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7月9日** (IT**認証**7160)
認証番号	C0118
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：**bizhub PRO C5500 / ineo+ 5500 **画像制御プログラム** **海外：**bizhub PRO C5500 / ineo+ 5500 Image Control Program
TOE**のバージョン**	A0E70Y0-00I1-G00-10
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9月27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　田渕　治樹

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：bizhub PRO C5500 / ineo+ 5500 画像制御プログラム、海外：bizhub PRO C5500 / ineo+ 5500 Image Control Program、バージョン：A0E70Y0-00I1-G00-10」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：bizhub PRO C5500 / ineo+ 5500 画像制御プログラム、海外：bizhub PRO C5500 / ineo+ 5500 Image Control Program、バージョン：A0E70Y0-00I1-G00-10」（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：bizhub PRO C5500 / ineo+ 5500 画像制御プログラム 海外：bizhub PRO C5500 / ineo+ 5500 Image Control Program
バージョン：	A0E70Y0-00I1-G00-10
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

本製品（以下「bizhub PRO C5500 画像制御プログラム(*1)」という。）はコニカミノルタビジネステクノロジーズ株式会社製デジタル複合機（以下「bizhub PRO C5500シリーズ」という。)に搭載され、bizhub PRO C5500シリーズ内部のドキュメントデータの漏洩に対する危険性を減ずることを目的としたソフトウェア製品である。

bizhub PRO C5500 画像制御プログラムは、コピー/プリンタなどを活用した機能において、bizhub PRO C5500シリーズ内部のドキュメントデータの漏洩を防止する。このため、ドキュメントデータを一時保存する媒体であるHDD（ハードディスク装置）から不正にデータが読み出される危険性に対して、ロックパスワードによる保護機能(*2)を提供する。

bizhub PRO C5500シリーズの利用環境として「図1-1 bizhub PRO C5500シリーズの利用環境」に示すオフィスを想定する。

（*1）日本：bizhub PRO C5500 / ineo+ 5500 画像制御プログラム、海外：bizhub PRO C5500 / ineo+ 5500 Image Control Programのことを示す。

（*2）ハードディスクを取外し他の機器で読み込みができないように、ハードディスクにパスワードを持たせる機能のことをいう。ハードディスクロック機能で設定するパスワードをHDDロックパスワードという。

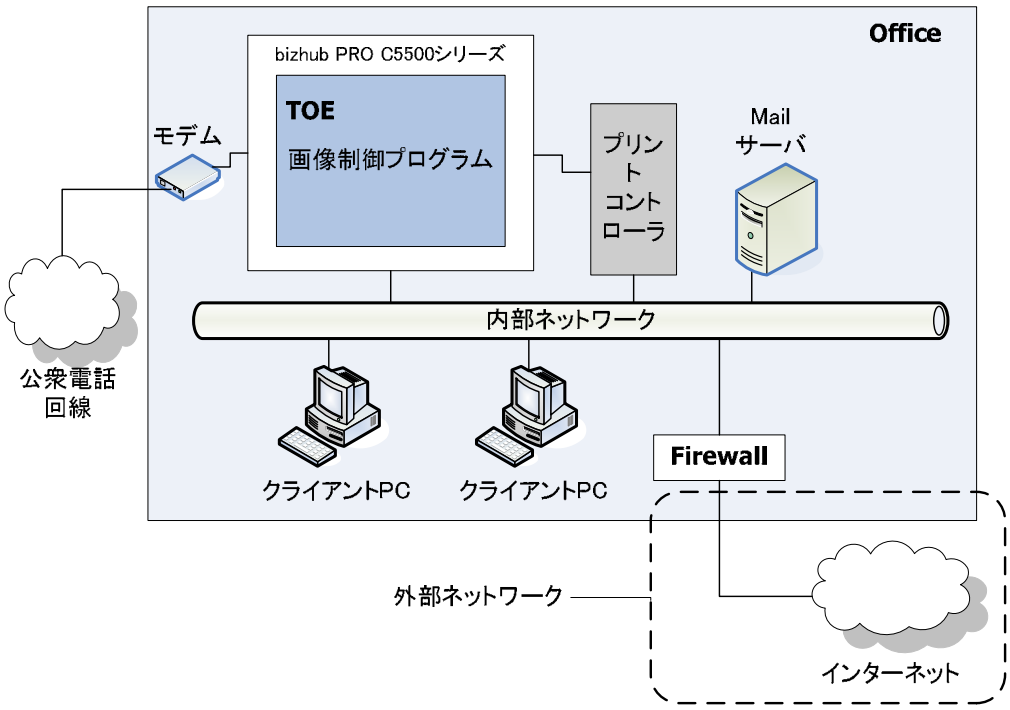

図1-1　bizhub PRO C5500シリーズの利用環境

本TOEを搭載するbizhub PRO C5500シリーズは、図1-1に示すように内部ネットワーク及び公衆電話回線網に接続される。また、内部ネットワークの各機器を保護するため、外部ネットワークとの接続を行う場合はFirewallを介して接続する。

1.2.3 TOEの範囲と動作概要

本TOEを含むbizhub PRO C5500シリーズの構成を図1-2に示す。

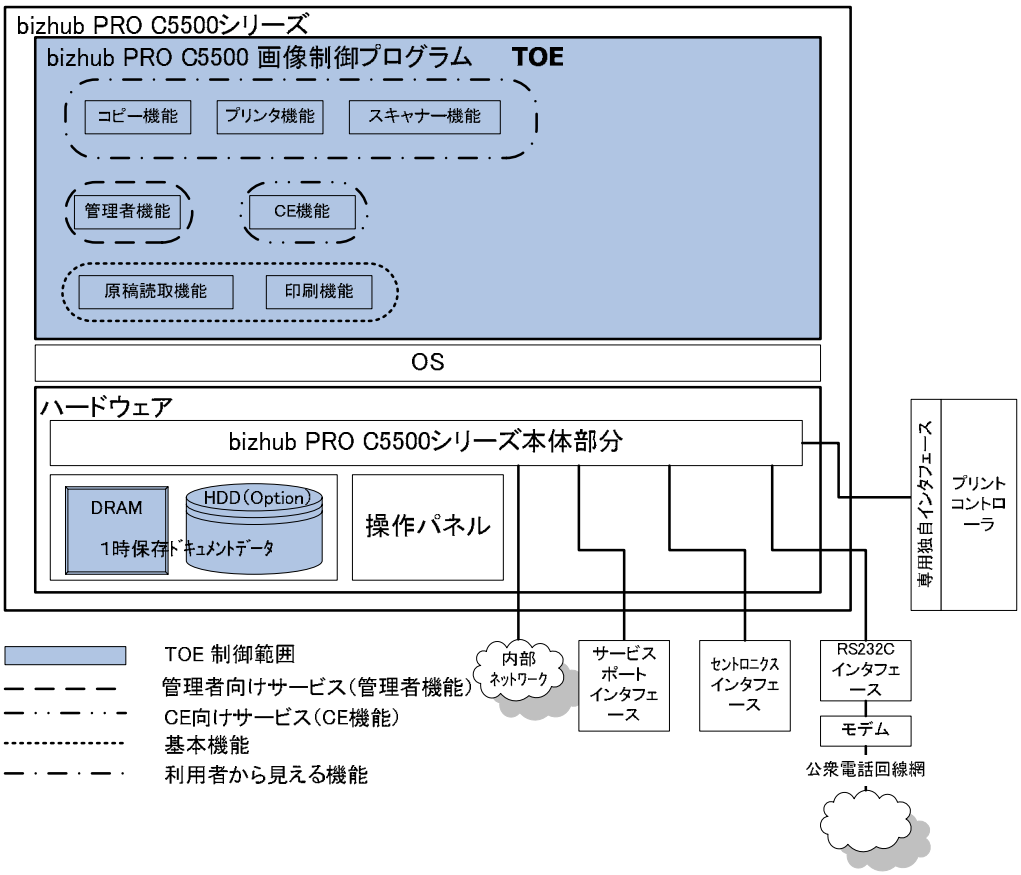

図1-2　bizhub PRO C5500シリーズの構成

bizhub PRO C5500シリーズは、ハードウェア、OS、bizhub PRO C5500 画像制御プログラムから構成される。ハードウェアは、bizhub PRO C5500シリーズ本体部分、DRAM/HDD部分、操作パネル及びネットワークカード、各種インタフェースである。なお、HDDは、オプションユニットであり標準では搭載されていない。DRAM/HDD部分は、ドキュメントの一時的な格納を行う。DRAMに関して、外部からDRAMへのアクセスは行えず、電源Offと共にDRAM内の一時保存データは消える。bizhub PRO C5500 画像制御プログラムは、OS上で動作する。

本TOEの制御範囲であるTOEに含まれる各機能と本TOEが管理するドキュメントデータの格納領域を図1-2の網掛けで示す。

1.2.4 TOEの機能

本TOEは、ドキュメントデータのコピー、プリント、スキャンを行う「基本機能」、管理者がTOEの設定を行う「管理機能」及び、CE(*3)がTOEの初期設定（管理者の

登録やTOEのインストール）を行う「CE機能」から構成される。

（*3）Customer Engineer：bizhub PRO C5500シリーズの保守を委託されている企業に在籍し、bizhub PRO C5500シリーズの保守をする者。

1.2.4.1 TOE の基本機能

本TOEの基本機能は、原稿読取機能、印刷機能である。これらの組合せにより、利用者へコピー機能、プリンタ機能、スキャナー機能を提供する。

コピー機能時は、紙文書を読み取ったドキュメントデータ（電子データ）は、一旦DRAM及びHDDの一時保存領域に格納した後、一時保存領域から読み出し印刷される。プリンタ機能時は、クライアントPCからのドキュメントデータは外部のプリントコントローラにてデータ変換された後に、bizhub PRO C5500シリーズへと入力され、一旦DRAM及びHDDの一時保存領域に格納した後、一時保存領域から読み出し印刷される。なお、一時保存DRAMに一時格納されたデータは、電源のOFFと共に消える。スキャナー機能時は、入力された紙文書を読み取った電子データは一時保存をせずに外部のプリントコントローラへと送信される。基本機能の処理概念を図1-3に示す。

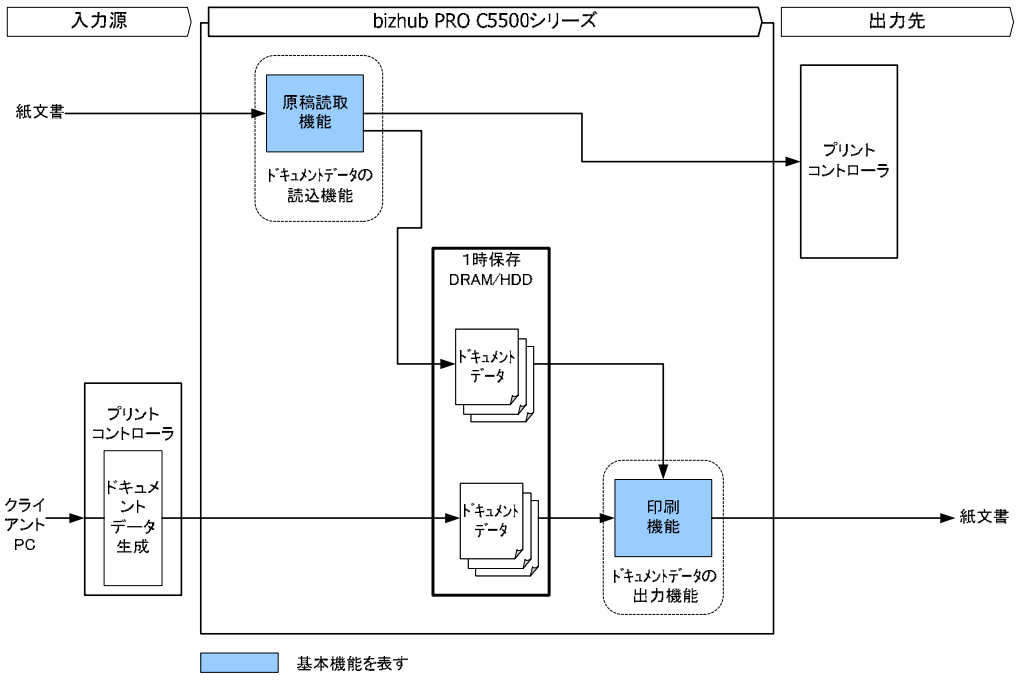

図1-3　基本機能の処理概念

利用者に提供する機能と基本機能の関係は以下のとおりである。

No	利用者機能	基本機能
1	コピー機能	原稿読取機能と印刷機能
2	プリンタ機能	印刷機能
3	スキャナー機能	原稿読取機能

各基本機能の詳細を以下に示す。

⑴原稿読取機能

一般利用者により操作パネルから指示された、紙文書の情報を読取り、電子データに変換する。コピー機能時は、その電子データを一時保存領域に格納する。また、スキャナー機能時は、その電子データをそのまま外部プリントコントローラに送信する機能。

⑵印刷機能

一時保存DRAMまたは、一時保存HDDに一時格納されたドキュメントデータを印刷する機能。

1.2.4.2 管理機能

管理者は、管理機能を使用して、管理者パスワードの変更、セキュリティ強化モードの設定（*4)、TOEのネットワーク情報の設定、TOEが有する機能の動作設定を行う。また、管理機能は、監査情報の印刷、プリンタ枚数の管理、トラブルシューティング及びトナーの管理など、デジタル複合機の運用に関わる情報を管理する。

（*4）セキュリティ強化モードを有効に設定することによりTOE提供機能をよりセキュアな状態とする。セキュリティ強化モード有効状態において、HDDにはHDDロックパスワードが設定され、読み書きのできないロック状態となる。bizhub PRO C5500シリーズが電源ONした時点で、TOEはHDDロックパスワードを使用して認証及びロック解除の指示を行う。HDDでは、正当なTOEであることの確認を行いHDDのロック状態を解除して、HDDの読み書きを可能とする。

1.2.4.3 CE 機能

CEが本TOEの初期設定及び保守を行うため、以下の機能が用意されている。

・サービス設定モード

操作パネルから操作し、管理者のパスワード登録と変更を実施する。

・CSRC（CS Remote Care）
公衆回線網に接続したコンピュータから、またはインターネットに接続したコンピュータから操作し、ハードウェア保守のため印刷枚数、ジャム回数、トナー切れなどに関する情報の取得を行う。

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「Multi functional printer (digital copier) bizhub PRO C5500/ineo$^+$ 5500 Series セキュリティターゲット第2版」（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、「Multi functional printer (digital copier) bizhub PRO C5500/ineo$^+$ 5500 Series　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、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。評価は、平成19年9月の評価機関による評価報告書の提出をもって完了し、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、攻撃者の攻撃能力について、低レベルであることを想定している。また、物理的な面と人的な面で十分なセキュリティを確保した条件下で運用されることを想定している。このため、セキュリティ強度は、低レベルの攻撃能力を有する脅威エージェントからの攻撃に対して、十分に対抗できるSOF-基本が妥当である。

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。

⑴識別認証

機能名称	セキュリティ機能の仕様
IA.ADM_ADD 管理者の登録	IA.ADM_ADDは、管理者をTOEに登録する。CEのみがIA.ADM_ADDを操作する。CEは、管理者のパスワードを登録する。 IA.ADM_ADDは、管理者登録のインタフェースを提供する。管理者登録のインタフェースは、登録する管理者に対応するパスワードの入力を要求する。 管理者が入力するパスワードに対して、以下の規則に従い、許容値を検証する。 ・パスワードは８文字とする。 ・パスワードは半角英大文字、半角英小文字、半角数字で構成する。 ・パスワードは一世代前のパスワードと同一の値を禁止する。 許容値の検証において、規則に従っている場合、管理者を登録する。規則に従っていない場合、登録を拒否する。
IA.ADM_AUTH	IA.ADM_AUTHは、操作者がTOEを利用する前に、TOE

管理者の識別と認証	に登録した管理者であることを識別し、操作者が管理者本人であることを認証する。 IA.ADM_AUTHは、管理者の識別と認証の前に管理機能の一切の操作を許可しない。管理者の識別と認証のインタフェースは、IA.ADM_ADDで登録、IA.PASSで変更したパスワードの入力を要求する。IA.ADM_AUTHは、管理者の識別と認証のインタフェースの表示により管理者であることを識別し、入力するパスワードを用いて管理者本人であることを認証する。管理者がパスワードを入力する際は、入力したパスワードの代わりにダミー文字(*)を表示する。 認証不成功時には、5秒後に管理者の識別と認証のインタフェースを提供する。
IA.CE_AUTH CEの識別と認証	IA.CE_AUTHは、操作者がTOEを利用する前に、TOEに登録しているCEであることを識別し、操作者がCE本人であることを認証する。 IA.CE_AUTHは、CEの識別と認証の前にCE機能の一切の操作を許可しない。IA.PASSで変更したパスワードの入力を要求する。IA.CE_AUTHはCEの識別と認証のインタフェースの表示によりCEであることを識別し、入力するパスワードを用いてCE本人であることを認証する。CEがパスワードを入力する際は、入力したパスワードの代わりにダミー文字(*)を表示する。 認証不成功時には、5秒後にCEの識別と認証のインタフェースを提供する。
IA.PASS パスワードの変更	IA.PASSは、管理者、及びCEの認証情報である管理者のパスワード、及びCEのパスワードを変更する。 IA.PASSは、パスワード変更のインタフェースを提供し、新しいパスワードの入力を要求する。 利用者により以下のパスワードの変更が可能である。 CE　　：CEのパスワード、管理者のパスワード 管理者　　：管理者のパスワード 製品関係者が入力するパスワードに対して、以下の規則に従い許容値を検証する。

	・CE 及び管理者パスワードは 8 文字とする。 ・パスワードは半角英大文字、半角英小文字、半角数字で構成する。 ・パスワードは一世代前のパスワードと同一の値を禁止する。 許容値の検証において、規則に従っている場合、パスワードを変更する。

⑵管理支援

機能名称	セキュリティ機能の仕様
MNG.MODE セキュリティ強化モードの設定	MNG.MODEは、管理者にのみセキュリティ強化モードを有効化する機能及びそれを停止にする機能を許可し実行する。
MNG.HDD HDD ロックパスワード機能	MNG.HDDは、管理者にのみ以下の処理を許可し実行する。 ・ＨＤＤロックパスワードの変更 管理者が入力するHDDロックパスワードに対して以下の規則に従い、許容値を検証する。 ・パスワードは 8 文字から 32 文字とする。 ・パスワードは半角英大文字、半角英小文字、半角数字で構成する。 許容値の検証において、規則に従っている場合、HDD装置にHDDロックパスワードを設定／変更する。規則に従っていない場合、変更を拒否する。

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.HDDACCESS（HDDへの不正なアクセス）	・一般利用者がセキュリティ強化モードに関する設定を変更し、HDDに不正な装置を接続してドキュメントデータが読み出される。

1.5.6　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はない。

1.5.7　構成条件

本TOEは、bizhub PRO C5500シリーズに搭載されるソフトウェア製品である。

本TOEは、bizhub PRO C5500シリーズ出荷時にセキュリティ機能付製品としてインストールして出荷する形態をとる。

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1-2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1-2　TOE使用の前提条件

識別子	前提条件
ASM.SECMOD（セキュリティ強化モードの動作設定条件）	・管理者はセキュリティ強化モードを有効化する。 ・bizhub PRO C5500シリーズにはオプションのHDDが装着されている。
ASM.NET（内部ネットワークの設置条件）	・TOEが搭載されたbizhub PRO C5500シリーズを設置する内部ネットワーク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bizhub PRO C5500シリーズへアクセスできない。
ASM.ADMIN（信頼できる管理者）	・管理者は、不正な行為を行わない人物である。
ASM.CE（CEの条件）	・CEは、不正な行為を行わない人物である。
ASM.SECRET（秘密情報に関する運用条	・TOEの利用において管理者パスワード及びHDDロックパスワードは、管理者から漏洩しない。

件）	・CEパスワードはCEから漏洩しない。

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。

●国内向け

＜CE向けマニュアル＞

・bizhub PRO C5500　インストールマニュアル　A0E7956000

・bizhub PRO C6500/C6500P/C5500　サービスマニュアル　フィールドサービス　CCA0E7-M-FJ2-0000

＜管理者向けマニュアル＞

・bizhub PRO C5500　ユーザーズガイド　コピー編　A0E7955000

・bizhub PRO C5500　ユーザーズガイド　POD管理者編　A0E7957000

・bizhub PRO C5500　ユーザーズガイド　セキュリティ編　A0E7955500

●海外向け

＜CE向けマニュアル＞

・bizhub PRO C5500 INSTALLATION MANUAL　A0E7956200

・bizhub PRO C6500/C6500P/C5500 SERVICE MANUAL Field Service CCA0E7-M-FE2-0000

・COLOR MFP 55ppm INSTALLATION MANUAL　A0E7956300

＜管理者向けマニュアル＞

・bizhub PRO C5500 User's Guide Copier　A0E7955100

・bizhub PRO C5500 User's Guide POD Administrator's Reference A0E7957100

・bizhub PRO C5500 User's Guide Security　A0E7955600

・ineo+ 5500 User's Guide ［Copier］　A0E7959500

・ineo+ 5500 User's Guide ［POD Administrator's Reference］　A0E7959700

・ineo+ 5500 User's Guide ［Security］　A0E7959600

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7月に始まり、平成19年9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8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8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。

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。

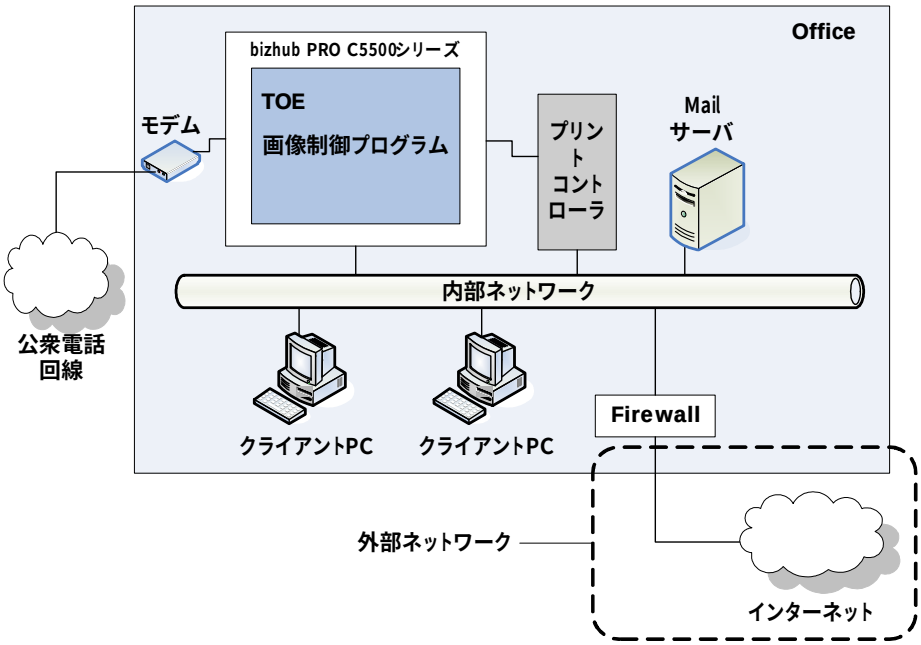

図2-1　開発者テストの構成図

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利用環境と同一のTOEテスト環境で実施されている。

・テスト機構成

bizhub PRO C5500 / ineo^{+} 5500
一部のテストで必要になるため合計で 2 台以上準備

・テスト環境構成

ネットワーク接続方法：イーサネット（10Base-T）環境に接続
クライアントPC：WindowsXP（日本語版/英語版）
使用アプリケーション：Internet Explorer（Ver.6）
Mailサーバ：内部ネットワーク（コニカミノルタ東京事業所内）に接続
プリントコントローラ：IC-408（内蔵タイプコントローラ）
（プリントコントローラは、今回のテスト内容に関与しないので
なくても可）

b.テスト手法

テストには、以下の手法が使用された。
①TSFIの操作によりセキュリティ機能の動作を確認する。
②TSFI、サブシステムインタフェースを、直接bizhub PRO C5500シリー

ズの外部インタフェース経由の操作でテストできない場合は、間接的にそのインタフェースを刺激する手法でテストを行う。

③テストのふるまいの観測について、外部TSFIにて確認できるものは、直接確認し、テスト結果のふるまいを観測できないものについては、測定用の機器を使用して、テスト結果を確認する。

④テストを実行したときの実際のテスト結果と、期待されるふるまいを比較して、テストの目標が達成されたか否かを決定する。

c.実施テストの範囲

テストは開発者によって22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を図2-2に示す。

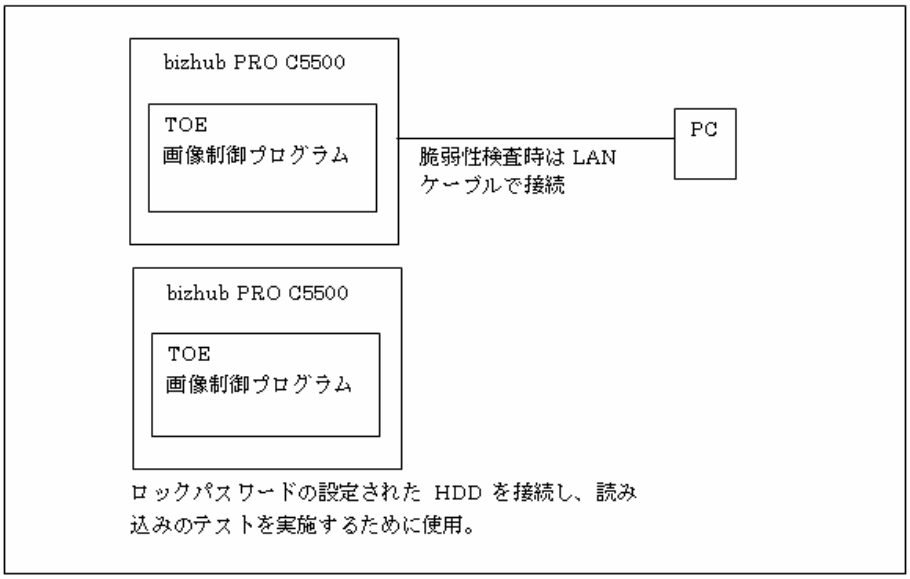

図2-2　評価者テストの構成図

評価者テストにおけるテスト環境の構成は、STにおいて識別されている利用環境と異なるが、同等であると判断した理由は以下のとおり。

TOEのセキュリティ強化モードが有効になっている状態では、内部ネットワークからTOEへアクセスできる機能は存在しない。したがって、ネットワークへの接続の有無はテストに影響を与えないため、ネットワーク接続を省略した評価者テストにおけるテスト環境は、STにおいて識別されている利用環境と同等であると判断できる。

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2-2に示す。評価者テストは、bizhub PRO C5500　インストールマニュアルに従って設定したTOEに対して実施されている。

b.テスト手法

テストには、以下の手法が使用された。

①TSFIの操作によりセキュリティ機能の動作を確認する。

②TSFI､サブシステムインタフェースを､直接bizhub PRO C5500シリーズの外部インタフェース経由の操作でテストできない場合は、間接的にそのインタフェースを刺激する手法でテストを行う。

③テストのふるまいの観測について、外部TSFIにて確認できるものは、直接確認し、テスト結果のふるまいを観測できないものについては、測定用の機器を使用して、テスト結果を確認する。

④テストを実行したときの実際のテスト結果と、期待されるふるまいを比較して、テストの目標が達成されたか否かを決定する。

c.実施テストの範囲

評価者が独自に考案したテストを5項目、開発者テストのサンプリングによるテストを8項目、評価者による侵入テストを7項目計20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。

＜独自に考案したテスト項目＞

①セキュリティパラメタを入力するセキュリティ機能

②ガイダンス及び機能仕様の検査により発見されたWebインタフェースから利用される機能

③HDDのロックパスワードの有効性に関するセキュリティ機能

＜開発者テストのサンプリングによるテスト項目＞

①開発者テストの総項目数に占める割合が20%を超す

②特定のセキュリティ機能に偏ることなくすべてのセキュリティ機能を網羅する
③セキュリティ強化モードをONにするために事前に動作させる必要がある機能を網羅する

＜侵入テストによるテスト項目＞
①セキュリティ強化モードで無効化されているべき機能
②セキュリティ強化モードの無効化の手段
③セキュリティ強化モードのON/OFFによる、セキュアでない状態の発生
④本体操作部のリセットボタン押下による、セキュアでない状態の発生
⑤ネットワークからの侵入によるセキュアでない状態の発生
⑥セキュリティ強化モードONのMFPに、ロックパスワードが設定されていないHDDを装着することによる、セキュアでない状態での起動

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 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。
② 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。
③ 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。

4 結論

4.1 認証結果

提出された評価報告書、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種別、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概説が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.1.1E	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.1.2D	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環境がないこと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
CE	Customer Engineer
CEM	Common Methodology for Information Technology Security Evaluation
CSRC	CS Remote Care
DRAM	Dynamic Random Access Memory
EAL	Evaluation Assurance Level
HDD	Hard Disk Drive
OS	Operating System
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用語を以下に示す。

RS232Cインタフェース	モデムを介して公衆回線網と接続するためのインタフェースのこと。
一時保存	入力されたドキュメントデータは紙文書に印刷されるまでの間に、DRAM/HDDに一時的に保存される。
外部ネットワーク	外部ネットワークは、内部ネットワーク以外のネットワーク(例えばインターネットなど)である。
紙文書	紙文書は、文字や図形などの情報を持つ紙媒体の文書である。
管理者	管理者は、bizhub PRO C5500シリーズを導入する組織に在籍し、bizhub PRO C5500シリーズの運用管理を行う。TOEが提供する運用管理の機能を利用する。
サービスポートインタフェース	TOEの設置生成を行う際に保守用のコンピュータと接続するためのインタフェースのこと。
セントロニクスインタフェース	TOEの設置生成を行う際に保守用のコンピュータと接続するためのインタフェースのこと。
操作パネル	操作パネルは、bizhub PRO C5500シリーズの筐体に付属するタッチパネル式ディスプレイ及び操作ボタンの名称である。

ドキュメントデータ	ドキュメントデータは、文字や図形などの情報を電子化したデータである。
内部ネットワーク	内部ネットワークは、bizhub PRO C5500シリーズを導入する組織のLANである。クライアントPCや各種サーバ(例えばMailサーバやFTPサーバなど)が接続されている。
ハードディスクロック機能	ハードディスクを取外し他の機器で読み込みができないように、ハードディスクにパスワードを持たせる機能のこと。
HDDロックパスワード	ハードディスクロック機能で設定するパスワードのこと。

6 参照

[1] Multi functional printer (digital copier) bizhub PRO C5500/ineo+ 5500 Series セキュリティターゲット 第２版（2007年8月10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] Multi functional printer (digital copier) bizhub PRO C5500/ineo+ 5500 Series 評価報告書 初版　2007年9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