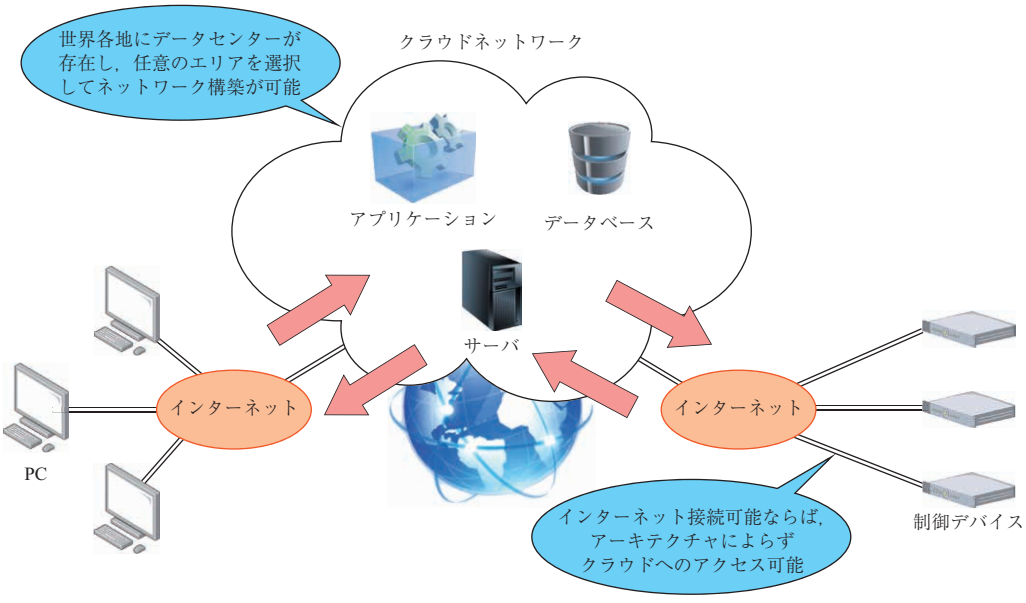
クラウド活用による セキュアな遠隔制御の開発

リモート化のニーズに応え，お客さまの 安全・安心に貢献する遠隔制御技術

新型コロナウイルスの影響後の新常態「ニューノーマル」において，あらゆる分野で ICT 活用によるリモート化のニーズが高まっている．IHI はクラウド基盤のメリットを活用することにより，工場で稼働するデバイスの遠隔制御や保守支援の効率化と安全・安心の両立を目指している．

株式会社 IHI
技術開発本部　技術基盤センター
制御・センシンググループ　　平田　圭史朗



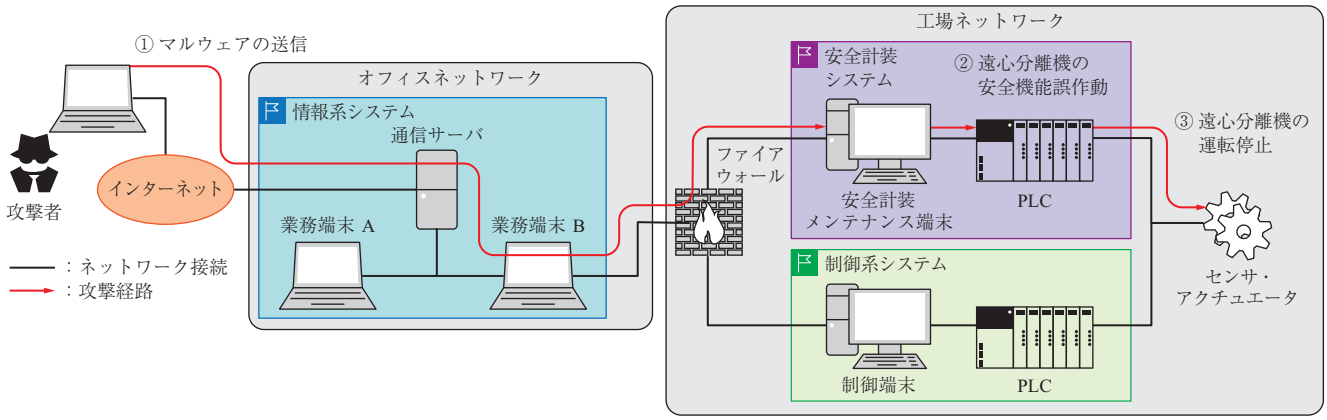
クラウド概念図

クラウドサービス利用の展望

クラウドサービスとは，上図のとおりインターネット経由でコンピュータ資源を提供するサービスの総称であり，企業の業務やサービスの中核となる IT（情報系）サービスに活用されている．クラウドサービスは，使用者が管理する施設の構内で機器を運用する形態（オンプレミス）と比較して，ハードウエア導入に伴う初期の多額の投資と，リソースの調達，メンテナンス，容量の使用計画などの作業に多大な人的リソースを費やす必要がなくなる点で優れる．

日本国内においても，少子高齢化や地方の過疎化といった課題を解決し，持続可能な経済成長を遂げるために政府情報システムの構築において，クラウドの活用を第一に検討する原則が 2018 年に打ち出されたことにより，民間においてもクラウド利用が促進されている．

クラウド市場規模は拡大の一途をたどっており，そ



Stuxnet 攻撃事例

の中で大きなシェアを占めているクラウドプラットフォームは，Amazon Web Service (AWS)，Microsoft Azure，Google Cloud Platform などである．いずれも全国各地にデータセンターを保有しており，ユーザは各エリアに存在するサーバを任意に利用可能である．特に，サービスではなく計算機資源をインターネット経由で利用する IaaS (Internet as a Service) 分野においては AWS が 45％のシェアを誇り，クラウド基盤としてのデファクトスタンダードとなっている．

制御システムセキュリティの動向

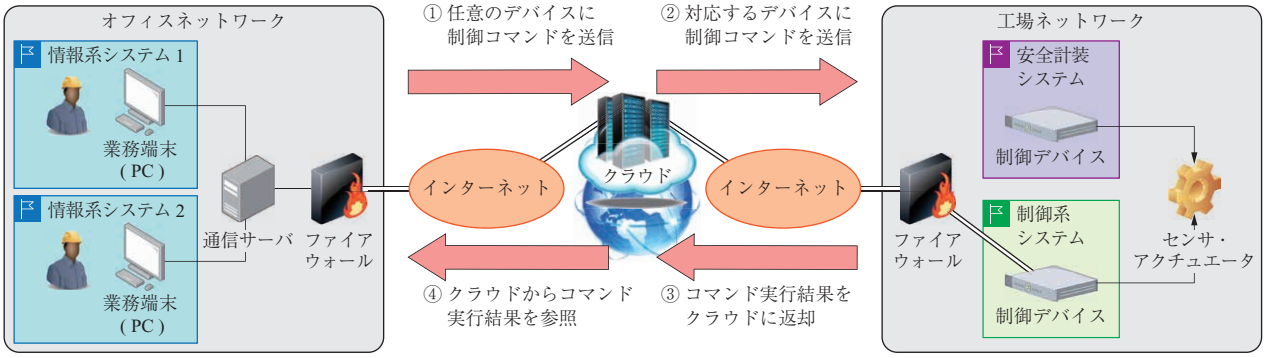
従来の電力，ガスなどの重要インフラの OT (制御系) システムは，インターネットや社内の情報系システムと接続しない独立したシステムとして設計，運用されており，独自 OS を使用した機器，独自の通信プロトコルを適用したネットワーク機器を使用してきた．しかしながら，最近では汎用 OS，標準プロトコルの採用など技術の標準化，オープン化が進みつつあるほか，IT ネットワークと OT ネットワークを統合したネットワークシステムとして構築し，データや資源の有効活用を図る傾向にある．この結果，サイバー攻撃の拡大と汎用的な仕様の利用による脆弱(ぜいじゃく)性の露呈が指摘されるようになった．

2010 年には，Stuxnet と呼ばれるマルウェア感染により，OT システムを狙った初のサイバー攻撃が発生した．このマルウェアはイランの核燃料施設に持ち込まれ，上図の攻撃フローによって遠心分離機を制御する PLC (Programmable Logic Controller) の設定ロジックが改ざんされ，約 8 400 台の遠心分離機のうち約 1 000 台が稼働不能に陥り，操業が一時停止する事態となった．これ以降，OT システムのセキュリティインシデントは継続的に報告されており，最近ではアメリカの石油パイプラインがランサムウェアによる攻撃を受けて一時的に操業を停止し，ガソリンの供給不足など一般市民の社会生活に直接影響を及ぼす事例も発生している．

OT システムのセキュリティ機能要件，機能設計，技術に関する国際規格としては，IEC62443 が多くの規格から参照される位置づけとなっており，現在，システムの安全性とセキュリティを両立するための標準が策定され始めている．また，IEC62443 に対する第三者認証制度が提供されるようになり，取得件数も増加傾向にある．国内においても総務省および経済産業省がセキュリティ法制度化に取り組んでいる．IHI もこれらのセキュリティ動向に注視しながら，安全・安心を担保するための技術開発を進めている．

クラウドベース遠隔制御システムの期待と課題

ICT を活用した働き方変革のためにクラウド活用の必要性は高まっており，製造業分野も例外ではない．クラウド上の高度な分析ツールによって工場のフロアデータを取得，分析，可視化するスマートファクトリー化や，クラウド上の潤沢な計算機資源を用いた大規模な並列計算への活用が期待されている．さらに，工場で稼働する制御デバイス類の保守操作について，物理的に離れた位置に存在するオフィスから制御する (次ページ図)，遠隔制御のニーズがコロナ禍により高まっている．多拠点，大量デバイスの遠隔制御シス



遠隔制御システム

テム構築は，クラウドの並列計算を活用することで，初期投資を抑えつつ短リードタイムで可能と考えられる．

一方，遠隔制御システムへのクラウド技術の適用にあたっては，次のような課題がある．

・クラウドを経由することによる通信遅延対策：
　オフィス－工場間の双方向通信のリアルタイム性を向上させるための通信仕様設計
・インターネット通信を経由した攻撃に対するセキュリティ侵害対策：
　ネットワークとの結合度が上がる状況下での不正なユーザや端末による接続防止，既知の脆弱性対策，および，通信堅牢性の評価

これらについての対策技術の概要を以下に示す．

(1) 通信遅延対策

通信遅延対策としては，PC －クラウド間通信，デバイス－クラウド間の通信を可能な限り軽量にする必要がある．前者は 1 度のコネクションで双方向通信を可能とする WebSocket，後者は軽量かつ一対多の通信が可能な MQTT (Message Queuing Telemetry Transport) 通信方式を採用し，クラウド側でこれらの通信を中継するためのサーバを構築することで通信遅延を低減した．これに加えて単一のサーバでリクエストを待ち受けるのではなく，リクエストに応じてクラウド上で複数のサーバが立ち上がるようにすることで，負荷上昇時の応答速度の低下を防いでいる．

(2) セキュリティ対策

不正接続を防止するため，クラウドが PC から制御コマンドを受信した際，クラウドがデバイスとの通信コネクションやデバイス側のコマンド実行状況を監視して，リクエスト制御を行う機能を実現した．PC とデバイスそれぞれがクラウドとの通信を行う際にはそれぞれの認証を行い，不正な端末の接続を防止するようにしている．PC 側は，WebSocket の通信コネクション開始時に ID とパスワードで操作者認証を行い，デバイスは個別に与えられた証明書を用いて MQTT セッション開始時に認証を行う．また，両者とも TLS (Transport Layer Security) によって暗号化されており，一定の盗聴対策を図っている．

遠隔制御システムの性能評価

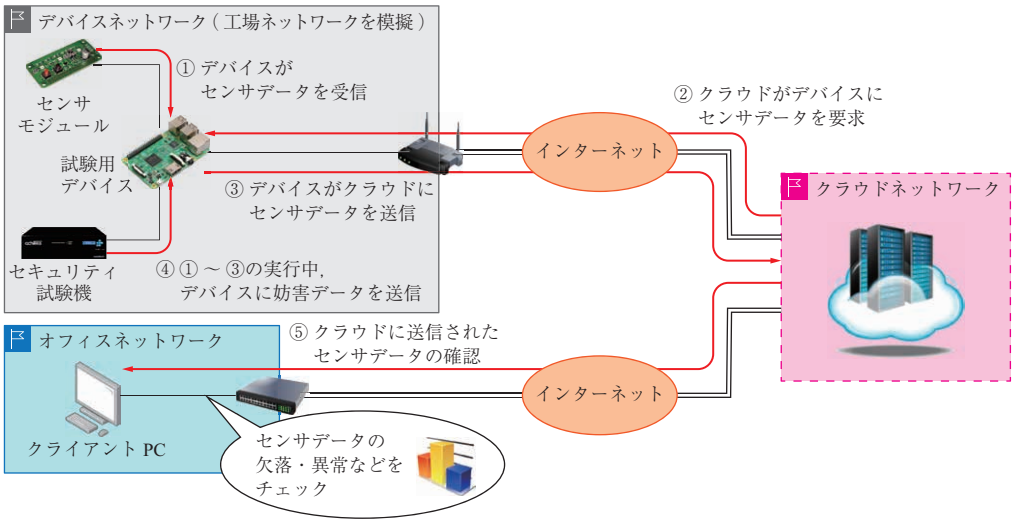
これらの検討に基づき試作した遠隔制御システムについて，通信応答性能評価，および，セキュリティ評価について述べる．試作システムに利用する制御デバイスは，一般的な制御コントローラ相当の性能をもつシングルボードコンピュータとしている．

(1) 通信応答性能評価

PC と制御デバイスとの物理的距離が最も近いクラウドサーバを用いて通信応答性を評価した．

PC からクラウドに対してリクエストを送信してその応答を得るまでが 260 ms 程度，クラウドが制御デバイスに制御コマンドを送信してその応答を得るまでが 150 ms 程度であった．後者について，制御デバイス側で稼働するプログラムの処理時間が 35 ms のため，通信処理自体には 115 ms 程度を所要している．

トータルでも 400 ms 程度ですべての処理が完了し，Web サービスとして標準的な応答時間にて運用可能と判明した．



遠隔制御システムのセキュリティ試験構成

(2) セキュリティ評価

セキュリティ評価として，IEC62443 をベースとした試験（デバイスの脆弱性試験および通信堅牢性試験）相当のものを実施した．

・ 脆弱性試験

制御デバイスの OS，ミドルウェア，アプリケーションに過去に報告された脆弱性に該当するものが存在するかを調査するため，テスト用パケットをデバイスに送信して調査した結果，致命的な脆弱性は検出されなかった．

・ 通信堅牢性試験

デバイスの機能停止や誤動作を誘発する大量のパケットや不正な構造をもつパケットをデバイスに送信した際の挙動を検査した結果，デバイスがクラウドに送信したデータの欠落はなく，CPU，メモリ使用率も一定値で推移したため，一定の堅牢性を有すると判断した．

以上より，今回試作した遠隔制御システムの通信応答性・セキュリティ面での評価結果においては，運用に向けた技術的な障害がないことを確認した．

今後の展望と課題

クラウドベース遠隔制御システムは，制御パラメータ調整といった実稼働中の操作だけでなく，IoT デバイスの導入，廃棄，再利用の設定操作などライフサイクル全般にわたり利用可能である．一方で，従来のシステムとはネットワーク構成環境や通信処理方式が大きく異なり，セキュリティポリシーの遵守や管理体制の構築など運用面での対応が必要である．また，各種クラウドアプリケーションのメジャーアップデートやセキュリティ規制動向に応じて，システム構成およびセキュリティ実装を随時見直す必要がある．これらの課題に対しては，社内外のクラウドプラットフォームのサポートチームやセキュリティの専門家などとも連携して取り組んでいく．今後，試験的なクラウド活用プロジェクトを推進する中で本技術の活用領域，クラウドのメリットを活かせる適用策を見極めていく．

技術的な展望として，クラウドを用いて試作した機能を，インターネットブラウザ上で操作可能な Web アプリケーションとして提供していく必要があると考えている．これにより PC，スマートフォンなど端末の種別を問わずに機能を提供できるようになり，開発効率・ユーザビリティ双方の向上が期待される．遠隔制御のほか，保守支援や予防保全技術などデジタルトランスフォーメーション／ライフサイクルビジネス分野での活用により，お客さまにとっての価値増大に貢献していきたい．

問い合わせ先
株式会社 IHI
技術開発本部　技術基盤センター
制御・センシンググループ
電話（045）759 - 2865
https://www.ihi.co.jp/