JOHO SYSTEM SINKAI

情報通

2007. June 6月号
発行日：平成19年6月1日
発　行：東京税理士会
　　情報システム委員会
題　字：金井塚　清（豊島）

悪意も進化していたWebサイト

－ＩＤ・パスワードに加えＩＣカード型電子証明書を使うわけ－

最近ではもはや当たり前ということなのか、Web2.0とかロングテールとかという言葉の露出度は低くなって来たようなきがしますが本紙情報通欄では昨年の12月号でこの辺の事情を取り上げました。「新聞はもういいですから、ヤフーに載るように記事を書いて!」と言われた始めた既存メディアの記者さんからの記事でしたが、それほどにインターネットの利便性が浸透してきたという内容でした。しかし冷静に振り返ってみると物事には肯定的な側面と、反面ネガティブな要素も併せ持つものだという、まことに当然のことで、今月号の情報通では、実は、インターネットの世界の裏側では悪意のある勢力が表側と同様にしっかり進化していて、それにどう対処すべきか、電子申告の実践が次第に広がりを見せてきた今、認定認証局として豊かな実績を誇る日本電子認証㈱社の技術者様より税理士向けに示唆に富むお話しをいただきました。

1. あなたのIDパスワードは安全ですか?

皆さんはインターネット上の様々なサービス、及び有料サイト等でIDパスワードを利用されていることと思います。

ちょっと、ここで振り返ってみてください。公開している自分のWebホームページが改竄されてしまった、或いは、会員制サービスで覚えのない利用履歴があった等の経験はありませんか?

これらは、もしかすると他人があなたのパスワードを盗んで「なりすまし」されている可能性があります。利用しているサービス内容によっては、利用されても本人、又は他人への影響はないものもありますし気が付かないことも考えられます。しかし関係者しか知らない情報が流出したとなると管理責任を問われる可能性も否定できません。

最近では急速なインフラ普及と発展により、様々な場所からインターネットが利用できるようになってきましたが、同時に多種多様な脅威も生まれています。情報漏洩のしくみとして、パソコン内に仕込まれるもの（スパイウェア）や、ファイルに感染して知らずに付いてくるもの（ウィルスメール）、疑似Webサイトで待ちかまえているもの（フィッシング）、或いは電子メールで怪しいサイトへ誘うもの（トラップメール）等、方式も数多くあります。

これら悪意を持ってパソコン上の情報を盗むしくみは非常に巧妙化してきており、最近のWeb2.0と呼ばれるJava言語を利用した技術では、Webサイトへのログイン情報となるクッキー情報を電子メールを利用して盗み出し、これを自分のWebブラウザに登録してIDパスワード情報を知らずとも、本人になりすましてWebサイトにログインできてしまうような方法も出てきています。

さてIDパスワードのことですが、IDパスワードは個人だけでなく、組織への発行もあります。その場合、組織内部ではIDパスワードを複数メンバで共有して運用することが良くあります。また、利便性を優先して、更にメンバ外の会社の上司、部下、協力会社の社員等の自分にとっての関係者に伝えられることもしばしばです。こうなると、内部情報が流出した場合、責任の所在が不明確になるのは必至です。パスワードの漏洩を防ぐために、パスワードを頻繁に変えるとういうことも必要となりますが、色々なシステムで様々なパスワード設定している等の理由から、忘れないように付箋紙やパソコンのメモ画面等に書き留めるような状態となっては意味がありません。机の上を含むパソコン周りの情報は社外の人（掃除業者、保守作業員等）にも晒されている可能性があります。ケータイのデジカメ等で容易にコピーされてしまいますので。

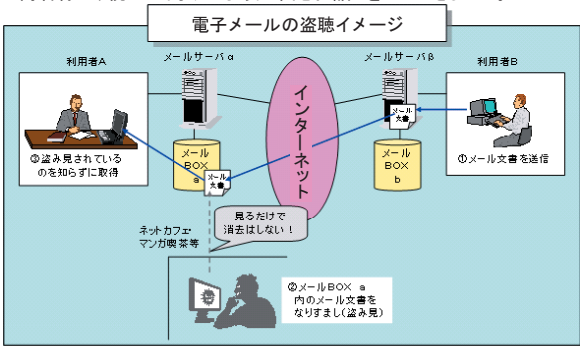
2. 電子メールのIDパスワードが盗難にあった場合

IDパスワードの盗難で一番気づき難いサービスの1つに電子メールがあります。仮に、電子メールのIDパスワードが盗難（及び流出）にあった場合を想定してみましょう。

例えば、あなたのIDパスワードが盗難に遭った場合、あなたになりすまして、電子メールBOX（＝電子メールサーバ）上のメールデータを消さずに残したまま、頻繁にメールデータを参照（なりすまし盗聴）していることが考えられます。あなたは、盗聴されているのを気づかずに、電子メールBOX上のメールデータを自分のパソコンにダウンロードし、通常通り操作を続けてしまいます。

あなたの電子メールBOXの情報が盗聴されている場合、あなたと情報交換をしている相手全員との大切な情報が流出している危険があります（自分の個人情報だけでなく、他人の情報漏洩まで行っている可能性がある）。なお、自分側の電子メールBOX、相手側の電子メールBOXどちらからの盗聴の危険もありますので、お互いに注意が必要です。したがって、お互いに、少なくとも管理者不明のフリーメール等は利用せず、安全な電子メールサービスを利用しましょう。推測し易いパスワード設定は避け、定期的に変更するのも大切です。

また、ネットカフェ、マンガ喫茶のような不特定多数の人が利用するパソコンはどんなソフトウェアが仕掛けられているとも限らないので、電子メールデータの受信等は控えたほうが無難です。



3. もし、銀行ＡＴＭがIDパスワードだったら

このような大切な情報を管理する仕組みに、IDパスワードは本人認証手段として適切なものと言えるのでしょうか?

昔は預金通帳と銀行に登録した印鑑の印影との照合だけが現金引き出しの手段でした。その後、磁気ストライプのキャッシュカードとパスワードによる照合によりATMでも現金引き出しが可能となりました。これは、窓口業務のサービス地域拡大と人件費削減を両立させた画期的なしくみですが、数字4桁のパスワードが電話番号、生年月日等の推測し易い番号であったり、磁気ストライプがスキミング装置等により一瞬で読みとられて複製されてしまうといった、簡単になりすましが可能となる決して安全とは言えない状況になってきました。そこで、キャッシュカードの複製を防ぐしくみとして、磁気ストライプからICカードへ、そして数字4桁のパスワードから指紋、掌紋認証等の本人しか持たない生体認証へと安全性を強化した経緯があります。

このような状況の中でIDパスワードを利用した現金引き出しの仕組みが想定できるでしょうか?つまりあなたが自分の最も重要な情報をネット上にさらすことになる場合のことです。例えば家族に磁気ストライプのキャッシュカードを渡して、パスワードを教えれば本人の代わりに現金を引き出してきてもらうことが出来ます。この場合、キャッシュカードが手元に戻れば引き出されることはありません。一方IDパスワード方式である場合は、パスワードを変えない限り、引き続き現金を引き出すことが可能となってしまいます。

これらの状況をインターネット上のサービスに適用してみると、特にユーザIDに電子メールアドレスを利用するようなサービスでは、パスワードを推測されて、なりすまし利用されることに成りかねませんので、パスワード管理には十分な注意が必要です。結局のところ今や、IDパスワードだけでは安全を確保できなくなってきたと言えるのではないでしょうか。そこで・・・

4. 電子証明書とICカードの強力タッグ

つい先日まで、相手との情報交換には電話とFAXが主流でしたが、これからはスピードと情報量、及び同報性を生かして、普及が高まってきたインターネットを利用したしくみが主役になってくるでしょう。実際に利用頻度から見ると電話、FAXを利用する回数よりも電子メールを読んだり、送信したりする回数の方が多い人も大勢いるはずです。携帯電話でさえも電話としての機能よりもメールの送受信やWebサイトの参照、及びダウンロード機能といったインターネット上のサービスを利用する機会の方が多いという統計があります。

今後はインターネットを利用して、更に重要な情報をやりとりするようなケースが増加するでしょう。その際に気を付けなければならないのが本人認証のしくみです。

携帯電話の場合は、iモード内のコンテンツを利用する際はNTTドコモ等の通信キャリアが間に入って、携帯電話機本体と利用者本人（又は法人）を結びつけており、端末識別情報を利用した確実な本人認証を実現しています。

左頁から

iモード以外のコンテンツ、或いはパソコンでインターネット上のサービスを利用する場合はどうでしょう?パソコンを購入する際には、運転免許証や健康保険証等の提示は必要ありませんので、パソコン本体と利用者本人を結びつけることはできませんし、オフィスや自宅だけでなく街中でも様々な環境に設置されていますので、誰がパソコンを利用しているのかは全く判りません。

したがって、インターネット上のサービスを利用する際に、サービス提供者と利用者間で直接的に本人認証のしくみが必要となりますが、前述した通り、重要な情報をやり取りするようなサービスでは、IDパスワードによる方式だと不安が残ります。

IDパスワードはサービス提供者側が管理しているものなので、本人が気づかないところでなりすましされ、利用されてしまうといったリスクもあります。

そこで、利用者本人しか持たない情報で本人認証できるよう、印鑑証明書を電子的に活用するしくみである電子証明書による本人認証方式が考案されました。

電子証明書の機能を利用する際は、パスワードの代わりにPIN（Personal Identification Number）コードを入力する必要があります。これは、秘密鍵を利用する処理（データの暗号化、複合化、署名付与等）を行う場合に、利用許可コードとして利用されます。

PINコードはサービス提供者側ではなく、利用者自身で管理する情報であるため電子証明書を持っている本人でなければ、PINコードを入力することが出来ません。

また、認定認証局の発行する電子証明書では、電子証明書上の一番大切な情報である秘密鍵のコピー、盗難を防止するために、銀行のキャッシュカード等と同様、物理的なID管理としてICカードに格納する方法が普及してきています。

ICカード型電子証明書の場合、紛失や盗難に遭った場合でも気づいた時点で電子証明書の失効処理を行うことにより、インターネット上のサービス等をなりすまし利用される前に未然に防ぐことが可能となります。また、ICカード型電子証明書は貸しても、コピーすることはできませんので、借用者を特定することができますし、返して貰えれば、借用者は電子証明書を利用することはできなくなるので、安心することができます。

なお、ICカードには閉塞機能を持つものも多く、ICカードを盗みPINコードを探り当てようとランダムな英数字を入力してもICカード自体がロックしてしまい、PINコード入力を受け付けなくなり、電子証明書のなりすまし利用を防ぐことができます。

ちなみに、弊社(日本電子認証㈱)の認定認証を取得しているAOSignサービスでは、ICカードのPIN入力誤りを連続10回迄としています。

5. 安心・安全なサービス利用

インターネット上のサービスは玉石混淆の状態と言って良いでしょう。機能の豊富さ、料金の安さをアピールするサービスは多々ありますが、価格だけでなく、セキュリティ面、サポート面、システムの信頼性、運用体制等総合的な評価を行い、自分にとって一番価値の高いサービスを選択し、活用すべきと思います。

『自分にとって一番価値が高い』とは、各自のITに関するリテラシーレベルは異なりますので、自分の期待するサービスレベルに一番近く、利用料金も相当であるということを確認した方が良いということです。車（車種、デザイン）やマンション（機能、間取り）、或いはパッケージ旅行（旅先、通訳）等を選択する際の感覚に近いものがあるかもしれません。

全てが整っていて価格も一番安いのであれば迷うことはありませんが、一般には色々な特徴がありますので、複数の基準を持って比較検討し、自分のフィーリングにマッチさせる必要があるはずです。

インターネット上のサービスでは、自分で対処できる、利用しないサービスがあっても費用の無駄ですし、逆に機能が豊富、高機能、かつ複雑過ぎてしまい、結局加入しても殆どサービスを利用せず、勿体ないので利用を止める。といった状況にならぬよう良く吟味して選択して欲しいと思います。なお、お試し利用サービス等が提供されているのであれば、興味のある機能だけでなく、とりあえず全ての機能を利用して見ることをお勧めします。また、同じような業種、専門分野の方々が集まるサービスを選択するもの利用価値があります。業務上において、同じ課題を持つ者が集まるサービスでは、情報交換も活発になり、業務の質とスピードアップに効果が期待できます。

そして、最後に忘れてはならないのが、やはりセキュリティ面です。個人利用であれば、自己責任の範囲でIDパスワードによる利用でも被害は自分だけで済みますが、顧客の情報を扱うようなサービス等では利用しないほうが無難です。なるべく、ICカード型電子証明書のような2要素認証（物理的な鍵＋論理的な鍵）による本人認証を採用した、セキュリティレベルの高いサービスを選択することが重要です。

日本電子認証株式会社

事業開発部　事業企画室長　木下寿夫

kinoshita@ninsho.co.jp

東京税理士会会員向け
IT研修会のご案内

東京税理士会情報システム委員会

◆◆会員向けIT研修の申込みについて◆◆

パソコン等の研修事業を実施している「中野キャリアスクール」の協力のもと、主にパソコン操作方法等に関して初心者を対象とした「会員向けIT研修」を開催しております。ここで紹介している研修の受講を希望される方は、本会事務局総務課までTEL又はFAXでご連絡下さい（書式は何でも結構です）。折り返し、申込み手順、申込み用紙、研修教室地図について詳細な内容を記載した「IT研修案内文書」をご希望のFAX宛に送付いたします。

東京税理士会事務局総務課　連絡先　TEL 03-3356-4461　FAX 03-3356-4469

1. IT研修・研修内容及び費用

① Word入門　全６時間

【内　　容】パソコン操作の基本となる文字入力、変換、文書編集、保存、印刷の基礎を習得する。
【受講の基準】日本語入力やマウスの操作も含めて、まったくパソコン操作経験のない方向けの研修（※1）
【費　　用】13,650円（受講料・教材費・消費税込み）

② Excel入門　全６時間

【内　　容】【表計算の基本となるデータ入力、表作成、四則計算、関数計算、グラフ作成、保存などの操作を習得する。
【受講の基準】パソコンを利用して日本語入力やマウス操作はできるが、Excelなど表計算機能は経験ない方向けの研修（※1）
【費　　用】13,650円（受講料・教材費・消費税込み）

※1・・・受講の基準は、目安に過ぎないので、自由にご希望の研修をお申込できます。

③インターネット入門　全３時間

【内　　容】インターネットの利用方法、ホームページ検索、閲覧、電子メールの送受信方法を習得する。
【受講の基準】パソコンを利用して日本語入力やマウス操作はできるが、電子メールとインターネットは経験ない方向けの研修（※1）
【費　　用】10,500円（受講料・教材費・消費税込み）

④セット講座（全４コース）

【内　　容】上記、①Word入門、②Excel入門、③インターネット入門を組み合わせて受講し、パソコンの全般的な操作方法を習得する。
【受講の基準】①Word入門、②Excel入門、③インターネット入門と同様。
【費　　用】A: ①Word入門＋②Excel入門・・・25,200円
B: ①Word入門＋③インターネット入門・・・21,000円
C: ②Excel入門＋③インターネット入門・・・21,000円
D: ①Word入門＋②Excel入門＋③インターネット入門・・・35,700円
（受講料・教材費・消費税込み）

2. 研修日程表及び研修場所について

①Word（6時間）コース

曜日	月・火曜日			水曜日	
時間	*1日3時間、2日間コース 17:00～20:00			*1日6時間コース 10:00～17:00（1h休）	
場所		新宿	京王八王子		新宿
月	実施日	講座NO	講座NO	実施日	講座NO
7月	2日・3日	7	37	4日	64
	23日・24日	8	38		
8月	20日・21日	9	39	22日	65

②Excel（6時間）コース

曜日	月・火曜日			水曜日	
時間	*1日3時間、2日間コース 17:00～20:00			*1日6時間コース 10:00～17:00（1h休）	
場所		新宿			新宿
月	実施日	講座NO		実施日	講座NO
7月	9日・10日	107		11日	134
	30日・31日	108			
8月	27日・28日	109		29日	135

③インターネット（3時間）コース

曜日	水曜日			金曜日			
時間	*夕方から実施するコース 17:00～20:00			*午後から実施するコース 13:00～16:00		*夕方から実施するコース 17:00～20:00	
場所		新宿	京王八王子		新宿		新宿
月	実施日	講座NO	講座NO	実施日	講座NO	実施日	講座NO
7月	11日		214	13日	237	13日	267
	25日	204		27日	238	27日	268
8月	22日		215	24日	239	24日	269

（ご注意）Excel入門は、新宿校のみでの実施となります。

3. しっかりマスターコース内容および費用（「会員向けIT研修」よりもさらにしっかりマスターしたい会員向けの講座）

全コース「フリータイム予約制」となっており、各自の進度にあわせたきめ細かい指導を受けられます。但し、指定された有効期間内の受講となりますので、その期間内で全時間消化していただくことになります。具体的な受講手続き、場所等の詳細につきましては、中野キャリアスクール新宿エルタワー校（TEL 03-3340-3915）へ直接お問い合わせ下さい。

◆受講コース名:学習時間内で各自の進度・ペースに合わせた実習を行うことが出来ます。（但し、教材費・消費税別）

◆16Hコース	※全16Hを1ヶ月以内に受講	33,600円
◆32Hコース	※全32Hを2ヶ月以内に受講	66,400円
◆48Hコース	※全48Hを3ヶ月以内に受講	96,000円
◆64Hコース	※全64Hを4ヶ月以内に受講	128,000円
◆96Hコース	※全96Hを6ヶ月以内に受講	168,000円

◆受講内容:学習時間内で以下の内容を、ご希望の順序で学習いただけます。

Word初級	基本操作をマスターし、一般的な文書作成ができるように学習します。
Excel初級	基本操作をマスターし、一般的な表作成及び基本的なグラフ作成ができるように学習します。
インターネット初級	インターネットのホームページ閲覧、検索、メールの送受信の基本、添付ファイルの作成を学習します。