IoT Security の重要性と発展の動向

TAcc+ スタートアップ分析チーム

情報セキュリティは、IoT を発展させる上で確実に整えるべき基礎的な技術である。だが、IoT デバイスの急速な普及に伴い、セキュリティ対策上の新たな脆弱性も増え続けている。ハッカーたちはその機に乗じて利益を奪い、政府、企業、個人が被る損失やリスクが増大し続け、その結果、IoT デバイスのセキュリティ対策は硬直的需要となっている。対策は、ハードウェア、セキュアな通信、クラウドセキュリティ、ライフサイクルのセキュリティ管理の 4 つのレイヤー（階層）に分けられる。そして、主となる IoT の情報セキュリティ対策の動向としては、設計段階からのセキュリティ強化、ゼロトラスト、セキュリティ面での AI 活用の拡大、IoT セキュリティの規制強化がある。また、業界のリーディングカンパニー主導による IoT デバイスの標準仕様と、各国政府の積極的な法整備に伴い、メーカーが開発する製品やサービスが、業界標準や各国の法規に追いつけるかどうかが、競争優位性に大きな影響を与えることになる。

IoT の情報セキュリティ対策

IoT を導入する際の最大の課題の一つは、情報セキュリティの問題である。十分なセキュリティ対策が講じられていなければ、それは衝突防止設計が不十分な車と同じであり、たとえ速度や快適性が優れていたとしても、誰も乗ろうとはしないはずだ。この例えは、それだけ情報セキュリティが重要であることを意味している。IoT NOW の調査によると、88%の企業が IoT のセキュリティ強化が必要だと考えており、その 3 分の一以上の 37%が大幅な改善が必要だと回答している。また、回答者の 60%が一定の改善が必要だと回答した。

IoT セキュリティの重要性とニーズ

SonicWall のサイバー脅威レポートによると、世界中で IoT デバイスに対するマルウェア攻撃が急速に増加している。

◆ 2019 年：3,427 万回以上

◆ 2020 年：5,690 万回（前年比 66%増）

◆ 2021 年：6,010 万回（前年比 6%増）

◆ 2022 年：1 億 1,230 万回（前年比 87%増）

◆ 2023 年上半期：すでに 7,800 万回に達し、増加速度は驚異的である。

レポートでは、IoT デバイスが攻撃を受けやすい主な要因として以下の点を挙げている。

◆ 98%の IoT データ伝送チャネルが暗号化されていない。ハッカーは伝送中のデータを容易に傍受し、盗み出すことができる。

◆57%の IoT デバイスの防御能力が極めて低い。それらのデバイスには基本的なセキュリティ対策が施されておらず、マルウェアに侵入されやすい。

◆83%の医療用画像装置が、サポートのない OS 環境で稼働している。それらの装置はセキュリティの更新や脆弱性の修正が困難であり、セキュリティリスクが増大する。

上記の理由から、医療機関はサイバー攻撃の標的となりやすい。なかでも最大の理由は、医療機関のネットワークシステムのセキュリティが総じて脆弱であることだ。機密データ（患者の個人情報や診療記録など）が漏洩すると、多大な損失が発生する。特に医療・保健分野では、一回の情報セキュリティインシデントが平均で 710 万ドルもの損害をもたらすと言われている。そのため IoT セキュリティの重要性は言うまでもない。

ネットワークセキュリティ企業の Palo Alto Networks が 2020 年に発表した『State of Enterprise IoT Security』レポートによると、医療用画像システムは最も攻撃を受けやすい IoT デバイスであり、攻撃を受ける割合は 51%に達している。次いで監視カメラが 33%、更新が遅くセキュリティが脆弱な患者モニタリングシステムは 26%、情報セキュリティ対策はしばしば軽視されがちなオフィス用プリンターも 24%に達している。また、街灯システムも、自動化の過程における情報セキュリティ設計が不十分なため、攻撃を受けやすい公共システムの一つとなっている。情報には機密データや経済的価値のあるデータが含まれており、加えて情報セキュリティ対策に対する意識の欠如や、重要性が低いと見なされがちなデバイスがあることが、攻撃の高い動機付けと低い侵入障壁という二大要因のベースとなっている。特に、公的インフラ、保健・医療機関、企業のオフィスなどの大規模な組織は、攻撃を受ける割合も極めて高い。そのほか、ME 機器のゲートウェイ（Medical Device Gateway）、エネルギー管理システム、コンシューマー向け電子機器、家庭用電話なども、数は多くないが攻撃を受けている。

サイバー攻撃の手法の中で最も高い割合を占めているのは、システムの脆弱性を利用した攻撃で、全体の 41%を占めている。攻撃者は AI を使って IoT のシステムアーキテクチャの弱点をスキャンし、隙を突いて侵入する。次に多いのは、マルウェアを利用した攻撃で、割合は 33%である。これは、ユーザーが誤ってマルウェアをダウンロードするか、またはトロイの木馬のようなマルウェアが、一見安全に見えるアプリケーションを通じてシステムに侵入することで発生する。さらに、例えば簡単すぎるパスワードやフィッシング対策ソフトなど、ユーザーの悪習慣（脆弱な情報セキュリティ管理）に乗じた攻撃も 26%を占めている。PC にはすでに十分な情報セキュリティ対策システムが確立されているが、IoT のセキュリティシステムは、統一された保守規格や専門の維持管理事業者がまだ存在しないため、サイバー攻撃を受けやすい状態が続いている。

サイバー攻撃が激化する中で IoT デバイスを効果的に守るには、まず、完璧なユーザー認証システムを確立しなければならない。IoT デバイスは機器設備であるので、ネットワークの仕組みに詳しい者であれば、簡単に LAN カード

アドレスを複製できるので、ID 認証が非常に困難だ。そのため、デバイスコントロール（Device-Level Control）をアイデンティティコントロール（Identity Level Control）へ転換させることが、情報セキュリティ管理の重要課題となる。次に、すべての IoT デバイスの追跡と管理が非常に重要である。PC やスマートフォンは比較的容易に追跡できるが、IoT デバイスは型式や機能が多様であるため、追跡をしようにも困難な点が多い。さらに、IoT デバイスのソフトウェアのアップデート問題も無視できない。定期的にソフトウェアの更新がある PC やスマートフォンとは異なり、多くの IoT デバイスはディスプレイやユーザーインターフェースを備えていないうえ、メーカーやブランドが多く、数も大量である。そのため、定期的なソフトウェア更新と脆弱性の修正がサプライヤーにとっての大きな課題となっている。以上の 3 つの問題は、IoT セキュリティ対策の実施に大きな影響を与えている。次に、IoT セキュリティを構成する 4 つのレイヤーについて説明する。

IoT の情報セキュリティ対策における 4 つのレイヤー

IoT で発生する情報セキュリティ問題は、4 つのレイヤーに分けられ、それぞれ重視すべき点が異なる。第 1 のレイヤーはハードウェアである。ハードウェア層において最も重要なのは、IoT デバイスの ID 認証である。IoT は多種多様で、センサーを備えたハードウェアを含むため、物理的な情報セキュリティ管理は IoT セキュリティを発展させるための手段の一つとなる。2021 年 10 月、米国食品医薬品局（FDA）は、医療機器の「機器固有識別子システム（Unique Device Identification System, UDI System）」のガイドラインの草案を発表した。これは、米国内で販売される医療機器を明確に識別できるようにし、製造から流通、患者の使用に至るまで、機器の出所と ID を把握することを目的としている。この取り組みは、患者の安全性向上と医療機器の販売後の監視を実現することを目的としている。

第 2 のレイヤーはセキュアな通信である。この層には、ファイアウォール、不正侵入検知システム（IDS）、不正侵入防御システム（IPS）、エンドツーエンド暗号化（E2EE）などが含まれる。ファイアウォールは、IoT の内部ネットワークとインターネットの間に配置され、監視・管理が可能なゲートウェイ（Gateway）を設置してすべてのメッセージパケットの出入りを制御し、ネットワーク上の特定のデータアクセス行為を許可または禁止する。その主な機能は、通過するすべての IP パケットをチェックし、IP アドレス、ポート（Port）、パケット転送方向によって、ネットワーク情報パケットの流れを制御することである。不正侵入検知システム（IDS）の主な機能は、ネットワークパケットの監視と検出であり、事前に設定したセキュリティポリシーに基づいて、ネットワークやシステムの動作状況を監視する。異常が見つかると自動で管理者にアラートを発し、さまざまな攻撃の企み、攻撃行為、攻撃の結果を記録する。一方、不正侵入防御システム（IPS）は、さらに進んだ主動的なシステムであり、ネットワークの異常なパケットや行為を発見した際に、管理者にアラートを発するだけでなく、攻撃元の IP をブロックするなど、即座に必要な対応処置を講じるシステムである。エンドツーエンド暗号化（E2EE）は、セキュアな通信方法の一つで、潜在的な盗聴者を防ぐことが目的である。それは、一つの

端末デバイスから別の端末デバイスへデータを送信する際、第三者がデータを取得できないようにする仕組みであり、端末の両当事者のみがデータを読み取ることができる通信システムである。IoT デバイスは数が膨大であり、かつ各種の異なる IoT デバイス間で頻繁に通信を行うため、エンドツーエンド暗号化は IoT の情報セキュリティの管理上、最も重要かつ最も主要な手段となる。

第 3 レイヤーはクラウドセキュリティである。クラウド環境での情報セキュリティ保護には、広範囲に適用可能なポリシー、技術、制御手法のセットが必要であり、それによってデータ、アプリケーション、クラウドインフラを守る。データや情報が、ネットワーク伝送を主たるアクセス方法としてクラウドに送られると、情報セキュリティの確保は極めて難しく、さまざまな状況を考慮しなければならない。特に、実務で複数の異なるクラウドシステムを使用していると、情報セキュリティの確保は一層困難となる。ハイブリッドクラウドとは、AWS、Azure、Google Cloud など、複数のクラウドプロバイダーを同時に活用し、データマネージド、ストレージ、アプリケーションスタック（Application Stacks）の実行を行うことを指す。

第 4 レイヤーはライフサイクルのセキュリティ管理である。IoT において、重視すべきはハードウェア、セキュアな通信、クラウドセキュリティだけではなく、デバイスのライフサイクル全体を通してのセキュリティ管理も非常に重要である。簡単に言えば、パッチ（Patch）適用やアップグレード・更新をいつ行うのか、更新、アップグレード、メンテナンスをどのように実施するのかという問題である。これらは、IoT デバイスが製造され、流通し、消費者の手に渡り、最終的に安全に廃棄されるまでの全ライフサイクルのセキュリティ管理をカバーするものである。例えば、多くの人は IoT デバイスのライフサイクル管理における安全なデータ・端末の廃棄（Secure Decommissioning）の重要性を見落としがちだ。ハードウェアが破壊されたとしても、多くの場合データの復元が可能であるため、使用済みのメモリチップは不用意に捨てられないため、安全な廃棄処理の手順が必要となる。IoT デバイスが安全に廃棄され、かつその内部データは完全に消去されていることが、重要な情報セキュリティ管理方針に加えられるべきである。

IoT の情報セキュリティ対策の動向

IoT Security 市場は、市場規模が 2022 年に 179 億米ドル、2023 年には 209 億米ドルに達し、2028 年には 592 億米ドル、年平均成長率 23.1%に達すると予測される急成長分野である（MarketsandMarkets，2023）。以下、IoT の情報セキュリティ管理における主な動向を紹介する。

1. 設計段階からのセキュリティ強化。開発チームは設計の初期段階で「セキュリティの考慮事項」を取入れる必要がある。それは、事後のセキュリティ措置では効果が半分しかないためである。具体的には、セキュリティ・バイ・デザインのハードウェアとソフトウェアの使用、確実な ID 認証とライセンス管理の実行、最新のセキュリティパッチの適用によってデバイスを最新の状態に維持することが含まれる。

2. ゼロトラスト（Zero Trust）セキュリティの拡大。いかなる人やデバイスも信頼しないことを前提とする方法を指し、ユーザーID とデバイスのステータスに基づき、リソースへのアクセスを制限することで情報セキュリティへの攻撃を防ぐ。

3. セキュリティ面での AI 活用の拡大。AI を活用することで、不審なアクティビティの識別、マルウェアの検出、セキュリティインシデントへの対応が可能となる。

4. IoT セキュリティの規制強化。

IoT ハードウェアの情報セキュリティ対策

IoT の情報セキュリティ管理の第 1 レイヤーであるハードウェア層は、前述したように、IoT デバイスの ID 認証をいかに実現するかが課題である。自動車を例にすると、従来のガソリン車において最も高価な部品はエンジンであり、そのためエンジンメーカーはエンジンに番号を刻印し、たとえ車両が盗難に遭ったり解体されたりした場合でも、エンジン番号によって盗まれた車両を追跡できるようになっている。だが、電気自動車は、バッテリーの集合体やコンピュータなどの電子製品で構成されている。では今後、電気自動車の ID 認証はどのように行えばよいのか。それは、電気自動車のモーター、制御システム、CPU をコンピュータと組み合わせて、車両の新たな ID 認証を確立することである。なかでも、IoT デバイスや半導体チップの ID 認証には複数の手法が存在するが、現在の主流は物理複製困難関数（Physical Unclonable Function, PUF）を利用してチップ上に記録する方法である。

PUF は、具体化された物理構造の関数であり、半導体における最新のセキュリティ認証技術の一つである。シリコンチップを製造する際に、製造過程で生じる微細な物理的誤差を利用し、一つひとつのチップにわずかに異なる物理特性を持たせることで、そのチップの DNA、もしくは指紋の役割を果たすことができる。PUF には、ランダム性、複製不可能性、安定性といういくつかの重要な特性があり、PUF が具体的な物理的特徴を与えることで、各チップの差異を識別する仕組みだ。PUF は、MAC アドレス（Media Access Control Address）がエンコードによって簡単に削除され、チップ間のデジタル・フォレンジックやデジタル認証を破壊するというリスクを解決できる。

データ型の ID 認証応用技術としては、公開鍵認証基盤（Public Key Infrastructure, PKI）がある。PKI は、ハードウェア、ソフトウェア、当事者、管理ポリシー、プロセスから構成される基盤システムであり、「電子証明書」の作成、管理、配布、使用、保存、復元を行うための仕組みである。PKI は、電子証明書の認証機関を通じて、使用者の IoT における ID を公開鍵と紐付けることで、それぞれの認証機関に IoT の ID の唯一性を確保させるものだ。PUF のような物理的な ID 認証と、データ型の ID 認証を組み合わせて二重に管理することで、IoT のハードウェア層における情報セキュリティを実現する。

2021 年、PKI as a Service のスタートアップ企業である Key Factor 社は、電

子証明書の発行を行う Prime Key 社を合併した。この合併により、エンドツーエンドの IoT デバイスの ID 管理が提供され、柔軟に証明書が発行されるようになった。Key Factor 社は、2024 年の売上高が 1 億米ドルを超え、直近 3 年間で売上成長率が 525%に達している。これは、企業にとって IoT の動向における情報セキュリティの必要性が切迫していることを示すとともに、その市場が急速に成長していることを反映している。

IoT デバイスの ID 識別標準の確立

これまで IoT デバイスや機器の多くはデフォルトのパスワードを使用し、維持管理の便宜上、共通パスワードが設定されることも多かった。そのパスワードは、0000、1234、admin など極めて単純なものが多く、購入後に進んで変更するユーザーも少ないため、悪意のある攻撃者が容易に推測できるという情報セキュリティ上の脆弱性を抱えていた。さらに、IoT デバイスを導入する際には、専門の技術者が、物理的なデバイスの設置やパスワード認証の設定を手動で行わねばならないため時間もかかる。担当者の異動があると維持管理にも影響し、全体の運用コストが高止まりになる要因となっていた。

こうした課題を解決するため、PayPal、Google、Apple、VISA、Intel、LINE などの大手企業が設立した国際的な認証標準化団体 FIDO アライアンス（Fast IDentity Online Alliance）は、IoT デバイスの ID 識別のための仕様である FIDO Device Onboard（FDO）を定め、2021 年 4 月に初版を発表した。この仕様により、運用コストの削減、管理の簡素化、導入および維持管理時間の短縮、セキュリティの向上が期待されている。FDO 仕様では、デバイスの製造段階で所有権を確定し、簡易的な自動化認証プロセスを通じて、IoT デバイスを改変することなく、安全に異なる IoT プラットフォームへ接続できる。

これまでにも、業界では同様の技術開発が進められてきたが、統一された標準が存在しなかった。FDO はオープンな業界標準として、仕様発表後に多くの企業からの支持を獲得し続けている。2023 年 9 月に FDO 認証プログラムが開始され、すでに多くの企業が製品認証を申請している。業界では、FDO の普及と拡大が進むにつれ、情報技術（IT）と制御・運用技術（OT）の統合促進と、IoT デバイスの異業種間・異分野間・異組織間での統合運用のニーズが満たされるだろうと広く考えられている。さらに、この仕様を通じて業界共通の課題が解決されることが期待されている。

IoT セキュリティに関する法整備

ハッカーによる IoT デバイスへの攻撃が激しさを増すにつれ、各国政府も積極的に法整備を進めている。先駆者である欧州連合（EU）を例に挙げると、EU は 2019 年に「NIS2 指令（改正ネットワークおよび情報セキュリティ指令）」を発表し、その適用範囲には IoT デバイスも含まれている。指令では、各加盟国に対し、2024 年までにこの指令を国内法に転換し、同年に正式施行することを求めている。さらに、2024 年 10 月 10 日には、EU 理事会が

サイバーレジリエンス法（Cyber Resilience Act, CRA）を可決した。これにより、デジタル製品のセキュリティ強化を目的とする同法が発効し、さらに2027年末までに関連するソフトウェア、ハードウェア、サービスの各事業者に対し、この法律に完全に準拠することが義務付けられた。IoTについても、製品、デバイス、サービスは、サプライチェーンおよびライフサイクル内において関連する情報セキュリティの要件を確実に満たさなければならい。

日増しに厳格化する法規は、メーカーに製品の設計・開発・維持管理の全ライフサイクルにおいて、確実なセキュリティを維持し、IoTデバイスの安全な利用を保証するよう要求している。海外市場への参入を目指す企業にとって、開発した製品やサービスが各国の法規に適合しているかどうかは、販売実績に大きな影響を与える。言い換えれば、より多くの国の法規に準拠できる製品やサービスが、競争力において大きな優位性を持つということだ。

出典：

- 【資安月報】2024年4月。iThome。2024。
- 2025年「物聯網」將會暗潮洶湧 安全法規與駭客威脅成關鍵。科技島。2024。
- Appier全線產品整合生成式AI創新應用，驅動智慧商業策略升級。經濟日報。2024。
- FIDO聯盟推IoT設備身分識別FDO標準，紅帽RHEL、Fedora開始支援。iThome。2022。
- StartUp創辦人對生成式AI的6項提問。AWS。2024。
- 生成式AI的產業應用與發展趨勢。數位發展部。2024。
- 最新IoT設備身分識別FDO標準，即將有4家廠商取得首波認證，臺灣工業電腦廠也包括在內。iThome。2024。
- 新法令力促工控IoT資安防護　企業迎向全生命週期合規挑戰。網管人。2024。
- 歐盟網路韌性法案CRA將於2027年強制執行。德國萊因TÜV。2024。