IoTセキュリティ
IoTシステムのセキュリティ課題と解決アプローチ

田中 晋輔 Tanaka Shinsuke
藤嶋 堅三郎 Fujishima Kenzaburo
三村 和 Mimura Nodoka
大橋 哲也 Oohashi Tetsuya
田中 真愉子 Tanaka Mayuko

IoTは，あらゆるモノをネットワークに接続し，データを集め分析することで，新たな顧客価値創出への貢献が期待されている。人々の生活や経済活動に影響を及ぼす重要インフラもIoTの適用領域となるため，IoTシステムへのセキュリティ対策は重要度が高い。一方，つながるモノの数が飛躍的に増加することで，影響範囲の拡大や攻撃の長期化など技術面の課題に加え，セキュリティ運用管理者の不足といった問題も生じる。
本稿では，重要インフラ向けIoTセキュリティの要件として重要視される「可用性」に着目し，可用性確保のために問題検知から暫定対策までを迅速に進めるアプローチ，および日立が開発した高感度かつ誤検知の少ない検知技術について紹介する。

1. はじめに

近年，IoT（Internet of Things）の普及に伴い，ネットワークにつながるモノの数が飛躍的に増加している。つながるモノの対象は，情報機器のみならず，自動車や医療機器など人命に関わるもの，さらには発電所や核関連施設のように社会に甚大な影響を及ぼす可能性のあるものなど，多様性が増している。

あらゆるモノがネットワークでつながることで，例えばあるモノがマルウェアに感染すると，そこを起点に他のモノにも感染が拡散し，最終的には本来守られるべき重要インフラまでが脅威にさらされる。実際，過去のセキュリティインシデント事例を見てみると，重要インフラにつながった作業用PCや監視カメラなどの通信ソフトウェアの脆（ぜい）弱性を狙って外部から不正にアクセスし，そこを起点に重要インフラを異常動作させるといった事例が発生している[1)]。

本稿では，IoTを導入した際のセキュリティ課題と，その課題解決に向けたアプローチについて述べる。

2. IoTシステムの特徴およびセキュリティ上の課題

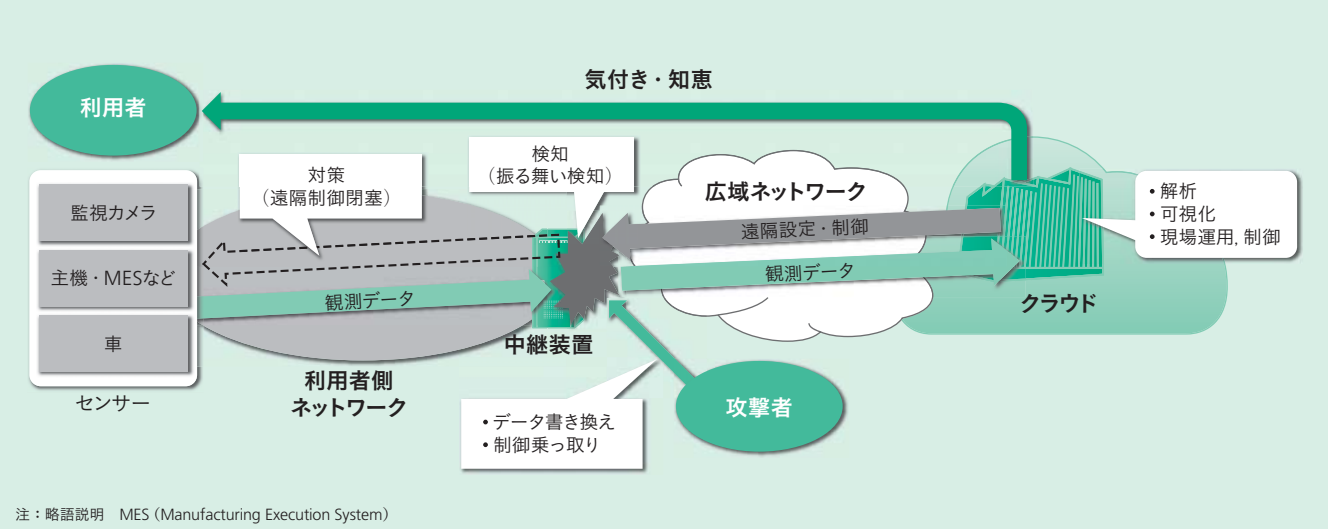
従来，通信とは無縁であったモノをネットワークへ接続するIoTシステムは，これまで見えなかった事象を見えるようにして新たな気付きを得たり，モノから集めたデータを解析して新たな知恵を得ることで，コスト低減や売り上げ拡大などの効率向上が期待されている。その一方で，IoT時代の新たなセキュリティ上の脅威について，産学官連携プログラムであるIoT推進コンソーシアムでは，(1) ネットワークに接続するIoT機器の増加，(2) ライフサイクルの長さ，(3) 人手による監視の行き届きにくさという3点への対策の必要性を提唱している[2)]。

1点目の課題に対しては，IoT機器の増加に伴う攻撃対象の増加および影響範囲の拡大が指摘されている。2点目および3点目の課題に対しては，人の関与の少なさから管理者不在の状態に陥りやすく，そのため攻撃の検知が難しくなり，さらに10年以上という長期ライフサイクルに伴う攻撃の長時間持続が指摘されている。これらの課題解決に向け，日立が考えるアプローチを以下に述べる。

3. 課題解決へのアプローチ

ネットワークに接続するIoT機器の増加に対しては，センサーとクラウドの間に中継装置を設置し，大量のセンサー情報を中継装置で集約する階層化アーキテクチャを導入する（図1参照）。中継装置は，顧客システムによって，ゲートウェイ，スイッチ，ルータなど，さまざまな形態が考えられる。

ライフサイクルの長さ，人手による監視の行き届きにく



注：略語説明　MES（Manufacturing Execution System）

図1｜IoTシステム階層化アーキテクチャ

センサーとクラウドの間に中継装置を設置し，センサー情報を中継装置で集約する。センサーの異常は中継装置で検知する。

さに対しては，問題発生を即時検知することと，システム稼働を継続しつつ被害拡大を防止するための暫定対策を速やかに行うことの2点が重要となる。

3.1　即時検知の重要性

即時検知の重要性について，IoTセキュリティ被害額算出モデルを用いた解説を**図2**に示す。

セキュリティ被害には，(1) インシデント発生に直接起因する一次的被害，すなわちインシデントに対処するための人件費や設備修繕費，設備停止による逸失利益などの直接的被害と，(2) 被害拡大に伴い発生する二次的被害，すなわち損害賠償，風評被害，信用度低下などの間接的被害がある。

IoTシステムでは，IT（Information Technology）システムと異なり，インシデント発生からその発覚までに数か月を要することもある。インシデント発生後，まず一次的被害が増加し始める。その後，t_1でインシデントが発覚し，原因究明後にt_2で暫定対策を行い，やがてt_3で復旧する。二次的被害はt_2で暫定対策を行った後もしばらくは増加し続ける。そこで，問題検知および暫定対策をt_1の自然発覚よりも早いT_1のタイミングで行うことができれば，被害額をd_2からd_1まで抑えることができる。即時検知に関する技術的な説明は次章で述べる。

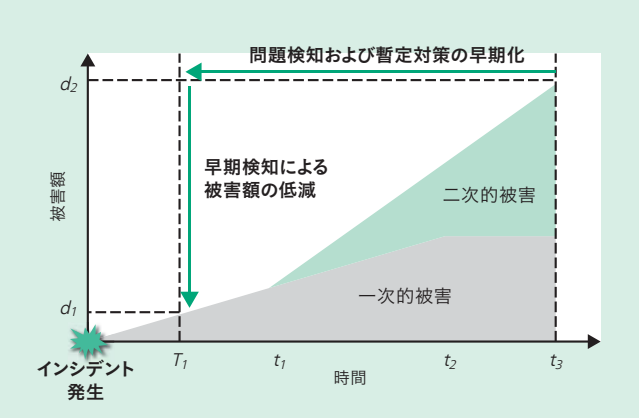


図2｜IoTセキュリティ被害額算出モデル

IoTセキュリティ被害額は，インシデント発生に直接起因する一次的被害と，被害拡大に伴い発生する二次的被害から成る。問題検知および暫定対策をT_1のタイミングで行うことで被害額の抑制が可能となる。

3.2　暫定対策の要件

問題検知の後は，速やかな暫定対策が必要になる。暫定対策の手段には，インシデント発生箇所の分離，攻撃からの防御，被害の緩和がある。重要インフラの場合，ITシステムとは異なり，インシデントが発生してもシステムを停止させることが困難な場合が多い。そのため，インシデントへの対処は，システム全体の可用性を最優先したうえで行う。

また，対処を行う際は，IoTを適用する顧客システム，すなわち製造ラインや電力システムなどの業務知識も必要となる。つまり，同じ攻撃が発生した場合でも，異なるシステムに対して同一の対処策が適用できるわけではなく，顧客システムの動作を熟知したうえでのカスタマイズが必要となる。

3.3　問題検知から暫定対策までの流れ

重要インフラの可用性確保のため，早期の問題検知と迅速な暫定対策を行う方法を整理する。

すでに対策手法が確立されている既知の問題については，問題検知から暫定対策までを自動化することで速やかに対処を行い，可用性を確保することができる。

しかし，未知の問題は対策手法が確立されておらず，ロ

グ解析などによる原因究明，原因解消のための対策立案，ならびに立案した対策の実効性検証が必要となるため，問題検知から暫定対策までに時間を要する。この時間を短縮するために，想定される問題について事前に対策手法の検討および効果検証を行い，暫定対策手順をマニュアルとして整備しておくことが有効である。

3.4　暫定対策の実現アプローチ

マルウェア感染などの被害拡大が予測される場合，被害拡大によるシステム全体停止という最悪の事態を回避するため，暫定対策は問題が発生した箇所のみを一時的にシステムから切り離すことが有効な手段の一つである。暫定対策による一時的な切り離しの範囲を最小限にするため，問題検知の分解能は,切り離しの粒度と同等以上であることが望ましい。そのうえで，システム全体を俯瞰（ふかん）的に観測し，問題発生箇所の切り離し範囲を確定する。

ラインAおよびラインBという2つの製造ラインの挙動を，カメラ監視および制御挙動監視という2つの手法で監視する場合の例を**図3**に示す。

まず，ラインAのカメラに不正プログラムが仕込まれ，ラインAに異常があると偽アラームが上がる状況を想定する。この場合，ラインAの制御そのものには異常がないため，被害拡大防止のため，切り離し点（1）でシステムを切り離す。同様に，ラインAのカメラおよび制御挙動の双方に異常が認められた場合は，ラインA自体に異常が発生していると判断し，切り離し点（2）で切り離す。

このように，状況に応じてシステムをどのように切り離すかを事前にマニュアル化しておくことで，業務知識に基づいた暫定対策が可能となる。さらに，このマニュアルに規定する暫定対策を切り離し点にプログラムなどで実装することで，暫定対策の自動化を図る。

本手法と次章で紹介する検知技術を組み合わせることで，問題検知から暫定対策までをいち早く行うことが可能となる。

4.　即時検知の技術

重要インフラのネットワークは，従来は，外部と隔離することでセキュリティを確保していた。しかし，業務革新のためにこれらネットワークは情報ネットワークと統合されるようになり，さらに近年は，IoTを活用した遠隔保守や他サービスとの連動のため，外部ネットワークとの接続も求められている（**図4**参照）。

従来のサイバーセキュリティ対策では，定義ファイルに基づきウイルスを検知するアンチウイルスソフトウエアや，既知のサイバー攻撃の特徴を示すシグネチャに基づき侵入を検知するIDS（Intrusion Detection System）が用いられてきた。これらはいずれも，既知の攻撃の検知には有効だがゼロデイ攻撃を検知できないという課題があった。

この課題を解決するため，あらかじめ正常なデータを定義しておき，そこから逸脱した場合に異常と判断するアノーマリ検知技術が重要となってきている。適切に「正常の定義」を行うためには，ネットワーク構成や顧客業務全般に精通し，かつ複雑な設定を行える運用管理者が求められる。しかし，現状はそのようなスキルを満たす人材が不足している。また，近年は，OS（Operating System）標準搭載のコマンドや，本来は攻撃用途に開発されたわけではないソフトウエアを悪用した巧妙な攻撃が増加しており，このような攻撃は正常状態との切り分けが難しい。

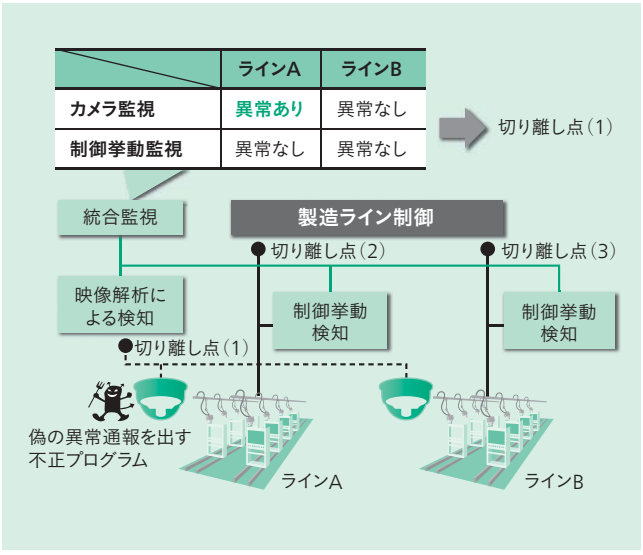


図3｜製造ラインにおける問題検知時の挙動
2つの製造ラインをカメラと制御挙動によって監視し，問題検知および切り離しを行う場合の例を示す。

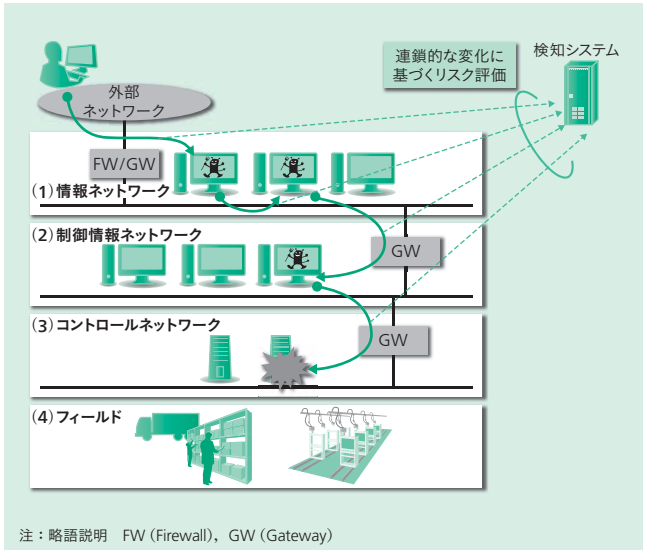


図4｜IoTバリューチェーン構成
情報ネットワークからコントロールネットワークまでを統合したうえで，外部ネットワークとも接続することで業務効率向上を図る。

そこで日立は，情報ネットワークにおいて従来は正常と見なされてきたOS標準コマンド実行などの振る舞いであっても，攻撃に悪用されうる振る舞いを高感度に検知する技術を開発した。高感度化により誤検知が増加するという懸念に対しては，サイバーキルチェーン※）によって「点（単一事象）」だけではなく，連鎖的変化に着目した「面（点間の関係や共起状態）」でリスク評価を行うことで誤検知を抑制する[3]。本技術は以下のとおり大きく3つの機能から成る。

(1) サーバやPCの内部動作監視機能

対象サーバやPC自体にインストールされる。USBメモリの挿抜やプログラムの起動などをモニタリングし，疑わしい挙動を検知する。

(2) トラフィックのアノーマリ検知機能

ネットワークを流れるトラフィックを可視化することに加え，OS標準コマンドが攻撃に使われている可能性がないか，またバックドア通信が発生していないかなど，疑わしい通信を検知する。本機能は，(1) の機能をインストールすることが困難な機器の挙動をネットワークトラフィックからモニタリングすることに有効である。

(3) サイバーキルチェーンによる評価機能

(1)，(2) で検知した疑わしい挙動および疑わしい通信から，統合的にリスクを評価する。

上記技術を用いることで，従来検知できなかった巧妙な攻撃の検知が可能となり，さらに運用管理者不足といった課題を解決できる。

5. おわりに

ここでは，IoTシステムの導入や普及に伴うセキュリティ上の課題と，課題解決のためのアプローチ，およびその要素技術となる検知技術について述べた。

日立の検知技術については，現在，国立研究開発法人新エネルギー・産業技術総合開発機構（NEDO）の委託事業「戦略的イノベーション創造プログラム（SIP：Cross-ministerial Strategic Innovation Promotion Program）／重要インフラ等におけるサイバーセキュリティの確保」にて，情報制御ネットワークやコントロールネットワークといった階層を持つネットワークへの適用など，より高度化をめざして研究・実証を行う計画であり，そこで得られた知見を製品にフィードバックする予定である。

※）標的型攻撃における「偵察（Reconnaissance）」，「武器化（Weaponization）」，「配送（Delivery）」，「エクスプロイト（Exploitation）」，「インストール（Install）」，「遠隔操作（Command & Control）」，「目的実行（Actions on Objectives）」の7つのステップを体系的にまとめた考え方。

参考文献など

1) IPAホームページ，制御システム利用者のための脆弱性対応ガイド，https://www.ipa.go.jp/files/000044733.pdf
2) IoT推進コンソーシアムホームページ，IoTセキュリティの動向について，http://www.iotac.jp/wg/security/
3) 川口，外：不審活動の端末間伝搬に着目した標的型攻撃検知方式，情報処理学会論文誌，Vol.57, No.3 (2016.3)

執筆者紹介

田中 晋輔
日立製作所 ICT事業統括本部 サービスプラットフォーム事業本部
IoT・クラウドサービス事業部 IoTビジネス本部
IoTセキュリティ推進センタ 所属
現在，IoTセキュリティソリューションの事業化活動に従事

藤嶋 堅三郎
日立製作所 研究開発グループ
情報通信イノベーションセンタ ネットワーク研究部 所属
現在，IoTセキュリティソリューションの研究開発に従事

三村 和
日立製作所 研究開発グループ
情報通信イノベーションセンタ ネットワーク研究部 所属
現在，IoTセキュリティソリューションの研究開発に従事
工学博士
電子情報通信学会会員，情報処理学会会員，IEEE会員

大橋 哲也
日立製作所 ICT事業統括本部 サービスプラットフォーム事業本部
IoT・クラウドサービス事業部 IoT開発本部
プラットフォーム第1部 所属
現在，サイバー攻撃対策技術の研究開発に従事

田中 真愉子
日立製作所 研究開発グループ
システムイノベーションセンタ セキュリティ研究部 所属
現在，サイバー攻撃対策技術の研究開発に従事