CISCO
SECURE

cisco The bridge to possible

Edgecross 工場セキュリティガイドライン 啓発・連続セミナ第5回

工場のデジタル化とセキュリティ対策の実態

2023年7月28日

中河 靖吉（ynakagaw@cisco.com）
セキュリティ事業
シスコシステムズ合同会社

Agenda

- はじめに
- 製造現場におけるセキュリティ取組みの背景
- 工場セキュリティ対策の実態と実現に向けた考慮点

はじめに

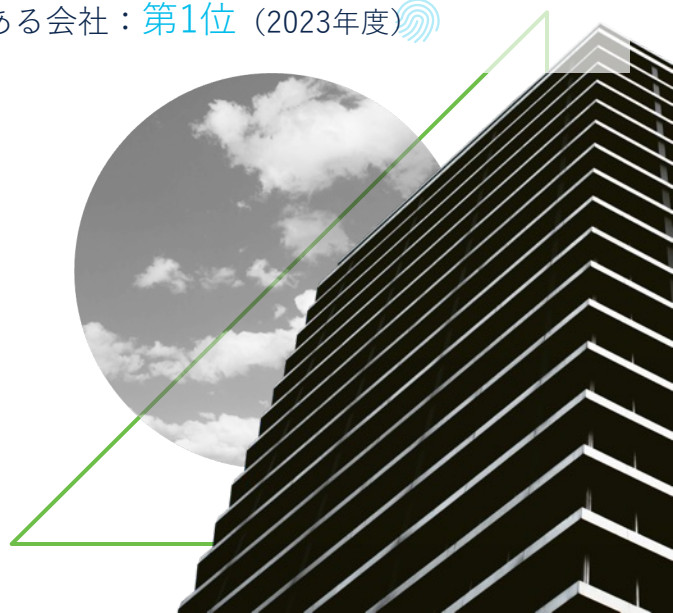
会社紹介

Cisco Systems Inc.

- ビジネス展開：95カ国 / 389拠点
- 社員数：81,000名＋パートナー 60,000名
- 買収企業：230社+（1993年以降）
- 研究開発費：68億ドル（2022年度）
- 売上高：516億ドル（2022年度）
- 純利益：118億ドル（2022年度）
- ソフトウェア販売：世界第6位（比率 53%）
- 働きがいのある会社：第1位（Fortune Best 100 2022）
- ブランド価値：世界第15位（Interbrand 2022）

シスコシステムズ合同会社

- ビジネス展開：7拠点（本社 東京）
- 社員数：1,300名＋パートナー 950名
- 働きがいのある会社：第1位（2023年度）

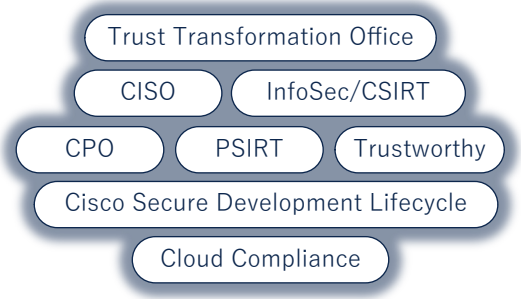


はじめに

セキュリティ事業

Security & Trust Organization (S&TO)

- 全社横断の情報セキュリティの専任組織
- シスコのデジタル事業を保護し、すべてのオファーが私たちの利害関係者のセキュリティとプライバシー要件を満たすように支援
- 教育とパートナーシップを通じて信頼を構築



Security Business Unit (セキュリティ事業)

- 2022年度シスコセキュリティ事業規模： 5,200億円
- 過去4年間セキュリティ領域に約9,000億円投資
- 1995年からセキュリティ関連企業を27社買収
  （最も広範囲なセキュリティーポートフォリオを保有）

TALOS

- 世界最大の民間セキュリティ研究機関
- 約500名の分析官が所属

Agenda

- はじめに
- 製造現場におけるセキュリティ取組みの背景
- 工場セキュリティ対策の実態と実現に向けた考慮点

製造現場のデジタル化とは？

企業としてのDX

生産性の向上

製造現場のデジタル化

従業員安全性向上

機械学習　AI検品　予兆保全　デジタルツイン

デジタルインフラの整備

製造現場のデジタル化実現のためにはネットワークの高速化と安定化が必須

センサー　端末　人　コンピューティング　設備

製造に関わる人や物

そもそも論

製造現場におけるDXは誰のため？何のため？

企業・経営の観点

- 市場の変化を受けたビジネス変革（ビジネス継続性、SDGs、カーボンニュートラル）
- 製造現場に対して、需要変化に適応出来る仕組みと経営観点での可視化をDXの取り組みとして要求（生産、サプライチェーン全体での生産効率）

製造現場（OT）の観点

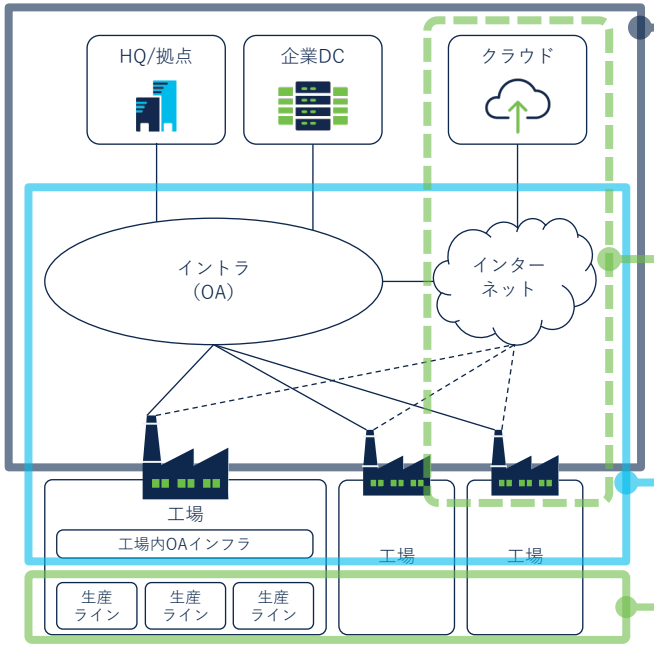
- 経営側からの要求に対する対応
- 製造現場における継続的な改善活動
- 市場の変化に伴い要求される製品の生産に対応

ITの観点

- 上記対応において必要となる企業横断的な施策を推進
- 企業におけるDX推進のサポートとIT資産の保護

そもそも論

ステークホルダー毎の対応範囲



企業・経営の観点

- ビジネス全体
- 工場単体ではなく工場、サプライチェーン全体
- ブランド価値

製造現場（OT）の観点

- 基本的には工場、生産ライン単位での生産効率、稼働率（分析基盤としてクラウド活用）
- セーフティ、生産ラインの無停止

ITの観点

- インフラ全体でのガバナンス、インフラのサービス品質、TCO
- デジタル資産の安全性

ステークホルダー毎の責任範囲とフォーカスは異なっており、現状、製造現場・工場内の

生産ラインや生産設備の責任の主体は工場側（OT側）にある

近年の製造現場におけるサイバーインシデントの実態

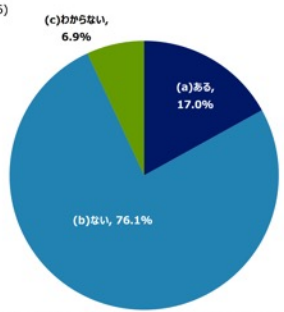
取引先等を経由したサイバー攻撃被害の主な内容
<①仕入・外注・委託先等の取引先>

分類	内容
Emotet	● 取引先がEmotetに感染し、不正なメールを受信
ランサムウェア	● 取引先がランサムウェアに感染し、自社関連情報が暗号化／外部漏洩 ● 取引先がランサムウェアに感染、業務停止し、自社業務に影響
不正アクセス	● 取引先のシステムが不正アクセスをうけ、自社関連の情報が漏洩
DDoS攻撃	● 委託先のシステムや利用するクラウドサービスがDDoS攻撃を受け、自社業務に影響
その他	● 取引先と情報共有を行うために利用するツール（ファイル転送サービス）が侵害を受け、情報が流出 ● 取引先のホームページの改ざんによる、不正サイトへの誘導、自社業務への影響 ● 取引先が提供する電子決済サービスの悪用による顧客口座の不正送金　等

取引先等を経由したサイバー攻撃被害の経験
<①仕入・外注・委託先等の取引先>

➢ 過去に取引先等がサイバー攻撃の被害を受け、それが貴社に及んだ経験がありますか（仕入・外注・委託先等の取引先）

(N=1876)



※「仕入・外注・委託先等の取引先を有していない」回答先を除く

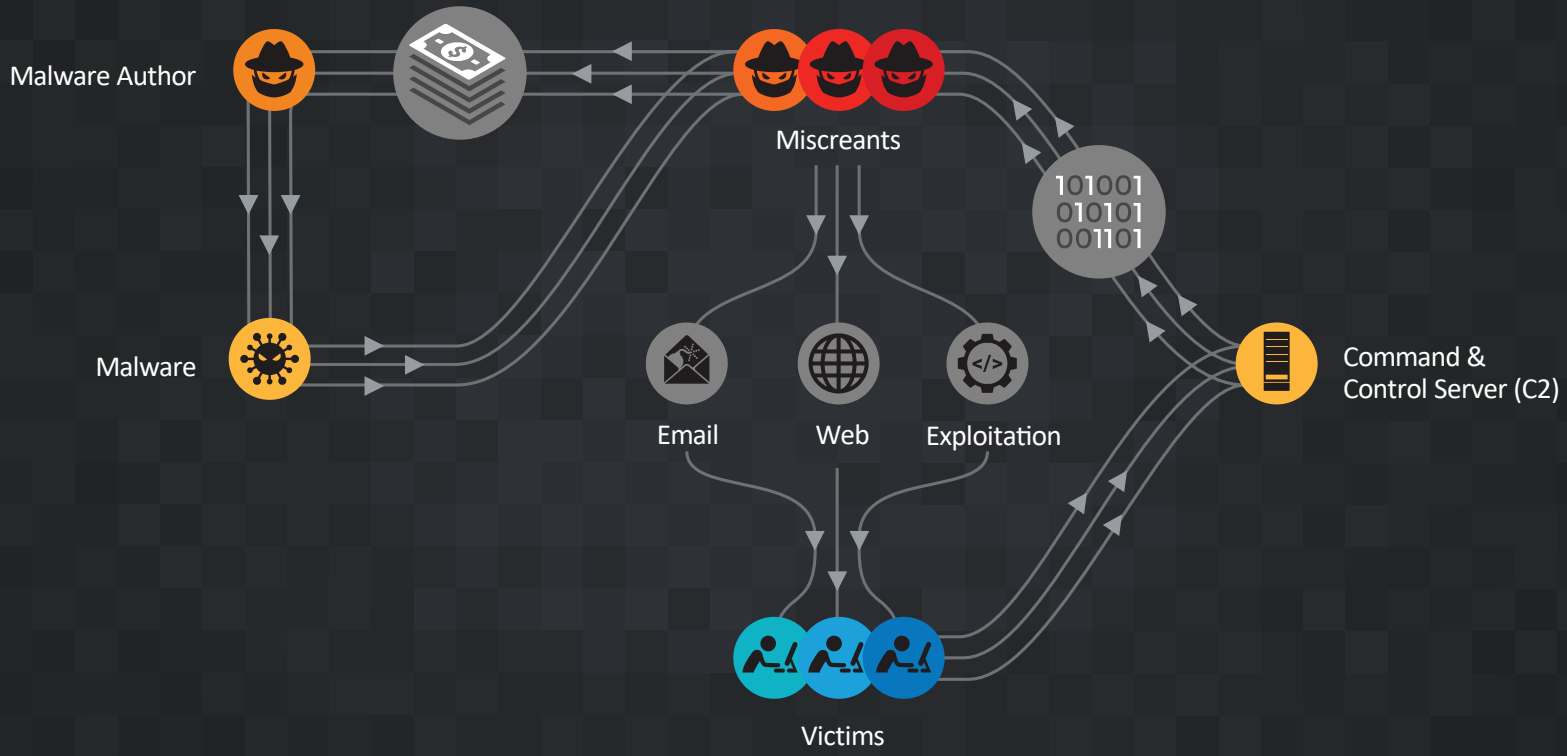
攻撃された企業	攻撃概要	被害規模
2020年6月 本田技研工業	ランサムウェア	• 国内外工場 10拠点以上での生産停止（2-5日） • PC端末数万台規模 • 北米でのリース契約業務停止
2021年2月 米 浄水システム	不正アクセス / データ改竄	• 米フロリダ州西部オールズマー市の浄水システムに何者かが不正侵入し、水酸化ナトリウムの濃度を変更して、通常の100倍以上に設定 ※管理者が即座に通常の値に戻したため、市の水道供給に重大な影響は与えず
2021年4月 仏 PIERRE FRABRE （化粧品会社）	ランサムウェア	• 工場の稼働が停止（約15日間）
2021年5月 米 Colonial Pipeline （パイプライン）	ランサムウェア	• ランサムウェアによりColonial Pipeline社内の一部のITシステムに影響 • わずか2時間で100GB近いデータ窃取が行われた可能性 • 予防的措置としてパイプライン全体の停止（約5日） ※発表としてはOTシステムへのラテラルムーブメントの兆候は確認していない
2021年7月 KESAYA および KESAYAが提供する VSA製品の利用企業	ランサムウェア / サプライチェーン 攻撃	• Kaseya VSAへの侵害を通じて100万台に影響 • 被害に遭った全ての組織に対する復号ツールと引き換えにKaseyaに対して7000万ドル（約77億円）相当のBTCを要求 • ターゲットとなったMSP事業者数は50～60程度 • 影響を受けた組織も800～1500と推計
2021年12月 デンソー メキシコ工場 /2022年3月デンソー ドイツ工場	ランサムウェア / サプライチェーン 攻撃	**メキシコ工場** • パソコン約20台のウイルス感染を確認し、業務に必要な情報については新しいネットワークへの移行を済ませていた。このため、サイバー攻撃による工場の稼働停止など事業活動への影響は起きなかったが、一部の情報が流出（ドイツ工場） • 生産活動や部品の受注・納品を管理するシステムに影響はなく、国内外の工場は通常通り稼働
2022年2月 小島プレス	ランサムウェア / サプライチェーン 攻撃	• トヨタ自動車は、部品仕入取引先の小島プレス工業のシステム障害を受けて国内の全ライン停止を公表

※出展
経済産業省　令和３年度サイバー・フィジカル・セキュリティ対策促進事業 （企業におけるサプライチェーンのサイバーセキュリティ対策に関する調査） - 株式会社NTTデータ経営研究所

近年、工場を発信源として発生したサイバーインシデントは少なくなっており、
工場に影響を与えるインシデントはIT（OA）側から来る傾向にある。

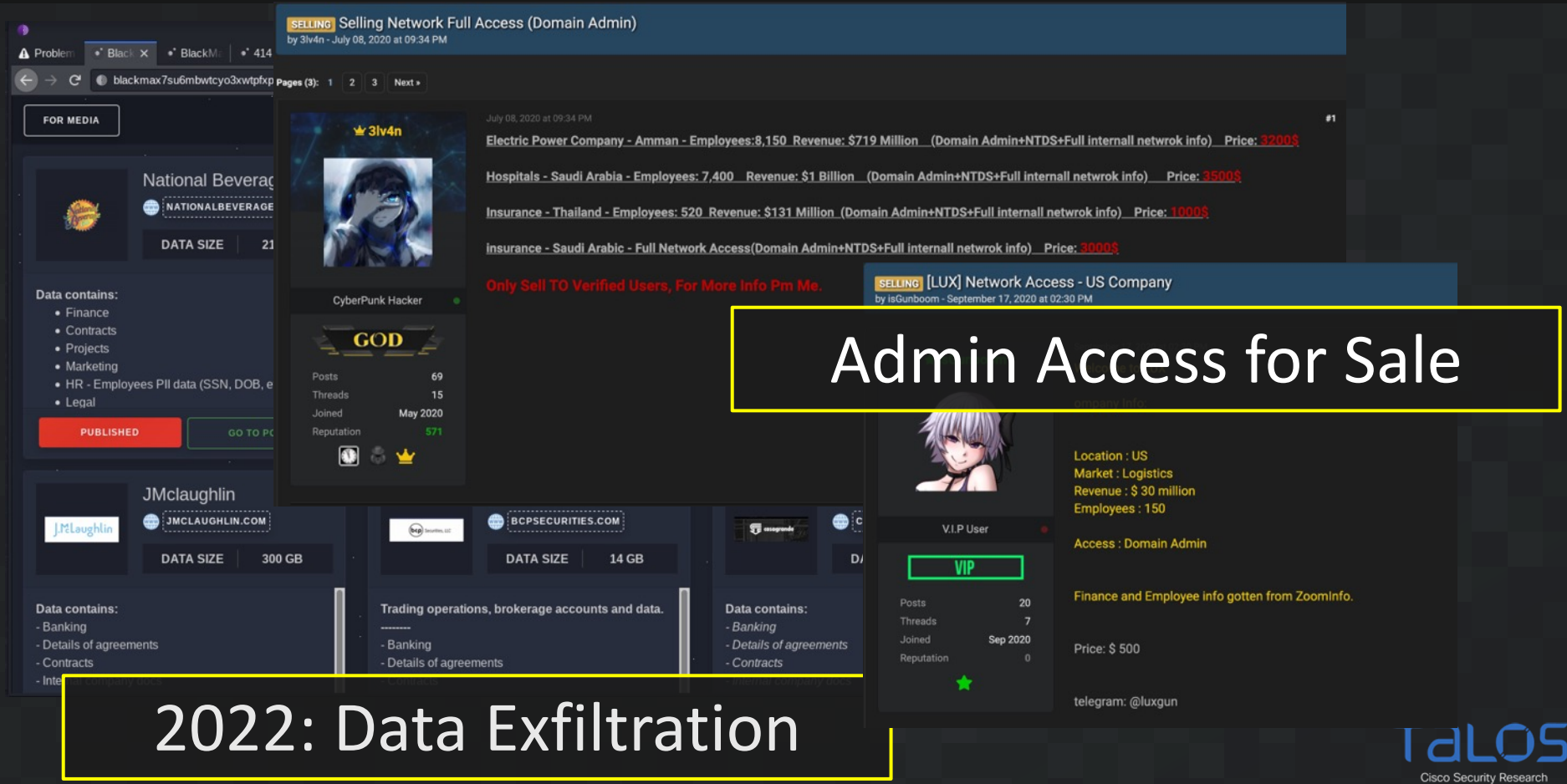
製造現場におけるセキュリティは工場側（OT側）での対応が必要

商品化されたマルウェアのライフサイクル



TALOS
Cisco Security Research

攻撃側の実際



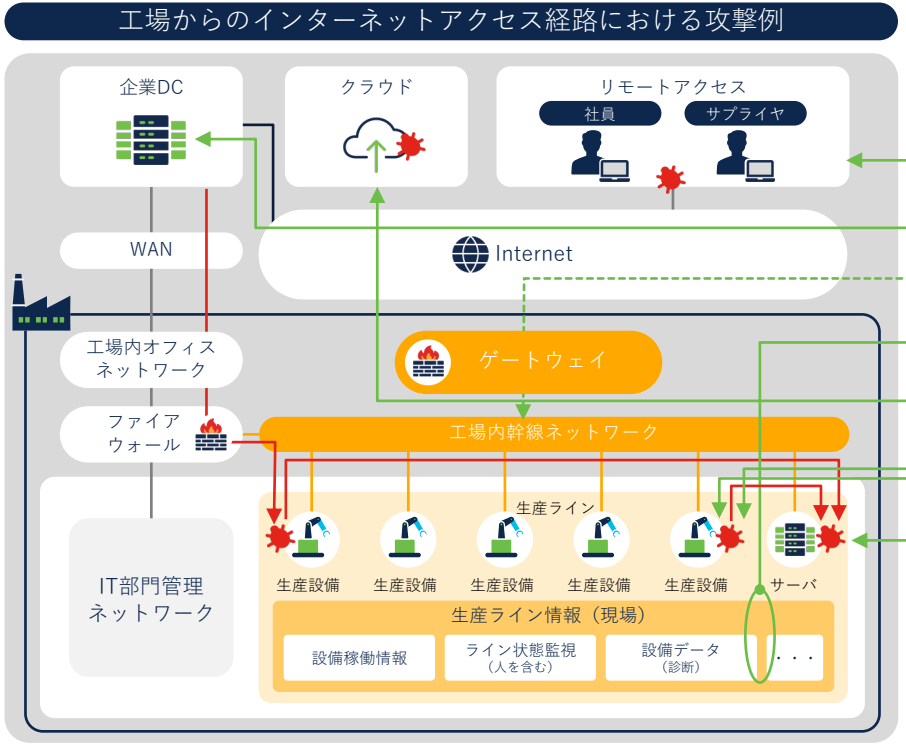
Admin Access for Sale

2022: Data Exfiltration

Cisco Security Research

工場におけるサイバー攻撃の概要

製造現場へのサイバー攻撃は、様々な経路から侵入し、拡散する。



攻撃者／組織

メールによる標的型攻撃（フィッシングなど）

- 社員宛にマルウェアを添付したメール（Emotetなど）、またはC&Cなどへの誘導リンクを含むメール（フィッシングメールなど）を利用し、侵入のための仕込みを行う（パスワード情報、ネットワーク環境、脆弱性の有無、など）

ネットワーク経由の攻撃（リモートアクセスなど）

- 脆弱性のあるネットワーク機器をついて侵入（不要なポートが空いている、脆弱性のあるソフトを利用している、など）
- リモートアクセスのセキュリティが脆弱である場合、ユーザーになりすまして侵入を行う

ラテラルムーブメント

- 社内に侵入したマルウェアが最終的に攻撃のターゲットとなる主要なデータと資産を検索するときにネットワーク内を徐々に移動する

C&C（コマンド・アンド・コントロール）

- 攻撃者がマルウェアに感染したコンピュータに指令を送り、遠隔操作するために用いる仕組み
- 実際の攻撃指示を行うためにマルウェアはインターネット上にあるC&Cサーバと通信を行う

近年のサイバー攻撃は高度化しており、
侵入を完全に防ぐことは難しくなっている

生産現場におけるセキュリティ対策の難しさと解決に向けたアプローチ

考慮すべきセキュリティのポイントは多く存在する一方で、生産現場ならではの課題も山積み。

セキュリティ考慮点	生産現場ならではの課題	解決に向けたアプローチ
新しく求められるOA->FA、 FA->OA間でのアクセス制御への対応	**脆弱性への対応を随時行うことが困難** • 変動要素が多い （関係者が多く、ラインごとに随時改善が行われる） • 生産重視のため、必要なタイミングでの作業（脆弱性の対応、など）が難しい • ライフサイクルがIT領域と違い長いため、OSサポート切れのデバイスが多く存在	**ネットワークで守る** • 資産を特定する • 必要最低限のアクセスに限定する • ネットワーク上の振る舞い監視により異常を検知する
利用するサーバ（OS）、 アプリケーションの脆弱性への対応		
デバイスの脆弱性への対応	**大きく異なるITとOTの運用観点と導入技術** • 生産を止めないことが最優先 • 分かり易いシンプルな運用/操作 • 独自生産システム/アプリケーション • IT観点での担当責任者の不在（国内）	**OT-ITの知識・経験を合わせて守る** • 生産・製造系部署を巻き込んだ体制構築 • 可用性を意識した現場との役割分担 • それぞれの担当者が実際に利用可能なソリューション選定
生産現場ネットワーク 接続資産の可視化		
生産現場で増加している クラウド活用ニーズへの対応	**ITとOTでの速度/温度感の差とセキュリティリスク** • 生産現場では常に改善が行われ、最新技術を積極的に取り入れる傾向 • IT部門では企業リスクを考慮し、通信要件の精査、段階的な導入を行う • 結果として、セキュリティリスクへの考慮が不十分な形で生産現場からインターネットへの直接的なアクセス環境が出来てしまう	**セキュリティリスクを認識する** • インターネット、クラウドと繋がることのセキュリティリスクを再度確認する • システムとしての連携範囲、影響範囲を明確にする • 関係者での周知を徹底する

セキュリティリスクを再認識し、OTとITが協力して

インフラ環境とセキュリティ、そしてその運用を考えていく必要がある

Agenda

- はじめに
- 製造現場におけるセキュリティ取組みの背景
- 工場セキュリティ対策の実態と実現に向けた考慮点

実際の検討例

一般的な工場領域でのチャレンジとCiscoご支援内容

お客様におけるチャレンジ

工場内デジタルインフラ構築
経営層視点でのデータ分析
生産現場での効率化のための分析

生産領域でのクラウド活用
生産現場での効率化のための分析基盤

サプライチェーン対策

データオープン化

Ciscoご支援内容

【IT部門向けご支援活動】

- 工場ガイドライン整備
- 工場インフラ設計支援
- 工場インフラ標準化支援（設計書作成）

【生産部門向けご支援活動】

- 新設ラインに対するインフラ検討支援
- 生産ラインインフラ標準化支援

実際の検討例

工場領域でのCiscoご支援内容と結果

【IT部門向けご支援活動と結果】

- 工場ガイドライン整備 → ❌ 強制的に推進しないと、IT部門で作成するだけではなかなか浸透が難しい
- 工場インフラ設計支援
- 工場インフラ標準化支援（設計書作成）

→ ✅ 新設されるラインや設備に対して新規でインフラ、セキュリティを整備し、最終的にはグローバルの標準的な設計としてドキュメント化

【生産部門向けご支援活動と結果】

- 新設ラインに対するインフラ検討支援 → ✅ 新設ラインのインフラとして標準的な構成決定のご支援
- 生産ラインインフラ標準化支援 → 🟠 生産部門間の関係に依存。類似設備の新設においては有効だが、部門間での連携がない場合は成立し辛い

国内工場におけるセキュリティ検討の論点

- 工場へのサイバーセキュリティ対策への取り組むきっかけは、大きく分けると「工場の新設計画」と「既存工場のセキュリティ強化」の２つ
- 工場の新設時のセキュリティ検討へのご相談は以前から継続して多く頂いているが、最近では既存工場のセキュリティ強化に関するご相談が増加傾向となっている
- 一方で、既存工場のセキュリティ強化のほうが難易度が高い

工場の新設計画

スマートファクトリー前提となり、OT、IoT等の様々なデバイスが大量に接続し、インターネットへアクセスする前提のため、セキュリティは初期段階から検討が開始される

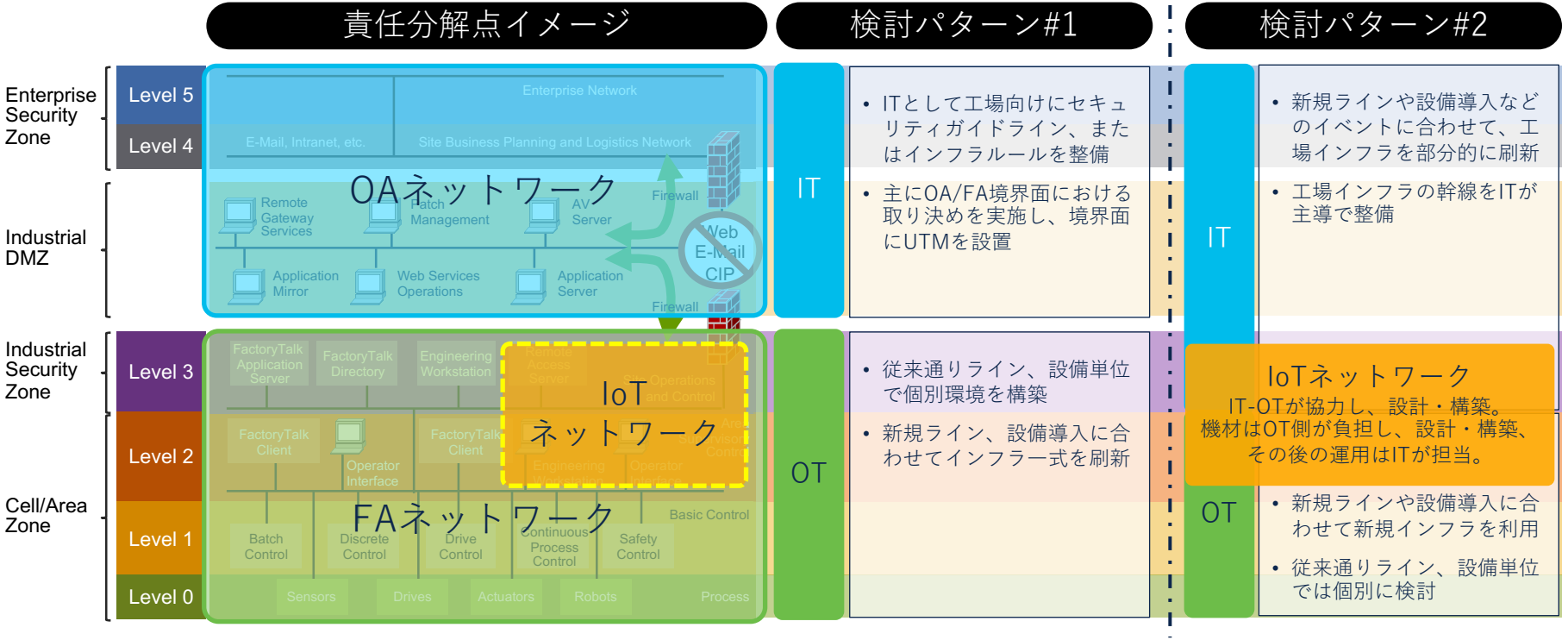
【特徴】
- プロジェクト体制が整備済み
- ゼロベースのインフラデザイン
- 導入するアセットが明瞭
- 確実に守るべき明確な期日がある

既存工場のセキュリティ強化

昨今のサイバー攻撃による同業他社の被害、社会的なセキュリティ意識の工場、業界・団体のガイドライン発出などにより、会社の施策としてセキュリティ強化への取り組みを実施

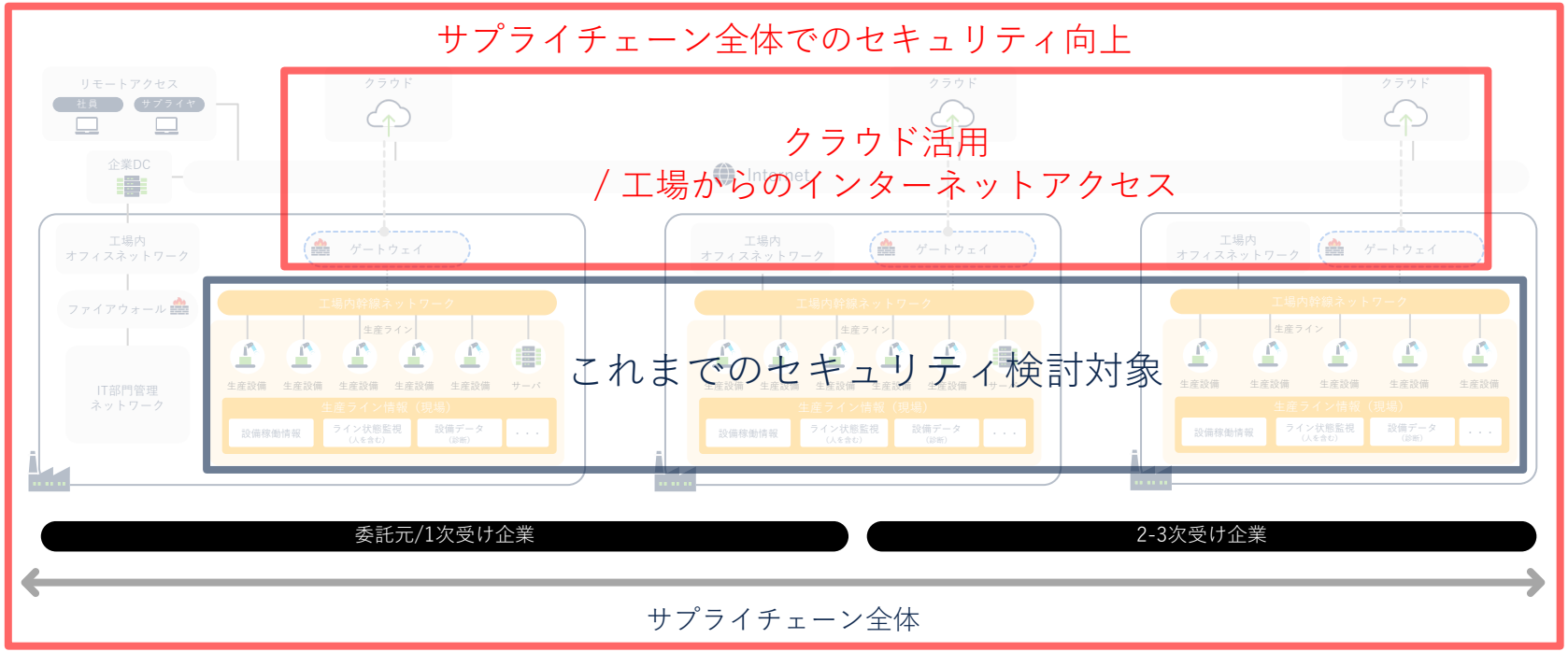
【特徴】
- 大半はIT部門主導の施策
- ツギハギまたはサイロ化され複雑なインフラ
- アセットが不明
- 確実に守るべき明確な期日がない

工場領域でのインフラ･セキュリティ検討の傾向



既存環境を対象にするかどうかにより、IT-OTの責任分解点は変わる。
インターネット、既存無線LANについては取り扱いが難しい。

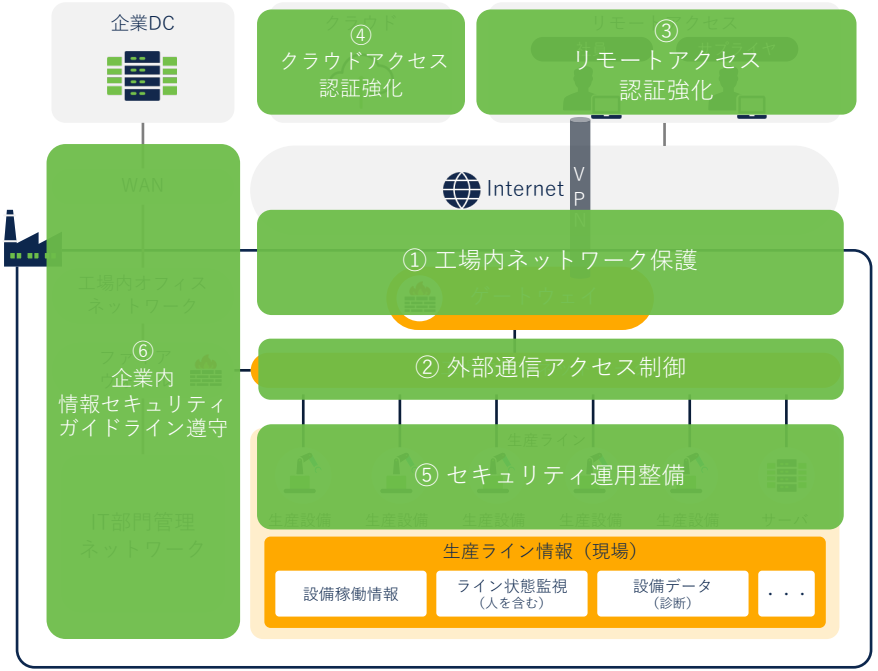
これまでの検討範囲と今後のセキュリティ検討範囲



エコシステム・サプライチェーンの拡大に合わせて、セキュリティの検討範囲も広がっている。
一方で、各社のデジタル化の進捗や企業規模により、セキュリティ対策の対象や内容は異なる 。

どのように対策を取るべきなのか？

侵入防止対策や万が一侵入されたあとの対処、緊急時の対応方法の整備まで、包括的な対策が必要です。



① 工場内ネットワーク保護

- 工場内でネットワークに繋がるデバイスを把握し、通信要件を把握する
- 用途や影響範囲に合わせて、ネットワークを物理/論理的に分割する（セグメンテーション）
- マルウェア感染対策としてデバイスの振る舞いを監視し、異常を検知する

② 外部通信アクセス制御

- 工場内ネットワークデバイスから外部向けの通信プロトコル、宛先の特定（送信元の特定と合わせて）する
- 重要なデータの有無や、データの取り扱いに関して整理を行う（リスク分析）

③リモートアクセス認証強化

- 工場内に外部から入ってくる通信の接続元および接続先の特定する
- リモートアクセス方式と、その際のユーザーおよびデバイスの認証方式（付帯設備との連携）を決める

④ クラウドアクセス認証強化

- クラウドに工場から、またはInternet経由で入ってくる通信の接続元および接続先の特定する
- クラウドアクセス時のユーザおよびデバイスの認証方式（付帯設備との連携）を決める

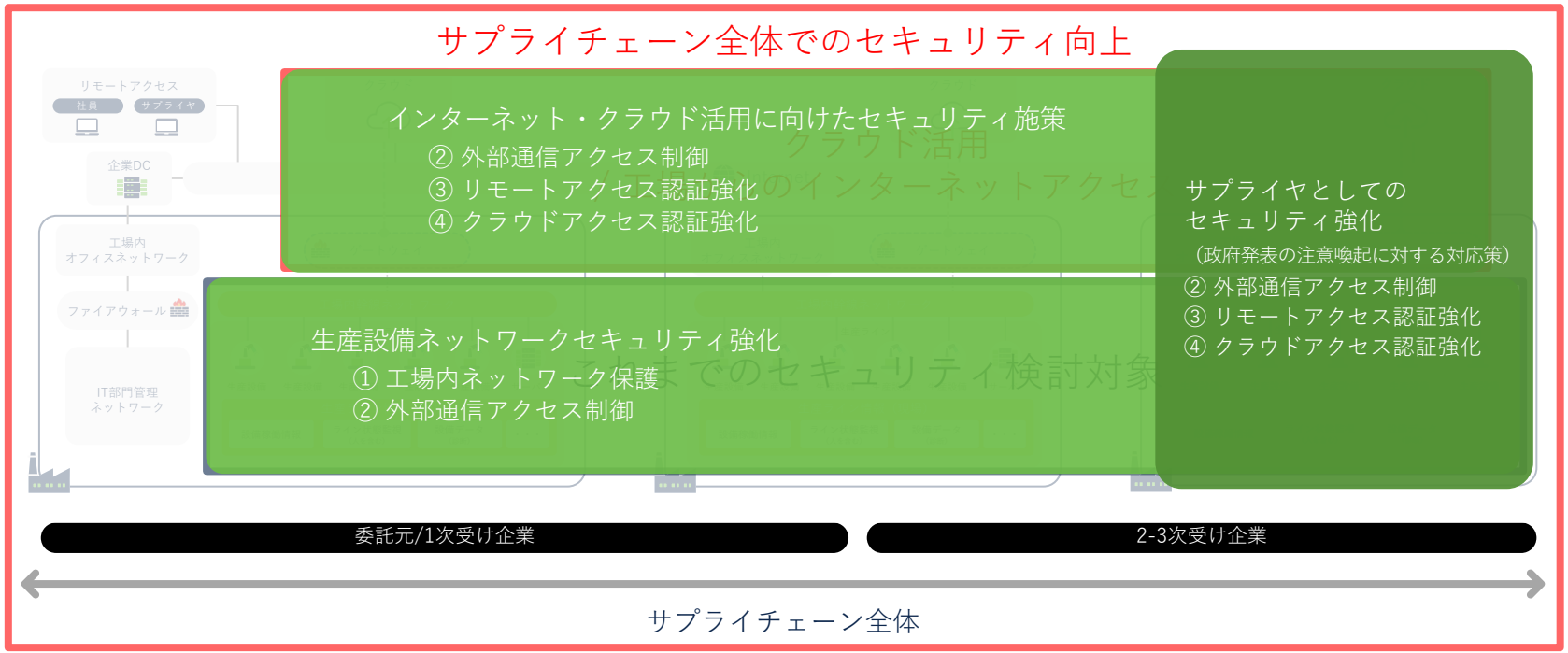
⑤ セキュリティ運用整備

- 監視する内容を決める（⑥の企業として整備されているセキュリティガイドラインがある場合にはその内容を踏まえて検討）
- 監視内容に基づき必要なログ取得、保存方法を決める
- インシデント発生時の対応手段、連絡方法、報告方法を決める

⑥ 企業内情報セキュリティガイドライン遵守

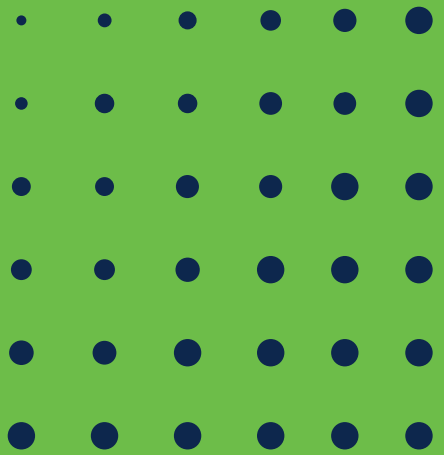
- 情報セキュリティ部門が定めるセキュリティガイドラインを参照し、対応が必要な内容を検討する

Cisco「工場セキュリティ対策ハンドブック」を活用した
製造現場における具体的なセキュリティ検討方法



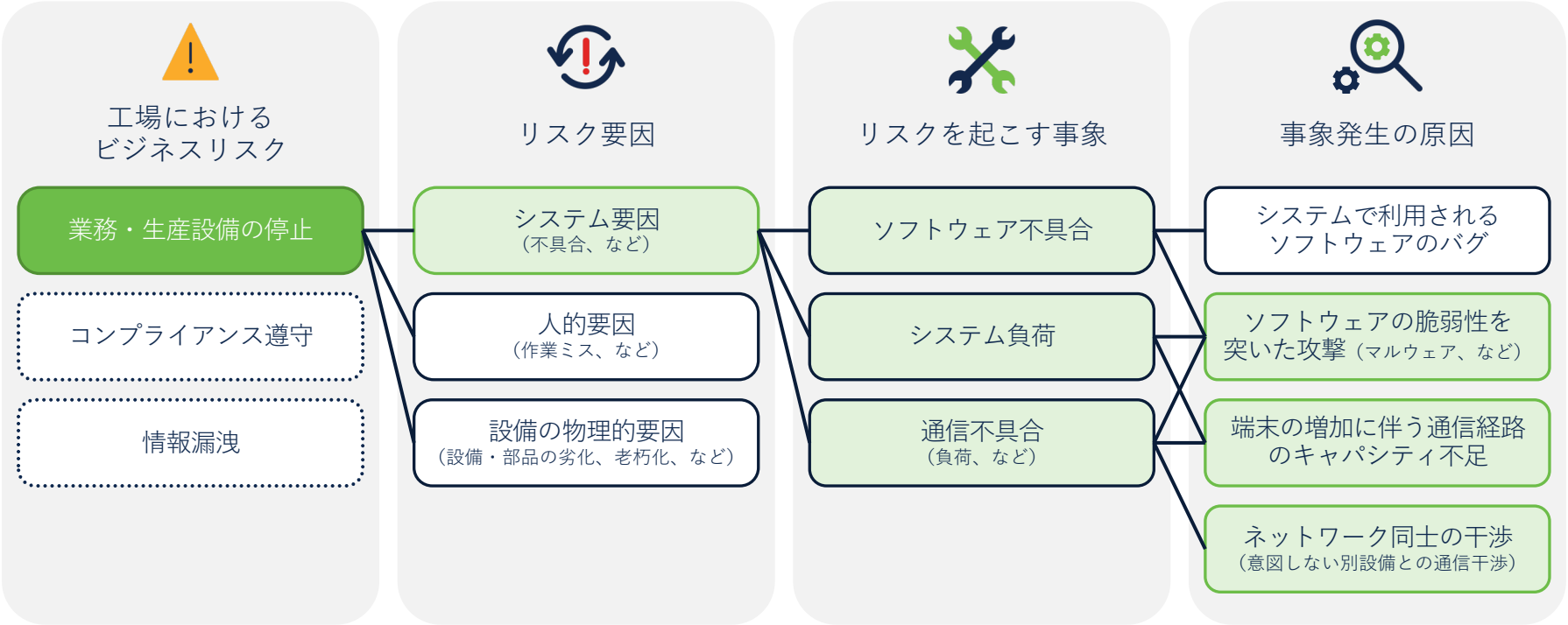
※ご参考：Cisco 「工場セキュリティ対策ハンドブック」
https://www.cisco.com/c/dam/global/ja_jp/products/catalog/pdf/cisco-factory-security-handbook.pdf

生産設備ネットワークセキュリティ強化施策



工場内生産ラインにおけるセキュリティ対策の考え方

工場におけるビジネスリスクとそれを引き起こす事象の関係は以下の通りです。



工場内生産ラインにおけるセキュリティ対策の考え方

生産設備におけるビジネスリスクへのアプローチは、ネットワークを適切に設計、実装することです。

事象発生の原因

- システムで利用されるソフトウェアのバグ
- ソフトウェアの脆弱性を突いた攻撃
- 端末の増加に伴う通信経路のキャパシティ不足
- ネットワーク同士の干渉（意図しない別設備との通信干渉）

事象発生原因のトリガー

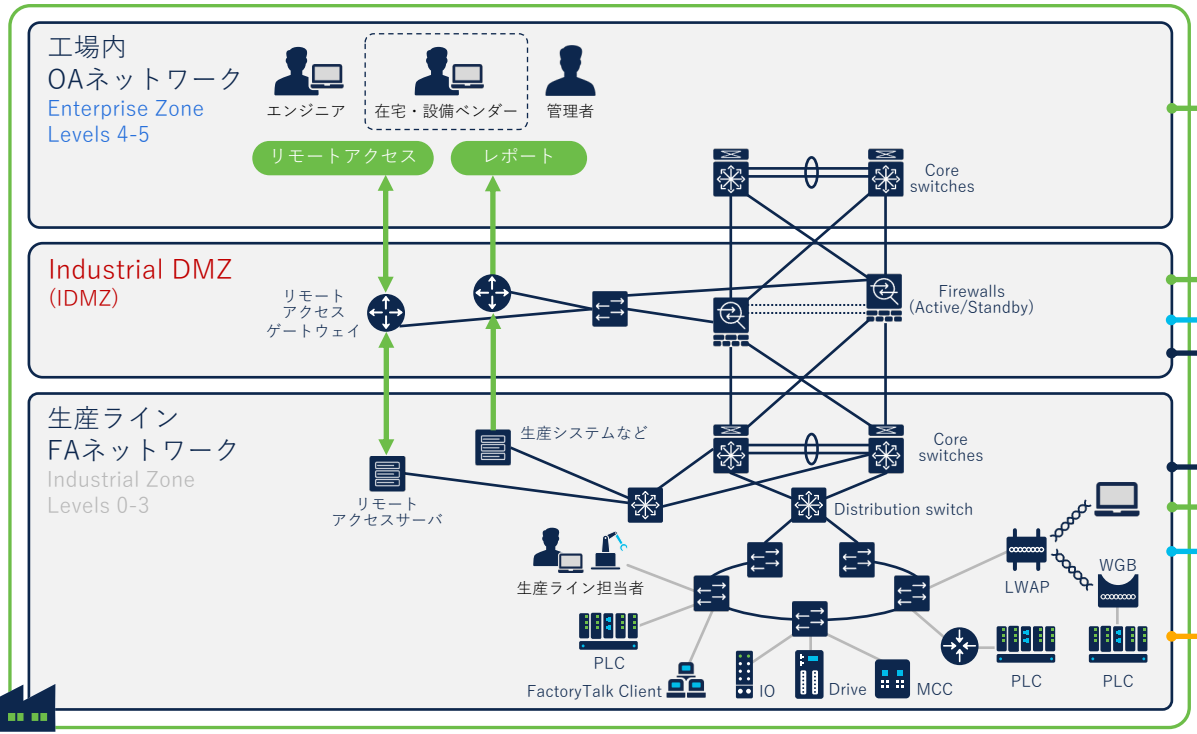
- 古いOSやデバイスの持つ脆弱性を突いた攻撃
- 想定していないデバイス（接続未許可端末）からの通信による影響
- 接続を許されているデバイス（接続許可端末）からの想定外の通信による影響
- 接続されるデバイスの通信特性に合わせたネットワークのキャパシティが不十分
- IPアドレスの割り当てや通信経路、ネットワーク分類（VLANなど）が適切でない

解決のためのアプローチ

- ふるまいの可視化（デバイスの異常なふるまい）
- 適切なネットワーク設計
- 接続デバイスの可視化（資産情報の可視化-脆弱性を含む）

生産設備ネットワークセキュリティ施策概要

【工場内でのセキュリティ対策の適用イメージ】



IT/OT統合SOC

- OT-ITで一貫したセキュリティ監視を行い、セキュリティイベントの内容に基づいた調査と対応を行う
- 調査、対応は、OT、ITの担当領域により役割分担を行う

ふるまい監視

- 通常時の通信の状態をベースラインとして学習する事により、脅威となる外部からの侵入や攻撃を検知する

ネットワークのセグメンテーション

- 資産情報や通信特性をもと必要最低限な通信となるように通信制御を行う

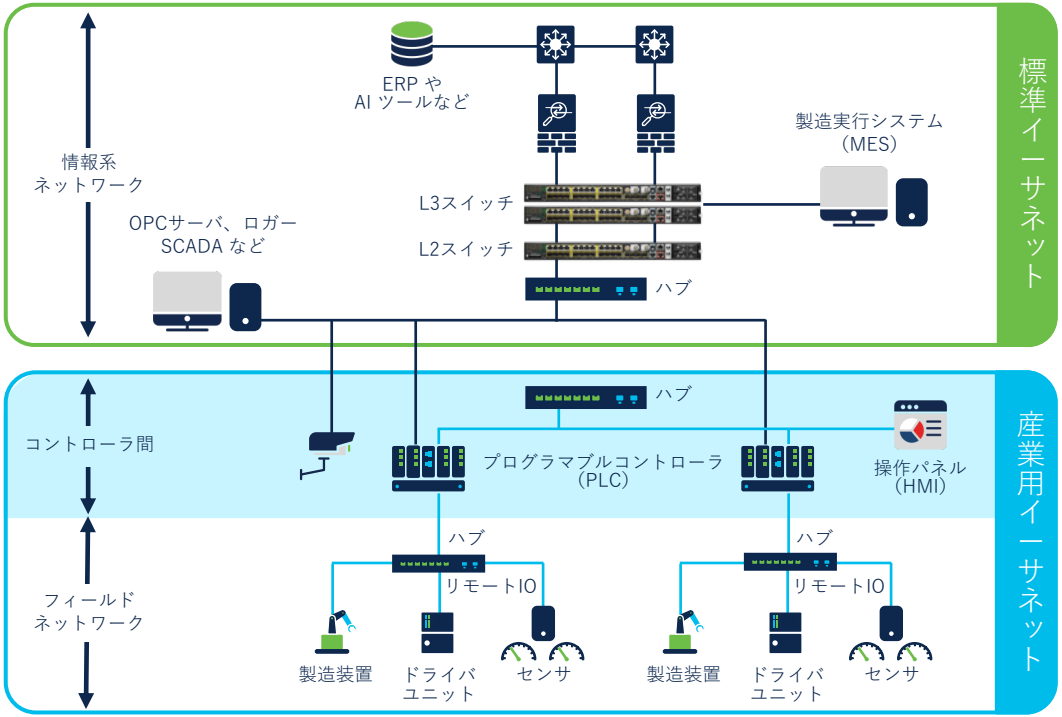
資産の特定

- IoT機器、非管理デバイスなどネットワーク上に繋がる資産（ハード、ソフト）を把握する
- それぞれのデバイスがどの様に繋がり、どう通信しているかを把握する

参考情報

生産設備における要素技術の違いとソリューションの役割

生産設備内の可視化においては、可視化した後にどのような対応が必要であるか？、そのためにどういった情報を可視化する必要があるか？、を考えることが重要です。



Secure Network Analyticsの役割

工場内ネットワークの通信可視化

- ✓ 工場内の通信（標準イーサネット以上）内容の把握
- ✓ 異常な通信発生時の原因調査

セキュリティ監視

- ✓ 異常な通信の検知（ふるまい検知）

CyberVisionの役割

生産設備の可視化

- ✓ IoTデバイス間のコミュニケーションログ(L2)
- ✓ 産業プロトコルの理解
- ✓ ISE側のデバイス情報（資産）の強化

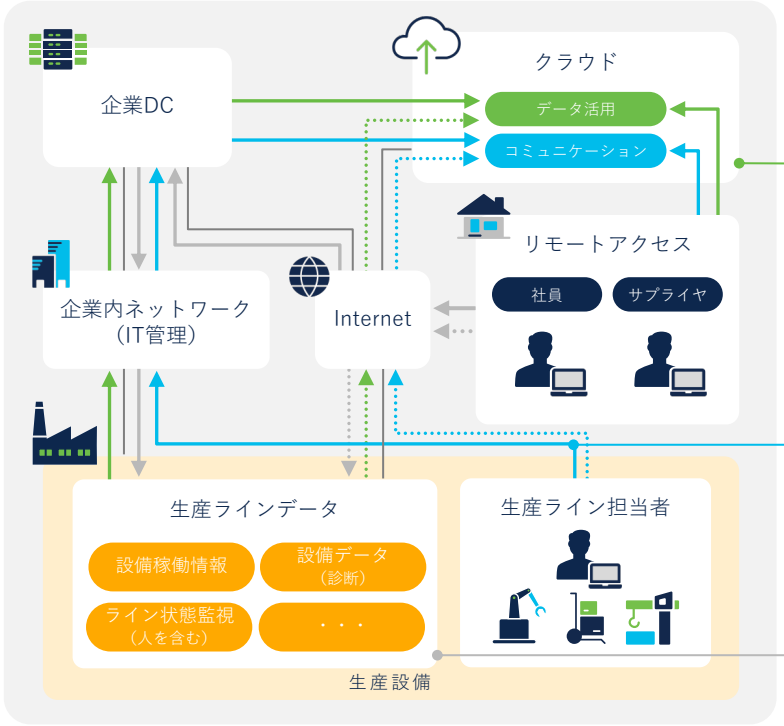
セキュリティ監視

- ✓ IoTデバイスの脆弱性把握
- ✓ コミュニケーションパターンの把握
- ✓ デバイスの状態把握

工場でのインターネット・クラウド活用に向けたセキュリティ施策

生産現場におけるインターネット活用の現状

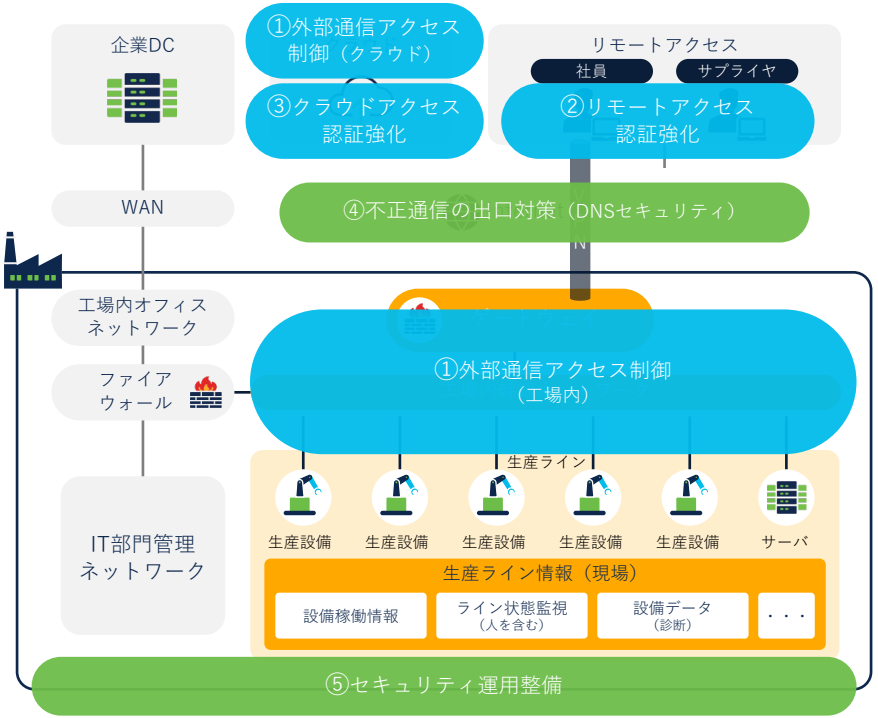
工場のインターネットやクラウドサービスへの接続方法は、企業によって様々なパターンがあります。



	工場内でIT部門と生産部門で個別にインフラを管理している企業のケース（主に大企業）	工場内でIT部門と生産部門の区別なくインフラを管理している企業のケース（主に中堅中小企業）
クラウドの活用に関して	• IT側主導により、企業としてのコミュニケーションツールとして生産現場でも導入が進んでいる • データ活用におけるクラウド利用ニーズは増えている	• 直接インターネットにアクセス出来る環境を用意し、クラウドサービスのやリモートアクセスを活用している
工場とインターネットの境界に関して	• 工場から直接インターネットにアクセスできる環境を、企業として許容するには時間がかかる • 生産現場側が期待するスピード感での対応が難しく、場合によっては工場やライン独自でのインターネット接続環境を用意する場合がある • 社外からのリモートアクセスについても、IT部門で用意される環境では通信帯域や通信速度などの制約がある • 工場独自でインターネット接続環境を用意する場合は、企業の持つセキュリティガイドラインに沿った対応が求められる	• 直接インターネットにアクセスできる環境を用意し、クラウドサービスやリモートアクセスを活用している
工場内のデータ・設備へのアクセスに関して	• OA/FA境界にUTMやFWを導入し制御することで、特定通信を許可し一部リモートアクセス環境を提供 • 一方、各現場で個別にアクセスルートを構築している（セキュリティホールの増加）	• 比較的自由度高く社外から工場内へのアクセスを行っている

インターネット・クラウド活用に向けたセキュリティ施策

侵入防止対策や万が一侵入されたあとの対処、緊急時の対応方法の整備まで、包括的な対策が必要です。



▶ 侵入を防ぐ

① 外部通信アクセス制御（工場内/クラウド）

- 工場内ネットワークデバイスから外部向けの通信プロトコル、宛先の特定（送信元の特定と合わせて）し、不要な通信は通さないように制御を行う
- 不正侵入検知（IDS）・防御（IPS）を導入し、通過する通信に異常がないかを確認する
- IaaS上にデータをアップロードしている場合には、工場内同様にIaaS上でのアクセス制御が必要となる
- 有事の際の調査や報告のために通信ログを保存する

② リモートアクセス認証強化

- 社内ネットワークや、サーバ・データへのアクセスの際に、接続する相手を認証する
- ユーザー認証の際には多要素認証（MFA）を導入する
- 有事の際の調査や報告のために通信ログを保存する

③ クラウドアクセス認証強化

- ②同様にクラウド側を利用する際の認証も強化と通信ログの保存を行う

▶ 侵入された後の本格的な攻撃を防ぐ

④ 不正通信の出口対策（DNSセキュリティ）

- 外部からの侵入が成功しマルウェアが動作した際に、外部からの攻撃やデータ採取を行う前の通信先（C&Cサイト）を特定し、通信を止める

* C&Cは動的に変わるため、①の特定通信の制御だけでなく、リアルタイムな分析に基づき常に最新の情報により制御を行う仕組みが必要

- 有事の際の調査や報告のために通信ログを保存する

▶ 平常時、有事の対応を明確にする

⑤ セキュリティ運用整備

- 有事の際の対応方法をルール化、プロセス化をする
- 必要に応じて企業として整備されている情報セキュリティガイドラインを参照し、IT部門や情報セキュリティ部門と連携を行う

今できる工場サプライチェーン セキュリティ対策

セキュリテイ施策と検討課題に対するアプローチ

政府発表の注意喚起に基づいた対策を全て実施するのは難しいため、優先度や投資対効果の高い施策の選定が必要です。

注意喚起に含まれる施策	施策に必要な要素
本人認証の強化	MFA（多要素認証）
IoT機器を含む情報資産の 保有状況を把握	資産可視化
情報資産の脆弱性対応	脆弱性管理
フィッシングメール対策	メールセキュリティ
サーバ等における各種ログ確認	SIEM/MSS
通信の監視・分析/アクセス コントロールの再点検	適切なネットワーク設計/ インターネット境界セキュリティ/ ネットワークとセキュリティの監視（MSS）
データバック実施と復旧手順の確認	データバックアップ/ データセキュリティ
インシデント対応のための体制や プロセス、対処手順の整備	SOC・CSRT立ち上げ/ インシデント対応手順作成

導入コスト

IT部門と生産部門における責任分界点

検討・運用を行う
人材の不足

ガバナンス範囲と
施策実施の実現方法

誰がどこまで
実施するのか？

委託先/仕入れ先
にとっての課題

委託元
にとっての課題

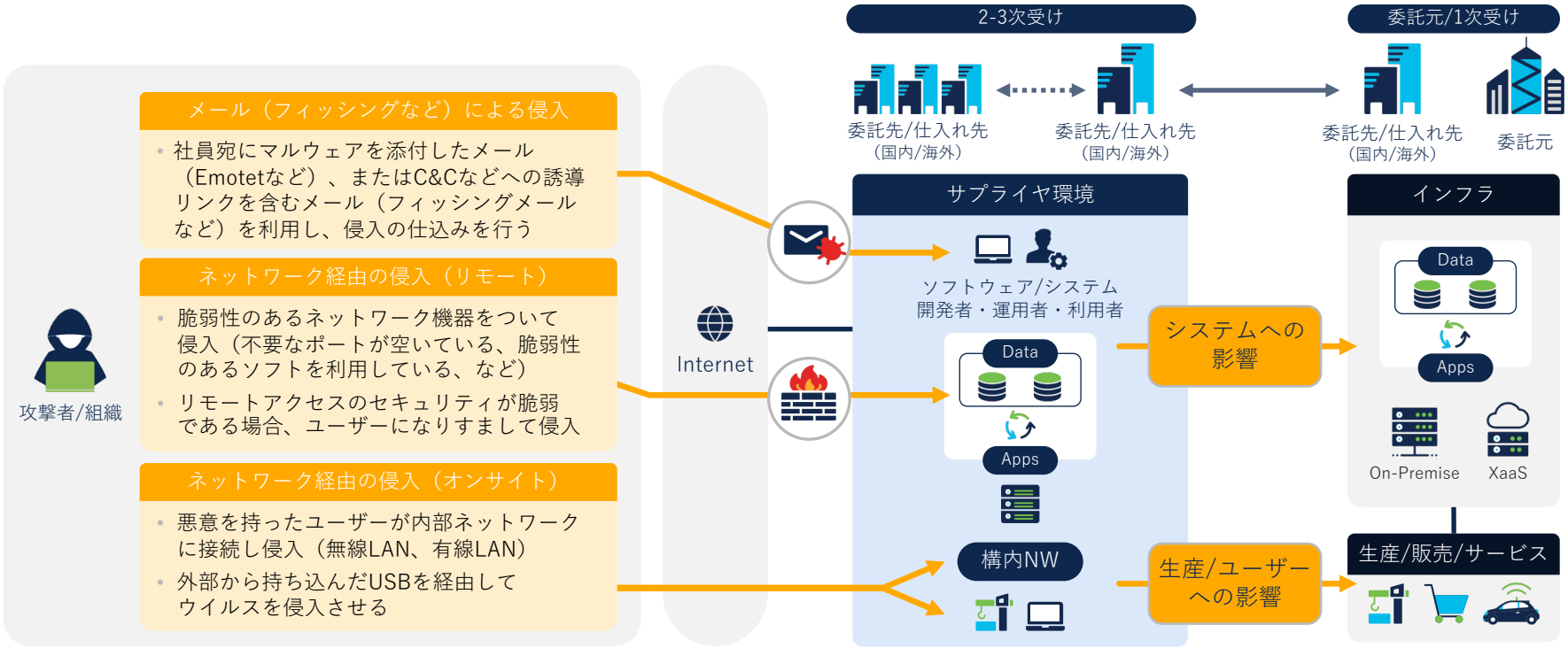
全ての施策を実施するのは、ヒト・モノ・カネの観点からも現実的には難しい。

▶ 解決のためのアプローチ

- ✓ 投資金額を抑えながら、より投資効果の高い施策をまずは実施
- ✓ 投資効果を事前に確認することでリスク回避

サプライチェーン攻撃はどこから来るのか？

サプライチェーン攻撃でも、フィッシングメールやネットワークなど複数の侵入経路があります。



政府発表の注意喚起における考慮点

製造業観点での解釈

▶ 検討範囲

- サプライチェーン全体を俯瞰し、発生するリスクを自身でコントロール出来るよう適切なセキュリティ対策を実施する
- 国外拠点についても、国内の重要システム等へのサイバー攻撃の足掛かりになることを考慮し、国内のシステム等と同様に支援・指示などによりセキュリティ対策を実施する

▶▶▶

- サプライチェーン全体でのガバナンス強化
- ガイドから実施へ

▶ 対応策

リスク低減のための措置

- 本人認証の強化（パスフレーズ強化、アカウント・権限整理、多要素認証）
- IoT機器を含む情報資産の保有状況を把握と脆弱性対応
- フィッシングメール対策

インシデントの早期検知

- サーバ等における各種ログ確認
- 通信の監視・分析やアクセスコントロールの再点検

インシデント発生時の適切な対処・回復

- データ損失などに備えたデータバック実施と復旧手順の確認
- インシデント発生時の対応のための体制やプロセス、対処手順の整備

生産設備ネットワークに関連するセキュリティ対策

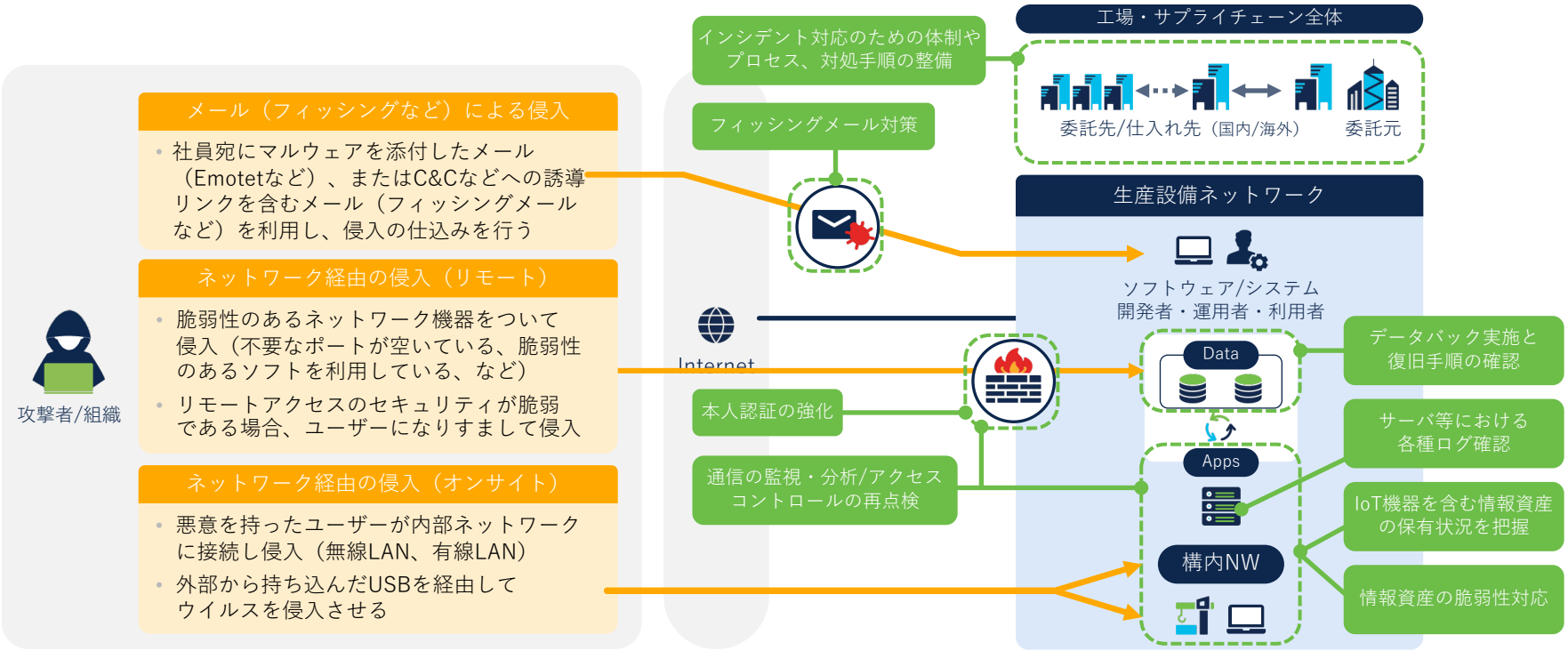
▶▶▶

- 情報資産の管理強化
- インフラにおけるセキュリティ対策強化
- セキュリティ運用の強化

▶▶▶ 生産設備ネットワークにおいてもセキュリティ施策を実施することが求められている

政府からの注意喚起における考慮点

政府からの注意喚起に基づいた対策イメージです。




cisco
SECURE

参考情報

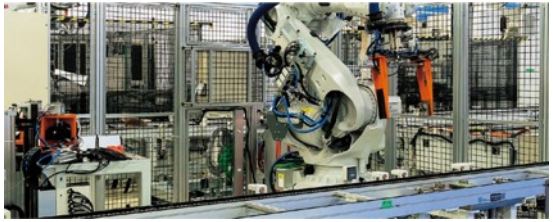
顧客事例

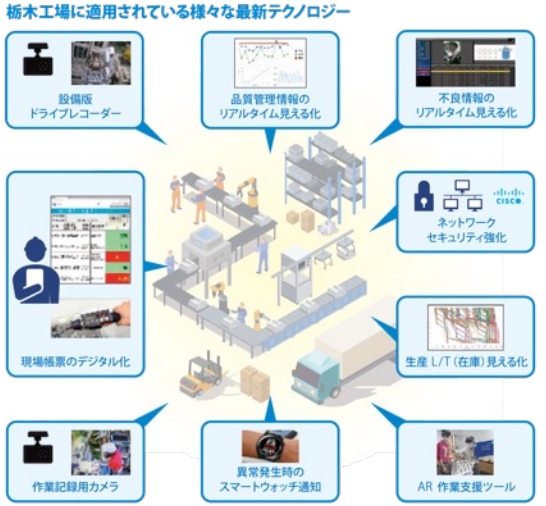
日産自動車株式会社

「生産技術のインテリジェント化」を目指し最新技術を採用したIoTネットワークを構築

「クルマの未来」を提案し続ける日産自動車。同社は、新型クロスオーバーEV「日産 アリア」の生産ラインで、IoTを活用した生産技術革新に取り組んでいます。シスコのネットワーク製品による制御で、ITとOT（生産技術）を融合。「ニッサン インテリジェント ファクトリー」の先駆け的取り組みとして期待されています。

課題	ソリューション	結果～今後
• 労働集約型の生産を脱却しつつ“匠”の技術を継承するため、**ロボットやIoTを活用した生産技術のインテリジェント化が重要に** • 様々な機器やデジタル技術を工場に導入する際は、それらの**稼働を見える化し、適切に管理・制御する仕組みが不可欠** • 生産ラインはビジネスの生命線であり、稼働を支えるIoTネットワークにも、**高い安定性・信頼性・拡張性**が求められる	• **製造業界向けの多彩な製品ポートフォリオとグローバルの実績で培った技術力**を評価 • 産業用イーサネットスイッチのCisco IEシリーズをベースに、**生産系と情報系を連携した統合ネットワークを構築** • Cisco Industrial Network Director（IND）とCisco Identity Services Engine（ISE）を活用した**IoTネットワーク接続デバイスのセキュリティ管理を実現**	• 正式稼働に向け、新ネットワークを活用した**e-パワートレイン自動生産ラインの立ち上げ作業が進行中** • 新ネットワークは生産ラインのテスト段階から活用し、**品質課題や設備稼働ロスなどの洗い出し・改善**を進めている • 情報系ネットワークとの連携メリットを活かしたリモートコミュニケーションを実施。**コロナ禍でも現場業務を継続** • 栃木工場で実現した**ネットワークデザインを標準化し、統一されたポリシーをグローバルに展開**していく





Why Cisco?

“最新のデジタル技術をキャッチアップして生産技術をインテリジェント化していく。これが次世代のクルマづくりのカギになっています。この活動を推進する上で、ネットワークは極めて重要な役割を担います”

— 日産自動車株式会社 パワートレイン技術企画部 主管　村井 勇一氏

詳細はこちら►►► https://www.cisco.com/c/ja_jp/about/case-studies-customer-success-stories/2171-nissan.html

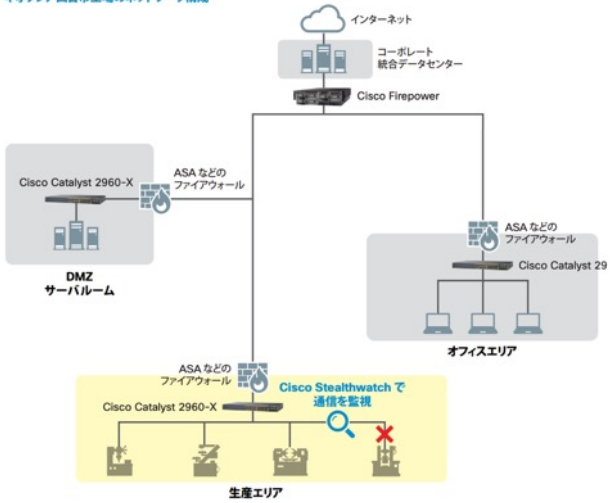
キオクシア株式会社

工場の生産活動を守るための新セキュリティネットワークが脅威を検知して早期に対処

キオクシアは生産設備を守るため、シスコのセキュリティソリューションを導入しました。ネットワーク可視化をベースとするソリューションで、仮に脅威が侵入してもネットワークが検知し、早期対処が可能。エンドポイントの対策が困難という生産エリアの課題を解決しました。

課題	ソリューション	結果～今後
• 工場の操業停止は大きな損失につながる	• ネットワークそのものが脅威を検知、駆除する仕組みを実装	• 仮に脅威が生産エリアに侵入しても早期に発見し、迅速に対処できる体制が整った
• 生産エリアのセキュリティを強化したい 生産設備はウイルス対策ソフトが実装できないケースがあり防御が困難	• 暗号化通信もそのまま可視化、分析が可能	• キャパシティプランニングの簡素化とTCO 削減を実現
• 生産エリアのネットワーク刷新は大規模になるが、できるだけコストを抑えたい	• 製品の購入方法として一定期間定額で柔軟な機器の追加が可能な Cisco Security ELA を選択	• ネットワークトラフィックの可視化がネットワークの全体最適化にも役立つ • スマートファクトリーなど、工場の進化を支える最適なネットワークを整備できた

キオクシア四日市工場のネットワーク構成



Why Cisco?

“生産設備はPCなどとは異なり、エンドポイントでセキュリティ対策を行えないケースがある。生産ラインを止めることが許されない工場にとって、シスコのネットワークセキュリティソリューションは最適な仕組みだと感じています”

—キオクシアホールディングス株式会社 情報セキュリティ統括責任者　川端 利明氏

詳細はこちら ▶▶▶ https://www.cisco.com/c/ja_jp/about/case-studies-customer-success-stories/2176-kioxia.html

株式会社 日立ハイテク

ものづくり中核拠点のネットワークを全面刷新　自由かつ安全なDX推進基盤として大きな期待

ハイテク製品と高付加価値ソリューションを提供する日立ハイテク。同社は、製造の中核拠点のネットワークをシスコのSDNソリューションで刷新しました。運用面、安全性の課題を解消し、デジタルトランスフォーメーションを推進するための重要な基盤と位置付けられています。

課題

- 既存ネットワークの老朽化で障害発生のリスクが増大
- 物理的な制約が多く、機器の移動に伴う設定変更などの負担が大きい
- 生産設備と情報システムの連携などを進めるに当たりセキュリティ面の不安がある

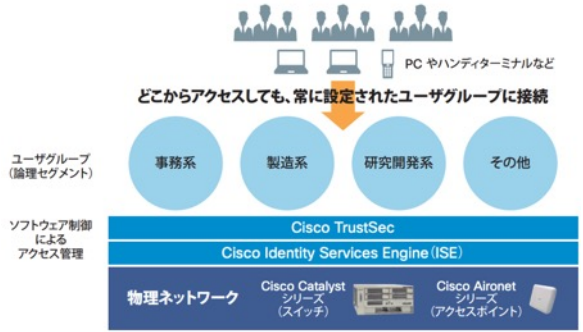
ソリューション

- 世界標準の技術と評価してシスコのSDNソリューションを採用
- IPアドレスやVLANに依存しないアクセス管理を実現
- 有線、無線を問わずネットワーク管理の一元化と可視化を実現

結果～今後

- どのポートに接続しても、自身のユーザグループに自動接続。どこでも仕事をできるようになり、生産設備の移動も容易に
- アクセスポイントの集中制御と電波の可視化で、無線LANのトラブル対応が迅速化
- マルウェアに感染したデバイスをソフトウェア上で隔離できる
- ネットワークの自由度と安全性が高まりDXを推進する環境が整った

新しく導入したアクセス管理の仕組み



Why Cisco?

“どのポートに接続しても、適切なネットワークに接続されるため、場所の制約がなくなりました。パソコンを持ち歩けば、どこにいても仕事ができるようになっています”

—株式会社 日立ハイテクノロジーズ デジタル推進本部 モノづくりDX部 部長　山口 浩二氏

詳細はこちら►►► https://www.cisco.com/c/ja_jp/about/case-studies-customer-success-stories/2124-hitachi-hightech.html

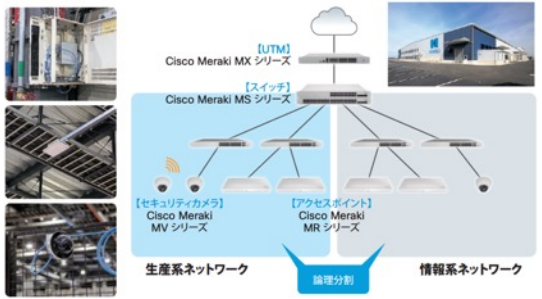
金剛株式会社

工場のスマート化を支える新ネットワーク　高い運用管理性で現場のチャレンジを促す

収納設備メーカーとして知られる金剛。同社は、新たに稼働を開始した新工場において、IT やデータを積極活用したスマートファクトリーの実現を目指しています。そのインフラとして採用したのがシスコのクラウド管理型ネットワークソリューション「Cisco Meraki シリーズ」です。無線LAN やカメラ映像を駆使した稼働情報の収集、監視などにチャレンジし、すでに様々な成果につなげています。

課題	ソリューション	結果～今後
• 多様化する市場ニーズに対応するには、多品種少量生産の実現、生産性の向上が必要 • 変革のために IT やデータを活用した「スマートファクトリー」を目指す • スマート化を支えるネットワークには、信頼性、安定性、管理性、柔軟性など高度な要件が求められる	• 工場のスマート化を支える新ネットワークを Cisco Meraki シリーズで構築 • セキュリティアプライアンスからアクセスポイント、セキュリティカメラまで Cisco Meraki シリーズで統一。ネットワークの統合管理を実現	• スマートフォンで稼働状況を確認、設備トラブルの原因究明に映像を役立てる • 独自アプリケーションを開発するなど、現場のチャレンジが活発化 • 蓄積したデータを分析することで、時間当たりの生産性を 30% 程度向上する見込み

図 金剛のネットワーク構成



新ネットワークを活用して様々な仕組みを構築

監視用のアプリケーションを独自に開発　　稼働情報を事務所内のモニターで確認

Why Cisco?

“これからのものづくりは IT やデータの活用が生命線になる。ネットワークはそのための欠かせないインフラ。Cisco Meraki シリーズにより、新たなチャレンジに向けた環境が整いました”

― 金剛株式会社 代表取締役社長　田中 稔彦氏

詳細はこちら►►► https://www.cisco.com/c/ja_jp/about/case-studies-customer-success-stories/1620-kongo.html