情報セキュリティ格付サマリー
(NIST/SP800-171 準拠性確認)

No. 19K0012

2020 年 3 月 18 日

株式会社 アイ・エス・レーティング

１． 格付結果

企業名	富士ゼロックス株式会社
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	10000370401C1901
格付スコープ	NIST への対応環境においてデジタル複合機を使用される事業者向けに提供する、デジタル複合機(*1) *1 ApeosPort-Ⅶシリーズ、DocuCentre-Ⅶシリーズ
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	AA^{+}_{is} (ダブル A プラス)
格付の方向性	ポジティブ
有効期間	2020 年 3 月 18 日から 2021 年 3 月 17 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 株式会社アイ・エス・レーティング 〒103-0023 東京都中央区日本橋本町 1-10-23 第 20 ビル 8 階
TEL:03-3273-8830 http://www.israting.com

２． 当該格付符号とした事由

デジタル複合機の商品開発・保守業務を営む富士ゼロックス株式会社（東京都港区、以下「FX社」という。）は、お客様の情報セキュリティに関する課題にお応えすべく、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。

複合機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複合機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「富士ゼロックスデジタル複合機のセキュリティ白書」（2019年10月1日：Version1.8）として取りまとめ、FX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
- 複合機のソフトウェアの改ざん・破壊
- 監査ログの改ざん
- 複合機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複合機を使用される事業者向けに提供するデジタル複合機における、重要情報の取得・利用・保管・移送・消去等の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審査を行った。主な取り組みは以下の通りである。

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」）はお客様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。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。お客様にて運用している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

●お問い合わせ先 株式会社アイ・エス・レーティング 〒103-0023 東京都中央区日本橋本町 1-10-23 第 20 ビル 8 階
TEL:03-3273-8830 http://www.israting.com

ートする外部ログサーバとの連携を図るなど、お客様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複合機のハードディスク(HDD)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、複合機との通信経路はすべて暗号化されており、情報漏えい・改ざんを抑止するとともに、FAX、複合機管理サービス（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、お客様先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、デジタル複合機のHDDを交換・廃棄するケースでは、お客様先で、サニタイゼーションを実施し、希望があれば、その場でHDDを物理的に破壊する等の対策を講じている（HDDの再利用はしていない）。

上記の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。

総じて、NISTへの対応環境にて、デジタル複合機を使用される事業者向けに提供する、デジタル複合機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）を網羅的に織り込んでおり、継続的な改善プロセスを有している。

以上

●お問い合わせ先 **株式会社アイ・エス・レーティング** 〒103-0023 東京都中央区日本橋本町 1-10-23 第 20 ビル 8 階
TEL:03-3273-8830 http://www.israting.com

情報セキュリティ格付サマリー
(NIST/SP800-171 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】

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・防滴管理策(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 **株式会社アイ・エス・レーティング** 〒103-0023 東京都中央区日本橋本町 1-10-23 第 20 ビル 8 階
TEL:03-3273-8830 http://www.israting.com