標的型サイバー攻撃における システム内部の諜報活動検知の提案

海野 由紀† 森永 正信† 山田 正弘† 鳥居 悟†

†株式会社 富士通研究所
211-8588 神奈川県川崎市中原区上小田中 4 丁目 1-1
†{yuki_m, morinaga, yamada-masahiro, torii.satoru}@jp.fujitsu.com

あらまし 近年，特定の個人，企業，官公庁をターゲットにした情報窃取型の標的型サイバー攻撃が増加している．標的型サイバー攻撃では，最初のマルウェアが内部ネットワークに侵入した後に，さまざまなマルウェアを拡散させ，目的の情報を探索する．本研究では，このシステム内部における諜報活動の検知について提案する．

Proposal for a method for detecting the intelligence activity of targeted cyber-attack in the internal system

Yuki Unno† Masanobu Morinaga† Masahiro Yamada† Satoru Torii†

†FUJITSU LABORATORIES LTD.
1-1, Kamikodanaka 4-chome, Nakahara-ku, Kawasaki 211-8588, Japan
†{yuki_m, morinaga, yamada-masahiro, torii.satoru}@jp.fujitsu.com

Abstract In recent years, targeted cyber-attacks aiming at a specific person, a company, government, and other public offices lead to theft of information have been increasing. In targeted cyber-attack the attacker spreads various malware to search objective information after the first malware invades the internal network. In this paper, we propose a method for detecting the intelligence activity in the internal system.

1. はじめに

近年，国内の重要産業や官公庁を狙った標的型サイバー攻撃があいついで発覚し，社会の注目を集めている．また，政府も企業も，危機意識を持ち始め，そのセキュリティ対策への関心が高まっている．

標的型サイバー攻撃では，ソーシャルエンジニアリングを利用して，標的型メール，USB メモリ，SNS[1]などを経由して，攻撃者が内部ネットワークへ侵入するケースが多い．ソーシャルエンジニアリングでは，人間の心理的な隙や，ミスにつけこむ手口が使われるため，メールに添付されたファイルを開くなどして，うっかりマルウェアに感染してしまう．

従来，ネットワークの入口にセキュリティ対策を施し，内部への直接侵入を防止してきた．しかし，今後は「攻撃者の侵入は避けられない．」という前提条件で，対策を施行しなければならない状況に移り変わっており，攻撃者よる内部システムでの諜報活動監視を監視する重要性が高まっている．

本稿では，2 章で，諜報活動の特徴と監視の重要性について述べる．3 章で，諜報活動の監視における既存技術の課題の考察と，研究の狙い，4 章で，諜報活動の監視方式の中心概念である「チョークポイント」と「システムふるまい

[1] Social Networking Service

解析」について述べる. そして, 5 章では, 諜報活動のチョークポイントの一つであるSMBを悪用したノード探査／リモート制御について述べ, 6 章では, ノード探査活動／リモート制御活動の検知方式について説明する. 7 章では, 提案方式のまとめと考察を, 8 章では, 今後の課題について述べる.

2. 諜報活動の特徴と監視の重要性

2.1 諜報活動の特徴

表 1 は, 文献[1]で述べられている標的型サイバー攻撃の進行について, 概要を表したものである.

表 1 攻撃フェーズと攻撃手法

フェーズ		手法
0	攻撃準備段階	標的に関係する組織を攻撃して情報収集
1	初期潜入	ソーシャルエンジニアリング 標的型メール ウィルス入り USB メモリ SNS の誘い
2	攻撃基盤構築	ドライブバイダウンロード バックドア(RAT)構築
3	諜報活動(システム調査)	ネットワーク, ホスト, アプリ情報の収集 アカウント情報の窃取 目的の情報の存在箇所の特定
4	攻撃目的の遂行	メールや Web アクセスなど通常のアクセスのふりをして, 機密情報を送出

標的型サイバー攻撃と APT[2]について考察した研究に文献[2]がある. 文献[2]で述べられているように, 情報窃取型の標的型サイバー攻撃には, ステルス性と攻撃の確度を高めて, 攻撃者のリスクを最小化するという特徴がみられる。

標的型サイバー攻撃では, 最初に内部ネットネットワークへ侵入したマルウェアが, 攻撃者の C&C サーバ[3]と通信して, 攻撃者の指示を実行する環境 RAT[4]を構築する. この RAT を介した情報の探査活動は, DoS／DDoS 攻撃などと異なり, 水面下でひっそりと行われる. 正規のプログラムになりすまし, システムに負荷をかけず, 業務通信に紛れて正常な通信と見分けがつかないようにし, 活動の痕跡を削除する. また, 大量感染ではなく, 入手した情報から標的を定め, アカウント情報を窃取して, 正当な利用者になりすます. さらに, 管理者アカウントの情報も窃取して, 高い職権を手に入れるなど, 巧妙な手口を使う.

2.2 監視の重要性

攻撃者は経済的利益を訴求しているため, 目的の情報が見つかるまで, 高度な技術で慎重かつ執拗に攻撃を続ける. そのためシステム管理者が, 内部ネットワークへ侵入されたことに気が付くまでに, 最初の侵入から, 数か月以上が経過している事例も少なくない. 出口側での対策を施していても, それを回避されて管理者が気付かないうちに, 機密情報を窃取される可能性もある. そのような事態を防ぐために, システム内部での諜報活動を迅速に検知するための監視が, より重要となってくる.

2.3 取り組みの方向性

諜報活動の迅速な検知のためには, RAT が C&C サーバからの指令を受けて, どのように情報を収集し, どのように結果を C&C サーバへ送信するかなど, 内部動作の仕組みをふまえた監視方式が必要である. 本研究では, 高度なマルウェアに侵入されたノードでは, 検知のための情報が正しく取得できない可能性があることを考慮し, ホスト型ではなく, ネットワーク型の監視方式を検討する.

3. 既存技術の課題と研究の狙い

3.1 既存技術と課題

諜報活動の監視の観点で, 既存の監視技術の特性をまとめる

1. シグネチャによる解析

予め定義されているマルウェアのシグネチャと調査対象のトラフィックを比較して検知する.

[2] Advanced Persistent Threat

[3] Command and Control サーバ

[4] Remote Access Trojan, Remote Administration Tool

代表的なツールに文献[3, 4]と文献[5, 6]がある.

誤検知が少ないという長所があるが, 亜種, 未知のマルウェア, クリプター等で処理されたマルウェアを検知できない. 諜報活動に利用されるマルウェアは, 標的の環境に適合するために, 機能が変更されたり, 検知されないための処置が施されたりするため, 検知もれが起こる可能性がある.

2. ふるまいによる解析

ウィルスやワームらしいネットワーク上のトラフィックの流れを見つける方法とネットワーク上のトラフィックからプログラムを復元し, 仮想的に実行して, マルウェアらしいふるまいをするか監視する方法とがある. 前者はワームによるポートスキャン(短時間に多くの IP にアクセス, 存在しない IP アドレス, 未使用のポートにアクセス)の検知が代表的である. 後者の代表的な研究に文献[7]がある.

クリプターなどで暗号化されたマルウェアを検知できるという長所があるが, 仮想的に実行されていることを感知して, 活動を停止するマルウェアの検知や, 時刻などの実行条件が揃わないと活動しないマルウェアの検知が難しい.

また, 検知能力と精度はふるまいの定義内容に依存する. 特定のマルウェアに特化した定義の場合, 検知できるマルウェアの種類に限界があったり, 定義が不十分な場合は, 誤検知が発生したりする.

3. プロトコルアノマリ

パケットの内容を解析して, プロトコルの仕様に違反している不正なアクセスを検知する.

システム内部の諜報活動で見られる「正常に見える通信に攻撃目的を持ったデータを紛れ込ませる偽装通信」を検知するのが難しい.

4. フロー解析

コネクション毎の流量, IP アドレスやポート番号, プロトコルの分布など, トラフィックの特徴を解析する. トラフィックの類似性を見るものに, Bot に感染しているホストと攻撃者の指令サーバ間の Bot 通信に対して, IP アドレスやペイロードの類似性を解析する研究 文献[8]がある.

DoS/DDoS 攻撃やワームのように, トラフィックが通常と大きく変化するような攻撃の検知に優れているが, 変化が現れないスローポートスキャンやピンポイントのポートスキャンの検知は難しい. 業務のトラフィックに紛れる標的型サイバー攻撃の検知も同様に難しいといえる. また, 標的型サイバー攻撃で利用される RAT の場合, 複数の RAT と C&C サーバ間で同一の指令とその実行結果がやり取りされるわけではないため, ペイロードの類似性解析による検知が難しい.

3.2 研究の狙い

以上のように, 既存の技術を諜報活動の監視に適用するにあたっては, まだ検討すべき課題が残っているといえる.

そこで, 我々は, ネットワーク型の監視方式で, ふるまいの中にみられる矛盾・異常を解析し, 以下を実現する監視方式を提案する.

1. 共通の方式で検知

異なる複数のマルウェアに共通する検知方式にし, 亜種/未知の攻撃に対応する.

2. 業務通信を偽装する攻撃の検知

業務通信に見せかけた攻撃, 正常な業務通信と区別がつかない攻撃を検知する.

3. 暗号化された攻撃の検知

暗号化されたマルウェアの攻撃や通信が暗号化された攻撃を検知できる.

4. 監視方式の中心概念

4.1 チョークポイント

標的型サイバー攻撃に使われるマルウェアの種類はさまざまである. 標的の環境で, 確実に実行されるよう, あるいは, アンチウィルスソフト, IDS[5]/IPS[6]に検知されないようなカスタマイズが, マルウェアに加えられるからである.

---

[5] Intrusion Detection System

[6] Intrusion Prevention System

しかしながら，マルウェアの種類が異なっていても，攻撃者が使わざるを得ない／内部的に共通して使われている攻撃手法が存在する．本稿では，この攻撃者が使わざるを得ない共通の攻撃手法をチョークポイントと呼ぶ．

4.2 チョークポイントによるシステムのふるまい解析

RAT のトンネル通信など，あるセッション上のパケットをプロトコル仕様の観点で解析しても違反は見つからず，複数のパケット，セッションを解析しなければ，異常が見つからない場合がある．そのような場合は，単一のふるまいで見るのではなく，横通しの通信，前後の通信などを解析するなどしてシステムのふるまいを見る．単一のふるまいでは正常に見える通信であっても，システムの全体のふるまいとしては，矛盾・異常が見つかる．そうすることで，攻撃されている可能性を見つけることができる．

その反面，システムのふるまいは千差万別である．そこで，我々はチョークポイントを捉えて，システムのふるまいに矛盾・異常がないか解析する．

5. 諜報活動のチョークポイント

5.1 諜報活動のシナリオ

諜報活動では，目的の情報の存在箇所を特定するために，ネットワーク／ホスト／アプリ情報の収集，アカウント情報の窃取などを行い，攻撃基盤を拡大していく．このうち，アカウント情報の窃取は，直接的に正当な利用者になりすまして侵入できる上に，管理者アカウントが窃取できた場合には，システムを制御することができるため，攻撃者にとって有用である．

アカウント情報の窃取によるシステム侵入は，キーロガー，画面キャプチャ，パケットキャプチャなどのツールを使う受動的な方法と，NTLM[7]／NTLMv2 認証，SMB[8]を悪用したツールを使う能動的な方法がある．最近では，後者の攻撃手法を使った事例として，アカウントサーバである Active Directory[9] が狙われたケースも複数見つかっている．攻撃基盤を拡大する過程における，SMB を悪用して次の標的を探すノード探査や，標的のノードのリモート制御は，攻撃者が使わざるを得ない共通の攻撃手法であり，「チョークポイント」の一つである．

なお，次節以降では，攻撃基盤拡大のためのノード探査／リモート制御について理解を深めるため，NTLM／NTLMv2 認証と SMB 悪用の概要について述べる．

5.2 NTLM／NTLMv2 認証

NTLM／NTLMv2 認証は Windows NT 4.0 Server[10]以前の OS で使われていたネットワークログオンのための認証方式である．それ以前の LM 認証と同じように，パスワードの受け渡しにチャレンジ／レスポンス方式を使っており，レスポンスはパスワードハッシュを用いて作成される．

Windows 2000 Server 以降では，デフォルトで Kerberos[11]認証がサポートされたが，互換性を保つために，現在でも NTLM／NTLMv2 認証が利用できる．そのため，Kerberos 認証が使えないクライアントからアクセスする場合は NTLM／NTLMv2 認証が使われる．また，Kerberos 認証が使えるクライアントであっても，同一ドメインに参加していない場合は NTLM／NTLMv2 認証を使う．

以上の背景により，現在でも NTLM／NTLMv2 認証が使われているのである．

---

[7] NT LAN Manager

[8] Server Message Block

[9] Active Directory は米国 Microsoft Corporation の米国およびその他の国における登録商標です

[10] Windows は米国 Microsoft Corporation の米国およびその他の国における登録商標です

[11] Kerberos は Massachusetts Institute of Technology の商標です

5.3 SMB の悪用

SMB は Windows が，ネットワーク上で，ファイルやプリンタを共有する際に利用するプロトコルであり，認証に NTLM／NTLMv2 認証が使われている．

1997 年に，Paul Ashton が pass-the-hash 攻撃について，NTBugtraq[12]に投稿した．攻撃者はパスワードを知らなくても，パスワードハッシュを利用して，SMB でリモートサーバ／サービスの認証を受けることができるという攻撃である．

この投稿以降，文献[9]，文献[10]で紹介されているように，pass-the-hash 攻撃を行うさまざまなツール，マルウェアが作られてきた．現在では，攻撃に必要なパスワードハッシュを取得できるツール／マルウェアや，標的を定めるために Windows バージョンを調査するためのツール／マルウェア，SMB の認証を利用してログインを試行するツール／マルウェアなどが揃っており，攻撃者が簡単に pass-the-hash 攻撃を行うことができる状態になっている．

6. SMB を悪用したノード探査／リモート制御の検知方式

SMB を悪用して，最初に侵入したホストから，次の標的を探す活動「ノード探査」と，次の標的に侵入して情報を窃取する活動「リモート制御」の検知方式について説明する．

6.1 ノード探査の検知

本稿では，次の標的を定めるために，対象の Windows を調べることを「Windows バージョンスキャン」，SMB の認証を利用してログイン試行することを「SMB ログインスキャン」と呼び，これらを総称して「SMB スキャン」と呼ぶ．

この SMB スキャンを捉えて，横通しでシステム全体の SMB 認証の矛盾／異常を解析し，ノード探査活動を検知する．

6.1.1. ノード探査の検知における課題

SMB によるノード探査の検知には，大きく二つの技術的な課題がある．一つ目は，SMB アクセスを許可されたサーバと禁止されたサーバとでは，SMB ログインスキャンとみなすための条件が異なり，両者において正しく検知するのが難しいことである．禁止されたサーバでは SMB 認証リクエストを受けること自体が異常であるが，許可されたサーバでは正常である．許可されたサーバでは，認証エラーが多発しているなど，禁止サーバとは別の条件での検知が必要である．また，同じサーバであっても，クライアントによって許可されるのか禁止されるのかが変わってしまうことも検知を難しくする．

二つ目は，Windows バージョンスキャンを実行したとき，サーバ上では認証エラーが発生しないため検知されににくく，正当な認証と区別がしにくいという課題がある．SMB ログインスキャンにおいても，同様の問題が発生する場合がある．

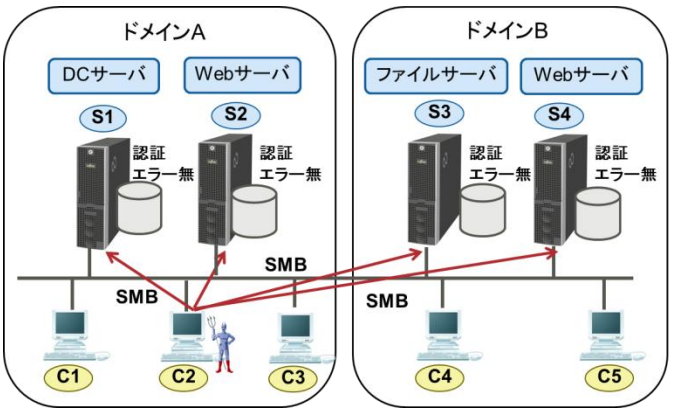

図 1 Windows バージョンスキャン

6.1.2. ホワイトリストと連動した判定

一つ目の課題に対しては，SMB アクセスを許可するサーバ／クライアントの組み合わせをホワイトリストに登録し，このホワイトリストと連動した条件で判定を行う．

[12] 1997年にRuss Cooper氏が創設したメーリングリスト.Windows NTとBackOfficeのセキュリティ攻略とバグを検討する

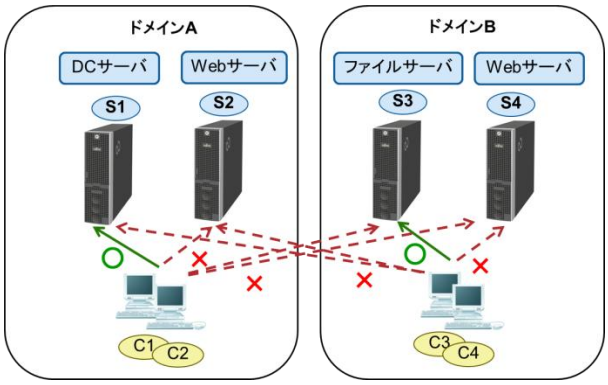

図 2　SMB アクセスルール

ホワイトリストに未登録のサーバ／クライアントの場合，SMB 認証が発生した時点で異常とみなし，ホワイトリストに登録されているサーバ／クライアントの場合，認証エラーの多発など，別の条件で異常とみなす．

6.1.3.　SMB 認証アカウントによる判定

二つ目の課題に対しては SMB 認証のアカウントを見て，正常か異常かの判定を行う．Windows バージョンスキャンにおいては，図 3 のようなシーケンスで認証が行われている．正当なアカウントが指定されている場合は，そのアカウントで認証されるが，アカウントを指定していない場合は，Guest として認証される[13]．

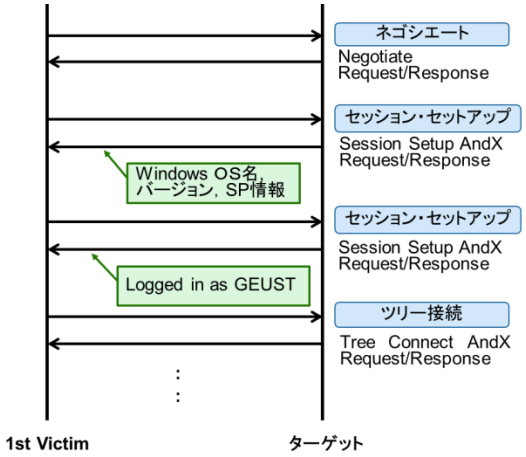

図 3　認証シーケンス（アカウント未指定）

SMB ログインスキャンの場合は，スキャン時に指定したアカウント情報（ID，パスワードハッシュ，ドメイン）で NTLM／NTLMv2 認証のリクエストを送信する．正しいアカウント情報を指定した場合，そのアカウントで認証されるが，誤ったパスワードを指定すると認証されず，ターゲットのサーバのログに認証エラーが出力される．存在しないアカウント情報を指定した場合は，バージョンスキャンと同様に，Guest として認証されるため，ターゲットのサーバのログファイルに認証エラーが残らない．

このアカウント未指定，誤ったアカウントを指定したときに Guest として認証された状態を見つけることで，認証エラーが発生しない場合でも，正常なアクセスと攻撃によるアクセスの区別を行うことができる．表 2 に図 2 の場合の，SMB 認証のシステムふるまいをまとめる．

表 2　SMB 認証におけるシステムふるまい

Dest	S1		S2	S3		S4
Src	C1 C2	C3 C4	C1 C2 C3 C4	C1 C2	C3 C4	C1 C2 C3 C4
SMB アクセス	許可	禁止	禁止	禁止	許可	禁止
認証エラーn 回/サーバ以上	異常	―	―	―	異常	―
指定したアカウントで認証	正常	―	―	―	正常	―
Guest 認証	異常	―	―	―	異常	―

上記のシステムふるまいと，実際のネットワークデータが矛盾した場合に，ノード探査が行われたと検知する．

6.2　リモート制御の検知

次の標的への exploit の転送／実行に利用される SMB 通信（シグナリング）を捉え，その後に続くリモート制御のためのリバースコネクションとの関連を解析することで，システムの異常を見つけ，リモート制御活動を検知する．

6.2.1.　リモート制御の検知における課題

1st Victim で窃取したアカウント情報（ユーザ ID，パスワードハッシュ）を指定して SMB 認

[13] Windows XP，Windows 2003 Server で検証

証を行い，ターゲット（2nd Victim）に侵入するが，正当な操作によるネットワークログオンの認証なのか，攻撃による認証なのか区別がつかないという課題がある．

また，SMB シグナリングとリバースコネクションの関連性を解析する際には，ファイル共有の正当な操作による SMB 通信と攻撃による SMB 通信との区別が難しいという課題がある．

6.2.2. SMB シグナリングとリバースコネクションの紐づけによる判定

図 4 は，SMB を利用して，1st Victim から 2nd Victim を exploit した様子を図に示したものである．

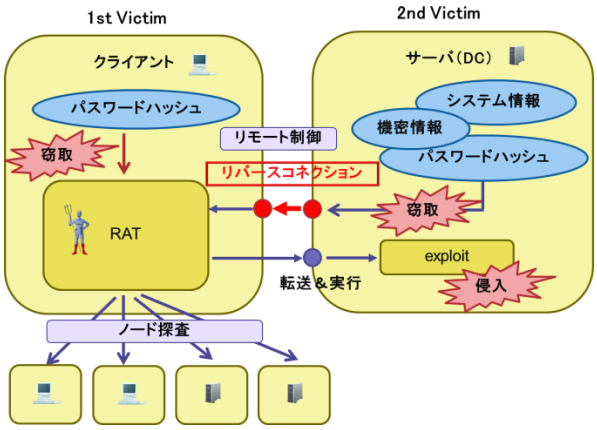

図 4 2nd Victim の exploit

SMB で 2nd Victim のサーバに侵入して，リモートから制御するまでの，想定される攻撃のシーケンスを以下にしめす．

1. 1st Victim 上で盗んだアカウント情報（ユーザ ID とパスワードハッシュ）を利用して，1st Victim のクライアントから 2nd Victim のサーバに対してアクセスする．
2. 1st Victim から 2nd Victim に，exploit を転送する．
3. 転送した exploit を，2nd Victim のサーバのサービスとして登録する．
4. 3 のサービスを実行する
5. 2nd Victim から 1st Victim にリバースコネクションがはられる．
6. 3 で登録したサービスを削除する．
7. 4 のリバースコネクションを使って，2nd Victim の情報を収集する．

リバースコネクションが正当な操作によるコネクションではなく，攻撃活動によるリモート制御のためのコネクションであることを判定するために，このシーケンスを解析して，シグナリングの SMB とリバースコネクションとの紐づけを行う．

まず，SMB リクエストと逆方向（2nd Victim→1st Victim）のコネクションの TCP 3 ウェイ・ハンドシェイクを見つける．この時点では，誤検知が多発する可能性が高く，まだリモート制御のリバースコネクションと判断できない．

そこで，直前に受信した SMB のヘッダなどを見て，シグナリングであるかを解析する．図 5 は，シグナリングが SMB である場合の関連付けを表した図である．

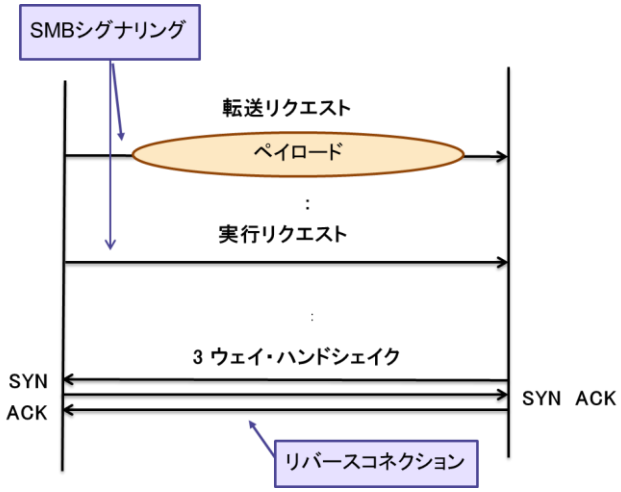

図 5 SMB シグナリングとリバースコネクション

実行可能形式の転送リクエストが存在するか，リモート実行のリクエストが存在するかを調べ，存在する場合は，シグナリングとリバースコネクションとを紐づける．

7. まとめと考察

諜報活動の特徴に着目した場合の各方式の適性については，これまで述べてきたが，表 3 にまとめる．

表 3 諜報活動の監視における比較

	方式				
	シグネチャ	ふるまい(単一)	プロトコルアノマリ	フロー	提案方式
検知方式の共通化		△	△		○
業務通信の偽装への対応	△	△	△		○
暗号化への対応		△			○

本方式の特長は以下である.

1. 共通の攻撃手法「チョークポイント」を捉えることで, 正規のプログラムになりすます攻撃も検知できる.
2. システムのふるまいを解析するため, リソースに負荷をかけない攻撃や業務通信に紛れる攻撃を検知できる.
3. 亜種, 未知のマルウェア, 難読化されたマルウェアの活動の検知に適している.

また, 提案方式により, 諜報活動において, 「アカウント情報を窃取されて, システムに侵入される. 」「管理者アカウントが窃取されて, システムを制御される. 」という, システムが危険な状態であることを監視できる効果は大きい.

8. 今後の課題

今後はさまざまなマルウェアを動作させた実験環境で, 提案方式の有効性(検知率, リアルタイム性など)について評価し, 検知方式の改善, 拡充を行っていく.

参考文献

[1] 「標的型サイバー攻撃の事例分析と対策レポート」, 独立行政法人情報処理推進機構, http://www.ipa.go.jp/security/fy23/reports/measures/documents/report20120120.pdf

[2] 二木, 佐藤, 山崎, 内. 標的型サイバー攻撃と APT に関する考察, Vol.2012-CSEC-56 No.20

[3] Snort, http://www.snort.org/

[4] M.Roesch , Snort – Lightweight Intrusion Detection for Network , In Proceedings of The 13th USENIX Conference on System Administration , pp.229-238, 1999

[5] The Bro Network Security Monitor, http://bro-ids.org/

[6] V.Paxon, Bro: A System for Detecting Network Intruders in Real-Time , Computer Networks: The International Journal of Computer and Telecommunications Networking, vol.31, no.23-24, pp.2435-2463, 1999

[7] Helen J. Wang , Chuanxiong Guo , Daniel R. Simon and Alf Zugenmaier , Shield: Vulnerability-driven Network Filters for Preventing Known Vulnerability Exploits, In ACM Siggcomm, pp.193-204, 2004

[8] Michael K. Reiter, Ting-Fang Yen, Traffic Aggregation for Malware Detection, In Proceedings of The 5th International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment

[9] SANS Institute InfoSec Reading Room, Pass-the-hash attacks: Tools and Mitigation , January 21st 2010 , Bashar Ewaida , http://www.sans.org/reading_room/whitepapers/testing/pass-the-hash-attacks-tools-mitigation_33283

[10]MANDIANT , M Trends 2012; An Evolving Threat https://www.blackhat.com/html/bh-us-12/bh-us-12-archives.htm