IPA
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

プレスリリース
2005 年 3 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/Netsky 出現から 1 年の軌跡を振り返る

●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 2 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－

2 月の届出件数(*1)は、**4,150 件**となり、1 月の 4,880 件から 15.0%の減少となりました。また、ウイルスの検出数(*2)は、**約 246 万**と、1 月の約 334 万個から 26.3%の減少となりました。

*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）
・ 2 月は、寄せられたウイルス検出数約 246 万個を集約した結果、4,150 件の届出件数となっています。

W32/Netsky は **1,064 件**となり、12 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/Bagle 458 件、W32/Mydoom 333 件となりました。

（1）W32/Netsky が出現して 1 年間の動向

2004 年 2 月 19 日に初めて届出が寄せられた **W32/Netsky ウイルス**は、2004 年 3 月以降、1 年にわたり届出件数の Top となっています（図 1 参照）。

W32/Netsky は、次々に亜種（Netsky.D, Netsky.P, Netsky.Q 等）が出現し、非常に多くのウイルスメールを撒き散らしている状況が、IPA の検知システムで観測されています（図 2 参照）。

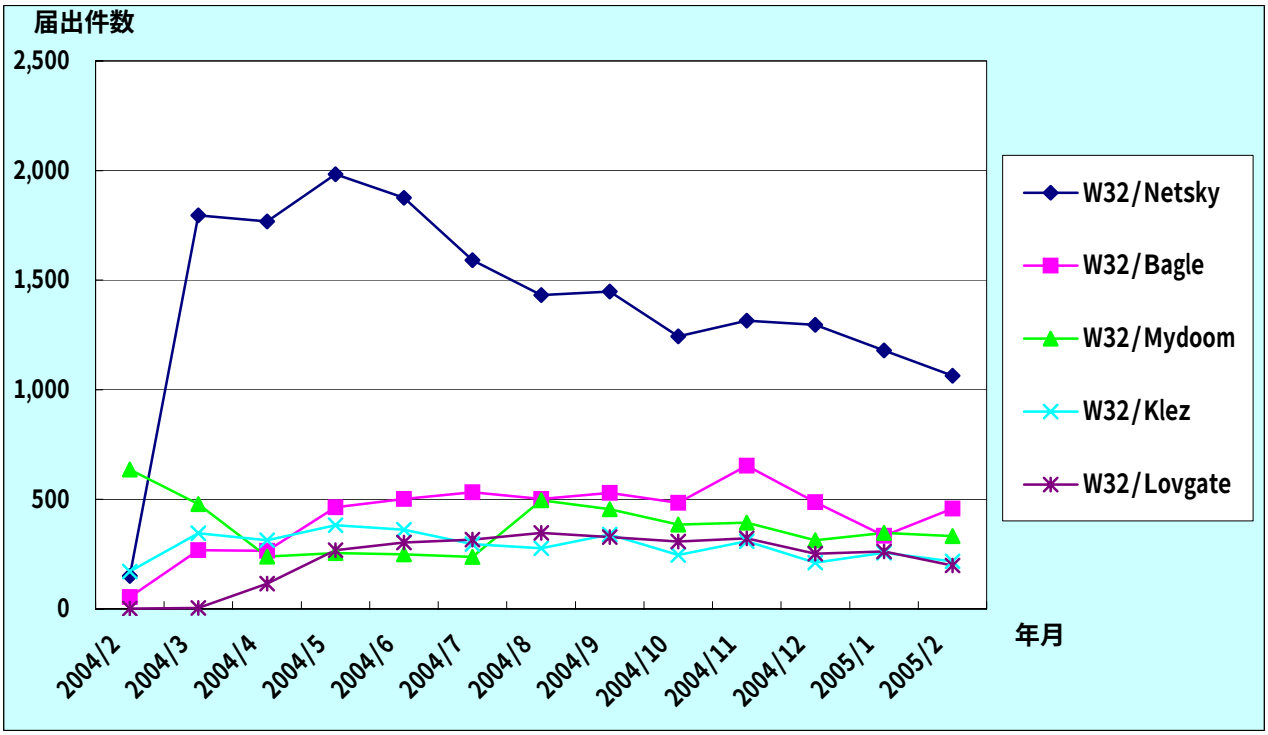


図 1： IPA へのウイルス届出件数 Top5

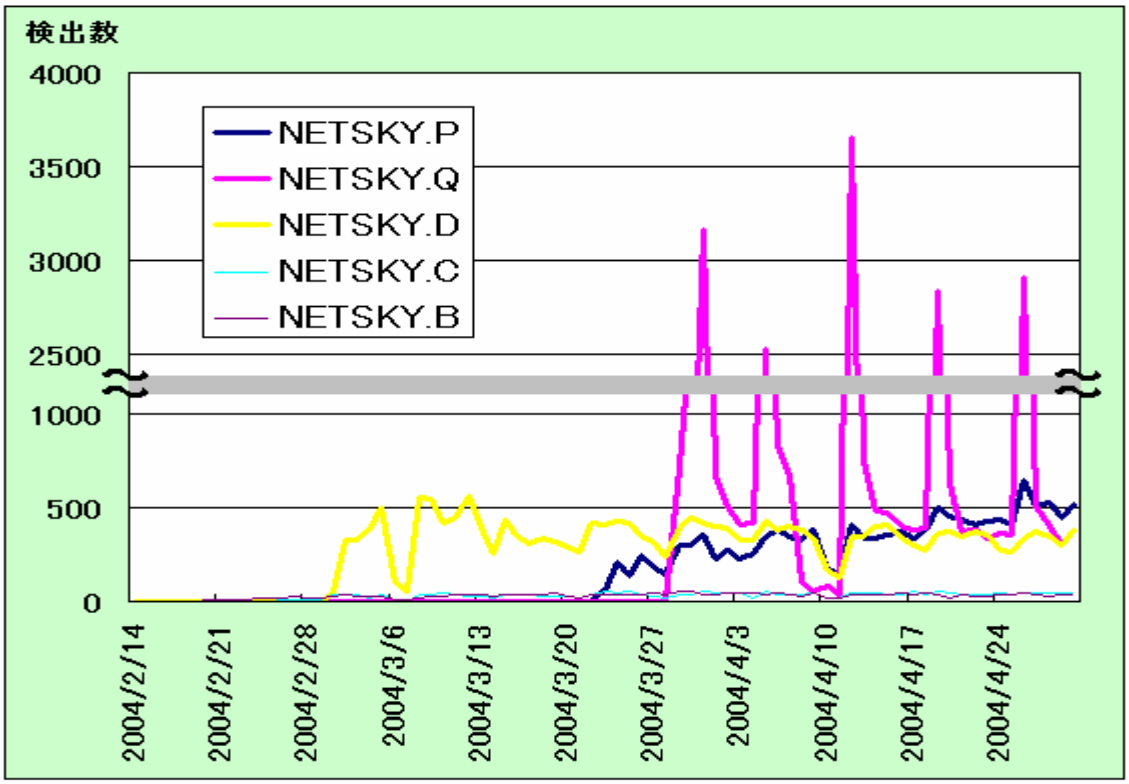


図 2： IPA における W32/Netsky 出現時の検知状況

何故 W32/Netsky ウイルスは蔓延しているのか…

W32/Netsky ウイルスが 1 年間も高い水準で感染活動をつづけている要因は、以下の特徴があるためと推測されます。

W32/Netsky ウイルスの特徴

- 感染したコンピュータ上で、見た目にわかる症状がでない
  → 感染していることに気付かない
- 受信したメールの件名に自分自身のメールアドレスが表示される
  → 自分が送信したメールのエラーと勘違いして添付ファイルを開いてしまう
  例：MAIL DELIVERY ERROR （virus-test@ipa.go.jp）
- 不特定多数への大量メール送信型ウイルスである （マスメール型ウイルス）
  → 感染すると大量にウイルスメールが送信され、感染が拡大する

W32/Netsky ウイルスを終息させるために…

上記の特徴にもあるように、感染しても見た目にわかる症状が表れないため、感染したことに気付かずにウイルスメールを撒き散らしている状況が推測されます。よって、全てのパソコンユーザがワクチンソフト、もしくは駆除ツールで検査を行うことが重要です。

自分は大丈夫と思っている貴方も、念のため検査することをお勧めします。また、知り合いの方にもこの状況をお知らせしてください。

駆除ツールを利用した検査方法（無償）：

（Netsky ウイルスの感染の有無の検査と、感染していた場合の駆除が可能）

・トレンドマイクロ：
http://www.trendmicro.co.jp/esolution/solutionDetail.asp?solutionId=4700

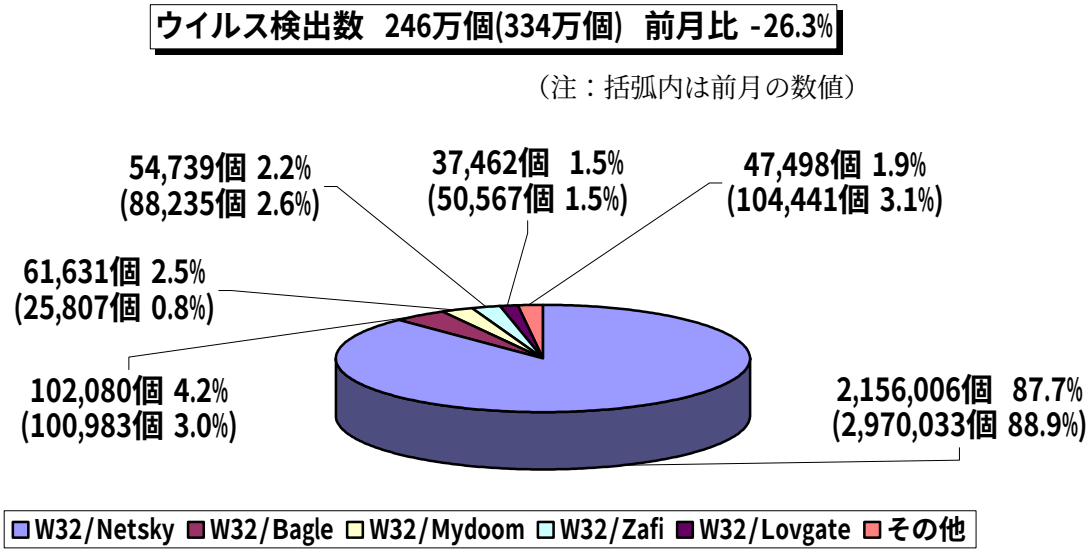
・マカフィー：
http://www.mcafeesecurity.com/japan/security/stinger.asp
・シマンテック：
http://www.symantec.com/region/jp/sarcj/data/w/w32.netsky@mm.removal.tool.html
・マイクロソフト：
http://support.microsoft.com/?kbid=890830

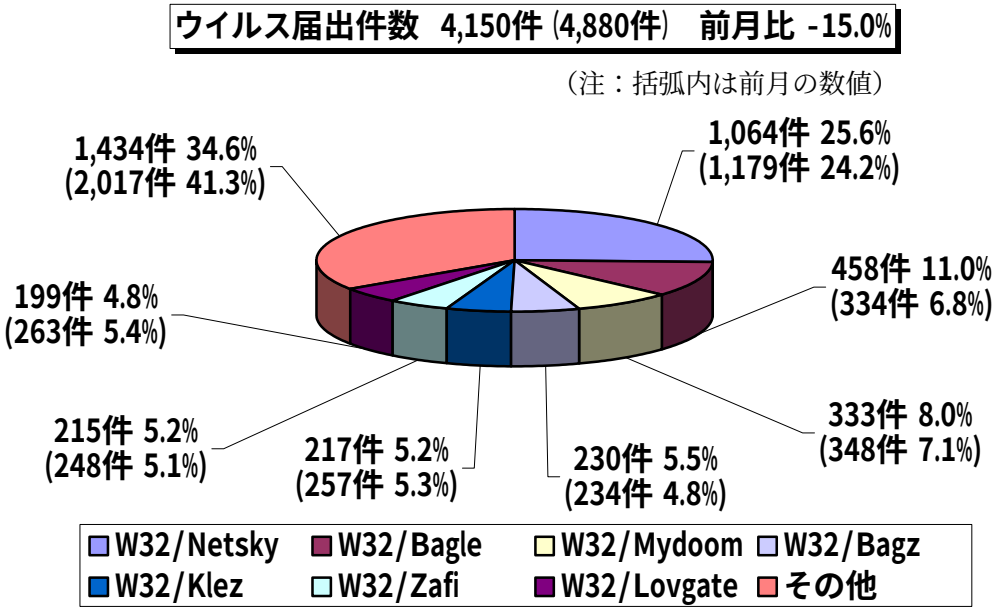
また、W32/Netsky の亜種には、Windows のセキュリティホールを悪用するタイプもありますので、Windows Update のサイトから修正プログラムを適用し、予防策を実施してください。

・マイクロソフト： http://windowsupdate.microsoft.com

（2）W32/Netsky が総検出数の約 9 割を占める

W32/Netsky の検出数が**約 216 万個**と、1 月の約 297 万個から 27.3%減少しました。しかし、全体の検出数に占める割合は、依然として約 9 割となっており、圧倒的に蔓延している状況が継続しています。





2．コンピュータ不正アクセス届出状況　－詳細は別紙 2 を参照－

2 月の届出件数は 63 件となり、1 月の 31 件と比較して約 2 倍となりました。しかし、**被害届出件数は 9 件**で 1 月（9 件）と同水準でした。

被害届出の内訳は、侵入 5 件、その他 4 件（非正規ユーザの正規ユーザ ID 使用によるなりすまし 3 件、不正プログラムの強制ダウンロード 1 件）でした。

侵入 5 件のうち、**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 1 月に引き続き 2 月もありました。

被害事例

- Web サーバーソフトウェア Apache の脆弱性を突かれて侵入され、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で本人に成りすましてログインされ、見知らぬメールアドレスが連絡先として書き換えられ、勝手に出品や落札をされた。
- インターネットのオンラインゲームに不正にログインされ、ゲーム上のお金やアイテムを盗まれた。
- 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、管理者権限パスワードの変更やファイルの改ざんが行われ、踏み台として外部への攻撃が実行された。
- 遠隔から作業が出来るように一時的に設定を変更したが、設定を戻さずに運用したため侵入され、Web サーバーのトップページを改ざんされた。

加害者や犯罪の加担者にならないために

コンピュータに侵入されると、ファイルの削除や改ざんなどの被害に遭うだけではなく、他のコンピュータを攻撃する踏み台とされたり、フィッシングや違法ファイルの交換などに悪用されるなど、加害者となったり、サイバー犯罪に加担することになりかねません。このような被害は一般の家庭ユーザの PC でも例外ではありません。

個人ユーザが行うべき対策として、

⑴　ワクチンソフトやパーソナルファイアウォールを導入する

⑵　推測されにくいパスワードを設定する、他人にパスワードを教えない

⑶　怪しいサイトを閲覧しない、信頼できないサイトから安易にファイルをダウンロードしない

などの対策を行うことが必要です。

また、**システム管理者が行うべき対策**として、

(1)　適切なパスワード設定と管理を行う

(2)　脆弱性を解消する（OS だけではなく、Web アプリケーションなども忘れずに）

(3)　アクセス制限やセキュリティ設定を適切に行う（不要なサービスも停止する）

などの対策を行うことが必要です。

なお、先月も記述いたしましたが、パスワードについては、以下の点に注意して適切な設定と管理を行うようにして下さい。

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、英語の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)
「情報セキュリティ対策実践情報　エンドユーザ･ホームユーザ向けのページ」
http://www.ipa.go.jp/security/awareness/end-users/end-users.html
「情報セキュリティ対策実践情報　システム管理者向けのページ」
http://www.ipa.go.jp/security/awareness/administrator/administrator.html

3．インターネット定点観測での 2 月のアクセス状況

－詳細は別紙 3 を参照－

2 月の期待しない(一方的な)アクセスは、**10 個の観測点**の合計で **575,582 件**ありました。

アクセス総数は 1 月に比べて大幅に減少していますが、**1 日あたりの 1 つの観測点(一般のインターネット利用者個人と同様な環境)で約 2,370 件のアクセスがあった計算になります。**

2 月も 1 月と同様に、ボット系と呼ばれるワーム(トロイの木馬)が猛威を振るっており、ほとんどのポートに対するアクセスは、このボット系のアクセスと推測されます。

4．今月の呼びかけ：「 今すぐウイルスチェックの実施を！ 」
―― あなたのパソコンは大丈夫ですか ――

W32/Netsky に見られるように、最近のウイルスは、感染しても見た目にわかる症状がでるものはほとんどなく、気付かずにウイルスメールを発信しているケースが多数存在していると推測されます。

ウイルスに感染しているかどうかを確認するためには、ウイルス対策ソフトで検査することが必要です。思い当たることがなくとも、いつの間にかウイルスに感染していることもあるので、今一度チェックすることをお勧めします。

すぐに最新のウイルス対策ソフトを用意できない場合は、以下のサービスを利用することでも検査することができます。

無償で利用できるウイルスチェックサービス ： ウイルス感染の有無をチェック可能

(1) トレンドマイクロ ウイルスバスターオンラインスキャン
http://www.trendmicro.co.jp/hcall/scan.htm
(2) シマンテック Security Check
http://www.symantec.com/region/jp/securitycheck/index.html
(3) マカフィー・フリースキャン
http://www.mcafeesecurity.com/japan/mcafee/home/freescan.asp

検査した結果、ウイルスを検出した場合は、ウイルスにより対処方法が異なりますので、各社のウイルス情報を確認してください。駆除する方法としては、専用の駆除ツールが提供されている場合は、ツールを利用してください。また、ウイルス対策ソフトを導入することでも対処でき、予防対策にも活用することができます。

ウイルスの駆除方法が不明な場合は、IPA セキュリティセンターで相談を受け付けていますので、下記窓口までご相談ください。
なお、2004 年 12 月より、自動音声応答にて一次受付をしておりますが、オペレータ（相談員）への電話転送も可能となっています。また、オペレータの対応時間外については、連絡先を録音していただければ、こちらからご連絡いたします。

IPA セキュリティセンター 相談窓口
E-mail: virus@ipa.go.jp TEL: 03-5978-7509
（オペレータ対応時間 平日 10:00～12:00、13:30～17:00）

■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