特集論文

IoT GWセキュリティ技術の実装

泉　裕作*
佐藤浩司*
平井博昭**

Implementation of Security Technology for IoT Gateway

Yusaku Izumi, Koji Sato, Hiroaki Hirai

要　旨

近年，サービス価値，生産性，保守性などの向上を図るIoT(Internet of Things)システムが多数構築されている。

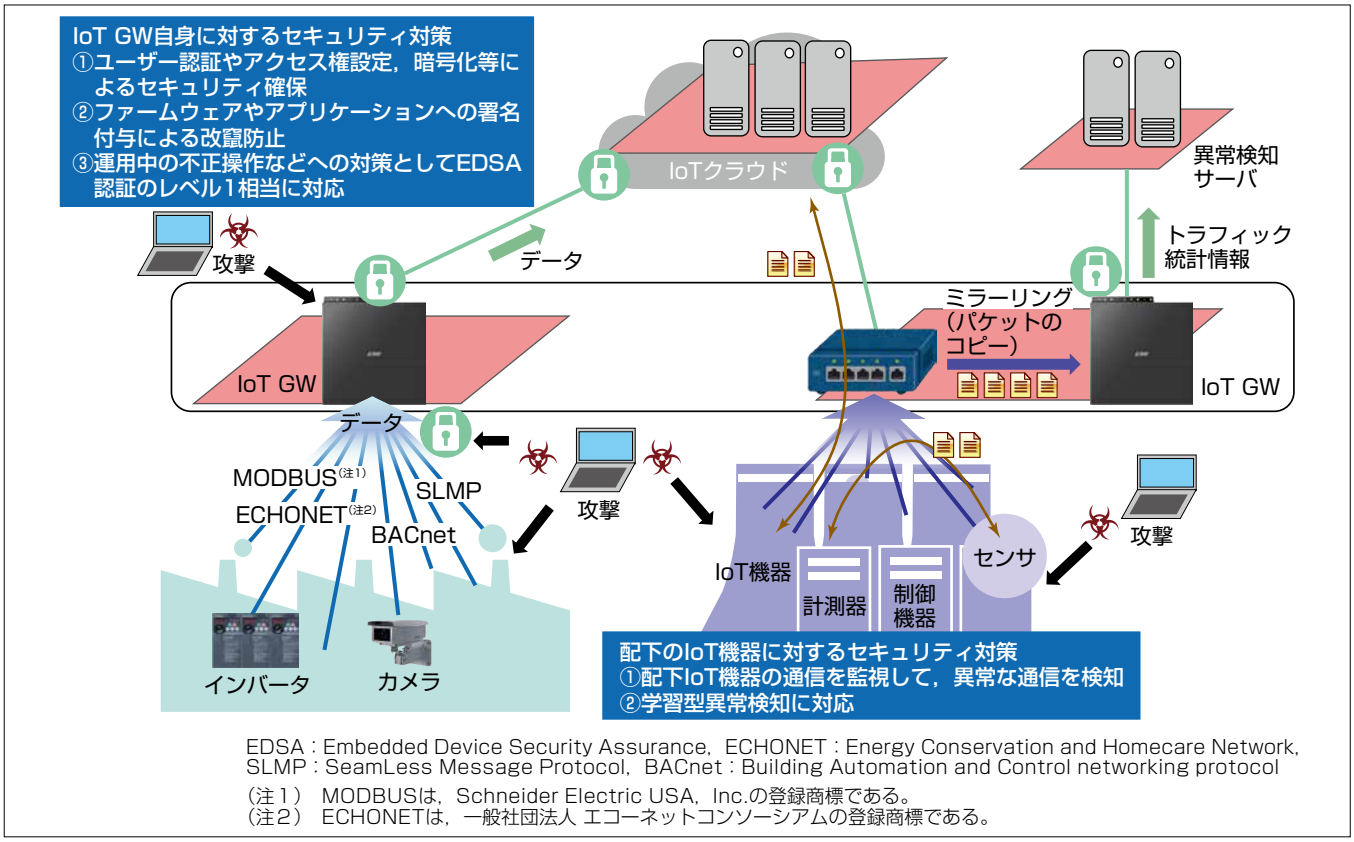
IoTシステムを構成するIoT機器は，CPUやメモリなどのリソース制約によって，十分なセキュリティ対策機能を持っていないものが多い。また，IoT機器を初期パスワードのまま運用してしまうケースも見られ，これらを背景として，IoTシステムへの攻撃事例が増えている。

次から次へと新しい攻撃手法が生み出されていく中，既に運用されている多数の脆弱(ぜいじゃく)なIoTシステムのセキュリティを将来にわたって守ることのできる仕組みを実現することが喫緊の課題となっている。

三菱電機は，この課題に対し，IoT機器と外部ネットワークを接続するIoTゲートウェイに配下のIoT機器を守る仕組みを搭載することが有効な手段の一つと考える。

この実現に向け，IoTシステム向けゲートウェイ装置(以下“IoT GW”という。)上に，自装置そのもののセキュリティを高める機能を実装したことに加え，サーバ機器と連携して配下のIoT機器に対する異常な通信を検知する学習型異常検知機能を実現した。さらに，IoT GWを既存システムに後付けするだけで，異常検知機能を提供できる仕組みを整え，これを活用して，既存の工場生産ライン設備を対象に評価・検証を行った。

今後，この技術を活用して，既存IoTシステムのセキュリティ向上に貢献し，IoTシステムがもたらす恩恵を安心して享受できる社会の実現を目指す。



EDSA：Embedded Device Security Assurance，ECHONET：Energy Conservation and Homecare Network，SLMP：SeamLess Message Protocol，BACnet：Building Automation and Control networking protocol

(注1)　MODBUSは，Schneider Electric USA，Inc.の登録商標である。
(注2)　ECHONETは，一般社団法人 エコーネットコンソーシアムの登録商標である。

IoT GWのセキュリティ技術

IoT GW自身に対するセキュリティ対策としてファームウェアやアプリケーションの改竄(かいざん)防止機能の実装や，運用中の不正操作対策としてEDSA認証のレベル1相当に対応している。また，セキュリティ的に脆弱な配下のIoT機器をサイバー攻撃から守るために，異常検知機能を搭載し，未知の攻撃も検知可能な学習型異常検知に対応したことで，IoT機器に新規機能を追加せずに，既存のIoTシステムのセキュリティ確保を実現できる。

*コミュニケーション・ネットワーク製作所　**情報技術総合研究所

1. まえがき

近年，サービス価値，生産性，保守性などの向上を図るIoTシステムが多数構築されている。また，IoTシステムに接続されるIoT機器数も，2015年の約200億個から2020年には約400億個へと急増すると予想されている(1)。

機器のIoT化は多くの利点をもたらす一方で，IoT機器を対象としたサイバー攻撃を増大させる要因にもなっている。しかし，多くのIoT機器やそこに実装されているソフトウェアは，セキュリティを意識した設計になってはいるものの，十分な対策がなされていないのが実情である。

実際に，2016年には，145,000台を超えるIoT機器からのDDoS(Distributed Denial of Service)攻撃によって，ピーク時に1Tbpsを超えるDDoSトラフィックが発生したとする報告が挙がっている(2)。今後もIoT機器は増加と多様化することが予測されているため，未知のサイバー攻撃が発生する可能性がある。

IoT機器が攻撃者から狙われる理由としては，機器数が多いだけでなく，パソコンと比較して，CPUやメモリのリソースが少なく，セキュリティ対策機能が搭載できないことが挙げられる。また，ファームウェアを最新化する機能の実装やメンテナンスがなされておらず，脆弱性への対策が不十分であることも理由の一つである。さらには，IoT機器の管理画面へのアクセス用アカウントやパスワード情報が工場出荷時の初期値のまま運用されているケースがあり，攻撃者の侵入を容易に許してしまうことも挙げられる。このような背景に基づき，2019年２月から総務省及び国立研究開発法人 情報通信研究機構(NICT)では，サイバー攻撃に悪用されるおそれのあるIoT機器の調査及び当該機器の利用者への注意喚起を行うため，NOTICE(National Operation Towards IoT Clean Environment)と呼ばれる取組みが行われている(3)。

今後，注意喚起によるセキュリティの向上が，ある程度進んだとしても，先に述べたハードウェアリソースの制約によってセキュリティ的に脆弱な機器は残存すると考えられる。そのため，IoT機器と外部ネットワークを接続するIoT GWには，IoT GW自身のセキュリティを十分確保する仕組みと，セキュリティ的に脆弱な配下のIoT機器をサイバー攻撃から守るための仕組みが求められる。

当社は，IoT GW上で動作する，IoT GW自身のファームウェアやアプリケーションの改竄を防止する仕組みを搭載することで，IoT GW装置自身の改竄防止機能を実装した。また，重要なシステムで使用されることを考慮して，産業用制御機器のセキュリティ保証に関する認証制度であるEDSA認証のレベル１(4)相当の機能を実装した。さらに，配下のIoT機器をサイバー攻撃から守るための仕組みとして，配下のIoT機器が行う通信の振る舞いから，通常とは異なる異常な通信を検知する，異常検知機能の実装と評価に取り組んでいる。

本稿では，IoTシステムでのセキュリティ脅威を**２章**で，IoT GW自身のセキュリティ対策を**３章**で，IoT GWによる配下IoT機器のセキュリティ対策を**４章**で述べる。

2. IoTシステムでのセキュリティ脅威

IoT機器を対象にしたサイバー攻撃は，脆弱なIoT機器を狙うウイルスとして2016年に問題になったMiraiによるIoT機器のボット化，及びサーバを対象としたDDoS攻撃など，国内外で急速に増大している。IPA(情報処理推進機構)の情報セキュリティ10大脅威では，IoTを対象とする脅威は，2016年度以降継続してランクインしている(5)。このような状況に対して，2017年度以降国内外で多数のIoTセキュリティに関するガイドライン文書などが作成された。**表１**に主な文書とその公開年月を示す。

表２には，近年のIoT機器への攻撃事例を示す。交差点監視カメラや石油プラントなどの物理的なシステムに対するサイバー攻撃によって，サービス停止や遅延といった深刻な被害がもたらされている(7)。IoT GWは，これらの脅威に対する対策となるように，IoT GW自身と配下のIoT機器のセキュリティを確保することが求められている。

表１．2017年度以降に公開されたIoTセキュリティ関連文書

機関名／団体名　公開資料名	公開年月
【国内】	
日本防犯設備協会 “防犯カメラシステムネットワーク構築ガイドⅡ ―インターネットとの接続に係る脅威と対策―”	2017年５月
CCDS(重要生活機器連携セキュリティ協議会) “製品分野別セキュリティガイドライン IoT-GW編 Ver 2.0”	2017年５月
IPA(情報処理推進機構) “つながる世界の開発指針 第２版”	2017年６月
IPA(情報処理推進機構) “IoT製品・サービス脆弱性対応ガイド”	2018年３月
JNSA(日本ネットワークセキュリティ協会) “IoTセキュリティ標準/ガイドライン ハンドブック2017年度版”	2018年５月
【海外】	
OTA(Online Trust Alliance) “IoT Security & Privacy Trust Framework v2.5”	2017年６月
OWASP(Open Web Application Security Project) “IoT Vulnerabilities”	2017年８月
GSMA(GSM Association) “GSMA IoT Security Guidelines Version 2.0”	2017年10月
ENISA(European Union Agency for Network and Information Security) “Baseline Security Recommendations for IoT”	2017年11月

（出典）　IPAの“情報セキュリティ白書2018”(6)の表から抜粋

表２．IoT機器への攻撃事例

発生	対象設備・機器	事象
2017年６月	自動車生産工場のパソコン	生産ライン停止
2017年６月	交差点監視カメラ	不正制御による動作不安定
2017年６月	物流業務システムのコンピュータ	サービス遅延
2017年８月	安全計装システムのコントローラ	一部システムダウン
2018年８月	半導体生産工場のコンピュータ	生産ライン停止

（出典）　IPAの“制御システムのセキュリティリスク分析ガイド第２版”(7)の表から抜粋

3. IoT GW自身のセキュリティ対策

IoT GWは，IoTシステムの外部ネットワークとの接続点となることから，IoT GW自身のセキュリティを十分確保する必要がある。当社は，IoT GW自身のセキュリティを確保するために，起動時のセキュアブートと，ファームウェア及びアプリケーションをインストールする際の改竄防止機能を実装した。また，重要なシステムで使用されることを考慮して，産業用制御機器のセキュリティ保証に関する認証制度であるEDSA認証のレベル１相当に対応した開発を行った。

3.1 ファームウェアの改竄防止機能

IoT GWのファームウェア改竄防止のために，当社では，RSA(Rivest，Shamir，Adleman)公開鍵暗号を用いた署名アルゴリズムによる署名を生成し，IoT GWのファームウェアに付加している。

また，IoT GWではプロセッサ内のOTP(One Time Programmable)メモリを信頼の起点とするセキュアブート機能によって，署名が正しく検証できた場合にだけ当該ファームウェアを起動する仕組みとしている。

3.2 アプリケーションの改竄防止機能

IoT GW上で動作するJava(注3)バンドルや，Java以外のC言語などで作成したOS上で直接動作するネイティブアプリケーションに対しては，RSA公開鍵暗号を用いた署名アルゴリズムによる署名を付与し，署名が正しく検証できた場合にだけ，インストール／起動を許可する改竄防止機能を提供している[8]。この機能を用いた，ネイティブアプリケーションインストール機能の仕組みを**図１**に示す。

(注３) Javaは，Oracle America，Inc.の登録商標である。

3.3 運用時の不正操作に対するセキュリティ対策

IoT GWでは，運用中の不正操作や不正プログラムの実行といった攻撃を防ぐために，産業用制御機器のセキュリティ要件を規定した，EDSA認証のレベル１相当の機能を実装した。これによって，ユーザー認証や各機能の使用制御に加え，送信中のデータの完全性や機密性も確保している。

4. IoT GWによる配下IoT機器のセキュリティ対策

4.1 ネットワーク異常検知方式

IoT GWの配下に接続されるセキュリティ的に脆弱なIoT機器を守る手段として，当社は，IoT GWでIoT機器が行う通信を監視し，異常な通信を検知する技術開発を行っている。

検知する方式として，ホワイトリスト型の異常検知と，学習型の異常検知の二つの方式を開発した。ホワイトリスト型では，あらかじめ，通信の“正常な状態”を定義しておき，定義から不一致が発生したことによって異常を検知する技術である。一方，学習型では，システムの正常状態での通信トラフィックを，機械学習によって，ホワイトリスト型と同様に“正常な状態”を表すモデルを構築し，これに基づき異常な振る舞いを検知する技術である[9]。

次に，ホワイトリスト情報の生成が困難な通信のタイミングや内容が変化するシステムに適している学習型異常検知機能の実装について述べる。

4.2 トラフィック統計監視機能の実装

IoT機器，IoT GW及びIoTサーバからなる基本的なIoTシステムの構成を**図２**に示す。この構成でIoT GWは，IoT機器から送信された通信の転送や，IoT機器及びIoTサーバの通信を終端する。IoT GWを通過する通信のトラフィック統計監視を，各IoT機器単位で行うことで，異常な振る舞いを検知する。

次に，**表３**に上記のトラフィック統計監視機能を実装するプラットフォームであるIoT GWのハードウェア仕様を示す。

IoT GWは，パケット転送エンジン(Packet Forwarding Engine：PFE)を搭載したデュアルコアCPUを備えて

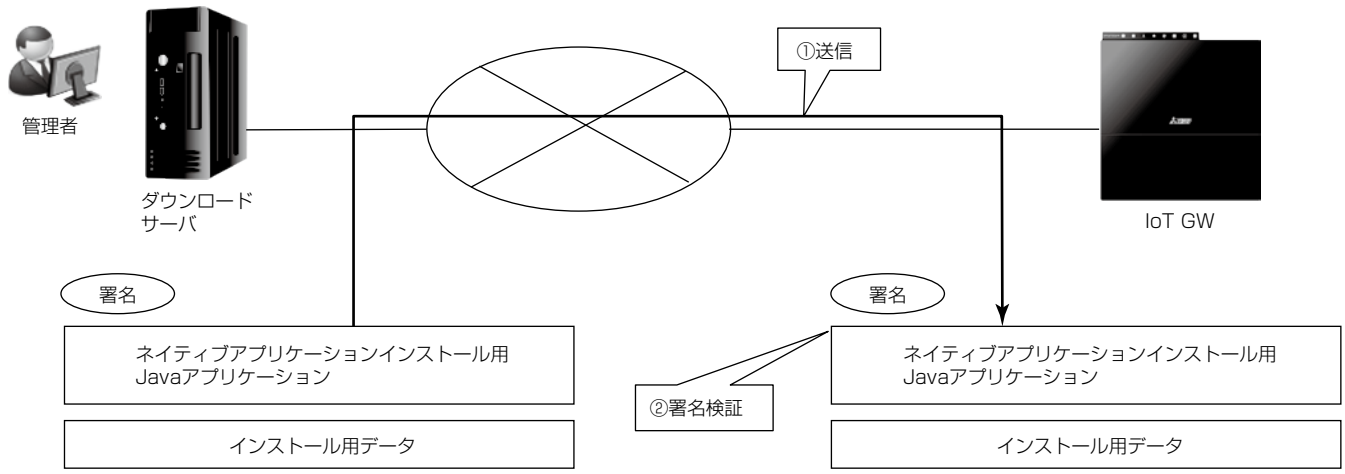


図１．ネイティブアプリケーションインストール機能の仕組み

おり，1 Gbpsの双方向通信が可能である。IoT GW上の大半のIPパケット転送処理はPFEにオフロードされるため，アプリケーションソフトウェアはCPUパワーの90%以上を使用できる。

図3には，IoT GWの転送処理機能ブロック図の一部を示す。IoT GWは，LANからWAN方向のIPパケットを受信すると，そのパケットが通信フローの最初のパケットの場合は，CPUに転送され，一方，PFEが既に通信フローを認識できている場合は，受信パケットをWAN側に直接転送することができる。これは，通信フローの最初のパケットをCPUが受信した場合は，フロー情報がPFEに入力され，残りのフローはPFEによって直接転送可能になり，ファストパスと呼ばれる高速転送処理が可能になるためである。そのため，もしこのファストパス機能を無効にした場合，転送処理は全て，CPU上でソフトウェア処理されるスローパスとなる。また，ファストパス機能が有効になっている場合は，通信フロー情報がPFEに設定されると，PFEだけで処理を行うため，転送タスクと転送されたパケット情報は，CPUで監視することができなくなってしまう。

そのため，IoT機器用のネットワーク異常検知システムに必要なトラフィック統計監視機能をPFEの専用ファームウェアとしてIoT GWに実装した。

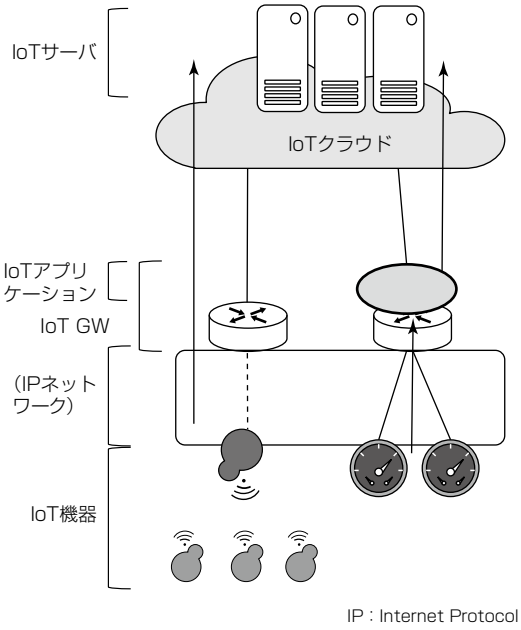


図2．基本的なIoTシステムの構成

表3．当社IoT GWのハードウェア仕様

SoC	CPU	ARM(注4) Cortex(注4) A9(900MHz)×2
		Lv1 cache： 32KB(Data)+32KB(Instruction)
		Lv2 cache： 256KB
	PFE	Total 2Gbps IP forwarding with NAT/NAPT，PPPoE
DRAM		512MB DDR3
Flash		256MB
OS		Linux(注5) 3.2
インタフェース		WAN：(1000BASE-T)×1
		LAN：(1000BASE-T)×4
		Wireless LAN：IEEE802.11a/n/ac，b/g/n selectable
		USB：USB2.0 type A receptacle×2

SoC：System on Chip，DRAM：Dynamic Random Access Memory，NAT/NAPT：Network Address Translation/Network Address Port Translation，PPPoE：Point to Point Protocol over Ethernet，WAN：Wide Area Network

（注4） ARMとCortexは，ARM，ltd.の登録商標である。

（注5） Linuxは，Linus Torvalds氏の登録商標である。

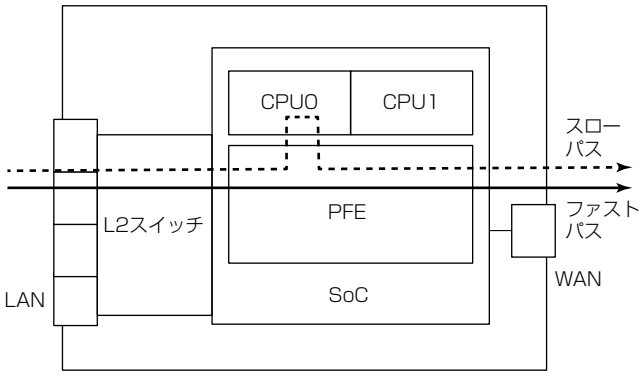


図3．IoT GWの転送処理機能ブロック図

4.3 IoT機器のネットワーク異常検知システム

IoT機器のネットワーク異常検知システムの構成を**図4**に示す。

IoT GWのトラフィック統計監視機能は，IoT機器のトラフィック統計情報を収集し，その情報を定期的に異常検知サーバに送信する。異常検知サーバは受信したトラフィック統計情報からトラフィックの特徴セットを計算し，学習プロセスがまだ終了していない場合はそれらを学習する。IoT機器の学習プロセスが終了したら，IoT機器の受信トラフィック統計情報を使用して異常を検知する。新規のIoTシステム構築に併せてネットワーク異常検知システムを導入する場合は，この構成が適している。

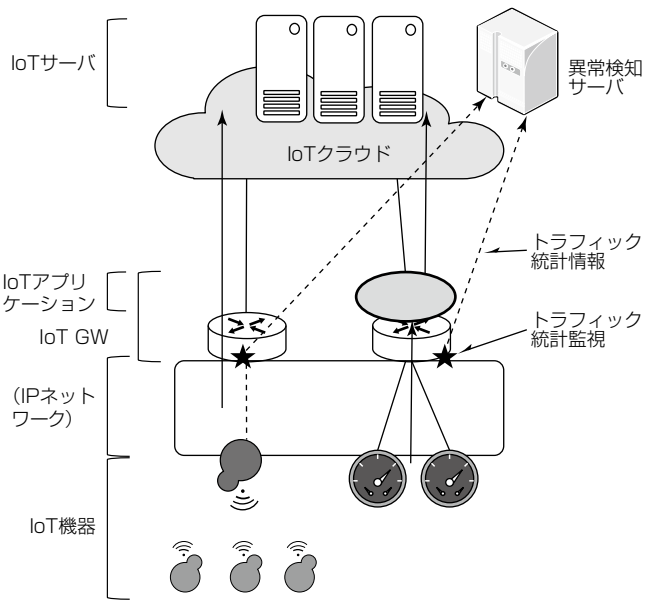


図4．IoT機器のネットワーク異常検知システムの構成

4.4　ボルトオン型のネットワーク異常検知システム

4.3節で述べたIoT GWをゲートウェイとして設置する構成とは異なり，L2スイッチなどの既存のネットワーク機器からのミラートラフィックを使用して，トラフィック統計情報を生成する，ボルトオン型のネットワーク異常検知システムの構成を**図5**に示す。この構成では，IoT GWはネットワーク異常検知のセンサとしてのみ機能し，ユーザーは既存のシステムに大きな変更を加えることなく，ネットワーク異常検知機能を簡単に追加できる。

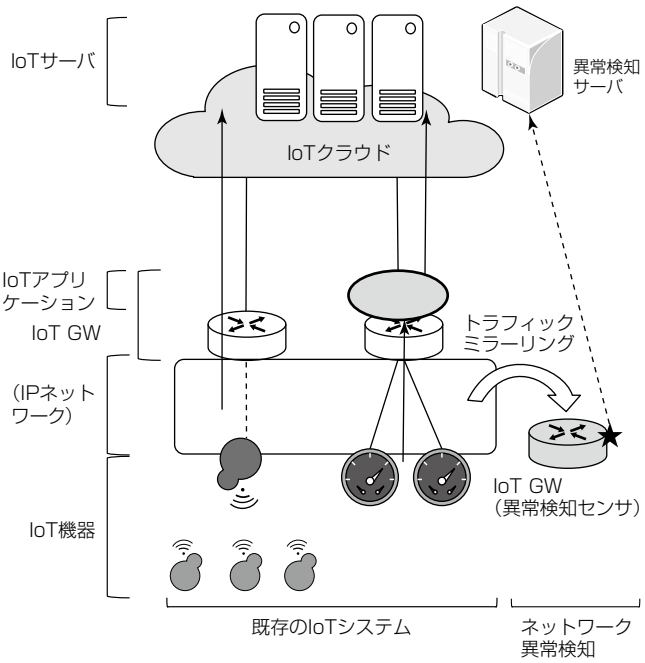


図5．ボルトオン型ネットワーク異常検知システムの構成

次に，IoT GW上での，ミラーリングされたトラフィック処理のフローを**図6**に示す。

IoT GWはミラーリングされたトラフィックの処理を全て，ソフトウェアで実行するため，IoT GWがトラフィックをPFEで処理する場合と比較して，CPU使用率が高くなるため，リソース消費状況を考慮する必要がある。

この点に関しては，**表3**でも示したとおり，当社IoT GWはハードウェア仕様として，デュアルCPUコアを採用しており，この評価中でも，常にCPU使用率が20パーセント未満であったことから，性能上問題ないことは確認済みであり，更に大容量のトラフィック処理も可能と考えている。

4.5　異常検知システムの実環境評価

当社では，**図4**に示した汎用的なIoTシステムのモデルとして，100台の監視カメラで構成されるIoTシステムを構築し，**4.3節**で述べたネットワーク異常検知システムを評価した結果から，監視可能であることは確認済みである。

今回，さらに**4.4節**で述べたボルトオン型のネットワーク異常検知システムのモデルとして，約100台のIoT機器で構成される工場の生産ラインネットワークを対象にボルトオン型のネットワーク異常検知システムの評価を実施した内容を述べる。評価構成を**図7**に示す。

また，評価条件として監視対象にした生産ラインネットワークでの通信トラフィック情報を**表4**に示す。IoT機器数は100を超えているが，トラフィック量は最大でも

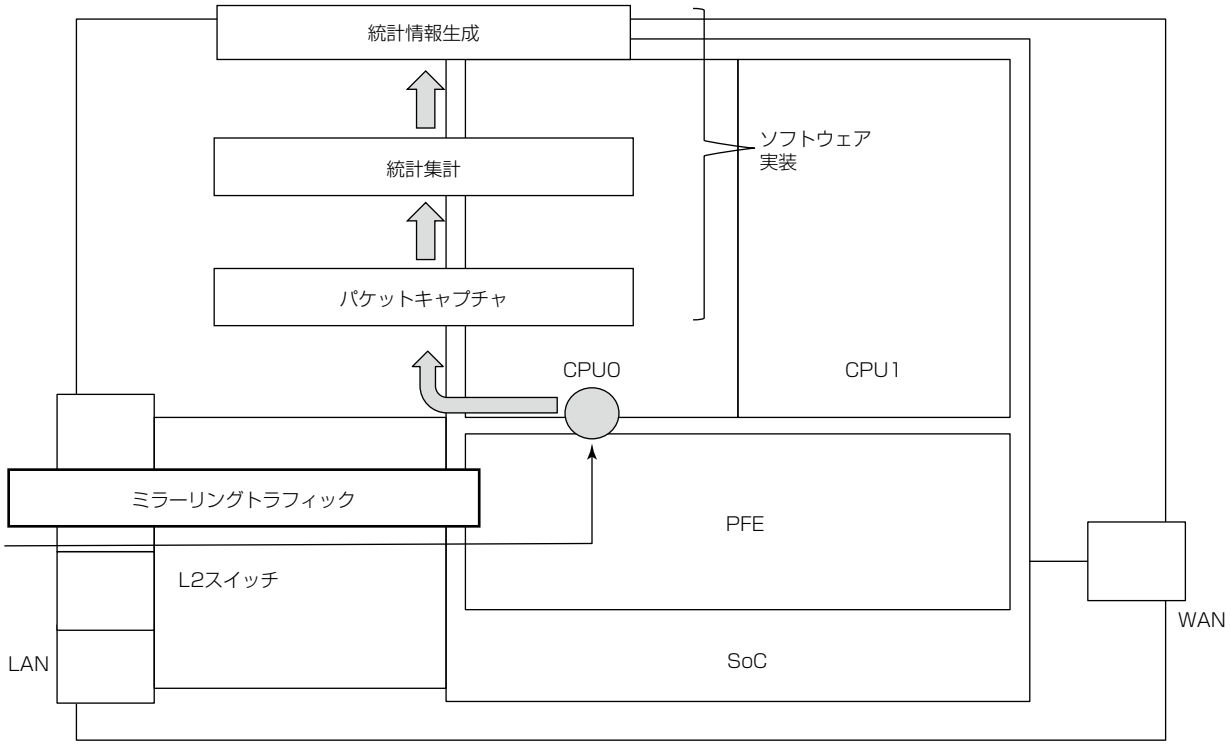
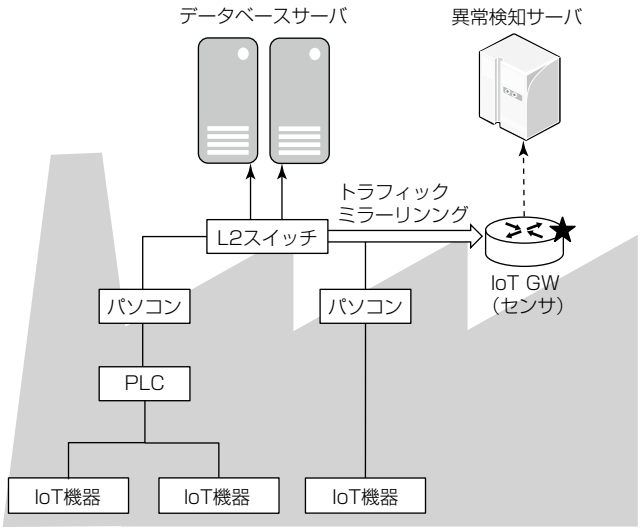


図6．ミラーリングされたトラフィックの処理フロー



PLC：Programmable Logic Controller

図7．ボルトオン型ネットワーク異常検知システムの評価構成

表4．評価環境の通信トラフィック情報

パラメータ	値
IoT機器数	108
平均トラフィックフロー数/台	8
プロトコル数	50
平均トラフィック量	80kbps
最大トラフィック量	1.4Mbps

1.4Mbpsであった。この環境では，1台のIoT GWで処理が可能であり，トラフィック統計情報の生成及び送信が正常に行われることが確認できた。

この評価によって，工場の既存生産ラインネットワークに対して，IoT GWを付け足すだけで，ネットワーク異常検知を利用できることが確認できた。

5. むすび

IoT化が急速に進む中，IoT機器を狙うサイバー攻撃が急増している現状を示した。そのような中，IoTシステムを構成するIoT GW自身のセキュリティ確保と，配下のIoT機器のセキュリティ確保に向けた当社の取組みについて述べた。IoT機器のセキュリティを確保するために，IoT機器の通信を監視し，異常な通信を検知する異常検知システムと，これを実現するために必要なトラフィック統計監視技術について述べた。

さらに，既設のネットワークへの適用を考慮して，ボルトオン型で動作可能なネットワーク異常検知システムの開発を行い，100台の監視カメラで構成されるIoTシステムと，OT（Operation Technology）システムの一つである工場生産ラインシステムでの評価結果を述べた。

今後も，様々なセキュリティ装置やセキュリティサービスとの併用・連携を推進しつつ，さらには当社IoT GWの処理能力の向上を実現することでネットワーク異常検知システムの適用範囲拡大を図り，安心・安全にIoTシステムを活用できる社会の実現を目指す。

異常検知サーバの研究開発は，日本電信電話㈱セキュアプラットフォーム研究所の協力で実施された。ここに謝意を表する。

この研究の一部は，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：国立研究開発法人新エネルギー・産業技術開発機構（NEDO））によって実施された。

参考文献

(1) 総務省：平成30年版 情報通信白書
(2) OVH：The DDoS that didn't break the camel's VAC
https://www.ovh.com/world/news/articles/a2367.the-ddos-that-didnt-break-the-camels-vac
(3) NOTICEホームページ
https://notice.go.jp/
(4) ISASecure：EDSA-311 ISA Security Compliance Institute-Embedded Device Security Assurance-Functional Security Assessment（FSA）v1.4 (2010)
(5) 独立行政法人 情報処理推進機構（IPA）：情報セキュリティ10大脅威2019
https://www.ipa.go.jp/security/vuln/10threats2019.html
(6) 独立行政法人 情報処理推進機構（IPA）：情報セキュリティ白書2018
https://www.ipa.go.jp/files/000070313.pdf
(7) 独立行政法人 情報処理推進機構（IPA）：制御システムのセキュリティリスク分析ガイド第2版 (2018)
https://www.ipa.go.jp/files/000069436.pdf
(8) 佐藤浩司，ほか：IoTゲートウェイのセキュリティ技術，三菱電機技報，**92**，No.6，356～360 (2018)
(9) 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）：IoT機器向けゲートウェイによる動作監視・解析技術
https://www.nedo.go.jp/content/100863673.pdf