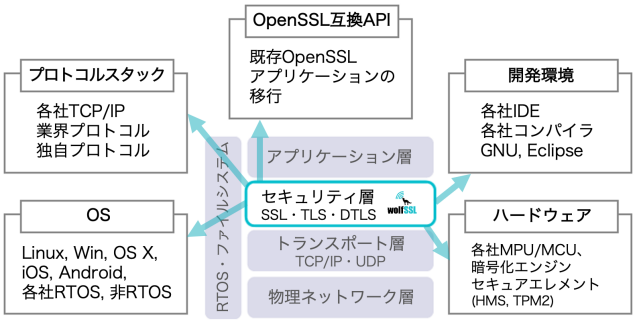
組み込みシステム向けSSL/TLSライブラリwolfSSL

製品組み込みのセキュリティをご検討ですか？

wolfSSLは、製品組み込み向けに開発した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最新プロトコル標準に対応し、世界中の組み込み製品で利用されています。

既存製品にセキュリティプロトコルを

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、無理なくセキュリティプロトコルの追加が可能です。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。



進化するTLSを先取り

リアルな世界に直結するIoTに対する安全への要求は厳しくなる一方です。wolfSSLは進化するTLSと共に常に新しい暗号アルゴリズムを実装。また、業界に先駆けて**TLS1.3**や**DTLS1.3**など最新のプロトコル仕様に準拠する製品を提供しています。

OpenSSLからの移行を支援

これまでの開発資源を無駄にしないよう、wolfSSLにはOpenSSL互換APIを用意しています。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。

さらに高い性能を目指して

TLSプロトコル処理で課題となる公開鍵暗号処理に、wolfSSL独自の最適化 (Single Precision 最適化) 機能を提供。従来型に比べ一桁早い処理速度 (弊社比) を実現しました。また、各社MCUのハードウェア暗号アクセラレータへの対応でさらなる高性能を実現。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。2024年8月に承認された3つの耐量子暗号アルゴリズムもサポートしています。

ライセンスモデル

wolfSSLはオープンソースと商用ライセンスの２つのライセンスを用意しています。オープンソース版は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ダウンロードしていただき、充分なご評価にお役立てください。

商用ライセンスは、製品単位のシンプルなワンタイムのライセンスです。適用範囲に応じてPoC限定のエントリーライセンス、製品ライン、製品ファミリーの３段階を用意しています。長期安定した商用サポートとともに安心してお客様の製品に組み込んでいただけます。

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

wolfSSL製品情報

SSL/TLS機能:

- サーバーおよびクライアント機能
- TLS 1.2, 1.3 のフル機能サポート
  (保守：SSL ver 3.0、TLS ver 1.0, 1.1)
- DTLS 1.2, 1.3のフル機能サポート（保守DTLS1.0）
- OpenSSL互換API
- X.509 v3証明書生成、管理
- コンフィグレーション機能による不要機能の削除

アルゴリズム・サポート:

- ハッシュ：SHA-2 (SHA-256, SHA-384, SHA512), SHA-3, Poly1305, (保守：MD2/5, SHA-1など)
- 共通鍵：Camellia, AES (CBC, CTR, CCM, GCM, OFB), ChaCha20, (保守：3DES, ARC4, RABBIT, HC-128など)
- 公開鍵, 鍵合意：RSA, DH, DHE, ECDH, ECDHE
- 楕円暗号：NIST P-256他, Curve25519/448, Blainpool
- メッセージ認証：HMAC, CMAC,
- パスワード：PBKDF2, PKCS#5
- 署名：ECDSA, EdDSA(Ed25519/448), (保守：DSA)
- 耐量子暗号：ML-KEM(CRYSTALS-Kyber)、ML-DSA (CRYSTALS-Dilithium)、SLH-DSA(SPHINCS+)

OSサポート:

- 汎用OS：各種Linuxディストリビューション, Windows, macOS, HP/UX, Solaris, FreeBSD, NetBSD, OpenBSD, AIX
- 携帯/端末/ゲーム機器用OS：iOS. Android, WinCE, Nintendo Wii and Gamecube with DevKitPro
- 組み込みLinux：MontaVista, NonStop, QNX, OpenWrt, PetaLinux
- リアルタイムOS：Apache Mynewt, Azure Sphere OS, CMSIS-RTOS, Does, embOS, FreeRTOS, SafeRTOS, GreenHills INTEGRITY, Keli RTX, Micrium, MQX, Nucleus RTOS, PikeOS, RIOT, TinyOS, TI-RTOS, ThreadX, TOPPERS/ASP, VxWorks, Zephyr, μITRON（各社）

サポートチップメーカー

ARM、Intel、Motorola、mbed、NXP/Freescale、Microchip (PIC32)/Atmel、STMicroelectronics (STM32)、Analog Devices、Texas Instruments、Xilinx SoCs/FPGA、Renesas、Espressif
上記以外での使用またはテストのご希望がありましたらお問い合わせください。

第三者認証製品と取得サービス

wolfSSLに含まれる各種暗号化アルゴリズムをライブラリ化したwolfCryptは、通常版とは別に各種認証製品、サービスを提供しています。

FIPS認証

FIPS140-3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の中核を担うwolfCryptはFIPS140-2の認証取得に多くの経験があり、最新の140-3認証も取得しています（2024年7月）。

DO-178C認証

wolfCryptは航空機搭載ソフトウェア向けのガイドラインDO-178Cに対応しています。

関連ライブラリ製品:

- 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：MQTT v3.1/5.0準拠のMQTTクライアントライブラリ。wolfSSLと共に使用
- wolfSSH：SSHサーバー機能を組み込み向けに提供するライブラリ
- cURL/libcurl/tiny-cURL：https, smtps他各種クライアントプロトコルコマンドと製品組み込み向けライブラリ
- wolfBoot：安全なファームウェア更新ライブラリ
- wolfSentry：製品組み込み型不正侵入検知、防止ソフトウェア

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