社団法人 情報処理学会 研究報告
IPSJ SIG Technical Report

2008－DPS－134 (46)
2008－CSEC－ 40 (46)
2008／3／7

ホットデジタルフォレンジックによるインシデント検知方法の提案

越智 貴夫* 小島 孝夫* 外川 政夫* 板倉 征男*

*情報セキュリティ大学院大学 〒221-0835 神奈川県横浜市神奈川区鶴屋町 2-14-1
E-mail: mgs064514@iisec.ac.jp, itakura@iisec.ac.jp

あらまし 情報セキュリティのインシデント発生時に解決されるべき問題は大きく 2 つにわかれる．それは，情報システムのサービスを維持する問題とインシデントの原因究明の問題である．情報システムのサービスを維持する問題に対応する技術の 1 つに IDS，インシデントの原因究明の問題に対応する技術の 1 つにデジタルフォレンジックが位置づけられる．本研究は，インシデント対応の事前対処のバックアップと事後対処のデジタルフォレンジックを組み合わせることにより，取りこぼしと性能低下の課題を解決できる「ホットデジタルフォレンジック」というコンセプトを提案し，そのための要求条件を満たすシステムを構築することを目的とする．本稿では，コンセプトと方式を提案し，事例を述べる．

キーワード インシデント，デジタルフォレンジック，IDS，イメージバックアップ

The Proposal of Incident detection Method using the Hot Digital Forensic

Takao OCHI* Takao KOJIMA* Masao TOGAWA* Yukio ITAKURA*

*INSTITUTE of INFORMATION SECURITY
2-14-1 Tsuruya, Kanagawa, Yokohama, Kanagawa, 2210835 JAPAN
E-mail: mgs064514@iisec.ac.jp, itakura@iisec.ac.jp

Abstract The problem which it should solve the time of incident of information security is recognized into two largely. One is the problem which maintains the service of the information system and the other is the problem of cause investigation of the incident. You can locate one of the technology which corresponds to the problem of the cause investigation of IDS and the incident in one of the technology which corresponds to the problem which maintains the service of the information system digital forensic. As for this research, combining digital forensic and image backup can solve drop and degradation to propose the concept of "Hot Digital Forensic", it designates that the system which satisfies the required condition for that is constructed as purpose. With this manuscript, concept and system are proposed, the case is expressed.

Keyword incident, digital forensic, IDS, image backup

1 はじめに

情報セキュリティのインシデント発生時に解決されるべき問題は大きく 2 つにわかれる．それは，情報システムのサービスを維持する問題とインシデントの原因究明の問題である．情報システムのサービスを維持する問題に対応する技術の 1 つに IDS，インシデントの原因究明の問題に対応する技術に 1 つにデジタルフォレンジックが位置づけられる．

本研究は，インシデント対応の事前対処のバックアップと事後対処のデジタルフォレンジックを組み合わせることにより，インシデント対応における課題である「取りこぼし」，「性能低下」を解決できる「ホットデジタルフォレンジック」というコンセプトを提案し，そのための要求条件を満たすシステムを構築することを目的とする．

本稿では，コンセプトと方式を提案し，事例を述べる．

2 課題とねらい

インシデント対応における課題として，次の 4 つあげることができる．

(1) 取りこぼしのため，情報収集時にインシデントの痕跡を正しく取得できない

IDS の検出方法には，シグニチャと呼ばれる特定の攻撃パターンをあらかじめ定義しておき，そのパターンとマッチするものを不正侵入として検知するシグニチャ検出方法と，通常の運用状態を定義，あるいは学習させておき，それから逸脱したものを不正侵入とし

て検知する異常検出方法がある．シグニチャ検出方法では，亜種の対応はできず，新しい攻撃手法が次々登場するため，シグニチャを絶えず更新する必要がある。一方，異常検出方法では，逸脱したという判断に，あいまいさが含まれるため，検知精度が低いという問題がある．そのため，インシデントを取りこぼしてしまい，適切な情報を収集できず，インシデントの痕跡を正しく取得できない可能性がある．[1][2][3]

(2)データ収集や証拠保全が性能低下・システム停止というシステムの運用へ悪影響を与える

IDS の動作には，予想以上に CPU パワーやメモリなどのコンピュータリソースを必要とする．検知対象とするインシデントの種類を多くすると収集するデータが多くなったり，IDS 自身からのログが大量に出力され，運用しているシステムの性能低下・システム停止といった悪影響を与える可能性がある．そのため，システムの可用性が低下しない範囲で監視を行う必要がある．[3]

(3)インシデントの検知遅れにより証拠自体が改ざん（削除や隠蔽）される

インシデントが発生してから，インシデントを速やかに検知しないと，検知するまでの間にインシデントの痕跡が削除され原因追求ができなくなる．そのために，なるべくインシデントの検知を速やかに行えるようにする必要がある．[4]

(4)インシデントの調査活動が証拠破壊につながる

インシデント発生した場合，事前にルールを理解し十分な訓練を受けていないと、ルールに基づかない場当たり的な調査やセキュリティ対策を実施することにより，インシデントの痕跡部分を上書きしたり，削除してしまい証拠破壊をしてしまう可能性がある．[5][6]

本研究の狙いは，これらの課題の中で、「取りこぼし」と「性能低下」に対する課題解決にある．

3　提案方式

本稿で提案するホットデジタルフォレンジックの方式を以下に示す．

3.1　ホットデジタルフォレンジックとは

ホットデジタルフォレンジックは，システムを稼働したホットな状態で取得したイメージバックアップファイルに対して、システム運用と並行してデジタルフォレンジックの調査・分析の技術を応用してインシデント検知を行う方法である．

3.2　監視対象

ホットデジタルフォレンジックが対象とする監視対象を図 1 に示す．

情報システムにおけるインシデントは，コンピュータに関するものとネットワークに関するものに区分でき，デジタルフォレンジックは，それぞれコンピュータフォレンジックとネットワークフォレンジックが対応する．[7][8][9]また，従来の IDS は，監視対象がコンピュータで，受信したパケット，出力するイベントやログ，ファイルの変更及びシステムコールとするホスト型IDSとネットワーク上を流れるパケットを対象とするネットワーク型 IDS がそれぞれ対応する．[1]

一方，本研究で提案するホットデジタルフォレンジックの監視対象は，コンピュータが出力するイベントやログとファイルの変更を対象とし，ネットワーク上を流れるパケットやコンピュータのシステムコールは対象としない．

フォレンジックの種類	項番	監視する機能	従来のIDS		ホットデジタルフォレンジック
			ネットワーク型IDS	ホスト型IDS	
ネットワークフォレンジック	1	ネットワーク上を流れるパケット	○	×	×
コンピュータフォレンジック	2	監視対象ホストが受信したパケット	×	○	×
	3	監視対象ホストが出力するイベントやログ	×	○	○
	4	監視対象ホストのファイルの変更	×	○	○
	5	監視対象ホストのシステムコール	×	○	×

凡例：○：適　×：不可

図 1 監視対象の比較表

3.3　ホットイメージバックアップ技術

ホットデジタルフォレンジックでは，ホットイメージバックアップ技術を使う．本技術は，ホットバックアップとイメージバックアップを組み合わせたバックアップ方式で，稼働中のコンピュータを停止することなく，そのコンピュータの OS やアプリケーションそしてデータなど，コンピュータ全体のディスクイメージ＝イメージバックアップファイル（以下，「IBF」という）をバックアップする技術である．

ホットバックアップは，OS を使いながら，コンピュータを再起動せずにディスクをバックアップする方法で，スナップショットを使用する．スナップショットは，バックアップ対象としているディスクやパーティションのファイルシステムのある瞬間を元データよりも格段に少ない容量でかつ短時間で保存することができ，変更があったデータを追跡できるという特徴を有する．

イメージバックアップは，ディスクのパーティションの内容をハードディスクのデータの読み書きを行う最小単位であるセクタの連続としてとらえて全てを一つのファイル＝イメージファイルとして保存する方法である．ドライブやパーティションを一つのディスクイメージとして保存するため，ディレクトリ（フォルダ）構造も含めてアプリケーションや OS そのものもそのままの形でイメージファイルとしてバックアップできるという特徴を有する．[10]

3.4　ホットデジタルフォレンジックの特徴

ホットデジタルフォレンジックには，次の２つの特徴がある．

(1)監視を分散処理できる

ホットデジタルフォレンジックは，システム運用と並行しつつ，インシデントの検知を監視対象のコンピュータではなく，調査を行うために用意した別のコンピュータ上で行う．そのため，従来の IDS と異なり，

システム運用への影響を最小限に抑えながらインシデント監視を行える．

(2) トレースバック式調査ができる

ホットデジタルフォレンジックでは，IBF は定時に取得され，時系列に管理され，任意の時点に遡って参照することができる．すなわち，任意の時点の IBF を用いてインシデントの検知を行うことができるため，従来の IDS では取りこぼししてしまうようなインシデントも，後からその痕跡を調査することにより検知が可能となる．

3.5 システム全体構成と検知手順

システムの全体構成を図 2 に示す．

ホットデジタルフォレンジックは，ホットイメージバックアップ作成機能（以下「HIBF 作成機能」という），イメージバックアップ管理機能（以下，「HIBF 管理機能」という），抽出機能，比較差分抽出機能，判定機能から構成される．HIBF 作成機能以外の機能は，監視対象となるコンピュータとは別に用意した調査用のホットデジタルフォレンジックコンピュータ（以下，「HDF コンピュータ」という）に実装される．

1) HIBF 作成機能：
定められた定時間起動で IBF を取得

2) HIBF 管理機能：
①IBF 保管庫を構成し IBF を時系列管理
②IBF 保管庫から任意の時間の IBF を取り出して HDF コンピュータのドライブにマウント

3) 抽出機能：
マウントされた IBF からファイル名やファイルサイズ等のファイル属性情報，ファイル内容からイベントログの内容やレジストリキー等を抽出し，出力ファイルとして取り出す

4) 比較差分抽出機能：
抽出された 2 つのファイルを比較して 2 ファイル間の差異を抽出．

5) 判定機能：
比較差分抽出機能の抽出結果と予め用意した HDF 判定 DB と比較し該当すると通知

インシデントの検知手順を図 3 に示す．

Step1:構造化　HIBF 管理機能で IBF 保管庫から 2 世代の IBF1,IBF2 を取り出し，ドライブにマウントする．

Step2:DF 解析　抽出機能を用いて IBF1,IBF2 から比較する特定の部分 F1,F2 を取り出す．比較差分機能を用いて，F1，F2 の差異 FD12 を抽出する．

Step3:判定　判定機能を用いて，FD12 と HDF 判定 DB と比較して該当すると通知する．

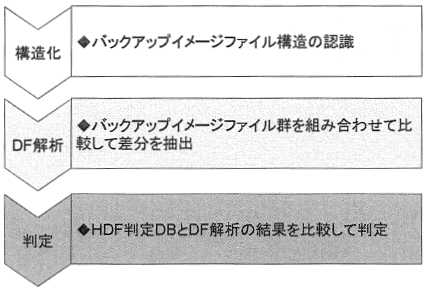

図 3 インシデントの検知手順

4 適用例

ホットデジタルフォレンジックの方式の適用例を 3 つ挙げる．【適用例 1】ではプロトタイプ実装を行い，

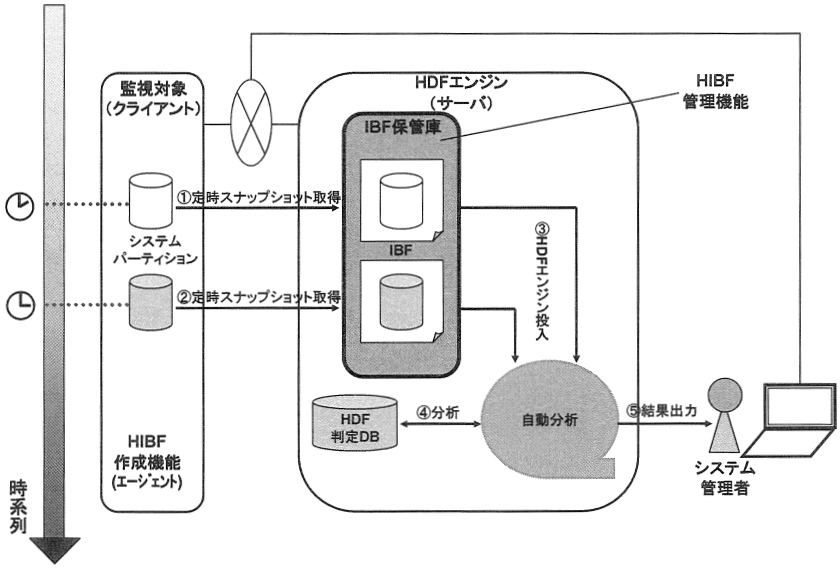

図 2 システムの全体構成図

従来のIDSと同様に監視ができることを示す．【適用例2】と【適用例3】では机上検討を行い，従来のIDSに対し優位となる点を評価する．

4.1【適用例1】ログやファイルの監視

3.項で提案したホットデジタルフォレンジックのプロトタイプを実装し，イベントログファイルの監視を行った．

(1)プロトタイプ環境

監視対象マシンは，OSとしてWindows 2003 Serverが動作するパソコン，HIBF作成機能はSymantec社のBackup Exec System Recovery 6.5を用いた．バックアップのタイミングは，1時間ごとに取得できるように設定した．HIBF管理機能はBackup Exec System Recoveryの付属品であるv2ibrowser.exe，抽出機能はセキュリティイベントログからログイン監査を行うツールであるntlast.exe，比較差分抽出機能はGNUのdiff.exe，判定機能はWindows標準のfind.exeを使用した．今回は，監視対象のパソコンと同じ環境で実験を行った．

通常，Windowsがインストールされたデフォルト状態では，セキュリティ監査の設定が無効になっているため，監査ログが出力されない．本実験では，ログインの成功と失敗の監査ができるように監査ポリシーの設定を設定しておく．[11]

(2)実験

実験環境において，1時間おきに取得された最新とそのひとつ前のIBFファイルを用いて，管理者(Administrator)で(1) ログインが成功した場合(2)ログインを失敗した場合(3)対話型でログインした場合について検知できることを行った．手順は，次の通りである．

準備：①管理者(Administrator)で(1) ログインが成功した場合(2)ログインを失敗した場合(3)対話型でログインした場合に異常としてHDF判定DBに登録しておく．②インシデントを発生するために，Windows XP(SP2)のパソコンから，監視対象のパソコンに管理者(Administrator)にログイン,ログインの失敗をしておく．

Step1:構造化　HIBF管理機能でIBF保管庫から直近とその一つ前のIBFであるIBF1,IBF2を取り出し，ドライブにマウントする

Step2:DF 解析　IBF1の解析ファイル群の一つである%Systemroot%¥system32¥config¥secEvent.Evtから，抽出機能であるログイン監査のツールntlast.exeを用いて，リモートでログインした場合の履歴を抽出する．

```
ntlast -s -n 3000 -file IBF1 >F1
```

IBF2も同様の処理を行い，F2を抽出する．なお，ログインが成功した場合以外のときは，-sをそれぞれ，-f,-iに置き換えることで抽出可能である．

比較差分機能であるdiff.exeを用いて，F1とF2の差異FD12を抽出する．

```
diff -dos F1 F2 >  FD12
```

Step3：判定　判定機能であるfind.exeを用いて，FD12とHDF判定DBと比較して該当すると通知する．

```
find "Administrator" FD12  | find  /C  "<"
```

件数が0でない場合には，インシデントとして検知する．

(3)実験の結果

実験を実施したところ，管理者（Administrator)で(1) ログインが成功した場合(2)ログインを失敗した場合(3)対話型でログインした場合について検知できることを確認した．

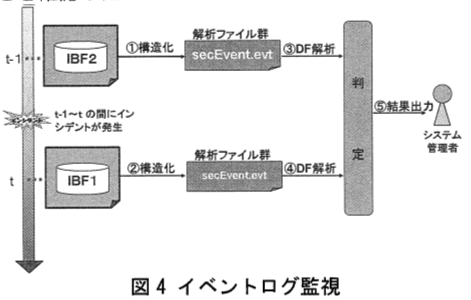

図4 イベントログ監視

4.2【適用例2】監視の分散処理

ホットデジタルフォレンジックの特徴である監視の分散処理が従来のホスト型IDSに対して優位であることについて机上検討をおこなった．

机上検討にあたって，図1で示した比較対象としてホットデジタルフォレンジックの監視対象と同じ領域で比較する．

従来のホスト型IDSは，監視するコンピュータに導入され動作する．よって，インシデント検知のための監視項目が増加すると，監視対象コンピュータが出力するイベントやログの内容が増え，それに伴いCPU処理の負荷は，増加していくことになる．また，ファイルの変更の検知については，監視対象となるファイルのハッシュ値を毎回計算する必要があり，これも比較項目が増えると，CPU処理の負荷の増加要因になる．このように，監視対象の項目が増加するに伴って，CPU使用率は右上がりに増加していくことになる．

一方，ホットデジタルフォレンジックは，監視対象コンピュータとは別に調査用にHDFコンピュータを準備する．監視対象コンピュータでは，IBFを取得するHIBF作成機能のエージェントが導入されており，IBFを取得するためにCPUを使用するが，監視する項目が増えてもCPU使用率はほとんど変わらない．一方，監視を行うHDFコンピュータは，監視項目ごとに2世代のIBFから対象となるファイルを抽出・差分・比較を行う必要があるため，CPU使用率は右上がりに増加していく．従って，監視を行う部分をHDFコンピュータで実施させ分散処理を行うことによって，監視項目が増加しても監視対象のコンピュータのCPU使用率が増加しないことがわかる．

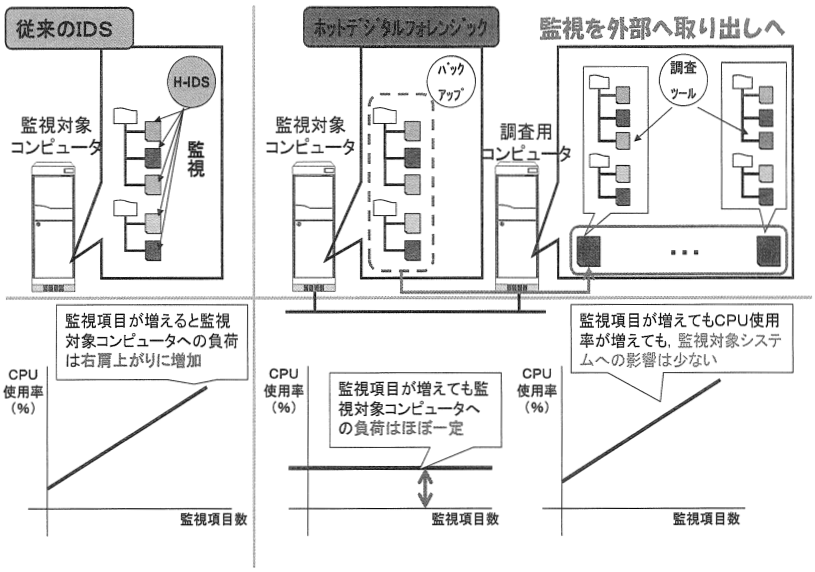

図 5 監視の分散処理

しかしながら，分散処理を行うためには，監視対象コンピュータと HDF コンピュータとの間の通信オーバヘッドが監視対象コンピュータに与える影響，及び HDF コンピュータで必要となるディスク容量サイズについても考慮が必要であり，これらは今後，実際にプロトタイプを実装して検証を行う必要がある．(図 5 参照)

4.3【適用例 3】トレースバック式調査

次に，ホットデジタルフォレンジックのもう一つの特徴であるトレースバック式調査について机上検討を行った．

《事例》

(セキュリティポリシー)

ログファイルの削除を監視対象としているが，バックドアツールは監視対象となっていない．[12]

(動作シーケンス)

(1)時刻 t-1 から t の間に，ログファイルを消去するバックドアツールが設置される．

(2)時刻 t+n-1 から t+n にバックドアが実行され，ログファイルが削除され，インシデントが検知される．

(3)時刻 t+m-1 から t+m(n<m)にそのバックドアツールが削除される．

(4)時刻 t+l(m<l)にインシデントの調査を開始し始める．

(5)調査の結果，バックドアツールが設置され，ログファイルが削除したことが判明する．

まず，従来の IDS で検証する．バックドアツールを設置された時点で，監視対象となっていないため，検知できない．強化のため，バックドアツールを検知できるように監視項目を追加しても，バックドアツールが削除されているため既に汚染されていたかどうか判定できない．

一方，ホットデジタルフォレンジックでは，時系列に管理された IBF 保管庫として，定時ごとにその時点のシステムパーティションの状態が保管されている．この IBF 保管庫から，直近の IBF と直近の一つ手前の IBF を順次時間を遡ってデジタルフォレンジックエンジンで自動分析を行うと，時刻 t+m-1 を分析したときに，バックドアツールが存在したことが検知できる．それから，順次遡っていくことにより，時刻 t-1 を分析したときに，バックドアツールが検知されなくなる．よって，バックドアツールが，時刻 t-1 から t の間に設置され，かつ，時刻 t+m-1 から t+m の間にバックドアのツールが削除されたことを検知することができる．

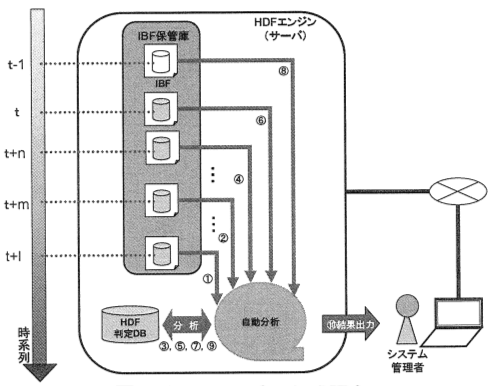

図 6 トレースバック式調査

5　考察

以上、本稿で提案するホットデジタルフォレンジックについて，３つの適用例を用いて実装評価，机上評価の両面から検討を行った．

その結果，【適用例 1】の実装評価では，新たなツール作成をしなくても，既存のツールをうまく組み合わせて利用することにより、監視対象はファイルやイベントログに制限されるが，その監視対象の範囲で市販の専用 IDS とほぼ同等の監視・検知が出来ることわかった．

また，【適用例 2】，【適用例 3】の机上評価を通して，従来の IDS やデジタルフォレンジックの機能を補完できる有用性もわかった．以下にその優位性について述べる．

1）取りこぼし問題について

従来のIDSによるシグニチャ検出方法や異常検出方法では取りこぼしが発生してしまい，インシデント発生時点で適切な情報を収集できないため，後からインシデントの痕跡を調査したくても正しく取得できないという可能性がある．また，ゼロデイ攻撃には対応できない．本提案方式では，一定間隔で監視対象の取得したい情報は全て取得して時系列で保管できるので，トレースバック式調査方式によりゼロデイ攻撃があったかどうか，また、ポリシー設定によりきめ細かな異常検知も対応でき，IDS では取りこぼしてしまうようなインシデント検知に役立てることが可能である．

2）性能低下問題について

業務運用しているシステムでは、運用業務に影響を及ぼさない範囲でのIDSによるセキュリティ対策を実施するため、IDS の監視範囲に制限が加えられることが多い．それが，結局，取りこぼし問題に繋がっていくことから，性能低下への対策は，大変重要である．本提案方式は，監視対象コンピュータとは独立の専用の監視コンピュータで取得した情報の調査・分析・評価を行うため，大量の情報を取得しても業務運用への影響は少なく，セキュリティ対策強化がし易い．また，分散処理方式を採用しているので，リモートの専門のセキュリティ分析者の組織内に置いて解析能力を高めることもできるし，他の監視対象コンピュータの監視コンピュータとの共同利用によるコストダウンなども可能である．

6　おわりに

本研究は，インシデント対応の事前対処のバックアップと事後対処のデジタルフォレンジックの調査・分析技術を組み合わせることにより、インシデント対応における課題である取りこぼし，性能低下を解決できる「ホットデジタルフォレンジック」というコンセプトを検討した．

その結果，ホットデジタルフォレンジックを用いることにより，インシデント対応の課題である取りこぼし，性能低下について解決することができる．

このことにより，「ホットデジタルフォレンジック」は，監視範囲は，ホスト型 IDS よりも狭いが，ホスト型 IDS と併用することにより，セキュリティを強化，補完することができる．又，昨今，J-SOX 法により内部統制の強化が求められているが，従来のデジタルフォレンジックを強化する手法の一つとしても有効である．

今後は，プロトタイプシステムの開発を実施し，ホットデジタルフォレンジック実用上の有効性や適用性を評価していきたい．

参考文献

[1] 日本ネットワークセキュリティ協会 IDS ワーキンググループ,"ホストベースの IDS の概要と適用について,",2002 年 6 月 24 日

[2] 日経ＢＰ社 ITPRO，"IDS の概要と導入のポイント ,"http://itpro.nikkeibp.co.jp/members/ITPro/SEC_CHECK/20010127/1/?ST=security

[3] 日経ＢＰ社 ITPRO，"IDS の弱点と運用上のポイント ,"http://itpro.nikkeibp.co.jp/members/ITPro/SEC_CHECK/20010202/1/

[4] "連載：管理者のためのセキュリティ推進室～インシデントレスポンス入門～第3回 インシデントを発見する方法（2）・システムの改ざんを検知する方法 ," http://www.atmarkit.co.jp/fsecurity/rensai/inci03/inci01.html

[5] Kevin Mandia,Chris Prosise,監修：坂井順行,新井悠,"インシデントレスポンス 不正アクセスの発見と対策,",2002,株式会社翔泳社,pp108-111

[6] 鈴木武,"プロアクティブ・セキュリティ―見えない敵に先手を打つ 第 10 回 フォレンジック［前編］,"IDG ジャパン ComputerWorld,October 2004,pp142-146

[7] 鈴木武,"プロアクティブ・セキュリティ―見えない敵に先手を打つ 第 11 回 フォレンジック［後編］,"IDG ジャパン ComputerWorld,November 2004,pp138

[8] 佐々木良一,芦野佑樹,増渕孝延,"デジタル・フォレンジックの体系化の試みと必要技術の提案,",日本セキュリティ・マネジメント学会誌 Vol.20, No.2 ,pp49-61

[9] 上原哲太郎,"ディジタルフォレンジック-電磁的証拠の収集と分析の技術- ,",2007,情報処理学会誌 2007 年 8 月 Vol.48 No.8,pp889-898

[10] Symantec,"Backup Exec 11d & Backup Exec System Recovery 記事稿抜き刷り,"http://www.symantec.com/content/ja/jp/downloads/pro/bews11_beflf.pdf

[11] Kevin Mandia,Chris Prosise,監修：坂井順行,新井悠,"インシデントレスポンス 不正アクセスの発見と対策,",2002,株式会社翔泳社,pp286-287

[12] 伊原秀明，渡辺勝弘,"不正アクセス調査ガイド rootkit の検出と TCT の使い方 ,"オライリー・ジャパン オーム社,2002 ,pp73-103