IPA
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

プレスリリース
2005 年 10 月 6 日
独立行政法人 情報処理推進機構

2005 年第 3 四半期［7 月～9 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 3 四半期[7 月～9 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 3 四半期の届出状況から、最近の傾向として

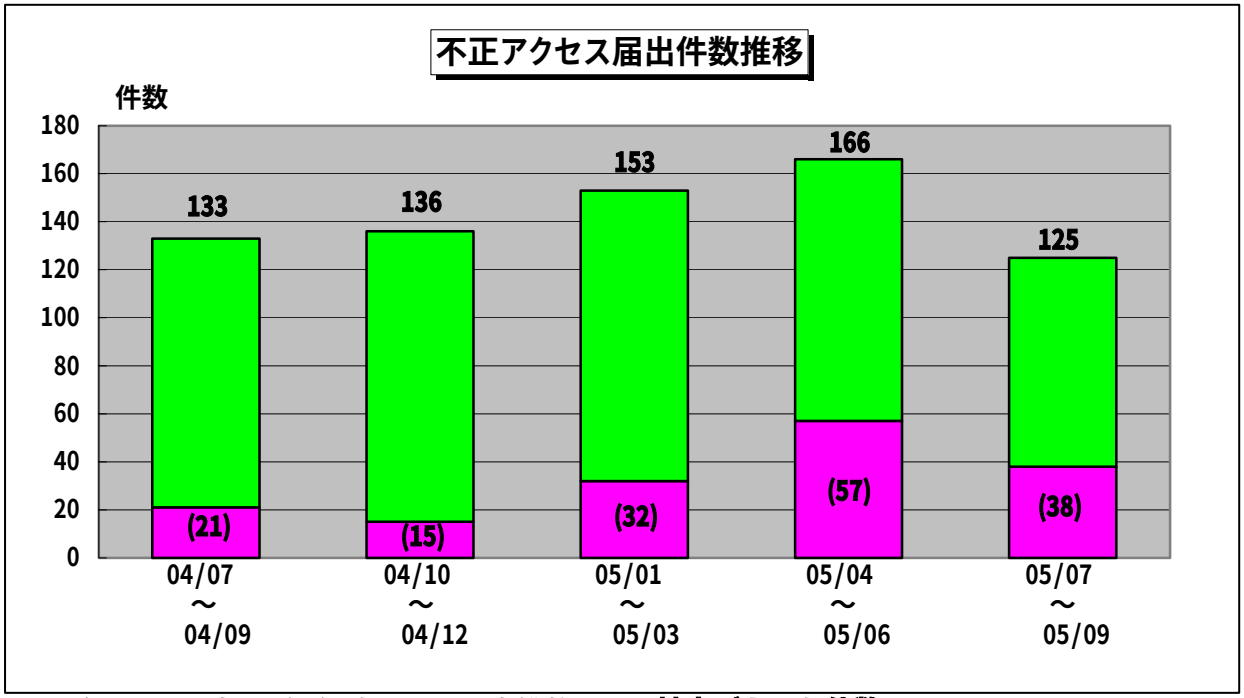
- 家庭ユーザの PC を含めたあらゆるコンピュータへの無差別な攻撃が多い
- Web サーバに侵入され、他サーバへの攻撃の踏み台に使われる被害が増えつつある

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

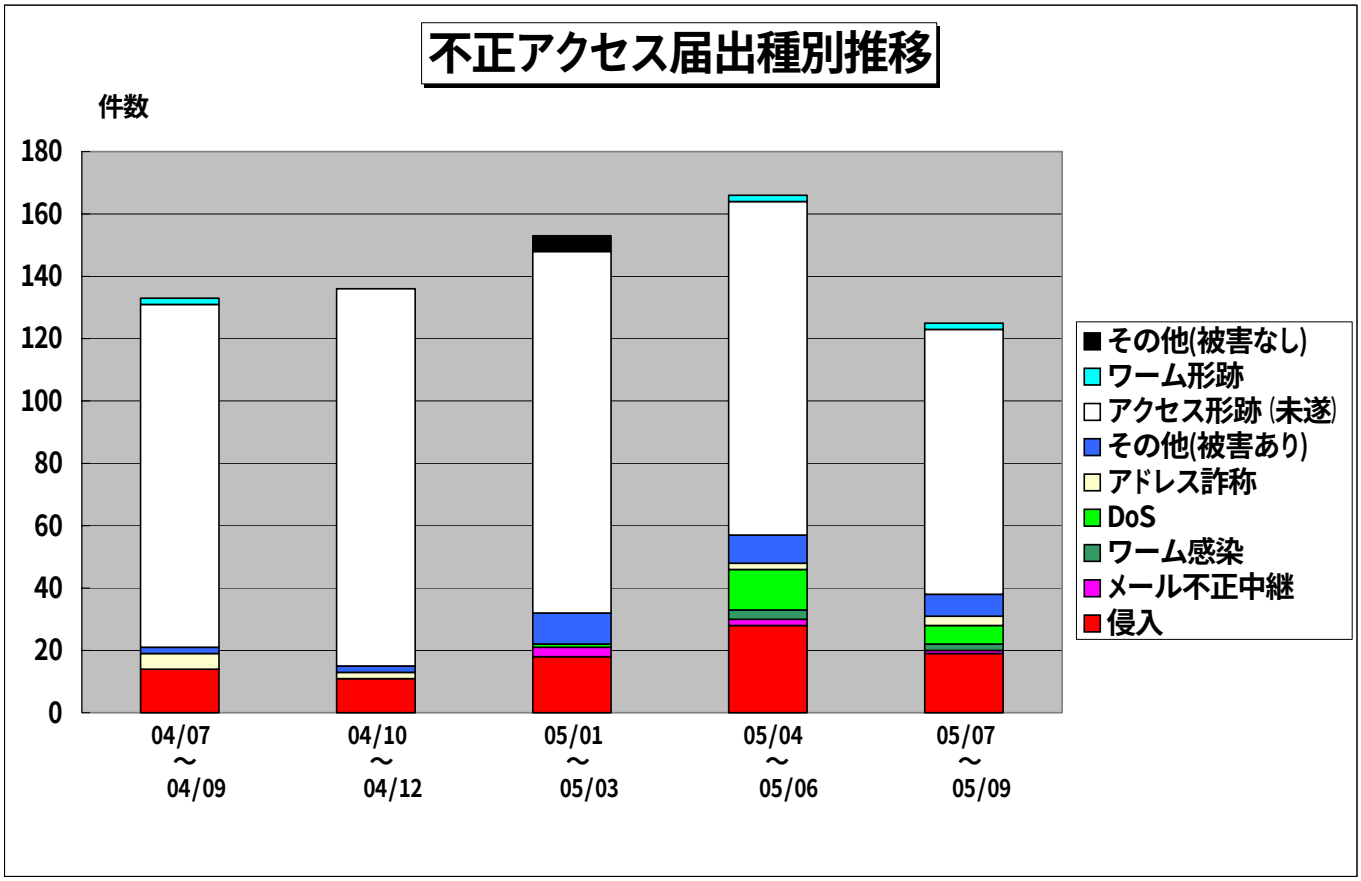
2005 年第 3 四半期(7 月～9 月)の届出件数は合計 125 件となり、届出総数は約 25%の減少でしたが、被害にあった件数の割合は約 33%の減少となりました。



注) 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 125 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 85 件（前期 107 件）**と全体の 68.0%を占めました。また、実際に被害があった届出は 38 件（前期 57 件）と全体の 30.4%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。

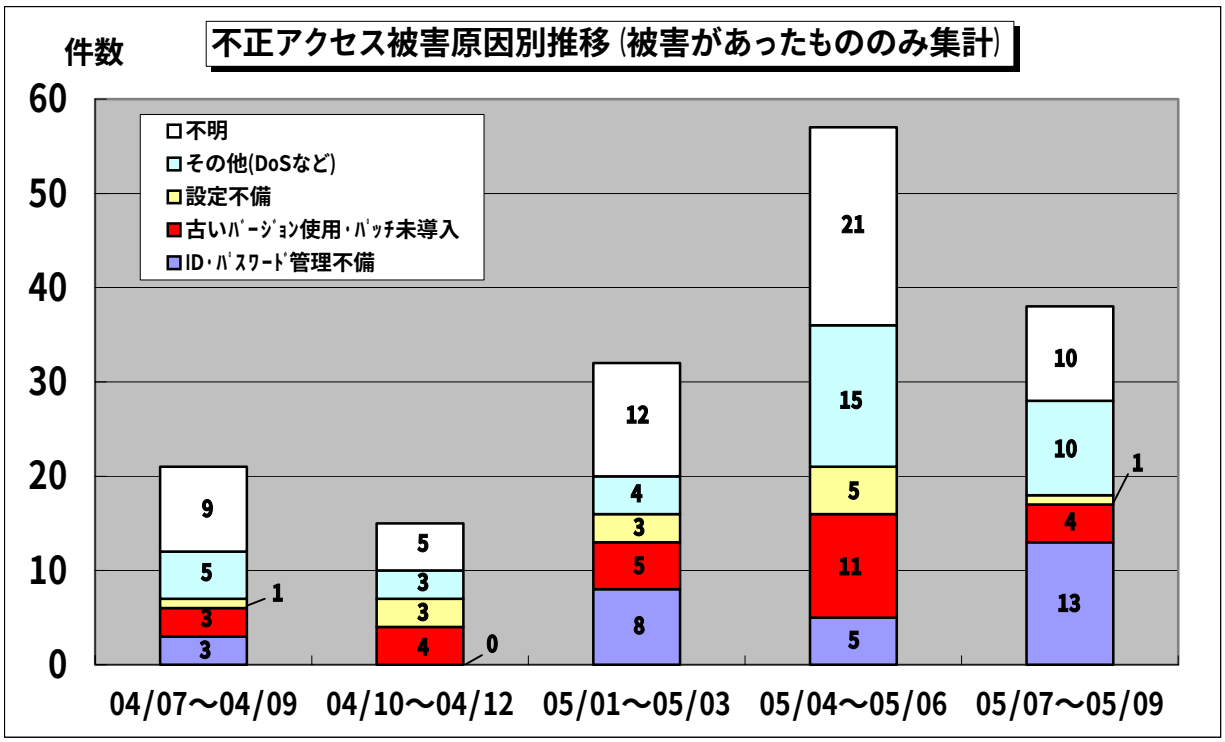


	2004年 第3四半期		2004年 第4四半期		2005年 第1四半期		2005年 第2四半期		2005年 第3四半期	
侵入	14	10.5%	11	8.1%	18	11.8%	28	16.9%	19	15.2%
メール不正中継	0	0.0%	0	0.0%	3	2.0%	2	1.2%	1	0.8%
ワーム感染	0	0.0%	0	0.0%	0	0.0%	3	1.8%	2	1.6%
DoS	0	0.0%	0	0.0%	1	0.7%	13	7.8%	6	4.8%
アドレス詐称	5	3.8%	2	1.5%	0	0.0%	2	1.2%	3	2.4%
その他(被害あり)	2	1.5%	2	1.5%	10	6.5%	9	5.4%	7	5.6%
アクセス形跡(未遂)	110	82.7%	121	89.0%	116	75.8%	107	64.5%	85	68.0%
ワーム形跡	2	1.5%	0	0.0%	0	0.0%	2	1.2%	2	1.6%
その他(被害なし)	0	0.0%	0	0.0%	5	3.3%	0	0.0%	0	0.0%
合 計(件)	**133**		**136**		**153**		**166**		**125**	

注）網掛け部分は、**被害があった**届出種類を示しています。
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（38 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 4 件、設定不備が 1 件など**でした。



注）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) サーバに侵入され、システム内部から spam メールを送信されていた。SSH に使用するポートが不用意に開けてあり、かつ管理者権限ユーザアカウントのパスワードが容易に推測可能であったことが原因。

(ii) インターネットと LAN との境界に設置したサーバに侵入され、フィッシングに悪用するための Web コンテンツを勝手に設置されていた。数日間に渡って管理者権限ユーザのアカウントに対してパスワードクラッキングを受けており、その結果としてパスワードが奪取されたのが原因。

(iii) ネットワーク外部から telnet 接続へパスワードクラッキングを受けてルータなどのネットワーク機器数台に侵入され、パスワードが勝手に変更されていたり、ログ記録機能などを無効にされていたりした。ネットワーク外部からルータなどへ telnet 接続が可能になっており、かつ接続用パスワードと管理者権限パスワードが同じだったために被害が拡大した。

(iv) Web サーバの 80 番ポートに、不正なものと思われる大量のアクセスが集中したため数時間の間、外部から Web コンテンツが閲覧不能になった。特定の IP アドレスからのアクセスを制限することで復旧した。

(v) 内部および外部ネットワークから、数分間の間に数百から数千アクセスのパスワードクラッキングを受けた。侵入は許さなかったもののサーバの負荷が過大となり、サーバの処理能力が一時的に著しく低下した。

(vi)　送信した覚えの無いメールが、宛先不明のエラーで返送されて来た。メールヘッダを調査したところ、自ドメイン内のメールサーバから送信されているらしいことが判明。原因は不明。

(vii)　銀行のオンライン取引に必要な ID やパスワードが不正に奪取され、預金が勝手に他の口座へ送金された。キーロガーと呼ばれるタイプのスパイウェアを埋め込まれていたのが原因。さらに、Web ブラウザの設定が勝手に変更されたり、保存していたファイルが破壊されていたりもした。

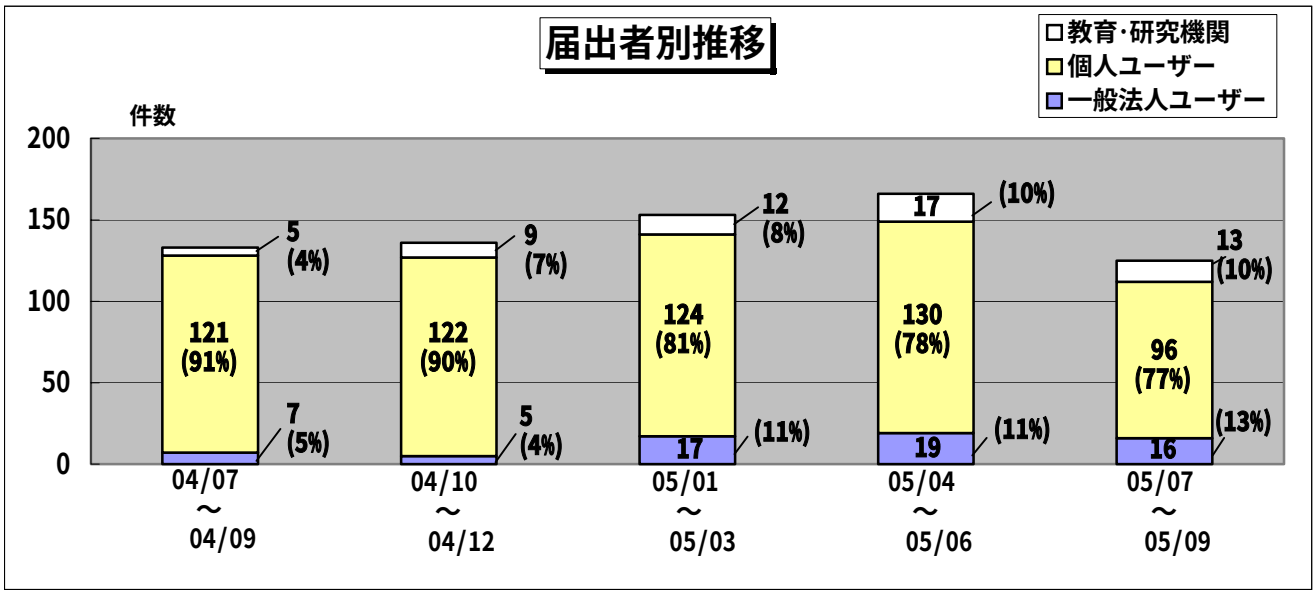
(viii)　メール送受信に支障が出たりウイルス対策ソフトの動作が異常になったりするなどの状況に陥った。パケットモニタリングソフトで調査したところ、送信パケットが不自然に多く出ていることが判明。スパイウェア対策ソフトを導入してスキャンしたところ、数種の不正なプログラムが検出された。

(ix)　ファイアウォールソフトが不正プログラムによる攻撃を遮断したためログを調べてみたところ、自身のコンピュータが数種の不正プログラムを埋め込まれており、それらが外部のコンピュータへ攻撃を仕掛けていた可能性が非常に高いことが判明。原因は不明。

(x)　アダルトサイトの年齢確認画面で「はい」をクリックしたところ、「入会ありがとうございます」などというメッセージとともに自分のメールアドレスが表示されていた。その後、数分毎に料金の請求画面が現れたり、料金支払いの督促メールが届いたりするようになった。ウイルス対策ソフトでは何も検出されない。

4.届出者の分類

届出者別の内訳は、**個人が約 77%**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