

自社暗号製品「MonoCrypt AES」が米国連邦標準規格「FIPS 140-3」認証を取得

株式会社フォーカスシステムズ（東京都品川区、代表取締役社長：森啓一、以下「当社」）は、自社開発の暗号モジュール*1「MonoCrypt AES」について、米国連邦標準規格「FIPS 140-3」の認証を取得いたしました。*2

昨今、AI の悪用等によるサイバー攻撃の巧妙化や情報漏洩リスクが高まる中、本製品は個人情報や機密情報等の重要データそのものを暗号化することで、企業や組織の情報セキュリティ強化に貢献します。

今回の認証取得により、国際的に活用されるセキュリティへの適合を客観的に示すことで、本製品の信頼性をさらに高め、高いセキュリティ要件が求められる分野への展開を推進してまいります。

*1 データを暗号化するためのシステム開発用ライブラリ

*2 証明書番号：FIPS140-3 Validated, Certificate #5488



【FIPS140-3 について】



FIPS 140-3 は、米国国立標準技術研究所（NIST）*3が定める、暗号モジュールのセキュリティ要件に関する米国連邦標準規格です。暗号機能の実装や鍵管理等について評価が行われ、所定の要件への適合が確認された暗号モジュールが認証されます。

米国政府機関等で重要な情報を保護するシステムに利用される暗号モジュールの選定基準の一つとして活用されています。

*3 アメリカ合衆国商務省の傘下の、標準化や測定技術の開発を行う連邦政府の研究機関

【MonoCrypt AES について】

「MonoCrypt AES」*4は、当社が開発・販売する、システムやアプリケーションに組み込んで利用するライブラリ型の暗号モジュール製品です。既存システムに組み込むことで、保存データや送受信データを AES*5により暗号化し、個人情報や機密情報等の重要データを保護します。

量子コンピュータ*6の発展に伴い、従来の暗号技術から耐量子暗号（PQC）への移行が進む中、

本製品が提供する AES は、今後も継続的な利用が見込まれる暗号技術です。^{*7} 米国国立標準技術研究所（NIST）も AES の継続利用を認めており、将来を見据えた重要データの保護にも活用が期待されます。

■製品ページ：<https://www.focus-s.com/service/monocryptaes>

- ^{*4} 本認証は対象バージョン・動作環境・承認された運用モード等の条件に基づくものであり、組込み先製品・システム全体の認証や、各案件の調達要件すべてへの適合を保証するものではありません。
- ^{*5} 世界標準の暗号化方式であり、保存・伝送されるデータ本体の秘匿性を確保し、情報漏洩を防ぐ。
- ^{*6} 物質やエネルギーの最小単位である「量子」の原理を利用し、従来のコンピュータでは膨大な時間がかかる特定の計算を、高速に処理できると期待される次世代のコンピュータ。
- ^{*7} 今回の FIPS 140-3 認証は、本製品の PQC 対応を認証するものではありません。

【今後の展望】

当社は本認証取得で培った知見や国内メーカーとしての技術サポート力を活かし、お客さまの製品に本製品を組み込むことで、FIPS 140-3 への適合が求められる海外市場への展開や政府調達関連案件への参入を支援してまいります。また、官公庁・金融・医療等の高いセキュリティ要件が求められる国内分野への提案力を強化し、本製品の適用領域拡大を図ります。

また、暗号モジュールの選定・導入をはじめとするお客さまのデータ保護に関する技術支援を通じて、新たな事業機会の創出につなげてまいります。

【フォーカスシステムズについて】

株式会社フォーカスシステムズは、1977 年に設立され、公共・通信ほか、社会性の高い分野におけるシステム開発・運用に携わるだけでなく、IoT、クラウドや AI 等、時代の流れを見据えたビジネス展開も積極的に推進しています。コーポレートスローガンは“テクノロジーに、ハートを込めて。”人と人との技術をつなぐ私たちフォーカスシステムズの仕事に、社員ひとりひとりが、情熱と誠意を持って臨む姿勢を込めました。

HP：<https://www.focus-s.com/>

【製品に関するお問い合わせ】	【報道・広報に関するお問い合わせ】
株式会社フォーカスシステムズ テクノロジーノベーション事業本部 E-MAIL： product@focus-s.com TEL：03-5420-2470	株式会社フォーカスシステムズ コーポレートマネジメント本部 IR・広報部 E-MAIL： koho@focus-s.com TEL：03-5421-7790