3-3　データマイニングを応用したダークネット分析技術

班　涛

ダークネットと呼ばれる未使用の IP アドレス空間の観測は、インターネットにおけるサイバー攻撃のグローバル動向を把握するための費用対効果の高い方法のひとつである。当研究室が運営している NICTER プロジェクトは、過去 10 年間で、分散型大規模グローバルダークネット観測網を構築・観測することにより、サイバー空間に発生したサイバー攻撃に関して、情報収集・発信・対策などの研究開発活動に取り組んできた。本稿では、新たに開発された NICTER の中核であるデータマイニングエンジン群を紹介する。評価実験では、ダークネット観測が、サイバー攻撃のグローバルな動向の把握に有効であり、費用対効果にも優れていることを確認した。本稿で報告された発見は、サイバー攻撃への戦略的対応策に活用できる。

1　概要

悪意のあるソフトウェア、いわゆるマルウェアの蔓延により、インターネットを使って蓄積及び通信されるデータの機密性、完全性、可用性が大きな脅威にさらされている。マルウェアの台頭による懸念に対処するため、グローバルな視点から見た全体像と新たなインシデントに対する詳細な情報をリアルタイムに提供できるネットワーク観測システムの開発が急務となっている。利用者数の多いグローバル規模のネットワークの観測には膨大な計算、保存、通信コストがかかるため不可能であり、通常は未使用の IP アドレス空間（別名ダークネット [1]-[3]）の観測が、コストパフォーマンスのよい妥協案となっている。

ダークネットは（ネットワークテレスコープ、ブラックホールモニター、シンクホールとも呼ばれる）、接続され割り当てられた IP 空間の一部で、一般に公開されたサービスを含まないものを指す [1]-[3]。ダークネットには正規のホストが存在しないため、ダークネットで観測されるトラフィックは、その存在自体が異常であり、悪意または設定ミスのどちらかによって生じたものである。これまで、既存のネットワークをその一部として含むような、より大きなネットワークに存在する悪意あるトラフィックの種類と送信元を特定するため、多くの研究においてダークネットが利用されてきた。これらのダークネットは、フローコレクタやバックスキャッタディテクタ、パケットスニファなどを設置するために使用される [4][5]。関連する研究では、検知率の大幅改善と偽陽性率の低下が報告されている。これにより、悪意のある、または誤ったアクティビティの認知度向上と脅威緩和の簡素化がもたらされた。

マルウェアによって発生する多様なサイバー攻撃の早期警告及び脅威緩和を促進するため、10 年以上にわたって NICTER（インシデント分析センター）[2][6][7] の開発及び運営が続けられている。NICTER は、グローバル規模でのダークネット観測や手作業で収集したマルウェアの亜種の静的・動的分析を行い、マクロ及びミクロの双方から分析結果をまとめることで、インターネットにおける悪意のあるアクティビティに関する豊富な情報を得て、獲得した知識をユーザーネットワークの保護に適用している。本稿では、NICTER の最近の動向を説明する。特に、新たなサイバー攻撃の検知、予防及び緩和を目的とした新開発のデータマイニング手法に注目する。

本稿は次のように構成されている。セクション 2 では、NICTER と関連する研究を簡単に紹介する。セクション 3 では、ダークネットで観測された攻撃側ホストの未来の状態を予測するためのホスト挙動分析に関する研究を示す。セクション 4 では、SYN_ACK パケットを発する不審ホストからの DDoS（分散型サービス妨害）攻撃を受けたサーバーを特定するためのアプローチを導入する。セクション 5 では、新たな脅威の早期検知に向けた新スキームについて説明する。最終セクションでは、結論を述べる。

2　NICTER と関連研究

本節では、NICTER と関連する研究を簡単に紹介する。特に、ダークネット観測の側面に注目する。

2.1　NICTER の概要

NICTER は、2 つマルウェア対策を組み合わせている。マクロのアプローチとしては、グローバル規模のネットワーク観測に基づく悪意のあるアクティビティのトレンド把握を行っている。ミクロのアプローチとしては、ハニーポットなどで捕捉したマルウェアのサンプルを分析してその特徴と挙動を理解することで、隔離や脅威緩和を可能にしている。

NICTER のマクロな構成要素、別名 MacS は、世界中にインストールされた分散型ダークネットセンサで収集したネットワークトラフィックを観測する。ダークネットパケットに固有の性質に従い、パケットを発する IP アドレスは攻撃側ホストとして取り扱われ、短時間のユニークホストからのパケットはインシデント候補として扱われる。NICTER のミクロな構成要素、別名 MicS は、ハニーポットや E メールトラップを利用して、マルウェアをそのまま捕捉する。入手したマルウェアのサンプルはマルウェア動的解析システムとマルウェアコード解析システムに入れられ、その挙動の特徴や主要な機能に基づいて、プロフィールが学習される。

NICTER は、インシデント対応のために MacS と MicS の結果を結合する 2 つのサブシステムで構成される。このシステムは、NemeSys（Network and Malware Enchaining System）と呼ばれ、現象（すなわちダークネットで観測されたインシデント候補）とその根本原因（すなわちマルウェア亜種）を対応付けることができる。MacS がインシデント候補を観測すると、NemeSys 内の相関分析エンジンが、マルウェアプロフィールがインシデントに合致するマルウェア亜種のリストを出力する。観測されたネットワーク攻撃の根本原因を見つけることで、インターネットで起こっていることをより明確に把握できるようになり、したがって脅威を緩和できる可能性が高まる。最後にオペレータが、IHS（インシデントハンドリングシステム）を使って上記分析結果の診断を行い、インシデントレポートを発行する。

本稿ではこれ以降、NICTER のマクロ的側面に注目する。NICTER のその他の側面に関する詳細は、文献 [2][6][7] を参照いただきたい。

2.2　NICTER の分析エンジン

ダークネットに到達したとして記録されるパケット数は、NICTER が観測するダークネット空間の規模とともに徐々に増加している。表 1 は、NICTER が観測しているダークネットの基礎統計を示している。2015 年、観測されたダークネットの IP アドレスの総数は 28 万、収集されたパケット数は 545 億 1000 万に上り、平均すると年間で 1 IP アドレス当たり 21 万 3500 パケットとなる。表の一番右の列から、10 年の観測期間中、各 IP アドレスに到達する平均パケット数は、明らかに増加傾向にあることがわかる。この傾向はスキャン／攻撃アクティビティが増加していることを意味し、サイバー攻撃緩和のためにデータの規則性を利用した最新のマイニング手法が必要となっている。

表 1　NICTER が観測するダークネットの年別統計

年	パケット数（10 億）	IP アドレス数（千）	1 IP アドレス当たりのパケット数
2006	0.81	100	17,231
2007	1.99	100	19,118
2008	2.29	120	22,710
2009	3.57	120	36,190
2010	5.65	120	50,128
2011	4.54	120	40,654
2012	7.79	190	53,085
2013	12.90	210	63,655
2014	25.70	240	115,323
2015	54.51	280	213,523

我々は、インシデントの報告や攻撃の緩和を促進するため、NICTER に関係する様々な可視化及びデータマイニングエンジンを開発してきた。文献 [6] では、井上らが Atlas、Cube、Tap View を導入した。Atlas は地理的トラフィック可視化エンジンで、発信元から目的地までのパケットの横断を地図上に示すことができる。Cube は包括的 3 D トラフィック可視化エンジンで、立方体内に描画される。Tap View は、ホスト挙動可視化エンジンで、インシデント中の攻撃側ホストの特徴をとらえる。

文献 [2] では、井上らが、変化点検出（CPD）、自己組織化写像（SOM）アナライザ、インシデント予測（IF）エンジンなどの主要な分析エンジンを発表した。CPD は観測中のトラフィックの急速な変化をリアルタイムに検知するために、自己回帰（AR）モデルに基づく 2 段階オンライン学習を用いた時系列分析エンジンを実装している。SOM アナライザは、ネットワーク挙動の特性を評価することで未知のマルウェアやその亜種を分類及び検知するためのクラスタリング及び可視化エンジンである。IF は、数時間後のインシデントに関するトラフィック量を予測し、迅速な対応を可能にするための予測エンジンである。

NICTER に関係する分析エンジンの詳細は、文献 [2] を参照いただきたい。

2.3　NICTER の副産物

NICTER が育んだ可視化及び分析技術は、侵入検知・防御システム（IDS/IPS）などの従来型セキュリティアプライアンスを補うことで、ユーザーネットワークにおけるセキュリティオペレーションの強化に応用されている。

DAEDALUS システム [8] は、ダークネット観測とライブネット上で実際に行われているセキュリティオペレーションの間のギャップを橋渡しする目的で開発されている。例えば、グローバルなトレンドを観測しても、ライブネットの保護には直接的に寄与しない。組織の外から受信したパケットだけが観測される従来手法とは対照的に、複数組織の IP 空間をカバーする分散したダークネットは、組織の枠を超えて送信される悪意のあるパケットを観測できる。DAEDALUS では、同一組織内のダークネットに向けたホストからのスキャンが検知されると組織内アラートが、異なる組織のダークネットに向けたホストからのスキャンが検知されると組織間アラートが発せられる。また、保護登録済みの IP アドレスからバックスキャッタパケット（SYN_ACK フラグがオンの TCP パケット）が送信されると、DDoS アラートが発せられる。文献 [9] で導入された可視化エンジンと DAEDALUS を併用することで、オペレータがリアルタイムかつ視覚的にアラートの状況の全体像を完全に把握できるようになると同時に、ダークネット及び発行されたアラートとの非常にフレキシブルかつ確実なインタラクティブ性を提供できる。

Atlas の拡張機能である NIRVANA（ライブネットトラフィック可視化エンジン）は、ネットワークの実際のトラフィックをリアルタイムで描画することで、ネットワーク障害や設定ミスのデバイスの検知を可能にし、ネットワーク管理者の負担軽減に役立っている。NIRVANA の詳細については、文献 [10] を参照いただきたい。

2.4　ダークネット観測に関連する研究

ダークネット観測に関して、文献で知られているたくさんのプロジェクトが現在進行中である。また、多数の観測システムがすでに運用段階に入っている [2][4][5][11]–[15]。これらのプロジェクトの多くは、ネットワークイベントを観測することでイベント分析が可能になり、特定のポート番号へのアクセス急増といった統計データを提供している。

3　長期的サイバー攻撃の挙動分析

本セクションでは、文献 [3] で行われた攻撃側ホストの挙動に関する研究を簡単に紹介する。この研究は、マルウェアに感染したホストが時間の経過とともにどのような挙動を示すのか理解を深めること、それらの一時的な規則性を特定すること及び過去の挙動に基づいて未来のアクティビティを予測することの必要性から行われた。

3.1　攻撃の送信先ポートに基づくクラスタリング

狙われるポートと攻撃の種類の間には密接な関係があることがよく知られている。クラスタリングは、送信先ポート情報を分析することにより、類似の行動を示す攻撃側ホストをグループ化するために導入されている。文献 [3] の実験によると、攻撃側ホストがターゲットとする送信先ポートの集合に基づいて定義される Jaccard 距離を近接性の指標とするリンケージ・アルゴリズムによって、2011 年時点で最も攻撃を受けているポートは 445、1433、22、3389、80 であることがわかった。類似の攻撃では時間的な挙動が一致することを利用して、これらの主要ポートに関する以下の分析が行われている。

3.2　時系列週間攻撃量に関する回帰分析

観測履歴に基づいてダークネットに送信されたパケット数に関するホストの攻撃挙動を予測するタスクは、時系列予測によるアプローチで行われている。観測された全ホストについて、各週にホストから受信したパケット数を数えることで、2011 年第 1 週から最終週までの時系列測定が示された後、学習と予測を行うためにサポートベクトル回帰（SVR）[16] が選択されている。

表 2　時系列週間攻撃量に関する交叉回帰パフォーマンス

送信先ポートで訓練されたモデル	送信先ポートでテストされた MSE				
	445	1433	22	3389	80
445	**3.61 e-4**	2.17 e-3	4.17 e-3	8.04 e-3	4.36 e-3
1433	4.69 e-4	**3.18 e-4**	4.35 e-3	7.84 e-3	4.80 e-3
22	8.57 e-4	2.44 e-3	**2.00 e-3**	8.16 e-3	4.32 e-3
3389	6.31 e-4	2.05 e-3	3.74 e-3	**3.77 e-3**	4.03 e-3
80	6.04 e-4	3.20 e-3	4.08 e-3	8.64 e-3	**1.28 e-3**

表 3　時系列週間攻撃量に関する交叉分類予測

送信先ポートで訓練されたモデル	送信先ポートでテストされた幾何平均					送信先ポートでテストされた F1-尺度				
	445	1433	22	3389	80	445	1433	22	3389	80
445	**0.91**	0.94	0.88	0.77	0.79	0.94	0.92	0.80	0.73	0.60
1433	0.87	**0.95**	0.86	0.75	0.82	0.92	0.92	0.80	0.71	0.69
22	0.89	0.92	**0.92**	0.73	0.79	0.92	0.90	**0.89**	0.69	0.66
3389	0.78	0.94	**0.92**	**0.88**	0.85	0.91	0.90	0.78	**0.82**	0.60
80	0.76	0.91	0.88	0.77	**0.88**	**0.95**	**0.94**	0.85	0.76	**0.82**

表 2 は、回帰の結果を示している。予測の精度を測るため、平均二乗誤差（MSE）を用いた。表の右側からわかるように、対角線上の MSE 値が各行の最小となっている。つまり、クラスタから訓練された回帰モデルは、同一のクラスタからのテストセットと最もフィットすることがわかる。対角線上の MSE が小さいということは、ホストの未来の挙動は、過去の挙動と密接に関係しており、そのような関係は定性的に学習できることを意味する。対角線以外では比較的 MSE が大きいことから、種類の異なる攻撃は、ダークネットに送信するパケット数という点で異なる挙動モデルに適合することがわかる。これは、我々の感覚とも一致する。

3.3　攻撃に関する定性的予測

本セクションでは、ホストに関する次のような定性的な疑問に答える。すなわち過去の時間枠 T において統計履歴があるとして、T+1 においても攻撃が続くのかという疑問である。

この疑問は、分類の問題としてモデル化するとよい。**3.2** の記述に基づいて、二項分類問題を次のように定義した。すなわち、分類器にとっての入力ベクトルは回帰モデルと同じとするが、出力ベクトルについては、出力ベクトルは二値化され、時刻 T+1 において攻撃が行われない場合はホストが +1 とラベル付けられ、そうでない場合は -1 とラベル付けられる。今回は、サポートベクトルマシン（SVM）[16] を利用して、問題を解決した。評価結果を表 3 に示す。一部のクラスタから形成された分類問題には不均衡が発生する。すなわち一方のクラスタからのサンプルが他方からのそれを圧倒しているように見えたため、分類器の一般化性能の測定に当たっては、精度よりも、幾何平均と F1 - 尺度を用いた。表 3 からもわかるように、幾何平均の値は、表 2 の MSE のパターンと類似している。つまり、同一クラスタに属するホストは、似通った挙動を示すことがわかる。若干のばらつきはあるものの、表 3 の F1 - 尺度は、上記の結論を裏付けるものである。

3.4　まとめ

機能回帰及び分類に基づく数値研究により、同一の送信先ポートを攻撃しているホストの攻撃挙動をより正確に予測できることが確認された。本研究結果は、適応型ブラックリスト化などのセキュリティオペレーションの裏付けとなる。

4　DDoS 攻撃を受けたホストの早期特定

本セクションでは、ダークネットで収集されたバックスキャッタの分析に基づく有効な DDoS イベント検知システム [17] を紹介する。実験の結果、我々のアプローチは、迅速かつ正確な DDoS 攻撃の検知を支持するものであることがわかった。この発見を基に、DDoS 攻撃のグローバルトレンドを知ることができるだけでなく、新種の DDoS 攻撃の発見も可能である。

4.1　システムの枠組み

提案するシステムは、所定の短い観測期間中にホストから受信したパケット数から、攻撃側ホストごとの特徴ベクトルを抽出した後、半教師あり学習を用いて学習と予測を行う。

システムの枠組みを図 1 に示す。図中左の特徴抽出ブロックでは、ダークネット内で観測したパケットを発信元 IP アドレス別にグループ化している。次に、特定のホストに関して、最初のパケットが観測された時刻から所定時間のパケットをすべて収集し、それらを特徴ベクトルに変換する。図中右側、検知ブロックでは、入力データを分類器に入れ、DDoS イベントと非 DDoS イベントを分けている。分類器が高い信頼度で DDoS 攻撃イベントを予測した場合、攻撃を受けるホストにアラートを発する。分類器の予測の信頼度が低い場合、インシデントが人間のオペレータに転送され、正当化を求める。正しいラベル情報を持つ正当化されたデータが分類器に入れられ、追加学習が行われる。分類器には、一般化性能が傑出しているサポートベクトルマシン（SVM）[16] を用いた。

検出に関しては、単一の送信元ホストから 30 秒間

に送られるダークネットパケットから、表 4 に示す 17 の特徴を採用した。特徴を描写するために、30 秒の観測期間中に少なくとも 20 パケットを送信するホストについての特徴ベクトルのみを生成した。ホストに関する検出は、60 分おきに実施した。

表 4　DDoS 攻撃イベント検知に関する特徴の抽出

ホストから観測されたパケット数
パケット間の時間間隔（平均及び標準偏差）
発信元ポート数
発信元ポートから送られたパケット数（平均及び標準偏差）
プロトコルタイプの数（TCP フラグのタイプを含む）
攻撃を受けた送信先ポート数
送信先ポートに送られたパケット数（平均及び標準偏差）
送信先 IP 数
送信先 IP に送られたパケット数（平均及び標準偏差）
送信先 IP の差異（平均及び標準偏差）
ペイロードサイズ（平均及び標準偏差）

4.2　実験結果

実験では、最初の 2 週間で作られた特徴ベクトルを用いて SVM 分類器の初期学習訓練を行った。その後の 6 週間で作られた特徴ベクトルは、テストと再訓練に用いた。追加学習は、以下のプロセスで行われる。最初の 2 週間のデータを用いて初期訓練を行った後、第 3 週の特徴ベクトルは、初期学習で取得したモデルに対してテストが行われる。次に、SVM 分類器は最初の 3 週間からすべての特徴ベクトルを再訓練する。以降の週も上記のプロセスを繰り返し、最終的に第 8 週の特徴ベクトルが訓練に含まれるまで続けられる。

表 5 に、追加学習あり／なしの結果をまとめた。表中左側から、DDoS イベントは追加学習なしでも非常に正確に検知されていることがわかる。とりわけ、リコールはほぼ 1 に達している。すなわち、ほぼすべての DDoS イベントが検知されている。このことから、17 の特徴と分類器を用いることで、DDoS バックスキャッタと非 DDoS バックスキャッタの違いをとら

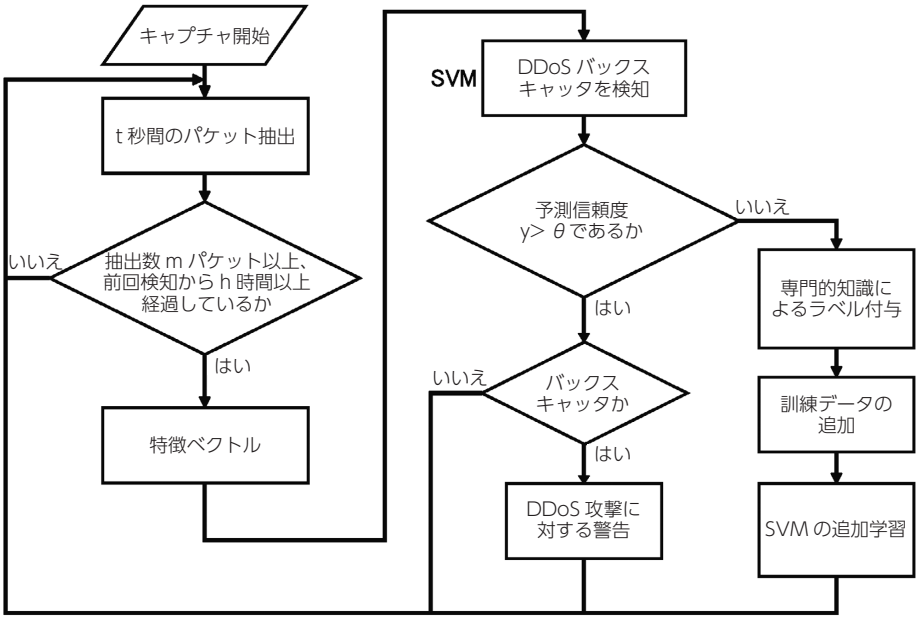


図 1　DDoS 攻撃イベント検知のための枠組み（図は [17] からの再利用）

表 5　DDoS イベント検知に関する性能評価

週	追加学習なし				追加学習あり			
	精度（%）	リコール（%）	F1-尺度	時間（秒）	精度（%）	リコール（%）	F1-尺度	時間（秒）
3	96.6	100	0.982	120	96.6	100	0.982	120
4	96.9	99.8	0.983	–	97.4	99.8	0.986	237
5	98.7	100	0.992	–	98.7	100	0.992	368
6	96.3	100	0.981	–	96.4	100	0.982	531
7	98.3	100	0.991	–	98.3	100	0.992	676
8	96.7	99.8	0.982	–	96.7	99.8	0.983	880

えられることがわかる。したがって、それらはDDoSイベント検知に有効である。表5の右側から、追加学習によって、第5週を除いて検知性能がさらに改善していることがわかる。これは、時とともにアクティビティのパターンが多様化し、追加学習によってシステムがそのような多様化に対応できることを示唆している。

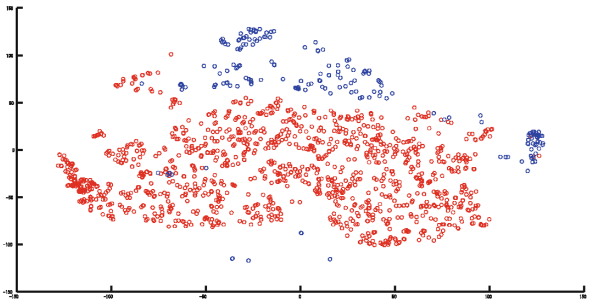
表5に示したように数週間で生成されたデータに関する訓練とテストが行われている限り、計算時間は重要でない。しかし、NICTERのような長時間の観測プロジェクトの場合、入力データを効果的に取り扱うことができるオンライン学習スキームが、今後の研究として求められるだろう。

4.3　考察とまとめ

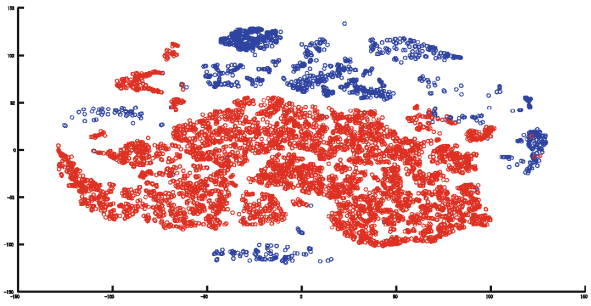
4.2で見たように、追加学習によって分類性能が改善される。このことは、時間とともに新たなアクティビティパターンが現れることを意味する。そのような変化とアクティビティパターンの多様化を可視化するために、t-SNE[18]と呼ばれる次元縮小法を用いた。t-SNEを利用して17次元の特徴ベクトルを2次元ベクトルに圧縮したものを、図2の散布図にプロットした。図2（a）–（c）はそれぞれ、1月1日から1月7日まで（第1週）、2月28日まで（ほぼ最初の8週間）、6月30日までの期間に観測されたデータを示している。赤と青はそれぞれ、最初の8週間に観測されたDDoSイベントと非DDoSイベントである。緑は、最初の8週間後に収集されたラベルなしのデータで、**4.2**の分析には使用されていない。図2（a）の分布と比較して、DDoSイベント及び非DDoSイベントのどちらも、図2（b）では広がっている。これは、アクティビティパターンが時とともに多様化していることを意味する。さらに、図2（a）には存在しないクラスタが、図2（b）には出現しており、新しいタイプのアクティビティパターンが出現していることがわかる。さらに図2（c）から、最初の8週間後、分布がより広がり、新たなクラスタが出現していることがわかる。これらの結果から、時とともにホストのアクティビティパターンが変化していること、そのような新たなパターンを区別するには追加学習が必要であることがわかる。

5　新たな脅威の早期検知

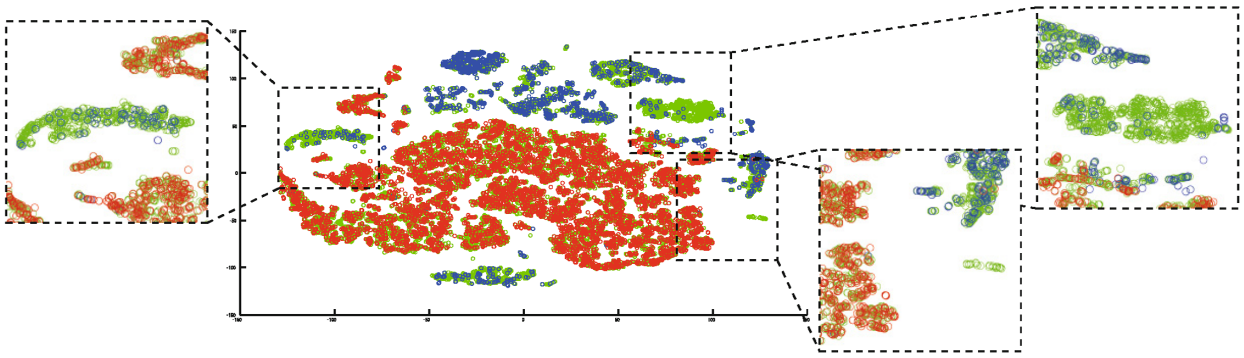
ダークネットで捕捉したトラフィックデータには、インターネットのスキャンに利用されているプログラミングテクニックに関する犯罪科学上の貴重な情報が



（a）1週間



（b）8週間



（c）6ヵ月間

図2　t-SNEを用いたホストアクティビティの可視化。プロットは、2014年（a）1月1日から7日まで、（b）2月28日まで、（c）6月30日を示している。（図は[17]からの再利用）

含まれる。本セクションでは、相関ルール分析を応用した、ダークネットで観測された攻撃側ホストの挙動特徴把握について説明する [19]。

5.1　相関ルール分析

相関ルール分析問題はもともと、一緒に購入される頻度の高い商品のグループを見出すために、スーパーマーケットのカゴの中身のデータを取るという文脈で提示されたものである [20]-[22]。文献 [20] におけるオリジナルの定義に従い、相関ルール分析を次のように定義する。

$D = \{T_1, T_2, ..., T_N\}$ は、「データベース」と呼ばれる N 回のトランザクションの集合である。$I = \{i_1, i_2, ..., i_M\}$ は、データベースに存在する M 個のアイテムすべての包括的集合である。D における各トランザクションは、固有のトランザクション ID を持ち、I 内のアイテムの部分集合を含む。アイテム集合 X（短いアイテム集合）のサポート s（X）は、そのアイテム集合を含むデータベース内のトランザクション数／割合として定義される。

頻出パターンマイニングは、少なくともトランザクションの割合 S に存在する、$P \subset I$ であるような全パターンを決定するためのものである。割合 S は、最小サポートと呼ばれ、絶対値、データベース内の全トランザクション数に対する割合のどちらの形でも表現できる。

相関ルールは、次の形の論理包含として定義される。

$$X \rightarrow Y, \text{ for } X, Y \subseteq I, X \cap Y = \phi \qquad (1)$$

アイテム集合 X と Y はそれぞれ、ルールの仮定と結果と呼ばれる。ルールの信頼度は、条件付確率 P(Y|X) によって示される。すなわち、

$$\text{conf}(X|Y) = s(X \cap Y)/s(X). \qquad (2)$$

考えられる全てのルールから興味深いルールを選択するために、最小サポートの閾値 S_0 と最小信頼度の閾値 C_0 の双方を満たすものは強いルールと呼ばれる。

一般的に、相関ルール分析は 2 つのステップで行われる。

1）頻出パターンマイニング：可能な全アイテムの組み合わせのべき集合において最小サポートを満たすアイテム集合を探す。アプリオリ [20] や FP ツリー [21] など、以下に示すアプリオリ特性を利用した有効なアルゴリズムが存在している。頻出アイテム集合の空でない部分集合はすべて、頻出である。つまり、頻出でない部分集合を含む集合はすべて頻出でない。

2）強い相関ルールの生成：頻出アイテム集合 l それぞれについて、空でない l の部分集合をすべて生成する。l の空でない部分集合 s それぞれについて、信頼度が最小信頼度の閾値 C_0 を越えている場合、ルール $s \rightarrow (l\text{-}s)$ を出力する。ルールは頻出アイテム集合から生成されているため、このような方法で作られたすべての相関ルールは自動的に最小サポートを満たす。

5.2　攻撃側ホストの挙動特徴把握への応用

攻撃側ホストの挙動の規則性を見つけることができれば、既存のマルウェア対策を以下の側面で補足できる。第 1 に、流行している攻撃パターンを発見することで、攻撃のメカニズムに対する洞察が深まり、攻撃への対策が可能になる。第 2 に、新たな攻撃パターン／グラフの出現は、大流行するインシデントの症状である可能性があるため、その早期検知と削除は重大な損害の予防につながる。第 3 に、そのような情報を利用して観測システムの性能を向上することで、限定的なシステム及びネットワークリソースを使用して収集可能な適切なマルウェア情報を増やすことができる。

以下に、攻撃を受けた送信先ポート間の相関を利用した相関ルール分析を提案する。オープンなサービスに関する重要な識別情報を提供するネットワークポートは、ネットワークにつながれたあらゆるデバイスの入口である。16 ビットの数値で示されるポート番号は、デバイスの IP アドレスとともに、通信セッションの送信先アドレスを完成させる。マルウェアは通常、デバイス上の開いているポートを探り、利用可能なサービスを決定する。その後、そのサービスに関して既知の脆弱性を利用する。

送信先ポートに関して発見された強い相関ルールは、以下の側面における有用な情報を提供する。第 1 に、異なるマルウェアプログラムは通常、異なる脆弱なポートの組み合わせを利用するため、送信先ポートは特定のマルウェアを識別するための犯罪科学上の情報を提供する、または攻撃者の意図に関するヒントを提供することができる。したがって、頻出パターンマイニングは、自動マルウェアシグネチャ抽出のための効率的なアプローチとなり得る。 第 2 に、頻繁に探索されるポートの組み合わせによって最も脆弱なサービスが明らかになる可能性があり、マルウェア診断のための貴重な手がかりとなる。

5.3　送信先ポート間の高次相関をマイニングする

送信先ポート間の相関を発見するために、1 日のうちに攻撃側 IP によって探索された固有のポート番号の組み合わせをデータベース内のトランザクションとして定義することで、マイニング問題を形成する。

表 6　送信先ポート 80 に関連する頻出アイテム集合 (/16 ダークネットセンサの 1 日のトラフィックから取得)

ID	送信先ポート 1	送信先ポート 2	送信先ポート 3	送信先ポート 4	発生件数
1	80				2,932
2	80	8			747
3	80	443			786
4	80	13	443		715
5	80	8	13		741
6	80	8	443		713
7	80	13	443		712
8	80	8	13	443	711

表 6 は、/16 センサの 1 日のトラフィックトレースから学習した頻出アイテム集合を示している。最小サポートは 700 と設定した。610 の頻出アイテム集合のうち、ウェルノウンポートであるポート 80 に関連する 8 つの頻出アイテム集合を選択した。ウェブサービスのホスティングにはポート 80 がよく使われているため、多くの攻撃がこのポートを探索する傾向がある。表からわかるように、1 日のうちに 2,932 のホストがポート 80 を攻撃している。ポート 80 とともに探索されているポートが多く、特にポート 8、13、443 が多い。表中、これら 4 つのポートとの関係が強いすべての頻出アイテム集合が示されており、一番右の列はその発生件数である。ポート 8、13、443 が強い相関を持つことは明確である。つまり、これらは同時に探索される傾向がある。

関係するポート上のネットワークサービスは下記の通りである。ポート 8：割当てサービスなし、ポート 13：daytime プロトコル、ポート 80：ハイパーテキスト・トランスファー・プロトコル (HTTP)、ポート 443：TLS/SSL によるハイパーテキスト・トランスファー・プロトコル (HTTPS)。

このことは、表 7 (表 6 の頻出パターンから作成した) に示す相関ルールによって確認できる。表 7 では、ポート 80 と 13 の同時発生件数の高さにも関わらず、相関ルール $P80 \rightarrow P13$ の信頼度は 24.3 % に過ぎないため、最小信頼度要件の 80 % を満たしていない。一方、相関ルール $P13 \rightarrow P80$ は 94.7 % と強い信頼度を示している。したがって、ポート 13 の探索は、ポート 80 探索の要因として考えることができる。すなわち、ポート 13 を目的地とするパケットがホストから観測された場合、ポート 80 が探索される可能性が高い。

また、表 7 のルール 5 から 7 を例にとると、これら 3 つのルールは、ポート 8、80、334 の間の相関を示している。3 ポートのうち 2 つが探索されると、3 つ目のポートが探索される確率は 94 % を超える。3 ポートの相関が高いことから、これらをスキャン挙動のシグネチャとして扱うことができる。

表 7　表 6 の頻出パターンから作成した相関ルールの一部

ID	Rule	Support	Confidence
1	$80 \rightarrow 8$	747	27.5%
2	$8 \rightarrow 80$	747	4.7%
3	$80 \rightarrow 13$	715	24.3%
4	$13 \rightarrow 80$	715	94.7%
5	$80, 443 \rightarrow 8$	741	94.3%
6	$8, 443 \rightarrow 80$	741	95.5%
7	$8, 80 \rightarrow 443$	741	99.2%
8	$13, 443 \rightarrow 80$	712	95.3%
9	$80, 443 \rightarrow 13$	712	90.6%
10	$13, 80 \rightarrow 443$	712	99.6%
11	$8, 13 \rightarrow 80$	713	95.2%
12	$8, 80 \rightarrow 13$	713	95.4%
13	$13, 80 \rightarrow 8$	713	99.7%
14	$13, 8, 443 \rightarrow 80$	711	95.4%
15	$8, 80, 443 \rightarrow 13$	711	96.0%
16	$13, 80, 443 \rightarrow 8$	711	99.9%
17	$8, 13, 80 \rightarrow 443$	711	99.7%

ルール 1～3 は、信頼度の閾値 (C0=0.8) を超えていないため、重要な相関ルールと認められない。

5.4　まとめ

上記の実験で発見された強い相関ルールは、相関の強い送信先ポートがマルウェア亜種を特定するシグネチャになり得ることを示している。しかしながら、これを証明するには、探索を実施しているマルウェアプログラムの正確な情報をつかむための他のデータソースからの情報が必要である。実際、上記の発見事項は、Carna ボットネットと関係することが確認されている [24]。Carna ボットネットは、デフォルトの認証情報によりオンラインでアクセス可能な 42 万以上の組み込みデバイスに侵入することで構築された。侵入後、それらのデバイスには小さなバイナリコードがアップロードされ、インターネット全体に対し IPv4 アドレス空間のスキャンを行う。Carna ボットネットの所有

者によると、Carna ボットネットは研究目的で作られたもので、その運用についての詳細な説明と 9 TB に及ぶスキャニングアクティビティの生ログが発表されている。文献 [25] の過去の研究によると、ポート 8、80、433 の探索及びポート 23 と 210 の探索は、同ボットネットの別の部分によるネットワークスキャンのシグネチャであると報告されている。

文献 [23] では、上記の発見を拡大し、最新の種類の攻撃を早期段階で識別することで、それらのサイバー攻撃に対する未然の対応を促進している。

6 結論

本稿では、グローバル規模のダークネット観測プロジェクト NICTER について、特にそのインシデントレポートや取扱いをサポートするバックエンド分析エンジンに注目しながら紹介した。ダークネットで観測された攻撃側ホストに関する全体的な情報不足にもかかわらず、収集されたトラフィックを分析することで、攻撃に関する興味深い規則性を明らかにし、マルウェア対策に貢献できる。これらの発見を基に、関連攻撃への対策が実現できると考えられる。

【参考文献】

1 M. Bailey, E. Cooke, F. Jahanian, J. Nazario, D. Watson, et al., “The internet motion sensor – a distributed blackhole monitoring system,” NDSS, 2005.
2 D. Inoue, K. Yoshioka, M. Eto, M. Yamagata, E. Nishino, J. Takeuchi, K. Ohkouchi, and K. Nakao, “An incident analysis system NICTER and its analysis engines based on data mining techniques,” ICONIP 2008, Part I. LNCS, vol.5506, pp.579–586, 2009.
3 T. Ban, L. Zhu, J. Shimamura, S. Pang, D. Inoue, and K. Nakao, “Behavior analysis of long-term cyber attacks in the darknet,” 19th International Conference Neural Information Processing (ICONIP 2012) , Part V, vol.151, no.3, pp.620–628, 2012.
4 U. Harder, M. W. Johnson, J. T. Bradley, and W. J. Knottenbelt, “Observing internet worm and virus attacks with a small network telescope,” Electronic Notes in Theoretical Computer Science, vol.151, no.3, pp.47–59, 2006.
5 K. Benson, A. Dainotti, K. Claffy, and E. Aben, “Gaining insight into as-level outages through analysis of internet background radiation,” in Computer Communications Workshops, INFOCOM, pp.447–452, 2013.
6 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 (JWIS 2007) , pp.267–279, 2007.
7 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.
8 D. Inoue, M. Suzuki, M. Eto, K. Yoshioka, 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, LNCS 5758, pp.381–382, 2009.
9 D. Inoue, M. Eto, K. Suzuki, M. Suzuki, and K. Nakao, “DAEDALUS-VIZ: novel real-time 3D visualization for darknet monitoring-based alert system,” In Proceedings of the Ninth International Symposium on Visualization for Cyber Security (VizSec 2012) , pp.72–79, 2012.
10 K. Suzuki, M. Eto, and D. Inoue, “Evaluation of NIRVANA: Real network traffic visualization system,” Journal of the National Institute of Information and Communications Technology, vol.58, no.3/4, pp.61–77, 2011.
11 D. Song, R. Malan, and R. Stone, “A snapshot of global Internet worm activity,” 14th Annual FIRST Conference on Computer Security Incident Handling and Response, 2002.
12 D. Moore, “Network telescopes: tracking denial-of-service attacks and Internet worms around the globe,” 17th Large Installation Systems Administration Conference (LISA 2003) , USENIX, 2003.
13 M. Bailey, E. Cooke, F. Jahanian, J. Nazario, and D. Watson, “The Internet motion sensor: A distributed blackhole monitoring system,” 12th Annual Network and Distributed System Security Symposium (NDSS 2005) , 2005.
14 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 2005) , 2005.
15 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.
16 V.N. Vapnik, “The Nature of Statistical Learning Theory,” Springer, 1995.
17 N. Furutani, J. Kitazono, S. Ozawa, T. Ban, J. Nakazato, and J. Shimamura, “Adaptive DDoS-event detection from big darknet traffic data,” ICONIP, vol.4 pp.376–383, 2015.
18 L., Van der Maaten, and G. Hinton, “Visualizing data using t-SNE,” Journal of Machine Learning Research, vol.9, pp.2579–2605, 2008.
19 T. Ban, M. Eto, S. Guo, D. Inoue, K. Nakao, and R. Huang, “A study on association rule mining of darknet big data,” IJCNN 2015, pp.1–7, 2015.
20 R. Agrawal, T. Imielinski, and A. Swami, “Mining association rules between sets of items in large databases,” in ACM SIGMOD Record, vol.22, no.2. ACM, pp.207–216, 1993.
21 J. Han, J. Pei, and Y. Yin, “Mining frequent patterns without candidate generation,” in ACM SIGMOD Record, vol.29, no.2. ACM, pp.1–12, 2000.
22 C. Borgelt, “Frequent item set mining,” Data Mining Knowledge Discovery, vol.2, no.6, pp.437–456, 2012.
23 T. Ban, S. Pang, M. Eto, D. Inoue, K. Nakao, and R. Huang, “Towards early detection of novel attack patterns through the lens of a large-scale darknet,” submitted to ATC 2016.
24 C. Stocker and J. Horchert, “Mapping the Internet: A hacker’s secret Internet census,” Spiegel Online, 22/3, 2013.
25 E. Le Malecot and D. Inoue, “The carna botnet through the lens of a network telescope,” in Foundations and Practice of Security, Springer, pp.426–441, 2014.

班　涛　（ばん　とう）

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
主任研究員
博士（工学）
機械学習、ネットワークセキュリティ