CISCO
SECURE

製造業サプライチェーン向け

工場セキュリティ対策ハンドブック

近年の製造現場では、これまで以上にデジタル化の取り組みが進み始めています。

コロナ禍の影響や、SDGs/ESGの流れを受けた市場の変化により、作るモノや作り方、モノと繋がるサービスの在り方も変化し続けています。この様な環境の中で、製造現場におけるデジタル化は必然となっています。

一方、製造現場のデジタル化は、生産ラインからの得られた情報(データ)を活用することで実現されますが、そのためには様々なデバイスやシステム、人を繋げる必要があります。この状況は、新たなセキュリテリスクを生むことになり、近年工場やサプライチェーンを狙ったサイバー攻撃が増加しています。

デジタル化を進めるには、データの流通を高めるためのデジタルインフラ整備と合わせて、セキュリティ対策を行うことが求められています。

本資料は、現在の製造現場(工場)に求められるデジタルインフラとそのセキュリティ対策について、実装方法の考え方を示すハンドブックとなります。

Contents

製造現場のデジタル化

製造現場のデジタル化は、生産ラインから得られる情報（データ）をインフラ内に流通させ、活用することに他なりません。

データを活用するためのアプリケーションとして、機械学習や、AI、デジタルツインの試行も進み始め、製造現場に単なる IT 技術を導入するだけでなく、データ活用の幅（利用する場所や人）も広がりを持ち始めています。

これら製造現場でのデジタル化を実現するには、データを流通させるためのインフラ“デジタルインフラ”の整備が重要となります。製造現場の様々なデバイスから得られたデータをアプリケーションに送るために、ネットワークに繋がるようになり、集まった膨大なデータを処理するためのコンピューティングリソースは、より多く必要となっています。

製造現場で扱われるデータ量が増加する中で、必要なデータを必要な場所に確実に送り届けるための、高速かつ安定したネットワークは欠かせません。

COVID-19 以降の生産管理における変化

製造現場の環境の在り方を見直す大きなきっかけとして、2019 年に発生した COVID-19 が挙げられます。COVID-19の影響による移動制限を受けて、従来からの「現地現物現実」での対応が困難となったことから、生産ライン立上げから量産の全体工程を通じて、リモート対応やクラウド活用の必要性が高まりました。この流れは、これまで部分的であった工場でのインターネット利用を再検討する契機となったと言えます。

従来よりニーズのあったリモートメンテナンスだけでなく、工場デジタル化の基盤としてのクラウド活用の検討が進みました。

工場におけるクラウド活用検討の動きのまとめ

- **製造現場のデジタル化を進める過程で必要な施策であったが、COVID-19の影響により対応が加速**
- **現在のリモートアクセス環境は様々な制約から限定的であり、「現地現物現実」をリモート環境で実現することが望まれている**
  - 工場外の専門家や設備ベンダーの支援をリモート化
  - 海外工場支援のリモート化
- **製造現場デジタル化に伴うデータ活用は、リモート化の影響も受けてクラウドを利用するニーズが増加**

製造業を狙ったサイバー攻撃の増加

製造現場でのデジタル化や、クラウドの活用が進む中、ここ数年で製造業を狙った攻撃は増加し、生産ラインの停止やサプライチェーン全体への影響など、被害が拡大しています。

これは、セキュリティ対策が不十分なままで製造現場のデジタル化が進んでいることが一つの要因と考えられます。攻撃者から見ると、セキュリティ対策が十分で無い製造現場は、その影響度からも魅力のある攻撃対象と言えるでしょう。既に大きな影響を与えた WannaCry、SolarWinds などは、生産設備や生産管理システムを狙った攻撃です。それ以外にも、デジタル化により様々な設備が繋がる環境では、これまで企業インフラ内で起きていたサイバー攻撃が工場インフラ側でも発生してしまうリスクがあります。

代表的なセキュリティインシデント

フィッシングメールによる標的型攻撃の継続（Emotet、など）

- **対象：個人、ビジネスに関連するデータなど**
- **影響：フィッシングメールを介してマルウェアを仕掛け、ランサムなどの起点となる**
  - 販売店における信頼性低下からの顧客離れ
  - 解析、調査、対処のための膨大な工数
  - ランサムウェアによる大規模被害（WannaCry、など）
  - 対象：オフィスだけでなく生産設備のデバイス
  - 影響：ビジネス活動に大きく影響
  - グローバルでの生産設備の停止
  - オフィス機能の停止
  - 一部顧客サービスの停止

ソフトウェアのアップデートを利用した大規模被害（SolarWinds、など）

- **対象：秘匿性の高いユーザー情報、データなど**
- **影響：ビジネス活動に大きく影響**
  - 不確定な情報漏洩による潜在的なビジネスリスク
  - 復旧、影響調査のための膨大な工数

これからの製造現場のデジタル化（データ利活用）においては、セキュリティ対策は必要不可欠になっています。

製造業へのサイバー攻撃の増加に対する日本政府の動き

製造業へのサイバー攻撃が増加している状況を受け、日本政府の各省庁では工場領域におけるセキュリティ検討を促進するための動きがあります。特に、2022 年には以下 3 つの主要な発表がありました。各省庁が発表した内容は、それぞれの目的や狙いに違いはありますが、いずれの発表もより具体的な施策の実装を促す内容となっています。

- **2022 年 3 月 1 日**

経済産業省 / 金融庁 / 総務省 / 厚生労働省 / 国土交通省 / 警察庁 / NICT 各省庁 7 組織連名で現在の情勢におけるサイバーセキュリティ注意喚起を発表（https://www.meti.go.jp/press/2021/03/20220301007/20220301007-1.pdf）

- 企業規模、国内外を問わず、サプライチェーンのサイバーセキュリティ対策強化を促すための注意喚起
- 主要な実施施策を明示し、対策の実施を呼びかけ

- **2022 年 3 月 31 日**

日本自動車工業会（JAMA）、日本自動車部品工業会（JAPIA）は、共同でセキュリティガイドライン（ 対策項目、基準 ）の更なるレベルアップ項目を追加したセキュリティガイドライン（v2.0）を 2022 年 3 月 31 日に改訂（https://www.jama.or.jp/operation/it/cyb_sec/docs/cyb_sec_guideline_V02_00.pdf）

- 自動車業界におけるサプライチェーン全体でのセキュリティ向上を目的としたセキュリティ対策のガイドラインの改訂
- 工場領域は含まれていないものの、自動車業界の各企業が企業
- （OA 環境）の目指すセキュリティレベルと具体的な内容を記載

- **2022 年 11 月 16 日**

経済産業省は、「工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン Ver 1.0」を策定（https://www.meti.go.jp/policy/netsecurity/wg1/factorysystems_guideline.html）

- 業界を問わず、工場領域での業務を意識し、工場全体でのセキュリティ対策をどのように実施するかを記載
- セキュリティ対策の自己評価を行うためのチェックリストも整備

セキュリティ注意喚起の内容とサプライチェーン全体像

政府の注意喚起の中では、概要レベルではありますが、工場を持つ企業にとって企業インフラ（OA）と工場インフラ（FA）の全体で必要となる対策のポイントがまとめられています。

重要なのは、単一の施策で昨今のサイバー攻撃を防ぐのは難しいという事実と、セキュリティに絶対はない（100%防げる手段は存在しない）という事実を踏まえて、全体的な施策の検討と合わせて、有事の際の対応手順を整備しておく必要があるということです。

また、それらの対応を委託元だけでなく、委託先を含むサプライチェーン全体で取り組む必要があるという点も重要なポイントとなります。

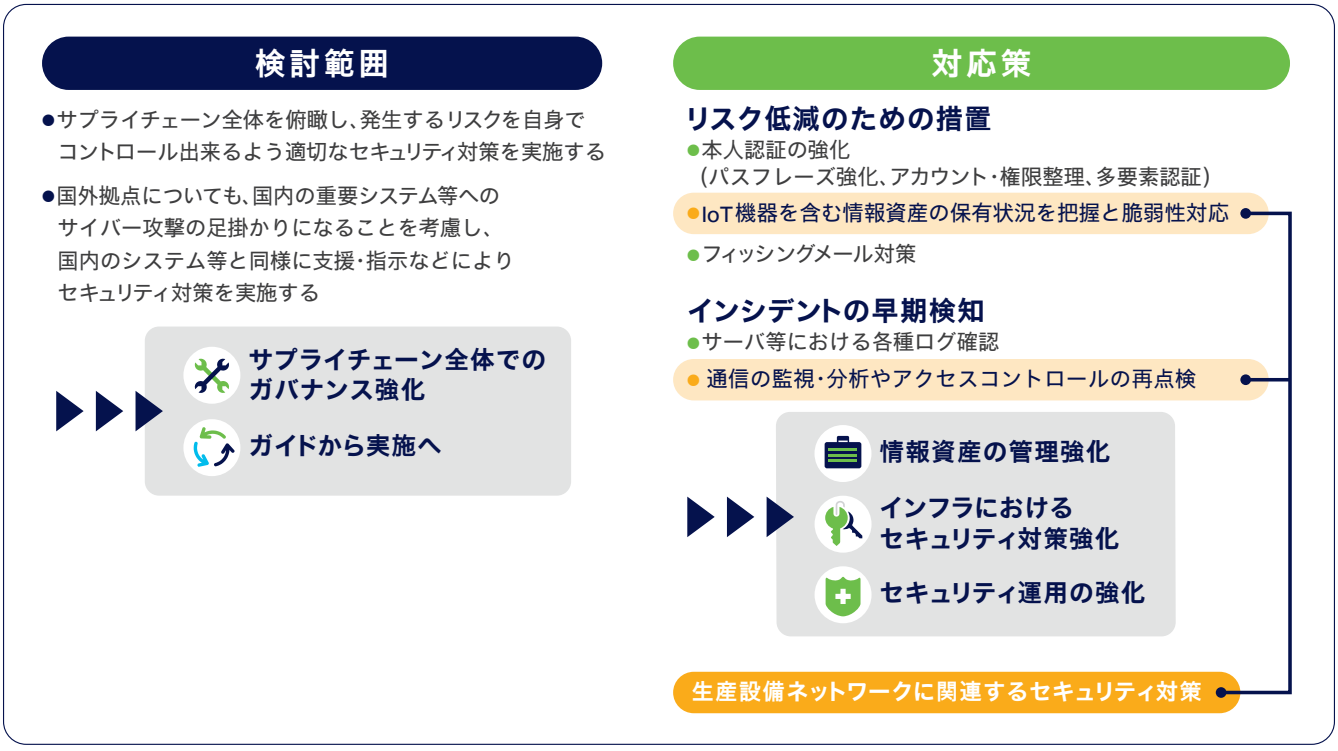
一方で、工場のデジタル化は、企業規模や各社の取組み速度の差異により、進捗状況は同じではありません。デジタル化の進捗により想定されるリスクは異なり、必要となる対策も異なります。実際のセキュリティインシデント事例を見ると、サプライチェーンを狙った攻撃は、必ずしもネシステム的に繋がったことによる影響だけではありません。

委託先の独自システムが攻撃されその工場の生産が止まることで、部品の供給が滞り、サプライチェーン全体に影響が出る場合があります。

そして、サプライチェーン全体を見た場合、セキュリティ対策に投資出来る予算や、セキュリティ対策の検討を推進出来る人材にも違いがあります。

セキュリティ対策が重要となっている昨今ですが、必要な対策全てを行うことは現実的に難しい状況です。大事なことは、自社のデジタル化において、リスクがどこにあるかを見極め、必要な投資を適正に行うことです。

政府発表の注意喚起における考慮点まとめ



工場セキュリティ施策検討のポイント

工場の中でセキュリティ対策を考えるには、攻撃者がどのように攻撃を行うかを理解し、自社の工場のどこにリスクがあるのかを見極める必要があります。また、企業のデジタル化の進捗や求められるインフラ環境によって、必要なセキュリティ施策は異なります。ここでは、工場内のセキュリティを考える上でのポイントについて説明します。

工場におけるサイバー攻撃の概要

製造現場に対するサイバー攻撃はどのように行われるでしょうか?

基本的な考え方として、オフィスエリアネットワークに対して行われるものと同じく、外から中に侵入してくる、侵入後に向上内部のネットワークを偵察しながら拡大（拡散）させ、最終的な侵害を行うと言う流れになります。

攻撃の各段階での特徴は、以下になります。

外からの侵入

- メールによる標的型攻撃
- 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

ネットワーク経由の攻撃

- 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

侵入後の拡大

- ラテラルムーヴメント
- 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
- ネットワーク内の横の動きにより、マルウェアを拡散させる

侵害

- C&C サーバへの接続
- 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
- 入手したデータを外部に持ち出す

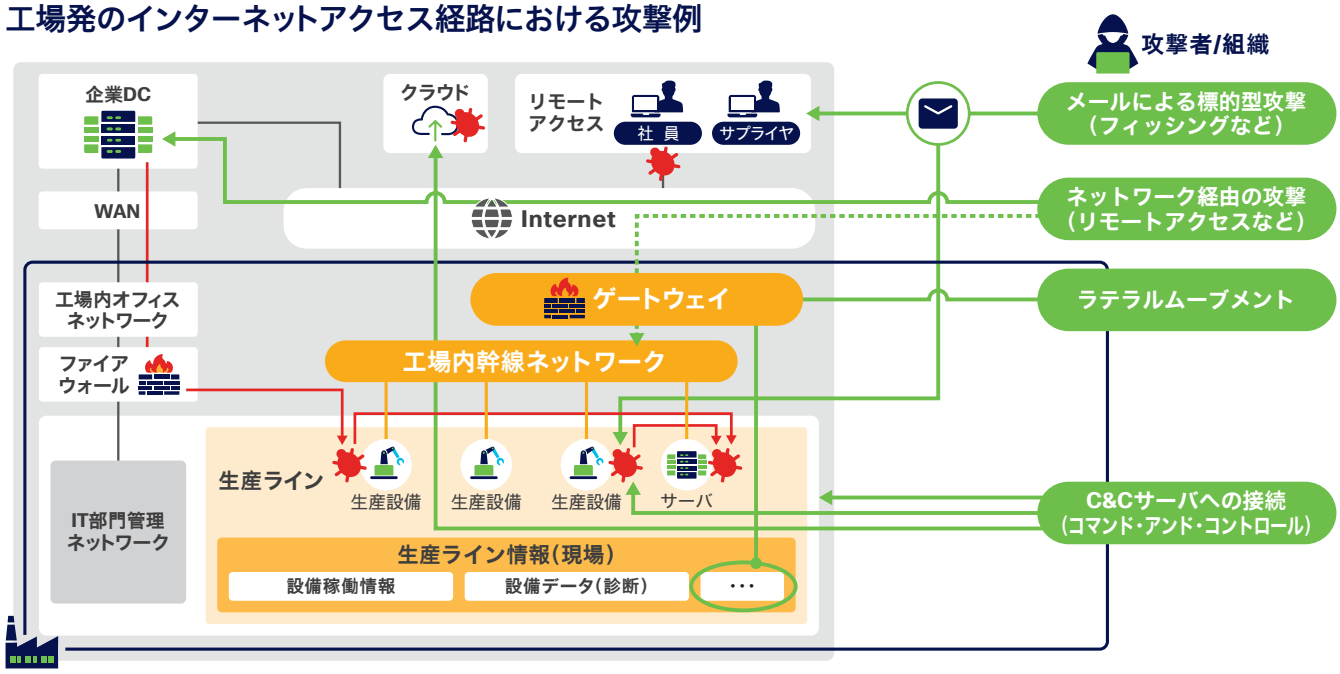
製造現場に対して行われるサイバー攻撃のアプローチは、前述の通り、オフィスエリア対して行われるものと同様なため、IT 部門の持つ考え方や知見を取り入れることは有用であると言えます。

ただし、工場内には、生産設備に代表される製造現場特有のデジタル資産（センサー、制御装置、など）がかず多く存在します。これらのデバイスに対するセキュリティの考え方や対策については、製造現場での知識が不可欠です。

また、会社全体で見た場合には、IT 部門の管理するネットワークと OT 側で管理するネットワークが繋がることも多いため、製造現場でのセキュリティ対策は、IT 側での知見と、OT 側の知識を合わせて考えていく必要があります。

そして、サイバー攻撃への対策を考える上で最も重要なことは、絶対的に全てを防ぐ防御方法は無いことを認識することが重要です。攻撃から守る “防御” 対策を考える一方で、侵入・侵害されることを前提とした “検知” や、その後の対応方法の取り決めなどの “運用” を考えることも重要です。

工場発のインターネットアクセス経路における攻撃例



現在のサイバーセキュリティ対策とこれから

ここで、COVID-19 前後で実施された一般的なセキュリティ対策と、今後必要と考えられるセキュリティ対策について、リモートアクセス環境を例に見てみましょう。

デジタル化に取り組む多くの製造業のお客様では、工場から直接的にインターネットに接続する環境を持っていないのが現状です。この状況は、大規模な製造業のお客様で見られる傾向で、工場側でのセキュリティ対策の実装が進んでいない環境において多く見られます。（セキュリティ対策が不十分な環境において工場で独自のインターネットを持つ場合、いわゆるシャドーIT と呼ばれ、企業としての IT 運用からは外れた状況となり、リスクが高い状況となります）

一般的に工場内のシステムへ外部からアクセスするには、IT 側の用意するリモートアクセスの仕組みを利用しています。COVID-19 以降、リモートアクセス利用は増加傾向にあり、新たな問題も出始めています。また、今後デジタル化が進む中では、リモートアクセスの在り方も変化しつつあります。

リモートアクセスの現状

- OA/FA の境界に UTM（または FW）を設置し、限定的な通信のみを許可することでセキュリティを担保
- リモート接続ルール（方式）が決まっていないため、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
- ネットワークへの接続設備管理ができていないため、誰でも接続し利用が可能 -> セキュリティ事故時に原因の解析不可

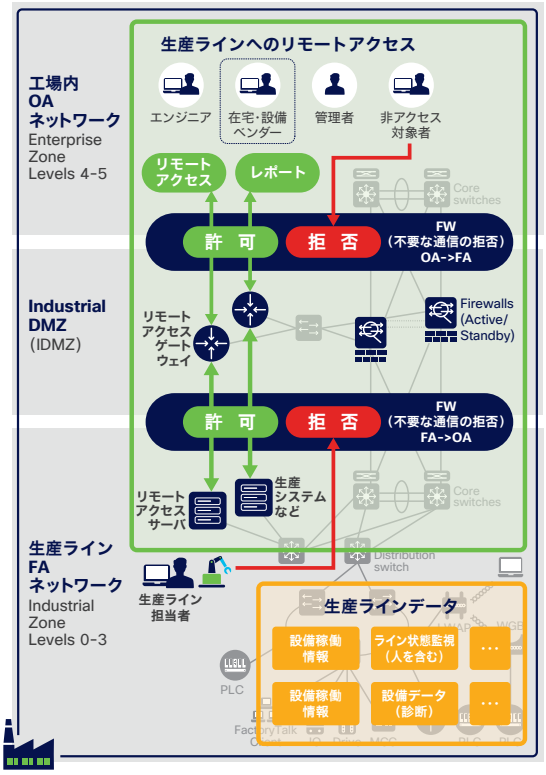
リモートアクセスの今後

- IT/OT のネットワーク信頼性を高めた上で相互接続し、利用形態に合わせリモート接続方式を共通化して提供
- 情報の精度向上・高詳細化のため、より多くのデバイスが繋がり、リモート化を進めることでアクセス方法が多様化

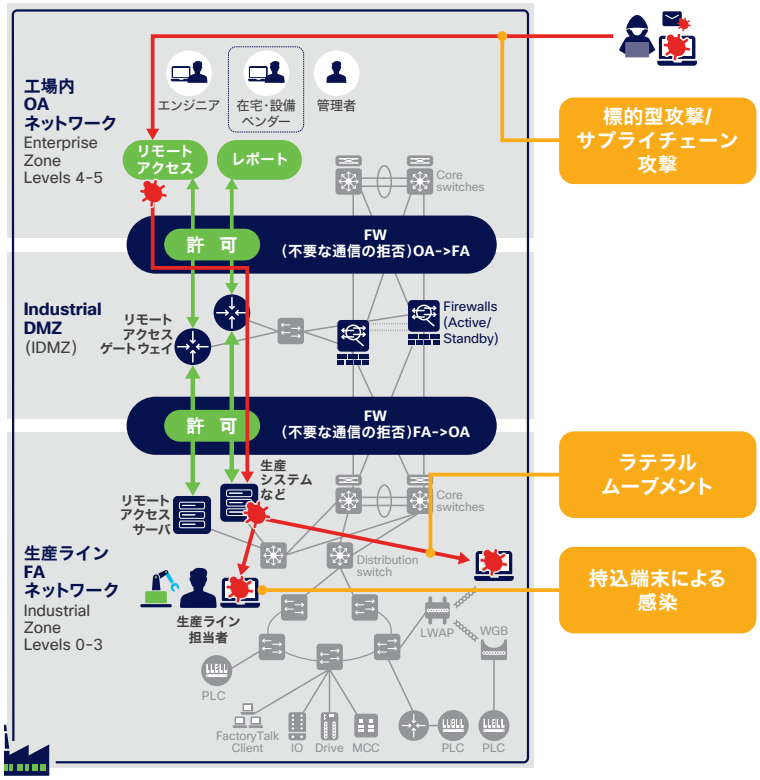
そんな中、近年の製造現場を狙ったサイバー攻撃は高度化しており、従来のアクセス制御、フィルタリングやアンチウイルスの仕組みでは検知出来ない傾向にあります。特に、SolorWinds に代表されるサプライチェーン攻撃においては、利用を認められたシステムや通信が侵害されてしまうため、これまでの防御方法では防ぐことが難しくなっています。

世の中に絶対的な防御方法はありませんが、サイバー攻撃の基本は、脆弱なところを狙うことにあります。これらの状況を踏まえ、製造現場に関わる人もセキュリティに対する意識、脆弱性への意識を高めて行くことが重要となります。

現在の製造現場におけるセキュリティ対策例



近年の製造業を狙った脅威の特徴



工場のセキュリティは誰が考えるのか？

製造現場におけるセキュリティ対策が、デジタル化を進める上で重要であることはご理解頂けたと思います。

では、工場のセキュリティは誰が考えるべきなのでしょうか?

製造現場でサイバー攻撃に備えるためには、IT と OT 双方の知見が必要であることは前述の通りです。お客様の企業規模や、組織・体制により担当領域が明確に分けられない場合はありますが、IT サービスとして提供されるものは IT 部門、OT 側が管理または判断する必要のあるインフラについては OT 部門で主体的に検討を行う必要があります。

先に述べたサイバー攻撃のアプローチに対しては、以下の形でそれぞれの攻撃への対策を考慮する必要があります。

IT 部門が主体的に検討

- メールによる標的型攻撃
- メールセキュリティ強化
- メール内に含まれる不正なサイトへのアクセスを制御
- 社員に対するセキュリティ啓蒙活動、教育

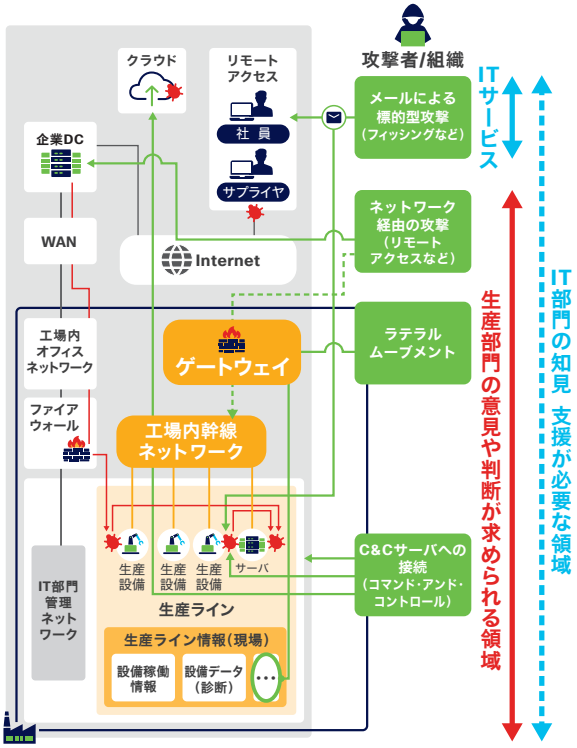
OT 部門が主体的に検討

- ネットワーク経由の攻撃
- 不要な通信の制御
- 通信相手（通信元）の特定強化（認証強化）
- 脆弱性対応
- ラテラルムーブメント
- ネットワークを細かく分割することでリスクを低減（セグメンテーション）
- 不要な通信を通さないように制御する（アクセス制御強化）
- 社内ネットワークにおけるデバイス通信に対する振る舞い検知
- C & C サーバへの接続
- マルウェアに感染した端末から C&C に対する通信を検知し、未然に止める（常に最新の不正サイトを把握する必要がある）

なぜ、製造現場のサイバーセキュリティ対策を OT 部門が主体的に検討する必要があるのでしょうか?

その大きな要因の一つには、製造現場の業務特性の違いからくる、現場ならではの課題にあります。オフィスエリアネットワークとは違い、生産ラインは常に稼働し、容易にメンテナンスが行えない他、生産設備を構成するデジタル資産には十分なコンピューティングリソースがないためデバイス単体でのセキュリティ実装が難しいことなどが挙げられます。このような業務特性の違う環境において、実装可能なセキュリティ対策は、OT 部門の判断が必要となります。また、オフィスエリアと違いデバイスでの対策が難しいため、ネットワークで守る施策が重要となります。

工場へのサイバー攻撃のアプローチと対策検討の担当領域



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

生産現場ならではの課題	解決に向けたアプローチ
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
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
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

工場におけるセキュリティ対策の検討ポイント

製造現場でセキュリティ対策を考えるポイントは多岐に渡りますが、デジタル化の進捗を踏まえて 6 つの領域に分けることが出来ます。

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
- 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
- マルウェア感染対策としてデバイスの振舞いを監視し、異常を検知

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）
- 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
- 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）の決定

④ クラウドアクセス認証強化

- クラウドに工場から、またはインターネット経由で入ってくる通信の接続元および接続先の特定
- 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）の特定

⑤ セキュリティ運用整備

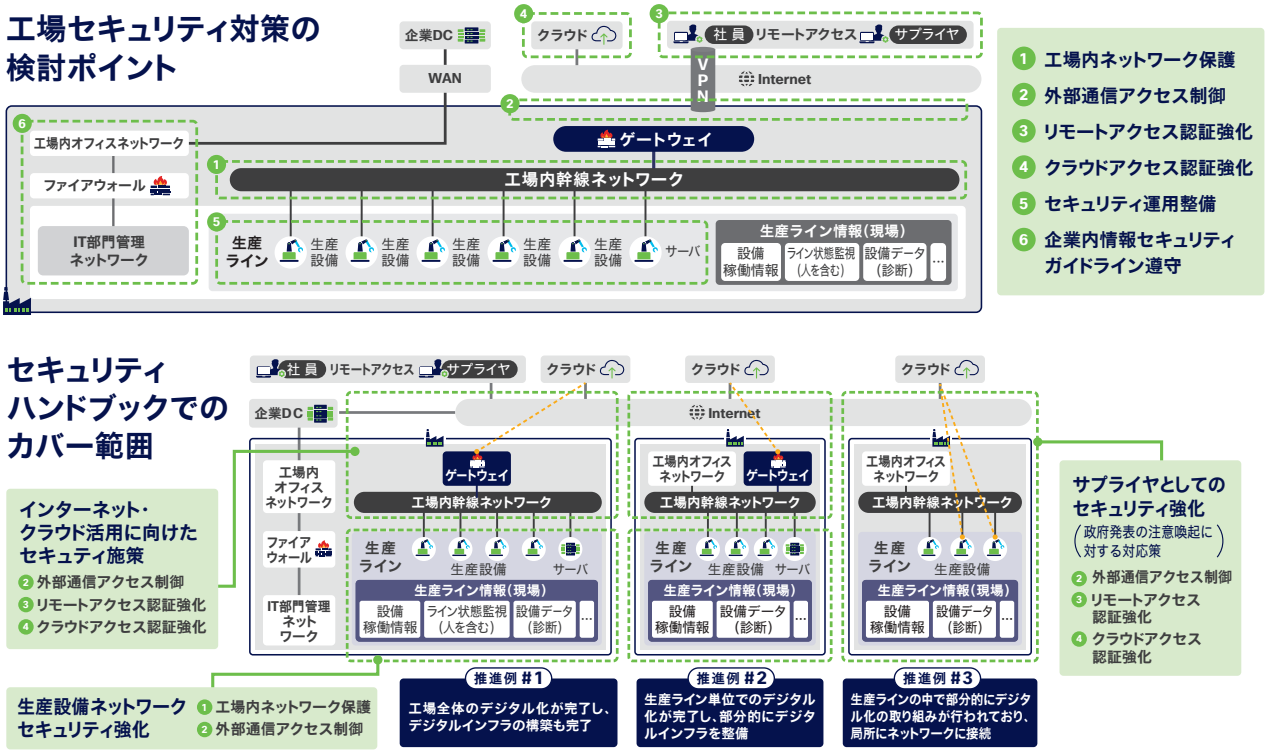
- 監視する内容の決定（⑥の企業として整備されているセキュリティガイドラインがある場合にはその内容を踏まえて検討）
- 監視内容に基づき必要なログ取得、保存方法を決定
- インシデント発生時の対応手段、連絡方法、報告方法を決定

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

本資料では、製造現場における検討領域を大きく3つに分けて、具体的な施策案を紹介します。

尚、“⑤ セキュリティ運用整備”、“⑥ 企業内情報セキュリティガイドライン遵守”については、各企業ごとに考え方や方針が異なるため、本資料の中では、有用と考えるソリューションの紹介までに留めています。シスコでは、⑤、⑥に対する有償支援サービスも提供しています。



今できる工場サプライチェーンセキュリティ対策

ここ数年、サプライチェーンを狙ったサイバー攻撃は増加しており、日本政府関連省庁からはサイバー攻撃に対する注意喚起や、セキュリティガイドラインが相次いで発表されています。自社がサプライチェーンにおいてどのように関わり、どの様なリスクと影響を与えるかを見極め、必要な対策を講じることを求められています。ここでは、どのような観点でセキュリティ対策を考えれば良いかについて説明します。

サプライチェーン攻撃とは？

製造業では、取引先などのサプライチェーンを利用して、侵害を試みる「サプライチェーン攻撃」の被害事例が見られます。「サプライチェーン攻撃」には、以下の傾向が見られます。

委託先や海外を踏み台にした攻撃

取引先などのサプライチェーン、海外拠点の中で、セキュリティ対策が甘い組織を攻撃の足がかりにして、大企業や政府組織など標的の組織を攻撃して不正アクセスする

ソフトウェアサプライチェーン攻撃

ソフトウェアの開発元や配布元などソフウェアのサプライチェーンを通じて、マルウェアや攻撃コードを挿入したソフトウェアを配布して攻撃の足がかりにする

いずれの攻撃も、ネットワークを介して既にビジネス上の取引のある相手を経由するため、発見し辛いという特徴があります。また、近年では、ネットワークやシステムが企業間で繋がっていなくとも、サプライチェーンを構成する一部の企業の生産が攻撃により停止することで、パーツ供給が滞りサプライチェーン全体に影響を与えるなど、被害が大きくなる事例も出ています。

サプライチェーン攻撃はどこから？

では、サプライチェーン攻撃はどのような形で、どこからやってくるのでしょうか?攻撃のきっかけとなる侵害は、工場に対して行われる攻撃手法と同様です。主な攻撃の侵入経路は、サプライチェーンに特化したものではなく一般的なものになります。

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、侵入の仕込みを行う

ネットワーク経由の攻撃（リモート）

- 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対策が脆弱である場合、ユーザーになりすまして侵入

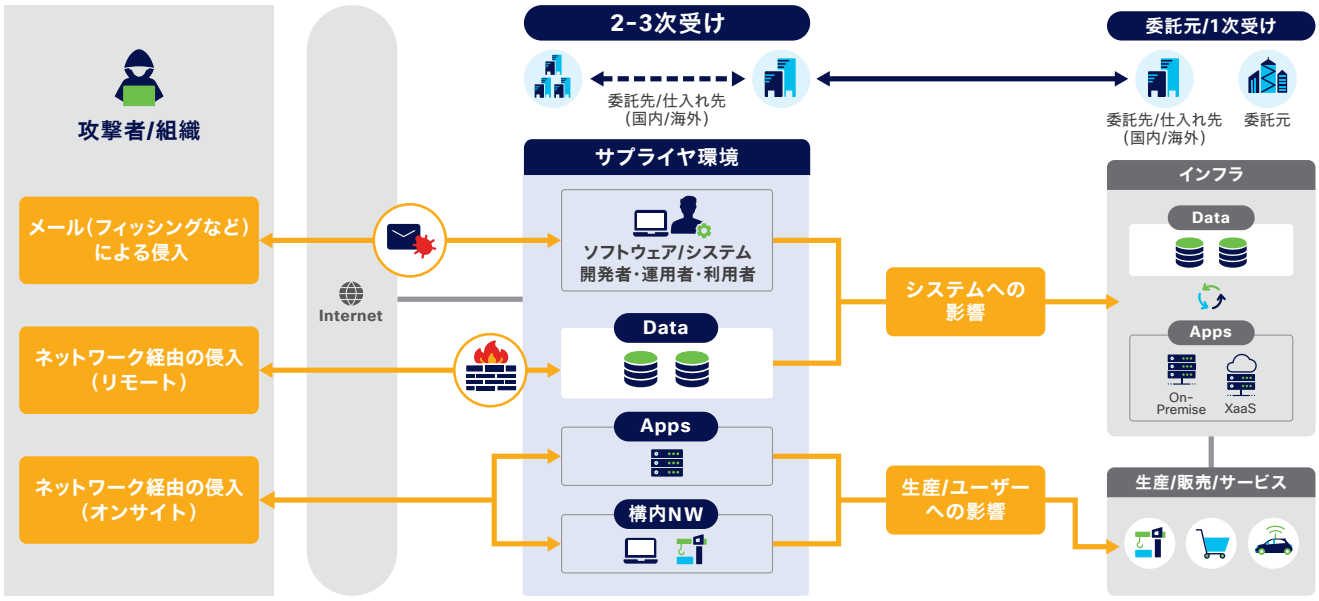
ネットワーク経由の攻撃（オンサイト）

- 悪意を持ったユーザーが内部ネットワークに接続し侵入（無線 LAN、有線 LAN）
- 外部から持ち込んだ USB を経由してウイルスを侵入させる

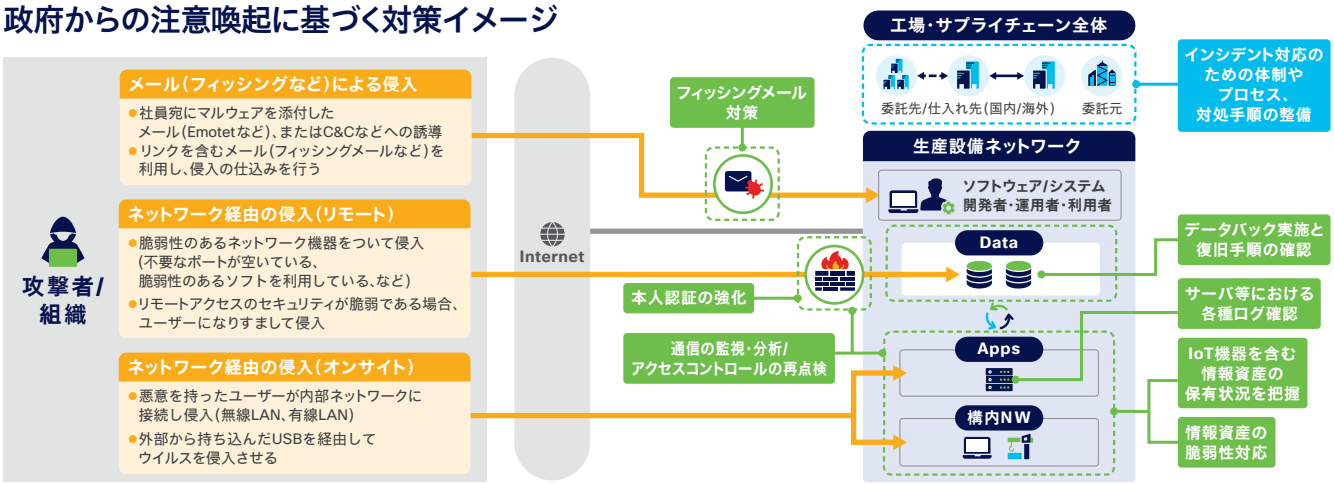
大きな違いは、これらの攻撃が自社ではなく、ビジネス上の取引やシステム的に関連のある企業を狙うため、いくら自社の防御を強化しても、発見が難しい点にあります。

そのため、サプライチェーンに関わる各企業でのセキュリティ対策を講じる必要があります。

サプライチェーン攻撃の概要



政府からの注意喚起に基づく対策イメージ



政府発表の注意喚起

製造業を狙ったサプライチェーン攻撃増加の状況に対して、2022 年 3 月 1 日、中央省庁 7 省庁の連名で注意喚起を発表しました。この発表の中では、どういった対策と、どのような運用を考える必要があるかがまとめられています。

その内容を要約すると以下になります。

- **IoT 機器を含む情報資産の保有状況を把握**
- **情報資産の脆弱性対応**
- **通信の監視・分析 / アクセスコントロールの再点検**
- **本人認証の強化**
- **フィッシングメール対策**
- **サーバ等における各種ログ確認**
- **データバック実施と復旧手順の確認**
- **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**

これらの対策は、いずれも一般的なセキュリティ対策であり、サプライチェーンにおける特別な対応が必要な訳ではありません。

サプライチェーン セキュリティ対策における課題

一方で、サプライチェーン全体に対してセキュリティ対策を行うには幾つかの課題があります。

一つ目は、導入コストと検討リソースの問題です。大企業とは違い、サプライチェーンを構成する 2 次受け、3 次受けのサプライヤーの中には、対策の検討行うための人的リソースや、対策を講じる十分な予算を持っていない場合があります。

二つ目は、何を基準にどこまで対策を行うかの判断が難しいという問題があります。サプライヤーの中には、単一の委託元企業だけではなく複数の委託元企業との取引を行っている企業も多くあります。ある委託元企業が、その企業のサプライチェーン全体に対してセキュリティ対策の方針を決めたとしても、取引先のサプライヤーにとって最適な対策とならない可能性があります。

このような状況を踏まえて、業界団体や関連省庁からは、業界共通の考え方としてのセキュリティ対策の検討項目と対策レベルを定めたガイドラインが発表されました。サプライヤーが検討を進める際に、これらのガイドラインを参照することは有用な手段と考えられます。

ただし、セキュリティガイドライン記載の検討項目は多岐に渡るため、検討に時間がかかることが想定されます。

すぐにでも有効な施策を実施したい場合、優先順位をつけ、投資効果の高い施策を実施するということは選択肢の一つと考えられます。現在の自社製造現場のインフラ環境を踏まえた上で、想定されるリスクに対して効果の高いところから着手することは、予算やリソースが限られた中でも確実にセキュリティレベルを向上させる有効なアプローチと言えます。

サプライチェーンセキュリティ対策における課題と解決アプローチ

投資効果の高いセキュリティ施策

サプライチェーンセキュリティ対策として投資効果の高い施策とは何でしょう?

その問いに対する答えについて、政府発表の注意喚起をもとに考えてみましょう。

注意喚起に含まれる検討ポイントは、大きく３つに分かれています。一つ目は、工場内の資産に対する施策、二つ目は工場に外から入ってくる通信に対する施策、三つ目はセキュリティインシデントに対する体制や対応プロセスなどのセキュリティ運用の整備となります。

一つ目のポイントについては、対象範囲が多岐にわたることや、生産ラインの稼働との兼ね合い、担当者とのへの確認など、ソリューションの導入だけでは対応が完了しないため、すぐに施策を行うことは難しいと考えられます。

二つ目のポイントについては、生産ラインへの影響が少ないことと、ソリューションの導入による解決が見込まれるため、施策の実装が容易であると考えられます。

三つ目のポイントについては、整備する内容の粒度は問わずとも、可能な限り対応が必要な内容となります。セキュリティ対策を行なっても、完全に防ぐことは不可能なため、有事の際の対応方法を考えておく必要があります。また、セキュリティ運用は、企業のリソースや、導入する施策により対応方法が変わることもあるため、実装する施策と、社内リソース状況を踏まえて検討する必要があります。

では、二つ目のポイントである、工場に外から入ってくる通信へのセキュリティ対策として、投資効果が高い領域はどこになるのでしょうか?

こちらの問いについては、各社の製造現場のインフラ環境に依存しますが、実装容易性やどのお客様でも必要となる以下の施策、および検討要素がその回答になると考えます。

- **本人認証の強化 -> MFA（多要素認証）**
- **フィッシングメール対策 -> メールセキュリティ**
- **通信の監視・分析 / アクセスコントロール**
  -> 次世代ファイアウォール
  -> DNS セキュリティ

それぞれの検討要素ごとに単一のソリューションで提供されることが多いためと、問題があった場合の対応を集約することが可能です。

次に、これらの施策にどの様な効果があるかを見てみましょう。

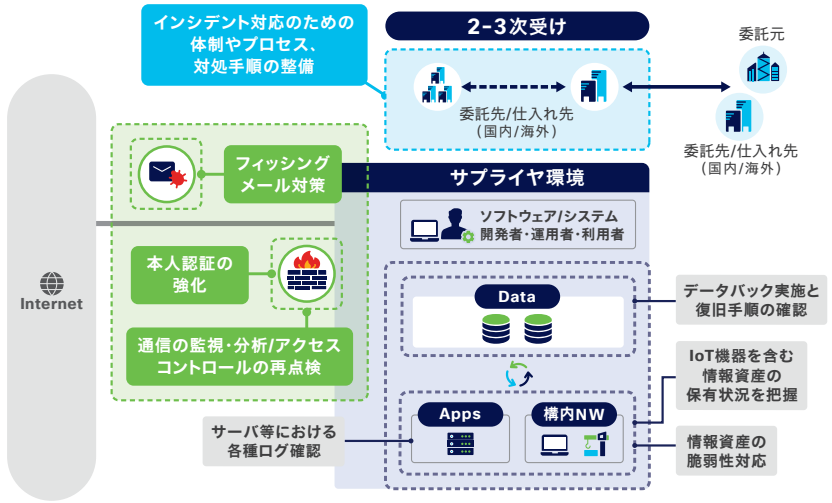
本人認証の強化 -> MFA（多要素認証）

この施策は、工場内のサーバや設備に対してリモートからアクセスする環境を持っている場合に、接続元が正しいユーザなのか身元確認を強化します。パスワードのみの単純な認証で運用されている企業では、セキュリティインシデントは数多く報告されており、各業界のガイドラインでも必須とされています。これらの状況から、リモートアクセス環境を持つ工場においては、多要素認証の導入は投資効果もさることながら、必須の施策と言えます。

フィッシングメール対策 -> メールセキュリティ

この施策は、未だに後を絶たないフィッシングメールへの対策となります。どの工場においても業務や取引の連絡にメールを利用することは一般的であり、そのメールを使った攻撃の手口であるフィッシングメールは年々高度化しています。フィッシングメールは人に標的を絞った攻撃であるため、狙われた人自身が気付かない場合、回避出来ません。これを防ぐ手段として、フィッシングメールへの対策が可能なメールセキュリティを導入することは、投資効果が高いと考えられます。

実現性の高い施策検討範囲と検討要素

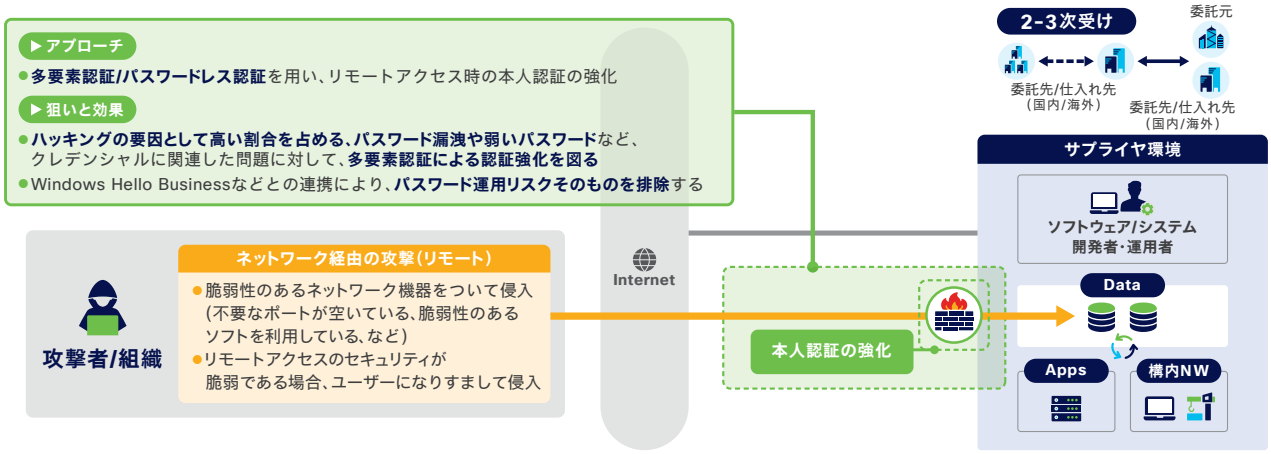


注意喚起に含まれる施策	施策に必要な要素
本人認証の強化	MFA（多要素認証）
IoT機器を含む情報資産の保有状況を把握	資産可視化
情報資産の脆弱性対応	脆弱性管理
フィッシングメール対策	メールセキュリティ
サーバ等における各種ログ確認	SIEM/MSS
通信の監視・分析/アクセスコントロールの再点検	適切なネットワーク設計/インターネット境界セキュリティ/ネットワークとセキュリティの監視（MSS）
データバック実施と復旧手順の確認	データバックアップ/データセキュリティ
インシデント対応のための体制やプロセス、対処手順の整備	SOC・CSRT立ち上げ/インシデント対応手順作成

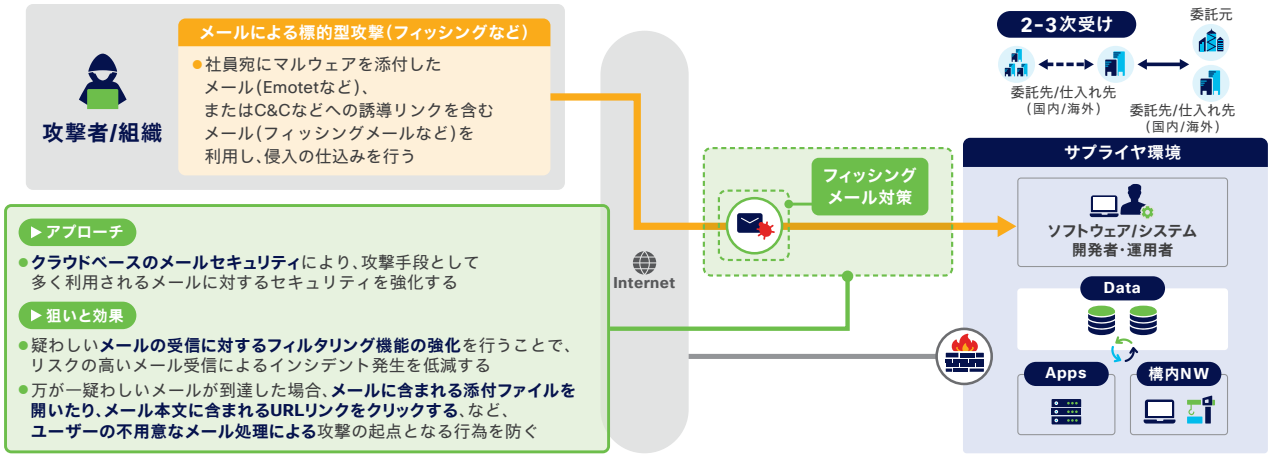
・通信の監視・分析 / アクセスコントロール
-> 次世代ファイアウォール

この施策は、外からの通信へのセキュリティ対策としてはある意味基本的な施策となります。重要な点は、近年の高度化する攻撃に対応するため、外からの通信に対して、より高度な分析や検知が行える次世代ファイアウォールを導入する点にあります。そしてもう一つ重要な点として、複数の工場を持つ企業においては各工場に導入されたファイアウォールを統合的に管理することです。工場毎に担当者が異なり、設定や運用が適切に行われていない場合は、その工場はリスクに曝されることになります。

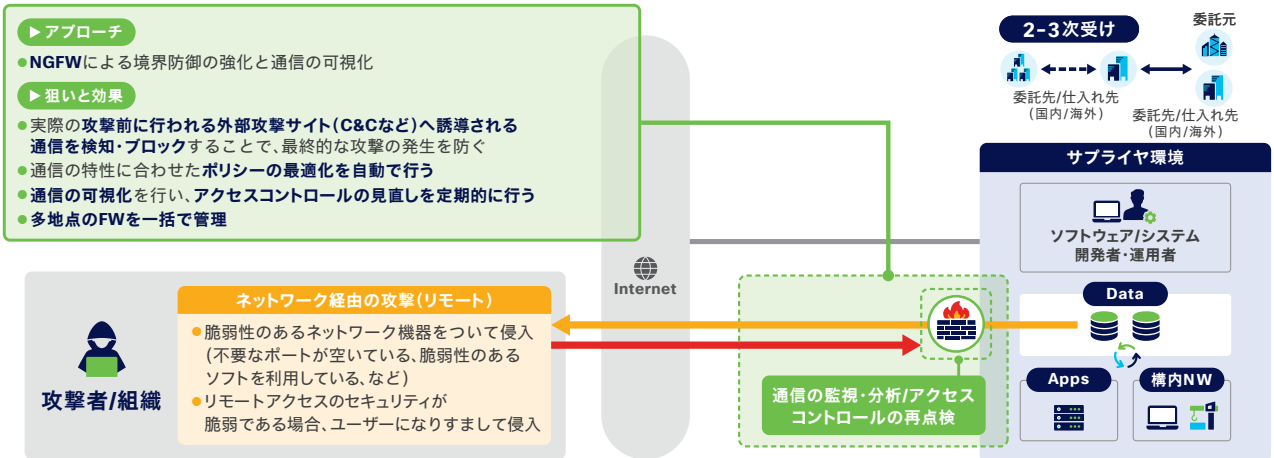
今できる工場サプライチェーンのセキュリティ対策：本人認証の強化



今できる工場サプライチェーンのセキュリティ対策：フィッシングメール対策



今できる工場サプライチェーンのセキュリティ対策：次世代ファイアウォール導入と統合管理



通信の監視・分析 / アクセスコントロール
-> DNS セキュリティによるアクセス制御

この施策は、外から中に入って来る通信への制御ではなく、中から外に出ていく通信に対する制御を行うものです。

外から中への通信に対して、投資効果が高い施策といいながら、なぜ中から外への通信への対策を考えるのか?

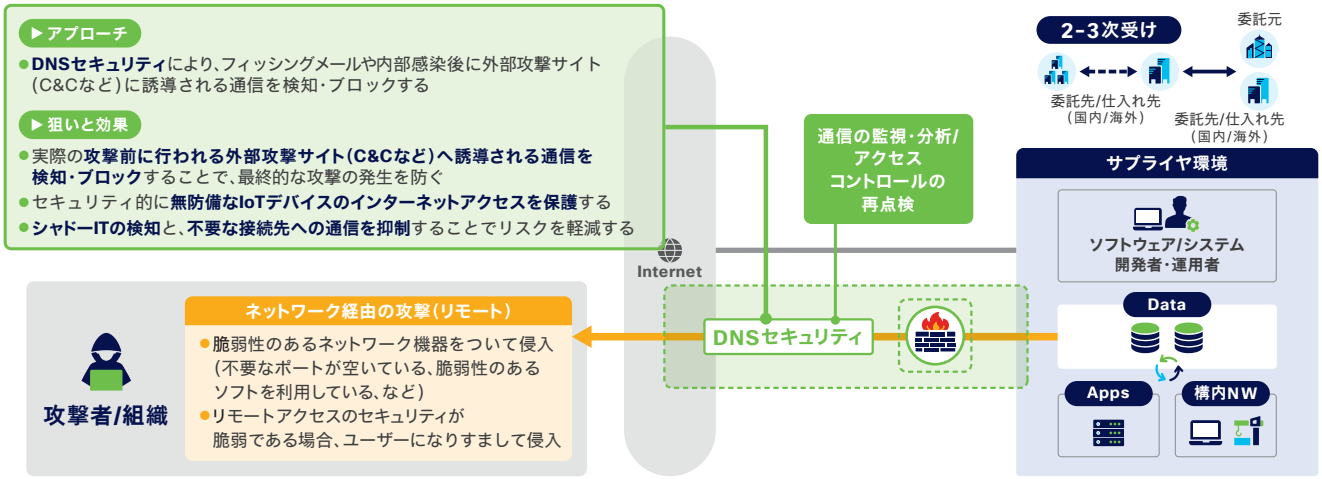
その理由としては、近年のサイバー攻撃の高度化と、製造現場におけるクラウド活用があります。

高度化したサイバー攻撃においては、先に述べた多要素認証や、メールセキュリティ、次世代ファイアウォールを導入したとしても、侵入を防ぐことは出来ません。ただし、それらの対策をしておくことで、侵入する際のマルウェアや、攻撃の動きは、初期段階では軽微なものとなります。その後、本格的な攻撃を行う前に、侵入したデバイスから C&C サーバと呼ばれるクラウド上に用意されたサーバにアクセスさせた後、本格的な侵害を開始します。

C&C サーバは、居場所を特定させないために絶えずアドレスを変更しているため、ファイアウォールの固定されたフィルタ設定では防ぐことが出来ません。

この対策として有効なのが、DNS セキュリティです。これにより、工場内に侵入を許したとしても、本格的な侵害を受ける前の水際で防ぐことが可能となります。

今できる工場サプライチェーンのセキュリティ対策：DNS セキュリティによるアクセス制御



生産設備ネットワーク セキュリティ強化施策

製造現場のデジタル化を進める上で、データを流通させるためのネットワークは重要な役割を持ちます。デジタル化に伴いデジタルインフラの整備を進める一方で、繋がるデバイスやシステムが増えることは新たなセキュリティのリスクを持つことになります。ここでは、工場内インフラにおけるセキュリティ対策の考え方について説明します。

工場内におけるセキュリティとは？

工場内でのセキュリティを考える上で重要なことはなんでしょう?

既に述べたように、製造現場には製造現場としての判断があり、ビジネスリスクや重要度は IT やオフィスエリアのインフラ環境とは異なります。

製造現場の担当者にとって重要なことは、生産ラインを止めないことです。業界や製造・生産する製品によっては、コンプライアンスや情報漏洩的な観点でのセキュリティが必要なケースもありますが、多くの場合、最も重要なビジネスリスクは生産設備が停止することだと言えるでしょう。

生産設備が停止する原因には様々なものがありますが、ここではサイバーセキュリティ観点で紐解いてみましょう。

システム化やデジタル化が進んだ生産設備が停止する要因は、大きく三つあります。一つ目は、システム要因により動作不良を起こしてしまうことです。二つ目は、作業ミスなどの人的要因により、生産ラインが停止してしまうことです。三つ目は、設備の部品劣化、老朽化などの物理的要因による故障により、生産ラインが停止してしまうことです。この中で、人的要因と物理的要因については、人とモノの動作に関連するため、その対策としてサイバーセキュリティ観点での対応は関連しません。

一つ目のシステム要因について考えてみましょう。

システムの動作不良は、ソフトウェアの不具合の他に、システム負荷や通信不具合などの事象が発生した結果として起きてしまいます。では、それらの事象は何が原因で発生するのでしょうか?大きくわけると、以下の４つの観点があります。

- **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**
- **インフラのキャパシティ不足**
- **ネットワークの干渉**

これら４つのうち、ソフトウェアのバグは、事前の対策が極めて困難なため、それ以外の３つに対して対応を考える必要があります。

セキュリティ対策の話にも関わらず工場内インフラ、ネットワークの観点を含む理由は、実際の現場（特に生産ラインに近いところ）で発生している生産設備停止の問題の多くが、これらの観点に起因するためです。

では、問題を発生させてしまうのは、結局どういったことが現場で起きているからでしょうか?

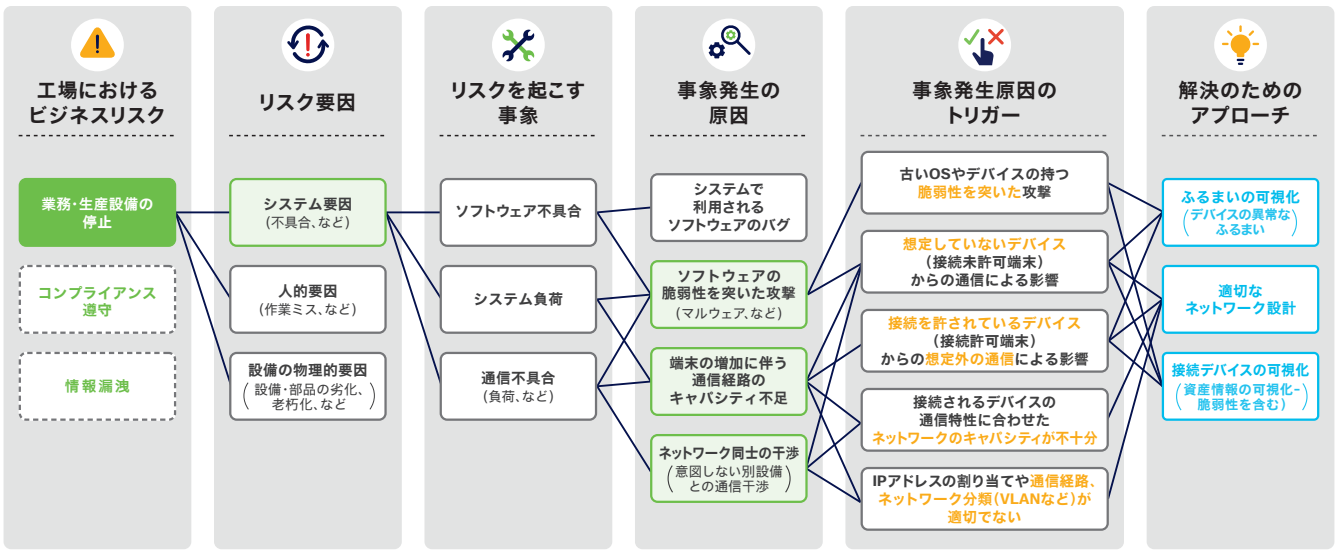
一つは、生産設備内の端末の脆弱性を突いた攻撃が考えられます。特に、メーカーサポート切れの OS を利用しているデバイスでネットワークに繋がっているデバイスは対象となりやすい傾向にあります。

それ以外に実際の製造現場で頻繁に発生していると考えられるのが、以下の状況です。

- **接続することを許可されていない（または想定されていない）端末がネットワークに繋がっている**
- **接続未許可の端末もしくは接続許可された端末が想定していない通信を行なっている**

この状態は、工場内の通信状態を可視化していないとわからないため、多くの場合、問題が発生しない限り気づくことは難しいでしょう。

製造現場におけるセキュリティ対策のアプローチ



上記３点はサイバーセキュリティ観点では重要なポイントとなりますが、上記以外にも重要な点として生産設備ネットワークの環境に関わるものが二つあります。ネットワークのキャパシティを含むネットワーク設計です。

これまで繋がっていなかった生産設備を繋げていく、または更なるデジタル資産を繋げていく上で、データが流れるネットワークの帯域が不十分な場合、特定のシステムが突発的な通信を流してしまうと、他のシステムが影響を受けしまいます。また、端末が利用する IP アドレスの重複による問題は、未だに現場で発生しています。

これらの問題を解決するアプローチとして、弊社では以下の三つの観点が重要と考えています。

- **接続デバイスの可視化**
- **適切なネットワーク設計**
- **ふるまいの可視化**

これら３つの要素を全て同時に対応することはなかなか難しいかもしれません。それぞれのアプローチには依存関係があるため、対策を進めるにあたっては段階的に進めることが良いでしょう。

まず、最初に重要なのは、接続デバイスの可視化（資産の特定）です。セキュリティの基本的な考え方として、見えないモノは守ることが出来ません。製造現場においてネットワークに接続されるデバイスを把握することは、前述の通り、製造現場でのセキュリティ対策としても重要です。

製造現場での資産の特定において需要なことは、その資産を管理している担当者や部門を合わせて整理しておくことです。その後の運用において何か問題があった場合に、誰が判断出来るかが製造現場においては極めて重要です。

次に重要なのが、資産の特定をした上で、接続されるデバイスの特性に合わせた適切なネットワーク設計を行うことです。今後の拡張を踏まえた、IP アドレス払出しの考え方や、通信経路とその帯域、ネットワークの分割などを考えることは、生産設備を安定稼働させる上でも非常に重要です。

資産の特定をして、ネットワークが適正に設計されると、次に重要なのがふるまい監視です。資産の特定や、ネットワークの設計を行う前にふるまい監視を行うことも可能ですが、先に進めてしまうと、実際に検知した内容を正しく判断するのは難しいでしょう。

ふるまい監視は、平常時の状態に対して異常なふるまいを検知することで、サイバー攻撃や生産システムの異常動作を未然に防ぐことが可能となります。

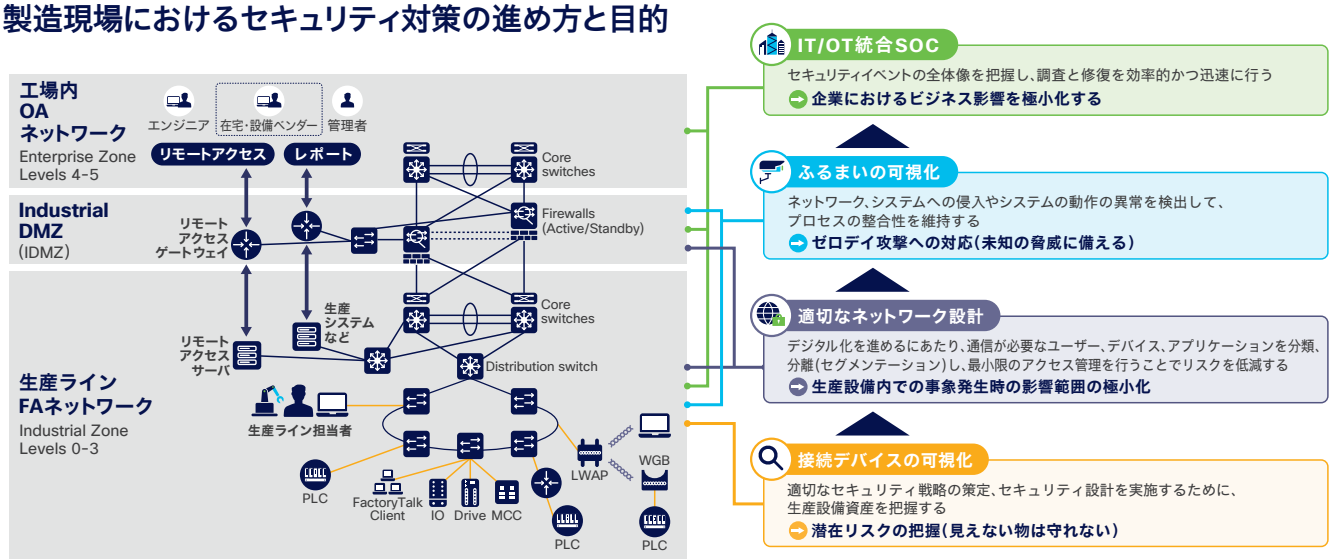
そして、それらの対応を進める中でもう一つ重要なのが、運用です。生産設備や関連するネットワークは、基本的には生産設備を管理する担当部門が運用を行われます。その一方で、セキュリティ運用（SOC）については、明確な役割分担がなく、現実的に議論がされないことが多いのが現状です。

今後、製造現場でのデジタル化が進み、工場全体でセキュリティ対策を実装する範囲が広がると、全体のセキュリティを横断的に運用する仕組みが必要となることが予想されます。

そしてこれら製造現場でのセキュリティ対策を検討する上で最も重要なことは、検討の段階でどこまでを目標に対策を行うかを予め決めた上で、製品設定や設計を進めることです。そうしないと、後付けの検討では、機能や設計の考慮が漏れてしまい、手戻りや追加でのコストが発生してしまいます。

セキュリティ対策の検討は、企業としてのセキュリティガイドラインも関わるため、既に述べた通り、可能な限り IT と OT 側の双方で擦り合わせを行い、進める必要があります。

製造現場におけるセキュリティ対策の進め方と目的



シスコの製造現場セキュリティ対策ソリューション

シスコでは、製造現場でのセキュリティ施策に対して、各種のセキュリティソリューションを提供しています。

①資産の特定

製造現場での資産の特定には、Cisco Identity Services Engine(ISE) と Cisco Cyber Vision の二つのソリューションを提供しています。ISE は、MAC アドレス、IP アドレス、ユーザ単位での資産の可視化とともに、ネットワーク機器と連携し、それら資産のアクセス制御を行うことが可能です。製造現場で利用される IoT 機器の詳細な可視化は、Cisco Cyber Vision での可視化が有効です。

②ネットワークのセグメンテーション

製造現場でのセキュリティ対策は、ネットワーク設計において、設備やデバイスの利用用途や特性別に、物理または論理的に分割を行うセグメンテーションが有効です。これらを実現するソリューションとして、ネットワークを構成する Cisco Industrial Ethernet(IE) スイッチと DNA Center(NW 管理ツール)、境界面を守るファイアウォールとして Cisco Secure Firewall ISA3000、Cisco Firepower を提供しています。

③ふるまい監視

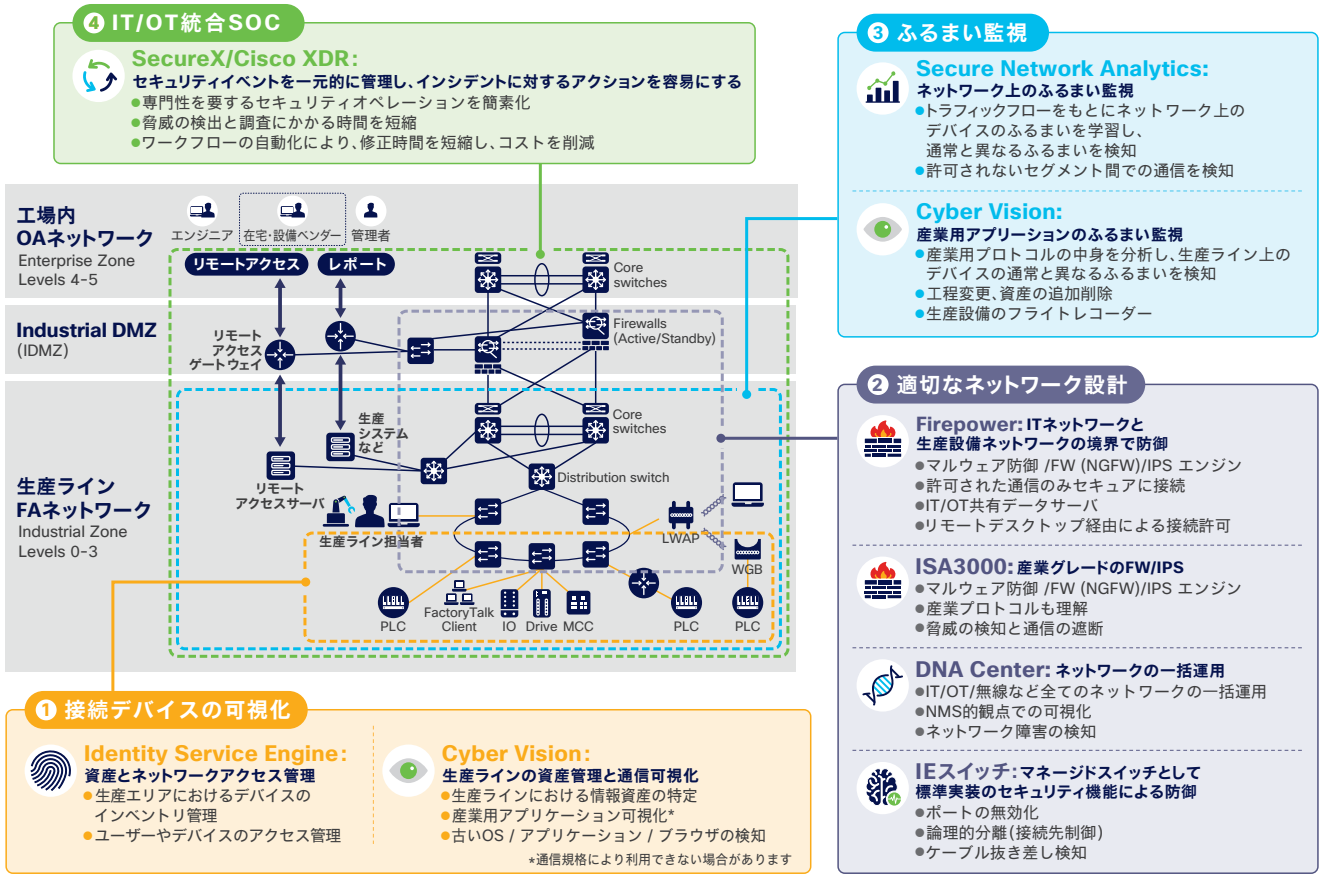
製造現場におけるふるまい監視は、設備デバイスに対する監視とネットワーク全体において監視する二つの観点があります。それぞれ利用する通信技術（プロトコル）に違いがあり、問題に対する判断基準が異なることから、それぞれ専用のソリューションとして、Cisco Secure Network Analytics(SNA) と Cisco Cyber Vision を提供しています。

④ IT/OT 統合 SOC

製造現場全体でのセキュリティ運用を効率的に行うソリューションとして、SecureX/Cisco XDR を提供しています。SecureX/Cisco XDR は、API を利用してシスコを含むセキュリティソリューションと連携し、セキュリティイベント発生時の調査、解析、対応を効率化します。

①～④の観点は、国際自動制御学会（ISA）、国際電気標準会議（IEC）が協力して文書化した “ISA/IEC-62443 シリー

製造現場におけるセキュリティ対策の進め方と目的



ズ標準規格および技術報告書”の“ISA/IEC-62443-3-3規格”についても有効です。この規格に含まれている要件、シスコがどのような支援を提供できるのかについては、以下のサイトで解説しています。
https://www.cisco.com/c/ja_jp/products/collateral/security/isaiec-62443-3-3-wp.html

また、シスコではソリューション提供以外に、検討を支援するサービス（有償）も提供しています。

【参考情報】

生産設備ネットワークにおける要素技術の違いとソリューションの役割

生産設備ネットワークには、異なる通信プロトコルが使われています。オフィスエリアネットワークでも広く利用さている標準イーサネットと、産業分野で利用されている産業用イーサネットです。

これらのプロトコルはその目的と用途が異なるため、それぞれに異なる技術仕様となっています。

そのため、資産の特定や、ふるまい監視を詳細に行うためには、それぞれのプロトコル特性にあったソリューションが必要となります。

シスコでは、工場内の標準イーサネットで構成されたネットワークに対しては ISE/SNA というソリューションを、産業用イーサネットで構成されたネットワークに対しては Cyber Vision をそれぞれ提供しています。

ソリューションを分けている大きな理由は、それぞれのプロトコルに対して適した分析エンジンが必要なためです。

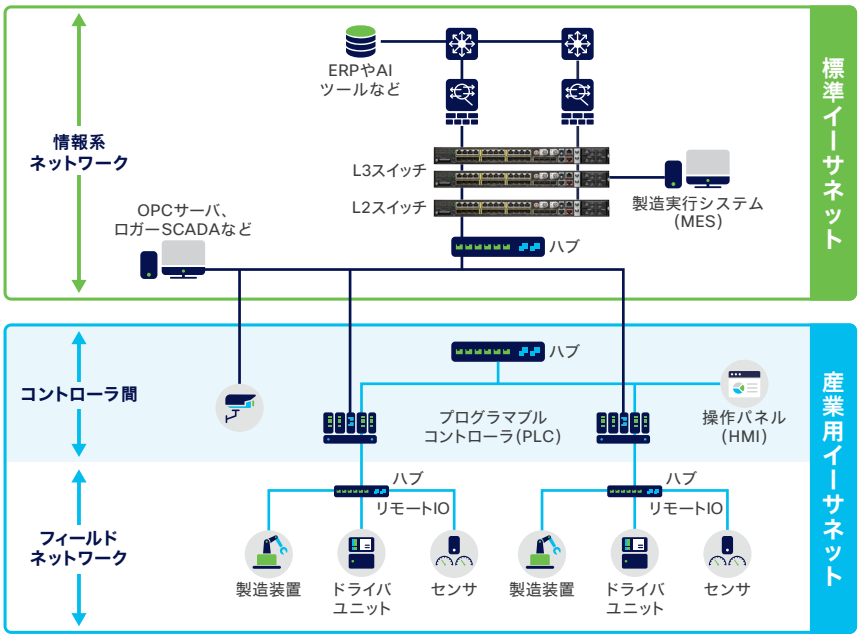
設備デバイスに対しては、各デバイス上で動作するソフトウェアやアプリケーションの動きを理解した上での判断が必要な一方で、製造現場に繋がる PC やサーバなどに対しては、IT 領域におけるサイバーセキュリティ観点での判断が必要となります。

また、これらの異なる環境に対しては、監視した結果として検知されるイベントに対して、誰が適切な判断、対応が行えるかということも重要なポイントとなります。

製造現場において生産設備や繋がる IoT 機器に関して検知されたイベントに対して、IT 側での判断は難しいでしょう。一方で、生産設備に繋がる PC やサーバで検知されたイベントを OT 側で判断することも難しいでしょう。

これらの特性や誰が何を監視し、対応を行うのかを見極めることは、適切なセキュリティ対策を確実に進める一つの考え方と言えます。

生産設備ネットワークにおける要素技術の違いとソリューションの役割



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

工場におけるインターネット、クラウド活用のニーズは徐々に増加しており、一部では、工場でのインターネットやクラウド活用を進めている企業もあります。一方、工場でのインターネット活用のニーズは以前からある中で、その導入については企業規模や組織体制などの要因により、思うように進められていない場合が多く有ります。また、既にインターネット活用を進めている企業においても、先に述べた昨今のセキュリティ脅威を考えた更なる施策が必要となっています。ここでは、これからインターネット活用を検討している企業、既に利用している企業において、今後どういった点を検討する必要があるかを説明します。

工場におけるインターネット活用の現状

現在工場で広がり始めているインターネット活用方法をまとめると、主に以下の３つに分けられます。

- **クラウドを使ったデータ分析**
- **クラウドを使ったパートナー企業とのコミュニケーション**
- **工場内設備またはシステムへのリモートアクセス**

上記は一般的な活用方法であると言えますが、企業や組織規模により、対応方法や考え方、対応の速度は異なります。この違いが生まれる理由は、工場インフラのインターネット接続に対するルールと責任の所在に依るところが大きいと考えられます。

IT 部門と生産部門で工場インフラの管理領域が分かれている企業では、インターネット接続に対するルールやガイドラインが整備されています。この状況において多くの企業では、特殊な事情を除き、インターネット接続は IT が管理する企業内ネットワークを経由してインターネットに接続することになります。サイバーセキュリティ対策が施されたネットワークを経由するため、安全な接続が提供されます。その一方で、IT 側への手続きや調整が入るため、製造現場側から見ると活用し辛い状況となっています。この状況が継続してしまうと、生産設備側で独自のインターネット環境を構築することとなり、新たなシャドウ IT を生むきっかけとなってしまいます。この問題を解決するためには、両者での相互理解を進め、セキュリティ対策強化に受けた双方にとってのより良い方向性を見出す必要があります。どうしても結論が出ない場合、生産部門が主体となって独自のインターネットアクセス環境を整備することは製造現場の生産性を上げる一つの手段ではありますが、企業としてはコスト重複となるほか、セキュリティリスクを抱える可能性があります。

もし、生産部門独自でインターネットアクセス環境を整備する場合においては、知見を持った外部に支援を求めることをお勧めします。

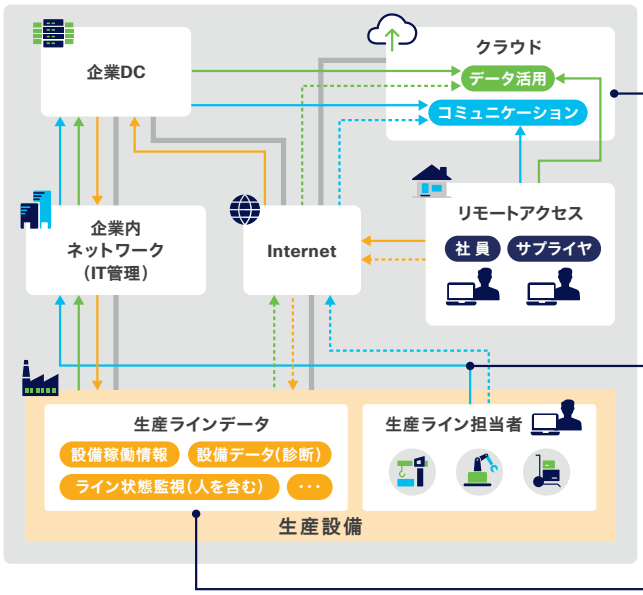
一方の IT 部門と生産部門の管理領域が分かれていない企業では、インターネット活用は前述の企業に比べて進んでいます。これは、比較的組織規模の小さい企業に見られる状況ですが、この場合、サイバーセキュリティに対する対策や運用体制の整備は十分でない場合が多く見受けられます。

自社内にセキュリティ対策の知識やスキルを持った担当者がいない場合は、外部に支援を求めることが必要です。2022 年に発生したサプライチェーンの問題が示すように、サプライチェーンに関わる企業のセキュリティリスクは、サプライチェーン全体に影響を及ぼす可能性が高いため、多くの企業においてセキュリティ対策の見直しが求められています。

以上の通り、企業の状況や組織体制によりインターネット活用における課題は異なりますが、一つ言えることはインターネットを活用する以上、セキュリティ対策の強化は必要ということです。

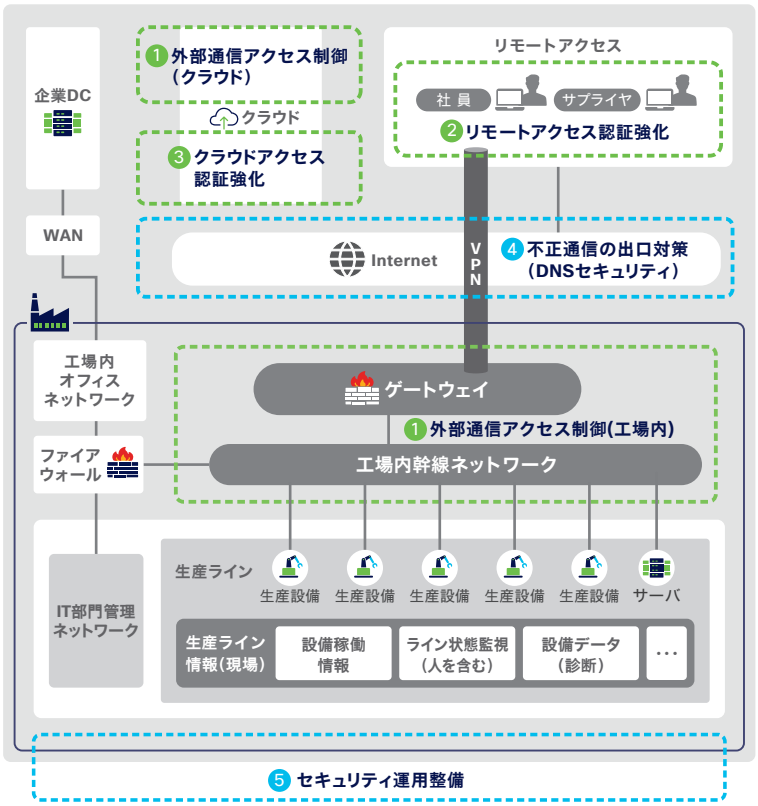
以降では、工場から直接インターネットアクセスを持つ際のセキュリティ対策について考えてみましょう。

製造現場におけるインターネット活用の現状



	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出来る環境を用意し、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と Cisco ソリューション



▶ 侵入を防ぐ施策

1 外部通信アクセス制御(工場内/クラウド) >>> Firepower Threat Defense(FTD)

- 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

2 リモートアクセス認証強化 >>> Duo

- 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

3 クラウドアクセス認証強化 >>> Duo

- ❷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施策

4 不正通信の出口対策 (DNSセキュリティ) >>> Umbrella

- 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、ルールによる制御だけでなく、リアルタイムな分析に基づく動的な制御を行う仕組みが必要

▶ 平常時、有事の対応を効率化する施策

5 セキュリティ運用整備 >>> SecureX/Cisco XDR

- 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

工場でインターネットを活用するには どのようなセキュリティ対策が必要なのか？

工場において今後インターネット活用する場合、どういったことを考える必要があるのでしょうか?

すでに工場の中に対する対策は説明しているため、ここではそれ以外にどういったポイントについて説明します。

図の中にある（1）～（5）は、9 ページに記載した内容となりますが、これらの対策は大きく 3 つの観点になります。

- **侵入を防ぐ施策**
- **侵入された後の本格的な攻撃を防ぐ施策**
- **平常時、有事の対応を効率化する施策**

一つ目の侵入を防ぐ施策は、工場で利用するシステムやアプリケーションに対する攻撃を守るためのものです。クラウドを利用する場合には、工場内だけではなくクラウド側に対しても同様の考慮が必要となります。また、工場、クラウドに展開されているシステムやアプリケーションへのアクセスに対しても、多要素認証などの認証強化の仕組みが必要となります。従来のユーザ名・パスワードの認証では、昨今の脅威は防ぎ切れない現状があり、多くのガイドラインでも必須の考慮事項となっています。シスコでは、それらのポイントに対して適用可能な Cisco Firepower Threat Defense(FTD)、Cisco Secure Access by Duo というソリューションを提供しています。いずれも、守る対象が工場、クラウドに関わらず適用可能なソリューションとなっています。

二つ目の施策は、攻撃者に侵入された後の対応として重要なポイントとなります。サイバーセキュリティの分野では、攻撃側が絶対的に有利であり、防御施策を突破される前提での施策が不可欠です。この点について有効な施策となるのが DNS セキュリティです。既に述べたように、製造現場で使用される IoT デバイスがクラウドと直接通信を行う場合、IoT デバイスの製品特性や製造現場の運用特性上、IoT デバイス上でのセキュリティ対策や迅速な脆弱性対応は難しいため、侵入後の対策としてネットワーク側での対策が効果的です。

DNS セキュリティの効果はどういった点になるのでしょうか?

工場を問わず、サイバー攻撃が高度化している昨今において、ある一定レベルのセキュリティ対策を実装している環境に対して、あからさまな攻撃が成立する可能性は極めて低いと言えます。そのため、攻撃者に狙われた場合、一般的・一定レベルのセキュリティ対策を通過して目標に到達します。ただし、侵入後、多くの場合はあからさまな攻撃はすぐに行わず、内部環境の偵察を行い、侵入されたデバイスは、本格的な攻撃を開始する前に一度インターネット上にあるコマンドアンドコントロール（C&C または C2C）と呼ばれる

サイトに接続します。この動き検知し、防ぐことを可能とするのが DNS セキュリティです。シスコでは、Cisco Umbrella というソリューションにより、高度な DNS セキュリティを提供します。

三つ目の施策は、運用の観点です。セキュリティはソリューションを入れて終わりではありません。導入したソリューションを使い、それらのソリューションを運用し、発生するイベントに対して適切な分析と対応をすることが重要です。また、セキュリティ施策は単一のソリューションで全て対応することが難しく複数ソリューションとなることと、属人的な対応となる場合が多いため、ソリューションや人に依存しない運用の仕組みが必要となります。シスコでは、SecureX/Cisco XDR と言うソリューションを適用しています。SecureX/Cisco XDR を利用することで、工場での異なるセキュリティソリューションの分析や対応を、人に依存せずに行うことが可能となります。

工場から直接インターネット通信を行う際のセキュリティ対策は、これまでと同様に工場におけるデジタル化の進捗状況や、組織体制、設備環境により異なります。以下に示す構成案は、主要なシステム（アプリケーション）がどこに存在し、誰にどのようにアクセスさせたいかにより、複数の実現方法があることを示しています。

その検討を進めるためには、何を考えれば良いでしょうか?

工場発のインターネット活用検討を具体的に進めるには？

それでは、工場から直接インターネット接続を行うためには、セキュリティソリューションを導入する以外にも検討が必要です。なぜなら、ソリューションを導入するだけでは、実際のインシデントが発生した際の対応、その判断の基準がわからないためです。

以下にソリューション以外で必要となる主な検討項目を記載します。

セキュリティポリシー/ ルール整備

- 企業における各種セキュリティガイドライン、ポリシーの確認（存在しない場合は整備を行う）
- セキュリティガイドライン、ポリシーに基づくセキュリティ機能の洗い出し

要件、機能、性能要求の整理

- 現状、今後想定される通信要件（通信帯域、送信元 / 送信先、利用するアプリケーション、など）の洗い出し
- 通信要件、セキュリティガイドライン、ポリシーなどを踏まえた上で想定されるネットワーク、セキュリティ要素機能の整理 - 将来的な拡張を踏まえた性能要求の整理

ログ運用管理

- セキュリティガイドラインや法規制などの観点で必要とされる保存期間を確認する
- 必要となる保存期間に対して十分なストレージ環境を確保する

セキュリティ運用及びインシデン対応プロセスの確立

- 定常的に何をどのポイントで監視するかをまとめる
- 各種セキュリティイベント情報をどのようにチェックするか、判断基準をまとめる
- インシデント発生時の報告方法（報告先、手段、含むべき内容、など）を整理する
- インシデント発生時の対応方法（誰が、何を、どのように行うか、実施後の連絡方法、作業完了後の確認方法、など）を整理する
- 対応後のレポート作成方法（報告内容、改善点、変更点、など）をまとめる
- セキュリティガイドライン、ポリシーへの適合状況を定期的に評価するプロセスを確立する
- セキュリティリスク、課題の評価
- 定期的に行うためのプロセスを確立する

まとめ

工場でのセキュリティ検討は多岐にわたるため、生産部門が単独で実施する場合、リソースや人材の問題により進めることが難しいと想定されます。したがって、以下の観点を持って進めることが重要です。

- **知見を持つベンダーや IT 部門などに課題を共有し、積極的に相談する**
- **全てを一度に実施することは難しいため、出来るところから確実に進めていく**
- **どのようなリスクが、どこにあるかを見極め、適切な投資を行う**
- **運用を見据えたソリューション選定**

事例

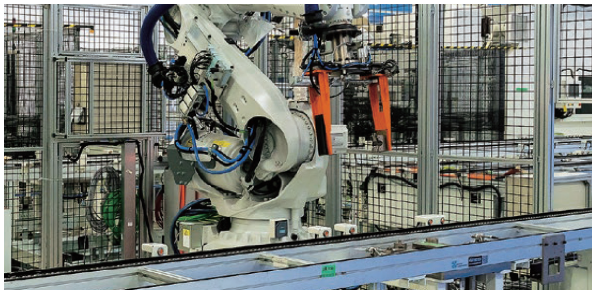
昨今のビジネス環境において、デジタル化への取り組みは避けて通れません。
これまでに述べた内容は、多くのお客様において日々検討が行われています。
製造現場でのデジタル化を支えるデジタルインフラの実現事例をご紹介します。

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。



> 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

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

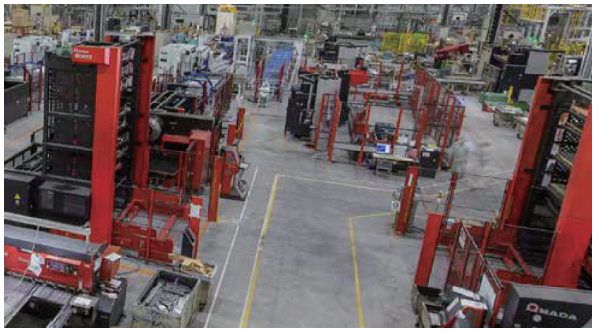
キオクシアは生産設備を守るため、シスコのセキュリティソリューションを導入しました。ネットワーク可視化をベースとするソリューションで、仮に脅威が侵入してもネットワークが検知し、早期対処が可能。エンドポイントの対策が困難という生産エリアの課題を解決しました。

> 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

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。



> 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

シスコ製造業向けソリューション
https://www.cisco.com/c/ja_jp/solutions/industries/manufacturing.html

シスコ お問い合わせ窓口

自社導入をご検討されているお客様へのお問い合わせ窓口です。
製品に関して ｜ サービスに関して ｜ 各種キャンペーンに関して ｜ お見積依頼 ｜ 一般的なご質問

お問い合わせ先

お電話での問い合わせ
平日 9:00 - 17:00
0120-092-255

お問い合わせウェブフォーム
cisco.com/jp/go/vdc_callback

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
cisco.com/jp

2361-2303-000-N