JPCERT CC®

USB メモリ経由の感染機能を持つ
マルウエア調査報告書

一般社団法人 JPCERT コーディネーションセンター

2009 年 6 月 19 日

JPCERT CC®

目次

JPCERT CC®

商品名称等に関する表示: Windows XP、Windows Vista は Microsoft Corporation の米国およびその他の国における登録商標または商標です。本書に記載されている会社名，製品名は，それぞれの会社の商標もしくは登録商標です。

1. 背景

インターネットが普及する前の時代のマルウエアはフロッピーディスク等のリムーバブルメディアを介して感染するものがほとんどであった。ブロードバンド時代の到来によって、マルウエアはより広範囲の対象に直接的にアプローチすることができるネットワーク感染という手段を得た。ところが、近年、USB メモリに代表されるリムーバブルメディア(以下、リムーバブルメディア)がマルウエアの感染媒体として悪用されるようになってきた。特に2008年以降は企業等におけるリムーバブルメディア経由のマルウエア感染事故はメディア等でも取り上げられるような社会的な問題となっている。

マルウエアをはじめセキュリティ上の脅威が主にネットワークを媒介に広まるという時代の中で、ネットワークのセキュリティ対策への意識は高まりつつある。一方でネットワークに繋がっていなければ安全であるという誤解もある。そのような状況の中、低価格化・大容量化によって普及したリムーバブルメディアが脅威の媒介として利用されるようになった。

JPCERT/CC ではマルウエアの発生や感染被害の状況に関するデータの収集やマルウエアが利用する技術等の分析を通してマルウエアの現状を把握する試みを続けている。それらの情報を適切なタイミング、相手に対して適切な形で展開することにより、効果的な対策に結びつけていただくことを目指して活動を行っている。

本報告書ではまず、リムーバブルメディア経由の感染機能を持つマルウエアの実態を把握していただくために出現数や感染被害数、そして感染被害事例等の調査結果を紹介する。さらに、実際の感染のメカニズムへの理解を深めていただくために身近な機器での感染実験を行った。

リムーバブルメディア経由の感染機能を持つマルウエアへの対策についてはベンダ等からも情報発信されている。しかしながら、その作業が難しいだけでなく、対策による影響の価値判断も容易ではない。それらの障壁を克服して対策を円滑に実施するために、本報告書を参照いただければ幸いである。

なお、本報告書の調査は株式会社ラックとトレンドマイクロ株式会社の協力により実現している。本報告書に掲載されている統計等の各種数値は特に明記しない限り、2007年1月～2009年1月(以下、調査対象期間)の間にトレンドマイクロワールドトラッキングセンター(WTC[1])に寄せられた感染報告の集計結果によるものである。

[1] http://wtc.trendmicro.com/wtc/default.asp

1.1. リムーバブルメディア経由で感染するマルウエアとは

マルウエアは登場以来、様々な手法でコンピュータに感染して個人情報の不正取得やシステムの破壊活動など多大な被害をもたらしてきた。

その手法は度々変化しており、インターネットの普及以前はフロッピーディスク等のリムーバブルメディア経由のものがほとんどであったが、インターネットの普及後はより莫大な対象に対し直接的にアプローチできるネットワーク型のマルウエアが優勢となり、Nimda や Slammer といった大規模な被害をもたらすものが登場してきた。

そして、近年は再び USB メモリ等のリムーバブルメディアによるマルウエアの感染が問題となっている。その要因として、インターネットを利用する際にはセキュリティ対策が必要であるということが一般にも浸透してきており攻撃が成功しにくくなっていることと、USB メモリの大容量化・低価格化により一般に広く普及してきたことが考えられる。

従来は、インターネットに接続していなければ攻撃を受けることは少なくなるため、「接続しない」という防護をセキュリティ対策の一部とする傾向があった。しかし、リムーバブルメディア経由のマルウエアは、そのようなネットワークに接続していないコンピュータにも感染する。この点が本報告書で取り扱うリムーバブルメディア経由で感染するマルウエアの大きな特徴である。

そして、ほとんどのマルウエアはリムーバブルメディア経由の感染以外にネットワーク越しの感染機能も持つため、一旦組織内のどこかのコンピュータに感染してしまうと、たちどころに感染が広がるようになっており、駆除対策にかなりの労力を取られてしまい業務への妨害となってしまう。このような複数の感染手法を使いわけるのも特徴である。

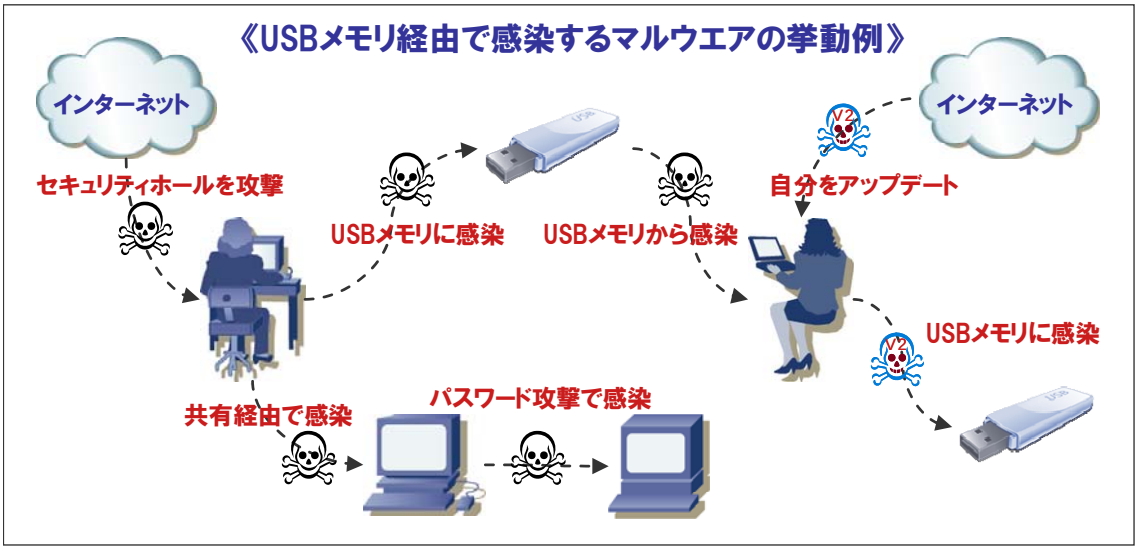

図 1. USB メモリ経由で感染するマルウエアの挙動例

1.2. マルウエアが利用する機能

本項では、マルウエアが感染手法として利用する「自動実行機能」と「自動再生機能」の概説をする。

「自動実行機能」と「自動再生機能」は、コンピュータに対して USB メモリの接続や CD-ROM の挿入などに応答してシステムが動作することを目的として実装された機能である。両機能はコンピュータに接続/挿入した媒体のルート上に配置された”AUTORUN.INF”ファイルの記載内容を解釈して、特定のプログラムを実行する、音楽を再生する、などの動作を行う。

マルウエアにとっての両機能の利用方法は、プログラムを起動するきっかけが違うだけであるため、本検証においては特に明確には区別しない。表1に両機能の特徴と差異を示す。

表1.「自動実行機能」と「自動再生機能」の特徴

	自動実行(Autorun)	自動再生(AutoPlay)
動作	媒体内のプログラムの実行	媒体内のデータ処理
	媒体外のプログラムの実行	
処理対象のファイル	媒体内のプログラム	媒体内のデータ
	媒体外のプログラム	
動作タイミング	媒体挿入時	媒体挿入時
	ドライブアイコンのダブルクリック時	自動再生ダイアログのメニュー選択時
	ドライブアイコンの右クリックの AUTORUN.INF による作成メニューの選択時	
	ドライブアイコンの右クリックのエクスプローラの選択時	
	ドライブアイコンの右クリックの開くの選択時	
設定	AUTORUN.INF による設定	AUTORUN.INF による設定
		ドライブのデータ毎の設定
処理媒体のタイプ	不明な種類のドライブ	
	リムーバブルドライブ	
	固定ドライブ	
	ネットワークドライブ	
	CD-ROM ドライブ	
	RAM ディスク	

「自動実行機能」における”AUTORUN.INF”ファイルの例

メニュー選択時にプログラムを実行

```
[autorun]

Shell¥verb¥command=Malware.exe
```

ディスク挿入時にプログラムを実行

```
[autorun]

Open=Malware.exe
```

ディスク挿入時にプログラムを実行

```
[autorun]

Shellexecute=Malware.exe
```

「自動再生機能」における”AUTORUN.INF”ファイルの例

自動再生ハンドラへのエントリ

```
[autorun]

Action = 不正プログラムの起動          ←ダイアログに表示する文字

shellExecute = Malware.exe          ←メニュー選択後に実行するファイル

Icon = Malware.ico                  ←ダイアログに表示するアイコン
```

「自動実行機能」や「自動再生機能」を悪用するマルウエアは、感染したコンピュータ内でリムーバブルメディアのコンピュータへの接続を監視しており、接続が確認されると、感染活動を開始する。具体的には、マルウエア内で保持しているマルウエアのコピーと、マルウエアを起動するための”AUTORUN.INF”ファイルをリムーバブルメディアのルートフォルダ上に配置する。

そして、感染したリムーバブルメディアが別のコンピュータに接続された際に、「自動実行機能」や「自動再生機能」により"AUTORUN.INF"ファイルが解釈され、感染のためにマルウエアのコピーが実行される。

2. 国内外における出現・被害状況の調査

本章ではリムーバブルメディア経由の感染を行うマルウエアの中から、グローバル(日本を含む全世界)と日本国内において最も感染報告数が多かった上位10種類に注目し、出現・被害状況について報告する。出現・被害状況を示す数値としては、感染被害数の他、ウイルス対策製品のウイルスパターンファイルに登録されたシグネチャ[2]の登録数についても調査した。

ここでは USB メモリ等に代表されるリムーバブルメディア経由の感染機能(以下、リムバーブルメディア感染機能)を有する亜種を含むマルウエアファミリ[3]を対象に種類分けを行っている。そのため、感染報告数の中にはリムーバブルメディア感染機能を持たない亜種に対する報告も含まれる。

2.1. 対象マルウエアの感染報告数

対象となるマルウエアファミリとその被害報告数をグローバルおよび日本国内についてそれぞれ表2および表3に整理した。

表2.グローバルの感染報告数と割合

順位	マルウエアファミリ	感染報告数	割合
1	WORM_SOHANAD	5,863,689	32.3%
2	WORM_AUTORUN	2,854,656	15.7%
3	PE_SALITY	2,619,418	14.4%
4	WORM_DELF	1,395,121	7.7%
5	PE_LUDER	1,388,678	7.7%
6	WORM_ONLINEG	1,031,771	5.7%
7	WORM_SILLY	933,964	5.2%
8	PE_CORELINK	788,580	4.3%
9	WORM_AGENT	715,806	3.9%
10	PE_FUJACKS	541,104	3.0%
	合　計	18,132,787	100.0%

グローバルにおいて最も感染報告が多かったのは「WORM_SOHANAD」ファミリであった。5,863,689 件の報告数があり、全体の 32.3%を占めている。次点は「WORM_AUTORUN」ファミリであり、トップの半分程度である15.7%を占めている。

3位の「PE_SALITY」は、2004年末からの古いファミリではあるが、継続的に亜種が

[2]マルウエアの特徴となる点を抜きだした、マルウエア識別のためのポイント。
[3]マルウエアやマルウエアファミリの名称は、トレンドマイクロによる。そのため、他のベンダでは違う名称の場合がある。

出現しており、対応して検出条件も当初より変更されている。そのため、元々の「PE_SALITY」ではなく、「PE_SALITY.EN-0」などの新しい亜種による感染報告が多数含まれている。

表3.日本国内の感染報告数と割合

順位	マルウエアファミリ	感染報告数	割合
1	PE_LUDER	885,227	33.5%
2	WORM_AUTORUN	413,834	15.7%
3	WORM_ONLINEG	371,343	14.1%
4	PE_SALITY	335,337	12.7%
5	WORM_SOHANAD	327,961	12.4%
6	PE_CORELINK	96,585	3.7%
7	WORM_AGENT	73,041	2.8%
8	WORM_DELF	70,557	2.7%
9	WORM_SILLY	37,239	1.4%
10	PE_FUJACKS	31,177	1.2%
	合　計	2,642,301	100.0%

日本国内での感染報告の傾向はグローバルとは大きく異なり、感染報告が最も多かったのは「PE_LUDER」ファミリである。同ファミリは全体の33.5%を占めており、次点の「WORM_AUTORUN」ファミリの15.7%を大きく引き離している。逆にグローバルで報告が多い「WORM_SOHANAD」ファミリは12.4%と少ない。

日本国内で感染報告数がトップの「PE_LUDER」は5位、全体に占める割合は7.7%と大きな違いが見られる。その理由として、日本国内においてはある一時期に、国内の掲示板に対し同じ不正な URL への誘導が多数書きこまれたことにより、一度に大量の感染被害が発生したことによる。

なお、対象となるマルウエアのうち代表的なものとして「WORM_AUTORUN」と「WORM_AGENT」について詳細な分析を行った結果を本報告書の末尾に「参考資料:関連マルウエアの解析情報」としてまとめた。

2.2. 感染報告数の推移

図 2は上位10マルウエアのグローバルおよび日本国内での感染報告数の推移を月単位で示したものである。

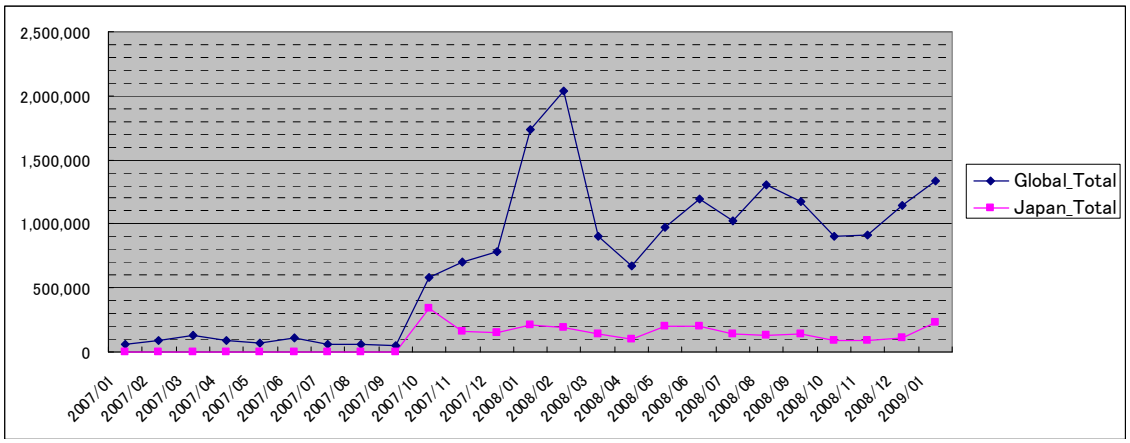

図 2. 感染報告数の推移

グローバルおよび日本国内共に、2007年10月を期に感染報告の大幅な増加が確認できる。ところが、その後グローバルの感染報告数が2007年10月から一定のペースで増減しながら着実に増加しているのに対して、日本国内では横ばいに近い状態が続いている。

日本国内では、情報漏えい事件が相次いで発生し報道されており、取り扱いに対する危険度の認識が進んでいる。感染報告数の差は、法人ユーザ等において運用ルールの厳格化等が行われた結果、海外と比較して相対的に対策が進んだためであると推測できる。

一方で2008年12月～2009年1月にかけてはグローバルと日本国内双方で同様の感染報告の増加傾向が見られることから、今後もリムーバブルメディア感染機能を持ったマルウエアの感染拡大に対する注意の喚起が必要と考えられる。

2.3. シグネチャ登録数の推移

図 3は、トレンドマイクロのウイルスパターンファイル中の上位10マルウエアのシグネチャにおいて、亜種の合計数の推移を示したものである。対象としたウイルスパターンファイルは調査対象期間の該当月1日リリースのものである。ウイルスパターンファイルはグローバルで同一のため、特に国内は区別していない。

例を挙げると、2009年1月1日にリリースされたウイルスパターンファイル(5.743.00)には、「WORM_AUTORUN」ファミリ(「WORM_AUTORUN.AA」「WORM_AUTORUN.AB」「WORM_AUTORUN.ZZZ」等)が合計2,581個登録されている。

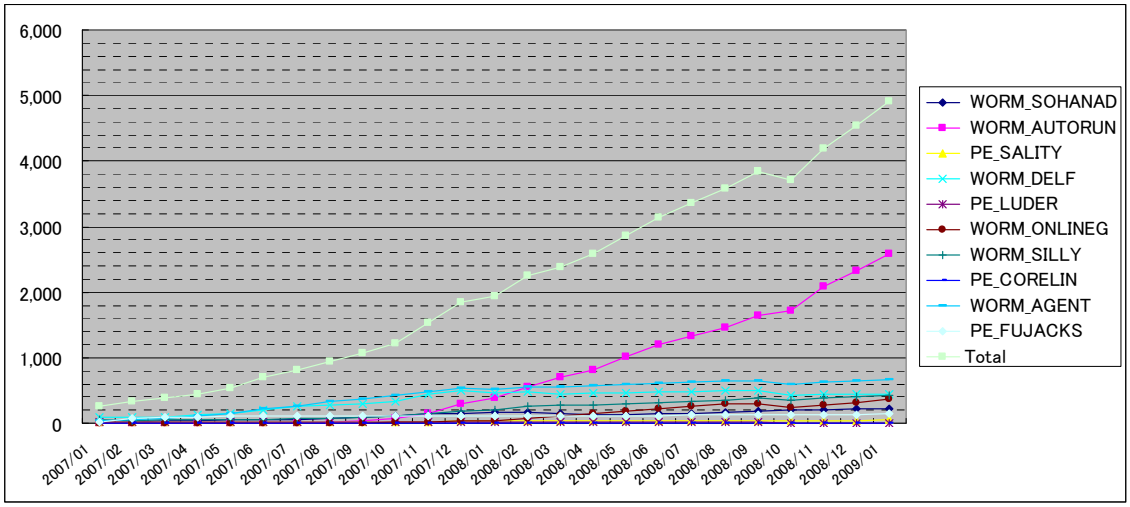

図 3. シグネチャ登録推移

シグネチャ登録数を見ると、他のファミリと比較して特に亜種数が多いのが「WORM_AUTORUN」ファミリである。「WORM_AUTORUN」は2007年6月に初めてウイルスパターンファイルへのシグネチャ登録が行われ、その後一定の割合で種類が増加している。2009年1月時点では、合計2,581個のシグネチャが登録されている。ひとつのシグネチャで複数の異なるバイナリファイルを検出するものもあるため、実際に流通している亜種数の合計は2,581種類を大きく上回るものと考えられる。

「WORM_AUTORUN」ファミリは主にリムーバブルメディア経由の感染だけを不正活動とするものが多い。中には、マルウエア自体にバグをもったその他の亜種の失敗作(たとえばファイル感染機能が正常に動作しない結果、リムーバブルメディア経由の感染のみ実施等)も「WORM_AUTORUN」として多数含まれている可能性がある。

亜種の増加は、USB メモリの普及に伴って、マルウエア作成者が Web サイト経由、電子メール経由に次ぐ有効なマルウエア感染ルートとして注目している結果と考えられる。

2.4. 対象マルウエアの感染傾向

対象となるマルウエアの感染傾向を把握するために、対象となるマルウエアと全マルウエアの感染報告数の推移をグローバルおよび日本国内についてそれぞれ図 4 および図 5にまとめた。

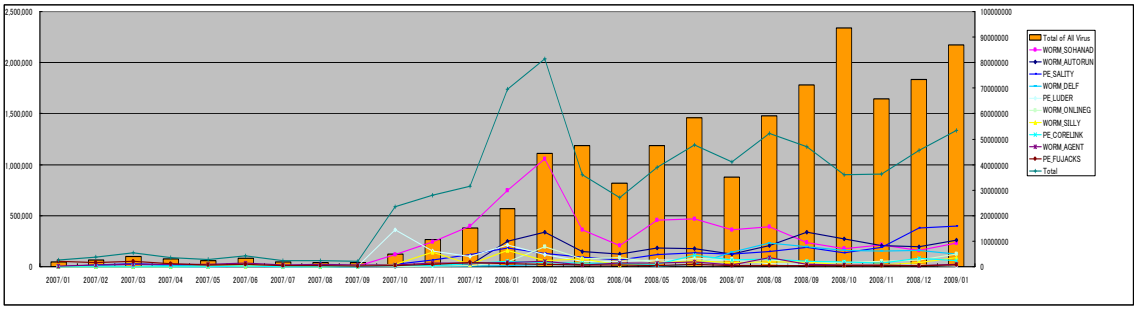

図 4. グローバルの感染報告の推移

グローバルにおいては対象となるマルウエアの感染報告数は、2007年9月までは比較的少ないものの、「PE_LUDER」ファミリとそれに続く「WORM_SOHANAD」ファミリの活発化とともに大幅に増えている。

「WORM_SOHANAD」は当初インスタントメッセンジャー経由による感染活動を主とするファミリであった。リムーバブルメディア感染機能を持つ亜種の出現により、感染報告数が増加したと考えられる。

2008年8月以降は「WORM_SOHANAD」が落ちつく一方で、「PE_SALITY」や「WORM_AUTORUN」など他のファミリの感染報告が増加しはじめ、全体としてはリムーバブルメディア感染機能を持つマルウエアの増加の傾向がみられる。

リムーバブルメディア感染機能を持つマルウエアの感染報告数の推移から、マルウエア作成者は最初にリムーバブルメディア感染機能のウイルスが頒布効果を持つか確認、その後積極的に感染手法として利用し始めたと推測できる。

現在ではリムーバブルメディア感染機能は、Web サイト経由、電子メール経由に並ぶ感染手法の一つとして、その地位を確立したと考えられ、今後の動向に注意が必要である。

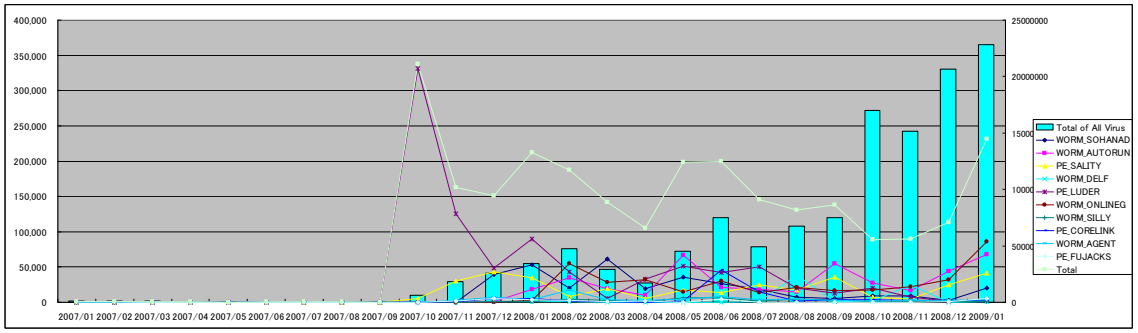

図 5. 日本国内の感染報告の推移

日本国内における感染報告数は2007年9月まで少ないものの、2007年10月の「PE_LUDER」ファミリの活発化ともに大幅に増えている。当初リムーバブルメディア感染機能を持っていなかった「PE_LUDER」ファミリが同機能を持った後に爆発的に拡散したことになる。

時間の経過とともに「PE_LUDER」ファミリの感染報告数は増減を繰り返しながら減少傾向となり、一旦は日本国内の報告が減りつつあるように見えた。しかし、2008年後半から「WORM_ONLINEG」「WORM_AUTORUN」「PE_SALITY」など他のファミリの感染報告が増えはじめているため、全体としてはリムーバブルメディア感染機能を持つマルウエアの増加の傾向がみられる。

日本国内においても、グローバル同様にリムーバブルメディア感染機能は感染手法として定着しており、今後の動向に注意が必要である。

3. 感染事例の調査

リムーバブルメディア経由で感染するマルウエアの感染事例はメディア上でも何度か取り上げられている。中でも国際宇宙ステーションに持ち込まれた USB メモリがオンラインゲームのアカウント情報を盗み出すマルウエアに感染していたという事例は話題になった。この事例の環境は非常に特異であるが、この種類のマルウエアの感染事例としては典型とも言える例である。

ここではこの種類のマルウエアの感染実態について理解を深めるために、日本国内で報告された感染事例を4件紹介する。

3.1. 事例 1: USB メモリによる標的型攻撃

関係者からの荷物を装い、USB メモリが郵送されてきた。受けとった人物が同梱されていた書類に従い、コンピュータで USB メモリの中身を確認しようとした。実は USB メモリはマルウエアに感染した内容であり、USB メモリに含まれたマルウエアが自動的に実行されてしまい、コンピュータがマルウエアに感染してしまった。

図 6. 不審な USB メモリからの感染

3.2. 事例 2: インターネットに直接接続していないコンピュータへの感染

2009年1月、病院・医療関係の法人にて「WORM_DOWNAD.AD」の感染被害が発生した。組織内の90%強のコンピュータに感染被害が拡大し。24時間体制の対応で復旧までに7日間を要し

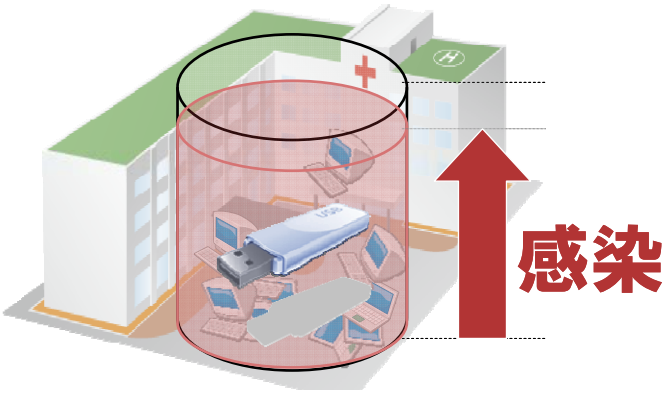

図 7. 組織内のコンピュータに感染拡大

た。

組織内のネットワークはインターネットに接続していない環境であり、OS のパッチ適用が実施されていない環境であった。感染後は「WORM_DOWNAD.AD」のもつネットワーク感染機能により感染被害が拡大した。

外部ネットワークとの接続がない環境での感染被害であるため、初期の感染は USB メモリ等外部記憶メディアであると考えられる。

3.3. 事例 3: 組織内への根深い感染

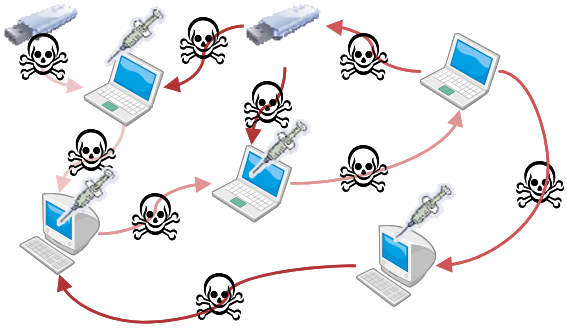

図 8. 新規感染と再感染による長期化

2008年10月に通信関係の法人にて「WORM_SILLY.ZX」の被害が発生し、組織内の一部のコンピュータ(200台程度)が感染した。同組織のネットワークは、インターネットに直接接続をしておらず、内部ネットワークの速度が遅かったため、ウイルス対策製品のパターンファイルのアップデートを月に1回のペースで行う運用方法を採っていた。

感染したコンピュータに対し、当初手動でマルウエアの駆除作業を実施していたが、後から駆除ツールによる駆除作業に切り替えて駆除を行った。

ところが、感染したコンピュータの設置場所が複数に渡ったことと、ネットワークの速度が遅いことにより、駆除ツールによる作業の実施に時間を要してしまい、すみやかな駆除を行えなかった。そのため、4ヶ月以上経過した時点においても完全な復旧には至らなかった。

業務アプリケーションのアップデートを実施する際に使用した USB メモリが「WORM_SILLY.ZX」に感染しており、組織内ネットワークに侵入したものと考えられる。

3.4. 事例 4: 国際会議経由の感染

2009年2月に、国際会議にて講師より発表ファイルを受けとった。利用したのは同会議で配布されたノベルティグッズの USB メモリである。

図 9. 外部からの持ち込みによる感染

翌日、会議より持ち帰った USB メモリをコンピュータに接続したところ、ネットワーク上で不審な445/tcp の通信が多発するようになった。

そのコンピュータはウイルス対策製品を一部無効化しており、パターンファイルのアップデートを行っていなかった。別の製品でスキャンしたところ、「WORM_DOWNAD.AD」系列のマルウエアへの感染が判明した。国際会議より持ち帰った USB メモリからも同じマルウエアが検出されており、感染経路はおそらくこれであろうと推測されている。

3.5. 事例から見られる特徴

リムーバブルメディアはその小型化も手伝って、文具的な取り扱われ方が浸透してきている。また、ストレージ機能そのものに限らず携帯音楽プレイヤーやデジタルカメラなど、必ずしもコンピュータとは接続されない形で使用することができるデバイスも多く存在する。このような、「コンピュータとは距離のある」位置づけがリムーバブルメディア経由での感染を誘発していると考えることができる。

事例1は送付元が偽装されている点から標的型攻撃と推察されるが、試用版等を装った DVD が不特定多数に配布されるというケースも想像に難くない。コンピュータとは異なる媒体が併用されることで警戒心がさらに抑えられてしまう。

事例2～4では基本的なセキュリティ対策の不備が感染拡大につながっており、本質的にはこの種類のマルウエア特有の問題ではない。しかしながら、ネットワーク経由のマルウエア感染に対する偏重がその危険性を高めているとも言える。

特に事例2のような環境では深刻である。医療設備をはじめとして、人命にかかわる問題や物理的な事故に結びつく可能性の高いところではインターネットからは隔離されたネットワークを構成することでセキュリティを維持しようとする考え方がある。それによって基本的なセキュリティ対策を犠牲にしてしまうことになると、ネットワーク以外の媒体からの脅威に対して非常に脆弱になる。

4. リムーバブルメディア感染機能の検証

本報告書の調査対象であるリムーバブルメディアを経由して感染するマルウエアにおいて、どのような機器が感染対象となりうるのかを検証した。

また、「ウイルス対策機能」や「認証機能」、「暗号化機能」を備えた USB メモリ(以下、機能拡張 USB メモリ)についても感染実験を行ったのであわせて報告する。

4.1. 検証の方針と環境

リムーバブルメディアを経由して感染するマルウエアには他の感染手法を持つものも珍しくなく、感染の条件も環境やユーザの行動によって異なる。ここでは次のようにコンピュータとリムーバブルメディアを介して拡散するシナリオを設定することとする。

1. 感染源として、何らかの手段によりリムーバブルメディア感染機能を持つマルウエアに感染したコンピュータ(以下、感染コンピュータ)が存在する
2. その感染コンピュータにまだ感染していないリムーバブルメディアを接続することで、そのリムーバブルメディアにもマルウエアが感染する
3. 感染したリムーバブルメディアをまだ感染していないコンピュータ(以下、未感染コンピュータ)に接続することで、そのコンピュータもマルウエアに感染する

このシナリオにしたがって検証を行うには、2種類の感染を確認する必要がある。それぞれについて感染の判断方法を明確にするため、マルウエアの挙動を以下に示す。なお、この挙動は実際の検証に利用した「WORM_AGENT.AERP」によるものである。参考情報に類似マルウエア「WORM_AGENT.AAQT」の解析情報を掲載したので、詳細については7.3も参照いただきたい。

◆ 感染コンピュータ上のマルウエアによるリムーバブルメディアへの感染

感染コンピュータにリムーバブルメディアが接続された場合、リムーバブルメディアのルートフォルダ直下に他のコンピュータへ感染活動を行うためのファイル群を作成する。検証では、ファイルが作成されるかどうか、およびウイルス対策製品によりマルウエアと検知されるかどうかを感染の判断基準とする。

◆ 感染したリムーバブルメディアから未感染コンピュータへの感染

未感染コンピュータに感染したリムーバブルメディアを接続した場合、Windows の自動実行機能や自動再生機能によりマルウエアが実行され、レジストリの書き換

えやシステムフォルダへの不正な実行ファイルの作成等が行われる。検証では、感染したリムーバブルメディアを未感染コンピュータに接続し、Windows 上でマイコンピュータからリムーバブルメディアのアイコンをダブルクリックした後に感染の確認を行う。レジストリの書き換えと不正なファイルの作成を感染の判断基準とする。

図 10. リムーバブルメディア感染

リムーバブルメディアとして次の2種類について、それぞれ USB 接続タイプの機器を選定し、感染媒体になり得るかを検証する。

- ストレージ機能を主としたリムーバブルメディア
  コンピュータに接続して利用することを主用途とした記憶デバイス
- ストレージ機能を内蔵する外部接続機器
  単体で使用する用途をもった、コンピュータに接続可能なデバイス

コンピュータとしては、次の2種類の OS について感染対象になり得るかを検証する。なお、検証のためにウイルス対策製品はインストールしていないが、インターネットから切り離された環境で実験したことを付記しておく。

- Microsoft Windows XP Professional SP3　　（以下 Windows XP SP3）
- Microsoft Windows Vista Enterprise SP1　　（以下 Windows Vista SP1）

4.2. ストレージ機能を主としたリムーバブルメディア

ストレージ機能を主としたリムーバブルメディアとしては、USB メモリや外付けハードディスクなどがあるが、今回は携帯電話やデジタルカメラの記憶媒体として広く利用さ

れている SD メモリーカードを対象とした。
なお、検証においては SD メモリーカードアダプタに microSD メモリーカードを挿入して利用した。

◆ SD メモリーカードの初期状態

検証用の SD メモリーカードは、データを保存していない状態で検証を行うために、あらかじめ GNU/Linux のディストリビューションである Ubuntu[4]を使い、ファイルシステムを FAT32形式としてフォーマットした。

◆ SD メモリーカードのロック機能による影響の検討

SD メモリーカードには仕様上、保有データの削除や上書きを禁止するためのロック

図 11. SD メモリーカードのロック機能(例)

機構が物理的に存在している(**図** 11の□部分)。
SD メモリーカードの検証では、このロックによる影響を見るため、ロックが有効な場合と無効な場合の両方のケースに対して検証を行った。

◆ 感染コンピュータから SD メモリーカードへのマルウエア感染の検証結果

感染コンピュータから SD メモリーカードに感染するかどうかを検証した。
検証の結果、環境によらず感染した(表4)。

表4.感染コンピュータから SD メモリーカードへのマルウエア感染の検証結果

OS	感染の有無
Windows XP SP3	×感染あり
Windows Vista SP1	×感染あり

[4] http://www.ubuntu.com

◆ 感染したSDメモリーカードから非感染コンピュータへのマルウエア感染の検証結果

非感染コンピュータにおいてマイコンピュータからリムーバブルドライブのアイコンをダブルクリックした際に、感染した SD メモリーカードから非感染コンピュータに感染するかどうかを検証した。

検証結果を表5に示す。Windows XP SP3 については感染したが、Windows Vista SP1 については感染しないことを確認した。

表5.SD メモリーカードからコンピュータへのマルウエア感染の検証結果(クリック)

OS	感染の有無
Windows XP SP3	×感染あり
Windows Vista SP1	○感染なし

◆ ロック機能を有効にした場合のマルウエア感染の検証結果

SD メモリーカードの物理的なロックが有効になっていた場合において、感染コンピュータから SD メモリーカードに感染するかどうかを検証した。

検証結果を表6に示す。検証の結果、ロック機能を有効にした場合感染しないことを確認した。

表6. リムーバブルメディア感染機能による SD メモリーカードのマルウエア感染の検証結果(ロック有効)

OS	感染の有無
Windows XP SP3	○感染なし
Windows Vista SP1	○感染なし

◆ まとめ

検証結果より、SD メモリーカードに対しマルウエアが感染すること、感染した SD メモリーカードからコンピュータへマルウエアが感染することを確認した。ただし、OS が Windows Vista である場合、リムーバブルドライブのアイコンのクリックによる感染は行われないことを確認した。また、SD メモリーカードのロック機能を有効にしている場合、感染コンピュータに接続したとしても感染活動が失敗し、SDメモリーカードに感染しないことを確認した。

これにより、ストレージ機能を主としたリムーバブルメディアがマルウエアに感染する可能性があることが確認できた。

4.3. ストレージ機能を内蔵する外部接続機器

ストレージ機能を内蔵する外部接続機器としては、携帯音楽プレイヤーや携帯電話、ゲーム機などがある。今回は特に身近な機器であるデジタルカメラを対象とした。デジタルカメラはデータ交換のために本体やメモリーカードをコンピュータや印刷装置に接続する機会が多く、マルウエアの拡散を仲介していたという事例もある。

なお、検証に使ったデジタルカメラには本体にフラッシュメモリ(以下、内蔵メモリ)が内蔵されており、さらに SD メモリーカードを装着することが可能である。そのため、内蔵メモリを利用した場合と、SD メモリーカードを装着して利用した場合のそれぞれについて検証を行った。

◆ 内蔵メモリと SD メモリーカードの初期状態

検証用の内蔵メモリおよびSDメモリーカードは、デジタルカメラのメモリフォーマット機能を使ってそれぞれ FAT12および FAT16でフォーマットを行った。このフォーマット作業により、内蔵メモリには3つのフォルダ、SD メモリーカードには1つのフォルダが作成される。この状態を初期状態として検証を行った。

◆ 感染コンピュータからデジタルカメラへのマルウエア感染の検証結果

本検証では利用した「感染していない内蔵メモリ」と「感染していないデジタルカメラ+SD メモリーカード」をマルウエアに感染コンピュータに USB 接続し感染の確認を行った。検証の結果を表7に示す。

表7.感染コンピュータからデジタルカメラへのマルウエア感染の検証結果

	デジタルカメラ内蔵メモリ	デジタルカメラ＋SD メモリーカード
Windows XP SP3	×感染あり	×感染あり
Windows Vista SP1	×感染あり	×感染あり

◆ 感染したデジタルカメラから非感染コンピュータへのマルウエア感染の検証結果

非感染コンピュータにおいてマイコンピュータからリムーバブルドライブのアイコンをダブルクリックした際に、「マルウエアに感染した内蔵メモリ」と「マルウエアに感染したデジタルカメラ+SD メモリーカード」から未感染コンピュータに感染するかどうかを検証した。

検証結果を表8に示す。検証の結果、Windows XP SP3 については感染したが、

Windows Vista SP1 については感染しないことを確認した。

表8.感染したデジタルカメラから未感染コンピュータへのマルウエア感染の検証結果（クリック）

	デジタルカメラ内蔵メモリ	デジタルカメラ＋SD メモリーカード
Windows XP SP3	×感染あり	×感染あり
Windows Vista SP1	○感染なし	○感染なし

◆ まとめ

検証結果より、デジタルカメラの内蔵メモリおよび装着した SD メモリーカードに対しマルウエアが感染すること、感染したデジタルカメラからコンピュータへマルウエアが感染することを確認した。ただし、OS が Windows Vista である場合、リムーバブルドライブのアイコンのクリックによる感染は行われないことを確認した。

これにより、ストレージ機能を内蔵する外部接続機器についても、ストレージ機能を主とするリムーバブルメディアと同様にマルウエアに感染する可能性があることを確認した。ただし、外部接続機器の場合は一般的にロック機構が装備されていないため、ロック機構による防護は行えない。

4.4. 機能拡張 USB メモリによる各種保護機能の検証

本項では USB メモリにはセキュリティ機能を売りにする製品がいくつか存在する。そのような機能拡張された USB メモリについてもマルウエアの感染対象になり得るか実験を行った。

◆ 機能拡張 USB メモリの概要

今回、「ウイルス対策機能」「パスワード認証機能」「暗号化機能」の3種類の機能拡張 USB を実験対象とした。以下に各機能の特徴を示す。

《ウイルス対策機能》

USB メモリ内にデータを保存する際に独自のウイルススキャンを行い、ウイルスと判断した場合は USB メモリ内に隔離する機能である。

《パスワード認証機能》

USB メモリの利用に認証が必要となっており、認証を通過するまでは保存されたデータの読み書きを行えなくする機能である。

《暗号化機能》

USB メモリ内にデータを保存する際に、自動的に暗号化を行う機能である。一般に、「パスワード認証機能」を前提に利用されている。

◆ 実験に利用した機能拡張 USB メモリ製品

実験に利用した機能拡張 USB メモリを表9に示す。USB メモリ A と USB メモリ B に備えられたウイルス対策機能は、同一のウイルス対策ベンダの製品を利用している。

表9.機能拡張 USB メモリの一覧

	ウイルス対策機能	認証機能	自動暗号化機能
USB メモリ A(B 社製)	○有り	○有り	○有り
USB メモリ B(I 社製)	○有り	○有り	○有り
USB メモリ C(I 社製)	×なし	○有り	○有り

◆ 各機能拡張 USB メモリの初期状態

実験用の各機能拡張 USB メモリは、各製品用に準備されている初期化ツールを使いディスク内容を初期状態にした。また、ウイルス対策機能については、最新のパターンファイルをアップデートによりあらかじめ適用した。

◆ 感染コンピュータから機能拡張 USB メモリへのマルウエア感染の実験結果

実験では利用した「感染していない機能拡張 USB メモリ」をマルウエアに感染コンピュータへ接続し感染の確認を行った。

実験の結果を表10に示す。

表10.感染コンピュータから機能拡張 USB メモリへのマルウエア感染の実験結果

	USB メモリ A	USB メモリ B	USB メモリ C
Windows XP SP3	○感染なし	○感染なし	×感染あり
Windows Vista SP1	○感染なし	○感染なし	×感染あり

「ウイルス対策機能」を持つ USB メモリ A/USB メモリ B は、ファイルがコピーされた直後に、そのファイルを「MAL_OTORUN1」として検知し、コピー先のファイルが無害化(0バイトのファイルになる)された上で、マルウエア自体はウイルス対策機能の隔離領域に隔離された。

一方、「ウイルス対策機能」を有さない USB メモリ C は、通常のリムーバブルメディア同様にマルウエアに感染した。

◆ 感染機能拡張 USB メモリから非感染コンピュータへのマルウエア感染の実験結果

未感染コンピュータにおいてマイコンピュータからリムーバブルドライブのアイコンをダブルクリックした際に、「マルウエアに感染した USB メモリ C」から未感染コンピュータに感染するかどうかを確認した。

実験結果を表11に示す。実験の結果、Windows XP SP3 については感染したが、Windows Vista SP1 については感染しないことを確認した。

表11.感染した機能拡張 USB から未感染コンピュータへのマルウエア感染の実験結果

	USB メモリ A	USB メモリ B	USB メモリ C
Windows XP SP3	―	―	×感染あり
Windows Vista SP1	―	―	○感染なし

◆ まとめ

機能拡張 USB メモリがもつ「ウイルス対策機能」「パスワード認証機能」「暗号化機能」のうち、「パスワード認証機能」「暗号化機能」のみを持つ製品は、マルウエアに感染する結果となった。一方、「ウイルス対策機能」を持つ製品は、感染コンピュータへの接続時にマルウエアが検知され、隔離されることにより感染を防止できることを確認した。

USB メモリを利用する場合、「ウイルス対策機能」を持つ製品を利用することで、感染の危険性を低減させることができる。ただし、通常のウイルス対策製品同様にパターンファイルで検知できるマルウエアである必要がある。そのため、新規に出現したばかりの亜種については、感染してしまう可能性が残る。

5. リムーバブルメディア経由の感染への対策

リムーバブルメディア経由で感染するマルウエアの特徴として、最新のサービスパックやセキュリティパッチを適用している場合でも感染してしまうことが挙げられる。そこで、そのような経路による感染を防ぐために取れる対策手法を以下に紹介する。

5.1. コンピュータにおける対策

コンピュータにおけるリムーバブルメディア経由の感染対策として、"AUTORUN.INF"ファイルによる「自動実行機能」「自動再生機能」を無効にする方法を記載する。この対策を行うことで、リムーバブルメディア経由の感染についての脅威が減らせる。

対策の前提として、マイクロソフトより提供されている最新のサービスパック及びセキュリティパッチの適用が必要である。なお、本対策はマイクロソフトの Web サイト[5]で公開されている情報を元としており、詳細が必要な場合は同情報を参照して欲しい。

対策は OS のバージョンにより多少異なる。Windows XP Professional および Windows Vista は個別のセキュリティパッチを適用した上でグループポリシーを設定することにより対策が可能だが、Windows XP Home Edition はグループポリシーを設定できないため、代わりにレジストリの操作により対策を行う必要がある。

◆ Windows XP Professional の対策(グループポリシーによる制限)

Windows XP Professional は、次の手順で対策を行う。

- 「Windows XP 更新パッチ(KB967715)」を適用する
- グループポリシーエディタでグループポリシーを設定する

《「Windows XP 更新パッチ(KB967715)」を適用する》

「Windows XP 更新パッチ(KB967715)」は、自動実行機能の無効化に関するパッチである。同パッチは、Windows の自動更新を有効にしている場合、既に適用されている可能性がある。確認のために、以下の作業を行う。

1. 「コントロールパネル」から、「プログラムの追加と削除」を実行する。
2. 「プログラムの追加と削除」において、「更新プログラムの表示」チェックボッ

[5] http://support.microsoft.com/kb/967715/ja

クスにチェックを入れ、「プログラムの変更と削除」の一覧を表示する。

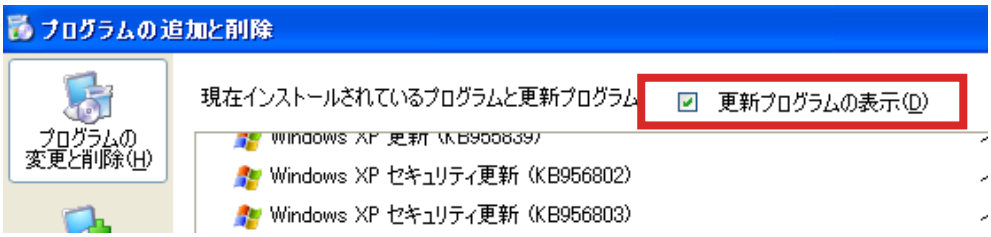

図 12. 更新プログラムの表示

3. 一覧の中に「Windows XP 更新(KB967715)」があるか確認する。

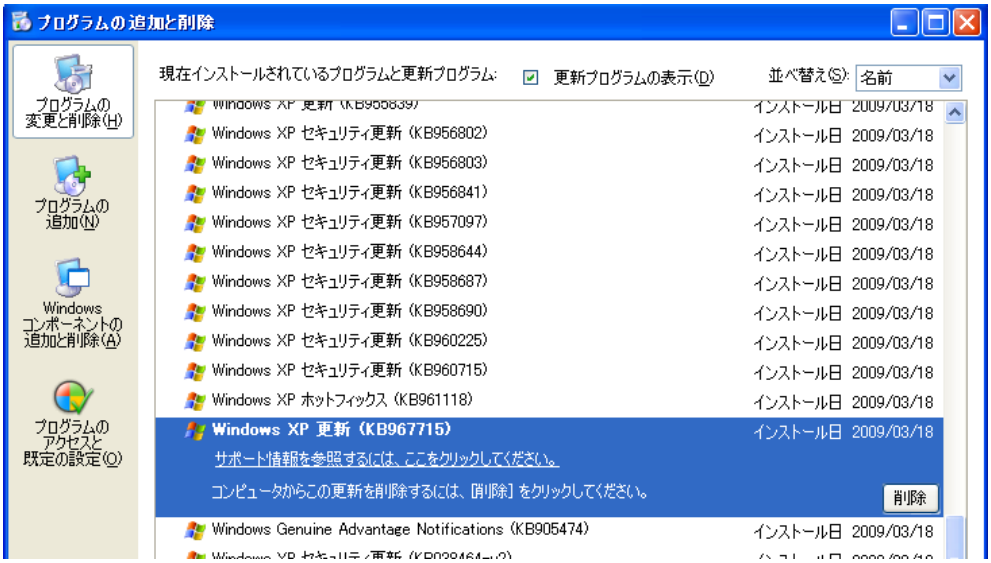

図 13. KB967715 の確認

一覧の中に無い場合は「Windows XP 更新パッチ(KB967715)」を Microsoft Update あるいはマイクロソフトの Web サイト[5]より適用する。

《グループポリシーエディタでグループポリシーを設定する》

1. 「スタート」ボタンから「ファイル名を指定して実行」を選択する。
2. 「ファイル名を指定して実行」の入力ボックスに「gpedit.msc」と入力し OK ボタンをクリック。グループポリシーエディタを起動する。

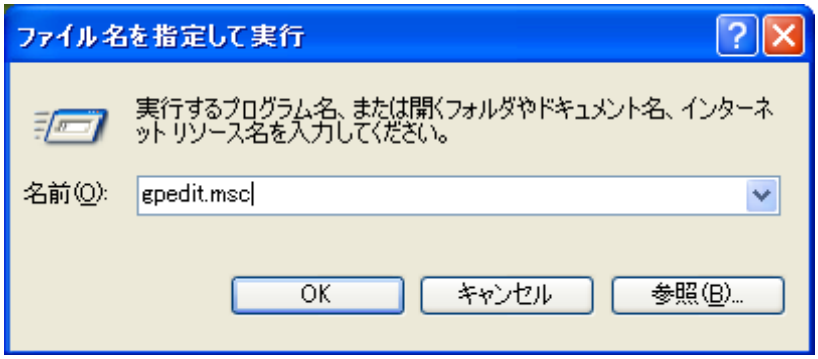

図 14. グループポリシーエディタの実行

3. グループポリシーエディタから「ローカルコンピュータ」→「コンピュータの構成」→「管理用テンプレート」→「システム」と辿り、内容を表示する。

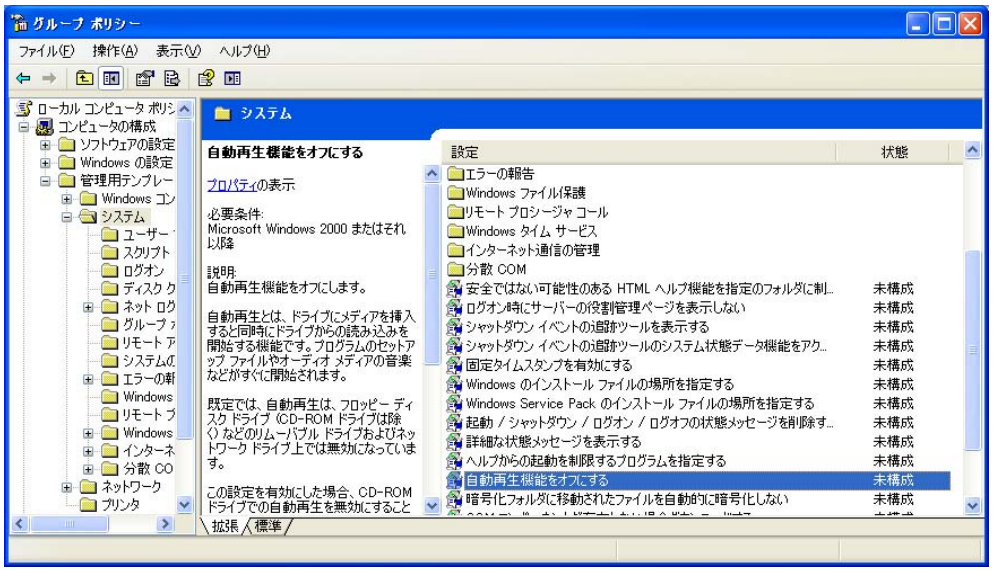

図 15. グループポリシーエディタ

4. 設定ウィンドウで「自動再生機能をオフにする」を右クリックして「プロパティ」をクリックする。

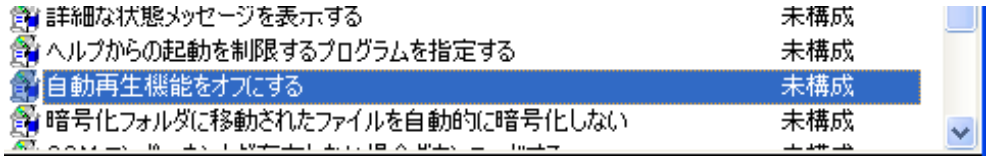

図 16. 自動再生機能の設定

5. 「自動再生機能をオフにするのプロパティ」の「設定タブ」から「有効」のチェックボックスをチェックすると、「自動再生機能をオフにする」が表示され

る。

6. 「自動再生機能をオフにする」の右ペインをクリックして、「すべてのドライブ」を選択して「自動再生機能をオフにするのプロパティ」の「OK」ボタンをクリックする。

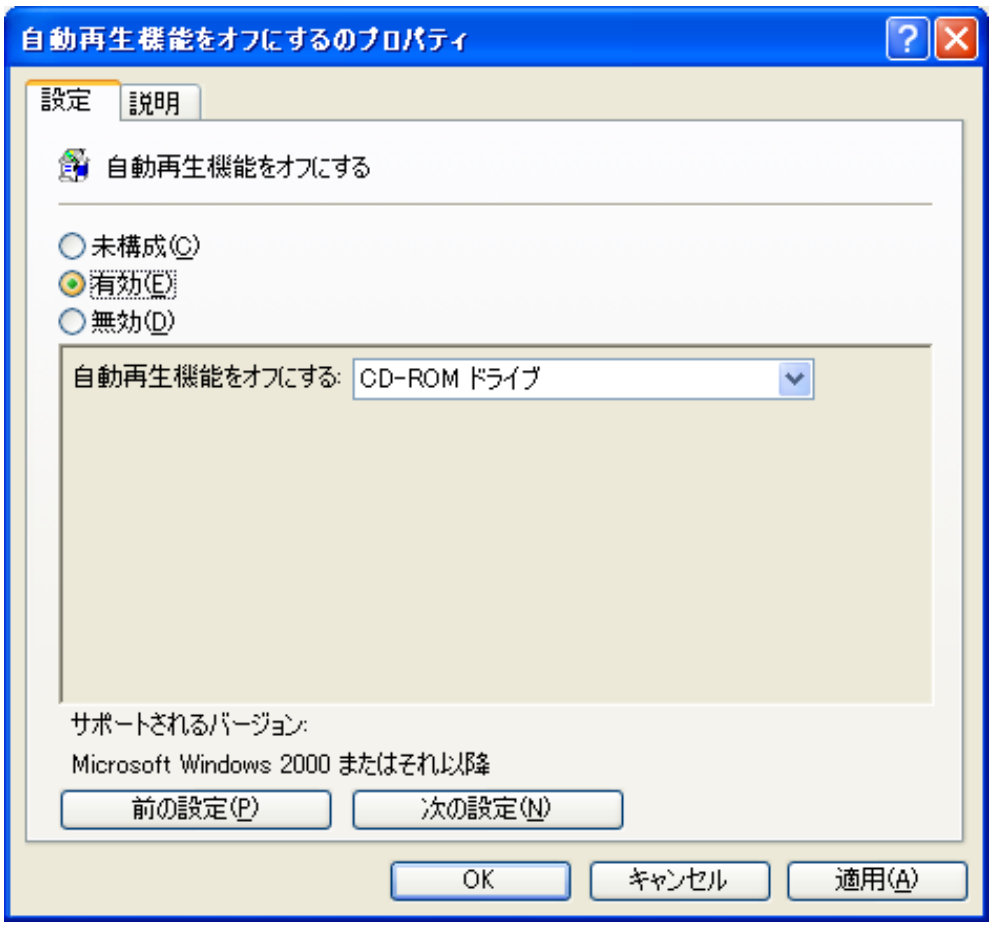

図 17. 自動再生機能の無効化

7. コンピュータを再起動して、変更したグループポリシーを有効にする。

◆ Windows Vista の対策(グループポリシーによる制限)

Windows Vista は、次の手順で対策を行う。

- 「Windows Vista 更新パッチ(KB950582)」を適用する
- グループポリシーエディタでグループポリシーを設定する

《「Windows Vista 更新パッチ(KB950582)」を適用する》

「Windows Vista 更新パッチ(KB950582)」は、自動実行機能の無効化に関するパ

ッチである。同パッチは、自動 Windows の自動更新では更新されない。

1. 「コントロールパネル」から、「プログラムと機能」をダブルクリックする。

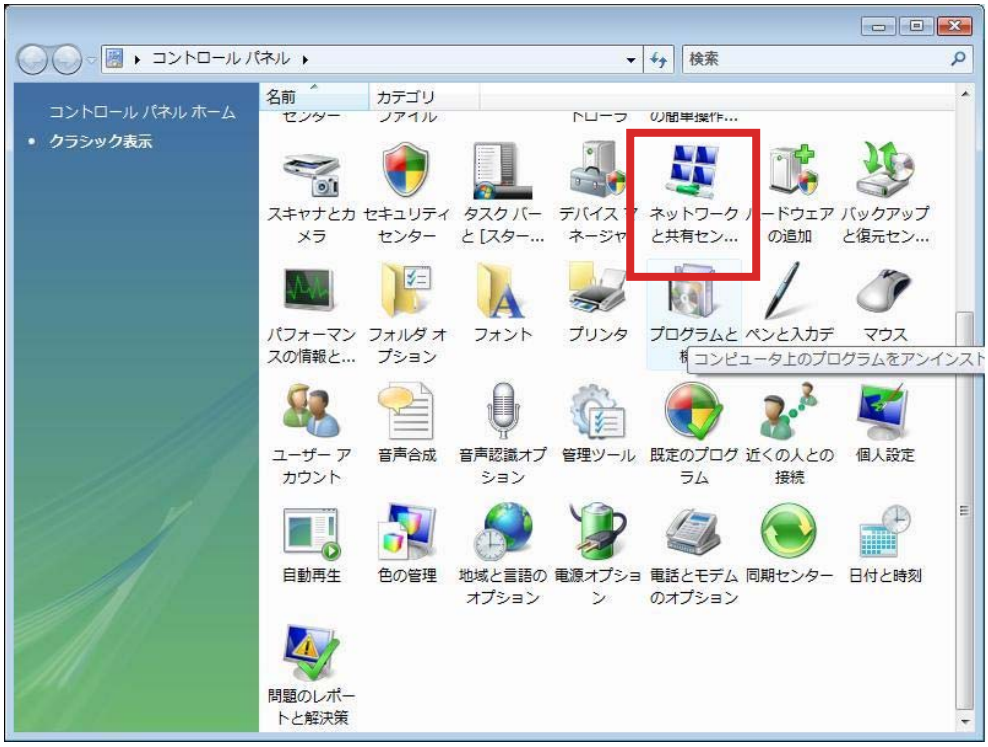

図 18. Windows Vista コントロールパネル

2. 「プログラムと機能」から「適用された更新プログラムを表示」をクリックする。

図 19. プログラムと機能

3. 「適用された更新プログラムを表示」から Windows Vista 更新パッチ

(KB950582)を確認する。

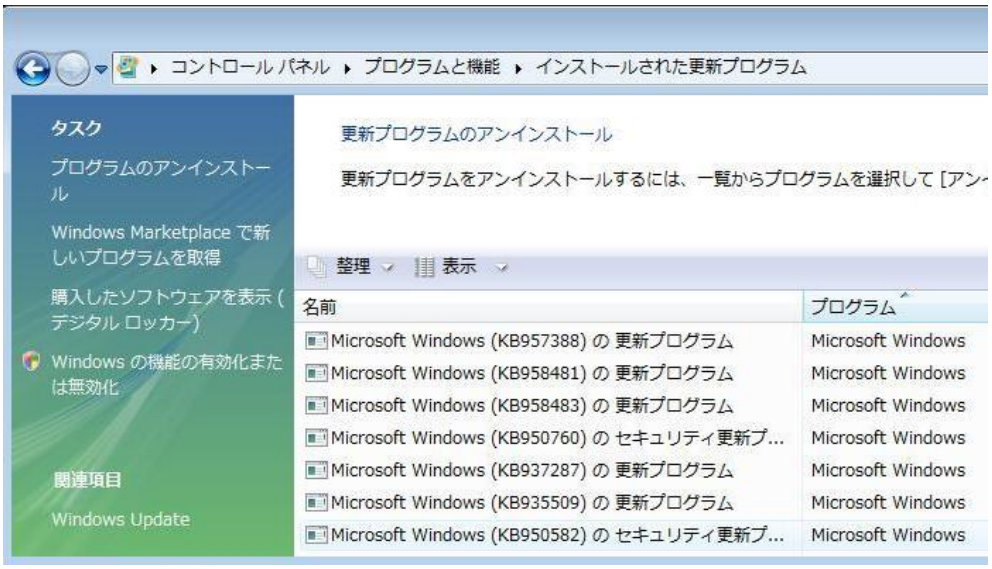

図 20. インストールされた更新プログラム

「Windows Vista 更新パッチ(KB950582)」が適用されていなければ、Windows Update や Microsoft Update により、「Windows Vista 更新パッチ(KB950582)」を手動適用する。

《グループポリシーエディタでグループポリシーを設定する》

1. 「スタート」ボタンから「検索開始のボックス」に「gpedit.msc」と入力し OK ボタンをクリックして、グループポリシーエディタを起動する。

図 21. グループポリシーエディタの検索

2. ローカルグループポリシーエディタから「ローカルコンピュータポリシー」ー「コンピュータの構成」ー「管理用テンプレート」ー「Windows コンポーネント」パスに移動して、「自動再生のポリシー」をクリックする。

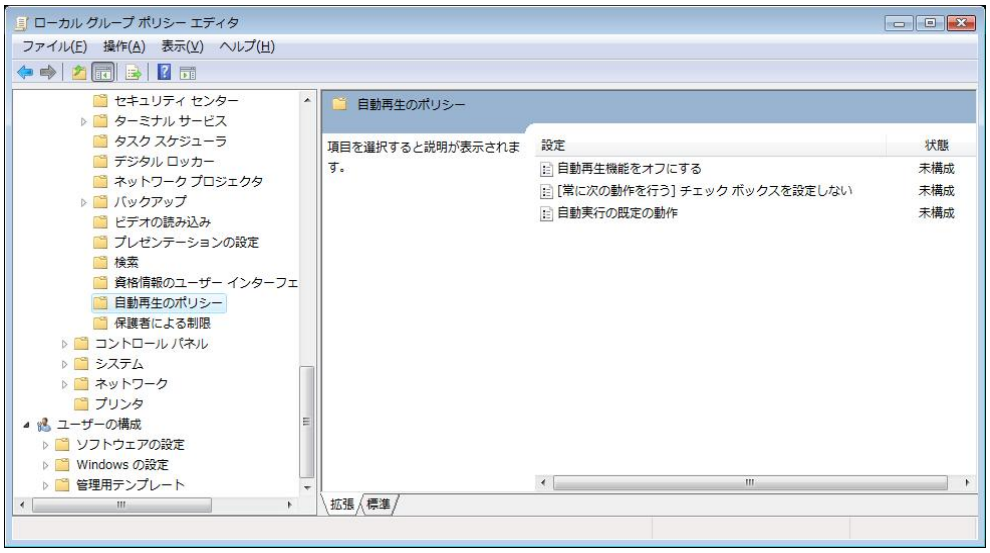

図 22. ローカルグループポリシーエディタ

3. 詳細ウィンドウ領域で「自動再生機能をオフにする」をダブルクリックする。
4. 「自動再生機能をオフにするのプロパティ」の「設定タブ」から「有効」のチェックボックスをチェックし、「自動再生機能をオフにする:」を表示する。

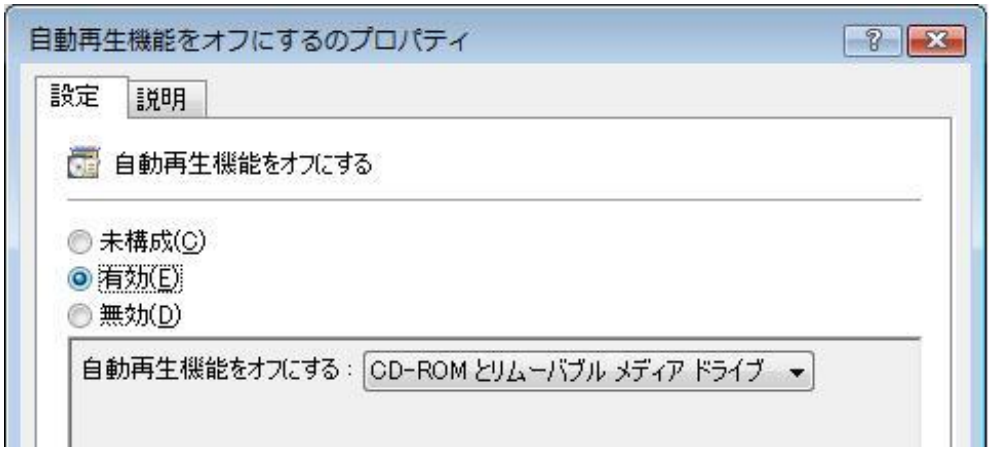

図 23. 自動再生機能の無効化

5. 「自動再生機能をオフにする:」の右ペインをクリックして、「すべてのドライブ」を選択して「自動再生機能をオフにするのプロパティ」の「OK」ボタンをクリックする。
6. コンピュータを再起動して、変更したグループポリシーを有効にする。

◆ Windows XP Home Edition の対策(レジストリ設定による制限)

Windows XP Home Edition は、次の手順で対策を行う。

- 「Windows XP 更新パッチ(KB967715)」が適用されていなければ、適用する
- レジストリエディタで設定を変更する
- コンピュータを再起動して、変更した設定を有効にする

「Windows XP 更新パッチ(KB967715)」は、自動実行機能の無効化に関するパッチである。同パッチは、自動Windowsの自動更新を有効にしている場合、既に適用されている可能性がある。確認の方法は Windows XP Professional の項の『「Windows XP 更新パッチ(KB967715)」を適用する』を参照。

ここでは、パッチ適用後のレジストリの変更による設定方法についてのみ記載する。

《レジストリエディタで設定を変更する》

本方法は、レジストリを操作するため、間違ったレジストリの操作によっては、システムに問題が起こる可能性もある。そういった問題に対処するため、あらかじめレジストリ操作の前にレジストリのバックアップをする必要がある。これにより問題が起こった場合でも、バックアップしたレジストリをリストアすることで以前の状態に戻せる。

1. 「スタート」メニューの「ファイル名を指定して実行」の入力ボックスに「regedit.exe」と入力し OK ボタンをクリックしてレジストリエディタを起動する。

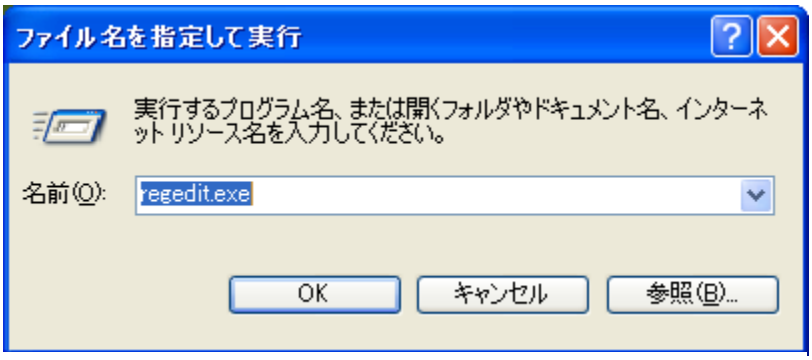

図 24. レジストリエディタの実行

2. メニューの「ファイル(F)」より、「エクスポート」を選択し、レジストリファイルのバックアップを作成する。バックアップ範囲は「全て」とする。

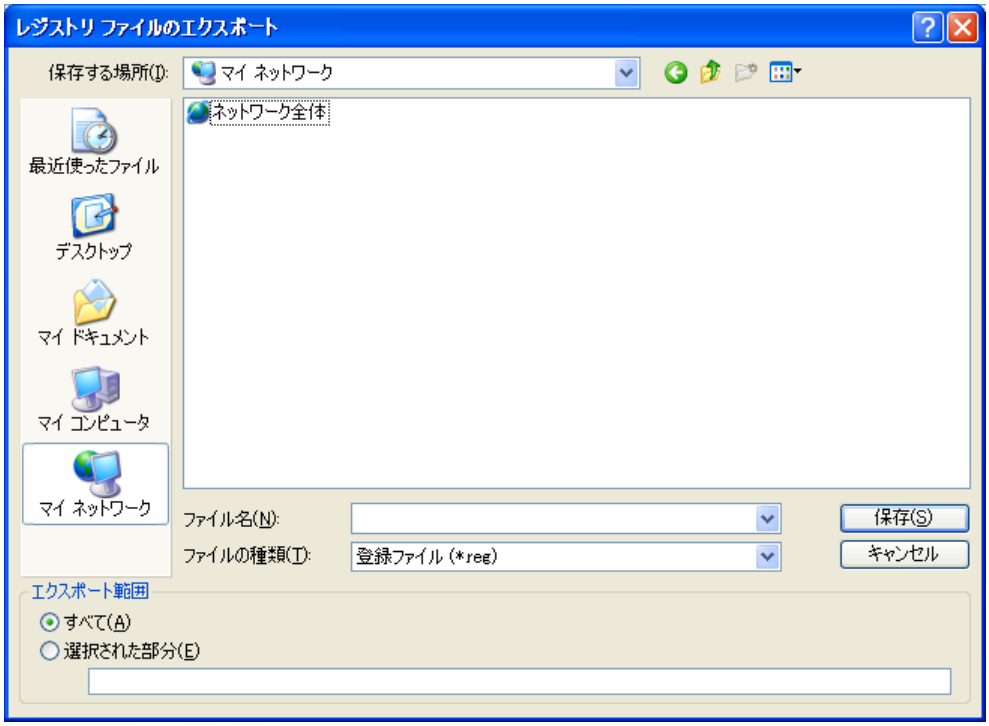

図 25. レジストリのバックアップ

3. レジストリエディタで「HKEY_CURRENT_USER¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥policies¥Explorer¥NoDriveTypeAutoRun」まで移動する。

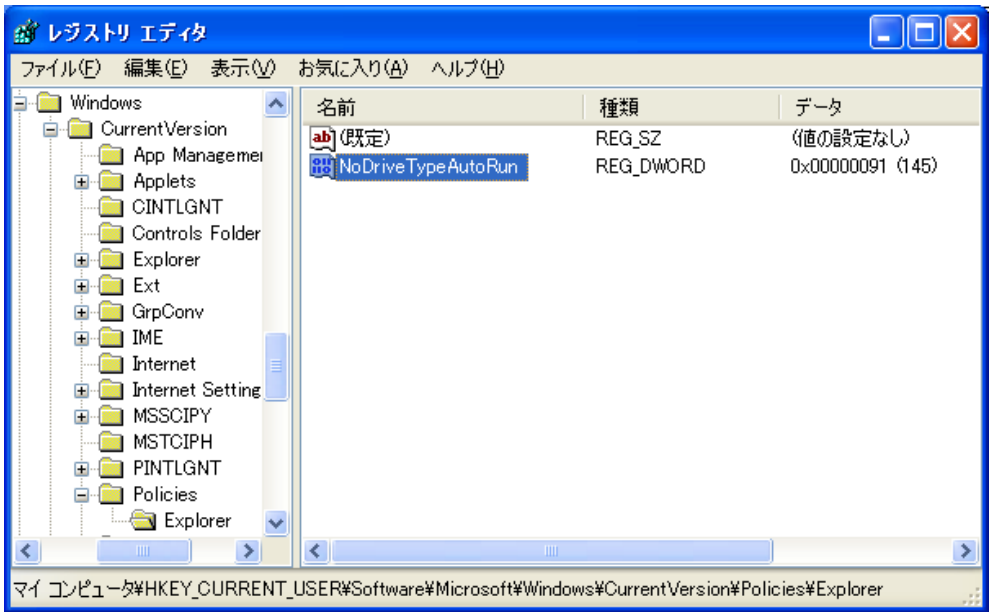

図 26. NoDriveTypeAutoRun

4. 「NoDriveTypeAutoRun」を右クリックし「修正」を選択する。
5. DWORD 値の編集で「値のデータ」入力ボックスの値を「ff」と入力する。表記として16進を選択して OK ボタンをクリックする。

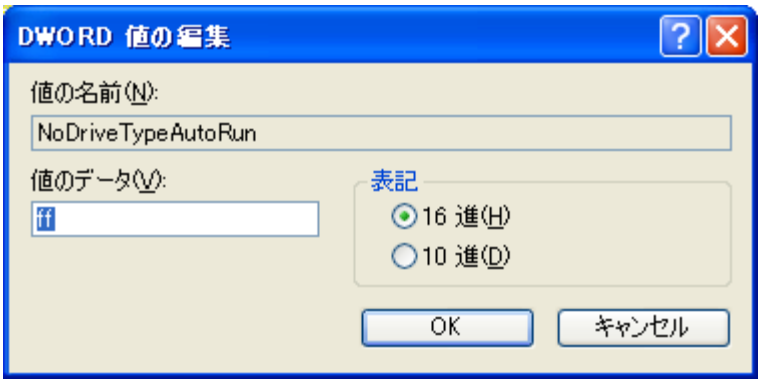

図 27. 値の編集

6. コンピュータを再起動して、変更したレジストリ値を有効にする。

5.2. リムーバブルメディアにおける感染への対策

リムーバブルメディアによっては備わっている機能を利用することで、コンピュータからリムーバブルメティアへのマルウエア感染のリスクを減らすことができる。そのような機能を持たない一般的なリムーバブルメディアについては、Windows 側での対策や運用ルールなどで対応する必要がある。

◆ 書き込み防止機能を持つリムーバブルメディアの利用

4.2の検証で利用した SD メモリーカードのロック機能のような書き込み防止機能を持つリムーバブルメディアを利用することで、同メディアへのマルウエアの感染を防止できる。簡単かつ確実に感染を阻止できるため、読み取り用途が多い利用形態であれば、検討する価値はあると考える。

防止できるのはリムーバブルメディアへの感染だけで、感染したリムーバブルメディアから非感染コンピュータへの感染は防止できない。そのため、感染したコンピュータからデータを書き込み、それを他コンピュータへと持ち出すといった経路には有効ではない。

◆ ウイルス対策機能を持つリムーバブルメディアの利用

ウイルス対策機能を持つリムーバブルメディアを利用することで、コンピュータからリムーバブルメディアに感染活動が行われようとした際に、マルウエアを検知することができる。一般のウイルス対策ソフト同様に定期的なパターンファイルのアップデート等は必要となるが、感染を防ぐ手段としては相応に有用であると考える。

6. 総論

リムーバブルメディア経由の感染機能を持つマルウエアによる被害はここ数年で顕著に増加している。

この報告書ではマルウエアファミリ単位での感染報告数をもとに感染実態の把握を試みた。その中で旧来からのマルウエアファミリが変化の過程でリムーバブルメディア感染の機能を獲得していることもわかった。マルウエアにとってはリムーバブルメディアもネットワークも感染媒体の一つである。したがって、セキュリティ対策においてはリムーバブルメディアについてもネットワークと同様に考慮する必要がある。

また、マルウエアにとって感染媒体はあくまで手段に過ぎず、マルウエアが意図した脅威が感染とは別にある可能性を忘れてはならない。個々を詳細に分析することでインターネット越しの攻撃、近隣ネットワークへの執拗な攻撃等の様々な攻撃手段、情報の盗聴や送信、自己アップデート等の機能を持つマルウエアが存在することがわかっている。特にアップデート機能は他のマルウエアへの感染の引き金となったり、対策を掻い潜る悪意ある機能が追加されたりする危険性を含んでいる。

そのため、一度組織内でこれらのマルウエアの感染を許してしまった場合、感染拡大の防止や組織内からの根絶のための手間が膨大なものとなる可能性が高い。

各組織や個人におかれては、この種類のマルウエアに対する理解を深め、感染経路に対する対策をいま一度確認していただきたい。特別な対応を行うのではなく、あくまで日常的なセキュリティ対策の一環として、OS やアプリケーションソフトを最新の状態に維持するとともにウイルス対策製品の正しい運用に加えて、リムーバブルメディアの運用ルールの制定・遵守を行い、PDCA(Plan-Do-Check-Action)による定期的なルールの見直しなどを行っていただきたい。その際に本報告書を参照していただければ幸いである。

7. 参考資料:関連マルウエアの解析情報

リムーバブルメディアを媒体とした感染活動を行う「WORM_AUTORUN.APR」「WORM_AGENT.AAQT」「WORM_DOWNAD.AD」について、詳細な解析を行った結果判明した動作を記載する。「WORM_AUTORUN.APR」「WORM_AGENT.AAQT」は、システムに侵入した後の攻撃フェーズで他の不正プログラムをダウンロードし、オンラインゲームのアカウント情報等を詐取することが確認されている。「WORM_DOWNAD.AD」[6]はOSの脆弱性の攻撃やパスワードクラック等、複数の感染方法を使いわけるマルウエアであり、2008年末以降、多数の被害報告が寄せられている。

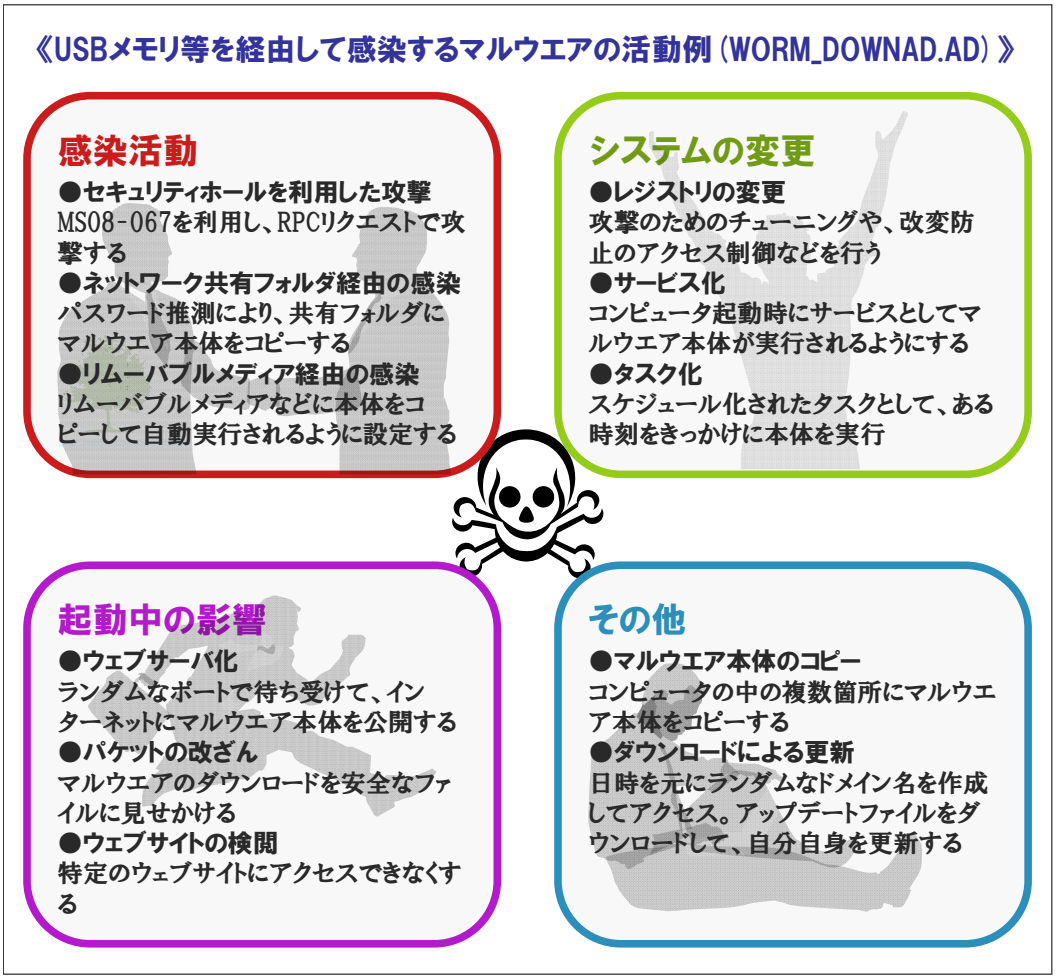

図 28. WORM_DOWNAD.AD の活動例

[6] Downad, Conficker(Conflicker), Kido 等、ウイルス対策製品によって名称が異なる。

7.1. フォルダ名表記の説明

フォルダ名についてはWindowsのバージョンやインストール時の設定等、環境によって異なる。個別のマルウエアの解析情報の中では共通の表現で表記している。以下に、個々の表記について標準的な環境での名前を記載する。

◆ ＜Windows システムフォルダ＞

- Windows 95/98/Me の場合

  C:¥Windows¥System

- Windows NT/2000 の場合

  C:¥WinNT¥System32

- Windows XP/Server 2003 の場合

  C:¥Windows¥System32

◆ ＜User Profile＞

- Windows 98 および Me の場合

  C:¥Windows¥Profiles¥＜ユーザ名＞

- Windows NT の場合

  C:¥WINNT¥Profiles¥＜ユーザ名＞

- Windows 2000, XP, Server 2003の場合

  C:¥Documents and Settings¥＜ユーザ名＞

◆ ＜Common Startup＞

C:¥Documents and Settings¥All Users¥Start menu¥Programs¥Startup

◆ ＜スタートメニュー＞

- Windows 2000/XP/Server 2003 の場合

  C:¥Documents and Settings¥＜ユーザ名＞¥スタートメニュー

- Windows NT の場合

  C:¥WINNT¥Profiles¥＜ユーザ名＞¥Start Menu

◆ ＜Windows フォルダ＞

- Windows9x, Me, XP, Server 2003の場合

  C:¥Windows

- WindowsNT, 2000の場合

  C:¥WINNT

◆ ＜Program Files＞

C:¥Program Files

◆ ＜Application Data＞

- Windows 2000, XP, Server 2003の場合

  C:¥Documents and Settings¥＜ユーザ名＞¥Application Data

- Windows NT の場合

  C:¥WINNT¥Profiles¥＜ユーザ名＞¥Application Data

- Windows 98, Me の場合

  C:¥Windows¥Profiles¥＜ユーザ名＞¥Application Data

◆ ＜Windows Temporary フォルダ＞

C:¥WINNT¥Temp もしくは C:¥Windows¥Temp

7.2. 「WORM_AUTORUN.APR」の解析情報

ファイルタイプ:	PE(Portable Executable 形式)	
メモリ常駐:	あり	
ファイルサイズ:	111,647 Bytes(.EXE)	86,528 Bytes(.DLL)

◆ インストール

① このマルウエアは、自身のコピーである以下のファイルを作成する。

```
<Windows システムフォルダ>¥mmvo.exe
```

② マルウエアは、以下のファイルを作成する。

```
<Windows システムフォルダ>¥mmvo<数字>.dll - このワームとして検出
```

③ マルウエアは、自身のコピーが Windows 起動時に自動実行されるよう以下のレジストリ値を追加する。

場所:

```
HKEY_CURRENT_USER¥Software¥Microsoft¥Windows¥CurrentVersion¥Run
```

値:

```
mmva = "<Windows システムフォルダ>¥mmvo.exe"
```

④ マルウエアは、以下のレジストリ値を変更し、システムファイルおよび読み取り専用の属性のファイルを非表示に設定する。

場所:

HKEY_CURRENT_USER¥Software¥Microsoft¥Windows¥CurrentVersion¥Explorer¥Advanced

値(変更前):

Hidden = "dword : 00000001"

値(変更後):

Hidden = "dword : 00000002"

場所:

HKEY_CURRENT_USER¥Software¥Microsoft¥Windows¥CurrentVersion¥Explorer¥Advanced

値(変更前):

ShowSuperHidden = "dword:00000001"

値(変更後):

ShowSuperHidden = "dword:00000000"

場所:

HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Explorer

¥Advanced¥Folder¥Hidden¥SHOWALL

値(変更前):

CheckedValue = "dword : 00000001"

値(変更後):

CheckedValue = "dword : 00000000"

⑤ マルウエアは、自身のコピーを全ての物理ドライブおよびリムーバブルメディア内に作成することにより感染活動を実施する。マルウエアは、これらのドライブへのアクセス時に自動実行されるよう ″AUTORUN.INF″ というファイルを作成する。この ″AUTORUN.INF″ というファイルは、作成されたコピーを自動実行するシステムファ

イルである。このファイルには以下の文字列が含まれる。

```
＜意味の無いゴミデータ＞
[AutoRun]
＜意味の無いゴミデータ＞
open=as.bat
＜意味の無いゴミデータ＞
shell¥open¥Command=as.bat
＜意味の無いゴミデータ＞
shell¥open¥Default=1
＜意味の無いゴミデータ＞
shell¥explore¥Command=as.bat
＜意味の無いゴミデータ＞
```

＜意味の無いゴミデータ＞の挿入については、”AUTORUN.INF”ファイルの難読化を図ることによるマルウエア解析の妨害目的と、不正な”AUTORUN.INF”ファイルのウイルス対策製品での検出を逃れるための目的とが考えられる。トレンドマイクロ製品では、不正な目的で使用される”AUTORUN.INF”ファイルを「MAL_OTORUN」[7]として検出する。

◆ Web サイトからのダウンロードと実行

① マルウエアは、Web サイトにアクセスし、以下の URL[8][9]よりファイルをダウンロードする。

```
hxxp://www.gamesrb.com/rbv/uu.rar
```

[7] 「MAL_OTORUN」のウイルス情報
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=MAL_OTORUN
[8] 誤アクセスを防止するため http:// を hxxp:// に変更済。以下危険な URL については同様。
[9] 解析時点（2009 年 4 月）では、ドメイン名の解決に失敗するため、これらの URL への接続はできない。

② uu.rar ファイル(RAR 形式ではない)の中には暗号化された URL 文字列が書かれており、復号した URL[10]から別のファイルのダウンロードを行う。そして、ダウンロードしたファイルを ″CreateProcess″ API(Application Programming Interface)を使用して実行する。この実行ファイルはトレンドマイクロ製品では「WORM_ONLINEG.AD」として検出される。

なお、ダウンロードされたファイルは、″GetTempPath″ API を利用してテンポラリフォルダに保存される。また、ダウンロードした uu.rar は利用後に即座に削除される。

◆ 他の不正プログラムの作成：

① マルウエアは、以下のファイルを作成する。

```
<User Profile>¥Local Settings¥Temp¥dtk9l7.dll - 「TSPY_ONLINEG.DYY」として検出
```

7.3. 「WORM_AGENT.AAQT」の解析情報

マルウエア名:	**WORM_AGENT.AAQT**
ファイルタイプ:	**PE**
メモリ常駐 :	**なし**
ファイルサイズ:	**80,060 Bytes（圧縮）**
発見日:	**2007年07月25日**
圧縮タイプ:	**UPX**

◆ インストール

① マルウエアは、自身のコピーである以下のファイルを作成する。

[10] 解析時点(2009 年 4 月)では hxxp://www gamesrb.com/rbv/uu.exe。別の URL となる可能性もある。

```
<Windows システムフォルダ>¥999

<Windows システムフォルダ>¥c_10810.nls

<Windows システムフォルダ>¥c_20462.nls

<スタートメニュー>¥Programs¥Startup¥officexp.exe
```

② マルウエアは、Windows 起動時に自身が自動実行されるよう自身のコピーである"OFFICEXP.EXE"というファイルを<*Common Startup*>フォルダ内に作成する。

③ またマルウエアは以下のファイルを<*Windows システムフォルダ*>内に作成する。以下のファイルは、このマルウエアとして検出される。

```
inter32.dll

shell64.dll
```

④ マルウエアは、上記で作成した DLL ファイルを"Explorer.exe"というプロセスに組み込み、システムのプロセスに常駐する。

⑤ マルウエアは、以下のレジストリ値を変更する。

場所:

```
HKEY_CLASSES_ROOT¥CLSID¥{AEB6717E-7E19-11d0-97EE-00C04FD91972}¥InprocServer32
```

値(変更前):

```
(既定) = "<Windows システムフォルダ>¥shell32.dll"
```

値(変更後):

```
(既定) = "<Windows システムフォルダ>¥shell64.dll"
```

◆ <u>リムーバブルメディアにコピーを作成</u>

① マルウエアは、"RECYCLED"というフォルダをリムーバブルメディア内に作成し、自身のコピーを作成したフォルダ内に作成する。また、マルウエアは

″DESKINF.PIF″ というファイルをリムーバブルメディア内に作成する。このファイルは、このマルウエアとして検出される。

② マルウエアは、″DESKTOP.INI″ という無害なファイルを作成した ″RECYCLED″ フォルダ内に作成する。このファイルには、以下の文字列が含まれる。

```
[.ShellClassInfo]

CLSID={645FF040-5081-101B-9F08-00AA002F954E}
```

文字列内の CLSID はごみ箱を意味する値である。上記.INI ファイルが上記のフォルダ内に作成されると、このフォルダはごみ箱と同様のアイコンとして表示される。これにより、ユーザにフォルダが正規のごみ箱フォルダであるように見せかける。″DESKTOP.INI″ ファイルが削除されると、作成されたフォルダのアイコンは標準のアイコンに戻る。

③ マルウエアは、リムーバブルメディアがアクセスされた際に、自身のコピーが自動実行されるよう、 リムーバブルメディア内に ″AUTORUN.INF″ というシステムファイルを作成する。このファイルは、以下の文字列を含む。

```
[Autorun]

shellexecute=.¥recycled¥deskinf.pif
```

◆ 他の不正プログラムを作成:

マルウエアは、″c_19460.nls″ というファイルを＜Windows システムフォルダ＞内に作成する。トレンドマイクロ製品では、作成されるファイルを「TSPY_AGENT.JPT」という不正プログラムとして検出する。

◆ ファイルの作成:

マルウエアは、″software.chk″ という無害なファイルを ″*＜Windows システムフォルダ＞*¥config″ フォルダ内に作成する。

◆ ファイルのダウンロード:

マルウエアは、以下の URL[11]からファイルをダウンロードする場合がある。

```
hxxp://ms.winibmhelp.com
```

7.4. 「WORM_DOWNAD.AD」の解析情報

マルウエア名:	**WORM_DOWNAD.AD**
ファイルタイプ:	**PE**
メモリ常駐 :	**なし**
ファイルサイズ:	**169,425 Bytes**
発見日:	**2008年12月30日**

◆ インストール

① マルウエアは、自身のコピーである以下のファイルを作成する。

```
<Windows システムフォルダ>¥<ランダムなファイル名>.dll
```

② マルウエアは、コマンドラインに文字列 "RUNDLL32.EXE" が含まれるか確認し、含まれる場合、スケジュールタスクとして実行されていると認識する。マルウエアは、自身を以下の正規のプロセスに組み込む。

```
SVCHOST.EXE

EXPLORER.EXE
```

③ このマルウエアは、他の不正プログラムにより利用される目的別のプログラムである。マルウエアは、自身のコピーファイルの作成時間を正規の Windows ファイル "KERNEL32.DLL" (正規のファイルは *<Windows システムフォルダ>*内に存在する)の作成時間と同様に設定する。これにより、マルウエアは、感染したコンピュータ上に

[11] 2007 年 7 月 26 日現在、上記の Web サイトはアクセス不能

追加された新しいファイルとして、ウイルス対策製品に検知されることを回避する。

④ 実行されると、マルウエアはランダムな Mutex を作成し、"AdjustTokenPrivileges" API を使用して自身のプロセスに「SeDebugPrivilege」特権を付与する。これにより、別のプロセスが管理するメモリ領域への書き込みが可能になる。マルウエアはまた、感染したコンピュータのコンピュータ名を基に2つめの Mutex を作成する。

⑤ マルウエアは、感染したコンピュータの OS バージョンを確認する。Windows 2000 の場合、マルウエアは、自身を "SERVICES.EXE" に組み込む。感染したコンピュータの OS バージョンが Windows Server 2003/Windows Server 2003 R2/Windows XP の場合、マルウエアは、自身を "SVCHOST.EXE" に組み込む。
⑥ コンピュータが Windows Vista 環境にある場合、マルウエアは、以下のコマンドを実行し自動チューニング機能を無効にする。

```
netsh interface tcp set global autotuning=disabled
```

⑦ マルウエアはまた、自身をプロセス "SVCHOST.EXE" に組み込み、"NetpwPathCanonicalize" API をフックして感染コンピュータの再感染を回避する。

⑧ マルウエアは、以下のフォルダ内に自身のコピーを作成する可能性がある。

- ＜Application Data＞
- 規定のシステムディレクトリ
- ＜Program Files＞¥Internet Explorer
- ＜Program Files＞¥Movie Maker
- ＜Windows Temporary フォルダ＞

⑨ 上記の活動により、マルウエアは、既に感染したコンピュータに自身のコピーを複数作成することを回避する。マルウエアはまた、作成した自身のコピーをロックし、ユーザによる読み取り、書き込みおよび削除を回避する。

⑩ マルウエアは、自身のコピーをシステムのサービスとして登録し、Windows 起動時に自動実行されるよう以下のレジストリ値を追加する。

場所:

HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥*＜ランダムなサービス名＞*

値:

Image Path = "*＜Windows フォルダ＞*¥System32¥svchost.exe -k netsvcs"

場所:

HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥*＜ランダムなサービス名＞*

¥Parameters

値:

ServiceDll = "*＜不正プログラムのパス名およびファイル名＞*"

＜ランダムなサービス名＞は、以下のキーのいずれかが利用される。

Boot	Center	Config	Driver	Helper	Image	Installer	Manager	Microsoft	Monitor
Network	Security	Server	Shell	Support	System	Task	Time	Universal	Update
Window									

⑪ マルウエアは作成したレジストリキーに対して、"RegSetKeySecurity" API により「SYSTEM」による「読み取り」のみ可能というアクセス権を設定する。これにより、ユーザはこのマルウエアが作成したレジストリキーおよび値を参照できなくなる。

⑫ マルウエアは、自身のコピーが Windows 起動時に自動実行されるよう以下のレジストリ値を追加する。

場所:

HKEY_CURRENT_USER¥Software¥Microsoft¥Windows¥ CurrentVersion¥Run

値:

＜ランダムな文字列＞ = rundll32.exe *＜システムフォルダ＞*¥*＜不正プログラムのファイル名＞*.dll,

＜パラメータ＞"

⑬ マルウエアはまた、以下のレジストリキーのデータリスト内に値を追加する。

キー:

HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥Windows NT¥CurrentVersion¥SvcHost

追加する値は、このマルウエアが作成したランダムなサービス名と同一である。

⑭ マルウエアは、特定のサービスを無効にするため以下のレジストリ値を変更する。

場所:

HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥BITS

値(変更前):

Start = "3"

値(変更後):

Start = "4"

場所:

```
HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥ERSvc
```

値(変更前):

```
Start = "2"
```

値(変更後):

```
Start = "4"
```

場所:

```
HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥wscsvc
```

値(変更前):

```
Start = "2"
```

値(変更後):

```
Start = "4"
```

場所:

```
HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥wuauserv
```

値(変更前):

```
Start = "2"
```

値(変更後):

```
Start = "4"
```

⑮ マルウエアは、”フォルダ オプション”(Folder Options)の設定を変更した後も、非表示のファイルをより効果的に隠蔽するために以下のレジストリ値を変更する。

場所:

HKEY_CURRENT_USER¥Software¥Microsoft¥Windows¥ CurrentVersion¥Explorer¥Advanced

値(変更前):

Hidden=1

値(変更後):

Hidden=2

場所:

HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥Windows¥ CurrentVersion¥Explorer¥Advanced¥Fol
der¥Hidden¥SHOWALL

値(変更前):

CheckedValue=1

値(変更後):

CheckedValue=0

⑯ マルウエアは、以下のレジストリ値を変更し、同時ネットワーク接続を可能にする。

場所:

HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥ Tcpip¥Parameters

値(変更前):

TcpNumConnections = "*<ユーザ設定値>*"

値(変更後):

TcpNumConnections = "00FFFFFE"

⑰ マルウエアは、インストールの過程で以下のレジストリ値を追加する。

場所:

```
HKEY_CURRENT_USER¥Software¥Microsoft¥Windows¥CurrentVersion¥Applets
```

値:

```
・dl = "0"

・ds = "0"
```

場所:

```
HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Applets
```

値:

```
・dl = "0"

・ds = "0"
```

◆ 感染活動のためのウェブサーバ機能

マルウエアは、感染活動のためにランダムなポートで待ち受けるウェブサーバ機能を持つ。

感染したマルウエアは、コンピュータの外部 IP アドレスを取得し、そのコンピュータがインターネットへ直接接続しているかを確認する。そして設定された IP アドレスが、イーサネットかモデムドライバかどうかを確認する。

具体的にはまず、感染したコンピュータをインターネット側から見た場合の IP アドレス(以下、外部 IP アドレス)を知るために以下のいずれかの一般 Web サイトに接続する。

- http://www.whatismyip.org
- http://checkip.dyndns.org
- http://www.getmyip.org
- http://www.whatsmyipaddress.com

感染したコンピュータの外部 IP アドレスを確認後、この IP アドレスが有効であるか、

ローカルアドレスではないかを確認する。また、取得した外部 IP アドレスが感染したコンピュータに設定されている IP アドレス(内部 IP アドレス)と同一であるか確認する。

ルータを介した NAT(Network address translation,)経由の接続など、外部 IP アドレスと内部アドレスが違う場合、マルウエアは、SSDP(Simple Service Discovery Protocol)リクエストを利用して、UPnP 対応のルータに対しポート番号を公開するよう働きかけ、自身が用いるランダムなポートをインターネット上で利用可能にする。

また、マルウエアは自身のコピーがランダムポートからダウンロードされた回数を確認するため、以下のレジストリ値にダウンロードされた回数を書き込む。

場所:

```
HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Applets
```

値:

```
gip = "dword:<回数>"
```

◆ セキュリティホールを利用した感染活動

マルウエアは、不正な RPC リクエストをランダムな IP アドレスに送信することにより、インターネットを介した感染活動を行う。

マルウエアは Windows のセキュリティホール(MS08-067)を利用し、感染活動を行う。このセキュリティホールは、不正な RPC(Remote Procedure Call)リクエストを攻撃対象のコンピュータに送信すると、RPC リクエストに含まれるシェルコードが、攻撃対象のコンピュータで実行されるものである。このセキュリティホールの詳細は、マイクロソフトの Web サイト[12]を参照。

この不正な RPC リクエストが、セキュリティホールを含んだコンピュータ内で受信されると、まずシェルコードが解読され、解読された内容に従い、特定の API が検索される。この API は、感染したコンピュータからマルウエアのコピーをダウンロードする機能を備えている。ダウンロードされたマルウエアのコピーは、"*<Windows システムフォルダ>*¥X" としてコンピュータに保存される。

攻撃元となるマルウエアに感染したコンピュータはウェブサーバの機能を持たされ

12 http://www.microsoft.com/japan/technet/security/Bulletin/MS08-067.mspx

ており、ランダムな TCP ポートにより接続を待ち受けている。攻撃対象のコンピュータは、攻撃元のコンピュータの URL から、マルウエアのコピーをダウンロードする。URL は下記のようになる。

```
http://<攻撃元のコンピュータの IP アドレス>:<マルウエアにより作成されたランダムなポート>/
                                                    <ランダムな文字列からなる不正プログラムのファイル名>
```

マルウエアは、ファイアウォールやセキュリティ関連のアプリケーションによる検知を回避するために、マルウエアのコピーがダウンロードされている間、パケットのヘッダを改ざんする。このため、ダウンロード中のマルウエアのコピー(実行ファイル)は一見すると無害な JPEG、BMP、GIF または PNG ファイルにみえる。この不正なパケットを攻撃対象のコンピュータが受信し続けた場合、最終的にシステムクラッシュする場合がある。

◆ 共有ネットワークおよびリムーバブルメディア経由の感染活動

マルウエアは、自身のコピーを全ての共有ネットワークドライブおよびリムーバブルメディア内の Recycler フォルダ(無い場合は作成)に作成することにより感染活動を実施する。

```
<リムーバブルドライブ>¥Recycler¥S-%d-%d-%d-%d%d%d-%d%d%d%d-%d%d%d%d-%d
```

マルウエアは、これらのドライブへのアクセス時に自動実行されるよう"AUTORUN.INF" というファイルを作成する。このファイルには、ウイルス対策製品等による検知を避けるため、ランダムな文字列が含まれている。

また、マルウエアは非表示のウィンドウを作成して、ドライブへのアクセスを監視する。アクセスが確認されると、上記の感染活動を行う。

◆ ネットワーク共有フォルダ経由の感染活動

マルウエアは、"NetWkstaGetInfo" API を使用してプラットフォーム特有の情報、ドメイン名とローカルコンピュータ名、オペレーティングシステムに関する情報など、コンピュータ環境に関する情報を取得する。そして、マルウエアは"NetServerEnum" API を使用してドメイン内に表示された特定のタイプのサーバを全てリストアップし、"WNetAddCoonection2" API を使用して順番に接続を試みる。この時、445/tcp

を利用するため、感染活動の間この TCP ポートのトラフィックが増加する。

マルウエアは接続の際、まず感染したコンピュータにログインしているユーザの ID とパスワードで認証を試みる。接続に失敗した場合、接続対象のコンピュータのユーザを"NetUserEnum" API を利用してリストアップし、以下のパスワードを用いて、ブルートフォース方式で接続を試みる。

000	0000	00000	0000000	00000000
0987654321	111	1111	11111	111111
1111111	11111111	123	123123	12321
123321	1234	12345	123456	1234567
12345678	123456789	1234567890	1234abcd	1234qwer
123abc	123asd	123qwe	1q2w3e	222
2222	22222	222222	2222222	22222222
321	333	3333	33333	333333
3333333	33333333	4321	444	4444
44444	444444	4444444	44444444	54321
555	5555	55555	555555	5555555
55555555	654321	666	6666	66666
666666	6666666	66666666	7654321	777
7777	77777	777777	7777777	77777777
87654321	888	8888	88888	888888
8888888	88888888	987654321	999	9999
99999	999999	9999999	99999999	a1b2c3
aaa	aaaa	aaaaa	abc123	academia
access	account	Admin	admin	admin1
admin12	admin123	adminadmin	dministrator	anything
asddsa	asdfgh	asdsa	asdzxc	backup
boss123	business	campus	changeme	cluster
codename	codeword	coffee	computer	controller
cookie	customer	database	default	desktop
domain	example	exchange	explorer	file
files	foo	foobar	foofoo	forever
freedom	fuck	games	home	home123
ihavenopass	Internet	internet	intranet	job
killer	letitbe	letmein	Login	login
lotus	love123	manager	market	money

monitor	mypass	mypassword	mypc123	nimda
nobody	nopass	nopassword	nothing	office
oracle	owner	pass	pass1	pass12
pass123	passwd	password	Password	password1
password12	password123	private	public	pw123
q1w2e3	qazwsx	qazwsxedc	qqq	qqqq
qqqqq	qwe123	qweasd	qweasdzxc	qweewq
qwerty	qwewq	root	root123	rootroot
sample	secret	secure	security	server
shadow	share	sql	student	super
superuser	supervisor	system	temp	temp123
temporary	temptemp	test	test123	testtest
unknown	web	windows	work	work123
xxx	xxxx	xxxxx	zxccxz	zxcvb
zxcvbn	zxcxz	zzz	zzzz	zzzzz

マルウエアは、対象コンピュータへの接続に成功すると、ランダムな名称のファイルを用い、感染時にログインしているユーザの個人情報を利用してディレクトリ″Admin$¥System32″内に自身のコピーを作成する。

ネットワーク上での感染活動に成功すると、″NetScheduleJobAdd″APIを用いてフォルダ″*＜Windows フォルダ＞*¥Tasks″内にスケジュール化されたタスクファイルを作成し、自身のコピーがタスクとして実行されるようにする。タスクの実行時間は、″GetLocalTime″APIの返す日時を利用して設定する。このスケジュール化されたタスクファイルは、トレンドマイクロの製品では「TROJ_DOWNADJOB.A」として検出される。

◆ Webサイトからのダウンロードと実行

マルウエアは2009年以降、1月以降である場合、UTC(世界協定時)を元にしてランダムなドメイン名を含む250種類のURL[13]を作成し、自身のアップデートファイルをダウンロード・実行しようと試みる。

[13] URLの一覧については、下記を参照。
http://www.trendmicro.co.jp/vinfo/secadvisories/default6.asp?VNAME=WORM%5FDOWNAD%2EAD+URLs&Page=

URL のおおまかな作成方法と利用方法を次に示す。

1. 一般的な Web サイトにアクセスし、現在の日付を確認する
2. 日付を元に、ランダムな文字列を計算する
3. ランダムな文字列に TLD(Top Level Domain)を付け加えて URL を作成する
4. URL にアクセスする
5. Web サイトの IP アドレスを取得する
6. IP アドレスを利用して URL を作成し、ファイルをダウンロードする
7. ダウンロードしたファイルを実行する

以上、ファイルの取得と実行までの各段階の詳細について述べる。

《一般的な Web サイトにアクセスし、現在の日付を確認する》

以下の一般的な Web サイトの URL に接続し、レスポンスヘッダから日付を読み出す。日付を読み出せない場合、ワームは感染したコンピュータの日付を利用する。

```
http;//www.aol.com                    http;//www.google.com

http://www.ask.com                    http://www.msn.com

http://www.baidu.com                  http://www.myspace.com

http://www.cnn.com                    http://www.w3.org

http://www.ebay.com                   http://www.yahoo.com
```

《日付を元に、ランダムな文字列を計算する》

読み出した日付を元に計算を行い、ランダムな文字列を作成する。ここでは例示として“abcdef”が作成されたとする。

《ランダムな文字列に TLD(Top Level Domain)を付け加えて URL を作成する》

ランダムな文字列の末尾に、次のいずれかの文字列を追加してドメイン名を作成する。この場合は ″abcdef.biz″, ″abcdef.cc″, ″abcdef.cn″ 等となる。ここでは、″abcdrf.com″ が選ばれたとする。このドメイン名が、そのままアクセスするための URL となる。

```
.biz            .cc             .cn             .com            .info
.net            .org            .ws
```

《URL にアクセスする》

マルウエアは、作成した URL に実際にアクセスし、URL の示す Web サイトがアクティブな状態にあるか確認する。

《Web サイトの IP アドレスを取得する》

マルウエアは、ホスト名に対応する IP アドレスを取得しようとする。

《IP アドレスを利用して URL を作成し、ファイルをダウンロードする》

マルウエアは、取得した IP アドレスをパラメータとして用いてスレッドを作成し、次のような URL からファイルのダウンロードを行い、"GetTempPath" API および "GetTempFileName" API を使用してテンポラリフォルダに保存する。

```
http://＜IP アドレス＞/search?q=0&aq=7
```

《ダウンロードしたファイルを実行する》

マルウエアは、ダウンロードしたファイルを"CreateProcess" API を使用して実行する。

◆ Web サイトへのアクセス妨害

マルウエアは、以下の Windows API をフックし、リストに示す文字列のいずれかを含む Web サイトにアクセスしようとした際、タイムアウトを返すように変更してアクセスを妨害する。ユーザには、サーバがダウンしているように見える。

- “DnsQuery_A” API
- “DnsQuery_UTF8” API
- “DnsQuery_W” API
- “Query_Main” API

対象となる文字列のリストを示す。これらの文字列は、主にウイルス対策プログラムに関連している。

```
ahnlab          arcabit         avast           avg.            avira
avp.            bit9.           ca.             castlecops      Ccert.
centralcommand                  clamav          comodo
computerassociates              cpsecure        defender        drweb
emsisoft        esafe           eset            etrust          ewido
f-prot          f-secure        fortinet        gdata           grisoft
hacksoft        hauri           ikarus          jotti           k7computing
kaspersky       malware         mcafee          microsoft       nai.
networkassociates               nod32           norman          norton
panda           pctools         prevx           quickheal       rising
rootkit         sans.           securecomputing sophos          spamhaus
spyware         sunbelt         symantec        threatexpert    trendmicro
vet.            virus           wilderssecurity windowsupdate
```