CM-003

仮想化による IoT デバイスのセキュリティ実現方式
Realizing IoT Device Security Based on Virtualization

大谷 武† 松倉 隆一† 角田 潤†
Takeshi Ohtani Ryuichi Matsukura Jun Kakuta

1. はじめに

近年，様々な産業分野への IoT（Internet of Things）の導入が進んでおり，今後もこの傾向が継続すると考えられている．特に，製造業に注目が集まっており，工場の生産効率の向上や予知保全を目的とした IoT 利用の試みが行われている．この動きは，単一企業内に留まらず，IIC（Industrial Internet Consortium）や IVI（Industrial Value Chain Initiative）などの業界レベルや，Industrie 4.0 のように国レベルの活動へと拡大し，工場間がネットワーキングされ始めている．

しかし，工場がインターネットに繋がると，必然的にセキュリティ脅威にさらされるようになってきた．実際，Mirai [1]や WannaCry [2]などのマルウェアの攻撃により，工場が閉鎖になった例は記憶に新しい．製造業は，ひとたびマルウェアの被害に遭い，生産ラインが停止すると，数 10 億～数 100 億円と莫大な損害が発生する．そのため，セキュリティが強く要望されている．

こうした問題を解決するため，今回，ゲートウェイ（GW）が，IoT デバイスを，セキュリティ機能を持つデバイスに仮想化することにより，IoT システムのセキュリティを実現する方式を提案する．本論文は，以下のように構成される．まず，第 2 章では，IoT の特徴に由来する問題点を述べる．次に，第 3 章で，問題を解決するための基本方針を，第 4 章は，基本方針を実現するシステム構成，第 5 章は，それを実現する上での課題と解決方法を述べる．第 6 章は提案方式のセキュリティ脅威の防御可能性を評価し，最後の第 7 章で，結論を述べる．

2. IoT セキュリティの問題

典型的なマルウェアの攻撃には，以下の 2 種類が存在する（図 1）．

- 外部からの攻撃
  未使用ポートの放置や初期ユーザ ID/パスワードによる運用など，デバイスの不適切な管理や，OS やファームウェアの脆弱性を利用し，LAN 外部からデバイスに侵入する．例えば，ポートスキャンやブルートフォースアタックと呼ばれる方法が知られている．
- 内部からの攻撃
  LAN 内のマルウェアに感染したデバイスが，別のデバイスやサービスを攻撃し，使用不能にしたり，感染を拡大したりする．攻撃元となるデバイスのマルウェア感染は，上記の外部からの攻撃もあるが，現場におけるデバイス設定用の作業端末や USB メモリからの侵入などもありうる．攻撃方法としては，DDoS (Distributed Denial of Service)や不正操作などがある．

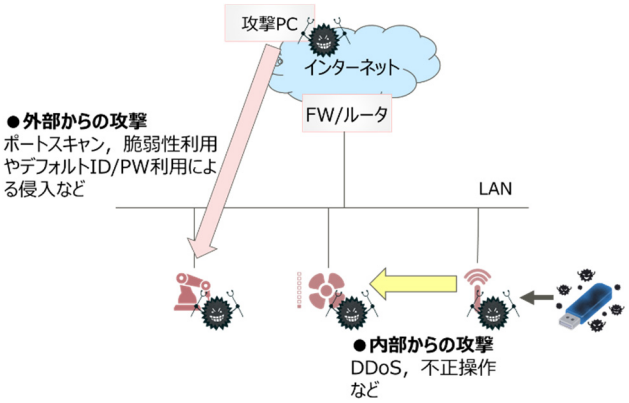

図 1 マルウェアの攻撃

IoT デバイスをセキュアにするには，上記 2 種類の攻撃を防御しなければならない．しかし，十分に防御されていないのが現状である．その理由は，以下の IoT 固有の特徴による．

(1) セキュリティソフトが導入不可能
IoT デバイスは，PC に比べ CPU やメモリが貧弱，自由にソフトウェアをインストールすることが想定されてない．例えば，温湿度や振動などを検知するセンサ類，ネットワークカメラ，PLC（Programmable Logic Controller）などは，機能が限定的であり，OS も PC とは異なっている．そのため，セキュリティソフトをインストールすることも，実行することもできない．

(2) 脆弱性が放置されたまま
工場で使用される IoT デバイスは 10 年以上使用される場合があり，製品の製造・サポート停止や，製造ベンダの変更により，パッチが提供されなくなる可能性がある．実際，制御システムに，既にサポートが終了した Windows XP が使用されている現場もある[3]．また，パッチが提供されたとしても，生産設備では稼働の継続が優先され，パッチ適用によるデバイスの再起動が許されない場合もある．

(3) 管理が行き届かない
現場の施設運用・製造担当者など，セキュリティに詳しくない人が IoT デバイスを管理しなければならない上に，IoT デバイスの台数が膨大で管理が行き届かない．実際，制御システムセキュリティの担当組織を設置している企業は，わずか 23%だけであるという報告がある[4]．また，IoT デバイスがインターネットに接続しているにも拘らず，未使用サービス用のポートを開放したままにしたり，ユーザ名やパスワードを初期値のまま運用していた例も多い．これは，SHODAN（https://www.shodan.io/）や Censys（https://censys.io/）という，インターネットに接続されて

† 株式会社富士通研究所．Fujitsu Laboratories Ltd.

Copyright © 2018 by
The Institute of Electronics, Information and Communication Engineers and
Information Processing Society of Japan All rights reserved.

いる機器の検索エンジンで確認できるため，攻撃対象となりうる．

上記の理由から，IoT デバイス自体を機能面および運用面から，セキュアにすることは困難である．そのため，IoT デバイスのセキュリティには，システム的な保護が必要であると考える．

3. 問題解決の基本方針

IIC などの標準化組織やネットワーク機器ベンダは，管理の行き届いたオフィスのような IT（Information Technology）エリアと，管理の行き届かない工場のような OT（Operation Technology）エリアをネットワークレイヤ（L1～L6）で分離し，GW がアプリケーションレベル（L7）でメッセージを中継する構成を推奨している（図 2）[5][6]．このような構成にすることで，GW が IoT デバイスに送信しても問題ないリクエストのみを中継し，IT エリアのセキュリティ脅威が，セキュリティの弱い OT エリアに波及しないようにしている．しかし，通信ポートレベルのフィルタリングは可能でも，IoT デバイスは多種多様で，インタフェースが異なる，あらゆる IoT デバイスに対するリクエストの危険性を判定することは実質的には不可能であり，外部からの攻撃をブロックすることは困難である．また，この構成では，OT エリアへの持ち込み端末や USB メモリから感染した IoT デバイスによる，内部からの攻撃も防御不可能である．

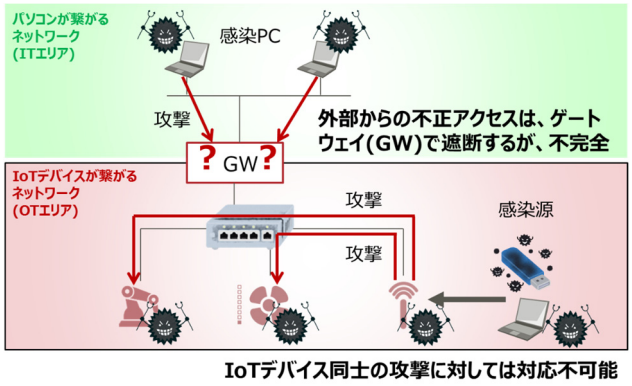

図 2 GW による IT エリアと OT エリアの分離

そこで，我々は，このような外部および内部両面の攻撃からデバイスを保護する，セキュアデバイス仮想化という方式を提案する

一般に，仮想化とは，サーバやネットワークなどのハードウェアリソースを，物理的な制約にとらわれず，利用目的に応じて使いやすい論理的な単位で扱えるようにすることである．例えば，サーバ仮想化は，1 台の物理サーバを，メモリやディスクなどのリソースや OS も異なる複数のサーバとして動作させ，複数のサービス間の干渉をなくし，運用上の利便性向上を図るものである．これは，ひとつの物理リソースを，複数の論理リソースに仮想化する例であるが，逆にデータベースクラスタのように，複数の物理的サーバを集約し，高可用かつ高性能なデータベースサーバに仮想化する例もある．

このような従来の仮想化とは違い，我々が提案するセキュアデバイス仮想化は，多種多様で，実際にはセキュリティ機能を持たない IoT デバイスを，GW 上に仮想的に共通インタフェースを持ち，セキュリティ機能を搭載するデバイスとしてオブジェクト化（仮想デバイス）し，すべての IoT デバイスへのアクセスを，仮想デバイス経由にする方式である（図 3）．当然，実際のデバイス（実デバイス）同士が直接通信することも禁止し，実デバイスは GW とのみ通信可能にする．そうすることで，仮想デバイスと実デバイスとは 1 対 1 に対応し，仮想デバイスに対してセキュリティ機能を実行することで，実デバイスもセキュアに保たれる．

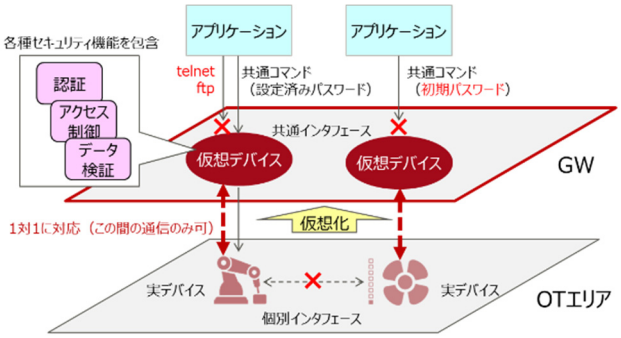

図 3 セキュアデバイス仮想化のコンセプト

図 4 は，外部および内部攻撃に対する防御方針の模式図である．以降の節で，それぞれの方針を述べる．

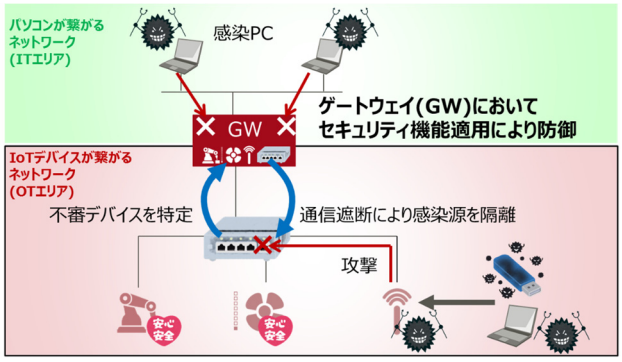

図 4 セキュアデバイス仮想化によるデバイス保護

3.1 外部からの攻撃に対する方針

IoT デバイスに対する外部からの攻撃に対しては，IoT デバイスを通信プロトコルも含め，共通インタフェース化し，不足しているセキュリティ機能を代行することで防御する．

IoT デバイスを共通インタフェース化するのは，二つの理由からである．ひとつは，外部の攻撃者に，IoT デバイスの特性を知られ，IoT デバイスが攻撃対象になりやすくなることを防ぐためである．例えば，IoT デバイスで telnetd や ftpd が動作していることが判明すれば，その脆弱性を利用することで，IoT デバイスに侵入・改竄することが容易となる．バージョンまで把握できれば，なおさらである．そこで，IoT デバイスの特性を隠蔽し，共通インタ

Copyright © 2018 by
The Institute of Electronics, Information and Communication Engineers and
Information Processing Society of Japan All rights reserved.

フェースで利用可能な仮想デバイスを利用させることで，外部からは IoT デバイスの実体を把握できなくなる．

もうひとつの理由は共通インタフェースにすることで，セキュリティ機能の代行を容易化するためである．インタフェースが IoT デバイス毎に異なると，セキュリティ機能を適用するためには，それぞれのインタフェースに適合させる必要が生じ，今後新たに開発される IoT デバイスへの対応が困難になるからである．

セキュリティ機能の代行は，アプリケーションが仮想デバイスを利用する際，実デバイスで実行できない，あるいは適切に設定されていないセキュリティ機能を，GW で代行することである．例えば，センサ類はアクセス時に認証しないものが多いが，GW 上で認証処理を行うことで，センサの不正設定やセンシングデータの不正取得を防ぐことが可能である．また，実デバイスが大量にあって，認証情報を初期値から変更せずに運用している場合でも，GW 上で適切な認証を行うことで，実デバイスへの不正アクセスを回避可能である．代行するセキュリティ機能は，認証，アクセス制御，データ検証（データのシグネチャマッチングによる攻撃判定や IoT デバイスの利用が想定内かの判定），ログ検証（ログ分析による攻撃判定）を想定しているが，今後更に必要な機能を検討予定である．

更に，仮想デバイスは IoT デバイスを利用するアプリケーション開発を容易化するというメリットも持つ．IoT デバイス毎に，通信プロトコルやデータモデルが異なっており，様々な IoT デバイスを利用するアプリケーションを開発するのは効率が悪い．しかし，共通インタフェースを持つ仮想デバイスを利用することで，煩雑な通信処理やデータ解釈処理の実装が不要になるからである．

3.2 内部からの攻撃に対する方針

OT エリア内の IoT デバイスは，GW 上に仮想化され，IoT デバイスを利用するアプリケーションはすべて仮想デバイスを介して，実デバイスを利用する．IoT デバイスは，他の IoT デバイスとは直接通信せずに，仮想デバイスを管理する GW とのみ通信するようにする．そうすることで，IoT デバイスが，マルウェアによって改竄され，ポートスキャンや他の IoT デバイスへの不正アクセスを試みても，防御可能である．

これを実現するには，OT エリア内の各 IoT デバイスに対して，GW とのみ通信可能な仮想ネットワークを構築し，そこに IoT デバイスを接続する方式が考えられる．しかし，既に OT システムを運用中の現場では，すでに仮想ネットワークを運用しているケースが考えられ，自由に仮想ネットワークを構築することが不可能な場合がある．また，大量の IoT デバイスを収容する場合，大量の仮想ネットワークが必要となり，仮想ネットワークの構築や，ネットワーク構成変更時の仮想ネットワークの維持が困難になる．

そこで，GW が OT エリア内の IoT デバイスやネットワーク機器間の接続関係（トポロジ）を管理し，そのトポロジに基づき，GW 以外と通信しようとする不審な IoT デバイスを特定し，その不審 IoT デバイスが他の IoT デバイスを攻撃しないように，通信を遮断する方式を採用した．

なお，シリアル系の Bluetooth Low Energy（BLE）や RS-232C/RS-485 などの通信を行うデバイスは，元々GW としか通信しないので，GW で異常通信を遮断することが容易である．このようにして， IoT デバイスに対する内部からの攻撃を防御する．

4. システム構成

セキュアデバイス仮想化を実現するシステムの構成を図 5 に示す．

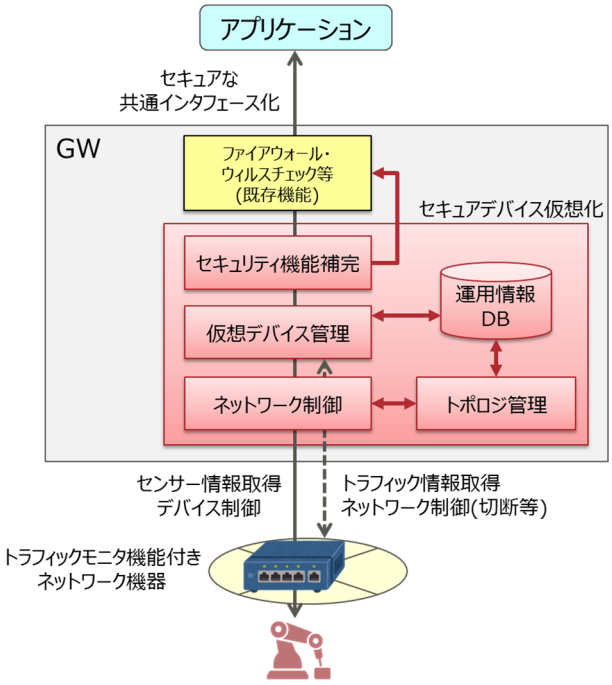

図 5 システム構成

中心的な役割を果たす機能モジュールは仮想デバイス管理であり，実デバイスを仮想化したオブジェクトである仮想デバイスを管理する．実デバイスは，通信プロトコルやデータモデルが多種多様であるが，デバイス毎の通信処理やデータ解釈処理を再利用可能なアダプタの組み合わせで実現することで，API の共通化を容易に実現可能な構成としている[7][8].

更に，仮想デバイス管理の OT エリア側にネットワーク制御を，IT エリア側にセキュリティ機能補完を配備する．セキュリティ機能補完は，外部からの攻撃を防御するために，IoT デバイスの代わりにセキュリティ機能を実行する（3.1 節）．GW 自体は，IoT デバイスとは違い，PC と同様に Linux のような汎用 OS が稼動し，ファイアウォールやウィルス対策ソフトが動作するハードウェアを想定している．セキュリティ機能補完は，そのような一般的なセキュリティ機能も利用しつつ，認証，認可（アクセス制御），データ検証，ログ検証を代行するが，随時適用するセキュリティ機能をカスタマイズ可能なように，プラグイン可能な構成にしている．ネットワーク制御は，内部からの攻撃を防御するために，トポロジ情報を利用して，不正な通信を行う不審デバイスを特定し，その通信を遮断する（3.2 節）．

トポロジ管理は，ネットワーク制御が利用する OT エリアのネットワークトポロジを管理する．仮想デバイス管理は，IoT デバイスやネットワーク機器から，どの機器と接続しているかの情報を収集し，運用情報 DB に蓄積する．

Copyright © 2018 by
The Institute of Electronics, Information and Communication Engineers and
Information Processing Society of Japan All rights reserved.

トポロジ管理は，その情報を参照し，OT エリアの全体トポロジを推定する．

更に，詳しい機能は次章で述べる．

5. セキュアデバイス仮想化の実現方法

本章では，セキュアデバイス仮想化を実現する上での課題と解決方法を述べる．

5.1 外部攻撃に対する防御に関して

● アプリケーションレイヤアクセスへの限定

本方式は，OT エリア外部から仮想デバイスのみをアクセスさせる必要がある．そのため，セキュリティ機能補完は，GW のファイアウォール設定を操作し，特定の通信プロトコルのみを受信可能なように，そのポートのみを開き，それ以外の通信ポートを閉じるようにする．使用する通信プロトコルは HTTP とし，インタフェースは W3C が標準化を進めている Web of Things（WoT）に準拠する．WoT は，様々なデバイスを仮想化し，web という共通のインタフェースにより利用可能にする基盤であり，親和性が良いからである．

● セキュリティ機能の適用

GW 自体をセキュアに運用する必要があるので，GW にはファイアウォールやウィルス対策などの一般的なセキュリティ対策が施される．セキュリティ機能補完は，その機能を利用しつつ，アプリケーションから IoT デバイスへのリクエストを受信すると，それ以外の認証・認可，データ検証など仮想デバイスに特有のセキュリティ機能を適用する．補完するセキュリティ機能は，システムを適用するソリューションのセキュリティ要件や，利用するデバイスに不足するセキュリティ機能により異なるので，アプリケーションやデバイス毎に適用するセキュリティ機能を選択可能にしている．

● 仮想デバイスと実デバイスとの同一性確保

実デバイスがネットワークに接続されると，それと 1 対 1 に対応する仮想デバイスを生成し，アプリケーションが利用可能にする必要がある．その際，本来構築したい IoT システムには想定されない不正デバイスの仮想デバイスを生成してはならない．さもないと，悪意を持つ第 3 者が持ち込んだ不正デバイスが GW に収容され，IoT サービスの正常運用を妨害する可能性があるからである．

これを解決するために，GW が収容すべき IoT デバイスの条件（デバイスのベンダ名，製品名，ファームバージョンなど）を，設計情報として保持しておき，デバイス接続時にデバイスプロファイルを取得し，設計情報と照合し，マッチする場合のみ仮想デバイスを生成する．デバイスプロファイルの取得方法として，BLE デバイスの場合は，BLE の仕様で規定されている DIS（Device Information Service）により，IP デバイスの場合は，UPnP（Universal Plug and Play）や HTIP（Home-network Topology Identifying Protocol）などが考えられる．プロファイル取得手段を持たないデバイスの場合は，事前にデバイスベンダからデバイスに関する情報を取得し，データベース化しておき，デバイスのリンク接続時に検出した，MAC アドレスや BD（Bluetooth Device）アドレスのようなデバイス識別情報を使って，データベースを検索し，設計情報と照合する．デバイスプロファイルと設計情報が，マッチしない場合は，不正デバイスと判断し，仮想デバイスを生成しない．更に，内部攻撃のリスクを回避するために，ネットワークから切断，あるいは通信を遮断する（図 6）[7].

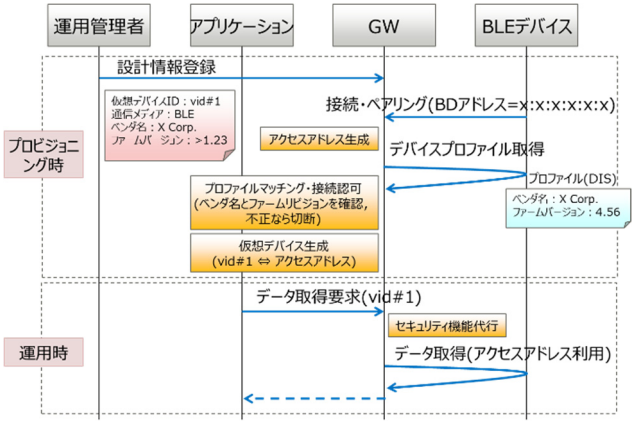

図 6 実デバイスと仮想デバイスとの対応付け処理

5.2 内部攻撃に対する防御に関して

● トポロジの管理

本方式は，仮想化により IoT デバイスは GW とのみ通信する．そのため，以降で述べる不審デバイスの検知と，その通信遮断を実現するのに，OT エリアのトポロジを利用する．

各 IoT デバイスやネットワーク機器は，HTIP あるいは LLDP（Link Layer Discovery Protocol）を使って，隣接する機器の情報を通知するようにしておく．また，Wi-Fi アクセスポイントには，HTTP や ssh など独自のインタフェースにより，接続中の Wi-Fi デバイスの一覧を参照する機能を持つものがある．このように，様々なインタフェースを持つネットワーク機器があるが，GW はネットワーク機器も仮想化しており，同じインタフェースで隣接機器の情報を収集することが可能である．

GW は，それを収集し，同じ機器 ID を持つ情報を結合して，全体のトポロジを推定する．この時，隣接機器の情報を通知する機能を持たない機器が存在すると，トポロジをひとつに統合できない場合がある．その場合には，GW までの経路がトポロジ的に連結していない機器に対し，TTL 値を 1 から増加させながら， ICMP パケットを順に送信し，通信経路上のネットワーク機器を順に検出し，不明な部分を補間する（traceroute コマンドの動作原理と同様）．

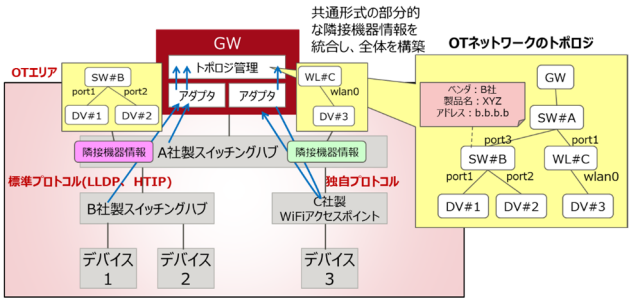

図 7 トポロジの構築・管理

Copyright © 2018 by
The Institute of Electronics, Information and Communication Engineers and
Information Processing Society of Japan All rights reserved.

● 不審デバイスの検知

前章で述べたように，IoT デバイスは，GW とのみと通信する．それ以外の不正通信を行う IoT デバイスを不審なデバイスと考える．IoT デバイスから GW の通信経路は，トポロジによって決まるため，ネットワーク機器が中継した通信パケットの送信元と送信先が分かれば，不正な通信か否かを判断できる．

GW は，OT エリア内のネットワーク機器から，ネットワーク機器の ID と，中継したパケットの送信元と送信先情報を収集する．例えば，ネットワーク機器がスイッチングハブの場合，ミラーポートに収集用デバイスを接続し，上記の情報を GW に送信する．ポートスキャンのような攻撃は，これで検知可能である．一方，DoS 攻撃は，ネットワーク機器から SNMP（Simple Network Management Protocol）でトラフィック量を収集して判断する．

このような通信状況に関する情報は，すべてのネットワーク機器から収集する必要はないが，なるべく IoT デバイスの近くから収集するのが良い．その方が，不正通信の発生元である IoT デバイスを特定しやすいからである．しかし，大量の IoT デバイスが広域に設置されている場合，IoT デバイスが直接繋がるネットワーク機器すべてに情報収集用デバイスを装着すると，たくさんの情報収集用デバイスが必要となり，高コストとなる．コストを下げつつ，不審デバイスの検知を効率的に行うための，情報収集対象ネットワーク機器の決定は，今後の課題である．

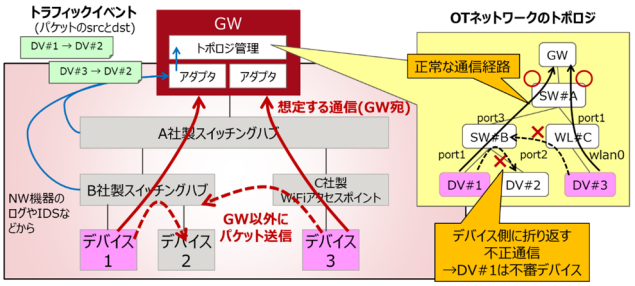

図 8 不審デバイスの検知

● 通信遮断

GW は，不審デバイスを検出すると，そのデバイスが，他のデバイスを攻撃しないように，ネットワーク機器の通信を遮断する．

ネットワーク機器の通信遮断機能は，機器によって異なっている．例えば，スイッチングハブは，ポート単位で通信をブロックすることが可能なものがあるが，Wi-Fi アクセスポイントは，SSID 単位での無線機能停止あるいは無線機能自体を停止する機能しか持たないものもある．そのため，ネットワーク機器毎に通信遮断機能が異なり，不審なデバイスの通信のみを遮断することができない場合がある．その結果，単純に不審デバイスが接続するネットワーク機器の通信遮断を行うと，他の正常なデバイスも同時に通信不能になり，システムの動作に支障を来たす場合がある．そこで，GW はネットワーク機器が持つ通信制御機能を管理し，通信遮断ポイントの決定の際，通信を遮断した場合の正常な IoT デバイスへの影響が最小となるネットワーク機器と制御内容を決定するようにした．しかし，使用するネットワーク機器やネットワーク構成によっては，常に不審デバイスを単独で通信遮断可能とは限らないため，IoT サービスに必要不可欠な IoT デバイスが通信不能になる可能性がある．また，通信経路に冗長性がある（例えば Wi-Fi のようにハンドオーバが発生する）場合は，通信を遮断しても，再度通信可能になる可能性がある．このように，IoT デバイスやネットワークの特性を考慮した，通信遮断方法は，更に検討が必要である．

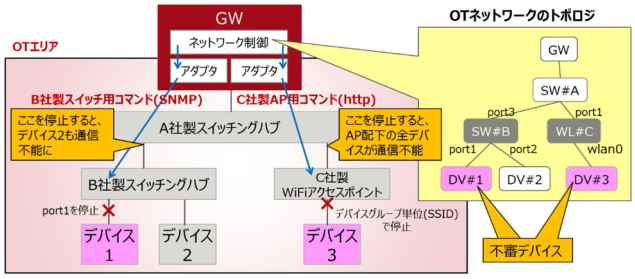

図 9 不審デバイスの通信遮断

6. 本方式で防御可能な脅威

図 10 は，提案方式の，様々な脅威に対する防御可能性を示す．脅威の分類は，主にコンシューマ向けの IoT セキュリティのガイドライン[9]を参照した．

多くの脅威は，仮想ネットワークによる通信元の限定および通信異常の検出・遮断，認証・アクセス制御・データ検証などのセキュリティ機能の補完によって，防御可能である．例えば，デバイス改竄は，デバイスに侵入し，ファームウェアを改竄して，誤動作させる脅威である．この場合，デバイスにセキュリティ機能がなくても，デバイスへの侵入をブロックするため，まず認証が実施される．認証をパスしてもアクセス制御，アクセス制御をパスしても，改竄用データの検証もパスしないと，攻撃に成功しない．このように，セキュリティ機能を多段適用することで，セキュリティ強度を向上させることが可能である．

一部の脅威は，システムだけで防止するのは困難である．例えば，盗聴は，GW とデバイス間の通信内容が第 3 者に盗まれる脅威である．これを防御するには，GW とデバイス間でエンドツーエンドの通信暗号化が有力であるが，エンドポイントであるデバイス側に暗号化機能がないと，実現不可能である．また，情報漏洩は，運用していたデバイスや GW を撤去し，廃却する際に，内部に保存していたデータが第 3 者に盗まれる脅威である．これは，GW 上のシステムがデータを保存する際に暗号化し，システム停止時には削除する方法が考えられるが，システムが異常終了すると，完全に削除するのが不可能な場合もある．したがって，システムだけでなく，物理的に破壊するなどの運用方法も含めた対策が必要である．

7. まとめ

本稿では，本来脆弱性が放置されたままの IoT デバイスの代わりに，GW がセキュリティ機能を補完実行することで，アプリケーションからの IoT デバイスの利用をセキュア化するセキュアデバイス仮想化というコンセプトを提案し，実現するための課題と解決方法を述べた．

IoT デバイスの管理やアプリケーション利用の容易化の目的で，インタフェースを共通化するという意味の，デバ

Copyright © 2018 by
The Institute of Electronics, Information and Communication Engineers and
Information Processing Society of Japan All rights reserved.

分類	脅威	内容	防御可否	備考
デバイス・GW・ネットワークの機能に関する脅威	盗難・破壊	現場に侵入し，デバイスを盗難，あるいは物理的に破壊.	×	堅牢化，固定，入退室管理や監視などシステム外の対策が必要.
	デバイス改竄	ネットワーク経由で，デバイスに侵入し，ファームを改変して，誤動作させる.	○	不正デバイスの通信遮断，認証・認可・ウィルスチェック適用により防御可能.
	不正利用	ネットワーク経由で，デバイスに侵入し，デバイスを勝手に操作する.	○	不正デバイスの通信遮断，認証・認可・ウィルスチェック適用により防御可能.
	DoS攻撃	不正にネットワーク接続した端末から大量のパケットを送信し，GW・デバイスの機能を利用不能にする.	○	不正デバイスの通信遮断により防御可能.
	ウィルス感染	ネットワーク経由で，デバイスをウィルス感染させて，デバイスを誤動作させる.	○	不正デバイスの通信遮断，認証・認可・ウィルスチェック適用により防御可能.
通信データに関する脅威	盗聴	現場に侵入し，電波やネットワーク機器から，GWとデバイス間の通信内容を盗む.	×	入退室管理や監視などシステム外の対策や，デバイスに暗号通信機能が必要.
	情報漏洩	GWを交換・廃棄する際に，内部に保存されているデータを盗む.	△	プラットフォームが保存するデータの暗号化により防御可能だが，完全に防御するには，耐タンパハードウェアも必要.
	不正データ送信	ネットワーク経由で，不正なデータを送信し，デバイスを誤動作・データ取得する.	○	不正デバイスの通信遮断，認証・認可・ウィルスチェック適用により防御可能.
	データ改竄	デバイスへの通信内容を改竄・送信し，デバイスを誤動作させる.	○	不正デバイスの通信遮断，認証・認可適用により防御可能.
	データ否認	ネットワーク経由で，データの送信元デバイスを詐称して，GWにデータを送信し，データを利用するサービスを誤動作させる.	○	不正デバイスの通信遮断，認証・認可適用により防御可能.

図 10 防御可能な脅威と対応するセキュリティ機能

イス仮想化のアイディアは，[10][11][12][13]などの先行研究がある．しかし，本稿で述べたように，仮想化を GW において実デバイスへのアクセスを一本化し，セキュリティ機能を補完し，セキュアなデバイスに見せかけるというセキュリティ観点で捉えた例はなかった．

一部の解決方法には，まだ課題が残っており，検討を続ける予定である．一方，試作開発も進めており，クローズドなネットワーク環境を構築し，実際のマルウェアを使用し，有効性を検証する予定である．また，実際の工場に適用し評価する計画も進めている．

なお，本稿では製造業を想定して議論を進めてきたが，管理の行き届いたエリアと，そうでないエリアとを分離してセキュリティを実現する場合に共通して適用可能な方式であり，他の領域への適用も並行して検討していく．

参考文献

[1] C. Kolias, G. Kambourakis, A. Stavrou, J. Voas. DDoS in the IoT: Mirai and Other Botnets. IEEE Computer. Vol. 50, Issue 7, pp.80-84, 2017.

[2] S. Mohurle, M. Patil. A Brief Study of Wannacry Threat: Ransomware Attack 2017. International Journal of Advanced Research in Computer Science. Vol. 8, No. 5, pp. 1938-1940, 2017.

[3] 情報処理推進機構．重大な経営課題となる制御システムのセキュリティリスク．https://www.ipa.go.jp/files/000044733.pdf．（参照 2018/6/28）

[4] 情報処理推進機構．制御システムユーザ企業の実態調査報告書．https://www.ipa.go.jp/files/000051551.pdf．（参照 2018/6/28）

[5] Industrial Internet Consortium. Industrial Internet of Things, Volume G4: Security Framework. http://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB-3.pdf. （参照 2018/6/28）．

[6] Cisco. The Cisco Connected Factory: Holistic Security for the Factory of Tomorrow. https://www.cisco.com/c/dam/en_us/solutions/industries/docs/manufacturing/cisco-connected-factory.pdf. （参照 2018/6/28）

[7] 佐野 健, 大谷 武, 中川 格, 角田 潤, 松倉 隆一. IoT の普及に向けたデバイス収容低コスト化方式. 電子情報通信学会 2017 年総合大会論文集. B-18-39. 2017.

[8] Y. Nishiguchi, A. Yano, T. Ohtani, R. Matsukura, J. Kakuta. IoT Fault Management Platform with Device Virtualization. In Proc. of IEEE 4th World Forum on Internet of Things, pp. 37-44, 2018.

[9] 日本ネットワークセキュリティ協会．コンシューマ向け IoT セキュリティガイド．http://www.jnsa.org/result/iot/data/IoTSecurityWG_Report_Ver1.pdf．（参照 2018/6/28）

[10] M. Eisenhauer, P. Rosengren, P. Antolin. HYDRA: A Development Platform for Integrating Wireless Devices and Sensors into Ambient Intelligence Systems. In Proc. of The Internet of Things: 20th Tyrrhenian Workshop on Digital Communications. pp. 367-373. 2010.

[11] P. L. Evensen, H. Meling. SenseWrap: A Service Oriented Middleware with Sensor Virtualization and Self-Configuration. In Proc. 5th International Conference on Intelligent Sensor, Sensor Networks and Information Processing (ISSNIP), pp. 261-266. 2009.

[12] D. Guinard, V. Trifa, S. Karnouskos, P. Spiess, D. Savio. Interacting with the SOA-Based Internet of Things: Discovery, Query, Selection, and On-Demand Provisioning of Web Services. IEEE Transaction on Service Computing. Vol. 3, No. 3, pp. 223-235. 2010.

[13] M. Caporuscio, P. G. Raverdy, V. Issarny. ubiSOAP: A Service-Oriented Middleware for Ubiquitous Networking. IEEE Transaction on Service Computing. Vol. 5, No. 1, pp. 86?98. 2012.

Copyright © 2018 by
The Institute of Electronics, Information and Communication Engineers and
Information Processing Society of Japan All rights reserved.