8 IoTセキュリティ

# Industrial IoTセキュリティの取り組み

NTT コミュニケーションズ（以下、NTT Com）は、長年培ったネットワーク監視運用技術や IT システム分野におけるセキュリティ脅威管理技術を活用・拡大し、Industrial IoT（以下、IIoT）における統合脅威管理技術の開発を進めている。本稿では、その背景・取り組みを紹介する。

NTT コミュニケーションズ株式会社
技術開発部
【左から】担当課長　**加島 伸悟**氏
主査　**野村 啓仁**氏

## Industrial IoT のセキュリティ課題

IIoT は、工場やプラントなど産業システムにおける IoT であり、製造業の革新の手段として大きな注目を浴びている。

従来は内部に閉じていた産業システムが、外部に繋がることでセキュリティが大きな課題となる。日本では、2017 年にマルウェア Wannacry によって、自動車製造工場が生産停止に追い込まれる事例が発生している。従来、産業システムは「外部 NW に繋がっていない」ことを理由にサイバーセキュリティを意識していなかったが、通信の IP 化や複数拠点間のデータ収集・分析のように、通信範囲が拡大することで、セキュリティ対策の重要度が増している。

IIoT システムには、資産管理台帳の更新が行われない、システム更改周期が非常に長い、通信プロトコルが産業分野・企業独自であるなど IT システムとは異なる特徴がある。これらの特徴を踏まえたセキュリティ対策が求められるが、必要なセキュリティレベルは産業分野やお客さま環境ごとに大きく異なる。さらに、お客さまによってはデータをクラウドに持ち出して処理することに大きな抵抗がある。また、システムに負荷を与える検査方法に対しては可用性低下への懸念からに抵抗感がある。そのため、従来の IT 向けセキュリティ製品や SOC サービスでは対応が難しい。

## IIoT 統合脅威管理技術

IIoT のセキュリティ課題解決に向けて、NTT Com は、NTT セキュアプラットフォーム研究所と連携し、セキュリティ機能をマイクロエッジサービスとして提供する IIoT 統合脅威管理技術の開発を行っている。本技術は、データの保管・処理をクラウドではなく、お客さまの工場やプラント内に設置したエッジサーバの上で行い、お客様環境に適合するセキュリティ機能を選択し、脅威管理サービスとして提供する。

IIoT 統合脅威管理技術は、資産管理を中心として、脆弱性診断、脅威検知等のさまざまなサービスを搭載可能である（表 1 参照）。例えば、検査による可用性低下に懸念のあるお客さま環境に対しては、検査パケットを送出しない方式による脆弱性診断サービスを導入する、Modbus/TCP のような産業プロトコル利用環境に対しては各プロトコルに対応した脅威検知サービスを導入するなどのユースケースが想定される。

今後はフィールド実証を通じて技術確立やビジネス展開を図っていく。

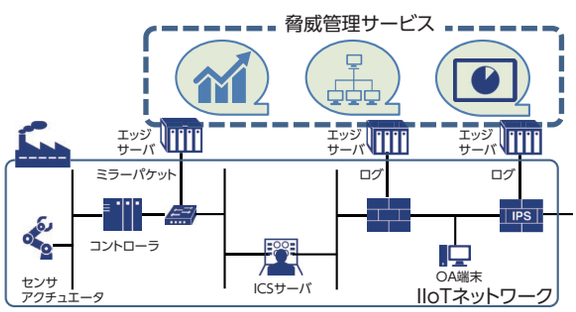


図 1　工場への IIoT 統合脅威管理サービスの適用イメージ

| 分類 | 脅威管理サービス |
|---|---|
| 資産管理 | ✓ 機器発見（検査パケット有）<br>✓ 機器発見（検査パケット無）<br>✓ 機器構成可視化 |
| 脆弱性診断 | ✓ OS・ファームウェア可視化（検査パケット有）<br>✓ OS・ファームウェア可視化（検査パケット無） |
| 脅威検知 | ✓ コンフィグレーション変更検知<br>✓ シグニチャ検知（ITプロトコル）<br>✓ ベースライン検知（IT・産業プロトコル）<br>✓ AI検知（非公開プロトコル） |

表 1　脅威管理サービスの例