IoT 機器のセキュリティ対策に関する検討の方向性

平 成 ３ ０ 年 ７ 月
IoT 推進コンソーシアム
IoT セキュリティ WG

１．これまでの取組

これまでインターネット等のネットワークに接続していなかった「モノ」が通信機能をもち、ネットワークに接続して動作する IoT(Internet of Things)が急速に普及している。IoT 機器やこれを組み合わせたシステムは、多様な性質を持った機器やネットワークで構成されており、このような IoT 機器、システムやこれを利用したサービス特有の性質を踏まえたセキュリティ対策の検討が急務である。

このような現状を踏まえ、IoT セキュリティワーキンググループにおいては、平成 28 年７月に IoT 機器・システム、サービスの供給者、利用者等が IoT 機器やリスクに応じた適切なサイバーセキュリティ対策を検討するための考え方を、「IoT セキュリティガイドライン ver 1.0」として取りまとめた。

その後も平成 28 年 10 月に米国において約 10 万台の IoT 機器を踏み台として 1.2Tbps に及ぶとされる DDoS 攻撃が発生するなど、IoT 機器を悪用したサイバー攻撃が多発している。また、国立研究開発法人情報通信研究機構の調査では、サイバー攻撃は、2015 年から 2017 年にかけて 2.8 倍に増加しており、特に IoT 機器を狙ったサイバー攻撃は、5.7 倍に増加している。このような状況を踏まえ、近く閣議決定予定のサイバーセキュリティ戦略などにおいても、IoT 機器のセキュリティ確保の取組が記載される見込みであり、IoT セキュリティワーキンググループとしても、今後の検討の方向性及び今後の進め方を取りまとめるものである。

２．検討の方向性

IoT 機器のセキュリティ対策については、守るべき対象やそのリスクの性質に応じて以下のとおり場合分けした上で、守るべき範囲や要件レベルについて検討することとする。

DDoS 攻撃などの多数の一般利用者等の機器を踏み台にした攻撃については、これまでの攻撃の実態を踏まえつつ、基本的にはインターネットに接続される機器を対象にして、守るべき範囲や要件の議論を行う。

不正アクセスやマルウェアを用いた標的型攻撃、ランサムウェア攻撃等による情報の搾取やシステムの機能停止等への対策については、守るべき範囲や想定されるリスクが分野（ユースケース）により異なることから、これまでの攻撃の実態を踏まえつつ、分野毎（ユースケース毎）に対策を検討する。

３．今後の進め方

総務省では、情報通信審議会において、電気通信事業法に基づく端末設備の接続の技術基準の原則である、電気通信事業者の電気通信回線設備の機能に障害を与えないといった観点から、大規模 DDoS 攻撃等のサイバー攻撃を抑止するため、IoT 機器を含む端末設備がマルウェアに大量感染する事態を防止すること等を目的とする最低限のセキュリティ対策を技術基準に追加することについて検討を行っている。また、技術基準適合認定等の対象機器の範囲について、恒常的に既認定機器を介して接続する機器は対象外とすることや、CC(Common Criteria)認証などの国際標準に基づくセキュ

リティ認証との整合性についても検討している。

また、現在既にインターネットに接続して使われている機器の対策として、国立研究開発法人情報通信研究機構においては、国立研究開発法人情報通信研究機構法の改正を踏まえ、今年度中にも、パスワード設定等に不備がありマルウェアに容易に感染する可能性がある機器について、調査・特定を開始し、電気通信事業者等の協力のもと当該機器の利用者への注意喚起を行うこととしている。対策の実施に当たっては、関係省庁が一体となって、電気通信事業者、機器製造事業者等と連携して取組を行う。

経済産業省においては、不正アクセスや標的型攻撃等の対策として、産業サイバーセキュリティ研究会の下に設置されたワーキンググループ１（制度・技術・標準化）及びそのサブワーキンググループ（ビルサブワーキンググループ、スマートホームサブワーキンググループ）等において、各産業分野のセキュリティ確保策等について検討を進める。具体的には、それぞれのシステムに係るサイバー攻撃のリスク等を関係者間で共有した上で、サプライチェーン全体で求められるセキュリティ要件を整理し、ステークホルダーが活用できるガイドライン等を取りまとめる。

また、分野毎の検討を進めた上で、分野毎の課題や対策等を相互に持ちより、分野を横断して共通する対策を洗い出す等の取組を進めるべく、産業サイバーセキュリティ研究会 WG1 に分野横断的な議論を行うための SWG を設置する。

業界団体においては、上記の検討状況、業界の対応状況等を踏まえ、必要な対策について検討を進める。

これらの検討や取組においては、「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」（平成 28 年８月 26 日 内閣サイバーセキュリティセンター）を基本原則としつつ、IoT 機器が様々な分野においてシステムに組み込まれることや他のシステムと接続して使用されること、機器の製造・販売は国をまたいで行われることなどを踏まえ、技術的動向や国際的な議論の動向を注視しつつ、検討を進める必要がある。

なお、分野毎のセキュリティ確保策等の検討等を通じて、サイバーセキュリティ上のリスクを抑える観点からセキュリティ対策を講ずることが必要と考えられる場合には、法令又は国際標準に基づく認証制度等による対応状況を踏まえつつ、認証の仕組の在り方について検討を行う。新たな認証については、IoT 機器の多様性や技術革新の進度等に鑑み、基本的には民間団体主体の自発的な取組に委ねることが望ましい。その際には、例えば以下のような論点に留意することが考えられる。

- 求めるセキュリティ要件（デフォルトパスワード使用の禁止、各分野の特性に応じた要件など）
- 認証手段（ツール検証、開発プロセス認証など）
- 基準・規格に適合している旨の表示（ラベリング）の仕組み
- 一定期間経過後の認証の更新の必要性
- 認証取得手段（要件適合の自己宣言、第三者認証など）

こうした分野毎のセキュリティ確保策等の具体的な検討の内容については、関係主体による情報共有を通じ、分野を超えて確保すべき対策水準をあわせつつ、そのボトムアップを図ることを通じ、全体的なセキュリティの確保・向上に取り組んでいくことが重要であると考えられる。

IoT セキュリティワーキンググループにおいては、上述の取組を定期的にフォローアップし、関係者間の情報共有を図りつつ、施策間の連携・調整を図っていくこととする。