制御システム向け攻撃検知技術の実現に向けて

内山 宏樹　　大和田 徹　　萱島 信

(株)日立製作所 横浜研究所
244-0817 神奈川県横浜市戸塚区吉田町 292 番地
{hiroki.uchiyama.tm, toru.owada.wq, makoto.kayashima.hh}@hitachi.com

あらまし 電力，鉄道，水道，ガスといった社会インフラや自動車で利用される制御システムは，これまで専用 OS や専用プロトコルを利用しており，外部ネットワークからアクセスできない領域に設置されているため，サイバー攻撃は受けないと考えられてきた。しかしながら，コスト削減や効率向上のために，汎用技術の利用や情報システムとの接続も進んでいる。これらの背景から，制御システムにおいてもセキュリティ対策技術が求められている。

本稿では，汎用化や相互接続が進展した制御システムに内在する脅威とその対策方針から，制御システムの制約上今後必須になってゆく制御システム向け攻撃検知技術を抽出し，その基本要件について報告する。

Towards Implementation of Attack Detection Technology for Industrial Control Systems

Hiroki Uchiyama　　Toru Owada　　Makoto Kayashima

Hitachi, Ltd., Yokohama Research Laboratory
292, Yoshida-cho, Totsuka-ku, Yokohama-shi, Kanagawa, 244-0817, JAPAN
{hiroki.uchiyama.tm, toru.owada.wq, makoto.kayashima.hh}@hitachi.com

Abstract According to use of open platform and connecting to information systems, industrial control systems of social infrastructure like electricity, water supply and railway are facing to cyber threats. In this paper, we describe basic requirements of attack detection technology for industrial control systems based on function and resource limitation of the system.

1 はじめに

電力，鉄道，水道，ガスといった社会インフラや自動車で利用される制御システムは，これまで専用 OS や専用プロトコルを利用しており，インターネット等の外部ネットワークからアクセスできない環境に設置されているため，サイバー攻撃の影響は受けないと考えられてきた。しかしながら，現在，コスト削減や効率性の向上のために，汎用技術の利用や情報システムの接続が進展している。これらの背景から，情報システムだけでなく，

制御システムにおいても同様にセキュリティ対策技術が求められている。しかしながら，制御システムはリアルタイム性や長期保守性といった情報システムとは異なる要件があり，情報システムに適用可能なセキュリティ技術をそのまま制御システムに適用することは困難であることが明らかとなっている[1]。本稿では，制御システムの制約上今後必須となってゆくセキュリティ技術である攻撃検知技術の基本的な要件について検討した結果を報告する。以下では，まず，第 2 章において典型的な制御システムに内在する脅威を明らかにする。次に，第 3 章で抽出した脅威への対策方針を立案し，第 4 章において制御システム向け攻撃検知技術に求められる要件の検討結果を示す。最後に第 5 章でまとめと今後の課題を示す。

2　制御システムに内在する脅威

本章では，典型的な制御システムに内在する脅威を明らかにするために脅威分析を実施した結果を示す。

2.1 制御システムの構成

本稿で対象とする典型的な制御システムの構成を図 1に示す。

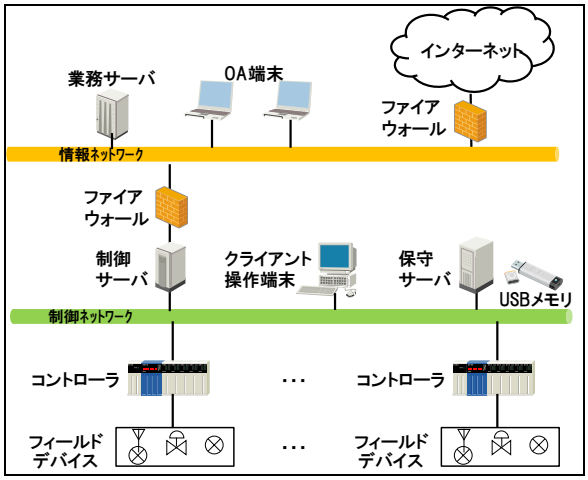

図 1　制御システムの構成

対象とする制御システムは，情報ネットワークと制御ネットワークの 2 層で構成されているシステムであり，制御ネットワークにセンサやアクチュエータといったフィールドデバイスを制御するコントローラや保守サーバが接続されている。情報ネットワークには業務用サーバや OA 端末が接続されており，インターネットにもアクセス可能である。情報ネットワークと制御ネットワークおよび情報ネットワークとインターネットはファイアウォールで遮断されている。

2.2 前提条件

図 1で示した制御システムに内在する脅威を抽出するために，表 1に示す前提条件を設定した。

表 1　前提条件

分類	前提	
利用環境	情報ネットワーク内の保護	ファイアウォール，アンチウィルス等の汎用的なセキュリティ対策技術が導入されている
	制御ネットワーク内の保護	セキュリティ対策技術は導入されていない
	自然災害の対策	自然災害の対策は実施されている
物理環境	システムのロケーション	対象システムは入退室管理がなされた環境に設置されており，外部者は直接アクセスできない
人的環境	ユーザの資質・適正	内部者は意図的に不正を行わない

2.3 脅威抽出

前節で設定した前提条件をもとに脅威の発生箇所（エントリポイント），脅威エージェント，保護対象資産を設定し，対象システム

に内在する脅威の抽出を行う。

2.3.1 エントリポイントの設定

対象システムの外部からのアクセス可能性という観点でエントリポイントを設定した。結果を表 2に示す。

表 2 エントリポイント

#	発生点	補足説明
1	インターネット境界	インターネットからファイアウォールをすり抜け侵入する
2	保守サーバ	保守員が保守作業時に接続した USB メモリを経由して侵入する

2.3.2 脅威エージェントの設定

対象システムにおいて脅威を顕在化させる主体を設定した。結果を**表** 3に示す。**表** 1で示した前提条件から，内部者による攻撃は発生しないと仮定しているため，外部者による脅威と内部者の不注意から侵入するマルウェアによる脅威が考えられる。

表 3 脅威エージェント一覧

#	脅威エージェント	意味
1	外部者	制御システムの運用や保守に携わらない無関係な第三者
2	マルウェア	保守員の USB 経由で感染する不正プログラム

2.3.3 保護対象資産の設定

対象システムにおいて保護すべき対象資産を設定した。情報システムでは，保護対象資産はデータ等の情報であり，これらの情報が漏洩しないことが最も重要となるが，制御システムでは，センサやアクチュエータといったフィールドデバイスを適切に制御し続けることにより，社会インフラとして提供されるサービスを維持することが最も重要となる。そのため，ここでは，フィールドデバイスの制御を行う「コントローラ」を保護対象資産であると設定した。

2.3.4 脅威抽出

前節までに設定したエントリポイント，脅威エージェント，保護対象資産から，**図** 1で示した対象となる制御システムにおいて発生する脅威の一覧を 5W 法[2]を活用して，発生場所(Where)，関与者(Who)，発生タイミング(When)，動機(Why)，脅威内容(What)の観点で抽出した。なお，ここでは，発生タイミング(When)は特定せず，動機(Why)は**表** 1で示した前提条件から悪意のあるもののみとした。また，脅威内容(What)は**表** 4に示す STRIDE[3]の中で，保護対象資産であるコントローラの動作に悪影響を及ぼす可能性がある”Spoofing”，”Tampering”，”Denial of Service”，”Elevation of Privilege”の 4 種類の攻撃手法を用いて脅威を抽出した。結果を**表** 5に示す。

表 4 STRIDE による攻撃方法の分類

攻撃方法	意味
Spoofing（なりすまし）	正当な機器やプログラムをなりすまし，不正にアクセスする
Tampering（改ざん）	正当なデータやプログラムを不正に改ざんする
Repudiation（否認）	あるアクションの実行を否定する
Information Disclosure（情報漏えい）	内部の機密情報を漏洩させる
Denial of Service（サービス不能攻撃）	大量のデータを送信し，アクセス不能にする
Elevation of Privilege（権限昇格）	脆弱性等を悪用し，上位権限を取得し，不正を行う

表 5 脅威一覧

脅威 ID	Where	Who	What	
1	インターネット境界	外部者	Spoofing	正当な端末であるとなりすまして，制御サーバ経由でコントローラにアクセスする
2			Tampering	制御サーバに侵入し，制御サーバからコントローラに送信するデータを改ざんする
3			Denial of Service	制御サーバに侵入し，制御サーバからコントローラに大量のデータを送信し，動作不能にする
4			Elevation of Privilege	制御サーバに侵入し，制御サーバの管理者権限を取得し，コントローラにアクセスする
5	保守サーバ	マルウェア	Spoofing	保守サーバ内の正当なプログラムなりすましてコントローラにアクセスする
6			Tampering	保守サーバからコントローラに送信するデータを改ざんする
7			Denial of Service	保守サーバからコントローラに大量のデータを送信し，動作不能にする
8			Elevation of Privilege	保守サーバの管理者権限を取得し，コントローラにアクセスする

脅威を抽出した結果，エントリポイントから保護対象資産であるコントローラへのアクセスルートは 2 種類あり，各ルートにおいて，コントローラの動作に悪影響を及ぼす脅威が想定されることが明らかとなった。

3 対策方針の立案

本章では前章で抽出した脅威への対策方針を明らかにし，制御システムで有効となるセキュリティ対策技術を検討した結果を示す。

3.1 対策方針の検討軸

脅威への対策方針の立案は，一般的にセキュリティ対策方針を検討する際に利用される**表 6**の検討軸を利用した。ただし，攻撃者の動機の抑制といった技術的な対策に繋がらない項目である「抑止」は除外した。

表 6 対策方針の検討軸

項目	内容
抑止	脅威の発生自体を抑制する
予防	脅威の発生確率を低減する
検知	脅威が発生したことを検知する
回復	保護対象資産を脅威発生前の状態に復旧する

3.2 対策方針一覧

表 5の各脅威のうち，インターネット境界をエントリポイントとして顕在化する脅威に対する対策方針を表 6の検討軸を用いて立案した。結果を表 7に示す。なお，ここでは記載を省略しているが，保守サーバをエントリポイントとする脅威の対策方針も同様に立案可能である。

表 7 対策方針一覧

脅威 ID	対策方針	
1	予防	サーバや端末のなりすましができないようにする
	検知	サーバや端末のなりすましを検知する
	回復	なりすましたサーバや端末からのアクセスを遮断する
2	予防	送信データの改ざんができないようにする
	検知	送信データの改ざんを検知する
	回復	改ざんされたデータを正常なデータに復旧する
3	予防	ネットワーク内に大量のデータを送信できないようにする

	検知	制御サーバからの大量のデータ送信を検知する
	回復	制御サーバからの大量のデータを遮断する
4	予防	制御サーバにパッチを適用し，既知脆弱性をなくす
	検知	制御サーバにアクセスログを残し，定期的に検証する
	回復	不正な管理者権限を用いたアクセスを遮断する

3.3 制御システムで有効な対策技術

前節で抽出した対策方針に対して，表 1で定めた前提条件から制御システムでの実現可能性を評価した。結果を表 8に示す。

表 8 対策方針の評価

対策方針	評価	理由
サーバや端末のなりすましができないようにする	×	なりすまし行為そのものの防止は困難
サーバや端末のなりすましを検知する	○	相互に機器認証を実施することにより検知可能
なりすましたサーバや端末からのアクセスを遮断する	×	遮断に伴い，通常の制御業務への影響が出る可能性あり
送信データの改ざんができないようにする	×	改ざん行為そのものの防止は困難
送信データの改ざんを検知する	○	メッセージ認証コードを用いることにより検知可能
改ざんされたデータを正常なデータに復旧する	×	復旧のためのデータバックアップは処理遅延に繋がり，実施困難
ネットワーク内に大量のデータを送信できないようにする	×	DoS 攻撃そのものの発生防止は困難
制御サーバからの大量のデータ送信を検知する	○	ネットワーク監視により検知可能
制御サーバからの大量のデータを遮断する	×	遮断に伴い，通常の制御業務への影響が出る可能性あり
制御サーバにパッチ適用し，既知脆弱性をなくす	×	構成変更が伴うため，パッチ適用は困難
制御サーバにアクセスログを残し，定期的に検証する	○	ログの記録と検証により検知可能
不正な管理者権限を用いたアクセスを遮断する	×	遮断に伴い，通常の制御業務への影響が出る可能性あり

○：実現可能性有　×：実現困難

以上の検討結果から，対象とする制御システムでは問題発生前に対策を施す予防的な対策や問題発生後の復旧策よりも，問題発生を素早く見つけ出す検知策の実現可能性が高いことが明らかとなった。これは情報システムがセキュリティ機能の導入や構成変更に対する許容度が高い点と大きく異なり，特徴的な点であると考えられる。よって本研究では，まず検知策に関する検討から進め，その後，予防策や復旧策の実現性向上に向けた検討を進めることとした。

4　制御システム向け攻撃検知技術

本章では，制御システム向け攻撃検知技術を検討する上で必要となる制御システムの要件と従来技術の問題点を明らかにし，制御システム向け攻撃検知技術の基本的な要件を導出する。

4.1 制御システムの要件

制御システムは，社会インフラ等で提供されるサービスの維持に利用されるため，情報システムとは求められる要件が大きく異なることが知られている。情報システムと制御シ

ステムの主な相違点を表 9に示す[1]。

表 9 情報システムと制御システムの比較

比較項目	情報システム	制御システム
保護対象	情報	物理プロセス
脅威 顕在化時 の影響	情報漏えい 金銭的被害	危険状態に陥る
対策 優先度	機密性(C) 完全性(I) 可用性(A)	可用性(A) 完全性(I) 機密性(C)
稼働率	95-99%	99.9%-99.999%
ライフ サイクル	3-5 年	10-20 年 (構成変更困難)
外部接続	インターネットと常時接続	なし
機器構成	ほぼ全ての機器が同スペック	様々なリソースを持つ機器が存在

このような要件の違いから，制御システム向け攻撃検知技術を実現するにあたっては，様々なリソースを持つ機器に適用可能であり，長期間構成変更や更新が不要であり，高稼働率を実現する技術が求められる。

4.2 従来技術とその課題

従来の攻撃検知技術として，暗号等を用いたセキュリティ技術，侵入検知技術，振る舞い検知技術が知られている。本節では各技術の概要と制御システムへの適用時の課題を示す。

4.2.1 暗号等を用いたセキュリティ技術

なりすまし，改ざん等の攻撃を検知する技術として暗号等を用いたセキュリティ技術が知られている。代表的なセキュリティ技術としてIPsec[4]がある。IPsecでは通信を行う二者間で鍵共有し，共有した鍵を用いて暗号通信を実施するため，共有した鍵を持たない不正な第三者によるなりすましや改ざんを検知することが可能となる。しかしながら，IPSecを実現するためには，従来組込まれていなかった暗号機能を各端末に実装する必要があるという問題や，データの暗号化に伴い，従来よりも送受信時に各端末の処理時間が増加し，制御システムの業務フローの再設計が必要になるといった問題も考えられる。

4.2.2 侵入検知技術

Snort[5]に代表される侵入検知システム（IDS）はホストベース IDS とネットワークベース IDS があり，用途によって使い分けられている。ホストベース IDS は各端末に侵入検知機能を実装する形態であり，端末への不正アクセスを検知可能であるものの，各端末の負荷は大きくなる。一方，ネットワークベース IDS は検知専用の機器を設置し，ネットワークを流れるパケットに不正なパケットが含まれていないか検証する形態であり，各端末の負荷は高くないものの，大量のパケットが流れるネットワークの場合，検知漏れが発生するケースがある。どちらのケースでもシグニチャと呼ばれるパターンファイルを定期的に更新する必要があり，このシグニチャを用いて，攻撃の発生有無を判断する。しかしながら，制御システムはインターネット等の外部ネットワークとは直接接続されていないことが多く，シグニチャを更新することは困難であるといった問題がある。また，制御システムは情報システムとは異なるデータフローであるため，情報システム向けに作成されたシグニチャを利用した場合，誤検知が多発する可能性があるといった問題も考えられる。

4.2.3 振る舞い検知技術

本技術は，正常時のネットワークの構成やデータフローをモデル化し，そのモデルに合致しないフローが発生した場合に攻撃検知を行う技術である[6][7]。情報システムでは，正常時のネットワークの構成やデータフローが固定化できないため，適用することは困難であったが，制御システムではネットワーク構成やデータフローがシステムの導入時から基本的に変化しないため，適用可能であると考

えられている。しかしながら，本技術を適用するためには正常運用時のデータフローだけでなく，緊急時にのみ実行されるデータフロー等も含めて全てをモデル化しておかなければならず，万が一漏れが発生した場合には，誤検知により緊急時の対応の遅れに繋がる可能性があるといった問題がある。

4.3 攻撃検知技術の要件

前節までの検討結果から，制御システム向け攻撃検知技術に求められる要件を明らかにする。表 10 に示す制御システムの特徴から，攻撃検知技術は長期間更新が不要で本来の業務に影響を与えず，リソースを消費しない方式が要求される。しかしながら，従来の情報システム向け検知技術では，制御システムの上記要件を満足できないと考えられる。よって，制御システム向け攻撃検知技術は，**表 10** に示す要件を満足することが必要となる。

表 10 制御システム向け攻撃検知技術の要件

#	特徴	従来技術の課題	要件
1	様々なリソースを持つ機器が存在	機器の使用リソースが増加	機器のリソースを消費しないこと
2	構成変更が困難	業務フローの再設計が必要	既存業務への影響がないこと
3	外部接続無	定期的なアップデートが必要	定期的な更新が不要であること
4	高稼働率	誤検知による業務停止が発生	誤検知が発生しないこと

今後，制御システム向け攻撃検知技術を実現してゆくためには，**表 10**の要件を満足した上で，制御システム内で取得可能な情報を活用し，かつ，社会インフラ向けに高度化する攻撃にも対応可能な実用性の高い方式を立案してゆく必要がある。

5 まとめと今後の課題

本稿では，制御システムで発生する脅威を明らかにし，その脅威の対策技術として，制御システムでは攻撃検知技術の実現可能性が高いことを示した。また，制御システム向け攻撃検知技術に求められる基本的な要件を制御システムの特徴をもとに抽出した。今後は抽出した要件を満足した制御システム向け攻撃検知技術を具体化し，プロトタイプシステムを用いた実現性評価を進めてゆく予定である。

参考文献

[1] “重要インフラの制御システムセキュリティと IT サービス継続に関する調査,” IPA, March 2009.

[2] 織茂,津原,山本,佐々木, ”情報システムにおけるセキュリティ対策立案のための計画手法,” 情報処理学会論文誌，Vol.41，No.1, pp.177--187, January 2000.

[3] Adam Shostack, “Experiences Threat Modeling at Microsoft,” Proceeding of the Workshop on Modeling Security (MODSEC08), September 2008.

[4] S. Kent and K. Seo, “Security Architecture for the Internet Protocol,” RFC 4301, December 2005.

[5] Martin Roesch, “Snort – Lightweight Intrusion Detection for Networks,” Proceedings of LISA ’99: 13th Systems Administration Conference, November 1999.

[6] S. Cheung et al., “Using Model-based Intrusion Detection for SCADA Networks,” Proceedings of the SCADA Scientific Symposium, 2007.

[7] A. Valdes and S. Cheung, “Communication Pattern Anomaly Detection in Process Control Systems,” Technologies for Homeland Security 2009(HST ’09), 2009.