2　インシデント対策技術
2　Network Security Incident Response Technology

2-1　インシデント分析センターnicterの研究開発概要
2-1　Overview of R&D Activities on nicter

中尾康二　　井上大介
NAKAO Koji and INOUE Daisuke

要旨

インターネットの発展と同調して、マルウェアをはじめとするセキュリティ上の脅威は高度化・巧妙化を続けており、時として組織やユーザにとって致命的なセキュリティインシデントを引き起こしている。情報通信セキュリティ研究センター インシデント対策グループでは、インターネット上で日々発生するセキュリティインシデントを迅速に把握し、その根本原因を究明するため、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きた。本稿では、nicterの全体像を俯瞰するとともに、その核となるネットワーク観測・分析技術やマルウェア自動解析技術、さらにそれらを融合させてセキュリティインシデントの原因特定を可能にする相関分析技術について概説する。

The Internet has faced various security threats ever since it became widespread. The malicious activities of malwares are spread all over the Internet and often lead to serious security incidents that can cause significant damages to both infrastructures and end users. There are two main approaches to fight against malwares: macroscopic (i.e., network monitoring) and microscopic (i.e., malware analysis) approaches. We have developed the Network Incident analysis Center for Tactical Emergency Response (nicter), which integrates both the macroscopic and microscopic approaches in order to promptly grasp the malicious activities and their root causes. In this paper, we describe a whole overview of the nicter and its sub-systems: macro analysis system, micro analysis system and macro-micro correlation analysis system.

[キーワード]
セキュリティインシデント，ネットワーク観測，マルウェア解析，相関分析
Security incident, Network monitoring, Malware analysis, Correlation analysis

1　研究背景

世界規模の社会インフラと化したインターネットは、我々の社会活動や経済活動に多大な恩恵をもたらし、インターネット普及以前の時代にはもはや逆戻りできない不可逆的変化を現代社会の隅々にまで及ぼしている。一方、その発展と同調するように、インターネットにおけるセキュリティ上の脅威も拡大の一途をたどっている。例えば、Webサービスに対する侵入攻撃やサービス不能（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*1が原因の一端を担っている。

マルウェアという言葉が定着する以前の80年代後半から90年代前半、ウイルスやワームなどの不正プログラムは愉快犯もしくは自己顕示を目的として作成・流布されることが多く、感染後はユーザに感染を知らせる画面表示やマシンの性能低下、データの破壊など、ある意味ユーザにとって分かりやすい現象を引き起こした。ところが90年代後半から、マルウェアは金銭搾取を目的とした組織的な犯罪のツールとして利用され始め、必然的にステルス性が高まるとともに次第に高度な機能を具備するようになっていく。そして2004年頃から、マルウェアにIRC（Internet Relay Chat）チャネル経由での遠隔一斉操作という技術革新が起こり、攻撃者が意のままに制御可能な大規模な感染ホスト群“ボットネット”がインターネット上に出現する。今日、ボットネットはスパムの大量送信や分散型サービス不能（DDoS）攻撃、大規模な感染活動など様々なセキュリティインシデントの一大源泉となっている。

このようなマルウェアに起因するセキュリティインシデントに対抗するため、ユーザレベルではウイルス対策ソフトやパーソナルファイアウォール、組織レベルでは侵入検知システム（IDS）や侵入防止システム（IPS）などの局所的な「点」で守るセキュリティ技術が導入されてきている。しかしながら、社会インフラとしてのインターネットそれ自身のセキュリティ確保は「点」の対策だけでは十分ではなく、俯瞰的な「面」の視点でインシデントを捉える必要がある。つまり、広大なインターネット空間で起こるセキュリティインシデントの全体像を迅速かつ正確に把握した上で、その原因を特定し、効果的な対策を打ち出す仕組みが求められていた。

情報通信セキュリティ研究センター インシデント対策グループでは、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し、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きた[1]-[3]。nicterの特徴は、多地点のインターネット観測による攻撃情報の収集とその解析技術（マクロ解析）、およびハニーポット等を用いて捕獲したマルウェア検体の解析技術（ミクロ解析）、さらにそれらを融合させる相関分析技術によって、インターネット上で発生しているインシデントが、どのようなマルウェアに起因しているのかを実時間で推定することにある。これにより、ゼロデイ攻撃*2による未知のマルウェアの拡散に対しても早期解決の手立てを与えることが期待できる。

本稿では、**2**でネットワーク観測とマルウェア解析のそれぞれの分野の概観を述べ、**3**でそれらを融合させるインシデント分析センターnicter、およびそのサブシステムであるマクロ解析システム、ミクロ解析システム、相関分析システムの各機能について解説し、**4**でまとめる。

2 ネットワーク観測とマルウェア解析

マルウェアに起因するセキュリティインシデントを分析するためのアプローチは、マクロ的アプローチとミクロ的アプローチに大別できる。マクロ的アプローチとは、ネットワーク観測によって得られたトラフィックを分析し、インシデントの現象を巨視的に把握するアプローチである。一方、ミクロ的アプローチとは、捕獲したマルウェアを解析し、インシデントの原因であるマルウェアの挙動を微視的に明らかにするアプローチである。マクロとミクロいずれのアプローチも、入力となるデータ、つまりトラフィックやマルウェアの検体をインターネットから収集するセンサが必要である。多くの場合、そのようなセンサは、ダークネットと呼ばれるIPアドレス空間に設置される。

ここではまず、ダークネットおよび各種のセンサについての解説を行う。次いでマクロ的アプローチの例として国内外のダークネット観測プロジェクト、ミクロ的アプローチの例として同じく

*1　ウイルス、ワーム、トロイの木馬、スパイウェア、ボットなど情報漏えいやデータ破壊、他のコンピュータへの感染など有害な活動を行うソフトウェアの総称。“malicious”と“software”を組み合わせた造語。

*2　OSやアプリケーションの脆弱性を修正するセキュリティパッチが公表される前に、その脆弱性を利用する攻撃のこと。最新のセキュリティパッチが適用されているシステムであってもゼロデイ攻撃は防げないため、大規模なインシデントに発展する可能性がある。

国内外のマルウェア解析プロジェクトについて紹介する。

2.1 ダークネットとセンサ

ダークネットとは、インターネット上で到達可能かつ未使用のIPアドレス空間のことを指す。未使用のIPアドレスに対しパケットが送信されることは、通常のインターネット利用の範囲においては起こる可能性が低いが、実際には相当数のパケットがダークネットに到着する。これらのパケットの多くは、ネットワークを経由して感染を広げるタイプのマルウェアが次の感染対象を探すためのスキャンや、マルウェア自身がペイロードに含まれているUDPパケット*3、マルウェア同士がP2Pネットワークを確立するためのランデブー用のパケット、送信元IPアドレスを詐称したDDoS攻撃を受けているサーバからの応答（SYN-ACK）であるバックスキャッタなど、インターネット上での何らかの不正な活動に起因している。そのため、ダークネットに到着するパケットを受動的に観測することで、インターネット上で発生している不正な活動の傾向把握が可能になる。またパケットに能動的に適切な応答をすると、さらに詳細な攻撃情報やマルウェアの検体を捕獲することも可能である。

ダークネット観測の利点は、トラフィックを正・不正で区別する必要がなく、全てのパケットを不正なものと見なして分析することが出来る点にある。また、観測主体が保有する未使用のIPアドレスをネットワークの端点で観測するため、通信のプライバシの問題に抵触しないという点も重要である。

ダークネット観測を行う場合、センサと呼ばれるパケット収集・応答用のサーバマシンを設置する。センサは、パケットの送信元に対する応答の程度によって次のように分類される。

- **ブラックホールセンサ**：パケットの送信元に対し、全く応答を行わないセンサ。メンテナンスが容易であり大規模なダークネット観測に向く。無応答であるため、外部からセンサの存在を検知することが困難であるという利点もある。ただし、マルウェアの感染活動の初期段階であるスキャンは観測可能であるが、それ以降の挙動を観測することは出来ない。

- **低対話型センサ**：パケットの送信元に対し、一定レベルの応答を返すセンサ。TCPのSYNパケットに対してSYN-ACKパケットを返すセンサや、OSの既知の脆弱性を模擬する低対話型ハニーポットがここに含まれる。リッスンしているポートや応答の傾向などからセンサの存在を検知され易く、アドレスが連続した大規模なダークネットでの運用には不向きである。

- **高対話型センサ**：実マシン、もしくはそれに準じた応答を返すセンサ（いわゆる、高対話型ハニーポット）。マルウェアの本体やその感染時の挙動、攻撃者が不正アクセスを試みた際の行動履歴など多様な情報が取得可能である。ただし、安全な運用を行うためのコストは非常に高く、大規模運用には不向きである。

2.2 ダークネット観測プロジェクト

ここでは、インシデント分析のマクロ的アプローチとして、国内外の主要なダークネット観測プロジェクトについての概要を記す。

- **Network Telescope**：米国のCAIDA（Cooperative Association for Internet Data Analysis）によるダークネット観測プロジェクト。16万アドレス以上のダークネットを観測し、バックスキャッタやワームによるトラフィックのデータセットを公開している。

- **Internet Motion Sensor**：米国のミシガン大学による1700万アドレス以上の大規模ダークネット観測プロジェクト。観測されたTCP SYNパケットの一部にセンサ側からSYN-ACKを返すことでTCPコネクションの確立を試み、コネクション確立後の最初のパケッ

*3　例えば、SQLSlammerと呼ばれるマルウェアは、データサイズが非常に小さく（376 Byte）、1つのUDPパケットのペイロードに収まる。

トのペイロードを収集・分析する機能を持つ。

- **Leurre.com**：フランスのEurecomによる分散型ハニーポットを用いた情報収集・分析プロジェクト。観測対象のIPアドレス数は比較的少数であるが、観測地域は世界各国に分散している。第1世代のLeurre.com v1.0は低インタラクションセンサのHoneydを使用していたが、第2世代のLeurre.com v2.0ではSGNETを使用して情報収集能力の向上を図っている。

- **REN-ISAC**：米国の研究教育ネットワーク（REN：Research and Education Networking）におけるセキュリティ情報の共有・分析プロジェクト。Internet2で観測されたトラフィックを分析し、観測結果を公開している。

日本国内ではJPCERT/CCによる**ISDAS**、警察庁による**@police**、情報処理推進機構による**MUSTAN**、三菱総合研究所ほかによる**WCLSCAN**などのネットワーク観測プロジェクトが進行中である。

2.3 マルウェア解析プロジェクト

マルウェア解析の手法は大別すると、動的解析と静的解析の2つのアプローチに分けられる。動的解析はブラックボックス解析とも呼ばれ、マルウェアの検体を犠牲となるマシンの上で実際に実行し、そのマシンの内部挙動やネットワークアクセスなどを解析するものである。静的解析はホワイトボックス解析とも呼ばれ、マルウェアの実行コードを逆アセンブルして、アセンブリレベルでマルウェアの持つ機能や特徴を詳細に解析するものである。動的解析は解析の自動化が比較的行いやすいのに対し、静的解析は逆アセンブルを阻害するコード難読化やアンチデバッグ機能が最近のマルウェアには備わっているため、高度な技術を持つ解析者による手動解析が主流である。

以下では、マルウェアの動的解析を自動システム化して、解析サービスを一般に提供しているプロジェクトについての概要を示す。いずれのシステムも、マルウェアのAPIコールやネットワークアクセスなどを観測することで、その挙動を抽出している。

- **CWSandbox**：ドイツのマンハイム大による動的解析システム。仮想マシン（VMware Server）上のWindows XPでマルウェアを実行する。解析中のマルウェアのインターネット接続を許可している。

- **Anubis**：オーストリアのウィーン工科大による動的解析システム。QEMUと呼ばれるPCエミュレータ上でマルウェアを実行する。解析中のマルウェアのインターネット接続を許可している。

- **Norman Sandbox**：ノルウェーのNorman社による動的解析システム。Windowsのクローン OS上でマルウェアを実行する。解析中のマルウェアのインターネット接続は許可していないが、解析環境内にダミーのDNSやWebサーバを用意している。

3 インシデント分析センターnicter

ここまで述べたように、ダークネット観測（マクロ的アプローチ）とマルウェア解析（ミクロ的アプローチ）は、様々な組織において研究開発や実運用が進められてきている。そして、セキュリティインシデントの原因追及という目的を考えたとき、双方のアプローチの連携は必須となってくる。しかしながら、ダークネット観測プロジェクトの多くはトラフィックの量的な分析に注力し、一方、マルウェア解析プロジェクトはマルウェアの機能解明に重きを置いているため、双方のアプローチの間の隔たりは大きく、今現在インターネットで観測されている現象が、どのような原因に基づくかを容易に知ることはできなかった。

そこで、情報通信セキュリティ研究センター インシデント対策グループでは、ダークネット観測とマルウェア解析を融合することで、ネットワークに大局的な悪影響を及ぼすインシデントの発生を早期に検出し、さらに迅速な原因追及と対策導出を目指した、インシデント分析センターnicterの研究開発を進めてきた。

nicterは、広域のダークネット観測によって収

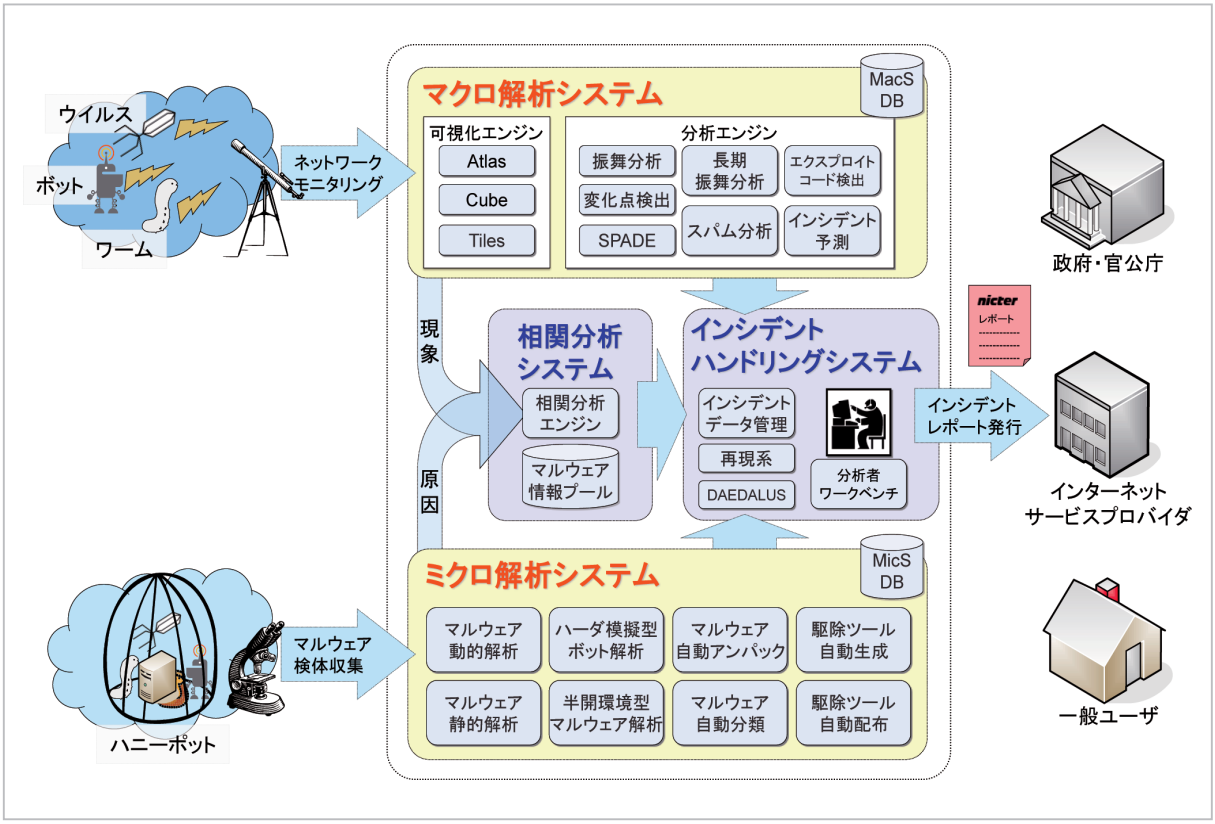

図 1　nicter の全体像

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。換言すると、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、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、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、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。

このように、マクロ的アプローチとミクロ的アプローチを融合させるというコンセプトを実現することにより、ダークネットで観測されたトラフィックの統計データの提示に留まらず、インシデントの原因とその対策にまで踏み込んだ実効性・即時性の高いインシデントレポートやアラート情報を、政府・官公庁、ISP および一般ユーザに向けて発行することが期待できる。**3.1 ～ 3.3** では、nicter のマクロ解析システム、ミクロ解析システム、相関分析システムについて、それぞれ概説する。

3.1　マクロ解析システム

マクロ解析システムの主な入力は、複数の観測地点に設置されたブラックホールセンサで観測したダークネットトラフィックである。nicter は現状、日本国内の 14 万を超える未使用 IPv4 アドレスを観測している。図 2 は nicter の保有するダークネットのうち約 78,000 の IPv4 アドレスを用いた観測結果（2011 年 3 月 1 ～ 31 日）であり、ダーク

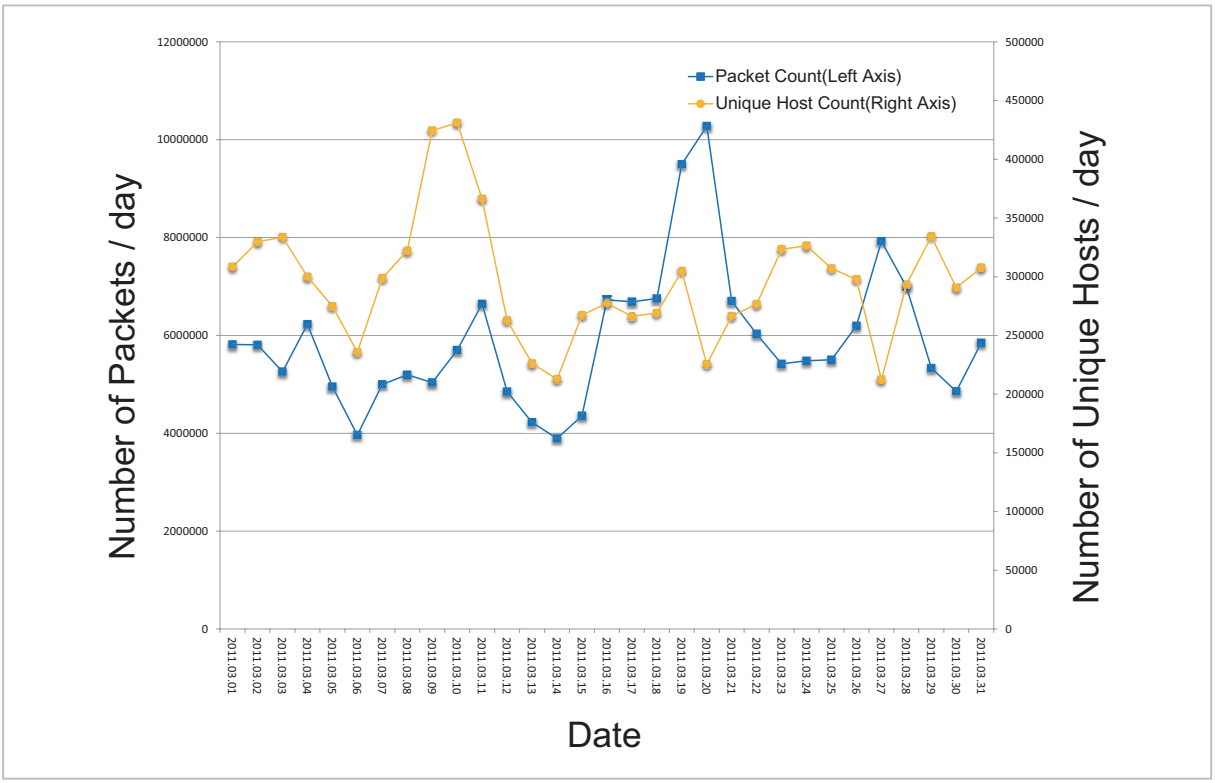

図 2　nicter のダークネット（78,000 アドレス）観測結果

ネットに到着したパケット数と、送信元のユニークホスト数（1 日ごとのユニークな送信元 IP アドレス数）を示している。図より、1 日あたり平均約 30 万のユニークホストが、平均約 590 万パケットをダークネットに向けて送信したことになる。

このように、ダークネットに到着するトラフィックを収集・分析することで、広域ネットワークにおける攻撃活動の巨視的な傾向を把握することが可能になる。マクロ解析システムは、分析者による直感的なインシデントの検出を支援する可視化エンジンと、トラフィックの自動分析を行う分析エンジンからなる。以下では、これらエンジンの一部についての概要を述べる。

3.1.1　可視化エンジン

(1)　Atlas

Atlas（図 3）は、ダークネットトラフィックを世界地図上でリアルタイムにアニメーション表示する可視化エンジンである。ダークネットに到着したパケットの 1 つ 1 つについて、送信元および宛先 IP アドレスが属する国を割り出し[*4]、送信元の国の首都から宛先の国の首都にパケットが飛来する様子をアニメーション表示することで、世界的なマルウェアの活動傾向を直感的に把握することができる。各パケットの色はパケットの種別[*5]を表し、パケットの軌道の高さはポート番号の大きさに比例（対数軸）している。また、マウス操作による視点の変更や拡大縮小、パケットオブジェクトのクリックによる詳細情報の表示（図 4）など、分析者のインタラクティブな操作を可能にしている。

(2)　Cube

Cube（図 5）は、ダークネットに到達したパケットを、その送信元と宛先の各種情報に基づいて、3 次元空間に浮かぶ立方体中にアニメーション表示する可視化エンジンである。立方体の縦軸に送信元／宛先 IP アドレスを、横軸に送信元／宛先ポート番号を取り、送信元（図 5 の左平面）から宛先（図 5 の右平面）に向けてパケットを通過させる

*4　IP アドレスと緯度・経度のマッピングは MaxMind 社の GeoIP City Database を利用。

*5　青：TCP SYN、黄：TCP SYN-ACK、緑：TCP ACK、桃色：TCP FIN、紫：TCP RST、橙：TCP PUSH、水色：TCP OTHER、赤：UDP、白：ICMP（後述の Cube、Tiles における色も同様）。

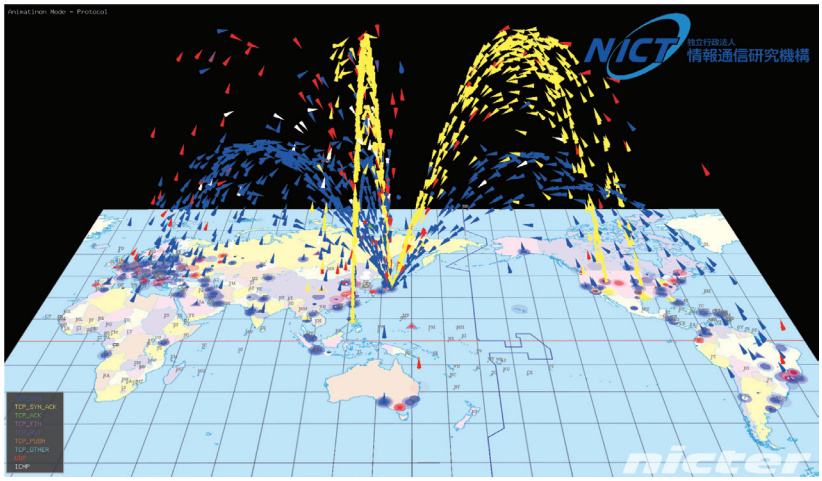

図3 Atlas

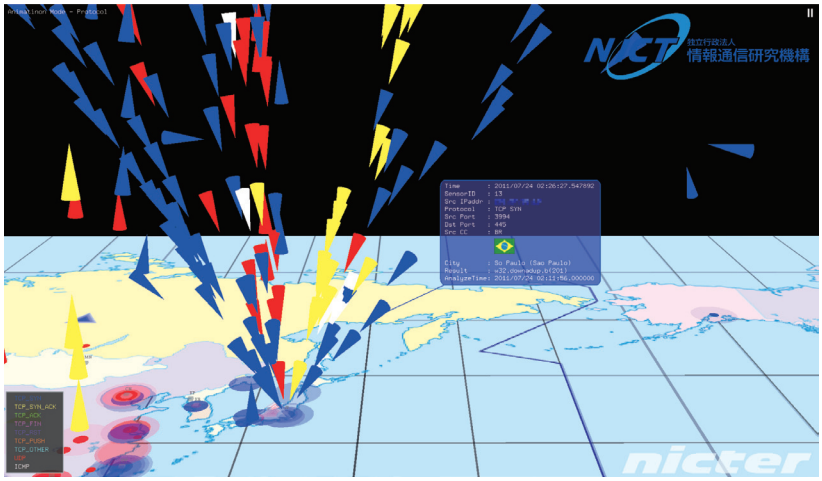

図4 Atlas（パケット情報詳細表示）

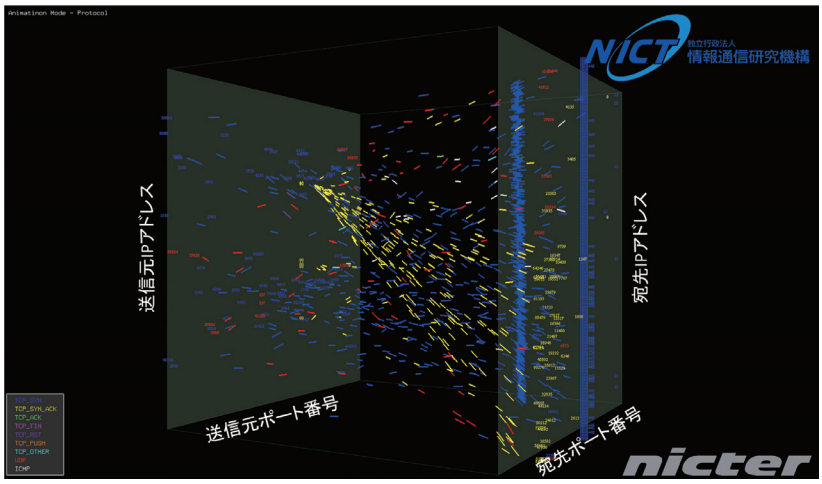

図5 Cube

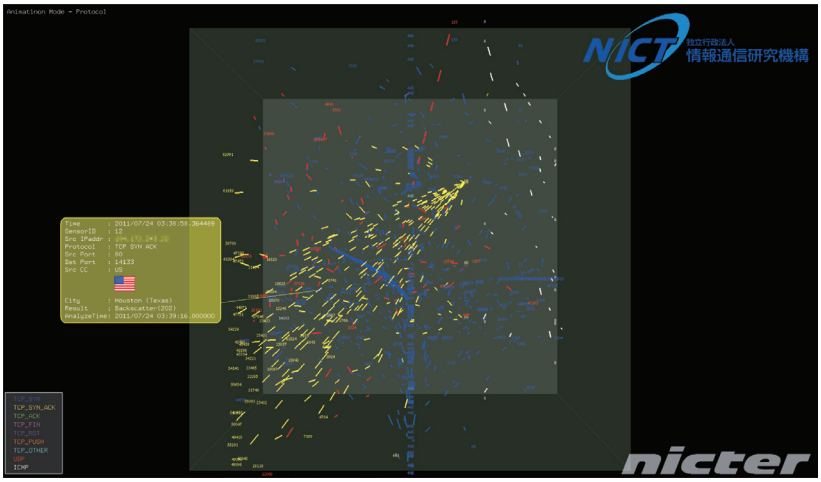

図6 Cube（パケット情報詳細表示）

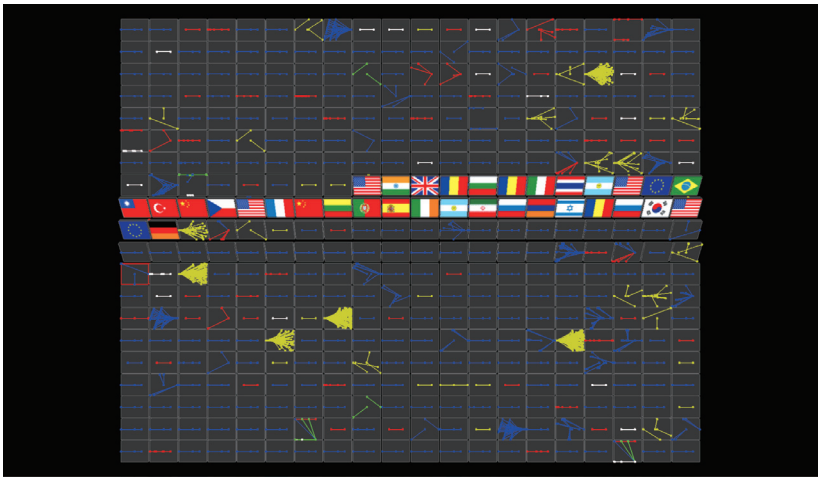

図7 Tiles

ことで、スキャンやバックスキャッタなどの形状が可視化される。Cube は Atlas と同様、マウス操作による視点の変更や拡大・縮小、パケットの詳細情報の表示（図6）などが行え、送信元ホストからの攻撃の様子をリアルタイムに把握することが可能であり、分析者が詳細な分析を開始するためのトリガとして非常に有用である。

(3) Tiles

Tiles（図7）は後述する振舞分析エンジンの分析結果をリアルタイム表示する可視化エンジンである。図7の小さなタイルの1つ1つが送信元ホスト毎の挙動を表しており、最新の分析結果に随時更新されていく。タイルの裏側は送信元ホストが属する国の国旗が示されている。1つのタイルは、ある送信元ホストが30秒間に送出したパケットの時刻、送信元／宛先ポート番号、宛先 IP アドレスを用いて図8の様に可視化される。ここで、1つのパケットは送信元（左半面）と宛先（右半面）を結ぶ1本の線で表現されている。図8は送信元ポート番号を増加させながら、複数の宛先 IP アドレスの単一宛先ポートに TCP SYN パケットを送信するネットワークスキャンの典型的なパターンである。また、1つのタイルをクリックすると、そのタイルと同じパターンを持つタイルが白くハイライト表示される（図9）。これは振舞分析エンジンによるスキャンパターンの自動分類の結果が反

映されている。

3.1.2 分析エンジン

(1) 変化点検出エンジン[4]

変化点検出エンジンは、特定ポートへの単位時間あたりのパケット数や、ユニークホスト数などの時系列データに対して2段階のオンライン忘却型学習を適用し、それら時系列データの急激な変化を迅速に検出するための分析エンジンである。変化点検出エンジンは、時系列データに単純な閾値を設定するのではなく、時系列データのモデルの変化度を変化点スコアとして算出する。これにより、ワームの大規模感染初期の微小な変化を検出するなど、インシデントの早期発見に有効である。図10は2003年8月に大規模感染を引き起こしたMSBlastによるtcp/135へのスキャンを、変化点検出エンジンで検出した例である。感染初期の8月12日前後に変化点スコアが大きく変動していることが分かる。図11は、変化点検出エンジンのWebインターフェイスである。特定ポートの変化点を検出し、アラート(図中の赤の「!」マーク)が自動発行されている。

(2) 振舞分析エンジン

振舞分析エンジンは、ダークネットトラフィックを送信元ホストごとにスライスし、各ホストの短期間(30秒間)の挙動を分析・分類するエンジンである。振舞分析エンジンがホストの分類に使用するパラメータは、パケットの個数、送信元／宛先ポートの個数、宛先ポート番号の組、宛先IPアドレスの個数、スキャンタイプ(シーケンシャル／ランダム)などである。この分類の履歴を蓄積することによって、ある送信元ホストの挙動が既知のスキャンパターンであるのか、あるいは新規のスキャンパターンであるのかをリアルタイムに判定することが可能となる。分析・分類の結果は前述のTilesによって可視化される。

マクロ解析システムでは、上記の2つの分析エンジンに加え、送信元ホストの長期的な挙動を分析する長期振舞分析エンジン、スペクトラム解析を用いてスキャンパターンの分類を行うSPADE分析エンジン、攻撃コードの検出を行うエクスプロイトコード検出エンジン、ダークネットトラフィックの増減予測を行うインシデント予測エンジン、さらにはダークネットトラフィックだけでなく、スパムメールの送信元と本文に含まれるURLのリンク先の解析を行うスパム分析エンジンなど、

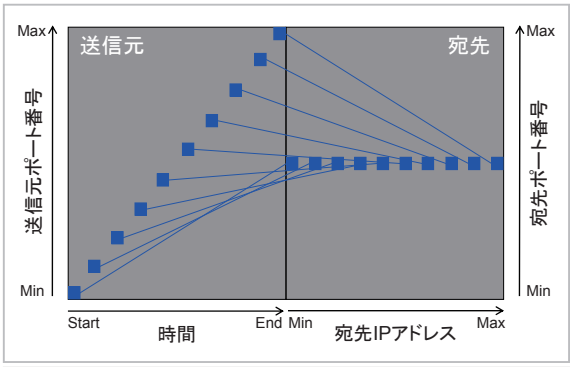

図8 各タイルの表現手法

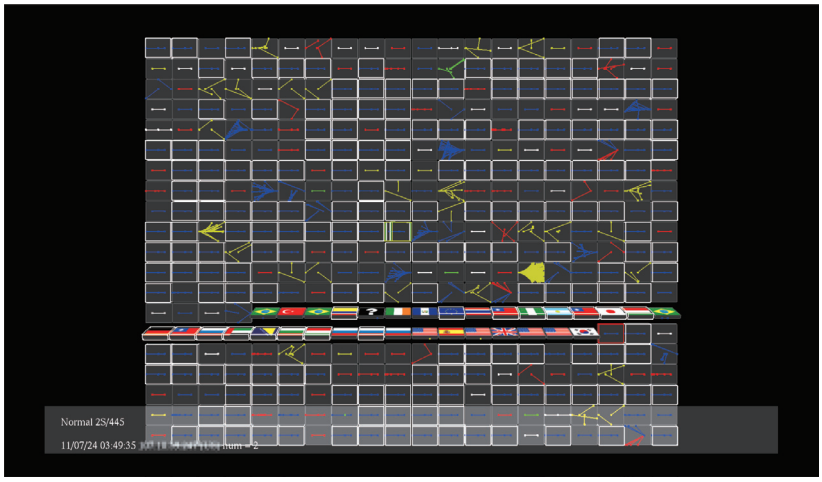

図9 同じパターンを持つタイルのハイライト表示

様々な分析エンジン群の研究開発を行った。

3.2 ミクロ解析システム[5][6]

ミクロ解析システムの入力は、ハニーポットやWebクローラなどで捕獲したマルウェアの検体である。nicterでは、マルウェア解析の自動化を進め、特に動的解析に関しては1検体あたり6～9分の高速な解析を実現し、さらに解析の並列化により1日あたり最大2,000検体の解析が可能となっている。以下では、ミクロ解析システムの主なエンジンである静的解析エンジンと動的解析エンジンの概要を述べる。

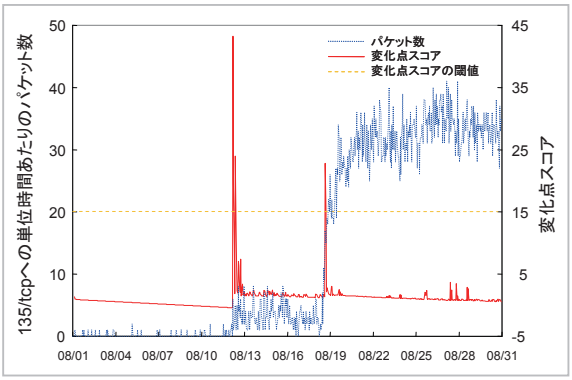

図10 変化点検出エンジンによるMSBlastの検出例

3.2.1 静的解析エンジン

静的解析はマルウェアの実行コードを逆アセンブルして、アセンブリレベルでマルウェアの持つ機能や特徴を詳細に解析する手法である。ところが、近年のマルウェアの多くは、逆アセンブルを阻害するコード難読化（code obfuscation）が施されているため、静的解析を困難なものとしている。そこで、nicterの静的解析エンジンでは、コード難読化されたマルウェアを犠牲となるマシン（以下、犠牲ホスト）上で一旦実行し、メモリに自己復号されたコードをダンプして逆アセンブルすることで、難読化の効果を無効化している。このようにして得られたアセンブリを自動解析することで、マルウェアの実行コードに含まれるAPIのリストや、ボットが使用するIRCのプライベートメッセージの文字列などの多様な情報が抽出可能である。

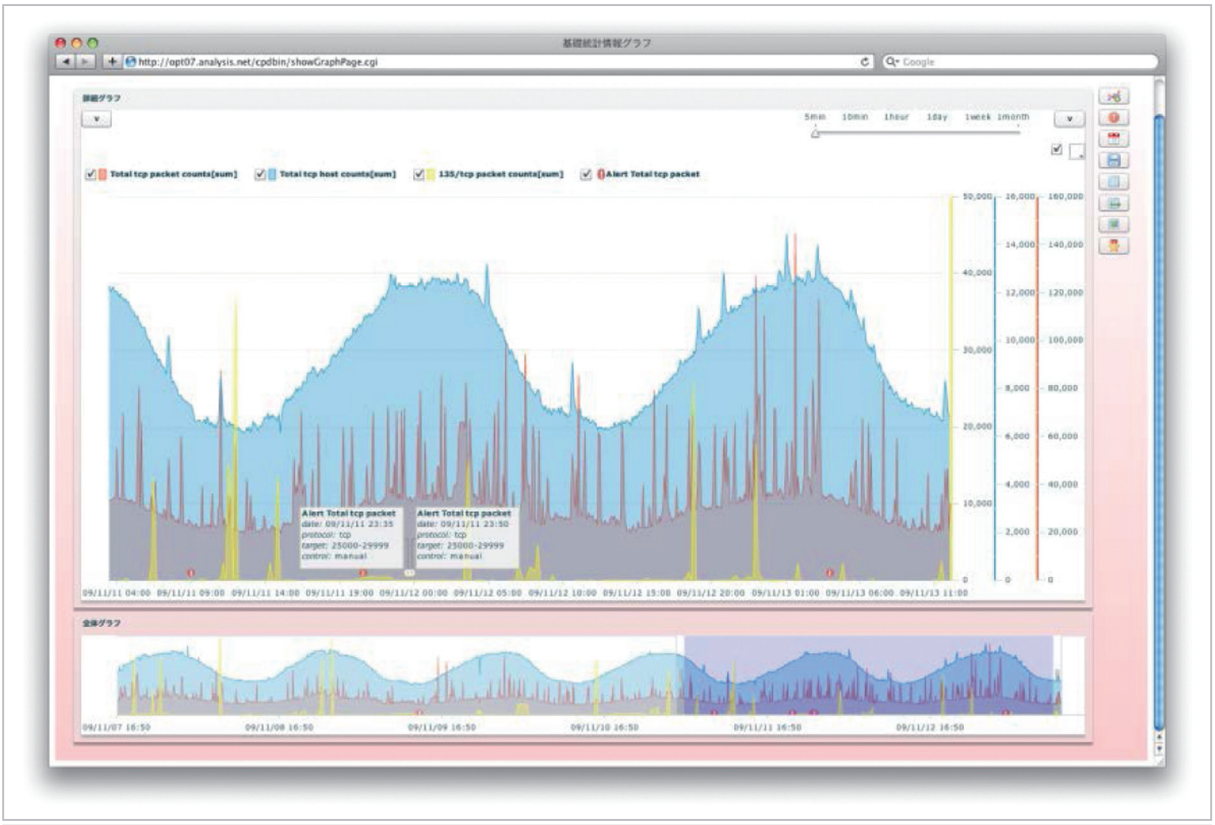

図11 変化点検出エンジンのWebインターフェイス

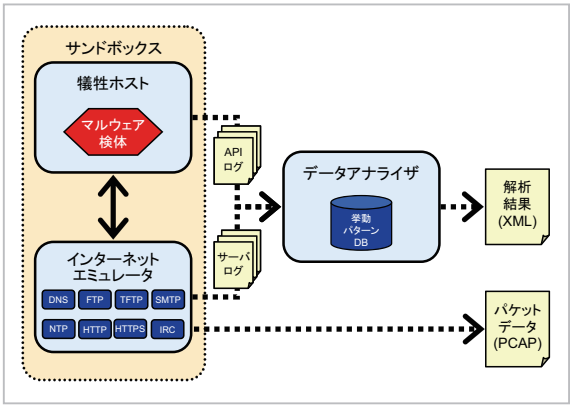

図 12　マルウェア動的解析エンジン

3.2.2　動的解析エンジン

動的解析はマルウェアを実行状態に置き、その際にマルウェアが使用したAPIやネットワークアクセスなどの挙動を解析する手法である。このような解析に対抗するため、近年のマルウェアは自己の周囲のネットワーク環境を監視し、自己が隔離環境下にあることを検知すると実行停止や自己削除を行うなど、動的解析を困難にする機能を持つものが多い。そのため、**2.3** で述べたマルウェア動的解析プロジェクトの一部は、解析の際に犠牲ホストがインターネットに接続することを許容しており、外部に実害を及ぼす危険性を秘めている。nicterの動的解析エンジンは、犠牲ホストをサンドボックス環境内に完全隔離し、その対向にDNSやIRCなど多数のダミーサーバからなる擬似インターネット（インターネットエミュレータ）を配置することで、安全な動的解析を実現している。さらに、多くのマルウェアが解析回避のために行う仮想マシン検出に耐性を持たせるために、犠牲ホストはOS自動復元機構とAPIフック機能を有する実マシンによって構成されている。

このようなサンドボックス環境内での動的解析の結果、犠牲ホストからはAPIログが、インターネットエミュレータからはサーバログが出力され、それらのログからマルウェアの挙動が抽出される。図13は、マルウェア動的解析結果の一例である。加えて、犠牲ホストからのトラフィックはパケットデータとして記録される。このパケットデータに含まれるスキャンが、後述する相関分析の鍵となる。

ミクロ解析システムでは、上記の静的／動的解析エンジンに加え、サンドボックス環境内でハーダ（ボットに指令を出す攻撃者）を模擬してボットの制御を可能にするハーダ模擬型ボット解析エンジンや、マルウェアの通信のうち安全なものだけを実インターネットに接続して動的解析を行う半開環境型マルウェア解析エンジン、難読化されたマルウェアのオリジナルエントリポイント（OEP）を自動検出することで難読化の自動解除を可能にするマルウェア自動アンパックエンジン、マルウェアの動的解析結果からマルウェアの分類を行うマルウェア自動分類エンジン、マルウェアの動的解析結果から簡易型の駆除ツールを自動生成する駆除ツール自動生成エンジン、さらにその駆除ツールを自動配布するシステム等の研究開発を行った。

3.3　相関分析システム[1]-[3]

相関分析システムでは、マクロ解析システムにおいて観測されたスキャンを各種の特徴*6によってプロファイリングし、ミクロ解析システムにおいてマルウェアから抽出されたスキャンのプロファイルとの照合を行い、類似したプロファイルを持つマルウェアの候補を探し出す。マクロ解析結果とミクロ解析結果はマルウェア情報プール（MNOP：Malware kNOwledge Pool）に蓄積されるとともに、相関分析エンジンによってリアルタイムに照合が行われる。

図14は可視化エンジンAtlas上で相関分析結果を可視化したものである。各パケットオブジェクトの上方に、相関分析の結果、第1候補として挙げられたマルウェア名（もしくはバックスキャッタ）を表示している。また、パケットの詳細情報の中にもマルウェア名（図14の例ではw32.downadup.b）を表示している。さらに、相関分析の結果を累計することで、マルウェアの世界的な傾向を把握することが可能である。図14の左下のボックスは、相関分析結果（マルウェア名ごとのユニークホスト数）の累計を表しており、2011年現在、70%を超えるホストがw32.downadup.b（あるいはそれと同様のスキャンエンジンを持つマルウェア）に感染し

*6　パケットのプロトコル、TCPフラグ、送信元ポート番号およびその変化、宛先ポートのセット、宛先IPアドレスの遷移（シーケンシャル／ランダム）、単位時間あたりのパケット数、ペイロード長など。

図 13 マルウェア動的解析結果

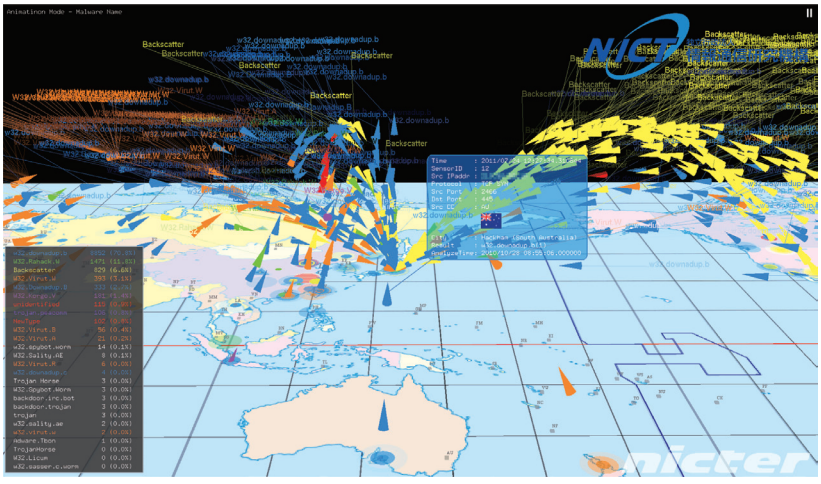

図 14 相関分析結果の可視化

ているものと推定される。

4　まとめと今後の課題

本稿では、ネットワーク観測とマルウェア解析を融合させて、セキュリティインシデントの早期発見、原因究明、対策導出を目的としたインシデント分析センターnicterについて概説した。nicterの研究開発によって、ネットワーク経由で感染を広げる（いわゆるリモート・エクスプロイト型）マルウェアの俯瞰的な活動傾向の把握と迅速な原因究明が可能となった。また、マルウェア動的解析を応用した簡易型駆除ツールの自動生成と配布や、nicterの大規模ダークネット観測網を応用したアラートシステムDAEDALUS*7（本季報で後述）など、対策技術の研究開発とその実証を推進した。さらに、nicterの可視化技術を応用した実ネットワーク可視化システムNIRVANA*8（本季報で後述）を開発し、機構内外への技術移転を行うなど、nicterから派生した技術の利活用も進みつつある。

一方、本稿の冒頭でも述べたように、インターネットにおける脅威は日々進化しており、Webを感染媒体とした（いわゆるドライブ・バイ・ダウンロード型）マルウェアや、SNSを経由したマルウェアなど、これまでのnicterの仕組みでは捉えられない新たな脅威が生まれてきている。今後も、このような新たな脅威に対抗可能な実践的研究開発を推進するとともに、攻撃者側が圧倒的に有利な現在の状況を一変させ得る根源的なセキュリティ技術の研究開発を、産学官の連携の下に取り組んでいく。

*7　direct alert environment for darknet and livenet unified security
*8　nicter real-network visual analyzer

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, D. Inoue, M. Eto, and K. Yoshioka, “Practical Correlation Analysis between Scan and Malware Profiles against Zero-Day Attacks based on Darknet Monitoring,” IEICE Trans. Information and Systems, Vol. E92-D, No. 5, pp. 787–798, 2009.
4　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.
5　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.
6　D. Inoue, K. Yoshioka, M. Eto, Y. Hoshizawa, and K. Nakao, “Automated Malware Analysis System and its Sandbox for Revealing Malware's Internal and External Activities,” IEICE Trans. Information and Systems, Vol. E92-D, No. 5, pp. 945–954, 2009.

（平成23年6月15日 採録）

なかおこうじ
中尾康二
ネットワークセキュリティ研究所
主管研究員
セキュリティ技術全般、セキュリティマネージメント

いのうえだいすけ
井上大介
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室長
博士（工学）
ネットワークセキュリティ、情報セキュリティ