理論とシステムソフトウェアの融合で安全・安心なIoTを実現する

# Society 5.0のためのゼロトラストIoT

**ZT-IoTプロジェクト**（竹房 あつ子，関山 太郎，福田 健介，蓮尾 一郎，合田 憲人，石川 裕）

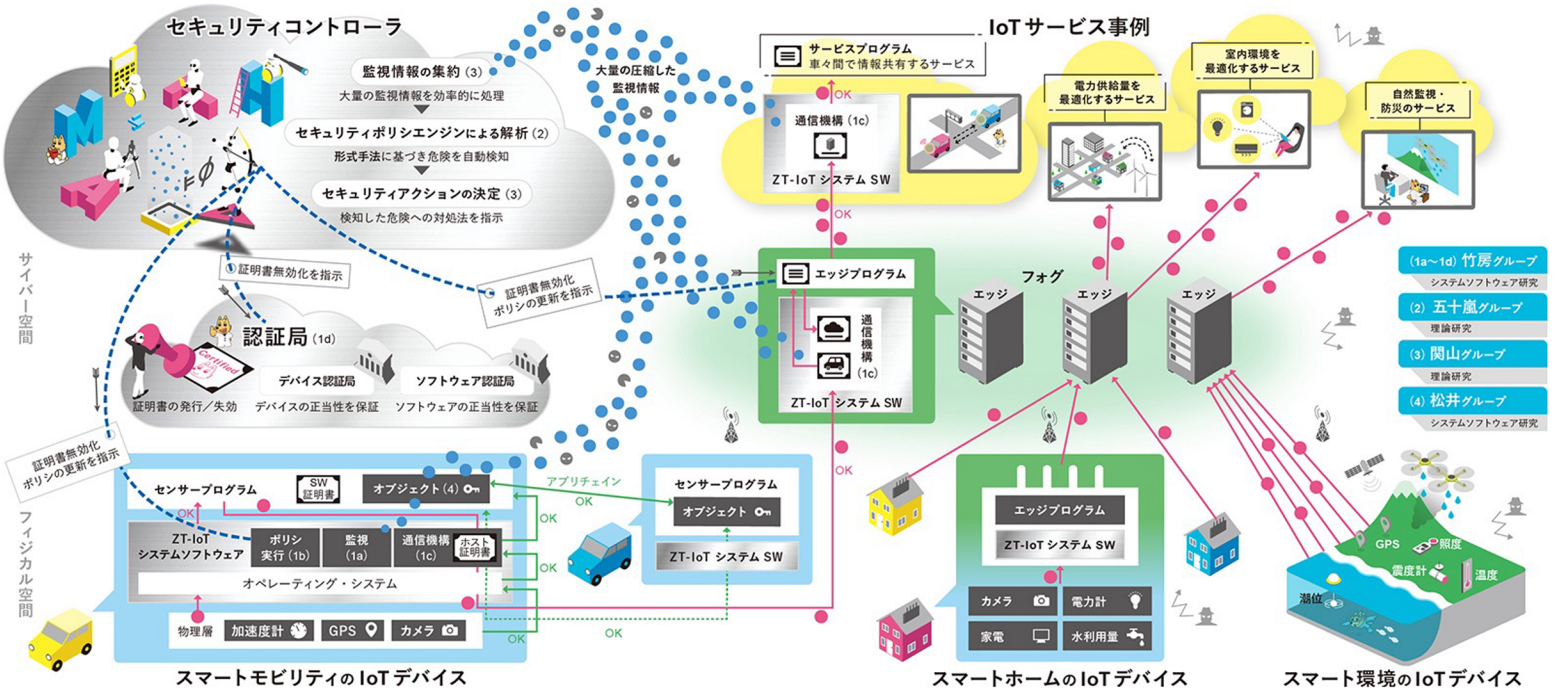
## どんな研究？

Society 5.0では，IoT情報をクラウドに収集，AI処理し，生活の質向上，CO2削減，防災・減災等へ活用することが期待されていますが，サイバー攻撃により重大な被害を及ぼす恐れもあります．理論とシステムソフトウェアの技術を融合して，**ゼロトラスト**の考え方を基本とした安全・安心なIoTシステムの実現を目指します．

## 何がわかる？

■Society 5.0とIoT (Internet of Things)の関係
■社会的インパクト
■ゼロトラストIoT (ZT-IoT)とは？
■ZT-IoTのための理論研究とは？
■ZT-IoTのためのシステムソフトウェア研究とは？

## 研究内容（方法・結果・結論）



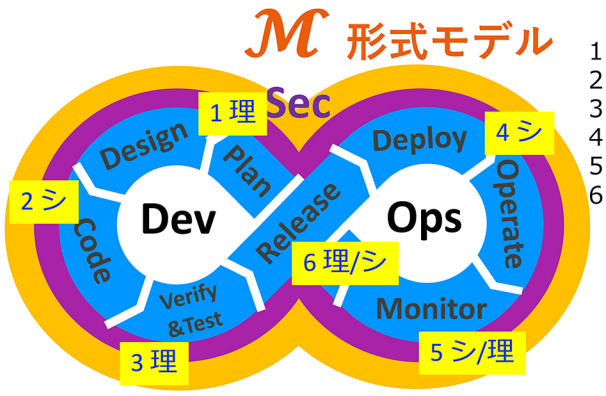

### ゼロトラストIoTとは

ゼロトラストは，ファイアウォールやVPNなど外部と隔離した安全な環境を前提とせず，継続的な監視，分析でセキュリティ対策を改善していく，という考え方です．これをSociety 5.0のためのIoTシステム(ZT-IoT)に適用します．

### 研究内容

セキュリティ対策が場当たり的であると，情報漏洩や乗っ取りなどの重大な事故につながります．我々は数学的理論に裏打ちされたセキュリティ対策技術を研究し，抜け穴のない，安心・安全なIoTシステムの検証技術を確立します．
システムソフトウェア研究では，理論研究の成果と連係し，継続的に監視，分析，対処するZT-IoTシステムソフトウェアを開発します．

### ZT-IoT的システムソフトウェアと形式検証の研究




1 モデル検証
2 実装
3 システム検証
4 運用
5 監視
6 見直し

*Proof-guided DevSecOps*を実証

JST CREST 「形式検証とシステムソフトウェアの協働によるゼロトラストIoT」https://zt-iot.nii.ac.jp/
国立情報学研究所，京都大学，情報セキュリティ大学院大学，東京情報デザイン専門職大学

理論とシステムソフトウェアの融合で安全・安心なIoTを実現する

# IoTシステムのソフトウェアの信頼性とレジリエンスを強化するソフトウェア更新

青木 信雄[1], 竹房 あつ子[1,2], 石川 裕[1,2], 小野 泰司[3], 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]情報セキュリティ大学院大学

## どんな研究？

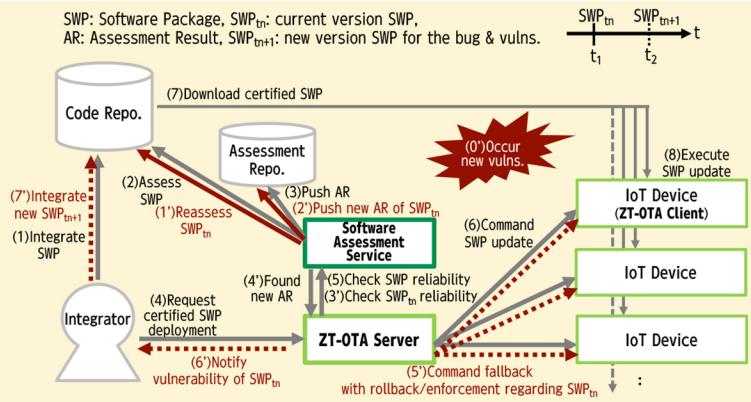
IoT機器をきっかけとしたサイバー攻撃が問題視されており、IoT機器上で動作するソフトウェアのセキュリティを保証し、悪意あるソフトウェアなどの脅威を自動的に軽減する仕組みが求められている。
「**IoTシステムのソフトウェアの信頼性とレジリエンス**」の実現を目指し、**IoT機器のソフトウェアを自動的かつ安全に更新する仕組み**を研究している。

## 解決すべき課題

- ■IoT向けの安全なソフトウェア更新(OTA)の仕組み
- ■ソフトウェア更新失敗時のIoT機器の振る舞い
- ■実行されるソフトウェアの安全性(信頼性)の保証の方法
- ■ソフトウェアの新たな脆弱性への自動的緩和処置

## 研究内容（方法・結果・結論）

### 提案するZT-OTA Framework[1]の概要




- ■安全なOTAの仕組みを提供
- ■ソフトウェア認証サービスとの連係でソフトウェアの安全性を保証
- ■ソフトウェアの新たな脆弱性への自動的緩和処置を提供

### 安全なOTAの仕組み

**従来のOTAと同様に既知のソフトウェア更新に対する攻撃への耐性を持ち、くわえてIoT機器がソフトウェア更新に失敗した際の原子性を強化する仕組みを提供**

- ■ソフトウェア更新に対する既知の攻撃への対策
  - ■(*e.g.* Roll-back攻撃, Check-time-to-use attacks攻撃)
- ■ソフトウェア更新の進捗の監視と失敗時の対処
  - ■ZT-OTA ClientはZT-OTA Serverへ随時ステータスを報告
  - ■A/B updateを用いて原子性を強化し、ソフトウェア更新の失敗によるIoT機器への人的復旧作業を最小化

### 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
  - ■脆弱性検査を提供する第三者機関[2]
  - ■ソフトウェアを独自の検証器で検査し、検査済みと示す証明書・検査結果の発行・失効操作を実施
  - ■外部の脆弱性データベースが更新されると、検証器を更新するかどうかをソフトウェア認証サービスが判断する
- ■ソフトウェア認証サービスとの連携
  - ■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)を信頼性の高いソフトウェアとして扱う

### ソフトウェアの新たな脆弱性への自動的緩和処置

**IoT機器へ配布済のソフトウェアに対する新たな脆弱性への対策を自動的かつ迅速に提供**

- ■修正パッチや更新ソフトウェアの作成を促す
  - ■ZT-OTA Serverは、IoT機器へ配布済のソフトウェアに新たな失効操作の発生や再検査結果の発行がないか探索する
  - ■新しい再検査結果を発見次第、IoT機器への自動的な緩和処置の命令、及び、Integratorへ修繕を要求
- ■IoT機器への自動的な緩和処置の命令
  - ■失効済みソフトウェアリストを通知し、事前に指定されたバックアップソフトウェアの縮退運転への切り替え、及び、モジュール・プロセス単位の最小権限の縮退実行を命令

### 用語説明

- ■OTA: 人の介在を最小限に抑え、維持管理費用・脆弱性の脅威の低減を目的に設計されていることが多く、無線通信などを用いたソフトウェア更新手法
  OTA update/OTA mechanism/FOTA/SOTAなどの総称として用いる
- ■ソフトウェア更新における原子性: ソフトウェア更新に失敗した際に更新前の状態へ復元できる能力
- ■A/B update: 原子性のあるソフトウェア更新手法の一つであり、一般にパーティション多重化を実装に要し、更新失敗に伴う計算機の不安定動作の誘発を防ぐ手法
- ■Check-time-to-use攻撃: リソースへアクセスする時点とリソースを利用する時点との間にリソースが改竄されることで予期せぬ動作を誘発する攻撃
- ■Roll-back攻撃: 過去に作成された既知の脆弱性を含むソフトウェアを計算機へインストールさせる攻撃
- ■その他の攻撃[3]

[1] N. Aoki *et al.*, "ZT-OTA Update Framework for IoT Device toward Zero Trust IoT," In NETSAP 2024, July 2024.
[2] S. Shimizu *et al.*, "Certification Mechanism to Assure Software Reliability with Digital Signature," Poster presented at ISGC 2023 HEPiX Spring 2023 Workshop, Mar. 2023.
[3] "The Update Framework Specification," Apr. 2023. [Online]. Available: https://theupdateframework.github.io/specification/v1.0.33/
本研究は、JST、CREST、JPMJCR21M3、科学技術イノベーション創出のための大学等フェローシップ創設事業、JPMJFS2136の助成を受けている