ネットワーク機能付き事務機セキュリティガイドライン Ver.1.10 要件チェックシート（1/3）

ネットワーク機能付き事務機セキュリティガイドライン Ver.2.00 要件チェックシート

申請者	株式会社リコー	製品分類	デジタル複合機
適合宣言者	リコーデジタルプロダクツBU WP事業本部 コントローラ開発センター CS開発統括室　堀内 義峯	製品名	RICOH IM C431/C431F
申請日	2025/1/20	確認した ファームウェア バージョン	システム V1.01

ネットワーク機能付き事務機セキュリティガイドライン Ver.2.00 要件チェックシート					回答欄		
ID	セキュリティ要件	ステータス[a)]	機能要件	確認項目	サポート[b)]	顧客向け公開情報 （識別情報/記載箇所）	補足
IA-1	管理者の認証	M	セキュリティ設定にアクセスする際に管理者の認証を要求する機能をもたなければならない。	管理者の認証機能の説明が顧客向け公開情報に記載されていること。	Y	■識別情報 使用説明書 ■記載箇所 管理者認証を有効にする	
IA-2	デフォルトパスワードの変更	M	1)　管理者の認証に用いるID及び／又はパスワードを変更する機能をもたなければならない。 2)　管理者の認証に用いるID及び／又はパスワードについて，初めてHCDを利用するときに，あらかじめ設定されている管理者ID及び／又はパスワードの変更を促す機能，又はこれに準ずるものをもたなければならない。	1) 管理者ID及び／又はパスワードの変更方法が顧客向け公開情報に記載されていること。	Y	■識別情報 使用説明書 ■記載箇所 標準権限管理者を登録する	
				2) 初めてHCDを利用するときに，あらかじめ設定されている管理者ID及び／又は管理者パスワードの変更を促す機能，又はこれに準ずるものについての説明が顧客向け公開情報に記載されていること。	Y	■識別情報 メーカーホームページ ■記載箇所 複合機/プリンターを安全にご利用いただくために https://www.ricoh.co.jp/mfp/security/setting/	
				3) 管理者の認証にID及び／又はパスワード以外を使用するHCDの場合は，認証方法に関する説明が顧客向け公開情報，又は申請資料に記載されていることによって，この要件を満足するものとみなす。	-	―	
IA-3	認証失敗時のアクション	M	HCD がネットワークインターフェース経由の認証機能をもつ場合は，ネットワークインターフェース経由の認証メカニズムに対する総当たり攻撃を困難にする仕組みを利用できるようにしなければならない。	総当たり攻撃を困難にする仕組みを利用するための方法が顧客向け公開資料，又は申請資料に記述されていること。	Y	■識別情報 使用説明書 ■記載箇所 セキュリティー脅威に対策する	
MT-1	機器のセキュリティ設定管理	M	セキュリティ設定は，管理者だけが設定・変更できるようにしなければならない。	1) セキュリティ設定のリストが申請資料に記載されていること。申請資料に記載するセキュリティ設定のリストは，この規格のセキュリティ機能要件に影響を与えるものに限定してもよい。	Y	■識別情報 セキュリティーリファレンス ■記載箇所 初期設定以外の設定項目の操作権限一覧 ・Web Image Monitor：機器 ・Web Image Monitor：インターフェース ・Web Image Monitor：ネットワーク ・Web Image Monitor：セキュリティー	
				2) セキュリティ設定の設定・変更を管理者だけに限定していることが顧客向け公開情報から読み取れること。	Y	■識別情報 使用説明書 ■記載箇所 標準権限管理者を登録する	
MT-2	セキュリティ設定の初期化	M	HCDの返却や譲渡，廃棄時にセキュリティ設定を初期化できる機能及び／又はセキュリティ設定値を消去する機能をもたなければならない。ただし，ネットワーク経由での初期化及び／又は消去の実施は管理者だけに限定される。	セキュリティ設定を初期化及び／又は消去するための操作方法が顧客向け公開情報に記載されていること。	Y	■識別情報 使用説明書 ■記載箇所 メモリー全消去で本機を初期化する	

ネットワーク機能付き事務機セキュリティガイドライン Ver.1.10 要件チェックシート（2/3）

ネットワーク機能付き事務機セキュリティガイドライン Ver.2.00 要件チェックシート					回答欄		
ID	セキュリティ要件	ステータス[a]	機能要件	確認項目	サポート[b]	顧客向け公開情報 （識別情報/記載箇所）	補足
PT-1	ファームウェアアップデート機能	M	1) HCDのファームウェア及び／又はソフトウェアの現在のバージョンを確認する機能をもたなければならない。 2) HCDのファームウェア及び／又はソフトウェアをアップデートする機能をもたなければならない。ただし，ネットワーク経由でのアップデート機能の実施は管理者だけに限定しなければならない。 3) HCDのファームウェア及び／又はソフトウェアをアップデートする前に，インストールするファームウェアの完全性を検証する機能をもたなければならない。	1) HCDのファームウェア及び／又はソフトウェアのバージョンを確認するための操作方法が顧客向け公開情報，又は申請資料に記載されていること。	Y	■識別情報 本資料 ■記載箇所 右記補足欄	下記手順で確認可能 ・Web Image MonitorのTop画面を開く ・「機器の情報」→「構成」を選択 ・「バージョン」の記載を確認
				2) HCDのファームウェア及び／又はソフトウェアのアップデート処理を開始するための操作方法，又はこれに準ずる手段の説明が顧客向け公開情報，又は申請資料に記載されていること。	Y	■識別情報 メーカーホームページ ■記載箇所 RICOH Firmware Update Tool https://www.ricoh.co.jp/service/firmware-update-tool	
				3) HCDのファームウェア及び／又はソフトウェアをアップデートする前に，インストールするファームウェアの完全性を検証する機能をもつことの説明が，顧客向け公開資料，又は申請資料に記載されていること。	Y	–	–
		R	4) HCDのファームウェア及び／又はソフトウェアのアップデートを確実に実施するために、アップデートを促進する機能，又はこれに準ずる手段を提供することが望ましい。なお，アップデートの適用タイミングは，ユーザーが指示及び／又は設定できることが望ましい。	4) アップデートを促進する機能，又はこれに準ずる手段を提供する場合は，その説明が顧客向け公開資料，又は申請資料に記載されていること。	Y	■識別情報 メーカーホームページ ■記載箇所 RICOH Firmware Update Tool https://www.ricoh.co.jp/service/firmware-update-tool	
DP-1	大容量記憶装置データ保護 （条件付き必須）	MC[c]	HCDが現地交換可能な大容量記憶装置をもつ場合は，大容量記憶装置内にユーザーが供給した情報の内容を，設定又は操作によって利用できなくする機能をもたなければならない。ただし，ネットワーク経由で設定又は操作する場合は，管理者だけに限定される。	1) 大容量記憶装置内のデータが流出することを防ぐための方法が顧客向け公開情報，又は申請資料に記載されていること。 1.1) データを完全消去する機能をもつ場合は，データを完全消去するための指示方法。 1.2) データを暗号化する機能をもつ場合は，暗号化機能を有効化するための指示方法。	Y	■識別情報 使用説明書 ■記載箇所 1. 1）メモリー全消去で本機を初期化する 1. 2）内部ストレージのデータを暗号化する	
				2) 以下のようなHCDで，この要件を必要としない場合は，その理由が顧客向け公開情報，又は申請資料に記載されていること。 2.1) 大容量記憶装置をもたないHCD。 2.2) その他，この要件を必要としない技術を用いた場合は，その手段。	-	—	
TP-1	インターネット通信データ保護 （条件付き必須）	MC[d]	1) インターネットを介して通信する機能をもつ 場合は，暗号通信機能をもたなければならない。 2) 暗号通信機能で使用可能な暗号通信方式とそのバージョンを明確にしなければならない。	1) 暗号通信機能をもつHCDの場合は，以下の項目が顧客向け公開情報，又は申請資料に記載されていること。 1.1) 暗号通信機能をもつ旨。 1.2) サポートする暗号通信方式（TLS等）とそのバージョン。	Y	■識別情報 使用説明書 ■記載箇所 1.1）SSL/TLSで通信を暗号化する 1.2) サポートする暗号通信方式 SSL3.0/TLS1.0/TLS1.1/TLS1.2/TLS1.3	
				2) ルータを越えられないプロトコルしかもっていないHCDで，この要件を必要としない場合は，その理由が顧客向け公開資料，又は申請資料に記載されていること。	-	—	
NI-1	PSTNファクスとネットワーク間の分離 （条件付き必須）	MC[e]	HCDがPSTNファクス機能を備えている場合は，PSTNファクスとネットワークの中継機能がないようにしなければならない。	1) PSTNファクスモデムがファクスプロトコルを用いた利用者データの送信又は受信だけに使用され，ファクスモデム経由のネットワーク通信はできないことが顧客向け公開情報，又は申請資料に記載されていること。	Y	■識別情報 メーカーホームページ ■記載箇所 複合機を取り巻くセキュリティ脅威と対策 -「電話回線からの不正アクセスと対策」 https://www.ricoh.co.jp/mfp/security/countermeasure/	
				2) PSTNファクス機能をもたないHCDで，この要件を必要としない場合は，その理由が顧客向け公開資料，又は申請資料に記載されていること。	-	—	

ネットワーク機能付き事務機セキュリティガイドライン Ver.1.10 要件チェックシート（3/3）

ネットワーク機能付き事務機セキュリティガイドライン Ver.2.00 要件チェックシート					回答欄		
ID	セキュリティ要件	ステータス[a)]	機能要件	確認項目	サポート[b)]	顧客向け公開情報 （識別情報/記載箇所）	補足
CM-1	構成管理	M	構成管理システムを使用し，少なくともバージョン管理によって製品及びその構成要素を一意に識別できなければならない。	構成管理システムを使用し，バージョン管理によって製品及びその構成要素を一意に識別していること。	Y	-	-
PR-1	運用環境	M	外部から保護されたネットワーク内で製品を使用すること，又は管理外のアクセスから保護される，制限された環境又は監視された環境に置かれることをユーザーに促さなければならない。	“外部から保護されたネットワーク内で製品を使用すること，又は管理外のアクセスから保護される，制限された環境又は監視された環境に置かれること” を促す記述が顧客向け公開情報に記載されていること。	Y	■識別情報 使用説明書 ■記載箇所 セキュリティー脅威に対策する	
FR-1	問い合わせ窓口	M	疑わしい脆弱性に対し，ユーザーが報告や問い合わせを行う手段をもたなければならない。	1) 以下のうちいずれか，又は複数が可能なことが顧客向け公開情報，又は申請資料に記載されていること。 1.1) 製造業者及び／又は販売事業者ホームページの問い合わせフォーム。 1.2) 製造業者及び／又は販売事業者への連絡窓口（電話，メール，SNS等）。	Y	■識別情報 メーカーホームページ ■記載箇所 1.1)ホームページの問い合わせフォーム 右記補足欄参照 1.2)メーカーの問い合わせ窓口 https://www.ricoh.co.jp/contact/	・ホームページの問い合わせフォーム https://webform.ricoh.com/form/pub/e00134/vulnerability_inq 上記URLは変更の可能性があるため、左記問い合わせ窓口からお辿りください
FR-2	ファームウェアの提供	M	1)　セキュアなファームウェア及び／又はソフトウェアの利用をユーザーに促さなければならない。 2)　脆弱性が確認された場合に，対策ファームウェア及び／又は対策ソフトウェアを提供する体制をもたなければならない。	1) 脆弱性の対策ファームウェア及び／又は対策ソフトウェアが提供可能であることを知らせる方法として，以下のうちいずれか，又は複数が可能なことが，顧客向け公開情報，又は申請資料に記載されていること。 1.1) 製造業者及び／又は販売事業者のホームページでの告知。 1.2) 製造業者及び／又は販売事業者からの連絡（電話，メール，SNS，訪問等）。	Y	■識別情報 メーカーホームページ ■記載箇所 脆弱性ごとの情報リスト https://jp.ricoh.com/security/products/vulnerabilities	
				2) 脆弱性の対策ファームウェア及び／又は対策ソフトウェアの提供方法として，以下のうちいずれか，又は複数が可能なことが顧客向け公開情報，又は申請資料に記載されていること。 2.1)　製造業者及び／又は販売事業者のホームページからの提供。 2.2)　担当サービスからの提供。 2.3)　ネットワーク経由の配信。	Y	■識別情報 メーカーホームページ ■記載箇所 脆弱性ごとの情報リスト https://jp.ricoh.com/security/products/vulnerabilities	
VA-1	脆弱性スキャナーによる検証	M	脆弱性スキャナーによる検証と検証結果に応じた対応を実施しなければならない。	1) 脆弱性スキャナーによる検証を実施済みであること。	Y	-	-
				2) 脆弱性スキャナーによる指摘に対して，その評価結果に応じた適切な対応を実施済みであること。	Y	-	-
VA-2	未使用TCP/UDPポートのクローズ	M	意図的に開けているもの以外のTCP/UDPポートは閉じなければならない。	1) ポートスキャンによるポート開閉状況の検証を実施済みであること。	Y	-	-
				2) 意図的に開けているポート以外のポートは閉じていることを確認済みであること。	Y	-	-
VA-3	デバッグポートのクローズ	M	開発中にだけ使用するデバッグポートは閉じなければならない。	全てのデバッグポートが閉じていることの確認を実施済みであること。	Y	-	-

注 a)　ステータス欄は，規定の状態を示す。以下の表記を用いる。
M　規定は必須要件である。
MC　規定は必須要件であり，条件付きである。
R　規定は勧告である。
b)　サポート欄は，本ガイドライン適合宣言書の宣言者が記入する
Y　実装によってサポートされる。
N　実装ではサポートされていない。
-　当該規定は適用されない。
c)　大容量ストレージデバイス（HDD/SSD）を内蔵するHCDは必須とする。
d)　インターネットを介して通信する機能をもつHCDは必須とする。
ルータを越えられないプロトコルのみもつHCDの場合は要求しない。
e)　PSTNファクス機能をもつHCDは必須とする。

ネットワーク機能付き事務機セキュリティガイドライン Ver.2.00 適合判定		
	回答欄の確認	☑
	適合判定	適合
	確認日	2025/1/16