組込システム用SSHセキュアログイン emSSH

Non-RTOS/RTOS・ハードウェア・開発環境の依存性なく利用可能なSSHサーバ

クライアント機能は未提供

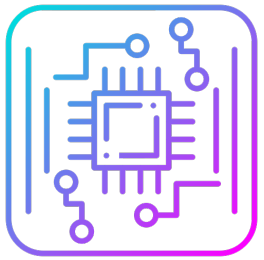
EmbiTeK

組込機器内のサーバ機能へセキュアなアクセスを実現

一般的なSSHv2 クライアントと接続可能なSSHログイン サーバ機能を提供

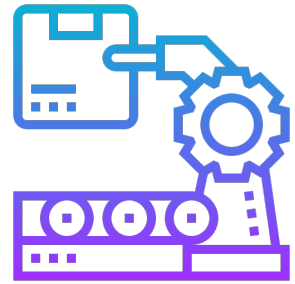
emSSH を活用することでクライアントとリモートマシン間の通信を暗号化し、セキュアなユーザ管理を実現
製品パッケージにはSSH を使用する単純なコマンドシェルと、emSSH を統合する方法を示すサンプルプロジェクトが含まれています。

コンパクト実装
小さなフットプリントで実装



幅広いCPU対応
Arm Cortex / RISC-V / RX
RH850 / RL78 / SH2A / AVR
PICxx / STM8 / MSP430他

ANSI-Cソースコード
MISRA-C2012コーディングルール
開発環境・コンパイラ依存なし



量産ロイヤリティなし
開発ライセンス
量産に対しての継続コストなし

洗練されたソースコード

信頼性・安定性の高いソースコード
emSSHはSSHv2に準拠、すべてのSSHのRFC仕様に対応したSEGGER独自開発のソフトウェアモジュール

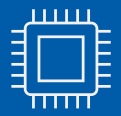
整理されたファイル構造とAPI構造
・利用するマイコンに合わせた最適化を柔軟に設定可能

導入容易性 開発しやすさ

習得しやすいサンプルソースコード
豊富な標準サンプルソースコードで利用方法の習得がしやすくなっています。

BSDソケットインターフェース
標準的なBSDソケットインターフェースで利用するTCP/IPスタックを自由に選択可能

ウェブマニュアル提供で製品導入前に導入技術検証が可能
・導入前にすべての機能のAPI利用方法、設定などをウェブマニュアルで確認できます。



ソフトウェア継続性を強化

突然のマイコン変更や製品横展開を容易に実現
・ハードウェア依存性のないソースコードでハードウェア変更を容易に実現
・コア制限のユーザライセンスで、追加コストなしにマイコン変更も容易に可能

SSHコマンドを利用したセキュアファイル転送について

SSH-SCP add-on

SCPはSSHプロトコルを利用したファイル転送を実現します。ファイルはもちろん、ログイン時のアカウント情報を平文でなくSSHによって暗号化された情報としてネットワークに流すことができ、セキュアなファイル転送を実現します。

ファイル単位でアクセスする場合は別途ファイルシステム(emFile）が必要
セクター単位でのアクセスであれば、ファイルシステム不要

SFTP

emSSH 未対応

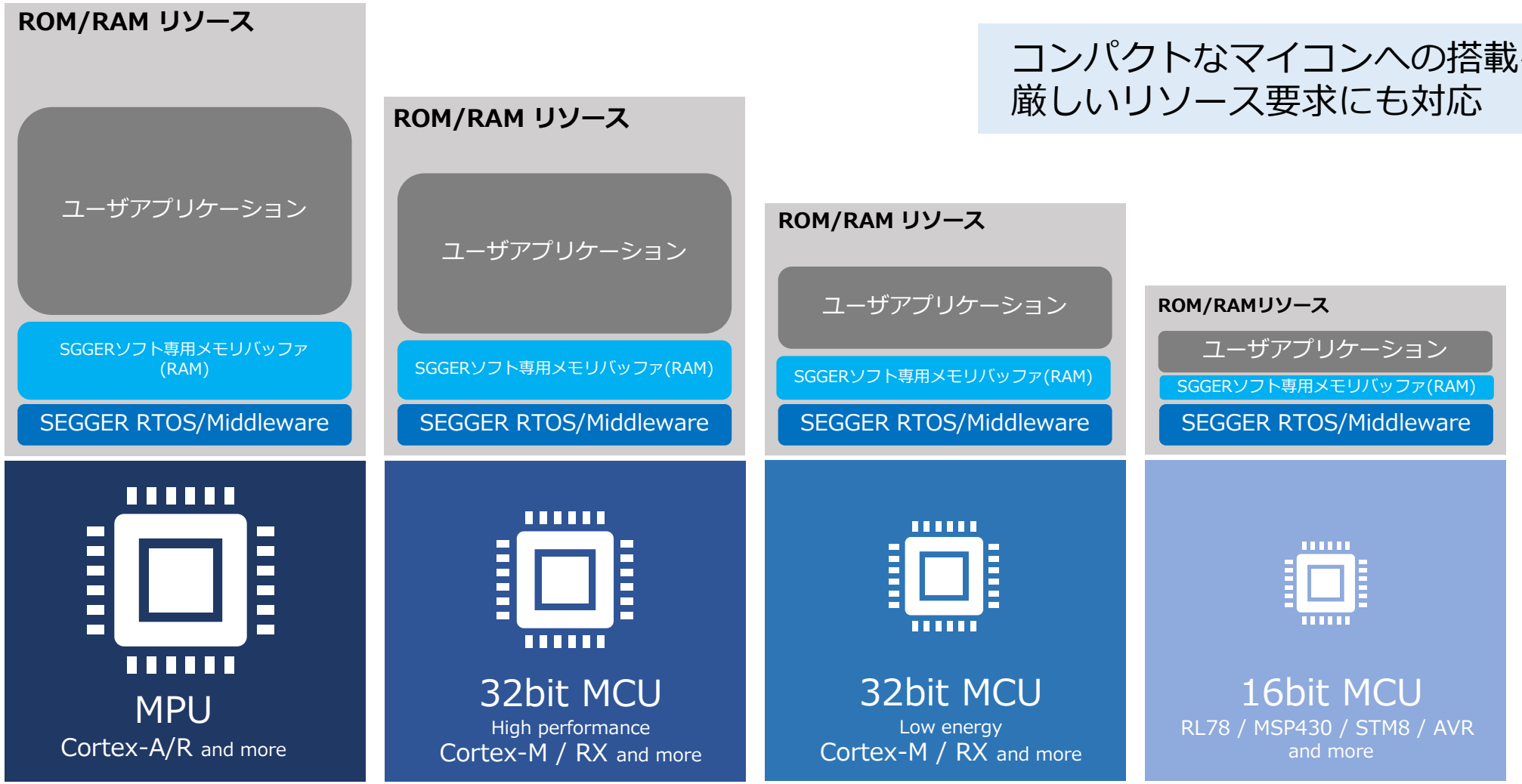
セキュアファイル転送で検討の場合は、SCP, FTPS
セキュアファームウェアアップデートで検討の場合は、emSecure、emLoad + encryption / signature add-onで代替提案いたします。

FTPS

TCP/IPスタック＋emSSL TLSサービス

TLSとFTPを利用し安全性の高いファイル転送を実現
FTPS / FTPESをサポートします。

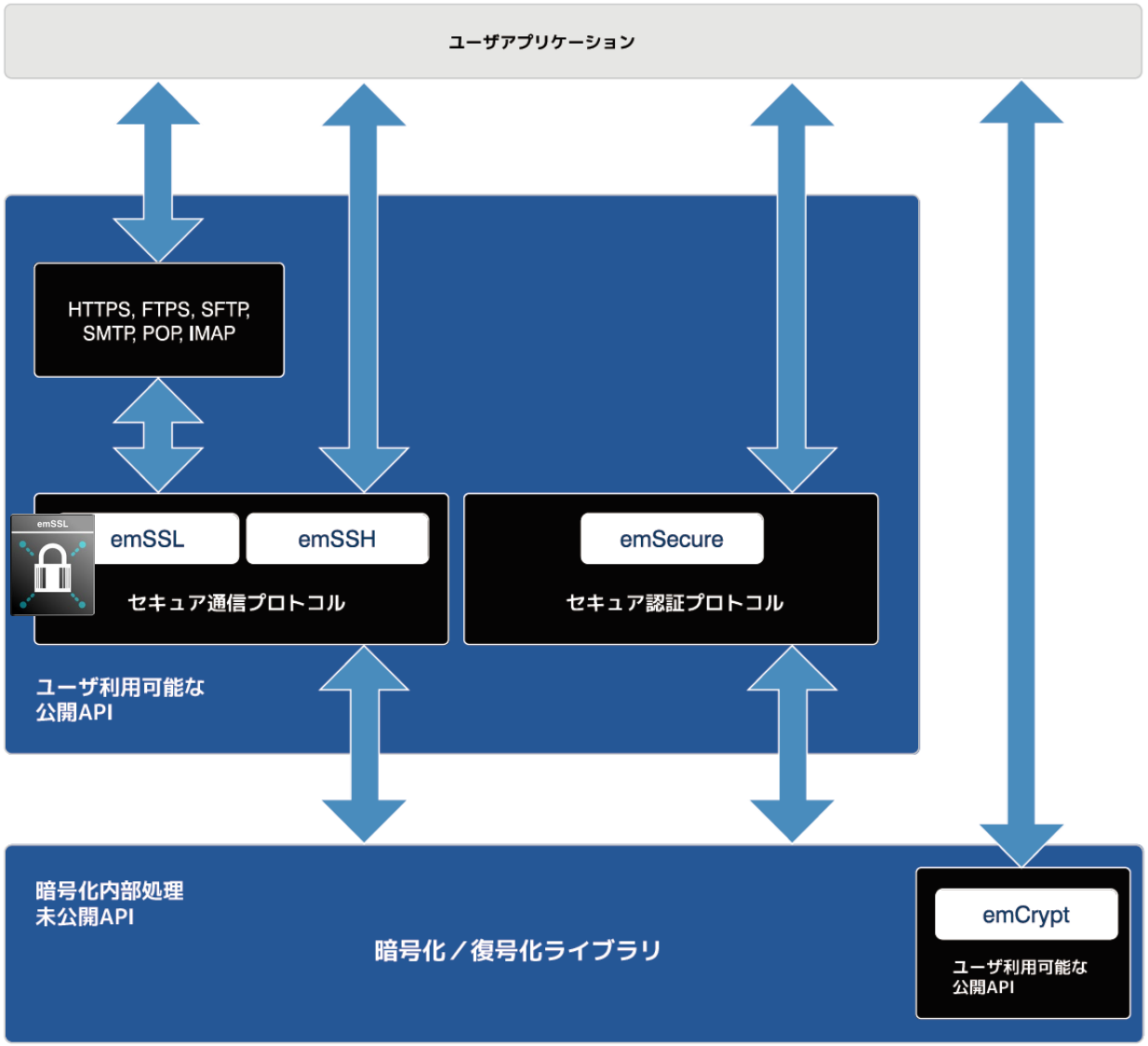
リソースの限られたマイコンでもハードウェアの性能を活かし、機能制限なく利用できるよう設計



コンパクトなマイコンへの搭載を前提に開発
厳しいリソース要求にも対応

SEGGERソフト専用メモリバッファ:
SEGGERソフトウェアが処理速度を向上させるために使用する一時的なメモリプール。ユーザアプリケーション、ハードウェアリソースに合わせて、領域サイズを変更可能です。

SSL/TLS暗号通信に必要なライブラリだけをSSL通信向けのAPIで提供



- サーバ認証・クライアント認証対応可能
- すべてオリジナルソースコード提供
- ハードウェア・コンパイラ依存性なし
- RTOS の有無にかかわらず利用可能
- ヒープメモリ管理
  長時間稼働でもメモリフラグメントなし
- FTPを利用したセキュアファイル転送サポート
- ハードウェアアクセラレータ対応（オプション）

すべてソースコードで提供されるため、コードの脆弱性やオブジェクト提供ではチェックできないバックドアの懸念を回避することができます。

動的暗号モジュールスイート

emSSH では、SEGGER emCrypt / emSSL / emSecureと共通の独自開発のコンパクトな暗号ライブラリを提供しています。
接続対象のクライアントに合わせた鍵交換 / 暗号 / MACアルゴリズムを実装可能

鍵交換アルゴリズム毎の暗号モジュールスイート（一部抜粋）

ECDHE-ECDSA	ECDH-ECDSA	ECDHE-RSA
ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256	ECDH-ECDSA-WITH-RC4-128-SHA	ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256
ECDHE-ECDSA-WITH-3DES-EDE-CBC-SHA	ECDH-ECDSA-WITH-3DES-EDE-CBC-SHA	ECDHE-RSA-WITH-3DES-EDE-CBC-SHA
ECDHE-ECDSA-WITH-AES-128-CBC-SHA	ECDH-ECDSA-WITH-AES-128-CBC-SHA	ECDHE-RSA-WITH-AES-128-CBC-SHA
ECDHE-ECDSA-WITH-AES-128-CBCSHA256	ECDH-ECDSA-WITH-AES-128-CBC-SHA256	ECDHE-RSA-WITH-AES-128-CBC-SHA256
ECDHE-ECDSA-WITH-AES-128-CCM	ECDH-ECDSA-WITH-AES-128-GCM-SHA256	ECDHE-RSA-WITH-AES-128-GCM-SHA256
ECDHE-ECDSA-WITH-AES-128-CCM-8	ECDH-ECDSA-WITH-AES-256-CBC-SHA	ECDHE-RSA-WITH-AES-256-CBC-SHA
ECDHE-ECDSA-WITH-AES-128-GCMSHA256	ECDH-ECDSA-WITH-AES-256-CBC-SHA384	ECDHE-RSA-WITH-AES-256-CBC-SHA384
ECDHE-ECDSA-WITH-AES-256-CBC-SHA	ECDH-ECDSA-WITH-AES-256-GCM-SHA384	ECDHE-RSA-WITH-AES-256-GCM-SHA384
ECDHE-ECDSA-WITH-AES-256-CBCSHA384	ECDH-ECDSA-WITH-ARIA-128-CBCSHA256	ECDHE-RSA-WITH-ARIA-128-CBC-SHA256
ECDHE-ECDSA-WITH-AES-256-CCM	ECDH-ECDSA-WITH-ARIA-128-GCMSHA256	ECDHE-RSA-WITH-ARIA-128-GCM-SHA256
ECDHE-ECDSA-WITH-AES-256-CCM-8 他	ECDH-ECDSA-WITH-ARIA-256-CBCSHA384 他	ECDHE-RSA-WITH-ARIA-256-CBC-SHA384 他

ECDH-RSA	DHE-RSA	RSA
ECDH-RSA-WITH-3DES-EDE-CBC-SHA	DHE-RSA-WITH-CHACHA20-POLY1305-SHA256	RSA-WITH-3DES-EDE-CBC-SHA
ECDH-RSA-WITH-AES-128-CBC-SHA	DHE-RSA-WITH-3DES-EDE-CBC-SHA	RSA-WITH-SEED-CBC-SHA
ECDH-RSA-WITH-AES-128-CBC-SHA256	DHE-RSA-WITH-SEED-CBC-SHA	RSA-WITH-AES-128-CBC-SHA
ECDH-RSA-WITH-AES-128-GCM-SHA256	DHE-RSA-WITH-AES-128-CBC-SHA	RSA-WITH-AES-128-CBC-SHA256
ECDH-RSA-WITH-AES-256-CBC-SHA	DHE-RSA-WITH-AES-128-CBC-SHA256	RSA-WITH-AES-128-CCM
ECDH-RSA-WITH-AES-256-CBC-SHA384	DHE-RSA-WITH-AES-128-CCM	RSA-WITH-AES-128-GCM-SHA256
ECDH-RSA-WITH-AES-256-GCM-SHA384	DHE-RSA-WITH-AES-128-CCM-8	RSA-WITH-AES-256-CBC-SHA
ECDH-RSA-WITH-ARIA-128-CBC-SHA256	DHE-RSA-WITH-AES-128-GCM-SHA256	RSA-WITH-AES-256-CBC-SHA256
ECDH-RSA-WITH-ARIA-128-GCM-SHA256	DHE-RSA-WITH-AES-256-CBC-SHA	RSA-WITH-AES-256-CCM
ECDH-RSA-WITH-ARIA-256-CBC-SHA384 他	DHE-RSA-WITH-AES-256-CBC-SHA256 他	RSA-WITH-AES-256-GCM-SHA384 他

emSSHログインサーバと接続確認済みのSSHクライアント

emSSH では汎用的なクライアントソフトウェアと接続を確認しています。

対応確認済みクライアントソフトウェア

- TeraTerm 4.84
- Putty 0.68
- OpenSSH 6.6.1p1
- Tectia Client 6.4.12.353
- libssh 0.7.0
- libssh 2 1.7.0

デフォルト設定で対応できるもの、
設定変更で対応できるものがあります。
詳細はemSSHマニュアルを参照ください。

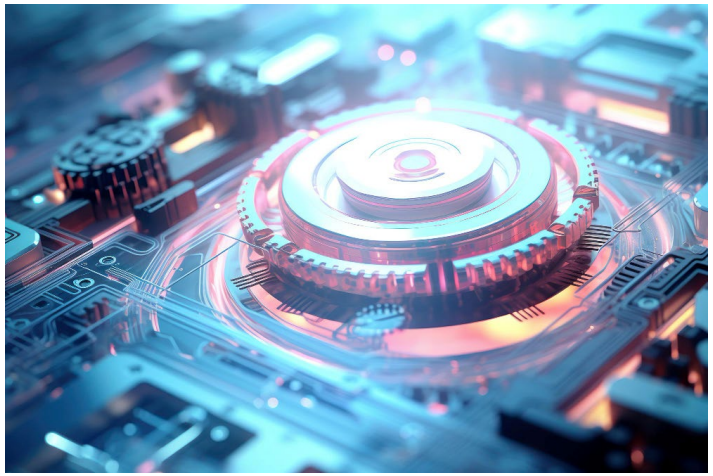
emSSH製品マニュアル「Compatibility」
https://www.segger.com/doc/UM20001_emSSH.html#Compatibility

Key exchange algorithms

Method	TeraTerm	PuTTY	Dropbear	Tectia	OpenSSH	libssh	libssh2	emSSH
rsa1024-sha1		•						•
rsa2048-sha256		•						•
diffie-hellman-group1-sha1	•	•	•	•	•	•	•	•
diffie-hellman-group14-sha1	•	•	•	•	•	•	•	•
diffie-hellman-group14-sha256	•				•			•
diffie-hellman-group15-sha512	•				•			•
diffie-hellman-group16-sha512	•				•			•
diffie-hellman-group17-sha512	•				•			•
diffie-hellman-group18-sha512	•				•			•
diffie-hellman-group-exchange-sha1	•	•		•	•		•	•
diffie-hellman-group-exchange-sha256	•	•		•	•		•	•
ecdh-sha2-nistp256	•	•	•		•	•		•
ecdh-sha2-nistp384	•	•	•		•			•
ecdh-sha2-nistp521	•	•	•		•			•
curve25519-sha256		•	•					•
curve448-sha512								•
SSH Communications Security Extensions								
diffie-hellman-group14-sha224@ssh.com				•				•
diffie-hellman-group14-sha256@ssh.com				•				•
diffie-hellman-group15-sha256@ssh.com				•				•
diffie-hellman-group15-sha384@ssh.com				•				•
diffie-hellman-group16-sha384@ssh.com				•				•
diffie-hellman-group16-sha512@ssh.com				•				•
diffie-hellman-group18-sha512@ssh.com				•				•
diffie-hellman-group-exchange-sha224@ssh.com				•				•
diffie-hellman-group-exchange-sha384@ssh.com				•				•
diffie-hellman-group-exchange-sha512@ssh.com				•				•
libssh Extensions								
curve25519-sha256@libssh.org			•		•	•		•

各クライアントソフトウェア毎の対応鍵交換/暗号/MACアルゴリズムを掲載しています。

HALオプション



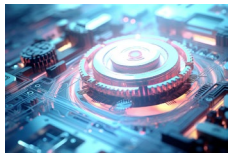
emSSH ハードウェアアクセラレータ

暗号化・復号化をハードウェアアクセラレータ利用で高速処理

暗号・復号製品はCPUメーカ各社の暗号ハードウェアアクセラレータに対応したドライバモジュールをオプション提供しています。ソフトウェア処理に変えてハードウェア処理する事により高速な演算が可能になります。emCrypt, emSSL, emSSH, emSecureで利用可能です。
（ハードウェアアクセラレータはそれぞれの製品毎に設定されています）

CPUメーカ	HAL	対応暗号・アルゴリズム
NXP	Kinetis-CAU	DES in ECB and CBC modes. TDES in ECB and CBC modes with keying options 1, 2, and 3. AES-128, AES-192, and AES-256 in ECB and CBC modes. MD5, SHA-1, SHA-256, RNG
	LPC18S / LPC43S HAL	AES-128 in ECB and CBC modes.
Silicon Labs	EFM32 CRYPTO	SHA-1, RSA, DSA
ST	STM32 CRYP	DES in ECB and CBC modes. TDES in ECB and CBC modes with keying options 1, 2, and 3. AES-128, AES-192, and AES-256 in ECB and CBC modes.

HALオプションの適用で暗号化・復号化処理を高速化



emSSH ハードウェアアクセラレータ ベンチマーク

NXP Kinetis-CAUでの測定

Cipher	Mode	Software Performance	Hardware Performance	Speedup
AES-128-ECB	Encrypt	2.17 MB/s	8.20 MB/s	x3.8
AES-192-ECB	Encrypt	1.86 MB/s	6.87 MB/s	x3.7
AES-256-ECB	Encrypt	1.62 MB/s	6.09 MB/s	x3.8
AES-128-CBC	Encrypt	1.72 MB/s	7.91 MB/s	x4.6
AES-192-CBC	Encrypt	1.52 MB/s	6.56 MB/s	x4.3
AES-256-CBC	Encrypt	1.36 MB/s	5.85 MB/s	x4.3
AES-128-CBC	Decrypt	1.61 MB/s	6.67 MB/s	x4.2
AES-192-CBC	Decrypt	1.43 MB/s	5.77 MB/s	x4.0
AES-256-CBC	Decrypt	1.29 MB/s	5.08 MB/s	x3.9

Mode	Software Performance	Hardware Performance	Speedup	
DES-ECB	Encrypt	1.05 MB/s	11.74 MB/s	x11.2
DES-EDE2-ECB	Encrypt	0.36 MB/s	11.74 MB/s	x32.6
DES-EDE3-ECB	Encrypt	0.36 MB/s	11.74 MB/s	x32.6
DES-CBC	Encrypt	0.90 MB/s	11.84 MB/s	x13.1
DES-EDE2-CBC	Encrypt	0.34 MB/s	11.85 MB/s	x34.7
DES-EDE3-CBC	Encrypt	0.34 MB/s	11.85 MB/s	x34.7
DES-CBC	Decrypt	0.84 MB/s	9.48 MB/s	x11.3
DES-EDE2-CBC	Decrypt	0.33 MB/s	9.48 MB/s	x28.7
DES-EDE3-CBC	Decrypt	0.33 MB/s	9.48 MB/s	x28.7

ハードウェアアクセラレータを利用することで処理速度を大幅に向上させることができます。

搭載必要リソース (Cortex-M4マイコン実装時)

Flash リソース要件

	Component	Size
公開鍵交換アルゴリズム Public key algorithms	DSA	0.5 KB
	ECDSA	0.4 KB
	RSA-PKCS1	0.5 KB
Hash / MAC	SHA-1	0.5 KB
	SHA-256 (including SHA-224)	0.9 KB
	SHA-512 (including SHA-384)	2.3 KB
	MD5	0.8 KB
	HMAC-SHA1	0.2 KB
	HMAC-SHA256	0.2 KB
	HMAC-SHA384	0.2 KB

	Component	Size
暗号 Cipher	DES and 3DES	3.1 KB
	AES	3.4 KB
	AES-GCM (requires AES)	0.5 KB
プロトコルサポート	SSH core	10.5 KB
共有サポートコード	MPI for RSA and ECC support	4.5 KB
	Curve storage (for all curves)	4.4 KB
	Curve arithmetic (requires MPI)	2.3 KB
	Memory management	0.3 KB

RAMリソース

emSSHの静的管理用リソースとしては、0.5KB

その他必要なRAMリソースは以下の様な要件があります。

- 状態とキーマテリアル　：接続状態と接続に必要なキーマテリアルを保存する、接続ごとの変動リソース
- 公開鍵メモリー　：接続時に公開鍵アルゴリズムを実行するための変動リソース
- プロトコルメモリー　：暗号化または復号化の前にプロトコルパケットを保存するために必要なリソース

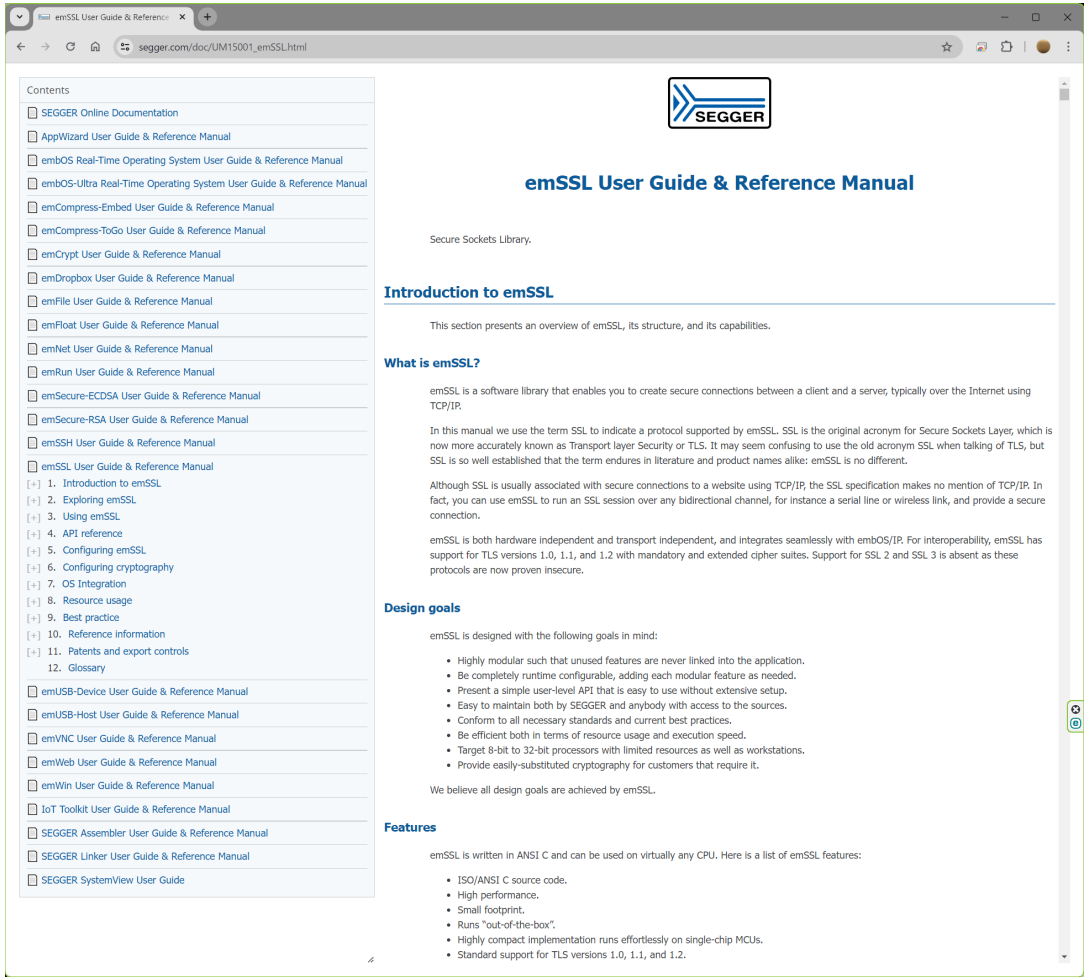
emSSH 開発・導入支援

- ウェブ公開の製品マニュアル
- サンプルアプリケーション
- 評価ボード無償評価版

使いやすいAPIでアプリケーション開発

emSSH – HTMLマニュアルで日本語表示対応

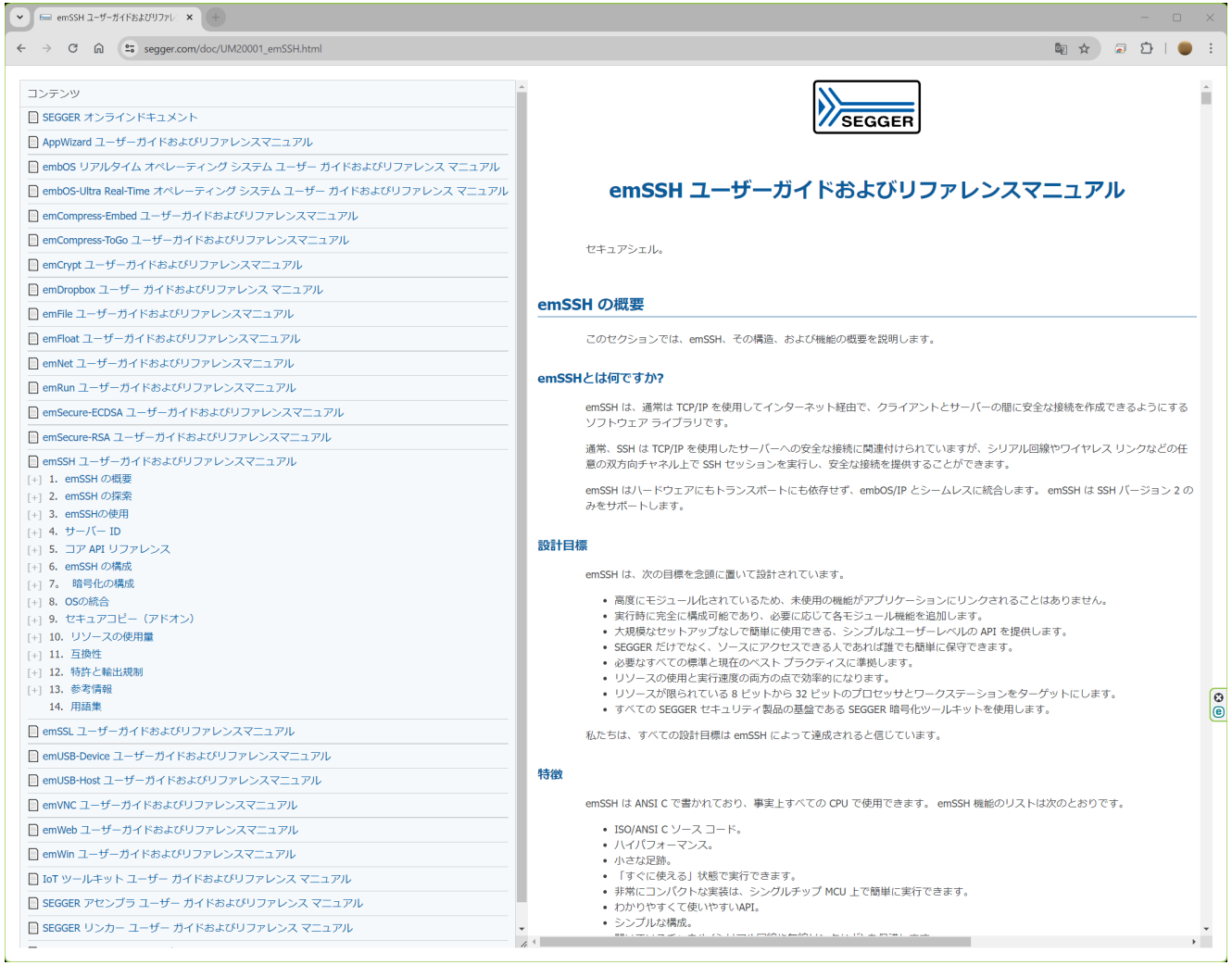
製品マニュアルをライセンス導入前から閲覧可能



ブラウザの翻訳機能で日本語表示可能

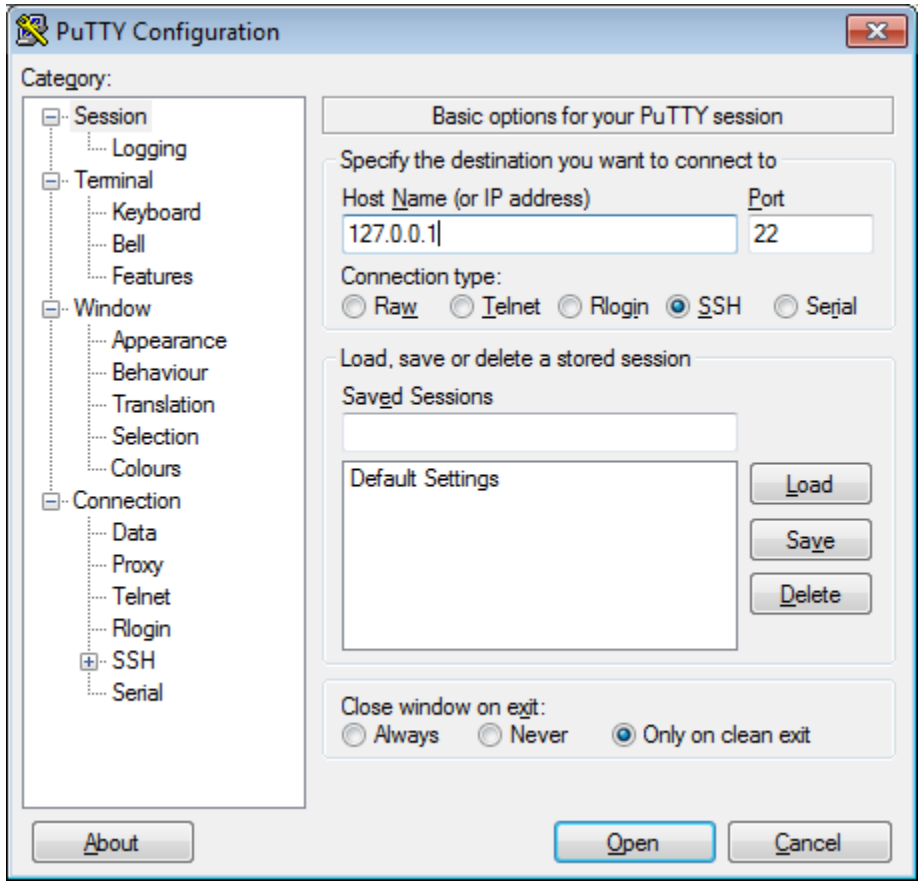
Google Chrome推奨

https://www.segger.com/doc/UM20001_emSSH.html



デモサンプルアプリケーション

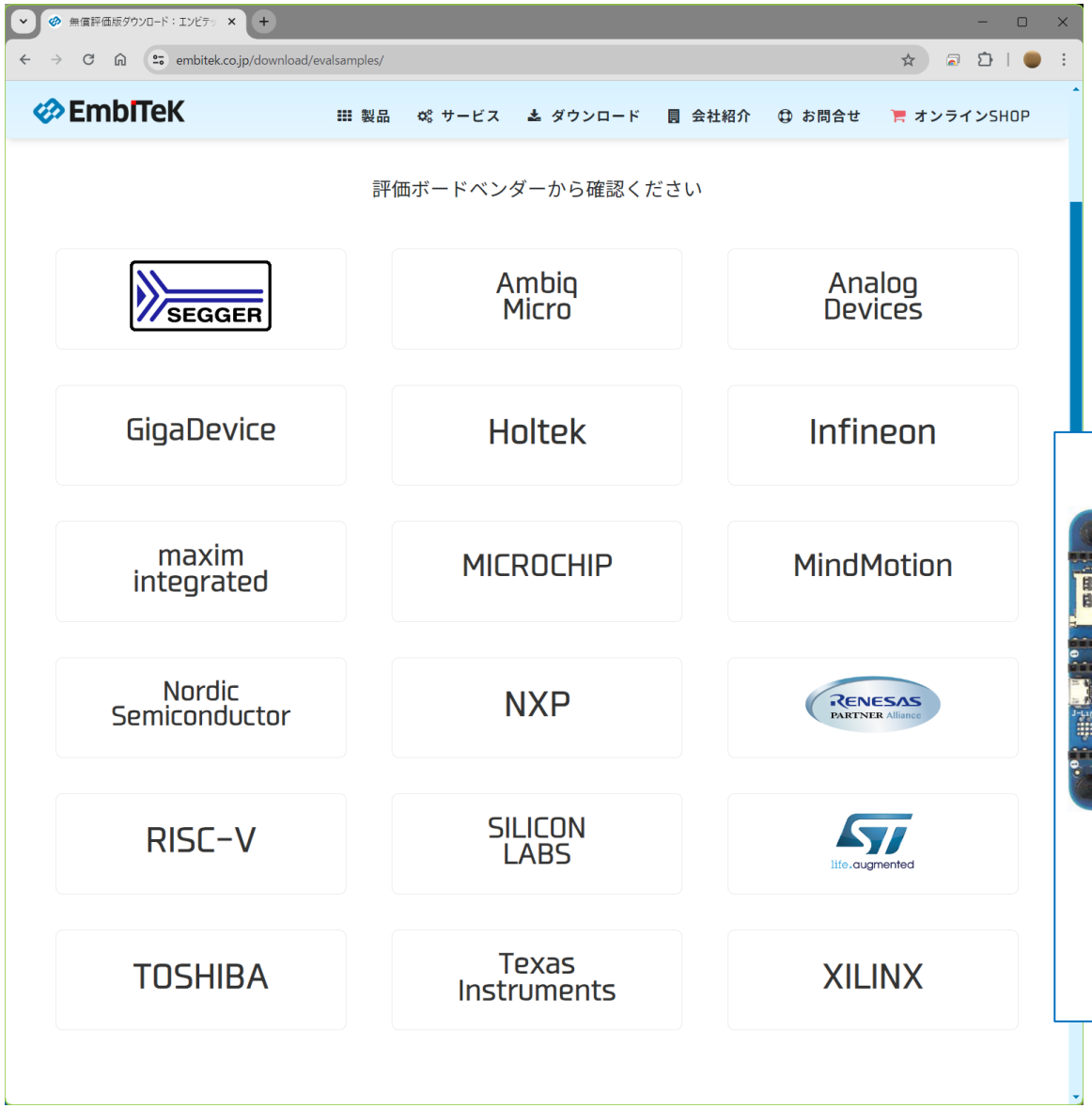
SSH を使用したコマンドシェルと、セキュアシェル ログインライブラリをアプリケーションに統合する方法を示すサンプルが付属しています。評価用にemSSH に基づいた単純なシェルを実装するデモがプリコンパイルされた実行可能ファイルとして利用可能です。




```
C:> SSH_Shell5.exe

(c) 2015-2017 SEGGER Microcontroller GmbH & Co. KG    www.segger.com
emSSH V2.40 - Shell5 compiled Jun  5 2017 11:52:46
```

```
login as: admin

************************************************************
* This server is powered by SEGGER emSSH.  It simply works! *
************************************************************

admin@127.0.0.1's password:

Welcome to the emSSH command line!  Type Ctrl+D to exit.

emSSH> Hello
...Hello
emSSH>
```

各種評価ボードで評価サンプルを利用できます。



ウェブからダウンロード可能

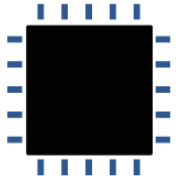
https://www.embitek.co.jp/download/evalsamples/

emSSHライセンスモデル

ニーズに合わせて選択可能なライセンスモデル

SEGGER社ソフトウェアライセンスモデル

永久ライセンス・量産ロイヤリティなしで継続的な費用は必須ではありません。

	シングルプロダクト	プロダクトファミリ （個別提案）	シングルデベロッパ （ユーザ）	CPU （個別提案）
				
開発可能製品数	1製品型番	1製品ファミリ	無制限	無制限
利用可能開発者数	無制限	無制限	1名	無制限
CPU	1CPU型番	1CPU型番	1CPUアーキテクチャ	1CPUアーキテクチャ
コンパイラ	1種類	1種類	1種類	1種類

多数の開発者で1つの製品を開発する。
プロジェクト単位で予算計上

複数の開発プロジェクトで共通利用
開発プラットフォーム化に最適

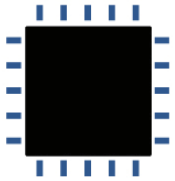
開発プロジェクトは無制限／開発者人数に応じたライセンス

シングルデベロッパ（ユーザ）	開発可能製品数	利用可能開発者数	CPU	コンパイラ
	無制限	1名	1CPUアーキテクチャ	1種類

「シングルデベロッパライセンス」は開発プロジェクトに制限されず、無制限に製品開発が可能です。開発者様が複数の開発プロジェクトを担当するなど、多品種開発に最適なライセンスです。

CPUアーキテクチャが同じCPUであれば、製品毎のCPU変更（デバイスメーカ変更）も対応可能です。

CPU	開発可能製品数	利用可能開発者数	CPU	コンパイラ
	無制限	無制限	1CPUアーキテクチャ	1種類



「CPUライセンス」は同一CPUアーキテクチャのCPUで複数の開発プロジェクト、開発者の人数に係わらず利用可能です。本ライセンスにより、SEGGER社製RTOS/ミドルウェアを含むソースコードを企業内で、共有ができます。御社内のソフトウェアプラットフォーム化に最適なライセンスです。
本ライセンスは、すべてお客様のご要望に従い都度提案となりますので、必ずしもCPUの制限事項が１CPUアーキテクチャになるわけではなく、ご要望に応じたライセンス提案をさせていただいています。

大規模な開発プロジェクトに最適なシングルプロダクト／プロダクトファミリライセンス

開発者の人数は無制限（外部協力会社含む）で特定の製品開発に利用可能なライセンス

シングルプロダクト	開発可能製品数	利用可能開発者数	CPU	コンパイラ
	1製品型番	無制限	1デバイス型番	1種類

複数の開発者で１つの製品（製品型番）開発が可能です。開発者様が多い大規模開発や品種展開を想定しない製品開発に最適。
製品メーカ様へのライセンスで、該当製品開発に係わる開発者は本ライセンスで利用可能です。受託開発で利用検討の場合は、ライセンス契約者として、受託元様での契約をお願いいたします。
例）「J-Link BASE」で契約し、「J-Link BASE」を開発する。

プロダクトファミリ	開発可能製品数	利用可能開発者数	CPU	コンパイラ
	1製品ファミリ	無制限	1デバイス型番	1種類

「プロダクトライセンス」の適用範囲を広げて、１製品シリーズの開発が可能です。開発者様が多い大規模開発で、派生製品開発を行う場合に最適となります。プロダクトファミリの定義は、お客様の要望に応じて、都度SEGGER社と協議の上、ライセンス費用提示となります。

例）「J-Linkシリーズ」で契約し、「J-Link BASE」「J-Link PLUS」「J-Link PRO」を開発する。
※適用範囲について、適宜ご相談ください。

提供会社

EmbiTeK | SEGGER

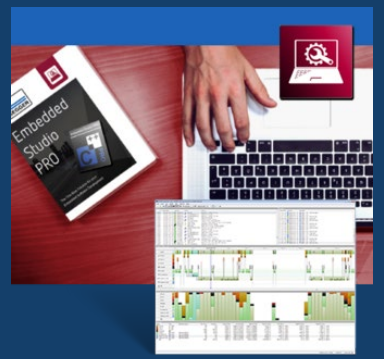
SEGGER Microcontroller GmbH

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
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

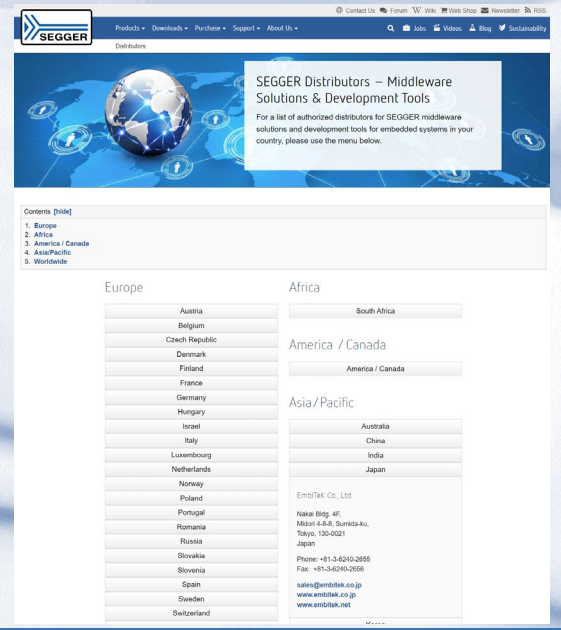
デバッグツール

書込みツール

EmbiTeK

EmbiTeK

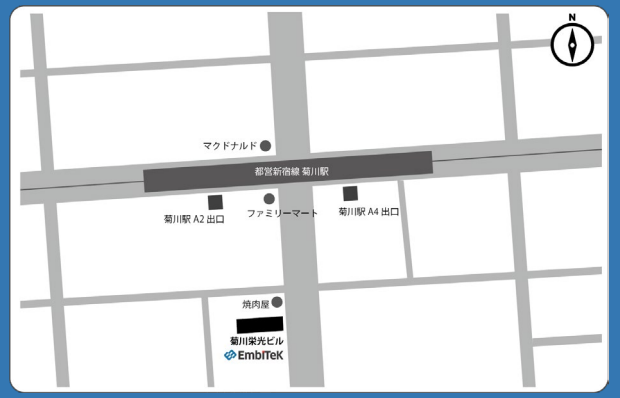
株式会社エンビテック



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

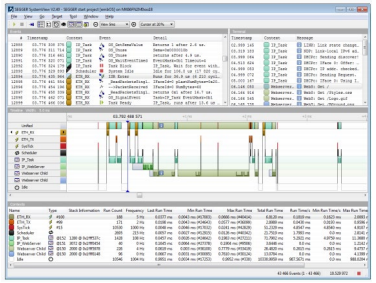
RTOS

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