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11月15日（IT認証6119）**
認証番号	C0093
認証申請者	**株式会社　沖データ**
TOE**の名称**	**[日本語名]オキカラーページプリンタ** C8800 **セキュリティモジュール** **[英語名]** OKI Color Page Printer C8800 Security Module
TOE**のバージョン**	DS 01.00
PP**適合**	**なし**
適合する保証要件	EAL3
TOE**開発者**	**株式会社　沖データ**
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4月27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

「オキカラーページプリンタ C8800 セキュリティモジュール」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 はじめに

この認証報告書は、「オキカラーページプリンタ C8800 セキュリティモジュール」（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株式会社　沖データ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]オキカラーページプリンタ C8800 セキュリティモジュール
　　[英語名] OKI Color Page Printer C8800 Security Module
バージョン:　DS 01.00
開発者:　株式会社　沖データ

1.2.2 製品概要

TOEは、セキュリティキットを装着したオキカラーページプリンタC8800 製品のコントローラユニット上のファームウェア内のセキュリティモジュールである。TOE は、オキカラーページプリンタC8800 にセキュリティキットが装着された場合に動作し、セキュリティキットの暗号化機能を使用し、印刷及び管理のためHDD に蓄えられるデータを暗号化して保存することにより、HDD が盗難されHDD に蓄えたデータが不正に読み出される場合の情報漏洩を防止する。

1.2.3 TOEの範囲と動作概要

TOE は、オキカラーページプリンタ C8800 製品のコントローラユニット上のファームウェア内のセキュリティモジュールであり、ハードディスク装置内に蓄積された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。

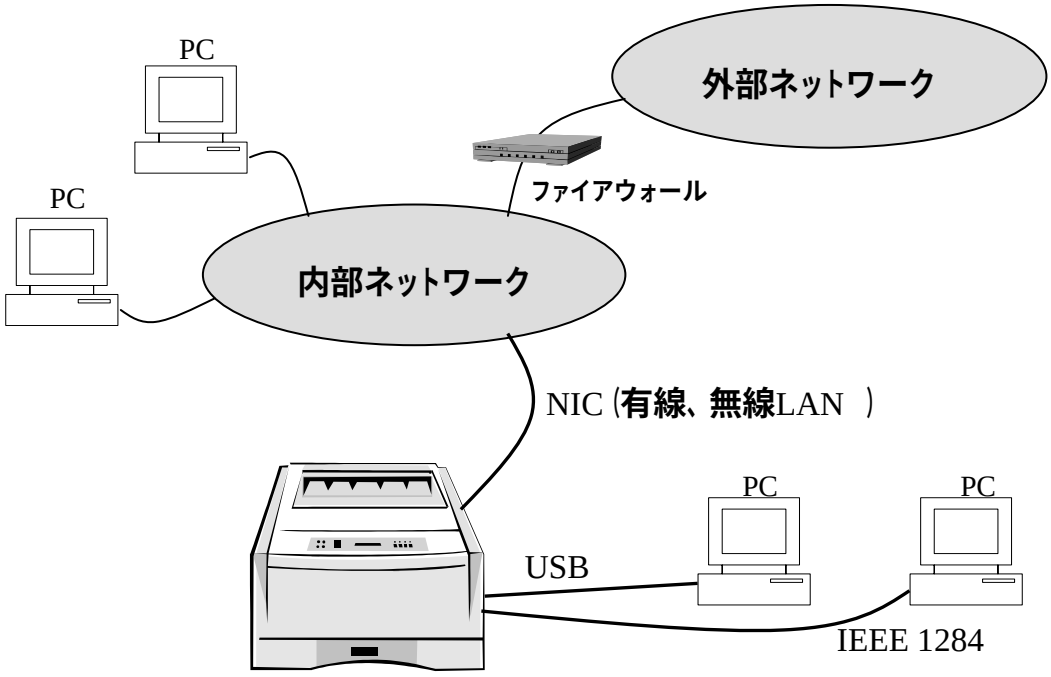

図 1-1　TOE の利用環境

次に本 TOE の物理的境界を以下に示す。

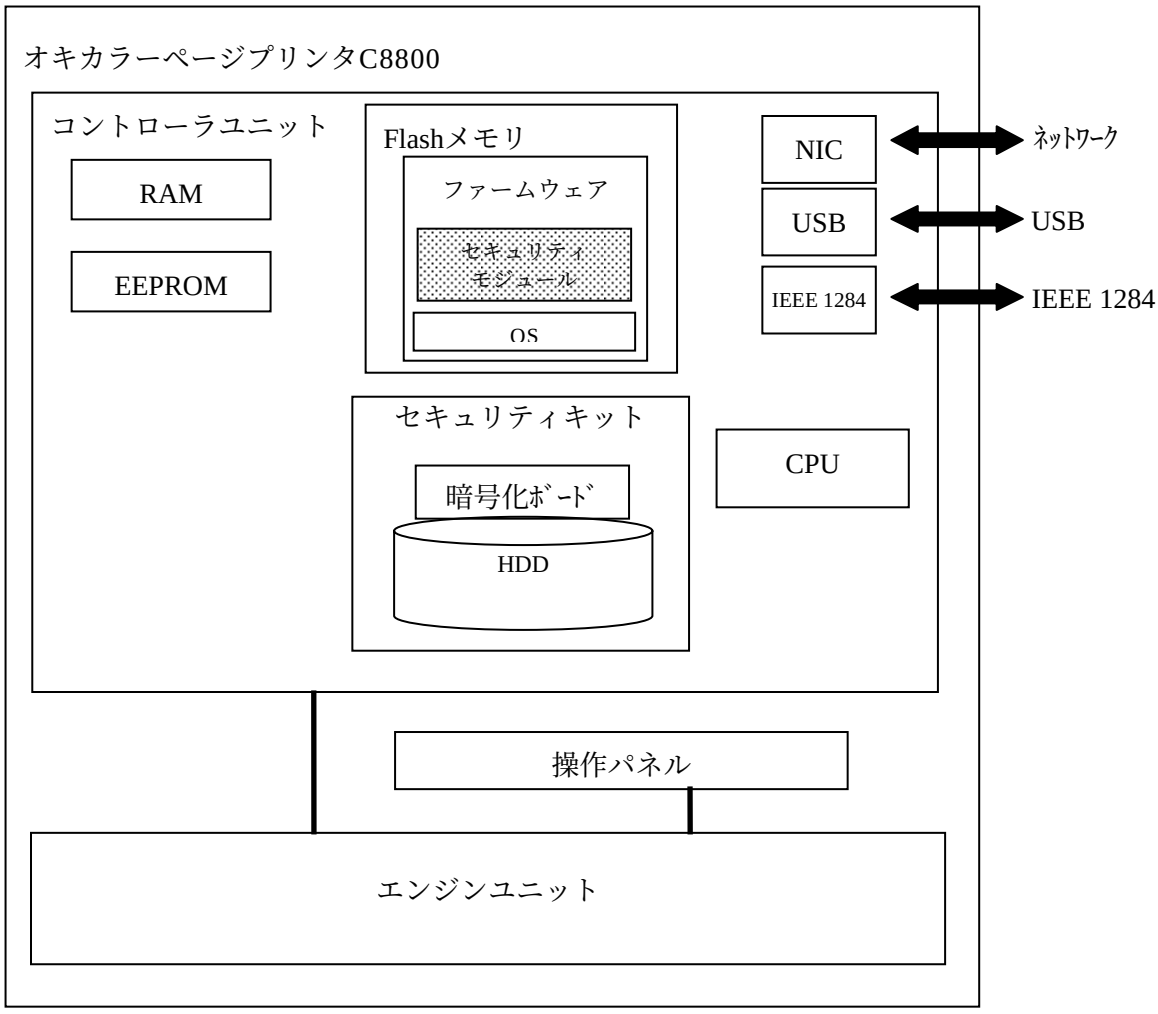

図 1-2　TOE の物理的境界

図 1-2 において TOE は、暗号化ボードと HDD から構成されるセキュリティキットを装着した場合に動作するコントローラユニット上のファームウェア内のセキュリティモジュール部である。TOE の部分を網掛けで示す。

Flash メモリは、コントローラユニットの各処理を制御するモジュールやセキュリティキットおよびセキュリティ機能を制御するセキュリティモジュール等のファームウェアが格納され、コントローラユニットが情報を格納するために利用する不揮発性メモリ記憶媒体である。

セキュリティキットは、HDD に書き込むデータを暗号化し、HDD から読み出すデータを復号する暗号化チップを搭載した暗号化ボードおよび HDD から構成されるユニットである。

RAM はコントローラユニットの各処理を制御するモジュールやセキュリティキットおよびセキュリティ機能を制御するセキュリティモジュール等のファームウェアが動

作中に必要に応じて任意に読み書きするためのメモリである。

EEPROM はコントローラユニットのメニュー設定情報等を保存しておく、不揮発性メモリである。

1.2.4 TOEの機能

TOE は以下のセキュリティ機能を有する。

・暗号鍵生成機能

乱数を発生させて暗号鍵を生成する。

・暗号鍵設定機能

暗号鍵生成機能にて生成された暗号鍵をセキュリティキットに設定する。暗号鍵設定後、セキュリティキットが正しく暗号鍵を受け付けたか否かの検証も行う。本機能は、セキュリティキット識別機能により正当性が確認された場合にのみ動作する。

・セキュリティキット識別機能

オキカラーページプリンタC8800 にセキュリティキットが一旦装着された以降に、セキュリティキットが取り外されたという不正を発見した場合は、操作パネルにサービスコールを表示するためのトリガを発生させる。これにより、オキカラーページプリンタC8800 は、操作パネルにサービスコールを表示し、オキカラーページプリンタC8800 の動作を停止する。

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「オキカラーページプリンタ C8800 セキュリティモジュール 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、「オキカラーページプリンタC8800セキュリティモジュール評価報告書」（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19年04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、確率的または順列的メカニズムに基づくセキュリティ機能要件はない。

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。

- 暗号鍵生成機能

  本機能は、セキュリティキットによる暗号操作に使用する暗号鍵を生成する

ものである。暗号鍵の生成は次の２つのケースが存在する。

① オキカラーページプリンタC8800 に初めてセキュリティキットを装着した後の初回起動時で、固定的なアルゴリズム（OKI PX 暗号鍵生成アルゴリズム）で暗号鍵を自動生成し、この暗号鍵をFlashメモリへ格納する。

② 利用者が、操作パネルから暗号鍵作成指示を実行した時。この時は、固定的なアルゴリズム（OKIPX 暗号鍵生成アルゴリズム）で暗号鍵を生成し、この暗号鍵をFlash メモリへ格納する。

なお、オキカラーページプリンタC8800 に初めてセキュリティキットを装着した後の初回起動時は、暗号鍵を自動生成し、この暗号鍵をFlash メモリへ格納する本機能は、迂回されず必ず実施される。

- 暗号鍵設定機能

  本機能は、電源が入れられた時に、暗号鍵をFlash メモリから読み出し、暗号鍵をセキュリティキットへ設定するものである。そして、暗号鍵設定後、セキュリティキットが正しく暗号鍵を受け付けたか否かの検証を行うものである。なお、本機能は、電源が入れられた時に、セキュリティキット識別機能で正当であると判断した場合、迂回されず必ず実行される。

- セキュリティキット識別機能

  本機能は、セキュリティキットが一旦装着された以降に、セキュリティキットが取り外されたという不正がないか検証するものである。

  セキュリティキットが一旦装着された以降に、オキカラーページプリンタC8800 の電源がＯＮされた時に不正を発見した場合は、操作パネルにサービスコールを表示するためのトリガを発生させる。これにより、オキカラーページプリンタC8800 は、操作パネルにサービスコールを表示し、オキカラーページプリンタC8800 の動作を停止する。なお、本機能は、電源が入れられた時に、迂回されず必ず実行される。

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	攻撃者が、プリンタから物理的にHDD を取り外し、HDD に蓄えたデータを読み出し再生することで、印刷データが暴露される。
T.STATE	攻撃者が、プリンタからセキュリティキットを取り外し、代わりのHDD を装着することでセキュリティ機能を無効化することにより、以降、暗号化されない印刷データをHDD に蓄えさせる。そして、このHDD を取り外し、HDD 内の印刷デー

	タを読み出し再生することで、印刷データが暴露される。

1.5.6 組織のセキュリティ方針

想定する組織のセキュリティ方針はない。

1.5.7 構成条件

セキュリティキットは株式会社　沖データ製オキカラーページプリンタC8800 シリーズ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1-2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
A.SECURITY_KIT	オキカラーページプリンタC8800 にセキュリティキットを装着し、電源をONして、セキュリティキットの初期化を行う。

1.5.9 製品添付ドキュメント

本TOE使用の前提条件となるセキュリティキットに添付されるドキュメントを以下に示す。

[日本語名] ユーザーズマニュアル セキュリティキット　タイプA1
[英語名]　User’s Manual　Security Kit Type A1

識別　: 43694501EE

バージョン : Rev.1

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11月に始まり、平成19年4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2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2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。

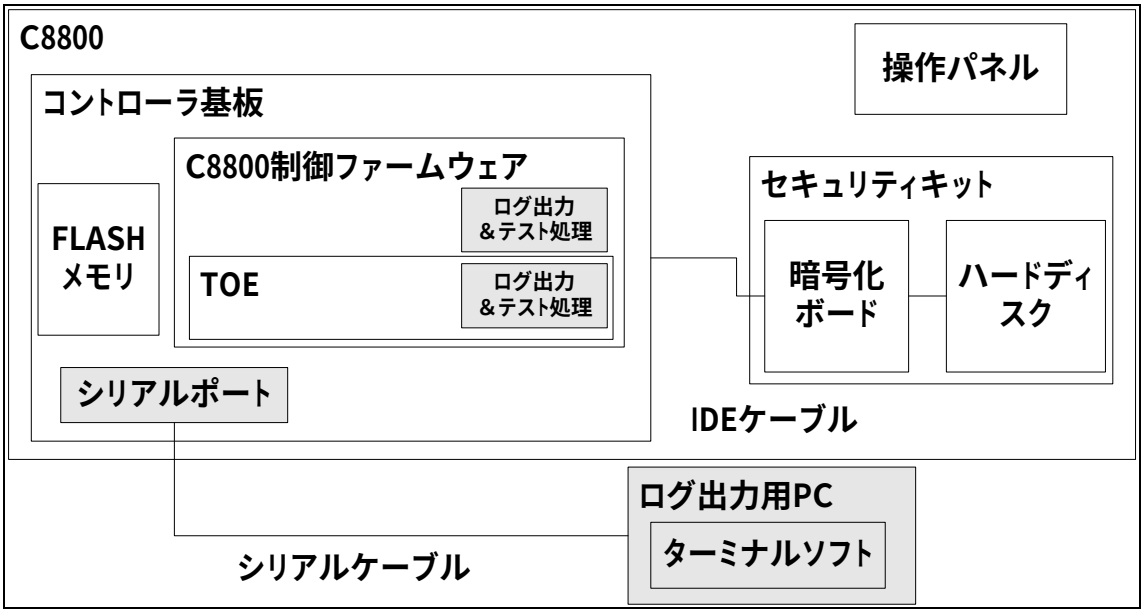

図2-1　開発者テストの構成図

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。

テストは、TOEの関数、及びTOEが利用する外部の関数を実行する際に入力パラメータ及び、処理結果を示すログ出力処理を追加したテスト用のTOE（ファームウェア）を使用して行った。テスト用のTOEと製品版のTOEの違いはログ出力処理の有無だけであり、テスト用のTOEと製品版のTOEで、セキュリティ機能のふるまいに違いはない。(「図2-1」の網掛け部分が製品版と異なる部分であるが、これはTOEのセキュリティ機能のふるまいに影響しない。) また、ログ出力のためにターミナルソフトとしてハイパーターミナルを使用した以外、ツールは使用していない。

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 TOEの動作をログをシリアルポートを用いて出力し、その動作確認を行う。

c.実施テストの範囲

テストは開発者によって5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 セキュリティ関連事象とTOEの動作の確認

② 電源OFF時のHDD取り付けによる動作確認

c.実施テストの範囲

評価者が独自に考案したテストを2項目、開発者テストのサンプリングによるテストを5項目、脆弱性テスト実施による7項目、計14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全てのセキュリティ機能の動作確認

② 電源OFF時の構成の変更による動作確認

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。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。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_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。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_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。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。
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。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。
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。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。
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。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。
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。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。
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。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。
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。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。
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	本TOEは確率的または順列的メカニズムを具備していない。よってSOFを主張すべき機能はなく、本ワークユニットは満たされている。
AVA_SOF.1.2E	本TOEは確率的または順列的メカニズムを具備していない。よってSOFを主張すべき機能はなく、本ワークユニットは満たされている。
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。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。
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。

印刷データ	オキカラーページプリンタC8800のプリンタドライバがインストールされたPCからC8800へ送信したデータ。
イメージデータ	オキカラーページプリンタC8800が受信した印刷データを印刷するために加工したデータおよび印刷データの加工処理中のデータ。
PC	Personal Computer等のオキカラーページプリンタC8800へ印刷データを送信する情報処理装置。
セキュリティキット	オキカラーページプリンタC8800 用 暗号化ボードおよびHDD から構成されるユニット。
メモリ	記憶装置、特に半導体素子による記憶装置。
ユニット	プリント基板に脱着可能な標準品や、オプション品を装備し、動作可能状態とした単位。また、機構部を含んで動作可能状態とした単位。
基板	プリント基板に部品を半田付け実装したものを指す。
操作パネル	表示部、ボタンキー、LED ランプを装備した、ユーザー（利用者）インターフェースのためのデバイス。または、そのユ

	ニット。
不揮発性メモリ	電源を切っても記憶内容を保持することができるメモリのこと。半導体素子、あるいは磁気記憶を用いたものがある。
OS	オペレーティングシステム（Operating System)。オキカラーページプリンタC8800 では、VxWorks 5.5.1 を使用する。

6 参照

[1] オキカラーページプリンタ C8800セキュリティモジュールセキュリティターゲット バージョン 2.30（2007年03月02日）株式会社 沖データ

[2] ITセキュリティ評価及び認証制度の基本規程　平成18年9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18年9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18年9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] オキカラーページプリンタ C8800セキュリティモジュール 評価報告書 初版 2007年03月30日　みずほ情報総研株式会社 情報セキュリティ評価室