マルウェア解析システムにおけるクライアントサーバモデルを用いた復元方法の提案とその実装

朝倉 康生 †　　曽根 直人 ‡　　森井 昌克 †

† 神戸大学大学院工学研究科
657–8501 兵庫県神戸市灘区六甲台町 1–1

yasakura@stu.kobe-u.ac.jp, mmorii@kobe-u.ac.jp

‡ 鳴門教育大学 高度情報研究教育センター
772–8502　徳島県鳴門市鳴門町高島字中島 748

naosone@naruto-u.ac.jp

あらまし マルウェアの動的解析では，システムにマルウェアを感染させるため，解析後にはシステムの復元を行なう必要がある。よって，効率良く解析を進めるためには早急にシステムを正常な状態へ復元する方法が必須である．本稿ではクライアントサーバモデルを用いた復元方法の提案とその実装を行う．提案システムを用いることで，パーティション全体の復元を高速に行うことができる．

A Proposal and Implementation of Recovering Method for Malware Analysis by Server-client Model

Yasuo Asakura†　　Naoto Sone‡　　Masakatu Morii†

†Graduate School of Engineering, Kobe University
1–1, Rokkodai, Nada-ku, Kobe-shi, Hyogo 657–8501, Japan

yasakura@stu.kobe-u.ac.jp, mmorii@kobe-u.ac.jp

‡Advanced Information Research and Education Center, Naruto University of Education
748 Naruto-cho, Naruto-shi, Tokushima 772–8502, Japan

naosone@naruto-u.ac.jp

Abstract Since the system is infected by malwares, it is necessary to restore the system with dynamic analysis of the malware. The malware is the malicious code which threats to computer systems and networks. When applying the dynamic analysis to the malware effectively, the analysts have to restore the system immediately. In this paper, we propose the recovering method by server-client model. Using the proposed system, The entire partition can be restored faster than conventional methods.

1　はじめに

近年，インターネットの常時接続が普及するのに伴い，マルウェアの脅威が大きなものとなっている．マルウェアによる被害を未然に防ぐためにはマルウェアの挙動を解析し，マルウェアに対する適切な対策をとる必要性がある．拡大するマルウェア被害を防ぐため，迅速なマルウェ

ア解析が今後より一層急務となる．

マルウェア解析には実際にマルウェアを動作させその挙動をモニタリング・ツール等で観測する動的解析手法がある．しかし，動的解析手法を用いることにより，解析に用いた計算機はマルウェアに感染してしまう．よって，解析に用いた計算機を解析後に正常な環境に復元する操作が必要となる．

従来，復元操作は解析用 OS がインストールされたパーティション全体をバックアップから復元する方法が一般的であった．パーティション全体を復元する方法では確実に正常な環境へシステムを復元することが可能ではあるが，多くの時間が必要である．高速なマルウェア解析を行うためにはシステムの復元自体も高速であることが望ましい．よって，本稿ではマルウェア解析システムにおける高速な復元方法の提案を行う．提案システムではクライアントサーバモデルを用いてサーバ上のブロックデバイスを解析に用いる計算機で仮想ブロックデバイスとして利用する．つまり，解析に用いる計算機のハードディスクをサーバ OS 上から制御可能となり，サーバ OS 上のファイルシステムがスナップショットやロールバック機能を有していれば，任意の時点でのバックアップや復元を行うことができる．よって，既存の方法より高速に復元を行うことができる．

2　マルウェア解析

マルウェア解析は一般的に 2 つの手法に分類される．本稿ではシステムの復元が特に重要となる動的解析手法についてその詳細を述べ，さらに，システムの復元方法を示す．

2.1　マルウェアの動的解析手法

動的解析手法とは外部から隔離された解析環境内で，実際にマルウェアを実行し，その挙動（Windows API の呼び出し, ファイルやレジストリへのアクセス，ネットワークパケット）をツールなどで観測することにより，マルウェアの挙動を類推する手法である．マルウェアの中には特定の条件下でのみ正常に動作するものが存在するため，解析環境ではマルウェアが動作するよう，ネットワークやインストールするプログラムの調整が必要となる [1][2]．また，マルウェアの動作条件として，仮想環境の評価を行い，仮想環境の場合動作しないマルウェアも多い．よって，解析環境に用いる計算機は実機であることが望ましい．

動的解析手法では実際にマルウェアを動作させるため，解析に用いた計算機はマルウェアに感染する．マルウェアに感染した環境では正常な動作を期待できないため，解析毎に正常な環境へシステムの復元を行う必要がある．ここで，正常な環境とは OS をクリーンインストールした後に最低限必要なドライバ等のみをインストールした環境と定義する．仮想環境を用いて解析を行った場合，正常な環境への復元は仮想環境を提供するシステムの持つスナップショット機能を利用することで非常に容易に行える．しかし，上述の理由により，実機を用いて解析を行う必要性があるため，正常な環境への復元は煩雑かつ時間を要する．

また，マルウェアのアセンブルコードを用いて解析を行う，静的解析手法においても，システムの復元が必要となる手法が存在する [3].

2.2　システムの復元

一般のソフトウェアと異なり，マルウェアはアンインストールのための構造を有していないため，マルウェアのみを取り除くのは困難である．よって，正常な環境への復元はパーティション自体をバックアップから復元する方法をとる場合が多い．

パーティションを復元する機能を有する著名なソフトウェアとして，Acronis True Image がある [4]．Acronis True Image を用いて正常な環境のときのパーティションのバックアップを取得しておき，マルウェアの解析が終了次第，バックアップからパーティションの復元を行うことで，正常な環境への復元が可能である．しかし，パーティション全体を復元する性質上，復元は非常に多くの時間が必要となる．また，パーティションのサイズに比例して必要な時間は大きくなる．

復元に必要な時間を削減した復元システムとして，森川らのシステムがある [5]．森川らのシ

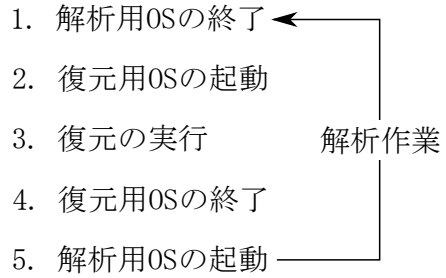
ステムはパーティション全体を復元するのではなく，OS の基幹部分にかかわるファイルのみをバックアップから復元することで高速な復元を実現する．特に，OS を Windows にに限定すると，基幹部分に関わるファイルは\Windows\system32 フォルダに集約されており，このフォルダのみをバックアップから復元する。system32 フォルダのみを復元することにより，パーティション全体を復元するより高速に正常な環境への復元が可能である．また，森川らのシステムは変更があったファイルの特定に高速な方法を用い，変更があったファイルのみバックアップから復元している．しかし，system32 フォルダ以外に対しては変更を加えないため，復元後もパーティション内にマルウェアが存在することは否定できない．さらに，Windows に特化したシステムのため，他の OS では用いることができない．

3 提案復元システム

本章では 2.2 節で述べた既存の復元方法の問題点を考慮し，既存の方法より高速であり，かつ，確実に正常な環境への復元が可能となるシステムを提案する．また，提案システムに対する実装を示す．

3.1 クライアントサーバモデルを用いた復元方法

既存の復元方法において一番問題となるのは復元に時間が必要な点である．ここで，既存の復元方法における復元の流れを示す．



まず，実際の復元方法について考察を与える．パーティション全体を復元する方法は確実に正常な環境への復元が行えるものの，大量のデータの読み書きが生ずるため，時間が必要となる．マルウェアに感染した環境の復元を考える場合，正常な環境との差異は非常に小さいため，パーティション全体を復元する方法は非効率的だと考えることができる．森川らの方法では改変が行われた場所のみを復元するが，その場所の特定に多くの時間がかかってしまい，改変箇所の特定が復元にかかる時間の中で支配的である．逆に，正常な環境との差異は非常に小さいため，改変が行われた場所の特定さえ高速に行えれば復元は容易であることがわかる．しかし，解析用 OS 上でパーティションの監視を行うことは OS 依存の技術を用いる必要があり，かつ，結果の保障が難しい．よって，提案システムではクライアントサーバモデルを用いることでサーバ上に解析用 OS を含む仮想ブロックデバイスを作成し，解析用計算機からサーバ上の仮想ブロックデバイスをマウントすることにより解析を行うものとする．以下，ハードディスク内に仮想ブロックデバイスをもつ計算機をサーバ，仮想ブロックデバイスをマウントして解析を行う計算機をクライアントと定義する．サーバから仮想ブロックデバイスはファイルシステム上の単なるファイルに見えるため，ファイルシステムの管理機能をそのまま適用することが可能である．例えば，ファイルシステムがスナップショットやロールバック機能を有していれば，任意の時点での仮想ブロックデバイスのバックアップや復元を行うことができる．また，クライアント上からはシステムがインストールされたブロックデバイスであるため，計算機に物理的に繋がれたデバイス同様にブートすることができる．

既存の復元方法では復元の実行に必要な時間以外にも復元用 OS の起動と終了に無視できない時間が必要である．通常，計算機に物理的に繋がれたハードディスクは何らかの OS をその計算機上で起動し，アクセスを行う．マルウェアに感染した OS を復元する場合，OS 自身を含むパーティションの復元は困難なため，復元用 OS を別途起動し作業を行なう必要がある。しかし，上述のクライアントサーバモデルを用いたシステムを考えると，復元の実行はサーバ上で動作する OS から行うことができる．解析を行う計算機と復元を行う計算機を別にすることで，復元用 OS の起動と終了を行わず復元する

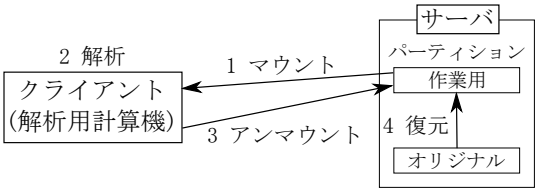


図 1: 提案システム

ことができる．

本稿で提案する復元システムの流れを図 1 に示す．まず，サーバ側でクライアント用のブロックデバイスを用意しておき，クライアントはサーバのブロックデバイスをマウントする．クライアントはマウントしたブロックデバイスから解析用 OS を起動し，マルウェアの解析を行う．解析が終了次第，解析用 OS を終了し，ブロックデバイスをアンマウントする．次に，サーバ OS 上からブロックデバイスの監視によって得た変更箇所に対してバックアップから復元を行う．上記の方法をとることで，復元の実行も高速に行うことができ，かつ，復元用 OS も必要としない．

3.2 実装方法

3.1 節で示した提案システムに対する実装を示す．提案システムの実装にはクライアント上でサーバのブロックデバイスをマウントする技術とサーバ上でブロックデバイスの監視を行い，変更点を取得する技術が必要となる．

まず，クライアント上でサーバのブロックデバイスをマウントする技術について説明を与える．提案システムではクライアント上でサーバのブロックデバイスをマウントし，そのブロックデバイスから解析用 OS をブートする必要がある．そのための技術として，提案システムでは iSCSI を用いる [7]．iSCSI は TCP/IP を用いて SCSI パケットのやりとりを行うプロトコルである．iSCSI を用いることでネットワーク上のファイルやブロックデバイスをクライアント上で外付け SCSI ディスクとして扱うことができる．クライアントとサーバ間の iSCSI による仮想 SCSI ディスクの構成を図 2 に示す．また，iSCSI を用いて認識された外付け SCSI ディスク

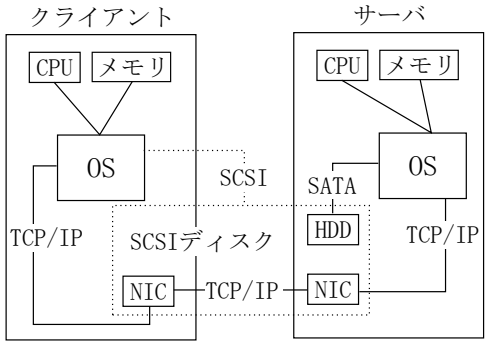


図 2: iSCSI による仮想 SCSI ディスクの構成

から OS をブートすることが可能である．さらに，TCP/IP を用いるので，既存のネットワークとブート用ネットワークを共用できる利点がある．よって，iSCSI は提案システムに適したプロトコルであり，かつ，費用的コストも非常に小さいと言える． 一般的に iSCSI はクライアント側に iSCSI ホストバスアダプタを用いてディスクをマウントする．しかし，iSCSI ホストバスアダプタを用いずに一般的なネットワークインタフェィスカードを用い，ソフトウェア的に iSCSI ホストバスアダプタを実現してディスクをマウントすることも可能である．提案システムでは入手が容易な一般的なネットワークインタフェイスカードを用いてシステムの構築を行う．ただし，一般的なネットワークインタフェイスカードを用いてはブートすることができないため，オープンソースのブートローダ gPXE を用いてブートする [6]．以下に gPXE を用いたブート方法を示す．

1. PXE[1]を用いて gPXE をロード
2. gPXE を用いてサーバ上の SCSI ディスクをマウント
3. SCSI ディスク上の MBR をロード

次に、サーバ上のブロックデバイスの監視方法について示す．ブロックデバイスの監視には ZFS ファイルシステムを用いる [8]．ZFS は OpenSolaris の標準ファイルシステムであり，コピー

[1]ネットワークブート行うための規格．TFTP を用いてイメージをダウンロードし，ブートすることができる．多くのネットワークインタフェィスカードで利用できる．

表 1: 評価に用いた計算機の性能

	サーバ	クライアント 1	クライアント 2
CPU	Intel Core 2 Quad Q9500	Intel Pentium 4 3.2GB	Intel Pentium 4 3.2GB
MEMORY	4GB	512MB	1GB
OS	OpenSolaris 2009.06	Windows XP SP3	Windows XP SP2
NIC	Intel PRO/1000 MT DA[3]	Intel PRO/1000 GT DA	Intel PRO/100 VE Network Connection

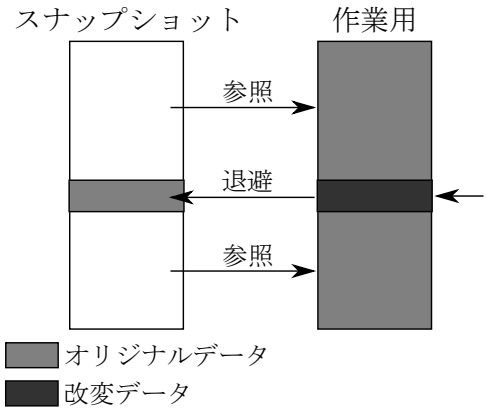


図 3: コピーオンライトによるスナップショット

表 2: 提案システムにおける処理時間

クライアント 1	クライアント 2
119(s)	93(s)

表 3: 既存システムとの処理時間の比較

提案システム	パーティション	system32
119(s)	283(s)	154(s)

表 4: 同時復元時における処理時間

クライアント 1	クライアント 2
147(s)	121(s)

表 5: RAID0 を用いた同時復元時における処理時間

クライアント 1	クライアント 2
116(s)	100(s)

オンライト[2]によるスナップショットを作成できる．コピーオンライトによるスナップショットは図 3 のようにスナップショット時点から変更のあった部分のみを差分として保持している．よって，スナップショットの時点にロールバックすることにより高速に復元することが可能である．また，ZFS はファイルシステム上に仮想ブロックデバイスを作成し，iSCSI により仮想ブロックデバイスを SCSI ディスクとして扱うことができる．上記の特徴により，ZFS は提案システムに最適なファイルシステムである．

4 評価

3 章で提案し，実装方法を示した提案システムに対して，復元時間の計測を行い復元性能の評価を行う．

まず，提案システムを用いて正常な環境への復元をおこなった際に必要な処理時間を示す．評価に用いた計算機の性能を表 1 に示す．また，すべての計算機は同じ GbE 対応スイッチングハブの下に繋がれている．処理時間は解析用 OS が終了プロセスに入った時点を計測開始とし，解析用 OS が再び起動し，ポインタの砂時計が初めて消えた時点を計測終了とする．また，同様の試行を 3 回行い，その平均を計測結果とする．さらに，正常な環境との差異を生成するため，ソフトウェアをインストールし，変更を加えた上で復元を行う．表 2 にクライアント 1，クライアント 2 を用いた提案システムによる処理時間を示す．表 2 より，2 つの計算機双方において，提案システムは高速に復元を行えていることがわかる．また，ネットワークの速度が遅いクライアント 2 の方が処理時間が短いことがわかる．よって，提案システムではネットワーク帯域として 100Mbps 程度あれば十分であると言える。

次に，既存の正常な環境への復元方法と提案システムの比較を行う．既存の方法として，パーティション全体を復元する方法と system32 のみを復元する方法を用いる．また，パーティション全体を復元する方法は Acronis True Image を用い，system32 のみを復元する方法は森川

[2]データをコピーする際に，コピーを実行した時点で物理的にコピーを行うのではなく，オリジナルに変更が加えられた場合に，その部分のみ物理的にコピーを行う仕組みのこと．

[3]DA=Desktop Adapter

らによるシステムを用いて評価を行う．但し，森川らによるシステムは時間の都合上，参考文献にある値から憶測した推測値[4] での比較とする．試行回数や計測方法は提案システムの評価と同様とし，計算機はクライアント 1 を用いた．表 3 に提案システム，パーティション全体を復元する方法，system32 のみを復元する方法における処理時間を示す．但し，表中のパーティションはパーティション全体を復元する方法，system32 は system32 のみを復元する方法を意味する．表 3 より既存のパーティション全体を復元する方法と比較して，提案システムが高速であることがわかる．また，system32 のみを復元する方法と比較しても信頼性，処理時間の双方において提案システムの方が優れていることがわかる．さらに，高負荷時における提案システムの性能評価を行うため，1 台のサーバを用いて 2 台のクライアントを同時に復元した場合の処理時間の比較を行う．試行回数や計測方法は提案システムの評価と同様とし，計算機はクライアント 1 とクライアント 2 を用いた．表 4 に 2 台のクライアントを同時に復元した場合の処理時間を示す．表 2 の単一復元時と比較して大幅に処理時間が増加していることがわかる．原因として，ハードディスク，またはネットワークの性能がボトルネックとなっていることが考えられる．しかし，表 2 の結果より，ネットワーク性能が低いクライアント 2 にクライアント 1 と比較して処理時間の大幅な増加は認められない．よって，ハードディスクの性能が頭打ちになっている可能性が高く，実際にサーバのハードディスク負荷を計測したところ高負荷を確認できた．複数台の同時復元時における性能改善方法として，ハードディスク以外の記憶装置を用いる方法がある．ハードディスクと比較して，SSD や RAM ディスク[5] はランダムリードの性能が高く，性能改善を期待できる．さらに，記憶装置を RAID を用いて多重化することでも性能改善の可能性がある．実際にハードディスク 2 台を用いて RAID0 を構成し，同時復元時の負荷を計測したことろ，表 5 のように単一復元時と同等の処理時間で復元を行うことが可能であった．但し，一般的なシステムの運用時において，同時に複数台のクライアントを復元する可能性は低く，同時復元時における性能がシステムの性能に与える影響は軽微だと考えることができる．

[4]参考文献による森川らのシステムにおける処理時間は 66 秒である．しかし，この処理時間は解析用 OS や復元用 OS の起動終了時間を含んでいない．森川らのシステムは解析用 OS と復元用 OS 双方に Windows を用いている．よって，クライント 1 における Windows XP の再起動時間 44 秒を 2 回分付加して 154 秒とした．

[5]メモリを記憶装置として用いる技術．ハードディスクとして比較して数倍の性能を得ることができる．一般的な弱点として，電源断時に記憶内容が失われてしまうが，本システムではサーバは常に起動状態にあるので大きな問題となりえない．

5 まとめ

本稿ではマルウェア解析に必要となるシステムの復元方法について，既存の復元方法より高速に復元を行える方法の提案を行った．また，提案システムにおける実装を示し，提案システムを用いた復元の性能評価を行った．

参考文献

[1] 三輪信介, 宮本大輔, 櫨山寛章, 井上大介, 門林雄基, “模倣ＤＮＳによるマルウェア隔離解析の解析能向上,” MWS2008, pp.19–24, Oct. 2008.

[2] 星澤裕二, 岡田晃市郎, 山村元昭, 椎木孝斉, “マルウェアの動作条件の抽出,” 情報処理学会研究報告, 2007-CSEC-38, pp.265–269, Jul. 2007.

[3] 岡田隼人, 伊沢亮一, 森井昌克, 中尾康ニ,“ウイルスコード自動解析システムの開発,” SCIS2007, 2F2-4, Jan. 2007.

[4] Acronis True Image, http://www.runexy.co.jp/personal/acronis_trueimage_11/outline/

[5] 森川輝, 村上求, 小篠裕子, 勝手壮馬, 伊沢亮一, 森井昌克, 中尾康二, “メモリ展開されたマルウェアの特徴抽出とその高速化に関する提案,” 信学技法, ICSS2009-28, pp.109–114, Jun. 2009.

[6] Etherboot/gPXE Wiki, http://etherboot.org/wiki/index.php

[7] RFC 3720 - Internet Small Computer Systems Interface (iSCSI), http://www.ietf.org/rfc/rfc3720.txt

[8] OpenSolaris コミュニティ:ZFS, http://jp.opensolaris.org/os/project/jp/zfs/