# ハイライトレポート

2025.11.12

OTA入門ウェビナ
~FWアップデートの仕組みとセキュリティ対策のポイント~

## OTAとセキュリティ対策で守るIoT機器の未来

IoT機器の普及に伴い、出荷後の不具合修正や機能追加のニーズが急増しています。しかし、従来の現場対応ではコストや工数が膨らみ、セキュリティリスクも高まります。この課題を解決するのが、OTAによるFW（ファームウェア）アップデートと強固なセキュリティ対策です。OTA導入により遠隔から効率的かつ安全なソフトウェア更新が可能となり、更新失敗時の復旧や暗号化通信による安全性も確保できます。

本ウェビナでは、**OTA導入のメリット**、**FWアップデートの仕組み**、**セキュリティ強化のポイント**、そして**実践的な対策方法**などをわかりやすくご説明いたしました。

## OTA導入による利点と課題

従来のFWアップデートは、デバイスを物理的に接続したりメモリーカードなどの外部記録媒体を使用する必要がありました。これに対し、**OTAによるFWアップデートは無線通信で遠隔実施が可能**となり、人員や時間コストの削減、大量デバイスへの一括配信、出荷後の機能追加や不具合修正が容易になります。

一方で、無線通信を利用する特性上、改ざんや不正アクセスへの**セキュリティ対策が不可欠**であり、更新中断時にも安全に再開できるフェールセーフ設計が求められます。
さらに、CRAやJC-STARといった法規制への対応も、製品開発における重要な検討事項となります。

## FWアップデート方式の比較と選定ポイント

FWアップデート方式は主に以下の3種類があります。

■シングルバンク半面更新
- 更新前FWを残しつつ、OTAによる書き込みを行いたい

■シングルバンク全面更新
- ROM容量が小さいMCUでもOTAを行いたい

■デュアルバンク更新
- OTA中もアプリ動作継続が必須
  フェールセーフ/設計容易性を優先したい

各方式は、メモリの使い方、復帰動作、更新中の安全性が異なるため、製品仕様やMCUの機能に応じて選定することが重要です。

## OTAセキュリティ対策の技術要素

OTAによるFWアップデートには、外部ネットワークを介する特性上、複数のセキュリティ対策が不可欠です。

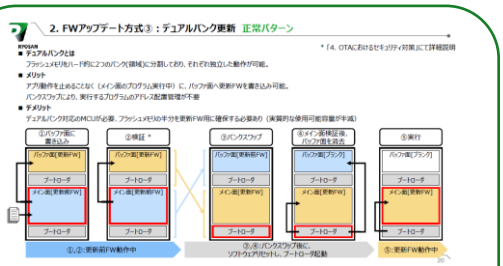
主な技術要素として、**「通信の暗号化」**、**「アップデートファイルの署名と検証」**、**「安全なブート機能」**、**「対象デバイスの事前認証」**、そして**「ロールバック」**が挙げられます。

これらを組み合わせることで、改ざんや不正アクセス、偽装アップデートなどのリスクを低減し、製品の信頼性を確保します。

### ■ 本日の登壇者 ■

株式会社リョーサン
木村 友哉
デバイス第一事業本部
技術支援部 第二課

株式会社リョーサン
内田 将之
技術本部
応用開発部 第一課




FWアップデート方式:
デュアルバンク更新 正常パターン


OTAセキュリティ対策の技術要素

他記事、ウェビナ情報はこちら

リョーサン テクラボ
エンジニアによりそうマガジンサイト