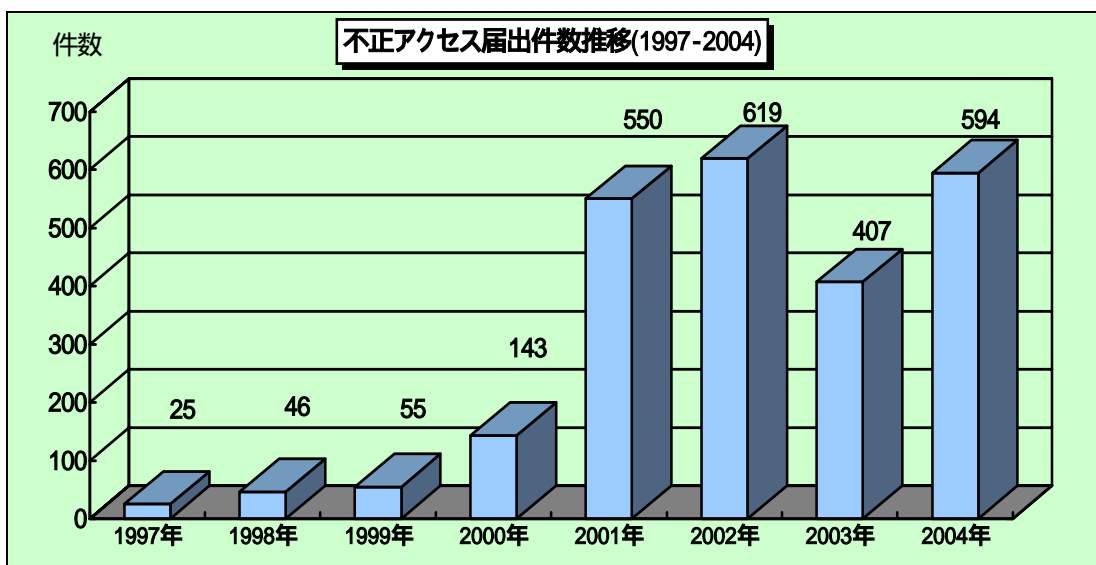


2004年不正アクセス届出状況

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、2004年1月～12月の不正アクセス届出データを集計しました。

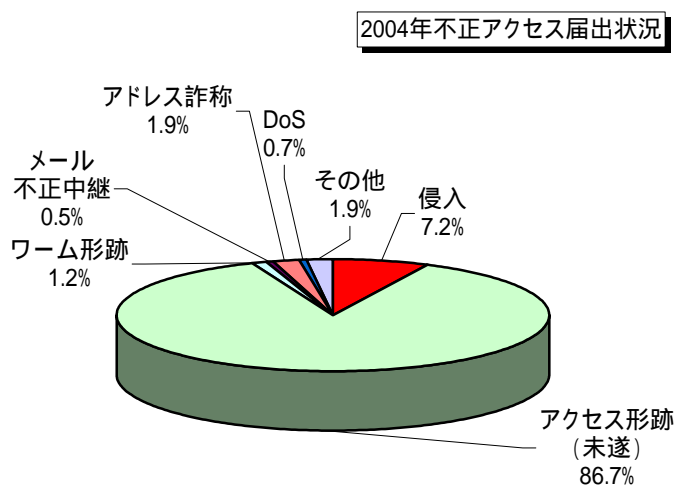
1. 届出件数

2004年の年間届出件数は**594件**となり、2003年の届出件数407件と比べて**45.9%増**と再び増加に転じました。なお、下記グラフは、過去8年間にIPAセキュリティセンターが受け付けた届出件数の推移を示したものです。



2. 届出種別

2004年は2003年と比べて、**アクセス形跡が115.5%増と大幅に増加しましたが、実被害件数は減少しました。企業・個人ユーザ問わず無差別に攻撃を受けている一方で、実被害届出が減少した理由としては、企業を中心にセキュリティ対策が普及していることが推測されます。**



届出種別	2004年	2003年
侵入	43(43)	64(64)
アクセス形跡(未遂)	515	239
ワーム感染	0	5(5)
ワーム形跡	7	39
メール不正中継	3(3)	9(9)
アドレス詐称	11(11)	18(18)
DoS(サービス妨害)	4(4)	8(8)
その他	11(11)	25(22)
合計	594(72)	407(126)

*1)「アクセス形跡(未遂)」はサーバーのログやファイアウォールのログに不正アクセスの痕跡があったもの

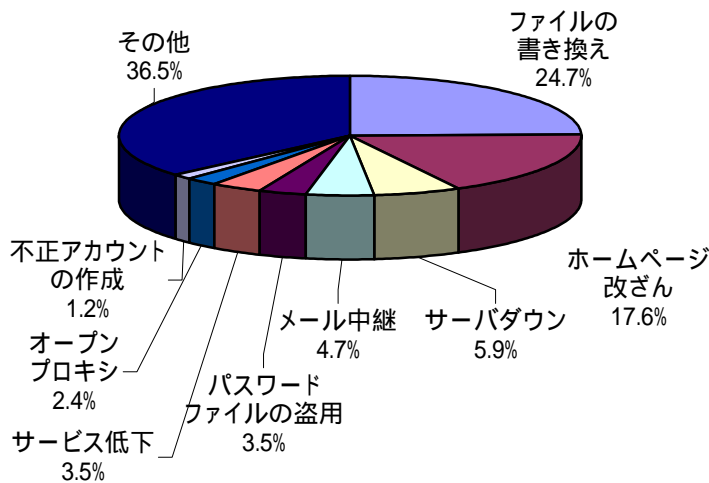
*2)「ワーム形跡」はワームによるアクセスを検知したが、感染の被害を受けなかったもの

括弧内は実被害件数

3. 被害内容

届出のうち実際に被害に及んだケースに関する被害内容の分類です。**ファイルの書き換え（プログラムの埋め込み含む）及びホームページの改ざんによる被害が多く届けられました。**

2004年被害内容



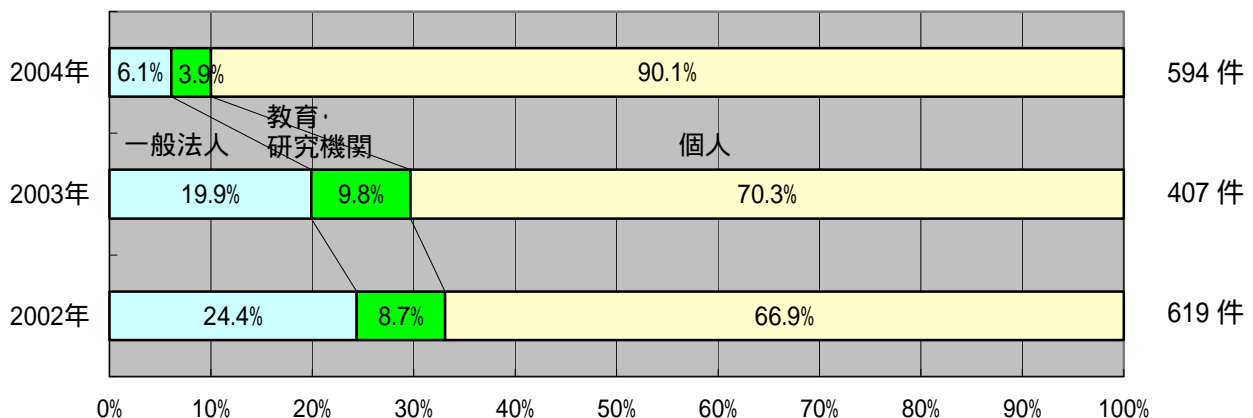
被害内容	2004年	2003年
ファイルの書き換え	21	43
ホームページ改ざん	15	15
サーバダウン	5	4
メール中継	4	9
パスワードファイルの盗用	3	4
サービス低下	3	7
オープンプロキシ	2	1
不正アカウントの作成	1	2
その他	31	61
合計	85()	146

実被害届出1件に複数の被害内容が存在するケースもあるため実被害届出件数合計と一致していません。

4. 届出者の分類

届出者別の内訳は、**個人からの届出の割合が90.1%**となり、2003年の70.3%から更に増加しました。個人ユーザにおけるADSL、FTTHなどの常時接続環境の普及に伴い**企業・個人ユーザを問わず無差別に攻撃対象になっている**ことが推測されます。

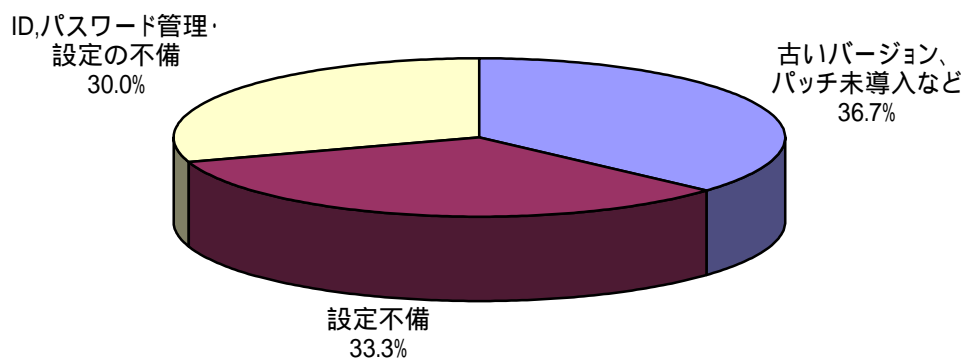
届出者別推移



5. 被害原因

実際に被害にあった届出を原因別分類に見ますと、古いバージョン・パッチ未導入などが11件(36.7%)、設定不備が10件(33.3%)、ID・パスワード管理・設定の不備が9件(30.0%)となっています。**様々なセキュリティ対策の不備が狙われている**ということが推測されます。

2004年被害原因



被害原因が不明もしくは被害原因が無いものは除いています。

6. 対策情報

基本的なセキュリティ対策を実施していなかったために被害に遭うケースが多く見受けられます。

今後の不正アクセス対策として、**システム管理者**は以下の点を確認して総合的に対策を行いまし
よう。

- ・ セキュリティホール^①の解消（パッチ適用不可の場合の回避策も含む）
- ・ ルータやファイアウォールなどの設定やアクセス制御設定
- ・ ID やパスワードの厳重な管理及び設定

また、**個人ユーザ**においても同様に以下の点に注意しましょう。

- ・ Windows Update や Office Update など OS やアプリケーションソフトのアップデート
- ・ PC の共有設定や無線 LAN のセキュリティ設定の確認
- ・ 推測されにくいパスワードの設定と管理（安易に他人に教えないなど）

システム管理者向け

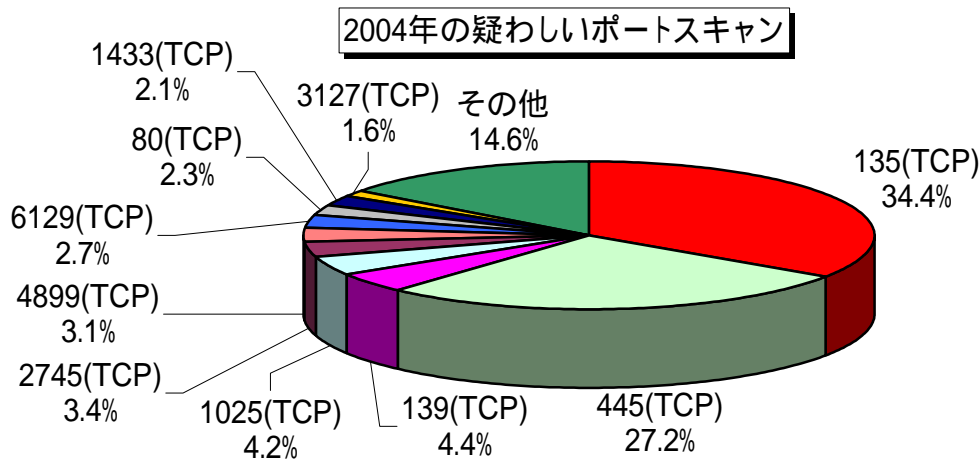
- ・ 「情報セキュリティ対策実践情報 システム管理者向けのページ」
<http://www.ipa.go.jp/security/awareness/administrator/administrator.html>
- ・ 「情報セキュリティ対策実践情報 SOHO(小規模サイト)向けのページ」
<http://www.ipa.go.jp/security/awareness/soho/soho.html>
- ・ 「セキュリティ対策セルフチェックシート」
<http://www.ipa.go.jp/security/ciadr/checksheet.html>
- ・ 「コンピュータ不正アクセス被害防止対策集」
<http://www.ipa.go.jp/security/ciadr/cm01.html>
- ・ 「セキュリティ脆弱性情報」
<http://www.ipa.go.jp/security/news/news.html>

エンドユーザ・ホームユーザ向け

- ・ 「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>
- ・ 「パソコンを守るための3つの手順」(マイクロソフト社)
<http://www.microsoft.com/japan/athome/security/protect/default.asp>

7.2004 年年度のネットワーク観測状況

IPA 独自の観測環境サーバーの各ポートへのアクセス件数を集計したデータです。135 番ポートや 445 番ポートへのアクセスが突出して多いことから、Windows の脆弱性を狙ったワームや不正なプログラムによるアクセスが増加していると推測されます。また、最近では国内からの不正なアクセスが増加しています。



これらのアクセスを行っているコンピュータはウイルスに感染しているか、乗っ取られている可能性があります。

こんな症状は要注意

- ・最近パソコンの起動時間が異様に遅くなったように感じる、あるいはパソコンの動作が遅くなったように感じる
- ・パソコンが勝手にシャットダウンする
- ・メモリ不足などのエラーメッセージが出るようになった
- ・何もしていない時に、ハードディスクの I/O ランプが点滅し続けている
- ・パソコンの画面が乱れる
- ・見たことも無いファイルができていて、あるいはあったはずのファイルが無い
- ・Internet Explorer を起動すると、いつもと違うページ(英語のページ等)が表示される
- ・ポップアップ広告がよく出るようになった
- ・いつも使っているアプリケーションが起動しないか、起動が遅い
- ・デスクトップやタスクバーに知らないアイコンが増えている
- ・知らない間にメールを送信しているようで、メール仲間からウイルスメールが来たと怒られた
- ・最近ウイルスメールやスパムメールがたくさん来るようになった

こんなことをした覚えがありますか？

- ・間違っ、不審なメールの添付ファイルを開いてしまった
- ・怪しげなフリーツールをダウンロードした、あるいは怪しげなリンクをクリックした

以上のような症状が自分のコンピュータで起きている場合は、**早急にウイルス検査を実施して下さい**。ウイルス対策ソフトを利用していない場合は、オンラインでのウイルス検査サービスを利用することにより、感染の有無を確認できます。以下の各ワクチンベンダーのWebサイトで提供されていますので、利用して下さい。

- i) トレンドマイクロ On-Line Scan
<http://www.trendmicro.co.jp/hcall/scan.htm>
- ii) シマンテック Security Check
<http://www.symantec.com/region/jp/securitycheck/index.html>
- iii) マカフィー・フリースキャン
<http://www.mcafeesecurity.com/japan/mcafee/home/freescan.asp>

また、対策として Windows Update を実施して下さい。

Windows Update (マイクロソフト社)
<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

花村 / 加藤 / 内山

Tel:03-5978-7527 Fax:03-5978-7518 E-mail:isec-info@ipa.go.jp