IPA®
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

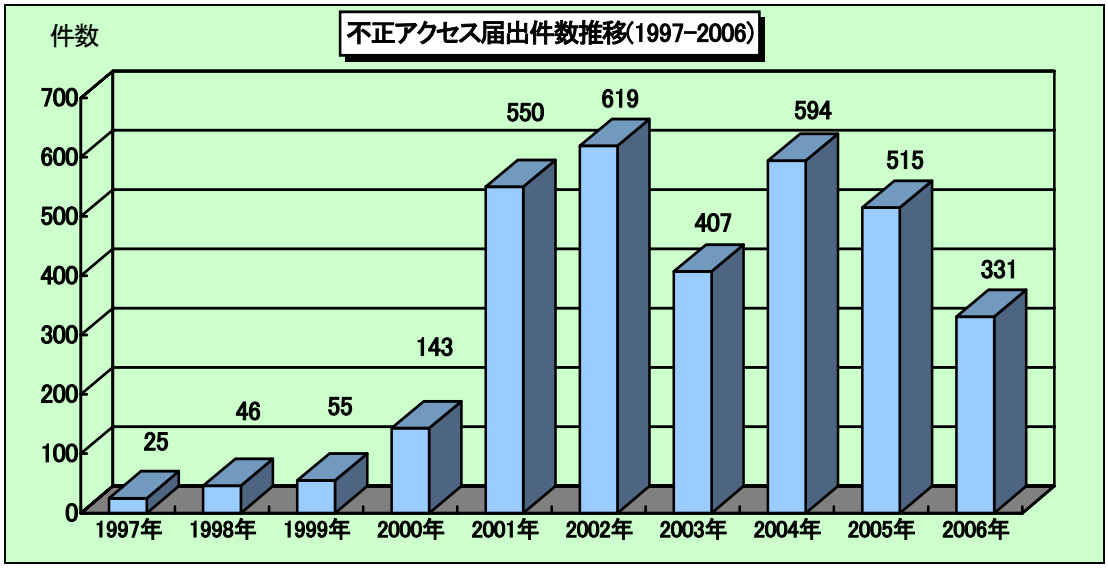
プレスリリース
2007 年 1 月 5 日
独立行政法人 情報処理推進機構

2006 年のコンピュータ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、2006 年 1 月～12 月のコンピュータ不正アクセス届出状況をまとめました。

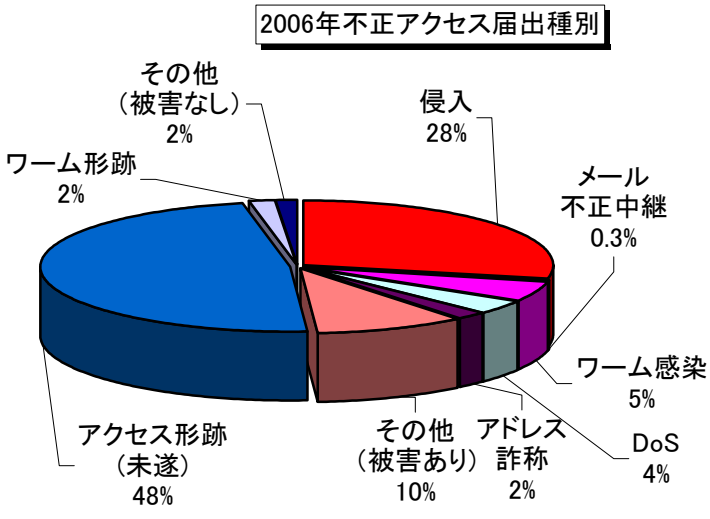
1. 届出件数

2006 年の年間届出件数は **331 件**となり、2005 年の届出件数 515 件と比べて約 **36%減少しました。**なお、下記グラフは、過去 10 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

2006 年は 2005 年と比べて、アクセス形跡の届出数が大幅に減少しました。また全体の届出数は大幅に減少したものの、**被害があった届出件数は微減に留まっています(前年比約 8%減)。**



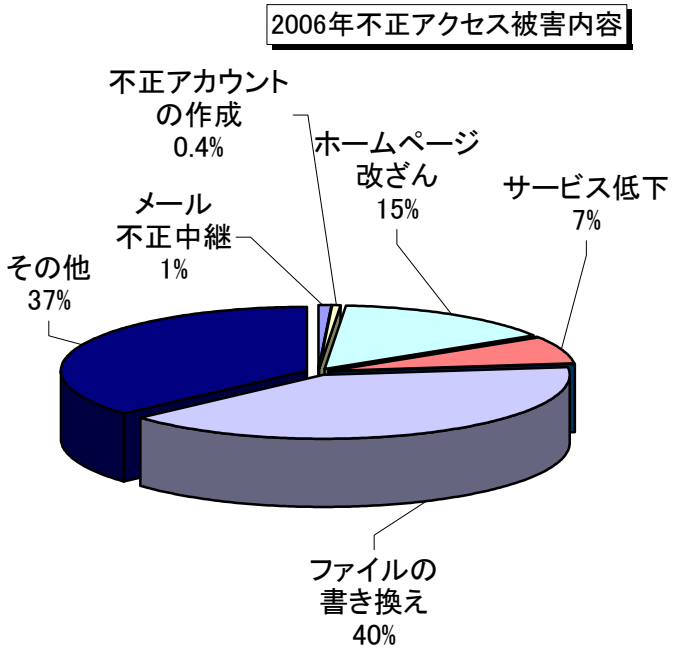
届出種別	2006 年	2005 年
侵入	94	98
メール不正中継	1	8
ワーム感染	16	8
DoS(サービス妨害)	12	21
アドレス詐称	7	6
その他(被害あり)	32	35
アクセス形跡(未遂)	159	325
ワーム形跡	5	7
その他(被害なし)	5	7
合計 (件)	**331(162)**	**515(176)**

※ 網掛け部分とカッコ内の数字は、被害があった届出種別を示しています。

*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試行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

3. 被害内容

届出のうち実際に被害があったケースにおける被害内容の分類です。被害内容件数は前年比約11%の微増でした。**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届出**が多く寄せられました。

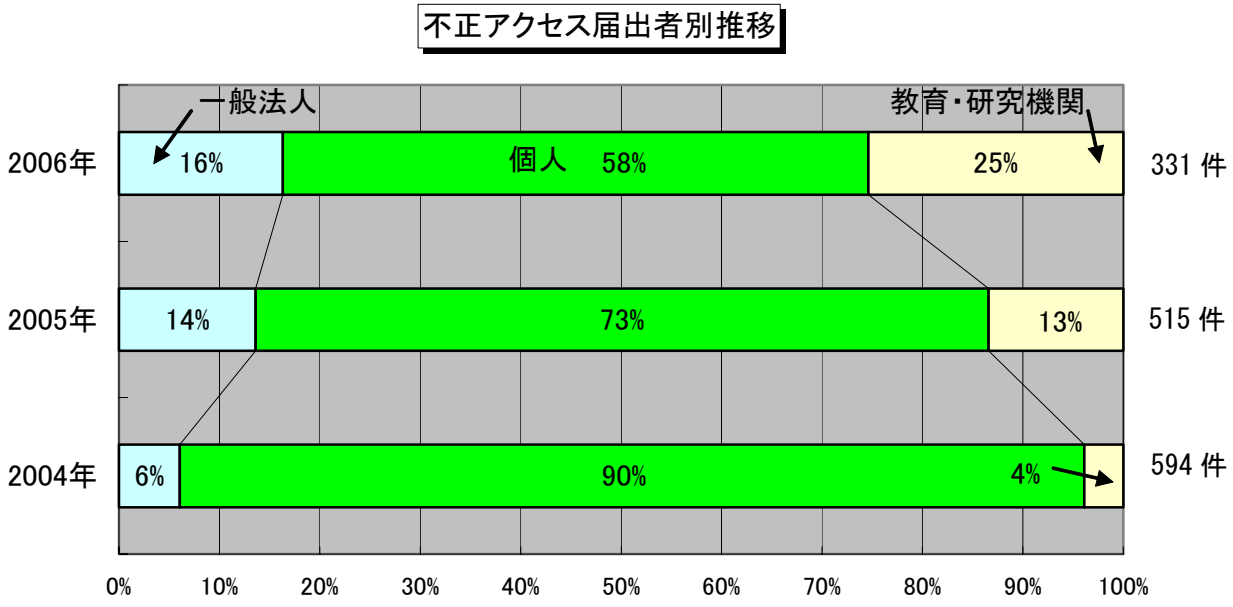


被害内容	2006 年	2005 年
メール不正中継	2	9
サーバーダウン	0	6
不正アカウントの作成	1	4
ホームページ改ざん	34	32
パスワードファイルの盗用	0	1
サービス低下	16	16
オープンプロキシ	0	1
ファイルの書き換え	92	69
その他	84	68
合計　（件）	**229（※）**	**206（※）**

※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。

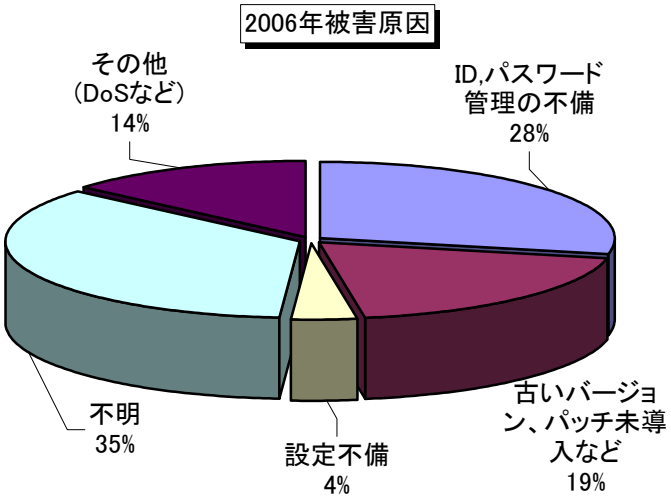
4. 届出者の分類

届出者別の内訳は、**個人からの届出割合が減少しましたが、依然として 58%**と大多数を占めています。相対的に、一般法人と教育・研究機関からの届出割合が増加しており、特に教育・研究機関からの届出数が伸びています。全体の傾向として、相変わらず**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。



5. 被害原因

実際に被害があった届出を原因別分類に見ますと、ID・パスワード管理・設定の不備が 46 件(28%)、古いバージョン使用・パッチ未導入などが 31 件(19%)、設定不備が 6 件(4%)、となっています。原因が不明なケースは 57 件(35%)もあり、**不正アクセスの手口が巧妙化するとともに原因究明が困難な事例が多い**ということが推測されます。



被害原因	2006 年	2005 年
ID, パスワード管理の不備	46	42
古いバージョン使用、パッチ未導入など	31	28
設定不備	6	14
不　明	57	60
その他（DoS など）	22	32
合計　（件）	**162**	**176**

6. 対策情報

2006 年の特徴として、**SSH で使用するポートへの攻撃で侵入された被害（ID、パスワードの設定不備が主な原因）や Web アプリケーションの脆弱性を突かれたことによる被害が特に目立っていた**ことが挙げられます。しかしながら、基本的なセキュリティ対策を実施していれば、被害を免れていたと思われるケースが非常に多く見受けられます。一度、原点に返り、**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ょう。

- **ID やパスワードの厳重な管理及び設定**
- **セキュリティホールの解消（パッチ適用不可の場合は、運用による回避策も含む）**
- **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**
- **こまめなログのチェック**

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**
- **パスワードの設定と管理（複雑化、定期的に変更、安易に他人に教えないなど）**
- **無線 LAN や PC 共有についてのセキュリティ設定確認**
- **ルータやパーソナルファイアウォールの活用**

システム管理者向け

・「安全なウェブサイトの作り方　改訂第 2 版」
　http://www.ipa.go.jp/security/vuln/websecurity.html
・「情報セキュリティ対策ベンチマーク」
　http://www.ipa.go.jp/security/benchmark/

・「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
・「脆弱性対策のチェックポイント」
http://www.ipa.go.jp/security/vuln/20050623_websecurity.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
・「他組織からの脆弱性情報」
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
・「コンピュータを守るために最低限必要なセキュリティ対策」（マイクロソフト社）
http://www.microsoft.com/japan/athome/security/protect/default.aspx

■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
加賀谷／花村／宮本
Tel:03-5978-7527 Fax:03-5978-7518 E-mail:isec-info@ipa.go.jp