フォレンジクス支援の為のWeb閲覧履歴構造化手法

鬼塚, 雄也
九州大学 | 九州先端科学技術研究所

松本, 晋一
九州大学 | 九州先端科学技術研究所

川本, 淳平
九州大学 | 九州先端科学技術研究所

櫻井, 幸一
九州大学 | 九州先端科学技術研究所

出版情報：火の国情報シンポジウム. 2014 (2B-3), 2014-03-04
バージョン：
権利関係：

フォレンジクス支援の為のWeb閲覧履歴構造化手法

鬼塚 雄也[1,2]　松本 晋一[1,2]　川本 淳平[1,2]　櫻井 幸一[1,2]

概要：パソコンやインターネットの普及に伴い，それを利用した犯罪に対しデジタルフォレンジクスが重要となっている．特に HTML5 の普及に伴い WebStorage にはユーザのブラウジングでの行動が残されており，犯罪立件に有用なデータが残されている可能性があるため，これに対するフォレンジクス調査の実施が今後より重要となると予想される．しかしこの調査は，調査の手法の設定，情報の収集，収集したものの結びつけによる証拠の発見に非常に時間がかかってしまう．この調査に要する時間を短縮する必要があり, 本稿ではこれを実現するための,Webstorage 内の対象データの構造化手法を提案する．

Structuration of Web browsing history for forensics

Yuya Onitsuka[1,2]　Shinichi Matsumoto[1,2]　Junpei Kawamoto[1,2]　Kouichi Sakurai[1,2]

Abstract: With the spread of PCs and Internet, Digital Forensics is very important to investigate the crimes using these. Especially, because of the spread of HTML5, WebStorage records the user's action in Internet, and there might be variable data for a crime prosecution, so Computer Forensics for WebStorage will become more important. But this investigation takes time very much to decide a method, collect data, and discover evidence. In this article, to realize shrtening of the time for investigation we propose the technique of structuring target data in Webstorage.

1. はじめに

世界中でのパソコン，インターネットの普及に伴い，デジタル技術は大きく進歩している．最近では, スマートフォン，タブレット端末市場の拡大による普及も進んでおり，日本でもスマートフォンの普及率は約 50 %にも上る．また, ゲーム機や，テレビなどの家電製品でもインターネットに接続できるものが増えてきており，[*1] 様々な機器でインターネットの利用が可能となっている．

パソコンやインターネットの普及により生活の利便性は飛躍的に向上しているが，その反面，これを利用した情報の不正取得，情報の不正流失，端末に対する不正な遠隔操作，等のサイバー犯罪もまた増加している．またメールや，Web ページ上での掲示板や SNS でのやりとりの上で行われるような不正も存在している．こうした犯罪を立証する上で，デジタルデータを証拠として確保し裁判で用いることは非常に重要となってくる．[1] しかし，対象がデータであるがゆえ偽造や改ざん，削除が容易にされうることから，実際の証拠として弱くなってしまう．

この問題を解決するための調査法として，デジタルフォレンジクスの需要が高まってきている．これは通信ネットワーク上やパソコンなどの端末上から証拠となるデータを発見し，改ざんされることなく証拠能力を保ったまま裁判に提出するための調査法である．

デジタルフォレンジクスを実施する際，調査員は

・正しく証拠となるデータをを取り出す
・データ同士の関連付けを行う
・データが改ざんされていないことを証明する

という 3 つのことに気を付ける必要があり，この 3 つの過程によりデータを証拠性のあるものとして扱うことができるようになる．

[1] 九州大学, 福岡県福岡市西区元岡 744 番地
Kyushu University, 744, Motooka, Nishi-ku, Fukuoka, 819-0395, JAPAN
[2] 九州先端科学技術研究所, 福岡県福岡市早良区百道浜 2 丁目 1 番 22 号 福岡 SRP センタービル 7 階
Institute of Systems, Information Technologies and Nanotechnologies (ISIT), Fukuoka SRP Center Building 7F, 2-1-22, Momochihama, Sawara-ku, Fukuoka, 814-0001, JAPAN
[*1] http://tech.hotsukyo.or.jp/seminar/list/003/pdf/20120326_digital_forensic.pdf

また近年，OS や機器に依存せずインターネットに接続させようという流れが高まってきており，このようなウェブアプリケーションのプラットフォームとして，HTML の最新版であり現在策定中の HTML5 が考案された．HTML5 対応のブラウザでは WebStorage の利用が可能で，これに調査を適用することで，より多くの情報を収集することが可能となる．しかしこの調査には，正しくデータを取り出すための手法の設定，実際のデータの収集，収集したデータ同士の結びつけによる証拠の発見という過程が存在し，これらを目視で行うことはに非常に長い時間がかかり非現実的であるという問題が存在する．

ユーザのブラウジングにより WebStorage に保存される情報は本来ブラウザが参照することを前提としているため，人間にとってはそのままのデータは見づらいという難点がある．また，ここに保存されているデータはブラウジングなどを補助するために保存されたもので，フォレンジクス調査に必要となりうるデータのみがあるわけではない．それゆえに WebStorage に保存されている大量のデータから必要なデータのみを取得する必要がある．

本研究の目的としては，調査効率を上げ，調査にかかる時間を短縮することで，デジタルフォレンジクスにかかる時間全体の短縮を目指す．そのために，調査に有益な情報取得の効率を上げ，取得した情報同士の関連付けの半自動化による簡易化，高速化について提案する．

2. デジタルフォレンジクス

フォレンジクスという単語には「法科学」「鑑識」などの意味がある．フォレンジクスに含まれる概念てしては，例えば，筆跡鑑定や DNA 解析，指紋採取などの鑑識調査が存在する．[2] これに対しデジタルフォレンジクスはフォレンジクスから派生した言葉で，デジタルデータを情報通信技術の観点から調査し，証拠を確定させ裁判所に提出していく手法である．これはデータの収集や解析，保管を行い，その法的な証拠性を明らかにする調査を表し，フォレンジクスが法科学という意味を持つように，犯罪に対し適切に法的な処理を行うための調査である．

ここで対象となるのは，パソコン，サーバ，ネットワーク機器，携帯電話，情報家電などのデジタルデータを扱う機器である．[3] 調査として，PC のハードディスクから証拠に当たるデータを探し出す，ログファイルから不正なアクセスの記録を割り出す，破損したまたは消去されたデータの復旧，データの捏造や改ざんの防止，またその検証，が行われる．デジタルフォレンジクス調査は，犯罪を立証するだけでなく，容疑者の無実を証明するためにも用いることができる．

2.1 実際の事例

以下に実際の事件でデジタルフォレンジクスが用いられた事例を幾つか紹介する．

BTK キラー事件

1974 年から 1991 年までアメリカのカンザス州ウィチタで起こった連続殺人事件である．1974 年 1 月 15 日に初の犠牲者でとある一家が殺害され，その 9 ヶ月後に犯人から犯行声明が地元の新聞社に送りつけられた．犯人は自らを，「縛る（bind)」「拷問する（torture)」「殺す（kill)」の頭文字から，BTK と名乗った．これが 1974 年から 1991 年までの間に 10 人もの人々が殺害された連続殺人事件となった．その後しばらく犯人からの音沙汰がなかったが，2004 年に再び地元テレビ局や他メディア局へ手紙を送ってきた．その際，1986 年に起こっていた殺人事件の犯人が自身であるとし，犠牲者の免許証や写真を送っていた．2005 年頃に警察に犯行声明のためフロッピーディスク送られ，FBI はこれに対しフォレンジクス調査を行った．この調査により発見されたデータからそのフロッピーディスクに書き込んだコンピュータとそれを所有する協会を特定し，ここに通う容疑者へたどり着いた．こうして 2005 年 2 月 25 日に犯人は逮捕された．

ライブドア事件

証券取締法違反の容疑で 2006 年 1 月 16 日に東京地検特捜部によりライブドア本社及び社長自宅にて家宅捜索が行われた．しかしこの捜索の際．当時の報道によると，数万通にも及ぶメールがすでに削除されていた状態であった．ここで東京地検はフォレンジクス調査を導入しメールの復元を試みた．その結果メールの大部分の復元に成功し，関係者の有罪を示した． その後同年 1 月 23 日に証券取引法違反の容疑で関係者 4 名が逮捕された．

大阪地検特捜部主任検証拠改ざん事件

郵便割引制度を悪用して多額の郵送料を免れたとして，大阪地検特捜部は 09 年 2 月から広告会社幹部らを摘発した．しかし，変換された証拠品であるフロッピーディスクのデータの一部の最終更新日が検察への提出時と変わっていることが判明した．これについて裁判の証拠としても保てるようにフォレンジクス調査が行われた．その結果確かに最終更新日が改ざんされていることが明らかになった．また改ざんされた日も判明し，フロッピーディスクが検察の手にあるときに意図的に改ざんされたものだということも判明した．証拠をを改ざんしたとして，捜査主任の検事が 2010 年 9 月に証拠隠滅容疑で逮捕された．また，翌 10 月には改ざんを隠したとして当時の特捜部長と副部長が逮捕された．

上記の例のように様々なところでデジタルフォレンジクスに関連する事件は発生している．他に，企業の内部からの情報流失や著作権関係での事件においても，漏洩事実や

漏洩経路の明確化，データ内容の時間関係の確認等にデジタルフォレンジクスは用いられている．

デジタルフォレンジクスは，法的な分野で刑事事件と民事事件，また調査を請け負うビジネスの分野での利用も存在し，3 つの分野をカバーするようになっており，デジタルフォレンジクスの需要は非常に高いものとなっている．

2.2 ネットワークフォレンジクスとコンピュータフォレンジクス

デジタルフォレンジクスは調査対象や調査方法から「ネットワークフォレンジクス」と「コンピュータフォレンジクス」の大きく 2 つに分けられる．

・ネットワークフォレンジクス

ネットワークフォレンジクスとはコンピュータネットワーク上を流れるデータを対象とした調査である．この調査では，まずネットワーク上を流れるすべてのパケットを取得し保管する．そして，すべての通信の断片から元のデータを復元することで，どの端末からどのネットワークを介して何が行われたのかを解析を行う．これによりマルウェアの挙動の解析や，情報流失の経路の解明などを行うことが可能である．ネットワークフォレンジクスで対象となり得るデータの例として，Web ページアクセスのログ，メールのやりとりのログ，ファイルの送受信ログなどが考えられる．

また，ネットワークフォレンジクスはインシデントが発生する前の予防としても活用可能である．内部ネットワーク上の通信データを取得し，不審な挙動を行っている PC を特定し，管理者に警告を出すことができる．これによりその端末の操作記録を追跡できるため，ネットワークフォレンジクスの存在を組織内に周知させることで，内部からの情報流失を抑制することができる．

・コンピュータフォレンジクス

コンピュータフォレンジクスはコンピュータ内に保存されているデータを対象とした調査である．コンピュータフォレンジクスでは，まず不正を行ったとされるコンピュータの確保を行い，ハードディスクを取り出す．これを，実際に法廷での証拠用のハードディスクと，調査員が使用するための解析用のハードディスクに，完全な複製を行う．証拠用のハードディスクは証拠性を証明する書類とともに厳重に保管される．これを用いることで証拠に一切の変更が加えられていないことを示し，法的な証拠性を保つようにする．次に解析用のハードディスクに対して実際の調査が行われる．存在するファイルの内容の分析，ファイルへのアクセス時刻の調査，改ざんされたデータの発見と修復，また削除されているデータの復元と解析などが行われる．この調査で対象となり得るデータの例としては，Web ページ閲覧履歴データ，パスワード履歴データ，フォーム履歴データ，メール送受信データ，削除されたファイルなどが考えられる．

このようにして原因や証拠となるデータまたはいくつかのデータを関連付けして作成した証拠を取得する．コンピュータフォレンジクスはこのようにインシデントが発生した後に行われる調査である．

2.3 組み合わせた適用例

上で上げたこの 2 つの調査はデジタルフォレンジクスの一連の手順となっており，ネットワークフォレンジクスにおける通信のデータ解析から不正を行っているパソコンを特定し，特定したパソコンをコンピュータフォレンジクスで調査していく．ここで，ネットワークフォレンジクスとコンピュータフォレンジクスの組み合わせによる調査を例を用いて紹介する．

とある企業で機密情報の内部流出が起こったとする．この場合，事後調査としてまずネットワークフォレンジクスが行われる．ここで情報の流出経路を特定し，今回の場合企業の内部ネットワークからの流出であったと特定したとする．次に端末の特定を行う．企業内部ネットワークに接続されていた端末から，情報を流出させた可能性のあるものを絞り込んでいく．ここでどの程度絞り込めるかで調査にかかる費用や時間も大きく変化してくる．以上がネットワークフォレンジクスに当たる部分である．

次に絞り込んだもしくは特定した端末への調査を行っていく．端末の HDD やメモリの状態をデータが専用機器で失われないよう別のストレージに複製する．この複製作業において揮発性の高いものから順に行っていく必要がある．[4] この複製したストレージを証拠の保存用と，調査用とを用意する．証拠の保存用をデータが失われないよう保存することで，オリジナルデータの保全を行い，このデータに法的証拠能力を持たせる．調査用のデータからコンピュータの使用履歴の確認，漏洩したファイルの特定，感染ウイルスによるものだった場合ウイルスの感染形跡の確認などを行い，事件の詳細の特定や犯人の特定を行う．

3. HyperText Markup Language

3.1 HTML5

HTML は 1990 年代前半に導入されてから何度も改訂されており，仕様の変更や導入，タグの追加や削除が行われている．現在，HTML の最新版として HTML5 が存在する．HTML5 は Web アプリケーションを OS に依存させずに動かすためのプラットフォームを目指して考案されたものである．また，HTML5 はすでに広く使われているコンテンツを取り扱う方法において，下位互換性が保たれるように規定されている．

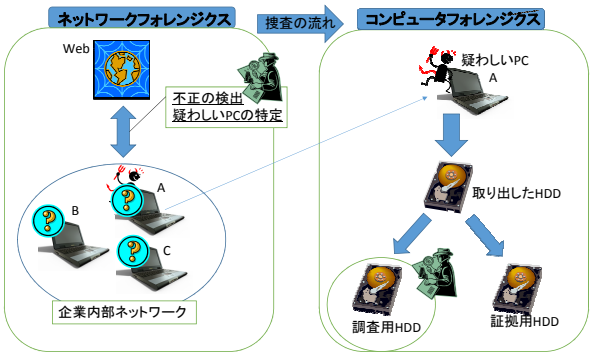

図 1　デジタルフォレンジクスの適用例

ウェブアプリケーションの共用プラットフォームとしても HTML5 は注目されている．これにより Web ブラウザ対応の端末であればどのような機器でも同じアプリケーションを使用することが可能となる．またスマートフォンなどのモバイル端末向けの機能も提供しており，HTML5 ベースのアプリケーションを使用して通話や，メールの送受信，写真撮影，端末の振動機能，などのスマートフォンでの機能の実装も可能となる．[5], [6]

3.2　WebStorage 機能

HTML5 で扱うことのできる機能に WebStorage がある．これは Web 上でのデータのやり取りの際にデータをクライアント側に保存する機能である．データをクライアント側で保存する方法としては Cookie が一般的であったが，WebStorage は従来使われている Cookie よりも簡単に，また大量のデータを長期間クライアント側に保存することができる．[7]

以下に WebStorage 機能の特徴を上げる．

保存容量

Cookie が 4KB であったのに対し，WebStorage は約 5MB の容量を持つ．これによりクライアント側でサイズの大きなデータを取り扱うことが可能となる．

有効期限

Cookie が有効期限が決まっており，それが過ぎると消去されていたのに対し，WebStorage では読み込んだデータの永続的な保存が可能となる．一部例外となる部分があるがそれについては後述する．

送信

データを毎回サーバに送受信せずとも格納，参照が可能となる．これによりネットワーク負荷が軽くなる．また自動的に送信されないためユーザーにとってセキュリティ的に安全となる．ブラウザによって一旦 Cookie を保存すると，その Cookie の提供元の Web ページはユーザの許可無く保存した Cookie から情報を得ることができる．

保存形式

データ保存の方法として，任意の保存したいデータに対して，対応する一意の標識を設定し，これらをペアで保存するキーバリューストアという形式で保存を行っている．

WebStorage には sessionStorage と localStorage という 2 種類のストレージが用意されており，目的によってそれぞれ使い分けられている．[8] これらのストレージについて説明していく．

- localSorage

  localStorage ではオリジン (origin) 単位でデータを保存, 管理している．[9] オリジンとは「http://www.kyu-shu.com:8080/」のように，「プロトコル」，ドメイン」，「ポート番号」の組み合わせからなる識別情報のことで，これらのうち一つでも異なるものがあった場合，localStorage では別物のデータとして扱われる．このため現在のホストで保存したデータを異なるホストで読み込むということは不可能となるが，localStorage は異なるタブやウィンドウ同士でも同じオリジン内であればデータを共有可能である．

  また，localSorage に保存されたデータはブラウザを閉じても消えることがなく，永続的に蓄積されていく．使用例として，ブラウザを閉じても保存されたデータが消えないという特徴を利用することで，ユーザー環境をレジストリのように維持することが可能となる．例えば Web ページ閲覧者が選択した背景色や文字色のテーマなどを localStorage に保存し維持する，ということが考えられる．

- sessionStorage

  sessionStorage もまたオリジン単位でデータの管理を行っている．しかし，localStorage と違い，複数のタブやウィンドウ間でのデータの共有はされないようになっている．

  sessionStorage はブラウザが起動している間のみ有効となるストレージである．[10] sessionStorage に保存されたデータはブラウザを閉じたタイミングで破棄される．

  使用例として，ブラウザを閉じたタイミングで保存されたデータが破棄されるという特徴から，ブラウザ起動後の初アクセス時にのみアプリケーションのチュートリアルを表示させたい場合などチュートリアルを表示したという情報を保存することで可能となる，というものが考えられる．

これらのような違いが存在する．それぞれの特徴にあわせて使い分けることで快適なブラウジングを行うことが可

表 1　使用したソフトウェア

Hardware
o 1- Desktop (PC- forensic workstation- 4GB RAM)
o 8- 160GB SATA Hard Drives (one dedicated drive)
o 1- USB Flash Drive (8GB)
o 1- USB External Drive (1TB WD Passport)
o 1- SATA to USB Adapter
o 1- Tableau USB Write Blocker (IDE/SATA)

表 2　使用したハードウェア

Software
o Microsoft Windows 7 Professional (64)
o Internet Explorer, Firefox, Safari, Chrome
o VMware- virtualization software
o DaemonFS- file integrity monitoring program
o Disk Wipe- to replace all data on disk with zeros
o Nirsoft Internet Tools- history, cache, and cookie viewers
o PortableApps- portable application Launchpad
o Firefox Portable, Chrome Portable, Opera Portable
o FTK Imager- used to create forensic images
o FTK Imager Lite- portable version
o AccessData FTK version 3.2 (Licensed)- used to analyze forensic images and organize information

能となる．

4. 関連研究 : プライベートブラウジング，ポータブルブラウザで残される情報の調査

インターネットユーザーにとって，通常のタスクとは別に，ブラウザの機能であるプライベートブラウジングを使用することも必要となってくる．プライベートブラウジングはセッションの終了時にブラウジング中にたまったデータを破棄する，またはセッション中にデータを蓄積させない機能である．これには 2 つの目的があり，前者はユーザーのインターネットでの行動履歴をウェブサイトのサーバーから追跡されることなくブラウジングを行うこと，後者は使用しているパソコンにユーザーのインターネットでの行動履歴を残さずにブラウジングを行うことである．この 2 つ目の目的は例えば複数人で共有のパソコンを使用する場合などに特に必要となり，この研究 [11] では後者の目的に焦点を当てている．

この研究では，4 つのブラウザ InternetExplorer，GoogleChrome，Firefox，Safari，での通常のブラウジング後，プライベートブラウジング後それぞれに対しディスクを完全分析することでクライアント側に残されているデータを収集している．また 3 つのポータブルブラウザ OperaPortable，FirefoxPortable，GoogleChromePortable，でのブラウジング後にも同様の調査を行っている．

実験手順は以下のとおりである．

表 1,2 に記した機器やソフトを使用し，通常ブラウジング，プライベートブラウジング，ポータブルブラウジングに対し実験が行われた．手順として，プライベートブラウジング時に一連の決められた行動を行い，プライベートブラウジング終了時にメモリをダンプし，レジストリファイル，システムファイルを取得し，RAM のイメージファイルを作成する．これと同様の操作をそれぞれのブラウザで行っていく．また，ポータブルブラウザを USB フラッシュから動作させ，プライベートブラウジング時と同様の操作を行う．その後，フォレンジクスツールでの解析をそれぞれのデータを保存したハードディスクに対し行うことで，それぞれのブラウジングについての実験を行う．

以上のような実験の結果，表 3 のような結果とそれぞれのファイルが発見された場所が得られた．この実験によりそれぞれのデータが残されるであろう場所の特定が行われた．

5. 提案手法

WebStorage に保存されている情報は機械可読なものであり人の目による閲覧性は考慮されていない．そのため，WebStorage に保存されているデータを調査する場合，そのままのデータでは見づらく，情報の精査や結びつけを目視で行うことは困難であるという難点がある．本研究では，ブラウザの sessionStorage 内のデータの構造化手法を提案する．これは WebStorage に残されている大量のデータから，ユーザーのページ既読情報を取得し閲覧したページ情報をを木構造的に表現するための手法である．

5.1 事前調査

主要なブラウザが WebStorage に対応済みであることは第 2 節で触れた．ブラウザごとの WebStorage の場所を以下にまとめる．

今回，Windows 版の Firefox 26.0 で自由にブラウジングを行い，sessiontorage に保存されたデータを削除が行われる前に確認することで，Sirefox の sessionStorage にキーバリュー形式でどのようにデータが保存されているかを調査した．結果として，図 2 のような形式で保存されており，図 3 のようなキーの構造が見られることがわかった．

図 3 に示したキーバリュー構造について今回の調査で判明したことをいくつか述べる．以下では [ ] で囲んでいるものをキーであるとして説明する．[windows][tabs][entries] 下に [url]，[title]，[ID]，[referrer] などのキーとバリューの集合が存在する．この集合ひとまとまりでひとつの Web ページ情報となっており，1 つの [entries] 下にこの集合が複数存在する．例えば [url] はその Web ページの URL 情報を持っており，[title] はその Web ページのタイトル，[referrer] はその Web ページのリンク元となった URL をバリューとして持っている．またこれらと同列に存在する [chldren] は，この Web ページに埋め込まれている広告の Web ページ情報などを持っている。この時，1 つの [entries]

表 3　実験結果一部

	IE 8.0 Inprivate Browsing	Chrome 23.0.1271.95- Incognito	Firefox 17.0.1- Private Browsing	Safari 5.1.7- Private Brows- ing	Google Chrome Portable	Opera Portable	Mozilla FireFox Portable
Browsing Indicators	✓	✓	✓	✓	✓	✓	✓
Browsing History	✓	✓	✓	✓	✓	✓	✓
Usernames/ Email Accounts	✓				✓		✓
Images	✓	✓	✓	✓	✓	✓	✓
Videos						✓	

下に存在する複数の Web ページ情報の集合で 1 つのタブの情報となっており，つまり 1 つのキー [entries] に対するバリューとして 1 つのタブで閲覧した Web ページ情報の集合が存在している．

この [entries] というキーもまた，一つの [tabs] 下に複数存在する場合があり，これはセッション中に複数のタブが存在したことを表す．

さらに，[tabs][selected][_closedTabs] などの同列のキーバリューの集合が複数存在していた場合，セッション中に複数のウィンドウが開かれていたということになる．以上のこととほぼ同じことが，閉じられたタブやウィンドウの情報が格納される [_closedTabs] や [_closedWindows] に対しても言える．

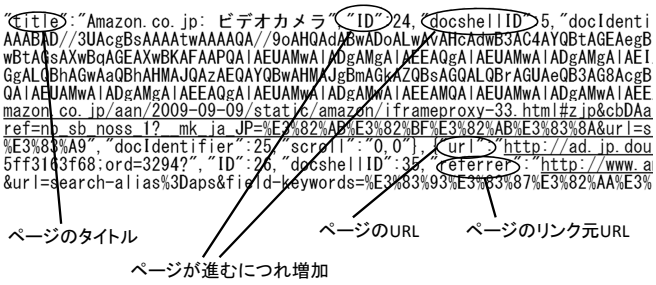

図 2　sessionstorage 内容一部抜粋

表 4　WebStorage 対応ブラウザ [12]

ブラウザ	対応バージョン	保存場所
Internet Explorer	8 以降	未確認
Firefox	3.6 以降	C:\Users\ <windowsUsername> \AppData\Roaming\Mozilla \Firefox\Profiles\ <profile folder>
Google Chrome	8 以降	C:\Users\ <windowsUsername> \AppData\Local\Google \Chrome\ UserData\Default
[13] Opera	11 以降	C:\Users\ <windowsUsername> \AppData\Roaming\ Opera Software\Opera Stable
Safari	5 以降	C:\Users\ <windowsUsername> \AppData\Local\ Apple Computer\Safari

sessionStorage はブラウジングの終了時に保存されたデータを消去することは第 3 節で言及したが，Firefox ではどのタイミングで消去されているのかを実際にブラウジングを行い sessionStorage の変化を見ていくことで調査した．ブラウザ起動時，ブラウジング途中，ブラウジング終了時，ブラウザプロセス終了時，次回ブラウザ起動時に調査した結果，sessionstorage に保存されたデータはブラウザプロセス終了時ではなく，次回ブラウザ起動時に消去されていることがわかった．これはブラウザの仕様により，前回のタブの復元を任意で行えるようにするためであると考えられる．

5.2　提案方式

フォレンジクス調査により essionStorage から蓄積されているデータを収集し犯罪捜査を行うことを仮定する．sessionStorage の内容はユーザーがブラウジングで自動的に蓄積したデータであるが，閲覧したページ上の広告情報やページの表示サイズの情報，ウィンドウのサイズの情報などのデータも大量に存在し，調査に必要なデータのみが

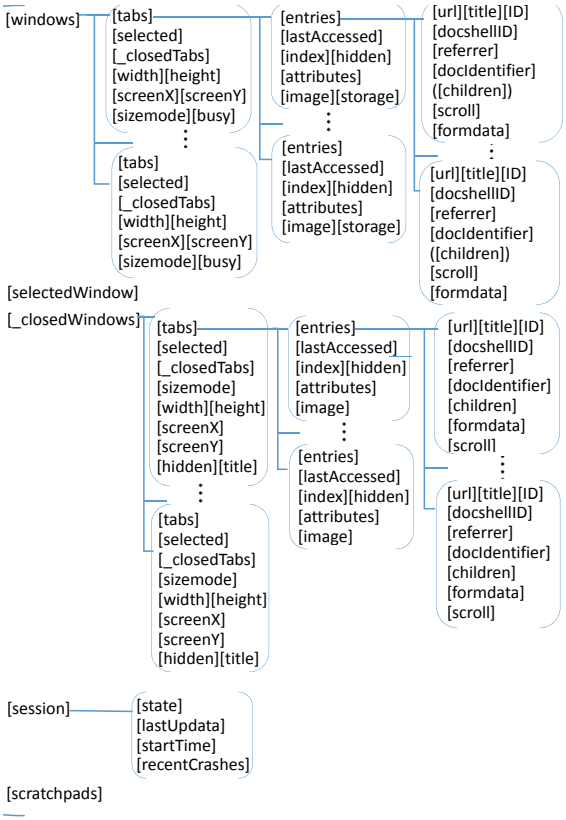

図 3　sessionstorage の key 構造

存在するわけではない．ここで，事件捜査に必要であると考えられるデータのみを抽出することが重要となってくる．目視のみでは調査に時間のかかってしまうこの過程において，必要な情報のプログラムによる半自動的な構造化を提案する．提案手法で今回は Firefox の sessionStorage に対し調査を行う．sessionStorage は複数ウィンドウが開かれている場合そのすべてのウィンドウが閉じられるまで情報を貯め続けることが事前調査で分かった．このことから sessionstorage からは最後に閉じたウィンドウの情報のみではなく，同じセッション中にすでに閉じられていたタブやウィンドウでの情報も取得することができる．また，sessionStoeage はバックアップファイルとして常に 1 つ前のセッションでの情報を保存している．このファイルと，Firefox の sessionStorage の内容を消去するタイミングの仕様により，閉じられたブラウザでのセッション情報，またバックアップファイルとしてさらにその一つ前でのセッションの情報を取得することができる．

5.3　実装内容

プログラミング言語 Python で提案手法の実装を行っていく．[14]

まず sessionStorage の存在するディレクトリを指定する．Firefox の sessionStorage へのパスは

”C:\Users\<WindowsUserName>\AppData\Roaming\Mozilla\Firefox\Profiles\<********.default>\ sessionstore.js”

である．調査手順として，

- ディレクトリを指定し sessionStorage の内容を実験環境に読み込む
- 収集した Web ページ情報の群を，木構造の根となり得る Web ページとそれ以外の Web ページに分類分けを行う
- 根となるページ情報に含まれる [url] と一致する url を [referrer] に持つページ情報を探す
- 見つかれば次はそのページ情報の [url] と一致する [referrer] を持つページ情報を探索する
- 見つからなければその根での探索は終了し，そこまでのページ情報の [url]，[title]，[ID]，[docshellID]，[referrer] の値を表示する
- 根からどれ程離れたノードかを”*”の数で表現する
- 次の根から探索を開始する
- すべての根での探索を終えたら終了する

を行う．また，sessionStorage には直接閲覧した Web ページ以外に，Web ページに埋め込まれている広告などの Web ページ情報も含まれているが，今回はそれは不要であるとみなし避ける．

6.　考察

実際に動作の評価実験を行った．ブラウザ Firefox26.0 を起動し，スタートページからブラウジングを行った．その際にどの Web ページからどの Web ページへ移動したか，どの順番で Web ページが開かれたかを記録した．一定時間ブラウジングを行い，その後 sessionStorage に対し調査を行った．これにより図 4 のような結果が得られた．”*”の数で根となるページからどれほど後に開かれたページかを表現する．通常ブラウザで閲覧した Web ページと等しい結果が得られたので，これにより必要となるページの情報のみを木構造で確認することが可能になった．また，実行結果に時間はかからず，効率面でも問題はなかった．

しかし，一部実験により [url] と [referrer] が一致しない場合が見られた．これは Google 検索でキーワードを検索しその結果からページを読み込んだ際に，表示したページ情報の [referrer] が変化しているように見られた．使用する検索ツールを google から yahoo，bing に代えそれぞれ同じ検索結果のページにアクセスし，sessionStorage を確認したが，どちらもその際の [url] と [referrer] は一致していた．よってこれは Google 検索ツールを使用した時のみに起こると考えられる．これに対する対策法も考えていく必要がある．

6.1　まとめ

本稿では，sessionStorage に保存される Web ページ情報に対する調査の為の，対象データの構造化の提案と調査

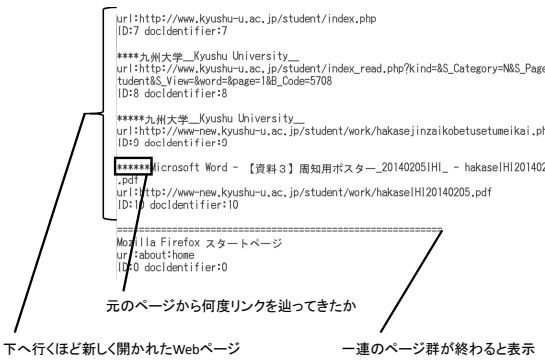

図 4 評価実験結果一部抜粋

を行った．これにより sessionStorage に残された情報からフォレンジクス調査に必要となるデータの確認と取得に成功した．

今後の課題として，例外の時に対する処理法の考案，sessionStorage 内のデータで何を表しているか不明なものも多いのでこれらに対する調査を行う必要がある．また，IE や Chrome などの他のブラウザに対してもデータの構造化を行えるようにすることで，ブラウザによらず実行できるようにしていく必要がある．

また，今回 localStorage は取り扱わなかったが，sessionStorage とは仕様が異なる部分があるため，sessionStorage にはないデータが localStorage に存在するのではないかと考えられる．よってこちらに対する調査も同様に進めていく必要がある．

参考文献

[1] Cory Altheide, Harlan Carvey “DIGITAL FORENSICS WITH OPEN SOURCE TOOLS”, Syngress, 20114 月 28 日

[2] 重みを増すデジタルフォレンジクスの役割 -法廷におけるデジタルフォレンジクスの活用の現状について- - DIGITAL GOVERNMENT & FINANCIAL TOPICS（最終確認日：2014 年 2 月 1 日）, http://e-public.nttdata.co.jp/topics_detail2/contents_type=2&id=421

[3] John Sammons, “THE BASICS OF DIGITAL FORENSICS The Primer for Getting Started in Digital Forensics”, Syngress, 2012 年 3 月 9 日

[4] Guidelines for Evidence Collection and Archiving（最終確認日：2014 年 1 月 30 日）, http://www.ipa.go.jp/security/rfc/RFC3227JA.html

[5] スマホ開発者が知るべき Tizen や Firefox OS の特徴～第 35 回 HTML5 とか勉強会 - Web+OS 最前線! レポート — イベントカレンダー＋ログ（最終確認日：2014 年 2 月 1 日）, https://event.atmarkit.co.jp/events/d559c6b95217176d7998a67c915d93c7/atmarkit_report

[6] HTML5 ベースのプラットフォーム：「Firefox OS」搭載のプレビュー端末、2 月めどに開発者向けに提供開始 - @IT（最終確認日：2014 年 1 月 29 日）, http://www.atmarkit.co.jp/ait/articles/1301/23/news101.html

[7] HTML5 Web Storage（最終確認日：2014 年 2 月 1 日）, http://www.w3schools.com/html/html5_webstorage.asp

[8] 連載：人気順に説明する初めての HTML5 開発：ブラウザでストレージ？ Web Storage を使いこなそう (1/3) - @ IT（最終確認日：2014 年 2 月 1 日）, http://www.atmarkit.co.jp/ait/articles/1108/12/news093.html

[9] DOM Storage - DOM — MDN（最終確認日：2014 年 2 月 1 日）, https://developer.mozilla.org/ja/docs/DOM/Storage

[10] Web Storage（最終確認日：2014 年 2 月 1 日）, http://dev.w3.org/html5/webstorage/

[11] Donny Jacob Ohana, Narashimha Shashidhar, “Do Private and Portable Web Browsers Leave Incriminating Evidences? A Forensic Analysis of Residual Artifacts from Private and Portable Web Browsing Sessions”, *EURASIP Jounal on Information Security 2013*, pp., November 2013

[12] Can I use... Suport tables for HTML5, CSS3, etc（最終確認日：2014 年 1 月 29 日）, http://caniuse.com/#cats=HTML5

[13] プロファイル — Firefox ヘルプ（最終確認日：2014 年 2 月 1 日）, https://support.mozilla.org/ja/kb/profiles-where-firefox-stores-user-data

[14] TJ O’Connor, “VIOLENT PYTHON A Cookbook for Hachers, Forensic Analysts, Penetration Testers, and Security Engineers”, Syngress, 2012 年 11 月 22 日