



Central department of security and information systems

TOE design

Date of Creation	: October 22, 2007
Project name	: TRUECRYPT
Reference	: SPM030-TDS
Version	: 2.00
Classification	: public
Status	: Issued
Number of Pages	: 37 (including 2 headers)
Comments	: None

序文

特に教育の現場での、本書の複製、および/または二次利用は、次の3つの条件を満たすことによって、国防総局情報セキュリティ中央局(SGDN/DCSSI)によって許可されている。

- 本書の配布を無償とすること。

- 本書を複製する場合には、完全性に注意を払うこと(原書に忠実であること); 修正、改ざんは認めない。

- 本書の複製版には、例えば「本書は、国防総局情報セキュリティ中央局(SGDN/DCSSI) (<http://www.ssi.gouv.fr/en>)によって策定されたものである。」など、出自を明らかにする文言を含めること。

目次

1.	序章	6
1.1.	コモン・クライテリア	6
1.2.	参照文書	6
2.	TSF のサブシステム	7
3.	サブシステム間の相互作用	11
4.	TSF モジュール	13
4.1.	サマリ	13
4.2.	TSF モジュールの説明	18
5.	TSFI とサブシステム間の対応	28
6.	TOE 設計に含まれる SFR	29
付録 A.	略語と頭字語	31
6.1.	略語と頭字語	31
付録 B.	参照文献	32
付録 C.	コモン・クライテリアに関する情報	33
C.1.	本書の目的	33
C.2.	ADV_TDS.3 コンポーネントの目的	34
C.3.	メソドロジ	34




図 1. - TrueCrypt のサブシステム構成..... 9

図 2. - モジュール表示..... 17

用語

CC:	コモン・クライテリア
CEM:	情報技術セキュリティ評価のための共通方法
SFR:	セキュリティ機能要件
SFR 実施:	最低でも 1 つの SFR のエレメントを実装するメカニズムを提供するか、SFR を実装するエレメントを直接サポートする。
SFR 支援:	SFR 実施のエレメントによるが、SFR を実装してはいるが、直接的な役割を果たしていない。
SFR 非干渉:	SFR を実装していない。
TOE:	評価対象 評価対象とは、評価の対象となる製品、またはシステムの部分を指す。
TSF:	TOE セキュリティ機能
TSFI:	TSF インタフェース

TOE design	
TRUECRYPTO-SPM030-TDS	

1. 序章

本書では、TrueCrypt 暗号化ソフトウェアの設計について説明する。

本書には、コモン・クライテリアの ADV_TDS.3 コンポーネントの要件に対応することができる情報が含まれている。

1.1. コモン・クライテリア

TOE の設計の説明では、TSF のコンテキストの説明、および TSF の完全な説明の双方を提供する。(セキュリティ)保証のニーズが高まるにつれ、説明に提供されるレベルも詳細になってきている。

基本的なモジュール設計(ADV_TDS.3)により、まず TSF を1つ複数の「サブシステム」として表現し、必要に応じてそれぞれのサブシステムは「モジュール」にブレイクダウンされる。

1.2. 参照文献

本書は、次の文書に基づき、記述されている。

- セキュリティ・ターゲット[ST]
- TOE 機能仕様[ADV_FSP]、および
- TrueCrypt の暗号化仕様[SPEC_CRYPTO]。

2. TSF のサブシステム

TSF は、次のような 10 のサブシステムに分類することができる。

番号	サブシステムの名称	SFR 実施
		<i>SFR 支援</i> SFR 非干渉
説明		

1	アプリケーション管理	SFR 実施
<p>このサブシステムでは、TrueCrypt の開始、設定、キャッシュ化されたパスワードのクリア、テスト・ツール、および TrueCrypt の終了が行われる。</p> <p>設定は、TrueCrypt のメイン・メニューの「Parameters」タブに対応している。この機能によってユーザは、言語、デフォルトのマウンティングオプション、Windows が開始された際に実行される動作などの設定を変更できる。</p> <p>テスト・ツール: 暗号化 - 復号結果が既知であるデータや鍵に基づくアルゴリズム・テスト、暗号化 - 復号操作のランダム検証、など。</p>		

2	ヘッダの処理	SFR 実施
<p>このサブシステムは、ヘッダに関する全ての操作を実施する: 暗号化ディスク作成時のディスク・ヘッダの作成、ディスクマウント時のディスク・ヘッダの読み出し、ヘッダのバックアップやリストアである。また、認証手法が変更された場合のヘッダの読み書きも実施する(旧パスワード / 鍵ファイル・ペアの読み出し検証し、変更された認証手法に応じた新ヘッダを書き込む)。</p>		

3	ディスク・フォーマット	SFR 実施
<p>このサブシステムは、暗号化ディスク作成時に使用される。ヘッダを作成し(ディスクの最初の 512 バイトに)書き込まれると、TrueCrypt は「TrueCrypt Format.exe」実行ファイルにより実施されるディスクのフォーマットを開始する。このフォーマットは、ファイル・システムごとに異なる(FAT、または NTFS)。</p>		

4	マウンティング管理	SFR 非干渉
<p>このサブシステムは、ユーザの暗号化ディスクを利用・アクセス可能にするマウントを実施する。マウントされるには、事前にヘッダ処理サブシステム(サブシステム 2 参照)によりユーザが認証されている必要がある。</p>		

5	暗号化ディスクのリスト管理	SFR 非干渉
<p>このサブシステムは、Windows ログイン中にマウントされた全ボリュームのリストを維持更新する。また、ユーザはマウントされた暗号化ディスクが関連付けられているドライブ、ディスクのサイズ、使用されているアルゴリズムやディスクのタイプ(隠しボリューム、通常ボリューム)などを知ることができる。このリストは、暗号化ディスクがマウント、またはアンマウント時に更新される。</p>		

6	アンマウンティング管理	SFR 実施
<p>このサブシステムは、既にマウントされているディスクをアンマウントする。TrueCrypt では、マウントされているボリュームと暗号化ディスクに対応するドライブとのリンクを削除し、暗号コンテンツを消去する(暗号鍵の消去など)。ユーザは、暗号化ディスクにアクセスすることができなくなる。</p>		

7	データ処理	SFR 実施
<p>このサブシステムは、マウントされている暗号化ディスク上でデータが読まれる場合(または、書き込まれる場合)に、自動復号(または、暗号化)を実行する。この操作はユーザに対して透過的であり、非暗号化ディスクを使用していると変わりはない。</p>		

8	暗号化ディスクの情報の表示	SFR 非干渉
<p>このサブシステムは、暗号化ディスクを使用するユーザにさまざまな情報を提供する:ディスクを暗号化するために使用するアルゴリズム、鍵のサイズ、PKCS-5 での繰り返し回数、など。</p>		

9	暗号化の操作	SFR 実施
<p>これが、TrueCrypt の主要システムである。このサブシステムは、乱数の生成、暗号化、復号、ハッシュ化操作などの暗号化の機能を提供する。</p>		

10	鍵ファイルの生成	SFR 非干渉
<p>このサブシステムは、鍵ファイル(ランダムな 64 バイトのバイナリ・ファイル)を生成する。</p>		

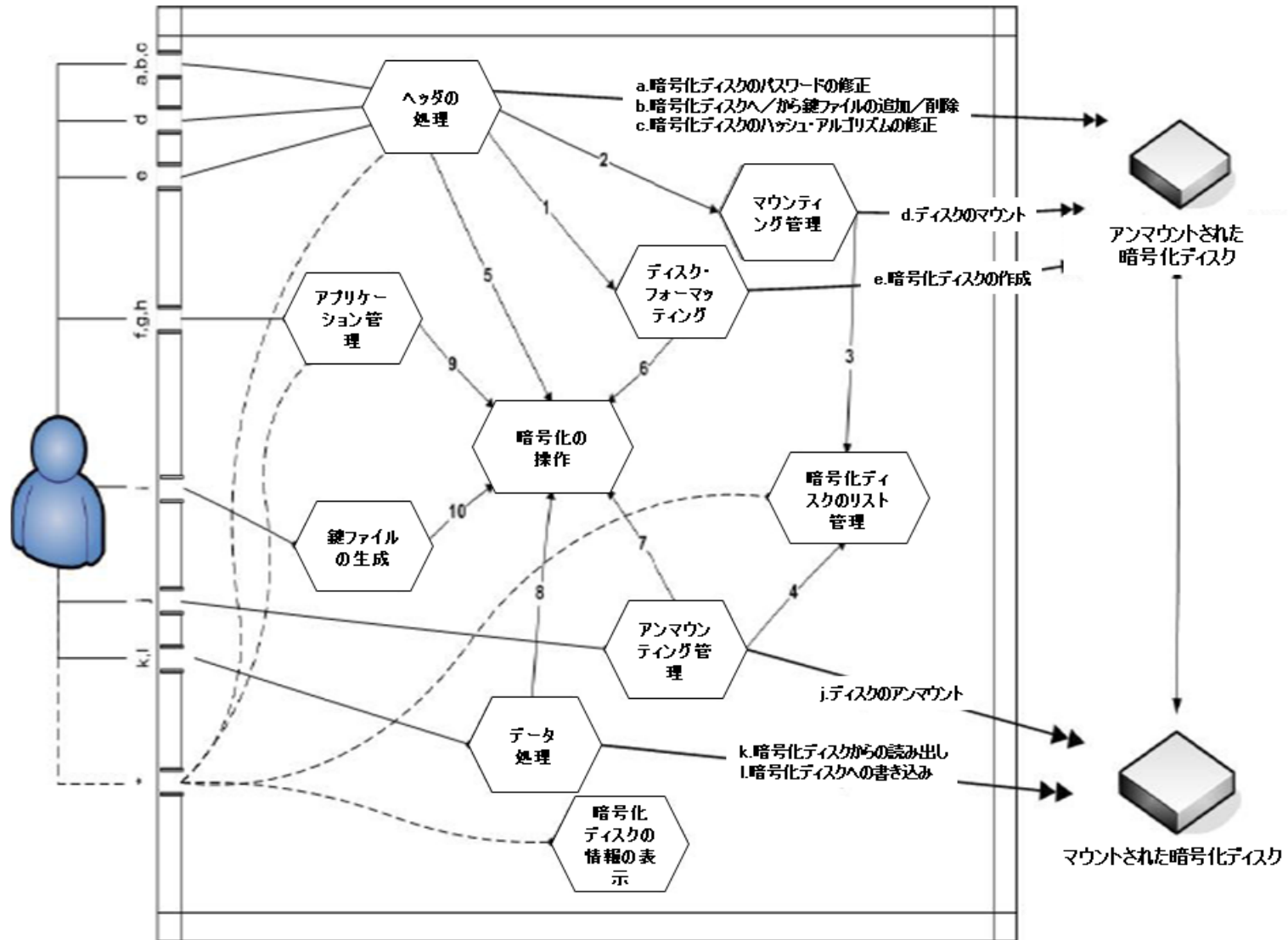








図 1: TrueCrypt のサブシステム構成

図 1 における要点:

 : TSFI a et b	<p>機能仕様ではTSFIは次のように定義されている。</p> <ol style="list-style-type: none"> a. 暗号化ディスクのパスワード修正 b. 暗号化ディスクからの鍵ファイルの追加 / 削除 c. 暗号化ディスクのハッシュ・アルゴリズム修正 d. ディスクのマウント e. 暗号化ディスクの作成 f. TrueCrypt の実行 g. TrueCrypt の終了 h. パスワードのクリア i. 鍵ファイルの生成 j. ディスクのアンマウント k. 暗号化ディスクからの読み出し l. 暗号化ディスクへの書き込み
	<p>TSFIとして見なされない機能仕様に記載されているアクセス・インターフェース:</p> <ul style="list-style-type: none"> - マウントされている暗号化ディスクの情報の表示 - マウントされているディスクに対応するドライブの表示 - TrueCrypt の設定の変更 - TrueCrypt メカニズムのパフォーマンスと適合性テスト - トラベラーディスクの作成 - ヘッダのバックアップ - ヘッダのリストア
	TSFI によるサブシステムの使用
	TSFI とは見なされていないインターフェースによるサブシステムの使用
	サブシステム A の 1 つ以上のモジュールが、サブシステム B の 1 つ以上のモジュールを使用する場合、サブシステム A とサブシステム B との関連。
	(マウント / アンマウントされている)暗号化ディスクに対しサブシステムにより実行される操作。

3 サブシステム間の相互作用

番号 サブシステム A サブシステム B との関連

相互作用の説明

1. ヘッダの処理 **ディスク・フォーマット**

暗号化ディスクの作成プロセスでは、はじめに「ヘッダの処理」サブシステムによって管理されている暗号化ヘッダの生成が要求される。ヘッダの生成には、暗号化ディスクのデータを暗号化・復号するために使用する暗号鍵が含まれる。このヘッダ自体は、パスワードと鍵ファイル・リストから導出された鍵によって暗号化されている。次にこのヘッダが暗号化ディスクの最初のバイトに書き込まれると、このディスクのその他のセクタは、上記で生成された鍵以外のランダムな鍵で暗号化された、ランダムなデータで満たされる(フォーマットは、「TrueCrypt Format.exe」で実行される)。

2. ヘッダの処理 **マウンティング管理**

暗号化ディスクのマウンティングプロセスでは、はじめに「ヘッダの処理」サブシステムによりヘッダを全て復号する必要がある。ヘッダが復号されると、「マウンティング管理」サブシステムがその後を引き継ぎ Windows により指定されたドライブに暗号化ディスクをリンクしアクセスできるようにする。

3. マウンティング管理 **暗号化ディスクのリスト管理**

暗号化ディスクのマウンティングが正常に実行されると、「マウンティング管理」サブシステムが「暗号可ディスクのリスト管理」サブシステムに情報を送信しこのリストが更新される。

4. アンマウンティング管理 **暗号化ディスクのリスト管理**

ディスクのアンマウンティング処理では、ボリュームに指定されたドライブと暗号化ディスクとのリンクを解消し、暗号化コンテンツ(マスタ鍵とマスタ鍵から導出された鍵)を消去する。従って、アンマウンティングするサブシステムは、「暗号化ディスクのリスト管理」サブシステムがリストを更新できるように、このディスクがアクセス不可になったという情報を送信する。

5. ヘッダの処理 **暗号化の操作**

「ヘッダの処理」サブシステムは、(例えばヘッダの暗号化、乱数の生成などの)処理に必要な暗号化の操作を実行するために「暗号化の操作」サブシステムを使用する。

6. ディスク・フォーマット**暗号化の操作**

ディスクのフォーマットは、ランダムな鍵を使用して暗号化された乱数データで満たすことである。これが、「ディスク・フォーマット」サブシステムが「暗号化の操作」サブシステムによって提供される機能を使用しなければならない理由である。

7. アンマウント管理**暗号化の操作**

暗号化ディスクがアンマウントされると、ディスクの暗号化コンテンツを含むメモリは「0」で満たされる。この処理は、セキュアな暗号鍵（マスタ鍵とヘッダ鍵）、および認証データの消去と同じである。従ってアンマウントングに關与するサブシステムは、暗号化の操作を実行するサブシステムを使用する。

8. データ処理**暗号化の操作**

データの読み出し、および書き込みは、ディスクの異なるセクタでの自動復号、または暗号化が要求される。これらの操作は、暗号化サブシステムにより実行される。

9. アプリケーション管理**暗号化の操作**

TrueCrypt のアプリケーションではさまざまなテストを実行することができるため、「アプリケーション管理」サブシステムは、暗号化の操作を管理するサブシステムを使用しなければならない。

10. 鍵ファイルの生成**暗号化の操作**

鍵ファイルの生成では、暗号化の操作を管理するサブシステムより提供される乱数生成モジュールを使用する必要がある。

4. TSF モジュール

4.1. サマリ

以下は、さまざまな TSF モジュールについてまとめた表である。

番号	サブシステムの名称	モジュールの名称	概要	SFR 実施 SFR 支援 SFR 非干渉
1.	アプリケーション管理			
		開始	このモジュールは、TrueCrypt.exe 実行時に起動される。これによって、TrueCrypt.exe の実行ファイルが開始する。	SFR 非干渉
		設定	このモジュールは、TrueCrypt の設定を変更することができる。	SFR 非干渉
		テスト	このモジュールより、アプリケーションの「Tools」メニューからさまざまなタイプのテストを実行することができる。	SFR 非干渉
		終了	このモジュールは、TrueCrypt のアプリケーションを起動する。アプリケーションを終了してもドライバはアンロードされない。このドライバは、TrueCrypt プロセスが開始されなくともマウントされているディスクへの書き込みや読み出しに対応しなければならない。	SFR 実施
2.	ヘッダの処理			
		パスワード処理	ヘッダ鍵を生成する前に、鍵ファイルを使用してユーザ・パスワードを変換することができる。	SFR 実施
		ヘッダ鍵の導出	変換パスワードと 64 バイトのシードから 2 つのヘッダ鍵(主ヘッダ鍵と二次ヘッダ鍵)を導出することができる。これらの鍵は、ボリュームのヘッダ(第一セクタ)を暗号化 / 復号するために使用される。	SFR 実施

n°	サブシステムの名称	モジュールの名称	概要	SFR 実施 SFR 支援 SFR 非干渉
		暗号化ヘッダの作成	ボリュームの暗号化ヘッダを作成することができる。ボリュームのヘッダには、次のような情報が含まれている:暗号とハッシュに使用されるアルゴリズム、マスタ鍵とその二次鍵(LRW モード)	SFR 実施
		暗号化ヘッダの読み出し	ボリュームの暗号化されたヘッダを読み出すことができる。ボリュームのヘッダには、次のような情報が含まれている:暗号とハッシュに使用されるアルゴリズム、マスタ鍵とその二次鍵(LRW モード)	SFR 実施
3. ディスク・フォーマット				
		フォーマット	ボリューム作成を可能にする。このモジュールは、最初に暗号化されたヘッダを作成する機能を使用し、次にユーザが選択したファイル・システムに基づいてボリュームをフォーマットする。	SFR 実施
4. マウント管理				
		リンクの作成	TrueCrypt は、Windows に対し、マウントされている暗号化ディスクが動作するドライブを割り当てるように要求する。このリンクが作成された時点で、ディスクにアクセスできるようになる。	SFR 非干渉
5. 暗号化されたディスクのリストの管理				
		リストの更新	TrueCrypt ドライバに、暗号化ディスクをリストに追加、または削除するよう要求する。	SFR 非干渉

n°	サブシステムの名称	モジュールの名称	概要	SFR 実施 SFR 支援 SFR 非干渉
6.	アンマウンティング管理			
		リンクの解消	TrueCryptは Windows に、暗号化ディスクがマウントされたときに確立されたリンクを解消するよう要求する。このリンクが解消されると、ディスクにアクセスすることができなくなる。	SFR 実施
		暗号化コンテンツの削除	マスタ鍵とマスタ鍵から導出されたパトリール鍵(訳注:管理鍵 = control key のことと思われる)の削除	SFR 実施
7.	データ処理			
		データの読み出し	この機能は、ボリューム上の暗号化されたデータを読み出すことができる。オペレーティング・システムは、この暗号化ボリュームに対応する「デバイス」に(データの)読み出しを要求する。この要求は、要求されたデータ・セクタを読み出す TrueCrypt パイロットを経由する。次にこのセクタで(データが)復号され、オペレーティング・システムへ返される。この読み出し機能は、ドライバのリクエスト・マネージャによって管理(operate)されている。	SFR 実施
		データの書き込み	この機能は、ボリューム上に暗号化されていないデータの書き込みと暗号化を実施する。オペレーティング・システムは、暗号化ボリュームに対応する「デバイス」に(データの)書き込みを要求する。この要求は、送信されたデータを暗号化し、ボリュームに書き込む TrueCrypt デバイスドライバを経由する。書き込みは、セクタごとに行われる。この書き込み機能は、ドライバのリクエスト・マネージャによって管理されている。	SFR 実施

n°	サブシステムの名称	モジュールの名称	概要	SFR 実施 SFR 支援 SFR 非干渉
8. 暗号化ディスクの情報の表示				
		情報の表示	TrueCrypt は、暗号化ディスクについて記録されている情報(位置、サイズ、タイプ、暗号化アルゴリズム、鍵サイズ...)をドライバに要求する。この情報は、「Volumes」メニューから「Volume properties」で確認することができる。	SFR 非干渉
9. 暗号化の操作				
		RNG	乱数生成器。このモジュールで生成されるデータが、マスタ鍵、IV(二次LRW モード鍵)、シード、および鍵ファイルの生成に使用されるランダムデータである。	SFR 実施
		暗号化の操作	このモジュールは、例えば、ハッシュ化、暗号化、復号など TrueCrypt のサブシステムによって要求される全ての暗号化の操作を実施する。	SFR 実施
10. 鍵ファイルの生成				
		鍵ファイルの生成	このモジュールは、鍵ファイル(ランダムな 64 バイトのバイナリ・ファイル)を生成することができる。	SFR 非干渉

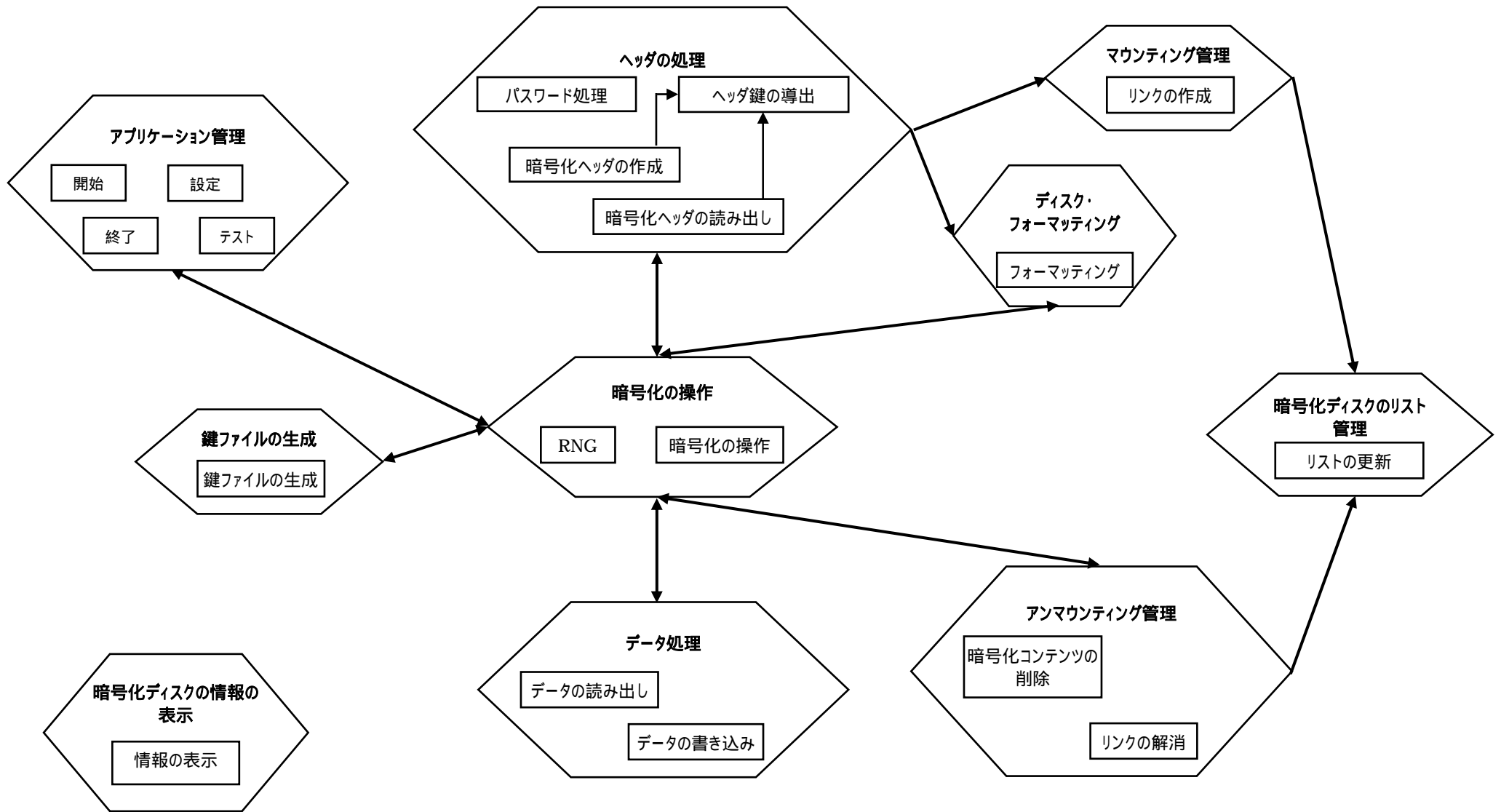


図 2: モジュール表示

4.2. TSF モジュールの説明

1.アプリケーション管理サブシステム			
開始	機能	<p>このモジュールは TrueCrypt.exe が実行時に起動される。アプリケーションは、TrueCrypt ドライバをロードする(ドライバが既にロードされている場合は、ドライバにアタッチ)ことで開始される。不具合が発生すると、このアプリケーションは初期化を正常に実施できないため終了する。</p> <p>一旦ドライバをロード(またはアタッチすると)、TrueCrypt は(Windows の VirtualLock 関数を使用して)メモリの中に機密性の高いグローバル変数をロックする。最後に、アプリケーションはユーザ・インタフェースを開始し、既にマウントされているボリュームをリストする(開始前に、ドライバが既にメモリにある場合)。</p>	
	インタフェース / 返される値	WINMAIN	0
	相互作用	なし	
設定	機能	<p>このモジュールは、TrueCrypt の設定を変更することができる。</p> <p>変更の対象となる設定には：</p> <ul style="list-style-type: none"> - デフォルトのマウントオプション - TrueCrypt を常駐タスクとして機能させる - Windows が起動した場合、またはセッションが開始された場合に実行される動作 - 自動アンマウントの条件 - TrueCrypt と Windows との関連性 - パスワードのキャッシングのポリシー 	
	インタフェース / 返される値	PreferencesDlgProc	0
	相互作用	なし	
テスト	機能	<p>このモジュールは、アプリケーションの「Tools」メニューからさまざまなタイプのテストの実行を可能とする。暗号アルゴリズム・シーケンスが、テスト*、および暗号アルゴリズム・ベクタ・テスト**を実施する。</p>	
	インタフェース / 返される値	PerformBenchmark* CipherTestDialogProc** AutoTestAlgorithms**	True / False 1 / 0 True / False
	相互作用	なし	
終了	機能	<p>このモジュールは、TrueCrypt のアプリケーションを起動する。アプリケーションを終了してもドライバがアンロードされたことにはならない。このドライバは、TrueCrypt が動作していなくてもマウントされているディスクへの書き込みや読み出しに対応しなければならない。</p>	

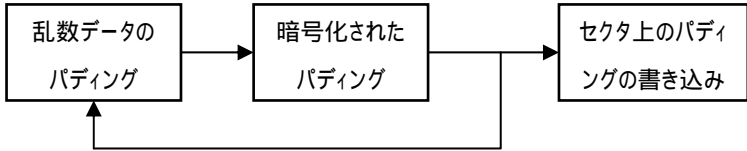
	インタフェース / 返される値	localcleanup	
	その他のモジュールが使用する(使用される)インタフェース	burn	localcleanup
	アルゴリズムの説明	機密性の高いグローバル変数値を消去したのちに、HMI を解消する。	

2.ヘッダの処理サブシステム

パスワード処理	機能	鍵ファイルを使用してヘッダ鍵を生成する前に、このファイルを使用してユーザ・パスワードを変換することができる。	
	インタフェース / 返される値	KeyFilesApply KeyFileProcess	True / False True / False
	その他のモジュールが使用する(使用される)インタフェース	なし	なし
	アルゴリズムの説明	[SPEC_TRUECRYPTO]の第 3.3.2.2.2 章「ユーザ・パスワードの処理」の項を参照。	

ヘッダ鍵の導出	機能	変換されたパスワードと 64 バイトのシードから 2 つのヘッダ鍵(主ヘッダ鍵と二次ヘッダ鍵)を導出することができる。これらの鍵は、ボリュームのヘッダ(第一セクタ)を暗号化 / 復号するために使用される。	
	インタフェース / 返される値	derive_key_sha1 derive_key_ripemd160 derive_key_whirlpool derive_u_sha1 derive_u_ripemd160 derive_u_whirlpool hmac_sha1 hmac_ripemd160 hmac_whirlpool	
	その他のモジュールが使用する(使用される)インタフェース	sha1_begin sha1_hash sha1_end RMD160Init RMD160Update RMD160Final WHIRLPOOL_init	hmac_sha1 hmac_sha1 hmac_sha1 hmac_ripemd160 hmac_ripemd160 hmac_ripemd160 hmac_whirlpool

		WHIRLPOOL_add WHIRLPOOL_finalize	hmac_whirlpool hmac_whirlpool
	アルゴリズムの説明	[SPEC_TRUECRYPTO]の第 3.3.2.2.3 章「PKCS#5v2 による導出」の項を参照。	
暗号化ヘッダの作成	機能	ボリュームの暗号化ヘッダを作成することができる。ボリュームのヘッダには、次のような情報が含まれている：暗号化とハッシュに使用されるアルゴリズム、マスタ鍵とその二次鍵 (LRW モード)	
	インタフェース / 返される値	VolumeWriteHeader	0 ERR_OUTOFMEMORY (2) ERR_CIPHER_INIT_WEAK_KEY (19) ERR_CIPHER_INIT_FAILURE (18)
	その他のモジュールが使用する (使用される) インタフェース	crypto_open RandgetBytes DetectWeakSecondaryKey derive_key_sha1 derive_key_ripemd160 derive_key_whirlpool crc32 EAInit EAInitMode EncryptBuffer burn	VolumeWriteHeader
	アルゴリズムの説明	[SPEC_TRUECRYPTO]の第 3.4.1 章「暗号化 / 復号」の項を参照。	
暗号化ヘッダの読み出し	機能	ボリュームの暗号化されたヘッダを読み出すことができる。ボリュームのヘッダにはボリュームに関する次のような情報が含まれている：暗号化とハッシュに使用されるアルゴリズム、マスタ鍵とその二次鍵 (LRW モード)	
	インタフェース / 返される値	VolumeReadHeader	0 ERR_OUTOFMEMORY (2) ERR_CIPHER_INIT_FAILURE (18) ERR_MODE_INIT_FAILED (39) ERR_NEW_VERSION_REQUIRED (17) ERR_PASSWORD_WRONG (3)

		FormatNtfs WriteSector	ERR_MODE_INIT_FAILED(39) ERR_OS_ERROR(1) True False True False
	その他のモジュールが使用する(使用される)インタフェース	VolumeWriteHeader burn crypto_close RandpeekBytes RandgetBytes EncryptoSectors	FormatVolume FormatVolume FormatNoFs FormatFat FormatVolume FormatNoFs FormatFat FormatNofs FormatFat WriteSector
	アルゴリズム説明		

4. マウンティング管理サブシステム

リンクの作成	機能	TrueCrypt は、Windows に対し、マウントされる暗号化ディスクにドライブ・レターを割り当てるよう要求する。このリンクが作成された時点で、ディスクにアクセスすることができるようになる。	
	インタフェース / 返される値	(Windows の IoCreateDevice 関数が使用する) TCCreatDeviceObject	
	その他のモジュールが使用する(使用される)インタフェース	なし	なし
	アルゴリズム説明	Windows API に対し、ボリュームが対応するディスク・レターを指定するよう要求する。	

5. 暗号化ディスクのリスト管理サブシステム

リストの更新	機能	TrueCrypt ドライバに、暗号化ディスクをリストに追加、または削除するよう要求する。	
	インタフェース / 返	GetMountList	Liste

	される値		
	相互作用	なし	
6.アンマウンティング管理サブシステム			
リンクの解消	機能	TrueCrypt は、Windows に暗号化ディスクのマウントにより生成されたリンクを削除するよう要求する。このリンクが削除されると、ディスクにアクセスすることができなくなる。	
	インタフェース / 返される値	(Windows の IoDeleteDevice 関数を使用する) TCDeleteDeviceObject	
	その他のモジュールが使用する(使用される)インタフェース	なし	なし
	アルゴリズム説明	Windows API に対し、ドライブ・レターとボリュームとのリンクを削除するよう要求する。	
暗号化コンテンツの削除	機能	マスタ鍵とマスタ鍵から導出された管理鍵の削除	
	インタフェース / 返される値		
	その他のモジュールが使用する(使用される)インタフェース	crypto_close	
	アルゴリズム説明	なし	
7.データ処理サブシステム			
データの読み出し	機能	この機能は、ボリューム上の暗号化されたデータを読み出すことができる。オペレーティング・システムは、この暗号化ボリュームに対応する「デバイス」に(データの)読み出しを要求する。この要求は、要求されたデータ・セクタを読み出す TrueCrypt ドライバを経由する。次にこのセクタで(データが)復号され、オペレーティング・システムへ返される。この読み出し機能は、ドライバのリクエスト・マネージャによって管理されている。	
	インタフェース / 返される値	DecryptSectors	
	その他のモジュールが使用する(使用される)インタフェース	DecryptBufferLRW64 DecryptBufferLRW128 DecryptBufferCBC InitSectorIVAndWhitening	DecryptSectors

	アルゴリズム説明	暗号化データがバッファに送信される。 バッファが RAM で復号される。 復号されたデータがユーザに返される。	
データの書き込み	機能	この機能は、ボリューム上のデータの暗号化と書き込みに対応している。オペレーティング・システムは、この暗号化ボリュームに対応する「デバイス」に(データの)書き込みを要求する。この要求は、送信されたデータを暗号化し、ボリュームに書き込む TrueCrypt ドライバを経由する。書き込みは、セクタごとに行われる。この書き込み機能は、ドライバのリクエスト・マネージャによって管理されている。	
	インタフェース / 返される値	EncryptSectors	
	その他のモジュールが使用する(使用される)インタフェース	EncryptBufferLRW64 EncryptBufferLRW128 EncryptBufferCBC InitSectorIVAndWhitening	EncryptSectors
	アルゴリズム説明	暗号化されていないデータがバッファに送信される。 バッファが RAM で暗号化される。 暗号化されたデータがディスクに書き込まれる。	

8. 暗号化ディスクの情報の表示サブシステム


情報の表示	機能	TrueCrypt は、暗号化ディスクについて記録されている情報(位置、サイズ、タイプ、暗号化アルゴリズム、鍵サイズ...)をドライバに要求する。この情報は、「Volumes メニュー」Volume properties」で確認することができる。	
	インタフェース / 返される値	VolumePropertiesDlgProc	
	相互作用	なし	

9. 暗号化の操作サブシステム

RNG	機能	乱数生成器。このモジュールで生成されるデータが、マスタ鍵、IV(二次LRW モード鍵)、シード、および鍵ファイルの生成に使用されるランダム・データである。	
	インタフェース / 返される値	Randinit Randfree RandgetBytes SlowPoll FastPoll RandaddBuf Randmix	0 / 1 True / False True True True

		RandaddInt32 RandAddInt RandaddByte RandpeekBytes	True
	その他のモジュール が使用する(使用 される)インタフェー ス	burn sha1_begin sha1_hash sha1_end RMD160Init RMD160Update RMD160Final WHIRLPOOL_init WHIRLPOOL_add WHIRLPOOL_finalize	Randfree SlowPoll FastPoll Randmix Randmix Randmix Randmix Randmix Randmix Randmix Randmix Randmix
	アルゴリズム説明	[SPEC_CRYPT0]の第 3.3.2.1.3 章「機能の説明」の項を参照。	
暗号化の操作	機能	このモジュールは、例えば、ハッシュ化、暗号化、復号など TrueCrypt のサブシステムによって要求される全ての暗号化の操作を実行する。	
	インタフェース / 返 される値	Sha1_begin Sha1_hash Sha1_end Sha1_compile RMD160Init RMD160Update RMD160Final RMD160Transform WHIRLPOOL_init WHIRLPOOL_add WHIRLPOOL_finalize ProcessBuffer burn DetectWeakSecondaryKey crypto_open crc32 EAInit	True / False Point.to CRYPTO_INFO NULL structure 4-byte ineger ERR_SUCCESS(1)

		<p>CipherInit</p> <p>BF_set_key BF_encrypt aes_encrypt_key aes_encrypt_key128 aes_encrypt_key192 aes_encrypt_key256 aes_decrypt_key aes_decrypt_key128 aes_decrypt_key192 aes_decrypt_key256 des_key_sched des_set_key des_is_weak_key CAST_set_key serpent_set_key twofish_set_key EAInitMode Gf64TabInit Gf128Tab64Init EncryptBuffer EncryptBufferLRW64 EncryptBufferLRW128 EncryptBufferCBC EncipherBlock BF_ecb_le_encrypt BF_encrypt BF_decrypt aes_encrypt des_encrypt</p>	<p>ERR_CIPHER_INIT_FAILURE(18) ERR_CIPHER_INIT_WEAK_KEY(19) ERR_SUCCESS(0) ERR_CIPHER_INIT_FAILURE(18) ERR_CIPHER_INIT_WEAK_KEY(19)</p> <p>EXIT_SUCCESS(0)</p> <p>EXIT_SUCCESS(0)</p> <p>0 / -2 0 / -2 0 / 1</p> <p>Level pointer 1_key True / False 1 / 0 1 / 0</p> <p>EXIT_SUCCESS(0) EXIT_FAILURE(1)</p>
	その他のモジュール が使用する(使用	なし	

TOE design	
TRUECRYPTO-SPM030-TDS	

	される)インタフェース	
	アルゴリズム説明	なし
10. 鍵ファイル生成サブシステム		
鍵ファイルの生成	機能	このモジュールは、鍵ファイル(64 バイトのランダム・データによるバイナリ・ファイル)を生成することができる。RNG モジュールに生成の要求が送られる、64 バイトのランダムなバイナリデータがファイルに送られる、ディスク上に鍵ファイルが生成される
	インタフェース / 返される値	KeyfileGeneratorDlgProc
	相互作用	なし

5. TSFI とサブシステムの対応

TSFI	サブシステム
暗号化ディスクの作成	ヘッダの処理
ディスクのマウント	
ディスクのパスワードの修正	
鍵ファイルの追加 / 削除	
ハッシュ・アルゴリズムの修正	
TrueCrypt の起動	アプリケーション管理
TrueCrypt の終了	
キャッシュ化したパスワードの消去	
ディスクへの書き込み	データ処理
ディスクからの読み出し	
鍵ファイルの生成	鍵ファイルの生成
ディスクのアンマウント	アンマウンティング管理

6. TOE 設計に含まれる SFR

サブシステム	モジュール	SFR																								
		FCS_CKM.1 / ヘッダ鍵	FCS_CKM.1 / マスタ鍵	FCS_CKM.3 / ヘッダ鍵	FCS_CKM.3 / マスタ鍵	FCS_CKM.4	FCS_COP.1	FDP_ACC.1	FDP_ACF.1	FDP_RIP.1	FIA_UID.1 / ディスク所有者	FIA_UAU.1 / ディスク所有者	FIA_SOS.1 / パスワード	FMT_MOF.1 / ディスク所有	FMT_MSA.2	FMT_MSA.3	FMT_MTD.1 / 認証データ	FMT_MTD.1 / マスタ鍵	FMT_MTD.1 / ヘッダ鍵	FMT_MTD.2 / 認証データ	FMT_MTD.3	FMT_SMF.1	FMT_SMR.1	FPT_FLS.1	FRU_FLT.1	
アプリケーション管理	開始																									
	設定																									
	テスト																									
	終了									X																
ヘッダの処理	パスワード処理						X					X	X			X			X	X	X	X				
	ヘッダ鍵の導出	X		X										X	X			X								
	暗号化ヘッダの作成		X	X			X						X	X	X		X	X		X	X	X				
	暗号化ヘッダの読み出し	X		X	X		X	X	X		X	X	X									X	X			
ディスク・フォーマッティング	フォーマッティング						X										X				X					
マウンティング管理	リンクの作成																									
暗号化ディスクのリスト管理	リストの更新																									

サブシステム	モジュール	SFR																								
		FCS_CKM.1 / ヘッド鍵	FCS_CKM.1 / マスタ鍵	FCS_CKM.3 / ヘッド鍵	FCS_CKM.3 / マスタ鍵	FCS_CKM.4	FCS_COP.1	FDP_ACC.1	FDP_ACF.1	FDP_RIP.1	FIA_UID.1 / ディスク所有者	FIA_UAU.1 / ディスク所有者	FIA_SOS.1 / パスワード	FMT_MOF.1 / ディスク所有	FMT_MSA.2	FMT_MSA.3	FMT_MTD.1 / 認証データ	FMT_MTD.1 / マスタ鍵	FMT_MTD.1 / ヘッド鍵	FMT_MTD.2 / 認証データ	FMT_MTD.3	FMT_SMF.1	FMT_SMR.1	FPT_FLS.1	FRU_FLT.1	
アンマウンティング管理	リンクの解消																								X	X
	暗号化コンテンツの削除					X	X			X															X	X
データ処理	データの読み出し				X	X												X								
	データの書き込み				X	X												X								
暗号化ディスクの情報の表示	情報の表示																									
暗号化の操作	RNG	X	X															X	X		X					
	暗号化の操作	X	X	X	X	X	X																			
鍵ファイルの生成	鍵ファイルの生成																									

付録 A. 略語と頭字語

6.1. 略語と頭字語

CC: コモン・クライテリア

CEM: 情報技術セキュリティ評価のための共通方法

SFR: セキュリティ機能要件

ST: セキュリティ・ターゲット

セキュリティ・ターゲットには、開発者の視点で捉えた特定の製品のセキュリティ要件が記載される。セキュリティ機能の仕様(要約仕様)を含み、1 つ以上のプロテクション・プロファイル(PP)に定義されたセキュリティ要件を含むこともある。


TOE: 評価対象。TOE は、評価対象となる製品、またはシステムの一部である。

TSF: TOE セキュリティ機能

TSFI: TSF インタフェース

付録 B. 参照文献

- [CC1] *Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model. Version 3.1, Revision 1, September 2006. CCIMB-2006-09-001.*
- [CC2] *Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements. Version 3.1, Revision 1, September 2006. CCIMB-2006-09-002.*
- [CC3] *Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements. Version 3.1, Revision 1, September 2006. CCIMB-2006-09-003.*
- [CEM] *Common Criteria for Information Technology Security Evaluation, Evaluation Methodology. Version 3.1, Revision 1, September 2006. CCIMB-2006-09-004.*
- [CRYPTO] *Mécanismes de cryptographie: règles et recommandations concernant le choix et la dimensionnement des mécanismes cryptographiques de niveau de robustesse standard. (Cryptographic mechanisms: rules and recommendations concerning the choice and sizing of cryptographic mechanisms of standard robustness) Version 1.02, 19 November 2004. DCSSI.*
- [ST] *TrueCrypt Security Target, Version 2.00, October 22nd 2007, SPM030-ST-2.00.*
- [ADV_FSP] *TOE functional specifications, Version 2.00, October 22nd 2007, SPM030-FSP-2.00.*
- [SPEC_CRYPTO] *Spécifications cryptographiques, Version 2.00, October 22nd 2007, SPM030-SPEC.*

TOE design	
TRUECRYPTO-SPM030-TDS	

付録 C. コモン・クライテリアに関する情報

C.1. 本書の目的

本書は ADV クラスの ADV_TDS ファミリに属す ADV_TDS.3 コンポーネントの要件に適合している。本書は、TRUECRYPT ソフトウェアの上位設計について説明する。

ADV 保証クラスはコモン・クライテリアの評価の観点の TOE の開発の情報を必要とする。この情報は脆弱性分析とテストに利用される。

このクラスは、異なるレベルで抽象化された TSF の構造と表現に応じ 6 つのファミリに分類されている。

- SFR の設計と実装に関する要件が含まれるファミリは、次の 3 つである。
 - + ADV_FSP (機能仕様)
 - + ADV_TDS
 - + ADV_IMP
- ドメイン分離、TSF 自己保護、セキュリティ機能の迂回防止に対応するシステム・アーキテクチャの説明に関する要件が含まれるファミリは、次の 1 つである。
 - + ADV_ARC
- セキュリティ・ポリシーのモデル記述、およびポリシー・モデルと機能仕様の対応の要件は、次のファミリに含まれている。
 - + ADV_SPM
- モジュール性の観点、レイヤ化し複雑さを最小限に抑えるなど、内部的な TSF 構造の説明に関する要件は、次のファミリに含まれている。
 - + ADV_INT

これらファミリのコンポーネントは、次のような 2 つの属性を立証することを目的としている。

- 第一に、TOE が正常に機能し、その機能仕様に適合していること。これを立証するための要件には、ADV_FSP、ADV_SPM、ADV_TDS、および ADV_IMP ファミリが対応している。
- 次に、TOE のセキュリティ機能がバイパスされたり、破壊されるようなことがないことである。これを立証するための要件には、ADV_ARC、および ADV_INT ファミリが対応している。

- 機能性では、読者がモジュールの機能する方法を一般的な概念として取得することができる、
- 提供されるインタフェース、即ち機能呼び出すために他のモジュールによって使用されるインタフェース、
- それらインタフェースによって返される値、
- (その他のモジュールによって提供され)使用するインタフェース、および
- アルゴリズム的な説明。

	TSF のサブシステム			TSF モジュール		
	SFR - 実施	SFR - 支援	SFR - 非干渉	SFR - 実施	SFR - 支援	SFR - 非干渉
ADV_TDS.3 基本モジュール設計	相互作用、 記述	相互作用、 記述	相互作用、 記述	共通データ、 インタフェース、 アルゴリズム	相互作用、 目的	相互作用、 目的

C.3.3. ADV_TDS.3 コンポーネントの要件

開発者のタスク:

CC パート 3 対応 エレメント	説明
ADV_TDS.3.1.D	開発者は、TOE の設計を提供しなければならない。
ADV_TDS.3.2.D	開発者は、機能仕様の TSFI から TOE 設計で利用可能な分解の最下位レベルへのマッピングを提供しなければならない。

コンテンツ、および証明用コンポーネントの表示:

CC パート 3 対応 エレメント	説明
ADV_TDS.3.1.C	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。
ADV_TDS.3.2.C	設計は、モジュールの観点から TSF を記述しなければならない。
ADV_TDS.3.3.C	設計は、TSF のすべてのサブシステムを識別しなければならない。
ADV_TDS.3.4.C	設計は、TSF の各サブシステムの記述を提供しなければならない。
ADV_TDS.3.5.C	設計は、TSF のすべてのサブシステム間の相互作用の記述を提供しなければならない。
ADV_TDS.3.6.C	設計は、TSF のサブシステムから TSF 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。
ADV_TDS.3.7.C	設計は、目的の観点から各 SFR 実施モジュールを記述しなければならない。
ADV_TDS.3.8.C	設計は、各 SFR 実施モジュールの SFR 関連インタフェース、それらのインタフェースからの戻り値、及び他のモジュールに対して呼び出されるインタフェースの観点から各 SFR 実施モジュールを記述しなければならない。
ADV_TDS.3.9.C	設計は、目的及びその他のモジュールとの相互作用の観点から各 SFR 支援モジュールまたは

	SFR 非干渉モジュールを記述しなければならない。
ADV_TDS.3.10.C	マッピングは、TOE 設計で記述されているすべてのふるまいが、そのふるまいを呼び出す TSFI にマッピングされていることを実証しなければならない。

C.3.4. 基本的な CEM のタスク

CEM(評価手法)には、評価者の基本的なタスクが記述されている。これらのタスクを正常に完了するには、評価者は、さまざまな評価関連文書に基づき評価を実施しなければならない。


評価に要求される要素：

- セキュリティ・ターゲット[ST]
- TOE 機能仕様[ADV_FSP]
- TOE 設計[ADV_TDS]
- セキュリティ・アーキテクチャ記述[ADV_ARC]

以下の表は、CEM の基本的なタスク、開発者によって提供される証拠資料での対応を示したものである。

CC パート 3 対応 エレメント	CEM の ワーク・ユニット	説明	開発者による対応
ADV_TDS.3.1.C	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。		
	ADV_TDS.3-1	評価者は、TOE 全体の構造がサブシステムの観点から記述されていることを決定するために、TOE 設計を検査しなければならない。	[SPEC_CRYPT0]の第 2 章、TrueCrypt の暗号仕様を参照。 TSF の 12、13 ページ、14 ページの図 1: TrueCrypt のサブシステム構成
ADV_TDS.3.2.C	設計は、モジュールの観点から TSF を記述しなければならない。		
	ADV_TDS.3-2	評価者は、TSF 全体がモジュールの観点から記述されていることを決定するために、その TOE 設計を検査しなければならない。	第 4 章、TSF モジュールの項 (17 ページ)参照。
ADV_TDS.3.3.C	設計は、TSF のすべてのサブシステムを識別しなければならない。		
	ADV_TDS.3-3	評価者は、TSF のすべてのサブシステムが識別されることを決定するために、その TOE 設計を検査しなければならない。	[SPEC_CRYPT0]の第 2 章、TrueCrypt の暗号仕様を参照。 TSF の 12 ページ。
ADV_TDS.3.4.C	設計は、TSF の各サブシステムの記述を提供しなければならない。		
	ADV_TDS.3-4	評価者は、TSF の各サブシステムが ST で記述された SFR の実施におけるそれぞれの役	[SPEC_CRYPT0]の第 2 章、TrueCrypt の暗号仕

		割を記述することを決定するために、その TOE 設計を検査しなければならない。	様を参照。 TSF の 12 ページ。
ADV_TDS.3.5.C	設計は、TSF のすべてのサブシステム間の相互作用の記述を提供しなければならない。		
	ADV_TDS.3-5	評価者は、TSF のサブシステム間の相互作用が記述されることを決定するために、その TOE 設計を検査しなければならない。	第 3 章、相互作用の項 (15、16 ページ) 参照。
ADV_TDS.3.6.C	設計は、TSF のサブシステムから TSF 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。		
	ADV_TDS.3-6	評価者は、TSF のサブシステムと TSF のモジュールの間のマッピングが完全であることを決定するために、その TOE 設計を検査しなければならない。	第 4.1 章、サブシステムに基づく TSF モジュールの識別に関する表 (17 - 21 ページ) 参照。
	ADV_TDS.3-7	評価者は、TSF サブシステムと TSF のモジュールの間のマッピングが正確であることを決定するために、その TOE 設計を検査しなければならない。	第 4.1 章、サブシステムに基づく TSF モジュールの識別に関する表 (17 - 21 ページ) 参照。
ADV_TDS.3.7.C	設計は、目的の観点から各 SFR 実施モジュールを記述しなければならない。		
	ADV_TDS.3-8	評価者は、各 SFR 実施モジュールの目的の記述が完全で正確であることを決定するために、その TOE 設計を検査しなければならない。	第 4.1 章、サブシステムに基づく TSF モジュールの識別に関する表 (17 - 21 ページ) 参照。
ADV_TDS.3.8.C	設計は、各 SFR 実施モジュールの SFR 関連インタフェース、それらのインタフェースからの戻り値、及び他のモジュールに対して呼び出されるインタフェースの観点から各 SFR 実施モジュールを記述しなければならない。		
	ADV_TDS.3-9	評価者は、各 SFR 実施モジュールによって提示されるインタフェースの記述に SFR 関連パラメタの正確かつ完全な記述、各インタフェースに対する呼び出し規則、及びインタフェースによって直接戻されるすべての値が含まれることを決定するために、その TOE 設計を検査しなければならない。	第 4.2 章、TSF の説明 (23 - 31 ページ) 参照。
ADV_TDS.3.9.C	設計は、目的及びその他のモジュールとの相互作用の観点から各 SFR 支援モジュールまたは SFR 非干渉モジュールを記述しなければならない。		
	ADV_TDS.3-10	評価者は、SFR 支援及び SFR 非干渉モジュールが正しく分類されていることを決定するために、その TOE 設計を検査しなければならない。	第 4.2 章、TSF の説明 (23 - 31 ページ) 参照。
	ADV_TDS.3-11	評価者は、各 SFR 支援もしくは SFR 非干	第 4.2 章、TSF の説明 (23

TOE design	
TRUECRYPTO-SPM030-TDS	

		<p>渉モジュールの目的の記述が完全で正確であることを決定するために、その TOE 設計を検査しなければならない。</p>	<p>- 31 ページ) 参照。</p>
	ADV_TDS.3-12	<p>評価者は、その他のモジュールと SFR 支援モジュール、もしくは SFR 非干渉モジュールとの相互作用の記述が完全で正確であることを決定するために、その TOE 設計を検査しなければならない。</p>	<p>第 4.2 章、TSF の説明(23 - 31 ページ) 参照。</p>
ADV_TDS.3.10.C	<p>マッピングは、TOE 設計で記述されているすべてのふるまいが、そのふるまいを呼び出す TSFI にマッピングされていることを実証しなければならない。</p>		
	ADV_TDS.3-13	<p>評価者は、TOE 設計が、機能仕様で記述されている TSFI から TOE 設計で記述されている TSF のモジュールへの完全で正確なマッピングを含むことを決定するために、その TOE 設計を検査しなければならない。</p>	<p>第 5 章、TSFI とサブシステム間の訴追性(32 ページ) 参照。</p>