認 証 報 告 書

独立行政法人情報処理推進機構
理事長　富田　達夫

原紙押印済

評価対象

申請受付日（受付番号）	平成27年3月9日 (IT認証5538)
認証番号	C0507
認証申請者	コニカミノルタ株式会社
TOEの名称	bizhub C3850 / bizhub C3350 / bizhub C3850FS / ineo+ 3850 / ineo+ 3350 / ineo+ 3850FS
TOEのバージョン	G0607-999
PP適合	IEEE Std 2600.2™-2009
適合する保証パッケージ	EAL2 及び追加の保証コンポーネントALC_FLR.2
開発者	コニカミノルタ株式会社
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28年4月25日

技術本部
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　山里　拓己

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 3.1 Release 4

② Common Methodology for Information Technology Security Evaluation
Version 3.1 Release 4

評価結果：合格

「bizhub C3850 / bizhub C3350 / bizhub C3850FS / ineo+ 3850 / ineo+ 3350 / ineo+ 3850FS」は、独立行政法人情報処理推進機構が定めるITセキュリティ認証等に関する要求事項に従い、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
1.1　評価対象製品概要 1
1.1.1　保証パッケージ 1
1.1.2　TOEとセキュリティ機能性 1
1.1.2.1　脅威とセキュリティ対策方針 2
1.1.2.2　構成要件と前提条件 2
1.1.3　免責事項 2
1.2　評価の実施 2
1.3　評価の認証 3
2　TOE識別 4
3　セキュリティ方針 5
3.1　セキュリティ機能方針 6
3.1.1　脅威とセキュリティ機能方針 6
3.1.1.1　脅威 6
3.1.1.2　脅威に対するセキュリティ機能方針 6
3.1.2　組織のセキュリティ方針とセキュリティ機能方針 9
3.1.2.1　組織のセキュリティ方針 9
3.1.2.2　組織のセキュリティ方針に対するセキュリティ機能方針 9
4　前提条件と評価範囲の明確化 12
4.1　使用及び環境に関する前提条件 12
4.2　運用環境と構成 12
4.3　運用環境におけるTOE範囲 14
5　アーキテクチャに関する情報 15
5.1　TOE境界とコンポーネント構成 15
5.2　IT環境 17
6　製品添付ドキュメント 17
7　評価機関による評価実施及び結果 18
7.1　評価機関 18
7.2　評価方法 18
7.3　評価実施概要 18
7.4　製品テスト 19
7.4.1　開発者テスト 19
7.4.2　評価者独立テスト 21
7.4.3　評価者侵入テスト 23
7.5　評価構成について 25

7.6　評価結果 26
7.7　評価者コメント/勧告 27
8　認証実施 28
8.1　認証結果 28
8.2　注意事項 28
9　附属書 28
10　セキュリティターゲット 29
11　用語 30
12　参照 31

1 全体要約

この認証報告書は、コニカミノルタ株式会社が開発した「bizhub C3850 / bizhub C3350 / bizhub C3850FS / ineo+ 3850 / ineo+ 3350 / ineo+ 3850FS、バージョン G0607-999」（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。）が平成 28 年 3 月に完了した 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株式会社に報告するとともに、本 TOE に関心を持つ調達者や消費者に対しセキュリティ情報を提供するものである。

本認証報告書の読者は、本書とともに提供されるセキュリティターゲット（以下「ST」という。）を併読されたい。特に本 TOE のセキュリティ機能要件、保証要件及びその十分性の根拠は、ST において詳述されている。

本認証報告書は、本 TOE を購入する調達者を読者と想定している。本認証報告書は、本 TOE が適合する保証要件に基づいた認証結果を示すものであり、個別の IT 製品そのものを保証するものではないことに留意されたい。

1.1 評価対象製品概要

本 TOE の機能、運用条件の概要を以下に示す。詳細は 2 章以降を参照のこと。

1.1.1 保証パッケージ

本 TOE の保証パッケージは、EAL2 及び追加の保証コンポーネント ALC_FLR.2 である。

1.1.2 TOEとセキュリティ機能性

本 TOE は、コピー機能、スキャン機能、印刷機能、ファクス機能、文書の保存と取り出し機能といった基本機能を有するデジタル複合機（以下「MFP」という。）である。

本 TOE は、それらの MFP の基本機能に加えて、基本機能で扱う文書データやセキュリティに影響する設定データ等を漏えいや改ざんから保護するセキュリティ機能を提供する。

これらのセキュリティ機能性について、その設計方針の妥当性と実装の正確性について保証パッケージの範囲で評価が行われた。本 TOE が想定する脅威及び前提については次項のとおりである。

1.1.2.1 脅威とセキュリティ対策方針

本TOEは､以下のとおりのセキュリティ機能によりそれぞれの脅威に対抗する。

TOE の保護資産である利用者の文書データは､TOE への不正アクセスによって、不正に暴露されたり改ざんされたりする脅威がある。

TOE の保護資産であるセキュリティに影響する設定データは、TOE への不正アクセスや､TOE が設置されているネットワーク上の通信データへの不正アクセスによって、不正に暴露されたり改ざんされたりする脅威がある。

それらの脅威に対抗するために、TOE は、識別認証、アクセス制御、暗号化などのセキュリティ機能を提供する。

1.1.2.2 構成要件と前提条件

評価対象製品は、次のような構成及び前提で運用することを想定する。

本 TOE は、MFP にオプション製品である FAX キットを搭載した形で構成される。この FAX キットは TOE 範囲には含まれない。

本 TOE は、TOE の物理的部分やインタフェースが不正なアクセスから保護されるような環境に設置されることを想定している。また、TOE の運用にあたっては、ガイダンス文書に従って適切に設定し、維持管理しなければならない。

1.1.3 免責事項

本 TOE が適合主張する Protection Profile では､ネットワーク上の通信データ保護対象範囲に、本 TOE の保護資産である利用者の文書データは含まれない。

1.2 評価の実施

認証機関が運営する IT セキュリティ評価・認証制度に基づき、公表文書「IT セキュリティ評価及び認証制度の基本規程」[1]、「IT セキュリティ認証等に関する要求事項」[2]、「IT セキュリティ評価機関承認等に関する要求事項」[3]に規定された内容に従い、評価機関によって本 TOE に関わる機能要件及び保証要件に基づいて IT セキュリティ評価が実施され、平成 28 年 3 月に完了した。

1.3 評価の認証

認証機関は、評価機関が作成した評価報告書[13]、所見報告書、及び関連する評価証拠資料を検証し、本 TOE の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については、認証レビューを作成した。認証機関が指摘した問題点は、すべて解決され、かつ、TOE の評価が CC（[4][5][6]または[7][8][9]）及び CEM（[10][11]のいずれか）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。

2 TOE識別

本 TOE は、以下のとおり識別される。

TOE名称：	bizhub C3850 / bizhub C3350 / bizhub C3850FS / ineo+ 3850 / ineo+ 3350 / ineo+ 3850FS
バージョン：	G0607-999
開発者：	コニカミノルタ株式会社

TOE のバージョンは、MFP 基板、SSD 基板、ファームウェアのバージョンの総称である。表 2-1 に TOE の識別の詳細を示す。

表2-1　TOEの識別の詳細

名称（MFP本体名称）	バージョン	
bizhub C3850 / bizhub C3350 / bizhub C3850FS / ineo+ 3850 / ineo+ 3350 / ineo+ 3850FS	MFP基板	A3GNH010-07
	SSD基板	A3GNM71A-01
	ファームウェア	A3GN30G0607-999

製品が評価･認証を受けた本 TOE であることを、利用者は以下の方法によって確認することができる。

TOE の名称は、MFP 本体の表面に印字されている機種名を確認する。TOE のバージョンは、サービスエンジニアに依頼して、MFP 基板と SSD 基板のバージョンである部品番号、及び操作パネルに表示されたファームウェアのバージョンを確認する。

3 セキュリティ方針

本章では、本 TOE が脅威に対抗するために採用したセキュリティ機能方針や組織のセキュリティ方針を説明する。

TOE は、コピー機能、スキャン機能、印刷機能、ファクス機能、文書の保存と取り出し機能といった MFP の基本機能を提供しており、利用者の文書データを TOE 内部の HDD に蓄積したり、ネットワークを介して利用者の端末や各種サーバとやりとりしたりする機能を有している。

TOE は、それらの機能を使用する際に、MFP 用の Protection Profile である IEEE Std 2600.2™-2009 [14]（以下「PP」という。）で要求されているセキュリティ機能要件を満たすセキュリティ機能を提供する。TOE の提供するセキュリティ機能には、利用者の識別認証とアクセス制御、HDD に蓄積した文書データの暗号化と文書データ削除時の上書き消去、暗号化通信などが含まれており、保護資産である利用者の文書データ及びセキュリティに影響する設定データが、不正に暴露されたり改ざんされたりすることを防止する。

なお、TOE は以下の利用者役割を想定している。

・一般利用者

TOE が提供するコピー機能、スキャン機能、印刷機能、ファクス機能、文書の保存と取り出し機能といった MFP の基本機能の利用者である。

・管理者

TOE のセキュリティ機能の設定を行うための特別な権限を持つ TOE の利用者である。

また、TOE の保護資産は以下のものである。

・User Document Data

利用者の文書データ。

・User Function Data

TOE によって処理される利用者の文書データやジョブに関連する情報。

・TSF Confidential Data

セキュリティ機能で使用されるデータの中で、完全性と秘匿性が求められるデータ。本 TOE では、ログインパスワード、暗号鍵の生成に使用される暗号化ワード、監査ログが該当する。

・TSF Protected Data

セキュリティ機能で使用されるデータの中で、完全性だけが求められるデータ。本 TOE では、利用者のユーザ ID と権限、ネットワーク設定など、TSF Confidential Data を除く、セキュリティ機能の各種設定値が該当する。

3.1 セキュリティ機能方針

TOE は、3.1.1 に示す脅威に対抗し、3.1.2 に示す組織のセキュリティ方針を満たすセキュリティ機能を具備する。

3.1.1 脅威とセキュリティ機能方針

3.1.1.1 脅威

本 TOE は、表 3-1 に示す脅威を想定し、これに対抗する機能を備える。これらの脅威は、PP に記述されているものと同じである。

表3-1 想定する脅威

識別子	脅威
T.DOC_REST.DIS	User Document Data at rest (stored) in the TOE may be disclosed to unauthorized persons
T.DOC_REST.ALT	User Document Data at rest (stored) in the TOE may be altered by unauthorized persons
T.FUNC_REST.ALT	User Function Data at rest (stored) in the TOE may be altered by unauthorized persons
T.PROT.ALT	TSF Protected Data may be altered by unauthorized persons
T.CONF.DIS	TSF Confidential Data may be disclosed to unauthorized persons
T.CONF.ALT	TSF Confidential Data may be altered by unauthorized persons

3.1.1.2 脅威に対するセキュリティ機能方針

本 TOE は、表 3-1 に示す脅威に対し、以下のセキュリティ機能方針で対抗する。

(1) 脅威「T.DOC_REST.DIS」「T.DOC_REST.ALT」「T.FUNC_REST.ALT」への対抗

これらは TOE への不正なアクセスによる利用者データ（User Document Data と User Function Data）への侵害（漏えい、改ざん）に関する脅威であり、TOE

は、以下に示す「識別認証機能」、「利用者制限制御機能」、「保存文書アクセス制御機能」及び「残存情報消去機能」で対抗する。

a. 識別認証機能

本機能は、TOE の利用者をユーザ ID とログインパスワードで識別認証する機能である。識別認証は、以下に示す利用者インタフェースのすべてに適用される。

- 操作パネル
- クライアント PC (Web ブラウザ、プリンタドライバ、各種ツール)

認証方式には、TOE に格納されたユーザ ID とログインパスワードを使用する「本体認証」と、TOE 外部の Kerberos サーバを使用する「外部サーバ認証」がある。

また、識別認証機能を補強するために、以下の機能を備えている。

- ログインパスワードは 8 桁以上の所定の品質が要求される。
- 連続した認証失敗回数が 3 回に達すると認証を停止する。
- 識別認証後、一定時間操作がない場合には、セッションを終了する。

ログインパスワードの品質チェックは、本体認証の場合にはログインパスワードの設定変更時に行われる。外部サーバ認証の場合にはログイン時に行われ、外部認証サーバに登録されたログインパスワードが TOE の品質を満足しない場合は、ログインは許可されない。

b. 利用者制限制御機能

本機能は、識別認証された利用者の操作に対するアクセス制御と、TOE の利用に伴って生成される文書データに対するアクセス制御を行う機能である。ただし、蓄積された文書データに対するアクセス制御は「保存文書アクセス制御機能」で行う。

利用者が、印刷機能、コピー機能、スキャン機能、ファクス機能、文書の保存と取り出し機能といった MFP の基本機能を使用する際には、利用者に設定された権限をチェックし、権限のある基本機能だけが実行を許可される。

利用者が、文書データに対して印刷などの操作を行う際には、文書データの所有者だけが操作を許可される。文書データを削除する場合には、文書データの所有者と管理者だけが削除を許可される。

c. 保存文書アクセス制御機能

本機能は、TOEのHDDに保存された文書データに対するアクセス制御を行い、権限のある利用者だけに文書データに対する操作を許可する機能である。

文書データが HDD に保存される際に文書データ毎に関連付けられた、利用者識別等の属性値を基に利用者からの操作要求に対して許可もしくは拒否の制御を行う。

なお、管理者は、保存されたすべての文書データの削除が可能である。

d. 残存情報消去機能

本機能は、文書データが格納される HDD の領域を上書き消去し、残存情報の再利用を防止する機能である。本機能は、以下のタイミングで実行される。

- MFP の基本機能が終了し文書データが不要になった時。TOE の処理の都合で TOE 内に一時的に作成されたデータも対象に含まれる。
- 利用者の指示で文書データを削除した時。
- 電源 ON にした時。電源 OFF 時に上書き消去処理が未完了の場合には、電源 ON 時に処理が再開される。
- 管理者により HDD 上のデータ領域全体の消去機能が実行された時。

上書きするデータのパターンは、管理者の設定で複数のパターンの中から選択することができる。

(2) 脅威「T.PROT.ALT」「T.CONF.DIS」「T.CONF.ALT」への対抗

これらは TOE への不正なアクセス及びネットワーク上の通信データへの不正なアクセスによる、セキュリティ機能で使用されるデータへの侵害（漏えい、改ざん）に関する脅威であり、TOE は「識別認証機能」、「セキュリティ管理機能」及び「ネットワーク通信保護機能」で対抗する。

a. 識別認証機能

(1)に記載の識別認証機能により、TOE を利用しようとする者が許可利用者であることを、利用者から取得した識別認証情報を使って検証し、許可利用者と判断された者だけに TOE の利用を許可する。

b. セキュリティ管理機能

本機能は、セキュリティ機能で使用されるデータの設定、参照、変更を、識別認証された管理者だけに許可する機能である。ただし、一般利用者は、本人のログインパスワードのみ変更可能である。

c. ネットワーク通信保護機能

本機能は、IT 機器との通信において、以下の暗号化通信を行う機能である。

・クライアント PC：TLS（v1.0、v1.1、v1.2）
・外部認証サーバ：IPsec
・SMTP サーバ：IPsec
・DNS サーバ：IPsec

3.1.2 組織のセキュリティ方針とセキュリティ機能方針

3.1.2.1 組織のセキュリティ方針

本 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 3-2 に示す。これらの組織のセキュリティ方針は、P.HDD.CRYPTO が追加されていることを除いて、PP に記述されているものと同じである。

表3-2 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.USER.AUTHORIZATION	To preserve operational accountability and security, Users will be authorized to use the TOE only as permitted by the TOE Owner.
P.SOFTWARE.VERIFICATION	To detect corruption of the executable code in the TSF, procedures will exist to self-verify executable code in the TSF.
P.AUDIT.LOGGING	To preserve operational accountability and security, records that provide an audit trail of TOE use and security-relevant events will be created, maintained, and protected from unauthorized disclosure or alteration, and will be reviewed by authorized personnel.
P.INTERFACE.MANAGEMENT	To prevent unauthorized use of the external interfaces of the TOE, operation of those interfaces will be controlled by the TOE and its IT environment.
P.HDD.CRYPTO	The Data stored in an HDD must be encrypted to improve the secrecy.

3.1.2.2 組織のセキュリティ方針に対するセキュリティ機能方針

TOE は、表 3-2 に示す組織のセキュリティ方針を満たす機能を具備する。

(1) 組織のセキュリティ方針「P.USER.AUTHORIZATION」への対応

TOE は、「識別認証機能」及び「利用者制限制御機能」で本方針を実現する。

3.1.1.2 に記述した「識別認証機能」及び「利用者制限制御機能」は、識別認証の成功した利用者だけに TOE の利用を許可し、その利用者が、コピー機能、スキャン機能、印刷機能、ファクス機能、文書の取り出し機能といった MFP の基本機能を使用する際に、利用者に付与された権限をチェックし、権限のある利用者だけに基本機能の実行を許可する。

(2) 組織のセキュリティ方針「P.SOFTWARE.VERIFICATION」への対応

TOE は、「自己テスト機能」で本方針を実現する。

a. 自己テスト機能

本機能は、TOE の起動時に以下の自己テストを行う機能である。

- TOE 内蔵の検証用データによる、暗号化ワードの検証
- 制御ソフトウェアのハッシュ値の確認による実行コードの完全性検証

(3) 組織のセキュリティ方針「P.AUDIT.LOGGING」への対応

TOE は、「監査ログ機能」で本方針を実現する。

a. 監査ログ機能

本機能は、監査対象となるセキュリティ事象が発生した際に、事象の発生日時、事象の識別情報、利用者識別、事象の結果等の項目からなる監査ログを生成し保存する。生成した監査ログは識別認証に成功した管理者のみに読み出しや削除等の操作を制限する。

(4) 組織のセキュリティ方針「P.INTERFACE.MANAGEMENT」への対応

TOE は、「識別認証機能」と「外部インタフェース分離機能」で、本方針を実現する。

a. 識別認証機能

3.1.1.2 に記述した「識別認証機能」により識別認証の成功した利用者だけに TOE の利用を許可する。また、利用者が操作をしない状態が規定時間経過した場合には、セッションを切断する。

b. 外部インタフェース分離機能

本機能は、電話回線を含む外部インタフェースから LAN への不正な転送を防止する機能である。TOE の外部インタフェースから受信したデータは、TOE が必ず介在して処理する。

(5) 組織のセキュリティ方針「P.HDD.CRYPTO」への対応

TOE は、「HDD 暗号化機能」で本方針を実現する。

a. HDD 暗号化機能

本機能は、HDD に保存するデータを暗号化する機能である。暗号アルゴリズムは、256bit の AES である。暗号鍵は、導入時に管理者が設定する 20 桁の暗号化ワードを元に、FIPS180-3 によって規定される SHA-256 アルゴリズムにより作成する。

4 前提条件と評価範囲の明確化

本章では、想定する読者が本 TOE の利用の判断に有用な情報として、本 TOE を運用するための前提条件及び運用環境について記述する。

4.1 使用及び環境に関する前提条件

本 TOE を運用する際の前提条件を表 4-1 に示す。これらの前提条件は、PP に記述されているものと同じである。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4-1 前提条件

識別子	前提条件
A.ACCESS.MANAGED	The TOE is located in a restricted or monitored environment that provides protection from unmanaged access to the physical components and data interfaces of the TOE.
A.USER.TRAINING	TOE Users are aware of the security policies and procedures of their organization, and are trained and competent to follow those policies and procedures.
A.ADMIN.TRAINING	Administrators are aware of the security policies and procedures of their organization, are trained and competent to follow the manufacturer's guidance and documentation, and correctly configure and operate the TOE in accordance with those policies and procedures.
A.ADMIN.TRUST	Administrators do not use their privileged access rights for malicious purposes.

4.2 運用環境と構成

本 TOE は、オフィスに設置されて、内部の LAN に接続し、同様に内部の LAN に接続されたクライアント PC から利用される。本 TOE の一般的な運用環境を図 4-1 に示す。

なお、図 4-1 には示されていないが、クライアント PC は、USB ポート経由で TOE である MFP と接続し、TOE の印刷機能を使用することもできる。

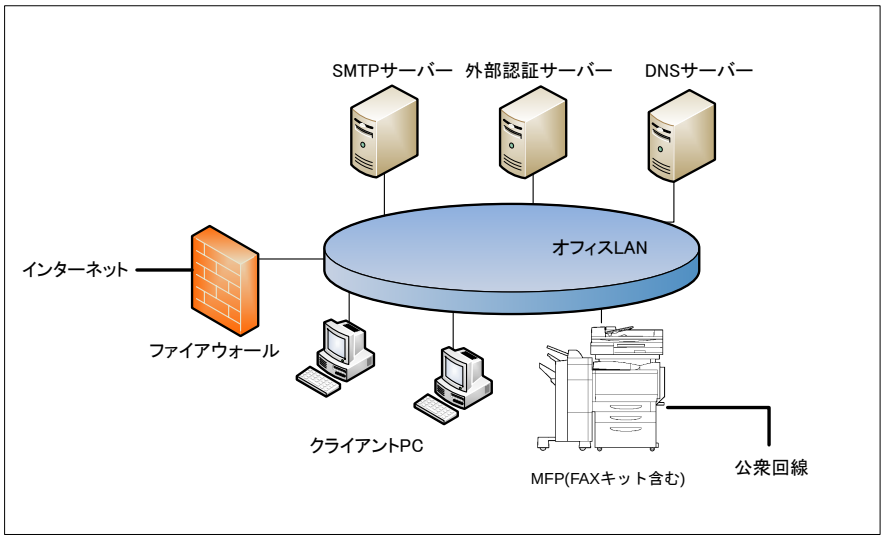

図 4-1 TOEの運用環境

図 4-1 において、MFP が TOE である。ただし、MFP に内蔵する FAX キットは TOE に含まない。TOE である MFP 以外の構成品を以下に示す。

(1) FAX キット

公衆回線を経由して、ファクスデータの送受信と遠隔診断機能の通信を行う。以下の MFP 用オプションが必要である。

・コニカミノルタ株式会社 FK-512

(2) クライアント PC

利用者が、LAN または USB ポート経由で、TOE の提供する機能を利用するために使用する。以下のソフトウェアが必要である。

表4-2　クライアントPCのソフトウェア

種別	名称とバージョン
Webブラウザ	・Microsoft Internet Explorer Ver.11 ・Mozilla Firefox Ver.36
プリンタドライバ	・KONICA MINOLTA C3850 Series PCL6 Ver. 3.0.1、XPS Ver. 3.0.2
管理者用ツール	・KONICA MINOLTA Data Administrator with Device Set-Up and Utilities Ver. 1.0.06000 ・KONICA MINOLTA Data Administrator 4.1.35000

(3) SMTP サーバ

TOE 内の文書データをメール送信する機能を使用する場合に必要である。

(4) 外部認証サーバ

TOE の利用者を Kerberos プロトコルで識別認証する。TOE の設定で、外部サーバ認証方式を選択した場合に必要である。本評価では、以下のソフトウェアを使用する。

・Microsoft Windows Server 2008 R2 Standard Service Pack1 に搭載される Active Directory

(5) DNS サーバ

ドメイン名を IP アドレスに変換するサーバである。本評価では、以下のソフトウェアを使用する。

・Microsoft Windows Server 2008 R2 Standard Service Pack1 に搭載される DNS サーバ

なお、本構成に示されている、TOE 以外のハードウェア及び連携するソフトウェアの信頼性は本評価の範囲ではない（十分に信頼できるものとする）。

4.3 運用環境におけるTOE範囲

本 TOE の範囲は MFP 製品全体である。但し本 TOE には FAX インタフェースを提供するオプション製品である FAX キットが内蔵されるが、この FAX キットは TOE の範囲外である。

5 アーキテクチャに関する情報

本章では、本 TOE の範囲と主要な構成（サブシステム）を説明する。

5.1 TOE境界とコンポーネント構成

TOE の構成を図 5-1 に示す。TOE は MFP 製品全体である。

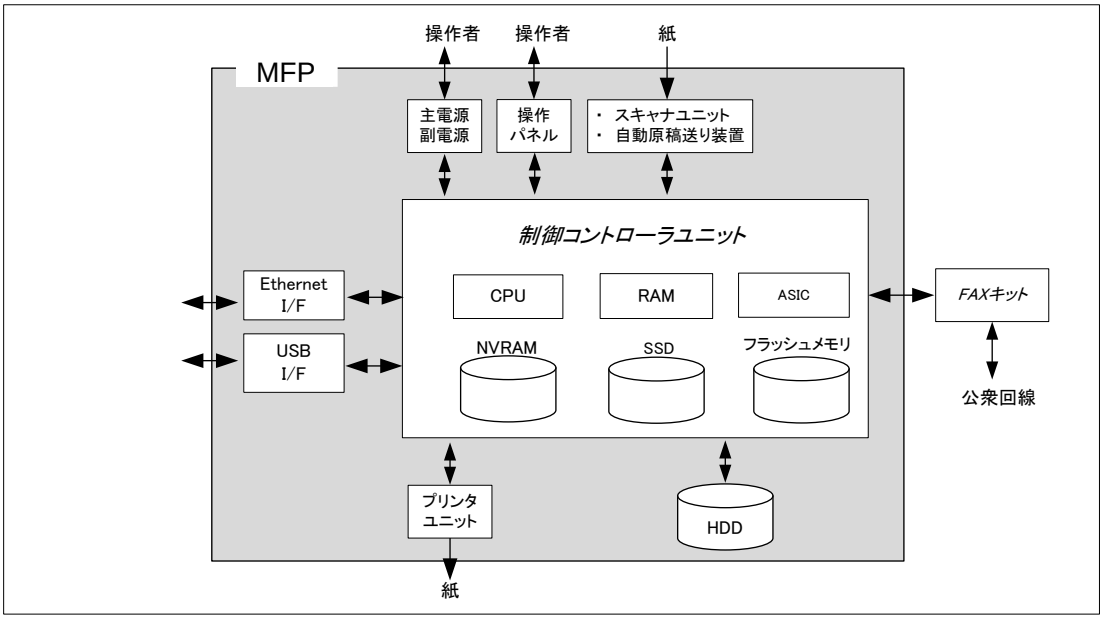

図 5-1 TOE境界

TOE は図 5-1 に示すように、主電源・副電源、操作パネル、スキャナユニット・自動原稿送り装置、制御コントローラユニット、プリンタユニット、HDD で構成される MFP である。以下に各構成要素の概要を示す。

(1) 主電源・副電源

MFP を動作させるための電源スイッチ。

(2) 操作パネル

タッチパネル液晶ディスプレイとテンキー やスタートキー、ストップキー、画面の切り替えキー等を備えた MFP を操作するための専用コントロールデバイス。

(3) スキャナユニット／自動原稿送り装置

紙から図形、写真を読み取り、電子データに変換するためのデバイス。

(4) 制御コントローラユニット

MFP を制御する装置。

(5) CPU

中央演算処理装置。

(6) RAM

作業領域として利用される揮発メモリ。

(7) ASIC

画像処理全般を行うために設計された集積回路。また、画像を印刷する時に画像の展開と色合いの調整等の処理も行う。

(8) NVRAM

MFP の動作を決定する TSF データが保存される不揮発メモリ。

(9) SSD

制御ソフトウェアのオブジェクトコード(操作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で表示するための各国言語メッセージデータを含む）が保存される記憶媒体。

(10) フラッシュメモリ

TOE(Boot 制御部)のオブジェクトコードが保存される不揮発性メモリ。

(11) プリンタユニット

制御コントローラからの指示により、印刷用に変換された画像データを印刷出力するデバイス。

(12) HDD

ハードディスクドライブ。電子文書がファイルとして保存されるほか、作業領域としても利用される。

(13) Ethernet I/F

10BASE-T、100BASE-TX、Gigabit Ethernet をサポートするインタフェース。

(14) USB I/F

TOE のアップデートなどを実施できるインタフェース。

(15) FAX キット

公衆回線を介して FAX の送受信や遠隔診断機能の通信に利用されるデバイス。これは TOE 外である。

5.2 IT環境

TOE は、外部サーバ認証方式の場合には、外部の認証サーバ（Kerberos プロトコル）を使用して、利用者の識別認証を行う。

TOE のファクス機能は、TOE に含まれていない FAX キットを介して、ファクスデータの送受信を行う。ただし、ファクス機能に関するアクセス制御や不正アクセス防止などのセキュリティ機能は、TOE 内で実現している。

6 製品添付ドキュメント

本 TOE に添付されるドキュメントの識別を以下に示す。本 TOE のドキュメントには日本語版と 2 種類の英語版があり、販売地域によりいずれかが添付される。

TOE の利用者は、前提条件を満たすため下記ドキュメントの十分な理解と遵守が要求される。

（日本語版）

・bizhub C3850 ユーザーズガイド　2015.3 Ver. 1.00

・bizhub C3850 ユーザーズガイド セキュリティー機能編　2.02

（英語版）

・bizhub C3850FS/C3850/C3350 user's Guide　2015.4 Ver. 1.00

・bizhub C3850FS/C3850/C3350 user's Guide [Security Operations]　2.02

（英語版）

・ineo+ 3850FS/3850/3350 User's Guide　2015.4 Ver. 1.00

・ineo+ 3850FS/3850/3350 User's Guide [Security Operations]　2.02

7 評価機関による評価実施及び結果

7.1 評価機関

評価を実施したみずほ情報総研株式会社 情報セキュリティ評価室は、IT セキュリティ評価及び認証制度により承認されるとともに、ILAC（国際試験所認定協力機構）と相互承認している認定機関（独立行政法人製品評価技術基盤機構認定センター）により認定を受けており、評価品質維持のためのマネジメント及び要員等の適切性についての要求事項を満たしていることが定期的に確認されている。

7.2 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た。評価報告書では、本TOEの概要と、CEMのワークユニットごとの評価内容及び判断結果を説明する。

7.3 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 27 年 2 月に始まり、平成 28 年 3 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 27 年 10 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 28 年 1 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。

また、認証機関が見つけた評価の問題点は、認証レビューとして記述されて、評価機関へ渡された。

これらの指摘は、評価機関及び開発者が検討したのち、評価報告書に反映された。

7.4 製品テスト

評価者は、開発者の実施したテストの正当性を確認し、評価の過程で示された証拠と開発者のテストを検証した結果から、必要と判断された再現・追加テスト及び脆弱性評定に基づく侵入テストを実行した。

7.4.1 開発者テスト

評価者は、開発者が実施した開発者テストの完全性と実際のテスト結果の証拠資料を評価した。評価者が評価した開発者テストの内容を以下に説明する。

(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 7-1 に、主な構成要素を表 7-1 に示す。

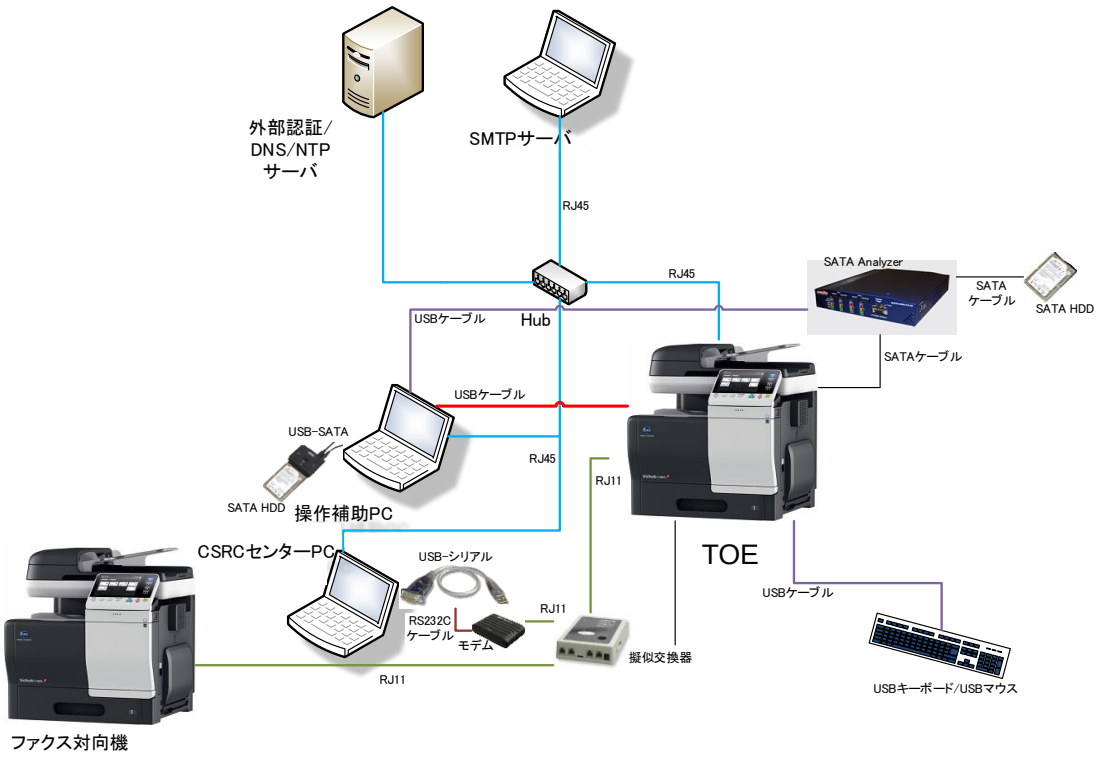

図 7-1 開発者テストの構成図

表 7-1 開発テストツール

名称	詳細
MFP本体 (TOE)	bizhub C3850/C3350/C3850FS

名称	詳細
MFP本体内蔵 FAXキット	コニカミノルタ社　FK-512
操作補助PC (クライアントPC)	・Windows7 SP1搭載PC ※上記に表4-2に示した各種ドライバやツールを搭載
外部認証サーバ	・Windows Server 2008 R2 Standard SP1搭載PC ・Kerberosソフトウェア: Active Directory (OS付属)
SMTPサーバ	・Windows7 SP1搭載PC
DNSサーバ	・Windows Server 2008 R2 Standard SP1搭載PC ・DNSソフトウェア: OS付属
CSRC センター PC	コニカミノルタ社の遠隔診断のサービスと同じ機能を提供するサーバ ・Windows7 SP1搭載PC ・CSRCセンターソフトウェア Ver.2.8.1
FAX対向機	bizhub C3850/C3350/C3850FS
疑似交換機 (公衆回線)	公衆回線を疑似的に実現する回線交換機
USBメモリ	ファームウェアの更新テスト、使用制限状態の確認テストに使用
USBキーボード、 マウス	USBポートの動作確認テストに使用
SATA Analyzer	HDD書き込み処理のキャプチャに使用
ターミナル用PC	RS232Cを経由してTOEの開発者用インタフェースと接続 ・Windows7 SP1 搭載PC ・ターミナルソフトウェア: Tera Term Ver.4.86

開発者テストで使用されたTOEはSTで識別されている複数のMFPの一部の機種であるが、他の機種はテストで使用したMFPのOEM製品で、製品名の違い以外は同一機種である。

このことから、開発者テストにおいてテスト対象に選択された機種「bizhub C3850」、「bizhub C3350」、「bizhub C3850FS」は、STの記載内容と矛盾がなく、STにおいて識別されているTOE構成をカバーしていると評価において判断され、開発者テストは本STにおいて識別されているTOE構成と同一のテスト環境で実施されていると判断された。

(2) 開発者テスト概説

開発者テストの概説は以下のとおりである。

a) **テスト概要**

開発者テストの概要は、以下のとおりである。

＜開発者テスト手法＞

TOE の外部インタフェースについて、TOE の操作パネル、PC、テストツールを使用して入力を行い、そのふるまいの確認を行った。ふるまいの確認には、以下のような手法が用いられている。

- TOE が提供しているインタフェースで確認可能なふるまいについては、それを利用して、入力に対する応答、TOE の動作、監査ログ、通信データを確認する。

- TOE が提供しているインタフェースでは確認できない TOE 内部のデータや HDD 上のデータについては、開発者インタフェースを使用して確認する。

暗号アルゴリズムについては、上記の方法で取得したデータと OpenSSL で暗号化したデータを比較することで、仕様どおりに実装されていることを確認している。

＜開発者テストの実施内容＞

開発者が提供した仕様書に記載された期待されるテスト結果の値と、同じく開発者が提供したテスト結果報告に記載された開発者テストの結果の値を比較した。その他結果、期待されるテスト結果の値と実際のテスト結果の値が一致していることが確認された。

b) **開発者テストの実施範囲**

開発者テストは開発者によって184項目実施された。

カバレージ分析によって、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テストされたことが検証された。

c) **結果**

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、テスト計画書に示された実施方法と実際の実施方法が一致することを確認した。評価者は、開発者が期待したテスト結果と開発者によって実施されたテスト結果が一致していることを確認した。

7.4.2 評価者独立テスト

評価者は、開発者テストから抽出したテスト項目を使用して製品のセキュリティ機能が実行されることを再確認するサンプルテストを実施するとともに、評価の過

程で示された証拠から、製品のセキュリティ機能が確実に実行されることをより確信するための独立テスト（以下「独立テスト」という。）を実施した。評価者が実施した独立テストを以下に説明する。

(1) 独立テスト環境

評価者が実施した独立テストの構成は、図 7-1 に示した開発者テストと同様の構成である。

(2) 独立テスト概説

評価者の実施した独立テストは以下のとおりである。

a) 独立テストの観点

評価者が、開発者テスト及び提供された評価証拠資料から考案した独立テストの観点を以下に示す。

＜独立テストの観点＞

①網羅性の観点で開発者テストが不足していると思われるパラメタの組み合わせ、境界値等のテスト項目を追加する。

② 開発者テストで実施されていない複数のインタフェースや操作を組み合わせたふるまいを確認する。

③ 例外処理に関して開発者テストと異なるバリエーションを追加したテスト項目を実施する。

④ サンプリングテストでは、以下の観点でテスト項目を抽出する。

・網羅性の観点から全てのセキュリティ機能、外部インタフェースが含まれるように項目を選択する

・異なるテスト手法、テスト環境を網羅するように項目を選択する

b) 独立テスト概要

評価者が実施した独立テストの概要は以下のとおりである。

＜独立テスト手法＞

独立テストは、開発者テストと同じテスト手法で実施された。

＜独立テストの実施内容＞

独立テストの観点に基づき、独立テスト 11 項目、サンプリングテスト 58 項目のテストが実施された。

独立テストの観点とそれに対応したテスト内容を表 7-2 に示す。

表 7-2 実施した主な独立テスト

観点	テスト概要
①	・ログインパスワード、暗号化ワードなどについて、変更時に最大文字数より一桁多い文字列を入力した場合のふるまいが仕様通りであることを確認する。
②	・異なるインタフェース経由でアクセスした場合でもアカウントロックに関する挙動が仕様通りであることを確認する。 ・アカウントロックに関するふるまいの確認を開発者テストとは違う認証モードでも行う。 ・利用者の複数の権限を一度の操作で変更した場合においても仕様通りのアクセス制御が行われることを確認する。
③	・公衆回線からのデータ制御のふるまいについて、開発者テストと異なるデータについても、不正なデータが拒否されることを確認する。

c) 結果

評価者が実施したすべての独立テストは正しく完了し、評価者は TOE のふるまいを確認した。評価者は、すべてのテスト結果と期待されるふるまいが一致していることを確認した。

7.4.3 評価者侵入テスト

評価者は、評価の過程で示された証拠から、想定される使用環境と攻撃レベルにおいて懸念される脆弱性となる可能性があるものについて、必要と思われる評価者侵入テスト（以下「侵入テスト」という。）を考案し実施した。評価者が実施した侵入テストを以下に説明する。

(1) 侵入テスト概説

評価者が実施した侵入テストの概説は以下のとおりである。

a) 懸念される脆弱性

評価者は、提供された証拠資料や公知の情報より、潜在的な脆弱性を探索し、侵入テストを必要とする以下の脆弱性を識別した。

① ネットワークインタフェースに公知の脆弱性が存在する可能性がある。
② TOEが意図しない値、形式のデータ入力が行われた場合、セキュリティ機能がバイパスされる可能性がある。
③ 過負荷状態でTOEを運用することにより、セキュリティ機能がバイパスされる可能性がある。

④ TOEのファームウェアからの情報収集や不正なファームウェアの書き換えによりセキュリティ機能が侵害される可能性がある。
⑤ 想定外の電源操作が行われることでセキュリティ機能がバイパスされる可能性がある。

b) **侵入テストの概要**

評価者は、潜在的な脆弱性が悪用される可能性を検出するために、以下の侵入テストを実施した。

＜侵入テスト環境＞

侵入テストは、図 7-1 に示した開発者テスト、及び評価者独立テストと同様の環境で実施された。

侵入テストで使用した主なツールを表 7-3 に示す。

表 7-3　侵入テスト使用ツール

名称（バージョン）	概要
Nessus (Version 6.5.4)	脆弱性スキャンツール
nmap (Version 7.01)	ポートスキャンツール
Nikto (Version 2.1.5)	脆弱性スキャンツール
Metasploit (Version 4.11.4)	Exploitの構築、実行フレームワーク
TamperIE (Version 1.0.1.13)	Webデバッガ

＜侵入テストの実施項目＞

懸念される脆弱性と対応する侵入テスト内容を表 7-4 に示す。評価者は潜在的な脆弱性が悪用される可能性の有無を決定するため、12 項目の侵入テストを実施した。

表 7-4　侵入テスト概要

脆弱性	テスト概要
①	・ポートスキャンツール、脆弱性スキャンツールを使用し、必要としないネットワークポートが開いていないことやオープンポートに公知の脆弱性がないことを確認する。

②	・USBキーボードからの入力データに対する脆弱性が存在しないことを確認する。 ・悪用される可能性のある印刷ジョブコマンドや、不正な処理を含むPDFファイルをTOEに入力しても、処理が実行されないことを確認する。 ・Webデバッガを使用して、WebブラウザからのTOEへの通信データを書き換えても、セキュリティ機能がバイパスされないことを確認する。 ・Web以外の独自インタフェースについても想定外の入力データによりセキュリティ機能がバイパスされないことを確認する。
③	・リソース枯渇状態においてTOEが非セキュアな状態にならないことを確認する。
④	・TOEのファームウェアをバイナリ解析し、容易に抽出可能な秘密情報がないことを確認する。 ・不正に改ざんされたファームウェアを用いた更新機能が実行できないことを確認する。
⑤	・セキュリティ機能の動作中に電源OFF等の操作が行われてもセキュリティ機能がバイパスされないことを確認する。

c) **結果**

評価者が実施した侵入テストでは、想定する攻撃能力を持つ攻撃者が悪用可能な脆弱性は確認されなかった。

7.5 評価構成について

本評価では、図 7-1 に示す構成において、評価を行った。ネットワークは IPv4 を使用している。本 TOE は、上記と構成要素が大きく異なる構成において、運用される場合はない。よって、評価者は、上記の評価構成は、適切であると判断した。

7.6 評価結果

評価者は、評価報告書をもって本 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。

評価では以下について確認された。

・PP 適合：
2600.2-PP, Protection Profile for Hardcopy Devices, Operational Environment B
（IEEE Std 2600.2™-2009）

また、上記 PP で定義された以下の SFR パッケージに適合する。
- 2600.2-PRT, SFR Package for Hardcopy Device Print Functions, Operational Environment B
- 2600.2-SCN, SFR Package for Hardcopy Device Scan Functions, Operational Environment B
- 2600.2-CPY, SFR Package for Hardcopy Device Copy Functions, Operational Environment B
- 2600.2-FAX, SFR Package for Hardcopy Device Fax Functions, Operational Environment B
- 2600.2-DSR, SFR Package for Hardcopy Device Document Storage and Retrieval (DSR) Functions, Operational Environment B
- 2600.2-SMI, SFR Package for Hardcopy Device Shared-medium Interface Functions, Operational Environment B

・セキュリティ機能要件：　コモンクライテリア　パート 2　拡張
・セキュリティ保証要件：　コモンクライテリア　パート 3　適合

評価の結果として、以下の保証コンポーネントについて「合格」判定がなされた。

・EAL2 パッケージのすべての保証コンポーネント
・追加の保証コンポーネント　ALC_FLR.2

評価の結果は、第 2 章に記述された識別に一致する TOE によって構成されたもののみに適用される。

7.7 評価者コメント/勧告

調達者に喚起すべき評価者勧告は、特にない。

8 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 所見報告書でなされた指摘内容が妥当であること。

② 所見報告書でなされた指摘内容が解決されていること。

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、本 ST 及び評価報告書において、認証レビューで指摘された問題点が解決されていることを確認し、本認証報告書を発行した。

8.1 認証結果

提出された評価報告書、所見報告書及び関連する評価証拠資料を検証した結果、認証機関は、本 TOE が CC パート 3 の EAL2 及び保証コンポーネント ALC_FLR.2 に対する保証要件を満たすものと判断する。

8.2 注意事項

本 TOE に興味のある調達者は、「1.1.3 免責事項」、「4.3 運用環境における TOE 範囲」及び「7.5 評価構成について」の記載内容を参照し、本 TOE の評価対象範囲や運用上の要求事項が、各自の想定する運用条件に合致しているかどうか注意が必要である。

9 附属書

特になし。

10 セキュリティターゲット

本 TOE のセキュリティターゲット[12]は、本報告書とは別文書として以下のとおり本認証報告書とともに提供される。

bizhub C3850 / bizhub C3350 / bizhub C3850FS /ineo+ 3850 / ineo+ 3350 / ineo+ 3850FS セキュリティターゲット
バージョン 1.16, 2016 年 3 月 11 日, コニカミノルタ株式会社

11 用語

本報告書で使用された CC に関する略語を以下に示す。

CC	Common Criteria for Information Technology Security Evaluation（セキュリティ評価基準）
CEM	Common Methodology for Information Technology Security Evaluation（セキュリティ評価方法）
EAL	Evaluation Assurance Level（評価保証レベル）
PP	Protection Profile（プロテクションプロファイル）
ST	Security Target（セキュリティターゲット）
TOE	Target of Evaluation（評価対象）
TSF	TOE Security Functionality（TOEセキュリティ機能）

本報告書で使用された TOE に関する略語を以下に示す。

MFP	デジタル複合機の略称

本報告書で使用された用語の定義を以下に示す。

暗号化ワード	HDD暗号化の暗号鍵の生成に使用される20桁の文字列
遠隔診断機能	MFPの保守のために、公衆回線を経由してコニカミノルタ社のサポートセンターと接続し、MFPの動作状態や印刷数等の機器情報を通信する機能

12 参照

[1] ITセキュリティ評価及び認証制度の基本規程, 平成27年6月, 独立行政法人情報処理推進機構, CCS-01

[2] ITセキュリティ認証等に関する要求事項, 平成27年10月, 独立行政法人情報処理推進機構, CCM-02

[3] ITセキュリティ評価機関承認等に関する要求事項, 平成27年10月, 独立行政法人情報処理推進機構, CCM-03

[4] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1 Revision 4, September 2012, CCMB-2012-09-001

[5] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1 Revision 4, September 2012, CCMB-2012-09-002

[6] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 4, September 2012, CCMB-2012-09-003

[7] 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3.1 改訂第4版, 2012年9月, CCMB-2012-09-001, (平成24年11月, 翻訳第1.0版)

[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2: セキュリティ機能コンポーネント, バージョン3.1 改訂第4版, 2012年9月, CCMB-2012-09-002, (平成24年11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3: セキュリティ保証コンポーネント, バージョン3.1 改訂第4版, 2012年9月, CCMB-2012-09-003, (平成24年11月, 翻訳第1.0版)

[10] Common Methodology for Information Technology Security Evaluation : Evaluation methodology, Version 3.1 Revision 4, September 2012, CCMB-2012-09-004

[11] 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3.1 改訂第4版, 2012年9月, CCMB-2012-09-004, (平成24年11月, 翻訳第1.0版)

[12] bizhub C3850 / bizhub C3350 / bizhub C3850FS /ineo+ 3850 / ineo+ 3350 / ineo+ 3850FS セキュリティターゲット, バージョン 1.16, 2016年3月11日, コニカミノルタ株式会社

[13] bizhub C3850 / bizhub C3350 / bizhub C3850FS /ineo+ 3850 / ineo+ 3350 / ineo+ 3850FS 評価報告書, 第1版, 2016年3月11日, みずほ情報総研株式会社 情報セキュリティ評価室

[14] IEEE Std 2600.2™-2009, IEEE Standard for a Protection Profile in Operational Environment B, Version 1.0, March 2009