# 認 証 報 告 書

独立行政法人 情報処理推進機構
理事長　藤原　武平太

原紙押印済

評価対象

| | |
|---|---|
| **申請受付日（受付番号）** | **平成19年3月22日** (IT**認証**7142) |
| **認証番号** | C0127 |
| **認証申請者** | **コニカミノルタビジネステクノロジーズ株式会社** |
| TOE**の名称** | **日本語名：**bizhub C353 / ineo+ 353 **全体制御ソフトウェア**<br>**英語名　：**bizhub C353 / ineo+ 353 Control Software |
| TOE**のバージョン** | A02E0Y0-0100-GM0-02 |
| PP**適合** | **なし** |
| **適合する保証パッケージ** | EAL3 |
| **開発者** | **コニカミノルタビジネステクノロジーズ株式会社** |
| **評価機関の名称** | **みずほ情報総研株式会社　情報セキュリティ評価室** |

上記のTOEについての評価は、以下のとおりであることを認証したので報告します。
平成19年11月26日

セキュリティセンター 情報セキュリティ認証室
技術管理者　鈴木　秀二

**評価基準等：「ITセキュリティ評価及び認証制度の基本規程」で定める下記の規格に基づいて評価された。**

① Common Criteria for Information Technology Security Evaluation Version 2.3
② Common Methodology for Information Technology Security Evaluation Version 2.3

**評価結果：合格**

「日本語名：bizhub C353 / ineo+ 353 全体制御ソフトウェア　英語名：bizhub C353 / ineo+ 353 Control Software」は、独立行政法人 情報処理推進機構が定めるITセキュリティ認証申請手続等に関する規程に従い、定められた規格に基づく評価を受け、所定の保証要件を満たした。

# 目次

# 1 全体要約

## 1.1 はじめに

この認証報告書は、「日本語名：bizhub C353 / ineo+ 353 全体制御ソフトウェア 英語名：bizhub C353 / ineo+ 353 Control Software　バージョン　A02E0Y0-0100-GM0-02」（以下「本TOE」という。）についてみずほ情報総研株式会社　情報セキュリティ評価室（以下「評価機関」という。）が行ったITセキュリティ評価に対し、その内容の認証結果を申請者であるコニカミノルタビジネステクノロジーズ株式会社に報告するものである。

本認証報告書の読者は、本書と共に、対応するSTや本TOEに添付されるマニュアル（詳細は「1.5.9 製品添付ドキュメント」を参照のこと）を併読されたい。前提となる環境条件、対応するセキュリティ対策方針とその実施のためのセキュリティ機能要件、保証要件及びそれらの要約仕様は、STにおいて詳述されている。また、動作条件及び機能仕様は本TOEに添付されるドキュメントに詳述されている。

本認証報告書は、本TOEに対して、適合の保証要件に基づく認証結果を示すものであり、個別のIT製品そのものを認証するものではないことに留意されたい。

注：本認証報告書では、ITセキュリティ評価及び認証制度が定めるITセキュリティ評価基準、ITセキュリティ評価方法の各々をCC、CEMと総称する。

## 1.2 評価製品

### 1.2.1 製品名称

本認証が対象とする製品は以下のとおりである。

| | |
|---|---|
| 名称： | 日本語名：bizhub C353 / ineo+ 353 全体制御ソフトウェア<br>英語名　：bizhub C353 / ineo+ 353 Control Software |
| バージョン： | A02E0Y0-0100-GM0-02 |
| 開発者： | コニカミノルタビジネステクノロジーズ株式会社 |

### 1.2.2 製品概要

本TOEは、コニカミノルタビジネステクノロジーズ株式会社が提供するデジタル複合機（bizhub C353 / ineo+ 353）（以下、「MFP」という。）に搭載される組み込み型のソフトウェアである。

TOEは、MFPに保存される機密性の高いドキュメントの暴露に対する保護機能を提供する。またMFP内に画像データを保存する媒体であるHDDが不正に持ち出される等の危険性に対して、MFPのオプション部品である暗号化基板を取り付けることによって、

HDDに書き込まれる画像データを暗号化することが可能である。他に、TOEは各種上書き削除規格に則った削除方式を有し、HDDのすべてのデータを完全に削除し、MFPを廃棄・リース返却する際に利用することによってMFPを利用する組織の情報漏洩の防止に貢献する。

### 1.2.3 TOEの範囲と動作概要

本TOEにてMFP制御コントローラはMFP本体内に据え付けられ、TOEはそのMFP制御コントローラ上のフラッシュメモリ上に存在し、ロードされる。本TOEとMFPの関係を図1-1に示す。なお、図1-1において本TOEは網掛けで示されており、図中の「※」はMFPのオプションパーツであることを示す。フラッシュメモリはTOEであるMFP全体制御ソフトウェアのオブジェクトコードが保管される記憶媒体である。TOEの他に、パネルやネットワークからのアクセスに対するレスポンス等などで表示するための各国言語メッセージデータやOS（VxWorks）なども保管される。NVRAMはTOEの処理に使われるMFPの動作において必要な様々な設定値等が保管される不揮発性メモリーである。暗号化基板はHDDに書き込まれるすべてのデータを暗号化するための暗号機能がハード的に実装されている。

HDD は画像データがファイルとして保管されるほか、伸張変換などで一時的に画像データ、送信宛先データが保管される領域としても利用される。特徴的な機能として、パスワードを設定することが可能で、パスワードに一致しないと読み書きすることができないセキュリティ機能（HDD ロック機能）が搭載されている。

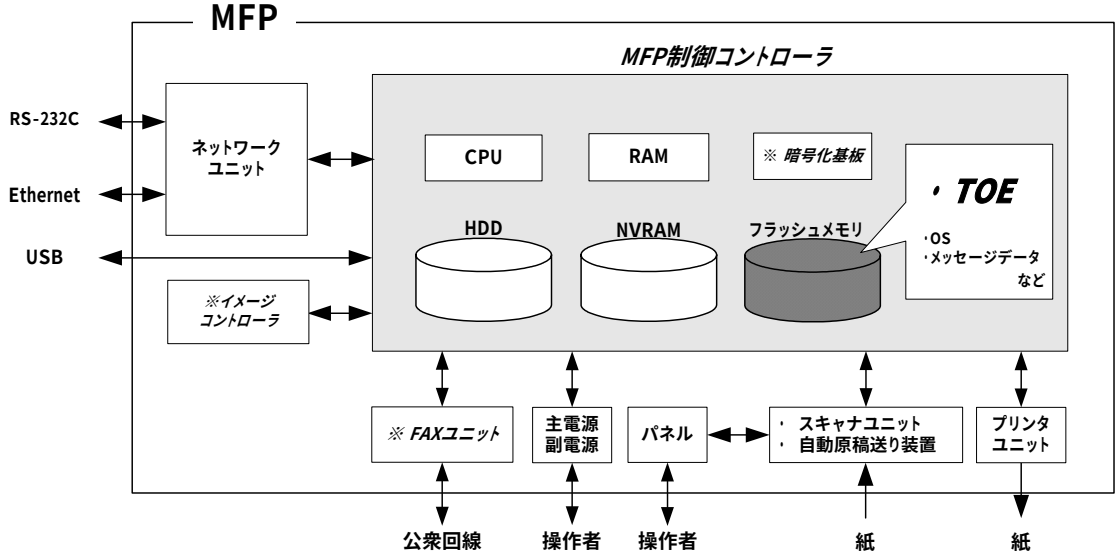


**図1-1：TOEに関係するハードウェア構成**

次に、本TOEの論理的な構成について示す。MFPには、「1.2.4 TOEの機能」に示す機能の他に、直接セキュリティとは関係の無い、基本機能、遠隔診断機能が存在する。

基本機能は、コピー、プリント、スキャン、FAXといった画像に関するオフィスワークのための一連の機能であり、TOEはこれら機能の動作における中核的な制御を行う。

遠隔診断機能は、FAX公衆回線口やRS-232Cを介したモデム接続経由、E-mailといった接続方式を利用して、コニカミノルタビジネステクノロジーズ株式会社が製造するMFPのサポートセンターと通信し、MFPの動作状態、印刷数等の機器情報を管理するために用いられる。

これらの機能を使用することができるMFPの利用者は、パネルやネットワークを介してTOEが提供する各種機能を使用する。

MFPの利用に関連する人物に対し、その役割を以下に示す。

1) ユーザ
   MFPに登録されるMFPの利用者。(一般には、オフィス内の従業員などが想定される。)
2) 管理者
   MFPの運用管理を行うMFPの利用者。MFPの動作管理、ユーザの管理を行う。(一般には、オフィス内の従業員の中から選出される人物がこの役割を担うことが想定される。)
3) サービスエンジニア
   MFPの保守管理を行う利用者。MFPの修理、調整等の保守管理を行う。(一般的には、コニカミノルタビジネステクノロジーズ株式会社と提携し、MFPの保守サービスを行う販売会社の担当者が想定される。)
4) MFPを利用する組織の責任者
   MFPが設置されるオフィスを運営する組織の責任者。MFPの運用管理を行う管理者を任命する。
5) MFPを保守管理する組織の責任者
   MFPを保守管理する組織の責任者。MFPの保守管理を行うサービスエンジニアを任命する。

この他に、TOEの利用者ではないがTOEにアクセス可能な人物として、オフィス内に出入りする人物などが想定される。

### 1.2.4 TOEの機能

TOEは以下の機能をもつ。

1) セキュリティ文書プリント機能
   プリントデータと共にセキュリティ文書パスワードを受信した場合、画像ファイルを印刷待機状態で保管し、パネルからの印刷指示とパスワード入力により印刷を実行する。
2) ボックス機能
   画像ファイルを保管するための領域として、HDDにボックスと呼称されるディレクトリを作成できる。ボックスには、ユーザが占有する個人ボックス、登録された

ユーザが一定数のグループを作って共同利用するための共有ボックス、所属部門のユーザ間で共有するグループボックスといった3つのタイプのボックスを設定することができる。個人ボックスは、所有するユーザだけに操作が制限され、共有ボックスは､そのボックスに設定されるパスワードを利用者間で共用することによって、アクセス制御を行っている｡グループボックスは､その部門の利用を許可されたユーザだけに操作が制限される。

TOEは、パネル、またはクライアントPCからネットワークを介したネットワークユニットから伝達される操作要求に対して処理を行う。

3) ユーザ認証機能

TOEは、MFPを利用する利用者を制限することができる。パネル、またはネットワークを介したアクセスにおいてTOEはMFPの利用を許可されたユーザであることをユーザID、ユーザパスワードを使って識別認証する。識別認証が成功すると、TOEはユーザに対して基本機能及びボックス機能などの利用を許可する。

ユーザ認証の方式には、本体認証と外部サーバ認証の２つの方式がある。本申請において想定する外部サーバ認証の方式は、Active Directoryの利用ケースのみとする。

4) 部門認証機能

TOEは､MFPを利用する利用者を部門単位でグルーピングして管理することができる。部門認証には、ユーザ認証連動方式と個別認証方式がある。

5) 管理者機能

認証された管理者だけが操作することが可能な管理者モードにて、ボックスの管理、ネットワークや画質等の各種設定の管理、本体認証の場合におけるユーザ情報の管理などの機能を提供する。また、その他の機能のふるまいに関係する動作設定機能を提供する。各種設定値、ユーザが保管したデータを削除する。

6）サービスエンジニア機能

サービスエンジニアだけが操作することが可能なサービスモードにて、管理者の管理、スキャナ・プリントなどのデバイスの微調整等のメンテナンス機能などを提供する。

7） 暗号鍵生成機能

オプション製品である暗号化基板がMFP制御コントローラに設置されている場合に、暗号化基板にてHDDのデータ書き込み、読み込みにおいて暗号化・復号処理を実施する。（TOEは、暗復号処理そのものを行わない。）

管理者機能にて本機能の動作設定を行う。動作させる場合は、TOEはパネルにて入力された暗号化ワードより暗号鍵を生成する。

8) HDDロック機能

HDDは、不正な持ち出し等への対処機能として、パスワードを設定した場合にHDDロック機能が動作する。MFPの起動動作において、MFP側に設定されたHDDロックパスワードとHDD側に設定されるHDDのパスワードロックを照合し、一致した場合にHDDへのアクセスを許可する。（HDDを持ち出されても、当該HDDが設置されていたMFP以外で利用することができない。）

9） 暗号通信機能

TOEはPCからMFPへ送信するデータ、MFPからダウンロードして受信するデータをSSL/TLSを利用して暗号化することができる。

10) セキュリティ強化機能

管理者機能、サービスエンジニア機能におけるセキュリティ機能のふるまいに関係する各種設定機能は、管理者機能における「セキュリティ強化機能」による動作設定により、セキュアな値に一括設定が行える。設定された各設定値は、個別に設定を脆弱な値に変更することが禁止される。また個別には動作設定機能を持たない機能として、ネットワーク設定のリセット機能、ネットワーク介したTOEの更新機能が存在するが、これら機能の利用は禁止される。

## 1.3 評価の実施

認証機関が運営するITセキュリティ評価・認証プログラムに基づき、公表文書「ITセキュリティ評価及び認証制度の基本規程」[2]、「ITセキュリティ認証申請手続等に関する規程」[3]、「ITセキュリティ評価機関承認申請手続等に関する規程」[4]に規定された内容に従い、評価機関によってTOEに関わる機能及び保証要件の評価が実施された。

本評価の目的は、以下のとおりである。

(1) 本TOEのセキュリティ設計が適切であること。
(2) 本TOEのセキュリティ機能が、セキュリティ設計で記述されたセキュリティ機能要件を満たしていること。
(3) 本TOEがセキュリティ設計に基づいて開発されていること。
(4) 上記(1)、(2)、(3)を、CCパート３及びCEMの規定に従って評価すること。

具体的には、評価機関は、本TOEのセキュリティ機能の基本設計である「bizhub C353 / ineo+ 353 全体制御ソフトウェアセキュリティターゲット」（以下「ST」という。）[1] 及び本TOE開発に関連する評価用提供物件及び本TOEの開発・製造・出荷の現場を調査し、本TOEがCCパート1 ([5][8][11]のいずれか) 附属書B、CCパート2（[6][9][12]のいずれか）の機能要件を満たしていること、また、その根拠として、TOEの開発・製造・出荷環境がCCパート3（[7][10][13]のいずれか）の保証要件を満たしていることを評価した。この評価手順及び結果は、「bizhub C353 / ineo+ 353 全体制御ソフトウェア評価報告書」（以下「評価報告書」という。）[18]に示されている。なお、評価方法は、CEM（[14][15][16]のいずれか）に準拠する。また、CC及びCEMの各パートは補足[17]の内容を含む。

## 1.4 評価の認証

認証機関は、評価機関が作成した、評価報告書、所見報告書、及び関連する評価証拠資料を検証し、本TOE評価が所定の手続きに沿って行われたことを確認した。認証の過程において発見された問題はなかった。評価は、平成19年10月の評価機関による評価報

告書の提出をもって完了し、認証機関が指摘した問題点は、すべて解決され、かつ、本TOE評価がCC及びCEMに照らして適切に実施されていることを確認した。認証機関は同報告書に基づき本認証報告書を作成し、認証作業を終了した。

## 1.5 報告概要

### 1.5.1 PP適合

適合するPPはない。

### 1.5.2 EAL

STが規定するTOEの評価保証レベルは、EAL3適合である。

### 1.5.3 セキュリティ機能強度

STは、最小機能強度として、”SOF-基本”を主張する。

本TOEは、本TOEは、外部ネットワークからの攻撃から保護された、一般のオフィス環境での利用を想定している。TOEへのパネルを経由したアクセス、あるいは内部ネットワークを経由したアクセスは、管理者による管理下にあり、複雑な攻撃は想定されない。このため、攻撃者の攻撃力を「低レベル」と想定することは妥当である。
よってSOF-基本で十分である。

### 1.5.4 セキュリティ機能

本TOEのセキュリティ機能は、以下のとおりである。

1) F.ADMIN（管理者機能）

F.ADMINとは､パネルやネットワークからアクセスする管理者モードにおける管理者識別認証機能、管理者パスワードの変更やロックされたボックスのロック解除などのセキュリティ管理機能といった管理者が操作する一連のセキュリティ機能である。

a. 管理者識別認証機能

管理者モードへのアクセス要求に対して、アクセスする利用者を管理者であることを識別及び認証する。

b. 管理者モードのオートログオフ機能

パネルから管理者モードにアクセス中でパネルオートログオフ時間以上何らかの操作を受け付けなかった場合は、自動的に管理者モードをログオフする。

c. 管理者モードにて提供される機能

管理者モードへのアクセス要求において管理者識別認証機能により、管理者

として識別認証されると、利用者を代行するタスクに管理者属性が関連づけられ、以下の操作、機能の利用が許可される。

① 管理者パスワードの変更

パネルより管理者であることを再認証され、且つ新規設定されるパスワードが品質を満たしている場合、変更する。

再認証に成功すると、認証失敗回数をリセットする。

再認証では、パネルからのアクセスの場合、管理者パスワード入力のフィードバックに1文字毎“＊”を返す。

管理者パスワードを利用する各認証機能において通算1～3回目となる認証失敗を検知すると､パネルからアクセスする管理者モードをログオフし、管理者パスワードを利用するすべての認証機能をロックする｡(管理者モードへのアクセスを拒否する｡)

認証機能のロックは、F.RESETが動作する、またはF.SERVICEにおける管理者認証機能のロック解除機能が実行されて解除する。

② ユーザの設定

ユーザ登録（ユーザ認証方式：本体認証において利用されるユーザのみ）ユーザID（ユーザ名と認証サーバ情報から構成されるが、本体認証時はユーザ名のみの登録｡）を設定し、ユーザパスワードを登録してユーザが登録される。新しく設定されるユーザパスワードはASCIIコード（0x20 ～ 0x7E） 8桁以上､1つのキャラクタで構成されないことを検証する｡なお、外部サーバ認証を有効にしている場合は、ユーザパスワードの登録はできない。また所属部門（部門ID）を登録し、関連付けする。（予め部門設定が必要｡）

ユーザ削除、ユーザに関連つけられた所属部門の変更を行う。

③ ボックスの設定

未登録ボックスIDに対して、ユーザ属性を選定して、個人ボックス、または共有ボックスを登録する。ボックスパスワードの設定・変更、ボックスのユーザ属性の変更を行う｡ボックスパスワードは､ASCIIコード（0x20 ～ 0x7E）（合計95文字が選択可能）を用いた8桁で設定される。また、1つのキャラクタで構成されることはない。

個人ボックスのユーザ属性に登録されたユーザを指定し、別のユーザの個人ボックス、またはグループボックス、共有ボックスに変更することができる。

④ ロックの解除

各ユーザの認証失敗回数、各セキュリティ文書プリント、各ボックスの認証失敗回数、各部門の認証失敗回数、SNMPパスワードによる認証失敗回数を0クリアする。

アクセスロックがあれば、ロックが解除される。

⑤ ユーザ認証機能の設定

ユーザ認証機能における認証方式を、本体認証、または外部サーバ認証に設定する。またユーザ認証機能と組み合わせて利用される部門認証機能における認証方式を設定する。

⑥ 不正アクセス検出閾値の設定

認証操作禁止機能における不正アクセス検出閾値を1～3回間で設定する。

⑦ 全領域上書き削除機能の設定と実行

以下の表に示される消去方式を選択し、HDDのデータ領域の上書き削除およびNVRAMの初期化を実行する。（F.OVERWRITE-ALLを実行する。）

**表 1-1 全領域の上書き削除のタイプと上書きの方法**

| 方式 | 上書きされるデータタイプとその順序 |
|---|---|
| Mode:1 | 0x00 |
| Mode:2 | 乱数 ⇒ 乱数 ⇒ 0x00 |
| Mode:3 | 0x00 ⇒ 0xFF ⇒ 乱数 ⇒ 検証 |
| Mode:4 | 乱数 ⇒ 0x00 ⇒ 0xFF |
| Mode:5 | 0x00 ⇒ 0xFF ⇒ 0x00 ⇒ 0xFF |
| Mode:6 | 0x00 ⇒ 0xFF ⇒ 0x00 ⇒ 0xFF ⇒ 0x00 ⇒ 0xFF ⇒ 乱数 |
| Mode:7 | 0x00 ⇒ 0xFF ⇒ 0x00 ⇒ 0xFF ⇒ 0x00 ⇒ 0xFF ⇒ 0xAA |
| Mode:8 | 0x00 ⇒ 0xFF ⇒ 0x00 ⇒ 0xFF ⇒ 0x00 ⇒ 0xFF ⇒ 0xAA ⇒ 検証 |

⑧ オートログオフ機能の設定

パネルオートログオフ時間を、1～9分の範囲で設定する。

⑨ ネットワークの設定

以下の設定データの設定操作を行う。

- SMTPサーバに関係する一連の設定データ（IPアドレス、ポート番号等）
- DNSサーバに関係する一連の設定データ（IPアドレス、ポート番号等）
- MFPアドレスに関係する一連の設定データ（IPアドレス、NetBIOS名、AppleTalkプリンタ名等）

⑩ バックアップ、リストア機能の実行

管理者パスワード、CEパスワードを除いて、NVRAM及びHDDに保管されるあらゆる設定データをバックアップ、リストアする。

⑪ HDDロック機能の動作設定機能

HDDロック機能をOFFからONにする場合､設定されるHDDロックパスワードが品質を満たしていることを検証する。

HDDロックパスワードを変更する。現在設定されるHDDロックパスワードを使い、管理者であることを再認証され、且つ新規設定されるパスワードが品質を満たしている場合、変更する。

HDDロックパスワードは､ASCIIコード（0x21 ～ 0x7E､ただし0x22、0x28、0x29、0x2C、0x3A、0x3B、0x3C、0x3E、0x5B、0x5C、0x5Dを除く）（合計83文字が選択可能）を用いた20桁で設定される。

照合では、HDDロックパスワード入力のフィードバックに1文字毎“＊”を返す。

また、1つのキャラクタで構成されることはない。

⑫ 暗号化機能の動作設定

暗号化機能をOFFからONにする場合、設定される暗号化ワードが品質を満たしていることを検証し、F.CRYPTが実行される。

暗号化ワードを変更する。現在設定される暗号化ワードを使い、管理者であることを再認証され、且つ新規設定される暗号化ワードが品質を満たしている場合、変更しF.CRYPTが実行される。

暗号化ワードは、ASCIIコード（0x21 ～ 0x7E、ただし0x22、0x28、0x29、0x2C、0x3A、0x3B、0x3C、0x3E、0x5B、0x5C、0x5Dを除く）（合計83文字が選択可能）を用いた20桁で設定される。

照合では、暗号化ワード入力のフィードバックに1文字毎“＊”を返す。

また、1つのキャラクタで構成されることはない。

⑬ セキュリティ強化機能に関連する機能

全領域の上書き削除の実行により、セキュリティ強化機能の設定を無効にする。

⑭ SNMPパスワードの変更

SNMPパスワード（Privacyパスワード、Authenticationパスワード）を変更、新規パスワードの品質の確認を行う

⑮ SNMPパスワード認証機能の設定

SNMPパスワード認証機能における認証方式を「Authenticationパスワードのみ」または「Authenticationパスワード且つPrivacyパスワード」に設定する。

⑯　部門の設定

部門IDを設定し、部門パスワードを登録して部門が登録される。新しく設定される部門パスワードがASCIIコード（0x20 ～ 0x7E）　8桁、１つのキャラクタで構成されないことを検証する。また、部門ID、部門パスワードの変更、部門削除を行う。

⑰　管理者認証ロック時間の設定

管理者認証ロック時間を1～60分で設定する。

⑱　高信頼チャネル機能の設定

SSL/TLSによる高信頼チャネル機能の設定データを設定する。

⑲　S/MIME送信機能の設定

ボックスファイルをS/MIME送信する際に利用される設定データ（送信宛先データ（e-mailアドレス）S/MIME証明書の登録、変更　暗号化強度の設定）を設定する。

2)　F.ADMIN-SNMP（SNMP管理者機能）

F.ADMIN-SNMPとは、PCからSNMPを利用してネットワークを介したアクセスにおいて管理者を識別認証し、識別認証された管理者だけにネットワークの設定機能の操作を許可するセキュリティ機能である。

a. SNMPパスワードによる識別認証機能

SNMPを用いてネットワークを介してMIBオブジェクトにアクセスする利用者が管理者であることをSNMPパスワードによって識別認証する。

b. SNMPを利用した管理機能

SNMPパスワードにより管理者であることが識別認証されると、MIBオブジェクトへのアクセスが許可され、以下に示す設定データの設定操作を行うことが許可される。

①　ネットワークの設定

以下の設定データの設定操作を行う。

・SMTPサーバに関係する設定データ（IPアドレス、ポート番号等）

・DNSサーバに関係する設定データ（IPアドレス、ポート番号等）

・MFPアドレスに関係する一連の設定データ（IPアドレス、NetBIOS名、AppleTalkプリンタ名等）

② SNMPパスワードの変更

SNMPパスワード（Privacyパスワード、Authenticationパスワード）を変更する。新しく設定されるSNMPパスワードがASCIIコード（0x20 ～ 0x7E）8桁以上であることを検証する。

③ SNMPパスワード認証機能の設定

SNMPパスワード認証機能における認証方式を「Authenticationパスワードのみ」または「Authenticationパスワード且つPrivacyパスワード」に設定する。

3) F.SERVICE（サービスモード機能）

パネルからアクセスするサービスモードにおけるサービスエンジニア識別認証機能、CEパスワードの変更や管理者パスワードの変更などのセキュリティ管理機能といったサービスエンジニアが操作する一連のセキュリティ機能である。

a. サービスエンジニア識別認証機能

パネルからサービスモードへのアクセス要求に対して、アクセスする利用者をサービスエンジニアであることを識別及び認証する。

b. サービスモードにて提供される機能

サービスモードへのアクセス要求においてサービスエンジニア識別認証機能により、サービスエンジニアとして識別認証されると、以下の機能の利用が許可される。

① CEパスワードの変更

サービスエンジニアであることを再認証され、且つ新規設定されるパスワードが品質を満たしている場合、変更する。

CEパスワードはASCIIコード（0x21 ～ 0x7E、ただし0x22と0x2Bを除く）8桁により構成される。また全て同じキャラクターで構成されない。再認証に成功すると、認証失敗回数をリセットする。CEパスワード入力のフィードバックに1文字毎“＊”を返す。

CEパスワードを利用する各認証機能において通算1～3回目となる認証失敗を検知すると、パネルからアクセスするサービスモードをログオフし、CEパスワードを利用するすべての認証機能をロックする。（サービスモードへのアクセスを拒否する。）

② 管理者パスワードの変更

管理者パスワードを変更する。新規設定される管理者パスワードは以下の品質を満たしていることを検証する。

- ASCIIコード（0x21 ～ 0x7E、ただし0x22と0x2Bを除く）8桁で構成される。また1つのキャラクタで構成されない。
- 現在設定される値と一致しない。

③　セキュリティ強化機能に関連する機能

以下の機能を提供する。

・HDD論理フォーマット機能

HDDにOSのシステムファイルを再書き込みする機能。この論理フォーマットの実行に伴い、セキュリティ強化機能の設定を無効にする。

・HDD物理フォーマット機能

HDDにトラック、セクター情報などの信号列を含めてディスク全体を規定パターンに書き直す機能。この物理フォーマットの実行に伴い、セキュリティ強化機能の設定を無効にする。

・HDD装着設定機能

搭載されたHDDを有効化するための機能。このHDD装着設定を無効化することにより、セキュリティ強化機能の設定を無効にする。

・イニシャライズ機能

NVRAMに書き込まれる各種設定値を工場出荷状態に戻すための機能。このイニシャライズ機能を実行することにより、セキュリティ強化機能の設定を無効にする。

④　パスワード初期化機能に関連する機能

以下の機能を提供する。

・イニシャライズ機能

NVRAMに書き込まれる各種設定値を工場出荷状態に戻す。

・HDD物理フォーマット機能

HDDにトラック、セクター情報などの信号列を含めてディスク全体を規定パターンに書き直す機能。

⑤　管理者認証機能のロックの解除

管理者認証失敗回数を0クリアする。アクセスがロックされていれば、ロックが解除される。

⑥　CE認証ロック時間の設定

CE認証ロック時間を1～60分で設定する

4）　F.USER（ユーザ機能）

MFPの諸機能を利用するにあたって、ユーザを識別認証する。また識別認証されたユーザには、F.BOXやF.PRINTなどの機能の利用を許可する他、本体認証時にMFP本体にて管理されるユーザパスワードの管理機能を提供する。

a. ユーザ識別認証機能

①　部門認証：連動方式のユーザ識別認証

ボックスへのアクセス要求、セキュリティ文書プリントファイルの登録要求において、ユーザであることを識別認証する。識別認証されたユーザには、ユーザID以外に予め設定される当該ユーザIDに対する所属部門（部門ID）が関連付けられ、F.BOX及びF.PRINTの利用を許可する。

②　部門認証：連動方式において所属部門が登録されていない場合の所属部門登録機能

ユーザ識別認証後、部門認証が要求され、部門認証に成功すると、成功した部門IDが所属部門として登録される。

③　部門認証：個別認証方式のユーザ識別認証

ボックスへのアクセス要求、セキュリティ文書プリントファイルの登録要求において、ユーザであることを識別認証する。ユーザ認証の詳細は、部門認証：連動方式のユーザ識別認証と同様である。パネルからのアクセスの場合、ユーザ識別認証されたユーザには、部門認証が要求され、部門認証に成功するとユーザIDに所属部門が関連づけられ、F.BOX及びF.PRINTの利用を許可する。

ネットワークからのアクセスの場合、ユーザ認証後に部門を認証するのではなく、ユーザ及び部門を1つのシーケンス内で処理する。認証されると、ユーザIDと部門IDは関連付けられ、部門認証：連動方式のユーザ識別認証と同じセッション情報より、ユーザID、部門IDを判定する。また、ユーザ認証方式に「外部サーバ認証」が選択されている場合、識別認証されたユーザは、識別認証に伴って利用されたユーザ名、認証サーバ情報と合わ

せてユーザIDとして登録する。

b. ユーザ識別認証ドメインにおけるオートログオフ機能

識別認証されたユーザがパネルからアクセス中、パネルオートログオフ時間以上何らかの操作を受け付けなかった場合、自動的にユーザ識別認証ドメインからログオフする。

c. ユーザパスワードの変更機能

識別認証され、ユーザ識別認証ドメインへのアクセスが許可されると、本人のユーザパスワードを変更することが許可される。なお外部サーバ認証が有効の場合には、本機能は利用できない。

5） F.BOX（ボックス機能）

登録ユーザであると識別認証されたユーザに対して、そのユーザの個人ボックスの操作、管理を許可し、共有ボックスへのアクセスに対して共有ボックスの利用を許可されたユーザであることを認証し、認証後に当該ボックス、ボックスファイルの各種操作を許可するアクセス制御機能などボックスに関係する一連のセキュリティ機能のことである。

a. ユーザ操作によるボックスの登録

選択した未登録ボックスIDに対して、ユーザ属性を選定して、個人ボックス、または共有ボックスを登録する。登録する際、ボックスのユーザ属性にはデフォルト値として「共有」が指定されるが、「ユーザID」を選択することも可能。

b. ボックスの自動登録

コピージョブ、プリントジョブにおけるボックス保管操作において、指定したボックスが未登録である場合、ユーザ属性に当該ジョブを操作するユーザのユーザIDが設定される個人ボックスを自動的に登録する。

c. 個人ボックス機能

① 個人ボックスに対するアクセス制御機能

識別認証されたユーザを代行するタスクは、ユーザ属性に識別認証されたユーザの「ユーザID」を持つ。このタスクは、このユーザ属性と一致するユーザ属性を持つ個人ボックスの一覧表示操作が許可される。

② 個人ボックス内のボックスファイルに対するアクセス制御機能

操作するボックスを選択すると、ユーザ属性に加えてそのボックスの「ボックスID」がボックス属性としてタスクに関連づけられる。このタス

クは、このユーザ属性及びボックス属性と一致するユーザ属性、ボックス属性を持つボックスファイルに対して印刷、E-mail送信（S/MIME送信を含む）、FTP送信、FAX送信、SMB送信、ダウンロード、他のボックスへの移動、他のボックスへのコピー操作を行うことを許可される。

③ 個人ボックスのユーザ属性変更

ユーザ属性を変更することができる。他の登録ユーザを指定すると、他のユーザが管理する個人ボックスになる。部門IDを指定すると、当該部門の利用を許可されたユーザがアクセス可能なグループボックスになる。共有を指定すると、共有ボックスになる。ボックスパスワードの登録が必要。この場合は、ボックスパスワードが定められた条件を満たすことを検証する。

d. 共有ボックス機能

① 共有ボックスへのアクセスにおける認証機能

個々の共有ボックスへのアクセス要求に対して、ユーザ ID の認証後、アクセスする利用者をそれぞれ当該共有ボックスの利用を許可されたユーザであることを認証する。当該共有ボックスに対して、通算 1～3 回目となる認証失敗を検知すると、当該共有ボックスに対する認証機能をロックする。失敗回数閾値は、不正アクセス検出閾値設定機能により管理者が指定する。認証機能のロックは、F.ADMIN の共有ボックスに対するロック解除機能が実行されることによって解除される。

② 共有ボックス内のボックスファイルに対するアクセス制御

ユーザを代行するタスクは、ユーザ属性に加えてそのボックスの「ボックス ID」がボックス属性としてタスクに関連づけられる。このタスクは、ユーザ属性に共有が設定され、且つサブジェクト属性のボックス属性と一致するボックス属性を持つボックスファイルに対して印刷、E-mail 送信（S/MIME 送信を含む）、FTP 送信、FAX 送信、SMB 送信、ダウンロード、他のボックスへの移動、他のボックスへのコピー操作を行うことを許可される。

③ 共有ボックスのユーザ属性変更

当該ボックスのユーザ属性を変更することができる。登録ユーザを指定し、登録ユーザの個人ボックスに変更できる。また部門 ID を指定し、当該部門の利用が許可されたユーザがアクセス可能なグループボックスに変更できる。

④ 共有ボックスパスワードの変更

共有ボックスのボックスパスワードを変更する。新しく設定されるボックスパスワードが決められた品質を満たしている場合、変更する。登録ユーザとして識別認証されると、識別認証されたユーザを代行するタスクは、

ユーザ属性に識別認証されたユーザの「ユーザID」を持つ。このタスクは、ユーザ属性に共有が設定される共有ボックスの一覧表示操作が許可される。

e. グループボックス機能

① グループボックスに対するアクセス制御機能

識別認証されたユーザを代行するタスクは、識別認証されたユーザと関連づけられた所属部門として「部門ID」を持つ。このタスクは、この部門IDと一致するユーザ属性を持つグループボックスの一覧表示操作が許可される。

② グループボックス内のボックスファイルに対するアクセス制御機能

操作するボックスを選択すると、ユーザ属性に加えてそのボックスの「ボックスID」がボックス属性としてタスクに関連づけられる。このタスクは、このユーザ属性及びボックス属性と一致するユーザ属性、ボックス属性を持つボックスファイルに対して印刷、E-mail送信（S/MIME送信を含む）、FTP送信、FAX送信、SMB送信、ダウンロード、他のボックスへの移動、他のボックスへのコピー操作を行うことを許可される。

③ グループボックスのユーザ属性変更

ユーザ属性を変更することができる。他の部門IDを指定すると、他の部門所属のユーザがアクセス可能なグループボックスになる。共有を指定すると、共有ボックスになる。ボックスパスワードの登録が必要。また登録ユーザを指定し､登録ユーザの個人ボックスに変更することも可能である。

6） F.PRINT（セキュリティ文書プリント機能）

F.PRINTとは、登録ユーザであると識別認証されたユーザに対して、パネルからのセキュリティ文書プリントファイルへのアクセスに対してセキュリティ文書プリントファイルの利用を許可されたユーザであることを認証し、認証後に当該セキュリティ文書プリントファイルの一覧表示、印刷を許可するアクセス制御機能などセキュリティ文書プリントに関係する一連のセキュリティ機能である。

a. セキュリティ文書パスワードによる認証機能

登録ユーザであることが識別認証されると、パネルからセキュリティ文書プリントファイルへのアクセス要求に対して、アクセスする利用者を当該セキュリティ文書プリントファイルの利用を許可されたユーザであることを認証する。

セキュリティ文書プリントの場合はパネルからのアクセスのみになるため、別途セッション情報によるセキュリティ文書認証メカニズムを必要としない。

セキュリティ文書パスワード入力のフィードバックに1文字毎“＊”を返す。認証に成功すると、認証失敗回数をリセットする。認証に失敗すると、パネルからのアクセスを5秒間受け付けない。当該セキュリティ文書プリントファイルに対して、通算1～3回目となる認証失敗を検知すると、当該セキュリティ文書プリントファイルに対する認証機能をロックする。

失敗回数閾値は、不正アクセス検出閾値設定機能により管理者が指定する。ロック状態は、F.ADMINにおいて当該セキュリティ文書プリントファイルに対してロック解除機能が実行されることによって解除される。

b. セキュリティ文書プリントファイルに対するアクセス制御機能

認証されると、セキュリティ文書プリントファイルアクセス制御が動作する。識別認証されたユーザを代行するタスクは、ファイル属性に、認証されたセキュリティ文書プリントファイルのセキュリティ文書内部制御IDを持つ。このタスクは、このファイル属性と一致するファイル属性を持つセキュリティ文書プリントファイルに対して印刷を許可される。

c. セキュリティ文書プリントファイルの登録機能

セキュリティ文書プリントファイルの登録要求において、登録されたユーザとして認証されると、セキュリティ文書パスワードを対象となるセキュリティ文書プリントファイルと共に登録することを許可する。

① セキュリティ文書パスワードの登録

登録されるセキュリティ文書パスワードが指定されたパスワードの品質を満たすことを検証する。

② セキュリティ文書内部制御IDの付与

セキュリティ文書プリントファイルの登録要求において、セキュリティ文書パスワードの検証が完了すると、一意に識別されるセキュリティ文書内部制御IDを当該セキュリティ文書プリントファイルに設定する。

7） F.OVERWRITE-ALL（全領域上書き削除機能）

F.OVERWRITE-ALLとは、HDDのデータ領域に上書き削除を実行すると共にNVRAMに設定されているパスワード等の設置値を初期化する。

HDDに書き込むデータ、書き込む回数など削除方式は、F.ADMINにおいて設定される全領域上書き削除機能の消去方式に応じて実行される。HDDロック機能及び暗号化機能は動作設定がOFFされることによって、設定されていたHDDロックパスワード、暗号化ワードが利用できなくなる。なお、本機能の実行においてセキュリティ強化機能の設定は無効になる。

8） F.CRYPTO（暗号鍵生成機能）

コニカミノルタ暗号仕様標準によって規定されるコニカミノルタHDD暗号鍵生成アルゴリズム（SHA-1）を利用し、HDDに書き込まれるすべてのデータを暗号化するための暗号鍵を生成する。コニカミノルタHDD暗号鍵生成アルゴリズム（SHA-1）とは、FIPS 180-1が規定するSHA-1を利用して暗号鍵を生成するアルゴリズムである。

F.ADMINにおいてアクセス制限される暗号化機能の動作設定において暗号化ワードが決定されると、コニカミノルタHDD暗号鍵生成アルゴリズム（SHA-1）を用いて暗号化ワードから128bit長の暗号鍵を生成する

9） F.HDD（HDD検証機能）

HDDに対してHDDロックパスワードを設定している場合、不正なHDDが設置されていないことを検証し、正当性が確認された場合だけHDDへの読み込み、書き込みを許可するチェック機能である。
HDDにHDDロックパスワードが設定されている場合、TOE起動時のHDD動作確認において、HDDのステータス確認を行う。ステータス確認の結果、HDDロックパスワードが確かに設定されていることが返された場合は、HDDへのアクセスを許可し、HDDロックパスワードが設定されていないことが返された場合は、不正な可能性があるためHDDへのアクセスを拒否する。

10）F.RESET（認証失敗回数リセット機能）

管理者認証、CE認証においてアカウントロックした場合にカウントされる認証失敗回数をリセットして、ロックを解除する機能である。
管理者認証機能ロックは、主電源のOFF/ONより実行され、管理者認証ロック解除時間後に解除する。CE認証機能ロックは、特定操作により実行され、CE認証ロック解除時間後に解除する。

11） F.TRUSTED-PASS（高信頼チャネル機能）

PCとMFP間で以下の画像ファイルを送受信する際に、SSLまたはTLSプロトコルを使用して、高信頼チャネルを生成、及び実現する機能である。

- ボックスファイル（MFPからPCへのダウンロード）
- ボックスファイルとして保存されることになる画像ファイル（PCからMFPへのアップロード）
- セキュリティ文書プリントファイルとして保存されることになる画像ファイル（PCからMFPへのアップロード）

12） F.S/MIME（S/MIME暗号処理機能）

F.S/MIMEとは、ボックスファイルをS/MIMEとして送信する際に、ボックスファイルを暗号化するための機能である。

a. ボックスファイル暗号鍵生成

FIPS 186が規定する擬似乱数生成アルゴリズムより、ボックスファイルを暗号化するための暗号鍵を生成する。（暗号鍵長は、128 bit、168 bit、192 bit、256 bitのいずれかである。）

b. ボックスファイル暗号化

- ボックスファイルを暗号化するための暗号鍵（128 bit、168 bit、256 bit）により、FIPS PUB 197によって規定されるAESによって暗号化される。
- ボックスファイルを暗号化するための暗号鍵（168 bit）により、SP800-67によって規定される3-Key-Triple-DESによって暗号化される

c. ボックスファイル暗号鍵の暗号化

- ボックスファイルを暗号化するための暗号鍵は、FIPS 186 -1が規定するRSAにより、暗号化される。
- この際利用される暗号鍵の鍵長は、1024bit、2048 bit、3072 bit、4096 bitのいずれかである。

### 1.5.5 脅威

本TOEは、表1-1に示す脅威を想定し、これに対抗する機能を備える。

**表1-1 想定する脅威**

| 識別子 | 脅 威 |
|---|---|
| T.DISCARD-MFP | ・リース返却、または廃棄となったMFPが回収された場合、悪意を持った者が、MFP内のHDDを取り出して解析することにより、セキュリティ文書プリントファイル、ボックスファイル、オンメモリ画像ファイル、保管画像ファイル、残存画像ファイル、画像関連ファイル、送信宛先データファイル、設定されていた各種パスワード等の秘匿情報が漏洩する。 |
| T.BRING-OUT -STORAGE | ・悪意を持った者や悪意を持ったユーザが、MFP内のHDDを不正に持ち出して解析することにより、セキュリティ文書プリントファイル、ボックスファイル、オンメモリ画像ファイル、保管画像ファイル、残存画像ファイル、画像関連ファイル、送信宛先データファイル、設定されていた各種パスワード等が漏洩する。<br>・悪意を持った者や悪意を持ったユーザが、MFP内のHDDを不正にすりかえる。すりかえられたHDDには新たにセ |

| | |
|---|---|
| | キュリティ文書プリントファイル、ボックスファイル、オンメモリ画像ファイル、保管画像ファイル、残存画像ファイル、画像関連ファイル、送信宛先データファイル、設定されていた各種パスワード等が蓄積され、悪意を持った者や悪意をもったユーザは、このすりかえたHDDを持ち出して解析することにより、これら画像ファイル等が漏洩する。 |
| T.ACCESS-PRIVATE-BOX | ・悪意を持った者や悪意を持ったユーザが、他のユーザが個人所有するボックスにアクセスし、ボックスファイルをダウンロード、印刷、送信（E-mail送信、FTP送信、FAX送信、SMB 送信）することにより、ボックスファイルが暴露される。 |
| T.ACCESS-PUBLIC-BOX | ・悪意を持った者や悪意を持ったユーザが、利用を許可されない共有ボックスにアクセスし、ボックスファイルをダウンロード、印刷、送信（E-mail送信、FTP送信、FAX送信、SMB送信）、他のボックスへ移動・コピーすることにより、ボックスファイルが暴露される。 |
| T.ACCESS-GROUP-BOX | ・悪意を持った者や悪意を持ったユーザが、そのユーザが所属していない部門が所有するグループボックスにアクセスし、ボックスファイルをダウンロード、印刷、送信（E-mail送信、FTP送信、FAX送信、SMB送信）することにより、ボックスファイルが暴露される。 |
| T.ACCESS-SECURE-PRINT | ・悪意を持った者や悪意を持ったユーザが、利用を許可されないセキュリティ文書プリントファイルを印刷することにより、セキュリティ文書プリントファイルが暴露される。 |
| T.ACCESS-NET-SETTING | ・悪意を持った者や悪意を持ったユーザが、ボックスファイルの送信に関係するネットワーク設定を変更することにより、宛先が正確に設定されていてもボックスファイルがユーザの意図しないエンティティへ送信（E-mail送信、FTP送信）されてしまい、ボックスファイルが暴露される。<br>＜ボックスファイル送信に関係するネットワーク設定＞<br>・SMTPサーバに関する設定<br>・DNSサーバに関する設定<br>・悪意を持った者や悪意を持ったユーザが、TOEが導入されるMFPに設定されるMFPを識別するためのネットワーク設定を変更し、不正な別のMFPなどのエンティティにおいて本来TOEが導入されるMFPの設定（NetBIOS名、AppleTalkプリンタ名、IPアドレスなど）を設定することにより、セキュリティ文書プリントファイルが暴露される。 |
| T.ACCESS-SETTING | ・悪意を持った者や悪意を持ったユーザが、セキュリティ強化機能に関係する設定を変更してしまうことにより、ボックスファイル、セキュリティ文書プリントファイルが漏洩する可能性が高まる。 |
| T.BACKUP-RESTORE | ・悪意を持った者や悪意を持ったユーザが、バックアップ機能、リストア機能を不正に使用することにより、ボックスファイル、セキュリティ文書プリントファイルが漏洩する。またパスワード等の秘匿性のあるデータが漏洩し、各種設定値が改ざんされる。 |

### 1.5.6 組織のセキュリティ方針

TOEの利用に当たって要求される組織のセキュリティ方針を表1-2に示す。

**表1-2 組織のセキュリティ方針**

| 識別子 | 組織のセキュリティ方針 |
|---|---|
| P.COMMUNICATION-DATA | IT機器間にて送受信される秘匿性の高い画像ファイル（セキュリティ文書プリントファイル、ボックスファイル）は、正しい相手先に対して、信頼されるパスを介して通信する、または暗号化しなければならない。 |

### 1.5.7 構成条件

TOEは、コニカミノルタビジネステクノロジーズ株式会社が提供するデジタル複合機、bizhub C353 / ineo+ 353において動作する。なお、暗号化基板についてはオプションパーツであるため、MFPには標準搭載されない。暗号化基板が装着されない場合は、画像データの暗号化に関する機能を利用することはできない。

### 1.5.8 操作環境の前提条件

本TOEを使用する環境において有する前提条件を表1-3に示す。

これらの前提条件が満たされない場合、本TOEのセキュリティ機能が有効に動作することは保証されない。

**表1-3　TOE使用の前提条件**

| 識別子 | 前提条件 |
|---|---|
| A.ADMIN | ・管理者は、課せられた役割として許可される一連の作業において、悪意を持った行為は行わない。 |
| A.SERVICE | ・サービスエンジニアは、課せられた役割として許可される一連の作業において、悪意を持った行為は行わない。 |
| A.NETWORK | ・TOEが搭載されるMFPを設置するオフィス内LANは、盗聴されない。<br>・TOEが搭載されるMFPを設置するオフィス内LANが外部ネットワークと接続される場合は、外部ネットワークからMFPへアクセスできない。 |
| A.SECRET | ・TOEの利用において使用される各パスワードや暗号化ワードは、各利用者から漏洩しない。 |
| A.SETTING | ・セキュリティ強化機能が有効化した上で、TOEが搭載されたMFPを利用する。 |
| A.SERVER | ・ユーザ認証方式に外部サーバ認証を利用する場合、TOEが搭載されるMFPを設置するオフィス内LANに接続されるユーザ情報管理サーバは、アカウントの管理、アクセス制御、パッチ適用などが適切に実施されている。 |

### 1.5.9 製品添付ドキュメント

本TOEに添付されるドキュメントを以下に示す。

＜管理者・一般利用者向けドキュメント＞

1) bizhub C353　ユーザーズガイド　セキュリティ機能編　（バージョン：1.01）

2) bizhub C353 User's Guide [Security Operations] （Ver.1.01）

3) ineo+ 353 User's Guide [Security Operations] （Ver.1.01）

＜サービスエンジニア向けドキュメント＞

1) bizhub C353 サービスマニュアル セキュリティ機能編(Ver.1.02)

2) bizhub C353 / ineo+ 353 Service Manual Security Function (Ver. 1.02)

# 2 評価機関による評価実施及び結果

## 2.1 評価方法

評価は、CCパート3の保証要件について、CEMに規定された評価方法を用いて行われた。評価作業の詳細は、評価報告書において報告されている。評価報告書では、本TOEの概要説明、CEMのワークユニットごとに評価した内容及び判断が記載されている。

## 2.2 評価実施概要

以下、評価報告書による評価実施の履歴を示す。

評価は、平成19年3月に始まり、平成19年10月評価報告書の完成をもって完了した。評価機関は、開発者から評価に要する評価用提供物件一式の提供を受け、一連の評価における証拠を調査した。また、平成19年9月に開発・製造現場へ赴き、記録及びスタッフへのヒアリングにより、構成管理・配付と運用・ライフサイクルの各ワークユニットに関するプロセスの施行状況の調査を行った。また、平成19年9月に開発者サイトで開発者のテスト環境を使用し、開発者が実施したテストのサンプリングチェック及び評価者テストを実施した。

各ワークユニットの評価作業中に発見された問題点は、すべて所見報告書として発行され、開発者に報告された。それらの問題点は、開発者による見直しが行われ、最終的に、すべての問題点が解決されている。

## 2.3 製品テスト

評価者が評価した開発者テスト及び評価者の実施した評価者テストの概要を以下に示す。

### 2.3.1 開発者テスト

1) 開発者テスト環境

開発者が実施したテストの構成を図2-1に示す。

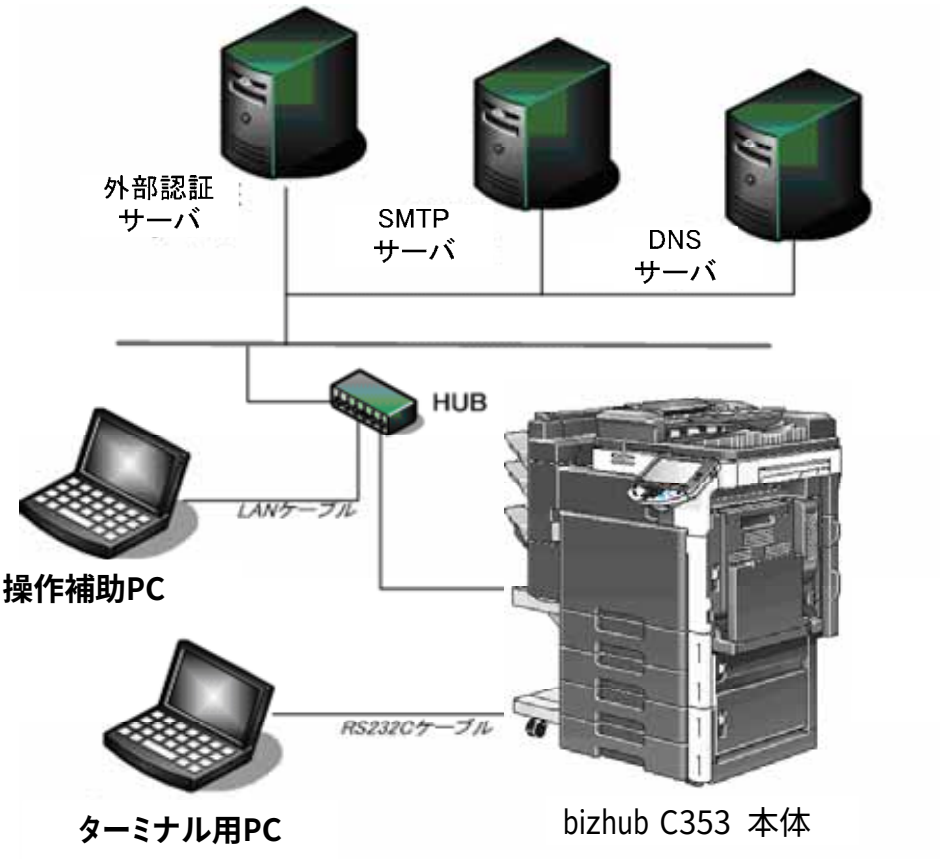


**図2-1　開発者テストの構成図**

2) 開発者テスト概説

開発者の実施したテストの概要は以下のとおり。

a.テスト構成

開発者が実施したテストの構成を図2-1に示す。開発者テストはSTにおいて識別されているTOE構成と同一のTOEテスト環境で実施されている。

b.テスト手法

テストには、以下の手法が使用された。

① 操作パネルに関連するTSFのふるまいは、操作パネルに対する操作及び操作パネルへの表示の観察でセキュリティ機能のふるまいを確認する。

② 電源OFF/ONに関連するTSFのふるまいは、本体の電源を一旦OFFし、再度ONした結果の動作の変化を操作パネル（又はネットワーク経由）により確認する。

③ ネットワークに関連するTSFのふるまいは、PSWCやテストツールよりTOEへ各種プロトコルを利用して接続し、PSWCはWEB画面での操作と観察・それぞれのプロトコルによるテストデータを送受信すること

でのセキュリティ機能のふるまいを確認する。

④　セキュリティ強化機能に関連する機能（HDD論理フォーマット、HDD物理フォーマット、HDD装着設定機能、イニシャライズ機能）のふるまいは、これらの機能がサービスエンジニア及び管理者（一部機能）のみに制限されること、これらの機能を実施後、セキュリティ強化設定ONを示す鍵アイコンのパネル表示がなくなること、それぞれの機能が初期化対象とする値が初期化状態になっていることを確認する。

⑤　開発者テストにおいて、セキュリティ機能に対する設定値の変更、認証方法、アクセス制御の確認等には、外部インタフェース（操作パネル、電源OFF/ON、ネットワーク）を利用し、出力メッセージ等を目視で確認する。

・　これらの外部インタフェースを利用しても検証できないセキュリティ機能については、個別のテスト手法を実施することにより、ふるまいが妥当であることを確認する。

c.実施テストの範囲

テストは開発者によって169項目実施されている。

カバレージ分析が実施され、機能仕様に記述されたすべてのセキュリティ機能と外部インタフェースが十分にテストされたことが検証されている。深さ分析が実施され、上位レベル設計に記述されたすべてのサブシステムとサブシステムインタフェースが十分にテストされたことが検証されている。

d.結果

開発者によるテスト結果は、期待されるテスト結果と実際のテスト結果が一致していることを確認している。評価者は、開発者テストの実施方法、実施項目の正当性を確認し、実施方法及び実施結果がテスト計画書に示されたものと一致することを確認した。

### 2.3.2　評価者テスト

1) 評価者テスト環境

評価者が実施したテストの構成は、開発者テストと同様の構成である。

2) 評価者テスト概説

評価者の実施したテストの概要は以下のとおり。

a.テスト構成

評価者が実施したテストの構成を図2-1に示す。評価者テストはSTにおいて識別されているTOE構成と同一のTOEテスト環境で実施されている。

b.テスト手法

テストには、以下の手法が使用された。

① 操作パネルに関連するTSFのふるまいは、操作パネルに対する操作及び操作パネルへの表示の観察でセキュリティ機能のふるまいを確認する。
② 電源OFF/ONに関連するTSFのふるまいは、本体の電源を一旦OFFし、再度ONした結果の動作の変化を操作パネル（又はネットワーク経由）により確認する。
③ ネットワークに関連するTSFのふるまいは、PSWCやテストツールよりTOEへ各種プロトコルを利用して接続し、PSWCはWEB画面での操作と観察・それぞれのプロトコルによるテストデータを送受信することでのセキュリティ機能のふるまいを確認する。
④ セキュリティ強化機能に関連する機能（HDD論理フォーマット、HDD物理フォーマット、HDD装着設定機能、イニシャライズ機能）のふるまいは、これらの機能がサービスエンジニア及び管理者（一部機能）のみに制限されること、これらの機能を実施後、セキュリティ強化設定ONを示す鍵アイコンのパネル表示がなくなること、それぞれの機能が初期化対象とする値が初期化状態になっていることを確認する。
⑤ 開発者テストにおいて、セキュリティ機能に対する設定値の変更、認証方法、アクセス制御の確認等には、外部インタフェース（操作パネル、電源OFF/ON、ネットワーク）を利用し、出力メッセージ等を目視で確認する。
・ これらの外部インタフェースを利用しても検証できないセキュリティ機能については、個別のテスト手法を実施することにより、ふるまいが妥当であることを確認する。

c.実施テストの範囲

評価者が独自に考案したテストを39項目、開発者テストのサンプリングによるテストを36項目、計75項目のテストを実施した。テスト項目の選択基準として、下記を考慮している。

① 開発者テストからは仕様通りに動作することが疑われるセキュリティ機能
② 他のセキュリティ機能よりも重要なセキュリティ機能
③ 機能強度の対象となるセキュリティ機能
④ 異なるインタフェースから利用される機能

d.結果

実施したすべての評価者テストは正しく完了し、TOEのふるまいを確認することができた。評価者はすべてのテスト結果は期待されるふるまいと一致していることを確認した。

## 2.4 評価結果

評価報告書をもって、評価者は本TOEがCEMのワークユニットすべてを満たしていると判断した。

# 3 認証実施

認証機関は、評価の過程で評価機関より提出される各資料をもとに、以下の認証を実施した。

① 当該所見報告書でなされた指摘内容が妥当であること。
② 当該所見報告書でなされた指摘内容が正しく反映されていること。
③ 提出された証拠資料をサンプリングし、その内容を検査し、関連するワークユニットが評価報告書で示されたように評価されていること。
④ 評価報告書に示された評価者の評価判断の根拠が妥当であること。
⑤ 評価報告書に示された評価者の評価方法がCEMに適合していること。

これらの認証において発見された問題事項を、認証レビューとして作成し、評価機関に送付した。

認証機関は、ST及び評価報告書において、所見報告書で指摘された問題点が解決されていることを確認した。

# 4 結論

## 4.1 認証結果

提出された評価報告書、当該所見報告書及び関連する評価証拠資料を検証した結果、認証機関は、本TOEがCCパート3のEAL3保証要件を満たしていることを確認した。

評価機関の実施した各評価者エレメントについての検証結果を表4-1にまとめる。

**表4-1 評価者アクションエレメント検証結果**

| 評価者アクションエレメント | 検証結果 |
|---|---|
| **セキュリティターゲット評価** | **適切な評価が実施された。** |
| ASE_DES.1.1E | 評価はワークユニットに沿って行われ、TOE識別、境界の記述が明瞭であることを確認している。 |
| ASE_DES.1.2E | 評価はワークユニットに沿って行われ、TOE記述が理路整然とし一貫していることを確認している。 |
| ASE_DES.1.3E | 評価はワークユニットに沿って行われ、TOE記述がST全体の内容と一貫していることを確認している。 |
| ASE_ENV.1.1E | 評価はワークユニットに沿って行われ、TOEのセキュリティ環境の記述が前提条件、脅威、組織のセキュリティ方針を漏れなく識別していることを確認している。 |
| ASE_ENV.1.2E | 評価はワークユニットに沿って行われ、TOEのセキュリティ環境の記述が理路整然とし一貫していることを確認している。 |
| ASE_INT.1.1E | 評価はワークユニットに沿って行われ、ST及びTOEの識別、概要及びCC適合が明確に述べられていることを確認している。 |
| ASE_INT.1.2E | 評価はワークユニットに沿って行われ、ST概説の記述が理路整然とし一貫していることを確認している。 |
| ASE_INT.1.3E | 評価はワークユニットに沿って行われ、ST概説の記述がST全体の内容と一貫していることを確認している。 |

| | |
|---|---|
| ASE_OBJ.1.1E | 評価はワークユニットに沿って行われ、セキュリティ対策方針の記述にTOE及び環境のセキュリティ対策方針が、脅威、組織のセキュリティ方針、前提条件へ遡れ、その対策方針の正当性をセキュリティ対策方針根拠が示していることを確認している。 |
| ASE_OBJ.1.2E | 評価はワークユニットに沿って行われ、セキュリティ対策方針の記述が完全で、理路整然としていて、かつ一貫していることを確認している。 |
| ASE_PPC.1.1E | 評価はワークユニットに沿って行われ、PP主張が行われていないため非適用であることを確認している。 |
| ASE_PPC.1.2E | 評価はワークユニットに沿って行われ、PP主張が行われていないため非適用であることを確認している。 |
| ASE_REQ.1.1E | 評価はワークユニットに沿って行われ、TOE及びIT環境の要件の記述、操作がCCに準拠していること、要件の依存性、機能強度が適切であること、各要件がそれぞれの対策方針に遡れ、それらを満たす根拠が示されていること、要件のセットが内部的に一貫し、相互サポート可能な構造となっていることを根拠が示していることを確認している。 |
| ASE_REQ.1.2E | 評価はワークユニットに沿って行われ、ITセキュリティ要件の記述が完全で、理路整然としていて、かつ一貫していることを確認している。 |
| ASE_SRE.1.1E | 評価はワークユニットに沿って行われ、CCを参照せずに明示された要件はないため非適用であることを確認している。 |
| ASE_SRE.1.2E | 評価はワークユニットに沿って行われ、CCを参照せずに明示された要件はないため非適用であることを確認している。 |
| ASE_TSS.1.1E | 評価はワークユニットに沿って行われ、TOE要約仕様の記述が適切なセキュリティ機能及び保証手段を示していること、それらが機能要件や保証要件を満たす根拠が示されていること、ITセキュリティ機能に対する機能強度主張が機能要件に対する機能強度と一貫していることを確認している。 |

| | |
|---|---|
| ASE_TSS.1.2E | 評価はワークユニットに沿って行われ、TOE要約仕様の記述が完全で、理路整然としていて、かつ一貫していることを確認している。 |
| **構成管理** | **適切な評価が実施された** |
| ACM_CAP.3.1E | 評価はワークユニットに沿って行われ、TOEとその構成要素が一意に識別され、TOEになされる変更の管理･追跡が可能な手続きが妥当であり正しく運用されていることを確認している。 |
| ACM_SCP.1.1E | 評価はワークユニットに沿って行われ、構成要素リストがCCによって要求される一連の要素を含んでいることを確認している。 |
| **配付と運用** | **適切な評価が実施された** |
| ADO_DEL.2.1E | 評価はワークユニットに沿って行われ、TOE配付についてセキュリティ維持のために必要な手続きが規定され、実施されていることを確認している。 |
| ADO_DEL.2.2D | 評価はワークユニットに沿って行われ、実際に配付手続きが使用されていることを、実地検査により確認している。 |
| ADO_IGS.1.1E | 評価はワークユニットに沿って行われ、TOEがセキュアにセットアップされるための手順が提供されていることを確認している。 |
| ADO_IGS.1.2E | 評価はワークユニットに沿って行われ、ADO_IGS.1.1Eにて提供されたセットアップの手順がセキュアであることを確認している。 |
| **開発** | **適切な評価が実施された** |
| ADV_FSP.1.1E | 評価はワークユニットに沿って行われ、明確かつ矛盾なく機能仕様が記述され、そこにすべての外部セキュリティ機能インタフェースとそのふるまいが適切に記述されていること、機能仕様にTSFが完全に表現されていること、機能仕様がTSFを完全に表現している論拠を含んでいることを確認している。 |
| ADV_FSP.1.2E | 評価はワークユニットに沿って行われ、機能仕様がTOEセキュリティ機能要件の完全かつ正確な具体化であることを確認している。 |

| | |
|---|---|
| ADV_HLD.2.1E | 評価はワークユニットに沿って行われ、上位レベル設計が明確で矛盾のないこと、サブシステムを規定しそのセキュリティ機能を記述していること、TSF実現に必要なIT環境としてのハードウェア、ソフトウェア、ファームウェアを説明していること、TSFサブシステムの外部とその他のインタフェースが識別され、それらの詳細を記述していることを確認している。 |
| ADV_HLD.2.2E | 評価はワークユニットに沿って行われ、上位レベル設計がTOEセキュリティ機能要件の正確かつ完全な具体化であることを確認している。 |
| ADV_RCR.1.1E | 評価はワークユニットに沿って行われ、機能仕様がTOEセキュリティ機能の正しく完全な表現であり、上位レベル設計が機能仕様の正しく完全な表現であり、下位レベル設計が上位レベル設計の正しく完全な表現であることを、それらの対応分析により確認している。 |
| **ガイダンス文書** | **適切な評価が実施された** |
| AGD_ADM.1.1E | 評価はワークユニットに沿って行われ、管理者ガイダンスがTOEのセキュアな運用に必要な管理機能、権限、利用条件とセキュアな状態維持のための適切なセキュリティパラメタ、管理が必要となる事象と対処法を記述してあること、他の証拠資料と一貫しておりIT環境に対するセキュリティ要件を記述してあることを確認している。 |
| AGD_USR.1.1E | 評価はワークユニットに沿って行われ、利用者ガイダンスがTOEの管理者でない利用者が利用可能なセキュリティ機能やユーザインタフェース、セキュリティ機能の使用法、対応すべき機能や特権に関する警告、TOEのセキュアな操作に必要なすべての利用者責任が記述してあり、他の証拠資料と一貫しておりIT環境に対するセキュリティ要件を記述してあることを確認している。 |
| **ライフサイクルサポート** | **適切な評価が実施された** |
| ALC_DVS.1.1E | 評価はワークユニットに沿って行われ、開発セキュリティ証拠資料がTOE開発環境のセキュア維持のための手段を記述しており、それが十分であること、その手段を実施した記録が生成されることを確認している。 |

| | |
|---|---|
| ALC_DVS.1.2E | 評価はワークユニットに沿って行われ、ALC_DVS.1.1Eで確認したセキュリティ手段が実施されていることを確認している。また、本評価時に行われたサイト訪問での調査方法も適切と判断される。 |
| **テスト** | **適切な評価が実施された** |
| ATE_COV.2.1E | 評価はワークユニットに沿って行われ、テスト証拠資料に識別されているテストが機能仕様に正確かつ完全に対応していること、テスト計画に示されたテスト手法がセキュリティ機能の検証に適切であること、テスト手順に示されるテスト条件、手順、期待される結果が各セキュリティ機能を適切にテストするものであることを確認している。 |
| ATE_DPT.1.1E | 評価はワークユニットに沿って行われ、テスト証拠資料に識別されているテストが上位レベル設計に正確かつ完全に対応していること、テスト計画に示されたテスト手法がセキュリティ機能の検証に適切であること、テスト手順に示されるテスト条件、手順、期待される結果が各セキュリティ機能を適切にテストするものであることを確認している。 |
| ATE_FUN.1.1E | 評価はワークユニットに沿って行われ、テスト証拠資料がテスト計画、手順、期待される結果及び実際の結果を含み、テスト計画が目的を記述しセキュリティ機能を識別し、ST及びテスト手順記述と一貫していること、テスト手順記述がテストするセキュリティ機能のふるまいを識別しており再現可能な記述であること、テスト証拠資料が期待されるテスト結果を含んでおりそれらが実施結果と一致していることを確認し、開発者のテスト成果を報告している。 |
| ATE_IND.2.1E | 評価はワークユニットに沿って行われ、テスト構成がSTの記述と一貫し、TOEが正しく設定され、開発者テストと同等の資源が提供されていることを確認している。 |
| ATE_IND.2.2E | 評価はワークユニットに沿って行われ、テストサブセットとその証拠資料を作成し実施している。実施したテスト内容を記述し、結果が期待されるべき結果と一貫していることを確認している。また、本評価時に行われたテスト実施方法も適切と判断される。 |

| | |
|---|---|
| ATE_IND.2.3E | 評価はワークユニットに沿って行われ、サンプリングテストを実施し、結果が期待されるべき結果と一貫していることを確認している。また、本評価のサンプリング方針及びテスト実施方法も適切と判断される。 |
| **脆弱性評定** | **適切な評価が実施された** |
| AVA_MSU.1.1E | 評価はワークユニットに沿って行われ、提供されたガイダンスがTOEのセキュアな運用に必要な情報を矛盾なく完全に記述していること、使用環境の前提事項、TOE以外のセキュリティ事項の要件がすべて明記されていること、ガイダンスの完全性を保証する手段を開発者が講じていることを確認している。 |
| AVA_MSU.1.2E | 評価はワークユニットに沿って行われ、提供されたガイダンスの管理者と利用者手続き、あるいはその他の手続き情報のみで、TOEを構成でき、TOEのセキュアな運用に関わる設定が行えることを確認している。 |
| AVA_MSU.1.3E | 評価はワークユニットに沿って行われ、提供されたガイダンスが、TOEが非セキュアな状態に陥ったことを検出する手段及び対処方法を記述していることを確認している。 |
| AVA_SOF.1.1E | 評価はワークユニットに沿って行われ、STでSOF主張がなされているセキュリティメカニズムに対して、正当なSOF分析が行われ、SOF主張が満たされていることを確認している。 |
| AVA_SOF.1.2E | 評価はワークユニットに沿って行われ、すべての確率的または順列的メカニズムがSOF主張を持ち、そのSOF主張が正しいことを確認している。 |
| AVA_VLA.1.1E | 評価はワークユニットに沿って行われ、脆弱性分析が脆弱性に関する情報を考慮していること、識別された脆弱性について悪用されない根拠とともに記述していること、脆弱性分析がSTやガイダンスの記述と一貫していることを確認している。 |
| AVA_VLA.1.2E | 評価はワークユニットに沿って行われ、侵入テストとそれを再現可能な詳細を持つ侵入テスト証拠資料を作成しテストを実施している。実施したテスト結果とテスト概要について報告がなされている。 |

## 4.2 注意事項

特になし。

# 5 用語

本報告書で使用された略語を以下に示す。

| | |
|---|---|
| CC | Common Criteria for Information Technology Security Evaluation |
| CEM | Common Methodology for Information Technology Security Evaluation |
| EAL | Evaluation Assurance Level |
| PP | Protection Profile |
| SOF | Strength of Function |
| ST | Security Target |
| TOE | Target of Evaluation |
| TSF | TOE Security Functions |

本報告書で使用されたTOE特有の略語を以下に示す。

| | |
|---|---|
| DNS | Domain Name System |
| FTP | File Transfer Protocol |
| HDD | Hard Disk Drive |
| IP | Internet Protocol |
| LAN | Local Area Network |
| MFP | Multiple Function Peripheral |
| NVRAM | Non-Volatile Random Access Memory |
| SMTP | Simple Mail Transfer Protocol |
| SNMP | Simple Network Management Protocol |
| SSL | Secure Socket Layer |
| USB | Universal Serial Bus |

本報告書で使用された用語を以下に示す。

| | |
|---|---|
| CE パスワード | サービスモードに入るときの認証時に照合する一種のパスワード。 |
| HDD 蓄積画像 | PC プリントにより MFP の HDD に蓄積される画像ファイル。 |
| MFP アドレスグループ | MFP の操作パネルから、管理者保守モードのネットワーク設定機能で設定される MFP の IP アドレス等の総称。 |
| MFP 制御コントローラ | MFP 本体のパネルやネットワークから受け付ける操作制御処理、画像データの管理等、MFP の動作全体を制御するためのコントローラ。TOE はそのコントローラ上で動作するソフトウェアである。 |
| PC プリント | パソコン（PC）からプリンタドライバーを使って MFP に印刷したいファイルのプリントデータを流し、MFP にてそのデータを画像ファイルに変換し、その画像データを印刷すること。 |
| アカウントロック | パスワード認証の操作で連続して失敗したときなどに、続けてパスワード認証をできなくしてしまうこと、またはその状態。 |
| サービスモード | サービスエンジニアのために用意された MFP 機能を動作することができる操作パネル画面領域。 |
| サービスエンジニア | MFP の保守管理を行う利用者。MFP の修理、調整等の保守管理を行う。一般的には、コニカミノルタビジネステクノロジーズ株式会社と提携し、MFP の保守サービスを行う販売会社または代理店のサービス担当者である。 |
| 残存画像ファイル | HDD データ領域に残存するファイルであり、通常の削除操作では削除できない画像ファイル。 |
| セキュリティプリント | PC プリントのうち、プリンタドライバーでパスワードを指定し、MFP からの印刷はそのパスワードで認証された場合に制限する印刷方法。 |
| 送信宛先データファイル | 画像を送信する宛先となる E-mail アドレス、電話番号などが含まれるファイル。 |
| フラッシュメモリ | EEPROM 構造を高速・高集積化し、一括型の消去機構を搭載したメモリデバイス。 |
| ボックス | 画像ファイルを MFP 内部に保管するために、HDD 領域に作成されたディレクトリのこと。 |

# 6 参照


[1] bizhub C353 / ineo+ 353 全体制御ソフトウェア セキュリティターゲット バージョン 1.03（2007年9月21日）コニカミノルタビジネステクノロジーズ株式会社

[2] ITセキュリティ評価及び認証制度の基本規程　平成19年5月　独立行政法人 情報処理推進機構　CCS-01

[3] ITセキュリティ認証申請手続等に関する規程　平成19年5月　独立行政法人 情報処理推進機構　CCM-02

[4] ITセキュリティ評価機関承認申請手続等に関する規程　平成19年5月　独立行政法人 情報処理推進機構　CCM-03

[5] Common Criteria for Information Technology Security Evaluation Part1: Introduction and general model Version 2.3 August 2005 CCMB-2005-08-001

[6] Common Criteria for Information Technology Security Evaluation Part2: Security functional requirements Version 2.3 August 2005 CCMB-2005-08-002

[7] Common Criteria for Information Technology Security Evaluation Part3: Security assurance requirements Version 2.3 August 2005 CCMB-2005-08-003

[8] 情報技術セキュリティ評価のためのコモンクライテリア パート1: 概説と一般モデル バージョン2.3 2005年8月 CCMB-2005-08-001　(平成17年12月翻訳第1.0版)

[9] 情報技術セキュリティ評価のためのコモンクライテリア パート2: セキュリティ機能要件 バージョン2.3 2005年8月 CCMB-2005-08-002　(平成17年12月翻訳第1.0版)

[10] 情報技術セキュリティ評価のためのコモンクライテリア パート3: セキュリティ保証要件 バージョン2.3 2005年8月 CCMB-2005-08-003　(平成17年12月翻訳第1.0版)

[11] ISO/IEC 15408-1:2005 Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model

[12] ISO/IEC 15408-2:2005 Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements

[13] ISO/IEC 15408-3:2005 Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance requirements

[14] Common Methodology for Information Technology Security Evaluation : Evaluation Methodology Version 2.3 August 2005 CCMB-2005-08-004

[15] 情報技術セキュリティ評価のための共通方法: 評価方法 バージョン2.3 2005年8月　(平成17年12月翻訳第1.0版)

[16] ISO/IEC 18045:2005 Information technology - Security techniques - Methodology for IT security evaluation

[17] 補足-0512　平成17年12月

[18] bizhub C353 / ineo+ 353 全体制御ソフトウェア 評価報告書 2007年10月19日 みずほ情報総研株式会社　情報セキュリティ評価室