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

2009－DPS－138 (47)
2009－CSEC－ 44 (47)
2009／3／6

マルウェア動的解析のネットワーク接続制御を支援するユーザインタフェースの提案

芝田 文　吉岡克成　四方順司　松本 勉
横浜国立大学

あらまし　マルウェア動的解析では，解析環境を実インターネットから完全に隔離するとマルウェアの挙動が十分に観測出来ない場合がある．一方で，適切なアクセス制御なしに実インターネットに接続すると解析環境内で実行されたマルウェア検体が外部に攻撃を行う可能性があるため，解析対象の検体ごとに適切なアクセス制御を行うことが重要である．本研究では，解析者によるネットワーク接続制御が可能なマルウェア動的解析システムを提案する．提案システムでは，ネットワーク接続制御が解析者の負担となるため，これを支援するユーティリティとしてGGMS (Graphical Gatekeeper for Malware Sandbox analysis)を導入する．まず，ユースケースによる作業内容の分析によりGGMSの要件を整理する．次に，導出された要件を満たす機能として，マルウェアの通信の全体把握を容易とするサマライズ可視化機能，解析者が注目した挙動の詳細情報の調査を可能とするドリルダウン機能，容易なネットワーク接続制御を可能とする対話型アクセス制御設定機能を示し，GGMSの外部設計を示す．

キーワード　マルウェア動的解析，ユーザインタフェース，アクセス制御，可視化

A Design of User-Interface for Manual Network Access Control of Malware Sandbox Analysis

Hitoshi Shibata　Katsunari Yoshioka　Junji Shikata　Tsutomu Matsumoto
Yokohama National University

ABSTRACT　Recent malware rely on networking when they propagate, talk to their herder, update themselves, and expose sensitive information from the infected host. Therefore, a sandbox for malware analysis should be connected to the real Internet otherwise important behaviors may not be observed. On the other hand, it is a risk to connect the sandbox to the real Internet as malware's attacks may exit the sandbox. In this study, we propose a malware sandbox system whose network access control can be easily configured by an analyst. As it is often a heavy task to control network access, we deploy an enhanced access control utility called Graphical Gatekeeper for Malware Sandbox analysis (GGMS). With the analysis of use cases as well as the requirements of the proposed system, we show an external design of GGMS. In the design, we propose functions such as traffic summary visualization, drilldown of relative information, and interactive access control.

Keyword Malware Sandbox Analysis, User-Interface, Access Control, Visualization

1. はじめに

近年，重要ファイルやパスワードの流出，個人情報の漏洩，迷惑メール，フィッシング，DoS攻撃などのサービス妨害攻撃といった，インターネット上のセキュリティ脅威が増加している．これらの脅威の原因の１つとして，高度に機能化された悪意のあるソフトウェア，いわゆるマルウェアが問題となっている．そのためマルウェアの挙動を詳細に分析し対策を導出するため，マルウェア解析技術の研究開発が活発に行われている[1-5, 7-13]．特に，マルウェアを安全な解析環境において実際に実行し，その挙動を観測・分析するマルウェア動的解析は，(1)パッキングやオブフスケーションといったマルウェアコード自体の解析を困難にする技術の影響を受けない(2)自動化することで効率的に大量のマルウェアを解析することが出来る，といった利点から注目されており，多くの研究が行われている[1, 4, 7]．

しかしながら，マルウェア動的解析においても解決しなければならない問題が存在する．そのうちの１つが，動的解析環境のネットワーク接続制御である．マルウェアの多くは感染ホストがインターネットに接続されていることを前提に作成されているため，解析環境が完全に外部から隔離されていると，本来の挙動を十分に観測できない場合が多い．一方で，解析環境を適切なアクセス制御なしに実インターネットに接続すると，他ホストへの感染行動や迷惑メール，サービス妨害攻撃などが外部に流出し，被害をもたらす可能性がある．

この問題を解決するため，我々は文献[1]でマルチパス解析による動的解析が提案している．この方式では，まず安全な隔離環境で動的解析を行い，観測されたマルウェアの通信の中から危険性が低い通信を自動判別し，これらについては実インターネットへの接続を許可した上で，再度，動的解析を行う．この処理を繰り返すことで安全にマルウェアの挙動を解析することを目指している．しかしながら，近年のマルウェアの通信挙動は多種多様であるため，その危険性を自動的に判断することが難しい場合には，最終的には人間である解析者が通信の内容を確認し，実インターネットへの接続可否を判断する必要がある．

そこで，本研究では，動的解析の利用者である解析者が，マルウェアの通信を把握し，それに基づくネットワーク接続制御を行うことが可能なマルウェア動的解析システムを提案する．提案システムでは，解析者が行うネットワーク接続制御を支援するための高機能なアクセス制御ユーティリティを導入する．当該ユーティリティは分析対象のマルウェアの通信の全体を解析者が直感的に把握できるように可視化し提示するサマライズ可視化機能，可視化された通信挙動の中から解析者がさらに詳細な検討を行うためのドリルダウン機能，各通信について実インターネット接続の可否を制御するための対話型アクセス制御機能を持つ．

本報告の構成は以下の通りである．まず2章で関連研究を説明する．3章では，提案するマルウェア動的解析システムについて説明する．4章では，アクセス制御ユーティリティの設計について述べ，5章でまとめと今後の課題を述べる．

2. 関連研究

従来からマルウェア解析においては，逆アセンブラやデバッガなどを用いてマルウェアコードの機能や構造を分析する方法が行われている．デバッガとしてはIDA pro [10]やOllyDbg [13]が広く知られているが，それらのデバッガでは，解析者の作業を支援するためのユーザインタフェースが工夫されている．例えば，Ollydbgでは解析者がデバッグにおけるブレークポイントの設定，ステップごとのソースコード実行等を，逆アセンブルしたソースコードを参照しながらGUI上で容易に行うことができる．

一方，マルウェア動的解析に関する従来研究としては，CWSandbox[7], Anubis[8], JoeBox[11], Norman Sandbox[12], nicter動的解析システム[4]等がある．これらのシステムは，解析対象のマルウェア検体を受け付けると，自動的に解析を開始し，解析結果をレポートとして出力する機能を有している．しかしこれらの先行研究では，解析者が解析結果を把握し，適切に解析環境の設定を行うためのユーザインタフェースについては，殆ど検討がなされていない．

本研究では，マルウェア通信の可視化を検討するが，このようにネットワークトラフィックを可視化する方法については様々な検討がなされている．文献[5]では，未使用IPアドレス群に届くパケットを世界地図や３次元上に可視化することで，解析者の攻撃動向検知を支援する手法を提案している． 3D-tcpdump[15]は複数ホスト間のトラフィックを3D画面上で可視化し，DoS攻撃等の発見やネットワーク設定を容易にしている．また，honeywall[9]はハニーポットシステムの監視のためのユーザインタフェースを有しており，通信ログだけではなくファイアウォールや侵入検知システムによって検出した通信情報も提示することで，解析者に攻撃動向の把握を促す．他にも，文献[6]では監視ホストにおける通信を時系列に並べ，さらに画面上で監視者の指定した通信ホストのIPアドレス，あて先ポート番号ごとに情報を整理できる可視化手法が提案されている．上記の手法はいずれも監視ホストにおける通信状況把握の支援が目的であるため，通信状況の把握とネットワーク接続設定とを同時に行うインタフェースに関して我々の知る限り検討されていない．

3. 解析者によるネットワーク接続制御が可能なマルウェア動的解析システム

本章では，解析者によるネットワーク接続制御が可能なマルウェア動的解析システム(以下，提案システムと呼ぶ)を提案する．提案システムは，我々が文献[1]で提案した自動マルチパス解析によるマルウェア動的解析システム(これを既存システムと呼ぶ)を基盤としている．但し，既存システムが自動で解析環境と実インターネットの接続制御を行うのに対して，提案システムでは，ユーザである解析者が接続制御を行う．そのため，解析者が解析結果を迅速に把握し，簡便にネットワーク接続制御を行うための高機能なアクセス制御ユーティリティ GGMS (Graphical Gatekeeper for Malware Sandbox analysis)を有している点が特徴である．以降では，まず 3.1 節で，マルウェア動的解析の評価指標と要件を説明し，提案方式の特徴を説明する．3.2 節では，提案システムの概要を示す．GGMS に関しては 4 章で詳説する．

3.1. マルウェア動的解析の評価指標と要件

以下にマルウェア動的解析の評価指標を挙げる．

- 観測可能性 (Observability)
- 安全性 (Security)
- 効率性 (Efficiency)

観測可能性とは，動的解析によりマルウェアの様々な挙動を観測できる性質を指す．次に，安全性とは，解析環境自体がマルウェアに感染したり，解析環境の外部に攻撃が流出することなく，安全に解析を行うことができる性質を指す．最後に効率性とは，マルウェアの挙動を安定的かつ効率的に観測できる性質を指す．

提案システムは，解析者によるネットワーク接続制御を想定しており，優れた解析者が利用する場合，高い観測可能性と安全性が両立できることが期待されるが，自動化システムに比べて効率性が低下することは否めない．そのため，本研究では，解析者によるアクセス制御設定を支援するためのアクセス制御ユーティリティである GGMS を提案する．

3.2. システム概要

提案システムの概要を図 1 に示す．図 1 において，実線はマルウェアの通信を示し，破線はシステム制御のための通

信を示す．提案方式は犠牲ホスト，擬似インターネット，アクセスコントローラ，解析マネージャの4つの構成要素からなる：

犠牲ホスト:犠牲ホストはマルウェア検体を実行し，その挙動を観測するためのホストである．観測対象の挙動には通信挙動と内部挙動があり，それぞれ事前に犠牲ホストにインストールされたモニタリングツールにより収集される[1]．マルウェア実行後はOSイメージを感染前の状態に戻す必要があるため，VMware, ZEN, QEMU等の仮想化技術により効率的なリカバリを実現する[1, 7, 8, 12]．一方，これらの仮想マシン環境は提案システムのような解析システムで利用されることが多いため，仮想環境を検知すると本来の挙動を示さないマルウェアが存在する．これに対して，犠牲ホストを実機により実装する方法も提案されている [4].

アクセスコントローラ:アクセスコントローラは，入力であるアクセス制御情報に基づき，犠牲ホストからの通信を擬似インターネットまたは実インターネットへと転送する役割を持つ．一方，擬似インターネットおよび実インターネットから犠牲ホストへの通信はそのまま転送する．

擬似インターネット:擬似インターネットは，実インターネット上のサーバ群を模倣することで，マルウェアに対してネットワークサービスを提供する．具体的には，FTPサーバ，NTPサーバ，IRCサーバ，HTTPサーバ，SMTPサーバといった実インターネットにおいて一般的に利用可能なサーバサービスを模擬する．さらに，低対話型ハニーポットであるNepenthes [2]も擬似インターネットに含めることで，ネットワークサービスだけでなく，インターネット上の脆弱なホストの模擬を行う．これらのダミーサーバ群は各サービスのデフォルトポートにおいてサービスを提供するが，サービスを用意していないポートに対しては，受信したデータをそのまま返信するECHOサーバが応答するようになっている．

解析マネージャ:解析マネージャは，動的解析システムの中核として，犠牲ホストのOSイメージ管理，マルウェア検体管理，犠牲ホストからの挙動ログの受信・保管，挙動ログの解析，ユーザへの解析結果の提示，ユーザが行ったアクセス制御設定のアクセスコントローラへの反映を担う．解析マネージャはアクセス制御ユーティリティ GGMS を内蔵しており，ユーザは効率的に解析結果の把握とアクセス制御設定を行うことが出来る．GGMSについては4章で詳説する．

解析の流れ:以下に解析の流れを示す．以降では，処理②から⑦までの処理をまとめて解析パスと呼ぶ．

① 解析者が解析対象のマルウェア検体をシステムに入力すると初期設定のアクセス制御情報がアクセスコントローラに反映される．

② 解析マネージャは，犠牲ホストを起動し解析を開始する．

③ 犠牲ホストは，解析マネージャからマルウェア検体をダウンロードし，これを実行する．マルウェアの全ての通信はアクセスコントローラを介して擬似インターネットまたは実インターネットに転送される．

④ 犠牲ホストは，設定されたマルウェア実行時間が経過すると，収集した内部挙動ログおよび通信挙動ログ(パケットキャプチャ)を解析マネージャに転送する．

⑤ 解析マネージャは，犠牲ホストからのログ転送が完了すると犠牲ホストを停止しOSイメージを復元する．

⑥ 解析マネージャは，GGMSを通じて通信挙動の解析者への提示を行う．

⑦ 解析者は，GGMSを通じてアクセス制御設定の変更操作を行い，再解析の指示を出す．解析マネージャは再解析の指示を受けるとステップ②に戻り，新たな解析パスを開始する．

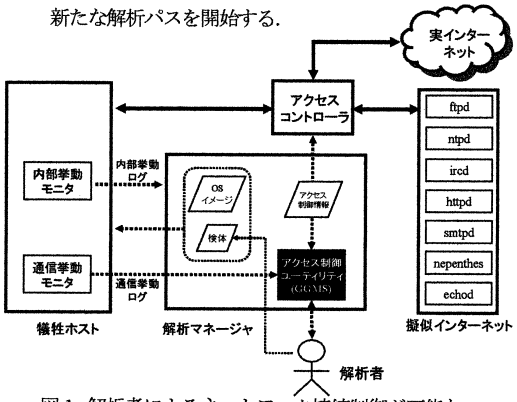


図1. 解析者によるネットワーク接続制御が可能なマルウェア動的解析システム

4. アクセス制御ユーティリティ GGMSの設計

本章では，アクセス制御ユーティリティGGMSの設計について説明する．まず，4.1節では，提案システムにおけるGGMSの要件整理を行う．次に4.2節では，4.1節において示された要件を満たすためのGGMSの特徴的な機能を示す．4.3節では，前節の機能を実現するGGMSの設計を示す．

4.1. 要件整理

3章の説明の通り，解析者の作業は，GGMSによって提示されたマルウェア検体の通信挙動を把握し，その内容を分析し，適切なアクセス制御設定を行った上で再解析を行うこと(または解析を終了すること)であると言える．図2に，これまでのマルウェア解析システムの運用経験から得られたユースケース図を示す．図において破線は包含，実線は汎化を示す．図2から，解析者の作業は大きく分けて，通信挙動の全体把握，特定の通信挙動の詳細把握，アクセス制御設定変更，再解析開始，解析終了であることが分かる．

[1]内部挙動観測については，filemon, regmonといった監視ツールやAPI hook [3]やWindows native API monitoring[8] など様々な観測手法が適用可能である．通信挙動についてはtcpdump等によりパケットキャプチャを行う．

このうち，システムの運用経験から特に作業負担が大きいことが予想される通信挙動の全体把握，特定の通信挙動の詳細把握，アクセス制御設定変更に注目し，整理した要件を以下に示す．

1. 解析者がマルウェアの通信挙動の全体を容易に把握できること
2. 解析者が注目する通信挙動の詳細が容易に調査できること
3. 適切なアクセス制御対象に対して，アクセス制御設定が容易に行えること

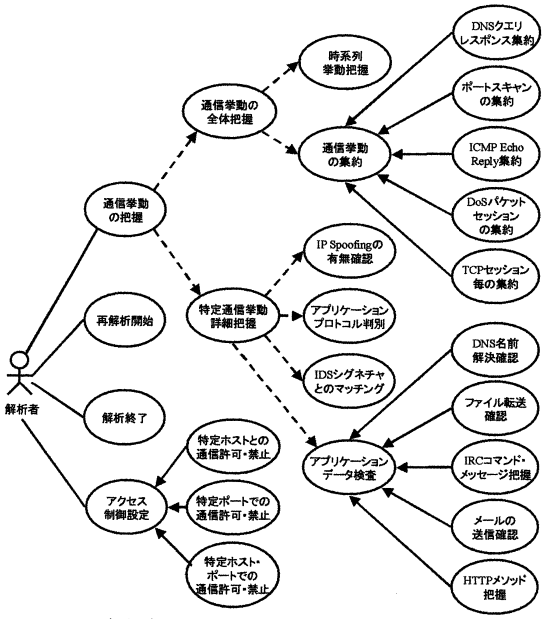


図2. 解析者によるネットワーク接続制御が可能なマルウェア動的解析システムのユースケース図

4.2. 機能

本節では，前節で整理した3つの要件を満たすGGMSの機能を示す．まず，第一の要件である「解析者がマルウェアの通信挙動の全体を容易に把握できること」を満たすため，通信挙動の自動集約と，集約された挙動を時系列表示する**サマライズ可視化機能**を提案する．通信挙動の自動集約処理では，単にTCPセッション毎に挙動を可視化するのではなく，同一のポートスキャンやDoSに含まれる複数のセッションを集約し，それぞれ単一のシンボルで表現することで効果的に挙動を表現する．また，各挙動について有用な情報を属性情報として表示することで，通信挙動の全体把握を支援する．具体的には，送信元IPアドレスのスプーフィングの有無，アプリケーションプロトコル名，サーバ・クライアントの区別，重要なアプリケーションデータ情報(メールの有無，HTTPメソッド，IRCコマンド/メッセージ，DNS名前解決の内容，ファイル転送の有無，転送データサイズ)などが各挙動の属性情報として表示される．

次に，「解析者が注目する通信挙動の詳細が容易に調査できること」を満たすため，上記のサマライズ可視化画面上の各挙動のシンボルに対してマウスクリック等の直感的な操作により詳細情報を表示可能な**ドリルダウン機能**を適用する．ドリルダウン時には，適切な抽象度での表示を段階的に行い最終的には各挙動を構成するパケット情報まで調査可能となるようにする．

最後に，「適切なアクセス制御対象に対して，アクセス制御設定が容易に行えること」を実現するため，上記のサマライズ可視化画面上の各挙動のシンボルに対してマウスクリック等の直感的な操作により，アクセス制御設定を行えるような**対話型アクセス制御設定機能**を適用する．

4.3. 設計

本節では，4.2 節で説明した GGMS の機能を実現する GGMS の設計を示す．まず，図 3 に GGMS の全体図を示す．GGMS はイベント抽出，イベント分析，サマライズ可視化，ドリルダウン，対話型アクセス制御設定という 5 つの主要な機能をもつ．

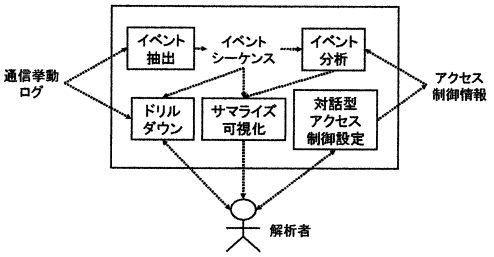


図 3. GGMS の全体図

イベント抽出　イベント抽出とは，通信挙動ログ(パケットキャプチャ)の実体であるパケット単位の挙動情報をイベント単位に集約し，時系列データとする処理を指す．ここでイベントとは解析者がマルウェアの通信の全体把握をする際に扱う抽象度の高い通信を指す．例えば，SMTP サーバに接続してメールを送る，HTTP サーバに接続してファイルをダウンロードする，特定のネットワークセグメントに対してポートスキャンを行う，といった通信がイベントにあたる．

まず，通信挙動ログを TCP, UDP, ICMP 通信に分割する．TCP 通信については 1 つの TCP セッションを 1 つのイベントと考える．UDP 通信については，送信元 IP アドレス，送信元ポート，宛先 IP アドレス，宛先ポートの 4 つ組から関連する UDP パケット群を選択し[2]，1 つのイベントとして集約する．ICMP を用いた通信については，送信元 IP アドレス，宛先 IP アドレスの組からイベントを集約する．さらに，多数のホストに接続を試みるポートスキャンや同一のホストに多数の TCP セッション確立を試みる DoS については，それぞれ判定ロジックを適用して 1 つのイベントへの集約を行う[3]．このように集約されたイベント群を，各

[2] 例えば DNS クエリとレスポンスの組を 1 つの挙動として集約したり，関連する TFTP 通信を集約する．

[3] 具体的には，一定数以上の異なる宛先 IP アドレスに対して同

挙動の開始時のタイムスタンプにより時系列データとしたものをイベントシーケンスと呼ぶ．図4にイベント抽出処理の流れを示す．

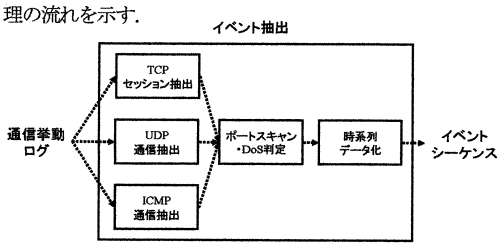


図4. イベント抽出処理の流れ

イベント分析　イベント分析は，イベント抽出により得られるイベントを分析し，分析結果を各イベントの属性情報として出力する処理を指す．分析の内容はイベントの種類により様々であるため，本稿では詳細は割愛するが，イベント分析の流れを図5に示す．

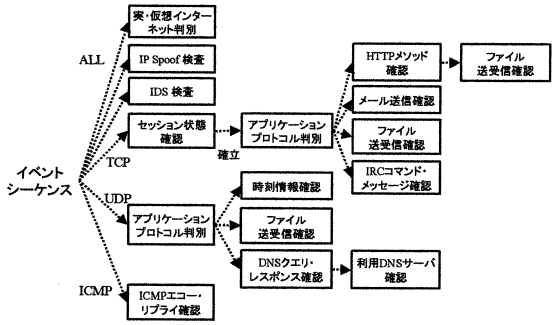
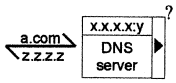


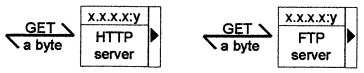
図5. イベント分析の流れ

サマライズ可視化　サマライズ可視化とは，イベント抽出およびイベント分析により得られたイベントシーケンスと属性情報を元に，マルウェアの通信の全体を要約して可視化する処理を指す．各イベントは1つのシンボルとして表示される．シンボルを各イベントの属性情報に依存して変更することで各イベントの概要を解析者が直感的に把握することを助ける．以下にシンボルの具体例を挙げる．

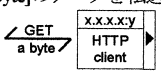
(1) 以下のシンボルは，IPアドレスx.x.x.x，待ち受けポートyのDNSサーバにドメイン名a.comの名前解決を行い，返答としてIPアドレスz.z.z.zを得たことを示す．（以下，サーバのIPアドレス，待ち受けポートについては同様であるので，割愛する．）また，シンボル右上の"?"は当該DNSサーバが犠牲ホストに設定されたDNSサーバではない場合に表示する．



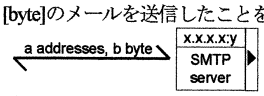
(2) 以下の2つのシンボルは，それぞれHTTPサーバとFTPサーバにデータを要求し，a[byte]のデータをダウンロードしたことを示す．



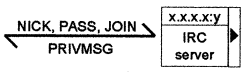
(3) 以下は，HTTPクライアントから犠牲ホストへデータ要求があり，a[byte]のデータを転送したことを示す．



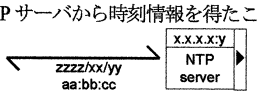
(4) 以下は，犠牲ホストがSMTPサーバを用いてa個のアドレスにb[byte]のメールを送信したことを示す．



(5) 以下はIRCサーバにNICK, PASS, JOINコマンドを送信し，サーバ側からPRIVMSGを受信したことを示す．



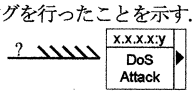
(6) 以下は，NTPサーバから時刻情報を得たことを示す．



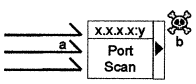
(7) 以下は，犠牲ホストが，それぞれHTTPSサーバとSSHサーバに暗号通信を行い，a[byte]のデータを送信し，b[byte]のデータを受信したことを示す．

(8) 以下は，犠牲ホストがそれぞれNepenthesサーバとECHOサーバに接続したことを示す．

(9) 以下は，犠牲ホストがサーバにDoS攻撃を行いa個のセッションの確立を試みたことを示す．また，"?"はIPスプーフィングを行ったことを示す．



(10) 以下は，犠牲ホストがa個のIPアドレスに対してポートyを用いてポートスキャンを行ったことを示す．なおアドレス表示部は192.168.*.*のようにアドレスブロックを示す形式で表示を行う．また，そのうち，右上のシンボルはb個のIPアドレスへの通信においてIDSシグネチャに一致する攻撃コードが検出されたことを示す．



(11) 以下は，TCPセッションが確立されなかったことを示す．

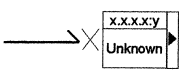


図6に，ある特定のマルウェア[4]を提案システムにより解析し，得られた通信挙動ログをGGMSによりサマライズ可視化した画面を示す．サマライズ可視化画面は，画面の上部から下部へと伸びる時間軸上に各イベントを示すシンボルを配置することで生成される．通信が擬似インターネット内のダミーサーバとの通信である場合と，実インターネ

じ宛先ポートを用いて接続する通信をポートスキャンとして検出する．また，同一の宛先アドレスと宛先ポートに対して一定数以上のセッションの確立を試みる通信をDoSとして検出する．

ット上のホストとの通信である場合によって，シンボルを配置する位置を変えることで，直感的な通信の全体把握を助ける．この例の場合，当該検体が DNS 名前解決後に実インターネット上の IRC サーバにアクセスし，さらに HTTP サーバにアクセスしていることが分かる．HTTP サーバへの接続を許可せず擬似インターネットに接続すると，それ以上イベントは発生しないが，当該サーバへの実インターネット接続を許可して再解析を行うと，さらに破線で囲った部分のイベントが現れる結果となった．

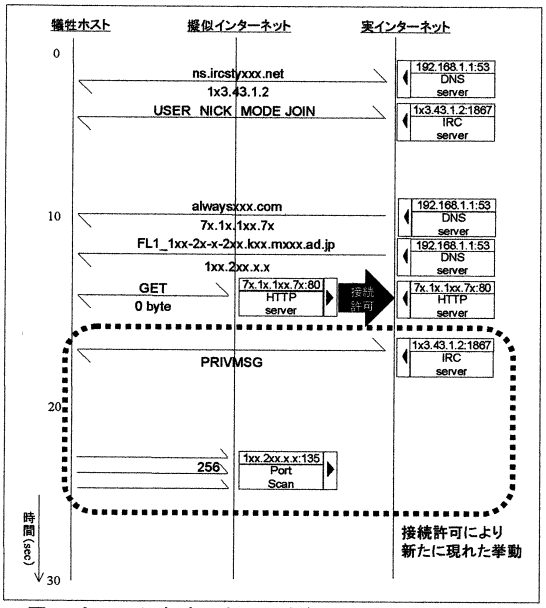


図 6. サマライズ可視化例と設定変更による挙動変化

対話型アクセス制御　対話型アクセス制御は，サマライズ可視化した各イベントに対して次回の解析時にどのようなアクセス制御を行うかを解析者が指示するための機能である．具体的には，サマライズ可視化画面の各シンボルにおいて，ボタンを配置し，それをクリックすることで，実インターネットへの接続と擬似インターネットへの接続を切り替える．図 7 の例では，HTTP サーバへの通信は擬似インターネットに対して行われており，そのためにその後のマルウェアからの通信が見られなくなったことが推察できる．そこで解析者は，HTTP サーバのシンボルをクリックすることで当該サーバへの接続に限って実インターネット接続を許可することができる．

ドリルダウン　ドリルダウン機能は，サマライズ可視化機能により表現された通信挙動の概略を元に関連する詳細情報を解析者に提供する機能を指す．最もシンプルな実現方法としては，シンボルをクリックすることで，別ウインドウを起動し，当該イベントを構成するパケットのダンプデータを表示する方法が考えられるが，特定の種類の通信についてはパケットダンプ以外の表示が望ましい場合がある．例えば IRC 通信の場合は，ホスト間でやり取りされたアプリケーションデータを表示することで，ボットの C&C 通信の内容を調べることができる．ドリルダウン機能の詳細については今後の課題とする．

5. まとめと今後の課題

本研究では，動的解析の利用者である解析者が，解析環境のネットワーク接続制御を行うことが可能なマルウェア動的解析システムを提案し，提案システムに導入する高機能なアクセス制御ユーティリティ GGMS の設計を行った．なお，挙動分析に誤りがあると，サマライズ可視化に影響を及ぼし，結果的に解析者が誤ったアクセス制御を行う可能性があるため，挙動分析の精度に関して評価をする必要がある．また，GGMS を実装し，複数の解析者による評価実験を行い，GGMS がアクセス制御設定の支援と成りえるかを検証し，ドリルダウン等のユーザインタフェースの改良を行っていきたい．

謝辞. 本研究を進めるにあたり，有益なご意見を頂いた独立行政法人情報通信研究機構 衛藤将史氏，井上大介氏に感謝する．

参考文献

[1] 吉岡 克成，松本 勉，"自動マルチパス解析によるマルウェア動的解析の提案，" 暗号と情報セキュリティシンポジウム 2009(SCIS2009), 2E1-1, 2009.

[2] P. Baecher, M. Koetter, T. Holz, M. Dornseif, and F. C.Freiling. "The nepenthes platform: An efficient approach to collect malware," Recent Advances in Intrusion Detection, RAID2006, pp. 165 – 184, 2006.

[3] H. Father, "Hooking Windows API - Technics of Hooking API Functions on Windows," CodeBreakers Journal, Vol. 1, No. 2, 2004.

[4] D. Inoue, K. Yoshioka, M. Eto, Y. Hoshizawa, K. Nakao, "Malware Behavior Analysis in Isolated Miniature Network for Revealing Malware's Network Activity," IEEE International Conference on Communications (ICC 2008), pp. 1715-1721, 2008.

[5] K. Nakao, K. Yoshioka, D. Inoue, M. Eto, K. Rikitake. "nicter: An Incident Analysis System using Correlation between Network Monitoring and Malware Analysis," Proc. 1st Joint Workshop of Information Security (JWIS 2006), pp. 363-373, 2006.

[6] D. Phan, J. Gerth, M. Lee, A. Paepcke, T. Winograd, "Visual Analysis of Network Flow Data with Timelines and Event Plots," Workshop on Visualization for Computer Security, VizSEC 2007, pp. 85 - 99 , 2007.

[7] C. Willems, T. Holz, and F. Freiling, "Toward Automated Dynamic Malware Analysis Using CWSandbox," Security & Privacy Magazine, IEEE, Volume 5, Issue 2, pp. 32 - 39, 2007.
http://www.cwsandbox.org/

[8] Anubis, http://analysis.seclab.tuwien.ac.at/.

[9] honeywall, http://honeywall.org/

[10] IDA Pro, http://www.datarescue.com/

[11] Joe Box, http://www.joebox.org/

[12] NORMAN Sandbox Information Center,
http://www.norman.com/microsites/nsic/

[13] OllyDbg, http://www.ollydbg.de/

[14] VirusTotal, http://www.virustotal.com/

[15] 3D-tcpdump, http://www.3d-tcpdump.org/