

「IoT 開発におけるセキュリティ設計の手引き」を公開

～4分野のIoTの脅威分析と対策検討の実施例を図解～

IPA（独立行政法人情報処理推進機構、理事長：富田 達夫）セキュリティセンターは、今後のIoTの普及に備えて、IoT 機器および、その使用環境で想定されるセキュリティ上の脅威に対し、事業者（開発者）の備えが急務であると考え、「IoT 開発におけるセキュリティ設計の手引き」を作成し、本日公開しました。

URL：<https://www.ipa.go.jp/security/iot/iotguide.html>

昨今、IoT^(*)が多くの注目を集めています。現在ではIoTと分類されるようになった、組み込み機器の情報セキュリティについて、IPAは2006年から脅威と対策に関する調査を実施してきました。現在IoTと呼ばれる機器には、最初からIoTを想定し開発されたものの他に、単体での動作を前提としていた機器に、ネットワーク接続機能が後付けされたものが多く存在すると考えられます。そのため、IoTの普及と利用者の安全な利用のためには、ネットワークで機器やサービスが繋がることで生じる様々な脅威、それらが原因のリスクや被害を予め踏まえておく必要があります。

そこで、IPAではIoTの定義について「サービス提供サーバ・クラウド」「中継機器」「システム」「デバイス」「直接相互通信するデバイス」と5つの構成要素に分類し、IPAのIoTモデルを設定しました。その上で、各々の構成要素における課題の抽出・整理を行いました。

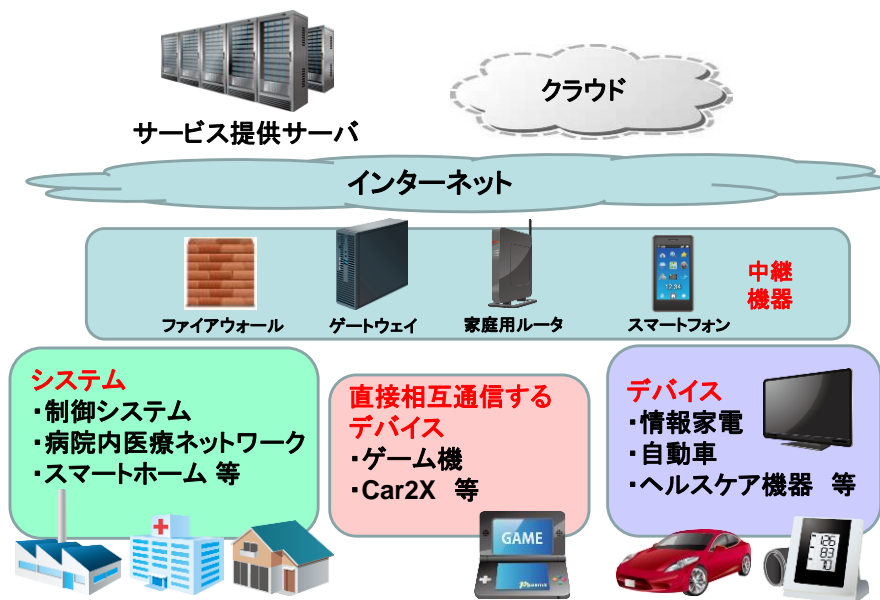


図1 IPAのIoTモデルの全体像

また、今まで蓄積してきた知見を基に、「デジタルテレビ」「ヘルスケア機器とクラウドサービス」「スマートハウス」「コネクテッドカー」の4分野を具体的なIoTシステムの事例として、脅威分析と対策検討の実施例を図解しています。この図解では、脅威が想定される箇所と、認証や暗号化など

(*) Internet of Things :モノのインターネット

該当する対策を明確化するとともに、業界のセキュリティガイドで述べられている要件との対応を示しています。この図は、網羅的にセキュリティ要件を整理することが困難な組織や、今後 IoT ビジネスを模索する組織にとって、安全な製品・サービスへの検討の材料になると考えられます。

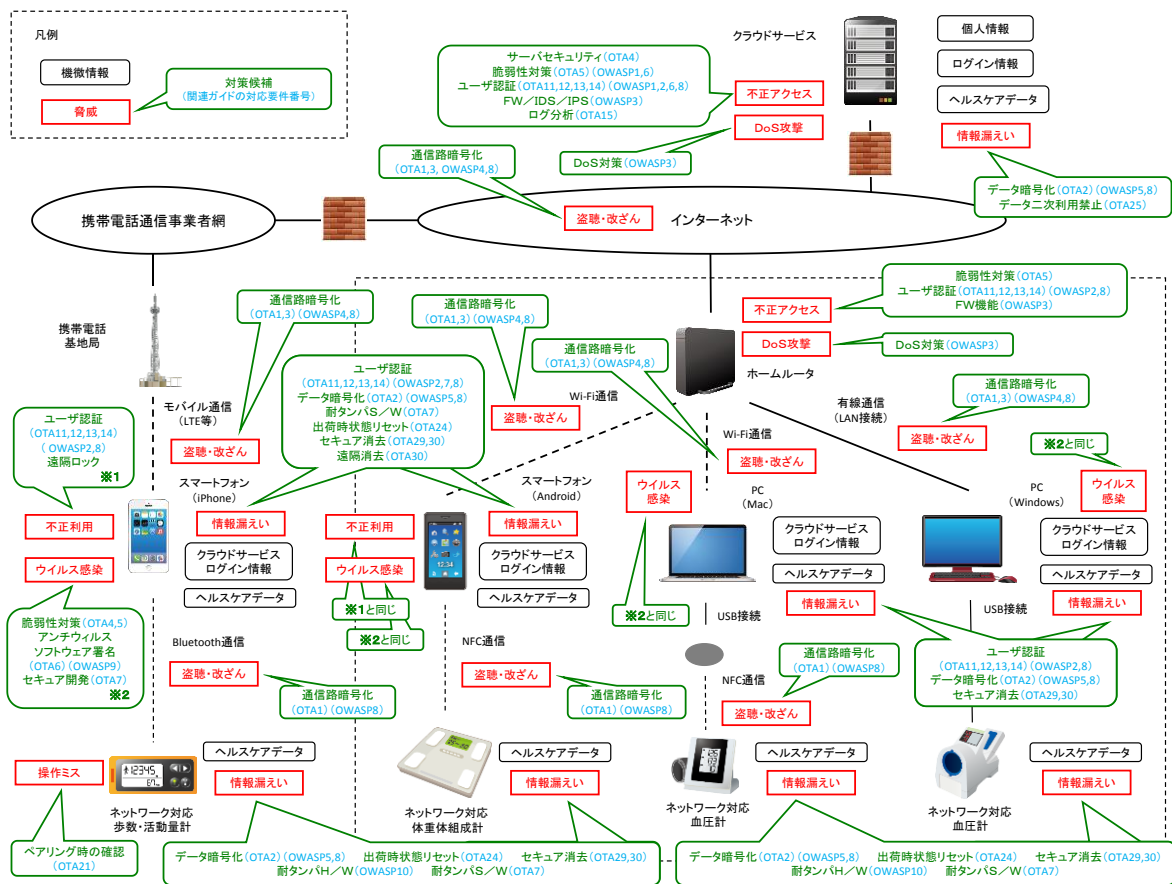


図2 ヘルスケア機器とクラウドサービスに対する脅威と対策の検討例

さらに、IoT システムのセキュリティを実現する上で根幹となる暗号技術に関して、実装した暗号技術の安全性を客観的に確認するためのチェックリストを付録として作成しました。開発者はこれを参照して暗号技術の利用・運用方針を明確化し、その安全性を評価することが容易になります。

なお、本書は去る 3 月 24 日に発表した IoT 製品を安全に開発するための 17 の開発指針^(*)に対し、具体的なセキュリティ設計と実装を実現するための手引きの位置づけです。手引きの公開に合わせ、17 の開発指針との対応表も公開します。

開発指針と本手引きを利用することで、IoT 製品・サービスのセキュアな実装と運用の一助になると考えられ、今後の安全な IoT の普及に期待しています。

■ 本件に関するお問い合わせ先

IPA 技術本部 セキュリティセンター 辻/岡下

Tel : 03-5978-7527 Fax : 03-5978-7518 E-mail : vuln-inq@ipa.go.jp

■ 報道関係からのお問い合わせ先

IPA 戦略企画部広報グループ 山北/白石

Tel : 03-5978-7503 Fax : 03-5978-7510 E-mail : pr-inq@ipa.go.jp

(*) 3 月 24 日に IPA ソフトウェア高信頼化センターが発表した「国内初 安全・安心な IoT 製品の実現に向けた 17 の開発指針を公開」<http://www.ipa.go.jp/about/press/20160324.html>