CPS 向け汎用プロトコル監視手法の一考察

南 拓也 [1,*]　中嶋 良彰 [1]

概要：近年急速に普及が進むサイバー・フィジカルシステム(Cyber Physical System : CPS)において，被害時のインパクトから，OT(Operational Technology)の領域へのセキュリティ対策が重要視されている．しかし，OT 分野は多種多様な通信プロトコルの使用という複雑さを特徴としてもつことから，対策の導入は困難となっており，まさに今，本課題の解決が求められている．本稿では，解決策の 1 つとして，プロトコル非依存の汎用的監視手法の提案を行う．また，従来の監視手法へ本提案手法を含めることで，OT 領域に適合性の高い総合的に優れた監視手法となりえることを評価により示す．

キーワード：CPS, 産業用プロトコル, プロトコル監視, ホワイトリスト, ルールベース, 機械学習

A Study of a Generic Protocol Monitoring Method for CPS

Takuya Minami[1,*]　Yoshiaki Nakajima[1]

Abstract: In the Cyber Physical System (CPS), which is rapidly spreading in recent years, security measures in the field of OT (Operational Technology) are emphasized because of the impact of damage. However, the complexity due to using a wide variety of communication protocols, which is a characteristic of the OT field, makes it difficult to implement countermeasures, a problem that needs to be solved now. In this paper, we propose a protocol-independent general monitoring method as one of the solutions. In addition, we evaluate that including our proposed method in the conventional monitoring method can provide a totally superior monitoring method suitable for the OT domain.

Keywords: CPS, Industrial Protocol, Protocol Monitoring, White List, Rule Base, Machine Learning

1. はじめに

2016 年，内閣府の第 5 期科学技術基本計画において，日本が目指すべき未来社会の姿として Society5.0 が提唱された[1]．Soicety5.0 は，サイバー空間とフィジカル空間を高度に融合させ付加価値を創出する人間中心の社会と定義される．このサイバーとフィジカルの空間が融合されたシステムは，サイバー・フィジカルシステム(Cyber Physical System : 以下 CPS)と呼ばれ，スマートファクトリーやスマートシティに代表される IT(Information Technology)と OT(Operational Technology)が融合した形態を取り，近年急速に普及が進んでいる．CPS の普及に伴い，その脅威も顕在化してきている．2019 年，サイバー・フィジカル・セキュリティ対策フレームワーク[2]が策定されるなど，新たに発生するリスクへの対応が求められている．

本稿では，CPS の中でも特に OT の領域に着目し，OT における多種多様な通信プロトコル監視における課題を取り上げる．2 章において OT でのセキュリティ対策の課題の詳細を述べ，3 章では多種多様な通信プロトコルを解説する．4 章ではこれら多様なプロトコルを汎用的に監視するための監視ルールを定義し，5 章において監視ルールづくりの手法と生成例を示し，本監視手法を含めた総合的な監視が OT 領域に適合性が高いことを定性的評価により示す．

2. CPS の特徴とセキュリティ監視

IT は，インターネット技術の発展によるオープン化により，セキュリティ対策も進化を続けてきた．それとは対照的に，OT は，工場内の産業用ネットワークなど，クローズドを前提とした文化が依然定着している．近年の OT 機器のオープン化で IT 同様の脅威にさらされる機会は増加の一途を辿っているが，IT と比較しセキュリティ対策は未成熟である．

OT のセキュリティ対策が未成熟の理由に，OT 独自の特徴が背景に存在する．“可用性重視”，“長い機器寿命”，“多種多様，独自仕様の通信プロトコル”，“機器に直接手を加えることが困難”が代表的な特徴である．これら特徴により，IT のように，パッチ適用やエンドポイントセキュリティの導入，新バージョンへの入替といった機器での直接的な対策が行えない他，ネットワーク構成の変更によるゲートウェイ設置やセグメンテーション化(IT と OT の分離)といった対策も行えない状況が多い．

この状況下での有効なセキュリティ確保の手段は，機器やネットワーク構成に極力手を加えず行えるパッシブな通信監視である．ネットワーク機器のミラーポートからのキャプチャにより行われることが一般的である．ただし，通信監視が有効な手段であるといえど，OT の特徴に起因し

1 NTT 社会情報研究所
NTT Social Informatics Laboratories
* takuya.minami.mx@hco.ntt.co.jp

発生する“多種多様，独自仕様の通信プロトコル”をどのように監視するかは，課題として立ちはだかってくる．

本稿では，通信プロトコルを汎用的に監視する技術を深堀していき，この課題の解決を目指す．

3. 多種多様な通信プロトコル群

3.1 OT 分野の通信プロトコル群

産業用ネットワークの市場調査[3]によると，近年の新規設置ノードの多くに産業用イーサネットが使用されている．フィールドバスとワイヤレスを含んだ母数に対し 2018 年に初めてシェアで半分を超え，2021 年度では 65%に上っており(図 1)，産業用ネットワーク市場において，産業用イーサネットの全体における割合は年々増加している．産業用イーサネットのシェアトップは PROFINET(28%)で，EtherNet/IP(26%)， EtherCAT(12%)， Modbus-TCP(8%)，POWERLINK(6%)と続く(図 2)．調査では，前述以外のイーサネットをベースとした Other Ethernet(20%)と分類されるものも割合として多く，多種多様の通信プロトコルの乱立が見てとれる．これらプロトコルにはそれぞれ特徴があり，ユーザが構築するシステムの要件に合わせ使用されるプロトコルは異なり，オプション設定も様々となる．中には自社システム専用に開発された独自仕様のプロトコルも存在している．

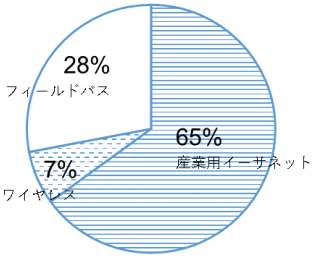


図 1　産業用ネットワーク市場シェア動向(2021 年)

Figure 1　Market share trends for industrial networks (2021).

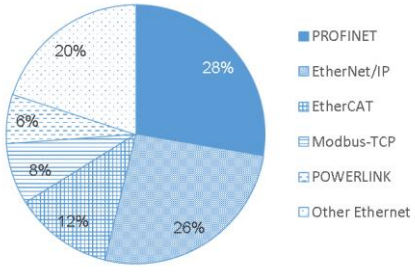


図 2　産業用イーサネット内訳(2021 年)

Figure 2　Detail of Industrial Ethernet(2021).

本稿では，今後もシェアを広げる産業用イーサネットに着目する．3.2 節から 3.6 節で，シェア上位の産業用イーサネットのプロトコルの特徴について表に整理する．表では，各プロトコルが主にもつオプショナルな種別，通信の特徴，L3-4(レイヤ 3,4 の有無)，転送方式(UC：ユニキャスト，MC：マルチキャスト，BC：ブロードキャスト)をまとめている．

3.2 PROFINET

PROFINET[4]は，フィールドバス向けの PROFIBUS を基に，イーサネットベースのプロトコルとして開発されており， PROFINET IO(分散型プリフェラル)と PROFINET CBA(Component based Automation)の 2 種類がある．特徴を表 1 にまとめる．PROFINET IO は，イーサフレーム上に直接乗るものと，UDP/IP のプロトコルスタックを使用するものがある．コントローラと分散型フィールドデバイス間の通信を組み合わせたプロトコルで，プロセスデータとアラームは常にリアルタイムでやりとりされる．PROFINET CBA も，イーサフレーム上に直接乗るものと，TCP/IP のプロトコルスタックを使用するものがある．システム全体およびメーカにまたがる通信のためのコンポーネントモデルに基づくプロトコルで，分散型オートメーションのアプローチをとる．

PROFINET はいくつかの通信種別をもつ．RT(Real-time)，SRT(Soft Real-time)は周期通信で，イーサフレーム上にリアルタイム用のフレームを定義し，10ms 程度の周期のリアルタイム通信を行うもので，主に工場設備のフィールドで使用される．IRT(Isochronous Real-time)も周期通信で，専用の通信サイクルを設け，1ms 以下の高いレベルのリアルタイム通信を行う．NRT(Non Real-time)は非同期通信で，UDP/IP，TCP/IP を使ったリアルタイム性を要求しないものに使用される．

表 1　PROFINET の特徴

Table 1　Characteristics of PROFINET.

種類	通信の特徴	L3-4	転送方式
IO	周期通信（RT, SRT, IRT）	—	UC
	非同期通信（NRT）	UDP/IP	UC
CBA	周期通信（RT）	—	UC
	非同期通信（NRT）	TCP/IP	UC

※RT：Real-time，SRT：Soft Real-time，IRT：Isochronous Real-time，NRT：Non Real-time

3.3 EtherNet/IP

EtherNet/IP[5]は，イーサネットをベースに，TCP/IP および UDP/IP を利用したプロトコルである．セッション～アプリケーション層の間で CIP(Common Industrial Protocol)アプリケーションを定義したオブジェクトモデルを採用している．CIP は，producer-consumer の送信モデルを使用するメディアに依存しないプロトコルであり，共通のインタフェースや動作を定義するアプリケーションオブジェクトとデバイスプロファイルのセットが，CIP アプリケーション層で定義されている．これにより，複数のベンダで構成される CIP ネットワーク間の相互運用性を向上している．

EtherNet/IP には，Implicit(暗黙)と Explicit(明示的)の 2 種類がある．特徴を表 2 にまとめる．Implicit は，UDP/IP を用いたリアルタイムデータの通信で，マルチキャスト／ユニキャストに対応し，通信相手ごとに異なる通信周期で一定周期のサイクリック通信を行う．Explicit は，TCP/IP を用いた非リアルタイムデータの通信で，1 対 1 を前提とした Request/Response の性質をもち，事前のコネクション確立の有無に関係なく実行ができる．

表 2　EtherNet/IP の特徴

Table 2　Characteristics of EtherNet/IP.

種類	通信の特徴	L3-4	転送方式
Implicit	周期通信（リアルタイムデータ通信）	UDP/IP	UC, MC
Explicit	非同期通信（非リアルタイムデータ通信）	TCP/IP	UC

3.4 EtherCAT

EtherCAT[6]は，標準イーサネットでは満たせないリアルタイム性を実現するために開発されたプロトコルである．ネットワークセグメント内のすべてのノードの送受信データを 1 つのフレーム内に実装している．マスタは 1 つの電文を送信し，各スレーブは自身にアドレス指定されたデータを読み／書きしつつ後方のデバイスに送信するという特有の動作をする．パケットの構造は，1 パケット内に複数のデータグラムが含まれデータグラムごとに宛先や機能の指定がある．イーサネットフレームの送信にはブロードキャストが指定される．

EtherCAT には，PDO(Process Data Objects)通信と Mailbox 通知の 2 種類ある．特徴を表 3 にまとめる．PDO 通信は周期通信であり，クリティカルに同期したいマスタとスレーブ間で行われる．Mailbox 通信は非同期通信であり，任意のタイミングでスレーブ内の各オブジェクトへのアクセスなどに使われる．

表 3　EtherCAT の特徴

Table 3　Characteristics of EtherCAT.

種類	通信の特徴	L3-4	転送方式
PDO 通信	周期通信	—	BC
Mailbox 通信	非同期通信	—	UC

3.5 Modbus-TCP

Modbus-TCP[7]は，TCP/IP 上で Modbus 通信を行うためのプロトコルである．シングルマスタ／マルチスレーブの方式をとる．マスタは指定のスレーブのみにクエリ，またはすべてのスレーブに対するブロードキャストのクエリを送ることができる．Modbus メッセージの構成は，ヘッダ，スレーブアドレス，ファンクションコード，データバイト数，データ，エラーチェック，トレーラとシンプルな構造をとる．ファンクションコードにより，どのような機能を実施するかが決まる．特徴を表 4 にまとめる．

表 4　Modbus-TCP の特徴

Table 4　Characteristics of Modbus-TCP.

種類	通信の特徴	L3-4	転送方式
—	非同期通信	TCP/IP	UC，BC

3.6 POWERLINK

POWERLINK[8]は，標準イーサネットでは満たせないリアルタイム性を実現するために開発されたプロトコルである．デバイスへの通信スロットの割り当てにより，常に 1 つのネットワークデバイスがネットワークメディアにアクセスする方式をとる．通信を管理する管理ノードにより通信が管理され，producer-consumer の送信モデルで，1 対 1，1 対 N の通信を行う．

POWERLINK は，時間固定された 1 サイクルを繰り返す方式で，1 サイクルの中に，機器の同期を取る Ph1，周期通信を行う Ph2，非同期通信を行う Ph3 という 3 種類のフェーズをもつ．特徴を表 5 にまとめる．Ph1 では，SoC(Start of Cycle)と呼ばれるメッセージをタイミング同期する機器すべてに送る．Ph2 では，機器は割り当てられたスロットで通信を行う．Ph3 では，パラメータ化データや IP トラフィックなどタイムクリティカルではない通信を行う．

表 5　POWERLILK の特徴

Table 5　Characteristics of POWERLINK.

種類	通信の特徴	L3-4	転送方式
Ph1	SoC を送信	UDP/IP	MC, BC
Ph2	周期通信（タイムクリティカルな通信）	—	UC
Ph3	非周期通信（タイムクリティカルではない通信）	UDP/IP, TCP/IP	UC, MC, BC

4. 通信監視ルールの検討

4.1 汎用監視に向けた監視ルールの基準づくり

3 章で，OT 分野の多種多様な通信プロトコルを見てきた．OT 環境の特徴には，工場の生産ライン等に代表される自動化された機器の繰り返し動作があり，通信は M2M がベースとなる．これは，人が介在することで不定型な通信が発生する IT 環境とは大きく異なる点の 1 つである．M2M のような定型通信は，何かしらの形に定式化し，それを監視ルールとして監視することで，ルールから逸脱する通信を発見するホワイトリスト型の監視が一般には適している．

ただし，ホワイトリストと一口にいってもベンダごとに様々な形式をとりうる．検討や評価の場面を考えると，監視ルールをベンダ非依存とすることが，検討をシンプルにする点や公平性を保つ点で望ましく，本稿では，まずは，監視ルールにおいて基準とする考え方を整理する．

具体的には，時間方向とレイヤ方向(空間)への“時間”と“空間”の分割により通信の表現の定式化を行う．本定式化により，監視ルールが，“どの時間”と“どの空間”をカ

バー可能かが可視化され，3 章の多種多様な通信プロトコルに対する監視の違いを，容易に把握できるようになる．

4.2 通信の定式化

図 3 に示すあるネットワーク 1 の中を流れる通信を定式化することを考える．ネットワークに流れる通信を時間区切りで見た際，通信のボリュームはそれぞれ異なっていると考えられ，時間方向への分割としていえる最もシンプルな定義は，区間 a では通信は存在することが正しく，区間 b は通信が存在しないことが正しいという定義になる．

次に通信が存在する区間の定義について考える．図 3 の S の面積を埋める通信は，OSI 参照モデルに従いレイヤごとに分けることができる．通信を，物理ペアからアプリまで縦方向に AND でつなげていくと，ドリルダウン型の詳細な定義となる(図 3 の詳細化の方向)．また，上下層とは独立に横方向にユニークな要素で集合を作ると，スライス型の抽象的な定義となる(図 3 の抽象度の集合の方向)．

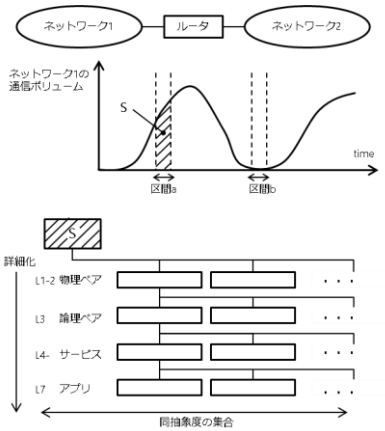


図 3　通信の定式化の概念

Figure 3　Concept of communication formulation.

4.3 監視ルール (L7 未満)づくり

イーサネットかつ IP ベースの監視ルールについて考える．物理ペアは，SrcMAC アドレスと DstMAC アドレスの対となる(それぞれ，A と B とする)．論理ペアは，SrcIP アドレスと DstIP アドレスの対となる(それぞれ a と b とする)．これらを AND でつなぐということは，(A, a, B, b)といったルールで表現できるといえる．さらに，サービス(使用するポート)も，Src ポートと Dst ポートの対となる(それぞれ α と β とする)ため，これらをすべて AND でつなぐと，(A, a, α, B, b, β)といったルールで表現できるといえる．IP および TCP，UDP により実装される通信プロトコルについては，これらのルールを使い監視ができ，実際に一般的な定義方法である．

前述のルールの考え方を，3 章で述べた多種多様な通信プロトコルにあてたものが表 6 である．TCP/IP および UDP/IP をサポートするプロトコルについては物理ペア，論理ペア，サービスでの監視ルールでの監視が可能であり，表中の L1-2, L3, L4-の行が“✓”となる．表中，論理ペア，サービスが△や空白となっているなっているものは，IP を使用せず，イーサフレーム上に直接アプリケーション情報が乗るものである．これらに当てはまる特徴は，アプリケーション層まで分析をしないと，論理的な宛先アドレスが抽出できないということである．また，中でも EtherCAT の PDO 通信は，物理レイヤではブロードキャストベースでの通信を行い，この場合，通信フレームの宛先が全機器となるため，物理ペアの監視ルールを作ることができない．△で記載しているものは，マルチキャストが利用されることから，特定の機器とのペアを見る上では制限を受ける場合があることを示す．ただし，各プロトコルにおいて，ユニキャストかマルチキャストかブロードキャストかはオプションの場合もあり，本表の限りではない．

表中，網掛けとしている L7 の行は，4.5 節でフォーカスする領域である．一般に，L7 未満を監視する際，TCP/IP, UDP/IP のようにデファクトスタンダート化されたものであれば，事実として汎用的な監視は充実している．しかし，表 6 からわかるように L7 未満では監視できないプロトコルは現実として存在しており，アプリケーション層も見ることは，通信監視において不可欠な要件といえる．OT 分野において L7 解析は，特徴の異なるプロトコル群を汎用的に監視するためには避けては通れない道であるといえる．

表 6　プロトコル vs 監視 (L7 未満)

Table 6　Protocol vs monitoring(< L7)

プロトコル名	PROFINET			EtherCAT		EtherNet/IP		Modbus-TCP	POWERLINK		
種類	IO(RT, SRT, RT)	IO(NRT), CBA(NRT)	CBA	PDO 通信	Mailbox 通信	Implicit	Explicit	—	Ph1	Ph2	Ph3
L1-2 物理ペア	✓	✓	✓			✓	✓	✓		△	△
L3 論理ペア		✓	✓			✓	✓	✓		△	△
L4- サービス		✓	✓			✓	✓	✓		△	△
L7 アプリ											

【凡例】✓：監視ルール生成可能，△：生成に制限あり

※入手した公開仕様，サンプルパケットから一般的利用方法を推定し表を作成

4.4 監視ルール(L7 未満)による監視

4.3 節で検討した，L7 未満のホワイトリスト型の監視ルールで監視を行った際に，検知可能と考えられるサイバー攻撃について考察する．考察にあたっては，MITRE 社のフレームワークである ATT&CK for ICS を使用する．

MITRE ATT&CK for ICS[9]では，敵対的戦術と攻撃テクニックが産業用システム向けに整理されており，攻撃テク

ニックの種類は2022年7月現在で68件が掲載されている．本稿では，主にOT分野のシステムの通信をパッシブに監視することに焦点をあてていることから，攻撃テクニックの中でも明示的に通信を発生するものを選択し，それが4.3節で定義した監視ルールで監視，検知が可能かを見ていく．

ATT&CK for ICS に掲載される攻撃テクニックの説明やリファレンスをもとに攻撃をトレースした結果，明示的に通信を発生させると判断できる攻撃テクニックは，表 7 の20件となった．

通信の見え方の具体例として，敵対者またはマルウェアによる情報収集のための普段アクセスしない機器へのアクセス，普段登場しない機器からの既設の機器へのアクセスといった通信がある．また，悪性なファイルを，通信がリーチャブルな不特定な相手に送る通信や，なりすましによる通信の仲介という通信も存在する．これらは，通信元や通信先がいつもの機器と同じかどうかで，不審な通信かを識別することができる

逆に，普段の通信を装い，いつもの相手にいつもの通信ポートを使い通信を行うものについては，L7での通信監視が必要であり，表中の攻撃テクニック中の 7 件(網掛けの行)がそれに該当するといえる．特にT0848のRogue Masterは，マスタとなる機器が乗っ取られ，スレーブに対し不正な命令を送るものであり，L7での監視なしでは検知は難しい．OT環境を，サイバー攻撃により復旧不可能な物理被害へ至らせないためには，マスタからの不審な通信の有無を監視することがとても重要となる．

表 7　攻撃テクニックの特徴と検知可否

Table 7　Attack techniques features and detection capability

ID	Technique Name	特徴	L7 未満での検知
T0802	Automated Collection	情報収集の通信	✓：不審な Src-Dst
T0811	Data from Information Repositories	情報収集の通信	✓：不審な Src-Dst
T0814	Denial of Service	通信による妨害	✓：不審な通信量
T0817	Drive-by Compromise	通常を装う通信	L7 監視が必要
T0819	Exploit Public-Facing Application	不正通信	✓：不審な Src-Dst
T0822	External Remote Services	不正通信	✓：不審な Src-Dst
T0830	Man in the Middle	通信の仲介	✓：不審な Src-Dst
T0840	Network Connection Enumeration	情報収集の通信	✓：不審な Src-Dst
T0843	Program Download	不正通信	✓：不審な Src-Dst
T0845	Program Upload	不正通信	✓：不審な Src-Dst
T0846	Remote System Discovery	情報収集の通信	✓：不審な Src-Dst
T0848	Rogue Master	不正通信(内容不正)	L7 監視が必要
T0866	Exploitation of Remote Services	不正通信	✓：不審な Src-Dst
T0867	Lateral Tool Transfer	通常を装う通信	L7 監視が必要
T0869	Standard Application Layer Protocol	通常を装う通信	L7 監視が必要
T0883	Internet Accessible Device	不正通信	✓：不審な Src-Dst
T0884	Connection Proxy	通常を装う通信	L7 監視が必要
T0885	Commonly Used Port	通常を装う通信	L7 監視が必要
T0886	Remote Services	通常を装う通信	L7 監視が必要
T0888	Remote System Information Discovery	情報収集の通信	✓：不審な Src-Dst

【凡例】✓：検知可能

4.5　監視ルール(L7)による監視の検討

OT分野における多種多様な通信プロトコルのL7での監視を考えるにあたり，仕様がシンプルで分析が容易なプロトコルの基本構造を捉えることから着手し，そこから規則性を見つけ，その他の複雑な構造をもつプロトコルへのルールの転用というアプローチを考える．本節では例として，3章で取り上げたプロトコル群の構造を見ていく．

プロトコル構造を分析していくにあたっては，IPベースのプロトコルが，IPレイヤの情報から階層的に解読が進められるため着手がしやすい．代表的なプロトコルとして，TCP/IPを使ったModbus-TCPとEtherNet/IP (Explicit)のデータグラムの構造を図 4 と図 5 に示す．これらのプロトコルの特徴は，L3レイヤで宛先が決まっているため，データグラムは宛先の機器に対して送るメッセージとなる．OT分野では，マスタとスレーブがRequestとResponseを行う通信が主たるものであり，一般には，データグラムのヘッダには Request 時に実行する機能(またはコマンド)を指定する情報が含まれている．呼び出す機能が書き込みであればRequestのデータ部には書き込みのデータが入り，呼び出す機能が読み出しであれば Response のデータ部には読み出しのデータが入ることが一般的となる．図 4 と図 5 とも，TCP Datagram にアプリケーションデータが格納されるが，その構造は異なっている．しかし，名称は異なるが，命令を表すものとして Modbus-TCP では Function ID，EtherNet/IP では Command という属性が存在している．

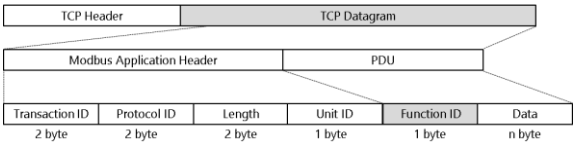


図 4　Modbus-TCP のデータグラム構造

Figure 4　Modbus-TCP datagram structure.

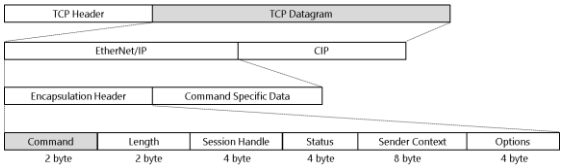


図 5　EtherNet/IP(Explicit)のデータグラム構造

Figure 5　EtherNet/IP(Explicit) datagram structure.

次に，イーサネット上に直接アプリケーション層が乗るプロトコルの代表として，PROFINET IOとEtherCATのデータグラム構造を図 6 と図 7 に示す．一般には，イーサネット上に直接アプリケーション層が乗るタイプのプロトコルは，同期のメカニズムやネットワーク上でのフレーム衝突を避ける機構等，通信のリアルタイム性を実現のための独自性の強い構造をとる．例えば，アドレスについては，PROFINET IOではイーサフレームヘッダのものを使うが，

よりリアルタイム性を重視する EtherCAT では，イーサフレームをブロードキャストでスレーブへ送信し，アドレスはアプリケーション層(EtherCAT Datagram Header の Address 部)に格納しているものを使うという違いがある．構造が大きく異なるとしても，汎用的に監視ルールを作るにあたっては，データグラム内を追い，共通に存在すると考えられる項目に着目していくことが有効であるといえる．

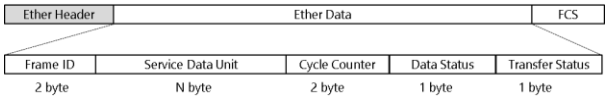


図 6　PROFINET IO のデータグラム構造

Figure 6　PROFINET IO datagram structure.

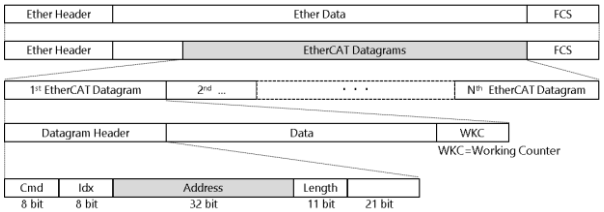


図 7　EtherCAT のデータグラム構造

Figure 7　EtherCAT datagram structure.

5. 提案手法

5.1 監視ルールの生成手法

4 章までで, OT 分野で使用されるイーサネットをベースとしたシェア上位のプロトコル群の特徴を挙げ，プロトコルの汎用監視の基準を作るため通信を定式化し，レイヤに着目した監視手法の検討を行った．通信の監視は，通信の有無が最もシンプルな監視手法である．その他には，基本的な 3 種類の手法に整理される．

1 種類目は，L7 未満で通信パケットのヘッダ情報のみを扱う手法で，詳細さを増す方向に属性を AND で組み合わせ監視ルールを作る手法である(図 8 の①)．例として(SrcMAC, SrcIP, SrcPort, DstMAC, DstIP, DstPort)といった組である．2 種類目は，ペイロード内の属性も AND で組み合わせてルールを作る手法(図 8 の②)である．例として，①により特定される通信において，ペイロード中の”Function ID”が入るバイト位置に，”0x0C”が入るといったルールである．3 種類目は，上下層とは独立に，あるレイヤで登場する属性値を集合としてルールを作る手法(図 8 の③)である．例として，あるネットワークで使用される IP アドレス(L3)は，{192.0.2.10, 192.0.2.11, 192.0.2.20}といったルールである．他にも監視ルールを作成することは可能であるが，それは応用的な監視ルールとして，基本的な監視ルールの組み合わせと考えることができる．

監視ルールごとに，生成手法と特徴について表 8 に整理する．生成手法の面で述べると，①に関しては，イーサネットや IP プロトコルとして仕様が明確かつ情報として枯れている世界であるため，ルール生成において特段工夫を必要としない．②に関しては，多様な仕様を柔軟に扱う工夫が必要であり，本稿では②-1 の手法について 5.2 節で提案を行う．②-2 に関しては，自然言語処理 AI[10]を使った手法が文献[11]で提案されており，これは，ペイロード部を 1 バイトずつの並びと捉え，バイトの種類ごとの登場の規則性を機械学習による学習により定義し，ルール生成を行う．③に関しては，①や②の生成手法の処理工程により抽出される属性値を使うため，①と②を検討することで手法の確立は可能である．

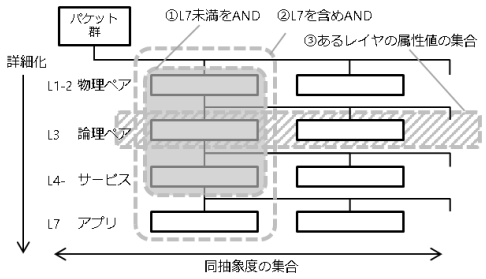


図 8　定式化とルールの対応

Figure 8　Relationship between formulation and rules

表 8　ルールと生成手法

Table 8　Rules and generation methods

対象		生成手法	特徴	精度の課題
①L7 未満/ヘッダ部	①-1	パケット 1 つ 1 つのヘッダ情報を解析	漏れなく確実性が高い	特になし
	①-2	フロー情報を解析	高スループットの通信に効果的	サンプリングレートに依存
②L7 含む/ペイロード部	②-1	仕様書を基にヒューリスティックに特徴を解析	シンプルな仕様に適す	汎用性とトレードオフ
	②-2	機械的に特徴を解析	機械学習	学習性能
③属性の集合/レイヤごと		①, ②の解析で属性を抽出し集合を作る	低レイヤほどシンプル	①, ②に依る

5.2 ペイロード部解析と監視ルール生成

OT 分野で使用される多種多様な通信プロトコルを汎用的に監視するには，プロトコルごとの差異を柔軟に扱う工夫が必要となる．監視ルール生成処理の流れを図 9 に示す．

図 9 は，本手法が，人による事前調査フェーズ，プログラムを使った学習フェーズ，プログラムを使った検査フェーズをもつことを示している．本手法の処理中，ヒューリスティックに発見された規則を“規則性の知識”として蓄えることを行う．仕様が異なる多様なプロトコルの分析には，各フェーズにおいて，規則性を知識として蓄えることが鍵となる．本知識をもって監視ルールを生成し，実際の通信監視にあてるが，一朝一夕にはルールが作れないことが多い．ルール作りの難易度を高めている要因は，大きくは 2 つ存在する．1 つは，監視対象における環境の独自性や把握しきれていないプロトコル仕様などがあった場合の学習や検査における例外発生が不可避ということである．そのケアは必ず必要となる．もう 1 つは，汎用性を重視す

ることで詳細な特徴が監視できないルールとなり，逆に詳細な特徴を監視しようとすると汎用性のないプロトコル個別のルールとなるというトレードオフの関係である．

多様なプロトコルの汎用監視を目指すにあたり，“どのオプション”のさらには“どの属性を使って”規則性を探索していくかは，ルール生成コストおよび汎用性と精度の間のトレードオフを鑑みる必要があり，セキュリティ監視の戦略を考える上での重要事項となる．

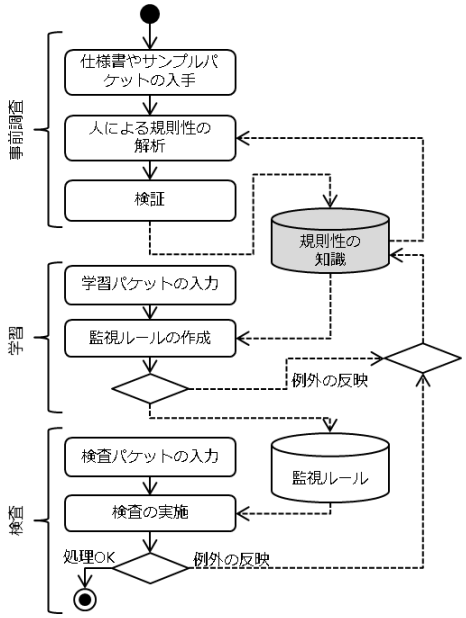


図 9　監視ルール生成処理

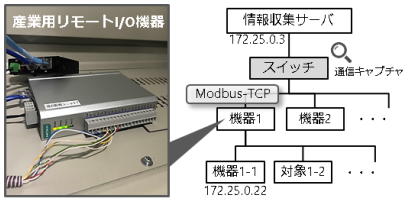
Figure 9　Monitoring rule generation process.

5.3 Modbus-TCP の実機通信の解析

ある商用設備のネットワークの通信キャプチャから抜き出した産業用リモート I/O 機器の Modbus-TCP 通信データを使い，実際の監視ルールを見つけ出す手法について説明する．

図 10 は, ネットワークに流れる 172.25.0.3 と 172.25.0.22 の間のある時間帯の Modbus-TCP の通信を抜き出したものである．表のラベルの 0 から 10 は，TCP レイヤのデータグラムを先頭から 16 進区切りで配列に格納した際の添え字に該当する．図 4 の Modbus-TCP のデータグラム構造からすると，0-1 が”Transaction ID”，2-3 が”Protocol ID”，4-5 が”Length”，6 が”Unit ID”，7 が”Fuction ID”，8 以降が”Data”となる. Modbus-TCP の仕様上, Transaction ID は，1 回の Request と Response により 1 インクリメントされる．また，この例では，Function ID として，”02”(Read Discrete Inputs), ”04”(Read Input Registers)が使用されている．

例えば, 本データは Lenth の”05”と Function ID の”02”でフィルタをかけると，Data に”02 40 01 ・・・”という値を取るということを見ることができる．フィルタによるグルーピングにより，同一バイト位置には，“連番”，“離散的な選択値”，“連続値による値範囲”といったプリミティブな規則が登場してくる．このように実通信キャプチャやプロトコル仕様に基づき，特定バイト位置に登場する値の規則性を発見することで，図 9 の“規則性の知識”を蓄えてくことを行う．“規則性の知識”において汎用性を上げるには，Modbus-TCP でいう Function ID は他のプロトコルでいうと何にあたるか，何でグルーピングをするとどのプリミティブな規則がどの位置に現れるかで，異プロトコル間の共通項を見極めることがポイントとなる．今回, Modbus-TCP での例を示したが，同様の手法で EtherNet/IP や EtherCAT でも規則の発見ができることを確認している．



#	Time	0	1	2	3	4	5	6	7	8	9	10	
	:												
1	03:16.9	41	47	00	00	00	06	00	02	00	00	00	…
2	03:16.9	41	47	00	00	00	05	00	02	02	40	01	…
3	03:16.9	41	48	00	00	00	06	00	04	00	10	00	…
4	03:16.9	41	48	00	00	00	43	00	04	40	00	00	…
5	03:17.1	41	49	00	00	00	06	00	02	00	00	00	…
6	03:17.1	41	49	00	00	00	05	00	02	02	40	01	…
7	03:17.1	41	4a	00	00	00	06	00	04	00	10	00	…
8	03:17.1	41	4a	00	00	00	43	00	04	40	00	00	…
9	03:17.3	41	4b	00	00	00	06	00	02	00	00	00	…
	:												

図 10　Modbus-TCP 通信の例

Figure 10　Modbus-TCP communication example.

5.4 提案手法の適用場面と評価

4.4 節で示したとおり, 通信を伴う攻撃テクニックの多くは正しい通信ペアを監視することで，異常の検知は可能である. 管理外の機器がつながれ通信が行われている状況は，敵対者による侵入の初期段階に現れる兆候である．その後の侵入したネットワークに関する情報の収集や横移動などは, 普段通信相手としない相手との通信として検知される．しかし，物理的な直接的侵入やサプライチェーンを通じた不正プログラムの混入，巧妙な入口対策のすり抜けを考えると，多層防御の観点からも，L7 監視は重要となる．

表 9 に, 環境の特徴に対する監視ルールの評価を整理している．環境の特徴項目は，従来 OT 分野で特徴として挙げられるものと, この先 IT との融合により取り込まれていくと考えられるものの中から 6 項目を選択した．1 から 6 の番号は, 若番ほど現在の OT に顕著な特徴と考えてよい．

表を項目ごとに見ていく．”1. 通信ボリューム”が高スループットな通信は，フローで監視する①-2 が”+ +”と適している。”2. プロトコル仕様”が複雑・把握困難なものは低レイヤの①で監視することが”+ +”と適すが、本稿の主張の L7 の監視を行うことが望ましい。”3. ネットワークの分離“が

未実施の環境は, IT と OT が混在するため IP ヘッダ等で監視する①が”+ +”と適している．”4. 機器の移動”が頻繁”，“5. 通信先が不特定多数”はホワイトリスト型が適さないことを示している．“6. 通信の暗号化”がある場合は，L7 を含む監視は，“-”となる．

本稿が取り上げた課題から，表中でとりわけ注目すべきは，“2. プロトコル仕様”の表中の網掛け部である．②-1 の L7 を含む監視手法は, 仕組みがシンプルであるため固定的に登場するバイト位置の監視に向くが，規則にマッチしない場合は監視をすることができない．しかし，図 11 に示すように②-2 でバイト位置の横方向への規則性を機械的に見つけ出す手法[11]を併用することで，互いに補完することが可能となる．“1. 通信ボリューム”においても，両者は相補的な関係になる． 表 9 は，網羅的な監視を考える上での助けとなる．これらの監視手法を，導入先の環境の特徴に合わせて選んでいくとよい．

表 9　環監視手法の評価

Table 9　Evaluation of monitoring methods.

	環境の特徴項目	1. 通信ボリューム	2. プロトコル仕様	3. ネットワークの分離	4. 機器の移動	5. 通信先	6. 通信の暗号化	1, 2, 3, 4, 5, 6
	特徴	高スループット	複雑・把握困難	未実施	頻繁	不特定多数	あり	左記以外
①L7 未満	①-1	+	+ +	+ +	+	+	+ +	+ +
	①-2	+ +	+ +	+ +	+	+	+ +	+ +
②L 7 含む	②-1	+	+	+	+	+	−	+ +
	②-2	−	+ +	+	+	+	−	+ +
③属性の集合	L7 未満	+ +	+ +	+ +	+	+	+ +	+ +
	L7	+	+	+	+ +	+	−	+ +

【凡例】”+ +”：適，”+”：条件に依存，” − “：不適

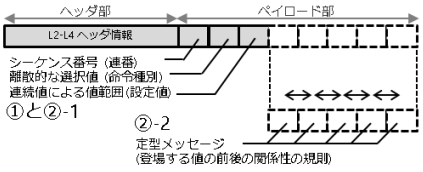


図 11　監視の組み合わせの例

Figure 11　Monitoring Combination Example

6. おわりに

本稿では，近年脅威の顕在化が進む CPS において，セキュリティ対策として通信監視が有効な手段であることを述べ，通信監視には OT の特徴の 1 つである多種多様な通信プロトコルの監視が課題となることを説明した．解決策として，多種多様な通信プロトコルの汎用的監視手法を提案し，マルチレイヤでの監視手法のポジションを示しつつ，総合的な評価を行った．

本稿の知見に基づくと，OT プロトコルにはオプションで IP をもち，L7 未満であれば汎用的に監視を行えるものもある．しかし，これに適合しないものに対しては，L7 監視は必要であり，多数の現場サンプルを用いた規則性の抽出は不可欠である．L7 の汎用監視では，異プロトコル間で共通する規則性の識別をプログラム実装により具現化させることになるが，この際，規則の例外をいかに吸収できるかが汎用性実現の決め手となる．本研究では，環境依存性が高く，最適解の導出が難しいこのチャレンジングな課題を解いていき，図 2 に示す多様なプロトコルの監視のカバレッジを挙げていくことを今後も目指す．

最後に，セキュリティ対策導入の現場目線では，複数の監視手法の導入は多層防御の効果を高めるが，コスト増にもなることから，適材適所やハイブリッドとなる組み合わせ，平時は抽象度高く監視しアノマリ時に監視解像度を上げる等，監視手法の応用的な組み合わせが最適解の一案となってくる．そのため，多様なプロトコルの監視のカバレッジを上げていくこと並び， 表 9 を磨き上げていくことは価値の高い営みとなると考える．

謝辞　本研究の一部は，内閣府が進める戦略的イノベーション創造プログラム（SIP）「IoT 社会に対応したサイバー・フィジカル・セキュリティ」（管理法人：NEDO）によって実施されています．

参考文献

[1] 内閣府, : 第 5 期科学技術基本計画, https://www8.cao.go.jp/cstp/kihonkeikaku/index5.html,(2016).
[2] 経産省, : サイバー・フィジカル・セキュリティ対策フレームワーク https://www.meti.go.jp/policy/netsecurity/wg1/CPSF_ver1.0.pdf, (2019)
[3] HMS Networks, : 産業用ネットワーク市場シェア動向 2021, https://www.anybus.com/ja/aboutus/news/2021/03/31/continued-growth-for-industrialnetworks-despite-pandemic, (2021).
[4] PROFIBUS & PROFINET International Organization, https://www.profibus.com/
[5] ODVA(Open DeviceNet Vendor Association, Inc.), https://www.odva.org/technology-standards/key-technologies/ethernet-ip/
[6] EtherCAT Technology Group,https://www.ethercat.org/default.htm
[7] Modbus Organization, https://www.modbus.org/specs.php
[8] Ethernet POWERLINK Standardization Group, https://www.ethernet-powerlink.org/powerlink/technology
[9] MITRE ATT&CK for ICS, https://attack.mitre.org/matrices/ics/
[10] Devlin, J., Chang, M.-W., Lee, K., and Toutanova, K., : Bert: Pre-training of deep bidirectional transformers for language understanding, arXiv preprint arXiv:1810.04805, (2018).
[11] 山中友貴, 山田真徳, 高橋知克, 永井智大, : BERT を用いたパケットペイロードの特徴抽出, 人工知能学会全国大会論文集, Vol. JSAI2021, (2021).