wolfSSLの耐量子暗号サポート

世界で初めて商用版 CNSA 2.0 に準拠

概要

量子コンピューティングの実用化が迫るに従って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に向けた新しいいロードマップ(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、オープンソースアルゴリズム(liboqs)への対応はもとより、自社開発のアルゴリズムにも取り組んできました。x86_64およびARMアーキテクチャはもちろん、RISC-V他幅広いMCU/MPUアーキテクチャーで高いパフォーマンスを発揮するように設計された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ティング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。当社のML-KEMおよびML-DSA実装は最新のFIPS 203およびFIPS 204標準に準拠しています。また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、ステートフルとステートレスの両方の署名オプションを提供します。

セキュアプロトコルとの統合

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と完全に統合し、TLS 1.3、DTLS1.3、SSH 2.0、MQTTv3/5、MQTT-SNなどの重要なプロトコルと共に動作します。P521(CNSA 2.0およびFIPS 140-3準拠)とKYBER_LEVEL5などのハイブリッド鍵交換、X.509証明書の代替署名スキームとしてのML-DSAなどの署名スキームを組み込むことで、従来の暗号化から耐量子暗号へのスムーズな移行が保証されます。これらはwolfBoot、wolfSSH、cURLなどの弊社製品、またApache Web Serverなどの一般的なプラットフォームやツールですぐに利用でき、将来を見据えたセキュリティ実装をお客様のシステムや製品で実現することができます。詳細は、info@wolfssl.jpまでお問い合わせください。

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