JPCERT-ED-2009-0002
JPCERT/CC

技術メモ － MACtime からわかるファイル操作

～MACtime 証跡リストの作成とその読み解き～

初　版：2009-11-02 (Ver. 1.0)
発行日：2009-11-02 (Ver. 1.0)
執筆者：宮﨑 清隆

本文書の掲載 URL：http://www.jpcert.or.jp/ed/2009/ed090002_20091102.pdf

本文書では、多くのファイルシステムにおいてファイル操作の実行時刻を記録している MACtime と、その調査ツールの活用方法を紹介します。MACtime の調査ツールから得られる情報は、ファイル操作の実行時刻、および、その順序、さらに、そこに隠れているファイル操作の意図や背景の推測に活用できます。

目次

1. はじめに

多くのファイルシステムは、MACtime と呼ばれるファイル操作の実行時刻を、ファイルやディレクトリの属性情報の中に記録している。本技術メモでは、MACtime の概要を述べ、MACtime の調査ツールと活用方法を紹介する。MACtime の調査ツールを用いると、ファイルシステム内の全ファイルと全ディレクトリの MACtime が一括収集できるだけでなく、ファイル操作の実行時刻を時系列順に整理したリストも作成できる。そのリストを読み解くことによって、ファイル操作の実行時刻、および、その順序がわかり、そこに隠れているファイル操作の意図や背景を推測できる。

情報セキュリティ分野の技術者であれば、サーバへの不正侵入時の被害調査や手口調査、マルウエア等の不正なプログラムのファイル操作調査などの場面において、特定のファイルに対する操作と操作の実施時刻を明確にしたいと考えたことがあるかも知れない。MACtime の調査ツールを用いれば、ファイルシステム内の全ファイルと全ディレクトリへのファイル操作をリスト形式で得られ、ファイル操作の意図や背景の推測に役立つ。特に、明確なファイルの改ざんや消去の痕跡がない不正侵入されたサーバやＰＣにおいて、その不正侵入の痕跡の探索や影響範囲の推定をする場合、MACtime の調査以外の方法では対応が困難な場面も考えられる。

以降本技術メモでは、第 2 章で MACtime そのものを紹介し、第 3 章で MACtime を整形したファイル操作イベントの作成方法を述べる。第 4 章では、MACtime の調査ツールの概要を紹介し、第 5 章で、具体的な調査ステップと調査ツールを活用する際の注意点を記した。第 6 章で、ファイル操作の意図や背景を、2 つの調査例を通じて実際に推測する。

2. MACtime とは？

MACtime とは、ufs、ext3、NTFS などのファイルシステムに保存されている 3 つのタイムスタンプ mtime、atime、ctime の総称である。ファイルシステムにおいて個々のファイルやディレクトリは、その名前、属性情報、ファイル本体もしくはディレクトリエントリの情報を持つ。MACtime は属性情報の一部にあたる。一般的に我々がよく目にするタイムスタンプは mtime で、最後に更新された時刻が記録されている。この他、atime には最後にアクセスされた時刻が、ctime にはタイムスタンプ以外の属性情報の最終更新時刻が記録されている。図 1 に、ファイルやディレクトリの属性情報と MACtime の関係を示す。

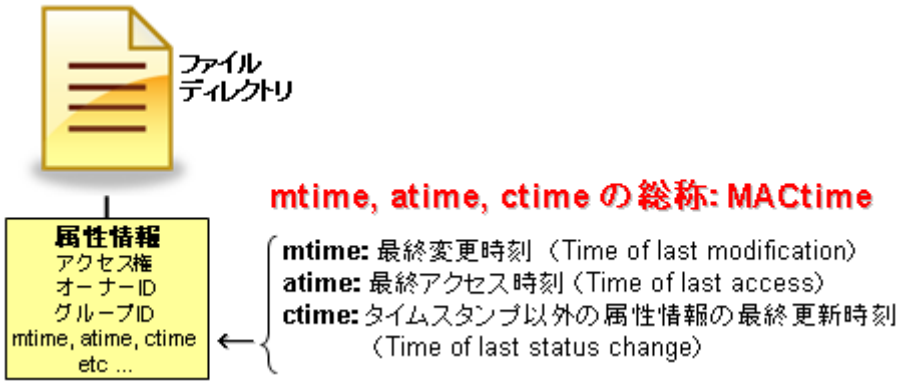

図 1. ファイルやディレクトリの属性情報と MACtime の関係

各ファイルやディレクトリの MACtime を調べることにより、ファイルやディレクトリに対する最終アクセス時刻や最終変更時刻が判明する。場合によっては、ある時間帯におけるファイルへのアクセスや変更の有無を特定することもできる。次に、ファイルの mtime、atime、ctime が変更される際の概要を、図 2 に示す。

図 2. ファイルの mtime、atime、ctime が変更される際の概要

なお、mtime、atime、ctime の値に影響を与えるファイル操作等の詳細については、付録を参照されたい。

3. MACtime 証跡リストへの変換

ファイルやディレクトリには、2 章で述べたように MACtime が記録されており、最後に変更された時刻、最後にアクセスされた時刻、最後にファイルやディレクトリの属性情報が変更された時刻を把握できる。調査したいファイルやディレクトリが特定できていれば、*stat* コマンドや *ls* コマンドを用いてそのファ

イルの MACtime を調べることにより、そのファイルに対する直近の操作時刻を得られる。しかし、調査に着手した時点では、調査すべきファイルやディレクトリが特定できていない場合も少なくない。そうした場合にも、MACtime を活用することで、ある期間内において操作されたファイルやディレクトリの特定と、それらに対して行われたファイル操作の特定が可能となる。

ある特定の時間帯に操作されたファイルやディレクトリを特定するために、各ファイルやディレクトリの MACtime を、図 3 の中央部分に示すように変換する。変換前は、各ファイルやディレクトリに対する MACtime を含む属性情報であったが、変換後は、ファイルと MACtime の主従関係が入れ替わり、何時、何のファイルやディレクトリに、どんなファイル操作がされたかを示す情報として解釈できるようになる。例えば、ファイル F の mtime、atime、ctime の値が、それぞれ t_1 、t_2 、t_1 であった場合、ファイル等の操作イベントとして表現しなおすと‘t_1 : F : {mtime, ctime}’と‘t_2 : F : {atime}’の 2 つイベントに変換される。これを、以降、MACtime 証跡とする。特に、後者の‘t_2 : F : {atime}’は、「時刻 t_2 にファイル F に対してアクセス操作が行われ、その後アクセスされていないこと」を意味するものと解される。図 3 の中央部分では、2 つのファイル a.txt、b.txt の MACtime を、5 つの MACtime 証跡に変換する例を示している。

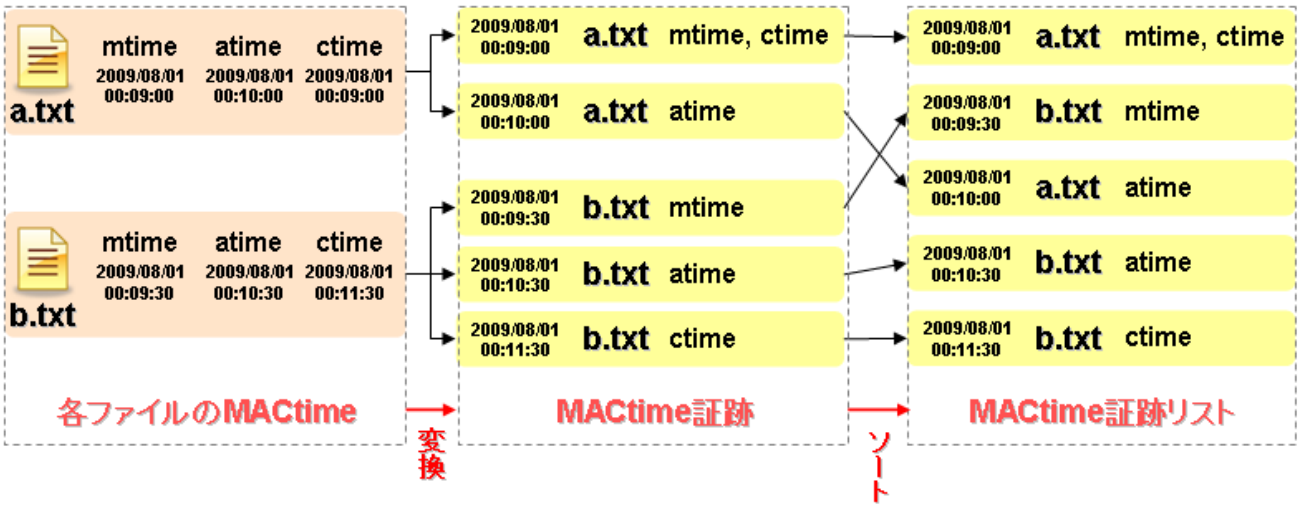

図 3. 各ファイルの MACtime から MACtime 証跡、MACtime 証跡リストへの変換

さらに図 3 の右側では、5 つの MACtime 証跡を時系列順に並び替えたリストの作成例も示している。このリストを、以降、MACtime 証跡リストとする。このリストは、時系列順のファイル操作を示している。

MACtime 証跡リストを用いて、ある期間内において操作されたファイルやディレクトリを特定する例を、図 4 に示す。図 4 中の緑色で囲ったリストは、とあるハードディスク内の全ファイル・全ディレクトリの MACtime を取得した後に、MACtime 証跡リストを作成したものから一部抜粋したものである。MACtime 証跡を時系列順に並び替えることで、特定の時刻に操作されたファイルの特定と、そのファイルに行われたファイル操作のイベントが明確になることが、この例から把握できる。

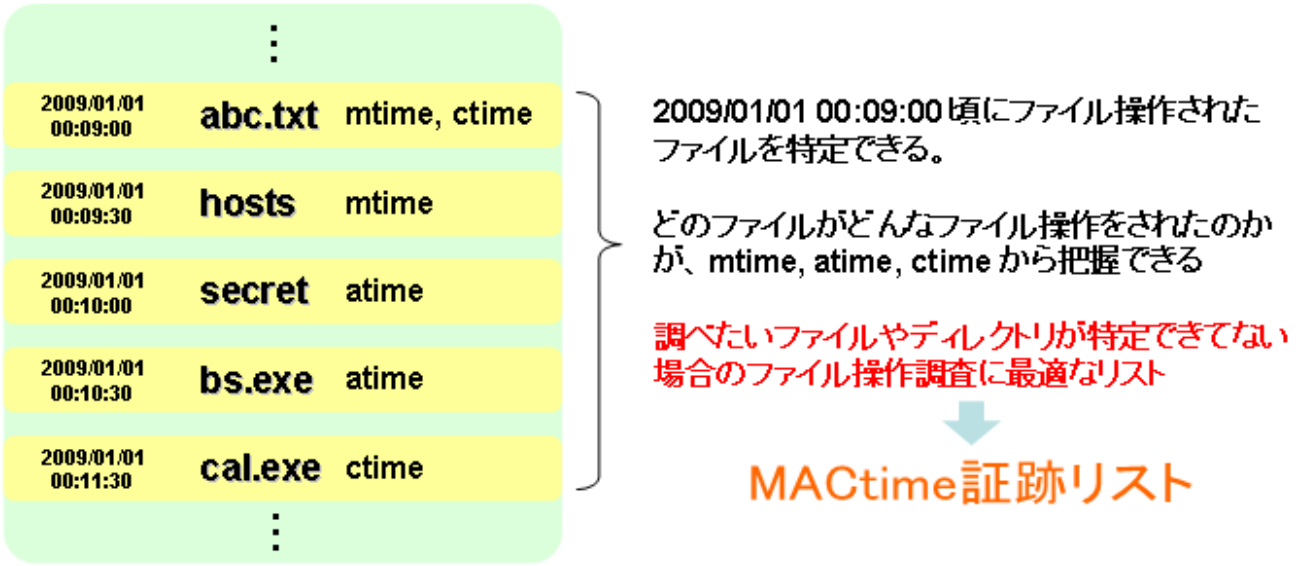

図 4. MACtime 証跡を時系列順に並び替えた MACtime 証跡リスト

MACtime 証跡リストは、MACtime の調査ツールを用いて容易に作成できる。以降、そのツールと MACtime 証跡リストの作成までの手順を紹介する。なお、MACtime 証跡リストの読解方法については、6 章で調査シナリオと共に紹介する。

4. MACtime の調査ツールの紹介

MACtime 証跡リストを作成できる MACtime の調査ツールとして、*mac-robber* ツールと *mactime* ツールがある。この 2 つの調査ツールを組み合わせて利用することで、MACtime 証跡リストを作成できる。まず *mac-robber* ツールを用いて、指定したディレクトリ以下に含まれる全てのファイルとディレクトリの属性情報を一括収集し、次に、*mactime* ツールを用いて、*mac-robber* ツールで得た属性情報に含まれる MACtime を整形・抽出し、MACtime 証跡リストを作成する。

mac-robber ツールと *mactime* ツールは、GPL ライセンスに基づいて配布されており、無料で利用できる。次の Web ページからダウンロードして入手することができる。

- *mac-robber*
  http://www.sleuthkit.org/mac-robber/desc.php
  執筆時点で公開されているのは Version 1.0.0 であり、これを利用する。

・ *mactime*

http://www.sleuthkit.org/sleuthkit/

mactime ツールは、他の調査ツールと共に The Sleuth Kit に含まれているので、これをダウンロードする。執筆時点の最新版は Version 3.0.1 であるが、*mac-robber* ツール Version 1.0.0 と組み合わせて利用する場合、Version 2 系の最新版である Version 2.5.2 の利用を推奨する。その Version 2.5.2 は、最新版同様ダウンロードページにて配布されている。

これらのツールは BSD、Solaris、Linux などの Unix 系 OS 環境で動作する。紹介した Web ページに記載されているインストール手順に従えば容易にインストールできる。

5. MACtime の調査ツールの利用

5.1 MACtime の調査ツール利用手順の概要

MACtime の調査ツールを利用した調査手順は、図 5 のように進められる。調査手順そのものは 5 つのステップで構成されている。図中にある緑色の文字による記述は、各ステップの作業で得られる中間成果物を示している。

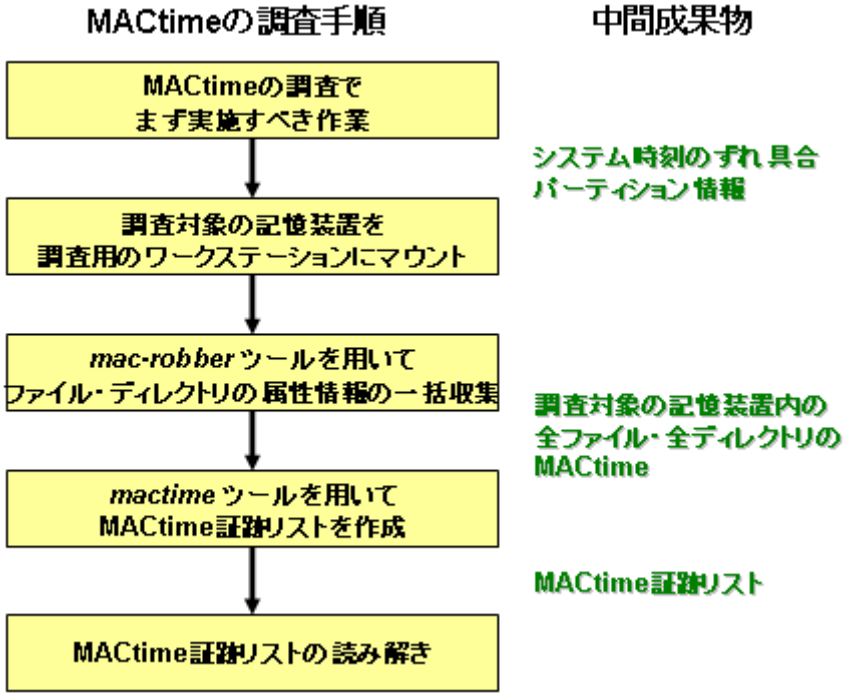

図 5. MACtime の調査ツールを用いた MACtime の調査手順

図 5 に示す調査手順は、一般的なＰＣやワークステーションの記憶装置で行われたファイル操作の調

査を想定して記述している。サーバなどで利用される RAID 構成の記憶装置におけるファイル操作の調査は、記憶装置のマウントの際に特殊な対応が必要であり、それを 5.3 章内の「解説」にまとめた。最後に示すステップ「MACtime 証跡リストの読み解き」は、章を改め、6 章で想定シナリオと共に記述する。

また、本格的な調査に先だって、MACtime の調査ツールの動作確認や試用をしてみたい場合には、5.3 章から 5.5 章を参照すれば、テスト用 Unix 系ワークステーションなどで MACtime の調査ツールを利用できるだろう。

5.2 MACtime の調査でまず実施すべき作業

MACtime の調査を行う前に実施すべき作業が 4 つある。そのうち 2 つは調査対象のコンピュータを停止する前に当該システム上で実施し、2 つは記憶装置を取り外した後で実施する。これらを図 6 に示す。

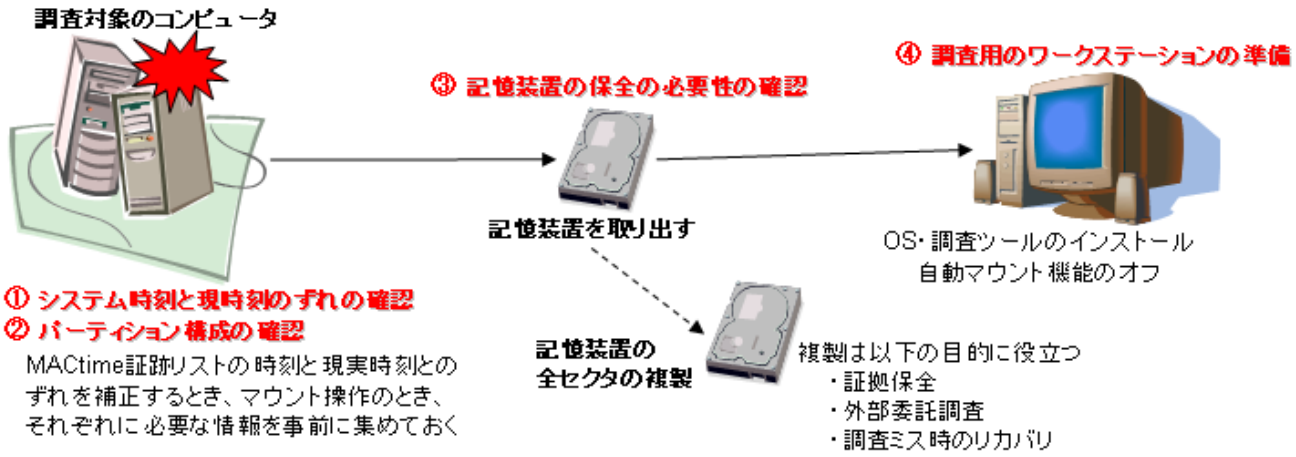

図 6. MACtime の収集を行う前に実施すべき 4 つのポイント

最初は、調査対象のコンピュータのシステム時刻と実時刻のずれの確認である（図 6 の①）。MACtime を収集した結果から構成される MACtime 証跡リストに上のタイムスタンプを実際の時刻に補正するために、起動状態にある調査対象のコンピュータにおけるシステム時刻を確認し、標準時など調査の基準になる時刻との差を調べておく。また、標準時との差異を把握することで、他のシステムのログやネットワークの通信記録と精密な照合も可能になる。なお、動作中のコンピュータにおける確認作業では、ファイル操作の痕跡を示す MACtime の上書きをしないよう、不必要な操作を極力避けるよう注意する。

次に、調査対象となる記憶装置を調査用のワークステーションにマウントする際の備えとして、調査対象のコンピュータが起動中に、その記憶装置のパーティション構成と各パーティションのフォーマット形式を調べておく（図 6 の②）。これにより、5.3 章で紹介するマウント操作時において、意図したパーティションを正しくマウントできる。システム停止後の記憶装置から同じ情報を得ることも可能だが、システム起動時に実施する方が容易であろう。ここでも MACtime の上書きをしないよう、不必要な操作

を極力避けるよう注意する。なお、これらマウントに必要な情報の取得には、Windows ではディスクマネージャ、Linux では *fdisk* コマンドを使うなど、OS により取得方法が異なるので、その作業手順の詳細は割愛する。

調査対象の記憶装置を取り外した後で実施しておくべきことは、情報保全確認である（図 6 の③）。組織内のインシデント対応ポリシや対応手順に、証拠保全や、他者による追加調査などの目的で、記憶装置内のデータの複製が定められている場合は、そのとおり実施しておく。特別な定めがない場合でも、調査対象となる記憶装置内のデータを複製して保存しておくことは、証拠の保存、操作ミスによる MACtime の上書き対策、他者による追加調査・検証などに有用である。さらに、複製の取得日時と作業者の記録、何の複製であるかを特定する情報の記録を行っておくとよい。また、記憶装置内のデータが複製後に変更されていないことを証明するために、その記憶装置全体のハッシュ値を取得する場合もある。

この記憶装置内のデータの複製は、*dd* コマンドを用いる方法、複製ソフトウェアを用いる方法、専用ハードウェアを用いて複製する方法などがある。複製の際には、全セクタを複製するように気をつけたい。これは、何らかのファイル操作の痕跡が残っている可能性がある未使用セクタの情報を含めて複製するためである。実際の操作方法については、利用するソフトウェアについての資料や操作マニュアルなどを参照されたい。

最後に、調査用のワークステーションの準備について記述する（図 6 の④）。MACtime 証跡リストを頻繁に作成する場合には、予め調査用のワークステーションを用意しておくとよい。調査用のワークステーションには、MACtime の調査ツールが利用可能な Unix 系 OS がインストールされたものを用意する。OS の設定で特に気をつけたいのは、*autofs* などで実現される自動マウント機能のオフである。これは、自動マウント機能によって MACtime が上書きされることを確実に回避するために必要な作業で、調査対象の記憶装置をマウントする前に必ず確認するよう心がける。

5.3 調査対象の記憶装置を調査用のワークステーションにマウント

調査対象の記憶装置を取り出したら、調査用のワークステーションに接続し、マウントする。

マウント操作の際には、この後に収集する MACtime の上書きを避けるために、*mount* コマンドにリードオンリー指定のオプション(-o ro)と、atime の更新を禁止するオプション(-o noatime)を明示的に指定することが重要である。これらのオプションを指定したコマンドラインの入力例を次に示す。赤文字の部分が、MACtime の上書きを避けるための指定を含む *mount* コマンド利用時の推奨オプションである。noexec はバイナリ実行禁止の指定、nodev はスペシャルデバイス使用禁止の指定、umask=000 は umask を 000 に設定する指定である。

```
mount -o ro,noexec,nodev,noatime,umask=000 /dev/hda1 /media/hda1
```

mount コマンド実行後に、マウントできていることを確認する。この後に、ファイルやディレクトリの属性情報を一括収集するが、情報の収集漏れが無いように、マウント確認の際には、特に日本語などマルチバイト文字コードを含むファイルやディレクトリが調査用ワークステーション上で参照できること

を確認する。

NTFS をマウントした際、日本語などマルチバイト文字コードを含むファイルやディレクトリの確認が行えない場合は、標準の *mount* コマンドと共に、*ntfs-3g* を用いることで問題を解決できる場合がある。*ntfs-3g* は FUSE(Filesystem in Userspace)用のプラグインであるため、FUSE と組み合わせて利用する。FUSE 自体は、Linux、FreeBSD、NetBSD、OpenSolaris、Mac OS X で利用できる。これらを事前にインストールした後、マウント操作時において、*mount* コマンドのオプションに「-t ntfs-3g」を追加する。次に、そのコマンドライン入力例を示す。前の入力例で指定したオプションも同様に指定する。

```
mount -t ntfs-3g -o ro,noexec,nodev,noatime,umask=000 /dev/hda1 /media/hda1
```

なお、*ntfs-3g* の詳細については、次の Web ページを参照されたい。この補助ツールも、*mac-robber* ツールや *mactime* ツール同様、GPL ライセンスに基づいて配布されており、無料で利用できる。

- NTFS-3G Stable Read/Write NTFS Driver
  http://www.ntfs-3g.org/

●解説

～RAID 構成の記憶装置における MACtime の調査での注意点～

RAID は、一般的に、ハードウェアで実現されるハードウェア RAID と、ソフトウェアで実現されるソフトウェア RAID に分類できる。共に、複数の記憶装置を RAID 構成にして利用するので、単体の記憶装置だけを取り出してマウントしてもファイルシステムを確認できない。そこで、RAID 構成の記憶装置内のファイルの調査においては、調査用のワークステーションを用いる代わりに、調査対象のシステムを CD-ROM や DVD などから起動できる Linux を利用する。

調査手順の相違点は、先に記載した CD-ROM や DVD などから起動できる Linux を利用する点と、マウント時に追加操作が必要になる点である。この追加操作とは、CD-ROM や DVD から起動した Linux OS に RAID 構成の記憶装置を認識させるために、RAID 構成を実現するための専用ドライバのインストールを行うことである。その他は、この技術メモで紹介している調査方法で実施できる。

5.4 *mac-robber* ツールを用いてファイル・ディレクトリの属性情報を一括収集

調査対象の記憶装置のマウントが完了したら、*mac-robber* ツールを使って、その調査対象となる記憶装置内に存在する全ファイル・全ディレクトリの属性情報を一括収集する。次に、*mac-robber* ツールの実行例を示す。

```
mac-robber /media/hda1 > hda1macrobber.txt
```

次に、その出力結果例を示す。これは、FreeBSD がインストールされたハードディスクで取得された *mac-robber* ツールの出力結果のうち、/etc/rc.d 以下の出力を一部抜粋したものである。

```
class|host|start_time
body|Helix|1250110806
md5|file|st_dev|st_ino|st_mode|st_ls|st_nlink|st_uid|st_gid|st_rdev|st_size|st_atime|st_mtime|st_ctime|st_blksize|st_blocks
0|/media/hda1/etc/rc.d/DAEMON|769|1719397|33133|-r-xr-xr-x|1|0|0|0|292|1250055298|1196110146|1196864288|4096|4
0|/media/hda1/etc/rc.d/FILESYSTEMS|769|1719398|33133|-r-xr-xr-x|1|0|0|0|405|1250055298|1196110146|1196864288|4096|4
0|/media/hda1/etc/rc.d/LOGIN|769|1719399|33133|-r-xr-xr-x|1|0|0|0|454|1250055298|1196110146|1196864288|4096|4
0|/media/hda1/etc/rc.d/NETWORKING|769|1719400|33133|-r-xr-xr-x|1|0|0|0|400|1250055298|1196110146|1196864288|4096|4
0|/media/hda1/etc/rc.d/SERVERS|769|1719401|33133|-r-xr-xr-x|1|0|0|0|304|1250055298|1196110146|1196864288|4096|4
0|/media/hda1/etc/rc.d/abi|769|1719402|33133|-r-xr-xr-x|1|0|0|0|750|1250055298|1196110146|1196864288|4096|4
0|/media/hda1/etc/rc.d/accounting|769|1719403|33133|-r-xr-xr-x|1|0|0|0|1011|1250055298|1196110146|1196864288|4096|4
0|/media/hda1/etc/rc.d/addswap|769|1719404|33133|-r-xr-xr-x|1|0|0|0|540|1250055298|1196110146|1196864288|4096|4
0|/media/hda1/etc/rc.d/adjkerntz|769|1719405|33133|-r-xr-xr-x|1|0|0|0|289|1250055298|1196110146|1196864288|4096|4
0|/media/hda1/etc/rc.d/amd|769|1719406|33133|-r-xr-xr-x|1|0|0|0|997|1250055298|1196110146|1196864288|4096|4
0|/media/hda1/etc/rc.d/apm|769|1719407|33133|-r-xr-xr-x|1|0|0|0|614|1250055298|1196110146|1196864288|4096|4
0|/media/hda1/etc/rc.d/apmd|769|1719408|33133|-r-xr-xr-x|1|0|0|0|824|1250055298|1196110146|1196864288|4096|4
0|/media/hda1/etc/rc.d/archdep|769|1719409|33133|-r-xr-xr-x|1|0|0|0|1116|1250055298|1196110146|1196864288|4096|4
0|/media/hda1/etc/rc.d/atm1|769|1719410|33133|-r-xr-xr-x|1|0|0|0|4188|1250055298|1196110146|1196864288|4096|12
0|/media/hda1/etc/rc.d/atm2|769|1719411|33133|-r-xr-xr-x|1|0|0|0|2628|1250055298|1196110146|1196864288|4096|8
0|/media/hda1/etc/rc.d/atm3|769|1719412|33133|-r-xr-xr-x|1|0|0|0|2406|1250055298|1196110146|1196864288|4096|8
0|/media/hda1/etc/rc.d/auditd|769|1719413|33133|-r-xr-xr-x|1|0|0|0|578|1250055298|1196110146|1196864288|4096|4
0|/media/hda1/etc/rc.d/auto_linklocal|769|1719414|33133|-r-xr-xr-x|1|0|0|0|581|1250055298|1196110146|1196864288|4096|4
0|/media/hda1/etc/rc.d/bgfsck|769|1719415|33133|-r-xr-xr-x|1|0|0|0|617|1250055298|1196110146|1196864288|4096|4
0|/media/hda1/etc/rc.d/bluetooth|769|1719416|33133|-r-xr-xr-x|1|0|0|0|9510|1250055298|1196110146|1196864288|4096|20
0|/media/hda1/etc/rc.d/bootparams|769|1719417|33133|-r-xr-xr-x|1|0|0|0|388|1250055298|1196110146|1196864288|4096|4
0|/media/hda1/etc/rc.d/bridge|769|1719418|33133|-r-xr-xr-x|1|0|0|0|2302|1250055298|1196110146|1196864288|4096|8
0|/media/hda1/etc/rc.d/bsnmpd|769|1719419|33133|-r-xr-xr-x|1|0|0|0|301|1250055298|1196110146|1196864288|4096|4
0|/media/hda1/etc/rc.d/bthidd|769|1719420|33133|-r-xr-xr-x|1|0|0|0|646|1250055298|1196110146|1196864288|4096|4
0|/media/hda1/etc/rc.d/ccd|769|1719421|33133|-r-xr-xr-x|1|0|0|0|374|1250055298|1196110146|1196864288|4096|4
0|/media/hda1/etc/rc.d/cleanvar|769|1719422|33133|-r-xr-xr-x|1|0|0|0|1332|1250055298|1196110146|1196864288|4096|4
0|/media/hda1/etc/rc.d/cleartmp|769|1719423|33133|-r-xr-xr-x|1|0|0|0|1707|1250055298|1196110146|1196864288|4096|4
0|/media/hda1/etc/rc.d/cron|769|1719424|33133|-r-xr-xr-x|1|0|0|0|432|1250055298|1196110146|1196864288|4096|4
0|/media/hda1/etc/rc.d/devd|769|1719425|33133|-r-xr-xr-x|1|0|0|0|444|1250055298|1196110146|1196864288|4096|4
0|/media/hda1/etc/rc.d/devfs|769|1719426|33133|-r-xr-xr-x|1|0|0|0|1408|1250055298|1196110146|1196864288|4096|4
0|/media/hda1/etc/rc.d/dhclient|769|1719427|33133|-r-xr-xr-x|1|0|0|0|1151|1250055298|1196110146|1196864288|4096|4
0|/media/hda1/etc/rc.d/dmesg|769|1719428|33133|-r-xr-xr-x|1|0|0|0|487|1250055298|1196110146|1196864288|4096|4
0|/media/hda1/etc/rc.d/dumpon|769|1719429|33133|-r-xr-xr-x|1|0|0|0|1123|1250055298|1196110146|1196864288|4096|4
0|/media/hda1/etc/rc.d/early.sh|769|1719430|33133|-r-xr-xr-x|1|0|0|0|242|1250055298|1196110146|1196864288|4096|4
0|/media/hda1/etc/rc.d/encswap|769|1719431|33133|-r-xr-xr-x|1|0|0|0|1155|1250055298|1196110146|1196864288|4096|4
0|/media/hda1/etc/rc.d/fsck|769|1719432|33133|-r-xr-xr-x|1|0|0|0|1271|1250055298|1196110146|1196864288|4096|4
（以下省略）
```

出力結果の 1、2 行目に調査用のワークステーションの host 名と *mac-robber* ツールを実行した時の時刻（UNIX タイムスタンプ形式）が記録され、3 行目は 4 行目以降に記載されるデータの項目名を示している。3 行目の項目名の説明と、出力結果の表記例を次に示す。

・出力結果の形式（3 行目以降のデータ）[1]

項目番号	項目名	説明	出力結果の表記例 ～4 行目～
1	md5	MD5 ハッシュ値	0
2	file	絶対パスでのファイル名	/media/hda1/etc/rc.d/DAEMON
3	st_dev	デバイス	769
4	st_ino	i ノード番号	1719397
5	st_mode	ファイルモード	33133

6	st_ls	パーミッション	-r-xr-xr-x
7	st_nlink	ハードリンクの数	1
8	st_uid	オーナーの UID	0
9	st_gid	オーナーの GID	0
10	st_rdev	デバイスタイプ	0
11	st_size	ファイルサイズ	292
12	st_atime	atime	1250055298
13	st_mtime	mtime	1196110146
14	st_ctime	ctime	1196864288
15	st_blksize	ブロックサイズ	4096
16	st_blocks	使用ブロック数	4

黄色で着色した項目番号 12、13、14 には、MACtime がそれぞれ UNIX タイムスタンプ形式で記載されていることが確認できる。なお、UNIX タイムスタンプからの時刻形式の変換は、次の章で紹介する *mactime* ツールを利用して実施する。

5.5 *mactime* ツールを用いて MACtime 証跡リストを作成

mac-robber ツールを用いて調査対象となる記憶装置内の全ファイル・全ディレクトリの属性情報を収集できたら、*mactime* ツールを用いて MACtime 証跡リストを作成する。次に、*mactime* ツールの実行例を示す。

```
mactime -b hda1macrobber.txt -d
```

次に、その出力結果例を示す。この例は、*shutdown* コマンド実行直後の時刻に注目し、その部分を抜粋したものである。

```
Date,Size,Type,Mode,UID,GID,Meta,File Name
Tue Aug 11 2009 23:34:56,10536,.a.,-r-xr-sr-x,0,4,522154,/media/hda1/usr/bin/wall
Tue Aug 11 2009 23:34:58,33451,.a.,-r--r--r--,0,0,1719298,/media/hda1/etc/defaults/rc.conf
Tue Aug 11 2009 23:34:58,2560,.a.,drwxr-xr-x,0,0,1719316,/media/hda1/etc/rc.d
Tue Aug 11 2009 23:34:58,3308,.a.,-rw-r--r--,0,0,1719358,/media/hda1/etc/rc.shutdown
Tue Aug 11 2009 23:34:58,36613,.a.,-rw-r--r--,0,0,1719359,/media/hda1/etc/rc.subr
Tue Aug 11 2009 23:34:58,16384,.a.,-rw-r--r--,0,0,1719372,/media/hda1/etc/login.conf.db
Tue Aug 11 2009 23:34:58,939,.a.,-rw-r--r--,0,0,1719381,/media/hda1/etc/rc.conf
Tue Aug 11 2009 23:34:58,292,.a.,-r-xr-xr-x,0,0,1719397,/media/hda1/etc/rc.d/DAEMON
Tue Aug 11 2009 23:34:58,405,.a.,-r-xr-xr-x,0,0,1719398,/media/hda1/etc/rc.d/FILESYSTEMS
Tue Aug 11 2009 23:34:58,454,.a.,-r-xr-xr-x,0,0,1719399,/media/hda1/etc/rc.d/LOGIN
Tue Aug 11 2009 23:34:58,400,.a.,-r-xr-xr-x,0,0,1719400,/media/hda1/etc/rc.d/NETWORKING
Tue Aug 11 2009 23:34:58,304,.a.,-r-xr-xr-x,0,0,1719401,/media/hda1/etc/rc.d/SERVERS
Tue Aug 11 2009 23:34:58,750,.a.,-r-xr-xr-x,0,0,1719402,/media/hda1/etc/rc.d/abi
Tue Aug 11 2009 23:34:58,1011,.a.,-r-xr-xr-x,0,0,1719403,/media/hda1/etc/rc.d/accounting
Tue Aug 11 2009 23:34:58,540,.a.,-r-xr-xr-x,0,0,1719404,/media/hda1/etc/rc.d/addswap
```

```
Tue Aug 11 2009 23:34:58,289,.a.,-r-xr-xr-x,0,0,1719405,/media/hda1/etc/rc.d/adjkerntz
Tue Aug 11 2009 23:34:58,997,.a.,-r-xr-xr-x,0,0,1719406,/media/hda1/etc/rc.d/amd
Tue Aug 11 2009 23:34:58,614,.a.,-r-xr-xr-x,0,0,1719407,/media/hda1/etc/rc.d/apm
Tue Aug 11 2009 23:34:58,824,.a.,-r-xr-xr-x,0,0,1719408,/media/hda1/etc/rc.d/apmd
Tue Aug 11 2009 23:34:58,1116,.a.,-r-xr-xr-x,0,0,1719409,/media/hda1/etc/rc.d/archdep
Tue Aug 11 2009 23:34:58,4188,.a.,-r-xr-xr-x,0,0,1719410,/media/hda1/etc/rc.d/atm1
Tue Aug 11 2009 23:34:58,2628,.a.,-r-xr-xr-x,0,0,1719411,/media/hda1/etc/rc.d/atm2
Tue Aug 11 2009 23:34:58,2406,.a.,-r-xr-xr-x,0,0,1719412,/media/hda1/etc/rc.d/atm3
Tue Aug 11 2009 23:34:58,578,.a.,-r-xr-xr-x,0,0,1719413,/media/hda1/etc/rc.d/auditd
Tue Aug 11 2009 23:34:58,581,.a.,-r-xr-xr-x,0,0,1719414,/media/hda1/etc/rc.d/auto_linklocal
Tue Aug 11 2009 23:34:58,617,.a.,-r-xr-xr-x,0,0,1719415,/media/hda1/etc/rc.d/bgfsck
Tue Aug 11 2009 23:34:58,9510,.a.,-r-xr-xr-x,0,0,1719416,/media/hda1/etc/rc.d/bluetooth
Tue Aug 11 2009 23:34:58,388,.a.,-r-xr-xr-x,0,0,1719417,/media/hda1/etc/rc.d/bootparams
Tue Aug 11 2009 23:34:58,2302,.a.,-r-xr-xr-x,0,0,1719418,/media/hda1/etc/rc.d/bridge
Tue Aug 11 2009 23:34:58,301,.a.,-r-xr-xr-x,0,0,1719419,/media/hda1/etc/rc.d/bsnmpd
Tue Aug 11 2009 23:34:58,646,.a.,-r-xr-xr-x,0,0,1719420,/media/hda1/etc/rc.d/bthidd
Tue Aug 11 2009 23:34:58,374,.a.,-r-xr-xr-x,0,0,1719421,/media/hda1/etc/rc.d/ccd
Tue Aug 11 2009 23:34:58,1332,.a.,-r-xr-xr-x,0,0,1719422,/media/hda1/etc/rc.d/cleanvar
Tue Aug 11 2009 23:34:58,1707,.a.,-r-xr-xr-x,0,0,1719423,/media/hda1/etc/rc.d/cleartmp
Tue Aug 11 2009 23:34:58,432,.a.,-r-xr-xr-x,0,0,1719424,/media/hda1/etc/rc.d/cron
Tue Aug 11 2009 23:34:58,444,.a.,-r-xr-xr-x,0,0,1719425,/media/hda1/etc/rc.d/devd
Tue Aug 11 2009 23:34:58,1408,.a.,-r-xr-xr-x,0,0,1719426,/media/hda1/etc/rc.d/devfs
Tue Aug 11 2009 23:34:58,1151,.a.,-r-xr-xr-x,0,0,1719427,/media/hda1/etc/rc.d/dhclient
Tue Aug 11 2009 23:34:58,487,.a.,-r-xr-xr-x,0,0,1719428,/media/hda1/etc/rc.d/dmesg
Tue Aug 11 2009 23:34:58,1123,.a.,-r-xr-xr-x,0,0,1719429,/media/hda1/etc/rc.d/dumpon
Tue Aug 11 2009 23:34:58,242,.a.,-r-xr-xr-x,0,0,1719430,/media/hda1/etc/rc.d/early.sh
Tue Aug 11 2009 23:34:58,1155,.a.,-r-xr-xr-x,0,0,1719431,/media/hda1/etc/rc.d/encswap
Tue Aug 11 2009 23:34:58,1271,.a.,-r-xr-xr-x,0,0,1719432,/media/hda1/etc/rc.d/fsck
Tue Aug 11 2009 23:34:58,363,.a.,-r-xr-xr-x,0,0,1719433,/media/hda1/etc/rc.d/ftpd
Tue Aug 11 2009 23:34:58,2177,.a.,-r-xr-xr-x,0,0,1719434,/media/hda1/etc/rc.d/gbde
Tue Aug 11 2009 23:34:58,2814,.a.,-r-xr-xr-x,0,0,1719435,/media/hda1/etc/rc.d/geli
Tue Aug 11 2009 23:34:58,1955,.a.,-r-xr-xr-x,0,0,1719436,/media/hda1/etc/rc.d/geli2
（以下省略）
```

mactime ツールの出力結果は、MACtime 証跡を時系列順に並べ替えた MACtime 証跡リストとなっている。次に、項目名の詳細と、出力結果の表記例を示す。

出力結果の形式

項目番号	項目名	説明	出力結果の表記例 ～2 行目～
1	Date	日時	Tue Aug 11 2009 23:34:56
2	Size	ファイルサイズ	10536
3	Type	MACtime 変更フラグ (m:mtime, c:ctime, a:atime)	.a.
4	Mode	ファイルモード	-r-xr-sr-x
5	UID	オーナーの UID	0
6	GID	オーナーの GID	4
7	Meta	属性情報の i ノード番号	522154
8	File Name	ファイル名	/media/hda1/usr/bin/wall

mactime ツールの出力結果である MACtime 証跡リストを読み解く際には、黄色で着色した MACtime 証跡を表す情報の項目番号 1 と 3 と 8 に注目すればよい。項目番号 1 では日時を、項目番号 3 では簡略表記された MACtime 変更フラグを、項目番号 8 ではフルパス表記のファイル名を、それぞれ表している。それ以外の項目は、*mac-robber* ツールを実行した際に取得した属性情報を表すので、ctime の変更を表す MACtime 変更フラグがある場合にのみ読み取るよう注意する。

また、*mactime* ツールのオプションに、日付と共に –y を指定すれば、その日以降の MACtime 証跡を抽

出した MACtime 証跡リストを作成できる。

```
mactime -b hda1macrobber.txt -d -y mm/dd/yyyy          ※指定日付以降のリストを作成
```

これは、予め調査したい日時が特定できている場合に特に有効で、対象日時を含んだ日付指定をすることで、その日以降のイベントだけを抽出した MACtime 証跡リストを作成できる。

6. MACtime 証跡リストの読み解き

本章では、2 つの例を通じて、MACtime 証跡リストを読み解く。

6.1 FreeBSD のシャットダウン時にアクセスされるファイルを調べる

図 7 は、MACtime 証跡リストを利用して、FreeBSD のシャットダウン時にアクセスされるファイルを調査した例を示している。

この例では、シャットダウンした FreeBSD マシンの記憶装置を取り外し、調査用のワークステーションにマウントした状態で、MACtime の調査ツールを用い、MACtime 証跡リストを作成した。図中に引用したものは、シャットダウンを実行した時刻以降の MACtime 証跡リストの一部抜粋で、5.5 章で示した出力例と同じものである。

MACtime 証跡リストを先頭から見て行くと、最初に、/usr/bin/wall の atime が更新されていることが読み取れる。*wall* コマンドは、ログインユーザに対してメッセージを表示することができるコマンドであり、シャットダウンする際に表示されるシャットダウンメッセージは、この *wall* コマンドで行われていることが認められる。それ以降は、rc.conf や/etc/rc.d などのファイルが次々と読み込まれていくのが読み取れる。シャットダウンプロセスで何を行うのかを OS 自体が把握するために、各種設定ファイルを確認していることが読み取れる。また、これらのアクセスは同時刻に集中していることにも注目したい。同時刻に複数のファイルにアクセスが集中している場合は、OS 自身によるファイル操作やプログラムによるファイル操作であると考えられる。なお、同時刻に複数の MACtime 証跡がみられる場合は、秒単位で記録される MACtime の時刻精度を考慮し、その記載順序にとらわれないよう注意したい。

ここで紹介した例では、同時刻に 199 個のファイルアクセスがあり、1 秒間に多数のファイルアクセスがあったことが確認できる。

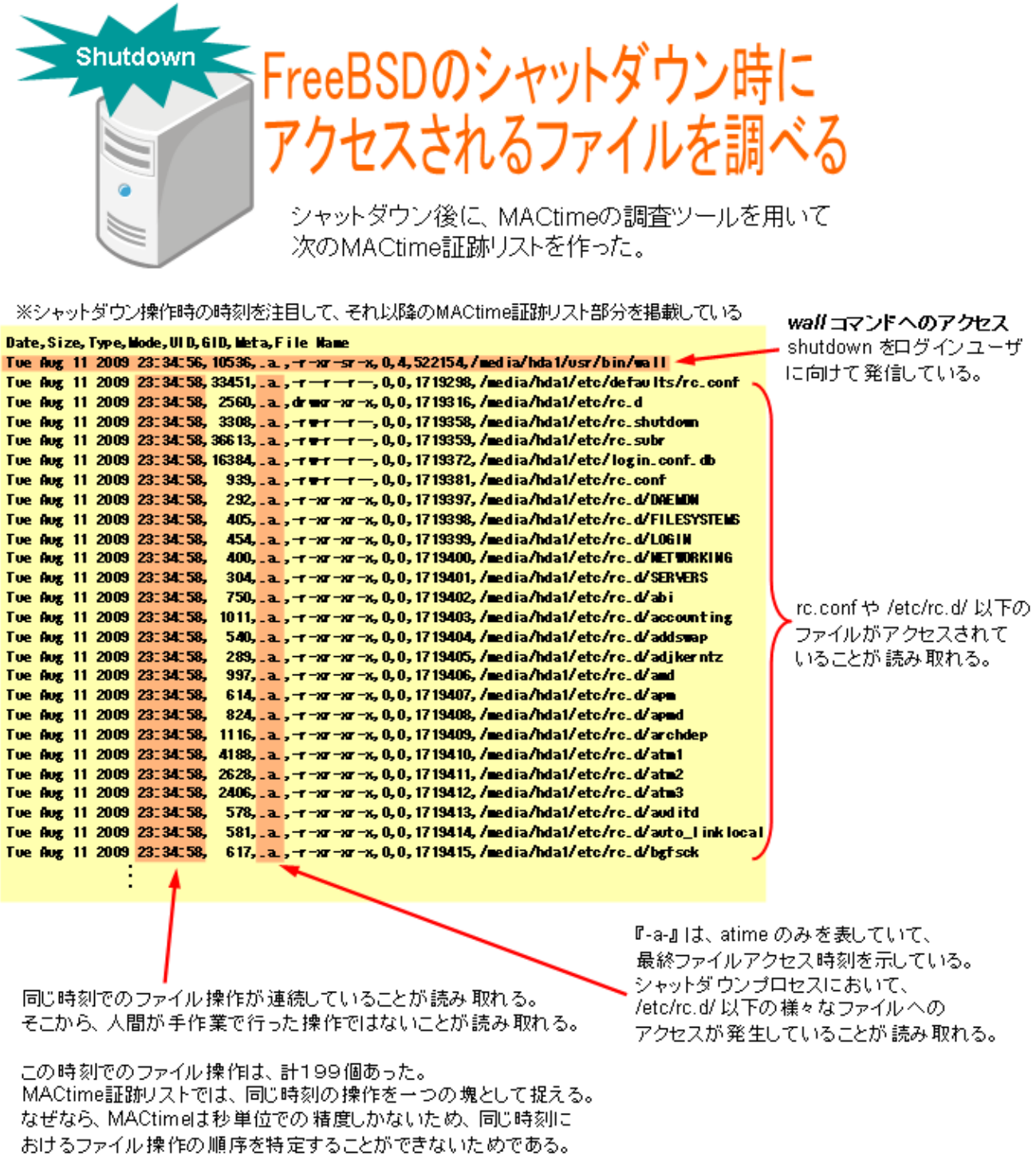

図 7. MACtime 証跡リストの読解 ～FreeBSD のシャットダウン時のファイルアクセス～

6.2 ファイル改ざんなど主だった被害がない不正侵入されたサーバのファイル操作を調べる

図 8 は、MACtime 証跡リストを利用して、ファイル改ざんなど主だった被害がない不正侵入されたサーバのファイル操作を調査した例を示している。

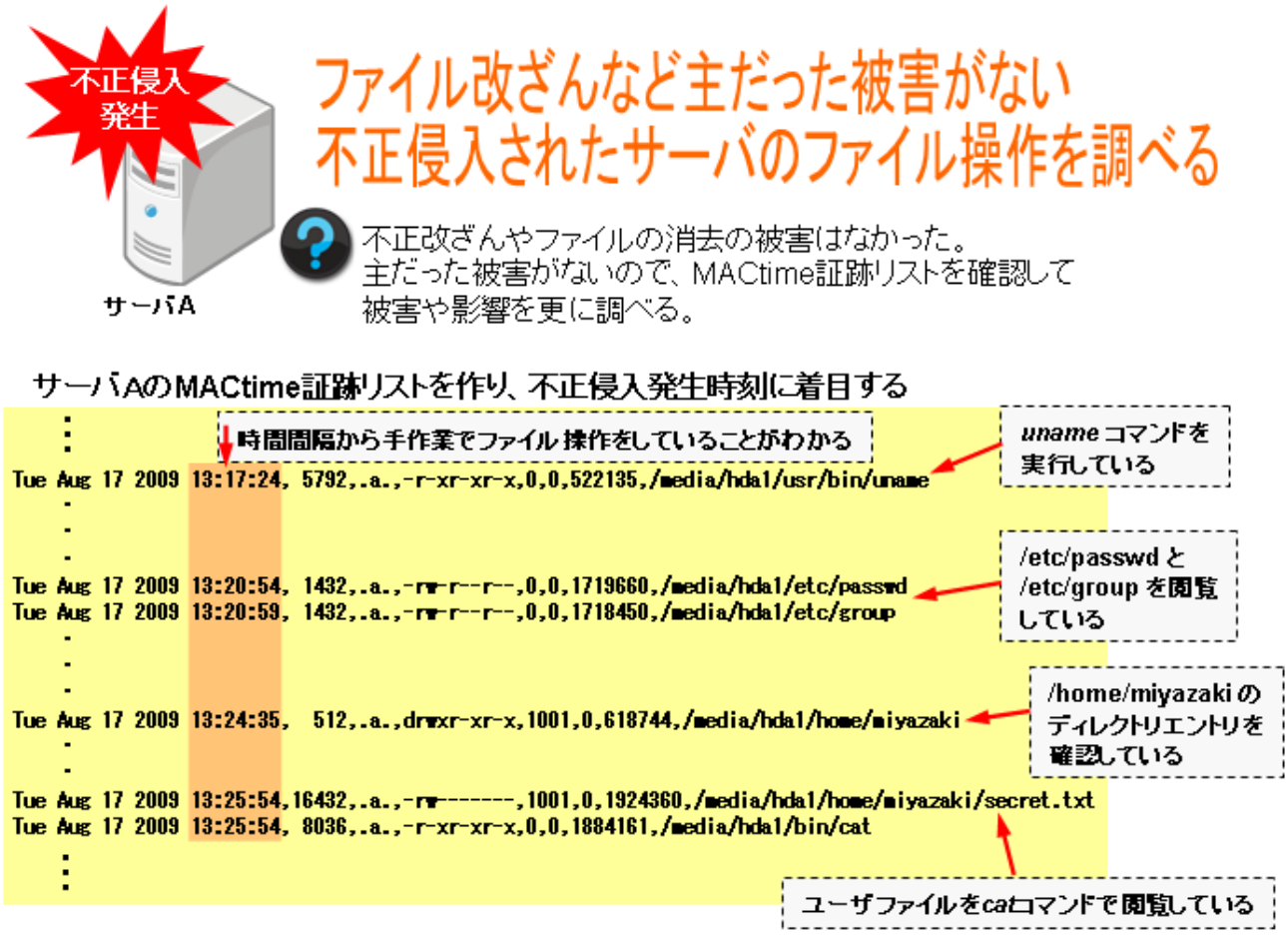

図 8. MACtime 証跡リストの読解 ～主だった被害のない不正侵入されたサーバのファイル操作を調べる～

この例では、サーバ A が不正侵入されたことがアクセスログなどからすでに判明している状況を想定している。不正侵入の目的を調べるため、MACtime 証跡リストを作成し、不正侵入時に行われたファイル操作を調べることにした。図に掲載した MACtime 証跡リストでは、説明に必要な部分のみを抜粋している。

不正侵入された時刻周辺の MACtime 証跡リストを見ると、/usr/bin/uname が実行され、その後、/etc/passwd と/etc/group を閲覧されていることが読み取れる。このことから、このサーバの OS や用途、ユーザアカウントを調べていることが推測される。また、これらのファイル操作の時間間隔が比較的あいていることから、手作業でのファイル操作であると考えられる。

その後、/home/miyazaki のディレクトリエントリの確認に続き、/home/miyazaki/secret.txt にアクセスされたことと、*cat* コマンドが最後に使われたことから、*cat* コマンドを用いて secret.txt ファイルを閲覧していることが認められる。これら一連の操作は、ユーザファイルへのアクセスを示しており、不審なファイル操作であることが疑われる。これ以降、不審なファイル操作らしき痕跡は見当たらない。

この調査の後、不審なファイル操作が行われた当該時刻にログインしていた利用者が居なかったことが確認され、さらに、secret.txt に機密情報が含まれていたことが判明した場合、不正侵入者が、ファイル改ざんなどを行わず、痕跡をなるべく残さないように注意しながら、サーバ上の機密情報を読み取ったことが推定される。

7. まとめ

この技術メモでは、ファイル操作の実施時刻を記録している MACtime の概要を述べ、MACtime 証跡リストを得るための調査ツールを紹介し、2 つの適用事例を示した。

MACtime の調査ツールに興味を持たれた読者には、手近なシステムの MACtime 証跡リストを作って読み解いてみることを推奨する。これにより、MACtime 証跡リストの読み取り訓練だけにとどまらず、システム上で行われているファイル操作の詳細を把握できる。更に、システムに何らかの事故が発生した場合、事前に取得した正常状態の MACtime 証跡リストがあれば、事故後に取得した MACtime 証跡リストと比較確認することで、正常時のファイル操作との差異を読み取り、不審なファイル操作の抽出や、事故発生原因の特定に役立てられる。

この技術メモによって、ファイル操作が MACtime によって調査できることへの理解が進み、様々なファイル操作の事後調査に MACtime の調査ツール、および、MACtime 証跡リストの活用が広がることを期待している。

付録：mtime、atime、ctime の値に影響を与えるファイル操作等の詳細

MACtime の構成要素である mtime、atime、ctime が変更される際のファイル操作等の詳細は次のとおりである。

・mtime(time of last modification：最終更新時刻)

stat や ls -l で表示される時刻で、ファイルの場合には、当該ファイルの作成、書込み、削除など、ファイルが更新されたとき、その瞬間の時刻が記録される。
ディレクトリの場合は、当該ディレクトリの情報が更新された時刻が記録される。
属性情報（ファイルアトリビュート、オーナー）の変更では変更されない。
root 権限ユーザによる mtime のみの改変は比較的容易にできる。
ufs、ext2/3、NTFS では、どのファイルシステムでも mtime はファイルやディレクトリの最終更新時刻を表す。
mtime は、しばしば ctime と同時刻になる。これは、ファイルやディレクトリの更新の多くで、i ノードもしくは MFT の変更が発生し、ファイルやディレクトリの属性情報も更新されるためである。

・atime(time of last access：最終アクセス時刻)

stat や ls -lu で表示される時刻で、ファイルの場合には、当該ファイルの読込み、実行で更新される。
ディレクトリの場合は、当該ディレクトリの参照で更新される。
ユーザの操作で変更されやすい情報である。
root 権限ユーザによる atime のみの改変は比較的容易にできる
ufs、ext2/3、NTFS では、どのファイルシステムでも atime はファイルやディレクトリの最終アクセス時刻を表す。
atime は、人間によるアクセスだけでなく、システムによるアクセスでも更新されるので、その更新理由を調べる際には十分注意する。

・ctime（time of last status change：タイムスタンプ以外の属性情報の最終変更時刻）

stat や ls -lc で表示される時刻で、ファイルの場合には、当該ファイルの属性情報が変更されると更新される。
ディレクトリの場合も同様で、当該ディレクトリの属性情報が変更されると更新される。
ファイルやディレクトリを削除した場合は、直上のディレクトリの ctime に時刻が記録される。
root 権限ユーザでも ctime のみを改変するのは難しい。
ufs と ext2/3 では、i ノードに記載されているタイムスタンプ以外の属性情報の最終更新時刻が記録される。NTFS では、MFT に記載されているタイムスタンプ以外の属性情報の最終更新時刻が記録される。
ctime の改変が難しい特徴を活用すると、カーネルルートキット（カーネルレベルルートキット）や、

MACtime 改変の発見が行える可能性がある。

なお、本技術メモでは取り上げなかったが、ファイルシステムによっては mtime、atime、ctime 以外のタイムスタンプも記録されているので、簡単に記述しておく。

まず、NTFS では Birth time、あるいは、Creation time と呼ばれるファイル作成時の時刻が記録されており、一般的に btime、あるいは、crtime として表される。Windows のエクスプローラでファイルのプロパティを確認した際に表示される「作成日時」がそれにあたる。本技術メモで紹介した *mac-robber* ツールでは収集できないタイムスタンプであるため、本技術メモ内での記載を割愛した。

また、Linux で用いられる ext3 では、dtime と呼ばれるファイル削除時刻が記録されている[2]。これも本技術メモで紹介した *mac-robber* ツールでは収集できないタイムスタンプであるため、本技術メモ内での記載を割愛した。

参考文献

[1] 渡辺 勝弘, 伊原 秀明著, 不正アクセス調査ガイド, オライリー・ジャパン, 2002 年 4 月発行
[2] Dan Farmer, Wietse Venema 著, Forensic Discovery, Addison-Wesley Professional, 2005 年 1 月発行