多様な既存システムに後付け可能なIoTセキュリティ監視の実現


日本電信電話株式会社 NTTセキュアプラットフォーム研究所
青柳 真紀子（あおやぎ まきこ）


日本電信電話株式会社 NTTセキュアプラットフォーム研究所
南 拓也（みなみ たくや）


三菱電機株式会社 コミュニケーション・ネットワーク製作所
佐藤 浩司（さとう こうじ）


三菱電機株式会社 情報技術総合研究所
平井 博昭（ひらい ひろあき）

1. はじめに

IoT（Internet of Things）は、近年その需要とビジネスの成長性で注目されている分野のひとつである。世界のIoT機器数の動向では、2022年には350億台にも到達するとみられている[1]。特に高成長が予測されているのは、スマート工場やスマートシティが拡大する「産業用途（工場、インフラ、物流）」、スマート家電やIoT化された電子機器が増加する「コンシューマ」などの分野である。

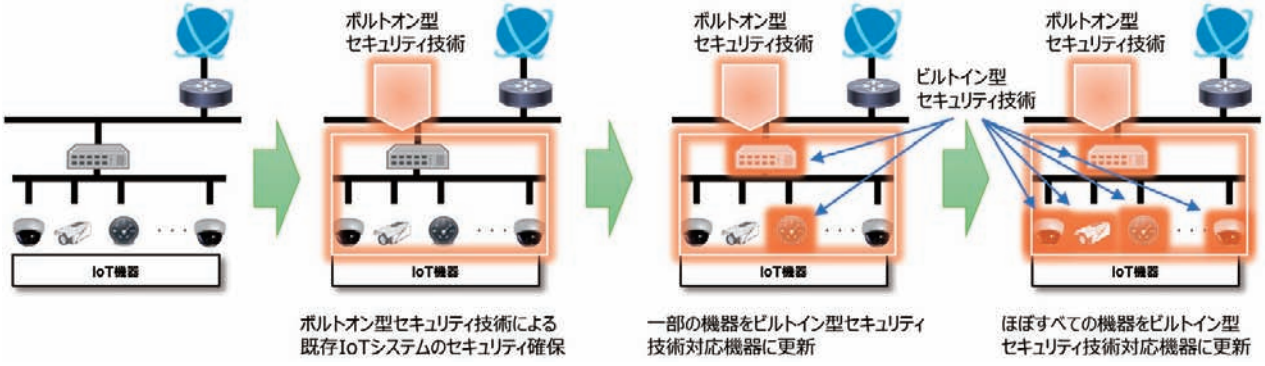
従来、情報通信機器に対するサイバーリスクとしては情報漏洩やなりすましなどの脅威が一般的に知られているが、IoT機器が攻撃対象となることによって新たな危険性が生まれることになる。例えば、ウクライナでは2015年と2016年に、電力システムを狙ったサイバー攻撃により大規模停電が発生した。電力会社のオペレータが利用するPCがマルウェアに感染したことにより変電所システムの一部制御システムが停止し、20万人以上の世帯が停電被害を受けた。電力網がデジタル化され、ITシステムによって制御されるようになったことが被害を拡大させた遠因とされている。このように、IoT機器への攻撃により、従来の脅威に加え物理的な安全性をも脅かされるという脅威に発展している。特にこれまでの標的と比較して、攻撃成功時の物理被害が大きいことから、先の例のように重要インフラを狙ったサイバー攻撃が世界中で増加している。

このような事例を受け、IoTセキュリティ対策に関しては、総務省・経産省が「IoTセキュリティガイドライン[2]」を公開している。当該ガイドラインでは、IoT機器特有のリスクとして、ライフサイクルが長い、危機に対する監視が行き届きにくい、機能・性能が限られる、など6つのリスクを挙げている。攻撃の容易性、攻撃成功時の影響力の大きさなどから、サイバー攻撃のメインターゲットは今後もますますIoT機器にシフトしていくと考えられる。実際、NICTERプロジェクト[3]のレポートでは、IoT機器を狙ったマルウェアの増加が観測されている。

重要インフラ等のサービスを支える設備やネットワークには、高度なセキュリティ対策機能を搭載できる制御・通信機器以外に、性能・運用・ビジネス性等の問題から同様のセキュリティ対策を施せない「弱い機器」や長時間稼働し続けている「古い機器」が存在し得る。このような強弱機器や新旧機器が混在する大規模ネットワークにおいてセキュリティを確保するためには、機器の健全性を確認する技術が不可欠となるため、機器の健全性確認を効果的かつ効率的に行える技術の確立が必要である。

2. IoTセキュリティ対策のあるべき姿

IoTシステム向けのセキュリティ技術としては、以下の2種類に分類できる。すなわち、セキュリティが確保されていな



■図1. IoTシステムへのセキュリティ技術導入シナリオ

い既存のIoTシステムに後から追加できるセキュリティ技術と、新設されるIoTシステムのセキュリティを確保すべくIoT機器やIoTシステムに最初から組み込まれるセキュリティ技術である。ここでは前者の後付け可能な技術をボルトオン型技術、後者の組み込み技術をビルトイン型技術と呼ぶ。

重要インフラ事業を含め、幅広い事業分野でIoT技術の活用が進んでいる現状を踏まえると、図1に示すように、これらの既存システムのセキュリティを早急にボルトオン型技術で確保しつつ、徐々にビルトイン型技術を浸透させていく、というシナリオが効果的である。

このため、筆者らはボルトオン型技術の確立が喫緊の課題であると位置付け、この課題解決に向けて、ボルトオン型のIoTシステム向けセキュリティ技術で必要とされる要求条件を以下のように定義した。

(a) 多様なIoT機器に対応できること
(b) 多数のIoT機器に対応できること
(c) 既存IoT機器を変更せず後付けできること
(d) 既知の攻撃に加え、未知の攻撃にも対応できること
(e) 自動化等により運用の手間を極力軽減できること

上記要求条件の内、(c) (d) を実現できる方式として、ネットワーク異常検知を選択した。ネットワーク異常検知は、正常な通信を定義した上で、そこから外れる通信を異常として検知するため、未知の攻撃によって生じる通信を検知できる。また、ネットワークを流れるパケットを入力として異常を検知するため、既存のIoT機器には何ら変更を加えずに、IoTシステムに後付けすることができる。

以下、IoTシステムを対象としたネットワーク異常検知を実現するIoT動作監視・解析技術の特長と、導入例について説明する。

3. IoT動作監視・解析技術

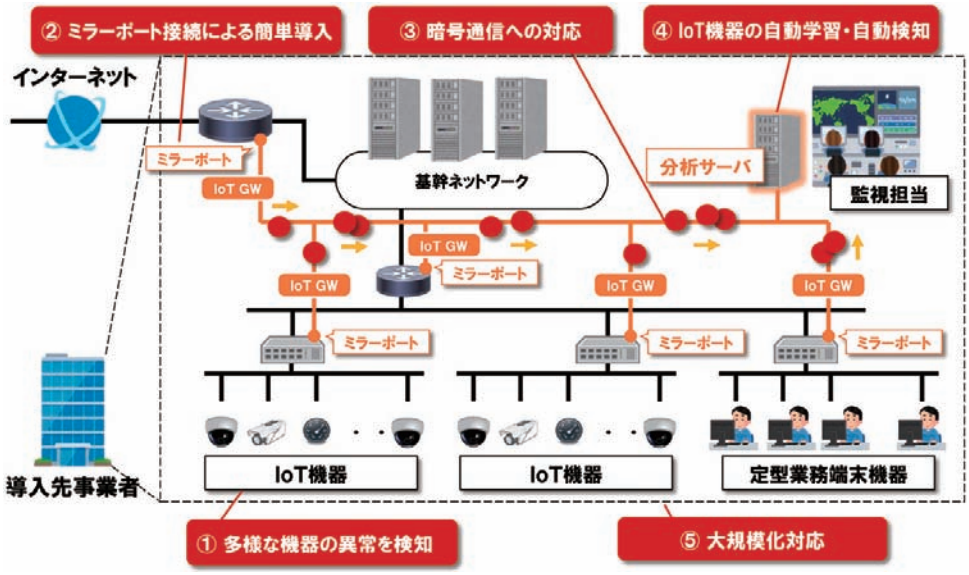
図2に開発したIoT動作監視・解析技術の構成例と特長を示す。IoT動作監視・解析技術は、前章で述べた要求条件を満足すべく、次の特長を持つ。

①多様な機器の異常を検知 (要求条件 (a) (d))
②ミラーポート接続による簡単導入 (要求条件 (c))
③暗号通信への対応 (要求条件 (a))
④IoT機器の自動学習・自動監視 (要求条件 (e))
⑤大規模化対応 (要求条件 (b) (e))

本技術では、ネットワークを観測する装置として、アプリケーションを追加搭載可能なIoT向けゲートウェイ装置 (以下、IoT GW) を用い、IoT GWで収集・加工した情報に基づいて異常を検知する分析サーバと組み合わせてシステムを構成する。以下、本技術の特長について説明する。

3.1 多様な機器の異常を検知

IoT機器の多種多様性から、その1つずつを定義することは難しく、IoT機器の台数が増えればそれはより困難を極める。さらに、同じIoT機器でもシステムごとに通信の挙動は異なるため、あらかじめ正常状態を定義することは難しい。そこで筆者らは機械学習によるアプローチで検討を行った。IoT GWが対象機器の情報を収集し、対象機器ごとに正常な通信挙動を学習した上で、学習した正常パター



■図2. IoT動作監視・解析技術の構成例と特長

ンとのズレを分析することにより異常を検知する。IoT機器は、種類や用途が決まれば正常状態の傾向がつかみやすいことに着目し、特徴量の自動抽出によって未知の機器への対応も可能である。

未知のサイバー攻撃によるあらゆる異常状態を事前学習することは不可能だが、教師なし学習を活用することにより、未知の攻撃に対しても有効な異常検知手法を確立した。

3.2　ミラーポート接続による簡単導入

ネットワーク異常検知を実現するためには、ネットワークを流れるパケットを観測する必要がある。ボルトオン型技術として実現するという観点では、既存システム内のレイヤ2スイッチ機器に設定したミラーポートからパケットのコピーを取得して動作する形が最も適している。このため、開発したIoT動作監視・解析技術では、ミラーポートを設定し、IoT GWを接続するだけで、既存システムへ簡単に導入できるしくみとした。

ボルトオン型技術が既存システムへの導入を容易にする一方、ビルトイン型技術は新規システムの構築を容易にする。例えば、システムを構成する通信機器内でネットワーク異常検知のための観測も行ってしまうことで、通信装置と観測装置の2つを用意する必要がなくなり、システムの構築は容易となる。このため、IoT GWには、パケットを転送しながら観測するビルトイン型技術も搭載し、既存システムと新規システムの両方に効果的に適用できるものとした。

3.3　暗号通信への対応

開発したIoT動作監視・解析技術では、観測したパケット内の一部の情報のみを抽出して、監視を行うことができる。具体的には、レイヤ2/3/4のヘッダ情報のみを使って特徴量を生成し、この特徴量から各機器の通信挙動を学習し、異常を検知することができる。これらのヘッダ情報は、パケット転送等に必要な情報であり、暗号通信においても暗号化されない領域である。つまり、本技術は、暗号通信と平文通信の両方において、共通的に観測できる情報のみを用いているため、暗号通信にもそのまま適用することができる。

また、ヘッダ情報のみを使う方式であるため、ペイロードデータは、ミラーポートに接続されたIoT GW内で直ちに廃棄され、ヘッダ情報に基づいて生成された特徴量のみが観測用の装置から解析用の装置に送信される。このため、機微なデータを扱うネットワークにも適用しやすいという利点や、IoT GWと分析サーバの間の通信量を低く抑えられるため、分析サーバを遠隔に設置するといった構成にも柔軟に対応できるという利点を持つ。

3.4　IoT機器の自動学習・自動監視

IoTシステムは、ITシステムと比較して大規模かつ構成が変化しやすいと想定されるため、IoTネットワークに接続されるIoT機器を自動的に検出し、監視対象として自動設定されることが望ましい。そこで、IoT GW構成技術により、IoTシステムに新規に接続されたIoT機器について分析サーバへの登録から、初期学習・監視実施からなる一連のプロセスの自動化を実現した。

また、本方式ではIoT機器の台数が増加するとIoT GWに対して求められる処理性能が増大するが、ソフトウェアとハードウェアによる連携動作によって必要な処理性能を確保する技術により、実用化システムの運用に耐え得る処理性能を実現することを確認した。

3.5　大規模化対応

重要インフラ事業者においてはIoTシステムの大規模化が想定される一方で、中小規模の事業者に対しても本技術の展開を図る際には、事業者ごとに異なる多様なIoT機器や設備構成への対応が必要となる。そのため、大規模化に伴い増加する対象システムの構成変更への自動追従を可能とするとともに、本技術のソフトウェアアーキテクチャを対象システムの規模拡大に応じて機動的にスケールアウト可能な構成に進化させた。

IoTシステムの構成変更に対する自動追従については、監視中のIoTシステムにおいてIoT機器の交換や収容位置変更などが発生した場合に構成変更として検出し、必要となる対応（対象IoT機器の学習モデル再利用・再構築等）を監視担当者にリコメンドすることが可能となった。本手法により、手動での対応を必要とした従来技術と比較して人為的ミスの発生を低減することが可能となり、監視業務の継続が容易となる。

さらに、機動的なスケールアウト機能により、IoTシステムの規模変化に応じて分析サーバの増減及び各構成機能に対するリソースの動的割当てを可能とした。監視対象とするIoT機器の通信トラフィック量等の特性に依存するものの、一般的なIoT機器を対象とする場合、設計上は数千台規模のIoTシステムに対して数台～十数台程度の物理サーバによって分析サービスを構成可能である。

4. IoT動作監視・解析技術の導入例

機械学習により監視対象機器の通信挙動を把握する方式は、定型的な通信が発生するシステムに対する監視に適している。

例えば、監視カメラからの映像がほぼ一定のパケットサイズ、パケット間隔で送信されるようなIoTシステムにおいては、通信の正常な振る舞いを的確に捉えやすい。一方、定型業務端末を含むOTシステムにおける通信は、定型業務とはいえ、オペレータ操作によって通信のタイミングが決まるなど、監視カメラシステムにおける通信に比べて、挙動のばらつきが大きいため、機械学習を用いた通信挙動の正確な把握は難易度が高いといえる。

筆者らが開発したIoT動作監視・解析技術は、機械学習の活用によって、監視カメラのようなIoTシステムに加えて、オペレータ操作がない定型業務端末を含むシステムや、オペレータが操作する定型業務端末を含むシステムにおいても、システム内の監視対象機器の通信挙動を把握することに成功している。

一例として、IoT機器に加え、オペレータ操作が少ない定型業務端末が多数含まれる工場内ネットワークへの適用事例を紹介する。

4.1　工場内ネットワーク監視の例

図3に工場内ネットワークにおける本技術の適用例を示す。この事例では、生産状況を把握するためのデータが生産ラインの各種機器からサーバPCに送信されるネットワークを本技術により監視した。100台規模の機器が通信する環境に対して、IoT GW1台を適用した。

ネットワークスイッチにミラーポートを設定し、IoT GWを接続した上で、IoT GWと分析サーバを接続するだけで既存工場システムへのボルトオン導入ができるとともに、工場内で流れる機微なデータを取り込まないことや、暗号通信に対応できること、生産ラインの停止・再開、生産品の変更に伴う機器の入れ替えに対しても、自動で監視を継続できることなど、本技術の特長の有効性を実環境で確認できた。また、設定誤りによる機器の挙動変化も検出できた。

5. おわりに

本稿では、多様な既存システムに後付け可能なIoTセキュリティ監視機能を提供するIoT動作監視・解析技術について紹介した。本技術ではIoTネットワークを構成するIoT機器等のトラフィックや状態を組み合わせた動作異常解析が可能であり、工場をはじめとする複数分野の事業者環境での実証評価により、その有効性を確認した。

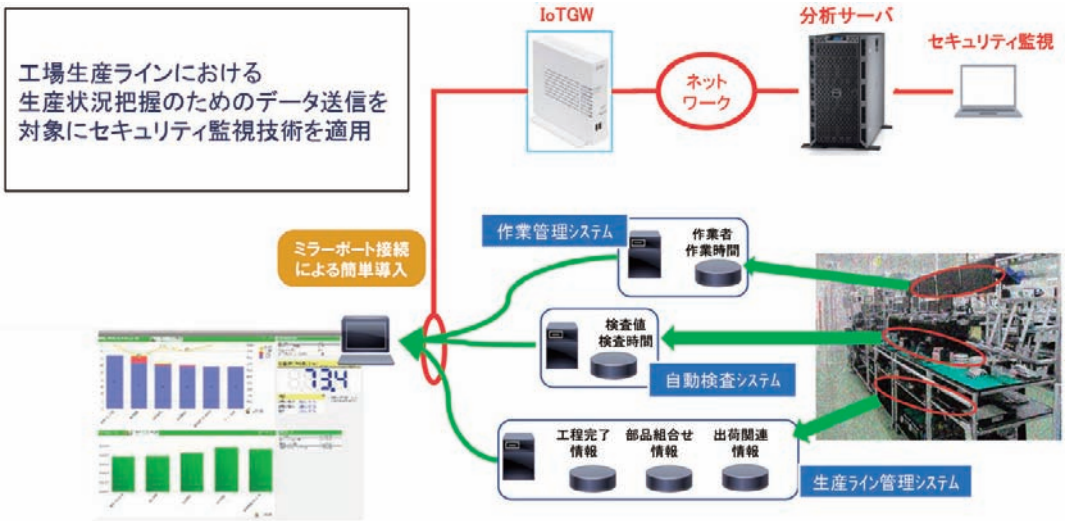
今後の取組みとして、より安全にIoT技術を活用できる社会を実現するために社会実装を継続して行っていく。また、Society5.0の実現に向けてサイバー・フィジカルシステムの特性に対応するより高度な異常検知技術の実現を目指し、より高度な技術の開発を行っていく予定である。

謝辞

本研究の一部は、内閣府が進める戦略的イノベーション創造プログラム（SIP）「重要インフラ等におけるサイバーセキュリティの確保」（管理法人：NEDO）によって実施されました。

参考文献

［1］令和2年版情報通信白書，総務省
［2］IoTセキュリティガイドライン，総務省・経産省，2016年
［3］https://www.nicter.jp/，NICTERプロジェクト，NICTサイバーセキュリティ研究室



■図3．工場内ネットワーク監視の例