4　仮想化技術の応用
4 Applied Virtualization Technology

4-1　マルウェア隔離実験環境の設計と実装
4-1 Design and Implementation of an Isolated Sandbox used to Analyze Malware

三輪信介　　門林雄基　　篠田陽一
MIWA Shinsuke, KADOBAYASHI Youki, and SHINODA Yoichi

要旨

ウィルス・ワーム・ボットなどのマルウェアの技術は日々進歩しており、その対策のためには、動作の検証・解析を行う必要がある。マルウェアの動作の検証・解析を行うためには、外部への感染や攻撃を避けるために隔離環境を用いることが必須である。

そこで、本稿では、隔離の度合いについて定義した上で、我々がこれまで研究開発してきた隔離実験環境を評価した上で、より多様なマルウェアの隔離実験を可能とするマルウェア隔離実験環境の設計と実装について述べる。

Recent viruses, worms, and bots, called malware, have to be analyzed their behaviors for drawing out countermeasures against them. To avoid any impacts to/from the Internet, analyzing environments should be isolated from the Internet.

In this paper, we defined the levels of containing malwares, also estimated our developed isolated sandboxes according to definition of the levels. Furthermore, we propose new isolated sandbox, which designed according to the estimation.

[キーワード]
マルウェア，動態解析，隔離，封じ込め
Malware, Live analysis, Isolation, Containment

1　はじめに

ウィルス・ワーム・ボットなどのマルウェア[1]は日々進化を続けている。これらに対抗するためには、その動作の仕組みを解析し、問題を明らかにする必要がある。このような解析を行うためには、解析環境の外部への感染や攻撃による影響を避ける目的で隔離環境を用いることが有効である。

我々は、実ノードの切替えや再生により仮想化技術と同程度の利便性を確保する方式や擬似インターネットによりマルウェアを騙し、隔離環境で解析されていることに気づかせない方式などの研究開発[2]を行ってきた。本稿では、隔離の度合いについて定義した上で、隔離へのマルウェア側の回避手法とその対抗方法を整理し、より多様なマルウェアの隔離実験を可能とするマルウェア隔離実験環境の設計と実装について述べる。

2　背景

まず、背景としてマルウェアの解析手法と隔離の必要性について述べる。マルウェアの解析を行う方法としては、大きく分けて二つの方法がある。

マルウェアの実行実体を実行することなく、そのプログラムコードから動作の仕組みを解析する静的解析と、マルウェアの実行実体を実行し、その動作を観測することで解析する動態解析である。

マルウェアの影響を知ることができれば、対策を策定し、実施することが可能となる。また、多くのマルウェア対策技術は、マルウェアが動作したときの通信内容やファイルへのアクセス履歴などの足跡から、マルウェアの検知と対応を行うため、マルウェアの動作による影響を知ることができれば、新種のマルウェアにも対応可能となる。そのため、マルウェアの解析として、動作による影響を計るため、動態解析が広く用いられている。

動態解析では、何らかの実行手段で、かつ、何らかの解析環境上で、マルウェアの実行実体を実際に実行し、その動作による作用を観測する必要がある。よって、マルウェアが実際に感染や攻撃などの活動を試みるため、解析環境が外部に接続されている場合には、感染が広がるなど、その影響が外部に及ぶため、何らかの対策が必要となる。

また、実際のインターネット上には、非常に多くのマルウェアが蔓延[3]しており、解析環境がインターネットに直接接続されている場合には、解析対象のマルウェア以外のマルウェアの影響を受けるおそれがある。そのため、外部からの影響を排除するための何らかの対策が必要となる。

このような外部への影響や外部からの影響を排除するために、物理的もしくはネットワーク的に何らかの障壁を設けて、マルウェアの実行環境を外部と分離することを、本稿では「隔離」と定義する。また、マルウェアの動態解析やその他の実験を行う環境を「実験環境」と呼ぶこととする。

3 隔離

前述のとおり、マルウェアの動態解析を行う場合には、実験環境には何らかの隔離が必要である。そこで本章では、隔離の対象となるマルウェアの活動や外部からの影響と隔離の手法、隔離の問題点などを整理する。

3.1 隔離の対象

隔離には「マルウェア活動の実験環境への封じ込め」と「外部から実験環境への影響の排除」の二つの側面がある。また、マルウェア活動や外部からの影響が及ぶ際には、物理的な直接の接触とネットワークなどを介した間接的な接触が考えられる。特に、ネットワークを媒介とする場合には、物理的に実験環境のネットワークに接続するような物理的な接触と、間接的な接触の両方が考えられるため、留意が必要である。これらを踏まえ、特に一つ目の側面である「マルウェア活動の実験環境への封じ込め」について述べる。

マルウェアの活動には、大きく分けて、感染活動、情報収集活動、攻撃活動の三つがある。

感染活動とは、マルウェア自身の実行実体やその一部などを、他のホストや媒体へ複製しようと試みる活動である。トロイの木馬と呼ばれる種類のマルウェアは、利用者に誤操作させ、この感染活動を開始する。脆弱性などを利用し、感染直後から、自動的に感染活動を開始するマルウェアもある。また、ボットと呼ばれる種類のマルウェアは、外部のボットハーダーからの指令に基づき、感染活動などを行う。感染活動は、マルウェアの被害の拡大を招く活動であり、多くのマルウェアの最も主要な活動である。この活動がなければ、マルウェアは単なる攻撃ツールや情報収集ツールに過ぎない。よって、この活動を封じ込めることが隔離の重要な目的である。

情報収集活動とは、マルウェアが実行されているホスト上で収集可能な情報を収集し、他のホストや媒体へ転送しようと試みる活動である。例えば、ホスト内からの特定のファイルの吸い出しや、キーロガーなどによる ID やパスワードの取得などが挙げられる。特に、マルウェアの作者が情報収集を目的としている場合には、特定のホストに向けて収集した情報が送信されることが多い。ボットの場合は、多くの場合は C&C（Command and Control）ネットワークに送信される。情報収集活動は、マルウェアを更なる攻撃の準備や犯罪活動に利用するためのものであり、機密情報を含めた重要な情報が漏えいする可能性があるため、封じ込める必要がある。

攻撃活動とは、マルウェアが実行されているホスト上から、そのホスト自身の内部や他のホストへ攻撃を試みる活動である。例えば、特定のホストへの DoS 攻撃やそのホスト自身の記憶媒体内のファイルの破壊などが挙げられる。マルウェア

の目的が攻撃である場合、感染後、他のホストへの感染活動とともに、特定のホストなどに攻撃を試みる場合が多い。ボットの場合には、ボットハーダーからの指令により、各種の攻撃を開始する。攻撃には、多くの種類があるが、攻撃の対象が感染ホスト自身である場合には、封じ込める必要はない。攻撃が感染ホスト以外を対象とする場合には、その攻撃による被害を避けるために、封じ込めが必要である。

3.2 隔離の手法と度合い

前述のとおり、マルウェアの活動も、外部からの影響も、どちらもそれらが及ぶ際には、物理的な直接の接触か、ネットワークなどを介した間接的な接触が必要となる。また、いずれの場合も何らかの媒介を介する。物理的接触の場合は、物理的な記憶媒体とネットワークの両方、間接的な接触の場合は、ネットワークが媒介となり得る。

よって、隔離の手法としては、物理的接触を防ぐことと、ネットワークが媒介として機能しないようにすることが考えられる。また、ネットワークを媒介とする場合、実験環境から外部へのマルウェアの活動の封じ込めと、外部から実験環境への影響の排除の二つの方向で、対策手法に違いがあると考えられる。

また、マルウェアの隔離実験環境の目的は、マルウェア検体を実行し、何らかの実験データを取得することである。そのため、隔離しながらも、検体の投入と実験データの取得は何らかの方法でできなければならない。さらに、マルウェアの活動を封じ込めながらも、マルウェアが本来行う活動が阻害されないようにせねばならない。

実際の隔離の手法には、様々なものが考えられるため、ここでは、どのくらい隔離が実現されているかの度合いを、上記の観点に合わせて定義する。物理的接触を防ぐ度合いを PSL（Physical Security Level）、ネットワークを媒介とする場合に、マルウェアの活動を封じ込める度合いを MCL（Malware Containment Level）、外部からの影響を排除する度合いを EIL（Environment Isolation Level）と呼ぶこととし、度合いを幾つかの段階に分け数値で表すこととする。段階は、0が最も低く、数値が大きくなるほど隔離の度合いが高いことを表すこととする。本稿では、マルウェア活動の封じ込めを重視し、MCL に着目し、PSL と EIL については、割愛する。

3.2.1 MCL（Malware Containment Level）

隔離の対象となる実験環境は、マルウェアを実行する実行環境と解析・観測などのための周辺機器、それらを管理・制御するための端末など管理用機器からなり、それらをつなぐネットワークやその他の配線などから構成されていると想定する。管理用機器は、既知の脆弱性に関しては十分なセキュリティ対策が取られていると想定する。実験環境のネットワークは、実際にマルウェアが活動し、実験データを観測するための実験用ネットワークと、マルウェアの実行や構成機器の管理のための管理用ネットワーク、そして、インターネットなど実験環境の外の外部ネットワークの三つからなると想定する。想定する環境の概念図を図 1 に示す。

ネットワークを媒介としたマルウェアの活動が行われる場合、実験用ネットワークと管理用ネットワークや外部ネットワークがどのように接続されているのかが重要になる。物理的に分離されているのか、VLAN などのリンク層で分離されているのかといった物理接続と、ルータや踏み台などを経由すれば接続できるかどうかという論理接続の観点が考えられる。また、通信をファイアウォールなどで一律に制限するのか、特定の通信のみに制限するのか、プロキシやアプリケーションゲートウェイを介し直接は通信しないのかなども、考える必要がある。また、管理用ネットワークから外部ネットワークへは、一度管理用機器へ

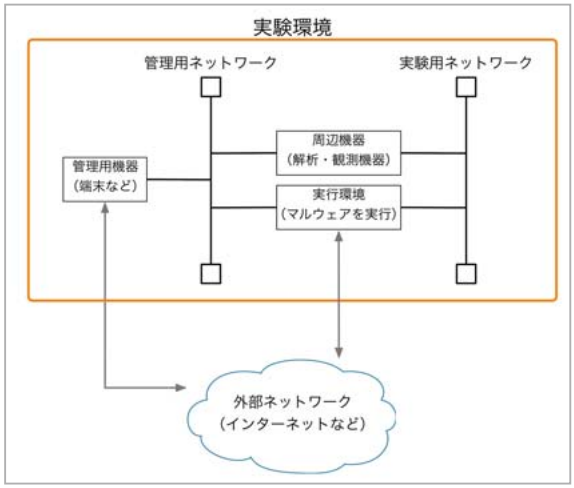

図 1 想定環境

表1 MCL（Malware Containment Level）の定義

段階	封じ込めの方法		実験の対象となるマルウェア
MCL-0	実行環境→外部 管理用→外部 接続	特に制限無し 特に制限無し 直接接続	既知で、外部に損害を与えないことが判明している
MCL-1	実行環境→外部 管理用→外部 接続	ファイアウォールなどで制限 ファイアウォールなどで制限 それぞれ論理的に分離	既知で、通信活動が判明しており、駆除が容易
MCL-2	実行環境→外部 管理用→外部 接続	特定の通信のみ許可 ファイアウォールなどで制限 それぞれ論理的に分離	詳細は未知だが、既知の脆弱性のみを利用する
MCL-3	実行環境→外部 管理用→外部 接続	直接通信は認めず専用のプロキシなどを介す 特定の通信のみ許可 実験用は物理的に分離、他は論理的に分離	未知で、未知の脆弱性への攻撃を含む
MCL-4	実行環境→外部 管理用→外部 接続	通信は認めない 直接通信は認めず専用のプロキシなどを介す 実験用は物理的に分離、他は論理的に分離	未知で、非常に危険な活動が含まれる可能性がある
MCL-5	実行環境→外部 管理用→外部 接続	通信は認めない 通信は認めない それぞれ物理的に分離	物理的分離以外では防ぐことができない

マルウェアの活動が波及し、その結果、管理用端末を介してマルウェア活動が外部へ伝搬するような二次感染などを想定する必要がある。

これらを踏まえ、MCL を表 1 のように 6 段階定義する。表中の段階は、封じ込めの度合いを示す。封じ込めの方法は、それぞれ、各ネットワークから他のネットワークへの接続がどうなっているべきで、通信の制限がどうなっているべきなのかを示す。実験の対象となるマルウェアは、その段階の封じ込めで外部に損害を与えずに安全に実験できるマルウェアがどのようなものかを示している。

「直接接続」は、接続方法に制限がなく、同じネットワークスイッチを共有し、同一のネットワークセグメントに設置されるような場合を示している。「論理的に分離」は、物理的なネットワークスイッチなどは共有するが、VLAN などを利用して違うネットワークセグメントに設置されていることを示している。「物理的に分離」はネットワークスイッチなども共有せず、物理的に別のネットワークセグメントに設置されていることを示している。「ファイアウォールなどで制限」は、ポートレベルの検査で通信の可否を判断することを意味し、「特定の通信のみ許可」は、特定のプロトコルによる通信のみを判別して許可することを意味する。「直接通信は認めず専用のプロキシなどを介す」は、通信を一端プロキシやアプリケーションゲートウェイで受け、プロキシから正常な通信のみが行われることを意味する。

ある実験環境が、ここに挙げた封じ込めの方法をすべて満たしている段階がその実験環境の MCL と定義し、例え一部に優れていたとしても、すべて満たしている段階以上ではないと考えることとする。なお、ここでは「管理用 → 外部」として管理用機器からのマルウェア活動の封じ込めを表記したが、実行環境から管理用ネットワークへの通信がこの表記より厳しい制限を与えている場合、管理用機器から外部ネットワークへも同じ制限を満たしていると解釈して問題ない。すなわち、「管理用→外部」と表に現れていない「実行環境 → 管理用」のいずれか強い方が「管理用 → 外部」を満たしているかどうかで、その段階を満たしているかを判断することとする。

3.3 隔離の問題点

マルウェアの動態解析においては、マルウェアの活動を封じ込めるための隔離は有効な手段である。しかし、隔離の度合いを高めることは、下記のような幾つかの問題を生じる。

1. マルウェアによる実行環境の判別がしやすくなる
2. マルウェアが活動するために必要な通信も阻害してしまう

それぞれについて概観し、対策手法について概説する。

3.3.1　マルウェアによる実行環境の判別

マルウェアによる実行環境の判別とは、マルウェア自身が解析を目的とした環境で実行されていないかを検査することである。隔離環境で動作していないかを判別し、結果に基づいて実行抑制や実体隠蔽を行い、動態解析を困難にする。

マルウェアによる隔離環境対策としては、利用IPアドレスの確認や接続性の検査が行われる。利用IPアドレスの確認は、IPアドレスを検査し、隔離環境でよく用いられるプライベートアドレス空間などで動作していないかを確認する方法である。また、インターネット上の特定のホストやサービスへの接続性を検査することで、隔離環境ではないかを判別する方法がある。手法が非常に単純であるため、広く用いられている。

IPアドレスの検査に関しては、外部への影響を排除した上で、プライベートアドレス以外のアドレスを実験環境に用いればよいので、大きな問題ではない。これに対し、接続性の検査については、封じ込めの度合いを犠牲にして特定のホストやサービスへの接続性を提供するか、インターネットの代わりをする機構を導入する方法[4]や、擬似的なインターネットを構築する[2]などの方法がある。

3.3.2　マルウェアが活動するために必要な通信

外部との通信が不可欠なマルウェアでは、隔離によって外部との通信を断絶した場合、その活動は、停止するか、正常ではなくなる。よって、実行時に本体をダウンロードするものや、ボットなどに代表される命令ネットワークに参加し指令を受けて活動するマルウェアは、MCL－2以上の隔離で想定外の通信を行う場合やMCL－4以上の隔離を行った場合、その活動を正しく観測することができない。

対策としては、封じ込めの度合いを犠牲にして、マルウェアの送信元など特定のホストのみとの通信を許容する[5]などの方法がある。

4　マルウェア隔離実験環境の設計と実装

これまで、隔離の度合いMCLについて定義し、隔離による問題点について述べた。本章では、まずこれらに基づいて我々が研究開発してきた既存のマルウェア実験環境について再評価し、その上で、新たなマルウェア隔離実験環境の設計と実装について述べる。

4.1　既存研究の評価

まず、我々が研究開発してきたVM Nebulaと擬似インターネット付きマルウェア隔離解析環境について、その隔離度合いと問題点について評価する。

4.1.1　VM Nebula

VM Nebula[6]は、マルウェアに限らず、インターネットセキュリティに関する実験を行う実験環境である。仮想化技術を利用して、4台のサーバで最大256台のPCホストを模倣することにより、大規模な実験を実現するとともに、破壊的な実験を行った場合でも容易に環境の再構築を行うことができる。構成の概要を図2に示す。

攻撃者模倣サーバと被害者模倣サーバ、ネットワークサーバ上でVMware社のVMware Serverを利用して、複数のPCを模倣する。実験の際の通信は実験用LANを介して行われ、各サーバの制御などは制御用LANを介して行われる。インターネットなど外部のネットワークへの接続は提供されていない。実験用LANと制御用LANは、別のネットワークスイッチを用いて物理的に分離されている。これらから、VM Nebulaは MCL－5の隔離実験環境であるといえる。

VM Nebulaは、MCL－5の隔離実験環境であ

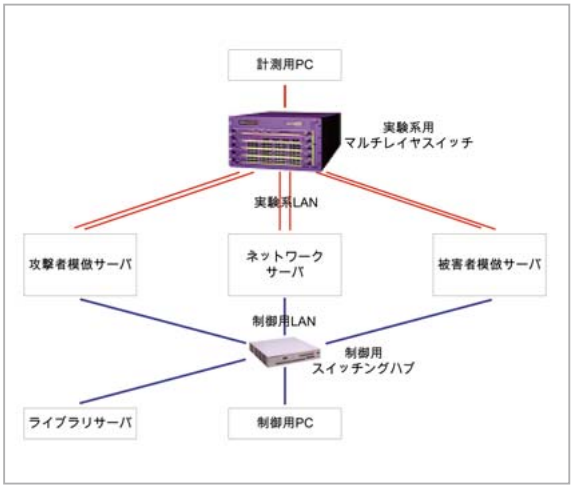

図2　VM Nebulaの構成

るため、危険なマルウェア検体の実験を安全に行うことができるが、外部から実行実体をダウンロードするようなマルウェアやインターネットとの接続性を確認するようなマルウェアの活動については、正しく観測することができない。また、実行環境や管理用機器の OS のアップデートなども外部から物理メディアを持ち込む必要があり、利便性が低いなどの問題がある。

4.1.2 擬似インターネット付きマルウェア隔離解析環境

擬似インターネット付きマルウェア隔離解析環境[2][7][8]は、仮想環境や隔離環境を判別するような解析困難化機能を持つマルウェアを安全に動態解析するための隔離解析環境である。マルウェアの解析困難化機能に対し、実ノードの切替えや再生により仮想化技術と同程度の利便性を確保する方式と擬似インターネットによりマルウェアを騙し、隔離環境で解析されていることに気づかせない方式を組み合わせて、対抗している。構成の概要を図 3 に示す。

再生可能な実ノードによるマルウェア実行環境である Malware Incubator と擬似インターネット機能を有する Mimetic Internet、それらを制御する制御用の Controller ノード群（以降、制御ノード群）と管理用端末からなっており、管理用端末以外はすべて隔離環境中にある。Malware Incubator 上でマルウェアを動作させ、マルウェアのインターネットへのアクセスは Mimetic Internet が模倣し、接続性検査などを騙すことができる。実験用のネットワークは物理的に分離されており、管理用のネットワークは論理的に分離されている。Malware Incubator から管理用ネットワークへの通信は、マルウェアの実行時は完全に遮断される。実験データの収集や検体の投入を必要とする場合には、一度 Malware Incubator を停止し、別のネットワークブートの OS で再起動した後に行うため、マルウェア活動が制御ノード群に及ぶことはない。さらに、制御ノード群と管理用端末の間には特定の通信のみを許可する Security Gateway が設置され、二重に隔離を行っている。これらから、MCL－4 相当の隔離実験環境であるといえる。

擬似インターネットによって、マルウェアの接続性検査を騙すことはできるが、ダウンロードを必要とする場合や命令ネットワークからの指令を必要とする場合などは、正しく観測することはできない。また、現在の擬似インターネットは準備した幾つかのサーバとネットワークを擬似する固定環境であるため、準備していないホストやサービスへの接続性検査を行うマルウェアには対応で

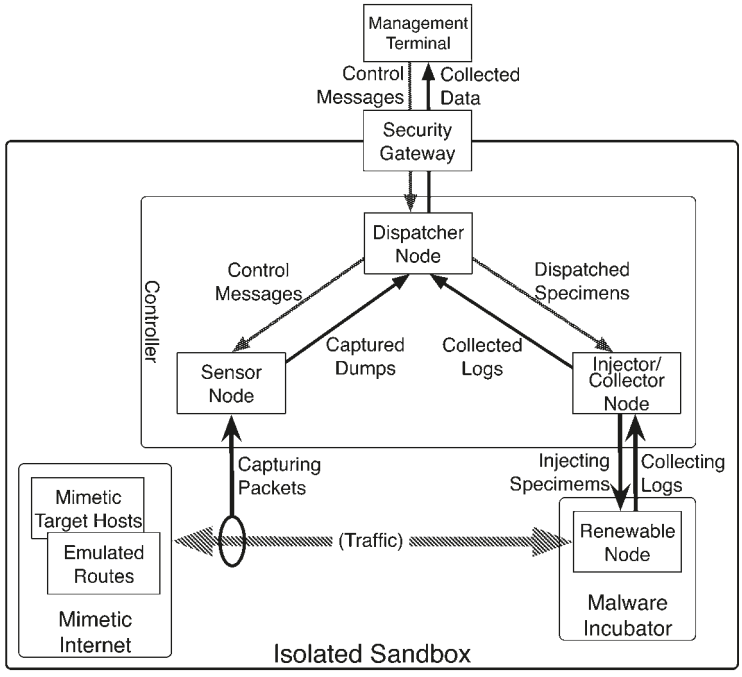

図3 擬似インターネット付きマルウェア隔離解析環境の構成

きないなどの問題がある。

4.2 提案手法

提案手法では、既存研究と同様に安全な動態解析を行うため、MCL－4以上の隔離実験環境を目指す。ただし、ダウンロードや命令ネットワークなどの外部との通信を必要とするマルウェアへの対応や、より複雑な接続性検査への対応を行うことで、より多様なマルウェアの隔離実験を可能とすることも同時に目指す。

4.2.1 設計

まず、基本構成は擬似インターネット付きマルウェア隔離解析環境を用い、これを拡張することでより多様なマルウェアの隔離実験環境とすることとする。実行実体のダウンロードや命令ネットワークへの参加、より複雑な接続性検査への対応など、いずれも擬似インターネットが十分な機能を持てば、解決可能な問題である。そこで、下記の二つの機能を追加することとする。

- 高忠実度擬似インターネット（HF－Mimetic Internet）
- 外部情報収集エージェント（Download Agent）

高忠実度擬似インターネットでは、現在の擬似インターネットに対し、大きく分けて下記の二つの機能を追加する。

- マルウェアからのアクセス情報の収集と記録（Access Collector）
- 動的な擬似サービス、擬似ホスト、擬似ネットワークの導入（Dynamic Constructor）

前者では、実際にマルウェアが活動に際して、どのようなホストのどのようなサービスへのアクセスをどのようなプロトコルで試みるのかを収集・記録する。この記録を基に、後者の機能を使って擬似インターネット上にマルウェアが必要とする擬似サービスやホストなどを新たに導入する。これによって、マルウェアが接続性検査に利用するアクセス情報を基にした擬似インターネットが構成されるため、どのような接続性検査を行ったとしても、擬似インターネットによって騙すことが可能となる。また、外部情報収集エージェントと連携し、外部からダウンロードする実行実体や命令ネットワークからの通信を導入することで、外部との通信を必要とするマルウェアの活動を観測することも可能となる。

外部情報収集エージェントは、高忠実度擬似インターネットで収集したマルウェアのアクセス情報のうち、ダウンロードに該当するものや命令ネットワークの参加要求などに該当するものを抜き出し、マルウェアの代わりに代理実行し、結果として得られたダウンロード物や命令通信を高忠実度擬似インターネットに送る。これにより、マルウェアから有害な通信が直接行われることなく、安全性を確保しながら、マルウェアが活動する上で必要な情報を隔離実験環境中に投入することが可能となる。

4.2.2 実装

この高忠実度擬似インターネット付きマルウェア隔離実験環境の概要を図4に示す。提案方式は、現在実装中であるが、以下にその概略を述べる。

Access Collectorは、単純に擬似インターネットの入り口でパケットキャプチャを行い、アクセスするホスト名やIPアドレス、プロトコルを列挙する。現在、DNSクエリとHTTPアクセスに対応したAccess Collectorを実装中である。

Dynamic Constructorは、Access Collectorからホスト名とIPアドレスのリストを取得し、対応したDNSレコードやサービスサーバを導入する。現在、DNSレコード生成と単純なHTTPサーバ設定の生成を実装中である。

Mimetic Targetsとしては、擬似DNSサーバや擬似サービスサーバ、擬似クライアント、擬似ネットワークなどがあり、Dynamic Constructoから得た設定に基づき、動的に生成する。現在、実装方式の検討中である。

Download Agentは、Access Collectorからホスト名やIPアドレス、アクセスプロトコルのリストを取得し、インターネットへの代理アクセスを試みる。現在、DNSクエリの代理アクセスとHTTPの代理アクセスの実装中である。

また、現在、仮想機械を利用するMalware Incubatorと実ノードのMalware Incubatorの両方を自動で使い分ける機構の実装を行っている。

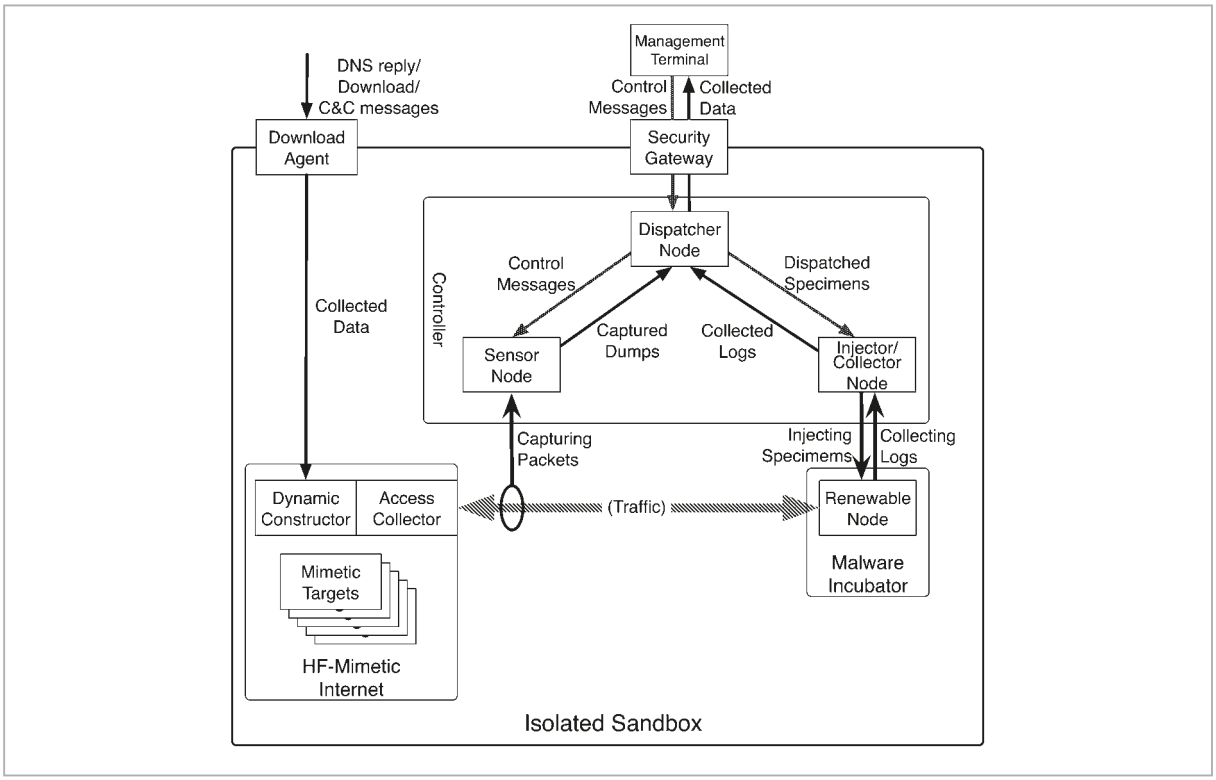

図4 高忠実度擬似インターネット付きマルウェア隔離実験環境の概要

5 課題と今後の展望

提案方式は、現在実装中であり、実装後に、実際のマルウェア検体を用いて有効性を検証する予定である。ここでは、隔離実験環境の課題や今後の展望について述べる。

5.1 提案方式の課題

提案方式のような隔離実験環境を用いる場合、**3.3** に述べたように、マルウェアによる実行環境の判別がしやすくなることやマルウェアが活動に必要とする通信も阻害してしまうことなどが問題となる。これは、隔離の度合いと解析可能なマルウェアの種類や数との間に、背反関係が成り立つことを意味する。

未知で危険なマルウェアは、隔離の度合いを高める必要があるが、最新の技術で作成されている場合には、実行環境の判別が高度であったり、より活動に際し、外部との連携を深めていたりすることが考えられる。そのため、隔離実験環境の需要が大きい未知で危険なマルウェアほど、この背反関係が強く働くと考えられる。

提案方式は、この背反関係の両立を目指しているが、マルウェアを騙すことができるかやマルウェアが活動に必要な情報だけを得られるかといったことは、高忠実度擬似インターネットの性能に依存している。高忠実度擬似インターネットの性能は、必要と思われる要素に対応した擬似機構を追加することで、向上されるが、マルウェア側の新しい隔離対策技術の導入によって、新たな機能追加を強いられるというイタチごっこを引き起こす可能性がある。いかに機能追加せずに自動で新しいマルウェアの活動に対応できるように構成するかが、今後の課題である。

5.2 今後の展望

提案方式のようなマルウェア隔離実験環境は、マルウェアの解析のみならず、セキュリティ製品の貫通テストやセキュリティの教育演習など他の用途への応用も考えられる。現在、セキュリティ専門家の教育環境として、提案方式を応用したマルウェア再現演習環境の研究開発を行っている。

また、本稿では **3.2** で隔離の度合いに関して整理を行った。このようなセキュリティ実験環境に関する評価の軸を用意することで、他の実験環境との間での性能比較や結果の流通などを支援す

ることができると考えている。

6　おわりに

マルウェアの技術は日々進歩しており、その解析・検証は不可欠である。本稿では、その動作や影響を解明する動態解析を安全に行うための隔離実験環境について、隔離の度合いを整理し、我々が行ってきた隔離実験環境を位置付けた。その上で、同程度の隔離度合いを保ちながら、高忠実度の擬似インターネットを提供することで、より多様なマルウェアの隔離実験を可能とする環境を提案した。

この手法により、従来は困難であった隔離実験環境でのダウンロードや命令ネットワークの参加、より複雑な接続性検査への対応などが可能となり、最新のマルウェアの振る舞いや影響を安全な隔離環境における動態解析で把握することができる。

提案手法は、現在、実装中であり、実装後に実際のマルウェア検体を利用して実証実験を行う予定である。

参考文献

1　E. Skoudis with L. Zeltser, "MALWARE – Fighting Malicious Code –", Prentice Hall PTR, ISBN 0-13-101405-6, Pearson Education Inc., 2004.
2　三輪信介，宮地利幸，篠田陽一，“擬似インターネット機能付きマルウェア隔離実験環境の提案”，電子情報通信学会，第３回情報通信システムセキュリティ時限研究会（ICSS 3rd），2007年2月.
3　情報処理推進機構，“情報セキュリティ白書（2008）”，実教出版，ISBN-10：4407316438，2008年6月.
4　須藤年章，富士原圭，“仮想インターネットを用いたボットネット挙動解析システムの評価”，情報処理学会，コンピュータセキュリティシンポジウム 2006（CSS 2006），2006年10月.
5　馬場俊輔，鈴木宏栄，鈴木和也，“ハニーポット環境を用いた未知の振る舞い解析手法”，電子情報通信学会，2007 年暗号と情報セキュリティシンポジウム（SCIS 2007），2007年1月.
6　三輪信介，大野浩之，“再現実験環境『VM Nebula』を用いたウィルス・ワームの解析”，Internet Conference 2003（IC 2003），2003年10月.

三輪信介（みわしんすけ）
情報通信セキュリティ研究センター
レーサブルネットワークグループ研究員　博士（情報科学）
ネットワークセキュリティ

門林雄基（かどばやしゆうき）
情報通信セキュリティ研究センター
レーサブルネットワークグループ客員研究員　博士（工学）
ネットワークセキュリティ

篠田陽一（しのだよういち）
情報通信セキュリティ研究センター長
工学博士
ネットワーク、次世代インターネットアーキテクチャ