異種センサ統合型ネットワーク観測プラットフォームの提案

衛藤将史† 井上大介† 鈴木 未央† 中尾康二†

† 独立行政法人 情報通信研究機構
184-8795 東京都小金井市貫井北町 4-2-1

あらまし 複雑化するサイバー攻撃に対応するため，さまざまなネットワーク観測技術が提案されているが，その運用にあたっては，IP アドレス空間の確保の難しさや，メンテナンスコスト，アドレスがブラックリストに載ることによる長期運用の難しさなどの問題が存在する．本稿では，これらの問題に対応するため，仮想センサ技術を用いて多様なセンサを管理する，統合ネットワーク観測プラットフォームを提案する．提案手法は L3 の透過プロキシとして動作する仮想センサを遠隔地に配置する一方で，センタ側で多種の実センサを統合的に管理することで，効果的な攻撃観測を狙いとする．本稿では，本プラットフォームの設計および実現可能性の検討を行う．

Proposal of Multipurpose Network Monitoring Platform

Masashi Eto† Daisuke Inoue† Mio Suzuki† Koji Nakao†

†National Institute of Information and Communications Technology (NICT)
4-2-1, Nukui-Kitamachi, Koganei, Tokyo, 184-8795, Japan

Abstract There have been several network monitoring projects launched to fight against cyber threats on the Internet. Meanwhile, we are facing some difficulties of operations of network monitoring system such as; difficulty of assigning much IP addresses enough for global observations, heavy burden of physical or logical maintenance of sensor system, obsolescence of the IP addresses due to be detected by attackers as ”monitored”. In order to solve these problems, this paper proposes a multipurpose network monitoring platform that can run any type of sensors on it with applying the virtual sensor mechanism and the dynamic address assigning technique. This paper presents the design of the platform and a preliminary evaluation of the proposed methods.

1 はじめに

深刻化するサイバー攻撃に対応するため，さまざまなセキュリティ対策技術の研究開発が世界中で進められている．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を把握するため，広域な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いる [1, 2, 3, 4, 5]．これらのプロジェクトからもわかるとおり，サイバー攻撃への対策としては，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が非常に重要である．その一方で，サイバー攻撃の手法も複雑化の一途を辿っており，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，技術の発展にともなって柔軟にその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さまざまな攻撃情報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] が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モニタリング [7] 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，ドライブ・バイ・ダウンロード攻撃への対策の一つとして，悪意の Web サーバを定期的に巡回探索する Web クローラもさまざまな組織において研究開発されている．これらのセンサは日本国内だけでなく，海外も含めて広く設置する (または海外組織と密な情報共有を行う) ことで初めて広域ネットワークでのサイバー攻撃の発生状況を把握す

ることが可能となる．

しかし，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，さまざまな課題が存在する．特に，上述の [1, 2, 3, 4, 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，ブラックホールモニタリング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，精度の高い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) を用いることが望ましい．しかし，国際的に見ると多くの国では，一部の先進国のように IPv4 アドレス資源が豊富ではないため，このように広大なダークネットによる観測を行うことが困難である．よって，仮に 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ることが望ましい．

ハニーポット運用の難しさ　ブラックホールモニタリング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にて，より深い攻撃情報を収集することが考えられる．しかし，囮ホスト，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，比較的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にメンテナンスコストが大きくなりがちである．

長期運用による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，攻撃者側に警戒心を抱かせて当該 IP アドレスがブラックリストに載り，効率的な観測が行えなくなる場合がある．ハニーポットでは，攻撃対象リストから外されてマルウェア検体の収集など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 Web サイトの運用者によってブラックリストに登録され，通常の Web アクセスも困難になる場合がある．

このような課題を受け，本論文では，物理的なマシンおよび IP アドレス資源を有効に用いながら，安定的・継続的にセンサ網を運用することを目的とした，異種センサ統合型ネットワーク観測プラットフォームを提案する．提案手法は，主な機能として仮想センサ技術とセンサへの動的なアドレス割り当て機構を有しており，これにより，上述のさまざま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，第 2 章において，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，第 3 章で本研究の提案手法である異種センサ統合型ネットワーク観測プラットフォームの構成と機能を紹介する．第 4 章では，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事前に調査することで，提案手法の実現可能性について検討する．最後に，第 5 章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，ブラックホールモニタリングを主とする [8, 3, 4] 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 [9, 10, 11, 12, 13]．

その中でも，Collapsar [10] 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 [11] は，Collapsar の機能に加えて，特定の IP アドレス宛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機能を有している．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理論的に有することから，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 [12] 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であっても，センタ側の実サーバにクエリを転送することでリアルタイムに応答することを可能としている．

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であるといえる．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百程度である．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においては，仮にこれらの運用技術を用いても多数の攻撃が到来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ハニーポット運用を対象としたもの，すなわちリモートエクスプロイト攻撃を対象と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．

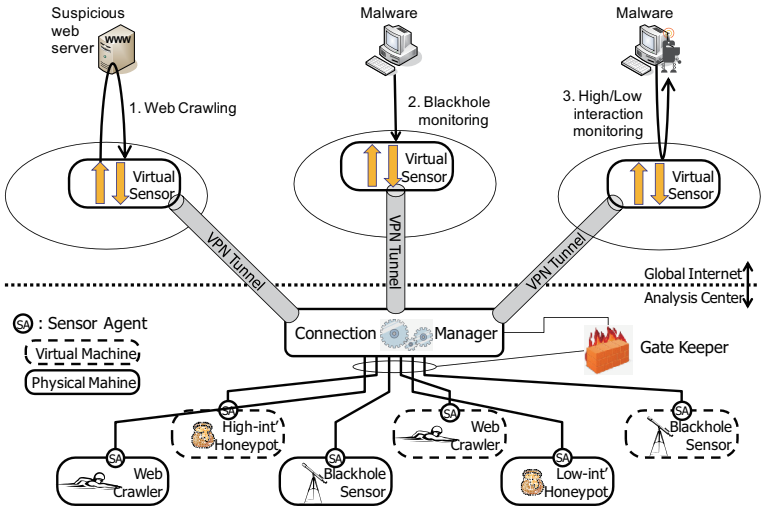

図 1: 異種センサ統合型ネットワーク観測プラットフォームの概要

3 異種センサ統合型ネットワーク観測プラットフォーム

前節で挙げた関連研究における課題を受けて，本論文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，さまざま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ためのシステムを提案する．

3.1 概要

提案システムの概要を図 1 に示す．提案手法では，Collapsar 等と同様に，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-int' High-int' Honeypot および Blackhole Sensor) する一方，観測拠点には L3 プロキシ機能を持つ仮想センサ (図 1：Virtual Sensor) 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 (および 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．

提案手法の大きな特徴は，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対して，さまざまな運用ポリシ (第 3.4 にて詳述) にしたがい，動的な IP アドレスの割り当てを行い，能動的な攻撃観測を行う点である．

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，提案手法では分析センタ内部ですべてのトラフィックを集中監視する事が可能となる．

3.2 主要コンポーネント

提案手法における主要なコンポーネントとその機能を以下で述べる．

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，自身宛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宛先に送信する．

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および各種の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できるのが，既存手法 ([11, 13]) と異なる点である．その理由は，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，提案手法においては，IP アドレスの反映を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．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．そのほかに，任意の Web サーバへのアクセスのようなユーザの行動をセンサエージェントにエミュレートさせることで，より本格的なクライアントマシンを装うことが可能となる．

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，接続マネージャは実センサの稼働状況や攻撃の種類などに応じて，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．このような調整を行うため，接続マネージャはセンサエージェントからの定期レポートを受け，アドレス変更の要否を検討した上で，必要に応じてセンサエージェントに命令を送信する．

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一カ所に集約することで，二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　アドレスの動的割り当て機能の検討

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 アドレスの割り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 [11]，DenseShip [13] 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り当てを行っている．これらの主目的は IP アドレスの動的な割り当てではないが，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 アドレスの割り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本手法は適さない．

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り当ての変更が可能となる利点がある．しかし，実センサが高対話型ハニーポットの場合，攻撃対象とされた IP アドレスと実センサ上の IP アドレスの違いを攻撃者に気づかれる可能性があるため，本手法も適切とはいえない．

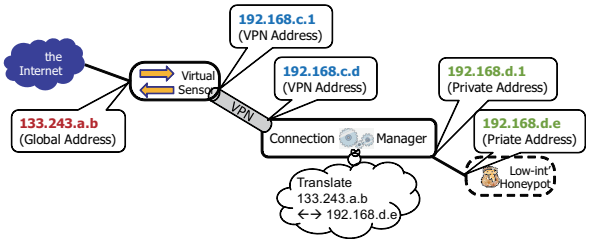

図 2: NAT 方式での動的 IP アドレス割り当て

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り当てを変更する手法である．これは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である．

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 アドレスの割り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り替えが可能となる．また，アドレスの切り替えだけでなく，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が可能となる．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，攻撃者によって他の全プロセスの通信を阻害するなどの攻撃を受けた場合には，実センサの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．

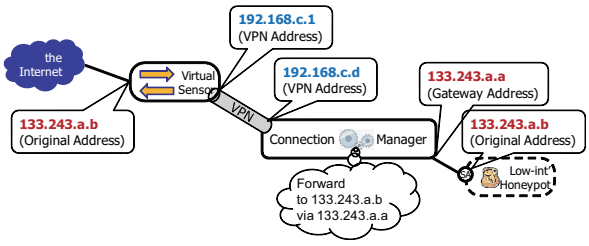

図 3: エージェント方式での動的 IP アドレス割り当て

以上の点を総合的に考慮して，本研究では提案手法の第一歩としてエージェント型の IP アドレス動的切り替え方式を採用することとした．

3.4 能動的ネットワーク観測の実現

提案手法では，実センサへの IP アドレス割り当てポリシを工夫することで，例として以下のように柔軟な攻撃観測が可能となり，より詳細な情報を得られる可能性がある．

新規ホストの詳細解析
新規の攻撃元 IP アドレスからのパケットを受信した場合に当該パケットを高対話型ハニーポットに転送し詳細な分析を行う．

サービス対応ルーティング
各実センサ上で動作させるサービスを分散させておくことを前提として，攻撃受信時に対象サービスに応じて対応実センサのアドレス割り当てを変更することで，実センサのマシンリソースを効率的に使用する．

二次感染状況の観測
外部からの攻撃だけでなく，感染状態の実センサの二次攻撃先アドレスを他の実センサに割り当てることで，二次感染の状況を詳細に確認する．

Web クローラ等のブラックリスト対策
Web クローラの取得サンプル数の減少時に IP アドレスを変更することで，定常的により多くのサンプルを収集する．

能動的アドレス割り当て
ブラックホールセンサで観測されたスキャンパターンから当該攻撃元ホストからの今後のスキャン対象アドレスを予測し，それを高対話型ハニーポットに割り当てることで効率的に検体等を収集する．

DDoS 攻撃の回避
観測対象の IP アドレスのいずれかが DDoS 攻撃を受けた場合には，処理負荷の高い高対話型ハニーポットからブラックホールセンサにアドレス割り当てを変更することで，被害を抑えながら観測を継続する．

提案手法では，以上の機能を接続マネージャに導入することで，より柔軟な攻撃観測の実現を目指す．なお，長期的に同一のセンサでの観測を行う必要のある IP アドレス (例えば 5 年間にわたる攻撃傾向を観測している IP アドレスなど) については，割り当ての対象から外す予定である．

4 事前調査

本節では，提案手法が攻撃観測におよぼす影響を実装に先立って調査する．提案手法では，攻撃に対する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，提案手法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検討している．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することとした．

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ハニーポット，および Nepenthes [6] で構成される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挿入して意図的に遅延を発生させることで，提案手法と同様の環境を構築した．この状態で 2011 年 8 月 16 日から 8 月 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，7 月 1 日から 8 月 25 日にかけての被攻撃回数および TCP の確立セッション数を示したグラフである．この検証で対象となった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・ブラックホール型にかかわらず，ハニーポットは攻撃を受動的に待ち受けるものであるため 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．したがって本評価では，移動平均によって影響を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 1,200,000 件程度の TCP セッション数，15,000 件程度の被攻撃回数であることがわかる．これは設置前の 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捉えることもできる．

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，検体取得数および確立した 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 400,000 〜 500,000 件程度となっているが，これはおおよそ前の期間と同程度の規模であることが確認できる．

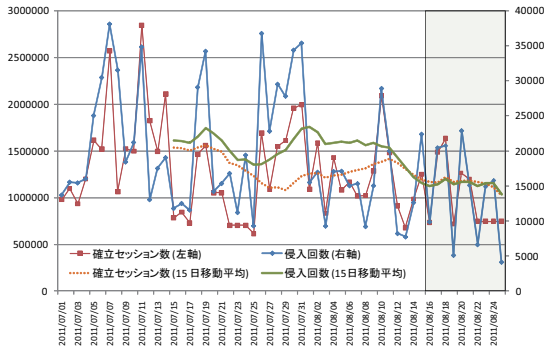

図 4: 低対話型ハニーポットにおける攻撃観測状況

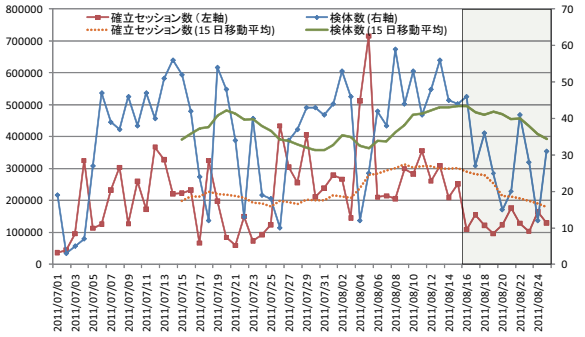

図 5: 高対話型ハニーポットにおける攻撃観測状況

4.2 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，攻撃の観測率に大きな影響を与えないことがわかった．

特に検体取得数は，日によってばらつきが非常に大きいため今回の調査では 15 日間での移動平均を確認に用いたが，今後も継続的に、より長期的な影響を調査する必要がある．また，今回は待ち受け型ハニーポットを調査の対象としたが，Web クローラなどの他の形態のセンサに与える影響についても調査する必要がある．今後のさらなる検討として，ハニーポットでは，ブラックホールモニタリングと比較してトラフィック量が増大するため，トラフィック量がセンサ・ゲート間の回線に与える影響についても，確認が必要である．

5 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さまざまな問題が存在する。ネットワーク観測システムの運用における問題を解決するため，本研究では異種センサ統合型ネットワーク観測プラットフォームを提案した。提案システムでは、仮想センサ技術を用いる一方で、さまざまな実センサに対して動的なアドレス割り当てを行い、柔軟な攻撃観測を実現する設計を行った。また実装に先立つ事前評価として遅延発生器を用いた調査を行い，センサ・ゲート間の往復遅延が攻撃の観測に明示的な影響を与えないことを確認した。今後は第 4.2 節で挙げたいくつかの検討事項の調査を行いつつ，提案手法のプロトタイプ実装，機能的な有効性確認に取り組む予定である．これと並行してシステムの実運用を行いながら、順次、海外を含めて観測拠点の拡大を進める予定である．

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] 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.

[8] M. Bailey, E. Cooke, F. Jahanian, J. Nazario, and D. Watson. The Internet Motion Sensor: A distributed blackhole monitoring system. In *Proceedings of the 12th ISOC Symposium on Network and Distributed Systems Security (NDSS)*, pp. 167–179. Citeseer, 2005.

[9] L. Spitzner. Know your enemy: Genii honeynets, 2003.

[10] X. Jiang and D. Xu. Collapsar: A vm-based architecture for network attack detention center. In *Proceedings of the 13th conference on USENIX Security Symposium-Volume 13*, pp. 2–2. USENIX Association, 2004.

[11] 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.

[12] C. Leita and M. Dacier. Sgnet: a worldwide deployable framework to support the analysis of malware threat models. In *Seventh European Dependable Computing Conference*, pp. 99–109. IEEE, 2008.

[13] 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.