対サイバー攻撃アラートシステム DAEDALUSとその社会展開

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
サイバー攻撃対策総合研究センター サイバー防御戦術研究室 室長

大学院博士課程後期修了後、2003年、独立行政法人通信総合研究所（現NICT）に入所。
2006年よりインシデント分析センター NICTERを核としたネットワークセキュリティの研究開発に従事。博士（工学）。

はじめに

侵入検知システムや侵入防止システムなどの従来のセキュリティ技術の多くは、組織内ネットワークがインターネットと接続しているネットワーク境界において、組織外からのサイバー攻撃を検知・防御する「境界防御」が主流となっています。しかしながら、USBメモリやメールの添付ファイル、持ち込みPCなどを媒体とした組織内を始点としたマルウェア*1感染によって境界防御を突破されるセキュリティインシデントが多発しており、従来の境界防御の仕組みを補完するセキュリティ対策の重要性が増しています。

対サイバー攻撃アラートシステムDAEDALUS*2（ダイダロス）は、マルウェア感染を完全に防止することは困難であるという事故前提の考え方に基づき、感染後の対策として、組織内のマルウェア感染端末（特に自己増殖機能を持つワーム型マルウェア）を早期検知し、その組織に向けたアラートの発報を可能にします。

DAEDALUSの仕組み

DAEDALUSが攻撃を検知し、アラートを発報する仕組みは次の通り非常にシンプルです。それは、

特定の組織からダークネットにパケットが届くと、その組織に向けてアラートを発報

するというものです。ここで、ダークネットとはインターネット上に点在する未使用のIPアドレス空間のことを指します。未使用のIPアドレスにパケット（インターネット通信の最小単位）が届くことは、通常の通信では考えにくいことですが、実際にダークネットを観測してみると、大量のパケットが到着することがわかります。これらのパケットの多くは、ワーム型マルウェアに感染した端末が次の感染対象を探索するために、インターネット上に拡散させるスキャンと呼ばれる通信なのです。マンションの空室の郵便受けには無駄なダイレクトメールしか届かないように、ダークネットに届くパケットの大部分はマルウェアに起因した不正な通信であり、その送信元はマルウェアに感染している疑いが強いと考えられます。そこで、その送信元IPアドレスを使用している組織にアラートを発報することで、迅速なインシデント対応のトリガとなります。

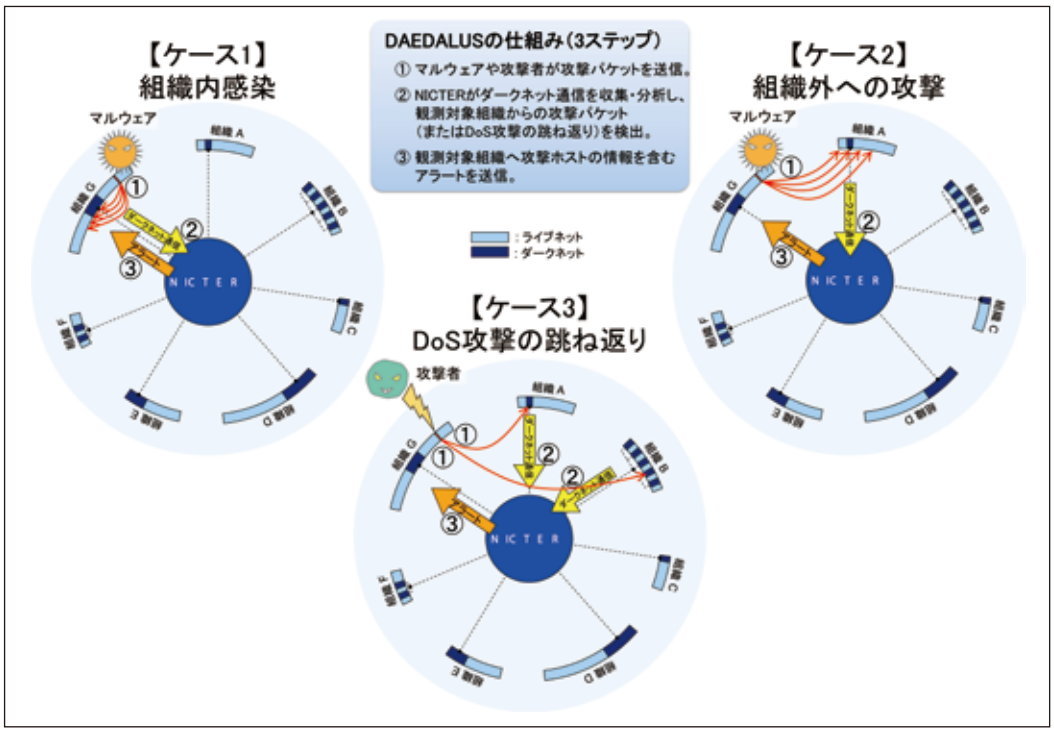

図1　DAEDALUSの攻撃検知 ケース1〜3

- ケース1: マルウェアに感染した端末による組織内への感染活動（ローカルスキャン）
- ケース2: マルウェアに感染した端末による組織外への感染活動（グローバルスキャン）
- ケース3: 外部の攻撃者による特定組織へのDoS攻撃の跳ね返り（バックスキャッタ*3）

*1 マルウェア
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 DAEDALUS
Direct Alert Environment for Darknet And Livenet Unified Security

*3 バックスキャッタ
送信元IPアドレスが詐称されたDoS攻撃（SYN-flood攻撃）を受けているサーバからの応答（SYN-ACK）パケットのこと。IPアドレスがランダムに詐称されている場合、DoS攻撃を受けているサーバから多くの応答パケットがダークネットにも到来するため、DoS攻撃の発生を検知できる。

図2　DAEDALUS-VIZの可視化画面

図3　新規アラート発報時の表示


図4　マルウェアによるローカルスキャンの実例

DAEDALUSで検知できる攻撃は、図1のように3つのケースに分けられます。なお、図1中のNICTERとは、DAEDALUSの基盤となっている大規模ダークネット観測網を含むインシデント分析システムであり、国内外に分散している約21万（2014年1月現在）の未使用IPアドレスをリアルタイムで観測しています。

なお、ケース1を観測するためには、組織内ネットワークにダークネット観測用センサの設置が必要となります。ケース2とケース3は、NICTERの大規模ダークネット観測網によって外部観測が可能であり、センサ設置は必要ありません。

DAEDALUSの可視化エンジン

図2はDAEDALUSのアラート発報状況を俯瞰的に把握するための可視化エンジンDAEDALUS-VIZの表示画面です。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、ダークネット観測用センサを設置している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への通信を表しています。リングの水色部分がライブネット（使用中IPアドレスブロック）、濃紺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IPアドレスを指し示しています。DAEDALUS-VIZ上でアラートが表示されるとほぼ同時に、該当組織には電子メールでアラートが自動送信されます。

図3に新規アラートが発報された際に画面全体に表示される「警」マークを、図4にマルウェアが組織内で感染活動（黄色の曲線がマルウェアによるローカルスキャン）を行っている様子を示します。

DAEDALUSの社会展開

NICTは国内外に向けてDAEDALUSの社会展開を進めています。

日本国内では、教育機関向けにダークネット観測用センサおよび可視化エンジンの設置とアラート提供を行っており、一般企業向けにはDAEDALUSに基づく商用のアラートサービス[*4]を始めています。また、2013年11月から財団法人地方自治情報センター（LASDEC）との協力の下、地方自治体に向けたアラート提供（およびアラート対応マニュアルの提供）を開始しており、2014年1月時点で110の地方自治体がアラート提供対象として登録されています（図5）。

国外向けには、総務省のASEAN各国を対象としたセキュリティ対策に関する総合的な技術協力プロジェクト（JASPER[*5]）の一環で、ASEAN諸国に対するDAEDALUSアラート提供を順次開始しています。

まとめ

2000年代初めから数々の大規模感染を引き起こしているワーム型マルウェアは、インターネット上で依然として猛威を振るっています。DAEDALUSは大規模ダークネット観測網の観測結果に基づいて、その感染源へ迅速なアラート提供を行っています。DAEDALUSはダークネット観測の輪に加わる組織が増加するほど、全体の検知能力が向上するという特性を有しており、連携機関へのセンサ設置とDAEDALUSからのアラート提供というWin-Winな関係をベースに、今後も産学官全方位への展開を図っていきます。

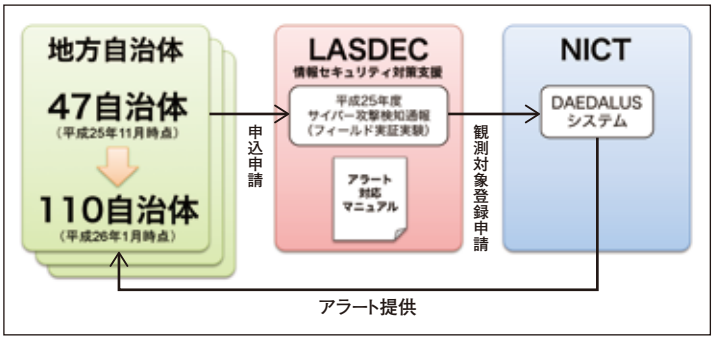

図5　地方自治体へのDAEDALUSアラート提供

＊4　アラートサービス
SiteVisor（http://sitevisor.jp）

＊5　JASPER
Japan ASEAN Security PartnERship