平成 29 年４月 12 日
ｻｲﾊﾞｰｾｷｭﾘﾃｨﾀｽｸﾌｫｰｽ

IoT セキュリティ対策に関する提言

あらゆるものがインターネット等のネットワークに接続される IoT/AI 時代が到来し、それらに対するサイバーセキュリティの確保は、安心安全な国民生活や、社会経済活動確保の観点から極めて重要な課題となっている。特に、IoT 機器については、その性質から、サイバー攻撃の対象になりやすく、我が国において IoT 機器を狙ったサイバー攻撃は年々増加傾向にある。また、諸外国においても、攻撃された IoT 機器による深刻な被害が発生しているところであり、早急な IoT セキュリティ対策が必要となっている。そのため、サイバーセキュリティタスクフォースでは、別紙のとおり、緊急に取り組むべき IoT セキュリティ対策の取組方針を提言する。総務省においては、関係府省等と連携しつつ、速やかに実施及び検討を開始することを求める。

別紙

IoT セキュリティ対策の取組方針 ver1.0

１．既に流通している脆弱性を有する IoT 機器のセキュリティ対策

既に流通している IoT 機器については、種類によって取るべき対策が異なることから、IoT 機器を

・国民生活・社会経済活動に直接影響を及ぼす可能性がある機器（重要インフラで利用される IoT 機器 等）

・サイバー攻撃の踏み台となってネットワークに悪影響を与えるおそれがある機器（家庭用ルータ、監視カメラ 等）

の 2 種類に分けて対策を検討し、実施することとする。また、対策の検討及び実施に当たっては、国民生活や社会経済活動への影響度合いを踏まえて、優先順位を付けて取り組むこととする。

（１）国民生活・社会経済活動に直接影響を及ぼす可能性がある機器のセキュリティ対策

重要インフラで利用される IoT 機器など、国民生活・社会経済活動に直接影響を及ぼす可能性がある機器（重要 IoT 機器）は、サイバー攻撃の対象となった場合に深刻な被害が生じることが想定されるため、迅速な対策が求められる。そこで、速やかに以下の実証事業を実施する。

① 重要 IoT 機器の脆弱性調査の実施（現地の設置環境や施工面の状況調査を含む。）

② 調査結果から脆弱性のある重要 IoT 機器のデータベースの作成

③ 特定された重要 IoT 機器の所有者・運用者・利用者に対して注意喚起を行い、各者による対策を促進

④ 特定された重要 IoT 機器の製造業者に対して情報提供を行い、今後製造する機器への対策を促進

（２）サイバー攻撃の踏み台となってネットワークに悪影響を与えるおそれがある機器のセキュリティ対策

家庭用 IoT 機器など、サイバー攻撃の踏み台となってネットワークに悪影響を与えるおそれがある機器については、幅広く調査を行い、脆弱性を有する機器を特定する必要がある。しかし、SHODAN や Censys といった海外の公開データベースに頼った調査では、詳細な仕様が公開されていないため、そのデータベースの信頼性が疑わしく、また把握できる機器にも限りがあることから、脆弱性を有する機器を特定するため、以下の取組を実施することを検討する。

① サイバー攻撃観測網（NICTER、ハニーポット等）による感染機器の把握

② 広域の脆弱性スキャンの実施（必要に応じて、調査ツールの研究開発）

③ 上述のサイバー攻撃観測網や脆弱性スキャンを活用し、特定のポートが開いている IoT 機器等について、データベースを作成

また、脆弱性を有する IoT 機器を特定した場合には、それらの機器がサイバー攻撃の踏み台となってネットワークに悪影響を与えることとならないよう、以下の取組を実施することを検討する。

④ 特定された脆弱性を有する IoT 機器が踏み台となることを防止するため、所有者・運用者・利用者に対して脆弱な機器の注意喚起を行い、各者による対策を促進。また、製造業者に対して情報提供を行い、今後製造する機器への対策を促進

⑤ 踏み台となったことが確認された際、被害拡大を未然に防止するため、ISP による C&C サーバとの通信制御を実施

２．今後製造する IoT 機器のセキュリティ対策

今後新たに製造される IoT 機器については、「IoT セキュリティガイドライン ver1.0」を踏まえ、ライフサイクルの各段階において、それぞれの役割・立場に応じた適切なセキュリティ対策が求められる。そこで、１．（２）のセキュリティ対策に加え、以下の各段階における取組について、必要に応じて関係府省、関係機関、企業等と連携しつつ、検討を進めることとする。なお、国内の事業者等を対象とした検討から着手することとするが、国外の IoT 機器については、国内の対策の検討を踏まえつつ、国際連携や国際標準化などの対策を検討する。

（１）設計・製造

設計・製造段階においては、所有者・運用者・利用者による安全な設定が行われるよう、ID/パスワード設定、ファームウェアのアップデート及び Wi-Fi 設定の仕様を設計時に盛り込むなど、製造業者におけるセキュリティ・バイ・デザインの考え方をいかに浸透させるかが重要となる。また、高齢者を含めた利用者の利便性にも配慮する必要がある。これらを踏まえ、IoT 機器の製造業者に対する意識啓発・支援の実施に向けた検討を行い、併せて、海外の事例も参考にしつつ、実効性を高める仕組みについても検討する。

（２）販売・輸入

販売・輸入段階においては、脆弱性を有する機器の流通を防止することが重要となる。そのため、セキュリティに適合している IoT 機器に認証マークを付与することや、比較サイトを通じて認証マークが付与された機器が推奨されることなどについて検討を行う。また、IoT 機器の中でも国民生活や社会経済活動への影響が大きい機器については、市場への流通後も管理が可能となるよう管理番号を付与できる仕組みについて検討する。

（３）構築・接続

機器の性格上セキュリティ対策を取ることが困難なものや海外製品など、流通している機器の中から、脆弱性を有する機器を完全に排除することは困難であることから、構築・接続段階において、脆弱性を有する機器が存在することを前提として、セキュアなシステム構築を実現する仕組みが重要となる。また、IoT 機器単体では必要なセキュリティ対策の実現が困難な場合や IoT 機器に精通していない利用者によりセキュリティ対策が不十分な場合が想定される。そのため、IoT システム・サービス全体としてセキュリティを確保する観点から、現在、総務省において実証を行うこととしている IoT 機器とインターネットの境界上にセキュアゲートウェイを設置する取組について、実証を進めるとともに、実際の導入が推奨される仕組みについて検討する。

（４）運用・保守

IoT 機器が実際に利用されている状況においても、運用・保守段階において、継続的に安全安心な状態を維持する必要がある。そのため、継続的な安全性を確保するためのセキュリティ検査の仕組み作りと対策が不十分な IoT 機器への対応について検討を行う。ただし、この検査の仕組みについては、家庭用の IoT 機器から重要インフラで利用される IoT 機器まで様々な IoT 機器がある中で、どの機器を対象とするか慎重に検討する必要がある。

また、利用者による十分な対応も重要となる中で、利用者に対する意識啓発が必要であり、ID/パスワード設定、ファームウェアのアップデート、Wi-Fi 設定の３点を中心にして行うことを検討する。利用している IoT 機器に脆弱性が有するか確認したい利用者に対して、簡易に脆弱性をチェックできるソフトを開発して配布する取組や、脆弱性を調査する民間サービスの実施を促進する取組を検討するとともに、利用者からの相談窓口や、脆弱性が見つかった場合の関係機関との調整窓口を設置することを検討する。さらに、「１．既に流通している脆弱性を有する IoT 機器のセキュリティ対策」と同様に、新たに IoT 機器に脆弱性が見つかった場合に、所有者・運用者・利用者へ注意喚起を行う仕組みを検討する。

（５） ネットワーク全体としてのセキュリティ対策

IoT セキュリティ対策は、例えば、IoT 機器を利用したサービス全体としてのセキュリティを考えれば、機器のライフサイクルの各段階にとどまらず、IoT 機器メーカ、流通業者、保守ベンダー、ISP 及び利用者といった各主体が補完し合いながら対応していく必要がある。これらの各主体と相互に連携し、ネットワーク全体のセキュリティを確保するため、情報共有のあり方を含め、総合的な IoT セキュリティ対策を実施する機関における対応を検討する。

３．まとめ

セキュリティ対策は継続的に取り組まなければならないものであり、総務省においては、この取組方針１．（１）のセキュリティ対策を速やかに実施するとともに、１．（２）及び２．（１）から（５）までのセキュリティ対策について速やかに検討を開始し、実施主体・体制、法制度、実施スケジュール等を整理しつつ、検討の進展・取組内容の具体化に伴い、必要に応じてこの取組方針の改訂を行うものとする。なお、検討を開始する事項については、ソフトウェアのみならずハードウェアに起因する脆弱性や、AI 等の技術開発の進展にも留意するものとする。

また、この取組方針を実施するに当たっては、IoT 機器が日本全国の企業や家庭において利用されるものであることを踏まえ、地域においてサポートできる様々な団体、企業、人材との連携を視野に入れて対策を検討・実施することが重要である。さらに、我が国におけるサイバーセキュリティの確保のためには、国内の IoT 機器のみならず、国外の IoT 機器へのセキュリティ対策が不可欠である一方、それらの機器に直接影響力を行使することは困難であることから、国際連携や国際標準化についても視野に入れて取り組むことが重要である。