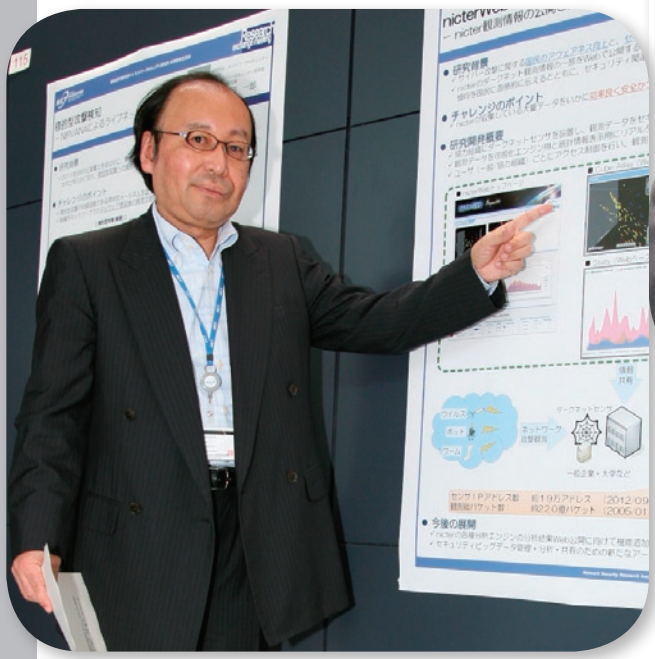
インシデント分析センター nicter

ー世界最先端のサイバーセキュリティ技術の研究開発ー



「nicter は進化型のセキュリティフレームワーク。日本の、そして世界のセキュリティを向上させるため、実践的なサイバーセキュリティ技術の研究開発を行っています。」

中尾 康二 (なかお こうじ)
ネットワークセキュリティ研究所
主管研究員

1979 年早稲田大学卒業後、国際電信電話株式会社に入社。KDD 研究所を経て、現在 KDDI 情報セキュリティフェロー、及び NICT ネットワークセキュリティ研究所 主管研究員兼務。ネットワーク及びシステムを中心とした情報セキュリティ技術に関わる技術開発に従事。

井上 大介 (いのうえ だいすけ)
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

2003 年横浜国立大学大学院工学研究科博士課程後期修了後、独立行政法人通信総合研究所(現 NICT)に入所。2006 年より nicter の研究開発に従事。現在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 室長と、ネットワーク研究本部 ネットワークシステム総合研究室 研究マネージャーを兼務。博士(工学)。SF 小説や SF 映画、テクノ、ハウス、エレクトロがエネルギー源。

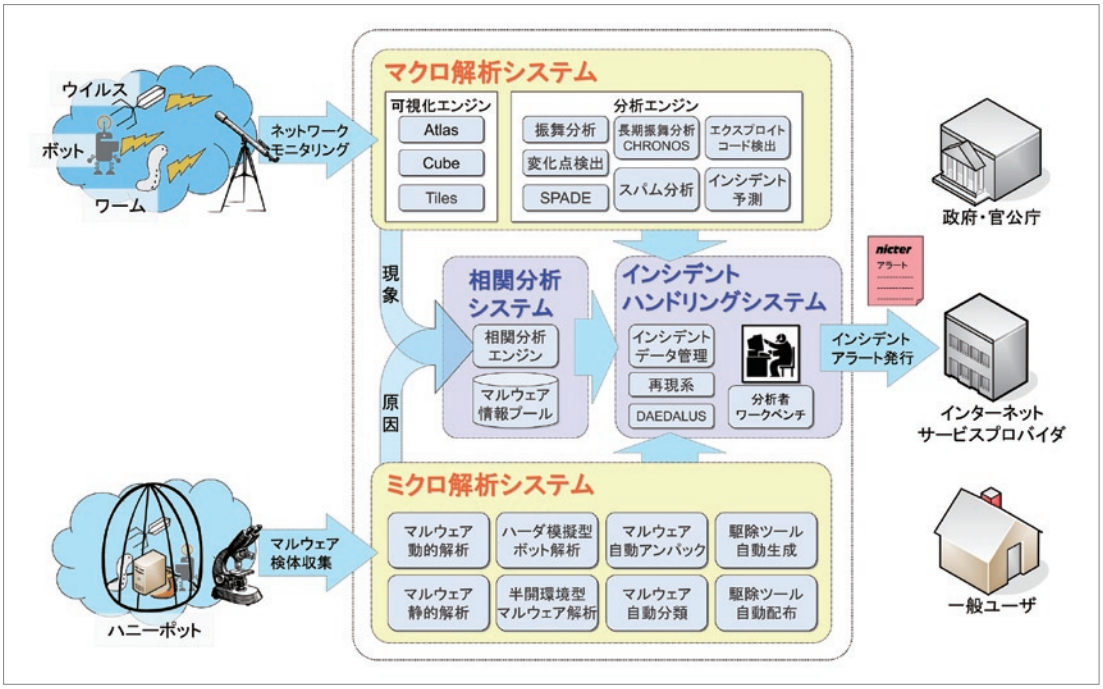


図1　nicterの全体像

はじめに

インターネットは私たち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ます。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サイバー攻撃の脅威も拡大の一途を辿っています。サイバー攻撃は人間であるクラッカー*1 が引き起こすものですが、そのツールとして使われるのがマルウェア*2 と呼ばれる不正なプログラムです。90 年代前半までマルウェア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かったのですが、90 年代後半以降は金銭詐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、高度化・巧妙化が急速に進んでいます。

このような、マルウェアに起因するサイバー攻撃に対抗するために、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では、インシデント分析センター nicter*3 の研究開発を進めています。

インシデント分析センター nicter

nicter はリモート感染型マルウェア*4 の世界的な活動傾向をリアルタイムに把握し、それに起因したサイバー攻撃の早期発見、原因究明、対策導出を可能にするため、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、インシデントハンドリングシステムの 4 つのサブシステムから構成されています(図 1)。以下では、これらのサブシステムの概要を紹介します。

● マクロ解析システム

マクロ解析システムでは、国内外の複数地点に観測用のセンサを設置し、「未使用」の IP アドレス

*1　悪意を持ってハッキング行為を行う者。
*2　ウィルス、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。
*3　Network Incident analysis Center for Tactical Emergency Response.
*4　ネットワークを経由して能動的に攻撃を行うことで感染を広げるタイプのマルウェア。最近では 2008 年 11 月に感染爆発を起こした Conficker や、2011 年 8 月から増加傾向が確認されている Morto などが有名。

を大量*5 に観測しています。本来、未使用の IP アドレスに対して通信は成立し得ませんが、実際に観測してみると相当数のパケットが届きます。これらの大部分は、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通信など、マルウェアに起因したパケットなのです。したがって、未使用の IP アドレス（以下、ダークネット）を観測・分析することによって、インターネットにおけるセキュリティインシデントの一大要因となっているマルウェアの活動傾向を捉えることが可能になります。以下、マクロ解析システムに含まれる可視化エンジンについて概説します。

(1) Atlas

Atlas（図 2）は、ダークネットに流れ込むトラフィック（以下、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す。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 IP アドレスから送信元の緯度・経度を割り出し*6、その送信地点から宛先 IP アドレスが属する国の首都に向けて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ます。各パケットの色はパケットの種別*7 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）しています。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など、分析者のインタラクティブな操作が可能です。

(2) Cube

Cube（図 3）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、三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す。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 3 の左平面）から宛先（図 3 の右平面）に向けてパケットを通過させることで、マルウェアによるスキャンの形状などが可視化されます。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などを表示でき、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す。

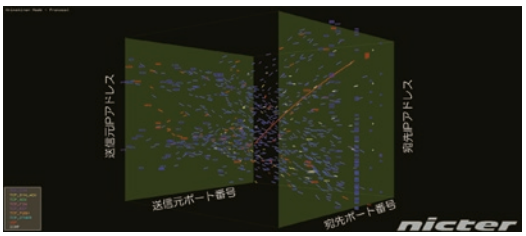


図3　Cube

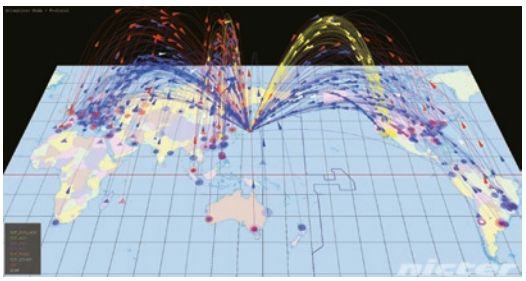


図2　Atlas

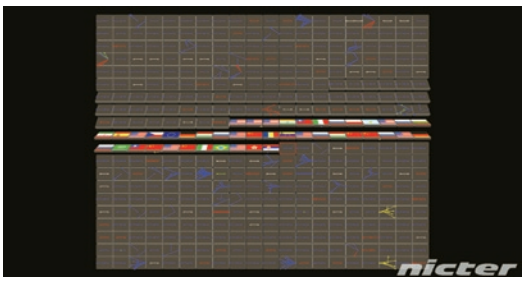


図4　Tiles

*5　2012 年 3 月末現在で約 19 万の IPv4 アドレス。
*6　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
*7　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）

(3) Tiles

Tiles(図 4) 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・可視化するエンジンです。図 4 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きます。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ます。1 つのタイルは、パケットの時刻、送信元 / 宛先ポート番号、宛先 IP アドレスを用いて可視化および分類されます。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ります。

マクロ解析システムでは前述の可視化・分析エンジンに加えて、図 1 上部に示すような各種分析エンジンの研究開発を行っています。

● ミクロ解析システム

ミクロ解析システムは、ハニーポットと呼ばれる囮(おとり)サーバや Web サイトの巡回を行う Web クローラなどでマルウェアの検体を捕獲し、その検体を自動解析するシステムです。以下、ミクロ解析システムに含まれる動的解析エンジン(図 5) について概説します。

リアル空間においてウィルスをシャーレで培養して観察するように、動的解析はマルウェアをサンドボックスと呼ばれる箱庭環境で実行し、その際にマルウェアが使用した API[*8] やネットワークアクセスなどの挙動を解析する手法です。ところが、近年の高度化されたマルウェアは動的解析に対抗するため、自己の周囲のネットワーク環境を調査して、自己がサンドボックス内にいることを検知すると実行停止や自己消去を行なうなどの解析回避機能を持っています。そのため、nicter の動的解析エンジンは、サンドボックス内に DNS サーバや Web サーバなど多数のダミーサーバからなるインターネットエミュレータを配置することで、マルウェアの解析回避機能を無効化しています。また、マルウェアが解析回避のために行う仮想マシン検出に対抗するため、マルウェアを実行する犠牲ホストは OS 自動復元機構を持った実マシンによって構成されています。

このようなサンドボックス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できます。加えて、犠牲ホストとインターネットエミュレータの間で観測される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ります。

動的解析エンジンは 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 7,000 検体の解析が可能となっています[*9]。

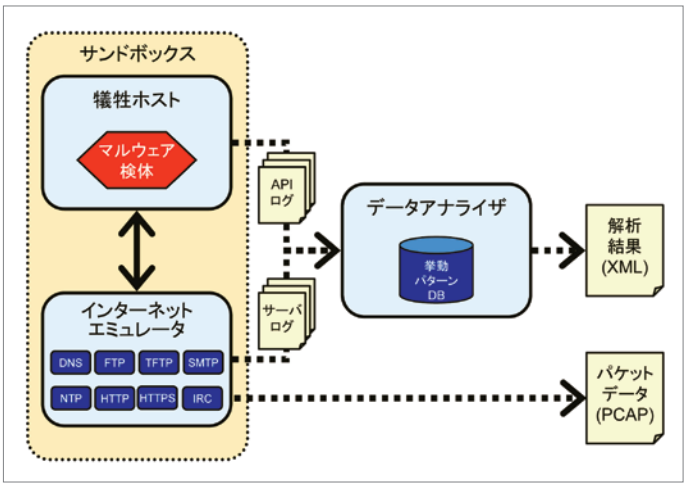


図5　マルウェア動的解析エンジン

*8　Application Program Interface.
*9　2012 年 3 月末現在。

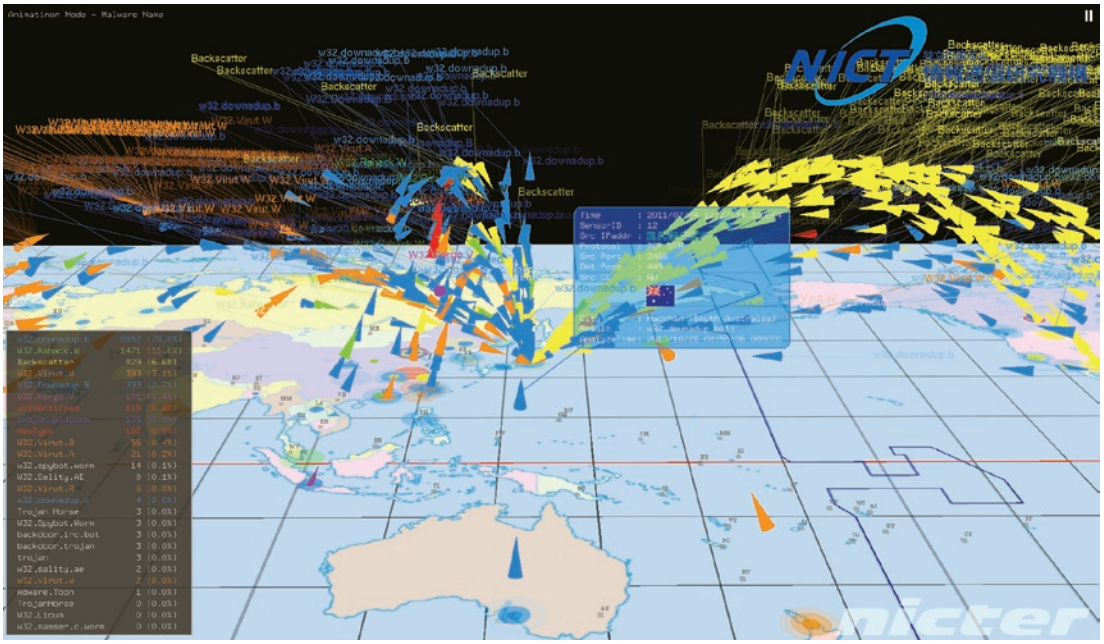


図6　相関分析結果の可視化

ミクロ解析システムでは、前述の動的解析エンジンに加えて、図1下部に示すような各種解析エンジンの研究開発を行っています。

● 相関分析システム

相関分析システムは、マクロ解析システムにおいて観測されたマルウェアからのスキャンを各種の特徴*10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します。つまり、マクロ解析システムで捉えた「現象」(サイバー攻撃)と、ミクロ解析システムで蓄積した「原因」(マルウェア)とを結びつける答え合わせのシステムです。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ます。

図6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す。各パケットオブジェクトの上方に、相関分析の結果、第一候補として挙げられたマルウェア名を表示しています。また、パケットの詳細情報の中にもマルウェア名(図6の例ではw32.downadup.b)を表示しています。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活動傾向を把握することが可能となります。図6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年時点で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)に感染しているものと自動推定しています。

● インシデントハンドリングシステム

インシデントハンドリングシステムは、マクロ解析、ミクロ解析、相関分析の各サブシステムからの出力を集約・蓄積し、インシデント発生時の

*10 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。

データ管理や、その再現を可能にします。また、DAEDALUS[*11] は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です。以下、DAEDALUSについて概説します。

従来のダークネット観測は組織外からダークネットに飛来するパケットを観測する、つまり“外から内”への異常な通信を収集するという考え方でした。一方、DAEDALUSは組織内から送出されたパケットを分散配置されたダークネットで観測する、つまり“内から外”(または内から内)への異常な通信を網にかけるという、従来とは逆転したダークネットの活用法に基づいています。換言すると、DAEDALUSは組織内で起こったマルウェア感染などをダークネットによって検知し、該当する組織にアラートを自動送信することで、ダークネット観測をサーバやホストが存在するライブネットの保護に活かすシステムです。

図7はDAEDALUSの可視化エンジンです。中央の球体がインターネット、その周りを周回している各リングが、nicterのセンサを設置している各組織のネットワークを表しています。球体とリングの間を飛び交う流星状のオブジェクトはダークネットトラフィックを表しています。リングの水色の部分がライブネット、濃紺の部分がダークネットであり、リングの外周の「警」のマークは組織内でアラートの原因となった送信元ホストを指し示しています。この可視化エンジン上でのアラート表示と同時に、該当組織にはメールベースのアラートが自動送信され、実際のセキュリティオペレーションのトリガとして活用されています。

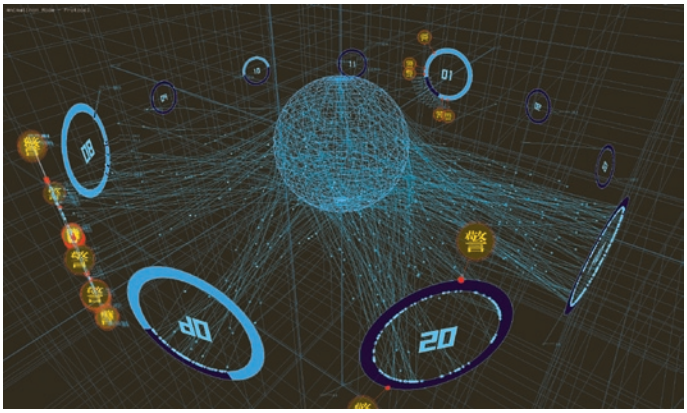


図7　DAEDALUSの可視化エンジン

まとめと今後の課題

本稿では、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について概説しました。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リモート感染型マルウェアの大局的な活動傾向の把握と迅速な原因究明が可能となり、その分析結果の一部はnicterWeb[*12] というサイトから一般公開を行っています。また、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の外部展開など、研究成果の社会還元を推進しています。

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を媒体とした攻撃手法(ドライブ・バイ・ダウンロード攻撃)や、SNSを媒介したマルウェア、特定の組織を狙った標的型攻撃など、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ます。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きます。

*11 Direct Alert Environment for Darknet And Livenet Unified Security.
*12 http://www.nicter.jp/