# 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

第1.0版

2014年3月12日

電子商取引安全技術研究組合
Electronic Commerce Security Technology Research Association

認証番号: C0427

(空白ページ)

# Foreword

本PPは、経済産業省の平成24年度情報セキュリティ対策推進事業（機器間相互認証に用いるLSIのセキュリティ対策に関する研究開発）実施計画3.(2)①に示された「セキュアM2Mモジュールのセキュリティ要求仕様書」である。

M2M機器間認証に用いられるモジュールは、ソフトウェア及びハードウェア（システムLSI）によって構成されるが、当該実施計画3.「事業内容及び実施方法」の冒頭に示されたとおり、本年度事業の目的は、M2M機器間認証用モジュールに実装されるシステムLSIチップのセキュリティ仕様を標準化することである。

本事業実施計画(1)①において、本PPのTOEのプロトタイプ（原型）として採択されたシステムLSIチップは、M2M機器間認証用モジュールに実装可能であるとともに、他の様々なアプリケーション用途に使用することができる。また、本PPが記述するTOEのセキュリティ機能は、TOEが搭載するソフトウェアの用途にかかわらず利用可能である。

本PPでは、作成検討の過程で、このようなTOEの汎用性を重視し、搭載されるソフトウェアの用途を限定せず、広く「組込み機器向けICチップ」のためのセキュリティ要件として記述することにした。そのため題名も「組込機器向けICチップセキュリティ要求仕様書」としたものである。

組込み機器向けICチップには、ICカード（スマートカード）向けICチップと異なるセキュリティ特性が要求される。ICカード向けICチップの場合、ICチップがプラスチックカードに埋め込まれ、接触型あるいは非接触型の標準化された外部インタフェース（利用者インタフェース）を介して利用される。利用者インタフェースに対する論理的攻撃の範囲は限定的である。一方、組込み機器向けICチップの場合、ICチップが機器に実装された状態で、IC内部へアクセス可能な外部インタフェースが設けられることがある。この外部インタフェースの例は、エミュレータ（あるいはデバッガ）用端子である。エミュレータは、組込み機器の保守・管理の一端として、ICチップ内のデータを読み書きするために使用される。エミュレータは、組込み機器ソフトウェアを経由せずにICチップを含む組込み機器の内部リソースへ直接アクセスできる。そのため、エミュレータが攻撃手段に悪用されると、組込み機器ソフトウェアによるセキュリティ機能が迂回されてしまい、ICチップ内の情報資産を保護できない。

組込み機器向けICチップに対しては、ICカード向けICチップと異なるセキュリティ対策が必要である。本PPは、そのような組込み機器向けICチップへのセキュリティ課題と、それに対応するセキュリティ要件を定義する。なお、組込み機器向けICチップにおいても、ICカード向けICチップと同様に物理的攻撃へ対抗しなくてはならない。物理的攻撃によるICチップ内部データの暴露・改変を防ぐため、ICチップに耐タンパ性が要求される。ICチップへの攻撃は、それが組込み機器に実装された状態で行われるので、ICチップ内部構成や組込み機器のタイプによって、対抗すべき物理的攻撃範囲が異なる。本PPを参照してPP/STを作成する者は、TOEの環境条件を考慮した物理的攻撃を想定し、必要な対策を追加すべきである。

本PPは、これを参照するPP/STに対して論証適合主張を要求する。本PPが提示するセキュリティ課題の解決を論証することで、本PPの記述に拘束されることなく本PPへの適合を主張できる。

# Contents

# 1 PP introduction

## 1.1 PP reference

タイトル: 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
版数: 第1.0版
発行: 2014年3月12日
作成者: 電子商取引安全技術研究組合
発行者: 電子商取引安全技術研究組合
登録: 認証番号 C0427
キーワード: 組込み機器、ICチップ、エミュレータ、M2M (machine to machine) 、相互認証、物理的攻撃

## 1.2 TOE overview

### 1.2.1 The TOE type

TOEは、組込み機器制御用ICチップである。内部に暗号機能を持ち、組込み機器が保護を必要とするデータを、TOEの暗号機能によって保護する。

### 1.2.2 Available non-TOE hardware/software/firmware

TOEは、組込み機器に搭載され、組込み機器全体をTOEのIT環境として動作する。TOEとTOE以外の組込み機器の機能分担は、TOEの実現方法に依存する。一例として、TOEが必要なセキュリティ機能をすべて内包する一つのICチップで実現されると仮定すると、組込み機器開発者 (TOEの消費者に相当) は、TOEを搭載するプリント基板、組込み機器の筐体、組込み機器の制御ソフトウェアなど、TOEを動作させるために必要なIT環境を準備してTOEを使用する。

### 1.2.3 Usage of the TOE

本TOEは、TOEを構成するICチップ内部に暗号機能を持つ。この暗号機能は、組込み機器のソフトウェアから呼び出され、組込み機器内部の利用者データ保護、あるいは他の暗号関連サービス(相互認証、電子署名など) に使用される。

組込み機器を制御するソフトウェアは、組込み機器のサービスを実行するAP (Application Program) と、APの下位で動作するOS (Operating System) である。一般に、ICチップ内に搭載されるソフトウェアは、組込みソフトウェアと呼ばれる。しかし、本PPのTOEでは、組込み機器を制御するAP/OSが必ずしもTOEのICチップ内に実装されるとは限らず、ICチップ外に置か

れるかもしれない。そのため、“組込みソフトウェア”という名称を使わず、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、“組込み機器ソフトウェア”と称する。

本TOEは、組込み機器ソフトウェアに暗号機能を提供するとともに、暗号機能の使用を、正当な組込み機器ソフトウェアだけに制限するセキュリティ機能を持つ。このセキュリティ機能は、本TOEの特徴的な機能であり、1.2.4で詳しく説明される。

### 1.2.4 Major security features of the TOE

TOEの主要セキュリティ機能（security features）を説明する。

(1) 組込み機器特有の脅威

本TOEが搭載される組込み機器では、運用・保守のために外部からエミュレータ接続が行われることを想定する。開発工程でも、デバッグ等にエミュレータが利用される。しかし、脅威として考慮すべきは、運用環境におけるエミュレータの使用である。

エミュレータは、組込み機器ソフトウェアを経由せず、ハードウェアレベルで組込み機器内の電子回路やデータへアクセスする。このことは、組込み機器ソフトウェアのセキュリティ機能がエミュレータに対して有効に働かないことを意味する。もし攻撃者がエミュレータを悪用すると、組込み機器の内部資源が許可なくアクセスされ、保護すべき利用者データが暴露・改ざんされたり、組込み機器の認証機能が不正利用されたりするかもしれない。

エミュレータのアクセス範囲は、組込み機器の開発方針に依存する。本PPでは、運用・保守での使用を想定する。開発者は、エミュレータのアクセス範囲を組込み機器の主制御装置と同等とし、TOE内のセンシティブな領域にエミュレータがアクセスできるようにしてはならない。センシティブな領域の例は、以下に述べる暗号機能の内部である。

組込み機器内の利用者データ保護のため、暗号機能が使用される。利用者データを暗号化し、あるいはMAC（Message Authentication Code）付与を行う。前者は、データの機密性を保護し、後者は、完全性を検証する。暗号機能は、TOE内の独立したハードウェア回路とし、TOEの内部バスを介して使用される。暗号機能内部に直接アクセスするインタフェースは設けない。しかし、エミュレータはCPUと同等のふるまいをする。内部バス経由で暗号機能が不正アクセスされ、暗号による保護対策が無効化される恐れが残る。

運用環境におけるエミュレータ使用を制限すれば、エミュレータによる攻撃を防ぐことができる。しかし、エミュレータは、組込み機器の運用・保守手段として有用なので、エミュレータの使用制限は、必ずしも適切な対策ではない。エミュレータ使用を許可したうえで、TOE暗号機能の不正使用を防ぐ対策が望ましい。

(2) 組込み機器の資産保護に使われるTOEのセキュリティ機能

本TOEは、エミュレータ等の外部デバイスが組込み機器内部へアクセスするような運用環境において、以下（a）、（b）のセキュリティ機能を提供する。これらは、TOEの資産保護に必要であるが、その本来の目的は、組込み機器の資産保護である。

(a) 暗号機能のセキュアな使用: 組込み機器における利用者データの機密性・完全性保護、あるいは他の機器との相互認証等のため、TOE外のエンティティ（組込み機器ソフトウェア、エミュレータなど）に対し、TOEの暗号機能のセキュアな使用を提供する。セキュアな使用とは、組込み機器所定の処理（すなわち、組込み機器ソフトウェアにプログラミングされた処理）に伴う暗号機能使用だけを許可し、それ以外の暗号機能使用を禁止することをいう。暗号機能の使用には、暗号操作（暗号化、復号、ハッシュ演算など）の実行のほか、暗号鍵の管理（更新など）を含む。

このセキュリティ機能を実現するメカニズムは、本PPでは規定しない。しかし、本PPが要求するセキュリティ機能の理解を深めるため、メカニズムの実現例を（3）項に示す。

(b) 物理攻撃への対抗: TSFに対する物理的攻撃に対抗する。

(3) 暗号機能のセキュアな使用を提供するメカニズム実現例

TOEの上位で動作する組込み機器ソフトウェアは、自身のセキュリティ機能方針（SFP）を実施するためにTOEの暗号機能を使用する。例えば、暗号化・MAC付与によって利用者データを保護し、あるいは外部装置の認証のために暗号機能を使用する。

組込み機器ソフトウェアのSFPを侵害しようとする攻撃者は、TOEの暗号機能の不正使用を試みる。外部エミュレータを用いてTOEの暗号機能にアクセスし、暗号化されたデータの復号、あるいは、暗号機能からの暗号鍵読出しなどを試みる。

TSFは、組込み機器ソフトウェアによるTOE暗号機能の正当な使用だけを許可し、それ以外の使用を禁止しなければならない。この実現例の一つとして、組込み機器による暗号機能使用パターンを監視し、正当な使用かそうでないかを区別するメカニズムを説明する。なお、これは一つの例示であり、他の実現手段を排除するものではない。

組込み機器が提供するサービスは、その処理実行パターンが固定的である。利用者の操作に応じた処理パターンのバリエーションは生じるが、バリエーションの範囲は有限であり、設計時にすべてのパターンを予測できる。

組込み機器のサービスは、ひとつひとつが、開始点と終了点の明確なスレッドを形成する。このスレッドの一部として、暗号機能が使用される。

組込みソフトウェアによる暗号機能の使用例として、単純化した使用手順を以下に示す。この例では、利用者データのセキュアな保管が目的である。

1) オブジェクトAのデータを暗号機能へ入力
2) 暗号鍵K1（暗号機能内部で生成）で暗号化
3) 暗号化データを暗号機能から出力し、オブジェクトBに保管
4) オブジェクトBの暗号化データを暗号機能へ入力
5) 暗号鍵K1で復号し、オブジェクトCへ出力

この処理は、組込みソフトウェアが実行する。この例では、オブジェクトA、Cでのデータ保護は説明されていない。各オブジェクトは、TOEの入出力端子やTOE内のファイルなどが該当する。

組込みソフトウェアの処理がこのパターン通りに実行されれば、暗号機能とオブジェクトBにおけるデータは、暗号機能によって保護されている。

TSFは、組込みソフトウェアによる処理が所定のパターンかどうかを判定するメカニズムを持ち、所定パターンの処理に伴う暗号機能の使用だけを許可する。このメカニズムは、上述の組込み機器のサービスを実行するスレッドの開始から終了までを監視し (例えば、内部バス上のコマンドやレスポンスを監視する) 、あらかじめ予測された処理パターンと一致するかどうかを判定する。

組込み機器ソフトウェアの処理パターンでは、利用者データは、常に保護された状態にある。

一方、攻撃者がエミュレータを使って暗号機能を不正使用すると、予測されたものと異なる処理パターンが生じる。例えば、暗号化されたデータを復号して平文で出力させる処理などである。

上記の処理パターン判定メカニズムは、予測した正しい処理パターンがセキュアに保管され、改ざんされずにTSFから参照できねばならない。さもないと、攻撃者が処理パターンの予測データ自体を偽造してしまう。この改ざん防止のメカニズムにも、暗号技術が有効である。

エミュレータは、組込み機器ソフトウェアと同一の処理パターンを実行し、暗号機能へのアクセスを成功させようとするかもしれない。しかし、組込み機器と同一の処理は、正当な処理パターンである。上述したように、正当な処理パターンを実行する限り、利用者データは常に保護された状態にある。このような攻撃は、TOEのセキュリティ方針を侵害しない。

以上の例は、1.2.5で実装上の構成例を用いて詳しく説明されるので、併せて参照されたい。なお、ここに示した例は、特定のメカニズム使用を指定するものではない。ST作成者は、この例に関わらず、別のセキュリティメカニズムを採用することができる。

(4) 暗号機能の内部保護

暗号機能の使用環境では、暗号機能が使用する暗号鍵は、暗号機能内部に保管され、保護されない状態で暗号機能外部に取り出せてはならない。暗号鍵が暗号機能の内部にある限り、エミュレータなどの外部エンティティは、その暗号鍵を悪用できず、TOEのセキュリティ方針が侵害されることはない。

(5) 実装に関わる補足

本PPは、TOEとなるICチップに特定の実装を規定しない。しかし、セキュリティ機能である暗号機能とその暗号機能へのアクセスを制御する機能は、採用するセキュリティメカニズムによっては、何らかの実装上の制約を伴うかもしれない。このような制約は、採用するメカニズムに依存するものであり、ST作成者によって考慮されるべきである。組込み機器ソフトウェアとそれを実行するハードウェアは、TOEと同一ICチップに実装してもよく、あるいは、組込み機器内の別のデバイスに実装してもよい。

本TOEでは、ICチップ内部に暗号機能が搭載される。この暗号機能とは、暗号アルゴリズム演算回路のほか、データ入出力・鍵管理用レジスタ、乱数生成器など、暗号演算に必要な周辺回路を含む。ICチップの他の構成要素には、CPU、メモリ、I/Oインタフェースなどが考えられる。これら構成要素は、暗号機能と同一ICチップに実装しても、別チップに実装してもよい。

(6) エミュレータに関わる補足

TOE運用環境におけるエミュレータ接続を説明する。TOEが搭載される組込み機器には、ICカードリーダライタのような可搬型小型装置から据え付け型大型装置まで、多様な製品形態がある。組込み機器では、運用・管理手段としてのエミュレータ接続が行われることがある。エミュレータは、組込み機器の外部端子に接続され、組込み機器内部のハードウェア資源にアクセスする。エミュレータは、保守・管理手段として有用である一方、セキュリティ上の問題となる恐れがある。なお、本PPでは、組込み機器内部に外部からアクセス可能な装置を包括的にエミュレータと呼ぶが、同様の装置がデバッガと呼ばれることもある。

### 1.2.5 Construction of the TOE

TOEの実装構成はPPでは規定されず、開発者の設計方針に委ねられる。しかし、読者の理解促進を目的とし、TOE構成の一例を図1-1に示す。この構成例は、1.2.4に例示したセキュリティメカニズムに基づくものである。この例では、暗号機能へのアクセスを制御するため、二つのゲート（HWゲート/SWゲート）が使用される。CPU、メモリ、各種周辺回路は、同一のICチップに含まれる。組込み機器ソフトウェアも、同じICチップに搭載される。

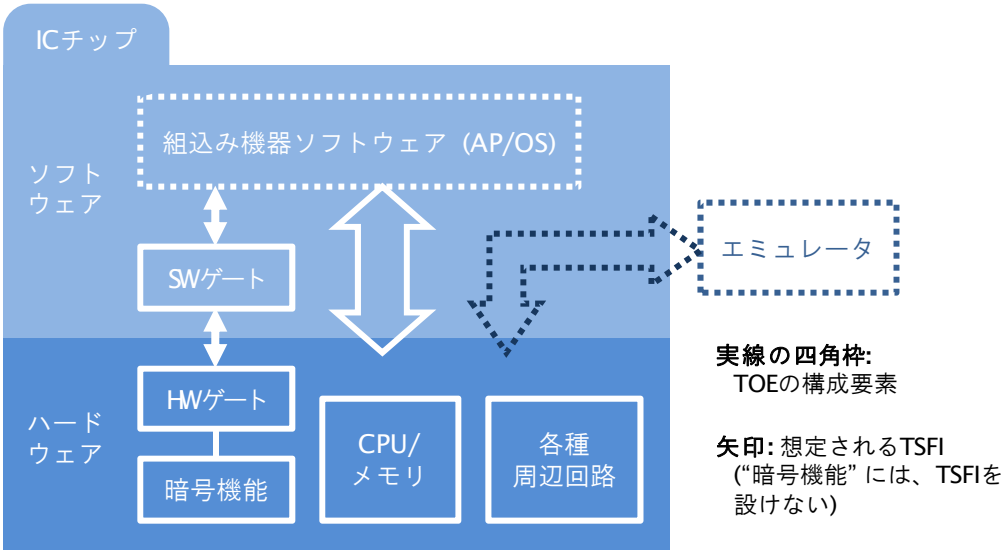


図1-1 TOEの構成例

図1-1に示す構成エレメントの動作を説明する。

暗号機能は、ハードウェアで実現される。組込み機器ソフトウェアは、TOE（TOE構成要素を実線の四角枠で示す）の上位に位置し、SWゲートとHWゲートを介して暗号機能を使用する。SWゲートとHW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る。SWゲートとHWゲートは、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を示す。

図1-1に示されるTOEの他のエレメント（CPU/メモリ、各種周辺回路）は、SFRを直接実施するものではないが、SFRの実施を支援するか、あるいはSFRの正確な実施に影響を及ぼすことがある。従って、それらもまたTSFの一部である。

ICチップ外部に接続されたエミュレータは、TOEのハードウェアにアクセスすることができる。ICチップ内のソフトウェア（組込み機器ソフトウェアあるいはSWゲート）からアクセス可能なハードウェアには、エミュレータからもアクセス可能である。ハードウェアの暗号機能は、ソフトウェアあるいはエミュレータから直接アクセスすることはできず、HWゲートを介したアクセスだけが可能である。組込み機器ソフトウェアあるいはエミュレータに対するTOEのインタフェースは、TSFIと呼ばれる。

TOEの動作を以下に示す。上述したように、図1-1は、実装の一例である。SWゲートやHWゲートと表示されたエレメントは、TOEの実装に依存するもので、必須機能ではない。

SWゲートとHWゲートは、TOE外部エンティティによる暗号機能へのアクセスを制御する。外部エンティティとは、組込み機器ソフトウェアとエミュレータである。組込み機器ソフトウェアによるアクセスは、正当かつ許可されるべきアクセスである。エミュレータによるアクセスは、TOEのセキュリティ方針を侵害する恐れがあり、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。

それらを区別する一つの方法は、組込み機器ソフトウェアの持つ特性を利用することである。組込み機器ソフトウェアの各サービスにおける処理パターンは、あらかじめ決まっている。従って、暗号機能に対するアクセスが所定の処理パターンかどうかを調べれば、暗号機能へのアクセスを許可するかどうかを判定できる。

SWゲートとHWゲートは、次のように動作する。HW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、HW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HW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。

SWゲートは、HWゲートの状態遷移を管理する情報を提供する。組込み機器ソフトウェアが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ものである。このアクセスパターンに伴うHWゲートの内部状態遷移をあらかじめ計算し、暗号化してSWゲートに格納する。SWゲートは、組込み機器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HWゲートの次の内部状態遷移データ（暗号化されている）を共にHWゲートへ転送する。HWゲートは、渡された内部状態遷移データ復号し、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。SWゲートからHWゲートへ渡す内部状態遷移データは、HWゲートが持つ共通暗号鍵で暗号化されており、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、暗号化した内部状態遷移データを提供できず、HWゲートによってアクセスを拒否される。

### 1.2.6 Lifecycle of the TOE

TOEのライフサイクルは以下のように定義される。この並び順は、必ずしも時系列に沿ったものではない。

TOEのライフサイクルは、TOEの実現方法、例えばハードウェアとソフトウェアの機能分担、開発体制などによって異なる。本章は、TOEの理解を助けるための参考として記述するものである。本PPを参照するST作成者は、実際のTOEに基づき、ライフサイクル記述を変更することができる。

(1) ICチップハードウェア開発

ハードウェア開発者によるICチップの開発。この工程は、さらにIC回路設計、ICマスク設計に分割され、それぞれ異なる開発者によって行われることもある。

(2) アクセス制御ソフトウェア開発

アクセス制御機能をソフトウェアで構成する場合のプログラム開発。アクセス制御機能の一部または全部をハードウェア化してもよい。すべてをハードウェアで構成する場合、このライフサイクルステップは省略される。

アクセス制御を実行するメカニズムは本PPで規定されないので、TOE開発者によって異なる実現方法が用いられるかもしれない。実現方法は、組込み機器ソフトウェアのサービス内容に依存するものとなるかもしれない。

(3) 組込み機器ソフトウェア（OS・AP）開発

ICチップに組み込まれるOS・APの開発。OS・AP開発は、それぞれを異なる開発者が行うかもしれない。APは、組込み機器の用途に応じて開発される。OS・APは、TOE外である。

(4) ICチップ製造

ICチップ製造工程。ICチップが製造され、(2) で開発されたアクセス制御機能が組み込まれ、(3) で開発された組込み機器ソフトウェアがTOE内のROMあるいは不揮発性メモリ上に搭載される。なお、ソフトウェアの一部あるいは全部は、この工程ではなく、(5) でTOEに搭載されてもよい。製造されたICチップは、開発者テストを経て製品となる。

(5) 組込み機器へICチップ搭載

組込み機器開発者によって、ICチップが組込み機器へ搭載される。この開発工程は、ICチップを搭載するプリント基板の開発、それを実装する組込み機器の開発の二つに区分されるかもしれない。完成した最終製品は、消費者へ配付される。

(6) 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、想定する運用環境下で使用される。本PPが想定する脅威は、この運用フェーズで発生する。

# 2 Conformance claims

## 2.1 CC conformance claims

本PPは、以下のとおりCC適合を主張する。

- CC適合: CC Version 3.1 Revision 4適合

  Part 1: Introduction and general model September 2012 Version 3.1 Revision 4 CCMB-2012-09-001

  Part 2: Security functional components September 2012 Version 3.1 Revision 4 CCMB-2012-09-002

  Part 3: Security assurance components September 2012 Version 3.1 Revision 4 CCMB-2012-09-003

- パート2適合: CC Part2拡張

  拡張するセキュリティ機能コンポーネントを第5章に定義する。

- パート3適合: CC Part3適合

## 2.2 PP claim

本PPは、以下のとおりPP適合を主張する。

PP適合: なし

## 2.3 Package claim

本PPは、以下のとおりパッケージ適合を主張する。

パッケージ適合: EAL4適合

## 2.4 Conformance rationale

本PPは、他のPPへの適合を主張しないので、適合根拠の記述はない。

## 2.5 Conformance statement

本PPへの適合を主張するPP/STは、論証適合を主張しなくてはならない。

# 3 Security problem definition

## 3.1 Protected assets and users

### 3.1.1 Protected assets

TOEの保護資産とは、TOEのセキュリティ機能（TSF）及び環境によって保護される情報資産である。CCパート1では、保護資産を、「TOEの所有者が価値を認めると推定されるもの(entities that the owner of the TOE presumably places value upon)」と定義している。本TOEの所有者は、TOEを組み込んだ組込み機器の所有者と推定される。組込み機器において、TOEは上位の組込み機器ソフトウェアにサービスを提供し、その組込み機器ソフトウェアが組込み機器としてのサービスを利用者に提供する。つまり、TOE所有者が価値を認めるのは、組込み機器ソフトウェアが提供する利用者へのサービス、あるいは組込み機器ソフトウェアが扱う利用者データなどである。TOEは、組込み機器ソフトウェアに暗号機能を提供することによって、間接的に、組込み機器ソフトウェアのサービスや利用者データ保護に貢献する。

TOEの暗号機能は、組込み機器ソフトウェアが利用者に提供するサービスの一環で使用される。例えば、組込み機器ソフトウェアが機器間相互認証を実行するのであれば、TOEは、相互認証のための暗号演算を実行する。組込み機器ソフトウェアが利用者データの機密性・完全性を保護するのなら、TOEの暗号機能は、利用者データの暗号化・復号、あるいはMAC付与・検証の機能を提供する。もし、攻撃者がTOEの暗号機能を悪用すると、組込み機器ソフトウェアの利用者サービスの信頼が失われる。つまり、TOEにとって、暗号機能の正しい使用を保証することが重要である。TOEの暗号機能が不正に使用されないことがTOE所有者にとっての価値となり、TOEの直接的な保護資産となる。

攻撃者は、保護資産を攻撃する手段として、TSF、あるいはTSFが使用するデータ（TSFデータ）を攻撃するかもしれない。TSFやTSFデータが侵害されると、保護資産は十分に保護されない。そのため、PPに脅威として明示しなくても、TSFとTSFデータは適切に保護されねばならない。これらは、本来の保護資産に対して、「二次資産」と呼ばれる。

### 3.1.2 Users

TOEの利用者とは、CCパート1によれば、TOEと対話するTOE外のエンティティをいう。利用者は、TOEが提供する外部インタフェース（TSFI）を介してTOEにアクセスする。

本TOEの利用者は、以下に示すとおりである。

| | |
|---|---|
| 組込み機器ソフトウェア | TOEが提供する暗号機能、及びそれ以外のTOEハードウェア資源を利用する。暗号機能の利用は、TOEが正しく利用された場合に限り許可される。正しい利用とは、組込み機器所定の動作パターンに沿った暗号機能の利用を指す。組込み機器ソフトウェアは、この所 |

定の動作パターンを正しく実行するので、TOEの暗号機能の利用が許可される。組込み機器ソフトウェアはTOEの正当な利用者であり、TOEに対する有害な動作は行わない。

エミュレータ　TOEを搭載するICチップの外部から、TOE内部のハードウェア資源に直接アクセス可能な装置。“エミュレータ”の呼称は、同様の機能を提供するIT装置（“デバッガ”など）全般を意味するものとする。エミュレータは、組込み機器ソフトウェアを介さずにTOEのハードウェア資源にアクセスするので、エミュレータが悪用されるとTOEに有害な動作をする。TOEのセキュリティ機能によって、エミュレータによる暗号機能の不正な利用を防がねばならない。

## 3.2 Threats

本TOEに関して、対抗すべき脅威を示す。これらの脅威は、TOE、その運用環境、あるいは両者の組み合わせによって対抗されねばならない。

**Application note [Threats]**　本章に示される脅威は、組込み機器向けICチップに共通的な脅威である。もし、TOE固有の特性に応じて生じる脅威があれば、ST作成者は、その脅威を追加すべきである。その場合、追加する脅威に対応して、セキュリティ対策方針、セキュリティ機能要件記述の追加修正が必要である。

以下の脅威は、TOE外部インタフェースからの論理的攻撃である。

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。

以下の脅威は、ICチップの物理的特性に関わる攻撃である。

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、乱数の品質に依存する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。 |

## 3.3 Organisational security policies

| | |
|---|---|
| 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。 |

**Application note [~~OSP~~P.Cryptography]** TOEの用途によっては、TOEの暗号機能に特定の暗号アルゴリズムが要求されるかもしれない。必要であれば、組織のセキュリティ方針として暗号アルゴリズムを特定できる。

## 3.4 Assumptions

なし

# 4 Security objectives

3章に示したセキュリティ課題に対して、TOE及びその環境におけるセキュリティ対策方針を示す。セキュリティ対策方針は、TOEによって対処するものを4.1に、その環境によって対処するものを4.2に記載する。さらに、これらのセキュリティ対策方針がセキュリティ課題に対して適切であることの根拠を4.3に示す。

TOEのセキュリティ対策方針、運用環境のセキュリティ対策方針は、それぞれ、先頭に“O.”、“OE.”を付与した識別名で表す。

## 4.1 Security objectives for the TOE

セキュリティ課題として定義された脅威と組織のセキュリティ方針に関して、課題解決のためにTOEが対処すべきセキュリティ対策方針を示す。

O.Internal-Access　TOEに接続されるエミュレータが暗号機能を不正に使用するのを防ぐため、TOEは、正当な組込み機器ソフトウェアだけに暗号機能の使用を許可しなければならない。ただし、外部エンティティ（組込み機器ソフトウェア・エミュレータを問わず）による暗号機能の使用が不正使用にあたらない場合は許可してもよい。

[注釈] [O.Internal-Access]　組込み機器ソフトウェアは、ひとつのサービスの開始から終了までの一連の処理を実行する過程で暗号機能を使用する。この暗号機能の使用では、セキュリティ侵害が生じない。もし、エミュレータがこの処理と全く同一手順で暗号機能を使用した場合、TOE動作は組込み機器ソフトウェアによる使用と同一であるから、セキュリティ侵害は生じない。なお、この注釈は、実現方法の特定を意図するものではない。

O.Leak-Inherent　TSFは、TOE外部から観測できる電力消費の変動（TOEの電源端子への流入電流あるいはTOEから漏洩する電磁波）が暗号演算に関わる内部処理との相関関係を持ち、その相関関係が分析されて暗号演算に使用した暗号鍵が暴露されることを防ぐ対策をとらねばならない。

O.Phys-Probing　TSFは、TSFを構成するハードウェア回路部分に対するプロービングを妨げる対策をとらねばならない。対策例には、プロービングを

物理的に困難にする回路構造、プロービング検出によるTOE動作停止などがある。

O.Malfunction TSFは、組込み機器ソフトウェアやTSF自身の誤動作・機能不全を防ぐため、環境ストレスの影響を軽減しなければならない。対策手段の例は、フィルタや電磁シールドでストレスを軽減する、あるいは、センサでストレスを検出し、TOE動作を停止する等である。これら適切な対策手段によって、T.Malfunctionに示された利用者データの暴露、組込み機器サービスの妨害を防止できる。

O.Phys-Manipulation TSFは、TSFに関わる回路部分の物理的操作を妨げるか、あるいは、物理的操作によるTOE内データの改変を防ぐ対策をとらねばならない。さらに、TSFは、攻撃者がTSFに関わる回路部分を解析するのを困難にする対策をとらねばならない。

O.RND TSFは、セキュリティ機能のメカニズムが必要とする品質を持ち、かつ攻撃者の予測が困難な乱数を提供しなければならない。

O.Cryptography TSFは、外部エンティティから利用できる暗号機能を提供しなければならない。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。

## 4.2 Security objectives for the operational environment

運用環境に関わるセキュリティ対策方針はない。

## 4.3 Security objectives rationale

本章では、上述のセキュリティ対策方針がセキュリティ課題定義の各項目に対して有効であることの根拠を示す。4.3.1では、各々のセキュリティ対策方針がいずれかのセキュリティ課題にさかのぼれること、4.3.2では、各々のセキュリティ課題が対応するセキュリティ対策方針によって有効に対処されることを説明する。

### 4.3.1 Correspondence between SPDs and objectives

セキュリティ課題定義とセキュリティ対策方針の対応を表4-1に示す。ここに示すとおり、すべてのセキュリティ対策方針は、一つ（以上）のセキュリティ課題定義の項目にさかのぼることができる。

表4-1　セキュリティ課題定義とセキュリティ対策方針の対応

| セキュリティ課題定義 ＼ セキュリティ対策方針 | O.Internal-Access | O.Leak-Inherent | O.Phys-Probing | O.Malfunction | O.Phys-Manipulation | O.RND | O.Cryptography |
|---|---|---|---|---|---|---|---|
| T.Internal-Access | x | | | | | | |
| T.Leak-Inherent | | x | | | | | |
| T.Phys-Probing | | | x | | | | |
| T.Malfunction | | | | x | | | |
| T.Phys-Manipulation | | | | | x | | |
| T.RND | | | | | | x | |
| P.Cryptography | | | | | | | x |

### 4.3.2 Sufficiency of the security objectives

TOEのセキュリティ対策方針によって、識別された脅威及び組織のセキュリティ方針がすべて十分に対抗あるいは実施されることの根拠を示す。

T.Internal-Access　攻撃者は、エミュレータを使用してTOE内部にアクセスし、暗号機能を悪用しようとする。O.Internal-Accessによって、TOEは、暗号機能の正しい利用だけを許可する。すなわち、組込み機器の所定の処理に沿った暗号機能の利用だけが許可される。攻撃者は、組込み機器の所定の処理以外の方法でTOEの暗号機能を悪用することはできない。その結果、暗号機能で保護された組込み機器ソフトウェアの保護資産が侵害されることはない。O.Internal-Accessによって、脅威が十分に軽減される。

T.Leak-Inherent　O.Leak-Inherentが実施されれば、暗号演算処理回路の動作電力変化パターンと暗号演算内容の相関を観測・分析することが困難になり、暗号演算に使用する秘密鍵が分析され暴露されるのを防止でき

| | |
|---|---|
| | る。O.Leak-Inherentによって、T.Leak-Inherentの脅威が十分に軽減される。 |
| T.Phys-Probing | O.Phys-Probingが実施されれば、物理的プロービングによる保護対象データの暴露を防止でき、T.Phys-Probingの脅威が十分に軽減される。 |
| T.Malfunction | O.Malfunctionが実施されれば、TOEにおける環境ストレスの影響を軽減できる。その結果、利用者データの暴露や組込み機器ソフトウェアの実行妨害（いずれも、TOEが関与する部分について）を防止でき、T.Malfunctionの脅威が十分に軽減される。 |
| T.Phys-Manipulation | O.Phys-Manipulationが実施されれば、物理的操作による保護対象データの改変を防止でき、さらに、攻撃者がTSFに関わる回路部分を解析するのを防止できる。O.Phys-Manipulationによって、T.Phys-Manipulationの脅威が十分に軽減される。 |
| T.RND | O.RNDが実施されれば、TSFが生成する乱数の品質がセキュリティメカニズムに必要とされるものとなる。O.RNDによって攻撃者による乱数値予測が困難になり、T.RNDの脅威が十分に軽減される。 |
| P.Cryptography | O.Cryptographyは、TSFが外部エンティティに暗号機能を提供し、外部エンティティが保護資産を暴露や改ざんから保護したり、あるいは、他のIT装置と相互認証を行ったりするのを支援する。O.CryptographyはP.Cryptographyを直接支持しており、P.Cryptographyが適切に実施される。 |

# 5 Extended components definitions

本PPでは、拡張セキュリティ機能要件を記述するため、CCパート2に含まれない拡張コンポーネントを定義する。

## 5.1 Extended security functional components

本PPで定義する拡張コンポーネントとそれを含むファミリを5.1.1に示す。この拡張ファミリ、拡張コンポーネントは、CCパート2（セキュリティ機能コンポーネント）の既存クラスであるFCSクラスに属する。これらは、CCパート2のファミリ及びコンポーネントをモデルとして構成された。

### 5.1.1 Definition of the Family FCS_RNG

TOEの一部である暗号機能が実施する暗号演算の一つに、乱数生成がある。乱数は、共通鍵暗号の鍵生成、セキュアな鍵交換、相互認証などに使用される。攻撃者から予想されにくい、十分なエントロピーを持つ乱数生成が必要である。CCパート2には乱数生成要件を規定するコンポーネントがないので、乱数生成に関わる拡張コンポーネントを定義する。本項では、まず“FCS_RNG”ファミリを定義し、そのファミリに属する拡張コンポーネントを定義する。これら拡張ファミリと拡張コンポーネントは、以下のPPから引用されたものである。

“Security IC Platform Protection Profile” Version 1.0, 15.06.2007; BSI-PP-0035

以下は、同PPの定義の再現である。

To define the IT security functional requirements of the TOE an additional family (FCS_RNG) of the Class FCS (cryptographic support) is defined here. This family describes the functional requirements for random number generation used for cryptographic purposes.

**FCS_RNG Generation of random numbers**

Family Behaviour

This family defines quality requirements for the generation of random numbers which are intended to be use for cryptographic purposes.

Component leveling:

| | |
|---|---|
| FCS_RNG: Generation of random numbers | 1 |

FCS_RNG.1 Generation of random numbers requires that random numbers meet a defined quality metric.

Management: FCS_RNG.1

There are no management activities foreseen.

Audit: FCS_RNG.1

There are no auditable events foreseen.

### FCS_RNG.1 Random number generation

Hierarchical to: No other components.
Dependencies: No dependencies.

**FCS_RNG.1.1 The TSF shall provide a [selection: *physical, non-physical true, deterministic, hybrid*] random number generator that implements: [assignment: *list of security capabilities*].**

**FCS_RNG.1.2 The TSF shall provide random numbers that meet [assignment: *a defined quality metric*].**

**Application note [EX_FCS_RNG.1]** A physical random number generator (RNG) produces the random number by a noise source based on physical random processes. A non-physical true RNG uses a noise source based on non-physical random processes like human interaction (key strokes, mouse movement). A deterministic RNG uses a random seed to produce a pseudorandom output. A hybrid RNG combines the principles of physical and deterministic RNGs.

# 6 Security requirements

## 6.1 Security functional requirements

本PPで規定するSFRは、CCパート2に含まれるコンポーネントに5章で定義する拡張コンポーネントを追加したものである。表6-1にSFRのリストを示す。

表6-1 SFRリスト

| 章番号 | 識別名 | |
|---|---|---|
| 6.1.1 | FCS_CKM.1 | Cryptographic key generation |
| 6.1.2 | FCS_CKM.4 | Cryptographic key destruction |
| 6.1.3 | FCS_COP.1 | Cryptographic operation |
| 6.1.4 | FCS_RNG.1 | Random number generation |
| 6.1.5 | FDP_IFC.1 | Subset information flow control |
| 6.1.6 | FDP_IFF.1 | Simple security attributes |
| 6.1.7 | FPT_PHP.3 | Resistance to physical attack |
| 6.1.8 | FPT_TST.1 | TSF testing |

それぞれのセキュリティ機能コンポーネントに必要な操作を施すことによってSFRを規定する。操作内容は、各SFRにおいて、以下の表記方法で示される。

- 割付あるいは選択操作の箇所を[割付: ×××(斜体)]、[選択: ×××(斜体)]の形式で示す。詳細化部分も斜体で示すが、本PPでは詳細化を行っていない。
- 選択操作において、選択対象外の項目を抹消線（~~抹消線~~）で示す。
- 本PPでは、一部の操作が未了であり、その個所を[割付: ×××(斜体・下線)]の形式で示す。ST作成者は、未了部分の操作を完了せねばならない。

以下、本PPで規定するSFRを示す。

### 6.1.1 FCS_CKM.1 Cryptographic key generation

Hierarchical to: No other components.
Dependencies: [FCS_CKM.2 Cryptographic key distribution, or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

**FCS_CKM.1.1** **The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: *cryptographic key generation algorithm*] and specified cryptographic key sizes [assignment:**

***cryptographic key sizes*** **] that meet the following: [assignment: *list of standards*].**

### 6.1.2 FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other components.
Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]

**FCS_CKM.4.1** **The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [assignment: *cryptographic key destruction method*] that meets the following: [assignment: *list of standards*].**

### 6.1.3 FCS_COP.1 Cryptographic operation

Hierarchical to: No other components.
Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

**FCS_COP.1.1** **The TSF shall perform [assignment: *list of cryptographic operations*] in accordance with a specified cryptographic algorithm [assignment: *cryptographic algorithm*] and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*].**

### 6.1.4 FCS_RNG.1 Random number generation

Hierarchical to: No other components.
Dependencies: No dependencies.

**FCS_RNG.1.1** **The TSF shall provide a [selection: *physical,* ~~*non-physical true, deterministic, hybrid*~~] random number generator that implements: [assignment: *list of security capabilities*].**

**FCS_RNG.1.2** **The TSF shall provide random numbers that meet [assignment: *a defined quality metric*].**

**Application note [FCS_RNG.1]** Refer to “the application note [EX_FCS_RNG.1]” in Chapter 5: Extended components definitions.

FCS_RNG.1.1: ST authors shall select and define appropriate parameters to address the security mechanisms implemented on the TOE.

The assignment can be completed with none or security capabilities needed for the random number generator, such as “total failure test of the random source”.

FCS_RNG.1.2: ST authors shall define the quality metric sufficient to prevent prediction of random numbers by an attacker to the degree that the security mechanism needs.

An example of quality metric for random numbers is quantified entropy level using “Min-entropy” or “Shannon entropy”. It depends on the use for the TOE or the embedded device.

### 6.1.5 FDP_IFC.1 Subset information flow control

Hierarchical to: No other components.
Dependencies: FDP_IFF.1 Simple security attributes

**FDP_IFC.1.1** **The TSF shall enforce the [assignment: *embedded device information flow control SFP*] on [assignment:**
**<*subjects*> *the cryptographic function of the TOE,***
**<*information*> *command data to the subject and response data from the subject,***
**<*operations*> *input of command data, execution of cryptographic operation and output of response data*].**

### 6.1.6 FDP_IFF.1 Simple security attributes

Hierarchical to: No other components.
Dependencies: FDP_IFC.1 Subset information flow control
FMT_MSA.3 Static attribute initialisation

**FDP_IFF.1.1** **The TSF shall enforce the [assignment: *embedded device information flow control SFP*] based on the following types of subject and information security attributes: [assignment:**
**<*subjects*> *the cryptographic function of the TOE,***
**<*information*> *command data to the subject and response data from the subject,***
**<*security attributes of the subjects*> *reference data* to verify authenticity of command data,***
**<*security attributes of the information*> *properties relevant to the command data; the attributes provide the TSF with capability verifying the authenticity of the command data*].**

**FDP_IFF.1.2** **The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [assignment: *only if the authenticity of the command data is successfully***

***verified by the security attributes, the information flow of the command data to the subject and/or the response data from the subject, which is the outcome of cryptographic operation, will be permitted*]**.

**FDP_IFF.1.3** **The TSF shall enforce the [assignment: *"additional information flow control SFP rules:" none*].**

**FDP_IFF.1.4** **The TSF shall explicitly authorise an information flow based on the following rules: [assignment: *"rules, based on security attributes, that explicitly authorise information flows:" none*].**

**FDP_IFF.1.5** **The TSF shall explicitly deny an information flow based on the following rules: [assignment: *"rules, based on security attributes, that explicitly deny information flows:" none*].**

* "Reference data" is used for verification of command data. For example, "predicted correct processing pattern" at 1.2.4 (3) corresponds to it. The whole "predicted correct processing patterns" are generated by the developer of the embedded device software and stored in the TOE at the developer's environment. It is the TSF data and must be protected not to be exploited by an attacker.

### 6.1.7 FPT_PHP.3 Resistance to physical attack

Hierarchical to: No other components.
Dependencies: No dependencies.

**FPT_PHP.3.1** **The TSF shall resist [assignment: *the physical tampering scenarios in the following list*] to the [assignment: *the hardware, the firmware and/or the software composing of the TSF*] by responding automatically such that the SFRs are always enforced.**

**[The list of the physical tampering scenarios]**

- **Physical attacks with microelectronic tools to access the inside of the TOE to extract data/signals, modify data/circuitry or acquire the construction information of the TOE exploitable for the subsequent attacks**
- **Overcoming sensors and filters to deactivate or avoid the protection functionalities of the TOE**
- **Perturbation attacks to change the normal behaviour of the TOE in order to create an exploitable error in the operation of the TOE**
- **Retrieving keys with DFA**
- **SPA/DPA to analyze cryptographic algorithm and retrieve keys**
- **Higher order DPA to defeat countermeasures for first order DPA**
- **EMA attacks to bypass countermeasures for SPA/DPA**
- **Attacks on RNG to get the ability to predict the output of the RNG**

**Application note [FPT_PHP.3]** These physical tampering scenarios are derived from the CCRA supporting document "Application of Attack Potential to Smartcards, May 2013 Version 2.9 CCDB-2013-05-002". Physical tampering attacks are carried out without undergoing the TSFI of the TOE.

### 6.1.8 FPT_TST.1 TSF testing

Hierarchical to: No other components.
Dependencies: No dependencies.

**FPT_TST.1.1** **The TSF shall run a suite of self tests [selection: *during initial start-up, periodically during normal operation, at the request of the authorised user, at the conditions [assignment: conditions under which self test should occur]*] to demonstrate the correct operation of [selection: *[assignment: parts of TSF], the TSF*].**

**FPT_TST.1.2** **The TSF shall provide authorised users with the capability to verify the integrity of [selection: *[assignment: parts of TSF data], TSF data*].**

**FPT_TST.1.3** **The TSF shall provide authorised users with the capability to verify the integrity of [selection: *[assignment: parts of TSF], TSF*].**

## 6.2 Security assurance requirements

本TOEに適用するセキュリティ保証要件は、表6-5に示す保証コンポーネントで定義される。これらは、すべて、CC パート3に含まれる。

表6-5に示すすべてのコンポーネントにおいて、本PPでは、操作を適用していない。

表6-5 保証コンポーネント

| Assurance class | Assurance components |
|---|---|
| Security target evaluation | ASE_CCL.1 |
| | ASE_ECD.1 |
| | ASE_INT.1 |
| | ASE_OBJ.2 |
| | ASE_REQ.2 |
| | ASE_SPD.1 |
| | ASE_TSS.1 |
| Development | ADV_ARC.1 |
| | ADV_FSP.4 |
| | ADV_IMP.1 |
| | ADV_TDS.3 |

| | |
|---|---|
| Guidance documents | AGD_OPE.1 |
| | AGD_PRE.1 |
| Life-cycle support | ALC_CMC.4 |
| | ALC_CMS.4 |
| | ALC_DEL.1 |
| | ALC_DVS.1 |
| | ALC_LCD.1 |
| | ALC_TAT.1 |
| Tests | ATE_COV.2 |
| | ATE_DPT.1 |
| | ATE_FUN.1 |
| | ATE_IND.2 |
| Vulnerability assessment | AVA_VAN.3 |

## 6.3 Security requirements rationale

### 6.3.1 Security functional requirements rationale

本章では、定義されたSFRがTOEのセキュリティ対策方針を適切に達成することの根拠を示す。6.3.1.1では、各々のSFRがいずれかのTOEのセキュリティ対策方針にさかのぼれること、6.3.2.2では、各々のTOEのセキュリティ対策方針が対応する有効なSFRによって適切に満たされることを説明する。

#### 6.3.1.1 Correspondence between the security objectives and the SFRs

TOEのセキュリティ対策方針に対応するSFRを表6-6に示す。この表は、すべてのSFRが少なくとも一つのTOEのセキュリティ対策方針にさかのぼれることの根拠となる。

表6-6　TOEセキュリティ対策方針とSFRの対応

| TOE security objectives ＼ SFRs | FCS_CKM.1 | FCS_CKM.4 | FCS_COP.1 | FCS_RNG.1 | FDP_IFC.1 | FDP_IFF.1 | FPT_PHP.3 | FPT_TST.1 |
|---|---|---|---|---|---|---|---|---|
| O.Internal-Access | | | | | x | x | | x |
| O.Leak-Inherent | | | | | | | x | x |
| O.Phys-Probing | | | | | | | x | x |
| O.Malfunction | | | | | | | x | x |
| O.Phys-Manipulation | | | | | | | x | x |
| O.RND | | | | x | | | x | x |
| O.Cryptography | x | x | x | x | | | | x |

#### 6.3.1.2 Sufficiency of the SFRs

TOEのセキュリティ対策方針がそれに対応づけられるSFRによって満たされることの根拠を示す。個々のSFRがTOEのセキュリティ対策方針を満たす上での有効性を持つことも同時に示される。

O.Internal-Access

このセキュリティ対策方針では、エミュレータなど、組込み機器ソフトウェア以外の外部エンティティがTOE内部のハードウェアにアクセスし、TOEの暗号機能を権限なく使用するのを防止する。正当な外部エンティティである組込み機器ソフトウェアの暗号機能の使用は許可される。この目的を達成するため、以下のSFRが規定される。

CCパート2では、FDP_ACFとFDP_IFCの二つのファミリがアクセス制御要件に対応する。FDP_ACFファミリはサブジェクトによるオブジェクトの操作を規定し、FDP_IFCファミリでは、サブジェクトへの情報入出力を規定する。このいずれかのファミリを使用すれば、O.Internal-Accessが要求する、組込み機器ソフトウェア及びエミュレータによる暗号機能へのアクセス制限を規定できる。

エミュレータは、TOE外からTOEの内部バスを介して暗号機能にアクセスする。組込み機器ソフトウェアも、同様にTOE外のエンティティである。FDP_ACFファミリは、サブジェクトとオブジェクトがTOE内に存在するケースに適用するので、TOE外のエミュレータや組込み機器ソフトウェアを管理する要件には適用しにくい。一方、FDP_IFCファミリは、暗号機能をサブジェクトとし、サブジェクトに対する情報入出力（暗号機能へのコマンド入力、レスポンス出力）を制御する要件を記述できる。そのため、O.Internal-Accessを記述するコンポーネントとして、FDP_IFC.1/FDP_IFF.1を要件定義に使用する。

これらSFRは、外部エンティティ（組込み機器ソフトウェア、エミュレータ）による暗号機能の操作要件を規定する。暗号機能へ入力されるコマンドデータの正当性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レスポンスデータが出力される。すなわち、暗号機能の正しい利用だけが受け入れられる。

TSFがこれらのSFRを満たすには、TSF自身が正しく動作することが条件となる。TSFの正しい動作を確認するSFRとして、FPT_TST.1が規定される。FPT_TST.1は、O.Internal-Accessを満たすSFRを支援する要件である。

これらSFRによって、O.Internal-Accessが適切に満たされる。

O.Leak-Inherent

動作中のTOEでは、処理に伴って内部回路の消費電流が変化する。攻撃者は、この電流変化から暗号演算処理を分析し、使用された暗号鍵を推測する。電流変化は、ICチップの電源端子で観測でき、あ

るいは、電流変化に伴う外部漏洩電磁波から観測できる。この攻撃は、DPA/SPAとして知られる。

この攻撃に対抗するため、TOEは、O.Leak-Inherentによって、暗号演算に伴う電力消費変動を観測しにくくする対策を講じる。このセキュリティ対策方針には、FPT_PHP.3が対応する。FPT_PHP.3に示された物理的攻撃シナリオのうち、SPA/DPA、Higher order DPA、EMAがTOEのハードウェアに対する直接的・間接的な接触によって動作中のTOE消費電力変化を観測しようとする攻撃に相当する。

TSFがこのSFRを満たすには、対抗策に関わるTSFのパーツが正しく動作することが必要である。そのTSFパーツの正しい動作を確認するSFRとして、FPT_TST.1が規定される。FPT_TST.1は、O.Leak-Inherentを満たすSFRを支援する要件である。

これらSFRによって、O.Leak-Inherentが適切に満たされる。

O.Phys-Probing

O.Phys-Probingは、TOEの内部に物理的に接触し、利用者データを攻撃したり、他の攻撃に利用できる情報を取得したりする脅威に対抗することを目的とする。O.Phys-Probingには、FPT_PHP.3が対応する。FPT_PHP.3に記載された物理的攻撃のシナリオのうち、“Physical attacks with …”がO.Phys-Probingに記載されたセキュリティ対策方針をカバーする。

TSFがこのSFRを満たすには、対抗策に関わるTSFのパーツが正しく動作することが必要である。そのTSFパーツの正しい動作を確認するSFRとして、FPT_TST.1が規定される。FPT_TST.1は、O.Phys-Probingを満たすSFRを支援する要件である。

これらSFRによって、O.Phys-Probingが適切に満たされる。

O.Malfunction

O.Malfunctionは、組込み機器ソフトウェアやTSFの正常な動作を阻害し、その結果として、保護された情報資産の機密性や完全性を侵害する脅威に対抗する。O.Malfunctionには、FPT_PHP.3とFPT_TST.1が対応する。FPT_PHP.3に記載された物理的攻撃のシナリオのうち、“Perturbation attacks”と“Retrieving keys with DFA”では、電磁波やレーザーなどの高エネルギー印加や電源へのグリッチ印加などによって、暗号機能や組込み機器ソフトウェアに予期しないふるまいを生じさせる。FPT_PHP.3は、これらの攻撃に自動的に対応し、TOEの正常な動作を維持する。攻撃への有効な対抗手段は、センサによる攻撃検出（TOEを停止）、フィルタや電磁シールドによる影響の軽減である。

上記対抗手段に伴い、その対抗手段への物理的攻撃シナリオ“Overcoming sensors and filters”が想定され、同様に

FPT_PHP.3によって自動的に対応される。対抗手段は、攻撃検出によるTOE停止などである。FPT_TST.1は、センサやフィルタの完全性のテストを要求し、FPT_PHP.3が適切に実施されることを支援する。

これらSFRによって、O.Malfunctionが適切に満たされる。

O.Phys-Manipulation

O.Phys-Manipulationは、TOEの内部の物理的操作によって、直接情報資産を攻撃したり、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。O.Phys-Manipulationには、FPT_PHP.3が対応する。FPT_PHP.3に記載された物理的攻撃のシナリオのうち、“Physical attacks with ...”がO.Phys-Manipulationに記載されたセキュリティ対策方針をカバーする。

TSFがこのSFRを満たすには、対抗策に関わるTSFのパーツが正しく動作することが必要である。そのTSFパーツの正しい動作を確認するSFRとして、FPT_TST.1が規定される。FPT_TST.1は、O.Phys-Manipulationを満たすSFRを支援する要件である。

これらSFRによって、O.Phys-Manipulationが適切に満たされる。

O.RND

O.RNDは、TSFの生成する乱数を攻撃者に予測させにくくすることが目的である。これに対応するSFRは、FCS_RNG.1とFPT_PHP.3である。FCS_RNG.1は、乱数生成器のセキュリティ能力、乱数生成メカニズム、生成される乱数の品質尺度を定義し、これらの要件を満たすことによって、攻撃者の乱数予測を防止する。FPT_PHP.3の“Attacks on RNG”は、RNGに対する物理的攻撃への対抗を要求する。

TSFがこのSFRを満たすには、対抗策に関わるTSFのパーツが正しく動作することが必要である。そのTSFパーツの正しい動作を確認するSFRとして、FPT_TST.1が規定される。FPT_TST.1は、O.RNDを満たすSFRを支援する要件である。

これらSFRによって、O.RNDが適切に満たされる。

O.Cryptography

O.Cryptographyは、外部エンティティに暗号機能の使用を提供する。暗号操作は、FCS_COP.1で規定される。暗号操作に使用される暗号鍵の生成と破棄は、FCS_CKM.1とFCS_CKM.4で規定される。暗号操作に関連して必要になる乱数生成は、FCS_RNG.1で規定される。

TSFがこれらのSFRを満たすには、TSFが正しく動作することが条件となる。TSFの正しい動作を確認するSFRとして、FPT_TST.1が規定される。FPT_TST.1は、O.Cryptographyを満たすSFRを支援する要件である。

これらSFRによって、O.Cryptographyが適切に満たされる。

#### 6.3.1.3 Dependencies of the SFRs

各SFRに規定された依存性とその対応状況を表6-7に示す。

表において、「依存性の要求」欄にはSFRに規定された依存性を示す。「依存性の対応」欄には、規定された依存性がPP中のどのSFRによって満たされるか、あるいは満たされない場合の正当性を示す根拠が記述される。

表6-7　SFRの依存性

| SFR | 依存性の要求 | 依存性への対応 |
|---|---|---|
| FCS_CKM.1 | [FCS_CKM.2または<br>FCS_COP.1]<br>FCS_CKM.4 | FCS_COP.1及び<br>FCS_CKM.4が対応し、依存性が満たされる。 |
| FCS_CKM.4 | [FDP_ITC.1または<br>FDP_ITC.2または<br>FCS_CKM.1] | FCS_CKM.1が対応し、依存性が満たされる。 |
| FCS_COP.1 | [FDP_ITC.1または<br>FDP_ITC.2または<br>FCS_CKM.1]<br>FCS_CKM.4 | FCS_CKM.1及び<br>FCS_CKM.4が対応し、依存性が満たされる。 |
| FCS_RNG.1 | なし | 不要 |
| FDP_IFC.1 | FDP_IFF.1 | FDP_IFF.1が対応し、依存性が満たされる。 |
| FDP_IFF.1 | FDP_IFC.1<br>FMT_MSA.3 | FDP_IFC.1が対応し、依存性を満たす。<br>FMT_MSA.3は、「情報のセキュリティ属性」の管理を規定する。本TOEでは、この属性は、TOE外で生成されるコマンドデータの属性であり、TOEの管理対象でない。そのため、FMT_MSA.3は適用されない。 |
| FPT_PHP.3 | なし | 不要 |
| FPT_TST.1 | なし | 不要 |

### 6.3.2 Security assurance requirements rationale

TOEが搭載される組込み機器は、高度のセキュリティが必要な用途も想定され、商用製品として十分に高い評価保証レベルであるEAL4が適用されるかもしれない。TOEには、組込み機器を下回らない評価保証レベルが求められるので、保証要件をEAL4とする。

# 7 Terms and definitions

## 7.1 Terms and definitions in the CC

PP Protection Profile: TOEの種別に対するセキュリティニーズについての実装に依存しないステートメント。

CC Common Criteria; IT装置のセキュリティ評価基準。CCと同一の内容がISO/IEC 15408規格としても制定される。

ST Security Target: 識別された特定のTOEに対するセキュリティニーズについての実装に依存するステートメント。

TOE Target of Evaluation; 評価対象。ソフトウェア、ファームウェア、及び/またはハードウェアのセットであり、ガイダンスを伴うこともある。

TSF TOE security functionality; TOEのすべてのハードウェア、ソフトウェア、及びファームウェアが結合した機能性であり、SFRの正確な実施のために信頼されねばならないもの。

## 7.2 Terms and definitions related to the TOE

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。