# 認 証 報 告 書

独立行政法人情報処理推進機構
理事長　藤江　一正

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） | 平成25年7月22日 (IT認証3469) |
| 認証番号 | C0427 |
| 認証申請者 | 電子商取引安全技術研究組合 |
| PPの名称 | 組込み機器向けセキュアICチップ プロテクションプロファイル |
| PPのバージョン | 第1.0版 |
| PP適合 | 他のPPへの適合主張なし |
| 適合する保証パッケージ | EAL4 |
| 開発者 | 電子商取引安全技術研究組合 |
| 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。

平成26年3月31日

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
技術管理者　近藤　潤一

**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 Common Criteria for Information Technology Security Evaluation Version 3.1 Release 4
② Common Methodology for Information Technology Security Evaluation Version 3.1 Release 4

**評価結果：合格**

「組込み機器向けセキュアICチップ プロテクションプロファイル」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、電子商取引安全技術研究組合が開発した「組込み機器向けセキュア IC チップ プロテクションプロファイル、バージョン　第 1.0 版」(以下「本 PP」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。）が平成 26 年 3 月 14 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電子商取引安全技術研究組合に報告するとともに、本 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]に適合する TOE の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 において詳述されている。

本認証報告書は、PP [12]に準拠した組込み機器向けセキュア IC チップを開発・納入する開発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性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、EAL4 である。

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

### 1.1.2 PP概要

PP [12]は、組込み機器制御用 IC チップに求められるセキュリティ要件を規定する。

PP [12]に適合する TOE は、内部に暗号機能を持ち、その暗号機能を組込み機器のソフトウェアが利用することにより組込み機器内部のデータ保護あるいは他の暗号関連サービスに使用される。

意図していない外部エンティティからの暗号機能へのアクセスを制限する目的で、組込み機器所定の処理に従う暗号機能の使用のみが許可される。

また、PP [12]に適合する TOE は、用途に照らして必要なエントロピーを有する乱数を生成する機能を提供する。

PP [12]において、TOE は組込み機器に含まれる IC チップの暗号機能を実現する機能ブロックである。したがって、組込み機器全体が TOE の IT 環境である。CPU は、TOE の IC チップ内にあっても、IC チップ外にあってもよい。

PP [12]に適合する TOE のブロック図の例を図 1-1 に示す。

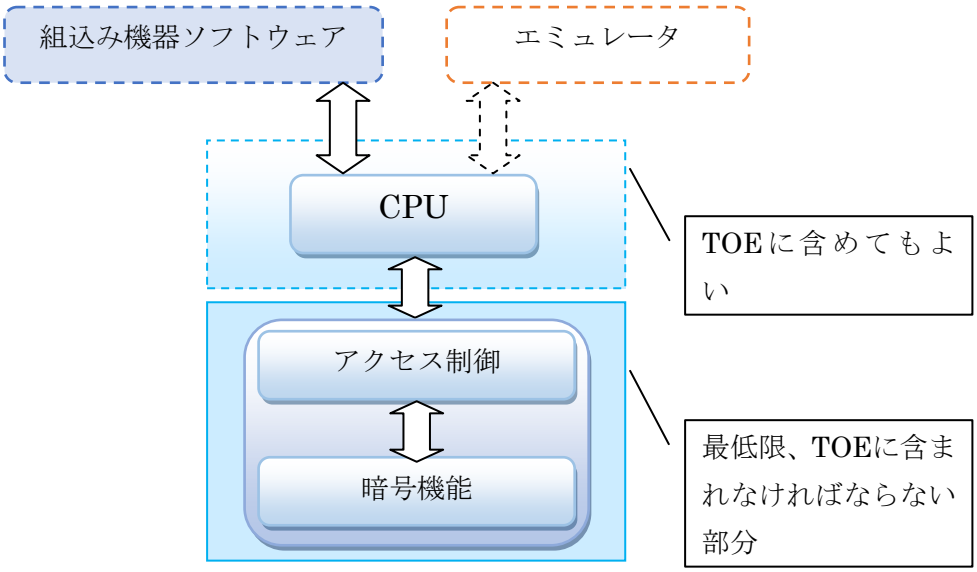


図 1-1 PP [12]に適合するTOEのブロック図の例

ここで、CPU は、その上で組込み機器ソフトウェアが実行されるものを指す。

加えて、TOE を対象とした物理攻撃に対抗する保護機能も提供する。

#### 1.1.2.1 セキュリティ機能概要

PP [12]では、組込み機器内部の利用者データの機密性 及び/又は 組込み機器の暗号に依存するサービスの完全性を維持するためのセキュリティ機能を要求する。その主要なものを次に示す。

(1) 暗号機能

TOE の外部エンティティである組込み機器ソフトウェアが、組込み機器ソフトウェアの保護資産の暴露・改ざんから保護するため、或いは、外部エンティティが他の IT 装置と相互認証を行ったりするために使用される暗号機能。

(2) 暗号機能へのアクセス制御

TOE の外部エンティティからの暗号機能の使用要求が、TOE 内部の検証データを用いて検証できた場合のみ、暗号機能の使用要求を受け付ける。

(3) 乱数生成

攻撃者の予測に耐え、セキュリティ機能のメカニズムが必要とする性質をもつ乱数を生成する機能。

(4) 物理攻撃からの保護

次のような物理攻撃から、TSF を保護する。

- TOE の消費電力・電磁放射から、内部で処理される情報の漏えい
- 物理的方法によるプローブ・改ざん
- 環境ストレスや、LASER を用いた故障注入攻撃による誤動作

#### 1.1.2.2 脅威とセキュリティ対策方針

PP [12]に適合する TOE は、以下のとおりのセキュリティ機能によりそれぞれの脅威に対抗する。

組込み機器では、エミュレータを接続するインタフェースが備わった構成がありうること、それによって意図した組込み機器ソフトウェア以外の外部エンティティが暗号機能にアクセスするかもしれない。そこで、暗号機能を実現する TOE 内に意図する組込み機器ソフトウェアに紐づけられた参照データを持つ構成とし、外部エンティティからの暗号機能の使用要求を、その参照データと照らし合わせ、照合に成功した場合にだけ暗号機能の使用を許可する。これによって、意図する組込み機器ソフトウェアと異なる暗号機能の使用方法を外部エンティティに対して防止することができる。

IC チップは、その物理形態の特性上、内部で処理している情報を、消費電力や放射電磁波を通じて漏えいしてしまう。また、物理的なプロービングによる IC チップ内部の情報の暴露や環境ストレスの印加による誤動作を考慮する必要がある。そこで、こういった物理攻撃から TSF を保護する機能を有する。

組込み機器のサービス又は暗号機能には乱数を必要とするものが考えられるが、(1) 攻撃者にある程度の予測が可能な乱数や (2) 用途に対して不十分なエントロピーしか持たない乱数では、最終的に実現されるサービスの信頼が失われる。そこで、エントロピーの数値目標を実現し、かつ物理的に保護された乱数生成器を実装することにより、この脅威に対抗する。

#### 1.1.2.3 構成要件と前提条件

PP [12]に適合する TOE は､次のような構成及び前提で運用することを想定する。

PP [12]に適合する TOE は、組込み機器に搭載された状態で運用されることを想定する。組込み機器の構成として、CPU は、PP [12]に適合する TOE の (1) 内部にある構成、または (2) 外部にある構成のどちらも許容される。前提条件は無い。

### 1.1.3 免責事項

PP [12]では、組込み機器の IC チップの中の暗号機能を担う機能部分が TOE である。組込み機器ソフトウェアが提供するサービスは、TOE 範囲外の部分にも依存する。PP [12]では、TOE 範囲外を攻撃することによって、サービスの機能を低下させる脅威に対しては対抗していない。

## 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・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、平成 26 年 3 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][15][16][17][18][19]）、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： | 組込み機器向けセキュアICチップ　プロテクションプロファイル |
| バージョン： | 第1.0版 |
| 開発者： | 電子商取引安全技術研究組合 |

# 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や組織のセキュリティ方針を説明する。

PP [12]では、組込み機器の中の暗号機能を担うセキュア IC としてのセキュリティ機能を要求する。TOE に要求されるセキュリティ機能性は、次の 4 つである。

- 組込み機器として利用者データを保護するため及び／又は機器認証のための暗号機能、
- その暗号機能へのアクセス制御、
- 乱数生成、
- TOE 自身の物理的保護

## 3.1 セキュリティ機能方針

PP [12]では、3.1.1 に示す脅威に対抗し、3.1.2 に示す組織のセキュリティ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 想定する脅威**

| 識別子 | 脅威 |
|---|---|
| T.Internal-Access | 組込み機器においてTOEの上位で動作する組込み機器ソフトウェアは、その利用者データを保護するためにTOEの暗号機能を利用する。その利用者データの攻撃（暴露、改ざんなど）を目的とする攻撃者は、攻撃手段の一つとして、エミュレータ等のツールを用い、TOE内部の暗号機能を許可なく使用しようとするかもしれない。 |

| 識別子 | 脅威 |
|---|---|
| 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、消費電力の変化パターンとTOEの暗号演算結果を分析することによって、TOEの暗号機能の一部である暗号鍵を暴露するかもしれない。消費電力変化データは、TOEの電源端子への流入電流観測やTOEの漏洩電磁波の観測など、物理的手段によって得られる。 |
| T.Phys-Probing | 攻撃者は、TOE内部の物理的プロービングによって、暗号機能内の利用者データ、暗号鍵、あるいは他の攻撃に役立つTOEの重要情報を暴露するかもしれない。 |
| T.Malfunction | 攻撃者は、動作中のTOEに環境ストレスを印加し、TOEが関与する組込み機器ソフトウェアの実行やTSF自身の動作に誤りや機能不全を生じさせる。その結果として、組込み機器の利用者データが暴露されたり、組込み機器のサービスが妨害されたりするかもしれない。 |
| T.Phys-Manipulation | 攻撃者は、暗号機能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変したり、あるいは他の攻撃のためにTOEのセキュリティメカニズムを改変したりするかもしれない。 |
| T.RND | 攻撃者は、TOEが生成する乱数値を予測し、それによって、乱数のエントロピーに依存するTSFデータ（ex. TOEが生成する暗号鍵や認証データ）の品質が低下するかもしれない。 |

#### 3.1.1.2 脅威に対するセキュリティ機能

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」に対抗するためのセキュリティ機能**

本脅威は、意図された組込み機器ソフトウェア以外の外部エンティティが TOE の暗号機能を使用することにより、意図された組込み機器ソフトウェアの資産を暴露、改ざんするかもしれないことを想定している。

この脅威に対して、TOE では、外部エンティティからの暗号機能の使用要求を、意図する組込み機器ソフトウェアに紐付けられた、TOE 内の参照データに照らして検証することにより、意図する組込み機器ソフトウェアによる暗号機能の使用又はそれと同じ使用方法のみを許可し、暗号機能の許可された使用の演算結果を外部エンティティに返す機能を提供する。

ここで、エミュレータを含めた外部エンティティからは、TOE 内の参照データを含め、TOE 内部の情報へのアクセスはできない。

また、このセキュリティ機能の正しい動作を確認するための、自己テスト機能も提供する。

**(2) 脅威「T.Leak-Inherent」に対抗するためのセキュリティ機能**

本脅威は、TOE の消費電力や漏洩電磁波などの物理量の分析から TOE の暗号機能に使用される暗号鍵が暴露されるかもしれないことを想定している。

この脅威に対して、TOE は、次の攻撃シナリオに耐えるべく、TSF に対する保護機能を提供する。

- 暗号アルゴリズム及び暗号鍵を分析しようとする SPA(Simple Power Analysis) / DPA (Differential Power Analysis) / SEMA (Simple Electro-Magnetic Analysis) / DEMA (Differential Electro-Magnetic Analysis)、
- Higher-order DPA、
- 乱数生成器の出力を予測しようとする攻撃

また、このセキュリティ機能を実現する回路の正しい動作を確認するための、自己テスト機能も提供する。

**(3) 脅威「T.Phys-Probing」、「T.Malfunction」及び「T.Phys-Manipulation」に対抗するためのセキュリティ機能**

PP [12]に適合する TOE は、IC という物理形態という特性上、物理的な改ざん（観察、分析、あるいは改変）にさらされる。また、TOE の振る舞いは、電圧、周波数、温度といった動作条件からの影響を受ける。

これらの脅威に対して、TOE は、次の攻撃シナリオに耐えるべく、TSF に対する保護機能を提供する。

- TOE 内部を流れる信号を読み取ろうとする攻撃、
- TOE 内部を流れる信号を改変しようとする攻撃、
- TOE の自己保護機能を非活性化又はバイパスすべくセンサー類を無効化する攻撃、
- 故障注入攻撃(DFA を含む)

また、このセキュリティ機能を実現する回路の正しい動作を確認するための、自己テスト機能も提供する。

**(4) 脅威「T.RND」に対抗するためのセキュリティ機能**

この脅威は、乱数が必要とされる局面で、攻撃者の能力を考慮した上で、利用できる乱数のエントロピーが、乱数の用途である TSF データに求められるエントロピーに足りないかもしれない、という状況を想定している。TSF データに求められるエントロピーを利用できなければ、その TSF データに依存するセキュリティ機能によって実現されるはずの機能や特性が利用できないかもしれない。

この脅威に対して、TOE は、次のいずれかの乱数生成器を提供する。

- 物理乱数生成器、
- 物理乱数生成器と決定論的乱数生成器を組み合わせたハイブリッド乱数生成器

また、乱数生成器の正しい動作を確認するための、自己テスト機能も提供する。

### 3.1.2 組織のセキュリティ方針とセキュリティ機能

#### 3.1.2.1 組織のセキュリティ方針

PP [12]に適合する TOE の利用に当たって要求される組織のセキュリティ方針を表 3-2 に示す。

**表 3-2 組織のセキュリティ方針**

| 識別子 | 組織のセキュリティ方針 |
|---|---|
| P.Cryptography | TOEは、TOEの上位で動作する組込み機器ソフトウェアなどの外部エンティティに暗号機能を提供する。この暗号機能は、その外部エンティティの保護資産を暴露や改ざんから保護したり、あるいは、外部エンティティが他のIT装置と相互認証を行ったりするために使用される。 |

#### 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

PP [12]は、表 3-2 に示す組織のセキュリティ方針を満たす機能を TOE に要求する。

**● 組織のセキュリティ方針「P.Cryptography」を満たすためのセキュリティ機能**

PP [12]に適合する TOE は、本組織のセキュリティ方針の中で指定された暗号機能を提供する。

# 4 前提条件と評価範囲の明確化

本章では、想定する読者が PP [12]に適合する TOE の利用の判断に有用な情報として、PP [12]に適合する TOE を運用するための前提条件及び運用環境について記述する。

## 4.1 使用及び環境に関する前提条件

PP [12]に適合する TOE は、組込み機器に搭載された状態で運用されることを想定する。PP [12]に適合する TOE を運用する際のその他の前提条件はない。

# 5 評価機関による評価実施及び結果

## 5.1 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、評価報告書において報告された。評価報告書では、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。

## 5.2 評価実施概要

以下、評価報告書による評価実施の履歴を示す。

評価は、平成 25 年 7 月に始まり、平成 26 年 3 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。

各ワークユニットの評価作業中に発見された問題点は、すべて所見報告書として発行され、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、評価報告書に反映された。

## 5.3 評価結果

評価者は、評価報告書をもって 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.2、APE_ECD.1、APE_REQ.2

評価では以下について確認された。

| 評価結果概要 |
|---|
| APE_INT.1　　PP 概説 |
| PP [12]は、組込み機器制御用 IC チップに求められる、次のセキュリティ機能を規定していることが、評価を通じて確認された。<br>・外部エンティティに対して、IC チップが提供する暗号機能のセキュアな使用を |

| |
|---|
| 提供する。<br>・IC チップの TSF に対する物理的攻撃に対抗する。 |
| APE_CCL.1　　適合主張 |
| 評価を通じて次の事実が確認された。<br>・CC Version 3.1 Revision 4 への適合<br>・セキュリティ機能要件：　CC Part 2　拡張<br>・セキュリティ保証要件：　CC Part 3　適合<br>・他の PP への適合主張をしないこと<br>・PP [12]への適合主張をする場合は、論証適合が求められていること |
| APE_SPD.1　　セキュリティ課題定義 |
| 評価を通じて次の事項が確認された。<br>・脅威及び組織のセキュリティ方針が、CC/CEM に従った観点で記述されていること<br>・PP [12]では前提条件を置かないこと |
| APE_OBJ.2　　セキュリティ目標 |
| 評価を通じて次の事項が確認された。<br>・セキュリティ課題定義で記述された脅威及び組織のセキュリティ方針を取り扱うセキュリティ目標が記述されていること、その根拠が適切であること |
| APE_ECD.1　　拡張コンポーネント定義 |
| 評価を通じて次の事項が確認された。<br>・拡張コンポーネント定義の中で、CC Part 2 に記述されていない、用途を限定しない乱数生成に関するセキュリティ機能要件が規定されていること |
| APE_REQ.2　　セキュリティ要件 |
| 評価を通じて次の事項が確認された。<br>・セキュリティ目標を満たすセキュリティ機能要件が記述されていること<br>・EAL4 というセキュリティ保証要件についての選択理由が記述されていること。 |

## 5.4　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、以下の項目について確認した。

① 所見報告書でなされた指摘内容が妥当であること。

② 所見報告書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の内容を検査し、関連するワークユニットが評価報告書で示されたように評価されていること。

④ 評価報告書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。

これらの確認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、所見報告書及び関連する評価証拠資料を確認した結果、認証機関は、PP [12]が CC パート 3 の保証コンポーネント APE_INT.1、APE_CCL.1、APE_SPD.1、APE_OBJ.2、APE_ECD.1、及び APE_REQ.2 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

なし。

# 7 附属書

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用語の定義を以下に示す。

| | |
|---|---|
| エミュレータ | ICチップのCPU動作をエミュレートする装置。エミュレータを接続すると、CPUが周辺デバイスにアクセスする動作をエミュレータから指示・実行できる。組込み機器開発フェーズでのデバッグだけでなく、運用フェーズでの組込み機器の運用・保守（テスト、データ収集、データ書き換えなど）にも使用できる。“デバッガ”と称されることもある。 |
| 組込み機器ソフトウェア | TOEの上位で動作し、組込み機器を制御するソフトウェアを指す。<br>TOEのICチップ内に実装される場合と、TOEのICチップ外に実装される場合の両方がある。 |
| 所見報告書 | 評価中に、問題の明確化を要求したり、問題を識別するために評価者が作成する報告書。 |
| DEMA | Differential Electro-Magnetic Analysis |
| DFA | Differential Fault Analysis |
| DPA | Differential Power Analysis |
| EMA | Electro-Magnetic Analysis |
| LASER | Light Amplification by Stimulated Emission of Radiation |
| SEMA | Simple Electro-Magnetic Analysis |
| SPA | Simple Power Analysis |

# 9 参照


[1] ITセキュリティ評価及び認証制度の基本規程, 平成24年3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, 平成25年4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, 平成25年4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 Part 1: Introduction and general model, Version 3.1 Revision 4, September 2012, CCMB-2012-09-001

[5] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1 Revision 4, September 2012, CCMB-2012-09-002

[6] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 4, September 2012, CCMB-2012-09-003

[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4版, 2012年9月, CCMB-2012-09-001, (平成24年11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4版, 2012年9月, CCMB-2012-09-002, (平成24年11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4版, 2012年9月, CCMB-2012-09-003, (平成24年11月, 翻訳第1.0版)

[10] Common Methodology for Information Technology Security Evaluation : Evaluation methodology, Version 3.1 Revision 4, September 2012, CCMB-2012-09-004

[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4版, 2012年9月, CCMB-2012-09-004, (平成24年11月, 翻訳第1.0版)

[12] 組込み機器向けセキュアICチップ プロテクションプロファイル, バージョン 第1.0版, 2014年3月12日, 電子商取引安全技術研究組合

[13] 組込み機器向けセキュアICチップ プロテクションプロファイル評価報告書, 第2.0版, 2014年3月14日, 株式会社ECSEC Laboratory評価センター

[14] 所見報告書 NDY-EOR-7001-00, 2013年9月6日, 株式会社ECSEC Laboratory評価センター

[15] 所見報告書 NDY-EOR-7002-01, 2013年9月30日, 株式会社ECSEC Laboratory評価センター

[16] 所見報告書 NDY-EOR-7003-00, 2013年10月2日, 株式会社ECSEC Laboratory評価センター

[17] 所見報告書 NDY-EOR-7004-00, 2013年11月29日, 株式会社ECSEC Laboratory評価センター

[18] 所見報告書 NDY-EOR-7005-00, 2013年12月4日, 株式会社ECSEC Laboratory評価センター

[19] 所見報告書 NDY-EOR-7006-00, 2014年1月9日, 株式会社ECSEC Laboratory評価センター