日本企業におけるIoTセキュリティ脅威分析

Analysis of IoT Security Threats in Japanese Enterprises

卓珮如・システム分科会・情報セキュリティ大学院大学

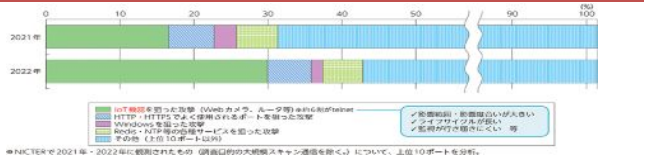
Abstract-It's focusing on the emerging IoT security threats faced by Japanese enterprises and their subsequent impact on supply chains. With the proliferation of IoT devices, anticipated to reach 340.9 billion by 2023, Japanese companies are increasingly vulnerable to cyber-attacks, which have surged by 85% in Japan alone. The economic repercussions are significant, with average losses due to security incidents amounting to approximately 328.5 million yen per organization in 2021. This study employs a methodology incorporating data collection through Shodan and Maltego, supply chain analysis via Google Dorks and OSINT tools, simulation of APT attack scenarios, and risk assessment and mitigation strategies. The analysis aims to provide concrete strategic and technical guidelines to enhance IoT security measures within Japanese enterprises, thereby bolstering their defense mechanisms against future security threats.

背景と目的

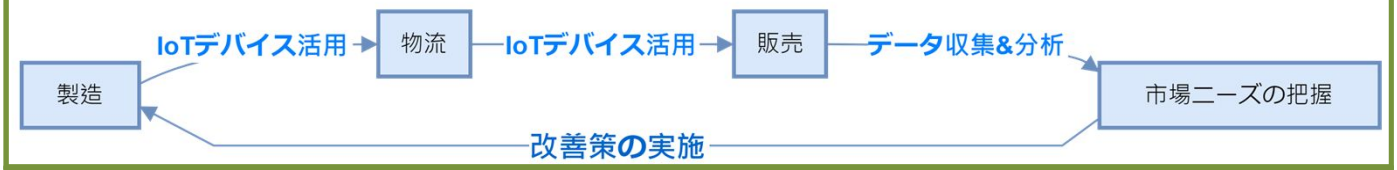
日本企業はIoTセキュリティ脅威の増加に直面しており、この研究は最新の攻撃手法と防衛戦略に焦点を当てる。OSINT情報とサプライチェーン攻撃の観点からIoTデバイスの脆弱性を評価し、企業がセキュリティ対策を強化するための実践的な指針を提供することを目指す。IoTデバイスは製造から物流、消費者までのサプライチェーン全体で広く利用され、これらのデバイスから収集されるデータは効率化や品質管理に不可欠だが、セキュリティ脅威のリスクも高まる。

年度	IoTデバイスの数量（億台）
2020	253
2021	277.9
2022	309.2
2023	340.9

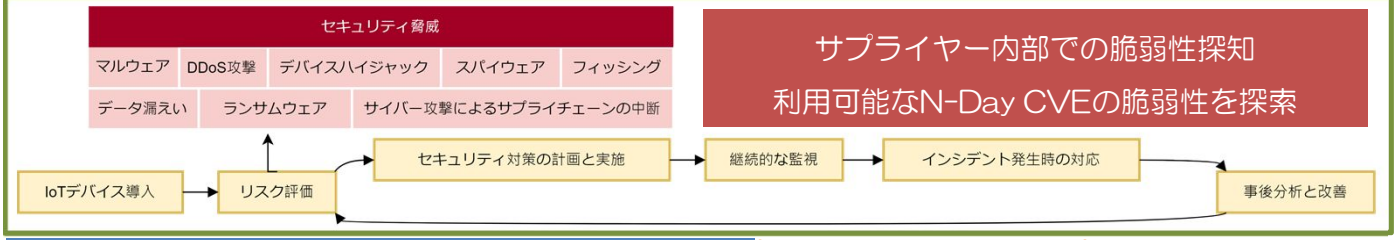
IoTデバイスの普及率とサイバー攻撃の件数は年々増加している



IoTとサプライチェーンの関係



セキュリティ対策のフローチャート



方法論

- データ収集：ShodanやMaltegoを使用した調査。
- サプライチェーン分析：Google DorksやOSINTツールの応用。
- APT攻撃シナリオの模擬。
- リスク評価と対策。

期待される成果

この研究は、日本企業がIoTセキュリティ脅威に効果的に対応するための戦略と技術的ガイドラインを提供することを目指す。最終的に企業のセキュリティ体制の強化と将来の脅威への備えを期待する。

ターゲットデバイス

- スマート工場機器
- スマート家電
- ウェアラブル
- センサー
- ビーコン
- アクチュエータ
- カメラ
- ゲートウェイ
- スマートメーター
- RFIDタグ