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

申請受付年月日(受付番号)	**平成18年8月30日(IT認証6097)**
認証番号	C0070
認証申請者	**パナソニック コミュニケーションズ株式会社**
TOEの名称	**日本　：データセキュリティーキット**　DA-SC02 **海外　：**Data Security Kit　DA-SC02
TOEのバージョン	V1.00
PP適合	**なし**
適合する保証要件	EAL2
TOE開発者	**パナソニック コミュニケーションズ株式会社**
評価機関の名称	**社団法人 電子情報技術産業協会 ITセキュリティセンター**

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18年12月15日

独立行政法人 情報処理推進機構
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

「データセキュリティーキット　DA-SC02」は、独立行政法人 情報処理推進機構が定める ITセキュリティ認証手続規程に従い、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
1.1 はじめに 1
1.2 評価製品 1
1.2.1 製品名称 1
1.2.2 製品概要 1
1.2.3 TOEの範囲と動作概要 2
1.2.4 TOEの機能 4
1.3 評価の実施 6
1.4 評価の認証 6
1.5 報告概要 7
1.5.1 PP適合 7
1.5.2 EAL 7
1.5.3 セキュリティ機能強度 7
1.5.4 セキュリティ機能 7
1.5.5 脅威 8
1.5.6 組織のセキュリティ方針 8
1.5.7 構成条件 8
1.5.8 操作環境の前提条件 8
1.5.9 製品添付ドキュメント 9
2 評価機関による評価実施及び結果 11
2.1 評価方法 11
2.2 評価実施概要 11
2.3 製品テスト 11
2.3.1 開発者テスト 11
2.3.2 評価者テスト 13
2.4 評価結果 14
3 認証実施 14
4 結論 15
4.1 認証結果 15
4.2 注意事項 19
5 用語 20
6 参照 23

1 全体要約

1.1 はじめに

この認証報告書は、「データセキュリティーキット　DA-SC02」（以下「本TOE」という。）について社団法人 電子情報技術産業協会 ITセキュリティセンター（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パナソニック コミュニケーション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　：データセキュリティーキット　DA-SC02
　　海外　：Data Security Kit DA-SC02

バージョン:　V1.00

開発者:　パナソニック コミュニケーションズ株式会社

1.2.2 製品概要

TOEは、フルカラーデジタル複合機に搭載されるデータセキュリティーキットDA-SC02であり、デジタル複合機の処理後のハードディスク装置内に蓄積された利用済み文書データを不正な暴露から保護するためのソフトウェア製品である。

TOEはパナソニック コミュニケーションズ株式会社製フルカラーデジタル複合機DP-C2635 / C2626 / C2121（日本国内対応機種、海外対応機種はDP-C354 / C264 / C323 / C263 / C213）

のオプション製品として提供され、デジタル複合機の標準ソフトウェアと置き換えることにより、セキュリティー機能を提供する。

1.2.3 TOEの範囲と動作概要

TOEは、フルカラーデジタル複合機に搭載されるデータセキュリティーキットDA-SC02であり、フルカラーデジタル複合機の処理後のハードディスク装置内に蓄積された利用済み文書データを不正な暴露から保護するためのソフトウェア製品である。TOEは図1-1のような環境下で使用される。

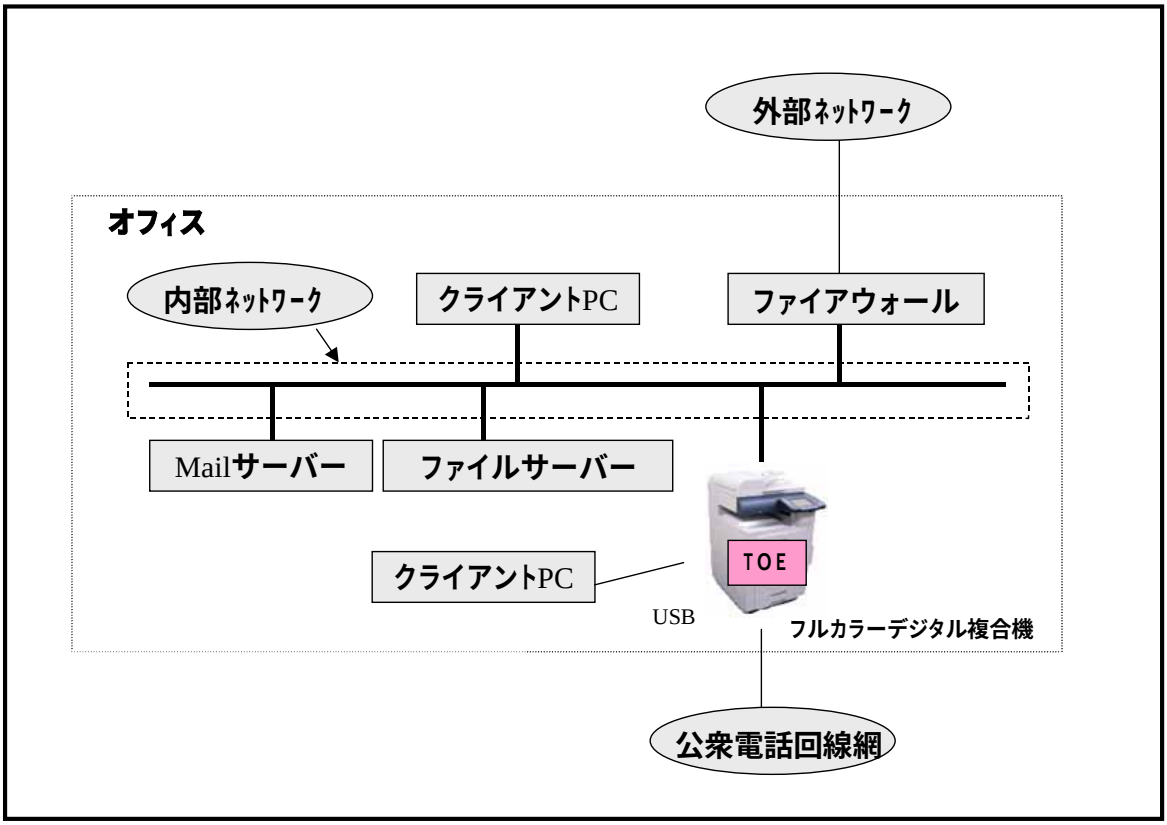

図1-1　想定される利用環境

次にTOEを搭載したフルカラーデジタル複合機の物理的構成を図1-2に示す。

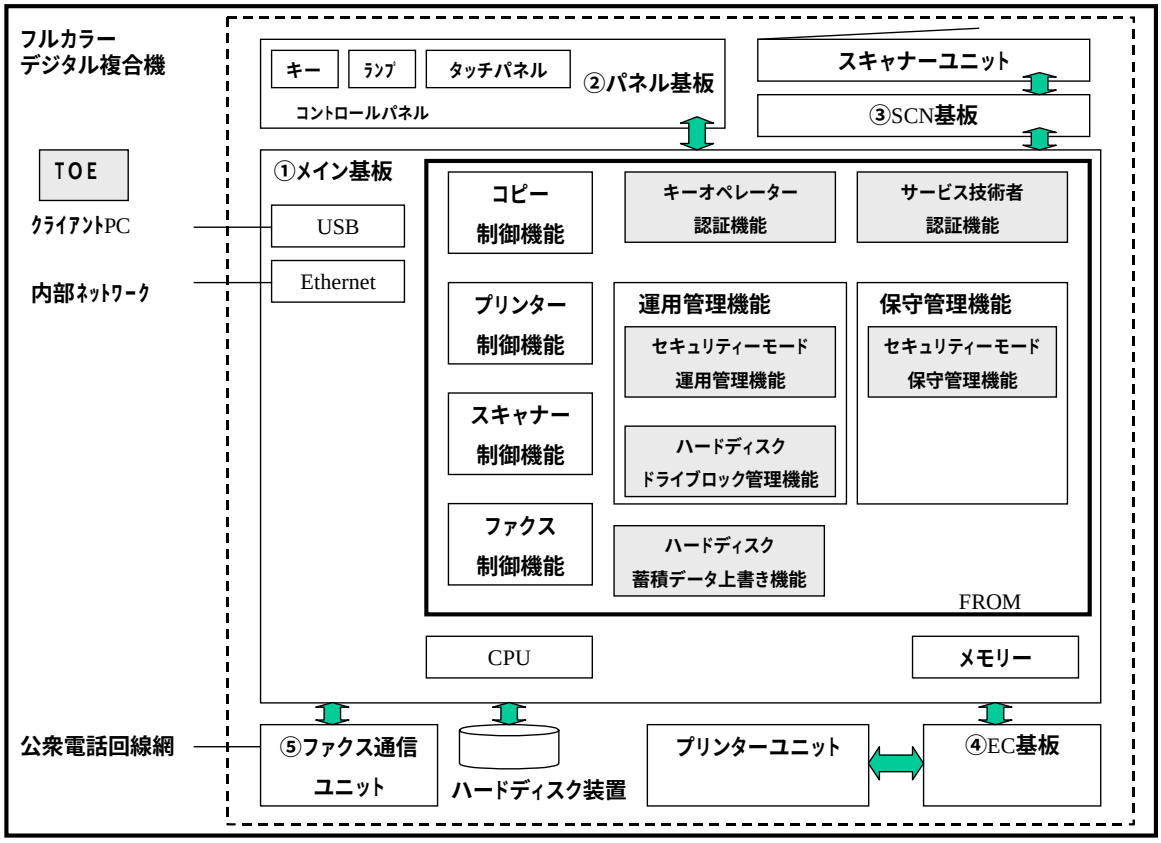

図1-2　物理構成図

フルカラーデジタル複合機DP-C2635 / C2626 / C2121（日本国内対応機種、海外対応機種はDP-C354 / C264 / C323 / C263 / C213）は、

① 複合機システム全体の制御を行うメイン基板
② 複合機の操作に必要なキー、ランプ、タッチパネルディスプレイが配置されたコントロールパネルの制御を行うパネル基板
③ スキャナーユニットのメカ制御を行うＳＣＮ基板
④ プリンターユニットのメカ制御を行うＥＣ基板
⑤ ファクス通信ユニット

の5つの基板から構成される。

①メイン基板と②パネル基板は、制御データの通信を行うために内部インターフェースで接続されている。

①メイン基板と③ＳＣＮ基板、④ＥＣ基板は、制御データや文書データの通信を行うために内部インターフェースで接続されている。

③ＳＣＮ基板はスキャナーユニットと制御データの通信をおこないスキャナーのメカ制御を行う。スキャナーから読み込まれた文書データは直接①メイン基板に送信される。また、④ＥＣ基板はプリンターユニットと制御データ・文書データの通信をおこない、プリンターのメカ制御を実行しながら文書データの印刷を行う。

①メイン基板と⑤ファクス通信ユニットは、内部インターフェースで接続され、⑤ファクス通信ユニットはファクスデータの送受信を行うため、公衆電話回線網に接続されている。

さらに、①メイン基板は、クライアントPC、Mailサーバーやファイルサーバーと接続するために、EthernetやUSBインターフェースを有している。また、文書データを蓄積するためのハードディスク装置も①メイン基板に接続される。
①メイン基板はＣＰＵ、ソフトウェアを格納するＦＲＯＭ、データを格納するメモリー、その他複合機システム全体の制御を行うための電気回路で構成される。

TOEはメイン基板に実装されているFROMに記録されている図1-2で網掛けされた部分

・キーオペレーター認証機能
・サービス技術者認証機能
・セキュリティーモード運用管理機能
・セキュリティーモード保守管理機能
・ハードディスクドライブロック管理機能
・ハードディスク蓄積データ上書き機能

のソフトウェアであり、コピー／プリンター／スキャナー機能の処理後のハードディスク装置内に蓄積された利用済み文書データを不正な暴露から保護するものである。

1.2.4 TOEの機能

TOEが持つ機能を以下に示す。

（１）ハードディスク蓄積データ上書き機能
コピー制御機能／プリンター制御機能／スキャナー制御機能の各動作処理後、ハードディスク装置内に蓄積された利用済み文書データをその利用が終了した時点で自動的に文書データのデータ領域も上書き消去する機能である。上書き消去の方法として、下記の３種類がある。

- 標準：文書データの管理情報のみを削除する
- レベル１：文書データのデータ領域にすべて０のデータを3回上書き消去する
- レベル２：文書データのデータ領域にランダムな値を2回、その後すべて０のデータを1回上書き消去する

後記のセキュリティーモード運用管理機能の「ハードディスクデータ消去レベル」でこの上書き消去の方法を設定する。標準は文書データの管理情報のみを削除する事が初期設定値なので、キーオペレーターはレベル１またはレベル２に設定してフルカラーデジタル複合機 DP-C2635 / C2626 / C2121（日本国内対応機種、海外対応機種は DP-C354 / C264 / C323 / C263 / C213）を運用する。また、（４）セキュリティーモード運用管理機能の「ハードディスク初期化」機能によりキーオペレーターのみが、廃棄時等ハードディスク装置内に蓄積された文書データをレベル１、レベル２の２種類の方法で上書き消去できる。

（２）キーオペレーター認証機能
コントロールパネルへの指示、入力されたキーオペレーター専用のパスワード（以下、キーオペレーターパスワードと記述する）により、キーオペレーターの識別と認証を行う機能である。　キーオペレーターのみ、（３）ハードディスクド

ライブロック管理機能、(４)セキュリティーモード運用管理機能の操作ができる。

（３）ハードディスクドライブロック管理機能

ハードディスク装置として、ハードディスク装置そのものに直接パスワードを設定することにより、そのパスワードを入力しない場合ハードディスク装置が認識できなくなるドライブロック機能付きのハードディスク装置を採用している。キーオペレーターのみ、「ハードディスクドライブロックパスワード」のフルカラーデジタル複合機内のメモリーおよびハードディスク装置に対するパスワードの設定・変更とパスワードを未設定状態にするドライブロックの解除を行うことができる。フルカラーデジタル複合機は起動時、複合機内のメモリーに格納されているパスワードをハードディスク装置に対して送信し、ハードディスク装置へのデータアクセスの許可を依頼する。

（４）セキュリティーモード運用管理機能

キーオペレーターのみ、以下のセキュリティーに関する設定データの設定・変更および処理の指示ができる。

・「ハードディスクデータ消去レベル」

コピー制御機能／プリンター制御機能／スキャナー制御機能の各動作処理後の利用済み文書データ発生時点で自動的に実行するハードディスク蓄積データ上書き機能の消去方法を設定する。標準（初期設定値）、レベル１、レベル２の３種類の上書き消去の方法が設定できる。

・「ハードディスク初期化」

キーオペレーターの指示により、ハードディスク装置内に蓄積された文書データすべてを上書き消去する機能である。上書き消去の方法として、レベル１、レベル２の２種類有する。

・「全ボックスファイル削除」

キーオペレーターの指示により、ハードディスク装置内のイメージボックスに蓄積された文書データをすべて「ハードディスクデータ消去レベル」で設定された上書き消去の方法で上書き消去する機能である。

・「キーオペレーターパスワード」

キーオペレーターパスワードを設定・変更する機能である。

（５）サービス技術者認証機能

コントロールパネルからのサービスモード設定手順の操作、入力されたサービス技術者パスワードにより、サービス技術者の識別と認証を行う機能である。サービス技術者のみ、（６）セキュリティーモード保守管理機能の操作ができる。

（６）セキュリティーモード保守管理機能

サービス技術者のみ、以下のセキュリティーに関する設定データの設定・変更および初期化（初期設定値に戻す操作）の指示ができる。

・「サービス技術者パスワード」

サービス技術者パスワードを設定・変更する機能である。

・「システム初期化」

サービス技術者の指示により、(３) ハードディスクドライブロック管理機能で記述した「ハードディスクドライブロックパスワード」、(４) セキュリティーモード運用管理機能で記述した「ハードディスクデータ消去レベル」および「キーオペレーターパスワード」、(６) セキュリティーモード保守管理機能で記述した「サービス技術者パスワード」の設定データを初期化（初期設定値に戻す操作）する機能である。

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セキュリティ認証手続規程」[3]、「評価機関承認手続規程」[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「データセキュリティーキット DA-SC02 セキュリティーターゲット」（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C、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、「データセキュリティーキット DA-SC02 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については、認証レビューを作成した。評価は、平成18年12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、EAL2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、攻撃能力が低レベルを想定した製品であり、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。

- ハードディスク蓄積データ上書き機能（SF.OVWRT）
  この機能は、ハードディスク装置内に蓄積された利用済み文書データのデータ領域を上書き消去する機能である。
- キーオペレーター認証機能（SF.ADM_IA）
  この機能は、ハードディスクドライブロック管理機能(SF.HDMNG)およびセキュリティーモード運用管理機能(SF.ADMMNG)で提供される「ハードディスクドライブロックパスワード」、「キーオペレーターパスワード」、「ハードディスクデータ消去レベル」の設定データの操作および「ハードディスク初期化」、「全ボックスファイル削除」の指示を認証されたキーオペレーターのみが行えるように制御する。
  操作や指示を許可する前に、コントロールパネルから入力されたキーオペレーターのパスワードにより、操作者がキーオペレーターであることを識別・認証する。
- ハードディスクドライブロック管理機能（SF.HDMNG）
  この機能は、キーオペレーターがハードディスクドライブロックの管理を行うための機能であり、SF.ADM_IA によりキーオペレーターと識別・認証された時のみ「ハードディスクドライブロックパスワード」の設定・変更およびドライブロックの解除ができるよう許可し、実行する。
- セキュリティーモード運用管理機能（SF.ADMMNG）
  この機能は、キーオペレーターが運用を行うための管理機能であり、SF.ADM_IA によりキーオペレーターと識別・認証された時のみ、「キーオペレーターパスワード」の設定・変更、「ハードディスクデータ消去レベル」の設定・変更、「ハードディスク初期化」、「全ボックスファイル削除」の指示をできるよう許可し、実行する。
- サービス技術者認証機能（SF.SE_IA）
  この機能は、セキュリティーモード保守管理機能(SF.SEMNG)で提供される「サー

ビス技術者パスワード」の設定データの操作および「システム初期化」の指示を認証されたサービス技術者のみが行えるように制御する。
　操作や指示を許可する前に、コントロールパネルから入力されたサービスモード設定手順、サービス技術者のパスワードにより、操作者がサービス技術者であることを識別・認証する。

- セキュリティーモード保守管理機能（SF.SEMNG）
この機能は、サービス技術者が保守作業を行うための管理機能であり、SF.SE_IAによりサービス技術者と識別・認証された時のみ、「サービス技術者パスワード」の設定・変更、「システム初期化」の指示をできるよう許可し、実行する。

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.RECOVER	・利用済み文書データの不正再生 悪意をもった一般利用者や**TOE**の非関連者がハードディスク装置に、**PC**やツール等直接接続して利用済み文書データを再生するかもしれない。

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.OWMETHOD	・　上書き消去の設定 ハードディスク装置内に蓄積された利用済み文書データを上書き消去する。

1.5.7 構成条件

本セキュリティーターゲットはパナソニック コミュニケーションズ株式会社製フルカラーデジタル複合機**DP-C2635 / C2626 / C2121**（日本国内対応機種、海外対応機種は**DP-C354 / C264 / C323 / C263 / C213**）に搭載されるオプション製品として提供される。

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1-3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.SETSEC	・セキュリティーモード設定 キーオペレーターは、下記の**TOE**の機能を有効にして運用する。「ハードディスクドライブロックパスワード」を設定する。
A.ADMIN	・キーオペレーターの信頼 キーオペレーターは不正な行為を行わない人物である。
A.SE	・サービス技術者の信頼 サービス技術者は不正な行為を行わない人物である。

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。

日本語マニュアル		対応する英語マニュアル
1	取扱説明書（基本編）フルカラーデジタル複合機 DP-C2635 / C2635F / C2635FS DP-C2626 / C2626F / C2121F	Operating Instructions(For Basic Operations) Digital Color Imaging Systems DP-C354 / C264 DP-C323 / C263 / C213
2	取扱説明書（セットアップ編）フルカラーデジタル複合機DP-C2635 / C2635F / C2635FS DP-C2626 / C2626F / C2121F	Operating Instructions(For Setting Up) Digital Color Imaging Systems DP-C354 / C264 DP-C323 / C263 / C213
3	取扱説明書（コピー編）フルカラーデジタル複合機 DP-C2635 / C2635F / C2635FS DP-C2626 / C2626F / C2121F	Operating Instructions(For Copier) Digital Color Imaging Systems DP-C354 / C264 DP-C323 / C263 / C213
4	取扱説明書（スキャナー/Eメール編）フルカラーデジタル複合機 DP-C2635 / C2635F / C2635FS DP-C2626 / C2626F / C2121F	Operating Instructions (For Scanner and Email) Digital Color Imaging Systems DP-C354 / C264 DP-C323 / C263 / C213
5	取扱説明書（ファンクション設定編）フルカラーデジタル複合機 DP-C2635 / C2635F / C2635FS DP-C2626 / C2626F / C2121F	Operating Instructions (For Function Parameters) Digital Color Imaging Systems DP-C354 / C264 DP-C323 / C263 / C213
6	取扱説明書 データセキュリティーキット DA-SC02	Operating Instructions Data Security Kit DA-SC02
7	サービス技術者用 設置工事手順書 データセキュリティーキット DA-SC02	Installation Instructions for Service Technicians Data Security Kit DA-SC02
8	Service Manual フルカラーデジタル複合機 DP-C2635 / C2626 / C2121 DP-C322 / C262	Service Manual Digital Color Imaging Systems DP-C354 / C264 DP-C323 / C263 / C213 DP-C322 / C262

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18年9月に始まり、平成18年12月に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18年11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18年11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。

また、評価の過程で認証機関による問題点の指摘として認証レビューが評価機関へ渡された。これらは評価機関及び開発者による検討ののち、評価に反映されている。

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及び図2-2に示す。

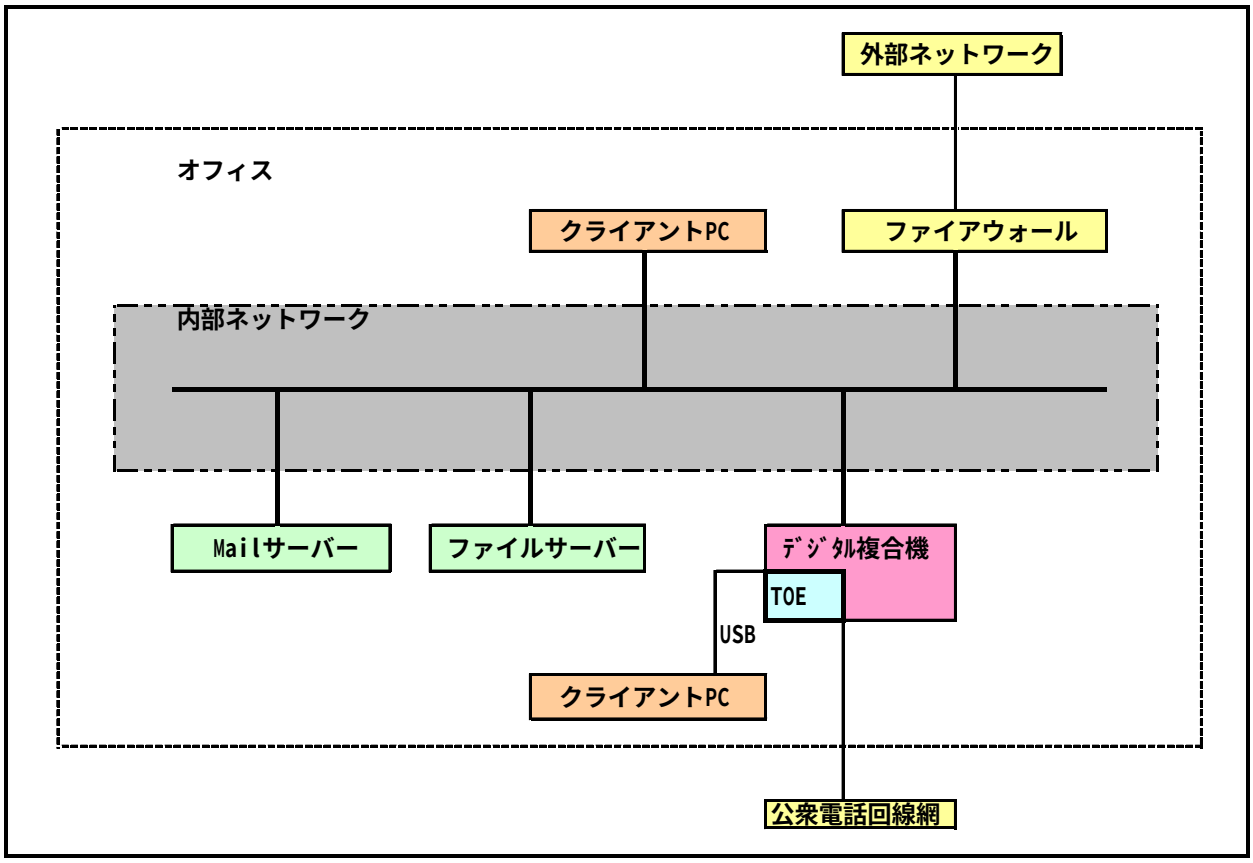

図2-1　開発者テストの構成図

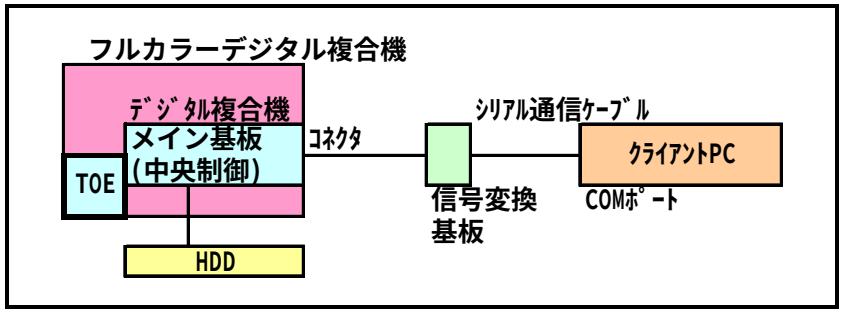

図2-2　ハードディスク蓄積データ上書きテストのテスト構成

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及び図2-2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 操作パネルからの操作＋プログラム動作状態のモニタリング
操作パネルより、TOEに対する操作を行い、その動作結果の確認を行う。

② リモートPCからの操作＋プログラム動作状態のモニタリング
TOEを搭載したフルカラーデジタル複合機に接続すべき機器（一般用クライアントPCなど）から操作を行い、その動作結果を確認する。

③ HDの上書消去機能確認のため、図2-2に示すようにフルカラーデジタル複合機をデバッグ用クライアントPCと信号変換基板を経由したシリアル通信ケーブルで接続し、その動作確認を行った。

c.実施テストの範囲

テストは開発者によって171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。

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 及び 図2-2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 フルカラーデジタル複合機の外部インタフェースであるコントロールパネルを使用してセキュリティー機能の刺激および観察

② フルカラーデジタル複合機の内部に取り付けられたHDDを取り外し、別に用意したフルカラーデジタル複合機のHDDと交換するなどのテスト

③ フルカラーデジタル複合機の開発者用内部インタフェースである、デバッグ用シリアルコネクタにデバッグ用環境を接続したテスト

c.実施テストの範囲

評価者が独自に考案したテストを36項目、開発者テストのサンプリングによるテストを62項目、計98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

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、所見報告書及び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EAL2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。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。
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、機能拡張要件が適切に定義されていることを確認している。保証要件はCCの範囲内であるため、対象外である。
ASE_SRE.1.2E	評価はワークユニットに沿って行われ、機能拡張要件の依存性が全て識別されていることを確認している。保証要件はCCの範囲内であるため、対象外である。
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.2.1E	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。
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.1.1E	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.1.2E	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。
テスト	**適切な評価が実施された**
ATE_COV.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機能仕様に正確に対応してい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_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
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用語を以下に示す。

フルカラーデジタル複合機	コピー／プリンター／スキャナー／ファクス等の機能を1台に集約した周辺機器。 本ＳＴでは、パナソニック コミュニケーションズ株式会社製の 日本国内対応機種：DP-C2635 / C2626 / C2121 海外対応機種　　：DP-C354 / C264 / C323 / C263 / C213 を総称してフルカラーデジタル複合機と記述する。
内部ネットワーク	フルカラーデジタル複合機を導入する組織のLANをいう。
外部ネットワーク	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）をいう。
リモートオペレーションパネル	フルカラーデジタル複合機のコピー／スキャナー／ファクス機能の一部の機能を、内部ネットワークに接続された一般利用者のクライアントPCから操作指示できる機能。（海外対応機種のみ）
USB	周辺機器とパソコンを結ぶデータ伝送路の規格のひとつ。

一般利用者	フルカラーデジタル複合機のコピー／プリンター／スキャナー／ファクス機能を利用する者。
キーオペレーター	フルカラーデジタル複合機の機械管理者。
サービス技術者	フルカラーデジタル複合機の設置／保守／修理を行うサービス実施会社の技術者。
サービスモード	サービス技術者がフルカラーデジタル複合機の設置／保守／修理を行う時に使用する保守管理機能。
サービスモード設定手順	サービス技術者がサービスモードへ移行するための設定手順。
初期化	保守管理機能の「システム初期化」で実行できる初期設定値に戻す操作。
コントロールパネル	フルカラーデジタル複合機の操作に必要なキー、ランプ、タッチパネルディスプレイが配置された操作パネル。
SCN	スキャナーユニットのメカ制御を行う基板。
EC	プリンターユニットのメカ制御を行う基板。
FROM	電気的な一括消去および任意部分の再書き込みを可能とした不揮発性メモリー。
文書データ	フルカラーデジタル複合機のコピー／プリンター／スキャナー／ファクス機能の利用時フルカラーデジタル複合機の内部で扱われるすべてのデジタル化された画像情報の総称。 ・スキャナーユニットから読み込まれた画像情報。 ・プリンターユニットで印字できる画像情報。 ・イメージデータを画像処理技術により変換した画像情報。 ・クライアントPCより受信した画像情報、画像情報に変換されるデータ。
利用済み文書データ	フルカラーデジタル複合機のハードディスク装置に一時蓄積され、利用が終了した文書データ。
イメージボックス機能	スキャナー機能の一つで、スキャナーユニットから読み込まれた文書データをハードディスク装置に蓄積、一般利用者のクライアントPCのWebブラウザーから閲覧・削除できる機能。

Webブラウザー	Webページを閲覧するためのPCアプリケーションソフト。インターネットからHTMLファイルや画像ファイルなどをダウンロードし、レイアウトを解析して表示・再生する。
ジョブ	フルカラーデジタル複合機のコピー／プリンター／スキャナー／ファクス機能等における一連の機能の動作単位。
ジョブ削除	フルカラーデジタル複合機のコピーやプリンター機能利用時、複数の処理（ジョブ）が指示された場合まだプリンターユニットで印字を開始していないジョブを、コントロールパネルからの指示で削除する機能。
受付音	フルカラーデジタル複合機のコントロールパネルからの入力時入力文字や操作等が正常に受付られた時に通知されるピというパネルタッチ音。

6 参照

[1] データセキュリティーキット　DA-SC02 セキュリティーターゲット バージョン 1.02（2006年11月9日）パナソニック コミュニケーションズ株式会社

[2] ITセキュリティ評価及び認証制度の基本規程　平成17年7月　独立行政法人 情報処理推進機構　EC-01

[3] ITセキュリティ認証手続規程　平成17年7月　独立行政法人 情報処理推進機構　EC-03

[4] 評価機関承認手続規程　平成17年7月　独立行政法人 情報処理推進機構　EC-05

[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] データセキュリティーキット　DA-SC02 評価報告書 第1.3版 2006年12月6日 社団法人 電子情報技術産業協会 ITセキュリティセンター