

「collaborative Protection Profile for Hardcopy Devices」適合の

認証申請と評価についてのガイドライン

第 1.3 版

目次

1	はじめに.....	3
1.1	対象とするプロテクションプロファイル	3
1.2	HCD-iTC テクニカルデシジョンの適用方針	4
1.3	用語.....	5
1.4	参照資料	6
2	認証申請について.....	7
2.1	提出書類	7
2.2	提出書類の補足事項	8
2.2.1	セキュリティターゲット	8
2.2.2	エントロピー記述	9
2.2.3	鍵管理記述	10
2.2.4	評価者テスト方針概要書.....	10
2.2.5	コンポーネントリスト	13
2.2.6	構成リスト	13
2.2.7	ガイダンス文書	13
3	評価について.....	14
3.1	評価方法の補足事項	14
3.2	暗号アルゴリズム試験の補足事項	14
3.2.1	JCMVP の活用について.....	14
3.2.2	テスト結果の再利用について	14
3.3	評価報告書の補足事項	16
3.3.1	評価基準.....	16
3.3.2	評価結果の報告方法	17
4	本制度における解釈	19
4.1	Root of Trust の暗号機能のテストに関する措置.....	19
4.2	FPT_KYP_EXT.1 (HCD0011 適用)に関する措置.....	20

改版履歴

版数	発行日	主な変更内容
1.0	2023/10/3	・新規作成
1.1	2024/6/3	・HCDcPP V1.0e に対応 ・Root of Trust の暗号機能のテストに関する措置を追加
1.2	2025/5/7	・HCD-iTC テクニカルデシジョンの適用方針を追加
1.3	2025/9/26	・FPT_KYP_EXT.1(HCD0011 適用)に関する措置を追加 ・3 章の記述改善

1 はじめに

本ガイドラインは、ハードコピーデバイスのプロテクションプロファイル (collaborative Protection Profile for Hardcopy Devices) に適合する製品の認証申請及び評価に対する IT セキュリティ評価及び認証制度 (JISEC、以下「本制度」という) の指針を示すものです。

1.1 対象とするプロテクションプロファイル

本ガイドラインは、以下の文書を対象としています。

表 1 対象文書

対象文書	名称	バージョン	本文書における略称
プロテクション プロファイル	collaborative Protection Profile for Hardcopy Devices	1.0e	[HCDcPP]
サポート文書	Supporting Document Mandatory Technical Document Evaluation Activities for collaborative Protection Profile for Hardcopy Devices	1.0e	[HCD SD]

1.2 HCD-iTC テクニカルデシジョンの適用方針

HCD-iTC から[HCDcPP]及び[HCD SD]に対するテクニカルデシジョン(以下、「TD」と言います。)が公開されています。

- 「Hardcopy Devices iTC Technical Decisions」の URL
<https://hcd-itc.github.io/TD/tech-dec.html>

JISEC では、HCD-iTC の TD 適用方針を以下に示します。

- 認証申請受付日に「Hardcopy Devices iTC Technical Decisions」のページに掲載されている TD のうち、[HCDcPP]及び[HCD SD]の該当するバージョンに対する TD は、原則全て適用してください。評価認証中に新たに公開された TD は、適用しても構いませんが、必須ではありません。

また、評価認証中に不具合が見つかった TD は適用を見合わせる場合があります。なお、適用及び適用しなかった TD の妥当性は、評価認証の合格によって承認されます。

申請者及び評価機関は、それぞれ以下のとおり対応してください。

- 申請者
適用する TD のリストを ST に記載してください。記載方法の詳細は 2.2.1.1.1 節を参照してください。
- 評価機関
ST の記載の有無にかかわらず、該当するすべての TD のリストを評価報告書に記載し、それらの適用/非適用の正当化を行ってください。記載方法の詳細は 3.3.1 節を参照してください。

1.3 用語

本ガイドラインで用いる用語を表 2 に示します。

表 2 用語

語句	説明
CC	コモンクライテリア (Common Criteria)
ETR	評価報告書 (Evaluation Technical Report)
HCDcPP	ハードコピーデバイスのプロテクションプロファイル (collaborative Protection Profile for Hardcopy Devices)
HCD-iTC	ハードコピーデバイスの国際技術委員会 (Hardcopy Device International Technical Community)
JCMVP	暗号モジュール試験及び認証制度 (Japan Cryptographic Module Validation Program)
JISEC	IT セキュリティ評価及び認証制度 (Japan Information Technology Security Evaluation and Certification Scheme)
SAR	セキュリティ保証要件 (Security Assurance Requirement)
SFR	セキュリティ機能要件 (Security Functional Requirement)
ST	セキュリティターゲット (Security Target)
TD	テクニカルデシジョン (Technical Decision)
エントロピー記述	[HCDcPP]の Appendix E: Entropy Documentation and Assessment の要求を満たす評価証拠資料
コンポーネントリスト	[HCD SD]の 6.6.1.1. Evaluation Activity (Documentation)の要求を満たす評価証拠資料 (TOE 内のハードウェアとソフトウェアのコンポーネントのリスト)
鍵管理記述	[HCDcPP]の Appendix F: Key Management Document の要求を満たす評価証拠資料
構成リスト	CC のセキュリティ保証要件 ALC_CMS.1 の評価証拠資料
評価アクティビティ	[HCD SD]の Evaluation Activity

1.4 参照資料

本ガイドラインで参照する資料を表 3 に示します。

表 3 参照資料

	名称	本文書における略称
[1]	Common Criteria for Information Technology Security Evaluation, Version 3.1, revision 5, April 2017.	[CC]
[2]	Common Methodology for Information Technology Security Evaluation: Evaluation methodology Version 3.1 Revision 5, April 2017, CCMB-2017-04-004	[CEM]

2 認証申請について

本章では、申請者が HCDcPP 適合の認証申請のために用意し提出する書類と各書類への補足事項を示します。

なお、認証申請のための書類に関する本制度の解釈は、第 4 章を参照してください。

2.1 提出書類

認証申請では、「IT セキュリティ認証申請等のための手引」(CCM-02-A) 5.1 節に記載されている書類に加え、表 4 の書類の提出を必要とします。

表 4 の書類に関する注意点は以下のとおりです。

- 各書類の記載事項および注意事項は、2.2 節に示します。
- 電子媒体で提出してください。提出時は、ファイルリストもしくはフォルダ・ファイル名等により、各書類が提出されていることを明確にしてください。
- 書類の提出のタイミングは、認証申請時と評価報告時の書類があります。なお、書類を更新した場合に再提出が必要な書類があります。
- 本制度では提出された各書類を認証申請及び評価の妥当性確認のためだけに使用します。JISEC の認証製品リストの Web ページ等による公開は行いません。

表 4 追加で提出が必要な書類

提出タイミング	書類名	更新時の再提出	公開の有無
認証申請時	・エントロピー記述	必要	非公開
	・鍵管理記述		
	・評価者テスト方針概要書	不要	
評価報告時	・コンポーネントリスト	必要	非公開
	・構成リスト		
	・ガイダンス文書		

2.2 提出書類の補足事項

本節では提出書類(セキュリティターゲット及び表 4)の記載事項、注意事項等を示します。

2.2.1 セキュリティターゲット

2.2.1.1 適合主張

2.2.1.1.1 PP 主張

以下の記載例のように適合する PP として、[HCDcPP]の名称とバージョンを記載します。

また、適用する TD のリストも記載します。リストには[HCDcPP]と[HCD SD]の適用する TD の ID 及びタイトルを記載してください。

なお、1.2 節で示したように、認証申請受付日に公開されている TD は原則全て適用してください。

記載例：

PP 主張

本 ST が適合する PP は下記のとおり。

名称： collaborative Protection Profile for Hardcopy Devices

バージョン： 1.0e

HCD-iTC の以下の Technical Decision を適用する。

ID	タイトル
HCD0010	Clarification on FPT_SBT_EXT.1 Root of Trust

2.2.1.1.2 適合根拠

以下の記載例のように [HCDcPP] の **2. CC Conformance Claims** の “Conformance to this Protection Profile” で示されている規則に適合していることを [HCDcPP] の用語で記載します。

さらに TOE の TOE 種別が、[HCDcPP] 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, Copying, Configuration, Auditing, Verifying firmware/software updates, Verifying HCD function

- Conditionally Mandatory Uses

Sending PSTN faxes, Receiving PSTN faxes, Storing and retrieving Documents, Nonvolatile Storage Devices

- Optional Uses

Image Overwrite, Wipe Data

2.2.2 エントロピー記述

エントロピー記述とは、評価対象製品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に、開発者が提供する資料です。エントロピー記述に記載すべき要求事項は[HCDcPP]の **Appendix E** に記述されています。

この **Appendix E** では、開発者がエントロピー源の未処理のデータの最小エントロピーを測定することが求められています。ただし、エントロピー源として第三者製品のエントロピー製品を使用しており、かつ、開発者がエントロピー源の未処理のデータを取得できない場合には、開発者が最小エントロピーを推定することが許容されています。その場合には、最小エントロピーの推定値(estimate)と推定内容(assumption)をエントロピー記述及びセキュリティターゲットに記載することが求められています。

最小エントロピーを推定した場合、セキュリティターゲットの TOE 要約仕様には、以下の内容を含めて記載ください。

- エントロピー源が含まれる第三者製品の製造者と識別
- エントロピー源の最小エントロピーの推定値
- 推定の根拠

例えば、最小エントロピーを推定した根拠となる、第三者製品の仕様、その製品が準拠している標準、または、その製品のエントロピー量に関する論文等。

2.2.3 鍵管理記述

鍵管理記述とは、評価対象製品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に、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、[HCDcPP]の Appendix F 及び[HCD SD]の SFR 毎の評価アクティビティ「KMD」の項目に記載されています。

2.2.4 評価者テスト方針概要書

[HCD SD]の評価アクティビティで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、その概要を評価者テスト方針概要書として提出いただきます。

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は、予定期間内に[HCD SD]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

テスト開始と終了の予定日を記載してください。もし、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、その理由も記載してください。

B. セキュリティ機能要件ごとのテスト方針

表5に示すセキュリティ機能要件について、以下のB.1～B.4を記載してください。

B.1 テスト対象

- TOE の識別

テストを行うすべての TOE 機種種の識別を記載してください。

もし TOE に複数の TOE 機種が含まれ、その一部の機種を選択してテストを行う場合は、テストに用いる TOE 機種を選択した根拠も記載してください。（例えば、言語の違い、印刷速度の違い、機種名の違い、搭載するオプションの違い、その他、を考慮してそれぞれの代表機種を選択）

- 暗号アルゴリズム名と実装の識別

暗号アルゴリズムのテストは、暗号アルゴリズムの名称と、その暗号アルゴリズムを含む暗号実装の識別（名称とバージョン等）を記載してください。同じ

暗号アルゴリズムで、複数の実装をテストする場合は、テスト対象のすべての実装の識別を記載してください。

B.2 テスト環境

- 使用する機器の構成

テストに使用する機器の構成を記載してください。

もし、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内容、PC 等の代替環境を使用する場合はハードウェア・ソフトウェア構成を記載してください。

B.3 テスト内容

- 実施するテスト内容の概要

[HCD SD]の評価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してください。

もし評価アクティビティで、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してください。

暗号アルゴリズムのテストの場合は、例えば AES の GCM モードであれば IV の長さ、DRBG であれば予測困難性の有効・無効のように、暗号アルゴリズムテストの具体的な条件を記載してください。

B.4 使用するテストツール

- テストに使用するツールの識別と用途

使用するツールの識別と用途を記載してください。識別はツール名称とバージョン等、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してください。

表 5 テスト方針概要書に記載が必要なセキュリティ機能要件

- すべての申請において記載
 - ・FCS_CKM.1/SKG Cryptographic key generation (Symmetric Keys)
 - ・FCS_CKM.1/AKG Cryptographic Key Generation (for asymmetric keys)
 - ・FCS_CKM.2 Cryptographic Key Establishment
 - ・FCS_CKM.4 Cryptographic key destruction
 - ・FCS_COP.1/DataEncryption Cryptographic Operation (Data Encryption/Decryption)
 - ・FCS_COP.1/SigGen Cryptographic Operation (Signature Generation and Verification)
 - ・FCS_COP.1/Hash Cryptographic Operation (Hash Algorithm)
 - ・FCS_RBG_EXT.1 Cryptographic Operation (Random Bit Generation)
 - ・FPT_SBT_EXT.1 Secure Boot
- 以下の Conditionally Mandatory Requirements が含まれる場合
 - ・FDP_DSK_EXT.1 Protection of Data on Disk
 - ・FDP_FXS_EXT.1 Fax separation
- 以下の Optional Requirements が含まれる場合
 - ・FPT_WIPE_EXT Data Wiping
 - ・FCS_TLSC_EXT.2 TLS Client support for mutual authentication
 - ・FCS_TLSS_EXT.2 TLS Server support for mutual authentication
 - ・FCS_DTLSC_EXT.2 DTLS Client support for mutual authentication
 - ・FCS_DTLSS_EXT.2 DTLS Server support for mutual authentication
- 以下の Selection-Based Requirements が含まれる場合
 - ・FCS_COP.1/StorageEncryption Cryptographic operation (Data Encryption/Decryption)
 - ・FCS_COP.1/KeyWrap Cryptographic operation (Key Wrapping)
 - ・FCS_COP.1/KeyEnc Cryptographic operation (Key Encryption)
 - ・FCS_COP.1/KeyTransport Cryptographic operation (Key Transport)
 - ・FCS_IPSEC_EXT.1 IPsec selected
 - ・FCS_TLSC_EXT.1 TLS Client Protocol without mutual authentication
 - ・FCS_TLSS_EXT.1 TLS Server Protocol without mutual authentication
 - ・FCS_DTLSC_EXT.1 DTLS Client Protocol without mutual authentication
 - ・FCS_DTLSS_EXT.1 DTLS Server Protocol without mutual authentication
 - ・FCS_SSHC_EXT.1 SSH Client
 - ・FCS_SSHS_EXT.1 SSH Server
 - ・FCS_COP.1/KeyedHash Cryptographic Operation (Keyed Hash Algorithm)
 - ・FCS_PCC_EXT.1 Cryptographic Password Construct and Conditioning
 - ・FCS_KDF_EXT.1 Cryptographic Key Derivation
 - ・FCS_COP.1/CMAC Cryptographic Operation (for cipher-based message authentication)
 - ・FIA_X509_EXT.1 X.509 Certificate Validation
 - ・FIA_X509_EXT.2 X.509 Certificate Authentication
 - ・FIA_X509_EXT.3 X509 Certificate Requests

2.2.5 コンポーネントリスト

コンポーネントリストは、脆弱性の評価のために開発者が提供する TOE 内のハードウェアとソフトウェアのコンポーネントのリストです。

コンポーネントリストに記載する内容は、[HCD SD]の 6.6.1.1. Evaluation Activity (Documentation)に記述されています。

2.2.6 構成リスト

構成リストは、ALC_CMS.1 の評価において開発者が提供する証拠資料です。構成リストに記載すべき対象は、CEM の ALC_CMS.1-1(以下の抜粋)のとおりです。

- a) the TOE itself;
- b) the evaluation evidence required by the SARs in the ST.

ただし、上記の b 項には、[HCD SD]の評価アクティビティで要求されている評価資料(エントロピー記述、鍵管理記述、コンポーネントリスト等)も含まれます。

2.2.7 ガイダンス文書

ガイダンス文書は、TOE に附属する取扱説明書です。以下の評価で必要な内容を記載したガイダンス文書を提出してください。

- [CEM]および[HCD SD]の ADV と AGD クラスの評価で使用するガイダンス文書
- [HCD SD]の評価アクティビティの Guidance Documentation の評価に使用するガイダンス文書

もし、TOE に日本向けと海外向けのように複数の同等の内容のガイダンス文書が含まれている場合、いずれかひとつのガイダンス文書のみを提出することが可能です。ただし、その場合は、選択した根拠と、他のセットとの差異の概要を記載した資料も提出してください。

3 評価について

本章では、評価者が HCDcPP 適合の評価を実施する際の補足事項を示します。

なお、評価に関する本制度の解釈は、第 4 章を参照してください。

3.1 評価方法の補足事項

HCDcPP 適合の評価は、[HCD SD]の記述に従って実施します。

[HCD SD]では、[HCD SD]に記述されている各種の評価アクティビティに加えて、[CEM]に記述されている評価も要求されています。ただし、ADV_FSP.1, AVA_VAN.1 では、[CEM]ワークユニットで実施すべき評価内容が変更されていますので注意してください。

3.2 暗号アルゴリズム試験の補足事項

本節では、[HCD SD]に記述されている、暗号アルゴリズムの実装の適切性を確認するテストの評価アクティビティに関する補足事項を示します。

3.2.1 JCMVP の活用について

暗号アルゴリズム実装の適切性の確認のためのテストは、TOE の評価中に評価者が所定のテストを実施する他に、IPA が運用する「暗号モジュール試験及び認証制度（JCMVP）」の暗号アルゴリズム確認の結果を根拠とすることを許容します。JCMVP は、暗号モジュールが暗号アルゴリズムを正しく実装していることを国際的な基準¹ に従って確認する制度であり、JCMVP が適切かつ厳密に実施されていることを、本制度と同様に IPA が管理しています。そのため本制度下で実施される評価者テストと同等とみなします。

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。

3.2.2 テスト結果の再利用について

暗号アルゴリズムを実装したモジュールは、TOE の複数の機種、あるいは、異なる TOE で、同一の実装が用いられる場合があります。

そのような場合でも、原則として、それぞれの TOE 機種の実装の適切性を確認するため、[HCD SD]が求める方法で、それぞれの TOE 機種をテストする必要があります。

¹ 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。

しかし、以下の条件を満たす場合、ある TOE 機種のテスト結果を、他の TOE 機種のテスト結果として再利用することを許容します。

- **テスト結果を再利用するための条件**

テスト結果を再利用する TOE における暗号アルゴリズムの実装が、以下のすべての条件を満たすこと。ただし、実装がハードウェアの場合は、1 項と 2 項の双方を満たすことによりテスト結果の再利用を許容する。

1. テスト済みの実装と識別(名称とバージョン等)が同一であること
2. テスト済みの実装と同一の実装が呼び出され、動作していること
3. テスト済みの実装とバイナリコードが同一であること
4. テスト済みの実装の動作環境と同一であること

なお、テスト結果を再利用する場合は、評価アクティビティの評価結果の報告に上記の再利用するための条件に対応する以下の内容も明記してください。

- **テスト結果を再利用する場合の報告内容**

1. テスト済みの実装の識別とテスト結果を再利用する実装の識別
2. テスト結果を再利用する TOE において、テスト済みの実装と同一の実装が呼び出され、動作していることの根拠
3. テスト済みの実装とテスト結果を再利用する実装のバイナリレベルで同一であることの根拠(たとえば、ハッシュ値)
4. テスト済みの実装とテスト結果を再利用する実装の動作環境(具体的なプロセッサや OS 等)

3.3 評価報告書の補足事項

評価報告書に関する補足事項を以下に示します。

3.3.1 評価基準

3.1 節で示したように[HCDcPP]では、[HCD SD]に記載された評価も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、[CC]と[CEM]に加えて[HCD SD]も記載してください。

記載例：

評価基準等

1. Common Criteria for Information Technology Security Evaluation, Version 3.1 Release 5
2. Common Methodology for Information Technology Security Evaluation, Version 3.1 Release 5
3. Supporting Document Mandatory Technical Document Evaluation Activities for collaborative Protection Profile for Hardcopy Devices, Version 1.0e

さらに、認証申請受付日に HCD-iTC で公開されている、[HCDcPP]及び[HCD SD]の当該バージョンに対する全ての TD のリストを記載してください。リストには、ST に記載されていない TD も含める必要があることに注意してください。また、認証申請受付日以降に公開され、適用した TD があれば、リストに追加してください。

リストには、それぞれの TD の ID、タイトル、適用/非適用、及び適用しない場合の正当化根拠を記載してください。

記載例：

HCD-iTC の Technical Decision の適用有無とその正当化根拠は以下のとおり。

ID	タイトル	適用 (Y/N)	正当化根拠
HCD0010	Clarification on FPT_SBT_EXT.1 Root of Trust	Y	
⋮	⋮	⋮	⋮
HCD00xx	Clarification on ⋯	N	当該 SFR は選択されていない。

また、本ガイドラインの「4 本制度における解釈」の解釈を適用した場合には、本ガイドラインの識別、及び、適用した解釈の項目の識別（例えば、「4.1 Root of Trust の暗号機能のテストに関する措置」）も記載してください。

3.3.2 評価結果の報告方法

評価報告書には、以下の3種類の報告を記述してください。なお、以下の「AVA 評価の“public-facing report”」と「評価アクティビティの評価結果の報告」は、公開の可能性を考慮して、別冊あるいは専用の節等に記述するなどして、他の非公開の評価とは明確に分離して記載してください。

A. [CEM]の評価結果の報告

[CEM]の評価結果は、[CEM]の 8.5.5.3.4 節のとおり記述し報告してください。ただし、AVA_VAN.1 のように[HCD SD]で報告の要件が示されている場合は、その要件も満たすように報告してください。

B. AVA 評価の“public-facing report”

AVA_VAN.1 では、通常の評価報告に加えて、秘密情報を含まない“public-facing report”も求められています。“public-facing report”は、[HCD SD] の A.3. Reporting において求められている報告内容を記述してください。

なお、公開の可能性を考慮して、認証者だけでなく調達者にも理解できるように報告を記述してください。

C. 評価アクティビティの評価結果の報告

[HCD SD]の評価アクティビティの評価結果（評価アクティビティには、SFR 毎と保証コンポーネントに対するものがあります）は、評価が再現可能なように以下を満たすように記述してください。

- [HCD SD]の評価アクティビティの個々の要求事項と評価結果との対応が容易に判別できること
- TSS、KMD、Guidance Documentation に関する評価アクティビティについては、評価証拠資料名とその章・節番号などにより、評価証拠資料の評価箇所を特定するための情報を含めること、ただし、評価証拠資料の記述の copy & paste はしないこと

なお、公開の可能性を考慮して、認証者だけでなく調達者にも理解できるように報告を記述してください。また、報告内容に他の非公開の評価結果を極力参照しないようにしてください。

評価アクティビティの報告内容の例を以下に示します。

[HCD SD]の評価アクティビティの報告内容の例：

2. TSS の評価アクティビティの評価結果

...

2.6.5 FPT_TUD_EXT.1 Trusted Update

評価アクティビティ

The evaluator shall check to ensure that the TSS contains a description of mechanisms that verify software for update when performing updates, which is consistent with the definition of the SFR.

評価結果

[ST] “7.1 Trusted Update”には・・・

評価アクティビティ

The evaluator shall check to ensure that the TSS identifies interfaces for administrators to obtain the current version of the TOE as well as interfaces to perform updates.

評価結果

[ST] “7.1 Trusted Update”には・・・

2.6.6. FTA_SSL.3 TSF-initiated termination

...

4 本制度における解釈

本章では、本制度における[HCDcPP]または[HCD SD]に関する解釈を示します。

HCD-iTC による解釈 (Technical Decision) の適用方針については 1.2 節を参照してください。

4.1 Root of Trust の暗号機能のテストに関する措置

[HCD SD]では、SFR で指定された各種暗号アルゴリズムについて、評価者テストを要求しています。しかし、Root of Trust 内に実装された暗号機能については、例外的に以下のように記述されています。

Note: Testing of cryptographic functions implemented in the Root of Trust for Secure Boot (FPT_SBT_EXT.1) may not be feasible and independent testing may not be available. In this situation, contact the CC Scheme.

本節は、上記の注釈(以下、「Root of Trust の注釈」と言います。)に該当する場合の本制度での取り扱いについて規定しています。

本制度では、[HCD SD]の Root of Trust の注釈に該当する場合、以下の対応が必要になります。

- セキュリティターゲットへの Root of Trust の情報の記載
セキュリティターゲットの TOE 要約仕様に、Root of Trust の製品または実装を特定するための情報(たとえば、製品を一意に識別する情報)を明記してください。
- Root of Trust に関する評価と報告
評価者は、TOE を検査して以下を確認し、その結果を評価報告書で報告してください。
 - ・TOE 要約仕様に記載されている Root of Trust を特定する情報と、TOE に実装されている Root of Trust が一致していること
 - ・該当する暗号機能が TOE の Root of Trust に実装されていること(注: 特定された Root of Trust に関する仕様等の確認でも良い。ただし、Root of Trust の製品または実装の仕様等において何らかのコンフィグレーションが存在する場合には、TOE への適用の仕方も含めて確認すること。)

- ・該当する暗号機能について、[HCD SD]で要求されているテストが実施できないこと

4.2 FPT_KYP_EXT.1 (HCD0011 適用)に関する措置

HCD iTC の TD(HCD0011)では、FPT_KYP_EXT.1 に関するアプリケーションノートに以下のように記述されています。

*In the case where a encrypted key is stored on media that is decrypted by a key stored in a protected storage device, the selection for **encrypting or wrapping a key that is encrypted or wrapped within a protected storage device using a key stored within that device** should be used. In this case, the key that the protected storage device generates and stores internally is considered to be the starting point of the key chain, so “the non-volatile memory where the key is stored on is located in a protected storage device” must also be selected as a means of protecting that key.*

Testing of cryptographic functions implemented in the protected storage device may not be feasible and independent testing may not be available. In this situation, contact the CC Scheme.

注：説明のため、一部を太字にしています。

本節は、上記のアプリケーションノート(以下、「HCD0011 のアプリケーションノート」と言います。)に対する本制度での解釈と取り扱いについて規定しています。

「HCD0011 のアプリケーションノート」では、該当する実装の場合、“*encrypting or wrapping a key that is encrypted or wrapped within a protected storage device using a key stored within that device*”を選択することを求めています。しかし、この選択肢を選択した場合、暗号アルゴリズムの SFR が指定されていないため、FCS_KYC_EXT.1 の 要 求 (FCS_COP.1/KeyWrap, FCS_COP.1/KeyEnc, FCS_COP.1/KeyTransport 等の中から選択しなければならない)と矛盾します。

そこで本制度では、「HCD0011 のアプリケーションノート」に該当する場合、以下のように対応してください。

- 鍵チェーンの範囲(FCS_KYC_EXT.1 と FPT_KYP_EXT.1 の矛盾の解消)

FCS_KYC_EXT.1 と FPT_KYP_EXT.1 の鍵チェーンは、原則同一であり、a protected storage device に保存された暗号鍵から、DEK を得るまでとなります。しかし、「HCD0011 のアプリケーションノート」を適用し”*encrypting or wrapping a key...*”を選択した場合、FCS_KYC_EXT.1 の鍵チェーンは、当該選択肢で復号された鍵から DEK までとします。

●TOE の実装

「HCD0011 のアプリケーションノート」を適用し”*encrypting or wrapping a key...*”を選択した場合、それに該当する暗号アルゴリズムと鍵長は、SFR の指定はありませんが、以下のとおりとします。

- 暗号アルゴリズム

FPT_KYP_EXT.1 の 本 来 の 選 択 肢 ”wrapped, as specified in FCS_COP.1/KeyWrap, or encrypted, as specified in FCS_COP.1/KeyEnc or FCS_COP.1/KeyTransport“に該当する暗号アルゴリズムでなければなりません。

- 鍵長

FCS_KYC_EXT.1 の要件”maintaining an effective strength of [selection: 128 bits, 256 bits]”に該当する鍵長でなければなりません。

●セキュリティターゲットの TOE 要約仕様の記載

セキュリティターゲットの TOE 要約仕様に以下を明記してください。

- (1) ”protected storage device”を特定するための情報(たとえば、製品を一意に識別する情報)
- (2) ”protected storage device”に実装されている上記の暗号アルゴリズムと鍵長(ただし、FCS_COP.1 の実装と誤解されないこと)

なお、「HCD0011 のアプリケーションノート」の”Testing of cryptographic functions...”については、上記の実装の場合、暗号アルゴリズムと鍵長に関する SFR の指定がないため、暗号アルゴリズムのテストは不要です。

以上