4-2　ライブネット高速分析技術

嶌田一郎　津田　侑

標的型攻撃では、攻撃者はあらゆる手法で境界防御型のセキュリティ対策を突破し、組織内ネットワークへ侵入、情報窃取や破壊活動など攻撃者の目的に沿った攻撃を実行する。したがって、その対策には境界防御だけでなく、攻撃者に組織内に侵入されることを想定した攻撃活動の迅速な検知が要求される。本稿では組織内の膨大なライブネット通信の中から悪性ホストとの通信やスキャン活動を高速に発見する手法を提案する。

1　はじめに

近年、国内の大手重工メーカを皮切りに衆参両議院や府省庁等のネットワークへの標的型攻撃が次々と明らかになり、標的型攻撃への抜本的な対策技術の確立が喫緊の課題となっている。侵入防止を目的とした境界防御型のセキュリティ対策を標的型攻撃メールなどにより突破後、マルウェアを組織内ネットワークへ侵入させ、情報を窃取し、組織外部の悪性ホストへ窃取した情報を送出する。このような標的型攻撃への対策としては、組織内部のライブネット通信から迅速に不正な通信を検知することが求められる。そこで本稿において、膨大なライブネット通信から悪性ホストへの不正な通信を早期検知する手法として研究開発を行った、NICTER[1] が持つダークネット観測情報（観測で得た膨大な量の悪性ホスト情報のデータベース）を利用したブラックリスト方式の不正通信検知技術及びベイズ意思決定を応用した低速スキャン検知技術について報告する。

2　関連技術

2.1　インシデント分析システム NICTER

情報通信研究機構（NICT）が研究開発を進めている NICTER は、大規模ダークネット観測網を用いてイベントを解析しインシデントを検出・分析するマクロ解析システムを持つ。マクロ解析システムでは、国内外に分散配置されたセンサによってダークネットの観測を行っている。ダークネット観測情報には膨大な悪性ホストの情報が含まれており、必然的に C & C サーバの情報も含まれる。センサにおいて収集されたパケットは、リアルタイムにデータベースシステム MacS DB[2] に蓄積される設計となっているため、MacS DB に蓄積されたパケットデータをブラックリストの IP アドレス（以下、ブラックリスト IP）として検知に利用した。

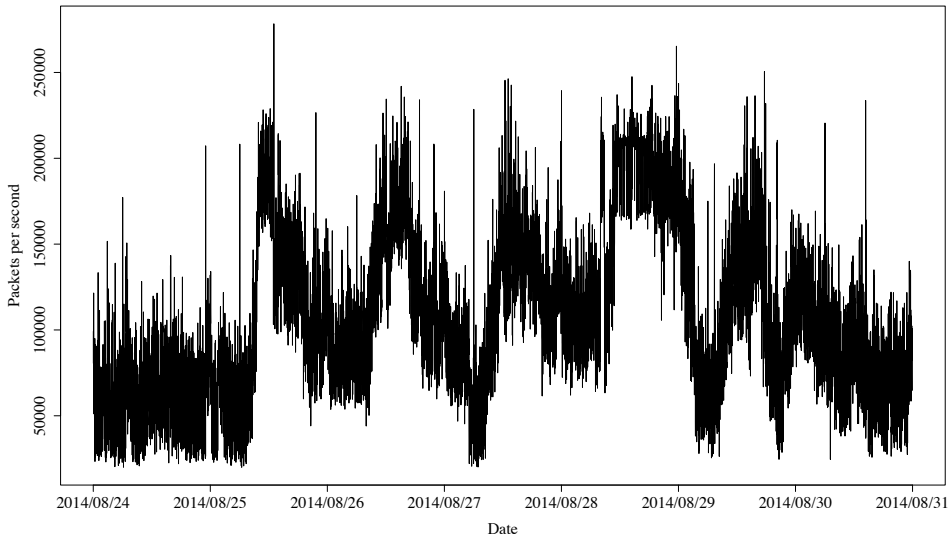

図 1　NICT 内のライブネット観測トラフィック量

2.2　ライブネットトラフィック可視化システム NIRVANA

NIRVANA[3] は、NICTER のダークネット観測パケットのリアルタイム可視化技術を、特定の組織内トラフィックの観測に応用したもので、組織内ネットワークを流れる膨大な量のパケットのネットワーク層、トランスポート層のヘッダ情報を収集、集約し、可視化用端末に送信することでライブネット通信の状態を可視化表示する。本研究では、NIRVANA が持つ組織内トラフィックのヘッダ情報の収集、集約機能を利用することでライブネットトラフィックを観測し、**3** 及び **4** で示す検知に利用した。トラフィック量のサンプルとして、2014 /8 /24 から 31 の期間の観測トラフィック量を図 1 に示す。

2.3　システム構成

本研究において構築したシステムの概念図を図 2 に示す。本システムでは、まず①解析時に照合する IP アドレスリスト（図 2 の IP LIST）を作成する。IP アドレスリストは、ブラックリスト検知においてはブラックリスト IP であり、低速スキャン検知においてはホワイトリストの IP アドレスである。次に NIRVANA で使用しているライブネットデータバスからパケットを取得し、②解析モジュールで IP アドレスリストとの照合を行う。③照合結果のデータを解析し不正通信を検出した場合、可視化システムにアラートを送信する。

3　ブラックリスト検知

3.1　概要

本研究の目的は、膨大なライブネット通信から悪性ホスト（C & C サーバ）との通信を、NICTER が持つダークネット観測情報をブラックリストとして利用して、迅速に検知することである。これを実現するためには、ライブネット通信と悪性ホストのリストをリアルタイムに高速分析する必要がある。一般に、ブラックリストによる検知方式は、過去のサイバー攻撃で使用された攻撃元情報をブラックリストとして利用することで検知する手法であり、事前定義型のシグネチャであるため、未知の攻撃に対しリアルタイムに適用することは難しい。しかし、NICTER によるダークネット観測情報はリアルタイムの攻撃情報であるため、この情報をリアルタイムにブラックリスト IP として定義し、不正通信を検知する。

3.2　リアルタイム検知

ブラックリスト IP の作成には、MacS DB を参照する。MacS DB とはダークネットへ送信されたパケットのネットワーク層、トランスポート層のヘッダ情報が全て保存されているデータベースであり、MacS DB から過去 1 週間分のデータをブラックリスト IP として、ブラックリストデータベースに保存する。保存するデータは、バックスキャッタを除外するために、ダークネットへ TCP SYN パケットを送信した外部の悪性ホストの送信元 IP アドレス及び受信時刻とする。ブラックリスト IP を常に最新の状態に保つために、1 時間ごとに最新のデータを MacS DB から読み込んで更新する。次に、ライブネットを流れる TCP パケットを読み込み、送信元／宛先 IP アドレスが、作成したブラックリスト IP と一致するか照合する。照合結果が一致し、該当ホストが、TCP SYN パケットに対して TCP SYN-ACK パケットを応答していた場合、セッションを接続しているものとみなし、アラートを送信する。

ブラックリスト IP の照合処理において、単純な線形探索ではブラックリスト IP 数の増加と共に照合処理時間も増加してしまう問題があった。このため、ブ

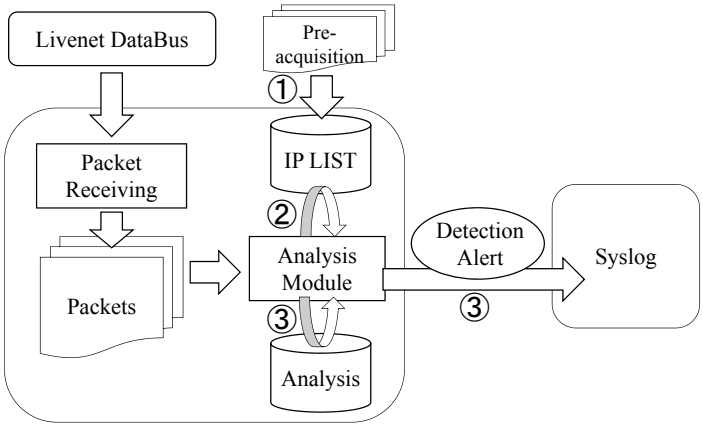

図 2　システムの概念図

ラックリスト IP の個数によらず高速に行えるように、IPv4 の全 IP アドレスを 1 ビットずつメモリ上に対応させて保持し、ビットの ON/OFF によりブラックリスト IP の有無を照合できる処理とした。照合処理はブラックリスト IP の個数によらず、数ステップで処理を完了でき、照合処理速度としては十分な性能を得ることができた [4]。

3.3　NICT ネットワーク環境での観測結果

ブラックリスト IP との通信状況をより明確にするために、接続方向で Inbound 通信と Outbound 通信に分類した。通信状況の模式図を図 3 に示す。NICT のネットワーク環境での観測結果、Inbound 通信において、DMZ 上のホスト、ハニーポット及び Web サーバなど外部公開サーバへのブラックリスト IP からのアクセスを検知した。また、Outbound 通信において、Proxy サーバ経由での内部ホストからの通信を検知した。さらに、他のセキュリティアプライアンスにおいてスキャンとしてとらえられていた外部ホストが、ブラックリスト検知においてもとらえられていた。これは、ダークネットを含むインターネット上のアドレス空間をスキャンしているホストが検知されているものと考えられ、ブラックリスト IP の重要度の判定への活用が期待できる。今後の課題として、アラート精度の向上がある。実現手法として、ダークネット観測情報以外の不正通信観測データを活用する等の手法が考えられる。

4　低速スキャン検知

4.1　概要

攻撃者は通常、対象となるネットワークに関する詳細情報を持たないため、侵入した組織内のホストに対してパケットを送信し、ホストの有無や脆弱性に関する情報を取得する。しかし、ネットワーク IDS は短時間に多数のパケットを送信する特徴を利用してスキャンを検知するため、攻撃者はネットワーク IDS による検知を回避しようとして、長い時間をかけ低速でスキャンを実行する場合がある。このような低速スキャンは、既存のネットワーク IDS で検知することは難しい。そこで、文献 [5] において、組織内の膨大なライブネット通信から低速の SYN ステルススキャンを検知する研究を行った。検知手法は次のとおりである。

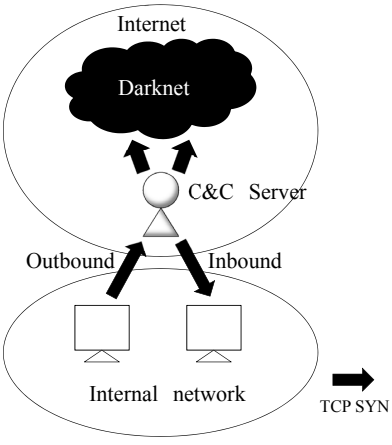

図 3　ブラックリスト IP との通信状況

まず、スキャンパケットによるコネクション接続試行の状況を、Threshold Random Walk [6]（以下、TRW）の枠組みを用い、ベイズ意思決定を応用することで検知を行った。さらに、スキャンパケットの抽出を容易にするために、通常のトラフィックをホワイトリストを用いて除去した。

4.2　検知手法

NIRVANA で使用されるライブネットトラフィックはパケットのネットワーク層、トランスポート層のヘッダ情報であるため、TRW の手法を用いるためには TCP によるコネクション接続の成功／失敗をヘッダ情報をもとに判定する必要がある。コネクション接続の成功／失敗を判定方法として、5-tuple、TCP フラグ、タイムスタンプ及びシーケンス番号により判定する文献 [5] の手法を用いた。本手法を用いることにより、パケット欠損によるコネクション判定誤りを低減しコネクション判定精度を向上させた。また、低速スキャン検知の False Positive（以下、FP）を低減させるために、ホワイトリストによるフィルタリングを導入し、通常のトラフィックを除外した。ホワイトリストは、上記のコネクション判定手法で判定したコネクション成功及び失敗情報をもとに、送信元／宛先 IP アドレス、宛先ポート番号、タイムスタンプ、成功／失敗回数の内容で作成した。

さらに、スキャンの状況を観測者にとってより容易に把握できるようにするために、コネクション接続試行の状況を確信度のランダムウォーク（主観確率の変化）で表すことを試みた。まず、良性ホスト及び悪性ホストのコネクション接続確率を推定し、次に、コネクション接続成功／失敗の情報をもとに逐次仮説検定を用いてスキャンを検出する TRW の枠組みを用い、1 回のコネクション接続試行が持つ情報量に着目して、ベイズ意思決定を応用した [5]。

4.3　NICT ネットワーク環境での観測結果

NICT のネットワーク環境で低速スキャンを実行し評価を行った。スキャンパケットを送信する間隔は、数分間隔から 1 日間隔で実行した。低速スキャンを実

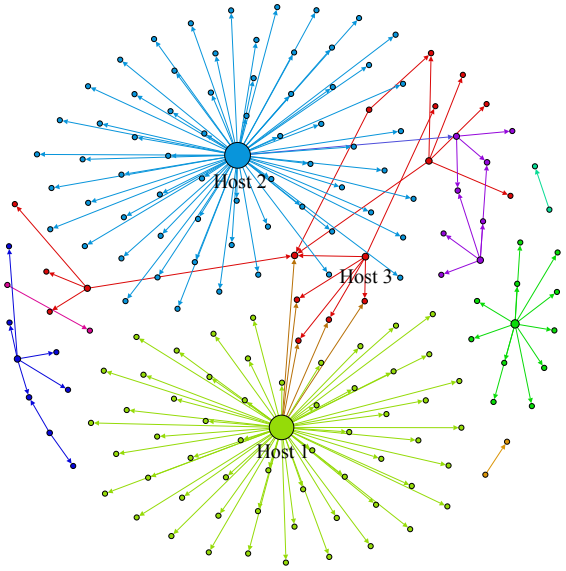

図 4　コネクション接続失敗と送信元ホスト

行したホストは、全て検知することができた。検知結果は、仮定する悪性ホストのコネクション接続成功／失敗確率を示すパラメータに依存しているが、少ないコネクション試行回数で低速スキャンを検知することができた。図 4 は、実験結果から抽出したコネクション接続失敗と送信元ホストのグラフを示している。グラフは、グラフマイニングツール [7] によって作成した。グラフのノードはホストを表し、エッジは接続試行の方向を表す。実験で使用したホスト 1-3 の出次数が多いことがわかる。今後、更にスキャンの状況を観測者にとってより容易に把握できるようにすることがインシデントへの即応の点で重要である。また、他の検知手法と比較し、検知精度を検証することが重要であると考えている。

5　おわりに

本研究では、ダークネット観測情報をブラックリストとして不正通信の検知を行う手法の有効性の検証を、NICT 内のネットワーク環境において実施した。また、低速スキャン検知手法を提案し、有効性の実証を行った。今後、更に NICT 内のネットワーク環境において検証を行い、成果を社会に展開できるよう研究に取り組みたい。

謝辞

本研究を進めるにあたり、NICT の情報通信システム室の皆様に、NICT 内トラフィックデータ及び各種セキュリティアプライアンスデータを提供頂いた。ここに感謝の意を表す。

【参考文献】

1　D. Inoue, M. Eto, K. Yoshioka, S. Baba, K. Suzuki, J. Nakazato, K. Ohtaka, 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.
2　衛藤将史，高木彌一郎，“インシデント分析センター nicter のシステム実装と社会展開，” 情報通信研究機構季報，vol.57, nos.3/4, pp.17–25, 2011.
3　鈴木宏栄，衛藤将史，井上大介，“実ネットワークトラフィック可視化システム NIRVANA の開発と評価，” 情報通信研究機構季報，vol.57, nos.3/4, pp.63–79, 2011.
4　嶌田一郎，津田侑，神薗雅紀，井上大介，中尾康二，“ライブネットにおける不正通信の早期検知手法，” コンピュータセキュリティシンポジウム 2013 (CSS2013)，2013.
5　I. Shimada, Y. Tsuda, M. Eto, and D. Inoue, “Using Bayesian Decision Making to Detect Slow Scans,” Workshop on Building Analysis Datasets and Gathering Experience Returns for Security (BADGERS 2015), 2015.
6　J. Jung, V. Paxson, A. W. Berger, and H. Balakrishnan, “Fast portscan detection using sequential hypothesis testing,” IEEE Symp. Sec. and Priv, 2004.
7　M. Bastian, S. Heymann, and M. Jacomy, “Gephi: An open source software for exploring and manipulating networks,” International AAAI Conference on Weblogs and Social Media 2009, 2009.

嶌田一郎　（しまだ　いちろう）
株式会社構造計画研究所
元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
専門研究員
ネットワークセキュリティ、ネットワークトラフィック解析

津田　侑　（つだ　ゆう）
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
博士 (情報学)
サイバーセキュリティ、標的型攻撃対策