OT セキュリティーの喫緊の課題 ー 次にとるべき戦略とは?

01 「つながった」世界における OT

デジタル化が進み「つながる」産業系制御システムが増えるにつれ、「脆弱性」がより深刻な課題となっています。

産業システムは、1800年代に起きた最初の産業革命を牽引した蒸気駆動の機械以来、絶えず進化を遂げてきました。その過程において、産業機器の革新は、より早く、より適切に、より安全に、そして低コストで労働者が仕事を成し遂げるための能力を向上させてきました。

自動化が浸透するにつれ、オペレーショナル・テクノロジー (OT)、つまりコンピューター・ハードウェアとソフトウェアを活用して、物理的機器を監視、制御するニーズも高まりました。産業制御システム (ICS) は、OT 環境に必須となりました。これらは、温度、圧力、流量などのプロセス値を監視、制御し、危険な状態や故障を検出し、予防するために機械を監視します。ICS は OT 環境の一要素なので、ICS にのみ関連する特定のポイントがある場合を除き、この文書全体を通じて OT として言及します。

これらの環境が進化を続けるにつれて、OT 環境は、より適切に、生産性を高めるため、ネットワークに接続したデジタル情報技術 (IT) ソリューションをより活用するようになっています。企業は、より多くの Industrial Internet of Things (IIoT) を統合しています。これは、機械とシステムが自動的に情報を共有し、分析することが可能なスマート・センサーです。デジタル変革のビジョンの1つは、IIoT 機器を活用して、産業制御システムを企業 IT システム、ビジネスプロセス、そして分析に接続し、統合することです。これにより、数多くの利点が得られます。

- **より優れた管理と可視性**
  産業システムを IT ネットワークに接続すると、産業環境は各装置、そして産業エコシステムの全体のより包括的な視野を得て、それらのシステムの管理と運用がより簡単に、そしてより効果的になります。

- **アップタイムの改善**
  IIoT センサーがシステムと装置の状態と性能を常に監視することにより、企業が高価な修理やダウンタイムを避けることを助ける、予測的メンテナンスのスケジュールを立てることが可能になります。これは、性能、品質、そして生産性を高め、収益性を高めることに繋がります。

IT と OT の統合による利点は否定できません。しかし、この統合により新たなリスクと課題がもたらされます。中でも主要なのは、ICS セキュリティーです。より複雑で、拡大したリスク、そして新しい脅威は、サイバーセキュリティーのインテリジェンスとアナリティクスを、よりデジタル化された OT 環境に統合するトレンドを高めました。

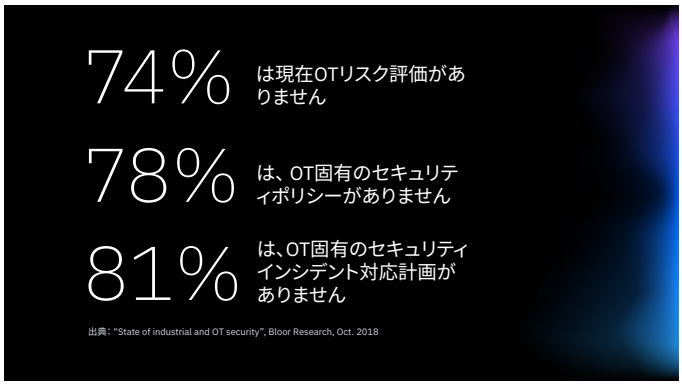
結果として、OT 環境の ICS の保護は現在の最優先事項となっています。

02 OT/IT の統合とサイバーセキュリティー

産業 OT 環境におけるサイバーセキュリティーは、セキュリティーの学習曲線の最も基礎のところになります。

数十年前、企業が最初にクライアント/サーバーのネットワークとインターネットの活用を開始した時、最初にセキュリティーについて考えることはありませんでした。犯罪者が IT システムをハッキングして、不正操作し、お金やデータを盗むことができると気がつくまで、セキュリティーは最優先事項にはなりませんでした。企業は、この新しい課題への対処を学習するのに、多大な影響を被りました。

ICS テクノロジーがネットワークに接続された時に、今日の OT 環境は同様の課題に直面します。つい最近まで、オペレーショナル・テクノロジーは、リモートからはアクセスできない、企業専用のベンダーベースの閉じられた接続とプロトコルで相互接続されていました。ICS テクノロジーが標準的な IT 通信プロトコルに移行する現在、IT セキュリティーの課題は OT 環境の一部となりました。しかし、多くの企業はこれらの新しいセキュリティーの課題に準備ができていません。



現在の統合された OT/IT 環境におけるサイバーセキュリティーの実装は、20年前の IT セキュリティーに相当します。しかし、OT 環境でのセキュリティー侵害の影響は非常に重大であり、さらに学習のプロセスを経る時間はありません。

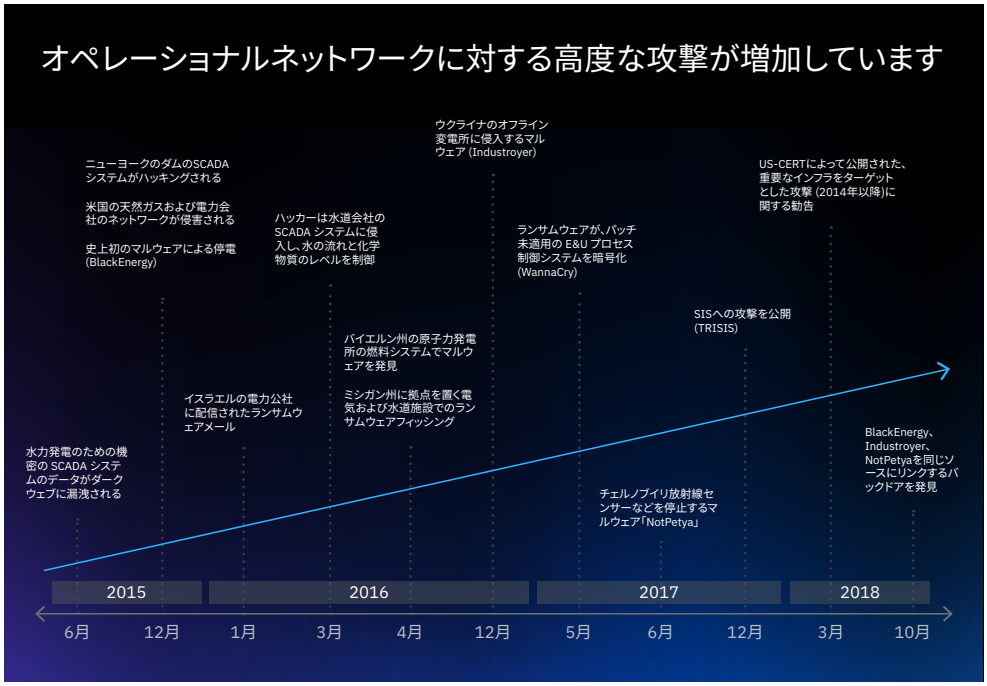
産業 OT のセキュリティーの課題

OT 環境は、セキュリティーに関する数多くの課題に直面しています。

- **リスク**
  - **リスク軽減と修正措置の不足**
    運用上のリスクとコストに強く焦点を当てるため、運用では、サイバーセキュリティーの脅威、つまり発生の可能性そして潜在的な影響に関する理解が一般的に不足しています。そしてしばしばこれを軽減するための戦略が取られていません。
  - **テストが難しい稼働環境**
    侵入テストは、IT セキュリティーでは重要なツールですが、ICS システムに重大なリスクをもたらす可能性があります。結果として OT 環境では、侵入テストは注意しながら利用、または他のテスト方法に変更しなければなりません。
  - **セキュリティーに対する限定的な認識**
    オペレーターやエンジニアといった産業環境の従業員は、サイバーセキュリティーを理解しておらず、IT セキュリティーの担当者は OT 環境のことを知りません。その結果、OT 環境にはリスクを軽減する技術やツールがほとんど存在しません。例えば、認証の慣行が弱いことも一般的です。
  - **限られたパッチ適用**
    ソフトウェアのアップデートとパッチ適用はセキュリティーにとって非常に重要です。しかし、OT パッチはベンダーの承認や、適用する前に広範なテストが必要なことが多いため、パッチ適用のプロセスは時間がかかります。パッチはまた、ダウンタイムも生み出します。

- **可視性**
  - **限定的な資産の可視性**
    OT 環境は通常、潜在的な ICS の脆弱性、ネットワークのトラフィックおよびセキュリティー管理機能の可視性が限定的であったり、なかったりします。実際、大部分の産業環境はその ICS 機器やそれらがどのプロセスを支援しているのかについて十分な説明責任がありません。これだけでも、悪意のある者が問題を引き起こす多くの機会を与えています。
  - **OT 専用プロトコル全体で機器を見ることが非常に重要**
  - **社外秘の管理データは安全ではない**
    OT 環境には、その企業 IT におけるシステムと同じく、扱いに注意を要する IP や、多くの場合守らなければならない管理されたデータが 含まれています。データの発見と分類が行われなかったので、このデータは適切に守られなければ広範な影響に脆弱性があります。オペレーターやエンジニアは、サイバーセキュリティーを理解しておらず、IT セキュリティーの担当者は OT 環境のことを知りません。その結果、OT 環境にはリスクを軽減する技術やツールがほとんど存在しません。例えば、認証の慣行が弱いことも一般的です。
- **影響**
  - **情報セキュリティー・インシデントによる壊滅的な影響**
    IT ネットワークがハッキングされると、データは損なわれ、盗まれ、失われます。しかし、産業制御システムがハッキングされると、その影響はさらに大きなものになります。生産品質の低下、ダウンタイムにより生産性と収益が低下し、環境汚染、そして負傷や死亡に繋がる可能性があるあ安全の問題となる可能性もあります。
  - **OT セキュリティー対応計画とシナリオの不足**
    ほとんどの OT 企業は、サイバーセキュリティーの脅威に対する対応計画がなく、したがって重大なインシデントが発生しても対処する準備ができていません。

増加し続ける OT 環境への攻撃



この数年間、公表されたオペレーショナル・ネットワークにおけるセキュリティー侵害の影響は大きく、高度化が進んでおり、リスク・ベースのセキュリティー対応への声が高まっています。残念なことに、多くの企業がセキュリティー管理が整っていないため、しばしばその OT 環境におけるセキュリティーの脆弱性に気がついていません。その証拠に、何ヶ月も何年も検出されることなく、これらの脆弱性を利用する侵入者が情報を集め、攻撃を準備します。いくつかのケースでは、この不正行為が攻撃されたときに明らかとなり、損害を被っています。OT セキュリティー対策の実装は、企業が今こそ実施すべき基本的な第一歩です。

03 「どれだけ自分たちは準備ができているか」というOT セキュリティーの優先事項を定めた戦略から始めるOT セキュリティー対策

OT 環境で直面する課題を理解してこそ、適切に守ることができるようになります。

まずは、これらの8つの基本的な質問について考えて、OT セキュリティーに関する現状認識や準備状況の評価から始めましょう。

質問 1

どのような ICS 機器が現場に設置されているか知っていますか？

資産の特定は、OT セキュリティー・プログラムの最も基本的な要素の1つです。何を持っているのか知らなければ、守ることはできません。従って、すべての機器とそれらがサポートするプロセスを特定しなければなりません。どのシステムが、どのように相互接続しているか、そしてどのようなセキュリティー管理がすでにほどこされているかを確認します。どのシステムがモダンなセキュリティー管理をサポートしていないかを知る必要があります。これによって補足する管理を取り付けて、リスクを軽減することができます。

質問 2

OT セキュリティーを管理し、維持するため、担当者を特定して研修を実施していますか？

テクノロジーだけでは、現行の OT サイバーセキュリティー問題に対応するには十分ではありません。さらに、システムを稼働し続ける責任のあるプラント・エンジニアとオペレーターは、セキュリティーに対応する時間と知識がありません。したがって、企業 IT 環境の一部としてセキュリティー担当者がいるように、OT セキュリティーの担当者を OT チームに追加して、OT セキュリティー・プログラムを確立して維持していくことを強く推奨します。この新しい専門分野におけるスキルが不足しているため、大部分の企業はサードパーティーにそのサポートを頼っています。

質問 3

最大リスクに対応するための特定の OT サイバーセキュリティー戦略ならびにポリシーがありますか？

プラントのオペレーションと IT 環境は、根本的に異なります。これらには異なる戦略とポリシーが必要です。セキュリティーの優先事項を定めることが重要です。OT 環境では、安全、プロセスの一貫性、そして可用性は常に最優先事項です。これらの要素に影響を与える脅威は最高のリスクですから、セキュリティー戦略はこれらにまず取り組む必要があります。

質問 4

機器からの出力を信頼できるか？

OT プロセスの一貫性は、ネットワーク上の機器を信頼することができるかにかかっています。その信頼を達成するため、セキュリティー戦略には権限の与えられていない変更に警告を出し、予防する仕組みを含まなければなりません。扱いに注意を要する、重要な、または管理されたデータを特定し、分類し、守ることが必須です。保護には、権限の与えられたユーザーのみにアクセスを制限し、データを使用する際にこれらのユーザーの活動を監視するアクセス制御を含む必要があります。

質問 5

OT 環境内で IT セキュリティー技術を使用していますか？

多くの IT セキュリティー技術は、OT 環境にとって非生産的です。例えば、5回ログインの試行に失敗した後にユーザーをロックアウトするパスワードの認証ポリシーは、エンジニアが重要なシステムの問題を数秒で解決しなければならない産業環境においては時間 (そして、潜在的に安全性) の観点から損害が大きい可能性があります。もっと悪いことには、攻撃者にとって正式のユーザーをシステムから簡単に締め出す方法となるかもしれません。OT セキュリティー管理は、特に OT 環境のために構築されなければなりません。

質問 6

OT セキュリティー・チームは、自社の OT 環境を理解していますか？

システムの文書化と理解なくして、OT システムに影響を与える脆弱性を分離するために必要な継承されたリスクと軽減策を理解することは困難です。これが、IT セキュリティーの担当者に頼るよりも、OT 環境を支援する OT セキュリティーの担当者を持つことが重要です。

質問 7

自社の OT セキュリティー・リスクを完全に理解していますか？

産業環境のデジタル変革の利点は、もちろんそのリスクを上回るものです。しかしそれはリスクを完全に理解して、積極的に管理してこそです。この進化によって、より多くの IIoT とクラウド・コンピューティング・ソリューションの利点をますます活用することになり、OT 環境のリスクの状況に影響を与え続けるでしょう。あなたの会社がその成長と競争力を加速できない理由を、不十分なセキュリティー・プログラムのせいにしないでください。

質問 8

OT 環境において、サイバー攻撃に対応する準備はできていますか？

サイバー攻撃は、OT 環境に破滅を招きかねません。これには、攻撃が成功した場合にも、素早く対応でき、損害を軽減するための、十分に訓練を行った計画が備わっている必要があります。最低限でも、この対応計画には次が含まれている必要があります

- 明確に文書化され、理解された役割、責任と対応シナリオ
- 攻撃されている産業プロセスそして関連している機器をピンポイントで指摘できる能力
- フォレンジックに検証することのできるログファイル
- OT 機器にアクセスしたユーザーのプロフィールとログファイル
- 影響を受けた可能性のあるデータの文書
- 災害回復計画と重要な資産とデータを復元するための冗長性

04 健全な OT セキュリティー戦略の創出

隙のない OT セキュリティーとは、技術だけが重要というわけではありません。プログラムが重要です。

技術は、OT セキュリティー・ソリューションの1つの部分にすぎません。包括的なセキュリティー戦略には、実現する技術に加えて、定義された役割、関与する人々の責任、明確なセキュリティー・プロセス、そして裏付けのあるポリシーが含まれます。

貴社の OT セキュリティー戦略は、基本に焦点を当てるところから始まります。

リスクを理解する

自社にとってリスク、ギャップそして脆弱性とは何か、それらを軽減するための全体的戦略とは何でしょうか？OT セキュリティー構築の取り組みを始めたばかりの企業には、リスクの理解を支援するソリューションを提供します。

IBM® は、リスクを特定するために何が必要か、企業の理解を支援します。適切なレベルのリスク理解を達成するには、段階を追ったアプローチが必要です。

- **OT セキュリティー戦略と計画の策定**
  自社のリスクの特定とリスクに対する耐性を評価を支援するプロセスを提供します。お客様の求める成熟レベルを達成するため、どのようなプロジェクトとプロセスを実装する必要があるかを見極め、実行可能なカレンダーに合わせた計画を設定します。
  – OT セキュリティー戦略と計画策定サービス
- **OT セキュリティー・リスクとコンプライアンス評価の実施**
  リスクとコンプライアンスの評価を実施し、貴社の産業に当てはまる規制と枠組みへのコンプライアンスのレベルを特定します。
  – OT セキュリティー・リスクとコンプライアンス・サービス
- **OT 脆弱性評価の実施**
  脆弱性評価を独自のアプローチで実施します。この精密なプロセスを通して、脆弱性を特定し、環境を守るための軽減計画の策定を支援します。
  – IBM X-Force® Red ICS テスト
- **OT ガバナンスと RACI (Responsible, Accountable, Consulted, Informed) 要件の確立**
  ガバナンスを高めるためのポリシー、手順、役割、責任の策定を支援します。
  – OT セキュリティー・ポリシー、手順および RACI 設計サービス

これらの初期評価と計画立案の段階を社内で実施する能力とスキルがない場合、または、すでにこれらを実施したが、独立した第三者のレポートが必要である場合、IBM の OT セキュリティーの専門家とソリューションなら、リスク発見のプロセスの全行程を支援することが可能です。

可視性を拡張する

優れたセキュリティー・プログラムにおける重要なコンポーネントは、自社の OT オペレーション全体が見えるようにすることです。ご利用中の OT 機器が何かを知り、それらに十分な説明責任を持つことが必要です。ネットワーク設計とインフラをセキュリティーに目を向けて見なければなりません。セキュリティーの対象と分類すべき重要なデータを特定します。システムを使用している人々を見て、安全なアクセス制御ポリシーを策定しましょう。

IBMとサードパーティーによるエコシステムを通じて、私たちは支援とガイダンスを提供します。

- **OT ならびに ICS 機器の発見**
  私たちは、貴社の資産が何なのか、資産管理ソリューションに取り入れる可能性を視野に入れて、正確に特定します。
  – OT セキュリティー資産管理サービス

- **ネットワークの発見とセキュリティー・アーキテクチャーのレビュー**
  お使いの機器がネットワークを通じて相互接続している今、ネットワーク・アーキテクチャーはリスクを管理するために設計されなければなりません。ネットワークのアーキテクチャーとすべてのエンドポイントの両方を評価して、その周辺に戦略を設計します。
  - OT インフラとエンドポイント・セキュリティー・サービス
- **データの発見、分類、解析**
  IT 環境におけるのと同様に、OT においてもデータは重要であり、そのデータの多くは扱いに注意が必要なものです。完全なデータ発見分析を実施するための、サービスと技術を提供しています。
  - OT データ・セキュリティー・サービス
  - IBM Guardium®
- **OT/ICS ユーザー・アクセス・レビュー**
  ユーザー・アクセス管理は、OT 環境において重要です。OT には数多くのサードパーティー業者がおり、従業員の数よりも多くなることもしばしばです。お客様の OT ならびに ICS システムで誰が何をしているかの追跡を、優れたアクセス管理および特権アクセス管理の導入により支援します。
  - OT ID と アクセス管理ソリューション

影響の軽減

リスクが特定され、OT 環境の十分な可視性を得られたら、セキュリティー・ソリューションを実装する時です。お客様と一緒に包括的なセキュリティー・ソリューションを設計、開発そして実装し、専門知識が自社にない場合には、そのソリューションの運用管理を支援します。

お客様の OT セキュリティー戦略を稼働させるまでのその行程全体で、安全であるために必要な支援やガイダンスのすべてを提供します。

- **安全なデータとエンドポイント**
  データがどこにあり、どれが機密性が高く、自社所有のものであるかがわかったら、IBM のサービス、専門家そしてテクノロジーでデータのリスク管理を支援します。
  - OT データ・セキュリティー・サービス
  - IBM Guardium
  - IBM MaaS360®
- **OT ID と アクセス管理 (IAM) ソリューションの計画と実装**
  IBM のスペシャリスト、ソリューションそしてサードパーティーのパートナーが、誰がシステムにアクセスしたが、いつアクセスしたか、そしてのアクセス中、どのような活動や変化が起きたかを常に把握できるように支援します。
  - ID と アクセス管理ソリューション
- **OT セキュリティー・オペレーション・センター (SOC) の設計、構築、最適化**
  OT SOC は、使用例、ポリシーそしてインシデント対応の点で、企業の IT SOC とは非常に異なります。OT 環境の特別なニーズに合わせて、お客様の SOC 設計および最適化を支援します。
  - セキュリティー・インテエリジェンスと オペレーション・コンサルティング
- **OT ネットワークと SOC セキュリティー・サービスの管理**
  お客様の OT 環境に常に合うようにネットワークとファイヤーウォールを管理していくことが可能です。また、OT 環境に最適化されたグローバルなマネージド・セキュリティー・サービスを通じて、貴社の OT セキュリティーを支援することも可能です。
  - マネージド・セキュリティー・サービス
- **OT セキュリティー・インシデントへの対応**
  OT インシデントへの対応は、IT とは異なり、より複雑です。OT エンジニアとオペレーター、ベンダー、請負業者と協力し合うことになります。それは時として労働組合の環境下ということもあります。そのようなユニークな状況に合わせたインシデント対応計画、様々なシナリオに対応したプレイブック策定を支援し、そして攻撃が発生した場合、フォレンジック・サービス、バックアップ、復元ソリューションを提供します。
  - IBM X-Force IRIS
  - IBM Resilient®
  - IBM Resiliency Services®

05 IT/OT のギャップを橋渡しする IBM Security ソリューション

IBM の OT セキュリティー・サービスは、様々な成熟度のお客様がそれぞれの OT セキュリティーの状況を改善させ、OT セキュリティーへの投資が迅速に価値を生み出すようにアプローチしていきます。

IT セキュリティー・ソリューションは、OT セキュリティーの課題に対応するために設計されていません。そしてテクノロジーのみに依存した OT ソリューションは、効果的ではありません。それは、優れた設計の OT セキュリティー戦略の一部でなければなりません。

IBM は、IT セキュリティーにおける世界的リーダーとして認知されており、IT 環境と同様に、企業がセキュリティー・リスクの理解、可視性の拡大そして重大な影響を防止することができるように長年の支援実績があります。世界中の企業が、自社の OT セキュリティー構築の取り組みに対する IBM の支援に信頼をおいています。お客様にも同じ体験を提供させていただきます。

なぜ IBM なのか？

- **専門性**
  OT のベスト・プラクティスに基づいた設計、実装、研修、管理に必要となるガイダンスを得ることができます。IBM は、拡大し続ける OT 業界の知識を持つセキュリティー業界のリーダー企業の一社です。IT と OT 両方の世界の最高のものを、お客様のユニークな環境にご提供します。
- **テクノロジー**
  クラス最高の技術を使用して、お客様の OT インフラ全体を単一のビューで把握することができます。市場をリードする OT 向けセキュリティー製品と必要となるすべてのインテグレーション技術が揃っています。
- **パートナー・エコシステム**
  オープンなパートナー・エコシステムを活用して OT リスクを管理します。

評価から実装、監視とサポートまで、IBM の総合的な OT セキュリティーへのアプローチにより、資産、データそして人々を安全に守ります。世界の OT セキュリティーのプロフェッショナルを雇用、訓練して、サイバーセキュリティーにおける知識と経験を活用して、OT 環境へと提供サービスを拡充しています。そして、さらなるサービス向上のため、業界の主要な OT セキュリティー・ソリューション・プロバイダーとパートナーシップを結んでいます。

IBM Securityは、Fortune 500の上位100社の95%を保護しています

- 世界**最大**の郵便ならびに小包会社 6 社
- 世界の**トップ10**の航空会社のうち 8 社
- 世界の産業資材**メーカーのトップ10社**のうち 8 社
- **世界**のエネルギーおよび公益企業**トップ30**社中 27 社
- 世界**最大手**の通信会社 10 社
- 世界**トップ50**の金融サービスおよび銀行会社のうち 49 社
- グローバルテクノロジー企業 **トップ15社**のうち 13 社
- 世界**最大**の食料品店およびドラッグストア 10 店
- 世界の小売および消費財企業**トップ25**社のうち 22 社
- 世界のヘルスケア企業**トップ15**社のうち 14 社
- 世界の自動車および部品の**トップ20**社のうち 19 社

06 さらに詳しく

IBM が、新たにデジタル化された OT 環境を保護するという課題を乗り越えるため、どのようにして完全な戦略策定を支援するのか、詳細をご覧ください。

詳細情報 →

IBM Security