認 証 報 告 書

東京都文京区本駒込2丁目28番8号
独立行政法人情報処理推進機構
理事長　富田　達夫

原紙押印済

プロテクションプロファイル（PP）

申請受付日（受付番号）	令和3年10月12日（IT認証1797）
認証識別	JISEC-C0764
PPの名称	セキュア暗号ユニット搭載 シングルチップマイクロコントローラ プロテクションプロファイル
バージョン及びリリース番号	バージョン1.20
開発者	国立研究開発法人産業技術総合研究所
機能要件適合	CCパート2拡張
プロテクションプロファイル	他のPPへの適合主張なし
保証パッケージ	EAL1 及び追加の保証コンポーネントASE_SPD.1、ADV_ARC.1、ADV_FSP.2、ADV_TDS.1、ALC_FLR.1、AVA_VAN.2、AVA_SCU_EXT.1
ITセキュリティ評価機関の名称	株式会社 ECSEC Laboratory 評価センター

上記のPPについての評価は、以下のとおりであることを認証したので報告します。
令和4年9月30日

セキュリティセンター セキュリティ技術評価部
技術管理者　佐藤 眞司

評価基準等：「ITセキュリティ評価及び認証制度の基本規程」で定める下記の規格に基づいて評価された。

① 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 バージョン3.1 リリース5
② 情報技術セキュリティ評価のための共通方法 バージョン3.1 リリース5

評価結果：合格

「セキュア暗号ユニット搭載 シングルチップマイクロコントローラ プロテクションプロファイル、バージョン 1.20」は、独立行政法人情報処理推進機構が定めるITセキュリティ認証等に関する要求事項に従い、定められた規格に基づく評価を受け、所定の保証要件を満たした。

目次

1 全体要約

この認証報告書は、国立研究開発法人産業技術総合研究所が開発した「セキュア暗号ユニット搭載 シングルチップマイクロコントローラ プロテクションプロファイル、バージョン 1.20」（以下「PP[12]」という。）について株式会社 ECSEC Laboratory 評価センター（以下「評価機関」という。）が令和 4 年 6 月 17 日に完了した IT セキュリティ評価に対し、その内容の認証結果を申請者である国立研究開発法人産業技術総合研究所に報告するとともに、PP[12]に関心を持つ調達者や消費者に対しセキュリティ情報を提供するものである。

本認証報告書の読者は、本書と共に、対応する PP[12]を併読されたい。特に PP[12]が要求するセキュリティ機能要件、保証要件及びその十分性の根拠は、PP[12]において詳述されている。

本認証報告書は、PP[12]に適合した製品開発を行う開発者及び製品調達者を読者と想定している。本認証報告書は、PP[12]が適合する保証要件に基づいた認証結果を示すものであり、個別の IT 製品そのものを保証するものではないことに留意されたい。

1.1 評価PP

PP[12]が要求するセキュリティ機能の概要を以下に示す。詳細は 2 章以降を参照のこと。

1.1.1 保証パッケージ

PP[12]において要求される保証パッケージは、EAL1 及び追加の保証コンポーネント ASE_SPD.1、ADV_ARC.1、ADV_FSP.2、ADV_TDS.1、ALC_FLR.1、AVA_VAN.2、AVA_SCU_EXT.1 である。

また、PP[12]への適合を主張する PP、及び ST は正確適合を主張しなければならない。

1.1.2 PP概要

PP[12]は、セキュリティ機能を提供するセキュア暗号ユニット（Secure Cryptographic Unit:SCU）を搭載した組込み機器用途向けシングルチップマイクロコントローラ（マイコンと称す）に関わるセキュリティ要件を規定する。

PP[12]において、TOE は、SCU を搭載した組込み機器用途向けシングルチップマイコンである。SCU の概念図を図 1-1 に示す。SCU は、SCU 内に実装する暗号エンジンと、その暗号エンジンに対して、ソフトウェアゲート API を介してアクセスできるソフトウェアゲートとハードウェアゲートで構成される。TOE はシングルチップマイコン内にメモリを搭載したメモリ内蔵型を想定する。メモリ外付け型は本認証の対象としない。

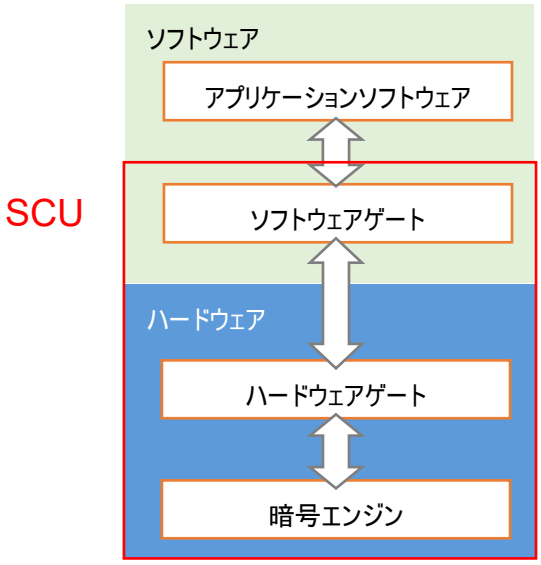

図 1-1　SCUの概念図

TOE は一般的に SoC で配付される。メモリ内蔵型である本 TOE の場合は、単一のダイに実装してパッケージにする場合がある。この SoC が、組込み機器の用途に必要なさまざまな回路を実装している基板にはんだ付けされ、組込み機器の筐体に収められる。

図 1-2 に TOE の構成例を示す。青線は TOE の物理的範囲を示し、SCU を搭載したマイコンの構成を示している。赤線は TOE の論理的境界を示す。図 1-2 では、アプリケーションソフトウェアは、論理的に TOE の外側に位置し、ソフトウェアゲートとハードウェアゲートを介して暗号機能を使用する。アプリケーションソフトウェアは TOE の不揮発メモリに格納する。

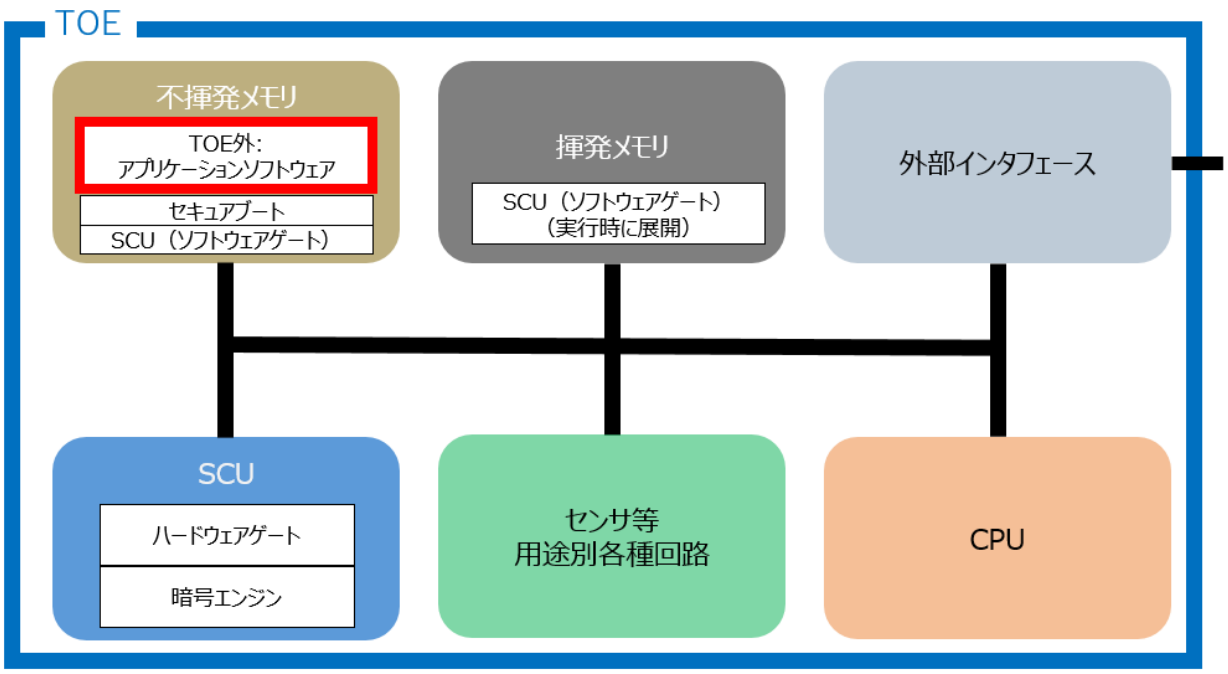

図 1-2　TOEの構成例

ソフトウェアゲートとハードウェアゲートは、暗号機能に対するアクセス制御のためのメカニズムであり、それぞれアクセス制御機能のソフトウェアパートとハードウェアパートである。アプリケーションソフトウェアによる暗号機能へのアクセスは、正当かつ許可されるべきアクセスであるが、それ以外のアクセスは拒否しなければならない。TOE のアクセス制御メカニズムは、この両者を区別するために実施される。

ソフトウェアゲートとハードウェアゲートは、次のように動作する。

ハードウェアゲートは、自らに向けられた暗号操作コマンドデータを受け取り、そのたびに、ハードウェアゲートの内部状態を遷移させる。あるコマンドデータを受けたときの内部状態は、前の内部状態と現在の入力(暗号操作コマンドデータ)によって一意に決まる。もしハードウェアゲートが内部状態の正しい遷移データを知っていれば、現在の入力による内部状態の遷移結果を正しい遷移データと比較し、入力されたコマンドデータが正当なものかどうかを判定できる。

ソフトウェアゲートは、ハードウェアゲートの状態遷移を管理する情報を提供する。暗号機能にアクセスするすべてのパターンは、開発者があらかじめ予測した独自のものであり、開発者しか知らない。このアクセスパターンに伴うハードウェアゲートの内部状態遷移をあらかじめ計算し、ソフトウェアゲートに格納する。ソフトウェアゲートは、アプリケーションソフトウェアから暗号機能へのアクセスコマンドデータを受けると、そのアクセスコマンドデータとハードウェアゲートの次の内部状態遷移データを共にハードウェアゲートへ転送する。ハードウェアゲート

は、渡された内部状態遷移データと、同時に受信したコマンドデータによる内部状態遷移結果と照合し、両者が一致すれば、受信したコマンドデータを正当なものと判断する。ハードウェアゲートへ渡す内部状態遷移データが格納されているソフトウェアゲートは、TOE 製造時に TOE の不揮発メモリに格納されるため、開発者以外は生成できない。つまり、開発者があらかじめ計算した暗号機能へのアクセスパターンは実行されるが、エミュレータなどがそれ以外のパターンで暗号機能を使用しようとしても、内部状態遷移データを提供できず、ハードウェアゲートによってアクセスを拒否される。ソフトウェアゲートにあらかじめ埋め込む内部状態遷移データを暗号によって保護する場合、実装するアルゴリズムは PP[12]の 7 章から選択する。

TOE は、SCU のセキュリティ機能を保護する自己保護機能を持つ。また、TOE は、RoT となる HGK と、外部エンティティが TOE を一意に識別する情報とを、SCU 内に格納する。TOE 開発者の責任において、十分なエントロピーを持つ乱数によって HGK を生成する。

TOE は、TSF データの機密性をハードウェアの自己保護機能によって保護する。TOE は、TOE の不揮発メモリに格納する利用者データを TOE の暗号機能で保護する。TSF データは、HGK、鍵ストレージを復号する鍵、鍵ストレージの完全性を検証するデータ、ソフトウェアゲートの完全性を検証するためのデータ、IV、内部状態遷移データ、チップ ID である。

TOE のセキュアブートプログラムは、起動時にソフトウェアゲートとアプリケーションソフトウェアを揮発メモリに展開し、ソフトウェアゲートの完全性を検証し、アプリケーションソフトウェアの完全性（オプションで真正性）を検証する。また TOE は、アプリケーションソフトウェアのアップデート時に、アプリケーションソフトウェアの完全性と真正性を検証し、検証に成功したのちにアップデートする。ここで真正性とは、正当なアプリケーションソフトウェア開発者が開発したアプリケーションソフトウェア、という特性を言う。

1.1.3 セキュリティ機能概要

PP[12]が TOE に要求するセキュリティ機能を次に示す。

TOE は、SCU の暗号機能を、ソフトウェアゲートを介してアプリケーションソフトウェアに提供する。アプリケーションソフトウェアは暗号機能を利用した通信プロトコルやメモリ暗号化、識別認証といったセキュリティ機能を実装する。

TOE は暗号機能と、暗号機能を利用したセキュリティ機能を保護する自己保護機能を実装する。

TOE は以下の主要なセキュリティ機能を持つ。この機能はベースライン機能であり、TOE の必須要件である。

- 暗号機能へのアクセス監視：ソフトウェアゲートとハードウェアゲートの協調により、暗号機能の不正な利用を検知して対応する機能
- 自己保護：SCU 動作中の放射電磁波及び消費電力に意図せず情報が漏洩し、攻撃者に有益な情報が暴露されることを妨げる機能と、物理的な攻撃を検知して対応する機能。
- セキュアブート：起動時にソフトウェアゲートとアプリケーションソフトウェアの完全性を検証する機能。
- 鍵の格納：暗号によって機密性と完全性を保護した TOE の不揮発メモリ内に鍵を格納する機能。
- ユーザ鍵のインポート：機密性を保護した状態で TOE の外部エンティティからユーザ鍵や秘密情報をインポートし、鍵ストレージに格納する機能。
- アップデート：正しいアプリケーションソフトウェアのバージョンを得て、ロールバックを防ぎつつ、アプリケーションソフトウェアの真正性と完全性を検証したのちにアップデートする機能。

TOE のベースライン機能を実現するための暗号機能は以下である。ST 作者は必要なセキュリティ機能要件を PP[12]の 7 章から選択する。

- 暗号化／復号：機密性を保護するため、平文を暗号化して暗号文にし、暗号文を復号して平文にする。
- デジタル署名検証：真正性と完全性検証のためにデジタル署名を検証する。
- ハッシュ値の計算：暗号学的ハッシュ関数によりハッシュ値を計算する。
- MAC の生成と検証：MAC を付与し、また MAC が付与されたデータの完全性を検証する。
- 乱数ビットの生成：RBG により乱数ビットを生成し、アプリケーションソフトウェアへ提供する。
- ソルト、ノンスの使用と IV の生成：暗号機能に必要なソルト、ノンスを適切に使用し、IV を生成する。
- 鍵の導出：鍵を導出する。
- 鍵の暗号化：鍵暗号化鍵を利用して鍵を暗号化する。

ソフトウェアゲートを介して TOE がアプリケーションソフトウェアに提供する暗号機能は以下である。この機能はオプション機能であり、ST 作者は必要なセキュリティ機能要件を PP[12]の 8 章から選択する。

- 鍵の生成：TOE が持つ RBG により、用途と暗号アルゴリズムに適した鍵を生成する。
- 鍵および鍵材料の破棄：揮発メモリ上の鍵および鍵材料を復元不可能な状態にする。なお、TOE の不揮発メモリ上の鍵ストレージに格納されている鍵は暗号化されているため、破棄を想定していない。
- デジタル署名生成：真正性と完全性の保護のためにデジタル署名を生成する。

TOE のライフサイクルは、図 1-3 のように 7 つのフェーズに分けられる。TOE 開発者は、フェーズ 1 の TOE 開発から、フェーズ 4 の TOE 製造までの工程と、フェーズ 6 の組込み機器開発者への TOE 配付をセキュアにしなければならない。また、フェーズ 5 のユーザ鍵書込みも TOE 開発者、または鍵インストールプロバイダがセキュアにしなければならない。

フェーズ 3 のアプリケーションソフトウェア開発、フェーズ 6 の組込み機器製造、フェーズ 7 の最終消費者への配付の環境は、PP[12]の対象範囲外であるが、TOE を購入した組込み機器開発者が責任を持ちセキュアにすることを想定している。

フェーズ 1：ハードウェア開発

TOE の開発。TOE 開発者は、SCU の IP を購入し、または SCU を開発し、CPU などのコンポーネントと共に TOE ハードウェアを構築する。

フェーズ 2：ソフトウェア購入／開発

TOE 開発者は暗号エンジンをセキュアに使用するためのソフトウェアゲートを SCU IP ベンダから購入するか、あるいは開発する。セキュアブートプログラムは、SCU IP ベンダから購入するか、TOE 開発者が開発する。

フェーズ 3：アプリケーションソフトウェア開発

組込み機器開発者は、組込み機器の用途を実現するアプリケーションソフトウェアを開発する。TOE 製造者にアプリケーションソフトウェア搭載を依頼する場合は、TOE 製造者へアプリケーションソフトウェアを送付する。組込み機器開発者がアプリケーションソフトウェアを搭載する場合は、フェーズ 6 で搭載する。

フェーズ 4：TOE 製造

TOE 開発者は TOE を製造し、HGK を書込み、セキュアブートとソフトウェアゲートを TOE の不揮発メモリに搭載する。また、組込み機器開発者に依頼された場合、フェーズ 3 で組込み機器開発者が開発したアプリケーションソフトウェアを受け取り、TOE の不揮発メモリに搭載する。なお、アプリケーションソフトウェアは、フェーズ 6 で組込み機器開発者が TOE に搭載する場合もある。製造した TOE は、開発者テストを経て製品となる。

フェーズ 5：ユーザ鍵書込み

TOE 開発者は鍵ストレージを生成する。TOE 開発者は、組込み機器開発者からアプリケーションソフトウェアが使用するユーザ鍵や秘密情報を受け取り、鍵ストレージに格納し、鍵ストレージ全体を暗号化し MAC を付与する。ソフトウェアゲートを介してその鍵ストレージを TOE の不揮発メモリに書込む。このデータの書き込みは、TOE 開発者が鍵インストールプロバイダへ委託する場合もある。いずれにせよ、データの受け渡し、データの書込みはセキュアな環境で行われることが必要になる。データ書込み後、フェーズ 5 からフェーズ 6 へ、TOE を配付する。

フェーズ 6：組込み機器製造

組込み機器開発者は、TOE を基板へ搭載し、組込み機器を製造する。組込み機器開発者がアプリケーションソフトウェアを TOE に搭載する場合もある。この開発工程は、TOE を搭載する基板の開発、それを実装する組込み機器の開発の二つに分かれるかもしれない。この工程は TOE にとっては保護されている前提である。完成した組込み機器は、消費者へ配付される。

フェーズ 7：最終利用者による運用

TOE ライフサイクルの最終フェーズ。TOE が組込み機器に搭載されている状態で、想定する運用環境下で使用される。PP[12]が想定する脅威は、この運用フェーズで発生する。

図 1-3 TOEのライフサイクル

TOE は鍵格納サービスを提供し、暗号を使用することによって暗号エンジンで利用される暗号鍵の機密性を保ち安全に保管する。鍵の完全性は MAC によって保護する。一例として、ハードウェアゲートで利用されるユーザ鍵が鍵ストレージに保持される際に、次のような処理を行う。まず、フェーズ 5 の TOE 開発者の工

場、または委託先の鍵インストールプロバイダにおいて、SCU の内部に書き込まれている HGK を起点として、KEK と MAC 鍵を導出する。次に、TOE で利用される鍵ストレージ（ユーザ鍵、その他データが含まれる）を、KEK を用いて暗号化し、MAC 鍵を用いて、暗号化された鍵ストレージに対して MAC を付与する。このように、暗号化され、さらに MAC が付与された状態で、鍵ストレージは SCU の外部かつ TOE の不揮発メモリに書き込まれる。

TOE には、製造時に生成されたデータオブジェクト（保護ストレージ）があり、TOE 開発者はそのデータオブジェクトに HGK を保管する。例えば、TOE 開発者が TOE 外部の RBG によって HGK を生成して製造工程で TOE の中に埋め込む。HGK は、TSF の完全性を保証し、鍵ストレージへのアクセス許可の基点になる。HGK は保護しなければならないため、TOE は自己保護機能が必要である。

1.1.4 免責事項

なし。

1.2 評価の実施

認証機関が運営する IT セキュリティ評価及び認証制度に基づき、公表文書「IT セキュリティ評価及び認証制度の基本規程」[1]、「IT セキュリティ認証等に関する要求事項」[2]、「IT セキュリティ評価機関承認等に関する要求事項」[3]に規定された内容に従い、評価機関によって PP[12]に関わる機能要件及び保証要件に基づいて IT セキュリティ評価が実施され、令和 4 年 6 月に完了した。

1.3 評価の認証

認証機関は、評価機関が作成した評価報告書[13]、所見報告書([14])、及び関連する評価証拠資料を検証し、PP[12]の評価が所定の手続きに沿って行われたことを確認した。認証の過程において発見された問題については、認証レビューを作成した。認証機関が指摘した問題点は、すべて解決され、かつ、PP[12]の評価が CC（[4][5][6]または[7][8][9]）及び CEM（[10][11]のいずれか）に照らして適切に実施されていることを確認した。認証機関は同報告書に基づき本認証報告書を作成し、認証作業を終了した。

2 PP識別

PP[12]は、以下のとおり識別される。

PP名称：	セキュア暗号ユニット搭載 シングルチップマイクロコントローラ プロテクションプロファイル
バージョン：	バージョン 1.20
開発者：	国立研究開発法人産業技術総合研究所

3 セキュリティ方針

本章では、PP[12]に適合する TOE が脅威に対抗するために採用したセキュリティ機能方針を説明する。

3.1 セキュリティ機能方針

PP[12]では、3.1.1.1 に示す脅威に対抗し、3.1.2.1 に示すセキュリティ機能方針を満たすセキュリティ機能を規定している。

3.1.1 脅威とセキュリティ機能方針

3.1.1.1 脅威

PP[12]は、表 3-1 に示す脅威を想定し、これに対抗する機能を TOE に要求する。

表3-1 脅威

識別子	脅威
T.Internal_Access	攻撃者は、アプリケーションソフトウェアあるいはソフトウェアゲートを改ざんして、TOEの暗号機能を不正に使用するかもしれない。その結果、利用者データを暴露したり、改ざんしたりできるかもしれない。
T.Weak_Import	攻撃者は、鍵ストレージへのインポート機能を悪用し、利用者データを暴露したり、改ざんしたりするかもしれない。

識別子	脅威
T.Unauthorized_Update	攻撃者は、組込み機器の利用者データを暴露したり、組込み機器のサービスを妨害したりするため、不正なアプリケーションソフトウェアをTOEにインストールするかもしれない。または、組込み機器の利用者データを暴露したり、組込み機器のサービスを妨害したりするため、セキュリティ機能の不具合があるバージョンに不正にロールバックするかもしれない。
T.Weak_Crypto	攻撃者は、不適切に選択された鍵生成方法、暗号化アルゴリズム、鍵長、鍵破棄方法、またはRBGを悪用することで、利用者データを暴露したり、改ざんしたりするかもしれない。
T.Leak_Inherent	攻撃者は、暗号演算中のTOEの消費電力変化を観測し分析することによって、暗号鍵のような利用者データあるいはTSFデータを暴露するかもしれない。
T.Phys_Probing	攻撃者は、TOE内部の物理的プロービングによって、暗号鍵のようなTOE内の利用者データ、あるいは他の攻撃に役立つTSFデータを暴露したり、改ざんしたりするかもしれない。
T.Phys_Manipulation	攻撃者は、TOE内部を物理的に操作することによって、そこに格納された利用者データや暗号鍵を改ざんしたり、あるいは他の攻撃のためにTOEのセキュリティサービスを改ざんしたりするかもしれない。

3.1.1.2 脅威に対するセキュリティ機能方針

PP[12]に適合する TOE は、表 3-1 に示す脅威に対し、以下のセキュリティ機能で対抗する。

(1) 脅威「T.Internal_Access」への対抗

以下のセキュリティ機能要件が、改ざんされたアプリケーションソフトウェアや改ざんされたソフトウェアゲートが TOE 内部のハードウェアゲートにアクセスし、TOE の暗号機能を使用するのを防止する。

- FDP_IFC.1/API, FDP_IFF.1/API は、外部エンティティであるアプリケーションソフトウェアによる暗号機能の操作要件を規定する。暗号機能へアクセスするソフトウェアゲートの内部状態遷移結果の正しさが検証された場合に限り、暗号機能から外部エンティティへ暗号機能の結果が出力される。すなわち、暗号機能の正しい利用だけが受け入れられる。

- FDP_MFW_EXT.1 は FPT_TST.1 から呼ばれ、起動時にアプリケーションソフトウェアの完全性を検証し、必要に応じて真正性を検証する。
- FPT_TST.1 は、起動時にソフトウェアゲートの完全性を検証することを定義し、FDP_IFC.1/API, FDP_IFF.1/API によるソフトウェアゲートの内部状態遷移データの検証を支援する。
- FPT_FLS.1/SG は、ソフトウェアゲートの内部状態遷移データの完全性が損なわれてもセキュアな状態を保持する。
- FPT_FLS.1/SB は、起動時にソフトウェアゲートの完全性、アプリケーションソフトウェアの完全性、必要に応じてアプリケーションソフトウェアの真正性が損なわれていてもセキュアな状態を保持する。

(2) 脅威「T.Weak_Import」への対抗

下記のセキュリティ機能要件により、あらかじめ暗号化され、完全性検証データを付与した鍵ストレージへのインポートと、完全性検証を行うことで、不正な利用者データのインポートを防止する。

- FDP_IFC.1/Import, FDP_IFF.1/Import は、外部エンティティであるアプリケーションソフトウェアによるインポート機能の操作要件を規定する。インポート機能へアクセスするソフトウェアゲートの内部状態遷移結果の正しさが検証された場合に限り、インポート機能を介して鍵ストレージへ格納される。すなわち、インポート機能の正しい利用だけが受け入れられる。
- FDP_UIT.1 は、鍵ストレージへインポートされる利用者データの完全性を検証する。

(3) 脅威「T.Unauthorized_Update」への対抗

下記のセキュリティ機能要件により、TSF は正しいアプリケーションソフトウェアのバージョンを得てアップデートを行い、アップデートしたアプリケーションソフトウェアを検証する。

- FPT_TUD_EXT.1 は、アプリケーションソフトウェアにアプリケーションソフトウェアの現在のバージョンを問い合わせ、アップデートを起動し、インストールの前にアップデートするアプリケーションソフトウェアを検証する。
- FPT_RPL.1 は、ロールバックの試みを防止する。
- FPT_FLS.1/UD は、アプリケーションソフトウェアの完全性エラーや真正性エラーの検出が起きてもセキュアな状態を保持する。

(4) 脅威「T.Weak_Crypto」への対抗

以下のセキュリティ機能要件に定義されている、承認された規格に基づく乱数ビット生成と十分なエントロピー源、十分な鍵長を持つ暗号アルゴリズムを実装し、アプリケーションソフトウェアに提供することで、脅威に対抗する。

- （オプション）FCS_CKM.1/AK は、非対称鍵を生成する。
- （オプション）FCS_CKM.1/SK は、対称鍵を生成する。
- （オプション）FCS_CKM.4 は、揮発メモリ上の鍵および鍵材料を復元不可能な状態にする。
- （選択）FCS_COP.1/SKC は、対称鍵アルゴリズムで暗号化・復号する。
- （選択）FCS_COP.1/KeyEnc は、鍵を暗号化・復号する。
- （選択）FCS_COP.1/Hash は、ハッシュを計算する。
- （選択）FCS_COP.1/MAC は、MAC を計算する。
- （オプション）FCS_COP.1/SigGen は、デジタル署名を行う。
- （選択）FCS_COP.1/SigVer は、デジタル署名を検証する。
- （選択）FCS_KDF_EXT.1 は、鍵導出を実行する。
- （選択）FCS_RBG_EXT.1 は、乱数ビットを生成する。
- （選択）FCS_SNI_EXT.1 は、TOE によって使用されるソルトとノンス、IV が鍵強度に悪影響を及ぼさないことを保証する。

(5) 脅威「T.Leak_Inherent」への対抗

以下のセキュリティ機能要件が、SCU が利用者データ、TSF データを処理する際に生じる放射電磁波、消費電力に不要な情報が漏洩することを軽減し、攻撃者が統計処理による有益なデータの暴露を困難にする。

- FPT_EMS_EXT.1 は、TOE からのユーザデータ、TSF データの漏洩を軽減する。

(6) 脅威「T.Phys_Probing」への対抗

以下のセキュリティ機能要件が、半導体解析に用いる機器を使用して、メモリ素子を撮影したり、TOE の内部に物理的に接触したりして、利用者データを改ざん、あるいは取得したりする脅威に対抗することを目的とする。

- FPT_PHP.3 は、物理的プロービングに対抗する。

- FCS_STG_EXT.1 は、SCU 外に鍵ストレージを実装する。
- FCS_STG_EXT.2 は、暗号を使用して SCU 外にある鍵ストレージの機密性を保持する。
- FCS_STG_EXT.3 は、暗号を使用して SCU 外にある鍵ストレージの完全性を保持する。

(7) 脅威「T.Phys_Manipulation」への対抗

下記のセキュリティ機能要件が、TOE の内部の物理的操作によって、直接的に情報資産を改ざんしたり、暴露するための他の攻撃の足がかりにしたりする脅威に対抗することを目的とする。

- FPT_PHP.3 は、TOE の物理的改ざんに対抗する。
- FCS_STG_EXT.1 は、SCU 外に鍵ストレージを実装する。
- FCS_STG_EXT.2 は、暗号を使用して SCU 外にある鍵ストレージの機密性を保持する。
- FCS_STG_EXT.3 は、暗号を使用して SCU 外にある鍵ストレージの完全性を保持する。

3.1.2 組織のセキュリティ方針とセキュリティ機能方針

3.1.2.1 組織のセキュリティ方針

組織のセキュリティ方針はない。

3.1.2.2 組織のセキュリティ方針に対するセキュリティ機能方針

組織のセキュリティ方針はないため、組織のセキュリティ方針に対するセキュリティ機能方針はない。

4 前提条件と評価範囲の明確化

本章では、PP[12]に適合する TOE を運用するための前提条件について記述する。

4.1 使用及び環境に関する前提条件

PP[12]に適合する TOE を運用する際の前提条件を表 4-1 に示す。これらの前提条件が満たされない場合、PP[12]に適合する TOE のセキュリティ機能が有効に動作することは保証されない。

表 4-1 前提条件

識別子	前提条件
A.Trusted_User	組込み機器開発者は、TOEの外部に保持されているデータを適切に保護する。

5 評価機関による評価実施及び結果

5.1 評価機関

評価を実施した株式会社 ECSEC Laboratory 評価センターは、IT セキュリティ評価及び認証制度により承認されるとともに、ILAC（国際試験所認定協力機構）の相互承認に加盟している認定機関（独立行政法人製品評価技術基盤機構認定センター）により認定を受けており、評価品質維持のためのマネジメント及び要員等の適切性についての要求事項を満たしていることが定期的に確認されている。

5.2 評価方法

評価は、CC パート 3 の保証要件について、CEM に規定された評価方法を用いて行われた。評価作業の詳細は、評価報告書[13]において報告された。評価報告書[13]では、PP[12]の概要と、CEM のワークユニットごとの評価内容及び判断結果を説明する。

5.3 評価実施概要

以下、評価報告書[13]による評価実施の履歴を示す。

評価は、令和 3 年 10 月に始まり、令和 4 年 6 月評価報告書の完成をもって完了した。評価機関は、開発者から評価に要する評価用提供物件一式の提供を受け、一連の評価における証拠を調査した。

評価作業中に発見された問題点は、所見報告書[14]として発行され、開発者に報告された。それらの問題点は、開発者による見直しが行われ、最終的に、すべての問題点が解決されている。

また、認証機関が見つけた評価の問題点は、認証レビューとして記述されて、評価機関へ渡された。

これらの指摘は、評価機関及び開発者が検討したのち、評価報告書[13]に反映された。

5.4 評価結果

評価者は、評価報告書[13]に記載されているとおり、PP[12]が CEM のワークユニットすべてを満たしていると判断した。

評価では以下について確認された。

セキュリティ機能要件： コモンクライテリア パート 2 拡張

セキュリティ保証要件： コモンクライテリア パート 3 拡張

評価の結果として、以下の保証コンポーネントについて「合格」判定がなされた。

APE_INT.1, APE_CCL.1, APE_SPD.1, APE_OBJ.1, APE_ECD.1, APE_REQ.1

5.5 評価者コメント/勧告

調達者に喚起すべき評価者勧告は、特にない。

6 認証実施

認証機関は、評価の過程で評価機関より提出される各資料をもとに、以下の観点で認証を実施した。

① 所見報告書[14]でなされた指摘内容が妥当であること。

② 所見報告書[14]でなされた指摘内容が解決されていること。

③ 提出された証拠資料を検査し、関連するワークユニットが評価報告書[13]で示されたように評価されていること。

④ 評価報告書[13]に示された評価者の評価判断の根拠が妥当であること。

⑤ 評価報告書[13]に示された評価者の評価方法がCEMに適合していること。

これらの認証において発見された問題事項を、認証レビューとして作成し、評価機関に送付した。認証機関は、PP[12]及び評価報告書[13]において、認証レビューで指摘された問題点が解決されていることを確認し、本認証報告書を発行した。

6.1 認証結果

提出された評価報告書[13]、所見報告書[14]及び関連する評価証拠資料を検証した結果、認証機関は、PP[12]が CC パート 3 の APE_INT.1、APE_CCL.1、APE_SPD.1、APE_OBJ.1、APE_ECD.1、及び APE_REQ.1 に対する保証要件を満たすものと判断する。

6.2 注意事項

PP[12]で規定する暗号アルゴリズムについては、PP[12]に適合する TOE の評価を行う時点での有効性を保証するものではない。したがって、PP[12]適合を主張する TOE の評価を行う際には、PP[12]が規定する暗号アルゴリズムの有効性の確認、及び危殆化についての評価が必要になる。

7 附属書

特になし。

8 用語

本報告書で使用された CC に関する略語を以下に示す。

CC	Common Criteria for Information Technology Security Evaluation（セキュリティ評価基準）
CEM	Common Methodology for Information Technology Security Evaluation（セキュリティ評価方法）
EAL	Evaluation Assurance Level（評価保証レベル）
PP	Protection Profile（プロテクションプロファイル）
ST	Security Target（セキュリティターゲット）
TOE	Target of Evaluation（評価対象）
TSF	TOE Security Functionality（TOEセキュリティ機能）

本報告書で使用された PP に関する略語を以下に示す。

アプリケーションソフトウェア	TOEから見ると利用者データであり、ソフトウェアゲートAPIを介してSCUの暗号機能を利用する。
外部エンティティ	TOEの外部にあってTOEと対話できる人間あるいはITのエンティティ
鍵ストレージ	ユーザ鍵や秘密情報を格納するデータオブジェクト
ハードウェアゲート	暗号機能に対するアクセス制御メカニズムのハードウェアパートであり、暗号エンジンにアクセスする。
保護ストレージ	HGKを格納する特殊なストレージ。半導体テストプロセスによってHGKを書込むOTP領域であったり、ハードコードして回路の一部であったりする。
ユーザ鍵	アプリケーションが使用する鍵であり、鍵暗号化鍵により暗号化され、完全性検証用データが付与される。
API	Application Program Interface、TOEの外部のソフトウェアから呼び出されるインタフェース
CPU	Central Processing Unit、中央処理装置
HGK	Hardware Gate Key、ハードウェアゲート鍵
IP	Intellectual Property、LSIを構成するための部分的な回路情報
IT	Information Technology
IV	Initialization Vector、初期化ベクタ
KDF	Key Derivation Functions、鍵導出関数
KEK	Key Encryption Key、鍵暗号化鍵の略
MAC	Message Authentication Code、メッセージ認証コード
OTP	One Time Programmable

RBG	Random Bit Generator、乱数ビット生成器
RoT	Root of Trust、信頼の起点
SCU	Secure Cryptographic Unit、セキュア暗号ユニット
SoC	System on a Chip、一個の半導体チップ上にシステムの動作に必要な機能の多く、あるいは全てを実装するという設計手法、また、その手法を使って作られたチップ

9 参照

[1] ITセキュリティ評価及び認証制度の基本規程, 令和2年10月, 独立行政法人情報処理推進機構, CCS-01

[2] ITセキュリティ認証等に関する要求事項, 令和2年10月, 独立行政法人情報処理推進機構, CCM-02

[3] ITセキュリティ評価機関承認等に関する要求事項, 令和3年10月, 独立行政法人情報処理推進機構, CCM-03

[4] Common Criteria for Information Technology Security Evaluation Part1: Introduction and general model Version 3.1 Revision 5, April 2017, CCMB-2017-04-001

[5] Common Criteria for Information Technology Security Evaluation Part2: Security functional components Version 3.1 Revision 5, April 2017, CCMB-2017-04-002

[6] Common Criteria for Information Technology Security Evaluation Part3: Security assurance components Version 3.1 Revision 5, April 2017, CCMB-2017-04-003

[7] 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 バージョン3.1 改訂第5版, 2017年4月, CCMB-2017-04-001（平成29年7月翻訳第1.0版）

[8] 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 バージョン3.1 改訂第5版, 2017年4月, CCMB-2017-04-002（平成29年7月翻訳第1.0版）

[9] 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: セキュリティ保証コンポーネント バージョン3.1 改訂第5版, 2017年4月, CCMB-2017-04-003（平成29年7月翻訳第1.0版）

[10] Common Methodology for Information Technology Security Evaluation : Evaluation methodology Version 3.1 Revision 5, April 2017, CCMB-2017-04-004

[11] 情報技術セキュリティ評価のための共通方法: 評価方法 バージョン3.1 改訂第5版, 2017年4月, CCMB-2017-04-004（平成29年7月翻訳第1.0版）

[12] セキュア暗号ユニット搭載シングルチップマイクロコントローラプロテクションプロファイル, バージョン1.20, 2022年6月15日, 国立研究開発法人 産業技術総合研究所

[13] PP評価報告書 SCV21-ETRPP-0001-03, 第1.3版, 2022年6月17日, 株式会社ECSEC Laboratory評価センター

[14] 所見報告書 SCV21-EOR-7001-00, 2021年11月26日, 株式会社ECSEC Laboratory評価センター