論文検索システム
操作マニュアル第 2 版

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

第 1 版 2015 年 1 月 26 日
第 2 版 2015 年 3 月 26 日

■INDEX

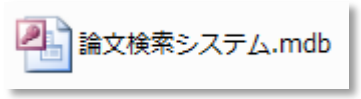
■図表 INDEX

1. プログラム操作

1.1. プログラムの起動

「論文検索システムプログラム.mdb」(又は「論文検索システムプログラム.mde」)(図 1)をダブルクリックしてください。

図 1 アイコンイメージ



1.2. 操作メニュー(起動画面)

起動すると以下の画面(図 2)が表示されます。以下に各ボタンについて説明します。
セキュリティの警告が表示される場合には、[開く]・[有効化]等を選択してください。(表示例:図 3)Access のバージョンによって表示される内容が異なりますので、詳細は Access のマニュアル等をご参照ください。

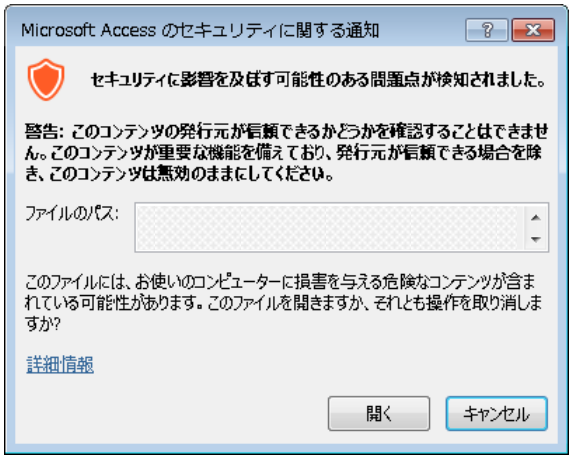
①. データ取込ボタン
論文データの CSV ファイルを取り込む画面を表示します。

②. 論文一覧ボタン
取り込まれた論文データの検索・一覧画面を表示します。

③. 閉じるボタン
本プログラムを終了します。

図 2 起動画面

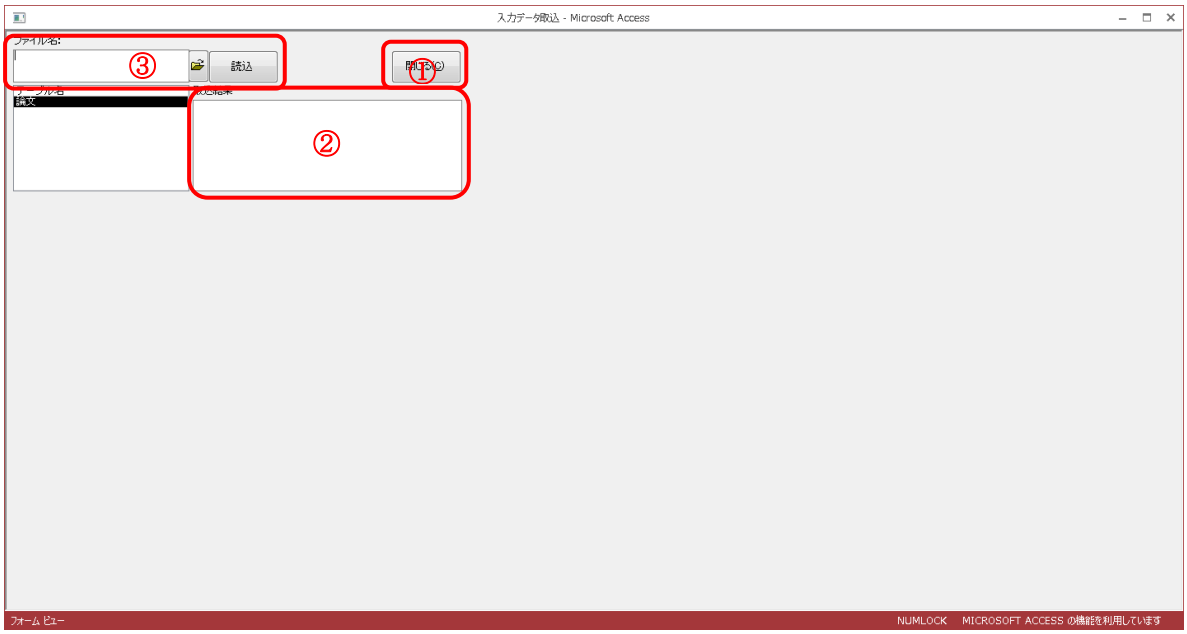
図 3 セキュリティ警告例



1.3. データ取込画面

論文データの CSV ファイルを取り込みます。(図 4)

図 4 データ取り込み画面



①. ファイルの選択

ファイルマークのボタンをクリックし、読み込む CSV ファイルを選択します。

選択されたファイルの場所(アドレス)が白枠部分に表示されます。

[読込]ボタンをクリックすると選択された CSV ファイルのデータが登録されます。

注) ファイル名(拡張子前以外)に「.(ドット)」が含まれていると正常に読み込めません。
該当する場合はファイル名を修正してください。

②. データ取り込み

正常に完了すると、②の白枠部分に取込件数が表示され、合わせて登録完了メッセージ（図 5）が表示されます。

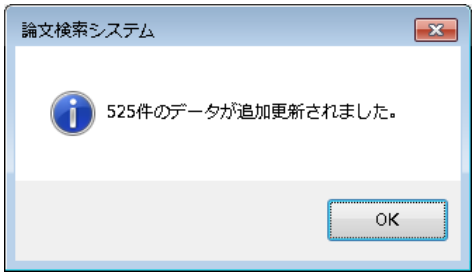
データにエラーがある場合にも②の白枠部分にエラー内容が表示されます。

該当するデータの行数・項目名・エラー内容が表示されますので、CSV ファイルの内容をご確認ください。

データ取り込み仕様は以下の通りです。

- 既に登録済みのデータがある場合、データの「No.」が重複している場合は、該当データを登録しません。
- 「No.」が重複していない場合は、追加登録します。

図 5 登録完了メッセージ



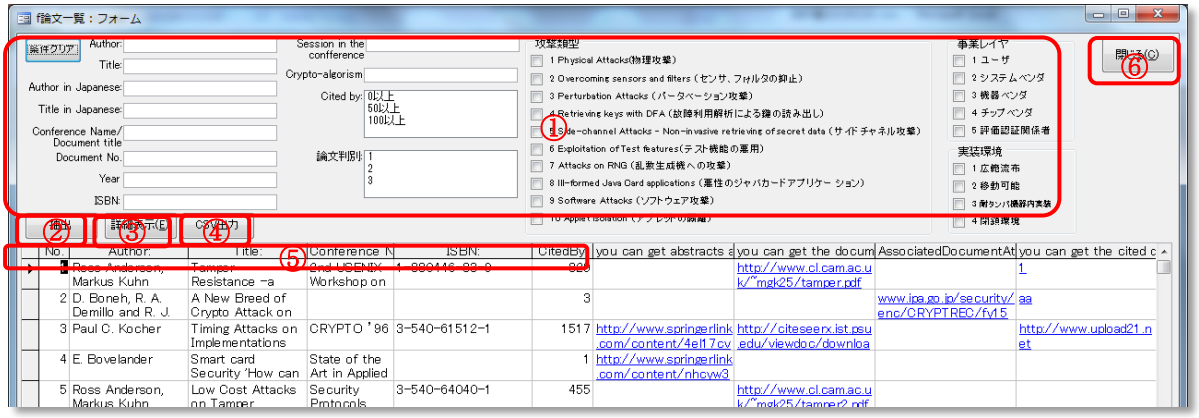
③. 閉じるボタン

[閉じる]をクリックすると起動画面（図 2）に戻ります。

1.4. 論文一覧画面

登録されたデータの検索・一覧表示をします。（図 6）

図 6 論文一覧画面



①. 検索条件設定

検索条件を入力または選択します。

テキスト入力する項目の検索条件は、全て「部分一致」になります。

②. 抽出ボタン

[抽出]ボタンをクリックすると、検索条件に該当するデータが画面下部に一覧表示されます。

また、データ内の URL(you can get abstracts at: 、you can get the document at: 、you can get the associated document: 、you can get the cited document at:の4項目)については、URL をクリックすると WEB ブラウザで WEB サイトが表示されます。

③. 詳細表示ボタン

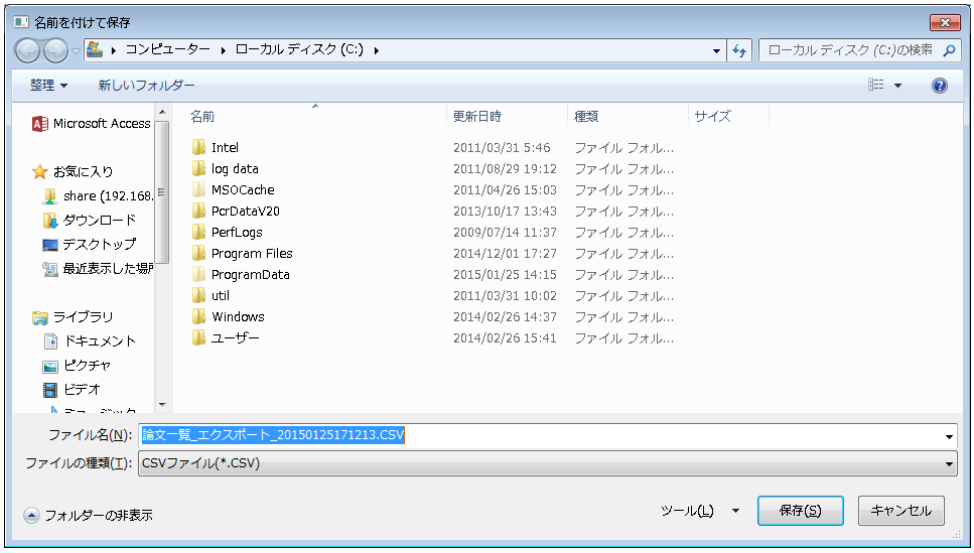
[詳細表示]をクリックすると、一覧表示内で選択された行の詳細情報画面(図 9)を表示します。

④. CSV 出力ボタン

[CSV 出力]ボタンをクリックすると、一覧表示されている内容を CSV ファイルに保存できます。

[名前を付けて保存]ウィンドウ(図 7)が表示されますので、任意の場所に保存してください。

図 7 [名前を付けて保存]ウィンドウ

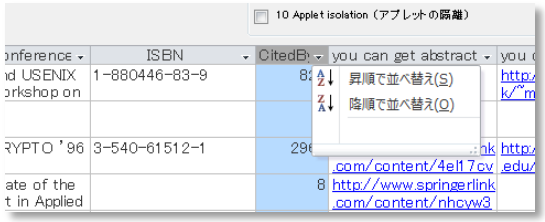


⑤. 並べ替え(昇順・降順)

一覧の項目名右にある「▼」をクリックすると、「昇順で並べ替え」「降順で並べ替え」メニューが表示されます。各メニューをクリックすると、選択した項目が並べ替えられます。(図 8)

注)データが URL の項目は並べ替えできません。

図 8 並べ替えメニュー



⑥. 閉じるボタン

[閉じる]をクリックすると起動画面（図 2）に戻ります。

1.5. 詳細情報画面

①. 印刷ボタン

[印刷]をクリックすると印刷プレビュー画面が表示されます。

Access メニューの「印刷」ボタン（図 10）から印刷を実行してください。

②. 閉じるボタン

[閉じる]ボタンをクリックすると、論文一覧画面（図 6）に戻ります。

図 9 詳細情報画面

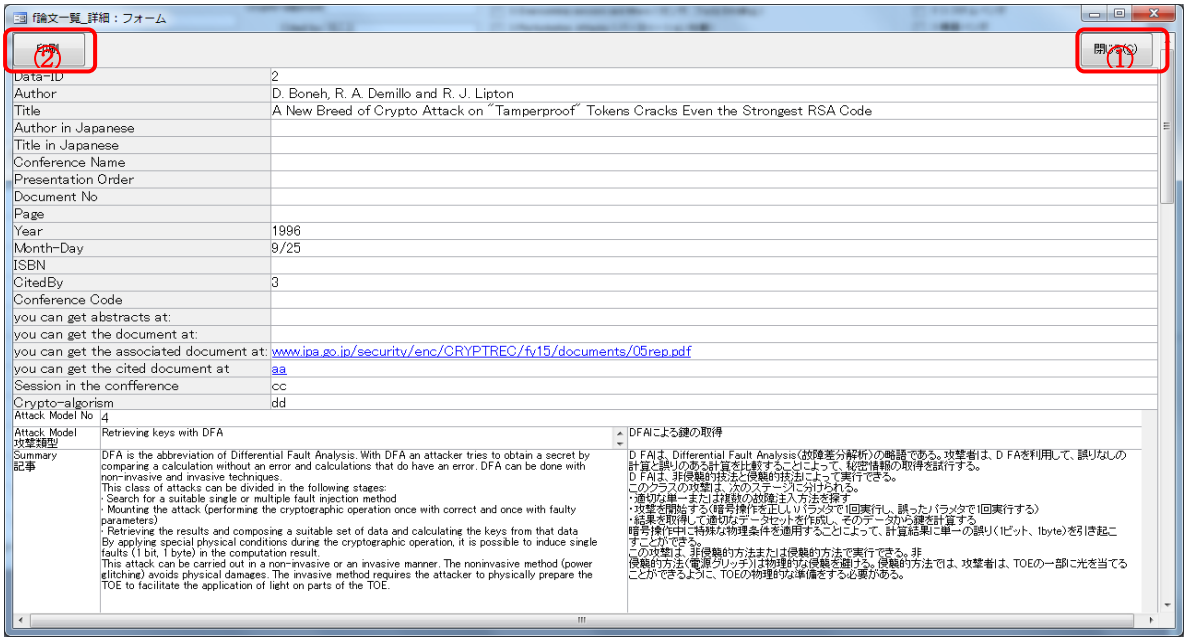
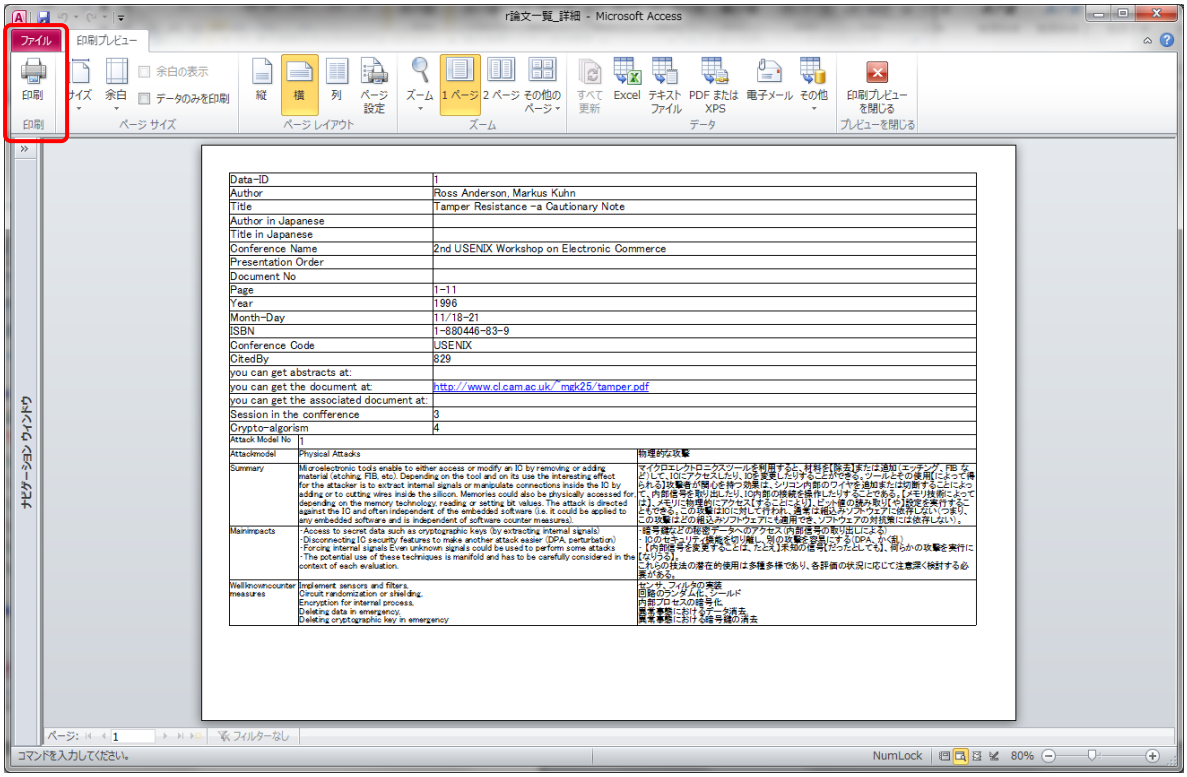


図 10 Access メニューの印刷ボタン



Data-ID	1
Author	Ross Anderson, Markus Kuhn
Title	Tamper Resistance -a Cautionary Note
Author in Japanese	
Title in Japanese	
Conference Name	2nd USENIX Workshop on Electronic Commerce
Presentation Order	
Document No	
Page	1-11
Year	1996
Month-Day	11/18-21
ISBN	1-880446-83-9
Conference Code	USENIX
CitedBy	829
you can get abstracts at:	
you can get the document at:	http://www.cl.cam.ac.uk/~mgk25/tamper.pdf
you can get the associated document at:	
Session in the conference	3
Crypto-algorism	4
Attack Model No	1

Attackmodel	Physical Attacks	物理的な攻撃
Summary	Microelectronic tools enable to either access or modify an IC by removing or adding material (etching, FIB, etc). Depending on the tool and on its use the interesting effect for the attacker is to extract internal signals or manipulate connections inside the IC by adding or to cutting wires inside the silicon. Memories could also be physically accessed for, depending on the memory technology, reading or setting bit values. The attack is directed against the IC and often independent of the embedded software (i.e. it could be applied to any embedded software and is independent of software counter measures).	マイクロエレクトロニクスツールを利用すると、材料を[除去]または追加(エッチング、FIB など)して、ICにアクセスしたり、ICを変更したりすることができる。ツールとその使用によって得られる攻撃者が関心を持つ効果は、シリコン内部のワイヤを追加または切断することによって、内部信号を取り出したり、IC内部の接続を操作したりすることである。[メモリ技術]によっては、メモリに物理的にアクセス(するごとにより)ビット値の読み取り(や)設定を実行することもできる。この攻撃はICに対して行われ、通常は組込みソフトウェアに依存しない(つまり、この攻撃はどの組込みソフトウェアにも適用でき、ソフトウェアの対抗策には依存しない)。
Mainimpacts	・Access to secret data such as cryptographic keys (by extracting internal signals) ・Disconnecting IC security features to make another attack easier (DPA perturbation) ・Forcing internal signals Even unknown signals could be used to perform some attacks ・The potential use of these techniques is manifold and has to be carefully considered in the context of each evaluation.	・暗号鍵などの秘密データへのアクセス(内部信号の取り出しによる) ・ICのセキュリティ機能を切り離し、別の攻撃を容易にする(DPA、かく乱)。 ・[内部信号を変更する]とは、たとえ[未知の信号]だったとしても、何らかの攻撃を実行に(なりうる)。 これらの技法の潜在的使用は多種多様であり、各評価の状況に応じて注意深く検討する必要がある。
Wellknowncounter measures	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の消去 異常事態における暗号鍵の消去

2. 推奨動作環境

対象	条件	備考
OS	Windows 7（32bit）	
ソフトウェア	Microsoft Access 2013	Microsoft Access 2013 Runtime 含む
画面サイズ	1280×700 以上	

※上記以外の環境で使用した場合の動作は保障できませんので、使用者の責任においてご利用ください。

以上