

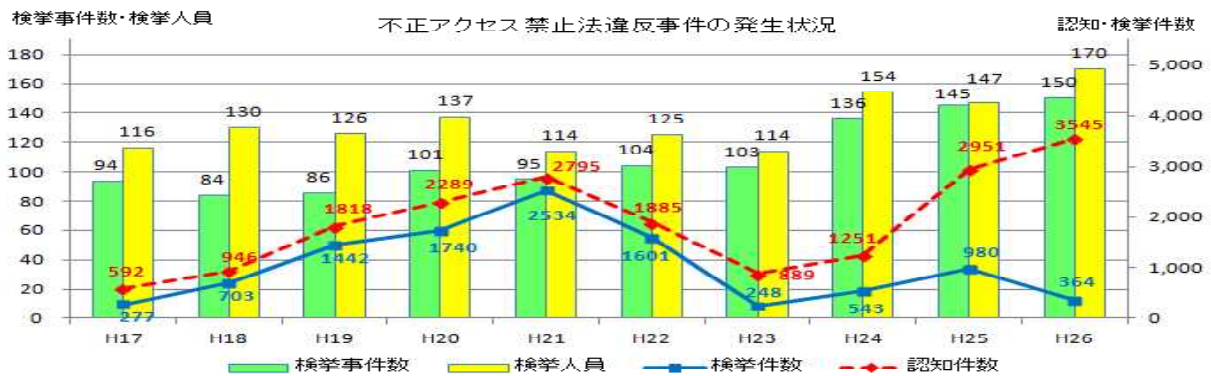
平成26年中の不正アクセス行為の発生状況等の公表について

不正アクセス行為の禁止等に関する法律に基づき、毎年、不正アクセス行為の発生状況等を公表するもの

1 不正アクセス行為の認知・検挙状況等（公表要旨）

(1) 認知・検挙状況

- 認知件数3,545件（前年比+594件）、検挙件数364件(-616件)
- 検挙人員170人(+23人)、検挙事件数150件（+5件）



(2) 認知・検挙事案の特徴

ア 不正アクセス行為後の行為

認知に係る不正アクセス行為後の行為は、インターネットバンキングの不正送金が1,944件（54.8%）と最も多く、次いで他人へのなりすましが1,009件（28.5%）となっている。

イ 不正アクセス行為の手口

検挙した不正アクセス行為の手口は、利用権者のパスワードの設定・管理の甘さにつけ込んだものが84件（24.9%）と最も多く、次いでフィッシングサイトにより入手したものが71件（21.0%）となっている。

(参考) 連続自動入力プログラムによる不正ログイン攻撃の状況

「連続自動入力プログラムによる不正ログイン攻撃」によるログイン行為が約80万件

(3) 防御上の留意事項

ア 利用権者の講ずべき措置

- ・ 使い回しをしない、推測が容易なものを避けるなど、ID・パスワードの適切な設定・管理
- ・ 金融機関等を装ったフィッシングメールに注意
- ・ ウイルス対策ソフトの利用、各種ソフトウェアのアップデート

イ アクセス管理者等の講ずべき措置

- ・ ワンタイムパスワード等による個人認証の強化
- ・ サーバの脆弱性の解消と監視体制の強化

2 今後の対応

- ・ インターネットバンキングに係る不正送金事犯等の組織的犯罪及び悪質中継サーバ等犯罪インフラの積極的な取締り
- ・ 一般財団法人日本サイバー犯罪対策センター（JC3）と連携し、産学官の情報共有を推進
- ・ 警察庁ホームページ、パンフレット等を活用し、ID等の使い回しの危険性等の不正アクセス防止対策に関する広報啓発を推進