不正アクセス禁止法改正Ｑ＆Ａ

平成24年３月、第180回国会において、不正アクセス禁止法が改正され、同年５月１日から改正法が施行されますが、改正内容等に関してよくある御質問とそれに対する回答を一問一答形式で掲載いたします。

Ｑ１　今回の改正の背景と改正概要について教えてください。

Ａ　　今回の改正の背景としては、サイバー犯罪の危険性が急速に増大しており、その対策の根幹として不正アクセス防止対策を強化することが喫緊の課題となっていたことが挙げられます。

(1)　サイバー犯罪情勢と不正アクセス防止対策

最近のサイバー犯罪の情勢は、インターネットバンキングに対する不正送金事案、大手防衛産業関連企業や衆・参両院に対するサイバー攻撃等の重大事件が発生するなど、サイバー犯罪の危険性が急速に増大していました。

不正アクセス行為は、他人のＩＤ・パスワードが第三者の手に渡ってしまえば、技術的にこれを防止することは極めて困難なものであり、そうした不正アクセス行為を防ぐためには、他人のＩＤ・パスワードの不正流通を防止するほかありません。加えて、不正アクセス行為の対策に当たっては、取締りによる抑止力のみに頼るのではなく、コンピュータ・ネットワークの参加者それぞれが、それぞれの立場で不正アクセス行為の防止を図るための取組を行う必要があるところ、その取組が必ずしも十分行われているとは言い難い状況となっていました。

(2)　改正概要

そこで、他人のＩＤ・パスワードの不正流通を防止し、不正アクセス行為禁止の実効性を確保するための規制の強化と、不正アクセス行為からの防御対策を向上させるための情報セキュリティ関連事業者団体に対する新たな援助を規定することとしたものです。

不 正 ア ク セ ス 禁 止 法 改 正 の 概 要

◆不正アクセス禁止法の考え方

目的：サイバー犯罪の防止・電気通信に関する秩序の維持

取締面、防御面の両方向からの対策が必要

取締対策面

・ 不正アクセス行為の禁止・処罰
※ 不正アクセス行為： 他人のＩＤ・パスワードを悪用したり、コンピュータ・プログラムの不備を衝くことにより本来アクセスする権限のないコンピュータ（サーバ）を利用する行為

→ 詐欺、個人情報の漏えい等を早い段階で予防

防御対策面

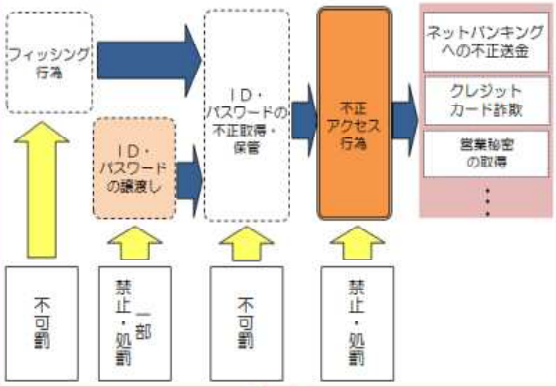
企業の努力義務
○ 防御機能の有効性の検証
○ 防御制御機能の高度化

国による援助
・ 不正アクセス行為に関する統計
・ 技術の研究開発状況等の公表

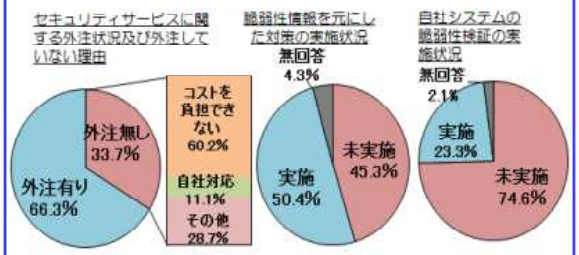
→ 防御力を向上させて不正アクセスを防ぐ

◆改正前

○ フィッシング行為、ＩＤ・パスワードの譲渡しにより、他人のＩＤ・パスワードが不正流通
○ ＩＤ・パスワードが不正流通することで不正アクセスが行われ、各種犯罪につながっている



○ 情報通信技術について専門的知識がなく、資金の制約等から情報セキュリティについて外注もできないアクセス管理者が多い
○ 自社システムの脆弱性の検証すら実施できていないアクセス管理者が存在



不正アクセス行為対策等の実態調査（平成24年２月警察庁）

→ **企業による防御措置が十分に講じられていない状況**

ＩＤ・パスワードの不正流通を防止するための規制強化が必要

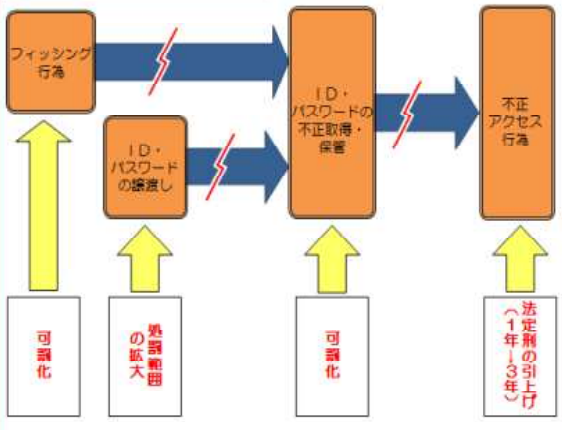
企業が努力義務を果たすための新たな環境整備が必要

取締対策の強化

防御対策の強化

◆改正後

規制の強化



防御措置の向上

情報セキュリティ関連事業者団体
（例）
・日本セキュリティオペレーション事業者協議会
・フィッシング対策協議会

国による新たな援助
○ 不正アクセス行為の手口や発生の実態に関する個別具体的な情報の提供
○ 不正アクセス行為の実態を踏まえた
・アクセス制御機能の有効性の検証
・アクセス制御機能の高度化
の在り方に関する助言 等

◆援助を受けた団体の自主的活動

アクセス管理者向けの
・アクセス制御機能の有効性の具体的な検証手段の提示
・事業の規模や性質に応じたアクセス制御機能の最適な高度化モデルつくりの支援

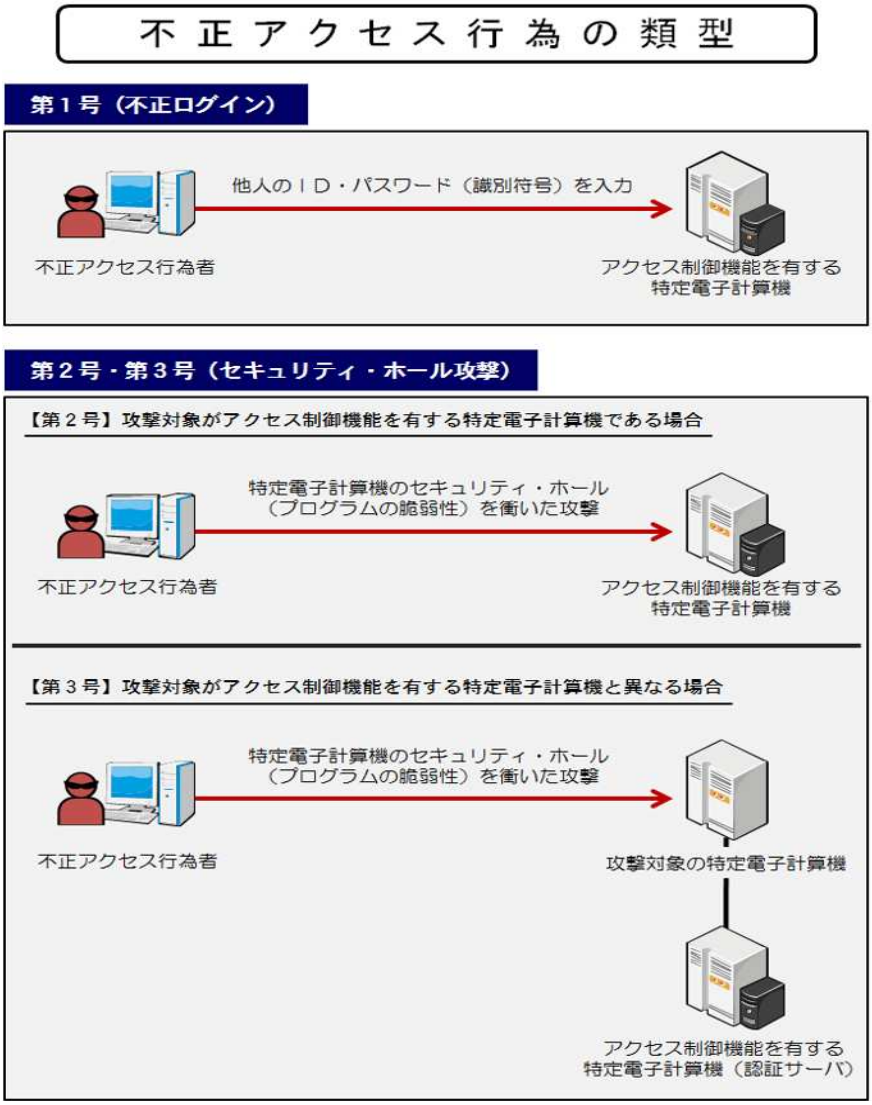
◆アクセス管理者による防御措置の向上

上記の取組を通じて、アクセス管理者が努力義務を果たすための環境整備

→ アクセス管理者による防御措置が向上

Ｑ２　そもそも、不正アクセス行為とはどのような行為をいうのですか。

Ａ　　不正アクセス行為とは、他人のＩＤ・パスワードを悪用したり、コンピュータプログラムの不備を衝くことにより、本来アクセスする権限のないコンピュータを利用する行為のことをいい、一般的に、前者は「不正ログイン」、後者は「セキュリティ・ホール攻撃」と呼ばれます。改正前の不正アクセス行為の禁止等に関する法律(以下「旧法」という。)では、不正アクセス行為を行った者の法定刑は１年以下の懲役又は50万円以下の罰金とされていましたが、改正法により３年以下の懲役又は100万円以下の罰金に法定刑が引き上げられました。



Ｑ３　改正法による規制の強化について教えてください。

Ａ　　不正アクセス行為を行うことを目的としている者が、他人のＩＤ・パスワードをひとたび手に入れてしまうと、不正アクセス行為を技術的に防止することは極めて困難であり、そのような不正アクセス行為を防止するためには、他人のＩＤ・パスワードの不正流通を防ぐほかありません。

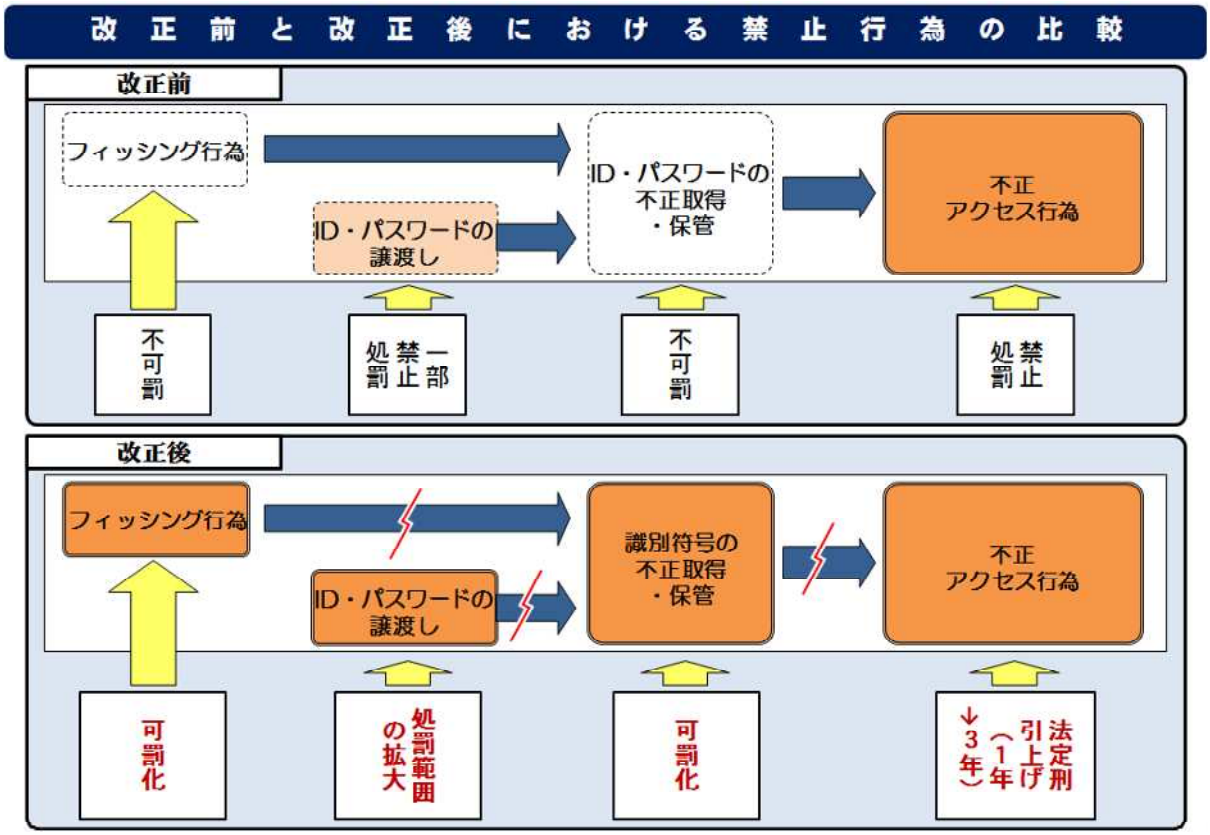
そこで、

・　フィッシング行為の禁止・処罰

・　他人のＩＤ・パスワードの不正取得行為及び不正保管行為の禁止・処罰

・　他人のＩＤ・パスワードを提供する行為の禁止・処罰範囲の拡大

により不正アクセスに至る一連の行為を規制対象にするとともに、不正アクセス罪の罰則を引き上げる改正が行われました。



Ｑ４　改正法により新設される不正取得罪(第４条)と不正保管罪(第６条)について教えてください。

A

○　不正取得罪(第４条)

改正法により、不正アクセス行為の用に供する目的で、他人の識別符号を取得する行為が禁止され、違反者は１年以下の懲役又は50万円以下の罰金が科されることとなりました。

不正取得罪の禁止対象は、「不正アクセス行為の用に供する目的」でアクセス制御機能に係る他人のＩＤ・パスワードを取得する行為となっています。不正取得罪は不正アクセス行為の禁止の実効性を確保するために新設したものであることから、処罰対象を不正アクセス行為につながる危険性がある行為に限定しているものです。

「取得」とは、ＩＤ・パスワードを自己の支配下に移す行為をいい、具体的には、ＩＤ・パスワードが記載された紙や、ＩＤ・パスワードが記録されたＵＳＢメモリ、ＩＣカード等の電磁的記録媒体を受け取る行為、自らが使用する通信端末機器の映像面にＩＤ・パスワードを表示させる行為、ＩＤ・パスワードを知得する行為（再現可能な状態で記憶する行為）等がこれに該当します。

なお、取得者には、取得することの認識が必要です。したがって、例えば、インターネット上での検索中にたまたま他人のＩＤ・パスワードが表示された場合や、他人のＩＤ・パスワードが電子メールで勝手に送りつけられてきたような場合には、取得することの認識がないことから、不正取得罪には該当しません。

○　不正保管罪(第６条)

改正法により、不正アクセス行為の用に供する目的で、不正に取得された他人の識別符号を保管する行為が禁止され、違反者は１年以下の懲役又は50万円以下の罰金が科されることとなりました。

保管罪も取得罪と同様、「不正アクセス行為の用に供する目的」で保管する行為が禁止対象となります。

保管の対象は「不正に取得された他人の識別符号(ＩＤ・パスワード)」です。「不正に取得された」とは、正当な権限なく取得されたことをいい、具体的には、第４条に該当する行為により取得されたＩＤ・パスワードや第５条に該当する行為により提供されたＩＤ・パスワードがこれに該当しますが、これに限定されるものではなく、例えば、不正アクセス行為の用に供する目的以外の別の目的で他人のＩＤ・パスワードを権限なく取得した場合、第４条の禁止対象とはなりませんが、当該ＩＤ・パスワードを不正アクセス行為の用に供する目的で保管した場合には本条に該当することとなります。

「保管」とは、有体物の所持に相当する行為であり、ＩＤ・パスワードを自己の実力支配内に置いておくことをいい、具体的には、ＩＤ・パスワードが記載された紙や、ＩＤ・パスワードが記録されたＵＳＢメモリ、ＩＣカード等の電磁的記録媒体を保有する行為、自らが使用する通信端末機器にＩＤ・パスワードを保存する行為等がこれに該当します。

なお、保管者には、保管することの認識が必要です。したがって、例えば、知らない間に他人のＩＤ・パスワードをダウンロードしていたような場合には、保管することの認識がないことから、不正保管罪には該当しません。

Ｑ５　改正法により禁止・処罰範囲が拡張される助長罪(第５条)について教えてください。

Ａ　改正前は、他人のＩＤ・パスワードを、そのＩＤ・パスワードがどのウェブサイト(のサービス)に対するＩＤ・パスワードであるかを明らかにして、又はこれを知っている者の求めに応じて、無断で第三者に提供する行為を禁止・処罰の対象としていました。

しかし、近年、一人の人間が利用するコンピュータのサービスの数が増加しており、同一のＩＤ・パスワードを多数のサイトで使い回す例が一般化しています。その結果、提供されたＩＤ・パスワードがどのウェブサイト(のサービス)に対するものかが明らかでなくとも、多数のＩＤ・パスワードを入力すれば一定程度の割合で不正ログインに成功する場合があることから、今回の改正により「業務その他正当な理由による場合」を除いて他人のＩＤ・パスワードを提供する行為が全て禁止され、違反者は１年以下の懲役又は50万円以下の罰金が科されることとなりました。

Ｑ６　改正により「業務その他正当な理由による場合」を除いて他人のＩＤ・パスワードを提供する行為が全て禁止された(第５条)ということですが、「業務その他正当な理由による場合」とはどのような場合を言うのですか。

Ａ　「業務その他正当な理由による場合」とは、社会通念上、正当と認められるような場合をいいます。例えば、

○　情報セキュリティ事業者が、インターネット上に流出しているＩＤ・パスワードのリストを契約している企業に提供する行為

○　インターネット上に流出している他人のＩＤ・パスワードを発見した者が、これを情報セキュリティ事業者や公的機関に届け出る行為

○　ＩＤ・パスワードとしてよく用いられている単純な文字列を、ＩＤ・パスワードとして設定すべきでないものとして示す行為

等は、不正アクセス行為を防止する目的で行われるものであり、「業務その他正当な理由による場合」に該当します。

また、

○　情報セキュリティに関するセミナーの資料等において、ＩＤ・パスワードのインターネット上への流出実態を示すために実際に流出したＩＤ・パスワードのリストを掲載する行為

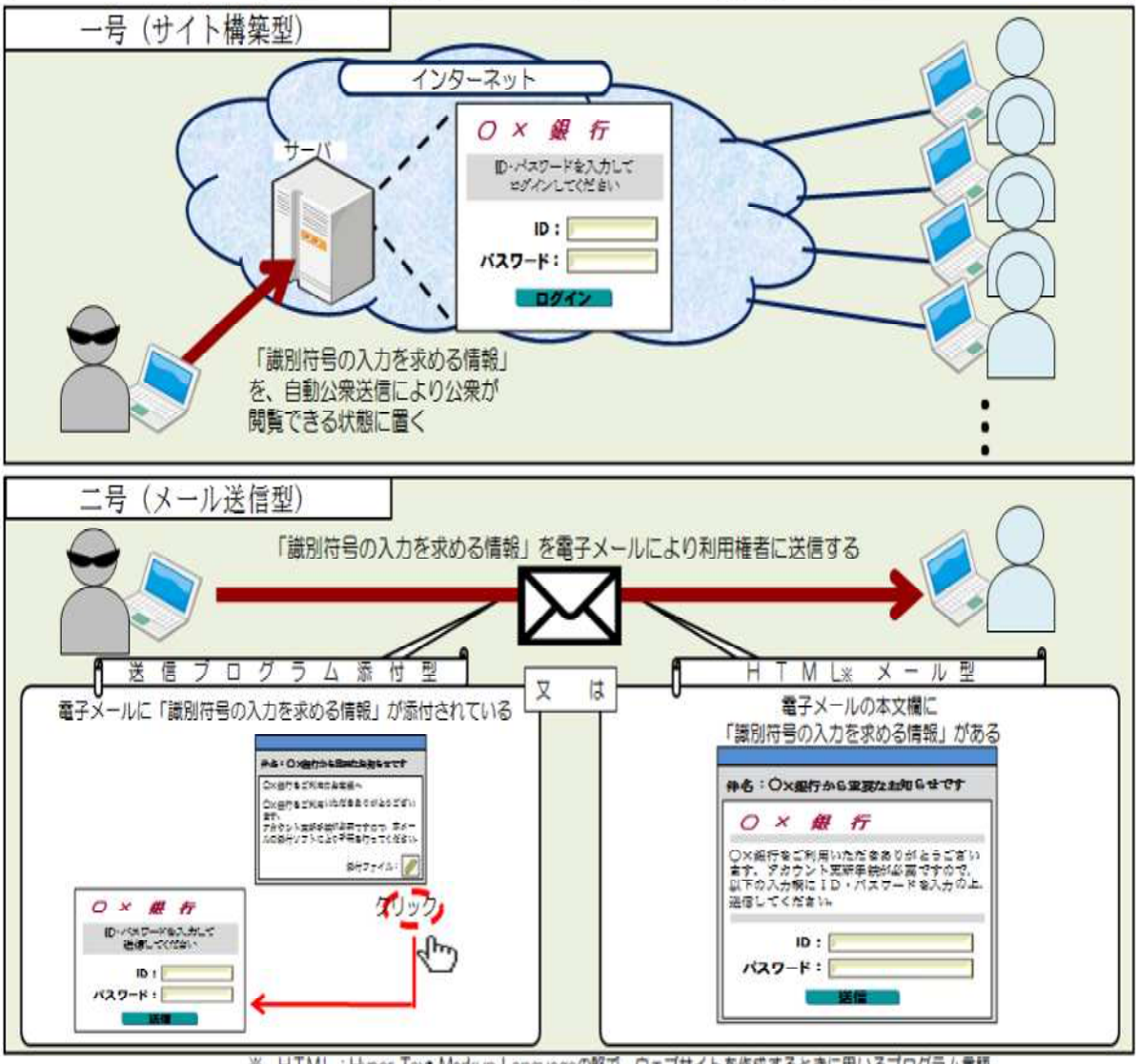
等も、流出実態の危険性を訴えることや対応策を検討することを目的に行われるものであるので「業務その他正当な理由による場合」に該当します。

Ｑ７　フィッシング行為について教えてください。

Ａ　　一般にフィッシングと呼ばれる行為は、その行為を詳細に見れば様々な形態のものがありますが、共通する特徴点は、アクセス管理者が公開したウェブサイト又はアクセス管理者が送信した電子メールであると利用権者に誤認させて、アクセス管理者がＩＤ・パスワードの入力を求める旨の情報を閲覧させようとすることにあります。そして、このような行為の結果、当該情報を閲覧した利用権者にＩＤ・パスワードを入力させてだまし取ることを企図しているものです。改正法によりフィッシング行為は禁止され、違反者は１年以下の懲役又は50万円以下の罰金が科されることとなりました。(第７条)。

本条では、第１号が、いわゆるフィッシングサイトを公開することを手口とするフィッシング行為の、第２号が、いわゆるフィッシングサイトを用いず、電子メールによってＩＤ・パスワードを詐取しようとするフィッシング行為の禁止規定となっています。

禁止・処罰するフィッシング行為の類型



※ HTML：Hyper Text Markup Languageの略で、ウェブサイトを作成するときに用いるプログラム言語。
HTMLを用いることで、メールの本文欄に入力欄や送信ボタンを設けることができる。

Ｑ８　フィッシング罪(第７条)の構成要件について教えてください。

Ａ

○　第７条第１号(サイト構築型)

第７条第１号は、フィッシングサイトを公開することを手口とするフィッシング行為を禁止している規定です。公開されたサイトが「正規のアクセス管理者が公開したウェブサイトであると誤認させるウェブサイト」であることが要件です。典型的にはアクセス管理者の名称やロゴを用いているウェブサイトがこれに該当します。

また、フィッシング行為は他人のＩＤ・パスワードを詐取するために用いられる手口ですから、当該サイトに「ＩＤ・パスワードを入力することを求める旨の情報」があることが要件となっています。典型的にはウェブサイト上にＩＤ・パスワードを入力するよう求める文章、入力欄及び送信用のボタンが表示されている場合がこれに該当します。

したがって、第７条第１号で規定している行為は、利用権者を誤認させようとする意図を持って、「正規のアクセス管理者が公開したウェブサイトであると誤認させるウェブサイト」であって「ＩＤ・パスワードを入力することを求める旨の情報」があるウェブサイトをネットワーク上に公開して公衆が見ることができる状態に置く行為ということになります。

○　第７条第２号(メール送信型)

第７条第２号は、フィッシングサイトを用いず、電子メールによってＩＤ・パスワードを詐取しようとするフィッシング行為を禁止している規定ですので、送信された電子メールが「正規のアクセス管理者が送信した電子メールであると誤認させる電子メール」であることが要件です。典型的にはアクセス管理者の名称やロゴを用いている電子メールが該当します。

また、第１号と同様に当該電子メールに「ＩＤ・パスワードを入力することを求める旨の情報」があることが要件となっています。典型的にはＨＴＭＬ（ＨＴＭＬとは、Hyper Text Markup Languageの略で、主にウェブサイトを作成するときに用いるプログラム言語です。ＨＴＭＬを用いることで、電子メールの本文欄に、ＩＤ・パスワードの入力欄や送信ボタンを設けることが可能となります。）を用いて電子メールの本文欄にＩＤ・パスワードを入力するよう求める文章、入力欄及び送信ボタンが表示されている場合がこれに該当します。

したがって、第７条第２号で規定している行為は、利用権者を誤認させようとする意図を持って、「正規のアクセス管理者が送信した電子メールであると誤認させる電子メール」であって「ＩＤ・パスワードを入力することを求める旨の情報」がある電子メールを、利用権者に送信する行為ということになります。

Ｑ９　なぜ、不正アクセス行為からの防御に関する啓発及び知識の普及に努める者に都道府県公安委員会が加えられたのですか。（第９条第５項）

Ａ　不正アクセス行為が行われにくい環境が構築されるようにするためには、アクセス管理者はもとより、ウェブサイト(のサービス)を利用することについてアクセス管理者の許諾を得た利用権者（エンドユーザ)、アクセス制御機能に関係するソフトウェアやハードウェアの製造業者などコンピュータ･ネットワークに参加し、又は関係する者がそれぞれの立場で不正アクセス行為の防御のための活動を行うことが重要です。行政は、これら関係者の活動が円滑に行われるよう各種施策を講じて支援していく必要がありますが、あらゆる分野において、老若男女を問わずにインターネット利用が拡大していること及び不正アクセス行為の手口が巧妙化・深刻化していることから、不正アクセス行為による被害を防止するためには、コンピュータ・ネットワークに参加し、又は関係する者それぞれの立場に応じてきめ細かな啓発及び知識の普及を行う必要があります。

そのような取組として、都道府県警察が、捜査を通じて蓄積した知見等を活用し、不正アクセス行為を始めとするサイバー犯罪を未然に防止し、国民の情報セキュリティに関する意識及び知識の向上を図るために、外部の有識者を情報セキュリティ・アドバイザーとして委嘱するなどした上で、一般企業、地方公共団体、学校等を対象として講習会を実施するなどの啓発及び知識の普及の活動を実施しているところであり、このような都道府県警察の活動が不正アクセス行為の防止に果たす役割の重要性に鑑み、本法において、都道府県公安委員会に不正アクセス行為からの防御に関する啓発及び知識の普及を図るべき責務があることを明記することとしたものです。

Q10　不正アクセス行為からの防御に関する啓発及び知識の普及とは具体的にはどのようなことをいうのですか。（第９条第５項）

A　「不正アクセス行為からの防御に関する啓発」とは、ネットワークに参加する一人一人に不正アクセス行為がいかにサイバー犯罪を助長し、又は電気通信の秩序を乱すものであるか、さらには我々国民に多大の便益をもたらすと期待されている高度情報通信社会の根幹を揺るがすものであるかといった社会に及ぼす害悪の大きさについての認識を促し、社会全体として不正アクセス行為からの防御措置を講ずることについての重要性の理解を深めるための活動を広く指すものです。啓発の方法に特に限定はなく、マスメディアを通じた広報、講演活動、ポスターやパンフレットの頒布、ホームページへの掲載などの方法等が考えられます。

「不正アクセス行為からの防御に関する……知識の普及」とは、不正アクセス行為やその準備行為であるフィッシング行為等の手口の紹介、これらの行為からの防御措置の紹介等を指します。

Q11　今回の改正で、国による情報セキュリティ関連事業者団体に対する情報提供の規定(第10条第２項)が新設されましたが、情報セキュリティ関連事業者団体とは具体的にはどのような団体ですか。

Ａ　具体的には、日本セキュリティオペレーション事業者協議会（ＩＳＯＧ－Ｊ）及びフィッシング対策協議会を想定しています（平成24年４月現在）。

ただし、当然これらの団体に限られるものではなく、第10条第２項に規定する要件を満たす団体には情報提供を行うことになります。団体の法人格の有無は問いませんが、本項の援助の対象となるのは事業者が集まって組織した団体であって、個々の企業や個人は援助の対象とはなりません。

Q12　情報セキュリティ関連事業者団体に対する情報提供とは、具体的にはどのようなことを行うのですか。（第10条第２項）

A　第10条第２項では、情報セキュリティ関連事業者団体に対し、「必要な情報の提供その他の援助」を行うことが努力義務とされていますが、具体的には、

○　国家公安委員会が、不正アクセス行為の具体的手口に関する最新の情報を提供すること

○　総務大臣が、総務省及び独立行政法人情報通信研究機構によるアクセス制御機能の高度化に資する研究開発の成果等の情報を提供すること

○　経済産業大臣が、独立行政法人情報処理推進機構を通じて不正アクセス行為に関する注意喚起を行うことやガイドライン策定等により対策情報を提供すること

等が考えられます。