PCネットワークの管理活用を考える会
ITマネジメント研究会 初心者編

我々は情報リスクに
どう立ち向かうべきか

帝塚山大学
経営情報学部
教授　高瀬　宜士

ＩＴスキルには
情報セキュリティーも含まれる

- 情報セキュリティは、JIS Q 27002（すなわちISO/IEC 27002）によって、情報の機密性、完全性、可用性を維持することと定義されている。それら三つの性質の意味は次のとおり。
- 機密性 (confidentiality): 情報へのアクセスを認められた者だけが、その情報にアクセスできる状態を確保すること
- 完全性 (integrity): 情報が破壊、改ざん又は消去されていない状態を確保すること
- 可用性 (availability): 情報へのアクセスを認められた者が、必要時に中断することなく、情報及び関連資産にアクセスできる状態を確保すること
- これら三つを、英語の頭文字を取って、情報のCIAとも呼ぶ

出所：ウィキペディアより

毎日新聞サイト改ざん、偽ウイルス対策ソフトで

（2010年9月28日09時51分　読売新聞）

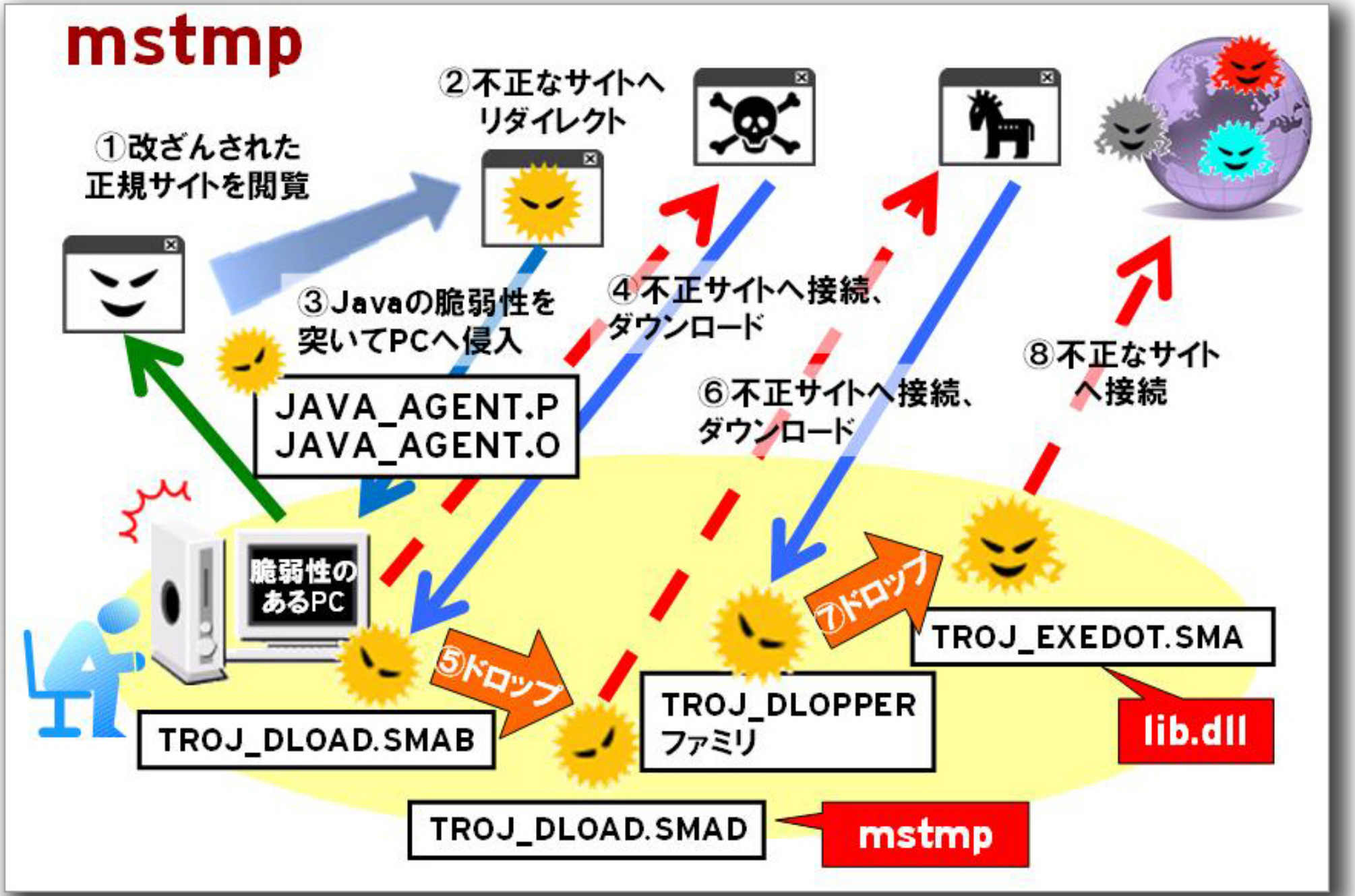
- 毎日新聞のニュースサイトなど国内９８サイトが２４日夜、ネット広告会社の広告配信を通じて改ざんされ、コンピューターウイルスを埋め込まれていたことが分かった。
- サイトを閲覧すると別の不正サイトに自動的に移動、偽のウイルス対策ソフトによってクレジットカード番号などの個人情報を盗まれた恐れがある。延べ閲覧者数は約８００万人に上るとみられる。
- ほかに改ざんが確認されたのは、口コミでグルメ情報を紹介する「食べログ」や家電などの価格を比較する「価格．ｃｏｍ」、ニュースを配信する「Ｊ―ＣＡＳＴニュース」など。
- これらのサイトにバナー広告を配信しているネット広告会社「マイクロアド」（東京）のサーバーが海外からのサイバー攻撃を受けてプログラムを書き換えられ、契約している各サイトへの広告配信を通じて次々と感染を広げたとみられる。同社によると、２４日午後９時半頃改ざんされ、午後１１時半頃に修復 した。同社はその間の延べ閲覧者数は約８００万人に上るとみている。
- 悪用されたのは、「セキュリティー・ツール」と呼ばれる偽のウイルス対策ソフト。パソコンにセキュリティー上問題があるかのような警告画面が出 て、ウイルス対策ソフトの購入を勧められ、購入しようとクレジットカード番号を入力すると、そのまま情報を抜き取られる仕組み。番号を入力しないまま放置 しても、インターネットに接続できなくなるなどの支障が出る。

国内100社以上で感染被害を確認。拡散する不正プログラム

- トレンドマイクロでは、”mstmp” や “lib.dll” といったファイル名で拡散する不正プログラムの攻撃により、日本国内の企業において100社以上の感染被害が発生していることを確認しています。
- 本攻撃の大まかな流れは以下の通りとなります。

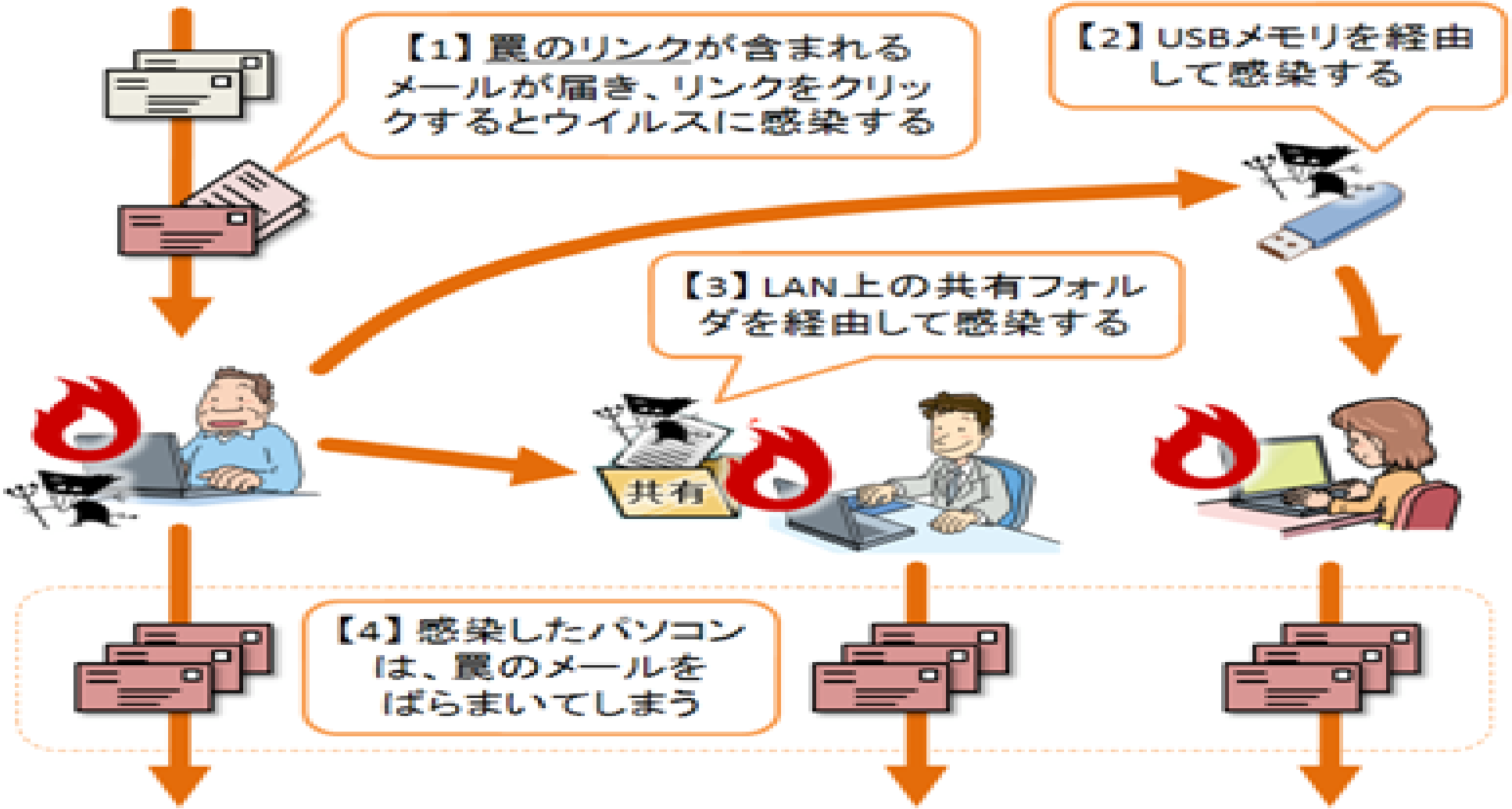
1. ユーザが改ざんされた正規Webサイトを閲覧
2. 正規サイト内に仕掛けられたコードによって不正サイトへリダイレクト
3. 不正サイトから、Java の脆弱性を悪用する不正プログラム「JAVA_AGENT.P」「JAVA_AGENT.O」をダウンロード
4. 「JAVA_AGENT.P」「JAVA_AGENT.O」が「TROJ_DLOAD.SMAB」をダウンロード
5. 「TROJ_DLOAD.SMAB」が「TROJ_DLOAD.SMAD」を作成
6. 「TROJ_DLOAD.SMAD」が「TROJ_DROPPER」ファミリの不正プログラムをダウンロード
7. 「TROJ_DROPPER」ファミリの不正プログラムが「TROJ_EXEDOT.SMA」を作成
8. さらに、「TROJ_EXEDOT.SMA」が不正なWebサイトへ通信

10月22日　http://blog.trendmicro.co.jp/archives/3723



「 迷惑メールをはじめとした様々な経路で拡散する新たなウイルスが出現！ 」

VBMania（ブイビーマニア）



2010年10月 5日　独立行政法人情報処理推進機構　セキュリティセンター(IPA/ISEC)

■対策・注意喚起

- 本攻撃の最終的な意図は明らかになっておりませんが、正規サイト改ざんを端緒とした「Web からの脅威」は引き続き巧妙化を続け、ユーザに忍び寄ることが考えられます。
- ユーザの方におかれましては、

1. OS、アプリケーションを最新の状態にする
2. 最新バージョンのセキュリティソフトを導入し、最新の状態に保つ

- といった2点を改めて徹底ください。

まずは基本を学ぶ
ウイルスって何？

- ウイルスは、人が病気になるときの病原体のひとつですが、コンピュータの世界のウイルスとはどのようなものなのでしょうか。
- ここでは、情報セキュリティの対策を立てる上で避けては通れないコンピュータウイルスについて、その動作、過去に発生したウイルスの解説、その対策について説明します。

コンピュータウイルスとは
ウイルスの変遷
基本的なウイルスの動作
ボットとは？
ウイルスを駆除するためには

出所：http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/kiso/k04.htm

コンピュータウイルスとは

- 第三者のプログラムやデータベースに対して意図的に何らかの被害を及ぼすように作られたプログラムであり、次の機能を一つ以上有するもの。
（1）自己伝染機能
自らの機能によって他のプログラムに自らをコピーし又はシステム機能を利用して自らを他のシステムにコピーすることにより、他のシステムに伝染する機能
（2）潜伏機能
発病するための特定時刻、一定時間、処理回数等の条件を記憶させて、条件が満たされるまで症状を出さない機能
（3）発病機能
プログラムやデータ等のファイルの破壊を行ったり、コンピュータに異常な動作をさせる等の機能

（1990年4月10日通商産業省制定「コンピュータウイルス対策基準」より）

ウイルスの変遷

- 1990年代後半から2000年代初めにかけては、コンピュータの利用形態がスタンドアロンからインターネットへ移行していく過程であり、Melissa（メリッサ）やLOVELETTER（ラブレター）などの電子メールの添付ファイルで感染するウイルスが増えてきました。さらには、CodeRed（コードレッド）、MSBlaster（エムエスブラスター）などのセキュリティホールを狙う大規模感染型のウイルスも現れました。これらのウイルスは、攻撃者の興味本位や自己技術の誇示、愉快犯的な発想により作成されたものと考えられています。
- これに対して、2002年ごろから、Agobot（アゴボット）をはじめとするボットが台頭してきました。ボットはそれまでの愉快犯的な発想によるウイルスとは異なり、金銭的な利益の追求という明確な目的をもって作られています。

出所：http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/kiso/k04.htm

ウイルスの変遷

- ボットは、ボットネットワークという巨大なネットワークを構成し、ボットネットワークをコントロールする犯罪組織によって、DoS 攻撃やDDoS 攻撃、迷惑メール配信、情報漏洩などに利用されています。
- 最近の傾向としては、旧来の愉快犯的な発想によるウ イルスと比べると、感染したことや活動していることに気付かれないように密かに動作するようになり、ウ イルスの脅威が見えにくくなっているのが特徴と言えます。

出所：http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/kiso/k04.htm

基本的なウイルスの動作

- コンピュータウイルスは、フロッピーディスクや電子メール、ホームページの閲覧など、そのウイルスのタイプによってさまざまな方法で感染します。また、ウイルスに感染すると、コンピュータシステムを破壊したり、他のコンピュータに感染したり、そのままコンピュータに残ってバックドアと呼ばれる不正な侵入口を用意したりするなど、さまざまな活動を行います。
- では、主なウイルスを感染経路と活動方法によって分類してみましょう。

出所：http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/kiso/k04.htm

ウイルスの感染経路

- マクロプログラムの実行
  - マイクロソフト社のOffice アプリケーション（Word、Excel、PowerPoint、Access）のマクロ機能を利用して感染するタイプのウイルスがあります。これらは、マクロウイルスと呼ばれています。Office アプリケーションのマクロ機能では、高度なプログラム開発言語であるVBA（Visual Basic for Applications）を使用することができるため、ファイルの書き換えや削除など、コンピュータを自在に操ることが可能になります。そのため、マクロウイルスに感染したドキュメントは、ファイルを開いただけでVBAで 記述されたウイルスが実行されて、自己増殖などの活動が開始されます。

出所：http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/kiso/k04.htm

ウイルスの感染経路

- **ホームページの閲覧**
  - 現在のWeb ブラウザは、ホームページ上でさまざまな処理を実現できるように、JavaScriptやVBScript、ActiveX コントロール、Javaなどのプログラムを実行できるようになっています。そのため、これらのプログラムでウ イルスが埋め込まれたホームページを閲覧した場合は、コンピュータがウ イルスに感染してしまいます。
  - 最近では、Web ブラウザやWeb ブラウザへのプ ラグインソフトの脆 弱性を利用した感染方法が増加してきており、ホームページを閲覧するだけでウ イルスに感染させる手口はますます巧妙化してきています。
  - かつては怪しいWeb サイトを訪問しなければ大丈夫と思われていましたが、近年ではSQL インジェクションという手口が横行し、正規のWeb サイトがウ イルス付きの内容に書き換えられてしまうケースが急増しています。この場合には、正規のWeb サイトを訪問した場合であっても、ウ イルスに感染してしまうことになります。

出所：http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/kiso/k04.htm

ウイルスの感染経路

- 電子メールの添付ファイル
  - ウイルスの感染経路として一般的なのは、電子メールの添付ファイルです。電子メールの添付ファイルとして送信されたウイルスを誤って実行すると、そのウイルスに感染してしまいます。
- USBメモリからの感染
  - 多くのコンピュータでは、USBメモリをコンピュータに差し込んだだけで自動的にプログラムが実行される仕組みが用意されています。この仕組みを悪用して、コンピュータに感染するウイルスがあります。このようなウイルスの中には、感染したコンピュータに後から差し込まれた別のUSBメモリに感染するなどの方法で、被害が拡大されていくこともあります。

出所：http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/kiso/k04.htm

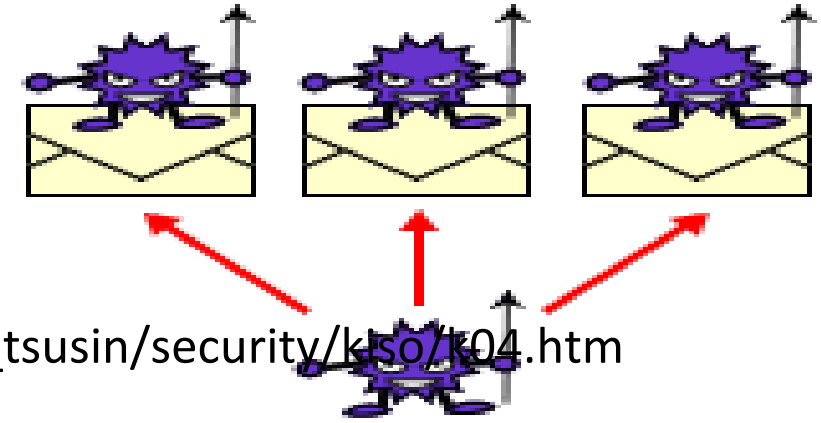
ウイルスの感染経路

- ファイル共有ソフトによる感染
  - ファイル共有ソフトとは、インターネットを利用してファイルをやり取りするソフトウェアのことです。ファイル共有ソフトでは不特定多数のユーザーが自由にファイルを公開することができるため、別のファイルに偽装するなどの方法でいつの間にかウイルスを実行させられてしまうことがあります。
- 偽のウイルス対策ソフト
  - あたかも無料のウイルス対策ソフトのように見せかけて、ウイルスがインストールされてしまう被害が増えています。その代表的な手口は、ホームページなどで「あなたのコンピュータはウイルスに感染しています」のようなメッセージを表示し、偽のウイルス対策ソフトのダウンロード用Web サイトに誘導する方法です。

出所：http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/kiso/k04.htm

ウイルスの活動内容

- **自己増殖**
- ウイルスのほとんどは、インターネットやLANを使用して、他の多くのコンピュータに感染することを目的としています。特にワーム型と呼ばれるウイルスは、自分自身の複製を電子メールの添付ファイルにして送信したり、ネットワークドライブに保存されているファイルに感染したりするなど、ユーザーの操作を介さずに自動的に増殖していきます。



出所：http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/kiso/k04.htm

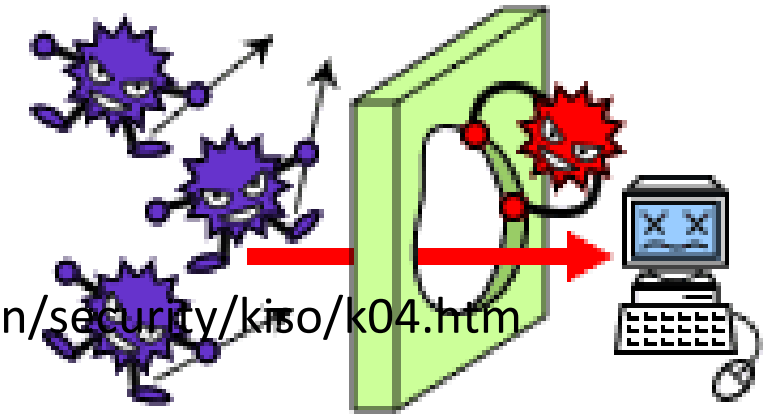
ウイルスの活動内容

- **情報漏洩**
- ウイルスによる情報漏洩は、大きく分類すると、インターネットの特定のWebサイトやメールアドレスにデータを送信するケースと、インターネット上に情報を公開するケースがあります。ウイルスによって漏洩する情報は、ユーザーアカウントやパスワード、コンピュータ内のファイル、メール、デスクトップの画像などさまざまです。そして、情報漏洩を目的としたウイルスでは、感染していることに気づかせないようにするため、コンピュータの画面上には何も変化が起こらないことが一般的です。
- なお、ファイル共有ソフトを介して感染するタイプのウイルスによって情報が漏洩した場合には、その情報をネットワークから完全に消去することは非常に困難です。

出所：http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/kiso/k04.htm

ウイルスの活動内容

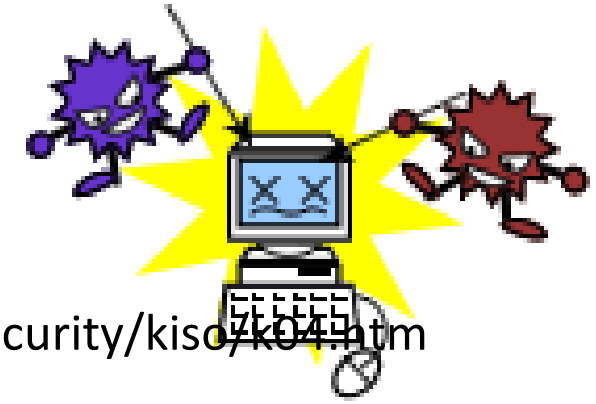
- **バックドアの作成**
- 感染したコンピュータの 内部に潜伏するタイプのウイルスをトロイの木馬と呼びます。この中でもバックドアを作成するタイプのウイルスは極めて悪質なもので、インターネットを通じて、感染したコンピュータを外部から自由に操作されてしまうこともあります。



出所：http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/kiso/k04.htm

ウイルスの活動内容

- **コンピュータシステムの破壊**
- ウイルスによっては、コンピュータシステムを破壊してしまうものがあります。その動作はウイルスによって異なりますが、特定の拡張子を持つファイルを探し出して自動的に削除するものから、コンピュータの動作を停止してしまうものまでさまざまです。



出所：http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/kiso/ku04.htm

ボットとは？

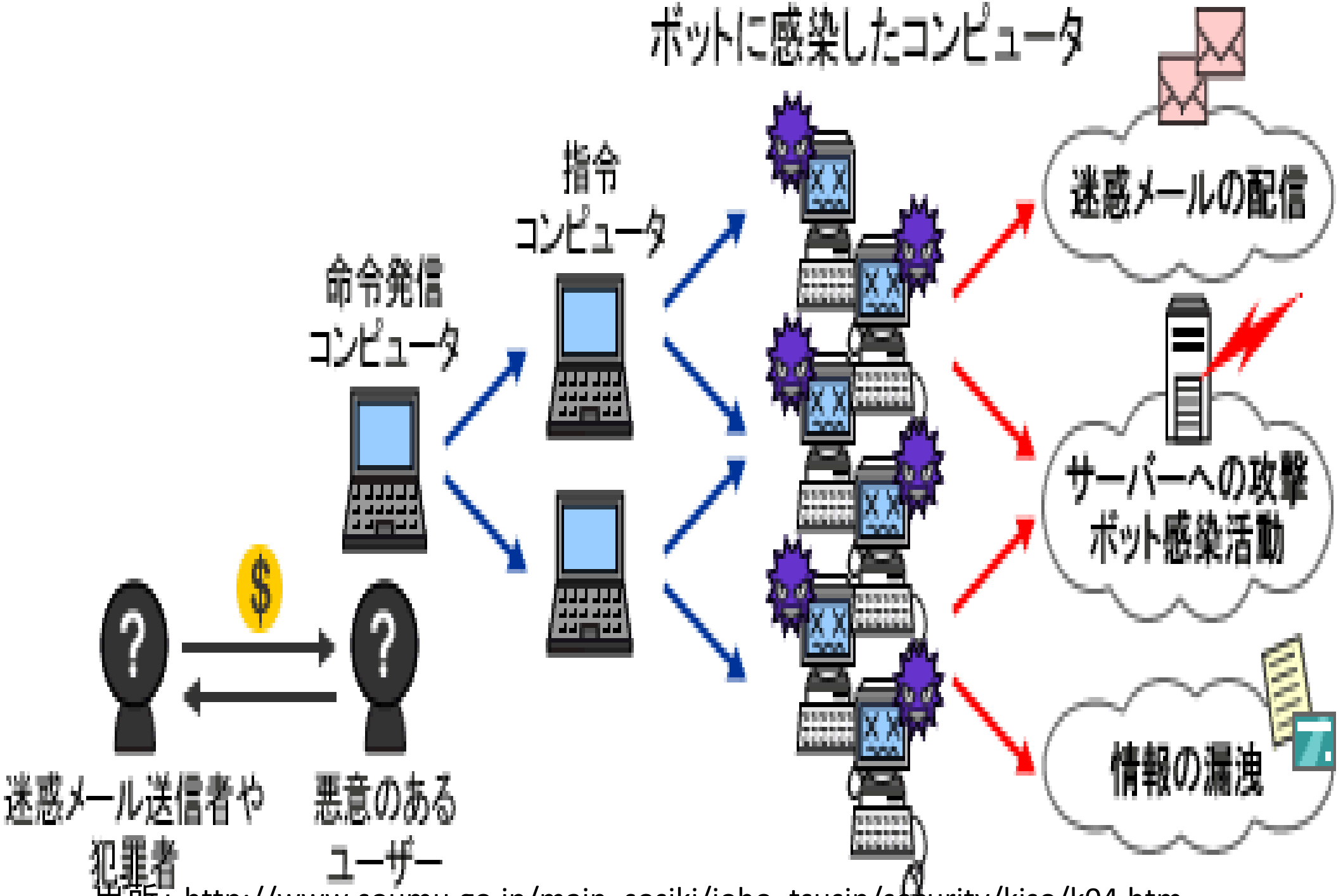
- ボット（BOT）とは、コンピュータを外部から遠隔操作するためのコンピュータウイルスです。ボットに感染したコンピュータは、ボットネットワークの一部として動作するようになります。そして、インターネットを通じて、悪意のあるハッカーが、常駐しているボットにより感染したコンピュータを遠隔操作します。外部から自由に操るという動作から、このような常駐型の遠隔操作ソフトウェアのことをロボット（Robot）をもじってボット（BOT）と呼んでいます。

出所：http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/kiso/k04.htm

ボットとは？

- ボットに感染させたハッカーは、その感染したコンピュータを遠隔操作することで、インターネットに対して、「迷惑メールの配信」、「インターネット上のサーバーへの攻撃」、「感染活動」などの迷惑行為や犯罪行為を行ないます。また、感染したコンピュータに含まれる情報やコンピュータを操作した情報を 盗み出す「スパイ活動」も行なうことがあります。ボットは旧来のウイルスのように愉快犯的な行為で作られたものではなく、迷惑メールの送信者や個人情報を不正に利用しようとする犯罪者と取引するために作られているという点が手口の巧妙化の要因のひとつとなっています。このような目的から、旧来のウイルスと比べると、感染しているということに気付きにくくしているというのも特徴のひとつです。

出所：http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/kiso/k04.htm



出所：http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/kiso/k04.htm

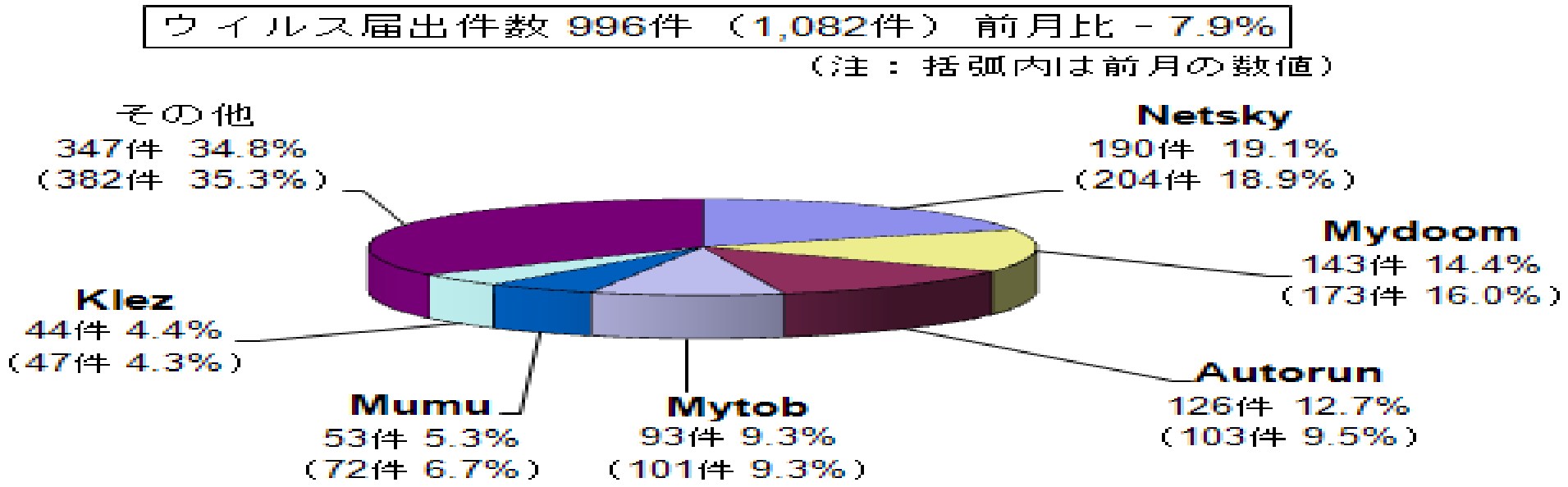
ボットとは？

- ボットに感染したコンピュータとそのコンピュータの持ち主はもちろん被害者なのですが、感染したコンピュータが迷惑メールを送信したり、別のサイトを攻撃したりするため、迷惑メールを受け取ったり、攻撃されたりしたコンピュータから見ると、ボットに操られたコンピュータは加害者になってしまいます。あなた自身が加害者にならないようにするためにも、ボットへの対策はとても大切なことです。

出所：http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/kiso/k04.htm

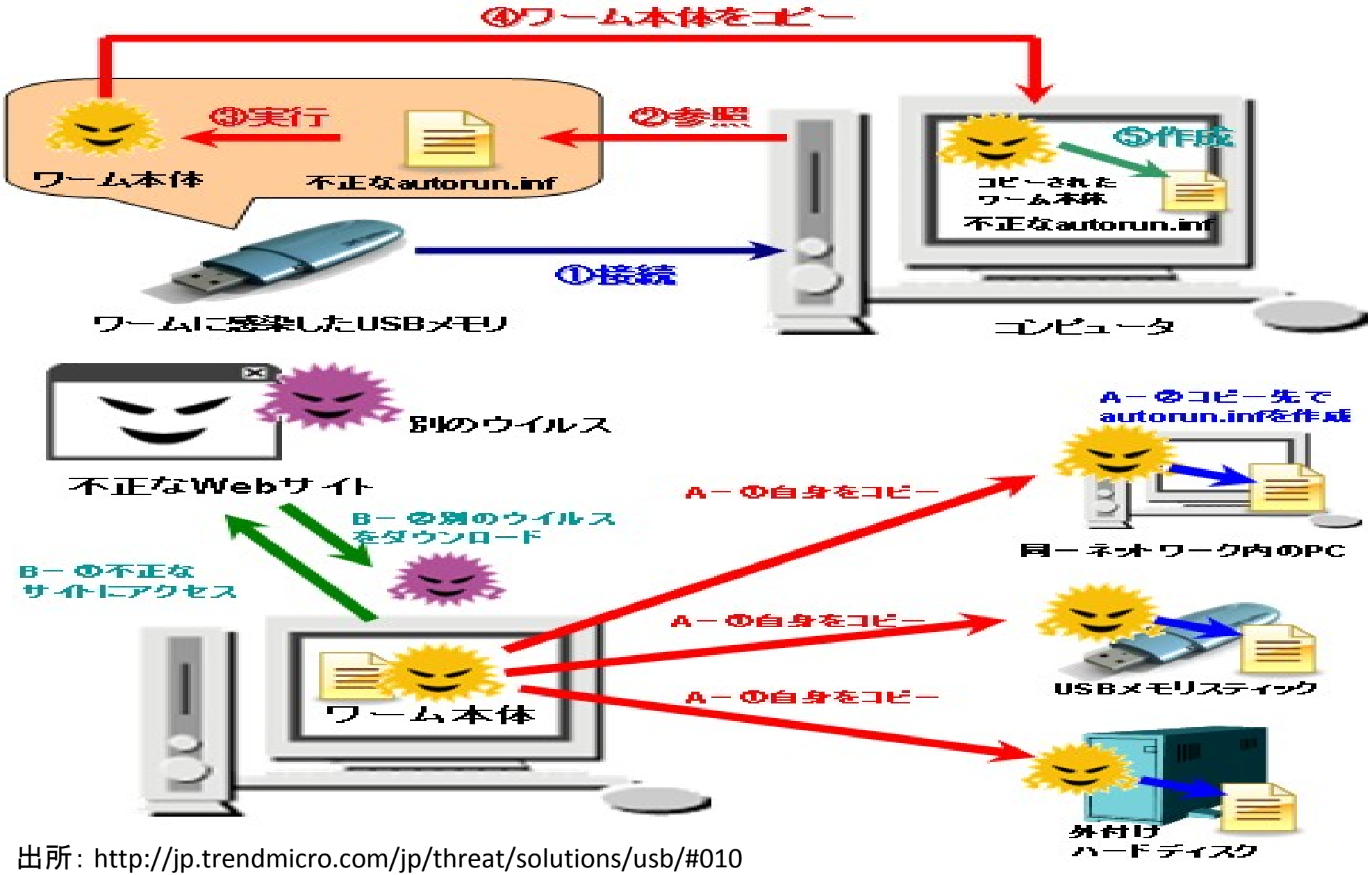
USBメモリーから感染するウイルス 2010年10月実績（オートランウイルス）

- 今、世界で流行しているウイルスの一つは、オートランウイルスです。
- このウイルスはUSBフラッシュメモリーを差すだけで移ることがあります。



出所：http://www.ipa.go.jp/security/txt/2010/11outline.html

オートランウイルスの感染方法



出所：http://jp.trendmicro.com/jp/threat/solutions/usb/#010

USBメモリーから感染するウイルス（オートランウイルス）

- 掲載日：2010年3月4日
  独立行政法人情報処理推進機構
  セキュリティセンター(IPA/ISEC)
- 「自動実行（オートラン）」機能を悪用し、USBメモリなどを経由して感染を広げる「USBメモリ感染型ウイルス」の 被害が続いています。この種のウイルスに対しては、パソコンの「自動実行」機能を無効化することが有効な対策となります。
- 本文書では、主に個人のパソコン利用者（初心者）を対象として、Windowsの「自動実行」機能を無効化するための 手順を紹介しています。

出所：http://www.ipa.go.jp/security/virus/autorun/

ウイルスを駆除するためには

- ウイルスを駆除するためには、コンピュータにウイルス対策ソフトを導入する必要があります。ウイルス対策ソフトは、ワクチンソフト、アンチウイルスソフトと呼ばれることもあります。一般的に、ウイルス対策ソフトはコンピュータの電源がオンであるときには常に起動した状態になり、外部から受け取るデータを常時監視することで、インターネットやLAN、フロッピーディスクなどからコンピュータがウイルスに感染することを防ぎます。また、逆に電子メールなどで外部に送信するデータにウイルスが含まれていないこともチェックしてくれます。コンピュータがウイルスに感染してしまった場合には、コンピュータからウイルスを除去する機能も持っています。

出所：http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/kiso/k04.htm

ガンブラー

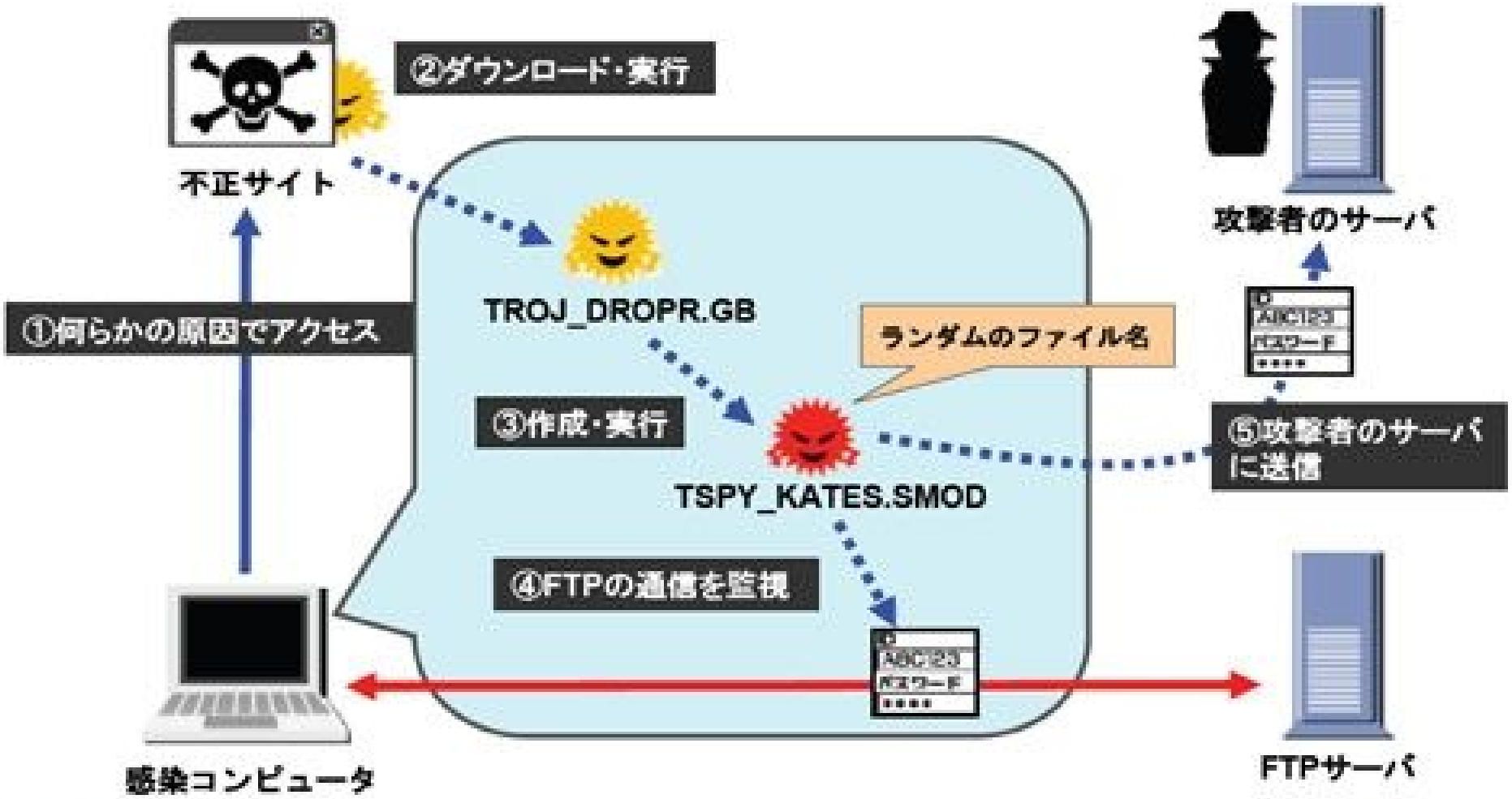
民主党、ホンダ、JR東日本など大手サイトが改ざん被害

- 民主党東京都総支部連合会のウェブサイトも改ざん被害を受けた。12月25日から1月4日にかけて改ざん された状態にあり、閲覧した人はウイルス感染している可能性がある
- ガンブラー（Gumblar、別名 GENOウイルス）と亜種のウイルスによる被害が急拡大している。昨年12月からの被害だけでも、JR東日本、民主党東京都総支部、本田技研、モロゾフ、ハウス食品、信越放送、ローソン、京王電鉄などの大手企業サイトが改ざんされた。また、検索サイトのムーター、ネット情報サイトのデジタルマガジン、輸入 品が中心の商社・三栄コーポレーションの一部ブランドのサイトも改ざんされている。
- この他にも、改ざんされた状態で放置されているサイトが現在もある。検索サイトで探しただけでも中小企業、歯科医院のサイト、通販サイトなどが改 ざんされた状態となっている。セキュリティー大手のカスペルスキーによれば、国内で3000以上のサイトが改ざん被害を受けているそうだ。これらのサイト を表示しただけでウイルスに感染する可能性がある。
- なお、12月中旬以降の改ざん被害の多くは、それ以前とは異なるタイプの攻撃コードが使われている。正確に言うと、それ以前のガンブラーとは異な るが、ガンブラーの亜種の一つと考えてもいいだろう。

ガンブラーという攻撃手法

- **Gumblar**（ガンブラー）とは「Webサイト改ざん」と「Web感染型ウイルス（Webサイトを閲覧するだけで感染するウイル ス）」を組み合わせて、多数のパソコンをウイルスに感染させようとする攻撃手法（手口）のことである。同攻 撃に関連するマルウェアを指す意味でも多用されるが、どの範囲のマルウェアを指すのかはメディアによって様々である。Gumblarによって、国内外で Webサイトの改ざん被害が相次いでいる。
- 日本国内においては、別名で**GENOウイルス**（ジェノウイルス）と呼ばれている

ガンブラー攻撃関連の不正プログラム「TSPY_KATES.SMOD（カテス）」動作概要



出所：http://www.yomiuri.co.jp/net/security/goshinjyutsu/20100108-OYT8T00898.htm

ウイルス対策ソフトの機能

出所：http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/kiso/k04.htm

ウイルスを駆除するためには

- ただし、ウイルス対策ソフトは、今までのウイルスに対応するウイルス検知用データからウイルスを見つけ出す仕組みになっているため、新しいウイルスは検知できないことがあります。そのため、ウイルス検知用データはいつでも最新のものに更新しておかなければなりません。最新のウイルス検知用データはインターネットやCD-ROMなどで配布されているので、ウイルス対策ソフトのマニュアルやヘルプ、メーカーのホームページなどで確認してみましょう。（ワクチン対策ソフトの更新は期限が切れる前に必ず行いましょう。）

出所：http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/kiso/k04.htm

注意

- 最近、無料のウイルス対策ソフトのように見せかけて、ウイルスをインストールさせる手口による被害が増えているため、注意してください。その代表的な手口は、ホームページなどで「あなたのコンピュータはウイルスに感染しています」のようなメッセージを表示し、偽のウイルス対策ソフトのダウンロード用Webサイトに誘導して、ウイルスをインストールさせる方法です。
- ホームページを見ているだけでウイルス対策ソフトのインストールを促された場合には、不用意にリンク先のホームページに接続したり、ソフトウェアをダウンロード/インストールしたりしないようにしてください。

出所：http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/kiso/k04.htm

クラウドコンピューティングって？

- クラウドコンピューティング（英：cloud computing）とは、ネットワーク、特にインターネットをベースとしたコンピュータの利用形態である。ユーザーはコンピュータ処理をネットワーク経由で、サービスとして利用する。
- 従来のコンピュータ利用は、ユーザー（企業、個人など）がコンピュータのハードウェア、ソフトウェア、データなどを、自分自身で保有・管理していたのに対し、クラウドコンピューティングでは「ユー ザーはインターネットの向こう側からサービスを受け、サービス利用料金を払う」形になる。
- ユーザーが用意すべきものは最低限の接続環境（パーソナルコンピュータや携帯情報端末などのクライアント、その上で動くブラウザ、インターネット接続環境など）のみであり、加えてクラウドサービス利用料金を支払う。実際に処理が実行されるコンピュータおよびコンピュータ間のネットワークは、サービスを提供する企業側に設置されており、それらのコンピュータ本体およびネットワークの購入・管 理運営費用や蓄積されるデータの管理の手間は軽減される。
- クラウドコンピューティングの階層（SaaSはApplicationを、PaaSはPlatformを、IaaSは Infrastructureを提供する）
- クラウドコンピューティングは、この3種類に分類される場合が多い。

クラウドのイメージ図

SaaSはApplicationを、
PaaSはPlatform を、
IaaSは Infrastructureを
提供する