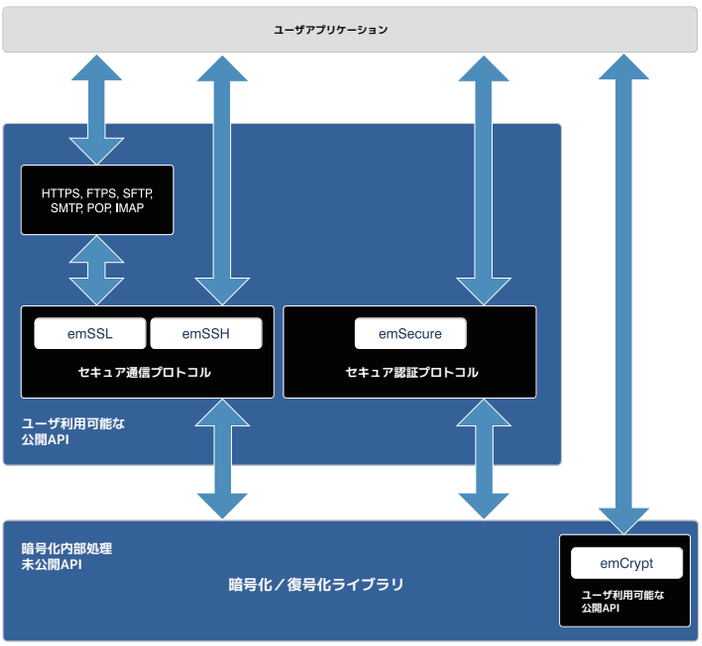
emCrypt 暗号化ライブラリ

高性能で信頼性の高い暗号ライブラリ

コンパクトで信頼性の高い暗号ライブラリ



組込システム向けに設計された、コンパクトで高速な暗号化ライブラリパッケージ。オープンソースコードを一切利用せずに、独自ソースコードでお客様のシステムを保護します。ユーザアプリケーションから利用可能な広範な API が提供されています。
「emCrypt」はターゲットマイコンのリソースに合わせて実装可能です。制約のある小さなマイコンでは、最小限のメモリフットプリントで、リソースの大きなマイコンでは、より高速なパフォーマンスを発揮できるように拡張可能

- 広範な暗号アルゴリズムをサポート
- 小さなメモリフットプリントで動作可能
- リソースの割り当てを増やすことで高速処理
- オープンソースコード・GPL コードを含みません
- 暗号アルゴリズムを除外・追加も簡単に対応
- RTOS の有無にかかわらず利用可能
- 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。

実装に必要な ROM/RAM はユーザアプリケーション要求の暗号・アルゴリズムによって異なります。

サポートしている暗号・アルゴリズム

Cipher(暗号)	ハッシュアルゴリズム	デジタル署名
AES-128, AES-192, AES-256 DES and TripleDES (3DES / TDES) CAST, ARIA, SEED, Camellia, Twofish Blowfish, IDEA	MD5, RIPEMD-160, SHA-1 SHA-224, SHA-256, SHA-384 SHA-512, SHA-512/224, SHA-512/256 SHA3-224, SHA3-256, SHA3-384, SHA3-512 SM3	RSASSA-PSS, RSASSA-PKCS1 ECDSA (NIST prime curves and Brainpool curves) Ed25519, Ed448
鍵生成アルゴリズム	**ランダムビット生成**	**MAC アルゴリズム**
KDF1-SHA-1, KDF1-SHA-224, KDF1-SHA-255, KDF1-SHA-384, KDF1-SHA-512, KDF1-SHA-512/224, KDF1-SHA-512/256, KDF2-SHA-1, KDF2-SHA-224, KDF2-SHA-255, KDF2-SHA-384, KDF2-SHA-512, KDF2-SHA-512/224, KDF2-SHA-512/256, X9.63-KDF-SHA-1, X9.63-KDF-SHA-224, X9.63-KDF-SHA-256, X9.63-KDF-SHA-384, X9.63-KDF-SHA-512, X9.63-KDF-SHA-512/224, X9.63-KDF-SHA-512/256 HKDF-MD5, HKDF-RIPEMD-160, HKDF-SHA-1, HKDF-SHA-224, HKDF-SHA-255, HKDF-SHA-384, HKDF-SHA-512, HKDF-SHA-512/224, HKDF-SHA-512/256 PBKDF2-SHA-1, PBKDF2-SHA-224, PBKDF2-SHA-256, PBKDF2-SHA-384, PBKDF2-SHA-512, PBKDF2-SHA-512/224, PBKDF2-SHA-512/256	Fortuna Hash-DRBG-SHA-1, Hash-DRBG-SHA-224, Hash-DRBG-SHA-256, Hash-DRBG-SHA-384, Hash-DRBG-SHA-512, Hash-DRBG-SHA-512/224, Hash-DRBG-SHA-512/256 HMAC-DRBG-SHA-1, HMAC-DRBG-SHA-224, HMAC-DRBG-SHA-256, HMAC-DRBG-SHA-384, HMAC-DRBG-SHA-512, HMAC-DRBG-SHA-512/224, HMAC-DRBG-SHA-512/256 CTR-DRBG-TDES, CTR-DRBG-AES-128, CTR-DRBG-AES-192, CTR-DRBG-AES-256	CMAC-AES, CMAC-TDES, CMAC-SEED, CMAC-ARIA, CMAC-Camellia, CMAC-Twofish GMAC-AES, GMAC-SEED, GMAC-ARIA, GMAC-Camellia, GMAC-Twofish HMAC-MD5, HMAC-RIPEMD-160, HMAC-SHA-1, HMAC-SHA-224, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512, HMAC-SHA-512/224, HMAC-SHA-512/256, HMAC-SHA3-224, HMAC-SHA3-256, HMAC-SHA3-384, HMAC-SHA3-512, KMAC

RTOS 依存性なし・ベアメタル（Non-RTOS）環境でも利用可能です。

RTOS 要件実装可否	embOS	FreeRTOS	iTRON	RTOS なし
	◎			

emCrypt

ライセンス製品パッケージ

パッケージ	内容
emCrypt BASE	■ AES-128, AES-192, AES-256 ■ DES ■ TripleDES (3DES / TDES) ■ MD5 ■ RIPEMD-160 ■ SHA-1 ■ SHA-224, SHA-256. SHA-384, SHA-512, SHA-512/224, SHA-512/256
emCrypt PRO	■すべての暗号 (ciphers) - AES, XTS-AES, DES, TripleDES, ARIA, SEED, Camellia, Blowfish, Twofish, IDEA ■すべてのハッシュアルゴリズム - MD5, RIPEMD-160, SHA-1, SHA-2 family, SHA-3 family, SM3 ■すべての MAC アルゴリズム - HMAC, CMAC, GMAC, KMAC, Michael ■すべての鍵生成アルゴリズム - KDF1, KDF2, HKDF, PBKDF2, X9.63 KDF ■すべての鍵認証アルゴリズム - DH, ECDH, X25519, X448 ■すべてのデジタル署名アルゴリズム - RSASSA-PSS, RSASSA-PKCS1, DSA, ECDSA, Ed25519, Ed448 ■ RSA / DSA 用の鍵生成アルゴリズム ■ランダムビット生成 - Fortuna, Hash_DRBG, HMAC_DRBG, CTR_DRBG ■出力関数 - SHAKE128, SHAKE256, cSHAKE128, cSHAKE256 ■鍵カプセル化関数 - RSAES-OAEP, AESKW, Camellia-KW, ARIA-KW, SEED-KW, Twofish-KW ■ NIST prime curves - P-192, P-224, P-256, P-384, P-521 ■ Brainpool curves and twisted curves - brainpoolP160r1 through brainpoolP512r1 ■自己診断サンプルコード

emLib

ローコストライブラリ製品

シンプルなライブラリ製品群

限定された用途で活用できるシンプルライブラリ

「emLib」は暗号化モジュール「AES」「DES」や、データ整合性チェックモジュール「CRC」「ECC」のみを提供するローコストなライブラリ製品となります。お客様のアプリケーションに必要となるライブラリを選択実装して、暗号化、データ整合性チェックを必要に応じて呼び出すことができます。

暗号ライブラリ

emLib AES

AES-128, AES-256 ライブラリ

16 バイトを超えるデータの暗号化 / 復号化のためのチェーンブロック処理

emLib DES

DES（56 ビット）ライブラリ

8 バイトを超えるデータを処理するための CBC も含まれます。
DES 関数を複数回呼び出して、
より高いセキュリティ（TDES、TripleDES）も実現可能

データ整合性チェックライブラリ

emLib CRC

CRC ライブラリ

emLib CRC は、汎用 CRC 機能に加えて、CRC-CCITT、CRC-16、CRC-32 など一般的な CRC の最適化されたライブラリ。

emLib ECC

ECC ライブラリ

複数ビットエラーの検出と修正のためのルーチンを提供します。
4、8、24、および 40 ビットのエラー訂正ライブラリ

ハードウェアアクセラレータオプションモジュール

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	STM32CRYP	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.

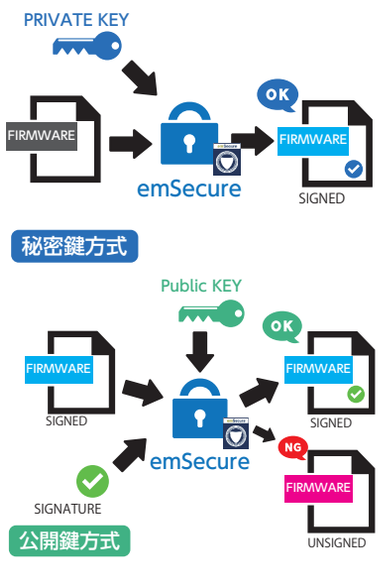
emSecure セキュリティゲートウェイ

ソフトウェア資産を守るセキュリティゲートウェイプロトコル

不正改造・不正量産を防ぐセキュリティゲートウェイ

「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ェアプログラムです。
お客様の製品をハードウェアコピー（偽物クローン）及びファームウェアコピー・編集（ハッキング）から守ることができます。
本製品はキーと署名を生成、データに署名して検証し、キーと署名をコンパイル可能な形式に変換、実行できるツールが含まれています。 emSecure には、署名生成を生産プロセスに直接統合し、データ検証をアプリケーションまたはファームウェアに統合するために必要なすべてのソースコードが含まれています。

ソフトウェアハッキング防止 - ファームウェアの認証



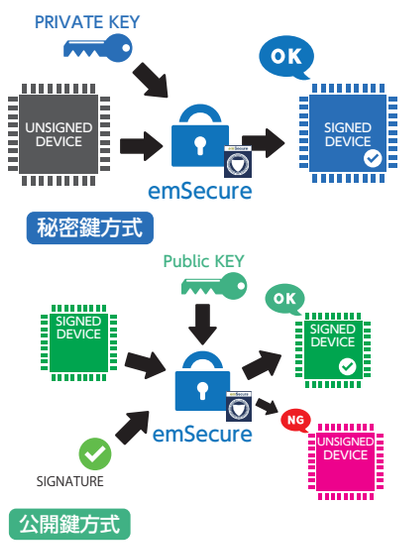
御社製品内でのファームウェア認証

承認されたファームウェアのみが製品で実行されるようにするため、ファームウェアイメージを「emSecure」で署名をつけます。これを実行するため、emSecure キーは 1 回生成され、秘密鍵はファームウェアの生産プロセス上で、署名され、ファームウェアと共に製品へ書き込まれます。

ブートローダ認証

公開鍵は製品のブートローダに含まれ、ファームウェアの更新を管理し、ファームウェアを起動します。ファームウェアの更新時、アプリケーションの起動時にブートローダは、署名によってファームウェアを検証します。一致すれば、ファームウェアは正常に開始されますが、一致しない場合は、アプリケーションはブートローダで停止するか、ファームウェアを消去します。

不正量産・複製品製造防止 - ハードウェアの認証



量産工程でのハードウェア認証

ハードウェアをコピーするだけで、悪意ある製造者が不正量産できないようにするため、量産時に emSecure キーペアが 1 回量産書き込み時に生成されます。

量産工程でのハードウェア認証

秘密鍵を製品の製造プロセスで生成します。マイコンの UID などユニークなデータを読取り、emSecure によって、秘密鍵を生成し、署名は、メモリ上の指定された場所へ書き込みます。公開鍵は製品で実行されるファームウェアに含まれ、ファームウェアの実行時に製品からユニークデータを読み取り、署名検証します。署名が一致しない場合、ファームウェアは実行を拒否します。

参考実装要件 - アルゴリズム・ハッシュ・キーサイズなどにより異なるため参考値（Cortex-M7 への実装時）

パッケージ	実装方法	ROM	RAM	Stack
emSecure-RSA ・2048 bit Key / SHA-1 アルゴリズム	署名のみ	5.8 KByte	0.03 KByte	2.1 KByte
	認証のみ	4.8 KByte	0.03 KByte	2.9 KByte
	署名・認証	6.3 KByte	0.03 KByte	2.9 KByte
emSecure-ECDSA ・SHA-256 アルゴリズム	認証のみ	9.2 KByte	0.04 KByte	2.4 KByte
	認証・鍵生成	10.8 KByte	0.04 KByte	6.2 KByte

RTOS 依存性なし・ベアメタル（Non-RTOS）環境でも利用可能です。

RTOS 要件実装可否	embOS	FreeRTOS	iTRON	RTOS なし
	◎			

emSSL

TLS1.1 / 1.2 対応 SSL 通信プロトコルモジュール

オープンソースではない SSL でより確実なセキュリティを提供

組込マイコン用に最適化された SSL 通信モジュール

組込機器とサーバ間の HTTP や FTP といった汎用的な TCP/IP 通信を暗号化し、セキュアなネットワークを実現します。
SEGGER 社製 emNet 以外にも BSD ソケットインターフェースをサポートする TCP/IP スタックに実装可能です。

サーバ認証・クライアント認証にも対応可能です。
オープンソースコード・GPL コードを一切含まないため、ソースコード開示義務は発生しません。
すべてソースコード提供で、お客様規定に基づくセキュリティ監査などの対応をスムーズに行う事が可能です。
ANSI-C 準拠コードのためすべての組込マイコン、x86 CPU などへの実装も可能です。コンパイラも任意に選択できます。

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

速度・パフォーマンス

ハードウェアアクセラレータを使用しないソフトウェア処理の場合、利用する暗号・アルゴリズムと利用可能なスタック RAM サイズにより異なりますが、SSL 通信でのオーバヘッドは数十 ms ～数百 ms となります。(Cortex-M7 利用時)

必要リソース

実装	実装方法	ROM
最小構成	emSSL with the smallest single cipher suite, RSA_WITH_RC4_128_SHA, and TLS protocol version 1.2	17 KByte
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。	19 KByte
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	43 KByte

RTOS 依存性なし・ベアメタル（Non-RTOS）環境でも利用可能です。

RTOS 要件実装可否	embOS	FreeRTOS	iTRON	RTOS なし
	◎	○ emNet 以外の場合、要ポーティング		

TCP/IP スタックは別途必要です。ベアメタル (non-RTOS) システムの場合、emNet のように OS レスで動作可能な TCP/IP スタックが必要になります。

emSSH

SSH セキュアログイン

SSH でセキュアログインを実現

emSSH を利用する事により、組込機器内のサーバ機能へセキュアなアクセスを実現

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します。
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。

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します。
オープンソースコード・GPL コードを一切含まないため、ソースコード開示義務は発生しません。
すべてソースコード提供で、お客様規定に基づくセキュリティ監査などの対応をスムーズに行う事が可能です。
ANSI-C 準拠コードのためすべての組込マイコン、x86 CPU などへの実装も可能です。コンパイラも任意に選択できます。

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）

鍵交換アルゴリズム	ECDH-ECDSA
curve25519-sha256 / curve25519-sha256@libssh.org rsa1024-sha1 / rsa2048-sha256 ecdh-sha2-nistp256 / ecdh-sha2-nistp384 / ecdh-sha2-nistp521 diffie-hellman-group1-sha1 / diffie-hellman-group14-sha1 diffie-hellman-group14-sha256 / diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 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-sha1 diffie-hellman-group-exchange-sha256 diffie-hellman-group-exchange-sha224@ssh.com diffie-hellman-group-exchange-sha384@ssh.com diffie-hellman-group-exchange-sha512@ssh.com	chacha20-poly1305@openssh.com aes256-ctr / aes256-cbc aes192-ctr / aes192-cbc aes128-ctr / aes128-cbc camellia256-ctr / camellia256-cbc camellia192-ctr / camellia192-cbc camellia128-ctr / camellia128-cbc 3des-ctr / 3des-cbc twofish256-cbc / twofish256-ctr twofish192-cbc / twofish192-ctr twofish128-cbc / twofish128-ctr / twofish-cbc blowfish-ctr / blowfish-cbc arcfour256 / arcfour128 / arcfour cast128-ctr / cast128-cbc aes128-gcm@openssh.com aes256-gcm@openssh.com rijndael-cbc@lysator.liu.
ECDH-RSA	**DHE-RSA**
ssh-ed25519 ecdsa-sha2-nistp256 / ecdsa-sha2-nistp384 / ecdsa-sha2-nistp521 ssh-rsa / ssh-rsa-sha224@ssh.com / ssh-rsa-sha256@ssh.com ssh-rsa-sha384@ssh.com / ssh-rsa-sha512@ssh.com ssh-dss / ssh-dss-sha256@ssh.com rsa-sha2-256 / rsa-sha2-512	hmac-sha2-512 / hmac-sha2-256 hmac-sha1 / hmac-sha1-96 / hmac-md5 / hmac-md5-96 hmac-sha2-512-etm@openssh.com / hmac-sha2-256-etm@openssh.com hmac-sha1-etm@openssh.com / hmac-sha1-96-etm@openssh.com hmac-md5-etm@openssh.com / hmac-md5-96-etm@openssh.com hmac-ripemd160@openssh.com / hmac-ripemd160-etm@openssh.com hmac-sha224@ssh.com / hmac-sha256-2@ssh.com hmac-sha384@ssh.com / hmac-sha512@ssh.com

emSSH SCP add-on

セキュアデータコピーアドオン（サーバ）

セキュアコピー（SCP）により、異なるホスト間でのファイルの安全な送信が可能になります。データ転送に ssh を使用し、同じレベルのセキュリティを提供します。

emSSH SCP でファイル単位で読み書きする場合は、ファイルアクセスできる「emFile」などのファイルシステムが必要となります。
（他社製可能）セクター単位でのデータ転送であれば、ファイルシステムなしでも実装可能です。

RTOS 依存性なし・ベアメタル（Non-RTOS）環境でも利用可能です。

RTOS 要件実装可否	embOS	FreeRTOS	iTRON	RTOS なし
	◎	○ emNet 以外の場合、要ポーティング		

TCP/IP スタックは別途必要です。ベアメタル (non-RTOS) システムの場合、emNet のように OS レスで動作可能な TCP/IP スタックが必要になります。

組込ソフトウェア RTOS / ミドルウェア ユーザ様のメリット

マイコン・開発環境・コンパイラなどの依存性を極力排除し、柔軟性の高いソフトウェア資産をご提供します。
既存 OS レスシステム ※1 、iTRON システムへ必要なソフトウェアをアドオンも対応可能

RTOS

embOS

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
ACD	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

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

すべてのソフトウェア製品は、ソースコードで提供。量産ロイヤリティはありません。
開発プロジェクト・開発対象製品無制限のライセンス（CPU ライセンス・ユーザライセンス）

低リソースかつ高性能

ローエンドなマイコンでも組込可能な低リソースソフトウェアモジュール。コンパクトにもかかわらず、高い性能、信頼性を実現した RTOS/ ミドルウェアです。マイコンのリソースを最大限に活用し、最大効率化できるお客様アプリケーションを可能にします。

プラットフォームに依存しない高い汎用性

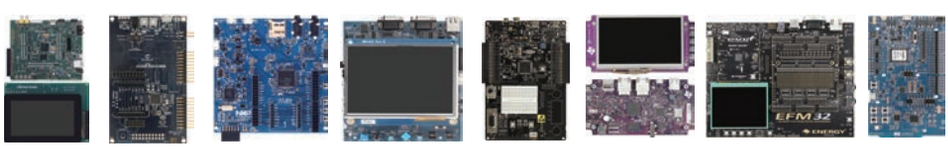
SEGGER 社製 RTOS/ ミドルウェアは、ANSI-C 準拠、MISRA-C2012 準拠の C 言語で開発されています。そのためマイコンやコンパイラなどに依存することなく利用可能です。ハードウェア依存部分のドライバもソースコードとしてモジュール化されているため、ハードウェアの変更にも柔軟に対応できます。お客様は、ターゲット製品開発に最適なマイコンを選択し、開発効率を最大化できる開発ツールを利用頂くことができます。

開発しやすいソフトウェア

製品には、利用方法を把握できるサンプルプロジェクトが同梱されているため、リファレンスガイドとサンプルを活用し、アプリケーションの動作を簡単に把握する事ができます。
それぞれのソフトウェアには、目的に応じた各種開発支援ツールが、合わせて提供されています。分かりやすい API、判読しやすいソースコードで、お客様の開発期間を短縮できます。

実績と信頼性

すでに欧州・米国を中心に多くのエンドユーザ製品に利用されています。
日本国内においても産業機器・医療機器開発を中心に多くのお客様でご採用いただいております。
ソースコード提供のため、アプリケーションの挙動はすべて把握でき、お客様における信頼性検証も対応可能です。全ての製品において、オープンソースコードや GPL コードを含まないため、オープンソースコードにつきまとうセキュリティリスク、GPL リーガルリスクを完全に排除できます。



充実した評価環境・サンプル

マイコンメーカ各社の評価ボード向けのサンプルを用意しておりますので、ご利用予定のマイコン、近しい環境でソフトウェアの評価を行うことが可能です。サンプルを利用して、そのままお客様製品開発に移行することもできます。

※1：お客様アプリケーションが、シングルタスクアプリケーション前提となります。マルチタスク処理が必要なソフトウェア（USB-Host や USB-Device 一部クラス、TCP/IP サーバ機能など）は OS レス環境ではご利用いただけません。

ユーザニーズに合わせて選べるライセンスモデル

大規模開発に優位なプロダクト（ファミリ）ライセンスや少量多品種、
プラットフォーム展開のしやすいユーザライセンスやＣＰＵライセンスなどユーザ様のソフトウェア開発計画に合わせて、
様々な提案が可能です。

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 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 型番	1 種類

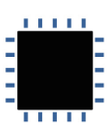
「プロダクトライセンス」の適用範囲を広げて、1 製品シリーズの開発が可能です。開発者様が多い大規模開発で、派生製品開発を行う場合に最適となります。

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。

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	1 CPU アーキテクチャ	1 種類

「ユーザライセンス」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	1 CPU 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。

バイアウト	開発可能製品数	利用可能開発者数	CPU	コンパイラ
	応相談	応相談	応相談	応相談

「バイアウトライセンス」はお客様ニーズに合わせて対応するライセンス契約です。お客様の開発ニーズ、利用対象開発者（御社内のみや御社のお客様、パートナーまで含む）、CPU 種別、開発環境などに合わせてご提案します。カスタマイズ契約となりますので、お客様のニーズからお聞かせください。
例）「○○ -SDK（開発キット）」を自社開発し、API を公開して、御社のお客様も利用可能にしたい。

すべての製品でソースコード提供となります。（embOS のみ、オブジェクト提供のローコストパッケージを提案可能です。）
量産に係わるロイヤリティは発生しません。

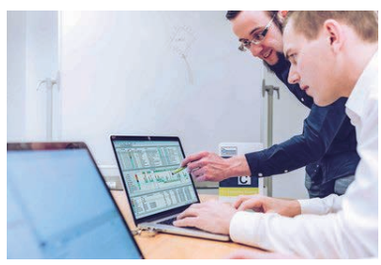
「コスト重視」か「日本語サポート対応」か選択可能

当社ではソフトウェアライセンス製品について、２種の基本テクニカルサポートモデルを用意しております。
基本サポートである SEGGER 社の直接サポート対応「SEGGER 社ソフトウェア製品サポート」と、当社日本語サポート対応まで拡張する「エンビテックサポートサービス」を提供。ソフトウェア製品ライセンスには、納品日から１年間の「SEGGER 社ソフトウェア製品サポート」が含まれております。（「エンビテックサポートサービス」は必要に応じて別途購入ください）次年度以降は、任意で更新が可能です。

SEGGER 社ソフトウェア製品サポート

「My PAGE」設定

お客様が購入された製品ライセンスについて、いつでもダウンロード可能な「MyPAGE」が設定されます。



製品のバージョンアップ

新機能追加に伴う製品バージョンアップの提供。

SEGGER 社によるテクニカルサポート

フォーラムやメールベースによる利用方法に関するサポート対応

製品不具合の対応・バグ修正対応

製品に不具合があった際の、ワークアラウンド提示や修正に関する対応

エンビテックサポートサービス

日本語問い合わせ窓口

購入頂いた製品に関する日本語テクニカルサポート窓口対応

製品不具合発生時における対応

汎用ハードウェア環境（評価キットなど）における再現確認と SEGGER 社への問題報告と SEGGER 社からの解決策の提示に関する日本語対応（SEGGER 社の保証範囲内）

別途費用にて対応の内容

お客様プログラムに起因する内容に関する調査・対応
SEGGER 社・当社提示の標準サンプルでは、問題が発生せず、お客様アプリケーション・プログラムに起因する不具合についての調査と対応

お客様特定環境下において発生した不具合の調査
汎用ハードウェア環境（評価キットなど）で再現確認できずに、特定（お客様開発など）のハードウェア下において発生している不具合の調査対応

C 言語やソフトウェア開発におけるコンサルティング対応
お客様アプリケーション記述やソフトウェア開発におけるアドバイス業務

サポート対応をお受けできないケース

他社提供物に起因する内容
他社製品に起因するサポート依頼・不具合調査対応

お客様ハードウェアに起因する不具合対応
お客様開発に起因する不具合における解決策の提示や修正対応

SEGGER 社製品において、SEGGER 社とのソフトウェアサポート契約が失効している場合

EmbiTeK
Embedded Development Solution

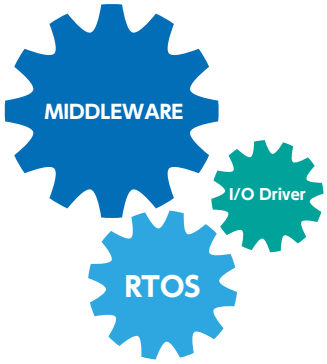
受託開発サービス

ポーティング・ドライバ開発

www.embitek.co.jp

受託開発サービス

ポーティング対応からドライバ開発まで対応



OS ポーティング

カスタマイズ・チューニング

ドライバ開発

アプリケーション開発

ミドルウェアポーティング

開発実績

ミドルウェア・スタックの開発（開発、カスタマイズ、移植、チューニング）

TCP/IP、HTTP、GUI、USB、File System などのミドルウェアのソフトウェア・スタックプログラムを移植します。ハードウェア化されたスタックプログラム（ハードウェア TCP/IP、IPSec 等）の移植も可能です。ご要望により、ミドルウェアスタックプログラムをカスタマイズします。

ファームウェア・I/O デバイスドライバの開発、移植、チューニング作業

ターゲットハードウェアに実装されている様々なコントローラのデバイスドライバプログラムを開発します。デバイスドライバとは、ハードウェア、ミドルウェア（又はアプリケーション）及び OS のインターフェースです。コントローラによって、同じ機能のコントローラでも内部のハードウェア管理が違います。

システム全体の最適化のため、それぞれのコントローラの内部ハードウェア管理ロジックを合わせて設計します。標準 I/O デバイスコントローラ以外に、お客様専用のハードウェア IP デバイスのドライバ開発サービスも提供します。

RTOS 移植・カーネルのチューニング、カスタマイズ

ARM、SH、PowerPC、MIPS 等のプロセッサベースのターゲットハードウェアの仕様及び特長に合わせて組込み向け OS 対応。

基板回路図又はハードウェア仕様書を参考にした移植済み OS のチューニング。

新しい開発環境へ乗り換える時の OS カーネルのマイグレーション。

命令・レジスタ構成変更可能な CPU へ移植する時の OS カーネルの対応。

対応 OS	RTOS	µITRON		
対応コア	Cortex-A15	Cortex-A8/9	Cortex-R4/5	Cortex-M33/32
	Cortex-M7	Cortex-M3/4	Cortex-M0/0+	ARM7/9/11
	RX	RL78	SH2/2A/3/4	PowerPC
ドライバ	キャッシュ・MMU I/F	CPU バス・メモリコントローラ	クロック PLL コントローラ	CAN
	割込コントローラ	タイマ・カウンタ	RTC	DMA コントローラ
	I2C / SPI / ESPI	EEPROM	フラッシュローダ	RS232 / RS485
	PCI / Compact PCI	LAN	CF / SD	ADC / DAC
	タッチスクリーン I/F	ARCNET コントローラ	USB	LCD
	カスタム FPGA			

プロフェッショナルサポート

SEGGER 製品・他社製品などトータルにサポートする窓口を設けていますので、お気軽に活用ください。

ハンズオントレーニング

ご相談

テクニカルサポート