別紙４

2005 年上半期［1 月～6 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 年上半期[1 月～6 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 年上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 アプリケーションの脆弱性を突かれた侵入被害が増えつつある

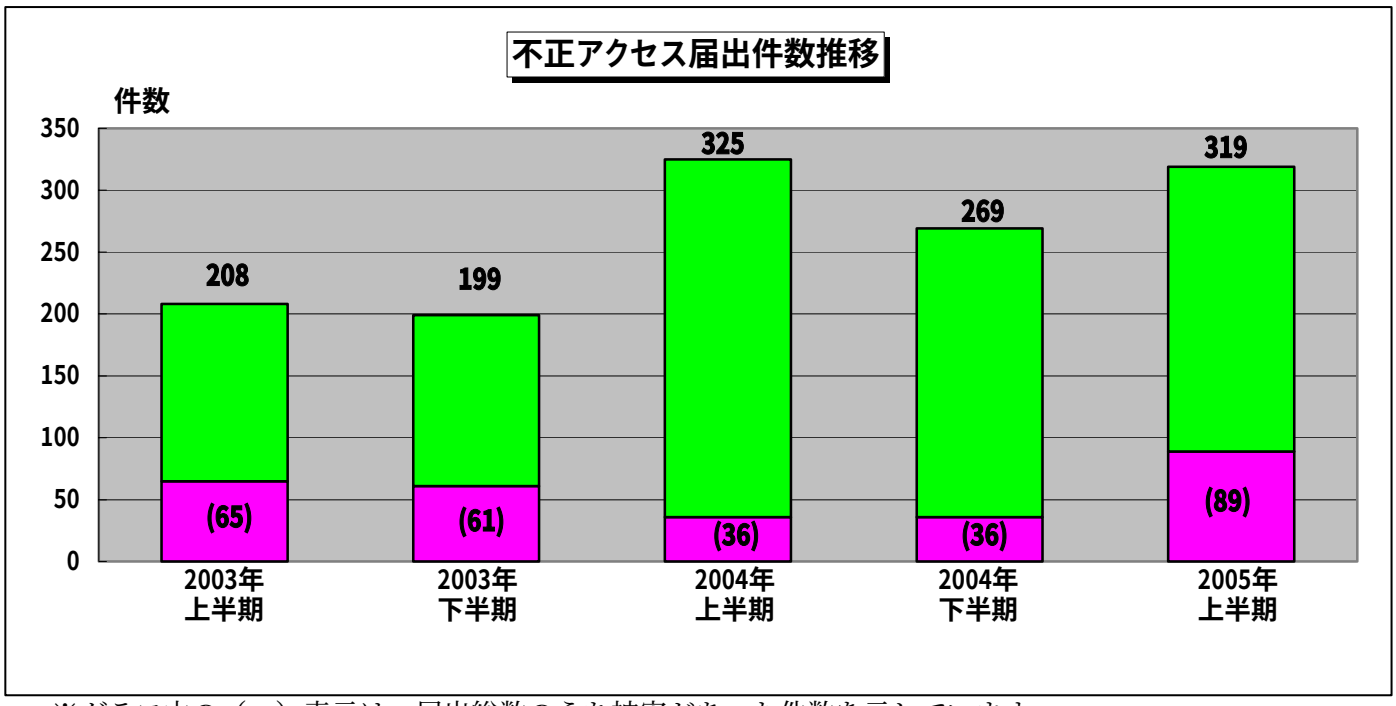
と言えます。以下のサイトを参考にコンピュータセキュリティ設定の徹底及び日常の運用管理によるセキュリティ対策を継続するよう心がけてください。

■ **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

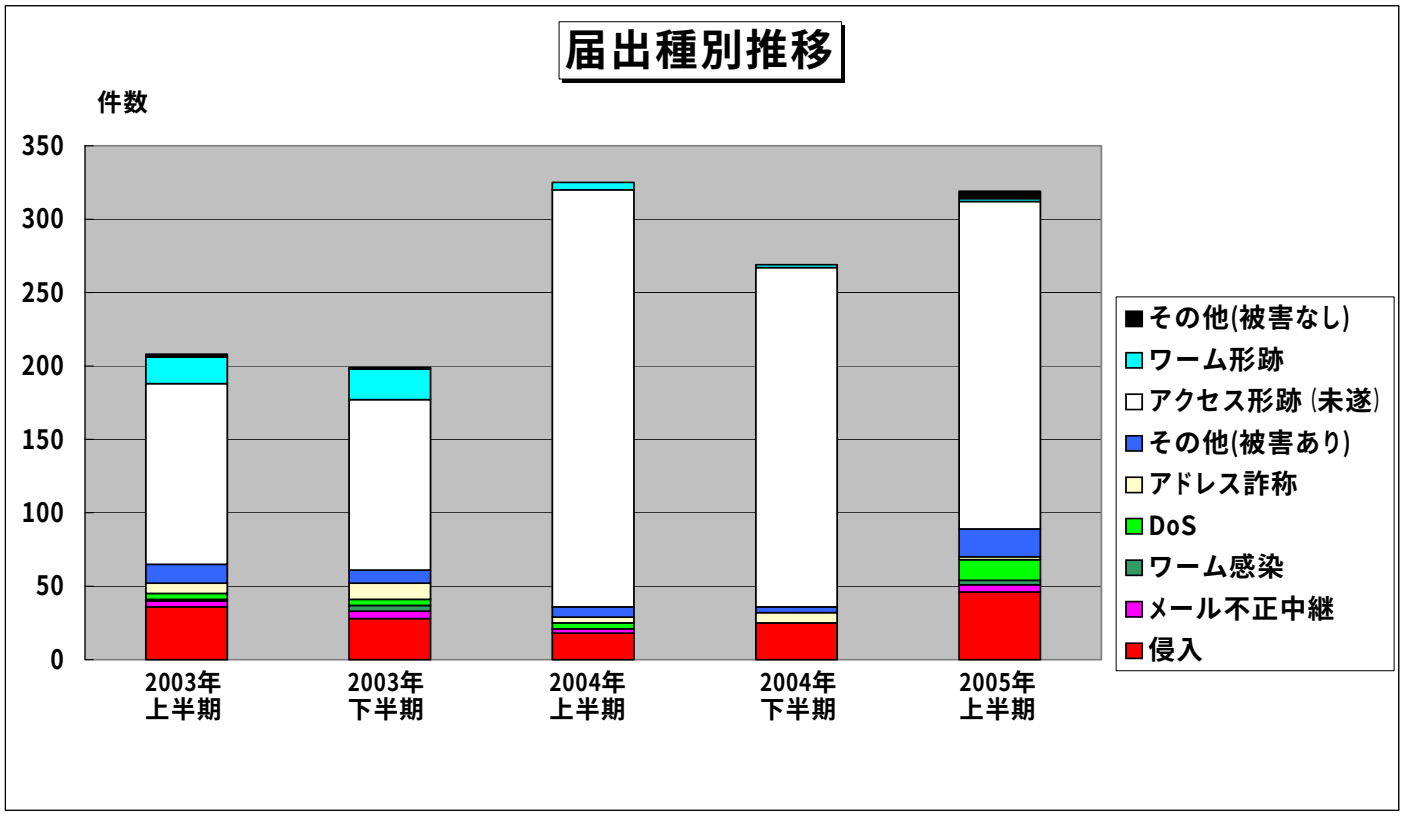
2005 年上半期(1 月～6 月)の届出件数は合計 319 件となり、届出総数は約 18%の増加でしたが、被害にあった件数は約 2.5 倍となりました。



※グラフ中の（ ）表示は、届出総数のうち被害があった件数を示しています。

2.届出種別

IPA に届けられた 319 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 223 件**（先期 231 件）と全体の 69.9%を占めました。また、**実際に被害に遭った届出は 89 件**（先期 36 件）と全体の 27.9%を占めました。実際に被害に遭った届出とは「侵入」「メール不正中継」「ワーム感染」「DoS」「アドレス詐称」「その他(被害あり)」の合計です。

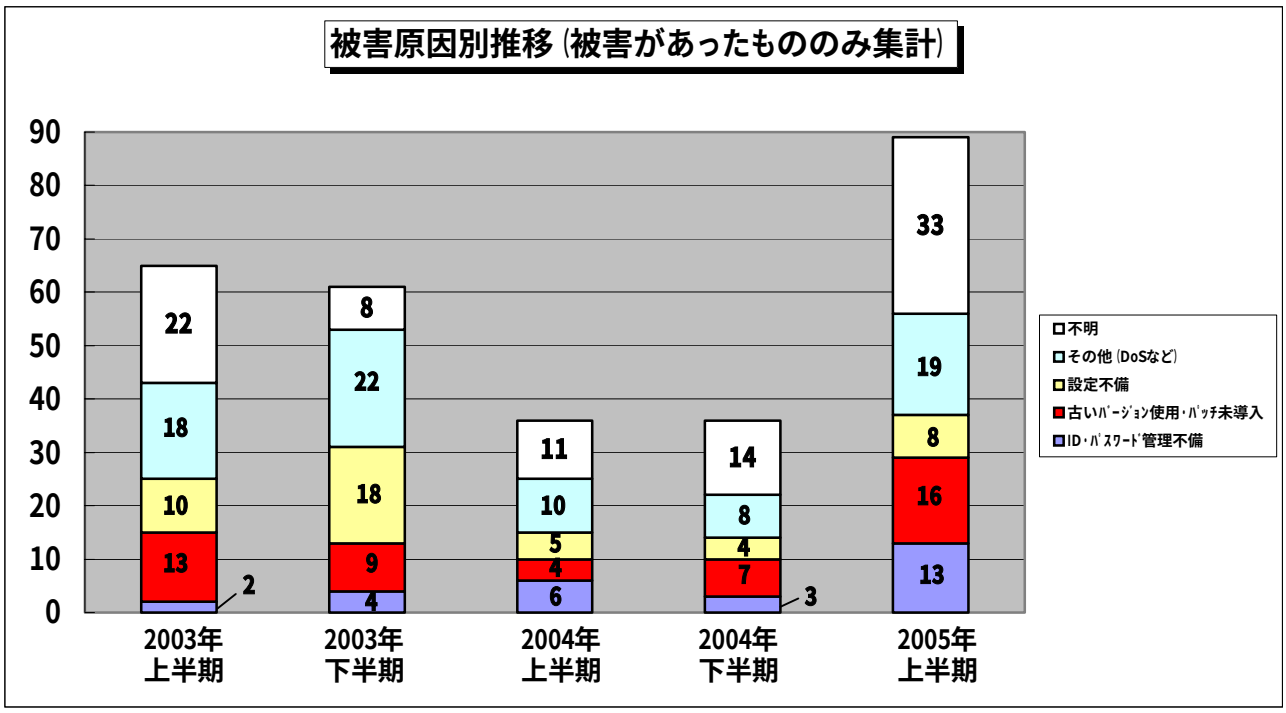


	2003 年 上半期		2003 年 下半期		2004 年 上半期		2004 年 下半期		2005 年 上半期	
侵入	36	17.3%	28	14.1%	18	5.5%	25	9.3%	46	14.4%
メール不正中継	4	1.9%	5	2.5%	3	0.9%	0	0.0%	5	1.6%
ワーム感染	1	0.5%	4	2.0%	0	0.0%	0	0.0%	3	0.9%
DoS	4	1.9%	4	2.0%	4	1.2%	0	0.0%	14	4.4%
アドレス詐称	7	3.4%	11	5.5%	4	1.2%	7	2.6%	2	0.6%
その他(被害あり)	13	6.3%	9	4.5%	7	2.2%	4	1.5%	19	6.0%
アクセス形跡(未遂)	123	59.1%	116	58.3%	284	87.4%	231	85.9%	223	69.9%
ワーム形跡	18	8.7%	21	10.6%	5	1.5%	2	0.7%	2	0.6%
その他(被害なし)	2	1.0%	1	0.5%	0	0.0%	0	0.0%	5	1.6%
合計(件)	208		199		325		269		319	

注）網掛け部分は、被害があった届出種類。
割合の数字は小数点第二位を四捨五入していますので、合計が 100%ちょうどにならない場合があります。

3.被害原因

実際に被害があった届出（89 件）のうち、原因の内訳は**ID・パスワード管理不備が 13 件、古いバージョン使用・パッチ未導入が 16 件、設定不備が 8 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：

[侵入]

(i)　Web サーバに侵入され、利用者が Web コンテンツを閲覧しただけで不正なプログラムをダウンロードさせられてしまう仕組みを埋め込まれているのを発見。改ざん箇所の調査を進めるうちに、データベースでの改ざん形跡が発見されるなどし、最終的には一時的なサイト閉鎖に追い込まれた。

(ii)　管理者権限を不正に奪取されて Web サーバに侵入され、不正にファイルを置かれたり Web ページを改ざんされたりした。データベースシステムに対する SQL インジェクション攻撃が原因。

(iii) 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。

(iv)　PHP を用いた掲示板プログラム「phpBB」の脆弱性を突かれて侵入され、フォーラムログおよびサイトテンプレートが改ざんされたり、削除されたりした。

(v)　SSH（Secure Shell）の 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、踏み台として外部へ攻撃を行われた。

[DoS]

(vi)　SSH で使用するポートへの不正なアクセスが多発したため、サーバがダウンした。

(vii)　通信障害が起きたため調査したところ、少なくても 1 秒間に 100 万パケット以上の SYN フラッド攻撃を受けていることが判明。ルータの使用率が 100%となり、通信が不能となった。ルータの DoS 攻撃対策機能を駆使しても対応し切れず、最終的にはプロバイダに対して、該当 IP アドレス宛のパケットを全て破棄する設定を施してもらい回復した。

[なりすまし]

(viii)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。

(ix)　オークションサイトで本人に成りすましてログインされ、見知らぬメールアドレスが連絡先として書き換えられ、勝手に出品や落札をされた。

(x)　インターネットのオンラインゲームに不正にログインされ、ゲーム上で使用するお金やアイテムを盗まれた。

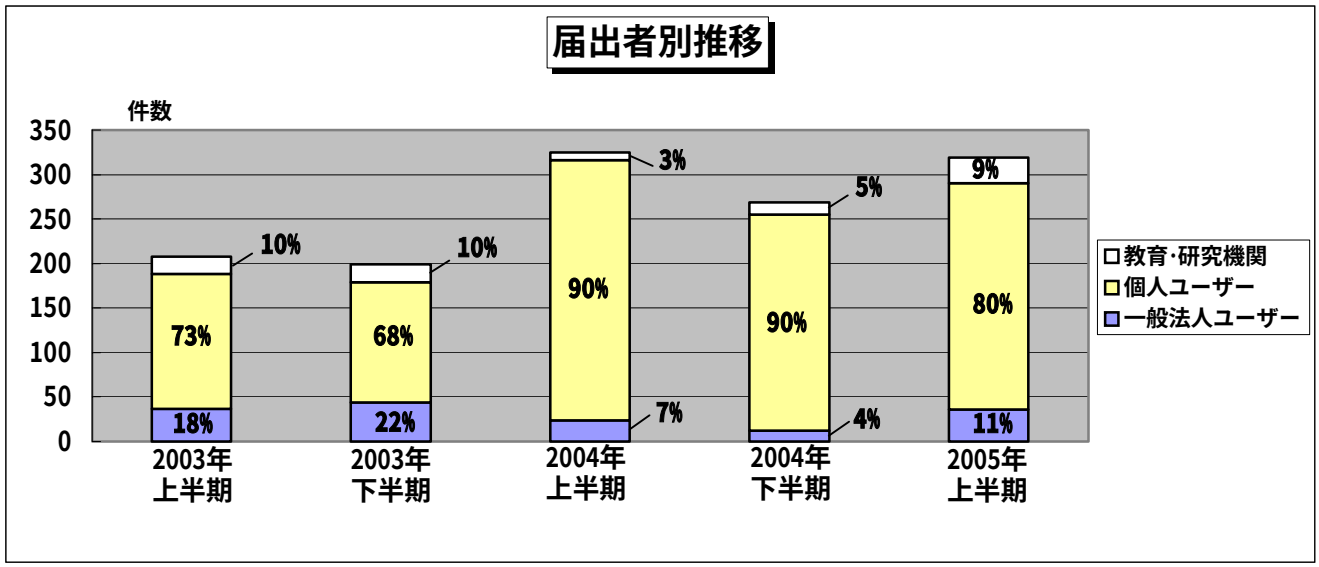
[その他]

(xi)　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。

(xii) 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。

4.届出者の分類

届出者別の内訳は、**個人が 80%**を占め、依然として高い割合を占めています。



注）割合の数字は小数点第一位を四捨五入していますので、合計が 100%ちょうどにならない場合があります。

■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