情報セキュリティ格付サマリー
(NIST SP800-171/172 準拠性確認)

No. 22K0013

2022 年 12 月 28 日

般社団法人 日本セキュリティ格付機構

JaSRO (Japan Security Rating Organization)

1． 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(*) (*) 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
格付対象	格付スコープに関する開発業務および保守業務
想定リスク	情報漏えい
格付符号	**AAA is** （トリプル A）
格付の方向性	ポジティブ
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）

●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** 〒104-0061 東京都中央区銀座 1-22-11
Japan Security Rating Organization（略称、JaSRO） E-mail:info@jasro.org http://www.jasro.org

情報セキュリティ格付サマリー
(NIST SP800-171/172 準拠性確認)

審査結果、「NIST SP800-171」（rev.2）及び「NIST SP800-172」が要求している対策について、高い水準で網羅的に対策を講じており、基準に準拠していると認定します。

※ 格付審査の方法は、責任者等へのヒアリング、規程及び台帳類の閲覧、関連設備の視察を用いております。

※ 当格付けは、現地審査の実施日における事象について事実であることを確認したものであり、継続的に当該事象が必ず存在することを保証するものではありません。また、格付対象の仕様変更や社会環境の変化に応じ、緊急時には随時、また平常時には年一回の再審査による点検を推奨しています。

※ 当格付けは、「NIST SP800-171」及び「NIST SP800-172」への準拠性の観点から審査を行っています。「NIST SP800-171」への準拠性の確認に際しては、要求管理策 110 件のうちリスクアプローチにより対象となった 86 件すべての準拠状況を審査しております。なお、対象外の要求管理策 24 件は、除外理由を確認したうえで、審査対象から除外しています。また、「NIST SP800-172」については、要求管理策 35 件のうちリスクアプローチにより対象となった 14 件すべての準拠状況を審査しております。なお、対象外の要求管理策 21 件は、除外理由を確認したうえで、審査対象から除外しています。

●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** 〒104-0061 東京都中央区銀座 1-22-11
Japan Security Rating Organization（略称、JaSRO） E-mail:info@jasro.org http://www.jasro.org

情報セキュリティ格付サマリー
(NIST SP800-171/172 準拠性確認)

当該格付符号とした事由

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（東京都港区、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。

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。

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。

●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　〒104-0061 東京都中央区銀座 1-22-11
Japan Security Rating Organization（略称、JaSRO）　E-mail:info@jasro.org http://www.jasro.org

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、「カストマーエンジニア」）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、カスト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。

●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 〒104-0061 東京都中央区銀座 1-22-11
Japan Security Rating Organization（略称、JaSRO） E-mail:info@jasro.org http://www.jasro.org

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。

●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** 〒104-0061 東京都中央区銀座 1-22-11
Japan Security Rating Organization（略称、JaSRO） E-mail:info@jasro.org http://www.jasro.org

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。

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　〒104-0061 東京都中央区銀座 1-22-11
Japan Security Rating Organization（略称、JaSRO）　E-mail:info@jasro.org http://www.jasro.org

情報セキュリティ格付サマリー
(NIST SP800-171/172 準拠性確認)

資料１．格付定義

【格付定義】

AAA_{is}	リスク耐性は極めて高く、多くの優れた要素がある。
AA_{is}	リスク耐性はかなり高く、優れた要素がある。
A_{is}	リスク耐性は高く、部分的に優れた要素がある。
BBB_{is}	リスク耐性は十分であるが、将来環境が大きく変化する場合、新たな対策が必要である。
BB_{is}	リスク耐性には注意すべき要素があり、将来環境が変化する場合、新たな対策が必要である。
B_{is}	リスク耐性に問題があり、絶えず注意すべき要素がある。
C_{is}	リスクが顕在化する可能性が極めて高い。

【格付定義の補足説明】 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_{is}	(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_{is}	(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_{is}	(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_{is}	(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_{is}	(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)および発見的管理策を織り込んでいる。
B_{is}	(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)発見的管理策(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_{is}	(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。

(注) 各々の格付けを付与するに際しては、下位の格付けの要件を満たす必要がある。なお、要件１や要件２は、格付定義を補足説明したものであり、被格付組織の特性や脅威の変化等により随時変更することがある。

●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** 〒104-0061 東京都中央区銀座 1-22-11
Japan Security Rating Organization (略称、JaSRO) E-mail:info@jasro.org http://www.jasro.org