TOSHIBA

e-STUDIO520/600/720/850用
システムソフトウェア
Security Target

2006年03月07日
Ver 2.1

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-STUDIO520/600/720/850 用 システムソフトウェア Security Target
ST バージョン	:	Ver2.1
ST 作成日	:	2006 年 03 月 07 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-STUDIO520/600/720/850 用 システムソフトウェア
【英語名】	:	System Software for e-STUDIO520/600/720/850
TOE バージョン	:	V1.0
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 2.1 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 では、東芝テック株式会社製のデジタル複写機、e-STUDIO520/600/720/850 に実装されるシステムソフトウェアのセキュリティ機能を定めている。
e-STUDIO520/600/720/850 は、ユーザが用意したユーザ文書を内部に取り込み、様々な形で出力する（以下、e-STUDIO 一般機能という）ものである。
TOE は、e-STUDIO520/600/720/850 のシステムソフトウェアであり、e-STUDIO 一般機能とセキュリティ機能を合わせ持っている。
尚、TOE のセキュリティ機能であるデータ消去機能は、e-STUDIO520/600/720/850 で使用中の HDD からファイル削除されるユーザ文書データを完全に消去する機能を提供する。
「完全に消去する」とは、復元不可能な方式で消去することを指す。
また、データ消去機能は、HDD の廃棄・交換時に e-STUDIO520/600/720/850 の HDD から、ユーザ文書データを一括して完全に消去する機能も提供する。この機能により、HDD 内に残留していたユーザ文書データを完全に消去することができる。

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 2.1 パート 2 適合
- CC バージョン 2.1 パート 3 適合
- 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。

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）：デジタル複写機
  コピー，プリンタ，ファックス等の機能を 1 台に集約した多機能周辺機器。

- e-STUDIO
  TOE が実装されている MFP。
  具体的には、e-STUDIO520/600/720/850（e-STUDIO520，e-STUDIO600，e-STUDIO720，e-STUDIO850）を指す。

- HDD
  Hard Disk Drive

- ユーザ文書データ
  e-STUDIO 一般機能を利用して、e-STUDIO 利用者の文書をデジタル化したデータ。
  ただし、通常の FAX 受信データは送信者のデータであり e-STUDIO 利用者のデータではないため、ユーザ文書データではない。

- ファイリングボックス
  e-STUDIO 利用者は、指定したファイリングボックスにユーザ文書データを保存することができ、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。
  尚、ファイリングボックスには共有ボックスとユーザボックスがあり、以下にそれぞれについて説明する。
  - 共有ボックス
    全てのユーザが、このボックスに保存されているユーザ文書データに対して参照や編集，印刷を行うことができる。
  - ユーザボックス
    全てのユーザは、ユーザボックスを作成し、ボックス名を付けることができ、作成したボックスには、パスワードをそれぞれ設定することができる。
    このボックスの作成者は、保存されているユーザ文書データに対して参照や編集，印刷を行うことができる。
    但しパスワードは、TOE が想定する脅威に対抗するデータ消去機能である、TOE セキュリティ対策方針に寄与するものではない。

- 共有フォルダ
  e-STUDIO 利用者は、共有フォルダにユーザ文書データを保存し、それを取得することができる。
  尚、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。

- GP-1060
  e-STUDIO520/600/720/850 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。
- 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-STUDIO520/600/720/850 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-STUDIO520，e-STUDIO600，e-STUDIO720，e-STUDIO850 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-STUDIO520/600/720/850 は、一般的なオフィス等に設置され、単独で複写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。

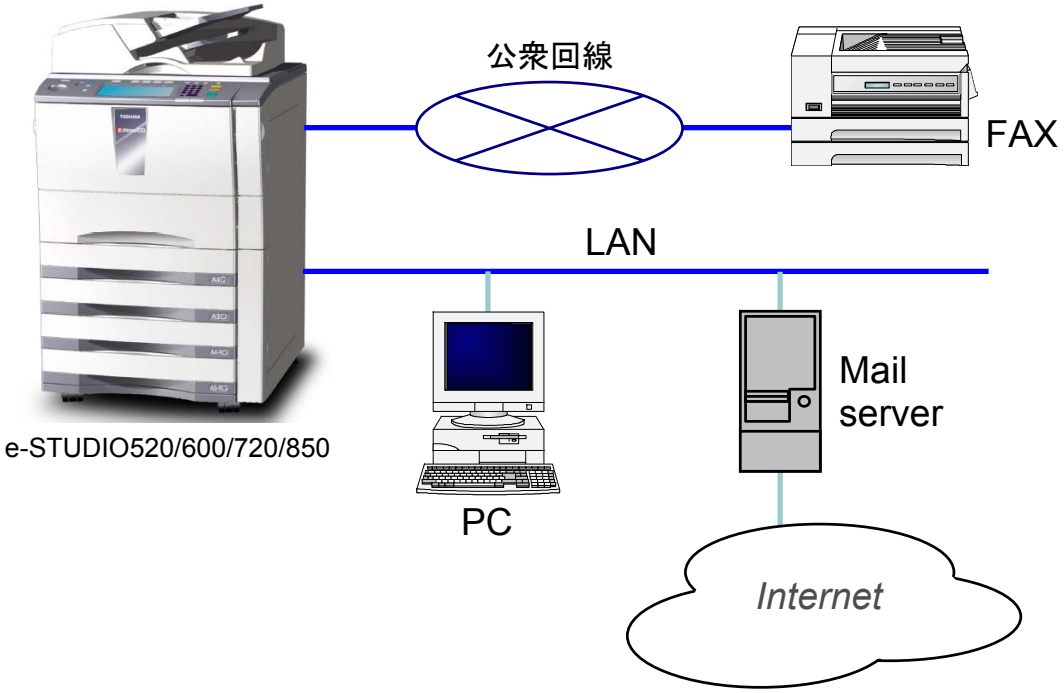

図 2.1　e-STUDIO のネットワーク環境での利用

MFP は、ユーザ文書を内部に取り込んで処理し、出力を行うデジタル複写機である。

出力に関係する処理には、コピー，プリント，スキャン，FAX 送信，FAX 受信の処理があり、各処理が完了したユーザ文書データは、e-STUDIO 利用者が HDD のファイリングボックス、および共有フォルダに保存する場合を除き、OS が提供するファイル削除機能で削除される。

HDD の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は、e-STUDIO 利用者が文書の重要性、及び機密性を判断して管理し、不要と判断した時点で削除する。この場合も、OS が提供するファイル削除機能で削除される。

しかし、OS が提供するファイル削除機能で削除した場合、OS が管理する FAT（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の実体が残ってしまっている。

この場合、OS のツールの知識を有する攻撃者であれば HDD に直接アクセスして、該当するユーザ文書データが書き込まれている領域をリバースエンジニアリングすることで、ファイル削除されたユーザ文書データが復元される可能性が脅威として存在する。

TOE のセキュリティ機能であるデータ消去機能は、ファイル削除されるユーザ文書データを完全に消去する機能と、HDD の廃棄・交換時に残留するユーザ文書データを一括して完全に消去する機能を提供する。

「完全に消去する」とは、復元不可能な方式で消去することを指す。

また、HDD のファイリングボックス、および共有フォルダに残留するユーザ文書データは、HDD が e-STUDIO 利用者にとって管理外となる時（廃棄・交換時など）に、e-STUDIO 利用者によって削除されずに HDD のファイリングボックス、および共有フォルダに残留しているユーザ文書データを指す。

尚、データ消去機能は、GP-1060 が装着されることによって有効となる。

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-STUDIO520/600/720/850	e-STUDIO520：52 枚／分 e-STUDIO600：60 枚／分　A4、または letter サイズにおける e-STUDIO720：72 枚／分　コピー／プリント速度 e-STUDIO850：85 枚／分
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 V1.0	e-STUDIO520/600/720/850 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：　V027.000 2 米英：V034.000 3 欧英：V030.000 4 仏：　V026.000 6 伊：　V027.000 10 独：　V026.000 7 西：　V026.000 11	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

2.2 製品の機能と TOE

本製品は、OS（VxWorks）上に e-STUDIO520/600/720/850 に必要な IT 機能、すなわち、コピー，プリント，スキャン， FAX 送信，FAX 受信，ファイリングボックス文書削除処理の各処理（以下、e-STUDIO 一般機能という）、及びデータ消去機能を搭載した専用機である。

TOE は、e-STUDIO520/600/720/850 のソフトウェアであり、e-STUDIO520/600/720/850 内の ROM に存在し、e-STUDIO520/600/720/850 全体を制御する。

e-STUDIO520/600/720/850 を立ち上げると、通常モードで起動される。通常 e-STUDIO 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（2.2.2.2 節参照）である。

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。

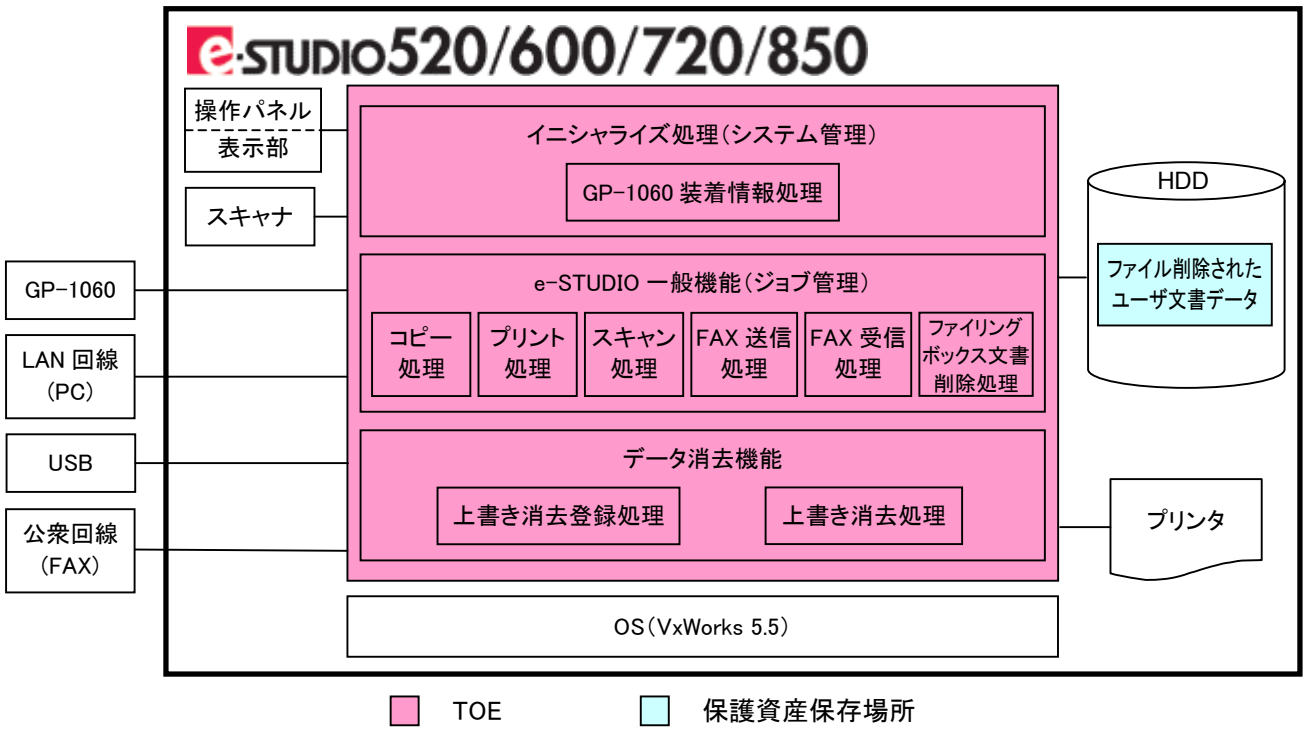

図 2.2.1 通常モード時の製品の構成

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 の装着確認を行う。

データ消去機能が有効になっていることを e-STUDIO 利用者に知らせるために、本体フロントカバーの機種名と、操作パネルの表示部に TOE 名称と TOE バージョン「SYS V1.0」を表示する。

(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。
- 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、および共有フォルダ文書削除処理

操作パネル、又は LAN 回線を経由して、PC から e-STUDIO520/600/720/850 内の 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）

(1) 上書き消去登録処理
- 上記 e-STUDIO 一般機能それぞれの処理において、ダストボックスにファイル削除する作業領域上のユーザ文書データの格納領域を登録する。
- 上記 e-STUDIO 一般機能（7）において、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、削除操作が行われると、ダストボックスにファイル削除するユーザ文書データの格納領域を登録する。

(2) 上書き消去処理

本 TOE は、ダストボックスに登録されたユーザ文書データがあるかどうかを監視し、ダストボックスにユーザ文書データが登録されていると、その格納領域を完全に消去する。
その際使用される消去方式は、米国国防総省方式（DoD5220.22-M）である。
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。

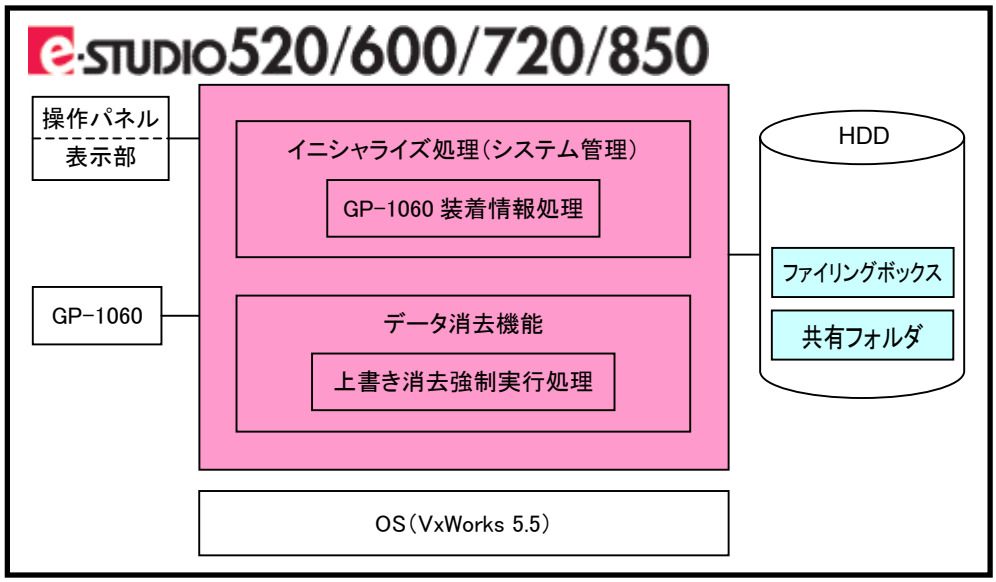

図 2.2.2 自己診断モード時の製品の構成

2.2.2.1 自己診断モード時の e-STUDIO 一般機能

・GP-1060 装着情報処理

GP-1060 の装着確認を行う。データ消去機能が有効になっていることを e-STUDIO 利用者に知らせるために、TOE 名称と TOE バージョンを表示部に表示する。

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

本 TOE は自己診断モードからファイルの全削除を行う時、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。

その際使用される消去方式は、米国国防総省方式（DoD5220.22-M）である。

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　e-STUDIO 利用者

e-STUDIO520/600/720/850 における e-STUDIO 一般機能を利用するユーザ。

2.3.2　e-STUDIO 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存在しない。

2.3.3　サービスエンジニア

e-STUDIO520/600/720/850 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-STUDIO520/600/720/850 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

本 TOE の保護資産は、ファイル削除時に HDD に残っているユーザ文書データの実体である。

尚、ファイル削除のタイミングは以下の通りである。

・ ジョブ終了時
・ ジョブ削除時
・ ジョブキャンセル時
・ 保存されているユーザ文書データ削除時
・ ファイル全削除

※ ジョブとは、e-STUDIO520/600/720/850 におけるコピーやプリントなどの e-STUDIO 一般機能の処理を示す。

※ FAX で自動受信したデータは FAX 送信者のデータであって受信者のユーザ文書データではないため、保護資産の対象とはならない。

※ ファイリングボックス、および共有フォルダに保存され、有効期限が経過したユーザ文書データは、保護資産の対象とはならない。

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-STUDIO520/600/720/850 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 e-STUDIO 利用者、または非関係者が既存のツールを使用して、e-STUDIO520/600/720/850 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リバースエンジニアリングすることで、ファイル削除されたユーザ文書データを復元し、解読するかもしれない。

・T.STOREDATA_ACCESS

悪意を持った e-STUDIO 利用者、または非関係者が既存のツールを使用して、ファイル全削除を行った e-STUDIO520/600/720/850 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し、解読するかもしれない。

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-STUDIO520/600/720/850 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、ファイル全削除を行った e-STUDIO520/600/720/850 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 管理者はファイル全削除時に、HDD の上書き消去強制実行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-STUDIO520/600/720/850 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-STUDIO520/600/720/850 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-STUDIO520/600/720/850 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-STUDIO520/600/720/850 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。
  その際使用される消去方式は、米国国防総省方式（DoD5220.22-M）である。

（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 STUDIO520/600/720/850 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、ファイル全削除を行う e-STUDIO520/600/720/850 の HDD のユーザ文書データに対し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。
  その際使用される消去方式は、米国国防総省方式（DoD5220.22-M）である。

（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-STUDIO520/600/720/850 用システムソフトウェア構成リスト e-STUDIO520/600/720/850 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	取扱説明書[共通編] Operator`s Manual for Basic Function[北米版] Operator`s Manual for Basic Function[欧州版] Data Overwrite Kit
	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	取扱説明書[共通編] Operator`s Manual for Basic Function[北米版] Operator`s Manual for Basic Function[欧州版] Data Overwrite Kit インサーションシート Insertion Sheet
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-STUDIO520/600/720/850
	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

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-STUDIO520/600/720/850 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、ファイル全削除時に HDD の上書き消去強制実行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ファイル全削除を行った e-STUDIO520/600/720/850 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 によって完全に消去を行い、**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-STUDIO520/600/720/850 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 によって一括して完全な消去を強制的に行い、**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、ファイル全削除を行った e-STUDIO520/600/720/850 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。

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-STUDIO520/600/720/850 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-STUDIO520/600/720/850 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、ファイル全削除を行う e-STUDIO520/600/720/850 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-STUDIO520/600/720/850 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、ファイル全削除を行うと、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-STUDIO520/600/720/850 用システムソフトウェア構成リスト ・e-STUDIO520/600/720/850 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	・取扱説明書[共通編] ・Operator`s Manual for Basic Function[北米版] ・Operator`s Manual for Basic Function[欧州版] ・Data Overwrite Kit	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	・取扱説明書[共通編] ・Operator`s Manual for Basic Function[北米版] ・Operator`s Manual for Basic Function[欧州版] ・Data Overwrite Kit ・インサーションシート ・Insertion Sheet	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-STUDIO520/600/720/850	
	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

8.4 PP 主張根拠

本 ST に適合する PP はない。