特集
Special Feature

［社会インフラシステムにおけるサイバーセキュリティ―レジリエントで持続可能なデジタル経済社会に向けて―］

5 産業制御システムセキュリティの動向

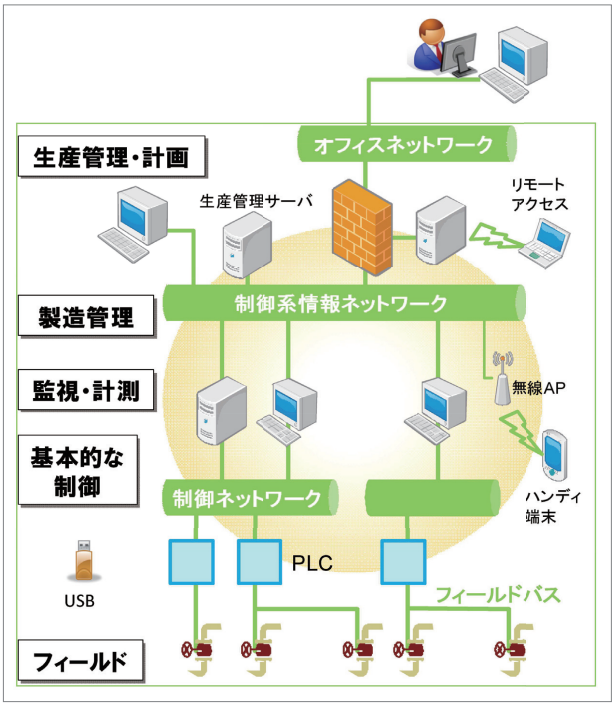
応般

新　誠一　電気通信大学

産業制御システム

電気やガス，水道，交通などの重要インフラや製品や部品，素材などを作る工場は社会生活に不可欠なものである．停電，断水，通信障害などに加え，食品，薬品，日用品，家電などの供給ひっ迫は，個人の生活や社会生活を停滞，停止させてしまう．あるのは当たり前，なくなって初めて受けている恩恵を自覚するものである．

そこでもコンピュータを中心とする計算機システムが幅を利かせている．具体的には，生産指示，燃料や材料などの残量情報，圧力や温度，流量などのセンサ情報などの内部の情報に基づいて操作情報を計算してゲートやバルブなどを制御する．これを産業制御システムと呼ぶ（図 -1）．このシステムの要素となる機器を産業制御機器と呼ぶことにする．対比となるネットワークとサーバおよび端末までのシステムを情報システムと呼び，そこに使われる機器を情報機器と呼びたい．図 -1 の上部に焦点を当てたものが情報システム，下部に当てたものが産業制御システムとお考えいただいてもよいと思う．そして，本稿の趣旨は，図 -1 全体に焦点を当ててサイバーセキュリティ対策を講じてほしいというものである．



■図 -1　産業制御システムの例

図 -1 の下部層では，温度や圧力などのセンサ情報に基づいて PLC（Programmable Logic Controller）がモータや油圧弁などのアクチュエータを操作する．ちなみに，PLC は自動車制御では ECU（Electrical Control Unit），家電などでは組込ボードに相当する．これらは一般にコントローラと呼ばれる．このコントローラレベルでは実時間性が必須である．たとえば，ミリ秒単位でセンシングし，操作をするものである．

この操作の実時間維持のために特殊な OS が用いられている，そのため，汎用のアンチウィルスソフトなどが使えなかった．さらに，工場などは油圧や空気圧による自動化から電動化・情報化という歩みを進めてきた．いわば，内部からの進化であり，外部接

続を目的とするものではなかった．このため，初期段階ではサイバー攻撃に対する配慮は薄かった．つまり，産業制御システムにおけるサイバーセキュリティ対策は，ネットワーク接続が前提となっている計算機システムとは違った捉え方をされてきた．

しかしながら，コンピュータ自体の高性能化，低価格化，堅牢化という発展と産業制御システムの横への拡大が様相を変えつつある．具体的には，IoT やコネクテッドと呼ばれるネットワーク利用の時代の到来である．家庭での質の高い生活や事業所などの高効率の生産活動の保証のために，天気などの環境情報，需要予測，燃料や部品供給情報などの外部からの情報が産業制御システムでも不可欠であり，ネットワーク接続なしでは工場は立ち行かない．以下，この辺の事情をもう少し詳しく見ていこう．

まずコンピュータの発展であるが，これは現代社会に不可欠なスマホに象徴される．100Mbps 以上の無線通信能力，数十 GB 以上の記憶能力，そして数 GIPS（Giga-IPS/billion Instructions Per Second）のマルチコア CPU（Central Processing Unit）を中心とし，GPU（Graphic Processing Unit），NPU（Neural Processing Unit）まで加えた処理能力．さらに GPS や高感度マイク，高精細カメラなどのセンサに NFC（Near Field Communication）に Wi-Fi，Bluetooth などのネットワーキング．それが手のひらサイズに収まり，クラウドがバックを支える魔法の道具，それがスマホである．

産業制御機器のコントローラは，ここまで進んでいない．しかし，影響を受けて変わりつつあるのも確かである．簡単に言えば，産業機器のパソコン化[1)]である．将来を見れば，クラウド化，スマホ化も視野に入れなければならない．

次に拡大である．ここでは拡大を物づくりのサプライチェーン化による広域連携であり，原材料費や需要変動までも考慮する最適化と捉える．簡単に言えば，現在の重要インフラや工場はネットワークなしでは稼働しない規模と精密さの下に運営されているという現実である．そして，インフラや工場などの停止はビジネスを止めるだけでなく，市民の生活も脅かすことは，災害が常態化している世界の共通認識である．

実は情報機器と呼ばれるものも実時間性が不可欠である．たとえば，株式の売買システムは HFT（High Frequency Trading）と呼ばれるマイクロ秒のつけ合いを間違いなく，確実にこなす必要がある．同様に，スマホを支えるネットワーク網も実時間性が不可欠である．この確実性がなければ，エレクトリックコマースもインターネットバンキングも意味をなさない．

以上の動向から，これまで情報システムと産業制御システムと区別していた時代から，両者を一体として扱わなければならない時代を迎えていると言ってよいだろう．産業制御システム側から見ると，Windows または Linux などの汎用 OS への収斂であり，イーサネットなどのインターネット技術へのネットワークの収斂である．このことは，産業制御システムへのサイバーセキュリティ対策の必要性を示している．逆に情報システムから見ると，エッジの先まで含めたリスクアナリシスとそれへの対策の必要性である．

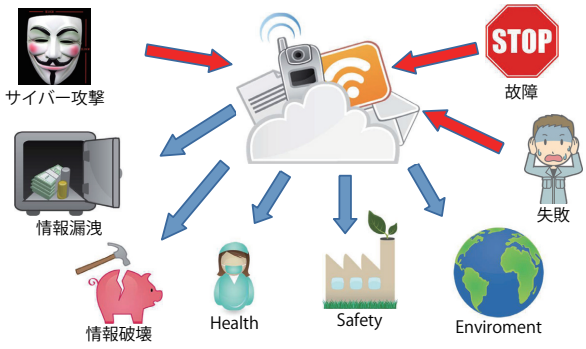
後者について，少し説明を加えると IS と呼ばれる情報システムを扱う部署の方々の関心は従来，サーバとネットワークと端末を視野にしていた．それに対し，クラウド，IoT デバイス，サプライチェーンと広がり，現在はセンサ，アクチュエータへのサイバーセキュリティをも視野に入れなければならないということである．

一方，産業制御機器の視点に立つと，閉鎖系であること，独自 OS であることを言い訳に十分なセキュリティ対策をしてこなかったことを見直す時期にきているということである．閉鎖系はリスクである．つなげば感染するリスクが生じる．そして，独自 OS もリスクである．サイバー攻撃リスクに対して十分な検査が行われていない可能性がある．それだけでなく，通信スタックや暗号化などを後付けしているために，OS やミドルウェアの全貌を把握できなくなってきている．中には，OSS（Open Source Software）が使われてい

ることを把握されていない場合や国外の会社が制作に関与していることも把握されていない可能性がある．一言で言えば，作成した会社も独自 OS の脆弱性を把握できていない．

実は情報システムも規模が大きくなりすぎている．そのため，脆弱性の種は尽きない．そこで，パソコンやスマホでは，頻繁にセキュリティアップデートが行われている．しかし，産業制御システムでのアップデートは難しいと言われてきた．24 時間，365 日休みなく稼働させなければならないのが，産業制御システム．しかも，不具合が起きれば，市民生活，生産活動にすぐに支障が出るのが産業制御システム．このため，十分なセキュリティアップデートが行われていない可能性が高い．それどころか，アップデートそのものを想定していない産業制御機器も多い．

以上を見ていくと，情報システムの方にアドバンスがあるように見える．しかし，人や社会の生命に直接かかわる産業制御システムのアドバンスももちろんある．それが HSE（Health, Safety, Environment）を守ることを軸に据えた機能安全である．産業機器において当たり前の機能安全にサイバーインシデントを加えたリスク解析と対策．同時に，情報セキュリティ解析に，エッジ下まで含んだリスク解析と対策を加えるべきということが本来の市民活動や生産活動を守るということである（図 -2）．安全とセキュリティの癒合



■図 -2　サイバーセキュリティ

であり，長年提案してきたことである [2]．ここに，ようやく両者が 1 つに収斂しつつあるということが，私が見る最近の動向である．

攻撃の変化

このような収斂の必要性は，重要インフラなどへのサイバー攻撃の様相の変化からもうかがえる．この変化を簡単に言えば，流れ弾から狙い撃ちである．または，拳銃から突撃銃である．拳銃からの数発の乱れ打ちなら，隠れていれば済むこともある．当たるのは運の問題と割り切ることもできた．しかし，突撃銃を持った戦闘員に襲われたら一般人はたまらない．

ちなみに，突撃銃は自動掃射と狙撃の二通りの攻撃が可能である．弾幕を張って一網打尽とする攻撃と静かに一発で距離を置いて仕留める攻撃である．この組合せもあるので，攻撃が高度化したと見ることもできる．

具体的にはランサムウェアと呼ばれる身代金攻撃に見て取れる．ご承知のように，攻撃を受けるとシステム内のデータを暗号化して使用できなくするものである．そして，復号化のために身代金を要求するものである．

対抗策はバックアップであった．元データがあれば，身代金を払う必要はない．しかし，最近の攻撃は，暗号化だけでなくデータ暴露も組み合わせている．お客様の個人情報やユーザの設計情報などを暴露すると脅しをかけているようである．さらに，ユーザにも脅しをかけて，暗号化された会社に身代金を払うように圧力をかけるという手の込んだ攻撃が相次いでいる [3]．

さらに，重要インフラ企業を狙って攻撃することで，インフラが停止する事態も引き起こしている．インフラは設備だけでない．顧客などの管理が伴わなければ稼働できない．この管理系のデータベースが暗号化されてインフラとしての使命を果たせなくなった事例も出現している．

もう1つの顕著な特徴はネットワーク管理機器やVPN（Virtual Private Network）などの脆弱性を突いた攻撃である．産業機器や社内ネットワークでは城壁を築けば，中は平穏という考え方をとってきた（図 -3）．しかし，城は外部との交流なしでは存続できない．だから門があり，警備する衛兵がいる．現在，この門には大量の出入りがある．数GBのデータが複数のポート，プロトコルを通じて出入りしている．ポートは門，プロトコルは出入りする種類，人，馬，荷物，破棄物だと思えばよいだろう．その門が多数で出入りが大量なら衛兵も見過ごす．それも，攻撃者は手を変え，品を変えて攻撃を仕掛けてくる．しかも，定常状態ばかりではない．在宅勤務が増えれば，容量アップ，危険情報が出れば警戒レベルアップ，故障に，テストに，設定変更．対応する衛兵であるネットワーク管理者は大変である．

情報機器でも，産業制御機器でも管理者は常に攻撃にされていることを痛感している．ファイアウォールの設定を1つ間違えば，瞬く間に感染が広がる．城壁に頼れば頼るほど，城壁に穴があいたときの被害は甚大である．VPNに頼れば頼るほど，その認証や暗号化に弱点があったときの被害は甚大である．実際，そのような攻撃が増加している．

このような脅威にさらされ，24時間，365日の対応をせざるをえない管理者が頼るのがネットワーク管理ソフトである．手動から自動へというDXの流れはセキュリティ対策にも及んでいる．

現在，このソフトが狙われている．管理ソフトもソフトである．そこには，必ず脆弱性が存在する．それを見つければ，その管理ソフトのユーザ企業に侵入したりなどの攻撃が可能である．最近，この管理ソフトの脆弱性をついた攻撃も増加している．桃源郷はない．仮にあったとすると，それは攻撃者にとって美味しい世界である．この桃源郷の住人は善人しかいない．ひとたび，悪人が混じれば阿鼻叫喚となる．これが，今の重要インフラや工場が置かれている現状である．

対策の変化

さて，以上の現状認識の下，その対策が気になるだろう．城を作る．それは水際対策．その対策が破綻する可能性がある以上，ファイアウォールやVPN以上の対策が求められる．続いて，その話をしていこう．

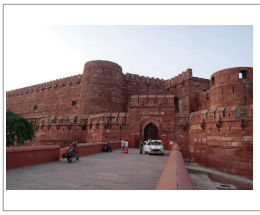
現在，対策側の合言葉は「Zero Trust」である（図 -3）．「何も信用するな」ということである．イントラネットも，孤立も，VPNも過信するなということである．一義的には，「自分の身は自分で守れ」ということである．ファイアウォールをネットワークレベルから自分，個，エッジレベルまで押し下げることである．

まず，最新のセキュリティアップデートを施して頑健とする．そして，外部との通信ポートは1つに制限する．さらに，通信プロトコルも1つに絞る．具体的には，HTTP（Hyper Text Transform Protocol）を使って，文字列のやりとりのみを行う．

これらの制限はセキュリティ対策で必須である．たくさんのポートやプロトコルではなく1つだけと決まれば，チェックしやすい．加えて，交換されるデータが文字列，つまり人が読める形式であれば，これもチェックしやすい．もちろん，セキュリティ対策だけでなく，バグ対策にも有効である．この制限は，計算能力を可読性，人に分かりやすくする方向に使うという第一歩である．

これをWindowsで言えば，DCOM（Distributed Common Object Model）から.NETへの移行に対応する．この移行はWindows XP時代に処置された．その意味で，古いOSは危険である．もちろん，常に最新のアップデートを行うことも必須である．

このアップデートは，OSとアプリのコンフリクトと



ファイアウォール，VPN
↓
End Point Security, 侵入検知，SOC

図 -3　水際対策から No Trust

いう大きな問題を生む．その対策は，アプリ制作側が OS の正規の API 内で動作するような開発を進める必要がある．画像メモリなどを直接アクセスしたり，TCP/IP スタックをいじったりすれば高速化することが可能であるが，それは OS のアップデートに支障を及ぼすし，セキュリティ対策という面からも問題である．このことから分かるように，複数の OS などで使えるアプリは正しく API を使っている可能性が高い．

このような対策を講じても OS とアプリのコンフリクトが生じる可能性がある．アプリ開発側が新しい OS での動作を常に確認するとともに，使用側もコンフリクトの可能性を視野に入れたアップデートが必要である．

その際，止められない産業機器でどのようにアップデートしていくかという技術が大事である．最前線では，情報機器のアップデートを参考にした対策が実行されている，たとえば，定期的に停止してアップデートを行う．また，事前に仮想 OS 上で，ほかのアプリとのコンフリクトのチェック．さらには，二重化した片方だけをアップデートする．様子を見て，もう片方もアップデートするなどである．エンジニアリングとはできない理由を探すことではない．エンジニアリングとは難しい問題のソリューションを構築していくことである．言い訳ではなく，解決が情報技術者にも産業制御技術者にも求められている．

以上は，重要インフラや工場というよりは情報システムセキュリティのイロハとも呼ばれる対策である．次に，主題の産業制御システムのセキュリティ対策を考えていこう．

産業制御システムが使われる場では，産業制御システムも，情報システムもおまけである．主人公は，建物や設備などの現物系である．費用は現物が中心であり，数十年使われる物は当たり前．だから，予算も数十年置きというのが昭和時代の実態である．更新周期が早い情報技術とは相性が悪い，さらに，セキュリティ系はおまけの情報システムのさらなるおまけ．できれば，費用をかけない理由を探す向きが多い．

さて，汎用ではない OS．誰が使っているのだろう．部品取りは古い機器維持の基本．破棄された産業用機器をもらい受けるのは，善人だけではない．悪人も欲しい．手に入れたら，種々の攻撃をして弱みを探すのが彼らの仕事．ベンダは汎用ではない OS の維持にお金をかけられるのだろうか．それだけの資金をユーザがお出しなのだろうか．古い機器は内部にパスワードが書かれているものもある．バッファオーバフロー攻撃に，DoS 攻撃．どこまで可愛い汎用ではない OS は耐えられるのだろうか．

そして，独自 OS の脆弱性を常に見守り，対策をし，アップデートまで行う負担は独自 OS 作成会社には負担が大きすぎる．Windows や Linux は利用者が多いから，この負担に耐えている．このことから，産業制御機器の OS も汎用化していくのは当然の流れと思われる．

目立たなければ大丈夫．本当に？　頭かくして尻隠さず．インターネット利用を拒否して生きていくのでなければ，隠れて生きていくのは不可能である．そして，隠者に守るべき資産があれば美味しい．頭を隠すような会社は，被害を隠そうとする．まさに，ランサムウェアの狙いどころである．

リスクアナリシスを行おう．予算が限られているなら，対処できていないリスクが現実化したときの対応を整理しよう．あきらめるのか，謝るのか，逃げ出すのか，それとも．また一からやり直すのか．

さらなる変化

桃源郷を守る情報技術が，ファイアウォールに VPN にパスワード付き ZIP ファイル．これらは，新型コロナウイルス対策で唱えられた水際対策そっくりである．有効であるが，破られたときの対策も講じないと全滅する恐れがある．

ファイアウォールも守る IS の苦労を CIO や CISO はご存じなのだろうか．変わる攻撃，変わる需要，ルータやスイッチの故障などに応じて設定を継続的に変え

なければならない．そして，その設定を間違えれば悲惨な結果を招く．24 時間，365 日の苦労は産業機器の維持管理をするエンジニアの苦労と変わらない．IS のエンジニア，現場のエンジニア，やっていることは同じである．ぜひ，仲良く産業機器を守ってほしい．

この大変さのため，自動で設定を変えてくれるセキュリティツールの利用が増えている．もっとも，このツールもソフトウェア．VPN もソフトウェア．いずれも，脆弱性と呼ばれるサイバー攻撃への弱みを抱えている．

ランサムウェア攻撃への対策として，USB メモリを使わない．変なサイトに接続しない．怪しいメールの添付ファイルを開かないというような水際の対策．次に感染した場合にファイルをミラーリングしておく対策．さらに，違う OS や違うデータベースを利用するヘテロ利用により感染を押さえる対策など多重坊業が施されている．もちろん，データベースの暗号化は必須である．さらに，前述の zero trust が現在のセキュリティベンダーのバズワードである．城壁は破られる．だから，内部の物も信用するなということである．ファイアウォールや VPN の内部機器の入出力，振舞いを監視し，異常を見つけたら警報を出したり，切断したりなどの対処をする．

特徴は監視機能である．この機能をシステムの内部に置くか，外部に置くかで扱いが変わる．前者の場合，内部だけで完結できる分かりやすさが特徴である．もっとも，監視機能もソフトウェア．OS やアプリが感染するなら，監視機能も乗っ取られる恐れがある．そこで，外部に監視機能を置くケースも考えられる．これは，オペレーションセンターであり，セキュリティに特化したものを SOC（Security Operation Center）と呼ぶ．

オペレーションセンターは IoT 時代には欠くことができない設備である．IoT を売った後も課金を続けるものと位置づけると，オペレーションセンターがなくてもビジネスができない．そこに，アップデート機能，監視機能を置くと SOC の役割を果たすことができる．

監視機能をソフトウェアである．SOC が乗っ取られたらどうするかも考えなければならない．鼬ごっこには深読みが必須であり，どこまで深読みしたかの勝負である．

サプライチェーン

SOC の設置は問題となっているサプライチェーンのセキュリティ確保でも有効である．これはプリントボード 1 つとっても多数のプレイヤがかかわっていることによって生じるセキュリティ問題である．IC 回路を設計する会社，それを元にウェハーを作成する会社，そのウェハーを切り出しパッケージにする会社，そのパッケージをボードに実装する会社．さらに，そのボードを動かすソフトの上位設計する会社．そこにさまざまな会社のファームウェアやミドルウェアを結合してボードに実装する会社．そして，このボードを複数使用して産業医機器が構成されている．さらに，この機器がネットワーク化されて産業システムとなっている．

このどこかの工程でバックドアやトロイの木馬と呼ばれるマルウェアや物理的なタッピングがなされると意図しない脆弱性が形成される．しかも，ハードもソフトもグローバル調達である．Windows OS だけで数億行，最新のチップセットは数十億個のトランジスターという状況を鑑みれば，産業システム全体を把握してる方は皆無である．それは，機器に限っても同様であり，ソフトに限っても同様であり，ハードに限っても同様である．

何か仕掛けられている可能性がある部品を含めて産業機器を構成し，産業システムを稼働させることは大変難しい．しかし，その難しさを踏まえて，全・安心に稼働させている枠組みも存在する．それが，産業システムの機能安全である．どのような部品や機器があるかというアセットを把握し，HSE（Health, Safety, Environment）へのリスクを解析する．その上で，各部品や機器が満足すべき機能を明確化する．

この段階でソフト側が注目しているのが，HAZOP で

あり，FTA であり，FMEA などの解析手法である．いずれも，産業制御システムで使われている手法である．それをソフトのバグ解析に使われ始めている．もちろん，サイバーセキュリティ解析にも有効である．ぜひ，図 -2 の見方で活用いただけると嬉しい．

水道情報活用プラットフォーム

産業制御システムのセキュリティ対策の進み具合は産業ごとに凸凹がある．自由化が進んでいる電力やガスは行政の支援もあり進んでいる．しかし，内閣サイバーセキュリティセンターが定める重要インフラ全般には普及していない．現在，水道業界では人口減対策などから産業制御システムのプラットフォーム化が進んでいる[4]．正に，図 -1 の上も下も含んだ形のプラットフォームである．上部は課金やアセットマネジメント，下部は制御用のネットワークまで含む垂直型のプラットフォームである（図 -4）．

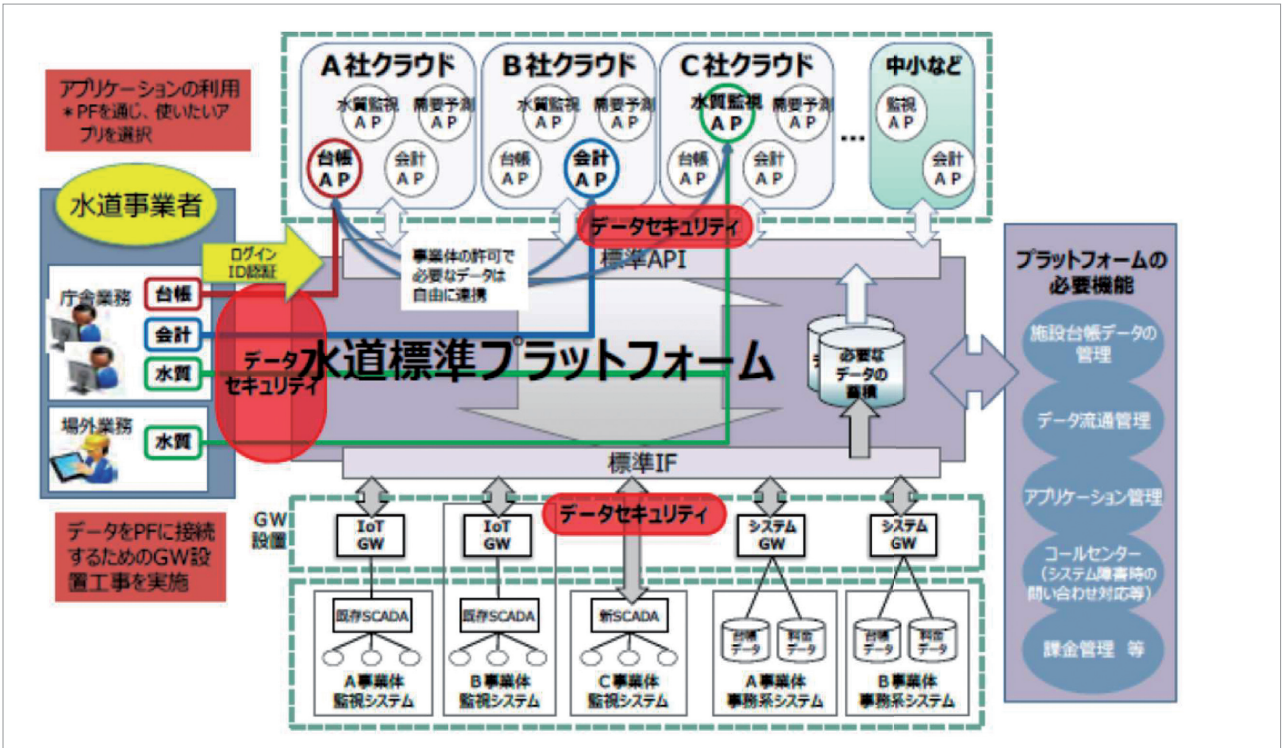
このプラットフォームは OPC で各種制御用ネットワークの差異を吸収し，NO（Not Only）SQL 仕様でデータベースの差異を吸収する構成である．管理者の不足をプラットフォームが担うとともに，プラットフォームのセキュリティは提供者である JECC が担う．

このプラットフォームを水道事業に普及させていくと同時に，ほかの事業にも広げていくことが私の現在の活動の 1 つである．これを本稿の締めくくりとさせていただく．

参考文献
1）電気学会編：公共プラントとパソコン応用－その光と影－，コロナ社（2001 年）．
2）新　誠一：社会インフラへのサイバー攻撃に対する課題と取り組み，情報処理，Vol.55, No.7, pp.640-646（2014）．
3）日経新聞：サイバー身代金，支払い 5 割　金額急増し攻撃に拍車応じた企業，米 87%，日本 33%，2021 年 9 月 20 日朝刊．
4）https://www.jecc.com/service/list/ws-platform.html

（2022 年 1 月 5 日受付）

■新　誠一　seiichi.shin@nifty.com
2020 年電気通信大学名誉教授．2013 年から 2020 年まで共同研究組合制御系セキュリティセンター理事長．2020 年水道情報化活用研究会会長．2021 年（株）アイシン社外取締役．



■図 -4　水道情報活用システム（https://www5.cao.go.jp/keizai-shimon/kaigi/special/reform/wg6/20200324/pdf/shiryou3-1-1.pdf）