認 証 報 告 書

独立行政法人 情報処理推進機構
理事長　西垣　浩司 原紙押印済

評価対象

申請受付日（受付番号）	**平成20年2月12日** (IT**認証**8195)
認証番号	C0189
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-SC06 **海外：**Data Security Kit DA-SC06
TOE**のバージョン**	V1.01
PP**適合**	**なし**
適合する保証パッケージ	EAL2
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	**有限責任中間法人 ITセキュリティセンター 評価部**

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20年10月30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

「データセキュリティーキット DA-SC06」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、「データセキュリティーキット DA-SC06」（以下「本TOE」という。）について有限責任中間法人 ITセキュリティセンター 評価部（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-SC06 海外：Data Security Kit DA-SC06
バージョン：	V1.01
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

本TOEは、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-SC06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。

本TOEは、以下に示すパナソニック コミュニケーションズ株式会社製デジタル複合機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、セキュリティ機能を提供する。

・日本国内適用機種(※)：DP-8032P / 8025P、DP-8032V / 8025V、
DP-8032VA / 8025VA
・海外適用機種(※)： DP-8032 / 8025

(※) すべての適用機種に、別途、オプション製品であるハードディスクユニットが必要。

1.2.3 TOEの範囲と動作概要

1) TOEの利用環境

本TOEは、デジタル複合機に搭載され、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である。本TOEを搭載したデジタル複合機は図1-1に示す環境で利用されることを想定している。図1-1では、タンデムコピー／リモートコピー機能を利用するために、2台のデジタル複合機が示されている。タンデムコピー／リモートコピー機能を使用しない場合には、1台のデジタル複合機で運用可能である。

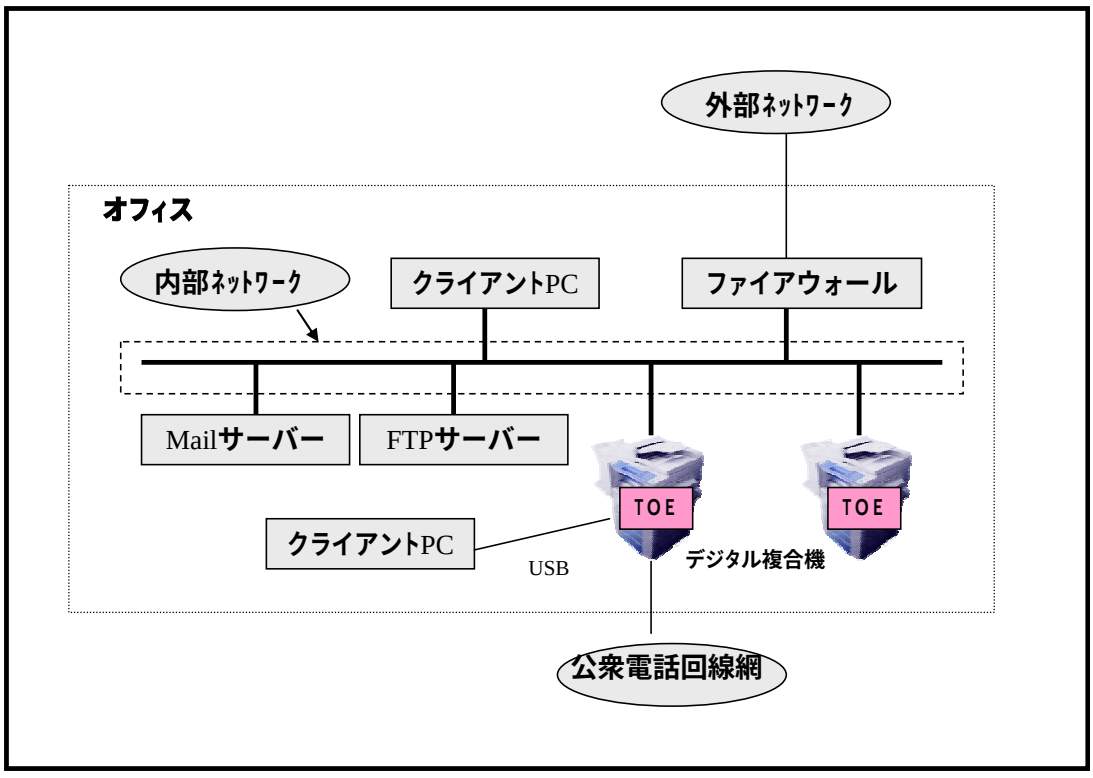

図1-1 想定する利用環境

2) TOEの範囲

本TOEを搭載したデジタル複合機の物理的構成を図1-2に示す。

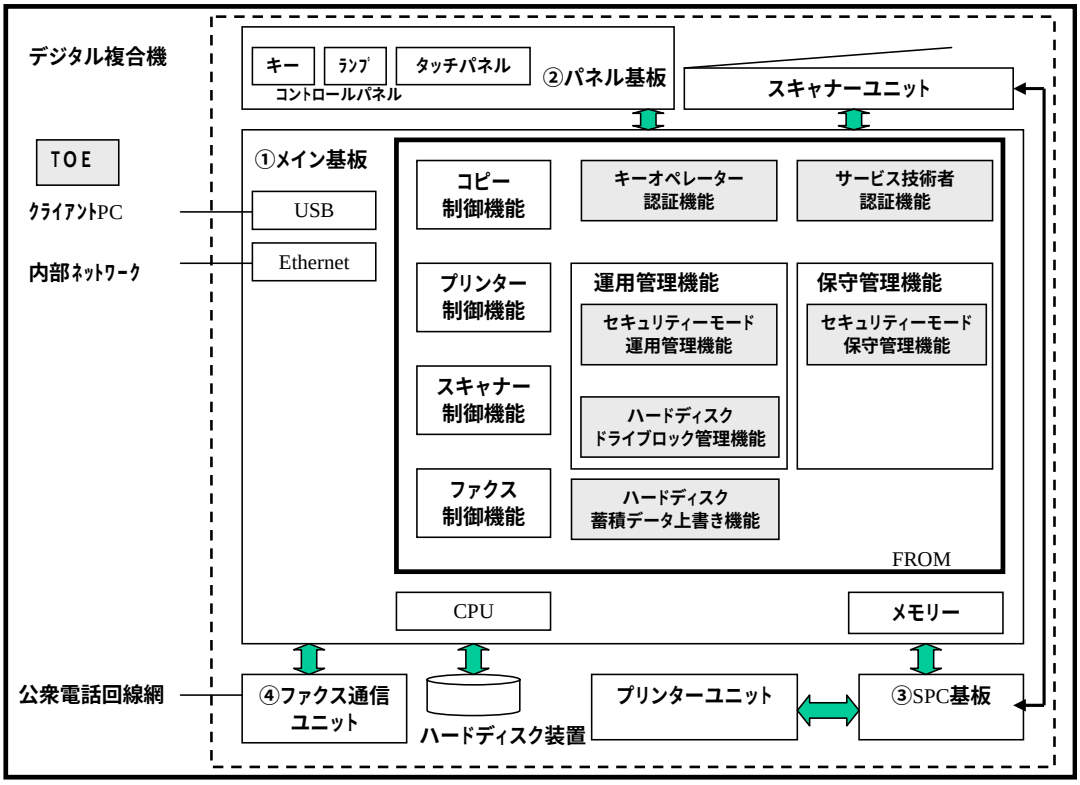

図1-2　物理的構成

図1-2で、デジタル複合機を制御するソフトウェアは、メイン基板のFROMに格納されている部分である。その中で、本TOEは以下のソフトウェア部分であり、図1-2では網掛けして示されている。

・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

なお、デジタル複合機のハードディスク装置は、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ハードディスク装置を採用している。本TOEのハードディスクドライブロック管理機能は、パスワードの管理機能を提供する。ハードディスク装置のドライブロック機能は、TOEの範囲外である。

3) TOEの関連者

本TOEを搭載したデジタル複合機の関連者は以下のとおりである。

・一般利用者

一般利用者はデジタル複合機のコピー／プリンター／スキャナー／ファクス等の一般利用機能の利用者である。

・キーオペレーター

キーオペレーターと呼ばれる機械管理者は、デジタル複合機の提供する運用管理機能を利用して、運用管理を行う。キーオペレーターはデジタル複合機の責任者から任命される。

・責任者

デジタル複合機の導入責任者で、キーオペレーターを選任し、管理・監督する。

・サービス技術者

サービス技術者は、デジタル複合機の提供する保守管理機能を利用して、設置／保守／修理等の作業を行う。サービス技術者はデジタル複合機の保守を委託されている企業に属する。

4) TOEの動作概要

本TOEは、以下のように使用される。

・一般利用者

一般利用者がデジタル複合機のコピー機能／プリンター機能／スキャナー機能を利用すると、文書データは、ハードディスク装置に一時蓄積され、各機能の利用が終了すると利用済み文書データとなる。

本TOEのハードディスク蓄積データ上書き機能は、一般利用者が意識する必要なく、利用済み文書データの発生時点で自動的に実行され、その文書データ領域を上書き消去する。

・キーオペレーター

キーオペレーターは、コントロールパネルを操作して、本TOEのキーオペレーター認証機能による識別・認証の後に、本TOEのハードディスクドライブロック管理機能とセキュリティーモード運用管理機能を使用する。

セキュリティーモード運用管理機能には、本TOEのハードディスク蓄積データ上書き機能に対して処理を指示する機能が含まれている。

・サービス技術者

サービス技術者は、コントロールパネルを操作して、本TOEのサービス技術者認証機能による識別・認証の後に、本TOEのセキュリティーモード保守管理機能を使用する。

1.2.4 TOEの機能

本TOEが提供する機能は、以下のセキュリティ機能である。

(1) ハードディスク蓄積データ上書き機能

本機能は、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。

上書き消去の方法は以下の3種類がある。上書き消去の方法はセキュリティーモード運用管理機能で設定する。

・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

本機能は、以下の時実行される。

・ 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利用済み文書データが発生した時。
・キーオペレーターがコントロールパネルより、セキュリティーモード運用管理機能「ハードディスク初期化」で指示した時。

(2) キーオペレーター認証機能

本機能は、コントロールパネルへの指示及び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・認証する機能である。識別・認証されたキーオペレーターのみが、ハードディスクドライブロック管理機能及び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

本機能は、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る。識別・認証された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」のデジタル複合機内のメモリー及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。

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

本機能は、キーオペレーターが運用を行うための管理機能である。識別・認証されたキーオペレーターのみ、以下の設定データの設定・変更及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」

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(「ハードディスク初期化」は除く)。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」

ハードディスク蓄積データ上書き機能に対して、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ように指示する機能である。上書き消去の方法として、レベル1、レベル2の2種類が選択できる。

・「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

本機能は、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及び入力されたサービス技術者パスワードにより、操作者がサービス技術者であることを識別・認証する機能である。識別・認証されたサービス技術者のみ、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

本機能は、サービス技術者が保守作業を行うための管理機能である。識別・認証されたサービス技術者のみ、以下の設定データの設定・変更及び初期化の指示ができる。

・「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、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」、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」及び「キーオペレーターパスワード」、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「データセキュリティーキット DA-SC06 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、「データセキュリティーキット DA-SC06 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20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、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、攻撃者の攻撃能力が低レベルであることを想定した製品である。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、「1.2.4 TOEの機能」に示したとおりである。

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.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	●利用済み文書データの上書き消去 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しなければならない。

1.5.7 構成条件

本TOEは、パナソニック コミュニケーションズ株式会社製デジタル複合機に搭載して使用する。本TOEの対応機種は以下のとおりである。

・日本国内適用機種(※)：DP-8032P / 8025P、DP-8032V / 8025V、
DP-8032VA / 8025VA
・海外適用機種(※)： DP-8032 / 8025

(※) すべての適用機種は、標準ではハードディスク装置を装着していない。本TOEを使用するためには、別途、オプション製品であるハードディスクユニットが必要である。

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。

(1) 日本国内対応機種
・取扱説明書 データセキュリティーキット DA-SC06
C0808-0(04)
・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-SC06
C0808-0(03)

(2) 海外対応機種

・Operating Instructions Data Security Kit DA-SC06
C0808-0 (04)

・Installation Instructions for Service Technicians
Data Security Kit DA-SC06
C0808-0 (03)

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20年2月に始まり、平成20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20年5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20年5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。

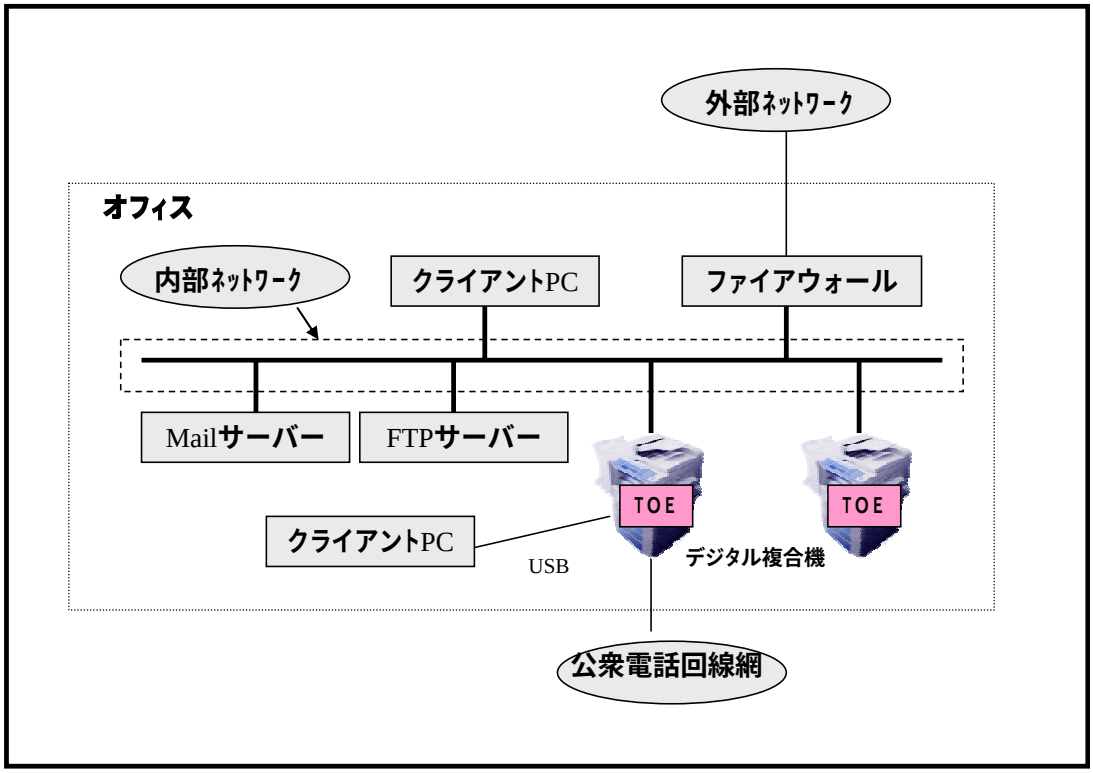

図2-1　開発者テストの構成

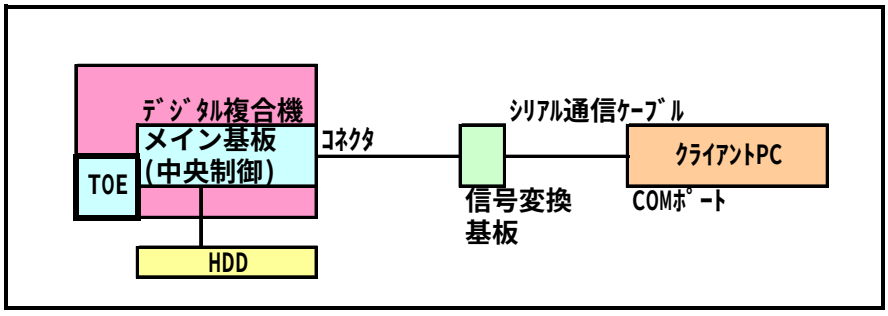

図2-2　ハードディスク蓄積データ上書きテストの構成

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。

テストに使用したデジタル複合機は、日本国内対応機種のDP-8032VA及び海外対応機種のDP-8032である。いずれの機種も、ハードディスク装置には、

オプションのハードディスクユニット（型番DA-HD31）を使用した。

なお、本TOEは複数機種に対応している。機種の違いはプリント速度、搭載可能機能（ファクス機能）及び装着可能なオプションユニット（自動両面ユニット）の違いである。これらの違いは、本TOEが提供するセキュリティ機能の対象ではないため、本TOEの動作に影響はなく、代表機種によるテストで十分であることを評価者が確認している。

b.テスト手法

テストには、以下の手法が使用された。

①コントロールパネル及びクライアントPC（内部ネットワーク及びUSB接続）からTOEに対する操作を行い、その表示と動作を確認する。

②ハードディスク蓄積データ上書き機能の確認のため、コントロールパネル及びクライアントPCからTOEに対する操作を行い、図2-2に示すデバッグ用のクライアントPCに出力されたログで動作を確認する。

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。

ただし、Mailサーバー、FTPサーバー及び公衆電話回線網は、それらを必要とするテストは実施しないため使用していない。

テストに使用したデジタル複合機は開発者テストと同一である。

b.テスト手法

テストには、以下の手法が使用された。

①コントロールパネルを使用してセキュリティ機能を刺激し、その表示と動作を確認する。

②コントロールパネル及びクライアントPC（USB接続）を使用してセキュリティ機能を刺激し、図2-2に示すデバッグ用クライアントPCに出力されたログでテスト結果を確認する。

③クライアントPC（内部ネットワーク接続）を使用して不正侵入の可能性を探索する。

c.実施テストの範囲

評価者が独自に考案した評価者独立テストを33項目、侵入テストを4項目、開発者テストのサンプリングによるテストを55項目、計92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、すべてのセキュリティ機能のふるまいがテストされている。

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に対する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、前提条件のいずれかへ遡れ、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が適切に定義されてい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の依存性がすべて識別されてい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.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

本TOEの脅威T.RECOVERに直接対抗しているのは、IT環境であるハードディスク装置のドライブロック機能であり、本TOEはその管理機能（パスワード設定、及び、設定操作をキーオペレーターに限定する識別認証）を提供していることに、読者は注意されたい。

ただし、本TOEの保護資産は、脅威に対抗するためのドライブロック機能と、組織方針によるハードディスク蓄積データ上書き機能で、二重に保護されている。本TOEを利用するにあたっては、ガイダンスの記載内容に従って、両機能を適切に運用することが必要である。

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。

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。本文書では、パナソニック コミュニケーションズ株式会社製の 日本国内適用機種： DP-8032P / 8025P、 DP-8032V / 8025V、 DP-8032VA / 8025VA 海外適用機種 ： DP-8032 / 8025 を総称してデジタル複合機と記述する。
内部ネットワーク	デジタル複合機を導入する組織のLAN。
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）。
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	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	デジタル複合機の機械管理者。

サービス技術者	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。
コントロールパネル	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。
SPC基板	スキャナー／プリンターユニットのメカ制御を行う基板。
FROM	電気的な一括消去及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。（Flash Read Only Memory）
文書データ	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、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。 ・ファクス通信ユニットから読み込まれた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	デジタル複合機のコピー／プリンター／スキャナー機能の利用時に、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。
タンデムコピー	スキャナーユニットから読み込まれたデータのコピー部数の半分を読み込んだデジタル複合機で、残り半分を内部ネットワークに接続された他のデジタル複合機で印刷する機能。
リモートコピー	スキャナーユニットから読み込まれたデータのすべてを内部ネットワークに接続された他のデジタル複合機で印刷する機能。

6 参照

[1] データセキュリティーキット DA-SC06 セキュリティーターゲット 第1.01版（2008年5月21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] データセキュリティーキット DA-SC06 評価報告書 第1.4版 2008年10月15日 有限中間法人 ITセキュリティセンター 評価部