サイバー攻撃観測網について

独立行政法人 情報通信研究機構 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
井上（いのうえ）　大介（だいすけ）

1．はじめに

日々高度化、巧妙化を続けるサイバー攻撃を大局的かつ迅速に把握するため、情報通信研究機構（以下NICT）では日本最大のサイバー攻撃観測網を持つインシデント分析センタnicter（Network Incident analysis Center for Tactical Emergency Response）の研究開発を推進している（**図1**）。本稿では、nicterのサイバー攻撃観測網とその応用について概説する。

2．ダークネット

サイバー攻撃観測網として、nicterでは大規模なダークネットを利用している。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、リモート感染型のマルウェア[1]が送信するスキャンや攻撃（エクスプロイト）コード、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SYNフラッド攻撃に対する応答であるバックスキャッタ等、インターネット上で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。

2013年1月現在、 nicterは約20万のIPv4アドレスをダークネットとして用いており、ダークネット観測網としては日本最大、世界でも最大級の観測規模となっている。このダークネット観測網は、NICTと協力関係にある日本国内外の組織に分散配置されたダークネット観測用センサによって構成されており、各組織の未使用IPアドレスに到来するパケットを収集して、nicterのセンタにリアルタイム送信している。

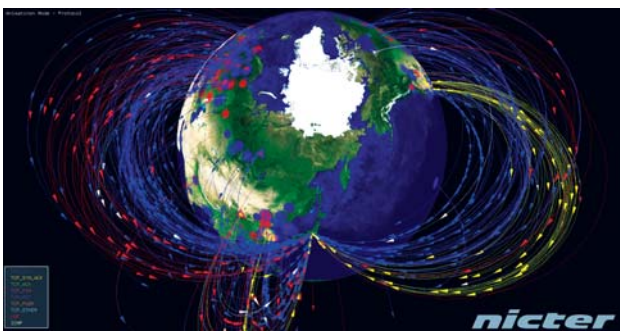

図１．nicterのサイバー攻撃観測網による観測結果のリアルタイム可視化

3．ダークネットセンサ

ダークネット観測を行うセンサは、パケットの送信元に対する応答の程度によって次の3種類に分類される。

＊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。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ため、収集できる情報の深度は浅い。

＊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 SYNパケットに対してSYN-ACKパケットを返すセンサや、OSの既知の脆弱性をエミュレートするロー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の傾向等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。

＊高対話型センサ：実ホスト、若しくはそれに準じた応答を返すセンサ（いわゆる、ハイインタラクションハニーポット）。マルウェア感染時の挙動や攻撃者のキーストロークまで多様な情報が取得可能であるが、センサ自身が実際にマルウェアに感染するため、二次感染やスパム送信を防ぐなど、安全な運用を行うためのコストは高く、大規模運用には不向きである。

図2は、上述した3種類のセンサそれぞれについて、設置の大規模性と、取得できる情報の深度を示している。

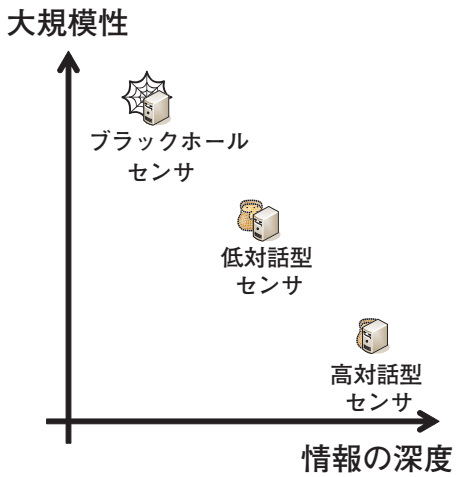

図２．センサの種類と大規模性ー情報深度の関係

４．ダークネット観測結果

図3はnicterのダークネット観測網全体の約33%の規模を持つ、/16ダークネット（6万5,536IPアドレスブロック）に設置したブラックホールセンサによって、2012年1月1日～2012年12月31日の期間に観測されたダークネットトラヒックの統計を示している。図中の赤色の実線は1日当たりのパケット数を、青色の実線は1日当たりのユニークホスト数（重複を除外した送信元ホスト数）を示している。

パケット数のピークは約1,074万パケットで8月26日に、ユニークホスト数のピークは約32万ホストで12月15日に、それぞれ観測している。1日平均では約589万パケットが、約27万ユニークホストからダークネットに向けて送信された計算になる。

このような、nicterのダークネット観測網の観測結果の一部はnicterWeb[2]の上で、リアルタイムに可視化されるとともに、統計情報や、ユニークホスト数/パケット数の国別及びポート別のTop10リストとして随時公開されており（**図4**）、リモート感染型のマルウェアの大局的な活動傾向を把握することができる。

５．大規模ダークネット観測に基づくアラートシステムDAEDALUS

DAEDALUS（Direct Alert Environment for Darknet And Livenet Unified Security）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ある。従来のダークネット観測は、ダークネットトラヒックからリモート感染型マルウェアの活動傾向を把握することが主な目的であったが、一方でサーバやホストが接続している、組織の実ネットワーク（以下、ライブネット）の保護に直結していないという課題があった。DAEDALUSはダークネットの観測結果をライブネットの保護に直接的に活用するために開発されたシステムである。

図5はDAEDALUSがアラートを発行する3つのケースを図示している。ケース1では、組織Gのライブネット（水色部分）の一部でマルウェア感染が起こり、組織内で感染を広げるためのローカルなスキャンを行っている。スキャンパケットは組織G内のダークネット（濃紺部分）にも届いているため、nicterはこのスキャンを検知して、組織GのPOC（Point of Contact）にアラートを送信している。ケース2では、組織G

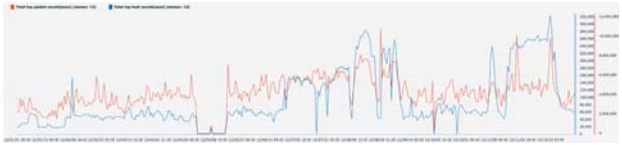

図３．/16ダークネットの観測結果（2012年）

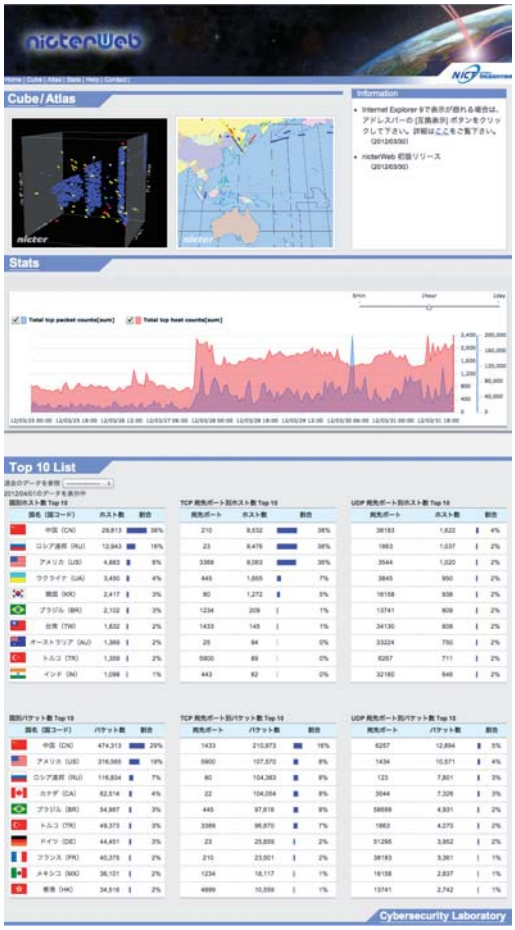

図４．nicterWeb

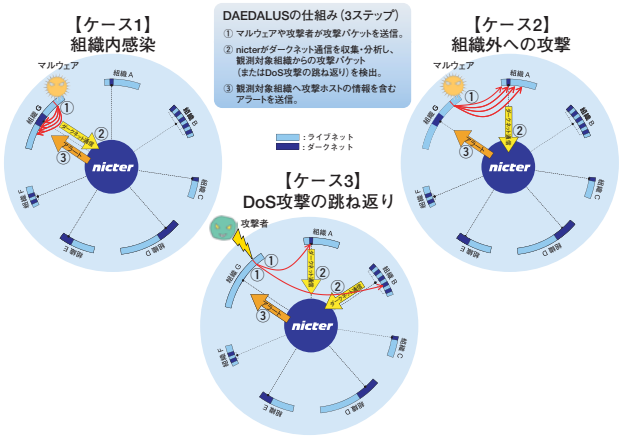

図５．DAEDALUSがアラートを発行する3ケース

内のマルウェア感染ホストが、組織Aのダークネットにスキャンを行っているため、同じくnicterがスキャンを検知して、組織Gにアラートを送信している。ケース3では、攻撃者が組織Gの特定アドレスに対して、送信元IPアドレスをランダムに詐称したDoS攻撃（SYN flood攻撃）を行っており、その跳ね返り（SYN-ACK）パケットが、複数の組織のダークネットで検知されている。この場合も、nicterから組織Gに対して、アラートが即時送信される。

このようにDAEDALUSは、ダークネット観測網に参加している組織が、組織の内外に攻撃を行った場合や、送信元IPアドレスをランダムに詐称したDoS攻撃を受けた場合に、nicterがそれを検知し、当該組織に即時アラートを送信することで、ダークネット観測結果をライブネットの保護に活かしている。DAEDALUSアラートは、nicter のブラックホールセンサを設置可能な大学等の教育機関には無償提供されている。また、DAEDALUSアラートを利用した商用のアラートサービスも民間企業がスタートさせている。

図6はDAEDALUSのアラート発行状況を俯瞰的に把握するための可視化エンジンDAEDALUS-VIZである。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組織のネットワークを表している。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ヒックを表している。リングの水色の部分

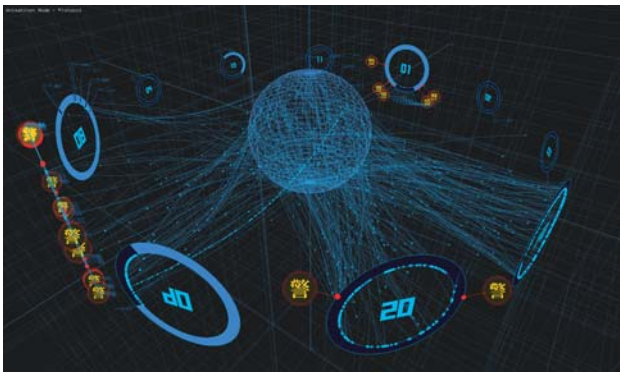

図６．DAEDALUSの可視化エンジン（DAEDALUS-VIZ）

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る。このDAEDALUS-VIZ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る。

6．おわりに

本稿では、NICTが研究開発を行っているnicterのサイバー攻撃観測網の仕組みと観測結果を示すとともに、その応用技術であるDAEDALUSについて概説した。

ダークネットでその活動を観測できるのは、能動的に感染活動を行うリモート感染型マルウェアであり、ユーザのWebアクセスをトリガとするドライブ・バイ・ダウンロード攻撃や、ターゲットとなる組織を絞った標的型攻撃などは、大規模観測の網にはかからない。そのため、NICTでは新たな観測・分析・対策の仕組みを確立するため、ドライブ・バイ・ダウンロード攻撃対策フレームワークや、標的型攻撃対策技術の研究開発に取り組んでいる。

注

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　http://www.nicter.jp/