SHARP

MX-FR15

セキュリティターゲット

Version 0.04

シャープ株式会社

履歴

日付	Ver.	変更点	作成	確認	発行
2009/8/31	0.01	• 初版作成	中川	坂本	山口
2009/11/12	0.02	• 所見報告 ASE001-01 対応 • TOE概要の誤記訂正	中川	坂本	山口
2010/2/10	0.03	• 所見報告 ASE002-01 対応	中川	坂本	山口
2010/3/10	0.04	• TOE記述の不備を補完	中川	坂本	山口

© 2009–2010, シャープ株式会社 (Sharp Corp.), all rights reserved.

目次

© 2009–2010, シャープ株式会社 (Sharp Corp.), all rights reserved.

© 2009–2010, シャープ株式会社 (Sharp Corp.), all rights reserved.

表のリスト

図のリスト

© 2009–2010, シャープ株式会社 (Sharp Corp.), all rights reserved.

1 ST 概説

本章では、2.1 節に示すコモンクライテリア (CC) に基づき、本セキュリティターゲット (ST) および本 ST への適合を主張する CC 評価対象 (TOE) に関し、ST 参照、TOE 参照、TOE 概要、および TOE 記述を記載する。なお、本 ST では、8.1 節および 8.2 節に示す用語を使用している。

1.1 ST 参照

本セキュリティターゲット (ST) を識別するための情報を記載する。

名称: MX-FR15 セキュリティターゲット

バージョン: 0.04

発行日: 2010 年 3 月 10 日

作成者: シャープ株式会社

1.2 TOE 参照

本 ST への適合を主張する CC 評価対象 (TOE) を識別するための情報を記載する。

名称: MX-FR15

バージョン: C.10

開発者: シャープ株式会社

1.3 TOE 概要

1.3.1 TOE タイプ

TOE は MFD (デジタル複合機) 内データ保護機能を持つ IT 製品である。

TOE は MFD 用ファームウェアであり、ROM に格納されている。これは MFD の標準ファームウェアを置き換えることにより、セキュリティ機能を提供すると共に MFD 全体の制御を行う。

MFD (Multi Function Device) すなわちデジタル複合機は事務機であり、主としてコピー機能、プリンタ機能、スキャナ機能およびファクス機能を有する。

1.3.2 要求される TOE 以外のハードウェア/ソフトウェア/ファームウェア

TOE の動作には、シャープ製 MFD (ハードウェア) の一部機種が必要である。対象の機種は MX-M363U, MX-M363UJ, MX-M453U, MX-M453UJ, MX-M503U および MX-M503UJ である。

1.3.3 主要なセキュリティ機能

TOE セキュリティ機能は、主として以下に列挙する各機能からなり、TOE を搭載した MFD 内部のイメージデータを不正に取得する試みに対抗することを目的とする。

a) 暗号操作機能: MFD が扱うイメージデータを MFD 内の不揮発性メモリに書き込む前に暗号化する。

b) データ消去機能: MFD 内の MSD (揮発性メモリまたは Flash メモリ) に保存されたイメージデータの領域に対し、ランダム値または固定値を上書きする。

1.3.4 TOE の使用方法

標準ファームウェアと同様に、TOE は MFD 機能、すなわちコピー、プリンタ、スキャナ、ファクス送信、ファクス受信および PC-Fax の各機能を持つ。MFD 機能については後述するものとし、本節では前節のセキュリティ機能を呼び出す方法の概略を記す。

a) 利用者がコピー等の MFD 機能を利用することにより、TOE の暗号操作機能およびデータ消去機能が自動的に動作する。MFD はコピー等のジョブ処理中のイメージデータを MFD 内の MSD に一時的にスプール保存し、読み出しながらジョブを処理し、ジョブ完了時に削除する。TOE は暗号操作機能に

© 2009–2010, シャープ株式会社 (Sharp Corp.), all rights reserved.

より、不揮発性メモリ (Flash メモリ) にスプール保存されるイメージデータを暗号化し、読み出し時に復号する。TOE はデータ消去機能により、MSD から削除されるイメージデータを上書き消去する。

b) 管理者が必要 (MFD 廃棄時等) に応じ、MFD の操作パネルより、全データエリア消去の操作を行う。このとき TOE はデータ消去機能により、MFD 内のイメージデータをすべて上書き消去する。

1.3.5 MFD 機能の使用方法

TOE を設置する MFD の利用環境を図 1 に示す。

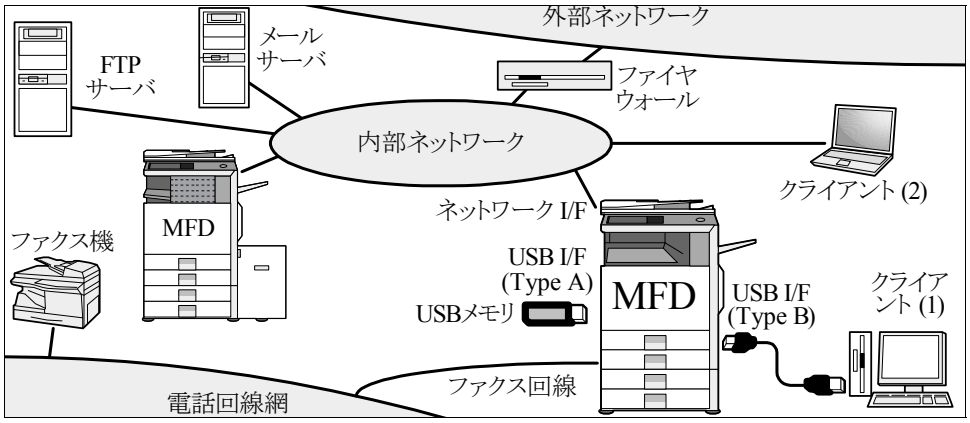

図 1: MFDの利用環境

以下、TOE が持つ MFD 機能について説明する。多くの機能は MFD の操作パネルでの操作によって発動する。一部の機能はデータ受信により発動する。

1.3.5.1 ジョブ機能

イメージデータを MFD のスキャナユニットまたは外部から受け取り、MFD 内の MSD にスプールし、イメージデータを MFD のエンジンユニット (印刷) または外部 (送信) へ送る。ジョブ制御機能および MFD 制御機能により実現される。

a) コピー: 操作パネルでの操作により、原稿を読み取り、その画像を印刷する。連結コピーが指示された場合、管理者が予め指定した MFD にイメージデータを送る。

b) プリンタ: 外部より受信したデータを印刷する。

- プリンタドライバ: クライアントで印刷データを生成し、ネットワークまたは USB 経由で MFD に送る。連結印刷が指示された場合、2 台の MFD にイメージデータを送る。
- プッシュプリント: クライアントより印刷データを E-mail, FTP または Web 経由で MFD に送る。MFD からの連結印刷要求も同様。
- プルプリント: 操作パネルの操作で FTP サーバまたは共有フォルダ内の印刷データを取得する。

c) スキャナ: 操作パネルでの操作により原稿を読み取り、原稿のイメージデータを以下の手段により送信する。

- E-mail: E-mail 添付ファイルとして送る。
- ファイルサーバ: FTP サーバに送る。
- デスクトップ: クライアント (MFD 同梱または別途提供ソフトウェア要) 宛に FTP で送る。
- 共有フォルダ: Windows 共有フォルダに送る。
- USB メモリ: MFD に取り付けた USB メモリに書き込む。

d) ファクス送信: 操作パネルでの操作により原稿を読み取り、原稿のイメージデータをファクス送信する。

e) ファクス受信: 他機から送られたファクスを受信し印刷する。

f) PC-Fax: クライアントからのデータをファクス送信する。

© 2009–2010, シャープ株式会社 (Sharp Corp.), all rights reserved.

1.4 TOE 記述

1.4.1 TOE の物理的構成

TOE の物理的範囲は、図 2 に網掛けで示すとおり、MFD のコントローラファームウェアである。これは 2 枚の ROM にて、シャープ製 MFD のセキュリティを強化するためのオプション製品 “データセキュリティキット MX-FR15” (DSK) として提供される。

- ROM: コントローラファームウェアを格納する。MFD に TOE を設置する際、コントローラ基板から標準ファームウェア ROM 2 枚を取り外し、代わりに DSK の ROM 2 枚を取り付ける。

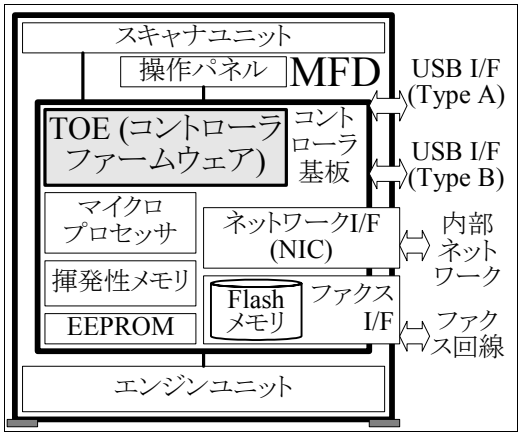

図 2: MFDの物理的構成とTOE

1.4.2 TOE の論理的構成

TOE の論理的構成を図 3 に示す。図中、TOE の論理的範囲を太い枠線内として示す。TOE 外のハードウェアを、角を丸くした長方形で示す。TOE の機能を長方形で示し、その中のセキュリティ機能を網掛けで示す。また、揮発性メモリ、Flash メモリおよび EEPROM 上にあるデータのうち、セキュリティ機能が扱うデータ (利用者データおよびTSF データ) を、同じく網掛けで示す。データの流れを矢印で示す。TOE の機能間で受け渡されるデータは、一時的に揮発性メモリを経由するが、セキュリティ機能上の意味を持つ場合を除いて省略している。

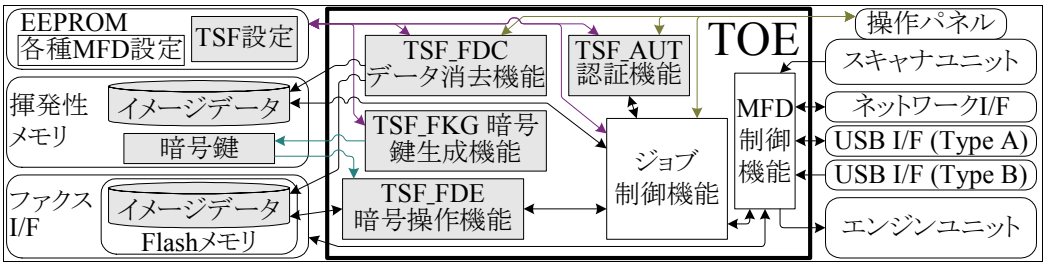

図 3: TOEの論理的構成図

TOE は MFD 用のファームウェアであり、セキュリティ機能を提供すると共に、MFD 全体の制御を行う。以下の機能が TOE の論理的範囲に含まれる。

a) 暗号操作機能 (TSF_FDE): Flash メモリに書き込むイメージデータを暗号化する。また、Flash メモリから読み出したイメージデータを復号する。ジョブ制御機能により、ジョブ処理の際に呼び出される。

b) 暗号鍵生成機能 (TSF_FKG): 暗号操作機能で使用する暗号鍵を生成する。生成された暗号鍵は、揮発性メモリに保存する。

c) データ消去機能 (TSF_FDC): MSD からの情報漏えいを防ぐため, MSD に対し上書き消去する。データ消去の各機能 (各ジョブ完了後の自動消去および全データエリア消去) からなる。各ジョブ完了後の自動消去は、ジョブ制御機能が呼び出すことにより、自動的に起動する。全データエリア消去は、管理者が操作することにより起動する。

d) 認証機能 (TSF_AUT): 管理者パスワードにより管理者の識別認証を行う。管理者パスワードを変更する管理機能を持つ。

e) ジョブ制御機能: MFD の各種ジョブのために、UI を提供し、動作を制御する。

f) MFD 制御機能: 各種 MFD ハードウェアを制御する。また、通信を伴うジョブにおいて、送受信するデータと MFD 内のイメージデータとの間でデータ形式を変換する。

1.4.3 ガイダンス

以下のガイダンスが、TOE の一部として、ファームウェアに同梱して提供される。文書およびバージョンを特定する一意識別子をブラケット [ ] と共に付す。

© 2009–2010, シャープ株式会社 (Sharp Corp.), all rights reserved.

- MX-FR15 Data Security Kit Operation Manual [CINSE4812FC51]
- MX-FR15 Data Security Kit Notice [CINSE4813FC51]

1.4.4 TOE の保護資産

本節では、TOE セキュリティ機能が保護対象とする資産について述べる。

1.4.4.1 保護資産の概要

利用者が TOE の MFD 機能を使用した場合、利用者が意図することなく TOE 自身が本章で述べた各種ジョブ処理のために、イメージデータが MFD 内の揮発性メモリ、もしくは Flash メモリに一時的にスプール保存される。ジョブ完了または中止の後に残存するイメージデータを、本 ST は保護資産とする。これは各利用者の機密情報、すなわち利用者自身が所有する情報や、利用者が顧客から預かっている情報を含み得る。

ジョブ完了または中止の際、MFD は資源の割当て解除のために上記のイメージデータを削除する。この削除とは、管理領域に削除情報を与えることによって、イメージデータ保持のために使用していた領域を、未使用状態にすることであり、一般のパーソナルコンピュータに接続されたハードディスク上のデータファイルを削除する場合と同様である。すなわち、未使用状態とされた領域が他のジョブにより再利用されるまでの間、削除されたイメージデータは残存し得る。

そこで本 ST は、MFD 内の揮発性メモリまたは Flash メモリに残存する削除済みイメージデータを保護資産に含める。TOE は、基本的な攻撃能力 (basic attack potential) を持つ攻撃者より、TOE の保護資産である残存するイメージデータからの情報漏えいを防止することを目的とする。

以下、各保護資産の具体的な内容を述べる。

1.4.4.2 Flash メモリに残存するイメージデータ

PC-Fax、ファクス送信、ファクス受信の各ジョブにおいて、ファクス送受信するイメージデータをスプール保存するために Flash メモリが使用される。ファクス送受信処理終了後または中止後のイメージデータは不揮発性の Flash メモリに残存するため、攻撃者が読み出し漏えいさせた場合、機密情報の漏えいとなり得る。また、組織のセキュリティ方針として、暗号化するか否か、読み出しの脅威があるか否かに関わらず、イメージデータの上書き消去を必須とする。従って、本 ST はこれを保護資産とする。

1.4.4.3 揮発性メモリに残存するイメージデータ

同様に、コピー、プリンタ、スキャナの各ジョブのイメージデータをスプール保存するために揮発性メモリが使用される。これらのジョブ終了後または中止後にイメージデータが揮発性メモリ内に残存しても、基本的な攻撃能力では読み出すことができず、攻撃の対象とはならない。ただし、上記のような組織のセキュリティ方針のため、本 ST は揮発性メモリに残存するイメージデータもまた保護資産とする。

1.4.5 TOE の関係者

本節では、本 TOE、及び、本 TOE を搭載する MFD の関係者について述べる。

- 所有者: TOE 及び MFD を占有し、管理下におく組織。
- 組織の責任者: 所有者に属し、MFD の管理責任を負う人物。
- 管理者: TOE 及び MFD の運用管理を任された人物。組織の責任者が任命する。
- 利用者: TOE 及び MFD の MFD 機能 (1.3.5 節) を使用する人物。

© 2009–2010, シャープ株式会社 (Sharp Corp.), all rights reserved.

2 適合主張

本 ST は以下を満たしている。

2.1 CC 適合主張

本 ST および TOE が適合を主張する CC のバージョンは次のとおり。

- パート 1: 概説と一般モデル
  2006 年 9 月 バージョン 3.1 改訂第 1 版 翻訳第 1.2 版
- パート 2: セキュリティ機能コンポーネント
  2007 年 9 月 バージョン 3.1 改訂第 2 版 翻訳第 2.0 版
- パート 3: セキュリティ保証コンポーネント
  2007 年 9 月 バージョン 3.1 改訂第 2 版 翻訳第 2.0 版

CC パート 2 に対する本 ST の適合は、CC パート 2 適合である。

CC パート 3 に対する本 ST の適合は、CC パート 3 適合である。

2.2 PP 主張

本 ST は PP 適合を主張しない。

2.3 パッケージ主張

本 ST は、保証要件パッケージ EAL3 適合である。

© 2009–2010, シャープ株式会社 (Sharp Corp.), all rights reserved.

3 セキュリティ課題定義

本章は、TOE のセキュリティ課題を定義する。

3.1 脅威

TOE に対する脅威を表 3.1 に示す。本 ST は、基本的な攻撃能力 (basic attack potential) を持つ攻撃者を想定している。表 3.1: 脅威

識別子	定義
T.RECOVER	攻撃者が、MFD内のFlashメモリを取り外して持ち出し、他の装置 (そのFlashメモリを搭載したMFD以外の装置) を接続することにより、Flashメモリ内に残存するイメージデータを読み出し漏えいさせる。

3.2 組織のセキュリティ方針

組織のセキュリティ方針を表 3.2 に示す。

表 3.2: 組織のセキュリティ方針

識別子	定義
P.RESIDUAL	ジョブ完了または中止時、MSDにスプール保存されたイメージデータの領域は、少なくとも1回上書き消去されなければならない。 MFDの廃棄または所有者変更の際、MSDのスプール領域はすべて、少なくとも1回上書き消去されなければならない。

3.3 前提条件

TOE の使用、運用時に、表 3.3 で詳述する環境が必要となる。

表 3.3: 前提条件

識別子	定義
A.OPERATOR	管理者は、TOEに対して不正をせず信頼できるものとする。

© 2009–2010, シャープ株式会社 (Sharp Corp.), all rights reserved.

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 4.1 に示す。

表 4.1: TOE のセキュリティ対策方針

識別子	定義
O.MANAGE	TOEは、正当な管理者を識別認証する機能を提供する。
O.REMOVE	TOEが組み込まれているMFDのFlashメモリに対し、スプール保存を実行したMFD自身以外から読み取られても、イメージとして表示不能なように、MFD固有の暗号鍵で実イメージデータを暗号化してから、Flashメモリにスプール保存する。
O.RESIDUAL	TOEは、ジョブ完了または中止時、MSDにスプール保存された利用者データの領域を、少なくとも1回上書き消去する。 TOEは、管理者の操作により、MSDのスプール領域全体を少なくとも1回上書き消去する機能を提供する。

4.2 運用環境のセキュリティ対策方針

運用環境のセキュリティ対策方針を表 4.2 に示す。

表 4.2: 環境のセキュリティ対策方針

識別子	定義
OE.ERASEALL	管理者は、MFDの廃棄または所有者変更の際、TOEの機能を用いて、MSDのスプール領域全体を少なくとも1回上書き消去する。
OE.OPERATE	組織の責任者は、管理者の役割を理解した上で、管理者の人選は厳重に行う。

4.3 セキュリティ対策方針根拠

セキュリティ課題定義に示した脅威、組織のセキュリティ方針、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 4.3 に検証する。表 4.3 は、脅威、組織のセキュリティ方針、前提条件の対応について、その根拠を記載している節番号を示したものである。

表 4.3: セキュリティ対策方針根拠

セキュリティ課題 セキュリティ対策方針	T.RECOVER	P.RESIDUAL	A.OPERATOR
O.MANAGE		4.3.2	
O.REMOVE	4.3.1		
O.RESIDUAL		4.3.2	
OE.ERASEALL		4.3.2	
OE.OPERATE			4.3.3

表 4.3 によれば、セキュリティ対策方針が達成された場合に、すべての脅威に対抗でき、すべての組織のセキュリティ方針を実施でき、かつ、前提条件をすべて満たす。以下、各々の根拠を具体的に示す。

4.3.1 T.RECOVER

T.RECOVER に対し、TOE はジョブのイメージデータを Flash メモリにスプール保存する際、O.REMOVE が定める通り MFD 固有の鍵により暗号化する。これにより、基本的な攻撃能力を持つ攻撃者が、Flash メモリよりイメージデータを読み出すことができたとしても、意味のあるものとして判読できない。

© 2009–2010, シャープ株式会社 (Sharp Corp.), all rights reserved.

なお、イメージデータを暗号化するための暗号鍵は、基本的な攻撃能力を持つ攻撃者に読み出されないよう扱う必要があり、MFD のメモリ (揮発性メモリ) に保存する。これにより、Flash メモリ内に残存するイメージデータからの情報漏えいが防止できる。

MFD 内の暗号鍵およびイメージデータが読み出される可能性について、以下に補足する。

- MFD 内のメモリを取り外して持ち出せば、メモリへの通電が遮断される。通電を遮断すれば、揮発性メモリ内のデータは消失し、Flash メモリ内のデータは消失しない。
- 稼動中の MFD からメモリ上のデータを直接に読み出すためのインタフェースは存在しない。MFD の端子や配線などに直接プローブを当ててデータを読み出すにはデータ領域や転送中データの特定などの高度な技術力を必要とするため、基本的な攻撃能力を持つ攻撃者の技術能力では不可能である。

よって、基本的な攻撃能力を持つ攻撃者が MFD 内のメモリからデータを読み出す可能性に関し、Flash メモリを取り外して持ち出す攻撃方法のみを、本 ST は脅威と考える。

4.3.2 P.RESIDUAL

P.RESIDUAL は、以下の対策により実施できる。

- O.RESIDUAL が定める通り、TOE は、ジョブ完了または中止時、MSD にスプール保存された利用者データの領域を、少なくとも 1 回上書き消去する。
- OE.ERASEALL が定める通り、管理者は、MFD の廃棄または所有者変更の際、MSD のスプール領域全体を少なくとも 1 回上書き消去する。そのためには TOE の支援が必要であり、次項の機能が利用できる。
- O.RESIDUAL が定める通り、TOE は、管理者の操作により MSD のスプール領域全体を少なくとも 1 回上書き消去する機能を提供する。
- 前項のサポートとして、O.MANAGE が定める通り、TOE はその運用に必要な設定を行う管理者を識別認証する機能を提供する。

これらの対策により、P.RESIDUAL は実施可能である。

4.3.3 A.OPERATOR

A.OPERATOR は、管理者が信頼できることを求めており、OE.OPERATE は、TOE を搭載した MFD を所有する組織の責任者が、管理者の役割を理解した上で、管理者の人選は厳重に行うことにより実施できる。

© 2009–2010, シャープ株式会社 (Sharp Corp.), all rights reserved.

5 拡張コンポーネント定義

本 ST は拡張コンポーネントを定義しない。

© 2009–2010, シャープ株式会社 (Sharp Corp.), all rights reserved.

6 セキュリティ要件

本章は、セキュリティ要件を記述する。

6.1 要件操作

本節では CC 機能および保証コンポーネントに対する操作の識別を定義する。

- 繰返し (iteration) 操作は、同一の要件の異なる側面をカバーするために使われる。
  - 本 ST では使用していない。
- 割付 (assignment) 操作は、コンポーネントにおいて、例えばパスワードの長さのような不確定のパラメータに特定の値を割り付けるために使われる。
  - パラメータに割り付ける値を、ブラケット [ ] 内に示す。値またはその一部としてリストを示す場合、要素間の切れ目は、コンマで区切るか、または、箇条書きスタイルによって示す。
  - パラメータ名のような、値を識別する情報を、必要に応じ丸括弧 ( ) に入れて値に付記する。
- 選択 (selection) 操作は、コンポーネントにおいて与えられた複数の項目から、一つあるいはそれ以上の項目を選択するために使用される。
  - 選択された項目を、斜体のブラケット *[ ]* 内に *[下線付き斜体]* で示す。
- 詳細化 (refinement) 操作は、コンポーネントに対する詳細付加のために使用され, TOE をさらに限定する。
  - 追加のテキストは **太字** で示す。
  - 元のテキストを削除する場合、削除するテキストを丸括弧 ( ) に入れる。
  - 元のテキストを新しいテキストで置き換える場合、置き換えられる元のテキストを丸括弧 ( ) に入れ、新しいテキストをその直前に **太字** で示す。
- *単純な斜体 (italic)* は要件操作を表すものでなく、本 ST 全体を通じて、単にテキストを強調するために使用されているに過ぎない。

6.2 セキュリティ機能要件

本節では TOE が満たすべきセキュリティ機能要件を CC パート 2 のクラス別に記述する。

6.2.1 クラス FCS: 暗号サポート

FCS_CKM.1 暗号鍵生成

下位階層: なし

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

FCS_CKM.1.1 TSF は、以下の[データセキュリティキット用暗号基準書]に合致する、指定された暗号鍵生成アルゴリズム[MSN-R2 拡張アルゴリズム]と指定された暗号鍵長[128 ビット]に従って、暗号鍵を生成しなければならない。

FCS_COP.1 暗号操作

下位階層: なし

依存性: [FDP_ITC.1 セキュリティ属性なし利用者データのインポート、または
FDP_ITC.2 セキュリティ属性を伴う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

FCS_COP.1.1 TSF は、[FIPS PUB 197]に合致する、特定された暗号アルゴリズム[AES Rijndael アルゴリズム]と暗号鍵長[128 ビット]に従って、[

© 2009–2010, シャープ株式会社 (Sharp Corp.), all rights reserved.

● Flash メモリに書き込む利用者データの暗号化
● Flash メモリから読み出した利用者データの復号
]を実行しなければならない。

6.2.2 クラス FDP: 利用者データ保護

FDP _RIP.1 サブセット残存情報保護

下位階層: なし

依存性: なし

FDP_RIP.1.1 TSF は、[MSD 内にスプール保存されるイメージデータファイル]のオブジェクト*[からの資源の割当て解除]* において、資源の以前のどの情報の内容も **少なくとも 1 回上書き消去することにより** 利用できなくすることを保証しなければならない。

6.2.3 クラス FIA: 識別と認証

FIA_AFL.1 認証失敗時の取り扱い

下位階層: なし

依存性: FIA_UAU.1 認証のタイミング

FIA_AFL.1.1 TSF は、[管理者認証操作における最後の認証成功以降の不成功認証試行]に関して、*[* [3 (*正の整数値*)] *]* 回の不成功認証試行が生じたときを検出しなければならない。

FIA_AFL.1.2 不成功の認証試行が定義した回数*[に達する]* とき、TSF は、[
● 不成功認証が 3 回に達するとき: 5 分間の認証試行受付を停止
● 停止より 5 分経過: 認証失敗回数をクリアし自動的に復帰
]をしなければならない。

FIA_SOS.1 秘密の検証

下位階層: なし

依存性: なし

FIA_SOS.1.1 TSF は、 **管理者パスワード** (秘密) が[5 文字以上 32 文字以下の英数記号、すなわち ISO/IEC 646 情報交換用符号化文字集合における 32 番から 126 番まで 95 種の文字] に合致することを検証するメカニズムを提供しなければならない。

FIA_UAU.2 アクション前の利用者認証

下位階層: FIA_UAU.1 認証のタイミング

依存性: FIA_UID.1 識別のタイミング

FIA_UAU.2.1 TSF は、その **管理者** (利用者) を代行する他の TSF 仲介アクションを許可する前に、各 **管理者** (利用者) に認証が成功することを要求しなければならない。

FIA_UAU.7 保護された認証フィードバック

下位階層: なし

依存性: FIA_UAU.1 認証のタイミング

FIA_UAU.7.1 TSF は、 **管理者の** 認証を行っている間、[入力された文字の個数]だけを **管理者** (利用者) に提供しなければならない。

FIA_UID.2 アクション前の利用者識別

下位階層: FIA_UID.1 識別のタイミング

依存性: なし

© 2009–2010, シャープ株式会社 (Sharp Corp.), all rights reserved.

FIA_UID.2.1 TSF は、その **管理者** (利用者) を代行する他の TSF 仲介アクションを許可する前に、各 **管理者** (利用者) に識別が成功することを要求しなければならない。

6.2.4 クラス FMT: セキュリティ管理

FMT_MOF.1 セキュリティ機能のふるまいの管理

下位階層: なし

依存性: FMT_SMF.1 管理機能の特定
FMT_SMR.1 セキュリティの役割

FMT_MOF.1.1 TSF は、機能[全データエリア消去] *[を動作させる, を停止する]* 能力を[管理者]に制限しなければならない。

FMT_MTD.1 TSF データの管理

下位階層: なし

依存性: FMT_SMF.1 管理機能の特定
FMT_SMR.1 セキュリティの役割

FMT_MTD.1.1 TSF は、[管理者パスワード]を*[改変]* する能力を[管理者]に制限しなければならない。

FMT_SMF.1 管理機能の特定

下位階層: なし

依存性: なし。

FMT_SMF.1.1 TSF は、以下の管理機能を実行することができなければならない。: [

- 全データエリア消去の起動および中止
- 管理者パスワードの改変

]

注: 管理要件への考慮は 6.4.1.5 *節で述べる。*

FMT_SMR.1 セキュリティの役割

下位階層: なし

依存性: FIA_UID.1 識別のタイミング

FMT_SMR.1.1 TSF は、役割[管理者]を維持しなければならない。

FMT_SMR.1.2 TSF は、利用者を役割に関連づけなければならない。

6.3 セキュリティ保証要件

以下、本 ST が主張する EAL3 適合のセキュリティ保証要件を、CC パート 3 の保証クラス別に示す。本 ST は、CC パート 3 に定義のあるセキュリティ保証コンポーネントを、そのままセキュリティ保証要件として使用する。

ADV クラス: 開発
ADV_ARC.1 セキュリティアーキテクチャ記述
ADV_FSP.3 完全な要約を伴う機能仕様
ADV_TDS.2 アーキテクチャ設計

AGD クラス: ガイダンス文書
AGD_OPE.1 利用者操作ガイダンス
AGD_PRE.1 準備手続き

ALC クラス: ライフサイクルサポート
ALC_CMC.3 許可の管理
ALC_CMS.3 実装表現の CM 範囲
ALC_DEL.1 配付手続き
ALC_DVS.1 セキュリティ手段の識別
ALC_LCD.1 開発者によるライフサイクルモデルの定義

© 2009–2010, シャープ株式会社 (Sharp Corp.), all rights reserved.

ASE クラス:	セキュリティターゲット評価
ASE_CCL.1	適合主張
ASE_ECD.1	拡張コンポーネント定義
ASE_INT.1	ST 概説
ASE_OBJ.2	セキュリティ対策方針
ASE_REQ.2	導き出されたセキュリティ要件
ASE_SPD.1	セキュリティ課題定義
ASE_TSS.1	TOE 要約仕様

ATE クラス:	テスト
ATE_COV.2	カバレージの分析
ATE_DPT.1	テスト: 基本設計
ATE_FUN.1	機能テスト
ATE_IND.2	独立テスト - サンプル
AVA クラス:	脆弱性評定
AVA_VAN.2	脆弱性分析

6.4 セキュリティ要件根拠

セキュリティ対策方針に対して、セキュリティ要件が有効であることを検証する。

6.4.1 セキュリティ機能要件根拠

セキュリティ機能要件とセキュリティ対策方針の対応について表 6.1 に示す。表 6.1 は、セキュリティ機能要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 6.1: セキュリティ機能要件根拠

対策方針 要件	O. MANAGE	O. REMOVE	O. RESIDUAL
FCS_CKM.1		6.4.1.2	
FCS_COP.1		6.4.1.2	
FDP_RIP.1			6.4.1.3
FIA_AFL.1	6.4.1.1		
FIA_SOS.1	6.4.1.1		
FIA_UAU.2	6.4.1.1		
FIA_UAU.7	6.4.1.1		
FIA_UID.2	6.4.1.1		
FMT_MOF.1			6.4.1.3
FMT_MTD.1	6.4.1.1		
FMT_SMF.1	6.4.1.1		6.4.1.3
FMT_SMR.1	6.4.1.1		

6.4.1.1 O.MANAGE

O.MANAGE は、以下の機能要件の組み合わせにより実現できる。

a) 管理者を FIA_UID.2 にて識別し, FIA_AFL.1, FIA_UAU.2 および FIA_UAU.7 にて認証する。

b) FMT_SMF.1 にて、TOE は、上記の管理者認証の運用に必要な、管理者パスワードの改変を行う能力を提供する。

c) FIA_SOS.1 により、管理者パスワードを改変する際、管理者パスワードが 5 文字以上 32 文字以下の英数記号であることが保証される。

d) FMT_MTD.1 にて、O.MANAGE を実施する TSF データである管理者パスワードを改変する能力は、管理者のみに制限される。

e) FMT_SMR.1 にて、管理者の役割は維持され、管理者はその役割に関連づけられる。

上記 a) は管理者識別認証の事象に関するものであり、b), c) および d) は管理者パスワード改変の事象に関するものである。これら二つの事象は独立に発生し、相互に競合しない。a) の四つの機能要件は、管理者識別認証を実施するために相互補完的に作用するので、競合は発生しない。b), c) および d) の三つの機能要件は、管理者パスワード改変を実施するために相互補完的に作用するので、競合は発生しない。e) は d) の依存性の要件であり a) にサポートされるので、競合は発生しない。以上から、O.MANAGE を実現する上で、機能要件の競合は発生しない。

6.4.1.2 O.REMOVE

O.REMOVE の目的は T.RECOVER への対抗であり、すなわち MFD 内の Flash メモリに対し、他の装置 (Flash メモリへのスプール保存を実行した MFD 自身以外) からアクセスされても、MSD 内の利用者データが再生されないようにすることである。これは、以下の機能要件の組み合わせにより実現できる。

- FCS_COP.1 により、Flash メモリにスプール保存するイメージデータが暗号化される。そのため、Flash メモリへの保存を実行した MFD 自身以外に Flash メモリを接続してイメージデータの再生を試みても、イメージデータの再生は阻止される。
- FCS_CKM.1 により、FCS_COP.1 を実施するための暗号鍵を生成する。

FCS_COP.1 および FCS_CKM.1 は相互依存である。よって、O.REMOVE を実現する上で、機能要件の競合は発生しない。

© 2009–2010, シャープ株式会社 (Sharp Corp.), all rights reserved.

6.4.1.3 O.RESIDUAL

O.RESIDUAL は、以下の機能要件の組み合わせにより実現できる。

- FDP_RIP.1 によって、オブジェクトからの資源の割当て解除において、それらの領域に対し少なくとも1回以上上書き消去する。対象となるオブジェクトは、揮発性メモリおよびFlashメモリ上のスプールイメージデータファイルである。資源の割当て解除が発生するのは、ジョブ完了または中止時、および、管理者の操作により全データエリア消去が実行されたときである。
- FMT_SMF.1 にて、FDP_RIP.1 に関する管理機能、すなわち全データエリア消去を起動および中止する機能を提供する。
- FMT_MOF.1 にて、FDP_RIP.1 に関する TSF のうち全データエリア消去を動作および停止させる能力が、管理者に制限される。

FMT_SMF.1 および FMT_MOF.1 は、相互補完的に FDP_RIP.1 の管理を規定するので、それらの間で競合はない。よって、O.RESIDUAL を実現する上で、機能要件の競合は発生しない。

6.4.1.4 セキュリティ機能要件全体の一貫性根拠

TOE のセキュリティ対策方針 O.REMOVE および O.RESIDUAL は相互に競合するものではなく、MFD 内部のイメージデータを不正に取得する試みに対し、各々独立に、かつ、相互補完的に対抗する。また、O.MANAGE は O.RESIDUAL をサポートする。

6.4.1.1 節から 6.4.1.3 に示すとおり、それぞれの TOE のセキュリティ対策方針を実現するセキュリティ機能要件の間には、競合は発生せず、一貫している。

以上から、TOE のセキュリティ対策方針を実現するセキュリティ機能要件全体においても、競合は発生せず、一貫している。

6.4.1.5 TOE セキュリティ管理機能の一貫性根拠

TOE セキュリティ機能要件のいくつかは、セキュリティ管理機能を必要とする。CC パート2は各機能コンポーネントに予見される管理アクティビティ (management activities foreseen) を、各コンポーネントの管理要件 (management requirements) として提案している。

表 6.2 は、すべての TOE セキュリティ機能要件コンポーネントについて、そのコンポーネントが必要とする管理機能を、管理要件への考慮とともに示す。FMT_SMF.1 が特定する管理機能と、表中で示された必要な管理機能とは、一致している。

よって、TOE セキュリティ機能要件は、セキュリティ管理機能に関し、内部的に一貫している。

表 6.2: TOE の管理機能

管理機能 被管理要件	必要な管理機能	管理要件への考慮
FCS_CKM.1	—	(管理要件なし)
FCS_COP.1	—	(管理要件なし)
FDP_RIP.1	• 全データエリア消去の起動および中止	残存情報保護の実施タイミングは、割当て解除時に固定
FIA_AFL.1	—	閾値とアクションは固定
FIA_SOS.1	—	品質尺度は固定
FIA_UAU.2	• 管理者パスワードの改変	管理要件に合致
FIA_UAU.7	—	(管理要件なし)
FIA_UID.2	—	管理者の識別は固定
FMT_MOF.1	—	役割のグループなし
FMT_MTD.1	—	役割のグループなし
FMT_SMF.1	—	(管理要件なし)
FMT_SMR.1	—	利用者のグループなし

6.4.1.6 セキュリティ機能要件の依存性根拠

表 6.3 は、CC が規定するセキュリティ機能要件が満足すべき依存性と、本 TOE が満足している依存性、満足していない依存性を示す。表中で # を付された依存性は、それの上位階層関係にあるコンポーネントにより満足されている。表 6.4 は、本 TOE が依存性を満足していないことの正当性を示す。これら二つの表は、共通の識別子 (J1 のような) により対応付けられる。

© 2009–2010, シャープ株式会社 (Sharp Corp.), all rights reserved.

表 6.3: 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	満足している	不満足	正当性
FCS_CKM.1	[FCS_CKM.2 or FCS_COP.1], FCS_CKM.4	FCS_COP.1	FCS_CKM.4	J1
FCS_COP.1	[FDP_ITC.1 or FCS_CKM.1], FCS_CKM.4	FCS_CKM.1	FCS_CKM.4	J1
FDP_RIP.1	—	—	—	—
FIA_AFL.1	FIA_UAU.1 #	FIA_UAU.2	—	—
FIA_SOS.1	—	—	—	—
FIA_UAU.2	FIA_UID.1 #	FIA_UID.2	—	—
FIA_UAU.7	FIA_UAU.1 #	FIA_UAU.2	—	—
FIA_UID.2	—	—	—	—
FMT_MOF.1	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1	—	—
FMT_MTD.1	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1	—	—
FMT_SMF.1	—	—	—	—
FMT_SMR.1	FIA_UID.1 #	FIA_UID.2	—	—

表 6.4: SFR 依存性不満足の正当性

	不満足	正当性の根拠
J1	FCS_CKM.4	暗号鍵は揮発性メモリ内に保持する。電源断 (電源オフ) により、揮発性メモリ内の電荷が消失し、暗号鍵が破棄される。そのため、標準の暗号鍵破棄方法を行うTSFを実装する必要がなく、標準を特定するFCS_CKM.4は不要。

6.4.2 セキュリティ保証要件根拠

本 TOE は、MFD 用の別売オプション品、すなわち商用の製品である。また、主要な脅威は、基本的な攻撃能力を持つ攻撃者が、MFD 内の Flash メモリに他の装置を接続する物理的手段により Flash メモリ内の情報を読み出し漏えいさせることである。このため本 TOE は、商用として十分である EAL3 を評価保証レベルとする。

保証要件は EAL3 適合であるので、すべての保証要件は依存性を満たす。

© 2009–2010, シャープ株式会社 (Sharp Corp.), all rights reserved.

7 TOE 要約仕様

本章は、TOE セキュリティ機能 (TSF) の要約仕様を記述することにより、セキュリティ機能要件が満たされることを示す。セキュリティ機能要件と TOE セキュリティ機能の関連性を表 7.1 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 7.1: 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_FKG	TSF_FDE	TSF_FDC	TSF_AUT
FCS_CKM.1	7.1			
FCS_COP.1		7.2		
FDP_RIP.1			7.3	
FIA_AFL.1			7.3	7.4
FIA_SOS.1				7.4
FIA_UAU.2			7.3	7.4
FIA_UAU.7			7.3	7.4
FIA_UID.2			7.3	7.4
FMT_MOF.1			7.3	
FMT_MTD.1				7.4
FMT_SMF.1			7.3	7.4
FMT_SMR.1				7.4

7.1 暗号鍵生成 (TSF_FKG)

本 TOE は、暗号鍵 (共通鍵) の生成を行い、次節で述べる暗号操作 (TSF_FDE) 機能をサポートする。MFD の電源がオンになると、必ず暗号鍵 (共通鍵) を生成する。

TOE は、MSN-R2 拡張アルゴリズムを用いて 128 ビット長のセキュアな鍵を生成し、暗号アルゴリズム AES Rijndael で使用するために、揮発性メモリ内に保存する。MSN-R2 拡張アルゴリズムは、データセキュリティキット用暗号基準書を満たす暗号鍵生成アルゴリズムである。

よって、本 TOE は FCS_CKM.1 を満たす。

7.2 暗号操作 (TSF_FDE)

ジョブ処理の途上において、ジョブのイメージデータを Flash メモリに書き込む必要が生じたときは、必ずそれらのデータを暗号化してから書き込む。また、それらのデータが必要になれば、Flash メモリから読み出し、復号して利用する。

上記 Flash メモリ上のイメージデータの暗号化および復号には、FIPS PUBS 197 に基づく AES Rijndael アルゴリズム、および、暗号鍵生成 (TSF_FKG) により生成された 128 ビット長の暗号鍵を用いる。

よって、本 TOE は FCS_COP.1 を満たす。

7.3 データ消去 (TSF_FDC)

以下、まず本 TSF の概要を述べ、続いて各構成要素を順に説明する。

7.3.1 データ消去の概要

本 TSF の全体像、および、SFR との対応を記述する。

本 TSF はスプール保存されたイメージデータを消去する。以下の各機能は本 TSF に含まれる。

a) 各ジョブ完了後の自動消去

b) 全データエリア消去

上記の各機能が本 TSF を構成し、以下のとおり SFR に対応する。

- 各機能とも揮発性メモリにはランダム値を 1 回以上上書きする。また, Flash メモリには固定値を 1 回上書きする。各機能は割り当て解除されるオブジェクト (イメージデータファイル) を上書き消去することにより、当該オブジェクトに保存されていた情報 (イメージデータ) の再生を不能とする。よって本 TOE は FDP_RIP.1 を満たす。
- 本 TSF は FMT_SMF.1 および FMT_MOF.1 に従い、上記 b) の起動を、TSF_AUT で識別認証された管理者に許す。
- 上記 b) は FMT_SMF.1 に従って停止できるよう中止機能 (7.3.3 節) を持ち、後述の TSF_AUT と共同で FIA_AFL.1, FIA_UAU.2, FIA_UAU.7 および FIA_UID.2 を満たす。中止機能は FIA_UID.2 および FIA_UAU.2 に従い管理者識別認証を要求する。認証の際 FIA_UAU.7 のフィードバック保護お

© 2009–2010, シャープ株式会社 (Sharp Corp.), all rights reserved.

よび FIA_AFL.1 の失敗対応を行う。これにより、FMT_MOF.1 が定めるとおり管理者のみが消去を途中で停止できる。

次節以降、各機能について記述する。

7.3.2 各ジョブ完了後の自動消去

本機能は、ジョブ処理のために揮発性メモリまたは Flash メモリにスプール保存されたイメージデータを、当該ジョブ完了時に上書き消去する。TOE は本機能を所定のタイミングで必ず起動し、非活性化する手段を提供しない。

7.3.3 全データエリア消去

本機能は、TSF_AUT で識別認証された管理者により操作パネルにて起動され、揮発性メモリまたは Flash メモリにスプール保存されたすべてのイメージデータを上書き消去する。

本機能は中止機能を持つ。本機能を途中で中止する場合、キャンセル操作を選択後、本 TSF は本機能を起動した管理者のパスワード入力を必ず要求する。キャンセル操作は FIA_UID.2 が定める管理者識別であり、管理者パスワード入力は FIA_UAU.2 が定める管理者認証である。

認証入力中, TOE は FIA_UAU.7 に従い、入力した文字と同数のアスタリスク (星型記号) を表示するが、入力した文字は表示しない。正しい入力が完了した場合のみ、上書き消去を中止する。

中止機能の認証入力において、FIA_AFL.1 が定めるとおり、連続して 3 回認証に失敗した場合、認証受付を停止、すなわち管理者パスワードをロックする。ロックからの経過時間が 5 分に達すれば、自動的にロックを解除、すなわち、認証失敗回数をクリアしてロック状態から復帰する。

7.4 認証 (TSF_AUT)

本 TSF は、管理者パスワードにより管理者の識別認証を行う。本 TSF は FMT_SMF.1 および FMT_MTD.1 に従い、管理者パスワードの変更を、本 TSF で識別認証された管理者のみに許す。このとき、FIA_SOS.1 に従い、長さ 5 文字以上 32 文字以下で、ISO/IEC 646 情報交換用符号化文字集合における 32 番から 126 番まで 95 種の文字から成るパスワードのみを受け入れる。各文字の字形は実行環境により異なるが、例えば次のとおり。

- 英字 52 種: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z a b c d e f g h i j k l m n o p q r s t u v w x y z
- 数字 10 種: 0 1 2 3 4 5 6 7 8 9
- 記号 33 種: ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [¥] ^ _ ` { | } ~ および空白。

管理者向け以外の機能は、管理者識別認証を経ることなく利用できる。

本 TSF は、TSF_FDC と共同で FIA_AFL.1, FIA_UAU.2, FIA_UAU.7 および FIA_UID.2 を満たす。

FIA_UID.2 に従い、管理機能の起動操作によって管理者を識別し、かつ、FIA_UAU.2 に従い、正しい管理者パスワードによって管理者認証に成功した場合に限り、管理者向け機能へのインタフェースを提供する。

操作パネルでの管理者パスワード入力時、FIA_UAU.7 に従い、入力した文字と同数のアスタリスク (星型記号) を表示するが、入力した文字は表示しない。

管理者パスワード認証において、連続して 3 回認証に失敗した場合、FIA_AFL.1 に従い、認証受付を停止、すなわち管理者パスワードをロックする。ロックからの経過時間が 5 分に達すれば、自動的にロックを解除、すなわち、認証失敗回数をクリアしてロック状態から復帰する。

本 TSF は管理者識別認証により、管理者を特定し、役割に関連づける。また、管理者のみに管理者パスワードの変更 (改変) 機能を提供することにより、役割の維持管理を図る。これらにより TOE は FMT_SMR.1 を満たす。

© 2009–2010, シャープ株式会社 (Sharp Corp.), all rights reserved.

8 付章

本章では、用語の定義を示す。

8.1 専門用語

本 ST で使用している専門用語を表 8.1 に示す。

表 8.1: 専門用語

用語	定義
Flashメモリ	不揮発性メモリの一種で、電気的な一括消去および任意部分の再書き込みを可能にしたROM (Flash Memory)。
MSN-R2拡張アルゴリズム	データセキュリティキット用暗号基準書に規定されている、シャープ株式会社独自の暗号鍵生成アルゴリズム。
イメージデータ	本書では特に、MFDの各機能が扱う二次元画像のデジタルデータを指す。
エンジン	給紙機能、排紙機能の機構を含み、受像紙に印刷画像を形成する装置。プリントエンジン、エンジンユニットともいう。
各ジョブ完了後の自動消去	MFD内のMSDに保存された、個々のジョブに対応するイメージデータを上書き消去するための機能。ジョブ完了または中止時に呼び出される。
管理者パスワード	セキュリティ管理機能等、TOE及びMFDの運用管理において重要な管理者専用の機能を、管理者以外に使用されないよう、保護するためのパスワード。
揮発性メモリ	電源を切れば記憶内容が消失する記憶装置。
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。
コントローラ基板	MFD全体を制御する基板。TOEのファームウェアを実行するためのマイクロプロセッサ、揮発性メモリ等を有する。
コントローラファームウェア	MFDのコントローラ基板を制御するファームウェア。ROM基板に格納してコントローラ基板に搭載する。
ジョブ	MFDのコピー、プリンタ、スキャナ、ファクス送受信およびPC-Faxの各機能において、その機能の開始から終了までの流れ、シーケンス。また、機能動作の指示についてもジョブと呼ぶ場合がある。
スキャナユニット	原稿をスキャンしてイメージデータを得る装置。コピー、スキャナおよびファクス送信の際に使用する。
スプール	入出力効率のため、ジョブのイメージデータを一時的にMSDに保持すること。
全データエリア消去	MFD内のMSD上にあるすべてのイメージデータを上書き消去するための機能。管理者の操作により呼び出される。
操作パネル	MFDの正面にあるUI用ユニット。スタートキー、数字キー、機能キーおよびタッチ操作式の液晶ディスプレイを含む。
データセキュリティキット用暗号基準書	MFD用のデータセキュリティキットに用いる暗号操作アルゴリズム、および暗号操作に用いる暗号鍵の生成に関しての標準を規定した、シャープ株式会社内の文書。
データファイル	本書では、割り当てられたMSD資源からなり、情報 (イメージデータ等) を格納するオブジェクトを指す。
標準ファームウェア	TOE設置前のMFDに搭載されているコントローラファームウェア。TOEはコントローラファームウェアを含んでおり、TOE設置時に標準ファームウェアはTOEのコントローラファームウェアに置き換えられる。
ファームウェア	機器のハードウェアを制御するために、機器に組み込まれたソフトウェア。本書では特に、コントローラファームウェアを指す。
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記憶装置。
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。
連結印刷	大量の印刷部数を、2台のMFDで折半することにより倍速でこなす機能。
連結コピー	MFDのコピー機能における連結印刷のこと。
ロック	誤ったパスワードが連続して入力されたとき、パスワードの受付を停止する機能。

© 2009–2010, シャープ株式会社 (Sharp Corp.), all rights reserved.

8.2 略語

本 ST で使用している略語を表 8.2 および表 8.3 に示す。

表 8.2: CC の略語

略語	定義
CC	Common Criteria (コモンクライテリア)
EAL	Evaluation Assurance Level (評価保証レベル)
PP	Protection Profile (プロテクションプロファイル)
ST	Security Target (セキュリティターゲット)
TOE	Target of Evaluation (評価対象)
TSF	TOE Security Functionality (TOEセキュリティ機能)

表 8.3: 他の略語

略語	定義
AES	Advanced Encryption Standard — 米国の商務省標準技術局 (NIST) が制定した米国政府標準暗号。
DSK	データセキュリティキットMX-FR15 — TOEの提供形態であり、MFDの別売オプション品。
EEPROM	Electronically Erasable Programmable ROM — 不揮発性メモリの一種で、低頻度であれば電気的に任意部分の書き換えを可能にしたROM。
I/F	Interface (インタフェース)
IP	Internet Protocol — インターネットプロトコル。データを複数のパケットに分割し、宛先へ届ける通信プロトコルの名称。
IT	Information Technology (情報技術)
MFD	Multi Function Device — デジタル複合機。事務機であり、主としてコピー機能、プリンタ機能、スキャナ機能およびファクス機能を有する。本書では、1.3.2節で識別する対象機種を指す。
MSD	Mass Storage Device — 大容量ストレージ装置。本STでは特にMFD内の、揮発性メモリの一部、および、Flashメモリを指す。
NIC	Network Interface Card (ネットワークインタフェースカード) — または — Network Interface Controller (ネットワークインタフェースコントローラ)
OS	Operating System (オペレーティングシステム)
PC	Personal Computer (パーソナルコンピュータ)
ROM	Read Only Memory — 読み出し専用メモリ。
UI	User Interface (ユーザーインタフェース)
USB	Universal Serial Bus — IT機器間を接続するシリアルバス標準の名称。
SMTP	Simple Mail Transfer Protocol — E-mail転送用通信プロトコルの名称。

© 2009–2010, シャープ株式会社 (Sharp Corp.), all rights reserved.