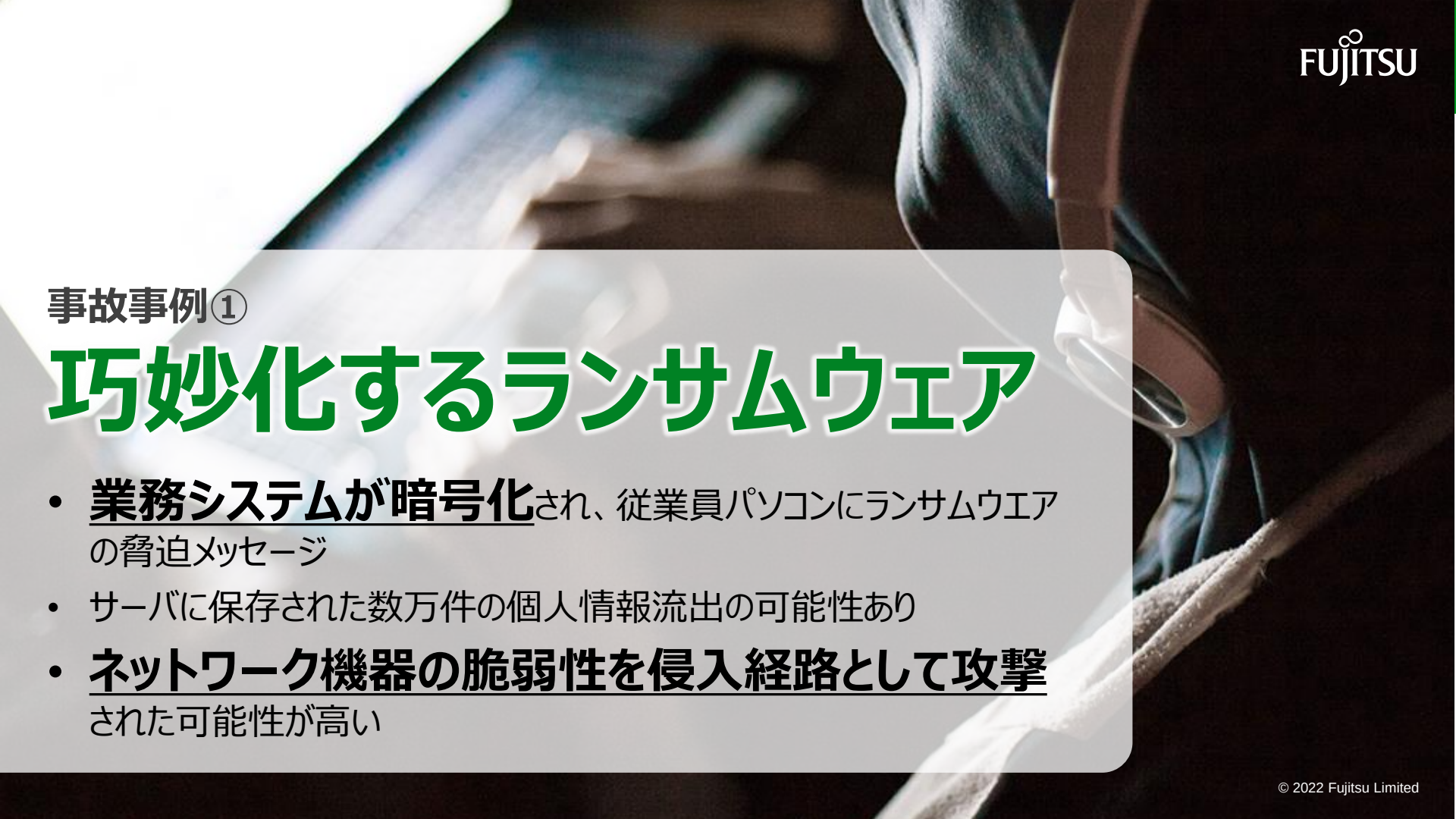
3. OTセキュリティ対策のベースとなるソリューション

製造業を取り巻く環境



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エ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

FUJITSU

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

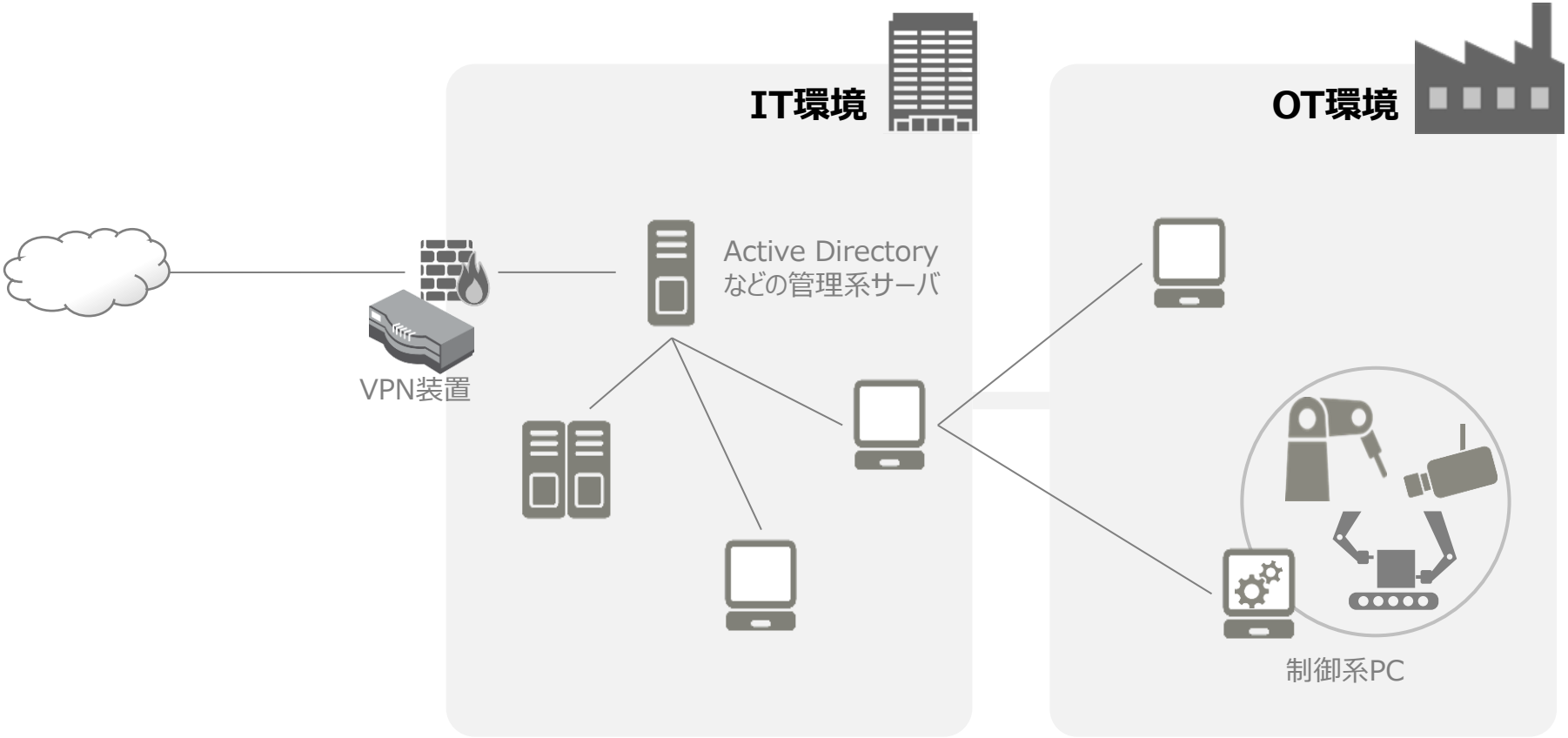
工場が攻撃対象に！

- **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**

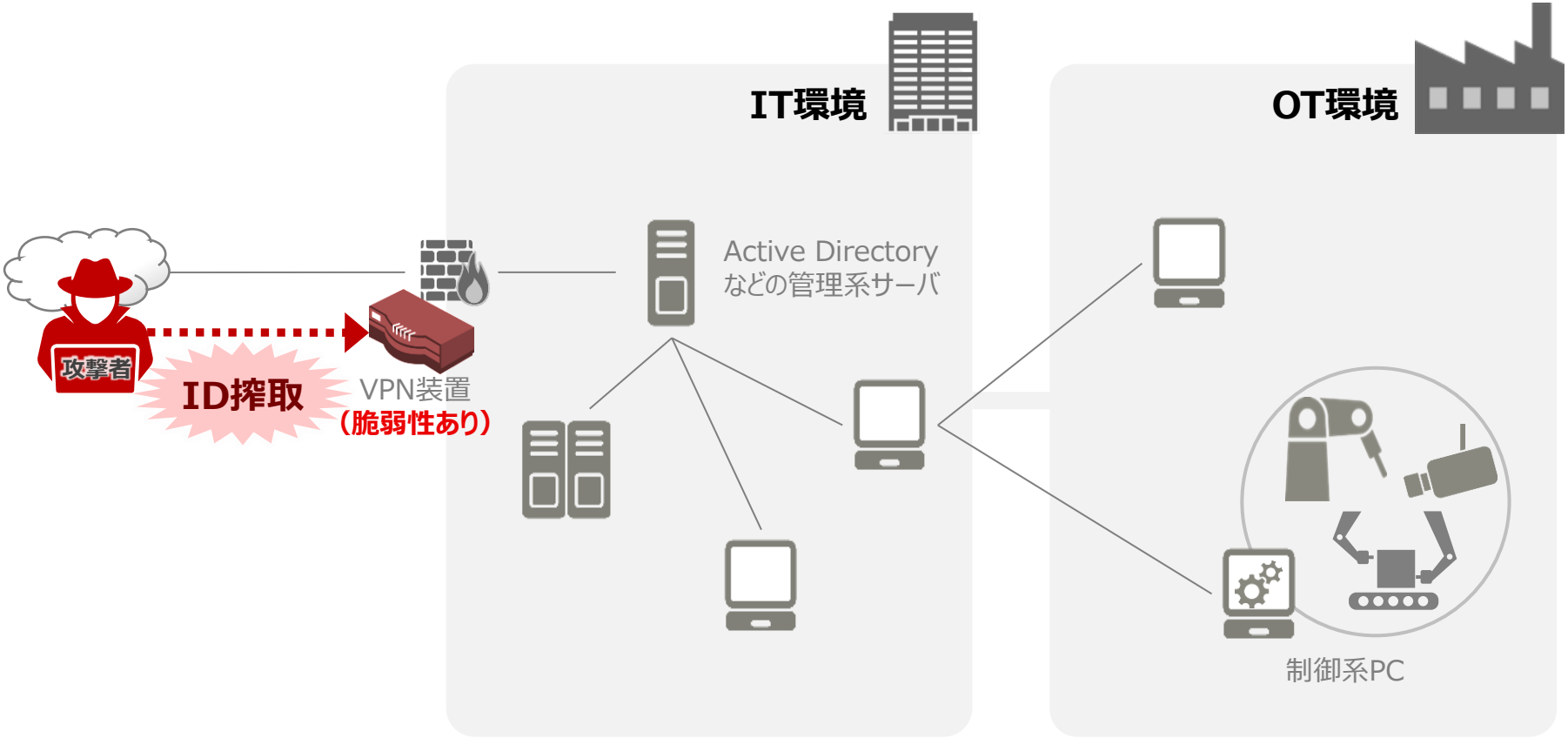
FUJITSU

背景を確認してみましょう！
～ 標的型攻撃 ～

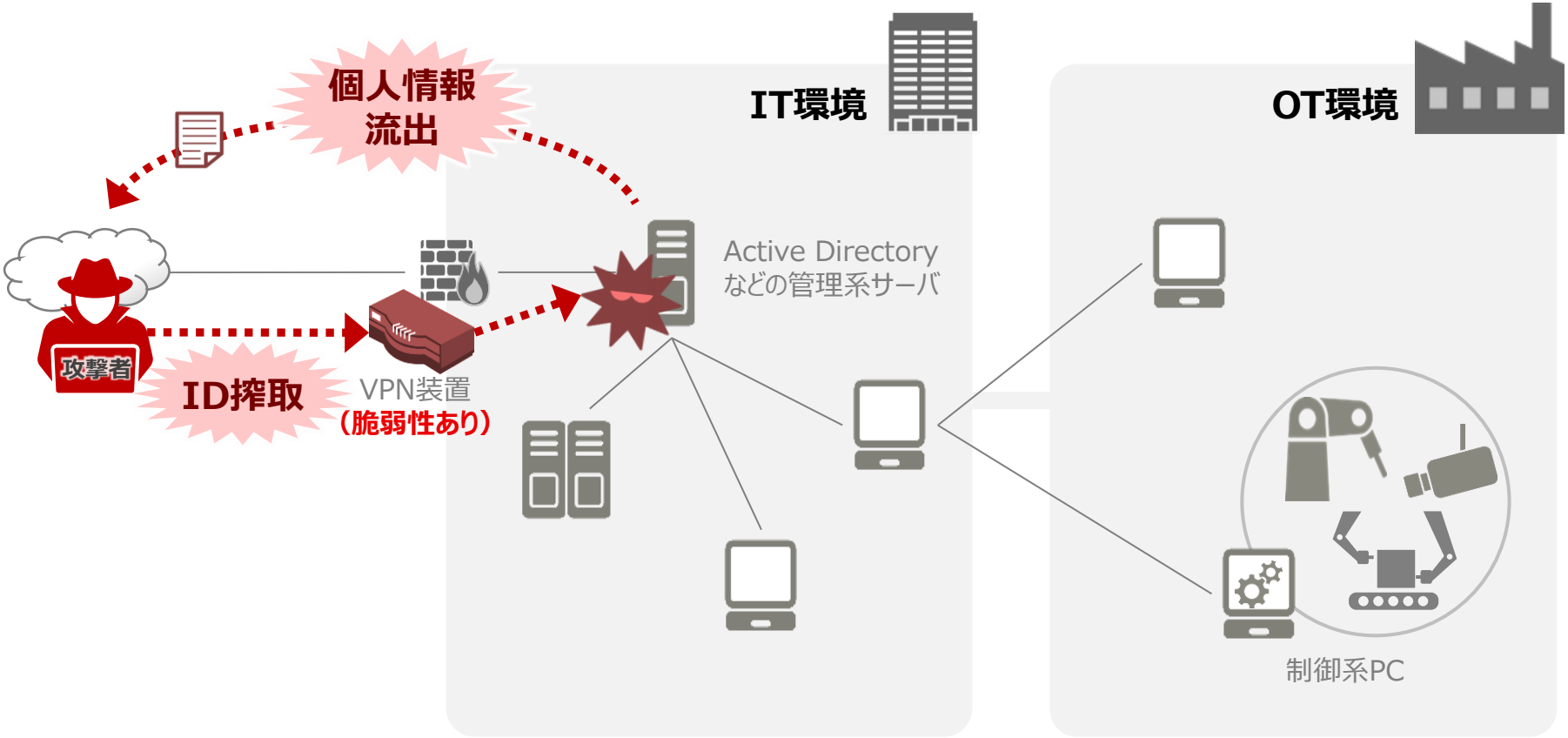
事故の流れ (1/5)



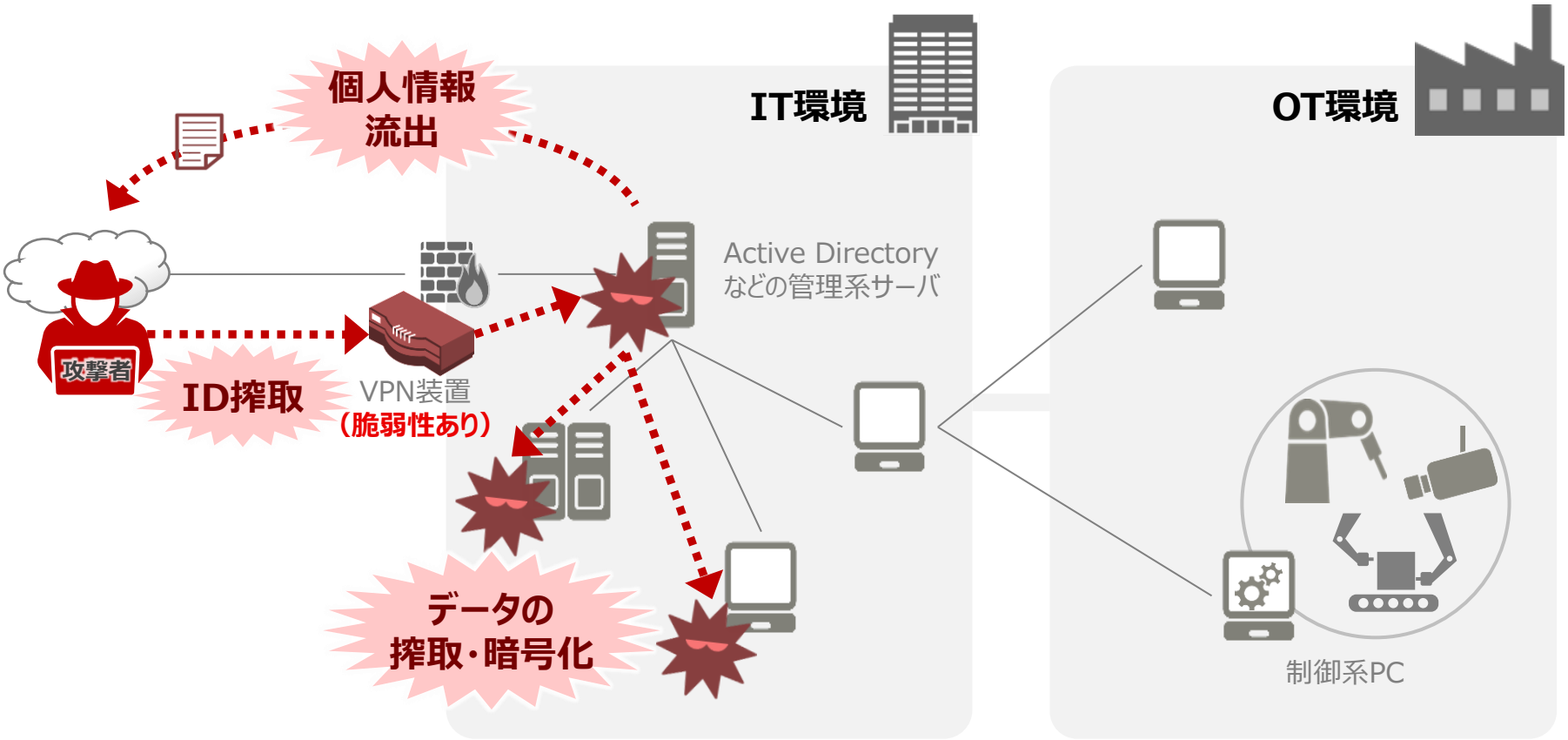
事故の流れ (2/5)



事故の流れ (3/5)

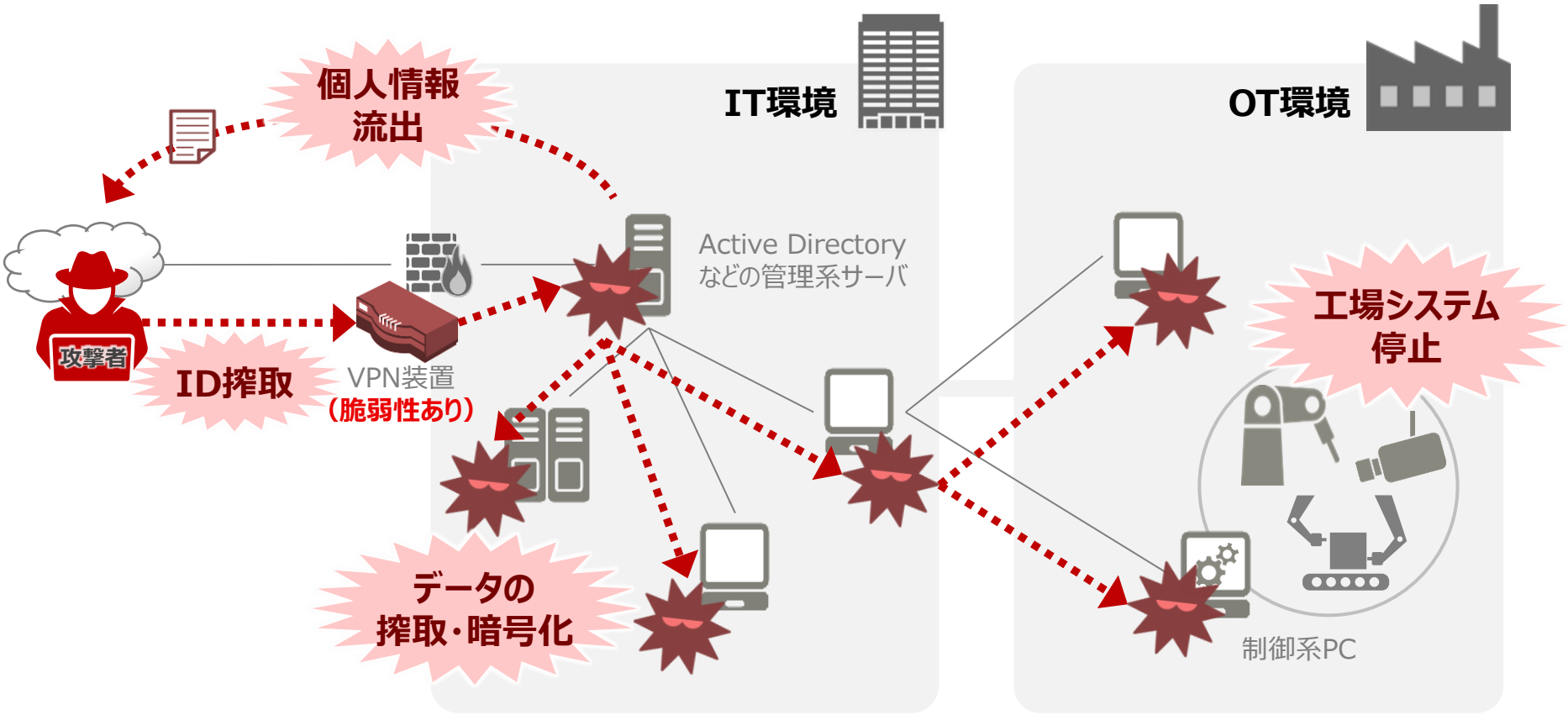


事故の流れ (4/5)

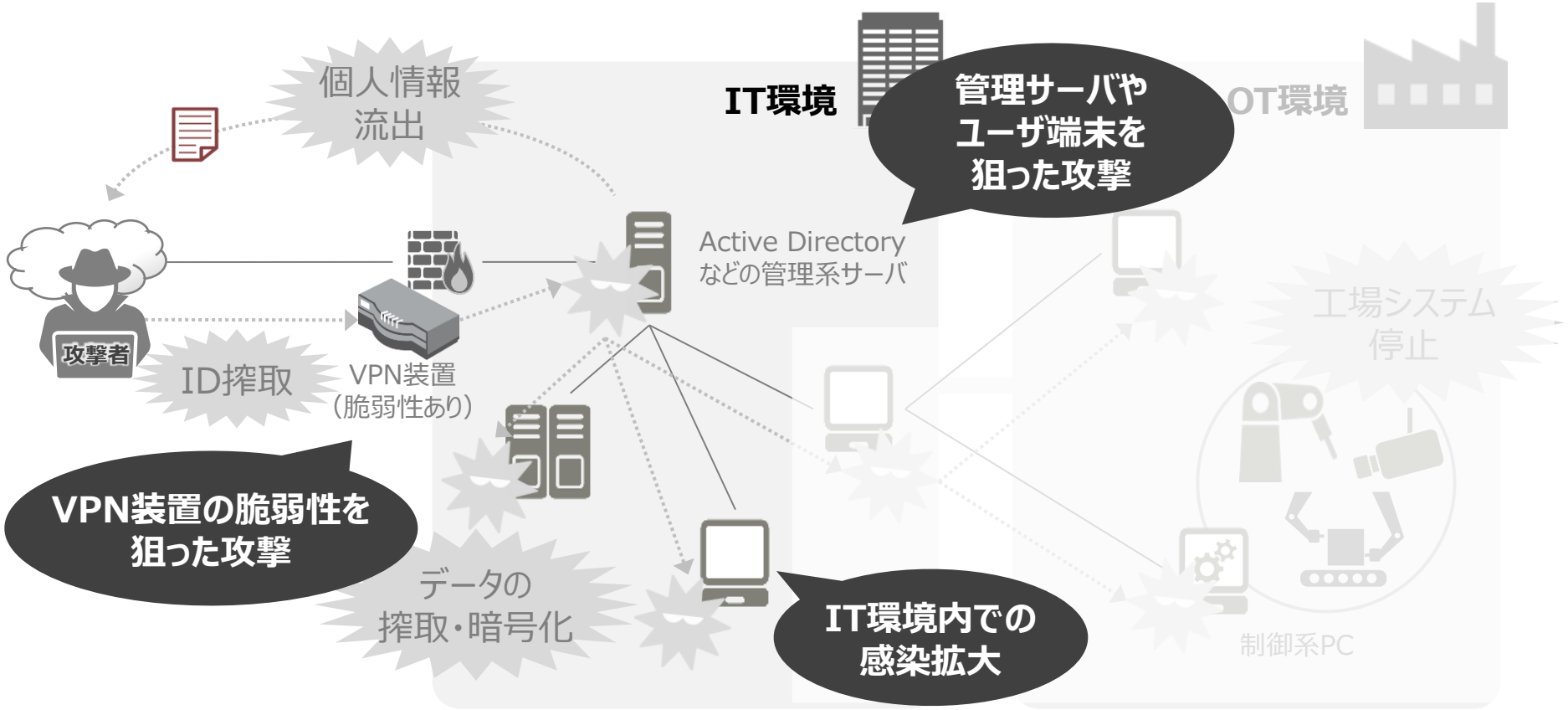


事故の流れ (5/5)

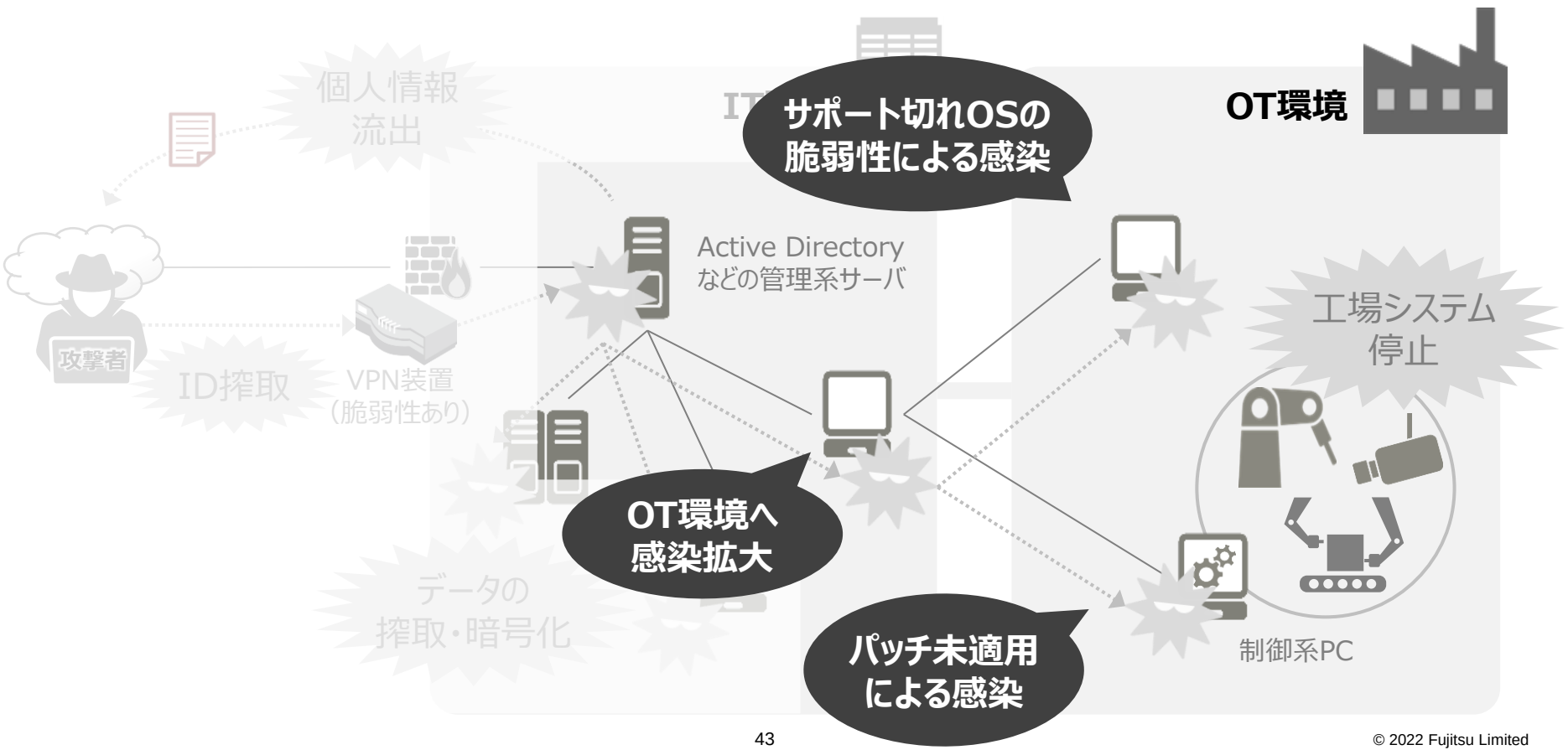
FUJITSU



セキュリティ課題はどこに？



セキュリティ課題はどこに？



FUJITSU

背景を確認してみましょう！
～ サプライチェーン攻撃 ～

アンコントローラブルな取引先

FUJITSU

自社

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

サプライヤ・取引先等、
全関係者を
把握しきれていない

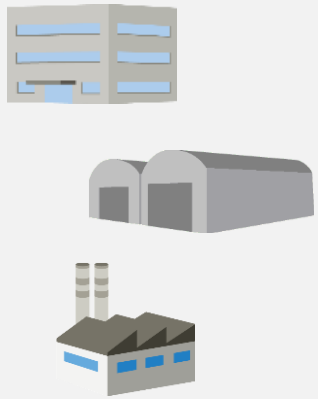
取引関係だから、
強くものが言えない

取引先の
セキュリティ状況を
勝手に調査できない

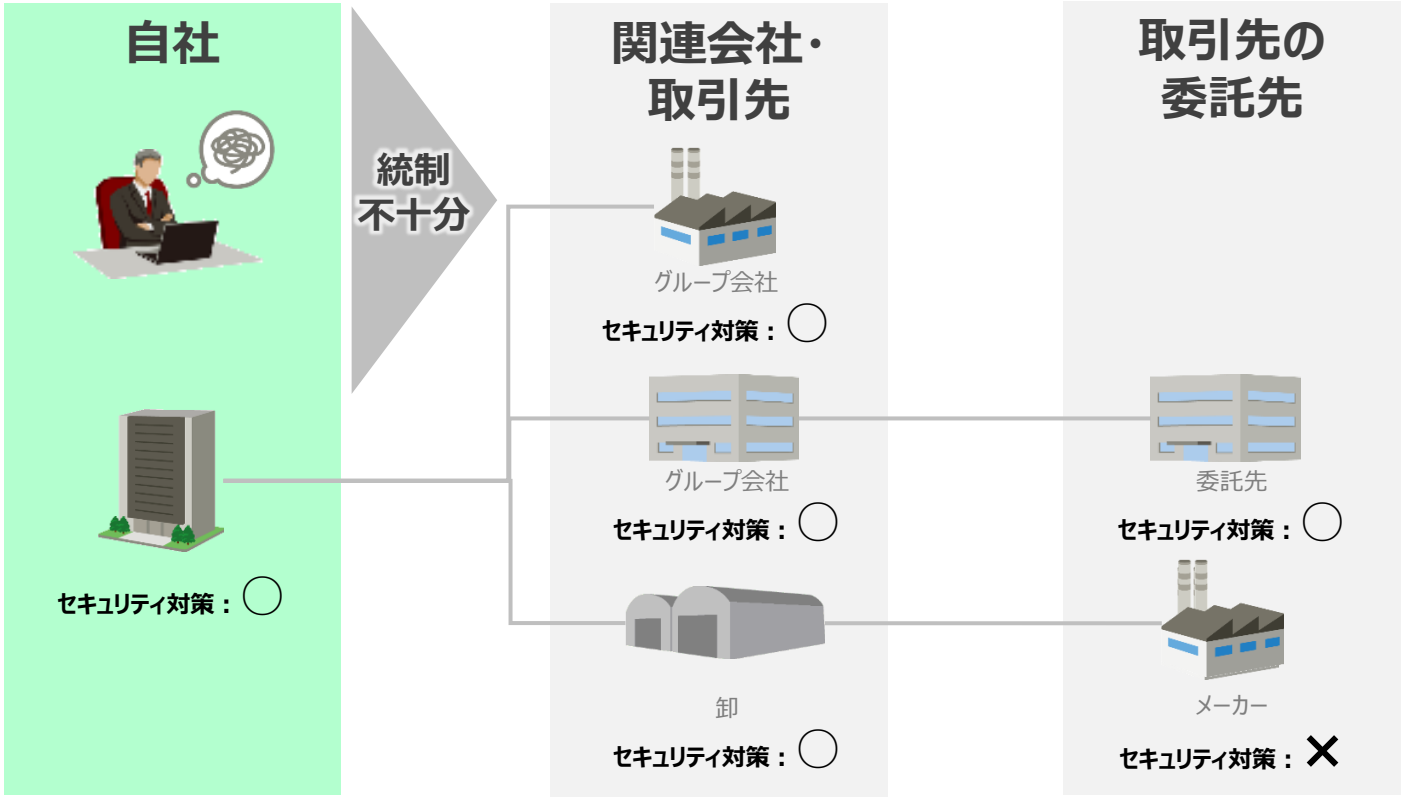
取引先が多く、
管理しきれない。
人海戦術で
対応せざるを得ない

統制
不十分

取引先

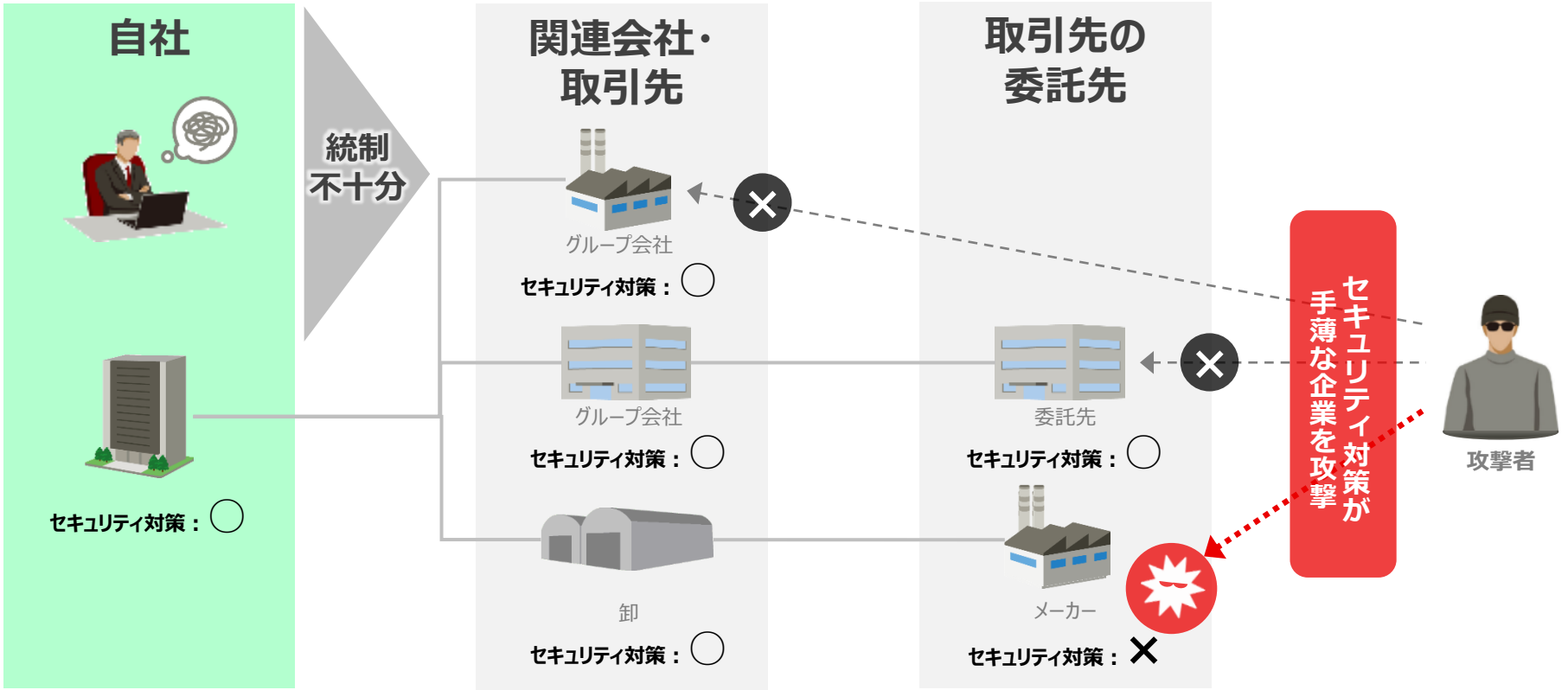


事故の流れ (1/3)

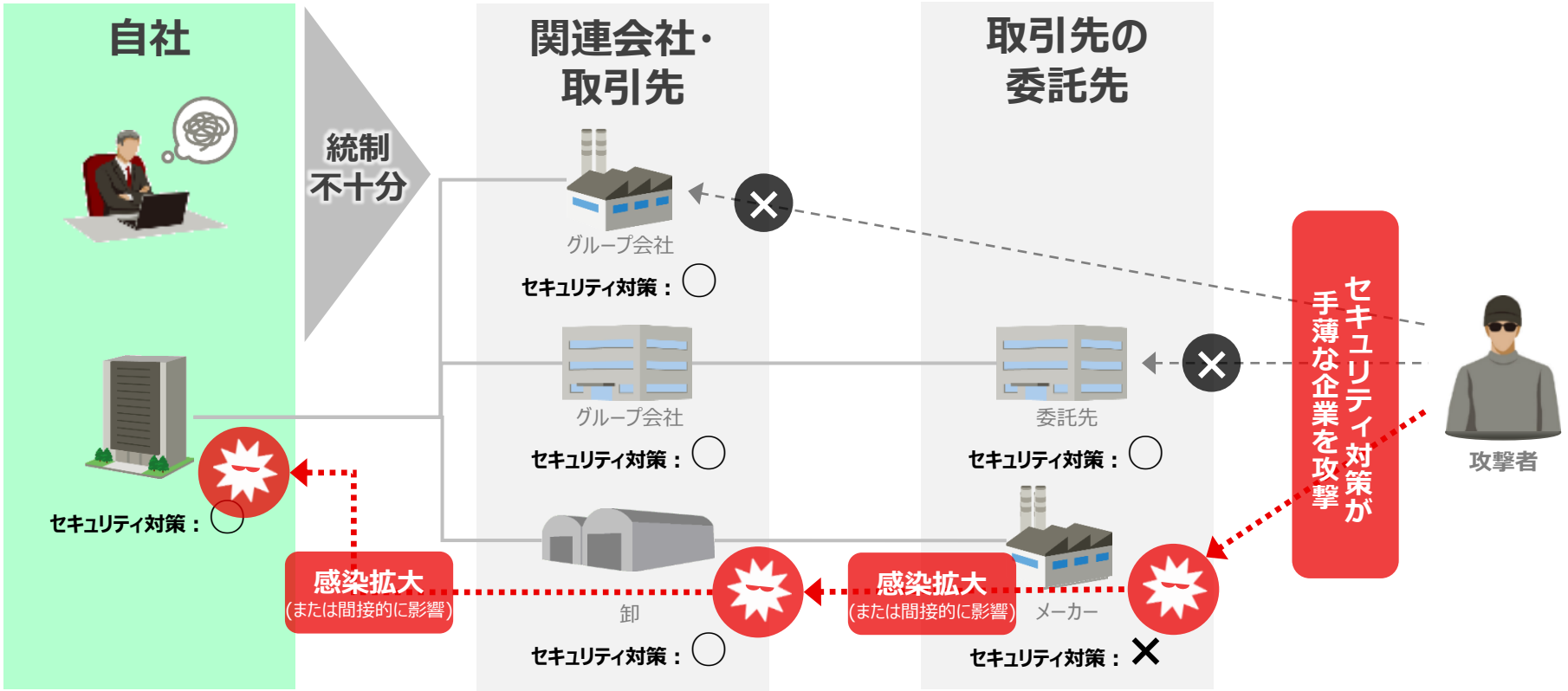


事故の流れ (2/3)

FUJITSU



事故の流れ (3/3)



対策をどう見直すべきか？

FUJITSU

自社

日々、スコアを再計算し
常に最新スコアを把握

取引先の変更に応じて
即座・客観的に評価実施

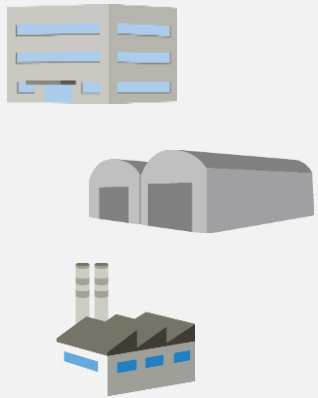
公平で
定量的に算出できる
調査手法

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

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

FUJITSU

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

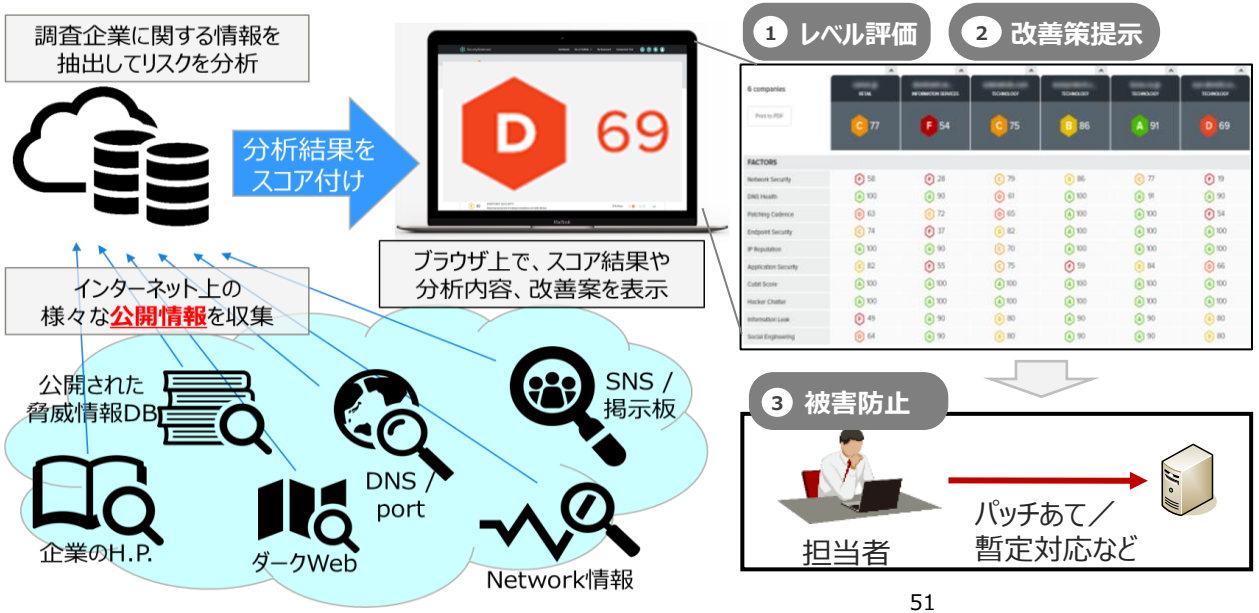
OTセキュリティ

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	ポイント②	ポイント③
セキュリティ対策状況 を客観的に**評価**	**弱点の洗い出し**により 改善策を検討	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

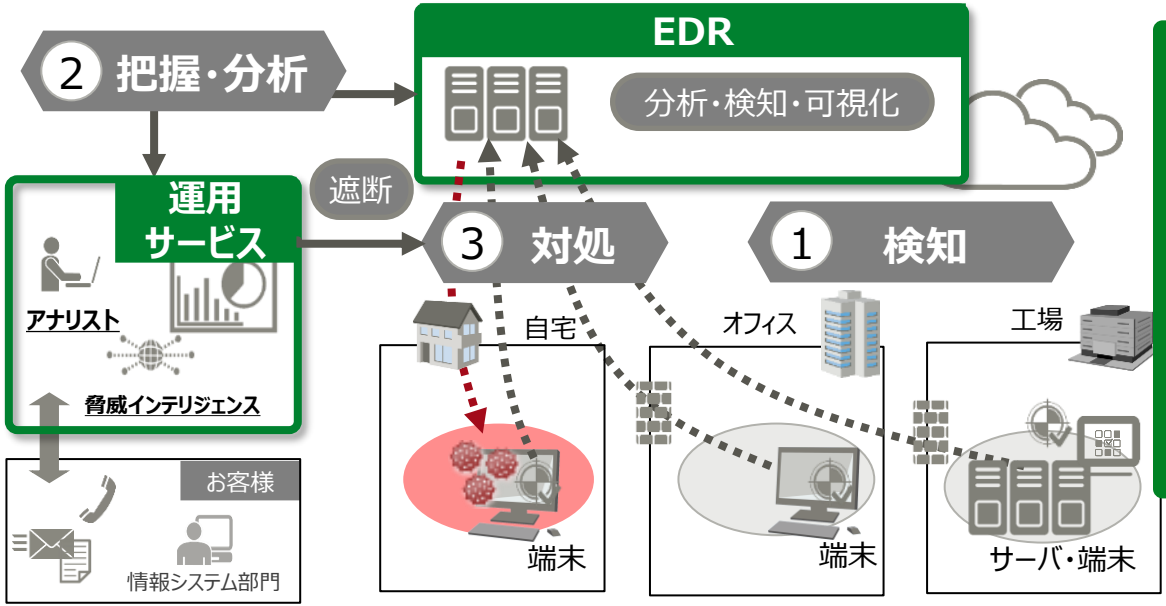
- SecurityScorecard
- 脆弱性診断・管理サービス

エンドポイントセキュリティ(EDR)

FUJITSU

エンドポイント上での疑わしい挙動を分析、迅速な検知・対処を実現

ポイント①	ポイント②	ポイント③
攻撃者による 端末の感染活動を**検知**	攻撃の全体像を **把握・分析**	運用サービスによる **迅速かつ適切な対処**



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)**

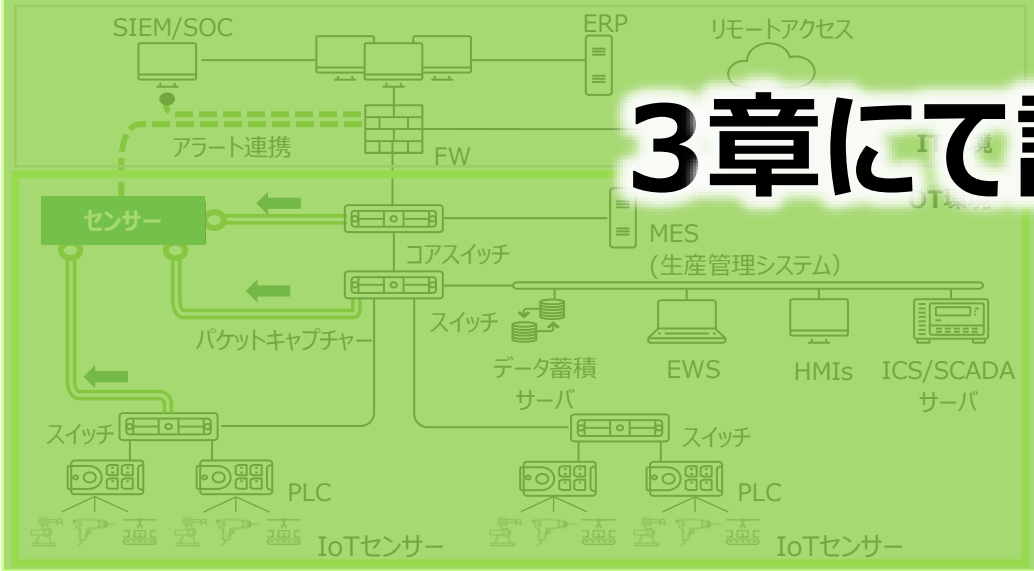
※1【サービス名称】FENICS CloudProtect エンドポイントセキュリティ powered by Apex One SaaS + XDRオプションサービス
※2【サービス名称】FENICS CloudProtect XDR for Endpoint powered by Cortex XDR from Palo Alto Networks

OTセキュリティ

FUJITSU

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	ポイント②	ポイント③
OTネットワーク上の機器情報の収集とリスク把握	通常の通信を自動学習し、異常通信を自動検知	アクセス元/先の情報を監視し、不正アクセスを検知

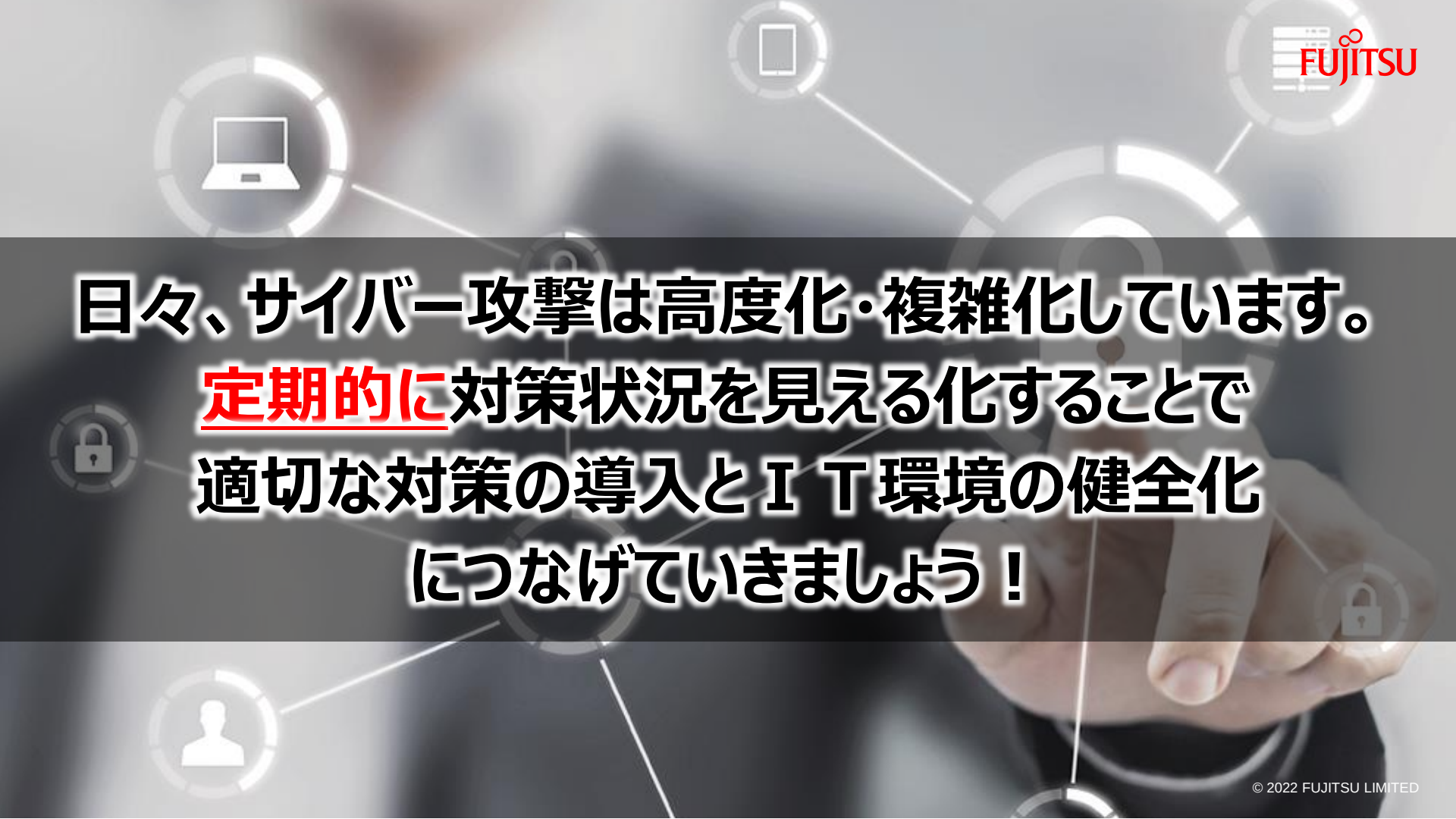


3章にて説明

ネットワーク状況の自動可視化により、運用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

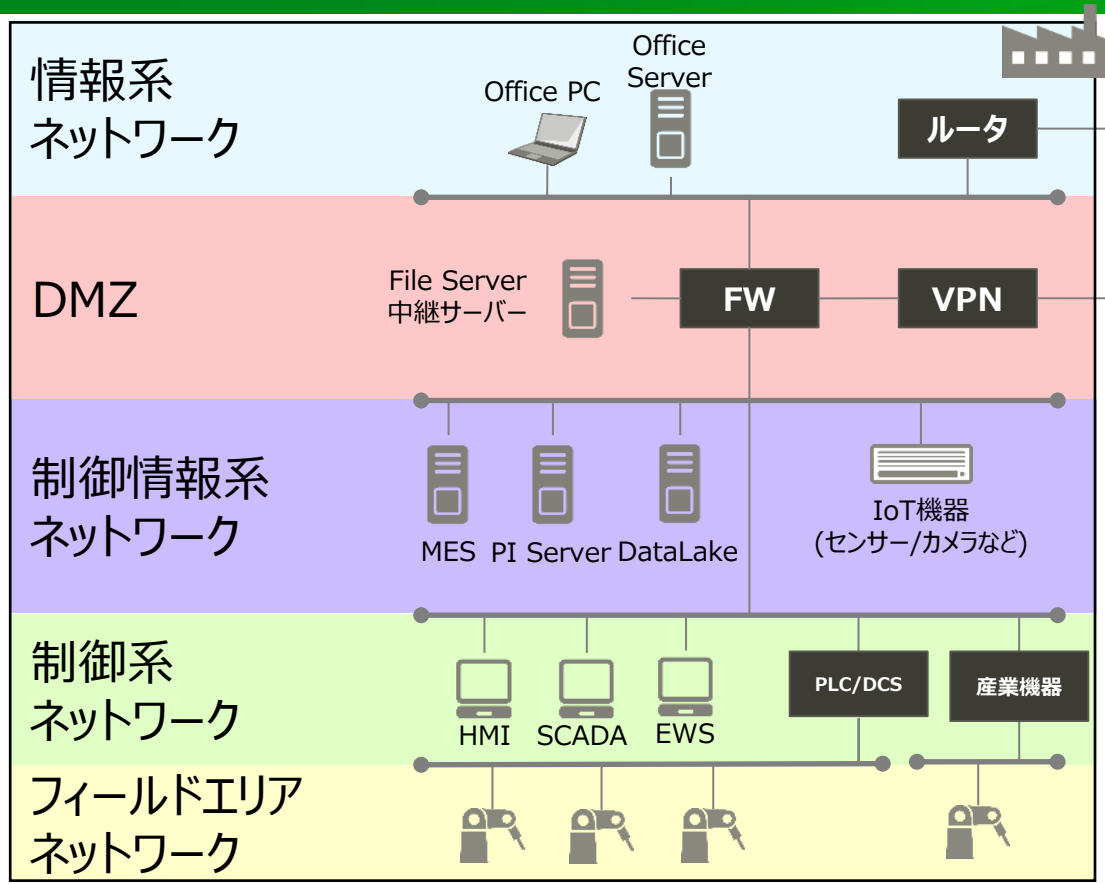


1. ITとOTを取り巻くサイバー状況

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

FUJITSU

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

だからこそ、生産現場もしっかり守る

FUJITSU

- 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**

OTネットワークセキュリティ可視化サービス

FUJITSU

- 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

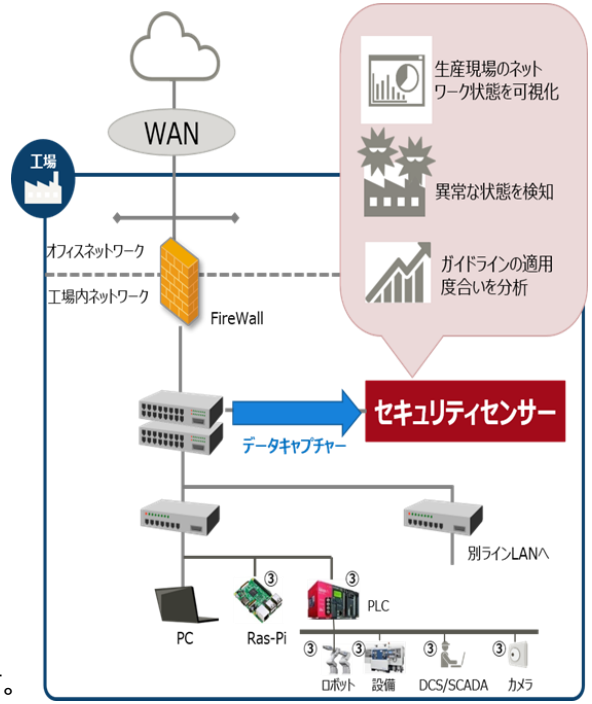
生産業務の継続性・健全性を向上

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メンドにより、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



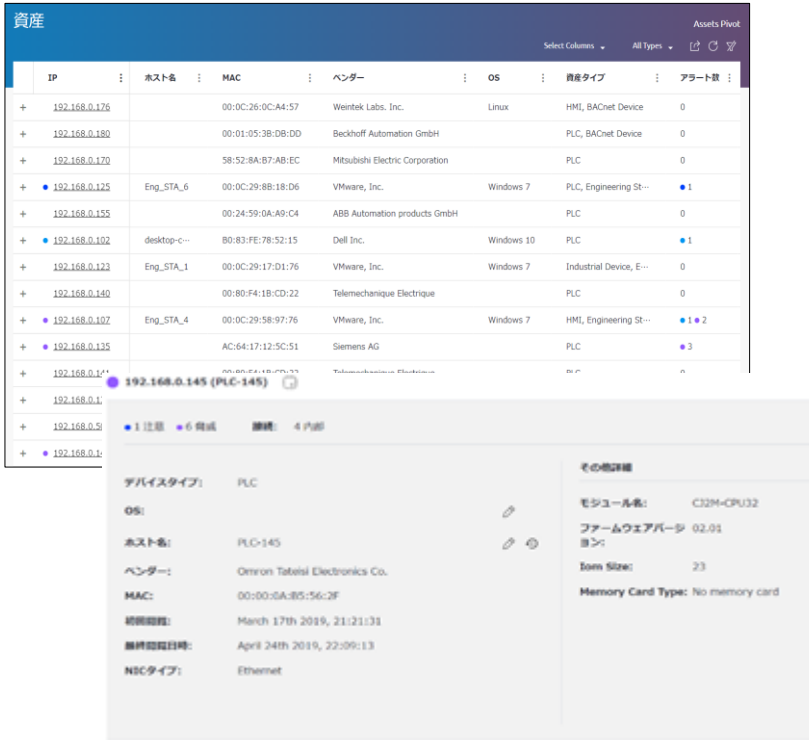
※セキュリティセンサーとしてSCADAfence社が提供する**SCADAfenceプラットフォーム**を利用しています。

※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。

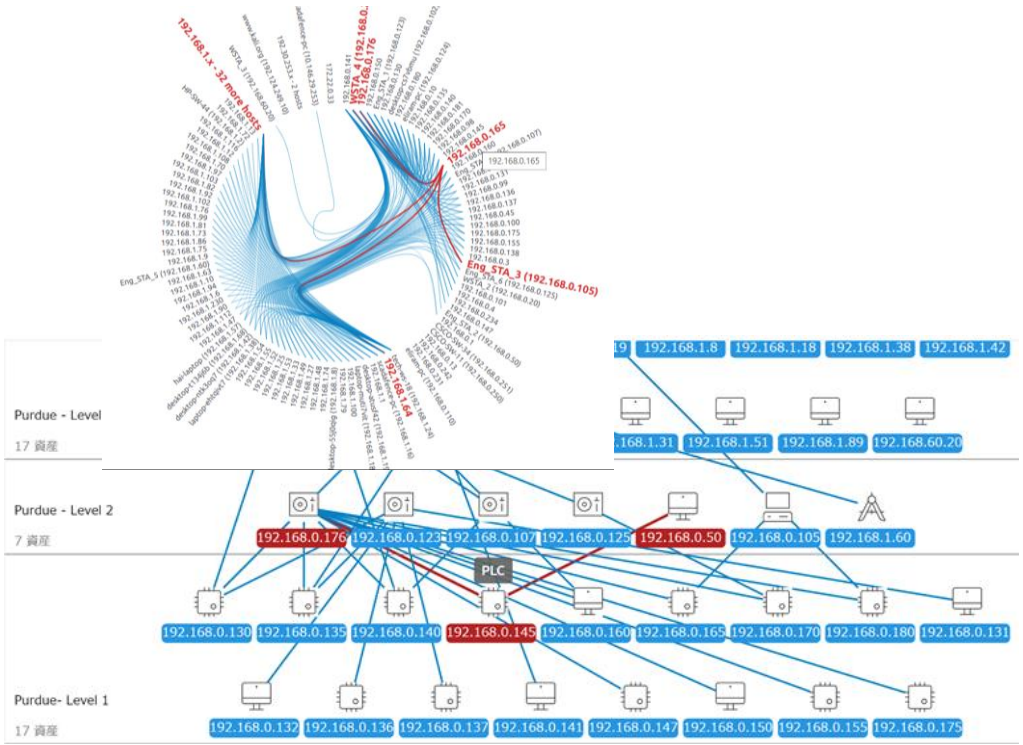
“いつもの状態”を知る

FUJITSU

何がつながっているか



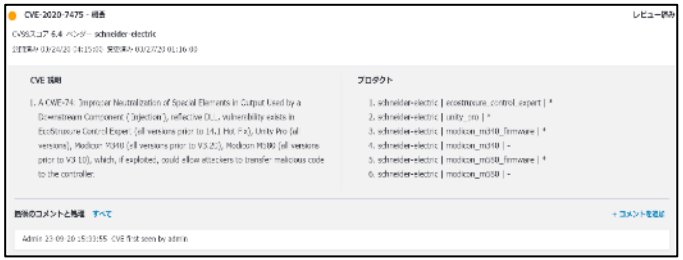
どことつながっているか



“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



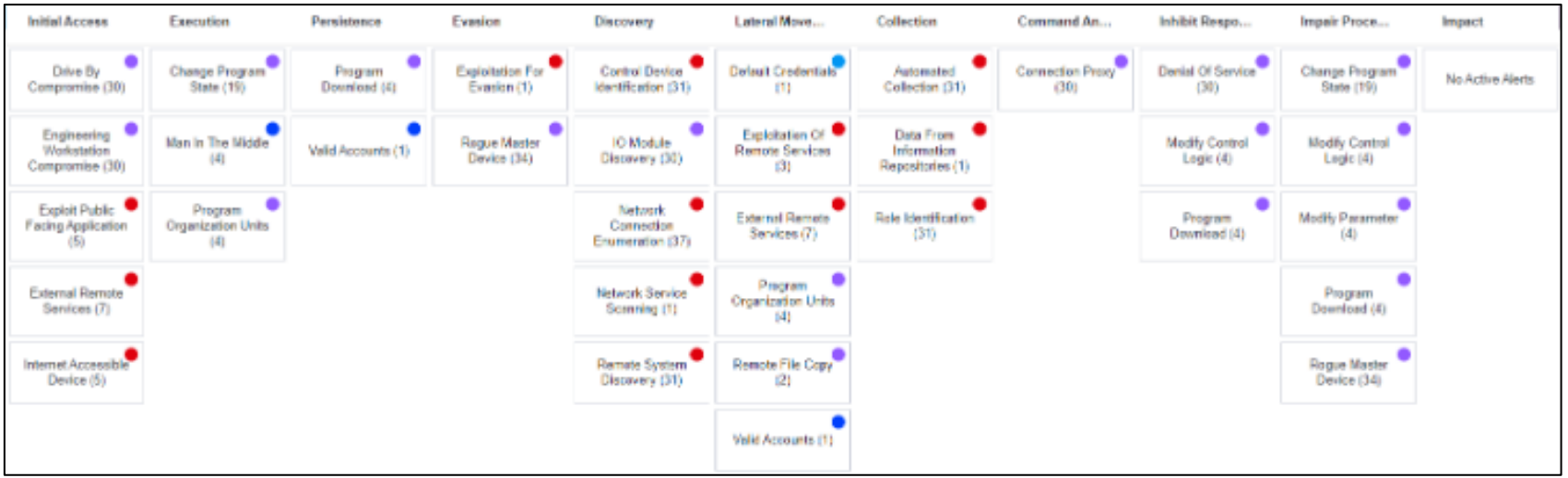
各CVEの説明や該当するOT機器ベンダー情報を把握

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

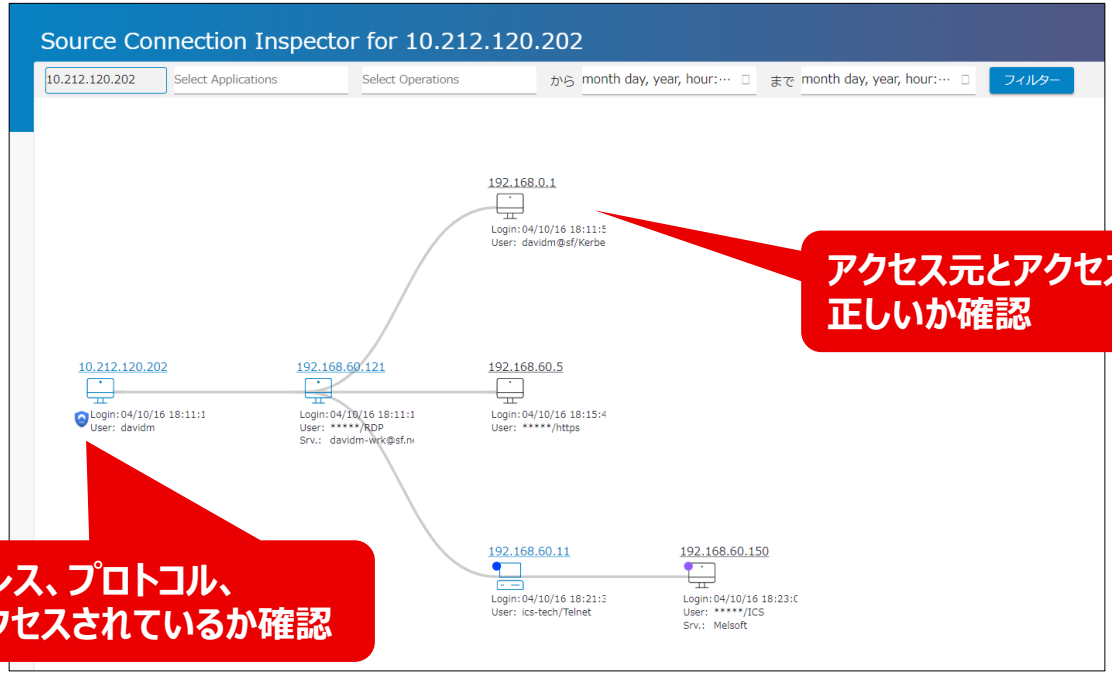
生産現場への影響度が高い



※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)」

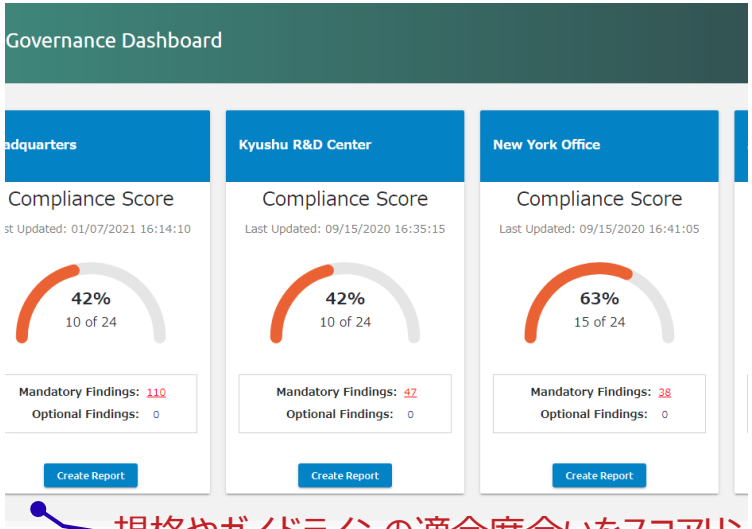
“異常”に気付く　③不正アクセスに気付く

- 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



おまけ：現在地を知る

- 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

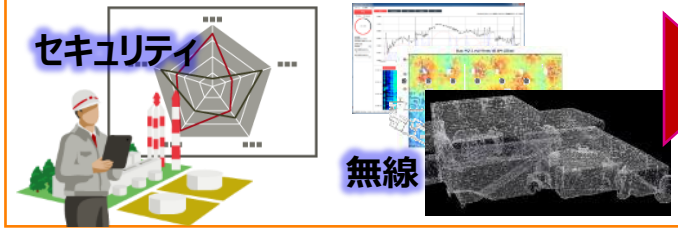
レポート出力、規格やガイドラインが持つ各項目に対して設備ごとの遵守状況を詳細に可視化.

(ご参考)富士通がお手伝いできること

FUJITSU

- 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

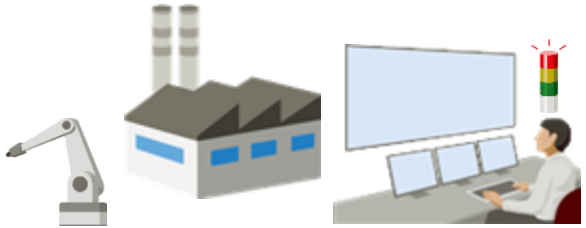
ベースの状態に応じて

③工場ネットワークグランドデザイン

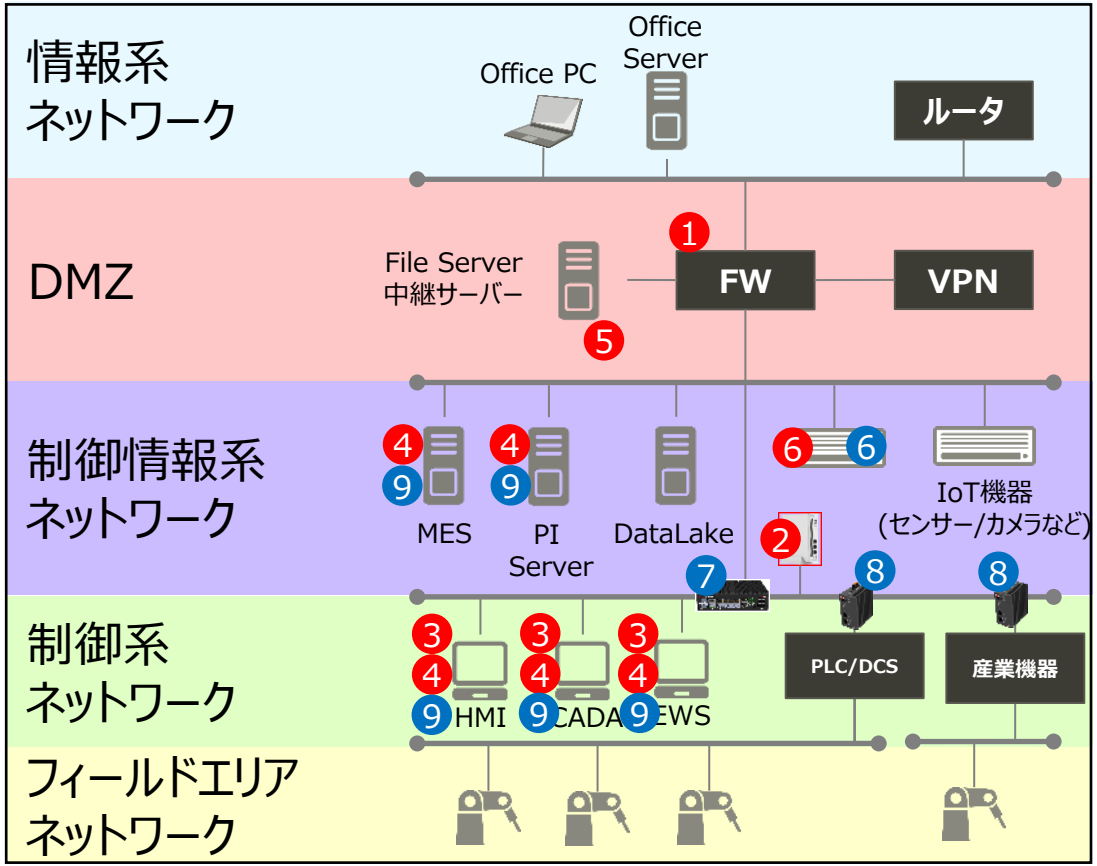
④ 工場ネットワークインテグレーション

⑤ 脆弱箇所の対処

⑥ ネットワーク運用支援サービス



(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(Stealthwatch)**
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

FUJITSU

【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