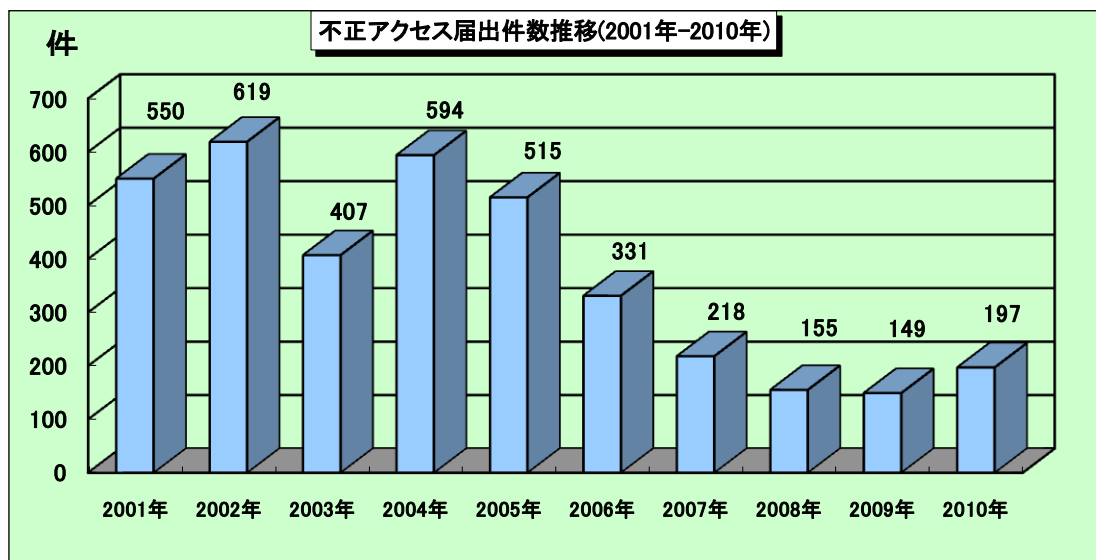


2010年のコンピュータ不正アクセス届出状況

IPA（独立行政法人情報処理推進機構、理事長：藤江 一正）は、2010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。

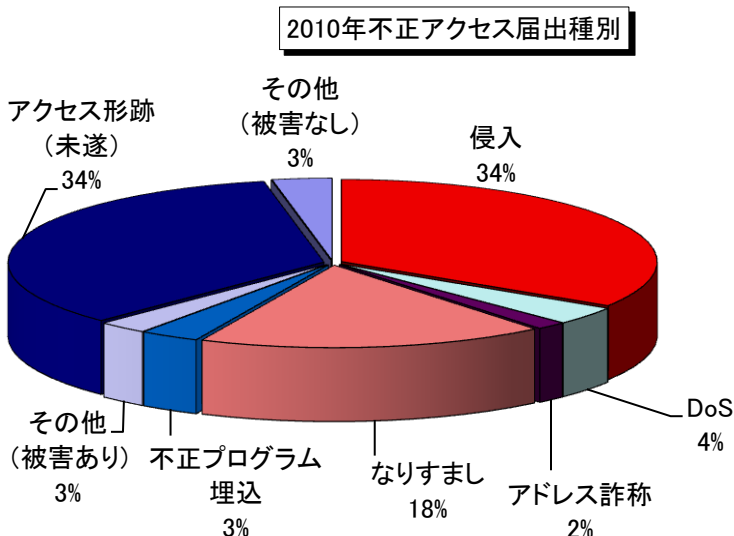
1. 届出件数

2010年の年間届出件数は**197件**となり、2009年の届出件数149件から48件（約**32%**）増加しました。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。2010年は、過去2年と比べ、増加に転じました。



2. 届出種別

2010年は2009年と比べて、「侵入」の届出数が増加し、結果として被害のあった総件数が増加しました。



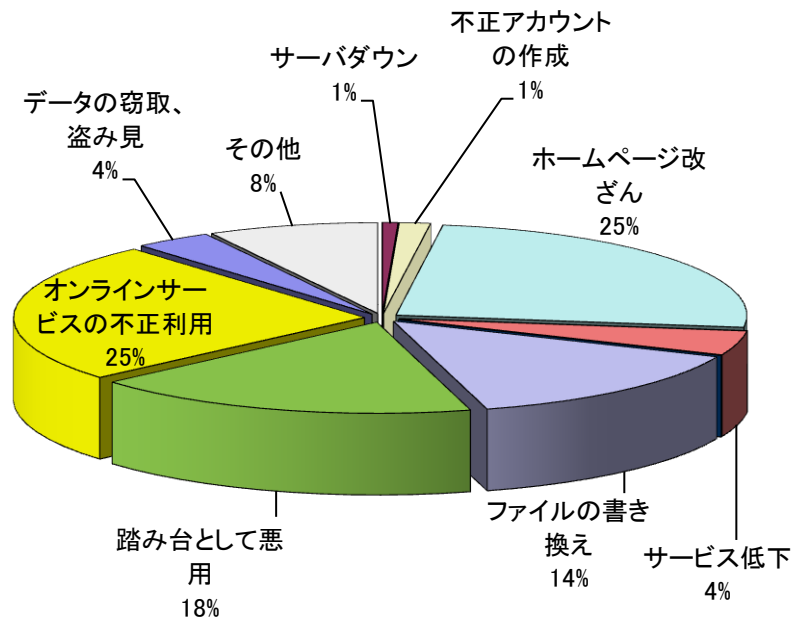
| 届出種別 | 2010年 | 2009年 |
|--------------|-----------------|----------------|
| 侵入 | 67 | 36 |
| メール不正中継 | 0 | 2 |
| ワーム感染 | 0 | 0 |
| DoS(サービス妨害) | 7 | 5 |
| アドレス詐称 | 3 | 2 |
| なりすまし | 35 | 32 |
| 不正プログラム埋込 | 6 | 12 |
| その他(被害あり) | 5 | 7 |
| アクセス形跡(未遂) | 68 | 52 |
| ワーム形跡 | 0 | 0 |
| その他(被害なし) | 6 | 1 |
| 合計(件) | 197(123) | 149(96) |

※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。

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33件(約31%)増加しました。「ホームページの改ざん」および「踏み台として悪用」が増加し、「ファイルの書き換え」が減少していると言えます。

2010年不正アクセス被害内容



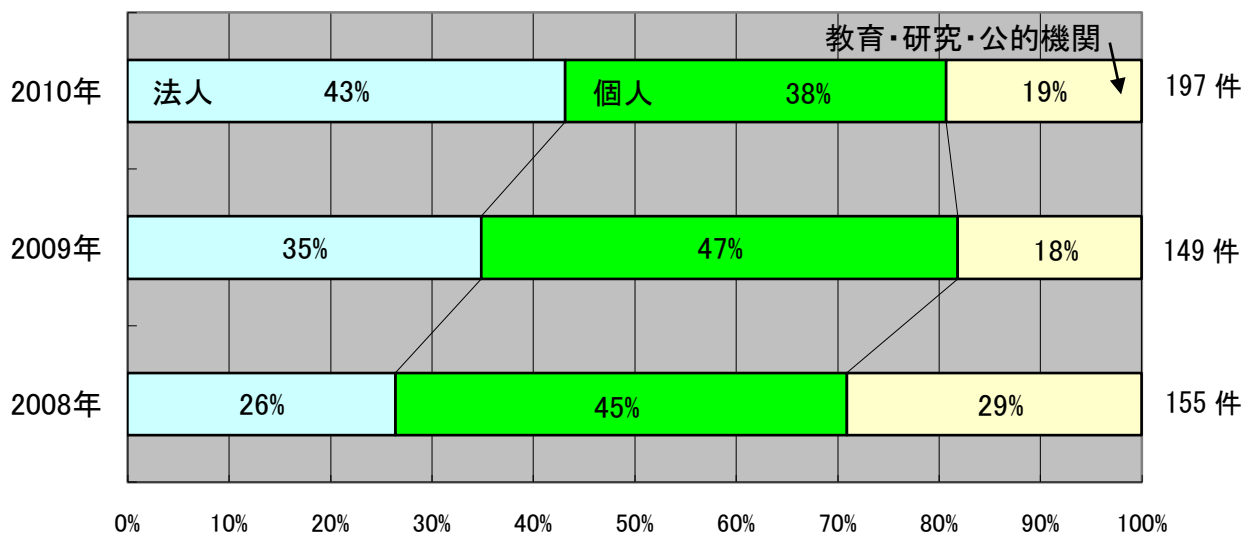
| 被害内容 | 2010年 | 2009年 |
|----------------|---------------|---------------|
| メール不正中継 | 0 | 2 |
| サーバダウン | 1 | 0 |
| 不正アカウントの作成 | 2 | 0 |
| ホームページ改ざん | 35 | 14 |
| パスワードファイルの盗用 | 0 | 0 |
| サービス低下 | 6 | 5 |
| オープンプロキシ | 0 | 1 |
| ファイルの書き換え | 20 | 30 |
| 踏み台として悪用 | 25 | 7 |
| オンラインサービスの不正利用 | 35 | 32 |
| データの窃取、盗み見 | 5 | 7 |
| その他 | 11 | 9 |
| 合計 (件) | 140(※) | 107(※) |

※ 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

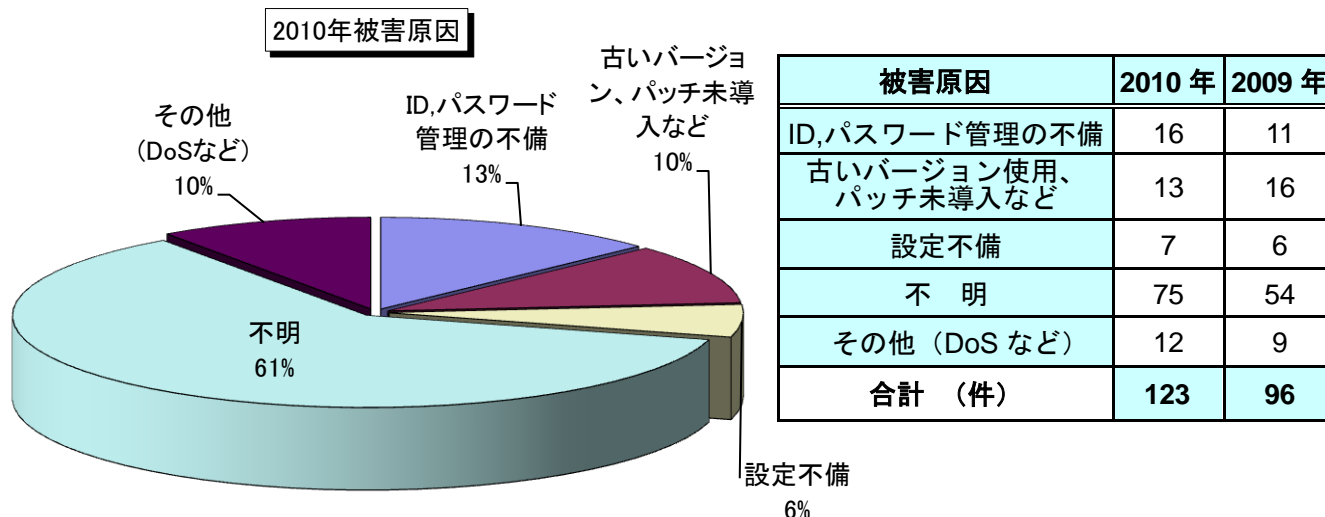
届出者別の内訳は、法人からの届出割合が個人を上回りました。

不正アクセス届出者別推移



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16件（13%）、古いバージョン使用・パッチ未導入などが13件（10%）、設定不備が7件（6%）、となっています。原因が不明なケースは75件（61%）と全体の半数を超えており、また、2009年と比べて21件（約39%）も増加していることから、2010年においても、不正アクセスの手口の巧妙化および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。



6. 対策情報

2010年の特徴として、いわゆる「ガンブラー」によるウェブサイト改ざんの被害が特に多かったことが挙げられます。また、その被害原因の多くが不明なケースだったことから、こうした改ざんを行うための攻撃手口の巧妙化が伺えます。その他では、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や、SSHで使用するポートへの攻撃で侵入（ID、パスワードの設定不備や不明が主な原因）され、他のコンピュータを攻撃するための踏み台に悪用されていた被害も目立っていたことが挙げられます。主に原因不明なケースが多く見受けられますが、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。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への解消（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4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
- ・「ウェブサイト管理者へ：ウェブサイト改ざんに関する注意喚起」
<http://www.ipa.go.jp/security/topics/20091224.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.aspx>
- ・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/>
- ・「一般利用者へ：改ざんされたウェブサイトからのウイルス感染に関する注意喚起」
<http://www.ipa.go.jp/security/topics/20091224.html>

■お問い合わせ先

IPA セキュリティセンター 加賀谷／宮本

Tel:03-5978-7591 Fax:03-5978-7518

E-mail:isec-info@ipa.go.jp