

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〕

2003年 ネットワークウイルス猛威を振るう！！

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、2003年の年間および12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

1-1. 2003年 年間届出状況 - W32/MSBlaster が猛威を振るう -

2003年の届出件数は17,425件となり、2002年20,352件から約15%の減少となりました。

届出件数は減少しましたが、1月にW32/SQLSlammer、8月にW32/MSBlaster、W32/Welchiaの出現など、インターネットに接続しているだけで感染するネットワーク型のウイルスが出現して、猛威を振りました。

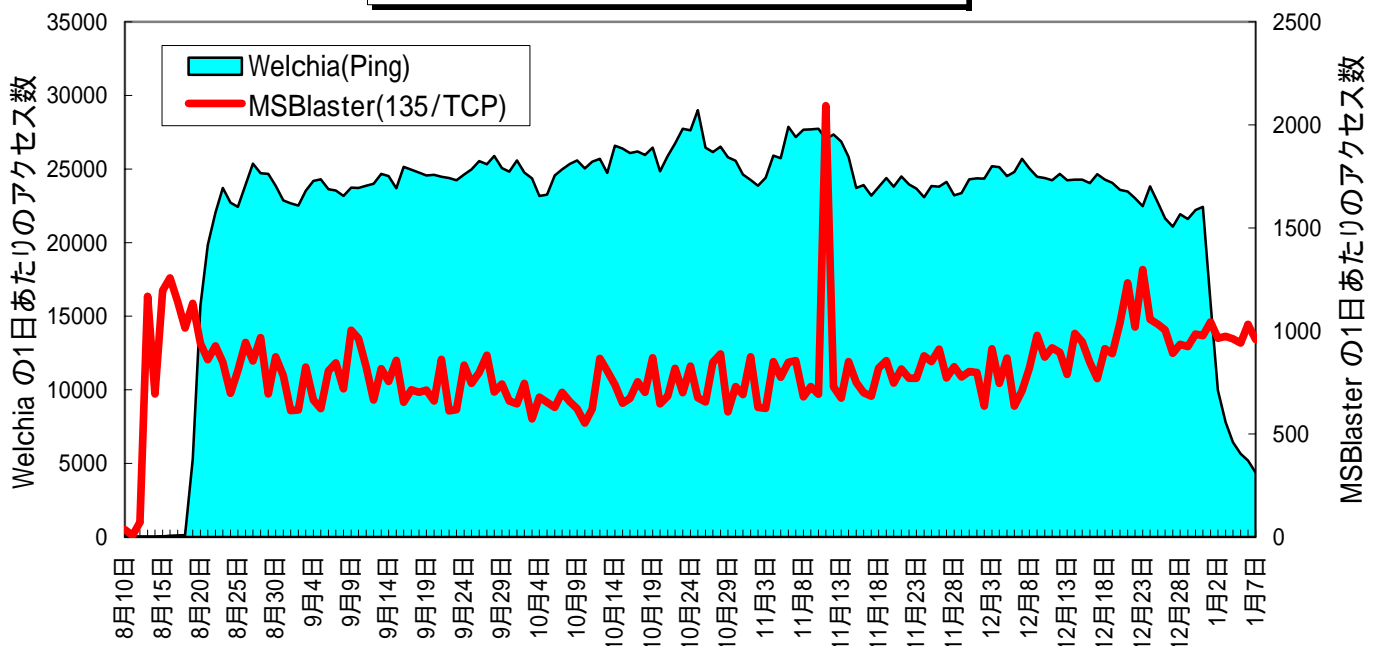
W32/MSBlasterについては、未だにその攻撃は続いている状況です。感染していることに気付かずに感染を拡大している可能性もありますので、Windows パソコンをお使いの方は、以下のサイトで紹介している無償の駆除ツールを利用して検査することをお勧めいたします。

「W32/MSBlaster」ワームに関する情報

<http://www.ipa.go.jp/security/topics/newvirus/msblaster.html>

一方、2004年に活動を停止するW32/Welchiaについては、1月1日以降、その攻撃は減少しています。このウイルスに感染することはなくなりましたが、セキュリティホールは解消など、引き続き対策を実施してください。

MSBlaster/Welchiaのアクセス数変化



1-2. 12月届出状況

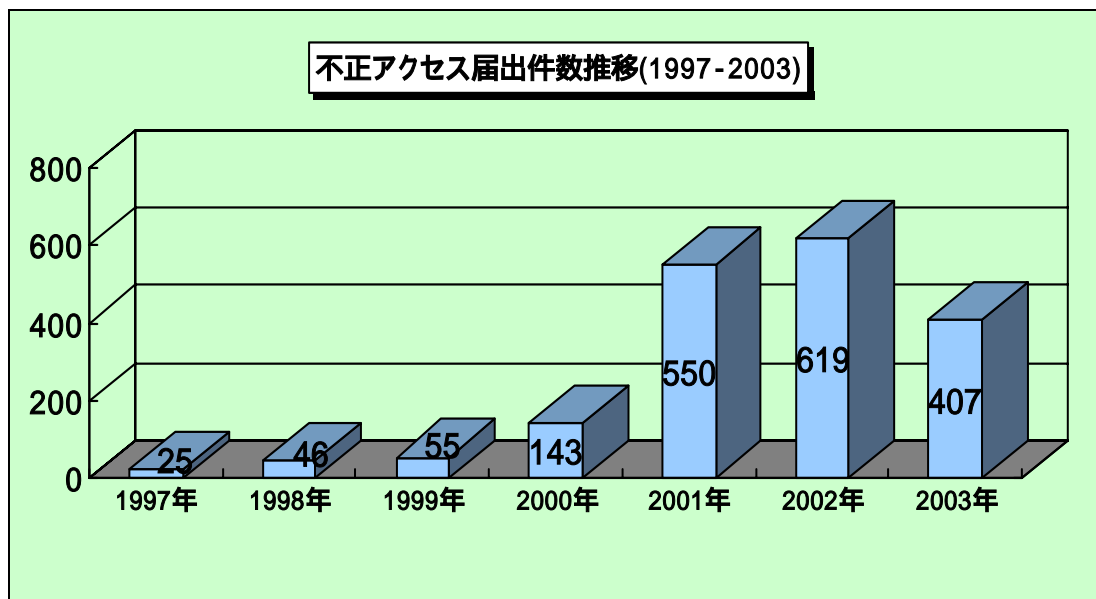
12月の届出件数は、1,452件と11月の1,786件から約2割の減少となりました。

ウイルス別の届出件数の上位は、W32/Swen 352件と3ヶ月連続でワースト1になりました。続いて、W32/Klez 290件、W32/Mimail 210件の届出が寄せられました。

2. コンピュータ不正アクセス届出状況

2-1. 2003 年年間届出状況

2003 年の 1 年間の届出件数は 407 件で、2002 年の届出件数(619 件)と比べて約 34%減少しました。



IPA に届けられた 407 件の届出種別は以下の通りです。

届出種別	2003 年	2002 年
侵入	64(64)	106(106)
アクセス形跡(未遂)	239	356
ワーム感染	5(5)	6(6)
ワーム形跡	39	34
アドレス詐称	18(18)	49(49)
spam	5(5)	3(3)
メール不正中継	9(9)	16(16)
DoS(サービス妨害)	8(8)	16(16)
その他	20(17)	33(29)
合計	407(126)	619(225)

*括弧内は実被害件数

詳細は別紙 2「2003 年不正アクセス届出状況」を参照

2003 年は 2002 年と比べて、ほとんどの届出種別項目で届出件数が減少しましたが、2003 年 8 月に発生した W32/MSBlaster や W32/Welchia によるアクセスと思われるワーム形跡の届出が若干増加しました。また、spam メールに係る不正アクセス届出件数も若干増加しました。

被害届出件数が減少した理由として、別紙 2 に示しますように、被害原因の内訳において「古いバージョン・パッチ未導入」が原因となった被害件数が減少したことが挙げられます。

一方、設定不備や ID・パスワード管理不備による被害原因の割合が増加しています。したがって、セキュリティホールへの対策は浸透しつつあるものの、設定や ID・パスワード管理への対策が不十分であると推測されます。

2 - 2 . 12 月届出状況

2003年12月度の届出件数は**29件**と、11月(23件)よりも若干増加しました。また、被害届出件数が**11件**を占めました。その内訳は、侵入5件、メール不正中継1件、メールアドレス詐称2件、spamメール被害1件、その他(ブラウザクラッシャ、ID不正利用)2件でした。

被害届出の中で、特筆すべきものを以下に示します。

- ・ 退職社員の行ったルーターの設定を放置し、更に当該社員のIDを失効させていなかったために社内LANに不正にアクセスされた
- ・ ファイアウォールの設定不備が原因で侵入されたサーバーを悪用され、銀行のIDとパスワードを盗むためのspamメールのリンク先URLとして指定されていた
- ・ 家庭ユーザーのPCで、ファイルやフォルダに共有設定をして、誰でもアクセスできるようにしていたため、インターネット経由で侵入された

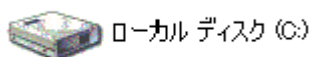
最近の届出内容として、**設定の不備が原因である被害**が目立ってきています。システム管理者は、**ルーターやファイアウォールなどの設定やアクセス制御設定**が適切に行われているか、また、一般ユーザーは、**ID・パスワードの設定や共有設定、無線LANのセキュリティ設定**がなされているかを確認してください。

Windows のディスク(ファイル)共有の確認方法と設定変更方法

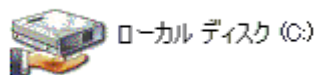
ここではWindowsXPでの画面で紹介합니다。お使いのOSのバージョンによりメニュー構成や表示の様子が異なる場合があります。

確認方法

「マイコンピュータ」か「エクスプローラ」で『手のマーク』が出たら共有を許可している設定になっていることを表しています。下図(b)もしくは下図(c)の状態では、それぞれ、ディスク、フォルダが共有を許可している設定になっていることを表しています。



図(a): 共有なしの状態



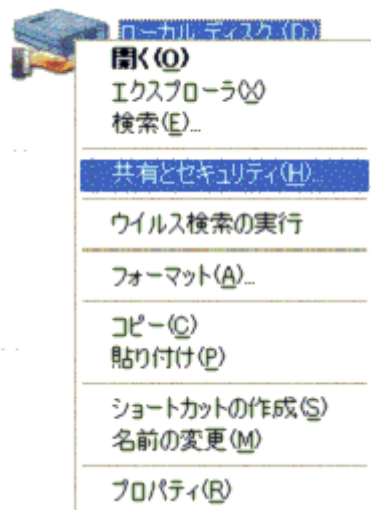
図(b): 共有可能なディスク



図(c): 共有可能なフォルダ

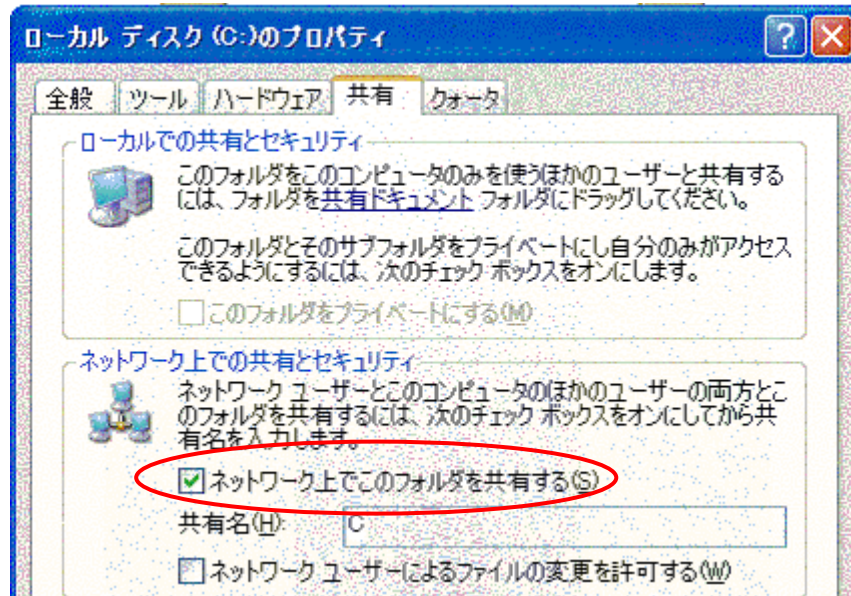
詳細確認と設定変更(解除)

当該ディスクもしくはフォルダの上で右クリックして、「共有とセキュリティ」を選択、もしくは、「プロパティ」を選択します。次に「共有」タブを選択し、実際に共有できる状態になっているかを確認したり、設定をすることができます(図(d))。



図(d): 右クリックしてメニューから選択

次に、「ネットワーク上での共有とセキュリティ」欄の「ネットワーク上でこのフォルダを共有する」のチェックをはずし、個別に共有の設定を解除します(図(e))。



図(e): プロパティで共有をオフ

また、「コントロールパネル」の中の「ネットワークとインターネット接続」アイコンをクリックし、更に「ネットワーク接続」アイコンをクリックします。普段使っているネットワーク接続設定のアイコンを右クリックし、「プロパティ」を選択します。「全般」タブを選択し、「Microsoft ネットワーク用ファイルとプリンタ共有」のチェックをはずすことでパソコン自体の共有ができなくなります(図(f))。



図(f): パソコン自体の共有をオフ

3. 今月の呼びかけ：「年始めから対策を！！」

基本はやっぱり7ヶ条！

2003 年は、従来から蔓延しているメールの添付ファイルにより感染を拡大するタイプに加え、**ネットワーク感染型のウイルスの流行**など、セキュリティホールを悪用するウイルスが猛威を振るいました。2004 年も、セキュリティホールの出現、それを悪用するウイルスの登場が考えられます。

ウイルスによる被害を未然に防止するために、以下の7ヶ条を参考に基本を再確認してください。特に、「**1. ワクチンソフトを活用する**」、「**5. セキュリティパッチをあてる**」の対策を怠ると、容易に感染する可能性が高いです。ワクチンソフトの導入、Windows Update でセキュリティパッチをあてるなど、万全な予防対策を行ってください。

- ウイルス対策7ヶ条 -

1. 最新のウイルス定義ファイルに更新し**ワクチンソフトを活用**すること
2. メール添付ファイルは、開く前にウイルス検査を行うこと
3. ダウンロードしたファイルは、使用する前にウイルス検査を行うこと
4. アプリケーションのセキュリティ機能を活用すること
5. **セキュリティパッチをあてる**こと
6. ウイルス感染の兆候を見逃さないこと
7. ウイルス感染被害からの復旧のためデータのバックアップを行うこと

「ウイルス対策7ヶ条」

<http://www.ipa.go.jp/security/antivirus/7kajonew.html>

「Windows Update」

<http://windowsupdate.microsoft.com/>

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

Tel:03-5978-7508 Fax:03-5978-7518 E-mail:isec-info@ipa.go.jp