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関する調査）

調査報告書

平成 27 年 3 月 31 日

電子商取引安全技術研究組合

目次

はじめに

0.1　定義

本報告書は、経済産業省の委託事業である「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）作成、及び DB 作成の過程で行った、攻撃、防御技術の分析整理等を記述したものである。。

この事業の成果が、我が国において、IC チップを実装した組込機器のハードウェアの脆弱性対策に貢献し、情報セキュリティ対策の向上に資することを期すると共に、関係各位の本事業成果活用を期待するものである。

0.2　事業の目的

事業の目的は、ハードウェアの脆弱性分析技術の研究結果を収集してデータベースを作成するとともに、脆弱性対策の提示等を行うこととし、もって我が国ハードウェア産業におけるセキュリティ対策の水準の向上を図り、産業競争力の強化に繋げることにある。

具体的には、ハードウェア脆弱性分析技術に関する研究報告の収集することにより、

- 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

などがシステム、機器、部品の設計開発やセキュリティ保証、学術研究の現場で、本事業の成果を活用し、最新の研究結果のみならず、過去の様々な脆弱性分析技術を踏まえた多面的な分析を行うことが期待され、我が国のハードウェア脆弱性分析技術の水準を向上させ、以て組込機器を用いたシステム、組込機器、組込機器の部品のセキュリティ向上に資するものである。

0.3　調査結果の概要

0.3.1　情報の収集

20 世紀末から現在に至る、組込機器に用いられるハードウェア（高等な論理回路を実装した IC チップ）のセキュリティ（攻撃技術、防御技術、脆弱性）に関する国内、国外の研究論文 1187 件の収集を行った。

詳細については、報告書本文第 3 章及び添付資料 3-1-1 を参照。

0.3.2　データベースの構築

データベースソフトウェア Microsoft Access を用いて、

- 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

などが、システム、機器、部品の設計開発やセキュリティ保証、学術研究の現場で利用しやすいように、データベースを構築した。

このデータベースには、前項で収集した 1187 件のデータを収録した。

また、本事業の成果を国際的に利用可能とするため、上記の英語版を作成した。

詳細については、報告書本文第 3 章及び添付資料 3-2-1,3-2-2 を参照。

0.3.3　解説書、同付属書類の作成

データベースの活用を促進するため、解説書と同付属書類を作成した。

解説書においては、対象とする読者、対象製品、対象とする攻撃の範囲、研究論文判別の基準、論文が他に引用された数等について解説すると共に、対象となるハードウェアを実装する組込機器の実装環境、対象が守るべき情報資産等について分析整理し、具体的な防御対策の提示に替えて、第三者評価認証制度の活用と認証されるべき脆弱性評定の程度について利用者に対して推奨を行っている。

また、本事業の成果を国際的に利用可能とするため、解説書のの英語版を作成した。

付属書類においては、具体的なデータベースの活用方法、とくに検索・絞り込み機能の使い方について解説している。

詳細については、本報告本文第 7 章、第 8 章及び 7-2-1,7-2-2、8-2 を参照。

1. HWV-WGの設置と運用

1.1 HWV-WG 委員の委嘱

事業の実施に当たり、当組合内に作業委員会(HWV-WGと呼称)を設置し、調査全般に関する討議と管理を行った。体制としては、ハードウェアの情報セキュリティ関連企業及び学識経験者によるものとした。

ハードウェアの情報セキュリティ関連企業:

当組合の組合員企業及び、当組合が事務局をつとめるICシステムセキュリティ協会CC評価認証部会（ICSS-JC）内の企業・団体に、HWV-WGへの参加を呼びかけた。

学者、有識者：

情報セキュリティに関する知見を有し、特にハードウェアへの暗号実装等に関心の深い電気通信大学崎山教授と、ハードウェア設計に関する知見を有し、情報セキュリティにも関心の深い神戸大学永田教授に委員を委嘱し、就任の承諾を得た。

1.2 WG の体制

HWV-WGの体制は次のとおり。

ＨＷＶ－ＷＧ委員	氏名	役職
ルネサスエレクトロニクス(株)	須藤祐介	技師
(株）東芝	川端健	研究主務
（独）産業技術総合研究所	堀洋平	主任研究員
(株）ＥＣＳＥＣ　Ｌａｂｏｒａｔｏｒｙ	山屋賢司	ＣＣ評価部長
(株）コスモスコーポレイション	佐藤誠	
パナソニックセミコンダクターソリューションズ（株）	佐藤勇樹	主任技師
神戸大学大学院	永田真	教授
電気通信大学	崎山一男	教授

（平成27年3月20日現在）

1.3 WG の開催と議事

1.3.1 第 1 回 HWV-WG

第1回HWV-WGは、平成26年12月19日(金)10:00-12:00、千代田プラットフォームスクウェア505会議室にて開催した。

討議事項:

- 在来データの確認
- 新規データのソースと例
- DBの仕様
- 実装環境と対策

1.3.2 第2回HWV-WG

第2回HWV-WGは、平成27年1月30日(金)10:00-12:00、千代田プラットフォームスクウェア504会議室にて開催した。

討議事項:

- データ収集状況
- 欧州各国からの連絡
- 論文の判別
- 攻撃類型の判別
- アルゴリズムの判別
- 防御対策の提示
- 解説書の作成
- 各委員作業分担
- DB初版のデモ

1.3.3 第3回HWV-WG

第3回HWV-WGは、平成27年2月19日(木)15:30-17:30、千代田プラットフォームスクウェア501会議室にて開催した。

討議事項:

- 委員査読作業状況
- PUFの取り扱いについて
- SCIS論文の取り扱いについて
- 攻撃類型、アルゴリズム判別状況
- データベース構築状況
  - ACCESSデモ
  - 新たな追加項目

- 解説書内容検討

1.3.4 第 4 回 HWV-WG

第4回HWV-WGは、平成26年3月20日(金)10:00-12:00、千代田プラットフォームスクウェア501会議室にて開催した。

討議事項：

- 攻撃防御記事査読(日英分)
- 解説書案査読(日英)
- 付属書の作成について
- DBの公開について

2. 基礎情報の収集

2.1 過去情報

当組合は、経済産業省より、企業・個人の情報セキュリティ対策促進事業（高度大規模半導体集積回路セキュリティ評価技術開発）を受託し、その中でハードウェア脆弱性分析技術に関する研究報告の収集し、データベースを作成した。本調査事業においては、平成21-22年度に行われた上記をベースに、その後、今回の調査により必要な更新を行い、平成22年度以降、これまでに公開された約5年分（22年度～26年度まで）の研究報告等の情報を加える形で、データベースを作成することとした。

2.2 欧州各国への情報照会と返信

提案書記載に添って、JHAS メンバー及び欧州 SOGIS ハードウェア認証提供国（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）の認証機関に照会を行い、フランス、ドイツ、イギリス、ノルウェーより回答を得た。
（なお、イタリア、オランダ、スペイン、スウェーデンについては、認証機関からの回答がなかったため、該当なしと判断した）

2.3 学識者等からの情報提供

各国調査の内、米国についてはハードウェアセキュリティの評価認証を行っていないため、認証機関への情報照会を行えなかった。一方で、当該分野の多数の国際学会（ＣＨＥＳ、ＨＯＳＴ等）が米国で開催されており、当該結果については、2.4 において記載している。一方、昨今情報セキュリティや暗号実装にかかる学会だけでなく、半導体設計に関する学会等においても、セキュリティ課題を取り上げる傾向があるので、HWV-WG の学識者委員からの情報提供を求め、情報提供のあった学会について、HWV-WG の企業側委員又は当組合研究員がプログラムを閲覧し、DB に収録すべき論文を抽出した。

2.4 国際学会及びその他各国学会の調査

国際学会については、次のいずれかに該当する学会について、HWV-WG の企業側委員または当組合研究員がプログラムを閲覧し、DB に収録すべき論文を抽出した。

- 2.1 において収録実績のある学会
- 2.2 または 2.3 において情報提供のあった学会

一方、次の国内学会についても調査の上、HWV-WG の企業側委員または当組合研究員が 2009 年から 2014 年までのプログラムを閲覧し、DB に収録すべき論文を抽出した。

- 我が国の当該分野の国内研究会 SCIS（情報通信学会の内部研究会）
- 2.1 において収録実績のあった国の国内学会（日本、韓国、インド、カナダ等）

2.5　基礎情報収集のまとめ

上記作業の結果、1187 件の基礎情報を得ることができた。

学会略称	開催年	開催場所	掲載論文数
CHES	1999	Worcester, MA, USA.	5
	2000	Worcester, MA, USA.	10
	2001	Paris, France.	12
	2002	Redwood Shores, CA, USA.	16
	2003	Cologne, Germany.	8
	2004	Cambridge, USA.	10
	2005	Edinburgh, Scotland.	13
	2006	Yokohama, Japan.	20
	2007	Vienna, Austria.	9
	2008	Washington, DC, USA.	15
	2009	Lausanne, Switzerlannd	32
	2010	Santa Barbara, California, USA	30
	2011	Nara, Japan	32
	2012	Leuven, Belgium	32
	2013	Santa Barbara, California, USA	27
	2014	Busan, Korea	31
FDTC	2006	Yokohama, Japan	12
	2007	Vienna, Austria	12
	2008	Washington DC, USA	13
	2009	Lausanne, Switzerland	14
	2010	Santa Barbara, CA, USA	10
	2011	Nara, Japan	12
	2012	Leuven, Belgium	11
	2013	Santa Barbara, CA, USA	8
	2014	Busan, Korea	13
HOST	2009	San Francisco, CA	13
	2010	Anaheim, CA	19
	2011	San Diego, CA	26
	2012	San Francisco, CA,USA	27
	2013	Austin, TX, USA	26
	2014	Arlington, VA USA	30
ASP/DAC	2011	Yokohama,Japan	1
	2013	Yokohama,Japan	1
	2014	SunTec,Singapre	2
DAC	2011	San Diego, CA USA	1
	2014	San francisco, CA USA	1
ICCAD	2013	San Jose,CA USA	1
	2014	San Jose,CA USA	3
ICCD	2012	Montreal, QC, Canada	1
	2014	Seoul, Korea (South)	1
ISCAS	2009	Taipei,Taiwan	2

	2010	Paris,France	3
	2011	Rio De Janeiro, Brazil	2
	2012	Seoul, Korea (South)	4
	2014	Melbourne,Victoria,Australia	1
DFT	2014	Amsterdam, Netherlands	1
ITC	2009	Austin, TX, USA	1
	2013	Anaheim, California,USA	1
	2014	Seattle, WA, USA	2
FSE	2000	New York, NY, USA	1
	2003	Lund, Sweden	1
	2008	Lausanne, Switzerland	2
	2012	Washington, DC, USA	1
	2013	Singapore	3
ACNS	2006	Singapore	3
	2007	Zhuhai, China	2
	2009	Paris-Rocquencourt, France	3
ASIACRYPT	2000	Kyoto, Japan	1
	2004	Jeju Island, Korea	1
	2009	Tokyo, Japan	6
	2010	Singapore	1
	2012	Beijing, China	2
	2013	Bengaluru, India	3
	2014	Kaoshiung, Taiwan, R.O.C.	6
Cardis	2010	Passau, Germany	8
CRYPT	1996	Santa Barbara, California, USA	1
	1997	Santa Barbara, California, USA	1
	1999	Santa Barbara, California, USA	2
	2000	Santa Barbara, California, USA	1
	2008	Santa Barbara, California, USA	2
	2009	Santa Barbara, California, USA	1
	2011	Santa Barbara, California, USA	2
	2012	Santa Barbara, California, USA	1
	2013	Santa Barbara, California, USA	2
	2014	Santa Barbara, California, USA	1
CSS	2007	奈良県奈良市	2
	2008	沖縄県宜野湾市	5
	2009	富山県富山市	2
CT-RSA	2001	San Francisco, CA, USA	1
	2002	San Jose, CA, USA	4
	2005	San Francisco, CA, USA	1
	2006	San Jose, CA, USA	3
	2007	San Francisco, CA, USA	1
	2008	San Francisco, CA, USA	4

	2009	San Francisco, CA, USA	10
	2010	San Francisco, CA, USA	9
	2011	San Francisco, CA, USA	2
	2012	San Francisco, CA, USA	8
	2013	San Francisco, CA, USA	3
	2014	San Francisco, CA, USA	4
e-smart	2001	Cannes, France	1
	2008	開催地不明	2
	2009	開催地不明	5
EUROCRYPT	1997	Konstanz, Germany	3
	2006	St. Petersburg, Russia	1
	2009	Cologne, Germany	2
FC	2000	Anguilla, British West Indies	1
	2003	Guadeloupe, French West Indies	1
	2009	Accra Beach, Barbados	1
	2010	Tenerife, Canary Islands, Spain	1
ICISC	2001	Seoul, Korea	4
	2002	Seoul, Korea	2
	2005	Seoul, Korea	1
	2008	Seoul, Korea	3
	2009	Seoul, Korea	3
	2010	Seoul, Korea	7
	2011	Seoul, Korea	5
	2012	Seoul, Korea	2
	2013	Seoul, Korea	2
IEICE	2004	日本国内（開催地不明）	1
	2005	日本国内（開催地不明）	1
	2008	日本国内（開催地不明）	2
	2009	日本国内（開催地不明）	2
Indocrypt	2000	Calcutta, India	1
	2008	Kharagpur, India	3
	2009	New Delhi, India	5
	2010	Hyderabad, India	2
	2012	Kolkata, India	2
	2014	New Delhi, India	2

ITCC	2004	Las Vegas, NV, USA	1
	2005	Las Vegas, NV, USA	1
PKC	1999	Kamakura, Japan	1
	2000	Melbourne, Victoria, Australia	1
	2002	Paris, France	4
	2003	Miami, Florida, USA	1
	2013	Nara, Japan	2
SAC	1998	Kingston, Ontario, Canada	1
	2004	Waterloo, Ontario, Canada	1
	2006	Montreal, Canada	4
	2007	Ottawa, Canada	3
	2008	Sackville, New Brunswick, Canada	2
	2010	Waterloo, Ontario, Canada	2
	2012	Windsor, Ontario, Canada	1
	2013	Burnaby, BC, Canada	1
	2014	Montreal, QC, Canada	2
SASC	2007	開催地不明	1
	2008	開催地不明	2
SCIS	1997	福岡県福岡市	1
	2003	静岡県浜松市	20
	2005	兵庫県神戸市垂水区	19
	2006	広島県広島市	13
	2007	長崎県佐世保市	13
	2008	宮崎県宮崎市	13
	2009	滋賀県大津市	45
	2010	香川県高松市	54
	2011	福岡県北九州市	28
	2012	石川県金沢市	30
	2013	京都府京都市	23
	2014	鹿児島県鹿児島市	18
	2015	福岡県北九州市	22
USENIX	1996	San Diego, CA,USA	1
	1999	Chicago, Illinois,USA	2

	2007	Santa Clara, CA, USA	1
	2008	Boston,MA,USA	1
WISA	2004	Jeju Island, Korea	1
	2008	Jeju Island, Korea	4
	2009	Busan, Korea	12
	2010	Jeju Island, Korea	4
	2011	Jeju Island, Korea	1
	2012	Jeju Island, Korea	1
合計			1120
		欠番	21
		その他	67
		収録論文数＋欠番＋学会名不明	1208

（注） 欠番は 2009 年における過去データと新規収録論文の重複分 21 件。また、過去データには論文名及びアクセス URL が記載されていながら発表された学会名が記載されていないもの等が 67 件ある。

2.6　知的財産権に関する確認

実施計画に添って、以下を、当組合顧問、弁護士法人小澤法律事務所、小澤哲郎弁護士に平成 26 年 11 月及び平成 27 年 3 月の 2 回にわたり確認している。

既に公開されている研究論文名、当該論文等にアクセスすることが可能な URL を第三者が公開することは、著作者が保有する著作権等の知的財産権を侵害するものではない。

2.7　付記事項（我が国 SCIS 論文の詳細情報取得及びフランス国内学会発表の取扱）

2.7.1　SCIS

我が国当該分野の研究会SCISは、情報通信学会の内部研究会であり、近年開かれた同研究会で発表された論文の著作権は情報通信学会に帰属している。情報通信学会は、当該論文を公表していない（研究会のプログラムは公開されているので外部者は論文名を知ることが可能である）が、外部より請求があった場合、論文の複写には応じているので、DBにおいては、情報通信学会の複写請求頁を「当該論文、要約、関連論文名等が見られる先のURL」として案内している。

2.7.2 フランス国内学会における一部発表の取り扱い

2.2において、フランス認証機関ANSSIより提供された情報の中には、フランス国内学会における発表の際のスライドが公開され、論文本文にはアクセスできないものが一部含まれている。

これらスライドについてはDBに収録すべき論文ではないので、収録しなかったが、参考のために下記にスライドへのアクセス先を公開し、情報として提供することとした。

- CryptoPuces
  http://iml.univ-mrs.fr/ati/crypto_puces/rencontres_cryptopuces.html

他に、詳細を見るには登録等が必要だが、学会の概要を知ることができるフランス国内学会のURLを下記する。

- CryptArchi　https://labh-curien.univ-st-etienne.fr/cryptarchi/index.html
- C2 (Codes and Cryptography)　https://crypto.di.ens.fr/c2:main
- YACC (Yet Another Conference on Cryptography)　http://yacc.univ-tln.fr/
- PHISIC　http://www.phisic.emse.fr/index.php

3. データベースの構築

3.1　基礎情報の整理

基礎情報を整理し、表計算ソフト「エクセル」（xlsx）の様式にまとめた。
これを csv ファイルの形式に転換し、データベースソフト「アクセス」に入力することとした。
＜添付資料＞
3-1-1　HW セキュリティデータベース xlsx 版
3-1-2　HW セキュリティデータベース csv 版

3.2　データベース仕様

データベースソフト「アクセス」をカスタマイズし、本調査事業用のデータベースの仕様を確定した。成果品であるプログラム（データ入力済み）は添付の通りである。
参考のため、「アクセス」の無料読み取りソフトダウンロード用 URL を以下に掲げる。
http://www.microsoft.com/ja-jp/download/details.aspx?id=39358

＜添付資料＞
3-2-1　論文検索システムプログラム（データ入力済み）
3-2-2　論文検索システムプログラム（データ入力済み）完全英語版
3-2-3　論文検索システムプログラム操作マニュアル

3.3　索引

3.3.1　学会におけるセッション名

データベースに、当該論文が発表された学会におけるセッション名による索引（部分一致検索）を設けた。
ここに任意の分野名等を入力することにより論文を検索することができる。

3.3.2　暗号アルゴリズム

データベースに、暗号アルゴリズム名による索引（部分一致検索）を設けた。ここに任意の暗号アルゴリズム名を入力することにより論文を検索することができる。とくに機器ベンダ、システムベンダなどの場合、自らが製品・システムに実装する予定の暗号アルゴリズムに関する論文だけを抽出することができる。

3.3.3　引用数

データベースにおいては、個別の論文が、調査時点（平成 27 年 3 月）で他の論文に引用された件数を掲載している。過去情報については、引用数を調査時点のものに更新している。

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。
データベースの索引機能により、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。

3.3.4　論文判別
データベースにおいては、個別の論文を以下の通り判別し判別番号を付している。
判別番号 1：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 2：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 3：その他
データベースの索引機能により、当該論文判別ごとに論文を抽出することができる。
なお、この判別は、HWV-WG 委員が分担し、論文要約を全数査読して行っている。

3.3.5　その他の索引
データベースにおいては、上記の他に、論文題名、著者名、当該論文が発表された学会名（乃至学会名の略号)、所載の論文集の題名と番号、学会の開催年又は論文集の発行年、所載の論文集の ISBN（出版コード）などにより、いずれも部分一致検索により索引が可能となっている。

3.4　**攻撃類型**
データベースにおいては、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 の攻撃類別番号を付している。
（攻撃類型番号は、下記 CC Supporting Document　CCDB-2013-05-002 Version 2.9 Application of Attack Potential to Smartcards 所載の攻撃類型の頭番号 4.を削除した下一桁の番号である）
データベースの索引機能により、当該攻撃類型別の論文を抽出することができる。
データにおいては、（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も付記している。
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。
HW 情報セキュリティの対象とする攻撃の類型は、次の通り定義する。
＜CC Supporting Document　CCDB-2013-05-002 Version 2.9 Application of Attack Potential to Smartcards　第 4 章＞より引用
4.1　Physical Attacks（物理的な攻撃）
4.2　Overcoming sensors and filters（センサやフィルタの無効化）

4.3　Perturbation Attacks（かく乱攻撃）

4.4　Retrieving keys with DFA（DFA による鍵の取得）

4.5　Side-channel Attacks – Non-invasive retrieving of secret data（サイドチャネル攻撃－秘密データの非侵襲的取得）

4.6　Exploitation of Test features（テスト機能の悪用）

4.7　Attacks on RNG（乱数生成器への攻撃）

4.8　Ill-formed Java Card applications（不正な形式の Java Card アプリケーション）

4.9　Software Attacks（ソフトウェア攻撃）

4.10　Applet isolation（アプレット分離）

なお、個別論文の攻撃類型判定は、当組合客員研究員松田航平、是永梨絵、長友一樹（いずれも神戸大学）が行った。

3.5　事業レイヤー

データベースが対象とするのは、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

データベースにおいては、これら読者の事業レイヤー別の索引を設けている。

なお、HWV-WG において検討の結果、研究論文と上記事業レイヤーの間に特定の関係を見いだすことはできないとの結論に達したので、データベースにおいては読者がどの事業レイヤーを入力しても、索引では論文全数が抽出されるような仕様としてある。

3.6　実装環境

データベースにおいては、対象となる製品の実装環境を次の通り定義している。

実装環境	環境 I	環境 II	環境III	環境IV
DB 上の表記	広範流布 Circulating in the market	移動可能 Easy to move	耐タンパ機器内実装 Resistant to external physical attacks	閉鎖環境 Protected by secure environment

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

データベースにおいては、読者が対象製品の実装環境を入力すると、当該実装環境に該当する攻撃類型に属する論文を抽出することができる使用となっている。
なお、実装環境と攻撃類型との関係は HWV-WG の審議により決定した。
詳細は第 7 章解説書を参照。

3.7 詳細表示

データベースにおいては、「論文一覧」「詳細表示」をクリックすることによって、個別論文に関する詳細記事を閲覧することができる。
詳細記事には次の項目が収録されている。

- データ番号
- 著者
- 題名
- 著者（和文の場合）
- 題名（和文の場合）
- 発表された学会名
- 当該学会における発表順
- 所載論文集の番号
- 所載論文集の収録頁
- 学会開催年
- 学会開催月日
- 所載論文集の出版コード（ISBN）
- 所載論文の引用数
- 学会略号（略称）
- 要約へのアクセス URL

- 本文へのアクセス URL
- 当該論文が参照している論文へのアクセス URL
- 当該論文を引用している論文へのアクセス URL
- 学会におけるセッション名
- 当該論文が取り扱っている暗号アルゴリズム
- 攻撃防御記事

なお、調査の結果判明しなかった事項、当該論文と特定の攻撃類型の関係を判定できなかった場合などについては、詳細表示の一部の項目を空欄としている場合がある。
末尾の攻撃防御記事には、当該論文が特定の攻撃類型に属すると判定した場合、当該攻撃類型の説明、主たる影響、よく知られた防御対策について詳しく説明している。
本項に示した、攻撃防御記事の内、攻撃類型に関する説明、主たる影響は＜CC Supporting Document　CCDB-2013-05-002 Version 2.9 Application of Attack Potential to Smartcards　第 4 章＞より引用している。また、和文は主に独立行政法人情報処理振興協会の CC 認証機関 JISEC が翻訳公開している、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、一部 HWV-WG での審議の上、当組合で独自に訳出した。独自訳部分は、記事中に【内】に記載している。

4. よく知られた対抗策

4.1 対抗策の粒度

3.10 末尾の攻撃防御記事中、防御対策に関する記事については、HWV-WG の審議により独自に作成している。この審議に際しては、委員より、対策の粒度については、記事の公開により社会の脅威が増進することのないよう、十分配慮してほしい旨の強い要請があった。このため、HWV-WG の審議を経て、

- 防御対策として、読者（とくにシステムユーザ、システムベンダ、機器ベンダ等）が製品開発に関与する際に、当該論文の示す攻撃類型に対して一般的にはどのような防御対策がよく知られているかについて理解できるレベルとする
- 防御対策はすでに論文等で公知となっている対策を一定程度抽象化して表記する

こととし、具体的には次項の通りとした。

4.2 よく知られた対抗策の整理

HWV-WG 審議を経て、「よく知られた対抗策」を次の通り整理した。

なお、「よく知られた対抗策」は、当該攻撃類型に対する対抗策の代表例であり、あり得るすべての対策を網羅したものではない。

攻撃類型 1 物理攻撃	Implement sensors and filters, Circuit randomization or shielding, Encryption for internal process, Deleting data in emergency, Deleting cryptographic key in emergency	センサ、フィルタの実装 回路のランダム化、シールド 内部プロセスの暗号化, 異常事態におけるデータ消去, 異常事態における暗号鍵の消去
攻撃類型 2 センサやフィルタの無効化	Implement sensors and filters (assumption), Deleting cryptographic key in emergency,	センサ、フィルタの実装（攻撃の前提), 異常事態における暗号鍵の消去,
攻撃類型 3 かく乱攻撃	Implement sensors and filters (assumption), Deleting cryptographic key in emergency,	センサ、フィルタの実装（攻撃の前提), 異常事態における暗号鍵の消去,
攻撃類型 4 DFA による鍵の取得	Implement sensors and filters Detect irregular behavior of calculation process and memory Verification in calculation process	センサ、フィルタの実装 演算過程やメモリにおける異常な振る舞いの検知 演算過程における検算
攻撃類型 5	Randomizing or flattening the	演算過程におけるランダム化または平準

サイドチャネル攻撃－秘密データの非侵襲的取得	calculation processes Randomizing clock or code Randomizing or flattening software processes Noise supplementation Implement retry counters in cryptographic processes	化 クロック又はコードのランダム化 ソフトウェア動作過程におけるにおけるランダム化または平準化 ノイズの印可 暗号プロセスへのリトライカウンタの実装
攻撃類型 6 テスト機能の悪用	Secure managing for procurement and testing Access control to test features	調達及びテスト過程のセキュアな管理 テスト機能へのアクセス制御
攻撃類型 7 乱数生成器への攻撃	Implement sensors and filters Random testing	センサ、フィルタの実装 乱数テストの実施
攻撃類型 8 不正な形式の Java Card アプリケーション	Access control to memories, files and other features Detection and management for integrity of software process Byte code verification	メモリ、ファイル等へのアクセス制御 ソフトウェア動作過程における完全性のための検証と管理 バイトコードの検証
攻撃類型 9 ソフトウェア攻撃	Access control to memories, files and other features Detection and management for integrity of software process Verification in calculation process Deleting data in emergency Randomizing or flattening software process Log management on irregular behavior of calculation process and memory Deleting cryptographic key in emergency Verification for availabilities Sequence control Implement retry counters in cryptographic process	メモリ、ファイル等へのアクセス制御 ソフトウェア動作過程における完全性のための検証と管理 演算過程における検算 異常事態におけるデータ消去 ソフトウェア動作過程におけるランダム化または平準化 演算過程、メモリにおける異常な振る舞いのログ管理 異常事態における暗号鍵の消去 可用性の検証 シーケンス管理 暗号プロセスへのリトライカウンタの実装

攻撃類型 10 アプレット 分離	Access control to memories, files and other features Verification in calculation process Verification for availabilities Sequence control Implement retry counters in cryptographic process	メモリ、ファイル等へのアクセス制御 ソフトウェア動作過程における完全性のための検証と管理 演算過程における検算 可用性の検証 シーケンス管理 暗号プロセスへのリトライカウンタの実装

5. 実装環境別のセキュリティ対策整理

5.1 実装環境とセキュリティ対策

本調査の対象とするHW製品が、どの程度のセキュリティ対策を実装すべきかをはかる一つの指標として、製品の実装環境がある。一般によりセキュアな環境で使用される製品は、セキュリティ対策の実装を緩和することができる。本調査おいて再三参照または引用している＜CC Supporting Document CCDB-2013-05-002 Version 2.9 Application of Attack Potential to Smartcards＞はスマートカード乃至は同様の製品を対象とするものであって、その実装環境における脅威はきわめて高いものがある。だが、製品の中には、より閉鎖的な環境の下で使用されるものもあるので、すべての製品がスマートカード類似製品と同じセキュリティ対策を装備すべきとは限らない。（ただしHW製品の実装環境は、HW製品が、どの程度のセキュリティ対策を実装すべきかをはかる一つの指標に過ぎず、別の観点からの指標、たとえば、情報資産価値等も顧慮する必要があることについては、第6章以下を参照）

このため、HWV-WGにおいて、実装環境とセキュリティ対策の関係について審議し、その結果を解説書（第7章参照）に反映することとした。

5.2 実装環境の整理

データベースにおいては、HWV-WG審議を経て、対象となる製品の実装環境を次の通り定義した。

実装環境	環境Ⅰ	環境Ⅱ	環境Ⅲ	環境Ⅳ
DB上の表記	広範流布 Circulating in the market	移動可能 Easy to move	耐タンパ機器内実装 Resistant to external physical attacks	閉鎖環境 Protected by secure environment
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

5.3 システム、製品、部品における適用例

前項の各実装環境のシステム、製品、部品における適用例について、HWV-WG審議を経て、次の通り整理した。この内容は、解説書において読者に開示される。（第7章参照）

実装環境	環境 I	環境 II	環境III	環境IV
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

5.4 攻撃類型と実装環境

HWV-WGにおいて、3.4項に示す製品の攻撃類型と製品実装環境との間にどのような関係があるかについて審議分析し、その内容を下記にまとめた。この内容は、解説書において読者に開示される。（第7章参照）

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	◎	○	○	△

凡例：◎: strong　○: medium　△: low　×: none

6. セキュリティ保証

6.1 セキュリティ対策とセキュリティ保証

データベースに附属する解説書（第 7 章参照）においては、データベース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ってない。その理由は、

- 個別論文所載の攻撃事例に対して対策を示すためには、当該論文を査読検証した上で、対策について客観的に妥当な実験を行って有効性を検証しなければならないこと
- 有効な対抗策を公開することは、一般に社会の脅威を増進する可能性があること
- 情報セキュリティ上の防御対策は、当該対策を実装する製造者の知的財産権やノウハウに帰属する例が多いこと。

である。

6.2 CC ハードウェア認証取得の推奨

そこで、前記の要求乃至推奨に替えて、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とした。

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について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）

本調査では、とくに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、次項以下の通り推奨することとした。

読者に対しては、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、それぞれ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することを推奨する。

（なお、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することとした。データベースに掲載

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）

6.3 対象と情報資産価値

攻撃に対抗して、対象製品が実装すべき防御策の強度は、対象製品が守るべき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。

そこで、HWV-WG の審議を経て、対象となる製品（システム、機器、部品）を例示し、守るべき資産の程度を下表の通り分析整理した。

	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			

6.4 情報資産価値と脆弱性分析の程度

HWV-WG 審議を経て、本調査の対象とする HW 製品が、どの程度のセキュリティ対策を実装すべきかをはかる一つの指標として、情報資産価値に注目した場合の推奨すべき脆弱性分析の程度を以下の通り整理した。

【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
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

6.5 実装環境と脆弱性分析の程度

HWV-WG 審議を経て、本調査の対象とする HW 製品が、どの程度のセキュリティ対策を実装すべきかをはかるもう一つの指標として、製品の実装環境に注目した場合の推奨すべき脆弱性分析の程度を以下の通り整理した。

【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
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	－

6.6 推奨される脆弱性分析の程度

解説書（第７章参照）の読者は、まず6.4,6.5所載の表に添って対象製品の保護する資産と実装環境を特定する。

HWV-WG 審議を経て、情報資産、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、対象製品に対して推奨される脆弱性分析の程度とした。

この内容は、解説書（第７章参照）によって開示される。

7. 解説書の作成

7.1 解説書の構成

第6章までのHWV-WGの整理と分析作業をまとめて、データベース利用者に対する解説書を英和両文でまとめた。その構成は下記の通りである。

7.1.1 このガイドが対象とする読者
7.1.2 このガイドが対象とする情報処理機能の定義
7.1.3 対象とする攻撃の範囲
7.1.4 攻撃類型
7.1.5 論文の判別
7.1.6 引用数
7.1.7 情報処理機能の実装環境
7.1.8 情報資産について
7.1.9 攻撃類型と実装環境の関係
7.1.10 セキュリティ保証

7.2 解説書の内容

解説書の内容は添付の通りである。

なお、英文は、HW情報セキュリティに関する述語に知見を有する、株式会社ECSEC Laboratoryに翻訳作成を委託した。

なお、解説書はデータベースとともに公開される。

＜添付資料＞

7-2-1 解説書（和文）
7-2-2 Guidance（英文）

8. 解説書附属書類（検索・絞り込みガイド）

8.1 検索・絞り込み機能の設計

提案書1.2.5に添って、解説書附属書類（検索・絞り込みガイド）を作成した。

個別論文を査読した結果、読者の事業レイヤー、対象製品と個別論文を関係づけることは困難（学術論文は殆ど個別の産業用製品事例を顧慮しておらず、攻撃防御事例を抽象化して一般論を述べている）との判断に達した。

一方で、できる限りデータベース利用者の便宜を図って、利用者が有効な絞り込みを行い、的確な少数の論文に行き着くことができるように、実装環境、攻撃類型、引用数、暗号アルゴリズムその他の要素から適当な絞り込みが行えるようにデータベースを設計した。

8.1.1 事業レイヤー

データベースには、読者の事業レイヤーによる絞り込み機能を設けた。

学術論文は殆ど個別の産業用製品事例を顧慮しておらず、攻撃防御事例を抽象化して一般論を述べているため、現在の所、この絞り込みのどの階層をチェックしても、すべての論文に該当する仕様としている。なお、とくにシステムユーザ、システムベンダ等の階層の利用者が、基礎文献として理解すべき少数の論文にすぐに到達することができるように、論文引用数による絞り込み機能を別に設けた。

8.1.2 対象製品

検討の結果、学術論文は殆ど個別の産業用製品事例を顧慮しておらず、攻撃防御事例を抽象化して一般論を述べているため、特定論文と読者の対象製品の分野を関係づけることは難しいとの結論に至ったので、対象製品による論文絞り込み機能は設けなかった。

これに替えて、製品の実装環境や、製品に実装されている暗号アルゴリズムを入力することによって、利用者が自己の取り扱っている製品にとって必要な論文を絞り込むことができるようにした。

8.1.3 実装環境

5.4 項所載の表を活用して、利用者が自己の取り扱っている製品の実装環境を入力することにより、プログラムが顧慮すべき攻撃類型を自動的に推定し、当該攻撃類型に該当する研究論文を絞り込むことができるようにした。

8.1.4 攻撃類型

3.4 項により判別した攻撃類型ごとに論文を絞り込むことができるようにした。

8.1.5 引用数

3.3.3 項により、データベースには個別の論文が、調査時点（平成 27 年 3 月）で他の論文に引用された件数を掲載している。過去情報については、引用数を調査時点のものに更新している。このデータを用いて引用件数 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絞り込み機能を設けた。

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り、とくにシステムユーザ、システムベンダ等の階層の利用者が、基礎文献として先ず理解すべきものであるといえる。

8.1.6　暗号アルゴリズム

3.3.2 項により、データベースに、暗号アルゴリズム名による索引（部分一致検索）を設けた。ここに任意の暗号アルゴリズム名（例:AES,RSA 等）を入力することにより論文を検索することができる。とくに機器ベンダ、システムベンダなどの場合、自らが製品・システムに実装する予定の暗号アルゴリズムに関する論文だけを抽出することができる。

8.1.7　論文判別

3.3.4 項により、データベースにおいては、個別の論文を以下の通り判別し判別番号を付している。

判別番号 1：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 2：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 3：その他

当該論文判別ごとに論文を抽出することができる絞り込み機能を設けた。

8.1.8　その他の検索機能

著者名、題名、和文著者名、和文題名、学会名/論文集名、論文集の当該論文番号、発行年、出版コード、学会セッション名で論文を検索することが出来る機能を設けた。

8.2　解説書付属書類の作成

8.1 の結果を、解説書付属書類（検索・絞り込みガイド）として作成し、解説書と共に提供することとした。

なお、予算及びスケジュールの都合から、英訳版は作成していない。

＜添付資料＞

8-2　解説書附属書類（検索・絞り込みガイド）

9. データベース及び調査報告書の公開等

9.1 当組合 HP 上の公開

平成 27 年 3 月 31 日、当組合のホームページに以下の通り公開した。

9.1.1 第 1 群：HW セキュリティデータベース（英和混交文）

- 告知文（和文）
- 解説書
- 解説書付属文書
- プログラム（英和混交文・データ入力済み）

9.1.2 第 2 群：HW セキュリティデータベース（英文）

- 告知文（英文）
- Guidance（英文）
- プログラム（英文・データ入力済み）

9.1.3 第 3 群 調査報告書（和文）

- 告知文（添付資料請求先付き）
- 調査報告書本文

9.2 ICSS-JC への DB 引継

平成 27 年 4 月開催予定の IC システムセキュリティ協会 CC 評価認証部会（ICSS-JC）通常部会において、データベースの公開及び内容と取り扱いの説明を行うことを予定している。平成 27 年 5 月開催予定の IC システムセキュリティ協会 CC 評価認証部会（ICSS-JC）代表者会議において、今後のデータベースの更新、メンテナンス継続の引き受けを要請することを予定している。

9.3 ICSS-RT への開示と活用促進の依頼

平成 27 年 5 月以降開催予定の IC システムセキュリティ協会セキュリティ会議において、データベースの公開及び内容と取り扱いの説明を行うとともに、活用の促進を依頼することを予定している。IC システムセキュリティ協会加入の業界団体（全国銀行協会等の法人 4 団体）に対しては、これら団体の加盟者への案内と活用の促進を依頼することを予定している。

9.4 電子商取引安全技術研究組合、組合員への開示と活用促進の依頼

平成 27 年 5 月開催予定の電子商取引安全技術研究組合通常総会において、組合員各社にデータベースの公開及び内容と取り扱いの説明を行うとともに、活用の促進を依頼することを予定している。

9.5　JHAS への情報提供

IC システムセキュリティ協会 CC 評価認証部会（ICSS-JC）のリエゾンを通じて、平成 27 年 5 月以降開催予定の JHAS 会議において、JHAS メンバーにデータベースの公開及び内容と取り扱いの説明を行うとともに、活用の促進を依頼することを予定している。

9.6　その他の内外団体への開示と活用促進の依頼

その他、平成27年度以降、当組合関係先の内外のHW情報セキュリティに関わる団体等には適宜の場で、データベース活用の促進を依頼することを予定している。

以上

添付資料一覧	ファイル形式
3-1-1　HW セキュリティデータベース xlsx 版	xisx
3-1-2　HW セキュリティデータベース csv 版	csv
3-2-1　論文検索システムプログラム（データ入力済み）	mdb
3-2-2　論文検索システムプログラム（データ入力済み）完全英語版	mdb
3-2-3　論文検索システムプログラム操作マニュアル	docx
7-2-1　解説書（和文）	docx
7-2-2　Guidance（英文）	docx
8-2　解説書附属書類（検索・絞り込みガイド）	docx