# 頼れる SSL/TLS ライブラリ wolfSSL

組込みセキュリティ専門ベンダーによる軽量 C 言語ライブラリ

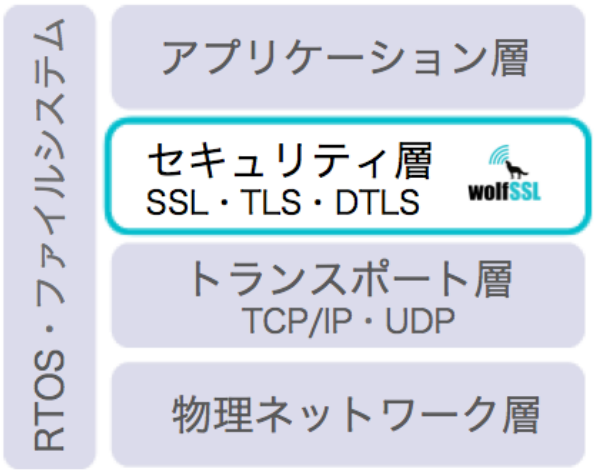
## 組込みネットワークのセキュリティをご検討ですか？

wolfSSL は、マイコン組込みシステム向けに開発された C 言語ベースの軽量 SSL/TLS ライブラリです。SSL/TLS 層のほぼ全機能を実現しながら、ROM サイズ 20～128kB と OpenSSL の 1/20 以下の小型化を実現しています。

セキュリティ専門ベンダーの製品として、TLS1.2、DTLS1.2 などの最新プロトコル標準はもちろん、最新 TLS1.3 の暗号アルゴリズムにも対応し、世界中の組込み製品で利用されています。

## 既存ネットワーク製品へのセキュリティ機能の追加をご検討ですか？

wolfSSL の標準 API は特定の MPU や OS に依存しない柔軟な適応性を実現しています。OS/非 OS を問わず、既存の TCP/IP ベースシステムに、無理なく各種セキュリティ機能が追加可能です。また、分野固有のプロトコルのセキュリティ対応などのために、暗号化アルゴリズムライブラリである wolfCrypt だけをご利用いただくことも可能です。

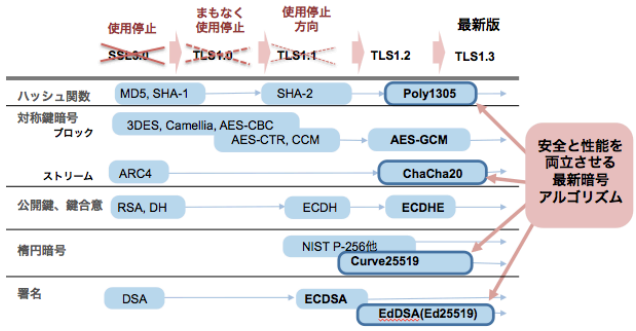



## 購入前に充分な検討、評価が必要ですか？

wolfSSL はデュアルライセンス型のオープンソース製品です。製品検討段階での社内のご評価などに全機能が無償でご利用可能です。ぜひ弊社サイトからご自由にダウンロードいただき、充分ご評価ください。

## 進化する TLS を先取り

リアルな世界に直結する IoT システム。安全への要求は厳しくなる一方です。wolfSSL は進化する TLS とともに常に新しい暗号アルゴリズムを業界に先駆けて実装。安全と性能の両立を実現します。




## 商用ライセンスの条件は？

wolfSSL の商用ライセンスは製品単位のシンプルなロイヤルティフリーライセンスです。適用範囲に応じて製品ライン、もしくは製品ファミリーのライセンスをご用意しています。

## OpenSSL からの移行をご検討ですか？

wolfSSL の OpenSSL 互換 API をご利用ください。使用頻度の高い API を厳選することで、wolfSSL のシンプルさを失うことなく互換性を提供します。移行サポート、サービスについてもお問い合わせください。

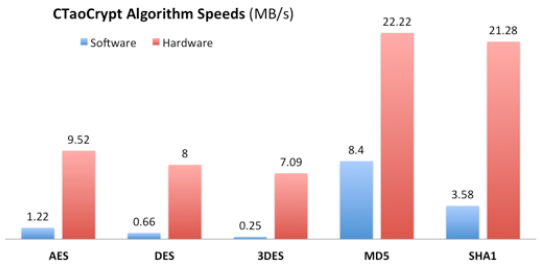

**wolfSSL Japan 合同会社 (ウルフエスエスエル)**

〒108-6028 東京都港区港南 2-15-1 品川インターシティ A 棟 28 階

E メール: info@wolfssl.jp　ウェブサイト: wolfssl.jp

## さらに高い性能が必要ですか？

wolfSSL はハードウェア暗号化アクセラレータのサポートでさらなる高性能を実現します。イメージデータなど大規模な暗号化データの転送に威力を発揮します。




## 製品向けカスタマイズが必要ですか？

組込みシステムでは応用分野固有の機能要求がつきものです。標準パッケージの特定製品へのカスタマイズなど各種ご要望がありましたらぜひご相談ください。経験豊富なエンジニアによるプロフェッショナルサービスも提供しています。

## wolfSSL 製品情報

**SSL/TLS 機能:**

- サーバーおよびクライアント機能
- SSL ver 3.0、 TLS ver 1.0, 1.1, 1.2, 1.3 、DTLS1.0 および 1.2
- OpenSSL 互換 API
- RSA 鍵生成。OCSP および CRL サポート
- クライアント認証。X.509 v3 証明書生成

**アルゴリズム・サポート:**

- ハッシュ: MD5, SHA-1, SHA-2 (SHA-256, SHA-384, SHA512), Poly1305
- 共通鍵: Camellia, 3DES, AES (CBC, CTR, CCM, GCM), ARC4, RABBIT, HC-128, ChaCha20
- 公開鍵, 鍵合意: RSA, DH, DHE, ECDH, ECDHE,
- 楕円暗号化: NIST P-256, Curve25519 他
- パスワード: HMAC, PBKDF2, PKCS#5
- 署名: DSA, ECDSA, EdDSA(Ed25519)

**OS サポート:**

- Win32/64, Linux, Mac OS X, Solaris, ThreadX, VxWorks, FreeBSD, NetBSD, OpenBSD,
- 各種組込み Linux, WinCE, Haiku, OpenWRT, iPhone (iOS), Android, Nintendo Wii および
- Gamecube through DevKitPro, QNX, MontaVista, OpenCL, NonStop, µITRON, µTKernel,
- Micrium µC/OS, FreeRTOS, SafeRTOS, Freescale MQX, Nucleus, TinyOS, HP/UX

**FIPS140-2: 認証#2425、#3389**

FIPS140-2 は暗号モジュールに関するセキュリティの仕様を規定する米国連邦標準規格です。wolfSSL の暗号化モジュール、FIPS 版 wolfCrypt は最新の FIPS140-2 を取得（認証番号#2425、#3389）しています（通常版とは別製品となります）。認証取得サポート、サービスについてもお問い合わせください。

**その他のライブラリ:**

- wolfCrypt: wolfSSL に含まれる各種暗号化アルゴリズムをライブラリ化
- wolfMQTT: MQTT5.0 準拠の MQTT クライアントライブラリ。wolfSSL と共に使用
- wolfSSH: SSH サーバー機能を組込み向けに提供するライブラリ

## wolfSSL 社について

wolfSSL は 2004 年創立。米国ワシントン州に本社を置く組込みセキュリティの専門ベンダーです。社名の「ウルフ」は強固なセキュリティ、また離れた仲間同士のコミュニケーションを大切にするオープンソースコミュニティーも象徴しています。

ご質問、お問い合わせは info@wolfssl.jp までお気軽にご連絡ください。

**wolfSSL Japan 合同会社 (ウルフエスエスエル)**
〒108-6028 東京都港区港南 2-15-1 品川インターシティ A 棟 28 階
E メール: info@wolfssl.jp　ウェブサイト: wolfssl.jp