2-2　インシデント分析センターnicterのシステム実装と社会展開

2-2　An Incident Analysis Center "nicter" and its Social Commitment

衛藤将史　　高木彌一郎
ETO Masashi and TAKAGI Yaichiro

要旨

インターネット上で深刻な社会問題となっている、マルウェアを中心としたさまざまなセキュリティインシデントに対し、筆者らはインシデント分析センターnicterの研究開発を推進している。nicterは、広域なネットワーク観測によるインターネット全体の攻撃傾向を把握する一方で、大規模なマルウェア検体の収集と完全自動解析を行い、これらの結果からインターネット上で発生したインシデントの原因を特定するマクロ-ミクロ相関分析を世界に先駆けて開発した。本稿では、nicterを構成する各コンポーネントのシステム設計を詳述する。また、nicterおよびその派生技術は、さまざまな形態での社会展開が進められており、それらの事例についても紹介する。

We have been developing the Network Incident analysis Center for Tactical Emergency Response (nicter), whose objective is to detect and identify propagating malwares. The nicter mainly monitors darknet, a set of unused IP addresses, to observe global trends of network threats, while it captures and analyzes malware executables. By correlating the network threats with analysis results of malware, the nicter identifies the root causes (malwares) of the detected network threats. This paper describes the system architecture of each component in nicter. Additionally, this paper reports the achievements of the nicter and its derivational systems that have been practically introduced to other organizations as an actual social commitment.

[キーワード]
ネットワーク観測，マルウェア解析，相関分析，システム，社会貢献
Network monitoring, Malware analysis, Correlation analysis, System architecture, Social commitment

1　はじめに

インターネットの一般化と同時に社会問題となったさまざまなセキュリティ上の脅威は、インターネット上で提供されるサービスの多様化にともない、増大化、複雑化の一途を辿っている。例えば、Webサービスに対する不正アクセスやサービス不能（DoS）攻撃、個人情報や組織の機密情報の漏洩、大量のスパムメールが誘導するフィッシングなど、多種多様なセキュリティインシデント（セキュリティ事故）が日々発生しており、その多くはユーザのマシンに感染したマルウェアが原因の一端を担っている。このような状況への打開策として、情報通信研究機構（NICT）では、インターネットの広範囲に影響を及ぼすセキュリティインシデントの早期発見、原因究明、対策法の導出を目的とする。インシデント分析センターnicter（Network Incident analysis Center for Tactical Emergency Response）の研究開発を進めている[1]-[3]。

nicterは、広域のダークネット観測[4]-[8]によって収集したイベントを解析し、その中からインシデントを検出するマクロ解析システムと、マルウェアの検体を収集・解析して、それらの挙動を抽出するミクロ解析システム[9]-[16]という2つの解析パスを持つ（図1）。これら2つのシステム

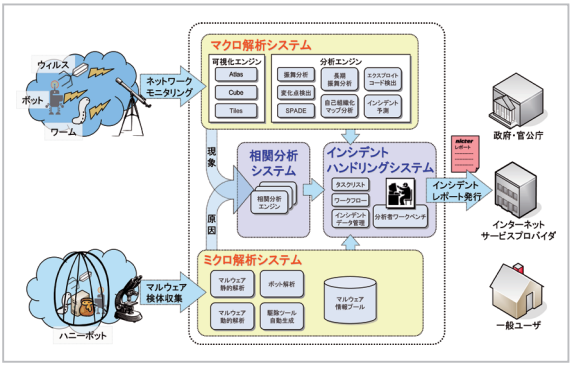

図1 nicterの全体像

から導き出された解析結果は、相関分析システムにおいてその相関関係が分析され、インシデントの「現象」と「原因」の対応付けが行われる。言い換えると、マクロ解析システムではネットワーク上で発生しているインシデントの現象を捉えることができ[17]、一方、ミクロ解析システムではインシデントの原因と考えられるマルウェアの挙動を把握できるため[18]、双方の解析結果を照合することで、発生中のインシデントの原因特定が可能となり[19]、さらに、特定されたマルウェアに応じた対策導出にも繋げることができる。マクロ解析システム、ミクロ解析システム、相関分析システムそれぞれの解析結果は、分析者に統合的なWebインターフェイスおよび可視化インターフェイスを提供するインシデントハンドリングシステムに集約され、最終的には分析者によってインシデントの詳細なレポーティングが行われる。

ここでは実際に、nicterが2010年7月9日にSIPサーバへの攻撃を検知した事例を紹介する。図2は、2010年4月1日から12月31日の間に

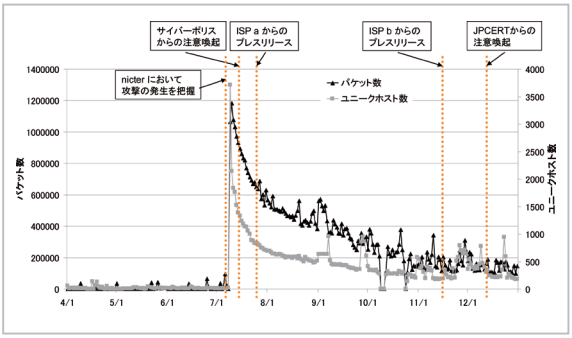

図2 ダークネット観測によるSIPサーバへの攻撃検知(2010/04/01～2010/12/31)

nicterのダークネット観測網で観測された、5060/UDPへの攻撃を行ったホスト数およびパケット数の統計データである。本事例では、7月9日に当該ポート番号への攻撃が急増しているが、これはIP電話の不正利用を目的として、セキュリティ対策が不十分なVoIP/SIPサーバを探索するための挙動である。nicterでは本事象を早期に検知した上で原因を分析・特定し、関連組織への情報提供を行っており、その後にISPなどからユーザに対して注意喚起が行われることとなった。なお、本事例ではnicterだけでなくサイバーポリスも同日に同様の攻撃を検知しており、7月14日に注意喚起を行っている。

以上のように、nicterは独自の広域ネットワーク観測網とマルウェア対策技術を用いることで、早期のインシデント検知とその原因特定を行うことを可能としている。

筆者らは「社会に役立つ技術の開発」を目的として極めて実体的な研究開発に5年以上にわたり取り組んできた。その結果として、nicterで培われた技術は実社会への技術移転や情報提供など、さまざまな形で結実している。本稿では、nicterを構成する各コンポーネントのシステム設計を詳述するとともに、さまざまな形態での社会展開が進むnicterとその派生技術に関する成果事例を紹介する。

2 nicterの概要

nicterは、広域のネットワークトラフィックを観測することによってイベントを解析しインシデントを検出・分析するマクロ解析システムと、マルウェアの検体を収集・解析して、それらの挙動を抽出するミクロ解析システム、これら2つの解析結果を分析し、インシデントとマルウェアの挙動を対応づけする相関分析システムによって構成される(図1)。

マクロ解析システムでは、国内外の組織に分散されたセンサによってダークネットの観測を行っている。ダークネットとは、インターネットに向けて公開されているIPアドレスのうち、未使用のアドレスによって構成されたネットワークであり、その規模は合計すると現在、約14万のIPアドレスとなる。ダークネットには、これらのIPアドレ

スを使用する通常のサーバやクライアント等のホストが存在しないため、ここで観測されるすべてのトラフィックは不正な通信、あるいは機器の設定ミスによってもたらされたものと見なすことができる。これに加えて、その設定の容易さから、ダークネットは観測範囲の大規模化とマルウェアからのスキャン（感染拡大活動）を観測するのに最適な手法であるといえる。特に、ダークネットにおいて受信されるパケットに対して一切の応答を行わず、到来するパケットを完全に受動的に記録のみを行う手法はダークネットにおけるブラックホールモニタリングと呼ばれ、nicterにおいてもこの手法による観測をもっとも大きな範囲で行っている。ここで収集されたトラフィックは攻撃元のホスト毎に、複数の分析エンジンによって解析され、各ホストが持つ攻撃の特徴抽出などが行われる。

一方で、ミクロ解析システムでは、ハニーポット、ダミーメールアカウント、Webクローラ等の手法を用いてマルウェアの検体収集を行っている。ここで収集されたマルウェア検体はマルウェア動的・静的解析システムに投入され、それぞれのマルウェアの挙動などの特徴抽出が行われる。

さらに、マクロ・ミクロ双方の分析結果はマルウェア情報プール（MNOP：Malware kNOwledge Pool）と呼ばれる統合データベースにすべて蓄積される。マクロ-ミクロ相関分析では、NemeSys（NEtwork and Malware Enchaining SYStem）がMNOPに対して効果的なクエリを行うことで実現される。NemeSysはMNOPに蓄積されたマクロおよびミクロ解析結果を検索し、マクロ解析システムにおいて検知された現象に対する原因を特定する役割を担う。具体的には、マクロ解析システムで特定のポート番号に対するトラフィックが急増した場合に、NemeSysはマクロ-ミクロ相関分析によって、その現象を引き起こした可能性の高いマルウェアの名称をリストとして出力する。このようにインシデントに対する原因を特定することで、インターネットにおいて現在流行している攻撃手法や、未知のマルウェアの急激な感染拡大といったインターネット全体の傾向を把握することが可能となる。

最終的に、人間のオペレータがインシデントハンドリングシステム（IHS）を用いてこれらの結果の確認作業を行った上で、インシデントレポートとして関連組織等に連絡される。

3　マクロ解析システム

マクロ解析システムは主に、広域に分散配置されたセンサ群と複数の可視化エンジン、分析システムによって構成されている。センサは各地のダークネットを主にブラックホールモニタリングによって観測しており、ここで得られたトラフィックはすべて分析センターに集約される。分析センターでは、収集されたトラフィックはリアルタイムの可視化エンジンを用いて可視化され、マルウェアからの顕著な攻撃を検出すべく、オペレータが目視による確認を行っている。その一方で、自動分析エンジンが新規の攻撃パターンやトラフィックの急増といったセキュリティイベントの自動検出を行い、必要に応じて分析結果をデータベースに格納する。

nicterでは現在、/16、/24等のサブネットを持つ複数のネットワークをブラックホールモニタリングによって観測しており、ここではTCPのSYNパケットやICMPのecho requestといったマルウェアによるスキャントラフィックが主に検出されている。その他にも、低対話型ハニーポットと呼ばれる、攻撃観測センサが配置されている。

3.1　データバスアーキテクチャ

インシデント対応を効果的に行うためには、得られたデータから疑わしいイベントを見つけ出し、その対策手法を迅速に導出することが重要である。このようなリアルタイム分析を実現するために、nicterでは複数の分析エンジンやデータベースに対して効率的にデータを提供するため、IPマルチキャストを利用した独自のデータ配送手法（データバスアーキテクチャ）を設計・構築した。

図3に示されるデータバスシステムでは始めに、センサモジュールにおいて取得された各パケットを分析に最低限必要となるデータ（IPヘッダ、TCPヘッダ、タイムスタンプ、パケット長等）によって構成される特定のフォーマットに変換した上で、分析センターに配置されたゲートモジュールに、VPN回線を通じて送信する。ゲートモジュールは集約されたパケットをUDPパケットと

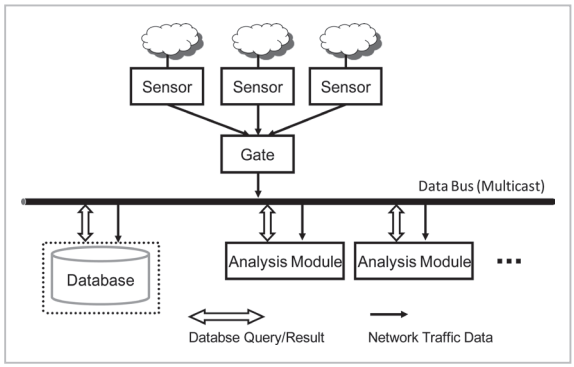

図3 データバスアーキテクチャ

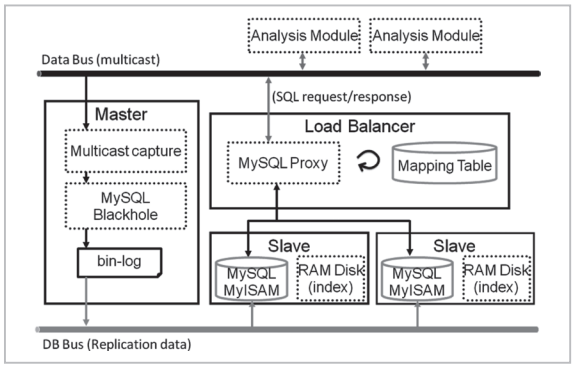

図4 MacS DB

して独自のセグメント（データバス）にマルチキャストを用いて送信する。このような構成を用いることにより、nicter ではすべての分析エンジンおよびデータベースが同時に分析対象となるデータを取得することが可能となったほか、トラフィック量の増加により各システムの負荷が増大した場合にも、分析エンジンやデータベースを追加することで容易にシステムのスケーラビリティを向上させることが可能となった。

3.2 MacS DB

3.1 のデータバスアーキテクチャは、リアルタイムな分析を行うエンジンに迅速にデータを配送するために構築されたが、いくつかのエンジンはリアルタイムではなく、一定期間（数分間、あるいは数時間）に蓄積されたデータをバッチ的に処理することでイベント分析を行っている。このような分析エンジンにとっては、データバスのようなリアルタイム配送システムではなく、長期間のデータを蓄積したデータベースシステムが適している。一方で、ダークネット観測が未使用の IP アドレスを観測対象としていることから、通常のサーバやクライアントホストが使用するライブネットワークと比較すれば相対的にトラフィック量は少ないといえるが、すべてのパケットを収集・蓄積するには通常のデータベースでは高負荷により十分に機能させることが困難である。よって nicter では、すべてのパケットをリアルタイムに蓄積するため、特別な工夫が施されたデータベースシステム（MacS DB）を構築した。

本システムの概要図を図 4 に示す。本システムは、データバスからトラフィックデータを取得しデータベースに挿入するマスタ、マスタからデータを複製（レプリケーション）し分析モジュールからの参照要求に対応するスレーブ、スレーブの負荷分散かつ参照要求とスレーブの対応付けをマッピングテーブル情報から行うロードバランサで構成される。また DB バスは、データバス上に流れるトラフィックデータとレプリケーションにより発生するネットワークトラフィックとを分離するために構成した。日々蓄積されていく大量のデータを 1 つのデータベースで管理していくことは効率的ではない。本システムでは、センサ毎にデータベースを作成し、さらに日毎にテーブルを作成・管理する。

一般的にデータベースの負荷分散を行うためには、更新と参照を分離させる事が多い。本システムにおいても、トラフィックデータを取得し挿入するマスタと参照要求に対応するスレーブに機能を分離することによりそれぞれの負荷を分散させる設計とした。本システムで採用したオープンソースである MySQL には、Blackhole と呼ばれるテーブルエンジンの選択が可能である。Blackhole エンジンにはストレージ機構が存在しないため全ての INSERT 文は破棄される。しかし、MySQL サーバは Blackhole エンジンに対するクエリを通常通りログファイルに書き出すため、レプリケーションによりスレーブ側でそのクエリを実行できる。本システムでは、マスタで Blackhole エンジンを指定することにより、インデックスの更新やテーブルにデータを挿入する負荷を排除した。またマスタでは、レプリケーションに必要なバイナリログの設定を行った。この設定により発行される SQL 文は、バイナリログファ

イルに追記され、レプリケーション機能によりスレーブ側で実行される。したがって、マスタはデータバスからトラフィックデータの取得に専念でき、マスタにおける高速性の要件を満たすことができる。

これらの機能に加えて、スレーブのI/O負荷低減のためにデータベースのインデックス領域をRAMディスク上に配置するなどの工夫を施すことで、MacS DBは最大で65,000pps（packet per second）という高速なデータ挿入処理が可能となった。これはゲートのデータ配信速度性能が最大でも約50,000ppsであることから、十分な性能であるといえる。

4　ミクロ解析システム（MicS）

ミクロ解析システムは、取得されたマルウェアの特徴や挙動を把握するために、完全に自動化された詳細な動的・静的マルウェア解析を行う。前述したとおり、nicterでは複数種類のハニーポットによってマルウェア検体を収集しており、これらのマルウェアがミクロ解析システムに投入され、最終的に分析結果はミクロ解析システム用のデータベースであるMicS DBに蓄積される。ミクロ解析システムでは、単一の解析セットで1検体をおよそ5分から10分程度（1日当たり150から250検体）で解析する能力を持つ。現在、nicterではこの解析セットを複数配置しており、合計で約2,000検体を1日で解析することが可能である。

4.1　マルウェア検体収集

前述のとおり、マルウェアの検体収集のため、nicterでは高対話型、低対話型ハニーポットやWebクローラなどの複数のハニーポットを運用している。高対話型ハニーポットの1つとして、nicterでは（仮想マシンなどではなく）実マシンにおいて通常のホストとして振る舞うハニーポットを構築した。このハニーポットは、マルウェア（特にボット）に侵入された場合に当該ハニーポットとボットネットの命令サーバ（C&C：Command and Control）サーバとの通信を観測することを目的の1つとしている。そのために、当該ハニーポットが送受信するすべてのメッセージは自動的に監視サーバに記録されると同時に、人間のオペレータによって常時監視されており、マルウェアのさまざまな挙動を把握することが可能となっている。なお、ハニーポットがマルウェアに感染した場合には、当該ハニーポットはインターネット上の他のホストに二次感染を試みる可能性がある。これを防ぐため、当該ハニーポットの前段にはIDSが設置されており、C&Cメッセージ以外の不審な通信を検知し、必要に応じてハニーポットのハードディスクイメージを自動的に復旧する機構を備えている。さらに、ハニーポットがマルウェアに感染した際には、当該ハニーポットは任意のタイミングで再起動を実施することで、ディスクイメージの再初期化をすることが可能となっている。また、再起動プロセスの中では、感染したハードディスクとオリジナル（感染前の）ディスクとのイメージ比較を行い、実行可能型のファイルのみを抽出することでマルウェア検体の取得も行われている。以上の技術によりnicterの高対話型ハニーポットでは、安全なマルウェアの挙動の観測とマルウェア検体の取得を行っている。

5　マクロ-ミクロ相関分析システム（NemeSys）

マクロ-ミクロ相関分析システム（NemeSys）は、マクロ解析システムにおいて観測された攻撃をより詳細に分析し、その原因を特定することを目的として開発された。NemeSysは攻撃元ホストのネットワーク挙動のプロファイリングにもとづいて実現される。すなわち、マクロ解析システムにおいて観測されたホストとミクロ解析システムによって抽出された各マルウェアとのネットワーク挙動のプロファイルを比較することにより、観測された攻撃元ホストと相関性の高いマルウェア検体を特定する手法を用いている。

この相関分析をより迅速かつ効率的に実現するため、我々はマルウェア情報プール（MNOP）と呼ばれる統合データベースを構築した。MNOPにはダークネットにおいて観測されたホストおよびハニーポット等によって収集されたマルウェア検体に関するサマリ情報（観測日時、攻撃元ホストのIPアドレス情報等）のほか、マクロ・ミクロ両解析システムの解析結果のすべてが蓄積されている。NemeSysはMNOPに対してさまざまな問い

合わせを行い、これらの情報の紐づけを行うことで相関分析を実現している。MNOP が構築されるまでは、相関分析を行うために複数の箇所に分散配置されたデータベースやログ情報等の情報を人手で探索する必要があったが、MNOP の実現により、これらの作業を自動的、効率的に行うことが可能となった。MNOP を用いたマクロ-ミクロ相関分析システムの概念図を図５に示す。

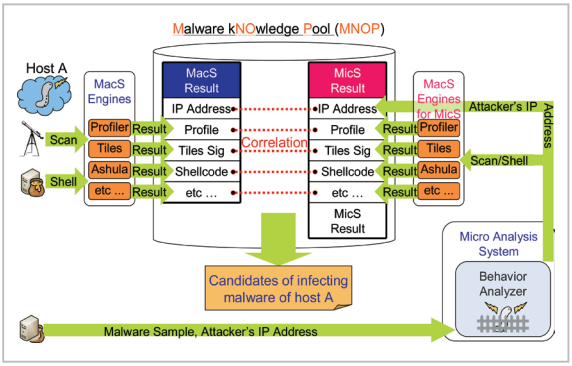

図５ マクロ-ミクロ相関分析システム概念図

マクロ解析システムにおけるブラックホールセンサやハニーポットによって収集されたトラフィックデータは、同じくマクロ解析システムで稼働するスキャンプロファイラ、Tiles、シェルコード検知エンジンなどの分析エンジンによって分析され、その分析結果は攻撃元ホストの IP アドレスとともに MNOP に蓄積される。一方で、ハニーポットで収集されたマルウェア検体はミクロ解析システムにおいて分析されるが、特に動的解析システムによって抽出された個々のマルウェアのネットワークトラフィックもマクロ解析システムにおける分析エンジンによって分析された上でその結果が MNOP に蓄積される。これにより、マクロ解析システムにおける観測データとミクロ解析システムにおけるマルウェア検体のネットワーク挙動は同じデータフォーマット（すなわち分析エンジンによる分析結果）で蓄積されるため、相互の比較が容易になる。NemeSys はこのデータベースに問い合わせを行うことで、ブラックホールモニタリングで観測された特定の攻撃元ホストのスキャンと一致する特徴を持つマルウェア検体を抽出する。

6 nicter の社会展開

6.1 NIRVANA

nicter のマクロ解析システムでは、ダークネット観測により収集されたトラフィックのリアルタイムでの可視化を行っている。特に Atlas と呼ばれるツールでは、攻撃パケットに含まれる IP アドレス情報から送信元／宛先の地理的な位置を割り出し、世界地図上でアニメーション表示させることで、ネットワーク攻撃の世界的な傾向を把握することを可能にしている。

このような nicter の可視化技術およびトラフィックモニタリング技術を（インターネット全体ではなく）特定のネットワークの監視目的に応用したものが NIRVANA である。NIRVANA は、Atlas と異なり世界地図上ではなく指定されたネットワークトポロジ上でトラフィックの流れを描画することにより、組織内ネットワークで発生したネットワークインシデントだけでなく、ネットワーク機器のミスコンフィギュレーションやボトルネックを視覚的に把握することを可能にした（図 6）。

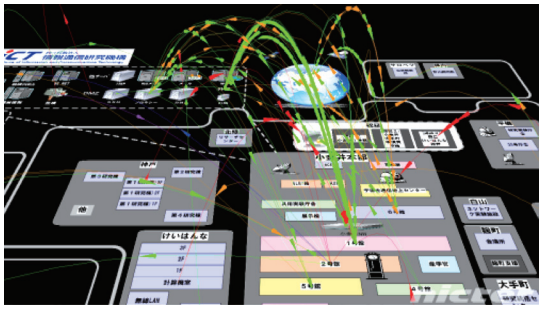

図６ NIRVANA による NICT 所内ネットワークの可視化の様子

NIRVANA では、ネットワーク内のルータやスイッチからルーティング情報などを定期的に収集し、この情報に基づいてネットワーク全体のパケットの流れを決定している。これにより、ネットワーク機器のトラブルによる不意の経路変更なども準リアルタイムで把握することができる。

NIRVANA は NICT の所内ネットワークにおいて活用されており、実際に数多くのネットワークインシデントや機器の設定ミス、通信のボトル

ネック等の発見に役立てられている。また、一般企業へも技術移転が行われ、国内複数拠点にまたがる大規模な社内ネットワークのボトルネック調査などに利用されている。

6.2 DAEDALUS

一般に、ダークネット観測は未使用のIPアドレス空間を対象としているため、ユーザやサーバなどが存在する実ネットワークの状況を把握することは困難であると言われている。これに対してnicterでは、ダークネット観測によって実ネットワークを保護するための技術、「DAEDALUS」を提案している。DAEDALUSは、協力組織のアドレスからのスキャンがnicterのダークネット宛に届いた場合に、協力組織のネットワーク管理者にアラートを送るという、いたってシンプルなものである。

図7で示すとおり、nicterでは複数の協力組織より未使用IPアドレスの一部をダークネットとして借り受けており（斜線部分）、そこで観測されたトラフィックは、すべてnicterに集約される。特定の組織内でマルウェア感染が発生すると、多くの場合マルウェアは感染拡大のために組織ネットワークの内外にスキャンを行う。よって、このスキャンがダークネットにおいて観測された場合、送信元ホストは、高い確率でマルウェアに感染していると推定されるため、当該組織ネットワークの管理者に向けてアラートを発行するのが、DAEDALUSの基本的な仕組みである。図7の例では、協力組織Gのネットワークにおいてマルウェアに感染したホストが、協力組織Aに向けて感染拡大のためのスキャンを行っている。DAEDALUSは組織Aのダークネットからこの事象を検知し、組織Gのネットワーク管理者に当該攻撃元ホストのアドレス情報などをアラートとして通知する。

このような仕組みは、広域なダークネット観測網によりカバーエリアを充実させているからこそ実現可能であると言える。よって、今後もより多くの組織と連携することで観測網を拡大することが重要であると考える。

実際に、DAEDALUSは国内のある組織において過去2年以上にわたり運用されている。これまでに数多くのマルウェア感染を検知し、管理者に向けてアラート情報を送ることで、当該組織内でのマルウェアの感染拡大を未然に防ぐことに役立っている。

6.3 日本国内における広域センサ展開

NICTでは、平成20年度より委託研究「インシデント分析の広域化・高速化技術に関する研究開発」において、国内の大学等をはじめとする複数の組織と連携した、nicter観測網の拡大と分析機能の強化に取り組んでいる（図8）。この取り組みにより、nicterのダークネット観測網は70,000IPアドレスがさらに追加され、より広域なネットワークを観測することが可能となった。

一方、連携組織に対しては前述のnicterの可

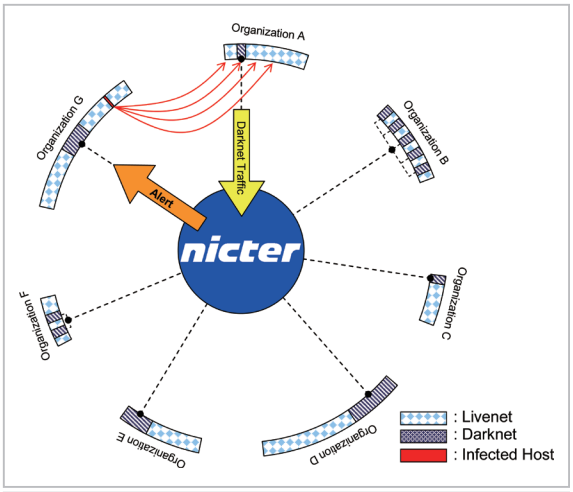

図7 DAEDALUSの仕組み

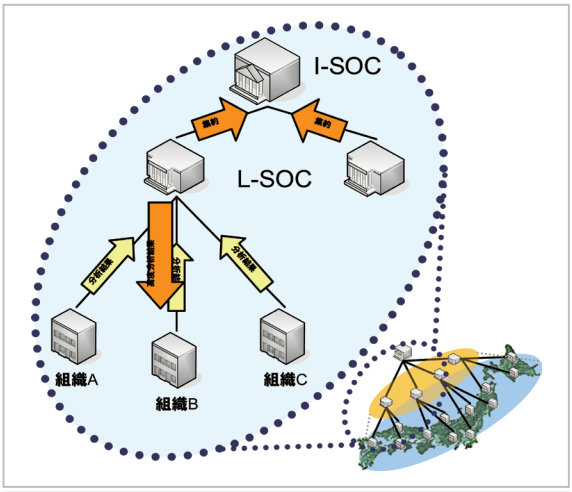

図8 平成20年度委託研究の概観図

視化エンジンや各種統計情報、DAEDALUSのアラートを提供することにより、各組織のネットワークセキュリティの向上に貢献している。実際に、平成22年度からの実証実験においては短期間の運用でありながら、すでに数多くの組織内ネットワークでのマルウェア感染やネットワーク機器のミスコンフィギュレーションをDAEDALUSが検知しており、連携組織からの好評を得ている。

この委託研究で構築した枠組みは委託研究終了後も継続し、今後はさらに協力組織を増やすことで観測網の強化にも取り組む予定である。

7 おわりに

nicterでは、ダークネット観測からマルウェア解析まで、ネットワークセキュリティに関する非常に幅広い分野での研究開発に取り組んでおり、そこで培われた技術は、これまでに述べたようにさまざまな形で実社会に貢献している。

その一方で、ネットワーク環境はより複雑になり、マルウェアを始めとするネットワーク上の攻撃も同様に高度化することが予想される。例として、IPv6環境におけるセキュリティ研究はいまだ不十分な点が多く、本格的な普及に先だって体系的な対策の検討を行うことが求められている。また現在は、スマートフォン市場やSNSなどを始めとする各種Webサービス、P2Pアプリケーションが隆盛を極めているが、これらのプラットフォーム、サービスアプリケーションのセキュリティについても検討が必要である。

nicterでは今後、これらの最新の環境におけるセキュリティに関しても検討を行い、その成果をもって実社会に貢献できるよう研究開発に取り組む予定である。

参考文献

1 K. Nakao, K. Yoshioka, D. Inoue, and M. Eto, “A Novel Concept of Network Incident Analysis based on Multi-layer Observations of Malware Activities,” The 2nd Joint Workshop on Information Security (JWIS07), pp. 267–279, 2007.

2 D. Inoue, M. Eto, K. Yoshioka, S. Baba, K. Suzuki, J. Nakazato, K. Ohtaka, and K. Nakao, “nicter: An Incident Analysis System Toward Binding Network Monitoring with Malware Analysis,” WOMBAT Workshop on Information Security Threats Data Collection and Sharing (WISTDCS 2008), pp. 58–66, 2008.

3 K. Nakao, K. Yoshioka, D. Inoue, M. Eto, and K. Rikitake, “nicter: An Incident Analysis System using Correlation between Network Monitoring and Malware Analysis,” The 1st Joint Workshop on Information Security (JWIS06), pp. 363–377, 2006.

4 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.

5 SANS Internet Storm Center, http://isc.sans.org/

6 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.

7 D. Moore, C. Shannon, G.M. Voelker, and S. Savage, “Network telescopes: Technical report,” CAIDA, April 2004.

8 M. Bailey, E. Cooke, F. Jahanian, A. Myrick, and S. Sinha, “Practical darknet measurement,” Information Sciences and Systems, 2006 40th Annual Conference on, pp. 1496–1501, IEEE, 2007.

9 N. Provos, “Honeyd-a virtual honeypot daemon,” 10th DFNCERT Workshop, Hamburg, Germany, 2003.

10 C. Leita, M. Dacier, and F. Massicotte, “Automatic handling of protocol dependencies and reaction to 0-day attacks with ScriptGen based honeypots,” Recent Advances in Intrusion Detection, pp. 185–205, Springer, 2006.

11 N. Provos, "A virtual honeypot framework," Proceedings of the 13th conference on USENIX Security Symposium-Volume 13, p. 1, USENIX Association, 2004.
12 E. Alata, V. Nicomette, M. Kaâniche, M. Dacier, and M. Herrb, "Lessons learned from the deployment of a high-interaction honeypot," Dependable Computing Conference, 2006, EDCC' 06. Sixth European, pp. 39–46, IEEE, 2006.
13 R. Isawa, S. Ichikawa, Y. Shiraishi, M. Mori, and M. Morii, "A Virus Analysis Supporting System-For automatic grasping virus behavior by code-analysis result," Joho Shori Gakkai Shinpojiumu Ronbunshu, 1(13): 169–174, 2005.
14 D. Inoue, M. Eto, K. Yoshioka, Y. Hoshizawa, Isawa R., M. Morii, and K. Nakao, "Micro analysis system for analyzing malware code and its behavior on nicter," Symposium on Cryptography and Information Security (SCIS) 2007, IEICE, Jan. 2007.
15 C. Willems, T. Holz, and F. Freiling, "Toward automated dynamic malware analysis using cwsandbox," IEEE Security & Privacy, pp. 32–39, 2007.
16 N. Solutions, Norman sandbox whitepaper, 2003.
http://download.norman.no/whitepapers/whitepaper/Norman SandBox.pdf
17 D. Inoue, K. Yoshioka, M. Eto, M. Yamagata, E. Nishino, J. Takeuchi, K. Ohkouchi, and K. Nakao, "An Incident Analysis System NICTER and Its Analysis Engines Based on Data Mining Techniques," 15th International Conference on Neuro- Information Processing of the Asia Pacific Neural Network Assembly (ICONIP 2008), 2008.
18 D. Inoue, K. Yoshioka, M. Eto, Y. Hoshizawa, and K. Nakao, "Malware Behavior Analysis in Isolated Miniature Network for Revealing Malware's Network Activity," IEEE International Conference on Communications (ICC 2008), pp. 1715–1721, 2008.
19 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, 92(5): 787–798, 2009.

(平成23年6月15日 採録)

衛藤将史（えとうまさし）
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主任研究員　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

高木彌一郎（たかぎやいちろう）
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技術員
ネットワークセキュリティ、ネットワークトラフィック解析