JISEC

「ハードコピーデバイスのプロテクションプロファイル」適合の

申請案件についてのガイドライン

第 1.7 版

旧版

注意 ： この文書は、参考のために公開しています。 本ガイドラインを使用する場合は、最新版を参照してください。

2015 年 9 月に複合機の技術部会及び日米認証機関共同で作成した PP である「Protection Profile for Hardcopy Devices, 1.0 dated September 10, 2015」を用いて IT セキュリティ評価及び認証制度において認証申請をする際の指針を示すものです。

独立行政法人情報処理推進機構
JISEC

2020 年 7 月 1 日発行

目次

1. はじめに 3
2. 申請時における補足事項 4
2.1 Errata の適用について 4
2.2 申請時の提出書類について 6
2.2.1 提出が必要な書類 6
2.2.2 評価者テスト方針概要書の記載事項 7
2.3 本制度における解釈 9
2.3.1 エントロピー源を第三者製品に依存している場合の補足事項 9
2.3.2 暗号モジュール試験及び認証制度の活用について 11
2.3.3 FDP_DSK_EXT.1 に関連する時限的措置について 11
2.3.4 FCS_RBG_EXT.1 のテストに関連する措置について 12
2.3.5 FCS_IPSEC_EXT.1.1 に関する措置について 13
2.3.6 FCS_TLS_EXT.1.1 のテストに関する措置について 16
3. 申請時の提出書類の確認について 17
3.1 ST の確認事項 17
3.2 エントロピー記述の確認事項 17
3.3 鍵管理記述の確認事項 18
3.4 評価者テスト方針概要書の確認事項 19
3.4.1 FCS_CKM.4 19
3.4.2 FCS_COP.1(a) 20
3.4.3 FCS_COP.1(b) 20
3.4.4 FCS_RBG_EXT.1 20
3.4.5 FDP_DSK_EXT.1 20
3.4.6 FDP_FXS_EXT.1 21
3.4.7 FCS_IPSEC_EXT.1 21
3.4.8 FCS_TLS_EXT.1 21
4. 評価に関する補足事項 22
4.1 評価報告書について 22

改版履歴

版数	発行日	おもな変更内容
1.0	2016/8/26	・新規作成
1.1	2017/4/26	・「評価者テスト方針概要書の記載事項」の記載内容更新
1.2	2017/6/28	・「認証済みPPとしてのHCD-PP 1.0」「ST作成時の注意点」の記載を追加
1.3	2018/6/6	・「2.3.3 FDP_DSK_EXT.1 に関連する時限的措置について」を追加 ・「3. 申請時の提出書類の確認について」を追加
1.4	2019/1/10	・エントロピー源に関する記載を変更
1.5	2019/4/10	・「2.3.4 FCS_RBG_EXT.1 のテストに関連する措置について」を追加
1.6	2019/8/1	・「2.3.5 FCS_IPSEC_EXT.1.1 に関する措置について」を追加 ・「4.評価における補足事項」を追加
1.7	2020/7/1	・「2.3.6 FCS_TLS_EXT.1.1 のテストに関する措置について」を追加

1. はじめに

本ガイドラインは、「Protection Profile for Hardcopy Devices, 1.0 dated September 10, 2015」（以下、“HCD-PP 1.0”という） に適合する製品を IT セキュリティ評価及び認証制度（JISEC、以下「本制度」という）において認証申請をする際の指針を示すものです。

2. 申請時における補足事項

本章では、申請者が HCD-PP 1.0 適合の認証を申請する際に申請書類とともに提出いただく資料について、必要となる記載事項や本制度における HCD-PP 1.0 適用の解釈を示しています。

2.1 Errata の適用について

HCD-PP 1.0 を認証済み PP として使用するには、以下の Errata[1] を適用する必要があります。

- HCD-PP 1.0
  名称： Protection Profile for Hardcopy Devices
  バージョン： 1.0 dated September 10, 2015
  認証識別： JISEC-C0553

- Errata
  名称： Protection Profile for Hardcopy Devices - v1.0 Errata #1, June 2017

Errata は、以下の JISEC の公開ウェブページからダウンロードすることができます。

- HCD-PP 1.0 の認証情報ページの URL

（日本語）
https://www.ipa.go.jp/security/jisec/certified_pps/c0553/c0553_it7627.html
(English)
https://www.ipa.go.jp/security/jisec/jisec_e/certified_pps/c0553/c0553_it7627.html

Errata を適用した HCD-PP 1.0 を使用して、ST を作成する場合の注意点を以下に示します。

A. PP 主張

適合する PP として、HCD-PP 1.0 の名称とバージョンに Errata の識別を併記します。

[1] 本 Errata は、CC/CEM における PP の評価を満足するため、機能要件に関する表記方法、依存性、拡張コンポーネント定義の誤記および用語定義の不足を訂正するものです。

記載例：

PP 主張 本 ST および TOE が適合する PP は下記のとおり。 PP 名称： Protection Profile for Hardcopy Devices PP バージョン： 1.0 dated September 10, 2015 Errata： Protection Profile for Hardcopy Devices – v1.0 Errata #1, June 2017

B. 適合根拠

HCD-PP 1.0 の“Conformance to this Protection Profile”（14～20 段落）で示されている規則に適合していることを HCD-PP 1.0 の語句で記載します。

さらに TOE の TOE 種別が、HCD-PP 1.0 の TOE 種別と一貫していることも記載します。

記載例：

適合主張根拠 PP が要求する以下の条件を満足し、PP の要求どおり「Exact Conformance」である。そのため、TOE 種別は PP と一貫している。 ・ Required Uses Printing, Scanning, Network communications, Administration ・ Conditionally Mandatory Uses Storage and retrieval, Field-Replaceable Nonvolatile Storage ・ Optional Uses なし

C. 拡張コンポーネント定義

Errata で拡張コンポーネント定義の訂正または依存性の訂正が示されている場合は、Errata で示されている記載内容に変更します。

D. セキュリティ機能要件

Errata で表記の訂正または依存性の訂正が示されている SFR は、Errata で示されている記載内容に変更します。

2.2 申請時の提出書類について

2.2.1 提出が必要な書類

HCD-PP 1.0 に適合する複合機の認証申請では、通常の認証申請（「IT セキュリティ認証申請等のための手引」（CCM-02-A）5 章を参照のこと）に加え、以下の資料の提出を必要とします。 CD-R 等の電子媒体に格納して提出してください。

なお、これらの資料は公開されません。

1. エントロピー記述 【附属書 E】

   エントロピー記述とは、評価対象である複合機において用いられる乱数生成機能が必要なエントロピーを提供していることを保証するため開発者が提供する資料です。このエントロピー記述に記載すべき事項は HCD-PP 1.0 の**附属書 E** に記述されています。

   エントロピー源は評価対象のセキュリティ機能の根拠となるため、評価の過程でその妥当性が確認できない場合には、評価作業が継続できなくなります。エントロピー源の生成の妥当性を関係者が事前に確認することにより、評価の過程での後戻りの発生を防ぐことになります。

   なお、エントロピー源に関する情報は ST にも記載が必要ですので、HCD-PP 1.0 の要求を確認願います。

   また、エントロピー記述には、エントロピー源を正当化するために実施したテストの結果を記載する必要があります。 ただし、開発者以外の第三者製品[2]を用いてエントロピー源としており、附属書 E を完全に満たす記述ができない場合については、「2.3.1 エントロピー源を第三者製品に依存している場合の補足事項」を参照願います。

2. 鍵管理記述 【附属書 F】

   鍵管理記述とは、評価対象である複合機において用いられる暗号鍵が適切に保護されていることを保証するため開発者が提供する資料です。この鍵管理記述に記載すべき事項は HCD-PP 1.0 の**附属書 F** に記述されています。

   鍵管理は評価対象の設計に係るため、評価の過程でその不備が確認された場合には、評価作業が継続できなくなります。鍵管理の適

[2] エントロピー源が、たとえばオープンソースの製品のように開発者による実装ではない場合でも、未処理のエントロピー量を取得できる場合は、本項の「第三者製品」には該当しません。

切性を関係者が事前に確認することにより、評価の過程での後戻りの発生を防ぐことになり、評価を効率的かつ適切に実施するための重要な入力となります。

3. 評価者テスト方針概要書

上記附属書に加え、HCD-PP 1.0 の保証アクティビティで評価に求められているテストについて、どのようなツールや技法、テストを用いて確認を行うのかを評価機関と合意の上、その概要を提出いただきます。

これらのテスト実施要件が明確でない場合、評価作業の長期化または認証申請の取下げとなる懸念があります。評価機関選定にあたり開発者はテスト実施内容について理解をし、開発者の責任において評価機関のテスト実施要件やテスト方針を確認したうえで申請を行ってください。

評価者テスト方針概要書に記載する情報の詳細は、「2.2.2 評価者テスト方針概要書の記載事項」を参照願います。

2.2.2 評価者テスト方針概要書の記載事項

評価者テスト方針概要書には、予定期間内に HCD-PP 1.0 で要求されているテストを開発者が実施可能と判断していることを示していただくため、以下の内容を記載願います。

A. テスト開始と終了の予定日

申請日からテストの終了の予定日までの期間が 6 か月を超える場合は、その理由も記載。

B. セキュリティ機能要件ごとのテスト方針

B.1. テスト対象

- テスト対象の識別

  たとえば、TOE 内に同じ暗号アルゴリズムの複数の実装がある場合は、テスト対象となる実装をすべて記載。

  たとえば、SHA-256 を使用する RSASSA-PSS の署名検証機能のように複数の暗号アルゴリズムで構成される場合は、使用する暗号アルゴリズムをもれなく記載。

- テスト対象のサポート範囲

  たとえば、AES の GCM モードの IV の長さ、DRBG の reseed 機能の

有無のように暗号アルゴリズムの仕様のうち、テスト対象がサポートするパラメータ範囲・機能を記載。

B.2. テスト環境

- 使用する機器の構成

  たとえば、テスト用に改造したモジュールを使用する場合は、モジュールの名称と改造の方針、PC 等の代替環境を使用する場合は、そのハードウェア・ソフトウェア構成も記載。

B.3. テスト内容

- 実施するテスト内容の概要

  HCD-PP 1.0 の保証アクティビティに従ったテストが実施されることの説明を記載。 もし保証アクティビティで、追加のテストによる補足が求められている場合は、追加のテストの方法、または追加のテストが不要である根拠を記載。

  たとえば AES の GCM モードの IV の長さや、DRBG の予測困難性の有効・無効など、暗号アルゴリズムのテストにおける具体的な条件を記載。

B.4. 使用するテストツール

- テストに使用するツールの名称と用途

  用途は、“ネットワークパケットをキャプチャするために使用”等のツールの役割を具体的に記載。

なお、以下の HCD-PP 1.0 のセキュリティ機能要件については、必ず記載してください。

- ◆ すべての申請において記載
  - FCS_CKM.4　暗号鍵破棄
  - FCS_COP.1(a) 暗号操作（対称鍵暗号化/復号）
  - FCS_COP.1(b) 暗号操作（署名生成/検証）
  - FCS_RBG_EXT.1 拡張：暗号操作（乱数ビット生成）
- ◆ 以下の条件付き必須要件（附属書 B）が含まれる場合
  - FDP_DSK_EXT.1 拡張：ディスク上のデータ保護
  - FDP_FXS_EXT.1 拡張：ファクス分離
- ◆ 以下の選択ベース要件（附属書 D）が含まれる場合
  - FCS_IPSEC_EXT.1 拡張：選択された IPsec
  - FCS_TLS_EXT.1 拡張：選択された TLS

2.3 本制度における解釈

2.3.1 エントロピー源を第三者製品に依存している場合の補足事項

本項は開発者が第三者製品をエントロピー源として用いているために、エントロピー記述に記載すべき要求を満たせない場合の、本制度での取扱いについて規定しています。

なお、第三者製品を用いる場合でも、開発者が未処理のエントロピー量を取得でき、エントロピー記述に記載すべき要求を満たすことができる場合は、本項には該当しません。

本来、十分なエントロピーを供給できない場合には、暗号の安全性に問題が生じる可能性があることから、そのエントロピーの量は評価の主要な関心事項です。しかしながら、現在ではこれらのエントロピー源を第三者の製品に依存しているものが多く、またそれらの製品においてエントロピーの量についても客観的な評価・認証を取得していないものが存在します。

本制度では、第三者製品を用いる場合には、暗号モジュール試験及び認証制度（JCMVP）等で十分なエントロピーを提供すると確認された製品の使用を推奨するとともに、本制度におけるエントロピー評価の過渡期として暫定的に下記対応において評価の実施を可能とします。

1. <u>エントロピー記述</u> 【附属書 E】

   エントロピー記述では、第三者製品の製造元が提供する情報を元に開発者自身がどのように適切なエントロピー量を得ることができたかについて、少なくとも以下の内容を説明しなければなりません。

   ・設計記述
   - エントロピー源が含まれる第三者製品の識別、製造者
   - 第三者製品のエントロピー源が、どのように処理されて DRBG のシードとして入力されるか

   ・エントロピーの正当化
   - 第三者製品のエントロピー量[3]
   - エントロピー源から DRBG までの設計において、どうして十分なエントロピー量のシードが供給されるのか

[3] 第三者製品の仕様、その製品が準拠している標準、その製品のエントロピー量に関する論文等に基づいてエントロピー量を決定します。

・運用条件
  - 第三者製品のエントロピー源の動作保証条件[4]
・ヘルステスト
  - 第三者製品のエントロピー源のヘルステストの仕様[5]
  - エントロピー源の極端な偏りの発生等の異常時の仕様とそれに基づく TOE のふるまい

2. TOE 要約仕様 【セキュリティターゲット】

セキュリティターゲットでは、調達者が本製品のエントロピー源に関する評価がどのような情報に基づいてなされたのかを判断できる必要があります。開発者はエントロピー源に関して、セキュリティターゲットの TOE 要約仕様に少なくとも以下の情報を含めなければなりません。

・ エントロピー源が含まれる第三者製品の識別、製造者
・ エントロピー源のエントロピー量の仕様（製品仕様からの抜粋等）
・ エントロピー源の使用方法（SFR を満たすことの説明）

記述では、第三者製品の製造元が提供する情報を元に開発者自身がどのように適切なエントロピー量を得ることができたかを説明しなければなりません。

以下に TOE 要約仕様の例を示します。

> 256 ビット以上のエントロピーを収集するために、A 社の B チップを使用する。
> B チップの物理乱数生成器の仕様では、1 回の乱数ビット列のリクエストに対し、16 ビットの乱数を出力する。ここで、B チップは乱数生成機能を含めて CC 評価・認証されているという事実があり、B チップの物理乱数生成器は、その乱数出力について、8 ビットあたり 5 ビット以上の最小エントロピーを含むことが、B チップの ST の SFR の記述から分かっている。
> そこで、TOE は、B チップに対して乱数ビット列を 52 回リクエストし、得られた 52 個の 16 ビットの乱数ビット列を連結して 832 ビットのビット列とする。このビット列には 520(=832*5/8)ビットのエントロピーが含まれると想定する。
> このビット列を Entropy Input として HMAC-SHA-512 を使用した HMAC_DRBG に入力する。

[4] TOE の動作保証条件を満たせば、エントロピー源の動作保証条件を満たすことも記載してください。

[5] 第三者製品のヘルステストの仕様を、製造元から開示された範囲で記載してください。なお、第三者製品内で後処理された出力データの偏りを第三者製品外から監視するようなヘルステストを行う場合は、後処理の内容に注意してください。後処理に DRBG が使われている場合、後処理されたデータの偏りを監視しても異常を検知できるとは限りません。

2.3.2　暗号モジュール試験及び認証制度の活用について

本項では、HCD-PP 1.0 に基づく暗号アルゴリズムの適切性を評価するにあたり、暗号モジュール試験及び認証制度（JCMVP）の確認結果の活用方針を規定します。

IPA は、暗号モジュールが正しく暗号アルゴリズムを実装していることを国際的な基準[6] に従って確認する JCMVP を運用しており、JCMVP が適切かつ厳密に実施されていることを保証する立場にあります。このことから、IT セキュリティ評価及び認証制度の評価において JCMVP の確認結果を参照し根拠とすることを許容します。

ただし、確認された暗号アルゴリズム実装が評価対象の各セキュリティ機能のどの部分にどのように実装されるかを評価し、JCMVP の確認結果を適用できることを保証するのは評価者の責務となります。

2.3.3　FDP_DSK_EXT.1 に関連する時限的措置について

FDP_DSK_EXT.1 では、FDE EE cPP に適合した現地交換可能な自己暗号化不揮発性ストレージデバイス（SED）の使用を選択することができます。

しかし、2018 年 5 月現在、FDE EE cPP に適合した SED の製品数が限られていることから、本制度では以下の条件において JCMVP で認証された SED で代替することを許容します。

なお、本措置の適用期間については市場動向等により決定するものとします。本措置の終了については事前に JISEC のホームページにより通知します。

1. 代替して使用可能な SED
   - JCMVP で認証されたハードディスク等の現地交換可能な不揮発性ストレージデバイス。 ただし、保存するデータの暗号化機能が認証の範囲に含まれていること。

2. ST の記載
   - TSS に以下を明記すること。
     ・JCMVP の認証番号
     ・FCS_KYC_EXT.1 で求められる鍵チェインの終端が HCD と SED の境界における BEV であること

[6] ISO/IEC 18367:2016。JCMVP、北米 CAVP で実施している暗号アルゴリズムの適合試験の内容を基に作成された基準。

3. TOE の評価

- テストに対する保証アクティビティ（962 段落～966 段落）は実施しなくてもよい。

2.3.4 FCS_RBG_EXT.1 のテストに関連する措置について

FCS_RBG_EXT.1 のテストに関する記述は、北米 CAVP の“The NIST SP 800-90A Deterministic Random Bit Generator Validation System (DRBGVS)”の古い仕様に基づいています。適切な参照実装を用いたテストの結果を活用するという観点から、DRBGVS の最新の仕様[7]に適合するように、HCD-PP 1.0 の 277 段落の 1 文目及び 2 文目の記述を次の記述で代替することを許容します。

> If the RBG has prediction resistance enabled, each trial consists of the following functions called in sequence: (1) instantiate DRBG, (2) generate `ReturnedBitsLen` random bits, (3) generate `ReturnedBitsLen` random bits, (4) uninstantiate. Here `ReturnedBitsLen` denotes the number of returned bits from each call to the generate function. The evaluator verifies that the `ReturnedBitsLen` random bits in step (3) is the expected value.

また、HCD-PP 1.0 の 278 段落の 1 文目及び 2 文目の記述を次の記述で代替することを許容します。

> If the RBG does not have prediction resistance, each trial consists of the following functions called in sequence: (1) instantiate DRBG, (2) reseed, (3) generate `ReturnedBitsLen` random bits, (4) generate `ReturnedBitsLen` random bits, (5) uninstantiate. Here `ReturnedBitsLen` denotes the number of returned bits from each call to the generate function. The evaluator verifies that the `ReturnedBitsLen` random bits in step (4) is the expected value.

[7] DRBGVS の Update Log の 2/14/13 の記述が該当します。JCMVP の「暗号アルゴリズム実装試験仕様書 -乱数生成器-(ATR-01-E)」も DRBGVS の最新の仕様に対応するように見直されています。

2.3.5 FCS_IPSEC_EXT.1.1 に関する措置について

HDC-PP 1.0 の 1126 段落から 1131 段落の FCS_IPSEC_EXT.1.1 では、RFC4301 で指定されたとおりに IPSec が実装されていることを求めており、保証アクティビティでは、SPD の DISCARD、BYPASS、PROTECT のすべてを管理者が設定できることが前提となっています。しかし、評価対象である複合機では、その利用方法において、必ずしも BYPASS を必要とはしません。

そこで、本制度では、HCD-PP 1.0 の 1126 段落から 1131 段落を以下で代替することを許容します。

FCS_IPSEC_EXT.1.1 The TSF shall implement the IPsec architecture as specified in RFC 4301.

Application Note:

RFC 4301 calls for an IPsec implementation to protect IP traffic through the use of a Security Policy Database (SPD). The SPD is used to define how IP packets are to be handled: PROTECT the packet (e.g., encrypt the packet), BYPASS the IPsec services (e.g., no encryption), or DISCARD the packet (e.g., drop the packet). The SPD can be implemented in various ways, including router access control lists, firewall rulesets, a "traditional" SPD, etc. Regardless of the implementation details, there is a notion of a "rule" that a packet is "matched" against and a resulting action that takes place.

While there must be a means to order the rules, a general approach to ordering is not mandated, as long as the SPD can distinguish the IP packets and apply the rules accordingly. There may be multiple SPDs (one for each network interface), but this is not required.

Assurance Activity:

TSS:

The evaluator shall examine the TSS and determine that it describes what takes place when a packet is processed by the TOE, e.g., the

algorithm used to process the packet. The TSS describes how the SPD is implemented and the rules for processing both inbound and outbound packets in terms of the IPsec policy. The TSS describes the rules that are available and the resulting actions available after matching a rule. The TSS describes how those rules and actions form the SPD in terms of the BYPASS (e.g., no encryption), DISCARD (e.g., drop the packet) and PROTECT (e.g., encrypt the packet) actions defined in RFC 4301.

As noted in section 4.4.1 of RFC 4301, the processing of entries in the SPD is non-trivial and the evaluator shall determine that the description in the TSS is sufficient to determine which rules will be applied given the rule structure implemented by the TOE. For example, if the TOE allows specification of ranges, conditional rules, etc., the evaluator shall determine that the description of rule processing (for both inbound and outbound packets) is sufficient to determine the action that will be applied, especially in the case where two different rules may apply. This description shall cover both the initial packets (that is, no SA is established on the interface or for that particular packet) as well as packets that are part of an established SA.

Operational Guidance:

The evaluator shall examine the guidance documentation to verify it instructs the Administrator how to construct entries into the SPD that specify a rule for processing a packet. The description includes all three cases - a rule that ensures packets are encrypted/decrypted, dropped, and flow through the TOE without being encrypted. The evaluator shall determine that the description in the guidance documentation is consistent with the description in the TSS, and that the level of detail in the guidance documentation is sufficient to allow the administrator to set up the SPD in an unambiguous fashion. This includes a discussion of how ordering of rules impacts the processing of an IP packet.

Test:

The evaluator uses the guidance documentation to configure the TOE to carry out the following tests:

a) Test 1: The evaluator shall configure the SPD such that there is a rule for dropping a packet, encrypting a packet, and (if configurable) allowing a packet to flow in plaintext. The selectors used in the construction of the rule shall be different such that the evaluator can generate a packet and send packets to the gateway with the appropriate fields (fields that are used by the rule - e.g., the IP addresses, TCP/UDP ports) in the packet header. The evaluator performs both positive and negative test cases for each type of rule (e.g. a packet that matches the rule and another that does not match the rule). The evaluator observes via the audit trail, and packet captures that the TOE exhibited the expected behavior: appropriate packets were dropped, allowed to flow without modification, encrypted by the IPsec implementation.

b) Test 2: The evaluator shall devise several tests that cover a variety of scenarios for packet processing. As with Test 1, the evaluator ensures both positive and negative test cases are constructed. These scenarios must exercise the range of possibilities for SPD entries and processing modes as outlined in the TSS and guidance documentation. Potential areas to cover include rules with overlapping ranges and conflicting entries, inbound and outbound packets, and packets that establish SAs as well as packets that belong to established SAs. The evaluator shall verify, via the audit trail and packet captures, for each scenario that the expected behavior is exhibited, and is consistent with both the TSS and the guidance documentation.

なお、本措置は、以下の NIAP のテクニカルデシジョンと同じ内容です。

Item	Title	Publication Date
TD0157	FCS_IPSEC_EXT.1.1 - Testing SPDs	2017/06/15

2.3.6 FCS_TLS_EXT.1.1 のテストに関する措置について

HCD-PP 1.0 の FCS_TLS_EXT.1.1 の 1226 段落項番 2.a. の TOE がサーバの場合のテストは、TLS_RSA_WITH_で始まる cipher suites にのみ適用可能であり、それ以外の cipher suites の動作を検証することはできません。

そこで、本制度では、HCD-PP 1.0 の 1226 段落項番 2.a. のテストを、以下で代替することを許容します。

> [Conditional: TOE is a server] Modify a byte in the data of the client's Finished handshake message, and verify that the server rejects the connection and does not send any application data.

なお、本措置は、以下の NIAP のテクニカルデシジョンのテストの変更部分と同じ内容です。

Item	Title	Publication Date
TD0474	Removal of Mandatory Cipher Suite in FCS_TLS_EXT.1	2019/12/04

3. 申請時の提出書類の確認について

本制度では、申請時に提出された ST、エントロピー記述、鍵管理記述、評価者テスト方針概要書に対し、本章に示す内容の確認を行います。

本確認は、申請時における品質確保を目的とした確認であり、網羅的な確認ではありません。最終的な保証については、評価において提出される評価証拠資料を基に評価機関によって判断されることに留意願います。

3.1 ST の確認事項

(1) TOE の範囲や特徴、想定の利用環境が、HCD-PP 1.0 の指定(1.3 節, 1.4 節)に従っている。

(2) SFR において、Errata で修正された依存性が適用されている。

(3) Exact Conformance であることへの明白な違反はない。

余計な環境のセキュリティ対策方針(HCD-PP1.0 に存在しない)は ST にない。

HCD-PP 1.0 で必須となっている SFR(条件付き必須要件も含む)がすべて ST にある。

余計な SFR(HCD-PP 1.0 に存在しない)は ST にない。

(4) エントロピー源を第三者製品に依存する場合に必要な記述がされている。

(5) 鍵管理記述と関係する部分が整合している。

FCS_KYC_EXT.1 の選択に合わせて以下の SFR が正しく選ばれている。

- FCS_COP.1(e), FCS_SMC_EXT.1, FCS_COP.1(f), FCS_KDF_EXT.1, FCS_COP.1(i)

3.2 エントロピー記述の確認事項

(1) FCS_RBG_EXT.1 で挙げられているエントロピー源とノイズ源がすべてエントロピー記述で扱われている。

(2) ランダム性の由来として、適切なノイズ源が使われている。

ノイズ源からエントロピーを得られることについての技術的な裏付けがある。

(3) 未処理(生の)データ(unprocessed (raw) data)をテスト目的で取得する方法が適切である。

(補足)ノイズ源からの出力を数値化したものが未処理(生の)データである。

(4) 運用条件が適切に記述されている。

(補足)運用条件としての温度、電圧、周波数、オプションの構成など、エントロピー量に影響を与え得る環境条件が、TOE の想定される利用環境と対応づけできることが適切性の 1 つの基準である。

(5) 乱数生成のためのシードが十分なエントロピー量を持つ。

エントロピー量のテストにおいて、運用条件の範囲で実施されている。

ノイズ源から乱数生成のためのシードを得るまでの処理において、ノイズ源から得られたエントロピー量が十分にシードに残る。

(6) ヘルステストの頻度や条件が適切であり、エントロピー源の異常が検出された場合の TOE のふるまいが記述されている。

3.3 鍵管理記述の確認事項

(1) 鍵チェイン全体の図と解説が記述されている。

(2) 現地交換可能な不揮発性ストレージの暗号化に関係する鍵等(DEK または BEV, KEK, 鍵材料)がすべて鍵管理記述で扱われている。

(3) 「現地交換可能な不揮発性ストレージデバイス」であることの理由が妥当である。

ストレージデバイスの実装方法の妥当性ではなく、理由が HCD-PP 1.0 の脚注 4(以下に引用)に基づいている。

A “Field-Replaceable Nonvolatile Storage Device” is any Field-Replaceable Unit (FRU) for which the primary purpose is to provide nonvolatile storage. This OSP does not apply to storage devices that are a non-field-replaceable component of a larger FRU that is not primarily used for storage.

(補足)「現地交換可能な不揮発性ストレージデバイス」については、ST に記載される場合もある。

(4) 鍵が適切に生成される。

(補足)特に非対称鍵には、満たすべき条件が多く存在する。それらの条件を満たすために、複雑な非対称鍵生成アルゴリズムが複数提示されており、SFR の選択を完了したとしても、依然として選択の自由度が存在する場合がある。

例えば、FCS_CKM.1(a)が参照する FIPS 186-4 では、FFC の鍵ペア、ECC の鍵ペアの生成について、必要なプライベート鍵のビット数分を乱数生成する方法と、必要なプライベート鍵のビット数より 64 ビット余計に乱数生成する方法の 2 つが規定されている。

FCS_CKM.1(a)が参照する NIST SP 800-56B からさらに参照される FIPS 186-4 では、RSA の鍵ペアに生成について、多数の選択肢を残している。

(5) 鍵等が適切に保護される。

保護されない状態(平文)で現地交換可能な不揮発性ストレージに保存されない。

(6) 鍵等の強度が適切である。

外部からの入力とエントロピー記述に記載されたエントロピー源が強度の由来となっている。

(補足)FCS_CKM.1(a)については、選択肢として残されている暗号アルゴリズムの標準のいずれも、非対称鍵の生成について、DRBG を用いた乱数生成を要求している。HCD-PP

1.0 の依存関係には表れていない、FCS_CKM.1(a)から FCS_RBG_EXT.1 への暗黙的な依存性が存在するという事情がある。

鍵チェインと整合する。

(補足)鍵チェインの中の処理の内容によっては、処理後に強度が小さくなる場合があることに注意する。

(7) 鍵等に関連する検証が適切に行われる。

TOE が鍵を使用するための条件として検証(利用者や機器の認証)が行われる場合、その認証が鍵の危殆化の要因とならない。(危殆化の例としては、認証に対するブルートフォースによりサブマスクとして使用されるパスワードの値が判明する。)

(補足)以下が検証に該当する。

- FCS_PCC_EXT.1, FCS_COP.1(h)の機能

(8) 鍵等が適切に破棄される。

すべての鍵等の保存場所の記述がある。

鍵等がどのような時に不要となりどのような方法で破棄されるかについて、鍵チェインおよび鍵等の保存場所と整合する。

(補足)保存場所に関わらず、現地交換可能な不揮発性ストレージの暗号化に関係する鍵等がすべて記述の対象となることに注意する。

3.4 評価者テスト方針概要書の確認事項

(1) 申請日からテストの終了の予定日までの期間が過度に長くない。

(補足) 合理的な理由がなくこの期間が 6 ヶ月を超える場合、何らかの準備不足が疑われる。

(2) 暗号アルゴリズムのテストにおいて、適切な参照実装(reference implementation)が使用される。

(補足)以下は適切な参照実装の例である。

- JCMVP で認められるツール(JCATT)
- CMVP で認められるツール

以降のセキュリティ機能要件に対しては、個別に評価者テスト方針の確認をする。

3.4.1 FCS_CKM.4

(1) テスト対象に抜けがない。

以下のすべてに該当する鍵と鍵材料がテスト対象となっている。

- 不揮発性ストレージに存在する
- 場所を指定して消去することが可能

(2) テスト環境とテストツールが適切である。

テスト対象の鍵または鍵材料の値を記録できる。

不揮発性ストレージの内容をダンプできる。

(3) ダンプする範囲が適切である。

ダンプする範囲が不揮発性ストレージの一部分である場合、その範囲が適切であることが明確にわかるようになっている。

3.4.2 FCS_COP.1(a)

(1) テスト対象に抜けがない。

通信の対称鍵暗号のすべての実装が対象になっている。

(補足) SFR の以下のエレメントが通信の対称鍵暗号の要件。

- FCS_IPSEC_EXT.1 内の FCS_IPSEC_EXT.1.4, FCS_IPSEC_EXT.1.6
- FCS_TLS_EXT.1 内の FCS_TLS_EXT.1.1
- FCS_SSH_EXT.1 内の FCS_SSH_EXT.1.4

(2) テスト環境とテストツールが適切である。

暗号機能の実装部分に、暗号アルゴリズム実装試験仕様書―共通鍵― (ATR-01-B)、AESAVS 等で指定されるデータを入出力できる。

3.4.3 FCS_COP.1(b)

(1) テスト対象に抜けがない。

署名生成/検証のすべての実装が対象になっている。

(補足) SFR の以下のエレメントが署名生成/検証の要件に該当する。

- FCS_IPSEC_EXT.1 内の FCS_IPSEC_EXT.1.10
- FCS_SSH_EXT.1 内の FCS_SSH_EXT.1.2
- FCS_TLS_EXT.1 内の FCS_TLS_EXT.1.1
- FPT_TUD_EXT.1 内の FPT_TUD_EXT.1.3

(2) テスト環境とテストツールが適切である。

暗号機能の実装部分に、暗号アルゴリズム実装試験仕様書―鍵確立手法― (ATR-01-F)、DSA2VS 等で指定されるデータを入出力できる。

3.4.4 FCS_RBG_EXT.1

(1) テスト対象に抜けがない。

SFR で挙げられた全ての DRBG がテストの対象になっている。

(2) テスト環境とテストツールが適切である。

DRBG に対してデータを入出力できる。

3.4.5 FDP_DSK_EXT.1

(1) テスト対象に抜けがない。

現地交換可能な不揮発性ストレージデバイスの領域(以下は除外される)がテスト対象となっている。

- FDE EE cPP 適合で認証済(または見込み)のストレージデバイス
- データの暗号化の機能が JCMVP で認証済(または見込み)のストレージデバイス
- 暗号化の対象とならないことが TSS に記載されている領域(暗号化で保護すべき情報が存在しないかどうか、鍵管理記述の内容にも注意する)

(2) テスト環境とテストツールが適切である。

利用者文書データと秘密の TSF データが書き込まれたストレージデバイスの領域から、データを読み取れる。

暗号化に使用された鍵と鍵材料を取得できる。

読み取ったデータを取得した鍵と鍵材料でテストツールによって復号できる。

(補足)暗号化の方法(セクタ単位、ブロック単位、ファイル単位)とデータを復号する方法の整合性に注意する。整合性がないと、復号ができない場合がある。

3.4.6 FDP_FXS_EXT.1

(1) テスト環境とテストツールが適切である。

データ通信が可能なモデムが使用される。

(補足)アナログ回線対応かデジタル回線対応かに注意。

(2) 追加のテストの内容(または追加のテストが不要であること)と、その理由が適切である。

(補足)例えば、FAX 通信のプロトコルが拡張されている場合に、拡張されたプロトコルに関するテストが必要となる。

3.4.7 FCS_IPSEC_EXT.1

(1) テスト環境とテストツールが適切である。

IP パケットをキャプチャして、IPsec のプロトコルとして解釈でき、それを改変して送信できる。

(補足)TOE が IPv4, IPv6 のどちらに対応しているか、または両方に対応しているかに注意する。TOE の対応状況に応じたテスト環境が必要。

(補足)FCS_IPSEC_EXT.1.5 で IKEv2 が選択される場合、NAT が可能な環境が必要。

3.4.8 FCS_TLS_EXT.1

(1) テスト環境とテストツールが適切である。

TCP の通信内容を TLS のプロトコルとして解釈でき、それを改変して送信できる。

(補足)TOE が IPv4, IPv6 のどちらに対応しているか、または両方に対応しているかに注意する。TOE の対応状況に応じたテスト環境が必要。

4. 評価に関する補足事項

4.1 評価報告書について

HCD-PP 1.0 では、PP 内に記載された保証アクティビティに基づいた評価を実施することが求められています。 したがって、評価報告書に記載する評価方法・基準には、HCD-PP 1.0 も記載してください。

さらに、本ガイドラインの「2.3 本制度における解釈」 のうち、「2.3.3 FDP_DSK_EXT.1 に関連する時限的措置について」のように、PP の保証アクティビティを変更する解釈を適用した場合は、本ガイドラインの識別と適用した解釈のセクション番号も記載してください。

本補足に該当する解釈：

- 2.3.3 FDP_DSK_EXT.1 に関連する時限的措置について
- 2.3.4 FCS_RBG_EXT.1 のテストに関連する措置について
- 2.3.5 FCS_IPSEC_EXT.1.1 に関する措置について
- 2.3.6 FCS_TLS_EXT.1.1 のテストに関する措置について