2015.03.31
2018.02.02 *1更新

解説書

はじめに

本書は、経済産業省平成　26　年度サイバーセキュリティ経済基盤構築事業（ハードウェアの脆弱性分析技術）により、電子商取引安全技術研究組合が受託した、HW セキュリティに対する脅威と脆弱性、セキュリティ対策及びこれらに関連する公開論文の DB（以下 DB と呼称する）を有効に活用するためのガイドブックである。

1. このガイドが対象とする読者

DB 及びこのガイドが対象とするのは、次の読者である。

- 組込機器のユーザ
- 組込機器のメーカ
- 組込機器部品のメーカ
- 半導体チップのベンダ
- セキュリティ評価・認証機関関係者
- 情報セキュリティ研究機関関係者

2. このガイドが対象とする情報処理機能の定義

本書において、情報セキュリティの対象とする情報処理機能を、次の通り定義する。

- 組込機器又はその部品に搭載されるシステム LSI（HW）とその上に搭載される SW（OS＋アプリケーション）
- ただし汎用 OS に依拠しない
- 暗号処理等セキュリティ機能の一部を HW 側に依拠している（たとえば、HW 暗号ライブラリを実装している）

3. 対象とする攻撃の範囲

本書において、HW 情報セキュリティの対象とする攻撃を、次の通り定義する。

- 2.において定義した、情報処理機能のHW 部分への攻撃を伴うもの（SW 部分だけに対する攻撃は対象としない）
- 攻撃者が直接対象にアクセスする攻撃であること（遠隔からの論理インターフェースを介する SW 攻撃については対象としない）

4. 攻撃類型

本書において、HW 情報セキュリティの対象とする攻撃の類型を、次の通り定義する。

4.1 Physical Attacks

4.2 Overcoming sensors and filters

4.3 Perturbation Attacks

4.4 Retrieving keys with DFA

4.5 Side-channel Attacks – Non-invasive retrieving of secret data

4.6 Exploitation of Test features

4.7 Attacks on RNG

4.8 Ill-formed Java Card applications

4.9 Software Attacks

4.10 Applet isolation

4.12 PUF(Physical Unclonable Function)*1

4.13 Machine Learning*1

4.15 Hardware Trojan*1

＜CC Supporting Document CCDB-2013-05-002 Version 2.9 Application of Attack Potential to Smartcards ＞より引用

ただし、4.8-4.10 の攻撃類型については、原則として 3 の定義外となる。
DB においては、各論文が取り扱う攻撃の種類が上記のどれに該当するか判別できる場合には、各々に 1-10 の攻撃類型番号を付している。

（攻撃類型番号は、上記の頭番号 4.を削除した下一桁の番号である）

読者は、DB の機能により、当該攻撃類型別の論文を抽出することができる。
DB においては、（当該論文が特定の攻撃類型に該当する場合）各論文の詳細情報欄に、その攻撃類型の解説と当該攻撃に対するよく知られた防御技術の例を付記している。ただし、当該論文 が扱う攻撃に具体的にどのような防御技術を以て対抗すべきかを示している訳ではない。
上記記事の英文は、Well known countermeasures をのぞき、CCDB-2013-05-002, Mandatory Technical Document, Application of Attack Potential to Smartcards を引用している。
上記記事の和文は概ね IPA 訳の CCDB-2013-05-002,必須技術文書 「スマートカードへの攻撃能力の適用」を引用したが、下線部については当組合で審議の上独自に訳出した。
なお CC サポート文書には、Well known countermeasures（よく知られた対策）の記載はない。この分は、当組合で独自に作成した。

*1 2017年度に攻撃類型に3分類を追加した。今回の論文追加で1～10に分類できない新しい攻撃類型がでてきたためである。

5. 論文の判別

DB においては、個別の論文を以下の通り判別し判別番号を付している。

- HW に対する攻撃、HW の脆弱性、HW の防御技術等を直接扱ったもの・・判別番号 1
- 暗号アルゴリズム等上記に関連した分野を扱った参考文献・・判別番号 2
- その他・・判別番号 3

読者は、DB の機能により、当該論文判別ごとに論文を抽出することができる。

6. 引用数

DB においては、個別の論文が、調査時点で他の論文に引用された件数を掲載している。

一般に、引用件数の多い論文には、セキュリティ上重要な情報を掲載しているものや、ある分野の

基礎的な文献が多く含まれている。また、発表年次が古く、引用が多数なされている論文は、一般に攻撃者が利用しやすいものであることに注意する必要がある。
読者は、DB の機能により、引用件数 50 件以上、または 100 件以上の論文を抽出することができる。

7. 情報処理機能の実装環境

2.に定義する情報処理機能は、多様な実装環境の中で組込機器に実装される。
その実装環境の類型を示したものが、下記である。

実装環境	環境Ⅰ	環境Ⅱ	環境Ⅲ	環境Ⅳ
定義	対象となる機器が一般に流通し、容易に攻撃者が多数入手可能	対象となる機器が移動可能で、攻撃者が入手可能	対象となる機器は移動可能だが、外部からの侵襲に物理的耐性を持つ	対象となる機器が、物理的に移動困難で、セキュアな環境によって保護されている場合
例	スマートカード 携帯電話・スマートホン SIM 等のメモリカード USB メモリ	自動車 金融端末機 ロボット 医療機器 警備機器	一部の金融端末機 外部からの侵襲時に内部情報の消去対策等を施した機器	厳重な人的警備区域内に固定されている移動不可能な機器

攻撃に対抗する防御策の強度は、上記の実装環境に依拠する。（一般に環境によるセキュリティ保 護の程度が強まるほど、情報処理部自体が施すべき防御策の程度は緩和される）
たとえば、3.に示した攻撃者が直接対象にアクセスする攻撃は、上記の環境Ⅳにおいてはかなり 困難である。

セキュリティ保証における、脆弱性分析の程度についても上記にある程度連動する。

8. 情報資産について

2.に定義した情報処理機能が守るべき情報資産の例と類型を示したものが下記である。

	資産Ⅰ	資産Ⅱ	資産Ⅲ	資産Ⅳ
定義	人命に直結するもの	個人・家庭の生活に重大な影響を及ぼすもの	個人・家庭の生活に一定の影響を及ぼすもの	個人・家庭の生活に軽微な影響を及ぼすもの
	国家の存立を脅かすもの	公的機関の活動継続に影響を及ぼすもの	高額の経済的価値を毀損するもの	一定額の経済的価値を毀損するもの

	多数市民の生活に重大な影響を及ぼすもの	企業法人の存立を脅かすもの	企業法人の活動継続に影響を及ぼすもの	企業法人の経済活動に一定の損害を与えるもの
システム例	重要インフラ（エネルギー、金融、通信等) 政府機関の情報システム	公的機関の情報システム 企業の情報システム スマートハウス	企業の情報システムの一部 電子マネーシステム 軽微な個人情報管理システム	ポイントシステム ゲームシステム
機器例	交通機器（自動車、飛行機等） 医療機器 一部のロボット 武器 重要な警備機器	スマートメータ 一部のロボット 補助的な警備機器 情報家電制御機器 駅務機器	公的機能を持つスマートカード クレジット・デビットカード ATM 等の金融機器・店舗用端末機 携帯電話・スマホ タブレット端末	前払い式電子マネー用カード 出退勤管理機 店舗用端末機等の一部
部品例	M2M モジュール等の部品は、それが実装され得る機器・システムの最高レベルの資産に準ずる			

攻撃に対抗する防御策の強度は、上記の情報資産に依拠する。（一般に資産価値の程度が高まるほど、情報処理部自体が施すべき防御策の強度も要求される）

セキュリティ保証における、脆弱性分析の程度についても上記にある程度連動する。

9. 攻撃類型と実装環境の関係

4.に示した攻撃類型と、7.に示した実装環境との関係を以下に示す。

実装環境	環境Ⅰ	環境Ⅱ	環境Ⅲ	環境Ⅳ
攻撃類型	対象となる機器が一般に流通し、攻撃者が容易に多数を入手可能	対象となる機器が移動可能で、攻撃者が入手可能	対象となる機器は移動可能だが、外部からの侵襲に物理的耐性を持つ	対象となる機器が、物理的に移動困難で、セキュアな環境によって保護されている場合
1. Physical Attacks	◎	○	△	×
2. Overcoming sensors and filters	◎	○	△	×

3. Perturbation Attacks	◎	○	△	×
4. Retrieving keys with DFA	◎	○	△	×
5.Side-channel Attacks – Non-invasive retrieving of secret data	◎	○	△	×
6. Exploitation of Test features	◎	○	△	×
7. Attacks on RNG	◎	○	△	×
8. Ill-formed Java Card applications	◎	○	○	△
9.. Software Attacks	◎	○	○	△
10. Applet isolation	◎	○	○	△
12. PUF*1	◎	◯	△	×
13.Machine Learning*1	◎	◯	◯	△
15.Hardware Trojan*1	◎	◯	◯	△

凡例：◎strong ○: medium △: low ×: none

10. セキュリティ保証

本書は、DB に掲載される各論文が示す脅威に、製造者、ユーザがどのような防御策を以て対抗すべきかについて、具体的な要求乃至推奨を行うものではない。
上記に替えて、ある時点において、ある製品が情報セキュリティ上必要なセキュリティ設計と実装を行っていることを保証する手段として、ISO/IEC15408（Common Criteria）に準拠した情報セキュリティ評価認証制度の活用を推奨することができる。
この制度は、国際相互承認のための機構である CCRA 加盟各国において運用されているが、2 に定義されている対象については、CCRA の全ての加盟国において評価認証されている訳ではなく、日本及び欧州 SOGIS（認証提供国は、フランス、ドイツ、イタリア、オランダ、ノルウェー、スペイン、スウェーデン、イギリス）各国が運用するハードウェアを対象とする CC 評価認証制度により、評価認証されている。
上記の制度においては、年々の攻撃防御技術の革新に対応しながら、当該時点で必要とされる程度のセキュリティ実装を対象製品が行っているかの脆弱性評定基準を、制度の内部で更新している。（このため、同一のセキュリティ保証レベルの認証が発行されても、認証発行日が異なれば、脆弱性評定基準も異なっている）

本書では、とくに 7.8.に示した製品の実装環境と情報資産の価値に注目して、ハードウェア CC 評価において取得すべきセキュリティ保証レベルを、下記の通り推奨する。
読者は、対象とする製品がどのような実装環境の下で使用され、どのような情報資産を守るかを特定し、下表において、推奨されるセキュリティ保証レベルを求め、そのいずれか高い方の値を、自らの取得すべき認証のセキュリティ保証レベルの目安とされることを推奨する。
（なお、下表におけるセキュリティ保証レベルは、CC 認証全体の保証レベル=EAL ではなく、CC 評価における AVA_VAN=脆弱性評定のレベルとして表示されている。DB に掲載される攻撃と防御、脆弱性に関する情報に直結する CC 評価の部分が、脆弱性評定だからである）

第 1 表 【組込機器例示*情報資産価値】

	資産Ⅰ	資産Ⅱ	資産Ⅲ	資産Ⅳ
定義	人命に直結するもの	個人・家庭の生活に重大な影響を及ぼすもの	個人・家庭の生活に一定の影響を及ぼすもの	個人・家庭の生活に軽微な影響を及ぼすもの
	国家の存立を脅かすもの	公的機関の活動継続に影響を及ぼすもの	高額の経済的価値を毀損するもの	一定額の経済的価値を毀損するもの
	多数市民の生活に重大な影響を及ぼすもの	企業法人の存立を脅かすもの	企業法人の活動継続に影響を及ぼすもの	企業法人の経済活動に一定の損害を与えるもの
システム例	重要インフラ（エネルギー、金融、通信等) 政府機関の情報システム	公的機関の情報システム 企業の情報システム スマートハウス	企業の情報システムの一部 電子マネーシステム 軽微な個人情報管理システム	ポイントシステム ゲームシステム
機器例	交通機器（自動車、飛行機等） 医療機器 一部のロボット 武器 重要な警備機器	スマートメータ 一部のロボット 補助的な警備機器 情報家電制御機器 駅務機器	公的機能を持つスマートカード クレジット・デビットカード ATM 等の金融機器・店舗用端末機 携帯電話・スマホ タブレット端末	前払い式電子マネー用カード 出退勤管理機 店舗用端末機等の一部
部品例	M2M モジュール等の部品は、それが実装され得る機器・システムの最高レベルの資産に準ずる			

第 2 表【情報資産価値*セキュリティ保証】

情報資産価値	資産Ⅰ	資産Ⅱ	資産Ⅲ	資産Ⅳ
セキュリティ保証	CC 等第三者評価による情報セキュリティ認証取得を推奨			
脆弱性評定推奨レベル	AVA_VAN.5	AVA_VAN.5	AVA_VAN.4	AVA_VAN.3

第 3 表【機器の実装環境*セキュリティ保証】

実装環境	環境Ⅰ	環境Ⅱ	環境Ⅲ	環境Ⅳ
定義	対象となる機器が一般に流通し、容易に攻撃者が多数入手可能	対象となる機器が移動可能で、攻撃者が入手可能	対象となる機器は移動可能だが、外部からの侵襲に物理的耐性を持つ	対象となる機器が、物理的に移動困難で、セキュアな環境によって保護されている場合
例	スマートカード 携帯電話・スマホ SIM 等のメモリカード USB メモリ	自動車 金融端末機 ロボット 医療機器 警備機器	一部の金融端末機 外部からの侵襲時に内部情報の消去対策等を施した機器	厳重な人的警備区域内に固定されている機器
セキュリティ保証	CC 等第三者評価による情報セキュリティ認証取得を推奨			ISMS 等による環境の保証で可
脆弱性評定推奨レベル	AVA_VAN.5	AVA_VAN. 4	AVA_VAN. 3	―
但し	情報資産による脆弱性評定値といずれか高い方を採用	情報資産による脆弱性評定値といずれか高い方を採用	情報資産による脆弱性評定値といずれか高い方を採用	情報資産による脆弱性評定値といずれか高い方を採用

【上表の使い方】

対象製品の保護する資産と実装環境を特定する。
第 2 表、第 3 表を参照し、特定された資産、実装環境がそれぞれ推奨する脆弱性評定レベルのいずれか高い方の値を採用する。

以上