<テリロジーICS読本>

ICSインフラのセキュリティ概論

～プロトコルとネットワークアーキテクチャ～

株式会社テリロジー

エグゼクティブフェロー　新美竹男

（注）以下のドキュメントは**INCIBE**(Spanish National Cybersecurity Institute)の「Protocol and Network security in ICS infrastructures」を参照して筆者が抄訳したものである。

1 はじめに

インターネットの普及、ネットワーク接続性と処理能力を備えたハードウエアデバイスの大幅な進歩により、産業分野の重要インフラにも新たなセキュリティ課題が浮上してきた。このような重要インフラは、通常、関連の産業分野で代表的な制御プロセスを監視および生産管理するために産業用制御システム（ICS）が用いられ、外部システムとの相互接続によって、サイバーセキュリティ脅威にさらされるようになった。最近の IPA 調査では、サイバー攻撃の脅威が、産業インフラでも多々検出されるようになり、海外のハッカーによる悪意な攻撃の標的になっていることが報告されている。下図からもわかるように、産業インフラに関連するインシデントが多発していることが分かる：

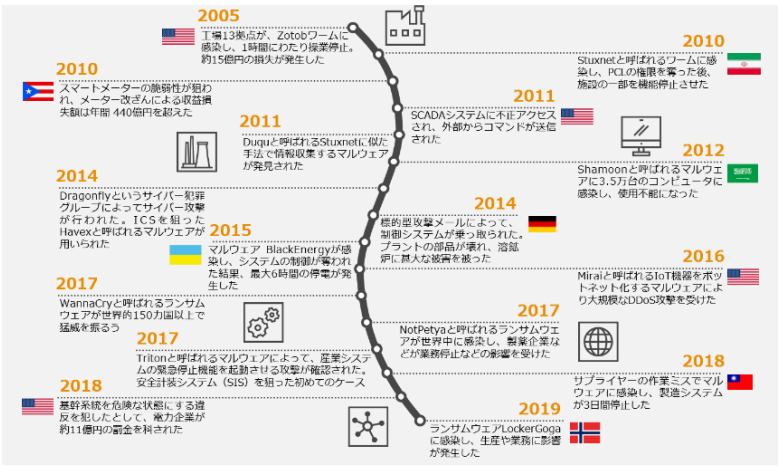


図１. *ICS* 脅威の変遷

（出典：PwC https://www.pwc.com/jp/ja/knowledge/column/awareness-cyber-security/cyber-intelligence03.html）

ICSセキュリティの専門家として著名なマリナ・クロトフィル(Marina Krotofil) 氏によれば、重要インフラを扱うセキュリティコミュニティでは、境界線(Perimeter)やネットワ

ークセグメントを守るのにITセキュリティ対策だけでは不十分であることは明らかだ。つまり、ICSセキュリティ対策では、脆弱性ポイント、攻撃ベクトル、およびその他考えられる多層防御策を考慮し、産業プロセスに関連する制御プロトコルを詳細に理解することが重要である。

1.1. ICS ネットワークアーキテクチャ

セキュリティの立場から、ネットワークアーキテクチャを設計する場合、ネットワークセグメントを明示したモデルは重要である。ネットワークを機能や役割の異なるセグメントに分離することで、セキュリティ対策をより細かく適用し、不要な情報の流れをシャットアウトする。ICS ネットワークセグメントは、企業 IT ネットワークから分離しておく必要がある。これは、トラフィックの性格上明らかに異なるためである。企業 IT ネットワークでは、インターネット、電子メール、ファイル転送プロトコル（FTP）などのサービスが通常であり、ICS ネットワークがこの IT ネットワークに接続するとリスクが伴う。従って、様々な ICS セグメント間のトラフィックを制御するゾーンを考慮した適切な設計は、ネットワークアーキテクチャの安心・安全な実装に向けた最初のステップである。ICS インフラのネットワークアーキテクチャでは、様々なレベルを確立する。各セグメントレベルは、プラットフォームの各レイヤーの役割に従って分類される必要がある。IT システムと OT 制御システムの統合に関し、ISA-95 業界標準/国際計測制御学会（ISA）によって提唱されている ICS アーキテクチャは、このレベルでの分離モデルである。この標準モデルは、図 2 に示すように、異なる機能を持つレベルを 5 つの論理レベルは“Purdue モデル”と呼ばれている。この Purdue モデルにより、各レベルで特定の施策を定義し、相互間のデータフローの安全なメカニズムを確立するセキュリティ戦略の設計が簡素化されている。

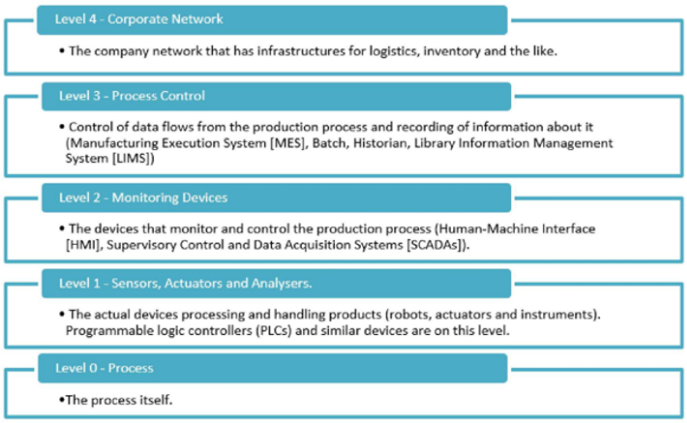


図 2. ICS レファレンスアーキテクチャ

2.1. ICS ネットワークにおける基本的なセキュリティ

Zone で区切られたネットワークアーキテクチャに基づき、ネットワークを必要な数のセグメントに分割して、それらを区分し、適切なセキュリティデバイスとトラフィック制御の配置を準備する必要がある。この分割は、ネットワークアーキテクチャを設計する時に効果的かつ不可欠な概念であり、ICS にも同様に適合できる。

これは、ドメイン間のデータフローにおいて適切な制御によって、ドメイン内のデバイス侵害によって引き起こされる損害を最小限に抑える。

2.2. ネットワークセキュリティ

ICS インフラのネットワークセキュリティは、ネットワークセグメントを分離および保護するためのソリューションモデルを組込むことで達成できる。以下に示す：

ゾーンのセグメンテーション：これは、ISA-95 提唱の標準規格に出来るだけ準拠するように、ネットワークアーキテクチャを機能別ゾーンに分割する。図 3 の ISA-95 モデルからもわかるように、制御ネットワーク、DMZ、および企業 LAN を分離して、少なくとも 3 つのエリアが必要。この対策により、感染を 1 つのゾーンに封じ込めることができ、これにより他のゾーンに拡大することを防ぐ。

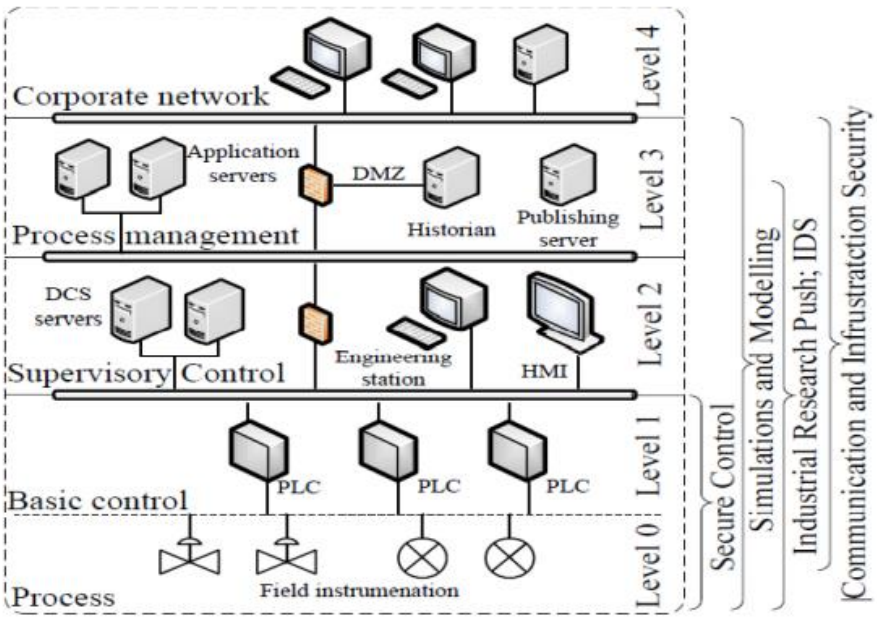


図 3. レファレンスアーキテクチャ ISA-95 モデル.

- VLAN および VPN 技術を使用したネットワークセグメント間の**通信の暗号化と論理的**

分離：この対策は、感染が 1 つのレイヤーから別のレイヤーに拡大するのを防ぐのにも役立つ。

- ネットワーク（IP）とポート、プロトコル、およびアプリケーションレイヤーの両レベルでトラフィックと通信を識別および分離することを目的としたファイアウォール、プロキシーによる**トラフィック制御とフィルタリング**：この対策は、ゾーンを変更しようとした時の感染を検出するのに役立つ。更に、ネットワーク上の IDS や SIEM で、イベント、侵入アラート、ログを管理する場合、その構成は図 4 に示す。
- **データリンクレイターとアプリケーションレイヤーにセキュリティを拡張**すると、802.1x に準拠したアクセス制御、MAC アドレスによるフィルタリング、WAF を使用したアプリケーションレベルなど、データリンクレイヤーのセキュリティ対策が可能である。
- ホワイトリストに基づくアクセス制御、認識されたデバイスへのアクセスルール、及びその他へのアクセス拒否。
- **ワイヤレスネットワーク**には新たなリスクが伴う。その場合、IEEE 802.1x メカニズムが認証に使用され、証明書を使用してクライアントを認証する拡張認証プロトコルの EAP-TLS が含まれるか、RADIUS サーバーが使用される場合がある。アクセスポイントは、分離されているか、ICS との相互接続が限定的なネットワーク上に配置される必要がある。WPA2 などのワイヤレス通信用の堅牢なプロトコルが導入され、更に一意の識別子（SSID）が使用され、ブロードキャストは非アクティブ化され、MAC アドレスでのフィルタリングが動作する。

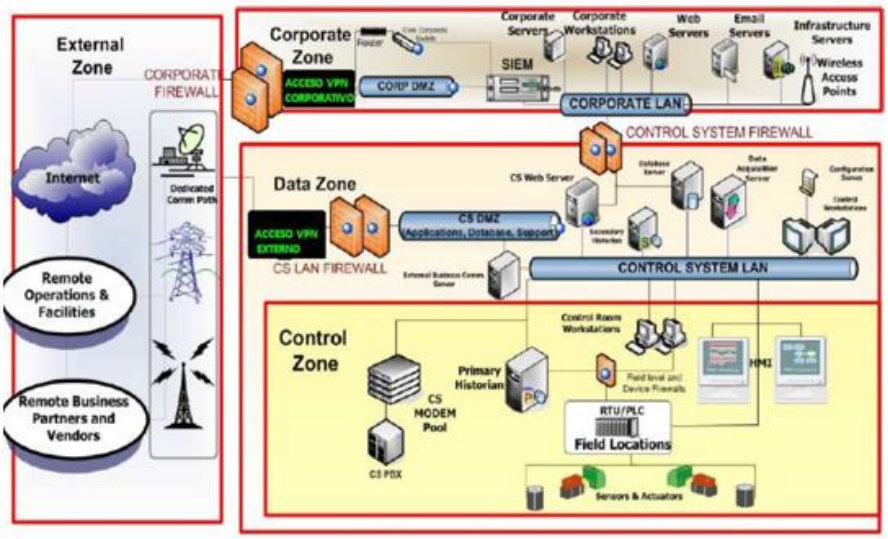


図 4. ネットワークセグメンテーションと通信制御

2.3. 通信の暗号化

殆どの産業用制御プロトコルは、実装に暗号化を組み込んでいない。
従って、ネットワークへの不正アクセスが成功すると、攻撃者はトラフィックを検査および操作出来てしまう。このため、HTTPS、SSH、及び SNMP-3 を使用している。

2.4. 認証とアクセス制御

ロールベースのアクセス制御（RBAC）は、認められたユーザのシステムアクセスを制限するコンピュータセキュリティ手法の一種で、特権管理は、各プロファイルに設定された制限を通じてセキュリティを強化する。従って、様々なユーザプロファイルを作成し、その機能に応じてそれぞれに運用上の役割を割り当てることは、価値のある補完手段となる。警告メッセージなどの対策を追加すると、意図しないエラーの可能性に対するガードとしてアクセスされているサービスを特定するのに役立つ。

2.5. リモートアクセス

外部インフラから制御ネットワークへのアクセスが必要な場合、VPN ソリューションを使用すると、接続を保護するために必要な暗号化と認証がもたらされる。
リモートアクセスには、更新に関連するセキュリティポリシーと共に、アクセスとユーザの管理に特化したソフトウェア、ハードウェア、またはその両方を利用する必要がある。

2.6. 可用性

プロセス制御システムでは、メッセージ送信の待ち時間と速度が重要である。 従って、これらは、制御ネットワークの設計が輻輳または接続の喪失という潜在的な問題の要因となる。これらの問題に対するネットワークの復元力（resilience）を強化するための推奨事項は次の通りである。

- VLAN でセグメント化し、サービス品質基準に基づいて特定タイプのトラフィックに優先順位を付けるスイッチを使用する。
- 冗長トポロジを使用して可用性を強化し、スパニングツリープロトコル（STP）を実装してネットワークループを制御する。
- IGMP を VLAN と一緒に使用して、パフォーマンスを向上させ、関連デバイスにマルチキャストメッセージを制限する。

2.7　セキュリティポリシー

ICS インフラのセキュリティに関連する全てのデバイスは、更新が必要かどうかを判断するために、定期的な監視とフォローアップをする必要である。

2.8　エンドユーザデバイスの物理セキュリティ

プロセス制御デバイスおよびネットワークデバイスへの物理的アクセスを制限することは、リモートアクセスおよび認証の制限を補完するために必要である。

ICS の通信プロトコル

3.1. 重要なプロトコル

広く使用されている ICS の通信プロトコルについて解説する。プロトコルは以下に示す：

- Common Industrial Protocol (CIP).
- MODBUS
- DNP3
- Profibus
- Profinet
- PowerLink イーサネット
- OPC
- EtherCAT

3.2. プロトコルの運用レイヤー

ISO の OSI モデルはよく知られているが、ICS では、TCP/IP モデルを使用する。

４つのレイヤーを以下に示す:

- アプリケーションレイヤー：OSI モデルのレイヤー5、6、および 7 に相当する。
- トランスポートレイヤー：OSI モデルのレイヤー4 に相当する。
- インターネットレイヤー：OSI モデルのレイヤー3 に相当する。
- ネットワークアクセスレイヤー：OSI モデルのレイヤー1 および 2 に相当する。

OSI モデルと TCP/IP モデルの比較を図 5 に示す。

このネットワークアクセスレイヤーは、ステーション間での個々ビット送信を担当するため、ビットが正しく送信されたことを確認する手段が含まれている。但し、現時点では、セキュリティ対策は含まれていない。

各プロトコルは個別に考慮されるため、ネットワークアクセスレイヤーの一般的な対策を補完する上位レイヤーでセキュリティ対策が行われる。

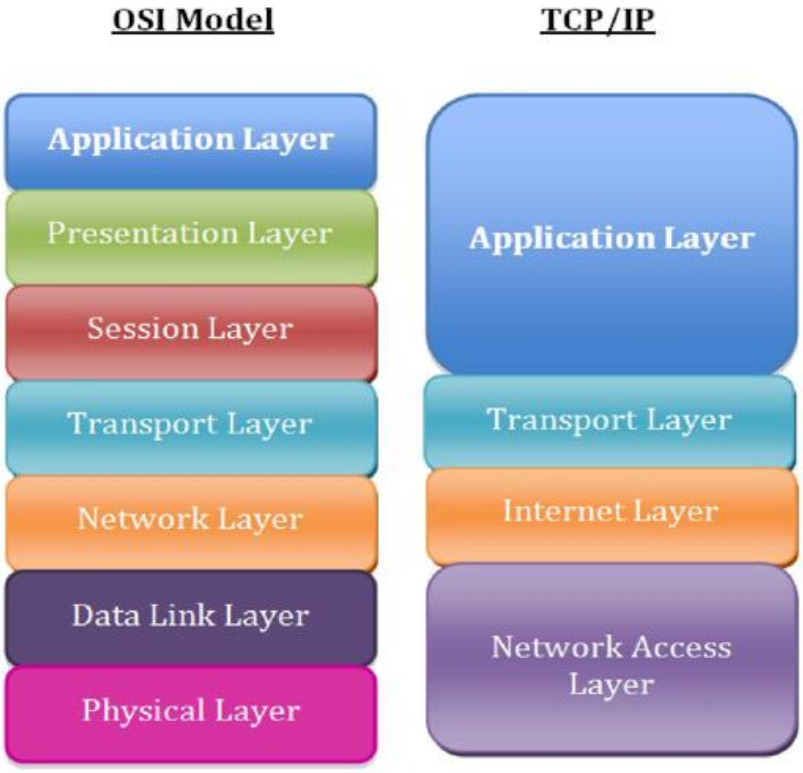


図 5: OSI と TCP/IP モデル

3.3. COMMON INDUSTRIAL PROTOCOL (CIP)

3.3.1. 概要

Common Industrial Protocol（CIP）は、産業プロセスを自動化するために ODVA によって作成されたプロトコルである。CIP は、イーサネットネットワークやインターネットに統合出来る制御、セキュリティ、同期、構成、情報などの一連のサービスとメッセージで構成されている。CIP には多くの適用があり、様々なタイプのネットワークに相互通信と統合を提供する。

Ethernet/IP: CIP の TCP/IP への適用。制御 レベル・情報レベル通信。

ControlNet: CIP と多元接続（CTDMA）統合。各 I/O を統合して使用する。

DeviceNet: CAN を使用した CIP の適用。デバイスレベル通信。

CompoNet: TDMA に適合したバージョン。センサー＆アクチュエータレベル通信。

このプロトコルの様々なファミリが OSI モデルにどのように対応しているか、及びそれら

の同等レベルを示す指標を図 6 に示す。

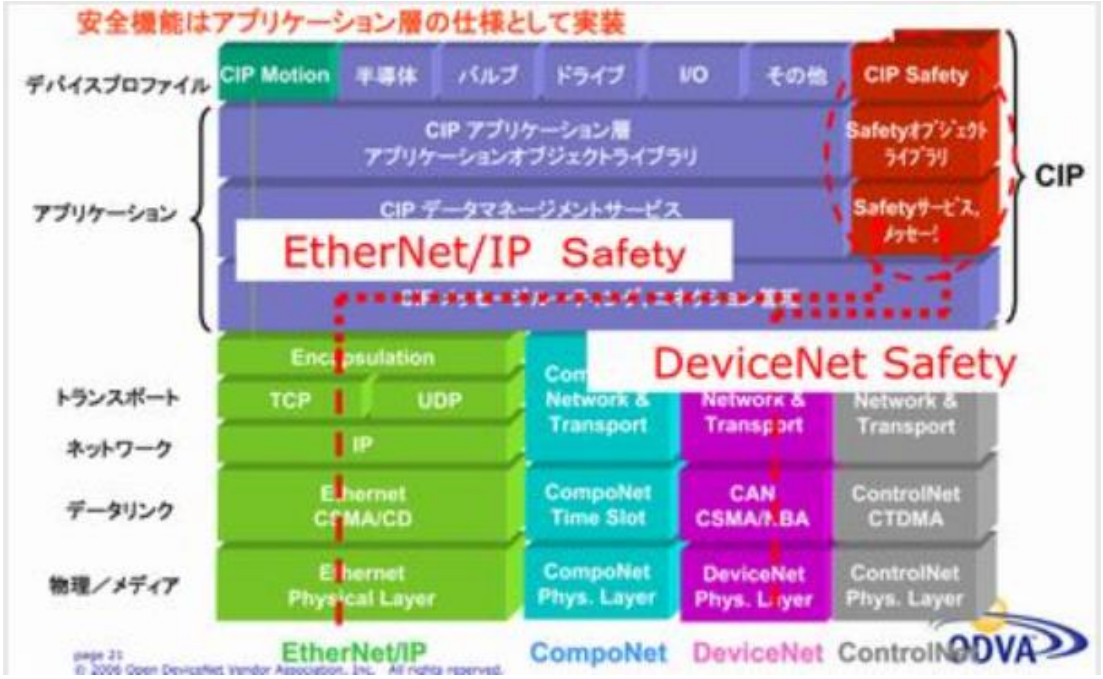


図 6. CIP アーキテクチャネットワークの OSI モデルへの適合 出典：odva Japan

3.3.1.1. オブジェクトの CIP モデル

CIP は、オブジェクトモデルに従うプロトコル。各オブジェクトは、属性（データ）、サービス（コマンド）、接続、及び動作（データとサービスの関係）で構成されている。

CIP には、アナログ及びデジタルの入力または出力デバイス、HMI、移動制御など、自動化プロセスの一般的な要素を備えた一般的な通信と機能をカバーする幅広いオブジェクトがある。相互通信を確実にするために、異なるデバイスに実装された特定の CIP オブジェクトは、全てで同じように動作する必要がある。これは、“デバイスプロファイル”と呼ばれるもので構成する。従って、プロファイルを取得するデバイスは、特定コマンドで同じように応答する。

3.3.1.2. CIP メッセージ

CIP は、プロデューサ/コンスーマパターンに従う。このタイプのアーキテクチャは、マルチキャストタイプである。これは、メッセージがプロデューサによって循環され、メッセージに付随する識別子フィールドに基づく。特定のメッセージ用であるかどうかを決定するのはネットワーク内の様々なコンシューマノードである。従って、2 つのタイプのメッセージを区別でき、2 つのアーキテクチャのいずれかで多かれ少なかれ識別される：

- 送信元アドレスと宛先アドレスではなく、識別子を持つ暗黙のメッセージ（図７）。そのため、この識別子に基づいて、メッセージが関係するかどうか、関係する場合はどのようなアクションを実行するかを知っているのはコンスーマノードである。
- デバイスの発信元アドレスと宛先アドレスに関する情報、及び IP モデルの場合の特定アクションに関する情報を含む明示的なメッセージ（図 8）。

イーサネット/IP や ControlNet などの CIP の一部の実装でも明示的なメッセージを使用する。

図 7. メッセージのプロデューサ-コンスーマモデル（マルチキャスト）

図 8. メッセージの送信元-送信先モデル

3.3.2. CIP の実装：DeviceNET、ControlNET、CompoNENT

3.3.2.1. 説明

これらの CIP は、送信に様々なメディアを用いる。それぞれ CANbus、同軸 RG-6、及び丸型ケーブル（フラットケーブルの代わり）を使用する。

３つの実装の違いは、情報を送信するための物理的なメカニズムにある。これには、セキュリティ対策を提供する特別な機能はない。

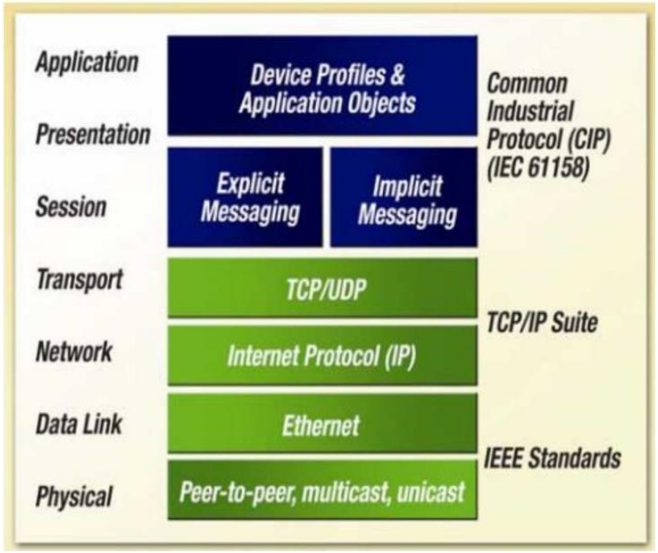
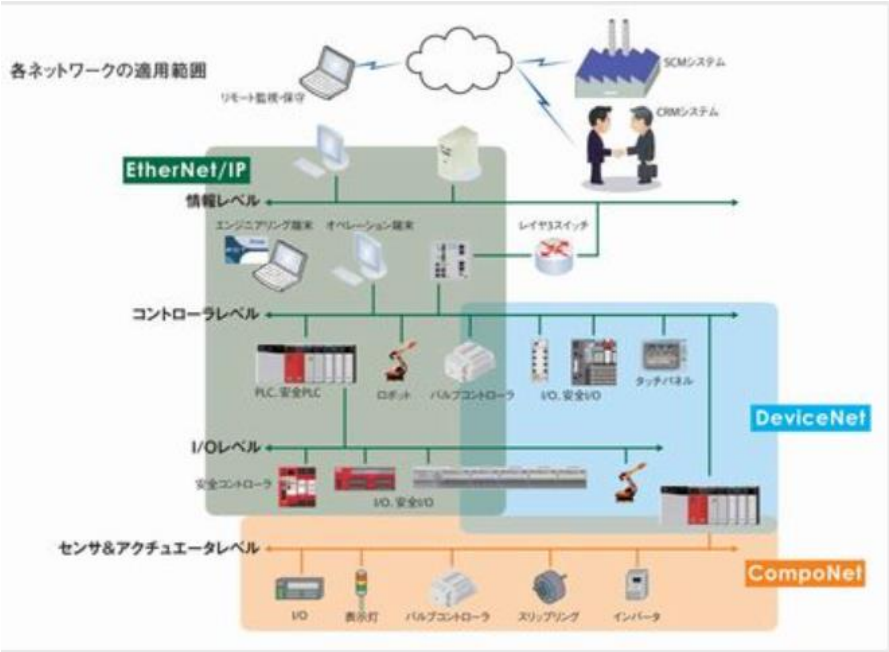


図 9. OSI モデルでのイーサネット/ IP の実装。OSI モデルでのイーサネット/ IP の実装。



出典：ODVA TAG Japan

3.3.2.2 セキュリティの推奨事項

CIP のこれらの実装を保護するための最善のセキュリティ対策は、ネットワークの他の部分から論理的に分離することである。つまり、外部接続から分離されるように展開する必要がある。更に、トラフィックの監視、侵入振舞いの検出、又はその両方のための IDS または IPS を推奨する。

3.3.3 CIP の実装: イーサネット/IP

3.3.3.1. 説明

イーサネット/IP は 2001 年に導入され、製造業の自動化に関して最も普及し、検証され、完全な CIP を実装するプロトコルの 1 つである。従って、イーサネット/IP は、本質的に TCP/IP にリンクされているイーサネットネットワークモデルへの CIP の適用である。その結果、イーサネット/IP は、全てのトランスポート及びネットワークタスクに TCP/IP スタックを使用し、図 9 に示すように、アプリケーションレイヤーに CIP を適用させる。

イーサネット/IP は TCP/IP 通信用に 2 つの接続方法を定義している。これらは、TCP を使用した明示的なメッセージと、UDP を使用した暗黙的な（入力または出力）メッセージ。明示的なメッセージは、クライアント/サーバ又はリクエスト/レスポンスパターンに従う。その中には、PLC と HMI 間のメッセージ、診断メッセージ、及びファイル転送がある。使

用されるポートは TCP448。暗黙のメッセージは重要であり、データの送信などのリアルタイム通信に使用されるメッセージであり、通常、効率を上げるためにマルチキャストアドレスで動作する。これらはポート UDP2222 を使用して送信される。図 10 は、このタイプの通信を示す。

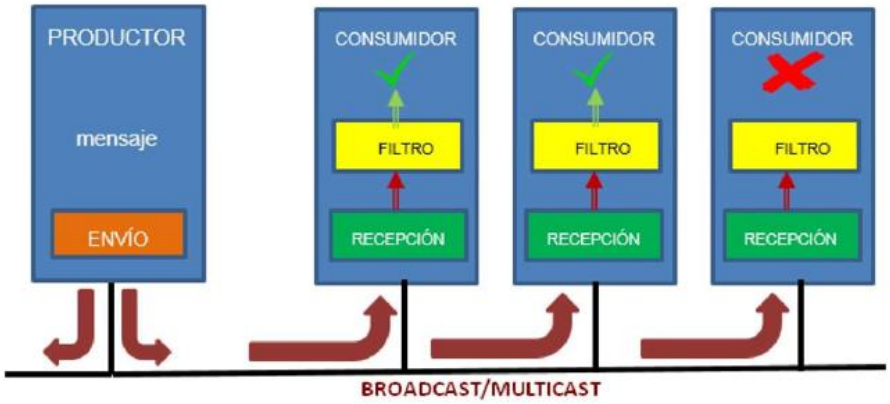


図 10. マルチキャスト通信での CIP プロデューサ-コンスーマメッセージングモデル

3.3.3.2. セキュリティ

イーサネット/IP は、個人情報の盗難やトラフィックのキャプチャなど、イーサネットの全ての脆弱性の影響を受けやすくなっている。更に、暗黙のメッセージに UDP を使用し、送信制御がないため、悪意のあるトラフィックを注入したり、IGMP を使用して送信ルートを操作したりする事が出来る。

3.3.3.3. セキュリティに関する推奨事項

イーサネット/IP は UDP と IGMP を使用するイーサネットベースのプロトコルであるため、イーサネットと IP に基づくすべての安全メカニズムをイーサネット/IP ネットワークの境界に提供する必要がある。又、イーサネット/IP トラフィックが明示的に識別された機器にのみ関連付けられ、ネットワークの外部から送信されないように、ネットワークのパッシブモニタリングを実施する。

3.3.4. CIP セキュリティ

CIP は明確に定義されたモデルを使用するが、セキュリティのために、暗黙的か明示的かを問わず、メカニズムを定義しない。更に、デバイスを識別するための必須のオブジェクトがあり、ネットワーク内の機器を簡単に見つけて、攻撃者にターゲットを提供する可能性があ

る。又、デバイス間で情報を交換するための共通のアプリケーションオブジェクトがあるため、侵入者はこのタイプのオブジェクトを送信して様々な産業用デバイスを操作出来る。更に、CIP のメッセージ特性（リアルタイム、マルチキャスト）は通信の暗号化と互換性がないため、CIP にはそれを許可するメカニズムが用意されていない。

3.4. MODBUS

3.4.1. 説明

Modbus は、最も古い産業用制御プロトコルの 1 つ。PLC との対話にシリアル通信を使用して 1979 年に導入された。1990 年代にはかなり採用され、最新システムとの統合を強化することで、1999 年に TCP/IP ネットワークのバージョンである Modbus/TCP が登場した。現在、重要インフラを含む幅広い業界で広く使用されている。Modbus は、TCP/IP プロトコルレイヤーを含むが、下位レイヤーの接続された様々な種類の機器間で、クライアントサーバモードで通信を提供する。Modbus の実装には 2 種類ある：

- **Serial Modbus**: 使用される伝送技術は、Modbus 本体が実装されている場合は HDLC 標準であり、マスター/スレーブモードで実装されている場合は RS232 または RS485 である。
- **Modbus-TCP**:TCP/IP プロトコルスタックを使用して情報を送信する。

シリアル通信	伝送方法	その他
Modbus ASCII	1バイト(8ビット)データを2文字のASCIIコードに変換して伝送	エラーチェック:LRC法
Modbus RTU	1バイト(8ビット)データをそのまま伝送	エラーチェック:CRC法 ASCIIモードより伝送効率が良いため、RTUモードが主流

TCP/IP通信	伝送方法	その他
Modbus/TCP	ModbusメッセージをTCP/IPネットワークに乗せて送信	産業用イーサネットで最も一般的

（出典：「通信の基本用語一覧」から）

3.4.2. セキュリティ

シリアル Modbus の実装では、物理レイヤー通信プロトコルである RS232 と RS485 の両方に対応する。これらのプロトコルは、定義上、あるデバイスから別のデバイスにビットを送信する。メディアへの物理アクセスでは、実装に応じて（シリアルまたは TCP）、データリンクレベルのプロトコル、HDLC およびイーサネットがある。Modbus は、このレベルでのセキュリティ特性を実装していない。

アプリケーションレイヤーによって提供されるセキュリティに関して、Modbus は高度に制御された環境で使用されるように設計されているので、このレイヤーにセキュリティメカニズムは含まれていない。認証が不足しているため、Modbus セッションに必要なのは、有効なアドレスと機能コードである。これは、ネットワークスニファを使用してインターネット経由で簡単に取得出来る。同様に、情報の暗号化は許可されていない。
TCP/IP スタック（IDS またはファイアウォール）に一般的な対策を適用することは可能ですが、イーサネットの実装にのみ適用され、シリアルバスに基づく実装には適用されない。更に、シリアル実装では、コマンドがブロードキャストで発行される。これは、接続されているすべてのデバイスが DoS 攻撃の影響を受ける可能性がある。Modbus は、RTU や PLC などの制御装置をプログラミングするために設計されたプロトコルであるため、これらのシステムへの悪意のあるコードの挿入が可能になる。

3.4.3. セキュリティに関する推奨事項

上述のセキュリティの欠陥のため、Modbus を使用するデバイス間通信を制御する必要がある。従って、Modbus トラフィックが特定デバイスからのみ許可され、それを確認するため、トラフィックアナライザーを導入する場合がある。更に、誤ったサイズのデータを含む ModbusTCP パケットと、TCP502 ポートの誤ったパケットをチェックする必要がある。追加の対策として、スレーブを強制的にリッスン専用モードにする機能、通信の再開を強制する機能、1 台のサーバから複数のスレーブへのカウンターやトラフィックなどの診断情報を消去またはリセットする機能も、ネットワークをセキュアにするために積極的に監視する必要がある。Snort のような一般的な IDS や IPS のような Modbus に特別に適用したソリューションでこのプロトコルのセキュリティを強化することを強く推奨する。

3.5. DNP3

3.5.1. 説明

DNP3 は、1993 年に開発された通信プロトコルであり、Distributed Network Protocol の略。電力会社や水道施設などの産業分野でよく利用される SCADA 通信プロトコルで、特に米国とカナダの電力分野で広く実装されている。ただ、IEC-60870-5-101 や IEC-60870-5-104 などの選択肢があるため、ヨーロッパではまばらにしか使用されていない。これは、データリンク、アプリケーション、およびトランスポートレイヤーレベルで動作する 3 レイヤープロトコルである。

3.5.2. セキュリティ

DNP3 は、システムの可用性を最大化するように設計されたプロトコルであり、機密性とデータの整合性にはあまり注意を払っていない。

データリンクレベルには、CRC 計算による伝送エラーの検出などの主な機能が含まれている。アプリケーションレベルでは、DNP3 Users group（米国カリフォルニア NPO）によって安全な認証標準が推進され、いくつかの取り組みが行われている。DNP3 はレイヤー1とレイヤー2 の様々な技術で使用出来るプロトコルであるため、この認証はアプリケーションレベルで実行され、最初から最後まで通信を保証している。安全な認証のためのこの業界標準は、いくつかの問題を解決する：

- 一般的に悪質な手口による個人情報の盗難。
- システム機能が変更されるようなメッセージの不正変更。
- 有効データを用いた不正な送信でトラフィックのインジェクション攻撃。
- ネットワーク上を流れる情報の不正盗聴。但し、通常は暗号化キー交換のみ。

この規格には、チャレンジ/レスポンスによる運用モデルなので、認証が必要な機能に対してリクエストが行われた場合、認証チャレンジが解決されない限り、リクエストは処理されない。この通信手順を図 11 に示す。

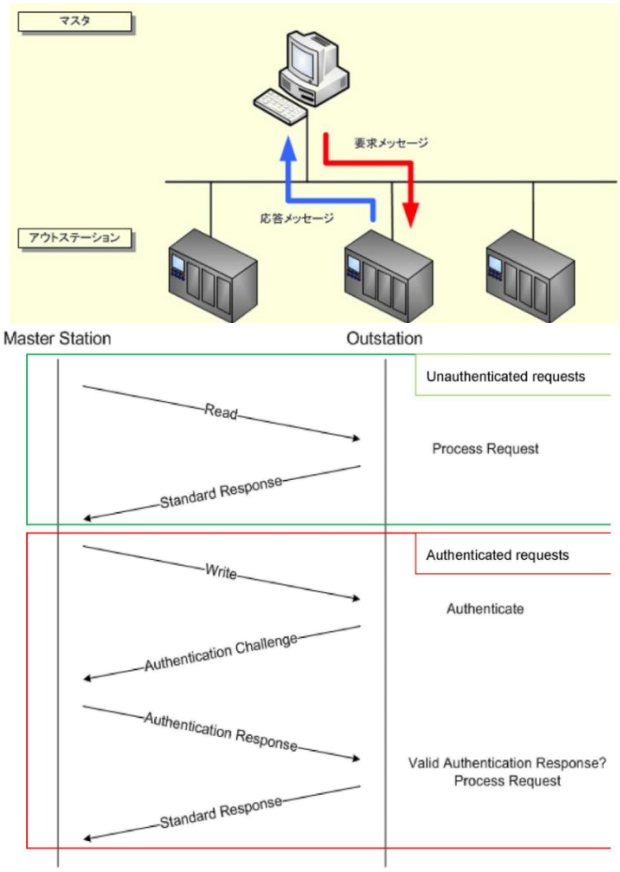


図 11: 異なるタイプの DNP3 要求メッセージ

遅延とネットワーク過負荷が含まれる場合、“Aggressive Mode”のメカニズムを用いて、チャレンジへの要求と応答を一緒に送信することが出来る。

3.5.3. セキュリティに関する推奨事項

DNP3 は安全な実装になっている。ただ、製造メディアによっては様々な理由でこのデプロイが問題になる場合がある。このような場合、TLS などの安全なトランスポートプロトコル内にカプセル化された DNP3 を使用することを推奨する。図 12 に示す。

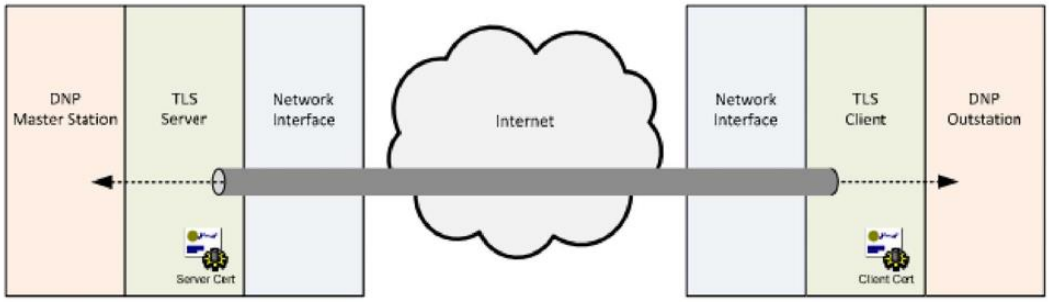


図 12: TLS での DNP3 カプセル化

3.6. PROFIBUS

3.6.1.説明

Profibus（PROcess Field BUS の略）は、1989 年にドイツ連邦教育科学研究技術省によって推進され、Siemens が最初に採用したフィールドバス向け通信手順標準である。これはケーブル（RS-485、MBP）又は光ファイバーケーブルによるシリアル通信に基づいている。現在、**ProfibusDP**（分散型周辺機器向け）と **Profibus PA**（プロセス自動化向け）の 2 つのタイプがある。図 13 に示す。

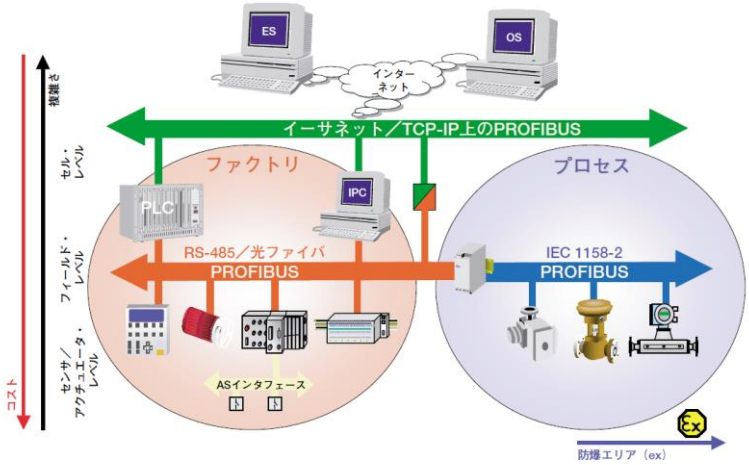


図 13: Profibus アーキテクチャ

3.6.2. セキュリティ

Profibus は、アプリケーション、リンク、および物理レイヤーで動作するプロトコル。このプロトコルのリンクレイヤーは、メディアへのアクセスを管理するためのメカニズムとして FDL（フィールドバスデータリンク）を使用する。この方式では、複数デバイスが同時に通信しないことが保証されるが、トラフィックインジェクション又は、DoS を含む攻撃を受けやすい可能性がある。

アプリケーションレイヤーでは、周期的なデータを交換する DP-V0、固定周期のない通信用の DP-V1、ブロードキャストメッセージ非同期通信用の DP-V2 の 3 つのレベルがある。

3.6.3. セキュリティに関する推奨事項

フィールドバスファミリの他プロトコルと同様に、認証がなく、プロトコルにセキュリティがないため、バスをネットワーク接続の他のコンポーネントから分離する必要がある。許可されていないトラフィックや疑わしいトラフィックを回避するには、境界セキュリティを非常に厳しくする必要がある。

3.7. PROFINET

3.7.1. 説明

Profinet は、RS485 ではなくイーサネット接続の物理インターフェイスとして採用する Profibus に基づく標準仕様であり、トークンの受け渡しに基づく繰返しシステムを備えている。データ転送用の完全な TCP/IP 機能を提供し、ワイヤレスアプリケーションと高速伝送を可能にする。Profinet を使用する機器は、使いやすさとともに、信頼性とリアルタイム通信を重視している。図 14 は、Profinet のアーキテクチャを示す。

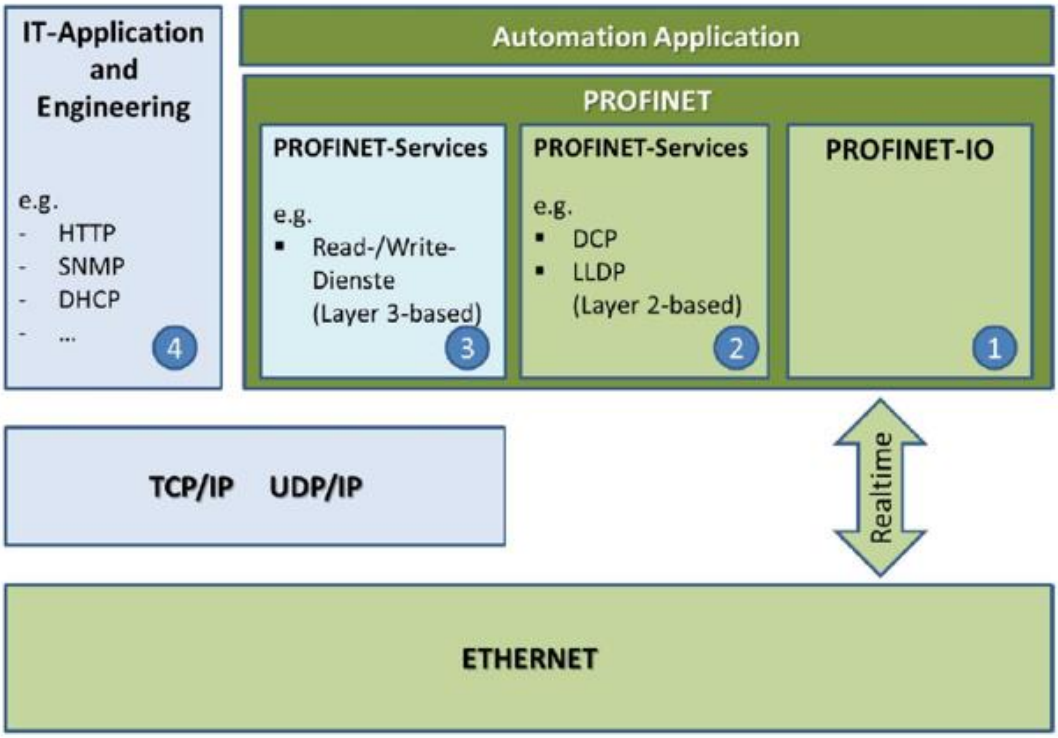


図 14: Profinet アーキテクチャ

3.7.2. セキュリティ

Profinet 機器には、エンドポイントセキュリティという意味でのネイティブセキュリティ機能がない。従って、Profinet 機器への攻撃を防ぐことが重要である。

プロトコルに組み込まれている対策は、特定のポイントで大量のトラフィックに直面した場合の機器の堅牢性とともに、システムの可用性と運用の信頼性の向上に重点を置いている。PROFINET セキュリティガイドラインでは、図 15 に示すように、VLAN を使用したネットワークのセグメンテーションや DMZ の設定など、IT システムへの潜在的な攻撃を防ぐための推奨事項を提供する。

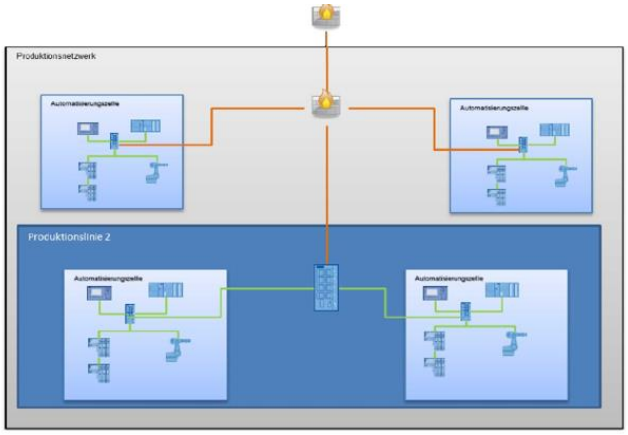


図 15: ProfiNet アーキテクチャ

3.7.3. セキュリティに関する推奨事項

フィールドバスの通信向けに開発された他のプロトコルと同様に、プロトコル認証がなく、セキュリティに欠けるため、他のネットワークから分離する必要がある。更に、IT 手法を用いてネットワークのコンポーネントを認証し、ネットワーク内の通信を暗号化することを勧める。最後に、境界線のセキュリティは、許可されていないトラフィックや疑わしいトラフィックを回避するために、非常に厳格にする必要がある。

3.8. イーサネット POWERLINK

3.8.1. 説明

イーサネット PowerLink は、イーサネットのリアルタイム通信で、IEEE 802.3 標準に従ってイーサネットを拡張し、正確な同期と予測可能な間隔で情報を送信するメカニズムを備えている。Profinet はイーサネットプロトコル向けの Profibus の適用のため、アプリケーションレイヤーは元々Fieldbus 向けに設計されている。図 16 を参照。PowerLink イーサネットは、以下に対応するメカニズムを提供する：

・非同期サイクルで時間がクリティカルな情報送信。
　情報の交換は、publication/subscription の手法に基づいている。
・ネットワーク内のノードを非常に正確に同期する。
・それほどクリティカルではない情報の送信。非同期通信では、TCP/IP スタック、または HTTP、FTP などの上位レイヤーからのプロトコルを使用できる。

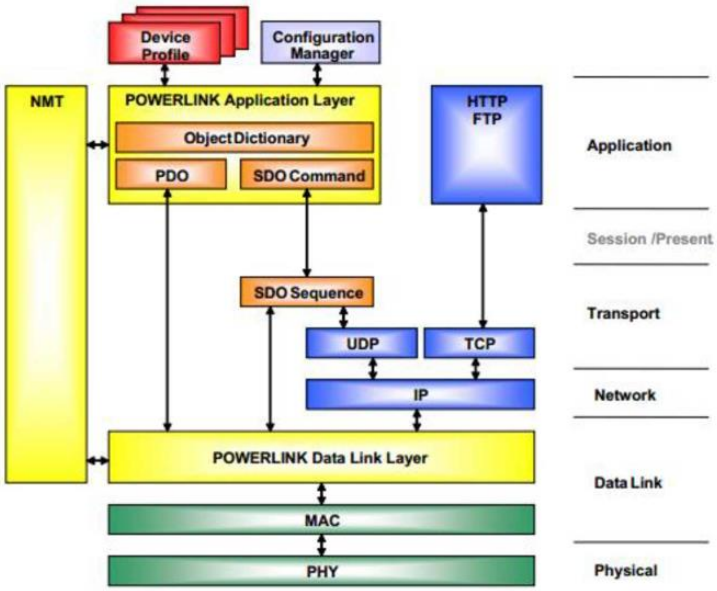


図 16: イーサネット Ethernet PowerLink のレファレンスモデル.

ネットワーク上のトラフィックは、同期および非同期の送信のために時間間隔が確保されるように管理され、ネットワーク内の機器のみが伝送媒体にアクセスできるようになっている。これにより、非同期で送信される情報が同期送信に干渉せず、通信間隔が維持される。データ衝突を避け、バンド幅を最大に利用するために、デバイス間のデータ交換はタイムスロットベースで行われる。POWERLINK のあるノードは“管理ノード（Managing Node:MN）”の役割を行う。それはコミュニケーションを制御し、全ノードの同期用のクロックパルスを制御し、個々のデバイスの送信権利を割り当てる。“制御ノード（Controlled Node;CN）”は MN から要求されたときのみ送信を行う。POWERLINK のサイクルは 4 つの時間に区切られている。

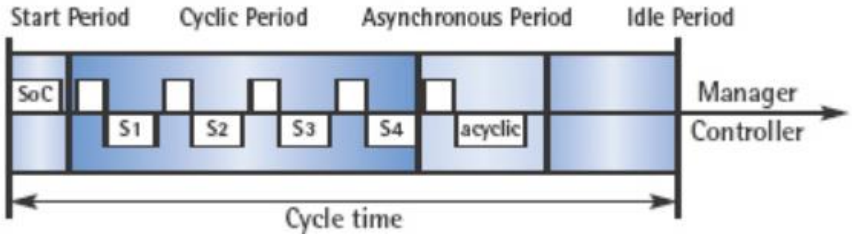


図 17: イーサネット PowerLink のスロット通信ネットワーク管理

3.8.2. セキュリティ

他の産業用プロトコルと同様に、ノードとメッセージの信頼性をチェックするメカニズムがこのプロトコルにはない。従って、正当なノードを偽造することによってネットワーク内のトラフィックを変更したり、ネットワークをメッセージで溢れさせるだけで DoS 攻撃をトリガーしたりすることはかなり簡単である。

送信にブロードキャストを使用すると、侵入者は通信ネットワークによって送信されたすべての情報を入手することも出来る。

3.8.3. セキュリティに関する推奨事項

遅延に対する SCNM（スロット通信ネットワーク管理）の感度には、イーサネット PowerLink を他のネットワークから分離して展開する必要がある。従って、境界セキュリティは、プロトコルをネットワークの他の部分から分離し、悪意のあるトラフィックを防ぐために、非常に厳格にする必要がある。

3.9. OPC

3.9.1　説明

OPC（プロセス制御用の OLE）は、産業用通信プロトコルではなく、オブジェクトリンク埋め込み（OLE）を使用する Windows ベースのプロセス制御システムでの通信運用フレームワークであり、RPC（Remote Procedure Call）等の通信プロトコルを使用する。従って、OPC は、プロセス制御システムが Windows の通信機能を使用して通信出来るようにする一連のプロトコルである。OPC は、通常 TCP/IP を介して Windows システムに接続する。OPC は元々DCOM（Distributed Component Object Model）に基づいており、はるかに安全な通信経路の暗号化（SOAP over HTTPS）の使用を可能にする OPC-UA と呼ばれる更新バージョンがあるが、多くの OPC システムはまだ OPC-DA(データアクセス)を使用している。

3.9.2　セキュリティ

DCOM と RCP（remote copy）を使用すると、OPC は攻撃の影響を非常に受けやすくなるが、OLE で発生するすべての脆弱性の影響を受ける可能性がある。その上、OPC は Windows システムでのみ実行されるため、この OS が抱えるすべての弱点にも見舞われる可能性がある。ICS にパッチを適用することは本質的に困難であるため、既にパッチが必要な多くの脆弱性が発見されており、引き続き悪用可能な産業用制御ネットワークとなっている。但し、OPC-UA には、ホワイトペーパーに記載されているセキュリティのモデルがあり、アーキテクチャのセキュリティが強化されているため、クラシックバージョンの OPC-DA ではなく OPC-UA を導入することを推奨する。

3.9.3　セキュリティに関する推奨事項

可能ならば、OPC-UA を推奨する。この推奨事項とは別に、OPC サーバは強化し、不要な全てのポートとサービスを遮断する必要がある。更に、Windows、OPC、OLE RPC、又は DCOM に影響を与える脆弱性と同様に、OPC サーバによって開始されたすべての非 OPC ポートとサービスを注意深く監視する必要がある。不明な OPC サーバから開始された OPC サービスと、OPC サーバでの認証の失敗も、OPC の展開のセキュリティを向上させるために、事前に監視する必要がある。

3.10. ETHERCAT

3.10.1. 説明

EtherCAT（Ethernet for Control Automation Technology）は、イーサネットを産業環境に組み込むために使用されるオープンコード通信プロトコルである。このプロトコルは、フィールドバスの標準化の範囲内で、IEC61158 の標準として規格化された。EtherCAT は、更新サイクルが短く（≤100μs）、ジッタが 18≤1μs のオートメーションアプリケーションで使用される。従って、これは現在利用可能な最速のシステムである。このシステムでは、イーサネットパケットは受信、解釈、および送信されない。むしろ、次のデバイスに送信されるときに、全てのスレーブノードで（関連情報の更新と共に）オンザフライで処理される。遅延はわずか数ナノ秒に短縮される。EtherCAT の基盤を図 18 に示す。

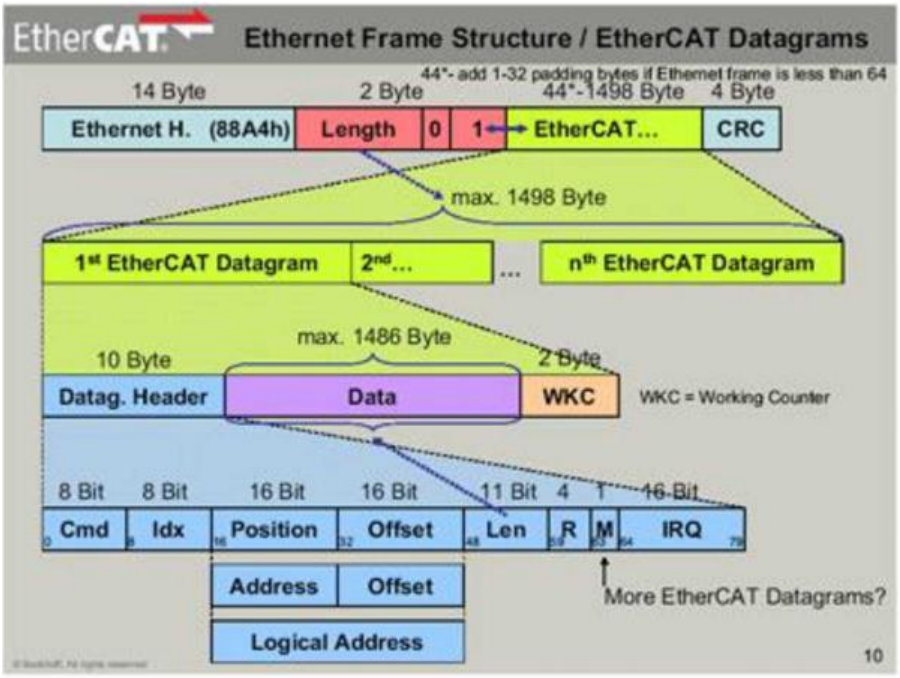


図 18: EtherCAT フレームワーク.

3.10.2. セキュリティ

EtherCAT はイーサネットから派生したプロトコルであるため、イーサネットのすべての脆弱性の影響を受けやすく、従って広範囲の DoS 攻撃のリスクがある。EtherCAT サービスは、イーサネットパケットをネットワークに挿入することで簡単に変更でき、同期を妨害し、認証の欠如の結果として偽造や中間者攻撃(MITM)に対して脆弱になる。そのため、EtherCAT ネットワークを他のイーサネットシステムから分離することを推奨する。

3.10.3. セキュリティに関する推奨事項

既に述べたように、EtherCAT は他のイーサネットネットワークから分離して展開する必要がある。又、ネットワークの整合性を確保するために、ネットワークのパッシブモニタリングを実行し、EtherCAT トラフィックが明示的に許可されたデバイスからのみ発信されていることを確認することを推奨する。

あとがき

今回の資料は、元々スペイン産業・エネルギー・観光省下の National Institute of Cybersecurity（INCIBE）が投稿した論文を参考にして抄訳および追加したものである。近年、多くの企業が高度な産業用オートメーションに移行し、DX 化も伴って生産性改善が促進されている。そして、各方面の産業分野の制御システムを取り巻くネットワーク環境では、IIoT 導入とか外部ネットワーク（クラウド等）により、必然的に工場現場でのセキュリティ課題も浮上している。又、モータ制御およびセンサをスケーラブルかつ効率的な方法で接続する必要もある。

そこで、IT と OT 融合が近づいている中で、ICS インフラで使用されているプロトコルとそのアーキテクチャについての本資料が役立てば幸甚である。

<参考文献>

1. ISA-95: https://www.isa.org/standards-and-publications
2. PwC「PwC's Cyber Intelligence 危機に瀕する日本の ICS セキュリティ 狙われる PLC」: https://www.pwc.com/jp/ja/knowledge/column/awareness-cyber-security/cyber-intelligence03.html
3. ODVA TAG Japan : http://odvatagjapan.blog69.fc2.com/
4. IEEE, IEEE Standard for Electric Power Systems Communications - Distributed Network Protocol (DNP3), 2010. : https://standards.ieee.org/standard/1815-2010.html
5. 制御システムのセキュリティ：IPA 独立行政法人 情報処理推進機構：https://www.ipa.go.jp/security/controlsystem/index.html