IPA
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

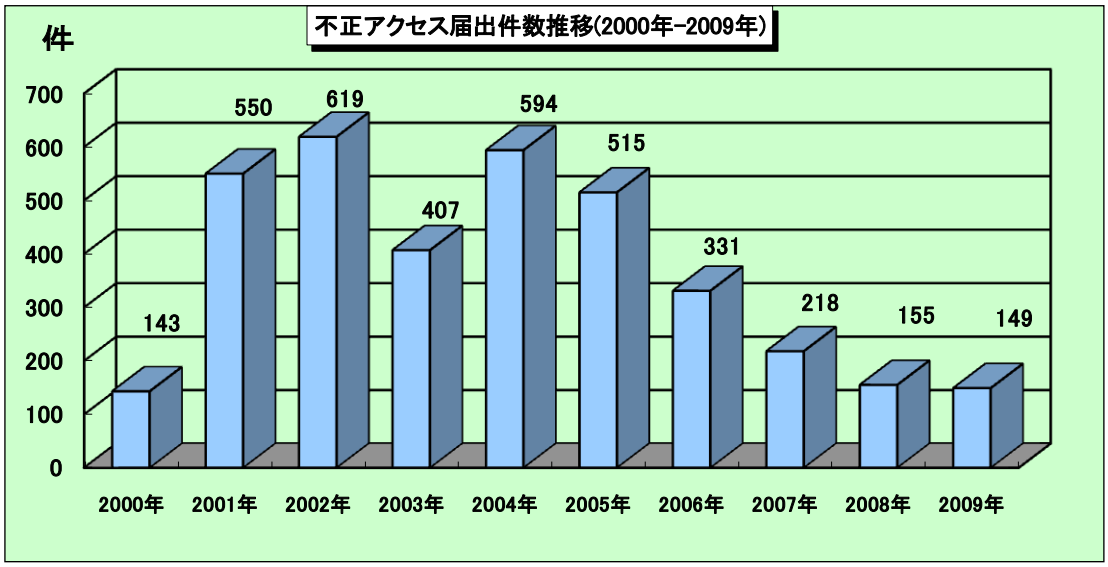
プレスリリース
2010 年 1 月 6 日
独立行政法人情報処理推進機構

2009 年のコンピュータ不正アクセス届出状況

IPA（独立行政法人情報処理推進機構、理事長：西垣 浩司）は、2009 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。

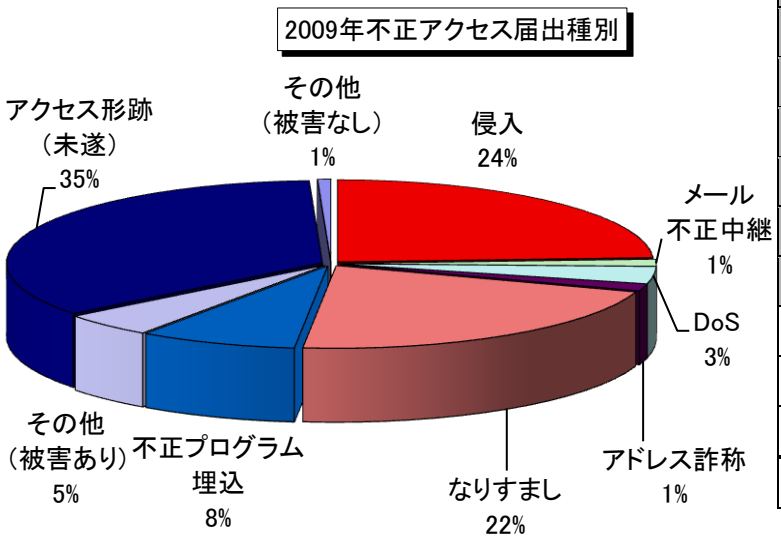
1. 届出件数

2009 年の年間届出件数は **149 件**となり、2008 年の届出件数 155 件から 6 件（約 **4%**）**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。特に、最近では減少傾向にあります。



2. 届出種別

2009 年は 2008 年と比べて、「侵入」の届出数が減少し、結果として被害のあった総件数が減少しました。

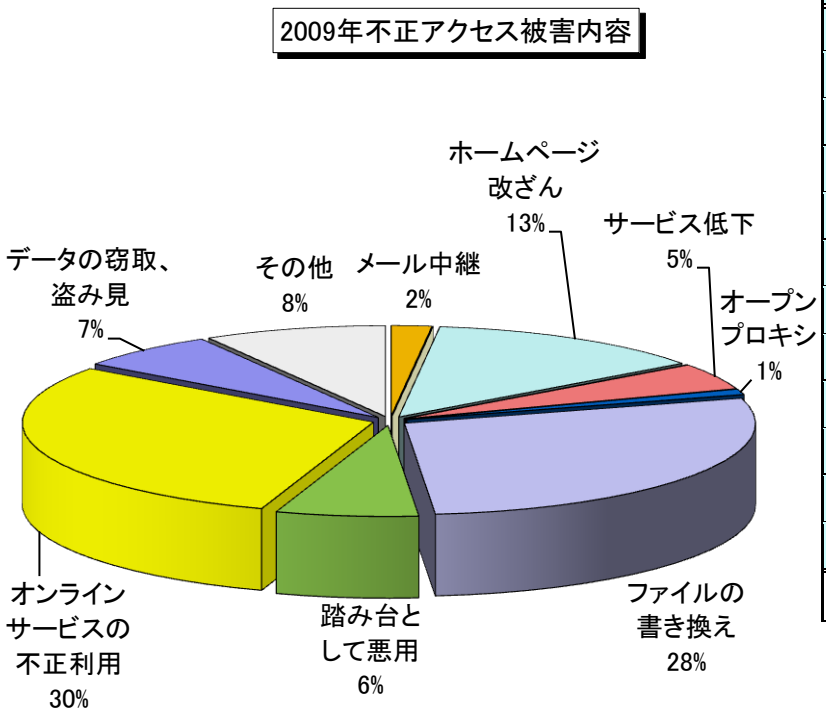


届出種別	2009 年	2008 年
侵入	36	55
メール不正中継	2	0
ワーム感染	0	0
DoS(サービス妨害)	5	11
アドレス詐称	2	9
なりすまし	32	*
不正プログラム埋込	12	*
その他（被害あり）	7	45
アクセス形跡（未遂）	52	21
ワーム形跡	0	0
その他（被害なし）	1	14
合計　（件）	**149(96)**	**155(120)**

※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。
＊ 2008 年までは、「その他（被害あり）」に含まれます。

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から 49 件（約 31%）減少しました。「**ホームページの改ざん**」が増加し、「**サービス低下**」および「**ファイルの書き換え**」が減少していると言えます。

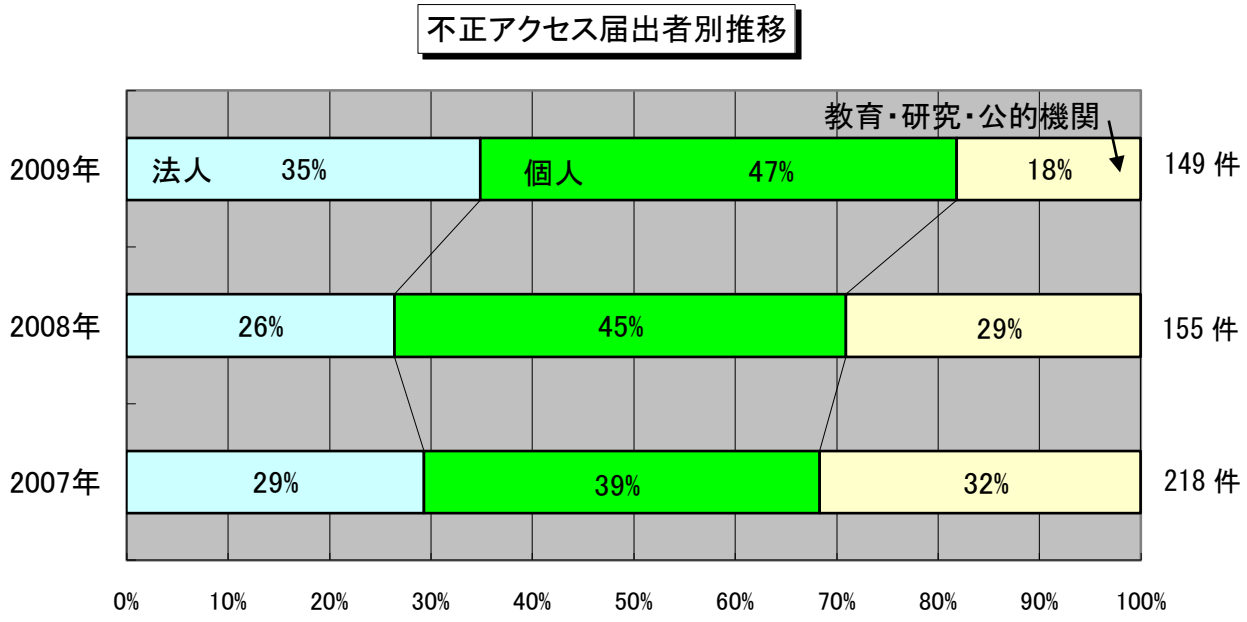


被害内容	2009 年	2008 年
メール不正中継	2	0
サーバーダウン	0	1
不正アカウントの作成	0	0
ホームページ改ざん	14	5
パスワードファイルの盗用	0	0
サービス低下	5	10
オープンプロキシ	1	1
ファイルの書き換え	30	54
踏み台として悪用	7	*
オンラインサービスの不正利用	32	*
データの窃取、盗み見	7	*
その他	9	85
合計 （件）	**107(※)**	**156(※)**

※ 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。
＊ 2008 年までは、「その他」に含まれます。

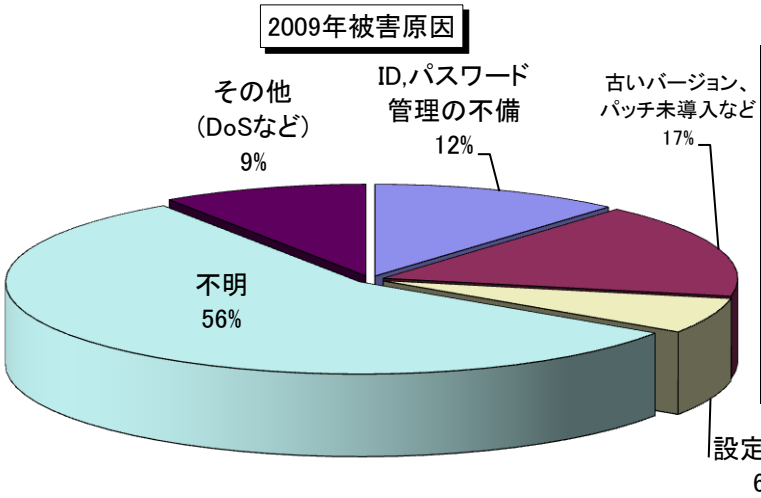
4. 届出者の分類

届出者別の内訳は、**個人からの届出割合がほぼ半数**でした。



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 11 件（12%）、古いバージョン使用・パッチ未導入などが 16 件（17%）、設定不備が 6 件（6%）、となっています。原因が不明なケースは 54 件（56%）と全体の半数を超えており、**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くなっている**ということが推測されます。



被害原因	2009 年	2008 年
ID,パスワード管理の不備	11	35
古いバージョン使用、パッチ未導入など	16	16
設定不備	6	4
不　明	54	39
その他（DoS など）	9	26
合計　（件）	**96**	**120**

6. 対策情報

2009 年の特徴として、**ID/パスワード不備や脆弱性が原因でサイトに侵入されて他サイト攻撃のための踏み台にされたりウェブページを改ざんされたりしたケースや、なりすましによってオンラインゲームなどのサービスを勝手に使われて金銭被害が出たケースが特に目立っていた**ことが挙げられます。特になりすまし被害については、原因が不明なケースがほとんどでした。「なりすまし」被害以外では、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多く見受けられました。**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）**
- **ルータやパーソナルファイアウォールの活用**
- **無線 LAN の暗号化設定確認（WEP は使用せず、できる限り WPA2 を使用する）**

下記情報も参考にしてください。

システム管理者向け

・「情報セキュリティに関する啓発資料」
http://www.ipa.go.jp/security/fy18/reports/contents/

・「脆弱性対策のチェックポイント」
http://www.ipa.go.jp/security/vuln/20050623_websecurity.html

・「安全なウェブサイトの作り方　改訂第 3 版」
http://www.ipa.go.jp/security/vuln/websecurity.html

・「JVN（Japan Vulnerability Notes）」　※脆弱性対策情報ポータルサイト
http://jvn.jp/

・「SQL インジェクション攻撃に関する注意喚起」
http://www.ipa.go.jp/security/vuln/documents/2008/200805_SQLinjection.html

・「ウェブサイトで利用されている DNS サーバの既知の脆弱性への注意喚起」
http://www.ipa.go.jp/security/vuln/documents/2009/200912_dns.html

・「古いソフトウェア製品を利用しているウェブサイトへの注意喚起」
http://www.ipa.go.jp/security/vuln/documents/2009/200903_update.html

エンドユーザ・ホームユーザ向け

・「IPA セキュリティセンター・個人ユーザ向けページ」
http://www.ipa.go.jp/security/personal/

・「マイクロソフトセキュリティ At Home」（マイクロソフト社）
http://www.microsoft.com/japan/protect/default.mspx

・MyJVN（セキュリティ設定チェッカ、バージョンチェッカ）
http://jvndb.jvn.jp/apis/myjvn/

■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／大浦

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