サポート文書
必須技術文書

IC評価の実施要件

2013 年 5 月

バージョン 1.1

CCDB-2013-05-001

平成 26 年 8 月翻訳第 1.0 版
独立行政法人情報処理推進機構
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

IPA まえがき

はじめに

本書は、「IT セキュリティ評価及び認証制度」において、「認証機関が公開する評価基準」の規格として公開している Common Criteria Supporting Document (以下、CC サポート文書という)を翻訳した文書である。

原文

Requirements to perform Integrated Circuit Evaluations

Version 1.1
May 2013 CCDB-2013-05-001

まえがき

本書は、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、及びそれに関連する共通評価方法を補完することを目的としたサポート文書である。

サポート文書は、「ガイダンス文書」または「必須技術文書」でもある。「ガイダンス文書」は、規格適用の相互承認を必要としない分野への固有のアプローチや規格適用に焦点を当てる文書であり、そのため規格という性格のものではない。「必須技術文書」は、サポート文書の適用範囲に含まれる評価への適用が義務付けられている文書である。必須技術文書の使用は、必須であるだけでなく、それを適用した結果発行される認証書は、CCRAのもとで承認されている。

技術編集者：NLNCSA

改訂履歴：
V1.1　2013年5月（PP参考文献の更新）
V1.0　2009年9月（CCRAサポート文書からCCサポート文書に変更、CCDB-2009-03-001－スマートカードへの攻撃能力の適用v2-7サポート文書と整合性を取るために更新）

全般的な目的：
ハードウェア製品とソフトウェア製品の両方のセキュリティ特性は、CCに従って認証できる。以降の各章では、共通の認識を持ち、現在の最先端のハードウェア評価に適合する方法でCCをハードウェアICに確実に適用できるように、共通評価方法[CEM]に加え、CC保証作業パッケージの個々の側面に関するガイダンスを示す。

特殊用途の分野：スマートカード及び類似デバイス

謝辞：

以下に示される政府組織は、Joint Interpretation Working Groupに所属し、このコモンクライテリアサポート文書の本バージョンの作成に貢献した。

フランス： *Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)*
ドイツ： *Bundesamt für Sicherheit in der Informationstechnik (BSI)*
オランダ： *Netherlands National Communications Security Agency (NLNCSA)*
スペイン： *Centro Criptológico Nacional (CCN)*
英国： *Communications-Electronics Security Group (CESG)*

また、以下の組織に加入しているスマートカードベンダ、評価機関、その他の企業による作業の貢献に対して感謝の意を表する。

- *International Security Certification Initiative (ISCI)*
- *JIL Hardware Attacks Subgroup (JHAS)*

目次

1 根拠

1 コモンクライテリア評価方法[1]は附属書A.5で、監督（制度）機関にガイダンスを提供し、制度で指定することを選択する場合がある主題を特定している。これらの主題の1つは、すべての制度が技術的能力を検証する手段を持つように、評価が十分に行われたことを保証する場合の特定の要件に関連する。この主な目標は、すべての評価機関が適格で、かつ、互角である制度を保証することである。

2 CCRAは、評価機関が、法律や規則の下に設立されていない場合は、EN 45001またはISO ガイド 25（現在はISO 17025に取って代わられた）に従って認定されることを要求している。さらに、CCRAは、評価機関がITセキュリティ評価の特定分野において技術的に有能であるという認証機関の達成を実証することを要求している。

3 認定の要件はISO/IEC 17025 [2]に記載されており、特に第5章に、技術的スキル及び利用できる必要な機器の要件が記載されている。

4 この手続きは、IC評価を実施するための認証機関の技術認定及びライセンスのガイドラインを提供することを目的としている。これは、欧州制度間の適用を調和させる責任を負うEuropean Joint Interpretation Working Group (JIWG)内で作成及び承認されている。

2 序説

5 コモンクライテリアに従ってスマートカード集積回路(IC)の評価からの信用できる結果を保証するために、ITセキュリティ評価機関（ITSEF）は最低限の一連の能力を持たなければならない。これらの能力は、必要な機器と、評価者に必要なスキル及び知識の両方において、ソフトウェアシステムに必要な能力と異なる。

3 必要な知識及びスキル

3.1 概要

6 評価者に必要な知識及びスキルは、以下のように分類できる。

- スマートカード設計と一般の生産プロセス、及びIC設計と製造プロセスに関する理解力（3.2節を参照）。
- スマートカード技術、その基本原理、及びIC製造者に使用される開発機器に関する理解力（3.3節を参照）。
- スマートカードの不正使用及び攻撃シナリオに関する知識。
- IC故障解析の知識と経験、基本的な物理的原理の理解、及び関連機器を使用するための能力（3.4節を参照）。
- 暗号攻撃技法の知識と経験、及び解析を実施する能力(データ収集ならびに信号処理手順を含む)(3.4節を参照)。

7 さらに、ITSEFは、IC故障解析、その他の様々なスマートカード攻撃技法、及び暗号攻撃技法に関連する機器を必要とする（3.4節を参照）。必要なツールは、標準（基本）、特殊、及び特別注文に分類できる（3.5節を参照）。

3.2 IC設計及び生産プロセス

8 ICのハードウェア及びソフトウェアは一般に、様々な会社で開発される。その後、これらのコンポーネントは組み込まれ、追加のセキュリティ関連データがカードに挿入される。

9 ICのセキュリティ上の目的は、以下の2つの要素からなる。

- 現場にあるカードのセキュリティレベルを保証する。
- 開発及び生産プロセスを通じてセキュリティレベルを維持する。

10 多くの専門家が現場のセキュリティに焦点を合わせているが（スマートカードが敵意のある無秩序な環境に配付され、改ざんされやすい可能性があるため）、開発、生産、及びパーソナリゼーションプロセス中のセキュリティも重要である。スマートカードコンポーネントが評定されるセキュリティ目標は、生産及びパーソナリゼーションプロセスに応じて異なる可能性があるアプリケーションの範囲に大きく依存する。特に、パーソナリゼーションは、スマートカードによって提供されるセキュリティ機能に影響を与える。

11 コモンクライテリアは、要件の定義をはじめとして、続いて、設計プロセス、実装、テスト、受入れ、配付、及び利用を記述する。コンポジット製品のコンポーネントを考慮する場合、このプロセスは解釈して再整理しなければならない。

12 例えば、チップ製造者はチップのハードウェア及びソフトウェアの設計を、テストできるように開発する。チップ製造者は、ソフトウェア開発者からソフトウェアを受け取り、ROMイメージを作成する。その後、マスクファイルはマスク製造者に送付される。マスクまたはレチクルはチップ製造者に返却される。

ウェハ生産後、チップをテストし、初期化データ（輸送鍵、追跡性データ）をE2PROM（または他の不揮発性メモリ）に導入する。初期化データは、カード製造者が定義する。動作ダイは、配付されるか、モジュールに直接組み込まれる。ダイ配付の保護は複雑になる可能性があり、認証メカニズムは、ソフトウェア製造者が実現するが、カード製造者（またはパーソナリゼーションセンター）が使用する。鍵はカード製造者が生成するが、カード製造者に規定された手続き（分散化等のため）を用いてチップ製造者がカードに導入する。

13 これらの例は、実際の開発プロセスが、コモンクライテリアで想定されるものよりも複雑である可能性があることを示している。入力及び出力は、必ずしもコモンクライテリアで予測されるほど単純ではない。結果として、コモンクライテリアの対応する保証コンポーネント（例えば、インスタンス配付）を必要に応じて、解釈、改良、及び再整理しなければならない。さらに、様々なコンポーネント（及びコモンクライテリア保証コンポーネントに関するそれらの記述）のプロセスが整合することを保証しなければならない。

14 評価者は、コモンクライテリア保証要件を適切な方法で解釈できるように、スマートカードのサプライチェーン及びそのアプリケーション範囲への組込みを理解しなければならない。特に、これらの保証要件は、以下の通りである。

- ガイダンス
- 配付
- 設置、生成、及び起動
- ツール及び技法
- ライフサイクルの定義
- 開発セキュリティ

15 さらに、標準ICの評価とソフトウェアの評価の違いは、クラスASE、ADV、ATE、及びAVAのコモンクライテリア保証コンポーネントの解釈も必要であることを意味している。

16 コモンクライテリア保証コンポーネントのこのような解釈、及び追加のガイダンスは、www.commoncriteriaportal.orgウェブサイトに公表されているスマートカードならびに類似デバイスの複数のCCサポート文書に記載されている。

17 評価者がスマートカードのIC設計及び製造プロセスも理解する必要があることに注意する。これは、各IC製造者が、そのような理解がないことを前提にプロセスやセキュリティ手段を記述していることが期待できないからである。

3.3 スマートカードのIC技術

18 評価者は、スマートカードのIC技術及び基本原理を、IC製造者の設計決定を把握するのに必要な程度まで理解しなければならない。以下の基本原理が必要である。

- 半導体（物理）の電子理論、及び半導体とトランジスタの電気的ふるまい
- IC製造に使用される標準物質（例えば、シリコン、ポリシリコン、金属、及び絶縁物質や保護物質）の物理的及ぶ電気的ふるまい

- 標準セル（単純ゲート）、メモリセル（E2PROM、RAM、ROM）、及びメモリブロックの物理的レイアウト（半導体基板上での実装）
- レイアウト原則、及び配線と多層化の方法
- 生産ステップ及び結果として生じるチップ表面上の層状構造

19 さらに、評価者は以下の詳細知識を持たなければならない。

- デジタル及びアナログ回路エンジニアリング（種々の複雑性を持つデジタルゲート、及び標準アナログ回路）
- デジタル及びアナログ回路の静的ならびに動的なふるまい
- マイクロコントローラのアーキテクチャ及び機能
- マイクロコントローラに使用される標準回路の実現

20 評価者は、回路図（ブロック図、ゲート及びトランジスタレベルの回路図）を理解できなければならない。機能コンポーネントは、標準回路図の形式、またはVHDLソースで記述できる。

21 評価者はVLSI設計の知識を持たなければならず、また、回路図またはVHDLソース（チップの論理的表現）から実際のレイアウト及びダイ/ウェハ（物理的表現）までのプロセスを基本的に理解しなければならない。評価者は、テクノロジ認定、機能テスト、特性評価、及び信頼性テストのプロセスを理解しなければならない。

22 評価者は、製造者がマイクロコントローラソフトウェア用に使用する開発機器を理解しなければならない。これには、シミュレータ、エミュレータ、及び特殊な評価ソフトウェアマスクが含まれる。評価者は、マイクロコントローラのソースコードの読み取り、及び侵入テストや他の検査の開発を実行できなければならない。このために、開発者は、CPU命令セット、メモリマップ、及びマイクロコントローラの他の周辺装置の使用方法を理解しなければならない。

3.4 スマートカード固有の攻撃

23 スマートカード固有の攻撃に関する概要を以下に説明する。これは完全なリストではなく、いくつかの例を示している。スマートカード固有の攻撃についての詳細は、本書の「附属書A：スマートカード特有の攻撃の例」を参照することができる。

24 評価者は標準的なスマートカードの不正行為及び攻撃シナリオを知らなければならず、原則として、そのような攻撃の新しいアイディアを開発できなければならない。さらに、評価者は、物理的な操作とプロービング、誤動作による攻撃、自発的および強制的な漏えい攻撃、テスト機能の悪用、暗号やソフトウェア攻撃（ここでは説明しない）などのICの攻撃シナリオに関して知らなければならない。

25 評価者は、評価を受ける個別のチップに対するこれらの攻撃シナリオを適応させ組み合わせることができなければならない。脆弱性分析時に、評価者は、潜在的な弱点を（回路図、チップ上でのその回路図の実現、及びそれらの組み合わせにおいて）見つけて、標準的な技法でそれらを評定することができなければならない。

26 評価者は、物理的な操作及びプロービングに使用されるIC故障解析の知識ならびに経験を持たなければならない。評価者は少なくとも、(3.5節で)「標準」及び「特殊」に分類される機器の物理的原理ならびに(必要に応じて)使用法を理解しなければならない。さらに、評価者は、トレーニングを受けた操作者の協力を得て「特別注文」ツールを使用できなければならない。評価者は、ICのセキュリティ特性及び機能にアクセスするために、これらのツールならびに技法を脆弱性分析時にどのように使用できるかについて知らなければならない。脆弱性評定に機器(特に、集束イオンビーム(FIB)、走査型電子顕微鏡(SEM)、または電子ビームテスタ)を使用する方法及び目的は、必ずしも操作担当者の期待に対応する必要はない。評価者は、操作担当者に指示すべきである。

27 評価者は、その他のスマートカード攻撃(差分電力解析(DPA)、差分電磁波解析(DEMA)、及び関連する攻撃など)、及びそのような攻撃を実行するために必要な機器(物理的ツールならびに解析ツール)に関する知識ならびに経験を持たなければならない。評価者は、この機器(データ収集手続きを含む)を操作できなければならず、また解析(数学)を実行できなければならない。暗号及び標準的な暗号攻撃技法の知識ならびに経験が必要である。タイミング攻撃及びその他の攻撃(差分故障解析(DFA)など)の原理が理解されなければならない。評価者は、そのような攻撃に関連する脆弱性を発見できなければならない。

28 評価者は、スマートカードと通信するためのソフトウェアを開発できなければならない。したがって、評価者は、サポートされるI/Oプロトコル、動作条件、及び外部コマンド(使用または攻撃される場合)を理解しなければならない。

29 評価者はチップカードリーダの取り扱い方法を知らなければならず、また、様々なパッケージ内のチップを使用したり、非標準の動作条件を適用したりするために、その取り扱い方法を変更できなければならない。このため、評価者は、電圧源、シグナルジェネレータ、ファンクションジェネレータ、オシロスコープ、はんだごてなどの標準機器を使用できなければならない。

3.5 ITセキュリティ評価機関(ITSEF)

30 ITセキュリティ評価機関(ITSEF)は、適切に組織化されて、評価者に指示を与えなければならない。これらの指示は、物理的、手続き的、及び組織上のセキュリティ手段を示したり、それらを他の文書を参照したりしなければならない。品質管理システムがなければならない。ISO/IEC17025の要件を満たさなければならない。3.4節に述べられている脆弱性分析と故障解析、物理的操作、及び攻撃シナリオを実行するために、ITセキュリティ評価機関は、それらの攻撃を実行するために必要なツールに制限なくアクセスできなければならず、また、それらのツールを効率的に使用できなければならない。これらの機器及びその分類の例を以下に示す。この分類の必要な機器の最新リストについては、CCサポート文書「スマートカードへの攻撃能力の適用」を参照すること。

31 標準機器、例:

- 紫外線発光体
- フラッシュライト
- 低性能の光学顕微鏡
- 環境試験装置

- 電圧源
- アナログオシロスコープ
- チップカードリーダ
- PCまたはワークステーション
- 信号解析ソフトウェア
- 信号生成ソフトウェア

32 特殊機器、例：

- 高性能の光学顕微鏡及びカメラ
- 紫外線顕微鏡及びカメラ
- マイクロプローブワークステーション
- レーザーカッター
- 信号及び機能プロセッサ
- 高性能デジタルオシロスコープ
- 信号アナライザ
- 化学エッチング用ツール（湿式）
- 化学エッチング用ツール（プラズマ）
- 研磨ツール

33 特別注文機器、例：

- 走査型電子顕微鏡（SEM）
- 電子ビームテスタ
- 原子間力顕微鏡（AFM）
- 集束イオンビーム（FIB）
- 新技術による設計検証及び故障解析ツール

34 光学顕微鏡及びカメラは、評定される技術に十分な倍率ならびに分解能を提供しなければならない。 マイクロプローブワークステーションには、適切な探針が装備されなければならない。供給機器（電圧源、信号及びファンクションジェネレータ）が利用できなければならない。

35 「特別注文」に分類される機器について、評価者は、基本的な物理的原理及びツールの機能をよく理解しなければならない。ITSEFがその他の施設を使用する場合、適切なセキュリティ手段を適用してチップベンダの情報とサンプル及びITSEFのノウハウを保護しなければならない。ITSEFが特別注文機器を借用する場合、評価者が同席して操作担当者に指示しなければならない。

3.6 専門のITセキュリティ評価機関への業務委託

36 ITSEFが作業を業務委託する場合、この作業は有能な下請者に委託しなければならない。有能な下請者とは、例えば、当該作業の国際規格に適合する下請者である。ISO/IEC 17025は、特定条件下での作業の業務委託を許可している。

4 まとめ

37 本書では、ITSEFがスマートカードICの評価を準備及び実行できる前に要求する知識、スキル、及び施設を記述する。これらの能力は、高性能型の機器、及びそれらの機器の使用方法に関する知識へのアクセスに限定されるのではない。さらに、ITSEF評価者は、スマートカードの設計及び生産プロセスを完全に理解すべきであり、新しい攻撃に対するテストを開発する能力を持つべきである。
この知識は、短期間のトレーニングでは身につけることができず、何年もの関連する経験を必要とする。

38 ITSEFが本書内のガイドラインを満たすと知らされている場合、信頼レベルが製造者（評価の費用を払う）と顧客（認証を受け入れる）の両方に提示される。これらのガイドラインがない場合、その信頼は、評価報告書の詳細情報を検査することによってしか推定できない（ただし、ITSEFの能力の最終測定は残る）。

5 文献

[1] ISO/IEC 17025：試験所及び校正機関の能力に関する一般要求事項

附属書A：スマートカード固有の攻撃の例

本書の目的は､ITSEFが評価中に実行すべきである攻撃のいくつかの例を提示することである。読者は、これが完全なリストでないことを理解すべきである。
以下の攻撃は、すべての種類の評価に適用できるわけではない（例えば、純粋なスマートカードのハードウェアは、特定のSWを装備したIC用のテスト以外のテストを受ける)。
スマートカードの潜在的な攻撃を理解するために、それらの攻撃の一般分類に関する簡潔な説明を以下に示す。

1 物理的変更

攻撃の特徴：
攻撃が侵襲的で、チップが物理的に変化する。

攻撃の目的：
2つの主な目標：

A) 許可なしに情報を抽出する
B) ICのふるまいを変更する

一般的方法：
攻撃者は物理層を除去し（全体的または局所的に)、対象デバイスあるいは配線を暴露し、配線をオープンにし、それに接触する。さらに、攻撃者は、回路のふるまいを変更するために配線またはデバイスを変更（切断、新たに接続）する場合がある（Bの場合の通り)。
対象は、アクティブデバイス及び接続ラインである。 多くの場合、攻撃者は、デバイスを破壊せずにこれらの物理的操作を適用しなければならない。
これらの方法の適用を成功させるには、ほとんどの場合、デバイスの改変を（少なくとも部分的に）実行する必要がある。

スキル及びツール：
基本的に、どちらの場合でも必要なスキルとツールは同じである。攻撃対象デバイスの技術及びレイアウトの詳細に応じて、必要なスキルとツールの選択ならびに高度化は大きく異なる場合がある。Bの場合の攻撃では、攻撃対象デバイスに関するより深い知識が必要である。

スキル：

- 例えば、機械的（研磨)、化学的（乾式または湿式エッチング)、局所的蒸発（レーザー）の選択除去（全体または一部）
- 接触パッドのデバイス及び接続ラインへの適用
- 局所的に非常に制限されている可能性のある領域の接触デバイス及び接続ライン（直接的に、または適用された接触パッドを介して）
- 回路または接続ラインの再配線（主にBの攻撃の場合）
- 電気信号の適用及び解析

ツール：

- エッチング機器（単純な湿式エッチング機器から高性能のプラズマエッチング機器まで多種多様）
- プローブステーション（単純なものから小型新技術の高性能のものまで）
- 顕微鏡
- オシロスコープ
- レーザーカッター
- FIB
- ロジックアナライザ
- PC及びソフトウェア（デバイスの制御用）
- インタフェースハードウェア（大部分がデバイス及び攻撃に合わせてカスタマイズ）

PPの例：

BSI-PP-0035	物理的な不正操作：T.Phys-Manipulation 強制的な情報漏えい：T.Leak-Forced

参考文献：

- Usenix Workshop on Smartcard Technology 1999: *Design Principles for Tamper-Resistant Smartcard Processors*. Markus Kuhn, Oliver Kömmerling. ISBN1-880446-34-0
- F.Beck: *Integrated Circuit Failure Analysis – A Guide to Preparation Techniques*. John Wiley & Sons, 1998
- T.W. Lee, S.V. Pabbisetty: *Microelectronic Failure Analysis, Desk Reference*. 3rd edition, ASM International, Ohio, 1993, ISBN 0-87170-479-X
- R.J. Anderson, M.G. Kuhn: *Tamper Resistance – a Cautionary Note. In The Second USENIX Workshop on Electronic Commerce Proceedings*, pp. 1 – 11, Oakland, California 1996
- J.H. Daniel, D.F. Moore, J.F. Walker: *Focused Ion Beam for Microfabrication*, Engineering Science and Education Journal, pp 53 – 56, April 1998

2 リバースエンジニアリング（観察）

攻撃の特徴：

この種類の攻撃は、チップの内部構造、チップの構成ブロックの場所と機能、及びそれらの内部接続を特定することを目指している。

攻撃の目的：

主な目的は、チップの構造、及びチップの構成ブロックの内部動作に関する詳細情報とそれらの内部接続を特定しようとすることである。

こうして、物理的攻撃の準備作業が行われる（プロービング、セキュリティ機能のプロービング、内部情報の抽出、ふるまいの変更）。

一般的方法：

- 以下のような多数のステップを実行する。
- ハウジングからチップを取り外し、チップのダイ表面が外観検査できるようにする。
- 層数、金属シールド、バス設計(スクランブル)、センサを特定する。
- 層を次々に取り外す。
- 個々の層を画像化する。
- 層の画像を解釈及び組み合わせて、個々のコンポーネント(CPU、メモリ、I/O、セキュリティロジック、センサ)ならびにそれらの相互関係を導き出す。

スキル及びツール：

- チップの設計及びアーキテクチャに関する知識
- エッチング技法に関する知識－エッチング液、被膜剥離、研磨ホイール
- 顕微鏡
- 写真または画像処理－マイクロ写真機器、画像処理機器

PPの例：

BSI-PP-0035	物理的なプロービング：T.Phys-Probing 物理的な不正操作：T.Phys-Manipulation 強制的な情報漏えい：T.Leak-Forced

参考文献：

- Usenix Workshop on Smartcard Technology 1999: *Design Principles for Tamper-Resistant Smartcard Processors*. Markus Kuhn, Oliver Kömmerling. ISBN1-880446-34-0
- F.Beck: *Integrated Circuit Failure Analysis – A Guide to Preparation Techniques*. John Wiley & Sons, 1998
- T.W. Lee, S.V. Pabbisetty: *Microelectronic Failure Analysis, Desk Reference*. 3rd edition, ASM International, Ohio, 1993, ISBN 0-87170-479-X
- R.J. Anderson, M.G. Kuhn: *Tamper Resistance – a Cautionary Note*. In The Second USENIX Workshop on Electronic Commerce Proceedings, pp. 1 – 11, Oakland, California 1996
- J.H. Daniel, D.F. Moore, J.F. Walker: *Focused Ion Beam for Microfabrication*, Engineering Science and Education Journal, pp 53 – 56, April 1998

3 暗号解析（DPA、DEMA、DFA）

攻撃の特徴：
この種類の攻撃は、スマートカードを観察しながら秘密に関わるデータを取得することを意図している。DPA/DEMA及びDFAの2つのクラスの技法を説明する。

3.1 DPA/DEMA

攻撃の目的：
2つの主な目的：

- スマートカードの電力消費量または電磁波放射を観察することによって情報へアクセスする。
- 秘密に関わるデータ、共通鍵及び秘密鍵を取得する。

一般的方法：
この方法は非侵襲的である。この方法は、カードに吸収される電力やカードに放射される電磁波放射などの有用な情報を記録する。その後、これらの記録された信号（トレース）は、統計的技法を用いて処理される。

スキル及びツール：

- 電圧源
- 信号及び機能プロセッサ
- アナログオシロスコープ
- デジタルオシロスコープ
- チップカードリーダ
- PCまたはワークステーション
- 信号アナライザ
- 信号収集及び処理ツール
- 電磁波放射用アンテナ（DEMA）

信号処理には、一般の評価機関用の機器が必要である。DEMAを実行するには、関連する電磁信号を取得及び測定するためのセンサが必要である。必要な知識は、暗号、信号解析、電磁波放射特性を指す。知識及びスキルの必要なレベルは、攻撃の特性ならびに正確な方法により異なる。中レベルからエキスパートレベル（高度な技法を使用する場合）まで多様である場合がある。
また、DPA/DEMAに必要なものは、(i) 攻撃対象の暗号アルゴリズムに関する深い知識、(ii) 信号収集及び処理用の特殊ソフトウェア、ならびに(iii) 統計解析の知識とソフトウェアである。

3.2 DFA

攻撃の目的：
この攻撃は、スマートカードから共通鍵を取得することを目的とする。

一般的方法：

この方法は、スマートカードが暗号計算を実行している間に誤りを引き起こすことによって、スマートカードから秘密情報を取得することを目的とする。こうして、誤った暗号文（暗号化動作の妨害から生じた暗号文）と正しい暗号文の、2種類の暗号文が取得される。
両方の種類の暗号文を比較すると、使用された暗号鍵に関する情報が明らかになる場合がある。

スキル及びツール：

- カードの暗号化動作中に単一故障を差し込むことができる電子機器
- 電圧源
- 信号及び機能プロセッサ
- アナログオシロスコープ
- デジタルオシロスコープ
- チップカードリーダ
- PCまたはワークステーション
- 信号収集及び処理ツール
- 信号生成ソフトウェア

必要な知識は、暗号、信号解析、及びチップ内部動作に関する高度な知識を指す。

PPの例：

BSI-PP-0035	自発的な情報漏えい：T.Leak-Inherent 機能の悪用：T.Abuse-Func 環境ストレスによる誤動作：T.Malfunction

参考文献：

P.Kocher, J.Jaffe, B. Jun, *“Differential Power Analysis”*, in Proceedings of Advances in Cryptology – CRYPTO99, Springer-Verlag, 1999, pp 388-397,
TS.Messerges, E.A. Dabbish and Robert H.Sloan, *“Investigations of Power Analysis Attacks on SmartCards”*, in Proceedings of Usenix Workshop on SmartCard Technology, May 1999, pp. 151-161,
E.Biham, A.Shamir, *Differential Fault Analysis of Secret Key Cryptosystems*, in Proceedings of CRYPTO’97, Lecture Notes in Computer Science, Vol. 1294, Springer, pp 513-528, 1997.
R.Anderson, M.Kuhn, *Low Cost Attacks on Tamper Resistant Devices*, in Proceedings of Security Protocols, 5th International Workshop, Paris, France, April 7-9, 1997, Lecture Notes in Computer Science, Vol. 1361, Springer, pp. 125-136, 1997.

4 プロトコル攻撃

攻撃の特徴：

この種類の攻撃は、スマートカードのプロトコル実装の欠陥を探す。

攻撃の目的：
スマートカードプロトコルは、スマートカードとの通信の可能性を指定する。このプロトコルは、スマートカードが秘密に関わる動作を実行する条件を定義する。
主な目的は、スマートカードがサポートするプロトコルに適合しないスマートカードの機能を見つけることである。言い換えれば、プロトコルに指定されない秘密に関わる動作をスマートカードが実行するかどうかを調べる。

一般的方法：
この枠組みでは、以下の事項に注意を払う。

- リプレイ攻撃
- スマートカードがコマンドを実行している間にスマートカードの動作を中断する。
- 文書化されていないコマンド（スマートカードに実行されるが文書化されていない「危険な」コマンドがあるか?）
- ファイル走査（ファイルのアクセス制御は、述べられている通りに実装されているか?）
- 文書化されていないコマンドシーケンス（スマートカードは、プロトコルで許可されていないコマンドシーケンスをサポートしているか?）

スキル及びツール：

- スマートカードプロトコルに関する知識
- PC、スマートカードリーダ、テストソフトウェア

PPの例：

BSI-PP-0035	機能の悪用：T.Abuse-Func

5 観察攻撃

攻撃の特徴：
この攻撃は非侵襲的である（チップは変化しない）。
この種類の攻撃は、スマートカードを観察しながら秘密に関わるデータ（一般に、定義された資産の特性に応じた共通鍵及び秘密鍵）を取得することを意図している。
例えば、タイミング攻撃（タイミング所見）、SPA、DPAの種類の攻撃など、スマートカードの直接的な所見から情報を取得するための様々な技法がある。
SPA攻撃を以下に説明する。

例：SPA攻撃（単純電力解析）
この攻撃は、スマートカードの電力消費量の直接解析に相当する。この攻撃の目的は、実行中のCPU命令セット、パラメタ（入出力）を反映した消費電力のレベルから、例えば共通鍵または秘密鍵の値を決定することである。ネイティブスマートカード実装により、暗号アルゴリズム部分が外部から可視的になる場合がある。この詳細情報は、共通鍵及び/または秘密鍵の値を取得する場合に役立つことがある。

攻撃の目的：

2つの主な目的：

- スマートカード出力信号を観察することによって情報にアクセスする
- 単純な方法または高度な統計的方法を用いて秘密性に関わるデータ、共通鍵及び秘密鍵を取得する

一般的方法：
通常、この方法は、時間、入出力、具体的な発生時の電源信号などの有用な情報の記録であり、また、これらの記録の悪用ならびに解析である。
これには、信号処理用の一般的な認証機関の機器、及び一般の信号処理技法の知識が必要である。

スキル及びツール：
通常、これらのツールは以下のものである。

- 電圧源
- 信号及び機能プロセッサ
- アナログオシロスコープ
- デジタルオシロスコープ
- チップカードリーダ
- PCまたはワークステーション
- 信号アナライザ
- 信号解析ソフトウェア
- 信号生成ソフトウェア

必要なスキルは、攻撃の特性及び正確な方法により異なり、熟練したレベルからエキスパートレベル（高度な技法を使用する場合）まで多様である場合がある。

PPの例：

BSI-PP-0035	自発的な情報漏えい：T.Leak-Inherent

6 ソフトウェア攻撃

攻撃の特徴：
この種類の攻撃は、スマートカードのソフトウェア誤動作を検査する。
これらの攻撃を実行する技法は多数ある。その中には、悪意のあるソフトウェアのロード、不正なフォーマットのコマンドがあり、そのすべてがスマートカードのセキュリティ欠陥を悪用する。

攻撃の目的：
主な目的は、スマートカードのセキュリティメカニズムを回避し、ソフトウェアのセキュリティ欠陥を悪用しようとすることである。

一般的方法：
攻撃者は、不正なソフトウェア（オペレーティングシステム、実行可能ファイル）またはセキュリティデータ（認証情報、鍵、アクセス制御情報）をTOEにロードする場合があり、これによって、ソフトウェアまたはTOE上のデータが変更されたり暴露されたりする可能性がある。

攻撃者は、システム開発者やアプリケーション開発者に配付される、仕様書に従って働かなかったり、セキュリティ欠陥を含んでいたり、動作使用に適していなかったりするコードを悪用する。攻撃者、またはTOEの正当なユーザは、無効な入力の導入を通じてTOEのセキュリティ機能を危殆化する場合がある。

スキル及びツール：
関連するツールは通常、スマートカードに対してコマンドを起動する基本ツールであり、低レベルの専門知識から非常に高度なエンジニアリング技法までの幅広いスキルが必要とされる。

PPの例：

BSI-PP-0035	PPの範囲にないスマートカード組込みソフトウェア。

7 かく乱攻撃

攻撃の特徴：
ストレス条件下のICは、予想外の方法で動作する可能性がある。ソフトウェアの正常なふるまいが変化する可能性がある。

攻撃の目的：
ICをストレス条件下（例えば、正常な電源範囲外にしたり、ICに光を当てたりする）に置くことによって、ソフトウェアの正常なふるまいが変化する可能性がある。この結果、テストが逆になったり、ジャンプが生成されたり、メモリからの読み取りデータが変更されたりする場合がある。これらの変更によって、攻撃者は、例えば、保護されたメモリにアクセスしたり、保護された動作を実行する権限を取得したりすることができる場合がある。

一般的方法：
かく乱を適用する一般的な方法は、DFA攻撃と同じである。ICをかく乱する様々な方法には、グリッチ、光、レーザーなどがある。スマートカードを正常な電源範囲外にするために加熱または冷却する特殊機器も使用される。

スキル及びツール：
- カードの暗号化動作中に単一故障を注入することができる電子機器
- 電圧源
- 信号及び機能プロセッサ
- アナログオシロスコープ
- デジタルオシロスコープ
- チップカードリーダ
- PCまたはワークステーション
- 信号収集及び処理ツール
- 信号生成ソフトウェア
- フラッシュライト発生器、レーザー機器

PPの例：

BSI-PP-0035	環境ストレスによる誤動作：T.Malfunction 強制的な情報漏えい：T.Leak-Forced

付録B：略語

IC	：	集積回路
FIB	：	集束イオンビーム
DPA	：	差分電力解析
DEMA	：	差分電磁波解析
DFA	：	差分故障解析
EM	：	電磁気
SPA	：	単純電力解析