WASEDA University

スマートエスイー 修了制作

WASEDA NEO Smart SE

IoTシステムのアジャイル開発時のセキュリティ対策の見える化

ドコモ・システムズ株式会社　　山本啓了

開発における問題点

IoTシステムは多種多様のシステム・機器等が使われており、アジャイル開発で段階的にリリースされる際に、アーキテクチャーが変更されるケースが想定されるが、セキュリティ対策をどの段階で何をどこまで対策すべきかの指針が明確ではない。

手法の適用による解決

ユーザーストーリーマッピング作成時にセキュリティ対策を検討する手法を提案する。これにより、事前にリスクを共有することになり、適切なタイミングで対策を実装できること、開発者内で認識合わせができ、セキュリティホールを防ぐ効果が期待できる。

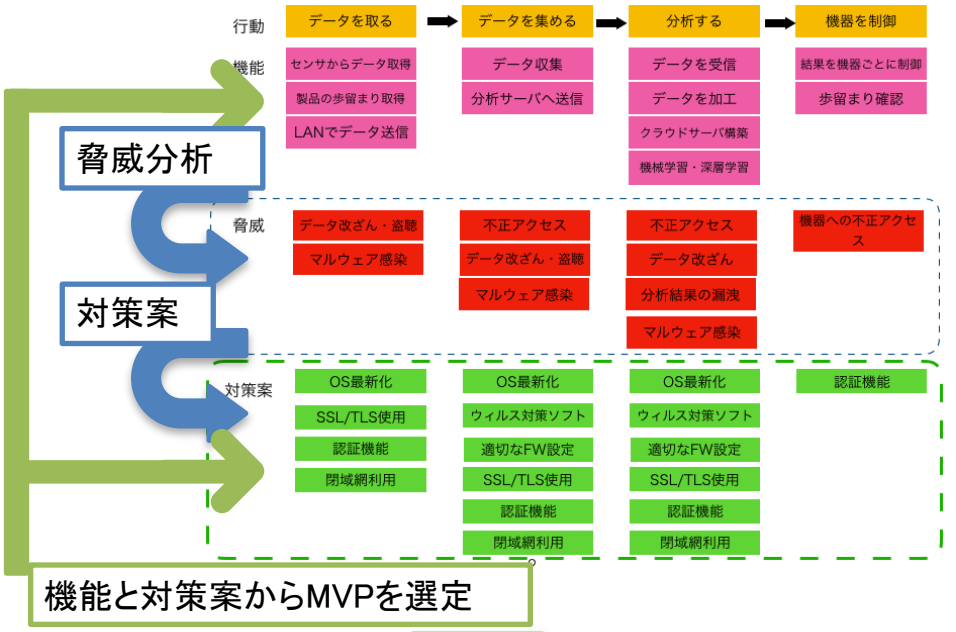
セキュリティを考慮したユーザーストーリーマッピング

提案手法は、ユーザーストーリーマッピングでMVP (Minimum Viable Product)を選定する前にセキュリティ対策を検討する。機能だけでなく対策案を含めてMVPを選定する方式。以下手順。(図2,図3参照)

1.ユーザーストーリーマッピング作成
2.守るべきモノを特定
3.各機能に対して脅威分析
4.脅威に対抗する対策案検討
5.対策案を含めてMVP選定
6.開発・実装
7.次イテレーションは4から

通常の手順(図1)では、セキュリティ対策状況は不明。本手法(図3)では、何の対策をどこにしているかが明確となる。

図2.本手法でのユーザーストーリーマッピング

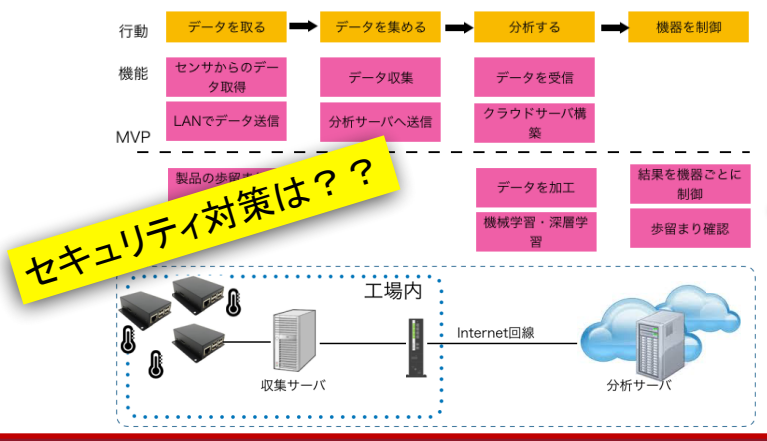


まとめ

本手法により、各イテレーションでMVPとして採用する機能に事前にどのようなリスク・対策があるか、また、開発時に何を対策したかを『見える化』することができる。

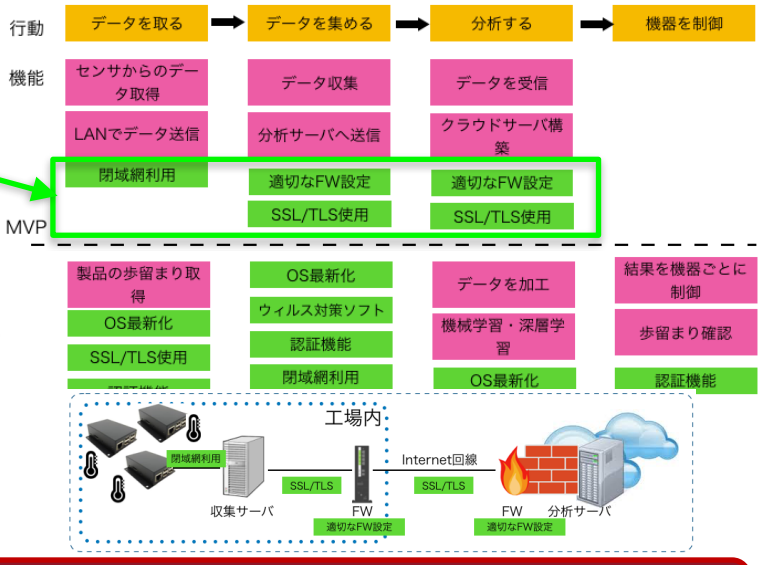
課題として、ユーザーストーリーマッピングの肥大化、対策案の組合せ・優先付けの明確化などがある。

図1.通常の手順の結果



セキュリティ対策実施

図3.本手法の結果



スマートエスイー　スマートシステム＆サービス技術の産学連携イノベーティブ人材育成