組込システムに特化したTLS/SSL
emSSL

Non-RTOS/RTOS・ハードウェア・開発環境の依存性なく
利用可能なTLS/SSL

EmbiTeK

TLS1.0/1.1/1.2に対応するSSLソフトウェアモジュール

完全オリジナルコードで高いセキュリティを実現

オープンソースを利用し続ける限りかかえるセキュリティホールのリスクを回避

SSLサーバ認証/クライアント認証対応可能

ソフトウェア処理でも高速実行（ハードウェアアクセラレータにも対応）

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

emSSLはTLS1.0 (RFC2246) / TLS1.1 (RFC4346) / TLS1.2 (RFC5246)に準拠した
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

・接続対象のサーバ・クライアントに必要な暗号ライブラリだけを選択実装
（スキャンテスト自動選択可能）
・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

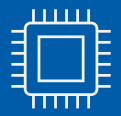
豊富な標準サンプルソースコードで利用方法の習得がしやすくなっています。

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

emNet TCP/IPスタック＋emSSL TLSサービス

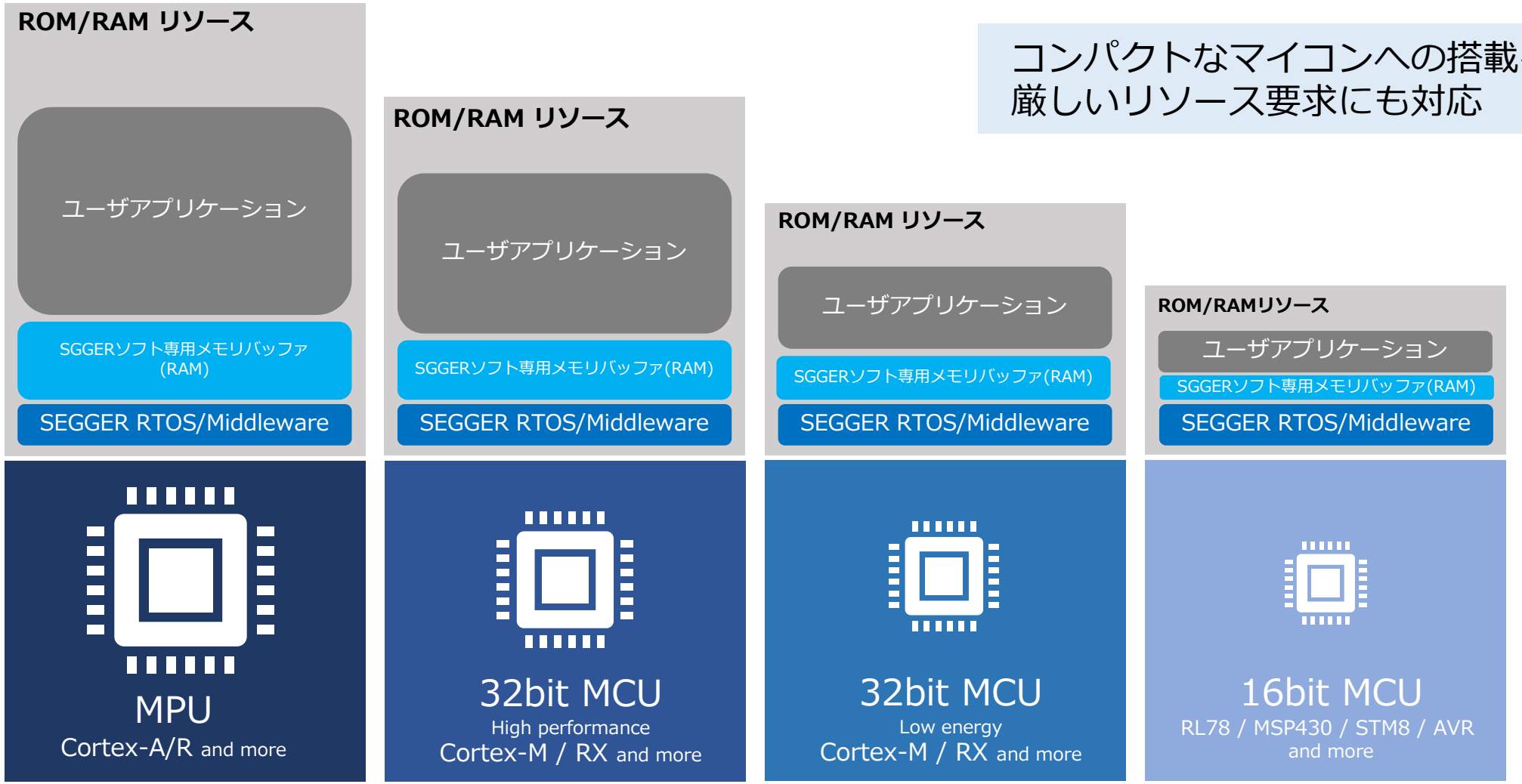
FTPS

Implicit mode:
HTTP => HTTPS と同様に、SSL/TLS を使って確立された TCP プロトコルを安全な接続で保護します。FTPSでは、よく知られている Port.21の代わりにPort.990が使用され、接続は最初からSSL/TLSで保護し、安全でないトランザクションは、単に接続時に拒否します。

FTPES

Explicit mode:
クライアントは、標準的なPort.21の標準的な非セキュア接続で開始し、セキュア接続に切り替えることを要求します。ほとんどのファイアウォールがport.21をブロックしないため、セキュリティポリシーに追加設定をする事なく利用できるというメリットはあります。サーバは、クライアントがセキュア接続に切り替えを要求しない場合、クライアントの接続を拒否します。

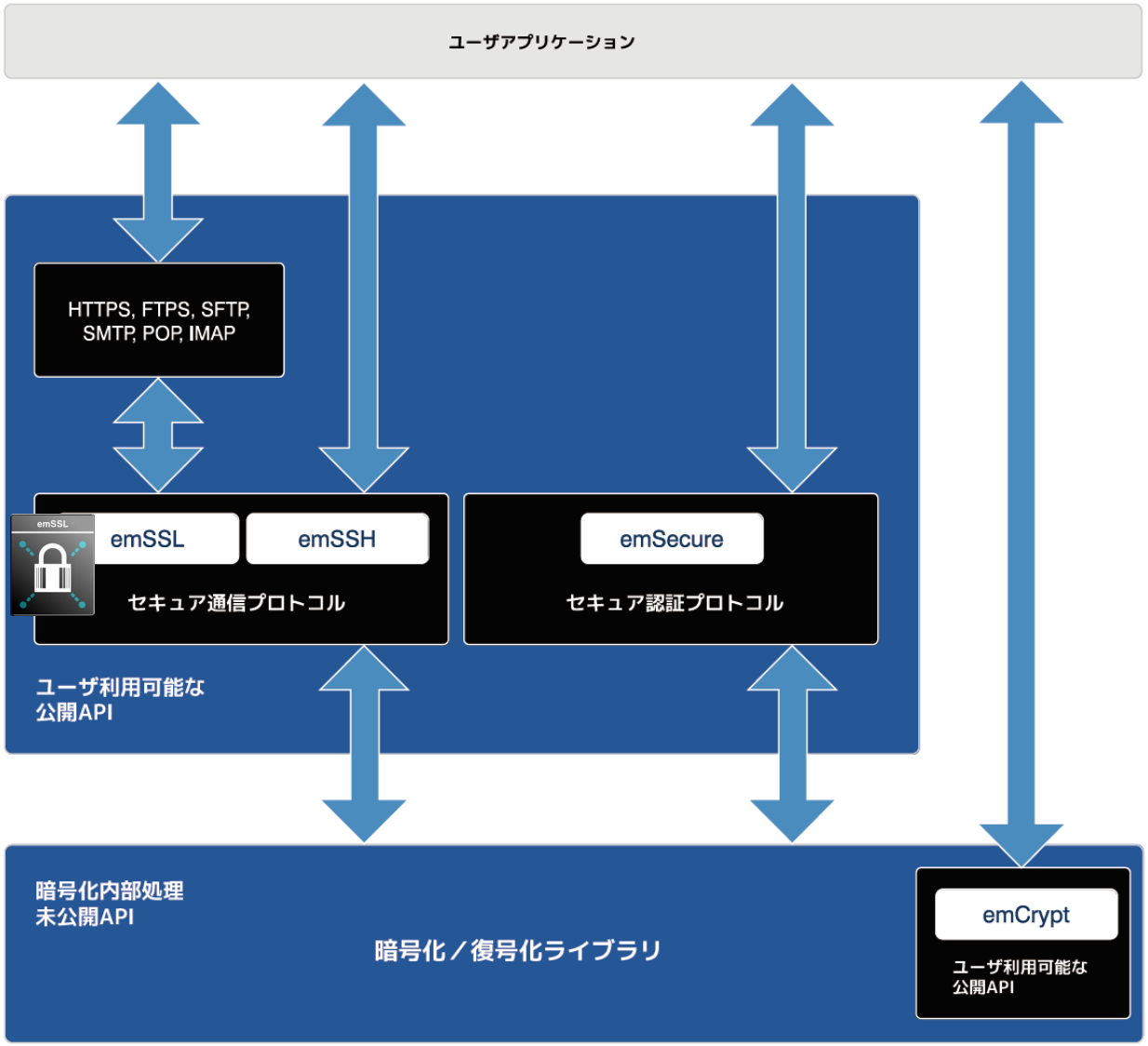
リソースの限られたマイコンでもハードウェアの性能を活かし、機能制限なく利用できるよう設計



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

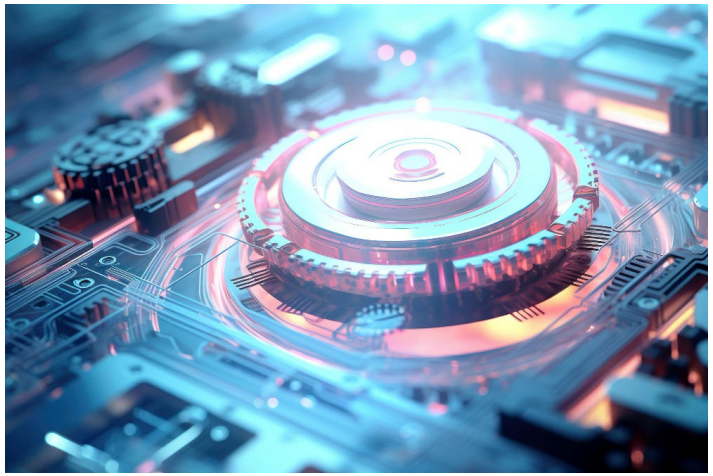
emSSL では、暗号モジュールスイートは実行時に動的に選択され、コードはシンプルに保たれる仕組みを用意しています。
また構成する必要性のない暗号モジュールは、コンパイル・リンク時に自動で排除され、最小の構成で出力されます。
製品パッケージに含まれる「Scan Suite Application」で特定のサーバが必要とする暗号モジュールを判別が可能です。

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

HALオプション



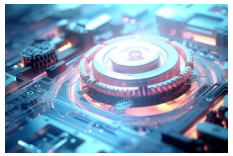
emSSL ハードウェアアクセラレータ

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



emSSL 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。

emSSL 性能ベンチマーク

- 必要リソース
- 速度ベンチマーク

最小のリソースで高速な処理を実現。

搭載必要リソース (Cortex-M3マイコン実装時)

Flash

実装	実装方法	ROM Size
最小構成	emSSL with the smallest single cipher suite, RSA_WITH_RC4_128_SHA, and TLS protocol version 1.2	17KByte
標準構成	emSSL with one single cipher suite, RSA_WITH_AES_128_CBC_SHA, and TLS protocol version 1.2 現状ほとんどのウェブブラウザで、HTTPs 接続を実現出来ます。	19KByte
最大構成	emSSL with all supported all cipher suites, all prime elliptic curves, TLS 1.0, TLS 1.1, and TLS 1.2	43KByte

コンパイラ：SEGGER Embedded Studio／CPU:Cortex-M4／アプリケーション：emNet Web server
この値にはサーバー証明書は含まれていないため、証明書ごとに約1.5KB追加リソースが必要です。

RSA_WITH_AES_128_CBC_SHA and TLS 1.2　実装に必要なコンポーネント	
Cipher	AES128 CBC
Signature verification	RSA
Signature algorithm	SHA with RSA
Pseudorandom function (PRF)	SHA256
Message authentication code (MAC)	SHA1, SHA256

RAMリソース

実装する暗号・アルゴリズムとTLS同時接続数に依存します。最小のケースはDES-RC4暗号スイートの単一接続で1.5KB以内です。
TLSの静的RAM要件は数十バイト程度ですが、接続時に鍵交換・証明書認証などの処理が必要となり、TLSネゴシエーションで
必要なRAMが増加します。

各鍵交換アルゴリズム毎のベンチマークテスト

Cortex-M4 (200MHz) / 内蔵Flash,RAMで動作ベンチマーク
各鍵交換アルゴリズムを使用して www.segger.com および www.google.com に安全な接続するためのTLSネゴシエーションで測定
※IPトランスポートでの送受信時間は含まれません。

Cipher Suite	Key algorithm	SSL time
C008 TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA	ECDSA	278 ms
C009 TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	ECDSA	274 ms
C023 TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	ECDSA	273 ms
C0AC TLS_ECDHE_ECDSA_WITH_AES_128_CCM	ECDSA	277 ms
C0AE TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8	ECDSA	276 ms
C02B TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	ECDSA	272 ms
C00A TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	ECDSA	276 ms
C024 TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	ECDSA	279 ms
C0AD TLS_ECDHE_ECDSA_WITH_AES_256_CCM	ECDSA	275 ms
C0AF TLS_ECDHE_ECDSA_WITH_AES_256_CCM_8	ECDSA	277 ms
C02C TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDSA	277 ms
C048 TLS_ECDHE_ECDSA_WITH_ARIA_128_CBC_SHA256	ECDSA	280 ms
C05C TLS_ECDHE_ECDSA_WITH_ARIA_128_GCM_SHA256	ECDSA	272 ms
C049 TLS_ECDHE_ECDSA_WITH_ARIA_256_CBC_SHA384	ECDSA	286 ms
C05D TLS_ECDHE_ECDSA_WITH_ARIA_256_GCM_SHA384	ECDSA	276 ms
C072 TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_CBC_SHA256	ECDSA	280 ms
C086 TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_GCM_SHA256	ECDSA	272 ms
C073 TLS_ECDHE_ECDSA_WITH_CAMELLIA_256_CBC_SHA384	ECDSA	277 ms
C087 TLS_ECDHE_ECDSA_WITH_CAMELLIA_256_GCM_SHA384	ECDSA	283 ms
C007 TLS_ECDHE_ECDSA_WITH_RC4_128_SHA	ECDSA	293 ms
CCA9 TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256	ECDSA	269 ms

Cipher Suite	Key algorithm	SSL time
C012 TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA	RSA	197 ms
C013 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	RSA	195 ms
C027 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	RSA	205 ms
C02F TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	RSA	198 ms
C014 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	RSA	192 ms
C028 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	RSA	202 ms
C030 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	RSA	196 ms
C04C TLS_ECDHE_RSA_WITH_ARIA_128_CBC_SHA256	RSA	194 ms
C060 TLS_ECDHE_RSA_WITH_ARIA_128_GCM_SHA256	RSA	202 ms
C04D TLS_ECDHE_RSA_WITH_ARIA_256_CBC_SHA384	RSA	200 ms
C061 TLS_ECDHE_RSA_WITH_ARIA_256_GCM_SHA384	RSA	192 ms
C076 TLS_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256	RSA	186 ms
C08A TLS_ECDHE_RSA_WITH_CAMELLIA_128_GCM_SHA256	RSA	191 ms
C077 TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384	RSA	200 ms
C08B TLS_ECDHE_RSA_WITH_CAMELLIA_256_GCM_SHA384	RSA	194 ms
C011 TLS_ECDHE_RSA_WITH_RC4_128_SHA	RSA	200 ms
CCA8 TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	RSA	200 ms

Cipher Suite	Key algorithm	SSL time
00D TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA	RSA	194 ms
C00E TLS_ECDH_RSA_WITH_AES_128_CBC_SHA	RSA	186 ms
C029 TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256	RSA	182 ms
C031 TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256	RSA	185 ms
C00F TLS_ECDH_RSA_WITH_AES_256_CBC_SHA	RSA	189 ms
C02A TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384	RSA	191 ms
C032 TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384	RSA	188 ms
C04E TLS_ECDH_RSA_WITH_ARIA_128_CBC_SHA256	RSA	187 ms
C062 TLS_ECDH_RSA_WITH_ARIA_128_GCM_SHA256	RSA	182 ms
C04F TLS_ECDH_RSA_WITH_ARIA_256_CBC_SHA384	RSA	190 ms
C063 TLS_ECDH_RSA_WITH_ARIA_256_GCM_SHA384	RSA	185 ms
C078 TLS_ECDH_RSA_WITH_CAMELLIA_128_CBC_SHA256	RSA	187 ms
C08C TLS_ECDH_RSA_WITH_CAMELLIA_128_GCM_SHA256	RSA	192 ms
C079 TLS_ECDH_RSA_WITH_CAMELLIA_256_CBC_SHA384	RSA	192 ms
C08D TLS_ECDH_RSA_WITH_CAMELLIA_256_GCM_SHA384	RSA	186 ms
C00C TLS_ECDH_RSA_WITH_RC4_128_SHA	RSA	185 ms

Cipher Suite	Key algorithm	SSL time
000A TLS_RSA_WITH_3DES_EDE_CBC_SHA	RSA	13 ms
0096 TLS_RSA_WITH_SEED_CBC_SHA	RSA	11 ms
002F TLS_RSA_WITH_AES_128_CBC_SHA	RSA	12 ms
003C TLS_RSA_WITH_AES_128_CBC_SHA256	RSA	12 ms
C09C TLS_RSA_WITH_AES_128_CCM	RSA	12 ms
009C TLS_RSA_WITH_AES_128_GCM_SHA256	RSA	12 ms
0035 TLS_RSA_WITH_AES_256_CBC_SHA	RSA	12 ms
003D TLS_RSA_WITH_AES_256_CBC_SHA256	RSA	12 ms
C09D TLS_RSA_WITH_AES_256_CCM	RSA	13 ms
009D TLS_RSA_WITH_AES_256_GCM_SHA384	RSA	15 ms
0041 TLS_RSA_WITH_CAMELLIA_128_CBC_SHA	RSA	12 ms
0084 TLS_RSA_WITH_CAMELLIA_256_CBC_SHA	RSA	12 ms
00BA TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256	RSA	12 ms
00C0 TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256	RSA	12 ms
C07A TLS_RSA_WITH_CAMELLIA_128_GCM_SHA256	RSA	12 ms
C07B TLS_RSA_WITH_CAMELLIA_256_GCM_SHA384	RSA	15 ms
C03C TLS_RSA_WITH_ARIA_128_CBC_SHA256	RSA	13 ms
C03D TLS_RSA_WITH_ARIA_256_CBC_SHA384	RSA	18 ms
C050 TLS_RSA_WITH_ARIA_128_GCM_SHA256	RSA	14 ms
C051 TLS_RSA_WITH_ARIA_256_GCM_SHA384	RSA	16 ms
0004 TLS_RSA_WITH_RC4_128_MD5	RSA	13 ms
0005 TLS_RSA_WITH_RC4_128_SHA	RSA	12 ms

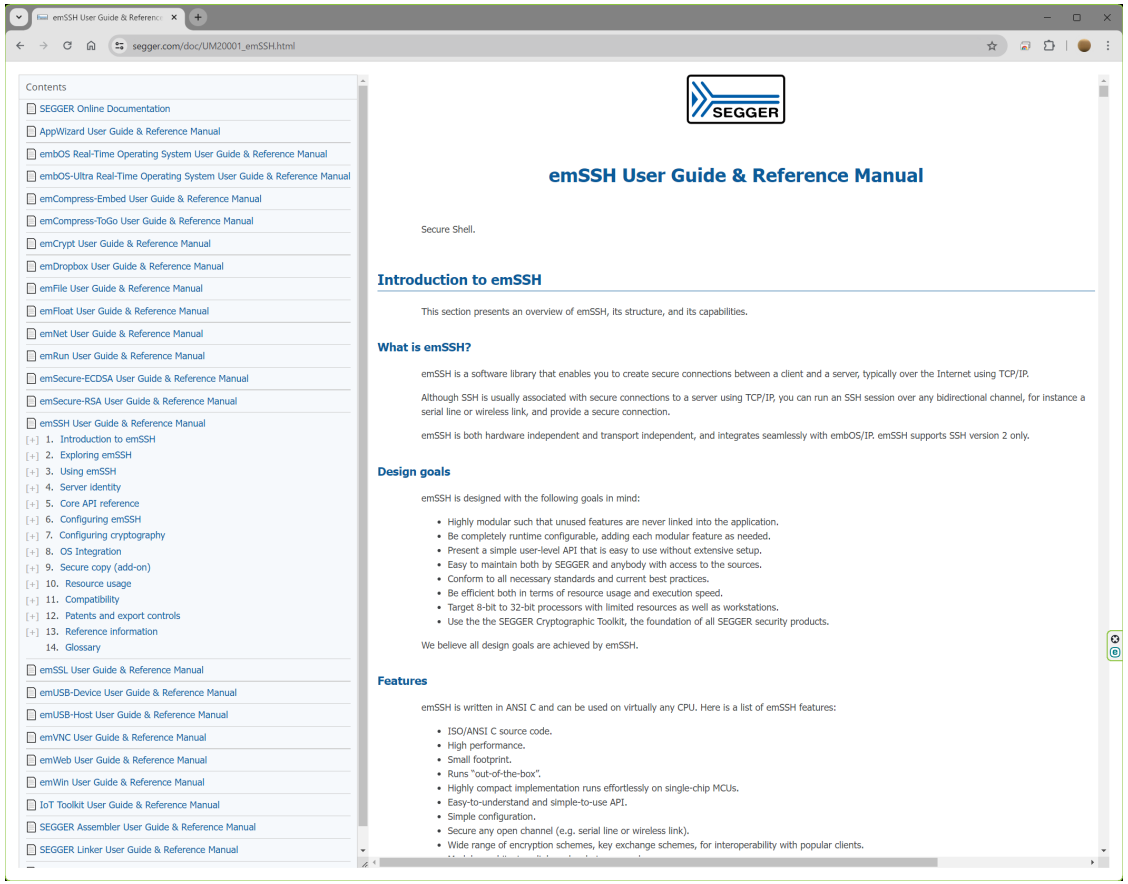
emSSL 開発・導入支援

- 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

emSSL – 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



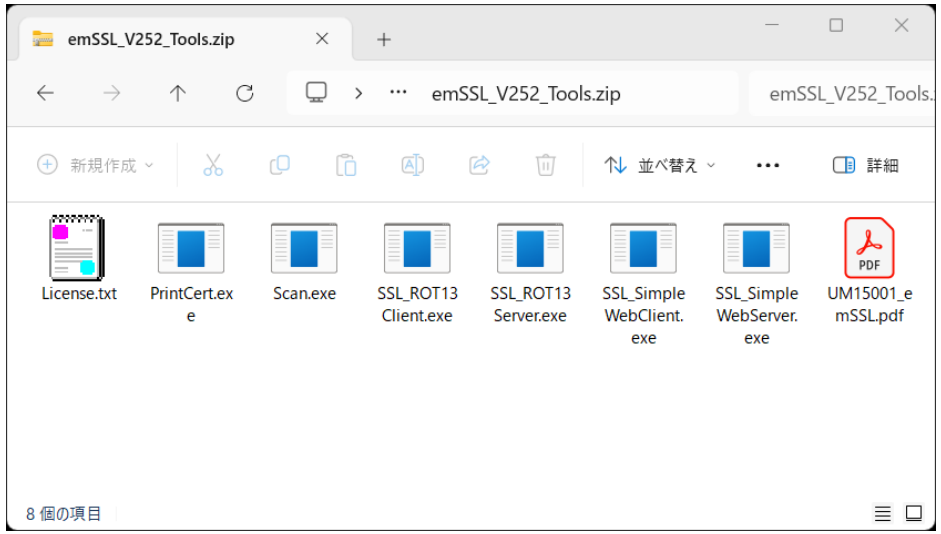
ブラウザの翻訳機能で日本語表示可能

Google Chrome推奨

https://www.segger.com/doc/UM15001_emSSL.html

同梱サンプルアプリケーション

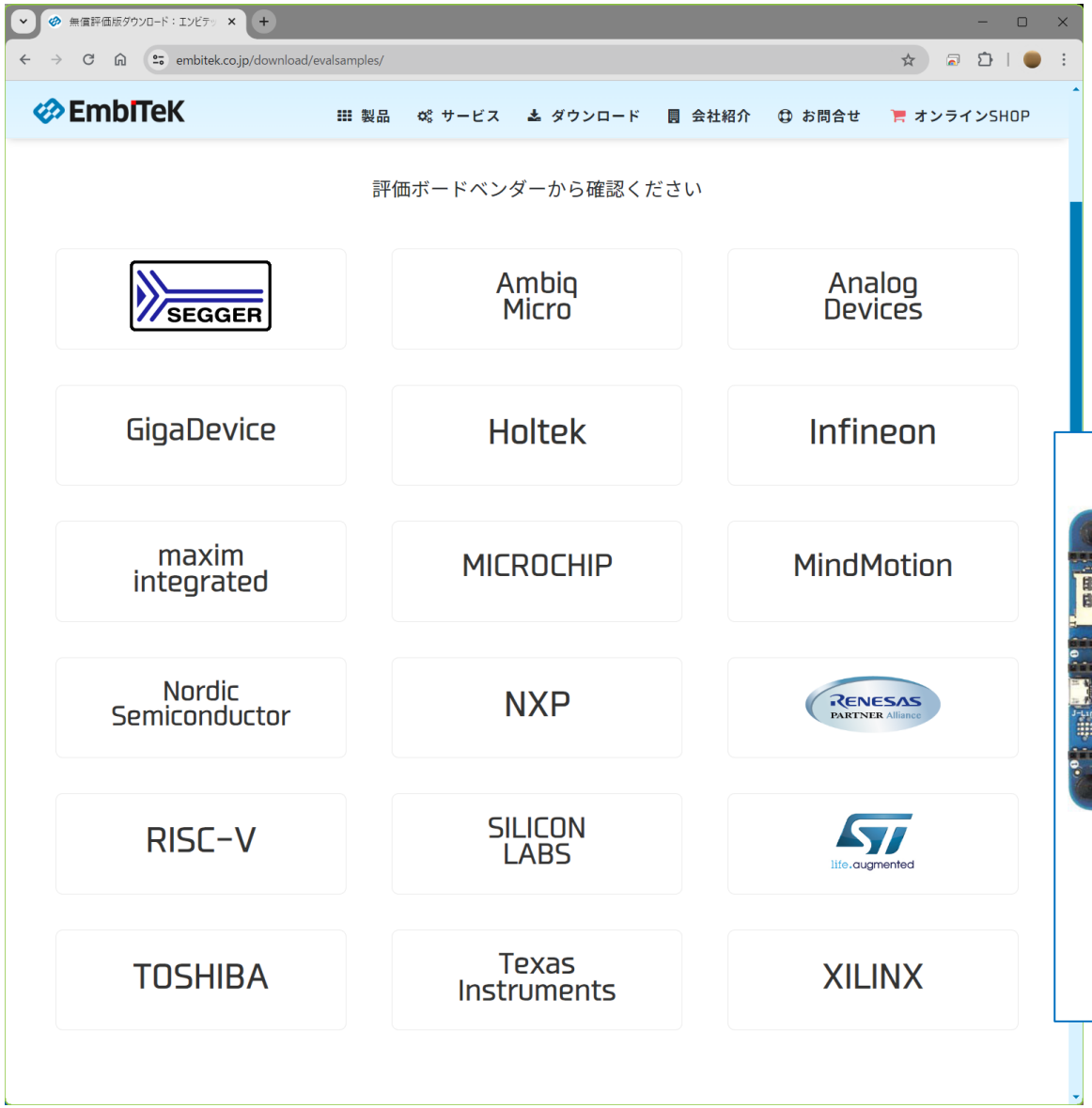
emSSLには、使用方法を示すサンプルユーティリティとツールが含まれています。
サンプルアプリケーションは、実行ファイルの評価版をダウンロード可能



アプリケーション名	説明	アプリケーション名	説明
SimpleWebClient	HTTPS経由でWebページを取得し、コンソールに印刷します。	スキャン	サーバーをスキャンして、サポートされている暗号スイートを探します。
SimpleWebServer	HTTPSを使用する最小限のWebサーバー	ROT13Server	ROT13サービスを提供するサーバー
PrintCert	X.509 SSL証明書を読み取り、その情報をコンソールに出力します。	ROT13Client	ROT13サービスを使用するクライアント

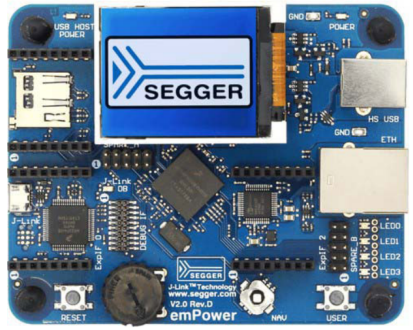
評価版ダウンロード：https://www.segger.com/downloads/emssl/emSSL_Tools

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

SEGGER emPower



MCU：Kinetis K66（Arm Cortex-M4）/ 180MHz

評価用ボード貸出可能

開発環境：Embedded Studio【開発環境無償評価版ダウンロード】

BSP パッケージ内容：

RTOS	embOS + Profiling
圧縮・解凍	emCompress-Embed, emCompress-ToGo
Modbus	emModbus Master, emModbus Slave
TCP/IP	emNet BASE + Web Server, CoAP Server / Client, DHCP Server, (m)DNS/LLMNR/DNS-SD Server, FTP Client, FTP Server, MQTT Client, NetBIOS Name Service, SMTP Client, SNMP Agent, SNTP Client, UPnP, WebSocket, emNet driver for Freescale Kinetis K60/K70
セキュリティ	emSSH Secure Shell, Secure Copy, emSSL Secure Sockets Layer, emSecure-RSA, emSecure-ECDSA
暗号・サイファー	emCrypt PRO
IoT Toolkit	HTTP Client, JSON Parser
GUI	emWin BASE + AntiAliasing, Bitmap Converter, Font Converter, Memory Devices, Simulation, VNC Server, Widgets, Window Manager, GUIDRV_FlexColor
FileSystem	emFile BASE + Encryption, FAT, FAT LFN, Journaling, SD/SDHC/SDXC/MMC, NAND, RAMDisk
USB-Device	emUSB-Device BASE + Audio, Bulk, CDC, DFU, HID, MSD, MSD-CDROM, MTP, Printer Class, IP-over-USB component, VirtualMSD, Video, Target Driver for Freescale Kinetis K60/K70 HighSpeed (EHCI)
USB-Host	emUSB-Host BASE + Bulk, CDC, FTDI UART, HID, MIDI, MSD, MTP, Printer Class, Freescale Kinetis FullSpeed Driver

BSP評価版ダウンロード（ZIP）

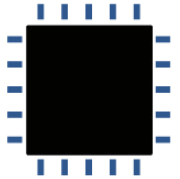
https://www.embitek.co.jp/download/evalsamples/

emSSL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

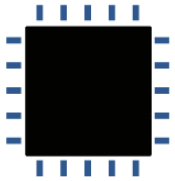
開発プロジェクトは無制限／開発者人数に応じたライセンス

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

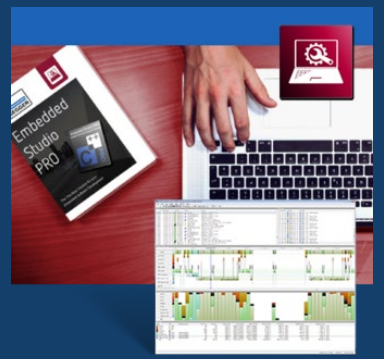
SEGGER Microcontroller GmbH

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

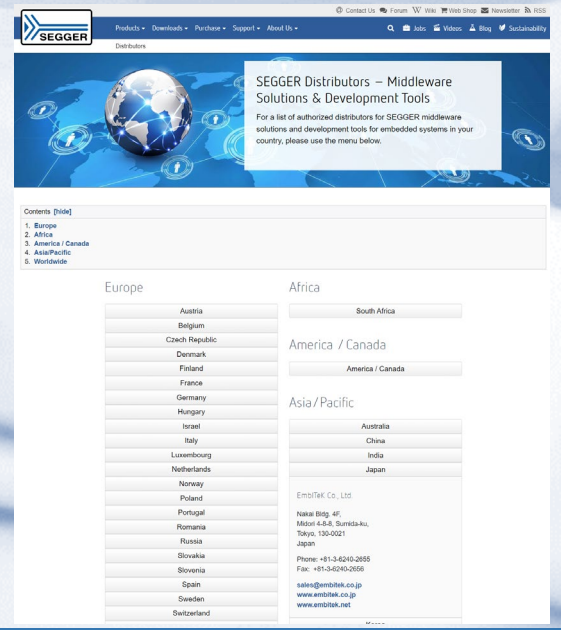
デバッグツール

書込みツール

EmbiTeK

EmbiTeK

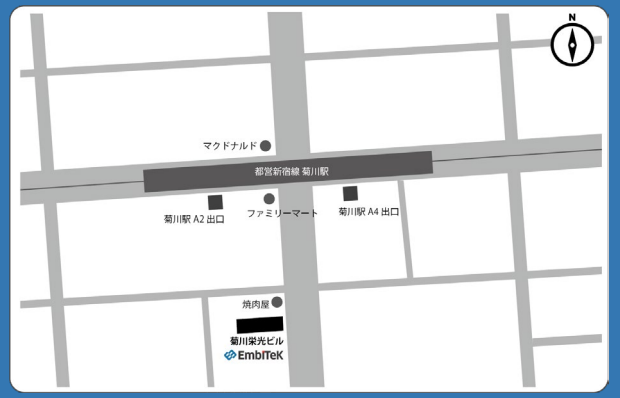
株式会社エンビテック



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

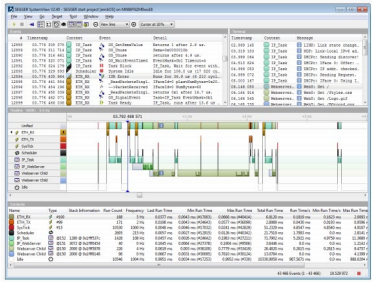
RTOS

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