暗号化ストレージ・デバイス
プロテクションプロファイル

本書は、スウェーデン政府が作成したプロテクションプロファイルの一部を調達要件の検討のため、参考として日本語に直訳したものです。IT セキュリティ評価及び認証制度における適合 PP として利用する場合は、正式な文書である英語版のみとなります。

正式な文書は、以下の URL よりダウンロード可能です。

http://www.fmv.se/Global/Dokument/Verksamhet/CSEC/PP%20USB.pdf

平成 25 年 6 月 3 日　翻訳 暫定第 0.1 版
独立行政法人情報処理推進機構
技術本部 セキュリティセンター
情報セキュリティ認証室

目次

1 はじめに

1.1 PP 参照

表 1: PP 参照	
PPタイトル	暗号化ストレージ・デバイス・プロテクションプロファイル
PPバージョン	2.1
TOE	データの一時保管に使用する個人用ストレージ・デバイス
評価保証レベル	EAL2（ATE_COV.2を追加）
CCバージョン	CC v3.1. 改訂第3版
PP作成者	Anna-Lena Hallgren

1.2 TOE 概要

本プロテクション・プロファイル（PP）は、あるデータが 2 つの高信頼ホストコンピュータ相互においてやり取りされるときに、そのデータの一時保管のために使用する暗号化された個人用の記憶装置（ストレージ・デバイス）に適用する。

ストレージ・デバイスの永続性メモリに記憶されている秘匿性の高い情報は、万が一当該ストレージ・デバイスが紛失にあったり盗難にあったりした場合に、許可されていない者がそれを不正に開示することを防ぐため、すべて暗号化されなければならない（shall）。

利用者は、他の操作の実行を許可される前に、ユーザシークレットの提供を受け、そのデバイスから認証を受けることを要求されなければならない（shall）。ユーザシークレットは、そのデバイス上で直接入力されるか、高信頼ホストコンピュータ上で動作しているアプリケーションを介して入力されなければならない（shall）。ユーザシークレットがホストコンピュータに入力されることになる場合、そのアプリケーションも TOE の一部とみなされる。そのユーザシークレットは、バイオメトリクス識別子（biometric identifier）であってはならない（shall not）。

当該ストレージ・デバイスを暗号化するために必要な鍵はいずれも、鍵導出スキームを使用したユーザシークレットに由来するものであるか、乱数生成器で生成されなければならない（shall）。ユーザシークレットは、対象とするクラスの敵対者（adversary）からのユーザシークレットに関する全数検索が計算量的に実行不可能（computationally infeasible）となる程度の十分なエントロピーを備えていなければならない（shall）。

全数検索を受けにくくするために、当該ストレージ・デバイスは、認証試行の間違いについては遅延機構（delay mechanism）を導入することができる（may）。これは推奨事項の1つであり、本プロテクションプロファイルには遅延メカニズムに関する要件はない。

ストレージ・デバイスに対して初期化又は認証を行う際に高信頼ホストコンピュータ上のアプリケーションが使用される場合には、そのアプリケーションの真正性は検証されなければならない（shall）。利用者がアプリケーションの真正性を検証できる手順は確立されなければならない（shall）。

ストレージ・デバイスで使用されるあらゆる暗号アルゴリズムと暗号スキームは、当該デバイスが使用されることになる国の関係国家当局により、目的とする用途のために承認を受けなければならない（shall）。国の規制がない場合には、HKV 12 830:51795「Swedish national list of approved cryptographic primitives for use with the PP for Encrypted Storage Devices（暗号ストレージ・デバイスについて PP で使用するための正規暗号プリミティブに関するスウェーデン国家リスト）」を使用しなければならない（shall）。ホストコンピュータ上で実行する認証用アプリケーションに実装され得る KDF の可能性を除いて、すべての暗号アルゴリズムや暗号スキームをはじめとするセキュリティ機能は、ストレージ・デバイスに実装されなければならない（shall）。ストレージ・デバイスは、乱数生成及び暗号メカニズムの自己テストを実装すべきである（should）。自己テストは推奨事項の 1 つであり、本プロテクションプロファイルでは自己テストに関する要件はない。

1.2.1 TOE アーキテクチャ

この TOE のアーキテクチャには、タイプ A とタイプ B の 2 つがある。

アーキテクチャのタイプ A では、初期化用アプリケーションと認証用アプリケーションは、ストレージ・デバイス上に保管され、このストレージ・デバイスによって実行される。ユーザシークレットはストレージ・デバイスに直接入力される。

アーキテクチャのタイプ B では、初期化用アプリケーションと認証用アプリケーションはホストにより実行される。ユーザシークレットは、ストレージ・デバイスにホスト経由で入力される。初期化用アプリケーションと認証用アプリケーションは、ホスト上にインストールされるか、ストレージ・デバイス上に保管されるかもしれない（may）。

いずれのタイプでも、初期化用アプリケーションと認証用アプリケーションは TOE に組み込まれている。

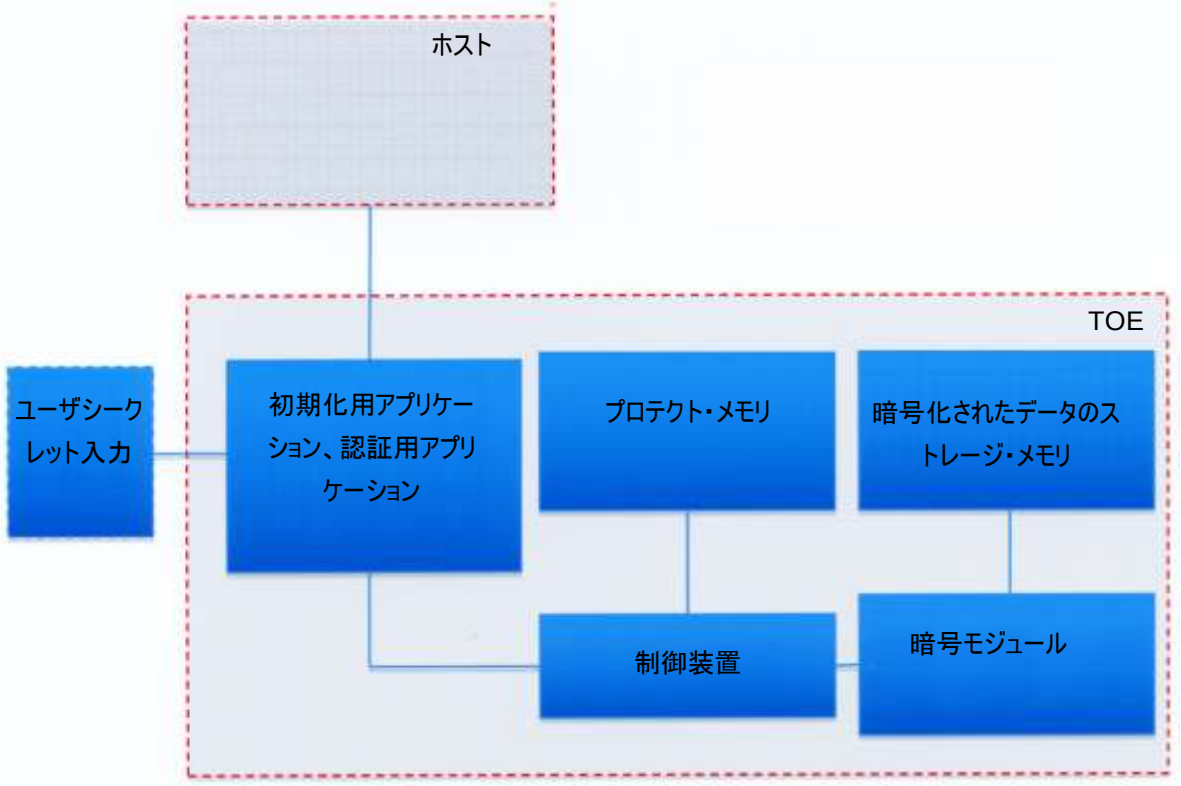

図 1 TOE アーキテクチャ タイプ A

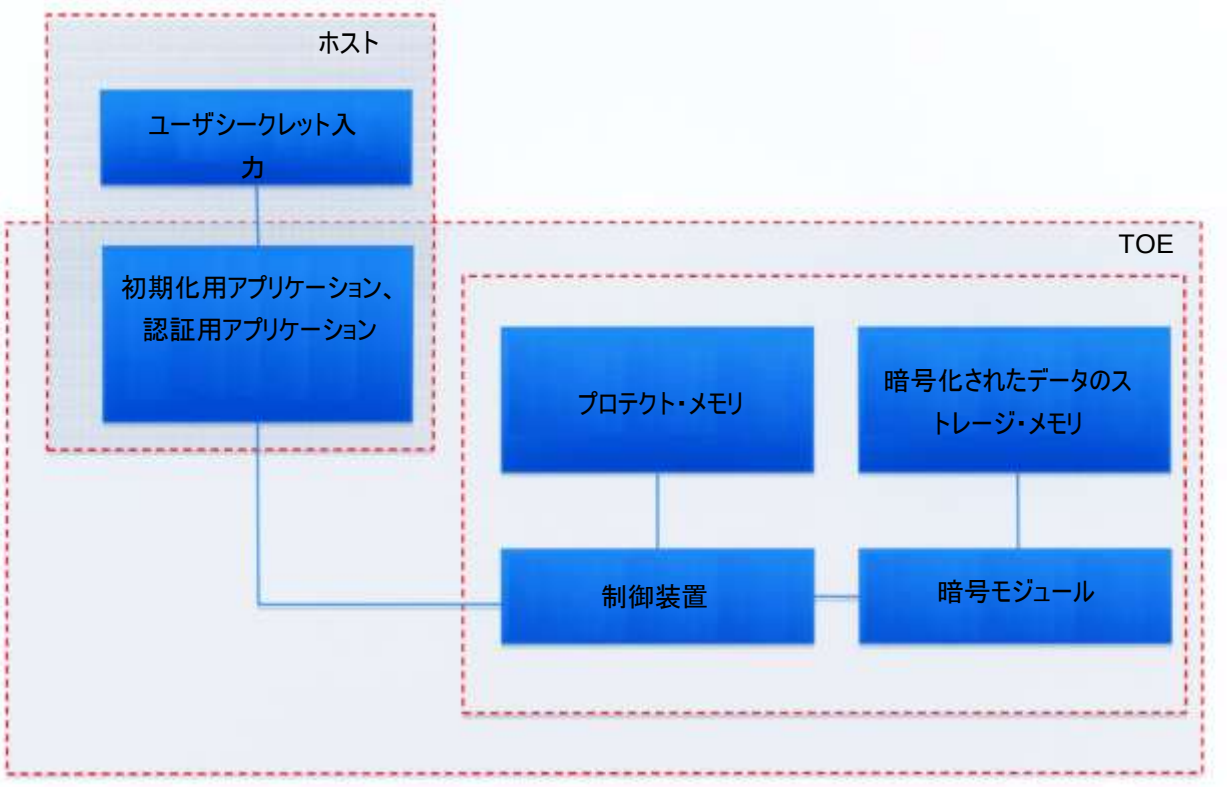

図 2 TOE アーキテクチャ タイプ B

1.2.2 TOE インタフェース

ストレージ・デバイスのアーキテクチャ タイプ A へのインタフェースはホストコンピュータである。

初期化用アプリケーションと認証用アプリケーション（又はこのうちのいずれか）がホスト内に置かれ、ユーザシークレット入力もホスト内に置かれる場合、ストレージ・デバイスのアーキテクチャ タイプ B へのインタフェースは、この初期化用アプリケーションと認証用アプリケーション（又はこのうちのいずれか）である。

1.2.3 TOE コンポーネント

TOE のコンポーネントは以下のとおりである。

1.2.3.1 プロテクト・メモリ（Protected memory）

プロテクト・メモリには、TOE を適切に操作するために必要となるシステム・ファイルが収められる。プロテクト・メモリに保管されているファイルは、巧みな操作を受けないよう保護されている。

プロテクト・メモリは、初期化用アプリケーションと認証用アプリケーションを保管するために使用することができる（may）。初期化用アプリケーションと認証用アプリケーションを格納しているこのメモリの一部は、ホストコンピュータにさらされるかもしれない（may）。

プロテクト・メモリは、ホストについては読み取り専用にされなければならない（shall）。プロテクト・メモリの内容を改変する可能性のある更新はいかなるものであっても、メモリの内容に巧みな操作が加えられないよう、信頼できる第三者によって署名されていなければならない（shall）。

秘匿性の高い利用者データはすべて、鍵暗号化鍵（KEK）により保護されているデータ暗号化鍵（DEK）を使用して暗号化される。KEK は、鍵導出関数（KDF）を使用してユーザシークレットから導出される。

暗号化された DEK と、KDF への入力として使用されるソルトは、プロテクト・メモリに保管することができる（may）。

1.2.3.2 ストレージ・メモリ

ストレージ・メモリは永続的で、読み込み/書き込み可能であり、暗号化されたデータ・ブロックを保管するために使用される。

1.2.3.3 制御装置

制御装置は、ストレージ・デバイスとホスト間の情報の流れを制御する。またこの装置は、ストレージ・メモリ及びプロテクト・メモリへのアクセスも制御する。

1.2.3.4 暗号モジュール

暗号モジュールは、ユーザシークレットがホスト上で実行するアプリケーションを介して入力される場合には、KDF の可能性を除いて、乱数生成をはじめとするあらゆる暗号操作を管理する。暗号化された DEK と、KDF への入力として使用されるソルトは、暗号モジュールに保管することができる（may）。

1.2.3.5 認証用アプリケーション

認証用アプリケーションは、認証中に利用者により実行される。利用者は、認証用アプリケーションを使用して、ユーザシークレットの情報をストレージ・デバイスに提供する。

認証用アプリケーションは、ホストコンピュータ上にインストールされてもよいし、ストレージ・デバイス上のプロテクト・メモリから直接実行されてもよい（may）。秘匿性の高い情報を扱う時には認証用アプリケーションが必要となる可能性がある。

このように秘匿性の高い情報は、ホストコンピュータ上の入力用周辺装置を経由するか、ストレージ・デバイスに直接接続された入力装置を経由して、認証用アプリケーションに供給される可能性がある。

1.2.3.6 初期化用アプリケーション

初期化用アプリケーションは、鍵階層をセットアップするために使用される。初期化に関する詳細は、第 1.2.5.2 章を参照されたい。

初期化アプリケーションは、ホストコンピュータ上にインストールされてもよいし、ストレージ・デバイス上のプロテクト・メモリから直接実行されてもよい（may）。

1.2.4 用途

この TOE は個人用であり、暗号化された個人用ストレージ・デバイス内のデータを一時的に保管するためのみに使用されるが、データは 2 つの高信頼ホストコンピュータ間を移動している。TOE 利用者は、TOE の取り扱いという点で信頼されており研修も受けている。TOE 利用者は、秘匿性の高い情報にアクセスする認可を受けている。TOE は高信頼の環境で正当な利用者によって使用されなければならない（shall）。

この TOE で移送されるデータは、たとえばプレゼンテーション資料、議事録、電子メール、事業計画書及び事業報告書、

政府文書などを挙げることができる。この情報はホスト・システム内の情報の複製である。

ストレージ・デバイスは、窃盗や巧みな操作が行われないような方法で保管され取り扱われなければならない（shall）。万一ストレージ・デバイスが紛失又は盗難に遭った後回収され、そのデバイスが改ざんされたことが疑われる場合には、そのデバイスは破棄されなければならない（shall）。ストレージ・デバイスには、デバイスの改ざんを困難にする改ざん保護手段を備えることができる（may）。これは推奨事項の1つであり、本プロテクションプロファイルには改ざん保護に関する要件はない。

ストレージ・デバイスは、輸送中にデバイスに対して第三者による巧みな操作が加えられないような方法で、製造業者から最終利用者に配付されなければならない（shall）。

ストレージ・デバイスに対して初期化又は認証を実行するために高信頼ホストコンピュータ上のアプリケーションが使用される場合には、そのアプリケーションの真正性が検証されなければならない（shall）。

1.2.5 セキュリティの特徴（Security features）

この TOE の特徴は、鍵管理、初期化、認証、暗号化、復号及びメモリ無害化のためのセキュリティ機能である。ファームウェアが更新可能であれば、ファームウェア更新用のセキュリティ機能が TOE 内に用意されている。オプションとして、読み取り専用モード設定用の手動スイッチが用意されている。これは推奨事項の 1 つであり、読み取り専用モードによる TOE 設定のための手動スイッチに関する要件はこの PP には含まれていない。

1.2.5.1 鍵管理

ストレージ・デバイス内の永続性メモリに保管されている秘匿性の高い情報はすべて、関係国家当局による用途での承認を受けた暗号アルゴリズムを使用して、十分な強度を備えた鍵の下で暗号化されなければならない（shall）。

ホストコンピュータ上で実行する認証用アプリケーションに実装され得る KDF の可能性を除いて、すべての暗号操作は暗号モジュールに実装されなければならない（shall）。

KDF は、ユーザシークレットから KEK を導出する場合に使用される。

1.2.5.2 初期化

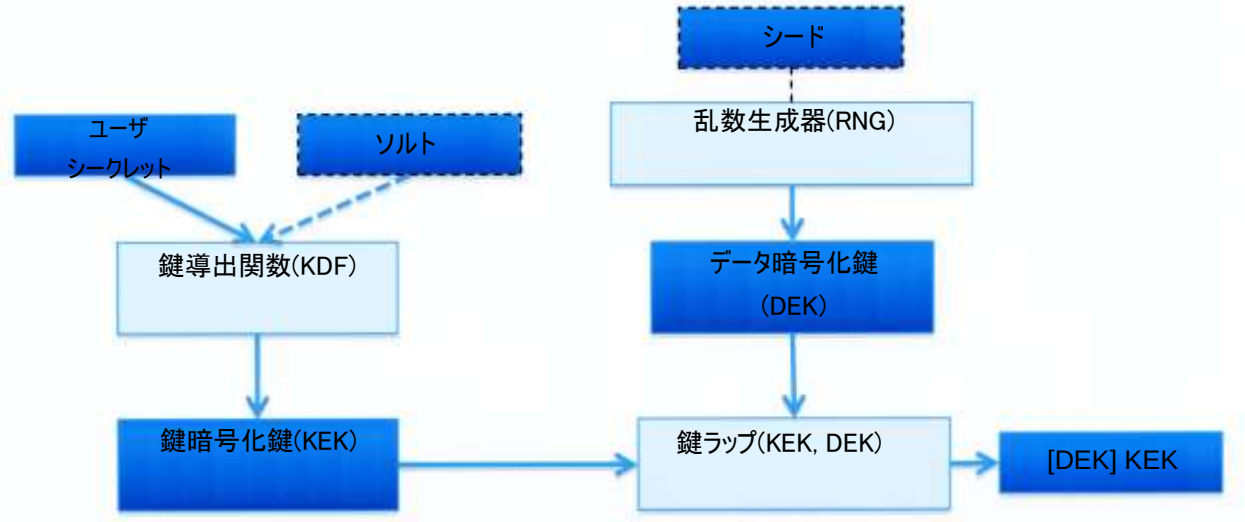

図 3 初期化

ストレージ・デバイスの初期化の段階で、利用者は、対象とする敵対者クラスからのユーザシークレットに関する全数検索を計算量的に実行不可能にする程のエントロピーを備えたユーザシークレットを選択しなければならない（shall）。TOE は、ユーザシークレットが、組織のセキュリティ方針によって定義された品質基準に適合することを検証するしくみを提供すべきである（should）。

DEK は、ストレージ・デバイス内の暗号モジュールに実装された乱数生成器（RNG）により生成されなければならない（shall）。シードを RNG に入力することは可能であり、決定論的疑似乱数生成器はシードから疑似ランダム・ビット・シーケンスを導出する。シードには、対象とする敵対者クラスからの全数検索を計算量的に実行不可能にする程度の十分なエントロピーが格納されていなければならない（must）。シードは一様に配付される必要はない。生成された DEK には、対象とする敵対者クラスが、可能性のあるすべての鍵に対して仕掛ける全数検索を計算量的に実行不可能にする程度の十

分なエントロピーが格納されていなければならない（must）。

ソルト（KDF が必要とする場合）及びユーザシークレットは、KEK を生成するための KDF への入力として供給されなければならない（shall）。DEK は、KEK の下で暗号化されなければならず、その結果は（$[DEK]_{KEK}$ で表示）はストレージ・デバイスに保管されなければならない（shall）。

すべての KDF がソルトを必要としているというわけではない。使用された KDF がソルトを必要とする場合には、対象とする敵対者クラスに対して予測不可能なソルトでなければならない（shall）。ソルトは、RNG によって生成されて TOE にインポートされる場合もあるし、稼働中に生成されて保管される場合もある。ソルトはストレージ・デバイスに保管されなければならない（shall）。ソルトは秘密（シークレット）ではないため、永続性メモリに保管することができる（may）。

平文の DEK 及び KEK は絶対に暗号モジュールを離れてはならない（shall never）。

また、エントロピー源、乱数生成器、暗号メカニズム又は鍵の導入がセキュリティに悪影響を及ぼさないということを示すことができる場合には、追加のエントロピー源、乱数生成器、暗号メカニズム又は鍵が導入されてもよい（may）。

すでに初期化されているストレージ・デバイスの再初期化は可能でなければならない（shall）。ストレージ・デバイスが再初期化された段階で、暗号化された鍵はすべてゼロ化され、上記に示した初期化の手順が繰り返し実行される。

1.2.5.3　認証

利用者には、他のアクションを実行することが許可される前に、認証することが要求されなければならない（shall）。認証の最中に、利用者にはユーザシークレットを提供することが要求されなければならない（shall）。

ユーザシークレットは利用者により提供され、ソルトはストレージ・デバイスに保管され、KEK を生成するために KDF に入力される。次に、暗号化された DEK を復号するために KEK が使用される。DEK が復号されてしまえば、利用者データのブロックは任意に暗号化されてもよく、復号されてもよい（may）。

ストレージ・デバイスがホストから切断される場合には、セッションは終了されなければならず、かつ、ストレージ・デバイスに保管されているデータにアクセスするために利用者には再認証することが求められなければならない（shall）。

1.2.5.4　暗号化

ホストコンピュータがデータ・ブロックをストレージ・デバイスに書き込む場合、平文のブロックは DEK の下でストレージ・デバイス内の暗号モジュールにより暗号化されなければならない（shall）。暗号化されたブロックは次に、ストレージ・デバイス内のストレージ・メモリに書き込まれなければならない（shall）。

1.2.5.5　復号

ストレージ・デバイスのブロックがホストコンピュータによって要求されると、保管されているブロックがストレージ・メモリから呼び出され、ストレージ・デバイス内の暗号モジュールにより DEK の下で復号されなければならない（shall）。復号された平文のブロックは、次にホストコンピュータに送信されなければならない（shall）。

1.2.5.6　メモリの無害化（Memory sanitization）

暗号鍵及びユーザシークレットは、TOE を適切に操作する上でその鍵とユーザシークレット（又はこのうちのいずれか）が不要になった時点で、セキュアにゼロ化されなければならない（shall）。

1.2.6 オプションとしてのセキュリティの特徴

ストレージ・デバイスにはオンボードで更新可能なファームウェアを搭載することができる（may）。ファームウェアが更新可能である場合には、ファームウェア更新パッケージは信頼される者によって署名されていなければならず、署名されたパッケージの真正性は、それが更新パッケージに関して他のアクションを実行する前に、ストレージ・デバイスによって検証されなければならない（shall）。署名の検証に使用される公開鍵は、製造時に生成され、ストレージ・デバイスに保管される。

1.3 追加的な TOE ソフトウェア、ハードウェア、ファームウェア

TOE セキュリティ機能は、TOE 外部のコンポーネントには依存しない。

1.4 略語

[DEK]KEK	鍵暗号化鍵（KEK：Key Encryption Key）の下で暗号化されたデータ暗号化鍵（DEK：Data Encryption Key）
CC	Common Criteria（コモンクライテリア）
DEK	Data Encryption Key（データ暗号化鍵）
EAL	Evaluation Assurance Level（評価保証レベル）
KDF	Key Derivation Function（鍵導出関数）
KEK	Key Encryption Key（鍵暗号化鍵）
PP	Protection Profile（プロテクションプロファイル）
RNG	Random Number Generator（乱数生成器）
TOE	Target Of Evaluation（評価対象）

1.5 用語集

エントロピー	ビットの集合により生成された情報の総量。 エントロピーとは、同じビットの集合を再生産することができる敵対者に対して必要となる労力（work effort）を代表するものである（ISO/IEC 18032）。 nビット長の鍵では、エントロピーは0～nの間にある。この場合、上限が達成されるのは、その鍵に対して起こり得るあらゆる値が等確率を持つ場合、及びこうした場合のみになる。
ファズ・テスト	ファズ・テストとは、無効なデータ、想定外のデータ又はランダムなデータをコンピュータ・プログラムの入力値として注入することを伴うソフトウェアのテスト手法の1つで、自動化または半自動化されていることが多い。これにより、プログラムは、クラッシュや組み込みコードのアサーション違

	反などの例外、又は潜在的なメモリ・リークの検出のために監視される。ファジングは通常、ソフトウェア又はコンピュータ・システム内のセキュリティ問題をテストするために使用される。
鍵導出関数（KDF）	鍵導出関数（KDF）は、エントロピーを格納している入力ビット・シーケンスから暗号鍵を導出する。入力ビット・シーケンスは、一様に配付される必要はない。
永続性メモリ（Persistent memory）	回路内に蓄積されたデータが、電源喪失時又は電源をいったん切ってすぐに入れ直した時に保持されているようなメモリ回路。
乱数生成器（RNG）	乱数生成器（RNG）とは、ビット・シーケンスを生成するアルゴリズム又は物理的装置である。RNGにより生成されたビット・シーケンスは、真性ランダム・ビット・シーケンスとコンピュータ的に見分けがつかないものでなければならない（shall）。 暗号アプリケーションで使用される乱数生成器（RNG）は、組み合わせることで乱数のサブシーケンス又はブロックになることもあるゼロ及び1ビットのシーケンスを生成する。方法としては主に、物理的真性RNG（physical true RNG）、非物理的真性RNG（non-physical true RNG）及び決定論的RNGの3つがある。物理的真性RNGは、TOE境界内部のみの物理的な乱数源に依存する出力を生成する。非物理的真性RNGは、TOE境界外部からエントロピー源を取得する（RAMデータ又はPCのシステム時刻などのシステム・データ、API関数の出力など、又はキー・ストローク、マウスの動きなどのような人間の動作など）。非物理的真性RNGは、初期乱数値（シード）からのビットのシーケンスを生成するアルゴリズムから成る。 物理的ハイブリッドRNG及び決定論的ハイブリッドRNGでは、乱数生成器は両方の方法を用いて乱数を計算する。たとえば、このRNGでは、疑似乱数を生成するアルゴリズムの初期値（通常シードという）として真性乱数を使用する。
ソルト（Salt）	ソルトとは、オフライン攻撃（pre-computation attack）を避けるために、ユーザシークレットとともにKDFに入力される値である。 新規ソルトは、対象とする敵対者クラスによってそのソルトが予測されないような方法で、製造されたストレージ・デバイスごとにランダムに選択されなければならない（shall）。
シード（Seed）	決定論的疑似乱数生成器は、シードから疑似ランダム・ビット・シーケンスを導出する。 シードには、対象とする敵対者クラスからの全数検索を計算量的に実行不可能にする程度の十分なエントロピーが格納されていなければならない（must）。シードは一様に配付される必要はない。
評価対象（TOE）	評価の対象となっている製品またはシステム。
ユーザシークレット（User secret）	秘匿性の高いデータにアクセスする際に利用者を認可するために使用されるパスワードなどの認証属性（SA.User_Secret）。
揮発性メモリ	回路内に蓄積されたデータが、電源喪失時又は電源をいったん切ってすぐに入れ直した時に保持されていないようなメモリ回路。
（暗号化鍵又は秘密	メモリ領域はその領域をアクティブに上書きすることでゼロ化される。メモリ領域がゼロ化してしま

（シークレット）の）ゼロ化	った後は、メモリ領域に元々保管されていたデータ又はその一部を再構築することは実行不可能になっていなければならない（shall）。 秘密（シークレット）がゼロ化された場合には、秘密（シークレット）又はその断片、あるいはそこから派生される内容が格納されているすべてのメモリ領域はゼロ化されていなければならないため、その秘密（シークレット）を再構築することは実行不可能である。

2 適合主張

2.1 CC 適合主張

本プロテクションプロファイルは、以下の各項目に適合していることを主張する。

- 「Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model（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：概説と一般モデル）」、CCMB-2009-07-001、バージョン 3.1、改訂第 3 版、2009 年 7 月
- 「Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components（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 2：セキュリティ機能コンポーネント）」、CCMB-2009-07-002、バージョン 3.1、改訂第 3 版、2009 年 7 月
- 「Common Criteria for Information Technology Security Evaluation, Part 3: Security Functional Components（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 3：セキュリティ保証要件）」、CCMB-2009-07-003、バージョン 3.1、改訂第 3 版、2009 年 7 月

以下のとおりである。

- 本プロテクションプロファイルは、コモンクライテリアのパート 2 拡張およびコモンクライテリアのパート 3 に適合している。
- 本プロテクションプロファイルは、ATE_COV.2 を追加した保証要件パッケージ EAL2 に適合している。

2.2 PP 主張

本プロテクションプロファイルは、他のプロテクションプロファイルへの適合性を主張しない。

2.3 適合性宣言（Conformance statement）

この PP は、この PP への適合性を主張する ST 又は PP によって論証適合を要求する。

3 セキュリティ課題定義

3.1 資産

保護すべき資産とは以下の表のとおりである。

表 2: 資産	
ID	説明
SA.User_Data	TOE内に保管されているか、TOEによって処理された秘匿性の高い平文の利用者データ。
SA.User_Secret	TOEから認証を受ける時に利用者によって使用される秘密（シークレット）。
SA.Keys	平文の暗号化鍵 （DEKやKEKなど）。

3.2 脅威エージェント

攻撃者（脅威エージェント）とは、失われたストレージ・デバイスを検出するか、（電源が切れている状態で）それを盗み、TOE に対して攻撃を仕掛ける人物を指す。攻撃者の主な目標は、秘匿性の高いデータ（SA.User_Data）にアクセスすることである。攻撃者には基本的な攻撃能力が備わっている。

3.3 脅威

表 3: 脅威	
ID	説明
T.Extract_User_Data	電源が切れている状態で、かつSA.User_Data又はその一部をメモリ回路から平文で抽出できる時、攻撃者はストレージ・デバイスにアクセスする。
T.Extract_User_Secret	電源が切れている状態で、かつSA.User_Secret又はその一部をメモリ回路から平文で抽出できる時、攻撃者はストレージ・デバイスにアクセスする。 攻撃者は、ストレージ・デバイスが切断されており、SA.User_Secretを平文で抽出できる時に認証用アプリケーション及び初期化用アプリケーションにアクセスする。
T.Extract_Keys	電源が切れている状態で、かつSA.Keys又は関連情報をメモリ回路から平文で抽出できる時、攻撃者はストレージ・デバイスにアクセスする。 KDFがホストコンピュータで実行されている場合： 攻撃者は、ストレージ・デバイスが切断されており、KEKを平文で抽出できる時に認証

	用アプリケーション及び初期化用アプリケーションにアクセスする。
T.Manipulation	攻撃者は、電源が切れているストレージ・デバイスに一時的にアクセスし、攻撃者が先々SA.User_Dataを抽出又は計算できるよう、そのストレージ・デバイス内のセキュリティ機能を操作する。 適用上の注意： 攻撃が可能となるのは、攻撃者による操作を受けてしまった後で利用者がストレージ・デバイスから認証を受ける場合、及びその後攻撃者がストレージ・デバイスへの物理的アクセスを2回目に取得する場合のみである。
T.Exhaustive_Search	攻撃者はストレージ・デバイスにアクセスし、全数検索を仕掛けることでSA.User_Secret又はSA.Keysの計算を試みる。
オプションとして、ファームウェア更新が可能な時に、以下が適用可能である： T.Malicious_Upgrade	攻撃者は、将来的に自らがSA.User_Dataを抽出又は計算できるようTOE内のセキュリティ機能を操作する目的で、不正なファームウェア又はソフトウェアの更新によってTOEを更新するか、TOE利用者をあざむいてTOEを更新させる。 適用上の注意： 攻撃が可能となるのは、攻撃者による操作を受けてしまった後、利用者がストレージ・デバイスから認証を受ける場合、及びその後攻撃者がストレージ・デバイスへの物理的アクセスを2回目に取得する場合のみである。

3.4 前提条件

表 4：前提条件	
ID	説明
A.Trusted_Users	TOE利用者は、TOEを取り扱うという点で信頼されており研修も受けている。TOE利用者は、秘匿性の高い情報にアクセスするための認可を受けている。
A.Trusted_Host	ホストコンピュータは信頼されている。ホストコンピュータにアクセスできるのは、許可された利用者のみである。ホストコンピュータの環境は信頼されている。
A.Legitimate_Usage	TOEは、高信頼の環境で信頼を受けている利用者の管理下になければならない（shall）。
A.Lost_Storage_Device	万一ストレージ・デバイスが紛失又は盗難に遭った後回収され、認可を受けていない者がそのデバイスを改ざんしたことが疑われる場合には、そのデバイスは破棄されなければならない（shall）。
オプションとして、ファームウェア更新が可能な時に、以下が必要である： A.Signing_Key	ファームウェア更新署名鍵（firmware upgrade signing key）は、信頼されている者により扱われ、正規のファームウェア更新パッケージに署名する場合にのみ使用される。信頼されている者が鍵を扱うため、鍵は漏洩や操作から保護される。 鍵は、対象の敵対者クラスからのプライベート署名鍵の暗号解読を防止する程度の強度を備えた鍵を提供する方法で生成される。

オプションとして、初期化用のアプリケーション及び認証用のアプリケーションがホスト上で実行されている時に、以下が必要である: A.Application_for_initializa-tion_and_for_authentication	初期化用アプリケーション及び認証用アプリケーションの真正性は、インストール又は更新の前に検証されなければならない（shall）。利用者がアプリケーションの真正性を検証できる手順は確立されなければならない（shall）。

3.5 組織のセキュリティ方針

表 5: 組織のセキュリティ方針

ID	説明
P.Entropy	ユーザシークレット（SA.User_Secret）は、対象とするクラスの敵対者からのユーザシークレットに関する全数検索を計算量的に実行不可能にする程度の十分なエントロピーを備えていなければならない（shall）。
P.Crypto	暗号鍵は、対象とするクラスの敵対者からの暗号鍵に関する全数検索を計算量的に実行不可能にする程度の十分な強度を備えていなければならない（shall）。

4 セキュリティ対策方針

4.1 TOE のセキュリティ対策方針

表 6: TOE の対策方針

ID	説明
O.Encrypted_Information	TOEは、ストレージ・メモリ内のSA.User_Data及びSA.Keysがこの PPに従って暗号化されていることを保証する。TOEは、SA.User_Data、SA.Keys及びSA.User_Secretが永続性メモリ内に平文で保管されていないことを保証する。永続性メモリに保管されている情報からはSA.KeysもSA.User_Secretも再構築することはできない（shall）。
O.Authentication	TOEは、利用者認証が適切に実行されるまで、SA.User_Dataが平文で利用不可であることを保証する。
O.Key_Derivation	TOEは、あらゆる可能な入力空間に対して行われる全数検索を計算量的に実行不可能にするに程度の複雑さをKDFが備えていることを保証する。 もし使用されるKDFがソルトを必要とする場合には、対象とする敵対者クラスが予測できない方法でソルトが生成されなければならない（shall）。
O.Key_Generation	TOEは、DEKの生成には、DEKが完全にランダムであった場合より効果的な暗号解読方法にはならないという特性があることを保証する。
オプションとして、ファームウェア更新が可能な時に、以下が必要である: O.Firmware_Upgrade	ファームウェア更新パッケージは信頼される者によって署名されていなければならず、署名されたパッケージの真正性は、更新パッケージに関してそれが他のアクションを実行する前に、ストレージ・デバイスによって検証されなければならない（shall）。
O.Key_Zeroization	TOEは、TOEの適切な操作にSA.Keysが必要ではなくなった時点でそれがセキュアにゼロ化されていることを保証しなければならない（shall）。 適用上の注意: ゼロ化は、敵対者がゼロ化の済んだデータを再作成できないことを保証しなければならない（shall）。
O.Secret_Zeroization	TOEは、TOEの適切な操作にSA.User_Secretが必要ではなくなった時点でそれがセキュアにゼロ化されていることを保証しなければならない（shall）。 適用上の注意: ゼロ化は、敵対者がゼロ化の済んだデータを再作成できないことを保証しなければならない（shall）。

4.2 環境のセキュリティ対策方針

表 7: 環境の対策方針

ID	説明
OE.Trusted_Users	TOE利用者は、TOEを取り扱う上で信頼されており研修も受けている。TOE利用者は、秘匿性の高い情報にアクセスするための認可も受けている。
OE.Trusted_Host	ホストコンピュータは信頼されている。ホストコンピュータにアクセスできるのは、許可された利用者のみである。
OE.Legitimate_Usage	TOEは、高信頼の環境で信頼を受けている利用者の管理下になければならない（shall）。
OE.Lost_Storage_Device	万一ストレージ・デバイスが紛失又は盗難に遭った後回収され、認可を受けていない者がそのデバイスに調整を加えていることが疑われる場合には、そのデバイスは破棄されなければならない（shall）。
OE.Entropy	ユーザシークレット（SA.User_Secret）は、対象とするクラスの敵対者（adversary）からのユーザシークレットに関する全数検索を計算量的に実行不可能にする程度の十分なエントロピーを備えていなければならない（shall）。
OE.Crypto	暗号鍵は、対象とするクラスの敵対者（adversary）からの暗号鍵に関する全数検索を計算量的に実行不可能にする程度の十分な強度を備えていなければならない（shall）。
オプションとして、ファームウェア更新が可能な時に、以下が必要である: OE.Signing_Key	ファームウェア更新署名鍵は、信頼されている者により扱われ、正規のファームウェア更新パッケージに署名する場合にのみ使用される。信頼されている者が鍵を扱うため、鍵は漏洩や操作から保護される。
オプションとして、初期化用のアプリケーション及び認証用のアプリケーション（又はこのうちのいずれか）がホスト上で実行されている時に、以下が必要である: OE.Application_for_initialization_and_for_authentication	初期化用アプリケーション及び認証用アプリケーション（又はこのうちのいずれか）の真正性は、それがインストール又は更新される前に検証されなければならない（shall）。利用者がアプリケーションの真正性を検証できる手順は確立されなければならない（shall）。

4.3 根拠

4.3.1 脅威 – セキュリティ対策方針

表 8: 脅威 – セキュリティ対策方針

脅威	セキュリティ対策方針
T.Extract_User_Data	O.Encrypted_Information O.Authentication
T.Extract_User_Secret	O.Encrypted_Information O.Secret_Zeroization
T.Extract_Keys	O.Encrypted_Information O.Key_Zeroization
T.Manipulation	OE.Lost_Storage_Device
T.Exhaustive_Search	O.Encrypted_Information O.Key_Derivation O.Key_Generation OE.Entropy OE.Crypto
オプションとして、ファームウェア更新が可能な時に、以下が適用可能である: T.Malicious_Upgrade	オプションとして、ファームウェア更新が可能な時に、以下が適用可能である: O.Firmware_Upgrade

T.Extract_User_Data は、SA.User_Data が平文で永続性メモリに保管されていないことを保証する O.Encrypted_Information により対応され、利用者認証が適切に実行されるまでは SA.User_Data が平文で利用できないことを保証する O.Authentication によりサポートされる。

T.Extract_User_Secret は、SA.User_Secret が平文で永続性メモリに保管されていないことを保証する O.Encrypted_Information により対応され、TOE の適切な操作に必要ではなくなった時点で SA.User_Secret がセキュアにゼロ化されることを保証する O.Secret_Zeroization によりサポートされる。

T.Extract_Keys は、SA.Keys が平文で永続性メモリに保管されていないことを保証する O.Encrypted_Information により対応され、TOE の適切な操作に必要ではなくなった時点で SA.Keys がセキュアにゼロ化されることを保証する

O.Secret_Zeroization によりサポートされる。

T.Manipulation は、ストレージ・デバイスが紛失や盗難に遭った後に回収され、認可を受けていない者が当該デバイスを改ざんしたことが疑われる場合には破棄されなければならない（shall）ことを保証する OE.Lost_Storage_Device によって対応される。

T.Exhaustive_Search は、ストレージ・メモリ内の SA.User_Data データ及び SA.Keys がすべて暗号化されていることを保証する O.Encrypted_Information により対応され、対象とするクラスの敵対者からのユーザシークレットに関する全数検索を計算量的に実行不可能にする程の十分なエントロピーを SA.User_Secret が備えていることを保証する OE.Entropy、対象とするクラスの敵対者からの暗号鍵に関する全数検索を計算量的に実行不可能にする程度の強度が暗号鍵に十分備わっていることを保証する OE.Crypto、あらゆる可能な入力スペースに対して行われる全数検索を計算量的に実行不可能にする程度の複雑さを KDF が備えていることを保証する O.Key_Derivation、及び DEK の生成には、DEK が完全にランダムであった場合より効果的な暗号解読方法にはならないという特性があることを保証する O.Key_Generation によりサポートされる。

オプションとして、ファームウェア更新が可能な時に、以下が適用可能である。

T.Malicious_Upgrade は、更新パッケージに関して他のアクションを実行する前に、署名されたパッケージの真正性がストレージ・デバイスによって検証されることを保証する O.Firmware_Upgrade により対応される。

4.3.2 前提条件 – セキュリティ対策方針

表 9: 前提条件 – セキュリティ対策方針	
前提条件	セキュリティ対策方針
A.Trusted_Users	OE.Trusted_Users
A.Trusted_Host	OE.Trusted_Host
A.Legitimate_Usage	OE.Legitimate_Usage
A.Lost_Storage_Device	OE.Lost_Storage_Device
オプションとして、ファームウェア更新が可能な時に、以下が必要である: A.Signing_Key	オプションとして、ファームウェア更新が可能な時に、以下が必要である: OE.Signing_Key
オプションとして、初期化用のアプリケーション及び認証用のアプリケーション（又はこのうちのいずれか）がホスト上で実行されている時に、以下が適用可能である: A.Application_for_initialization_and_for_ authentication	オプションとして、初期化用のアプリケーション及び認証用のアプリケーション（又はこのうちのいずれか）がホスト上で実行されている時に、以下が必要である: OE.Application_for_initialization_and_for_authentication

A.Trusted_Users は、TOE 利用者が TOE を取り扱う上で信頼されており研修も受けていること、及び秘匿性の高い情報にアクセスする認可も受けていることを保証する OE.Trusted_Users により対応される。

A.Trusted_Host は OE.Trusted_Host によって対応され、これにより、ホストコンピュータが高信頼であること、ホストコンピュータにアクセスできるのは許可された利用者のみであること、及びホストコンピュータの環境が高信頼であることが保証される。

A.Legitimate_Usage は OE.Legitimate_Usage によって対応され、これにより、TOE が、信頼できる環境内で信頼できる利用者の管理下にあることが保証される。

A.Lost_Storage_Device は OE.Lost_Storage_Device によって対応され、これにより、もしストレージ・デバイスが、紛失や盗難に遭った後に回収され、認可を受けていない者が当該デバイスを改ざんしたことが疑われる場合には、破棄されなければならない（shall）ことが保証される。

オプションとして、ファームウェア更新が可能な時に、以下が適用可能である。

A.Signing_Key は、ファームウェア更新署名鍵が信頼されている者によって扱われ、かつ、正規のファームウェア更新パッケージに署名する場合にのみ使用されることを保証する OE.Signing_Key により対応される。信頼されている者が鍵を扱う

ため、鍵は漏洩や操作から保護される。

オプションとして、初期化用のアプリケーション及び認証用のアプリケーション（又はこのうちのいずれか）がホスト上で実行されている時に、以下が適用可能である。

A.Application_for_initialization_and_for_authentication は、インストール又は更新の前に初期化用アプリケーションと認証用アプリケーションの真正性が検証されること、及びアプリケーションの真正性を利用者が検証できる手順が確立されていることを保証する OE.Application_for_initialization_ and_for_authentication により対応される。

4.3.3 組織のセキュリティ方針 – セキュリティ対策方針

表 10: 組織のセキュリティ方針（OSP） – セキュリティ対策方針	
組織のセキュリティ方針（OSP）	セキュリティ対策方針
P.Entropy	OE.Entropy
P.Crypto	OE.Crypto

P.Entropy は、対象とする敵対者クラスからのユーザシークレットに関する全数検索を計算量的に実行不可能にする程度の十分なエントロピーを SA.User_Secret が備えていることを保証する OE.Entropy により対応される。

P.Crypto は、対象とする敵対者クラスからのユーザシークレットに関する全数検索を計算量的に実行不可能にする程度の十分な強度を暗号鍵が備えていることを保証する OE.Entropy により対応される。

4.3.4 セキュリティ対策方針 – 脅威 – 前提条件 – 組織のセキュリティ方針（OSP）

表 11: セキュリティ対策方針 – 脅威 – 前提条件 – 組織のセキュリティ方針（OSP）			
セキュリティ対策方針	脅威	前提条件	組織のセキュリティ方針（OSP）
O.Encrypted_Information	T.Extract_User_Data T.Extract_User_Secret T.Extract_Keys T.Exhaustive_Search	-	-
O.Authentication	T.Extract_User_Data	-	-
O.Key_Derivation	T.Exhaustive_Search	-	-
O.Key_Generation	T.Exhaustive_Search	-	-

O.Key_Zeroization	T.Extract_Keys	-	-
O.Secret_Zeroization	T.Extract_User_Secret	-	-
オプションとして、ファームウェア更新が可能な時に、以下が必要である: O.Firmware_Upgrade	オプションとして、ファームウェア更新が可能な時、以下が適用可能である: T.Malicious_Upgrade	-	-
OE.Trusted_Users	-	A.Trusted_Users	-
OE.Trusted_Host	-	A.Trusted_Host	-
OE.Legitimate_Usage	-	A.Legitimate_Usage	-
OE.Lost_Storage_Device	T.Manipulation	A.Lost_Storage_Device	-
OE.Entropy	T.Exhaustive_Search	-	P.Entropy
OE.Crypto	T.Exhaustive_Search	-	P.Crypto
オプションとして、ファームウェア更新が可能な時に、以下が必要である: OE.Signing_Key	-	オプションとして、ファームウェア更新が可能な時に、以下が必要である: A.Signing_Key	-
オプションとして、初期化用のアプリケーション及び認証用のアプリケーション（又はこのうちのいずれか）がホスト上で実行されている時に、以下が必要である: OE.Application_for_initiali-zation_ and_for_authentica-tion	-	オプションとして、初期化用のアプリケーション及び認証用のアプリケーションがホスト上で実行されている時に、以下が必要である: A.Application_for_initiali-zation_and_for_authenti-cation	-

5　拡張コンポーネント定義

5.1　FCS_RNG 乱数の生成

FCS_RNG.1 乱数の生成には、乱数生成器が定義済みのセキュリティ機能を実装していること、及びその乱数が定義済みの品質基準に適合していることが必要である。

5.1.1　ファミリのふるまい

このファミリは、暗号目的で使用されることを意図した乱数の生成に関する品質要件を定義する。

5.1.2　コンポーネントのレベル付け

FCS_RNG.1 は FCS_RNG ファミリ内の他のコンポーネントとの階層関係はない。

5.1.3　管理

想定される管理アクティビティはない。

5.1.4　監査

監査対象として定義されたアクションはない。

5.1.5　FCS_RNG.1 乱数生成

下位階層:　なし。

依存性:　なし。

FCS_RNG.1.1　TSF は［割付: セキュリティ機能のリスト］を実装する［選択: 物理的、非物理的真性、決定論的、物理的ハイブリッド、決定論的ハイブリッド］乱数生成器を提供しなければならない（shall）。

FCS_RNG.1.2　TSF は［割付: 定義済みの品質基準］に適合する乱数を提供しなければならない（shall）。

5.1.6　根拠

乱数生成器の品質は、この SFR を使用して定義される。

6 IT セキュリティ要件

6.1 情報フロー制御方針

6.1.1 利用者データ アクセス制御 SFP

サブジェクト:ホスト

オブジェクト: SA.User_Data

属性:暗号化又は復号されたと認められるデータ

適用すべき規則:ストレージ・デバイス上の SA.User_Data がアクセス可能になるのは復号完了後のみでなければならない(shall)。

6.1.2 ユーザシークレット・アクセス制御 SFP

6.1.2.1 TOE アーキテクチャ タイプ A

サブジェクト:ホスト

オブジェクト: SA.User_Secret

属性:SA.User_Secret と認められるデータ

適用すべき規則:ストレージ上の SA.User_Secret はホストからアクセス不可でなければならない(shall)。

6.1.2.2 TOE アーキテクチャ タイプ B

サブジェクト:ホスト、又はホスト上の初期化用アプリケーション及び認証用アプリケーション

オブジェクト: SA.User_Secret

属性:SA.User_Secret と認められるデータ

適用すべき規則:ストレージ・デバイス上の SA.User_Secret は、ホスト又は初期化用アプリケーション及び認証用アプリケーションにアクセス不可でなければならない(shall)。

6.2 セキュリティ機能要件

6.2.1 暗号化のサポート

6.2.1.1 FCS_CKM.1_DEK 暗号鍵生成

FCS_CKM.1.1 TSF は、次の［割付: *規格のリスト*］に適合する、規定の暗号鍵生成アルゴリズム［割付: 暗号鍵生成アルゴリズム］及び規定の暗号鍵サイズ［割付: *暗号鍵サイズ*］に従って、暗号鍵を生成しなければならない(shall)。

適用上の注意: TSF は、TOE 内の暗号モジュールに実装された RNG を使用して、DEK を生成しなければならない(shall)。生成された DEK には、対象とする敵対者クラスが、可能性のあるすべての鍵に対して仕掛ける全数検索を計

算量的に実行不可能にする程度の十分なエントロピーが格納されていなければならない（must）。

適用上の注意：ストレージ・デバイスで使用されるあらゆる暗号アルゴリズムと暗号スキームは、当該デバイスが使用されることになる国内の関係国家当局による承認を受けなければならない（shall）。

6.2.1.2 FCS_CKM.1_KEK 暗号鍵生成

FCS_CKM.1.1 TSF は、次の［割付: *規格のリスト*］に適合する、規定の暗号鍵生成アルゴリズム［割付: *暗号鍵生成アルゴリズム*］及び規定の暗号鍵サイズ［割付: *暗号鍵サイズ*］に従って、暗号鍵を生成しなければならない（shall）。

適用上の注意：TSF は、TOE 内に実装された鍵導出関数（KDF）を使用して鍵暗号鍵（KEK）を導出しなければならない（shall）。

適用上の注意：ストレージ・デバイスで使用されるあらゆる暗号アルゴリズムと暗号スキームは、当該デバイスが使用されることになる国内の関係国家当局による承認を受けなければならない（shall）。

6.2.1.3 FCS_RNG.1 乱数生成

FCS_RNG.1.1 TSF は［割付: *セキュリティ機能のリスト*］を実装する［選択: 物理的、非物理的真性、決定論的、物理的ハイブリッド、決定論的ハイブリッド］乱数生成器を提供しなければならない（shall）。

FCS_RNG.1.2 TSF は［割付: *定義済みの品質基準*］に適合する乱数を提供しなければならない（shall）。

6.2.1.4 FCS_CKM.4 暗号鍵破棄

FCS_CKM.4.1 TSFは、次の［割付: *規格のリスト*］に適合する規定の暗号鍵破棄方法の**ゼロ化**に従って、暗号鍵を破棄しなければならない（shall）。

適用上の注意：SA.Keys は、TOE の適切な操作に必要ではなくなった時点でセキュアにゼロ化されなければならない（shall）。

適用上の注意：ストレージ・デバイスが再初期化されるとすぐに、暗号化された鍵はすべてゼロ化され、初期化手順が繰り返し実行されなければならない（shall）。

適用上の注意：ストレージ・デバイスで使用されるあらゆる暗号アルゴリズムと暗号スキームは、当該デバイスが使用されることになる国内の関係国家当局による承認を受けなければならない（shall）。

6.2.1.5 FCS_COP.1_Data 暗号操作

FCS_COP.1.1 TSF は、次の［割付: *規格のリスト*］に適合する規定の暗号アルゴリズム［割付: *暗号アルゴリズム*］及び暗号鍵サイズ［割付: *暗号鍵サイズ*］に従って、**秘匿性の高いデータの暗号化と復号**を実行しなければならない（shall）。

適用上の注意：TSFは、ストレージ・デバイスの永続性メモリに保管すべき SA.User_Data の暗号化を実行し、利用者が認証された時点では SA.User_Data の復号を実行しなければならない（shall）。

適用上の注意：ストレージ・デバイスで使用されるあらゆる暗号アルゴリズムと暗号スキームは、当該デバイスが使用されることになる国内の関係国家当局による承認を受けなければならない（shall）。

6.2.1.6 FCS_COP.1_Key 暗号操作

FCS_COP.1.1 TSF は、次の［割付: *規格のリスト*］に適合する規定の暗号アルゴリズム［割付: *暗号アルゴリズム*］及び暗号鍵サイズ［割付: *暗号鍵サイズ*］に従って、**鍵の暗号化と復号**を実行しなければならない（shall）。

適用上の注意：KEK は、DEK の暗号化及び復号のために使用される。

適用上の注意：ストレージ・デバイスで使用されるあらゆる暗号アルゴリズムと暗号スキームは、当該デバイスが使用されることになる国内の関係国家当局による承認を受けなければならない（shall）。

6.2.1.7 FCS_COP.1_Signature_Verification 暗号操作

オプションとして、ファームウェア更新が可能な時に、以下が適用可能である。

FCS_COP.1.1 TSF は、次の［割付: *規格のリスト*］に適合する規定の暗号アルゴリズム［割付: *暗号アルゴリズム*］及び暗号鍵サイズ［割付: *暗号鍵サイズ*］に従って、**ファームウェア更新パッケージの署名の検証**を実行しなければならない（shall）。

適用上の注意：ストレージ・デバイスで使用されるあらゆる暗号アルゴリズムと暗号スキームは、当該デバイスが使用されることになる国内の関係国家当局による承認を受けなければならない（shall）。

6.2.2 利用者データ保護

6.2.2.1 FDP_ETC.1 セキュリティ属性を持たない利用者データのエクスポート

FDP_ETC.1.1 TSF は、TOE の外部にあり、1 つ以上の SFP の下で制御を受けている利用者データをエクスポートするときには**利用者データ・アクセス制御 SFP** を実施しなければならない（shall）。

FDP_ETC.1.2 TSF は、その利用者データに関連するセキュリティ属性なしで利用者データをエクスポートしなければならない（shall）。

6.2.2.2 FDP_ACC.1_User_Data サブジェクト・アクセス制御

FDP_ACC.1.1 TSF は、**ホスト上の利用者データ・アクセス制御 SFP** から、**ストレージ・デバイス上の SA.User_Data へのアクセス**を実施して、**ホストが SA.User_Data にアクセスできるのはその復号が済んだ後のみであることを確認**しなければならない（shall）。

6.2.2.3 FDP_ACC.1_User_Secret サブジェクト・アクセス制御

FDP_ACC.1.1 TSF は、**ホスト上のユーザシークレット・アクセス制御 SFP からストレージ・デバイス上の SA.User_Secret へのアクセスを実施して、SA.User_Secret がホストによりアクセス不可であること、又はホスト上の初期化用アプリケーション及び認証用アプリケーションによりアクセス不可であることを確認**しなければならない（shall）。

適用上の注意： TSF は、TOE の SA.User_Secret がホストからはアクセス不可であること（TOE アーキテクチャのタイプ A）を保証するか、初期化用アプリケーションと認証用アプリケーションに対してアクセス不可であることを（TOE アーキテクチャのタイプ B）保証しなければならない（shall）。

6.2.2.4 FDP_ACF.1_User_Data セキュアな属性ベースのアクセス制御

FDP_ACF.1.1 TSF は、次の内容に基づき、オブジェクトに対して**利用者データ・アクセス制御 SFP** を実施しなければならない（shall）：**サブジェクト：ホスト、オブジェクト：SA.User_Data、セキュリティ属性：暗号化又は復号されたと認められるデータ。**

FDP_ACF.1.2 TSF は、制御されたサブジェクト及び制御されたオブジェクト間の操作が許可されるかどうか決定するために、次の規則を実施しなければならない（shall）：**SA.User_Data に対するホスト・アクセスは、復号されたと認められるデータに対してのみ許可される。**

FDP_ACF.1.3 TSF は、次の追加規則に基づいて、サブジェクトからオブジェクトへのアクセスを明示的に認可しなければならない（shall）：**追加規則はなし。**

FDP_ACF.1.4 TSF は、次の追加規則に基づいて、サブジェクトからオブジェクトへのアクセスを明示的に却下しなければならない（shall）：**追加規則はなし。**

適用上の注意： 復号された情報とは、TOE によって復号が完了した情報である。この情報は TOE 外部の他の手段によって暗号化されたと推測されるが、TOE の立場から見れば、これは TOE によって復号が完了した時点で復号されたものとみなされる。

6.2.2.5 FDP_ACF.1_User_Data セキュリティ属性ベースのアクセス制御

FDP_ACF.1.1 TSF は、次の内容に基づいて、オブジェクトへの**ユーザシークレット・アクセス制御 SFP** を保証しなければならない(SFP)：**サブジェクト: ホスト、オブジェクト: SA.User_Secret、セキュリティ属性: SA.User_Secret と認められるデータ。**

FDP_ACF.1.2 TSF は、制御されたサブジェクト及び制御されたオブジェクト間の操作が許可されているかどうか決定するために、次の規則を実施しなければならない(shall)：**SA.User_Secret へのホスト・アクセスは、SA.User_Secret と認められるデータについては許可されることはない。**

FDP_ACF.1.3 TSF は、次の追加規則に基づいて、サブジェクトからオブジェクトへのアクセスを明示的に認可しなければならない(shall)：**追加規則はなし。**

FDP_ACF.1.4 TSF は、次の追加規則に基づいて、サブジェクトからオブジェクトへのアクセスを明示的に却下しなければならない(shall)：**追加規則はなし。**

適用上の注意： FDP_ACF.1.2 のホスト・アクセスには、ホストからのアクセス(TOE アーキテクチャのタイプ A)と、初期化用アプリケーション及び認証用アプリケーション(TOE アーキテクチャのタイプ B)が含まれることに留意されたい。TOE アーキテクチャのタイプ B では初期化用アプリケーションと認証用アプリケーションはいずれもホスト上に置かれているため、両者はいずれもホスト・アクセスとみなされる。SA.User_Secret が TOE に一時的にのみ存在することにも留意されたい。FDP_RIP.1 は、SA.User_Secret が TOE 内で必要ではなくなった時点でゼロ化されることを保証する。

6.2.2.6 FDP_RIP.1 サブセット残存情報保護

FDP_RIP.1.1 TSF は、次に示すオブジェクト **SA.User_Secret から資源の割当を解除**した時に、その資源の以前の情報内容がいずれも利用可能な状態にされていることを保証しなければならない(shall)。

適用上の注意： TSF は、TSF の適切な操作に SA.User_Secret が必要ではなくなった時点でそれがセキュアにゼロ化されていることを保証しなければならない(shall)。ゼロ化は、敵対者がゼロ化の済んだデータを再作成できないことを保証しなければならない(shall)。

6.2.3 識別情報及び認証

6.2.3.1 FIA_UAU.2 アクション前の利用者認証

FIA_UAU.2.1 TSF は、各利用者を代行する他の TSF 介在アクション(TSF-mediated action)を許可する前に、適切に認証されることを当該利用者に要求しなければならない(shall)。

適用上の注意： 認証中、利用者には SA.User_Secret を提供することが要求されなければならない(shall)。

6.2.4 セキュリティ管理

6.2.4.1 FMT_SMF.1 管理機能の仕様

FMT_SMF.1.1 TSF は、次の管理機能を実行できなければならない（shall）：**利用者は SA.User_Secret を選択する、利用者はもう一度初期化を実行する。**

適用上の注意： TOE 利用者は 1 人のみである。

6.3 機能コンポーネント間の依存性

表 12：機能コンポーネント間の依存性

セキュリティ機能コンポーネント	依存性	注記
FCS_CKM.1_DEK	FCS_CKM.2又はFCS_COP.1	あり FCS_COP.1_Key FCS_COP.1_Data
	FCS_CKM.4	あり
FCS_CKM.1_KEK	FCS_CKM.2又はFCS_COP.1	あり FCS_COP.1_Key
	FCS_CKM.4	あり
FCS_RNG.1	なし	-
FCS_CKM.4	FDP_ITC.1又はFDP_ITC.2、あるいはFCS_CKM.1	あり FCS_CKM.1_DEK FCS_CKM.1_KEK
FCS_COP.1_Data	FDP_ITC.1又はFDP_ITC.2、あるいはFCS_CKM.1	あり FCS_CKM.1_DEK
	FCS_CKM.4	あり
FCS_COP.1_Key	FDP_ITC.1又はFDP_ITC.2、あるいはFCS_CKM.1	あり FCS_CKM.1_DEK FCS_CKM.1_KEK
	FCS_CKM.4	あり
オプションとして、ファームウェア更新が可能な時に、以下が必要である： FCS_COP.1_Signature_Verification	FDP_ITC.1又はFDP_ITC.2、あるいはFCS_CKM.1及び FCS_CKM.4	なし 署名の検証に使用される公開鍵は、稼働中のストレージ・デバイスで生成・保管されるため、FDP_ITC.1又

		はFDP_ITC.2は適用不可である。 TOEは署名検証用の鍵を生成しないため、FCS_CKM.1は適用不可である。 署名認証に使用される鍵は公開であるため、FCS_CKM.4は適用不可である。
FDP_ETC.1	FDP_ACC.1又はFDP_IFC.1	あり FDP_ACC.1_User_Data
FDP_ACC.1_User_Data	FDP_ACF.1	あり FDP_ACF.1_User_Data
FDP_ACC.1_User_Secret	FDP_ACF.1	あり FDP_ACF.1_User_Secret
FDP_ACF.1_User_Data	FDP_ACC.1及びFMT_MSA.3	FDP_ACC.1_User_Dataではあり。FMT_MSA.3に対してはなし。 FMT_MSA.3は、属性を初期化することも管理することもできないため適用不可である。
FDP_ACF.1_User_Secret	FDP_ACC.1及びFMT_MSA.3	FDP_ACC.1_User_Secretではあり。FMT_MSA.3に対してはなし。 FMT_MSA.3は、属性を初期化することも管理することもできないため適用不可である。
FDP_RIP.1	なし	-
FIA_UAU.2	FIA_UID.1	なし FIA_UID.1は適用不可である。TOEの一人の利用者であることだけがサポートされているため、識別は必要なく、認証だけが必要である。
FMT_SMF.1	なし	-

6.4 セキュリティ保証要件

TOE の評価、その開発及び操作環境に関する保証要件は、ATE_COV.2 を追加した事前定義済みの保証パッケージ EAL2 である。

EAL2 パッケージの保証要件にはすでに 2 点の改良が加えられている。ADV_TDS.1 及び AVA_VAN.2 がこれに当たる。

この改良は、EAL2 パッケージの元の SAR を作成し直すこと行われており、改良部分は目立つように太字で記載されている。

6.4.1 ADV_TDS.1 の詳細化

開発者アクションエレメント:

ADV_TDS.1.1D	開発者は、TOEの設計を提供しなければならない（shalll）。
ADV_TDS.1.2D	開発者は、機能仕様のTSFIから、TOEの設計で利用可能な最下位の分解（decomposition）へのマッピングを提供しなければならない（shall）。
ADV_TDS.1.3D	**開発者は、FCS SFRを実装するTSFの実装表現の各部分を利用できるようにしなければならない（shall）。**
ADV_TDS.1.4D	**開発者はTOE設計記述とFCS SFRを実装するTSFの実装表現の各部分との間のマッピングを提供しなければならない（shall）。**

内容及びプレゼンテーションエレメント:

ADV_TDS.1.1C	設計は、サブシステムの観点からTOEの構造を記述しなければならない（shall）。
ADV_TDS.1.2C	設計は、TSFのサブシステムをすべて識別しなければならない（shall）。
ADV_TDS.1.3C	設計は、非SFR実施であることを決定するために、TSFの各SFR支援又はSFR非干渉サブシステムのふるまいを十分詳細に記述しなければならない（shall）。
ADV_TDS.1.4C	設計は、SFR実施サブシステムのSFR実施のふるまいを要約しなければならない（shall）。
ADV_TDS.1.5C	設計は、TSFのSFR実施サブシステム間の内部動作、及びTSFのSFR実施サブシステムとそれ以外のTSFのサブシステム相互の内部動作の説明を提供しなければならない（shall）。
ADV_TDS.1.6C	マッピングは、すべてのTSFIが、自らが呼び出すTOE設計内で説明されているふるまいを追跡することを実証しなければならない（shall）。

ADV_TDS.1.7C	**設計は、クラスFCSのSFRを実施しているTSFのサブシステムからTSFの複数のモジュールへのマッピングを提供しなければならない（shall）。**
ADV_TDS.1.8C	**設計は、クラスFCSの各SFR実施モジュールを、その目的及び他のモジュールとの関係の観点から説明しなければならない（shall）。**
ADV_TDS.1.9C	**設計は、SFR関連インタフェース、インタフェースからの戻り値、他のモジュールとの内部動作、及び他のSFR実施モジュールに対してコールされたSFR関連インタフェースの観点からクラスFCSの各SFR実施モジュールを説明しなければならない（shall）。**
ADV_TDS.1.10C	**実装表現は、設計の決定をさらに行わなくてもTSFを生成できるほど詳細にTSFを定義しなければならない（shall）。**
ADV_TDS.1.11C	**実装表現は、開発要員が使用する形式になっていなければならない（shall）。**
ADV_TDS.1.12C	**TOE設計記述と実装表現のサンプルとの間のマッピングは、FCS SFRを実装するTSFの実装表現の各部分の対応を実証しなければならない（shall）。**

評価者アクションエレメント：

ADV_TDS.1.1E	評価者は、提供された情報が証拠の内容と記述に関する要件をすべて満たしていることを確認しなければならない（shall）。
ADV_TDS.1.2E	評価者は、その設計がセキュリティ機能要件を正確かつ完全にインスタンス化したものであると判定しなければならない（shall）。
ADV_TDS.1.3E	**評価者は、選択された実装表現の部分に関して、提供された情報が証拠の内容と記述に関する要件をすべて満たしていることを確認しなければならない（shall）。**

6.4.2 AVA_VAN.2 の詳細化

開発者アクションエレメント：

AVA_VAN.2.1D	開発者は、テスト用のTOEを提供しなければならない（shalll）。

内容及びプレゼンテーションエレメント：

AVA_VAN.2.1C	TOEはテストに適していなければならない（shall）。

評価者アクションエレメント:

AVA_VAN.2.1E	評価者は、提供された情報が証拠の内容と記述に関する要件をすべて満たしていることを確認しなければならない（shall）。
AVA_VAN.2.2E	評価者は、TOEの潜在的な脆弱性を識別するためにパブリック・ドメイン・ソースの検索を実行しなければならない（shall）。
AVA_VAN.2.3E	評価者は、ガイダンス文書、機能仕様、TOE設計、**実装表現**、及びTOE内に潜む脆弱性を識別するためのセキュリティ・アーキテクチャに関する記述を使用して、TOEの独立脆弱性分析を実施しなければならない（shall）。
AVA_VAN.2.4E	評価者は、そのTOEが基本的な攻撃能力を持つと思われる攻撃者によって実行される攻撃に対して耐性があると判定するために、すでに識別されている潜在的な脆弱性に基づいて、侵入テストを実施しなければならない（shall）。
AVA_VAN.2.5E	**評価者は、ホストとのTOEインタフェースのファジー・テストを実施しなければならない（shall）。そして、このファジー・テストがそのインタフェース上で見えている暗号プリミティブをすべて網羅していること。**

6.5 保証コンポーネント間の依存性

保証パッケージ EAL2 に含まれている依存性はいずれも解決済みであるため、この表では実施された要件追加からの依存性のみが識別されている。

表 13: 保証コンポーネント間の依存性		
セキュリティ保証コンポーネント	依存性	注記
ATE_COV.2	ADV_FSP.2	Yes (EAL2の一部として)
	ATE_FUN.1	Yes (EAL2の一部として)

6.6 セキュリティ要件根拠

6.6.1 セキュリティ機能要件根拠

表 14: セキュリティ機能要件（SFR）の根拠	
セキュリティ対策方針	セキュリティ機能要件（SFR）
O.Encrypted_Information	FCS_COP.1_Data FCS_COP.1_Key

	FCS_CKM.1_KEK FIA_UAU.2 FDP_ACC.1_User_Secret FDP_ACC.1_User_Data FDP_ACF.1_User_Secret FDP_ACF.1_User_Data FDP_ETC.1
O.Authentication	FIA_UAU.2 FCS_CKM.1_KEK FCS_COP.1_Key FCS_COP.1_Data FMT_SMF.1
O.Key_Derivation	FCS_CKM.1_KEK
O.Key_Generation	FCS_CKM.1_DEK FCS_RNG.1
オプションとして、ファームウェア更新が可能な時に、以下が必要である： O.Firmware_Upgrade	FCS_COP.1_Signature_Verification (オプション)
O.Key_Zeroization	FCS_CKM.4
O.Secret_Zeroization	FDP_RIP.1

O.Encrypted_Information は以下により保証される：
FCS_COP.1_Data は、SA.User_Data の暗号化を保証し、FCS_COP.1_Key は DEK が KEK で暗号化され TOE に保管されることを保証する。KEK は TOE には保管されない。KEK は TOE 利用者認証 FIA_UAU.2 中に毎回 FCS_CKM.1_KEK で生成される。

FDP_ACC.1_User_Secret は、SA.User_Secret 転送のための規則を定義する。これは、FDP_ACF.1_User_Secret とともに、SA.User_Secret がホスト（TOE アーキテクチャのタイプ A）からアクセス不可であること、又は初期化用アプリケーションと認証用アプリケーションを含むホスト（TOE アーキテクチャのタイプ B）からアクセス不可であることを保証する。

FDP_ACC.1_User_Data は、SA.User_Data の規則が TOE からアクセス不可であることを定義する。復号された SA.User_Data のみがホストに対してアクセス可能であることを保証する FDP_ACF.1_User_Data とともに、FDP_ETC.1 は、TOE から SA.User_Data をエクスポートできることを保証する。

O.Authentication は以下により保証される：
FIA_UAU.2 は、TSF 介在アクション前に TOE 利用者が認証されることを保証する。利用者は SA.User_Secret を提供するよう要求される。次に、FCS_CKM.1_KEK に定義されているように KEK を生成するために、SA.User_Secret が KDF への入力として使用される。そして、FCS_COP.1_Key に規定されているように DEK を復号するために、生成された KEK が使用される。DEK が適切に復号された後、TOE に保管された SA.User_Data は、FCS_COP.1_Data に規定されているように復号することができる（may）。TOE 利用者は、FMT_SMF.1 に定義されているように初期化の時点で SA.User_Secret を選択する。

O.Key_Derivation は以下により保証される：
FCS_CKM.1_KEK は、あらゆる可能な入力スペースに対して行われる全数検索を計算量的に実行不可能にする程の複雑さを KDF が備えていることを保証する。

O.Key_Generation は以下により保証される：
DEK は、FCS_RNG.1 に定義された乱数生成器（RNG）により、FCS_CKM.1_DEK に定義されたとおりに生成される。

O.Firmware_Upgrade（オプション）は以下により保証される：
FCS_COP.1_Signature_Verification は、署名の検証が更新パッケージに関して実行されることを保証する。これは、ファームウェア更新が可能な時に必要である。

O.Key_Zeroization は以下により保証される：
FCS_CKM.4 は、TOE の適切な操作に SA.Keys が不要になった時点で、それがセキュアにゼロ化されていることを保証する。

O.Secret_Zeroization は以下により保証される：
FDP_RIP.1 は、TOE の適切な操作に SA.User_Secret が不要になった時点で、それがセキュアにゼロ化されていることを保証する。

6.6.2 セキュリティ保証要件根拠

保証パッケージ EAL2 には ATE_COV.2 が追加されている。EAL2 は、完全な開発記録を入手することが難しい場合に、開発者又は利用者が自主的に保証された低レベルから中レベルのセキュリティを要求する環境で適用することが可能である。ATE_COV.2 の追加は、TSFI 全体を完全にテストで網羅することを保証するために実施されたものである。

暗号機能の脆弱性分析の必要性に対処するために、ADV_TDS.1 には改良が加えられ、設計情報の追加情報及び暗号機能の実装表現が収録された。この情報は AVA_VAN.2 を実行する時に使用されることになる。また、MSB で必要とされる固有のテストを規定するために AVA_VAN.2 にも改良が加えられた。