IPA
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

プレスリリース
2005 年 2 月 3 日
独立行政法人 情報処理推進機構

コンピュータウイルス・不正アクセスの届出状況について［要旨］

W32/Bagle ウイルスの新たな亜種が出現

●独立行政法人 情報処理推進機構（略称：IPA 理事長：藤原 武平太）は、2005 年 1 月のコンピュータウイルス・不正アクセスの届出状況をまとめました。

1．コンピュータウイルス届出状況 －詳細は別紙 1 を参照－

1 月の届出件数(*1)は、**4,880 件**となり、12 月の 4,905 件から同水準での推移となりました。なお、ウイルスの検出数(*2)は、**約 334 万**と、12 月の約 260 万個から 28.5%の増加となりました。

*1 届出件数： 同じ届出者から寄せられた届出の内、同一発見日で同一種類のウイルスの検出が複数ある場合は、1 日何通(個)でも届出 1 件としてカウントしたもの。
*2 検出数 ： 届出にあたり届出者から寄せられたウイルスの発見件数（通数）
・ 1 月は、寄せられたウイルス検出数約 334 万個を集約した結果、4,880 件の届出件数となっています。

W32/Netsky は **1,179 件**となり、11 ヶ月連続で千件を超える届出が寄せられました。続いて、W32/Mydoom 348 件、W32/Bagle 334 件となりました。

（1）W32/Bagle ウイルスの新たな亜種が出現

1 月 28 日に新たに出現した **W32/Bagle ウイルスの亜種**は、ウイルス対策ソフトの定義ファイルが提供される前に国内で拡散したため、検出できずに被害に遭うケースが見受けられました。

このウイルスは、メールの添付ファイルを開くことにより感染するウイルスです。下記の件名・本文の組み合わせのメールを受信された場合は、決して添付ファイルを開くことなく、そのまま削除してください。

件名： Delivery service mail、 Delivery by mail、 Registration is accepted、
Is delivered mail、 You are made active
本文： Thanks for use of our software、 Before use read the help

このウイルスに感染すると、アドレス帳などのファイルからアドレスを収集し、取得できたアドレス宛にウイルスメールを送信します。また、感染したパソコンに、**外部から侵入するためのバックドア（裏口）を作成**します。

さらに、ファイル共有ソフトを利用して感染を拡大する活動やセキュリティ対策製品（ウイルス対策ソフトやパーソナルファイアウォール等）の機能を停止させようとします。

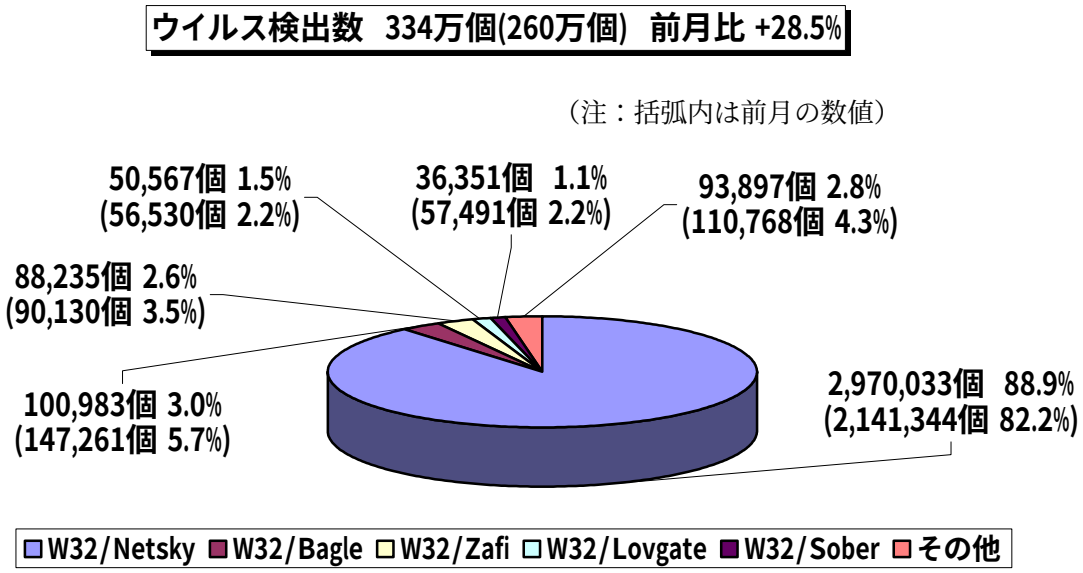
感染してしまった場合は、ウイルス対策ソフトで検査・削除できない可能性がありますので、専用の駆除ツールを利用して対処することが必要になります。

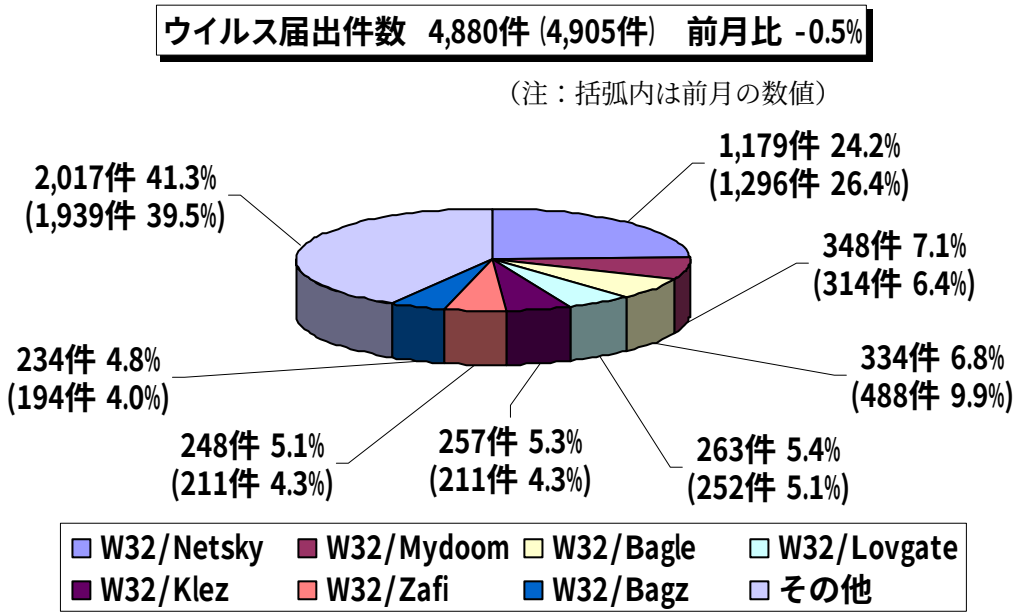
シマンテック （W32.Beagle@mm 駆除ツール）
http://www.symantec.com/region/jp/avcenter/venc/data/jp-w32.beagle@mm.removal.tool.html
トレンドマイクロ （ダメージクリーンナップサービス）
http://www.trendmicro.co.jp/esolution/solutionDetail.asp?solutionId=4700
マカフィー （AVERT ウイルス駆除ツール）
http://www.mcafeesecurity.com/japan/security/stinger.asp

（2）W32/Netsky の検出数が増加！

W32/Netsky の検出数が**約 297 万個**と、12 月の約 214 万個から増加しました。全体の検出数の内、約 89%を占める状況になっており、依然として注意が必要です。

また、全体のウイルス検出数も 2004 年 11 月、291 万個、12 月、260 万個と減少傾向にありましたが、1 月は 334 万個と、再び 300 万以上となりました。1 月には W32/Bagle ウイルスの亜種なども出現していますので、不審なメールの取り扱いには十分注意するようにしてください。





2．コンピュータ不正アクセス届出状況　－詳細は別紙 2,3 を参照－

1 月の届出件数は 31 件と 2004 年 12 月の 55 件と比較して 44%の減少となりました。しかし、**被害届出件数は 9 件**と 12 月の 4 件より増加しました。

被害届出の内訳は、侵入 4 件、メール不正中継 2 件、DoS（サービス妨害）1 件、その他（非正規ユーザの正規ユーザ ID 使用によるなりすまし）2 件でした。

特筆されるべきものとして、Web サーバーが乗っ取られ、フィッシングに悪用されたという被害事例がありました。

被害事例

- Web サーバーに侵入され、フィッシングに悪用することを目的としたコンテンツを設置された。
- オークションサイトの ID とパスワードを成りすましてログインされ、勝手にメールを送られたり、ID を削除されたりした。
- サービスプロバイダを利用した個人開設のホームページに成りすましてログインされ、コンテンツや画像を改ざんされたり削除されたりした。
- SSH（Secure Shell）の IDとパスワードに対する辞書攻撃により侵入され、不正なプログラムを埋め込まれ、外部サイトへの攻撃の踏み台に悪用された。

フィッシングへの悪用に注意！！

銀行等の企業からのメールを装い、メールの受信者に偽のホームページにアクセスするよう仕向け、そのページにおいて個人の金融情報（クレジットカード番号、ID、パスワード等）を入力させるなどして個人情報を不正に入手するような行為である**「フィッシング」に日本国内のウェブサイトが悪用されるようなケースが発見されています。**

侵入されWeb改ざんが行われるケースだけではなく、**ウェブアプリケーションなどの脆弱性により本物サイト上に偽情報が表示される可能性**もあり、フィッシングに悪用されるケースが今後も増大する可能性があります。

ウェブサイト運営者は、自己が管理するウェブサイトがこのような犯罪に加担することが無いようセキュリティホールの解消などの不正アクセス対策を徹底するようにして下さい。

（ご参考）
「ソフトウエア等の脆弱性関連情報に関する届出状況[2004 年第 4 四半期（10 月～12 月）]
http://www.ipa.go.jp/security/vuln/report/vuln2004q4.html

ID･パスワードの適切な設定と管理を！

ID やパスワードの設定不備や管理不備によるものと推測される被害届出や相談が寄せられています。

不適切なパスワードとしては、ID と同じ、名前･電話番号･誕生日などの自分や家族の情報、辞書に載っている単語の利用、単純な数字や文字の並び、長さが不十分、固有名詞、過去に使用したパスワードの再利用等が挙げられます。

推測されにくいパスワードにするには、大文字･小文字･数字･記号の組み合わせ、長いパスワード、推測しづらく自分が忘れないパスワードなどに設定することが必要です。

更に、**パスワードを適切に管理する**には、絶対に人に教えない、定期的に変更する、紙に書き留めない、コンピュータ内に保存しないという対策が必要です。

また、システム管理者としては、パスワードの有効期限を設定する、ワンタイムパスワードを導入する、通信経路を暗号化する、エンドユーザに ID 作成時に付与したパスワードを変更させるなどの対策を行うよう心がけてください。

（ご参考）
「たかがパスワード、されどパスワード」（一般ユーザ向け）
http://www.ipa.go.jp/security/crack_report/20020606/0205.html
「パスワードの管理と注意」（システム管理者向け）
http://www.ipa.go.jp/security/fy14/contents/soho/html/chap1/pass.html

3．今月の呼びかけ：「こんな操作は危険がいっぱい」
―― 被害のきっかけは人にあり ――

ウイルスに感染したり、ブラウザ（Internet Explorer 等）の設定を改変されたりといった被害に遭うケースでは、以下のような操作が要因となります。

- 件名や本文が英語のメールの添付ファイルを開く、本文のリンクをクリックした。
- 見知らぬホームページでリンクをクリックした。
- 提供元が不明な無料ソフトをダウンロードした。
- ファイル共有ソフトを利用して様々なファイルをダウンロードした。

普段、何気なくやっていることが原因で被害に遭う可能性があります。逆に、これらの操作に注意を払っていれば、簡単に被害に遭うことはありません。インターネットを利用する上で、これらの操作には危険が潜んでいることを忘れないようにしてください。

なお、最低限実施しておかなければならない点は、**利用するソフトウェア(OS、ブラウザ、メールソフト等)を最新版に更新し、欠陥(セキュリティホール)がない状態に保つ**ことです。なぜなら、欠陥がある状態では、いくら気をつけていても、自動的に不正なプログラムが実行されてしまうことがあるからです。

下記の情報を参考に、欠陥がない状態に、定期的に更新することをお勧めします。

「Windows Update 利用の手順」（マイクロソフト社）
http://www.microsoft.com/japan/security/square/guard/a04g11.asp
「ソフトウェアアップデート」（アップルコンピュータ）
http://www.apple.co.jp/ftp-info/
「日本の Linux 情報」
http://www.linux.or.jp/

■お問い合わせ先
独立行政法人 情報処理推進機構 セキュリティセンター
花村／加藤／内山
Tel:03-5978-7527 Fax:03-5978-7518 E-mail:isec-info@ipa.go.jp