下水道における制御セキュリティリスクマネジメントに関する共同研究

研究第一部　総括主任研究員
古屋　勇治

1 背景と目的

これまで上下水道システムの制御システムは，外部ネットワークに接続されていない，過去長期にわたってセキュリティ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ました。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などに伴い，情報システムで起きているセキュリティの脅威（サイバー攻撃）を受ける可能性が増大しています。

下水道においては，下水処理場等の監視・制御システムに対するベンダーロックインの解消（ベンダーフリー化）が推奨され，それに向けた対応として，汎用技術の適用等が挙げられており，セキュリティの脅威が増大することは必至です。今後，下水道における情報セキュリティと制御セキュリティを考えるに当たり，サイバー攻撃に対して，何を考え，何をすべきかを抽出し，それをもとに対応策を実施していく必要があります。

本研究では，令和５年度自主研究報告書をベースに，下水道業界，他業界のセキュリティに関する現状を調査し，セキュリティに関する情報や考え方を「情報セキュリティ」と「制御セキュリティ」の２つの側面から整理した上で，主として下水処理場におけるセキュリティ（制御セキュリティ）に関するリスクマネジメントの実施を促す技術資料を作成することを目的としています。

2 研究体制

2.1　研究体制

㈱NJS，㈱日水コン，東芝インフラシステムズ㈱，㈱日立製作所，三菱電機㈱，㈱明電舎，メタウォーター㈱，（公財）日本下水道新技術機構

2.2　研究期間

令和６年６月～令和８年３月

3 研究内容

3.1　セキュリティの現状把握

監視制御システムにおける情報セキュリティと制御セキュリティを考えるに当たり，サイバー攻撃に対して，何を考え，何をすべきかを抽出し，それをもとに対応策を実施して行く必要があります。

国内外の情報収集（上下水道業界，その他業界，規格の状況など），セキュリティ技術（プロダクト，研究など），セキュリティマネジメントシステム（IEC，ISA，JIS など）に関する調査内容を検討します。

3.2　情報セキュリティと制御セキュリティの違い

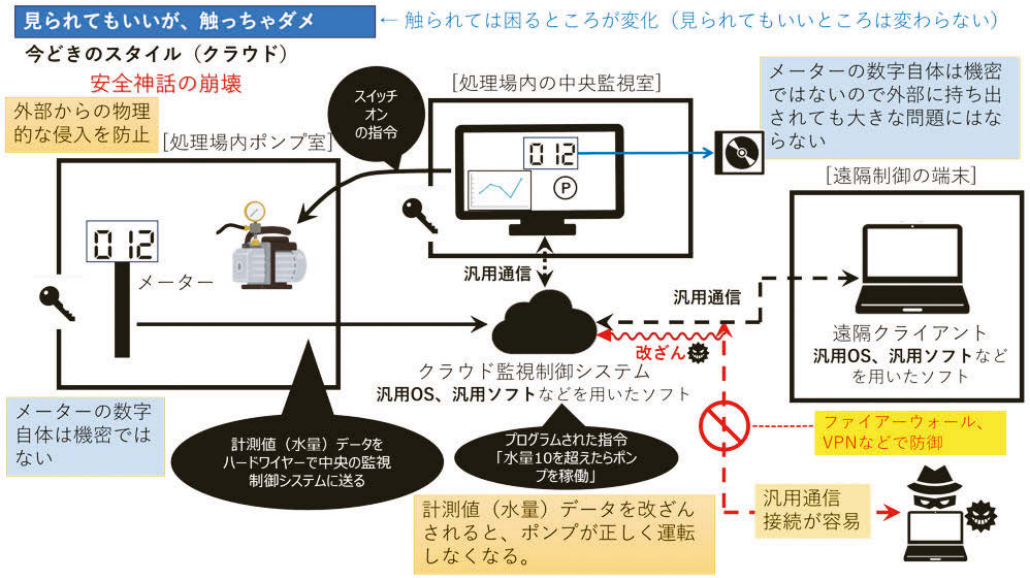
現状を把握して，「情報セキュリティ」と「制御セキュリティ」の２つの側面から整理した上でそれぞれの領域に対して守るべきものと防御の方法，防御が突破されたときのリスクを抽出し，主として下水処理場におけるセキュリティ（制御セキュリティ）に関するリスクマネジメントの実施を促す技術資料を作成します。

3.3　提言

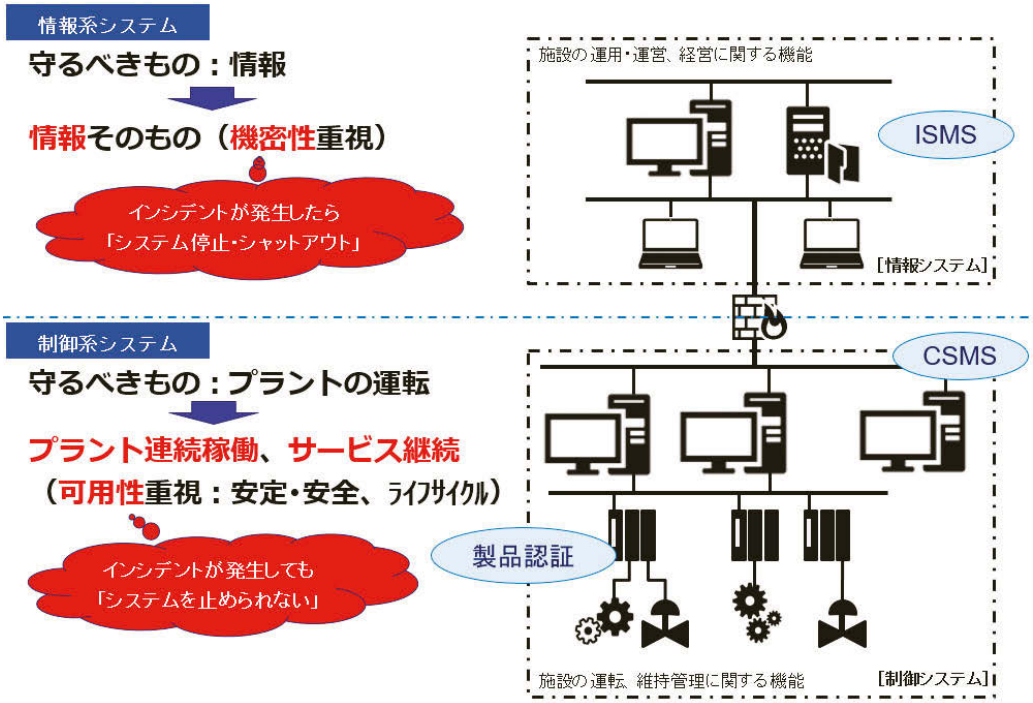
下水処理場等の制御セキュリティに関するリスクマネジメントの実施促進（セキュリティマネジメントシステムの適用）など。

・リスクアセスメントの方法
（リスクの特定，分析，評価）
・受容できないリスクへの対応方針の決定
（リスクの低減，回避，移転，保有）
・事業フェーズごとの具体的な対策例
（自ら実施すること，委託することのすみ分け，および委託する場合の注意点等）

監視・制御システムに関するセキュリティ対策の検討を行う際の予備知識を共有するための技術資料を作成します。



図－1　クラウドでの防御



図－2　情報系システムと制御系システムの守る対象の違い