報道関係者各位

2024 年 7 月 17 日
wolfSSL Japan 合同会社

wolfSSL、世界初の SP800-140Br1 準拠の FIPS 140-3 認証を取得

組み込み向けネットワークセキュリティ専門ベンダの wolfSSL Inc.（本社：米国ワシントン州エドモンズ）は本日、同社の wolfCrypt 暗号ライブラリが世界初の SP800-140Br1 準拠の FIPS 140-3 認証を取得したことを発表しました(証明書番号 4718)。

FIPS 140 認証は、暗号化モジュールの安全性、機密性に関する要件を定める米国政府機関の NIST が制定した標準規格です。これまで FIPS 140-2 が長年使われてきましたが、2019 年に FIPS 140-3 が承認され、2026 年 9 月までに完全に移行することが決まっています。

wolfSSL は AEGISOLVE, INC と提携し、これまで前例のない、FIPS 140-3 認証取得の自動化パイロットプログラムを進めてきました。AEGISOLVE 社は、暗号化ベースのセキュリティシステムと通信インフラストラクチャを評価、検証するための暗号とセキュリティテスト (Cryptographic and Security Testing、CST) を実施できる、米国自主試験所認証プログラム (National Voluntary Laboratory Accreditation Program、NVLAP)の認定を得ています (NVLAP Lab Code: 200802-0)。

wolfSSL の CTO、Todd Ouska は次のように述べています。
「wolfSSL はセキュリティの継続的な革新に注力してきました。今後も自社のテクノロジー強化と機能の拡張に努めていきます。この度の FIPS 140-3 認証取得は、今日のサイバーセキュリティ環境の厳しい要求を満たす最先端の暗号化ソリューションを提供するという当社の取り組みを強調するものです。

AEGISOLVE 社とのコラボレーションは、暗号化セキュリティの新時代のはじまりに過ぎず、将来の革新と業界標準への道を切り開くものと考えています。」

AEGISOLVE 社 の創設者兼社長である Travis Spann 氏は次のように述べています。
「今回の認証取得はこの種のものとして初となる非常に大きな成果であり、次世代の FIPS 140-3 認証済み暗号化モジュールの大きな一歩です。AEGISOLVE は、NIST SP800-140Br1 パイロットプロジェクトにおいて、優秀な wolfSSL チームと協力しこの画期的なマイルストーンを達成できたことを誇りに思っており、他の企業が同じ目標を達成できるよう支援したいと考えています。」

FIPS 140-3 検証テストは、詳細なソースコードレビュー、設計レビュー、ドキュメントレビュー、有限状態マシン検証、CVE 脅威分析、エラーインジェクション、ポートスニッフィング、構成管理検証、運用テスト、FIPS 140-3 派生テスト要件および FIPS 140-3 実装ガイダンスの適用要件に対するテスト証拠監査など、厳格で広範なプロセスです。

NIST は、暗号モジュール検証プログラム (CMVP) の下で、米国連邦政府の部門や機関が使用する暗号モジュールの要件と標準を調整するために、140 の出版シリーズを発行しています。

wolfCrypt FIPS 140-2 と wolfCrypt FIPS 140-3 の違いには以下が含まれます。
+ CAST (条件付きアルゴリズムの自己テスト)
  wolfCrypt FIPS 140-2 では、モジュールの電源投入時のセルフテスト要件により、標準ターゲットと組み込みターゲットの電源投入時間が遅くなる可能性があります。wolfCrypt FIPS 140-3 モジュールでは、アルゴリズムを初めて使用するタイミング、または最初のアルゴリズム使用の前のアプリケーションがテストを実行するのに理想的なタイミングを選んで、ゆっくりとしたイベントサイクルでセルフテストを実行できるようになります。
- モジュールから 3DES が削除され、安全性に問題のある古い 3DES は利用できなくなりました
+ KDF-TLS、TLS v1.2 KDF、TLSv1.3 KDF
+ SSH KDF
+ AES-OFB モード
+ RSA 3072、4096、PSS
+ 新しい劣化動作モード。一部のアルゴリズムで CAST が失敗した場合でも、他のアルゴリズムサービスは引き続き利用できます。

FIPS140-2 から 140-3 への移行に関する情報については、以下で最新情報を更新していきます。
https://wolfssl.jp/products/wolfcrypt-fips/

wolfSSL について

wolfSSL Inc.は、米国ワシントン州エドモンズに本社を持ち、組み込みシステム向けに軽量なセキュリティライブラリを提供しています。スピード、サイズ、移植性、機能、標準への準拠にこだわり、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。

wolfSSL の SSL/TLS 製品と暗号ライブラリは、政府機関、自動車、航空宇宙などでの業界特有の高度なセキュリティデザインをサポートしています。FIPS 140-2/3 認証取得では数多くの実績があり、Common Criteria もサポートしています。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 カスタマーに採用されています。社名と同名の組込み向け TLS ライブラリである wolfSSL は、現在の最新 TLS1.3 と DTLS1.3 までをサポートする商用版ライブラリです。

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