情報処理学会論文誌 Vol.57 No.9 2021–2033 (Sep. 2016)

マルウェア感染ホストへのリモート再侵入により感染拡大を阻止する手法

田辺 瑠偉[1,a)] 鈴木将吾[1] イン ミン パ パ[1] 吉岡 克成[2] 松本 勉[2]

受付日 2015年12月3日, 採録日 2016年3月4日

概要：マルウェアには，攻撃対象ホスト上のネットワークサービスの脆弱性を突いてその権限を奪取するリモートエクスプロイト攻撃や脆弱なパスワードが設定されている機器へ不正侵入を行うことで感染を拡大するものが存在し，インターネット上の重大な脅威となっている．こうしたマルウェアに感染したホストは，その脆弱性を修正しない限り感染中もさらなるリモート侵入を受ける可能性がある．一部のマルウェアは自らが侵入する際に悪用した脆弱性を感染後に修正することで他のマルウェアによる侵入を防ぐことが知られているが，マルウェア感染ホストへのリモート再侵入の可能性についてはこれまで詳しく検証されていない．そこで本稿では，実マルウェア検体を用いた動的解析実験によりマルウェア感染ホストへのリモート再侵入の可否を検証し，マルウェアに感染したホストへのリモート再侵入により感染の拡大を阻止する手法を提案する．検証実験では，ハニーポットを用いて収集したリモートエクスプロイト攻撃を行う 294 検体のうち，181 検体においてリモート再侵入が成功した．同様に，ハニーポットを用いて収集した組み込みシステムを狙うマルウェア 18 検体のうち 7 検体においてリモート再侵入が成功した．リモート再侵入が成功したマルウェア感染ホストについては，侵入に用いたサービスや感染拡大を行っているプロセスの停止，通信の制限を行うことができた．提案手法を用いることで，保護対象ネットワーク内で発生した感染拡大活動を観測し，マルウェア感染ホストへのリモート再侵入により感染が拡大するのを阻止する，マルウェアへの早期対応を目指す．

キーワード：マルウェア対策，再侵入，脆弱性，組み込みシステム

Malware Expansion Interception Method Focused on Remote Takeover against Malware-infected Hosts

Rui Tanabe[1,a)] Shogo Suzuki[1] Yin Minn Pa Pa[1] Katsunari Yoshioka[2] Tsutomu Matsumoto[2]

Received: December 3, 2015, Accepted: March 4, 2016

Abstract: Malware which expand infection by exploiting vulnerable network services have been a great threat on the Internet for several years. Moreover machines with default passwords and configurations, mainly embedded device, are being attacked and many security incidents have been reported. Malware infected hosts have the possibility of being takeover by other malware unless the vulnerability which the first malware abused is replaced. Although some malware are known to replace the vulnerability, not much research has been done for inspecting remote takeover. In this paper, by executing several malware samples which expand infection using remote exploit attack and password cracking, we examine the potentiality of remote takeover against malware infected hosts and propose a malware infection expansion interception method. From the results of our experiment, out of 294 malware samples which were collected by honeypot and expanding infection by remote exploit attack, 181 malware samples were successful for remote takeover. Equally, out of 18 malware samples which targeted embedded device and expanded infection by password cracking, 7 malware samples were successful for remote takeover. By using remote takeover, we were successful to stop the service which was used for remote takeover and the malicious processes which was expanding infection. We were also successful to drop packets which were targeted to expand infection for embedded devices. Our proposal method is to intercept malware infection expansion at target network by conducting remote takeover against hosts which are attacking others.

Keywords: anti malware, takeover, vulnerability, embedded device

1. はじめに

近年，コンピュータウィルスやワーム，ボットなどといった，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による被害が増加しており大きな問題となっている．これまで，マルウェアの多くは Windows マシンを狙うものが多かったが，最近ではブロードバンドルータをはじめとする通信機器やビデオレコーダなどの家電製品，プリンタ，監視カメラ，自動車，など多くの組み込みシステムがインターネットにつながる状況になっており，従来の対策に加え，こうした組み込みシステムへの対策も求められている．

マルウェアの感染経路は多岐にわたるが，その 1 つに攻撃対象ホスト上のネットワークサービスの脆弱性を突いてその権限を奪取することでマルウェア感染を引き起こすリモートエクスプロイト攻撃がある．これまで，リモートエクスプロイト攻撃による感染機能を有するマルウェアの多くは Windows マシンを狙うものが多く，なかでも 2003 年に発見された SQL Slammer [1] や 2008 年に発見された Conficker [2] などは世界中で猛威を振るった．このようなマルウェアに感染したホストは依然として多数存在し，今なおインターネット上の重大な脅威となっている．一方，組み込みシステムの場合，Telnet や Web 管理ページの ID やパスワードがデフォルト設定のままになっているものが存在し，攻撃者にとって魅力的な攻撃対象となっている [3]．実際に，2010 年に発見された Chuck Norris [4], [5] や 2014 年に発見された Moon [6]，2015 年に発見された Linux Moose [7] などは多数の組み込みシステムに感染し，大きな話題となった．リモートエクスプロイト攻撃やパスワードクラッキングによりマルウェア感染したホストは，その脆弱性を修正しない限り，感染中もさらなるリモート侵入（以降では，リモート再侵入と呼ぶこととする）を受ける可能性がある．一部のマルウェアは自らが侵入する際に悪用した脆弱性を感染後に修正することで他のマルウェアによる侵入を防ぐことが知られているが [8]，リモート再侵入の可能性についてこれまで詳しく検証されていない．

本稿では，マルウェア感染ホストへのリモート再侵入の可否について，実マルウェア検体を用いた動的解析実験により検証し，リモート再侵入によりマルウェアの感染拡大を阻止する手法を提案する．一般に，企業や官公庁などといった組織では，SOC（Security Operation Center）を中心にネットワークや利用されている機器の監視が行われる．一方，実際にインシデントが発生した場合には，CSIRT（Computer Security Incident Response Team）が ① 初期対応，② インシデントハンドリング，③ 再発の防止に向けた対応を行う．しかし，マルウェアの感染経路や攻撃対象の多様化にともない，監視システムが報告するアラートの数は増加しており，すべての攻撃に対応することは難しい．そこで，上記目的の中で「初期対応」に注目し，保護対象ネットワーク内でリモートエクスプロイト攻撃やパスワードクラッキングをはじめとするマルウェアの感染拡大活動を観測した場合に，攻撃元ホストに対してリモート再侵入を行い，マルウェアの感染拡大活動の停止や侵入に用いた脆弱性の修正を行うことで，CSIRT が現場に到着して対応を行うまでの間に被害が広がるのを防ぐシステムを提案する．提案手法は，マルウェアの駆除を目的としておらず，保護対象ネットワーク内で発生したインシデントへの早期対応を目指す．この際，保護対象ネットワーク内にいるホストに専用の監視ツールをインストールすることなく，リモートからマルウェアの感染拡大活動の停止や脆弱性を修正できる点が有用といえる．また，Windows マシンだけでなく組み込みシステムに対しても有効に働く点が特徴的である．

検証実験では，様々な脆弱性を有する第 1，第 2 の犠牲ホストを動的解析環境内に用意し，第 1 犠牲ホストでマルウェア検体を実行し，発生した感染拡大活動を第 2 犠牲ホストに転送することで，実インターネット上で起きているマルウェア感染を再現した．そして，第 2 犠牲ホストへ脆弱性スキャンツールなどを用いて再侵入を試みることで，リモート再侵入の可否について検証した．実マルウェア検体を用いた実験の結果，ハニーポットを用いて収集したリモートエクスプロイト攻撃を行う 294 検体のうち，181 検体においてリモート再侵入が成功した．同様に，ハニーポットを用いて収集した組み込みシステムを狙うマルウェア 18 検体のうち 7 検体においてリモート再侵入が成功した．加えて，リモート再侵入が成功したマルウェア感染ホストについては，侵入に用いたサービスやマルウェアのプロセスの停止，通信の制限を行うことができた．一方，実験に用いたマルウェアの中には感染後に脆弱性の修正や通信の制限を行うことで，他のマルウェアによる侵入を防ぐものも存在した．

以降，2 章で関連研究を紹介し，3 章ではマルウェア感染ホストへのリモート再侵入により感染拡大を阻止する手法について説明する．4 章では実マルウェア検体を用いた検証実験について説明し，考察を行う．最後に，5 章でまとめと今後の課題を述べる．

2. 関連研究

マルウェアへの対策を考えるうえで，マルウェアの挙動

[1] 横浜国立大学
Yokohama National University, Yokohama, Kanagawa 240–8501, Japan
[2] 横浜国立大学大学院環境情報研究院/横浜国立大学先端科学高等研究院
Graduate School of Environment and Information Sciences and Institute of Advanced Sciences, Yokohama National University, Yokohama, Kanagawa 240–8501, Japan
[a)] tanabe-rui-nv@ynu.jp

を把握することは重要であり，解析環境内で実際にマルウェア検体を実行する動的解析に関する研究が広く行われている．動的解析では，外部へ攻撃が流出しないようにフィルタリングを行うのが一般的であり，これまでに隔離環境に近い環境から解析を繰り返し，危険性が低いと判断された通信を徐々にインターネットに接続をする手法 [9], [10] や擬似的な応答を返す仮想インターネットによりマルウェアの挙動を観測する手法 [11] が提案されている．一方，動的解析では短時間でマルウェア検体の挙動を観測できるが，すべての挙動を観測できるわけではない．そのため，マルウェア動的解析環境内に犠牲ホストを複数設置することでリモートエクスプロイト攻撃を効果的に観測する手法 [12], [13] や，マルウェアが行う通信をダミークライアントにより模擬することで，攻撃者のサーバからの応答を効率的に収集する手法が提案されている [14]．また，最近では組み込みシステムに感染するマルウェアの挙動を観測するための手法 [15] や Linux マシン上で動作するマルウェアを解析するためのネットワーク制御方式などが提案されている [16]．

動的解析に加え，ダークネットと呼ばれる，インターネット上で到達可能かつ未使用の IP アドレス空間に到達するパケットを観測・分析することで，マルウェアによる不正活動を把握する研究 [3], [17], [18], [19], [20] や，ハニーポットと呼ばれる脆弱なサービスやシステムを模擬した囮ホストをインターネット上に用意しておくことで，マルウェア検体の収集や攻撃の分析を行う研究 [21], [22], [23] が行われている．また，Shodan [24] のように能動的にインターネット空間を探索し，インターネットに接続された組み込みシステムを探索しているプロジェクトや，インターネット空間をスキャンすることで攻撃対象ホストを分析した結果が報告されている [25]．このように，マルウェアの挙動を観測する手法やその分析結果に関する研究が活発に進められている．しかし，マルウェア感染時に悪用された脆弱性に対するリモート再侵入の可能性についはこれまで詳しく検証されていない．

我々は，文献 [26] において Windows マシンを狙ったマルウェア感染ホストへのリモート再侵入により，攻撃者が効率的に感染を拡大する攻撃手法について検討したが，リモート再侵入をマルウェア対策に利用することについては検討していなかった．また，組み込みシステムを狙ったマルウェアについても，マルウェアが侵入する際に悪用した脆弱性を利用して，マルウェア感染ホストに再侵入できる可能性がある．以上より，本稿ではハニーポットを用いて収集した実マルウェア検体に対して動的解析を行い，マルウェア感染したホストへのリモート再侵入の可否について検証する．そして，マルウェア感染ホストへのリモート再侵入によりマルウェアの感染拡大を阻止する手法を提案する．

3. マルウェア感染ホストへのリモート再侵入により感染拡大を阻止する手法

本章では，マルウェア感染ホストへのリモート再侵入により感染拡大を阻止する手法を提案する．まずはじめに 3.1 節で提案手法の基本アイディアを説明し，3.2 節で提案手法の実現形態であるマルウェア感染ホストへのリモート再侵入により感染拡大を阻止するシステムについて説明する．そして，3.3 節でシステムの実装について説明する．

3.1 基本アイディア

提案手法は，リモートエクスプロイト攻撃やパスワードクラッキングによりマルウェア感染したホストに対してリモート再侵入することで，マルウェアの感染拡大活動の停止や脆弱性の修正を行うものである．**図 1** に提案システムの基本アイディアを示す．

マルウェアの感染経路に，ネットワークサービスの脆弱性を突いてマルウェア感染を引き起こすリモートエクスプロイト攻撃や，脆弱なパスワードが設定されているリモート接続サービスの認証を突破するパスワードクラッキングという方法がある．こうした攻撃では，感染を拡大するために広範囲の IP アドレスをスキャンする場合が多く，スキャンの宛先となる IP アドレスが無作為に選ばれる場合が多い．このため，ダークネット上でもこうした攻撃を観測することができる．たとえば文献 [19] による統計では，2010 年におけるクラス C ネットワークにスキャンなどのアクセスを行うホストの数は 1 日あたり数万ホストであった．また，ダークネットに届くパケットの統計情報を日ごとにまとめた NicterWeb [18] の結果によると，2015 年 11 月現在，リモートエクスプロイト攻撃と思われる 445/tcp や 1434/tcp 番ポート宛のパケット，パスワードクラッキング攻撃と思われる 22/tcp や 23/tcp，3389/tcp 宛のパケットが数多く観測されており，様々なネットワークサービス

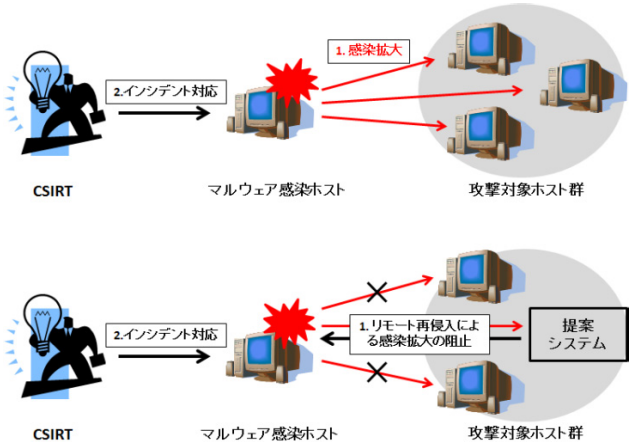

図 1 提案システムの基本アイディア
Fig. 1 The basic idea of proposal system.

が狙われている．特に近年では，Windows マシンだけでなく組み込みシステムを狙った攻撃が多く見られる．

企業や官公庁などといった組織の多くに，保護対象ネットワーク内で発生したセキュリティインシデントへの対応を行う CSIRT が存在する．CSIRT が行う具体的な対応としては，感染マシンのネットワークからの隔離といった ① インシデントの早期対応，マルウェアの駆除やシステムの修復といった ② インシデントハンドリング，システムのアップデートといった ③ 再発への防止，などである [27]．マルウェアへの対策が万全であれば，マルウェアに感染することはないが，組織内にはセキュリティパッチが適用されていないマシンや，システムアップデートが困難な状況下にあるマシンも存在する．このため，すべての攻撃を未然に防ぐことは難しい．また，近年では組み込みシステムの登場によりネットワークの構造が複雑化しており，マルウェアに感染していることが判明した場合にも，実際にマシンを特定することが困難な場合や時間を要する場合がある．加えて，感染マシンを利用しているユーザが多数存在する場合には，従来のネットワークから隔離するという対策が行えない場合がある．そこで，本稿では保護対象ネットワーク内でマルウェアによる感染拡大活動が発生した場合に，マルウェア感染ホストにリモート再侵入による早期対応を行うことで，CSIRT が対応を行うまでの間にマルウェア感染が保護対象ネットワーク内で拡大するのを阻止するシステムを提案する．

一般に，ネットワークの管理者は保護対象マシン群に対するアクセス権限を持つ立場にあるが，運用上，実際にリモートアクセスできるとは限らない．このため，マルウェア感染ホストに対して脆弱性スキャンツールやリモート接続用のツールなどを用いてリモート再侵入し，侵入に用いたサービスの停止や感染拡大を行っているプロセスの停止，通信の制限を行うことでマルウェアによる感染が拡大するのを阻止する手法を提案する．提案手法は，保護対象ホストに専用の監視ツールをインストールすることなく，リモートからマルウェア感染の拡大を阻止できる点で有用である．一方，マルウェアの中には自らが侵入する際に悪用した脆弱性を感染後に修正することで他のマルウェアによる侵入を防ぐものも存在する．しかし，4 章の検証実験に用いた実マルウェア検体の多くはリモート再侵入可能であった．これらの中には，組み込みシステムを狙ったマルウェアも含まれており，提案手法は Windows マシンだけでなく組み込みシステムに対しても有効に働く点が特徴的である．

3.2 マルウェア感染ホストへのリモート再侵入により感染拡大を阻止するシステム

本節では，3.1 節で説明した基本アイディアの実現形態であるマルウェア感染ホストへのリモート再侵入により感染拡大を阻止するシステムについて説明する．まずはじめに，**図 2** に本システムの構成を示す．本システムは，マルウェア感染ホストによる感染拡大活動を観測する**攻撃観測部**，観測された攻撃を分析することで攻撃元ホストがマルウェア感染時に悪用された脆弱性の特定を行う**脆弱性分析部**，攻撃元ホストに対してリモート再侵入を行い感染の拡大を阻止する**リモート再侵入部**の 3 つから構成され，本システムを保護対象ネットワーク内に設置することで，保護対象ネットワーク内で発生したインシデントによる被害が広がるのを防ぐことを目指す．以降では，本システムの構成要素について説明する．

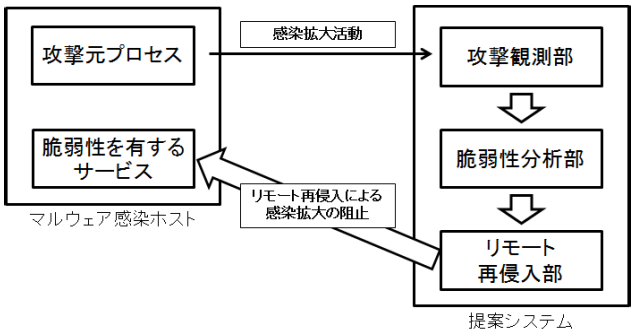

図 2 提案システムの構成
Fig. 2 Structure of proposal system.

攻撃観測部：保護対象ネットワーク内で発生したリモートエクスプロイト攻撃やパスワードクラッキング攻撃などのマルウェアの感染拡大活動を観測する．観測には，ハニーポットなどの既存技術を用いる場合や，モニタリングツールなどで収集したトラヒックデータを入力する場合が想定される．複数の IP アドレスを監視することで攻撃を観測できる可能性が高くなる．

脆弱性分析部：攻撃観測部で観測したデータをもとに，攻撃観測部へ攻撃を行ってきたホストがマルウェア感染した際に悪用された脆弱性の特定を行う．脆弱性の特定には，ハニーポットのログの分析や，IDS・IPS などのパケット分析ツールを用いる．

リモート再侵入部：脆弱性分析部で特定した脆弱性に対してリモート再侵入を行う．リモート再侵入が成功した場合には，脆弱性を有するサービスの停止・更新，通信の制限，マルウェアの活動の停止・駆除を行う．リモート再侵入には脆弱性スキャンツールやリモート接続ツールを用いる．

4 章の検証実験では，提案システムを実装した動的解析環境内でマルウェア検体を実行することで，リモート再侵入の可否を検証した．**図 3** に実験に用いたシステムの全体像を示す．実験には，実際に保護対象ネットワーク内で発生したマルウェア感染を再現するため，第 1，第 2 の犠牲ホストを用意した．第 1 犠牲ホスト上でマルウェア検体を実行し，攻撃対象ホストの探索を目的とするスキャン活動が開始されることを確認する．そして，発生したスキャン

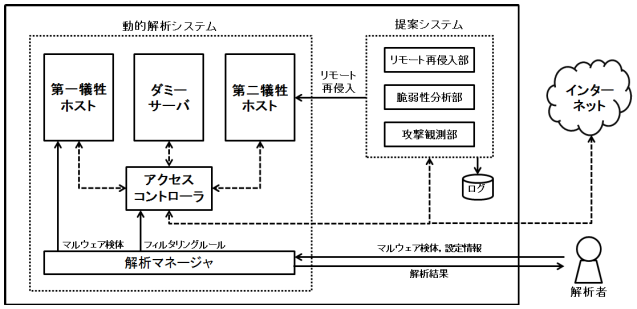

図 3 マルウェア感染ホストへのリモート再侵入により感染拡大を阻止するシステム

Fig. 3 Malware infection expansion interception system focused on remote takeover against malware-infected hosts.

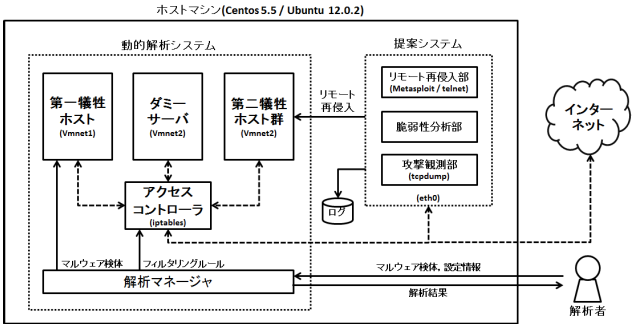

図 4 マルウェア感染ホストへのリモート再侵入により感染拡大を阻止するシステムの実装

Fig. 4 Implementation of Malware infection expansion interception system focused on remote takeover against malware-infected hosts.

を第 2 犠牲ホストに転送することで，マルウェアに脆弱性を悪用された状態で第 2 犠牲ホストをマルウェアに感染させる．最後に，第 2 犠牲ホストから感染拡大活動が開始されることを確認し，第 2 犠牲ホストにリモート再侵入を試みることで，マルウェア感染ホストへのリモート再侵入の可能性について検証する．以降では，システムの構成要素について説明する．

第 1 犠牲ホスト：第 1 犠牲ホストはマルウェア検体を実行し，実行後に発生するリモートエクスプロイト攻撃やパスワードクラッキング攻撃によって第 2 犠牲ホストを感染させるためのホストである．

アクセスコントローラ：アクセスコントローラは，第 1，第 2 犠牲ホスト上でマルウェアが行う通信を制御する役割を持つ．事前に設定されたフィルタリングルールに従い，マルウェアが行う通信のうち，危険性が十分に低いと判断された通信のみ実インターネットへと転送し，攻撃と思われる通信についてはダミーサーバへ転送する．ただし，第 1 犠牲ホストから発生したリモートエクスプロイト攻撃やパスワードクラッキング攻撃については，宛先 IP アドレスを変換して第 2 犠牲ホストに転送する．同様に，これらのパケットへの第 2 犠牲ホストからの応答についても，宛先 IP アドレスを変換して第 1 犠牲ホストに転送する．また，第 2 犠牲ホストから発生した感染拡大活動についても，同様に攻撃観測部に転送する．なお，アクセスコントローラのフィルタリングルールの詳細設定については，当該検体の動的解析を複数回行い，前述の例に加え，通信量や宛先 IP アドレスの決定方法など複数の基準に基づき危険性の判定を行う，文献 [10] の手法を用いる．

ダミーサーバ：ダミーサーバは，実インターネット上に存在する攻撃者が用意したサーバを模擬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．マルウェアの中には C&C サーバやダウンロードサーバと通信を行い，通信内容に応じてその後の挙動が変わるものが存在する．しかし，動的解析時に攻撃者がインターネット上に用意したサーバが活動しているとは限らない．そこで，あらかじめマルウェア検体が攻撃者の用意したサーバと行う通信を収集し，サーバからの応答を蓄積したダミーサーバを構築することで，感染拡大活動を発生させる．ダミーサーバの構築については，文献 [14] の手法を用いる．

第 2 犠牲ホスト：第 2 犠牲ホストは，アクセスコントローラにより第 1 犠牲ホストから転送された感染拡大活動によってマルウェア感染し，リモート再侵入の可否を調査するためのホストである．

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，第 1 犠牲ホストと第 2 犠牲ホストの OS イメージの管理，第 1 犠牲ホスト上で実行するマルウェア検体の管理，マルウェアが行う通信を制御するアクセスコントローラの設定，マルウェアが行う通信のキャプチャ，ダミーサーバの管理を行う．

攻撃観測部：攻撃観測部は，アクセスコントローラにより第 2 犠牲ホストから発生した感染拡大活動を観測する．

脆弱性分析部：脆弱性分析部は，攻撃観測部で観測された第 2 犠牲ホストからの攻撃をもとに，第 1 犠牲ホストが第 2 犠牲ホストに侵入するのに用いたサービスやサービスが起動しているポート番号を特定する．

リモート再侵入部：リモート再侵入部は，攻撃元ホストに対して，脆弱性スキャンツールやリモート接続ツールを用いてリモート再侵入を試みる．リモート再侵入が成功した場合には，侵入に用いたサービスの停止やマルウェアの拡大活動の停止，通信の制限を第 2 犠牲ホスト内で行う．また，リモート再侵入の可否やリモート再侵入後の動作のログを作成する．

3.3 マルウェア感染ホストへのリモート再侵入により感染拡大を阻止するシステムの実装

本節では，3.2 節で紹介した提案システムの実装について説明する．**図 4** に本システムの全体像を示す．4 章の検証実験では，実験を効率的に行う理由からマシン A と

マシン B の 2 台の実マシン上に実装した．マシン A では Windows を狙うリモートエクスプロイト攻撃を行うマルウェアへのリモート再侵入の可否について，マシン B では組み込みシステムを狙うパスワードクラッキング攻撃を行うマルウェアへのリモート再侵入の可否について検証した．以降では，各構成要素の実装について説明する．

ホストマシン：ホストマシンには，マシン A には CentOS v5.5 を，マシン B には Ubuntu 12.0.2 を用いた．

第 1 犠牲ホスト：第 1 犠牲ホストは，マシン A では VMwareServer v1.0.1 のゲスト OS により，マシン B では VirtualBox のゲスト OS により実現した．今回の実験では，マシン A の第 1 犠牲ホストの OS に Windows XP Professional SP1 を，マシン B の第 1 犠牲ホストの OS に Ubuntu 12.0.2 を用いたが，OS イメージの差し替えと初期設定を行うことで容易に変更が可能である．解析マネージャにより第 1 犠牲ホストが起動されると，タスクスケジューラに登録したプログラムによりマルウェア検体を解析マネージャから SSH 経由でダウンロードし，実行する．また，第 1 犠牲ホストは VMware/VirtualBox の仮想ネットワーク Vmnet1 内に配置され，すべての通信はアクセスコントローラを介して行われる．

第 2 犠牲ホスト群：第 2 犠牲ホスト群も第 1 犠牲ホスト同様，VMware Server/VirtualBox のゲスト OS により実現した．第 2 犠牲ホストの OS は，マシン A では Windows 2000 Professional，Windows XP Professional SP1，SP2，SP3 であり，マシン B では Ubuntu 12.0.2 である．第 1 犠牲ホスト同様，容易に変更が可能である．また，第 2 犠牲ホスト群は VMware/VirtualBox の仮想ネットワーク Vmnet2 内に配置され，すべての通信はアクセスコントローラを介して行われる．マシン A の第 2 犠牲ホストは，ファイアウォールなどのセキュリティレベルを最弱に設定するとともに，FTP や SMTP などのサービスをあらかじめ起動しておいた．マシン B の第 2 犠牲ホストは，文献 [23] で用いられている Telnet を模擬したサービスをあらかじめ起動しておいた．本サービスは，どのようなユーザ名とパスワードの組でもログイン可能なサービスである．また，その他の機能については Linux のリモート接続ツール Telnet と同様である．

アクセスコントローラ：アクセスコントローラは Linux のパケットフィルタリングツールである iptables を用いた．第 1 犠牲ホストから外部ホストへの接続要求に対して，23/tcp，135/tcp，139/tcp，445/tcp，3389/tcp といった感染拡大活動の対象となるポートへの通信に対しては iptables の DNAT ターゲットを用いて第 2 犠牲ホスト群の各ホストへ転送する．DNAT ターゲットでは，転送先ホストの宛先 IP アドレスを複数指定することで，対象ポートの通信をセッションごとに異なる宛先 IP アドレスに転送するラウンドロビン機能を用いる．DNAT により宛先が第 2 犠牲ホストとなった通信については，iptables の PREROUTING チェインで ACCEPT ターゲットを用い，POSTROUTING チェインで MASQUERADE ターゲットを適用することで IP アドレスの NAT 変換を行う．また，第 2 犠牲ホストから発生する接続要求についても NAT 変換を行い，つねに第 1 犠牲ホストへ転送されるように設定する．一方，第 1 犠牲ホストから外部ホストへの接続要求については，53/udp に対しては実インターネットへの接続を許可し，それ以外の通信については REDIRECT ターゲットを用いてダミーサーバへ転送する．以上の流れで，第 1 犠牲ホストからリモートエクスプロイト攻撃やパスワードクラッキング攻撃に関する通信が第 2 犠牲ホスト群の各ホストへと転送されるように設定する．このとき，第 1 犠牲ホストのマルウェアからは実際のインターネット上のホストへ通信を行っているように見える．同様に，第 2 犠牲ホストはインターネット上に存在するホストから攻撃を受けているように見える．

ダミーサーバ：ダミーサーバについては Perl スクリプトにより実装した．実装には，あらかじめマルウェア検体が攻撃者の用意したサーバと行う通信を収集し，サーバからの応答を蓄積した．ダミーサーバは，マルウェアが C&C サーバへ通信しようとしている場合には攻撃命令を，ダウンロードサーバへ通信しようとしている場合にはマルウェア検体がダウンロードされる通信を応答する．ダミーサーバは第 2 犠牲ホストと同じネットワーク Vmnet2 内に配置され，すべての通信はアクセスコントローラを介して行われる．

解析マネージャ：解析マネージャについては Perl スクリプトにより実装した．解析マネージャは文献 [10] で示されている機能のほかに，第 2 犠牲ホスト群の OS イメージ管理や第 2 犠牲ホスト群の通信ログを取得する役割を持つ．

攻撃観測部：攻撃観測部は，攻撃の観測には Linux のパケットモニタリングツールである tcpdump を用いた．第 2 犠牲ホストから発生した感染拡大活動や，リモート再侵入部が第 2 犠牲ホストへリモート再侵入を行うときのトラヒックを収集する．攻撃観測部は第 2 犠牲ホストから攻撃を観測した場合に応答は返さない．

脆弱性分析部：脆弱性分析部については Perl スクリプトにより実装した．4 章の検証実験では，アクセスコントローラにより第 2 犠牲ホストから攻撃観測部へ転送されたパケットの宛先ポート番号を抽出し，当該ポート上で起動しているサービスへの攻撃により第 2 犠牲ホストはマルウェア感染したと判断する．脆弱性の判定には Snort [28] や Bro [29] などといったパケット分析ツール，Nmap [30] などのセキュリティ検査ツール，検疫ネットワーク [31] を用いることも可能である．

リモート再侵入部：リモート再侵入部については Perl スクリプトにより実装した．リモート再侵入部は，脆弱性分

析部で特定したポート番号に対して，マシン A の場合にはフリーの脆弱性スキャンツールである Metasploit Framework [32]（以降では，Metasploit と呼ぶこととする）を，マシン B の場合には Linux のリモート接続ツール Telnet を用いてリモート再侵入を試みる．Metasploit は，検査対象のマシンに対しスキャンしたい脆弱性と使用するペイロードの種類などを指定するだけで簡単に脆弱性を検査できるツールである．2011 年時点で登録されていた検査可能な脆弱性の種類は 765 種類であった（このうち，Windows 用は 603 種類）．また，権限奪取後の動作を指定するためのペイロードとして 228 種類登録されていた．なお，Metasploit に登録されている検査可能な脆弱性はその脆弱性の種類だけでなく，実際には「windows/smb/ms08_netapi」というように，どの OS の/どのサービスの/どの脆弱性を検査するのか，という形式で登録されている．ペイロードについても，検査可能な脆弱性同様，どの OS の/どのサービスで/どのような動作を行うのかという形式で登録されている．このため，本稿でもこの表記方法を用いる．脆弱性スキャンツールの代表的なものとしては Metasploit 以外に Nessus [33] や Penetrator [34] などがある．一方，リモート再侵入後の動作として，侵入に用いたサービスの停止，セキュリティパッチの適用，通信の制限，AV ベンダが公開しているマルウェア駆除ツール [35], [36], [37] の適用，電源を強制的に落とす，工場出荷状態に戻すなどの方法が考えられる．4 章の検証実験では，マシン A ではネットワーク関連の情報を表示する netstat コマンドを用いて侵入に用いたポート上で起動しているサービスや，リモートエクスプロイト攻撃の対象となるポートへ通信を試みているプロセスの ID を特定し，taskkill コマンドを用いてプロセスを停止する．一方，マシン B では iptables を用いて侵入に用いたポート上で起動しているサービスへの通信の遮断，外部へ感染拡大を試みている通信の遮断を行う．また，リモート再侵入の可否やリモート再侵入後の動作のログを作成する．

4. 検証実験

提案手法は，マルウェア感染ホストへのリモート再侵入により感染拡大を阻止する手法である．このため，まずはじめに，マルウェア感染したホストへのリモート再侵入の可否について検証する．次に，リモート再侵入によりマルウェアの感染拡大を阻止する手法について検証する．以降では，4.1 節で実験方法について説明し，4.2 節で実験結果について説明する．そして，4.3 節で考察を行う．

4.1 実験方法

事前実験：攻撃に悪用される脆弱性の調査

これまで多くの脆弱性が報告されており，そのたびにセキュリティパッチが公開されている．そこで，まずはじめに Web 上で公開されているマルウェアの解析レポートなどを参考に，マルウェアが悪用する脆弱性を調査した．続いて，第 2 犠牲ホスト群として用意した各ホストの脆弱性を Metasploit により調査した．**表 1** がその結果である．この結果から，第 2 犠牲ホストのうち Windows XP Professional SP1 から最も多くの脆弱性が検出された．また，すべての犠牲ホストにおいて「windows/smb/ms08_netapi」の脆弱性を突いた乗っ取りが成功した．この脆弱性は 445/tcp 番ポートで起動するネットワークサービスの脆弱性であり，マルウェアの多くも攻撃に利用する．このため，実験 1 では Metasploit のエクスプロイトの種類に「windows/smb/ms08_netapi」を，ペイロード部分には管理者権限で相手を乗っ取り，シェルを開いて操作することを可能にする「windows/shell/bind_tcp」を設定し，リモート再侵入の可否について検証した．一方，組み込みシステムを狙うマルウェアは，「root，admin，1234」などといった脆弱なパスワードが設定された機器を狙うものが多い．このため，実験 2 では第 2 犠牲ホスト上で文献 [23] で用いられている Telnet サーバをあらかじめ起動しておき，リモート再侵入の可否について検証した．

表 1 第 2 犠牲ホストの脆弱性検証結果
Table 1 Vulnerability-scan result using Metasploit against Vicitim 2.

脆弱性の種類	XP SP1	XP SP2	XP SP3	Win 2000
Windows Server サービスの脆弱性, ms08_067_netapi	成功	成功	成功	成功
Microsoft ASN.1ライブラリの脆弱性, ms04_007_killbill	成功	失敗	失敗	失敗
RPC インターフェイスの脆弱性, ms03_026_dcom	成功	失敗	失敗	成功
上記以外の ms03~ms11 の脆弱性，合計66種類	失敗	失敗	失敗	失敗

実験 1：リモートエクスプロイト攻撃により感染を拡大するマルウェアへのリモート再侵入の可否の検証

低対話型ハニーポット nepenthes [22] を用いて 2007 年 8 月から 2010 年 7 月の間に収集した 4952 検体のうち，事前にリモートエクスプロイト攻撃を行うことが確認された 870 検体のマルウェア（以降では，検体セット 1）に対してリモート再侵入の可否を検証した．本実験では，第 1 犠牲ホストから発生したリモートエクスプロイト攻撃により，第 2 犠牲ホストのうちいずれかのホストを感染させ，Metasploit を用いてリモート再侵入を試みた．このとき，管理者権限で相手を乗っ取り，シェルが開いた場合にリモート再侵入に成功したと判断した．動的解析時の設定項目を下記に示す．

続いて，リモート再侵入が成功した検体のうち Korgo Family 4 検体と Virut Family 3 検体，dionea [38] を用いて 2011 年 8 月 17 日に収集した Conficker Family 3 検体から

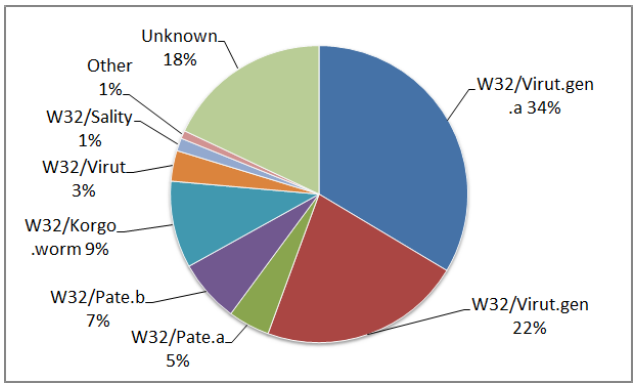

図 5 検体セット 1 の内訳

Fig. 5 Details of malware samples used for experiment 1 (sample set 1).

表 2 検体セット 2 の内訳

Table 2 Details of malware samples used for experiment 1 (sample set 2).

McAfee	MD5ハッシュ値
W32/Korgo.worm.p	0384096b85ed0f843f2fc0e1a3fb4f9e
W32/Korgo.worm.s	0179a81592d44942304d513dd12879bf
W32/Korgo.worm.i	0c803048e4e4342cb96e62ec9cf844b1
W32/Korgo.worm.q	6de05d4ef7330df83fd3e9998216917a
W32/Virut.gen	b011787882871d9140c12e46b8fb3f86
W32/Virut.gen	c30dae6c8f87d83cd646ead95625be40
W32/Virut.gen.a	c34ede5b1ad62675e2a86b7fae3f18e4
W32/Conficker.worm	38202f889d57f7a3dbbd1d55f503d466
W32/Conficker.worm.gen.a	3ce10bf31ff9145db3f887a3f9ad6652
W32/Conficker.worm.gen.b	6dbd5d68fddd42e4429870017abd7e97

なる検体セット（以降では，検体セット 2）を用いて，マルウェア感染したホストへのリモート再侵入の可否について検証した．また，リモート再侵入が成功した場合には，侵入に用いたサービスの停止や感染拡大を行っているプロセスの停止を試みた．動的解析環境の設定や，Metasploit の設定は同様である．なお，第 2 犠牲ホストの OS のイメージは Windows XP Professional SP1 のみとした．検体セット 1 の内訳を**図 5** に，検体セット 2 の内訳を**表 2** に示す．表の作成には，アンチウィルスソフトによる検知結果を提供するサービスである VirusTotal [39] から，McAfee による検知結果を用いている．

実験 1 における動的解析環境の設定

- 第 2 犠牲ホスト群へ転送するポート
  135/tcp，139/tcp，445/tcp，1025/tcp，5000/tcp
- インターネットへの接続を許可する通信
  Google の DNS サーバ（8.8.8.8，53/udp）への通信
- 検体実行時間
  検体セット 1：90 秒　検体セット 2：60 秒

実験 2：パスワードクラッキングにより感染を拡大するマルウェアへのリモート再侵入の可否の検証

組み込みシステムを狙うマルウェアの収集を目的とするハニーポット IoTPot [23] を用いて，2015 年 1 月から 9 月に収集した，Linux 上で動作する 30 検体のうち，事前に 23/tcp 番ポートでスキャンを行うことが確認された 18 検体のマルウェア（以降では，検体セット 3）に対してリモート再侵入の可否を検証した．本実験では，第 2 犠牲ホストに対して Telnet を用いてリモート再侵入を試み，リモート接続に成功した場合にリモート再侵入に成功したと判断した．

続いて，リモート侵入が成功した場合には，侵入に用いたサービスへの通信と第 2 犠牲ホストからの感染拡大を目的とする通信の制限を試みた．動的解析時の設定項目を下記に示す．また，検体セット 3 のうち，VirusTotal [39] に登録されているアンチウィルスソフトのいずれにおいても検知されなかった検体が多かった（2015 年 11 月 30 日に検査）．検体セット 3 の内訳を**表 3** に示す．

表 3 検体セット 3 の内訳

Table 3 Details of malware samples used for experiment 2 (sample set 3).

23c6d202f0777c772cf792d90fc7d68e	7df780f115cecd3219e7b0a55239abd4
267d57370e7e0eea242dfcd22b0aede9	805b48b3b9a54cb94edd79701895567f
4a452491b0660b5ed3f54773bf66b4df	8c04e5b2bcf7b12eed8f3f3c5d900dd0
86f9fc4e914d358d05bd5d1d93a0d673	b2475f415edb7d22fdc057fef7ecd7dc
c1ef1dd4232e14c45661e0a8a976867e	b581c5b091957869e7242ec34579ccd7
f3c580d7684ac4fd8064cca8b8f741bc	ba3948687423c3f7b35b6f8f5211dae1
0e54692eed81cfc4435d52e2a60805e7	e04781bd52095450259e0f3a3f986460
116c976ee5d7bae0c30a35f7cdc4fcf0	fcc3292ffe2dc796573229b0d8d6d939
751ca60155c29ebc41998843fdcd4d5b	6d9f7123e8692087bdb2822e44854eef

実験 2 における動的解析環境の設定

- 第 2 犠牲ホストへ転送するポート
  23/tcp
- インターネットへの接続を許可する通信
  Google の DNS サーバ（8.8.8.8，53/udp）への通信
- 検体実行時間
  30 秒

4.2 実験結果

実験 1 の結果

検体セット 1 に対してリモート再侵入の可否を検証した結果，全 870 検体のうち 819 検体が第 1 犠牲ホストから第 2 犠牲ホスト群にリモートエクスプロイト攻撃を行い，そのうち，294 検体が第 2 犠牲ホスト群のいずれかのマシンに感染し，第 2 犠牲ホストがリモートエクスプロイト攻撃を開始した．リモートエクスプロイト攻撃の宛先となったポートは 445/tcp などであった．マルウェアに感染した第 2 犠牲ホストのうち，リモート再侵入が成功したケースは 181 検体であり，約 61%のマルウェア検体においてリモート再侵入が成功した．

リモート再侵入の結果（実験 1）

- 動的解析を行った検体：　870 検体
- リモートエクスプロイト攻撃を
  行った検体：　819 検体
- 第 2 犠牲ホストのいずれかのホストを

表 4 検体セット 2 へのリモート再侵入の結果と感染拡大阻止（実験 1）
Table 4 Remote Takeover and malware infection expansion interception result against malware sample set2 (experiment 1).

McAfee / Symantec MD5ハッシュ値	リモート再侵入の対象ポート	リモート再侵入の可否	再侵入に用いたサービスの停止	感染拡大を行っているプロセスの停止
W32/Korgo.worm.p / W32.Virut.B 0384096b85ed0f843f2fc0e1a3fb4f9e	445/tcp	成功	成功	成功
W32/Korgo.worm.s / W32.Korgo.S 0179a81592d44942304d513dd12879bf	445/tcp	成功	成功	成功
W32/Korgo.worm.i / W32.Korgo.I 0c803048e4e4342cb96e62ec9cf844b1	445/tcp	成功	成功	成功
W32/Korgo.worm.q / W32.Korgo.Q 6de05d4ef7330df83fd3e9998216917a	445/tcp	成功	成功	成功
W32/Virut.gen / W32.Virut.H b011787882871d9140c12e46b8fb3f86	445/tcp	成功	成功	成功
W32/Virut.gen / W32.Virut.U c30dae6c8f87d83cd646ead95625be40	445/tcp	成功	成功	成功
W32/Virut.gen.a / W32.Virut.B c34ede5b1ad62675e2a86b7fae3f18e4	445/tcp	成功	成功	成功
W32/Conficker.worm.gen.a/W32.Downadup.B 3ce10bf31ff9145db3f887a3f9ad6652	445/tcp	失敗	–	–
W32/Conficker.worm.gen.b/W32.Downadup.B 6dbd5d68fddd42e4429870017abd7e97	445/tcp	失敗	–	–
W32/Conficker.worm / W32.Downadup.B 38202f889d57f7a3dbbd1d55f503d466	445/tcp	失敗	–	–

表 5 検体セット 3 のうち第 2 犠牲ホストを感染させることができたマルウェアへのリモート再侵入の結果と感染拡大阻止（実験 2）
Table 5 Remote Takeover and malware infection expansion interception result against malware sample which were successful to infect victim2 from malware sample set3 (experiment 2).

MD5ハッシュ値	リモート再侵入の対象ポート	リモート再侵入の可否	再侵入に用いたサービスへの通信の制限	感染拡大を行うプロセスの通信の制限
23c6d202f0777c772cf792d90fc7d68e	23/tcp	成功	成功	成功
267d57370e7e0eea242dfcd22b0aede9	23/tcp	成功	成功	成功
4a452491b0660b5ed3f54773bf66b4df	23/tcp	成功	成功	成功
8c04e5b2bcf7b12eed8f3f3c5d900dd0	23/tcp	成功	成功	成功
b581c5b091957869e7242ec34579ccd7	23/tcp	成功	成功	成功
ba3948687423c3f7b35b6f8f5211dae1	23/tcp	成功	成功	成功
e04781bd52095450259e0f3a3f986460	23/tcp	成功	成功	成功

感染させることができた検体： 294 検体
- リモート再侵入が成功した検体： 181 検体
- リモート再侵入が失敗した検体： 27 検体
- リモート再侵入の可否を検証できなかった検体： 86 検体

続いて，検体セット 2 に対してリモート再侵入の可否を検証した．**表 4** にその結果をまとめる．実験の結果，Korgo や Virut として検知される 7 検体については，いずれもリモート再侵入が成功した．一方，Conficker として検知される 3 検体についてはリモート再侵入が失敗した．実験環境はインターネット接続を許可していないため，Conficker は内部に修正プログラムを保持しており，感染後に脆弱性を修正することが分かった．

実験 2 の結果

検体セット 3 に対してリモート再侵入の可否を検証した．**表 5** にその結果をまとめる．全 18 検体のうち 7 検体が第 2 犠牲ホストに感染し，第 2 犠牲ホストが 23/tcp 番ポートでスキャンを開始した．また，スキャンの宛先となったポートは 23/tcp のみであった．マルウェア感染した第 2 犠牲ホストのうち，リモート再侵入が成功したケースは 7

検体であった．

リモート再侵入の結果（実験 2）

- 動的解析を行った検体： 18 検体
- 23/tcp 番ポートへのスキャンを行った検体： 18 検体
- 第 2 犠牲ホストを感染させることができた検体： 7 検体
- リモート再侵入が成功した検体： 7 検体

リモート再侵入が成功したマルウェア検体（Md5 hash：23c6d202f0777c772cf792d90fc7d68e，VirusTotal による検出率 0）は，C&C サーバと 7632/tcp 番ポート通信を試み，「!* SCANNER ON」という攻撃命令を受信することで 23/tcp 番ポートへのスキャンを開始した．当該検体のスキャンを第 2 犠牲ホストに転送したところ，第 2 犠牲ホストもマルウェアに感染した．第 2 犠牲ホストが感染した検体（Md5hash: 57fc1c955e2658eee4a6c03d260e905b，VirusTotal による検出率 0）は，第 1 犠牲ホスト上で実行した検体とは異なる検体であったが，しばらくすると第 2 犠牲ホストからダウンロードサーバへ新たな検体をダウンロードする通信が発生し，第 1 犠牲ホストで実行した検体と同じ検体に感染した．そして，第 2 犠牲ホストに対して Telnet を用いて再侵入を試みたところ，リモート再侵入に成功した．一方，検体セット 3 の中には，第 2 犠牲ホストを感染させることには失敗したが，侵入に用いたポートへの通信を制限しようとするものが存在した．マルウェア検体（Md5 hash：86f9fc4e914d358d05bd5d1d93a0d673，VirusTotal による検出率 0）は，C&C サーバと 1981/tcp 番ポート通信を試み，「!* SCANNER ON」という攻撃命令を受信することで 23/tcp 番ポートへのスキャンを開始した．当該検体のスキャンを第 2 犠牲ホストに転送したが，第 2 犠牲ホストをマルウェアに感染させることはできなかった．しかし，新たなマルウェア検体のダウンロードを試みるとともに，iptables を用いて第 2 犠牲ホストの 23/tcp 番ポートへの接続要求を遮断するように設定の変更を試みていた．このように，本実験に用いた組み込みシステムを狙うマルウェアの中には，スキャンを行う検体のほかに，23/tcp 番ポートへの通信を制御する検体をダウンロードするものが存在した．

4.3 考察

実験 1 では，第 2 犠牲ホストへ感染拡大活動を転送しているにもかかわらずマルウェア感染させることができなかった検体が存在した．このような結果になった理由として，以下のことが考えられる．

パケットルーティングの問題

今回の実装では iptables による第 2 犠牲ホストへのパケット転送では複数のポート間での関連性は考慮されないため，本来同一ホストの異なるポートに届くはずの通信が，異なるホストに届いてしまい，攻撃が適切に観測できなくなる可能性がある．たとえば，リモートエクスプロイト攻撃によって開いたバックドアへの接続が，実際にバックドアが開いているホストとは異なるホストに転送されている可能性がある．これらの問題の解決のためにはアクセスコントローラを改良する必要がある．

第 2 犠牲ホストで動作しているサービスの問題

今回の実装では第 2 犠牲ホスト上で事前にいくつかのサービスを起動した状態で実験を行った．しかし，マルウェアの中には特定のサービスが起動しているホストに対してのみ攻撃を行うものが存在する．たとえば，morto [40] と呼ばれるマルウェアは 3389/tcp 番ポートで起動しているリモート接続サービス（Remote Desktop Protocol）を攻撃することが知られている．また，組み込みシステムを狙うマルウェアの中には，第 2 犠牲ホスト上で起動している Telnet サービスへログインに成功するが，Telnet サービスがマルウェアから送られたコマンドを認識できず，通信が終了してしまう場合があった．これらの問題の解決のためにはマルウェアが行う攻撃についてさらに詳しく分析する必要がある．

第 2 犠牲ホストの OS の種類の問題

今回の実装では第 2 犠牲ホストに Windows XP Professional SP1，SP2，SP3，Windows 2000 Professional，Ubuntu12.0.2 を使用したが，これだけではホストの種類が十分であるとはいえない．特に組み込みシステムを狙うマルウェアの中には，特定のアーキテクチャでしか動作しないものも存在した．また，マルウェアの中には特定の言語版の OS に対してのみ感染拡大活動を行う場合や第 2 犠牲ホスト群の設定に応じて攻撃の成否が依存する場合もある．これらの問題の解決のためには第 2 犠牲ホスト群を改良する必要がある．

検証実験で使用した検体の中には第 2 犠牲ホストをマルウェア感染させたにもかかわらず，リモート再侵入が失敗したケースが存在した．このような結果になった理由として，以下のことが考えられる．

Metasploit/Telnet によるリモート再侵入が成功しない場合

リモート再侵入が成功しない検体については，感染後にマルウェアが脆弱性を修正した可能性などが考えられる．また，今回の実験では調査を行っていないが，パスワードクラッキングにより侵入したサービスのパスワードを変更するマルウェアが存在する可能性がある．このようなマルウェアについてはさらなる調査が必要である．

感染後に脆弱性を修正するマルウェア

検体セット 2 の Conficker は「MS08-067」の脆弱性を利用して感染を拡大させることが知られている．今回の検証実験により，Conficker は感染後に「MS08-067」の脆弱性を修正することが分かった．ただし，Conficker は「MS08-067」

以外の脆弱性は修正しないため，「MS03-026，MS04-007」による再侵入は可能であることが分かった．同様に，組み込みシステムを狙うマルウェアの中には感染後に iptables を用いて 23/tcp 番ポートへの通信を制限するものが存在することが分かった．

最後に，リモート再浸入による感染拡大の阻止が失敗する場合や，リモート再侵入を悪用した新たな感染活動の脅威について考察する．

リモート再浸入による感染拡大阻止が失敗する場合

今回の検証実験では，リモート再侵入後に侵入に用いたサービスや感染拡大を行っているプロセスの特定・停止に成功したが，マルウェアの中には悪性プロセスを通常のプロセス管理コマンドで見えないようにする（ルートキットなど）場合がある．また，正規プロセスを乗っ取ることで不正活動を行うマルウェア（dll インジェクション）の場合，プロセスの停止を行うことは難しい．加えて，プロセスの停止に成功した場合にも，その後，プロセスが再起動する可能性がある．4 章の検証実験においても，脆弱性を有するサービスを停止した後，しばらくすると再起動される挙動が見られた．このため，実際には定期的な検査や通信の制限などと組み合わせることが望ましい．

リモート再侵入を悪用した新たな感染活動

今回の検証実験により，リモートエクスプロイト攻撃やパスワードクラッキング攻撃によりマルウェア感染したホストの多くは，感染中もさらなるリモート侵入を受ける可能性があることが分かった．攻撃者はこのことを利用し，以下のように効率的に自らの制御下のマシンを増やすことが考えられる．感染拡大活動を行うマルウェアのほとんどは攻撃対象ホストを探索するために広範囲のスキャンを行う．スキャン先の IP アドレスは無作為に選ばれることが多いため，攻撃者が管理するホストにも到達する可能性がある．特にボットネットなどの多数のホストを制御している攻撃者のもとには多くのスキャンが届くものと思われる．このため，攻撃者はスキャンの送信元に対してリモート再侵入を行うことで，そのホストの制御を奪取できる可能性がある．近年は OS のセキュリティが向上し，リモートエクスプロイト攻撃が可能なホストの割合は減少していると思われるが，これらのスキャン元ホストはすでに何らかのマルウェアに侵入されていることから，セキュリティパッチが適用されていないシステムである可能性が高い．また，組み込みシステムについてはユーザが感染していることに気付いていない場合も多く，今後も脆弱性が修正されない可能性がある．リモート再侵入による感染は，スキャンなどの探索活動を必要としないため，ダークネット観測による広域モニタリングシステムに捕捉されずに感染活動を行うことができる．加えて，インターネット上には SQL Slammer などの古いワームに感染したホストが多数存在するため，攻撃者は効率的に自らの勢力を拡大することができる．このように古い脆弱性を有する感染ホストは多くないかもしれないが，今後新たな脆弱性が発生した際には世界中に依然として蔓延している感染ホストはすべて再侵入の対象となる．

5. まとめと今後の課題

マルウェアに感染したホストへのリモート再侵入の可否を，実マルウェア検体を用いた動的解析により調査した．また，マルウェアに感染したホストへのリモート再侵入により感染拡大を阻止する手法を提案した．検証実験の結果，リモートエクスプロイト攻撃によりマルウェア感染したホストの多くは，感染中もさらなる侵入を受ける可能性があることが分かった．また，組み込みシステムを狙ったマルウェアについても同様に，感染中もさらなる侵入を受けるが可能があることが分かった．一方，こうしたマルウェアに感染したホストに対してリモート再侵入を行い，侵入に用いたサービスの停止や感染拡大活動を行っているプロセスの停止，通信の制限を行うことで，マルウェアの感染拡大を阻止することができることが分かった．今後の課題は，より多くのマルウェア検体で実験を行うとともに，その他のプロトコルについても調査を行うことである．

謝辞 本研究の一部は，文部科学省国立大学改革強化推進事業の支援を受けて行われた．A part of this work was conducted under the auspices of the MEXT Program for Promoting the Reform of National Universities.

参考文献

[1] Travis, G., Balas, E., Ripley, D.A.J. and Wallace, S.: Analysis of the “SQL Slammer” worm and its effects on Indiana University and related institutions (2003).
[2] Symantec W32.Downadup, available from ⟨http://www.symantec.com/ja/jp/security_response/writeup.jsp?docid=2008-112203-2408-99⟩ (accessed 2015/06/30).
[3] 笠間貴弘，島村隼平，井上大介：マルチモーダル分析による組込みシステムからの攻撃活動状況の把握，情報処理学会コンピュータセキュリティシンポジウム 2014（CSS2014），2A1-4 (2014).
[4] Celeda, P., Krejci, R., Vykopal, J. and Drasar, M.: Embedded Malware – An Analysis of the Chuck Norris Botnet, *Proc. 2010 European Conference on Computer Network Defense*, pp.3–10 (October 2010).
[5] Chuck Norris botnet karate-chops routers hard - Good Gear Guide by PC World Australia, available from ⟨http://www.pcworld.idg.com.au/article/336938/chuck_norris_botnet_karate-chops_routers_hard/⟩ (accessed 2015/06/30).
[6] SANS ISC Linksys Worm “TheMoon” Summary: What we know so far, available from ⟨https://isc.sans.edu/forums/diary/Linksys+Worm+TheMoon+Summary+What+we+know+so+far/17633⟩ (accessed 2015/06/30).
[7] Dissecting Linux/Moose, available from ⟨http://www.welivesecurity.com/wp-content/uploads/2015/05/Dissecting-LinuxMoose.pdf⟩ (accessed 2015/06/30).
[8] Symantec Blogs, Is there an Internet-of-Things vigilante

out there?, available from ⟨http://www.symantec.com/connect/blogs/there-internet-things-vigilante-out-there⟩ (accessed 2015/11/30).
[9] Yoshioka, K., Kasama, T. and Matsumoto, T.: Sandbox Analysis with Controlled Internet Connection for Observing Temporal Changes of Malware Behavior, *Proc. 4th Joint Workshop on Information Security, JWIS 2009*, 3a-2 (2009).
[10] Yoshioka, K. and Matsumoto, T.: Multi-pass Malware Sandbox Analysis with Controlled Internet Connection, *IEICE Trans.*, Vol.E93-A, No.1, pp.210–218 (2010).
[11] 青木一史，川古谷裕平，岩村 誠，伊藤光恭：半透性仮想インターネットによるマルウェアの動的解析，コンピュータセキュリティシンポジウム論文集，pp.1–6 (2009).
[12] Yoshioka, K., Inoue, D., Eto, M., Hoshizawa, Y., Nogawa, H. and Nakao, K.: Malware Sandbox Analysis for Secure Observation of Vulnerability Exploitation, *IEICE Trans.*, Vol.E92D, No.5, pp.955–966 (2009).
[13] 村上洸介，藤井孝好，吉岡克成，松本 勉：リモートエクスプロイト攻撃を効率的に観測可能なマルウェア動的解析手法の提案，情報処理学会コンピュータセキュリティシンポジウム 2011（CSS2011），3B3-3 (2011).
[14] 笠間貴弘，吉岡克成，松本 勉，山形昌也，衛藤将史，中尾康二：疑似クライアントを用いたサーバ応答蓄積型マルウェア動的解析システム，情報処理学会コンピュータセキュリティシンポジウム 2009（MWS2009），A7-2 (2009).
[15] Zaddach, J., Bruno, L., Francillon, A. and Balzarotti, D.: Avatar: A Framework to Support Dynamic Security Analysis of Embedded Systems' Firmwares, *Network and Distributed System Security Symposium* (Feb. 2014).
[16] 田辺瑠偉，筒見拓也，小出 駿，牧田大佑，吉岡克成，松本 勉：Linux 上で動作するマルウェアを安全に観測可能なマルウェア動的解析手法の提案，情報処理学会コンピュータセキュリティシンポジウム 2015（CSS2014），3B2-4 (2014).
[17] Nakao, K., Yoshioka, K., Inoue, D., Eto, M. and Rikitake, K.: nicter: An Incident Analysis System using Correlation between Network Monitoring and Malware Analysis, *Proc. 1st Joint Workshop on Information Security* (June 2006).
[18] nicterWeb, available from ⟨http://www.nicter.jp/nw_public/scripts/index.php#nicter⟩ (accessed 2015/11/27).
[19] 中里純二，大高一弘：nicter レポート—長期ネットワーク観測に基づく攻撃の変遷に関する分析，独立行政法人情報通信研究機構季報，Vol.57, No.3/4 (2011).
[20] 小出 駿，鈴木将吾，牧田大佑，村上洸介，笠間貴弘，島村隼平，衛藤将史，井上大介，吉岡克成，松本 勉：通信プロトコルのヘッダの特徴に基づく不正通信の検知・分類手法，情報処理学会コンピュータセキュリティシンポジウム（CSS）(2014).
[21] 神保千晶，藤井孝好，村上洸介，吉岡克成，四方順司，松本勉，衛藤将史，井上大介，中尾康二：ハニーポット・トラフィック分析によるゼロデイ・リモート・エクスプロイト攻撃検出，電子情報通信学会暗号と情報セキュリティシンポジウム 2012（SCIS2012），2E2-3 (2012).
[22] Baecher, P., Koetter, M., Holz, T., Dornseif, M. and Freiling, F.C.: The Nepenthes Platform: An Efficient Approach to Collect Malware, *Proc. 9th International Symposium on Recent Advances in Intrusion Detection* (*RAID 2006*), pp.165–184 (2006).
[23] Pa, Y.M.P., Suzuki, S., Yoshioka, K., Matsumoto, T., Kasama, T. and Rossow, C.: IoTPOT: Analysing the Rise of IoT Compromises, *Proc. 9th USENIX Workshop on Offensive Technologies, ser, WOOT* (2015).
[24] SHODAN — Computer Search Engine, available from ⟨https://www.Shodan.io/⟩ (accessed 2015/06/30).
[25] Durumeric, Z., Bailey, M. and Halderman, J.: An Internet-Wide View of Internet-Wide Scanning, *Proc. 23rd USENIX Security Symposium 2014*, pp.65–78 (2014).
[26] 田辺瑠偉，村上洸介，吉岡克成，四方順司，松本 勉：マルウェア感染ホストへのリモート侵入の可能性，電子情報通信学会暗号と情報セキュリティシンポジウム 2012（SCIS2012），1E1-3 (2012).
[27] Symantec, Incident Response, available from ⟨https://www.symantec.com/ja/jp/page.jsp?id=incident-response⟩ (accessed 2015/11/30).
[28] Snort, available from ⟨https://www.snort.org/⟩ (accessed 2015/12/03).
[29] Bro, available from ⟨https://www.bro.org/⟩ (accessed 2015/12/03).
[30] Nmap, available from ⟨http://nmap.org/5/⟩ (accessed 2015/06/30).
[31] @iIT，特集：検疫ネットワークとは（前編），入手先 ⟨http://www.atmarkit.co.jp/ait/articles/0502/18/news128.html⟩（参照 2015/11/30）.
[32] Metasploit Frame work, available from ⟨http://metasploit.com/⟩ (accessed 2015/06/30).
[33] Penetrator, available from ⟨http://penetrator.blue.co.jp/⟩ (accessed 2015/06/30).
[34] Nessus, available from ⟨http://www.nessus.org/products/nessus⟩ (accessed 2015/06/30).
[35] SOPHOS, Virus Removal Tool, available from ⟨https://www.sophos.com/ja-jp/products/free-tools/virus-removal-tool.aspx⟩ (accessed 2015/11/30).
[36] Symantec, Symantec Power Eraser, available from ⟨http://www.symantec.com/ja/jp/security_response/malware.jsp⟩ (accessed 2015/11/30).
[37] Kaspersky，テクニカルサポート，入手先 ⟨http://support.kaspersky.co.jp/viruses⟩（参照 2015/11/30）.
[38] The Honeynet Project, Dionaea catches bugs, available from ⟨https://www.honeynet.org/project/Dionaea⟩ (accessed 2016/03/16).
[39] VirusTotal, available from ⟨https://www.virustotal.com/⟩ (accessed 2015/12/03).
[40] Symantec W32.Morto, available from ⟨http://www.symantec.com/ja/jp/security_response/writeup.jsp?docid=2011-082908-4116-99⟩ (accessed 2015/06/30).

田辺 瑠偉 （学生会員）

2012 年 3 月横浜国立大学工学部電子情報工学科卒業．学士（工学）．2014 年 3 月横浜国立大学大学院環境情報学府情報メディア環境学専攻博士課程前期修了．修士（情報学）．同年 4 月横浜国立大学大学院環境情報学府情報メディア環境学専攻博士課程後期に進学．情報セキュリティ，特にネットワークセキュリティの研究に従事．

鈴木 将吾

2016 年 3 月横浜国立大学大学院環境情報学府情報メディア環境学専攻博士課程前期修了．修士（工学）．同年 4 月 PwC サイバーサービス合同会社入社．在学中，ネットワーク攻撃観測等のネットワークセキュリティの研究に従事．

イン ミン パ パ

2006 年マンダレー工科大学（ミャンマー）卒業．学士（情報技術）．2013 年横浜国立大学国際社会科学研究科インフラストラクチャマネジメント学専攻修士課程修了．修士（学術）．2016 年 3 月横浜国立大学大学院環境情報学府情報メディア環境学専攻博士課程後期修了．博士（工学）．同年 4 月 PwC サイバーサービス合同会社入社．在学中，ネットワーク攻撃観測・分析等のネットワークセキュリティの研究に従事．

吉岡 克成 （正会員）

2005 年 3 月横浜国立大学大学院環境情報学府情報メディア環境学専攻博士課程後期修了．博士（工学）．同年 4 月独立行政法人情報通信研究機構で研究員として勤務．2007 年 12 月より横浜国立大学学際プロジェクト研究センター特任教員（助教）．2011 年 4 月横浜国立大学大学院環境情報研究員准教授．マルウェア解析やネットワーク攻撃観測・検知等のネットワークセキュリティの研究に従事．2009 年文部科学大臣表彰・科学技術賞（研究部門）受賞．

松本 勉 （正会員）

1986 年 3 月東京大学大学院工学系研究科電子工学専攻博士課程修了，工学博士．同年 4 月横浜国立大学講師．2001 年 4 月より同大学院環境情報研究員教授．2014 年 12 月より同大学先端科学高等研究員（IAS-YNU）情報物理セキュリティ研究ユニットリーダーを兼務．ネットワーク・ソフトウェア・ハードウェアセキュリティ，暗号，耐タンパー技術，生体認証，人工物メトリクス等の「情報・物理セキュリティ」の研究教育に 1981 年より従事．1982 年にオープンな学術的暗号研究を目指した「明るい暗号研究会」を 4 名で創設．2005～2010 年国際暗号学会 IACR 理事．1994 年第 32 回電子情報通信学会業績賞，2006 年第 5 回ドコモ・モバイル・サイエンス賞，2008 年第 4 回情報セキュリティ文化賞，2010 年文部科学大臣表彰・科学技術賞（研究部門）各受賞．