自律型IoTシステムのためのレジリエント・アーキテクチャに関する研究

Research on Resilient Architecture for Autonomous IoT Systems

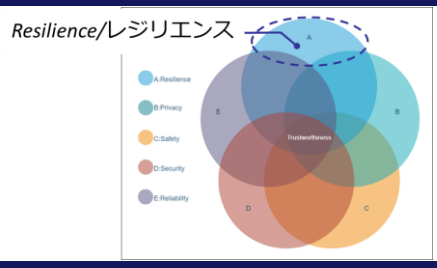
白石敬典・法制倫理分科会・情報セキュリティ大学院大学

Abstract — In recent years, trustworthiness has been attracting attention in the IoT field. The IoT, which is becoming increasingly widespread, is expected to realize autonomous IoT systems through the application of new network models and new technologies, but at the same time, it is becoming a target of various attacks. In particular, the damage to critical infrastructure is enormous. In this research, we analyzed and organized typical threats to IoT systems, and proposed an architecture that focuses on resilience, which is one of the components of trustworthiness.

この研究のモチベーションって？　攻撃からの「回復・事後」の研究は未成熟！回復力が必要です！

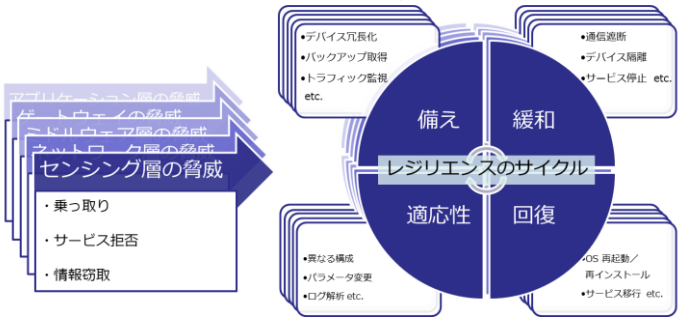
近年IoT分野では，トラストワージネスが注目されている．普及の進むIoTでは，新しいネットワークモデルや，新技術の適用により，自律型IoTシステム*1の実現が期待されている反面，様々な攻撃の標的になっている．特に重要インフラ分野における被害は甚大である．本研究では，IoTシステムに対する代表的な脅威を分析，整理し，トラストワージネスの構成要素の1つである，レジリエンス”に着目したアーキテクチャを提案した．

*1：本研究では，IoTデバイス自身が状況を判断，制御し，可能な限り人間による判断が介在しない仕組み．重要インフラ等のシリアスな分野での利用を想定



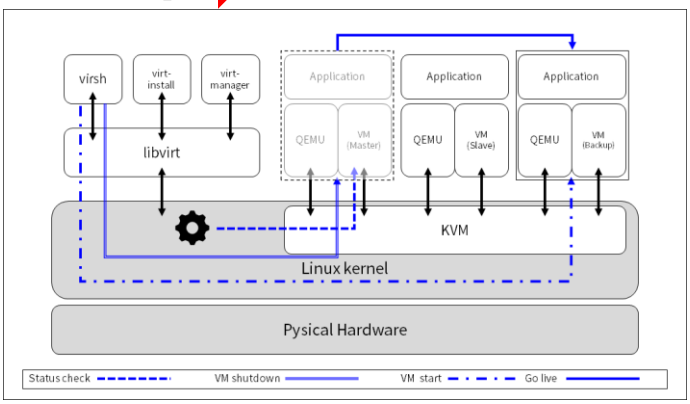
何をやったの？　脅威／対策の整理と分析です！

・5層27個の脅威を整理・分析 ➡被害・影響毎に分類



どう評価したの？　プロトタイプ実装と考察です！

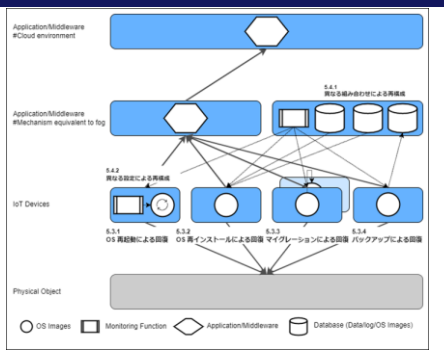
・「マイグレーションによる回復」　「異なる組み合わせによる再構成」 ➡低コスト且つ導入難易度の低い実装



何を提案したの？　アーキテクチャの提案です！

・脅威／対策の整理と分析をもとに，アーキテクチャに必要な要素を明確化

・4つの回復手段と，2つの適応性手段＋備えと緩和手順を提案



結論どうなの？　つまりこういうことです！

・実現が期待されている自律型IoTシステムのための，回復力を備えたレジリエント・アーキテクチャを提案
・レジリエンスの回復と適応性に着目
・仮想マシンの切り替えを平均1分18秒で実施
・可用性を維持しつつサービスの切り替え可能
・切り替え前後で異なる状態 ➡多様性・信頼性のあるIoTシステムを実現

参考文献

[1] ISO/IEC 30147:2021 — IEC Webstore, IEC 2021. https://webstore.iec.ch/publication/62644 (visited on Feb. 8, 2022)
[2] National Infrastructure Advisory Council, https://www.dhs.gov/xlibrary/assets/niac/niac-a-framework-for-establishing-critical-infrastructure-resilience-goals-2010-10-19.pdf (visited on Feb. 8, 2022)
[3] Vikas Hassija, Vinay Chamola, Vikas Saxena, Divyansh Jain, Pranav Goyal and Biplab Sikdar, A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures, IEEE Access (Volume: 7), June 2019, Pages 82721 - 82743, DOI: http://dx.doi.org/10.1109/ACCESS.2019.2924045 (visited on Feb. 8, 2022)
[4] 松井俊浩(2020) 『IoT セキュリティ技術入門』，日刊工業新聞社.