制御システムセキュリティ対策支援コンサルティング

Consulting Support Services for Control System Security

木下 弦 *1　　新井 保廣 *1
Gen Kinoshita　　Yasuhiro Niii

世界的なサイバー犯罪が急増する中，制御システムにおけるインシデント件数も日々増加の一途をたどっている。この背景には，これまで独自の技術を採用してきた制御システムが，汎用 IT 技術の採用へとシフトしたことにより，情報システムと同様のセキュリティリスクを抱え込んだことが大きな要因である。

制御システムにおけるセキュリティ対策では，横河電機が推奨する技術対策・管理対策・運用対策のベストミックスによる多層防御戦略を実践するうえで，まず前提となるのはセキュリティポリシーであると考えている。制御システムユーザが最適なアプローチによってセキュリティポリシーを策定することを，横河電機は制御システム導入の豊富な経験や国際規格への貢献による知見をもとに，コンサルティングで支援する。

本稿では，セキュリティポリシーの考え方と，セキュリティコンサルティングによる支援プロセスについて紹介する。

As the number of cyber crimes soars globally, the number of security incidents involving control systems is also increasing. This is because control systems are shifting from their original technologies to general-purpose commercial IT. This imposes the same security-risk on control systems as on information systems.

As a security countermeasure for control systems, Yokogawa recommends the “defense in depth” strategy, which is achieved by a best mix of measures in technology, management, and operation. Appropriate security policies are key to the implementation of this strategy. By offering consultation based on knowledge obtained through a wealth of experience in supplying control systems and developing international standards, Yokogawa helps control system users establish security policies with the best approach.

This paper introduces both how to draw up security policies and Yokogawa’s security consulting services.

1. はじめに

制御システムへのセキュリティ脅威が増す今日，ユーザにおいてもセキュリティに対するリスク意識が強まっている。しかし，セキュリティ対策をユーザ自身でまとめることは難しく，当社においてもユーザのシステムにおいて，工場レベルでのセキュリティ対策強化の検討依頼を受けている。

こういった依頼を受ける背景には，横河電機がセキュリティを専門とするラボを設け，最新の脅威や脆弱性の検証を実施し，先進的な制御システムのセキュリティ機能を開発していること，制御システムセキュリティの国際規格（IEC/ISA）の標準化に長年貢献した実績をもつこと，また海外の先進ユーザに鍛えられたベストプラクティスの蓄積とユーザ要件に応えられる素地を築いてきたことが挙げられる。これらの実績をもとに，当社は安心・安全操業をサポートする制御システムセキュリティ対策支援コンサルティングをコンサルティングメニューの一角に備えた。

我々は既知の脅威に対する万全な防御策だけでなく，インシデントが万が一発生した場合に，早期に察知・対応し，復旧する為の事後対策を準備しておくことが重要であると考える。

そのためには，まずセキュリティポリシーとしての「考え方」を確立し，そのセキュリティポリシーをベースとした対策を導入することが必要である。

*1 横河ソリューションサービス株式会社
ソリューションビジネス本部コンサルティング 2 部

2. 制御システムセキュリティの課題

従来，制御システムは独自の OS やプロトコルを使用し，専用のクローズド型ネットワークを採用していた。しかし近年では，操業の効率化，迅速な経営判断，コスト効率化などの市場の要求に応えるため，制御システムは Windows や UNIX/Linux といった汎用の OS に，TCP/IP をベースとするオープン型ネットワークを採用している。

その結果，いわゆる情報システムがもつセキュリティリスクを，制御システムも抱え込む時代へとシフトした。かつてはクローズドなネットワークで構成されているため安全であると言われていた制御システムの安全神話は，今や崩壊したことになる。

しかし，汎用技術を採用はしたものの，ISMS (Information Security Management System) を始めとした“情報システムの対策アプローチを制御システムにも適用する”という解は成立しない。なぜなら，情報システムとは異なり，制御システムは 24 時間 365 日の稼働を前提とするシステムであり，可用性を重視するため，情報システムのような隔離・遮断・停止といったセキュリティインシデント対応にはなじまないためである。

また，制御システムの場合，システム停止が伴うセキュリティ対策（OS セキュリティパッチの適用など）は安易に許容できず，システム更新周期の観点でも，情報システムは 3 ～ 5 年であるのに対し，制御システムは 10 ～ 20 年となり，長期間にわたりシステムを維持する必要がある [(1)]。場合によっては，メーカーサポート終了後の OS による運用を余儀なくされ，その結果，脆弱性を包含したままシステムを運用し続けなければならないケースもあり得る。

そういった可用性優先の運用を前提に，制御システムでは情報システムとは異なる対策アプローチを考えなければならない。

制御システム固有のセキュリティポリシーと，ポリシーに沿った具体的な対策の導入を検討するうえで，セキュリティを担当する人材確保や対策組織の確立も課題となる。これらを実践するためには，ある程度の経営資源の投入と，効率的に組織を動かすための経営層の支援が必要である。

また，自社におけるセキュリティリスクの洗い出しも課題であり，洗い出したリスクへの対応策も準備しておく必要があることは言うまでもない。

これらの課題に対し，当社はユーザの視点に立ち，最適なアプローチや対策を検討することを，セキュリティ対策支援コンサルティングとして行っている。

3. セキュリティ対策支援コンサルティング

前項の課題に対応するためには，まずセキュリティポリシーの確立が重要であり，セキュリティポリシーとして，全社レベルのセキュリティ対策方針（基本方針）や組織固有のセキュリティ対策方針（一般方針）の確立を前提に，各方針に沿った管理項目標準や運用手順書 (SOP:Standard Operating Procedure)，及びシステム設計書を用意しておく必要がある。本項では，セキュリティを考える上で一番重要となるセキュリティポリシーの策定を中心に，コンサルティングによる支援策を説明する。

3.1 前提となるセキュリティポリシー

コンサルティングで策定支援するセキュリティポリシーの概念は，**図 1** に示すように 4 つの階層で構成される。

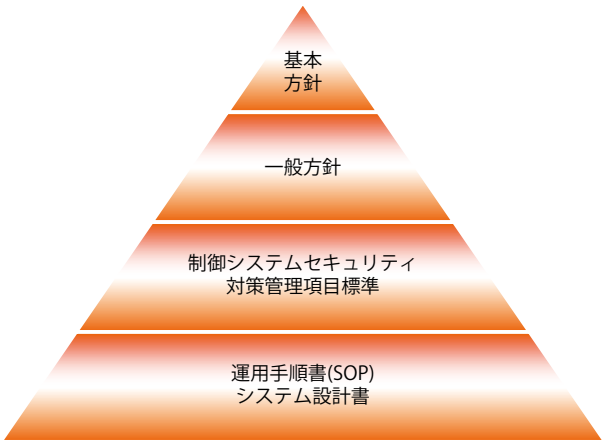

図 1 セキュリティポリシー

1) 基本方針

最上位の基本方針は，企業の経営理念や経営計画の一つとして，サイバーセキュリティを確保するための考えをまとめたものである。組織全体で統一した考えに沿って活動することを目的とし，経営陣の合意のもと，企業のセキュリティに対する大きな全体方針を定める。

2) 一般方針

一般方針は，基本方針に沿ったシステムや装置，ラインごとの個別方針と位置付けられる。導入するシステムや環境ごとに，独自の個別方針が必要となる。

3) 管理項目標準

基本方針に基づく一般方針ごとの考え方や取組み内容を定めたものが，制御システムセキュリティ対策の管理項目標準である。

管理項目標準では，セキュリティの具体的な対策内容と，システムやネットワークのセキュリティに関する設計基準について定めておく必要がある。この基準はユーザ自らが設定する目標値（セキュリティレベル）に対して，セキュリティレベルを維持する施策として定めなければならない。

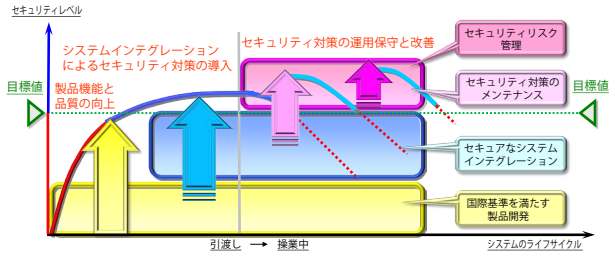

図 2 システムライフサイクルとセキュリティレベル

図 2 はユーザが設定した上で，対策を講じることによって維持することを目指すセキュリティレベルと，システムライフサイクルとの関係を表したイメージ図である。

この図に示すように，セキュリティレベルは一度対策を講じれば継続維持できるものではない。システム導入や更新の際にセキュリティレベルを担保していたとしても，環境の変化により経時劣化を招くため，継続的な改善（セキュリティリスク管理やセキュリティ対策のメンテナンス）が必要となる [1]。策定したセキュリティレベルを維持向上する為の管理方針を始め，各項目を実践する為の管理体制や役割を策定しておく必要がある。

4) 運用手順書・システム設計書

最後に，セキュリティレベルに沿った対策機能の実践，導入に向けた運用の実践，及びシステム導入におけるセキュリティ設計を実施するため，管理項目標準を運用手順書やシステム設計書に落とし込むことが重要である。

当社では 1) から 4) で策定したものを「セキュリティポリシー」と呼ぶ。

3.2 コンサルティングの活動

セキュリティ対策支援コンサルティングは，ユーザの対策状況に応じて支援範囲を選択できるよう，**図 3** に示す 5 つのステップでメニュー化している。

図 3 コンサルティングメニュー

1) Step1 セキュリティ安全性調査

Step1 では，セキュリティインシデントの “ 予防策 ”，セキュリティインシデントによる影響を最小限に抑える “ 緩和策 ”，また重度の影響によりシステム停止レベルに至った際の “ 復旧策 ” の 3 つのフェーズで，現状の対策を独自のヒアリングシートを使用して，フィジビリティスタディ形式で把握する。物理セキュリティを含めて，組織・要員のセキュティ，技術・管理・運用対策などの対策状況について，ユーザ自身の現状把握を支援する。

2) Step2 セキュリティ対策概説トレーニング

Step2 では，横河電機のベストプラクティスや，制御システムセキュリティ対策の基本的な考えを取りまとめたセキュリティ対策要領書をユーザに提供し，制御システムにおけるセキュリティ対策の概念をユーザ自ら学習してもらうステップとなる。必要に応じて講習会なども開催する。

以上のステップでは，現状の対策における課題と，制御システムセキュリティ対策の考え方を把握することが目的である。

3) Step3　セキュリティ対策支援コンサルティング

Step3 では，ユーザ自身のセキュリティポリシー策定を支援する。**図 1** の “ 基本方針 ”，“ 一般方針 ” と “ 管理項目標準 ” における考え方の策定までを支援する。

コンサルティングでは，ユーザが検討する方針や対策案に対して，有効性や一貫性，網羅性などの客観的視点から助言を行う。

このステップの最初のアプローチは，リスクアセスメントとなる。顕在化する脅威の想定や，事業上の負の要因となる側面（事業機会損失やブランド信用低下，社会問題など），資産価値などからリスクの洗い出しを行う。次に，それらの対象範囲において，物理的リスク，要員のリスク，ネットワーク上のリスク，個々のシステムリスクや事業継続上のリスクなど，Step1 と同様に予防・緩和・復旧の側面からアセスメントを実施する。

アセスメントの結果，識別したリスクに対し優先付けを行い，対応するための管理方針，対策の管理項目標準をユーザ主体で検討してまとめる。その際の検討過程と内容に関して当社の提言を添えて，関係者全員の討議後に最終方針を決定してもらう。ユーザはこの決定方針をもとに，自社の正式なセキュリティポリシーの文書化を進めることになる。

当社のコンサルティングの成果物として，リスクアセスメントの結果を基に，管理方針，管理項目標準について検討･協議した内容と決定した方針の内容をまとめ，“ 活動報告書 ” として提出する。

4) Step4　セキュリティ対策機能導入コンサルティング

Step4 では，策定したセキュリティポリシーに基づくセキュリティ対策機能を導入する。当社が納めるシステムに関わるセキュリティ機能設定内容の策定や，ネットワーク及びサーバ・クライアント PC といったエンドポイントのセキュリティ強化機能を導入するための，セキュリティ要求仕様の策定を支援する。

5) Step5　セキュリティマネジメントサービス

Step5 では，ユーザの内部監査を支援するコンサルティングを提供する。

ユーザは，策定したセキュリティポリシーの関連文書や手順書を基に，組織・要員への教育と責任の割当てを行ったうえで，初めてセキュリティマネジメントシステムとしての運用を開始する。運用段階においては，策定されたセキュリティレベルを遵守しているか，また外部環境の変化に対応し得るレベルかを適正に監視する必要があり，そのために内部監査を実施する。

内部監査を行うにあたり，日々発生するインシデントの状況や，公開されている脆弱性情報，業界プラクティスなどを分析して，効果的なリスクアセスメントの実施やセキュリティポリシー・手順の改善につなげるためにコンサルティングを行って，ユーザの内部監査を支援している。

4. CSMS 構築支援コンサルティング

経済産業省は，2014 年 4 月に制御システムにおけるセキュリティマネジメントシステムの認証制度となる CSMS (Cyber Security Management System for Industrial Automation and Control System) をスタートさせた。CSMS は制御システムの開発・運用プロセスにおける組織マネジメントを，国際規格 IEC62443-2-1 の勧告を基準に評価する制度である。

端的に言えば，OA 情報系の ISMS と対をなす制御システム向けのマネジメントシステムと言えるだろう。当社は，この開発プロセスの規格基準に沿って，DCS のエンジニアリング業務において国内第一号で認証取得している。CSMS の認証取得としては世界初である。

認証取得に臨んだ背景のひとつは，“ 当社が納めるシステムが，高いレベルでセキュリティを維持している ” と社会からお墨付きが得られることである。

もうひとつの背景は，取得の実証を糧として CSMS をユーザに啓蒙し，継続的にセキュリティを維持できる環境，つまりセキュリティマネジメントシステムの導入を支援することである。ユーザは CSMS を構築することで，制御システムのセキュリティ対策の確立を目指すことができ，当社はコンサルティングによる CSMS の展開を今後加速する。

5. おわりに

横河電機は，多層防御戦略をもとに予防・緩和・復旧の 3 つのフェーズを念頭に置いた，継続的に運用や対策を改善する考え方，これを “ セキュリティライフサイクル ” と呼び，この考えに沿った製品・エンジニアリング・サービスを提供している。

ユーザにおいても，セキュリティライフサイクルに基づくサイバーセキュリティマネジメントシステムを確立し，システムを構築・提供する当社と共に連携を図り，切磋琢磨することによって，安心・安全なプラントを実現できると確信している。当社はその信念を持って，日々精進している。

参考文献

(1) ARC Advisory Group，“ARC 白書：プロセス制御システムに最適なセキュリティライフサイクル　横河電機の包括的なアプローチ ”，横河電機，2011，
https://www.yokogawa.co.jp/dcs/pdf/whitepaper/
/dcs-Cyber-Security_WhitePaper.pdf