上下水道分野の事例
広域監視制御システムにおけるセキュリティ技術

渡辺 忠雄 Watanabe Tadao
山口 浩介 Yamaguchi Kosuke
田所 秀之 Tadokoro Hideyuki
舘 隆広 Tachi Takahiro

重要な社会インフラである上下水道では，直面する事業経営課題を克服するべくさまざまな取り組みが検討されている。その一つに事業経営の広域化があり，事業体統合に関して国内各方面で検討され，成果報告[1]がなされている。広域化に伴い既存のシステムを「つなぐ」機会を考える場合，サイバーセキュリティへの対策が不可欠となる。セキュリティの脅威は多様化しており，広域化という事業環境の変化により，従来，閉鎖型だったシステムを再構築などによってつなぐ場合，セキュリティ施策を講じる必要がある。
日立は，上下水道分野におけるセキュリティ動向に注目し，日立監視制御システムAQUAMAX-AZシリーズのセキュリティ対応を進めている。

1. はじめに

国内の上下水道インフラは，高度経済成長期を経てその普及率は過去最高となり，水道普及率97.7%（2013年度）[2]，下水道普及率77.6%（2014年度，福島県を除く。）[3]に達している。今後の上下水道インフラの維持管理は上下水道事業における重要な課題であり，少子高齢化が進むとされる人口推計より水需要は減少していくことから，事業経営環境はますます厳しくなると予想されている。中小規模の事業体では職員の減少に直面し，技術継承の課題解決に苦慮する事業体が多いとされる。

そこで安全・安心な上下水道インフラを持続していくための有効な施策の一つとして，事業の広域化を促進する動きが活発になっている。水道分野では，2015年12月現在，22道府県で検討しているとされ，協議会が設置されるなど多様な統合案が示されている[4]。下水道分野では，2015年5月に公布された改正下水道法[5]において，下水道管理者どうしが広域連携について方向性を協議するための協議会制度創設規定を緩和し，広域化事業を促している。

一方，監視制御システムでは，従来のシステムを「つなぐ」こと，または，新たな統合システムを構築することで，プラント運転の広域化を実現していく。プラント運転の個別最適にとどまっていた従来型から，全体最適運転をめざすことが可能となってきた。安定運用，動力費削減を事業体間の水融通，電力融通を活用し，リアルタイム制御技術によって全体最適を実現しようとするものである。従来の監視制御システムをつなぐことは，全体を見渡した最適制御だけではなく，中央監視室の相互バックアップによる信頼性向上や，システム統合による少人数での運転管理の実現を期待することができる。

本稿では，こうした背景を踏まえ，上下水道事業体におけるサイバーセキュリティに関する動向を考察し，日立監視制御システムAQUAMAX-AZ/SPが備えるセキュリティ技術を紹介する。

2. セキュリティの動向

2.1 上下水道分野を取り巻くセキュリティの現状

「つなぐ」ことに伴って課題となるのが，セキュリティである。事業体をまたがってつなぐ場合は，事業体間のセキュリティポリシーに相違があることを前提にそのリスクを検討する必要がある。複数の監視制御システムがネットワークを介してつながる場合は，接続点を介したマルウェアの感染，拡散などのリスク対策が不可欠である（図1参照）。また，セキュリティの脅威，またその攻撃手法が多様化してきていることで，セキュリティ対策が複雑化しているとも言える（図2参照）。したがって，セキュリティ対策を検討するときには，リスクとして発生頻度とプラン

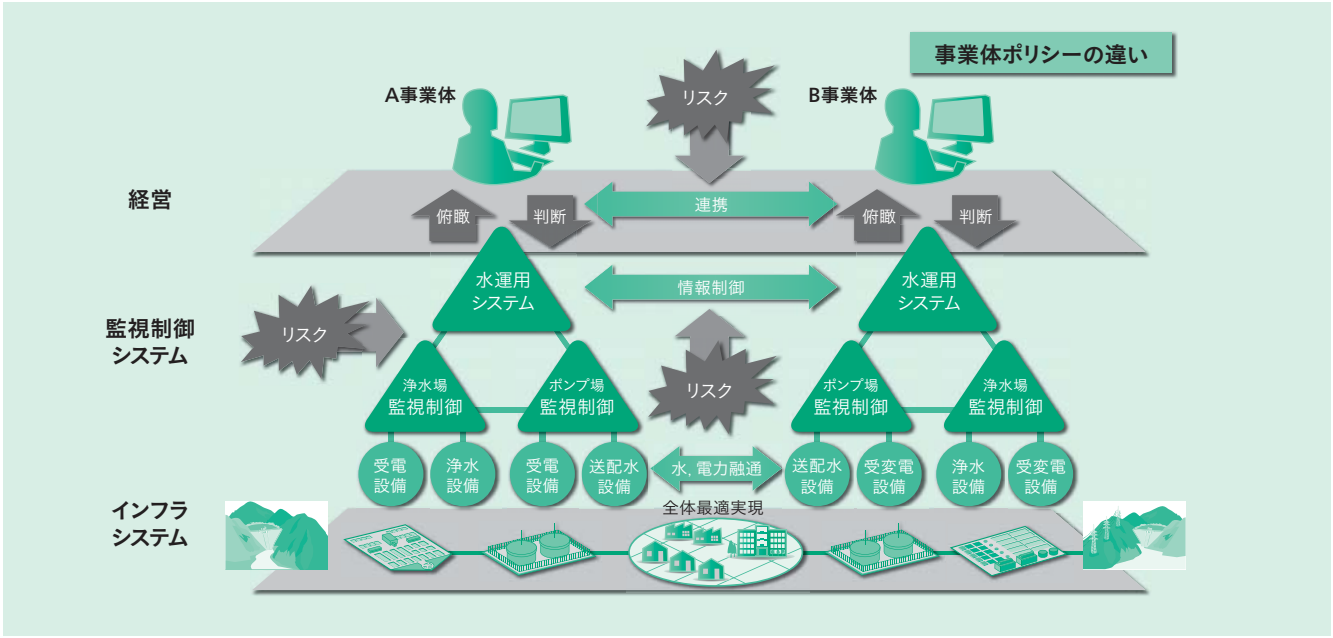
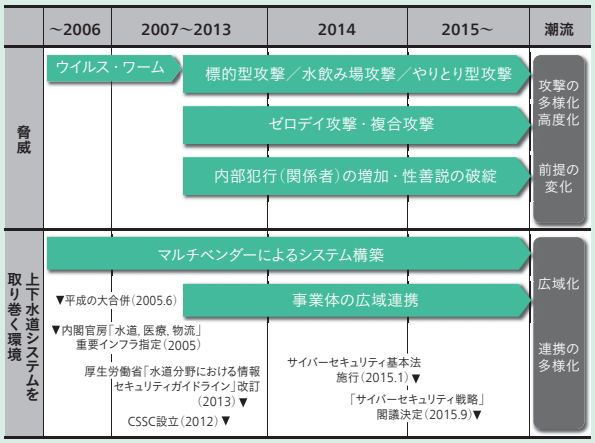


図1｜システム連携に伴うセキュリティリスク

地域の全体最適を実現する際にシステムを「つなぐ」ことが必要になる。接続点のリスクをはじめ，異なる事業体間で連携する場合には，事業体のセキュリティポリシーが異なることを前提にセキュリティ対策を講じる必要がある。



注：略語説明　CSSC（Control System Security Center：技術研究組合制御システムセキュリティセンター）

図2｜セキュリティ関連の変遷

脅威が多様化，高度化し，セキュリティ対策の前提条件は変化している。上下水道システムは広域化，多様なシステム連携も進み，セキュリティ対策が課題となっている。

ト運転への影響度を明らかにしたうえで，対策内容やその優先順位を論理的に導くことが重要となる。

2015年10月，電気学会「上下水道施設におけるセキュリティ技術の現状と課題調査専門委員会」は，上下水道事業体へのアンケート形式により，セキュリティへの対応状況に関する調査を実施した[6]。本調査では前回の2007年調査時点からの変化が考察されている。これによると，事業環境の変化によりシステムをつなぐ機会は微増である。また，外部ネットワークとの分離が基本であり，セキュアであることに変化はないと認識されている。しかし，今後，上下水道の広域化が推進されることで，これまでの前提条件が崩れていく可能性がある。広域化に伴ってセキュリティ対策が求められていくと考えられる。

2.2　行動指針となるガイドライン

これまでにも政府主導によりセキュリティ対策に関する指針が発行されており，その必要性，重要性を示している。

2006年10月，厚生労働省健康局水道課は，「水道分野における情報セキュリティガイドライン」を発行し，重要インフラとしての水道を停止させないための対策など，基本的な行動指針を示している。当ガイドラインは2008年3月に改訂されたあと，2013年6月，第3版として標的型攻撃などの新たな脅威やスマートデバイスなど情報通信技術の利用形態の変化などへの対応について新たに反映している[7]。

2015年1月施行の「サイバーセキュリティ基本法」では，「水道」を含む重要インフラ事業者に対するセキュリティ対応基準の策定，演習および訓練の実行についてその自主性を求めている。また，同法に基づき2015年9月「サイバーセキュリティ戦略」[8]が閣議決定され，国の危機管理，安全保障を踏まえ，政府と重要インフラ事業者，および関係企業が主体的に連携し，高度化したサイバー攻撃への対処を求めている。

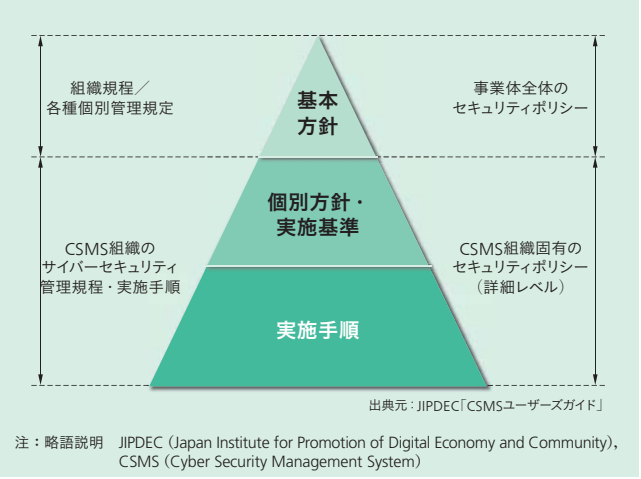
一方，国際的には，電力，石油化学，鉄道といった分野別の業界標準に続いて，制御システム全般を対象としたIEC62443規格の整備が進められている。

IEC62443-1-xシリーズは，共通概念，用語を扱う。IEC62443-2-xシリーズは制御システム保有者を想定し，セキュリティポリシーや組織に関わる管理システムを扱

う。IEC62443-3-xシリーズはシステム構築者を想定し，制御システムの技術要件を扱う。IEC62443-4-xは装置製造者を想定し，制御装置のセキュリティ要件を扱う。

制御システムにセキュリティを継続して確保するためには，各システムに求められるセキュリティ要件や監視制御システムの構成の変化に適応するPDCA（Plan, Do, Check, Act）が不可欠である。このPDCAの活動を支えるフレームワークとして，CSMS（Cyber Security Management System：サイバーセキュリティマネジメントシステム）認証がある。CSMS認証は，情報システムにおいてISO/IEC27001で規定されているISMS（Information Security Management System）の制御システム版と位置づけられ，JIPDEC（Japan Institute for Promotion of Digital Economy and Community：一般財団法人日本情報経済社会推進協会）がIEC62443-2-1に基づいた認証基準として2014年4月に公表した[9]（図3参照）。

今後，上下水道事業体でもCSMSに則したセキュリティマネジメントが求められると考えられる。



注：略語説明　JIPDEC（Japan Institute for Promotion of Digital Economy and Community），CSMS（Cyber Security Management System）

図3｜CSMS認証の体系イメージ

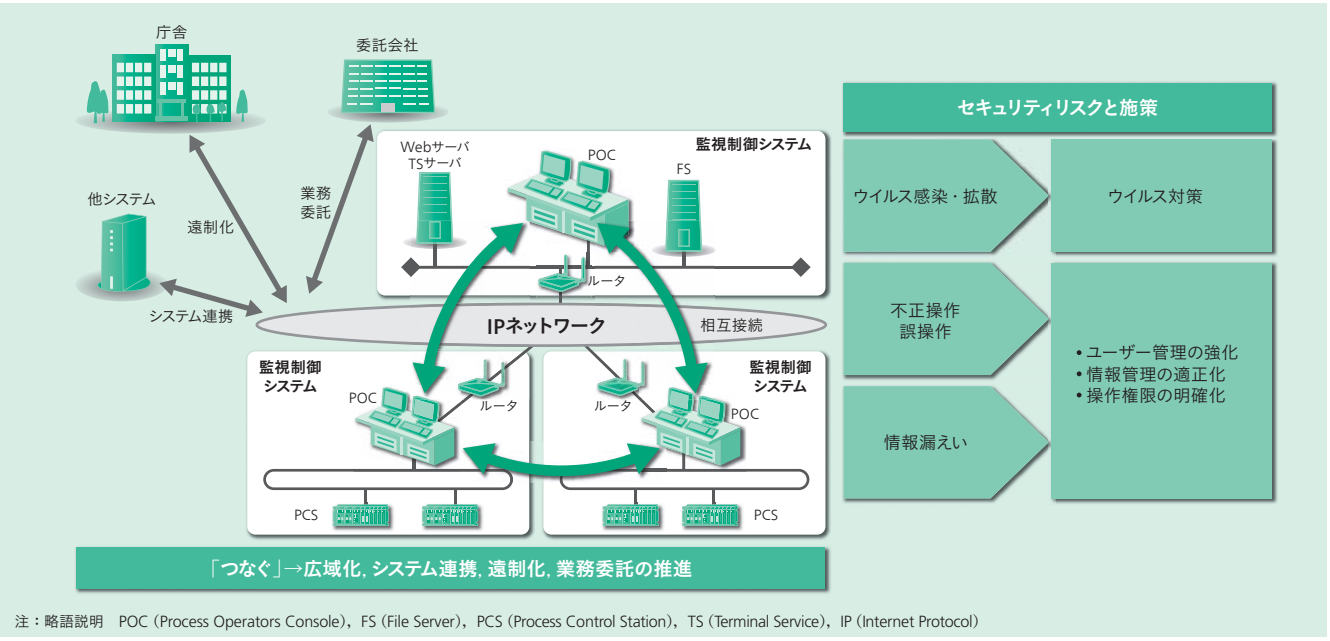
制御システムを運用する個別組織のセキュリティポリシーは，その上位組織のセキュリティポリシーや情報管理規定と関連づけられる。策定したセキュリティポリシーはその経営者の承認が必要となる。

3. AQUAMAX-AZ/SPにおけるセキュリティ施策

監視制御システムをつなぐことで，監視業務の統合を促進し，少ない運転員での運用を実現するとともに，業務委託による故障対応の迅速化や技術職員不足を補うことが可能となる。また，近隣事業体とのシステム連携を行うことで広域運用によるさらなる効率化や，ノウハウの蓄積，水平展開により技術継承の支援が期待できる。また，他業種，他システムと情報連携を行うことで新たな価値の創出を可能とする。

このような背景から，日立監視制御システムAQUAMAX-AZ/SPでは，複数の拠点間を閉鎖的なIP（Internet Protocol）ネットワークで接続して相互監視を実現する分散サーバを提唱し，「ドメイン化」という新たな考え方で広域監視制御を実現している[10]。また，WebサーバやTS（Terminal Service）サーバを設置して，よりオープンなIPネットワークを介した監視や制御を可能としている。

従来は，監視制御システムは閉鎖型を前提としていたが，システムの発展に伴い，つなぐことで，さまざまなセキュリティリスクが顕在化する（図4参照）。AQUAMAX-AZ/SPでは，このようなセキュリティリスクへの対処を行っているので，以下に紹介する（図5参照）。



注：略語説明　POC（Process Operators Console），FS（File Server），PCS（Process Control Station），TS（Terminal Service），IP（Internet Protocol）

図4｜監視制御システムの連携とセキュリティリスク

IPネットワークの発展に伴い，監視制御システムの相互接続が可能となり，広域化に貢献できるようになった。一方，つなぐことで生じるセキュリティリスクへの対応が必要である。

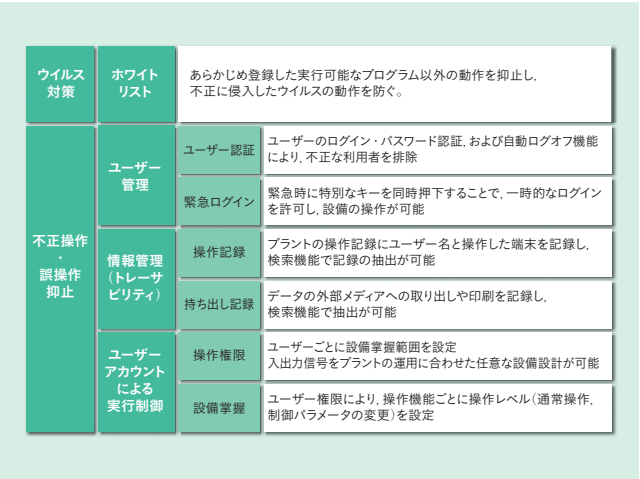


図5｜AQUAMAX-AZ/SPのセキュリティ機能

AQUAMAX-AZ/SPでは，システムの有する資産や機能をセキュリティリスクから保護するため，ウイルス対策やユーザー認証，ユーザーごとの操作権限を実装し，システムの安定稼働，設備の安全な操作環境を提供する。

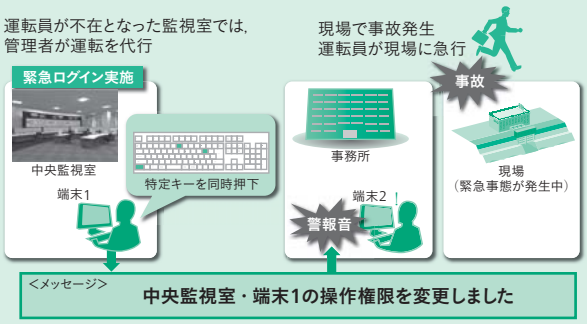


図6｜緊急ログイン機能

事故発生時や災害時に操作権限を持つ運転員が不在となる場合を想定し，一定時間，操作を許可する緊急ログイン機能を搭載している。

3.1　ホワイトリスト型ウイルス対策

監視制御システムを他システムと接続する場合，1台の装置がウイルスに感染すると，たちまち接続しているすべての装置にウイルスが拡散するリスクがある。

ウイルス対策としては，ウイルスの感染・拡散を防ぐため，ホワイトリスト型ウイルス対策を導入している。本方式は，あらかじめ登録したプログラムのみの実行を許可するもので，未登録のプログラムの実行を抑止することから，未知のウイルスへの感染を未然に防止する。ホワイトリスト方式は，ブラックリスト方式に比べて，ウイルスパターン更新のためのインターネット接続が不要であることから，閉鎖型システムでも導入が容易であることと，定期スキャンによるシステム安定性・応答性の低下を招くことがないという利点がある。

一方，ホワイトリスト方式の場合，感染済みのウイルスを除去する機能はない。そこで，持ち運び可能なUSBメモリタイプのブラックリスト方式によるウイルススキャンを併用して，確実なウイルスの感染・拡散防止策を提供している。

3.2　ユーザー管理とトレーサビリティ

遠制化や業務委託の進展により，監視操作を行う場所のフィジカルセキュリティが必ずしも十分でない可能性があり，不適正者が操作やデータ取得を行うリスクがあるため，ユーザー管理や情報管理の強化が必要である。

ユーザー管理機能では，システム使用時にIDとパスワードによる認証を行い，正規ユーザー以外の不正なログインを排除する。ログイン後は，一定時間操作がない場合に自動でログオフする機能があり，ログオフの操作を忘れても不適正者の侵入を防止する。パスワード管理では，パスワードの管理要件の向上に合わせて，パスワードの有効期限設定や一定回以上パスワード入力に失敗した際にユーザーIDを無効化する機能を実装している。

また，大規模な事故・災害発生時，現場対応などを行うために運転員が中央監視室から不在になることを想定し，中央監視室の運転業務を代行できる管理者用の緊急ログイン機能を実装した。これは，あらかじめ決められたキーボードの特別なキーを同時に押下することで，一時的にログインを許可し緊急を要する機器操作を可能とする。緊急ログイン中は，端末の警報音を鳴らし続け，非常時運用であることを通知する（図6参照）。

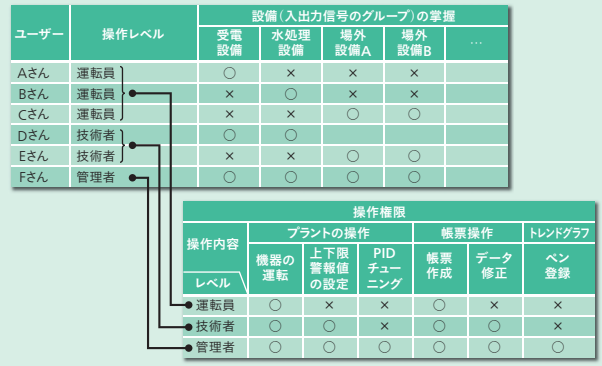
情報管理機能では，プラントの操作時に，操作記録にユーザー名，操作端末名を付加して記録するため，不正な操作や誤った操作の有無を後で検証することができる。さらに，システムが有するデータの取り出しや印刷操作についても記録を行い，いつ誰がどの端末から情報の持ち出しを行ったかを確認することができる。

3.3　ユーザーアカウントによる実行制御

図4のように相互接続された監視制御システムでは異なる拠点の運転員が利用するため，掌握外の設備への誤操作が危惧される。

そこで，ユーザーアカウントによる実行制御では，ログインユーザーに対して，どのレベルの操作を許可するかを指定する操作権限と，操作可能な設備の範囲を指定する設備掌握との組み合わせを可能とした（図7参照）。

操作権限では，運転員や技術者，管理者などについて事前に操作レベルを決めておき，各ユーザーにその操作レベルを割り当てることができる。例えば，運転員は機器の運転操作のみ，技術者は運転操作に加え上下限警報設定値の変更まで，管理者はさらに制御パラメータの変更まで操作可能というように登録することができる。また，一般の運転員と熟練運転員を区別して操作可能なレベルを分けると



注：略語説明　PID（Proportional - Integral - Differential）

図7｜操作権限のレベル設定

ユーザーごとに設備掌握と操作権限を設定可能とする。

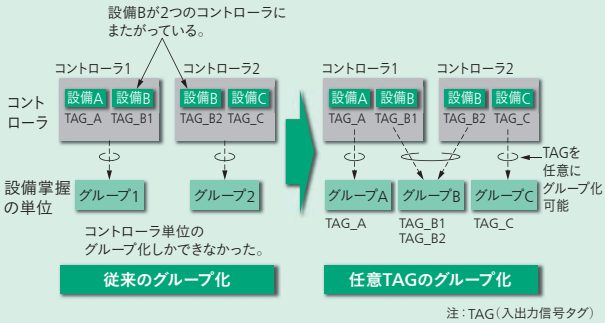


図8｜入出力信号のグループ化

入出力信号を任意にグループ化することが可能になり，運転員の監視操作範囲をきめ細かく管理できる。

いった利用も可能となる。その他，帳票データ修正やトレンドグラフのペン登録の可否など，ユーザーごとにきめ細かい権限の設定が可能である。

設備掌握では，入出力信号をグループ化することで，運転員ごとの監視操作範囲をきめ細かく設定することができ，設備への誤った操作を未然に防止する。従来の入出力信号のグループ化の考え方では，コントローラ単位にしか定義することができなかったため，1つのコントローラに複数の設備が収容されているケースや，1つの設備が複数のコントローラにまたがって収容されているケースには，適用が困難だった。新たなグループ化の設定では，システムに収容しているすべての入出力信号を任意にグループ化することが可能になり，運転員の監視操作範囲をきめ細かく管理できる（**図8**参照）。

4.　おわりに

本稿では，広域化の潮流によるサイバーセキュリティ対策の必要性と，それに対応して日立監視制御システムAQUAMAX-AZ/SPが提供するセキュリティ技術を述べた。

日立は，適切なセキュリティ対策こそが，「つなぐ」ことへの利便性を向上させ，安全・安心な上下水道インフラの持続的発展につながっていくものと考える。引き続き，セキュリティ技術のより優れた製品開発を行い，ソリューションの提供を図っていく所存である。

参考文献など

1）総務省自治財政局公営企業経営室：水道事業における広域化等の導入事例，http://www.soumu.go.jp/main_content/000382947.pdf
2）厚生労働省：水道普及率の推移，http://www.mhlw.go.jp/file/06-Seisakujouhou-10900000-Kenkoukyoku/0000122560.pdf
3）国土交通省：下水道処理人口普及率，http://www.mlit.go.jp/common/001103039.pdf
4）厚生労働省：水道広域化の必要性，平成27年12月水道課調べ，http://www.mhlw.go.jp/file/05-Shingikai-10901000-Kenkoukyoku-Soumuka/0000112382.pdf
5）下水道法，http://law.e-gov.go.jp/htmldata/S33/S33HO079.html
6）上下水道施設におけるセキュリティ技術の現状と課題調査専門委員会：上下水道施設におけるセキュリティ対策の現状とセキュリティ・マネジメントの考え方，電気学会，技術報告，1362号（2015.10）
7）厚生労働省健康局水道課：水道分野における情報セキュリティガイドライン第3版（2013.6），http://www.mhlw.go.jp/file/06-Seisakujouhou-10900000-Kenkoukyoku/0000046638.pdf
8）閣議決定：サイバーセキュリティ戦略（2015.9），http://www.nisc.go.jp/active/kihon/pdf/cs-senryaku-kakugikettei.pdf
9）JIPDEC（一般財団法人日本情報経済社会推進協会）情報マネジメント推進センター：制御セキュリティにおけるサイバーセキュリティマネジメントシステム（CSMS）認定・認証制度に関する文書の公表について，http://www.isms.jipdec.or.jp/csms/csmspublish.html
10）渡辺，外：上下水道の計画・運用・維持管理に貢献する情報・制御システム技術，日立評論，96，6，417～422（2014.6）

執筆者紹介

渡辺 忠雄
日立製作所 サービス&プラットフォームビジネスユニット
制御プラットフォーム統括本部 電機システム本部
社会制御システム設計部 所属
現在，上下水道監視制御システムの開発に従事

山口 浩介
日立製作所 サービス&プラットフォームビジネスユニット
制御プラットフォーム統括本部 電機システム本部
社会制御システム設計部 所属
現在，上下水道監視制御システムの開発に従事

田所 秀之
日立製作所 サービス&プラットフォームビジネスユニット
制御プラットフォーム統括本部 電機システム本部
社会制御システム設計部 所属
現在，上下水道監視制御システムの開発に従事
技術士（上下水道，情報工学，総合技術監理）
電気学会会員，計測自動制御学会会員

舘 隆広
日立製作所 水ビジネスユニット 水事業部 所属
現在，国内外の水環境事業および研究開発統括業務に従事
環境システム計測制御学会会員，触媒学会会員