



USB 接続機器を介して拡散する ウイルスの被害報告が急増しています。

現在、USB フラッシュメモリをはじめとする USB 接続機器を介して拡散するウイルスの被害報告がアジア圏にて急増しています。トレンドマイクロでは、利便性の高まった外部記憶媒体による安全なデータ交換を実現するべく、新たな事前予防検出技術を逐次投入しています。ここでは、最新の拡散手法とその対策手法についてご紹介いたします。

■新たなウイルス拡散経路として注目されるUSBネットワーク

USB (Universal Serial Bus: ユニバーサル・シリアル・バス) ネットワークとは、多くのデジタル機器における標準的な接続規格として採用されているものです。

USB ネットワーク規格を採用したデジタル機器のうち、代表的なものがリムーバブルディスクです。

特に USB フラッシュメモリが広く一般に普及しています。コンパクトな外観にもかかわらず、数 GB 以上の大容量データの保存が可能であり、オペレーティングシステムベンダー各社による「USB Mass Storage Class」規格の採用によって、USB ポートさえあればソフトウェアや専用読み取り装置を意識することなく利用可能となりました。

普及と共に低価格化が進んでいます。これまで長らくデータ交換メディアの主役を務めてきた「フロッピーディスク」に代わり、データ大容量時代におけるデジタルデータの交換媒体として、USB フラッシュメモリをはじめとする USB ネットワークを使用したリムーバブルメディアが新たな主役として活躍していくことが予測されます。

こうした背景とともに、悪意あるユーザによるウイルス拡散媒体としての悪用事例が報告されています。

■グローバルランキングから見るウイルス脅威

2007年10月度のトレンドマイクロ ウイルストラッキングセンター¹データによれば、PE_LUDER.CH が363,544の感染数により、グローバルランキングの1位にランクインしています。

同ウイルスはPE_LUDER.CH-Oと呼ばれるマザーウイルスによって安全なファイルが書き換えられています。このマザーウイルスがリムーバブルメディアによって拡散されています。

同ウイルスは台湾の教育機関において、USB フラッシュメモリを介して大規模拡散したことが報告されています。

■アジア太平洋地域に特化したウイルス脅威

リムーバブルメディアによるウイルス拡散は、アジア太平洋地域 (APAC: Asia-Pacific) からの報告が顕著です。下記は2006年12月から2007年10月までのウイルスランキングより、リムーバブルメディアによる拡散機能を持つウイルスを抽出し整理したデータです。

順位	検出名	APAC 地域 感染数	World Wide 感染数に占める APAC 感染割合
1	PE_LUDER.CH	339,324	91%
2	PE_FUJACKS.EA-O	33,158	77%
3	WORM_VB.CBY	30,514	86%
4	WORM_RJUMP.A	27,654	28%
5	WORM_VB.CII	24,839	60%

上記の通り、World Wideの感染数に占めるAPAC地域の感染割合が非常に高い数値を示しています。APAC地域を狙ったウイルスにおいて、リムーバブルメディアによる拡散機能を実装している傾向が高いといえます。

¹トレンドマイクロ ウイルストラッキングセンターのデータは、弊社のオンラインスキャンで検出された実際のウイルス感染数と、弊社製品「Trend Micro Control Manager」で検出されたウイルス感染情報をまとめたものになります。

※TRENDMICRO、ウイルスバスターはトレンドマイクロ株式会社の登録商標です。

※各社の社名および製品名は、各社の商標または登録商標です。

Copyright (c) 2007-2008 Trend Micro Incorporated. All Rights Reserved.

■攻撃の事例

USB 接続機器を介して拡散するウイルスの攻撃事例は、管理されていない機器を安易に接続したことにより拡散に至っていることが多く報告されています。

USB フラッシュメモリは企業のノベルティとして配布されているケースがあります。このため、管理されていない機器が管理者の知らないところで増加している可能性があります。こうした管理の行き届いていない機器は、時として企業に甚大な被害を与えうる場合があります。

悪意あるユーザは USB フラッシュメモリにウイルスと USB フラッシュメモリ利用時にウイルスが自動起動するよう設定したファイルを混入させておきます。ユーザが何も知らずに USB フラッシュメモリを利用することによって、PC にウイルス感染します。

さらに、ウイルス感染した PC がより悪質化したウイルスをインターネットからダウンロードしてくるケースも報告されています。



図1. クリーンな PC へ感染 USB が接続された例（悪意あるユーザによりウイルスが混入された USB フラッシュメモリを使用したことにより、攻撃が開始）



図2. USB フラッシュメモリを介した拡散活動例（ウイルス感染した PC へクリーンな USB フラッシュメモリが挿入され、汚染。感染 USB フラッシュメモリの再利用によりウイルスが拡散）

ウイルスはドライブ接続状態の監視の結果、拡散可能なリムーバブルメディアであると判定した場合に、挿入された USB フラッシュメモリに自身をコピーし、クリーンな USB フラッシュメモリへウイルス感染させます。

感染 USB フラッシュメモリはデータ交換のため、再利用されます。再利用時に更にウイルスが拡散されることによって、被害が拡大していきます。

次に、拡散活動に注目してみましょう。

感染 PC へクリーンな USB フラッシュメモリが挿入されます。感染 PC ではウイルスによって、ドライブの接続状態が常に監視されています。ウイルスによってはドライブの種類（ネットワークドライブ、リムーバブルドライブなど）まで監視しているものも報告されています。

※TRENDMICRO、ウイルスバスターはトレンドマイクロ株式会社の登録商標です。

※各社の社名および製品名は、各社の商標または登録商標です。

Copyright (c) 2007-2008 Trend Micro Incorporated. All Rights Reserved.

■自動起動を実現させる「Autorun.inf」ファイル

Windows OS では、自動起動と呼ばれる機能により、設定ファイル「Autorun.inf」に記述された内容に従って、リムーバブルメディア接続時の振る舞いを制御することができます。

本来この機能を利用することによって、CD-ROMドライブにCDを挿入することによって、アプリケーションのインストーラを自動的に起動したり、音楽CDを自動再生させたりします。

悪意あるユーザはこの機能を悪用し、リムーバブルメディア利用時にウイルスである実行ファイルを起動するように「Autorun.inf」を記述します。

Windows Vista の場合

初期設定において、「Autorun.inf」に実行ファイルが起動するように指定されているリムーバブルメディアを接続した場合、直ちに該当の実行ファイルが起動されます。

Windows XP/2000 の場合

初期設定において、「Autorun.inf」に実行ファイルが起動するように指定されているリムーバブルメディアを接続した場合でも、直ちに該当の実行ファイルが起動されることはありません。

ただし、[マイコンピュータ]からリムーバブルメディアアイコンをクリックし、ファイル内容を確認した際に該当の実行ファイルは起動されます。

■ニュースで見るUSB接続機器の脅威

USB 接続機器を発端にさまざまな被害が実際に発生しています。

ウイルス関連のニュースから USB 接続機器が発端になっているものを集めました。

報告日	タイトル
2007-10-11	USB フラッシュメモリ製品の一部にウイルスが混入 http://is702.jp/news/detail.php?id=76
2007-07-13	防水型 SD オーディオプレーヤーにウイルス混入 http://is702.jp/news/detail.php?id=42
2007-07-04	USB メモリを介して感染するウイルスが増加 http://is702.jp/news/detail.php?id=40
2007-01-31	パソコン周辺機器から USB 経由でウイルス感染 http://is702.jp/news/detail.php?id=4

情報提供: インターネット・セキュリティ・ナレッジ
<http://is702.jp/>

※TRENDMICRO、ウイルスバスターはトレンドマイクロ株式会社の登録商標です。

※各社の社名および製品名は、各社の商標または登録商標です。

Copyright (c) 2007-2008 Trend Micro Incorporated. All Rights Reserved.

■ベストプラクティス

許可されていない機器を利用しない、許可されていない場所で利用しない

利用者は許可されていない機器を利用すべきではありません。

管理者は安全と利便性を最大限考慮し、セキュリティポリシー（機器の利用許可）を設計しています。無許可な機器の利用は想定外の問題を引き起こし、多くの関係者に損害を与える危険性があります。新しい機器の利用には、まず管理者の許可を得た後に開始してください。

また、許可された機器であっても、許可されていない場所で利用すべきではありません。携帯性の優れた機器は外出先で利用する場合があります。このような場合においても、インターネットカフェやホットスポットなど管理者の管理が行き届いていないところで使用すべきではありません。

このような場所はセキュリティ対策が施されていない場合があります。このため、機器が汚染される可能性があります。外出先で汚染された機器を社内で再利用することにより、損害を与える危険性があります。

必要最小限の権限で利用する

管理者は必要最小限の権限を利用者へ付与する必要があります。

Administrator や Power User といった高い権限は必ずしもすべてのユーザに必要なものではありません。必要最小限の権限を付与することで、利用者の誤操作による影響範囲を最小限に留めることが期待できます。

Windows Vista では、ユーザーアカウント制御 (UAC: User Account Control) と呼ばれる新機能が実装されています。オペレーティングシステムにより提供される機能を活用し、セキュリティ強度を高めていくことは非常に有効です。

セキュア USB フラッシュメモリを過信しない

企業においては、セキュリティ機能が実装された USB フラッシュメモリを利用している場合があります。このような場合においてもその機能を過信することなく注意を行うことが重要です。

セキュア USB フラッシュメモリの多くは、「情報漏洩」対策としてデータ暗号化機能が実装されています。本機能は情報の機密性を維持する上で高い効果を発揮しますが、ウイルス拡散防止への効果は低いです。利用している機器によって提供されるセキュリティ機能をご確認ください。

ウイルス検索実施後に接続機器を利用する

利用者は外部機器を接続した後にまず、ウイルス検索を実施することがセキュリティ上有効です。

このとき、最新のウイルス脅威に対応できるよう、必ずウイルスパターンファイルをアップデートする必要があります。

※TRENDMICRO、ウイルスバスターはトレンドマイクロ株式会社の登録商標です。

※各社の社名および製品名は、各社の商標または登録商標です。

Copyright (c) 2007-2008 Trend Micro Incorporated. All Rights Reserved.

対処療法を施しセキュリティ強度を高める

対処療法は一時的なセキュリティ対策としては有効です。

1. 自動起動を無効にする。
自動起動の無効方法は Windows のバージョンにより異なります。マイクロソフト社の公開する情報を確認し、設定を施してください。
 - ・ Microsoft Windows XP プログラム CD の自動再生をオフにする
<http://www.microsoft.com/japan/windowsxp/expertzone/tips/february/knox1.msp>
 - ・ Microsoft Windows Vista ヘルプ : CD および DVD を自動的に再生しないようにする
<http://windowshelp.microsoft.com/Windows/ja-JP/Help/e78dd11a-7dd3-4a06-8436-757bca78e97b1041.msp>
2. リムーバブルドライブのルートフォルダに予め「Autorun.inf」フォルダを作成しておく。

リムーバブルドライブのルートフォルダに予め「Autorun.inf」フォルダを作成しておくことで、ウイルスによる「Autorun.inf」ファイル作成の阻止が期待できます。

ウイルスがリムーバブルドライブに「Autorun.inf」ファイルの作成を試みた場合、図 3 のとおり[ファイルまたはフォルダのコピー エラー]が発生します。



図 3. 「Autorun.inf」フォルダを含むリムーバブルドライブへ「Autorun.inf」ファイルのコピーを行った結果、エラーが発生しています。

※TRENDMICRO、ウイルスバスターはトレンドマイクロ株式会社の登録商標です。

※各社の社名および製品名は、各社の商標または登録商標です。

Copyright (c) 2007-2008 Trend Micro Incorporated. All Rights Reserved.

■悪質化する手口

悪意あるユーザは利用者による対処療法を見越して、より悪質化した手口によってリムーバブルメディアへの拡散を試みているケースが報告されています。ここでは、報告された手口の一部を紹介いたします。

自動起動を強制的に有効にする

自動起動を無効にする対処療法を過信すべきではありません。レジストリの変更により、自動機能を強制的に有効にさせるウイルスの流通が報告されています。このため、自動機能を予め無効にしておく対処療法が無効化させられる危険性があります。

フォルダオプションの変更を無効化する

「Autorun.inf」ファイルには[システムファイル]属性、[隠しファイル]属性が付与されています。このため、隠しファイルが表示されるようにフォルダオプションを変更しておかなければ、Windows エクスプローラ上で「Autorun.inf」ファイルを表示させることができません。

フォルダオプションの変更方法

1. Windows エクスプローラを起動します。
2. [ツール]メニューの[フォルダ オプション]をクリックし、[表示]タブをクリックします。
3. [ファイルとフォルダの表示]の[すべてのファイルとフォルダを表示する]をクリックし、[OK]をクリックします。

しかしながら悪質化したウイルスにおいては、フォルダオプションの変更を受け付けないようにシステム改変するウイルスの流通が報告されています。

このような場合、attrib コマンドにより属性を解除することで、Windows エクスプローラ上で表示させることが可能です。

```
C:¥> attrib -R -S -H <リムーバブルドライブレター>:¥autorun.inf
```

図 4. コマンドラインよりリムーバブルドライブ上の「autorun.inf」より[読み取り]/[システム]/[隠しファイル]属性を取り除く方法。<リムーバブルドライブレター>は、リムーバブルドライブに割り当てられたドライブ文字になります。

「Autorun.inf」ファイルを隠蔽する

Windows エクスプローラによる「autorun.inf」ファイルの有無確認を過信すべきではありません。悪質化したウイルスにおいては、Windows のシステムファイルを改変し、Windows エクスプローラから「autorun.inf」の表示を隠蔽する技術(ルートキット)が悪用されているケースが報告されています。

CD-R、CD-RW への拡散も試みる

狙われている USB 接続機器は USB フラッシュメモリに止まりません。Windows の CD ライティング機能を悪用し拡散を試みるウイルスの流通が報告されています。Windows XP では CD 書き込み用データを一端ステーjing領域と呼ばれる隠しフォルダに格納します。この隠しフォルダ内にウイルスをコピーし、作成する CD メディアにウイルス感染させるケースが報告されています。

```
C:¥Documents and Settings¥<ユーザ名>¥Local Settings¥Application Data¥Microsoft¥CD Burning
```

図 5. ステージング領域として設定されている隠しフォルダ

■新たな脅威の報告にご協力ください：事前予防検出名「Mal_Otorun」

トレンドマイクロでは、USB 接続機器を介して発生する脅威の高まりを受け、ウイルスパターンファイルの事前予防検出機能を強化し、ウイルスを実行させる疑いのある「Autorun.inf」を Generic パターンで検出させる機能を追加しています。

これにより、既知のウイルスにて使用されている技術を転用して作成したような新種・亜種ウイルスについて、事前に予防措置を施しておくことが可能となります。

お客様の環境において、「Mal_Otorun1」「Mal_Otorun2」が繰り返し検出される場合、新種・亜種ウイルスが存在している可能性があります。下記の手順にて、ウイルス検体ファイルおよび「Mal_Otorun」として検出されたファイルを、サポートセンターへご提供いただきますようお願い申し上げます。

【手順】

1. 隠しファイルを表示する設定にします。
2. MAL_OTORUN が検出されたリムーバブルドライブをウイルスログなどから確認します。
例：F:\autorun.inf
3. 「スタート」ボタンを右クリックし、「エクスプローラ」をクリックします。
4. 左側のツリーからリムーバブルドライブをクリックします。
(注：右側のウィンドウでドライブを開くと、ウイルスが実行される可能性があります。必ず左側のツリーからドライブを開いてください。)
5. 表示されたファイル名のうち以下の拡張子のファイル名を確認し、メモ等に記録します。
(注：該当するファイルが存在しない場合は、MAL_OTORUN として検出されたファイルを弊社テクニカルサポートセンターまでご送付ください。)
 - * .bat
 - * .cmd
 - * .com
 - * .exe
 - * .pif
 - * .scr
 - * .vbe
 - * .vbs
 - * .wsf
6. メモしたファイルをトレンドマイクロ製品で隔離します。
(注：隔離できない場合は、不正プログラムがメモリ上に常駐している可能性があります。不正プログラムを終了した後、トレンドマイクロ製品で隔離してください。)
7. 以下のファイルを弊社テクニカルサポートセンターまでご送付ください。
 - * 手順 6 で隔離したファイル
 - * MAL_OTORUN として隔離されたファイル

※2008/3/17 更新

ウイルス検出名変更により一部を修正いたしました。

「Possible_Otorun1」はウイルスパターンファイル 4.965.00 より、「Mal_Otorun1」へ名称が変更になりました。

「Possible_Otorun2」はウイルスパターンファイル 5.113.00 より、「Mal_Otorun2」へ名称が変更になりました。

■参考情報

Trend Micro Security Blog : 「USB ドライブの危険性」(2007 年 10 月 12 日)

<http://blog.trendmicro.co.jp/archives/1230>

Trend Micro Security Blog : 「ターゲット攻撃による不正プログラムの大規模拡散に対する対症療法」(2007 年 10 月 23 日)

<http://blog.trendmicro.co.jp/archives/1237>

※TRENDMICRO、ウイルスバスターはトレンドマイクロ株式会社の登録商標です。

※各社の社名および製品名は、各社の商標または登録商標です。

Copyright (c) 2007-2008 Trend Micro Incorporated. All Rights Reserved.

トレンドマイクロ株式会社