TOSHIBA

e-STUDIO2330c/2820c/2830c/3520c/3530c/4520c用

Security Target

2008年11月17日
Ver 2.0

東芝テック株式会社

目次

用語，略語 3
- 資産の専門用語 3
- TOE 関連の用語/略語 3
- CC 関連の略語 4
- 商標 4

1. ST 概説 5
1.1 ST 参照 5
1.2 TOE 参照 5
1.3 TOE 概要 5
1.3.1 TOE の説明 5
1.3.2 TOE の使用方法 6
1.3.3 TOE 以外で必要なハードウェア、ソフトウェア及びファームウェア 7
1.3.4 TOE の関係者 7
1.3.5 保護資産 8
1.4 TOE 記述 8
1.4.1 TOE の物理的範囲 8
1.4.1.1 通常モード時の構成 9
1.4.1.2 自己診断モード時の構成 10
1.4.2 TOE の論理的範囲 11
1.4.2.1 通常モード時の e-STUDIO 一般機能 11
1.4.2.2 通常モード時のセキュリティ機能（データ消去機能） 13
1.4.2.3 自己診断モード時の保守用の設定/機器情報の表示処理 14
1.4.2.4 自己診断モード時のセキュリティ機能 14
1.4.3 TOE を構成するガイダンスの識別 14

2. 適合主張 15
2.1 CC 適合主張 15
2.2 PP 主張、パッケージ主張 15
2.3 適合根拠 15

3. セキュリティ課題定義 16
3.1 脅威 16
3.2 組織のセキュリティ方針 16
3.3 前提条件 16

4. セキュリティ対策方針 17
4.1 TOE のセキュリティ対策方針 17
4.2 運用環境のセキュリティ対策方針 17
4.3 セキュリティ対策方針根拠 18

5. 拡張コンポーネント定義 19

6. セキュリティ要件 20
6.1 TOE セキュリティ機能要件 20
6.2 TOE セキュリティ保証要件 20
6.3 セキュリティ要件根拠 21
6.3.1 セキュリティ機能要件根拠 21
6.3.2 セキュリティ保証要件根拠 21

7. TOE 要約仕様 22
7.1 データ消去機能 22
7.2 上書き消去強制実行処理 22

用語，略語

本 ST で使用している用語，略語，商標は、以下の通りである。

・ **資産の専門用語**

ユーザ文書	いわゆる Word 文書、Excel 文書、PDF 文書、テキスト文書、JPEG 画像など利用者が保有する文書を指す。
ユーザ文書データ	MFP 内に存在する電子化された状態のユーザ文書を指す。スキャナにて電子化され取り込まれたユーザ文書や、MFP が受信した電子化されているユーザ文書や、それらを MFP 内にて加工したデータ。
資源	TOE を包括する物理的なコンポーネントや内蔵しているフォントなどのデジタルコンポーネント、そしてトナーなどの TOE のための消耗品。

・ **TOE 関連の用語/略語**

MFP (Multi Function Peripherals)	デジタル複合機。主に、コピー，スキャン，プリンタ，ファックスの機能を 1 台に集約した多機能周辺機器。
e-STUDIO	MFP（Multi Function Peripherals） デジタル複合機。主に、コピー，スキャン，プリンタ，ファックスの機能を 1 台に集約した多機能周辺機器。本 ST では、e-STUDIO2330C/2820C/2830C/3520C/3530C/4520C を指す。
e-STUDIO 一般機能	e-STUDIO に実装されている機能の内、一般の利用者が利用可能な、コピー，スキャン，プリント，ファクス，ファイリングボックス/共有フォルダ機能を指す。
ジョブ	e-STUDIO 一般機能の処理が行われる単位。ジョブ中又はジョブ終了時(キャンセル含む)に処理の為一時的に HDD に記録されたユーザ文書データは TSF により完全消去が行われる。
TopAccess	Webベースのジョブ、およびデバイスの管理ツール このツールを使用すると、インターネットを介して e-STUDIO の情報を取得することができ、ユーザ用、および管理者用の 2 種類の Web サイトを使用することができる。
ファイリングボックス	利用者が、ユーザ文書データの保存を行う場所。 保存後、操作パネルや TopAceess より、データの参照，印刷，編集が行える。ファイル保存の有効期限が過ぎると、保存されているユーザ文書データは削除される。
共有フォルダ	ユーザ文書データを JPEG や PDF といったファイル形式で保存し、ネットワーク上のクライアント PC よりファイルの取得が行える場所。ファイル保存の有効期限が過ぎると、保存されているユーザ文書データは削除される。
インターネットファクス	LAN 回線を使用して、原稿を TIFF-FX（Profile S）形式の添付ファイルで E メールとして通信を行う。利点としては、通信費の節約や通常のファクスよりも高い解像度が挙げられる。 対応機種どうしのインターネットファクス送受信の他、PC から対応機種へと、ドキュメントや画像をインターネットファクスとして送信できる。また、対応機種から PC に送信した場合、PC 側はメールとして受信できる。 本機はインターネットファクスを受信すると、通常のファクスと同様に自動的に出力を行う。
WS スキャン	WS（Web Service）スキャンは、Windows Vista コンピュータに搭載される機能を利用し、ネットワークを介したコンピュータとのスキャン操作を行う機能。本機でスキャンを行った画像のコンピュータへの保存や、コンピュータの WIA (Windows Imaging Acquisition)Scan Driver 対応アプリケーションから本機にスキャン要求を行っての画像取得ができる。
削除	資源の割り当てを解除し、ユーザにとって使用不可能な状態にす

	ること。
消去	痕跡を残さずに消し去ること。
完全消去	削除するデータの領域に対し無意味なデータの上書を行い、ユーザ文書データが再利用できないよう、完全に消去を行う。
GP-1070、GP-1090	e-STUDIO2330C/2820C/2830C/3520C/3530C/4520C へ接続してセキュリティのライセンス登録を行う機器。ライセンス登録されることでシステムソフトウェア内のセキュリティ機能が有効になる。

・ **CC 関連の略語**

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
SOF　(Strength Of Function)	機能強度
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 Function)	TOE セキュリティ機能
SFR　(Security Functional Requirement)	セキュリティ機能要件

・ **商標**

- VxWorks は、Wind River Systems,Inc.の登録商標または商標です。
- Windows Vista の正式名称は、Microsoft Windows Vista Operating System です。
- Microsoft、Windows、Windows NT、またはその他のマイクロソフト製品の名称及び製品名は、米国 Microsoft Corporation の米国およびその他の国における商標または登録商標です。
- 本 ST に記載の製品名称は、それぞれ各社が商標として使用している場合があります。

1. ST 概説

本章では、ST 参照，TOE 参照，CC 適合について記述する。

1.1 ST 参照

本 ST の識別情報は、以下の通りである。

ST 名称	：	e-STUDIO2330C/2820C/2830C/3520C/3530C/4520C 用 Security Target
ST バージョン	：	Ver2.0
ST 作成日	：	2008 年 11 月 17 日
ST 作成者	：	東芝テック株式会社 画像情報通信カンパニー
評価保証レベル	：	EAL3
評価基準	：	Common Criteria for Information Technology Security Evaluation Version 3.1
評価方法	：	Common Methodology for Information Technology Security Evaluation Version 3.1

1.2 TOE 参照

本 TOE の識別情報は、以下の通りである。

TOE 名称

【日本語名】	：	e-STUDIO2330C/2820C/2830C/3520C/3530C/4520C 用 システムソフトウェア
【英語名】	：	System Software for e-STUDIO2330C/2820C/2830C/3520C/3530C/4520C
TOE バージョン	：	V3.0
TOE 開発者	：	東芝テック株式会社

1.3 TOE 概要

1.3.1 TOE の説明

本 ST が定義する TOE は東芝テック株式会社製 MFP 「e-STUDIO2330C/2820C/2830C/3520C/3530C/4520C」の制御ソフトウェアであり、オプション製品 GP-1070 または GP-1090 にて e-STUDIO のセキュリティ機能が活性化された状態にて TOE は有効となる。

e-STUDIO はユーザ文書を内部に取り込んで処理を行うデジタル複合機であり、その主な機能にはコピー，スキャン，プリント，ファクス，ファイリングボックス/共有フォルダ機能がある。各機能を使用すると、e-STUDIO に取り込んだユーザ文書データは一時的に HDD に書き込まれ処理終了時に削除されるが、FAT ファイルシステムで行う削除は完全な消去は行えず、復元可能な状態で残ってしまう。これはファイリングボックス/共有フォルダに保存されたユーザ文書データの削除にも同じ事が言える。

TOE はこれら e-STUDIO の機能使用時に HDD に書き込まれたユーザ文書データを削除する際、HDD に残存せず復元不可能な方法にて消去を行う。また、HDD の廃棄・交換の際サービスエンジニアによって全ての記録領域を消去し、HDD 内の全てのユーザ文書データは消去される。

1.3.2 TOE の使用方法

本 ST の定義する製品は、プリント速度が異なる e-STUDIO2330C、e-STUDIO2820C、e-STUDIO2830C、e-STUDIO3520C、e-STUDIO3530C、e-STUDIO4520C の 6 種類の MFP であり、TOE は、それらを制御する共通のソフトウェアである。
e-STUDIO は、一般的なオフィス等に設置され、単独で複合機として利用される他に、図 1.3.2 に示すようなネットワーク環境でも、FAX とのデータ送受信端末，メールサーバへのメール発信端末，リモートにある PC のリモートプリンタとして使われる。

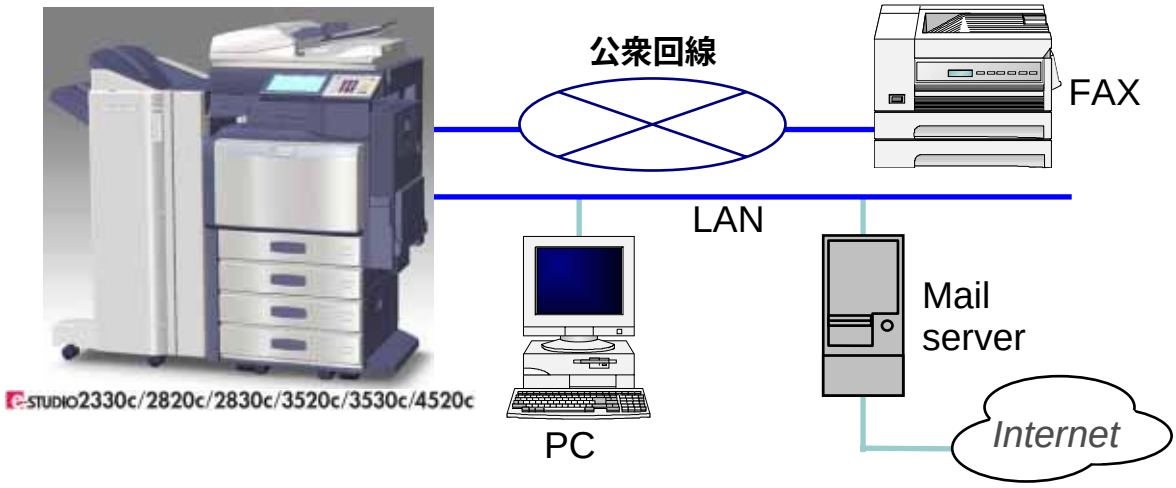


図 1.3.2　e-STUDIO のネットワーク環境での利用

e-STUDIO のオプション機能であるセキュリティ機能は、サービスエンジニアが GP-1070 または GP-1090 を使用し、e-STUDIO へライセンス登録を行うことで有効となる。ライセンスが有効になっている状態を TOE とする。
有効となったセキュリティ機能は以下のデータ削除時に復元不可能な方法にて消去を行う。

・利用者が指定したジョブ中又はジョブの終了（キャンセルを含む）により e-STUDIO がユーザ文書データを削除した時
・e-STUDIO が有効期限の切れたユーザ文書データを自動的に削除した時

e-STUDIO 一般機能を使用すると、スキャナや LAN/FAX/USB 回線よりユーザ文書データを一時的に e-STUDIO 内の HDD へ格納し、そのデータを使用して印刷や FAX 送信やファイリングボックス/共有フォルダへの保存を行う。処理の過程で一時的に格納したユーザ文書データは不要となった時点で OS が提供するファイル削除機能で削除される。
これは OS が管理する FAT32（File Allocation Table）のファイル領域ポインタをクリアするだけであり、e-STUDIO 利用者が HDD 内に存在していると思っていないユーザ文書データが記録された領域が e-STUDIO 内に残ってしまう。また、削除された領域に新しいデータを上書きしても過去のデータは残留磁気として存在する。OS やデータ復元ツールの知識を有する攻撃者であれば HDD を取り外してポインタがクリアされただけの実データの参照や、データの残留磁気を読み取り情報を引き出す事が可能という脅威が存在する。ファイリングボックス/共有フォルダのデータを削除した場合も同様に、削除したはずのデータが読み取られてしまう脅威が存在する。

TOE の通常モード時のセキュリティ機能であるデータ消去機能(1.4.2.2　通常モード時のセキュリティ機能)は削除されるユーザ文書データを完全消去する機能を提供する。セキュリティ機能が有効である場合、利用者は残存データ消去に特別な操作を行うことは無い。
また、HDD の廃棄・交換時にファイリングボックス/共有フォルダ内に保存されたまま残っているユーザ文書データを自己診断モード時のセキュリティ機能である上書き消去強制実行処理(1.4.2.4 自己診断モード時のセキュリティ機能)で一括して完全消去する機能を提供する。

1.3.3 TOE 以外で必要なハードウェア、ソフトウェア及びファームウェア

TOE が動作するためには以下に識別されたハードウェアが必要である

・ＴＯＥのセキュリティ機能が依存するハード/ソフトを識別

ハードウェア構成	仕様 (A4、または letter サイズにおけるコピー／プリント速度)
e-STUDIO2330C	モノクロ：２８枚／分、カラー：２３枚／分
e-STUDIO2820C	モノクロ：２８枚／分、カラー：２８枚／分
e-STUDIO2830C	モノクロ：３５枚／分、カラー：２８枚／分
e-STUDIO3520C	モノクロ：３５枚／分、カラー：３５枚／分
e-STUDIO3530C	モノクロ：４５枚／分、カラー：３５枚／分
e-STUDIO4520C	モノクロ：４５枚／分、カラー：４５枚／分

なお図 1.3.2 の構成で通常モードの機能を使用するためには、PC にはプリンタドライバまたはファクスドライバ、Web ブラウザ、メーラなどのソフトウェアが必要である。
TOE をテストする際、PC には以下のソフトウェアを搭載して評価を行った。

・プリンタドライバ
e-STUDIO4520 Series PrinterDriver Ver 5.11.68.0

・ファクスドライバ
e-STUDIO4520 Series N/W-Fax Driver バージョン 5.11.68.0

・ブラウザ
InternetExplorer ver6.0 sp1 または Firefox ver2.0.0.14

・メーラ
AL-MaiL32 Version1.13 または Thunderbird ver2.0.0.14

・WIA Scan Driver 対応アプリケーション
Windows FAX とスキャン　　バージョン 6.0

1.3.4 TOE の関係者

以下に TOE の運用の関係者、および IT 機器を記す。

・ 利用者
e-STUDIO において、e-STUDIO 一般機能を利用するユーザ。

・ 管理者
TOE の一般機能の各種設定（コピー設定，ネットワーク設定，ファクス設定など）を行い、HDD の上書き消去強制実行処理をサービスエンジニアに依頼して消去を行わせる。
但し、本 TOE に関するセキュリティ機能の管理は行わない。

・ サービスエンジニア
e-STUDIO の運用において、e-STUDIO の設置（GP-1070/GP-1090 にてセキュリティのライセンス登録を含む）やインストール等の保守業務を行う。
管理者からの依頼により、e-STUDIO の HDD 内のユーザ文書データを削除するために、自己診断モードで TOE を起動し、上書き消去強制実行処理によって HDD の全領域を一括して完全消去する。

1.3.5 保護資産

以下に通常モード及び自己診断モードにおける保護資産を記す。

- 通常モードにおける保護資産
  ユーザ文書データ削除後に HDD に磁気的に残っている残存データが保護資産である。保護資産は次の場合に発生する。
  ① 利用者が指定したジョブ中又はジョブの終了（キャンセルを含む）により e-STUDIO がユーザ文書データを削除した場合
  ② e-STUDIO が有効期限の切れたユーザ文書データを自動的に削除した場合

- HDD の廃棄・交換時の保護資産
  廃棄する e-STUDIO 内の HDD や交換する HDD に残っているユーザ文書データが保護資産である。

1.4 TOE 記述

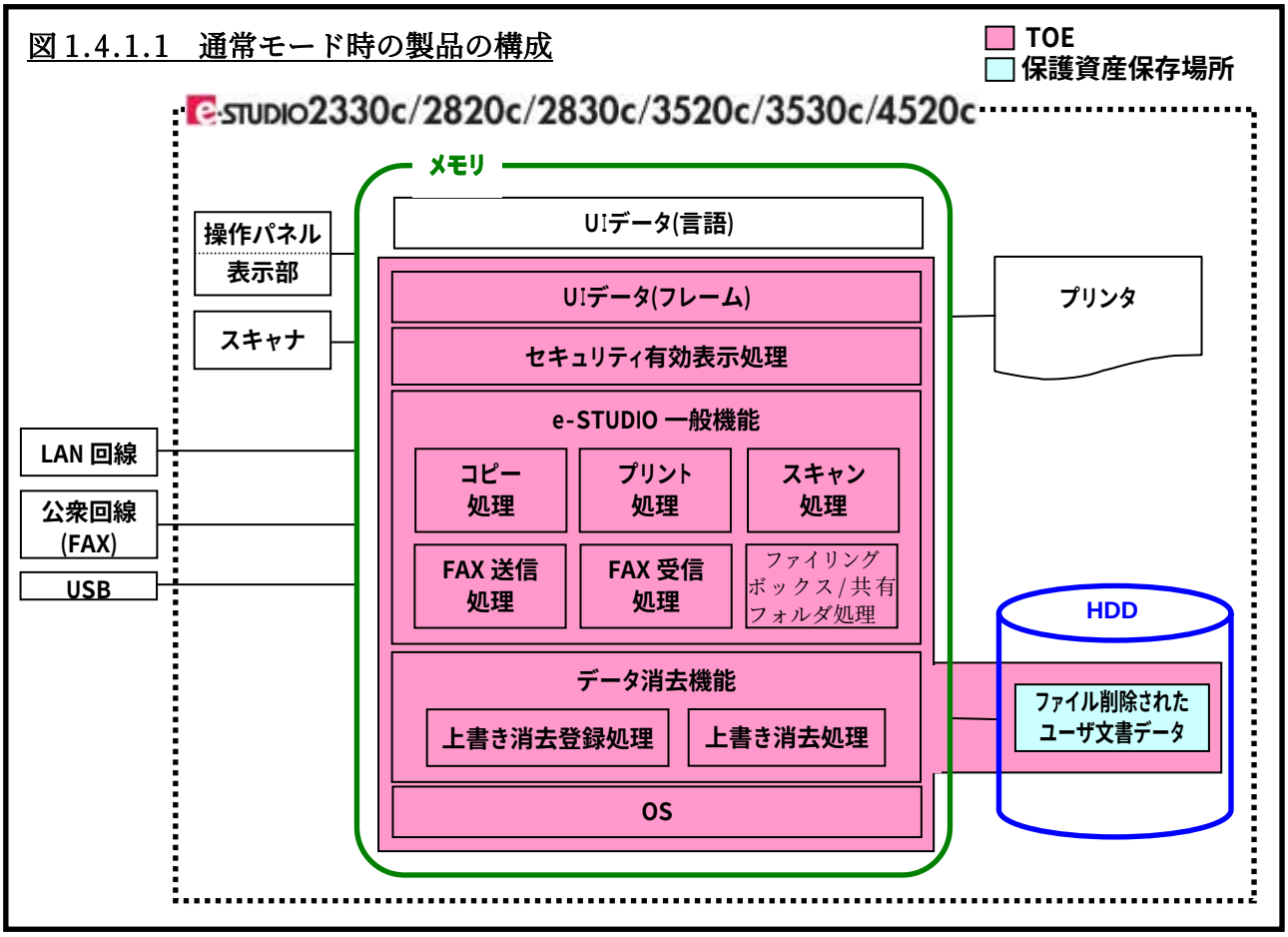
1.4.1 TOE の物理的範囲

本製品は、e-STUDIO 一般機能、すなわち、コピー，スキャン，プリント，ファクス，ファイリングボックス/共有フォルダ機能を搭載したデジタル複合機である。TOE のうち、OS は ROM 上に、それ以外は HDD 上にインストールされる。
e-STUDIO の電源を投入すると、通常モードで起動される。e-STUDIO の利用者は通常、このモードで製品を使用する。
通常モードでは、e-STUDIO 一般機能（1.4.2.1　通常モード時の e-STUDIO 一般機能）と、通常モード時のセキュリティ機能（1.4.2.2　通常モード時のセキュリティ機能）が利用可能である。
通常モードの他に、サービスエンジニアが保守のために使用するモードとして自己診断モードがあり、このモードで起動したときは、e-STUDIO 一般機能と、通常モード時のセキュリティ機能は利用できない。
このモードで利用可能な機能は、自己診断モード時のセキュリティ機能（1.4.2.4　自己診断モード時のセキュリティ機能）である。

1.4.1.1 通常モード時の構成

以下に、本製品の通常モード起動後の構成を示す。
図 1.4.1.1 は本製品に電源投入後、HDD よりプログラムデータをロードし、実行可能となった状態である。
尚、ユーザ文書データが存在する場所は、HDD の作業領域と、指定されたファイリングボックス，共有フォルダのみである。
図 1.4.1.1 のシステムソフトウェア全体が、本 ST の通常モード時の TOE である。

図 1.4.1.1　通常モード時の製品の構成



操作パネル,表示部	タッチパネルと操作ボタンからなるインターフェイス。 コピー処理、プリント処理、スキャン処理、FAX 送信処理、ファイリングボックス/共有フォルダ処理の実行に使用される。
スキャナ	原稿を読み取る装置。
LAN 回線	ネットワークに接続して本機をネットワークプリンタとして使用 TopAccess の使用、ネットワーク経由でのスキャンに使用する。 プリント処理、スキャン処理、FAX 送信処理、ファイリングボックス/共有フォルダ処理の実行に使用される。
公衆回線(FAX)	電話回線へ接続し FAX 送受信に使用される。 FAX 受信処理の実行に使用される。
USB	市販の USB ケーブルで本機と PC を接続しプリンタとして使用するほか、PDF などのファイルを格納した USB メモリを接続して操作パネルよりそのファイルの印刷が行える。 プリント処理、FAX 送信処理の実行に使用される。
プリンタ	印刷を行う装置。
HDD	プログラムデータ,UI データ(言語),設定データが格納されているほか、利用者の操作によりファイリングボックスや共有フォ

	ルダにユーザ文書データを保存できる。また、e-STUDIO 一般機能を使用すると e-STUDIO に取り込んだユーザ文書データが一時的に HDD に書き込まれる。 通常モードにおける保護資産はユーザ文書データ削除後に HDD に磁気的に残っている残存データである。
UI データ(フレーム)	パネルおよび TopAccess の画面構成の情報を持ち、ボタンやメッセージの表示や画面遷移を制御する。表示されるボタンやメッセージは UI データ(言語)を参照する。
UI データ(言語)	各国の言語に対応するデータが格納されており、UI データ(フレーム)より参照される。各言語は同じ構成でボタンやメッセージが格納されている。TOE の範囲外。

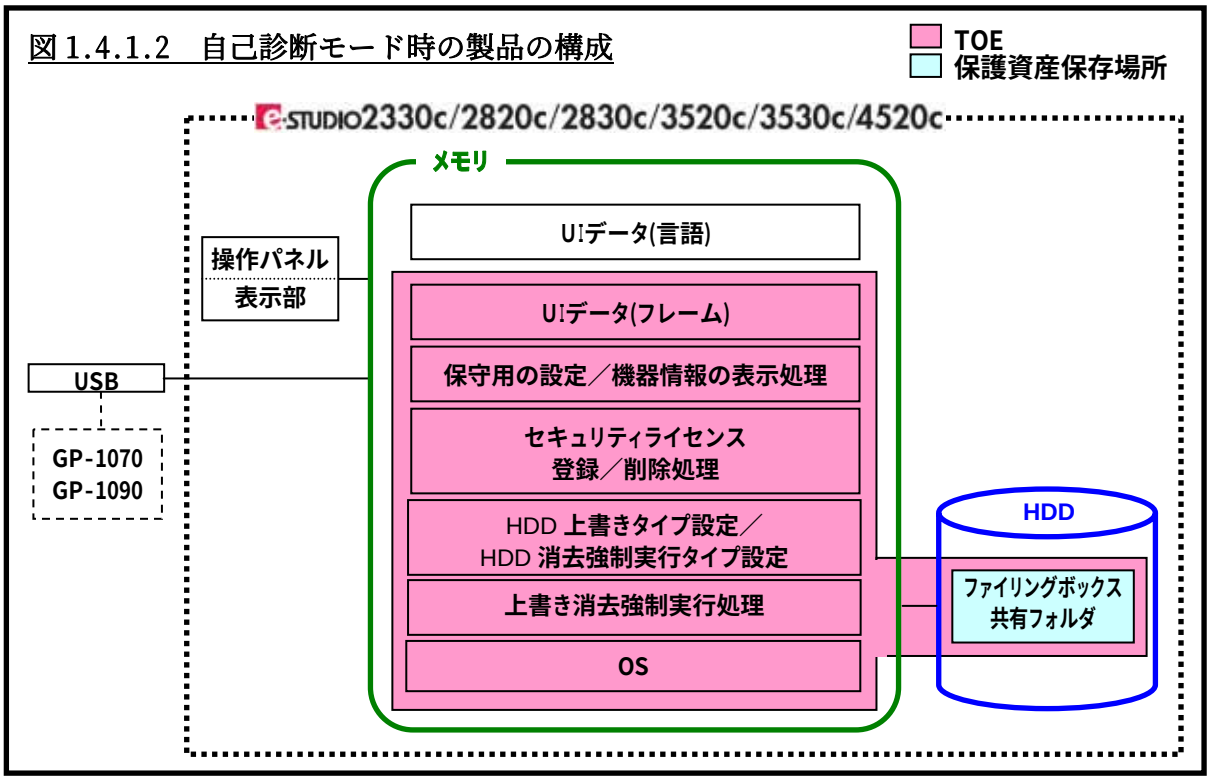
1.4.1.2 自己診断モード時の構成

以下に、本製品の自己診断モード時の構成を示す。

図 1.4.1.2 は本製品に電源投入後、HDD よりプログラムデータをロードし、実行可能となった状態である。

図 1.4.1.2 のシステムソフトウェア全体が、本 ST の自己診断モード時の TOE である。

図 1.4.1.2　自己診断モード時の製品の構成



※GP-1070/GP-1090 **はセキュリティのライセンス登録を行う機器であり、ライセンス登録後に取り外す。**

操作パネル,表示部	サービスエンジニアがパネル操作を行い自己診断モードを起動する。このモードでは保守用の設定のほか e-STUDIO の廃棄や HDD の交換を行う際に上書き消去強制実行処理を行う。 上書き消去強制実行処理の実行に使用される。
USB	GP-1070 または GP-1090 の接続に使用される。
GP-1070/GP-1090	セキュリティのライセンス登録を行う機器。操作はサービスエンジニアによって行われ、ライセンス登録後は取り外される。
HDD	自己診断モードでは e-STUDIO 一般機能は利用できないため、ファイル削除されたユーザ文書データは存在しない。 自己診断モードにおける保護資産は廃棄する e-STUDIO 内の HDD や交換する HDD に残っているユーザ文書データである。
UI データ(フレーム)	通常モード時と同じ。ただし自己診断モード時に TopAccess は使用できない。

UI データ(言語)	通常モード時と同じ。

1.4.2 TOE の論理的範囲

以下に、e-STUDIO 一般機能、およびセキュリティ機能を示す。

1.4.2.1 通常モード時の e-STUDIO 一般機能

(1) セキュリティ有効表示処理

セキュリティのライセンスが登録されているかの確認を行う。
操作パネルからカウンタボタンを押すと印刷カウンタ画面が表示され、セキュリティ機能が有効になっているとデータ消去を表すアイコンと TOE バージョン[SYS V3.0]の表示を行う。

(2) コピー処理

操作パネルよりコピーボタンを選択し、コピーの設定を行った後スタートボタンを押下するとコピー処理が起動される。スキャナからユーザ文書データを読み取り HDD の作業領域へ書き出し、その作業領域のデータを利用してプリンタより出力を行う。
また、コピー設定にてプリンタ出力と同時に HDD のファイリングボックスまたは共有フォルダへの保存が行える。作業領域のデータを利用してデータの保存を行う。

(3) プリント処理

本処理は LAN 回線及び USB 回線より起動するものと、操作パネルより起動するものがある。

・LAN 回線, USB 回線からの起動 (e-STUDIO をプリンタとして使用する)
e-STUDIO は LAN 回線上のネットワークプリンタとしての使用や、USB ケーブルで PC と接続してローカルプリンタとして使用できる。接続された PC にて印刷を実行すると LAN 回線や USB ケーブルより e-STUDIO へユーザ文書データが送られ、プリント処理を起動する。
また、設定にてユーザ文書データをファイリングボックスへ保存する。

・LAN 回線からの起動 (TopAccess)
上記の e-STUDIO をプリンタとして使用する方法で、直にプリンタ出力をせず TopAccess またはパネルからの操作によってプリンタ出力を行う設定が有る。
TopAccess からは[ジョブ]タブより[印刷]メニューを開き、一覧より印刷したいユーザ文書を選択して[リリース]ボタンを押すとプリント処理を起動する。

・操作パネルからの起動
本処理では e-STUDIO に接続された USB メディアの中のドキュメントファイルを印刷でき、操作パネルよりプリントボタンを選択後[USB]ボタンを押し、印刷したいドキュメントを選択後、スタートボタン押下にてプリント処理を起動する。
また、LAN 回線からの起動 (TopAccess)の説明にもあるようにプリンタ出力されない印刷ジョブを操作パネルまたは TopAccess よりプリント処理を起動してプリンタ出力する。操作パネルからはプリントボタンを選択後[プライベート印刷],[お試し印刷],[部門コード無し]のいずれかのボタンを押し、印刷したいドキュメントを選択後、スタートボタン押下にてプリント処理を起動する。

これらのインターフェイスによりプリント処理が起動されるとユーザ文書データを HDD 上の作業領域へ書き出す。その作業領域のデータを利用してプリンタより出力を行う。ユーザ文書データをファイリングボックスへ保存する場合は作業領域のデータを利用してデータの保存を行う。

(4) スキャン処理

本処理は操作パネルからの起動と LAN 回線からの起動がある。操作パネルからはスキャンボタンを選択し、スキャン設定を行った後スタートボタンが押下されるとスキャ

ン処理が起動される。スキャナからユーザ文書データを読み取り HDD 上の作業領域へ書き出す。その作業領域のデータを利用してファイリングボックス，共有フォルダへの保存や USB メディアへの保存や、指定した送信先への E-Mail 送信を行う。
LAN 回線からの起動では、WindowsVista 搭載 PC より LAN 上の e-STUDIO をスキャナとして使用できる WS スキャン機能があり、その PC より e-STUDIO に対しスキャンを要求することでスキャン処理が起動する。スキャナからユーザ文書データを読み取り、スキャン要求を行った PC に画像データを送信する。

(5) FAX 送信処理
本処理は操作パネルより起動するものと、LAN 回線及び USB 回線より起動するものがある。

・操作パネルからの起動
操作パネルよりファクスボタンを選択し、ファクスの設定を行った後スタートボタンを押下すると FAX 送信処理が起動される。スキャナからユーザ文書データを読み取り HDD 上の作業領域へ書き出し、その作業領域のデータを利用して公衆回線(FAX)より FAX 送信、または LAN 回線よりインターネットファクスの送信を行う。

・LAN 回線及び USB 回線からの起動
e-STUDIO は LAN 回線上のネットワークプリンタとしての使用や、USB ケーブルで PC と接続してローカルプリンタとして使用できる。印刷の設定にて N/W-Fax ドライバを選択すると、ユーザ文書データの FAX 送信またはインターネットファクス送信が行える。
e-STUDIO は N/W-Fax ドライバよりユーザ文書データを受信すると FAX 送信処理を起動する。受信したユーザ文書データは HDD 上の作業領域へ書き出し、その作業領域のデータを利用して公衆回線(FAX)より FAX 送信、または LAN 回線よりインターネットファクス送信を行う。

(6) FAX 受信処理
公衆回線(FAX)より FAX データを受信した時、または LAN 回線よりインターネットファクスデータを受信した時に FAX 受信処理が起動される。受信したデータを HDD 上の作業領域へ書き出し、そのデータを利用してプリンタへの出力を行う。
また、データを保存する設定となっている場合、受信したデータを指定したファイリングボックスまたは共有フォルダへ保存する。

(7) ファイリングボックス／共有フォルダ処理
ファイリングボックス／共有フォルダに保存されているユーザ文書データを使用する場合にファイリングボックス／共有フォルダ処理が起動される。本処理は操作パネルより起動するものと、LAN 回線(TopAccess)から起動するものと、時間によって起動するものがある。

・操作パネルからの起動
操作パネルよりファイリングボックスボタンを選択し、ボックスに保存されているユーザ文書データの印刷、編集、削除、E-Mail 送信を行う時に本処理が起動される。
印刷及、編集、E-Mail 送信ではファイリングボックスのユーザ文書データを HDD 上の作業領域へ書き出し、そのデータを利用してプリント出力や編集したユーザ文書データの保存や E-Mail 送信を行う。

・LAN 回線(TopAccess)からの起動
TopAccess 画面よりボックスに保存されているユーザ文書データの印刷、編集、削除、E-Mail 送信、アーカイブ、アーカイブのアップロードを行うと本処理が起動される。
ファイリングボックスに保存されているユーザ文書データを HDD の作業領域へ書き出し、処理に応じてプリント出力、編集後ファイリングボックスへ保存、E-Mail 送信、PC(TopAccess)へユーザ文書データのアーカイブの送信を行う。
また、PC(TopAccess)よりアーカイブデータのアップロードが行われると、e-STUDIO は受信したデータを HDD の作業領域へ書き出し、そのデータを利用してファイリングボックスへ保存を行う。

・時間経過による起動
ファイリングボックスや共有フォルダに保存され有効期限の切れたユーザ文書データファイルを削除する。

1.4.2.2 通常モード時のセキュリティ機能（データ消去機能）

通常モード時のセキュリティ機能には上書き消去登録処理と上書き消去処理があり、この２つの処理をまとめてデータ消去機能と呼ぶ。

上書き消去登録処理
1.4.2.1 通常モード時の e-STUDIO 一般機能(2)～(7)の処理にてユーザ文書データを削除する際に上書き消去登録処理が起動される。この処理では削除要求があったユーザ文書データを上書き消去登録(パスのみ登録)する。この処理により削除ファイルは上書き消去処理の対象ファイルとなる。

上書き消去処理
e-STUDIO の電源投入後起動され上書き消去登録処理により削除されるユーザ文書データの格納領域を監視し、その領域に対し完全消去を行う。
なお、ユーザ文書データの完全消去処理実行中は、「データ消去中」を操作パネルに表示する。

1.4.2.3 自己診断モード時の保守用の設定/機器情報の表示処理

自己診断モードはサービスエンジニアにより起動及び使用される。
保守用の設定/機器情報の表示処理
表に示す 8 タイプに分かれており、それぞれ起動方法が異なる。
「設定」タイプにてセキュリティに影響する項目があり、それは 1.4.2.4 自己診断モード時のセキュリティ機能にて述べる。

表 1.4.2.3 自己診断モードのタイプ一覧

タイプ	概要
コンパネチェック	パネル LED の点灯チェックを行う
テスト	LAN 回線、USB 回線の入力信号の状態チェックを行う
テストプリント	テストパターンを印刷
調整	ハードウェアの調整を行う
設定	各種項目の設定を行う
リスト印刷	カウンタ類のリスト印刷を行う
PM サポート	各カウンタのクリアを行う
ファームウェアアップデート	システムファームウェアを更新する

1.4.2.4 自己診断モード時のセキュリティ機能

上記 表 1.4.2.3 自己診断モードのタイプ一覧の「設定」タイプにて e-STUDIO 起動後にコード入力にて機能を起動する。

上書き消去強制実行処理
本処理は e-STUDIO の廃棄や HDD の交換を行う際、操作パネルから実行する。処理を実行すると HDD に残っているユーザ文書データを一括して完全消去する。

セキュリティライセンス登録／削除処理
GP-1070 または GP-1090 によりライセンス登録または削除を行う。セキュリティライセンスが削除されると e-STUDIO は使用不可能になり e-STUDIO を復旧させるためにはサービスエンジニアにより TOE のインストールが必要となる。

HDD 上書きタイプ設定／HDD 消去強制実行タイプ設定
通常モード時のデータ消去機能と、自己診断モード時の上書き消去強制実行の上書きタイプ設定を行う。

1.4.3 TOE を構成するガイダンスの識別

・ＴＯＥを構成するガイダンスを以下に記す

種別	識別番号	ドキュメント名	仕向	説明
取扱説明書	**0MJ080001A0**	安全にお使いいただくために	日本	※1
	0ME080002A0	Safety Information	海外	
	0MJ08003900	クイックスタートガイド	日本	※2
	0ME08004000	Quick Start Guide	海外	
サービスマニュアル	**SMJ070009D0**	e-STUDIO2330C/2830C/3520C/4520C サービスマニュアル	日本	※3
	SHJ070002D0	e-STUDIO2330C/2820C/2830C/3520C/3530C/4520C Service Manual	海外	

※1 本機を安全に使用するためのお願いについての説明
※2 本機を使用するための準備や基本的な使用方法などの説明
※3 本機のハード/ソフトのメンテナンスに必要な情報を記したマニュアル

2. 適合主張

本章では、ST 参照，TOE 参照，CC 適合について記述する。

2.1 CC 適合主張

本 ST 及び TOE の CC 適合主張は、以下のとおりである。
ST と TOE が適合を主張する CC のバージョン ：
パート 1: 概説と一般モデル 2006 年 9 月 バージョン 3.1 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 2006 年 9 月 バージョン 3.1 翻訳第 1.2 版
パート 3: セキュリティ保証コンポーネント 2006 年 9 月 バージョン 3.1 翻訳第 1.2 版

CC パート 2 に対する ST の適合 :CC パート 2 適合
CC パート 3 に対する ST の適合 :CC パート 3 適合

2.2 PP 主張、パッケージ主張

本 ST は、以下の評価保証レベル、および PP に適合している。

- 評価保証レベルは、EAL3 適合である。
- 本 ST が適合している PP はない。

2.3 適合根拠

無し。

3. セキュリティ課題定義

本章では、TOE、および TOE の運用環境により対処されるセキュリティ課題を定義する。

3.1 脅威

e-STUDIO に対して想定される攻撃者からの攻撃による脅威の詳細は、以下の通りである。

- T.TEMPDATA_ACCESS
  悪意を持った利用者または非関係者が人目につかずに e-STUDIO から HDD を取り外し、既存のツールを使用して、e-STUDIO の HDD から削除されたユーザ文書データを復元・解読することにより、ユーザ文書を取り出すかもしれない。

- T.STOREDATA_ACCESS
  悪意を持った利用者または非関係者が、既存のツールを使用して、廃棄又は交換した e-STUDIO の HDD からユーザ文書を取り出すかもしれない。

3.2 組織のセキュリティ方針

組織のセキュリティ方針は無い。

3.3 前提条件

TOE の前提条件は以下の通りである。

- A.TRUST_SE
  サービスエンジニアは e-STUDIO の自己診断モードの操作に必要な知識を持ち、不正な操作は行わないと想定する。

- A.NO_ERASE_STOP
  電源の切断により通常モード時の上書き消去処理が中断されることは想定していない。

4. セキュリティ対策方針

本章では、TOE セキュリティ対策方針、及び環境のセキュリティ対策方針について記述する。

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は以下の通りである。

- O.TEMPDATA_OVERWRITE
  TOE は、e-STUDIO の HDD から削除されるユーザ文書データを完全に消去後削除し復元・解読されないようにしなければならない。

- O.STOREDATA_OVERWRITE
  TOE は、廃棄または交換する HDD の全てのユーザ文書データを完全に消去する能力を提供しなければならない。

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は以下の通りである。

- OE.HDD_ERASE
  管理者はサービスエンジニアに e-STUDIO の破棄または交換を依頼する。サービスエンジニアは e-STUDIO の破棄または交換時に、HDD の完全消去を行い、全てのユーザ文書データを復元・解読されないようにしなければならない。

- OE.TRUST_SE
  管理者は、東芝テックが認めたサービスエンジニアに自己診断モードの操作を行わせなければならない。東芝テックはサービスエンジニアが必要な知識を持ち、不正な行為をしないことを保証しなければならない。

- OE.NO_ERASE_STOP
  e-STUDIO 利用者及び管理者は通常モード時の「データ消去中」の表示が操作パネル上にされている間、e-STUDIO の電源を切断してはならない。

4.3 セキュリティ対策方針根拠

以下に、セキュリティ対策方針と前提条件、脅威との対応を示す。表の通り、全てのセキュリティ対策方針は少なくとも一つの前提条件、脅威と対応している。

	O.TEMPDATA_OVERWRITE	O.STOREDATA_OVERWRITE	OE.HDD_ERASE	OE.TRUST_SE	OE.NO_ERASE_STOP
T.TEMPDATA_ACCESS	✓				
T.STOREDATA_ACCESS		✓	✓		
A.TRUST_SE				✓	
A.NO_ERASE_STOP					✓

以下に、セキュリティ対策方針による TOE セキュリティ環境（前提条件, 組織のセキュリティ方針, 脅威）の十分性について記述する。

- T.TEMPDATA_ACCESS
  O.TEMPDATA_OVERWRITE により e-STUDIO の HDD からファイル削除されたユーザ文書データの完全消去が行われるため、HDD に磁気的に残っている残存データが復元され、解読される脅威に対抗できる。

- T.STOREDATA_ACCESS
  O.STOREDATA_OVERWRITE により、上書き消去強制実行処理において e-STUDIO の HDD からユーザ文書データの領域を完全消去する能力を提供し、OE.HDD_ERASE により e-STUDIO を廃棄又は交換前を管理者がサービスエンジニアに依頼し、サービスエンジニアは HDD の完全消去を行うため、全てのユーザ文書データを復元・解読されないようにすることができ脅威に対抗できる。

- A.TRUST_SE
  OE.TRUST_SE により、東芝テックは認めたサービスエンジニアが e-STUDIO の操作に必要な知識を持ち、不正な行為をしないことを保証し、管理者はそのサービスエンジニアに自己診断モードの操作を行わせるため前提条件を充足している。

- A.NO_ERASE_STOP
  OE.NO_ERASE_STOP により、e-STUDIO 利用者及び管理者は通常モード時に操作パネル上に「データ消去中」の表示がされている場合は電源の切断を行わないので上書き消去処理の電源断による中断がなされないため前提条件を充足することができる。

5. 拡張コンポーネント定義

拡張コンポーネントは無い。

6. セキュリティ要件

本章では、TOE セキュリティ要件について記述する。

6.1 TOE セキュリティ機能要件

・ FDP_RIP.1_TEMPサブセット情報保護_TEMP

下位階層： なし

依存性： なし

FDP_RIP.1_TEMP.1 TSF は、［割付：以下のオブジェクトのリスト］のオブジェクト［選択：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利用できなくすることを保証しなければならない。

オブジェクトのリスト

1．ジョブ処理中又はジョブ終了後にユーザ文書を削除する際に HDD に残っているユーザ文書データの格納領域

2．ファイリングボックス/共有フォルダ内の保存期間を過ぎ、削除するユーザ文書データの格納領域

・ FDP_RIP.1_ALL サブセット情報保護_ALL

下位階層： なし

依存性： なし

FDP_RIP.1_ALL.1 TSF は、［割付：以下のオブジェクトのリスト］のオブジェクト［選択：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利用できなくすることを保証しなければならない。

オブジェクトのリスト

HDD に存在する全てのユーザ文書データファイル

6.2 TOE セキュリティ保証要件

評価保証レベルは EAL3 であり、TOE セキュリティ保証要件コンポーネントは以下の通りである。

- 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 派生し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
- 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
- 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
- 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
- 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
・ 脆弱性評定
・ AVA_VAN.2　脆弱性分析

6.3 セキュリティ要件根拠

6.3.1 セキュリティ機能要件根拠

以下に TOE セキュリティ機能とセキュリティ機能要件との対応を示す。
表の通り、全ての TOE セキュリティ機能は、少なくとも一つの TOE セキュリティ機能要件と対応している。

	0.TEMPDATA_OVERWRITE	0.STOREDATA_OVERWRITE
FDP_RIP.1_TEMP	✓	
FDP_RIP.1_ALL		✓

セキュリティ機能要件の根拠は以下の通りである。

・ 0.TEMPDATA_OVERWRITE
　・ FDP_RIP.1_TEMP（サブセット情報保護_TEMP）
　FDP_RIP.1_TEMP（サブセット情報保護_TEMP）により、ファイル削除を行う資源の割当て解除時に、TOE が資源の以前のどの情報の内容も利用できなくすることで、TOE が e-STUDIO の HDD からファイル削除を行ったユーザ文書データ領域の完全消去を行うことが実現でき、0.TEMPDATA_OVERWRITE は満たされる。

・ 0.STOREDATA_OVERWRITE
　・ FDP_RIP.1_ALL（サブセット情報保護_ALL）
　FDP_RIP.1_ALL（サブセット情報保護_ALL）により、e-STUDIO の廃棄、または HDD の交換を行う際に上書き消去強制実行処理によって全てのユーザ文書データ(オブジェクト)を完全に消去し、TOE が資源の以前のどの情報の内容も利用できなくするため 0.STOREDATA_OVERWRITE は満たされる。

6.3.2 セキュリティ保証要件根拠

本 TOE は、一般のオフィス等の環境で使用されるため、攻撃の機会は制限される。
従って本 TOE は、低レベルの攻撃能力を有する脅威エージェントを想定することができる。
これに対抗するために、TOE 開発のセキュリティ対策の分析（設計の系統だった分析とテスト、及び開発環境が安全であること）でカバーされる範囲を評価することとした。
よって、評価保証レベル 3 の保証パッケージが妥当である。

7．TOE 要約仕様

本章では、TOE の要約仕様を記述する。

7.1 データ消去機能

e-STUDIO の一般機能の処理によって一時的に作業領域を生成し格納されたユーザ文書データまたは、ファイリングボックス/共有フォルダ内に格納されているユーザ文書データは、次の削除タイミングでこれらの格納領域が資源の割り当て解除される。

- 利用者が操作したジョブの処理中又はジョブの終了
- ファイリングボックス/共有フォルダ内のユーザ文書データの保存期限切れ

このとき TSF は格納領域のパスを上書き消去登録し、上書き消去登録を監視するプロセスによって消去登録されたパスより該当領域が再読み出しされない方法で直ちに上書きしその後領域を解放する。上書き中「データ消去中」を操作パネルに表示する。

このように TOE のセキュリティ機能（データ消去機能）は、上書き消去登録処理及び上書き消去処理から構成される。

上書き消去はパスから特定された格納領域に 00、FF、ランダムのデータを上書した後、領域を開放することにより完全消去する。TOE ではこの消去タイプを使用するが、よりセキュアな消去タイプも自己診断モードで選択できる。

データ消去機能により、ユーザ文書データの領域が復元され、解読されることがないようにするという完全消去が実現でき、FDP_RIP.1_TEMP が実現される。

7.2 上書き消去強制実行処理

TSF は上書き強制実行処理により、HDD に存在するユーザ文書データファイルを含む HDD の全記憶領域を 00、FF、ランダムのデータで上書後初期化する。すべてのユーザ文書データの領域が復元され、解読されることがないことが保証され、FDP_RIP.1_ALL が実現される。