セキュリティ通信プロトコルを使用する Edgecross システムの研究

［研究代表者］内藤克浩（情報科学部情報科学科）
［共同研究者］中條直也（情報科学部情報科学科）
水野忠則（情報科学部情報科学科）
梶　克彦（情報科学部情報科学科）
大谷治之（三菱電機(株)）

研究成果の概要

産業界では製造現場における装置稼働状況のリアルタイム把握など、生産性向上手段を模索する試みが続けられている。製造現場で利用される FA (Factory Automation)機器も同様の流れに基づいて様々な提案が行われている。具体的には、FA と情報技術との協調を実現するオープンなエッジコンピューティング領域のソフトウェアプラットフォームとして、Edgecross が日本初の技術として提案されており、Edgecross を導入することにより、各工場の FA 機器の稼働状態をリアルタイムに集約することが可能となるため、生産現場の効率向上手段として着目されている。一方、多数の生産拠点が存在する場合、生産現場間をセキュアに接続する技術も必要となる。現状は専用線サービスなど高価なサービスを利用することが多いが、本研究では一般的なインターネット回線を用いたセキュリティ通信技術の確立を目指す。

本研究では、今まで検討を進めてきたシステムを拡張することにより、FA 機器の管理で利用されているシステム構成に影響を与えないセキュリティ通信プロトコルの設計を行う。拡張システムでは、Boarder Bridge と呼ばれるセキュリティ通信プロトコル機能をエッジサーバーに提供可能な外付けデバイスを新たに設計することにより、容易に既存のエッジサーバーに新たな機能を実装する手段を設計する。拡張システムを利用することにより、FA 機器を工場内などで管理するエッジサーバー間をセキュアに接続可能となり、工場内外からのセキュリティアタックに対する耐性が大幅に向上することが期待される。

研究分野：モバイルネットワーク

キーワード：Factory Automation, Internet of Things, Secure communication, end-to-end communication

1. 研究開始当初の背景

通信技術と半導体技術の発展にともない、IoT(Internet of Things)と呼ばれるネットワークに接続されるデバイスを用いたサービスが注目されている。産業界においても、IoT への注目は高く、製造現場における装置稼働状況のリアルタイム把握など、生産性向上手段として多数の企業がサービスを開始しつつある。製造現場で利用される FA (Factory Automation)機器も同様の流れに基づいて様々な提案が行われている。具体的には、FA と情報技術との協調を実現するオープンなエッジコンピューティング領域のソフトウェアプラットフォームとして、Edgecross が日本初の技術として提案されており、多数の会社　が参画するコンソーシアムが運営されている。Edgecross を導入することにより、各工場の FA 機器の稼働状態をリアルタイムに集約することが可能となるため、生産現場の効率向上手段として着目されている。一方、多数の生産拠点が存在する場合、生産現場間をセキュアに接続する技術も必要となる。現状は専用線サービスなど高価な

サービスを利用することが多いが、本研究では一般的なインターネット回線を用いたセキュリティ通信技術の確立を目指す。

2. 研究の目的

本研究では、Edgecross の主要メンバーである三菱電機との共同研究として、Edgecross におけるセキュリティ通信プロトコルの設計を目的とする。Edgecross 向けのセキュリティ通信プロトコルでは、今まで検討を進めてきたシステムを拡張することを想定する。開発してきたシステムは、端末管理を行うクラウドサービスと通信処理を行う端末機能により構成されており、一般的なインターネット接続機器を想定したシステムである。本研究では、開発してきたシステムを拡張することにより、FA 機器の管理で利用されているシステム構成に影響を与えないセキュリティ通信プロトコルの設計を行う。拡張システムを利用することにより、FA 機器を工場内などで管理するエッジサーバー間をセキュアに接続可能となり、工場内外からのセキュリティアタックに対する耐性が大幅に向上することが期待される。FA 機器が攻撃された場合、生産設備の一時停止だけではなく、停止に伴う不良製品の発生など、被害は甚大になることが予想される。本研究課題は、今後の IoT を活用する生産現場におけるセキュリティ担保技術になり得るものであり、研究成果の波及効果は大きいものと考える。

3. 研究の方法

(1) Edgecross の通信手法調査

Edgecross の通信は、FA 機器との通信と Edgecross サービス間の通信に大別され、前者は FA 機器で利用されている様々な規格を想定したものである。一般に FA 機器では、高速・低遅延・高信頼性などの特殊な要求があるため、一般的な PC などが利用するネットワーク技術とは異なるものが利用されている。また、閉域網を想定していることから、暗号化などの処理遅延につながる技術はあえて利用していないことも多い。一方、後者は Edgecross のサービスが汎用 PC を用いて実現されていることから、一般的な IP(Internet Protocol)を用いた通信を利用している。

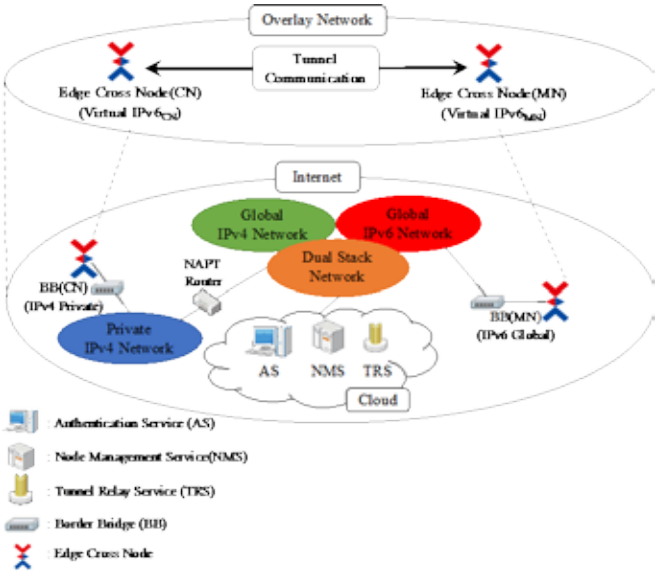

図 1　通信システム概要

(2)セキュリティ通信プロトコルの設計

本研究では、検討を進めてきた通信システムが IP を想定していることから、IP を用いた Edgecross サービスのセキュリティ通信を検討する。図 1 は提案する通信システムの概要を示し、提案システムはシステム全体を管理するクラウド群と、Edgecross サービスにセキュリティ通信を提供する Boarder Bridge(BB)により構成される。Edgecross サービスが動くサーバーは一般的な IP ネットワークを利用しているが、セキュリティ通信のプロトコルを新たに実装するには、既存サービスへの影響の可否なども判断する必要があり、導入は容易ではないと考えられる。一方、特定のネットワークインタフェースを追加することは、既存サービスへの影響はほぼないと考えられることから、提案手法では、追加するネットワークインタフェースに対してセキュリティ通信を提供する BB と呼ばれる機器を追加する。BB はクラウド群と連携することにより、異なる BB 間のセキュリティ通信経路の確立を行う。Edgecross サービスからのデータは、接続されている BB を経由することにより、遠方の BB に到着する。また、取り出されたデータは Edgecross サービスに送信され、セキュアな相互通信を実現可能となる。

4. 研究成果

図 2 に本研究において提案するセキュリティ通信のプロトコル手順を示す。提案プロトコルでは、既存の Edgecross サーバーのネットワーク機能に変更を加えることを防ぐために、セキュリティ通信に関する処理を BB において実施する。一方、通信開始などの制御は Edgecross サーバー上のアプリケーションから実施できるように設計した。提案プロトコルでは、BB が接続されるネットワーク情報をクラウド群に通知するための登録作業が必要となる。その後、通信を実際に行う際には、通信相手の Edgecross サーバーを管理する BB までの通信経路の確立を行うことにより、2 台の Edgecross サーバーのセキュリティ通信を実現する。詳細な通信手順を以下に示す。

1. Edgecross サーバーは BB に対してサービス開始要求を行う。
2. BB は接続ネットワークの情報をクラウドサービスの NMS 機能に通知することにより、接続を受け入れるためのネットワーク情報を登録する。
3. Edgecross サーバーは BB に対して、通信対象の端末にむけた通信開始要求を行う。
4. BB は NMS に問い合わせることにより、通信対象端末へのセキュリティ通信路の確立を依頼する。
5. NMS は通信対象端末と通信開始端末のネットワーク情報を確認することにより、適切な通信手段を通信対象端末に通知する。
6. 通信対象端末の BB はセキュリティ通信路の確立に同意する旨の確認応答を NMS に返信する。
7. NMS は通信開始端末側の BB に対して、セキュリティ通信路の確立方法を通知する。
8. 通信開始端末側の BB は通信対象端末の BB に向けたセキュリティ通信路の構築を開始する。
9. 通信対象端末の BB はセキュリティ通信路の確立に対する応答を行う。
10. 通信開始端末側の BB はセキュリティ通信路の確立が終了したことを通信開始側の Edgecorss サーバーに通知する。

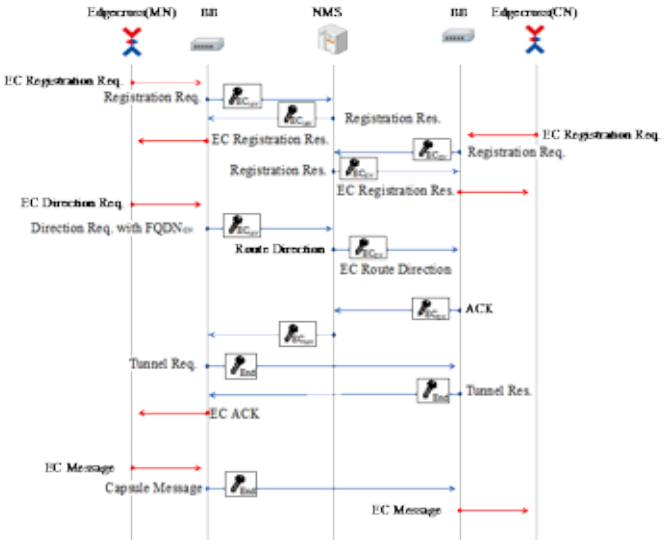

図 2 セキュリティ通信のプロトコル手順

11. 通信開始端末側の Edgecross サーバーからのメッセージは、BB において暗号化処理が行われた上で、通信対象端末側の BB に送信される。通信対象端末側の BB は、届いた暗号化されたメッセージを復号することにより、Edgecross サーバー間の通信を実現する。

5. 本研究に関する発表

(1) Shuhei Isomura, Takahiro Nimura, Katsuhiro Naito, “Design of end-to-end connection technology of microcomputer equipment using overlay network,” KES-IIMSS-19, June 2019.

(2) Katsuhiro Naito, Kohei Tanaka, Naoki Yamamoto, Ryota Murate, Hiroto Mori, Ayumu Kurata, Kensuke Tanaka, “Development of Management Cloud Software for Overlay Network,” WMSCI 2019, July 2019.