

令和4年12月28日

## 米国基準「NIST SP800-171/172」への準拠性を示す情報セキュリティ格付け ～わが国で最初のAAA格を富士フイルムビジネスイノベーションが取得～

富士フイルムビジネスイノベーション株式会社（本社：東京都港区）が提供するデジタル複合機・プリンターに対して、一般社団法人日本セキュリティ格付機構（略称：JaSRO、本社：東京都中央区）は、NIST（米国国立標準技術研究所：National Institute of Standards and Technology）の基準を用いた情報セキュリティ格付け最高位の「AAAis」（\*1）をわが国で最初に付与した。

デジタル複合機・プリンターの商品開発・保守業務を営む富士フイルムビジネスイノベーション株式会社（以下「FB社」という。）は、ユーザーの情報セキュリティに関する課題に応えるべく、商品を開発するにあたり、各種のセキュリティ機能の拡充、暗号アルゴリズムの危殆化対応などを通じて、情報セキュリティの拡充と品質の確保に取り組んでいる。

今回の格付スコープ「NIST への対応環境においてデジタル複合機・プリンターを使用される事業者向けに提供する、デジタル複合機・プリンター」の開発業務および保守業務において、「NIST SP800-171」及び「NIST SP800-172」への準拠性の観点で求められる対策（特定、防御、検知、対応、復旧の管理策）を極めて高い水準で織り込んでいるため、わが国で最初の「AAAis」を付与した。

### <格付結果>

企業名	富士フイルムビジネスイノベーション株式会社
格付種別	情報セキュリティ格付
格付タイプ	NIST SP800-171/172 準拠性
格付 ID コード	10000370402C2201
格付スコープ	NIST への対応環境においてデジタル複合機・プリンターを使用される事業者向けに提供する、デジタル複合機・プリンター *2
想定リスク	情報漏えい
格付符号	AAAis（トリプルA）*1
格付の方向性	安定的
有効期間	2022年12月28日から2023年12月27日まで交付日から1年間



\*1: AAAis は全 17 段階中最高位の格付。AAAis に求められるセキュリティ水準は「リスク耐性は極めて高く、多くの優れた要素がある」状態であり、次の2つの要件を満たす必要がある。

要件1 「新たな脅威に迅速に対応し、常時、高水準の管理状態を維持、発展させている。」

●お問い合わせ先 一般社団法人日本セキュリティ格付機構

Japan Security Rating Organization（略称、JaSRO）

〒104-0061 東京都中央区銀座1-22-11

E-mail: info@jasro.org <http://www.jasro.org>

情報セキュリティ格付は、被格付組織等から入手した情報に依拠して形成した当機構の意見であり、その正確性、完全性、網羅性等は必ずしも保証されてはいません。格付事由書、格付レポート等は、原則として被格付組織または被格付組織の格付けを要請した者からの依頼に基づき有償で作成されたものであり、被開示者、閲覧者等には参考情報としてご提供されるものです。格付事由書および格付レポート等は、被格付組織の事業やサービス、被格付組織との取引や情報共有等を推奨するものではありません。当機構は、情報セキュリティ格付に関するクレーム、訴訟その他の紛争、被格付組織その他の第三者に関して生じうる一切の損害、損失、費用等について責任を負うものではありません。なお、情報セキュリティ格付に関する一切の著作権その他の知的財産権、営業秘密、ノウハウその他の権利・利益は当機構に留保され、当機構に専属的に帰属するものとします。

要件2「SP800-171/172の適切な対策を、極めて高い水準で織り込んでいる。」

\*2: ApeosPrint 4560 S/3960 S/3360 S  
Apeos 7580/6580/5580  
ApeosPrint C5570/C4570  
Apeos C7070～C2570  
Apeos C8180～C6580  
ApeosPro C810～C650  
Apeos 4570 / 3570  
Apeos C2360 / C2060  
Apeos 3060 / 2560  
Apeos 1860  
Apeos C5240  
Apeos 6340  
ApeosPrint C5240  
ApeosPrint 6340

デジタル複合機・プリンターのセキュリティ上の脅威と対策として、情報漏えい、データ改ざんおよび情報への不正アクセスの攻撃の観点から、以下の主な項目がオフィスのデジタル複合機・プリンターに対するセキュリティ上のリスクと捉え、最適な対策を講じており、取り組み内容は「富士フイルムデジタル複合機のセキュリティー白書」(2021年11月24日:Version2.2)として取りまとめ、FB社Webサイトからダウンロードできるよう開示している。

- 他の利用者による不正な操作
- 通信データの盗聴、改ざん
- 管理機能への不正アクセス
- デジタル複合機・プリンターのソフトウェアの改ざん・破壊
- 監査ログの改ざん
- デジタル複合機・プリンター内に保存された文書の漏えい  
(リース終了返却、又は廃棄処理時)
- 管理者またはエンドユーザーのうっかりミスによる情報漏えい

また、セキュリティの信頼性を保証すべく、情報セキュリティ技術のマネジメントシステムである国際標準規格「ISO/IEC27001」の認証を取得しており、その取り組みをベースとし、情報技術セキュリティの設計や運用などの国際標準規格「ISO/IEC15408(CC 認証)」の認証を取得している。

●お問い合わせ先 **一般社団法人日本セキュリティ格付機構**  
Japan Security Rating Organization (略称、JaSRO)

〒104-0061 東京都中央区銀座 1-22-11  
E-mail:info@jasro.org <http://www.jasro.org>

情報セキュリティ格付は、被格付組織等から入手した情報に依拠して形成した当機構の意見であり、その正確性、完全性、網羅性等は必ずしも保証されてはいません。格付事由書、格付レポート等は、原則として被格付組織または被格付組織の格付けを要請した者からの依頼に基づき有償で作成されたものであり、被開示者、閲覧者等には参考情報としてご提供されるものです。格付事由書および格付レポート等は、被格付組織の事業やサービス、被格付組織との取引や情報共有等を推奨するものではありません。当機構は、情報セキュリティ格付に関するクレーム、訴訟その他の紛争、被格付組織その他の第三者に関して生じうる一切の損害、損失、費用等について責任を負うものではありません。なお、情報セキュリティ格付に関する一切の著作権その他の知的財産権、営業秘密、ノウハウその他の権利・利益は当機構に留保され、当機構に専属的に帰属するものとします。

今回、NIST（米国国立標準技術研究所：National Institute of Standards and Technology）への対応環境においてデジタル複合機・プリンターを使用される事業者向けに提供するデジタル複合機・プリンターにおける、情報漏えい、データ改ざん、情報への不正アクセスの攻撃、重要情報の取得・利用・保管・移送・消去等におけるトータルな取り組み状況について、「NIST SP800-171」及び「NIST SP800-172」への準拠性の観点から審査を行った。主な取り組みは以下の通りである。

高水準のセキュリティ機能として、複合機が起動する際のすべてのプロセスで改ざんを検知、自動復旧できることや、ASLR（Address Space Layout Randomization）に対応しており、メモリ上のデータ配置をランダム化することで、万が一、脆弱性があった場合にも、同じ攻撃ツールで多数の複合機を攻撃できないようにしている。

重要情報の取得・利用については、保守要員（以下、「カスタマーエンジニア」）はユーザーの許可がないと機械管理機能にアクセスできないよう制御している。なお、機械管理者の認証手段は、多要素認証を実装している。また、ネットワーク／セキュリティ／集計管理機能への設定変更ができる権限者、監査ログへのアクセス権限者等、機能別に権限者を細かく設定することができ、牽制機能を働かせることが可能である。ユーザーにて運用しているActive Directoryなどの外部認証システムとの連携やSyslogプロトコルをサポートする外部ログサーバとの連携を図るなど、ユーザーの環境に合わせて強化を図ることができるよう設計されている。また、ユーザー利用時において、操作パネル内にあるスタートボタンを意図せず触れてしまい送信してしまったということがないように、スタートボタンをスライドさせないと起動しないようスライドスタート機能を組み込んでいる。

重要情報の保管については、重要情報が含まれるデジタル複合機・プリンターのストレージは、暗号化されており、仮に持ち出されて他の機器に設置しても復号することができない対策を講じている。また、TPMチップにルート暗号鍵を格納しているが、TPM2.0の採用により、コントローラとTPMチップ間のデータ通信の暗号化を実現している。

重要情報の移送については、デジタル複合機・プリンターとの通信経路はすべて、新たなTLS暗号設定基準でも要求されている最新のTLS v1.3に対応し、無線LANによる接続には、WPA3への対応を実装することで、ネットワーク通信の暗号化を強化しており、情報漏えい・改ざんを抑止するとともに、FAX、デジタル複合機・プリンター管理サービス（EP-BB）等、外部ネットワークへの接続を無効とすることで、不正アクセスなどでの情報漏えいの脅威を排除している。また、故障等により解析するためであっても重要情報を持ち帰ることはせず、すべて、ユーザーにて対応するよう体制を整えている。

重要情報の消去については、デジタル複合機・プリンターのストレージを交換・廃棄するケースでは、ユーザーで、上書き消去機能によるサニタイゼーションを実施し、希望があれば、その場でストレージを物理的に破壊する等の対策を講じている（ストレージの再利用はしていない）。

取り組みが確実に行われるには、カスタマーエンジニアの力量も大きく左右することから、通常の保守教育に加え、NIST対応向けの教育を受講し、合格した者のみが、NIST対応での保守を実施するよう、人的対策についても強化を図っている。

また、2022年度には、これまでの対策に加えてさらに充実した次の機能を装備しており、セキュリティ強化の経営方針が具体的な取り組みとして確認できる。

① 改ざん検知復旧機能の強化

ハードウェア内のRoot of Trust を使った起動時改ざん検知（セキュアブート）機能として、セキュアブートの信頼の起点（Root of Trust）をハードウェア内に持つことで、改ざんをより困難（殆ど不可能）にしている。Bootloaderが改ざん検知した際の自動復旧機能に追加して、OS、Middleware/Applicationの改ざんを検知、自動復旧する機能を実装している。また、改ざんを検知した／復旧したことを監査ログにて確認することができる。

② 監査ログ機能の強化

サイバー脅威ハンティング活動の一部として、監査ログの監視・分析・報告を可能とするために、Syslogを用いて監査ログを外部サーバに送信しているが、その項目に「スキャン文書の転送先」「複合機を特定できる情報」を追加している。監査ログのデータ形式は、SIEM（Security Information and Event Management）などで解析しやすいものとしている。

③ SMB3.1.1のサポート

スキャン送信（SMB）・ジョブフロー（SMB転送）にてSMBプロトコル（ファイル共有プロトコル）が、Windows10、Windows11に搭載しているSMB3.1.1に対応するよう機能を追加している。SMB3.1.1には、暗号化と認証を同時に行うことができる共通鍵暗号方式であるSMB暗号化の機能AES-GCM（Advanced Encryption Standard - Galois/Counter Mode）が実装されている。

④ TLS通信のセキュリティ強化

脆弱性が指摘されている古い暗号スイートの使用を停止することでセキュリティ強化を図ることができる機能を追加している。具体的には、TLS通信時にPFS（Perfect Forward Secrecy：暗号化された通信と秘密鍵の両方が漏えいしても復号化できないという鍵交換の概念）の特性を持たない暗号スイートを使用しない動作をTLSクライアント／TLSサーバの両方に適用している。

⑤ SSD管理機能の強化

機能設定リストの機械構成の欄にストレージ（SSD）情報が印字される機能を追加している。定期的に機能設定リストを出力することで、付け替えられたとしても気が付けるようセキュリティ強化を図ることができる。

総じて、NISTへの対応環境にて、デジタル複合機・プリンターを使用される事業者向けに提供する、デジタル複合機・プリンターの開発業務および保守業務において、「NIST SP800-171」への準拠性の観点で求められる対策（特定、防御、検知、対応、復旧の管理策）を極めて高い水準で織り込んでいる。

また、「NIST SP800-172」への対応として、起動する際のすべてのプロセスで改ざんを検知し、自動復旧できる機能の実装や、メモリ上のデータ配置をランダム化する機能の実装、「ISO/IEC 15408(CC 認証)」での評価等、極めて高い水準で織り込んでいる。

「NIST SP800-171/172」への準拠性に加え、「NIST SP800-53」への対応も実施しており、新たな脅威に迅速に対応し、常時、高水準の管理状態を維持、発展させており、マネジメントの成熟度は高いレベルにある。

更なる強化策として計画している対策を実施することを期待する。また、保守業務では、NIST対応によるサービスはリリースして間もないことから、長年培ったノウハウを活かしつつ、新たなノウハウを蓄積し、更なる強化を図っていくことを期待する。

●お問い合わせ先 **一般社団法人日本セキュリティ格付機構**  
Japan Security Rating Organization (略称、JaSRO)

〒104-0061 東京都中央区銀座 1-22-11

E-mail:info@jasro.org <http://www.jasro.org>

情報セキュリティ格付は、被格付組織等から入手した情報に依拠して形成した当機構の意見であり、その正確性、完全性、網羅性等は必ずしも保証されてはいません。格付事由書、格付レポート等は、原則として被格付組織または被格付組織の格付けを要請した者からの依頼に基づき有償で作成されたものであり、被開示者、閲覧者等には参考情報としてご提供されるものです。格付事由書および格付レポート等は、被格付組織の事業やサービス、被格付組織との取引や情報共有等を推奨するものではありません。当機構は、情報セキュリティ格付に関するクレーム、訴訟その他の紛争、被格付組織その他の第三者に関して生じうる一切の損害、損失、費用等について責任を負うものではありません。なお、情報セキュリティ格付に関する一切の著作権その他の知的財産権、営業秘密、ノウハウその他の権利・利益は当機構に留保され、当機構に専属的に帰属するものとします。

## ○格付定義の補足説明

セキュリティ格付制度は産業構造審議会での協議を経て考案された制度です。

下記は、「NIST SP800-171/172」の準拠性を示す格付定義の補足説明です。

AAA <sub>is</sub>	(要件1) 新たな脅威に迅速に対応し、常時、高水準の管理状態を維持、発展させている。 (要件2) SP800-171/172 の適切な対策を、極めて高い水準で織り込んでいる。
AA <sub>is</sub>	(要件1) 継続的な改善プロセスを有し、高水準の管理状態を維持、発展させている。 (要件2) SP800-171/172 の適切な対策を、高い水準で網羅的に織り込んでいる。
A <sub>is</sub>	(要件1) 検証したプロセスを用いて、目標を指標化したうえで管理、実行している。 (要件2) 一定水準 (ISO/IEC27001 水準) に加え、SP800-171/172 の対策を部分的に織り込んでいる。
BBB <sub>is</sub>	(要件1) 明確に定義した手順書等に基づき、組織的に管理、実行している。 (要件2) 一定水準 (ISO/IEC27001 水準) の予防・防止的管理策 (前もって防ぐこと) を織り込んでいる。
BB <sub>is</sub>	(要件1) 手順書等は整っていないが、一定水準の管理をしている。 (要件2) 一定の抑止的管理策 (行動を思いとどまらせること) および発見的 management 策を織り込んでいる。
B <sub>is</sub>	(要件1) 特定の人員に依存して、非公式な管理をしている。 (要件2) 発見的 management 策 (事故の発生を発見できること) 等の対策が不十分である。
C <sub>is</sub>	(要件1) プロセスが確立しておらず、管理が不十分である。 (要件2) 対策が講じておらず、絶えず脅威にさらされている。

## ○格付結果

富士フイルムビジネスイノベーション株式会社の格付結果は弊機構 HP (下記リンク) を参照ください。

<http://jasro.org/client/index.html>

○富士フイルムビジネスイノベーションの複合機については同社 HP (下記リンク) を参照ください。

[https://www.fujifilm.com/fb/product/multifunction/promotion/security\\_measure](https://www.fujifilm.com/fb/product/multifunction/promotion/security_measure)

<お問い合わせ先>

一般社団法人日本セキュリティ格付機構

企画部

E-mail : [info@jasro.org](mailto:info@jasro.org)

以上

●お問い合わせ先 **一般社団法人日本セキュリティ格付機構**

Japan Security Rating Organization (略称、JaSRO)

〒104-0061 東京都中央区銀座 1-22-11

E-mail:[info@jasro.org](mailto:info@jasro.org) <http://www.jasro.org>

情報セキュリティ格付は、被格付組織等から入手した情報に依拠して形成した当機構の意見であり、その正確性、完全性、網羅性等は必ずしも保証されてはいません。格付事由書、格付レポート等は、原則として被格付組織または被格付組織の格付けを要請した者からの依頼に基づき有償で作成されたものであり、被開示者、閲覧者等には参考情報としてご提供されるものです。格付事由書および格付レポート等は、被格付組織の事業やサービス、被格付組織との取引や情報共有等を推奨するものではありません。当機構は、情報セキュリティ格付に関するクレーム、訴訟その他の紛争、被格付組織その他の第三者に関して生じうる一切の損害、損失、費用等について責任を負うものではありません。なお、情報セキュリティ格付に関する一切の著作権その他の知的財産権、営業秘密、ノウハウその他の権利・利益は当機構に留保され、当機構に専属的に帰属するものとします。