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

Version 2.30

2007/03/02

株式会社　沖データ

ドキュメント履歴管理表

版数	変更年月日	修正事項 修正内容	担当
1.00	06-11-03	新規作成	小澤(長)
1.10	06-11-06	ST 名称に C8800 機種名を追加、TOE 識別に C8800 機種名を追加、TOE 識別に英語名追加	小澤(長)
1.20	06-11-22	ST識別にSTの適応製品情報を追加	小澤(長)
1.30	06-12-13	指摘事項修正、ST名称変更、TOE識別変更、TOEの概要説明追加	小澤(長)
1.40	06-12-23	指摘事項修正	小澤(長)
1.50	07-01-09	指摘事項修正	小澤(長)
1.60	07-01-22	指摘事項修正	小澤(長)
1.70	07-01-26	指摘事項修正	小澤(長)
1.80	07-02-05	指摘事項修正，文字間違い修正	小澤(長)
1.90	07-02-09	指摘事項修正	小澤(長)
2.00	07-02-13	指摘事項修正	小澤(長)
2.10	07-02-14	指摘事項修正	小澤(長)
2.20	07-02-22	指摘事項修正	小澤(長)
2.30	07-03-02	誤記修正、出典付記。	小澤(長)

目次

1. ST 概説

1.1. ST 識別

本書と TOE を識別するための情報を記載する。

ST 名称：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：Version 2.30

作成日： 2007/03/02

作成者： 株式会社　沖データ

TOE 識別：

［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

CC 識別：CC バージョン 2.3,ISO/IEC 15408:2005,Interpretations-0512

キーワード：沖データ、オキ、オキデータ、オキカラーページプリンタ、C8800、暗号化、HDD、セキュリティモジュール、セキュリティキット タイプ A1

適応製品：本 ST は、オキカラーページプリンタ C8800 シリーズ（以降オキカラーページプリンタ C8800 と記述する）の次の製品に適応される。
C8800dn,C8800n,C8800cdtn,C8800dtn

1.2. ST 概要

本 ST は､オキカラーページプリンタ C8800 にオキカラーページプリンタ C8800 のオプションキットであるセキュリティキット タイプ A1（以降セキュリティキットと記述する）を装着した場合に動作するオキカラーページプリンタ C8800 のコントローラユニット上のプリンタファームウェア内のセキュリティモジュールについて説明したものである。

本 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的確に使用し、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。

1.3. CC 適合

本書は、以下を満たしている。

（1） CC バージョン 2.3 パート 2 適合

（2） CC バージョン 2.3 パート 3 適合

（3） EAL3

（4） 本 ST が参照する PP はない。

（5） 補足-0512(Interpretations-0512)適合

1.4. 参照資料

本書作成について、表１記載の資料を参照している。

表１　参照資料

略称	文書名
[CC_PART1]	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 2005年8月　バージョン2.3 CCMB-2005-08-001 (平成 17 年　12 月翻訳第 1.0 版　独立行政法人情報処理推進機構　セキュリティセンター)
[CC_PART2]	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 2005年8月　バージョン2.3 CCMB-2005-08-002 (平成 17 年　12 月翻訳第 1.0 版　独立行政法人情報処理推進機構　セキュリティセンター)
[CC_PART3]	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 2005年8月　バージョン2.3 CCMB-2005-08-003 (平成17年　12月翻訳第1.0版　独立行政法人情報処理推進機構　セキュリティセンター)
[INTPR_0512]	補足-0512 (平成17年12月　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)

1.5. 略語、専門用語

本書固有の略語、専門用語を表２に示す。

表２　略語、専門用語

用語	定義
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。
ジョブ	PDL で記述された、一塊の印刷データおよびその印刷データに対応する一塊のイメージデータ。
PDL	Page Description Language の略であり、ページプリンタにおいて、印刷フォーマットや印刷画像を作成するためのプリンタを制御する言語。
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。

2. TOE 記述

2.1. TOE の概要

オキカラーページプリンタ C8800 は、10～20 人以上の規模のグループまたはオフィスで利用されることを想定している。そして、オキカラーページプリンタ C8800 は、HDD を装着することが可能で、HDD を装着した場合には、印刷データやイメージデータを HDD に蓄える等の HDD を利用した機能が利用できる。しかし、HDD を盗難された場合、HDD に蓄えたデータが漏洩してしまう可能性がある。このように HDD が盗難され、HDD に蓄えたデータの漏洩を防ぐためにセキュリティキットが必要となる。TOE は、このセキュリティキットを装着した時に動作するソフトウェアで、セキュリティキットを正しく使うための制御を行う。

2.1.1. TOE 種別

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。

2.1.2. TOE の機能及び利用方法

本節は、TOE の機能及び利用方法について述べる。

2.1.2.1. 利用方法

オキカラーページプリンタ C8800 は、PC から送信された印刷データから画像を形成し画像を印刷する印刷装置であり、利用者は、オキカラーページプリンタ C8800 プリンタにセキュリティキットを装着した場合、TOE のセキュリティ機能を利用することができる。TOE の利用環境を図１に示す。

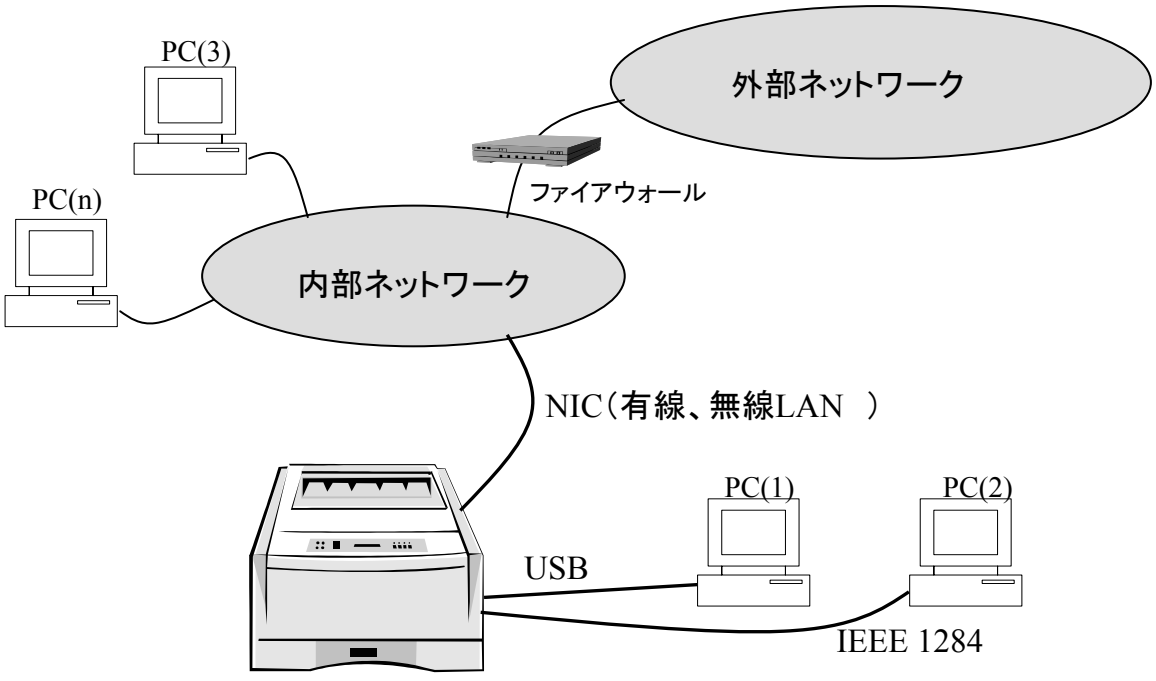

図１　TOE の利用環境

2.1.2.2. TOE の機能

2.1.2.2.1 TOE のセキュリティ機能

⑴暗号鍵生成機能

乱数を発生させて暗号鍵を生成する。

⑵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。

⑶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。

2.1.2.2.2 TOE 外のセキュリティ機能

⑴暗号化/復号化機能

セキュリティキット内の暗号化ボードにて、HDD に書き込むデータを暗号化し、蓄積する。また、同ボードにて、暗号化された HDD 内のデータを復号化して読み出す。

2.2. TOE の構成

本節は、TOE の物理的、論理的構成について述べる。

2.2.1. TOE の物理的構成

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 の物理的構成を図 2 に、各構成要素の説明を表 3 に示す。図において 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。

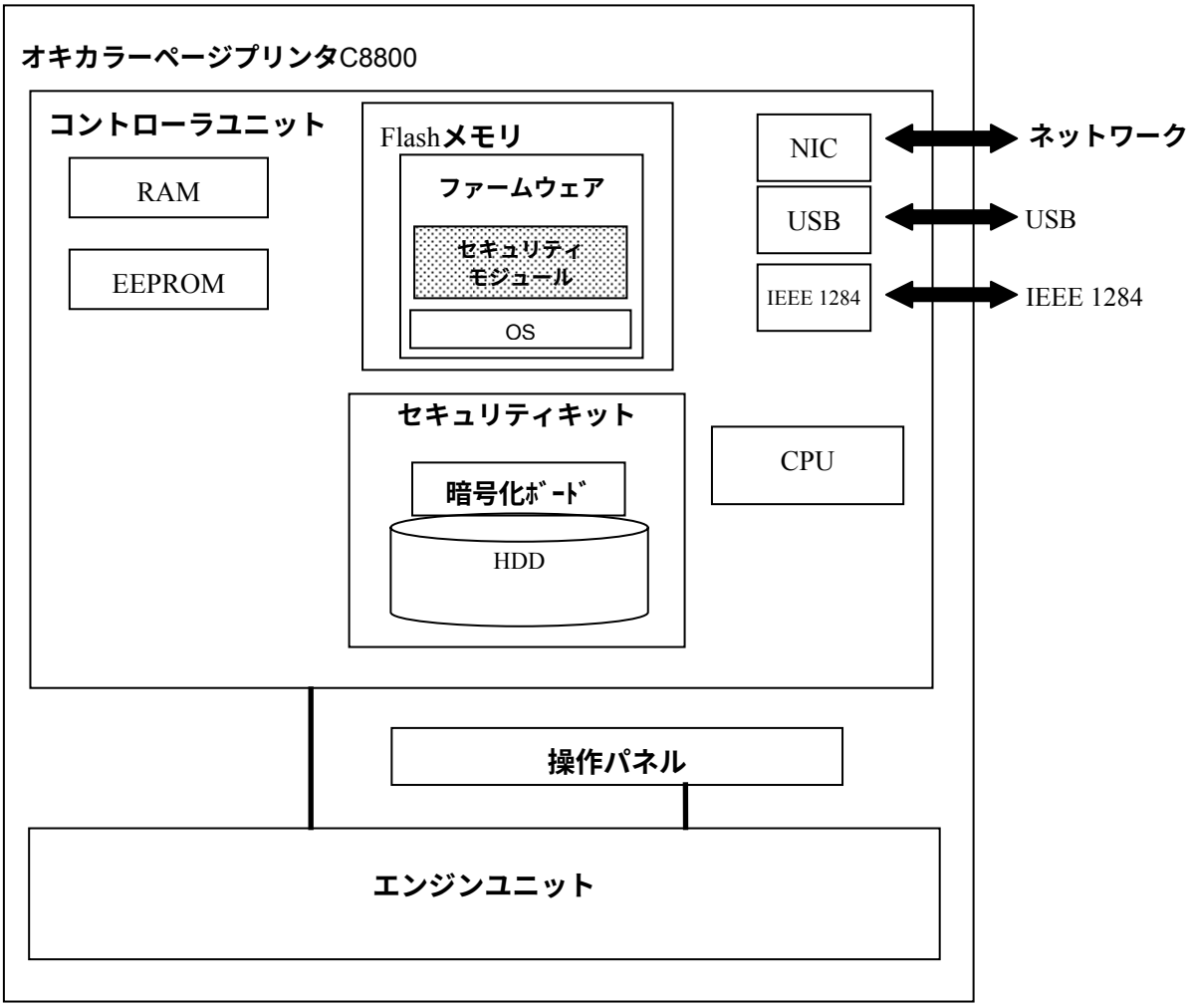

図 2　C8800 の物理的構成と TOE

表 3　構成要素の説明

構成要素名	説明
コントローラユニット	PC 等からネットワーク、USB インターフェース、IEEE 1284 インターフェースを介して送信されてくる印刷データを受信し、エンジンユニットで印刷するためのイメージデータを作成し、作成したイメージデータをエンジンユニットへ渡すことを主な機能とする装置。
エンジンユニット	コントローラユニットから渡されたイメージデータが示す画像を紙に印刷する装置。
操作パネル	ステータスやメニュー等を表示する表示部、メニュー等を操作するためのボタン、ステータス等を示す 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装置。
プリンタ	主に、コントローラユニット、エンジンユニット、操作パネルから構成され PC 等から受信した印刷データを印刷する装置。
CPU	コントローラユニットの制御を行うための中央演算処理装置。
Flash メモリ	・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ている不揮発性メモリ。 ・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。
RAM	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（Random Access Memory）。
EEPROM	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。(Electronically Erasable Programmable ROM)。
ファームウェア	コントローラユニットの制御を行うためのソフトウェア。
セキュリティモジュール	ファームウェアの中に存在する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ためのソフトウェア。
セキュリティキット	暗号化ボードおよび HDD から構成されるユニット。
暗号化ボード	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基板。
HDD	ハードディスク装置。
NIC	Network Interface Card
USB	Universal Serial Bus
IEEE 1284	IEEE std 1284-1994 準拠双方向パラレルインターフェース

2.2.2.　TOE の論理的構成

TOE の論理的構成図を図 3 に、機能の説明を表４に示す。TOE の論理的範囲を太線枠で示す。網掛け部分がセキュリティ機能である。

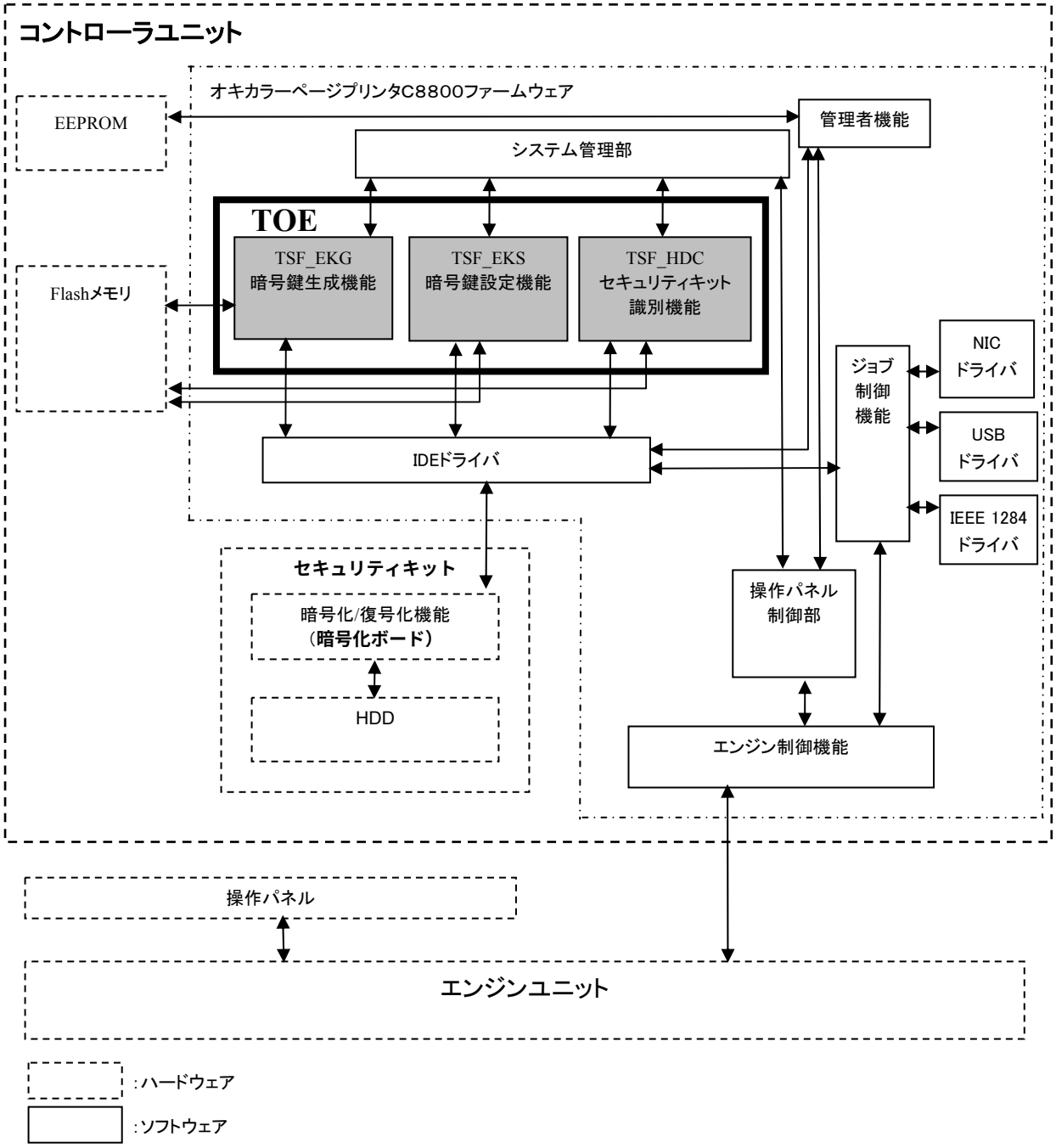

図３　TOE の論理的構成図

表４　機能の説明

機能名	機能説明
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。正当性が確認された場合にのみ暗号鍵をセキュリテイキットに設定する。
暗号化/復号化機能	セキュリティキット内の暗号化ボードにて、HDD に書き込むデータを暗号化し、蓄積する。また、同ボードにて、暗号化された HDD 内のデータを復号化して読み出す。
システム管理部	オキカラーページプリンタ C8800 の状態を管理するための制御部。
操作パネル制御部	システム管理部が管理するステータスをエンジン制御機能を介して操作パネルに表示したり、操作パネルのボタン押下情報をエンジン制御機能から取得して、管理者機能、暗号鍵生成機能へボタン押下情報を渡すための制御部。
管理者機能	HDD のフォーマット等を行う管理者のための機能。
ジョブ制御機能	印刷データを HDD へ蓄えたり、印刷データからイメージデータを作成し、エンジン制御機能へイメージデータを渡す機能。
エンジン制御機能	・エンジンユニットと通信し、ジョブ制御機能から渡されたイメージデータをエンジンユニットへ渡すための機能。 ・操作パネルのボタン押下情報をエンジンユニットから取得し、操作パネル制御部を介して管理者機能、暗号鍵生成機能へボタン押下情報を渡すための機能。 ・操作パネル制御部から渡されたプリンタのステータスをエンジンユニットを介して操作パネルに表示するための機能。
IDE ドライバ	HDD のデータの読み書きを行うための機能。
NIC ドライバ	ネットワークに接続されている機器との通信制御を行うための機能。
USB ドライバ	USB インターフェースに接続されている機器との通信制御を行うための機能。
IEEE 1284 ドライバ	IEEE 1284 パラレルインターフェースに接続されている機器との通信制御を行うための機能。

2.3. TOE の保護資産

本 TOE における保護資産は、HDD に蓄えたデータである。

3. TOE セキュリティ環境

本章は、TOE セキュリティ環境について述べる。

3.1. 前提条件

TOE が、HDD に蓄えたデータを保護するためのセキュリティ機能を発揮するための前提条件は表５の通りである。

表５　前提条件

識別子	定義
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。

3.2. 脅威

オキカラーページプリンタ C8800 は、HDD が装着されている状態では、例えば操作パネルからパスワードを入力しパスワードが一致した場合に印刷を行う認証印刷のように HDD に蓄えたデータを操作パネルの操作により印刷することが可能である。また、ファイル読み出しコマンドを送信することにより、HDD に蓄えたデータを読み出すことも可能であるが、TOE に対する脅威は表６に示す通り、HDD が持ち去され HDD から直接データを読み出されることである。

TOE の攻撃者としては、TOE の動作について一般知識を有し、プリンタから物理的に HDD を取り出す技能を有し、簡単に入手することができるハードウェアやソフトウェアのツールを使用して、HDD に蓄えられたデータの再生、または不正な入手をはかる低レベルな攻撃者を想定する。

なお、攻撃者の定義は IPA 翻訳文書「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 CCMB-2005-08-004」における 「A.8 機能強度及び脆弱性分析」の記載による。

表６　TOE に対する脅威

識別子	定義
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。

3.3. 組織のセキュリティ方針

本 ST が想定する組織のセキュリティ方針はない。

4. セキュリティ対策方針

本章は、セキュリティ対策方針における施策について述べる。

4.1. TOE のセキュリティ対策方針

TOE のセキュリティ対策方針を表７に示す。

表７　TOE のセキュリティ対策方針

識別子	定義
O.KEY	TOE は、セキュリティキットに適用する暗号鍵を生成する。
O.SET_KEY	TOE は、セキュリティキットへの暗号鍵の設定を行う。
O.STATE	TOE は、セキュリティキットが、一度装着されたら、そのセキュリティキットが装着され続けていることを確認する。もし、セキュリティキットが取り外された場合には、プリンタの動作を停止し、操作パネルにサービスコールを表示させるトリガを発生させる。このトリガによりオキカラーページプリンタ C8800 の操作パネルにサービスコールが表示され、利用者に正常でないことを通知する。

4.2. 環境のセキュリティ対策方針

TOE の利用環境における環境のセキュリティ対策方針を IT 環境のセキュリティ対策方針、Non-IT 環境のセキュリティ対策方針を表８に示す。

表８　環境のセキュリティ対策方針

環境	識別子	定義
IT 環境	OE.KIT	セキュリティキットは、TOE が設定した暗号鍵で印刷データを暗号化してから HDD に蓄える。
Non-IT 環境	OE-N.SETTING_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。

5. IT セキュリティ要件

5.1. TOE セキュリティ要件

5.1.1. TOE セキュリティ機能要件

本節は、TOE セキュリティ機能要件を[CC_PART2]のクラス別に記述する。最小機能強度は、5.1.3 節で規定する。本節に記述するすべての TOE セキュリティ機能要件は[CC_PART2]から抜き出したものであり拡張要件はない。

クラス FCS:暗号サポート

・FCS_CKM.1　暗号鍵生成
　下位階層：　なし
　FCS_CKM.1.1　TSF は、以下の[割付：なし]に合致する、指定された暗号鍵生成アルゴリズム[割付：OKI PX 暗号鍵生成アルゴリズム]と指定された暗号鍵長[割付:168 ビット]に従って、暗号鍵を生成しなければならない。
　依存性：　[FCS_CKM.2 暗号鍵配付または FCS_COP.1 暗号操作]
　FCS_CKM.4 暗号鍵破棄
　FMT_MSA.2　セキュアなセキュリティ属性

・FCS_CKM.2　暗号鍵配付
　下位階層：　なし
　FCS_CKM.2.1　TSF は、以下の[割付：なし]に合致する、指定された暗号鍵配付方法[割付：OKI PX 暗号鍵配付アルゴリズム]に従って暗号鍵を配付しなければならない。
　依存性：　[FDP_ITC.1　セキュリティ属性なしデータ利用者データのインポート、または、FCS_CKM.1 暗号鍵生成]
　FCS_CKM.4 暗号鍵破棄
　FMT_MSA.2　セキュアなセキュリティ属性

クラス FAU:セキュリティ監査

・FAU_ARP.1　セキュリティアラーム
　下位階層：　なし
　FAU_ARP.1.1　TSF は、セキュリティ侵害の可能性が検出された場合、[割付：セキュリティキットの使用中止およびサービスコールを表示させるためのトリガを発生させること]を実行しなければならない。
　依存性：　FAU_SAA.1 侵害の可能性の分析

・FAU_SAA.1　侵害の可能性の分析

下位階層：　なし

FAU_SAA.1.1　TSF は、監査事象のモニタに規則のセットを適用し、これらの規則に基づき TSP 侵害の可能性を示すことができなければならない。

FAU_SAA.1.2　TSF は、監査事象をモニタするための以下の規則を実施しなければならない。

a)セキュリティ侵害の可能性を示すものとして知られている[割付：セキュリティキットが取り外されている事象]をすべて合わせた、あるいは組み合わせたもの；

b)[割付：その他の規則は、なし]

依存性：　FAU_GEN.1 監査データ生成

クラス FPT:TSF の保護

・FPT_RVM.1　TSP の非バイパス性

下位階層：　なし

FPT_RVM.1.1　TSF は、TSC 内の各機能の動作進行が許可される前に、TSP 実施機能が呼び出され成功することを保証しなければならない。

依存性：　なし

5.1.2. TOE セキュリティ保証要件

本書が選択した保証レベルについて保証コンポーネントを表９に示す。表９は EAL3 適合を主張するために満たすべき保証要件である。すべての依存性は満たされている。

表９　保証要件

コンポーネント	コンポーネント名称	依存性
ACM_CAP.3	許可の管理	ALC_DVS.1
ACM_SCP.1	TOE の CM 範囲	ACM_CAP.3
ADO_DEL.1	配付手続き	なし
ADO_IGS.1	設置、生成及び立ち上げ手順	AGD_ADM.1
ADV_FSP.1	非形式的機能仕様	ADV_RCR.1
ADV_HLD.2	セキュリティ実施上位レベル設計	ADV_FSP.1,ADV_RCR.1
ADV_RCR.1	非形式的対応の実証	なし
AGD_ADM.1	管理者ガイダンス	ADV_FSP.1
AGD_USR.1	利用者ガイダンス	ADV_FSP.1
ALC_DVS.1	セキュリティ手段の識別	なし
ATE_COV.2	カバレージの分析	ADV_FSP.1,ATE_FUN.1
ATE_DPT.1	テスト：上位レベル設計	ADV_HLD.1,ATE_FUN.1
ATE_FUN.1	機能テスト	なし
ATE_IND.2	独立テスト－サンプル	ADV_FSP.1,AGD_ADM.1,AGD_USR.1,ATE_FUN.1
AVA_MSU.1	ガイダンスの検査	ADO_IGS.1,ADV_FSP.1,AGD_ADM.1,AGD_USR.1
AVA_SOF.1	TOE セキュリティ機能強度評価	ADV_FSP.1,ADV_HLD.1
AVA_VLA.1	開発者脆弱性分析	ADV_FSP.1,ADV_HLD.1,AGD_ADM.1,AGD_USR.1

5.1.3. 最小機能強度

本 TOE の最小機能強度は SOF-基本である。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。

5.2. IT 環境に対するセキュリティ要件

5.2.1. IT 環境に対するセキュリティ機能要件

FCS_COP.1　暗号操作

下位階層：　なし

FCS_COP.1.1　TSF は、[割付：FIPS PUB 46-3]に合致する、特定された暗号アルゴリズム[割付：TripleDES]と暗号鍵長[割付：168 ビット]に従って、[割付：印刷データの暗号化と復号]を実行しなければならない。

依存性：　FCS_CKM.1 暗号鍵生成

FCS_CKM.4 暗号鍵破棄

FMT_MSA.2　セキュアなセキュリティ属性

5.2.2. IT 環境に対するセキュリティ保証要件

TOE の IT 環境が満たすべきセキュリティ保証要件はない。

6. TOE 要約仕様

本章は、セキュリティ要件に対する TOE のセキュリティ機能と保証手段を述べる。

6.1. TOE セキュリティ機能（TSF）

TOE セキュリティ機能要件と TOE セキュリティ機能の対応関係を表 10 に示す。表中に、各々の対応関係を記載している節番号を示す。

表 10　機能要件と仕様概要

機能 機能要件	TSF_EKG 暗号鍵生成機能	TSF_EKS 暗号鍵設定機能	TSF_HDC セキュリティキット識別機能
FCS_CKM.1	6.1.1		
FCS_CKM.2		6.1.2	
FAU_ARP.1			6.1.3
FAU_SAA.1			6.1.3
FPT_RVM.1	6.1.1	6.1.2	6.1.3

6.1.1.　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（OKI PX 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。

この①②のうち、本セキュリティターゲットの対象となるセキュリティ機能は①のみである。

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。

6.1.2.　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。

6.1.3. 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。

6.2. 保証手段

本 ST におけるセキュリティ保証要件の各コンポーネントに対する保証手段となるドキュメントを表 11 に示す。

表 11　保証手段

コンポーネント	保証手段
ACM_CAP.3	構成管理説明書
ACM_SCP.1	構成リスト
ADO_DEL.1	配付手順説明書
ADO_IGS.1	配付手順説明書 ユーザーズマニュアル　セキュリティキットタイプ A1 (User's Manual Security Kit Type A1)
ADV_FSP.1	機能仕様書
ADV_HLD.2	機能仕様書
ADV_RCR.1	表現対応分析書
AGD_ADM.1	ユーザーズマニュアル　セキュリティキットタイプ A1 (User's Manual Security Kit Type A1)
AGD_USR.1	ユーザーズマニュアル　セキュリティキットタイプ A1 (User's Manual Security Kit Type A1)
ALC_DVS.1	開発セキュリティ仕様書
ATE_COV.2	カバレージ分析書
ATE_DPT.1	テスト仕様書
ATE_FUN.1	テスト仕様書 テスト環境説明書
ATE_IND.2	テスト環境説明書
AVA_MSU.1	ユーザーズマニュアル　セキュリティキットタイプ A1 (User's Manual Security Kit Type A1)
AVA_SOF.1	対象資料なし
AVA_VLA.1	脆弱性分析書

6.3. セキュリティ機能強度

本 TOE において、SOF 主張を実現すべき IT セキュリティ機能はない。

7. PP 主張

本 TOE は、PP には準拠していない。

8. 根拠

本章は、本書の完全性と一貫性を検証する。

8.1. セキュリティ対策方針根拠

TOE セキュリティ環境に示した脅威、前提条件に対してセキュリティ対策方針で示した対策が有効であることを表 12 に検証する。表 12 は、脅威、前提条件とセキュリティ対策方針の対応について、その根拠を記載している節番号を示したものである。

表 12　セキュリティ対策方針根拠

セキュリティ 対策方針	脅威 T.RECOVER	脅威 T.STATE	前提条件 A.SECURITY_KIT
O.KEY	8.1.1		
O.SET_KEY	8.1.1		
O.STATE		8.1.2	
OE.KIT	8.1.1		
OE-N.SETTING_KIT			8.1.3

8.1.1.　T.RECOVER

脅威 T.RECOVER に対して、O.KEY で作成した暗号鍵を O.SET_KEY が安全にセキュリティキットに設定し、その設定された暗号鍵をセキュリティキットが使って、OE.KIT により印刷データを人間が意味のあるものとして判読できないように、印刷データを暗号化した後に HDD へ書き込むことで対抗する。これによりオキカラーページプリンタ C8800 内の HDD が盗難された場合でも、HDD に蓄えたデータの漏えいを防止できる。

8.1.2.　T.STATE

脅威 T.STATE に対して、O.STATE でセキュリティキットが取り外されたことを認識し、この不正な状態を認識した場合には、サービスコールを表示し、プリンタを動作させないことで、他の HDD に印刷データを書き込ませ、この HDD を持ち去り、HDD に蓄えたデータを読み出すことによる HDD に蓄えたデータの漏えいを防止できる。

8.1.3.　A.SECURITY_KIT

前提条件 A.SECURITY_KIT は、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ことであり、OE-N.SETTING_KIT は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ことであるため、A.SECURITY_KIT は、OE-N.SETTING_KIT によって満たされる。

8.2. セキュリティ要件根拠

セキュリティ対策方針に対して、IT セキュリティ要件が有効であることを検証する。

8.2.1. TOE セキュリティ機能要件根拠

本節では、TOE セキュリティ機能要件が TOE のセキュリティ対策方針を達成するのに適していることの根拠を示す。

TOE セキュリティ機能要件と TOE のセキュリティ対策方針の対応について表 13 に示す。表 13 は、各々の対応関係についてその根拠を記載している節番号を示したものである。

表 13　TOE セキュリティ機能要件根拠

対策方針 要件	O.KEY	O.SET_KEY	O.STATE	OE.KIT
FCS_CKM.1	8.2.1.1			
FCS_CKM.2		8.2.1.2		
FAU_ARP.1			8.2.1.3	
FAU_SAA.1			8.2.1.3	
FCS_COP.1				8.2.1.4
FPT_RVM.1	8.2.1.1	8.2.1.2	8.2.1.3	

8.2.1.1. O.KEY

O.KEY は、オキカラーページプリンタ C8800 の HDD に対して、印刷データの保存を実行したオキカラーページプリンタ C8800 以外からアクセスされても、HDD に蓄えたデータの漏えいを防止するため、OE-N.SETTING_KIT により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ことでセキュリティキットが使用するそのオキカラーページプリンタ C8800 固有の暗号鍵を、FCS_CKM.1 により生成する。

また、FPT_RVM.1 により FAU_SAA.1 が必ず実行され、正常な状態を検出した場合は、O.KEY を実現する FCS_CKM.1 は、必ず実行される。

8.2.1.2. O.SET_KEY

O.SET_KEY は、オキカラーページプリンタ C8800 の HDD に対して、印刷データの保存を実行したオキカラーページプリンタ C8800 以外からアクセスされても、HDD に蓄えたデータの漏えいを防止するため、OE-N.SETTING_KIT によりオキカラーページプリンタ C8800 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ことでセキュリティキットが使用するそのオキカラーページプリンタ C8800 固有の暗号鍵を、FCS_CKM.2 により設定する。

また、FPT_RVM.1 により FAU_SAA.1 が必ず実行され、正常な状態を検出した場合は、O.SET_KEY を実現する FCS_CKM.2 は、必ず実行される。

8.2.1.3. O.STATE

O.STATE は、オキカラーページプリンタ C8800 に装着されているセキュリティキットが取り外されたことを FAU_SAA.1 により認識し、この不正な状態を認識した場合には、FAU_ARP.1 によりサービスコールを表示し、オキカラーページプリンタ C8800 を動作させないことで利用者に異常を認識させるという対策方針を実現できる。

また、FPT_RVM.1 により FAU_SAA.1 は、必ず実行され、FAU_SAA.1 で不正な状態を検出した場合は、FAU_ARP.1 も必ず実行され O.STATE を実現する。

8.2.1.4. OE.KIT

FCS_COP.1 によりセキュリティキットの HDD に蓄えたデータは、すべて暗号化してから HDD に蓄えることで HDD の盗難による HDD に蓄えたデータの漏えいを防止するという対策方針を実現できる。

8.2.2. セキュリティ機能要件の依存性根拠

セキュリティ機能要件の依存性について表 14 に示す。表 14 は、満足すべきと CC が規定する依存性と本 TOE が満足している依存性、満足していない依存性、及び満足していないことの妥当性を記載している節番号を示したものである。

表 14 セキュリティ機能要件の依存性

依存性 機能要件	満足すべき 依存性	満足している 依存性	不満足の依存性	依存性不満足の 妥当性
FCS_CKM.1	[FCS_CKM.2 または FCS_COP.1], FCS_CKM.4, FMT_MSA.2	FCS_CKM.2	FCS_CKM.4 FMT_MSA.2	8.2.2.1
FCS_CKM.2	[FDP_ITC.1 または FCS_CKM.1], FCS_CKM.4, FMT_MSA.2	FCS_CKM.1	FCS_CKM.4 FMT_MSA.2	8.2.2.1
FAU_ARP.1	FAU_SAA.1	FAU_SAA.1		
FAU_SAA.1	FAU_GEN.1		FAU_GEN.1	8.2.2.2
FCS_COP.1	FCS_CKM.1 FCS_CKM.4 FMT_MSA.2	FCS_CKM.1	FCS_CKM.4 FMT_MSA.2	8.2.2.3

8.2.2.1. FCS_CKM.4 と FMT_MSA.2 の依存性を必要としない根拠

暗号鍵は、Flash メモリに格納され電源が入れられるたびにセキュリティキットに設定されるものであり、Flash メモリに保存されるデータである。また、Flash メモリ上のデータ構造は開示されておらず、攻撃者が Flash メモリから暗号鍵を特定し、取り出すことは困難であるため、標準の方法を用いて暗号鍵を破棄する FCS_CKM.4 は必要としない。

また、暗号鍵は、管理されるべきセキュリティ属性を持たないため、セキュアなセキュリティ属性を規定する必要はなく、FMT_MSA.2 は必要としない。

8.2.2.2. FAU_GEN.1 の依存性を必要としない根拠

TOE 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ている不正を認識した場合は、オキカラーページプリンタ C8800 の動作を停止させてしまうので FAU_GEN.1 の監査データの生成は必要ない。

8.2.2.3.　FCS_CKM.1 と FCS_CKM.4 と FMT_MSA.2 の依存性を必要としない根拠

暗号鍵の生成は、TOE が行うので FCS_CKM.1 の依存性は必要としない。

暗号鍵は、オキカラーページプリンタ C8800 の電源が ON された時に TOE からセキュリティキットに対して設定され、オキカラーページプリンタ C8800 の電源が OFF された時にセキュリティキット上の鍵は、消滅するので標準の方法を用いて暗号鍵を破棄する必要性がなく、標準の方法を用いて暗号鍵を破棄する FCS_CKM.4 は必要としない。

また、この暗号鍵は、前述の通りオキカラーページプリンタ C8800 の電源が ON された時に TOE からセキュリティキットに対して設定され、電源が OFF された時にセキュリティキット上の鍵は、消滅するので、FMT_MSA.2 によってセキュアな値を保証しなければならないセキュリティ属性が存在しない。

8.2.3.　TOE セキュリティ機能要件の相互作用

本 TOE のセキュリティ機能要件の相互作用の関係について表 15 に示す。

表 15　TOE セキュリティ機能要件の相互作用

対策方針 要件	迂回防止	非活性化防止	干渉防止	無効化防止
FCS_CKM.1	FPT_RVM.1	なし	なし	なし
FCS_CKM.2	FPT_RVM.1	なし	なし	なし
FAU_ARP.1	FPT_RVM.1	なし	なし	なし
FAU_SAA.1	FPT_RVM.1	なし	なし	なし

＜迂回防止＞

暗号鍵を生成する FSC_CKM.1 は、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に初めて電源が入れられた時に、必ず実行されるので迂回防止がサポートされる。

暗号鍵を配付する FCS_CKM.2 は、装置起動時に、検出すべき侵害が発生したことの判定処理が必ず起動され、侵害が検出されなければ、必ず実行されるので迂回防止がサポートされる。

セキュリティアラーム FAU_ARP.1 は、装置起動時に、通知すべきアラームが発生したことの判定処理が必ず起動され、該当する条件が存在する場合に必ず実行されるので、迂回防止がサポートされる。

侵害の可能性の分析する FAU_SAA.1 は、装置起動時に、検出すべき侵害が発生したことの判定処理が必ず起動され、該当する条件が存在する場合に必ず実行されるので、迂回防止がサポートされる。

＜非活性化防止＞

セキュリティ機能に対して、利用者の操作により機能が停止したり、そのふるまいを変更することができないため、非活性化防止について考慮する必要はない。

＜干渉防止＞

本 TOE に対する不正なサブジェクトが存在せず、干渉・改ざん防止について考慮する必要はない。

＜無効化防止＞

セキュリティ機能に対して、利用者の操作により機能が停止することができないため、無効化防止について考慮する必要はない。

8.2.4. TOE セキュリティ保証要件根拠

本 TOE は、セキュリティキットを搭載した場合に動作するオキカラーページプリンタ C8800 のファームウェア内のセキュリティモジュールである。また、脅威に対しては、暗号鍵生成、暗号鍵設定、セキュリティキット識別、環境のセキュリティ方針の OE.KIT による暗号化という簡単なメカニズムの組合せで対抗することができる。このため本 TOE は、商用として十分である EAL3 を品質保証レベルとする。

8.2.5. 最小機能強度根拠

本 TOE は、攻撃者のレベルとして低レベルを想定したセキュリティ対策方針を規定しており、最小機能強度として SOF-基本の選択は妥当である。また、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。従って一貫している。

8.2.6. IT セキュリティ機能要件セットの内部一貫性

競合する機能要件が選択されておらず、内部的に一貫している。

8.3. TOE 要約仕様根拠

本節は、IT セキュリティ要件に対して、TOE セキュリティ機能とその保証手段の有効性について検証する。

8.3.1. TOE セキュリティ機能根拠

TOE セキュリティ機能要件に対する、TOE セキュリティ機能（TSF）の有効性を表 16 に示す。表 16 は、TOE セキュリティ機能要件と TOE セキュリティ機能の対応について、その根拠を記載している節番号を示したものである。

表 16 TOE セキュリティ機能要件と TOE セキュリティ機能

機能 機能要件	TSF_EKG 暗号鍵生成機能	TSF_EKS 暗号鍵設定機能	TSF_HDC セキュリティキット識別機能
FCS_CKM.1	8.3.1.1		
FCS_CKM.2		8.3.1.2	
FAU_ARP.1			8.3.1.3
FAU_SAA.1			8.3.1.4
FPT_RVM.1	8.3.1.5	8.3.1.5	8.3.1.5

8.3.1.1. FCS_CKM.1

FCS_CKM.1 は、セキュリティキットを装着して初めて電源が入れられた時と、利用者が操作パネルから暗号鍵生成操作を実行した時に、TSF_EKG が OKI PX 暗号鍵生成アルゴリズムにより暗号鍵を生成するため、満足される。

8.3.1.2. FCS_CKM.2

FCS_CKM.2 は、電源がＯＮされた時に、TSF_EKS が、TSF_EKG が生成した暗号鍵をオキカラーページプリンタ C8800 内の Flash メモリから読み出しセキュリティキットに設定するため､満足される。

8.3.1.3. FAU_ARP.1

FAU_ARP.1 は、TSF_HDC がセキュリティキットに不正な状態を検出した時に、サービスコールを表示する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 の動作を停止するため、満足される。

8.3.1.4. FAU_SAA.1

FAU_SAA.1 は、セキュリティキットが一旦装着された以降に、TSF_HDC がセキュリティキットが取り外されているという不正な状態を検出するため、満足される。

8.3.1.5. FPT_RVM.1

FPT_RVM.1 は、TOE の各セキュリティ機能の動作進行が許可される前に、必ず TSP 実施機能が呼び出されることをサポートすることを規定している。
によるサポートが、各 TSF により実施されていることを以下に示す。
・TSF_EKG は、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に初めて電源が入れられた時、および利用者が操作パネルから暗号鍵生成操作を実行した時に、必ず FCS_CKM.1 が定める通り暗号鍵を生成する。
・TSF_EKS 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不正を検出しなかった場合は、必ず FCS_CKM. 2 が定める通り暗号鍵を設定する。
・TSF_HDC は、電源が入れられた時に、必ず FAU_SAA.1 が定める通りセキュリティキットが不正な状態かどうか検出する。不正な状態を検出した場合、TSF_HDC は、必ず FAU_ARP.1 が定める通り不正な状態に対応する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。
従って本機能要件は、満足される。

8.3.2. TOE 保証手段根拠

6.2 節の保証手段の有効性を検証する。表 11 に示すように、すべての TOE セキュリティ保証要件は、保証手段により示されたドキュメントにより対応付けられており、また保証手段に示されたドキュメントによって、本書が規定した TOE セキュリティ保証要件 EAL3 が要求している証拠に合致している。

8.3.3. TOE セキュリティ機能強度根拠

本 TOE の最小機能強度レベルは、SOF-基本であるが、本 TOE において、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がないという主張、および SOF 主張を実現すべき IT セキュリティ機能はないという主張で一貫している。