組み込みシステム用に暗号ライブラリ、SSL/TLSをお探しですか？

wolfSSLがそのご要望にお応えできるかも知れません。

ネットワークセキュリティの専門ベンダーであるwolfSSLは、組み込みシステム向けに特化したソフトウェアライブラリの開発、販売、およびサポートを行っています。国内外の航空宇宙、車載、医療を含む高い信頼性を求める分野のOEMカスタマーがwolfSSL製品を使用し、セキュア通信、ストレージ内データの暗号化、ファームウェア更新などを実現しています。

セキュア通信には

ウルフエスエスエル

wolfSSL

処理スピードやメモリーなど、リソースに制限がある組み込みシステムやITRONなどのRTOS、また非RTOS向けに、C言語で開発した小型のTLS/SSLライブラリです。

TLS1.3とDTLS1.3までをサポートし、SFTP、SCP、MQTT、またハードウェア暗号やTPM、HSMにも対応可能です。

暗号化には

ウルフクリプト

wolfCrypt

C言語によるポータビリティ性の高い軽量暗号ライブラリです。ストレージ暗号化や安全なドキュメント交換、また署名検証用に特定のアルゴリズムに絞った使用も可能です。

米国FIPS 140-2認証取得済みで、FIPS 140-3認証は現在承認待ちです。航空宇宙ではRTCA DO-178CレベルA認証をサポートしています。

ファームウェア更新には

ウルフブート

wolfBoot

OS非依存の安全なブートローダーソリューションです。ファームウェアの改ざん、デバイスの不正制御、データの不正取得などの攻撃からデバイスを保護します。

セキュアなプロトコルと組み合わせることで、OTA（Over the Air）などのファームウェアアップデートも実現可能です。

wolfSSL Inc.について

米国ワシントン州に本社を持つwolfSSL Inc.は、社名と同名のSSL/TLSライブラリであるwolfSSLを主力製品とし、自社の専門エンジニアが開発、サポート、コンサルティングを行っています。2004年の創業以来、世界各国で2,000社を超えるOEMカスタマーに選ばれています。

wolfSSLのソフトウェアは、オープンソースと商用の2つのライセンスモデルで提供しています。オープンソース版は、商用ライセンスご契約前の十分な評価、検討にご利用いただけます。また商用ライセンスご契約後は、wolfSSL Japanサポートセンターの専任エンジニアが、長期間の安定した技術サポートを提供いたします。

wolfSSL Japan合同会社

info@wolfssl.jp

〒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

詳しくはウェブサイトをご覧ください。

https://wolfssl.jp

wolfSSL製品体系

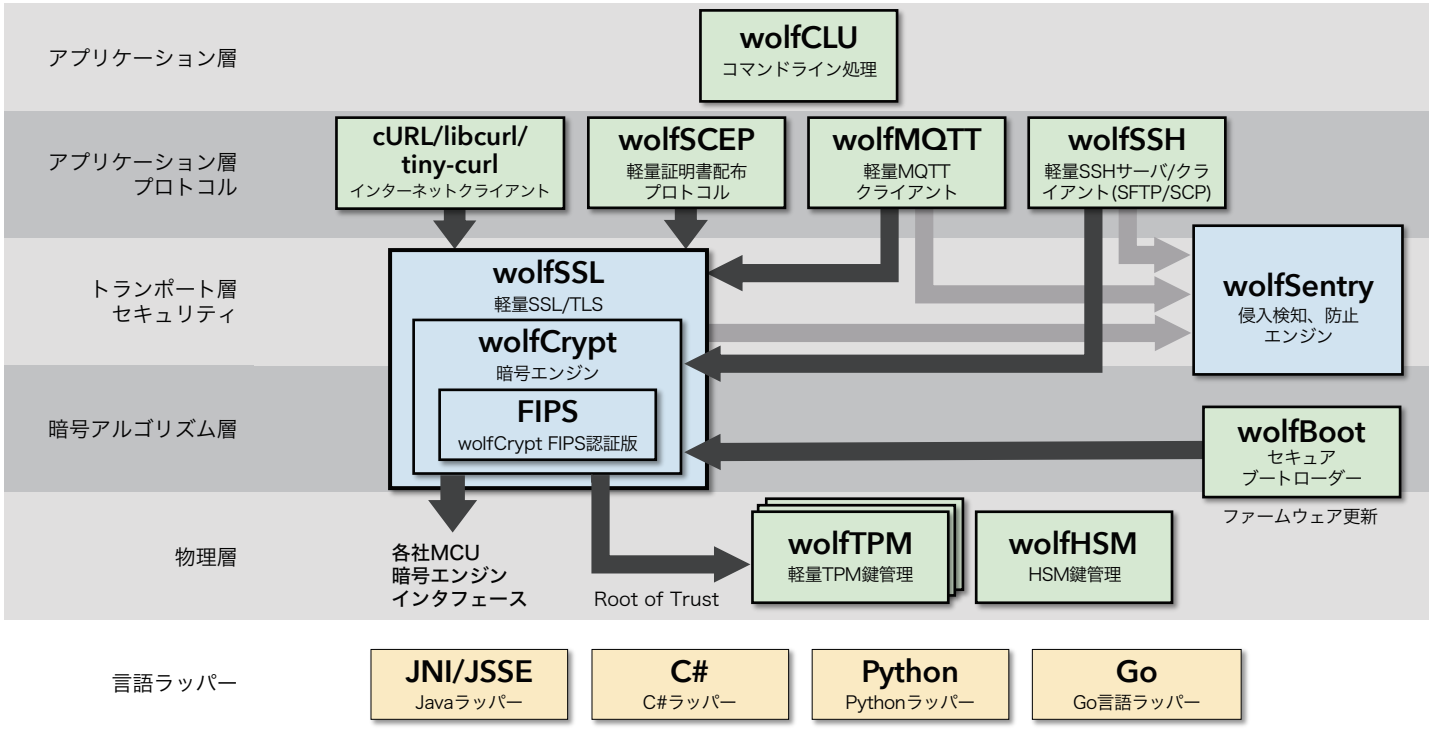
製品組込み向けセキュリティプロトコル・ライブラリ

wolfSSLは、お客様の製品への組み込みにフォーカスした、インターネット標準準拠のセキュリティプロトコル・ライブラリです。オープンソースながら、自社のセキュリティ、暗号技術、ネットワークプロトコル、組み込みシステムの専門エンジニアによる徹底した自社開発、品質保証にこだわりぬいた製品を、商用ライセンス、商用サポートとのセットで長期安定的に提供します。wolfSSLの製品は、世界で2,000社以上に採用され、日本でも業界を代表する各社の製品でご利用いただいています。

セキュリティ専門ベンダーの製品として、プロトコルレイヤーではTLS1.3、DTLS1.3など最新のプロトコルバージョンに対応。暗号レイヤーでは耐量子アルゴリズムなどを含む最新の暗号アルゴリズムを早期にサポートし、FIPS、DO178Cなど第三者による認証取得もサポートします。

製品コアはすべて一旦C言語だけで動作するように記述した上で各MCU/MPUアーキテクチャ、暗号エンジン、セキュアエレメントなどに対応した最適化を行っています。これにより、ほぼすべての商用アーキテクチャをサポートし幅広いプラットフォームへの適応と最高の性能を両立しています。各標準をほぼフルスペックでサポートする一方で、製品組込みを強く意識し、お客様の製品に必要な機能だけに絞り込んだ軽量、コンパクトなコンフィグレーションも可能です。

wolfSSL製品関連図



wolfSSLの製品

wolfSSL

TLSレイヤーだけにフォーカスし、TLS1.3やDTLS1.3など業界標準プロトコルにいち早く対応。ほぼすべてのTCPレイヤー製品、汎用OS、RTOS、非RTOS環境をサポート。コンフィグレーション機能により、必要機能だけに絞り込んで製品組込み向けとして最小のフットプリントサイズを実現することができます。

wolfCrypt

軽量暗号ライブラリ。wolfSSL/wolfSSHなどと連携する一方、カスタムプロトコル開発、データ保護などの基盤ライブラリとしても利用できます。インターネットプロトコルに必要とされる標準アルゴリズムに加えて、ChaCha/Poly、Curve/Ed25519/448、耐量子暗号など最新の暗号アルゴリズムを提供。各社暗号エンジン、HSM、セキュアエレメントなどをサポートします。

wolfCrypt FIPS DO-178C

wolfCryptをベースとした米国の連邦情報処理規格FIPS140-3取得向けの暗号ライブラリ。TLS1.3、SSH v2などで必要とされる暗号アルゴリズム、スキームに対して、迅速な認証取得をサポートします。また、航空機向けにはDO-178C取得に必要なトレーサビリティを提供します。

wolfBoot

安全なファームウェアアップデートに必要となる公開鍵署名、検証、イメージの更新処理などをコンパクトにまとめて提供。最小化されたハードウェア依存部であらゆるMCUアーキテクチャへ容易に対応。既存のブートローダーに組み込むことができます。

wolfTPM

TPM 2.0に準拠したデバイスインタフェースを、統一されたIOコールバックを提供。外部依存がなくリソース使用量が少ないコンパクトなコードにより高い移植性を実現します。

wolfHSM

HSM(ハードウェアセキュリティモジュール)はセキュリティの核となる暗号処理を物理的に独立したプロセッサに隔離し、暗号鍵と暗号処理の堅牢性を飛躍的に向上させる技術です。このHSMの適用を容易にするセキュリティフレームワークです。HSM機能をサポートする各社マイコンの上で動作します。

wolfMQTT

MQTT v 3.1.1/5.0対応のPub/Sub型のクライアントライブラリ。wolfSSLライブラリと連携しMQTTSを提供。各社クラウドサービスによるブローカとのインターオペラビリティを保証。MQTT-SN対応。

wolfSSH

組み込み機器にモニター機能、コンソール機能、ファイル/データ転送機能などを追加します。wolfCryptと連携してSSHv2サーバー、クライアントの両方をサポート。SFTP、SCPなどの関連プロトコルも提供します。

wolfSentry

製品組み込み向け IDPS (侵入検知および防止システム)。動的なルール定義を埋め込み可能なファイヤーウォールエンジン。wolfSSL、wolfMQTT、wolfSSH、アプリケーションなどと連携しネットワークイベントを検出。お客様の製品に侵入検知、防止機能を容易に追加することができます。

cURL/libcurl tiny-curl

インターネット開発や運用のさまざまな局面で利用されるcURL/libcurlの商用サポート。tiny-curlはcURLとのAPI互換性を保ちながら、製品組み込み向けにサポートプロトコルを絞り込み軽量化を実現したコンパクトバージョンのcURLです。

wolfSSL会社概要

wolfSSL Inc. は、米国ワシントン州に本社を持つネットワークセキュリティ専門ベンダーです。スピード、サイズ、移植性、機能、標準への準拠にこだわったセキュリティプロトコルライブラリを、自社の専門エンジニアが独自開発し製品として提供しています。また、製品の技術サポート、コンサルティングも行っています。

第三者認証の取得サービスでは、米国連邦標準規格FIPS認証で多くの経験と実績を持ちます。また、航空宇宙分野ではRTCA DO-178CレベルA認証をサポートします。

2004年の創業以来国内外の航空宇宙、車載、医療を含む、製品への高い信頼性と安定した長期サポートが求められる分野で2,000社を超えるOEMカスタマーに採用されています。日本でも、それぞれの業界トップクラスの企業様の製品に組み込まれご使用いただいています。

wolfSSL Japan合同会社の技術サポートセンターでは、日本人専任スタッフによるサポートサービス、カスタマイズサービスなどを提供しています。

wolfSSL会社情報

wolfSSL Inc.	本社所在地：Edmonds Way, Suite C-300, Edmonds, WA 98020 USA 代表者：Larry Stefonic 設立：2004
wolfSSL Japan 合同会社	本社所在地：〒108-6028 東京都港区港南2-15-1 品川インターシティーA棟28F 代表者：須賀 葉子 設立：2018年
事業内容	ネットワークセキュリティと関連ソフトウェアの開発、提供、サポート
ビジネスモデル	商用ライセンスのほか、商用ライセンス契約前の評価用オープンソース版を提供しています。 契約前のお客様はオープンソース版で社内評価、技術検討を十分行った上で商用ライセンス契約への切り替えが可能です。商用ソフトウェアライセンス、コンサルティング、サポートによる収益を柱としたビジネスモデルで、高い専門性を持つ技術者による長期安定した製品およびテクノロジーの開発を実現しています。

wolfSSL Japan合同会社 (ウルフエスエスエル)
Eメール: info@wolfssl.jp　ウェブサイト: wolfssl.jp