2-5　大規模ダークネット観測に基づくアラートシステムDAEDALUS

2-5　DAEDALUS: Practical Alert System Based on Large-scale Darknet Monitoring for Protecting Live Networks

鈴木未央　　井上大介
SUZUKI Mio and INOUE Daisuke

要旨

未使用のIPアドレス群をモニタリングするダークネット観測は、ネットワークを流れる不正なトラフィックの傾向把握に有用であるが、サーバやホストが存在する実ネットワークの保護との直接的な結びつけや、センサと呼ばれるパケット収集用サーバマシンを広域展開する際の導入組織へのインセンティブの確立が課題である。本稿ではダークネット観測の別の利活用法として、組織内部のネットワークに存在する不正ホストを検知し、管理者に対するアラート通知を可能とするシステムDAEDALUS（Direct Alert Environment for Darknet And Livenet Unified Security）について概説し、その設計と実装、および試験運用について報告する。DAEDALUSの、試験運用を通じて、本システムが組織内部の不正ホストや誤設定が行われたホストの検知に有用であることを確認した。

A darknet is a set of globally announced unused IP addresses and using it is a good way to monitor network attacks such as malware's scans. However, large-scale darknet monitoring systems had two problems: 1) the systems have less direct contribution to protect the live networks; 2) the systems provide less incentive to organizations that will deploy a sensor on their darknet. In this paper, describe a novel darknet monitoring architecture to solve the above two problems. Based on the architecture, we designed, implemented, and conducted trial operations of an alert system named DAEDALUS. The DAEDALUS enables us to detect malicious hosts in an internal network of an organization, and to send alerts to an operator of the organization. After the trial operations, we have confirmed that the DAEDALUS is effective to detect malicious hosts and misconfigured hosts in the internal networks.

[キーワード]
ダークネット観測，ブラックホールセンサ，実ネットワーク保護，アラート
Darknet monitoring, Black hole sensor, Live network protection, Alert

1　はじめに

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[1]-[3]。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が送信するスキャンやエクスプロイトコード、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。ダークネット観測の最大の利点は、トラフィックを正・不正で区別する必要がなく、大半のパケットを不正なものと見なすことが出来る点にある。

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。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 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の傾向等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。
- **高インタラクションセンサ**：実ホスト、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、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。

著者らが研究開発を進めているインシデント分析センターnicterでは、日本国内に点在する複数のダークネットにブラックホールセンサを設置し、定常的な観測を行っている[4]-[6]。このようなダークネットの定常的観測を通して、我々は次に示す2つの課題に直面した。

(1) 実ネットワーク保護への直結

ダークネット観測は、インターネット上の不正な活動の傾向把握に有用であるが、サーバやホストが存在する、組織の実ネットワークの保護に直結していなかった。

(2) センサの広域展開

ダークネット観測の精度は、観測するアドレス数が多いほど向上するため、センサの広域展開が重要であるが、他組織にダークネットの提供とセンサ設置を促すためのインセンティブが必要となっていた。

本稿では、上記2つの課題を同時に解決する新たなダークネット観測のアーキテクチャについて解説し、このアーキテクチャを具現化したアラートシステムDAEDALUS（Direct Alert Environment for Darknet And Livenet Unified Security）の設計と開発、並びに試験運用結果について報告する。DAEDALUSによって、これまでは疎な関係であったダークネット観測と実ネットワーク保護を直接的に結びつけることができ、ダークネット観測の可能性を押し広げるとともに、nicterセンサの広域展開を促進することができた。

以下、**2**で関連研究について述べ、**3**で提案アーキテクチャについて述べる。**4**ではアラートシステムDAEDALUSの設計と実装について述べ、**5**、**6**でDAEDALUSの試験運用結果を示し、**7**で考察と今後の課題について述べる。

2 関連研究

2では、国内外の主要なネットワーク観測プロジェクトについての概要を記す。

- Network Telescope[2]

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。

- IMS（Internet Motion Sensor）[3]

米国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[9][10]

仏国の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[11]を使用していたが、第2世代の

Leurre.com v2.0 ではSGNET [12] を使用して情報収集能力の向上を図っている。

- REN-ISAC [13]

  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。

- ISC（Internet Storm Center）[14]

  米国のSANS（SysAdmin, Audit, Networking, and Security）による、セキュリティ情報の収集・分析プロジェクト。50万アドレス以上のファイアウォールログを、DShield [15] と呼ばれるシステムに集約し、統計情報やボランティアによる分析レポートを公開している。

国内ではISDAS [16]、@police [17]、MUSTAN [18]、WCLSCAN [19] 等のネットワーク観測プロジェクトが進行中である。

上記の各種プロジェクトは、インターネット上の不正なトラフィックの傾向把握に主眼を置いている。一方、本稿で提案するアーキテクチャは、ダークネット観測と実ネットワーク保護の直接的な結びつけを目的としている。

3　提案アーキテクチャ

ここでは、ダークネット観測結果を用いて実ネットワーク保護を行うための提案アーキテクチャについて述べる。従来のブラックホールセンサを用いたダークネット観測では、インターネット上の不正なトラフィックの傾向把握を目的として観測を行っている。このため、従来の観測アーキテクチャは、組織が保有するダークネットに到達したトラフィック（以下、ダークネットトラフィック）を、組織内に設置したセンサに向けて転送し、センサがダークネットトラフィックを中央の分析センターに送信する。分析センターは各組織のセンサから集まったダークネットトラフィックを分析し、トラフィックの統計情報等を公開するという形が一般的であった。

著者らが提案する新たなアーキテクチャは、従来のダークネット観測アーキテクチャを踏襲し、特に各組織に設置したセンサには変更を必要としない。このため、nicterで構築してきた大規模ダークネット観測網をそのまま活用でき、かつ、実ネットワーク内のマルウェア感染やネットワーク機器の設定ミスなどを検知することが可能となる。提案アーキテクチャを以下に示す。

3.1　想定環境

図1に提案アーキテクチャの想定環境を示す。ダークネットを提供する組織（Organization A～G）は、組織内にブラックホールセンサを設置し、ダークネットトラフィックをセンサに向けて転送する。従来のダークネット観測と異なるのは、各組織が実ネットワーク（以下、ライブネット）として使用しているIPアドレスのレンジを分析センター（Analysis Center）に登録しておく点である。

分析センターは、従来のダークネット観測を行うと同時に、ダークネットトラフィックの中に、各組織が登録したライブネットのアドレスを送信元IPアドレスに持つパケットの検出を行う。仮にそのようなパケットが検出された場合、パケットの送信元の組織のPOC（Point of Contact）にアラートを送信する。

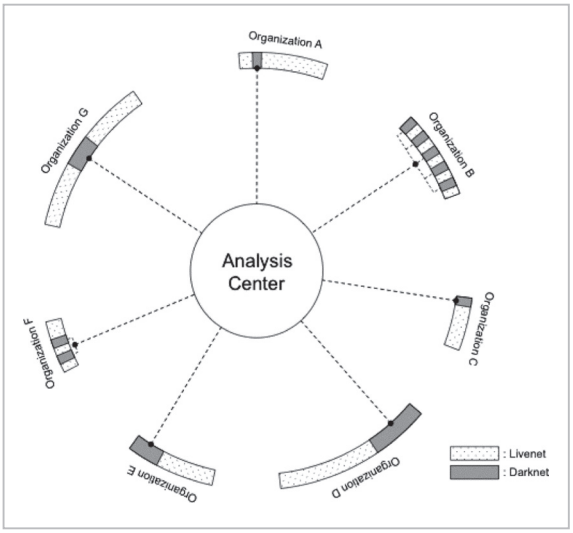


図1　提案アーキテクチャの想定環境

3.2　内部ダークネットでの不正ホスト検出

ある組織において、自組織が管理するIPアドレスのレンジ内に含まれるダークネットを、内部ダークネットと呼ぶこととする。組織内で、マル

ウェアに感染したホストがローカルスキャン（典型的には感染ホストを含む /24 や /16 ネットワークへのスキャン）を行い、内部ダークネットにスキャンが到達した場合、分析センターがそれを検出し、該当する組織にアラートを送信する。図 2 の例では、組織 G 内でマルウェアに感染したホストがローカルスキャンを行った結果、組織 G に対して分析センターからアラートが送信されている。内部ダークネットではローカルスキャン以外にも、組織内でのネットワーク設定の間違い等によって、自組織からのパケットが検出される場合もあるが、いずれにせよ不正なパケットであるため、アラートはネットワーク管理上の有用な情報となり得る。

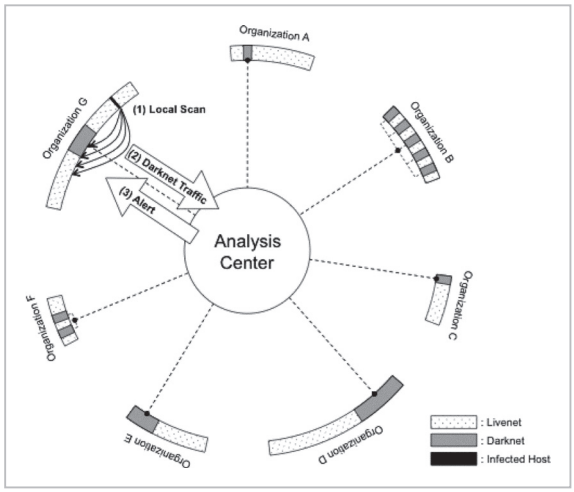


図 2 内部ダークネットでの不正ホスト検出

3.3 外部ダークネットでの不正ホスト検出

ある組織において、自組織が管理する IP アドレスのレンジ外のダークネットを、外部ダークネットと呼ぶこととする。組織内で、マルウェアに感染したホストがグローバルスキャン（感染ホストが属する組織外へのスキャン）を行い、外部ダークネットにスキャンが到達した場合、分析センターがそれを検出し、スキャン元のホストが存在する組織にアラートを送信する。図 3 の例では、組織 G 内でマルウェアに感染したホストがグローバルスキャンを行い、スキャンが組織 A のダークネットに到達した結果、組織 G に対して分析センターからアラートが送信されている。外部ダークネットではグローバルスキャン以外にも、分析センターに登録されたライブネットからのバックスキャッタが検出された結果、アラートが送信される場合もあるが、それは自組織のサーバが何らかの攻撃を受けている可能性を示唆しており、セキュリティ上重要な情報である。

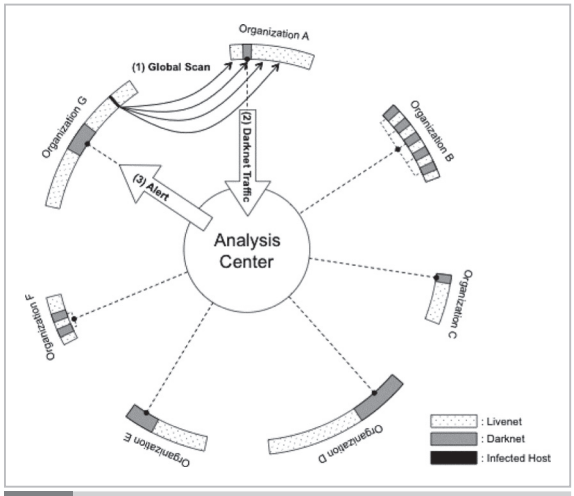


図 3 外部ダークネットでの不正ホスト検出

4 アラートシステム DAEDALUS の設計と実装

ここでは、**3** で概要を述べた提案アーキテクチャに基づくアラートシステム DAEDALUS の設計と実装について述べる。

4.1 DAEDALUS の設計

DAEDALUS の目的は、従来のダークネット観測を実ネットワークの保護に結びつけることである。この DAEDALUS の設計要件として、既存の nicter のシステムと親和性を持ち、nicter で収集されたデータや分析結果を利用できることを重要視した。

4.1.1 DAEDALUS の構成要素

前述の要件を念頭に設計した DAEDALUS の構成要素とデータフローを図 4 に示す。

DAEDALUS は **3** で述べたとおり、ダークネットを提供する複数の組織（Organizations）と分析センター（Analysis Center）により構成される。各組織はブラックホールセンサ（Blackhole Sensor）を設置し、ダークネットトラフィックを

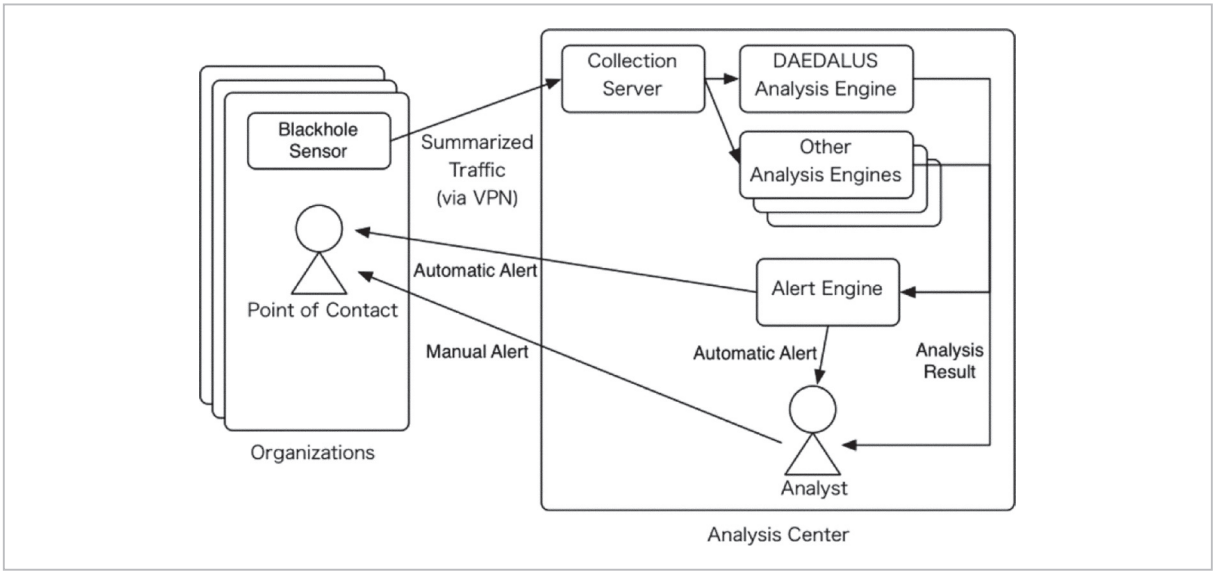


図4 DAEDALUSのデータフロー

収集する。収集されたトラフィックは、センサにより分析に必要な情報のみを残したサマリデータとしてVPNを介して分析センターに送信される。サマリデータはセンサのID、収集時刻、パケット毎のID、IPヘッダ、トランスポートプロトコルのヘッダ、ペイロード部分のハッシュから構成される。分析センターでは収集サーバ(Collection Server)が各組織から送信されたサマリデータを受信し、DAEDALUS分析エンジン(DAEDALUS Analysis Engine)や他の既存分析エンジン(Analysis Engines)に対して配付する。なお、これらの仕組みのうちDAEDALUS分析エンジンを除く要素については、既存のnicterに備わっている構成[20]をほぼそのまま利用している。

DAEDALUS分析エンジンには、各組織が使用しているIPアドレスレンジ(ライブネット)と未使用のIPアドレスレンジ(ダークネット)が登録されている。センサにおいて、ライブネットのIPアドレスレンジを送信元IPアドレスに持つパケットを検出すると、その頻度等を分析し、分析結果(Analysis Result)をアラートエンジン(Alert Engine)と分析者(Analyst)に送信する。アラートエンジンは分析結果を元に頻度等により重要性を判断し、組織のPOCや分析者に対して自動送信アラート(Automatic Alert)を送信する。また、分析者は受け取った解析結果やアラートを元に、重要なもの選り分けた後、組織のPOCに連絡(Manual Alert)する。

4.1.2 自動送信アラート

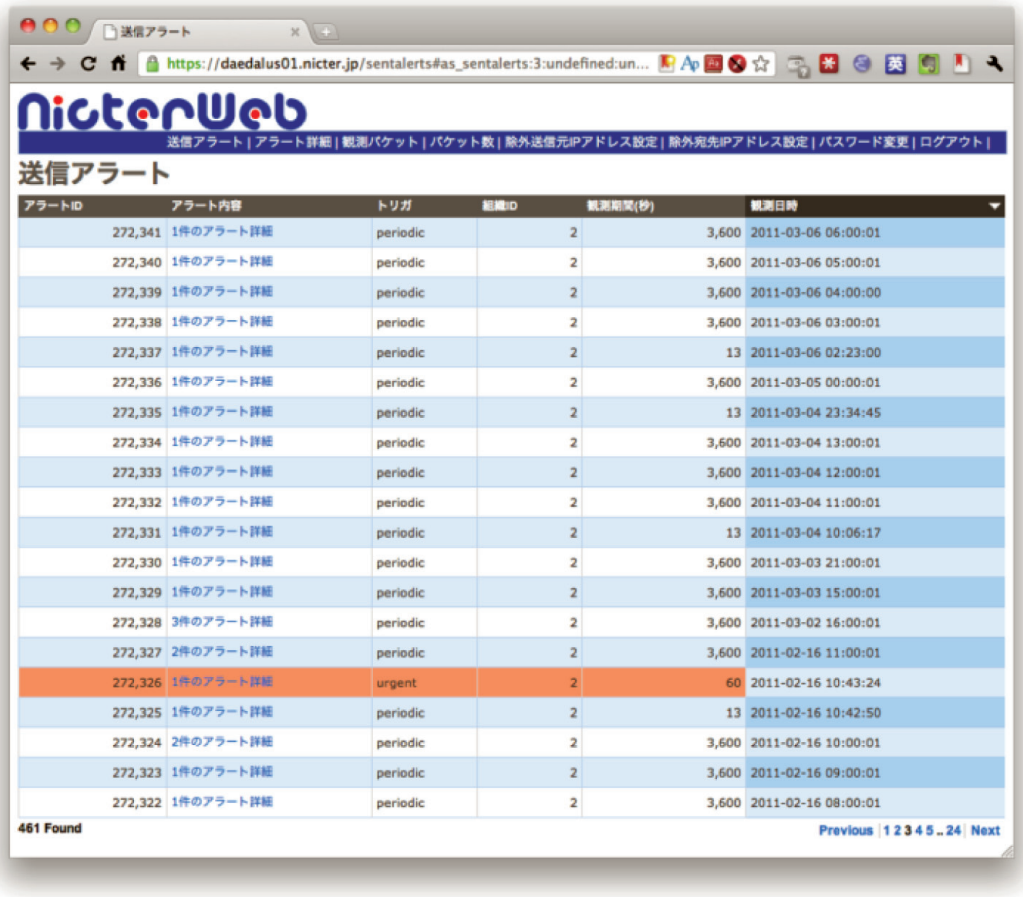
ここではDAEDALUSアラートエンジンが送信する自動送信アラートについて述べる。DAEDALUSは不正なトラフィックひいては不正なホストを検出することを目的としている。このため、著者らは不正トラフィックに含まれる送信元IPアドレスに着目し、検出されたパケットを送信元IPアドレス毎に、ある単位時間で集計する設計とした。送信元IPアドレス毎に集計することにより、1つのアラートを見るだけでその不正ホストの挙動を把握できる。また、ある単位時間で集計することにより、アラートの送信数を削減できる。具体的な集計後のアラートとして、新規アラート、継続アラート、緊急アラートの3種類のアラートを送信する設計とした。ここで具体的な例を挙げ、各アラートについて説明する。ある送信元IPアドレスがダークネットに向けてシーケンシャルスキャンを開始したと仮定する。ここで、最初にダークネットを宛先アドレスとするパケットが観測された時点で、新規アラートが送信される。その後、継続的にパケットが観測された場合、単位時間毎に継続アラートが送信される。また、一定時間内にある閾値以上のパケットが観測された場合は、緊急アラートが送信される。これらのアラートはDAEDALUSがPOC又は分析者に対してほぼリアルタイムに自動送信される。

4.2 DAEDALUSの実装

ここでは、前述した設計に基づくDAEDALUSの実装について述べる。図4のうち、ブラックホールセンサ、収集サーバ、既存分析エンジンについては、既存のnicterのシステムをそのまま利用した。DAEDALUS分析エンジンとアラートエンジンについてはFreeBSD 7.3上のRubyで実装を行った。これは、POCに対してアラートの詳細な情報を閲覧させるためのWebインタフェイスを作成するにあたり、効率的に実装を進めるためにオープンソースのWebアプリケーションフレームワークであるRuby On Rails[21]を採用したことによる。また、システムのバックエンドのデータベースとしてMySQLを利用した。送信元IPアドレス、宛先IPアドレスが登録されているライブネット、ダークネットに含まれるかどうかの判定にはPatricia Trieのライブラリを用いた。

POCに送信するアラートは、概要はメールで送信し、詳細情報はWebインタフェイス経由で閲覧できるように実装した。これはメールに大量の情報を盛り込んで送信するよりも、Webインタフェイスで対話的に表示した方が可視性が高いためである。図5にWebインタフェイスのスクリーンキャプチャを示す。このWebインタフェイスでは、アラート詳細情報の閲覧だけではなく、送信元IPアドレス、宛先IPアドレスのホワイトリスト等を編集することができる。

アラートについては、継続アラートが集計される単位時間は1時間とする。また、緊急アラートが送信される条件はある送信元アドレスを含むパケットが1分間に1,000パケット以上検出された場合とする。またこれらの閾値は容易に変更可能となるよう実装を行った。この1,000パケットという値は、過去に爆発的な感染活動を行ったCodeRed[22]やSlammer[23]が出力するパケット数を参考にした。



アラートID	アラート内容	トリガ	組織ID	観測期間(秒)	観測日時
272,341	1件のアラート詳細	periodic	2	3,600	2011-03-06 06:00:01
272,340	1件のアラート詳細	periodic	2	3,600	2011-03-06 05:00:01
272,339	1件のアラート詳細	periodic	2	3,600	2011-03-06 04:00:00
272,338	1件のアラート詳細	periodic	2	3,600	2011-03-06 03:00:01
272,337	1件のアラート詳細	periodic	2	13	2011-03-06 02:23:00
272,336	1件のアラート詳細	periodic	2	3,600	2011-03-05 00:00:01
272,335	1件のアラート詳細	periodic	2	13	2011-03-04 23:34:45
272,334	1件のアラート詳細	periodic	2	3,600	2011-03-04 13:00:01
272,333	1件のアラート詳細	periodic	2	3,600	2011-03-04 12:00:01
272,332	1件のアラート詳細	periodic	2	3,600	2011-03-04 11:00:01
272,331	1件のアラート詳細	periodic	2	13	2011-03-04 10:06:17
272,330	1件のアラート詳細	periodic	2	3,600	2011-03-03 21:00:01
272,329	1件のアラート詳細	periodic	2	3,600	2011-03-03 15:00:01
272,328	3件のアラート詳細	periodic	2	3,600	2011-03-02 16:00:01
272,327	2件のアラート詳細	periodic	2	3,600	2011-02-16 11:00:01
272,326	1件のアラート詳細	urgent	2	60	2011-02-16 10:43:24
272,325	1件のアラート詳細	periodic	2	13	2011-02-16 10:42:50
272,324	2件のアラート詳細	periodic	2	3,600	2011-02-16 10:00:01
272,323	1件のアラート詳細	periodic	2	3,600	2011-02-16 09:00:01
272,322	1件のアラート詳細	periodic	2	3,600	2011-02-16 08:00:01

図5 DAEDALUSのWebインタフェイス

5　センサ設置組織における運用結果

ここでは、nicterのブラックホールセンサを設置している国内のある組織（以下、組織X）に対してDAEDALUSを導入し、試験的に運用を行った事例について紹介する。組織Xは/16ネットワークの中に、ダークネットとライブネットが混在する（図1の組織Bの様な）ネットワーク構成となっている。そこで、組織Xのライブネットを DAEDALUSに登録するIPアドレスとし、組織Xのダークネットを内部ダークネットと見なす。一方、その他の組織が保有するダークネットを外部ダークネットと見なす。運用期間は2010年8月1日から2011年1月31日までである。

5.1　検出パケット数と送信アラート数

表1に、運用期間中の月毎の全ダークネットで観測されたユニークホスト数、全ダークネットで観測された総パケット数、DAEDALUSで検出した組織Xの送信元アドレスを持つパケット数、DAEDALUSが自動で送信したアラート数、その自動送信アラートからnicterの分析者が抽出したマルウェアに起因すると推測されるアラート数をそれぞれ示す。自動送信アラートの数は、月平均452件、1日平均で15.1件となっている。著者らが調査した結果、この自動送信アラートの大半は、機器の設定ミスや機器に古い設定が残っているためであった。一方で、組織内のPC等に感染しているマルウェアに起因するアラートも少数ながら含まれていることが分かっている。このマルウェアに起因するアラートに対しては、感染拡大防止のために迅速な対処が必要となる。このため、試験運用においては、自動送信アラートの中からマルウェアに起因すると推測されるアラートに着目し、nicterの分析者がそのようなアラートを抽出して、組織XのPOCに連絡して対処を依頼するワークフロー（図4におけるAnalystからのManual Alert）を実施した。

なお、運用期間中にnicterの分析者から、組織XのPOCに連絡した20件のうち、現地において該当ホストのマルウェア感染が確認されたものは6件、であった。

5.2　検知したインシデント例

ここでは運用期間中に検知したインシデントのいくつかを紹介する。

5.2.1　マルウェアに関連する事例

- **事例1**：2010年9月10日、あるIPアドレスからTCP 445番ポートへのシーケンシャルスキャンを検出した。パケット数は1宛先アドレスにつき2または3、平均3秒間に1パケットであった。nicterの分析者から組織XのPOCに連絡し、調査を依頼したところ、該当ホストはW32.Downadup.B、W32.Downadup!autorun、Trackware.Rewardnetに多重感染していたとの報告があった。
- **事例2**：2010年12月14日、あるIPアドレスからTCP 445番ポートへのランダムスキャンを検出した。パケット数は1宛先アドレスにつき1つ、平均3秒間に1パケットであった。調査を依頼したところ、該当ホストはBackdoor.Graybird、Trojan.Gen、Trojan.ADH、Trojan.ADH.2に感染していたとの報告があった。

5.2.2　その他の事例

- **事例3**：2011年1月18日、あるIPアドレスからUDP 137番ポートへのシーケンシャルスキャ

表1　月ごとの送信アラート数

日付	ユニークホスト数	総パケット数	検出パケット数	自動送信アラート数	分析者連絡数
2010/8	23,685,324	306,523,808	562,532	712	0
2010/9	21,240,024	290,529,367	703,055	952	3
2010/10	22,659,297	309,694,496	787,756	227	5
2010/11	28,562,141	296,772,713	1,450,179	113	0
2010/12	29,126,062	324,485,640	2,475,351	352	7
2011/1	28,863,449	276,093,022	2,111,713	358	5

ンを検出した。パケット数は1宛先アドレスにつき1つ、平均1秒間に93パケットであった。調査を依頼したところ、該当ホストはあるAndroid端末の標準動作であるとの報告があった。著者らが調査したところ、このAndroid端末はネットワーク共有ディスクへの接続を迅速化するために、このような挙動をすることが判明した。

- **事例4**：2011年1月21日、あるIPアドレスからUDP 137番ポートへのシーケンシャルスキャンを検出した。パケット数は1宛先アドレスにつき1つ、平均1秒間に56パケットであった。調査を依頼したところ、該当ホストでIP Scanner Pro[24]というソフトウェアを動作させていたためとの報告があった。IP Scanner ProはMac用のスキャンツールであり、デバイスの種類やOSを識別する機能を持つ。

6 NICTにおける運用結果

ここでは、NICTのネットワーク運用を行っている情報システムチーム（現情報システム室）にDAEDALUSを導入し、運用を行った事例について紹介する。NICTのネットワークは/16ネットワークの中に、ダークネットとライブネットが混在する（図1の組織Bの様な）ネットワーク構成となっている。そこで、NICTネットワークのライブネットをDAEDALUSに登録するIPアドレスとし、NICTのダークネットを内部ダークネットと見なす。一方、その他の組織が保有するダークネットを外部ダークネットと見なす。POCは情報システムチームの担当者とした。運用期間は2011年1月13日から2011年3月31日までである。この運用期間に発生したアラートのうち実際に役立ったものは1件であった。次節にて情報システムチームの担当者からの報告を記す。

6.1 アラート事例

- **事例1**：内部ダークネットアドレスから、内部ダークネットアドレスへのICMPパケット送信（同アドレスへの通信）を検出した。期間は1月13～16日の間で観測回数は8回であった。これは、外部接続用のBGPルータにingress filterが入っていなかったため、Source Spoofされたパケットが発生していたと考えられる。情報システムチームでは本事例をふまえ、IPv4、IPv6ともに新たにingress filterの設定を行うこととした。

7 むすび

DAEDALUSはnicterの大規模ダークネット観測網を、実ネットワークの保護に活かすためのアラートシステムである。従来のダークネットの利用法は、組織外から飛来する不正なパケットを観測する、つまり外から内へのアクセスを捉えるという考え方であった。一方、DAEDALUSは、組織内から送出された不正な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）へのアクセスを捉えるという、従来とは逆転したダークネットの利用法を提示している。

DAEDALUSでは、組織内で起こったマルウェア感染等を分析センターが検出し、該当する組織にアラートを送信することで、ダークネットの観測結果が実ネットワークのセキュリティオペレーションのトリガとなっている。これは**1**で述べたダークネット観測の2つの課題の前者、実ネットワーク保護への直結の一実現形態といえる。

ダークネットを提供する組織側の観点から見ると、組織内の一部の未使用IPアドレスの提供とブラックホールセンサの設置によって、広域のダークネット観測網からアラートという直接的なフィードバックが得られ、組織内のホストによる外部への不正アクセスを迅速に検出できるというインセンティブが働く。このため、ダークネット観測の2つの課題の後者、センサの広域展開の進展が期待でき、さらにダークネット観測網の拡大、分析精度の向上、参加組織の増加という、正のスパイラルに乗ることが期待できる。

5、**6**で紹介した事例から、DAEDALUSはマルウェアに起因する不正ホストの検出や誤設定の検出に有効であることがわかる。試験運用においては自動送信アラートの中からnicterの分析者がマルウェアに起因すると推測されるアラートを手動で抽出し、組織のPOCに連絡を行っていた。このフローでは分析者が介在するため、リアルタイム性や処理能力の面で分析者がボトルネックと

なる。今後は既存のnicterシステムと連携し、分析者が介在しなくともワークフローが完結するように研究開発を進める。具体的には、nicterの相関分析[4]-[6]の技術を用いて、検出パケットの送信先アドレス、ポート番号、到着間隔等によるパターンから、自動的にアラートの原因を推測して優先度と原因のタグ付けを行い、組織のPOCに必要なアラートのみを自動的に送信できる仕組みを導入していく。

参考文献

1 D. Song, R. Malan, and R. Stone, "A Snapshot of Global Internet Worm Activity," The 14th Annual FIRST Conference on Computer Security Incident Handling and Response, 2002.

2 D. Moore, "Network Telescopes: Tracking Denial-of-Service Attacks and Internet Worms around the Globe," The 17th Large Installation Systems Administration Conference (LISA '03), USENIX, 2003.

3 M. Bailey, E. Cooke, F. Jahanian, J. Nazario, and D. Watson, "The Internet Motion Sensor: A Distributed Blackhole Monitoring System," The 12th Annual Network and Distributed System Security Symposium (NDSS05), 2005.

4 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.

5 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.

6 Koji Nakao, Daisuke Inoue, Masashi Eto, and Katsunari 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.

7 井上大介，衛藤将史，中尾康二，"ダークネット観測に基つく実ネットワーク保護技術の提案," 第5回情報通信システムセキュリティ時限研究会（ICSS2008），2008.

8 D. Inoue, M. Suzuki, M. Eto, K. Yoshioka, and K. Nakao, "DAEDALUS: Novel Application of Large-scale Darknet Monitoring for Practical Protection of Live Networks," 12th International Symposium On Recent Advances In Intrusion Detection (RAID 2009), Poster Session, 2009.

9 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.

10 C. Leita, V. H. Pham, O. Thonnard, E. Ramirez-Silva, F. Pouget, E. Kirda, and M. Dacier, "The Leurre.com Project: Collecting Threats Information using a Worldwide Distributed Honeynet," WOMBAT Workshop on Information Security Threats Data Collection and Sharing (WISTDCS 2008), pp. 40–57, 2008.

11 N. Provos, "A Virtual Honeypot Framework," The 13th USENIX Security Symposium, 2004. http://www.honeyd.org/

12 C. Leita and M. Dacier, "SGNET: A Worldwide Deployable Framework to Support the Analysis of Malware Threat Models," The 7th European Dependable Computing Conference (EDCC 2008), 2008.

13 REN-ISAC, http://www.ren-isac.net/

14 M. V. Horenbeeck, "The SANS Internet Storm Center," WOMBAT Workshop on Information Security Threats Data Collection and Sharing (WISTDCS 2008), pp. 17–23, 2008. http://isc.sans.org/

15 DShield, http://www.dshield.org/

16 JPCERT/CC ISDAS, http://www.jpcert.or.jp/isdas/

17 @police, http://www.cyberpolice.go.jp/detect/observation.html

18 MUSTAN, http://mustan.ipa.go.jp/mustan web/
19 WCLSCAN, http://www.wclscan.org/
20 鈴木和也，馬場俊輔，和田英彦，中尾康二，高倉弘喜，岡部寿男，“複数手法によるリアルタイム解析を支援するトラヒックデータ配送システムの実装と評価,” 電子情報通信学会論文誌，Vol. J92-B, No. 10, pp. 1619–1630, 2009.
21 Ruby On Rails, http://rubyonrails.org/
22 C. Zou, W. Gong, and D. Towsley,“Code red worm propagation modeling and analysis,”9th ACM conference on Computer and communications security (CCS '02), 2002.
23 D. Moore, V. Paxson, S. Savage, C. Shannon, S. Staniford, and N. Weaver,“Inside the SlammerWorm,” IEEE Security and Privacy, Vol. 1, No. 4, pp. 33–39, 2003.
24 IP Scanner Pro, http://10base-t.com/macintosh-software/ip-scanner/

（平成 23 年 6 月 15 日 採録）

鈴木未央（すずきみお）
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
博士（工学）
ネットワークセキュリティ、IPv6 セキュリティ、ネットワークエミュレーション

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
博士（工学）
ネットワークセキュリティ、情報セキュリティ