米国連邦情報処理規格（FIPS）検証済みのセキュアなファイル転送製品

MOVEit Transfer、MOVEit Automation、WS_FTP Server 製品は、NIST によって FIPS の検証を受けています。

FIPS とは？

米国連邦情報処理規格（FIPS）140-2 は、2001 年に米国商務省の非監督機関であるアメリカ国立標準技術研究所（National Institute of Standards and Technology、NIST）によって制定されました。NIST は、米軍や様々な政府機関が遵守すべき各種の基準を制定しています。米国政府機関や米軍と協業するベンダー、請負業者などの組織も、FIPS を遵守する必要があります。カナダ政府も、導入するソフトウェアが FIPS 検証済みであることを前提としており、FIPS の制定にあたって NIST に協力しています。

FIPS には、ロケーションと個人識別情報のフォーマット、暗号化アルゴリズム、キーストレージ、その他のデータ処理に関する標準が含まれています。FIPS の目的は、種々のサービスのセキュリティ、品質、および処理の互換性を容易に確認できる方法で保証することです。

FIPS 140-2 の要件

高度なセキュリティが必要な場合、FIPS 検証済みデータ送信アプリケーションは、FIPS 140-2 で承認されたアルゴリズムとハッシュ関数の両方を使用し、暗号モジュール検証プログラム（Cryptographic Module Validation Program、CMVP）によって検証されなければなりません。CMVP は、米国 NIST とカナダ通信安全保証部（Communications Security Establishment Canada、CSEC、カナダにおける NIST の検証部門）の監督下で行われるテストプロセスです。

FIPS 検証済みソリューションが使用すべき FIPS 140-2 で承認された暗号化アルゴリズムとハッシュ関数には、次のようなものがあります。

- AES（Advanced Encryption Standard）は、2001 年に NIST が採用した新しいアルゴリズムです。キーを強化すると、トリプル DES（Triple Data Encryption Standard）よりも強力になります。
- トリプル DES は IBM の 56 ビット DES 暗号の変形で、3 つのキーを組み合わせるので合計 168 ビットの強さになります。トリプル DES は 1999 年に NIST から使用の承認を受けました。
- HMAC SHA-1 は、国家安全保障局（National Security Agency、NSA）によって設計された暗号ハッシュ関数です。メッセージを認証し、秘密キーと組み合わせて展開します。

FIPS セキュリティの 4 レベル

レベル 1

FIPS は、「暗号モジュールのソフトウェアおよびファームウェアコンポーネントが検証済みでないオペレーティング・システムを使用する汎用コンピューティング・システム上で実行されることが可能」なレベルをレベル 1 と指定しています。ユーザーは通常のハードウェアでこのレベルのセキュリティを実行できます。

レベル 2

ロール・ベースの認証、ソフトウェアのオペレーティング・システムに関する物理的な改ざんや保護の証拠を提供するシールが必要です。

レベル 3

物理的な改ざん防止を含むレベル 2 を超えるいくつかの要件が加わります。

レベル 4

環境ハザードへの耐性を含む、より厳しい改ざん防止要件が追加されます。

FIPS 準拠と FIPS 検証済みとの違い

多くのソリューション提供者は、そのソリューションが「FIPS 準拠」であると強調しますが、FIPS 準拠はそのソリューションが FIPS の要件に沿っているという主張に過ぎません。本当の意味で FIPS を遵守するには、FIPS の検証が必要です。FIPS の検証には、NIST の検査機関に詳細な文書とソースコードを提出する必要があります。ほとんどの場合、検査プロセスは数カ月（平均 6～9 か月）かかります。つまり、FIPS 検証済みのソリューションは、承認されたアルゴリズムを使用しているだけでなく、きちんと文書化され、しっかりした技術の裏打ちがあり、検査を受け、検証プロセスがスムーズに進行するよう簡単にテストできるという特長があります。

NIST は、ソフトウェア操作をテストするだけでなく、メモリ内のキーの誤った使用や廃棄、「ランダムな」番号生成の予測可能性などのセキュリティ上の欠陥もチェックします。また、モジュールの自己整合性チェック（改ざんを防止）の有無を検証し、バックドアとハードコード・キーについてもチェックします。ファイル転送ソフトウェアでは、クライアント・アプリケーションとサーバー・アプリケーションの両方を検証する必要があります。ソフトウェアの操作に関わる他のシステムやプロセスも検証する必要があります。

検証プロセスは、ソフトウェア・ソリューションが、FIPS を実装しているサード・パーティーのために、文書化されたテスト可能なソースコードの作成に関与するほど複雑です。そのため、現在のところ、FIPS で検証された暗号化および処理が含まれているファイル転送製品はほんの一握りに限られます。

イプスイッチの FIPS 検証済み製品

WS_FTP Server

WS_FTP Server の FIPS モジュールは、OpenSSL FIPS（Hewlett Packard、DoD Military Health System、Open-Source Software Institute が主催するオープンソースプロジェクト）を使用して、AES（最大 256 ビット）、トリプル DES、および HMAC SHA-1 暗号化転送をサポートします。WS_FTP Server の暗号化転送、整合性チェック（FTP、HTTP、および HTTPS）、HTTPS 転送、FTP コマンド、およびデータストリーム暗号化はすべて、FIPS 検証済みのモジュールで検証されています。これらはすべてトランザクション・プライバシーのために AES 暗号化を使用し、データ完全性チェックのために HMAC SHA 1 を使用します。WS_FTP ソリューションは、（OSSI のオープン SSL の下で）613、668、701、および 352 で検証された特定のプロトコルとともに、FIPS サティフィケイト 918 で検証されています。

MOVEit

イプスイッチの MOVEit Transfer アプリケーションと MOVEit Automation アプリケーションはどちらも、暗号化に FIPS で検証された AES と SHA-1 を使用します。MOVEit は、サティフィケイト 30 と 124 で検証された特定のプロトコルとともに、NIST サティフィケイト 1363 で検証されています（米国とカナダの両方で認められています）。FIPS 検証済みのモジュールを使用して、ファイルの暗号化、HTTP と HTTPS、FTP 整合性チェック、機密データベース・フィールドの暗号化を行います。MOVEit Transfer は、FIPS 検証済みの Windows オペレーティング・システムで稼動し、HTTPS 転送、FTP コマンド、およびデータストリーム暗号化に FIPS 検証済みの暗号化を使用します。MOVEit Automation も同様に、設定ファイルの暗号化と、HTTP、HTTPS、FTP の整合性チェック（MOVEit 独自の整合性チェックと標準の XSHA1 の両方を使用する）のために FIPS 検証済み暗号化を使用します。FIPS 検証済みの Windows オペレーティング・システムで稼動する MOVEit Automation の、HTTPS トランスポート暗号化、FTP コマンド、およびデータストリーム暗号化も FIPS 検証済みです。