TOSHIBA

e-STUDIO3511/4511用
スクランブラボード GP-1031
Security Target

TOEバージョン：V2.0

2004年11月18日

Ver 1.6

東芝テック株式会社

変更履歴

バージョン	変更日	変更内容	変更箇所	担当
1.0	2004/07/29	新規作成		仲吉/日永
1.1	2004/09/01	・JEITA殿 ST Ver1.0指摘事項(1-1, 2-1, 2-2, 2-3, 2-4, 4-2)の反映 ・ST Ver1.0見直しによる修正	P.5-6, P.8, P.10, P.14-18, P.21-23, P.25-27	仲吉/日永
1.2	2004/09/29	・JEITA殿 ST Ver1.0指摘事項(2-5, 2-6, 5-2)の反映 ・ST Ver1.1見直しによる修正	P.5, P.13-17, P.19, P.21-22, P.27, P.39	仲吉/日永
1.3	2004/10/14	・JEITA殿 ST Ver1.2指摘事項(1-1, 2-1, 2-2, 2-3, 3-1, 8-1, 8-2)の反映 ・JEITA殿 ST Ver1.2に対する所見報告書ASE001-01の内容反映 ・ST Ver1.2見直しによる修正	P.5, P.8-10, P.13, P.15-17, P.20-23, P.30-31, P.34, P.36, P.38-40	仲吉/日永
1.4	2004/11/05	・JEITA殿との打ち合わせ(04/10/20)での指摘事項の反映	P.5-6, P.9, P.13-16, P.20, P.23, P.28, P.30, P.33, P.35-36, P.38	仲吉/日永
1.5	2004/11/09	・JEITA殿 ADV指摘事項(04/10/22)FSP-8の反映 ・ST Ver1.4見直しによる修正	P.5, P.13, P.16, P.20-22	仲吉/日永
1.6	2004/11/18	・JEITA殿 ST指摘事項(04/11/12)(2-1, 2-2, 2-3, 2-4, 3-1, 6-1, 6-2, 8-1, 8-2, 8-3, 8-4, 8-5)の反映 ・JEITA殿 ST Ver1.5に対する所見報告書ASE002-01の内容反映	P.5, P.10, P.14, P.17, P.20, P.23-24, P.28, P.31, P.33, P.34-37	仲吉/日永

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-STUDIO 3511/4511用 スクランブラボード GP-1031 Security Target
STバージョン :Ver 1.6
ST作成日 :2004年11月18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 :スクランブラボード GP-1031【日本語名】
Scrambler Board GP-1031【英語名】
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 :EAL2
キーワード :デジタル複合機, e-STUDIO, スクランブラボード, GP-1031, ハードディスク暗号化, 東芝テック
CCのバージョン :JIS X 5070-1:2000 セキュリティ技術－情報技術セキュリティの評価基準－第1部:総則及び一般モデル
JIS X 5070-2:2000 セキュリティ技術－情報技術セキュリティの評価基準－第2部:セキュリティ機能要件
JIS X 5070-3:2000 セキュリティ技術－情報技術セキュリティの評価基準－第3部:セキュリティ保証要件
CCIMB Interpretations-0407

尚、日本語訳は、以下のものを使用している。

- 「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～パート3」平成13年1月翻訳 第1.2版
  情報処理振興事業協会(IPA) セキュリティセンター発行
- 「補足-0407」
  独立行政法人情報処理推進機構(IPA) セキュリティセンター発行
- 「補足-0210第2版」
  独立行政法人情報処理推進機構(IPA) セキュリティセンター発行

1.2 ST概要

本STは、東芝テック株式会社製 デジタル複合機e-STUDIO 3511/4511用のスクランブラボード GP-1031のセキュリティ仕様を定めたセキュリティターゲットである。
e-STUDIO 3511/4511は、一般的なオフィス等に設置されるデジタル複合機で、コピー、プリント、スキャン、ファイリングボックス及びFAX機能を用いることで、オフィス業務を電子的に支援する製品である。
スクランブラボード GP-1031は、e-STUDIO 3511/4511にオプションで実装され、ユーザ文書データをHDDに書込み及び読出しを行う際に、ユーザ文書データの暗号化及び復号を行う製品である。

1.3 CC適合

本STは、以下のCCに適合している。

- 機能要件は、JIS X 5070 第2部適合である。
- 保証要件は、JIS X 5070 第3部適合である。
- 評価保証レベルは、EAL2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、略語は以下のものである。

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
- SFP(Security Function Policy):セキュリティ機能ポリシー
- SOF(Strength Of Function):機能強度
- TSF(TOE Security Functions):TOEセキュリティ機能
- TSP(TOE Security Policy):TOEセキュリティポリシー

- TSC(TSF Scope of Control):TOEセキュリティ機能制御範囲

TOE関連の用語、略語

- e-STUDIOアプリケーション
  コピー、プリンタ、スキャン、FAX及びファイリング機能を利用した時に動作するソフトウェア群。

- e-STUDIO利用者機能
  デジタル複合機における、コピー、プリンタ、スキャン、FAX及びファイリング機能。

- FAT (File Allocation Table) 情報
  ハードディスク装置に格納されているファイルの管理領域の情報。

- ROMデータ
  e-STUDIO 3511/4511用の制御ソフトウェアで、Flash ROMに格納されるデータ。

- TOEの関係者
  e-STUDIO利用者、及びe-STUDIO管理者，サービスエンジニア，e-STUDIO非関係者。

- UIデータ
  タッチパネル上に表示される操作メッセージや表示アイコンなどに使用する各国語向けの言語データ。

- Webユーティリティ
  PC上で動作するWebブラウザベースのソフトウェア。
  e-STUDIO管理者がe-STUDIOの設定を行ったり、e-STUDIO利用者がファイリングボックスに対し編集、印刷を行なうことができる。

- 暗号鍵作成会社
  「FIPS140-2の統計的乱数性の検定に適合し、機密性と一意性を保証された暗号鍵」を作成する会社。
  暗号鍵は鍵コードとしてメーカーに提供される。

- 暗号鍵データ
  e-STUDIO管理者により入力された鍵コードが変換され、電子的に保存されている128bitのデータ。
  暗号化/復号操作で使用される暗号鍵は、パリティビットが除かれて112bitとなる。

- 解読装置
  HDD内のデータを読み出し、解読する装置。

- 鍵コード
  e-STUDIO管理者に提供される封筒に記載された、アルファベット(A～F)と数字(0～9)から成る暗号鍵のコード。

- サービスマンコール表示
  e-STUDIO 3511/4511の障害や故障、セキュリティ侵害の可能性検出時において、サービスエンジニア呼び出しの旨を示すメッセージ表示。

- スクランブラボード
  暗号化/復号操作を司るハードウェア(基板)単体。

- スクランブラボード GP-1031
  TOE。暗号化/復号操作を司るハードウェアと、関連するソフトウェア。

- 正規の社員
  e-STUDIO 3511/4511のメーカー、または守秘義務契約を締結しているメーカーの関連会社、販売会社の社員。

- デジタル複合機：MFP (Multi Function Peripherals)
  コピー、FAX、プリンタなどの機能を1台に集約した多機能周辺機器。

- ファイリングボックス
  ユーザ文書データを保存するために、MFPのHDD内に生成されるフォルダ。

- ユーザ
  e-STUDIO 3511/4511のコピー機能などの一般機能を利用するお客様を指す。具体的には、e-STUDIO利用者。

- ユーザ文書
  ユーザが扱う機密情報などの重要文書を含む文書。

- ユーザ文書データ
  ユーザ文書をデジタル化したデータ。

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、TOEの概要，TOEの関係者，物理的構成，論理的構成，保護資産、及びTOEの機能について記述する。

2.1 TOEの概要

2.1.1 TOE種別

TOEは、ユーザ文書データをHDDに書込み及び読出しを行う際にユーザ文書データの暗号化及び復号を行う、スクランブラボード、及びスクランブラボードを動作させるソフトウェアから成る製品である。

2.1.2 利用目的

スクランブラボードGP-1031はe-STUDIO 3511/4511において、HDDに格納されるユーザ文書データを暗号化及び復号する製品である。
HDDに格納されたユーザ文書データは、コピー機能、プリント機能等の完了後にユーザ文書残存データとなる。本TOEは、そのユーザ文書残存データを保護することを目的としている。

2.1.3 利用環境

e-STUDIO 3511/4511は、一般的なオフィス等に設置され、内部ネットワーク並びに電話回線に接続して使用される。

図2.1-1に、e-STUDIO 3511/4511の想定する一般的な利用環境を示す。

図2.1-1 e-STUDIO 3511/4511想定利用環境

※本図は代表的な接続例を示す。

e-STUDIO 3511/4511想定利用環境における構成要素を以下に示す。

名称	機能
内部ネットワーク	e-STUDIO 3511/4511が接続されている、ローカルなネットワーク。
電話回線	e-STUDIO 3511/4511が接続されている、電話回線。
外部ネットワーク	ローカルなネットワーク同士を専用線で接続した世界規模のネットワーク(インターネット)。
Firewall	内部ネットワークと外部ネットワークとの間に、外部からの不正なアクセスを 防ぐ目的で設置されるルータやPC。
クライアントPC	内部ネットワークに接続し、e-STUDIO利用者が使用するPC。

2.1.4 主な機能

e-STUDIO 3511/4511はデジタル複合機であり、TOEは保護資産であるHDD内のユーザ文書残存データを暗号化/復号する機能を提供する。
以下に、ユーザ文書残存データが発生する機能、及びそれに関連するセキュリティ機能を示す。

2.1.4.1 TOEの機能

TOEが提供する主な機能は以下の通りである。

(1) 暗号化/復号機能

e-STUDIO 3511/4511のe-STUDIO利用者機能である、コピー機能、プリント機能、スキャン機能、ファイリングボックス機能、FAX機能において、HDDに書込まれるユーザ文書データの暗号化/復号を行う機能。

2.1.4.2 e-STUDIO 3511/4511の機能

e-STUDIO 3511/4511が提供する主な機能で、実行時にユーザ文書残存データが発生するものは、以下の通りである。

(1) コピー機能

ユーザ文書をスキャナエンジンから読込み印刷する機能。
ボタン操作により、ユーザ文書をスキャナエンジンから読込み、HDDに一時的に保存する。HDDに一時的に保存されたユーザ文書データを印刷する。
印刷完了後、ユーザ文書データを、内部ネットワークで接続されたクライアントPCのフォルダに保存することもできる。

(2) プリント機能

e-STUDIO 3511/4511と接続されたクライアントPCから印刷する機能。
クライアントPCから送られたユーザ文書データを、HDDに一時的に保存する。 HDDに一時的に保存されたユーザ文書データを印刷する。

(3) スキャン機能

ユーザ文書をスキャナエンジンから読込み、HDDに一時的に保存する機能。
HDDに一時的に保存されたユーザ文書データに対して、以下の操作ができる。

・クライアントPCのフォルダに保存
ユーザ文書データを、内部ネットワークで接続されたクライアントPCの記憶媒体上のフォルダに保存する。

・Eメールとして送信
ユーザ文書データを、操作パネル上で指定されたメールアドレスに送信する。

(4) ファイリングボックス機能

ファイリングボックスに保存されたユーザ文書データを管理する機能。
コピー機能、プリント機能、スキャン機能、FAX送信機能、FAX受信機能実行時に、ユーザ文書データをファイリングボックスに保存することができる。
ファイリングボックス内のユーザ文書データに対しては、Webユーティリティにより、印刷、表示、編集、削除、プロパティ表示を行なうことができる。

(5) FAX機能

・FAX送信
ユーザ文書をスキャナエンジンから読込み、電話回線で接続されたFAX機器に送信する機能。
ユーザ文書をスキャナエンジンから読込み、HDDに一時的に保存する。HDDに一時的に保存されたユーザ文書データを、FAX機器に送信する。

・FAX受信
FAX機器からユーザ文書データを受信し、印刷する機能。
電話回線を介して受信したユーザ文書データをHDDに一時的に保存する。 HDDに一時的に保存されたユーザ文書データを印刷する。

・インターネットFAX送受信
外部ネットワークを介して、クライアントPCまたはインターネットFAX機との間で、ユーザ文書データの送受信を行う機能。

・オンランプゲートウェイ
FAX機器から受信したユーザ文書データを、ネットワークに接続されたクライアントPCやインターネットFAX機に送信する機能。
電話回線を介して受信したユーザ文書データは、HDDに一時的に保存される。 HDDに一時的に保存されたユーザ文書データを、外部ネットワーク上のクライアントPCやインターネットFAX機に送信する。

・オフランプゲートウェイ
ネットワークに接続されたクライアントPCやインターネットFAX機から受信したユーザ文書データを、FAX機器に送信する機能。
ネットワークを介して受信したユーザ文書データは、HDDに一時的に保存される。 HDDに一時的に保存されたユーザ文書データを、FAX機器に送信する。

(6) HDDデータ全消去機能

HDD上の全てのユーザ文書データ、及びユーザ文書残存データを消去する機能。

2.2 TOEの関係者

2.2.1 TOEの正規の関係者

本TOEにおける正規の関係者は、以下のものである。正規の関係者の役割、信頼度、知識について以下に記述する。

- e-STUDIO利用者
  【役割】 e-STUDIO 3511/4511におけるコピー等、デジタル複合機の一般的な機能を利用する。
  【信頼度】 信頼度は必ずしも高いとは言えない。悪意を持った利用者がいる可能性がある。
  【知識】 ネットワークに関する知識は必要ない。

- e-STUDIO利用部門の責任者
  【役割】 e-STUDIO管理者を任命する。
  【信頼度】 信頼度は高い。
  【知識】 e-STUDIO利用部門の各メンバーの信頼度やスキルに関する知識を有する。

- e-STUDIO管理者
  【役割】 e-STUDIO 3511/4511に関する運用管理を行う。
  TOEに関しては、以下の役割を担う。
  - スクランブラボード GP-1031導入時に、インストール作業を行うサービスエンジニアが、メーカーまたはその関連会社や販売会社の社員であることを確認する。
  - スクランブラボード GP-1031導入時のインストール作業において、サービスエンジニアからの依頼により、鍵コードが記載された封筒を開封して、それに記載されている鍵コードの入力を行う。鍵コード入力後は、その封筒を厳重に管理する。
  - e-STUDIO 3511/4511を廃棄または交換する前に、サービスエンジニアにその旨を連絡し、HDDデータ全消去の依頼を行う。

  【信頼度】 e-STUDIO利用部門の責任者より、e-STUDIO管理者として任命された者であり、信頼度は高い。TOEに対して、悪意をもった行為は行わない。
  【知識】 e-STUDIO 3511/4511の利用、運用管理、及びネットワークに関する知識を有する。

- サービスエンジニア
  【役割】 e-STUDIO 3511/4511の設置場所(オンサイト)において、e-STUDIO 3511/4511の設置、インストール、及び保守業務を行う。
  TOEに関しては、以下の役割を担う。
  - スクランブラボード GP-1031のインストールとして、スクランブラボードの装着，ソフトウェアのインストール，鍵コード入力後のHDDの初期化操作などの作業を行う。
  - e-STUDIO管理者からの依頼により、e-STUDIO 3511/4511の廃棄または交換時にHDDデータ全消去の作業を行う。

  【信頼度】 e-STUDIO 3511/4511のメーカー、または守秘義務契約を締結しているメーカーの関連会社、販売会社の社員であり、信頼度は高い。TOEに対して悪意をもった行為は行わない。
  【知識】 e-STUDIO 3511/4511に関する保守技術、及びe-STUDIO 3511/4511に関するセキュリティの知識に精通している。ITや情報処理技術については特に限定はしない。

2.2.2 TOEの正規でない関係者

本TOEにおける正規でない関係者は以下のものである。正規でない関係者の役割、信頼度、知識について以下に記述する。

- e-STUDIO非関係者
  【役割】 特定の役割はなく、e-STUDIO 3511/4511に物理的、または外部ネットワークや電話回線を介してアクセス可能な人。
  【信頼度】 悪意を持った第三者がいる可能性がある。
  【知識】 一般的なITの知識を有している。

2.3 物理的構成

TOEを構成するハードウェアとソフトウェアの範囲を以下に示す。

2.3.1 ハードウェア構成

図2.3-1に、スクランブラボードを装着したe-STUDIO 3511/4511のハードウェア構成を示す。

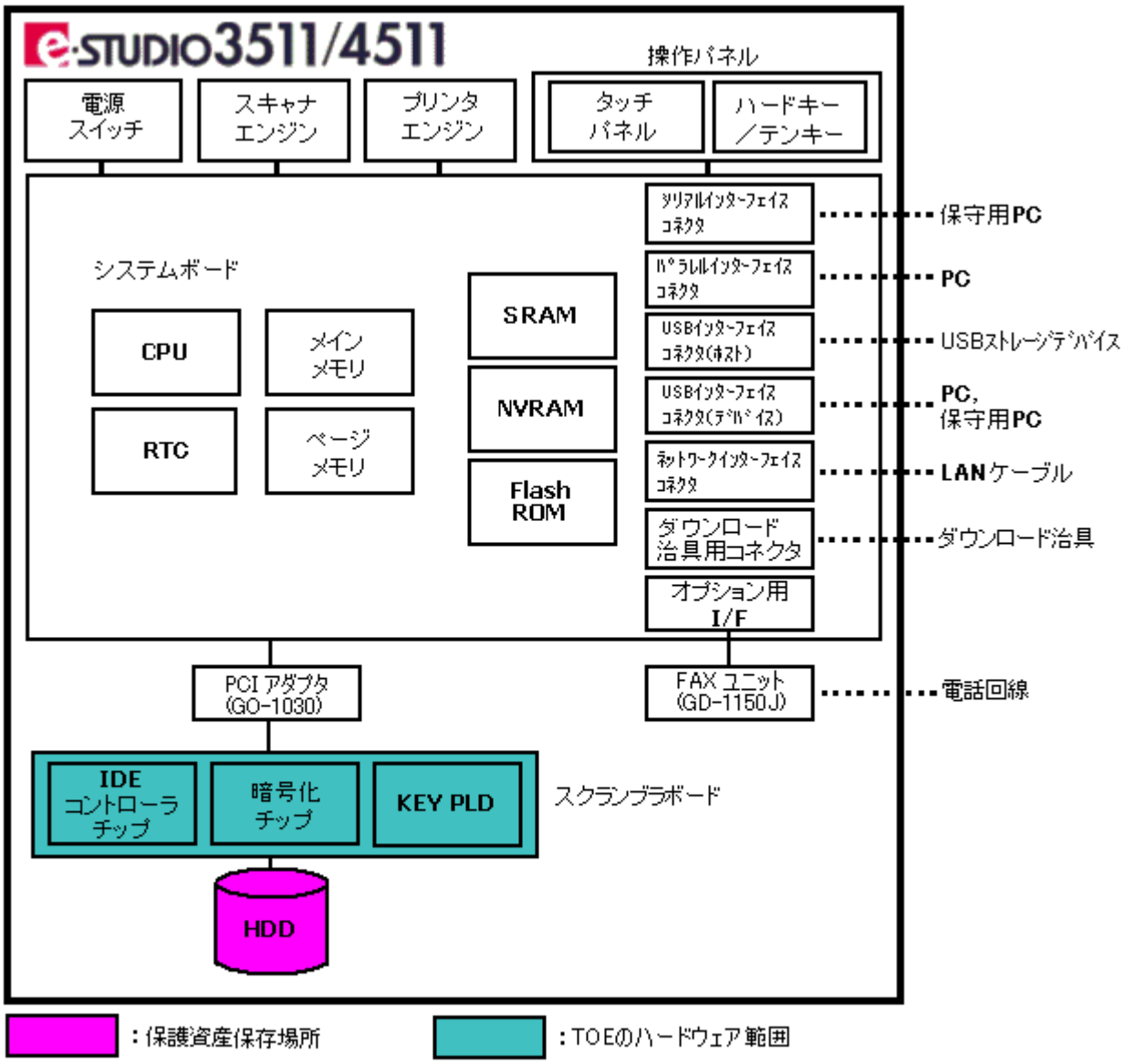

図2.3-1 スクランブラボード装着時のe-STUDIO 3511/4511のハードウェア構成

※ 本TOEのソフトウェアは、システムボード上のFlash ROMに格納される。

2.3.2 ハードウェアのTOE範囲

ハードウェアのTOE範囲は、以下のものである。

- スクランブラボード
  - IDEコントローラチップ
  - KEY PLD
  - 暗号化チップ

2.3.3 ハードウェア構成要素

ハードウェア構成における構成要素を以下に示す。

ハードウェア	仕様
スキャナエンジン	ユーザ文書をユーザ文書データに変換する機器。
プリンタエンジン	HDD上のユーザ文書データを紙へ印刷する機器。
操作パネル	e-STUDIO 3511/4511の操作を行うための機器。 「タッチパネル」「ハードキー/テンキー」で構成されている。
タッチパネル	タッチパネル付グラフィック液晶ディスプレイ。
ハードキー/テンキー	コピー機能におけるコピー操作を行うキー(ボタン)。 テンキーは0から9までの数字キー(ボタン)。
システムボード	e-STUDIO 3511/4511全体の機能の制御を行なう基板。 「CPU」「メインメモリ」「ページメモリ」「NVRAM」「SRAM」「Flash ROM」「RTC」が実装されている。
CPU	システムの制御を行うための中央演算処理装置。
メインメモリ	起動時にFlash ROMからシステムプログラムなどがロードされ、実行時のメモリとして使用される。
ページメモリ	原稿読取り時や印刷時に使用するメモリ。
NVRAM	e-STUDIO 3511/4511の各種設定情報を格納する不揮発性メモリ。設定情報の一部にスクランブラボードの装着有無情報や各種パラメータが含まれる。
SRAM	e-STUDIO 3511/4511の各種設定情報を格納する、リチウムコイン電池により電源バックアップされている揮発性メモリ。設定情報の一部に暗号鍵データが含まれる。
Flash ROM	e-STUDIO 3511/4511、及びスクランブラボードを制御するためのソフトウェアがインストールされている不揮発性メモリ。
RTC	実時間に準じた時間データを発生するIC。
スクランブラボード	HDDにデータを書込むときに暗号化を、データをHDDから読み出すときに復号を行う。 「IDEコントローラチップ」「KEY PLD」「暗号化チップ」が実装されている。
PCIアダプタ (GO-1030)	スクランブラボードを装着するためのオプションボード。
IDEコントローラチップ	HDDへのデータ転送を制御する論理素子(チップ)。
KEY PLD	e-STUDIO 3511/4511起動時にシステムボード上のSRAMからスクランブラボード上に転送される暗号鍵データを保存する揮発性の論理素子(チップ)。
暗号化チップ	HDDに書込むデータを暗号化し、HDDから読出すデータを復号するチップ。
HDD	e-STUDIO 3511/4511に実装されているハードディスク装置。 3.5インチIDEハードディスク。 保護資産が格納される。
シリアルインターフェイス コネクタ	サービスエンジニアの保守情報収集用インターフェイス。 サービスエンジニアが保守情報収集のための専用ソフトウェアを搭載した保守用PCを接続する場合に使用する。
FAXユニット (GD-1150J)	e-STUDIO 3511/4511をFAX機器として使用する際に必要なオプション機器。
オプション用I/F	FAXユニットを装着するためのインターフェイス。
ダウンロード治具用コネクタ	サービスエンジニアのプログラム及びUIデータダウンロード用の治具用コネクタ。 サービスエンジニアが、システムボードのソフトウェアまたはUIデータが書込まれているダウンロード治具(基板)を、ダウンロード治具用コネクタに接続し、スクランブラボードのソフトウェアをシステムボード上のFlash ROMに、UIデータをHDDにそれぞれダウンロードする。
USBインターフェイスコネクタ (ホスト)	USBインターフェイス(アップストリームポート)。 サービスエンジニアが、システムボードのソフトウェアまたはUIデータが書込まれているUSBストレージデバイスを接続し、スクランブラボードのソフトウェアをシステムボード上のFlash ROMに、UIデータをHDDにそれぞれダウンロードする。
USBインターフェイスコネクタ (デバイス)	USBインターフェイス(ダウンストリームポート)。 ・PCをダイレクトに接続して、e-STUDIO 3511/4511をプリンタとして利用する際に使用される。 ・サービスエンジニアが保守情報収集のための専用ソフトウェアを搭載した保守用PCを接続する場合に使用する。
パラレルインターフェイス コネクタ	IEEE1284インターフェイス。 PCをダイレクトに接続して、e-STUDIO 3511/4511をプリンタとして利用する際に使用される。
ネットワークインターフェイス コネクタ	有線LANのためのネットワーク用インターフェイス。 ネットワーク上のデータ送受信のために使用される。
電源スイッチ	e-STUDIO 3511/4511の電源を入れる、または切るための機器。

2.3.4 ソフトウェア構成

図2.3-2に、スクランブラボード GP-1031を実装したe-STUDIO 3511/4511のソフトウェア構成を示す。

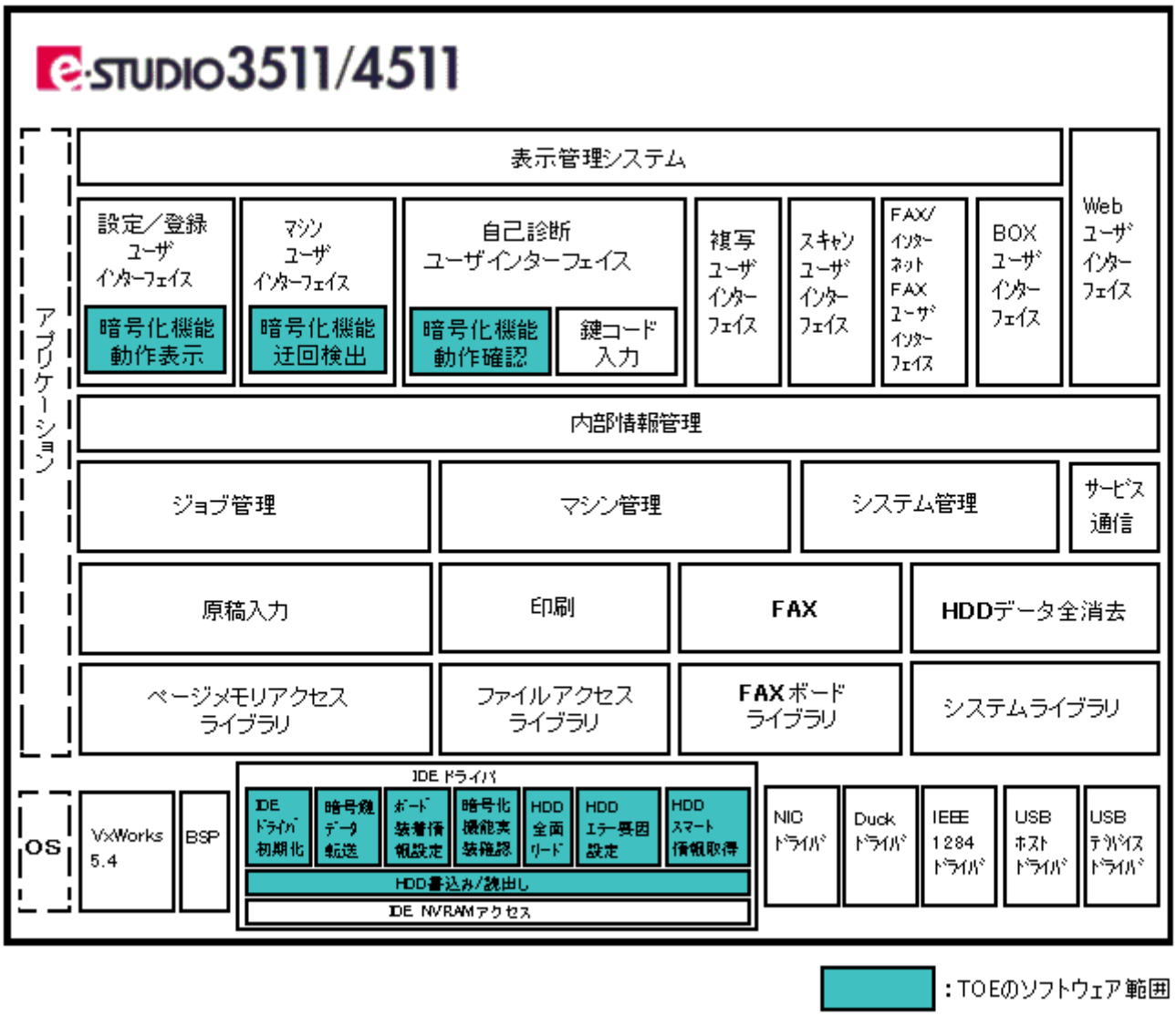

図2.3-2 スクランブラボード GP-1031実装時のe-STUDIO 3511/4511ソフトウェア構成

2.3.5 ソフトウェアのTOE範囲

ソフトウェアのTOE範囲は、以下のものである。

・暗号化機能動作確認　　V 1.1
・IDEドライバ　　V 1.0
　-HDD書込み/読出し
　-IDEドライバ初期化
　-暗号鍵データ転送
　-ボード装着情報設定
　-暗号化機能実装確認
　-HDD全面リード
　-HDDエラー要因設定
　-HDDスマート情報取得
・暗号化機能動作表示　　V 1.0
・暗号化機能迂回検出　　V 1.0

2.3.6 ソフトウェア構成要素

ソフトウェア構成における構成要素を以下に示す。

ソフトウェア	機能
表示管理システム	操作パネルにおけるタッチスクリーンの制御ドライバ。操作パネルで操作画面の表示とタッチスクリーン操作の入力座標データの受け取りを行う。入力座標のデータから、対象機能のユーザインターフェイスプログラムへの実行指示を行う。
自己診断ユーザインターフェイス	サービスエンジニア用の保守用ユーザインターフェイス。保守用の情報確認のための自己診断機能実行時の操作制御を行う。また、鍵コードの入力やスクランブラボードの装着有無の表示、「HDDデータ全消去」の実行指示を行う。
暗号化機能動作確認	スクランブラボードの装着有無情報をNVRAMから読出す要求を行う。
鍵コード入力	TOEのインストーラ。 鍵コードが未入力であることの確認を行い、未入力時に鍵コード入力を許可し、暗号鍵データとしてSRAMへの書込みを行う。
マシンユーザインターフェイス	ジャム解除や、サービスマンコール時(サービスエンジニアによる保守、点検が必要になったとき)の操作制御を行う。
暗号化機能迂回検出	暗号化機能実装確認により設定されたHDDエラー要因情報を取り出し、エラーが検出された時、操作パネルにサービスマンコール表示を行う。
複写ユーザインターフェイス	コピー機能実行時の操作制御を行う。
設定/登録ユーザインターフェイス	アドレス帳登録、カウンタ表示、初期設定の操作制御を行う。
暗号化機能動作表示	暗号化機能正常動作時にTOEの型名とバージョンの表示を行う。
スキャンユーザインターフェイス	スキャン機能実行時の操作制御を行う。
FAX/インターネットFAXユーザインターフェイス	FAX機能、インターネットFAX機能実行時の操作制御を行う。
BOXユーザインターフェイス	ファイリングボックス機能実行時の操作制御を行う。
Webユーザインターフェイス	Webユーティリティの機能実行時の制御を行う。
内部情報管理	e-STUDIO 3511/4511の状態や設定に関するデータを管理し、他のモジュールからの要求を受けて、これらのデータの読出し、書込みを行う。
サービス通信	e-STUDIO 3511/4511の状態に関する情報やカウンタ情報を収集し、データセンタ(エンドユーザのe-STUDIO 3511/4511に関する情報を集中管理する)に送信する。
ジョブ管理	・主な機能の操作において、ユーザ文書の読取り指示や紙への印刷、HDDへのファイルの格納や読出し等のジョブ全般の管理を行う。 ・各機能実行時に、ジョブの制御を行う。 ・保守機能の制御を行う。
マシン管理	・e-STUDIO 3511/4511のウォームアップ動作、予熱動作、スリープ動作、キャリッジ移動動作などの管理を行う。 ・プリンタエンジンの状態を監視する。
システム管理	e-STUDIOアプリケーションの起動、初期化を行う。また、節電タイマーや指定時間後のファイリングボックスのファイル削除などの機能を実現する。
原稿入力	ユーザ文書を、ユーザ文書データに変換するための光学的な読取り制御を行う。
印刷	原稿入力により読込んだ、ユーザ文書データに対して、印刷用のデータ変換処理を行い、紙への印刷を行う。
FAX	・原稿入力により読込んだ、ユーザ文書データに対して、電話回線を介した送信を行う。 ・電話回線を介して受信したユーザ文書データに対して、印刷用のデータ変換処理を行う。
HDDデータ全消去	自己診断ユーザインターフェイスからの実行要求により、HDDのデータ領域(ファイルの内容が記録されている領域)をデータ上書きにより消去する。消去の進捗状況を自己診断ユーザインターフェイスに通知する。
システムライブラリ	・e-STUDIO 3511/4511のマシン制御及びマシン情報の取得を行う。 ・システムボード上のNVRAMからスクランブラボードの装着有無情報の読出しを行う。 ・システムボード上のSRAMに鍵コードの書込みを行う。 ・暗号鍵データが正常に転送されたことを示す情報をSRAMに書込む。
ファイルアクセスライブラリ	HDD内のファイルに対する生成、変更、削除などのアクセス要求を行う。
ページメモリアクセスライブラリ	ページメモリへの入出力制御を行う。
FAXボードライブラリ	FAXユニットとの通信制御を行う。
BSP (ボードサポートパッケージ)	Board Support Packageの略でe-STUDIO 3511/4511のシステムボードに依存する処理をパッケージ化したソフトウェア。
IDEドライバ	HDDにアクセスするための基本的な機能を提供する。 「HDD書込み/読出し」「IDEドライバ初期化」「暗号鍵データ転送」「ボード装着情報設定」「暗号化機能実装確認」「HDD全面リード」「HDDエラー要因設定」「HDDスマート情報取得」「IDE NVRAMアクセス」で構成される。
HDD書込み/読出し	HDDへの全ての書込み/読出し処理を行う。
IDEドライバ初期化	IDEドライバの初期化を行う。

ソフトウェア	機能
暗号鍵データ転送	・システムボード上のSRAM から暗号鍵データを取り出し、スクランブラボード上のKEY PLDに暗号鍵データの転送を行う。 ・転送時に暗号鍵データのチェックを行い、正しければ、システムライブラリを使用して暗号鍵データが正常に転送されたことを示す情報をSRAMに書込む。
ボード装着情報設定	システムボード上のNVRAMにスクランブラボードの装着有無情報の設定を行う。
暗号化機能実装確認	スクランブラボードの装着状態の確認を行う。
HDD全面リード	HDDに書込み/読出しできない領域が無いか確認を行う。
HDDエラー要因設定	暗号化機能実装確認時のHDDエラー要因情報へのアクセスを行う。
HDDスマート情報取得	スマート情報(HDD自身によってHDD内に保存される動作履歴情報。通電時間、電源を入れた回数、内部エラー回数など)の取得を行う。
IDE NVRAMアクセス	・システムボード上のNVRAMにスクランブラボードの装着有無情報の書込みを行う。 ・システムボード上のSRAMから鍵コードの読出しを行う。
NICドライバ	LANに接続されている機器との通信制御を行う。
USBホストドライバ	USBインターフェイスコネクタ(ホスト)に接続されている機器との通信制御を行う。
USBデバイスドライバ	USBインターフェイスコネクタ(デバイス)に接続されている機器との通信制御を行う。
IEEE1284ドライバ	パラレルインターフェイスコネクタに接続されている機器との通信制御を行う。
Duckドライバ	RTCより時刻情報の取得を行う。
VxWorks 5.4	オペレーティングシステム

2.4 論理的構成

2.4.1 論理構成

図2.4-1に、スクランブラボード GP-1031を実装したe-STUDIO 3511/4511の論理構成とそのTOE範囲を示す。

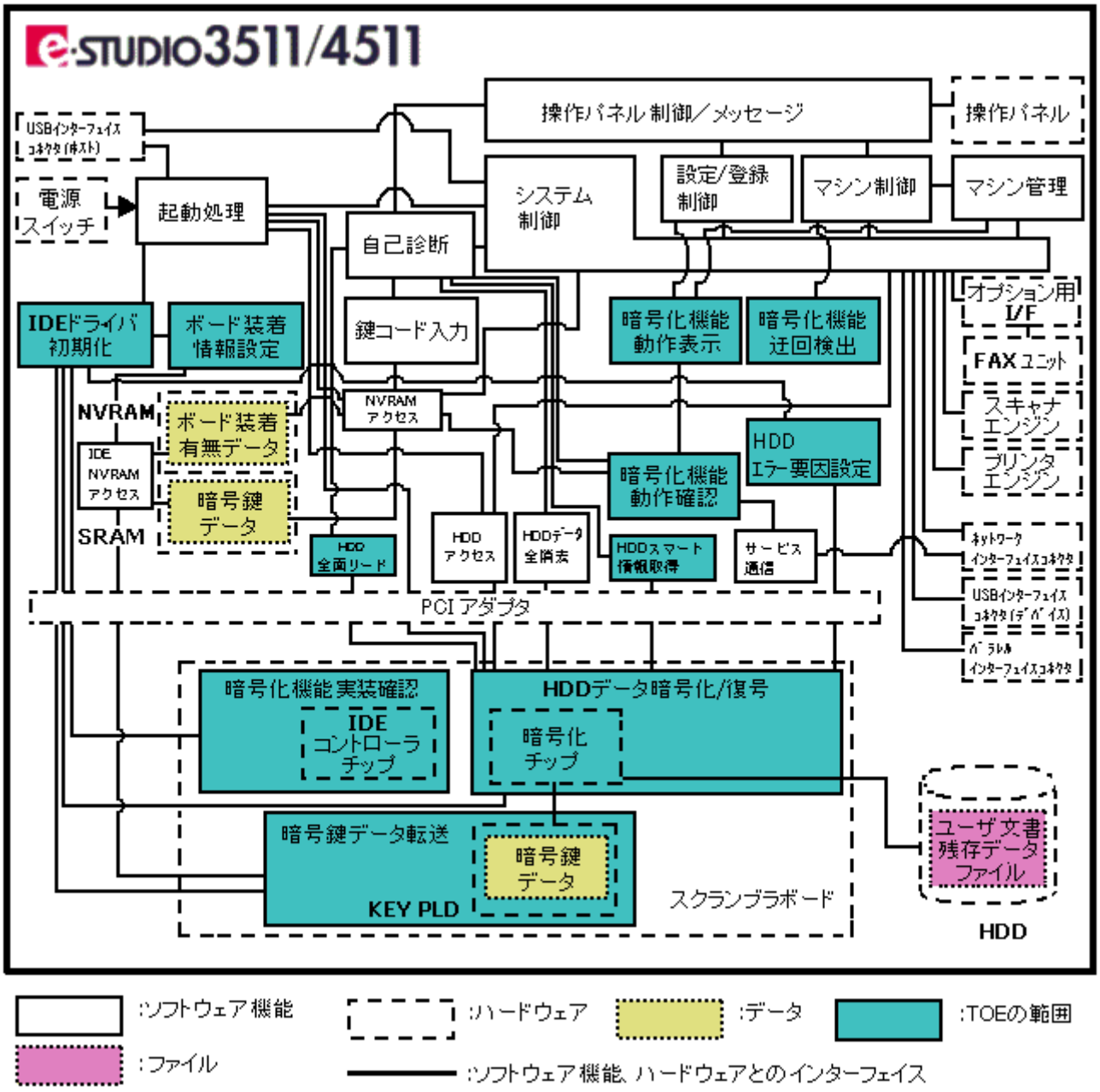

図2.4-1 e-STUDIO 3511/4511の論理構成

2.4.2 論理構成のTOE範囲

論理構成のTOE範囲は、以下のものである。

- IDEドライバ初期化
- 暗号化機能実装確認
- 暗号鍵データ転送
- ボード装着情報設定
- 暗号化機能動作表示
- 暗号化機能動作確認
- 暗号化機能迂回検出
- HDDエラー要因設定
- HDDデータ暗号化/復号
- HDD全面リード
- HDDスマート情報取得

2.4.3 論理構成要素

論理構成における機能とハードウェア/ソフトウェア構成要素対応は、以下のものである。

機能名称	ハードウェア/ソフトウェア構成要素対応づけ
暗号化機能実装確認	S/W:暗号化機能実装確認(IDEドライバ) H/W:IDEコントローラチップ
暗号化機能動作表示	S/W:暗号化機能動作表示(設定/登録ユーザインターフェイス)
暗号化機能迂回検出	S/W:暗号化機能迂回検出(マシンユーザインターフェイス)
HDDデータ暗号化/復号	S/W:HDD書込み/読出し(IDEドライバ) H/W:暗号化チップ
IDEドライバ初期化	S/W:IDEドライバ初期化(IDEドライバ)
暗号鍵データ転送	S/W:暗号鍵データ転送(IDEドライバ) H/W:KEY PLD
ボード装着情報設定	S/W:ボード装着情報設定(IDEドライバ)
鍵コード入力	S/W:鍵コード入力(自己診断ユーザインターフェイス)
暗号化機能動作確認	S/W:暗号化機能動作確認(自己診断ユーザインターフェイス)
HDDエラー要因設定	S/W:HDDエラー要因設定(IDEドライバ)
起動処理	S/W:BSP、USBホストドライバ
操作パネル制御/メッセージ	S/W:表示管理システム
自己診断	S/W:自己診断ユーザインターフェイス
設定/登録制御	S/W:設定/登録ユーザインターフェイス
マシン制御	S/W:マシンユーザインターフェイス
マシン管理	S/W:マシン管理
システム制御	S/W:ジョブ管理、システム管理、原稿入力、印刷、FAX、NICドライバ、IEEE1284ドライバ、USBデバイスドライバ、FAXボードライブラリ、内部情報管理
サービス通信	S/W:サービス通信
HDDデータ全消去	S/W:HDDデータ全消去
HDDアクセス	S/W:ファイルアクセスライブラリ
HDD全面リード	S/W:HDD全面リード(IDEドライバ)
NVRAMアクセス	S/W:システムライブラリ
HDDスマート情報取得	S/W:HDDスマート情報取得(IDEドライバ)
IDE NVRAMアクセス	S/W:IDE NVRAMアクセス(IDEドライバ)

2.5 保護資産

本TOEの保護資産は、ユーザ文書残存データである。
保護資産が生成される過程には、以下の2つのケースがある。

＜保護資産生成過程1＞
・ジョブ実行処理の過程で、一時的に生成され保存されたユーザ文書データは、ジョブ完了後にFAT情報が削除され、ユーザ文書残存データとなる。図2.5-1を参照。

＜保護資産生成過程2＞
・ファイリングボックスに保存されたユーザ文書データが不要となったとき、FAT情報が削除され、ユーザ文書残存データとなる。図2.5-2を参照。

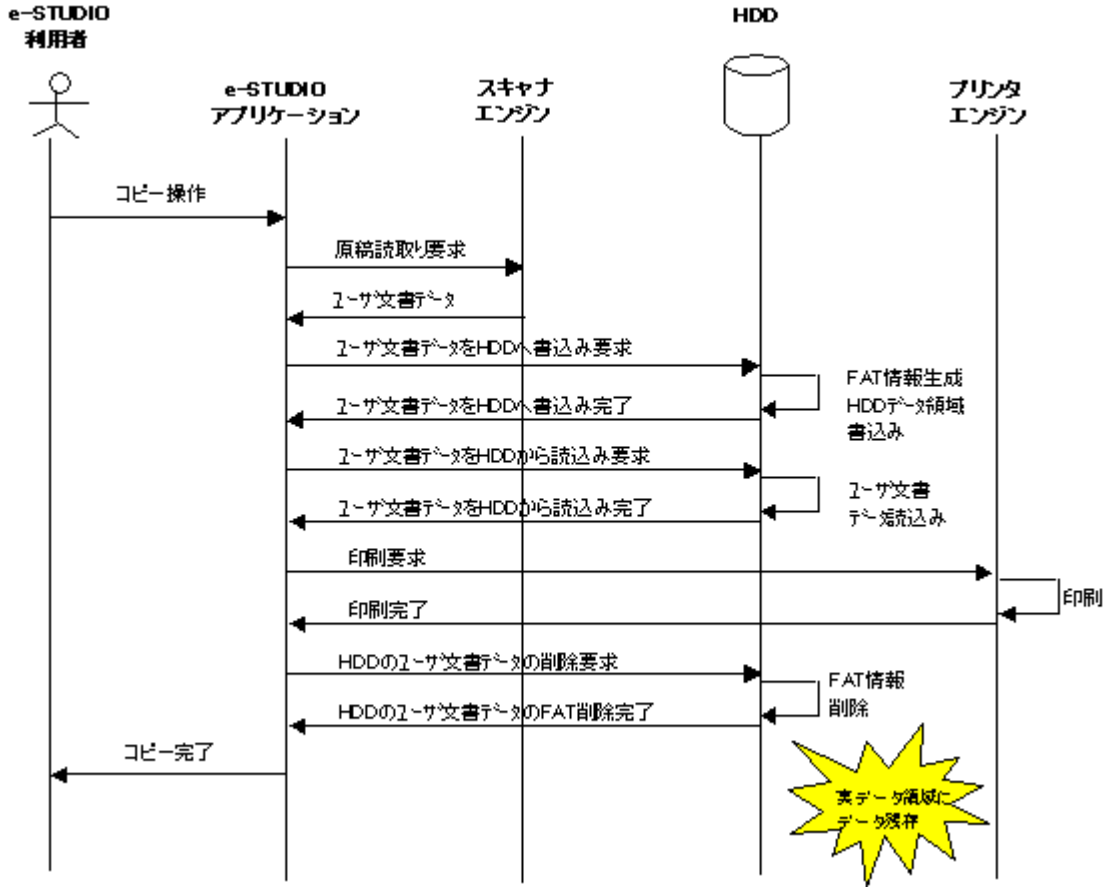

図2.5-1 コピー機能時の処理の流れ

図2.5-1は、＜保護資産生成過程1＞で保護資産が生成される代表例である、コピー機能を実行したときの処理の流れを示している。
スキャナエンジンにより取り込まれたユーザ文書データは、HDDに一時的に保存される。一時的に保存されたユーザ文書データは、印刷完了後、FAT情報が削除されるが、HDD上にユーザ文書データの実体は存在している。

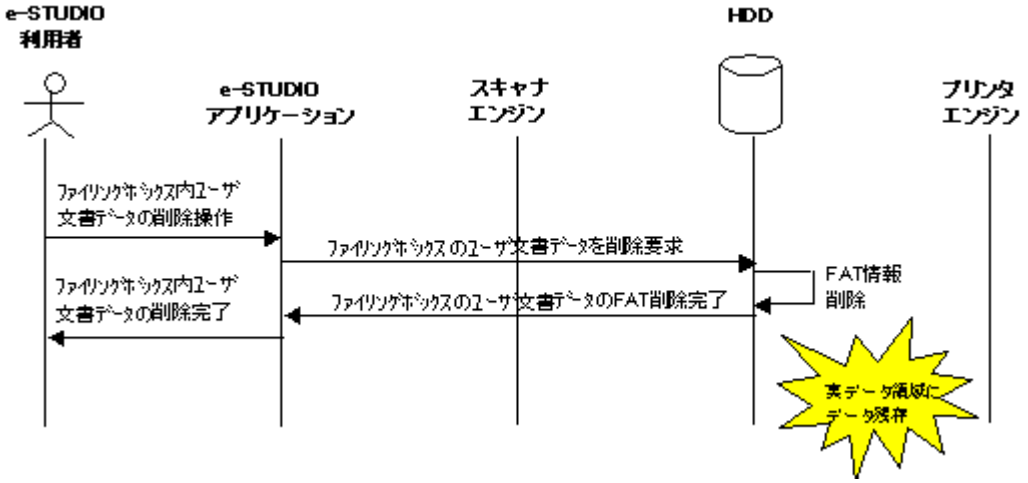

図2.5-2 ファイリングボックス機能(削除)時の処理の流れ

図中2.5-2は、<保護資産生成過程2>で保護資産が生成される代表例である、ファイリングボックス内のユーザ文書データの削除を実行したときの処理の流れを示している。
e-STUDIO利用者が、ファイリングボックスに保存されたユーザ文書データの削除操作を行うことにより、ファイリングボックス内のユーザ文書データのFAT情報は削除されるが、HDD上にユーザ文書データの実体は存在している。

上記の機能以外の、2.1.4節で述べた他の機能に関しても、入力元及び出力先は違うものの、同様の処理が行われ、ユーザ文書残存データが生成される。

以下の表 2.5-3で、2.1.4節で述べた各機能において、<保護資産生成過程1>, <保護資産生成過程2>のどちらの過程で、保護資産が生成されるかを示す。

機能	保護資産生成過程1	保護資産生成過程2
コピー	○	
プリント	○	
スキャン	○	
ファイリングボックス(編集)	○	
ファイリングボックス(削除)		○
FAX送信	○	
FAX受信	○	
インターネットFAX送受信	○	
オンランプゲートウェイ	○	
オフランプゲートウェイ	○	

表2.5-3 各機能における保護資産生成過程

以上のように、FAT情報は削除されているが、HDD上に実体が存在しているユーザ文書データを、ユーザ文書残存データと定義し、保護資産とする。
また、FAT情報が存在するユーザ文書データは、保護資産とはしない。

保護資産であるユーザ文書残存データは、FAT情報が削除されているため、e-STUDIO利用者に提供されている機能ではアクセスできない。

2.6 TOEの機能

2.6.1 TOEが提供する機能

本TOEが提供する機能は、以下のものである。

- HDDデータ暗号化/復号
  e-STUDIO利用者が、e-STUDIO 3511/4511が提供する主な機能を利用する際に、ユーザ文書データを暗号化してHDDに保存する。ジョブ要求時に、HDDに暗号化されて保存されているユーザ文書データを読出して復号する。

- 暗号化機能迂回検出
  スクランブラボードの装着状態の確認結果が異常であれば、操作パネル上にサービスエンジニアの呼出しを要求するサービスマンコール表示を行い、e-STUDIO 3511/4511の機能利用を停止する。

- 暗号化機能実装確認
  e-STUDIO 3511/4511の起動時に、スクランブラボードの装着状態の確認を行う。

- 暗号化機能動作表示
  暗号化機能が正常に動作しているとき、操作パネルからの表示要求により、TOEの型名とバージョンの表示を行う。

- 暗号化機能動作確認
  NVRAMに設定されているスクランブラボードの装着有無情報を取得する。

- IDEドライバ初期化
  e-STUDIO 3511/4511 の起動時に、暗号化機能実装確認を実行する。暗号化機能実装確認による、スクランブラボードの装着状態の確認結果が正常であれば、暗号鍵データ転送を実行する。

- HDDエラー要因設定
  スクランブラボード装着確認で異常の場合、HDDエラー要因情報の取得を行う。

- 暗号鍵データ転送
  システムボードのSRAMから暗号鍵データを取り出し、スクランブラボード上のKEY PLDに暗号鍵データの転送を行う。

- ボード装着情報設定
  スクランブラボードの装着有無の情報をシステムボードのNVRAMに設定する。

- HDD全面リード
  HDDに書込み/読出しできない領域が無いか確認を行う。

- HDDスマート情報取得
  スマート情報の取得を行う。

2.6.2 TOEが提供しない機能

暗号鍵は暗号鍵作成会社が作成し、鍵コードとしてメーカーに提供されるものであり、FIPS140-2の統計的乱数性の検定に適合し、機密性と一意性を保証された暗号鍵である。鍵コードは本TOEのインストール時に、サービスエンジニアよりe-STUDIO管理者に、TOEと一緒に提供される。e-STUDIO管理者が鍵コードをTOEに入力後、128bitの暗号鍵データに変換され、保存される。一度保存された暗号鍵データは、継続して使用することから、暗号鍵を生成、及び暗号鍵を破棄する必要はない。よって、以下の機能は提供しない。

- 暗号鍵生成
- 暗号鍵破棄

2.6.3 TOEの利用手順

TOEの利用手順を以下に説明する。

・スクランブラボード GP-1031導入時

図2.6-1 スクランブラボード GP-1031導入時の作業手順

[1] サービスエンジニアは、e-STUDIO管理者にCheck sheetを渡し、設置のための説明（Check sheetの説明，鍵コードの保管についての説明，廃棄または交換時の説明など）を行う。

[2] サービスエンジニアは、HDD内のデータのバックアップを行う。

[3] サービスエンジニアは、FUNCTION LIST FOR MAINTENANCEの印刷を行う。

[4] e-STUDIO管理者は、システム設定リストの印刷のために、[設定/登録]ボタンを押下し、タッチパネル上の[管理者設定]ボタンを押下して、管理者パスワードの入力を行う。

[5] e-STUDIO管理者は、ネットワークなどに関する設定のバックアップのために、システム設定リストの印刷を行う。
但しe-STUDIO管理者の許可がある場合には、サービスエンジニアが対応する。

[6] e-STUDIO管理者は、スクランブラボードが入っている袋のセキュリティシール、及び取扱説明書と鍵コードが記載されている封筒が入っている袋のセキュリティシールが剥されていないことの確認を行い、Check sheetの(1)項にチェックをする。

[7] e-STUDIO管理者は、鍵コードが記載されている封筒の未開封確認を行い、Check sheetの(2)項にチェックをする。

[8] サービスエンジニアは、ダウンロード治具またはUSBストレージデバイスから、ROMデータのダウンロードを行う。

[9] サービスエンジニアは、鍵コード入力画面の表示を行い、e-STUDIO管理者に鍵コードの入力を促す。

[10] e-STUDIO管理者は、鍵コードが記載されている封筒の開封を行う。

[11] e-STUDIO管理者は、サービスエンジニアを含む他の人に鍵コードを見られないように、鍵コード入力を行う。

[12] e-STUDIO管理者は、確認のために二回目の鍵コード入力を行い、Check sheetの(3)項にチェックをする。

[13] サービスエンジニアは、e-STUDIO 3511/4511の電源を切断する。

[14] サービスエンジニアは、GP-1031開梱据付指示書に従ってスクランブラボードの取付け作業を行う。

[15] サービスエンジニアは、HDDのパーティションの作成、HDDプログラムデータとUIデータのダウンロード、HDDの初期化、FAXの初期化、プリンタガンマ調整（ユーザ文書データに対し、より自然に近い印刷表示を得るための補正操作）を行う。

[16] サービスエンジニアは、e-STUDIO 3511/4511の再起動を行う。

[17] サービスエンジニアは、スクランブラボード設置の前に設定されていたユーザ設定項目を再設定する。また、[2]でバックアップしたHDD内のデータのリストアを行う。

[18] サービスエンジニアは、[3]で印刷したFUNCTION LIST FOR MAINTENANCEを参照して、再設定を行う。

[19] e-STUDIO管理者は、システム設定リスト中の設定内容の再設定のために、[設定/登録]ボタンを押下し、タッチパネル上の[管理者設定]ボタンを押下して、管理者パスワードの入力を行う。

[20] e-STUDIO管理者は、[5]で印刷したシステム設定リストを参照して、ネットワークなどに関する再設定を行う。
但しe-STUDIO管理者の許可がある場合には、サービスエンジニアが対応する。

[21] e-STUDIO管理者は、[設定/登録]ボタンを押下し、タッチパネル上の[カウンタ]ボタンを押下してTOEのバージョンが表示されることの確認を行い、Check sheetの(4)項にチェックをする。

[22] サービスエンジニアは、e-STUDIO管理者に対して運用の説明を行う。

[23] e-STUDIO管理者は、自分以外の人に鍵コードを知られないように、鍵コードが記載されている封筒を厳重に管理し、Check sheetの(5)項にチェックをする。

[24] サービスエンジニアは、Check sheetの回収を行う。

[25] e-STUDIO管理者は、サービスエンジニアからCheck sheetのコピーを受け取る。

[26] e-STUDIO管理者は、運用を開始する。

・通常運用時

[1] 電源の投入により、e-STUDIO 3511/4511の起動処理が開始される。

[2] e-STUDIO利用者は、e-STUDIO 3511/4511の立上げが完了したら、操作パネル上のボタン押下により、暗号化機能が正常に動作していることを示すTOEの型名とバージョンの表示の確認が可能となる。

[3] TOEの型名とバージョンの表示が確認できれば、暗号化機能の利用が可能であり、e-STUDIO利用者がユーザ文書をコピー、及びファイリングした際に、HDDに格納されるユーザ文書データは暗号化される。

[4] e-STUDIO 3511/4511の起動処理中にスクランブラボードの取り外し、またはスクランブラボードの代わりに不正なボード装着の可能性が検出された場合、操作パネル上にサービスマンコールが表示されると同時に、全ての機能の利用ができなくなる。その場合、e-STUDIO管理者がその旨をサービスエンジニアに連絡する。

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

前提条件は以下の通りである。

A.KEYCODE_MANAGE

e-STUDIO管理者は、TOEの生成時に入力する鍵コードを、本人以外の者に知られないように管理する。

A.NO_EVIL_ADM

e-STUDIO管理者は、悪意を持った行為を行わない。

A.NO_EVIL_ENG

サービスエンジニアは、悪意を持った行為を行わない。

A.SECURE_KEYCODE

TOEの生成時に入力される鍵コードは、機密性と一意性を保証された鍵コードであり、e-STUDIO管理者によって正しくTOEにインストールされる。

3.2 脅威

e-STUDIO 3511/4511に攻撃を行う者の攻撃能力は低レベルであり、その攻撃による脅威は以下の通りである。

T.HDD_THEFT

悪意を持ったe-STUDIO利用者、またはe-STUDIO非関係者が、HDDに不正な解読装置を接続し、ユーザ文書残存データを暴露するかもしれない。

T.SBOARD_REMOVE

悪意を持ったe-STUDIO利用者、またはe-STUDIO非関係者が、スクランブラボードを取り外したり、スクランブラボードの代わりに不正なボードを装着してセキュリティ機能を無効化することにより、ユーザ文書残存データを暴露するかもしれない。

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.HDD_UNANALYZABLE

TOEは、HDDに不正な解読装置が接続され、ユーザ文書残存データが解読されることのないようにしなければならない。

O.REMOVE_DETECT

TOEは、TOEの関係者がTOEの利用を開始する前に、システムボードにスクランブラボードが正常に装着されていることを検査しなければならない。
セキュリティ機能が正常に動作していることを、TOEの関係者が認識できるようにしなければならない。
またセキュリティ侵害として、スクランブラボードが取り外されたり、スクランブラボードの代わりに不正なボードが装着された場合には、その事象を検出し、TOEの関係者に通知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.KEYCODE_MANAGE

e-STUDIO管理者は、TOEの生成時に入力する鍵コードを、本人以外の者に知られないように管理しなければならない。

OE.SECURE_KEYCODE

e-STUDIO管理者は、TOEの生成時に、密封されている封筒に記載されたコード値の通りに鍵コードを正しく入力しなければならない。

OE.TRUST_ADM

e-STUDIO利用部門の責任者は、信頼できる人物をe-STUDIO管理者として任命しなければならない。

OE.TRUST_ENG

e-STUDIO管理者は、サービスエンジニアが正規の社員であることを確認しなければならない。

IT環境のセキュリティ対策方針は以下の通りである。

OIE.TIMESTAMP

IT環境は、セキュリティ機能を使用するために、信頼できる時刻を提供しなければならない。

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。

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: 混乱を最小にするアクションのリスト]を実行しなければならない。

[割付: 混乱を最小にするアクションのリスト]

- サービスマンコール表示
- e-STUDIO利用者機能の受付拒否

依存性: FAU_SAA.1 侵害の可能性の分析

FAU_GEN.1 監査データ生成

下位階層: なし

FAU_GEN.1.1 TSFは、以下の監査対象事象の監査記録を生成できなければならない:

a) 監査機能の起動と終了;

b) 監査の[選択: 最小、基本、詳細、指定なし: から一つのみ選択]レベルのすべての監査対象事象;及び

c) [割付: 上記以外の個別に定義した監査対象事象]。

[選択: 最小、基本、詳細、指定なし: から一つのみ選択]
指定なし

[割付: 上記以外の個別に定義した監査対象事象]

- スクランブラボードの取り外し事象
- スクランブラボード以外の不正なボードの装着事象

FAU_GEN.1.2 TSFは、各監査記録において少なくとも以下の情報を記録しなければならない:

a) 事象の日付・時刻、事象の種別、サブジェクト識別情報、事象の結果(成功または失敗);及び

b) 各監査事象種別に対して、PP/STの機能コンポーネントの監査対象事象の定義に基づいた、[割付: その他の監査関連情報]

[割付: その他の監査関連情報]
なし

依存性: FPT_STM.1 高信頼タイムスタンプ

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: 定義された監査対象事象のサブセット]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]。

[割付: 定義された監査対象事象のサブセット]

- スクランブラボードの取り外し事象
- スクランブラボード以外の不正なボードの装着事象

[割付: その他の規則]
なし

依存性: FAU_GEN.1 監査データ生成

FAU_SAR.1 監査レビュー

下位階層: なし

FAU_SAR.1.1 TSFは、[割付: 許可利用者]が、[割付: 監査情報のリスト]を監査記録から読み出せるようにしなければならない。

[割付: 許可利用者]

- TOEの関係者

[割付: 監査情報のリスト]
事象の結果（正常）

FAU_SAR.1.2 TSFは、利用者に対し、その情報を解釈するのに適した形式で監査記録を提供しなければならない。

依存性: FAU_GEN.1 監査データ生成

FCS_COP.1 暗号操作

下位階層: なし

FCS_COP.1.1 TSFは、[割付: 標準のリスト]に合致する、特定された暗号アルゴリズム[割付: 暗号アルゴリズム]と暗号鍵長[割付: 暗号鍵長]に従って、[割付: 暗号操作のリスト]を実行しなければならない。

[割付: 標準のリスト]
FIPS PUB 46-3

[割付: 暗号アルゴリズム]
Triple DES

[割付: 暗号鍵長]
112bit

[割付: 暗号操作のリスト]

- ユーザ文書データのHDD書込み時の暗号化操作
- ユーザ文書データのHDD読出し時の復号操作

依存性: [FCS_CKM.1 暗号鍵生成
または
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]
FCS_CKM.4 暗号鍵破棄
FMT_MSA.2 セキュアなセキュリティ属性

FPT_AMT.1 抽象マシンテスト

下位階層: なし

FPT_AMT.1.1 TSFは、TSFの下層にある抽象マシンによって提供されるセキュリティ前提条件の正しい操作を実証するために、[選択: 初期立ち上げ中、通常操作中に定期的に、許可利用者の要求で、[割付: その他の条件]]に、テストのスイートを走らせなければならない。

[選択: 初期立ち上げ中、通常操作中に定期的に、許可利用者の要求で、[割付: その他の条件]]
初期立ち上げ中

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

TOEセキュリティ保証要件は、EAL2であり、以下の通りである。

- ACM_CAP.2 構成要素
- 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.1 記述的上位レベル設計
- 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
- ASE_DES.1 セキュリティターゲット、TOE記述、評価要件
- ASE_ENV.1 セキュリティターゲット、セキュリティ環境、評価要件
- ASE_INT.1 セキュリティターゲット、ST概説、評価要件
- ASE_OBJ.1 セキュリティターゲット、セキュリティ対策方針、評価要件
- ASE_PPC.1 セキュリティターゲット、PP主張、評価要件
- ASE_REQ.1 セキュリティターゲット、ITセキュリティ要件、評価要件
- ASE_SRE.1 セキュリティターゲット、明示されたITセキュリティ要件、評価要件
- ASE_TSS.1 セキュリティターゲット、TOE要約仕様、評価要件
- ATE_COV.1 カバレージの証拠
- ATE_FUN.1 機能テスト
- ATE_IND.2 独立テスト-サンプル
- 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。確率的または順列的なメカニズムを利用する機能要件はない。FCS_COP.1は、暗号アルゴリズムを利用した機能要件であるため、本最小機能強度宣言の対象としない。

5.2 IT環境のセキュリティ要件

本TOEにおけるIT環境は、e-STUDIO 3511/4511に実装されるシステムボード上のRTCが対象であり、そのIT環境のセキュリティ要件は以下の通りである。

FPT_STM.1 高信頼タイムスタンプ

下位階層: なし

FPT_STM.1.1 TSFは、それ自身の使用のために、高信頼タイムスタンプを提供できなければならない。

[詳細化]
RTCは、TSF自身の使用のために、高信頼タイムスタンプを提供できなければならない。

依存性: なし

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。

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

	FAU_ARP.1	FAU_GEN.1	FAU_SAA.1	FAU_SAR.1	FCS_COP.1	FPT_AMT.1	FPT_RVM.1
SF.HDD_ENCRYPT					O		O
SF.REMOVE_DETECT	O		O				O
SF.RUN_MESSAGE				O			O
SF.SBOARD_CHECK		O				O	O

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.HDD_ENCRYPT

TOEは、以下の操作に対し、暗号化アルゴリズムとして、Triple DES（FIPS PUB 46-3）、鍵長112bitを使用する。
【暗号操作】
・ユーザ文書データのHDD書込み時の暗号化操作
・ユーザ文書データのHDD読出し時の復号操作
（FCS_COP.1）

またTOEは、本機能が迂回されないように、スクランブラボード装着時において、システムボードからHDDへのデータ経路と、その逆の経路を単一化し、HDDへの書込み、またはHDDから読出しするデータが必ず暗号化チップを介するようにすることで、HDDへ書込むデータは必ず暗号化チップにより暗号化操作が実施され、HDDから読出されるデータは必ず暗号化チップにより復号操作が実施されるようにする。
（FPT_RVM.1）

SF.REMOVE_DETECT

TOEは、以下の監査対象事象のサブセットに示す事象のどれかを検出した場合、セキュリティ侵害と判定する。
【監査対象事象のサブセット】
・スクランブラボードの取り外し事象
・スクランブラボード以外の不正なボード装着事象
（FAU_SAA.1）

TOEは、セキュリティ侵害の判定により、セキュリティ侵害の可能性を検出した場合、以下のアクションを行う。
【アクション】
・操作パネルへのサービスマンコール表示
・e-STUDIO利用者機能の受付拒否によるデジタル複合機の機能停止
（FAU_ARP.1）

またTOEは、本機能が迂回されないように、e-STUDIO 3511/4511の起動処理におけるIDEドライバ初期化処理にて、SF.SBOARD_CHECK実行後にマシンユーザインターフェイス内のSF.REMOVE_DETECTを実行する。その手段として、SF.SBOARD_CHECKによる監査記録が生成された後に本機能が呼び出されるようにする。
（FPT_RVM.1）

SF.RUN_MESSAGE

TOEは、TOEの関係者に、暗号化機能が適切に動作していることを認識できるように、以下の監査記録情報を読出せるようにする。
【監査記録情報】
・事象の結果（正常）
TOEの関係者に、暗号化機能が適切に動作していることを認識するための情報提供としては、操作パネルからのボタン操作により、事象の結果が正常の場合、TOEの型名とバージョンを生成し、操作パネルにそれを表示する。
（FAU_SAR.1）

またTOEは、本機能が迂回されないように、ボタン操作時に実行される設定／登録ユーザインターフェイスにおける設定情報取得処理の最初に、SF.RUN_MESSAGEを実行する。その手段として、操作パネルからのボタン操作のタイミングで本機能が呼び出されるようにする。
（FPT_RVM.1）

SF.SBOARD_CHECK

TOEは、e-STUDIO 3511/4511の電源投入による初期立ち上げ中に、システムボードにスクランブラボードが正常に装着されていることを確認するために、妥当性テストを実施する。
妥当性のテストでは、以下の事象を検知する。
【検知事象】
・システムボードがスクランブラボード上の識別情報を正しく検知できる。(スクランブラボード正常事象)
・スクランブラボード上の識別情報を検知できない。(スクランブラボード取り外し事象)
・不正な識別情報を検知した。(スクランブラボード以外の不正なボードの装着事象)
(FPT_AMT.1)

TOEは、スクランブラボードの妥当性テストの結果からセキュリティ侵害の可能性を検出するため、以下の監査対象事象の監査記録を生成する。TOEは、監査データを記録するのに必要なタイムスタンプ情報を、RTCから取得する。
【監査対象事象】
①監査の起動(スクランブラボード正常事象)
②スクランブラボード取り外し事象
③スクランブラボード以外の不正なボードの装着事象

監査の終了が監査対象事象となっていない理由を以下に示す。
デジタル複合機の運用は、一般の計算機と異なり、終了操作によるタスクの終了といったシャットダウン処理は存在せず、監査機能を単独で終了させることはできない。監査機能を強制終了させるためには、監査機能を実行しているタスクを、OS(VxWorks)を介して終了させることが唯一の方法である。VxWorksにアクセスする方法としては、e-STUDIO 3511/4511のシリアルインターフェイスコネクタ、USBインターフェイスコネクタ(ホスト)、PCIアダプタから侵入する必要があるが、この方法は悪用不能である。
よって、監査機能の終了は、e-STUDIO 3511/4511の電源を切断した時にのみ行なわれる。e-STUDIO 3511/4511の電源の切断操作のタイミングで、デジタル複合機の全ての機能は停止してしまうことから、e-STUDIO 3511/4511の電源切断後に、e-STUDIO 3511/4511、及びTOEに対してアクセスすることは不可能である。
従って、e-STUDIO 3511/4511の起動(監査の起動)、及び②, ③の事象を記録すれば、セキュリティ上の問題は発生しないため、監査の終了を記録する必要はない。
以上の理由から、監査の終了を監査対象事象としない。

また、生成された監査記録には、以下の情報を記録する。
【監査記録情報】
・事象の日付, 時刻(RTCから取得したタイムスタンプ)
・事象の種別(スクランブラボードの装着有無)
・サブジェクト識別情報(監査要求元タスク情報)
・事象の結果(正常、またはエラー)
(FAU_GEN.1, FPT_STM.1)

またTOEは、本機能が迂回されないように、e-STUDIO 3511/4511の起動処理におけるIDEドライバ初期化処理の最初に、SF.SBOARD_CHECKを実行する。その手段として、e-STUDIO 3511/4511の起動処理が開始され、IDEドライバ初期化処理が開始されたタイミングで、本機能が呼び出され、監査記録を取得するようにする。
(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は以下の通りである。

表6.1-2 セキュリティメカニズムとTOEセキュリティ機能

セキュリティメカニズム	セキュリティ機能
Triple DES暗号化メカニズム	SF.HDD_ENCRYPT

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。

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

	ACM_CAP.2	ADO_DEL.1	ADO_IGS.1	ADV_FSP.1	ADV_HLD.1	ADV_RCR.1	AGD_ADM.1	AGD_USR.1	ASE_DES.1	ASE_ENV.1	ASE_INT.1	ASE_OBJ.1	ASE_PPC.1	ASE_REQ.1	ASE_SRE.1	ASE_TSS.1	ATE_COV.1	ATE_FUN.1	ATE_IND.2	AVA_SOF.1	AVA_VLA.1
リリースバージョン管理規約	O																				
VSS管理規約	O																				
サービスドキュメント資料番号 発番規定	O																				
製品技術資料(TB)体系規程	O																				
品名コードの発番および品名記載規程	O																				
スクランブラボード GP-1031 暗号化機能動作確認ファイル構成一覧	O																				
スクランブラボード GP-1031 暗号化機能迂回検出ファイル構成一覧	O																				
スクランブラボード GP-1031 暗号化機能動作表示ファイル構成一覧	O																				
スクランブラボード GP-1031 IDEドライバファイル構成一覧	O																				
PWA-F-DES-340	O																				
スクランブラボード GP-1031 ソフトウェアバージョン管理表	O																				
スクランブラボード GP-1031 TOE構成表	O																				
スクランブラボード GP-1031【日本語名】 Scrambler Board GP-1031【英語名】																	O	O	O		
スクランブラボード GP-1031 表現対応分析書						O															
スクランブラボード GP-1031 脆弱性分析書																					O
スクランブラボード GP-1031 機能強度分析書																				O	
スクランブラボード GP-1031 テスト成績書																	O	O	O		
スクランブラボード GP-1031 テスト仕様書																	O	O	O		
スクランブラボード GP-1031 上位レベル設計書(HLD)					O																
スクランブラボード GP-1031 機能仕様書(FSP)				O																	
e-STUDIO 3511/4511用 スクランブラボード GP-1031 Security Target									O	O	O	O	O	O	O	O					
GP-1031 with GO-1030 開梱据付指示書【日本語名】 GP-1031 with GO-1030 Unpacking Instruction【英語名】		O	O																		
スクランブラボード GP-1031 ROMデータ配付手順書		O																			
スクランブラボード GP-1031 梱包・倉入れ手順書		O																			
スクランブラボード GP-1031 物流手順書		O																			
スクランブラボード GP-1031 構成管理規約	O																				

スクランブラボード GP-1031 構成リスト	O																				
Check sheet		O	O																		
スクランブラボード GP-1031 取扱説明書【日本語名】 Scrambler Board GP-1031 Operator's Manual【英語名】		O	O				O	O													
スクランブラボード GP-1031 サービスマニュアル【日本語名】 Scrambler Board GP-1031 Service Manual【英語名】		O	O																		

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。

表8.1-1 セキュリティ対策方針と前提条件、脅威

	A.KEYCODE_MANAGE	A.NO_EVIL_ADM	A.NO_EVIL_ENG	A.SECURE_KEYCODE	T.HDD_THEFT	T.SBOARD_REMOVE
O.HDD_UNANALYZABLE					O	
O.REMOVE_DETECT						O
OE.KEYCODE_MANAGE	O					
OE.SECURE_KEYCODE				O		
OE.TRUST_ADM		O				
OE.TRUST_ENG			O			
OIE.TIMESTAMP						O

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。

A.KEYCODE_MANAGE

e-STUDIO管理者が、OE.KEYCODE_MANAGEにより、鍵コードをe-STUDIO管理者以外の者に知られないように管理することによって、e-STUDIO管理者以外への鍵コードの暴露を防ぐことを実現できる。

A.NO_EVIL_ADM

e-STUDIO管理者は、OE.TRUST_ADMにより、e-STUDIO利用部門の責任者が適切な人物を任命することによって、悪意を持った行為を行わないことを実現できる。

A.NO_EVIL_ENG

e-STUDIO管理者は、OE.TRUST_ENGにより、サービスエンジニアに対して正規の社員であることを証明させることによって、セキュリティ違反を行なわないことを実現できる。

A.SECURE_KEYCODE

e-STUDIO管理者が、OE.SECURE_KEYCODEにより、密封された封筒に記載されたコード値の通りに正しく鍵コードを入力することによって、機密性と一意性を保証された鍵コードが、TOEにインストールされることを実現できる。

T.HDD_THEFT

T.HDD_THEFTに対抗するためには、HDDから読出した内容を解読できなくすることが必要であり、O.HDD_UNANALYZABLEにて、HDDに保存されているデータが読出せた場合でもその内容を解読できなくすることにより対抗できる。

T.SBOARD_REMOVE

T.SBOARD_REMOVEに対抗するためには、セキュリティ機能が正常に動作しているのか、または無効な状態なのかを認識する必要があり、O.REMOVE_DETECTにてセキュリティ機能が正常に動作している場合は、その状態をTOEの関係者に認識させることと、スクランブラボードを取り外したり、スクランブラボードの代わりに不正なボードを装着することによるセキュリティ侵害の場合は、その事象を検出し、TOEの関係者に通知することにより対抗できる。

尚、OIE.TIMESTAMPは、O.REMOVE_DETECTを実現するのに必要なTOEセキュリティ機能要件の依存性をIT環境のセキュリティ要件により実現することで、本脅威に関係づけるものである。

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。

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

	O.HDD_UNANALYZABLE	O.REMOVE_DETECT	OIE.TIMESTAMP
FAU_ARP.1		O	
FAU_GEN.1		O	
FAU_SAA.1		O	
FAU_SAR.1		O	
FCS_COP.1	O		
FPT_AMT.1		O	
FPT_RVM.1	-	-	
FPT_STM.1		-	O

(注: 'O'は対策方針と直接対応している事を、'-'は機能要件の依存性、或いは相互サポートの対応を辿って関係している事を示す。)

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.HDD_UNANALYZABLE

FCS_COP.1によって、FIPS PUB 46-3に基づいたTriple DESにより暗号化することで、ユーザ文書残存データが解読され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.REMOVE_DETECT

①FPT_AMT.1によって、e-STUDIO 3511/4511初期立ち上げ中に、システムボードにスクランブラボードが正常に装着されていることを検知するテストを実行する。
②FAU_GEN.1によって、セキュリティ機能が正常に動作していることを確認するためと、スクランブラボードの取り外し事象やスクランブラボード以外の不正なボードの装着事象によるセキュリティ侵害を、検出するための監査データを生成する。
尚、その時に用いられる時刻は、IT環境により提供される。
③FAU_SAA.1によって、FAU_GEN.1で生成された監査データから、スクランブラボードの取り外し事象やスクランブラボード以外の不正なボードの装着事象によるセキュリティ侵害を、検出するための分析を行う。
④FAU_ARP.1によって、FAU_SAA.1の分析の結果、セキュリティ侵害の可能性が検出された場合、サービスマンコール表示を行うことにより、TOE関係者に通知し、e-STUDIO利用者機能の受付拒否を行う。
⑤FAU_SAR.1によって、FAU_GEN.1で生成された監査データの事象の結果が正常の場合、その情報を表示する。
①により、TOEの関係者がTOEの利用を開始する前に、TOEがセキュリティ機能の正常動作を確認するという対策方針を実現できる。
②, ③, ④により、スクランブラボードの取り外し事象や、スクランブラボード以外の不正なボードの装着事象によるセキュリティ侵害を、検出しTOEの関係者に通知するという対策方針を実現できる。
⑤により、セキュリティ機能が正常に動作していることを、TOEの関係者に認識させるという対策方針を実現できる。

OIE.TIMESTAMP

FPT_STM.1により、RTCが実時間に準じた時間データを発生させることで、セキュリティ機能を使用するために、信頼できる時刻を提供するというIT環境の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。

FAU_ARP.1
FAU_SAA.1により、依存性は満たされている。

FAU_GEN.1
FPT_STM.1により、依存性は満たされている。

FAU_SAA.1
FAU_GEN.1により、依存性は満たされている。

FAU_SAR.1
FAU_GEN.1により、依存性は満たされている。

FCS_COP.1
FCS_COP.1の依存関係は満たされていないが、問題がない根拠を以下に示す。
①暗号鍵はTOE外の暗号鍵作成会社で作成され、鍵コードとして提供される。e-STUDIO管理者は、鍵コードをTOEインストール時に一度だけ入力し、システムボード上のSRAMに暗号鍵データとしてインポートされる。鍵コード入力機能はインストーラであり、TOEインストール時に一度しか実行されない。その後の暗号化、復号操作においては、インポートされた暗号鍵データを継続して使用するため、TOEにおいて暗号鍵を生成する必要と、暗号鍵を破棄する必要はない。
②暗号鍵のインポートは、TOEインストール時に行われることから、TOE利用時におけるTSC外からのインポートの必要はない。
③暗号鍵は、暗号鍵作成会社より提供されるもので、FIPS140-2の統計的乱数性の検定に適合し、機密性と一意性を保証された暗号鍵である。暗号鍵のセキュリティ属性は、暗号鍵長のみである。暗号鍵は指定の暗号鍵長で生成され、その暗号鍵がインポートされる。機密性と一意性を保証された暗号鍵がTOEのインストール時に運用によりインポートされ、その暗号鍵が継続して使用されることから、セキュリティ属性としてセキュアな値だけが受け入れられることを保証する機能要件(FMT_MSA.2)は必要ない。
①により、FCS_CKM.1, FCS_CKM.4の依存関係は不要である。
②により、FDP_ITC.1の依存関係は不要である。
③により、FMT_MSA.2の依存関係は不要である。

FPT_AMT.1
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。

FPT_STM.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、機能要件とその機能要件をサポートする要件の対応を示す。

表8.2-2 機能要件と相互サポート対応

機能要件	相互サポート要件
FAU_ARP.1	FPT_RVM.1
FAU_GEN.1	FPT_RVM.1
FAU_SAA.1	FPT_RVM.1
FAU_SAR.1	FPT_RVM.1
FCS_COP.1	FPT_RVM.1
FPT_AMT.1	FPT_RVM.1
FPT_RVM.1	なし

FPT_RVM.1＜迂回防止＞

①e-STUDIO 3511/4511の起動処理において、デジタル複合機の機能が実行される前のIDEドライバ初期化処理にて、暗号化機能実装確認(FPT_AMT.1, FAU_GEN.1), 暗号化機能迂回検出(FAU_SAA.1, FAU_ARP.1)の順に必ず呼び出され、成功することが保証される。
②TOEの関係者による操作パネルからの確認操作時に、設定／登録ユーザインターフェイスにおける設定情報取得処理の初めに、暗号化機能動作確認でスクランブラボードの装着有無情報をNVRAMから取得し、その後、暗号化機能動作表示機能(FAU_SAR.1)は必ず呼び出され、成功することが保証される。
③e-STUDIO 3511/4511に、スクランブラボードが正常に装着されている状態で、HDDへの書込みの時のシステムボードからHDDへのデータ経路と、HDDからの読出し時のその逆の経路は単一化されており、データは必ず暗号化チップを介することにより、HDDデータ暗号化／復号(FCS_COP.1)の機能は必ず呼び出され、成功することが保証される。
以上、FPT_RVM.1により、デジタル複合機の各種機能が実行される前に必ず対象のセキュリティ機能が呼び出され、成功することが保証されることにより迂回されない。

FPT_SEP.1＜改ざん防止＞

本TOEでは、許可利用者といったTOEを操作するために必要な権利や特権を有するTSFはない。TOEには、外部からの利用者を代行して働くサブジェクトは存在せず、TSFの他の利用者のデータにアクセスする利用者について関知する必要がないため、アクセス制御や情報フロー制御を実施しない。 よって本TOEでは、信頼できないサブジェクトによる外部の干渉、及び改ざんからTSFを保護する必要が無いため、相互サポートにおけるFPT_SEP.1の要件は不要である。

8.2.5 最小機能強度の妥当性

本TOEは、一般のオフィス等で使用される商業的製品であるデジタル複合機に実装されるものであり、想定される攻撃は公開情報を利用した不正行為である。
一般のオフィス等で使用されるため、攻撃者である悪意を持ったe-STUDIO利用者及びe-STUDIO非関係者は、攻撃を行う際に周囲に注意する必要がありTOEにアクセス可能な時間を制限され、また攻撃者が利用できる情報は公開情報のみであることを併せて考えれば、攻撃能力は低レベルとなることが想定される。
従って攻撃力が低レベルであるため、最小機能強度はSOF-基本が妥当である。

8.2.6 評価保証レベルの妥当性

評価保証レベルは、EAL2である。
本TOEは、一般のオフィス等で使用される商業的製品であるデジタル複合機に実装されるものである。悪意を持ったe-STUDIO利用者及びe-STUDIO非関係者の攻撃能力は低レベルであり、保護資産に対する攻撃の種別は限られている。
以上により、コストに見合うセキュリティ侵害に対抗できればよい。 従って、評価保証レベル2の保証パッケージが妥当である。

8.2.7 セキュリティ保証要件の根拠

以下のセキュリティ保証要件は、評価保証レベル2を満たす為に必要である。

- ACM_CAP.2 構成要素
- 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.1 記述的上位レベル設計
- 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
- ATE_COV.1 カバレージの証拠
- ATE_FUN.1 機能テスト
- ATE_IND.2 独立テスト-サンプル
- 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

また、以下のセキュリティ保証要件は、セキュリティターゲット評価に必要である。

- ASE_DES.1 セキュリティターゲット、TOE記述、評価要件
- ASE_ENV.1 セキュリティターゲット、セキュリティ環境、評価要件
- ASE_INT.1 セキュリティターゲット、ST概説、評価要件
- ASE_OBJ.1 セキュリティターゲット、セキュリティ対策方針、評価要件
- ASE_PPC.1 セキュリティターゲット、PP主張、評価要件
- ASE_REQ.1 セキュリティターゲット、ITセキュリティ要件、評価要件
- ASE_SRE.1 セキュリティターゲット、明示されたITセキュリティ要件、評価要件
- ASE_TSS.1 セキュリティターゲット、TOE要約仕様、評価要件

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。

表8.3-1 TOEセキュリティ機能とセキュリティ機能要件

	FAU_ARP.1	FAU_GEN.1	FAU_SAA.1	FAU_SAR.1	FCS_COP.1	FPT_AMT.1	FPT_RVM.1
SF.HDD_ENCRYPT					O		O
SF.REMOVE_DETECT	O		O				O
SF.RUN_MESSAGE				O			O
SF.SBOARD_CHECK		O				O	O

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。

FAU_ARP.1

SF.REMOVE_DETECTにより、セキュリティ侵害の可能性を検出した場合、操作パネル上にサービスマンコール表示と、e-STUDIO利用者機能の受付拒否により機能の使用を停止させる。
以上により、SF.REMOVE_DETECTでのセキュリティアラームは保証できる。

FAU_GEN.1

SF.SBOARD_CHECKにより、スクランブラボード上の識別情報から、
・監査の起動
・スクランブラボード取り外し事象
・スクランブラボード以外の不正なボードの装着事象
の監査記録を生成し、その中の情報として、
・事象の日付，時刻（RTCから取得したタイムスタンプ）
・事象の種別（スクランブラボードの装着有無）
・サブジェクト識別情報（監査要求元タスク情報）
・事象の結果（正常、またはエラー）
の記録を生成する。
以上により、SF.SBOARD_CHECKでの監査データ生成は保証できる。

FAU_SAA.1

SF.REMOVE_DETECTにより、監査対象事象として、
・スクランブラボード取り外し事象
・スクランブラボード以外の不正なボードの装着事象
を検出した場合にセキュリティ侵害であると判定する。
以上により、SF.REMOVE_DETECTでの侵害の可能性の分析は保証できる。

FAU_SAR.1

SF.RUN_MESSAGEにより、TOEの関係者に暗号化機能が適切に動作していることを認識させるため、操作パネルからの確認要求時に、TOEの型名、バージョン表示を行う。
以上により、SF.RUN_MESSAGEでの監査レビューは保証できる。
尚、監査記録をTOEの関係者に提供することについては、監査記録は秘密情報でないことから問題は無い。

FCS_COP.1

SF.HDD_ENCRYPTにより、鍵長112bitのTriple DES（FIPS PUB 46-3）のアルゴリズムによって、ユーザ文書データのHDD書込み時の暗号化操作、及びHDD読出し時の復号操作を実施する。
以上により、SF.HDD_ENCRYPTでの暗号操作は保証できる。

FPT_AMT.1

SF.SBOARD_CHECKにより、e-STUDIO 3511/4511の電源投入による初期立ち上げ中に、システムボードにスクランブラボードが正常に装着されていることを確認するために、妥当性テストを実行する。
以上により、SF.SBOARD_CHECKでの抽象マシンテストは保証できる。

FPT_RVM.1

①SF.HDD_ENCRYPTにより、スクランブラボード装着時に、システムボードからHDDへのデータ経路と、その逆の経路を単一化し、HDDへの書込み、またはHDDから読出されるデータは、必ず暗号化チップを介するようにする。
②SF.SBOARD_CHECKにより、e-STUDIO 3511/4511の起動処理が開始され、IDEドライバ初期化処理が開始されたタイミングで、スクランブラボードの装着確認を行い、監査記録を生成する。

③SF.REMOVE_DETECTにより、SF.SBOARD_CHECKによる監査記録が生成されたタイミングで、セキュリティ侵害の判定を行い、セキュリティ侵害と判定された場合、サービスマンコール表示と、e-STUDIO利用者機能の受付拒否によるデジタル複合機の機能停止を行なう。
④SF.RUN_MESSAGEにより、ボタン操作時に実行される設定／登録ユーザインターフェイスにおける設定情報取得処理の最初に、暗号化機能の動作確認情報を読出し、その結果が正常な場合、TOEの型名、バージョンの情報を操作パネルに表示されるようにする。
①により、SF.HDD_ENCRYPTでのTSPの非バイパス性は保証できる。
②により、SF.SBOARD_CHECK, ③により、SF.REMOVE_DETECT, ④により、SF.RUN_MESSAGEでのTSP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EAL2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、各保証手段毎の内容を示す。

表8.3-2 セキュリティ保証手段一覧

ドキュメント／TOE名称	内容	保証要件 クラス	保証要件 コンポーネント
スクランブラボード GP-1031 TOE構成表	TOEの構成表。 TOEの構成するバージョン、及び識別子が記述されている。	ACM 構成管理	ACM_CAP.2
スクランブラボード GP-1031 ソフトウェアバージョン管理表	TOE部分のソフトウェアバージョン管理表。 TOE部分のソフトウェアのバージョンアップ規定と、TOEを構成するモジュールの一覧が記述されている。		
PWA-F-DES-340	スクランブラボードの図面。 TOEであるスクランブラボードに実装されている部品構成や変更履歴が記述されている。		
スクランブラボード GP-1031 IDEドライバファイル構成一覧	IDEドライバのファイル構成一覧。 e-STUDIO 3511/4511用システムソフトウェアバージョンと、IDEドライバを構成するファイル一覧が記述されている。		
スクランブラボード GP-1031 暗号化機能動作表示 ファイル構成一覧	暗号化機能の動作表示ファイル構成一覧。 e-STUDIO 3511/4511用システムソフトウェアバージョンと、暗号化機能動作表示を構成するファイル一覧が記述されている。		
スクランブラボード GP-1031 暗号化機能迂回検出 ファイル構成一覧	暗号化機能の迂回検出ファイル構成一覧。 e-STUDIO 3511/4511用システムソフトウェアバージョンと、暗号化機能迂回検出を構成するファイル一覧が記述されている。		
スクランブラボード GP-1031 暗号化機能動作確認 ファイル構成一覧	暗号化機能の動作確認ファイル構成一覧。 e-STUDIO 3511/4511用システムソフトウェアバージョンと、暗号化機能動作確認を構成するファイル一覧が記述されている。		
スクランブラボード GP-1031 構成リスト	TOEの構成要素リスト。 TOEを構成するハードウェア，ソフトウェア，ドキュメントを一意に識別するための情報が記述されている。		
スクランブラボード GP-1031 構成管理規約	TOEの構成管理の対象とその管理方法を定めた規約。 TOEの開発に関連するドキュメント，ソースコード、及びオブジェクトコードなどを対象とした構成管理方法が記述されている。		
品名コードの発番 および品名記載規程	図面の発番規定。 図面等の品名コードの発番と、設計変更についての規程が記述されている。		
製品技術資料 (TB)体系規程	製品技術資料の体系及び発番規定。 製品技術資料及びセキュリティ保証手段ドキュメント等の発番、分類及びファイリング，保管についての規程が記述されている。		
サービスドキュメント 資料番号発番規定	ガイダンス関係の発番規定。 取扱説明書等ガイダンスの発番と、変更についての規定が記述されている。		
VSS管理規約	ソフトウェアのVSS登録管理規約。 ソフトウェアのVSSへの登録ルールが記述されている。		
リリースバージョン管理規約	SYS-ROMのバージョン名付与規定。 ROMﾃﾞｰﾀが書込みされたFlashROMのバージョン名の付与基準が記述されている。		

ドキュメント／TOE名称	内容	保証要件 クラス	保証要件 コンポーネント
スクランブラボード GP-1031 サービスマニュアル 【日本語名】 Scrambler Board GP-1031 Service Manual 【英語名】	サービスエンジニア向けガイダンス文書。 サービスエンジニアに対するTOEの設置手順、及びトラブルシューティング手順が記述されている。TOEの設置に関し、e-STUDIO管理者と実施するTOEの装着及び立上げ作業における注意事項、TOEのソフトウェアインストール手順が詳述されている。また、TOEを含むデジタル複合機の廃棄(交換)時における、HDDの消去手順も記述されている。	ADO 配付と運用 AGD ガイダンス文書	ADO_DEL.1 ADO_IGS.1
スクランブラボード GP-1031 取扱説明書 【日本語名】 Scrambler Board GP-1031 Operator's Manual 【英語名】	e-STUDIO管理者とe-STUDIO利用者向けガイダンス文書。 e-STUDIO利用者向けに、TOEの機能説明、及びTSFの作動確認方法、e-STUDIO管理者向けに、鍵コードの入力や管理方法の説明や残存データ全消去の確認方法が記述されている。		ADO_DEL.1 ADO_IGS.1 AGD_ADM.1 AGD_USR.1
Check sheet	TOEの配付、及び設置から立上げまでのチェックシート。 TOEが配送途中で改変されていないことをe-STUDIO管理者がチェックするためのシートであり、TOEの梱包状態、鍵コード封筒の状態、TSFの作動などの確認を行うための項目が記述されている。		ADO_DEL.1 ADO_IGS.1
スクランブラボード GP-1031 物流手順書	TOEの配付手続きに関する証拠資料。 TOEのハードウェアとドキュメントを対象に、メーカーの倉庫からの倉出しから客先据付までの管理と配送設備、手続きについて記述されている。		ADO_DEL.1
スクランブラボード GP-1031 梱包・倉入れ手順書	TOEの配付手続きに関する証拠資料。 TOEのハードウェアとドキュメントを対象に、梱包からメーカー倉庫への倉入れまでの管理と配送設備、手続きについて記述されている。		ADO_DEL.1
スクランブラボード GP-1031 ROMデータ配付手順書	TOEの配付手続きに関する証拠資料。 TOEのソフトウェアであるROMデータをe-STUDIO 3511/4511のシステムボードのFlash ROMにダウンロードするまでの管理と配送設備、手続きについて記述されている。		ADO_DEL.1
GP-1031 with GO-1030 開梱据付指示書【日本語名】 GP-1031 with GO-1030 Unpacking Instruction【英語名】	TOEの設置から立上げまでの手順書。 サービスエンジニアが行う、TOEの設置から立上げまでの手順が記述されている。		ADO_DEL.1 ADO_IGS.1
スクランブラボード GP-1031 機能仕様書(FSP)	機能仕様書。 TSFのふるまいとTSFインターフェイス、TSF以外の機能についての外部インターフェイスについて記述されている。	ADV 開発	ADV_FSP.1
スクランブラボード GP-1031 上位レベル設計書(HLD)	上位レベル設計書。 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ーフェイスについて記述されている。		ADV_HLD.1
スクランブラボード GP-1031 表現対応分析書	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におけるセキュリティ機能の関係、機能仕様書におけるセキュリティ機能と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。		ADV_RCR.1
e-STUDIO 3511/4511用 スクランブラボード GP-1031 Security Target	セキュリティターゲット。	ASE セキュリティターゲット評価	ASE_DES.1 ASE_ENV.1 ASE_INT.1 ASE_OBJ.1 ASE_PPC.1 ASE_REQ.1 ASE_SRE.1 ASE_TSS.1

ドキュメント／TOE名称	内容	保証要件 クラス	保証要件 コンポーネント
スクランブラボード GP-1031 テスト仕様書	テスト証拠資料。 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について記述されている。	ATE テスト	ATE_COV.1 ATE_FUN.1 ATE_IND.2
スクランブラボード GP-1031 テスト成績書	テスト証拠資料。 テスト仕様書に基づいて、TSFがその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。		
スクランブラボード GP-1031 【日本語名】 Scrambler Board GP-1031 【英語名】	TOE。		
スクランブラボード GP-1031 機能強度分析書	機能強度分析書。 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。但し、本TOEでは機能強度分析対象となる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は存在しない。	AVA 脆弱性評定	AVA_SOF.1
スクランブラボード GP-1031 脆弱性分析書	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_VLA.1

8.4 PP主張根拠

本STにて適合するPPはない。