IoTシステムのセキュリティ

IoT System Security

梅﨑　一也　UMEZAKI, Kazuya

近年のIoT（Internet of Things）機器の急速な増加に伴い，IoT機器を標的としたサイバー攻撃，セキュリティインシデントも急増している。このため，国内外でIoTセキュリティに関する規格やガイドラインの整備が進められている。富士電機では，IoTシステムへの脅威に対して，IoTセキュリティに関する規格やガイドラインに即したセキュリティポリシーを策定し，技術的対策，物理的対策，組織的対策，人的対策を実施することによって，安全・安心に利用できるIoTシステムを構築している。

The current rapid growth of the Internet of Things (IoT) leads to a significant increase in cyberattacks and security incidents on the IoT devices. To address the IoT security risks, efforts to produce standards and guidelines has been progressing in Japan and other countries. Fuji Electric has established the information security policy based on the IoT security standards and guidelines and takes technical, physical, organizational, and personnel measures to build IoT systems that are secure and safe from their threat.

1　まえがき

近年，IoT（Internet of Things）機器は急速に増加しており，2020年には約300億台のIoT機器がインターネットに接続されると予測されている[1]。これに伴い，IoT機器を標的としたサイバー攻撃，セキュリティインシデントも急増している。このため，国内外でIoTのセキュリティに関する規格やガイドラインの整備が進められている。

この状況を踏まえ，富士電機では，IoTのセキュリティに関する取組みを進めている。

本稿では，IoTシステムのセキュリティの課題や脅威の事例，国内外のガイドラインなどを踏まえたIoTのセキュリティ対策の考え方，および富士電機における取組みについて述べる。

2　IoTのセキュリティ動向

2.1　IoTシステムのセキュリティの課題

IoTとは，“情報社会のために，既存もしくは開発中の相互運用可能な情報通信技術により，物理的もしくは仮想的なモノを接続し，高度なサービスを実現するグローバルインフラ[2),3)]”とされており，次のようなことが期待されている[3)]。

(a)　モノがネットワークにつながることで，迅速かつ正確な情報収集，ならびにリアルタイムでの機器やシステムの制御が可能になる。

(b)　異なる分野の機器やシステムが相互に連携し，新しい機能が提供可能になる。

IoTのセキュリティ上の課題として次の事項が挙げられる[3)]。

○多様な機器やシステムが接続されていることによる，脅威の影響範囲の広さ

○多様な機器やシステム間でのセキュリティに対する考え方や要件の違い

○IoT機器の機能・性能の制約に伴う，取りうるセキュリティ対策の制限

○IoT機器に対する監視の不十分さ

○IoT機器の長いライフサイクル

このように，IoTはつながることにより価値を生む反面，従来はつながっていなかった装置や機器がインターネットにつながることによって，これらの機器がサイバー攻撃を受けるなどのセキュリティ脅威が増加することが懸念される。

2.2　IoT機器へのセキュリティ脅威の事例

IoT機器に対するセキュリティインシデントとしては，次のような事例が知られている[3)]。

(a)　インターネットに接続されたWebカメラや，HEMS（Home Energy Management System）が，設定不備などの原因により，外部からアクセス可能になっていた。

(b)　自動車のマルチメディアシステムの脆弱（ぜいじゃく）性を攻撃することにより，運転に影響を及ぼす不正な遠隔操作が可能になっていた。

いずれも，インターネットあるいはWi-Fi[注]など外部との接続経路から不正アクセスが行われている。不正アクセスが成功した原因としては，機器の利用者が適切な設定・管理をしていなかったこと（開発・保守用のインタフェースによるアクセスが可能のままであった，パスワードがデフォルトのまま変更されていなかったなど），およびIoT

〈注〉Wi-Fi：Wi-Fi Allianceの商標または登録商標

機器に脆弱性があったことが挙げられる。

IoT 機器が乗っ取られると，それを踏み台にしてさらに内部に侵入されたり，他の攻撃に使用されたりする恐れがある。2016 年 9 月には，IoT 機器をターゲットにしたマルウェア“Mirai”ボットネットによる複数の DDoS（分散型サービス妨害）攻撃が行われ，米国東海岸全域でインターネット利用に大混乱が起きるという事例が発生している。

3　IoT のセキュリティ対策

IoT のセキュリティについては，国内外でセキュリティに関する規格やガイドラインが策定されている。主なものを**表 1** に示す。

これらのセキュリティに関する規格・ガイドラインにおける IoT のセキュリティへのアプローチはさまざまであるが，基本的な考え方は次のとおりである。

⑴　リスク分析

守るべき対象を特定し，想定される脅威とその影響を分析する。

⑵　セキュリティ対策

リスク分析の結果を踏まえ，重要性に応じて脅威に対する対策を決定して実施する。

3.1　リスク分析

リスク分析においては，システム構成の明確化，情報資産の特定，脅威分析を実施する。

⑴　システム構成の明確化

規格・ガイドラインによって若干の差異はあるが，IoT システムは，**図 1** に示すように四つの階層に分類される。

これらの各階層において，どのような機器やシステムがあり，相互にどのように連携（情報交換）するかを分析し，文書化する。

表 1　IoT のセキュリティに関する規格・ガイドライン

区　分	発行元*	規格・ガイドライン名称	発行日
海　外	oneM2M	oneM2M技術仕様書 セキュリティ技術の適用	2016-03（V1.0.0） 2018-02（V2.0.1）
	GSMA	GSMA IoT Security Guidelines	2016-02（V1.0） 2017-10（V2.0）
	IIC	IIC Security Framework	2016-09（V1.0）
	CSA	IoTの早期導入者のための セキュリティガイダンス	2016-02（V1.0）
	OTA	OTA IoT Trust Framework	2016-03（V1.0） 2017-06（V2.5）
国　内	IPA	IoT開発におけるセキュリティ設計の手引き	2016-05（初版） 2018-04
	IoT推進コンソーシアム	IoTセキュリティガイドライン	2016-07（V1.0）

＊oneM2M　：電気情報通信分野におけるM2M/IoT技術の国際標準化団体
GSMA　：GSM Association 携帯電話システムの一種であるGSM方式の業界団体
IIC　：Industrial Internet Consortium インダストリアルIoTの産業実装を推進する業界団体
CSA　：Cloud Security Alliance クラウドのセキュリティに特化して活動する非営利団体
OTA　：インターネットに関する国際非営利団体Internet Socieryの下部組織
IPA　：情報処理推進機構

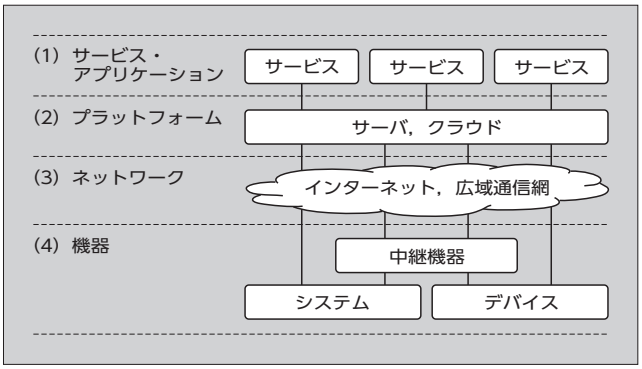

図 1　IoT システムの階層構造

⑵　情報資産の特定

IoT システムの構成要素に含まれる情報，機能，資産を洗い出した上で，重要性によって保護すべき対象を特定する。

⑶　脅威分析

脅威分析には，既存の分析手法が適用されている。分析手法の一つである STRIDE では，**表 2** に示す脅威のタイプに対して分析し，脅威の影響を受ける可能性がある箇所（脆弱性）を抽出する[(3)〜(5)]。

抽出した脅威に対して，影響度を分析する。分析手法の一つである DREAD では，**表 3** に示す評価軸によって脆

表 2　STRIDE における脅威のタイプと例

脅威のタイプ	脅威の例
Spoofing （成り済まし）	各種IDや資格情報（パスワードなど）を不正入手されることにより，IoT機器やユーザに成り済まされる
Tampering （改ざん）	IoTシステムにおけるデータの収集，加工，移送，保存のいずれかの段階において，データが書き換えられる
Repudiation （否認）	不正な機器が接続され，不良なデータがシステムに供給されることによりシステムが正常運転できなくなる
Information Disclosure （情報漏えい）	IoTシステムにおけるデータの収集，加工，移送，保存のいずれかの段階において，データに許可されていないアクセスが行われる
Denial of Service （サービス拒否）	IoTシステムの構成要素に対して大量データ送信が行われ，システムの機能が使用できない状態になる
Elevation of Privilege （特権の昇格）	IoTシステムの機能やデータに対して，本来権限を持たない機器やユーザがアクセスできてしまう

表 3　リスク評価手法 DREAD

影響の評価軸	説　明
Damage potential （潜在的損害）	脆弱性を攻撃された場合の損害の程度
Reproducibility （再現性）	攻撃の再現（成功）のしやすさ
Exploitability （攻撃利用可能性）	攻撃への悪用のしやすさ
Affected users （影響を受けるユーザ）	攻撃の影響を受けるユーザの規模
Discoverability （検出可能性）	脆弱性が攻撃者に発見される可能性

表 4　セキュリティ対策の分類

対策の種類	対策の例
技術的対策	利用者識別・認証，機器の識別・認証，アクセス制御，ファイアウォール，侵入検知システム，通信路暗号化，データ暗号化，ログ収集・分析 など
物理的対策	情報処理区域の管理，情報資産の盗難防止，電子媒体などの管理，情報資産の削除・廃棄管理 など
組織的対策	組織体制の整備，取扱規定などに基づく運用，システム監視体制，脆弱性対応体制，インシデント対応体制 など
人的対策	従業員の意識向上，教育・訓練 など

弱性への攻撃の影響を評価する。[4]

3.2　セキュリティ対策

リスク分析の結果を踏まえて，影響が大きなものについてセキュリティ対策を選定し，実施する。

セキュリティ対策は，**表 4** に示すように，技術的対策，物理的対策，組織的対策，人的対策の 4 種類に分けられる。

4　富士電機の IoT のセキュリティへの取組み

4.1　富士電機 IoT プラットフォーム

富士電機 IoT プラットフォームは，**図 2** に示すように，現場のフィールド機器を，エッジコントローラと呼ばれる IoT 機器をゲートウェイとして，クラウド上のサービスと連携する構成である。

この IoT プラットフォームのセキュリティのために，リスク分析結果および各種ガイドラインを踏まえてセキュリティポリシーを策定し，それに基づいて**図 3** に示すような対策を推進している。

4.2　IoT システムのセキュリティポリシー

IoT システムのセキュリティに関する社内基準を策定した。この基準は，IoT ビジネスにおいて富士電機が提供する IoT システムおよび，その開発，構築，運用，保守などビジネスのために必要な業務，ならびにそれら業務に使用する PC や電子記憶媒体とそれらを取り扱う全ての従業員を適用対象としている。

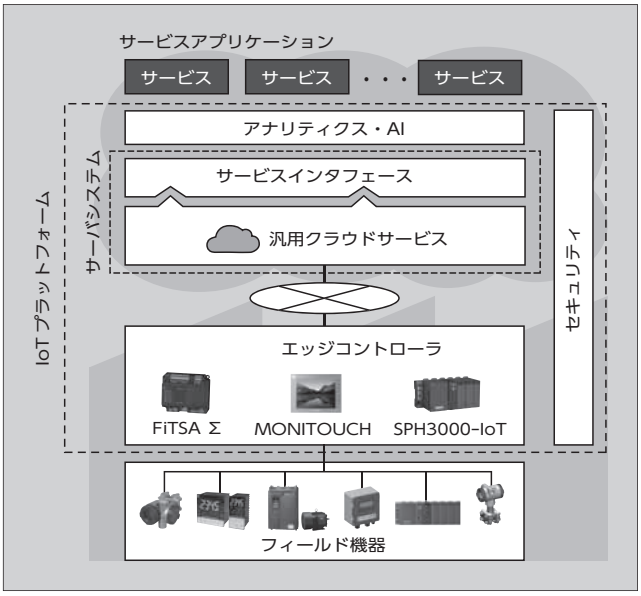

図 2　富士電機 IoT プラットフォームの構成

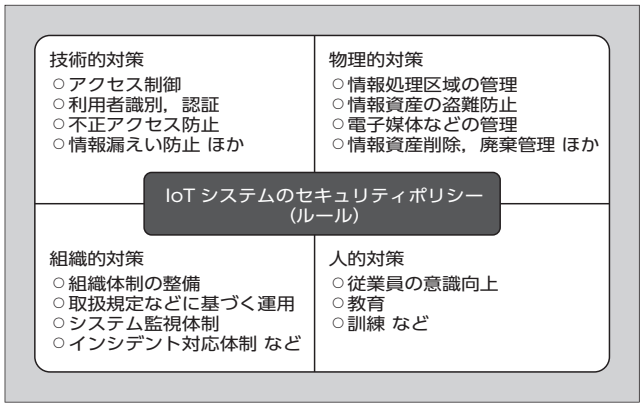

図 3　富士電機における IoT のセキュリティポリシー

この基準を策定するに当たり，クラウドセキュリティの標準規格である ISO/IEC 27017：2015[6] および IoT セキュリティガイドライン[3] をはじめとするセキュリティ規格・ガイドラインの考え方を取り込んでいる。

4.3　技術的・物理的セキュリティ対策

(1)　汎用クラウドサービスにおける対策

IoT プラットフォームにおけるサーバシステムは，外部の汎用クラウドサービス上に構築する。この汎用クラウドサービスは，そのセキュリティ対策状況を確認した上で選定し，使用している。具体的には，ISO 27001 および ISO 27017 の認証を取得し，CIA（Confidentiality：機密性，Integrity：完全性，Availability：可用性）を確保するために次のような対策を行っている。

(a)　データセンターとしての対策

侵入防止，入退室管理，操作証跡管理など

(b)　ネットワークへの対策

ファイヤウォール，侵入検知，通信暗号化，冗長化など

(c)　物理ストレージや物理サーバへの対策

アクセス制限，データ暗号化，ウィルス感染防止，操作証跡管理，冗長化など

(d)　仮想化基盤への対策

ネットワーク仮想化による分離，脆弱性情報対応，オートフェールオーバなど

(2)　クラウド上のサーバシステムやサービスへの対策

富士電機が開発しているサービスインタフェースやアナリティクス・AI などの IoT プラットフォームは，次に示す従来のサーバ・クラウドアプリケーションのセキュリティ対策を適用している。

(a)　脆弱性の作りこみの回避

セキュアソフトウェア開発のガイドラインに準拠など

(b)　不正アクセスの防止

サービス使用ユーザの識別・認証，アクセス制御，重

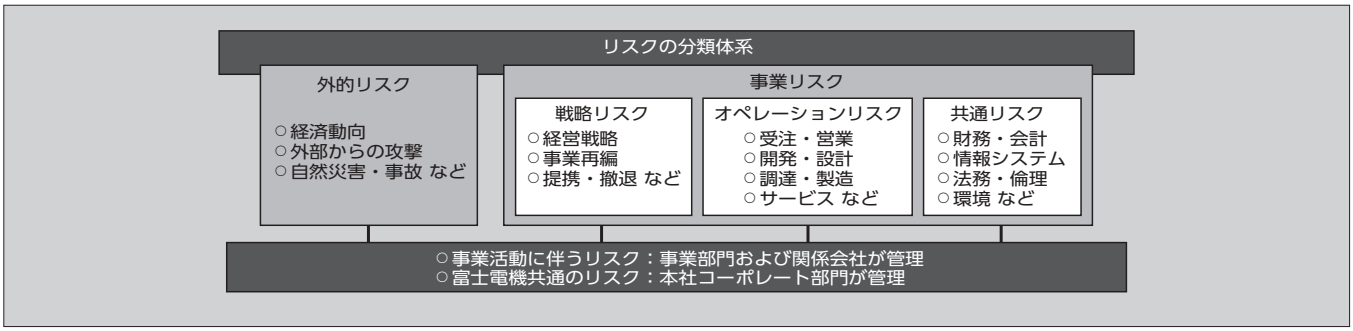

図 4　富士電機のリスク分類体系と管理体制

要データの保護など

(3)　エッジコントローラと通信における対策

クラウド上の IoT プラットフォームにアクセスを行うエッジコントローラについては，次のように識別し，認証および通信暗号化を実施することで，不正アクセスを防止している。

(a)　通信経路の接続時認証および暗号化

(b)　ネットワークとの接続点（ファイヤウォール，VPN など）における侵入防止

(c)　サーバシステムとエッジコントローラ間の相互認証

(d)　サーバシステムへのアクセス制御

(e)　サービスインタフェースによるデータ送信元エッジコントローラの機器認証

4.4　組織的・人的セキュリティ対策

(1)　富士電機のリスクマネジメント体制

富士電機は，2006 年 5 月に策定した“富士電機リスク管理規程”に基づき，リスクを組織的，体系的に管理している。情報セキュリティ対策にもリスクマネジメントの一環として取り組んでいる（**図 4**）。

情報セキュリティの推進においては，富士電機は，機密情報や個人情報を適切に保護するため，情報セキュリティに関する方針および規程類を整備・展開し，毎年社員の教育を行うなどの情報セキュリティの強化を図り，情報漏えいの防止に努めている。

顧客の重要な情報や個人情報を取り扱う，高いレベルの情報セキュリティ管理が必要な部門は，ISMS（情報セキュリティマネジメントシステム）認証やプライバシーマーク認定などの外部認証を取得している。

(2)　Fe−CSIRT

標的型サイバー攻撃，制御システムや IoT の脆弱性に対する攻撃など，多様化，高度化するセキュリティ脅威への対応力，防衛力の強化を図るため，Fe−CSIRT（Computer Security Incident Response Team）を 2017 年 4 月に設置した。

富士電機の IT 戦略部門の一組織として，既存の情報セキュリティマネジメント体制において，監視，監査，教育などを主導する事務局と共同で，富士電機グループ内で発生する情報セキュリティインシデントへの対応および予防を担っている。

IoT についても，この Fe−CSIRT 体制に準じる形でインシデント対応のための組織および運用体制を構築している。

5　あとがき

IoT システムのセキュリティについて述べた。IoT 機器の増加に伴い，サイバー攻撃やセキュリティインシデントも増加している。富士電機では，IoT システムへの脅威を踏まえたセキュリティポリシーを策定し，体制面とメカニズム面からの対策を実施することによって，安全・安心に利用できる IoT システムを構築している。

サイバー攻撃は日々進化しているため，セキュリティ対策は継続的な取組みが不可欠である。今後も引き続き，IoT システムのセキュリティを確保するための技術開発を進めていく所存である。

参考文献

(1)　平成30年版情報通信白書. 総務省.

(2)　ITU−T Y. 2060（4000），Overview Of Internet Of Things. 2012.

(3)　IoTセキュリティガイドラインVer1.0. IoT推進コンソーシアム・総務省・経済産業省. 2016.

(4)　IoT早期導入者のためのセキュリティガイダンス. Cloud Security Alliance. 2015.

(5)　IIC Security Framework. 2016.

(6)　ISO/IEC 27017：2015.

梅﨑　一也

IoT システムに関するセキュリティ技術開発に従事。現在，富士電機株式会社技術開発本部イノベーション創出センターデジタルプラットフォーム開発室組込システム研究部主査。

富士電機

Innovating Energy Technology