スマートデバイスからセキュアなシステムへ：日本のIoTサイバーセキュリティへの取り組み

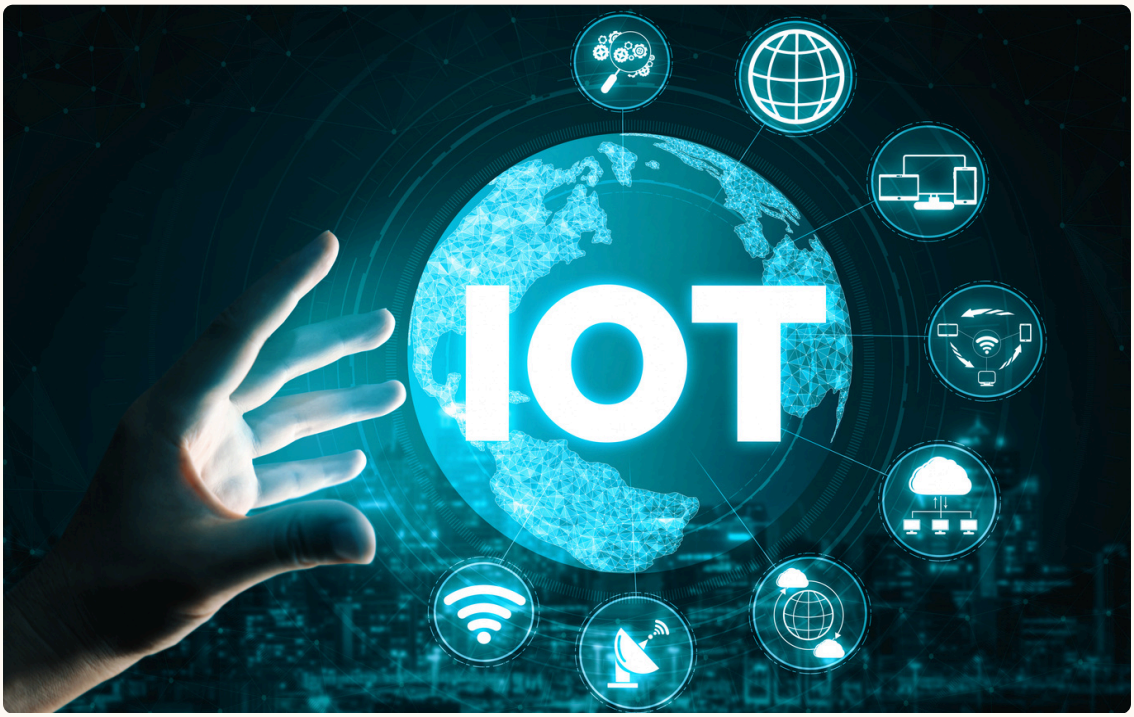
はじめに

本記事では、IoT（モノのインターネット）に特有のサイバーセキュリティ上の脆弱性を取り上げ、それらの脆弱性と影響を軽減するための企業戦略を考察する。

さらに、リスクマネジメントおよびテクノロジーライフサイクルマネジメントのフレームワークを参照し、組織が「技術」「人」「プロセス」を組み合わせて効果的なサイバーセキュリティ戦略を計画し、実行できるよう支援する。

IoTの現状

IoTは、ビジネス戦略の強化、人間の能力拡張、産業プロセスの自動化、公共サービスの改善といった目的で広く導入されている。世界全体では2023年時点で166億台以上のIoTデバイスが接続されており、この数は2030年までに400億台に達すると予測されている。日本に限ると、2023年には約9億3,000万台のIoTデバイスが存在し、2030年までにはほぼ倍増して17億7,000万台に達すると見込まれている。また、日本のIoTデバイス市場は2024年に約32億7,000万米ドル規模を生み出し、2025年から2030年にかけて年平均成長率（CAGR）19.3%で拡大すると、Grand View Researchは予測している。



IoTに固有のセキュリティ課題

近年のセキュリティ侵害に関する調査から、IoT技術に特有の重大な脆弱性が明らかになっている：

アセットマネジメントの不備– 侵害されたシステムは、サイバーセキュリティの専門知識を持たない非IT部門によって管理されているケースが多い。デフォルトパスワードは依然として大きな脆弱性となっている。

多様性 – IoTデバイスは複雑さが異なり、多くはコストやシンプルさが理由で、暗号化や最新のセキュリティ機能を備えていない。

限定的な基準と規制– 従来、IoTの導入はセキュリティよりもコストやスケーラビリティに重点がおかれてきた。

限定的な多層防御– IoTデバイスは、セキュアな境界の外で稼働することが多く、多層的な防御がないまま運用されている。

日本ではIoT関連のサイバー攻撃が急増している。2019年から2024年の間に、複数のグループが200件を超えるキャンペーンを日本の組織に対して実行した。さらに、2024年末以降、IoTボットネットを基盤にしたDDoS攻撃が繰り返し日本企業を標的としている。

IoTデバイスを保護するためのベストプラクティス

企業のサイバーセキュリティ計画には、「人」「プロセス」「技術」が必要である。技術だけでは脅威を排除できない。人には脅威を検知し対応するためのトレーニングが必要であり、プロセスは従業員の行動指針となり、ベストプラクティスを徹底させる。

セキュリティ設計

IoT構成要素は多様であり、画一的な戦略は効果を発揮しない。システムズエンジニアリングのアプローチでは、セキュリティを設計上の制約として組み込み、コスト、複雑さ、運用への影響のバランスを取る。

リスクマネジメントフレームワーク

組織は、体系的なリスクマネジメントのアプローチを採用すべきである。すなわち、低減、移転、受容、回避の4つである。進化する脆弱性に対応するには、定期的な再評価と審査が不可欠である。

日本のフレームワークは、このプロセスをさらに強化している：
JC STARラベリング制度 – 2025年3月にIoT製品向けに開始。2025年度から調達においてSTAR 1準拠が必須となる。

能動的サイバー防御法（ACD法） – 2025年に施行。日本の当局に、脅威を積極的に無効化する権限を与え、侵害報告を義務付け、情報共有を強化する。

トレーニングと人材の即応性

IoTシステムを保護する上での主要な課題は、技術的なアーキテクチャだけではなく、人的要因にもある。従業員はコンプライアンス要件、インシデント対応、ガバナンスについて理解していなければならない。PECBのISO/IEC 27001認証コースは、日本企業や専門家が情報セキュリティ体制を強化するための体系的な道筋を提供する。

結論

日本におけるIoTの急速な普及は、機会とリスクの両方をもたらしている。2030年までに約20億台のデバイスが導入されると予測される中で、セキュリティは後回しにできるものではない。JC STARやACDといったフレームワークは、IoTによる脅威に対して組織のレジリエンスを維持する助けとなる。一方、PECBのような認証機関によるトレーニングは、専門家が方針を実務に落とし込み、コンプライアンス、技術、持続可能なIoTセキュリティの間のギャップを埋めることを可能にしている。