事故・被害の事例

正しい情報セキュリティの対策を施していないと、どんな問題があるのでしょうか？ここでは、実際に起こった事故・被害を元に、再構成した事例を紹介します。

事例１：資料請求の情報が漏洩した 2
事例２：私の名前で誰かがメールを 3
事例３：ホームページを見ただけで… 4
事例４：ホームページが書き換えられた 5
事例５：猛威！デマウイルス 6
事例６：メールが他人に読まれている？ 7
事例７：ネットストーカーに注意 8
事例８：顧客のメールアドレスが漏洩 9
事例９：対策は万全なはずなのに… 10
事例１０：送った覚えがないのに… 11
事例１１：オークションの商品が届かない 12
事例１２：そんな簡単に儲かるの？ 13
事例１３：他人のＩＤで不正にオンライン株取引 14
事例１４：中古パソコンによるデータの漏洩 15
事例１５：クレジットカード番号が盗まれた 16
事例１６：情報セキュリティ対策は万全だったはずなのに… . 18
事例１７：ファイル共有ソフトが原因で… 19
事例１８：ワンクリック詐欺って怖い… 20
事例１９：ＳＱＬインジェクションでサーバーの情報が… 21

事故・被害の事例

事例1：資料請求の情報が漏洩した

大手エステ会社のホームページで、資料の請求のために登録された3万件以上の氏名、住所、年齢、メールアドレスなどの個人情報が漏洩したという事件がありました。原因は、Web サーバーの初歩的な設定ミスでした。この情報漏洩事件では、登録情報の中に、エステに関心を持っている理由や体のサイズという項目があったために、とても大きな問題になりました。

この事件だけでなく、ホームページで登録された個人情報が漏洩する事件は数多く発生しています。たとえば、懸賞やプレゼントの応募者名簿、アンケートの情報、商品の購入者名簿などの漏洩事件が発生しましたが、これらのほとんどは基本的なサーバーの設定ミスが原因であったようです。

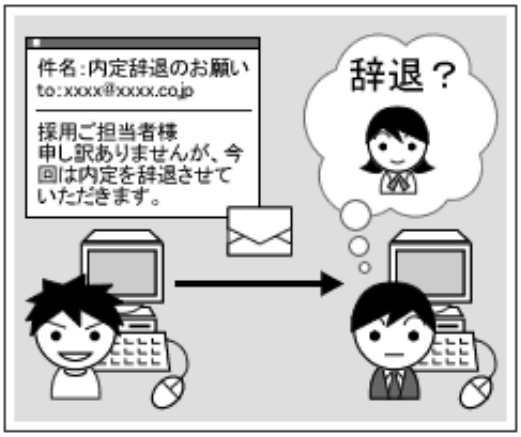
事故・被害の事例

事例2：私の名前で誰かがメールを

大学4年生のA子さんは、ある会社に就職が内定していました。ところがいつまで待っても、肝心の採用通知が送られてきません。そこで、会社の人事担当者に連絡すると、なんとA子さんから電子メールで内定を辞退するという連絡があったというのです。驚いたA子さんは、担当者に再度電子メールを確認してもらいましたが、間違いなくそれは大学で使用しているメールアドレスでした。

慌てて大学に調査を依頼したところ、同じサークルのB君がA子さんになりすまして、人事担当者に電子メールを送っていたことがわかりました。B君は、A子さんのユーザー名とパスワードを盗み出していたそうです。

これは実際に起こった事件です。なお、他人のユーザー名を使用して、認証サーバーに侵入したということで、犯人の男子学生は不正アクセス禁止法違反容疑で逮捕されています。



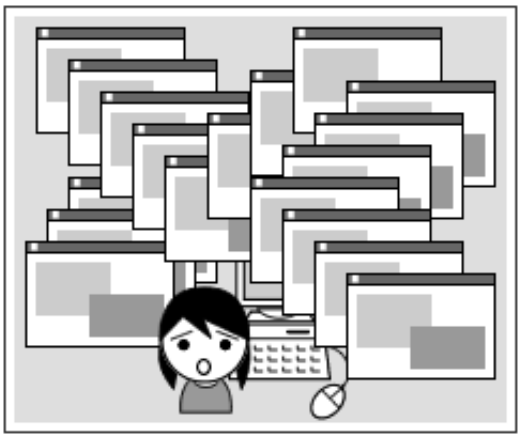
一言アドバイス

パスワードは、人に推測されにくいものにして、絶対に他人にわからないように管理しなければなりません。もし、人に知られてしまった可能性がある場合には、すぐに変更するようにしましょう。

事例3：ホームページを見ただけで…

好きな歌手のファンが集まる電子掲示板を見ていたA さんは、「次回のコンサートのチケットが安く手に入るみたい。限定30 枚だって。」という書き込みを発見しました。早速、参照先のホームページのリンクをクリックしてみると、画面にウィンドウが次々と現れて、マウスで閉じても閉じても、とても間に合いません。しばらくすると、キーボードもマウスも動かなくなり、コンピュータが停止してしまいました。

これは、リンク先のホームページがブラウザクラッシャ、通称ブラクラと呼ばれる悪質なホームページであったことが原因です。ブラウザクラッシャにはいくつかの方法がありますが、無限に新しいウィンドウを開くスクリプトや、電子メールの新規ウィンドウを呼び出すスクリプトを利用したものが有名です。電子掲示板やチャットなどで、参加者に対するいやがらせとして行われることが多いようです。



事故・被害の事例

事例4：ホームページが書き換えられた

ホームページの改ざん（書き換え）は、インターネットにおいて頻繁に発生する事件のひとつです。

2000 年には、官庁のホームページが狙われて、相次いで改ざんされました。その後、同じような手口で、自治体や大手企業、学校などのホームページが改ざんされています。

ホームページの改ざんは、ある目的を持って特定の団体や企業を攻撃する場合と、無差別に情報セキュリティ対策の甘いホームページを改ざんする場合のどちらかに分類することができます。

ホームページの改ざんというと、とても高度なハッカーの仕業であるように思うかもしれませんが、現実的にはファイアウォールさえも存在していなかったり、安易なパスワードを設定していたり、既知のセキュリティホールをそのまま残していたりといった具合に、適切な情報セキュリティ対策を怠ったことが原因であることがほとんどです。

事故・被害の事例

事例5：猛威！デマウイルス

K さんはメール友達の J さんから「K さんのコンピュータはウイルス大丈夫？私のコンピュータはやられちゃったみたい。もし、sulfnbk.exe というファイルがあったら、すぐに削除しないとまずいよ。このウイルス、だいぶ流行っているみたいだから、他の友達にも知らせてあげてね。」という電子メールを受け取りました。すぐに K さんが自分のコンピュータを確認したところ、確かにこのファイルがあったので、慌てて削除してしまいました。でも、K さんのコンピュータにはちゃんとウイルス対策ソフトがインストールされていたのです。では、このウイルスはどのように感染したのでしょうか。

これは、デマウイルスというちょっと変わったウイルスです。簡単に言ってしまうと、この電子メールの内容自体が「デマ」つまり嘘であるというわけです。この sulfnbk.exe というファイルは、Windows が使用しているもので、これを消してしまうとコンピュータの動作がおかしくなってしまいます。実際に、このデマウイルスの情報は、チェーンメールとして日本中に広まり、多くのユーザーに影響を与えてしまいました。なお、同じようなデマウイルスに、jdbgmgr.exe というファイルの削除を促すものがあります。

一言アドバイス

このような話を聞いても、すぐには対応しないようにして、必ず詳しい人に確認したり、インターネットなどで調べたりしてから作業を行うようにしましょう。

事故・被害の事例

事例6：メールが他人に読まれている？

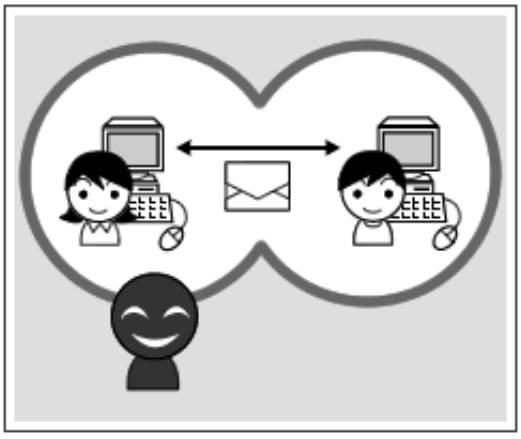
「E さん、温泉はどうだった？」

雑談の中で、なにげなくもらした同僚のF 君のひとことに、E さんは驚きました。週末の旅行は急に決まったため、会社内ではまだ誰にも話していないはずです。そういえば、この前もF 君が話していないことを知っているので、不思議に思ったことがありました。あのときは、誰か他の人から聞いたのかな、と思っていたのですが。

そういえば、この間外から会社に戻ってきたときに、なぜか読んでいないはずの電子メールが既読になっていました。もしかして、F 君に電子メールを盗み読まれているのでは・・・。

このように、他人に電子メールを読まれてしまうという事件は非常に多く発生しています。ほとんどの場合、電子メールはユーザー名とパスワードだけで読むことができるため、何らかの方法でパスワードを入手してしまえば、他人の電子メールを読むことはそれほど難しいことではありません。実際に犯人が逮捕された事件は、ほとんどが身近な人間による犯行ですが、好きな芸能人の電子メールをパスワードを推測して読み出したという珍しい事件も発生しています。

犯人が逮捕された事件の中には、コンピュータの設定を手伝ってもらう際にパスワードを教えて、その後も変更せずにそのまま利用していたり、簡単に推測できるパスワードを使用していたりなどのように、利用者側の不注意が原因のケースもあるようです。



一言アドバイス

パスワードは、人に推測されにくいものにして、絶対に他人にわからないように管理しなければなりません。もし、人に知られてしまった可能性がある場合には、すぐに変更するようにしましょう。

事故・被害の事例

事例7：ネットストーカーに注意

Ｎさんは、自分のホームページで自己紹介や自分の写真、日記などを公開していました。

Ｎさんは、ホームページを見た人たちから送られてくる電子メールを毎日楽しみにしていたのですが、ある日「僕とつきあってください」という電子メールが届けられました。最初は適当に返事をしていたのですが、あまりにもしつこく電子メールが送られてくるため、「迷惑ですので、もうメールしないでください」という返事をしたときから事態が急変しました。

次の日から、脅迫的な言葉が並べられた電子メールが、次々と送られてくるようになったのです。さらにしばらくすると、「おまえの住んでいる場所はわかっているんだ」という電子メールも送られてきました。そこにかかれているのは確かにＮさんの住所でした。気味が悪くなったＮさんは、自分のホームページを閉鎖して、引越しを検討するしかありませんでした。

これはひとつの例ですが、実際にこのようなネットストーカーの事件は数多く発生しています。ホームページの電子掲示板にいやがらせをされたり、大量の電子メールを送りつけてきたりといったことだけでなく、実際に自宅にまで押しかけてきたり、後をつけまわしたりといったストーカー行為を働くなど、ネット上から実世界に移行する例も珍しくありません。

事例8：顧客のメールアドレスが漏洩

P さんは、いつも利用しているお店のメールマガジンに登録しています。このメールマガジンでは、新製品の紹介やバーゲンセールの案内を定期的に送信してくれるものです。

ある日、このお店からメールマガジンが届けられましたが、何かいつもと違いました。よく確認してみると、なんと電子メールのヘッダに大量のメールアドレスが記載されています。確かに自分のメールアドレスもその中に含まれているのですが、それ以外のメールアドレスにはまったく見覚えがありません。

実は、ここで記載されている大量のメールアドレスは、メールマガジンの他の登録者のものだったのです。

本来、メールマガジンなどのように多くのユーザーに電子メールを送信する場合には、受信者に他人のメールアドレスがわからないようにしなければなりません。そのためには、専用のソフトウェアを利用するか、メールアドレスを TO や CC ではなく、BCC に指定する必要があります。

そのようにしなければ、このケースのように受信者全員にすべてのメールアドレスを教えてしまうことになってしまうというわけです。現在でも、このような単純なミスが原因で顧客のメールアドレスを漏洩してしまう事件が発生しています。

事故・被害の事例

事例9：対策は万全なはずなのに…

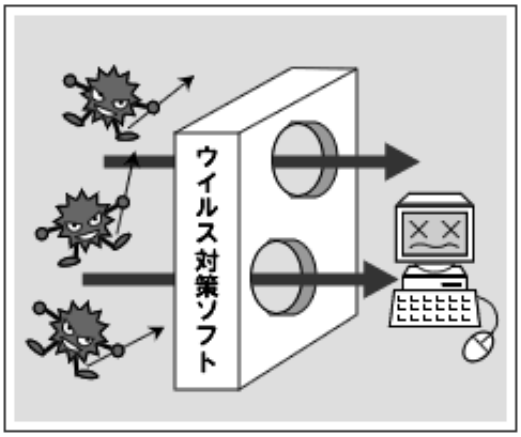
S さんが使用しているコンピュータは、1 年ほど前に購入したものです。当時、コンピュータを使用している友人がウイルスに感染して大騒ぎになったこともあり、安心して利用できるように、ウイルス対策ソフトが初めからインストールされているコンピュータを選択しました。

S さんは、そのコンピュータで電子メールやホームページの閲覧、ショッピングなどを楽しんでいました。しかし、ある日、友達の T さんからの電子メールを見てびっくりしました。その電子メールには、「あなたからウイルス付きの電子メールが送られてきた」と書かれていたのです。

そんなはずはありません。S さんのコンピュータには、購入したときからウイルス対策ソフトがインストールされているのです。それなのに、ウイルスが侵入したと言うのでしょうか。

これは、S さんが大切なことを忘れていたのが原因です。ウイルス対策ソフトは、電子メールやホームページのデータに今までに発見されているウイルスが含まれていないかどうかを検出する仕組みになっています。つまり、まったくの新種のウイルスは、発見することができない可能性があるのです。

このケースでは、S さんが 1 年前に購入してからウイルス対策ソフトのウイルス検知用データを最新のものに更新していなかったため、新しいウイルスに感染してしまったというわけです。



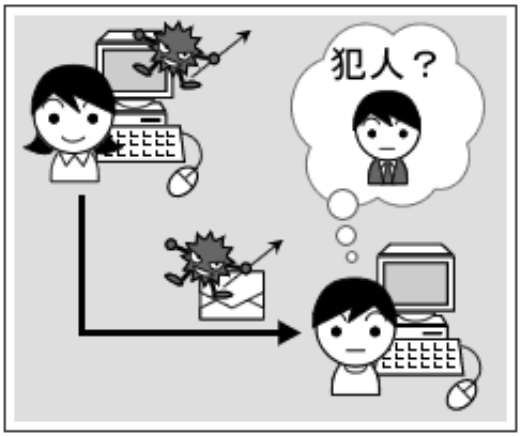
事故・被害の事例

事例10：送った覚えがないのに…

ある日、H 君のもとに、友達の O 君から電子メールが届きました。その電子メールによると、昨日 H 君からウイルス付きの電子メールが送られてきたというのです。でも、H 君は最近帰りが遅くなることが多く、ここ 1 週間ほど自宅のコンピュータは電源さえも入れていません。もちろん、きちんとウイルス対策ソフトをインストールして、ウイルス検知用データも定期的に更新しています。つまり、ウイルスに感染しているはずも、ウイルス付きの電子メールを送信したはずもないのです。

実は、このウイルス付きの電子メールは、H 君からではなく、O 君と共通の友達である R さんから送られていたのです。最近のウイルスの中には、アドレス帳に登録されているメールアドレスや過去に受け取った電子メールからメールアドレスを探し出して、あたかもその人が電子メールを送信しているかのようにふるまうものがあります。

つまり、これはウイルスに感染した R さんのコンピュータが、H 君の名前で O 君にウイルス付きの電子メールを送信していたというわけです。



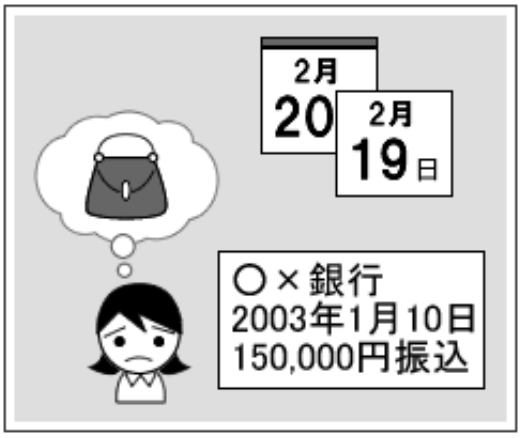
事故・被害の事例

事例11：オークションの商品が届かない

Y さんは、いつもオークションサイトでお気に入りのブランド品の出物を探しています。今回も、オークションサイトで限定品のバッグを見つけたため、早速オークションに参加しました。その出品者は業者であるらしく、ある理由で手持ちの多くの商品をすぐに売りたいということでした。市価よりもずっと安いとはいえ、かなり高額な商品であったため、最初は少し迷いましたが、既に何人かの会員がその業者から商品を受け取って喜んでいるのを見て、安心して銀行から代金を振り込みました。

しかし、何日たっても商品は送られてきません。あらかじめ教えてもらった相手の電話番号に連絡しても、既に解約されているようでした。住所も偽の住所だったようです。しばらくすると、初期に購入した会員以外には、誰も商品が送られて来ていないということが発覚しました。

最近は、商品を時期をずらして大量に出品して、初めの頃の相手にだけ商品をきちんと送ることで、他の入札者を安心させるという手口が多くなっています。悪質なケースでは、最初の頃は犯人が自ら別の名前で落札していただけで、実は初めから何ひとつ商品を用意していなかったという事件も発生しています。



事故・被害の事例

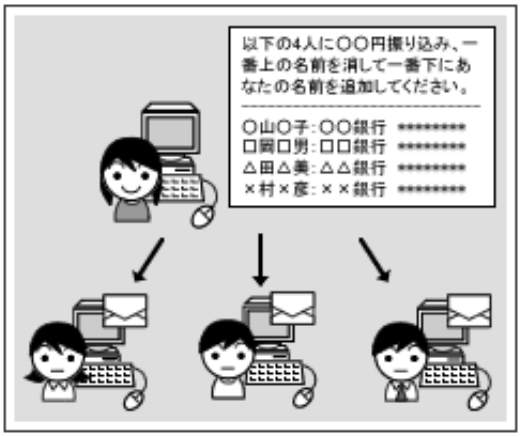
事例12:そんな簡単に儲かるの？

2001年1月に、ある男性が電子メールを使用した無限連鎖講防止法違反の疑いで摘発されました。無限連鎖講とは、いわゆるねずみ講のことです。

この男性が送った電子メールは、記載されている4人の会員に1000円を振り込んだ上で、自分の口座を一番下に書き加えて、多くの知り合いに電子メールを送ってくださいというものです。

電子メールには、たくさんの知人に転送するだけで、いつの間にかあなたの銀行口座には毎日のようにたくさんの人からお金が振り込まれますという記載がありました。この男性は、このねずみ講によって最終的に100万円以上の利益を得ましたが、懲役10ヶ月、執行猶予3年の有罪判決を下されています。

このようなねずみ講を誘う電子メールは、この事件以降にも、文面を変えて何種類も出回っています。



一言アドバイス

チェーンメールの中には、このように安易に儲かるというキャッチフレーズで、ねずみ講への勧誘を行う事例もあります。ねずみ講は、ねずみ講を始めた人だけでなく、犯罪という意識がないまま知人を勧誘した場合にも罪に問われる場合があるので、十分な注意が必要です。

事故・被害の事例

事例13：他人のIDで不正にオンライン株取引

これは、2002年6月に発生した事件です。

証券会社の顧客になりすまして、オンライントレードのシステムを利用して株の売買を行った情報処理サービス会社の社員Aが、不正アクセス禁止法違反、私電磁的記録不正作出・同供用で逮捕されました。

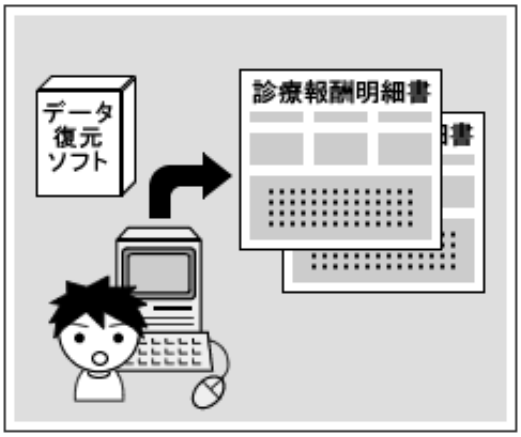
情報処理サービス会社の社員であったAは、派遣先の証券会社でオンライントレードのシステムに関わる作業を行った際に、ユーザー名やパスワードなど、約3万8000人分の顧客情報を自分のノートパソコンにコピーして不正に入手していました。社内の自分の評価に不満があり、トラブルを起こすことそのものが目的であったそうです。

なお、「自己中心的な犯行で、電子商取引の安全に不安を投げ掛けた」として、Aには、懲役2年6ヶ月、執行猶予3年の判決が言い渡されています。

事故・被害の事例

事例14：中古パソコンによるデータの漏洩

名古屋市内で、ある大学生が中古のパソコンを購入したそうです。購入後、その大学生が市販のデータ復元ソフトを使用して、ハードディスクのデータを復元してみたところ、なんとある医療機関が健康保険組合などに医療費を請求するために作成した診療報酬明細書の画像データが残されていたということです。



一言アドバイス

企業内の機密情報収集を目的として、中古パソコンを購入するという手口も行われているようです。コンピュータやハードディスクは、必ずデータが復元できない状態にしてから廃棄しなければなりません。

事故・被害の事例

事例15：クレジットカード番号が盗まれた

いつもインターネットでショッピングを楽しんでいるＯさんの元に、ある日、次のような内容の電子メールが届きました。

○×カードより
いつも当社のクレジットカードをご利用頂きまして、誠にありがとうございます。
最近、他人のクレジットカードを利用して、不正にショッピングを行う悪質な犯罪が増加しています。そのような不正利用への対策として、当社では一定期間ごとに暗証番号の変更をお願いしています。
以下のＵＲＬアドレスから弊社のホームページに接続して頂き、お名前、クレジットカード番号、暗証番号をご登録ください。

http://www.××××.com/henkou/

なお、このメールをお受け取り頂いてから１ヶ月以内にご登録頂かなければ、お持ちのクレジットカードがご利用できなくなるため、ご注意ください。

この電子メールを受け取ったＯさんは、早速メールに記載されたＵＲＬアドレスをクリックして、表示されたホームページで、自分の名前、クレジットカード番号、新しい暗証番号を登録しました。

事故・被害の事例

・・・そして、1ヶ月後・・・

郵送されてきたクレジットカードの請求書を見たO さんは、とてもびっくりしました。そこに記載されていたのは、自分が想像していたものよりもずっと大きな金額だったのです。明細を見ると、まったく買い物をした記憶がないお店で、クレジットカードを使用したことになっていました。

最近、このように電子メールとホームページを利用した悪質な詐欺が増えてきています。このような情報収集の手口をフィッシング詐欺と言います。フィッシング詐欺の多くは、クレジットカード会社や銀行、ショッピングサイトなど、実在する有名な会社の名前を装って、多くの人に電子メールを送信します。そして、電子メールに記載されたURL アドレスで接続されるホームページによって、利用者に重要な個人情報やカード番号などを登録させる方法をとっています。

フィッシング詐欺による電子メールの多くは、受信者がついうっかり個人情報を登録してしまうような巧妙な文面になっています。

一言アドバイス

自分の利用しているクレジットカードの会社や銀行の名前で電子メールが送られてきても、すぐに信用してはいけません。電子メールに記載されている内容をよく読んで、不明な点や怪しい点がある場合には、その会社に問い合わせを行うようにしてください。電子メールに記載されているURL アドレスが本当にその会社のものであるかどうかを確認することも大切です。

URL アドレスがその会社のものであるように見える場合でも、ホームページでクレジットカード番号や暗証番号、パスワードなどを登録したり変更したりするように促す電子メールについては、リンクが詐称されている可能性があるという点にも注意するようにしてください。

事故・被害の事例

事例16：情報セキュリティ対策は万全だったはずなのに・・・

ある会社での出来事です。S さんが会社の情報管理担当者になって、もう 3 年になります。もともとコンピュータが好きな S さんだけあって、会社内の情報セキュリティ対策は万全と考えています。

それぞれの社員が使用するコンピュータはもちろん、サーバーにもウイルス対策ソフトが導入されています。ウイルス対策ソフトに対しては、定期的なウイルス検知用データの更新も行っています。そして、外部からの侵入に備えて、ネットワークにファイアウォールも装備しました。

しかし、ある日、S さんがインターネットの電子掲示板を見てみると、なんと自分の会社の顧客情報が漏洩していることがわかりました。いったいどうして・・・。

最近では、このように情報セキュリティ対策を施していたにも関わらず、情報が漏洩してしまったという事例も増えています。たとえば、このケースでは、ある 1 人の社員が仕事のデータを自宅に持ち帰った際に、自宅のコンピュータがウイルスに感染していて、そこから個人情報が漏洩してしまったということが考えられます。もしくは、誰かが業務データファイルの保存されていた USB メモリをどこかで紛失してしまったのかもしれません。つまり、情報セキュリティ対策には、完璧な対策というものはないと言わざるを得ないのです。

個人情報や機密情報を保有する企業や組織は、システムやソフトウェアによる情報セキュリティ対策だけでなく、厳密な社内ルール（情報セキュリティポリシー）の策定とその徹底、データベースやファイルサーバーに対する権限設定など、多角的なセキュリティ対策が要求されるものです。

一言アドバイス

情報管理担当者は、基本的な情報セキュリティ対策だけでなく、社員への教育の徹底も、大切な情報セキュリティ対策のひとつであるということを心に止めておいてください。

また、情報セキュリティ上のリスクは、時間とともに変動するものです。そのため、現状の情報セキュリティ対策に満足するのではなく、最新の情報セキュリティ脅威の動向に常に気を配り、継続的に適切な対策を実施することが大切です。

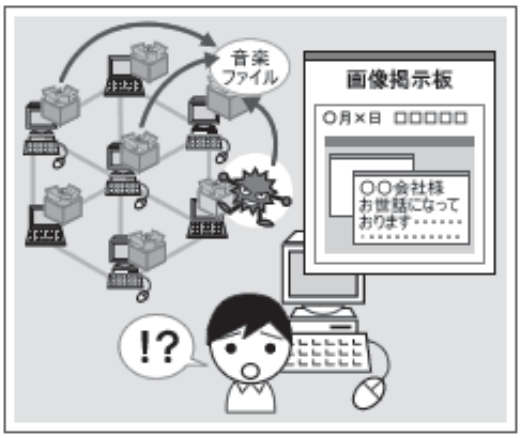
事故・被害の事例

事例17：ファイル共有ソフトが原因で・・・

T 君は大の音楽好きです。T 君は大量の音楽データをまとめてダウンロードするために、ちょっと会社のネットワークを拝借することにしました。会社で自分が使っているパソコンに、ファイル共有ソフトを入れてみると、あっという間に好きな音楽データがたまっていきます。

そんなある日のことです。ファイル共有ソフトでダウンロードしたひとつのファイルを開いたときに、T 君の使用するパソコンがウイルスに感染してしまったのです。しかし、T 君はウイルスに感染したことにはまったく気づきません。しばらくすると、社内でインターネットの電子掲示板に、会社の名前が出ているということを耳にしました。

T 君がその電子掲示板にアクセスしてみると、なんとそこにはT 君が使用しているパソコンのデスクトップ画面の画像が公開されているではありませんか。そして、デスクトップ画面には、大切なお客様に送信した重要な電子メールの内容がしっかりと記されていたのです。



一言アドバイス

ファイル共有ソフトを導入した場合には、ウイルスに感染してしまうと、機密情報や個人情報が漏洩する危険性が高いということを認識しておかなければなりません。特に、会社のパソコンにファイル共有ソフトを本当に入れる必要があるのかをしっかりと考えてみましょう。

事故・被害の事例

事例18：ワンクリック詐欺って怖い・・・

ある日、E 君の携帯電話に電子メールが送信されてきました。送信元の名前は知らない人でした。でも、電子メールには、なにやら楽しげな文字が躍っています。ちょうど時間を持て余していたE 君は、何となく電子メールに記載されているリンクをクリックしてしまいました。

すると、そこには次のように表示されていたのです。

> ご入会ありがとうございます。あなたの個体識別番号は以下の通りです。
>
> 2468XXXXX
>
> サービスのご利用料金は1ヶ月間で8,000円です。1週間以内にお振り込み頂けなかった場合には、ご自宅にまで回収にお伺いすることになります。その場合には、延滞料金30,000円および回収にかかる実費と交通費で32,000円、合計62,000円を追加して頂戴することになりますのでご了承ください。なお、お支払い頂けない場合には、裁判所からご連絡がいくことになります。

びっくりしたE 君は、怖くなって指定された口座番号に料金を振り込むことにしました。

これは代表的なワンクリック詐欺の手口です。電子メールを携帯電話やパソコンに送りつけて、そこに記載されているWeb サイトを訪問した人に対して、脅迫めいた手口で料金の振り込みを迫るというものです。

一言アドバイス

知らない人からの電子メールに記載されたリンクをクリックしないようにしましょう。また、誤ってクリックしてしまった場合でも、正しい契約を行っていない場合の料金請求は無効となるため、慌てずに行動してください。自分の行った操作が契約したことになるのかどうかがわからない場合には、総務省電気通信消費者相談センター、消費生活センター、警察などに相談しましょう。

事故・被害の事例

事例19：SQLインジェクションでサーバーの情報が・・・

W さんの会社は、自社製品を販売するためにショッピングサイトを構築することになりました。会社には情報システム部もないし、IT に精通したスタッフもいません。担当部署の中で一番若く、コンピュータに詳しいという理由で、W さんが専任者に選ばれたのです。

さて、早速業者にホームページ制作とシステムの構築を依頼し、なんとかショッピングサイトの公開にこぎ着けました。直販サイトなので価格も安く、ここでしか販売しない商品を取りそろえたのが良かったのでしょうか、運用開始直後から少しずつ売り上げも伸びてきました。このまま行けば、人気サイトと呼ばれる日も近いのかもしれません。

そんなある日のことです。このサイトが繁盛していることを知った悪意のある人間がいました。彼は会員ページの入り口にあるログオンページに目を付けました。ログオンページのユーザーID 入力欄にコマンドを含む特殊な文字列を入力するSQL インジェクションという手法を試みたところ、なんとパスワードを知らなくても会員ページにログオンできてしまうことが分かりました。会員ページに入ってしまえば、会員の住所や氏名、電話番号、購入履歴の他に、クレジットカード番号まで参照できるのです。このような方法で、W さんの会社のショッピングサイトから会員の個人情報が大量に漏洩してしまったのです。

実際に、このW さんの会社のように、数多くのホームページでSQL インジェクションによる被害が多発しています。中には、会員情報がまとめて漏洩するケースや、ホームページが改ざんされて悪質なサイトに誘導するような仕掛けを組み込まれたケースもあります。