「IoT のセキュリティ

～IoT セキュリティ対策を進めるために、リスクから
IoT セキュリティ関連団体の取組み動向を踏まえた対策を考える～」

兜森　清忠　氏

■IoT セキュリティの課題

従来の Information Technology（IT）は、業態に関わらずクライアント／サーバー通信が主である共通のシステムが多いのに対し、IoT は利用するレイヤー機能（アプリケーション、プラットフォーム、ネットワーク、デバイス・センサー）が業種ごとに異なり、エンドポイントとなるセンサーやネットワーク経路も多様化している。

さらに IT は、個人情報、知的財産等機密情報を多く保有し機密性が重視される一方、応答時間の長短はそれほど重視されず、マシンの更新頻度も比較的短期である。他方 Operational Technology（OT）は生産ライン／インフラの停止、応答遅延による影響が大きいため機密性よりも可用性が重視され、パッチをあてることによるレスポンスタイム遅延等を避けるため十分なセキュリティ対策が講じられないこともある。機密情報を多く保有し、システム停止、レスポンス遅延による影響も大きい IoT デバイスには機密性も可用性も求められることからセキュリティ対策を一層困難にしている。

■主なガイドラインの動向

内閣サイバーセキュリティセンター（NISC）の「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について」（平成 28 年 8 月）は、安全な IoT システムが具備すべき一般要求事項としてのセキュリティ要件の基本的要素を明らかにしたもので、「IoT システムは、従来の情報セキュリティの確保に加え、新たに安全確保が重要」であり、「セキュリティ・バイ・デザインの思想で設計・構築・運用されることが不可欠」としている。基本原則にはシステム構築、運用・保守の各段階の要件定義で必要な項目が列挙されており、これをブレークダウンし実装することが重要である。またここでは、個別分野固有の要求事項を追装する 2 段階のアプローチが適切とされている通り、IoT のセキュリティを考える際には分野別に、分野のなかでもユースケース、ビジネスモデルごとに考えていく必要がある。

IoT 推進コンソーシアム、総務省、経済産業省が公開した「IoT セキュリティガイドライン Ver1.0」（平成 28 年 7 月）では、IPA（(独）情報処理推進機構）の「つながる世界の開発指針」の 5 つのフェーズ（方針、分析、設計、保守、運用）に「構築・接続」を加え、開発のほかネットワークに接続する際に考えるべきことを盛り込んだ（図 1）。

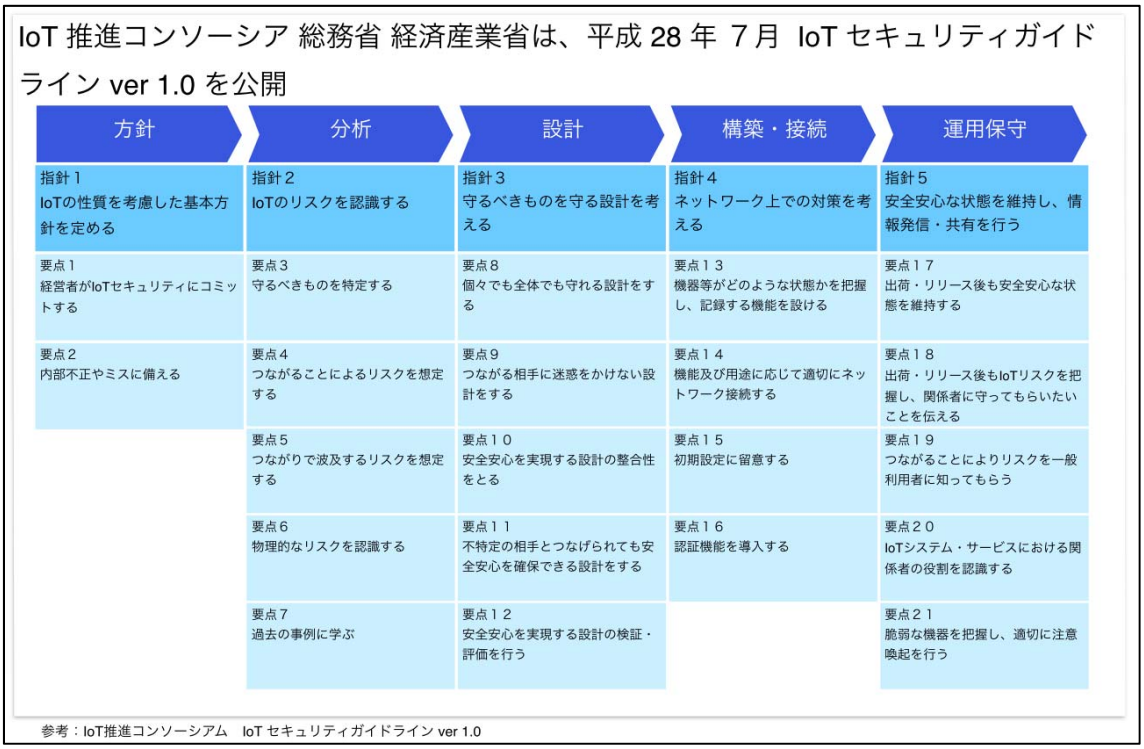

図 1

「CCDS 分野別セキュリティガイドライン」（平成 28 年 6 月）は、NISC が提唱した「セキュリティ・バイ・デザイン」をより具体的な産業分野で理解しやすくすることを目指して策定している。CCDS（(一社）重要生活機器連携セキュリティ協議会）は IPA の開発指針や IoT 推進コンソーシアムのガイドラインの策定検討にも参画しており、その思想や目標は同じところにあり、IPA の 17 の指針を網羅したものとなっている。

IoT の括りで考えるとセキュリティの要求事項が異なるが、ユースケースで分類すると要件と対策項目が類似する。今後ユースケースがさらに充実することによってこれらガイドラインのカバレッジも増えていくと思われる。それまでは、類似するユースケースを選択しギャップを補いながら対策を講じることが必要だ。

■IoT 関連のインシデント事例

□Mirai に IoT デバイスが感染し、大規模な DDoS 攻撃が発生した 2016 年の事例は、ネットワークカメラのパスワード設定の不備、ネットワークカメラ自体が Telnet を利用できるようになっていたこと、□監視カメラ映像が閲覧可能な事例もカメラのパスワード設定の不備が原因であり、□、□ともに「Shodan」等によってインターネット上の IoT デバイスが簡単に見つけられることから被害を深刻化している。□Smart TV が盗聴器になった事例は、Smart TV の OS「Tizen」の脆弱性対策がなされないままリリースされたことが原因であった。IoT セキュリティでは、バリューチェーン、サプライチェーンを含めた対策が重要であることから、自社製品のみならずサードパーティソフトウェア利用時の機能要件、アセスメント／ファジングツールを用いた検証評価の実施が必要である。

■IoT セキュリティの勘所

IoT を IT 面から捉えると“インターネットに接続されるもの”であるが、利用者（組織）にとっては利便性、生産性を向上させるものであり、提供側にとってはビジネスのコアのはずである。企業組織として、「モノ」ではなく「サービス」として考える必要がある。

IoT セキュリティのポイントは、

1. 俯瞰的にビジネスとして掌握することが重要である。ビジネスを生み出す一要素としてセキュアな状態でなければならない。また、サプライチェーン、バリューチェーンの視点も重要である。

2.出荷前の検証と評価プロセス、ユーザーが利用時に行わなければならないことを確実に実施してもらうこと、

3.運用し見つかった不具合の修正と廃棄まで含めたセキュリティ対策、

4.OWASP IoT セキュリティ Top10（図 2)、CWE 最も危険なプログラミングエラーTop 25 といったチェックリストを活用することである。

OWASP はウェブアプリケーションを主要業務としており、インターネット接続において現在起こっている事象という枠組みで OWASP IoT セキュリティ Top10 をまとめている。CWE は脆弱性のタイプでまとめており、OWASP IoT セキュリティ Top10 にマッチングさせてそれぞれの脆弱性に対する対策と検討すると検証すべき項目や対応済みのカバレッジも明確になる。

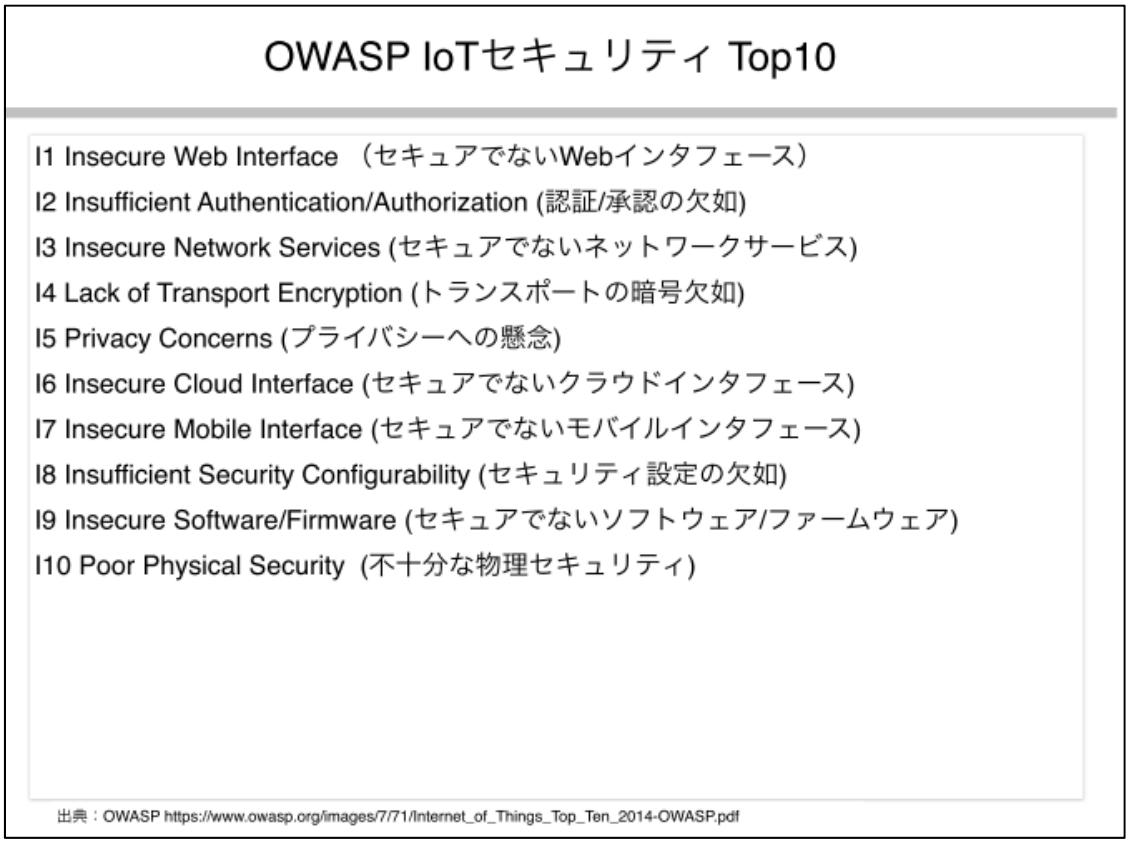

図 2

■まとめ

IoT には、オペレーショナルテクノロジーのセキュリティ要素が加わり、コンポーネントのレイヤーが増えたこと、また産業ごとにシステムが異なり成熟していないところもあるという、従来の情報システムのセキュリティと異なる点がある。IoT のセキュリティ対策においては、分野別のセキュリティ対策を参考に検討する必要がある。

従来のセキュリティ対策は、脅威に対して機能の足し算的な対応がなされ、アンチウイルスソフトも高負荷になっている。そのため一部には小型、省機能なデバイスが存在する IoT のセキュリティ対策には限界もある。ビジネスを俯瞰的に捉え、セキュリティを一要素と位置づけて考え、ビジネスのバリューチェーンにおける関連組織と連携して対策を講ずる必要がある。

製品の開発サイクルが短期化し、セキュリティ対策においても迅速化が望まれるなか、IoT ビジネスイノベーターには、最低限、OWASP、CWE のチェックリスト等を参考にしてセキュリティ管理策まで落とし込む一サイクルを回してみることが望まれる。そして、脆弱性が混入しないよう品質管理を行い、開発サイクル、早期問題解決のためにツールを活用することが有効である。