制御システムのセキュリティエンジニアリング

Security Engineering for Control System

川澄 優樹 *1　落合 一郎 *1　横山 憲一 *1
Masaki Kawasumi　Ichiro Ochiai　Kenichi Yokoyama

重要インフラを支えている制御システムには高度な可用性が求められるため，近年散見されるサイバー攻撃からシステムを守ることは必須である。しかし，そのセキュリティ対策においては，制御システム特有の要件や運用上の条件に配慮した適切なエンジリアリングを実施しなければ，逆にシステム停止を誘発してしまいかねない。横河電機では長年にわたりお客様に制御システムを納めてきた経験と，標準化活動への参加を通して得られた知見をもとに，セキュリティ対策実現のベストプラクティスを確立している。横河電機ではこのベストプラクティスをもとに適切なセキュリティエンジニアリングを提供している。本稿では，制御システムに対する横河電機のセキュリティの考え方やそのエンジニアリングについて紹介する。

High availability is required in control systems that support critical infrastructures. Therefore, they must be protected from a growing number of cyber-attacks. However, without appropriate consideration of the requirements and operational conditions specific to control systems, engineering for security measures may cause system failure. Meanwhile, Yokogawa has established its own best practices for security measures based on its wealth of experience in providing control systems to customers over many years and through knowledge obtained through its involvement in international and governmental standardization. Yokogawa can offer proper security engineering based on these best practices. This paper introduces Yokogawa's security concept for control systems and the related engineering.

1. はじめに

情報システムには様々なセキュリティ対策がある。しかし，高度な可用性を求められる制御システムにおいては，それらをそのまま導入することはできず，対策の選別，適切なエンジニアリングが必要である。横河電機ではそれら対策を研究し，制御システムに相応しいセキュリティ対策を選別している。更にセキュリティ対策実現のベストプラクティスを確立，それに基づいたセキュリティエンジニアリングを提供している。本稿ではこのセキュリティエンジニアリングについてその概要を紹介する。

2. ネットワークアーキテクチャ

横河電機では例え上位層の防御が破られても下位層内の資産（ワークステーションなど）は守るといった多層防御ポリシーを提唱している。多層防御を実現するためには適切なネットワークアーキテクチャを構築することが重要である。そして，このネットワークアーキテクチャはセキュリティ対策の土台となるものである。制御システム向けセキュリティの標準規格である ISA99 ではリスク，コスト，エラーを減らし，堅牢，安全，費用効果のあるシステムを構築するために機能毎に Level に分けることを推奨している。これを Purdue model[1] と呼んでいる。横河電機ではこの ISA99 で提唱されている Purdue Model に従ったアーキテクチャを提供している（**図 1**）。以下，各 Level の役割を説明する。

- Level 3.5 – DMZ (Demilitarized Zone) エリア
  ビジネスエリアからのデータトラフィックを管理して，Level 3 以下の制御システムエリアを守るためのエリアである。
- Level 3 – 生産管理エリア
  例えばビジネスエリアの ERP (Enterprise Resource Planning) システムと連携するといった，製品の生産管理のエリアである。
- Level 2 - システム監視エリア
  製品の製造プロセスを監視したり制御したりするエリアである。
- Level 1 - プラント制御エリア
  フィールド機器からデータを読み込んで，制御アルゴリズムに従って製品の製造プロセスを操作するエリアである。

*1 YEI System Integration Technology Centre

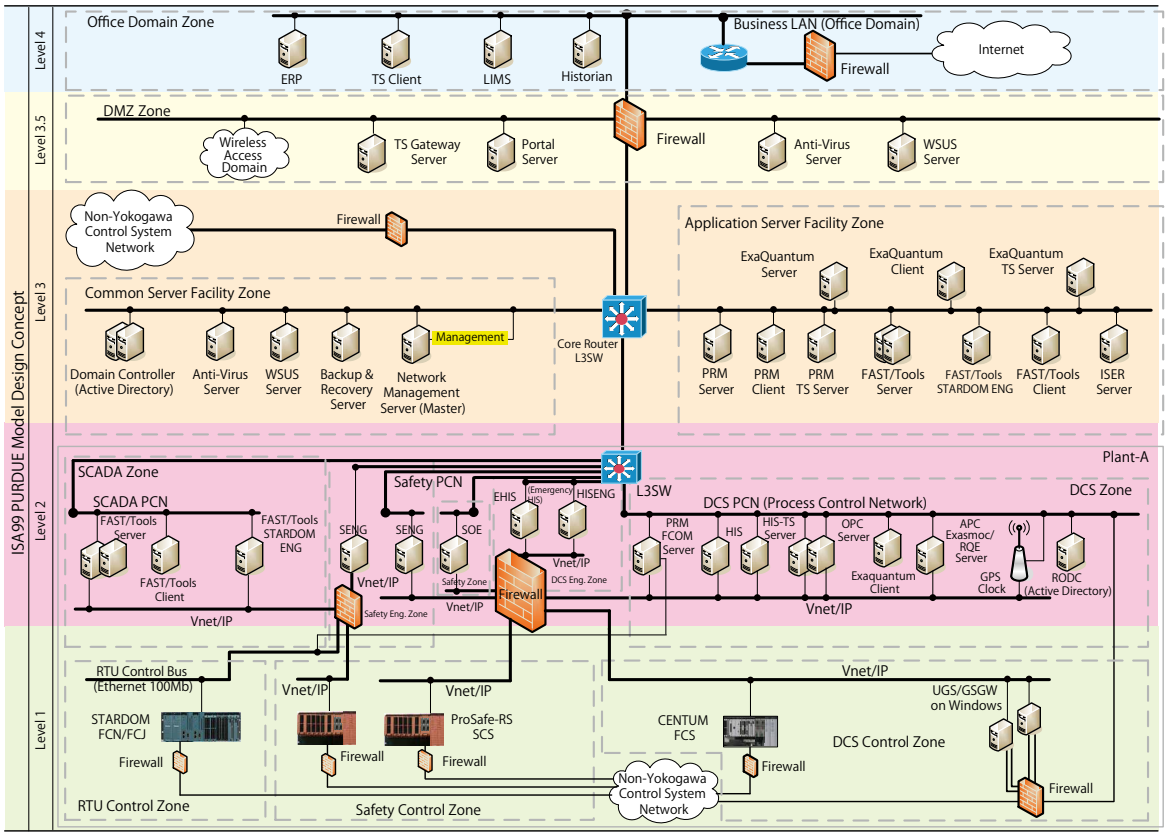

図 1 ネットワークアーキテクチャ

3. セキュリティ対策

3.1 アンチウイルスソフトウェア管理

アンチウイルスソフトウェアによるシステム防御は，多層防御の最終ラインであるエンドポイントセキュリティの位置付けにあたる。アンチウイルスソフトウェアは，日々増加するマルウェアに対応して，定義（パターン）ファイル，エンジンファイルなどの情報が随時更新される。これらの情報は，定期的に横河電機社内で検証を行っており，適時更新していくことが望ましい。

横河電機が提供する EPS (End Point Security) サービス[注 1)]では，サービスエンジニアにより，個々のクライアントに対して手動で情報を更新する手法を提供している。これに加える形として，本稿では，アンチウイルスソフトウェア管理サーバ（以降 AV (Anti-Virus) サーバ）による統合管理の方法を紹介する。

AV サーバによる統合管理は，情報更新に関する工数を削減する。AV サーバがない場合，作業者は個々の PC に対して手動で情報の更新作業を行う。対象機器の台数が少なく，かつ，設置場所が近接していれば，手動更新は有効である。しかし，対象機器の台数が多い，もしくは，設置場所が点在しているとなれば，AV サーバの導入を検討すべきである。最終的に，AV サーバを導入するか，EPS サービスによる手動更新を選ぶかは，対象機器の台数，配置，AV サーバの管理コスト等を考慮し，ユーザと協議の上，決定される。

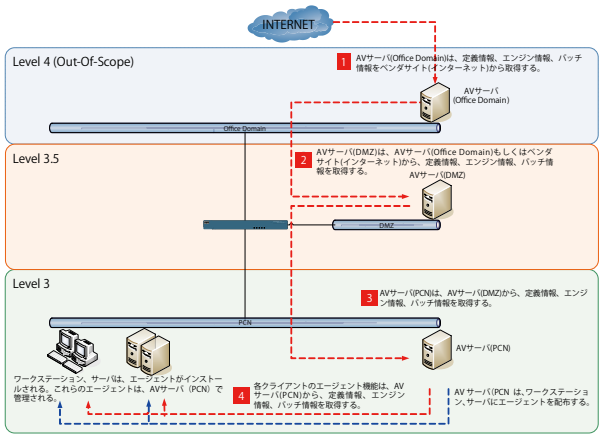

図 2 AV サーバシステム構成の代表例

図 2 に AV サーバシステムの代表例を示す。システム内に AV サーバを多段構成で設置している。これは，Level 3 の AV サーバを直接インターネットに接続させないことにより，制御システムエリアである Level 3 の AV サーバの安全性を高めるためである。

注 1) EPS サービスの詳細については，本技報内の別稿「制御システムのエンドポイントセキュリティ対策」を参照

Level 4 の AV サーバで取得した情報は，Level 3.5 の AV サーバで取得され，さらに Level 3 の AV サーバで取得される。Level 3 の AV サーバから，各ワークステーション，サーバへ情報が配布される。

3.2 マイクロソフトセキュリティ更新プログラム適用管理

マイクロソフト社が毎月（もしくは臨時）に提供するセキュリティ更新プログラム（MS パッチ）は，セキュリティホールを塞ぐ為の更新プログラムである。これらを適切に適用することは，アンチウイルスソフトウェアと同様，多層防御の最終ライン，エンドポイントセキュリティの位置付けにあたる。

EPS サービスでは，サービスエンジニアにより，個々のクライアントに対して手動で MS パッチを更新する手法を提供している。これに加える形として，本稿では，WSUS (Windows Server Update Service) サーバによる統合管理の方法を紹介する。WSUS サーバは，マイクロソフトの Web サイト，もしくは，上位の WSUS サーバより MS パッチを取得し，対象機器に提供する機能を持つ。

WSUS サーバによる統合管理は，MS パッチ適用作業工数を削減する。AV サーバと同様，WSUS サーバの導入効果は，対象機器の台数及び配置場所に依存して決まる。最終的に，WSUS サーバを導入するか，EPS サービスによる手動更新を選ぶかは，対象機器の台数，配置，WSUS サーバの管理コストを等考慮し，ユーザとの協議の上，決定される。

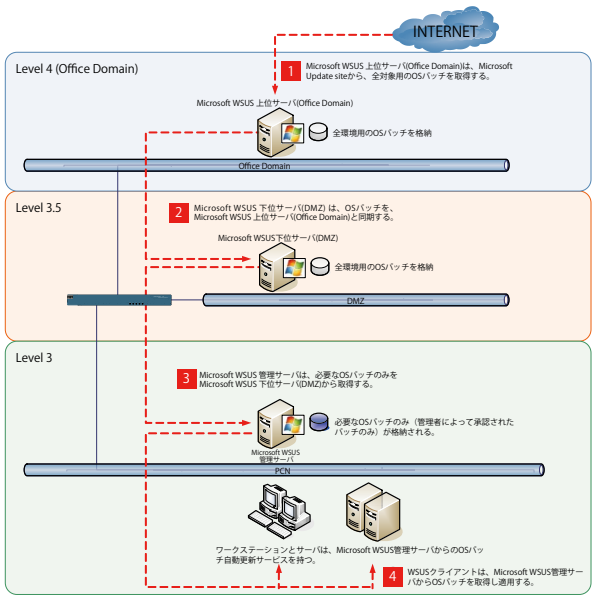

図 3 MS パッチ適用管理環境の代表例

図 3 に MS パッチ適用管理システムの代表例を示す。システム内で WSUS サーバを多段構成で設置している。これは，前節の AV サーバと同様に，Level 3 の WSUS サーバを直接インターネットに接続させないようにしている。Level 3 の WSUS サーバは，更新対象の横河製品に必要な MS パッチのみを上位の WSUS サーバから取得する。

ここで必要な MS パッチとは，定期的に横河電機社内の検証環境で検証済みの MS パッチのことである。

3.3 Windows ドメイン管理とアカウントの管理

近年，制御システムの大規模化，複雑化により，プラント内で使われているワークステーション等のエンドポイントの数が増加し，従来のように個別エンドポイント上でパスワード，セキュリティポリシーなどを設定・管理することが難しくなっている。そのため AD (Microsoft Active Directory) によるリソース管理とセキュリティの中央一括設定を検討するケースが増えている。

AD によって，プラント内のリソースとユーザアカウントをディレクトリ内に論理的な構造として定義することで，実際の物理的な構造とは切り離して定義・管理することが可能となる。また，ユーザの役割を元にした（Role-Based）アクセス権の設定など，高度なセキュリティ要件を満たす設定管理が可能となる。

実際に制御システムに AD を導入するエンジニアリングにおいては，下記のような項目を適切に設定する必要がある。

a) Active Directory Forest/Domain モデル
b) Domain Controller の設置場所
c) DNS (Domain Name Service) の構成
d) Forest/Domain Function Level
e) FSMO (Flexible Single Master Operation) , GC (Global Catalog)
f) サイト構成
g) 時刻同期

横河電機では，制御システムの規模，要件に合わせて適切なエンジニアリングを行っている。

3.4 システムハードニング

ネットワークからの攻撃，端末の不正操作，盗難等に対する保護対策として，システムハードニングの設定が推奨される。横河電機は，下記の設定を一括設定できる IT セキュリティツールを提供している。

- ソフトウェア実行制限
- 「Auto Run」の無効化
- NetBIOS over TCP/IP の無効化
- Audit ポリシーの設定
- リムーバルメディアの無効化

横河電機のエンジニアは，上記の IT セキュリティツール実行に加えて，以下のようなシステムハードニングの設定を行っている。

a) Administrator アカウントの変更

Windows のインストール時に作成されるビルトインア

カウントは，パスワードクラックなどの対象となりやすいため，Administrator ユーザの名前変更，または無効化することが推奨される。

b) 不要なサービスの停止

Windows OS では多くのサービスがデフォルトで有効となっている。これらのサービスの脆弱性を狙って攻撃されることにより，最悪の場合，攻撃者にドメイン管理者権限が奪われる可能性もある。このようなリスクを低減するために，横河電機では使用していないサービスを停止することを推奨している。しかし，サービスの停止はインストールされているアプリケーションに従って注意深く実行することが必要となる。

3.5 バックアップ＆リカバリ管理

システム障害が発生して事業が停止すると，その間の損失だけにとどまらず，市場からの信頼も失うこととなり，最悪の場合，事業そのものの存続に関わるリスクとなる可能性がある。従って，障害発生後の速やかな復旧のために，データ保護とシステム保護の両面を考慮して，バックアップ＆リカバリシステムを設計する必要がある。

横河電機は，最適なバックアップメディア，ソフトウェアの選択から，業務や運用を考慮したバックアップ計画やリカバリ手法まで，総合的なソリューションを提供している。

今日のバックアップ＆リカバリテクノロジの優位性は，システムリカバリにかかる時間の大幅な短縮化である。数時間，数日という期間は必要ない。さらに，各ソフトウェアのライセンスの考慮は必要ではあるが，異なる構成の環境へのリカバリも可能となっており，より柔軟なシステムリカバリを提供している。

3.6 安全計装システム (SIS) の制御ネットワーク保護強化

プラントの安全確保において，安全計装システム (SIS: Safety Instrumented System) の果たす役割は大きく，そのシステムの可用性の確保は最優先とされるべきである。一方，制御システム全体の最適構成と，エンジニアリングとプラント運転の効率化のため，分散制御システム (DCS) と制御ネットワークを接続することが通常となっている。

このような制御ネットワーク構成において，万が一 DCS がウイルスに感染しても，SIS に影響を及ぼさないために，横河電機では，ネットワーク隔離装置（ファイアウォール等）を経由して DCS システムの制御ネットワークに接続するエンジニアリングを提供している。

4. セキュリティトレーニング

制御システムのセキュリティ対策においては，制御システム自体，および，プラントの可用性確保，安全確保の理解の上に，情報システムの技術を元にしたセキュリティソリューションを適用する必要がある。

このため，横河電機では，制御システムのエンジニアに対して，制御システムに適合する，ベストプラクティスに基づいたセキュリティシステムを理解し，実際にエンジニアリングを行うためのトレーニングを実施している。

トレーニングは，以下の 3 段階の構成として実施し，受講後の完了テストに合格したエンジニアを，横河電機セキュリティ認定エンジニアとして登録管理している。

- Total System Architecture
- Advanced Module for Each Security Solution
- Practical Module for Each Security Solution

2013 年に，重要インフラのセキュリティ対策担当者向け専門資格として，GICSP (Global Industrial Cyber Security Professional) 認定制度が新たに創設された。GICSP は，Cyber Security 関連の資格認定制度を数多く提供している外部機関である GIAC (Global Information Assurance Certification) の認定資格の 1 つである。この GICSP においては，セキュリティ対策システムの設計・導入にとどまらず，ポリシー策定，導入計画策定等の初期段階から，導入後の実運用時の事故発生時対応手順等に至るまでのライフサイクルを通した包括的な知識が求められている。

横河電機では，この GICSP の重要性を鑑み，資格取得のための内部トレーニングモジュールを開発し，各グローバル拠点でトレーニングを実施することにより，この資格取得を組織的に推進している。

5. おわりに

本稿では制御システムに対する横河電機のセキュリティの考え方やそのエンジニアリングについて紹介してきた。セキュリティ対策は，一般的な情報システムセキュリティから学び，制御システムへ適用するに相応しいソリューションを選別し，そのアーキテクチャおよび実装や運用をベストプラクティス化した。重要インフラを支えている制御システムをサイバー攻撃から守ることは必須である。横河電機ではベストプラクティスをもとにした適切なセキュリティエンジニアリングの提供によって，セキュリティリスク軽減を実現する。そして今後もプラントの安全安定操業に貢献していく。

参考文献

(1) ANSI/ISA-99.00.01-2007, Security for Industrial Automation and Control Systems Part 1: Terminology, Concepts, and Models, ISA, 2007, pp. 69-73