情報管理担当者のための情報セキュリティ対策

企業や組織においては、情報管理担当者が全体の情報セキュリティ対策を指導しなければなりません。情報管理担当者は、どのようなことを理解していなければならないのでしょうか。

ここでは、企業・組織における情報管理担当者のための情報セキュリティ対策について説明します。

ウイルスからの防御 2
ユーザー権限とユーザー認証の管理 4
パスワード管理の推奨 5
バックアップの推奨 8
ソーシャルエンジニアリングの対策 9
サーバーの設置と管理 11
機器障害への対策 12
ハッキングによる被害と対策 13
社員の不正による被害 15
廃棄するコンピュータやメディアからの情報漏洩 16
情報セキュリティポリシーの導入と運用方法 17
持ち運び可能なノートパソコンを利用する上での危険性と対策 19
持ち運び可能なメディアを利用する上での危険性と対策 22
ASP・SaaS を利用する際の情報セキュリティ対策 24
SQL インジェクションへの対策 26

※特に重要な項目には マークがついています。

なお、企業や組織においては、実施する情報セキュリティ対策の方針や行動指針を明確にした情報セキュリティポリシーを策定しておくことが理想的です。情報セキュリティポリシーには、社内規定といった組織全体のルールから、どのような情報資産をどのような脅威からどのように守るのかといった基本的な考え方、ならびに情報セキュリティを確保するための体制、運用規定、基本方針、対策基準などを具体的に記載するのが一般的です。既に組織内で情報セキュリティポリシーが策定されている場合には、その内容を元にして情報セキュリティ対策を進めるようにしてください。

ウイルスからの防御

最近は、組織内のネットワークを介して、ファイルサーバーやWeb サーバーに感染するタイプのウイルスが増えてきています。ネットワークに接続しているたった1 台のコンピュータがウイルスに感染しただけで、組織内のコンピュータに被害が拡大する可能性があるため、情報管理担当者にかかる責任はとても大きいものです。さらに、インターネットに接続しているWebサーバーにウイルスが感染してしまうと、企業の社会的な信頼を失うことになります。

このような被害を受けないためには、まずサーバー、クライアントを問わず、すべてのコンピュータにウイルス対策ソフトをインストールします。

また、常にウイルス検知用データを最新のものに更新するようにして、同時にこれをすべてのユーザーに指導しなければなりません。その上で、信用できないホームページは閲覧しないようにする、不明な内容の添付ファイルは開かないなどの基本的な防衛策と、ウイルスに対する理解を広めるようにすべきです。導入しているウイルス対策ソフトのメーカーのニュースレターなどで常に最新の情報を収集し、感染力が高いウイルスが発見された場合は、その現象や対処方法をユーザーに連絡して、ウイルスの感染予防に努めてください。

ウイルス感染が発生してしまったときには、ユーザーから情報管理担当者まで必ず報告をするように指導することで、感染をいち早く認識できるようにすることが大切です。さらに、感染したコンピュータを組織内のネットワークから切り離した上で、ウイルスの駆除をしたり、他のコンピュータやサーバーなどの感染状況を確認して駆除したりすることで、ウイルス感染の被害を最小限に留めるようにしましょう。

ユーザーひとりひとりのコンピュータや、数多くのサーバーをウイルスから防御するためには、単純にすべてのクライアントやサーバーにウイルス対策ソフトをインストールする以外に、企業として一元的にウイルスの侵入口の防御や、感染状態などの把握をすることが有効です。たとえば、メールサーバー用のウイルス対策ソフトをインストールすることで、外部との電子メールの送受信の段階でウイルスを除去することができます。また、企業や組織向けの統合的なウイルス対策ソフトを導入することで、すべてのクライアントやサーバーごとのウイルス検知用データの更新状況や、ウイルスの感染状況を、情報管理担当者が一元的に管理することができます。このようなツールを使って、情報管理担当者によるウイルス対策の労力を低減することができるので、検討してみるのもよいのではないでしょうか。

また、ウイルス対策ソフトを導入する以外にも、プロバイダが自社の接続サービスの利用者向けに提供しているウイルス対策サービスを利用する方法もあります。ウイルス対策サービスの提供の有無や提供内容などについては、プロバイダのホームページで確認するか、加入しているプロバイダに問い合わせてください。なお、プロバイダのウイルス対策サービスを利用する場合には、プロバイダがウイルス検知用データを自動的に更新するため、情報管理担当者やユーザーによる更新作業は不要になります。

注意

最近、無料のウイルス対策ソフトのように見せかけて、ウイルスをインストールさせる手口による被害が増えているため、注意してください。その代表的な手口は、ホームページなどで「あなたのコンピュータはウイルスに感染しています」のようなメッセージを表示し、偽のウイルス対策ソフトのダウンロード用Web サイトに誘導して、ウイルスをインストールさせる方法です。

ホームページを見ているだけでウイルス対策ソフトのインストールを促された場合には、不用意にリンク先のホームページに接続したり、ソフトウェアをダウンロード / インストールしたりしないようにしてください。

ユーザー権限とユーザー認証の管理

重要!

社内ネットワークに対する情報セキュリティ管理のためには、個々のユーザーごとに適切な権限を設定する必要があります。ユーザーに与える権限は、すべてのユーザーにすべての権限を与えるのではなく、最低限必要なユーザーにのみ必要最低限のアクセスを許可することが大切です。

ユーザー権限は、ファイルサーバーやデータベースサーバーなどで個別に設定することも、ネットワーク全体でまとめて設定することも可能です。いずれの場合にも、ユーザーごとやグループごとに個別の権限を設定することができます。

たとえば、サーバーに対しては、アドミニストレータ（管理者）権限やユーザー（利用者）権限などがあります。データベースの場合には、データの登録や削除の権限、読み取りの権限、プログラムの実行権限などが設定できます。ある程度のユーザー数を持つネットワークの場合には、ユーザー権限を管理するための認証サーバーを用意することで、ネットワーク全体の管理業務を軽減させることが可能になります。

さらに、ユーザーに対しては、アクセス権限の設定も必要です。アクセス権限としては、システムの利用権限、ファイルサーバーの共有フォルダへのアクセス権限などがあります。

それぞれのユーザーアカウントを使用するためには、すべてのユーザーが自分の所有するユーザー名とパスワードを使用して、本人性の確認のためにユーザー認証を受けなければなりません。もちろん、ユーザーごとに適切な権限を設定していても、すべてのユーザーがパスワードを設定していなかったり、誰にでもわかるようなパスワードを設定していては何の意味もありません。適切なユーザー管理のためには、適切なパスワード管理が必須と言えます。

また、なりすましを防ぐ技術として、最近はユーザー名とパスワードのコンピュータの入力によるユーザー認証以外に、ＩＣ カードによるユーザー認証や、指紋や網膜などのバイオメトリックス（生体情報）を使ったユーザー認証も実用化され始めています。

パスワード管理の推奨

重要!

社内のユーザーに対して、アクセス権限に応じた個別のユーザーアカウントを発行していたとしても、実際にそれぞれのユーザーが適切なパスワード管理を行っていなければ意味がありません。そのためには、すべてのユーザーに対して、適切なパスワードの管理方法を指導する必要があります。

適切なパスワード管理には、以下の 4 つの要素があります。

■安全なパスワードの作成

安全なパスワードとは、他人に推測されにくく、ハッキングツールなどの機械的な処理で割り出しにくいものを言います。

安全なパスワードの作成条件としては、以下のようなものがあります。

- 名前などの個人情報からは推測できないこと
- 英単語などをそのまま使用していないこと
- アルファベットと数字が混在していること
- 適切な長さの文字列であること
- 類推しやすい並び方やその安易な組み合わせにしないこと

逆に、危険なパスワードとしては、以下のようなものがあります。

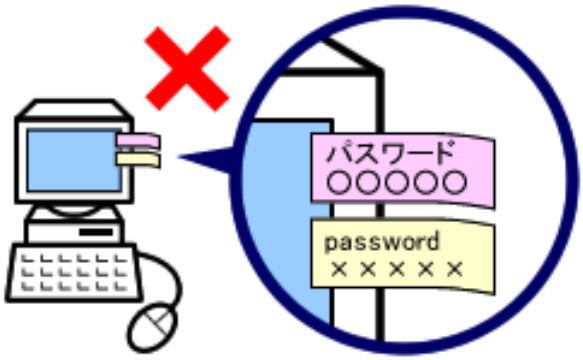
- ✖ 自分や家族の名前、ペットの名前
- ✖ 電話番号や郵便番号、生年月日など、他人から類推しやすい情報
- ✖ 社員コード
- ✖ 辞書に載っているような一般的な英単語
- ✖ “aaaaa”など、同じ文字の繰り返し
- ✖ ユーザー名と同じ文字列
- ✖ 短かすぎる文字列

インターネットなどで配布されているハッキングツールの中には、機械的にパスワードを推測する機能を持つものがあります。それらのハッキングツールでは、辞書に載っている英単語や簡単な英数字の繰り返し（123 や abc、aaa など）を自動的に組み合わせることで、パスワードを探し出そうとします。このようなハッキングツールでパスワードを割り出されないようにするためには、機械的に推測しやすい文字列を使わないようにすることが大切です。

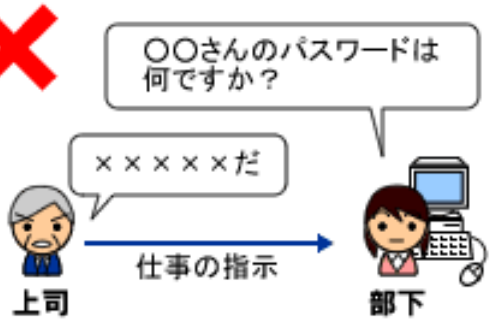
■パスワードの保管方法

せっかく安全なパスワードを設定しても、ユーザーのパスワードが他人に漏れてしまえば意味がありません。以下が、パスワードの保管に関してユーザーに指導すべきものです。

- パスワードは、同僚などに教えないで、秘密にさせること
- ユーザー名やパスワードを電子メールでやりとりさせないこと
- パスワードのメモを作ったり、ディスプレイにそのメモを貼ったりさせないこと
- パスワードを Web ブラウザなどのソフトウェアに記憶させないこと



ディスプレイにパスワードを貼り付けている



他のユーザーにパスワードを教えている

■パスワードの発行方法

情報管理担当者としてユーザーにパスワードを発行する際に、以下のようにいくつか留意しなければならない点があります。

- 初期にパスワードを発行する際の方法の検討（メモや電子メールを使うことが妥当であるか）
- ユーザーからパスワードの再発行依頼があった時の対応方法の検討

ユーザー数が多く、初期のパスワードの伝達に電子メールやメモを使わざるを得ない場合は、ユーザーが初めてログオンした際に、サーバー側でユーザーに強制的にパスワードを変更させるということも可能なシステムが多いので、このような方法を検討しましょう。

ユーザーからパスワードの再発行依頼があったときには、ユーザーの本人性の確認が必要になります。単に電話で問い合わせがあったから回答するというのでは、なりすましなどのソーシャルエンジニアリングが起きやすい状態であると言えます。受け付けは電子メールで、再発行は電話でという方針を取るなど、あらかじめ適切な対応方法を決めておきましょう。

■パスワードの定期的な変更

安全なパスワードを作成し、パスワードの保管方法も徹底したとしても、同一のパスワードを長期間使い続けることは避けなければなりません。ユーザーには定期的にパスワードを変更するように指導しましょう。また定期的な変更といっても、2 つか 3 つのパスワードをあらかじめ決めて、使いまわすのも避けるように指導した方が良いでしょう。

初期パスワードの変更と同一の仕組みを使い、一定期間が過ぎたらサーバー側で強制的にパスワードを変更させる仕組みを導入したり、パスワードの変更の際には何回か前までのパスワードに変更できないといったサーバーのパスワードの世代管理機能を導入したりすることで、ユーザーの定期的なパスワードの変更を手助けする仕組みもあります。

パスワードを定期的に変更しなければならない理由には、以下のようなものがあります。

●他人に推測されにくいパスワードでも、ハッキングツールを使って長時間かければパスワードが割り出されてしまうこと
●仮にパスワードが割り出されてしまっても、なりすましなどの被害を受け続けることを避けることができること

正しい管理方法をユーザーに理解してもらうとともに、ソーシャルエンジニアリングなどによるパスワード漏洩の危険性の認識を広めながら、定期的にパスワードを変更するといったルールを策定することも情報管理担当者の重要な役割です。

バックアップの推奨

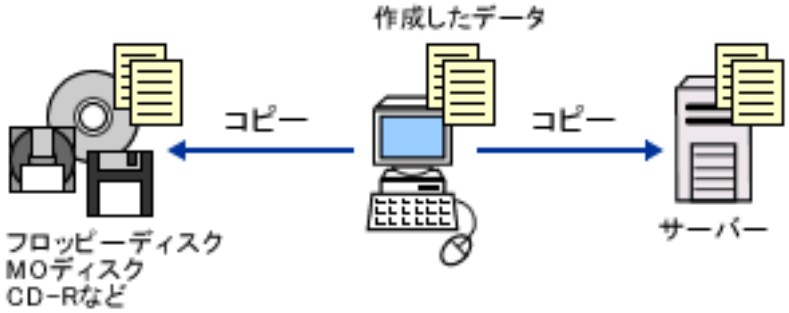
重要!

企業や組織内のユーザーが安全にコンピュータを利用できるようにするには、定期的なバックアップを推奨しなければなりません。クライアントのコンピュータでは、ワープロソフトや表計算ソフトなどで作成したドキュメントファイルだけでなく、送信した電子メールや受信した電子メール、よく利用するホームページのＵＲＬ アドレスなどもバックアップする必要があります。

バックアップには、フロッピーディスクや光磁気ディスク（ＭＯ ディスク）、ＣＤ-Ｒ などの外部の記憶媒体を利用する方法と、バックアップ用のファイルサーバーにコピーする方法がありますが、できるだけ手間をかけずにバックアップするには、バックアップ用のファイルサーバーを用意した方がよいかもしれません。

手動によるバックアップは面倒で間違いの多い作業です。できるだけ、すべてのユーザーに毎日忘れずに作業してもらうためには、ＯＳ に付属しているバックアップツールや市販のバックアップソフトなどを導入して、効率が良く手間のかからないバックアップ方法を推奨することが大切です。

なお、ユーザーによって外部の記憶媒体にバックアップされた情報は、外に持ち出されたり、机の上に放置されることは避けなければなりません。企業・組織にとって重要な情報が含まれる場合がありますので、鍵のかかる場所に保管するなど、適切な保管方法をユーザーに指導するようにしましょう。



注意

外部の記憶媒体を使用する場合には、データの持ち出しによる機密情報や個人情報の漏洩が発生する可能性が高くなるという点に注意してください。バックアップにおいて、外部の記憶媒体を推奨する場合には、情報セキュリティポリシーなどで、不必要な持ち出しを禁止したり、保管場所を規定したりといった情報管理上のルールを徹底することも重要です。

ソーシャルエンジニアリングの対策

重要!

ソーシャルエンジニアリングとは、ネットワークに侵入するために必要となるパスワードなどの情報を、コンピュータを使用せずに盗み出す方法です。ソーシャルとはsocial、つまり社会を表す言葉で、IT 技術を利用したハッキングではなく、実社会において情報を盗み出すことと考えるとわかりやすいかもしれません。

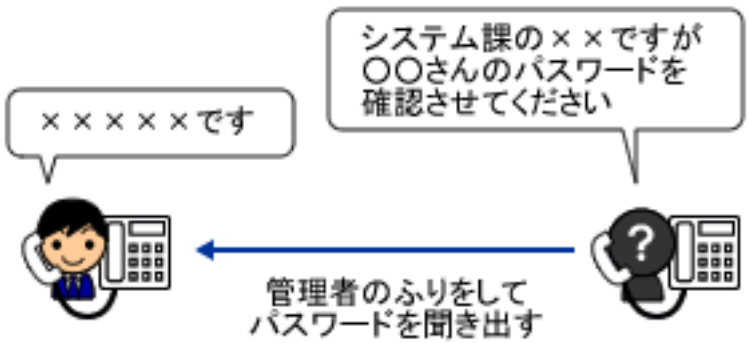
ひとりのユーザーの情報が漏洩するということは、組織全体の情報セキュリティレベルの低下につながります。必ずすべてのユーザーにソーシャルエンジニアリングに対する適切な対策を心がけるように指導しましょう。

ソーシャルエンジニアリングにはさまざまなやり方がありますが、ここでは代表的な方法と対策を紹介します。

■電話でパスワードを聞き出す

電話を利用したソーシャルエンジニアリングは、昔からある代表的な方法です。何らかの方法でユーザー名を入手したら、そのユーザーのふりをして、ネットワークの管理者に電話をかけ、パスワードを聞き出したり、パスワードの変更を依頼したりします。また、逆に管理者になりすまして、直接ユーザーに利用しているパスワードを確認するといったこともあります。これらの対策としては、あらかじめ電話ではパスワードなどの重要な情報を伝えないというルールを決めておくしかありません。

なお、この方法はキャッシュカードの暗証番号を調べるために使われることも多く、ほとんどの金融機関では「当行では電話でお客様の暗証番号をお聞きすることはありません」という案内を出しています。



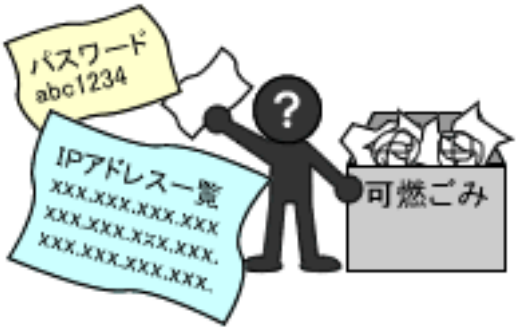
■肩越しにキー入力を見る（ショルダハッキング）

パスワードなどの重要な情報を入力しているところを後ろから近づいて、覗き見る方法です。肩越しに覗くことから、ショルダ（shoulder ＝肩）ハッキングと呼ばれています。たとえオフィス内であっても、パスワードやクレジットカードの番号など、キーボードで重要な情報を入力する際には、周りに注意しなければなりません。

■ごみ箱を漁る（トラッシング）

外部からネットワークに侵入する際に、初期の手順として行われることが多いのがトラッシングです。ハッキングの対象として狙ったネットワークに侵入するために、ごみ箱に捨てられた資料から、サーバーやルーターなどの設定情報、ネットワーク構成図、ＩＰ アドレスの一覧、ユーザー名やパスワードといった情報を探し出します。

面倒なようですが、やはり社内ネットワークや個人情報に関連する資料は、シュレッダーを利用する等の方法で確実に廃棄しなければなりません。なお、書類の廃棄方法については、社内のルールを確認してください。



ごみ箱の紙くずから情報を探し出す

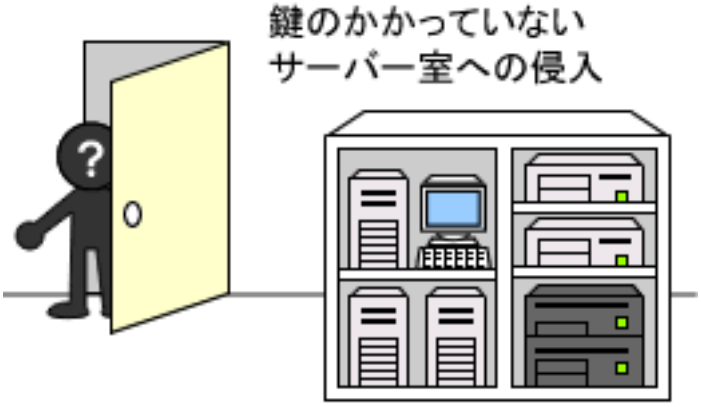
サーバーの設置と管理

企業や組織内にサーバーを設置する場合には、いくつかの点に考慮しなければなりません。まず、サーバーの設置場所として、外部の人間や権限のない社員、職員が容易にサーバーに近づけないような情報セキュリティ上の問題がない場所であるかどうかを検討します。特に、多くの人が出入りする場所をサーバーの設置場所に選ぶことは、許可のない外部の人間にサーバーを直接操作されてしまったり、サーバーの情報が盗み出されてしまったりする危険があるため、できるだけ避けるべきです。

逆にオフィスの隅やサーバー室など、人の目につきにくい場所にサーバーを配置する場合には、扉に鍵をかけるなど、外部から人が出入りできないようになっているかどうかを確認してください。

次に重要なこととして、サーバーに適切なパスワードを設定した上で、常にログオフした状態にしておくことです。短時間の内にログオンするためのパスワードを見つけ出すということはとても困難であるため、サーバーが不正に利用される可能性を減らすことにつながります。

最後に、地震などの天災からサーバーを守るために、耐震を考慮したサーバーの設置を検討すべきです。専用のサーバーラックにサーバーを固定して、サーバーラック自体に耐震機能を持たせるなどの方法があります。サーバーラックには鍵をかけることができるものが多いため、サーバーラックの導入を通して、情報セキュリティをさらに向上する効果も期待できます。最近では、インターネットデータセンターと呼ばれるサーバーの管理をすべて請負ってくれるサービスもありますので、社内に適切なサーバーの設置場所が見つからない場合には、そのようなサービスを検討するのもよいでしょう。



機器障害への対策

社内の情報機器を安全に利用するためには、不正侵入に対する防御だけでなく、停電の対策や機器に障害が発生した場合の対策も検討しておかなければなりません。

まず、停電対策として、サーバーには無停電電源装置（ＵＰＳ）を設置しなければなりません。無停電電源装置は、電気の供給が停止したり、電圧が低下したときに、内蔵しているバッテリから一時的に電気を供給できるようになっています。供給できる時間はバッテリによって異なり、数分から数十分程度ですが、無停電電源装置の設定によって一定時間電気の供給が停止した場合には、サーバーを自動的にシャットダウンすることができます。さらに、ほとんどの無停電電源装置には、雷による機器の破損も防備する機構が備わっています。

また、サーバーに障害が発生したときのために、必ずテープなどのバックアップメディアに毎日バックアップをとっておくことが大切です。バックアップソフトの中には、コンピュータのＯＳや、常に更新されるデータベースなどを、コンピュータを停止することなく自動的にバックアップすることができるものもあります。

さらに、緊急時にすぐに代替機を設定できるようにするために、あらかじめすべてのサーバーの設定内容を資料として安全に保管しておかなければなりません。社内の基幹サーバーなどのように、サーバーの停止が業務に大きな影響を与える場合には、あらかじめ同じソフトウェアをインストールした交換用のサーバーを用意しておくこともよいでしょう。交換用サーバーにバックアップされたデータを復元するだけで、ダウン時間を最小限に留め、基幹サーバーの可用性を高めることができます。

ハッキングによる被害と対策

重要!

外部からハッキングを受けると、さまざまな被害を受けることが考えられます。以下に代表的な被害を列挙します。

- ホームページを改ざんされる。
- サーバーに格納されていたデータが盗難される。
- サーバーのシステムが破壊される。
- サーバーやサービスが停止してしまう。
- メールサーバーを利用した迷惑メールの中継に利用される。
- 他のコンピュータを攻撃するための踏み台として利用される。
- バックドアを仕掛けられ、いつでも外部から侵入できるようにされる。

これらの被害から企業や組織の情報資産を守るためには、ひとつめの対策としてサーバー設定の確認が有効です。

- 不要なサービスが実行されていないか。
- 不要なスクリプトが残されていないか。

まず、確認しなければならない代表的なサービスとして、Telnet サービスと FTP サービスがあります。Telnet サービスは、ネットワークを介してサーバーを遠隔操作できるサービスです。また、FTP サービスは、コンピュータ間でのファイル転送に利用される代表的なサービスです。本来であれば、これらのサービスはインターネットを便利にするためのサービスですが、反面、ハッキングに利用されやすい代表的なサービスでもあります。自分で管理しているサーバーで、本当にこれらのサービスが必要かどうかを検討してみてください。

また、Web サーバーやデータベースサーバーにインストールされるスクリプトにも注意が必要です。スクリプトの中にはサーバーの管理用のものも含まれており、過去にハッキングに悪用されたケースがありました。これらのスクリプトは、Web サーバーやデータベースサーバーをインストールしたときに、自動的に追加されてしまうものが大部分です。Web サーバーやデータベースサーバーをインストールする際には、メーカーの情報セキュリティに関するホームページなどを参考にして、不要なスクリプトを削除するといった対策を行うことが必要です。

2 つ目の対策として、インターネット上で Web サーバーでデータベースに接続された Web アプリケーションを利用している場合における SQL インジェクションへの対応が必要です。SQL インジェクションは、特殊な文字列を Web サーバーに受け渡すことで Web アプリケーションに本来はあり得ない動作をさせて、データベースに格納されているデータを盗み出す手法です。SQL インジェクションは、Web アプリケーションとデータベースに適切な対策を実施することで防御することができます。

3 つ目の対策として、ファイアウォールの導入も検討してみましょう。守るべきサーバーの外側にファイアウォールを導入することで、インターネットからの Telnet や FTP といった通信をブロックすることもできます。

4 つ目の対策として、社員や職員が、勝手にクライアントコンピュータの機器構成を変えたり、企業や組織内で許可していないソフトウェアをインストールしたりすることを禁止するようにしましょう。機器構成を変える代表例として、モデムや回線の接続があります。回線の接続は、情報管理担当者がもっとも発見しにくいものであり、そのような回線を利用され、ハッキングされてしまった事例もあります。また、ユーザーが許可していないソフトウェアをインストールすると、それがセキュリティホールに直結することもあります。

5 つ目の対策として、ユーザーによるモバイル機器などの持ち出しを記録して、モバイル機器には社内システムのユーザー名やパスワードを記憶させないことです。ユーザーがモバイル機器を紛失しても、すぐにそのユーザー認証情報を変更することで、ハッキングなどの危険から情報資産を守ることができます。

このような情報セキュリティ対策を通して、ハッキング被害の可能性を減少させましょう。

社員の不正による被害

外部からのハッキングに対して、万全の情報セキュリティ対策を行っていたとしても、社内の人間が機密データを持ち出せるような管理体制をとっていては意味がありません。内部の不正による被害を減らすためには、まずすべてのユーザーに適切な権限を設定したユーザーアカウントを配布することです。次に、適切なパスワード管理方法を全社に浸透させた上で、自分の権限を他人に利用されることのないように指導しなければなりません。

データの持ち出しなどの不正行為は、大量の印刷物を外部に持ち出すことよりも、小さな電子メディアを持ち出すことの方が罪の意識が低いということもひとつの原因になっているようです。そのため、ノートパソコンやモバイルコンピュータを社内のネットワークに不正に接続できないように環境を設定したり、電子メディアを共通の保管場所で管理するなどによって、電子データに対する情報管理の意識を高めるとともに、社内のデータを外部に持ち出すことが犯罪行為になり得るということをしっかりと教育することが最大の防御策となります。

廃棄するコンピュータやメディアからの情報漏洩

重要!

企業や組織内の情報が漏洩するのは、ネットワーク経由とは限りません。コンピュータを廃棄したり、他人に譲渡したりする場合に、搭載されているハードディスクから情報が漏洩する可能性があります。中古のコンピュータに前の所有者が利用しているデータがそのまま残されていたというトラブルが発生しているだけでなく、企業で利用していた形跡のある中古のコンピュータを意図的に購入して、そこに保存されているデータを探し出すという方法で機密情報を入手するという手口も実際に使われているようです。

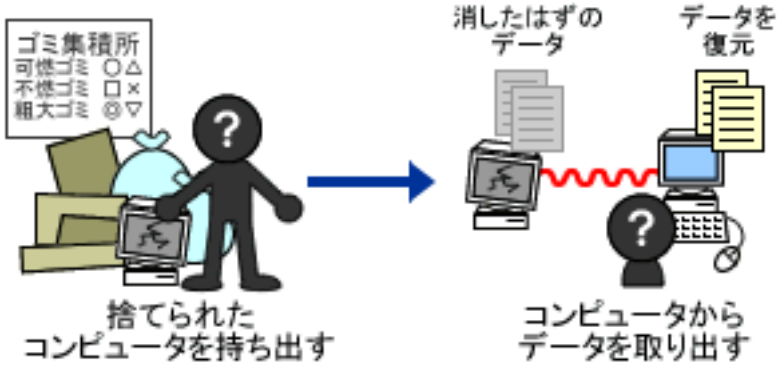
特に注意が必要なのは、格納されているデータを削除したり、ハードディスクをフォーマットしただけで、コンピュータを処分してしまう場合です。画面上でデータが消えているように見えても、実際にはハードディスク上にデータが残されたままになっていることがあり、特殊なソフトウェアを利用することで、削除されたはずのファイルを復元することが可能です。

不要になったコンピュータのハードディスクの処理方法には、以下のようなものがあります。

- データ消去用のソフトウェアを利用する。
- 専門業者のデータ消去サービスを利用する。
- コンピュータのハードディスクを取り出して、物理的に破壊してしまう。

これらの方法のいずれも、一長一短があり、現時点で絶対にこの方法が最良であるとは残念ながら言い難い状況です。これらの方法を企業・組織の情報資産の重要度に応じて組み合わせ、最適な方法を取るようにしましょう。また、当然のことですが、フロッピーディスクや光磁気ディスク（MO ディスク）、CD-R などの記憶媒体を廃棄する場合にも、同様の処理を心がけなければなりません。

このような廃棄物からの情報漏洩を防ぐには、コンピュータや記憶媒体は、必ず情報管理担当者が取りまとめて廃棄するなど、社内で統一のルールを確立し、徹底することが一番理想的です。



情報セキュリティポリシーの導入と運用方法

この企業・組織の情報管理担当者の対策のページでは、「ウイルスからの防御」、「ユーザー権限とユーザー認証の管理」、「パスワード管理の推奨」、「バックアップの推奨」などの内容を、企業・組織の情報管理担当者が実施しなければならない内容として記載しています。

これらを個別に検討し、その都度ルール化したのでは、各ルール間で矛盾が発生し、企業や組織として統一のとれた情報セキュリティのレベルが保てないことがあります。それを回避するために、策定する企業や組織として統一のとれた情報セキュリティ方針のことを情報セキュリティポリシーと呼んでいます。

情報セキュリティポリシーには、社内規定といった組織全体のルールから、どのような情報資産をどのような脅威から、どのようにして守るのかについての基本的な考え方、ならびに情報セキュリティを確保するための体制、運用規定、情報セキュリティ基本方針及び情報セキュリティ対策基準などを記載するのが一般的です。

情報セキュリティポリシーを作成する目的は、企業の情報資産を情報セキュリティ脅威から守ることですが、その導入や運用を通して社員や職員の情報セキュリティに対する意識の向上や、顧客に対する信頼性の向上といった副次的なメリットも得られます。

また、既に情報セキュリティポリシーを導入している企業や組織、これから導入を検討している企業や組織の情報管理担当者として、以下の点に十分留意しなければなりません。

●高度にネットワーク化した情報システムは、情報資産への脅威を招くなど負の側面があるが、適切な情報セキュリティ管理を行うことにより、負の側面よりも大きな利便性を与えるものであることを認識する。
●企業や組織として意思統一され、明文化した情報セキュリティポリシーを策定する。
●企業や組織として情報資産の重要度を分類、評価して、守るべき情報資産のレベルに応じた情報セキュリティ対策を情報セキュリティポリシーに反映する。
●情報セキュリティが「いかに破られないか」という予防の視点のみならず、「破られたときどうするか」という対策の視点も情報セキュリティポリシーに盛り込む。
●情報セキュリティポリシーは、「策定」、「導入」、「運用」、「評価」、「見直し」をひとつの実施サイクルとし、このサイクルを止めることなく実施していく。
●「評価」、「見直し」の手法として、情報セキュリティ全般に関する組織監査や、ネットワークやサーバーの情報セキュリティ監査を取り入れる。
●情報セキュリティポリシーの導入に際しては、ユーザーの教育及び啓発の実施方法を十分に考慮する。

以上のような留意点に基づき、情報セキュリティポリシーの導入や継続的な運用を行うことが必要です。

持ち運び可能なノートパソコンを利用する上での危険性と対策

最近では、外出先でもインターネットが利用できるようなインフラが整ってきたこともあり、持ち運び可能なノートパソコンを利用するケースが増えてきています。しかし、外部に持ち出したノートパソコンに関する情報セキュリティ対策を怠っていたがために、情報の漏洩を起こしてしまった事例が多数報告されています。

企業や組織の情報セキュリティを確保するためには、どのようなリスクがあるかを把握して、適切な対策を実施することが重要です。

外部にノートパソコンを持ち出した場合には、以下のような事例による情報漏洩の危険性が考えられます。

- 喫茶店等へ置き忘れることによるノートパソコンの紛失
- 電車の網棚等へ置き忘れることによるノートパソコンの紛失
- 車上荒らしによるノートパソコンの盗難
- 自宅や外出先にてノートパソコンをインターネットに接続することによるウイルス感染

特に、情報管理担当者として対策を講じておかなければならないのは、機密情報や個人情報の漏洩です。ノートパソコンを外部に持ち出した際の情報漏洩に対するリスクを軽減させるためには、次のような対策が考えられます。

- 盗難、紛失に備えて、持ち運ぶ必要のない機密情報、個人情報は格納しない。
- ハードディスクには、できるだけファイルを暗号化して保存する。
- 容易に推測されにくいログオンパスワードを設定して、他人には利用できないようにする。もしくは、指紋認証などの生体認証付きのノートパソコンを使用するのもよい。ただし、生体認証の情報セキュリティ対策機能は、緊急時の対策用にパスワードによるログオンも可能にしていることが多いため、やはり容易に推測されにくいパスワードを設定しておくことが不可欠であるという認識が大切である。
- 扱うデータの重要性によっては、OS だけでなく、BIOS やハードディスクにもパスワードを設定するなどの方法で、より強固な対策を検討する。

これらの対策は個人のユーザーでは困難なことも多いため、できるだけ情報管理担当者が主体となって企業や組織全体におけるルールを決めておくようにした方がよいでしょう。また、これらの対策はいずれも情報漏洩に対するリスクを軽減するだけのものであり、万全な対策にはなり得ません。やはり外部にノートパソコンを持ち出した場合には、情報セキュリティ上の危険性があるということを念頭に置き、そのことをそれぞれのユーザーに理解させることが大切です。

そして、情報セキュリティポリシーなどで組織全体としてのルールを明確に決めて、ユーザーに順守させることも大切です。以下のようなルールを検討してください。

●持ち出し用の専用のノートパソコンを準備しておいて、あらかじめ上記のような強固な情報セキュリティ対策を施しておく。
●持ち出し専用以外のノートパソコンは、社外への持ち出しを禁止する。
●外部にノートパソコンを持ち出す場合には、事前の申請を義務づける。可能であれば、持ち出す情報の種類（個人情報、機密情報など）や内容（顧客名簿など）、目的も申請させるようにするとよい。
●万一、実際に事件や事故が発生した場合の対処策や責任の所在を明確にし、申請時に確認させる。

■ＢＩＯＳのパスワードとハードディスクのパスワード

ＢＩＯＳとは、Ｂａｓｉｃ Ｉｎｐｕｔ Ｏｕｔｐｕｔ Ｓｙｓｔｅｍの略で、コンピュータの電源を入れたときに最初に起動するプログラムです。また、ＢＩＯＳには、キーボードやマウス、ハードディスク等を制御するプログラムが含まれており、ＯＳがこれらの機器とやり取りするための基本的な機能を提供しています。

ＢＩＯＳパスワードとは、このＢＩＯＳに対して、設定できるパスワードのことで、コンピュータを起動したときにパスワードの入力を要求するものと、ＢＩＯＳの設定変更画面を利用するときにパスワードの入力を要求するものとがあります。コンピュータの起動時にパスワードの入力を要求する場合は、ＯＳのパスワードとは別にパスワードの入力が必要になるため、コンピュータに不正にログオンされる危険性を減らすことができます。また、ＯＳの再インストールなどの操作もできなくなることから、ＯＳのログオンパスワードだけを設定した場合に比べて、１段階上の強固な対策を施すことができるようになります。ただし、ＢＩＯＳのパスワードを忘れてしまった場合には、コンピュータの製造元に依頼しなければ解除できないという問題もあるため、注意が必要です。

ハードディスクのパスワードとは、コンピュータに内蔵されているハードディスクに設定できるパスワードのことです。ハードディスクのパスワードを設定してしまえば、コンピュータが分解されてハードディスクを他のコンピュータにつなげられてしまっても、ハードディスクに保存されているデータを読み取ることは困難になります。

なお、ＢＩＯＳとハードディスクのパスワードについては、使用するコンピュータによって、装備されていなかったり、機能が異なったりすることがありますので、コンピュータの説明書やメーカーのホームページなどで確認してください。

持ち運び可能なメディアを利用する上での危険性と対策

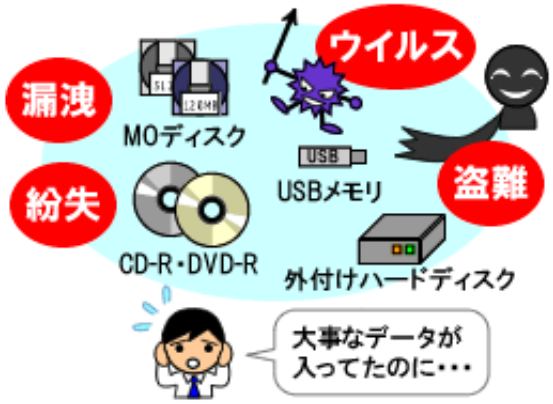
最近、手の中に隠れるほど小さなサイズのＵＳＢ メモリの人気が高まっており、自宅や取引先とのデータのやり取りにUSB メモリを利用するケースが増えてきています。USB メモリは、コンピュータのＵＳＢ 端子に接続するだけで手軽に利用でき、多くのユーザーに支持されています。

しかし、小さくて持ち運びが楽であるため、紛失してしまう危険性が高いという点に注意しなければなりません。また、データをそのままメディアに記録していた場合、紛失時にメディア内の情報が漏洩する危険性が非常に高くなります。もちろん、このことは外付けハードディスク、CD-R、DVD-R、MO ディスクなど、持ち運び可能なメディア全般について言えることです。

最近では、外部に情報を持ち出すことによる紛失や漏洩の事故、ＵＳＢ メモリを媒介としたウイルス感染が多数報告されています。このような事件を起こさないようにするためには、外部に情報を持ち出した際にどのようなリスクがあるかを把握して、リスクに応じた対策を実施することが重要です。

これらの持ち運び可能なメディアを外部へ持ち出した際には、以下のような危険性が考えられます。

- メディアを入れたカバンを置き忘れることにより紛失して情報漏洩
- ワイシャツのポケットなどに気軽に入れておいたために紛失して情報漏洩
- ＵＳＢ 媒介ウイルスによりウイルスに感染
- 自宅のパソコンにデータを移して作業。その後、ウイルスに感染して情報流出



可搬性のあるメディアを利用する際の情報漏洩に対するリスクを軽減するためには、次のような対策が考えられます。

●盗難、紛失に備えて、持ち運ぶ必要のない機密情報、個人情報は格納しない。
●ファイルは、できるだけ暗号化して保存する。
●USB メモリや外付けハードディスクでは、製品に情報セキュリティ対策機能の仕組みやソフトウェアが装備されているものも多いので、外部に持ち出すために利用する場合にはできるだけそのような製品の購入を検討する。
●USB メモリでは、指紋認証などの生体認証付きの機器を企業や組織全体として選択するのもよい。ただし、生体認証の情報セキュリティ対策機能は、緊急時の対策用にパスワードによるログオンも可能にしていることが多いため、他人からは容易に推測されにくいパスワードを設定しておくことが不可欠である。
●すべてのコンピュータの設定を変更して、USB メモリの自動再生機能を停止する。
●USB メモリを差し込んだときには、ファイルを開く前に必ずウイルスチェックを行う。

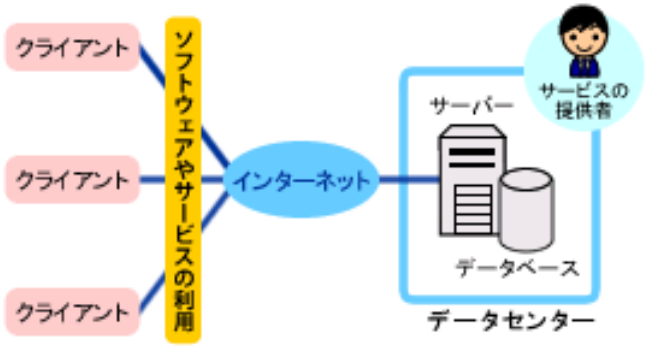
ただし、これらの対策はいずれも情報漏洩に対するリスクを軽減するだけのものであり、万全な対策にはなり得ません。やはり外部にメディアを持ち出した場合には、情報セキュリティ上の危険性があるということを念頭に置いておくことが大切です。

そして、情報セキュリティポリシーなどで組織全体としてのルールを明確に決めて、ユーザーに順守させることも大切です。以下のようなルールを検討してください。

●外部に持ち出すメディアの利用は、上記のような強固な情報セキュリティ対策を施したものだけに制限し、個人のUSB メモリや持ち主の分からないUSB メモリの使用は許可しない。
●メディアを持ち出す場合には、事前申請を行う制度を作ることによって、社員や職員の情報セキュリティに対する認識を高めさせる。
●特別な理由がある場合を除き、基本的にはメディアの利用に何らかの制限をかける。情報セキュリティ対策を重視している企業や組織には、BIOS の設定でUSB 端子を使用できなくしたり、FD ドライブ、CD-R ドライブ、DVD-R ドライブなどの外部メディアへの書き込みを可能にする機器を取り除いたコンピュータを使用したりしている場合もある。

ASP・SaaSを利用する際の情報セキュリティ対策

ASP・SaaSはインターネットを通じてアプリケーションの提供を受けるサービスです。そのため、これまでのパッケージソフトおよび独自に構築していたサービスや業務システムを利用する場合と比較すると、その特性に応じた情報セキュリティ対策が要求されます。



特に注意すべき点は、インターネット回線を利用するということ、自社のサーバー室ではなくサービスの提供者が管理するデータセンターにサーバーを保管するということ、ASP・SaaSのサービス提供者側に運用やデータが依存されるということにあり、これらは利用者にとって情報システムの保守、運用、管理に関する負担が軽減される等のメリットがある一方で、情報セキュリティ対策がASP・SaaSのサービス提供者に大きく依存することになります。

そのため、ASP・SaaSを利用する際には、そのサービス提供者が主に以下のような情報セキュリティ対策を継続して適切に行っているかどうかをきちんと確認した上で選定する必要があります。

サービス提供者が行うべき主要な情報セキュリティ対策（「ASP・SaaSにおける情報セキュリティ対策ガイドライン」より）

- データセンターの物理的な情報セキュリティ対策（災害対策や侵入対策等）
- データのバックアップ
- ハードウェア機器の対策
- OS、ソフトウェアの対策
- OS、ソフトウェア、アプリケーションにおける脆弱性の判定と対策
- 不正アクセスの防止
- アクセスログの管理
- 通信の暗号化

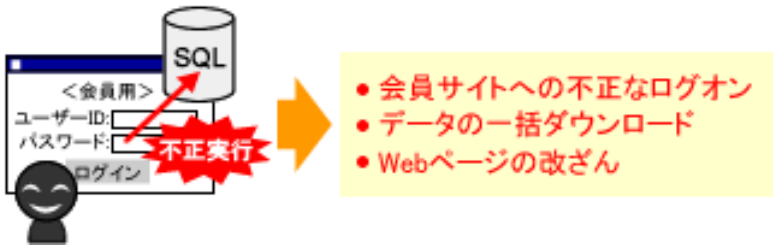
これらの対策内容については、利用するサービスや業務システムの機密性や可用性の要求レベルによって、必要となる項目やレベルが異なります。利用するASP・SaaSの内容や利用方法、そこに格納されるデータの重要性、機密性等をしっかりと検討して、十分な情報セキュリティ対策を行っている事業者やサービスを選定するようにしてください。

なお、総務省ではASP・SaaSの情報セキュリティ対策に関する研究会を開催しています。研究会に関する情報や成果物については、以下のリンクから報告書やガイドライン等を参照してください。

また、FMMC（財団法人マルチメディア振興センター）では、「ASP・SaaS　サービスの安全・信頼性に係る情報開示認定制度」を運営しています。これは、ASP・SaaSサービスの利用を考えている企業や団体などが事業者やサービスを比較、評価、選択する際に必要な「安全・信頼性の情報開示基準を満たしているサービス」を認定するものです。

SQLインジェクションへの対策

企業や組織のホームページやショッピングサイトなどでデータベースを利用したWeb アプリケーションを公開している場合には、SQL インジェクションへの対策が大切です。SQL インジェクションは、Web サーバーを経由したデータベース接続を利用した攻撃方法です。



SQL インジェクションへの対策を行っていないWeb サイトでは、例えばログオン画面でパスワードの欄に不正なデータベース命令を実行するための文字列を入力することで、パスワードを知らなくてもそのユーザーとしてログオンし、クレジットカード番号などの個人情報を取得されてしまうことがあります。また、別の方法によって、データベースに格納されているデータを一括で取り出されてしまったり、データが不正に改ざんされたりすることもあります。最近は、このような手法による個人情報の漏洩事件が相次いで発生しています。

また、SQL インジェクションを利用した特殊な命令によって、サーバー上のファイルを書き換えることで、Web ページが改ざんされてしまう事件も発生しています。書き換えられたWeb ページでは、多くの場合、訪問者には分からないような状態（表面上は正規サイトがそのまま表示される）で、ユーザーを悪質なWeb サイトに誘導したり、iframe タグで埋め込んだ別のWeb サイトからウイルスに感染させたりすることが多いようです。

自社のWeb サーバーでデータベースと連携したプログラムを利用している場合には、開発担当者または委託先の業者に必ず以下のような対策を講じるように依頼してください。

- Web サーバー上のプログラム（スクリプト）でSQL インジェクション対策（不正な入力値による処理を防ぐなど）を行うこと。
- Web サイトにシステムから表示されるエラーメッセージをそのまま表示しないようにすること（攻撃者に対してヒントを与えてしまうことになるため）。
- システムで利用するデータベースアカウントに対しては、最低限の権限だけを設定すること。
- 定期的にアクセスログから攻撃数を検出し、攻撃内容の解析を行うこと。
- 定期的にWeb サイト全体の脆弱性検査を行うこと。

外部の業者に開発、運用を依頼している場合には、ＳＱＬ インジェクションの対策状況について、しっかりと確認しておくことが大切です。また、ツールを利用して外部からの侵入テスト（ペネトレーションテスト）を実施したり、専門の業者にテストや診断を依頼する方法もあります。

何よりも大切なことは、常に情報セキュリティに関する情報を収集して、新しいハッキング方法が公開された場合には、利用しているサーバーで必要な対策を迅速に実施することです。