報道関係者各位

2025 年 8 月 20 日
wolfSSL Japan 合同会社

wolfSSL、Evergreen FIPS 140-3 を発表

FIPS140-3 認証取得版 wolfCrypt のサブスクリプションプログラム

暗号化およびネットワークセキュリティソリューションのグローバルリーダーである wolfSSL Inc.（本社：米国ワシントン州エドモンズ）は、FIPS140-3 認証取得版 wolfCrypt のサブスクリプションプログラム、「Evergreen FIPS 140-3」を発表しました。

wolfCrypt は昨年、業界に先駆け FIPS 140-3 認証証明書 4718 を取得しました。FIPS140-3 認証の有効期限は 5 年のため、この証明書は 2029 年 7 月まで有効です。これに加え先月には証明書 5041 を取得し、こちらは 2030 年 7 月まで有効です。wolfCrypt は証明書 5041 の取得により証明書 4718 のライフサイクルを延長し、進化する FIPS 140-3 要件下でも俊敏性、安全性、そしてコンプライアンスに準拠した暗号ライブラリを提供するという wolfSSL の長期戦略における新たな一歩を踏み出しました。

wolfSSL 社の Evergreen FIPS 140-3 サブスクリプションプログラムは、FIPS 140-3 認証における有効期限のギャップを解消します。Evergreen FIPS 140-3 サブスクリプションをご契約のお客様は、証明書 4718 の有効期限が切れると、自動的に証明書 4718 から 5041 へ移行します。今後も既に複数の認証取得計画があり証明書 5041 の有効期限後も新しい証明書へと移行するため、お客様はこれまでより格段にお求めやすい年間サブスクリプションで、継続的な FIPS 認証コードのライセンスを維持できるようになります。

wolfSSL の CTO である Todd Ouska は次のように述べています。
「今回の新しい証明書は単なる継続性を示すだけでなく、セキュリティリーダーシップとお客様の成功に対する揺るぎないコミットメントを反映したものです。Evergreen FIPS 140-3 サブスクリプションにより、wolfSSL をご利用のお客様は継続的なコンプライアンスを維持し、中断やコンプライアンスギャップを生じることなく、最新の認証にシームレスに移行できます。」

このライセンスモデルは、圧倒的に低価格で、政府機関や規制産業に安心を提供し、運用上の遅延なく暗号コンプライアンスを確保します。

今後の複数の認証取得計画については、まずは SRTP と XTS を追加し、セキュアなリアルタイム通信と暗号化ストレージをサポートする予定です。それに続き、Full Linux FIPS 140-3、耐量子暗号対応 FIPS 140-3 認証取得を計画中です。

Full Linux FIPS 140-3

wolfSSL 社が Linux 対応 FIPS140-3 認証を取得後には、様々な暗号ライブラリをホストするオペレーティングシステムの FIPS コンプライアンスの簡素化を実現します。これは Alpine、Alma、Debian、Dynebolic、Gentoo、Kali、 NVIDIA Open GPU、Rocky、Yocto、および現在 FIPS ソリューションを提供していないその他の Linux ディストリビューション向けです。GnuTLS、OpenSSL、NSS、libgcrypt、Linux カーネルなどの主要ライブラリに wolfSSL のパッチを適用することで FIPS 140-3 取得済みの wolfCrypt を使用し、アプリケーションコードを変更することなく FIPS 140-3 準拠を実現します。また、BSD にも対応しています。政府機関向けに FIPS 140-3 準拠を実現する必要があるデバイスメーカーは、使用中の Linux のディストリビューションを離れ、CPU 毎に高額なサブスクリプションに加入して FIPS 準拠を実現するという負担から解放されます。wolfCrypt の検証済みアルゴリズムにすぐにアクセスできるため、FIPS 認証にかかる時間と複雑さが数年から数ヶ月に激的に短縮します。

耐量子暗号対応 FIPS 140-3 認証取得

CNSA 2.0 ガイダンスに準拠した ML-KEM、ML-DSA、LMS、XMSS などの耐量子アルゴリズムを含む、耐量子暗号対応の FIPS 140-3 認証取得は年内に開始予定です。

本件に関するお問い合わせは、 info@wolfSSL.jp までご連絡ください。

wolfSSL について

wolfSSL Inc.は、速度、サイズ、移植性、機能、標準規格への準拠に重点を置き、高性能で軽量なセキュリティソリューションを提供しています。セキュリティライブラリを製品として提供するほか、技術サポートやコンサルティングも行っています。

当社の TLS 製品と wolfCrypt 暗号ライブラリは、政府機関、自動車、航空電子工学などの業界におけるセキュアな設計を支援します。政府機関向けには FIPS140-3 認証を複数取得済みで、お客様への FIPS 認証取得代行サービスも提供しており、10 年の経験と多くの実績があります。
航空宇宙では RTCA DO-178C レベル A 認証、車載向けでは MISRA-C をサポートしており、2004 年の創業以来世界各国で 2,000 社を超えるカスタマーに採用されています。

オープンソース企業として、透明性を保ち、お客様が内部構造を確認できるようにしています。量子脅威から保護するための自社開発の耐量子暗号アルゴリズムは CNSA 2.0 標準に準拠しています。また脆弱性修正への対応時間は平均 36 時間であり、長期間にわたり安定した商用サポートを提供しています。

wolfSSL Inc.は米国ワシントン州シアトルに本社を置き、モンタナ州ボーズマン、オレゴン州ポートランドなどに拠点があります。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。

【お問い合わせ先 】
wolfSSL Japan 合同会社　担当: 須賀
Email: info@wolfSSL.jp
TEL: 050-3698-1916
https://www.wolfssl.jp
https://x.com/wolfSSL_Japan