2017 年 1 月 30 日
独立行政法人情報処理推進機構（IPA）

米国土安全保障省（DHS） ― IoT セキュリティの戦略的原則（ファクトシート）

本ドキュメントは、米国土安全保障省（Department of Homeland Security）発行の“*Strategic Principles for Securing the Internet of Things*”のファクトシートの日本語訳となります。内容の詳細につきましては、ファクトシート原文および本編をご参照ください。
URL：https://ics-cert.us-cert.gov/Securing-Internet-Things

背景

モノのインターネット（IoT）[1]を構成する、ネットワークに接続された機器・システム・サービスの発展は、我々の社会に非常に大きな機会と利益を創出している。インターネットに接続された機器は、人やネットワーク、物理的なサービスのシームレスな接続を可能にする。そのような IoT 機器は、フィットネス・トラッカーからペースメーカー、車、家庭に電気や水道をもたらす制御システムまで、我々の日常生活の様々な側面にユビキタスに存在し、無くてはならないものになりつつある。しかし、IoT のもたらす利益が疑問の余地のないものである一方、イノベーションの進化にセキュリティが追いついていないのもまた事実である。

セキュリティを優先事項に

国を支える重要インフラのネットワーク化が進むにつれ、かつては手動で行われていた（それ故に、サイバー攻撃の影響を受け難いという恩恵を享受していた）重要なプロセスが、サイバー攻撃の脅威に晒されるようになった。急速に増加した「ネットワーク化」への依存が、セキュリティ対策の速度を上回ったと言える。

「IoT セキュリティの戦略的原則」は、設計、製造、導入などの様々な段階における IoT セキュリティを向上するための指針であり、提唱される実践対策を紹介している。IoT の開発者、製造者、サービスプロバイダ、および IoT 機器・サービス・システムを購入し利用するユーザに、IoT のセキュリティについて考え、議論してもらう第一歩とするためのものである。

IoT セキュリティの戦略的原則

- 設計段階からセキュリティを組込みこと
- 脆弱性の管理およびセキュリティアップデートを行うこと
- 確立されたセキュリティ対策を採用すること
- 想定される影響に応じ、優先度を付けてセキュリティ対策を行うこと
- IoT 全体において透明性を促進すること
- ネットワーク接続には注意を重ね、慎重に検討すること

[1] 本ドキュメントでは、IoT とは主に物理的な目的（センシング、暖房／冷房、照明、電動アクチュエーション、輸送など）を持つシステムや機器が、（多くの場合）組込みシステムに組み込まれた相互運用のためのプロトコルを介して（インターネットを含む）情報ネットワークとつながっていることを言う。

IoT セキュリティの戦略的原則（バージョン 1.0）

これらの原則は、ステークホルダーがネットワークに接続された機器を開発、製造、導入または利用するにあたって、セキュリティを包括的に考慮するためのツールとなることを目的としている。とりわけ、IoT の開発者、製造者、サービスプロバイダ、および産業ユーザ／ビジネスユーザのためのものとなっている。

設計段階からセキュリティを組み込むこと： ネットワークに接続されるあらゆる機器において、セキュリティは不可欠の構成要素として検討されるべきである。例外はあるものの、一般にコストの問題が企業がセキュリティを考慮しない IoT 機器を市場に送り込むのを後押ししている。

脆弱性管理およびセキュリティアップデートを行うこと： 例えセキュリティ対策が設計段階で組み込まれたとしても、機器がユーザの手元に渡ってから脆弱性が発見される可能性がある。これらの脆弱性は、脆弱性管理およびパッチ／セキュリティアップデートによって低減が可能になる。

確立されたセキュリティ対策を採用すること： IoT のセキュリティ対策は、既に検証され、確立された IT セキュリティ対策およびネットワークセキュリティ対策を出発点として検討することができる。IT セキュリティおよびネットワークセキュリティのアプローチは、IoT 機器における脆弱性の特定、イレギュラーの検知、潜在的なインシデントへの対処、問題や障害からの復旧に関して支援してくれる。

想定される影響に応じ、優先度を付けてセキュリティ対策を行うこと： リスクモデル同様、セキュリティ上の問題がもたらす結果（被害）は、IoT エコシステム全体で大きく異なる。障害や情報漏洩などサイバー攻撃によって想定される被害を考えることは、IoT エコシステムの中でどこにどんなセキュリティ対策が為されるべきか見定めるのに重要となる。

IoT 全体において透明性を促進すること： 開発者と製造者は可能な限りサプライチェーン、とりわけ他社製のハードウェアおよびソフトウェアコンポーネントに脆弱性が存在するか把握しておくべきである。セキュリティ意識を向上させることにより、製造者や産業ユーザはセキュリティ対策をどこにどう実施するか、または冗長性をどう作り込むか、分かるようになる。

ネットワーク接続には注意を重ね、慎重に検討すること： IoT ユーザは、とりわけ産業環境においては、継続的なネットワークへの接続性が IoT 機器の利用やその障害により発生するリスクを踏まえて本当に必要なのか、慎重に検討する必要がある。

米国土安全保障省（DHS）

米国におけるサイバーセキュリティの主導機関として、DHS は社会インフラ、国民の安全、デジタル・エコノミーを脅かすサイバー攻撃との闘いおよび抑止に強く取組んでいる。最近の IoT を活用した前例のない規模とスコープの悪意あるサイバー活動により、IoT のキュリティは DHS にとっても優先度の高い喫緊の取組みとなっている。IoT セキュリティへの取組みは、サイバー空間のセキュリティを確保し、重要インフラを防御し、国民の安全を守るという DHS のミッションに連なるものである。DHS 内では、Office of Cyber, Infrastructure, and Resilience Policy（CIR）が DHS 全体のサイバー、技術、インフラおよびレジリエンスポリシーを担当している。

問い合わせ先

お問い合わせは、https://www.dhs.gov/securingtheIoT まで。