制御システム向けセキュリティ監視サービスの提供を可能にする不正アクセス検知技術

Unauthorized Access Detection Technique to Provide Security Monitoring Services for Operational Technology Systems

熊崎　裕一郎 KUMAZAKI Yuichiro　　福井　佳宏 FUKUI Yoshihiro

東芝ITサービス(株)は，これまで情報システムを対象にしたセキュリティ監視サービスを提供してきた。近年，情報システムをインフラ施設や工場などの制御システムと接続してデータを利活用するニーズが高まるとともに，制御システムのセキュリティ対策が重要になっている。

そこで今回，情報システム向けで長年の実績があるIDS（Intrusion Detection System：不正侵入検知システム）を応用し，制御システムへの不正アクセスなどを検知するための技術を開発した。制御システム向けセキュリティ監視サービスへの開発技術の提供を目指し，検証を進めている。

Toshiba IT-Services Corporation has been developing and delivering security monitoring services targeted at information technology (IT) systems. Accompanying the increase in demand for effective utilization of data collected by operational technology (OT) systems in infrastructure facilities and factories by directly connecting IT systems to OT systems, there is a growing need for enhanced countermeasure techniques to protect OT systems from cyberattacks.

With this as a background, we have developed an unauthorized access detection technique for OT systems utilizing our intrusion detection system (IDS), which has already established a long track record in the field of IT systems. We are now conducting verification tests with the aim of applying this technique to security monitoring services for OT systems.

1. まえがき

東芝ITサービス(株)は，マネージドサービスの一環として，情報システムを対象としたセキュリティ監視サービスを提供してきた。しかし近年，サイバー攻撃の対象として，インフラ事業者の供給システムや製造業者の生産システムなど，いわゆる制御システムが含まれるようになっており，制御システム向けのセキュリティ監視サービスの需要が高まっている。

ここでは，情報システム向けのセキュリティ対策製品を応用した，制御システム向けのセキュリティ監視に必要な技術の開発について述べる。

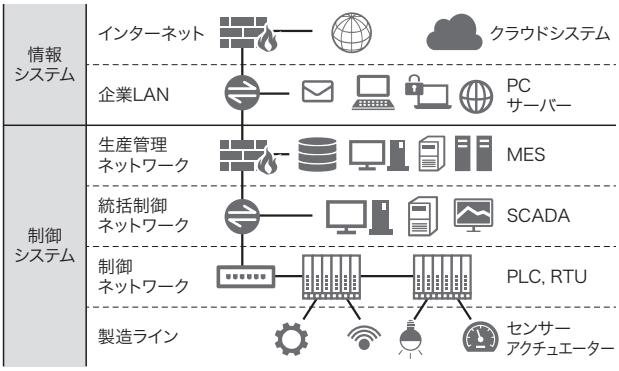
2. 情報システムと制御システムの違い

これまで，コンピューター，その周辺機器，及びネットワーク機器で構成されたシステムを，情報システムと呼んできた。

それに対して，工場で生産工程の自動化を目指して，各種の加工装置や搬送装置及び検査装置を通信用ケーブルで接続する仕組みも独自の発達を遂げており，これらのシステムを制御システムと呼んでいる。

かつて，制御システムの物理的な通信規格は，加工装置メーカーごとの独自規格であったが，2000年頃から，EthernetやIP（Internet Protocol）ネットワークなど，オープン技術が導入されてきた[1]。

2000年頃にはサイバー攻撃が現実のものとなり，情報システム向けのセキュリティ対策製品が数多く提供されるよう



PC：パソコン
MES：Manufacturing Execution System
SCADA：Supervisory Control and Data Acquisition
PLC：Programmable Logic Controller
RTU：Remote Terminal Unit

図1. 情報システムと制御システムの接続例

インターネットと制御ネットワークが接続され，製造ラインもサイバー攻撃に遭うおそれがある。

Example of connections between IT and OT systems

になった。オープン技術を導入した制御システムもサイバー攻撃の被害を受けるおそれがあったが，その時点では情報システムと制御システムは完全に切り離されている環境にあり，制御システムにおけるセキュリティ対策は余り考慮されなかった。

しかし，近年では，迅速な経営判断の実現や顧客への情報提供のため，**図1**に示すように情報システムと制御システムを接続し，生産実績などの情報を情報システムに取り込む事例が増えており，制御システムにおけるセキュリティ対策は重要な課題となっている。

当社は，豊富な情報システム向けセキュリティ対策製品を制御システムに応用することで，制御システムにおいても強固なセキュリティ対策の実現を目指している。

3. 制御システムにおけるセキュリティ対策

情報システムで利用されているセキュリティ対策機器を制御システムに応用する場合，次のような課題がある。それぞれへの対応方法を示す。

3.1 プロトコルの乱立への対応

図1の制御ネットワークのレイヤーでは，Ethernetの利用が進んでいるが，通信プロトコルは情報システムとは大きく異なっており，**図2**に示すように乱立ともいえる状態である。そのため，情報システムで使用されるIDSやファイアウォールは，プロトコルを解析して不正アクセスを検知するという原理上，制御システムで利用することができない。これを解決するため，強力なカスタムシグネチャー定義機能を持ったIDSを用いて，個別にプロトコルを定義することで，制御システムのプロトコルを認識する技術を開発した。

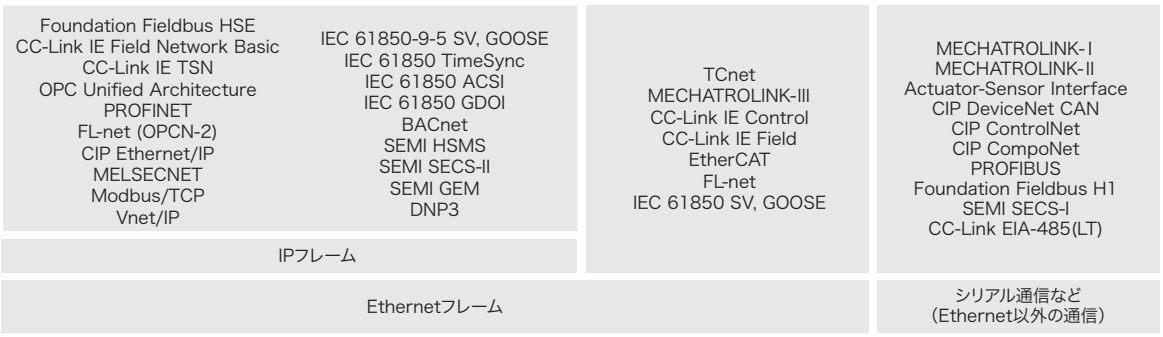
当初，制御システムプロトコルの机上調査を実施したが，プロトコルの開発各社は，機密保持の観点から仕様の開示に消極的であり，成果が得られなかった。そのため，まず自社内に検証環境を用意し，パケットを解析するところから開始した。解析結果を反映したカスタムシグネチャーを設定したIDSで，プロトコルの認識ができることを確認した。その後，幾つかの生産現場の協力を得てパケットを採取し，IDSで制御システム向けプロトコルが認識できるかどうかの検証を繰り返した。

その結果，IDSでプロトコルは認識できるが，現実の生産現場のネットワークでは加工機器の都合などでプロトコル仕様を拡張している場合もあり，個々の現場に合わせた調整が不可欠であることが分かった。また，製造ラインの変更があった場合にも，調整が必要であることが分かった。

最終的に，実際の生産現場で制御ネットワークを介して送受信されるパケットを採取して，そのパケットの内容を分析してカスタムシグネチャーを作成し，不正アクセス検知を実現する技術を開発できた。パケットの分析は，理論も必要だが，それ以上に経験に頼る部分が多く，十分な解析経験を積んだ技術者が必要である。より多くの技術者の育成が，今後の課題である。

3.2 不正アクセス検知の考え方の違いに対する対応

情報システムでは，各端末が任意のタイミングで多種多様な処理を行うので，正常な動作パターンの定義が難しい。



HSE：High-Speed Ethernet
TSN：Time-Sensitive Networking
OPC：Open Platform Communications
CIP：Common Industrial Protocol
TCP：Transmission Control Protocol
Vnet: Azure Virtual Network
IEC 61850：国際電気標準会議規格 61850
SV：Sampled Values
GOOSE：Generic Object Oriented Substation Events
ACSI：Abstract Communication Service Interface
GDOI：Group Domain of Interpretation
SEMI：Semiconductor Equipment and Materials International
HSMS：High-Speed Message Service
SECS：SEMI Equipment Communications Standard
GEM：Generic Equipment Model
DNP：Distributed Network Protocol
EtherCAT：Ethernet for Control Automation Technology
CAN：Controller Area Network
PROFIBUS：Process Field Bus
EIA：Electronics Industries Alliance
LT：Long Term

図2. 制御システムのプロトコル
制御システムでは，情報システムとは異なり，多数のプロトコルが乱立しているのが現状である。
Protocols for OT systems

そのため，既知の攻撃手法を収集し，照合することで，不正アクセスを検知する仕組みが確立している。

一方，制御システムでは，原則として，各種機器が所定のタイミングで，所定の動作を行うので，正常な動作パターンが定義できる。更に，制御システムを構成する加工装置などでは，内部にコンピューターがあり，汎用OS（基本ソフトウェア）が動いている場合も多いが，加工装置としての品質保証上の観点から，ウイルス対策ソフトウェアなどのセキュリティ対策ソフトウェアがインストールできない。そのため，正常な動作パターンを定義して，そこから逸脱した通信を発見することで不正アクセスを検知する仕組みが有効である[2]。

このような違いがあるため，情報システムに熟練したセキュリティ技術者を，制御システムへ転換することが簡単ではなく，制御システムに特化した技術者を育成する必要がある。

3.3　データ部の改ざんへの対応

図3に，FL-netと呼ばれる制御用プロトコルのパケット例を示す。

情報システムのIDSでは，主にパケットのヘッダー部だけを参照して不正アクセスを検知し，データ部まで参照することは多くない。

制御システムを妨害する場合は，パケットのデータ部であるユーザーデータの中で，特定箇所の値を改ざんするだけで目的は達成できる。例えば，アクチュエーターなどに指示する数値を改ざんすれば，アクチュエーターが想定外の動きをして，製造ラインを混乱させることができる。したがって，制御システムにおける不正アクセス検知では，対象の制御システムにおけるユーザーデータの内容を，その意味レベルで特定し，その上で意味的に正常な範囲の数値を指示した通信であることを特定するためのカスタムシグネチャーを作成する必要がある。

当社は，生産現場で送受信されるパケットを分析することで，ユーザーデータ部も含めて解析する技術を確立した。ただし，カスタムシグネチャーの制約から，解析結果のとおりに厳密な実装ができない場合がある。

3.4　高可用性への対応

情報セキュリティの三要素には，機密性・完全性・可用性があり，情報システムでは機密性が重視されることが多いが，制御システムでは可用性が重視される。

IDSの設置位置を例に取ると，情報システムでは，重要なサーバーの手前にIDSを配置し，攻撃と判断した通信を排除する構成が一般的である。特に重要な情報を扱う情報システムでは，障害などでIDSが停止した場合，機密性の確保を優先してシステム全体を停止させる場合もある。

一方，制御システムでは，生産継続が最重要課題であり，IDSが停止した場合にも生産ラインを停止させることはできない。

当社は，制御システムで不正アクセス検知を行う場合，IDSをネットワークの経路上に設置するのではなく，ネットワークを介して送受信されるパケットのコピーを受け取る位置に設置することを提案している（**図4**）。ポートミラー機能は，SCADA（Supervisory Control and Data Acquisition）とPLC（Programmable Logic Controller）を接続しているスイッチングハブにより提供される機能であり，装置の増設の必要はなく，障害ポイントが増えることもない。

しかし，この構成を採用すると，不正アクセスを検知できても不正なパケットを排除できなくなる。そのため，IDSで不正アクセスを検知した場合は，直ちに生産管理者に伝える仕組みを整える必要がある。

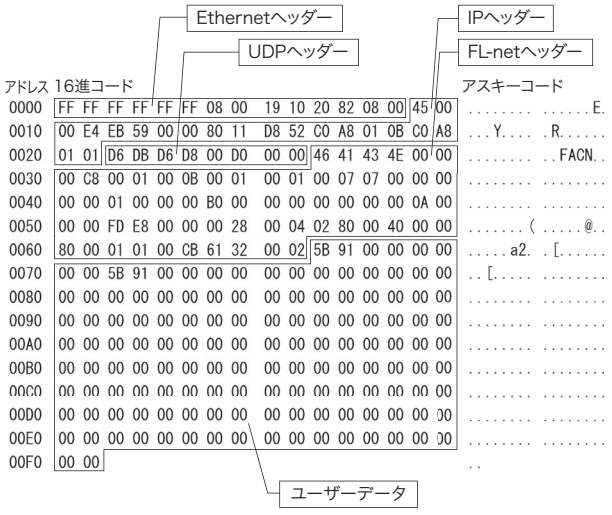


図3. 制御システム用プロトコルのパケット例

FL-netプロトコルのパケットでは，UDP（User Datagram Protocol）ヘッダーの次に，FL-net独自のヘッダーがある。

Example of packet format of OT system

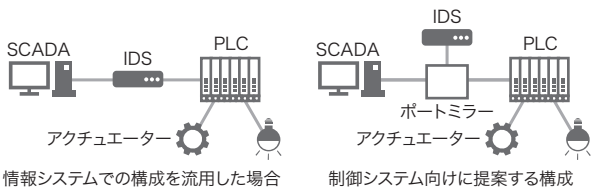


図4. IDSの設置位置

制御システム向けの構成では，万一，IDSに障害が発生しても，生産ラインには影響がない。

Examples of IDS installation position in case of IT and OT systems

4. 開発した技術の特長と今後の課題

4.1 不正アクセス検知技術

IDSのカスタムシグネチャー定義を用いて制御システムプロトコルを認識させることにより，当初の目的である情報システム向けセキュリティ対策製品を制御システムへ応用することは実現できた。また，制御システム向けに，正常な動作パターンをIDSに組み込み，その動作パターンからの逸脱を不正アクセスとして検知する方法を採用した結果，新たな攻撃手法が生まれても，検知できる可能性が高いというメリットが得られた。

一方，この検知方法では，IDSに組み込んだ動作パターンから少しでも逸脱したものを不正アクセスとみなすため，業務の遂行に支障が出ることがある。これを避けるために，時間と費用を掛けてIDSに組み込む動作パターンを更新する必要がある。

今回開発した制御システム向け不正アクセス検知技術でも，動作パターンに相当するカスタムシグネチャーの，最初の定義及びその後生産現場に変更が発生した際の更新については，個々の生産現場の状況に適合するよう，確実に実行する必要がある。カスタムシグネチャーの定義に失敗すると，過検知率が高くなり，実用に耐えられないおそれもある。

今後，動作パターンの維持に掛かる時間と費用の削減を目指し，AI技術の適用[3]や，統計的なパケット分析手法の適用[4]を検討していく。

4.2 セキュリティ監視サービスへの展開

IDSは，元々情報システムで利用されてきた機器であり，当社のリモート監視サービスやリモート運用サービスにおいても，長年，サービスの対象機器としてきた実績がある。

制御システムにおいて，今回開発した，カスタムシグネチャーによる不正アクセス検知の仕組みは，IDSを応用したものであり，これまで情報システム向けに提供してきたセキュリティ監視サービスと同一の枠組みで，制御システム向け監視サービスを提供できる。

4.3 将来に向けて

無人運転をしている制御システムの場合，不正アクセスに気付きにくいことがある。そのような場合に備えて，カスタムシグネチャーを用いたIDSで不正アクセスを検知し，制御システム向けセキュリティ監視サービスにより監視することで，異常事態発生を顧客へ直ちに通知できるようになる。顧客は，通知を受けて迅速に対処できるようになり，制御システムの可用性を確保できる。

5. あとがき

今回，多数の生産現場の協力を得て，実証実験を行うことができた。その実証実験を通じて，情報システム向けのIDSを応用した，制御システム向けの不正アクセス検知技術を確立した。制御システム向けセキュリティ監視サービスへこの技術を適用することで，インフラシステムや製造ラインを対象としたサイバー攻撃の防止に貢献できる。

今後は，見逃し率と過検知率が実用に耐える範囲に収まることの検証を進めて，技術の完成度を高めていく。

文　献

(1) 中谷昌幸. “つながる制御システムをサイバー攻撃から守る”. JPCERTコーディネーションセンター. <https://www.jpcert.or.jp/magazine/icsr-articles/ics-sec-nikkan1.html>, (参照 2022－01－26).
(2) 高山祐磨，ほか. IoT時代における制御システムサイバーセキュリティ. 信学技報. 2016, **116**, 131, ICSS2016-25, p.65–70.
(3) 原田雄基，ほか. SVMを用いた制御システムに対する偽装命令攻撃の検知. 信学技報. 2021, **121**, 118, ISEC2021-15, p.35–40.
(4) 桂井銀河，ほか. 制御ネットワーク向けトラフィック監視方式に関する検討. 信学技報. 2021, **121**, 198, CS2021-56, p.20–25.

熊崎　裕一郎　KUMAZAKI Yuichiro
東芝 IT サービス (株)
サポート & ソリューション統括部 ソリューション推進部
システム監査学会会員
Toshiba IT-Services Corp.

福井　佳宏　FUKUI Yoshihiro
東芝 IT サービス (株)
サポート & ソリューション統括部 ソリューション推進部
Toshiba IT-Services Corp.