

# Windows 7 検索インデックス

2010年7月23日

第二回コンピュータフォレンジクス

技術解説 無料セミナー

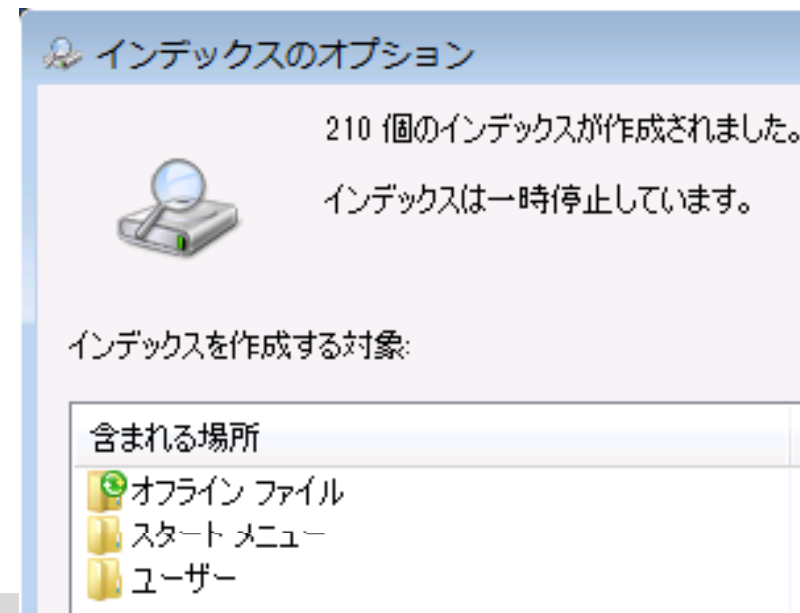
Ihara, Hideaki



# Windows Search



- デスクトップ検索機能
- Windows XP用 Windows Search 4.0
  - 別途インストールが必要
- Windows Vista / Windows 7
  - 標準機能
  - インデックス作成



- インデックス対象ファイルの設定
  - 拡張子とフィルタを設定
  - デフォルトで多数が定義済み
- インデックス作成方法
  - ①プロパティのみインデックスを作成
  - ②プロパティとファイルのコンテンツのインデックスを作成する
- iFilterによる制御
  - SearchFilterViewを使うと確認可能

# Index(Windows.EDB) Path



## 詳細オプション

インデックスの設定 **ファイルの種類**

### ファイルの設定

- 暗号化されたファイルのインデックスを作成する(O)
- 区分発音符付きの同様の単語は別の単語とし

### トラブルシューティング

インデックスを削除して再作成します。

[検索とインデックス作成のトラブルシューティング](#)

### インデックスの場所

現在の場所:

C:\ProgramData\Microsoft

新しい場所 (サービスの再起動後)

EFS暗号化ファイル  
にも対応が可能

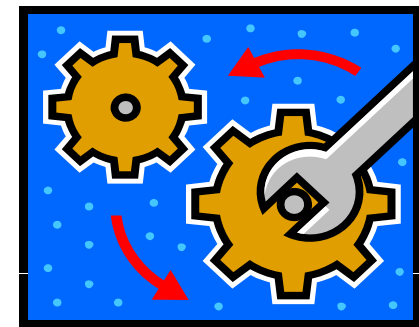
The screenshot shows the Windows Search Indexing and Privacy Control window. The left pane displays a tree view of the search index structure, with the path **Microsoft > Search > Data > Applications > Windows** selected. The right pane shows a list of files and folders indexed, with **Windows.edb** highlighted in a red box.

	Name
1	Config
2	GatherLogs
3	Projects
4	MSS00002.log
5	MSSres00001.jrs
6	MSSres00002.jrs
7	MSS.chk
8	Windows.edb
9	MSS.log
10	tmp.edb

- Windows Search は ESEDB を利用  
→ Windows.edb
- Extensible Storage Engine (ESE)  
Database File (EDB)
- ファイル形式に関する資料  
<http://libesedb.sourceforge.net/>
- ESEDBをパースするツールが必要  
→ EDBファイルでも対応が異なる



- ESEDBが作成された環境を確認
  - Windows Vista/7 のEDBファイルは、XP 上では解析困難
- “Dirty Shutdown” 状態のDBは修復が必要
  - ESENTUTLツールを利用
  - esedbinfoはDirtyでも解析を試みるが…



- Extensible Storage Engine Utilities for Microsoft Windows (ESENTUTL.EXE)
- ヘッダのダンプ  
例) *esentutl /mh Windows.edb*
- ページ (メタのみ) ダンプ  
例) *esentutl /mm /p2 Windows.edb*
- データベースの修復 (Repair or Recovery)  
例) *esentutl /p*  
例) *esentutl /r mss*

“Dirty Shutdown”  
状態への対応

# ESEDBの閲覧



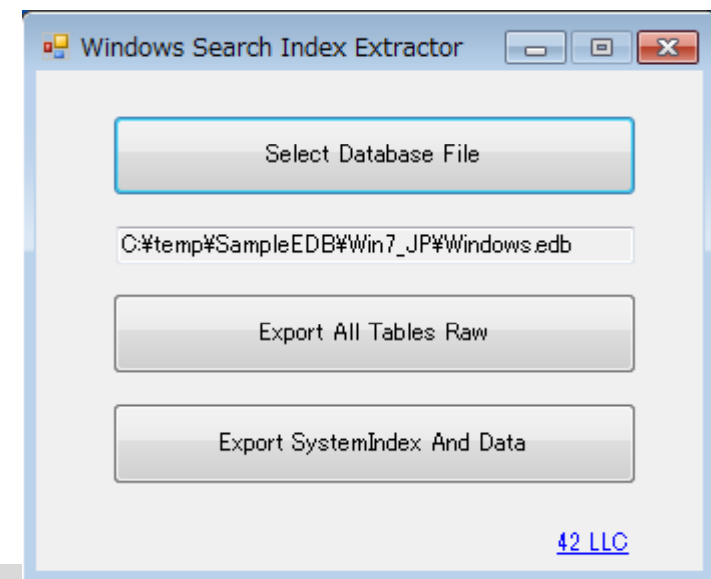
- Windows.EDBファイル内部を閲覧
- バイナリ状態での閲覧
  - DBファイルなので目視は困難
  - データの一部は圧縮されている
- Windows Vista では多くがBinary形式
  - Windows Vista → Big-endian
  - Windows XP/7 → Little-endian
- Windows Search Index Analyzer (商用)



# Windows.EDBのExport



- Windows Search Index Data Extractor  
→42 LLC, CEIC 2010 の資料と共に公開
- インデックスコンテンツをエクスポート  
→フォルダ構造を再現(Vistaはバイナリ…)  
→UTF-16LEでコンテンツを出力
- メタ情報をCSVで出力  
Systemindex\_0A



# Windows.EDB抽出例(Win7)



名前	更新日時
02_本文.doc	2009/05/07 17:45
000024768.doc	2009/10/01 14:48
CIO育成に関する資料.doc	2009/10/01 11:42
C I O育成に関する資料②.doc	2009/10/01 11:42
h17shinpojiumu_houkoku.doc	2009/10/01 14:11
hikakukyousouryokujittai.doc	2009/10/01 14:31
IT投資評価に関する調査研究1.doc	2009/10/01 12:16
IT投資評価に関する調査研究2.doc	2009/10/01 12:17
IT投資評価に関する調査研究3.doc	2009/10/01 12:17
IT投資評価に関する調査研究4.doc	2009/10/01 12:17
エネルギー情勢について.d	2009/10/01 14:42
消防計画_1-2-1.doc	
消防	
消防	

フォルダ構造の再現

6. 4 IT投資事前評価の具体的方法  
現在使っているIT投資事前評価書と今回の施策概要部分（第1部）は同じであるので、これまでのワープロで作成したものを使ってもよいし、新しいフォームで記入してもよい。それに加え多面的評価を実施する。評価ツールはエクセルで作成されている。以下において事前評価書の入力方法・使用方法について詳述する。

全体における注意事項  
評価書を使用する前に、注意事項を以下に記述する。  
ブックを開く際、マクロを有効にする。  
「評価書原本」には、何も入力しない。  
「評価書原本」をコピーして、同じブック内に評価用のシートを作成する。（その際、シート名はわかりやすいように変更してもよい。）

2,050 byte

# 参考資料URL



- インデックスを使用して Windows 検索を効率化する: よく寄せられる質問  
<http://windows.microsoft.com/ja-JP/windows7/Improve-Windows-searches-using-the-index-frequently-asked-questions>
- 詳細インデックス オプションを変更する  
<http://windows.microsoft.com/ja-JP/windows7/Change-advanced-indexing-options>
- SearchFilterView  
[http://www.nirsoft.net/utils/search\\_filter\\_view.html](http://www.nirsoft.net/utils/search_filter_view.html)
- Windows Search index analyzer software  
<http://www.edbsearch.com/>
- Extensible Storage Engine (ESE) Database File (EDB)  
<http://libesedb.sourceforge.net/>
  - Windows Search.pdf
  - Forensic analysis of the Windows Search database.pdf
  - Extensible Storage Engine (ESE) Database File (EDB) format.pdf
- Windows Search Index Data Extractor  
[http://42llc.net/index.php?option=com\\_myblog&show=CEIC-2010-scripts.html&Itemid=39](http://42llc.net/index.php?option=com_myblog&show=CEIC-2010-scripts.html&Itemid=39)



**eDiscovery & Incident Response Solutions**