〈研究発表〉

クローズ空間における制御システムセキュリティに関する一考察

中川拓巳[1)]，梅木聖己[1)]，潰田純也[1)]
高村忠克[1)]，松田佳久[1)]

[1)] メタウォーター㈱　システムソリューション事業本部　プロダクトセンター　システム開発部
（〒191-0065　東京都日野市旭が丘3丁目1-30　E-mail:nakagawa-takumi@metawater.co.jp）

概　要

汎用OSやオープンなネットワークの採用，遠隔監視・操作を実現するための外部接続等，制御システムを取り巻く環境は変化しており，情報システム同様，サイバー攻撃を受ける可能性が高まっている。上下水道施設も同様に環境が変化しているが，施設内の制御システムの多くは，外部接続されていないクローズされたシステムである。本稿では，外部接続されていない制御システムの社内設備に対して，IEC 62443-2-1を参考にセキュリティ対策を行った経験を基に，クローズされた空間における制御システムのセキュリティ対策に関する考察を行う。

キーワード：制御システムセキュリティ，IEC 62443-2-1，脆弱性，サイバーインシデント，セキュリティ対策
原稿受付 2024.7.1　　**EICA**: 29(2・3) 170-173

1. はじめに

従来，上下水道施設等の産業用制御システムは，外部ネットワークに接続されておらず，長期に渡ってサイバーインシデントが発生しない安全なシステムであると思われてきた。しかし近年，制御システムでは，WindowsやLinuxなどの汎用OSの採用，FL-netなどのオープンなネットワークの採用，また遠隔監視・操作を実現するための外部接続に加え，データ収集に利用されるUSBメモリを介したマルウェア感染など，ネットワークを活用した情報システムで発生しているサイバーインシデントと同様のことが発生する可能性が増大している[1)]。

Fig. 1は米サイバーセキュリティ・インフラセキュリティ庁（CISA: Cybersecurity & Infrastructure Security Agency）が公表した産業用制御システム（Industrial Control System）関連アドバイザリーの件数を示しており，脆弱性の件数は年々増加していること，また，2021年以降は，毎年371件の脆弱性が公表されており，急増していることがわかる[2)]。

上記の背景を踏まえ，筆者の所属する部門では制御システムに係るソフトウェアの開発，設計，実験を行うプロセス，および，環境のセキュリティレベルを向上させるためのセキュリティマネジメントを実施している。

本稿では，**Fig. 2**に示すような外部とはネットワーク接続されていないクローズされた環境（以降「セ

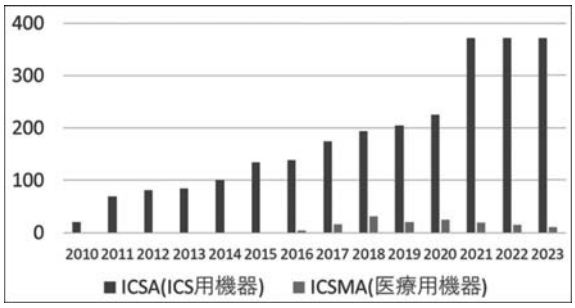

Fig. 1　Number of advisories by CISA[2)]

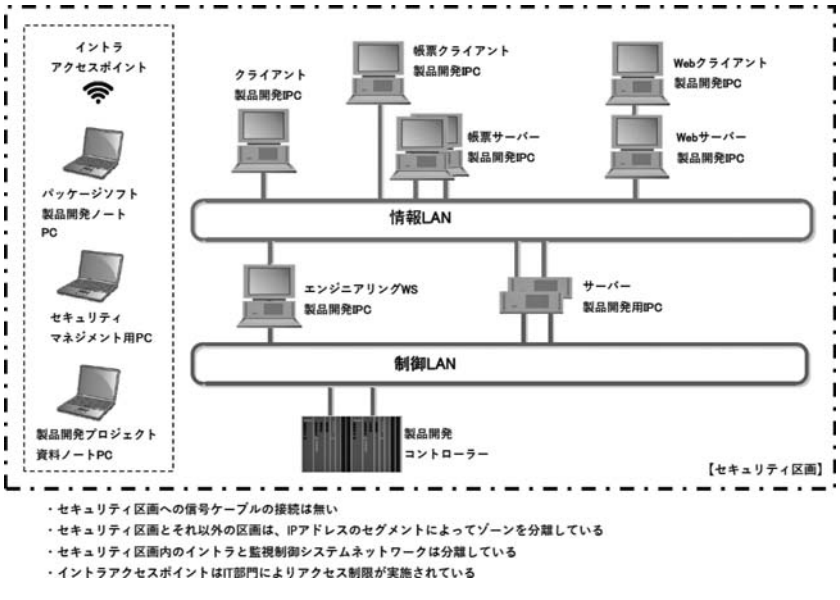

Fig. 2　Security division network overview

キュリティ区画」と記載）における制御システムへのセキュリティ対策の一部を事例として紹介するとともに，クローズされたシステムにおける制御システムセキュリティについて考察を行う。なお，当部門で実施しているセキュリティマネジメントシステムは，国際標準規格 IEC 62443-2-1 を参考に構築したものである。

2. 事　例　紹　介

セキュリティ区画における制御システムへのセキュリティマネジメントを紹介する。

2.1　セキュリティの 3 要素の優先度

制御システムと情報システムのセキュリティに対する考え方の違いについて説明する。一般的に情報セキュリティにおいて守るべき対象は「情報」そのもの，例えば，クレジットカードの番号のような「個人」「カネ」に直結する「情報」，制御セキュリティにおいては「モノ（設備，製品）」「サービス（連続稼働）」と言われている。そのため，**Table 1**[3] に示すよう，セキュリティの 3 要素である機密性（Confidentiality），完全性（Integrity），可用性（Availability）の優先順位は，情報システムでは機密性が最重要視された C，I，A の順であるが，制御システムでは一般的に可用性が最重要視された A，I，C の順である[3] と言われている。

一方，当部門で開発している製品は，制御システムに標準実装され，不特定多数の上下水道施設で利用されることを前提としたパッケージソフトであり，高い品質と信頼性が求められる。そのため完全性（情報やプログラムが正確で，改ざん・破損されていないこと）を最重要視し，優先度を I，C，A の順としたセキュリティマネジメントシステムを構築している。

セキュリティの 3 要素の優先順位には一般的な優先順位は存在するものの，守るべき対象により優先順位を検討する必要があると考える。

Table 1　Security concept differences[3]

	制御システム	情報システム
セキュリティ優先度	A.I.C（可用性重視）	C.I.A（機密性重視）
セキュリティの対象	モノ（設備，製品） サービス（連続稼動）	情報
システム更新	10–20 年	3–5 年
稼働時間	24 時間 365 日連続	通常業務時間内
運用管理	現場技術部門	情報システム部門

C（Confidentiality：機密性），I（Integrity：完全性），A（Availability：可用性）

2.2　セキュリティマネジメントシステムの構築

セキュリティマネジメントシステムの構築手順を **Fig. 3** に示す。

最初に現存するリスクを **Fig. 4**，**Table 2** に示す手順で認識し，対応計画を立案する。この対応計画を基に現状業務の見直しを行い，その結果を基準，手順として文書化・資料化する。これらの基準，手順を用いた仮運用・修正を施すことで，実用に耐え得るようブラッシュアップする。その後マネジメントレビュー，監査を経て，初版の基準・手順を制定する。

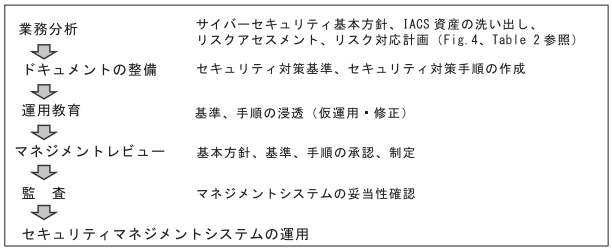

Fig. 3　Procedure for establishing a security management system

Fig. 4　Procedure for risk assessment and risk treatment[4]

Table 2　Risk assessment and risk treatment process [5]

プロセス		ISO/IEC 27000: 2018（JIS Q 27000: 2019）における規定
リスクアセスメント（risk assessment）		リスク特定，リスク分析およびリスク評価のプロセス全体
	リスク特定（risk identification）	リスクを発見，認識および記述するプロセス
	リスク分析（risk analysis）	リスクの特質を理解し，リスクレベルを決定するプロセス
	リスク評価（risk evaluation）	リスクおよび／またはその大きさが受容可能か，または許容可能かを決定するために，リスク分析の結果をリスク基準と比較するプロセス
リスク対応（risk treatment）		リスクを修正するプロセス（リスク回避，低減，移転，保有）

2.3　セキュリティ対策（リスクアセスメント，リスク対応）[5]

セキュリティ対策を検討する際には，運用中のシステムがどのようなリスクにさらされているかを想定し，そのリスクを低減するための対策を講じる必要がある。

Fig. 4 にセキュリティ対策手順を，**Table 2** にセキュリティ対策を行うにあたり必要なプロセスの概要を記す。

2.3.1　IACS※資産台帳の作成

守るべき制御システムに関する機器，ソフト，電子データなど IACS 資産を洗い出し，リスト化し，各 IACS 資産に対する脅威レベル，脆弱性レベル，お

よび資産価値を記入した「IACS 資産台帳」を作成した。

（※　Industrial automation and control system(s)：産業用オートメーション及び制御システム）

2.3.2　リスクアセスメント

国際標準規格 IEC 62443-2-1 を参考にしてセキュリティ要件を決め，その要件を満たしていることを確認した（ベースライン分析）。加えて，2.3.1 項に記載した「IACS 資産台帳」を基にブレインストーミングやリスクシナリオの作成を行い，各 IACS 資産に対して発生しうるリスクを抽出した（詳細リスク分析）。

2.3.3　リスク対応

リスクアセスメントで抽出したリスクへの対応例を以下(1)～(3) に示す。リスク対応を検討・実施するにあたり，「可用性を重要視する納入施設」に対してセキュリティ対策を施すことを想定し，外部とは接続されていないクローズされた環境「セキュリティ区画（**Fig. 2**）」を開発，設計，試験環境として構築することとした。

(1) ウイルススキャン

情報セキュリティにおけるアンチウイルス対策としては，ブラックリスト型アンチウイルスソフトをインターネット接続されたパソコンにインストールすることが一般的である。対して外部接続されていない制御システムでは，パターンファイルの更新ができないこと，また，ウイルススキャンの実行に伴い CPU の負荷が上がり，監視・操作のリアルタイム性（可用性）を阻害する恐れがあることから，一般的なブラックリスト型アンチウイルスソフトは適用することができない。その対策として，ソフトウェアをインストールすることなくマルウェアを検索・駆除することができる USB メモリ型のポータブルツールを利用して，定期的にスキャンを実行することとした。

(2) アカウント管理

一般的に情報システムにおいては，セキュリティ対策として，システム本体に **Fig. 5** 左側に示すよう，使用する個人を特定するためのアカウント管理機能（ID，パスワードを入力しないとアクセスできない仕組み）を取り入れている。しかし，現在多くの上下水道施設で稼働している「可用性を重視したシステム（異常発生時に誰でも直ちに監視・制御を行うことができるシステム）」に対し，セキュリティ対策としてアカウント管理機能を取り入れるための改造は難しい。そこで開発，設計，試験フェーズにおいてセキュリティ区画（**Fig. 2**）では，**Fig. 5** 右側に示すように制御システム本体にはアカウント管理機能を取り入れるための改造を施さず，セキュリティ区画（**Fig. 2**）に入退室する際に個人を特定すること，およびセキュリティ区画（**Fig. 2**）内の画像をビデオカメラで記録することで制御システムにアクセスする個人を特定することとした。

(3) 運用教育

セキュリティ対策の基盤となる「セキュリティマネジメントシステム」は，関係者全員の理解と日常業務への徹底が重要である。年間を通してセキュリティ教育を定期開催し，アンケートによる理解度調査を参考に，教育内容の改善に役立てている。

2.4　セキュリティマネジメントシステムの継続

Fig. 6 に示すよう，期初にセキュリティに係るイベントの年間計画を立案し，それに則って計画的に実施している。各々の計画に基づいてこれを継続的に改善していくことで，マネジメントシステムの有効性を向上させるようにしている。

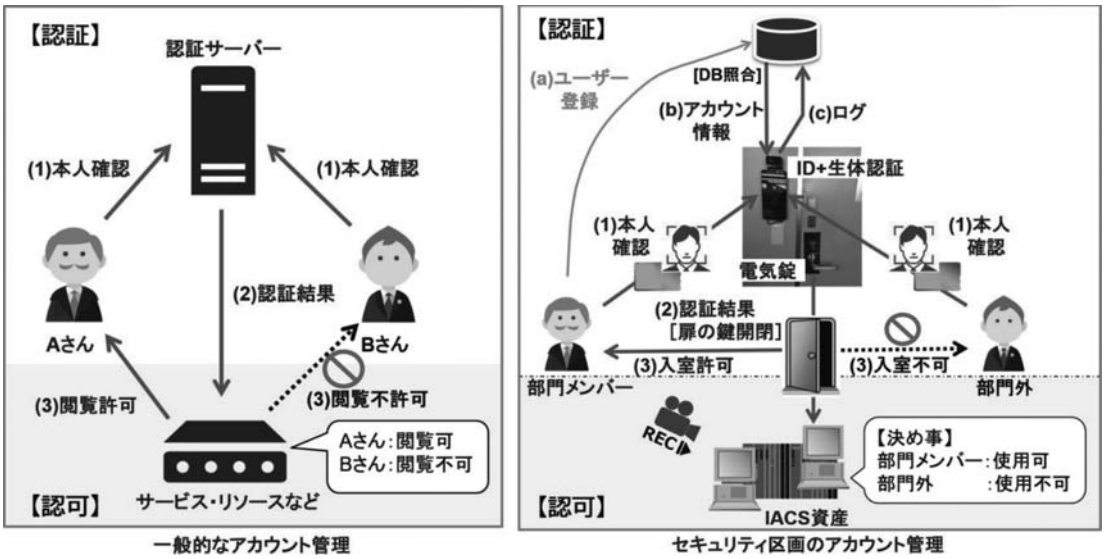

Fig. 5　Account administration（Authentication and Authorization）

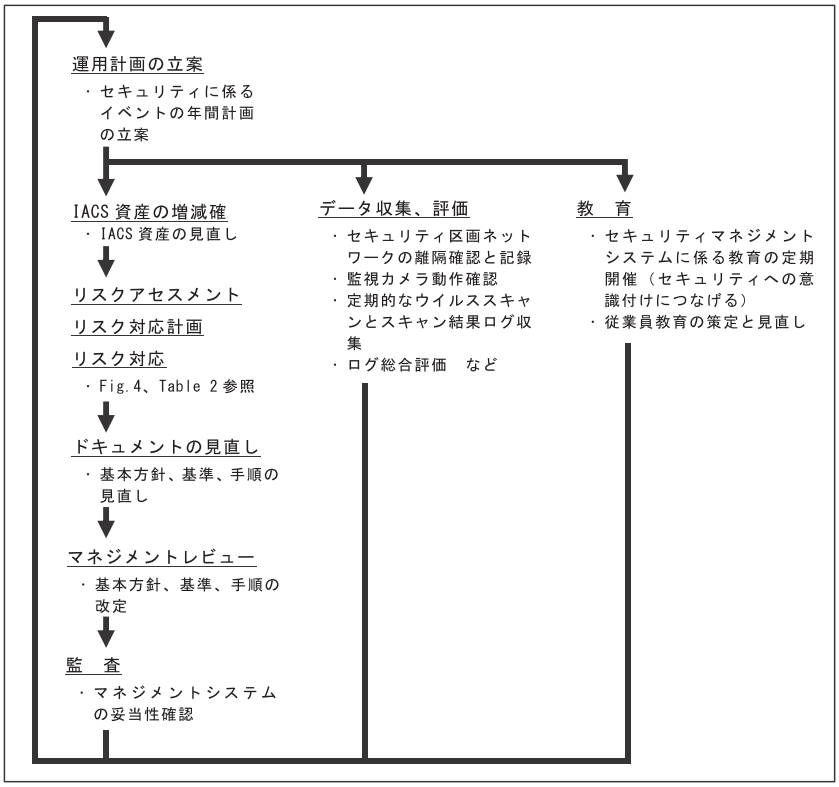

Fig. 6　Procedure for ongoing security management system operation

3. 考　　察

昨今，情報漏洩，ランサムウェアによる身代金の請求など，サイバーインシデントに関するニュースを耳にする機会が増えている。その影響か，新しいセキュリティ対策製品の発売，サイバーセキュリティに関する書籍やベストプラクティスなどの発行，情報セキュリティに係るコンサルティング業務の Web 広告などを目にする機会も増えている。

サイバーセキュリティに関する情報があふれ返り，何を参考に／何を頼りに，どのような対策を施すことが適切であるのか，また，多くの上下水道施設はクローズされたネットワーク環境が多く，果たして情報システムと同等のセキュリティ対策が必要であるのか，混沌とした状況に陥ってしまうことが懸念される。

これを解決するための方法として，現在運用中の制御システムや現存する運用ルールにどのようなセキュリティリスクが内在しているかを想定・特定すること（リスクアセスメントを実施すること），加えて，想定・特定したセキュリティリスクへの対応策を立案し，対策を実施すること（リスク対応を実施すること）が重要であると考える。

内在するセキュリティリスクは施設毎に異なり，リスク対応も施設毎に異なるものであり，一意に決まる／決められるものではないと考える。想定・特定されるリスクをベースに必要となる対策案を立案し，対策を講じることにより，その施設に合った最適な（無理，無駄のない）セキュリティ対策を行うことができるのではないかと考える。

4. お　わ　り　に

本稿では，当部門における制御システムセキュリティ対策事例を紹介し，クローズされたシステムにおける制御システムセキュリティについて考察を加えた。本稿に記載した事例や考察が，制御システムセキュリティに係るリスクマネジメントを行う際の参考になると幸甚である。

参 考 文 献

1）　公益財団法人　日本下水道市技術機構：下水道における情報セキュリティと制御セキュリティの考え方に関する自主研究，p. 8（2024）
2）　宮地利雄：制御システム・セキュリティの現在と展望　～この 1 年間を振り返って～，JPCERT コーディネーションセンター，p. 32（2024）
3）　独立行政法人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，p. 22（2009）
4）　梅木聖己：下水道における制御セキュリティに関する調査・研究について，上下水道情報，公共投資ジャーナル社，第 2010 号，pp. 24-26（2024）に加筆
5）　独立行政法人情報処理推進機構セキュリティセンター：制御システムのセキュリティリスク分析ガイド第 2 版　～セキュリティ対策におけるリスクアセスメントの実施と活用～，p. 23（2023）に加筆