3-4　対サイバー攻撃アラートシステム DAEDALUS

鈴木未央　鈴木宏栄　高木彌一郎　伊沢亮一

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」が主流となっている。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る。我々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、対サイバー攻撃アラートシステム DAEDALUS（ダイダロス：Direct Alert Environment for Darknet And Livenet Unified Security）の研究開発を行っている。本稿では DAEDALUS の仕組みについて述べるとともに DAEDALUS の社会展開の状況についても報告する。

1　背景

一般的な組織では自組織のネットワークをサイバー攻撃から守るために、侵入検知システム（IDS）や侵入防止システム（IPS）などを導入するケースが多い。これらのセキュリティ技術は「境界防御」と呼ばれており、組織内ネットワークとインターネットの境界において、主に組織外からのサイバー攻撃を検知・防御する仕組みである。しかしながら、メールの添付ファイルや USB メモリ、持ち込み PC などを媒体とし、組織内を始点としたマルウェア感染が多発している。これらの感染事例の多くは組織内の“人”が介在しているため、境界防御の仕組みだけでサイバー攻撃を未然に防ぎ切ることは難しくなってきており、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る。

我々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、対サイバー攻撃アラートシステム DAEDALUS の研究開発を行っている [1]–[3]。DAEDALUS は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）を検知し、その組織に向けたアラートを発報するシステムである。加えて、特定の種類の DDoS 攻撃（分散型サービス不能攻撃）など組織外からのサイバー攻撃も検知することができる。

本稿では DAEDALUS の仕組みや社会展開などの状況について報告する。以下、**2** で DAEDALUS の仕組みを説明し、**3** で DAEDALUS の可視化システムである DAEDALUS-VIZ、**4** で社会展開の状況についてそれぞれ述べ、**5** でまとめる。

2　サイバー攻撃検知発報

2.1　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ある。

> 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発報

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だが、実際にダークネットを観測すると、大量のパケットが到着することがわかる。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パケットを拡散させるスキャンと呼ばれる通信である。例えるならば、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る。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が、それが迅速なインシデント対応のトリガとなる。

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る。なお、図 1 中の NICTER

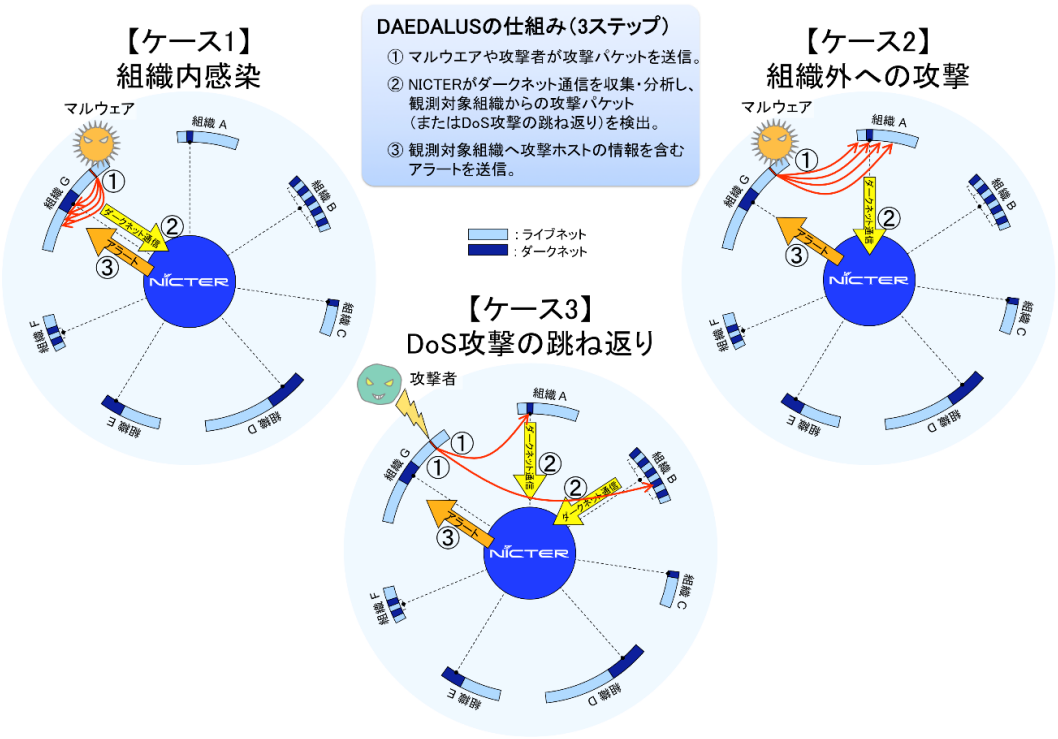

図 1　DAEDALUS の攻撃検知ケース 1 ～ 3

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 30 万以上（2016 年 3 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る [4]–[6]。

● ケース 1：組織内感染
　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：組織外への攻撃
　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：Dos 攻撃の跳ね返り
　外部の攻撃者による特定組織への DDoS 攻撃の跳ね返り（バックスキャッタ）

　なお、ケース 1 を観測するためには、組織内ネットワークへのダークネット観測用センサの設置が必要となる。ケース 2 と 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、DAEDALUS に組織で使用しているネットワークのアドレスレンジを登録するだけで、センサ設置は必要ない。

2.2　アラートの種類

　DAEDALUS のアラートは、アラートの発生要因となったダークネットに届いたパケット（アラートパケット）ごとにメールを送信するのではなく、ある送信元IPアドレスからのアラート対象パケット（アラートパケット）を、あるまとまった単位で集約してアラートメールを送信する。また、そのアラートが緊急のものか、または新規／継続かを区別する。各アラートには監視タイマー間隔が設定されており、アラートパケットが発生した場合、監視タイマー間隔の終了のタイミングで、アラート情報が送信される（アラート発報）。以下に各アラートの発生条件を示す。

● 新規アラート
　ある送信元 IP アドレスからアラートパケットを検知した場合、監視タイマー間（13 秒間）の、該当送信元 IP アドレスからのアラートパケットを集計しアラートとする。下記の条件を全て満たす場合、新規アラートとなる。
　1. 該当送信元 IP アドレスから過去 1 週間以内にアラートパケットを観測していない
　2. 該当送信元 IP アドレスから監視タイマー間（13 秒間）に 1 パケット以上のアラートパケットを観測
● 継続定期アラート
　ある送信元 IP アドレスからアラートパケットを検知した場合、監視タイマー間（60 分間）における該当送信元 IP アドレスからのアラートパケットを集計し、アラートとする。下記の条件を満たす場合、継続定期アラートとなる。
　・該当送信元 IP アドレスから監視タイマー間（60 分間）に 1 パケット以上のアラートパケットを観測
● 緊急アラート
　ある送信元 IP アドレスからアラートパケットを検

知した場合、監視タイマー間（15 分間）における該当送信元 IP アドレスからのアラートパケットを集計し、アラートとする。下記の条件を満たす場合、緊急アラートとなる。

・該当送信元 IP アドレスから監視タイマー間（1 分間）に 1 ,000 パケット以上のアラートパケットを観測

2.3　アラートメール

DAEDALUS で検知された攻撃は、アラートとしてメールにより登録組織に送信（発報）される。アラートメールにはダークネットに届いたパケットの受信時刻、送信元 IP アドレス（登録組織の IP アドレス）、送信元ポート番号、送信先ポート番号、プロトコルの種類（TCP や UDP など）、プロトコルのフラグ（TCP であれば SYN や SYN/ACK など）が記載されている。

2.4　マルウェア感染以外のアラート

登録組織の PC にインストールされているネットワークアプリケーション（特に P2P ソフトウェア）がダークネットにパケットを送信した場合は、ケース 2 と同様の仕組みで当該組織にアラートが発報（アラート送信）される。

また、登録組織のネットワークにオープン・リゾルバが存在し、攻撃者が DNS サーバに送信元 IP アドレスを詐称したスキャンを行うと、登録組織からダークネットに DNS 応答が送信される場合がある。この場合、ケース 3 と同様の仕組みでアラートメールが当該組織に発報される（図 1）。

3　DAEDALUS のアラート可視化エンジン

DAEDALUS は多組織に分散した観測網により観測した情報に基づき、多組織に対してアラートを発報するシステムで、アラートの発報数が多くなることから、かねてよりアラートの発報状況の把握が課題であった。このため我々は、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である DAEDALUS-VIZ を開発した。図 2 に DAEDALUS-VIZ の画面を示す。この画面では、インターネットを中央の球体で表現し、各組織のネットワークを周りのリングとして表現している。各リングにおいて、明るい水色部分はライブネット（利用中の IP アドレスブロック）であり、暗い部分はダークネットである。DAEDALUS で観測されている各組織のダークネットへの通信は、球体とリングの間を流れるオブジェクトとして表示される。各組織に対して新規アラートを発報した場合、図 3 のように画面全体に「警」マークが表示され、その後の指定時間はリング外周の「警」マークとして表示され続ける。実際のアラート発報の際の

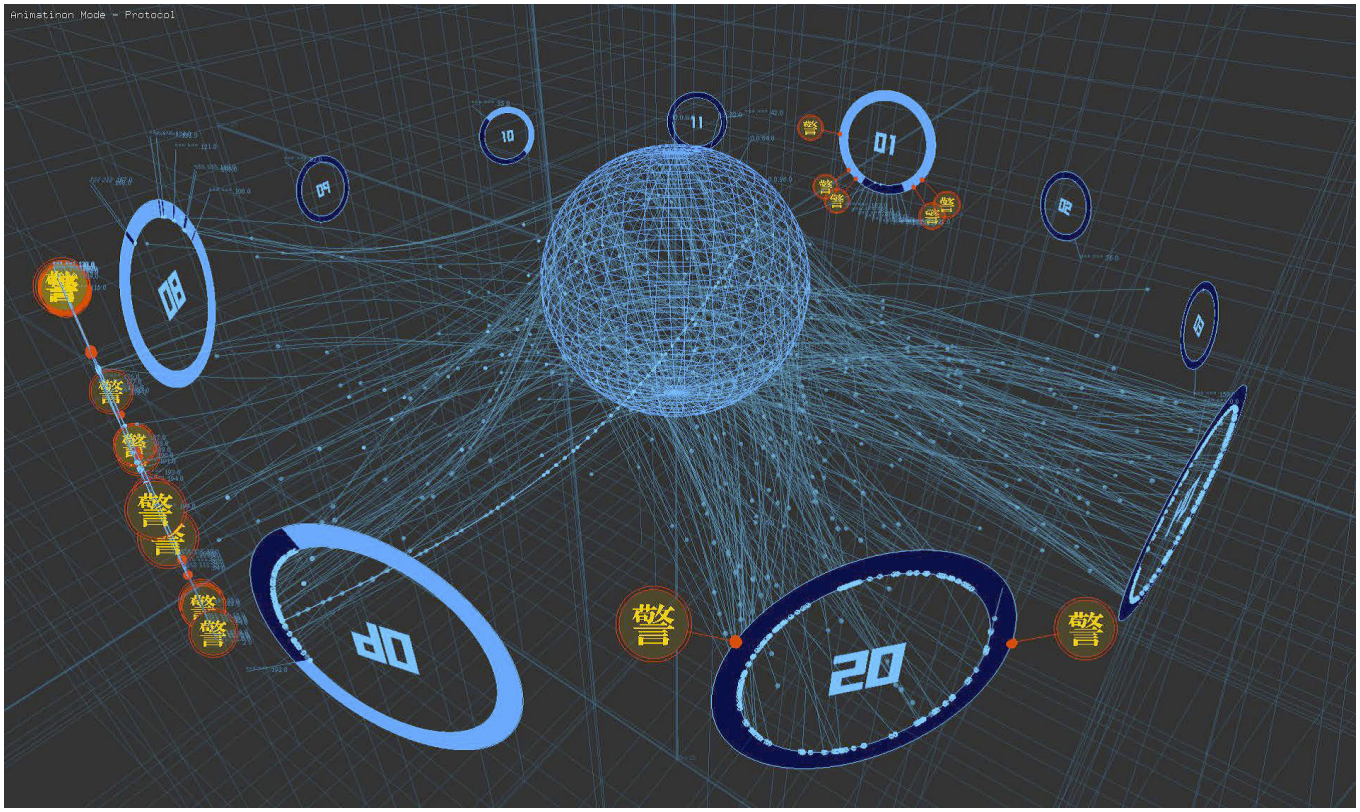

図 2　DAEDALUS-VIZ の可視化画面

例として、図 4 にマルウェアに感染した端末が組織内へ感染活動を行っている際の様子を、図 5 にある組織のサーバに対する DDoS 攻撃が行われ、そのバックスキャッタ（TCP の仕組みによる反射パケット）を観測した際の様子を示す。どちらの例でも、黄色の曲線は攻撃に関係するパケットを表している。

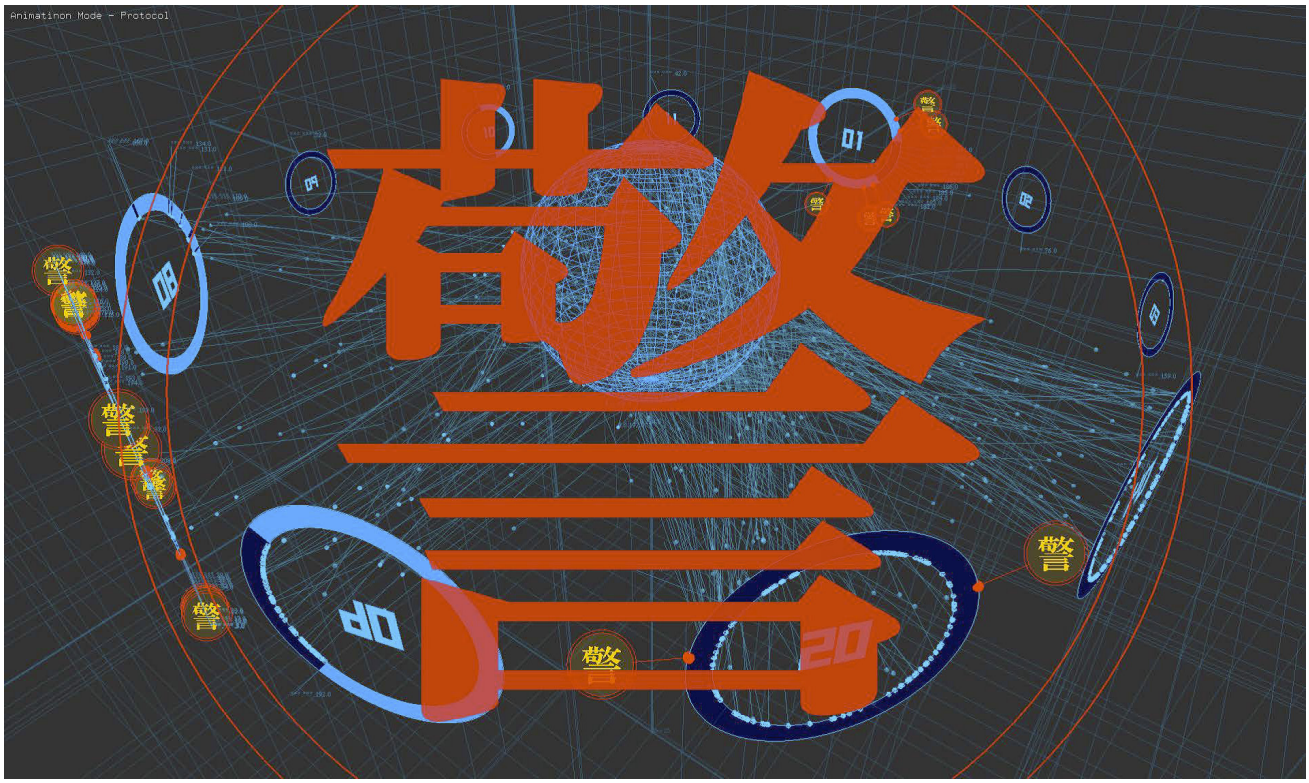

図 3　DAEDALUS-VIZ の新規アラート発報画面

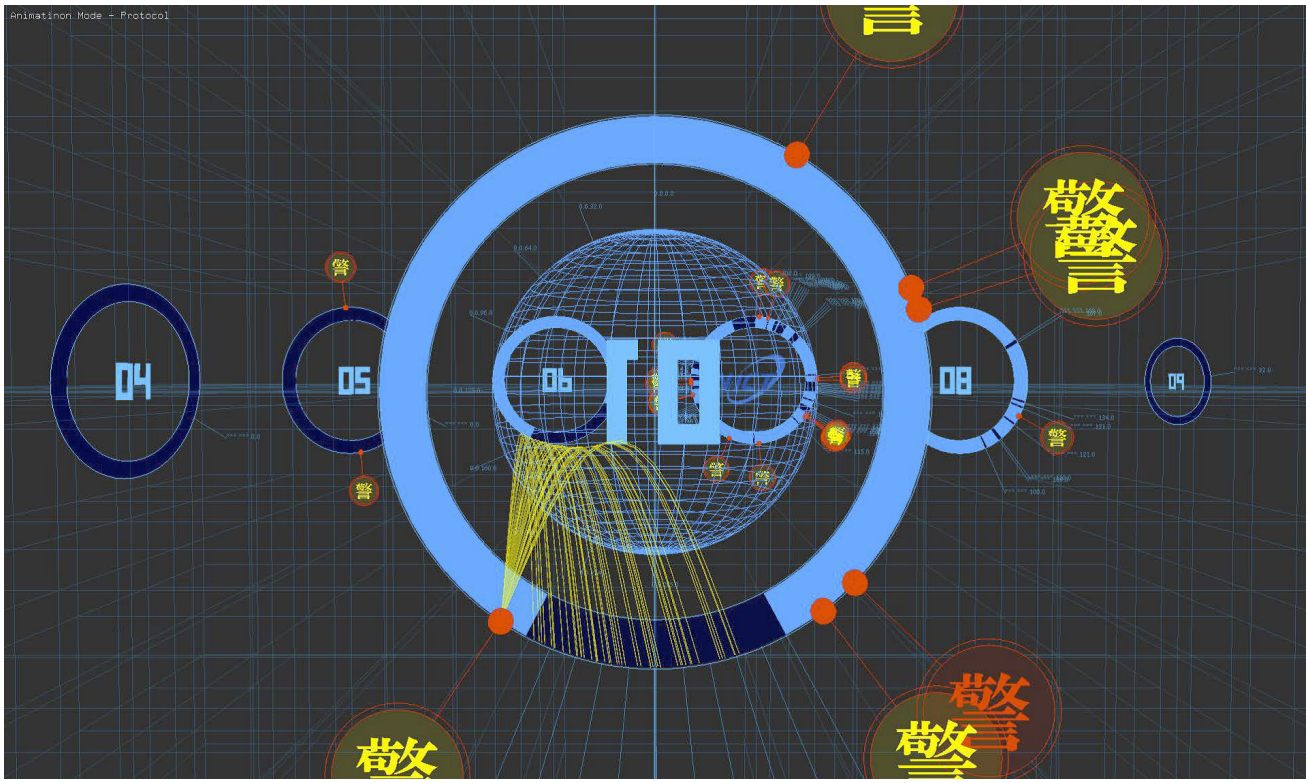

図 4　マルウェアによるローカルスキャンの実例

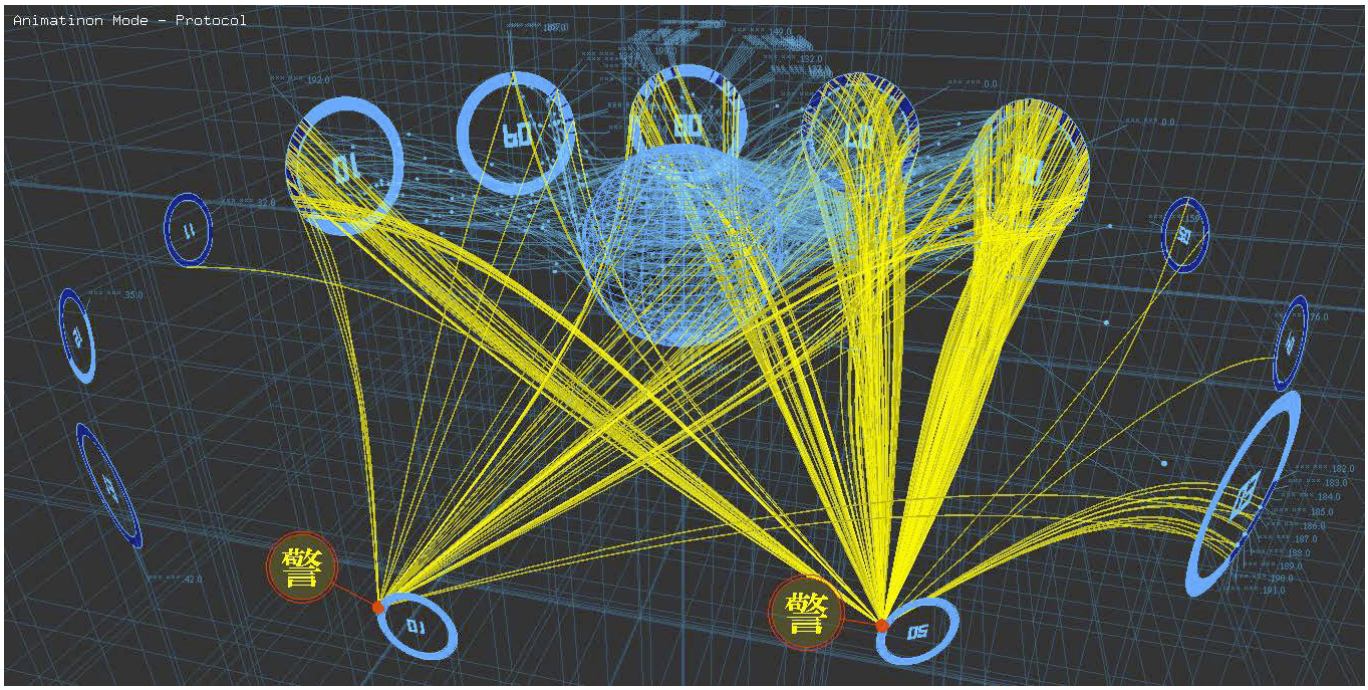

図 5　DDoS による Backscatter の実例

4　DAEDALUS の社会展開状況

我々は、かねてより国内外に向けて DAEDALUS の社会展開を進めてきた。日本国内では、教育機関向けにダークネット観測センサ及び可視化エンジンの設置と DAEDALUS によるアラート発報提供を行っており、一般企業に向けては技術移転先と連携し、DAEDALUS に基づくアラート発報サービスを行っている。また、地方自治体に対しては、2013 年 11 月から、J-LIS（地方公共団体情報システム機構、旧財団法人地方自治情報センター）の協力の下、DAEDALUS のアラート発報提供を行っている。2013 年 11 月時点では 47 自治体であった提供自治体は、2016 年 8 月の段階では 598 自治体まで拡大している。

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: Japan ASEAN Security PartnERship）の一環で、ASEAN 諸国に対する DAEDALUS アラート発報提供を行っている。

5　まとめ

我々は、これまで、境界防御の仕組みを補完するセキュリティ対策手法のひとつとして DAEDALUS の研究開発を行ってきた。前述したように、DAEDALUS は大規模ダークネット観測網の観測結果に基づき、DAEDALUS の参加組織に対してアラート発報提供を行う仕組みである。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、連携機関へのダークネット観測センサ設置と DAEDALUS からのアラート発報提供という Win-Win な関係をベースに、今後も産学官全方位への展開を推進していく。

【参考文献】

1　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.
2　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.
3　D. Inoue, M. Eto, K. Suzuki, M. Suzuki, and K. Nakao, “DAEDALUS-VIZ: novel real-time 3D visualization for darknet monitoring-based alert system,” 9th International Symposium on Visualization for Cyber Security (VizSec '12), pp.72–79, 2012.
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,” WOMBATWorkshop on Information Security Threats Data Collection and Sharing (WISTDCS 2008), pp.58–66, 2008.
6　K. Nakao, D. Inoue, M. Eto, and K. 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.

鈴木未央　（すずき　みお）

サイバーセキュリティ研究所
サイバーセキュリティ研究室
研究員
博士（工学）
ネットワークセキュリティ、ネットワーク運用

鈴木宏栄　（すずき　こうえい）

サイバーセキュリティ研究所
サイバーセキュリティ研究室
主任研究技術員
ネットワークセキュリティ

高木彌一郎　（たかぎ　やいちろう）

サイバーセキュリティ研究所
サイバーセキュリティ研究室
研究技術員
ネットワークセキュリティ

伊沢亮一　（いさわ　りょういち）

サイバーセキュリティ研究所
サイバーセキュリティ研究室
主任研究員
博士（工学）
マルウェア解析、ネットワークセキュリティ