2F-01

制御システムにおけるセキュリティフレームワーク

李　哲†　　原田　要之助‡
情報セキュリティ大学院大学†　情報セキュリティ大学院大学‡

あらまし

制御システムは，クローズドなネットワークの中で独自プロトコルやハードウェア，ソフトウェアで構築されてきたため，一定のセキュリティ品質を保ち続けられた．しかし，近年の顧客需要への対応や運用方法の変化により，外部ネットワークへの接続やシステムにオープン化技術が導入される等の変化があり，従来のセキュリティ対策では十分な対応ができないという問題が起きている．また，独自の技術発展を遂げてきた制御システムに，ISMS などの管理策を適用することが難しく，また，現場，エンドユーザからの支持も得られない．そこで本稿では，独自のシステム構成，運用，マネジメント体系を維持しながら， ISMS 対策を部分的に活用する新しいセキュリティフレームワークを提案する．

１．背景

本稿では，制御システムと情報システムにシステムを区分して表現する．制御システムとは主に，エネルギー分野（電力，ガス等）や石油・化学，鉄鋼等のプラント，鉄道等の交通インフラ，機械，食品等の生産・加工ライン，ビルの管理システムなど社会・産業基盤を支える産業用オートメーション及び制御システム(IACS：Industrial Automation and Control System)[1]を指す．

まず，情報システムと制御システムの特徴の違いについて以下の表１に示す．

表１．制御システムと情報システムの違い

	制御システム	情報システム
(1)守るべき資産	制御機器 サービス提供	情報，ソフトウェア
(2)システム停止要求条件	難しい	サービス提供時間外等
(3)システム更新間隔	10-20 年	3-5 年
(4)運用部門	現場，ベンダー	情報システム部門
(5)エンドポイント数	数百~数万点 (全ｾﾝｻ，端末)	数十～数百 (規模によるが同時接続ユーザ最大数)

A study on security framework for operation and control system
†Choru Ri・Institute of Information Security

表１によると，セキュリティ対策に５つの相違点がある．まず，守るべき資産内容が異なることで，制御システムでは可用性を重視する傾向にあり，セキュリティ対策の優先度が異なる[2]．次に，システム停止の要求条件から，即時のセキュリティパッチの適用ができない．また，繋がるエンドポイント数が多いことから全ての端末等に対策や管理を行うことは困難である．さらに，システム更新間隔が長いことで抜本的なセキュリティ対策を取りにくいという問題が起きる．本来は，システムの違いを踏まえてセキュリティポリシーや規定を社内で構築・更改する必要があるが，情報システムのポリシーをそのまま適用するままとなっている．

２．制御システム変化とセキュリティ課題

近年，制御システムにおいて外部ネットワークへの接続や機器のオープン化など以前にはなかったシステム上の変化が起きてきている．鉄道信号制御システムを一例として取り上げる．鉄道制御システムでは、制御技術、顧客へのサービスや運用方法の多角化が進み、従来（1990年頃まで）の鉄道制御システムとは構成が大きく変化している。他システムとの接続と連携、列車在線位置情報の提供サービス、遠隔地でのリモート保守など，様々な機能が追加され、その結果，クローズドなネットワークであった鉄道制御システムが外部ネットワークに接続された。また、コスト、運用面を考慮し、オープン化技術が積極的に導入され、汎用製品・OS が広く採用されるようになった。1990 年代と 2010 年代の鉄道制御システムの変化を図１に示す。

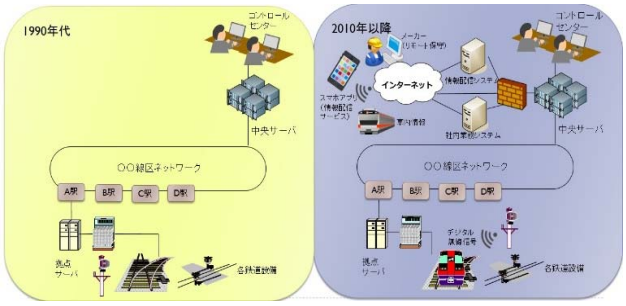

図１．鉄道信号制御システム変化

これらの運用の変化，オープン化機器の導入により，外部ネットワークからのサイバー攻撃，他システムや可搬型デバイス（USB メモリ

等）からのマルウェア感染など，様々な脅威に晒されるようになった．

近年では，イランのウラン濃縮用遠心分離機を破損させた Stuxnet [3] の感染事例や，ウクライナの送電システム障害を発生させ，数十万世帯を停電させた BlackEnergy [4]の感染事例など，制御用システム等に対するサイバー攻撃が発生している．制御システムにおいて，セキュリティインシデントが発生することは人命事故や社会インフラへの停止に直結する．そのため，制御システムについても危急なセキュリティ対策が求められる．

３．国際規格

制御システムにおいて，情報セキュリティを行う指標として，ISO/IEC27001:2013 が認証基準の国際認証規格の ISMS（Information Security Management System）適合性評価制度 [5]があり、制御システムでは国際規格 IEC62443 をベースとした CSMS(Cyber Security Management System)適合性評価制度 [1]がある。CSMS は ISO/IEC27001:2005 を基準として，HSE（衛生・安全・環境）について追記し，制御システムに対応した認証基準である．しかし，基本的なセキュリティ管理策は ISMS がベースであり，制御システムの違いを考慮した管理策に修正されていない．そのため制御システムの実運用には適切とは言えず，CSMS 認証取得組織も 6 社(2018 年 12 月時点)と少なく社会的に認知されているとは言えない． ISMS の管理策は制御システムに共通するものも多いので，どのように修正して制御システムに適用させていくかがポイントとなる．

４．提案手法

制御システムの特徴，変化，また国際規格背景などを踏まえて適切なセキュリティ対策を行う新しいセキュリティフレームワークを以下に述べる．このフレームワークでは，制御システムを情報システムと明確に区別するために，制御システムにおける OT(Operational Technology)の違いを明確化する．制御システムの課題からも見えるとおり，ISMS の管理策には情報システム機器と同等であり準拠できるものと可用性や運用性など OT の特性のために準拠困難なものが存在する．しかし，OT の運用があるために ISMS への準拠が困難となり，ISMS をベースに策定されたセキュリティポリシーが形骸化する．または，運用部門の独自判断で不明瞭な基準で例外を広げるために，適切な情報セキュリティ対策までも実施されない可能性がある．これより組織統制が不明瞭になり，組織における情報セキュリティの脆弱性となる．そこで，組織で予め例外対象となる管理策を定め，ルールを定める組織の機能部門による統制，またどの管理策を例外措置対象とするかを明確にすることが考えられる．具体的な方法としては，まず，制御システムの ISMS 準拠をベースとして情報セキュリティの基本方針，対策基準を作成する．次に，制御システムの運用課題上，準拠が難しい管理策については，理由・代替管理策を明確にし，例外とする項目を明確にする．制御システムの運用部門では，当該の基準の実施手順を作成し，組織の機能部門による，例外対象項目の承認を得る．組織における運用例を，鉄道会社組織をモデルにした例を図２に示す．本社信号部，本社電力部，経営層が組織機能部門を指し，配下が運用部門（現場部門）を指す．

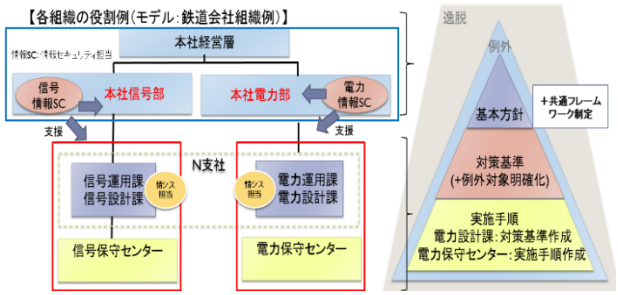

図２．情報セキュリティ決定のために各組織役割例（鉄道会社組織例）

４．まとめ

本稿では，制御システムの情報セキュリティ対策を行う上での運用上の課題を明確にし，その課題を解決し，明確な組織の情報セキュリティマネジメントを行うための新しいフレームワークを提案した．実際に運用を行うためには，セキュリティパッチを行う際の更新頻度などの明確な基準とその理由を定めて運用し，評価する必要がある．今後，本フレームワーク適用に向け，詳細について検討を進める．

参照文献

[1] 情報マネジメントシステム認定センター，“CSMS 適合性評価制度”．

[2] 情報処理推進機構セキュリティセンター，“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，” 2009.

[3] S. Mooney，“‘危機回避’ サイバー攻撃による核施設活動阻止，” cybereason，2018.

[4] Robert Lipovsky, Anton Cherepano, “BlackEnergy trojan strikes again: Attacks Ukrainian electric power industry,” eset, 2016.

[5] 情報マネジメントシステム認定センター，“ISMS 適合性評価制度”．

[6] 村﨑康博，原田要之助，“情報セキュリティポリシーにおける例外措置，” 情報処理学会論文誌 Vol.58 No12 1856-1862，2017.