

No. 22K0012

2022年9月24日

一般社団法人 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 準拠性 (NIST Special Publication 800-171 rev.1)
格付 ID コード	10000370401C2204
格付スコープ	NIST への対応環境においてデジタルカラー複合機・プリンターを使用される事業者向けに提供する、デジタルカラー複合機・プリンター(*1,*2)
	*1 2020 年春発売の新機種
	・ ApeosPort C7070～C2570
	・ ApeosPort 4570 / 3570
	・ ApeosPort C2360 / C2060
	・ ApeosPort 3060 / 2560 / 1860
	・ ApeosPort Print C5570 / C4570
	・ ApeosPort-VII C4422 / C3322
	・ ApeosPort-VII 5022
	・ ApeosPort-VII CP4422 / CP3322
	・ ApeosPort-VII P4022
	*2 2021 年春発売の新機種
	・ Apeos C8180
	・ Apeos C7580
	・ Apeos C6580
	・ Apeos C2570
	・ Apeos C3070
	・ Apeos C3570
	・ Apeos C4570
	・ Apeos C5570
	・ Apeos C6570

●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。

Copyright (C) 2022 JaSRO All rights reserved.

	<ul style="list-style-type: none">・ Apeos C7070・ ApeosPro C650・ ApeosPro C750・ ApeosPro C810
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9月24日から2023年9月23日まで(交付日から1年間)

審査結果、NIST/SP800-171 (NIST Special Publication 800-171 rev.1) の要求事項への対策を高い水準で網羅的に講じており、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」への準拠性の観点から審査を行っています。準拠性の確認に際しては、要求管理策 110 件のうち対象となった 86 項目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。

●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。

Copyright (C) 2022 JaSRO All rights reserved.

2. 当該格付符号とした事由

デジタルカラー複合機・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。

デジタルカラー複合機・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カラー複合機・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
- デジタルカラー複合機・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
- デジタルカラー複合機・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」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カラー複合機・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カラー複合機・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」への準拠性の観点から更新審査を行った。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>

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。

Copyright (C) 2022 JaSRO All rights reserved.

情報セキュリティ格付サマリー (NIST/SP800-171 準拠性確認)

高水準のセキュリティ機能として、情報漏えいに繋がる OS レベルでの改ざんを起動時に検知する、起動時改ざん検知(セキュアブート)機能や、稼働中に OS/Application 領域へのアクセス監視と書き換えを防止する稼働時改ざん防止(ホワイトリストリング)機能を実装している。

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。

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カラー複合機・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。

重要情報の移送については、デジタルカラー複合機・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、デジタルカラー複合機・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、デジタルカラー複合機・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、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、2021年春発売の新機種は、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 セキュアブートの強化(自動検知+自動アラート)

●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。

Copyright (C) 2022 JaSRO All rights reserved.

情報セキュリティ格付サマリー (NIST/SP800-171 準拠性確認)

Hardware Root of Trustを使用して、Bootloader、OS、Middleware/Applicationの改ざんを検知する機能を実装している。また、改ざんを検知したことを監査ログにて確認することができ、監査ログを用いて異常時には自動的にアラートを発する機能が装備されている。

② TPMチップ2.0 の採用

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。

③ 無線接続時のWPA3対応

無線LANによる接続には、WPA3への対応を実装しており、鍵交換のセキュリティが強化され、強固な暗号方式が使われます。

④ 誤送信防止にもなるスライドスタート

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。

総じて、NISTへの対応環境にて、デジタルカラー複合機・プリンターを使用される事業者向けに提供する、デジタルカラー複合機・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。

「NIST/SP800-171」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。

Copyright (C) 2022 JaSRO All rights reserved.

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】

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 の対策を、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 の対策を、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 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 management 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 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 _{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>

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。

Copyright (C) 2022 JaSRO All rights reserved.