エッジコンピュータを用いた遠隔監視サービスシステム向けセキュリティ技術

The Security Technology for Remote Monitoring Service Systems Using the Edge Computing

高尾 健司*1 Kenji Takao
木村 修*2 Osamu Kimura
西村 利通*3 Toshimichi Nishimura
吉貝 太*4 Futoshi Yoshikai

クラウドシステムを用いた状態分析/予兆検知を行うサービスは広く浸透しているが，プラントなどの監視対象を外部ネットワークに常時接続することはセキュリティ上の懸念がある。そこで，外部にデータを出すことなく状態監視を行うエッジコンピュータを用いた遠隔監視サービスシステムが近年注目されている。しかし，エッジコンピュータでプラントの状態監視を行う場合でも，異常検知時の原因究明には，いかに効率よく，かつセキュアに現在のプラント状況を遠隔保守員と共有するかが課題となっていた。

そこで，比較的容易かつ安価に，エッジコンピュータと外部ネットワークを，必要な時のみセキュアに接続できる技術を開発した。これにより，高いセキュリティ性を保持した状態で遠隔監視サービスを提供することが可能となる。

1. はじめに

近年の機械学習/AI 技術の進展に伴い，日々収集されるプラントデータに基づく異常検知，異常予測を行う遠隔監視サービスの適用事例が増加している。またクラウドサーバの信頼性向上，低コスト化に伴い，遠隔監視システムをクラウド上に構築するケースが多い。しかし，クラウドサーバを用いて遠隔監視を行うには，常時外部ネットワークに接続し，運転データをクラウドサーバにアップロードする必要がある。常時接続は，制御装置へのサイバー攻撃や運転データの流出リスクなどが高まることから，遠隔監視システム/サービスの導入に踏み切れないプラントオーナも多いが，エッジコンピューティングによるデータ分析サービスが一つの解決手段となる。エッジコンピューティングでは，プラント内に監視/分析ロジックが含まれる計算機を設置し，現場でデータを処理し異常検知/異常予知を行うため，外部にデータを出すことなくプラントの状態監視が可能となる。しかし，エッジコンピュータを用いた監視サービスには以下のような課題が考えられる。

1) エッジコンピュータが収集したデータ，及び分析結果の，遠隔保守員との共有
2) エッジコンピュータ上にインストールしているデータ分析プログラムの更新

上記に対しては，一般的には，VPN（バーチャルプライベートネットワーク）が用いられることが多いが，機器/サービスが高価となり，設定が煩わしい。そこで，“比較的安価”かつ“煩わしい設定が必要なく比較的容易に設定可能”なセキュリティ技術を用いて，“必要な時のみ”外部ネットワークとセキュア接続を確立し，“必要な操作のみを許可”できる遠隔監視サービス向けシステムを開発した。

*1 ICT ソリューション本部 CIS 部 主席部員 工学博士
*2 MHPS エンジニアリング(株)長崎事業部サービス推進部 グループ長
*3 MHPS エンジニアリング(株)長崎事業部サービス推進部 主席T統括
*4 MHPS エンジニアリング(株)長崎事業部総務部

2. セキュア通信技術 － NATトラバーサル＋独自暗号化通信

2.1 セキュア通信技術の特徴

開発したシステムは，remot3.it 社(米国)[1]が提供するセキュア通信技術を利用している。本技術は，NAT トラバーサルと remot3.it 社独自の暗号化通信をベース技術とするもので，“小さく”，“軽く”，“簡単”であることが特徴である。特に，以下の機能により高いセキュリティを確保している。

1) セキュア接続を行う際に，グローバル IP(Internet Protocol)アドレスを要求しない。またプライベート IP アドレスも接続相手に公開する必要がない(図1)。

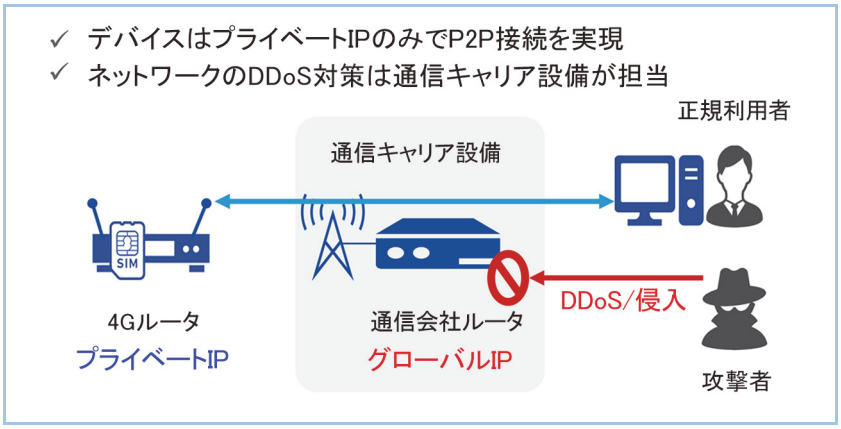

図1 セキュア通信技術の特徴①:
P2P(Pier-to-Pier)接続にパブリック IP アドレスを利用しない

2) インバウンド通信(外から内への方向の通信)に対して，接続先マシンのポートを全て閉じた状態でもセキュア通信が可能である(図2)。

図2 セキュア通信技術の特徴②:
接続先マシンの外部ポートを全て閉じることができる。

また，本技術は，暗号化通信や NAT トラバーサルの知識が無くても，簡単にセキュア通信技術が利用できるパッケージ技術であり，比較的容易に導入することができる。

2.2 セキュア通信技術の詳細

remot3.it 社独自の NAT トラバーサルと暗号化を組み合わせたセキュア通信技術の仕組みを図3に示す。図3において“管理サーバ”はクラウドに配置されており，本サーバが全ての接続を管理している。各端末は，自身の所在地(自身のローカル IP アドレス，接続されているルータのパブリック IP アドレス)を暗号化し，UDP により管理サーバにその情報を定期的に送信する。これにより，端末が別のルータに接続された場合でも，管理サーバは端末から送信される情報に基づき端末の情報を適宜更新することにより，端末の所在地を常に把握することができる。

端末間で接続を開始する場合は，接続要求元から管理サーバに対して接続要求先のサービ

ス名（マシン名＋サービス名）を送信する(①)。サーバは要求元の認証を行った上で（②，③，④），その要求情報を解釈し，接続に必要な情報を暗号化した上で接続要求元に送信する（⑤－1）。同時に，接続要求先にも接続要求元の情報を送信する（⑤－2）。この際，接続要求元，接続要求先のUDPポート番号を基にStateful Inspectionの原理を用いた情報交換（⑤－1，2）が行われ，端末間で独自暗号化トンネルを確立させる(⑥，⑦)。確立した独自暗号化トンネル上で例えば SSH 接続時には，SSH 接続先のホスト情報を用いず，ローカルホスト（ループバックアドレス127.0.0.1）を利用することで，SSH接続先のIPアドレスとポート番号を完全に隠すことができる。本技術の利用に際し，事前準備は，専用のアプリケーションを接続したいマシンにインストールし，“マシン名とサービス名”を登録するのみであり，簡単な設定，操作で高いセキュリティを確保できる。

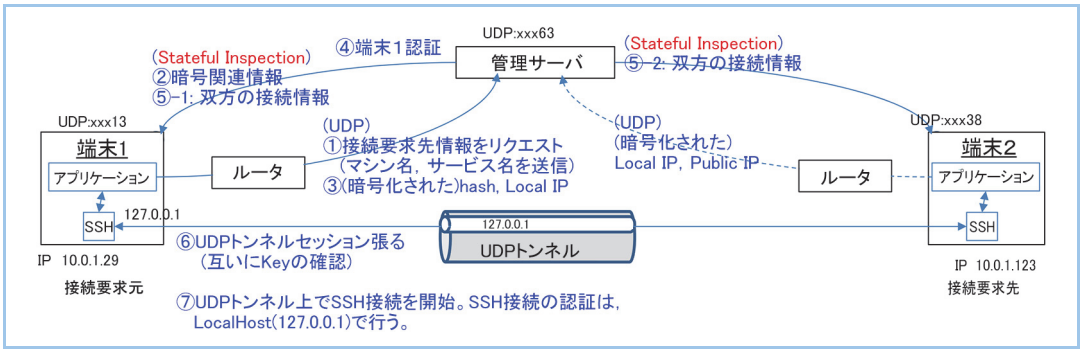

図3　NATトラバーサルと独自の暗号化技術を組合わせたセキュア通信の仕組み

3. セキュアな遠隔監視サービスシステム

3.1 システム構成

本章では，2章で述べたセキュア通信技術を用いて開発した，遠隔監視サービスシステムについて述べる。本システム構成を図4に示す。尚，Web サーバを閲覧して監視する機能だけを利用する場合(3.2(1)の機能))は，接続元である遠隔監視PC，お客様側監視PC にはremot3.it 社のソフトウェアのインストールは不要である。(注: 3.2(2)，(3)の機能を利用する場合は，インストールが必要である。)

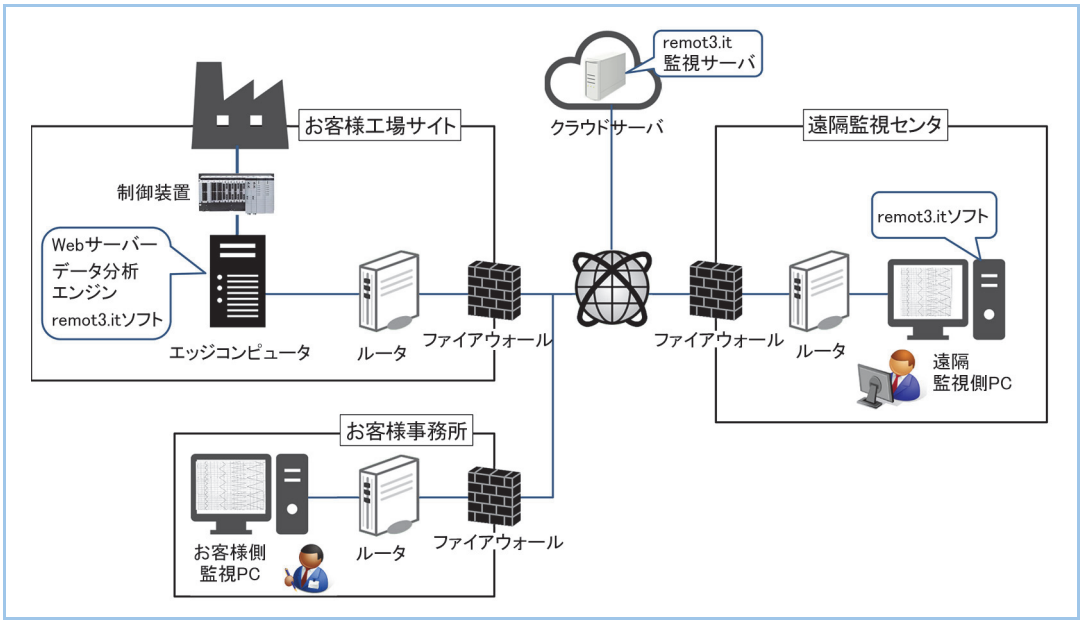

図4　エッジコンピュータを用いた遠隔監視サービスシステム

3.2 機能

遠隔監視サービスでは，以下の機能が利用できる。これらの機能を用いることで，セキュアな遠隔監視サービスの導入が可能となり，異常の早期発見や異常時の早期復旧による稼働率向上が期待できる。

1) http/https による Web アプリケーション画面閲覧機能

本機能により，Web サービス利用を特定の利用者に限定させることでセキュリティレベルを上げることができる。本機能利用者は，Web サーバが含まれるマシンへの接続を確立した後，ブラウザに，ローカルホストアドレス(127.0.0.1)を入力するだけで，該当の Web アプリケーション画面を閲覧することが可能となる。実際の IP アドレスを利用しないため，高いセキュリティが確保される(図5)。

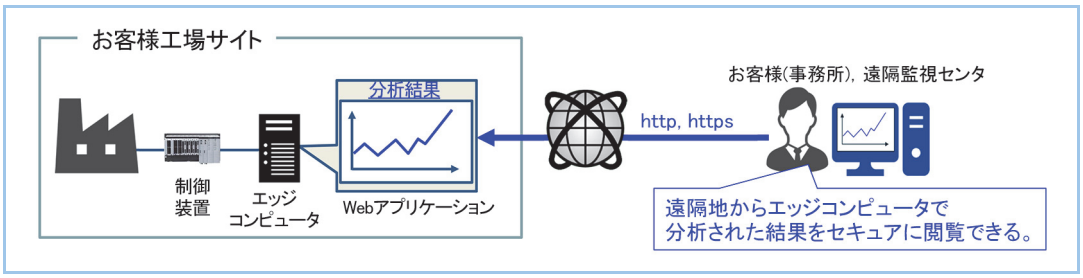

図5 http/https による Web アプリケーション画面の閲覧機能

2) リモートデスクトップによる遠隔地マシンへのアクセス機能

お客様工場サイトに置かれたデータ分析エンジンや Web サーバが含まれるコンピュータ(エッジコンピュータ)を運用する場合は遠隔保守が必要になる。遠隔アクセスの権限はお客様に持たせることで，外部からのアクセス管理をお客様自身が容易に行うことが可能となる。1)と同様に，リモートアクセス時の IP アドレスはローカルホストアドレス(127.0.0.1)を利用する(図6)。

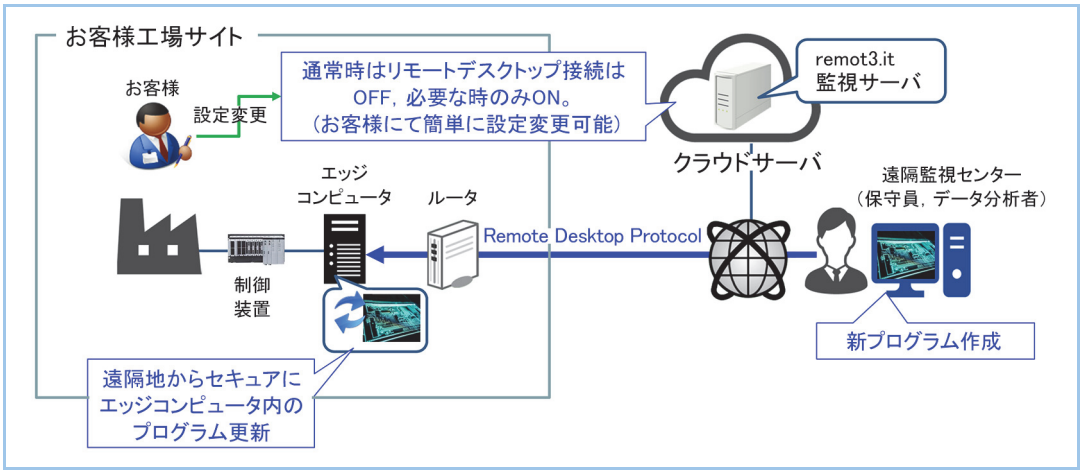

図6 リモートデスクトップによる遠隔地マシンの操作

3) データの自動セキュア送信機能

エッジコンピュータを用いた監視サービス提供中でも，異常発生時などには，遠隔地にいるデータアナリストによる詳細データ分析が必要となる場合がある。その際，データのセキュアな送受信を行う場合に本機能が活用できる。例えば，エッジコンピュータである計測値の予測を行っていたとする。予測精度が悪化したことを検知すると，原因分析に必要なデータをセキュアデータ転送プロトコル(sFTP)により該当マシン(遠隔地)に送信し，送信完了後にセキュア接続を自動切断する。これにより，人を介さず自動的にデータが共有でき，迅速な原因特定が可能となる。また同様に，エッジコンピュータに対してセキュリティパ

ッチを送信する場合など，遠隔地からエッジコンピュータへセキュアにファイルを送信することもできる(図7)。

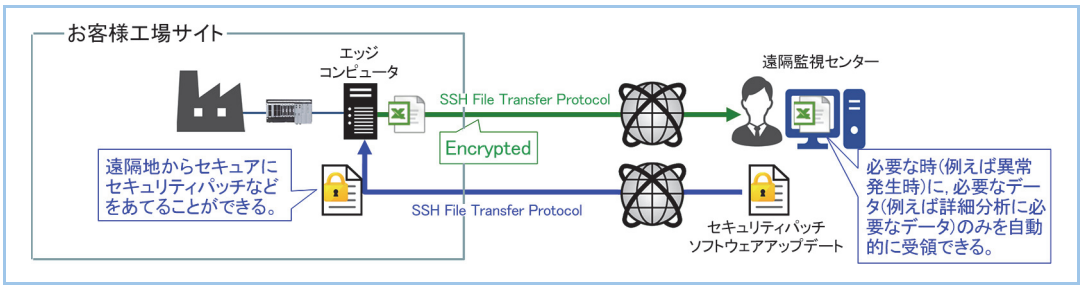

図7　セキュアなファイル送信機能(イベント発生時の自動接続/送信/切断機能含む)

4. 適用事例

本報で述べたシステムのうち，一部の機能について，MHPS エンジニアリング(株)(以下，MHPS エンジ)長崎事業部にて実施されている“VPSA(真空圧力スイング吸着)式酸素発生装置”のアフターサービスを対象として実証試験を実施した。

従来，MHPS エンジでは，顧客プラントでアラームが発生した際，原因究明に必要なデータをお客様から電子メールで送信してもらい，詳細分析を実施していた(図8)。このプロセスでは，復旧までに多くの時間を要し，お客様プラントの稼働率低下を招いていた。

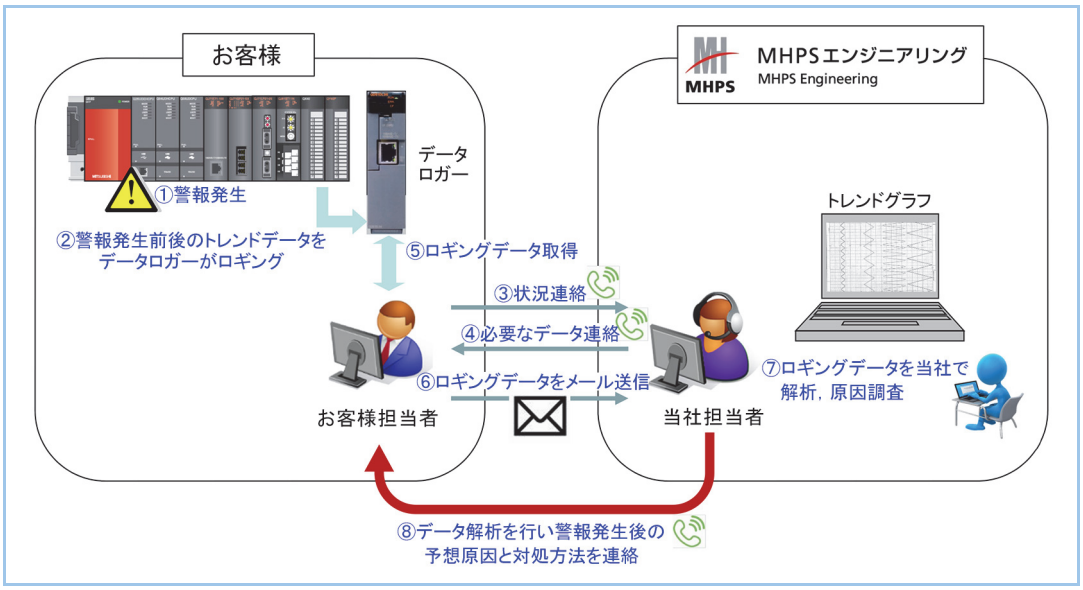

図8　MHPS エンジニアリングにおける従来の異常発生時の対処プロセス

開発したセキュア通信システムを本遠隔監視サービスに適用した。その概要図及びセキュア接続プロセスを図9に示す。本サービスシステムに実装した機能は以下の通りである。

1) グラフィックオペレーションターミナルによる運転支援
2) 制御装置(PLC)のラダープログラムの表示，プログラム改良
3) お客様工場の制御装置から得られるデータのトレンドグラフ監視
4) データ詳細分析のための運転ログファイルのセキュア送信機能

開発した本システムを，あるお客様プラントに適用し実証試験を行った。実証試験の結果，上記すべての機能が MHPS エンジから遠隔実行でき，所望の要求を満足することが確認できた。

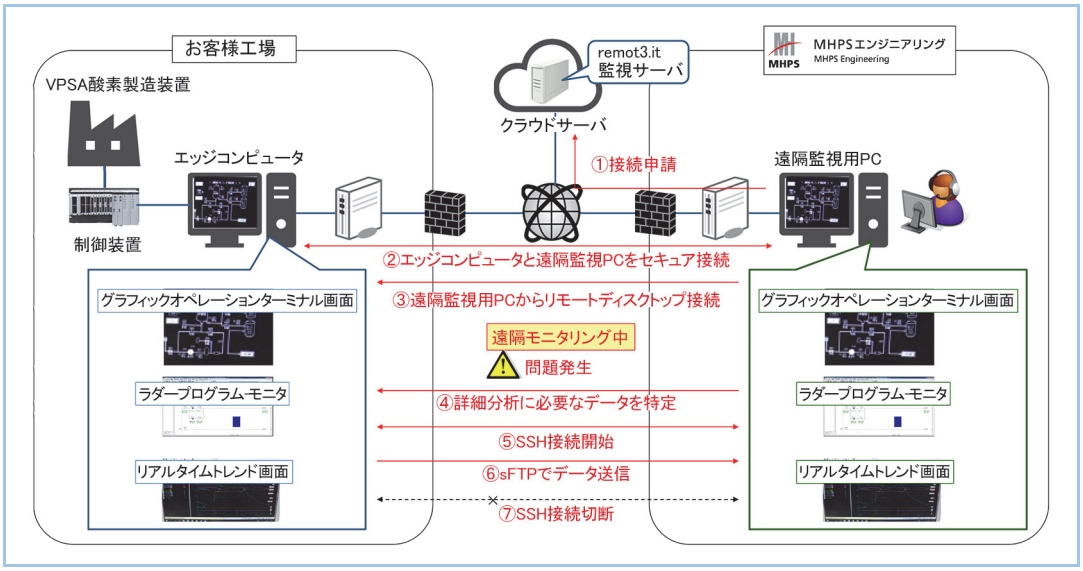

図9 VPSA 遠隔監視サービスシステムの概要及びセキュア接続プロセス

本システムは MHPS エンジにてさらに複数のお客様工場にて実証試験を実施している。実証試験を経て，2020 年度にサービス開始を行う予定である。

5. まとめ

本報では，当社が開発した，NAT トラバーサルと独自の暗号化技術を組み合わせたセキュア通信を用いた遠隔監視システムについて紹介した。

NAT トラバーサルと独自の暗号化技術を組み合わせたセキュア通信を用いることで，従来のエッジコンピュータで課題となっていた，データ共有方法などを解決することが可能となり，幅広くお客様に遠隔監視サービスを提供することができるようになる。

開発したシステムは，MHPS エンジにて計画中の遠隔監視サービスに適用し，その有効性を検証した。今後は，他のプラントにも展開を図っていくとともに，さらに顧客価値向上に寄与できる機能開発を行っていく。

本システムを開発するにあたり，remot3.it 社には技術的な支援をいただきました。ここに感謝の意を表します。

参考文献

(1) remot3.it ホームページ https://remote.it/