IPA
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

プレスリリース
2005 年 4 月 6 日
独立行政法人 情報処理推進機構

2005 年第 1 四半期［1 月～3 月］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、2005 年第 1 四半期[1 月～3 月]のコンピュータ不正アクセスの届出状況をまとめました。

2005 年第 1 四半期の届出状況から、最近の傾向として

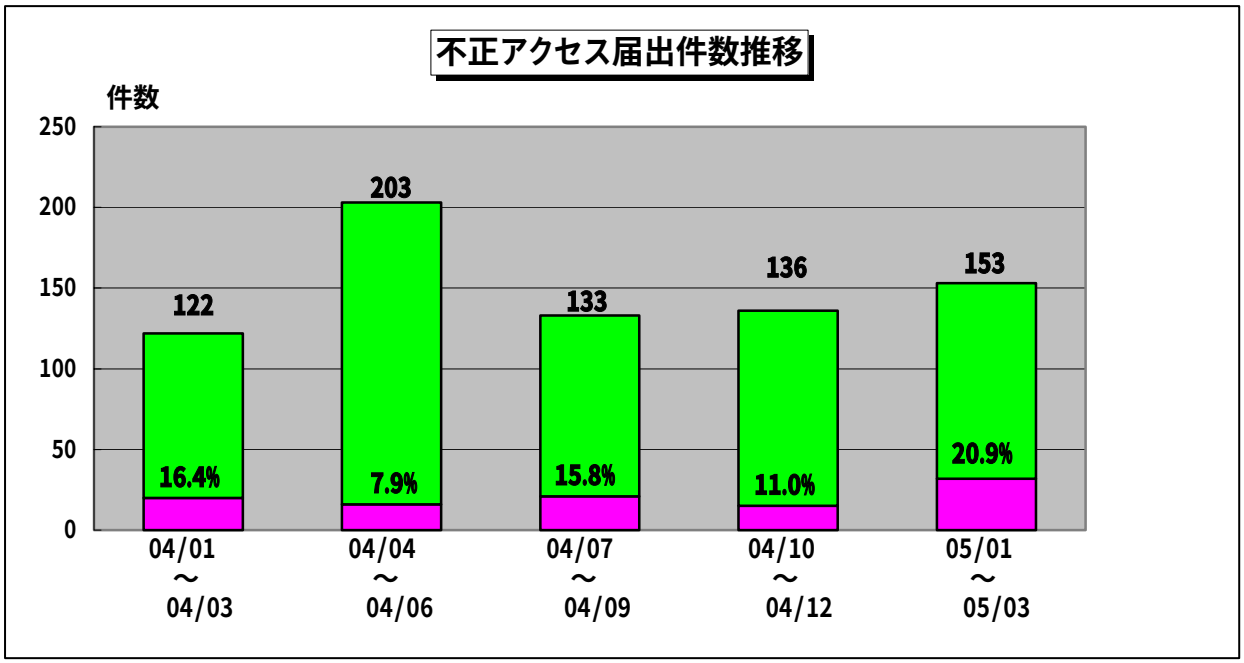
- 家庭ユーザの PC を含めたあらゆるコンピュータへの無差別な攻撃が多い
- Web サーバに侵入され、フィッシングに使うための偽の Web コンテンツを設置される被害が増えつつある

と言えます。以下のサイトを参考にコンピュータセキュリティ設定の徹底及び日常の運用管理によるセキュリティ対策を継続するよう心がけてください。

- **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**
  http://www.ipa.go.jp/security/awareness/end-users/end-users.html
- **情報セキュリティ対策実践情報 システム管理者向け**
  http://www.ipa.go.jp/security/awareness/administrator/administrator.html

1. 届出件数

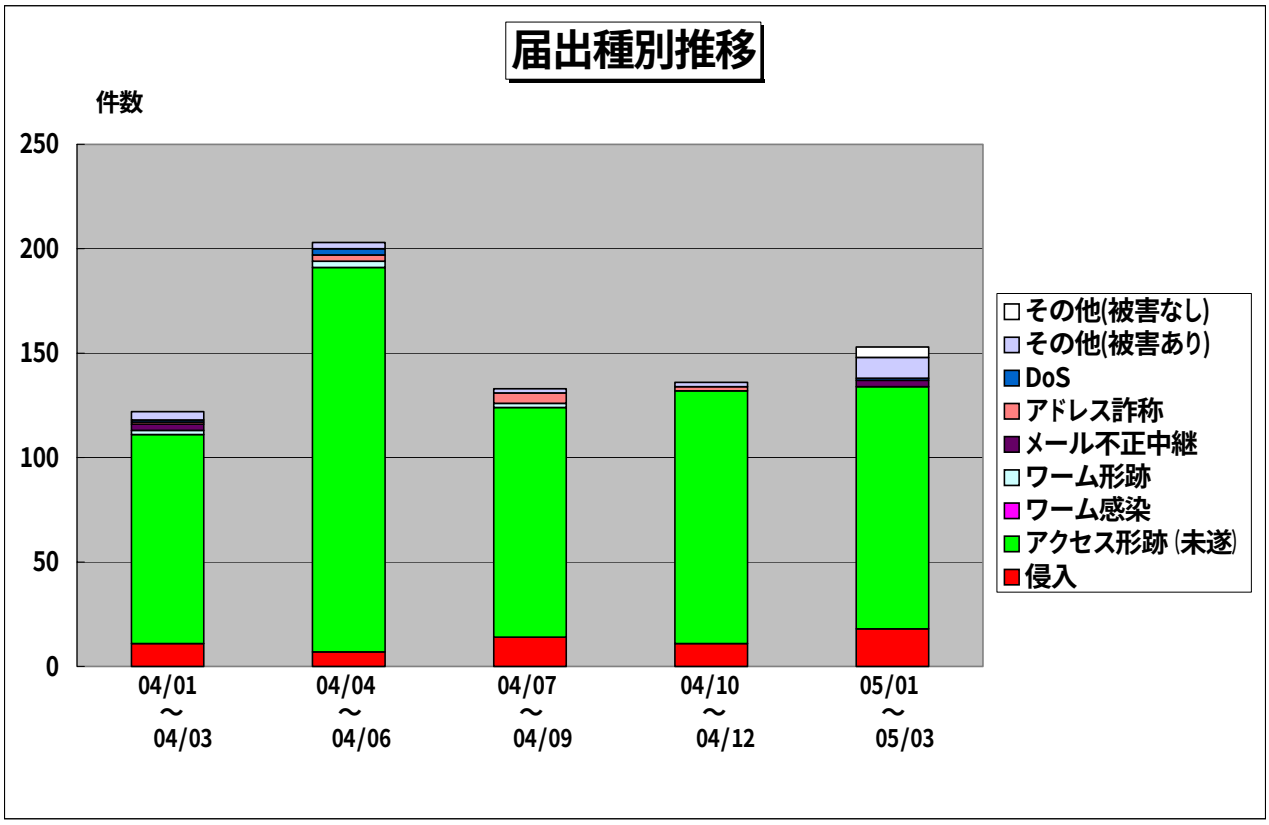
2005 年第 1 四半期(1 月～3 月)の届出件数は合計 153 件となり、届出総数は約 13%の増加でしたが、被害にあった件数の割合はほぼ倍増となりました。



※グラフ中の%表示は、届出総数のうち被害に遭った件数の割合を示している。

2.届出種別

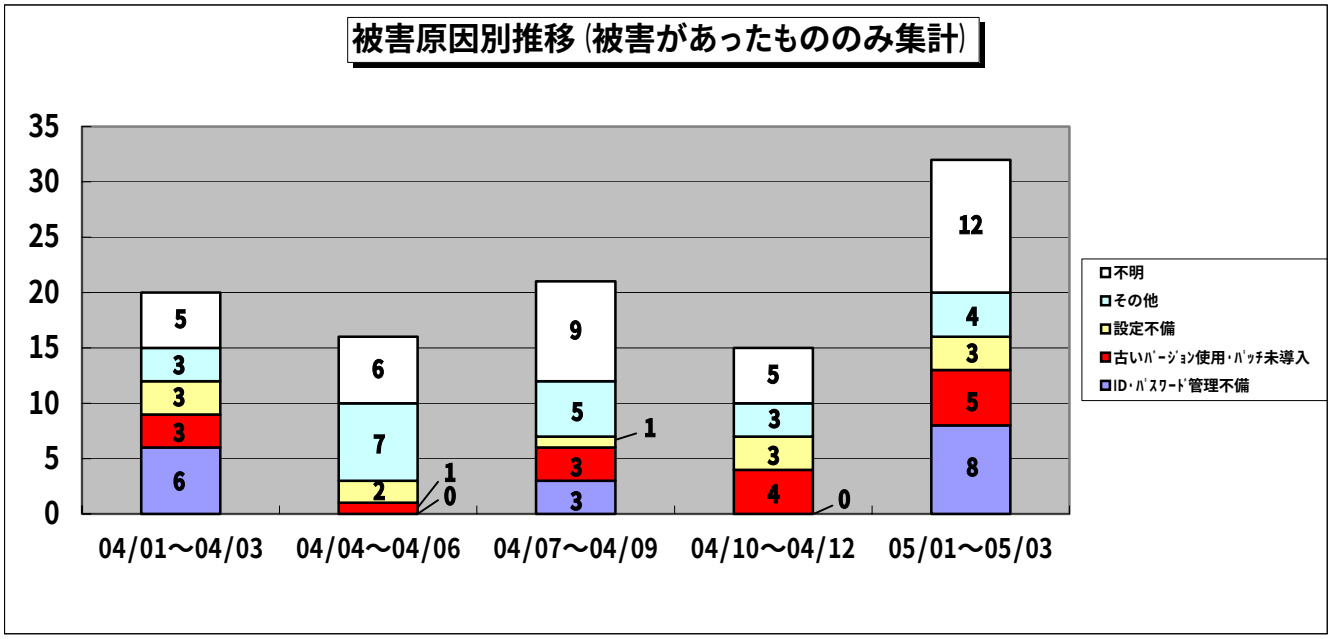
IPA に届けられた 153 件のうち、不正なアクセス形跡を発見した**「アクセス形跡（未遂）」の届出が 116 件（前期 121 件）**と全体の 75.8%を占めました。また、実際に被害に遭った届出は 32 件（前期 15 件）と全体の 20.9%を占めました。実際に被害に遭った届出とは「侵入」「ワーム感染」「アドレス詐称」「メール不正中継」「DoS」「その他(被害あり)」の合計です。



	2004 年 第 1 四半期	2004 年 第 2 四半期	2004 年 第 3 四半期	2004 年 第 4 四半期	2005 年 第 1 四半期
侵入	11(9.0%)	7(3.4%)	14(10.5%)	11(8.1%)	18(11.8%)
アクセス形跡(未遂)	100(82.0%)	184(90.6%)	110(82.7%)	121(89.0%)	116(75.8%)
ワーム感染	0(0.0%)	0(0.0%)	0(0.0%)	0(0.0%)	0(0.0%)
ワーム形跡	2(1.6%)	3(1.5%)	2(1.5%)	0(0.0%)	0(0.0%)
メール不正中継	3(2.5%)	0(0.0%)	0(0.0%)	0(0.0%)	3(2.0%)
アドレス詐称	1(0.8%)	3(1.5%)	5(3.8%)	2(1.5%)	0(0.0%)
DoS	1(0.8%)	3(1.5%)	0(0.0%)	0(0.0%)	1(0.7%)
その他(被害あり)	4(3.3%)	3(1.5%)	2(1.5%)	2(1.5%)	10(6.5%)
その他(被害なし)	0(0.0%)	0(0.0%)	0(0.0%)	0(0.0%)	5(3.3%)
合計(件)	122	203	133	136	153

3.被害原因

実際に被害があった届出（32 件）のうち、原因の内訳は **ID・パスワード管理不備が 8 件、古いバージョン使用・パッチ未導入が 5 件、設定不備が 3 件など**でした。



※被害原因が複数あった届出については、1 件の届出につき主たる原因を代表として 1 件と集計しています。

被害事例：

I. Web サーバソフトウェアの脆弱性を突かれたりパスワード管理が不備だったりしたために Web サーバに侵入され、フィッシングに悪用することを目的とした偽の Web コンテンツを設置された。

II. Web サーバ管理 ID とパスワードに対する辞書攻撃や OS の脆弱性を突いた攻撃により侵入され、管理者権限パスワードの変更やファイルの改ざんが行われたり、踏み台として外部へ攻撃を行われたりした。

III. サービスプロバイダを利用した個人開設のホームページに、本人に成りすましてログインされ、コンテンツや画像を改ざんされたり削除されたりした。

IV. オークションサイトの ID とパスワードを本人に成りすまして利用され、ID を削除されたり評価を荒らされたり、勝手にメールを送られたりした。

V. IIS（Internet Information Server）の設定不備により WebDAV 機能を悪用され、Web コンテンツを改ざんされた。

VI. 遠隔から作業が出来るように一時的に設定を変更したが、設定を戻さずに運用したため侵入され、Web コンテンツのトップページを改ざんされた。

VII. DDoS と思われるアクセスにより、Web サーバ機能が低下した。

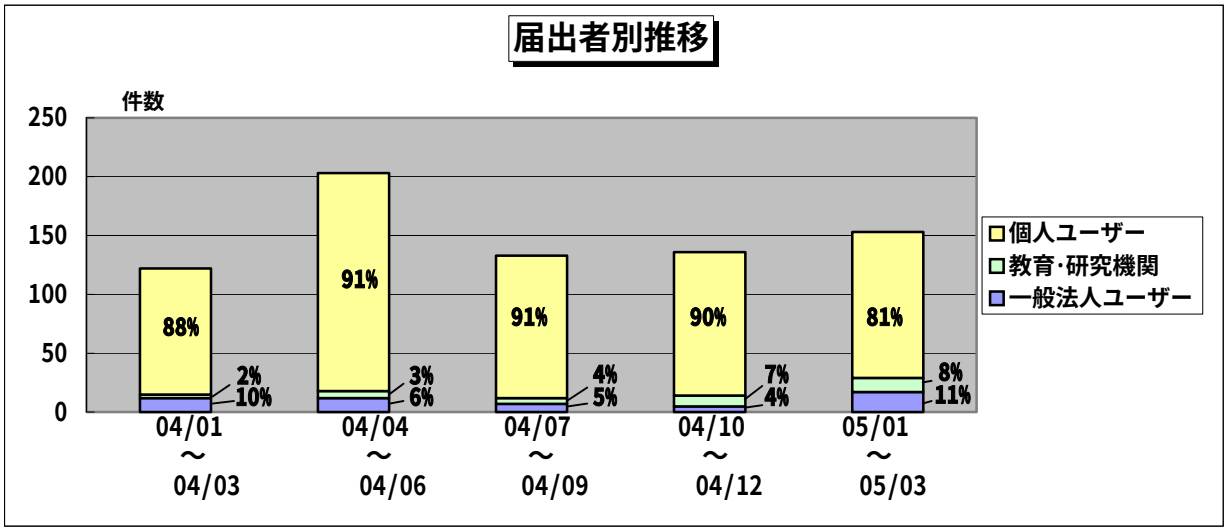
VIII. あるサービス登録案内メールが届いたため、Web アクセスして自分のメールアドレスとパスワードを入力し、登録手続きをした。後日、そのサービスが架空のものと判明し、個人情報を不正に奪取されたことに気が付いた。

IX. 怪しいサイトにアクセスしたところ、Internet Explorer のスタートページ設定が改変され元に戻せなくなったり、セキュリティソフトの機能を停止させられたりした。

X. アダルトサイトにアクセスし、プログラムのダウンロードの許可を問う画面で安易に[はい]をクリックしたところ、不正なプログラムがインストールされたり、身に覚えの無いサイトの利用料請求画面が表示されたりした。

4.届出者の分類

届出者別の内訳は、**個人が約 81%**を占め、依然として高い割合を占めています。



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