強者の戦略

【はじめに】

第２回は「ビジネス基礎済」からの出題でしたが、受験生のみなさん、いかがだったでしょう。

今回は「インターネットのセキュリティー」に関して、みなさんの考えを記述する問題でしたが、うまくまとめることができたでしょうか。

それにしても、先月１７日、参議院特別委員会の強行採決における、与党と野党の攻防は見ていてどっちもどっちという感じがしました。与党側が自民党の女性議員に対して民主党の男性議員がセクハラ（セクシャルハラスメント）行為をしたと批判すれば、野党側も殴られたと互いに批判の応酬です。しかし、安保法案が可決されたのですから、今後、自衛隊の海外での活動について、私たち国民がその動向を注視する必要があります。

しかし、今の日本経済は株安、消費低迷など先行きが不安な状況です。そこで安倍内閣は、女性閣僚を登用する内閣改造を行い、臨時国会に挑みます。そこで、先日安倍首相が表明した「新三本の矢」の審議が行われます。

ところで、前の「三本の矢」はどうなったのでしょうか。日銀の金融政策、政府の財政出動により、株価は上昇したものの、中国経済の失速やアメリカが今年中に金利の引き上げを行うことなどが要因となって、株安と円安が起こっています。

話が逸れてしまいましたので、元に戻します。インターネットが普及して、今やインターネットでの買い物はもちろん、送金や入金などネットバンキングも次第に普及してきています。しかし、便利になった反面、さまざまな問題もあります。みなさんの中に利用されている人もいるでしょうから、今回の問題は比較的書きやすいと思いますが、いかがでしょう。

それでは、解答・解説へといきます。

【解答例】

インターネットのセキュリティーについては、パスワードを外部に知られないことが大切です。しかし、パスワードを１回だけでなく、２回や３回かけるようにしておくことが考えられますが、それでも安心はできません。そこで、一定期間が経過すると、パスワードを変更するように設定することも必要だと思います。また、利用しているパソコンに、最新のウィルス対策用ソフトをインストールし、日々、ウィルススキャンするように設定をしておくようにしておくことも大事だと思います。それと、使用するパソコンに、パスワードを記憶させないようにしておく。このようにして、パスワードを他人に知られないようにすることが第一である。

しかし、数字と文字を入力するパスワードの場合、忘れることもあり、また、機械でランダムに入力させて盗み取ることも可能である。そこで、パスワードを文字や数字ではなく、指の指紋や手のひらにすることも考えられる。（３９４字）

【解説】

１．パスワードの適切な管理

・ID・パスワードは他人に「絶対に」教えない

ID とパスワードは、インターネット上で個人を特定する、非常に重要なものである。他人に教えることなく、適切に管理する。

・他人が推測できるようなパスワードを設定しない

パスワードを、ID と同じ、生年月日や電話番号、自分の名前、好きな言葉や簡単な英単語、数字のみというものに設定していませんか？これらのパスワードは、辞書攻撃（注１）や総当たり攻撃（ブルートフォースアタック）（注２）で破られてしまうことがある。不正アクセスの被害にあってしまった人の多くは、他人に推測されやすいパスワードを設定している。パスワードは、大文字、数字、記号（@、！、－）などを混ぜ、８文字以上のできるだけ長い文字列にし、他人が推測できないものを設定する。

注１　辞書攻撃：辞書に載っている単語を、片っ端から入力していく攻撃手法

注２　総当たり攻撃（ブルートフォースアタック）：考えられる全ての文字列の組合せを、片っ端から入力していく攻撃手法

・パスワードは定期的に変更する

　長期間利用しているパスワードは破られる可能性もあるため、パスワードを定期的に変更することでセキュリティーを高めることができる。

・ID・パスワードは使いまわしたりせず、利用するサイトごとに設定をする

　複数のサイトにおいて、ID・パスワードを共通にしていると、どこか一つのサイトで不正アクセスにあってしまった場合、他のサイトにも侵入される危険性がある。

・ウィルス対策を徹底する

　ウィルスやスパイウェアによって、ID とパスワードが盗まれてしまうこともある。パスワード管理に加え、ウィルス対策もしっかりと行う。

・パスワードを忘れた時などに利用する「秘密の言葉」や、「秘密の質問に対する回答」等は、他人が推測できないものを利用する

　パスワードを忘れてしまった時のために、登録時など、あらかじめ本人しか分からない情報を登録しておき、パスワードの再発行時に、本人確認としてその情報を利用するサイトがある。しかし、この情報を他人が推測できるものに設定していると、第三者にパスワードの再発行を行われてしまう可能性もありますので、注意すること。

・ワンタイムパスワードや、第二暗証番号の利用を検討する

　サイトによっては、不正利用防止のために、ワンタイムパスワードや第二暗証番号を導入しているところがある。現在利用中のサイトが対応してれば、セキュリティーを高めるために利用するように。

・ネットカフェなど複数の人が利用するパソコンでは ID・パスワードは入力しない

　不特定多数の人が利用するパソコンには、スパイウェアやキーボードの入力を監視するキーロガー等が仕掛けられている可能性がある。このようなパソコンでは、ID とパスワードを知らないうちに盗まれてしまう可能性もあることから、ID とパスワードを必要とするサイトへアクセスすることは避ける。

２．パスワードの定期変更で守られるのはサービス提供者側のセキュリティー

　ウェブサービスを提供する側は何故セキュリティー対策としてパスワードの定期変更を促すのか。これは、利用者側のセキュリティーではなく、サービス提供者側のセキュリティーを高めるためである。ここでサービス提供者側がとっているセキュリティー対策はリスクの移転つまり責任転嫁です。セキュリティー対策はリスクへの対処方法として４つに分類される。

･リスク回避
･リスク低減
･リスク保有
･リスク移転

パスワード情報の漏洩は、利用者側もしくはサービス提供者側どちらかの落ち度で発生します。利用者側の落ち度は、サービス提供者側でコントロールできませんし、その場合にはサービス提供者側に非はありません。

一方、サービス提供者側で情報を漏洩した場合には提供者側に責任が発生します。しかし、提供者側がセキュリティー対策の努力を怠っていないと「看做され」、利用者側がセキュリティー対策を怠っていたと「看做される」場合、提供者側の責任はある程度免責されます。

利用者側にパスワードの定期的変更を求めるのは

･提供者側が利用者喚起により対策努力を怠っていないと「看做される」ため

･利用者側が喚起無視により対策努力を怠っていたと「看做される」ため

に必要な要件になるからです。これは、利用者側へのリスク移転となります。つまり、パスワードの定

期変更はセキュリティー対策ではあるけど、利用者のセキュリティーを高める対策ではない、提供者のセキュリティーを高めるために利用者のセキュリティーを下げる対策です。

パスワードの定期更新は安全どころか、むしろ危険な行為です。サービス提供者はセキュリティー対策としてパスワードの定期更新を促すべきではなく、二段階認証といったシステムを導入することに力を入れるべきであると考えます。もちろん二段階認証を予算やコールバックのための個人情報の保管条件によって導入できない場合もあるとおもいますが、その場合でも、利用者側がパスワードを定期的に変更しないことをもって提供者側の非を免責するべきではない。

３．指紋認証のセキュリティー

パスワードよりもセキュリティーとしては安全性が高いといわれているが、本当にそうであるのか。インターネットではないが、指紋認証が盗まれた事例がある。

ドイツ・ベルリンのハッカー集団「Chaos Computer Club」が、指紋の情報を盗み、iPhone を解除するために指紋を再生成することが可能であることを証明した。それによると、まず 2400dpi の解像度のカメラで撮影した写真 1200dpi で出力。それからラテックス（樹脂）製の指紋の"マスク"を作り iPhone を解除する方法である。

この方法は技術的には不可能ではないが、かなり面倒である。普通に考えて、誰かの指紋を盗んでセキュリティーの抜け穴をくぐるのは、そう簡単なことではない。

このように、パスワードに比べて指紋認証の方が安全性は高いが、絶対ではないということである。いずれにせよ、一人一人がインターネットを使用するときに、安全性を意識することが大切である。

みなさんも、個人情報を盗みと取られないように、日頃から意識しておきましょう。