シスコ IoT eBook

産業向け サイバーセキュリティ：

モニタリングと異常検出

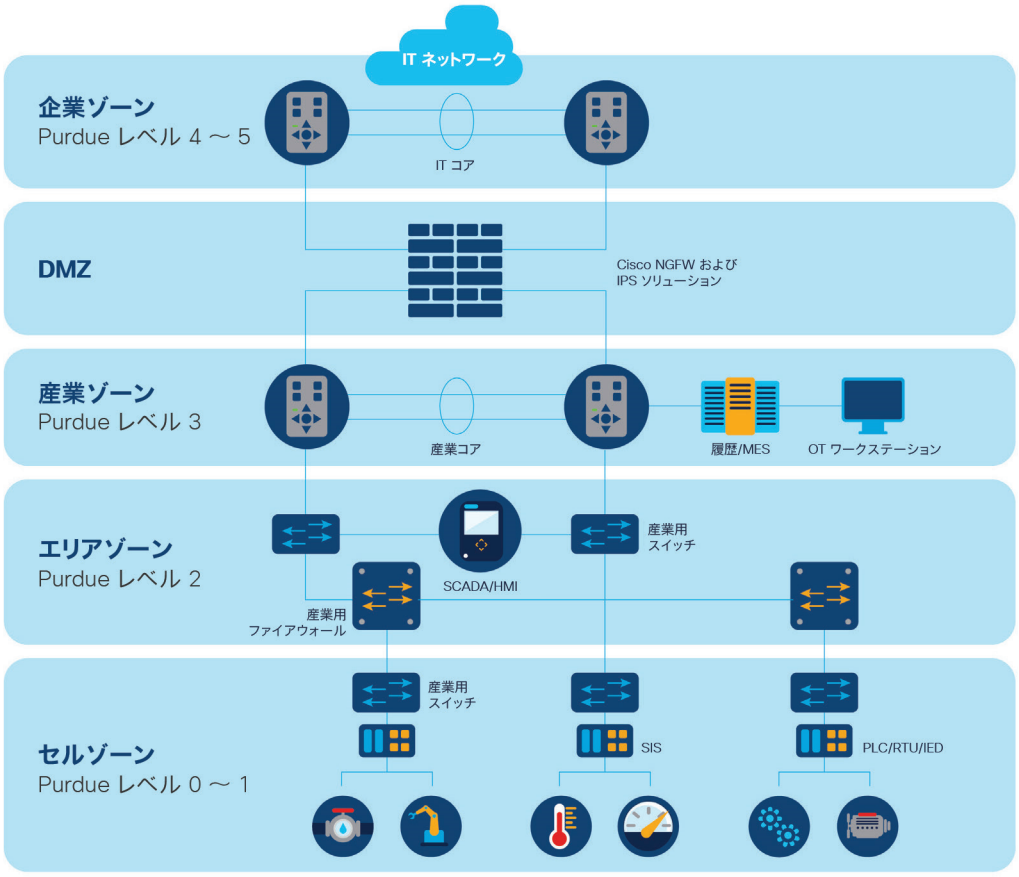
cisco

背景

産業用制御システム（ICS）は、水、ガス、送電ネットワーク、発電所などのライフラインをはじめ、生産ライン、輸送ネットワークなど、あらゆる場所に存在します。

ICS はこの数十年間に開発・導入され、産業組織における生産インフラストラクチャや重要設備の運用に役立ってきました。また、業界横断的な組織（ISA、IEC など）やセクター別の組織（原子力業界の IAEA、鉄道業界の CENELEC など）によって策定された国際規格に準拠しています。

ICS の構造は、ISA95 および IEC-62264 規格で定義されている以下のモデルで表されます。



産業 - レベル 0 - フィールド：センサー、アクチュエータ、モーター

産業 - レベル 1 - プロセス：オートメーションデバイス、安全システム、コントローラ

産業 - レベル 2 - 監視：SCADA ステーション、DCS オペレータステーション、エンジニアリングステーション

産業 - レベル 3 - 製造業務：MES、LIMS

IT - レベル 4 および 5 - ビジネス：オフィス、PC、メッセージング、イントラネット

技術的な特性だけを見れば、IT と見なされるネットワークを分類することは困難な場合が少なくありません。実際、2000 年代以降、産業システムは従来の IT コンポーネント（Microsoft Windows、イーサネット、IETF、TCP/IP など）を ICS ネットワークに統合しており、その区別をさらに難しくしています。ですが、産業用制御ネットワークを正確に定義する方法があります。**以下の 5 つの特性のうち、少なくとも 4 つが満たされていれば、産業用制御ネットワークと見なせます。**

- 物理プロセスの運用と監視を目的としている。
- 特定のハードウェア抵抗（最大 70 °C、12V または 24V DC 電源、防塵、IP レベル 20 ～ 80 など）を必要とする環境に導入されている。
- IEC 標準通信プロトコルまたは認定メーカー（下記 ICS デバイスメーカーのリストを参照）の独自プロトコルを使用している。
- 低帯域幅の「マシンツーマシン」通信（10 ～ 100 Mbps のローカルエリアネットワーク、512 kbps のリモートネットワーク）で構成されている。
- IT テクノロジー（HTTP IETF プロトコルなど）の使用は、Web 管理、SNMP、ICMP モニタリングなどの管理処理に限定されている。反対に、「ユーザ」による通信（Web サーフィン、メッセージングなど）は発生しない。

産業用制御システム

ABB、Ansaldo、Bombardier、Beckhoff、Belden およびその子会社（Tofino、Hirshmann）、Emerson、General Electric、Honeywell、Moxa、Pilz、Schneider およびその子会社（Invensys、Foxboro、Telemecanique、Modicon）、Siemens、Yokogawa、Wago、その他

リスクの状況

従来の IT の世界では、データとシステムの機密性、整合性、可用性を損なう脅威がリスクとされてきました。被害は主に金融関係に多く見られます。たとえば、恐喝（Cryptolocker ウイルス）、銀行詐欺、e コマースサイトで利用されている Web サーバに対する DoS 攻撃などが該当します。

産業用制御システムは、オペレーショナル テクノロジー（OT）が利用されている物理的環境を制御するシステムです。ICS 環境に存在するリスクには、運用上の安全性（商品や人の物理的安全性、環境への影響）や可用性、さらには、生産ツールの物理的整合性を損なう脅威などがあります。また、重要な産業データの盗難も大きな脅威となっています。産業データには経済的影響と同時に社会的影響もあり、責任者の民事責任および刑事責任も問われます。

これまでに特定された脅威媒体

消費者ベースのネットワーク（脅威媒体はインターネットを介したものがほとんど）とは異なり、ICS では、悪意のあるプログラムが **USB キーを介して**侵入するか、ICS を運用するステーションにマルウェアが侵入して拡散することが脅威となっています。

リモート診断やリモートメンテナンスを行うには、ネットワークと産業用制御システムへのリモートアクセスが必要です。リモートアクセスはさらに深刻な脅威媒体と言えます。重要度の異なるネットワークを相互接続し、時にはサードパーティが介在するからです。

リモート アクセス ワークステーションは、重要な産業用制御システムの中心部に接続し、重大な影響を与えうる操作（ソフトウェアの更新や新しいファームウェアのダウンロードなど）を実行します。これを単純に禁止することはできませんが、**効果的な監視メカニズムを通じて制御する必要があります。**

これらの脅威媒体の大部分は産業界に特有のものです。産業用制御システムで講じられるセキュリティ対策では、運用上の現実が考慮されていなければなりません。OT 運用スタッフが継続的に設備を運用でき、作業を効率的に進められるようにする必要があります。単にすべてのリモートアクセスを禁止したり、アクセス制御や組織的対策だけに頼るわけにはいきません。

OT システムは悪意のあるアクティビティを防止するように設計されていない

加えて、産業用制御システムは、サイバーセキュリティの脅威に対応するようには設計されていません。ICS は、運用上の安全性と運用の継続性を確保する目的で作られており、悪意を持って侵入しようと試みる者がシステムのデジタルインターフェイスに到達できる可能性を考慮していない場合も少なくありません。

これまでのオートメーション製品にサイバーセキュリティ機能がほとんど備わっていないのはそのためです。さらに、ほとんどの産業組織では、サイバーセキュリティ機能を有効にしていません。

独自プロトコル

産業用システムは、ネットワーク上のコンポーネント間の通信を可能にする、一連のプロトコルに基づいて構築されています。MODBUS や PROFINET などの標準規格もありますが、**制御システムの再プログラミングや変更のためのプロトコルは、ほとんどが独自仕様であり非公開です。**大半の規格（Siemens、Schneider、ABB、Rockwell Automation など）のプロトコルは、知的財産上の理由により、今後も公開されることはないでしょう。

そのため、プロトコル準拠テスト（すべてのメッセージのシンタックスやセマンティックが標準規格に準拠しているかどうかの検証）をはじめとする IT 技術を適用することができません。この技術は、オープン標準（MODBUS など）に基づくメッセージ部分（プロトコルヘッダー）では有用ですが、非公開プロトコルに適用するのは非常に困難です。

対象となる運用上のイベント

さらに、ネットワークの観点からすると、本質的に、プログラマブル ロジックコントローラ（PLC）に送信される「STOP」コマンドが悪意を持ったものかどうかを判別することはできません。**メンテナンスのための処理である場合もあれば、マルウェアである場合もあります。**いずれにしても、ブラックリストベース設計を使用する従来型の侵入検知システム（IDS）のように、「STOP」コマンドを「攻撃シグニチャ」と見なすことはできません。そのため、「STOP」コマンドを受信するたびにセキュリティイベントを生成して一元管理し、コンテキストと履歴(「誰が、何を、いつ（繰り返し）行ったのか」）を追跡するソリューションを通じてコンテキスト化する必要があります。

ICS 攻撃戦術の概要

効果的な ICS サイバーセキュリティ戦略を構築するには、最も発生率の高いセキュリティイベントを特定することが重要です。これにより、標的となる可能性が最も高い資産を保護するうえで最適な対策にフォーカスでき、攻撃者による ICS 侵入の標的となる可能性がある機密資産のセキュリティを強化することができます。

脅威となるサイバーセキュリティ イベント

産業用サイバーセキュリティ分野で脅威となるセキュリティイベントの 1 つに、産業情報システムに対するサイバー攻撃があります。企業運営、生産ツール、生産出力、さらには従業員や顧客にまで重大な被害が及ぶ可能性があるからです。これらのイベントは現実世界において物理的な被害を実際にもたらします。場合によっては、企業の経営陣を狙った犯罪につながる可能性もあります。

以降では、3 種類のイベントについて説明します。
各イベントは、以下の 3 つのセクションに分けられています。

分類	攻撃者の目標、ターゲット、影響、技術的手段
説明	攻撃者の動機とプロセス
プロセス	攻撃シナリオの詳細

サイバーキルチェーン

このドキュメントでは、サイバー攻撃のシナリオを体系化して各フェーズの詳細を示すために、「サイバーキルチェーン」という概念を使用します。この概念を使用すれば、最近の攻撃で多く見られる複雑な侵入行為の構造を詳細に説明することができます。

サイバーキルチェーンの各ステージは、認識、武器化、デリバリー、実行、インストール、コマンド & コントロール、目的達成のためのアクションに分けられます。以下で紹介する恐ろしい事例では、攻撃者がすでに産業用制御ネットワークに「接続している状態」であることが想定されています。攻撃者はそれまでのすべてのステージを突破し、インストールの段階まで到達しています。攻撃に関与しているのは、外部から産業用ステーションに侵入した悪意のあるプログラムである可能性もあれば、システムへの物理的なアクセスが可能な人物である可能性もあります。

したがって、攻撃者がすでに突破したものと見なされる以下のステージについては、詳しく説明しません。

- 対象組織の人間およびテクノロジーによる認識（組織のソーシャルネットワーク、公開入札、出版物など）
- Web または電子メール経由で送信されたマルウェア（ウイルスに感染した MS Office ファイルや PDF ファイル、罠が仕掛けられたビデオゲーム、「水飲み場」型 Web サイト）を介した武器化とデリバリー
- 産業用ネットワークとの相互接続ポイントへの水平拡散によるインストール、または産業用制御ネットワークへの侵入（具体的には、エンジニアリングステーションを含むプロセス制御ネットワークへの侵入）

組織の弱点を知る

攻撃者がどのようにして標的となる産業用ネットワークに侵入するかを理解することが極めて重要です。監視プロセスを設計する際に考慮すべき脆弱な侵入ポイントは多数あります。これらは、侵入の可能性の高さに基づいて以下のように分類されます。

1

産業用ステーションの乗っ取り

攻撃者は標的とした IT 伝播メカニズムを利用して、産業ドメイン内のワークステーションに到達するまで、標的ネットワーク内でマルウェアを伝播します。主なターゲットは、プロセスに関する重要情報（プログラミングで使用されるセットポイントや変数など）が保存されている監視制御システム(SCADA) とエンジニアリング ステーションです。

2

サードパーティに対して認可されたリモートアクセスへのなりすまし

攻撃者は再委託先などのサードパーティに対して認可されたリモートアクセスを利用します。オープンになったままの ADSL や VPN 接続、あるいは特定の IP アドレスに対してのみ使用される ADSL 接続や VPN 接続が利用される可能性があります。多くの場合、これらのリモートアクセスには産業施設の中心部へのアクセス権が付与されているため、攻撃者にとって「質の高い」侵入ポイントとなります。

3

ワイヤレスリンクのハイジャック

攻撃者は、使用されているワイヤレスリンクの公開済みの脆弱性または固有の脆弱性を利用します (WEP または WPA に対する既知の攻撃)。そうすることで攻撃者は産業用制御ネットワークに接続します。その後、エンジニアリング ステーション、SCADA ステーション、PLC システムの中心部に直接アクセスします。

4

ターゲットのフィールドネットワークへのアクセス

攻撃者は施設のフィールドネットワークへ物理的に直接アクセスして攻撃を実行します。たとえば配水軸 (下水道のパイプラインやダクト) を通じてコンピュータキャビネットにアクセスします。フィールドネットワークでは、入出力モジュールの制御に使用される ICS 機器に直接アクセスできます。これは運輸セクターにおいて特に重要です。

5

ネットワークをリモートで変更するための異質な物理コンポーネントのインストール

侵入口となる場所に直接立ち入ることなく物理的なアクセスを可能にするために、攻撃者は産業用ネットワークにリモート制御モジュールをインストールします。たとえばバッテリと 4G モデムを備えた小型の Raspberry Pi 使用すれば、リモートアクセスしてネットワークを制御できます。

脅威事例 A：知的財産の盗難

分類

- **攻撃者の目的**：プロセスデータや産業データの窃取
- **ターゲットの種類**：製造プロセス（個別）、非分散型
- **影響**：データの機密性が損なわれる
- **技術的手段**：ターゲットの PLC プログラムのダウンロード

説明

知的財産の窃取は、価値のあるプロセスデータや産業データを盗み出すことを目的とした、産業用制御システムに対する攻撃です。**攻撃者の動機としては、以下が考えらます。**

- **経済的動機**：競合他社から製造に関する機密情報を盗み出し、コピー製品や作製したり、製造方法を模倣したりする。
- **愛国的動機**：航空機や兵器（フリゲート艦や潜水艦など）といった国家機密に関わる製品の製造計画を盗み出して複製する。

攻撃者の最終的な目標は、ターゲットが対策を講じられないように検出を逃れて、目的のデータを盗み出すことです。プロセス自体には変更を加えず、システムの機密性を損なうことだけを目的としています。

攻撃は長期間にわたって行われます。つまり、攻撃者はアクセスを可能な限り長く維持するか、少なくとも必要なデータをすべて抽出できるまではアクセスを維持しようとします。物理的に直接アクセスできない場合、攻撃者は、産業用制御ネットワークにインストールされたマルウェアと攻撃者のコマンド & コントロール サーバの間の「制御」接続を維持する必要があります。

プロセス

1. PLC に接続する：プログラムの抽出、変数の抽出
2. エンジニアリング ステーションからの PLC プログラムの漏洩
3. モニタリングステーションからの機密データの抽出
   （プログラム、シノプティックス、セットポイント、アラームしきい値）
4. データベースに保存されている情報の抽出（履歴）
5. データを取得したら、最後にインターネットまたはリムーバブルメディアを介して可能な限り慎重に必要なデータのみを抽出する必要があります。データ量が膨大な場合、この作業は極めて複雑になることがあります。

脅威事例 B：産業破壊活動

分類

- **攻撃者の目的**：産業プロセスの改ざん
- **ターゲットの種類**：製造プロセス（個別または連続）
- **影響**：産業プロセスの整合性が損なわれる
- **技術媒体**：1 つまたは複数のコントローラのプログラムの変更、SCADA 監視の誤誘導

説明

以下のシナリオでは、生産妨害につながる産業用製造システムに対しての攻撃を紹介しています。攻撃者の動機は、サイバーテロ、競合他社に対する妨害活動、さらには 2 国間の戦争行為にまで及びます。

攻撃者は、検出を逃れることにより産業プロセスに影響を与えようと目論見ます。データを盗み出すことが最終目標ではありません。このシナリオでは、産業プロセスに永続的かつ検出不可能な変更が加えられることにより、プロセスがもはや通常の機能を果たさなくなり、不適合製品が生産されるようになります。**この目的を達するために、攻撃者は以下を試みます。**

- 産業プロセスとその制御システムに変更を加えられるよう、可能な限り詳細な知識を入手する。これにはアーキテクチャのデータ（ネットワーク計画、構成など）だけでなく、圧力、温度、回転速度などの純粋な産業データも含まれます。攻撃者がこれらのデータを誰にも気付かれずに変更するには、公称値やアラートしきい値を入手する必要があります。
- 産業プロセスの詳細を調べ上げた後、一部のコントローラのプログラムを変更して、産業プロセスを改ざんする。改ざんが発覚するのを防止するには、SCADA ステーションを制御して、誤った情報を表示したり、アラームしきい値を変更したりしなければならない場合もあります。

プロセス

このシナリオは、論理的にはシナリオ A の延長線上にあります。途中まではシナリオ A と同じ攻撃手順が使用されますが、その後の手順が異なり、シナリオ A よりも格段に複雑になります。

コントローラプログラムを抽出した後、攻撃者はプログラムを変更し、コントローラに再注入して産業プロセスを改ざんします。攻撃者は、プロセスが監視されている可能性を考慮して、慎重に変更を加える必要があります。

以下は、遠心分離機の回転速度の変更を目的とした Stuxnet 攻撃の事例に関する概要説明です。ただし、攻撃者がプログラムを変更したのか、オペレーティングシステムの低レベルコンポーネントのソフトウェア（ドライバ）を変更したのかは確認されていません。

このシナリオに登場する攻撃者は、コントローラにインストールされているプログラムを直接変更することを選択していますが（これは確認可能である場合があります）、変数の値に直接アクセスしたり、産業用機器と通信するソフトウェア（監視ソフトウェアなど）を変更したりすることもできます。

脅威イベント C：産業施設に対するサービス妨害（DoS）攻撃

分類

- **攻撃者の目的：**稼働停止の誘発
- **ターゲットの種類：**連続的な分散型プロセス（製油所、水、ガス）
- **影響：**産業プロセスの稼働に障害が生じる
- **技術的手段：**コントローラの機能停止

説明

このシナリオは、より直接的に産業活動の妨害を目的としています。**目標は産業プラントの連続稼働プロセスを停止させることであり、**製油所、水処理プラント、ガス配給ネットワークなどがターゲットとなります。

攻撃者は、インフラストラクチャの一部を制御して機能不全に陥れ、生産ツールに物理的な損傷を与え、サービスの復旧を極めて困難にします。こうした施設が稼働停止に陥ると、その施設に依存するすべての利用者に直接影響が及び、人命に関わる可能性もあります。

また、この種の施設は多くの場合、分散されています。施設が極めて広域に分散されているため、攻撃者は、インターネットを介さず、物理的に施設を乗っ取ることができます。

プロセス

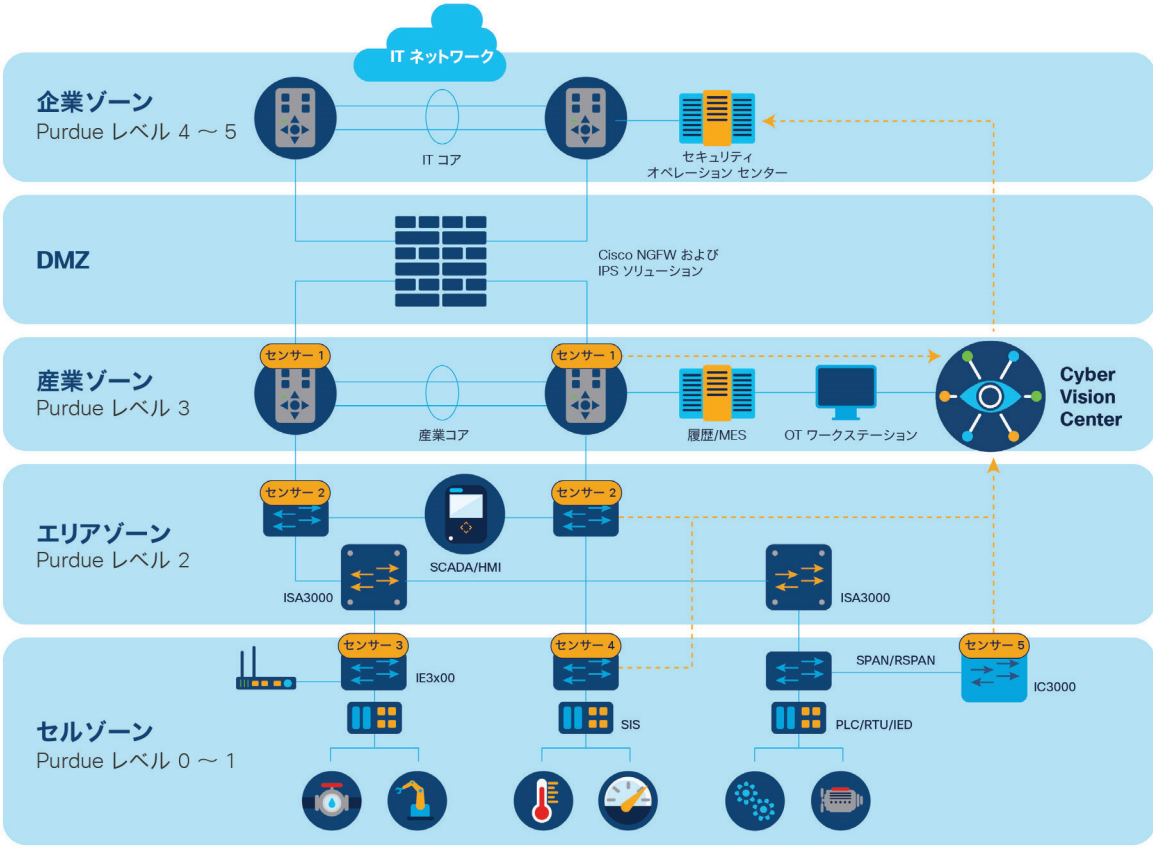
このシナリオに登場する攻撃者は、サービス妨害（DoS）攻撃を通じて、アクセス可能なすべてのコントローラまたは一部のコントローラを機能不全に陥れます。利用できる技術的手段には以下のものがあります。

- **ネットワーク飽和によるサービス妨害：**コントローラが応答不能または機能不能に陥るまで、大量のトラフィックを生成し続ける。この手法は、IT 分野でよく知られているサービス妨害（DoS）攻撃に似ています。
- **再プログラミングによるサービス妨害：**産業ネットワークに直接アクセスして、正常に機能しないプログラムを PLC（プログラマブル ロジック コントローラ）にインストールする。

モニタリングシステムと異常検出

多くの場合、産業用制御ネットワークは地理的に分散され、コンポーネントの少ない多数の「小規模ネットワーク」で構成されています。複雑でコストのかかるインフラストラクチャを展開せずにすべてを監視できるようにするため、検出システムは一般的に以下のコンポーネントで構成されています。

- センサー：デバイス間の通信データを抽出するプロセスの近くに配置されます
- 中央サーバ：センサーによって収集されたデータを集約、保存、分析します



センサーは、産業システムのさまざまな相互接続ポイントを監視できるように配置する必要があります。

センサー 1： IT ベースのネットワークと OT ネットワークの間の相互接続（履歴データフロー、統計情報、ドライビング）

センサー 2： PLC と Windows マシンの間のプロセスネットワーク（監視・制御コマンドフロー、SCADA ステーション、エンジニアリング）

センサー 3： ワイヤレス相互接続またはリモートメンテナンス（DSL、LTE、または MPLS ルータ）

センサー 4： 制御システム間、および制御システムと安全システムの間のフロー制御

センサー 5： 物理的にオープンなフィールドネットワークとの接続

上記のリスクに対応するため、検出システムは次のような各コンポーネントのプロパティ、制御メッセージ、各種マーカーを分析します。

- **識別プロパティ**：MAC アドレス、プロトコル ID、TCP ポート、UDP ポート
- **インベントリプロパティ**：ベンダー名、PLC 名、プロジェクト名、プロジェクトバージョン、モデル名、ファームウェアバージョン、ハードウェアバージョン、ハードウェアシリアル番号、ロケーション / スロットサブモジュール、製品コード、コンポーネントのロール（SCADA、エンジニアリング）
- **コントローラ / PLC のシンプルな制御**：PLC との間でのプログラムのダウンロード、停止 / 開始コマンド、クロック変更、ファームウェアアップデート
- **高度なコントローラ /PLC 制御**：PLC プログラムの内容、プログラムメタデータ（プログラミングブロックのリスト、タイムスタンプ、サイズ）、認証データ（ログインおよびパスワード）の監視、残存データベースの変更、メモリ消去、メンテナンスモードへの変更、診断モードへの切り替え
- **プロセス制御**：書き込み / 読み取りコマンド、変数 / レジスタのリスト
- **侵害の兆候 (IOC)**：産業用ステーションまたは HTTP/FTP メタデータを検索条件にした DNS クエリ。これらの IoC は、産業用ステーションにインストールされたマルウェアと通信するコマンド アンド コントロール サーバのアクティビティを示している可能性があります。

いわゆる「コントローラのシンプル制御」コマンドが攻撃者にさまざまな可能性をもたらすことを理解することが重要です。検出の観点からは、ネットワーク上でこれらのコマンドを検出する方法を理解する必要があります。

産業システムのサイバーセキュリティの監視に必要な情報を抽出するには、プラットフォームにより産業ネットワーク上で収集されたアプリケーションフローを復号する必要があります。**これらのフローでは、次のようなネットワークプロトコルが複数使用される場合があります。**

- 仕様が公開されていて容易に利用可能なオープンプロトコル。国際機関によって標準化されたプロトコルがこれに該当します。
- オープンプロトコルに追加された独自の拡張機能このような拡張機能は、オープンなデータ領域を使用しますが、ドキュメント化されていない独自のデータ構造が組み込まれています。
- 仕様が公開されていない独自のプロトコル

残念ながら、制御システムの変更（プログラムやパラメータの変更）に利用されるのは、独自仕様のプロトコルです。

シスコ IoT eBook

産業向け サイバーセキュリティ：

モニタリングと異常検出

産業向けサイバーセキュリティ プロジェクトの開始

ネットワークのセグメント化を開始するために自社の産業資産を総点検する必要がある場合であれ、侵入や異常動作の検出を目的とした ICS アプリケーションフローのライブモニタリングが必要な場合であれ、Cisco® Cyber Vision を使用すれば、今後の方針を定めて、サイバーセキュリティ ポリシーを OT の領域にも適用することができます。

Cisco Cyber Vision は産業ネットワークを完全に可視化できるように設計されています。そのため、プロセスの整合性を確保し、安全なインフラストラクチャを構築して、規制に準拠し、セキュリティポリシーを適用することで、リスクを制御できます。

独自のエッジ監視アーキテクチャとシスコの主要なセキュリティポートフォリオとの緊密な統合により、Cisco Cyber Vision は広範囲にわたって容易に導入でき、生産工程の継続性、復元力、安全性を確保できます。

詳しくは https://www.cisco.com/c/ja_jp/products/security/cyber-vision/index.html にアクセスするか、こちらから地域のシスコ アカウント担当者にお問い合わせください。

Cisco-IoT-CyberVision-EB-02202020