JPCERT CC®

「マルウェアの最近の傾向と
ウェブアプリケーションの脆弱性を狙うボットの実態」
調査レポート

有限責任中間法人 JPCERT コーディネーションセンター

平成 19 年 6 月 21 日

JPCERT CC®

目次

本レポートの一部は、悪用されることを回避する目的で公開を差し控えています。

1. はじめに(背景)

昨今、コンピュータネットワークにおけるボット及びボットネットの脅威が深刻な問題ととらえられてきた。JPCERT/CC では、2004 年よりボットの脅威に着目し、過去 2 回にわたってその脅威、実態についての調査を行い、ボットが DoS 攻撃機能、スパムメール不正中継機能、バックドア機能など多くの機能を実装し、また様々な金銭詐取の道具として悪用されていることをつきとめた[1]。また、調査の中でボットの原型のひとつに Sobig.F というコンピュータウイルスが存在していたことが判明しており[2]、この Sobig.F は、メールの添付ファイルを媒介として感染し、かつ以下の 2 種の主機能を併せ持つものであった。

(ア) スパム送信を目的としたプロキシ機能
(イ) 特定 URL に接続して自己更新を実施する機能

これら調査結果をふまえ、マルウェアの一類型として(ア)のスパム送信機能を強化し、かつ外部からの操作性を向上させた高機能なプログラムが「ボット」であると定義づけられた[3]。そして、ボットによって構成されるボットネットが、無差別に広範な被害を及ぼしかねないことに関しても調査研究が行われており、喫緊の対策が望まれている[4]。
一方、昨今ではこのような高機能なボットの存在とは別に、単機能、または最低限必要な機能のみを実装したマルウェアが増加傾向にあるという報告もあり[5]、マルウェアの実態が新たなステージに移行しているという懸念もある。特に(イ)の機能に特化したウイルスの存在についての調査が国内で行われたという報告はなく、「DOWNLOADER」と呼ばれる特定 URL に接続して別のマルウェア単体、または複数をダウンロードし、感染させるタイプについての知見の集積はないと考えられる。
このような背景から、本調査ではボットの実態の継続調査に加え、単機能化されたマルウェアに焦点をあて、これら機能を限定したマルウェアが作成された目的や、その特徴などについて調査を行い、それらが使用されはじめた背景や対策などについて考察する。

---

1 JPCERT/CC 「ボットネットの概要」
http://www.jpcert.or.jp/research/2006/Botnet_summary_0720.pdf
2 日経 ITPro「ネットの脅威「ボット」の実態をつかめ！」
http://itpro.nikkeibp.co.jp/article/OPINION/20050831/220371/
3 サイバークリーンセンター「ボットについて」
https://www.ccc.go.jp/bot/index.html
4 日経 ITPro 『「ボットネットを“飼って”みました」, Telecom-ISAC Japan)』
http://itpro.nikkeibp.co.jp/article/NEWS/20060426/236401/
5 IT セキュリティのアライ出し 第 19 回 2006 年を振り返る
http://journal.mycom.co.jp/column/itsecurity/019/

2. 調査概要

本調査では、以下の 3 つのテーマについて調査を行う。
また、調査を実施するにあたってウイルスの発生動向、脆弱性、攻撃情報などの分析にインターネットセキュリティシステムズ株式会社（以下、ISS)、トレンドマイクロ株式会社(以下、トレンドマイクロ)、米マイクロソフト(以下、マイクロソフト)、株式会社ラック(以下、ラック)の情報を利用させていただいた。

① Web アプリケーションの脆弱性を使用するボットに関する調査
従来、OS の脆弱性を悪用することでボットはその勢力を拡大させていった。一方、国内では SQL インジェクション等の Web アプリケーションに関連した脆弱性に関する届出数が、ソフトウェア製品の届出を上回っているという報告[6]があり、Web アプリケーションの脆弱性を悪用するモジュールをボットが実装するようになっていることが懸念される。このような懸念点から、以下の調査を行う。

- ボットが使用する Web アプリケーションの脆弱性
- Web アプリケーションの脆弱性を使用するボットの機能

② 2005 年から 2006 年にかけてのウイルス発生動向
ボットを含む広義のウイルスの実態を把握するために、トレンドマイクロのパターンファイル（以降、特に明記がない限りトレンドマイクロのパターンファイルを指す）に登録されているウイルス情報から、2005 年～2006 年にかけてのウイルス亜種発生動向の調査を行う。また、トレンドマイクロのウイルス感染被害レポートやマイクロソフトによるレポート、ニュースサイトの報道などの関連情報も参考に調査を行う。

- オンラインゲームのアカウントを盗むウイルス
- ネットバンクのアカウントを盗むウイルス
- インスタントメッセンジャーのアカウントを盗むウイルス

---

[6] IPA「最近の脆弱性関連情報の届出事例とその対策方法」
http://www.ipa.go.jp/security/vuln/event/documents/20060228_1.pdf

③ DOWNLOADER の調査

DOWNLOADER と呼ばれる特定 URL に接続して別のマルウェアをダウンロードし、感染させるウイルスの実態を把握するため、パターンファイルおよび同社のウイルスデータベース（以降、特に明記がない限りトレンドマイクロ社のウイルスデータベースとは指す）に登録されているウイルス情報を用いて、その種類や機能、使用する脆弱性の調査を行う。また、ニュースサイトの報道などの関連情報も参考に調査を行う。

- DOWNLOADER の種類
- DOWNLOADER の機能
- DOWNLOADER が使用する脆弱性

3. 調査結果

3.1. Web アプリケーションの脆弱性を使用するボットの調査

3.1.1. ボットが使用する Web アプリケーションの脆弱性

国内における脆弱性を使用したインターネット経由の攻撃の実態を明らかにするには、より広域の統計情報を分析することが望ましい。そこで、ISS が所有する国内のセキュリティオペレーションセンター(SOC[7]：Security Operation Center)の IDS・IPS で収集された攻撃トラフィックデータの調査を行い、ボットによるものと想定される攻撃トラフィックを浮き彫りにし、そのトラフィックデータと既知のウイルスの関連性を、ウイルスデータベース[8]に登録されているウイルス情報を用いて分析を行った。また、ラックの所有する SOC のレポートやインターネット上に公開されているニュースリソースなどの関連情報も参考に調査を行った。

---

[7] ネットワークシステムのセキュリティを監視・管理する施設
[8] トレンドマイクロ ウイルスデータベース
http://www.trendmicro.co.jp/vinfo/virusencyclo/default.asp

図 3-1 は、ISS の SOC において、2005 年 1 月 1 日から 2006 年 12 月 31 日の間に IDS・IPS で収集されたデータから、ボットによる攻撃と思われるものを抽出し、攻撃に使用された脆弱性の割合を示したものである。この図からボットが感染活動に使用する脆弱性の種類の推移を確認することができる。

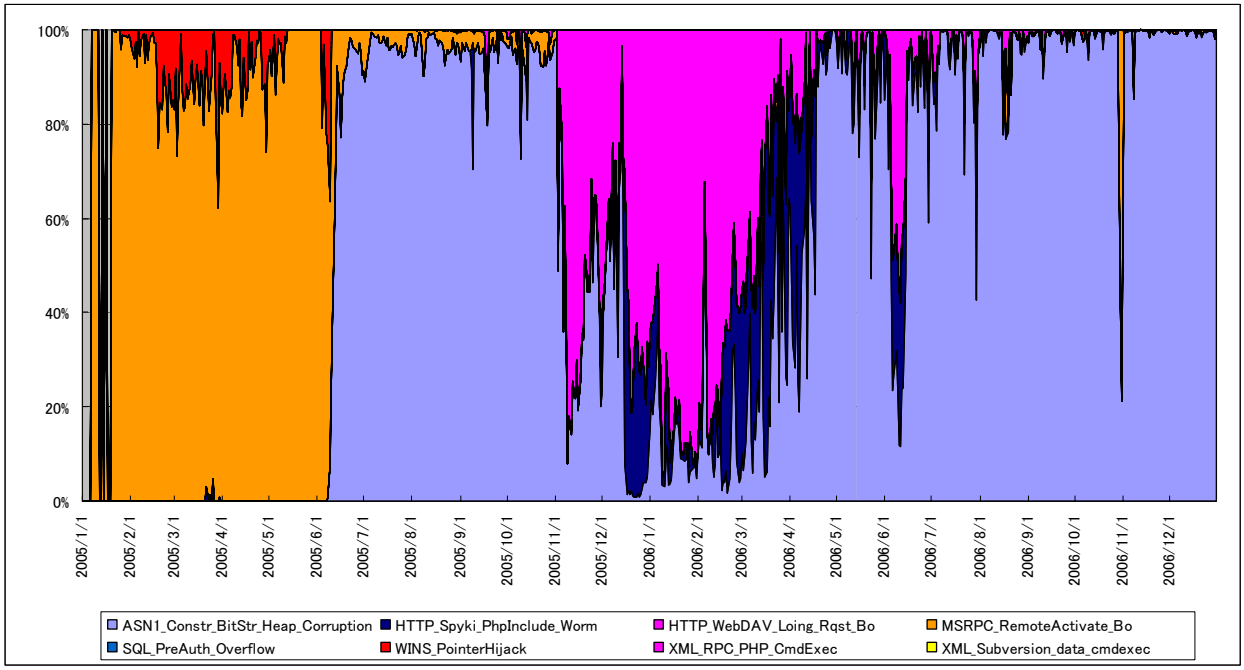

図 3-1　ボットが感染拡大に使用する脆弱性の推移

2005 年 1 月 20 日頃から同年 6 月 8 日までは RPCSS サービスの脆弱性(MS03-039) [9]に対する攻撃が多く、6 月 8 日以降は ASN.1 の脆弱性（MS04-007) [10]に対する攻撃が大半を占めている。これらは共に Windows の脆弱性である。

---

[9] RPCSS サービスのバッファ オーバーランによりコードが実行される（MS03-039）
http://www.microsoft.com/japan/technet/security/bulletin/MS03-039.mspx

[10] ASN.1 の脆弱性により、コードが実行される（MS04-007）
http://www.microsoft.com/japan/technet/security/bulletin/ms04-007.mspx

Web アプリケーションの脆弱性を使用するボットの感染活動として、2005 年の 9 月 8 日から 9 日にかけて主に韓国で利用されている掲示板プログラム「Zeroboard」の脆弱性に対する攻撃が確認された[11]。その後、2005 年 11 月 8 日頃、アクセスログ解析プログラム「AWStats」の脆弱性や PHP で作成された XML-RPC ライブラリ「XML-RPC for PHP」および「PEAR XML-RPC」の脆弱性に対する攻撃が大量に確認された[12]。XML-RPC ライブラリは、広く使われている CMS(Content Management System:コンテンツマネジメントシステム)の「XOOPS」のほか、PHP で開発された複数の Web アプリケーションに使用されていたため、脆弱性の影響が大きかった[13]。XML-RPC ライブラリの脆弱性への攻撃は、2006 年 3 月までボットによる Web アプリケーションに対する攻撃の大半を占めている(図 3-1: 桃色の部分 XML_RPC_PHP_ CmdExec)。

図 3-2 は、2005 年 11 月以降に ISS の SOC で観測された Web アプリケーションの脆弱性に対する主要な攻撃について、攻撃元 IP アドレス数の推移を示したものである。

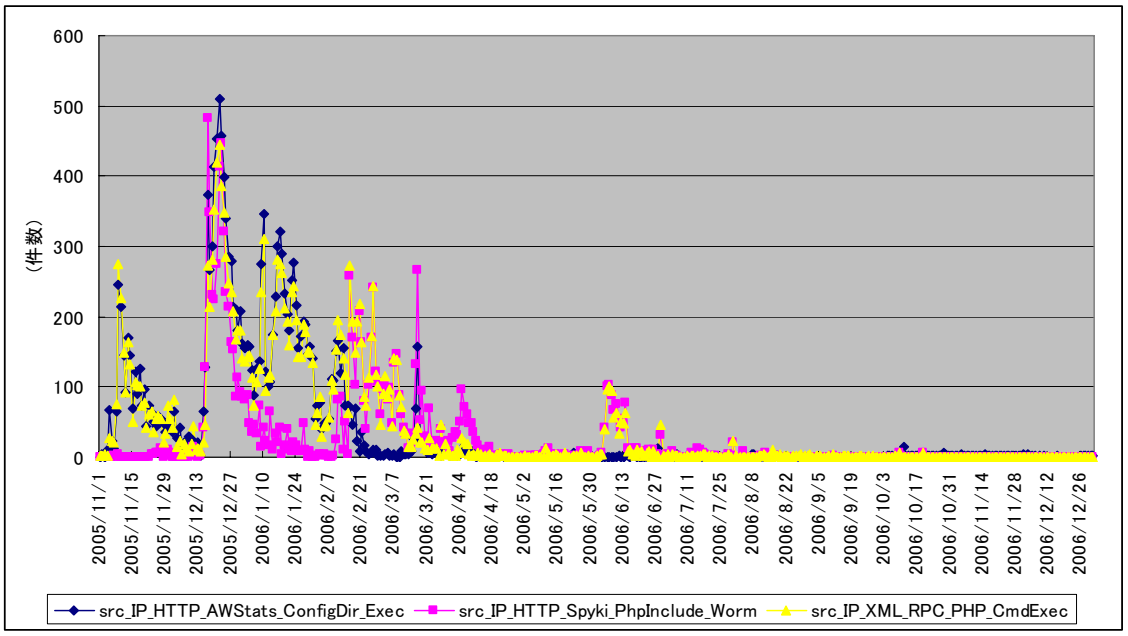

図 3-2　攻撃元 IP アドレス数の推移

---

[11] 9 月 8 日、9 日の 2 日間のみ検知され、ISS は短期的に特定の国を対象とした攻撃と分析
http://internet.watch.impress.co.jp/cda/event/2005/12/09/10168.html

[12] XML_RPC_PHP_CmdExec / HTTP_AWStats_ConfigDir_Exec の検知について
http://www.isskk.co.jp/security_center/xml_rpc.html

[13] Web サイトの管理者は要注意, PHP アプリ用ライブラリの脆弱性を突くコードが出回る
http://itpro.nikkeibp.co.jp/free/ITPro/NEWS/20050708/164223/

この図から、AWStats の脆弱性に対する攻撃と XML-RPC ライブラリの脆弱性に対する攻撃は、11 月 8 日に確認されてから 12 月上旬にかけて一時的に減少傾向が見られた後、12 月 13 日頃に急増している（図 3-2src_IP_HTTP_AWStats_ConfigDir_Exec、src_IP_XML_RPC_PHP_CmdExec)。11 月の攻撃は、Lupper ワーム(別称 Lupii、Plupii)によるものと推測される[14]。図 3-3 は、ラックが所有する SOC である JSOC での Lupper ワームによる攻撃検知数の推移を示したものである。JSOC でも、同様の傾向が観測されており、亜種が出現したと推測される[15]。

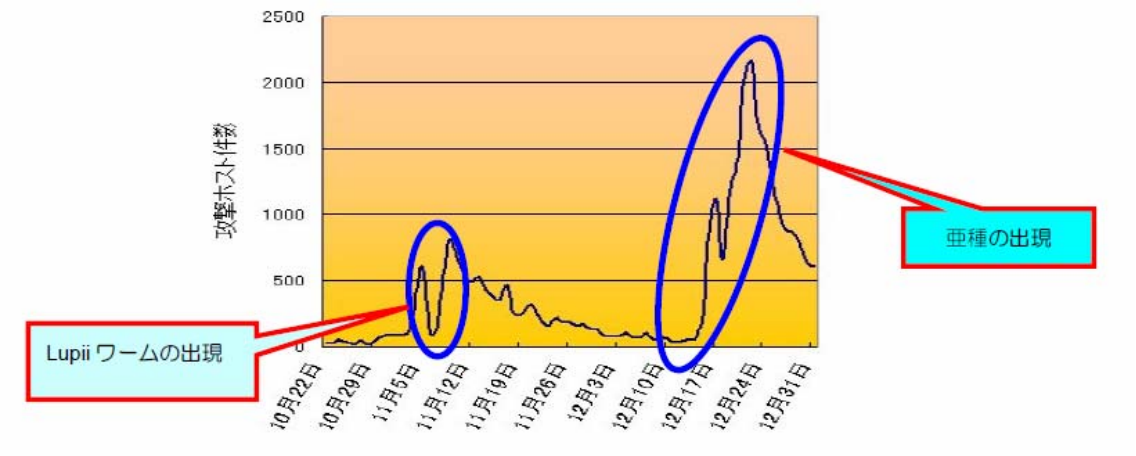

図 3-3　JSOC で検知した Lupper ワームによる攻撃件数の推移

図 3-2 において、亜種が出現したと考えられる 12 月中旬に着目すると AWStats および XML-RPC ライブラリの脆弱性に対する攻撃の急増と同時に、PHP で開発された多数の Web アプリケーションに発見されている Remote File Include(以下、RFI)の脆弱性への攻撃も急増している(src_IP_HTTP_Spyki_PhpInclude_Worm)。脆弱性に対する攻撃の増加は図 3-1 からも確認できる（図 3-1:紺色の部分 HTTP_Spyki_PhpInclude_Worm)。2004 年に発見された SANTY ワームは、掲示板システム「phpBB」に存在した RFI の脆弱性を使用して感染活動を行うものであった。また、その亜種にはボットが存在する[16]。このことをふまえ、2005 年 12 月中旬に AWStats や XML-RPC ライブラリの脆弱性と RFI の脆弱性を使用して感染活動を行うボットが出現した可能性が考えられる。

---

[14] Linux を狙うワーム「Lupper」，アンチウイルス・ベンダー各社が警告
http://itpro.nikkeibp.co.jp/article/USNEWS/20051109/224243/

[15] JSOC 侵入傾向分析レポート Vol.6(ラック)
http://www.lac.co.jp/business/sns/intelligence/report/20060614_lac_report.pdf

[16] PERL_SANTY.F (トレンドマイクロ)
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=PERL%5FSANTY%2EF&VSect=T

表 3-1 は、2005 年以降にパターンファイルに登録されたウイルスのうち、ELF 形式(UNIX・LINUX などの実行可能形式)で、かつ脆弱性を使用するものについて、発見日および使用する脆弱性を調査したものである。

表 3-1　脆弱性を使用する ELF 形式のウイルス

発見日	ウイルス名	利用する脆弱性
2005/8/14	ELF_SSHSCAN.A	OpenSSHの脆弱性
2005/11/5	ELF_SSHD22.B	SSH1のCRC32攻撃検知コードの脆弱性
2005/11/6	ELF_LUPPER.A	XML-RPCライブラリの脆弱性 AWStatsの脆弱性 Webhintsの脆弱性
2005/11/8	ELF_LUPPER.B	XML-RPCライブラリの脆弱性 AWStatsの脆弱性
2005/11/16	ELF_LUPPER.C	XML-RPCライブラリの脆弱性 AWStatsの脆弱性
2005/12/13	ELF_SMALL.AYW	SolarisのKernelにおける脆弱性
2005/12/14	ELF_SMALL.AYY	SolarisのKernelにおける脆弱性
2005/12/21	ELF_KAIGENT.A	MamboにおけるRFIの脆弱性
2005/12/21	ELF_KAIGENT.B	AWStatsの脆弱性 MamboにおけるRFIの脆弱性
2005/12/21	ELF_KAIGENT.C	PHP-NukeにおけるRFIの脆弱性
2006/1/24	ELF_KAITEN.U	MamboにおけるRFIの脆弱性
2006/2/15	ELF_LUPPER.F	XML-RPCライブラリの脆弱性 AWStatsの脆弱性
2006/2/18	ELF_MARE.C	XML-RPCライブラリの脆弱性 MamboにおけるRFIの脆弱性
2006/2/25	ELF_MARE.E	XML-RPCライブラリの脆弱性
2006/3/4	ELF_MARE.G	XML-RPCライブラリの脆弱性
2006/3/6	ELF_MARE.J	XML-RPCライブラリの脆弱性 MamboにおけるRFIの脆弱性
2006/3/14	ELF_MARE.K	XML-RPCライブラリの脆弱性 MamboにおけるRFIの脆弱性
2006/3/16	ELF_LUPPER.H	WebCalendarにおけるRFIの脆弱性 PHP-NukeにおけるRFIの脆弱性
2006/4/1	ELF_KAITEN.AM	MamboにおけるRFIの脆弱性
2006/6/4	ELF_KAITEN.AQ	MamboにおけるRFIの脆弱性

これらのウイルスは、亜種をまとめて分類すると 7 種類になり、その半数以上である 4 種類「LUPPER」、「KAIGENT」、「KAITEN」、「MARE」が Web アプリケーションの脆弱性を使用するウイルスであった。これらのウイルスが使用する共通の脆弱性は、ISS の SOC でも多数検知されている PHP の XML-RPC ライブラリの脆弱性と CMS「Mambo」の RFI の脆弱性である。また、この 4 種類のウイルスのうち KAITEN 以外が複数の脆弱性を使用する。

KAITEN は、「ボットネットの概要」でも紹介されているボットであり、ウイルスデータベースにおいても、ボットまたはボットをダウンロードしボットネットを形成するとされている[17]。同様に MARE もボットである[18]。

これらはいずれも 2005 年 12 月中旬以降に発見されており、ボットによる Web アプリケーションの脆弱性への攻撃が頻発した時期と重なる。ボットによる Web アプリケーションの脆弱性に対する攻撃は、2006 年 7 月頃から減少の傾向が見られ同年 11 月以降は収束していることが、図 3-2 からわかる。

なお、これらのウイルスはそれぞれが使用する脆弱性が発見されてから、一定の期間が経過した後に発見されている。LUPPER は XML-RPC ライブラリの脆弱性が発見されてから約 5 ヶ月後、KAITEN は Mambo の RFI の脆弱性が発見されてから 1 年 5 ヶ月後、KAIGENT は PHP-Nuke の RFI の脆弱性が発見されてから約 9 ヶ月後、MARE も XML-RPC ライブラリの脆弱性が発見されてから約 9 ヶ月に発見されている。

クライアント OS などの脆弱性は、発見されてから直ぐにボットに使用される場合があるが、Web アプリケーションの場合は悪用されるまでの期間が長いと言える。

これは、ハーダーがボットネット拡大の手段として Web アプリケーションの脆弱性に着目していなかったためと推測される。今後、ボットに悪用されるまでの期間が短縮される可能性が考えられる。

---

[17]ウイルス感染被害マンスリーレポート【2005 年 12 月度】(トレンドマイクロ)
http://www.trendmicro.com/jp/security/report/report/archive/2005/mvr060110.htm

[18] Linux を狙う新たなワームが出現，“ボット”の機能を持つ
http://itpro.nikkeibp.co.jp/article/NEWS/20060221/230155/

3.1.2. Web アプリケーションの脆弱性を使用するボットの機能

本項では、PHP で開発された Web アプリケーションに存在する RFI の脆弱性を使用して感染活動を行う PBOT[19]のソースコードを入手し、その機能を調査した。
入手した PBOT のソースコードは、pbot.php と gspread.php という 2 つの PHP スクリプトから構成されており、添付されていた README ファイルには、「pBot v2」という名称が記載されていた。pbot.php には既知のボットと同様に C&C サーバ(Command and Control サーバ)である IRC サーバに接続して、ハーダーからのコマンドを受信して実行する機能が実装されていた。
一方、gspread.php には RFI の脆弱性を使用して感染活動を行う機能が実装されていた。

pbot.php は約 700 行のスクリプトで、IRC プロトコルの PRIVMSG メッセージを介してコマンドを受信・実行し、ハーダーに疑似シェルインターフェイスを提供する。表 3-2 は、ソースコードの調査により明らかになった PBOT のコマンドの一覧である。コマンドは機能別に「IRC 接続関連」、「ファイル操作関連」、「情報収集関連」、「コマンド実行関連機能」の 4 つに分類できる。
IRC 接続関連の機能の一部として、従来のボットと同じくパスワードによる IRC チャンネルの保護やハーダーの認証といったボットネットを保護する機能が実装されていた。また、全ての機能は PHP の関数を使用して実装されているため、シェルが使えないサーバでもハーダーは容易にファイル操作やコマンドの実行が行える。また、PHP がインストールされ、動作する環境であれば OS を問わず動作する。
情報収集系の機能は、HTTP の環境変数から得られる情報を表示する「srvinfo」コマンドや PHP の uname 関数により OS の情報の取得する「uname」コマンドが実装されていた。なお、キーロガーやサーバ上のファイルの検索、設定ファイルを読み取る機能などは実装されていなかった。

メール送信機能も PHP の関数で実装されていたが、これまでのボットに多く見られた Proxy サーバ機能は実装されていなかった。このことから、スパムメール送信の中継を第一の目的としたボットではない可能性が考えられる。また、DDoS 攻撃を行う機能も実装されていない。
ただし、別のサイトからファイルをダウンロードする機能が実装されており、この機能を使用してファイルをダウンロードすることによって、ボットのアップデート、モジュール

---

[19] PHP_PBOT 詳細(トレンドマイクロ)
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=PHP%5FPBOT%2EA&VSect=T

の追加や別のマルウェアを感染させることが可能と考えられる。

表 3-2　PBOT のコマンド一覧

＜非公開＞

gspread.php に実装されていた感染活動機能は、Google 検索エンジンを利用して URL に特定のキーワードを含むサイトを検索し、検索結果として得られたサイトに対して攻撃コードを送り込むものである。キーワードには、RFI の脆弱性が存在する Web アプリケーションを特定するファイル名(＜非公開＞) が使用される。gspread.php は、ハーダーが IRC を介して送信するコマンドによって実行される。実行例を表 3-3、使用されるパラメータの解説を表 3-4 に示す。
2004 年末に出現した SANTY ワームでも同様に Google の検索機能を利用した感染手法が使用されており、その際 Google は SANTY ワームによる検索リクエストをフィルタリングする対処を実施した[20]。

表 3-3　gspread.php の実行例

＜非公開＞

表 3-4　gspread.php で使用されるパラメータ

＜非公開＞

以上のように Web アプリケーションの脆弱性を使用する PBOT は、IRC サーバを C&C サーバとしたボットネットを形成し、感染した Web サーバ上でファイル操作や任意のコマンドの実行が可能である。クライアントを標的としていたボットと比較すると基本的な機能のみが実装されていた。しかし、ファイルのダウンロードおよび任意のコマンドの実行が可能であるため、感染後にスパム送信や DDoS 攻撃を行う機能を別のコンポーネントとして追加される可能性がある。

---

[20] 米 Google,「Santy」ワームが“標的”を探せないようにフィルタリングを開始
http://itpro.nikkeibp.co.jp/free/ITPro/NEWS/20041222/154202/

3.2. 2005 年から 2006 年にかけてのウイルス発生動向の調査

2005 年から 2006 年にかけてのウイルスの発生動向をパターンファイルから調査を行った。トレンドマイクロでは、ウイルスを感染・拡散方法、活動の特徴などにもとづいて分類し、ウイルス名に接頭語をつけている[21]。ウイルス名の代表的な接頭語と各接頭語をもつウイルスの特徴を表 3-5 に示す。

表 3-5 トレンドマイクロによるウイルス名の接頭語とその特徴

接頭語	特徴
TROJ	有用なソフトウェアを装い、不正な活動するウイルスで一般的にトロイの木馬と呼ばれる。 単体プログラムとして存在し、ネットワークを通じた拡散や他のファイルへの感染は行わない。 別のウイルスをダウンロードし感染させるものがある。
TSPY	トロイの木馬型ウイルスの一種で主に情報漏洩につながる不正活動を行うもの。 パスワードなど重要な情報を盗むことを目的とする。一般的にスパイウェアと呼ばれる場合がある。
BKDR	トロイの木馬型ウイルスの一種でネットワークを介して感染したマシンを自由に操ることを目的とするもの(ボットを含む)。
WORM	ネットワークを通じてほかのコンピュータに拡散することを目的としたもの。 一般的にワームと呼ばれ、メールの添付ファイルとして自動的に自分自身のコピーを拡散させるものやネットワークを利用して次々に感染していくものがある(ボットを含む)。
PE	一般的にファイル感染型ウイルスと呼ばれる。単体でプログラムを実行したり複製するのではなく、PEファイル(※)に付着して制御を奪い、プログラムを書き換えて感染増殖する。 ※Portable Executableの略、拡張子が.EXE、.SCR、.COMなどのWindowsの実行可能ファイル
ELF	ファイル形式が、ELF形式(UNIX、LINUXなどの実行可能ファイル)であるもの。

ウイルス発生動向の調査では、上記期間にウイルスパターンファイルに登録されたウイルスの上位 6 タイプを選択し、調査を行った。

図 3-4 は、名称に表 3-5 に示した接頭語をもつウイルスの 2005 年 1 月から 2006 年 12 月の間におけるパターン登録数の推移を示したものである。この図から、ウイルスの発生動向を確認することができる。なお、図 3-4 から図 3-7 において、パターン登録数が前の月と比較して減少している箇所がある。これは、未知の亜種ウイルスや圧縮形式の異なるウイルスを 1 つのパターンで検出可能にする機能が追加されたためである[22]。

---

[21] ウイルスを知ろう - ウイルス名の接頭語
http://www.trendmicro.com/jp/security/general/type/virusname/head.htm

[22] トレンドマイクロ、パターンファイルに未知の亜種ウイルスを防ぐ新機能

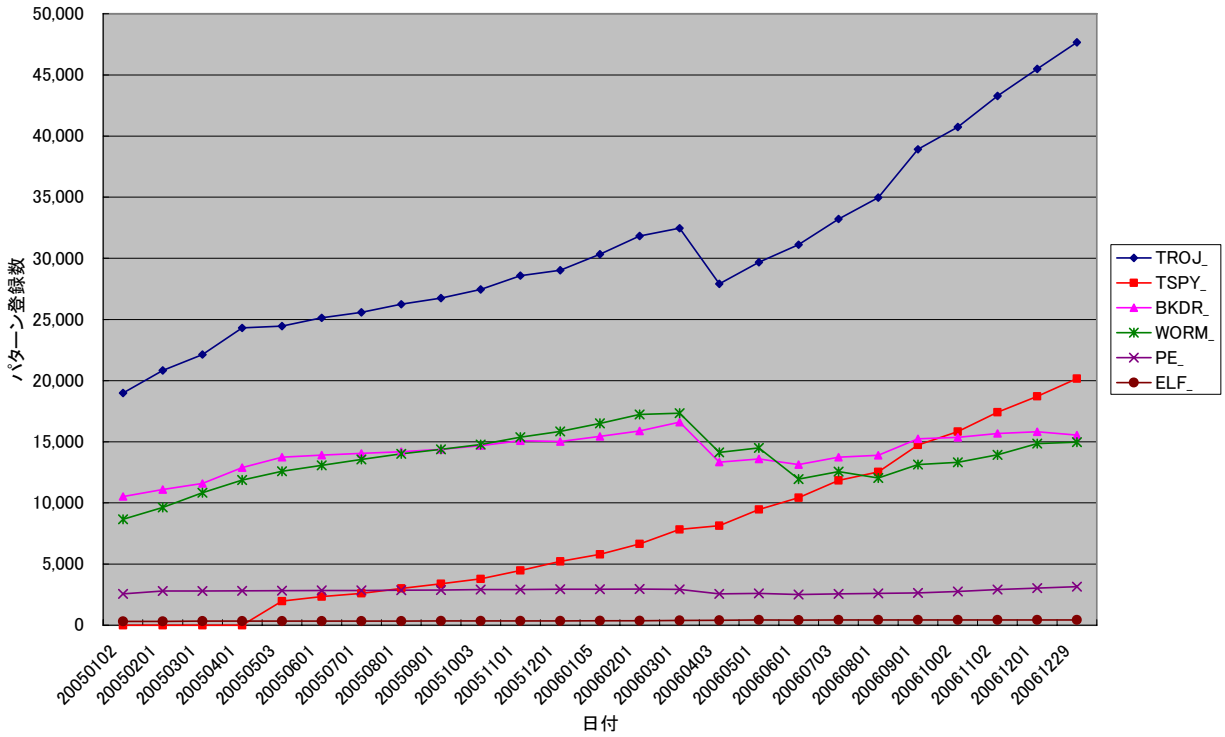

図 3-4　2005 年から 2006 年にかけてのウイルス発生動向

2005 年 1 月から 2006 年 12 月に発生したウイルスのパターンファイルへの登録数は、2005 年 1 月に 83,630 件であったものが、2006 年 12 月末までに 63,970 件増加し、147,600 件になっている。なかでもウイルス名の接頭語が TROJ であるウイルス(以下、TROJ ウイルス)および接頭語が TSPY であるウイルス(以下、TSPY ウイルス)の登録数の増加が顕著であり、これらの亜種が多数出現したと考えられる。

これまで JPCERT/CC でも深刻な脅威と捉えてきたボットは、トレンドマイクロによるウイルス名で接頭語 WORM または BDKR がつけられている場合が多い(WORM_AGOBOT、WORM_RBOT、WORM_SDBOT、BKDR_SDBOT など)[23]。ボットを含むこれら WORM・BKDR ウイルスの登録数の増加は、TROJ・TSPY ウイルスと比較すると緩やかである。しかし、2005 年および 2006 年のウイルス感染被害をまとめたトレンドマイクロのレポートによると、WORM_RBOT、WORM_SDBOT への感染被害が多いことが分かる[24] [25]。また、マイクロソフトによる悪意のあるソフトウェアの削除

http://internet.watch.impress.co.jp/cda/news/2006/05/08/11869.html

[23] ボット系ウイルス対策 Web > ウイルス詳細情報
http://www.trendmicro.com/jp/security/web/bot/subtitle/vinfo.htm

[24] ウイルス感染被害レポート - 2005 年度（最終版）
http://www.trendmicro.com/jp/security/report/report/archive/2005/mvr2005.htm

ツール(MSRT)の成果とマルウェアの傾向をまとめたレポートでも、2005年1月から2006年3月の間に最も削除されたものが、RBOT(Win32/Rbot)であり、次いでSDBOT(Win32/Sdbot)だとされている[26]。このように、ウイルス感染の被害状況を見る限り、ボットは依然として脅威であることに変わりはない。

パターンファイルへの登録数が大幅に増加したTROJウイルスは、2005年1月に18,986件であった登録数が2006年12月には、28,669件も増加し47,655件になっている。この期間に流行したTROJウイルスには、TROJ_AGENT、TROJ_IESER、TROJ_SMALL、TROJ_DELF、TROJ_DLOADER、TROJ_ROOTKIT、TROJ_ISTBARなどがある。これらのウイルスは、Webからのダウンロードによって感染し、活動内容は、別のウイルスをダウンロードしてシステムに感染させる「DOWNLOADER」と呼ばれるものが多数存在する[27]。
また、2005年の半ばから増加が指摘されはじめた標的型攻撃やゼロデイ攻撃に使用されたものもある。ジャストシステムの一太郎の脆弱性を使用するTROJ_MDROPPER.BL(別称Trojan.Tarodrop[28])やマイクロソフトWordの脆弱性を狙ったDOWNLOADERのTroj/DwnLdr-FXG(別称TROJ_TINY.DU[29])もTROJウイルスであった。
その他、ANNTINYをはじめとするP2Pファイル共有ネットワーク上で蔓延しているウイルスの亜種にも、TROJウイルスに分類されるものが存在するなど多種に渡る。
TROJウイルスに伴ってTSPYウイルスも増加していることが図3-4から読み取ることができる。このことから、TROJウイルスがTSPYウイルスをダウンロードし、感染させていると推測される。2005年1月にはパターンに登録されていなかったTSPYウイルスが、2006年12月には20,164種に増加している。代表的なTSPYウイルスには、オンラインゲームのアカウント情報を盗むTSPY_LINEAGE、ネットバンクのアカウント情報を盗むTSPY_BANCOSやインスタントメッセンジャーのアカウント情報を盗むTSPY_QQPASSなどが存在する。
次項3.2.1から3.2.3では、主要なTSPYウイルスについての調査結果を記載する。
3.3節では、DOWNLOADERについての調査結果を記載する。

---

25 ウイルス感染被害レポート - 2006年度（最終版）
http://www.trendmicro.com/jp/security/report/report/archive/2006/mvr2006.htm
26 Windows 悪意のあるソフトウェアの削除ツール: これまでの成果と悪意のあるソフトウェアの傾向
http://www.microsoft.com/downloads/details.aspx?displaylang=ja&FamilyID=47ddcfa9-645d-4495-9eda-92cde33e99a9
27 ウイルス対策Web一覧(トレンドマイクロ)
http://www.trendmicro.com/jp/security/web/archive/overview.htm
28 一太郎を狙うゼロデイ攻撃
http://www.itmedia.co.jp/enterprise/articles/0608/17/news072.html
29 Wordのパッチ未公開セキュリティ・ホールを突く「トロイの木馬」出現
http://itpro.nikkeibp.co.jp/article/NEWS/20061208/256395/

3.2.1. オンラインゲームのアカウントを盗むウイルス

昨今、Real-Money Trading(以下、RMT)と呼ばれる仮想貨幣と実貨幣との取引行為が広がっている。加えて RMT を目的とし、ウイルスを使用した仮想貨幣の詐取も発生しているという[30]。こうしたウイルスの機能は、単純にオンラインゲームのアカウントを盗み出すのみに特化していると言われている。
これら単機能化されたウイルスの実態について、パターンファイルに登録されているウイルス登録数およびウイルスデータベースに登録されている情報などから調査を行った。

図 3-5 は、2005 年 1 月から 2006 年 12 月の間にパターンファイルに登録された TSPY ウイルスのうち、オンラインゲームのアカウント情報を盗むウイルスのパターン登録数の推移を示したものである。この図から、オンラインゲームのアカウント情報を盗むウイルスの発生動向を確認することができる。

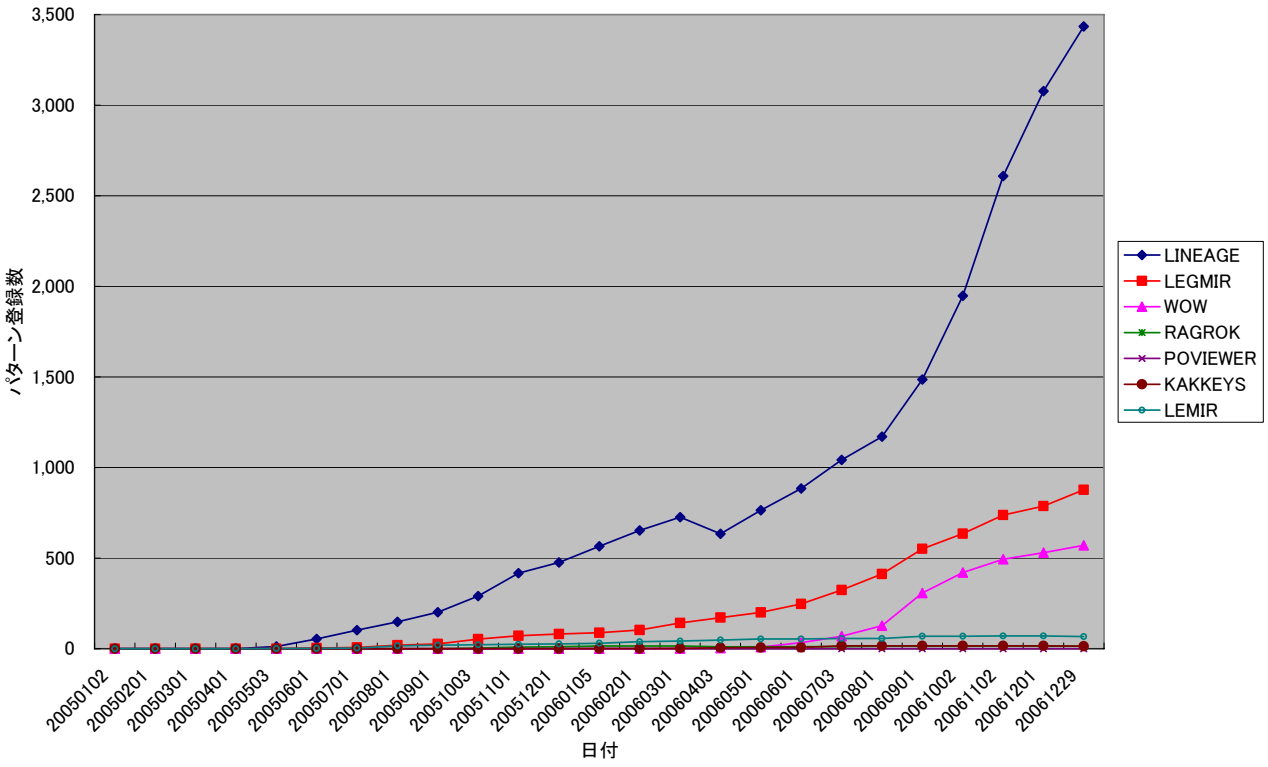

図 3-5 オンラインゲームのアカウントを盗むウイルス

---

[30] MYCOM「マルウェアを悪用した RMT 行為を警告 - 米 Symantec」
http://journal.mycom.co.jp/news/2007/03/19/380.html

オンラインゲームのアカウントを盗むウイルスは、TSPY_【標的のオンラインゲーム名を表す文字列】という名称になっているものが多い。
表 3-6 に代表的な TSPY ウイルスとその概要を示す。
オンラインゲームのアカウントを盗むウイルスは、2005 年 5 月からパターンファイルに登録され、調査対象期間中に全体で 4,978 種類登録されている。なかでも TSPY_LINEAGE の亜種が 3,435 種類登録され、約 70％を占める。次いで TSPY_LEGMIR が 877 種類、TSPY_WOW が 571 種類であり、これら 3 種の亜種だけで全体の約 98%にあたる。

表 3-6　オンラインゲームのアカウントを盗む主要な TSPY ウイルスとその特徴

ウイルス名称	概要(※記載と異なる挙動をとる亜種も存在する)
TSPY_LINEAGE	オンラインゲーム "Lineage(リネージュ)" などのアカウント名およびパスワード等を収集し、ファイルとしてシステムのルート(通常C:ドライブ)内に保存する。また、保存したファイルを、HTTPもしくは SMTPを使用して、不正リモートユーザに送信する。"Lineage(リネージュ)"以外のオンラインゲームを標的とした亜種も存在する。
TSPY_LEGMIR	オンラインゲーム "Legmir" のアカウント名およびパスワード等を収集する。自身のSMTPエンジンを利用して、収集した情報を不正リモートユーザに送信する。
TSPY_LEMIR	オンラインゲーム "Legend of Mir" のアカウント名およびパスワード等を収集する。
TSPY_WOW	Internet Explorerのアドレスバーの URLを監視し、オンラインゲーム "World of Warcraft" のアカウント名およびパスワード等を収集する。また、収集した情報を自身のSMTPエンジンを使用して電子メールで不正リモートユーザに送信する。
TSPY_RAGROK	オンラインゲーム "Ragnarok Online" のアカウント名およびパスワード等の情報を収集する。また、収集した情報を自身のSMTPエンジンを介して電子メールで送信する。
TSPY_POVIEWER	オンラインゲーム "FINAL FANTASY XI" などが提供されているポータル "Play Online" のアカウント名およびパスワード等の情報を収集する。また、収集した情報と"Play Online"クライアントのスクリーンショットをHTTPを利用して不正リモートユーザが用意したWebサイトに送信する。
TSPY_KAKKEYS	オンラインゲーム "Ragnarok Online" のアカウント名およびキャラクタ名などを収集、ゲームのスクリーンショットの保存を行う。その他、デスクトップ画面のスクリーンショットやInternet Explorerの「お気に入り」を収集する。ファイル共有ソフトウェア「Winny」および「Share」がインストールされているフォルダを検索し、ランダムな日本語名称のフォルダを作成する。このフォルダがファイル共有ソフトウェアのアップロードフォルダとなるように登録し、収集した情報を流出させる。また、"Ragnarok Online" のレジストリの書き換えや、収集した情報を「2ちゃんねる」や「したらば」などの掲示板に対する書き込みを行う。

TSPY_LINEAGE は、MMORPG(Massively Multiplayer Online Role-Playing Game:多人数同時参加型オンラインロールプレイングゲーム)というジャンルのオンラインゲーム「Lineage」のアカウントを主な標的とするウイルスである。TSPY_LEGMIR も同じく韓国で開発された MMORPG「Legends of Mir 2」、TSPY_WOW は、米国で開発された MMORPG「World of Warcraft」のアカウントを標的とする。

オンラインゲームのアカウントを盗むウイルスの大半を占めるこれら 3 系統の亜種登録数は、2006 年に急増している。特に 2006 年 8 月以降の TSPY_LINEAGE の増加が顕著である。この理由の 1 つとして、TSPY_LINEAGE の亜種の中には、「Ragnarok Online」など Lineage 以外のオンラインゲームを標的とするものが存在することが考えられる[31]。このように、ウイルス名で示されるオンラインゲームのみが標的となっているわけではなく、他のオンラインゲームもウイルスの標的になっていると推測される。
その他、国内の開発・運用会社によって展開されている「FINAL FANTASY XI」などを標的とする TSPY_POVIEWER も確認されている。

これらのウイルスの挙動は、ユーザがゲームへログインする際のキーボードからの入力を監視し、アカウント名やパスワードを記録することである。そして、記録した情報を自身に組み込まれた SMTP エンジンを使用し、メールで悪意のある人物へ送信する。
また、SMTP ではなく HTTP を用いて送信する種類も存在する。
表 3-6 に挙げた TSPY_KAKKEYS 以外は、アカウントを盗むことが第一の目的と考えられる。しかし、TSPY_KAKKEYS はアカウント名・キャラクタ名とゲームのスクリーンショットを収集し、「Winny」や「Share」による P2P ファイル共有ネットワークに流出させる。また、収集した情報を「2 ちゃんねる」や「したらば」などの大規模掲示板サイトへ書き込む。ユーザのプライバシーを漏洩させる暴露型ウイルスの性質が強く、主に日本のオンラインゲームユーザを標的として作成されたウイルスと推測される。

アカウントを盗もうとする悪意のある人物は、ゲームのコミュニティサイトやユーザのブログなどに、ゲームの情報や関連するツールなどに見せかけてアップロードしたウイルスへのリンクを作成する。そして、ダウンロードおよび実行するようにユーザを誘導すると考えられる。また、オンラインゲームの攻略サイトに見せかけたフィッシングサイトにウイルスが仕掛けられる可能性も考えられる。

---

[31] TSPY_LINEAGE.RN 詳細
http://www.trendmicro.co.jp/vinfo/grayware/ve_graywareDetails.asp?GNAME=TSPY_LINEAGE.RN&VSect=Td

3.2.2. ネットバンクのアカウントを盗むウイルス

一部報道によると、金融庁が把握しているネットバンクの不正引き出し額が 2005 年以降の累計で約 1 億 7 千 4 百万円にのぼるという[32]。また、こうした被害の一因にウイルス感染があるという。
このような背景を鑑み、パターンファイルに登録されているウイルス登録数およびウイルスデータベースに登録されている情報などから、ネットバンクのアカウントを盗むウイルスの調査を行った。

図 3-6 は、2005 年 1 月から 2006 年 12 月の間にパターンファイルに登録された TSPY ウイルスで、かつネットバンクのアカウント情報を盗む TSPY_BANCOS の亜種登録数の推移を示したものである。この図から、ネットバンクのアカウント情報を盗むウイルスの発生動向を確認することができる。

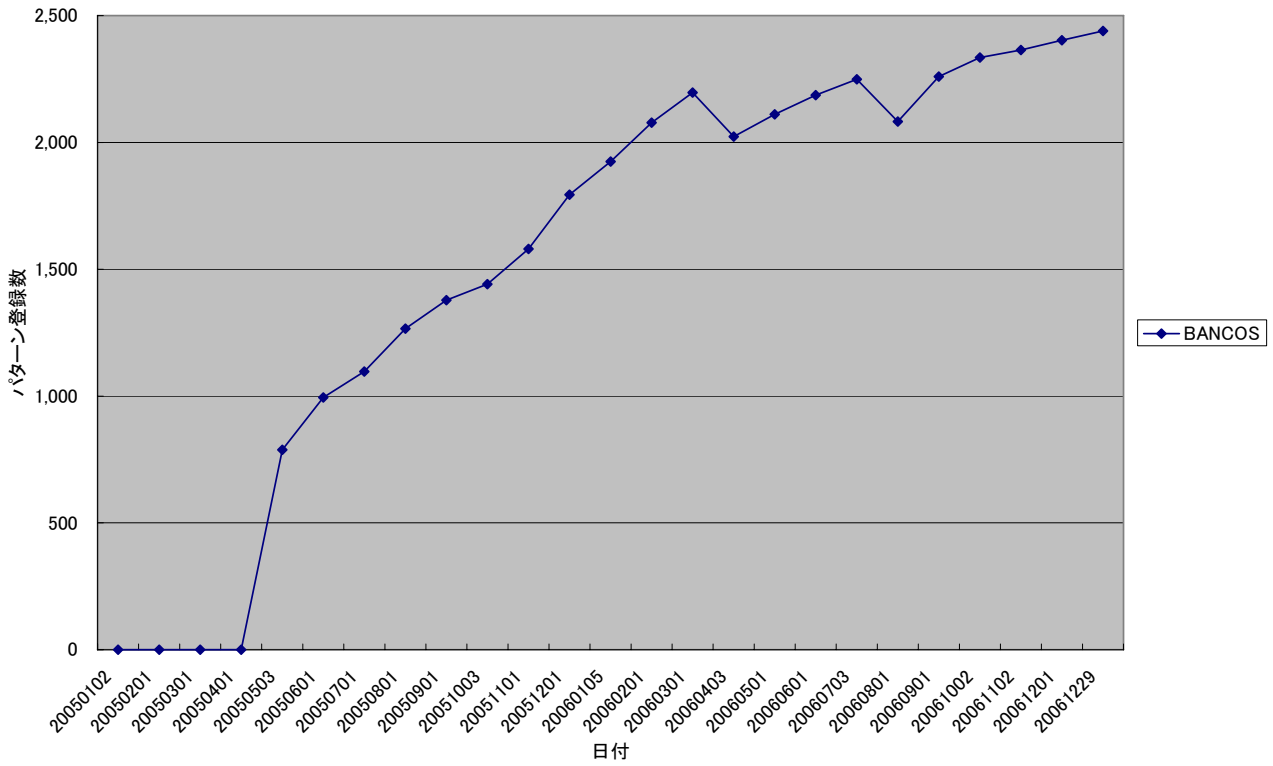

図 3-6 ネットバンクのアカウントを盗むウイルス

TSPY_BANNCOS は、2005 年の 5 月にはじめてパターンファイルに登録されている。

---

[32] 2007 年 3 月 22 日 毎日新聞一面
「ネットバンク：不正引き出し１９９件、被害額は３億円」

これは、オンラインゲームのアカウントを盗むウイルスがパターンファイルに登録された時期と重なるが、2006 年になってから大幅な増加が見られた同ウイルスとは異なり、2005 年 5 月の最初のパターン登録において 788 件もの亜種が登録されている。
このことから、2005 年 4 月から 5 月にかけて大量の亜種が出現したと考えられる。
2005 年の 6 月以降パターン登録数は、平均すると毎月約 100 件程度増加している。2006 年末には 2,439 件になっており、非常に多数の亜種が存在する。

2005 年に開かれた PacSec[33]において株式会社シマンテック(以下、シマンテック)は、ネットバンクのアカウントを盗むウイルスについての発表を行った[34]。
このなかで、PWSteal.Bancos という名称のウイルスについて、ユーザから提出された検体数の推移が示されている。これをみても、ネットバンクのアカウントを盗むウイルスは 2005 年の 4 月から 5 月にかけて多数出現したと考えられる。
また、PWSteal.Bancos は当初、ブラジルのネットバンクのみを標的としていたが、その後、ドイツやイギリスなどヨーロッパの国を標的に加えたとされている。その亜種である PWSteal.Bancos.T は、2,746 ものドメインを標的とする。TSPY_BANCOS.ANM (別称 PWSteal.Jginko)は、日本のネットバンクのみを標的とするウイルスである[35]。
このように、特定の国や地域のネットバンクのみを標的とする亜種も存在する。2005 年 7 月、この TSPY_BANCOS.ANM によって、日本の複数のネットバンクで不正送金による直接的な金銭詐取の被害が発生した[36]。
これらのウイルスの挙動は、ユーザがネットバンクにログインする際のブラウザへの入力を監視し、アカウント名・口座番号やパスワード・暗証番号を記録することである。そして、記録した情報を主に HTTP を用いて悪意のある人物に送信する。なお、前述のシマンテックの発表によると、これらのウイルスは Internet Explorer と密接に関係しており、単なるキーロガーではなく自身を隠蔽する機能や通信の傍受機能を持っているとされる。

---

33 PacSec http://pacsec.jp/
34 Bank Trojan の進化 Symantec http://pacsec.jp/psj05/psj05-shinotsuka-jp.ppt
35 トレンドマイクロ、国内のネットバンクを標的にしたウイルス「TSPY_BANCOS.ANM」を警告
http://www.rbbtoday.com/news/20050708/24043.html
36 ITmedia エンタープライズ：邦銀を狙い打ちにしていたトロイの木馬
http://www.itmedia.co.jp/enterprise/articles/0507/09/news007.html

2003 年 4 月、ネットカフェの PC に仕掛けられたキーロガーによってネットバンクのアカウントが盗まれ、1,600 万円が不正に送金された事件があった[37]。こうした事件もあり、ネットバンクのセキュリティに対する懸念があったはずだが、対策よりも実際の被害が先行した。その後、一部のネットバンクでは、ソフトウェアキーボードや乱数表だけでなく、ワンタイムパスワードトークンも導入し、認証に対するセキュリティの強化を図っている。2006 年には、ネットバンクのアカウントを盗むウイルスのパターン登録数の増加が緩やかになっている。

[37] ネットバンクで 1600 万円が突然消える / デジタル ARENA
http://arena.nikkeibp.co.jp/trend/zoom/20030408/104344/

3.2.3. インスタントメッセンジャーのアカウントを盗むウイルス

特定のインスタントメッセンジャー向けに発行されている仮想貨幣もRMT行為の対象になっているという。特に中国で使用されているインスタントメッセンジャー「QQ」の付帯サービス利用者向けに発行されている「Q幣」は、RMT行為の対象になっているという[38]。このような背景を鑑みると、2.2.2.「ネットバンクのアカウントを盗むウイルスの調査」と同様に、特定インスタントメッセンジャーのアカウントを盗むウイルスの出現が想定される。
このような背景を鑑み、パターンファイルに登録されているウイルス登録数およびウイルスデータベースに登録されている情報などから、インスタントメッセンジャーのアカウントを盗むウイルスの調査を行った。

図 3-7は、2005年1月から2006年12月の間にパターンファイルに登録されたTSPYウイルスで、かつインスタントメッセンジャーのアカウント情報を盗むTSPY_QQPASSの亜種登録数を示したものである。この図から、インスタントメッセンジャーのアカウント情報を盗むウイルスの発生動向を確認することができる。

[38] CNET Japan「中国文化部、バーチャルマネーとリアルマネーの取引にメスか」
http://japan.cnet.com/column/china/story/0,2000055907,20338818,00.htm

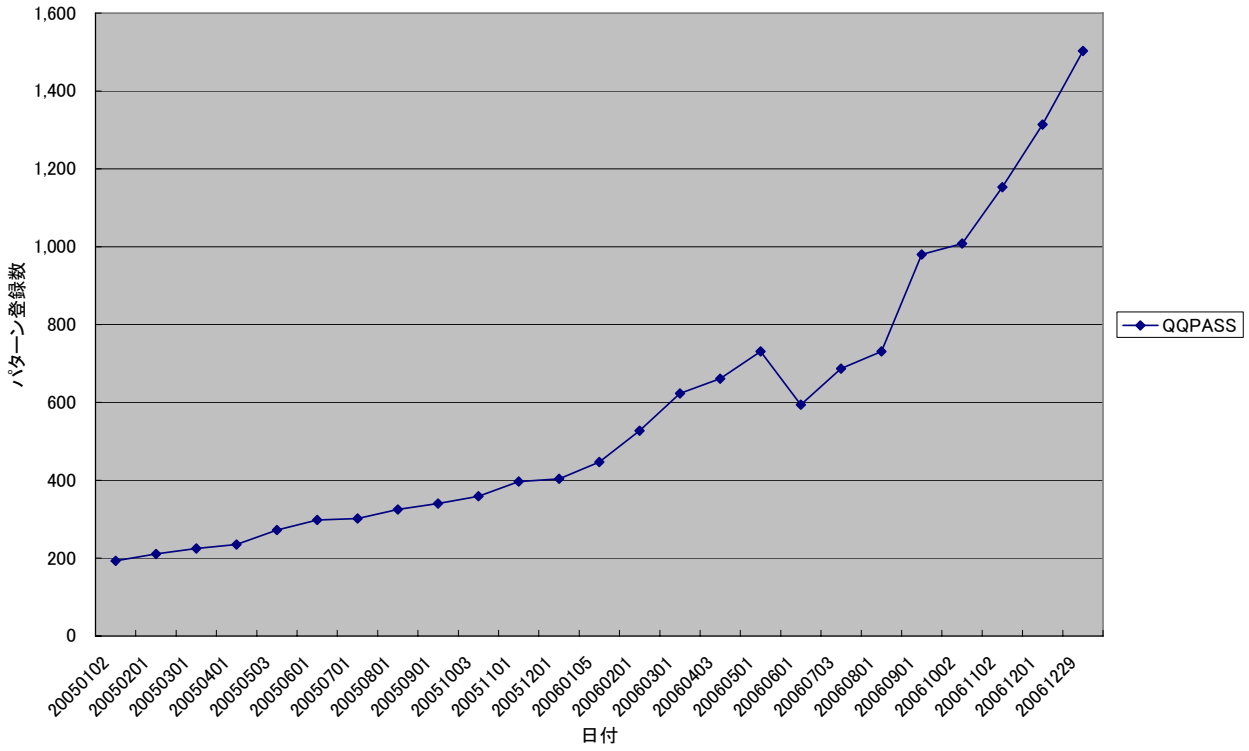

図 3-7　インスタントメッセンジャーのアカウントを盗むウイルス

TSPY_QQPASS は、主に中国で利用されているインスタントメッセンジャーである「QQ」のアカウントを盗むものである。パターン登録数は、2005 年 1 月に 193 件であったが、2006 年末には 1,503 件まで増加しており、多数の亜種が存在する。オンラインゲームのアカウントを盗むウイルスと同じく 2006 年に大幅な増加が見られる。

TSPY_QQPASS の挙動はオンラインゲームやネットバンクのアカウントを盗むウイルスと同じである。ユーザが QQ にログインする際のキーボードからの入力を監視し、アカウント名やパスワードを記録し、それらの情報を SMTP や HTTP を用いて悪意のある人物へ送信する。

中国では、多数のインターネットユーザがインスタントメッセンジャーを使用しており、数あるインスタントメッセンジャーの中でシェアが最も高いのが QQ だという[39]。
QQ の運営会社は、QQ の他にブログやアバター、オンラインゲームといったサービスも提供している。これらのサービスは QQ と同一のアカウントで利用することができる。さらに、同社が提供するオンラインゲームの中で獲得したポイントをインターネット上の仮想貨幣「Q 幣」に換金できるサービスを提供していた。この Q 幣は、オークションサイトで RMT が行われるほど需要があるという。
このような背景から、QQ のアカウントには金銭的な価値があり、TSPY_QQPASS は、ゲームやネットバンクのアカウント盗むものと同じく金銭詐取を目的として作成されたと考えられる。ショッピングサイトなどへの不正侵入の罪で摘発された集団が、侵入したサイトにウイルスを仕掛け、アクセスしたユーザに QQ のアカウントを盗むウイルスを感染させる手口を使っていたという[40]。
なお、QQ 運営会社は、現在同社の提供するオンラインゲームで獲得できるポイントを Q 幣に換金するサービスを停止している。

---

[39] 【中国 IT 事情】インスタントメッセンジャーの利用者は 1 億 1872 万人
http://pc.nikkeibp.co.jp/article/NEWS/20070208/261405/?ST=pc_news
[40] バーチャルマネーの規制強化で「Q 幣」自己規制
http://japan.internet.com/wmnews/20070320/8.html

3.3. DOWNLOADER の調査

昨今、前節で示した TSPY ウイルスのような単機能または機能毎にコンポーネント化されたボットなどを悪意のあるサイトからダウンロードし、感染させるウイルスが増加しているという報告がある。
このようなウイルスは、「DOWNLOADER（ダウンローダー)」と呼ばれている。トレンドマイクロによるウイルス名称では、TROJ ウイルスに多くの DOWNLOADER が分類されている。3.2.節では、TROJ ウイルスが TPSY ウイルスをダウンロードし、感染させていると推測した。本節では、DOWNLOADER の種類、機能および使用する脆弱性について調査した結果を記載する。

3.3.1. DOWNLOADER の種類

パターンファイルに登録されているウイルス登録数およびウイルスデータベースに登録されているウイルス情報などから、代表的な DOWNLOADER の調査を行った。

図 3-8 は、2005 年 1 月から 2006 年 12 月の間にパターンファイルに登録された主要な DOWNLOADER の亜種登録数の推移を示したものである。この図から、DOWNLOADER の亜種発生動向を確認することができる。

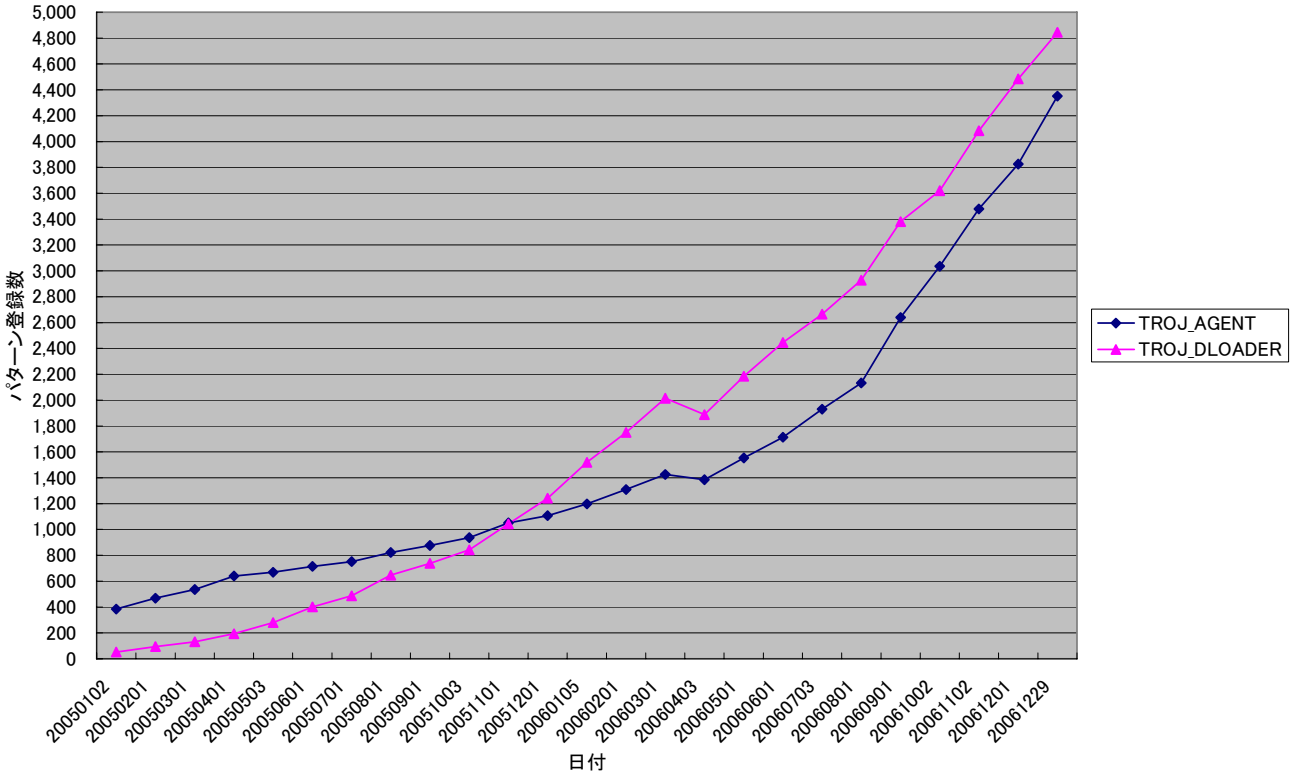

図 3-8　主要な DOWNLOADER の亜種登録数の推移

2005 年 1 月から 2006 年 12 月にかけてパターン登録数が 28,669 件増加している TROJ ウイルスのうち、感染動作が DOWNLOADER であり、かつ亜種の数が多いものに TROJ_AGENT と TROJ_DLOADER がある。TROJ_AGENT は、2005 年 1 月に 384 件であった登録数が 2006 年 12 月までに 3,968 件増加し、4,352 件となっている。また、TROJ_DLOADER は 2005 年 1 月に 52 件であった登録数が 2006 年 12 月までに 4,793 件も増加し、4,845 件となっている。図 3-8 から、TROJ_AGENT は 2006 年 5 月頃、TROJ_DLOADER は 2005 年 11 月頃から大幅に増加していることが読み取れる。
この 2 種の亜種を合計すると 9,638 件になる。これは、TROJ ウイルス全体 28,669 件の約 30%にあたり、代表的な DOWNLOADER と言える。

3.3.2. DOWNLOADER の機能

パターンファイルおよびウイルスデータベースに登録されているウイルス情報などから DOWNLOADER の機能の調査を行った。

DOWNLOADER の主な機能は、その名称が表す通り悪意のあるサイトからのファイルのダウンロードである。3.2 節および 3.3 節で述べたように、別のウイルスを感染させるために使用される。主に HTTP でダウンロードしたファイルを実行または特定のフォルダに配置することによって感染させる。
トレンドマイクロのウイルス情報によると、DOWNLOADER は種類によりダウンロードするウイルスの種類や数が異なり、ダウンロード先のサイトも様々である。1 つの DOWNLOADER が複数のウイルスをダウンロードする場合もある[41]。また、ダウンロードされるウイルスは、単体で動作する EXE 形式の場合もあれば、DLL などの形式で別のウイルスのコンポーネントとして動作するものもある[42]。
単機能のウイルスや機能毎にコンポーネント化されたボット等の感染過程で DOWNLOADER が使用される理由として以下のことが考えられる。

- DOWNLOADER は、ウイルスのインストーラーまたはアップデートクライアントの役割を果たしていると考えられる。ウイルス作者は、任意のタイミングでダウンロードされるファイルの中身を変えることができ、機能拡張や変更を加えることや 1 つの DOWNLOADER で複数のウイルスを感染させることができると推測される。

- コンポーネント化したウイルスを DOWNLOADER にダウンロードさせることで全容の把握を困難にし、ウイルスが完全に駆除されることを回避していると考えられる。一部のコンポーネントのみが駆除されても DOWNLOADER が残存している場合、再度ウイルスに感染する可能性がある。

- ゲートウェイでのウイルス対策として、メールのウイルススキャンが一般的になりつつあるのに対し Web コンテンツのフィルタリングは実施されている場合が少ないため、HTTP を利用することにより経路上で検知される可能性を低減していると考えられる。

---

41 複数の TSPY_BANCOS をダウンロードする「TROJ_DLOADER.HW」
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=TROJ%5FDLOADER%2EHW

42 「TROJ_AGENT.BO」にダウンロードされる「TROJ_AGENT.CE」
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=TROJ%5FAGENT%2ECE&VSect=T

3.3.3. DOWNLOADER が使用する脆弱性

本項では、DOWNLOADER がどのような脆弱性を使用するかをパターンファイルおよびウイルスデータベースに登録されているウイルス情報から調査する。加えて、DOWNLOADER とゼロデイ攻撃の関連性をラックのレポートやニュースサイトの報道などの情報から調査する。本項で言う感染とは、ユーザによる Web サイトやファイルの閲覧などの受動的な操作を介して、DOWNLOADER に感染することを指している。

ウイルスデータベースの情報を調査した結果を表 3-7 に示す。TROJ_DLOADER の亜種で脆弱性を使用するものに TROJ_DLOADER.XH および TROJ_DLOADER.JHV が存在した。TROJ_DLOADER.XH は、Windows のカーソルおよびアイコンのフォーマットの処理の脆弱性を使用して、"WEB.EXE"という名称のファイルを Windows のシステムフォルダへダウンロードする。一方、TROJ_DLOADER.JHV は、米アップル社の QuickTime の脆弱性を使用し、”sqltrack.js[43]”というファイルをダウンロードする。
その他に、接頭語が「JS」であるウイルス[44]にも脆弱性を使用する DOWNLOADER が複数存在した。これらに使用される脆弱性はリモートでコードが実行されるもので、攻撃コードが Java スクリプトで実装され HTML に埋め込まれるものが多い。
脆弱性の存在するアプリケーションによる Web サイトの閲覧やムービーの再生などを介してこれらの DOWNLOADER に感染し、別のウイルスがダウンロードされる。

表 3-7 脆弱性を使用する DOWNLOADER

発見日	ウイルス名称	利用する脆弱性
2005/8/2	TROJ_DLOADER.XH	カーソルおよびアイコンのフォーマットの処理の脆弱性により、リモートでコードが実行される (MS05-002)
2005/12/8	JS_DLOADER.AZZ	Internet Explorer の不適切な Document Object Model オブジェクトの処理方法による脆弱性のため、リモートでコードが実行される (MS05-054)
2005/12/28	TROJ_NASCENE.A	Graphics Rendering Engine の脆弱性によりコードが実行される可能性がある (MS06-001)
2006/9/19	EXPL_EXECOD.A (Trojan.Vimalov)	Vector Markup Language の脆弱性により、リモートでコードが実行される (MS06-055)
2006/9/30	JS_PLOIT.BC	Windows Explorer の脆弱性により、リモートでコードが実行される (MS06-057)
2007/1/18	JS_WONKA.AS	Microsoft Data Access Components (MDAC) の機能の脆弱性により、コードが実行される可能性がある (MS06-014)
2007/3/16	TROJ_DLOADER.JHV	QuickTime の脆弱性(CVE-2007-0711～CVE-2007-0718)
2007/3/28	TROJ_ANICMOO.AX	GDI の脆弱性により、リモートでコードが実行される (MS07-017)

---

[43] SNS サイト"MySpace" のアカウントを収集するウイルス JS_SPACESTALK.A
[44] HTML 内に埋め込めるオブジェクト指向スクリプト言語である Java スクリプトで記述されたウイルス

次に、オフィスアプリケーションの未知の脆弱性を使用したゼロデイ攻撃と DOWNLOADER の関連について調査した結果を示す。ラックが 2006 年 2 月に発表したレポート[45]によると、マイクロソフトの Office 製品を標的としたゼロデイ攻撃は 2005 年には確認されておらず、2006 年に 8 件確認されている（図 3-9)。ただし、ここで挙げるゼロデイ攻撃は一般に報道されたもののみである。

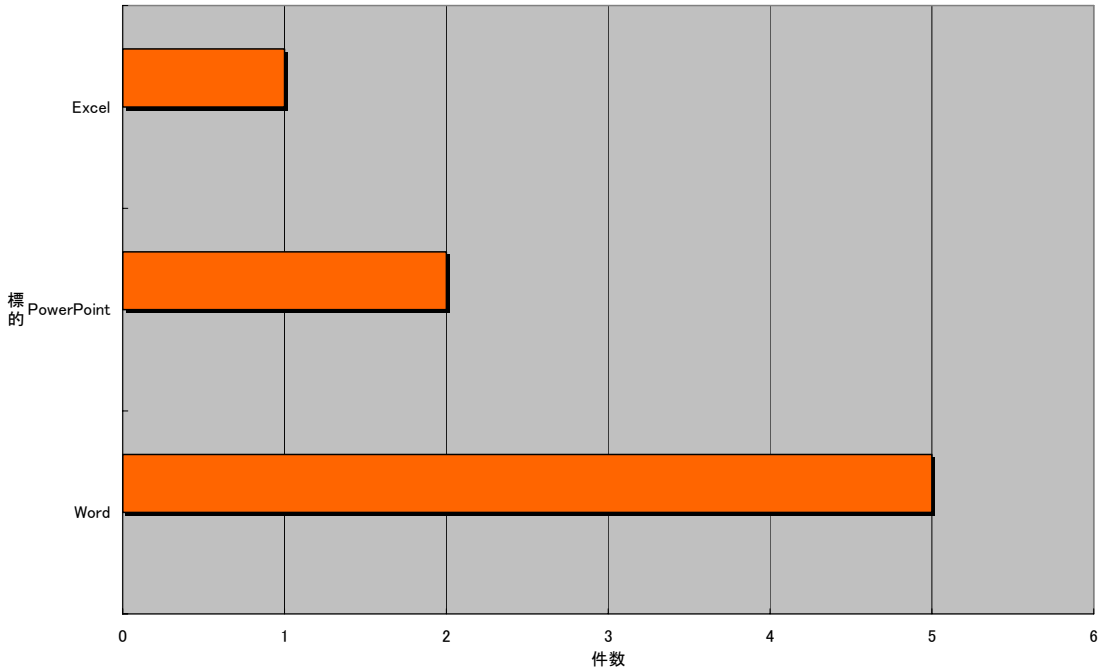

図 3-9　マイクロソフトの Office 製品に対するゼロデイ攻撃の件数

ニュースサイトによる 2006 年の報道および複数のウイルス対策ベンダの公開情報から、オフィスアプリケーションの未知の脆弱性を使用したウイルスが 9 種類確認された。
ゼロデイ攻撃に使用されたウイルスの名称および発見日、使用された脆弱性、生成されるウイルスについて調査した結果を表 3-8 に示す。このうち、2006 年の 8 月 16 日に確認された Trojan.Tarodrop は、ジャストシステムの一太郎における未知の脆弱性を狙うもので、主に日本を標的としたものと考えられる。また、2006 年の 12 月 14 日に確認された Exploit-MSWord.c.demo は脆弱性を実証するデモファイルであった。

---

45 マイクロソフト社オフィス製品に関連した脆弱性と脅威の動向
～オフィス関連製品を介した攻撃が増加傾向～
http://www.lac.co.jp/business/sns/intelligence/report/20070213_cslreport.pdf

表 3-8　ゼロデイ攻撃に使用された DROPPER

発見日	ウイルス名称	利用された脆弱性	生成されるウイルス
2006/5/19	Trojan.Mdropper.H	Wordの脆弱性(MS06-027)	Backdoor.Ginwui
2006/6/12	TROJ_EMBED.AN	Excelの脆弱性(MS06-037)	TROJ_SMALL.AWC
2006/7/11	TROJ_MDROPPER.AS	PowerPointの脆弱性(MS06-048)	BKDR_BIFROSE.KN
2006/8/16	Trojan.Tarodrop	一太郎のUnicodeスタックバッファオーバーフローの脆弱性	Backdoor.Papi
2006/9/1	Trojan.Mdropper.Q	Wordの脆弱性(MS06-060)	Backdoor.Femo
2006/9/26	Trojan.PPDropper.F	PowerPointの脆弱性(MS06-058)	Backdoor.Ginwui.E
2006/12/11	TROJ_MDROPPER.EB	Wordの脆弱性 (CVE-2006-6456, MS07-014)	TSPY_AGENT.IWI
2006/12/13	Trojan.Mdropper.T	Wordの脆弱性 (CVE-2006-5994, MS07-014)	Downloader
2006/12/14	Exploit-MSWord.c.demo	Wordの脆弱性 (CVE-2006-6561, MS07-014)	なし

表 3-8 に示したウイルスは、名称に「DROPPER」という語を含むものが多い。ゼロデイ攻撃に使用されたこれらの DROPPER と呼ばれるウイルスは、拡張子が.doc、.xls、.ppt、.tdc などであり、一見通常のファイルに見える。しかし、アプリケーションの脆弱性を悪用する細工がなされており、内部に実行可能形式のウイルスが埋め込まれている。したがって、DROPPER であるファイルを脆弱性の存在するアプリケーションで閲覧すると、埋め込まれたウイルスがシステム内に生成される。このような DROPPER の動作する様子を示すビデオが、シマンテックによって公開されている[46]。

一般的に、DROPPER は埋め込まれたウイルスの生成を行い、DROPPER によって生成されるウイルスが悪意のある活動を行う場合が多い。生成されるウイルスには、バックドア型のウイルスが多く見られる。しかし、6 月 12 日に発見された TROJ_EMBED.AN に生成される TROJ_SMALL.AWC は DOWNLOADER であった。また、12 月 13 日に発見された Trojan.Mdropper.T も DOWNLOADER を生成する。この DOWNLOADER は Troj/DwnLdr-FXG、Troj/DwnLdr-FXH であると推測される[47]。

---

[46] YouTube で米シマンテックが Word のゼロデイ攻撃ビデオを公開
http://itpro.nikkeibp.co.jp/article/NEWS/20070201/260193/

[47] Trojans spread via unpatched Microsoft Word vulnerability
http://www.sophos.com/pressoffice/news/articles/2006/12/wordvuln.html

4. 考察

4.1. Web アプリケーションの脆弱性を使用するボットに関する考察

SOC の攻撃検知データから、2005 年の 12 月中旬から 2006 年の半ばまでの間に Web アプリケーションの脆弱性を使用するボットによる攻撃が多数確認された。
2005 年 11 月に AWStats の脆弱性および PHP の XML-RPC ライブラリの脆弱性を使用する Lupper ワームが出現したが、この Lupper ワームはボットネットを形成するボットではなかった。Lupper ワームによる攻撃は 2005 年 11 月に発見されて以来、収束の気配を見せていたが 2005 年 12 月中旬に再び攻撃が増加した。
また、この同時期に PHP で開発された多数の Web アプリケーションに発見されている RFI の脆弱性に対する攻撃も増加した。これらの攻撃は、ウイルス対策ソフトウェアのパターンファイルのデータから、AWStats の脆弱性と RFI の脆弱性を使用するボット「KAIGENT」、「KAITEN」、XML-RPC ライブラリの脆弱性と RFI の脆弱性を使用するボット「MARE」によるものと推定される。
このことから、Web アプリケーションの脆弱性を使用するボットも従来のボットと同様にワームが使用する脆弱性を感染活動に組み込む、また感染活動に複数の脆弱性を使用する可能性があると言える。

RFI の脆弱性を使用して感染活動を行う PBOT のソースコードを解析したところ、C&C サーバである IRC サーバへの接続など、基本的な機能は従来のボットと同様であった。これまでのボットに見られたスパムメール不正中継機能(Proxy サーバ機能)、DDoS 攻撃機能などは実装されていなかったが、ファイルのダウンロード機能が実装されていた。ボットを機能毎にコンポーネント化し、ボットネットの機能拡張の効率化を図っていると考えられる。また、Google 検索エンジンを使用して感染先を選定するという特徴があった。
SOC で検知されたボットによる攻撃が 2006 年の半ばまでに収束した理由は、Web アプリケーション側の脆弱性が修正されたことに加え、Google などの検索エンジンが対策として、ボットによるクエリのフィルタリングを実施したためと考えられる[48]。

---

[48] MSN Search refusing phpbb searches?
http://www.f-secure.com/weblog/archives/archive-012006.html#00000774

なお、Web アプリケーションの脆弱性を使用するボットは、それまで主流であった Windows の脆弱性を使用するものを置き換えるものではなく、脆弱性に対する攻撃コードの開発が容易に行える Web アプリケーションを新たな標的とし、ボットネットの領域の拡大を図ったものと推測される。XML-PRC ライブラリの脆弱性の影響が、多数の Web アプリケーションに及んだことと、RFI の脆弱性が多数の Web アプリケーションに存在していたため攻撃数が大幅に増加したと考えられる。また、Web アプリケーションを提供するためには、通常 TCP の 80 番ポートや 443 番ポートを公開する必要があり、ネットワーク型のファイアウォールでは感染を防止できないということがボットの標的とされる 1 つの理由と考えられる。

現在も日々新たな RFI の脆弱性が PHP で開発された多数の Web アプリケーションに発見されている。今後、パッケージ化されている Web アプリケーションへの攻撃だけでなく、独自に開発された Web アプリケーションを標的とするボットが増加する可能性も考えられる。

4.2. 2005 年から 2006 年にかけてのウイルス発生動向に関する考察

2005 年から 2006 年にかけてのウイルス発生動向をウイルス名の接頭語毎のパターン登録数の推移から調査した結果、TROJ ウイルスと TSPY ウイルスのパターン登録数に著しい増加が見られた。TROJ ウイルスは 2 年間に約 6 万件増加しており、これらの中には、他のウイルスを悪意のあるサイトからダウンロードして感染させる DOWNLOADER が多数存在する。一方、TSPY ウイルスは 2 年間で約 3 万件増加しており、これらの中には、ネットバンクやオンラインゲームのアカウントといった金銭価値のある情報を詐取する目的で作成されたウイルスが多数存在する。TROJ ウイルスと TSPY ウイルスの増加には相関性が見られ、TROJ ウイルスが TSPY ウイルスをダウンロードし、感染させていると推測される。
これまで深刻な脅威と捉えられてきたボット(WORM_RBOT、WORM_SDBOT など)を含む WORM・BKDR の接頭語を持つウイルスは、TROJ・TSPY ウイルスと比較するとパターン登録数の増加は少なかった。しかし、トレンドマイクロのウイルス感染被害レポートやマイクロソフトのレポートによるとボットの感染被害が最も多く、大きな脅威であることに変わりはない。また、TROJ_ROOTKIT のようなボットの存在を隠蔽するウイルスやボット自身の自己隠蔽機能によって発見されにくくなり、パターンへの登録に多くの時間が必要となったとも考えられる。

オンラインゲーム、ネットバンクおよびインスタントメッセンジャーのアカウントを盗む主要な TSPY ウイルスのパターン登録数推移を図 4-1 に示す。

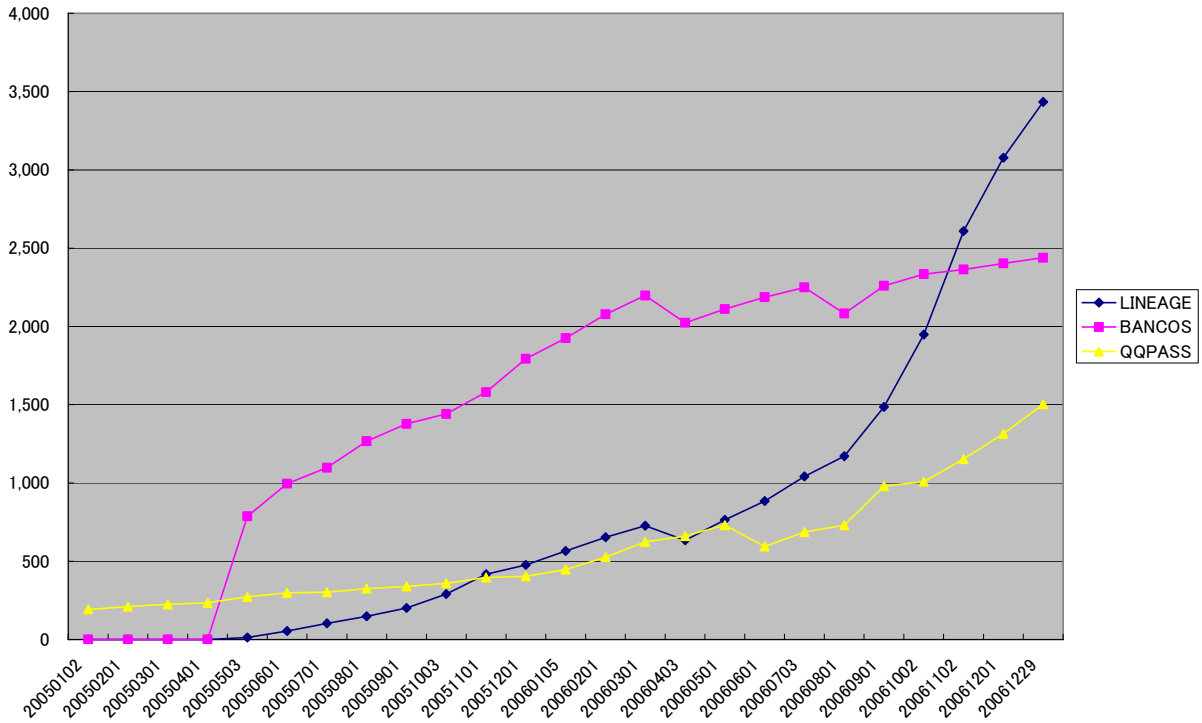

図 4-1　TSPY_LINEAGE、TSPY_BANCOS、TSPY_QQPASS の比較

オンラインゲームのアカウントを盗むウイルスである TSPY_LINEAGE のパターン登録数は 2006 年に大きく増加し、様々なオンランゲームがウイルスの標的となっている事が分かる。こうしたアカウントを盗むウイルスの増加の背景には、盗んだアカウントの不正利用行為だけでなく、RMT の存在がある。盗まれたアカウントが、現金で売買されるという犯罪が多数発生し問題とされている[49]。オンラインゲーム業界は、ゲームのクライアントプログラムにセキュリティソフトウェアを組み込むなどの対策を実施しているが、増え続ける亜種への対応に苦慮していると言う側面もある。

また、インスタントメッセンジャーQQ のアカウントを盗むウイルスである TSPY_QQPASS のパターン登録数も、オンラインゲームのアカウントを盗むものと同じく 2006 年に大きく増加している。QQ は主に中国で利用されており、QQ と同一のアカウントで利用できるオンラインゲームも提供している。また、同オンラインゲームで獲得したポイントを仮想貨幣である「Q 幣」に換金するというサービスも提供されていた。

---

[49]【AOGC2007】2006 年はオンラインゲームを巡る犯罪が急増
http://www.rbbtoday.com/news/20070226/38888.html

このため QQ のアカウントには他のインスタントメッセンジャーより金銭価値があり、ウイルスの標的となったと考えられる。
一方では、ネットバンクのアカウントを盗むウイルスの増加傾向は鈍化している。TSPY_BANCOS は、2005 年の 4 月から 5 月にはじめてパターンに登録され、3 ヵ月後の 2005 年 7 月に TSPY_BANCOS を利用した不正送金事件が発生した。2006 年のパターン登録数の増加は 2005 年に比べると緩やかになっている。
2006 年に TSPY_BANCOS の増加が緩やかになり、TSPY_LINEAG が急増している理由として、ネットバンクのセキュリティ対策の効果も考えられるが、ウイルスを利用して金銭詐取を狙う悪意のある人物・集団が、より目立たず効率的な対象としてオンラインゲームや IM アカウントの RMT に着目していると推測される。
今後、このように標的を広く浅くし、金銭詐取を狙うウイルスの増加が懸念される。

4.3. DOWNLOADER に関する考察

単機能化されたウイルスや機能毎にコンポーネント化されたボットなどを悪意のあるサイトからダウンロードし、感染させる DOWNLOADER の実態を調査した。
増加が著しい DOWNLOADER は TROJ_AGENT、TROJ_DLOADER であり、これら 2 種でパターンファイルに登録されている TROJ ウイルスの約 30%を占めていた。TROJ ウイルスには、その他にも数種類の DOWNLOADER が存在した。
このことから、DOWNLOADER は多種多様なウイルスが分類されている TROJ の中でも多くの割合を占めていると考えられる。

DOWNLOADER の機能は、悪意のあるサイトからファイルをダウンロードし、それを実行または特定のフォルダへ配置することで、別のウイルスを感染させることである。ダウンロードされるウイルスの種類や数は DOWNLOADER によって様々であり、1 つの DOWNLOADER が複数のサイトからウイルスをダウンロードする場合もある。
また、ダウンロードされるウイルスは単体で動作するものだけでなく、ボットなどのコンポーネントの場合もある。
DOWNLOADER が使用される理由は、ウイルス作者が任意のタイミングでダウンロードされるファイルを変更でき、ウイルスの機能拡張や修正が可能になるためと推測される。ダウンロードされるファイルを差し替えることで、1 つの DOWNLOADER で複数のウイルスを感染させることが可能である。このように、DOWNLOADER はウイルスのインストーラーやアップデートクライアントの役割を担っていると言える。また、コンポーネント化したボットや別の DOWNLOADER をダウンロードさせることで、全容把握および完全駆除を困難にしていると推測される。このため、ダウンロードされた 1 つのウイルスのみを駆除しても DOWNLOADER が残存していると再感染する可能性がある。

また、脆弱性を使用して感染する DOWNLOADER が複数存在した。脆弱なアプリケーションによる悪意のあるサイトの閲覧や細工されたメディアファイルの再生などによって DOWNLOADER に感染する可能性がある。
2006 年に多く報告されたオフィスアプリケーションの未知の脆弱性を突くゼロデイ攻撃に使用された DROPPER に DOWNLOADER を生成するものが存在した。
今後、このようなゼロデイ攻撃に DOWNLOADER を組み込む手法が一般化することで、単一のゼロデイ攻撃で複数のウイルスに感染することも懸念される。

5. 対策

調査の結果、Web アプリケーションの脆弱性を標的とするボットが出現したこと、目的が金銭詐取に特化されたウイルスの増加が著しいこと、また、DOWNLOADER によってウイルスの感染活動が複雑化していることが判明した。このように、マルウェアはその目的・標的および感染活動が変化しており、それらをふまえた対策が必要である。

5.1. Web アプリケーションの脆弱性を狙うボットへの対策

Web アプリケーションは、自動更新機能が実装されているクライアント OS やアプリケーションに比べてソフトウェアの更新が管理者に依存している場合が多い。ベンダが脆弱性を修正したバージョンをリリースしても、脆弱性による問題が顕在化せず安定稼動を続けている場合、すぐにバージョンアップやパッチの適用が行われず、脆弱性が残存している可能性が高い。このことがボットの標的とされた理由の 1 つと考えられる。
そのため、まずは脆弱性の修正による感染の抑制が最も優先すべき対策である。
また、Web アプリケーションファイアウォールを利用して、ボットによる攻撃を遮断することも感染を抑制する有効な対策の 1 つである。

感染抑制策に加えて、ファイアウォールや IPS において不必要なアウトバウンド通信を制限することは、ボットに感染してしまった場合に C&C サーバとの通信を遮断し、ボットの活動を抑制する有効な対策である。
ボットへの感染を早期に検知するためには、ファイアウォールや IPS のログを常時監視し、遮断された内部ネットワークからの通信を発見することである。ラックの所有する JSOC では、IDS/IPS による検知よりもファイアウォールのログの監視によって、多くのボット感染ホストの通信を発見している[50]。ファイアウォールがどのような通信を遮断しているかをリアルタイムで監視することは、ボットのみならずワームや不審な通信を発見するために有効な対策である。

---

[50] ラック 侵入傾向分析レポート Vol.8
http://www.lac.co.jp/business/sns/intelligence/report/20070313lac_report.pdf

5.2. アカウント情報を盗むウイルスおよび DOWNLOADER に対する対策

ネットバンクやオンラインゲームのアカウントなど金銭価値のある情報を盗むウイルスの感染を抑制するには、ウイルス対策ソフトウェアを最新のパターンファイルと共に利用することが重要である。これは、ウイルス全般に対する基本的な対策であるが、本調査において各種アカウントを盗むウイルスは、非常に多くの亜種が出現していることが判明した。このことから、ウイルス対策ソフトウェアを使用しない場合や、パターンファイルが最新でない場合に非常に多数のウイルスに対して無防備な状態であると言える。
非常に多くの亜種が出現しているため、ウイルス対策ソフトウェアだけでなく、オンラインゲームやネットバンクのサービスベンダの提供するセキュリティ情報やセキュリティ機能を利用して、多層防御を行うことが有効であろう。
また、この種のウイルスはゲームの攻略サイトなどで有益な情報やツールなどを装い、ユーザを騙す手口で感染する場合があることを念頭に置き、不用意なファイルのダウンロードや閲覧・実行を避けることも重要である。

感染を検知するための対策として、パーソナルファイアウォールの使用がある。アカウント情報を盗むウイルスは、ネットワークを介して収集した情報を悪意のある人物へ送信する。そのため、パーソナルファイアウォールで許可されていない不審なプログラムによる通信が発生した場合、ウイルスに感染している可能性がある。
また、ウイルス対策ソフトウェアなどによってアカウント情報を盗むウイルスが 1 種以上発見された場合、そのウイルスを感染させた DOWNLOADER や DOWNLOADER によってダウンロードされた他のウイルスにも感染している可能性がある。ウイルスを駆除しても直ぐに再感染してしまう場合、確実に駆除を行うために OS の再インストールを検討すべきである。

DOWNLOADER への対策は、前述のウイルス対策に加え Windows XP SP2 以降に実装されている DEP[51]、セキュリティソフトウェアに搭載されているバッファオーバーフロー攻撃防止機能が、脆弱性を使用するものに対して有効である。多層防御の観点から、ゲートウェイでの HTTP 通信に対するウイルススキャンも有効である。
パーソナルファイアウォールや URL フィルタリングの実施、インターネットとの通信を認証付きプロキシサーバ経由に制限することで、DOWNLOADER に感染してしまった場合に別のウイルスをダウンロードされる可能性が低減し、被害を抑制できる。また、URL フィルタやプロキシサーバのログを監査することにより、感染を検知できる場合がある。

---

[51] Windows XP SP2 のデータ実行防止機能について
http://support.microsoft.com/kb/884515/ja

5.3. セキュリティ対策およびインシデントレスポンスを円滑に進める体制

前述した各対策はそれぞれ、サーバ上の Web アプリケーション、ネットワークインフラおよびクライアントコンピュータという異なる対象に実施するものである。企業などの一般的な組織においてそれらの対策を漏れなく効率的に実施するためには、それぞれの対象の管理者・担当者が個別に実施するのではなく、組織的な体制を整備し、インシデントの発生を前提として実施することが重要であると考えられる。また、こうした体制にはインシデント発生時に組織としての意思決定が求められる場面に直面することが想定される。したがって、このような体制には経営層の関与が望ましい。

以上のことから、企業においては、多層防御の概念のもとでの技術的手段の整備と、経営陣の判断・関与が可能な組織内 CSIRT の構築が必要である。

6. 総論

本調査の結果、ボットは Web アプリケーションの脆弱性も感染手段のひとつとしていることが判明した。このことは、ボットは主にクライアント OS の脆弱性やパスワード設定の不備を悪用して感染を広げるという従来の認識を改めるべき実態と考えられる。 Web アプリケーションをサービス用途として提供するサーバも、ボットの標的の一つとなっており、ボットの脅威が広まりつつあることを示している。このことから、ボットは引き続き注視すべき脅威であることは間違いないであろう。

加えて、単機能化されたマルウェアがその数を増やしており、企業や家庭の PC から金銭目的でデータを盗もうとしていることも判明した。現在の高度情報通信社会において仮に、ネットバンクのアカウント情報が盗み出されたとすれば、その持ち主の財産が失われてしまいかねないこととなりうる。よって、企業においてこれらアカウント情報をビジネス用途で使用している場合、その盗用を目的としたマルウェアの増加は、対策を取るべき大きな脅威である。また、オンラインゲームや IM など主に個人・家庭で利用されるサービスのアカウント情報を狙うマルウェアの増加が顕著であり、金銭詐取の標的が企業から個人へ移行していると考えられる。これは、セキュリティ対策およびセキュリティリテラシーの低い個人ユーザが多く存在することに加えて、新しい視点や手口による犯罪行為には公的機関の捜査が及びにくいという理由も考えられる。

さらには、これら単機能化されたマルウェアは従来の機能豊富な形態をとらず、簡素な機能のみを保持することで、その活動を抑制化・潜行化している傾向がみられた。企業においてこれら抑制化された活動を行うマルウェアを検出・駆除していくためには、技術的な手段と共に組織的な体制の整備が重要であると考えられる。また、こうした体制にはインシデント発生時に組織としての意思決定が求められる場面に直面することが想定される。したがって、このような体制には経営層の関与がふさわしいであろう。
以上のことから、企業においては、多重防衛の概念のもとでの事前の対策案と技術的手段の整備、そして、経営陣の判断・関与が可能な組織内 CSIRT の構築が急務であろう。

7. 参考資料

7.1. 用語の定義

マルウェア：
「悪」を意味する接頭詞の“mal-”にソフトウェア全般を意味する“ware”を繋げた語で、悪意あるソフトウェアの総称である。クラックツールやウイルス・ワーム、スパイウェア・アドウェア等、非常に広い範囲を含む。

ボット：
マルウェアの一種で、マシンに感染させ、悪意を持った第三者がネットワーク越しに外部から操ることを目的として作成されたプログラムである。命令を送り込むことにより、それに従って感染したマシンから情報を盗む、他のマシンを攻撃する、といった行動をさせることが出来る。

ボットネット：
ボットに感染し、悪意を持った第三者に遠隔操作されているマシンで構成されているネットワークのこと。

バックドア：
侵入されたマシンに設けられた、不正侵入を行なうための「裏口」のこと。主に、次回侵入の際に所有者に気づかれないようにするために設置される。ボット感染の環境下では、外部からの操作を受け入れる目的もある。

ワーム：
マルウェアの一種で、マシンに感染した後に自己増殖、ファイルの改ざんや破壊、外部への感染を行なうソフトウェアのこと。ボットと違い、外部からの命令によって行動を起こす機能は備えていない。

ハーダー：
ボットネット全体を管理統括している人間のことで、リモートから感染 PC をコントロールし、スパムメールの送信や、DDoS 攻撃を仕掛ける指令を出すことができる。元は牧夫の意。

C&C：
Command and Control の略語で、感染したコンピュータへの指令を中継するサーバのこと。

ハーダーの指令は C&C サーバを介して、ボット感染マシンへ到達する。

DOWNLOADER：
マルウェアの一種で、悪意のあるサイトに接続して別のマルウェアをダウンロードし、感染させるもののこと。

DROPPER：
マルウェアの一種で、ワームやバックドアを生成する機能を持つもののこと。DROPPER は、ワームやバックドアをコンピュータの中に組み込む仕組みを備えている。

ゼロデイ攻撃：
OS やアプリケーションに脆弱性が発見された際に、修正プログラムが提供される前にその脆弱性を悪用して行なわれる攻撃のこと。修正プログラムが提供された日を対策 1 日目とし、それ以前に攻撃が行われるためこう呼ばれる。

7.2. PBOT ソースコード

＜非公開＞

7.3. ウイルス関連情報

WORM_SOBIG.F - 詳 細
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=WORM%5FSOBIG%2EF&VSect=T

PHP include worm infects search engine-listed sites（ISS X-Force）
http://xforce.iss.net/xforce/xfdb/18706

Spyki.A
http://www.pandasoftware.com/virus_info/encyclopedia/overview.aspx?lst=det&idvirus=56741

ELF_LUPPER.A - 詳 細
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=ELF%5FLUPPER%2EA&VSect=T

ELF_LUPPER.B - 詳 細
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=ELF%5FLUPPER%2EB&VSect=T

ELF_LUPPER.C - 詳 細
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=ELF%5FLUPPER%2EC&VSect=T

ELF_LUPPER.F - 詳 細
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=ELF%5FLUPPER%2EF&VSect=T

ELF_LUPPER.H - 詳 細
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=ELF%5FLUPPER%2EH&VSect=T

Linux.Plupii - Symantec.com
http://www.symantec.com/ja/jp/security_response/writeup.jsp?docid=2005-110612-3334-99

PERL_SANTY.F - 詳 細
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=PERL%5FSANTY%2EF&VSect=T

Perl.Santy - Symantec.com
http://www.symantec.com/ja/jp/security_response/writeup.jsp?docid=2004-122109-4444-99

ELF_SSHSCAN.A - 詳 細
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=ELF%5FSSHSCAN%2EA&VSect=T

ELF_SSHD22.B - 詳 細
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=ELF%5FSSHD22%2EB&VSect=T

ELF_SMALL.AYW - 詳 細
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=ELF_SMALL.AYW&VSect=T

ELF_SMALL.AYY - 詳 細
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=ELF_SMALL.AYY&VSect=T

ELF_KAIGENT.A - 詳 細
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=ELF%5FKAIGENT%2EA&VSect=T

ELF_KAIGENT.B - 詳 細
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=ELF%5FKAIGENT%2EB&VSect=T

ELF_KAIGENT.C - 詳 細
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=ELF%5FKAIGENT%2EC&VSect=T

ELF_MARE.C - 詳 細
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=ELF%5FMARE%2EC&VSect=T

ELF_MARE.E - 詳 細
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=ELF%5FMARE%2EE&VSect=T

ELF_MARE.G - 詳 細
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=ELF%5FMARE%2EG&VSect=T

ELF_MARE.J - 詳 細
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=ELF%5FMARE%2EJ&VSect=T

ELF_MARE.K - 詳 細
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=ELF%5FMARE%2EK&VSect=T

ELF_KAITEN.U - 詳 細
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=ELF%5FKAITEN%2EU&VSect=T

ELF_KAITEN.AM - 詳 細
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=ELF%5FKAITEN%2EAM&VSect=T

ELF_KAITEN.AQ - 詳 細
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=ELF%5FKAITEN%2EAQ&VSect=T

WORM_AGOBOT.A - 詳 細
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=WORM%5FAGOBOT%2EA&VSect=T

WORM_AGOBOT.P - 詳 細
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=WORM%5FAGOBOT%2EP&VSect=T

WORM_RBOT.CBQ - 詳 細
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=WORM%5FRBOT%2ECBQ&VSect=T

WORM_RBOT.GEN - 詳 細
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=WORM%5FRBOT%2EGEN&VSect=T

WORM_RBOT.TF - 詳 細
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=WORM%5FRBOT%2ETF&VSect=T

WORM_SDBOT.CJR - 詳 細
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=WORM%5FSDBOT%2ECJR&VSect=T

WORM_SDBOT.CUJ - 詳 細
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=WORM%5FSDBOT%2ECUJ&VSect=T

WORM_SDBOT.GEN - 詳 細
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=WORM%5FSDBOT%2EGEN&VSect=T

WORM_SDBOT.DAM - 詳 細
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=WORM%5FSDBOT%2EDAM&VSect=T

BKDR_SDBOT.GAA - 詳 細
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=BKDR%5FSDBOT%2EGAA&VSect=T

BKDR_SDBOT.GEN - 詳 細
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=BKDR%5FSDBOT%2EGEN&VSect=T

TROJ_AGENT.AC - 詳 細
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=TROJ%5FAGENT%2EAC&VSect=T

TROJ_AGENT.CE - 詳 細
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=TROJ%5FAGENT%2ECE&VSect=T

TROJ_AGENT.PNN - 詳 細
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=TROJ%5FAGENT%2EPNN&VSect=T

TROJ_AGENT.POP - 詳 細
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=TROJ%5FAGENT%2EPOP&VSect=T

TROJ_IESER.A - 詳 細
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=TROJ%5FIESER%2EA&VSect=T

TROJ_SMALL.AFG - 詳 細
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=TROJ%5FSMALL%2EAFG&VSect=T

TROJ_SMALL.APH - 詳 細
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=TROJ%5FSMALL%2EAPH&VSect=T

TROJ_SMALL.EDW- 詳 細
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=TROJ%5FSMALL%2EEDW&VSect=T

TROJ_SMALL.SN - 詳 細
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=TROJ%5FSMALL%2ESN&VSect=T

TROJ_DELF.DS - 詳 細
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=TROJ%5FDELF%2EDS&VSect=T

TROJ_DELF.RM - 詳 細
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=TROJ%5FDELF%2ERM&VSect=T

TROJ_DLOADER.ABF - 詳 細
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=TROJ%5FDLOADER%2EABF&VSect=T

TROJ_DLOADER.F - 詳 細
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=TROJ%5FDLOADER%2EF&VSect=T

TROJ_DLOADER.XH - 詳 細
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=TROJ%5FDLOADER%2EXH&VSect=T

TROJ_DLOADER.IMM - 詳 細
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=TROJ%5FDLOADER%2EIMM&VSect=T

TROJ_DLOADER.OO - 詳 細
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=TROJ%5FDLOADER%2EOO&VSect=T

TROJ_ROOTKIT.E - 詳 細
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=TROJ%5FROOTKIT%2EE&VSect=T

TROJ_ROOTKIT.H - 詳 細
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=TROJ%5FROOTKIT%2EH&VSect=T

TROJ_ROOTKIT.N - 詳 細
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=TROJ%5FROOTKIT%2EN&VSect=T

TROJ_ROOTKIT.S - 詳 細
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=TROJ%5FROOTKIT%2ES&VSect=T

TROJ_ISTBAR.FN- 詳 細
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=TROJ%5FISTBAR%2EFN&VSect=T

TROJ_ISTBAR.DU- 詳 細
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=TROJ%5FISTBAR%2EDU&VSect=T

TROJ_ISTBAR.PM- 詳 細
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=TROJ%5FISTBAR%2EPM&VSect=T

TROJ_MDROPPER.BL - 詳 細
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=TROJ_MDROPPER.BL&VSect=T

Trojan.Tarodrop - Symantec.com
http://www.symantec.com/ja/jp/security_response/writeup.jsp?docid=2006-081615-5201-99

TROJ_TINY.DU - 詳 細
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=TROJ%5FTINY%2EDU&VSect=T

Troj/DwnLdr-FXG - Trojan - Sophos threat analysis
http://www.sophos.com/security/analyses/trojdwnldrfxg.html

TROJ_ANTINNY.A- 詳 細
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=TROJ%5FANTINNY%2EA&VSect=T

TROJ_ANTINNY.AX- 詳 細
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=TROJ%5FANTINNY%2EAX&VSect=T

TROJ_LINEAGE.A- 詳 細
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=TROJ%5FLINEAGE%2EA&VSect=T

TSPY_BANCOS.ANM - 詳 細
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=TSPY%5FBANCOS%2EANM&VSect=T

TSPY_QQPASS.AY - 詳 細
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=TSPY%5FQQPASS%2EAY&VSect=T

TSPY_LEGMIR.CE - 詳 細
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=TSPY%5FLEGMIR%2ECE&VSect=T

TSPY_LEGMIR.SS - 詳 細
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=TSPY%5FLEGMIR%2ESS&VSect=T

TSPY_LEMIR.HK - 詳 細
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=TSPY%5FLEMIR%2EHK&VSect=T

TSPY_WOW.BU - 詳 細
http://www.trendmicro.co.jp/vinfo/grayware/ve_graywareDetails.asp?GNAME=TSPY%5FWOW%2EBU&VSect=Td

TSPY_RAGROK.U - 詳 細
http://www.trendmicro.co.jp/vinfo/grayware/ve_graywareDetails.asp?GNAME=TSPY_RAGROK.U&VSect=Td

TSPY_RAGROK.P - 詳 細
http://www.trendmicro.co.jp/vinfo/grayware/ve_graywareDetails.asp?GNAME=TSPY_RAGROK.P&VSect=Td

TSPY_POVIEWER.A - 詳 細
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=TSPY%5FPOVIEWER%2EA&VSect=T

TSPY_KAKKEYS.AI - 詳 細
http://www.trendmicro.co.jp/vinfo/grayware/ve_graywareDetails.asp?GNAME=TSPY_KAKKEYS.AI&VSect=Td

TSPY_KAKKEYS.F - 詳 細
http://www.trendmicro.co.jp/vinfo/grayware/ve_graywareDetails.asp?GNAME=TSPY_KAKKEYS.F&VSect=Td

PWSteal.Bancos.D
http://www.symantec.com/region/jp/sarcj/data/p/pwsteal.bancos.d.html

Infostealer.Bancos.T - Symantec.com
http://www.symantec.com/ja/jp/enterprise/security_response/writeup.jsp?docid=2005-042522-3953-99

Symantec Security Response - PWSteal.Jginko
http://www.symantec.com/region/jp/avcenter/venc/data/pf/jp-pwsteal.jginko.html

TROJ_ DLOADER.HW - 詳 細
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=TROJ%5FDLOADER%2EHW&VSect=T

TROJ_AGENT.BO - 詳 細
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=TROJ%5FAGENT%2EBO&VSect=T

TROJ_ DLOADER.JHV - 詳 細
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=TROJ%5FDLOADER%2EJHV&VSect=T

JS_SPACESTALK.A - 詳 細
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=JS%5FSPACESTALK%2EA&VSect=T

TROJ_EMBED.AN - 詳 細
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=TROJ%5FEMBED%2EAN&VSect=T

TROJ_SMALL.AWC - 詳 細
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=TROJ%5FSMALL%2EAWC&VSect=T

TROJ_MDROPPER.AS - 詳 細
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=TROJ%5FMDROPPER%2EAS&VSect=T

Trojan.PPDropper.B - Symantec.com
http://www.symantec.com/ja/jp/security_response/writeup.jsp?docid=2006-071212-4413-99

BKDR_BIFROSE.KN - 詳 細
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=BKDR%5FBIFROSE%2EKN&VSect=T

Backdoor.Papi - Symantec.com
http://www.symantec.com/ja/jp/security_response/writeup.jsp?docid=2006-081615-5607-99

TROJ_MDROPPER.BH - 詳 細
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=TROJ%5FMDROPPER%2EBH&VSect=T

TROJ_SMALL.CMZ - 詳 細
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=TROJ%5FSMALL%2ECMZ&VSect=T

TROJ_MDROPPER.BO - 詳 細
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=TROJ%5FMDROPPER%2EBO&VSect=T

BKDR_PCCLIENT.PX - 詳 細
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=BKDR%5FPCCLIENT%2EPX&VSect=T

Troj/DwnLdr-FXH - Trojan - Sophos threat analysis
http://www.sophos.com/security/analyses/trojdwnldrfxh.html

EXPL_EXECOD.A - 詳 細
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=EXPL%5FEXECOD%2EA&VSect=T

JS_DLOADER.AZZ - 詳 細
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=JS%5FDLOADER%2EAZZ&VSect=T

TROJ_ANICMOO.AX- 概 要
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=TROJ%5FANICMOO%2EAX&VSect=T

JS_PLOIT.BC - 詳 細
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=JS%5FPLOIT%2EBC&VSect=T

TROJ_NASCENE.A - 詳 細
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=TROJ%5FNASCENE%2EA&VSect=T

7.4. 脆弱性関連情報

RPCSS サービスのバッファ オーバーランによりコードが実行される (824146) (MS03-039)
http://www.microsoft.com/japan/technet/security/bulletin/MS03-039.mspx

ASN .1 の脆弱性により、コードが実行される (828028) (MS04-007)
http://www.microsoft.com/japan/technet/security/bulletin/ms04-007.mspx

Zeroboard Two Vulnerabilities（Secunia）
http://secunia.com/advisories/13649/

AWStats - Free log file analyzer for advanced statistics (GNU GPL).
http://awstats.sourceforge.net/

Advisory regarding SSH protocol version 1 CRC-32 compensation attack detector vulnerability
http://www.ssh.com/company/newsroom/article/213/

AWStats "migrate" Shell Command Injection Vulnerability
http://secunia.com/advisories/19969/
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-2237

XML-RPC for PHP Homepage
http://phpxmlrpc.sourceforge.net/

PEAR :: Package :: XML_RPC
http://pear.php.net/package/XML_RPC/

Multiple PHP XML-RPC implementations vulnerable to code injection
http://www.kb.cert.org/vuls/id/442845
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-1921

XOOPS 公式サイト
http://www.xoops.org/

phpBB Creating Communities Worldwide
http://www.phpbb.com/

phpBB viewtopic.php fails to properly sanitize input passed to the "highlight" parameter
http://www.kb.cert.org/vuls/id/497400

WebScripts: WebHints
http://awsd.com/scripts/webhints/

WebHints Shell Command Injection Vulnerability
http://secunia.com/advisories/15652/

Darryl Burgdorf Webhints Remote Command Execution Vulnerability
http://www.securityfocus.com/bid/13930

#57479: Security Vulnerability With Loading Arbitrary Kernel Modules in Solaris Kernel
http://jp.sunsolve.sun.com/search/document.do?assetkey=1-26-57479-1

Mamboserver.com - Home
http://mamboserver.com/

Mambo Function.php Arbitrary Command Execution
http://osvdb.org/displayvuln.php?osvdb_id=10180

NFN Address Book for Mambo "mosConfig_absolute_path" File Inclusion Vulnerability
http://www.frsirt.com/english/advisories/2007/1073

PHP-Nuke admin_styles.php phpbb_root_path Variable Remote File Inclusion
http://osvdb.org/displayvuln.php?osvdb_id=16244

WebCalendar "includedir" Arbitrary File Inclusion Vulnerability
http://secunia.com/advisories/16528/

PHP-Nuke "phpbb_root_path" Arbitrary File Inclusion
http://secunia.com/advisories/15244/

カーソルおよびアイコンのフォーマットの処理の脆弱性により、リモートでコードが実行される (891711) (MS05-002)
http://www.microsoft.com/japan/technet/security/bulletin/ms05-002.mspx

QuickTime 7.1.5 のセキュリティコンテンツについて
http://docs.info.apple.com/article.html?artnum=305149-ja

Microsoft Excel の脆弱性により、リモートでコードが実行される (917285) (MS06-037)
http://www.microsoft.com/japan/technet/security/Bulletin/MS06-037.mspx

Microsoft Office の脆弱性により、リモートでコードが実行される (922968) (MS06-048)
http://www.microsoft.com/japan/technet/security/bulletin/ms06-048.mspx

マイクロソフト セキュリティ アドバイザリ (911302)
Internet Explorer の不適切な Document Object Model オブジェクトの処理方法による脆弱性のため、リモートでコードが実行される
http://www.microsoft.com/japan/technet/security/advisory/911302.mspx

Internet Explorer 用の累積的なセキュリティ更新プログラム (905915) (MS05-054)
http://www.microsoft.com/japan/technet/security/bulletin/ms05-054.mspx

Graphics Rendering Engine の脆弱性によりコードが実行される可能性がある (912919) (MS06-001)
http://www.microsoft.com/japan/technet/security/bulletin/MS06-001.mspx

Microsoft Data Access Components (MDAC) の機能の脆弱性により、コードが実行される可能性がある (911562) (MS06-014)
http://www.microsoft.com/japan/technet/security/bulletin/MS06-014.mspx

Vector Markup Language の脆弱性により、リモートでコードが実行される (925486) (MS06-055)
http://www.microsoft.com/japan/technet/security/bulletin/MS06-055.mspx

Windows Explorer の脆弱性により、リモートでコードが実行される (923191) (MS06-057)
http://www.microsoft.com/japan/technet/security/bulletin/ms06-057.mspx

GDI の脆弱性により、リモートでコードが実行される (925902) (MS07-017)
http://www.microsoft.com/japan/technet/security/Bulletin/MS07-017.mspx