ライブネットにおける不正通信の早期検知手法

嶌田 一郎† 津田 侑† 神薗 雅紀† 井上 大介† 中尾 康二†

†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, masaki_kamizono, dai, ko-nakao}@nict.go.jp

あらまし 標的型攻撃は，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.したがって，標的型攻撃の対策の一つとして，悪性ホストとの通信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の中から迅速に不正通信を検知する手法の一つとして，nicterのダークネット観測情報（膨大な悪性ホストのリスト）とライブネット通信をリアルタイムに照合し，不正通信検知に応用する手法を提案する.

Realtime Detection Method to Malicious Traffic in Livenet

Ichiro Shimada† Yu Tsuda† Masaki Kamizono† Daisuke Inoue† Koji Nakao†

† National Institute of Information and Communications Technology (NICT)
4-2-1, Nukui-Kitamachi, Koganei, Tokyo 184-8795, JAPAN
{i-shimada, tsuda, masaki_kamizono, dai, ko-nakao}@nict.go.jp

Abstract In targeted cyber attacks, malicious software is first used to breach into the internal network of an organization. That software then usually searches the network for valuable information and if found, transmits it to a remote server to be processed by the attacker. Therefore, it is important to detect suspicious communications with external hosts as early as possible to prevent information leakage. In this paper, we propose a method to identify such malicious traffic in "live" networks based on the observation of the traffic sent to the darknet overseen by the nicter project from NICT.

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. 文献[1]によると，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．組織内部の人物が攻撃を発見したときには，侵入されて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．

そこで本研究では，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一つの手法として，nicter が持つダークネット観測情報を利用したブラックリスト方式の不正通信検知を提案する．nicter は観測で得た膨大な量の悪性ホストをデータベース化しており，このデータベースを応用して組織内部のライブネット通信と高速に照合することで，リアルタイムな不正通信検知を実現する．

本稿では，2 章では，本研究で使用する関連技術について述べ，3 章では，ライブネットにおける不正通信の検知について述べる．そして，4 章では，提案手法について述べ，5 章では，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

情報通信研究機構が研究開発を進めている nicter[4]では，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，必然的に悪性ホスト（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[5]に蓄積される設計となっているため，本稿の提案手法では MacS DB に蓄積されたパケットデータを利用する．

2.2 ライブネット・トラフィック可視化システム NIRVANA

NIRVANA[6]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の収集，集約機能を利用し検知を行う．

3 ライブネットにおける不正通信の検知

3.1 基本方針

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照合する必要があり，照合処理の高速化を行う必要がある．

以上を踏まえ，本目的を実現するために必要となる基本要件を，次の通りとした．

・nicter におけるダークネット観測情報（膨大

な悪性ホストのリスト)をもとに，攻撃元の IP アドレスをブラックリスト IP(以下、ブラックリスト IP と記す)として不正通信を検知する.

・ダークネット観測情報には悪性ホストとの通信情報だけでなく，良性ホストとの通信情報も含まれている. そのため，不正通信の検知にあたり，良性ホストを検知しないようにブラックリスト IP を抽出し偽陽性(False Positive: 誤検知)を低減する.

・一般に，ブラックリストは過去のサイバー攻撃で使用された攻撃元情報であり，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.

・ライブネット通信パケットの収集方法として，NIRVANA 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，高速，且つ簡易な手法で検知する.

3.2 観測対象パラメータ

本研究では，TCP プロトコルによる悪性ホスト(C&C サーバ)との通信を観測対象とする.

検知処理において参照するヘッダ情報としては，送信元／宛て先 IP アドレス，送信元／宛て先ポート番号，プロトコル，TCP フラグ，シーケンス番号，確認応答番号を用いる.

3.3 システム方針

前節までに述べた目的，基本要件をもとに本システムの方針を示す.

1. 偽陽性(False Positive)を低減すること
2. リアルタイムに検知すること
3. 高速に検知すること
4. TCPのヘッダ情報だけを用いること

4 提案手法

4.1 システム概要

本研究で構築したシステムの概念図を図 1 に示す. 本システムでは，まず①Macs DB からブラックリストを作成する. ブラックリスト作成後，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解析モジュールでブラックリスト IP との照合を行う. ③照合したデータを解析した結果，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.

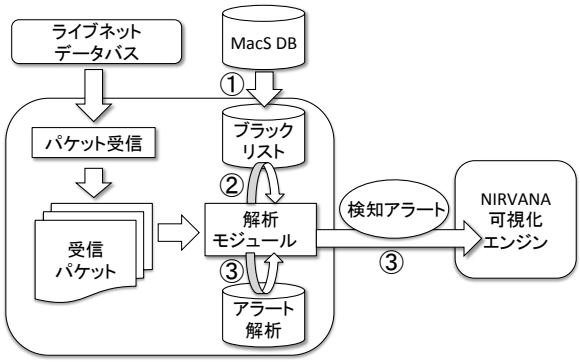

図 1 システムの概念図

以下の各節で，ブラックリストに関する事前調査(4.2)，ブラックリスト IP の作成(4.3)，ブラックリスト IP との照合処理(4.4)，セッション確立の解析とアラート送信(4.5)について述べる.

4.2 ブラックリストに関する事前調査

検知手法を検討するに当たり，nicter のダークネット観測情報を直接ブラックリストとして利用できるかどうか事前調査を行った. 事前調査で使用した観測ネットワークを表 1 に示す.

表 1 観測ネットワーク 1

対象ネットワーク	Interop2012 ShowNet[7]の一部
観測期間	2012/6/5
ネットワーク規模	/16 x 1 ブロック

表 2 犠牲ホストの通信内容の分析

外部ホストIPアドレス	SYN	ACK	SYN ACK	PSH ACK	FIN ACK	RST ACK	OTHER	IDS検知結果	SYNパケット受信時刻	MacS DB登録時刻
..18.204	1111	0	0	0	0	0	0		2012/6/5 12:40	2012/6/5 0:01
..111.9	676	0	0	0	0	0	0		2012/6/5 12:51	2012/6/5 9:25
..222.107	359	0	0	0	0	0	0	○	2012/6/5 13:04	2012/6/5 0:56
..4.31	86	0	0	0	0	0	0		2012/6/5 13:06	2012/6/5 12:03
..79.188	41	0	0	0	0	0	0		2012/6/5 13:15	2012/6/5 23:04
..148.104	352	0	0	0	0	0	0	○	2012/6/5 13:18	2012/6/5 0:53
..221.154	390	0	0	0	0	0	0	○	2012/6/5 14:45	2012/6/5 9:38
..126.90	1448	0	0	0	0	0	0	○	2012/6/5 15:49	2012/6/5 0:14
..217.215	439	0	0	0	0	0	0	○	2012/6/5 15:53	2012/6/5 3:43
..51.167	327	0	0	0	0	0	0	○	2012/6/5 16:34	2012/6/5 12:20
..34.123	317	0	0	0	0	0	0	○	2012/6/5 16:39	2012/6/5 1:41
..91.252	306	0	0	0	0	0	0	○	2012/6/5 16:41	2012/6/5 0:26
..26.231	146	0	0	0	0	0	0	○	2012/6/5 17:26	2012/6/5 3:29
..114.24	408	0	0	0	0	0	0	○	2012/6/5 17:29	2012/6/5 0:21
..22.11	402	0	0	0	0	0	0	○	2012/6/5 17:29	2012/6/5 1:01
..0.215	109	0	0	0	0	0	0	○	2012/6/5 17:33	2012/6/5 8:35
..101.22	351	0	0	0	0	0	0		2012/6/5 17:51	2012/6/5 1:26
..227.149	291	0	0	0	0	0	0		2012/6/5 18:05	2012/6/5 16:53
..201.115	24	0	0	0	0	0	0	○	2012/6/5 18:26	2012/6/5 19:45
..38.220	239	0	0	0	0	0	0	○	2012/6/5 19:08	2012/6/5 16:05
..186.233	2	0	0	1	3	40	0		2012/6/5 19:22	2012/6/5 17:03
..250.230	32	0	0	0	0	0	0	○	2012/6/5 20:25	2012/6/5 19:30
..230.240	155	0	0	0	0	0	0	○	2012/6/5 20:35	2012/6/5 16:49
..230.158	2410	0	0	0	0	0	0		2012/6/5 20:40	2012/6/5 0:18

事前調査の結果，例えばインターネット上で一般に利用されている検索ポータルサイトへの送信パケットなど良性の正常通信も検知されてしまい，False Positive が大量に発生した．この中から不審な通信を抽出するために，観測ネットワーク環境 1 で観測したインシデント事例を分析し，MacS DB 上のデータからブラックリスト IP を抽出する条件を分析した．

表 2 は，Windows XP Professional SP1 のファイアウォール機能を停止した犠牲ホストと外部ホストとの通信内容を，MacS DB のデータと突き合わせて分析したものである．表 2 の「外部ホスト IP アドレス」は，犠牲ホストと通信を行った外部ネットワーク上のホストを示す．各 TCP フラグは，外部ホストが，その TCP フラグでダークネットへ送信したパケット数（MacS DB に登録されたパケット数）を示す．「IDS 検知結果」は，アノマリベースの IDS（Intrusion Detection System）が，C&C サーバと犠牲ホストとの通信を検知した結果（検知した場合○）を示す．「SYN パケット受信時刻」は TCP SYN パケットを外部ホストから犠牲ホストが受信した時刻を示す．「Macs DB 登録時刻」は，外部ホストからの通信がダークネットで観測された時刻を示す．表 2 から，外部ホストがダークネットへパケットを送信した時の TCP フラグとして，TCP SYN パケットが特徴的であることが分かる．

また，外部ホストが IDS においても悪性ホストとして検知されていることが分かる．このことから，TCP フラグに着目し，ダークネットへ TCP SYN パケットを送信したホストを特徴抽出し，ブラックリスト IP（悪性ホスト）として定義した．

4.3 ブラックリスト IP の作成

ブラックリスト IP の作成には，MacS DB を参照する．MacS DB に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．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・テーブルに保存する．保存するデータは，送信元 IP アドレス，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 時間毎に最新のデータを MacS DB から読み込み更新する．

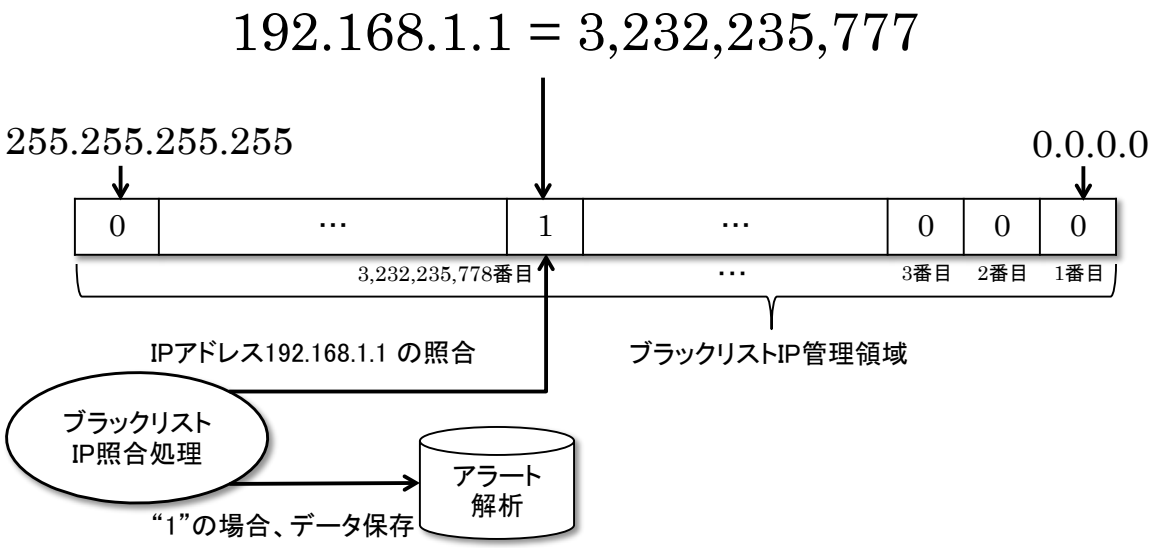

図 2 照合処理方式

4.4 ブラックリスト IP の照合処理

ライブネットを流れるTCPパケットを読み込み，送信元／宛て先 IP アドレスが，4.2 で作成したブラックリスト IP と一致するか照合する．一致した場合，送信元／宛て先 IP アドレス，送信元／宛て先ポート番号，プロトコル，TCP 種別，シーケンス番号，確認応答番号をアラート解析テーブルに保存する．

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 の増加と共に照合処理時間も増加してしまう問題がある．ブラックリストIPとの照合処理は，ライブネットの大量の通信パケットをリアルタイムに照合する必要があるため，照合するブラックリスト IP の個数に寄らず高速に行う必要がある．本研究で提案する照合処理方式を図 2 に示す．IPv4 の全 IP アドレスを 1 ビットずつブラックリスト IP 管理領域としてメモリ上に対応させ確保する．ブラックリスト IP 管理領域は，IP アドレスが”0.0.0.0”（数値：0）を先頭ビットとし，”255.255.255.255”（数値：4,294,967,295）を末尾ビットとして使用する．

図 2 の例では，”192.168.1.1”（数値：3,232,235,777）がブラックリスト IP であった場合を示しており，先頭から 3,232,235,778 番目のビットを”1”に設定している（ブラックリスト IP でない場合は”0”を設定する）．ライブネット通信パケットがブラックリスト IP か判定する場合は，先頭から 3,232,235,778 番目のビットが”1”に設定されているかどうかで判定する．ブラックリスト IP と判定した場合，アラート解析テーブルに通信データを保存する．

ブラックリスト IP 管理領域は，4.2 のブラックリスト作成処理で作成する．

4.5 セッション確立の解析とアラート送信

4.4 でアラート解析テーブルに保存されたデータをもとに，3-way handshake でブラックリスト IP とセッションを確立しているか解析する．ブラックリスト IP とセッションを確立していた場合，不審な通信として可視化エンジンにアラートを送信する．

5 実装

実装で使用した OS，ミドルウェアは以下の通りである．OS は CentOS 6.4[8]，Fedra release 16[9]，を使用した．ミドルウェアとしては，MySQL 5.5[10]をブラックリスト・テーブル，アラート解析テーブルのために使用した．

また，解析モジュールの実装で使用したハードウェアを表 3 に示す．

表 3 実装で使用したハードウェア

Model	DELL PowerEdge R610
CPU	Intel PentiumX 3.47GHz x 24 core
Memory	48GByte
NIC	BroadcomNetXtreme IITM 5709c ギガビットイーサネット NIC

表 4 観測ネットワーク 2

対象ネットワーク	Interop2013 ShowNet[11] の一部
観測期間	2013/6/14 0:00～17:00
ネットワーク規模	/16 x 1 ブロック
観測総パケット数	451,917,396
観測トラフィック量	平均 7,384 パケット/秒 ピーク時 11,552 パケット/秒

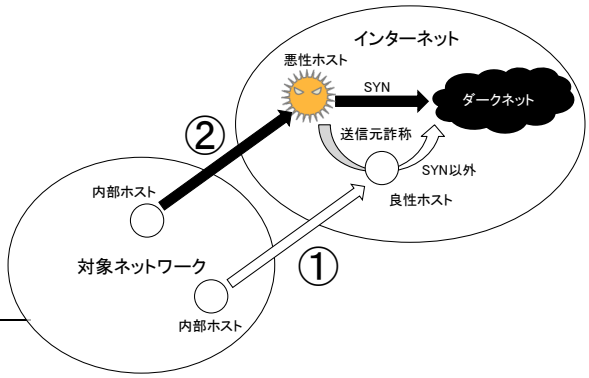

図 3 Inbound 通信

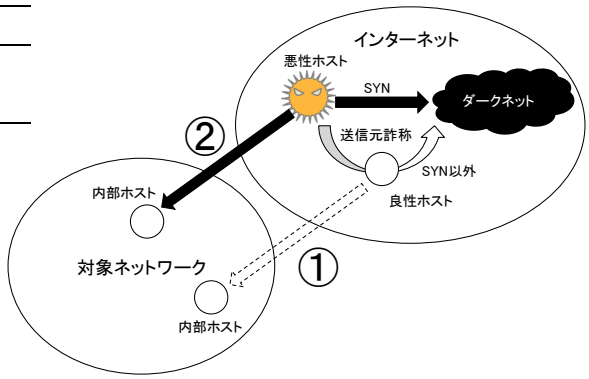

図 4 Outbound 通信

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，観測総パケット数，及び観測トラフィック量を表 4 に示す．

6.2 実験結果と考察

本節では，4 章で提案した検出手法で実験を行った結果と考察を述べる．

6.2.1 実験結果

4.2 のブラックリストに関する事前調査で抽出した条件で，観測ネットワーク 2 により実験を行った．実験結果を，ブラックリスト IP の通信状況をより明確にするために，Inbound 通信と Outbound 通信に分類した．図 3（Inbound 通信），及び図 4（Outbound 通信）に，観測ネットワーク 2 での，ブラックリスト IP の通信状況を模式的に示す．

Inbound 通信では，ブラックリスト IP ではないホストから内部ホストへの通信（①）は，観測環境では存在しなかった．①の外部ホストが良性ホストであったため，外部ホストの側からはセッション接続を行っていないものと想定される．ブラックリスト IP から内部ホストへの通信（②）は，18 セッションあった．

Outbound 通信では，殆どは内部ホストからブラックリスト IP ではないホストとの通信（①）であった．接続先の外部ホストは，一般に利用されている検索ポータルサイトなどの良性ホストであった．内部ホストからブラックリスト IP への通信（②）は，14 セッションあった．

実験結果，False Positive を低減し，ライブネット通信からブラックリスト IP との不正通信を抽出し検知することができた．

6.2.2 リアルタイム検知

表 5 に，観測ネットワーク 2 における，ブラックリスト IP からダークネット，及びライブネットへのパケット到着時刻を示す．表 5 のダークネットへのパケット到着時刻は，ライブネットへのパケット到着時刻に最も時間差が近い時刻を採取して

表 5 パケット到着時刻の比較

送信元IPアドレス（ブラックリストIP）	ライブネット		ダークネット（ブラックリスト情報）			時間差(分) A - B
	アクセス時刻(A)	宛先ポート番号	宛先ポート番号	アクセス時刻(B)	送信元国コード	
..101.86	2013/6/14 3:20	3389	3389	2013/6/14 2:56	MX	24
..240.253	2013/6/14 3:35	445	445	2013/6/14 3:20	HU	15
..30.76	2013/6/14 4:44	445	445	2013/6/14 3:48	IL	56
..63.198	2013/6/14 5:18	445	445	2013/6/14 4:57	CN	21
..123.71	2013/6/14 5:54	445	445	2013/6/14 5:39	US	15
..160.140	2013/6/14 6:05	445	445	2013/6/14 6:05	AD	0
..212.158	2013/6/14 8:01	445	445	2013/6/14 7:48	JM	13
..41.91	2013/6/14 8:02	445	445	2013/6/14 7:58	US	4
..72.115	2013/6/14 8:41	22	22	2013/6/14 8:34	GA	7
..57.108	2013/6/14 8:53	23	23	2013/6/14 8:51	GB	2
..115.29	2013/6/14 9:26	445	445	2013/6/14 9:10	US	16

いる. ブラックリスト IP からダークネットへのパケット送信と, ライブネットへのパケット送信の時間差は, 1 時間以内であった. 表 5 から, ダークネットへの攻撃パケットが観測されるのと同じタイミングで, 同じブラックリスト IP から同じポートに対して攻撃パケットが観測されている.

このことから, ダークネットで攻撃が観測されるのと同時にブラックリスト IP としてフィードバックしなければ検知できないことが分かる. このため, ダークネットで攻撃が観測されるのと同時にブラックリストに反映する仕組みの構築が必要である.

6.2.3 照合処理の高速化

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る. 実験の結果, トラフィック量で約 1000 万パケット/秒の照合が可能であることが分かった. 観測ネットワーク 2 のトラフィック量は平均 7,384 パケット/秒, ピーク時 11,552 パケット/秒であったため, 照合処理速度としては十分な性能が得られた.

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, nicter のダークネット観測情報からブラックリストを作成し, 大量のライブネット通信から不正通信を検知する手法の提案を行った. また, 評価実験を行い, 提案手法により不正通信をリアルタイム, 且つ迅速に検知できることを示した.

今後の課題として, 現在 MacS DB を一定時間毎に読み直しブラックリストを最新化している部分を, ダークネットで攻撃が観測されると同時にブラックリストに反映する仕組みを構築し, リアルタイム性の更なる向上を目指す.

さらに, 今回提案したブラックリスト方式の不正検知以外にも, スキャン検知や内部ホスト間不正通信の検知とも連携させることで, 不正通信検知の精度向上に取り組む.

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/000024429.pdf（2013 年 8 月 26 日閲覧）.

[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] Daisuke Inoue, Masashi Eto, Katsunari Yoshioka, Syunsuke Baba, Kazuya Suzuki, Junji Nakazato, Kazuhiro Ohtaka, and Koji 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.

[5] 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 September/December, pp.17 – 25, 2011.

[6] 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.

[7] INTEROP 2012
http://www.interop.jp/2012

[8] CentOS
http://www.centos.org

[9] Fedora
http://fedoraproject.org

[10] MySQL
http://www.mysql.com

[11] INTEROP 2013
http://www.interop.jp/2013