ライブネットにおける低速スキャン検知手法

嶌田 一郎 †　　津田 侑 †　　衛藤 将史 †　　井上 大介 †

† 独立行政法人　情報通信研究機構
184-8795 東京都小金井市貫井北町 4-2-1
{i-shimada, tsuda, eto, dai}@nict.go.jp

あらまし　標的型攻撃により組織内ネットワークへ侵入した攻撃者は，長い時間をかけ索敵を行い，攻撃の踏み台となるホストを増殖させる．索敵活動は，ネットワーク IDS による検知を回避するために，低速スキャンにより数ヶ月にわたり行われる場合がある．したがって，標的型攻撃への対策の一つとして，索敵活動を攻撃の兆候と捉え，低速スキャンを迅速に検知することが有効と考えられる．そこで，本研究では組織内の膨大なライブネット通信から低速スキャンを簡易かつ効率的に検知する手法を提案する．

A Slow-Scan Detection Method for Live Network Environments

Ichiro Shimada†　　Yu Tsuda†　　Masashi Eto†　　Daisuke Inoue†

†National Institute of Information and Communications Technology.
4-2-1, Nukui-Kitamachi, Koganei-shi, Tokyo 184-8795, JAPAN
{i-shimada, tsuda, eto, dai}@nict.go.jp

Abstract　In targeted cyber attacks, attackers intrude into the internal network of an organization. They perform a search for vulnerable hosts, and increase the number of hosts they can use as stepping stone for further attacks. In particular, reconnaissance activity may be performed through slow scanning. Such scans can be spread over several months to evade Network Intrusion Detection Systems (NIDSes). In that context, we regard reconnaissance activity as a sign of future attacks, and therefore it is important to detect slow scanning as early as possible. In this paper, we propose a simple and efficient approach for detecting slow scanning within a live network.

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．

標的型攻撃の攻撃フェーズについて記述された文献 [1, 2, 3] はいくつかあるが，本研究では文献 [1] の攻撃フェーズの分類を用いる．標的型攻撃では，SNS や Web 検索エンジンなどを用いたソーシャル･エンジニアリングにより標的に関する情報を収集し（フェーズ 1），標的の関係者を装った標的型攻撃メールを送ることにより標的の組織内部の PC へ侵攻し（フェーズ 2），攻撃ツールをインストールする（フェーズ 3）．侵入防止を目的とした従来の境界防御型のセキュリティ対策では，このような経路を通る攻撃を防ぐことは難しい．組織内部に攻撃ツールを送り込んだ後に，C&C サーバ（悪性ホスト）との通信を開始する（フェーズ 4）．そして，標的

組織内部の PC を支配し橋頭堡を確保した上で，そこを拠点として索敵を行い（フェーズ 5），攻撃の踏み台となる PC を増殖させる（フェーズ 6）．攻撃者は踏み台を介して目的となるサーバを占領し（フェーズ 7），目的の情報を組織外部のホストへ送信する（フェーズ 8）．最後に，攻撃の痕跡を消去し撤収する（フェーズ 9）．これらの攻撃フェーズのうち，特にフェーズ 4 から 6 は長い時間をかけて実施される．組織内部で攻撃が発見されたときには，侵入から既に数ヶ月経過している場合もある．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．本研究では，索敵フェーズでの不正通信として，低速スキャンの検知に焦点を当てる．

スキャンは，攻撃者がホストの有無や脆弱性などの情報を得るために，対象となるネットワーク上のホストにパケットを送信することで行われる．攻撃者は通常，詳細なネットワーク情報を持たないため，多くのホストに対してパケットを送信することで情報を得ようとする．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．実際に低速スキャンが行われた事例として，文献 [4] では，1 時間に平均数回程度という低頻度で，数ヶ月にわたり宛先ポート番号がランダムなスキャンが行われたと報告されている．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．したがって，標的型攻撃への対策の一つとして，低速スキャンを策敵フェーズの兆候と捉え迅速に検知することが有効と考えられる．本研究において，組織内の膨大なライブネット通信から通信シーケンスに着目しコネクション確立失敗をカウントすることで，低速スキャンを簡易かつ効率的に検知する手法を提案する．

本稿では，2 章では，関連研究について述べ，3 章では，基本方針について述べる．4 章では，低速スキャン検知手法について述べ，5 章では，システム設計・実装について述べる．6 章では，実験結果と考察を述べる．7 章では，まとめと今後の課題について述べる．

2 関連研究

低速スキャンを検知するために，コネクション確立失敗をカウントする研究がある．文献 [5] では，NetFlow[6] の観測データをデータベースへ登録し，コネクション確立失敗イベントを閾値により，最大で 60 秒間隔の低速スキャンを検知している．しかし，トラフィック量が大きくなると，大規模なリソースが必要となり，簡易に検知することは難しくなる．

また，低速スキャン検知としてではないが，TCP RST パケットを観測する方法で検知する研究として文献 [7] がある．文献 [7] では，Close ポートからのエラーパケット（TCP RST-ACK パケット）を観測し検知している．しかし，TCP RST パケットがフィルタリングされている場合，宛先ポートが閉じていても TCP RST が返信されないため検知できない．

文献 [8] では，コネクション成功，失敗を判断し複数の評価基準を用いて検知している．文献 [8] では，コネクション確立成功を TCP SYN-ACK パケットの応答で判定し，コネクション確立失敗を TCP RST-ACK パケットの応答か，t 時間経過しても何も応答しないことで判定している．しかし，TCP SYN-ACK パケットが欠損した場合，応答なしと判定されコネクション確立失敗と判定される．

低速スキャンの評価については，文献 [9] の研究がある．文献 [9] では，Bro[10] 及び Snort[11] に対して，nmap[12] による 60 秒間隔の低速スキャンの実験と評価を行っている．Bro 及び Snort では，time window や閾値を調整することで，60 秒以上の時間間隔の低速スキャンも検知できるが，誤検知率が大きくなる．

標的型攻撃を対象とした場合，大規模でパケットの欠損や TCP RST パケットのフィルタリングがある環境で，分～時間間隔のスキャンに対して低い誤検知率で攻撃を検知することが求められる．本稿において，情報通信研究機構内の大規模トラフィック環境で，まず，数分間隔の

低速スキャンの検知手法の研究を行った．

3　基本方針

本研究の目的は，膨大なライブネット通信から低速スキャンを簡易且つ効率的に検知することである．本目的を実現するために以下を基本方針とした．

1. TCP SYN によるスキャンを対象とする

   攻撃者は，通常のトラフックに紛れて索敵活動を行うものと考え，通信で一般的に使用される TCP SYN パケットによる低速スキャンを検知することを目標とする（XMAS スキャンなど規格外のパケットは対象外）．スキャンの種類としては，IP アドレススキャン（水平スキャン）及びポートスキャン（垂直スキャン）（以下，本稿では単にスキャンと呼ぶ）を検知することを目標とする．

2. IP,TCP ヘッダ情報だけを用いる

   ライブネット通信パケットの収集方法として，NIRVANA[13] を利用し，ネットワーク層，トランスポート層のヘッダ情報だけを用い簡易な手法で検知する．参照するヘッダ情報としては，送信元／宛先 IP アドレス，送信元／宛先ポート番号，プロトコル，TCP フラグ，シーケンス番号，タイムスタンプを用いる．

3. パケットの欠損を考慮する

   収集するライブネット通信パケットは大規模になるため，収集過程でパケットの欠損（取りこぼし）が発生し得る．このため，検知においてパケット欠損を考慮する．

4　低速スキャン検知手法

4.1　スキャンの特徴，及び検知方針

スキャンは，攻撃者がホストの有無や脆弱性などの情報を得るために，対象となるネットワーク上のホストにパケットを送信することで行われる．攻撃者は通常，詳細なネットワーク情報を持たないため，多くのホストに対してパケットを送信し，コネクション確立失敗が多く発生する．このため，コネクション確立失敗数をカウントすることでスキャンを検知する方法が考えられる．しかし，ライブ・トラフィックは大規模であり, 全てのパケットをカウントしようとすると，観測すべきパケットが大量となってしまい，カウント処理が遅延してしまう．そこで，4.2 節で情報通信研究機構内のトラフィック分析を行い，効率良くカウントする仕組みを検討した．

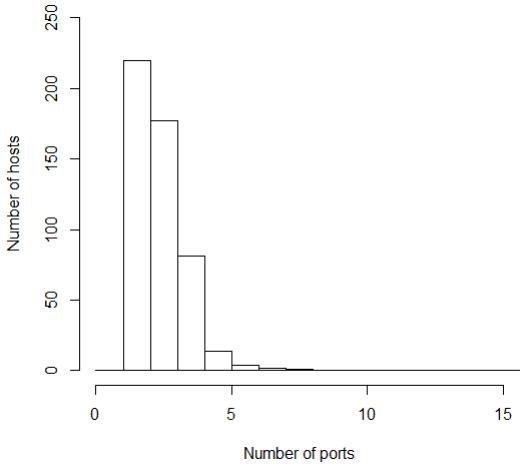

図 1: ホスト数と宛先ポート数

4.2　情報通信研究機構のトラフィック分析

ライブネット・トラフィック可視化エンジン NIRVANA は，NICTER[14] 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ある．NIRVANA は組織内ネットワークを流れる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収集，集約機能を利用し検知を行う．

NIRVANA により収集した情報通信研究機構内のライブネット通信パケットをもとにトラフィック分析を行った．分析したのは，2014/6/24 9:00 から 18:00 の期間の TCP プロトコル（TCP

表 1: 使用頻度の高いポート top10

サービス名	ポート番号
Proxy	3128/tcp
HTTP	80/tcp
NRPE	5666/tcp
HTTPS	443/tcp
LPD(Print Service)	515/tcp
SSH	22/tcp
Microsoft-DS AD	445/tcp
telnet	23/tcp
POP3S	995/tcp
POP3	110/tcp

SYN）による内部ホスト間通信のトラフィックデータである．図 1 に，ホスト数を度数とするヒストグラムを示す（データ区間は宛先ポート数）．殆どのホストは，宛先ポートとして 10 ポート程度しか使用していないことが分かる．また，表 1 に，上位 10 位の宛先ポート番号の種類を示す．宛先ポート番号は，well-known ポート，及び 1024 番以上の特定のポート番号で占められていることが分かる．本研究では，内部ホスト間通信で使用される宛先ポート番号の殆どが，使用頻度の高いポート番号で占められる特徴をホワイトリストとして低速スキャン検知に利用する．

4.3 検知方法

ホワイトリストにより，ライブパケットをフィルタにかけ，観測パケット数を削減する．フィルタ後のパケットについて，5.4 節で述べる通信シーケンスを用いた判定方法によりコネクション確立の成功／失敗を判定し，失敗数をカウントする．

カウント方法は，宛先 IP アドレスと宛先ポート番号の組み合わせが一意（destination IP-port combination unique）となるように行い，カウント値が閾値を超過した場合にスキャンと判定する．また，カウントは time window 内で送信元 IP アドレス毎に行い，time window で指定した時間を超過したら，それまで蓄積していたコネクション確立失敗情報はクリアする．

5 章で具体的な実装内容について述べる．

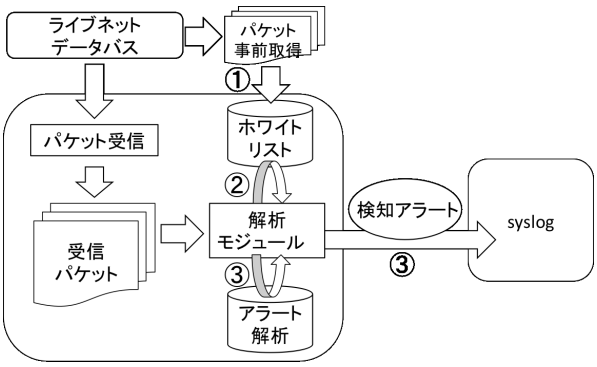

図 2: システム概要

5 システム設計・実装

5.1 システム概要

本研究で構築したシステムの概要を図 2 に示す．本システムでは，まず①事前にホワイトリスト作成期間を設けホワイトリストを作成する．ホワイトリスト作成後，ライブネット･データバスからライブパケットを取得し，②解析モジュールでスキャンと疑われるパケットか解析を行う．③解析結果，低速スキャンを検出した場合，アラートを送信する．

以下の各節で，ホワイトリストによるフィルタリング（5.2），コネクション確立失敗判定時の問題（5.3），通信シーケンスを用いた判定手法（5.4），検知処理フロー（5.5）について述べる．

5.2 ホワイトリストによるフィルタリング

ホワイトリストには，コネクション確立が成功した宛先ホスト（IP アドレス＋ポート番号）の情報を登録する．コネクション確立が成功したかどうかは，5.4 節の通信シーケンスによるコネクション確立判定の手法を用いる．登録するポート番号は，well-known ポート，及びポート番号 1024 番以上でサービス内容が確定している使用頻度の高いポートとする（cf. 4.2 節）．

宛先 IP アドレス，ポート番号がホワイトリストにあればコネクション確立成功とみなして 5.4 節で述べる判定処理は行わない．例えば，Proxy サーバの 3128 番ポートがコネクション確立成功実績があり，ホワイトリストに登録されていれば，当該ポートは待ち受け状態（LISTEN）にあるオープンポートである蓋然性が高いと考え，当該ポート宛てのパケットはコネクション確立成功としてフィルタリングする．

5.3 コネクション確立失敗判定時の問題

TCP プロトコルにおいてコネクション確立を行う場合，3 way-handshake により行われる．TCP プロトコルで通信を行う場合，最初に送信元ホストから宛先ホストの特定ポート番号へ TCP SYN パケットを送信する．宛先ポートが待ち受け状態（LISTEN）である場合，宛先ホストは TCP SYN-ACK パケットを返信する．宛先ポートが閉じている場合，宛先ホストは TCP RST-ACK パケットを返信する．したがって，コネクション確立成功、及び失敗を判定する場合，TCP SYN-ACK パケット，及び TCP RST-ACK パケットを観測することで判定することができると考えられる．

しかし，この方法で判定する場合，以下の問題がある．

1. TCP RST-ACK パケットがフィルタされ返信されない場合がある
2. 収集パケットに欠損があり返信パケットが観測できない場合がある

以下，コネクション確立判定に関する問題解決への提案を行う．

5.4 通信シーケンスを用いた判定手法

パケットが返信されることを期待してコネクション確立失敗の判定を行うと，5.3 節で述べた問題がある．解決策として、通信シーケンスを用いたコネクション確立判定を行う．3 way-handshake 時に，TCP SYN-ACK パケットが欠損する場合を例に，通信シーケンスを用いたコネクション確立判定手法を示す．

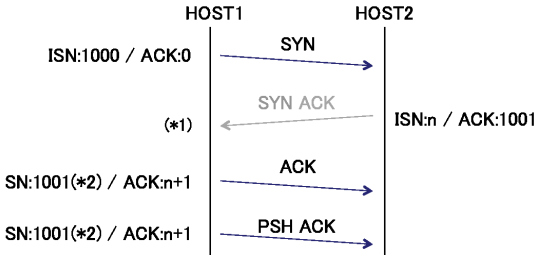

図 3: コネクション確立成功時のシーケンス

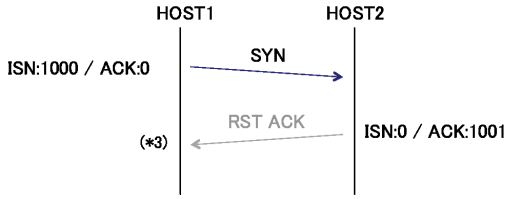

図 4: コネクション確立失敗時のシーケンス

図 3 は，HOST1 から HOST2 へ 3 way-handshake でコネクションを確立しようとして，TCP SYN-ACK パケットが欠損した場合を示している．TCP SYN パケットが，仮にシーケンス番号 1000 番で送信されると，欠損がなければ，HOST2 から TCP SYN-ACK パケットが返信されるので，この時点でコネクション確立成功である（図 3 *1）．しかし，欠損がある場合，コネクション確立判定ができない．このため，次の方法でコネクション確立判定を行う．即ち，5-tuple(送信元／宛先 IP アドレス，送信元／宛先ポート番号，プロトコル) が同一で， 且つ TCP SYN パケットのタイムスタンプを含めその時刻以降で，シーケンス番号＋ 1 の 1001 番の後続のパケットがあれば，シーケンス番号 1000 番の TCP SYN パケットに連なる通信シーケンスとみなし，コネクション確立成功と判定する（図 3 *2）．後続パケットの TCP フラグ種別は，TCP ACK，TCP PSH-ACK，TCP FIN，TCP FIN-ACK を用いた．

宛先ポートが閉じていた場合も，HOST2 からの返信パケットは参照しない．代わりに上記の判定条件に合う後続パケットを参照して，なければコネクション確立失敗とみなす（図 4 *3）．また，宛先ホストそのものが存在しない場合も，

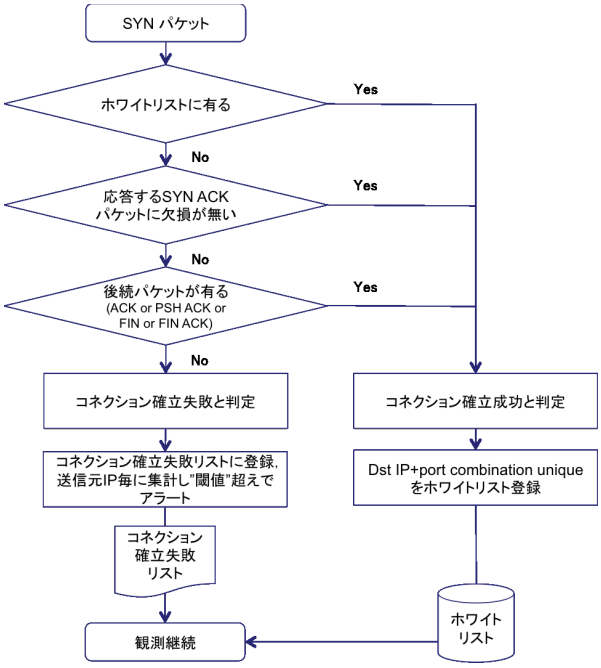

図 5: 検知処理フロー

返信パケットがないためコネクション確立失敗とみなす.

5.5 検知処理フロー

提案した検知方法について，処理フローを図 5 に示す．本研究では，図 5 の解析処理を最新 1 分間のトラフィックについて繰り返し行った．

6 実験結果と考察

6.1 観測対象ネットワーク環境

実験で使用した対象ネットワーク，観測期間，ネットワーク規模，及び観測期間 2) の観測総パケット数，及び観測トラフィック量を表 2 に示す．

6.2 実験内容

ホワイトリストを事前に観測期間 1) の期間に作成し，観測期間 2) の期間で実験を行った．実験期間中に nmap により 300 秒間隔の低速スキャンを 1 時間にわたり実行した．実行した低速スキャンの内容を表 3 に示す．

表 2: 観測ネットワーク環境

対象ネットワーク	情報通信研究機構内 のネットワークの一部
対象通信	内部ホスト間通信
観測期間	1)2014/6/24 9:00-18:00 2)2014/6/25 9:00-18:00
ネットワーク規模	/16 × 1 ブロック
観測総パケット数	(全パケット) 419,925,449 (TCP SYN) 1,318,546
観測トラフィック 量 (パケット/秒)	平均 13,155 ピーク時 68,688

表 3: 実行したスキャンの内容

スキャン時間間隔	300 秒
カテゴリ	1) ポートスキャン 2) IP アドレススキャン
スキャン種別	SYN Stealth スキャン
スキャン範囲	1) 1-65535 2) /24

6.3 実験結果

表 4 は，閾値と time window をそれぞれ変化させながら実験した結果である．表中のどの閾値と time window の組み合わせでも，nmap により実行したスキャンを検知することに成功した．表中の数値は，nmap によるスキャンデータを除外した出力アラート数，及びアラート送信元ホスト数（ユニークホスト数 : 表中括弧内）である．尚，time window が，”なし”とは，実験した 9 時間中で 1 回もクリアしていないことを意味している．

6.4 誤検知率の評価

表 4 に示す検知アラートについて，実際にスキャンが行われていたか通信内容の確認を行った．スキャンかどうかの判定は，宛先を変化させながら 10 以上のコネクション失敗が観測された時にスキャンと判定した．確認の結果，nmap によるスキャン以外の検知アラートは，全てスキャンではなかった．表 5 に，閾値が 6，time window が ” なし ” の場合の検知ホスト数を示

表 4: 実験結果

time window	閾値					
	4	5	6	7	8	9
600(秒)	76(4)	13(1)	0(0)	0(0)	0(0)	0(0)
3600(秒)	97(5)	22(1)	1(1)	0(0)	0(0)	0(0)
なし	113(10)	30(6)	4(3)	1(1)	1(1)	0(0)

表 5: 検知ホスト数

検知/非検知	スキャナ/正常ホスト		
	スキャナ	正常	計
検知	1(TP)	3(FP)	4
非検知	0(FN)	910(TN)	910
計	1	913	914

表 6: 誤検知率 (False Positive Rate):%

time window	閾値					
	4	5	6	7	8	9
600(秒)	0.4	0.1	0.0	0.0	0.0	0.0
3600(秒)	0.5	0.1	0.1	0.0	0.0	0.0
なし	1.1	0.7	0.3	0.1	0.1	0.0

す．誤検知率（False Positive Rate : FPR）は次の通りである．

$$\mathrm{FPR} = \mathrm{FP}/(\mathrm{FP}+\mathrm{TN}) = 3/913 \fallingdotseq 0.3(\%)$$

また，TP(True Positive) の 1 ホストは，実験で用いたスキャナホストである．

表 6 に，全ての組み合わせの誤検知率を示す．実験結果から，本手法を用いた場合，閾値を 10 程度に設定すれば誤検知アラートの抑止が期待できることが分かる．また，検知漏れ (False Negative:FN) については，time window が 600 秒では閾値を超過する前に失敗情報をクリアするため検知できなかったが，3600 秒以上では全て検知に成功した．

6.5 コネクション確立失敗パケット分析

図 6 に，コネクション確立失敗時の集計で，ホスト数を度数とするヒストグラムを示す（データ区間は宛先ポート数）．コネクション確立を失敗した宛先ポート数は，殆どのホストで 1〜2 ポートであることが分かる．宛先としては，共用サーバの 80 番ポートが最も多く，全体の約 60%を占めている．共用サーバの 80 番ポートへ，同様の送信元ホストから繰り返しコネクション確立試行して失敗しており，スキャンではなく送信元ホストの設定ミスと考えられる．

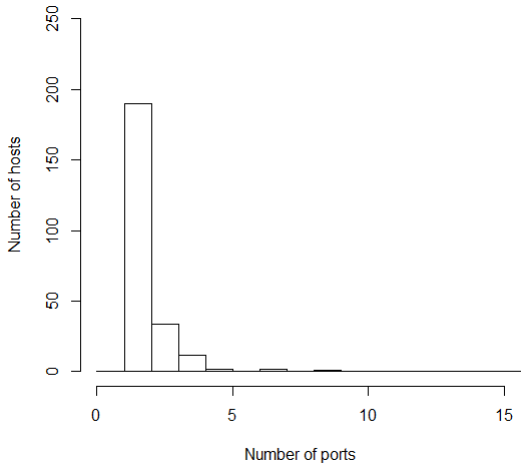

図 6: ホスト数と宛先ポート数

7 まとめと今後の課題

本稿では，標的型攻撃への対策の一つとして，ライブネットにおいて低速スキャンを検知する手法の提案を行った．また，評価実験を行い，提案手法により nmap による 300 秒間隔の TCP SYN パケットを用いた低速スキャンを，低い誤検知率，及び閾値で検知できることを示した．

今回の試みで，パケット欠損がある環境でもコネクションの確立成功数，及び失敗数を計測することが可能になった．今後の課題として，この計測データを活用し，オンラインによる観測を行い，さらに長期の低速スキャンの早期検知，及び検知精度の向上に取り組む．

参考文献

[1] 特定非営利活動法人 日本セキュリティ監査協会, “APT 対策入門　新型サイバー攻撃の検知と対応,” インプレス R&D, 2012.

[2] 独立行政法人情報処理推進機構, “標的型サイバー攻撃の事例分析と対策レポート,” http://www.ipa.go.jp/files/000024536.pdf (Visited:2014-8-20)

[3] Eric M. Hutchins, Michael J. Cloppert, Rohan M. Amin, “Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains,” International Conference on Information Warfare and Security (ICIW 2011), 2011.

[4] 武仲 正彦, 鳥居 悟, 古川 和快, 清水 聡, “ランダムで低速なポートスキャンの検知についての検討 2 ,” Symposium on Cryptography and Information Security 2013 (SCIS2013), 2013.

[5] B. Malmedal, “Using Netflows for slow portscan detection,” Master’s thesis, Gjøvik University Collage, 2005.

[6] NetFlow http://www.ietf.org/rfc/rfc3954.txt (Visited:2014-08-20)

[7] N. Kato, H. Nitou, K. Ohta, G. Mansfield, and Y. Nemoto, “A Real-Time Intrusion Detection System (IDS) for Large Scale Networks and Its Evaluations,” IEICE transactions on communications E82-B(11), 1817-1825, 1999-11-25

[8] 小原 正芳, 堀 良彰, 櫻井 幸一, “TCP に対するポートスキャンの高速検知手法,” CSEC, 2005.

[9] Roger Larsen, “Slow Port Scanning With Bro,” Master’s thesis, Gjøvik University Collage, 2013.

[10] Bro 2.3 Manual https://www.bro.org (Visited:2014-06-20)

[11] Snort Users Manual 2.9.6 http://www.snort.org (Visited:2014-06-20)

[12] Lyon, G. F. Nmap - free security scanner for network exploration & security audits. http://nmap.org (Visited:2014-06-23)

[13] 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 September/December, pp.63-79, 2011.

[14] 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.