様々なリスクからIoT組込製品を守る
セキュリティーソリューション

株式会社エンビテック

EmbiTeK

SEGGER Microcontroller GmbH & Co. KG

SEGGER（セガー）社は組込みシステム向けに高機能な開発ツール、生産ツール、統合開発環境、フットプリントの小さいリアルタイムOS、ミドルウエアなどを提供するメーカです。

SEGGER
www.segger.com

Complete R&D and production chain out of one hand!!

本社：ルッセルドルフ
代表：ロルフ・セガー
設立：1997年
社員数：40人
拠点：マサチューセツ

SEGGERというと日本でもユーザ様が多いデバッガ

J-Link BASE

J-Link PLUS

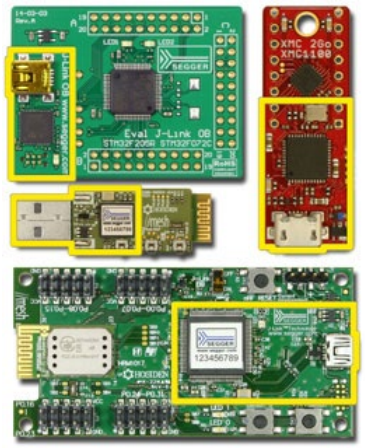
J-Link ULTRA+

J-Link PRO

J-Trace PRO Cortex

J-Link EDU
（学生、大学、NPO向け）

販売実績
50万台以上



J-Link OB / J-Link LITE
評価ボードメーカーパートナー様向けのPR製品
（評価ボード製品とのセット販売）

J-Trace PRO Cortex-M

64 MB トレースバッファ
（トレースクロック300MHzまで）
ストリーミングトレース可能

Cortex-M搭載IoT機器に最適なミドルウェア製品も充実

RTOS
16 – 32bit MCUを幅広くカバー

ファイルシステム
小さなフットプリント、暗号化処理、
RAID1システムサポート

USB Host/Device
USB2.0対応
IP-over-USB / CDC-ECM / RNDIS対応

TCP/IP v4/v6
Non-RTOS環境でも利用可能
※サーバ機能などは除く

Wifiサポート
各種Wifiモジュールサポート対応
※対応については、ご相談ください。

LTE/UMTS/GPRSサポート
PPP/PPPoEにより接続サポート

GUI
ワンチップマイコンに最適
グラフィックライブラリ

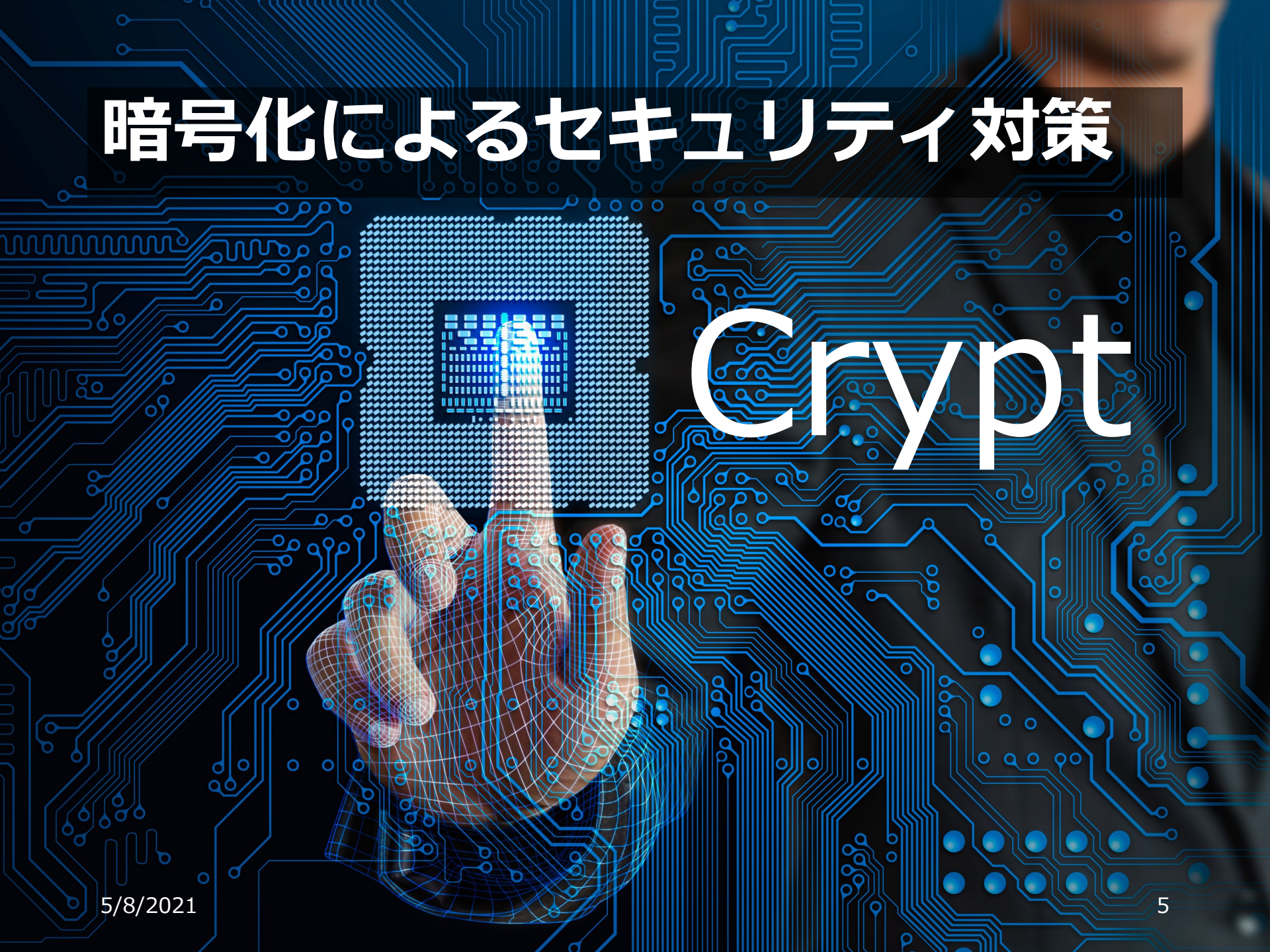
Dropboxクライアント
Dropbox APIを活用した
組込機器のファイル共有

圧縮・解凍
マイコンに搭載可能な解凍システム
様々なCODECに対応

Modbus
産業機器向けプロトコルスタック
※TCP/IPレイヤーの依存性無し

MQTTクライアント
M2M通信用MQTT ver3.1対応
※TCP/IPレイヤーの依存性無し

暗号化によるセキュリティ対策



暗号化を利用して、IoTセキュリティを守る

対象となる脅威

ファームウェア不正改造

ファームウェア・
内部コンテンツ盗難

→ emSecure セキュア認証プロトコル

通信経路における情報漏洩

サーバ不正ログインによる
不正操作・情報漏洩

→ 通信プロトコル上での暗号化
emSSH SSH　emSSL SSL

製品コピー・不正生産

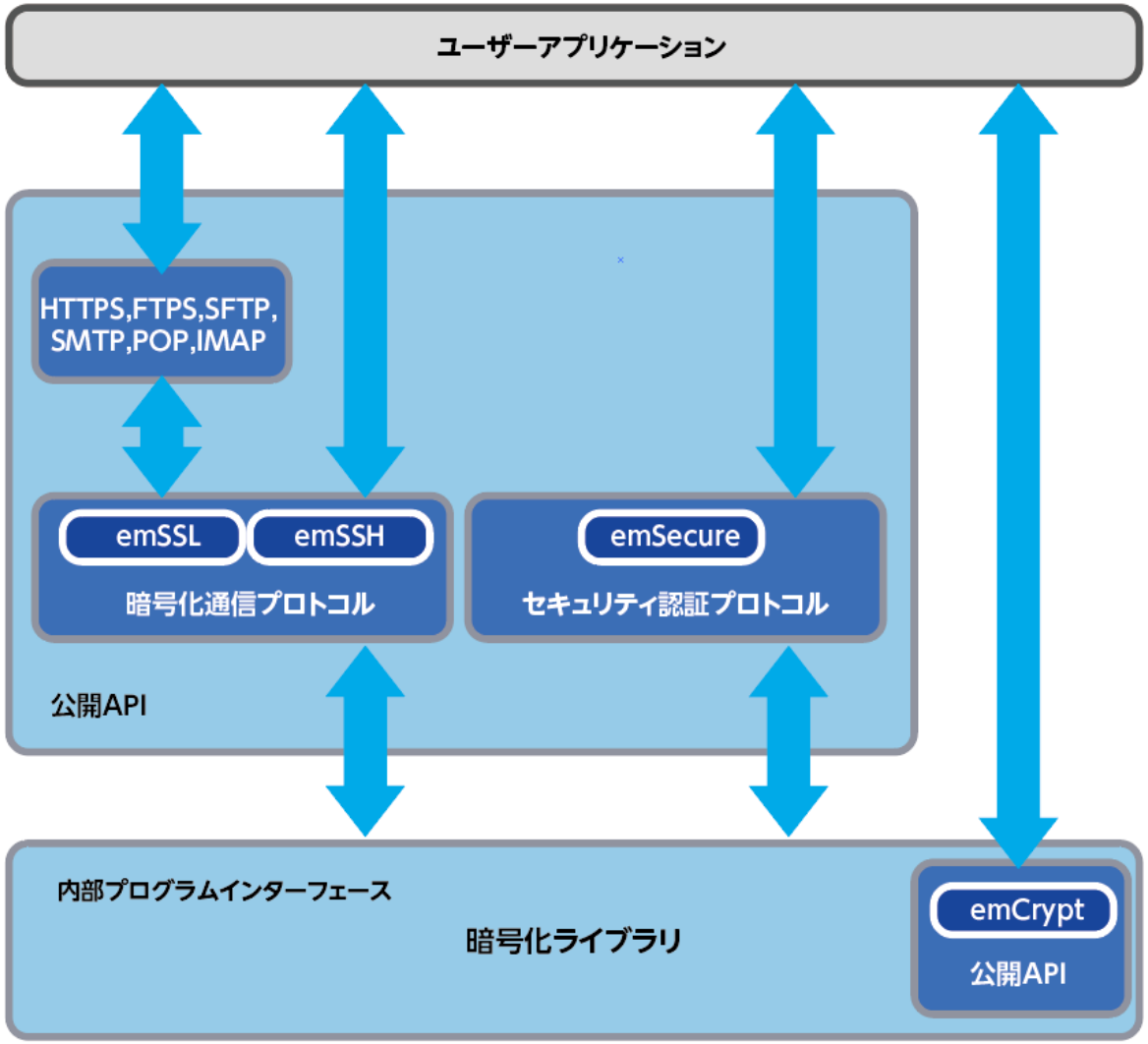
→ 

セキュア書込ツール

暗号化技術を活用して、「守る」

暗号化技術製品の概要

暗号化ライブラリを様々なプロトコルで活用できるように準備



組込機器を守る！

製品（ソフトウェア）を守る。

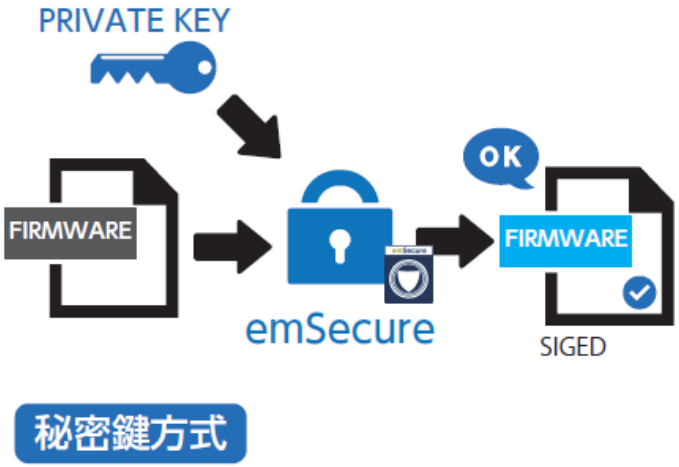
1. 製品のハッキング、クローニングから守る

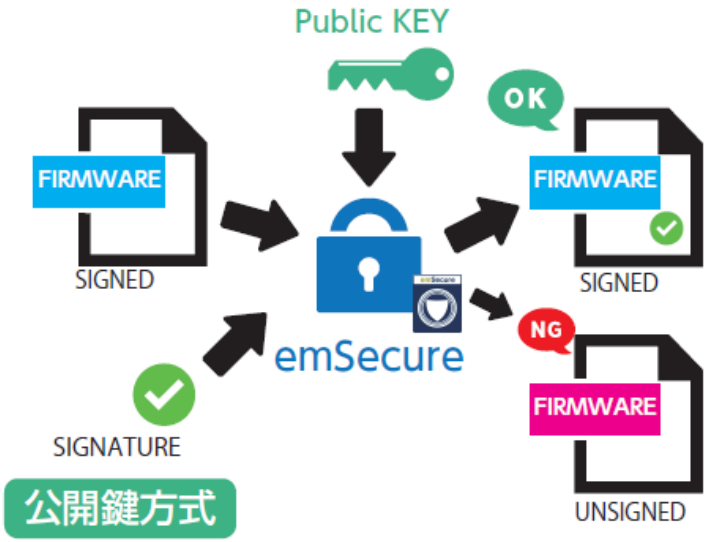
具体的にどのような事を実現するか？

ファームウェア不正改造

製造者（管理者）ではない悪意あるファームウェアの書込を防ぐ。

ファームウェアのセキュリティ認証を導入することにより守る。





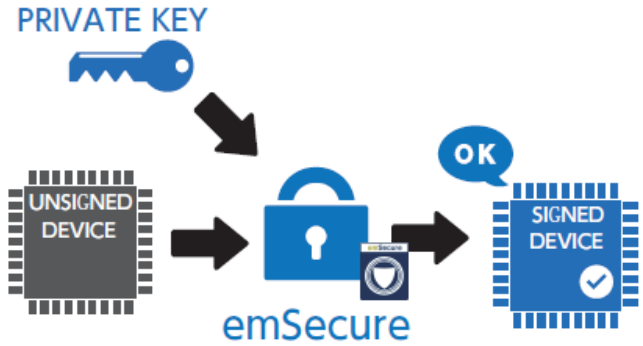
2. 製品のハッキング、クローニングから守る

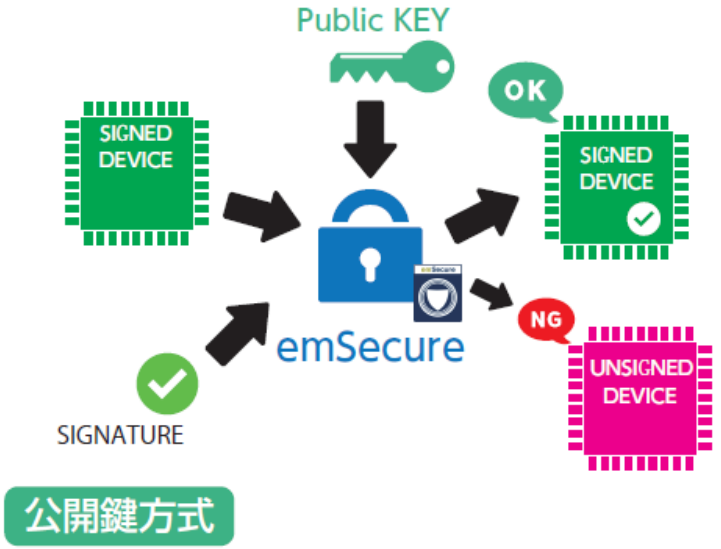
具体的にどのような事を実現するか？

ファームウェア・内部コンテンツ盗難
不正なハードウェアへ移植されることを防ぐ

製造者（管理者）が認証していないハードウェアへ移植

ハードウェアUIDを活用したセキュリティ認証により、不正移植を防ぐ





emSecure の特徴

128～16384bit 暗号セキュリティ認証技術により、組込機器を守る。

emSecure とは、デジタルデータ署名の作成及び検証を行うためのソフトウエアプログラムです。emSecure セキュリティモジュールでお客様の製品をハードウエアコピー（偽物クローン）及びファームウエアコピー・編集（ハッキング）から守ることが出来ます。

選挙機器、ATM マシン、金融アプリケーション、センサー機械等の重要なシステムに必要な機能です。
emSecure は組込みシステム向けのセキュリティシステムとしてスクラッチから開発されたオリジナル製品ですが、組込みシステム以外の環境（パソコン等）でも使用可能です。

- RSA / ECDSA デュアルキー（秘密鍵及び公開鍵）設計で100% セキュア
- ROM/RAM リソース使用量が低い
- ハードウエア、CPUに依存しない設計で移植作業が簡単
- 組込みターゲット向けに設計された高速度パフォーマンス
- 簡単なドラッグ＆ドロップ操作でサインキーの作成及び確認可能なツールが付属
- ソースコード及びキー作成ツールが付属
- ロイヤリティー費用なし

emSecure - RSA
emSecure - ECDSA

emSecure：パフォーマンス・モデル比較

■ **速度パフォーマンス：**

データサイズ	キーサイズ	合計時間（HASH計算を含む）	
		Verifying data	Signing data
1 kByte	512 bit	3.31 ms	41.64 ms
100 kByte	512 bit	14.50 ms	52.83 ms
1 kByte	1024 bit	8.61 ms	192.06 ms
100 kByte	1024 bit	19.80 ms	204.25 ms
1 kByte	2048 bit	24.74 ms	1026.11 ms
100 kByte	2048 bit	35.93 ms	1037.30 ms

■ **メモリフットプリント：**

	ROM	RAM（Stack）	
		1024 bit key	2048 bit key
Verification only:	4.6 KByte	1.9 KByte	2.6 KByte
Verification & Generation:	5.8 KByte	1.6 KByte	2.3 KByte

※Cortex-M4マイコンデバイス（CPUクロック：200 MHz）でのテスト結果

■ **速度パフォーマンス：**

データサイズ	キーカーブ	合計時間（HASH計算を含む）	
		Verifying data	Signing data
1 kByte	P-256	156.38 ms	151.82 ms
100 kByte	P-256	176.34 ms	171.75 ms

■ **メモリフットプリント：**

	ROM	RAM（Stack）
		P-256 key
Verification only:	10.2 KByte	2.4 KByte
Verification & Generation:	12.2 KByte	6.2 KByte

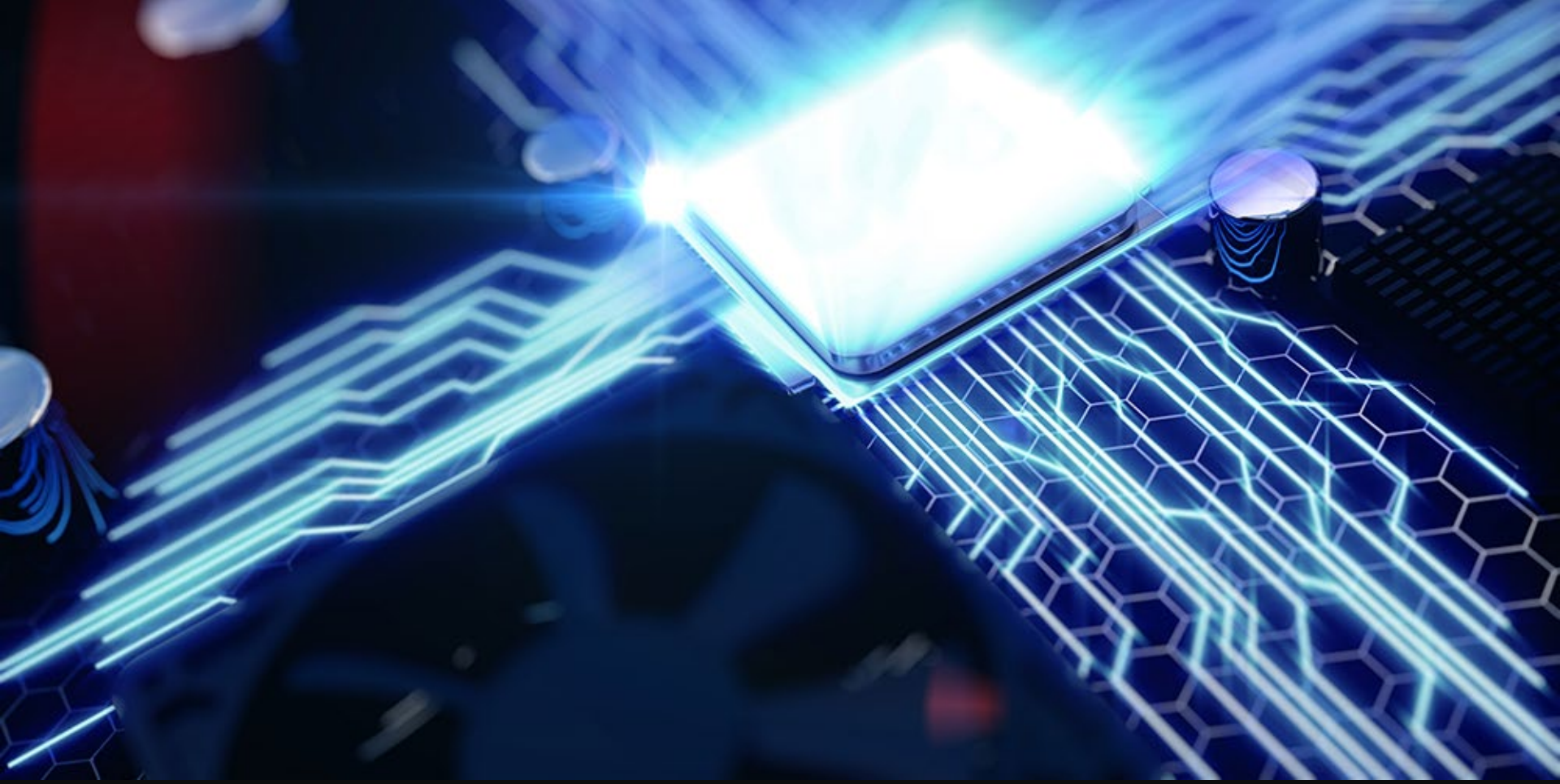
※Cortex-M4マイコンデバイス（CPUクロック：200 MHz）でのテスト結果

RSA版

数十年にわたる実績があるアルゴリズム
低ROM（コードメモリ）要件
迅速な署名検証

ECDSA版

現代の最新式のアルゴリズム
より小さいキーサイズで高レベルのセキュリティ
低RAM要件、高速署名生成



通信経路を守る！

情報通信を守る。

3. 通信経路における情報漏洩、改ざんから守る

具体的にどのような事を実現するか？

情報漏洩・改ざん
通信経路における情報漏洩・改ざん
データの不正利用・情報の流出

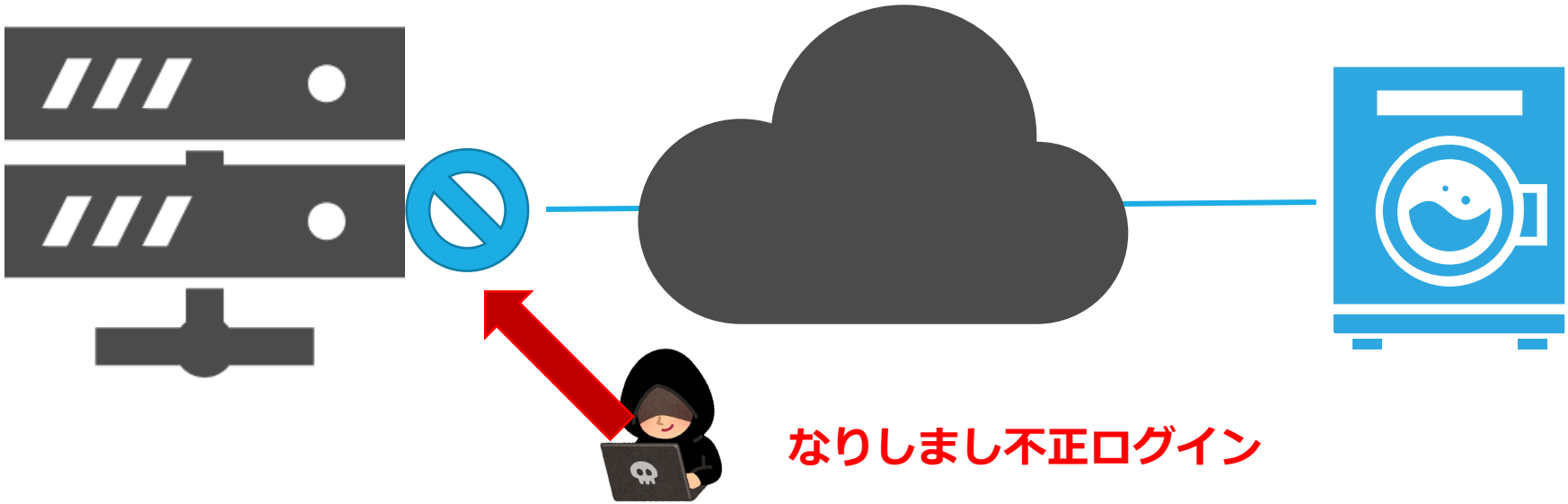
SSL暗号化通信により、守る

4. サーバアプリケーションへの不正ログインから守る

具体的にどのような事を実現するか？

情報漏洩・改ざん
サーバ機能を搭載した機器へなりすまし侵入
データの不正利用・情報の流出

SSH暗号化ログイン通信により、守る



SSL/TLS/SSH （セキュア通信・セキュアログイン）

IoT 機器はもちろん、機器間通信にSSL 通信暗号化を活用することにより、通信の安全性を確保します。
組込機器に最適化されたemSSL は少ないフットプリントでワンチップマイコンにも搭載可能です。

	最小構成	標準構成	最大構成
ROMサイズ	17KB	19KB	43KB

セキュリティモジュールプログラムはSEGGERのオリジナル製品で、Open-SourceコードやGNUライセンスが含まれておりません。

emSSH を活用することで、クライアントとリモートマシン間の通信を暗号化し、セキュアな通信を実現します。
ターゲットや開発環境に依存しない設計ですので、様々な環境で簡単に移植出来ます。

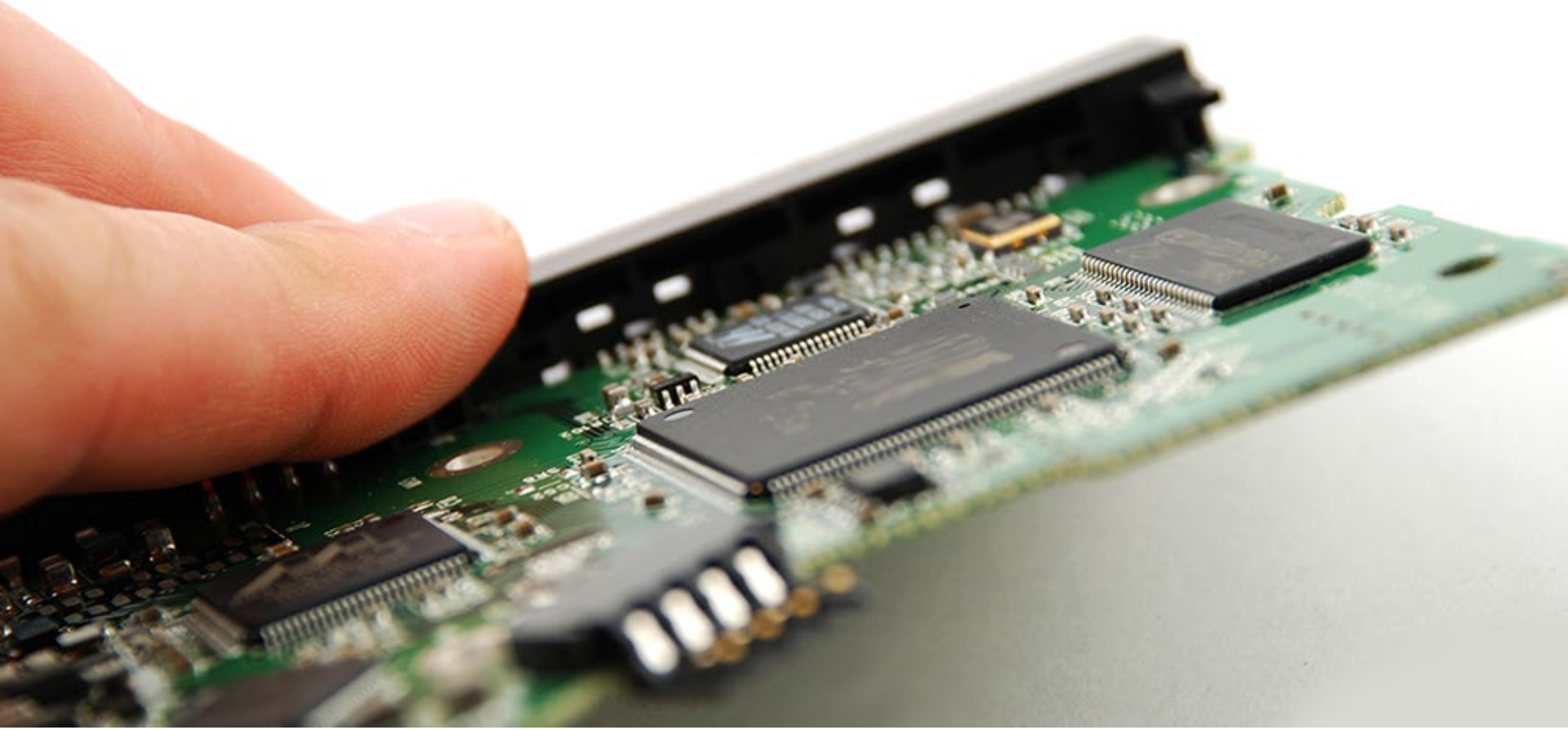
多品種展開には開発ユーザライセンスがおすすめ！

暗号化ソリューションを
御社の開発基盤に！

多品種展開に対応可能なライセンス

柔軟なライセンス体系をニーズに合わせて選択可能

ライセンスモデル	提供コード	対象製品	開発者人数	CPU/ コンパイラ
プロダクト ライセンス	ソースコード	一つの製品	無制限	1CPU型番 1コンパイラ
プロダクト ファミリー ライセンス	ソースコード	製品シリーズ	無制限	1CPU型番 1コンパイラ
ユーザー ライセンス	ソースコード	無制限	1名	1CPUアーキテクチャ 1コンパイラ
CPU ライセンス	ソースコード	無制限	無制限	1CPUアーキテクチャ 1コンパイラ



量産工程を守る！

ソフトウェア資産の流出を防ぐ

5. 不正生産・生産時のソフトウェア資産を守る。

具体的にどのような事を実現するか？

ファームウェア・内部コンテンツ盗難
量産時におけるファームウェアの流出

量産時ソフトウェア資産を不正に利用される事による損害

セキュア書込を実現した書込ツールにより、守る。

セキュア領域にある
ソフトウェアの
不正読み出し不可

書込回数制限により
生産計画外の
数量書込は不可

機器を盗難されても、読み出しは不可

Flasher の特徴

このようなニーズに対応できます。

1. PC環境なしで**スタンドアロンモード**で書込作業を行いたい
2. ソフトウェア**資産を保護**しながら、フィールド展開したい
3. 年間**ライセンス更新費用、ラーニングコスト**を避けたい
4. 量産書込みを海外の第三社に依頼しますので**不正生産を防止**したい
5. 同じハードウエアツールを**開発用途としても利用**したい
6. 一部のプログラムだけ（**パッチ**）を更新したい
7. 現場に簡単に持ち運べる書き込みツール（**サービスツール**）がほしい

Flasherシリーズ製品ラインナップ

モデル	Flasher ARM	Flasher Portable PLUS	Flasher Secure
対象ターゲット	ARM（JTAG/SWD）	ARM（JTAG/SWD/FINE）	ARM（JTAG/SWD）
接続方法	USB/RS232C/LAN	USB	USB/RS232C/LAN
特徴	128MBの内蔵ROMに格納可能な複数イメージを保持することが可能、LAN/RS232経由で遠隔操作可能、外部トリガー信号で書き込み開始可能、Patch及びバッチコマンドをサポート	8個までのイメージを保持して、ボタン選択による書き込みが可能、内蔵リチウムイオン電池で動作可能 対応デバイス：ARM、Cortex、RX、RL78	製品メーカーと第三社に依頼した量産現場を直接つなぐシステム インターネット暗号化通信認証により、不正生産を防止

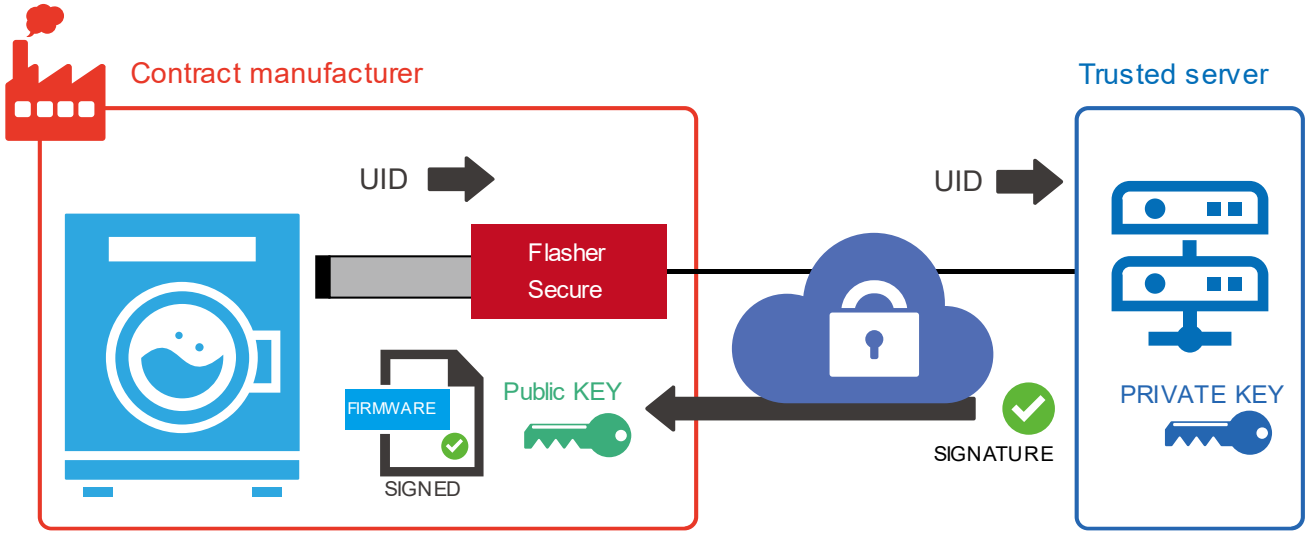
社外の生産ラインにおける不正操作を防止

- セキュアフラッシング機能で大切なイメージデータを保護
- 書き込む回数の制限設定可能

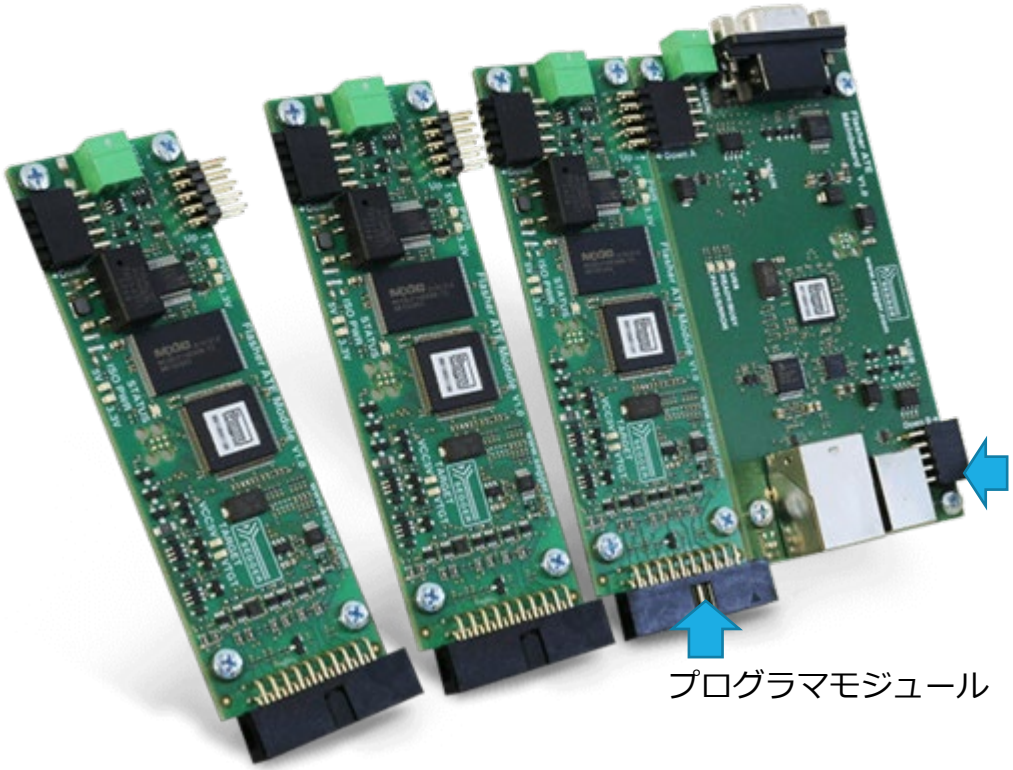
ソフトウェア資産を守る量産体制

Flasher Secure

ファームウェアの書込を制御することにより、不正生産を防止することが可能です。
Flasher Secureから暗号送信されたUIDをインターネット経由で認証を行い、書込キーを発行します。



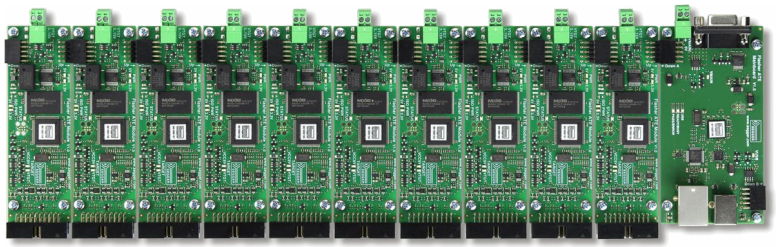
Flasher ATE



対応デバイス
ARMコア（Synergy, R-IN, RZシリーズ）
RXシリーズ
RL78シリーズ

Device Under Test (DUT) 機能サポートで
ターゲットに書き込まれたプログラムが
正常に動作するかを確認することも可能です。

詳細はお問合せください。



プログラマモジュールを最大10ユニットまで
1つのメインモジュールでコントロール可能

IoT組込機器を守るために

どのような脅威から守る必要性があるのかというアセスメントから

機器・ソフトウェア資産を守る**「不正コピー」「不正改ざん」**防止

インターネット上のデータを守る**「盗聴」「改ざん」「不正利用」**防止

サーバ機能を有した機器に対する**「不正ログイン」**防止

量産時における**「ソフトウェア資産の盗難」**防止

このような脅威に対応するために組込機器で動作可能な
暗号化ソリューションをご検討頂ければ幸いです。

課題となるのは？

コスト！多彩な製品ラインを用意したい！

担当窓口

株式会社エンビテック
営業担当 :村井一仁
E-mail: sales@embitek.co.jp
TEL: 03-6240-2655
FAX : 03-6240-2656
https://www.embitek.co.jp