SEGGER
www.segger.com

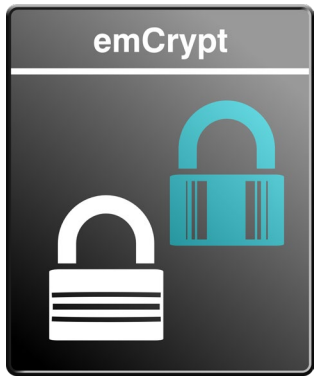
暗号セキュリティ

emCrypt

Non-RTOS/RTOS・ハードウェア・開発環境の依存性なく
利用できるセキュリティプラットフォーム

EmbiTeK

暗号セキュリティの基盤ソフトウェアとして利用できる暗号ライブラリ



完全オリジナルコードで高いセキュリティを実現

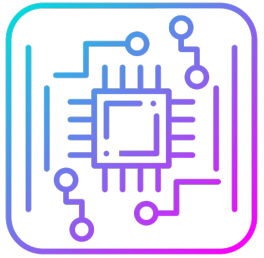
オープンソースを利用し続ける限りかかえるセキュリティホールのリスクを回避

多くのCipher / Hashアルゴリズム / 鍵生成認証アルゴリズム
ランダムビット生成をサポート

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

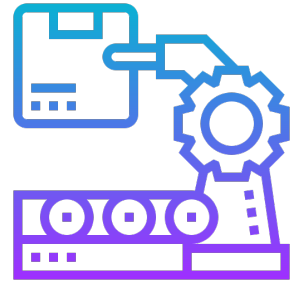


幅広いCPU対応

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

emCrypt はFIPS PUB, NIST, IETF RFCなどスタンダード規格/ドキュメントに準拠し、SEGGERがコンパクトな組込機器向けに独自開発したオリジナルソースコードで低リソースの組込マイコンで安定性の高い運用を実現

整理されたファイル構造とAPI構造

・各種設定・導入を分かりやすいAPIで実装
・必要な暗号ライブラリだけを選択実装
・利用するマイコンに合わせた最適化を柔軟に設定可能

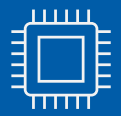
導入容易性 開発しやすさ

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。

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。

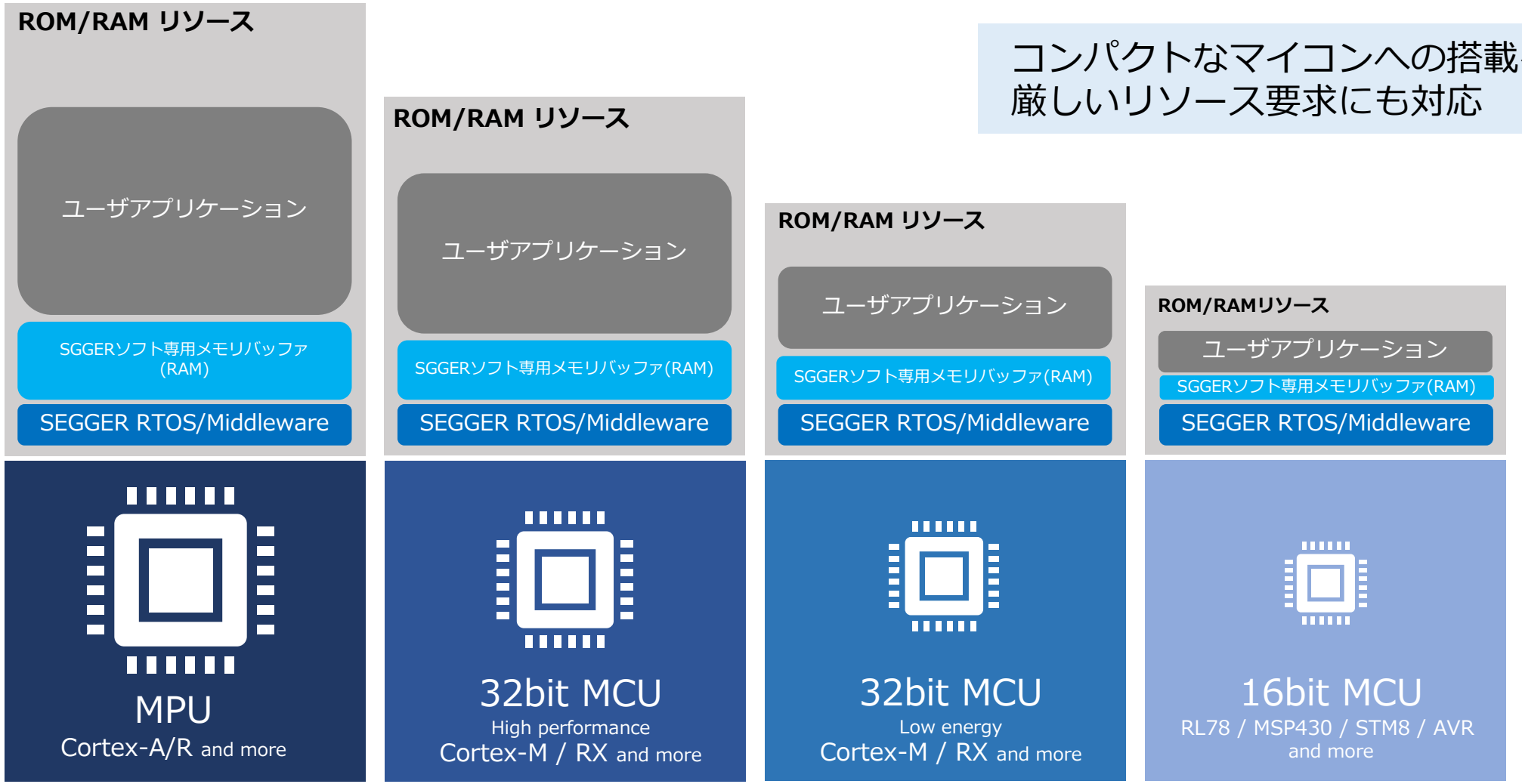


ソフトウェア継続性を強化

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

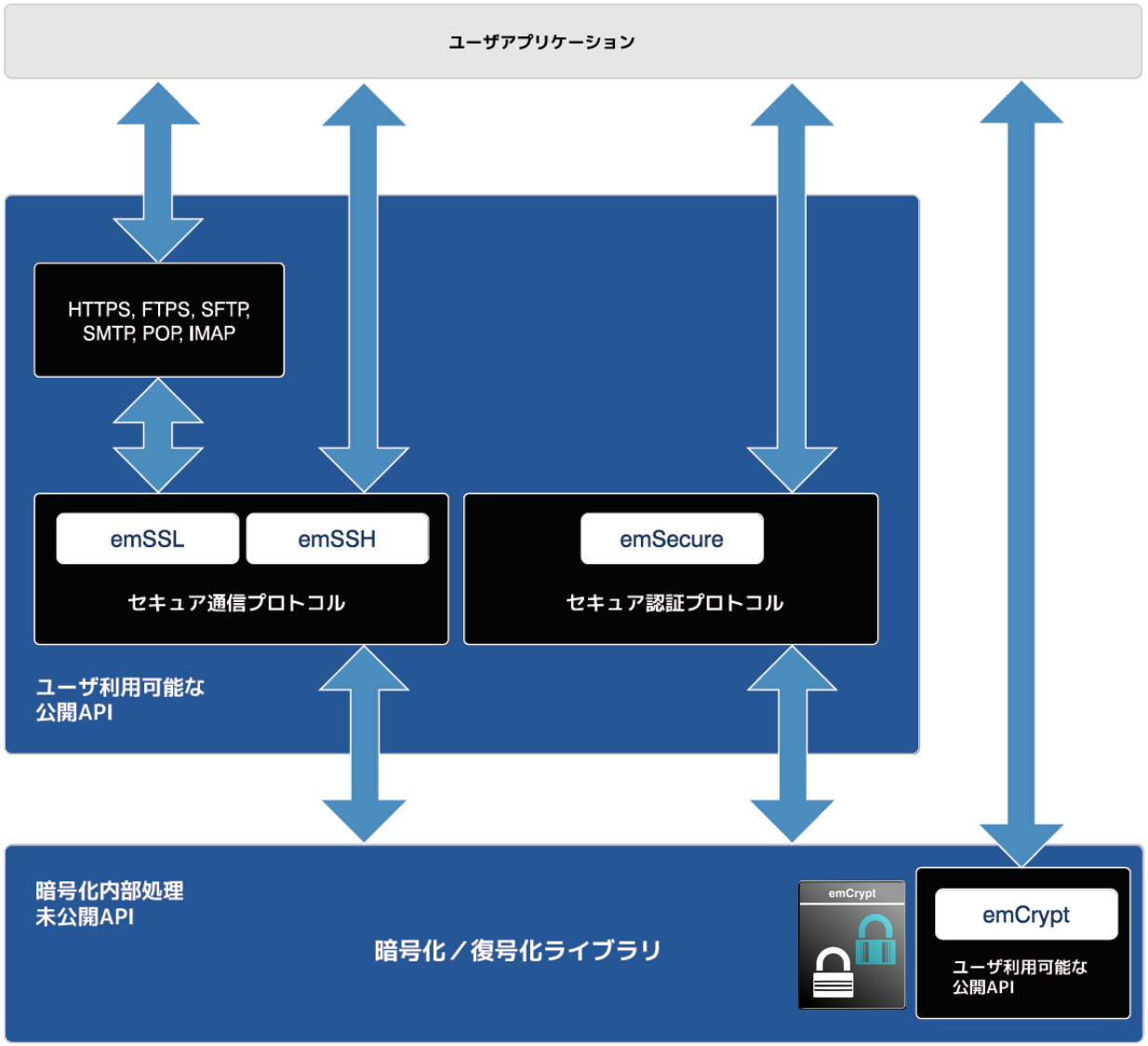
リソースの限られたマイコンでもハードウェアの性能を活かし、機能制限なく利用できるよう設計



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。

暗号セキュリティで共通化された暗号ライブラリ

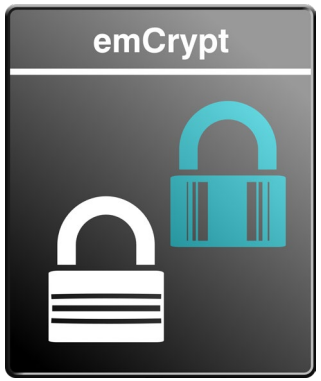


- 広範な暗号アルゴリズムをサポート
- 小さなメモリフットプリントで動作可能
- リソースの割り当てを増やすことで高速処理
- オープンソースコード・GPL コードを含みません
- 暗号アルゴリズムを除外・追加も簡単に対応
- RTOS の有無にかかわらず利用可能
- ハードウェアアクセラレータ対応（オプション）

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。

対応する暗号・アルゴリズムなど



サポートしている暗号・アルゴリズム

Cipher(暗号)

AES-128, AES-192, AES-256
DES and TripleDES (3DES / TDES)
CAST, ARIA, SEED, Camellia, Twofish
Blowfish, IDEA

ハッシュアルゴリズム

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

デジタル署名

RSASSA-PSS, RSASSA-PKCS1
ECDSA (NIST prime curves and Brainpool curves)
Ed25519, Ed448

鍵生成アルゴリズム

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

ランダムビット生成

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

MAC アルゴリズム

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

暗号セキュリティで共通化された暗号ライブラリ

BASE パッケージ

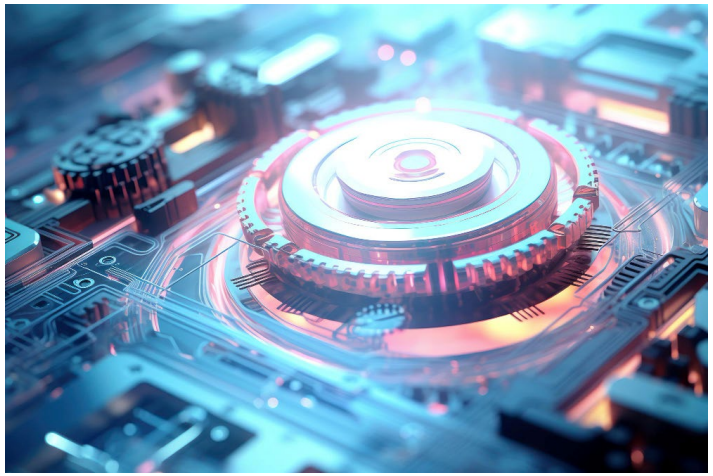
Ciphers	AES-128, AES-192, AES-256, DES TripleDES (also known as 3DES or TDES) with all keying options
hash algorithms	MD5, RIPEMD-160 SHA-1, SHA-224, SHA-256. SHA-384, SHA-512, SHA-512/224, SHA-512/256

PRO パッケージ

自己診断
サンプルコード含む

Ciphers	AES, XTS-AES, DES, TripleDES, ARIA, SEED, Camellia, Blowfish, Twofish, IDEA
hash algorithms	MD5, RIPEMD-160, SHA-1, SHA-2 family, SHA-3 family, SM3
MAC algorithms	HMAC, CMAC, GMAC, KMAC, Michael
key derivation algorithms	KDF1, KDF2, HKDF, PBKDF2, X9.63 KDF
key agreement protocols	DH, ECDH, X25519, X448
digital signature protocols	RSASSA-PSS, RSASSA-PKCS1, DSA, ECDSA, Ed25519, Ed448
key generation algorithms	RSA and DSA, probabilistic and proven primes
random bit generators	Fortuna, Hash_DRBG, HMAC_DRBG, CTR_DRBG
extendable output functions	SHAKE128, SHAKE256, cSHAKE128, cSHAKE256
key encapsulation functions	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 / twisted curves	brainpoolP160r1 through brainpoolP512r1

HALオプション



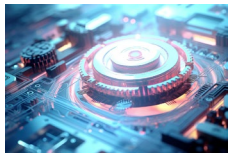
emCrypt ハードウェアアクセラレータ

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



emCrypt ハードウェアアクセラレータ ベンチマーク

NXP Kinetis-CAU

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。

単機能を実現するライブラリ製品

emLib

アプリケーションの目的に合わせて利用可能な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		データ整合性チェック	
emLib AES	emLib DES	emLib CRC	emLib ECC
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	DES（56ビット）ライブラリ、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	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	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。4、8、24、および40ビットのエラー訂正ライブラリ

emCrypt 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。

各機能ごとの必要リソース (Cortex-M3マイコン実装時)

MD5

Setting	Context size	LUT	LUT size	Code size	Total size
0	0.16 KB	Flash	0.3 KB	0.4 KB	0.7 KB
1	0.16 KB	-		2.0 KB	2.0 KB

RIPEMD-160

Setting	Context size	LUT	LUT size	Code size	Total size
0	0.16 KB	Flash	0.3 KB	0.7 KB	1.0 KB
1	0.16 KB	-		4.6 KB	4.6 KB

SHA-1

Setting	Context size	LUT	LUT size	Code size	Total size
0	0.16 KB	Flash		0.6 KB	0.6 KB
1	0.16 KB	-		3.6 KB	3.6 KB

SHA-256

Setting	Context size	LUT	LUT size	Code size	Total size
0	0.17 KB	Flash	0.3 KB	0.5 KB	0.8 KB
1	0.17 KB	-	-	7.7 KB	7.7 KB

SHA-512

Setting	Context size	LUT	LUT size	Code size	Total size
0	0.20 KB	Flash	0.7 KB	1.1 KB	1.8 KB
1	0.20 KB	Flash	0.7 KB	10.3 KB	11.0 KB
2	0.20 KB	Flash	0.1 KB	41.5 KB	41.6 KB

DES

Setting	Context size	LUT	LUT size	Code size	Total size
0	0.38 KB	Flash	2.1 KB	1.3 KB	3.4 KB
1	0.38 KB	Flash	2.1 KB	2.1 KB	4.2 KB
2	0.38 KB	Flash	2.1 KB	5.3 KB	7.4 KB
3	0.38 KB	RAM	2.1 KB	1.3 KB	3.4 KB
4	0.38 KB	RAM	2.1 KB	2.1 KB	4.2 KB
5	0.38 KB	RAM	2.1 KB	5.3 KB	7.4 KB

各機能ごとの必要リソース (Cortex-M3マイコン実装時)

AES

Setting	Context size	LUT	LUT size	Code size	Total size
0	0.24 KB	Flash	2.0	3.2	5.2
1	0.24 KB	Flash	2.0	2.7	4.7
2	0.24 KB	Flash	8.5	2.4	10.9
3	0.24 KB	Flash	1.9	12.5	14.4
4	0.24 KB	RAM	2.0	3.2	5.2
5	0.24 KB	RAM	2.0	2.7	4.7
6	0.24 KB	RAM	8.5	2.4	10.9
7	0.24 KB	RAM	1.9	12.5	14.4

SEED

Setting	Context size	LUT	LUT size	Code size	Total size
0	0.14	Flash	0.5	0.5	1.0
1	0.14	Flash	4.0	0.4	4.4
2	0.14	RAM	0.5	0.5	1.0
3	0.14	RAM	4.0	0.4	4.4

ARIA

Setting	Context size	LUT	LUT size	Code size	Total size
0	0.28	Flash	1.0 KB	1.9 KB	2.9 KB
1	0.28	RAM	1.0 KB	1.9 KB	2.9 KB

CAST

Setting	Context size	LUT	LUT size	Code size	Total size
0	0.10	F lash	8.0 KB	3.5	11.5
1	0.10	RAM	8.0 KB	3.7	11.7

Camelia

Setting	Context size	LUT	LUT size	Code size	Total size
0	0.27 KB	Flash	1.0 KB	28.8 KB	29.8 KB
1	0.27 KB	Flash	4.0 KB	20.7 KB	24.7 KB
2	0.27 KB	RAM	1.0 KB	28.8 KB	29.8 KB
3	0.27 KB	RAM	4.0 KB	20.7 KB	24.7 KB

各機能ごとの必要リソース (Cortex-M3マイコン実装時)

Twofish

Setting	Context size	LUT	LUT size	Code size	Total size
0	0.2	Flash	0.6 KB	3.4	4.0
1	0.2	Flash	4.6	3.1	7.7
2	0.2	Flash	8.5	3.2	11.7
3	0.2	Flash	12.5	2.8	15.3
4	4.2	Flash	0.6	3.4	4.0
5	4.2	Flash	4.6	3.1	7.7
6	4.2	Flash	8.5	3.2	11.7
7	4.2	Flash	12.5	2.8	15.3

Setting	Context size	LUT	LUT size	Code size	Total size
8	0.2	RAM	0.6	3.4	4.0
9	0.2	RAM	4.6	3.1	7.7
10	0.2	RAM	8.5	3.2	11.7
11	0.2	RAM	12.5	2.8	15.3
12	4.2	RAM	0.6	3.4	4.0
13	4.2	RAM	4.6	3.1	7.7
14	4.2	RAM	8.5	3.2	11.7
15	4.2	RAM	12.5	2.8	15.3

Blowfish

Setting	Context size	LUT	LUT size	Code size	Total size
0	4.0 KB	Flash	4.0 KB	0.7 KB	4.7 KB
1	4.0 KB	RAM	4.0 KB	1.1 KB	5.1 KB

各機能・マイコンごとの速度ベンチマーク

AES benchmark

```
(c) 2014-2017 SEGGER Microcontroller GmbH & Co. KG    www.segger.com
AES Benchmark V1.16 compiled Apr 21 2017 16:00:55

Compiler: clang 3.9.1 (tags/RELEASE_391/final)
System:   Processor speed               = 168.000 MHz
Config:   CRYPTO_CONFIG_AES_OPTIMIZE    = 15
Config:   CRYPTO_CONFIG_AES_HW_OPTIMIZE = 1

+--------------+------+----------------+----------------+
|              |      | ECB        MB/s | CBC        MB/s |
| Cipher       | Bits |     Enc     Dec |     Enc     Dec |
+--------------+------+----------------+----------------+
| AES          |  128 |    2.03    2.18 |    1.64    1.61 |
| AES (HW)     |  128 |    8.14    7.70 |    7.52    6.72 |
| AES          |  192 |    1.74    1.88 |    1.44    1.44 |
| AES (HW)     |  192 |    6.83    6.52 |    6.30    5.66 |
| AES          |  256 |    1.53    1.64 |    1.29    1.30 |
| AES (HW)     |  256 |    6.05    5.89 |    5.63    5.00 |
+--------------+------+----------------+----------------+
|              |      | GCM        MB/s | CCM        MB/s |
| Cipher       | Bits |     Enc     Dec |     Enc     Dec |
+--------------+------+----------------+----------------+
| AES          |  128 |    0.05    0.05 |    0.83    0.83 |
| AES (HW)     |  128 |    0.05    0.05 |    1.23    1.24 |
| AES          |  192 |    0.05    0.05 |    0.73    0.73 |
| AES (HW)     |  192 |    0.05    0.05 |    1.16    1.16 |
| AES          |  256 |    0.06    0.06 |    0.65    0.65 |
| AES (HW)     |  256 |    0.06    0.06 |    1.10    1.11 |
+--------------+------+----------------+----------------+

Benchmark complete
```

ECDSA benchmark

```
(c) 2014-2017 SEGGER Microcontroller GmbH & Co. KG    www.segger.com
ECDSA Sign and Verify Benchmark compiled Apr 21 2017 16:03:45

Compiler: clang 3.9.1 (tags/RELEASE_391/final)
System:   Processor speed                   = 168.000 MHz
Config:   Static heap size                  = 4440 bytes
Config:   CRYPTO_MPI_BITS_PER_LIMB          = 32
Config:   CRYPTO_CONFIG_ECDSA_TWIN_MULTIPLY = 1

+-----------------+----------+----------+----------+----------+
|                 |     Sign |     Sign |   Verify |   Verify |
| Curve           |       ms |    bytes |       ms |    bytes |
+-----------------+----------+----------+----------+----------+
| secp192r1       |    40.54 |     1152 |    37.64 |     1920 |
| secp224r1       |    50.85 |     1296 |    48.27 |     2160 |
| secp256r1       |    79.07 |     1440 |    75.86 |     2400 |
| secp384r1       |   129.00 |     2016 |   122.00 |     3360 |
| secp521r1       |   238.67 |     2664 |   218.50 |     4440 |
| brainpoolP160r1 |    68.87 |     1008 |    66.81 |     1680 |
| brainpoolP160t1 |    62.88 |     1008 |    60.50 |     1680 |
| brainpoolP192r1 |    98.67 |     1152 |    90.92 |     1920 |
| brainpoolP192t1 |    89.42 |     1152 |    80.86 |     1920 |
| brainpoolP224r1 |   130.87 |     1296 |   122.40 |     2160 |
| brainpoolP224t1 |   119.50 |     1296 |   111.20 |     2160 |
| brainpoolP256r1 |   171.33 |     1440 |   162.00 |     2400 |
| brainpoolP256t1 |   158.00 |     1440 |   145.62 |     2400 |
| brainpoolP320r1 |   260.75 |     1728 |   242.83 |     2880 |
| brainpoolP320t1 |   241.00 |     1728 |   216.00 |     2880 |
| brainpoolP384r1 |   399.00 |     2016 |   372.00 |     3360 |
| brainpoolP384t1 |   376.25 |     2016 |   327.75 |     3360 |
| brainpoolP512r1 |   754.50 |     2592 |   694.00 |     4320 |
| brainpoolP512t1 |   649.00 |     2592 |   613.50 |     4320 |
+-----------------+----------+----------+----------+----------+

Benchmark complete
```

各機能・マイコンごとの速度ベンチマーク

Modular exponentiation benchmark

```
(c) 2014-2017 SEGGER Microcontroller GmbH & Co. KG    www.segger.com
Modular Exponentiation Benchmark compiled Apr 21 2017 15:54:06

Compiler: clang 3.9.1 (tags/RELEASE_391/final)
System:   Processor speed          = 168.000 MHz
Config:   Static heap size         = 39600 bytes
Config:   CRYPTO_MPI_BITS_PER_LIMB = 32

Modular Arithmetic Performance
==============================

CRT private key, exponent length = modulus length, all times in ms

+--------------------------+--------------+--------------+--------------+
| Algorithm                |          512 |         1024 |         2048 |
+--------------------------+--------------+--------------+--------------+
| Basic, ladder            |   67.87  1.0x |  287.25  1.0x | 1497.00  1.0x |
| Basic, fast              |   50.55  1.3x |  202.80  1.4x |  955.00  1.6x |
| Basic, 2b, FW            |   47.41  1.4x |  192.50  1.5x |  923.50  1.6x |
| Basic, 3b, FW            |   44.35  1.5x |  182.50  1.6x |  909.50  1.6x |
| Basic, 4b, FW            |   43.33  1.6x |  176.17  1.6x |  887.00  1.7x |
| Basic, 5b, FW            |   44.13  1.5x |  174.83  1.6x |  872.00  1.7x |
| Basic, 6b, FW            |   47.41  1.4x |  178.67  1.6x |  865.00  1.7x |
+--------------------------+--------------+--------------+--------------+
| Basic, 2b, RM            |   46.73  1.5x |  189.33  1.5x |  911.00  1.6x |
| Basic, 3b, RM            |   43.87  1.5x |  180.17  1.6x |  889.50  1.7x |
| Basic, 4b, RM            |   42.58  1.6x |  173.67  1.7x |  870.00  1.7x |
| Basic, 5b, RM            |   42.33  1.6x |  171.00  1.7x |  856.50  1.7x |
| Basic, 6b, RM            |   43.38  1.6x |  171.00  1.7x |  847.00  1.8x |
+--------------------------+--------------+--------------+--------------+
| Barrett, ladder          |   53.84  1.3x |  202.00  1.4x | 1021.00  1.5x |
| Barrett, fast            |   40.08  1.7x |  145.14  2.0x |  666.50  2.2x |
| Barrett, 2b, FW          |   38.73  1.8x |  139.12  2.1x |  645.50  2.3x |
| Barrett, 3b, FW          |   35.59  1.9x |  129.00  2.2x |  620.50  2.4x |
| Barrett, 4b, FW          |   34.48  2.0x |  123.78  2.3x |  599.50  2.5x |
| Barrett, 5b, FW          |   35.10  1.9x |  122.56  2.3x |  587.50  2.5x |
| Barrett, 6b, FW          |   37.78  1.8x |  125.50  2.3x |  583.00  2.6x |
+--------------------------+--------------+--------------+--------------+
| Barrett, 2b, RM          |   37.11  1.8x |  133.75  2.1x |  628.00  2.4x |
| Barrett, 3b, RM          |   34.79  2.0x |  126.50  2.3x |  606.00  2.5x |
| Barrett, 4b, RM          |   33.73  2.0x |  121.78  2.4x |  588.50  2.5x |
| Barrett, 5b, RM          |   33.57  2.0x |  119.56  2.4x |  577.50  2.6x |
| Barrett, 6b, RM          |   34.43  2.0x |  119.56  2.4x |  570.50  2.6x |
+--------------------------+--------------+--------------+--------------+
| Montgomery, fast         |   21.17  3.2x |   92.64  3.1x |  486.33  3.1x |
| Montgomery, 2b, FW       |   21.40  3.2x |   93.73  3.1x |  484.67  3.1x |
| Montgomery, 3b, FW       |   19.35  3.5x |   84.17  3.4x |  433.00  3.5x |
| Montgomery, 4b, FW       |   18.61  3.6x |   80.08  3.6x |  409.00  3.7x |
| Montgomery, 5b, FW       |   18.94  3.6x |   79.08  3.6x |  398.67  3.8x |
| Montgomery, 6b, FW       |   20.36  3.3x |   81.15  3.5x |  398.00  3.8x |
+--------------------------+--------------+--------------+--------------+
| Montgomery, 2b, RM       |   19.84  3.4x |   85.50  3.4x |  446.00  3.4x |
| Montgomery, 3b, RM       |   18.65  3.6x |   81.08  3.5x |  419.00  3.6x |
| Montgomery, 4b, RM       |   18.14  3.7x |   78.23  3.7x |  401.33  3.7x |
| Montgomery, 5b, RM       |   18.07  3.8x |   76.92  3.7x |  392.67  3.8x |
| Montgomery, 6b, RM       |   18.59  3.7x |   77.08  3.7x |  387.00  3.9x |
+--------------------------+--------------+--------------+--------------+

Public key, exponent length = 17 bits, all times in ms

+--------------------------+--------------+--------------+--------------+
| Algorithm                |          512 |         1024 |         2048 |
+--------------------------+--------------+--------------+--------------+
| Basic, ladder            |    4.38  1.0x |    9.62  1.0x |   25.77  1.0x |
| Basic, fast              |    2.23  2.0x |    4.68  2.1x |   12.14  2.1x |
| Basic, 2b, FW            |    2.41  1.8x |    4.87  2.0x |   12.42  2.1x |
| Basic, 3b, FW            |    2.62  1.7x |    5.00  1.9x |   12.44  2.1x |
| Basic, 4b, FW            |    3.14  1.4x |    5.67  1.7x |   13.09  2.0x |
| Basic, 5b, FW            |    4.17  1.1x |    6.99  1.4x |   15.07  1.7x |
| Basic, 6b, FW            |    5.88  0.7x |    9.18  1.0x |   18.70  1.4x |
+--------------------------+--------------+--------------+--------------+
| Basic, 2b, RM            |    2.29  1.9x |    4.73  2.0x |   12.20  2.1x |
| Basic, 3b, RM            |    2.52  1.7x |    4.87  2.0x |   12.27  2.1x |
| Basic, 4b, RM            |    2.99  1.5x |    5.48  1.8x |   12.82  2.0x |
| Basic, 5b, RM            |    3.89  1.1x |    6.66  1.4x |   14.64  1.8x |
| Basic, 6b, RM            |    5.69  0.8x |    9.02  1.1x |   18.22  1.4x |
+--------------------------+--------------+--------------+--------------+
| Barrett, ladder          |    3.46  1.3x |    7.83  1.2x |   22.22  1.2x |
| Barrett, fast            |    1.78  2.5x |    3.82  2.5x |   10.42  2.5x |
| Barrett, 2b, FW          |    2.15  2.0x |    4.24  2.3x |   11.02  2.3x |
| Barrett, 3b, FW          |    2.32  1.9x |    4.38  2.2x |   11.00  2.3x |
| Barrett, 4b, FW          |    2.87  1.5x |    5.23  1.8x |   11.95  2.2x |
| Barrett, 5b, FW          |    3.96  1.1x |    6.91  1.4x |   14.85  1.7x |
| Barrett, 6b, FW          |    5.93  0.7x |    9.96  1.0x |   20.34  1.3x |
+--------------------------+--------------+--------------+--------------+
| Barrett, 2b, RM          |    1.88  2.3x |    3.89  2.5x |   10.50  2.5x |
| Barrett, 3b, RM          |    2.06  2.1x |    4.07  2.4x |   10.60  2.4x |
| Barrett, 4b, RM          |    2.45  1.8x |    4.69  2.0x |   11.31  2.3x |
| Barrett, 5b, RM          |    3.18  1.4x |    5.90  1.6x |   13.44  1.9x |
| Barrett, 6b, RM          |    4.63  0.9x |    8.30  1.2x |   17.70  1.5x |
+--------------------------+--------------+--------------+--------------+
| Montgomery, fast         |    1.41  3.1x |    3.37  2.9x |    9.98  2.6x |
| Montgomery, 2b, FW       |    2.06  2.1x |    5.12  1.9x |   15.38  1.7x |
| Montgomery, 3b, FW       |    2.13  2.1x |    5.29  1.8x |   15.89  1.6x |
| Montgomery, 4b, FW       |    2.69  1.6x |    6.77  1.4x |   20.34  1.3x |
| Montgomery, 5b, FW       |    3.61  1.2x |    9.20  1.0x |   27.73  0.9x |
| Montgomery, 6b, FW       |    5.41  0.8x |   13.97  0.7x |   42.13  0.6x |
+--------------------------+--------------+--------------+--------------+
| Montgomery, 2b, RM       |    1.60  2.7x |    3.87  2.5x |   11.47  2.2x |
| Montgomery, 3b, RM       |    1.72  2.5x |    4.19  2.3x |   12.46  2.1x |
| Montgomery, 4b, RM       |    2.09  2.1x |    5.14  1.9x |   15.43  1.7x |
| Montgomery, 5b, RM       |    2.58  1.7x |    6.41  1.5x |   19.40  1.3x |
| Montgomery, 6b, RM       |    3.48  1.3x |    8.66  1.1x |   26.37  1.0x |
+--------------------------+--------------+--------------+--------------+

Benchmark complete
```

SEGGER社Wikiページでデータ提供
https://wiki.segger.com/emCrypt

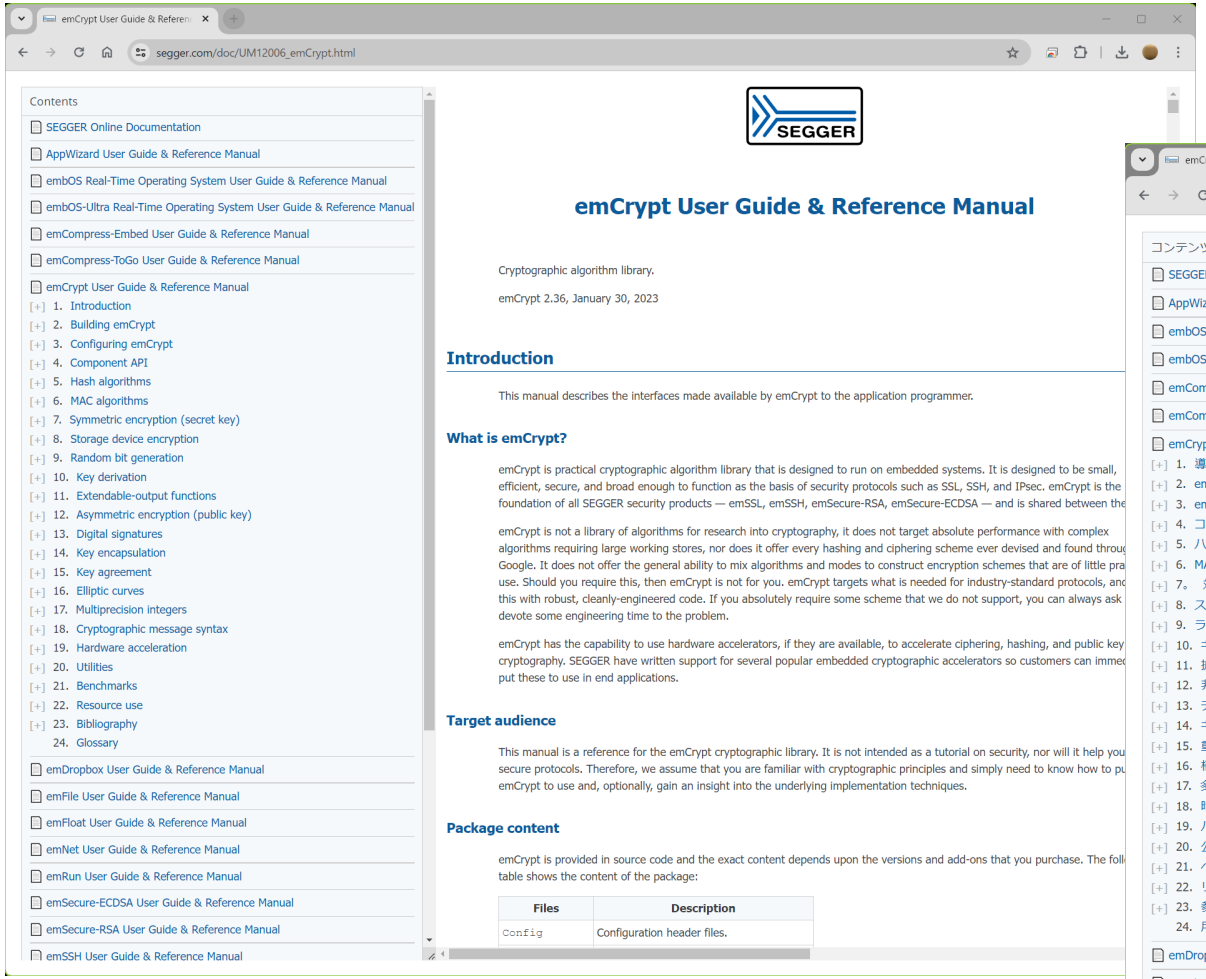
emCrypt 開発・導入支援

- 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

emCrypt – 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

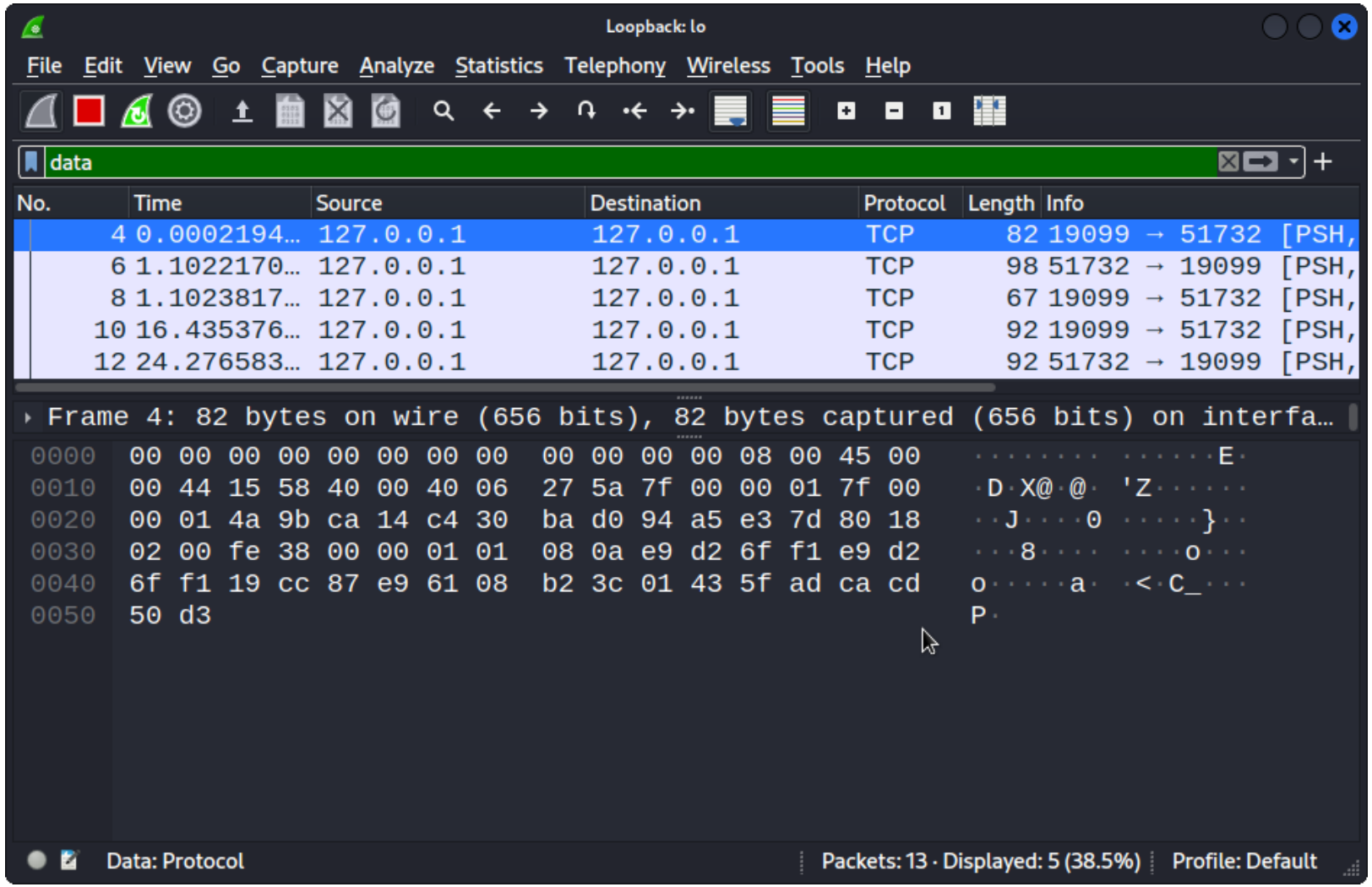


https://www.segger.com/doc/UM12006_emCrypt.html

ブラウザの翻訳機能で日本語表示可能

Google Chrome推奨

emCryptライブラリを使った「End-to-End 暗号化通信」



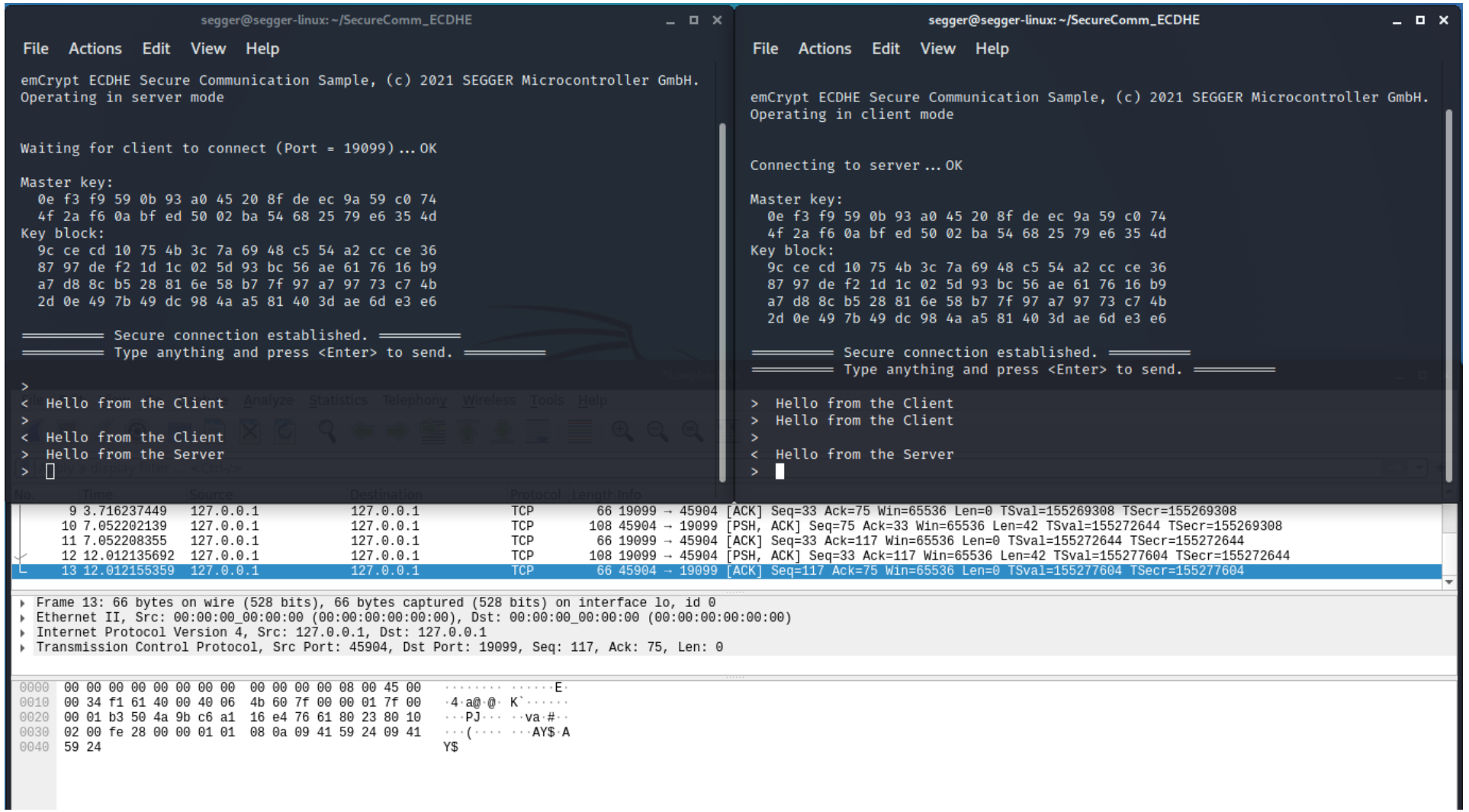
「emCrypt」を利用することで、SEGGER暗号ライブラリをユーザアプリケーションから直接利用し、独自の暗号処理を実現することができます。

SEGGER社サンプルアプリケーション「End-to-End 暗号化通信」

2 つのクライアント間で、End-to-End暗号化通信を簡単に有効にする方法を示します。このサンプルは、300行未満のコードで構成される、認証および暗号化された通信のリファレンスです。

https://www.segger.com/downloads/emcrypt/

emCryptライブラリを使った「ECDHE鍵交換」

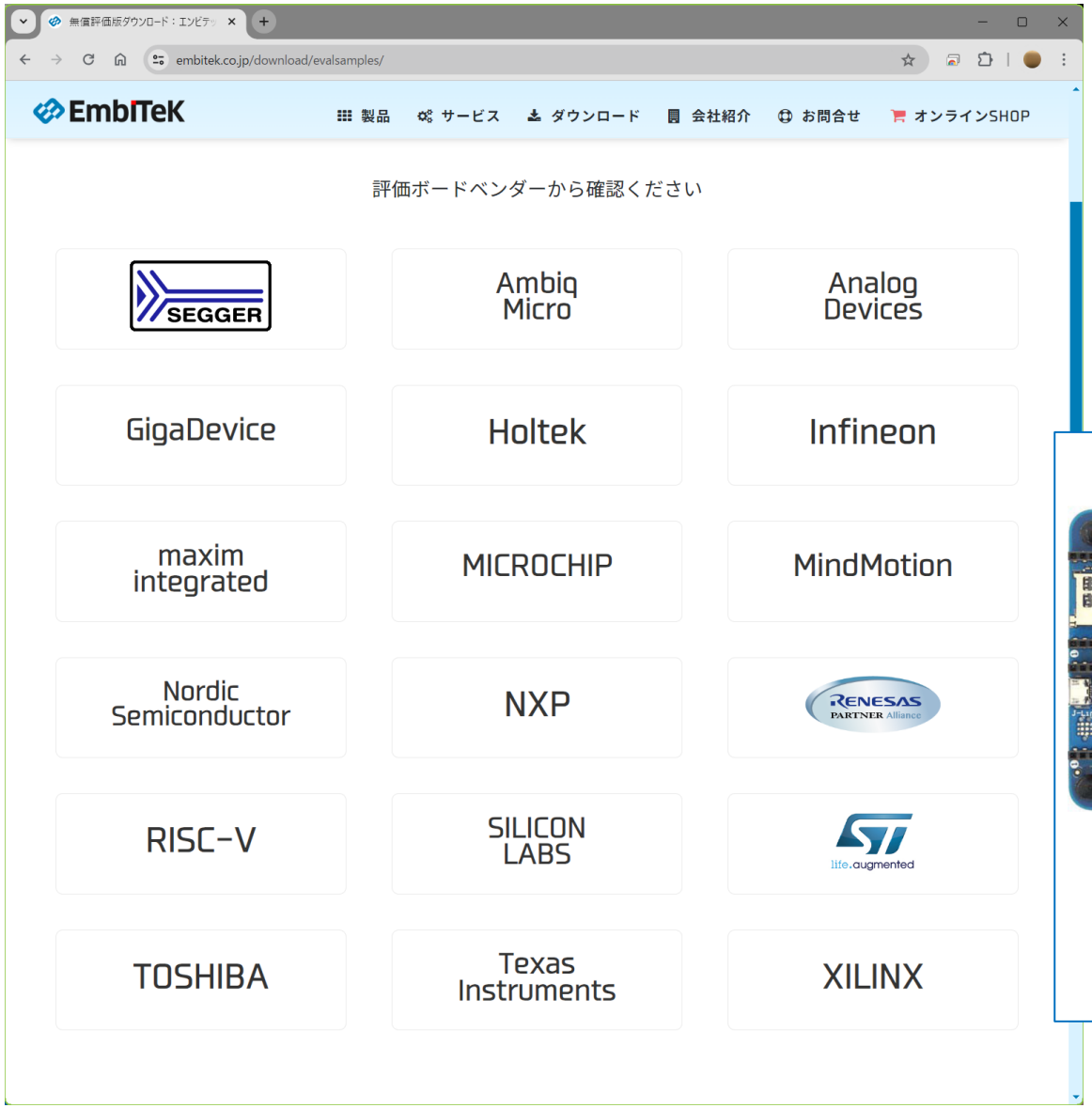



```
/*********************************************************************
*
*       Local types
*
**********************************************************************
*/
//
// KeyBlock[0]: Client Tx Stream Cipher / Server Rx Stream Cipher
// KeyBlock[1]: Client Tx Counter/IV    / Server Rx Counter/IV
// KeyBlock[2]: Client Rx Stream Cipher / Server Tx Stream Cipher
// KeyBlock[3]: Client Rx Counter/IV    / Server Tx Counter/IV
//
typedef struct {
  U8                  aMasterKey[MASTER_KEY_LEN];
  U8                  aKeyBlock[CRYPTO_AES128_KEY_SIZE * 4];
  struct {
    CRYPTO_AES_CONTEXT  Context;
    U8*                 pIV;
  } Rx;
  struct {
    CRYPTO_AES_CONTEXT  Context;
    U8*                 pIV;
  } Tx;
} SESSION_CONTEXT;

typedef struct {
  SYS_SOCKET_HANDLE   hSock;
  SESSION_CONTEXT*    pSession;
} THREAD_INFO;

/*********************************************************************
*
*       Static data
*
```

サンプルソースコード

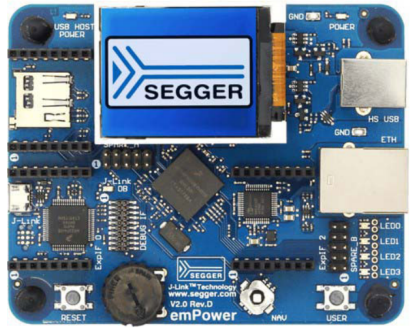
https://www.segger.com/products/security-iot/emcrypt/examples/ecdhe-key-agreement/

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）

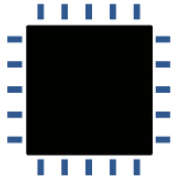
https://www.embitek.co.jp/download/evalsamples/

emCrypt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

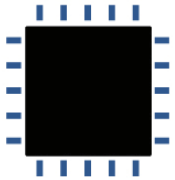
開発プロジェクトは無制限／開発者人数に応じたライセンス

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。

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

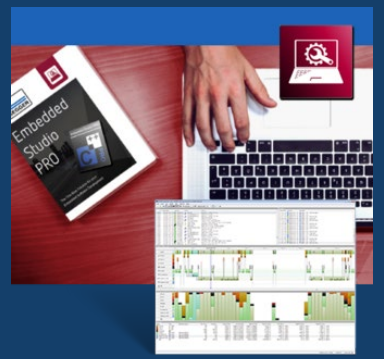
SEGGER Microcontroller GmbH

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

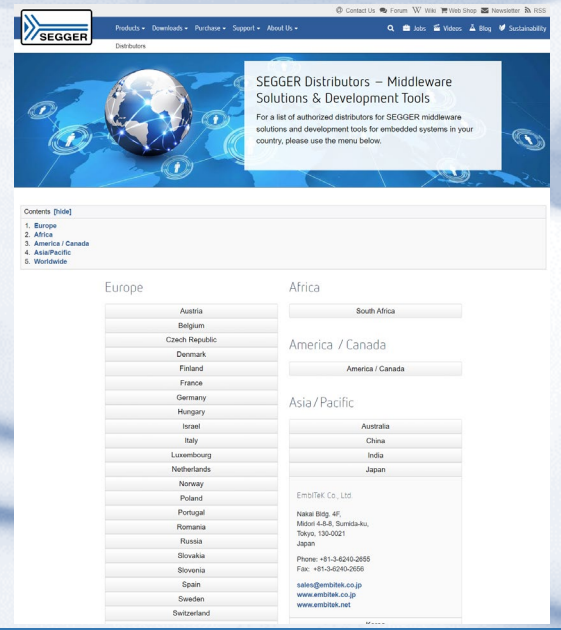
デバッグツール

書込みツール

EmbiTeK

EmbiTeK

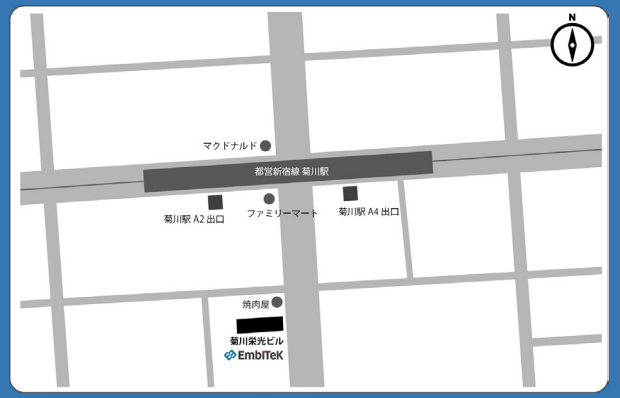
株式会社エンビテック



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

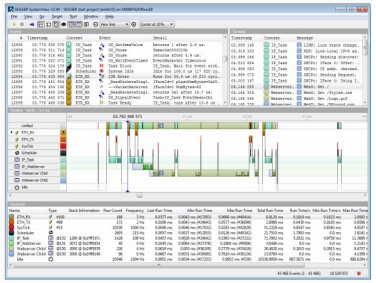
RTOS

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