広　報　資　料
平成24年３月15日
警　　察　　庁

平成23年中の不正アクセス行為の発生状況等の公表について

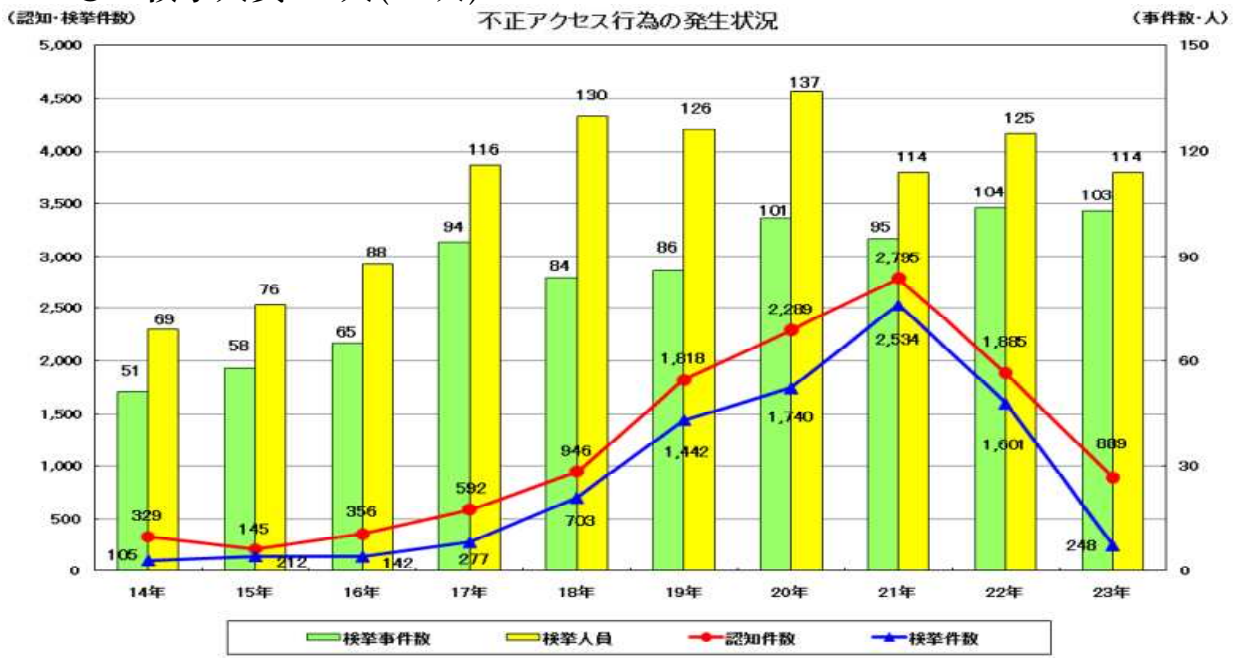
１　公表の根拠

不正アクセス行為の禁止等に関する法律第７条第１項の規定に基づき、不正アクセス行為の発生状況及びアクセス制御機能に関する技術の研究開発の状況を国家公安委員会、総務大臣及び経済産業大臣が公表するもの。

２　不正アクセス行為の発生状況等

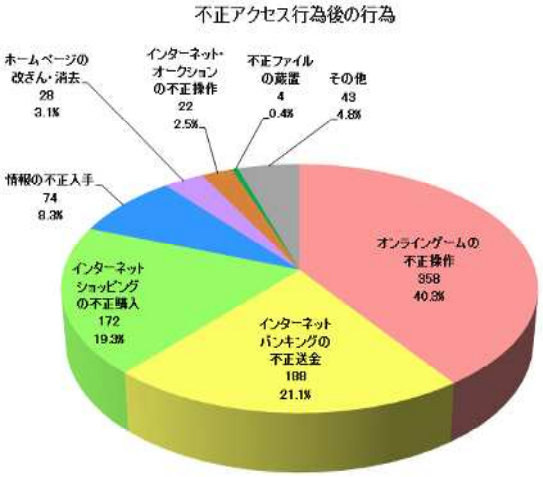
(1)　認知・検挙状況［１～６頁］

○　認知件数889件 (前年比-996件)
○　検挙件数248件 (-1,353件)
○　検挙事件数103事件 (-1事件)
○　検挙人員114人 (-11人)



(2)　不正アクセス行為後の行為

○　オンラインゲームの不正操作が358件(認知件数全体の40.3%)
○　インターネットバンキングの不正送金が188件(21.1%)
○　インターネットショッピングの不正購入が172件(19.3%)
○　情報の不正入手[注1]が74件(8.3%)



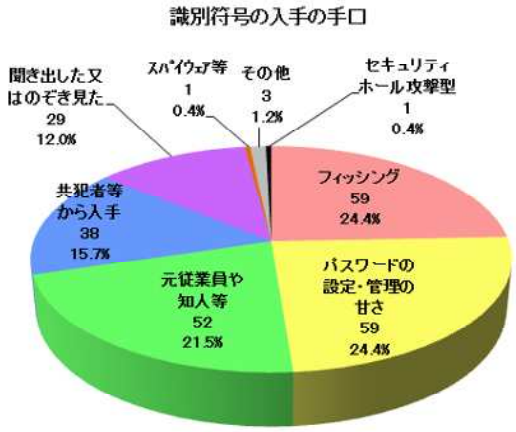
注１　登録されているクレジットカード番号や個人情報を不正に取得する行為

(3)　識別符号の入手の手口

○　フィッシングサイトにより入手したものが59件(検挙件数の24.4%)

○　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59件(24.4%)

○　識別符号を知り得る立場にあった元従業員や知人等によるものが52件(21.5%)



(4)　不正アクセス防御上の留意事項［６～９頁］

ア　利用権者の講ずべき措置

○　フィッシング被害防止のため、安易に個人情報を入力しないなどの個人情報の適正な取扱い。

○　推測が容易なパスワードを避けるとともに定期的に変更するなどパスワードの適切な設定・管理。

○　ウイルス対策ソフトウェアの利用及び随時更新。

イ　アクセス管理者の講ずべき措置

○　ワンタイムパスワード[注2]等による個人認証の強化。

○　定期的にパスワードの変更を促す仕組み等の構築。

○　元従業員の識別符号を削除するなどの適切な管理の徹底。

○　ＳＱＬインジェクション[注3]被害防止のためのプログラムの点検。

注２　インターネット銀行等における認証用のパスワードであって、認証の度にそれを構成する文字列が変わるものをいう。

注３　ＳＱＬというプログラム言語を用いて、企業等が個人情報を管理するデータベースを外部から不正に操作する行為をいう。

３　不正アクセス関連行為の関係団体への届出状況について［10～19頁］（経済産業省担当部分）

４　アクセス制御機能に関する技術の研究開発の状況［20～44頁］（総務省担当部分）

５　警察の今後の対応

(1)　被害通報の促進

不正アクセス行為を認知した場合の通報を促進するとともに、全国における不正アクセス行為等の発生状況を集約・分析し、事案の規模・内容に即した都道府県警察間の合同・共同捜査等により、効率的、効果的な捜査を推進する。

(2)　広報啓発活動の推進

「不正アクセス防止対策に関する行動計画」に基づき、情報セキュリティ関連企業・団体等と連携して、不正アクセス行為やＩＤ・パスワードの使い回しについての注意喚起や対策の周知を行うとともに、警察庁ホームページ、パンフレット等を活用した広報啓発を推進する。

※　ここ数年、ＩＤ・パスワードが使い回しされている状況につけ込んだ「連続自動入力プログラムによる不正ログイン攻撃」が発生している（別紙参照）。

(3)　フィッシング等の処罰化

フィッシング等により他人の識別符号を不正に取得する行為が多発していることから、フィッシング行為やＩＤ・パスワードの不正取得の禁止・処罰化等を含む不正アクセス禁止法の改正案を今国会に上程している。

別紙

連続自動入力プログラムによる不正ログイン攻撃の観測結果について

１　観測の実施

不正アクセス行為の防止対策について検討するため、平成23年９月からインターネットで各種サービスを提供する企業に対しヒアリングを実施したところ、うち数社が「連続自動入力プログラムによる不正ログイン攻撃(*1)」を受けていることが判明した。

そこで、同攻撃の実態を把握するため、インターネットで各種サービスを提供する企業（インターネットショッピング、オンラインゲーム、金融、コミュニティサイトの各分野）13社の協力を得て、本年２月を対象に観測を実施した。

*1　インターネット利用者の多くが複数サイトで同一のＩＤ・パスワードを使い回ししている状況に目を付け、不正取得した他人のＩＤ・パスワードのリストを悪用して、連続自動入力プログラムを用いてＩＤ・パスワードを入力し、不正アクセス行為を敢行する手口の攻撃を言う。

２　観測結果

観測結果は次のとおりであった。

協力企業数	のべログイン試行回数(*2)	のべ不正アクセス回数(*2)	侵入率
13社	260,896回	17,514回	6.7%

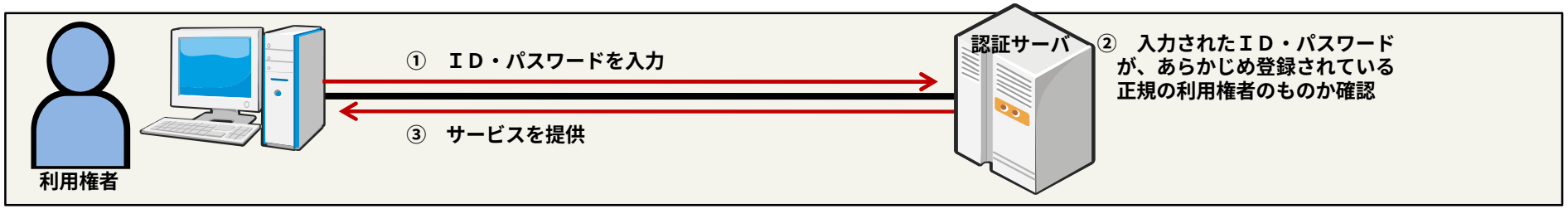
*2　「のべログイン試行回数」は、①同一のＩＰアドレスから②短時間の間に③多数のＩＤ・パスワードを入力された等の基準により、各企業が連続自動入力プログラムによる不正ログイン攻撃であると独自に認めたもので、「のべ不正アクセス回数」に正規利用権者が行った正当なログインが含まれている可能性は理論的には排除できない。

３　警察への通報

この攻撃によるログインが成功した場合、企業では、みかけ上正規のＩＤ・パスワードを使用したログインとして処理されること、また当該ログインはＩＤ・パスワードの利用可能性を確認するだけでその時点では実害を伴わないケースが多い等の理由により、これまで警察への通報はほとんどされていない。

■ アクセス制御機能による利用権者認証の仕組み

アクセス制御機能：　コンピュータの管理者が、利用権者にID・パスワードを入力させて、コンピュータ利用権の有無を自動的に識別するためのプログラム。



■ 連続自動入力プログラムによる不正ログイン攻撃

インターネット利用者の多くが複数サイトで同一のＩＤ・パスワードを使い回ししている状況に目を付け、不正取得した他人のID・パスワードのリストを悪用して、連続自動入力プログラムを用いてID・パスワードを入力し、不正アクセス行為を敢行する手口の攻撃。