情報管理担当者のための情報セキュリティ対策－実践編

企業や組織が保有している情報資産を安全に利用するためには、情報管理担当者が中心となって、すべてのユーザーに適切な情報セキュリティ対策を実践してもらうことが大切です。また、組織内のネットワークやサーバーに対する情報セキュリティ対策も、情報管理担当者が担当すべきものです。

ここでは、情報管理担当者が実践すべき情報セキュリティ対策について説明します。

※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。

ファイアウォールの導入

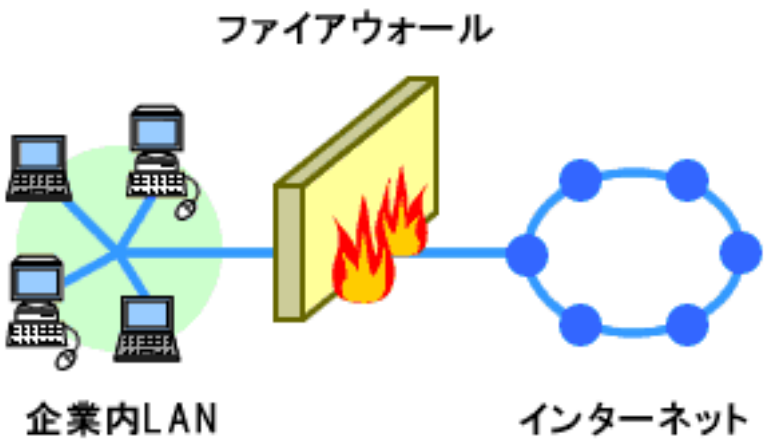
重要!

企業や組織のネットワークに対する不正アクセスから防御するためには、ファイアウォールの導入は欠くことができません。ファイアウォールにはソフトウェアとして提供されているものや、システムが組み込まれたハードウェアとして提供されているものなど、さまざまな種類のものがありますが、いずれの製品であっても、外部からの不正なパケットを遮断する機能や許可されたパケットだけを通過させる機能を持っています。また、最近では、ルーターにファイアウォールの機能が装備されているものが多くなっています。

一般的なファイアウォールは、通過させるパケットや遮断するパケットに対する詳細なルールを設定して利用するため、TCP/IP プロトコルなどに対して、ある程度の知識を必要とします。TCP/IP プロトコルやインターネットについての基本的な知識を習得した上で、適切な状態にファイアウォールを設置することができれば、サーバーの情報セキュリティを一段階強化させることにつながります。

さらに情報セキュリティを強化する場合には、ファイアウォールを二重化したり、ファイアウォール以外に侵入検知システム（IDS）や侵入防止システム（IPS）を導入する方法が考えられます。侵入検知システムとは、外部から送信されるパケットをチェックして、不正アクセスと判断されるパケットが発見された場合には、管理者に連絡する機能を持つシステムです。侵入防止システムは、侵入検知システムの機能に加えて、不正なパケットを自動的に遮断する機能を持ちます。

また、プロバイダが自社の接続サービスやハウジングサービスを利用しているユーザーを対象として、ファイアウォールをサービスとして提供している場合もあります。そのサービスの内容は、ウイルス対策機能を含めた統合的なセキュリティサービスなど、プロバイダによって異なります。ファイアウォールのサービスの提供の有無や、サービスの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、プロバイダに問い合わせてください。



セキュリティ診断

セキュリティ診断を実施することで、サーバーやネットワークの持つ脆弱性を発見することができます。セキュリティ診断にはいくつかの方法がありますが、もっとも確実な方法はコンサルタントによる診断サービスを依頼することです。

一般的なセキュリティ診断サービスは、外部からの診断と内部からの診断の 2 通りのサービスを用意しています。外部からセキュリティ診断は、インターネットから擬似的にアタックを試みるものが多く、攻撃に利用される可能性のあるセキュリティホールなどを発見するのに役立ちます。内部からのセキュリティ診断は、主にネットワーク全体のセキュリティ強度を診断することを目的していて、事前に依頼者が提供したネットワークやサーバーの情報を元にして、さらに詳細な診断を実施します。

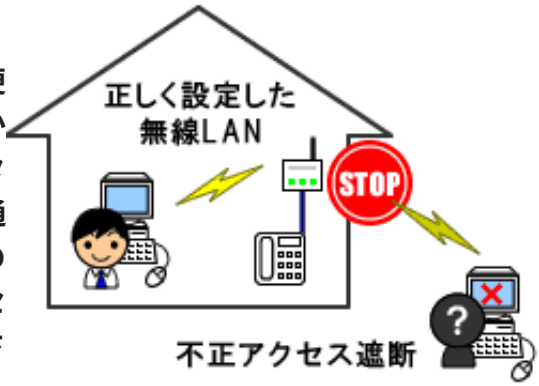
外部からのセキュリティ診断は、対象とするサーバーのグローバル IP アドレスを通知するだけで、すぐに依頼できるものもありますが、内部からのセキュリティ診断は、ネットワークやサーバーの情報をコンサルタントに提供しなければならないため、手間と時間が掛かります。

これらのセキュリティ診断によって、設置したサーバーのセキュリティ強度が確認でき、さらに強化すべきポイントを明確にすることができます。

なお、これらのセキュリティ診断は一般的には有料のサービスとして提供されていますが、コンサルタント会社によっては、一定レベルの診断までは無料で実施してくれることもあります。また、予算が取れない場合には、インターネットで公開されているフリーウェアの診断ツールを入手して、自分で最低限のチェックを試みる方法も検討してみましょう。

安全な無線LANの利用

重要!



無線LANは、レイアウトの変更が容易であるなどの利便性から、オフィスにおいても導入が進んでいます。しかし、無線LANは無線を利用するという性質上、機密データや顧客データを持つ企業や組織で利用するためには、通信内容の傍受（盗聴）や不正利用、アクセスポイントのなりすまし等の危険性を十分認識し、できる限りのセキュリティ設定を行った上で利用するようにしてください。

無線LANを安全に利用するためには、暗号化の設定を行ってください。現時点では、WPA-PSK方式またはWPA2-PSK方式による暗号化を推奨します（WPA2-PSK方式の方が、より強固な暗号化技術です）。パスワードの設定に関しては、「パスワード管理の推奨」を参照してください。また、文字数は21文字以上としてください。

無線LANの暗号化方式としては、旧来からWEPという方式がありますが、近年WEP方式を短時間で解読する手法が発見されたという調査結果も発表されており、必ずしも安全ではありません。
パスワードは、無線LANのネットワーク識別子であるSSIDから類推できるようなものにしないよう注意が必要です（SSIDは一般的に公開されて使用されているため）。

なお、以下の設定を行うことで、第三者からの不正なアクセスを受けにくくなります（ただし、これらの設定は、無線LANの安全性を保証するものではありません）。

- MACアドレスによるフィルタリングを設定し、接続するクライアントを制限する。
- SSIDを隠す機能（ステルス機能）を利用する。

上記設定については機種に依存するため、無線LANのアクセスポイントに付属しているマニュアルを参照してください。

また、現在はセキュリティ機能を強化した無線LAN機器が普及していますので、新たに導入を検討しているのであれば、そのような機器を購入することをお勧めします。

全コンピュータに対するウイルス対策

重要!

組織内のコンピュータをウイルスから防御するためには、ネットワークに接続するすべてのクライアントおよびサーバーに対して、ウイルス対策を実施しなければなりません。その際には、以下のことに注意してください。

■ウイルス検知用データの更新

すべてのコンピュータにおいて、ウイルス対策ソフトがインストールされているだけでなく、常に最新のウイルス検知用データに更新されるようにしなければなりません。そのためには、すべてのコンピュータにおいて、ウイルス検知用データの更新の設定を正しく行うことが必要です。

また、ウイルス対策ソフトによっては、サーバーからすべてのクライアントにウイルス検知用データを自動的に配信するためのソフトウェアがオプションとして販売もしくは提供されていることもあります。詳しくは、導入しているウイルス対策ソフトのメーカーに問い合わせてください。

ヒント

ウイルス検知用データは、ウイルス対策ソフトによって、パターンファイル、ウイルス定義ファイルなどの名前で呼ばれています。

■ウイルス検知用データの契約更新

ウイルス対策ソフトのウイルス検知用データは、メーカーとの契約に基づいてユーザーに配信されます。そのため、すべてのコンピュータにおいて、ウイルス対策ソフトの契約を継続的に更新しなければなりません。契約方法や契約期間については、導入しているウイルス対策ソフトのメーカーに問い合わせてください。

■定期的なウイルススキャンの実行

ウイルス対策を万全にするためには、すべてのコンピュータで定期的なウイルススキャンを実行することが大切です。ほとんどのウイルス対策ソフトでは、指定したスケジュール（毎週金曜日の夜 8 時など）で、システム全体に対するウイルススキャンを実行することができるようになっています。

クライアントの場合には、そのコンピュータを使用しているユーザーに、自分のスケジュールに合わせたスケジュール設定を推奨しておくとよいでしょう。また、サーバーの場合には、深夜や早朝など、ユーザーが利用していない時間帯にウイルススキャンを実行しておくように設定しておきましょう。

■個人のコンピュータのネットワークへの接続

ネットワークに接続されているすべてのコンピュータにウイルス対策ソフトが導入されていたとしても、ウイルス対策ソフトが導入されていない個人のコンピュータが、後からネットワークに接続されてしまうと、ネットワークに接続している他のコンピュータやサーバーにウイルスが感染してしまうことがあります。

そのためには、情報セキュリティポリシーに個人のコンピュータを接続することに対するルール（接続の禁止、またはウイルス対策ソフトの導入されていないコンピュータの接続の禁止）を記載して、組織内にルールを徹底することが大切です。

■ウイルス対策サービスの利用

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。

なお、ウイルス対策サービスを利用する場合であっても、個人のコンピュータをネットワークに接続する場合には、事前にウイルススキャンを行なうなどの対処が必要です。

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。

情報資産のバックアップ

重要!

企業や組織内の情報資産に対する可用性を維持するためには、保有している情報に対する適切なバックアップが必要です。情報管理担当者には、コンピュータやネットワークの障害、システムの操作ミスなどが発生した場合にも業務にできる限り影響を与えない、迅速に復旧可能なバックアップ運用が要求されています。

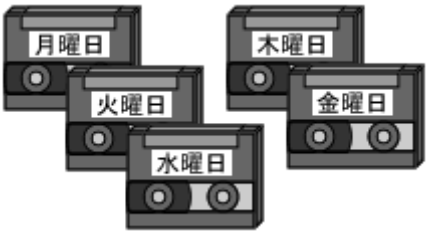
企業や組織内において、情報管理担当者が情報のバックアップとして行うべきことは主に2つあります。ひとつめは、共有データのバックアップで、もうひとつは各個人の持つデータのバックアップです。

まず、情報セキュリティポリシーにバックアップの方法や頻度を組織内のルールとして、明確に記載しておくとよいでしょう。

■サーバーのバックアップ

データベースサーバーやファイルサーバーに格納されている共有データは、情報管理担当者が責任を持ってバックアップしなければなりません。通常、サーバー上のデータは、DATやDLT、AITといったテープメディアにバックアップします。

バックアップを実行するためには、OSに装備されているバックアップユーティリティや専用のバックアップツールを利用します。なお、サーバーのバックアップは、OSやバックアップツールの持つスケジューリング機能を利用して、ユーザーが操作を行わない深夜や早朝などに実施します。



■バックアップの指示

社員や職員が各クライアントに保存しているデータも、大切な情報資産のひとつです。そのため、組織内のユーザーに対しても、各クライアントに保存されている情報のバックアップを指示しなければなりません。その際には、バックアップの保存先（メディアやバックアップサーバーなど）、使用するバックアップツールや方法、バックアップの頻度など、各ユーザーの持つ情報資産の重要度をきちんと把握して、適切なアドバイスや方法を具体的に行う必要があります。

注意

ユーザーがバックアップに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。

コンピュータやメディアの廃棄

重要!

最近、廃棄されたコンピュータやメディアから情報が漏洩するという事件が発生しています。そのため、コンピュータやメディアを廃棄する場合には、記憶されているデータを復元不可能な方法で抹消しなければなりません。コンピュータやメディアを廃棄する際に、以下の方法を検討してください。

●データ消去用のソフトウェアを利用する。
データ消去用のソフトウェアを使用すると、ハードディスクやメディアのファイルを復元できないように完全に消去することができます。なお、データ消去用のソフトウェアは、パソコンショップや家電販売店などで販売されています。

●専門業者のデータ消去サービスを利用する。
サービスを提供している業者は、インターネットの検索エンジンで探すことができます。「データ消去サービス」などのキーワードで検索してください。

●ハードディスクやメディアを物理的に破壊する。
ただし、ハードディスクの場合には、外側のケースだけを破壊しても、中にあるディスクが破損していない場合には、ディスクを取り出してデータを復元することも可能なので注意してください。なお、FD や MO、CD、DVD などの記憶媒体については、メディアを破壊するために利用できるメディア専用のシュレッダが販売されています。

専門業者に依頼する場合には、できる限り、依頼先の会社の信頼度やその会社におけるプライバシーポリシーのあり方にも考慮して選定しなければなりません。

また、コンピュータを修理する場合にも、作成したドキュメントや電子メールなどのデータを消去してから依頼するようにしましょう。

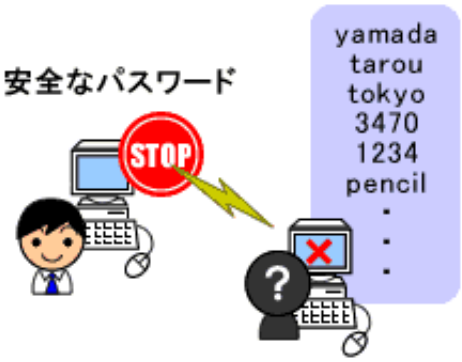
なお、コンピュータやメディアの廃棄については、全社員、全職員における徹底した対策が必要です。そのためには、以下のように実施することが理想的です。

●コンピュータやメディアは各個人や部署で廃棄せずに、必ず情報管理担当者が回収してから廃棄するようにする。

●廃棄におけるルールを情報セキュリティポリシーに明確に記載する。

適切なパスワード管理の推奨

重要!



各ユーザーが自分のコンピュータにログオンしたり、企業や組織のネットワークに接続したり、業務データが格納されているデータベースシステムにログオンしたりする際において、なりすましを防ぐための情報セキュリティ対策には、一般的にパスワードが利用されています。

企業や組織の情報管理担当者にとって、組織内の情報資産にアクセスする可能性のあるすべてのユーザーに対して、適切なパスワード設定を指導することも、重要な情報セキュリティ対策のひとつです。

そのためには、パスワード管理について、主に以下のことを心がけなければなりません。

- 「個人情報からは推測できない」や「英単語などをそのまま使用しない」などの条件を満たす安全なパスワードの作成を推奨する。
- 「パスワードは同僚や部下であっても教えない」、「パスワードを記載したメモを貼り付けない」などのパスワード管理のルールを徹底する。
- 初回および再発行時のパスワードの発行方法を適切な形でルール化する。
- パスワードを定期的に変更するように指導する。可能であれば、クライアントの設定またはドメインの設定によって、一定期間ごとに強制的に再設定するようにしておくとよい。また、サーバーのパスワードの世代管理機能を導入すると、パスワードの変更時に以前のパスワードを使用できないようにすることもできる。

これらのパスワード発行手順および管理方法については、明確にルールを策定して、情報セキュリティポリシーに記載しておくことが理想的です。その上で、パスワードの作成方法や管理方法について、情報セキュリティポリシーに基づいた教育を実施することで、企業や組織内にルールを浸透させることが大切です。

ヒント

現在の一般的なＯＳのスクリーンセーバーでは、元の操作画面に復帰する際にパスワードの入力を促す設定を行うことができます。このように設定することで、離席中に不正なユーザーがそのコンピュータを操作することを防ぐことができるようになります。

サーバー室の情報セキュリティ対策

サーバー室でサーバーを集中管理する場合には、適切な情報セキュリティ対策を実施していないと、人の出入りが少ない分だけ、逆に情報セキュリティ上の問題が大きくなってしまうことがあります。

サーバー室を設置した場合には、以下のような点を検討してみましょう。

●鍵の管理や入退室時間を記録するなど、サーバー室に対する入退室の方法とルールを明確に決定する。
●業者などが出入りする場合のルールを決定する（必ず担当者が付き添うなど）。
●サーバーは、使用後に常にログオフしておくようにルールを徹底する。
●可能であれば、カメラの設置を検討する（抑止効果がある）。

なお、これらのサーバー室の利用方法については、情報セキュリティポリシーに記載して、関係者にルールを徹底するようにしておくとよいでしょう。

不正アクセス防止対策促進に関する優遇措置

法人または個人事業者における不正アクセス対策に対して、以下のような税制支援を行っています。

■情報基盤強化税制

対象：

国税（所得税、法人税）

適用期間：

平成18年4月1日から平成20年3月31日までの取得等（2年間）

対象とする設備：

ISO/IEC15408に基づき評価・認証を受けた

1）サーバー用オペレーティングシステム又はこれがインストールされたサーバー

2）データベース管理ソフトウェア又はその機能を利用するアプリケーション

3）ファイアウォール（　1）又は2）と同時に設置する場合に限る）

■ネットワークセキュリティ維持税制

対象：

地方税（固定資産税）

適用期間：

平成18年4月1日から平成20年3月31日まで（2年間）

対象とする設備：

ネットワークセキュリティ維持装置（対象の情報システムについて、情報通信ネットワークにおけるセキュリティ脅威から情報システムを防護するために必要な電気通信設備）であって、取得価格250万円以上のもの。