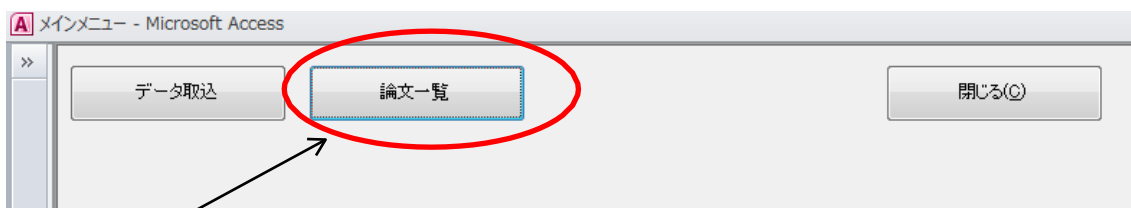
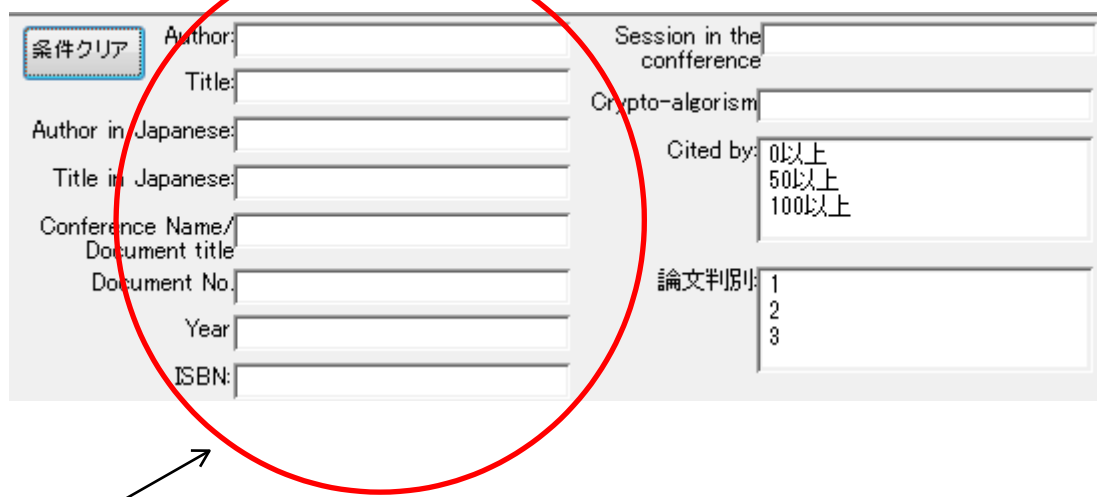


### 解説書附属書類（検索・絞り込みガイド）

1. データベースのプログラムを開きます。



2. 論文一覧を選択します。
3. 論文一覧の画面が開きます。（1182件の全データが表示されています）



条件クリア	Author:	Session in the conference
	Title:	Crypto-algorithm
	Author in Japanese:	Cited by: 0以上 50以上 100以上
	Title in Japanese:	論文判別: 1 2 3
	Conference Name/ Document title	
	Document No.	
	Year	
	ISBN:	

4. 検索その 1

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、出版コードで論文を検索することができます。

これらは部分位置検索ですので、たとえば PUF とか Trojan といった単語を題名欄に入力することにより、関心のある分野の論文を複数検索することも可能です。

条件クリア	Author:		Session in the conference	
	Title:		Crypto-algorithm	
	Author in Japanese:		Cited by:	0以上 50以上 100以上
	Title in Japanese:		論文判別:	1 2 3
	Conference Name/ Document title			
	Document No.			
	Year			
	ISBN:			

#### 5. 検索その2

学会におけるセッション名で論文を検索することができます。  
 特定の暗号アルゴリズム名で論文を検索することができます。  
 これらは部分一致検索ですので、たとえば、Higher order であるとか、Random 等の述語の部分でも検索することが可能です。

条件クリア	Author:		Session in the conference	
	Title:		Crypto-algorithm	
	Author in Japanese:		Cited by:	0以上 50以上 100以上
	Title in Japanese:		論文判別:	1 2 3
	Conference Name/ Document title			
	Document No.			
	Year			
	ISBN:			

#### 6. 絞り込みその1

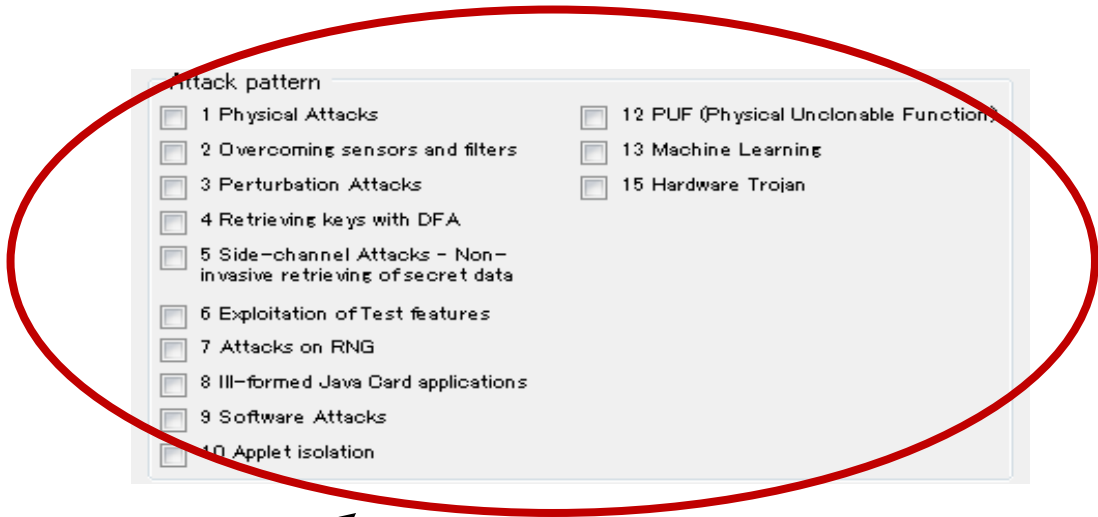
当該論文が他に引用された数（2015年3月調査現在）により、50以上、100以上の2段階で論文を絞り込むことができます。

論文判別として、

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

の3種類に論文を絞り込むことができます。

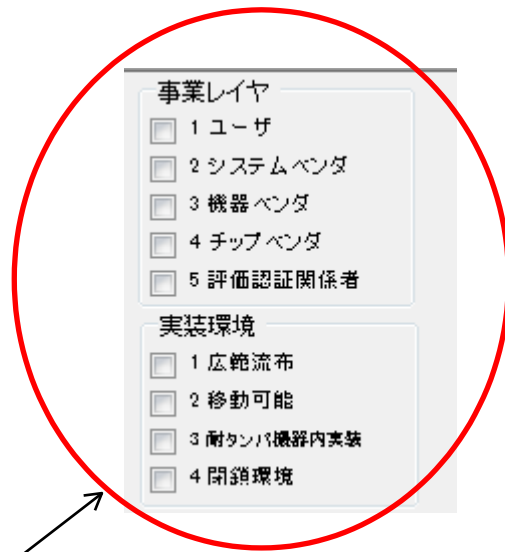


7. 絞り込みその2

当該論文が取り扱っている攻撃技術の類型を CCDB-2013-05-002, Mandatory Technical Document, Application of Attack Potential to Smartcards 第4章に示す類型に添って分類しています。

但し、データベース所載の論文によっては、上記攻撃類型の判別が出来ないものがあり、そのような論文は、上記の攻撃類型による絞り込み検索を行うと、絞り込み結果に出てきませんのでご注意ください。

\*1 2017年度版では攻撃類型3分類を追加しています。



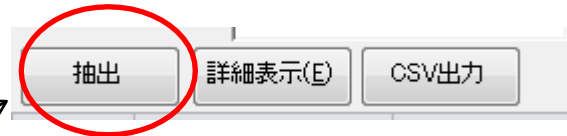
7

8. 絞り込みその3

このデータベースには、読者が取り扱う製品の実装環境により、配慮を要する論文を絞り込む機能があります。この機能の詳細は、解説書の第9項を参照ください。

このデータベースには、読者の事業レイヤーによる絞り込み機能があります。が、学术论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、検討の結果、特定の論文と読者の事業レイヤーとを関係づけることは難しいとの結論に至り、現在この絞り込み機能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なっています。



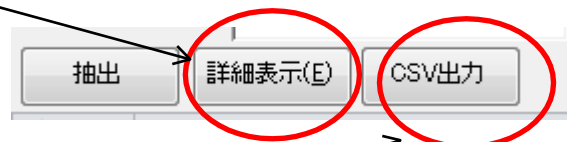
#### 9. 抽出

このデータベースでは、上記 1.-8.の検索及び絞り込み機能により、同時に複数のボックスをチェックした場合、より狭くデータが抽出されるプログラムとなっています。たとえば、題名欄に DPA を入力し、アルゴリズム欄に AES を入力し、攻撃類型に 5 をチェックして、抽出ボタンをクリックすると、題名に DPA を含み、且つアルゴリズムとして AES を扱い、且つ論文がサイドチャネルアタックを扱っていると判定されたデータだけが抽出されます。

6	Dan Boneh, Richard A. DeMillo,	On the Importance of	CRYPTO '97	3-540-63384-
7	Eli Biham, Adi Shamir,	Differential Fault Analysis of Secret	CRYPTO '97	3-540-63384-
8	M. Joye and J.-J. Quisquater	Faulty RSA encryption	UCL Report	

#### 10. 詳細表示

論文一覧（抽出された一覧も含む）の個別論文をひとつ選択し、当該論文上をクリックします。さらに、詳細表示ボタンをクリックすると、当該論文に関する詳細情報が表示されます。



#### 11. CSV 出力

CSV 出力ボタンをクリックすると、論文一覧（抽出された一覧も含む）を、CSV 形式で出力することができます。

以上