製造DXの実現と製造現場でのセキュリティ

日本マイクロソフト株式会社
インダストリアル＆製造事業本部
安並裕

Agenda

1. OTセキュリティーを強化すべき背景
2. ITセキュリティーとOTセキュリティーの違い
3. 先進企業の取組姿勢
4. Why MS
5. 答えるべき問い

Agenda

1. OTセキュリティーを強化すべき背景
2. ITセキュリティーとOTセキュリティーの違い
3. 先進企業の取組姿勢
4. Why MS
5. 答えるべき問い

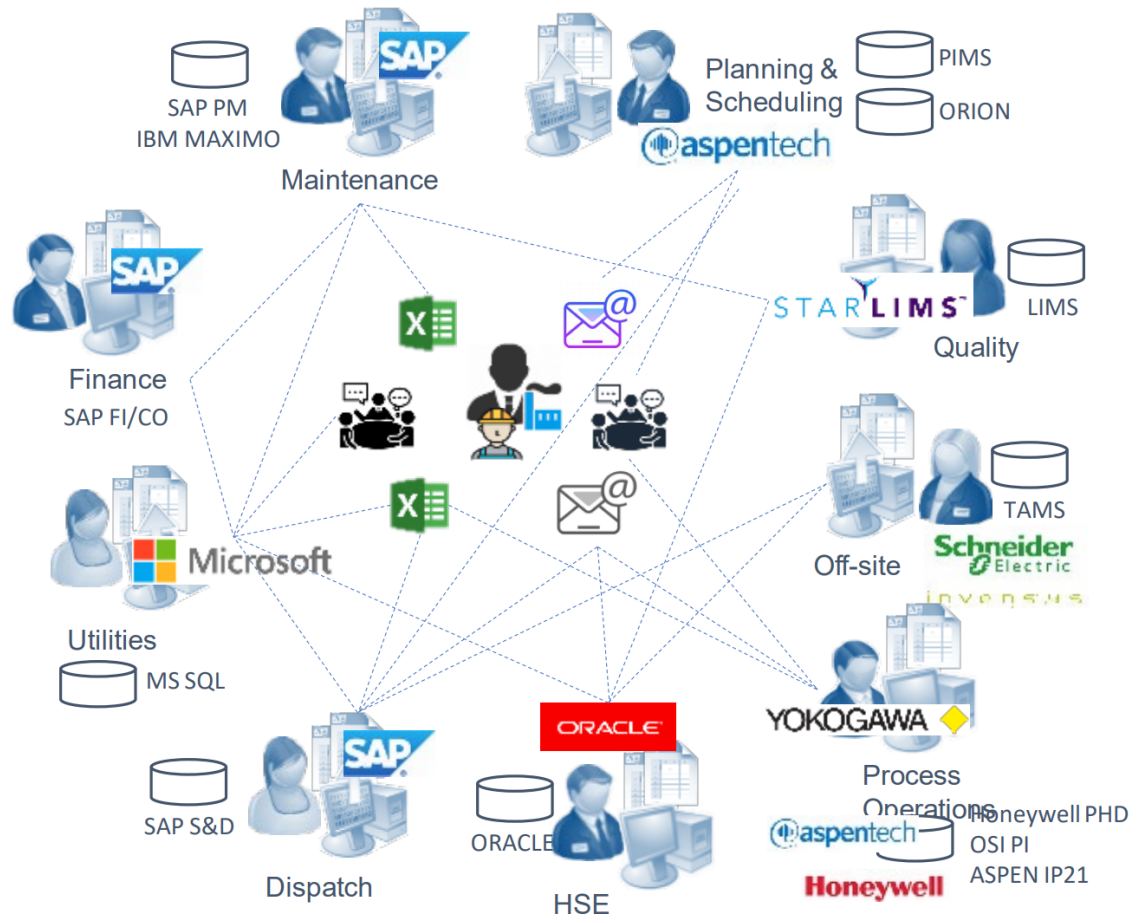
デジタルファクトリー化を妨げる要因　～　「様々な形で、バラバラに格納された情報」

dDriven 社資料より

The Problem Space & Opportunity

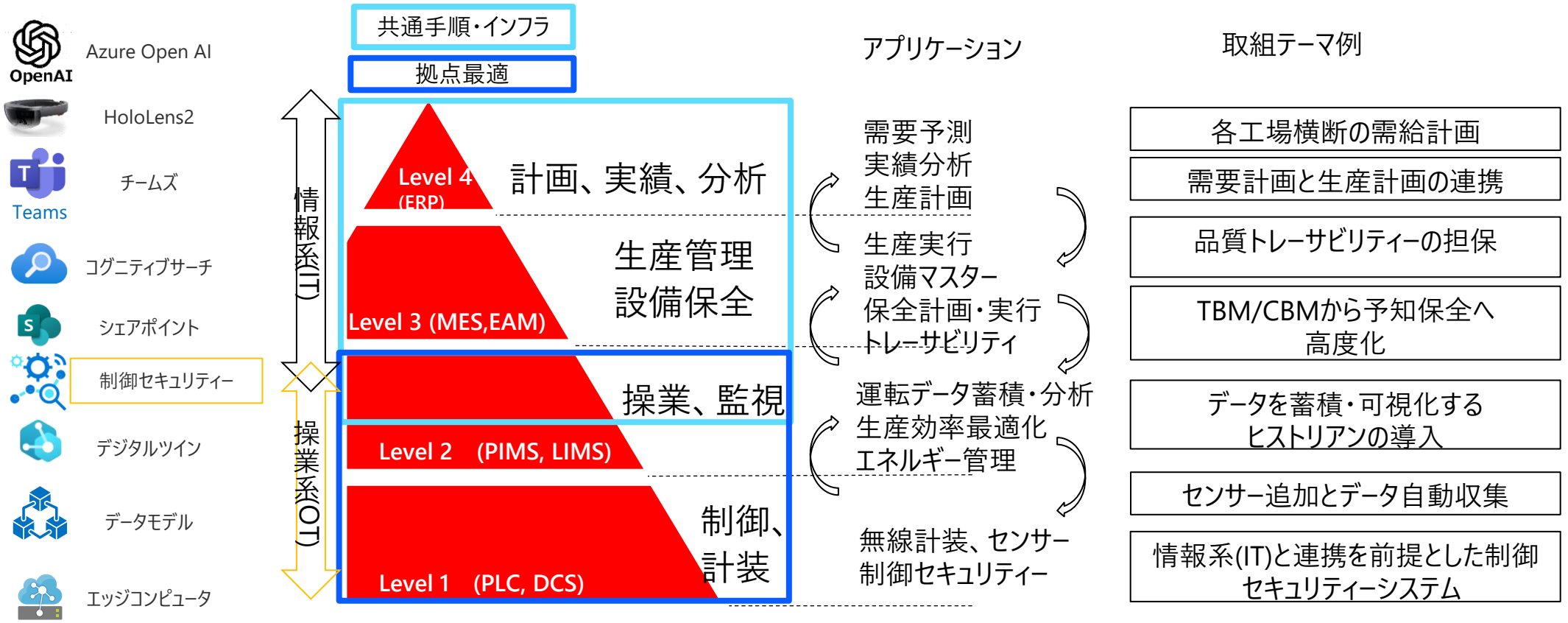
ぶつ切りの情報　＝＞　事後データに基づく操業

- 多くの種類の異なるシステムが散在
- 長年にわたるベンダーロックイン
- 部門をまたがる情報活用できず
- 必要な時間内に情報を入手できない
- 多くの死角が発生している



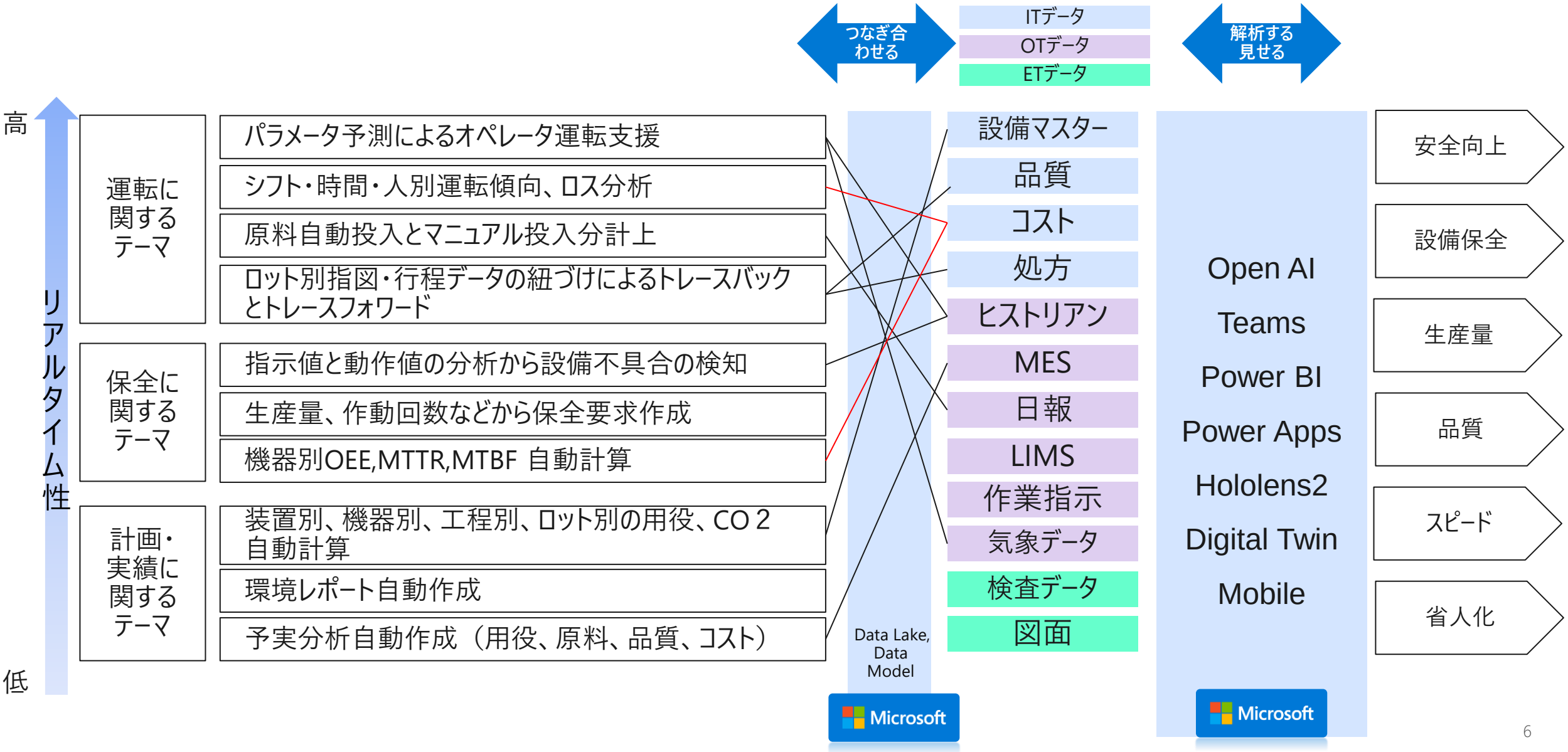
IT/OT 情報連携の構図＜タテの流れ＞

ISA95に準拠したL1～L4の情報連携を想定し、関連業務と各種データがシステム連携する仕組みづくりを検討する必要がある。



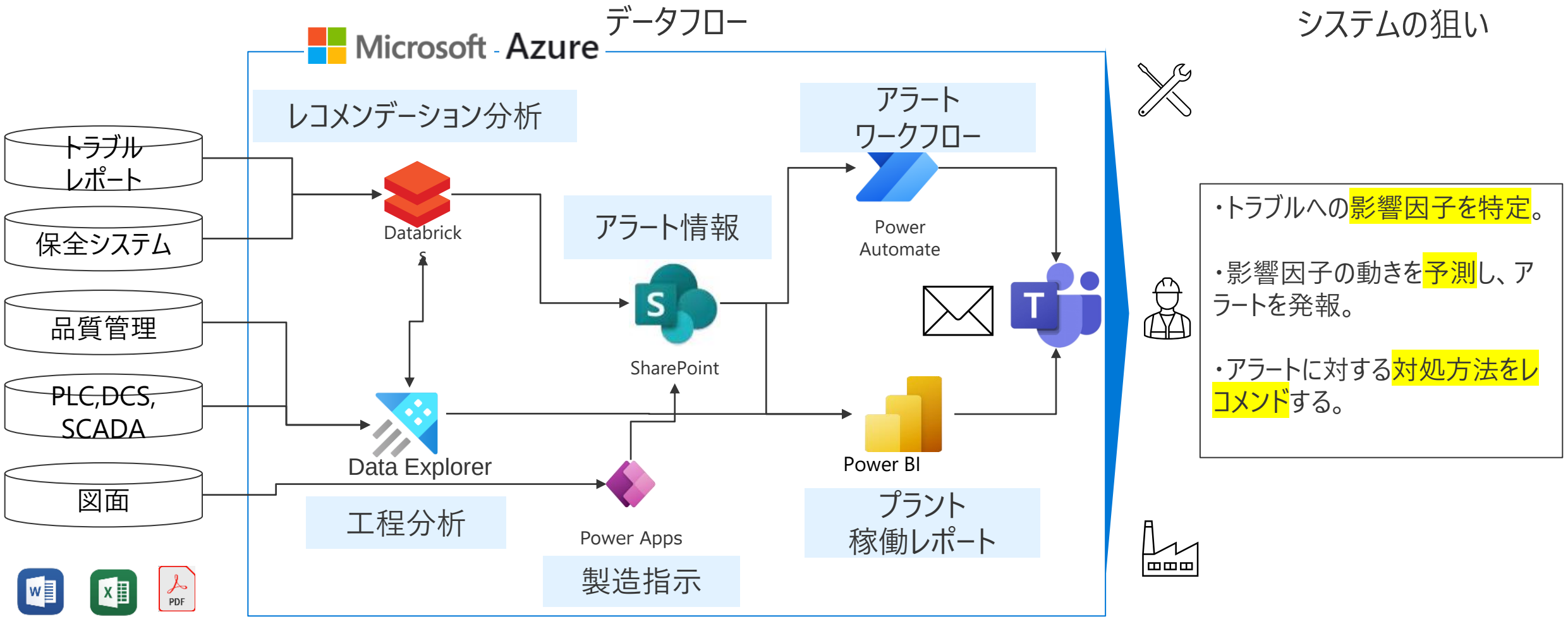
IT+OT +ET データ活用を想定したシステム連携の目的

“これによってこれまで年単位でかかっていたデータの可視化が数週間で可能になる” 米国シェブロン社



技能伝承＋生産最適化を狙った「ファクトリーデータプラットフォーム」

IT+OT+ ET データを連携させたプランデータを常に解析し、異変を予測してアラートを発報し、対処法方法をレコメンドすることで、オペレータの負荷低減や適切な対応を素早く行い、トラブルや事故防止と対応力向上を目指す。



サイバーセキュリティー対策

Microsoft Defender for IoT

スマート化を進めていくにつれ、コントロールシステムへの脅威は増えつつある。　プロセスエンジニアと計装エンジニアの立場で対策を検討する必要がある。

世の中の変化

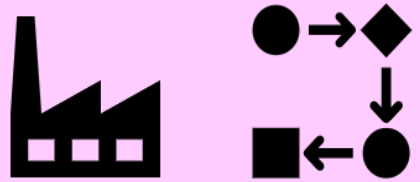
- システムベンダーによるプロトコル標準化・汎用化への変化
- インターネット、WiFi接続機会の増加
- 管理の行き届かないIoT 機器の増加
- セキュリティへの準備・意識不足
- IT/OT 連携によるデータ活用
- 攻撃パターン・手法の多様化と巧妙化、マルウエアの流通

製造現場でのデバイス増加

- ✓コントローラとアクチュエータ間の通信攻撃
- ✓アクチュエータ制御不具合
- ✓センサー測定値操作と記録データの改ざん
- ✓HMI, スマホの不正操作
- ✓SIS（安全計装システム）への攻撃

悩ましい対処

- ✓物理的変化が起きてからでは手遅れ
- ✓故障・人為的ミスと攻撃の見極めが困難
- ✓通信遮断後の手動操作による対処が不安
- ✓ネットワーク技術とプロセス制御の視点での対策が必要



簡易アセスメントサービス提供中

このような経験はありませんか？

インシデントが起きている可能性を持つ異常現象

– 制御動作が時々遅くなる。
– 通信エラーが出るようになった。
– 制御データが抜けている。
– 制御動作変化しているべき制御データが変化していない。
– 制御信号が突然変化する。（突変現象）
– 壊れるはずの無い部分が壊れ 。おかしな ストレスがかか ったと思われる 。
– 制御機器のメンテナンスチェックが終了しない。
– 閉まっていなければならない操作端（自動弁など）が開いている。また、その逆。
– 再起動してしばらくは正常動作していたが また 同じ異常になった.。
– ソフトウェア更新をしたら、異常になった。
– USBで作業をしたら、異常が出るようになった。
– 外部サポ ートを受けた後に 異常が出るようになった。
– 制御異常現象は出ていないがインシデント発生

出典：制御システムセキリティシステムセキュリティ検討タスクフォ スタスクフォース (2012)

最近の事例　～IPA(情報処理推進機構）公開資料より抜粋

2019年3月ノルウェー：
Norsk Hydro がラン サムウェア『LockerGoga』の被害を受け数カ月の長期間にわたり生産量が低下。

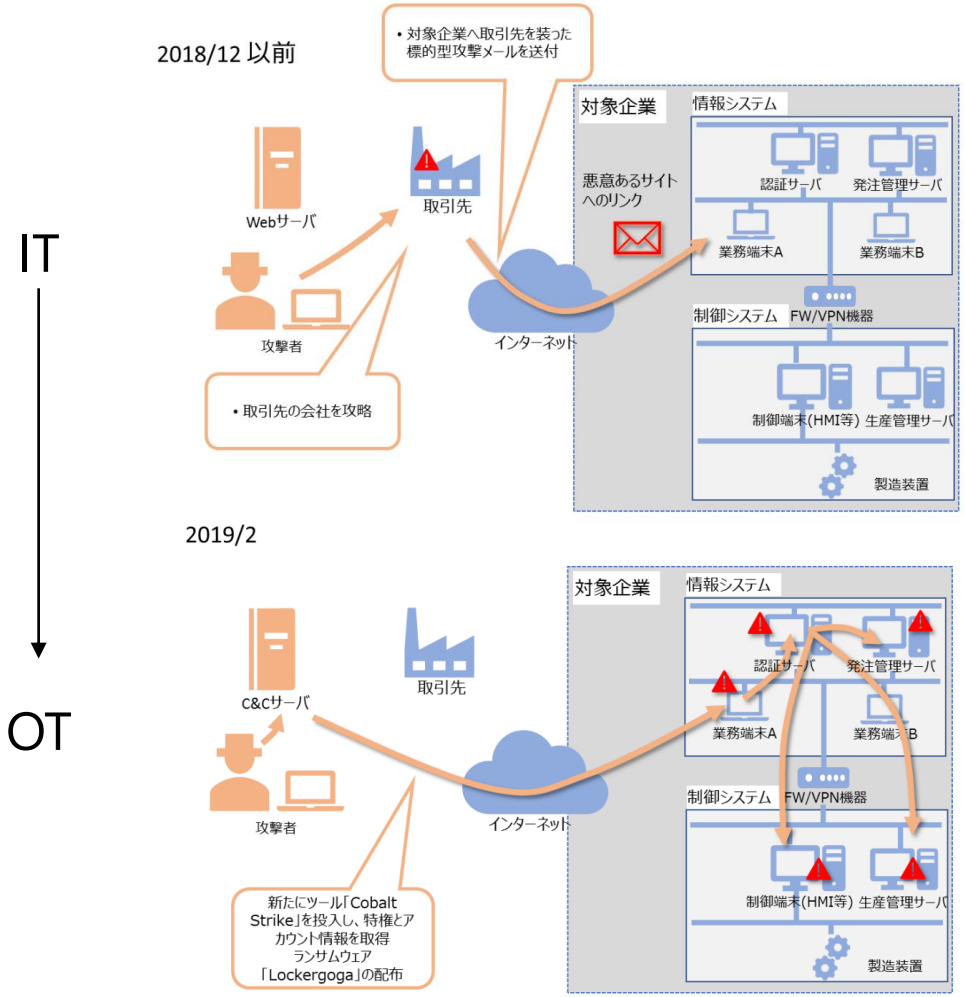


図 1-4 攻撃の足場確立

侵入経路

1. 取引先と従業員のメールのやりとりを傍受し、取引先を装って悪意のあるサイトのリンクを仕込む。
2. 従業員がそのリンクをクリックし、バックドアが開きトロイの木馬が侵入
3. バックドアを通じ攻撃用ツールCobalt Strikeを投入し、管理者権限を獲得
4. 制御システム側に侵入し、PC内のファイルを次々と暗号化しOSを無効に

日本のガイドライン

経済産業省：2023年３月２４日サイバーセキュリティーガイドラインv3.0

「。。。。。。制御系を含むデジタル基盤を守ることへのサイバーセキュリティーの対象の変化・拡大」

「。。。演習の対象は情報系のインシデントに限らず、制御系に影響が及ぶようなインシデントも含める」

Agenda

1. OTセキュリティーを強化すべき背景
2. ITセキュリティーとOTセキュリティーの違い
3. 先進企業の取組姿勢
4. Why MS
5. 答えるべき問い

プラント制御システムのセキュリティ確保の課題

制御システムは保護対象や特徴が従来のITシステムと異なるため、専門性の高い対応が必要。

	情報システム	プラント制御システム
システムの特徴	• トランザクション中心 • 情報管理が重要	• 周期処理中心 • 常時安定稼働が必須 • 情報システム系から隔離されている
データ保護の優先順位	C -> I - >A	A -> I -> C
耐用年数	３－５年	１０－２０年
担当組織	情報システム部	生産技術部、計装
パッチ適用	高頻度・定期的 自動配信	不定期、定修時 システムリプレース時 （制御通信に影響しないよう）
リアルタイム性	遅延は許容される	不可欠
技術標準	標準化、汎用OS	独自・専用プロトコル
攻撃の目的	情報搾取、金銭搾取	設備破壊、業務停止、社会の混乱、人命・環境への影響

C:Confidentiality（機密性）, I: Integrity（完全性）、A: Availability（可用性）

Effective solution

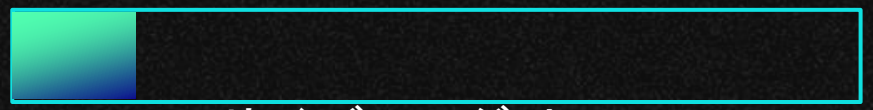
ISO 27001

情報セキュリティ管理体制

IT情報セキュリティ

技術的解決策の欠如

OTには言及せず



OTサイバーレジリエンス
の管理?

NO

IEC 62443

サイバーセキュリティマネジメントシステム

OTサイバーレジリエンス

OTのためのデータフローモデル

対策の明示

OTサイバーレジリエンス
の管理?

YES

Agenda

1. OTセキュリティーを強化すべき背景
2. ITセキュリティーとOTセキュリティーの違い
3. 先進企業の取組姿勢
4. Why MS
5. 答えるべき問い

先進企業のICS領域取組とコメント

ARC Industry Leadership Forum Orlando 2023 Feb

Shell, Exxon Mobil, Petronas, Petrobras, Chevron, bp, BASF, Celanese, Dow, Pfizer, PepsiCo
& Microsoft

- 「未来の制御システム」について討議
- 複数制御システムを遠隔でコントロールする
- クラウド活用は大前提
- AI , 機械学習はあたりまえ
- サイバーセキュリティーは常に進化させなければならない

ビジョン

自動制御

クラウド &
セキュリティ

先進企業のOTセキュリティーに関するコメント

ARC Industry Leadership Forum Orlando 2023 Feb

業務の変化	・ Security はoperational excellence の一部 ・ プラント外からプラント情報にアクセスすることが増えており、ウイルス感染のきっかけを作っている。 ・ いろんなリスクの為にいろんな投資をしているかもしれないが、運用が複雑になったり、必ずしもリスク低減になってないこともあるし、新たなリスクを招くこともある。
対応方針・施策	・ Cybersecurity を整備しておけば、プラントでいろんなことができる。システム連携やデータ連携・活用が進む。 ・ オペレータはCybersecurity 教育を受けており、何かおかしいと気づいたら何をすべきか理解している。 ・ IT team, OT team, Engineering team、が連携しサービス組織として全社支援をしている。 ・ OTのリスクアセスメントをしっかりとやっており、どんなリスクがあるか常に理解して管理している。

Agenda

1. OTセキュリティーを強化すべき背景
2. ITセキュリティーとOTセキュリティーの違い
3. 先進企業の取組姿勢
4. Why MS
5. 答えるべき問い

業界最高レベルのセキュリティ

監視
140以上[3]
脅威グループの数

40以上[1]
国家主導グループの数

全世界の数十億のお客様にサービスを提供して学習し、今後の動向を予測

65兆[4]
分析
1 日に分析される脅威シグナルの数

370億[4]
ブロック
1 年にブロックされるメール脅威の数

200億ドル[1]
今後 5 年間の投資
知識の向上と共有、インサイトの獲得、サイバー犯罪への対応に向けた投資

時間とリソースを節約しながら、お客様のセキュリティを確保

60%↑
マルチベンダーのセキュリティ ソリューションと比較した場合の平均 **コスト削減率**

1.5万[1]
セキュリティ エコシステムのパートナーの数

86万[4]
自社を保護するためにマイクロソフトのセキュリティを選んだお客様の数

全世界で信頼され、組織のマルチクラウドおよびマルチプラットフォーム インフラストラクチャを保護

1. 決算プレス リリース、22 年度第 4 四半期2022 年 7 月 26 日、マイクロソフト IR
2. 「Microsoft Digital Defense Report」、2021 年 10 月、Microsoft Security
3. 決算プレス リリース、22 年度第 2 四半期2021 年 12 月 16 日、マイクロソフト IR
4. 「Microsoft Security が新たなマイルストーンに到達 ― インクルーシブで顧客志向のソリューションが成果をもたらす」、Microsoft Security ブログ

ハイブリッド・マルチクラウドのセキュリティ・ガバナンス強化

50 以上の製品カテゴリーを統合

もっとも信頼性の高い包括的なクラウド

Do more with less

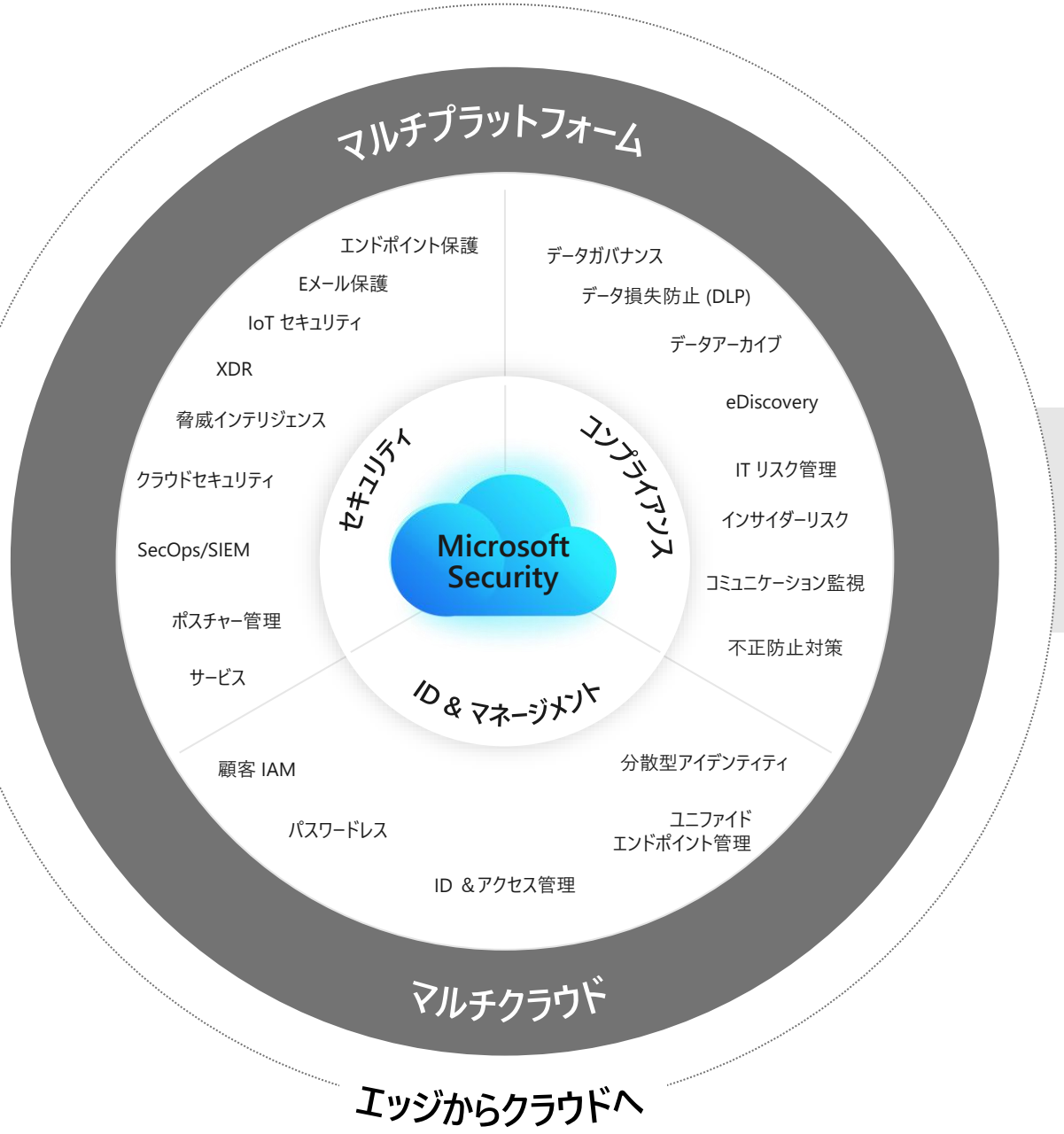
より少ない時間・資源で、より多くのことを実現する

ビルトイン エクスペリエンス

AI & 自動化スケール

カテゴリーを超えた統合

コンプライアンス	Microsoft Compliance　Microsoft Purview
セキュリティ	Microsoft Defender　Microsoft Sentinel
デバイス管理	Microsoft Intune
ID とアクセス管理	Azure Active Directory
クラウドプラットフォーム	
デバイス OS	

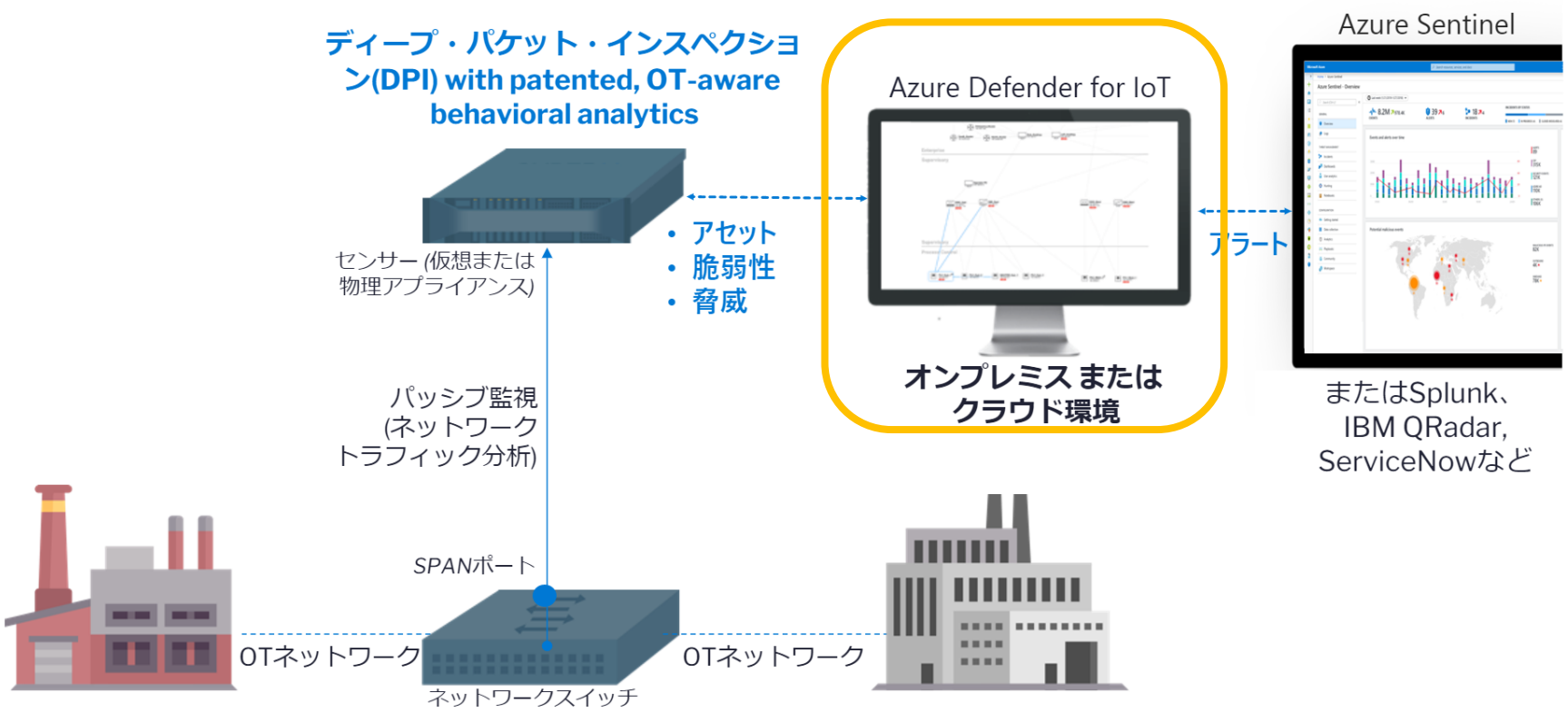


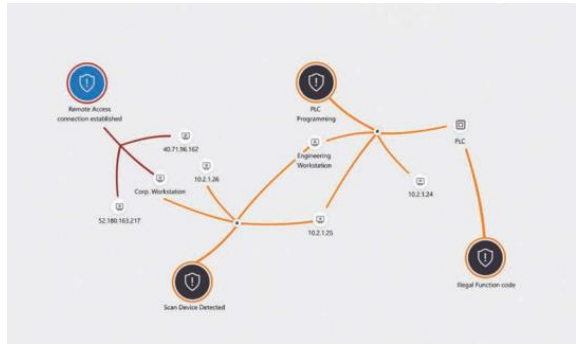
Defender for IoT: 制御システムへのサイバーセキュリティー対策

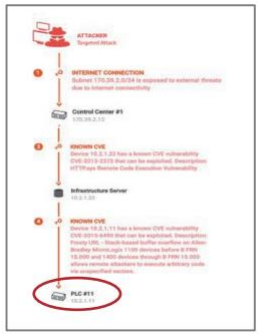
スマート化を進めていくにつれ、コントロールシステムへの脅威は増えつつある。　プロセスエンジニアと計装エンジニアの立場で対策を検討する必要がある。

① OTネットワークの可視化　アセット情報、脆弱性の情報をシングルコンソールで管理
② リスクの可視化　機械学習を活用した振る舞い分析、脅威検知
③ Microsoft Sentinelとの連携　IT環境とOTの環境の統合

パフォーマンスに影響を与えず素早く展開







簡易アセスメントサービス提供中

被害にあうケースに共通して言える OT 環境の課題

- どのような機器が OT ネットワークに接続されているかの**実態**がわからない

  ＜例＞
  ①　勝手に持ち込んだ管理されていない機器がアクセスポイントを設置している。（そのアクセスポイント経由で部外者が既に侵入されているリスクもある）

  ②　管理されていない機器経由で OT 機器を制御できる HMI へのアクセスやコマンド発行もできてしまう。

  ③　OT 環境の機器を勝手に操作するなど、業務環境に影響がでる危険性がある

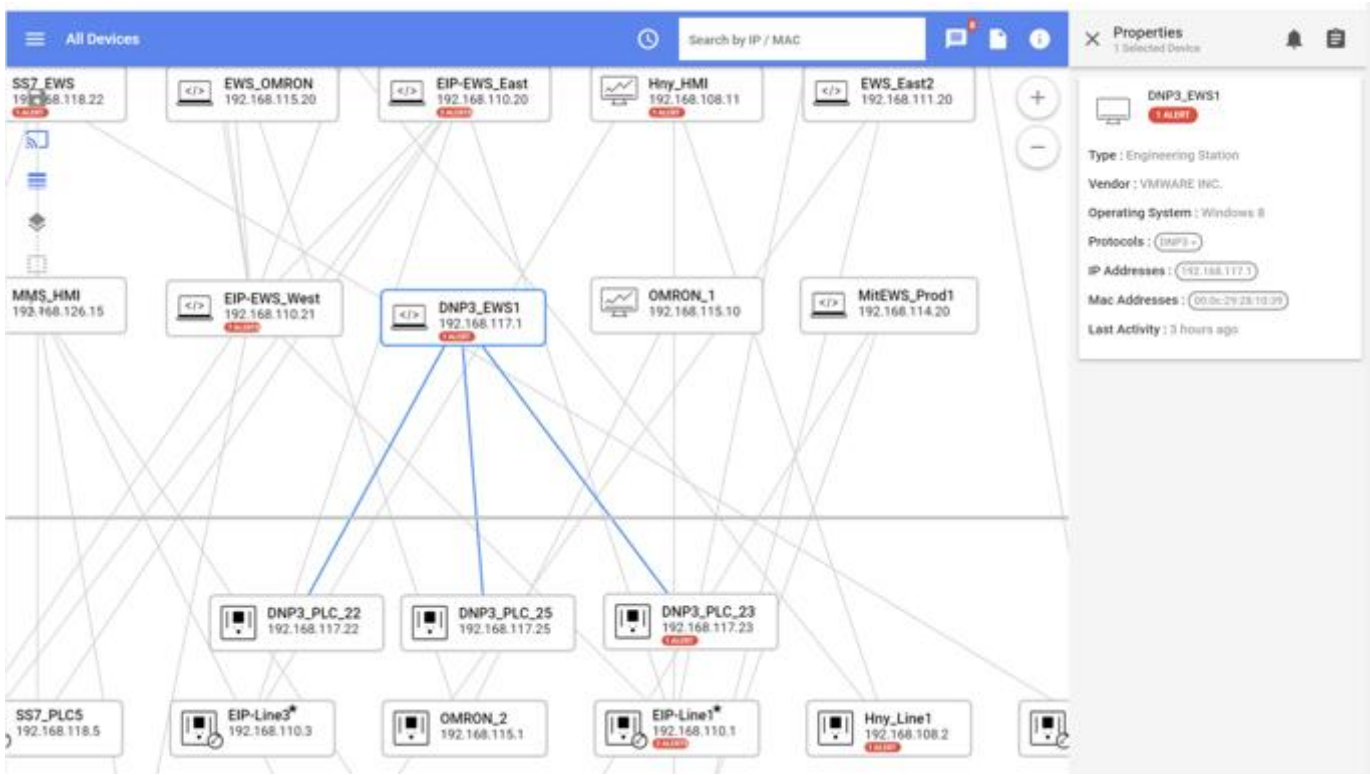
OT 資産管理のための資産の棚卸が第一歩。

手元の台帳でどの機器がどこに接続されているか、ではなく、**利用実態を把握すること**が、
リスクの顕在化を未然に防ぐことにつながります。

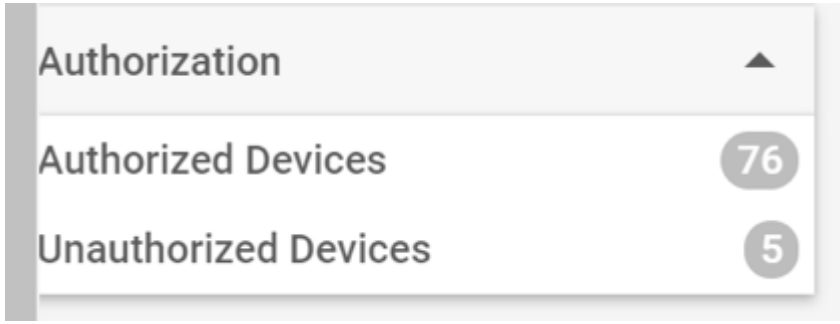
Authorized Devices

- ネットワーク上にどのデバイスがあるか知っていますか?
- 彼らが誰と通信しているか知っていますか?

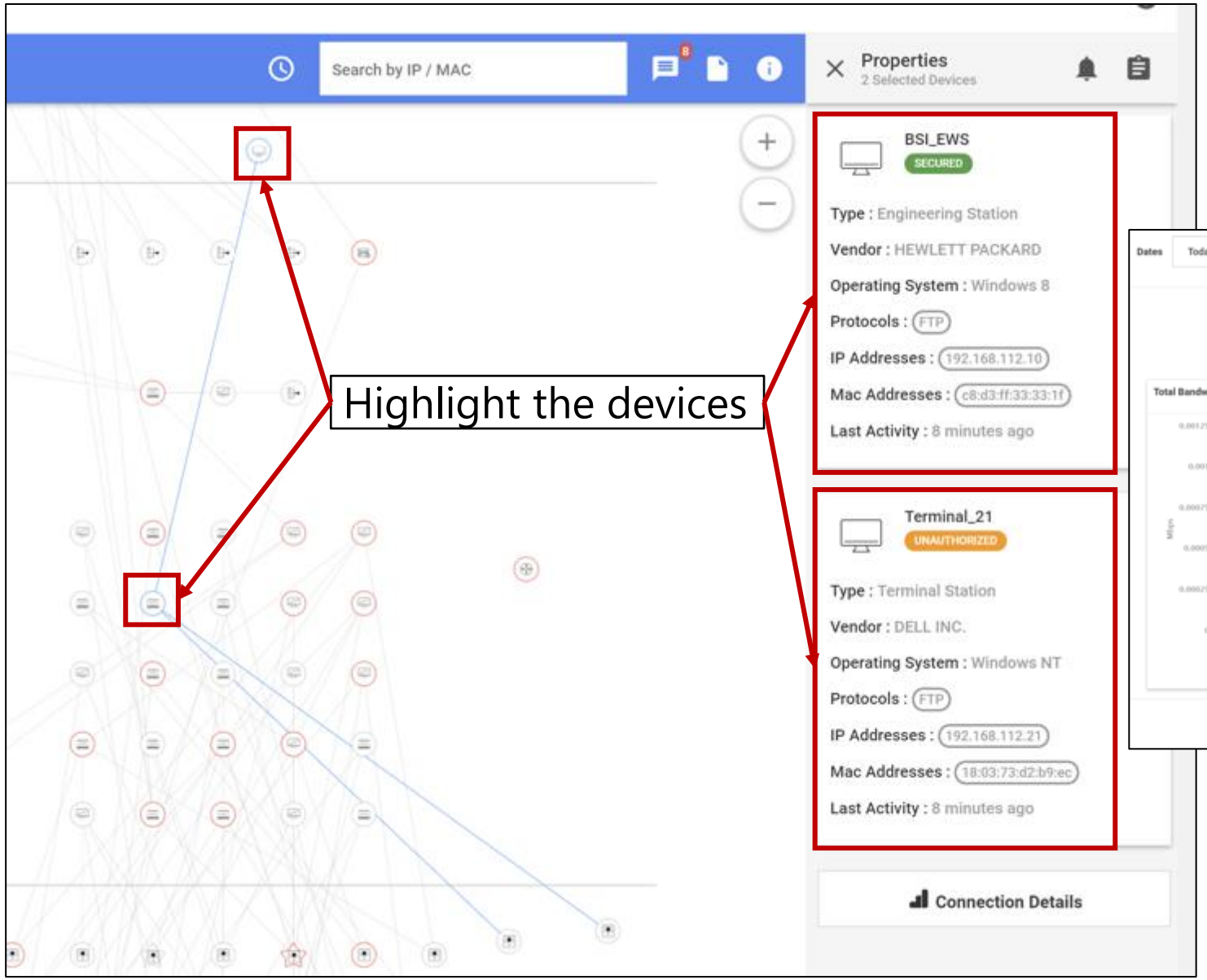
- もし理解しているならそれらは「承認された」デバイスである可能性があります...



- どのデバイスが「未承認」であるか知っていますか？
- どのくらい早くそれらを識別できますか?
- 彼らが何をしているのかをどうやって知るのですか?



Unauthorized Device – What are they doing?



See the details

アセスメント実施の想定スケジュール*

Sample

	1. アセスメント説明・QA	2. pcap データ収集	3. Microsoft で解析/レポート作成	4. 報告
お客様	本対策の必要性や製品、本アセスメントメニューに関してご理解いただく (オプション) ・Defender for IoT のポータルの利用検討 ・Microsoft Sentinel との併用検討	Pcap データ収集** データ送付		・報告会へのご参加 (1 時間) ・Q＆A ・利用ご検討
マイクロソフト	Microsoft Defender for IoT 製品説明 アセスメント内容のご紹介 QA		ログ受領 解析およびレポート作成***	・報告会の実施 (1 時間) ・Q&A ・今後のご提案

*上記のスケジュールはあくまで標準的な想定です、柔軟に変更可能ですので必要に応じてお申し付けください。

収集いただくトラフィック量は、約3時間分くらいを目安に収集ください。　**pcap (packet **cap**ture)

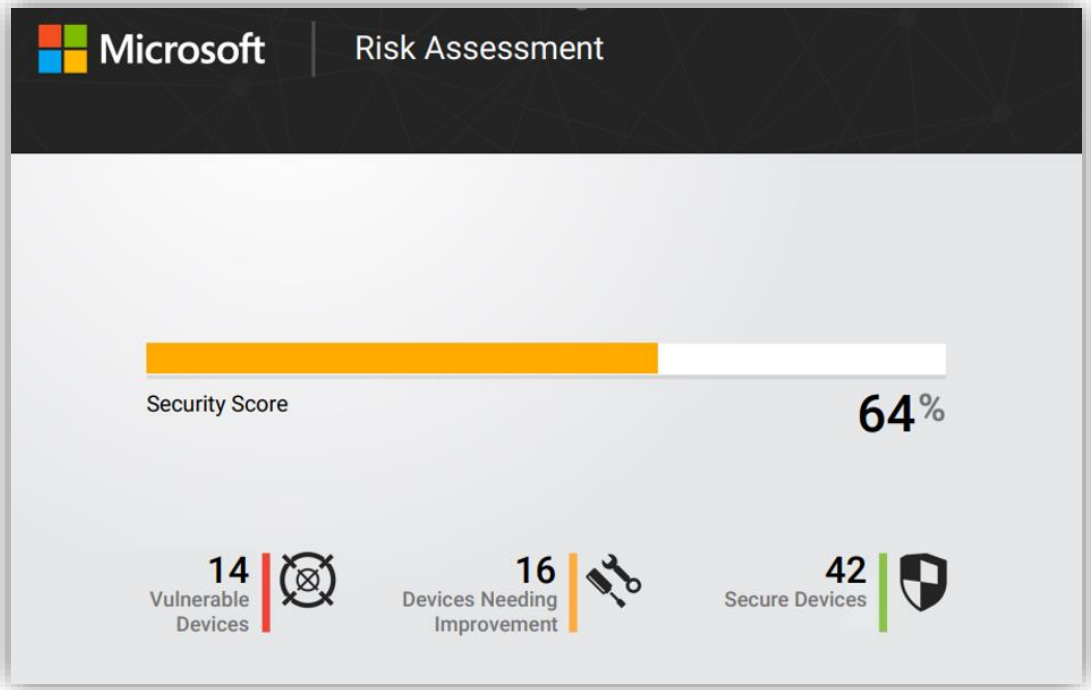
***レポート作成には平均1週間-2週間いただいております。

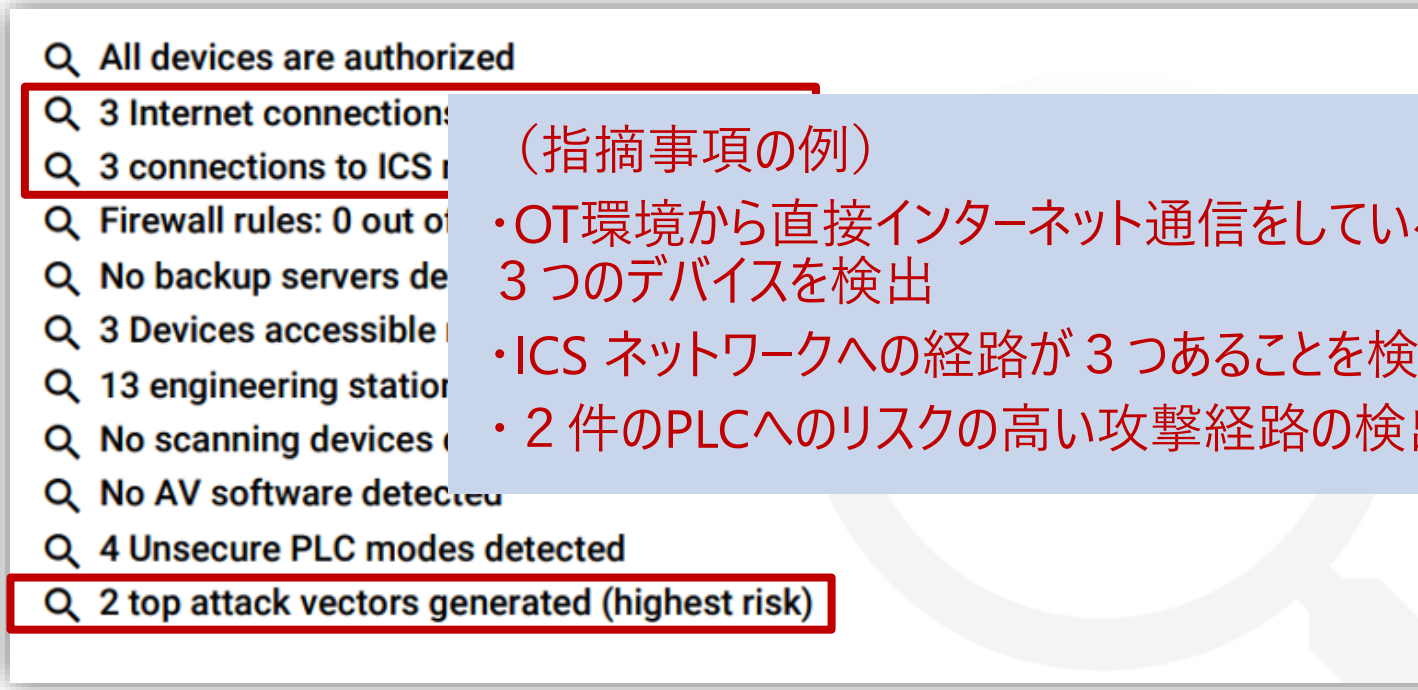
サンプルレポート – OT 資産可視化アセスメント結果概要

Microsoft Defender for IoT

Sample

診断項目	要確認度	アセスメント結果	推奨対処
非管理デバイス検出	高	■ 複数のデバイスを検出しました。これがすべて把握できている資産でない場合、不正に接続されたデバイスの可能性があり、当該資産の特定が急務です。	■ 管理台帳との照合 ■ 未管理デバイスの設置場所の確認
プレインパスワード	中	■ FTPでプレインパスワードの利用が検出されました。パスワードが暗号化されていないためパスワード流出の危険があります。	■ 暗号化通信の利用
インターネット通信	低	■ インターネットとの通信が検出されました。これが意図した通信ではない場合、機器が勝手にインターネット上のサーバーと通信している可能性があるため、通信内容の特定が急務です。	■ インターネット通信をしているアプリケーションの特定





（指摘事項の例）

・OT環境から直接インターネット通信をしてい
3 つのデバイスを検出

・ICS ネットワークへの経路が 3 つあることを検

・2 件のPLCへのリスクの高い攻撃経路の検

Agenda

1. OTセキュリティーを強化すべき背景
2. ITセキュリティーとOTセキュリティーの違い
3. 先進企業の取組姿勢
4. Why MS
5. 答えるべき問い

答えるべき問い　例

- サイバーセキュリティ防御が適切に展開されていることをどのように測定できているか？
- 展開する特定のアクションや組織機能が、特定の攻撃からユーザーを保護していることをどのように確認できるか？

「チェックリストに、レ点をつけるような単純な確認作業ではダメ。」
米国大手エネルギー会社

Microsoft

Our operational strength is your advantage (+3,500 experts)