wolfSSLの耐量子暗号サポート

世界で初めて CNSA 2.0 に準拠した商用版

概要

量子コンピューティングの実用化が迫り、セキュリティの脅威が現実的なものとなりつつあります。HNDL攻撃(Harvest Now, Decrypt Later)の観点からも、さらに前からの対策が重要です。この脅威に対応するために、米CNSAで2030年に向けた新しいロードマップ(CNSA2.0)が策定されています。2024年8月には米NISTからはそのための耐量子暗号(PQC)アルゴリズムの標準がドラフトから正式版となったことで、こうした脅威への現実的な対応が可能となってきています。

wolfSSLは、耐量子暗号のサポートに早くから力を注ぎ、自社開発のアルゴリズム実装を実現。世界で最初の商用組み込み向けに利用できるPQC対応の暗号ライブラリとして提供を開始しました。wolfSSLのアルゴリズム実装は、幅広い耐量子暗号のニーズとの互換性を確保し、さまざまなプラットフォームで量子コンピュータの脅威に対する堅牢な保護を提供します。移植性に優れ、ベアメタル環境や幅広い汎用OS、RTOSで動作し、フットプリントが最小限であるため組み込みシステムに適しています。

wolfSSL製品のPQC

wolfSSLは商用セキュリティライブラリとして世界で初めてCNSA 2.0に準拠した、安全な鍵カプセル化のためのML-KEM (Kyber)、デジタル署名のためのML-DSA(Dilithium)などの耐量子暗号アルゴリズムを包括的に提供し、堅牢な耐量子の鍵交換と認証を実現しています。また、CNSA 2.0およびFIPS 140-3準拠の楕円曲線P521とKYBER_LEVEL5などのハイブリッドアルゴリズムをサポートします。

セキュアプロトコル

先に挙げた最先端の耐量子アルゴリズムはコアの暗号化ライブラリwolfCryptにて提供しています。wolfSSLを始めセキュアプロトコル製品はwolfCryptと完全に統合し、PQC対応のTLS 1.3、DTLS1.3、SSH 2.0、 MQTTv3/5、MQTT-SNなどの主要なインターネットプロトコルを提供します。ハイブリッド鍵交換についても、IETFやNISTの検討状況に従ってX25519やP256などの楕円曲線暗号との組み合わせを提供しています。

ファームウェア更新

wolfSSLはさらに、IETFのRFCとして標準化されているLMS(Leighton-Micali Signature)、XMSS(eXtended Merkle Signature Scheme)などのハッシュベースの署名スキームをサポートし、ステートフルの署名オプションを提供します。これらはwolfBoot, wolfHSMと統合して、PQC対応の安全なブートロード、ファームウェア更新を実現します。

NIST標準の耐量子暗号アルゴリズム

NISTによる標準		開発名称	FIPS	用途	wolfSSLの対応
略称	正式名称				
ML-KEM	Module-Lattice Key Encapsulation Mechanism 格子ベースの鍵カプセル化メカニズム	CRYSTALS-Kyber	FIPS-203	鍵のカプセル化(鍵交換)	wolfSSL v5.5.4 (2022/12)で独自実装
ML-DSA	Module-Lattice Digital Signature Algorithm 格子ベースのデジタル署名アルゴリズム	CRYSTALS-Dilithium	FIPS-204	デジタル署名	wolfSSL v5.7.2 (2024/07)で独自実装
SLH-DSA	Stateless Hash-based Digital Signature Algorithm ステートレスなハッシュベースのデジタル署名方式	SPHINCS+	FIPS-205	デジタル署名	wolfSSL v5.5.1 (2022/9)でliboqs対応

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

IETF による階層型ハッシュ方式の署名検証標準

RFC	正式名称	略称	主な用途	特徴	wolfSSLの対応
RFC8391	eXtended Merkle Signature Scheme	XMSS XMSS^MT	ファーム ウェア更新	高い柔軟性・効率的な署名 サイズ削減	独自実装
RFC8554	Leighton-Micali Signature	LMS LMS/HSS	ファーム ウェア更新	実装の単純化・軽量デバイス 向け効率化	独自実装

ハイブリッド・アルゴリズム

wolfSSLのTLS1.3鍵交換では、IETFで標準として定義されているX25519MLKEM768 / P-256MLKEM768 / P-384MLKEM1024はもちろん、P-521、X448などの組み合わせも利用可能です。X.609証明書では、ML-DSAとRSAまたはECDSAの組み合わせをサポートしています。

PQCアルゴリズムのFIPS認証

NISTのPQCアルゴリズム標準はFIPS認証対象として定義されています。wolfSSLのアルゴリズムは全て独自開発。従来型アルゴリズムの認証と同様にFIPS140-3認証取得可能です。ML-KEM、ML-DSAの認証取得をご検討のお客様はwolfSSLにご相談ください。

wolfSSLでPQCを試してみる

これらの製品はすべてオープソース版(GPLv3)としても公開しています。弊社サイトからダウンロードし実際にコンパイル、実行させて技術評価をすることができます。操作方法は従来型アルゴリズムの場合と変わりなく利用することができます。

1)　wolfSSLのダウンロード、ビルド

```
$ git clone -depth 1 https://github.com/wolfssl/wolfssl
$ cd wolfssl
$ ./autogen.sh
$ ./configure -enable-kyber -enable-dillithium
$ make all
```

2)　ベンチマークプログラムの実行

製品にはアルゴリズムごとのベンチマークプログラムが含まれています。従来型アルゴリズムの比較など、PQCアルゴリズムの性能の目安を知ることができます。

```
$ ./wolfcrypt/benchmark/benchmark.
ML-KEM 1024   256  key gen     49400 ops/Sec
ML-KEM 1024   256    encap     47800 ops/Sec
ML-KEM 1024   256    decap     37300 ops/Sec
```

3)　サンプルクライアント、サーバの実行

クイックスタートとして、次のようにクライアントとサーバーをTLS1.3とPQCの暗号スイートを指定して実行することができます。

```
$ ./examples/server/server -v 4 --pqc P521_KYBER_LEVEL5
$ ./examples/client/client -v 4 --pqc P521_KYBER_LEVEL5
```

wolfSSLのポスト量子暗号について詳しい情報をご希望の方は、info@wolfssl.jp まで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