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

Security Guidelines for Business Machines with Network Functions

Ver.1.10

令和 04 年 09 月改正
（Sep, 2022）

一般社団法人　ビジネス機械・情報システム産業協会
Japan Business Machine and Information System Industries Association

BMSec 運営委員会　委員構成表

(委員長)	萩 原 豊 隆	セイコーエプソン株式会社
(プリ複部会代表)	赤 池 彰 俊	富士フイルムビジネスイノベーション株式会社
(情セキ委代表)	松 田 誠	ブラザー工業株式会社
(企画推進 G 代表)	今 泉 広 海	富士フイルムビジネスイノベーション株式会社
(技術推進 G 代表)	佐 藤 俊 至	東芝テック株式会社
	千 葉 徳 聰	キヤノン株式会社
	大 矢 隆 一 郎	富士フイルムビジネスイノベーション株式会社
	柳 哲	ブラザー工業株式会社
	松 田 宗 久	ブラザー工業株式会社
	山 田 章 広	ブラザー工業株式会社
	角 谷 正 樹	コニカミノルタ株式会社
	羽 賀 達 由	コニカミノルタ株式会社
	藤 井 律 雄	コニカミノルタ株式会社
	佐 藤 公 俊	沖電気工業株式会社
	斎 藤 裕	株式会社リコー
	太 田 雄 介	株式会社リコー
	小 川 昌 宏	株式会社リコー
	神 保 潤 哉	株式会社リコー
	佐 藤 淳 一	理想科学工業株式会社
	曽 根 正 樹	京セラドキュメントソリューションズ株式会社
	金 川 彰 宏	京セラドキュメントソリューションズ株式会社
	中 村 一 男	セイコーエプソン株式会社
	仁 木 祐 司	セイコーエプソン株式会社
	藤 田 房 之	シャープ株式会社
	東 田 恭 子	シャープ株式会社
（事務局）	村 本 光 男	一般社団法人 ビジネス機械・情報システム産業協会
	小 林 信 昭	一般社団法人 ビジネス機械・情報システム産業協会

制　　定：令和 03 年 6 月 14 日
改　　正：令和 04 年 11 月 21 日
原案作成：一般社団法人 ビジネス機械・情報システム産業協会　情報セキュリティ委員会

本書は、改正に伴い JBMIA が管理・運営するビジネス機械・情報システム産業協会規格 （ 以下、JBMS という。）から廃止され、BMSec 運営委員会が管理・運営します。

本書についての意見又は質問は，お問い合わせフォームより一般社団法人 ビジネス機械・情報システム産業協会 BMSec 運営委員会 へお寄せください。

お問い合わせ　https://bmsec.jbmia.or.jp/contact/

目　次

まえがき
Foreword

この規格は，著作権法で保護対象となっている著作物である。

この規格の一部が，特許権，出願公開後の特許出願又は実用新案権に抵触する可能性があることに注意を喚起する。一般社団法人　ビジネス機械・情報システム産業協会は，このような特許権，出願公開後の特許出願及び実用新案権に関わる確認について，責任はもたない。

This standard is copyrighted work protected by copyright laws.

Attention should be drawn to the possibility that a part of this Standard may conflict with a patent right, application for a patent right after opening to the public or utility model right which have technical properties. The Japan Business Machine and Information System Industries Association is not responsible for identifying the patent right, application of a patent right after opening to the public and utility model right which have the technical properties of this kind.

ビジネス機械・情報システム産業協会規格
Japan Business Machine and Information
System Industries Association Standard

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

Security Guidelines for Business Machines with Network Functions
Ver.1.10

序文（Introduction）

この規格は，ネットワーク機能をもつ一般オフィス／スモールオフィス／ホームオフィスユーザー向けのプリンター，スキャナー，ファクス，デジタルコピー機，デジタル複合機等のHard Copy Device（HCD）の購入者が必要とする基本的なセキュリティ要件を定義するものである。

This standard defines the basic security requirements for purchasers of hard copy devices (HCDs) with network functions such as printers, scanners, fax machines, digital copiers, and digital multi-function machines for general office/small office/home office users.

1　適用範囲（Scope）

この規格で規定するガイドラインは，ネットワーク機能をもつ一般オフィス／スモールオフィス／ホームオフィスユーザー向けのプリンター，スキャナー，ファクス， デジタルコピー機，デジタル複合機等の HCD に適用できる。

The guidelines defined in this standard can be applied to HCD with network functions such as printers, scanners, fax machines, digital copiers, and digital multi-function machines for general office/small office/home office users.

2　用語及び定義

この規格で用いる主な用語及び定義は，次による。

2.1

HCD

Hard Copy Device の略語。この規格が対象とするネットワーク機能をもつプリンター，スキャナー，ファクス，デジタルコピー機，デジタル複合機の総称。

2.2

申請資料

適合宣言書，要件チェックシート，及びその補足資料からなる。JBMIA のウェブサイト内で公開される。要件チェックシートでは，証拠資料となる顧客向け公開情報を参照する。

2.3

顧客向け公開情報

この規格で要求するセキュリティ要件に関する機能説明や利用方法を記載した取扱説明書，カタログ，公式ウェブサイト等の顧客向け公開資料。HCD 及び／又は PC 上の管理ツールが GUI や WEB UI などの画面に表示する操作方法の案内を含む。

2.4

要件チェックシート

この規格で要求するセキュリティ要件を満足していることを顧客に周知するためにベンダーが作成する申請資料の一つ。顧客向け公開資料に記載するには適さないと思われる内容を記載する。別紙の補足資料を参照できる。

2.5

補足資料

要件チェックシートから参照され，別紙として提供される申請資料。 HCD 及び／又は PC 上の管理ツールが GUI や WEB UI の画面に操作方法の案内を表示する場合は，画面キャプチャ等を補足資料とすることで，HCD 操作時の状況を確認できるようにする。

2.6

セキュリティ設定

この規格におけるセキュリティ機能要件に影響を与える設定。セキュリティ設定には，ネットワーク接続に関わる設定や時刻に関わる設定なども含まれる。

2.7

識別

HCD が管理対象とする複数のアカウントの中から，管理者やユーザーを一意に特定すること。複数アカウントを想定しない HCD の場合は，識別機能をもたない。

2.8

認証

管理者やユーザーが本人であることを証明すること。

2.9

管理者

HCD の一部又は全体を管理する権限を持ち，そのアクションが HCD セキュリティ方針に影響を与える利用者。

2.10

一般ユーザー

デバイスを使用する権限はあるが，セキュリティ設定を構成又は変更する権限はないユーザー。

2.11

完全性

データや情報が正確であるということ。改ざんや欠落がないことを示す。

2.12

デジタル署名

データからハッシュ関数を使ってダイジェストを生成し，自分の秘密鍵で暗号化したもの。デジタル署名に公開鍵暗号技術を適用することで，データの完全性を検証することができる。

2.13

ウェアレベリング

SSD（Solid State Drive）等に用いられるフラッシュメモリの記憶素子には書き換え限度回数が存在する。そのため特定の記憶素子に書き込みが集中しないように書き込み位置を分散させる。この分散技術をウェアレベリングと呼ぶ。コントローラによって書き込み位置が分散するため，論理的な削除を行うことで削除データの復元は困難となる。

2.14

脆弱性

HCD のセキュリティを損なうような弱点の存在，設計や実装におけるセキュリティ上の欠陥。ソフトウェアの脆弱性以外に，セキュリティ上の設定が不備な状態においても，脆弱性があるといわれることがある。

2.15

脅威

セキュリティ上のリスクを発生させる要因。脅威と脆弱性がむすびつくとセキュリティ上のリスクが生じる。

2.16

ファームウェア

電子機器の動作を制御するため，本体内に組み込まれたソフトウェア。

2.17

ファイアウォール

外部ネットワークと内部ネットワークの間に設けられ，通信を許可するか否かを判断するソフトウェアやハードウェアシステムであり，内部ネットワークへの不正アクセスを防止することができる。

2.18

PSTN

Public Switched Telephone Networks の略で，公衆交換電話網のこと。 HCD では PSTN ファクスモデム（ファクスを電話網に接続するための送受信装置）の接続先になる。

2. 19

構成管理システム

電子機器を構成するハードウェア，ソフトウェアをバージョン管理するシステム。

2.20

ネットワーク機能

この規格におけるネットワーク機能とは，インターネット層に IP を使用し，トランスポート層で TCP 及び／又は UDP を使用するネットワークサービス機能をいう。なお，この規格では，ネットワークインターフェイス層の実現方法（有線 LAN，無線 LAN など）は規定しない。

3 セキュリティ機能要件

3.1 概要

この規格で規定するセキュリティ機能要件は，次による。条件付き必須要件は，該当する機能が製品仕様に含まれる場合は必須となる。

a) 識別認証機能

b) セキュリティ管理機能

c) ファームウェアアップデート機能

d) 大容量記憶装置データ保護（条件付き必須）

e) インターネット通信データ保護要件（条件付き必須）

f) PSTN ファクスとネットワーク間の分離（条件付き必須）

3.2 識別認証機能

3.2.1 管理者の認証

a) 要件 ID：IA-1

b) 機能要件

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つこと。

c) 対抗すべき脅威又は従うべきポリシー

権限のない第三者が不正に HCD のセキュリティ設定にアクセスし， セキュリティ設定を変更することによって，HCD 内のデータが漏えい及び／又は改ざんされる懸念がある。

d) 確認項目

管理者の認証機能の説明が顧客向け公開資料に記載されていること。

e) 適用上の注意点

1) 管理者を一意に識別する機能は要求しない（例えば，管理者アカウントを指定しないパスワード確認だけでも可）。

2) 開示が許容されるセキュリティ設定への参照に関しては，管理者の認証は要求しない。

3) 管理者でない一般ユーザーの識別認証機能については要求しない。

4) この要件はネットワーク経由でセキュリティ設定にアクセスする場合に要求される。パネルからのアクセスについては要求しない。ネットワーク経由のセキュリティ設定へのアクセスを提供しない場合は，この要件を満足するものとみなす。

3.2.2 デフォルトパスワードの変更

a) 要件 ID：IA-2

b) 機能要件

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つこと。

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つこと。

c) 対抗すべき脅威又は従うべきポリシー

権限のない第三者が容易に管理者 ID 及び／又はパスワードを推定して管理者として認証を行い，セキュリティ設定を変更することによって， HCD 内のデータが漏えい及び／又は改ざんされる懸念がある。

d) 確認項目

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。

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。

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資料，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。

e) 適用上の注意点

1) この要件は HCD が ID 及び／又はパスワードを管理する場合に要求される。HCD が ID 及び／又はパスワードを管理せず，ID 及び／又はパスワード以外の認証手段（デジタル署名等），あるいは外部の認証サーバー等を利用する場合は，この要件は適用されない。

2) 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に準ずるものとは，以下のようなものを想定する。

2.1) ID 及び／又はパスワードを初期値から変更するよう顧客向け公開資料に記載されている。

2.2) HCD の個々の機器ごとに異なる ID 及び／又はパスワードが付されている。

3) この要件はネットワーク経由でセキュリティ設定にアクセスする場合に要求される。パネルからのアクセスについては要求しない。ネットワーク経由のセキュリティ設定へのアクセスを提供しない場合は，この要件を満足するものとみなす。

3.3 セキュリティ管理機能

3.3.1 機器のセキュリティ設定管理

a) 要件 ID：MT-1

b) 機能要件

セキュリティ設定は，管理者だけが設定・変更できること。

c) 対抗すべき脅威又は従うべきポリシー

権限のない第三者が製品のセキュリティ設定を変更することで，セキュリティ機能が正常に働かなくなり，HCD 内のデータが漏えい及び／又は改ざんされる懸念がある。

d) 確認項目

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。

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資料から読み取れること。

e) 適用上の注意点

この要件はネットワーク経由でセキュリティ設定にアクセスする場合に要求される。パネルからのアクセスについては要求しない。ネットワーク経由のセキュリティ設定へのアクセスを提供しない場合は，この要件を満足するものとみなす。

3.3.2 セキュリティ設定の初期化

a) 要件 ID：MT-2

b) 機能要件

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をもつこと。ただし，ネットワーク経由での初期化の実施は管理者だけに限定される。

c) 対抗すべき脅威又は従うべきポリシー

HCD の返却や譲渡，廃棄等で手元を離れた後，攻撃者が HCD のセキュリティ設定情報を読み出し，その情報を基にユーザーのネットワークに不正アクセスを行い，ユーザー情報が漏えい及び／又は改ざんされる懸念がある。

d) 確認項目

セキュリティ設定を初期化するための操作方法が顧客向け公開資料に記載されていること。

e) 適用上の注意点

ネットワーク経由での初期化が PC 上の管理ツールで実現される場合は，該当機能を実行する前に，管理ツールの利用者は管理者として認証されなければならない。

3.4 ファームウェアアップデート機能

a) 要件 ID：PT-1

b) 機能要件

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つこと。

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つこと。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される。

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。

c) 対抗すべき脅威又は従うべきポリシー

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できなければ，機器に内在する脆弱性を管理者が把握できない。

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機能がなければ，脆弱性が発見された場合に対処できない。

3) HCD のファームウェア及び／又はソフトウェアの完全性を検証できないと，壊れたファームウェア及び／又はソフトウェアのインストールを排除できない。

d) 確認項目

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資料，又は申請資料に記載されていること。

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代替手段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。

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。

e) 適用上の注意点

1) 管理者の代わりに，自動化されたアップデート機能又はサービスマンによるアップデートで代替できてもよい。自動アップデートの機能がある場合は，現在バージョンの確認機能に関する要件（機能要件 1) ）は適用されない。なお，ネットワーク経由でのアップデート機能が PC 上の管理ツールで実現される場合は，該当機能を実行する前に，管理ツールの利用者は管理者として認証されなければならない。

2) ファームウェア及び／又はソフトウェアが正しいことの検証手段は，デジタル署名を使うことが望ましい。

3) ファームウェア及び／又はソフトウェアが正しいことの検証の結果，正しくない場合はエラー表示する，もしくはアップデートを止めること。

3.5 大容量記憶装置データ保護（条件付き必須）

a) 要件 ID：DP-1

b) 機能要件

HCD が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つこと。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。

c) 対抗すべき脅威又は従うべきポリシー

HCD の返却や譲渡，廃棄等で手元を離れた後，攻撃者が大容量記憶装置を取り外して，PC 等を使って大容量記憶装置内のデータを読み出す懸念がある。

d) 確認項目

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資料，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。

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資料，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。

e) 適用上の注意点

1) この要件は，HDD/SSD を対象にする。基板上に実装されるなどして，通常，取り外すことができない不揮発性メモリには適用しない。

2) 大容量記憶装置内のデータを利用できなくする方法として，“暗号化”及び／又は“完全消去”が適用可能である。

3) 大容量記憶装置内のデータを完全消去する機能として，HDD の場合は上書き消去が適用可能である。SSD の場合はウェアレベリング機能を持つため論理的な削除機能（FAT 情報の削除）をもって完全消去の手段と見なす。

4) データを利用できなくする方法を PC 上の管理ツールを用いてネットワーク経由で操作する場合は，該当機能を実行する前に，管理ツールの利用者は管理者として認証されなければならない。

5) 管理者の許可を受けたサービスマンによる設定又は操作によって，大容量記憶装置内のデータを利用できなくする方法の場合も，この要件を満足するものとみなす。

6) USB メモリや SD メモリカードなどの外部インターフェイスポートを介して接続する記録メディアに対しては，この要件は適用しない。

3.6 インターネット通信データ保護（条件付き必須）

a) 要件 ID：TP-1

b) 機能要件

1) インターネットを介して通信する機能をもつ場合は，暗号通信機能をもつこと。

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すること。

c) 対抗すべき脅威又は従うべきポリシー

外部の通信経路には悪意のあるユーザーが存在し，ネットワークデータが漏えい及び／又は改ざんされる懸念がある。

d) 確認項目

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資料，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。

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。

e) 適用上の注意点

1) ルータを越えられないプロトコルしかもっていない HCD の場合は，暗号通信機能を要求しない。

2) この要件は，インターネット層以上の階層での暗号通信機能を要求しており，Wi-Fi については規定しない。Wi-Fi 環境については，Wi-Fi アライアンスが推奨している暗号化プロトコルや暗号アルゴリズムを使用し，脆弱な暗号化プロトコルや暗号化アルゴリズムが使用されていないことを前提としている。

3.7 PSTN ファクスとネットワーク間の分離（条件付き必須）

a) 要件 ID：NI-1

b) 機能要件

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こと。

c) 対抗すべき脅威又は従うべきポリシー

ファクスとネットワークが分離されていない場合は，PSTN ファクスモデムを経由して，攻撃者が保護されたネットワーク環境に侵入する可能性がある。このようなファイアウォール又はその他の外部保護を迂回する不正アクセスによって，データ漏えい及び／又は改ざんされる懸念がある。

d) 確認項目

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資料，又は申請資料に記載されていること。

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。

e) 適用上の注意点

この要件は，PSTN ファクス機能をもつHCDに適用される。

4 セキュリティ保証要件

4.1 概要

この規格で規定するセキュリティ保証要件は，次による。

a) 構成管理

b) 運用環境

c) 欠陥修正

4.2 構成管理

a) 要件 ID：CM-1

b) 保証要件

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していること。

c) 対抗すべき脅威又は従うべきポリシー

製品の構成要素であるファームウェア及び／又はソフトウェアについてバージョン管理による構成管理が行われていないと脆弱性への対策が十分に行われなくなる懸念がある。

d) 確認項目

申請資料で本要件（CM-1）が“適用”となっていることを確認する。具体的な構成管理システムを明示する必要はない。

e) 適用上の注意点

ファームウェア及び／又はソフトウェアを含む製品の構成部品について，構成管理システムによるバージョン管理を行っていれば，本要件を満たす。

4.3 運用環境

a) 要件 ID：PR-1

b) 保証要件

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していること。

c) 対抗すべき脅威又は従うべきポリシー

インターネットに直接接続された場合は，外部の攻撃者による不正アクセスの脅威に晒される。こうした脅威を取り除くために，ファイアウォールが設置されるなど，外部から保護されたネットワークで利用されることが重要である。

d) 確認項目

“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資料に記載されていること。ユーザーが容易に理解できるようにファイアウォールを例示するなどしてもよい。

e) 適用上の注意点

本ガイドラインでは、管理者は特権的なアクセス権を悪意のある目的のために使用せず、製品が監視された環境に置かれることを想定している。

4.4 欠陥修正

4.4.1 問い合わせ窓口

a) 要件 ID：FR-1

b) 保証要件

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があること。

c) 対抗すべき脅威又は従うべきポリシー

脆弱性の報告，問い合わせ窓口がないと脆弱性への対策が遅れる懸念がある。

d) 確認項目

1) 以下のうちいずれか又は複数が可能なことが，顧客向け公開資料，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）。個別の脆弱性専用の窓口である必要はない。電話・メール等を用いた一般的なユーザー問い合わせ窓口であっても本要件を満たす。

e) 適用上の注意点

なし。

4.4.2 ファームウェアの提供

a) 要件 ID：FR-2

b) 保証要件

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していること。

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があること。

c) 対抗すべき脅威又は従うべきポリシー

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を利用しない場合は，セキュアでない状態で製品が使用され続けることによって，情報漏えいなどに繋がる懸念がある。

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を提供する体制がないと，脆弱性の対策を行うことができず，セキュアでない状態で製品が使用され続けることによって，情報漏えいなどに繋がる懸念がある。

d) 確認項目

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，以下のいずれか又は複数が可能なことが，顧客向け公開資料，又は申請資料に記載されていること。

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）。

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，以下のいずれか又は複数が可能なことが，顧客向け公開資料，又は申請資料に記載されていること。

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。

e) 適用上の注意点

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とは，提供可能であることの通知と対策ファームウェア及び／又は対策ソフトウェアそのものの提供を意味する。

5 脆弱性評定

5.1 概要

この規格で規定する脆弱性評定の要件は，次による。

a) 脆弱性スキャナーによる検証

b) 未使用 TCP/UDP ポートのクローズ

c) デバッグポートのクローズ

5.2 脆弱性スキャナーによる検証

a) 要件 ID：VA-1

b) 保証要件

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ていること。

c) 対抗すべき脅威又は従うべきポリシー

脆弱性が残存していると，サイバー攻撃に悪用される懸念がある。

d) 確認項目

1) 脆弱性スキャナーによる検証が実施済みである旨が申請資料に記載されていること。

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が実施済みである旨が申請資料に記載されていること。使用する脆弱性スキャナーツールによって，脆弱性検出レベルが異なるため脆弱性スキャナーの種別，及びスキャン結果に対する対応レベルについては規定しない。脆弱性スキャンの実施，及びスキャン結果に対する対応判断の実施を宣言することで，本要件が満たされたと見なす。

e) 適用上の注意点

なし。

5.3 未使用 TCP/UDP ポートのクローズ

a) 要件 ID：VA-2

b) 保証要件

意図的に開けているもの以外の TCP/UDP ポートは閉じていること。

c) 対抗すべき脅威又は従うべきポリシー

未使用ポートが開いている（通信可能な状態となっている）と，サイバー攻撃に悪用される懸念がある。

d) 確認項目

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旨が申請資料に記載されていること。

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旨が申請資料に記載されていること。

e) 適用上の注意点

HCD で使用する TCP/UDP ポートを規定し，使用していないポートを閉じる。

5.4 デバッグポートのクローズ

a) 要件 ID：VA-3

b) 保証要件

開発中にだけ使用するデバッグポートは閉じていること。

c) 対抗すべき脅威又は従うべきポリシー

デバッグポートが開いている（通信可能な状態となっている）と，サイバー攻撃に悪用される懸念がある。

d) 確認項目

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旨が申請資料に記載されてい

ること。

e) 適用上の注意点

1) 容易にアクセスできる場所（外部に露出している，又は工具を使わないで着脱可能なカバーで囲われているなど）にデバッグポート用コネクタがある場合は，使用できないようソフト的に禁止されていること。

2) デバッグポート用コネクタがない場合，又は容易にアクセスできない場所にデバッグポート用コネクタがある場合は，ソフト的に禁止されていなくても，この要件を満足するものとみなす。

附属書 A
（参考）
適合宣言書

A.1 目的

適合宣言書は，HCD の開発又は製造に関与する事業者が，HCD の購入者に対して，宣言の対象製品が“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”の要求事項に適合していることを証明するものである。

A.2 適合宣言書書式

表 A.2.1－ガイドライン適合宣言書

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 適合宣言書		
本製品は，一般社団法人　ビジネス機械・情報システム産業協会が定めた“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”に準拠して開発されています。		
申請者		
適合宣言者		
申請日		
製品分類		
製品名		
ファームウェアバージョン a)		
機能概要	（例）本製品は，コピー，スキャン，プリント，ファクス，文書の保存と取り出し機能を備えたネットワーク機能をもつデジタル複合機である。	
搭載機能	サポート	備考
プリント機能		
スキャン機能		
ファクス機能		
コピー機能		
インターネット通信機能		
大容量ストレージ機能		
注 a) このバージョンと、これより新しいバージョンが“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”に適合する。		

表 A.2.2－ガイドライン実施状況

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 実施状況					
分類	参照 a)	要件 ID	機能要件	ステータス b)	サポート c)
セキュリティ機能要件	3.2.1	IA-1	管理者の認証	M	
	3.2.2	IA-2	デフォルトパスワードの変更	M	
	3.3.1	MT-1	機器のセキュリティ設定管理	M	
	3.3.2	MT-2	セキュリティ設定の初期化	M	
	3.4	PT-1	ファームウェアアップデート機能	M	
	3.5	DP-1	大容量記憶装置データ保護	MC d)	
	3.6	TP-1	インターネット通信データ保護	MC e)	
	3.7	NI-1	PSTN ファクスとネットワーク間の分離	MC f)	
セキュリティ保証要件	4.2	CM-1	構成管理	M	
	4.3	PR-1	運用環境	M	
	4.4.1	FR-1	問い合わせ窓口	M	
	4.4.2	FR-2	ファームウェアの提供	M	
脆弱性評定	5.2	VA-1	脆弱性スキャナーによる検証	M	
	5.3	VA-2	未使用 TCP/UDP ポートのクローズ	M	
	5.4	VA-3	デバッグポートのクローズ	M	

注 a) 参照欄は，この規定の箇条番号を示す。
b) 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　規定は条件付き必須要件である。
c) 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（条件付き必須要件の規定で，当該条件が当該製品に適用されないと判断された場合にだけ適用される）。
d) 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。
e) 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だけもつ HCD の場合は要求しない。
f) PSTN ファクス機能をもつ HCD は必須とする。

表 A.2.3－ガイドライン適合宣言書資料確認

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 適合宣言書資料確認	**表 A.2.1**－ガイドライン適合宣言書　記載事項確認	□
	表 A.2.2－ガイドライン実施状況　記載事項確認	□
	確認日	

附属書 B
（参考）
要件チェックシート

B.1　要件チェックシート

このチェックシートの目的は，HCD の開発又は製造に関与する事業者が，HCD の購入者に対して“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”の実施状況に関する情報を提供するための仕組みを提供することである。

表 B.1.1－事務機セキュリティガイドライン Ver1.10 要件チェックシート

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				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／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つこと。	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。		
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つこと。 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つこと。	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。 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。 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。		
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・変更できること。	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。 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。		
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をもつこと。ただし，ネットワーク経由での初期化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。		

表 B.1.1－事務機セキュリティガイドライン要件 Ver.1.10 チェックシート（続き）

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／ 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つこと。 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つこと。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される。 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。	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資料，又は申請資料に記載されていること。 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代替手段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。 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。		
DP-1 大容量記憶装置 データ保護 （条件付き必須）	MC c)	HCD が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つこと。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。 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，暗号通信機能をもつこと。 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すること。	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。 2) ルータを越えられないプロトコルしか持っていない 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。		

表 B.1.1－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（続き）

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／ 補足
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こと。	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。 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。		
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していること。	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。		
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していること。	“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。		
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があること。	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）。		
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していること。 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があること。	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）。 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。		

表 B.1.1－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（続き）

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／ 補足
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ていること。	1)　脆弱性スキャナーによる検証が実施済みである旨が申請資料に記載されていること。 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。		
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 ポートは閉じていること。	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。 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。		
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ていること。	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。		

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　規定は条件付き必須要件である。
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(条件付き必須要件の規定で，当該条件が当該製品に適用されない場合)
c) 大容量ストレージデバイスを内蔵する 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場合は必須とする。ルータを越えられないプロトコルだけもつ HCD の場合は要求しない。
e) PSTN ファクス機能をもつ HCD の場合は必須とする。

表 B.1.2－ガイドライン適合判定

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 適合判定	回答欄の確認	
	適合判定	
	確認日	

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
解　説

この解説は，本体及び附属書に規定・記載した事柄を説明するもので，規格の一部ではない。

1　制定の趣旨

この規格は，ネットワーク機能付き事務機の購入者が必要とする基本的なセキュリティ要件を定義したものである。この規格で定めるガイドラインは，ネットワーク機能を有する一般オフィス／SOHO 向けのプリンター，スキャナー，ファクス， デジタルコピー機，デジタル複合機等の HCD に適用できる。

2　改正の経緯

2021 年 6 月，ネットワーク機能付き事務機に対応し，IoT デバイスとしての最低限のセキュリティ要件を定義したセキュリティガイドラインとして，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.1.00 を制定，発行した。又，ISO/IEC SC28 では，本ガイドラインをベースにした ISO 規格策定が進行中であり，ドラフト作成まで進んでいる。ISO 化ドラフト作成過程において，用語の説明など一部表現の修正が行われたが，その中には本ガイドラインに反映することが望ましいものがあったため，表現を修正するための改正を決定した。

今回の改正は表現の修正のみであり，セキュリティ機能要件の修正は行っていない。

3　主な改正点

主な改正点は，次のとおりである。

a) 「2 用語及び定義」において，「管理者」，「一般ユーザー」，「ウェアレベリング」の表現を修正し，「チェックサム」の用語を削除。

b) 「3.2.1 管理者の認証」の　e) 適用上の注意点 1) の表現を修正。

c) 「3.4　ファームウェアアップデート機能」の e) 適用上の注意点」のチェックサムの記述を削除。

d) 「3.5　大容量記憶装置データ保護」の（条件付き必須）d) 確認項目 2.2) の表現を修正。

e) 「3.5　大容量記憶装置データ保護」の（条件付き必須）e)適用上の注意点 3) の表現を修正。

f) 「4.3　運用環境」の b) 保証要件，d) 確認項目，e) 適用上の注意点 に想定される運用環境の記述を追記。

g) 委員構成表を BMSec 運営委員会に修正。

h) バージョン表記を Ver.1.00 から Ver.1.10 に修正。

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

本書は，改正に伴い JBMIA が管理・運営するビジネス機械・情報システム産業協会規格から廃止され，BMSec 運営委員会が管理・運営します。

本書についての意見又は質問は，お問い合わせフォームより一般社団法人
ビジネス機械・情報システム産業協会 BMSec 運営委員会 へお寄せください。

お問い合わせ　https://bmsec.jbmia.or.jp/contact/