

wolfBoot

安全なファームウェアの更新、起動を実現するセキュアブートローダー

概要

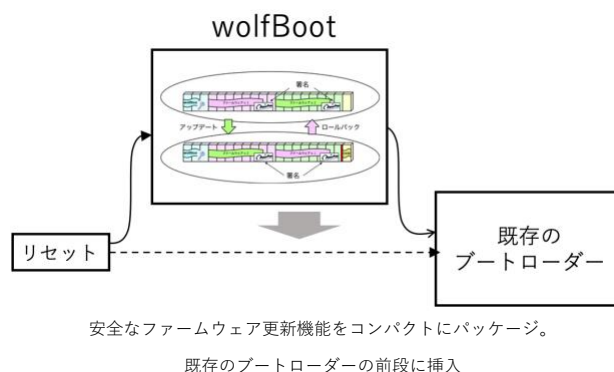
wolfBootはwolfSSLの暗号技術、セキュリティ技術を使い安全なファームウェアの更新、起動を実現したセキュアなブートローダーです。

従来この領域は、組み込まれるハードウェアやシステム構成、要求されるセキュリティレベルなどさまざまな条件に依存してしまうため、なかなか汎用のコンポーネントとして提供することは難しいとされてきました。その一方で、現実利用されるIoTデバイスや組み込みシステムでは、長期化する製品ライフサイクルの中で、進化させていかなければならないファームウェアをいかに安全に速やかに更新するかが重要な課題になってきています。

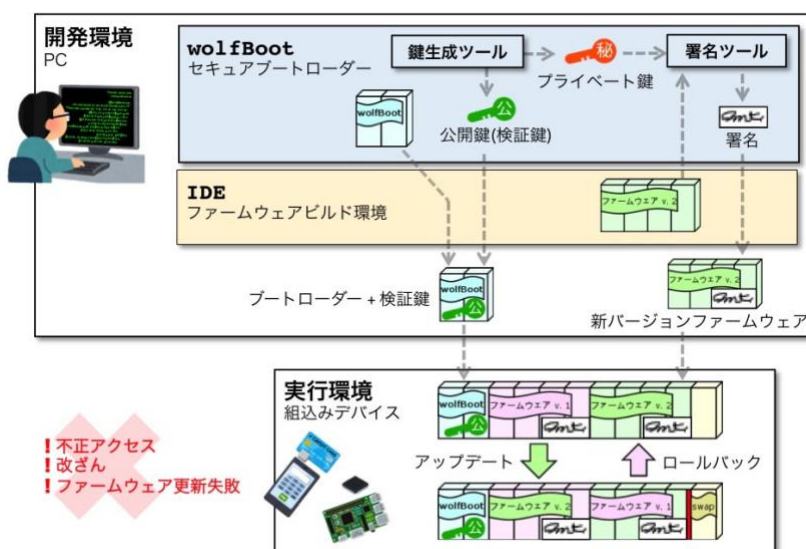
wolfBootは

1. 更新内容の一貫性や署名の検証
2. どんなタイミングで障害が発生しても必ず安全で完全なロールバック

など、安全なファームウェア更新のために必要となる機能のみにフォーカスした組み込み製品です。



他のwolfSSLの製品同様、組み込み向けを強く意識した小型、軽量である特徴を持つと同時にハードウェア依存部分を最大限に局所化しています。一方、一貫性や署名の検証のための暗号アルゴリズムエンジンにはwolfCryptを使用するため、楕円曲線暗号(ECC)はもちろんEd25519による署名検証など、最新の暗号アルゴリズムを使用した妥協のない安全で高速な検証を実現することができます。



拡張性

wolfBootは耐タンパー性などハードウェアレベルのセキュリティに対応するためのwolfTPMやその他のセキュアエレメントとの連携、遠隔からの安全な更新のためのwolfMQTT、wolfSSLなどの安全な通信チャネルとの連携など、トータルなファームウェアライフサイクル管理ソリューション構築のためのコンポーネントとしてご利用いただけます。

提供コンポーネント

- ・ wolfBootブートローダー本体
- ・ OS、サードパーティソフトに依存しない非OS実行
- ・ 署名ツール: 鍵生成とファームウェアへの署名
- ・ テスト用非OSアプリケーション
- ・ 単純ブート、OTAなどのサンプル集
- ・ ユーザマニュアル

ライセンスモデル

wolfBootはオープンソースと商用ライセンスの2つのライセンスを用意しています。オープンソース版は製品検討段階での社内のご評価などに全機能が無償でご利用可能です。ぜひ弊社サイトからダウンロードしていただき、充分なご評価にお役立てください。

商用ライセンスの詳細については<https://wolfssl.jp/license/> をご覧ください。

サポート対象プロセッサ

wolfBootはOSにとらわれないため簡単に移植でき、既存の組み込みソフトウェアプロジェクトに統合できます。プラットフォームの実例は特にテストされており、以下を含む多くのターゲットがすでにサポートされています：

STMicroelectronics STM32C0, STM32-F407, STM32L0x3, STM32G0x0/STM32G0x1, STM32WB55, STM32-F769, STM32H7, STM32L5xx, STM32U5

NXP i.MX-RT-1040, i.MX RT-1050, i.MX RT-1060, i.MX RT-1064, MCXA-153, T2080, LPC54606

SiFive HiFive1 RISC-V

Xilinx Zynq UltraScale+ (Aarch64)

TI TMS570LC435

ARMv8-m (Cortex-m33)

ARM Cortex-R

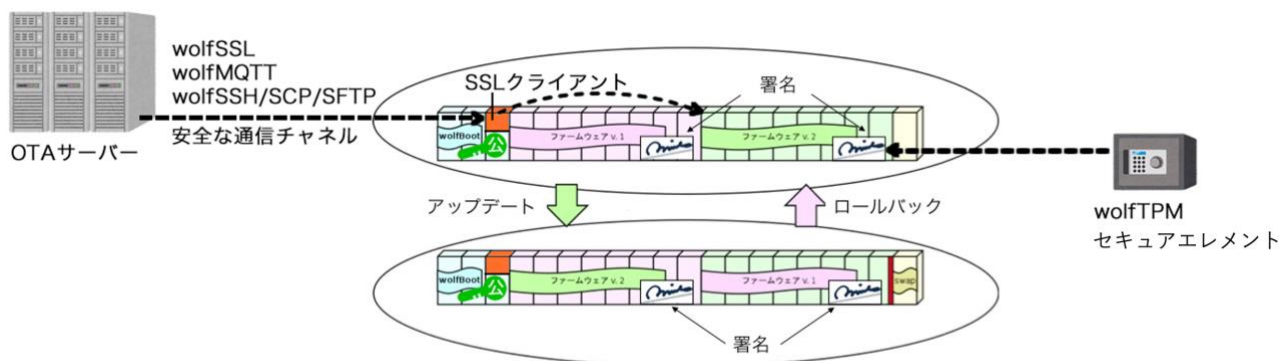
Cortex-A53 / Raspberry Pi 3

PowerPC

Renesas RA6M4, RX72N, RZ/N2L

Intel 11th Gen Core i7 (Tiger Lake)

最新のサポート状況については弊社までお問い合わせください。



ご質問、お問い合わせは info@wolfssl.jp までお気軽にご連絡ください。