特集論文

IoTゲートウェイのセキュリティ技術

佐藤浩司*
平井博昭**
山口晃由***

Security Technologies of IoT Gateway

Koji Sato, Hiroaki Hirai, Teruyoshi Yamaguchi

要　旨

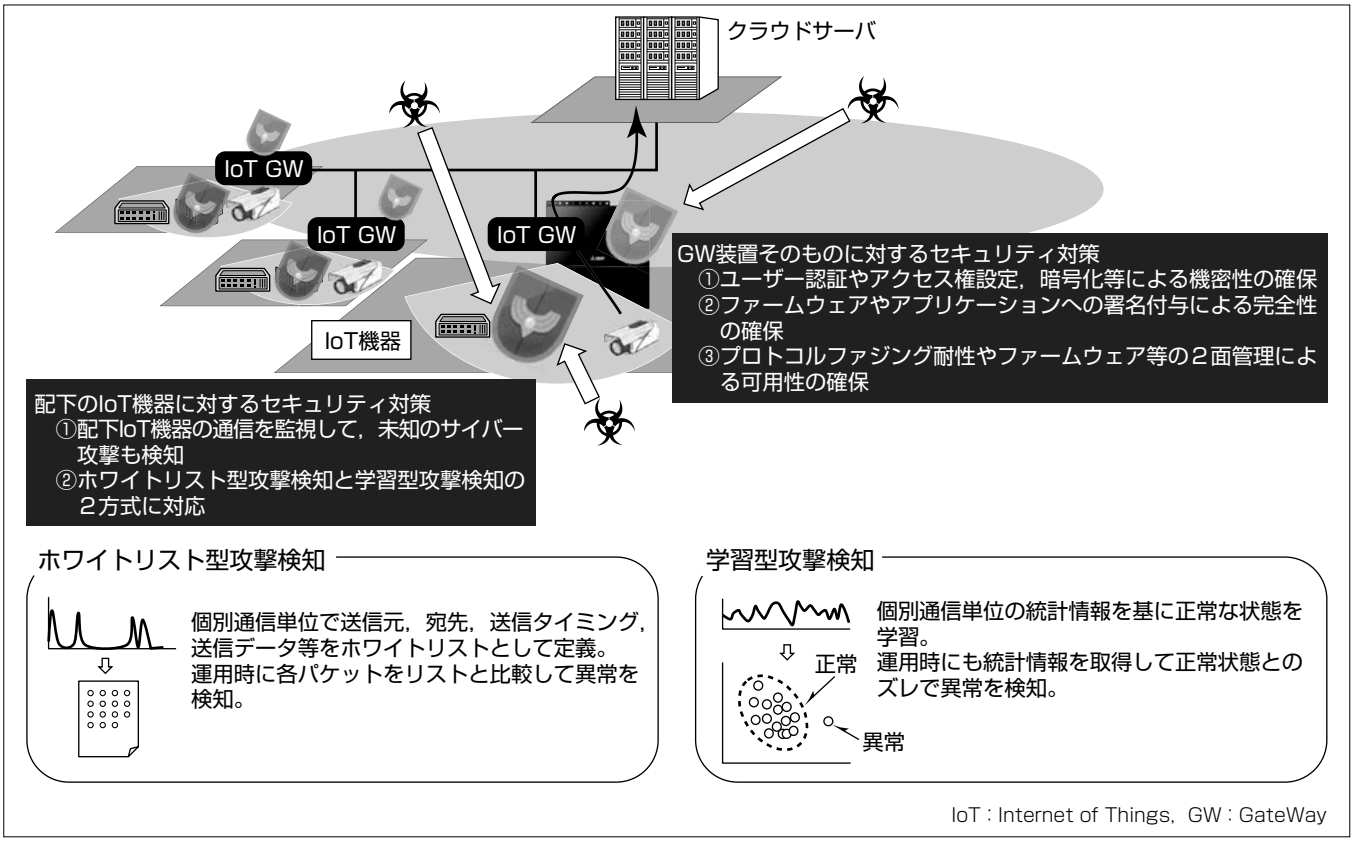
近年，デバイス機器から自動的に各種データを収集し，サービス価値／生産性／保守性などの向上を図るIoT(Internet of Things)システムが多数構築されている。

IoTシステムに接続されるIoT機器の数が急激に増加するにつれ，これらのIoT機器を標的としたサイバー攻撃の事例も増加している。処理性能等の制約によって十分なセキュリティ対策機能を持たないIoT機器や，初期パスワードのままであるなど適切な運用がなされていないIoT機器が多数ネットワークに接続されていることが攻撃事例増加の原因と考えられる。

このような状況のもと，脆弱(ぜいじゃく)なIoT機器をサイバー攻撃から守る仕組みの実現が，喫緊の課題となっている。

この課題の解決に向けて，三菱電機はセキュアなIoTシステム向けのゲートウェイ装置(IoT GW)を開発した。具体的には，GW装置そのものに対する脅威への対策として，機密性／完全性／可用性を確保する仕組みを搭載するとともに，配下のIoT機器を守るための仕組みとしてホワイトリスト型攻撃検知機能と学習型攻撃検知機能を開発した。未知の攻撃も検知できる可能性のある二つの攻撃検知機能によって，サイバー攻撃への対策を強化したIoTシステムの実現に貢献する。

今後，攻撃検知機能の改良を継続し，他のセキュリティ装置／サービスなどとの併用・連携を進めることで，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。



IoT GWのセキュリティ技術

IoT GWには，GW装置そのものに対するセキュリティ対策として機密性／完全性／可用性を確保する各種機能が実装されている。また，配下に接続されるセキュリティ的に弱いIoT機器をサイバー攻撃から守るために，攻撃検知機能を搭載している。IoT機器へ特別な機能を追加することなく，未知の攻撃も検知可能なホワイトリスト型と学習型の二つの攻撃検知方式に対応したことで，既存の多種多様なIoT機器のセキュリティ監視が実現できる。

*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
***同研究所(工博)

1. まえがき

近年，デバイス機器から自動的に各種データを収集し，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。IoTシステムに接続される機器(IoT機器)の数は，2017年に約200億個に達し，2020年には約300億個になると予想されている(1)。

IoT機器数が急激に増加するにつれ，IoTシステムへのサイバー攻撃事例数も増えている。2016年にはIoT機器に感染したマルウェア“Mirai”による大規模な分散型サービス妨害(Distributed Denial of Service：DDoS)攻撃が観測された。マルウェアに感染しボット化した14万５千台以上のIoT機器からのDDoS攻撃トラフィックは，ピーク時に１Tbpsを超える規模であったとされている(2)。

2016年に観測されたサイバー攻撃のパケット数は2015年比で約2.4倍であったが，このうちIoT機器を狙った攻撃は2015年比で約5.8倍に増加しており，攻撃全体の64％を占めていた(3)。また，ファイアウォールでブロックした通信のうち，“Mirai”が利用するtelnetポートへのアクセスは2015年から2016年で約6.4倍に増加したとの統計情報もあり，“Mirai”とその亜種が多数のIoT機器へ急激に感染を図った様子が見て取れる(4)。

IoT機器が攻撃者から狙われる理由としては，機器数が多いことに加え，パソコンなどのIT機器と比較してセキュリティ的に弱い場合が多いことが挙げられる。IoT機器がセキュリティ的に弱い理由としては，CPU処理性能等の制約によってセキュリティ対策機能が搭載できないこと，又は，運用開始後にファームウェアの最新化などの管理作業が省略されてしまうこと等が挙げられる。さらには，導入に際して守るべきセキュリティガイドラインが整備・徹底されていないためアカウント情報を初期値のままで運用開始する場合や，管理が十分に行き届かずマルウェアに感染しても長期間感知されずに運用継続される場合も多く，IoT機器は攻撃者から見て狙いやすい標的となっている。

このような状況のもと，IoT機器と外部ネットワークを接続するIoTゲートウェイ(IoT GW)には，配下の脆弱な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ている。当社が開発したIoT GWでは，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(Embedded Device Security Assurance)認証(5)のレベル１相当に対応するとともに，機密性／完全性／可用性を確保する仕組みを搭載することでIoT GW装置そのもののセキュリティを確保した。また，配下のIoT機器のセキュリティを確保するための仕組みとして，攻撃検知機能を実装した(6)。

本稿では，以下，IoTシステムでのセキュリティ脅威を**２章**で，IoT GW装置そのものに対するセキュリティ対策を**３章**で，最後に，配下のIoT機器を守るための技術として，IoT GW上に実装した攻撃検知機能について**４章**で述べる。

2. IoTシステムでのセキュリティ脅威

IoT機器の不適切な管理や，脆弱性への対策遅れを背景に，2016年頃からIoT機器に対するサイバー攻撃が多数観測されている。IPA(情報処理推進機構)から毎年発表されている情報セキュリティ10大脅威でも，2015年度にはランク外であったIoTを対象とする脅威が，2016年度に10位以内にランクインし，2017年度には順位を更に上げている(7)。

このような状況の中，2016年には国内外で多数の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2016年に公開された主な文書とその公開月を示す。

IoT機器に対するサイバー攻撃は，“Mirai”とその亜種のようにIoT機器をDDoS攻撃のためにボット化することにとどまらない。

表２に示すように，発電所や石油パイプラインなどの物理的なシステムに対して実際に行われたサイバー攻撃によって，設備の破壊やサービス停止といった深刻な被害がもたらされている。また，これ以外にも，医療機器，自動車，家電など様々な分野の機器に対する，サービスの妨害・停止・不正利用，データの漏えい・改竄(かいざん)・破壊，乗っ取り，不正操作などの攻撃が可能との報告もある(9)。また，最近ではIoT機器の計算リソースを不正に利用し，仮想通貨の発掘(マイニング)を行う攻撃も確認されている(10)。

表１．2016年に公開されたIoTセキュリティ関連文書

機関名／団体名： 公開資料名	公開月
【国内】	
IPA(情報処理推進機構)： つながる世界の開発指針	３月
IPA(情報処理推進機構)： IoT開発におけるセキュリティ設計の手引き	５月
JNSA(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	６月
IoT推進コンソーシアム： IoTセキュリティガイドライン ver1.0	７月
NISC(内閣サイバーセキュリティセンター)： 安全なIoTシステムのためのセキュリティに関する一般的枠組み	８月
【海外】	
GSMA(GSM Association)： GSMA IoT Security Guidelines	２月
NIST(米国国立標準技術研究所)： NIST Special Publication 800－183 Networks of 'Things'	７月
IIC(Industrial Internet Consortium)： Industrial Internet of Things, Volume G4：Security Framework	９月
IoT Security Foundation： IoT Security Compliance Framework	12月

出典：IPA「情報セキュリティ白書2017」(8)の表から抜粋

表２．IoT機器への攻撃事例

発生	対象機器	事象
2008年８月	石油パイプライン	不正制御によって破壊
2010年９月	核燃料施設	不正制御によって稼働停止
2014年６月	電子交通標識	不正制御によってサービス停止
2015年７月	IP電話交換機	不正利用
2016年11月	ビル空調設備	不正制御によって空調停止
2016年12月	変電所	不正制御によって停電

表3．IoTでの10大脅威[11]

No.	脅威
1	安全でないWebインタフェース
2	不十分な認証と許可
3	安全でないネットワークサービス
4	通信暗号化の欠如
5	プライバシーの侵害
6	安全でないクラウドインタフェース
7	安全でないモバイルインタフェース
8	不十分なセキュリティ設定項目
9	安全でないソフトウェアとファームウェア
10	弱い物理的セキュリティ

OWASP(Open Web Application Security Project)によれば，IoTでの10大脅威は，**表3**のとおりである[11]。

IoT GWは，GW装置そのものでのこのような脅威への対策を行う必要があるのと同時に，これらの脅威に十分対処できないIoT機器が配下に接続されることも想定する必要がある。

3. IoT GWのセキュリティ対策

IoT GWでは，GW装置そのものに対する脅威への対策として，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相当のソフトウェア開発セキュリティ評価(Software Development Security Assessment：SDSA)，機能セキュリティ評価(Functional Security Assessment：FSA)，通信ロバストネス試験(Comminication Robustness Testing：CRT)に対応した。SDSAによってソフトウェア開発の各フェーズでのセキュリティ評価を，FSAによって機能や初期設定等を対象としたセキュリティ評価を，また，CRTによって通信堅牢(けんろう)性を確認している。

また，IoT GWでのC(Confidentiality：機密性)，I(Integrity：完全性)，A(Availability：可用性)，それぞれの観点の個別対策は次のとおりである。

3.1 機　密　性

IoT GWは，FSAレベル１に規定されるユーザー認証要件を満たす。設定用GUI(Graphical User Interface)へのアクセスなど，公開される全てのサービスへのアクセスでユーザー認証を必須としている。また，IoT GWから装置外部へ取り出せる重要データ(設定情報など)は，必ず暗号化する。

IoT GWには，Java(注1)バンドル形式のIoTアプリケーションを搭載することができる。IoT GWは，IoTアプリケーションや，配下のIoT機器からの通信を暗号化するVPN(Virtual Private Network)機能を提供する。この他，IoTアプリケーションからデータ暗号化や，TLS(Transport Layer Security)による暗号化通信の利用も可能である。

(注１)　Javaは，Oracle Corp.の登録商標である。

3.2 完　全　性

3.2.1 ファームウェアの完全性

EDSAレベル１相当のセキュリティを確保したIoT GW用ファームウェアに対し，RSA(Rivest-Shamir-Adleman cryptosystem)公開鍵暗号を用いた署名アルゴリズムによって当社が署名を生成して付加している。IoT GWにはプロセッサ内の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を搭載しており，ファームウェアに付与された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が起動される。これによって，起動するファームウェアの完全性を担保している。

3.2.2 アプリケーションの完全性

IoTアプリケーションはファームウェアとは一体化せず，各IoTアプリケーションの単位で個別にIoT GW装置へ搭載できる。このため，Javaバンドルについても，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限り，インストール／起動を許可することでアプリケーションの完全性を担保している。

3.3 可　用　性

IoT GWは，FSAレベル１で要求されるプロトコルファジング攻撃への耐性を備える。また，ファームウェアや設定情報のデータ破壊に備えたフラッシュメモリ上での２面管理や，IoTアプリケーションのリソース利用制限によるGW基本機能の優先動作などによって，可用性の向上を図っている。

4. IoT機器攻撃検知機能

IoTシステムでは，急激に増加しつつある多種多様なIoT機器に対して，機器個別の対策を漏れなく実施することは困難である。このため，IoT機器が様々なサイバー攻撃を受けることを前提として，それらの攻撃を早期に検知し，迅速に対処できるようにすることが有効と考えられる。このため当社はIoT GWに配下IoT機器のための攻撃検知機能を搭載した。次に，当社が考える攻撃検知機能要件と攻撃検知方式を述べる。

4.1 攻撃検知機能要件

攻撃検知機能に対する要件としては，監視対象となるIoT機器に関する要件と，検知対象となる攻撃に関する要件の２種類がある。

IoT機器に関する要件は，新規に市場投入されるIoT機器を含めて，多種多様なIoT機器を監視対象にできることである。また検知対象となる攻撃に関する要件は，将来的に新たに現れる可能性がある攻撃も検知できることである。

IoT機器に関する要件で，既存機器に加えて新規に市場投入されるIoT機器も含める理由としては，これらの新しい機器が備えるサイバー攻撃対策が，継続して巧妙化する攻撃手法に対して将来にわたって100％の効果を保証でき

るとは限らないことが挙げられる。また，将来にわたって効果が見込まれる対策を搭載している場合でも，多層防御の観点から監視対象にできることが望ましい。

4.2　攻撃検知方式

攻撃検知の方式としては，大きくブラックリスト方式とホワイトリスト方式が存在する。攻撃そのものや攻撃から直接的に生じる振る舞いを定義しておき，これと比較することで攻撃を検知するのがブラックリスト方式である。一方ホワイトリスト方式では正常な振る舞いを定義しておき，これを比較し，不一致が発生したことをもって異常(＝攻撃)の発生として検知する。

ブラックリスト方式は，攻撃そのものや攻撃から直接的に生じる振る舞いを定義しておくことができない未知の攻撃の検知には不向きである。一方ホワイトリスト方式では正常状態を定義するだけで，攻撃について事前に定義する必要がないため未知の攻撃を検知できる可能性がある。

これらの特性から，IoT GWに搭載すべき攻撃検知機能として，ホワイトリスト方式を採用した。

また，先に述べた監視対象とするIoT機器に関する要件を考慮すると，既存機器も監視対象にする必要があるが，監視のためにIoT機器へ特別な機能を追加することはできないため，IoT機器の通信トラフィックを監視し，そこから攻撃を検知する方針とした。

次に，IoT GW上に実装した二つの攻撃検知機能について概要を述べる。

4.2.1　ホワイトリスト型攻撃検知機能

通信トラフィックを対象とするホワイトリスト型攻撃検知機能の基本的な機能ブロック図を**図1**に示す。

IoT GWの通信処理部で，監視対象とする通信フローをパケットキャプチャによって捕捉する。取得されたキャプチャデータは，ホワイトリスト定義との照合を行う照合エンジンに入力される。照合エンジンは，あらかじめ設定されたホワイトリスト定義と入力データを照合し，ホワイトリスト定義に合致しない入力データを検知する。検知情報は検知通知インタフェース部を介して通知先へと通知される。また，ホワイトリスト定義はリスト更新インタフェース部を介して更新可能とする。

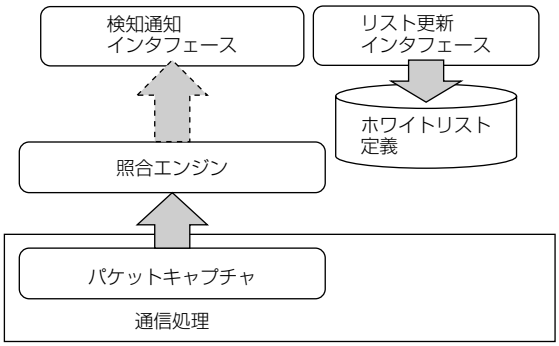


図1．IoT GWでのホワイトリスト型攻撃検知

攻撃検知に用いるホワイトリスト定義には，単純なパケットフィルタリングで用いられる送信元・宛先の各IP(Internet Protocol)アドレス・ポート番号とプロトコル種別から構成される5タプルで規定されるリストに加えて，通信周期やプロトコル依存のコマンド種別，コマンド順序なども定義可能にした[12]。

また，適用するIoTシステムによっては，単一のホワイトリスト定義の適用が難しい場合もあるため，システムの動作状態に応じて複数のホワイトリスト定義を切り替えることで，リアルタイム性を確保しつつ攻撃検知を可能にした[13]。

4.2.2　学習型攻撃検知機能

先に述べたホワイトリスト型攻撃検知は，ホワイトリスト定義の内容を見ても分かるように，対象とするIoT機器の通信がタイミングや順序も含めて厳密に規定できる場合に最も効果的な方法である。一方で，オペレータなど人間の操作が介在し，その操作のタイミングや内容に応じて通信のタイミングや内容が変化するシステムでは，ホワイトリストを厳密に定義すること自体が適さない場合がある。このようなシステムでは，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学習させることで，ホワイトリスト定義に相当する“正常状態を表すモデル”を構築し，これに基づき異常な振る舞いを検知することが効果的である[14]。このような仕組みで攻撃を検知する機能をここでは学習型攻撃検知機能と呼ぶ。**図2**にホワイトリスト型攻撃検知と学習型攻撃検知の使い分けを示す。

学習型攻撃検知機能もまた，正しい状態を定義する方式であるためホワイトリスト方式の一種であり，未知の攻撃も検知可能である。学習型攻撃検知で構築される正常状態を表すモデルは，通常のホワイトリストと比較すると，定義が曖昧(あいまい)である短所を持つが，一方で，既知の攻撃については，正常状態からの差異の程度に応じて，原因推定が可能となる点が長所として挙げられる。

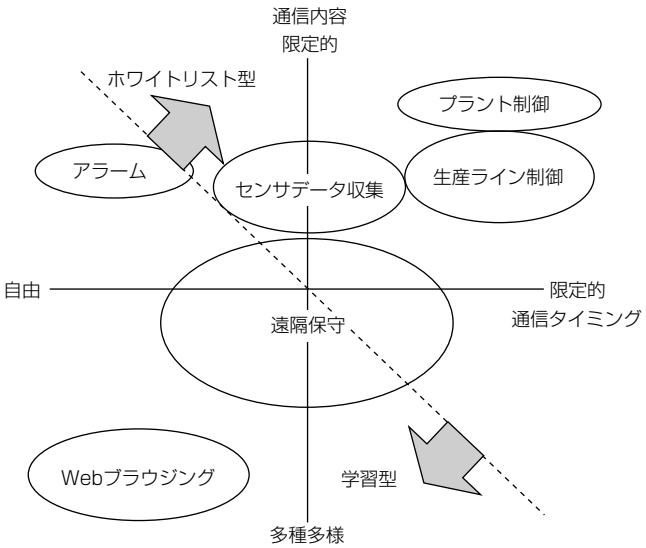


図2．ホワイトリスト型と学習型の使い分け

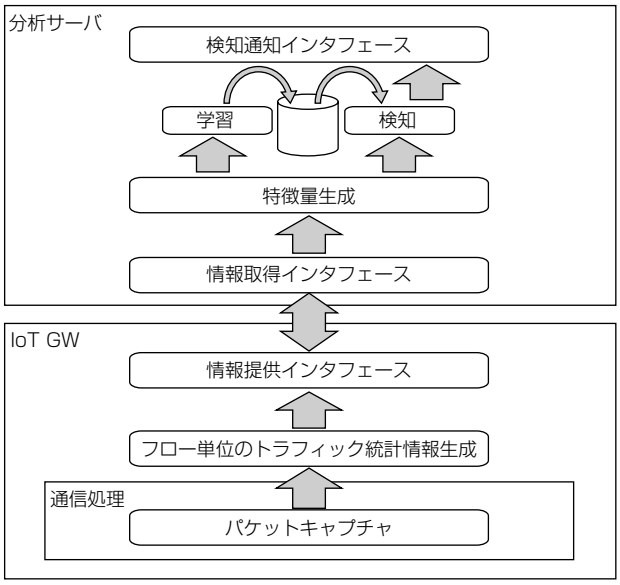


図３．学習型攻撃検知機能の機能配備例

図３は学習型攻撃検知機能の機能配備の一例を示す。IoT GWは，IoT機器の送受信トラフィックに関するフロー単位の統計情報を周期的に取得し，これを分析サーバが取得，特徴量化した上で学習・検知に用いる。

このようにIoT GWは攻撃検知機能で，自らが専用のネットワークセンサとして振る舞う。

4.2.3　両方式の併用に向けて

IoT GW上にホワイトリスト型攻撃検知機能と学習型攻撃検知機能をそれぞれ個別に実装して機能確認を行ったが，今後に向けては，適用先ごとの単純な使い分けにとどまらず，両方式を併用して効果的に連携させることも含めて攻撃検知機能としての機能を最大限に活用できるよう検討を進めていく。

5. むすび

急激に普及が進むIoTシステムでは，サイバー攻撃対策が不十分な機器も多数使われている。実際にこれらの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。このような状況に対する解決策の一つとして期待されているのが，GW装置などによる配下IoT機器のセキュリティ確保である。本稿では，この実現に向けた当社の取組みとしてIoT GWのセキュリティ技術について述べた。

今後も，他のセキュリティ装置やセキュリティサービスなどとの併用・連携を進め，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。

この研究の一部は，総合科学技術・イノベーション会議の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(国立研究開発法人 新エネルギー・産業技術総合開発機構))によって実施された。

参考文献

(1) 総務省：平成29年版情報通信白書 (2017)
(2) OVH：The DDoS that didn't break the camel's VAC (2016)
https://www.ovh.com/world/news/articles/a2367.the-ddos-that-didnt-break-the-camels-vac
(3) 内閣 サイバーセキュリティセンター サイバーセキュリティ戦略本部：次期サイバーセキュリティ戦略の検討について，第16回会合 資料１ (2018)
https://www.nisc.go.jp/conference/cs/dai16/pdf/16shiryou01.pdf
(4) 内藤陽介：サイバーセキュリティ傾向分析レポート2017，第257回NRIメディアフォーラム資料 (2017)
https://www.nri.com/jp/event/mediaforum/2017/pdf/forum257.pdf
(5) ISASecure：EDSA-311 ISA Security Compliance Institute-Embedded Device Security Assurance-Functional Security Assessment(FSA) v1.4 (2010)
(6) 大野聖信，ほか：IoTシステム対応三菱通信ゲートウェイ，三菱電機技報，**91**，No.6，325～328 (2017)
(7) 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2018 (2018)
https://www.ipa.go.jp/security/vuln/10threats2018.html
(8) 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 (2017)
(9) 独立行政法人 情報処理推進機構(IPA)：顕在化したIoTのセキュリティ脅威とその対策 (2017)
https://www.ipa.go.jp/files/000059579.pdf
(10) トレンドマイクロ：つながる時代の脅威に対して企業がいま取り組むべきIoTセキュリティとは？【前編】(2018)
https://www.trendmicro.com/jp/iot-security/special/20148
(11) Open Web Application Security Project(OWASP)：Internet of Things Top Ten (2014)
https://www.owasp.org/images/7/71/Internet_of_Things_Top_Ten_2014-OWASP.pdf
(12) 中井綱人，ほか：プラント制御システム向けホワイトリスト型攻撃検知機能の設計，SCIS2016 2B2-4 (2016)
(13) 山口晃由，ほか：産業制御システムにおける侵入検知手法の調査と検討，SCIS2015 2A4-3 (2015)
(14) 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 (2016)
http://www.nedo.go.jp/content/100863673.pdf