

第四回 調査技術ゼミ

2005年11月22日

**『ブラウザ履歴の調査』
ブラウザ履歴情報の解析ツール**

ネットエージェント株式会社

Webブラウザの使用状況

- ・ 依然、Internet Explorerのシェアが高いが、欧米ではMozilla Firefoxも高い伸びを示している
 - IEは欧米では8割程度のシェアがあるがドイツでは7割程度との調査もある
 - Firefoxも1割程度、調査会社や国(フィンランド)によっては2割を超えている
 - 日本ではIEのシェアが9割を超えている
- ・ 参考：
 - Adtech社(ドイツ)プレスリリース：
http://www.adtech.de/NewsPresse/news_detail.php?lang_id=en&node=4¤t=190
 - OneStat社(オランダ)プレスリリース：
http://www.onestat.com/html/aboutus_pressbox40_browser_market_firefox_growing.html
 - WebSideStory社(アメリカ)の調査結果に関するCNET Japanの記事
<http://japan.cnet.com/news/media/story/0,2000047715,20083424,00.htm>

IE履歴情報の種類

- ・ index.datで管理
 - 「履歴」
 - Cookie
 - Internet Temporary Files (インターネット一時ファイル)
 - UserData
- ・ Protect Strage Area (レジストリ) で管理
 - パスワードキャッシュ
 - オートコンプリート (フォーム、BASIC認証)
- ・ レジストリで管理
 - アドレスバー履歴
 - 検索バー (Google)

履歴

- 場所 : %userprofile%\Local Settings\History\History.IE5
- 保存形態 : index.dat内に保持
- IEの履歴内の「マイコンピュータ」
 - デスクトップ上での操作がのこる
 - ネットワークフォルダも
 - 参考 : 「Internet Explorer で履歴のマイコンピュータを削除すると、他の履歴も削除される」
 - <http://support.microsoft.com/default.aspx?scid=kb;ja;418235>

Cookie (1) 概要

- ・ 場所:
 - 永続的なCookie
 - ⇒ %userprofile%\¥Cookiesに保存
 - 一時的なCookie
 - ⇒ ブラウザ(セッション)を閉じると削除
 - ・ [常にセッション Cookie を許可する] にチェックが入っていると削除されない
- ・ 内容: サイト側に依存だがURLは見える
- ・ 日本語はURLエンコードされる
- ・ RFCもある(2965)がブラウザの実装に依存
- ・ インポート、エクスポートが可能

Cookie (2) ダウングレード処理

- ・ 永続的なCookieを一時的なCookieとして処理
- ・ プライバシーレベル[中]のとき (IEヘルプより)
 - コンパクト ポリシー (コンピュータで読み込むことができる圧縮されたプライバシー ステートメント) を持たないサードパーティ Web サイトからの Cookie がブロックされます。
 - 暗黙的な同意を得ずに個人情報を使用するサードパーティ Web サイトからの Cookie がブロックされます。
 - 暗黙的な同意を得ずに個人情報を使用するファーストパーティ Web サイトからの Cookie を、Internet Explorer を終了するときにコンピュータから削除します。
- ・ 参考: 「IE 6のプライバシー管理機能」
 - http://www.atmarkit.co.jp/fwin2k/experiments/ie6privacy/ie6privacy_01.html

参考：コンパクトポリシー

- ・ W3Cが推進するP3P (Platform for Privacy Preferences Project) による
- ・ プライバシーポリシーをチェックするだけでコンテンツの中身とは結びつかない
- ・ HTTPヘッダに埋め込み
 - 参考：「最新IT用語解説 第8回P3P(Platform for Privacy Preferences)」
 - ・ <http://pcweb.mycom.co.jp/series/ityougo/008>

サインイン - Microsoft Internet Explorer

アドレス http://login.passportnet/ui/login.srf?lc=1041&id=2

MSN ホーム | Hotmail | ニュース | ショッピング | マネー | スペース

msn.co.jp **msn** Hotmail

無料 Hotmail がアップグレード! 250 MB のメールボックス容量、10 MB までの添付ファイル送受信 Hotmail.co.jp ドメイン

MSN Hotmail はすべて無料。今すぐはじめよう!
新規登録はこちら

- hotmail.co.jp ドメインのご提供開始!
新しいドメインの開始により、お好きな名前前のメールアドレスが取りやすくなりました。この機会にぜひ、ご登録ください!
- アクセスは簡単、デジカメ写真などの共有にも便利!
インターネットに接続できる環境なら、どこからでもメールの送受信が可能。メールボックスも余裕の 250 MB、添付ファイルも 10 MB まで送受信できます。
- セキュリティ強化でさらに安全なメール体験!
強力な迷惑メール処理機能と、さらに強化されたウイルス検知・駆除機能が、メールボックスを守ります。

[新規登録](#)

* アカウントの新規作成時には、メールボックスの容量は 25 MB となります。250 MB に増量されるためには、少なくとも 30 日の期間を要します。

Hotmail にサインイン

メール アドレス:

パスワード:

[パスワードを忘れたら? >>>](#)

メール アドレスとパスワードの保存
 メール アドレスの保存
 メール アドレスおよびパスワードを常に強化されたセキュリティでサインイン

[Microsoft Passport Network](#)
アカウント サービス | プライバシー | 1041
© 2005 Microsoft Corporation. All rights reserved.

この Web サイトの完全なプライバシー ポリシーを読むには、[ここをクリックしてください](#)。

このサイトには複数のプライバシーに関する声明があります:

[ポリシー 1](#)
[ポリシー 2](#)
[ポリシー 3](#)

サイトのポリシー 1

この Web サイトにより収集される情報の種類

HTTP Cookie のような仕組みです。個人とのアクティブな接続を維持したり、特定のサイトを参照したり、特定のコンテンツにアクセスしたことがある個人を自動的に識別したりする、ことが目的です。

この情報が収集される理由

情報の提供目的の操作を完了するために Web サイトが使用する可能性がある情報です。提供された操作には、Web 検索の結果を返す、電子メール メッセージを送信する、注文を出す、など 1 回限りの操作、または購読サービスを提供する、オンライン住所録や電子財布へのアクセスを許可する、などの繰り返し実行される操作があります。

Web サイトやコンピュータシステムの技術サポートに使用される可能性がある情報です。たとえば、コンピュータ アカウント情報を処理する、サイトのセキュリティを保護しサイトを維持する、あるいは Web サイトまたはそのエージェントによりサイトの操作を確認する、などです。

この情報にアクセスする人

この Web サイトは、エージェントとして動作するエンティティに対するエンティティおよび...

“passport.com” からの Cookie をどう処理しますか?

Cookie のプライバシー ポリシーを自分の設定と比較する(E)
 常にこのサイトに Cookie の使用を許可する(A)
 常にこのサイトに Cookie の使用を許可しない(N)

OK
キャンセル

プライバシー レポート

プライバシーの設定に基づいて、制限やブロックされた Cookie はありません。

表示:

現在のページ(コンテンツ)を提供する Web サイト(宛):

サイト	Cookie
http://g.msn.co.jp/s3/83204_B34200/5_c8317/1?cm=Big4-1-hl	
http://www.hotmail.com/	
http://loginnet.passport.com/login.srf?id=2&svc=mail&cbid=243...	言語済み
http://login.passportnet/ui/login.srf?lc=1041&id=2	言語済み
http://login.passportnet/pp320/CSS/WEBblue1041.css?c=3200...	
http://login.passportnet/pp320/JS/PPPrimary.js?x=3200.4104.0	
http://login.passportnet/pp320/images/icon_err.gif?x=3200.410...	
http://login.passportnet/pp320/images/c028.gif?x=3200.4104.0	

サイトのプライバシーの概要を表示するには、一覧から項目を選択してから [概要] をクリックしてください。

[プライバシーの詳細](#)

一時ファイル(1) Internet Temporary Files

- ・ 場所:
 - %userprofile%\Local Settings\Temporary Internet Files\Content.IE5
- ・ 保存形態:
 - Index.datで索引情報を保持 + 実データ

一時ファイル(2)UserData

- ・ 場所: %userprofile%\UserData
- ・ DHTMLのビヘイビアで保存可能
- ・ サーバからの呼び出しはできない
- ・ 比較的大容量が保存可能
- ・ 主にWindowsUpdateが使用

パスワード情報(基本認証)

- ・ 場所: ProtectStrageArea(レジストリ)
- ・ 内容: 「ホスト」「ポート番号」「認証名」「ユーザー」「パスワード」

オートコンプリート(1)

(フォーム、ユーザ名、パスワード)

- ・ 場所: ProtectStrageArea (レジストリ)
- ・ 内容: 「フォーム名」「オートコンプリート文字列」「保存年月日」
- ・ Webアドレスは履歴を参照する

参考 : ProtectStrageArea

- ・ 暗号化されて保存 (IPStoreインターフェース経由でアクセスする)
- ・ レジストリエディタからの参照は不可
- ・ アクセス権限があればツールで参照可能
- ・ 参考 :
 - CodeZine「Internet Explorerの認証パスワードとオートコンプリートの操作」
 - <http://codezine.jp/a/article.aspx?aid=147>

アドレスバー履歴 (Typed URL)

- ・ 場所: レジストリ
 - HKEY_CURRENT_USER¥Software¥Microsoft¥Internet Explorer¥TypedURLs
- ・ 内容:
- ・ オートコンプリートのWebアドレスとは別?

検索バー Google

- ・ レジストリ
 - HKEY_CURRENT_USER¥Software¥Google¥NavClient¥1.1¥History
 - EnCase 5.04a で該当レジストリを確認すると name で漢字を使用しているものは (Default) の表示になる。

ツール Pasco (1)

- Foundstone社



Foundstone
A DIVISION OF McAfee

- McAfee傘下のセキュリティソリューションベンダ
- インシデントレスポンスやフォレンジックサービスも実施
- Forensic Tool Kit などフォレンジックツールをフリーで提供、ホワイトペーパーなども公開
 - ・ Forensic Analysis of Internet Explorer Activity Files
 - http://www.foundstone.com/pdf/wp_index_dat.pdf

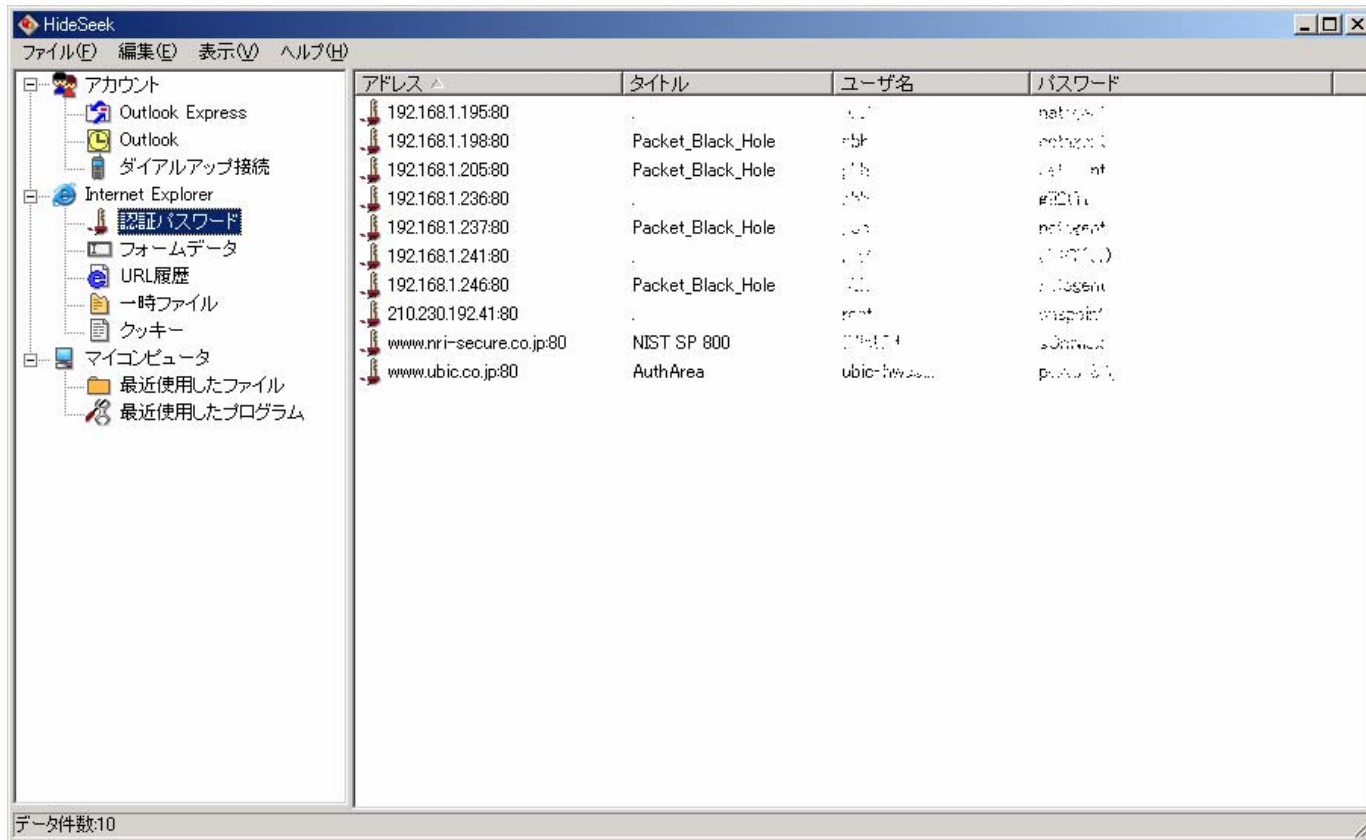
ツール Pasco (2)

- ・ 機能: Index.datを解析してテキスト出力
 - GUIなし: ./pasco index.dat > index.txt
 - オプション: -d Undelete Activity Records
 - t 区切り記号を指定
 - 出力データ
 - ・ TYPE: URL、REDR(リダイレクト)、LEAK(URLの内部分類)
 - ・ URL
 - ・ MODIFIED TIME: MSNやGoogleで乱れることも
 - ・ ACCESS TIME
 - ・ FILENAME
 - ・ DIRECTORY: Contents.IE5以下のフォルダ名
 - ・ HTTP HEADERS: 全て入っている?

ツール Pasco (3)

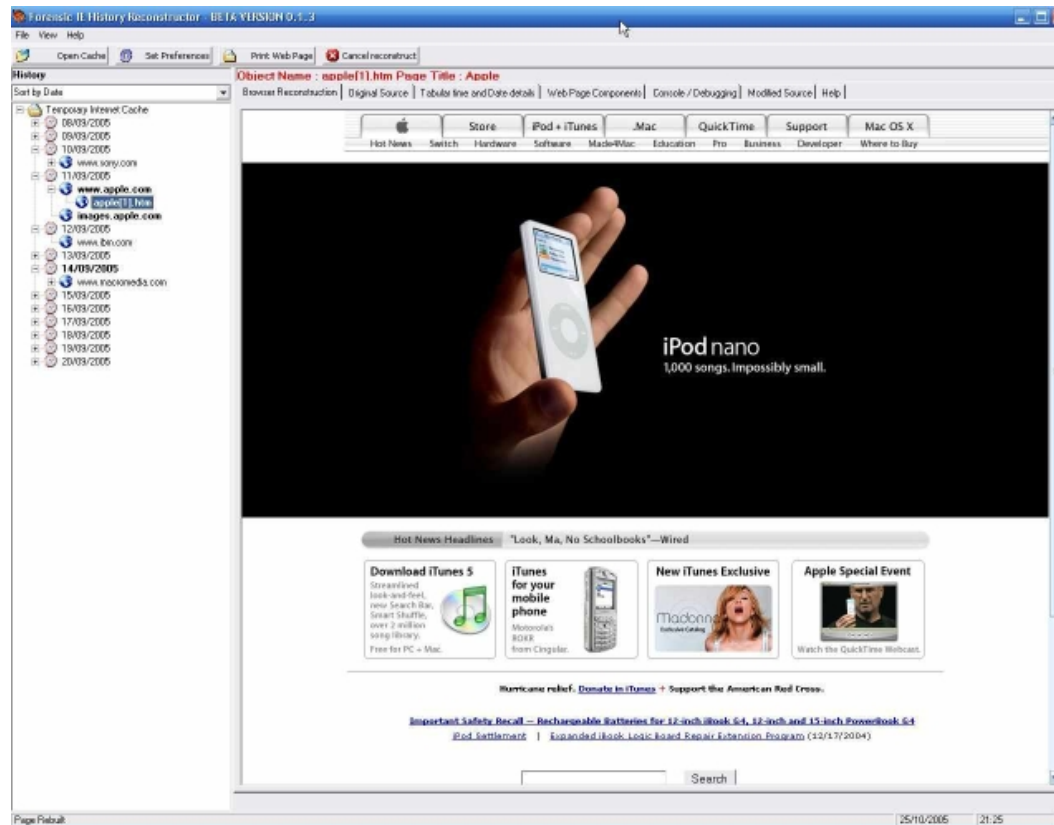
- ・ 特徴：索引情報 (Index.dat内のハッシュテーブル) から削除されているエントリも取り出すことが可能 (Undelete Activity Records)
 - 各レコードは128byteで区切られていて、最初の4byteでType (URL、REDR、LEAK) が見つければ復元が可能

ツール Hideseek



- 札幌ソフト開発工場(セキュリティ関連ソフト・情報を多数公開)
- <http://homepage2.nifty.com/spw/software/hideseek/>

ツール Forensic Internet Explorer



- イギリスの大学院生が作成しているツール
- <http://www.forensicfocus.com/index.php?name=Forums&file=viewtopic&t=516>

今後の課題

- ・ 他のブラウザは？
- ・ Webアプリケーションのキャッシュ情報
 - Webメール
 - サイボウズ
- ・ その他のアプリケーションの履歴情報
 - IME
 - Word

解き明かす力、今すぐにでも。 フォレンジック・サービス

NetAgent

The Forensics Company

<http://forensic.netagent.co.jp/>