中小企業デジタル化・DX促進マッチングフェア2023
最新セキュリティ対策
プラットフォームファームウェア
レジリエンスのご提案

Kyoto Software Research

株式会社京都ソフトウェアリサーチ

2023/08/31

Doc.No. ： 006366J-201

Galba

Fugue
FLASH FILE SYSTEM

サイバー攻撃

IoT機器のサイバー攻撃被害事例

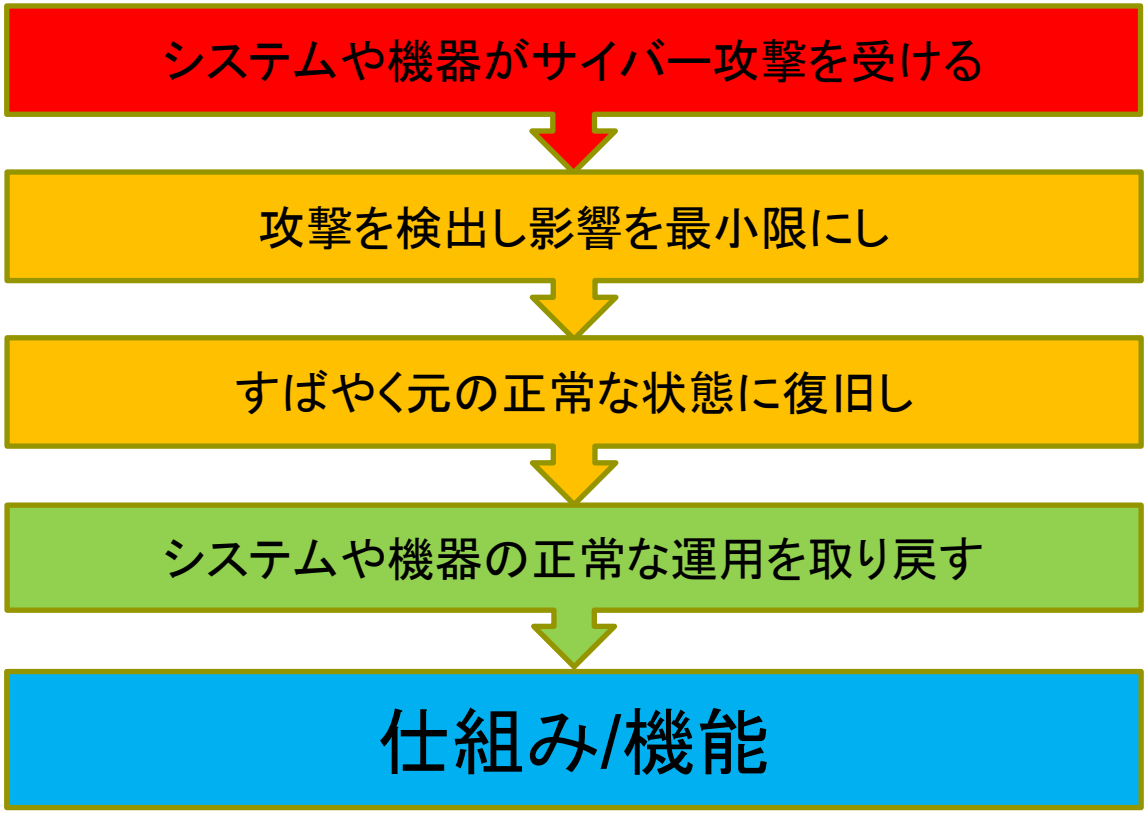
- 2016年10月、DNSサービス・プロバイダDyn社、大規模なDDoS攻撃を受ける
  - 同社DNSを利用するNetflixやTwitter等の多数の有名サービスがアクセス不能
  - IoTマルウェア“Mirai”に感染したIoT機器が踏み台に利用され、Dyn社のサーバに攻撃をしかける
- 2021年5月、燃料供給のコロニアル・パイプライン社、ランサムウェア攻撃を受ける
  - 犯罪者グループDarkSideからのランサムウェア攻撃
  - アメリカ最大規模のパイプラインが1週間にわたって操業停止
  - 身代金440万ドル（約4億8000万円）を支払う
    - 対策についてバイデン政権での大統領令が発令

サイバーセキュリティの取り組みの必要性

- IoT機器の場合は、直接攻撃されるだけではなく、踏み台にされ、加害者となるケースがある
- 攻撃によりサービスの停止などが発生すると、企業の社会的信用などにも被害が及ぶ
- 事が起こってからの対応コストは甚大
- 総務省、経産省、
  - サイバーセキュリティ政策の対応
  - ガイドラインの公開とその適応
  - HPにて公開
- サイバーセキュリティ対策はもう他人事ではない

サイバーレジリエンス

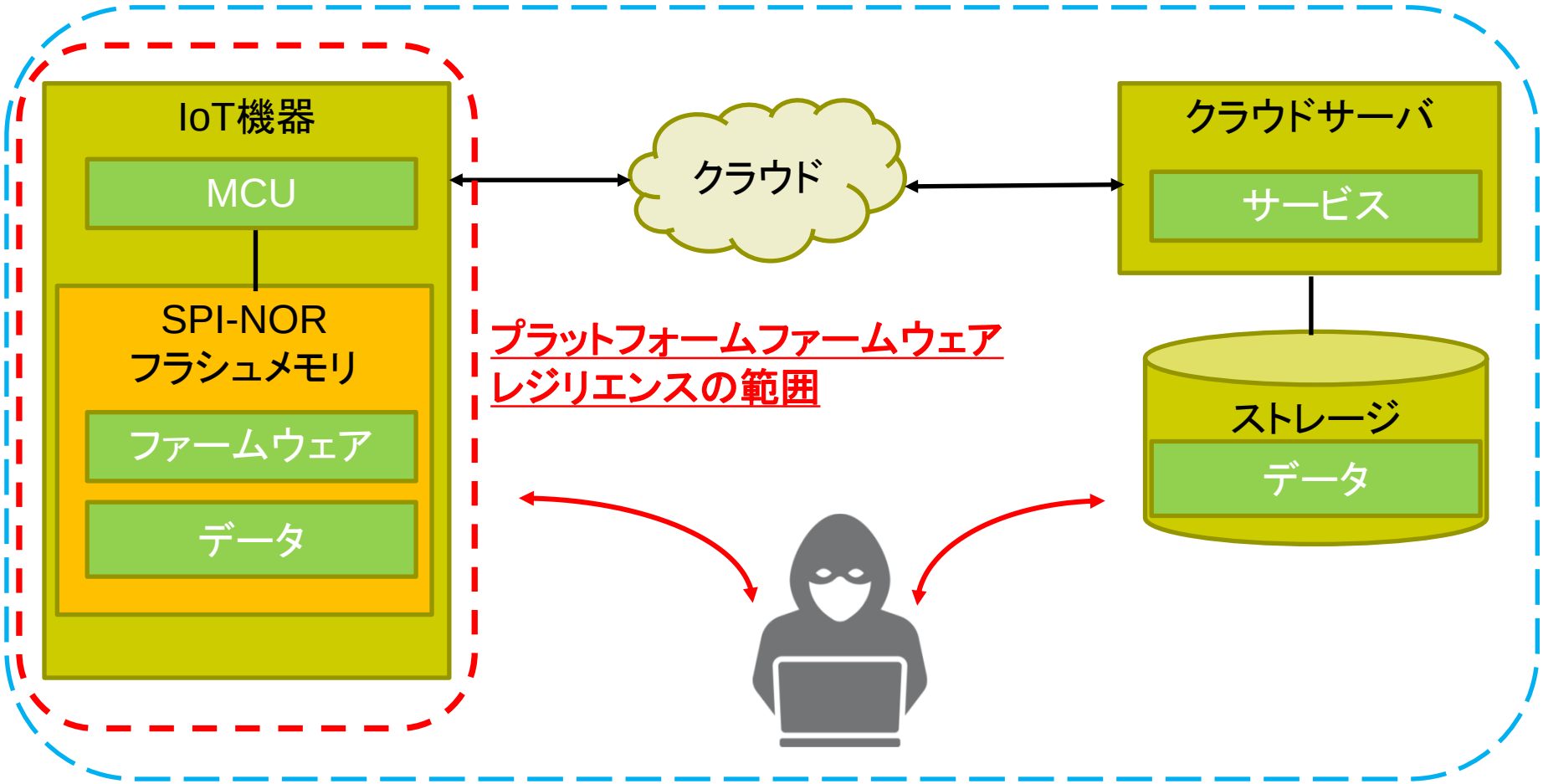
サイバーレジリエンスとは



プラットフォームファームウェアレジリエンス

- プラットフォーム ファームウェア レジリエンスとは
  - サイバーレジリエンス全体の中での
  - クラウドと通信するIoT機器のプラットフォームとしての
  - ファームウェア及びデータを
  - 対象としたレジリエンス（回復力、適応力）
    - プロテクション
      - 機器側のファームウェアとデータを保護し
    - ディテクション
      - 機器側のファームウェアとデータの異常を検出し
    - リカバリー
      - 機器側のファームウェアとデータを復旧する
  - 米国国立標準技術研究所「NIST SP800-193」文書に定義
    - NIST SP800-147をサイバーレジリエンスの観点で拡張、整理
  - 「NIST SP800-160 Vol.2 Rev.1」文書にサイバーレジリエントなシステムの開発、として発行

プラットフォームファームウェアレジリエンスの範囲



プラットフォームファームウェアレジリエンスを支える機能（1）

従来のセキュリティ対策の問題点（1）

- セキュリティ対策の主眼が攻撃に対する防御となっている
  - 攻撃の影響を素早く検知できない
  - 攻撃の影響からの復旧方法と連動していない
- ハードウェア由来のRoT（信頼の起点）を使用していない
  - ソフトウェアベースだと信頼性が保てない
- セキュアな対応がMCU（プロセッサ）までとなっている
  - ファームウェア、重要なデータが格納されるストレージのアクセスまでセキュアになっていない
  - 機器ストレージ↔クラウドストレージ間でセキュアになっていない

従来のセキュリティ対策の問題点（2）

- 最近のMCU（プロセッサ）は外付けのSPI-NORフラッシュメモリが必須になっている
- このSPI-NORには重要な情報が保存されいる
  - ファームウェア
    - IP、ノウハウ等
  - データ
    - センシングデータ
    - AIモデル等
- これらユーザの価値の源泉を保護できていない
- 攻撃はネットワークからだけとは限らない
  - サプライチェーンの中でも攻撃は可能

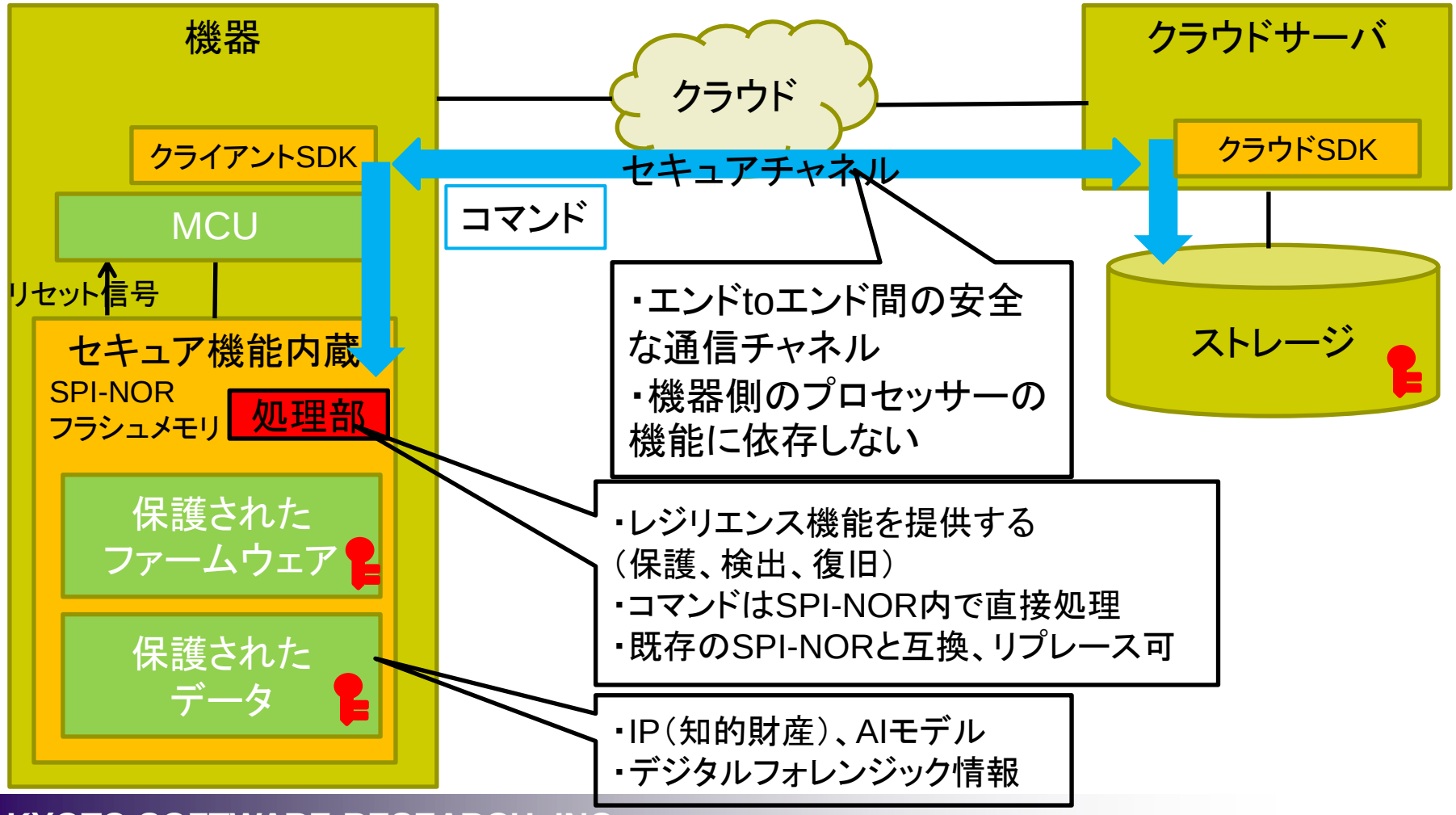
本提案システムのメリット（1）

- ファームウェア、データの改ざんの検出とリカバリ機能の提供
- 機器の真正性の確認
- セキュアWDTとクラウド側との連携による機器のリセット実行
  - SPI-NORからリセット信号を生成可能
- 機器側ストレージ、クラウド側ストレージ間の真のセキュアチャネルの確立
  - 既存のセキュア機能に依存しないで実現
- クラウド側からの機器の安全なファームウェアの更新
- 既存のセキュア機能、技術との相互補完

本提案システムのメリット(2)

- ハードウェア由来のセキュア機能を提供
- ローコストで導入可能
  - SPI-NORフラッシュメモリとして提供
  - レジリエンス機能を支援する機能を内蔵
- 秘匿データのセキュアエリアへの安全な格納
  - デジタルフォレンジックのための情報の格納
- MCU(プロセッサ)のセキュア機能に依存しない
- セキュア機能の後からの有効化可能
- 既存のSPI-NORフラッシュメモリとリプレース可能
  - ピン互換、張替えだけでOK

本提案システムの構成図



提案内容

- 次世代のセキュリティ技術として求められている、レジリエンス機能をシステム/機器開発に提供したいと考えています
- 本提案技術では、セキュア機能内蔵SPI-NORフラッシュメモリを適切に操作するために、
  - 機器側に搭載する「クライアントSDK」と、
  - クラウドサーバ側に搭載する「クラウドSDK」

  を提供します
- 長年にわたって培ってきた組込み技術による
  - フラッシュメモリの操作技術
  - 独自の高信頼性ファイルシステム

  をベースに効果的な「SDK」を提供します

御社のメリット

- エッジデバイスでは、セキュリティは今後重要な項目となります
- レジリエンス機能を、機器とクラウドに搭載することによって、攻撃により影響を受けた場合、影響をいち早く検出し、回復する機能を低コストで実現することができます
- この事により、被害を最小化し、システム/サービスの速やかな復旧を実現できるものと考えます
- デジタル・ホレンジック情報の格納による証明能力の向上が考えらえます
- サプライチェーン上での脅威についても対応できます
- 電子デバイスのサイバーアタックからの脅威に対応できます

デモシステム

- デモシステムの実施ができます
  - 実際のチップ（SPI-NOR）を使ったデモシステム
  - 別途お時間をいただければ、デモを後日ご覧いただけます

会社紹介

会社概要

- 社名：株式会社京都ソフトウェアリサーチ
- 設立：1990年4月設立
- 本社：京都市下京区堀川通綾小路下ル綾堀川町
- 事業：
  - 組込みシステム向けに電断耐性のある高信頼性ファイルシステムを提供
    - フラッシュメモリの扱いは1994年から（28年の実績）
    - 国内唯一のファイルシステム専業メーカー
  - ソフトウェアの受託開発

お問合せ先

- 窓口　　：株式会社京都ソフトウェアリサーチ
  営業部　田中
- TEL　　：075-342-0794
- WEB　　：http://www.kyoto-sr.co.jp/
- E-Mail　：tanaka@kyoto-sr.co.jp

ご清聴ありがとうございます