TOSHIBA

e-STUDIO352/452/353/453用
システムソフトウェア
Security Target

2008年7月22日
Ver 2.3

東芝テック株式会社

目次

1. ST 概説

本章では、ST 識別，ST 概要，CC 適合について記述する。
また、本 ST 内で使用している用語や略語、及び商標についても記述する。

1.1 ST 識別

本 ST の識別情報は、以下の通りである。

ST 名称	:	e-STUDIO352/452, e-STUDIO353/453 用 システムソフトウェア Security Target
ST バージョン	:	Ver2.3
ST 作成日	:	2008 年 7 月 22 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
TOE 名称		
【日本語名】	:	e-STUDIO352/452, e-STUDIO353/453 用 システムソフトウェア
【英語名】	:	System Software for e-STUDIO352/452, e-STUDIO353/453
TOE バージョン	:	V2.0
TOE 製作者	:	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
キーワード	:	デジタル複写機，MFP，e-STUDIO，GP-1060，データ消去機能，上書き消去，東芝テック株式会社
評価基準	:	Common Criteria for Information Technology Security Evaluation Version 2.3 CCIMB Interpretations－0407
評価方法	:	Common Methodology for Information Technology Security Evaluation Version 1.0 CCIMB Interpretations－0407

1.2 ST 概要

本 ST が定義する TOE は東芝テック株式会社製 MFP「e-STUDIO352/452, e-STUDIO353/453」の制御ソフトウェアであり、オプション製品 GP-1060 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 は使用される。
MFP 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、MFP 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では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 MFP 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 の破棄・交換時にはサービスエンジニアによってファイリングボックス/共有フォルダの全ての記録領域に対し消去が行われ、HDD 内の全てのユーザ文書データは消去される。

1.3 CC 適合

本 ST は、以下の CC に適合している。

- CC バージョン 2.3 パート 2 適合
- CC バージョン 2.3 パート 3 適合
- 評価保証レベル EAL3 適合
- 本 ST が適合している PP はない。

1.4 用語，略語

本 ST で使用している用語，略語は、以下の通りである。

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
- ST (Security Target)　：セキュリティターゲット
- TOE (Target Of Evaluation)　：評価対象
- SOF (Strength Of Function)　：機能強度
- TSF (TOE Security Function)　：TOE セキュリティ機能
- TSP (TOE Security Policy)　：TOE セキュリティポリシ
- TSC (TSF Scope of Control)　：TSF 制御範囲

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。本 ST では、e-STUDIO352/452, e-STUDIO353/453 (e-STUDIO352, e-STUDIO452, e-STUDIO353, e-STUDIO453) 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。

- 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。

- 削除
  資源を解放し、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。

- 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 MFP 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。

・ GP-1060
e-STUDIO に装着して、システムソフトウェア内のセキュリティ機能であるデータ消去機能を有効にするための製品。

1.5 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、InternetExplorer 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。
- Firefox 及び Thunderbird は、米国 Mozilla Foundation 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。

2. TOE 記述

本章では、e-STUDIO352/452, e-STUDIO353/453 の製品タイプ，利用環境，製品の構成，機能、及び脅威について記述する。

2.1 製品タイプと利用環境

本 ST の定義する製品は、プリント速度が異なる e-STUDIO352，e-STUDIO452，e-STUDIO353，e-STUDIO453 の 4 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 2.1 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。

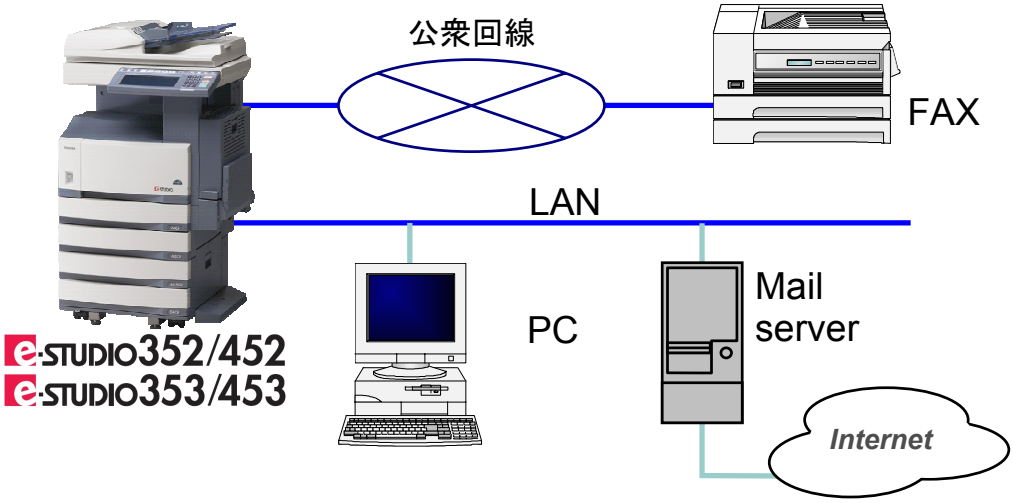

図 2.1　e-STUDIO のネットワーク環境での利用

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によりセキュリティイネーブラ GP-1060 を e-STUDIO へ接続することで有効となる。セキュリティ機能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、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に復元不可能な方法にて消去を行う。

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 MFP 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 HDD に格納したユーザ文書データは不要となった時点で削除される。ファイルは 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、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 を取り外して残留磁気を読み取り情報を引き出す脅威が存在する。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(2.2.1.2　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(2.2.2.2 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。

以下に、e-STUDIO のハードウェア、及びソフトウェアの構成を示す。

ハードウェア構成	仕様
e-STUDIO352/452, e-STUDIO353/453	e-STUDIO352/353：35 枚／分　※A4、または letter サイズにおけ e-STUDIO452/453：45 枚／分　るコピー／プリント速度
GP-1060	USB インタフェース

表 2.1-1 e-STUDIO ハードウェア構成

ソフトウェア構成	機能
システムソフトウェア V2.0	e-STUDIO352/452, e-STUDIO353/453 を制御するシステムソフトウェア
UI データ（オプション言語） 日　：V040.000 2 米英：V039.000 3 欧英：V039.000 4	仕向け（国）別言語データ
VxWorks 5.5	OS

表 2.1-2 e-STUDIO ソフトウェア構成

なお図 2-1 の構成で 2.2.1 節の通常モードで使用するやめには、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-STUDIO452 Series PrinterDriver Ver 4.6.63.0

・ファクスドライバ
　e-STUDIO452 Series N/W-Fax Driver バージョン 4.9.60.0

・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

2.2 製品の機能と TOE

本製品は、OS（VxWorks）上に 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 は、e-STUDIO のソフトウェアであり、e-STUDIO 内の ROM に存在し、e-STUDIO 全体を制御する。
e-STUDIO を立ち上げると、通常モードで起動される。利用者は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（2.2.1.1 節参照）と通常モード時のセキュリティ機能（2.2.1.2 節参照）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。
このモードでは、自己診断モード時のセキュリティ機能（2.2.2.2 節参照）が使用可能になる。

2.2.1 通常モードの機能と TOE

図 2.2.1 に、本製品の通常モード時の構成図を示す。
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 2.2.1 の OS を除く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。

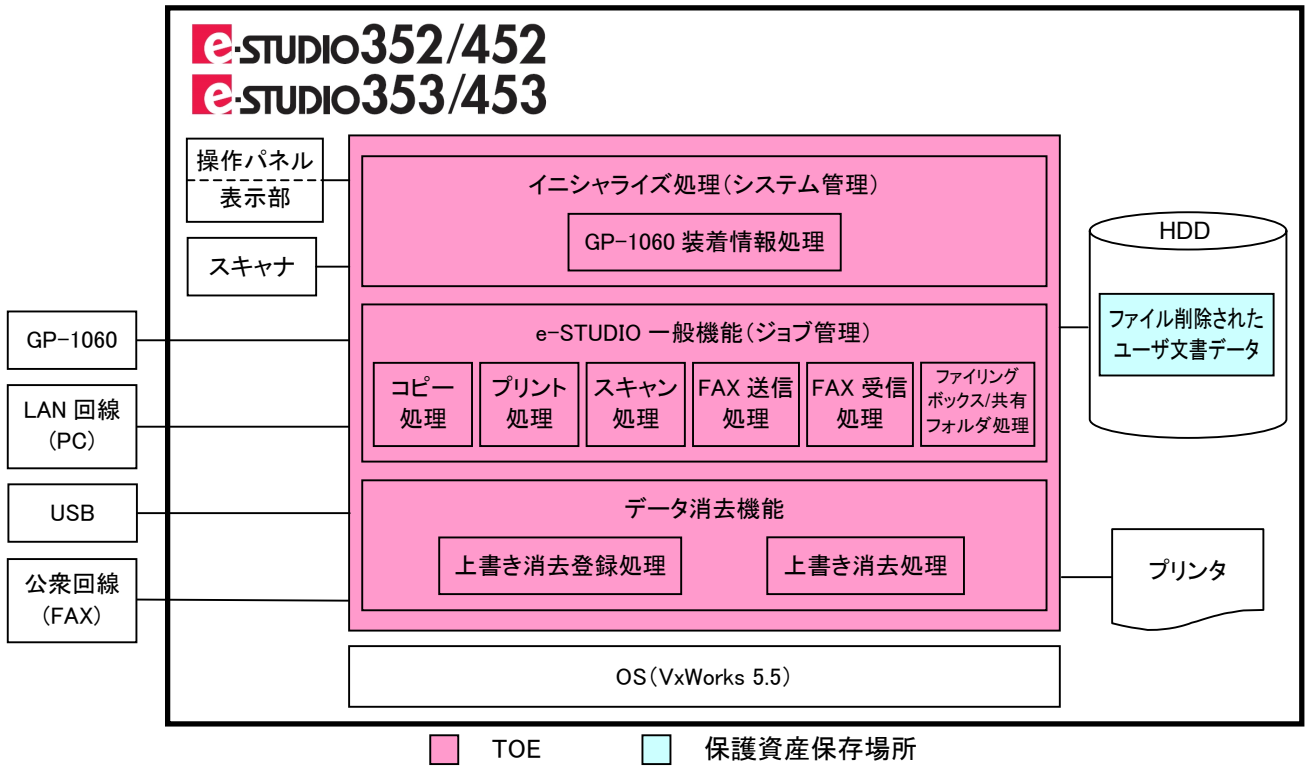

図 2.2.1 通常モード時の製品の構成

2.2.1.1 通常モード時の e-STUDIO 一般機能

(1) GP-1060 装着情報処理

GP-1060 の装着により TOE は使用される（未装着の状態は TOE ではない）
MFP が GP-1060 の装着を認識すると操作パネルに TOE の識別［SYS V2.0］を表示する。
ユーザは TOE を確認するため MFP のカバーの機種名及び操作パネルに表示される識別を確認する。

(2) コピー処理

コピー機能が選択された状態でスタートボタンが押下されると、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。
次に、作業領域上のユーザ文書データを読み取り、以下のいずれか、あるいは両方の処理を同時に行う。

- プリンタへ出力する。

・ e-STUDIO 利用者が指定した HDD のファイリングボックス、または共有フォルダに保存することができる。

(3) プリント処理

LAN 回線（PC)、および USB から、ユーザ文書データを受信、またはファイリングボックス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。
次に、作業領域上のユーザ文書データを読み取り、以下のいずれか、あるいは両方の処理を同時に行う。

・ プリンタへ出力する。
・ e-STUDIO 利用者が指定した HDD のファイリングボックスに保存する。

(4) スキャン処理

スキャンボタンが選択された状態でスタートボタンが押下されると、スキャナからユーザ文書データを読み取り、以下のいずれか、あるいは両方の処理を同時に行う。

・ e-STUDIO 利用者が指定した HDD のファイリングボックスまたは共有フォルダに保存する。あるいは WS スキャンにて指定したコンピュータへの送信を行う。
・ e-STUDIO 利用者が指定した送信先に E-Mail 送信する。

(5) FAX 送信処理

ファクスボタンが選択された状態でスタートボタンが押下されると、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。
次に、作業領域上のユーザ文書データを読み取り、FAX へ送信する。
尚、共有フォルダに保存することもできる。

(6) FAX 受信処理

FAX データを受信し、HDD 上の作業領域へ書き出す。
次に、作業領域からデータを読み取り、以下のいずれか、あるいは両方の処理を同時に行う。

・ プリンタへ出力する。
・ e-STUDIO 利用者が指定した HDD のファイリングボックス、または共有フォルダに保存することもできる。

(7) ファイリングボックス/共有フォルダ処理

操作パネル、又は LAN 回線を経由して、PC から e-STUDIO の HDD のファイリングボックス、および共有フォルダに保存されているユーザ文書データの削除処理を行う。

2.2.1.2 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。

(1) 上書き消去登録処理

2.2.1.1 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ゴミ箱フォルダにパスのみ移動(リネーム)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。

(2) 上書き消去処理

本処理は、ゴミ箱フォルダに登録されたユーザ文書データの有無を監視する。登録されていると、その格納領域を完全に消去する。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」の表示を操作パネルに行う。

2.2.2 自己診断モードの機能と TOE

図 2.2.2 に、本製品の自己診断モード時の構成図を示す。
図 2.2.2 の OS を除く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。

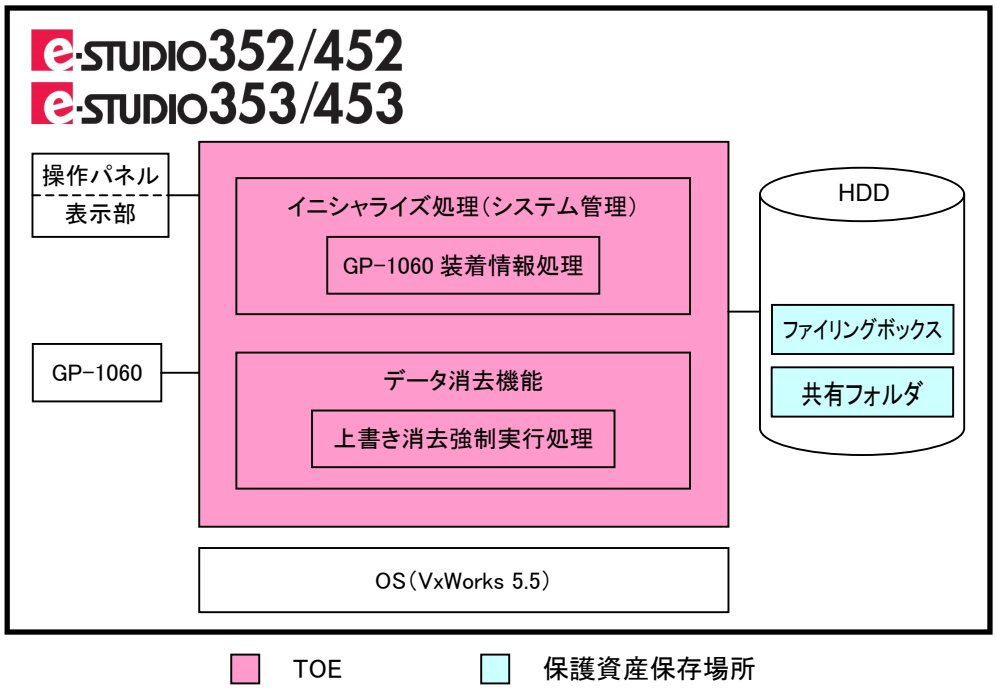

図 2.2.2 自己診断モード時の製品の構成

2.2.2.1 自己診断モード時の e-STUDIO の機能
自己診断モード時の e-STUDIO 一般機能には保守用の設定、機器情報の表示などがあるが、セキュリティ機能に関係する以下の処理のみ記述する。

・GP-1060 装着情報処理
GP-1060 の装着確認を行う。セキュリティ機能が有効となっている場合 2.2.1.4 自己診断モード時のセキュリティ機能が使用できる。

2.2.2.2 自己診断モード時のセキュリティ機能
・上書き消去強制実行処理
HDD 内に保存されているユーザ文書データが書き込まれている全領域を一括して完全に消去する。

2.3 TOE の関係者
以下に、TOE の運用に必要な人物を定義する。

2.3.1 利用者
e-STUDIO における e-STUDIO 一般機能を利用するユーザ。

2.3.2 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。

2.3.3 サービスエンジニア
e-STUDIO の運用において、設置（GP-1060 の設置作業を含む）やインストール等の保守業務を行

う。
e-STUDIO 管理者からの依頼により、e-STUDIO の HDD 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に消去する。

2.4 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に発生する。
ただし、以下の処理にて削除されたユーザ文書データの残存データは保護の対象から除外する。

①FAX 受信

FAX 送信者は受信側の FAX 機がセキュリティ機能を備えているかを意識しないと思われる。また、一般的な FAX 機はデータを受信すると直ちに自動で印刷を行うため、FAX 送信者は受信側の FAX 機での文書の保護を期待しないものと想定し、MFP が受信した FAX データを保護資産より除外する。

②ファイリングボックス/共有フォルダのファイル保存日数超過による自動削除

保存日数が設定されている場合、ユーザ文書データはその設定日数超過時に TOE によって削除される。自動で行われる処理を利用者がその都度セキュリティ機能にて消去されたことの確認を行うとは考えられず、保護資産より除外する。

・ 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。

3. TOE セキュリティ環境

本章では、前提条件、脅威、組織のセキュリティ方針について記述する。

3.1 前提条件

前提条件はない。

3.2 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 MFP 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。

3.3 組織のセキュリティ方針

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 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 からファイル削除された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完全に消去しなければならない。

- **O.STOREDATA_OVERWRITE**
  TOE は、廃棄又は交換した e-STUDIO の HDD からユーザ文書データを解読されないよう、上書き消去強制実行処理により完全に消去しなければならない。

4.2 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.OVERWRITE_COMPLETE**
  e-STUDIO 利用者は印刷物を回収する際、「データ消去中」の表示が操作パネル上にされている場合、その表示が消えることを確認することでユーザ文書データが完全に消去された事を確認しなければならない。

- **OE.HDD_ERASE**
  e-STUDIO 管理者は e-STUDIO の廃棄又は HDD の交換時に、HDD の上書き消去強制実行処理をサービスエンジニアに行わせなければならない。

5. IT セキュリティ要件

本章では、TOE セキュリティ要件、及び IT 環境のセキュリティ要件について記述する。

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

TOE セキュリティ機能要件は以下の通りである。

- FDP_RIP.1　サブセット残存情報保護
  - 下位階層：　なし
  - FDP_RIP.1.1　TSF は、以下のオブジェクト[選択：への資源の割当て、***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：[割付：オブジェクトのリスト]。

    [割付：オブジェクトのリスト]
    e-STUDIO の HDD からファイル削除されたユーザ文書データの格納領域。

  - 依存性：　なし

- FDP_RIP.2　全残存情報保護
  - 下位階層：　FDP_RIP.1
  - FDP_RIP.2.1　TSF は、すべてのオブジェクト[選択：への資源の割当て、***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。

  - 依存性：　なし

- 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

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。

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

5.1.3 最小機能強度宣言

本 TOE における最小機能強度は、SOF-基本である。

確率的、又は順列的なメカニズムを利用する機能要件はない。

5.2 IT 環境のセキュリティ要件

IT 環境のセキュリティ要件はない。

6. TOE 要約仕様

本章では、TOE の要約仕様を記述する。

6.1 TOE セキュリティ機能

表 6.1-1 に示すように、6.1.1 節で説明する TOE セキュリティ機能は、5.1.1 節で記述したセキュリティ機能要件を満たすものである。

	FDP_RIP.1	FDP_RIP.2	FPT_RVM.1
SF.TEMPDATA_OVERWRITE	✓		✓
SF.STOREDATA_OVERWRITE		✓	✓

表 6.1-1　TOE セキュリティ機能とセキュリティ機能要件の対応

6.1.1 TOE セキュリティ機能

TOE セキュリティ機能は、以下の通りである。

SF.TEMPDATA_OVERWRITE

TOE は、e-STUDIO の HDD からファイル削除されるユーザ文書データに対して以下の保護を行い、ダストボックスに登録された格納領域を開放し、ファイル削除されたユーザ文書データが復元され解読されることがないようにする。

【残存情報保護】

- 通常モードにおいて、e-STUDIO の HDD からファイル削除されるユーザ文書データの格納領域をダストボックスへ登録する。
- ダストボックスに登録された e-STUDIO の HDD からファイル削除されたユーザ文書データの格納領域に対し完全に消去を行う。

(FDP_RIP.1)

また、TOE は、本機能が迂回されないように e-STUDIO 一般機能において、ユーザ文書データ使用後、必ず SF.TEMPDATA_OVERWRITE を実行し、ダストボックスに登録された STUDIO の HDD からファイル削除されたユーザ文書データの格納領域に対し完全に消去を行い、格納領域を開放するようにする。

(FPT_RVM.1)

SF.STOREDATA_OVERWRITE

TOE は、e-STUDIO の HDD のユーザ文書データに対して上書き消去強制実行処理によって以下の保護を行いファイル領域を開放しユーザ文書データが読み出され解読されることがないようにする。

【残存情報保護】

- 自己診断モードにおいて、HDD の全領域に対し一括して完全に消去を行う。

(FDP_RIP.2)

また、TOE は、本機能が迂回されないように自己診断モードにおいて、操作パネルからの指示で、必ず SF.STOREDATA_OVERWRITE を実行し、HDD の全領域に対して上書き消去を行い、領域を開放するようにする。

(FPT_RVM.1)

6.1.2 セキュリティメカニズム

本 ST で参照されているセキュリティメカニズムと、それを使用している TOE セキュリティ機能の対応を以下に示す。

セキュリティメカニズム	セキュリティ機能
DoD5220.22-M	SF.TEMPDATA_OVERWRITE
	SF.STOREDATA_OVERWRITE

表 6.1 セキュリティメカニズムと TOE セキュリティ機能

DoD5220.22-M 準拠：0x00 Fill + 0xFF Fill + 乱数 Fill + 検証

6.1.3 機能強度主張

TOE セキュリティ機能の内、非暗号で且つ確率的、或いは順列的メカニズムに基づくものは TOE には存在しない。

6.2 保証手段

セキュリティ保証手段として提供される文書、及び TOE に対応するセキュリティ保証要件の対応は以下の通りである。

保証要件 クラス	保証要件 コンポーネント	ドキュメント名称、及び TOE
ACM 構成管理	ACM_CAP.3 ACM_SCP.1	e-STUDIO352/452, e-STUDIO353/453 用システムソフトウェア構成リスト e-STUDIO352/452, e-STUDIO353/453 用システムソフトウェア構成管理計画
ADV 開発	ADV_FSP.1 ADV_HLD.2	機能仕様書/上位レベル設計書
	ADV_RCR.1	表現対応分析書
ALC ライフサイクルサポート	ALC_DVS.1	開発環境基準書
ATE テスト	ATE_COV.2 ATE_DPT.1 ATE_FUN.1 ATE_IND.2	機能テスト TOE
AVA 脆弱性評定	AVA_MSU.1	クイックスタートガイド Quick Start Guide
	AVA_VLA.1 AVA_SOF.1	脆弱性分析書
AGD ガイダンス文書	AGD_ADM.1 AGD_USR.1	クイックスタートガイド Quick Start Guide
ADO 配付と運用	ADO_IGS.1	サービスマニュアル[概要編] サービスマニュアル[サービス編] SERVICE MANUAL SERVICE HANDBOOK GP-1060 for e-STUDIO352/452, e-STUDIO353/453
	ADO_DEL.1	e-STUDIO シリーズ TOE 配付手順書 システムソフトウェア配付手順書

表 6.2-1 セキュリティ保証手段とセキュリティ保証要件

※ガイダンスに記されている機種番号が仕向(国)ごとに異なるが、これはガイダンスに記されていない機種はその仕向(国)に出荷されないためである。(日本向けガイダンスに e-STUDIO520 などが記載されていない等)

7. PP 主張

PP への適合は主張しない。

8. 根拠

本章では、セキュリティ対策方針、セキュリティ要件、TOE 要約仕様、PP 主張の根拠について記述する。

8.1 セキュリティ対策方針根拠

8.1.1 セキュリティ対策方針の必要性

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。

	T.TEMPDATA_ACCESS	T.STOREDATA_ACCESS
O.TEMPDATA_OVERWRITE	✓	
OE.OVERWRITE_COMPLETE	✓	
O.STOREDATA_OVERWRITE		✓
OE.HDD_ERASE		✓

表 8.1-1 セキュリティ対策方針と前提条件、脅威

8.1.2 セキュリティ対策方針の十分性

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、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領域を復元され、解読されることを防止することができ、OE.OVERWRITE_COMPLETE により、O.TEMPDATA_OVERWRITE が確実に実行されたことを確認することで、T.TEMPDATA_ACCESS の attack method の無効化を図っている。

・T.STOREDATA_ACCESS

OE.HDD_ERASE により、e-STUDIO 管理者の判断により、e-STUDIO の廃棄又は HDD 交換時に HDD の上書き消去強制実行処理をサービスエンジニアに行わせ、O.STOREDATA_OVERWRITE の上書き消去強制実行処理により e-STUDIO の HDD からユーザ文書データを解読されることを防止することで、T.STOREDATA_ACCESS の attack method の無効化を図っている。

8.2 セキュリティ要件根拠

8.2.1 セキュリティ機能要件の必要性

以下に、セキュリティ機能要件とセキュリティ対策方針との対応を示す。

表の通り、全ての TOE セキュリティ機能要件は少なくとも一つの TOE のセキュリティ対策方針と対応している。

	O.TEMPDATA_OVERWRITE	O.STOREDATA_OVERWRITE
FDP_RIP.1	✓	
FDP_RIP.2		✓
FPT_RVM.1	✓	✓

表 8.2-1 TOE セキュリティ機能要件と TOE のセキュリティ対策方針

8.2.2 セキュリティ機能要件の十分性

以下に、セキュリティ機能要件によるセキュリティ対策方針の十分性を記述する。

・O.TEMPDATA_OVERWRITE

FDP_RIP.1 によってファイル削除されたユーザ文書データの格納領域を完全に消去し、FPT_RVM.1 によってセキュリティ機能のバイパスを防止することで、e-STUDIO の HDD からファイル削除された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セキュリティ対策方針を実現できる。

・O.STOREDATA_OVERWRITE

FDP_RIP.2 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、FPT_RVM.1 によってセキュリティ機能のバイパスを防止することで、e-STUDIO の HDD からユーザ文書データの領域が解読されることがないようにするというセキュリティ対策方針を実現できる。

8.2.3 セキュリティ機能要件の依存性の根拠

以下に、セキュリティ機能要件の依存性の根拠を記述する。

・FDP_RIP.1

満たすべき依存性は存在しない。

・FDP_RIP.2

満たすべき依存性は存在しない。

・FPT_RVM.1

満たすべき依存性は存在しない。

8.2.4 セキュリティ要件の相互作用

以下に、セキュリティ機能要件全体が相互に補完しあい、迂回，干渉，非活性化から保護されていることを説明する。

尚、FDP_RIP.1 と FDP_RIP.2 は動作するモードが異なるため、同時に動くことはない。

・FPT_RVM.1＜迂回防止＞

FPT_RVM.1 によって、通常モード時の FDP_RIP.1、あるいは自己診断モード時の FDP_RIP.2 がバイパスさせることなく動作する行動を実装する。

・ ＜干渉防止＞

TOE は e-STUDIO 全体を制御するもので、ROM に存在し外部から TOE 自体を改ざんすることはでき

ない。また TSF データ（ダストボックス内の情報）を改変する不正なサブジェクトは存在しない。
従ってセキュリティ機能の改ざんを防止する機能要件は必要とせず、信頼できないサブジェクトによる干渉は防止できている。

・＜非活性化防止＞
TOE のセキュリティ機能を非活性化する機能は存在しない。

8.2.5 最小機能強度の妥当性
本 TOE では低レベルの攻撃能力を有する攻撃者を想定しているため、最小機能強度は SOF－基本が妥当である。

8.2.6 セキュリティ保証要件の根拠
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、低レベルな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。

8.3 TOE 要約仕様根拠
8.3.1 セキュリティ機能の必要性
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。

	FDP_RIP.1	FDP_RIP.2	FPT_RVM.1
SF.TEMPDATA_OVERWRITE	✓		✓
SF.STOREDATA_OVERWRITE		✓	✓

表 8.3-1 TOE セキュリティ機能とセキュリティ機能要件

8.3.2 セキュリティ機能の十分性
以下に、セキュリティ機能によるセキュリティ機能要件の十分性を記述する。
・FDP_RIP.1
SF.TEMPDATA_OVERWRITE により、e-STUDIO の HDD からファイル削除されるユーザ文書データの完全な消去を行うことにより、ファイル削除されたユーザ文書データの利用ができなくなる。
以上により、SF.TEMPDATA_OVERWRITE での残存情報保護は保証できる。

・FDP_RIP.2
SF.STOREDATA_OVERWRITE により、e-STUDIO の HDD のユーザ文書データを含む HDD の全領域に完全な消去を行うことにより、HDD 上の全てのデータが利用できなくなる。
以上により、SF.STOREDATA_OVERWRITE での残存情報保護は保証できる。

・FPT_RVM.1
SF.TEMPDATA_OVERWRITE により、e-STUDIO の HDD からファイル削除されると、ユーザ文書データの完全な消去が必ず行われる。
また、SF.STOREDATA_OVERWRITE により、上書き消去強制実行処理を行うと、全てのユーザ文書データの完全な消去が必ず行われる。
以上により、SF.TEMPDATA_OVERWRITE と SF.STOREDATA_OVERWRITE での非バイパス性は保証できる。

8.3.3 機能強度の根拠
本 TOE において、根拠を示すべき、確率的或いは順列的メカニズムを持つセキュリティ機能は存在し

ない。

8.3.4 保証手段の根拠

セキュリティ保証手段が、保証要件を満たすのに適切な根拠を記述する。

全ての EAL3 のセキュリティ保証要件は、セキュリティ保証手段となるドキュメント、及び TOE に対応付けられている。

また、当該ドキュメント、及び TOE によって、セキュリティ保証要件が要求する証拠は網羅されている。表 8.3-2 に、各保証手段の内容を示す。

保証要件 クラス	保証要件 コンポーネント	ドキュメント名称/TOE	内容
ACM 構成管理	ACM_CAP.3 ACM_SCP.1	・e-STUDIO352/452, e-STUDIO353/453 用システムソフトウェア構成リスト ・e-STUDIO352/452, e-STUDIO353/453 用システムソフトウェア構成管理計画	TOE に関する構成管理方法が記述されている。 これらは、TOE のリファレンスや構成リスト，CM 計画，CM システムに関して記述されている。
ADV 開発	ADV_FSP.1 ADV_HLD.2	機能仕様書/上位レベル設計書	TSF のふるまいと TSF インタフェース、TSF 以外の機能についての外部インタフェースについて（機能仕様書）と、サブシステムの観点から TSF を記述したものであり、TSF の構造、サブシステムのインタフェースについて（上位レベル設計書）記述されている。
	ADV_RCR.1	表現対応分析書	ST における要約仕様のセキュリティ機能と機能仕様書／上位レベル設計書におけるサブシステムの関係について分析した結果について記述されている。
ALC ライフサイクル サポート	ALC_DVS.1	開発環境基準書	開発環境の中で、TOE の設計や実装の機密性と完全性を保証するための手段について記述されている。
ATE テスト	ATE_COV.2 ATE_DPT.1 ATE_FUN.1 ATE_IND.2	・機能テスト ・TOE	TSF が仕様通りに実行されることを実証するための機能テスト項目，テスト手順，期待されるテスト結果、及びそれらに基づいて、TSF が機能仕様に対応してテストを行った結果について記述されている。
AVA 脆弱性評定	AVA_MSU.1	クイックスタートガイド Quick Start Guide	これらの文書は、関係者が TOE のセキュアな配付，設置，運用を実行するための手順が記述されている。
	AVA_VLA.1	脆弱性分析書	明らかなセキュリティ脆弱性の存在を探索し、TOE の意図する環境において、それらの脆弱性が悪用され得ないことを確認する脆弱性分析を実施した結果について記述されている。

	AVA_SOF.1		TOE における暗号化メカニズムを除く、確率的または順列的セキュリティメカニズムを有するセキュリティ機能に対して、機能強度分析を実施した結果について記述されている。
AGD ガイダンス文書	AGD_ADM.1 AGD_USR.1	クイックスタートガイド Quick Start Guide	これらの文書は、関係者が TOE のセキュアな配付，設置，運用を実行するための手順が記述されている。
ADO 配付と運用	ADO_IGS.1	・サービスマニュアル[概要編] ・サービスマニュアル[サービス編] ・SERVICE MANUAL ・SERVICE HANDBOOK GP-1060 for e-STUDIO352/452, e-STUDIO353/453	
	ADO_DEL.1	・e-STUDIO シリーズ TOE 配付手順書 ・システムソフトウェア配付手順書	

表 8.3-2 セキュリティ保証手段一覧

※ガイダンスに記されている機種番号が仕向(国)ごとに異なるが、これはガイダンスに記されていない機種はその仕向(国)に出荷されないためである。(日本向けガイダンスに e-STUDIO520 などが記載されていない等)

8.4 PP 主張根拠

本 ST に適合する PP はない。