資料38－3－2

Information-technology
Promotion
Agency, Japan

CC認証された複合機が保証するセキュリティについて

参照PP: **Protection Profile for Hardcopy Devices Version1.0**

2018年4月27日

情報処理推進機構
技術本部セキュリティセンター

CC認証された複合機が
対策している脅威とセキュリティ機能

CC認証された複合機が想定している脅威

① **他の利用者による不正な操作**
認証突破やバイパスにより利用者本来の権限を越えた不正操作を行う

② **通信データの盗聴、改ざん**
MFPと利用者端末、MFPと他のIT機器間の通信の盗聴、改ざんする

③ **管理機能への不正なアクセス**
脆弱性などを利用して利用者の追加、権限付与、ファームウェア更新などを不正に実行する

④ **複合機のソフトウェアの改ざん・破損**
不正なファームウェアを導入させてマルウェア感染、ボット化させる

⑤ **監査ログの改ざん・不正な削除**
IT機器への通信路や複合機上のログデータを改ざん、削除する

⑥ **複合機内に保存された文書データの漏えい**
MFP廃棄時のHDDやSSDからの情報漏えい

※上記は経産省の「IT製品の調達におけるセキュリティ要件リスト」のMFPに対する脅威

PPで保証されているセキュリティ機能

1. 識別、認証、及び権限付与
管理者によって権限を与えられた利用者のみが、認証（ログイン）後に利用できること

2. アクセス制御
秘密情報や設定機能が、権限を持つ利用者のみにアクセス可能であること

3. データ暗号化
ストレージ（HDDやSSD）のデータは暗号化されていること

4. 高信頼な通信
利用者やログサーバとの通信は暗号化されていること

5. 管理者の役割
利用者の追加、権限付与、ファームウェア更新が管理者しかできないこと

6. 監査
ログが外部のIT機器にセキュアに送られること（MFP上のログ閲覧は管理機能とする）

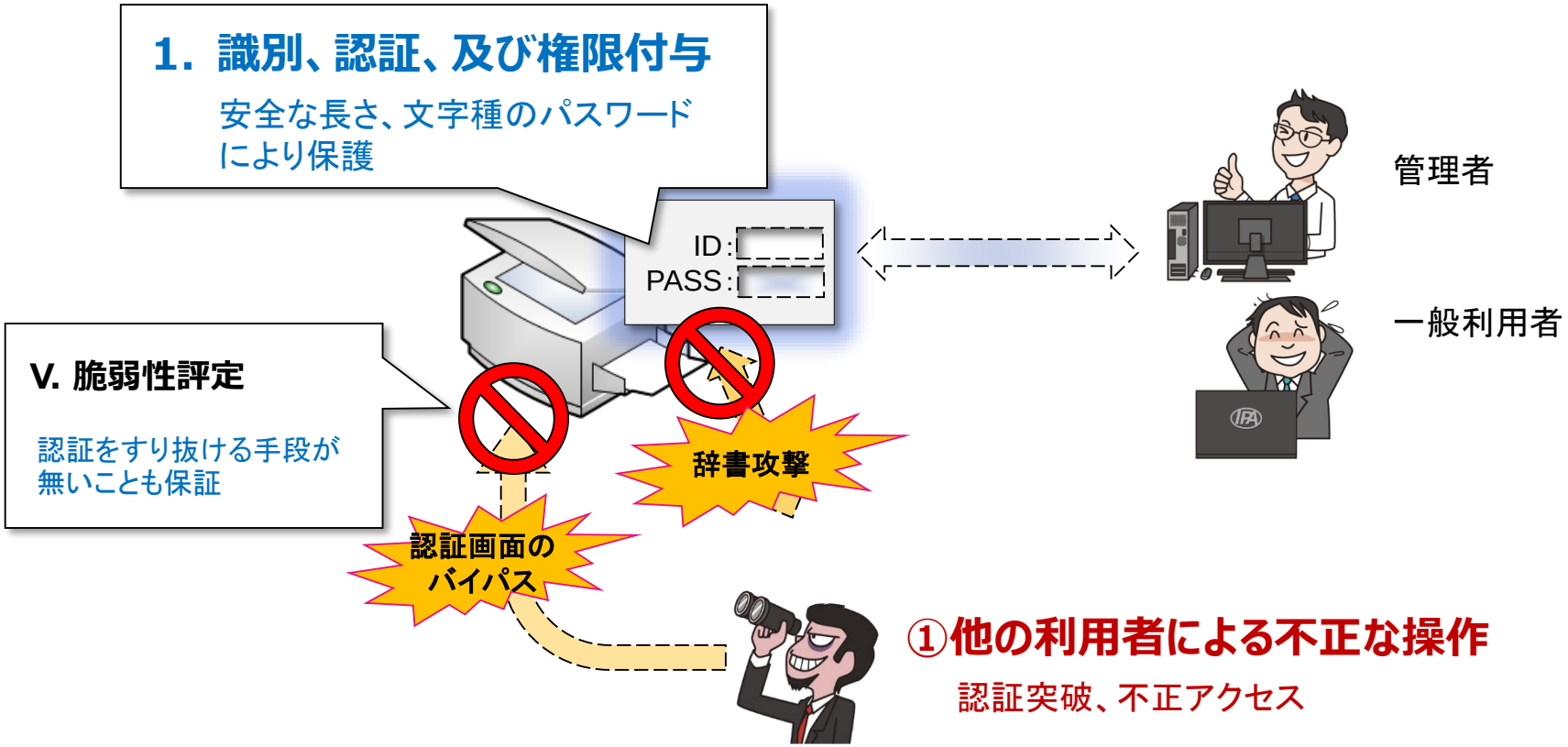
7. 高信頼な運用
署名検証による、セキュアなファームウェアアップデートをすること

＋

V. 脆弱性評定
識別認証のバイパスや、悪用される不要なサービスがないことを検査

脅威vs.セキュリティ機能の例
「①他の利用者による不正な操作」

①他の利用者による不正な操作 に対しては、安全なパスワードが設定されることが**「1.識別、認証、及び権限付与」**で保証されている



PPの記載（セキュリティ機能要件）「１．識別、認証、及び権限付与」

FIA_PMG_EXT.1 Extended: Password Management

パスワードの文字種

Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and the following special characters: [selection: “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”, [assignment: other characters]];

アルファベット大文字、小文字、数字、及び1つ以上の特殊文字（@や！など）がパスワードの文字として設定可能であること

パスワード長

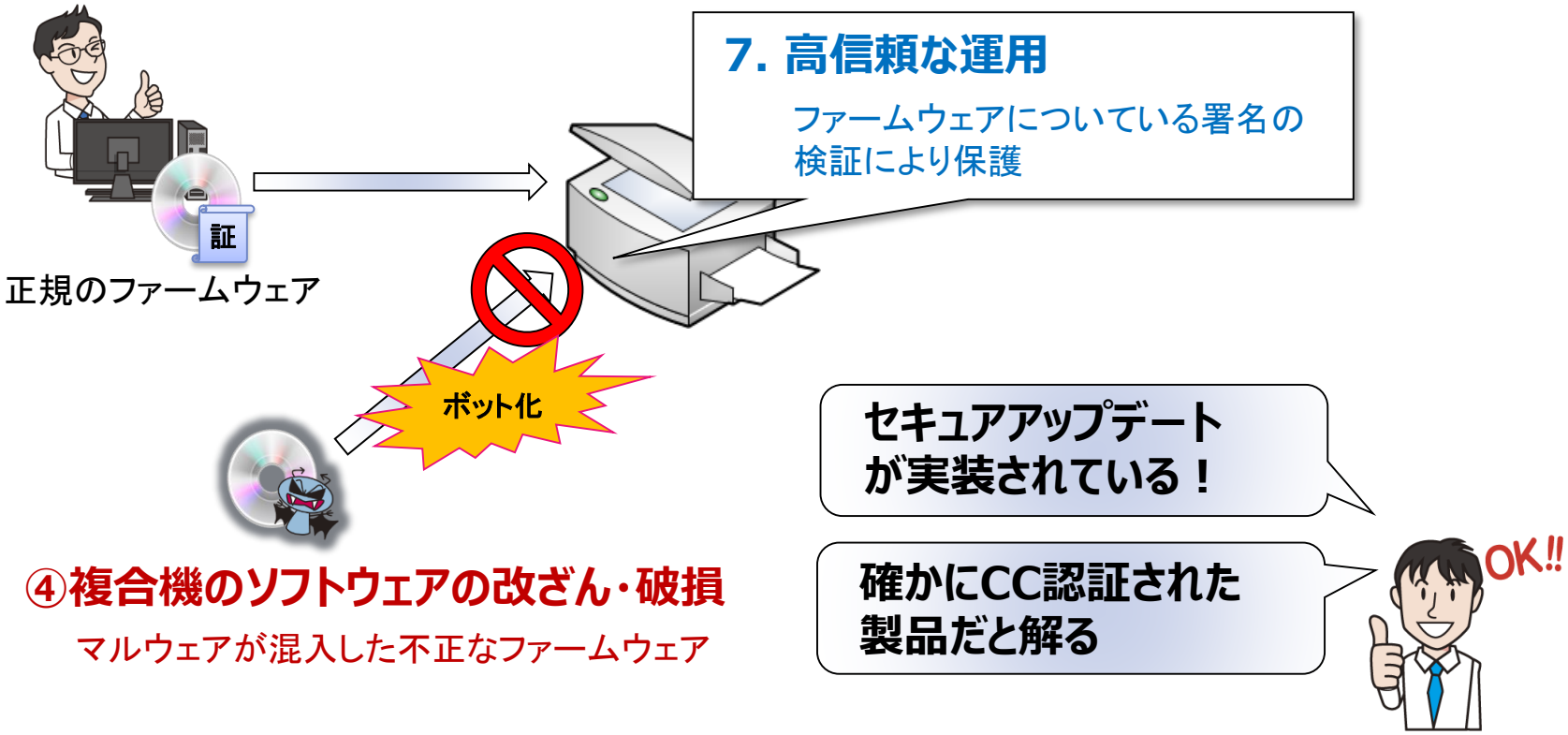
Minimum password length shall be settable by an Administrator, and have the capability to require passwords of 15 characters or greater;

パスワードの最低長を15文字以上に設定可能であること

これらの要件が、間違いなく製品に実装されていることを評価機関がチェック！

脅威vs.セキュリティ機能の例
「④複合機のソフトウェアの改ざん・破損」

④複合機のソフトウェアの改ざん・破損に対しては、インストール時に、署名検証することが**「7. 高信頼な運用」**で保証されている

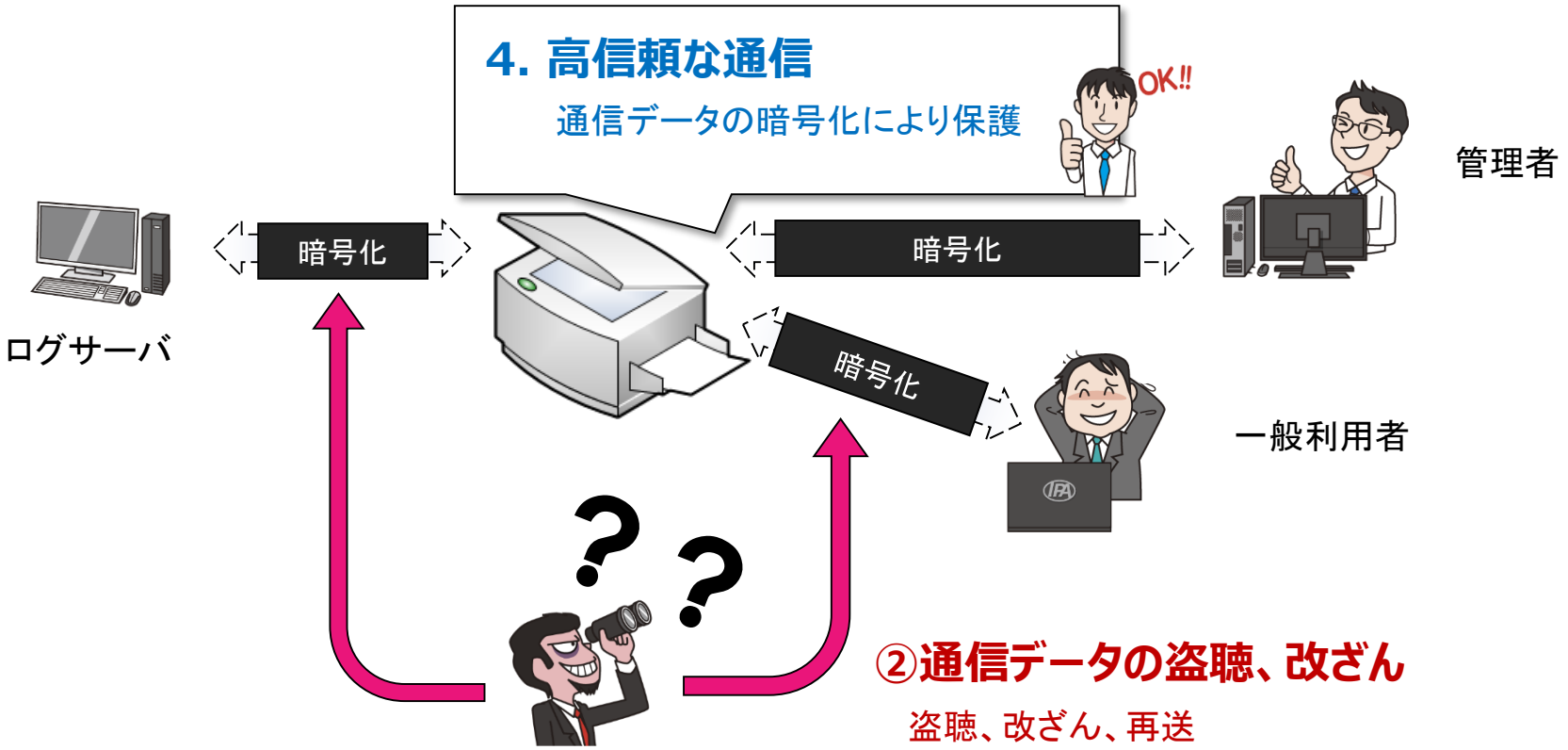


④複合機のソフトウェアの改ざん・破損

マルウェアが混入した不正なファームウェア

脅威vs.セキュリティ機能の例
「②通信データの盗聴、改ざん」

②通信データの盗聴、改ざんに対しては、複合機と利用者やログサーバ間の通信が暗号化されることが**「4. 高信頼な通信」**で保証されている



参考情報
セキュリティ機能要件

セキュリティ機能要件（SFR）の例
「１．識別、認証、及び権限付与」

FIA_PMG_EXT.1 Extended: Password Management

パスワードの文字種

Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and the following special characters: [selection: “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”, [assignment: other characters]];

アルファベット大文字、小文字、数字、及び1つ以上の特殊文字（@や！など）がパスワードの文字として設定可能であること

パスワード長

Minimum password length shall be settable by an Administrator, and have the capability to require passwords of 15 characters or greater;

パスワードの最低長を15文字以上に設定可能であること

その他

FIA_AFL.1：ログインパスワードを一定回数間違った際にロックなどを行うこと

2. アクセス制御 の主なSFR

Class FDP: User Data Protection

アクセス制御

The TSF shall enforce the User Data Access Control SFP on subjects, objects, and operations among subjects and objects specified in Table 2 and Table 3.

以下のポリシーに従ってアクセス制御できること

（抜粋）

	操作:	プリントされる文書を投入	画像を閲覧またはプリント結果を出力	保存された文書を改変	保存された文書を削除
プリント	所有者				
	識別及び認証された管理者				
	識別及び認証された一般利用者		拒否	拒否	拒否
	未認証		拒否	拒否	拒否

	操作:	スキャンする文書を投入	スキャンされた画像を閲覧	保存された文書を改変	保存された文書を削除
スキャン	所有者				
	識別及び認証された管理者				
	識別及び認証された一般利用者		拒否	拒否	拒否
	未認証	拒否	拒否	拒否	拒否

3. データ暗号化　の主なSFR

FCS_COP.1(d) Cryptographic operation (AES Data Encryption/Decryption)

特定された暗号アルゴリズムでの暗号化

ストレージに保存するデータを処理する暗号アルゴリズムを定義すること

FDP_DSK_EXT.1 Extended: Protection of Data on Disk

交換可能なストレージの暗号化

The TSF shall [selection: perform encryption in accordance with FCS_COP.1(d), use a self-encrypting Field-Replaceable Nonvolatile Storage Device that is separately CC certified to conform to the FDE EE cPP] such that any Field-Replaceable Nonvolatile Storage Device contains no plaintext User Document Data and no plaintext confidential TSF Data.

ストレージに保存する秘密データは暗号化すること

FCS_COP.1(a) Cryptographic Operation (Symmetric encryption/decryption)

特定された暗号アルゴリズムでの暗号化

高信頼な通信でつかわれる暗号アルゴリズムを定義すること

4. 高信頼な通信　の主なSFR

FTP_TRP.1 Trusted path　（管理者／一般理利用者）

高信頼パス

The TSF shall use [selection, choose at least one of: IPsec, SSH, TLS, TLS/HTTPS] to provide a trusted communication path between itself and remote administrators/users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from disclosure and detection of modification of the communicated data.

利用者端末のアプリとの通信には暗号通信プロトコルを使用すること（接続先識別、暗号化、改ざん検知のため）

FTP_ITC.1 Inter-TSF trusted channel

高信頼チャネル

認証サーバ等、信頼する**IT機器との通信**には暗号通信プロトコルを使用すること

5. 管理者の役割　の主なSFR

FMT_SMF.1 Specification of Management Functions

管理機能の定義

The TSF shall be capable of performing the following management functions: [assignment: list of management functions provided by the TSF].

管理機能（利用者の追加/変更/削除、ソフトウェアアップデートなど）**を定義すること**

FMT_MOF.1 Management of security functions behavior

（管理）機能の許可

The TSF shall restrict the ability to [selection: determine the behaviour of, disable, enable, modify the behaviour of] the functions [assignment: list of functions] to U.ADMIN.

定義した**管理機能の操作を、管理者のみに許可すること**

6. 監査　の主なSFR

FAU_GEN.1 Audit data generation

監査データの生成

利用者認証失敗、管理機能の利用、及びログサービスの停止といったログを監査データとして生成すること

FAU_STG_EXT Extended: External Audit Trail Storage

管理機能の定義

The TSF shall be able to transmit the generated audit data to an External IT Entity using a trusted channel according to FTP_ITC.1.

監査データは、高信頼チャネルを使って外部のIT機器（syslogサーバ）に送付すること

オプション：C.1 Internal Audit Log Storage

MFP内部への監査データを保存する場合の要件

・MFP内部へ保存した**監査データは、管理者だけが読み出せること**

7. 高信頼な運用 の主なSFR

FAU_STG_EXT Extended: External Audit Trail Storage

現在のバージョンの表示

The TSF shall provide authorized administrators the ability to query the current version of the TOE firmware/software.

管理者がTOEのファームウェアの現在のバージョンを確認できること

セキュアなアップデート

The TSF shall provide authorized administrators the ability to initiate updates to TOE firmware/software.

The TSF shall provide a means to verify firmware/software updates to the TOE using a digital signature mechanism and [selection: published hash, no other functions] prior to installing those updates.

ファームウェアのアップデート前に署名検証を行うこと

V. 脆弱性評定

セキュリティ機能をバイパス、停止、改ざんできないことを保証している