

IoTソフトウェアの信頼性とレジリエンスを高める ZT-OTA Update Framework

青木 信雄¹, 竹房 あつ子^{1,2}, 石川 裕³, 小野 泰司⁴, 坂根 栄作², 合田 憲人^{1,2}

¹総合研究大学院大学, ²国立情報学研究所, ³大妻女子大学, ⁴情報セキュリティ大学院大学

どんな研究？

IoT機器をきっかけとしたサイバー攻撃が問題視されており，IoT機器上で動作するソフトウェアの安全性を保証し，悪意あるソフトウェアによる脅威を自動的に軽減する仕組みが必要

「IoTシステムのソフトウェアの信頼性とレジリエンス」の実現を目指し，IoT機器のソフトウェアを自動的かつ安全に更新する仕組みを構築

何が課題？

■ソフトウェア更新（OTA）の安全性

- インターネットを介するソフトウェア更新は便利
- 一方、OTA自体の悪用を防ぐことが不可欠

■ソフトウェアの信頼性（安全性）の保証方法

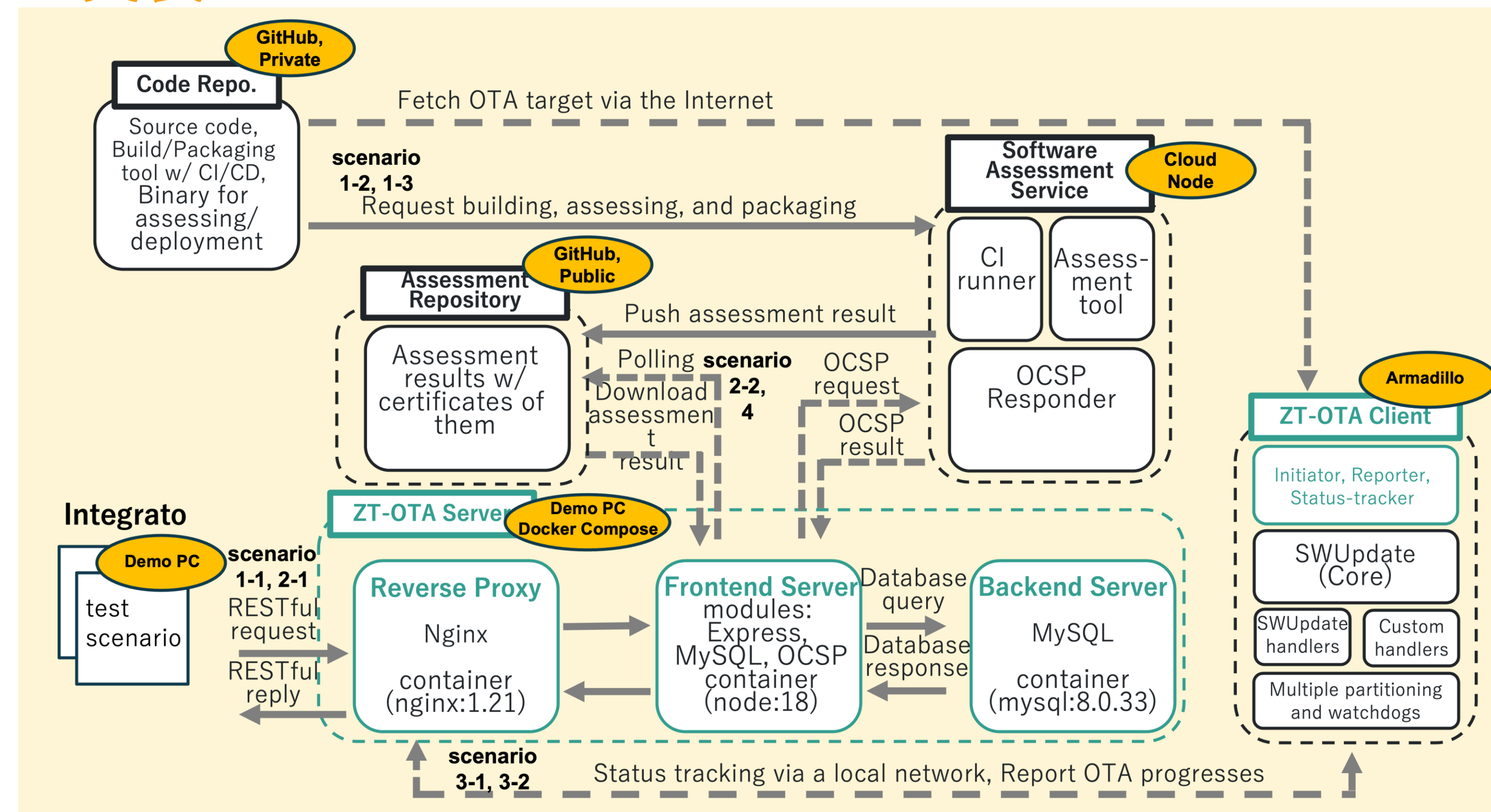
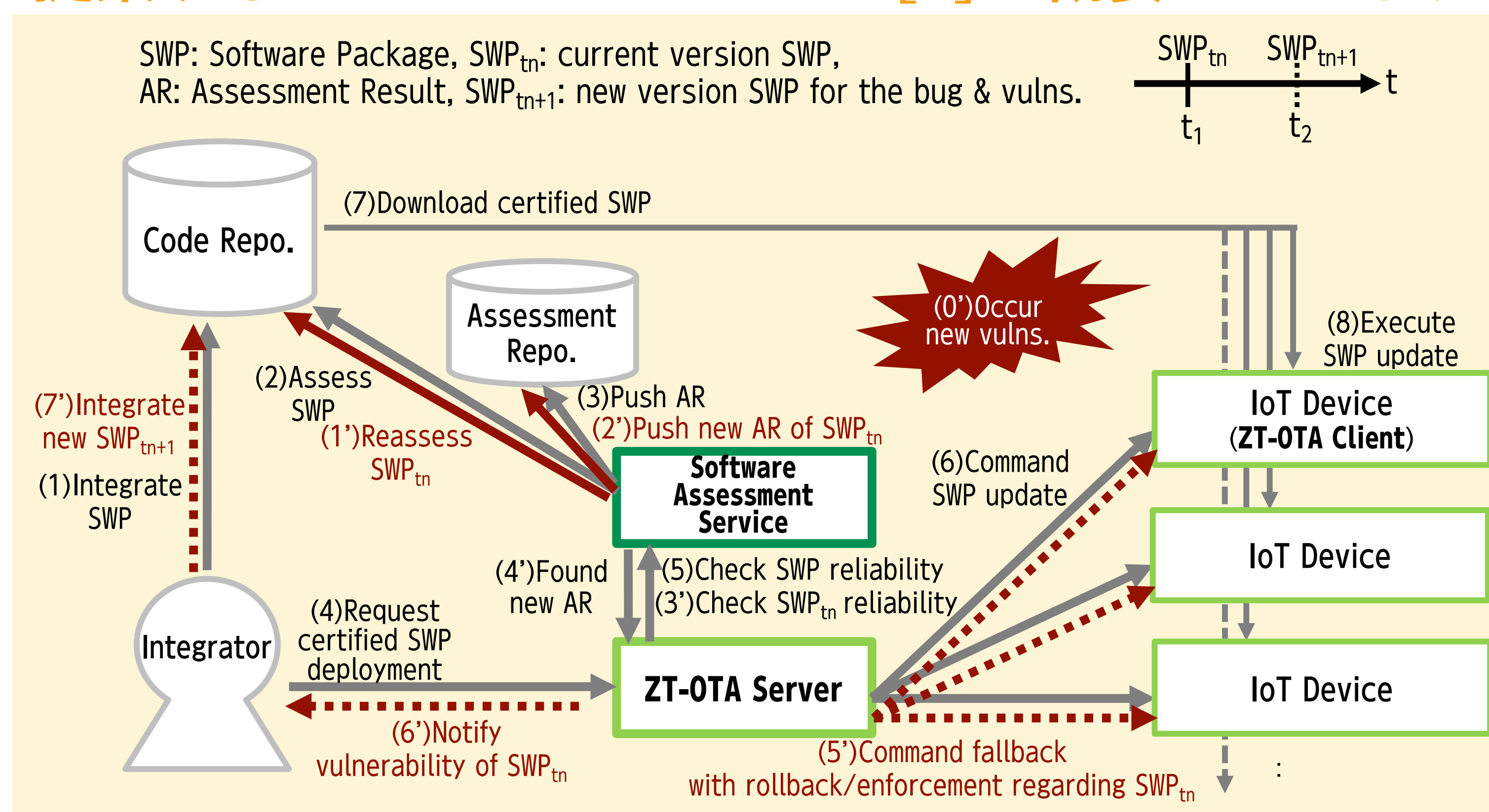
- OTAの一連のプロセスの中でどう保証すべきか

■デプロイ後の継続的対策

- デプロイ後も増え続ける脆弱性にどう立ち向かうか

研究内容（方法・結果・結論）

提案するZT-OTA Framework[1]の概要とプロトタイプ実装



安全なOTAの仕組み

ソフトウェア更新に対する攻撃への耐性を持ち，IoT機器の状態を常に監視し，ソフトウェアのインストール失敗時においても継続的OTAを提供

- ソフトウェア更新に対する既知の攻撃への対策
 - 意図的に駆動ソフトウェアのバージョンを下げる攻撃や

バージョン管理の脆弱性を悪用する攻撃など

- ソフトウェア更新の進捗の監視と失敗時の対処
 - OTA ClientはOTA Serverへ随時ステータスを報告
 - インストール後のIoT機器内での死活確認を行い，

ソフトウェアの新たな脆弱性への対処

IoT機器へ配布済のソフトウェアに影響しうる新たな脆弱性を瞬時に認識し，早期対処へつなげる

- ソフトウェア認証サービスと連携し，
 - 配備済みソフトウェアの深刻な脆弱性を監視
- 深刻な脆弱性が確認された場合
 - IoT機器へ対処内容を指示
 - Integratorへ更新ソフトウェアの修正等の対処を指示
- 対処済みソフトウェアのIoT機器への配備，再実行

ソフトウェアの安全性を保証

第三者機関がソフトウェアの脆弱性検査を実施し，ソフトウェアとともに検査結果を公開する仕組みを提供

- ソフトウェア認証サービス[2]との連携
 - ソフトウェア認証サービスによる検査済みソフトウェア（認証済ソフトウェア）を高信頼なソフトウェアとする

デモシナリオと見どころ

1. ソフトウェア認証サービスと連携しOTAを使ってデプロイしたいソフトウェアを準備
 - 1. ソフトウェア認証サービス側を参照
2. OTAの実行準備
 - 1. ZT-OTAサーバへOTAを使ってデプロイしたいソフトウェア，IoT機器の情報登録
 - 2. IoTソフトウェアの信頼性の継続的検証
3. IoT機器上でOTA実行
 - 1. IoT機器はOTAの実施有無を確認
 - 2. OTAサーバはOTAの実施・進捗状況の監視
4. デプロイ後に発見された新規脆弱性対策
 - 1. 外部から新規脆弱性が発見され，その脆弱性がIoT機器上にデプロイ済みのソフトウェアに対して影響があることを確認
 - 2. 必要な対処の実施

参考文献 [1] N. Aoki *et al.*, "ZT-OTA Update Framework for IoT Device toward Zero Trust IoT," In NETSAP 2024, July 2024. [2] 合田他, "研究ソフトウェアの信頼性保証のためのソフトウェア認証機構," SCIS2024 4D1-4, IEICE, Jan. 2024. [3] "The Update Framework Specification," Apr. 2023. [Online]. Available: <https://theupdateframework.github.io/specification/v1.0.33/> [4] B. Moran *et al.*, "A Firmware Update Architecture for Internet of Things," RFC 9019, IETF, Apr. 2021.

謝辞 本研究は，JST，CREST，JPMJCR21M3，次世代研究者挑戦的研究プログラム JPMJSP2104の助成を受けている