解説

ネットワーク観測とマルウェア解析の融合に向けて
—インシデント分析センター nicter の研究開発—

中尾 康二[*1]　井上 大介[*1]　衛藤 将史[*1]　吉岡 克成[*2]　大高 一弘[*1]

[*1] （独）情報通信研究機構　[*2] 横浜国立大学

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辿っている．たとえば，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☆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，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さまざま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る．

情報通信研究機構では，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いる[1), 2)]．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，現在問題となっているゼロデイ攻撃☆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，まずネットワーク観測とマルウェア解析のそれぞれ分野の概観を述べ，次に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

☆1 ウイルス，ワーム，トロイの木馬，スパイウェア，ボットなど情報漏洩やデータ破壊，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．

関分析システムの各機能について解説し，最後にまとめる．

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．

本章ではまず，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．

●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している．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，感染対象のルート権限を奪取するためのエクスプロイトコード，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が送信する応答（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技術上の利点は，トラフィックを正・不正で区別する必要がなく，すべてのパケットを不正なものと見なして分析することができる点にある．また，制度上の利点として，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，まった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できない．

- **低インタラクションセンサ**：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インタラクション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やすく，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．

- **高インタラクションセンサ**：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，高インタラクションハニーポット）．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．

●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/8ネットワークを含む1,700万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．

●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学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学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．

インシデント分析センター nicter

ここまで述べたように，ダークネット観測とマルウェア解析は，さまざまな組織において研究開発や実運用が進められている．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，著者らはマクロ的アプローチであるダークネット観測と，ミクロ的アプローチである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いる．

nicter は，広域のダークネット観測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

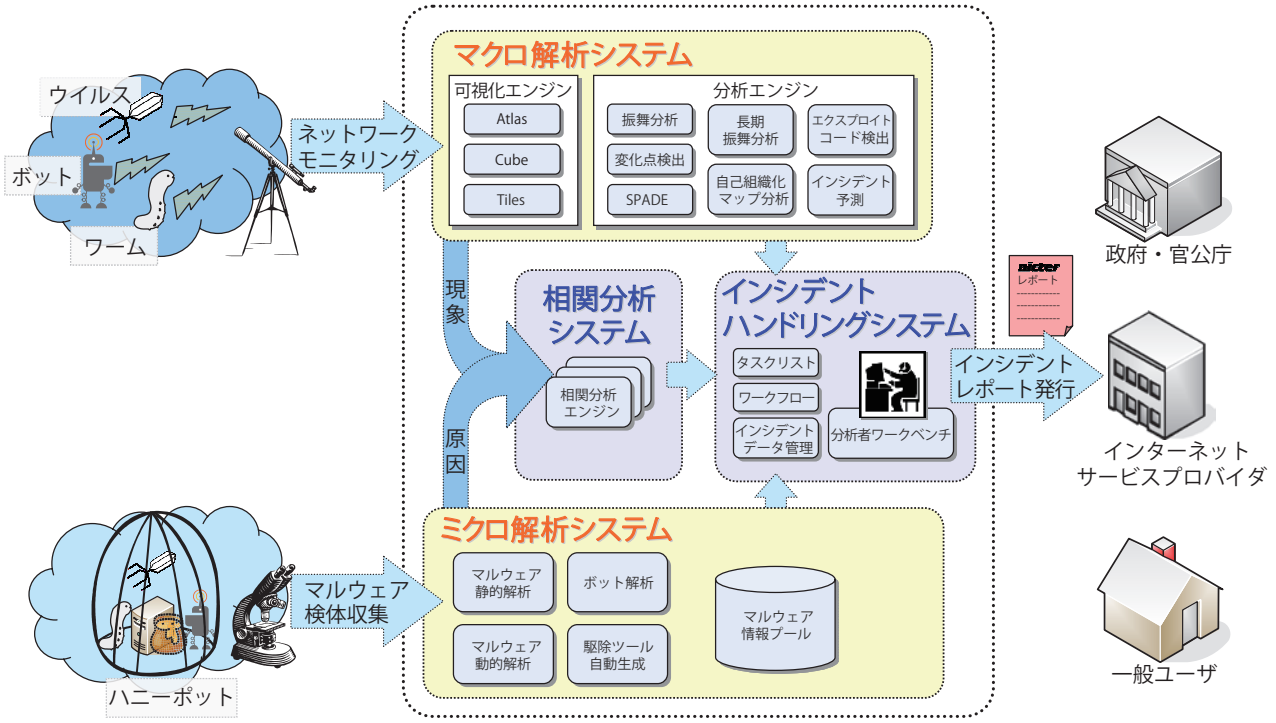

図 -1　nicter の全体像

的な Web インタフェースおよび可視化インタフェー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．

nicter は研究開発の途上にあるが，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とどまらず，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．以降の節では，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．

●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 10 万を超える未使用 IP アドレスを観測している．図 -2 は nicter の観測地点の 1 つである /16 ダークネットに 2008 年 7 月に到着したパケット数と，送信元のユニークホスト数を示している．1 日平均で約 2,700,000 パケット，約 45,000 のユニークホストが観測されている．

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．

可視化エンジン [2)]

(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，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．なお，各パケットの色はパケットの種別[☆3]を表し，パケットの高度はポート番号に対応して変化する．

(2) Cube

Cube（図 -4）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 -4 の

☆3 青：TCP SYN，黄：TCP SYN-ACK，緑：TCP その他，赤：UDP，白：ICMP（後述の Cube，Tiles における色も同様）．

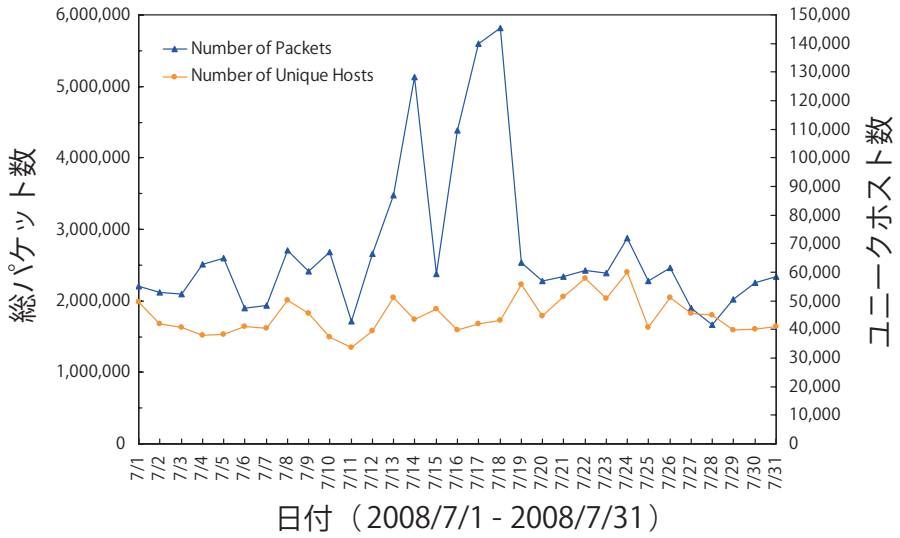

図 -2　nicter の /16 ネットワークの観測結果

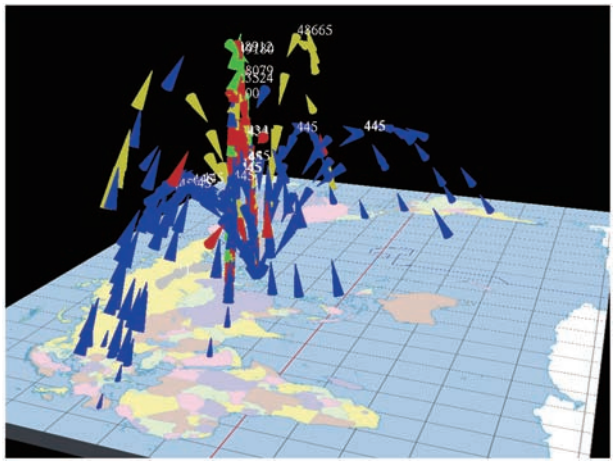

図 -3　Atlas

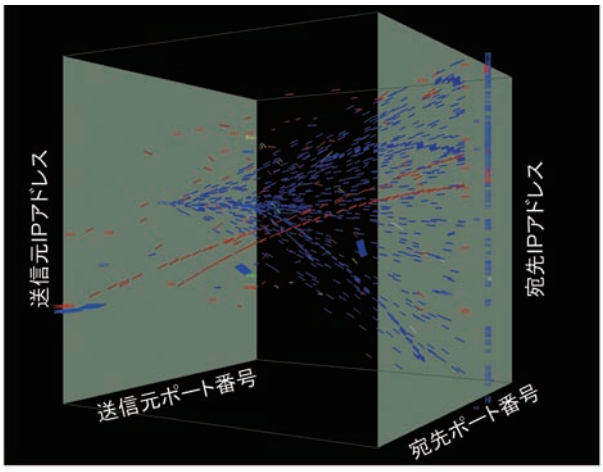

図 -4　Cube

左平面）から宛先（図 -4 の右平面）に向けてパケットを通過させることで，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 は視点の変更や拡大・縮小が自由に行え，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 -5）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 -5 の小さなタイルの 1 つ 1 つが送信元ホストごと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 -6 のように可視化される．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 -6 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例である．

分析エンジン

（1）変化点検出エンジン[3)]

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 -7 は 2003 年 8 月に大規模感染を引き起こした MSBlast に

図 -5　Tiles

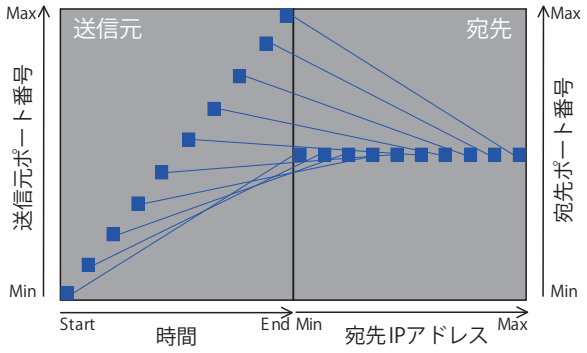

図 -6　各タイルの表現手法

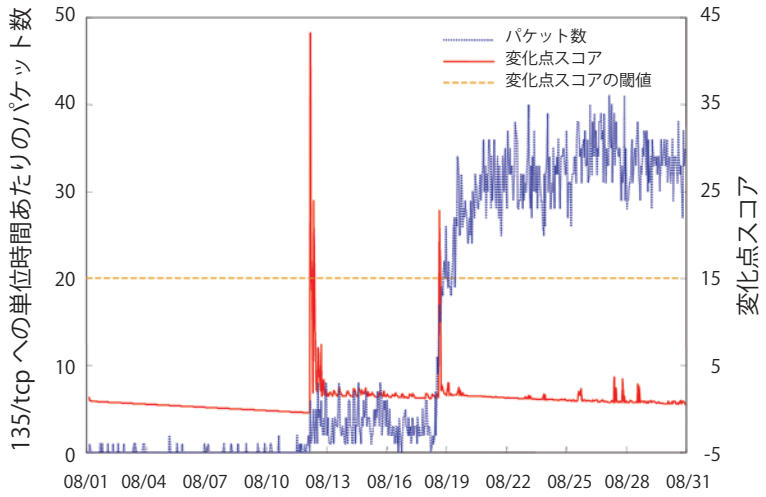

図 -7　変化点検出エンジンによる MSBlast の検出例

よる 135/tcp 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．

(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，自己組織化マップ（SOM）でホストのクラスタリングを行う SOM 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など，さまざまな分析エンジン群を研究開発中である．

●ミクロ解析システム[4)]

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

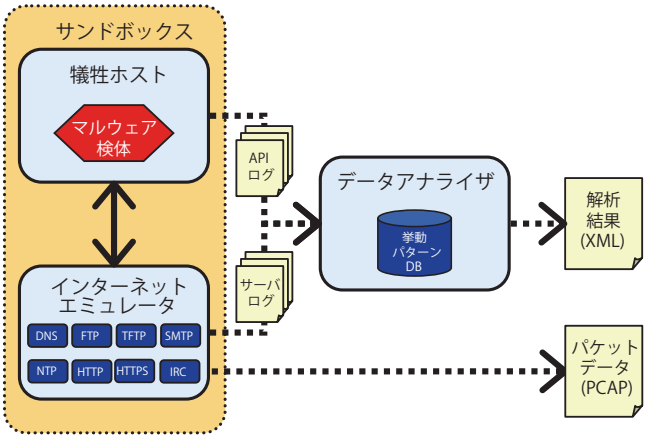

図 -8　マルウェア動的解析エンジン

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．

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）上でいったん実行し，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．

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，先に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（図 -8）．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．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，ボットの実行コードからボット制御コマンドおよびパスワードを抽出するボット解析エンジン，動的解析の結果を利用した駆除ツール自動生成エンジン，そしてマルウェアに関連したあらゆる情報を蓄積するマルウェア情報プールなどの研究開発が進行中である．

●相関分析システム [1), 2)]

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[☆4]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．このように，マクロとミクロの解析結果を融合することで，発生中のインシデントとそ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を導き出すことも可能となる．

ここでは，相関分析システムによって，新規のスキャンパターンの発見からマルウェアの特定に至った一事例を示す．この事例では最初に，マクロ解析システムの振舞分析エンジンが tcp/42，tcp/445，tcp/1025，tcp/1433 の 4 つのポートに対して大量の TCP SYN パケットを送信するホスト群を新規スキャンパターンとして検出した．変化点検出エンジンもまた，これらのポート番号に対するパケット数が急激に増加していることを検出していた．そこで，相関分析システムは，ミクロ解析システムでハニーポットによって捕獲したマルウェアの解析結果の中から，マクロ側で観測されたスキャンのプ

☆4 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．

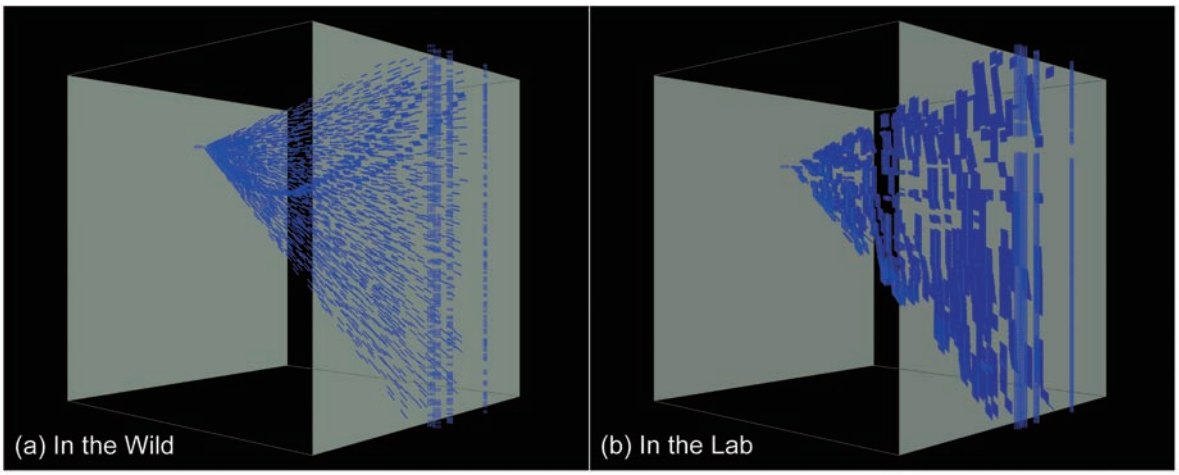

図 -9　W32.Dasher.D のスキャン

ロファイルと類似したスキャンパターンを持つものを探索した．その結果，マクロ側のスキャンときわめて高い相関性を示すスキャンを行うマルウェアの検体が特定された．その検体は W32.Dasher.D（Symantec 社による分類）と呼ばれるワームであった．**図 -9** の（a）はマクロ解析システムで観測されたスキャン，（b）はミクロ解析システムで動的解析の結果得られたスキャンを，Cube で可視化したものである．

より高精度なインシデント対策に向けて

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，対策法の導出を目指すインシデント分析センター nicter について解説した．一般に，ネットワーク経由のマルウェア感染行為は，脆弱点を探索するスキャン，エクスプロイトコードの送信，マルウェア本体の感染という段階を踏む．現状の nicter は，マルウェア感染の初期段階であるスキャンに基づく相関分析に注力しているが，今後の研究開発では，エクスプロイトコードの送信やマルウェア本体の感染の段階を含めた相関性の解析を深め，より精度の高いインシデント対策の実時間での提供を目指していく．

参考文献

1) Nakao, K., Yoshioka, K., Inoue, D. and Eto, M. : 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) Inoue, D., Eto, M., Yoshioka, K., Baba, S., Suzuki, K., Nakazato, J., Ohtaka, K. and Nakao, K. : 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) Inoue, D., Yoshioka, K., Eto, M., Yamagata, M., Nishino, E., Takeuchi, J., Ohkouchi, K. and Nakao, K. : 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).
4) Inoue, D., Yoshioka, K., Eto, M., Hoshizawa, Y. and Nakao, K. : Malware Behavior Analysis in Isolated Miniature Network for Revealing Malware's Network Activity, IEEE International Conference on Communications (ICC 2008), pp.1715-1721 (2008).

（平成 21 年 1 月 29 日受付）

中尾 康二（正会員）
ko-nakao@nict.go.jp
1979 年 早稲田大学卒業後，国際電信電話（株）に入社．KDD 研究所を経て，現在 KDDI（株）情報セキュリティフェロー，および（独）情報通信研究機構（NICT）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リーダー兼務．ネットワークおよびシステムを中心とした情報セキュリティ技術にかかわる技術開発に従事．2002 年より早稲田大学非常勤講師．本会研究賞，経済産業省大臣賞，総務省局長表彰等を受賞．電子情報通信学会会員．

井上 大介
dai@nict.go.jp
2003 年横浜国立大学大学院工学研究科博士課程後期を修了後，通信総合研究所（現（独）情報通信研究機構）に入所．新世代モバイル研究開発プロジェクトを経て，nicter の研究開発に従事．博士（工学）．

衛藤 将史
eto@nict.go.jp
2005 年奈良先端科学技術大学院大学情報科学研究科博士後期課程を修了後，（独）情報通信研究機構において nicter の研究開発に従事．博士（工学）．

吉岡 克成（正会員）
yoshioka@ynu.ac.jp
2005 年横浜国立大学大学院環境情報学府博士課程後期を修了後，（独）情報通信研究機構において nicter の研究開発に従事．現在，横浜国立大学学際プロジェクト研究センター特任教員（助教）．博士（工学）．

大高 一弘
ohtaka@nict.go.jp
1988 年電気通信大学短期大学部卒業，電離圏電波伝搬の研究，南極オーロラレーダ開発に従事．31 次および 36 次隊で南極越冬隊に参加．宇宙天気予報研究開発を経て，2007 年 7 月より情報通信セキュリティー研究センターインシデント対策グループにて nicter の研究開発に従事．