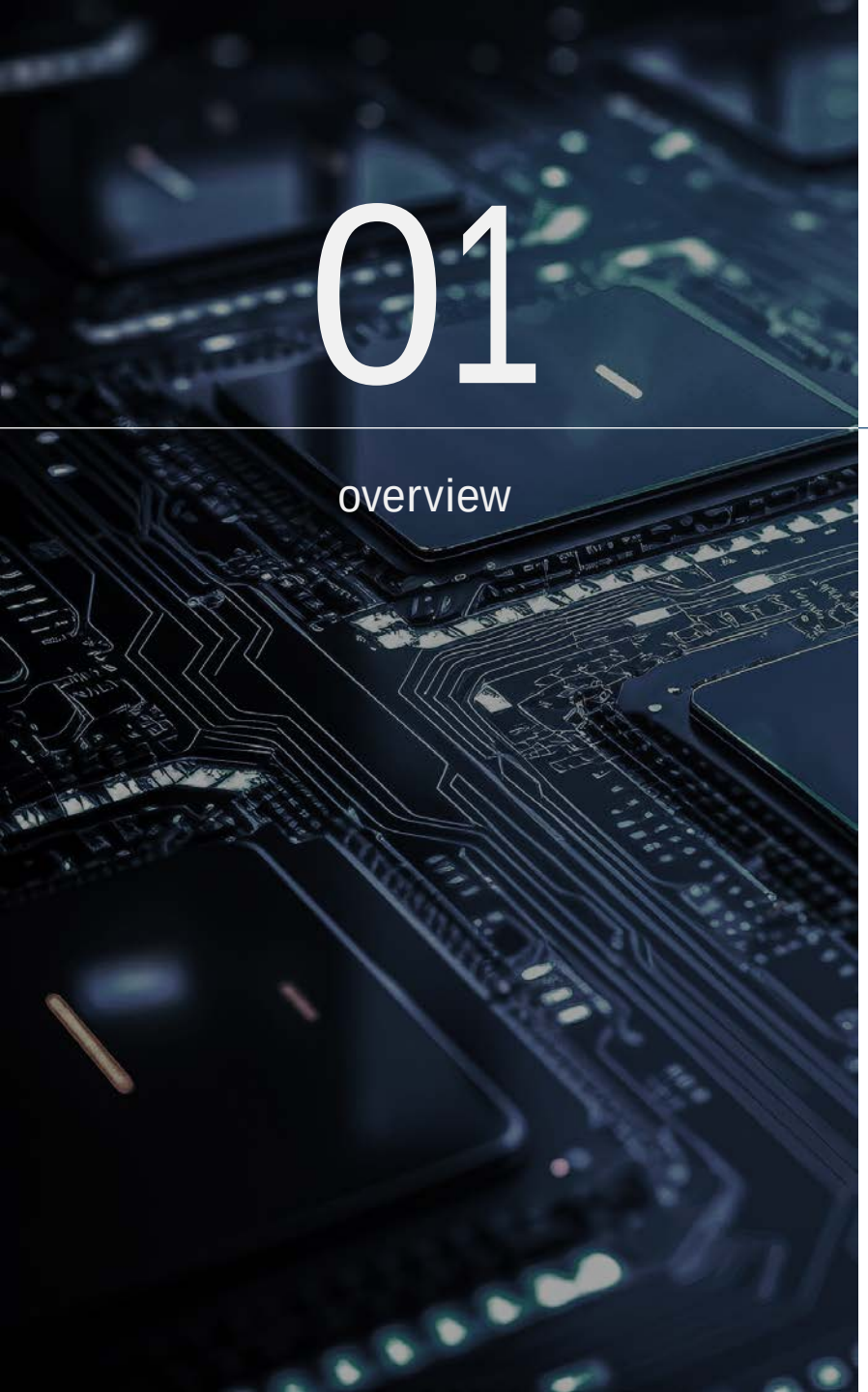
emBoot-Secure

安全なファームウェアアップデートソリューション



01

overview

emBoot-Secure製品概要

法令準拠／安全なファームウェア更新をサポートするブートローダ

emBoot-Secureが解決する課題

組み込み製品の脅威と課題

セキュリティ対応が製品の付加価値ではなく必須となった背景

EU CRAなど法令対応

EUサイバーレジリエンス法（CRA）などの厳格な規則により、製品のライフサイクル全体にわたる安全なアップデート機能が法的に義務付け

知的財産の盗難からの保護

暗号化されてないファームウェアは、リバースエンジニアリングやコード解析によるIP盗難リスクに常にされされています。

不正なクローン品作成

暗号化ファームウェアに認証のメカニズムがなければ、偽造品が製造販売されることにより、ビジネス的な損失を受けます。

emBoot-Secure

課題解決をサポート

emBoot-Secureとは？

組込ファームウェア更新用のセキュアなブートローダモジュール

RTOSの有無／CPU、コンパイラ依存性なしで、利用可能。
ハードウェア制御／ソフトウェア制御、ブートローダを起動する仕組みの柔軟性を持たせることができます。

デジタル署名によるファームウェアの真正性を確保

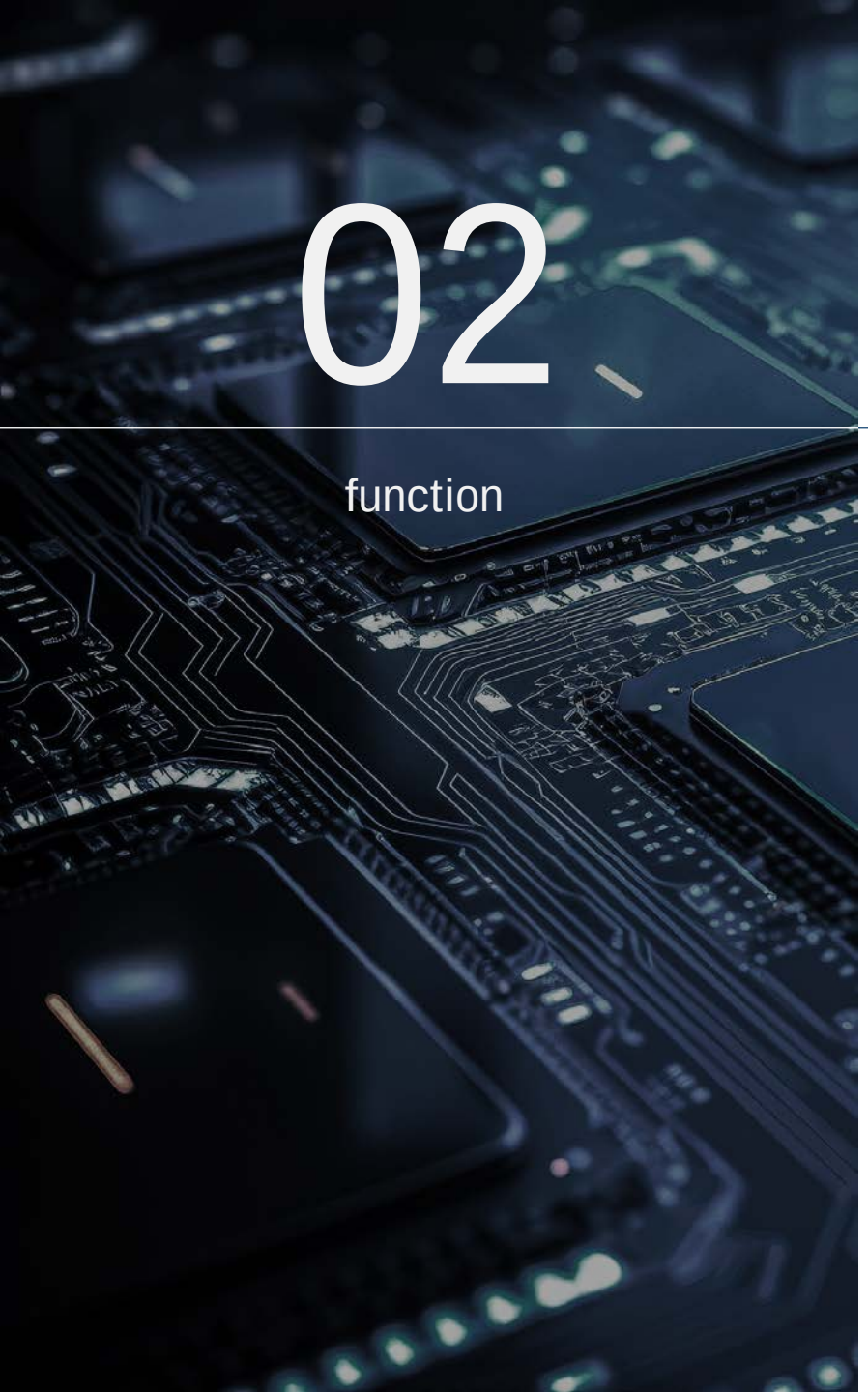
すべてのファームウェアアップデートに最新の暗号アルゴリズムによるデジタル署名を付与、デバイス側でのインストール実行前に署名検証を行います。これにより、ファームウェアの完全性を担保するとともに、第三者による改ざんや不正なコード変更を遮断します。

圧縮と暗号化で保護されたアップデートパッケージ

ファームウェアのアップデートパッケージは、転送効率の向上とストレージ占有率の低減を目的に圧縮します。また、配信フェーズにおいては強固な暗号化を施すことで、通信経路上のコンテンツ保護を実現。リバースエンジニアリングや不正な解析を未然に防ぎ、機密性の高いファームウェア資産を保護します。

生産ラインへシームレスな統合

emBoot-Secureは、現在のビルド・リリース工程に最小限の手間で導入いただけます。専用の署名サーバーを追加するだけで、機密性の高い秘密鍵を安全に管理しつつ、すべての署名プロセスを自動化。開発現場や製造ラインの既存業務を止めることなく、迅速かつ確実なセキュリティ強化を可能にします。



02

function

EmbiTeK
www.embitek.co.jp

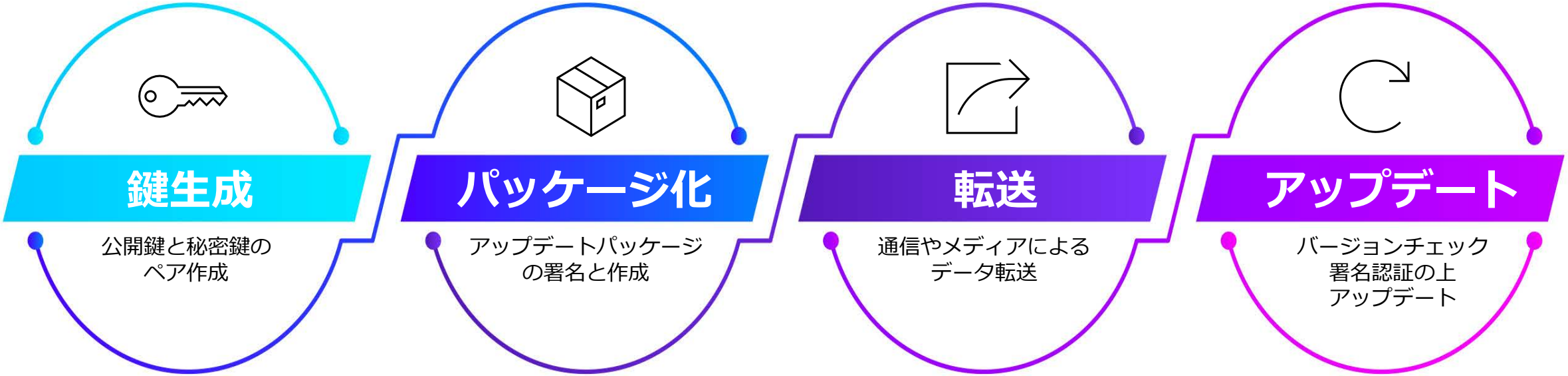
emBoot-Secure製品機能

お客様ファームウェアに実装

emBoot-Secureの適用プロセス

署名認証の実装

セキュアなファームウェアアップデートに必要な一連の機能を提供します。
既存製品にも対応可能

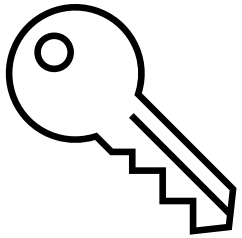


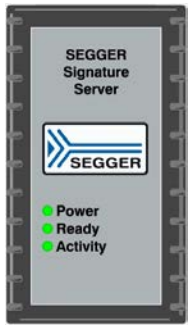
お客様製品ニーズに合わせて様々なシナリオに適合可能なフレームワーク

emBoot-Secure 鍵生成

鍵の生成と管理インフラの選択

ニーズに合わせて鍵生成と管理方法を選択可能です



	SEGGER Signature Server	SEGGER KeyGen
		
鍵の管理環境	専用ハードウェアベース 署名コンポーネント	ローカルPC上 ソフトウェア
秘密鍵の保護	秘密鍵はサーバに保管、外部へ一切 送信されません 【最高レベルの保護】	ローカルPCをユーザが制御 （バックアップ可能）
鍵の管理数	最大100個の鍵を管理可能	制限無し （Signature Serverへインポート可能）

emBoot-Secure パッケージ化

アップデートパッケージの署名と作成

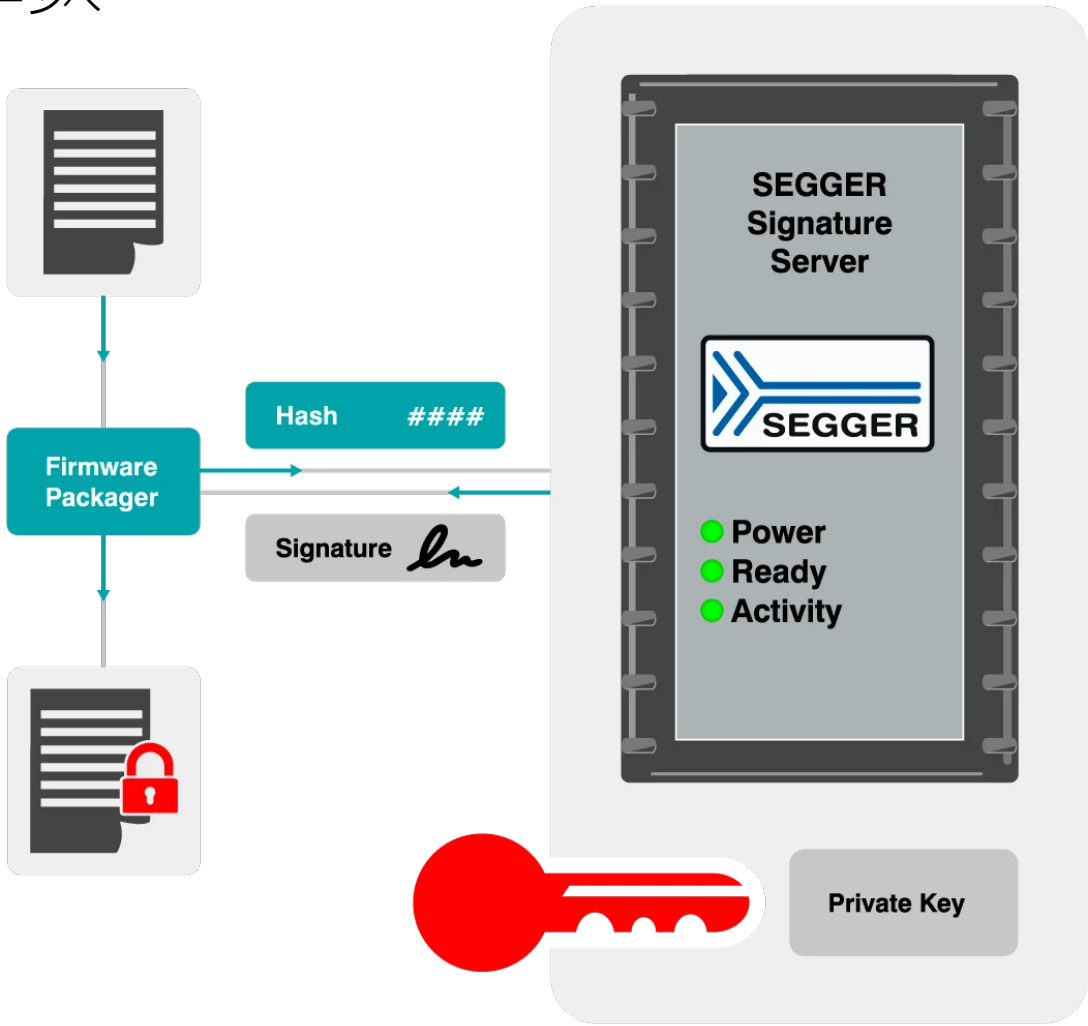
ファームウェアを署名・圧縮・暗号化することで安全なアップデートパッケージへ

Firmware Packagerを利用することで、複雑なアップデートパッケージの作成を簡単なステップで完了できます。

プロセス内では、ファームウェアのハッシュ値のみをSEGGER署名サーバーに送り、サーバー内で安全に保管された秘密鍵によってデジタル署名を発行します。

最終的にデータ圧縮と暗号化が施された、配信に最適なコンパクトかつ認証済みのアップデートファイルが自動生成されます。

このプロセス全体を通じて、最重要資産である秘密鍵がサーバー外に出ることは一切なく、最高水準のセキュリティ体制を維持したまま運用が可能です。



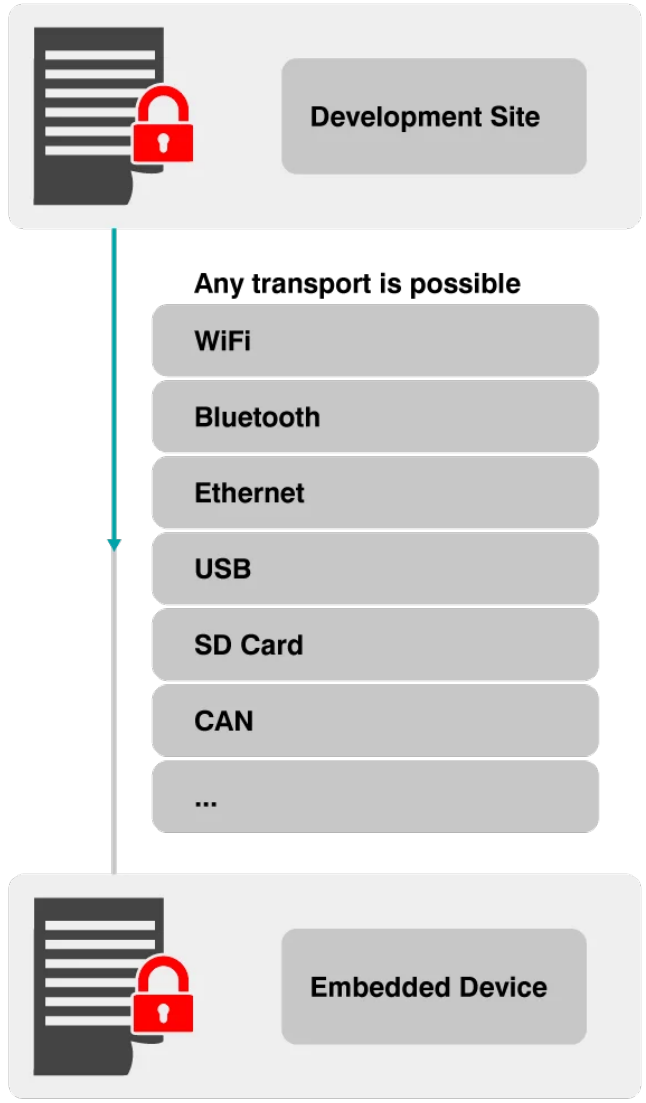
emBoot-Secure アップデートパッケージの転送

様々なインターフェースをサポート

保護されたアップデートパッケージは転送するインターフェースの
セキュリティに依存しません。

アップデートの配信にはWi-FiやBluetoothから産業用のCAN通信、シリアルインターフェース、さらにはUSBやSDカードによる物理的な配布まで、お客様の既存インフラをそのまま活用いただけます。

受信したデータはデバイス内の安全な領域に保存され、再起動時にブートローダーが確実に処理を行うため、通信環境が不安定な状況下でも、
安全かつ確実なアップデート運用が可能です。



emBoot-Secure アップデート処理

正常なアップデート完了をサポート

ファームウェアの正当性、データ欠損の有無を確認し、
最適なファームウェアアップデートを管理・実行します。

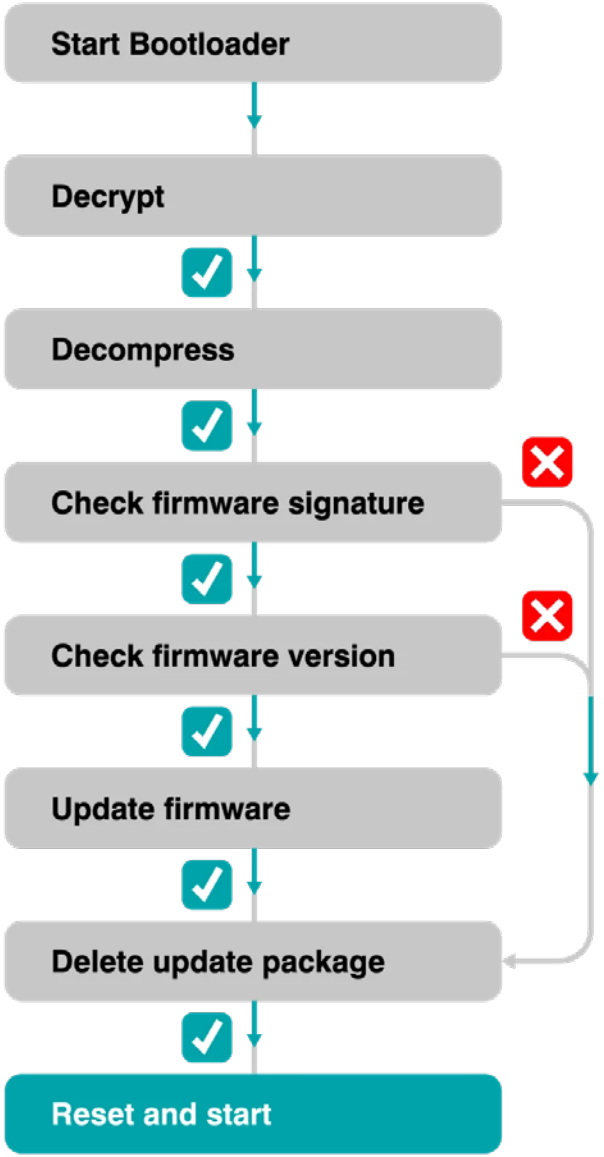
emBoot-Secureブートローダはアップデートが正しく行われるかを常に監視・管理します。

■ 新しいアップデートがある場合：
ブートローダーが自動でデータの正当性を確認し、バージョンチェックを行った上で安全に更新を実行します。万が一のインストール失敗に備えてバックアップを保持する機能や無駄な更新を省く自動判定機能も備わっています。

■ アップデートがない／通常時：
起動のたびに『中身が改ざんされていないか』を瞬時にチェックします。
もし不具合が見つかれば、あらかじめ用意した正常な状態（リカバリイメージ）へ自動的に復旧させることが可能です。
この二段構えの防衛策により、製品は常にメーカー公認の安全な状態で動作し続け、現場での動作不良やサービス停止のリスクを最小限に抑えます。

■ ブートローダそのもののアップデートにも対応
暗号セキュリティの強化に迫られた際など将来的なリスクにも対応可能

アップデートフローはお客様・製品ニーズに合わせて提案します。



emBoot-Secure 暗号・アルゴリズム

標準的で高度な暗号／圧縮アルゴリズム対応

オープンソースコードを含まないSEGGERオリジナルのソースコードで極めて高い安全性を実現

Signature	RSA up to 8192 bits, ECDSA up to 521 bits (secp521r1)
Hash	SHA 1/256/384/512
Encryption	AES-128 .. 256
Compression	SMASH-2, LZMA

サポートするECDSA曲線

- brainpoolP256r1: 256 bits
- brainpoolP320r1: 320 bits
- brainpoolP384r1: 384 bits
- brainpoolP512r1: 512 bits
- NIST P-256 (secp256r1): 256 bits
- NIST P-384 (secp384r1): 384 bits
- NIST P-521 (secp521r1): 521 bits

BSI（ドイツ連邦情報セキュリティ庁）・NIST（米国国立標準技術研究所）推奨事項に完全準拠

提供会社

EmbiTeK | SEGGER

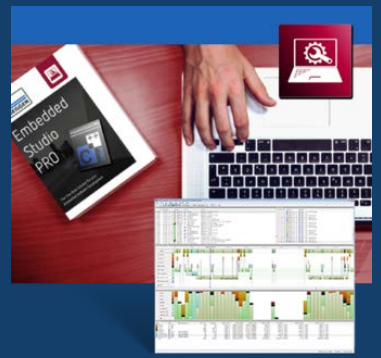
SEGGER Microcontroller GmbH

組込みシステムで30年以上の経験を持ち、最先端のRTOSおよびソフトウェアライブラリを開発
ハードウェアツール(開発 / 生産用)とソフトウェアツールをカバーします。

CEO：Ivo Geilenbruegge,
Hendrik Sawukajtis
設　立：1992年
本　社：モーンハイム・アム・ライン（ドイツ）
拠　点：米国 / 中国

30カ国以上に販売代理店を通して展開


RTOS/ミドルウェア


IDE

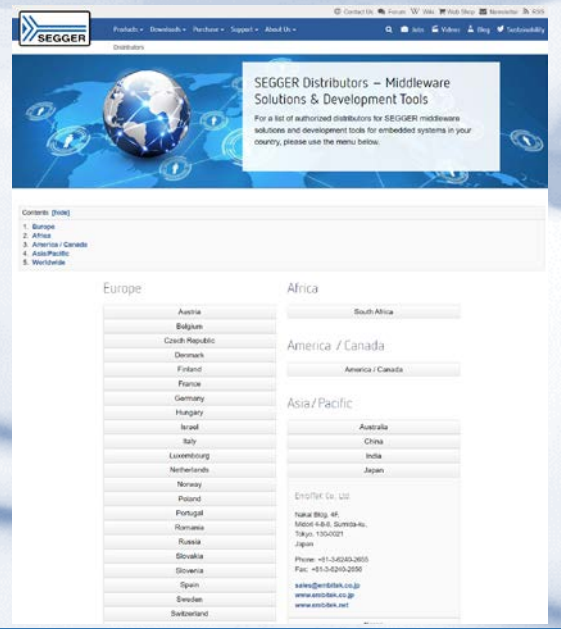

デバッグツール


書込みツール

EmbiTeK

EmbiTeK

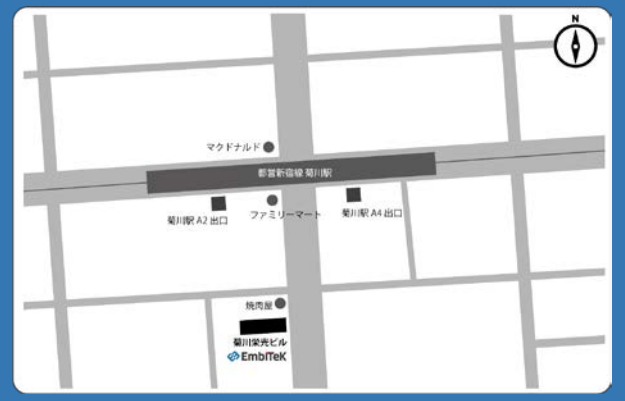
株式会社エンビテック



お客様の要件に合わせ、様々なシナリオで適合できる最適なソフトウェア開発環境
ソフトウェアコンポーネントを提供します。

代表取締役：サントシュ パワル
設　立：2007年
本　社：東京都墨田区菊川2-3-6 菊川栄光ビル 601

日本国内唯一のSEGGER社製品販売オフィシャルパートナー
テクニカルサポート／ポーティング受託開サービスを提供



都営新宿線「菊川駅」徒歩3分

Arm Cortex/RXソフトウェア開発から量産をサポート

製品開発フローの課題に合わせて対応

SEGGER
www.segger.com

EmbiTeK

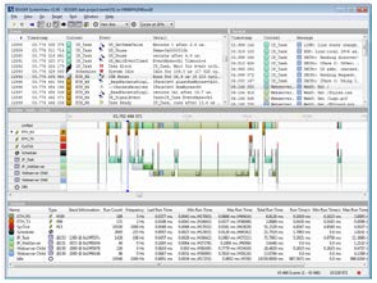
RTOS

embOS

MPU 対応

機能安全認証
IEC61508 SIL3
IEC62304 class C

デバッガ
開発ツール



SSL
暗号ライブラリ
セキュリティ認証
GUI
Modbus
SSH
ブートローダ
圧縮・解凍

IoT Toolkit
- HTTP client
- JSON Parser

MQTT

Dropbox Client

TCP/IP

IPv4 / IPv6	DHCP server	DHCP client
ACP	ARP	AutoIP
DNS client	mDNS server	LLMNR
DNS-SD	Loopback	ICMP
NetBIOS NS	CoAP	RAW sockets
FTP server	FTP client	SMTP client
SNMP Agent	SNTP client	NTP client
PTP OC client	TCP	UDP
Web Socket client	Web server	UPnP
Web Socket server	PPP/PPPoE	Wifi support

USB Host

HID	MTP
MassStorage	CDC
Printer	FTDI
LAN	MIDI
Audio	HUB
CCID	CP21xx UART
Video	

USB Device

HID	MSD (virtualMSD)
MTP	CDC-ACM
CDC-NCM	CDC-ECM
RNDIS	IP-over-USB
Printer	MIDI
Audio	Video
Bulk	DFU

ファイル
システム

- NAND
- SPI/QSPI フラッシュ
- NOR
- SD
- SDHC
- SDXC
- MMC
- eMMC
- CF
- USB メモリ

Arm Cortex / RX CPU

量産書込

EmbiTeK

製品については、お気軽に以下窓口へお問い合わせください。

TEL : 03-6240-2655
FAX : 03-6240-2656
e-mail : sales@embitek.co.jp
website : https://www.embitek.co.jp

EmbiTeK Online Shop
https://www.embitek.shop/

YouTube
http://www.youtube.com/@embitek