情報処理学会論文誌 Vol.54 No.7 1921–1929 (July 2013)

推薦論文

ユーザのPC利用時間帯を考慮したマルウェア対策ユーザサポートシステムの性能評価

川口 信隆[1,a)] 余田 貴幸[1] 山口 演己[1] 笠木 敏彦[2] 衛藤 将史[2] 井上 大介[2] 中尾 康二[2,3]

受付日 2012年12月7日, 採録日 2013年4月5日

概要：本稿では，ユーザのPC利用時間帯を考慮したマルウェア対策ユーザサポートシステムの検体処理時間の性能評価について報告する．マルウェア対策ユーザサポートシステムはマルウェア動的解析システムと連携し，ユーザPCに感染したマルウェアを検知・駆除する．このシステムは単独のマルウェア対策機能では不可能であった，包括的なマルウェア検知・駆除対策を実現する．システムのプロトタイプの性能を評価するために，フィールド実験を実施し，システムがユーザPCから検体を受信する頻度は時間帯により大きく異なることを明らかにした．そしてシミュレーションを通じて，検体の到着時間帯によってシステムの検体処理時間に10倍以上の違いが生じることを示した．本実験結果は，システムを実際に，数百から数千のPCが含まれる組織ネットワークで運用した場合の，処理時間の性能を見積もるうえで大変有用といえる．

キーワード：マルウェア，侵入検知，シミュレーション

Evaluation of Anti-malware User Support System Considering Hours of Day

Nobutaka Kawaguchi[1,a)] Takayuki Yoda[1] Hiroki Yamaguchi[1] Toshihiko Kasagi[2] Masashi Eto[2] Daisuke Inoue[2] Koji Nakao[2,3]

Received: December 7, 2012, Accepted: April 5, 2013

Abstract: In this paper, we describe evaluation results of Anti-Malware User Support System considering hours of day. Anti-Malware User Support System is a system that detects and removes malwares that infect User PCs through the corporation with dynamic malware analysis systems. To measure the performance of the prototype system, we have conducted field experiments, and the results show that the frequency that the system receives samples from User PCs significantly changes over hours of day. Then, through computer simulation experiments in accordance with the experiments results, we demonstrate that the difference of processing time for a sample reaches to more than 10 times depending on the time when a sample arrives. This experiment result will be useful for estimating the system performance when it is deployed in actual organization networks consisting of from hundreds to thousands PCs.

Keywords: malware, intrusion detection, simulation

1. はじめに

今日，日々数千から数万規模で，マルウェアの新種が出現している[15]．新種の急増にともない，シグニチャファ

[1] 株式会社日立製作所
Hitachi, Ltd., Chiyoda, Tokyo 100–8280, Japan
[2] KDDI株式会社
KDDI Corporaion, Chiyoda, Tokyo 102–8460, Japan
[3] 独立行政法人情報通信研究機構
National Institute of Information and Communications Technology, Koganei, Tokyo 184–8795, Japan
[a)] nobutaka.kawaguchi.ue@hitachi.com

本稿の内容は2012年7月のマルチメディア，分散，協調とモバイル（DICOMO2012）シンポジウム2012で報告され，マルチメディア通信と分散処理研究会主査より情報処理学会論文誌ジャーナルへの掲載が推薦された論文である．

イルを基にユーザ PC 内からマルウェアを検知するアンチマルウェアソフトでは，シグニチャファイルの更新が新種マルウェアの出現頻度に間に合わず，検知率が低下している [5]．また，感染のたびに自身のコピーを再暗号化するポリモフィックマルウェアや，感染のたびに挙動が変わるポリモフィックマルウェアの増加も，シグニチャ型対策の有効性低下に拍車をかけている [15]．

これにともない，近年では多数のセキュリティベンダや研究機関がシグニチャに依存しない独自のマルウェア対策機能を開発している．特に主流となっているのは，プログラムの挙動（ファイルアクセスやネットワーク活動など）を解析することで，マルウェアを検知するマルウェア動的解析システム [1], [2], [3], [6] である．しかし，マルウェア動的解析システムはシステムの構成や規模の点から，通常のユーザ PC 上で動作させるにはハードルが高い．また，マルウェア動的解析システムは，通常のアンチマルウェアソフトと異なり，検知したマルウェアを駆除する機能を有していない．これらの点から，一般のユーザ PC 上で，シグニチャに依存しない，包括的なマルウェア対策を実施するのは容易ではない．

この課題を解決するために，複数のマルウェア対策機能と連携して，ユーザ PC に侵入した新種マルウェアの発見から自動駆除までの包括的なマルウェア対策を実施する「マルウェア対策ユーザサポートシステム」が提案されている [13]．このシステムでは，サービスに加入する一般または組織内ユーザの PC から検体を受信して検知・解析処理を行い，検体がマルウェアの場合は自動駆除する．本システムは既存アンチマルウェアソフトを補完するマルウェア対策サービスとして，各組織ネットワークの管理者により運用されることを想定している．

ここで，本システムは，PC 内で起動した実行ファイルを擬陽性ファイル（マルウェアの可能性があるファイル）と判断すると，検体としてユーザサポートセンタに送信する．このため，同一のタイムゾーンにいるユーザを対象としてサービスを実施する場合，多数のユーザが PC を頻繁に利用する時間帯ほど，多数の検体がセンタに送信される．一方で，センタ内で同時に解析できる検体数は限られているため，短時間に多くの検体を受信するほど，検体処理時間（検体の到着から処理が完了するまでにかかる時間）は長くなる傾向にある．すなわち，検体受信時間帯によって処理時間は大きく変動する．処理時間の変動はシステムのサービス品質に影響する．そこで，本システムの実運用にあたっては，時間帯により処理時間がどの程度変動するのかを分析し，システムがサービス品質を満たしているかを検証する必要がある．

本稿では，文献 [13] で提案・実装されているシステムが実運用される際，時間帯によって処理時間にどの程度の違いが生じるかを計測することを目的に，フィールド実験と，実験結果を基に実施したコンピュータシミュレーションを実施した．フィールド実験には数十人のユーザが参加し，数カ月の間，システムを実際に利用した．コンピュータシミュレーションでは，キューイングネットワークモデルを用いてシステムをモデル化した．そして，フィールド実験で得られた結果を基に，数千人のユーザが利用した場合の検体処理時間を求めた．その結果，到着時間帯によって処理時間に 10 倍以上の違いが生じ，その差はユーザ数が増えると指数関数的に増加することを明らかにした．

これまでに Epidemic モデルや AAWP モデルなど数多くのマルウェア感染・駆除モデルが提案されてきたが，筆者らが知る限り，検体の到着頻度がユーザ PC の利用時間帯によって変化する場合の処理時間を分析した例はこれまでにない．本稿で報告する到着時間帯が時間帯に依存するモデルは，到着率が時間帯に依存しない定常到着モデルよりも精度が高く，今後実用的なマルウェア対策を設計・運用するうえで有用といえる．

以下，2 章では関連研究を，3 章ではマルウェア対策ユーザサポートシステムの概要を述べる．4 章でフィールド実験とコンピュータシミュレーションの結果を基に検体処理時間の時間帯依存性を分析する．5 章を本稿のまとめとする．

2. 関連研究

2.1 マルウェア対策

1 日に数千から数万にのぼる新種マルウェアの発生 [15]，および感染ごとに形態を変化させる自己変貌型マルウェアの出現 [16] にともない，シグニチャに依存せず，マルウェア挙動を分析して検知を行うマルウェア動的解析システム [1], [2], [3], [6] の研究がさかんになってきている．また一方で，マルウェアではないことが確認されているプログラムのリスト（ホワイトリスト）[4] を活用して，リストに含まれないプログラムをマルウェアと見なす技術も研究されている [17]．しかし，一般的なアンチマルウェアソフトとは異なり，これらのマルウェア対策機能は，単体では PC 内からのマルウェアの発見から解析，検知・駆除までの包括的なマルウェア対策を実現できない．このため，これらのマルウェア対策機能を利用してユーザのマルウェア対策を支援するには，対策機能と連携するプラットフォームが必要となる．

マルウェア対策機能を連携させて，高度なマルウェア対策を実現するプラットフォームに関する既存研究は数少ない [5], [7]．CloudAV [5] は一般的なアンチウイルスソフトや動的解析システムなどの複数のマルウェア検知機能を統合して検知を行うプラットフォームである．CloudAV はユーザ PC を監視し，アクセスが発生したファイルを解析対象ファイルとして解析システムに送信する．解析システムでは複数のマルウェア検知機能を用いてファイルを分析する．そして，分析結果を統合して最終的な検知結果を求

める．しかし，CloudAV ではファイルがマルウェアと判断された場合にも駆除ツールは生成されないため，包括的対策を実現しているとはいえない．また，擬陽性ファイルを発見する機能を有しておらず，PC 中の全ファイルが解析対象となるため，解析システムやネットワークに大きな負荷がかかるという問題がある．

3 章で説明するマルウェア対策ユーザサポートシステムは，複数のマルウェア対策機能を組み合わせることで，マルウェアの検知から駆除までの包括的対策を効率的に実施する．

2.2 マルウェアの感染シミュレーション

インターネットや大規模ネットワークを対象としたマルウェアの感染シミュレーションモデルは，Epidemiological Model [8] や Analytical Active Worm Propagation（AAWP）モデル [9] を代表に様々に提案されている [8], [9], [10], [11]．これらのモデルでは感染端末数やセキュリティパッチが適用される端末数の時間変化を微分方程式や差分方程式で表現する．しかし，これらのモデルは CodeRed など 24 時間稼働するサーバを狙った大規模感染型ワームの感染パターンを対象としており，電子メールの添付ファイルや WEB からのダウンロードなどを通じて散発的にユーザ PC にインストールされる検体を逐次的に解析・駆除するマルウェア対策技術の性能評価には適用できない．

文献 [13] は，キューイングネットワークモデルに基づきマルウェア対策ユーザサポートシステムのモデルを導出し，文献 [9] でモデル化された大規模感染型マルウェア（CodeRed）に対するシステムの性能評価をコンピュータシミュレーションにより行っている．本稿ではフィールド実験の結果を基に大規模感染型マルウェアが発生していない通常運用時の検体到着モデルを導出し，文献 [13] で導出したシステムモデルを用いてシステムの検体処理時間を分析し，時間帯により検体時間に大きな差が生じることを定量的に明らかにしている．

3. マルウェア対策ユーザサポートシステム

3.1 概要

マルウェア対策ユーザサポートシステムは様々なマルウェア対策機能を連携させて，マルウェアの検知から駆除までの包括的なマルウェア対策を行う．

図 1 に本システムの概要を示す．

本システムはマルウェア対策に必要な処理を 4 種類のマルウェア対策機能（検査ツール，ホワイトリストフィルタ，マルウェア動的解析システム，駆除ツール生成システム）を用いて実現する．

検査ツール（詳細仕様は文献 [12] に記載）は新規プロセスが起動するたびに実行プログラムを静的解析し，マルウェアである可能性があるファイル（以下，擬陽性ファイル）を発見する．解析では，マルウェアの見逃しを防ぐため，マルウェアに見られる特徴を少しでも有するファイルを擬陽性ファイルと判断する．たとえば，マルウェアは静的解析を防ぐためパッカを使いファイルの中身を圧縮・難読化する．検査ツールは，パッカに固有な名称のセクションを持つファイルを擬陽性ファイルと判断する．検査ツールにより，PC 内から擬陽性ファイルを効率的に発見することが可能になる．

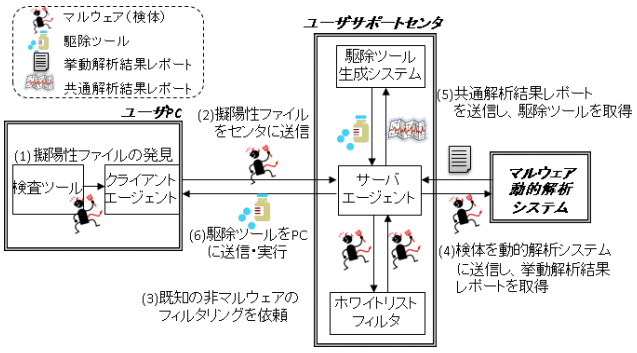

図 1 マルウェア対策ユーザサポートシステム
Fig. 1 Overview of Anti-Malware User Support System.

ホワイトリストフィルタ（詳細仕様は文献 [18] に記載）は，与えられた検体が既知の非マルウェアであるか否かを判定する．判定には，既知の非マルウェアのハッシュ値が格納されたマスタホワイトリスト DB [4] を用いる．ホワイトリストフィルタにより，擬陽性ファイルの集合から，既知の非マルウェアであるものを高速に取り除くことが可能になる．

マルウェア解析システム [1], [2], [3], [6]（本システムで利用したシステムの詳細仕様は文献 [2] に記載）は，サポートセンタから受信した検体を解析環境内で実行する．解析環境は検体が実行される計算機や検体のネットワーク活動を再現するためのネットワークエミュレータなどから構成される．解析環境には検体が呼び出したシステムコールや送受信パケットを記録する機構が備えられており，検体の挙動を記録する．そして，実行開始から数分程度の挙動記録を基に検体がマルウェアであるか否かを判定する．判定では検体の振舞いがマルウェアに固有なものであるか，あるいは非マルウェア（正規アプリケーション）の振舞いから大きく外れていないかをチェックする．判定完了後，マルウェア解析システムは検体の挙動や判定結果などの一連の解析結果を解析結果レポートとしてサポートセンタに返信する．最後に，検体が実行された計算機を実行前の状態に復旧する．マルウェア解析システムにより，既知の非マルウェアではない擬陽性ファイルがマルウェアであるか否かを判定することが可能になる．

駆除ツール生成システム（詳細仕様は文献 [14] に記載）は解析結果レポートを基に，ユーザ PC からマルウェアを駆除する駆除ツールを生成する．駆除ツールは，パターン

ファイルと駆除エンジンから構成される．パターンファイルは，どのファイルやレジストリを削除するのかといった駆除手順を指定する．駆除エンジンは，パターンファイルに従いユーザPC上で駆除処理を行う．駆除ツール生成システムは駆除ツールの一部であるパターンファイルを生成する．駆除エンジンはあらかじめユーザPC上にインストールされている．駆除ツール生成システムにより，マルウェア動的解析システムにマルウェアと判定された検体の，ユーザPCからの駆除が可能となる．

以上，上記の4つのマルウェア解析機能の連携により，PC内からの擬陽性ファイルの発見と既知の非マルウェアのフィルタリング，擬陽性ファイルの解析とマルウェアの検知，検知されたマルウェアの駆除，までの包括的なマルウェア対策が実現される．

ユーザサポートシステムでは，これらの機能を連携させるために，クライアントエージェント（Client Agent, CA），サーバエージェント（Server Agent, SA）という2つの機能を設ける．CAはユーザPC上で，SAはユーザサポートセンタ上で動作する．

3.2 検知・駆除の手順

マルウェア検知・駆除の手順を以下に示す．

1. 最初に，ユーザはユーザサポートセンタからCAをダウンロードしてPCにインストールする．検査ツールはプロセスの起動を監視し，擬陽性ファイルを発見してCAに渡す．
2. CAは擬陽性ファイルを検体としてSAに送信する．送信前に，ファイルはCA・SA間の共通鍵またはSAの公開鍵により暗号化される．また検体と同時にユーザPC内の環境情報を送信する．環境情報にはユーザPCにインストールされているOSやアプリケーションの種類やバージョンなどが含まれる．
3. 検体と環境情報を受信したSAは検体を復号してホワイトリストフィルタに送信する．ホワイトリストフィルタは検体が既知の非マルウェアであるか否かの判定結果を出力する．
   ホワイトリストフィルタが検体を既知の非マルウェアと判定した場合，SAは検体のファイル名とハッシュ値をCAに通知する．CAは，SAから通知されたファイル名とハッシュ値をローカルホワイトリストというファイルに保存する．ローカルホワイトリストはユーザPC内にある既知マルウェアのファイル名とハッシュ値の一覧を保持する．以降，検査ツールが同一検体を発見した場合，ローカルホワイトリストフィルタによりフィルタリングされ，SAには送信されない．また，ローカルホワイトリストには各ユーザが任意のファイルを登録することができる．これにより，特定の個人や組織のみが使用するソフトウェアなど，セキュリティの観点からPC外に出すことが好ましくないファイルのSAへの送信を防止する．
4. ホワイトリストフィルタが検体を既知の非マルウェアと判定しなかった場合，SAは検体と環境情報をマルウェア動的解析システムに送り検体の解析を依頼する．マルウェア動的解析システムは検体を解析し，検体の挙動に関する情報と検知結果を含む解析結果レポートを返答する．マルウェア動的解析システムが検体を非マルウェアと判定した場合，検体はホワイトリストフィルタとCAのローカルホワイトリストに登録されサポートシステムの処理は完了する．
5. マルウェア動的解析システムが検体をマルウェアと判定した場合，SAは検体と解析結果レポートおよび環境情報を駆除ツール生成システムに送信する．駆除ツール生成システムはこれらの情報を基に駆除ツールのパターンファイルを生成してSAに返答する．
6. SAは駆除ツールのパターンファイルをCAに送信する．CAは駆除ツールエンジンを実行してパターンファイルに記された駆除処理を行い，マルウェアをPCから駆除する．以上でサポートシステムの処理は完了する．

3.3 実装

次章で述べるフィールド実験で用いたシステムの実装について述べる．

SAはOSにCentOS5.4を用い，HTTP通信を通じて，CAと検体・駆除ツールの送受信を行う．

駆除ツール生成システムはOSにCentOS5.4を用い，SOAP通信を通じてSAと解析結果レポート・駆除ツールパターンファイルの送受信を行う．

ホワイトリストフィルタはOSにWindows 2003 Serverを用い，SOAP通信を通じて検体・判定結果を送受信する．マスタホワイトリストDBにはセキュリティベンダから提供された800万件以上の既知の非マルウェアのハッシュ値が登録されている．

マルウェア動的解析システムにはNICTが研究開発を行っているnicterミクロ解析システム（以下nicter）[2]を用いた．実験に用いたnicterには8つの動的解析環境が搭載されており，8つの検体を同時に解析することができる．解析環境は検体の解析完了後にディスクイメージの書き戻しを行って環境を復旧する．この処理には5分程度の時間を要する．

4. マルウェア対策ユーザサポートシステムの性能評価

本章では，フィールド実験とコンピュータシミュレーション実験を基に，検体受信時間帯により検体処理時間にどの程度の違いが発生するかを評価，考察する．

表 1 実験結果の概要
Table 1 Result of field experiments.

ユーザサポートシステムに送信された検体数	1985
nicter が解析した検体数	998
nicter がマルウェアと判断した検体数	144
検体処理時間（検体登録処理の開始から駆除ツール作成の完了までにかかる時間）	平均：282 秒 最大：980 秒 最小：146 秒

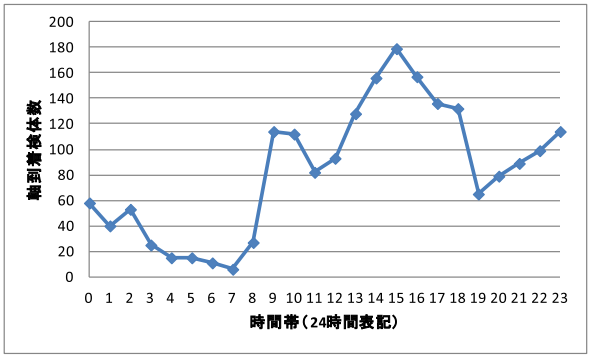

図 2 時間帯ごとの検体到着頻度
Fig. 2 Histogram of malware sample arrivals per each hour of day.

4.1 フィールド実験

システムのプロトタイプを用いたフィールド実験を，5 校の大学・専門学校と共同で，2011 年 9 月から 2011 年 12 月まで約 3 カ月間実施した．

実験は，協力機関の希望に合わせ，検証用に準備した PC を学校内の共通スペースに設置して多数のユーザで共用する形と，各ユーザに 1 人 1 台貸与し期間中占有に使用する形で行った．配布した PC は累計 45 台で，実験に参加したユーザ数は延べ 50 名程度である．ユーザの多くは大学生・専門学校生である．

表 1 に実験結果の概要を示す．実験期間中に送信された検体数は延べ 1,985 体であり，このうち nicter に解析されたのは 998 体となった．

図 2 に，システムが受信した 1,985 体の検体の 0 時台～23 時台までの 1 時間ごとの到着数を示す．図が示すとおり，時間帯によってシステムが受信する検体数には大きな違いがある．検体到着数は日中に多く，9 時～19 時の 10 時間で全体の 65%を占めている．一方で深夜から明け方にかけての検体到着数は少なく，1 時～7 時までの 6 時間で全体の 6%程度にとどまっている．

この結果から，ユーザの PC 利用時間帯を反映して検体到着頻度には時間帯によって大きな偏りがあることが分かる．フィールド実験ではユーザ数と比較してマルウェア動的解析システムの規模が大きかったため，ほとんどのケースで検体はシステムに到着すると待ち時間なく，すぐに処理された．しかし，システムに参加するユーザ数が増えるとシステム内での処理待ち時間が発生する．この場合，処理待ち時間は検体の到着時間帯によって大きく異なる可能性がある．次節ではコンピュータシミュレーションを用いてこの仮説を検証する．

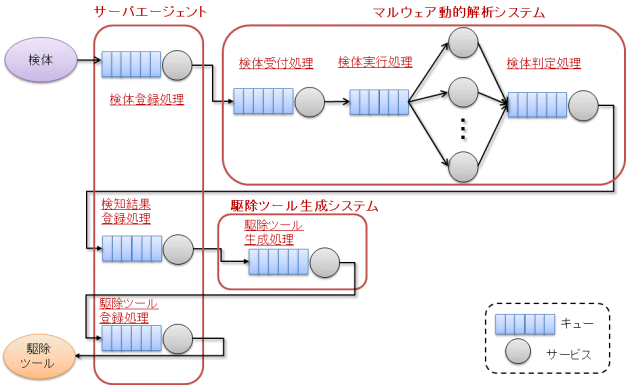

図 3 ユーザサポートセンタのキューイングネットワークモデル
Fig. 3 Queuing network model of the user support center.

4.2 ユーザサポートセンタのシミュレーションモデル

本節では，フィールド実験で得られた検体到着頻度を基に，システムの代表的な適用先である数百台～数千台の PC から構成される典型的な組織ネットワーク [13] における，検体処理時間の時間変化をシミュレーションにより求める．本シミュレーションにより，典型的な組織ネットワークでシステムを 24 時間稼働した場合の処理性能が明らかになる．この結果より，ある性能要求（検体処理時間は最大 30 分以内など）を満たすのに必要なシステム規模（検体の同時並列解析数など）を導出することができる．

ユーザから見た場合のシステムの処理性能は，検体を投入してから結果が返ってくるまでの時間であるため，検体処理時間を，処理性能を測る主なメトリックとして用いた．また，検体は 24 時間何時でも投入される可能性があるため，対象とする時間帯は 0 時～23 時までの 24 時間とした．

図 3 に，キューイングネットワークを用いたユーザサポートセンタのシミュレーションモデル [13] を示す．モデルは 7 種類のサービスおよびキューから構成される．各処理の詳細は割愛するが，最も重要な処理は検体実行処理である．検体実行処理には，検体を解析環境で実行しその挙動を分析する挙動記録処理と，検体実行後の環境を復旧する環境復旧処理が含まれる．挙動記録処理を完了した検体は，解析環境の復旧（環境復旧処理）を待たずに次の処理（検体判定処理）に廻される．検体実行処理は並列して行われ，その並列度はマルウェア動的解析システムに設置された解析環境数と等しい．

表 2 にシミュレーションで用いる各処理の設定値を示す．各値はフィールド実験で得られた実測値を基にしてい

表 2 シミュレーションの設定値
Table 2 Parameters of the simulation.

検体登録処理		10 秒
検体受付処理		10 秒
検体実行処理	挙動記録処理	300 秒
	環境復旧処理	300 秒
検体判定処理		10 秒
検知結果登録処理		10 秒
駆除ツール生成処理		10 秒
駆除ツール登録処理		10 秒
検体実行処理並列数		8 並列

る．システム内に解析待ち検体が存在しない場合，検体処理時間は 360 秒となる．

本モデルは，以下の 7 種類の処理から構成される．(1) は 3.2 節の検知・駆除手順 3 に対応する．(2)〜(5) は検知・駆除手順 4 に対応する．すなわち，検知・駆除手順 4 で行われる処理を細分化したものである．特に，(3) と (4) はシステム中最も時間がかかる処理であり，全体の処理性能に大きく影響する．(6)〜(7) は検知・駆除手順 5 に対応する．(6) は駆除ツール生成までの処理に対応する．(7) は生成された駆除ツールのサーバエージェントへの配信処理に対応する．

検知・駆除手順 1，2 および 6 はユーザ PC に依存する処理であるため，ユーザサポートセンタの処理性能には含めないものとする．

(1) 検体登録処理
ユーザサポートセンタ内で実行される処理．端末から送信された検体をセンタに登録し，マルウェア解析機能に送信する．なお，既知非マルウェア判定機能も，この処理に含まれることとする．

(2) 検体受付処理
マルウェア解析機能で実行される処理．ユーザサポートセンタから取得した検体を検体実行処理のキューに登録する．なお，後述のとおり，検体実行処理は，複数の検体実行環境により並列に行われるが，断りがない限り検体実行処理のキューは 1 つとする．

(3) 検体実行処理
マルウェア解析機能内で実行される処理．検体を，検体実行環境内で実行して，挙動を記録する．挙動記録後は，実行環境を元の状態に復旧する．このため，検体実行処理には，挙動記録処理と環境復旧処理の，2 つの処理が含まれる．
なお，挙動記録処理完了後すぐに，検体は，後段の検体判定処理に回され，環境復旧処理はその後行われるものとする．検体実行処理には，通常，数分の時間を要し，解析機能の中で，最も負荷が大きい．このため，多くのマルウェア解析機能は，複数の実行環境を持ち，複数の検体の実行を並列して行う．

(4) 検体判定処理
マルウェア解析機能内で実行される処理．検体実行処理での検体記録を基に，マルウェア判定を行い，解析結果レポートを生成する．

(5) 検知結果登録処理
ユーザサポートセンタ内で実行される処理．検体の解析結果レポートをマルウェア解析機能から取得して，センタに登録する．検体がマルウェアである場合は，検体と解析結果レポートを駆除ツール自動生成機能に送信し，駆除ツール生成要求を行う．

(6) 駆除ツール生成処理
駆除ツール自動生成機能内で実行される処理．ユーザサポートセンタから取得した解析結果レポートと検体を基に，駆除ツールを生成する．

(7) 駆除ツール登録処理
駆除ツール自動生成機能内で実行される処理．駆除ツールを駆除ツール生成システムから取得し，センタに登録する．

駆除ツール登録処理が完了した段階で，端末内のマルウェアは駆除されるものとする．なお，実際には，端末がマルウェアに感染してから，検体をサポートセンタに送信するまでに，数秒程度のインターバルが発生するが，本シミュレーションではこの時間は，考慮しないものとする．

4.3 評価方法
評価では図 2 で示した頻度に従って，検体が到着した場合の検体処理時間を測定した．各時間帯（60 分）内での検体到着分布はポワソン分布に従うと仮定した．図 2 はユーザ PC 数が 50 台の場合の結果であるため，シミュレーションで用いるユーザ PC 数に比例して，各時間帯に到着する検体数は増加すると仮定した．

表 2 が示すとおり，到着したすべての検体がマルウェア動的解析システムに解析されマルウェアと判定されるわけではないが，本評価ではシステムに最も負荷がかかるケースを想定して全検体が解析されマルウェアと判定されると仮定した．

また，比較対象として，検体到着頻度が時間帯に依存せず一定である場合を仮定した定常モデルについても評価した．定常モデルでは検体到着分布は全時間帯で同一のポワソン分布に従うと仮定した．

4.4 評価結果
図 4 に，ユーザ PC 数が 1,000，1,500，2,000 台の場合の各時間帯における検体処理時間を示す．ユーザ PC 数が 1,000 台の場合，到着時間帯による検体処理時間の違いは小さく，360 秒〜400 秒台で推移している．しかしユーザ

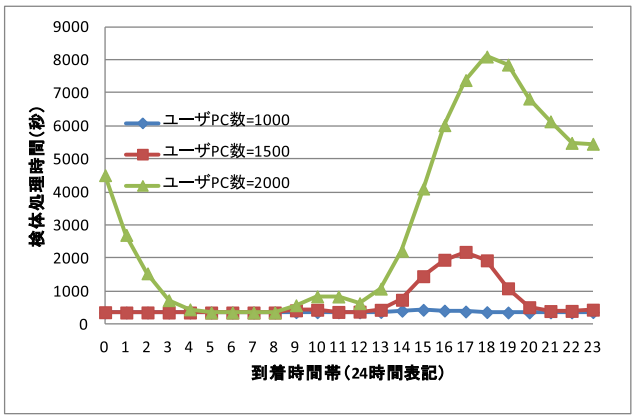

図 4 到着時間帯ごとの検体処理時間
Fig. 4 Sample processing time per each hour of day.

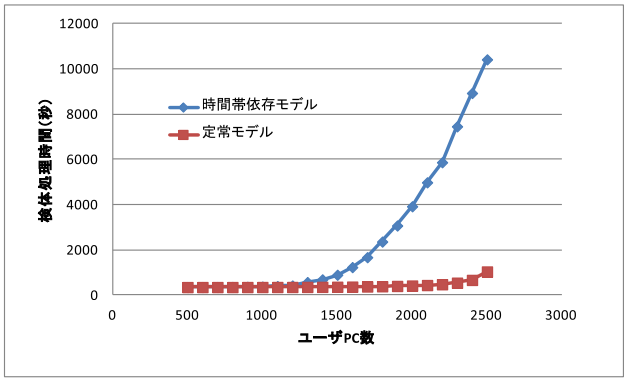

図 5 検体処理時間の平均値の比較
Fig. 5 Comparison of average sample processing times.

PC 数の増加とともに検体処理時間が増大する時間帯が発生する．ユーザ PC 数が 1,500 台の場合，15 時から 19 時台に到着した検体の検体処理時間は 1,000 秒を超える．さらにユーザ PC 数が 2,000 台にまで増加すると，検体処理時間は最大 8,000 秒を超える．また，比較的到着頻度が低い 1 時～2 時台に到着した検体であっても検体処理時間は 1,000 秒を超える．

図 5 に，到着頻度が時間帯に依存するモデルと依存しないモデルでの検体処理時間の平均値の比較を示す．ユーザ PC 数が 1,000 台程度の場合は，どちらのモデルでも検体処理時間は大きく変わらない．しかし，ユーザ PC 数の増加とともに時間帯依存モデルでの検体処理時間は大きく増加する．一方，定常モデルでは検体処理時間の変化は小さい．

4.5 考察

図 4 に示したとおり，時間帯依存モデルでは，検体の到着時間帯によって検体処理時間は 10 倍以上異なる．また，図 5 が示すとおり，定常モデルと比べて平均検体処理時間が非常に長くなる．検体処理時間の長大化は，ユーザ PC がマルウェアに感染している期間の長期化を意味する．このため組織ネットワークにユーザサポートセンタを導入す

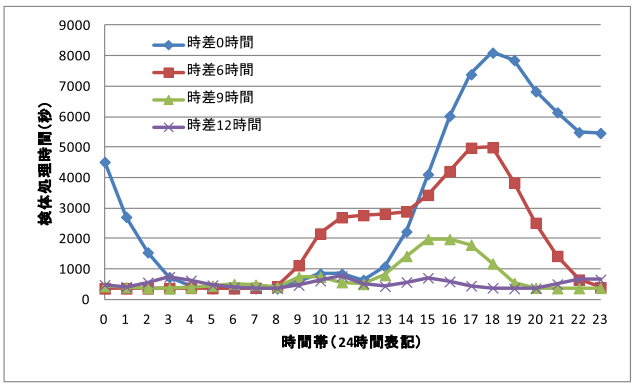

図 6 タイムゾーン間の時差の検体処理時間への影響
Fig. 6 Effects of thee differences of time zones for sample processing time.

る際は，対象となるユーザ PC の稼働時間帯の特性を見極め，適切な規模のシステムを構築・運用する必要がある．たとえば，検体処理時間の平均値を任意の値以下に抑えたい場合，どの程度の規模の PC を収容できるかを考える．仮に平均値を 1,000 秒以内に抑えたい場合，到着頻度の分布が定常モデルに従えば 2,400 台までのユーザ PC を収容できるが，時間帯依存モデルに従うと 1,500 台までしか収容できない．また平均値を，本シミュレーション環境での最小値である 600 秒（10 分）以内に抑えたい場合，到着頻度が定常モデルに従えば 2,300 台までを収容できるが，時間帯依存モデルに従うと 1,300 台までしか収容できない．なお，実際に，平均値をどの程度に設定すればよいかは，システムを運用する組織のセキュリティポリシや，システム構築に費やせる費用に依存する．

一方で，検体到着のピーク時間帯の検体処理時間を低減するために多大なリソース（たとえばマルウェア動的解析システムの解析環境数）を投資すると，それ以外の時間帯のリソースの稼働率が低くなり非効率的である．この問題を解決する 1 つの方法として，複数のタイムゾーンのユーザを 1 つのサポートセンタで扱い，検体到着頻度を平準化する方法がある．たとえば日本と米国ではユーザの活動時間帯が大きく異なるため，両国のユーザ PC 数が同程度であれば，検体到着頻度は平準化され，リソースの利用効率が上昇すると考えられる．**図 6** に，2 つのタイムゾーンにそれぞれ 1,000 台のユーザ PC が存在する場合に，タイムゾーン間の時差が検体処理時間に与える影響を示す．時差が大きくなるほどピーク時間帯は平準化されるため，検体処理時間の時間帯による変動は小さくなる．タイムゾーン間の時差が 12 時間の場合，検体処理時間は全時間帯で 1,000 秒以下となる．

5. おわりに

本稿では，ユーザ PC の利用時間帯を考慮したマルウェア対策ユーザサポートシステムの検体処理時間の性能評価

について述べた．評価結果より，検体到着時間帯により検体処理時間には 10 倍以上の差が生じること，利用時間帯を考慮しないモデルと比べて検体処理時間が長大化することが明らかになった．

今後は，サポートセンタのリソースの利用効率を下げずに検体処理時間の長大化を抑制する方式を検討していく予定である．また文献 [13] に述べられている大規模感染型マルウェアが発生した場合の，定常的に発生する検体の処理時間への影響について分析を進める予定である．

謝辞 本研究成果の一部は，独立行政法人情報通信研究機構の委託研究「マルウェア対策ユーザサポートシステムの研究開発」によるものです．

参考文献

[1] Willems, C., Holz, T. and Freiling, F.: Toward Automated Dynamic Malware Analysis Using CWSandbox, *IEEE Security and Privacy Magazine*, Vol.5, No.2 (2007).
[2] Inoue, D., Yoshioka, K., Eto, M., Hoshizawa, Y. and Nakao, K.: Automated Malware Analysis System and its Sandbox for Revealing Malware's Internal and External Activities, *IEICE Trans. Information and Systems*, Vol.E92-D, No.5 (2009).
[3] Lanzi, A., Balzarotti, D., Kruegel, C., Christodorescu, M. and Kirda, E.: AccessMiner: Using System-Centric Models for Malware Protection, *Proc. 17th ACM Conference on Computer and Communications Security* (2010).
[4] National Software Reference Library, available from ⟨http://nsrl.nist.gov/⟩.
[5] Oberheide, J., Cooke, E. and Jahanian, F.: CloudAV: N-Version Antivirus in the Network Cloud, *Proc. 17th Usenix Security Symposium* (July 2008).
[6] Norman Solutions: Normand sandbox whitepaper, available from ⟨http://download.norman.no/whitepapers/whitepaper_Norman_SandBox.pdf⟩.
[7] Virustotal, available from ⟨http://www.virustotal.com⟩.
[8] Zou, C.C., Towsley, D. and Gong, W.: On the performance of internet worm scanning strategies, *International Journal on Performance Evaluation*, Vol.63, No.7, pp.700–723 (2006).
[9] Chen, Z., Gao, L. and Kwiat, K.: Modeling the spread of active worms, *Proc. IEEE INFOCOM 2003* (2003).
[10] Onwubiko, C., Lenaghan, A.P. and Hebbes, L.: An improved worm mitigation model for evaluating the spread of aggressive network worms, *Proc. IEEE International Conference on Computer as a Tool 2005*, pp.1710–1713 (2005).
[11] Zou, C.C., Gong, W. and Towsley, D.: Worm propagation modeling and analysis under dynamic quarantine defense, *Proc. 2003 ACM Workshop on Rapid Malcode*, pp.51–60 (2003).
[12] 川口信隆，余田貴幸，川口龍之進，寺田真敏，笠木敏彦，星澤裕二，衛藤将史，井上大介，中尾康二：マルウェア対策ユーザサポートシステムを用いた CCC DATASet 2010 の解析，マルウェア対策研究人材育成ワークショップ 2010 予稿集 (2010).
[13] 川口信隆，余田貴幸，山口演己，笠木敏彦：マルウェア対策ユーザサポートシステムのキューイングネットワークモデル，情報処理学会論文誌，Vol.53, No.11 (2012).
[14] 川口信隆，余田貴幸，山口演己，笠木敏彦：マルウェア解析システムを用いたマルウェア自動駆除手法の検討，電子情報処理学会第 14 回 ICSS 研究会予稿集 (2011).
[15] Symantec: INTERNET SECURITY THREAT REPORT 2011 Trends, available from ⟨http://www.symantec.com/connect/sites/default/files/b-istr_main_report_2011_21239364.en-us.pdf⟩ (2012).
[16] Wichersk, G.: PeHash: A novel Approach to Fast Malware Clustering, *Proc. USENIX LEET 2009* (2009).
[17] 特開 2012-185745，携帯端末，プログラム，および通信システム．
[18] 川口信隆，余田貴幸，山口演己：マルウェア対策ユーザサポートシステムにおける既知非マルウェアフィルタ機能の設計，電子情報通信学会 2011 年総合大会予稿集 (2011).

推薦文

ユーザの PC だけでなくサポートセンターと連携することにより，マルウェアを検出する方法を提案しており，今後のマルウェア対策として有用であるといえる．また，提案するマルウェア検出方法に対し，ユーザの PC 利用傾向が与える影響について，実証実験を通じて評価しており，実用性の面で高い貢献が認められる．よって，本研究会からの推薦に値する．

（マルチメディア通信と分散処理研究会主査 勝本道哲）

川口 信隆 （正会員）

2008 年 3 月慶應義塾大学大学院理工学研究科後期博士課程修了．博士（工学）．2008 年 4 月株式会社日立製作所に入社．同社横浜研究所でネットワークセキュリティおよびマルウェア対策の研究開発に従事．2008 年 IPSJ 論文船井若手奨励賞，2012 年 DICOMO シンポジウム優秀論文賞受賞．2011 年より情報処理学会グループウェアとネットワークサービス研究会運営委員．IEEE，ACM 各会員．

余田 貴幸

1999年3月早稲田大学理工学部電子・情報通信学科卒業．2001年3月早稲田大学大学院修士課程修了（工学）．2001年4月日立製作所入社，情報・通信プラットフォームグループ通信事業部に配属．2002年4月日立製作所公共システム事業部でセキュリティ関連システムのシステムエンジニアとして従事．

山口 演己

1998年（株）日立製作所入社．情報システム部でセキュリティ・ネットワーク等の運用管理を行った後，セキュリティ・トレーサビリティ事業部でセキュリティ製品の開発やセキュリティシステムの構築に従事．

笠木 敏彦

1985年国際電信電話株式会社入社．無線・伝送システムの建設，保全業務に従事後，ISPにおけるネットワーク，セキュリティ対策およびサーバホスティングの業務を担当．現，KDDI株式会社情報システム本部共通業務システム部所属．

衛藤 将史 （正会員）

2005年情報通信研究機構入所．以来，ネットワーク運用管理技術，アプリケーショントレースバック技術，nicterプロジェクトやIPv6セキュリティ等，情報通信セキュリティ技術の研究開発に従事．nicterプロジェクトでは主に次世代型サイバー攻撃観測プラットフォームの研究に取り組む．2009年科学技術分野の文部科学大臣表彰（科学技術賞）を受賞．博士（工学）．

井上 大介 （正会員）

2003年横浜国立大学大学院工学研究科博士課程後期修了．2003年通信総合研究所（現，情報通信研究機構）に入所．2006年よりインシデント分析センターnicterの研究開発に従事．現在，情報通信研究機構ネットワークセキュリティ研究所サイバーセキュリティ研究室室長，同機構サイバー攻撃対策総合研究センター（CYREC）サイバー防御戦術研究室室長（兼務）．2002年暗号と情報セキュリティシンポジウム論文賞，2009年科学技術分野の文部科学大臣表彰（科学技術賞）等を受賞．博士（工学）．

中尾 康二 （正会員）

1979年早稲田大学教育学部数学科卒業．1980年国際電信電話株式会社入社．2000年株式会社KDD研究所．2003年KDDI株式会社技術開発本部．現在，KDDI株式会社運用統括本部情報セキュリティフェロー，独立行政法人情報通信研究機構（NICT）ネットワークセキュリティ研究所主管研究員，同機構サイバー攻撃対策総合研究センター（CYREC）研究統括，早稲田大学/名古屋大学非常勤講師，ISO/IEC SC27国内委員会WG4主査，ITU-T SG17副議長，セキュリティ対策推進協議会代表，日本セキュリティ監査協会理事，内閣官房重要インフラ専門委員会専門委員等．情報処理学会研究賞，標準化貢献賞（日本規格協会），経済産業省大臣賞，英国KPMG賞，総務省局長表彰，文部科学大臣賞等を受賞．