3-2　GHOST Sensor: 能動的サイバー攻撃観測プラットフォームの研究開発

衛藤将史

インターネットにおけるサイバー攻撃の状況を把握するため、様々なネットワーク観測技術が提案されているが、既存の観測システムは攻撃者に応じて最適なセンサ（ハニーポット）で攻撃への対応を行うといったように柔軟性に乏しいため、結果的に観測機会を逸することが多い。また、広域なネットワーク観測システムの運用にあたっては、IP アドレス空間の効率的な利用の難しさや、メンテナンスコスト、観測用 IP アドレスが攻撃者のブラックリストに載ることにより観測精度が低下するなどの問題が存在する。これらの問題に対応するため、本研究では仮想センサ技術と柔軟なセンサの割当て機構を用いて多様なセンサを管理する、能動的サイバー攻撃観測プラットフォーム GHOST センサを開発した。本技術は L3 の透過プロキシとして動作する仮想センサを遠隔地の観測組織に配置する一方で、センタ側で多種の実ハニーポット を一元的に管理し、攻撃者のプロファイルに応じた柔軟な対応をすることにより、攻撃観測精度を向上している。本稿では、本プラットフォームの技術的な詳細について紹介する。

1　まえがき

深刻化するサイバー攻撃に対応するため、現在、様々なサイバーセキュリティ技術の研究開発が世界中で進められている。その中でもいくつかの研究開発プロジェクトでは、インターネットにおけるサイバー攻撃の状況把握を目的として、広域ネットワークの観測技術の研究開発と運用が進められてきた [1]–[5]。サイバー攻撃への対策として、これらのプロジェクトに共通するのは、世界中で発生する攻撃の様子を広範囲に、かつ深いレベルで収集し、大局的に状況を把握することに注力している点である。

その一方で、サイバー攻撃の手法は複雑化の一途をたどっており、現在も活発に継続する OS やサーバアプリケーションへのリモートエクスプロイト攻撃に加え、近年ではドライブ・バイ・ダウンロード攻撃に代表されるように、Web やメールなどのアプリケーションを媒介して感染するマルウェアも急増している。

このように、柔軟に攻撃対象を変えるサイバー攻撃に対応するため、脅威の種類に応じて様々な攻撃情報や収集手法が提案されている。特にリモートエクスプロイト攻撃を対象とした攻撃情報収集システムとしては、脆弱な実ホストを装って攻撃の様子を観測する高対話型・低対話型ハニーポット [6][7] や HTTP、SSH、DNS といったサービスに特化したハニーポットなども多く用いられている。また、外部ネットワークからの通信に対して一切の応答をせずに攻撃の様子を観測するブラックホール観測 [8][9] は、ハニーポットと比較してその運用が容易なために、より広範囲でのネットワーク観測に適しており、多くの研究プロジェクトで運用されている。

さらに、エクスプロイトコードを含んだ応答によりクライアントへの侵入を試みるドライブ・バイ・ダウンロード攻撃への対策のひとつとして、Web サーバを定期的に巡回探索する Web クローラも様々な組織において研究開発されている。これらのセンサを日本国内だけでなく、海外も含めて広範囲に設置する（または海外組織と密な情報共有を行う）ことで、初めてインターネットでのサイバー攻撃の状況を把握することが可能となる。

しかしながら、これらの技術を用いて構築されたサイバー攻撃観測システムを運用する上では、「見たい攻撃を最適なハニーポットで見る」ことが困難であるという課題がある。たとえ広域な観測網を有していても、ハニーポットが固定的な IP アドレスの下で運用されている環境では、そのハニーポットの IP アドレスあてに攻撃が到来しないかぎり、攻撃を詳細に観測することは困難である。Web 通信での攻撃であれば Web サーバ型ハニーポット、SSH 通信での攻撃であれば SSH サーバ型ハニーポットといった形で、攻撃を最適なセンサで観測しなければ深い情報は得られないが、既存の固定 IP アドレスによる運用では、こういった柔軟な観測は困難である。

また、このように論理的・物理的に広範囲にわたる

センサの運用にあたっては、様々な運用上の課題も存在する。特に、上述の[1]–[5] のように国際的な広域ネットワークにおけるセンサ網の構築を行うプロジェクトの観点から、広域ネットワーク観測システムの運用上の課題を以下に挙げる。

広域ダークネット確保の難しさ　前述のとおり、ブラックホール観測はその運用の容易さから広域ネットワーク観測に適しているが、受動的な攻撃観測手法であるため、効果的に攻撃情報を収集するためには、より広範囲な（例えば /16 サブネットなど）ダークネット（未使用の IP アドレス群）に適用することが望ましいとされる。しかし、国際的に見ると多くの国では IPv4 アドレス資源が豊富ではないため、既存研究のように広大なダークネットによる観測を行うことは困難である。よって、たとえ 2、3 程度の数少ない IP アドレスであっても有効に観測に用いられる技術が必要となる。

メンテナンスコスト　ブラックホール観測に適した広大なダークネットが確保できず、数個程度の数少ない IP アドレスしか使用できない場合、高対話型、あるいは低対話型ハニーポットを設置して、より深い攻撃情報を収集することが考えられる。しかし、おとりホスト、あるいはエミュレータによって実際に攻撃を受けることで詳細な観測を行うこれらのハニーポットシステムは、その反面、ブラックホール観測と比較して複雑なシステム構成とマシンリソースを必要とするため、二次感染の防止やシステムトラブル対応のためのメンテナンスコストが大きくなりがちである。

IP アドレスのブラックリスト化問題　同一の IP アドレスを使用して、観測センサを長期間にわたって運用すると、攻撃者側に観測ネットワークであることを検知され、当該 IP アドレスが攻撃者のブラックリストに載り、攻撃を避けられる場合がある。結果としてハニーポットでは、マルウェア検体の収集が行いづらくなるほか、特に Web クローラのようなアクティブ型のセンサでは、アクセス元アドレスが攻撃者のブラックリストに登録され、攻撃者の Web サイトへのアクセスが拒否される場合もある。

このような課題を受け、本研究では、攻撃者に応じた柔軟なセンサ割当て機構を有しながら、物理的なマシン及び IP アドレス資源を有効に用い、安定的・継続的にセンサ網を運用することを目的とした、能動的サイバー攻撃観測プラットフォーム GHOST センサを開発した。本手法は、主な機能として仮想センサ技術とハニーポットへの動的なアドレス割当て機構を有しており、これにより、上述の様々な形態のセンサを統合的に運用することが可能となる。

本稿ではまず、**2** において、攻撃観測網の運用技術に関する先行研究について述べる。次に、**3** で本研究の提案システムである GHOST センサの構成と機能を紹介する。**4** では、提案手法が実際に運用された際に攻撃情報の収集に与える影響を調査し、提案手法の実現可能性について検討を行い、**5** で実装に基づく提案手法の評価を行う。最後に、**6** でまとめと今後の課題を述べる。

2　関連研究

サイバー攻撃観測技術としては、ブラックホール観測を主とする [3][4][9] のほかに、ハニーポット運用時の有効なリソース利用を目的とした提案が数多く行われている [10]–[14]。その中でも、Collapsar[11] は、遠隔地の観測拠点にいわゆる仮想センサを配置して、分析センタ（またはインターネット）へのパケット転送のみを行わせ、分析センタ内において仮想マシンで構成された高対話型ハニーポットを稼働させる、ハニーポット運用技術を提案した。

また、Potemkin[12] は、Collapsar の機能に加えて、特定の IP アドレスあてへの攻撃が来た際に、その IP アドレスを有する仮想マシンを動的に起動して応答を行う構成となっている。必要な時にのみ仮想マシンを起動させることで、マシンリソースの消費を抑制するほか、所有する IP アドレスすべてについて対応する仮想マシンを有することから、観測対象の IP アドレスを有効に活用している手法であるといえる。

一方、SGNET[13] では、Collapsar、Potemkin と類似した構成において、攻撃者からのクエリに対する一般的なサーバ応答を遠隔地のセンサが記憶し、可能な限り応答することで、観測拠点と分析センタ間の通信量を削減させている。注目すべき点として、未知のクエリの場合にはセンタ側の実サーバにクエリを転送することで、実時間での応答を可能としていることが挙げられる。

これらのハニーポット運用技術は、いずれも高対話型ハニーポットの運用におけるリソースの有効利用、効率的な検体取得という目的に特化しており、その点においては有効な手法といえる。しかし、いかに高度な仮想化技術を用いても同時に起動できるハニーポットインスタンスは高々数千程度である。これに対して万単位のダークネットアドレスを観測するプロジェクトも存在する。だが、高度な運用技術を用いても多数の攻撃を観測した場合にはマシンリソースが枯渇する

ことが予想される。したがって、IP アドレスを無駄にすることなく可能な限り効率的に使用する方法を検討する必要がある。さらに、これらの運用技術は主に待ち受け型ハニーポットの運用を想定した技術であるため、他の観測手法にそのまま応用することは難しい。前章において述べた Web クローラによる観測における課題なども考慮した、運用手法を考える必要がある。

3 能動的サイバー攻撃観測プラットフォーム GHOST センサ

前章で挙げた関連研究における課題を受けて、本研究では高対話型ハニーポットだけでなく、ブラックホールセンサや Web クローラなど、様々なネットワーク観測システムに対して動的に IP アドレスを割り当てることで、物理的・論理的な資源を有効に活用する能動的サイバー攻撃観測プラットフォーム GHOST（Global, Heterogeneous, and Optimized Sensing Technology）センサを開発した。

3.1 概要

提案システムの概要を図 1 に示す。

提案システムでは、Collapsar 等の先行研究と同様に、これまで遠隔地の観測拠点で運用されていた実センサを分析センタ側に配置（図 1：Low-interaction Honeypot, High-interaction Honeypot 及び Blackhole sensor）する一方、観測拠点側には L3 プロキシ機能を持つ仮想センサ（図 1：Virtual sensor）のみを配置する。仮想センサは受信した攻撃パケットを分析センタに転送することのみに注力し、具体的な攻撃への対応は分析センタの実センサが行う構成である。

なお、仮想センサは、観測拠点において提供されている L3 ネットワーク（及び IP アドレス）を VPN 回線を通じて分析センタまで延伸する。したがって攻撃者からは、あたかも協力組織自体に対して攻撃を行っているように見えるが、実際には分析センタにおいてすべての攻撃が処理されることになる。

提案システムの大きな特徴は、分析センタ内で接続マネージャ（図 1：Connection manager）がハニーポットだけでなく、Web クローラやブラックホールセンサなどに、様々な運用ポリシに従って、動的な IP アドレスの割当てを行い、能動的な攻撃観測を可能とする点である。さらに、高対話型ハニーポットによる外部への二次感染を防ぐには、IPS やファイヤウォール等の監視システムを設置する必要があるが、これまでは各分析拠点でこれらの措置を施す必要があったのに対し、提案システムでは分析センタ内部で集中管理する事が可能となる。

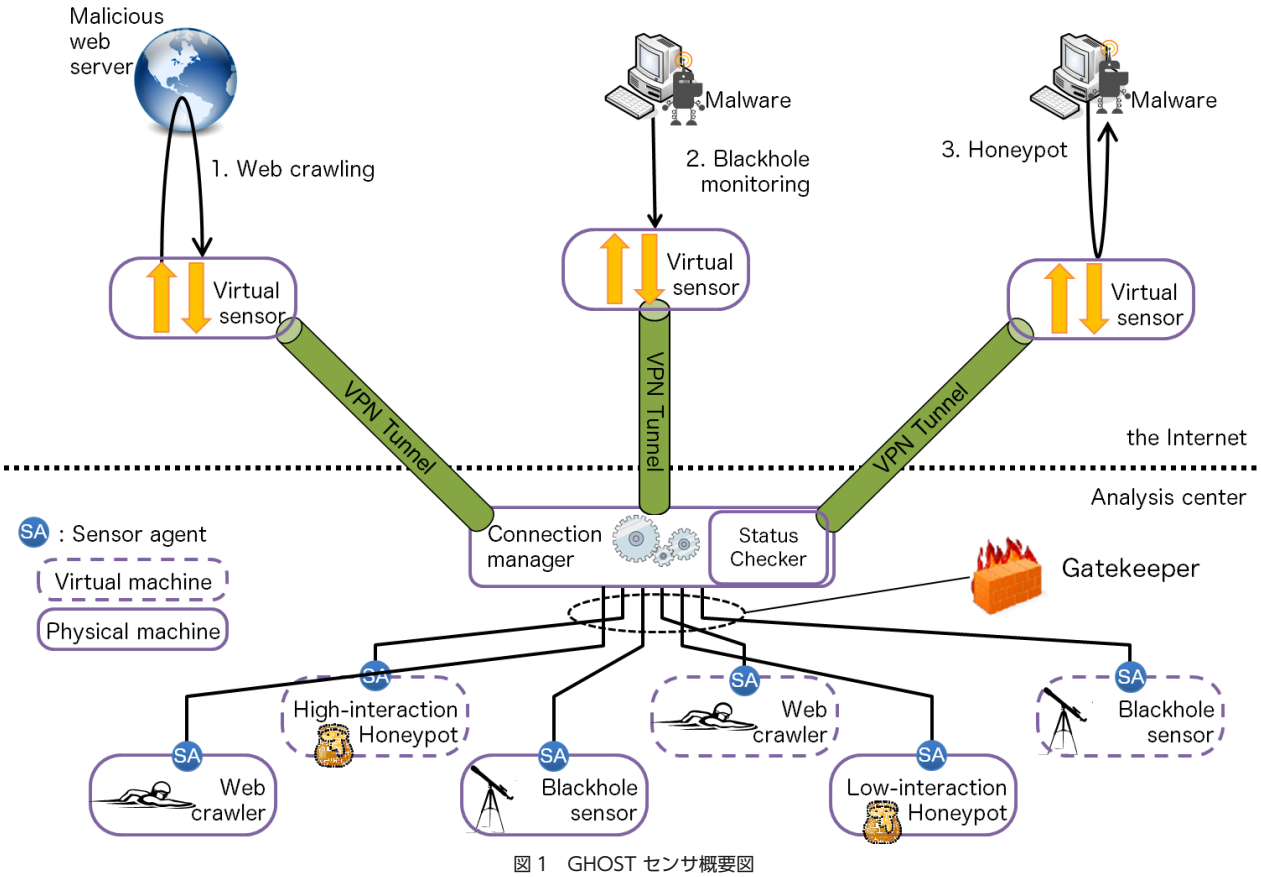

図 1　GHOST センサ概要図

3.2　主要コンポーネント

提案システムにおける主要なコンポーネントとその機能を以下に述べる。

仮想センサ　仮想センサは地理的に離れた観測拠点に設置される L3 プロキシ型のセンサプログラムであり、観測拠点の物理マシン上に構築された仮想マシン上で動作することを前提としている。仮想センサは、分析センタとの間に IPsec による VPN 回線を結び、自身あてのすべてのパケットをカプセル化して分析センタに転送する。その一方で、分析センタ内の実センサからの応答パケットを適切なあて先に送信する。

実センサ ／ センサエージェント　実センサは、これまでにも紹介したブラックホールセンサ、高対話型・低対話型ハニーポット及び各種の web クローラなどによって構成される。実センサには、物理マシン・仮想マシンのいずれを用いることも可能であることが、仮想マシンを想定した既存手法 [11][12] とは異なる点である。この理由は、実センサ上の IP アドレスの管理を、既存研究においては仮想マシンのハイパーバイザを用いて行うのに対し、すべての実センサ上に配置されたセンサエージェントが行うためである（**3.3** の「エージェント方式」を用いた場合）。センサエージェントは、接続マネージャのメッセージにしたがって、実センサの IP アドレスをリアルタイムに変更するほか、取得検体数・パケット数などの統計データを定期的に接続マネージャに送信する機能を有する。

接続マネージャ　接続マネージャは、分析センタの境界に設置され、仮想センサからのパケットを適切な実センサに転送するとともに、その応答パケットを仮想センサ側に返送する機能を有する。また、もっとも重要な機能として、接続マネージャは攻撃者のプロファイルや実センサの稼働状況などに応じて、センサエージェントにアドレス変更命令を送信し、常に最適な実センサ構成を維持する役割を持つ。割当て lua 言語によってあらかじめ記述された割当てルールに従って実施される。このように割当てルールをソフトウェアによって定義できる点が提案システムの大きな特徴である。

ゲートキーパ　ゲートキーパは実センサと分析センタとの間に設置され、特に外部向けのトラフィックの監視と制御を行う。このように監視点を 1 カ所に集約することで、2 次感染防止のためのオペレーションの負担を軽減することが可能となる。ここでは、例えば実センサに感染したボットによる C&C 通信や著名 Web サイトへの接続確認通信などのみを許可し、その他の通信は遮断するといった制御を行う。

3.3　アドレスの動的割当て機能の検討

前節で述べたとおり、接続マネージャは仮想センサからのパケットを実センサに転送するとともに、必要に応じて実センサの IP アドレスの割当てを変更する機能を持つ。この際に、実センサのアドレスを動的に変更する方法として以下の検討を行った。

仮想マシン方式　Potemkin[12]、DenseShip[14] 等では、仮想マシンの特徴を生かした IP アドレスの動的な割当てを行っている。ここでは任意の IP アドレスに対応する仮想マシンをリアルタイムに起動する、という形で動的な IP アドレスの割当てを実現している。これに対して、本研究では仮想マシンだけでなく、物

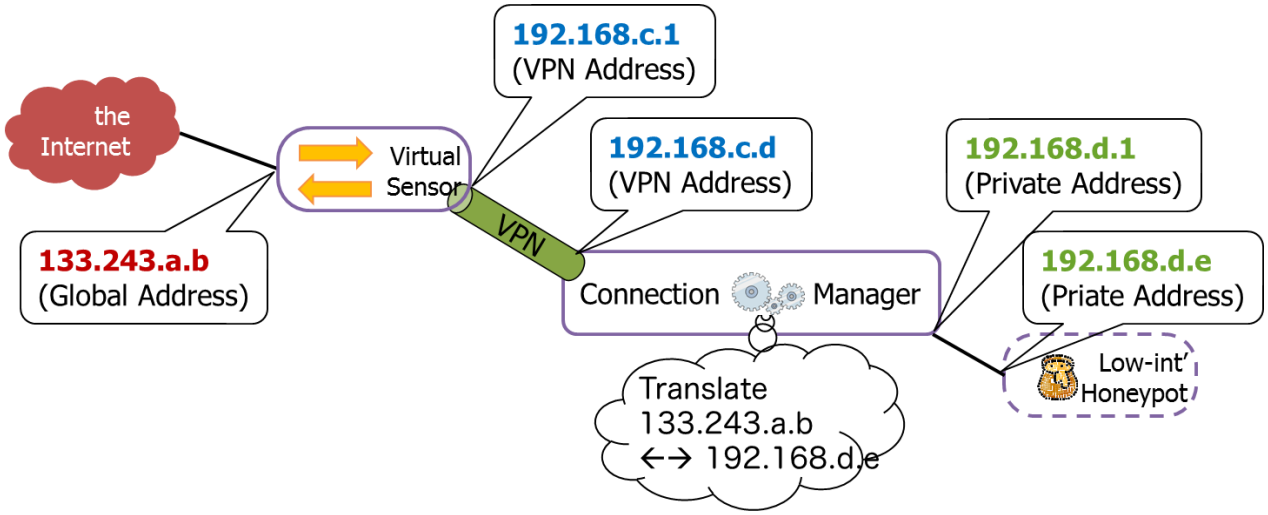

図 2　NAT 方式での動的 IP アドレス割当て

理マシンをも実センサのプラットフォームとする必要があるため、仮想マシンを必要とするこの手法は適さない。

NAT 方式　実センサに固定アドレスを永続的に割り当て、接続マネージャが NAT 変換によって仮想センサと実センサの対応付けを切り替える手法である（図 2）。実センサ側の動的な設定変更は行わず、NAT テーブルを切り替えることで実現できるため、他の方式に比べて高速に割当ての変更が可能となる利点がある。ただし、実センサが高対話型ハニーポットなどの高度な環境を有している場合、攻撃対象とされた IP アドレスと実センサ上の IP アドレスの違いについて攻撃者に気づかれる可能性がある。

DHCP 方式　接続マネージャが DHCP サーバとなり極端に短い期間で任意の IP アドレスを実センサに配布し、必要に応じて動的に割当てを変更する手法である。実センサ側に変更を加える必要が無い点で有効である。しかし、どれだけ短くとも IP アドレスの変更に秒オーダの時間が必要となるため、本研究においては不適切といえる。

エージェント方式　実センサの OS 上に常駐するセンサエージェントが、接続マネージャからのメッセージを受信することで動的な IP アドレスの割当てを行う手法である（図 3）。

センサエージェントが OS 上で動作するため、高速なアドレスの切替えが可能となる。また、アドレスの切替えだけでなく、例えばエージェントが実ユーザのアクションを模倣するなどにより、実センサをより柔軟に制御することも可能でなる。センサエージェントは、対象の実センサのステータスを常時確認し、仮に任意の TCP セッションが設立中であった場合などには、アドレスの変更を行わないよう制御される。ただし、他の全プロセスの通信を阻害する攻撃などを受けた場合には一切の制御が行えなくなるため、他の方式と組み合わせるなどの、バックアップ体制を検討する必要がある。

以上の点を総合的に考慮して、本研究では NAT 方式及びエージェント方式の両形態での IP アドレス動的切替え方式を採用し、これらの形態を GHOST センサの設定によって切り替えられるように実装することとした。

4　事前調査

本研究では提案システムの実装に先立ち、提案システムが攻撃観測におよぼす影響について調査した。提案システムでは、すべての攻撃に対して実際の応答を行うのは分析センタ内にある実センサである。したがって、すべてのパケットは仮想センサと分析センタの間を通過することになり、その分の往復遅延が発生する。そこで本研究では、この通信時の往復遅延が攻撃情報の収集にどのような影響を与えるかを検証した。

筆者らは提案システムを用いて海外にも仮想センサを設置し、観測範囲を拡大させることを想定している。海外との間では数百ミリ秒という大きな値の遅延が発生する場合があるため、本評価では片道 500 ミリ秒の遅延を導入した環境で遅延が検体収集に与える影響を調査した。

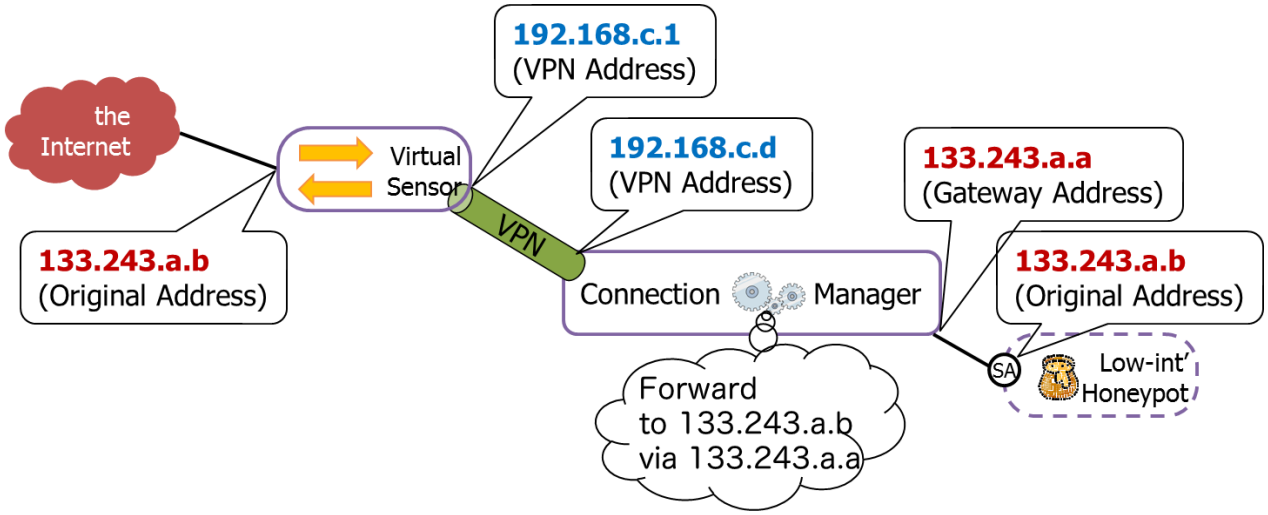

図 3　エージェント方式での動的 IP アドレス割当て

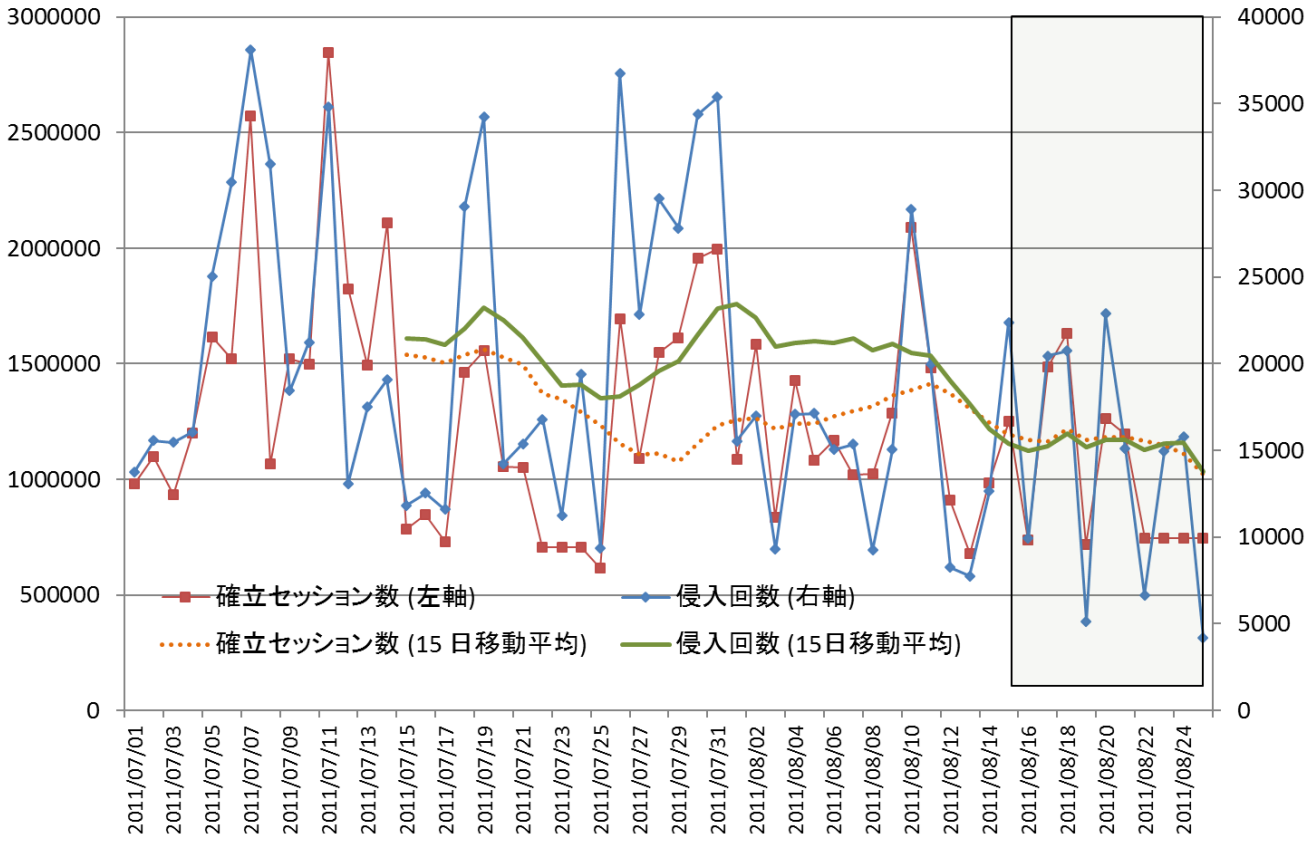

図 4　低対話型ハニーポットにおける攻撃観測状況

4.1　センサ・ゲート間の往復遅延が与える攻撃への影響

本評価では、Windows XP で実マシンとして構成される高対話型・低対話型ハニーポット（Nepenthes）で構成されるうちの低対話型ハニーポットに対して、その上流インターフェイス上に遅延発生器を導入し、意図的に遅延を発生させることで、提案システムと同様の環境を構築した。この状態で 2011 年 8 月 16 ～ 25 日の 10 日間にわたって観測を行い、検体取得数、被攻撃（エクスプロイト成立）回数、TCP セッション数が、無遅延の場合と比較してどのように変化するかを検証した。

図 4 は、低対話型ハニーポットにおける、2011 年 7 月 1 日から 8 月 25 日にかけての被攻撃回数及び TCP の確立セッション数を示したグラフである。なお、低対話型ハニーポットは、245 個の IP アドレスの観測を行っている。基本的に、高対話型・低対話型の各ハニーポット、ブラックホールセンサにかかわらず、ハニーポットは攻撃に対して受動的に待ち受けるため 1 日あたりに観測できる情報は、日によって大きく変動する。したがって、移動平均を求めて確認することとした。遅延発生器が設置された期間（8 月 16 日以降の網掛け部分）は平均的に 1 日あたり 120 万件程度の TCP セッション数、1.5 万件程度の被攻撃回数であることがわかる。これは遅延発生器導入前の 8 月 15 日以前よりは低いが、もとより低下傾向にあった攻撃数が、その傾向のまま低下を続けているととらえることもできる。

図 5 は、3 つの IP アドレスを用いて観測を行う高対話型ハニーポットを対象として、前述と同じ条件で観測をした際の、検体取得数及び確立した TCP セッション数を表している。高対話型ハニーポットにおいては、遅延発生器の導入後は、移動平均で 1 日あたりの検体取得数が 35 ～ 40 件、確立セッション数が 40 ～ 50 万件程度となっているが、これはおおよそ遅延発生器導入前の期間と同程度の規模であることが確認できる。

4.2　往復遅延に関する考察

2 種類のハニーポットセンサについて、片道 500 ミリ秒の遅延を導入したところ、15 日の移動平均で見たときに、遅延発生器導入前の期間とおおよそ同程度の攻撃を検出することが確認できた。仮に遅延が攻撃回数等に影響するのであれば、遅延発生器を導入した当日から急激な回数の低下を見せるはずであるが、各日の実測値で見ても、遅延発生器導入前と同程度の値を記録する日も多く見られている。このことから、仮想センサと分析センタ間の往復遅延は、攻撃の観測率

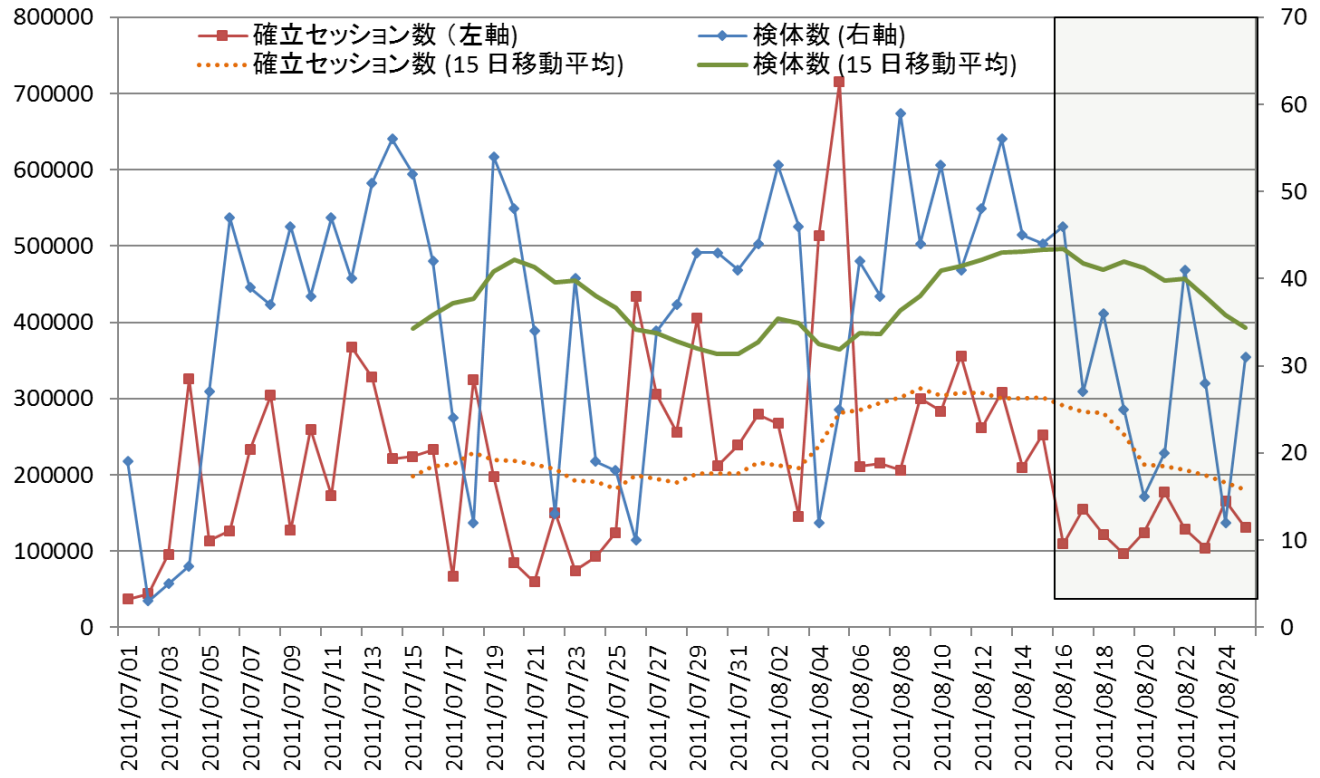

図 5　高対話型ハニーポットにおける攻撃観測状況

に大きな影響を与えないことがわかった。

5 評価

これまでの検討に基づいて GHOST センサのプロトタイプ実装を行い、小規模な観測環境を構築し、実際にインターネットに接続した上で実証実験を行った。この環境にはセンサとしてブラックホールセンサと低対話型ハニーポットを設置し、より新規の攻撃者（送信元 IP アドレス）に対して（ブラックホールセンサよりも高機能な）低対話型ハニーポットを用いる割当てルールとした。新規の送信元 IP アドレスには低対話型ハニーポットで対応し、それ以外の（既知の）攻撃者はブラックホールセンサに回す設定としているため、低対話型ハニーポットでは同一 IP アドレスから重複したマルウェア検体を収集する機会が減少する。

よって本評価作業では、実験環境の低対話型ハニーポットで同一のマルウェアが少ないこと、すなわち観測された検体のユニーク性についての評価を行った。また、GHOST センサの重要な目的の 1 つであるリソースの有効利用という観点で、センサ及び IP アドレスの使用率に関する評価を行った。

5.1 実験環境

実験環境の概要を図 6 に示す。

本実験では GHOST センサの有効性を確認するため、GHOST センサを用いた環境（GS 環境）と用いない環境（非 GS 環境）の 2 つを用意した。またセンサグループとして低対話型ハニーポット Dionaea（高優先度）とダークネットセンサ（低優先度）を用いた。GS・非 GS 環境のそれぞれには低対話型ハニーポットを 8 台、ダークネットセンサ 1 台が設置されている。観測に用いる IP アドレスについては、より類似した環境での比較を行うため単一のグローバルクラス C（/24 サブネット）アドレスを 4 つ（A、B、C、D の /26 サブネット）に分割し、GS 環境に A、C を非 GS 環境に B、D を割り当てている。GS 環境では GHOST センサの機能により、これらのアドレスが動的にセンサに割り当てられる。非 GS 環境では 8 台の低対話型ハニーポットにそれぞれ 1 つずつ静的な IP アドレスを割り当て、それ以外をブラックホールセンサに割り当てている。

本環境において 2013 年 11 月 19 日 0 :00 :00 から 11 月 20 日 23 :59 :59 までの 24 時間で攻撃観測を行った。なお、GS 環境における IP アドレス割当てのパラメータとして、各センサは IP アドレスの割当て後 300 秒で自動的に当該 IP アドレスをリリースする設定となっている。また、対処済データベースに登録された（既知ホストの）IP アドレスは登録後 5 時間で削除される設定となっている。

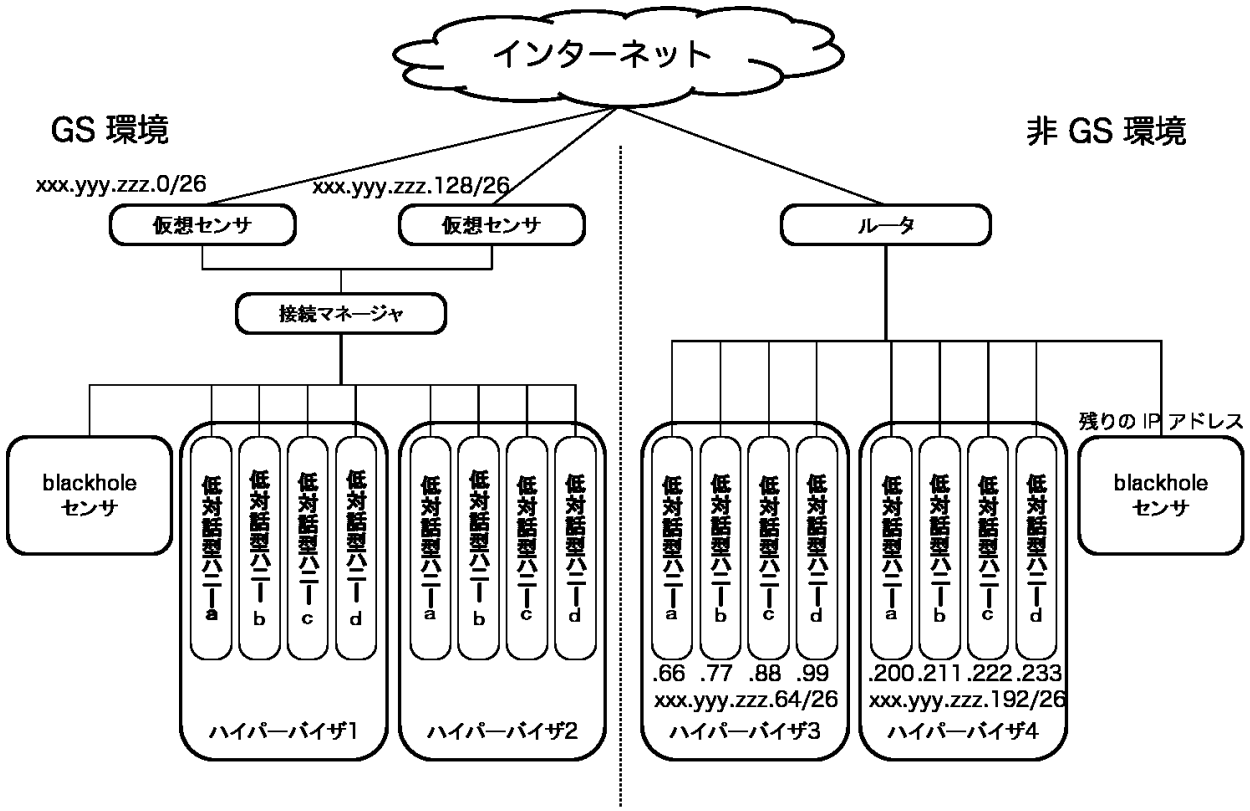

図 6　実験環境

5.2　評価 : 取得検体のユニーク性

本節では低対話型ハニーポット Dionaea で取得されたマルウェア検体のハッシュ値に着目し、取得された検体のユニーク性について検証する。なお、GS・非 GS 環境に設置した各 8 台の低対話型ハニーポットはそれぞれ独自に検体の収集を行っているが、他の 7 台では取得されていないハッシュ値を持つ検体のことをここではユニークな検体と定義する。参考として、GS 環境の各低対話型ハニーポット（d1 a ～ d2 d）及び非 GS 環境の各低対話型ハニーポット（d3 a ～ d4 d）のそれぞれにおいて実際に取得されたマルウェア検体とそのハッシュ値の内訳を表 1、表 2 に示す。

各表において、下線太字で示される検体は該当するハニーポットのみで取得されているユニークな検体である。GS、非 GS 双方の環境で取得された検体数とその中に含まれるユニーク検体数及びその割合は表 3 のとおりである。

GS、非 GS の各環境で取得された検体数が 33、37 と比較的近いのに対して、そのうちのユニーク検体数は 17（51.5 %）、9（24.3 %）と 2 倍近い差がある。反対に非ユニーク検体に着目すると 非 GS 環境では非ユニークな検体を延べ検体数の 76.7 % 取得しており、同じ攻撃元からの検体を（GS 環境と比較して）より重複して取得していることがわかった。

5.3　IP アドレス使用効率の評価

本実験では 1 つのクラス C（/24 サブネット）IP アドレス（256 IP アドレス）を 4 つに分割し、GS・非 GS 環境にそれぞれ 2 ブロック（128 IP アドレス）ずつ割り当てて観測を行った。GS 環境の 128 の IP アドレスがどの程度の時間、低対話型ハニーポットに割り当てられたかを接続マネージャのログから調査した結果を図 7 に示す。

図 7 では、各 IP アドレス（X 軸）が低対話型ハニーポットに割り当てられた秒数の総観測期間（24 時間 : 172,800 秒）に対する割合を示している。多少のばらつきはあるが、おおよそ 3 % から 5 % の間で一定して IP アドレスが使用されていることがわかった。これは、攻撃者が対象ネットワークの全体にわたってスキャンをした結果、攻撃先 IP アドレスが平均的にハニーポットに割り当てられたことを示している。なお 1 から 5 の IP アドレスの使用率がほかよりも高いのは、これらの IP アドレスが攻撃の対象となる機会が確率的に多いためである。

以上のことから、既存の手法では固定的にハニーポットに割り当てられた IP アドレスのみが攻撃観測に使用されてきたのに対して、本手法ではどのような IP アドレスでもハニーポットとして稼働できることが確認された。

表 1　GS 環境における取得検体

Honeypot	Hash
d1a	3c3011089708c7a49346f648f1e79384
	9b175f5f727bcf1153e1aaf99798556a
	4f37e1e3ab27feba48038ea03dc55901
	65de48b370a61412435074479c6219fc
d1b	3c3011089708c7a49346f648f1e79384
	9b175f5f727bcf1153e1aaf99798556a
	9521d5fe45b1211e886da8b7ba813ac3
	cc32d0ee45e3f69e4e9b689c8c01c01c
	4d56562a6019c05c592b9681e9ca2737
	ffb4628a96fa19abab9bbded0324fecd
	64b4345a946bc9388412fedd53fb21cf
	7867de13bf22a7f3e3559044053e33e7
d1c	3c3011089708c7a49346f648f1e79384
	8535926634662a4e332121a6d2b01032
d1d	3c3011089708c7a49346f648f1e79384
	eb073edcb3340705a0a45f1d14231d47
	a4619b7dc17f18ef00b714db37a0ef19
	cb4c05cae975d30d7cac15df3cdbfe3e
	64b4345a946bc9388412fedd53fb21cf

Honeypot	Hash
d2a	3c3011089708c7a49346f648f1e79384
	ebfaf4383932b3ef39f1b29e1e574459
	9a1f8268805f01a7c3e0bfce07111cf4
d2b	**92675d3f5d76e4170230d1c0294f7be9**
	4d56562a6019c05c592b9681e9ca2737
	e5db14583694d3ff53d3b0b9c95d82b0
	3c3011089708c7a49346f648f1e79384
d2c	3c3011089708c7a49346f648f1e79384
	b202f4b1bdbb2615bb579d64fecd76a6
	7a676b8a1ad9d1efdde6ad9b0a663960
	7867de13bf22a7f3e3559044053e33e7
d2d	3c3011089708c7a49346f648f1e79384
	76e669836f48491f118c8e41c678e230
	b7d4ed11a02cd3f4867299640e1e52a8

表 2　非 GS 環境における取得検体

Honeypot	Hash
d3a	3c3011089708c7a49346f648f1e79384
	e616b165d15a59d672918bf920d4faab
	c0fa3206395854b1eb55c47edd7011b5
	c443480243fbbd8cb11ade4ecdff1d45
	ffc8c1873be79006b4b221fe27e655e9
	7867de13bf22a7f3e3559044053e33e7
d3b	3c3011089708c7a49346f648f1e79384
	e616b165d15a59d672918bf920d4faab
	3c4351bc00f07b94d0fd189d2419d742
	c0fa3206395854b1eb55c47edd7011b5
	7867de13bf22a7f3e3559044053e33e7
d3c	3c3011089708c7a49346f648f1e79384
	e616b165d15a59d672918bf920d4faab
	c5862fe0aeb55594e1f74aa9cfbaa2a8
	c0fa3206395854b1eb55c47edd7011b5
	7867de13bf22a7f3e3559044053e33e7
d3d	3c3011089708c7a49346f648f1e79384
	e616b165d15a59d672918bf920d4faab
	a0194a481b12c590acd6bd8228b4c6d3
	c0fa3206395854b1eb55c47edd7011b5
	7867de13bf22a7f3e3559044053e33e7

Honeypot	Hash
d4a	3c3011089708c7a49346f648f1e79384
	e616b165d15a59d672918bf920d4faab
	207704c559f7b91f24b1b77f0f702da1
	7867de13bf22a7f3e3559044053e33e7
d4b	3c3011089708c7a49346f648f1e79384
	e616b165d15a59d672918bf920d4faab
	42801cfe875896daa5a6990b57567bad
	7867de13bf22a7f3e3559044053e33e7
d4c	3c3011089708c7a49346f648f1e79384
	e616b165d15a59d672918bf920d4faab
	114567ed87eb9723d7be3e9a66fd70d9
	7867de13bf22a7f3e3559044053e33e7
d4d	3c3011089708c7a49346f648f1e79384
	e616b165d15a59d672918bf920d4faab
	41c64356a9618a31785e505e5048047c
	7867de13bf22a7f3e3559044053e33e7

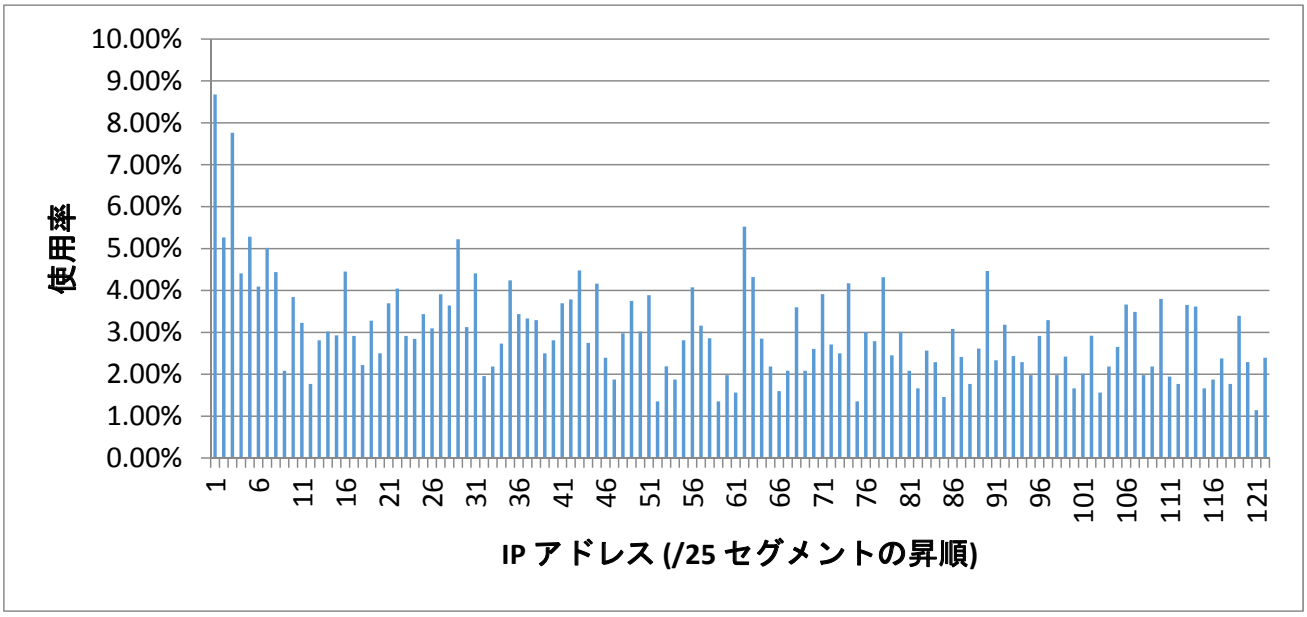

図 7　IP アドレスの使用率

表 3　両環境におけるユニーク検体取得率

	GS 環境	非 GS 環境
検体総数	33	37
ユニーク検体数	22	13
ユニーク検体率	66.7 %	35.1 %
非ユニーク検体率	33.3 %	64.9 %

表 4　ハニーポットマシンの使用効率

Honeypot	時間（秒）	稼働率（ /172800 秒）
d1a	64062.673	37 %
d1b	64062.200	37 %
d1c	63882.519	37 %
d1d	63882.670	37 %
d2a	63882.079	37 %
d2b	63882.976	37 %
d2c	64062.588	37 %
d2d	63882.710	37 %

5.4　マシン稼働率の評価

5.3 での IP アドレス使用率に関する評価と同様に、本節ではハニーポットマシンの稼働率に関する評価を行う。GHOST センサにおけるハニーポットマシンの稼働率は、ハニーポットに IP アドレスが割り当てられた時間を計測することで算出することができる。表 4 は、GS 環境における各ハニーポット（d1 a ～ d2 d）に IP アドレスが割り当てられていた時間の総観測期間（24 時間：172,800 秒）に対する割合を示している。

検証の結果、各ハニーポットマシンの稼働率はいずれも 37 % と一定していることがわかった。また、より詳細な調査で、1 台のハニーポットはおよそ 5 分から 10 分（平均 7 分 45 秒）に 1 回の頻度で IP アドレスが割り当てられている（攻撃対応をしている）こともわかった。このことから、既存の手法では対応する IP アドレスに攻撃が来ない限りハニーポットマシンは稼働せず、計算資源の無駄となっていたのに対して、本手法を用いれば一定の割合で稼働させることが可能であることが確認された。

しかし、マシンの効率的な使用という観点では、これらの稼働率がより 100 % に近いことが望ましい。したがって、IP アドレスとハニーポットマシン台数を適切な数に調整する必要があることがわかった。

6　おわりに

複雑化するネットワークシステムとその脅威に追随するために、いくつかのネットワーク観測プロジェクトが世界中で推進されているが、その運用にあたっては様々な問題を抱えている。ネットワーク観測システムの運用における問題の解決するため、本研究では能動的サイバー攻撃観測プラットフォーム GHOST センサを提案した。提案システムでは、仮想センサ技術を用いる一方で、様々な実センサに対して動的にアドレスを割り当てることで、柔軟な攻撃観測を可能とする設計を行った。また実装に先立つ評価として遅延が検体収集に与える影響を調査し、センサ・ゲート間の往

復遅延が攻撃の観測に有意な影響を与えないことを確認した。さらに、クラスCのIPアドレスと8台の低対話型ハニーポット等で構成される評価環境を構築し、割当てルールのとおりに新規の検体が収集されることを確認し、本手法の有効性を示した。

現在GHOSTセンサはNICTERの観測網に組み込まれ、本格的な運用が行われているところである。今後は、より柔軟に「見たい攻撃を最適なハニーポットで見る」ことができるよう、効果的なセンサの割当てルールを適用していく予定である。

【参考文献】

1 WOMBAT : Worldwide Observatory of Malicious Behaviors and Attack Threats. http://www.wombat-project.eu/.
2 PREDICT : the Protected Repository for the Defense of Infrastructure Against Cyber Threats. http://www.predict.org/.
3 SANS Internet Storm Center. http://isc.sans.org/.
4 F. Pouget, M. Dacier, and V.H. Pham. Leurre.com: On the Advantages of Deploying a Large Scale Distributed Honeypot Platform. E-Crime and Computer Conference (ECCE'05) , 2005.
5 K. Nakao, D. Inoue, M. Eto, and K. Yoshioka, "Practical Correlation Analysis between Scan and Malware Profiles against Zero- Day Attacks Based on Darknet Monitoring," IEICE TRANSACTIONS on Information and Systems, vol.92, no.5, pp.787–798, 2009.
6 Nepenthes Development Team. http://nepenthes.carnivore.it/contact.
7 H. Project, "Dionaea honeypot." http://dionaea.carnivore.it/.
8 D. Moore. Network Telescopes: Tracking Denial-of-Service Attacks and Internet Worms around the Globe. In 17th Large Installation Systems Administration Conference (LISA'03) , 2003.
9 M. Bailey, E. Cooke, F. Jahanian, J. Nazario, and D. Watson, "The Internet Motion Sensor: A distributed blackhole monitoring system," Proceedings of the 12th ISOC Symposium on Network and Distributed Systems Security (NDSS) , pp.167–179, Citeseer, 2005.
10 L. Spitzner. Know your enemy: Genii honeynets, 2003.
11 X. Jiang and D. Xu, "Collapsar: A vm-based architecture for network attack detention center," Proceedings of the 13th conference on USENIX Security Symposium-Vol.13, pp.22, USENIX Association, 2004.
12 M. Vrable, J. Ma, J. Chen, D. Moore, E. Vandekieft, A.C. Snoeren, G.M. Voelker, and S. Savage. Scalability, fidelity, and containment in the potemkin virtual honeyfarm. In ACM SIGOPS Operating Systems Review, vol.39 (5) , pp.148–162. ACM, 2005.
13 C. Leita and M. Dacier, "Sgnet: a worldwide deployable framework to support the analysis of malware threat models," Seventh European Dependable Computing Conference, pp.99–109, IEEE, 2008.
14 川古谷裕平 , 岩村誠 , 伊藤光恭 . Dense ship: サーバ型ハニーポット用仮想マシンモニタ (情報通信システムセキュリティ) . 電子情報通信学会技術研究報告 , vol.111, no.82, pp.63–68, 2011.

衛藤将史　(えとう　まさし)

ソーシャルイノベーションユニット
セキュリティ人材育成研究センター
研究マネージャー
博士 (工学)
ネットワークセキュリティ、マルウェア解析、
ネットワーク運用