

資料2

平成23年 9月

「不正アクセス行為の防止対策に関する行動計画」(骨子案)

1 前文概略

(適正な実態把握)

不正アクセス行為は、アクセス管理者が当該行為による被害を自ら把握することが難しいことや金銭的な被害が発生しない場合には警察、独立行政法人情報処理推進機構(IPA)等にあえて相談しないことなどから、潜在化する傾向にある。その結果、不正アクセス行為に関し、適正な危機意識の形成が阻害されるとともに、対応策の実施が遅れるという問題を惹起している。これらの問題を解決するためには、潜在化する傾向にある不正アクセス行為の実態を適正に把握することが第一の課題である。

適正な実態の把握のため、不正アクセス行為の発生件数の把握(量的把握)と不正アクセス行為の手口の把握(質的把握)の観点から取組を推進する必要がある。

(効果的な普及啓発)

適正な実態把握に基づき、普及啓発により、社会全体が適正な危機意識を形成し、自律的防御を図ることが第二の課題である。

不正アクセス行為を始めとするサイバー犯罪等に関する普及啓発については、これまでも継続実施されてきたところであるが、今後は、適切な普及啓発内容の選定、既存の普及啓発資料の相互利用、実施主体の連携等を通じ、普及啓発の対象に見合ったより効果的なものとしていく必要がある。また、日進月歩の情報通信技術の動向に社会全体が追い付いていけるよう、タイムリーな情報提供を推進する必要がある。

(的確な取締り・防御措置)

適正な実態把握に基づき、不正アクセス行為に対処するため、的確な取締り・防御措置を強化することが第三の課題である。

現在、不正アクセス行為の手段となるID・パスワードの詐取は、フィッシングによるものが代表例であることから、フィッシング対策を強化する必要がある。また、フィッシング対策のみならず、不正ログインを防止するため、アクセス管理者による対策を推進するとともに、取締りを強化する必要がある。さらに、防御措置の高度化、とりわけ攻撃の対象となるウェブサイト等のぜい弱性の対策を推進する必要がある。

2 社会全体として取り組むべき施策

(1) 適正な実態把握のために必要な施策

次の二つを目標に、以下の施策を実施し、不正アクセス行為の実態の適正な把握を図る。

不正アクセス行為の発生件数の把握(量的把握)

不正アクセス行為の手口の把握(質的把握)

ア 不正アクセス行為の発生件数の把握

不正アクセス行為の増減や発信地域を把握するため、認知・通報件数等の集約を行う。

(ア) 多面的把握

警察、IPA、サイバー犯罪警戒防止事業者等が保有する不正アクセス行為についての情報を集約分析することにより、不正アクセス行為の発生件数を推測・把握する。

(イ) 警察の統計による把握

不正アクセス行為認知時における警察への通報を促進し、認知件数によって不正アクセス行為の発生件数をより正確に把握する。

イ 不正アクセス行為の手口の把握

不正アクセス行為の手口を把握するため、同行為の態様、被害状況等の分析を行う。

(ア) ウェブサイトの管理者その他アクセス管理者による不正アクセス行為の適正な認知

アクセス管理者に対し、不正アクセス行為の事実を簡易に確認するツールの活用を促し、不正アクセス行為の認知件数を高めるための改善を行う。

(イ) 対応マニュアル作成による不正アクセス行為認知時の対応方針の明確化

警察、IPA、JPCERT/CC等の届出等受理機関は、不正アクセス行為の届出等受理時における対応マニュアル等の資料を共同作成し、お互いの対応手順を明確化する。

(ウ) 不正アクセス行為レポートの作成・公表

届出等受理機関は、それぞれが受理した不正アクセス行為の内容を分析し手口を把握するとともに、時々々の傾向等について他の機関と定期的に情報交換を行い、届出者固有の情報を匿名化した上で、レポートを作成、公表する。

(2) 効果的な普及啓発のために必要な施策

次の普及啓発を通じて、不正アクセス行為に関する社会全体の適正な危機意識を形成し、不正アクセス行為に対する自律的防御を図る。

ア 普及啓発内容の斉一化

普及啓発の対象に見合った的確な内容で活動を行うため、IPAやNISC、総務省の情報セキュリティの普及啓発に係るポータルサイトの充実、既存の情報セキュリティの普及啓発のための資料の相互利用等を図る。

イ 有機的かつ重層的な普及啓発

NISC、警察庁、総務省、経済産業省等の政府機関、IPAを始めとした情報セキュリティ関連事業者・団体等は、2011年に情報セキュリティ政策会議が策定した「情報セキュリティ2011」に沿って有機的に連携しながら、成長の過程にある子どもやその保護者、インターネット利用者、企業経営者等のあらゆる啓発対象に対し、学校教育活動、企業内研修、情報セキュリティ講習会等のあらゆる機会を通じて一人一人の啓発対象が情報セキュリティについて重層的に学ぶことができるよう、有機的かつ重層的な普及啓発活動を推進する。また、その際には、

不正アクセス行為の適正な実態把握に資するよう、不正アクセス行為の被害に遭った場合の対応方法等についても周知活動を推進する。

ウ 最新の技術動向を踏まえた的確な情報提供

スマートフォン等の情報端末やソーシャル・ネットワーク・サービス等の最新の情報通信技術を悪用した犯罪等の身近な脅威について、NISC、警察庁、総務省、経済産業省等の政府機関、IPA、JPCERT/CCを始めとした情報セキュリティ関連事業者・団体等は、事例等の情報提供に向けた取組を推進する。

(3) 不正アクセス行為等への対処のために必要な施策

的確な取締り・防御措置その他必要な施策を実施し、不正アクセス行為等への対処を図る。

ア フィッシング対策の推進

不正アクセス行為の手段となるフィッシングに対処するため、JPCERT/CCによるフィッシングサイトの閉鎖等の取組を推進するとともに、利用者への啓発、技術的な対応策及び法的措置の検討を含め、新たなフィッシング対策の在り方について検討する。

イ 不正ログイン対策の推進

自動入力プログラムを用いたID・パスワードの連続入力による不正アクセス行為の取締り及びID・パスワードのリストの不正流通への対策を強化する。また、乱数表やワンタイムパスワード等の導入等、アクセス管理者による不正ログイン対策の取組を推進する。

ウ セキュリティ・ホール攻撃対策等アクセス管理者による技術的なセキュリティ対策の推進

経済産業省告示「ソフトウェア等脆弱性関連情報取扱基準」に基づくIPAやJPCERT/CCを通じたソフトウェア製品及びウェブサイトのセキュリティ・ホール攻撃対策の取組等、アクセス管理者による技術的なセキュリティ対策の取組を推進する。

(4) 施策の効果検証

(1)から(3)に掲げた施策について、適切な評価指標を基に施策の効果を検証し、必要に応じ、見直し等所要の改善を図る。

3 達成目標

不正アクセス行為の防止に関し、不正アクセス行為の発生件数等の実態を適正に把握した上で、効果的な普及啓発活動や的確な取締り・防御措置の実施を通じて、不正アクセス行為の発生件数の減少を図る。