総務省 安心してインターネットを使うために

国民のためのサイバーセキュリティサイト

情報管理担当者の情報セキュリティ対策

情報管理担当者は、情報セキュリティポリシーで定めた事項が組織全体で実際に実行されるように、情報システムの管理・運用や、社員・職員に対する教育・監督を適切に行う必要があります。また、情報通信技術の進歩は早く、企業・組織の情報資産を脅かす新しい脅威が次々に登場しています。よって、情報管理担当者には、これらの脅威について情報を収集し、必要に応じて組織幹部や外部の専門家とも連携しながら、継続的に組織全体の情報セキュリティ体制を見直していく役割も期待されています。

ここでは、企業・組織における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。

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。

情報管理担当者の情報セキュリティ対策

【技術的対策】

【情報セキュリティポリシー】

【物理セキュリティ】

ソフトウェアの更新

ソフトウェアを導入する際には、その時点での最新版を使用することが適切な対応ですが、時間の経過とともに新たな脆弱性（ぜいじゃくせい）が発見されるため、情報管理担当者はソフトウェアを常に最新にする対応を行う必要があります。

ソフトウェアの開発元やシステム機器メーカーから、ソフトウェアに対する更新プログラムが配布されることがあります。更新の内容には、ソフトウェアへの機能の追加・修正や、脆弱性の修正などがありますが、特に脆弱性の修正に関するものについては日々注視しておく必要があります。

脆弱性の修正に関する更新が発表されたときは、まず自分が管理するシステムについての影響や緊急性を検討します。特に、外部に広く公開しているWebサーバなどに深刻な脆弱性が発表されたときは、迅速な判断と対応が求められます。不正アクセスなどの被害を受けないよう、事前に行うべきことや作業の手順を確認し、可能な限り迅速に更新プログラムを適用しましょう。

また、脆弱性を有することのみが先に発表され、メーカーなどが修正プログラムを作成するまでに時間を要することもあります。そのような場合は、修正プログラムが発表されるまでの間は、一時的回避策を適用してシステムを保護し、修正プログラムが発表された後に脆弱性の修正対応を行うようにしましょう。

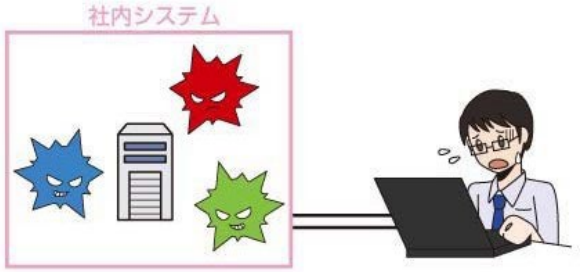
脆弱性対応で慌てないために、常日頃からソフトウェア開発元、メーカーの脆弱性に関するサポート情報や、国内外の脆弱性情報に関する調整機関の発表に注意し、迅速な対応を行えるように意識しましょう。

なお、基幹業務で使用しているサーバでは、止められないなどの理由によりソフトウェアの更新が先延ばしにされがちです。このようなサーバがサイバー攻撃を受け、長期間の業務停止や休業を強いられる可能性があるため、安易な先延ばしを行わないようにしましょう。場合によっては、更新作業が日常の業務に影響する場合も考えられますが、組織幹部の判断を仰ぐなどして対応することが必要です。

参照 脆弱性（ぜいじゃくせい）とは？（基礎知識）

ウイルス対策

最近は、組織内のネットワークを介して、ファイルサーバやWebサーバ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台のパソコンがウイルスに感染しただけで、組織内のパソコン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、前項の通りサーバ、クライアントを問わず、全てのパソコンのOSやソフトウェアをアップデートし、既知の脆弱性が残らないようにします。

加えて、必要に応じてウイルス対策ソフトを導入します。導入した場合は、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、同時にこれを全ての利用者に指導しなければなりません。その上で、怪しいホームページは閲覧しないようにさせる、怪しい添付ファイルは開かないなどの対策と、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利用者に連絡して、ウイルス感染防止に努めてください。

それでも、ウイルス感染が発生してしまったときには、利用者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、感染したパソコン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、他のパソコンやサーバ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。

利用者ひとりひとりのパソコンや、数多くのサーバをウイルスから防御するためには、単純に全てのクライアントやサーバ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、全てのクライアントやサーバ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。

ウイルス対策を実施する際には、管理者として以下のことに注意してください。

■ 個人のパソコン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全てのパソコン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パソコンが、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パソコンやサーバ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パソコン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パソコンの接続の禁止など）を記載して、組織内にルールを徹底することが大切です。

また、ウイルス対策ソフトでも、パソコンウイルスを防げないことがあります。新種のウイルスは、検知データにないために検知ができないことがあるからです。

また、自分の組織でウイルス対策をしていても、インターネット経由で取引先やパートナーなどからの感染、標的型攻撃からの感染などもあります。

管理者としては、ウイルス対策ソフトを導入し運用するだけでなく、プロキシやファイアウォール、侵入防止システム(IPS)などのログの確認などを併せて行うようにしましょう。ウイルス対策ソフトで検知できなかった場合も、これらの確認から感染に気づくことができる場合があります。

もし、ウイルスに感染してしまった場合の対策なども、「まず、ネットワークケーブルをはずし、無線LANをOFFにする」「電源は切らない」「その後、管理者に連絡する」など、組織でどのような手順になっているか確認をしておきましょう。

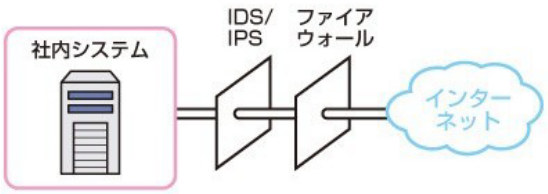
参照 ウイルスとは（基礎知識）
ウイルスに感染しないために（基礎知識）

ネットワークの防御

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。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。

ファイアウォールは、通過又は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サーバの情報セキュリティを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）を導入したりする方法があります。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っています。



また、インターネットサービス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の契約者を対象として、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、インターネットサービス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、インターネットサービスプロバイダのホームページで確認するか、インターネットサービスプロバイダに問い合わせてください。

参照 ファイアウォールの仕組み（基礎知識）

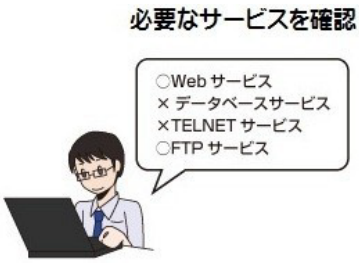
不正アクセスによる被害と対策

外部から不正アクセスを受けると、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。
- サーバ内に保存されていたデータが外部に送信される。
- サーバのシステムが破壊される。
- サーバやサービスが停止してしまう。
- 迷惑メールの送信や中継に利用される。
- 他のパソコン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、管理下のサーバで稼働しているサービスを把握し、各種設定が適切であるか確認を行い、必要なセキュリティ機能を導入し対策を行うことが重要です。

サーバで利用するサービスの確認



確認しなければならない代表的なサービスとして、ネットワークを介してサーバを遠隔操作できるTelnetなどのリモート接続サービスと、パソコン間でのファイルの転送に利用されるFTPがあります。これらのサービスは、ホームページの改ざんや不正侵入などにも利用されやすいものですので、自分で管理しているサーバでこれらのサービスが不要であればサービスを停止します。サービスを利用する必要がある場合は、アカウントを厳重に管理し、アクセス制御を適切に設定することが大切です。

また、最近はこれらに替わって通信路の暗号化を行うSSH、SFTPなどが利用されるようになってきていますが、ポリシーに応じて適切な認証方式を選択し、アクセス制御を確実に行うようにしましょう。

ソフトウェアの更新

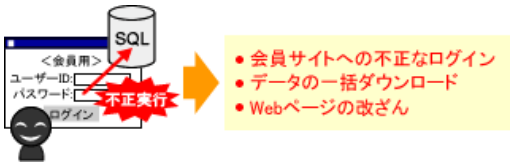
自分が管理するシステムに関して、ソフトウェアの開発元やシステム機器メーカーから、脆弱性（ぜいじゃくせい）の修正に関する更新が発表されることがあります。このときは、まず自分が管理するシステムについての影響や緊急性を検討します。特に、外部に広く公開しているWebサーバなどに深刻な脆弱性が発表されたときは、迅速な判断と対応が求められます。不正アクセスなどの被害を受けないよう、可能な限り迅速に更新プログラムを適用しましょう。

■ パーミッションを正しく設定

パーミッション（ディレクトリやファイルへのアクセス権限）を設定して、収集した情報を保存しているファイルには、インターネットから接続する利用者がアクセスできないようにしなければなりません。実際に発生している個人情報の漏洩（ろうえい）事件の多くは、このパーミッションの設定を怠ったことが原因となっています。

■ SQLインジェクションへの対策

インターネット上のWebサーバ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は、SQLインジェクションへの対策が必要です。SQLインジェクションは、悪意を持った攻撃者が特殊な文字列をWebサーバに入力することでWebアプリケーションに本来はあり得ない動作をさせて、データベースに保存されているデータを盗み出す攻撃手法です。



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。対策としては、利用者から受け付けた入力をチェックすることが基本ですが、ウェブアプリケーションファイアウォール(WAF)の導入も有効な手段と言えます。

■ ファイアウォールや侵入防止システム(IPS)の導入

守るべきサーバの外側にファイアウォールを導入することで、インターネット側からの不要な通信をブロックしたり、実際に行われた通信の記録を取ることもできます。また、IPSを導入することで、インターネットとの通信内容を監視し、不正に侵入を行おうとする通信や、ソフトウェアの既知の脆弱性を狙った攻撃と言える通信を防御することができます。

さらに、自分が管理するネットワークのセキュリティレベルを維持するためには、ファイアウォールやIPSの導入を行った後にも、適宜ログを確認したり、システムが発するセキュリティ警告などの内容を確認して、必要な対応を行っていくことが重要です。このような日常の運用にかかるコストも考慮して導入を計画しましょう。

■ 機器構成の変更やソフトウェアのインストール制限

社員や職員が、勝手にクライアントパソコン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。利用者が許可されていないソフトウェアを勝手にインストールすると、ソフトウェアの管理が適切に行えないばかりか、それが脆弱性に直結することもあります。

■ モバイル機器の適切な管理

モバイル端末には社内システムのユーザ名やパスワードを記憶させないようにしましょう。社員や職員がモバイル機器を紛失しても、すぐにそのユーザ認証情報を変更することで、不正アクセスなどの危険から情報資産を守ることができます。次項にて説明しているMDMの導入も有効です。

このような情報セキュリティ対策を通して、不正アクセス被害の可能性を減少させましょう。

テレワークで業務用端末を利用する場合の対策

テレワークの導入等で、社員や職員にノートパソコンなどの業務用端末を自宅や外出先で利用することを許可する場合、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（ろうえい）についてです。情報漏洩（ろうえい）のリスクを軽減させる対策は、職員個人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べきです。

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、職員に徹底させることも大切です。たとえば、以下のようなルールを検討してください。

- 持ち出し専用の端末を別途準備し、あらかじめ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、通常オフィスなどで利用する端末よりも強固な情報セキュリティ対策を施しておく。
- 持ち出し用端末についても、ソフトウェアの更新やウイルス対策ソフトの導入・更新などのメンテナンスを適切に行う。
- ハードディスクのデータを暗号化して利用する。
- 持ち出し用以外の端末は、原則社外への持ち出しを禁止する。
- 外部に端末を持ち出す場合には、事前の申請を義務づける。さらに、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。
- 万一、実際に事件や事故が発生した場合の対処方法や責任の所在を明確にし、申請時に確認させる。

また、パソコンの紛失や盗難によって情報漏洩（ろうえい）を引き起こさないための技術的な対策として、シンクライアントや仮想デスクトップの利用も検討しておきましょう。

シンクライアント / 仮想デスクトップの利用

シンクライアントとは、ソフトウェア管理やデータ処理をサーバ側に集中させて、利用者が使う端末には必要最小限の処理をさせるシステムです。利用者の端末で処理をしているように見えますが、実際はサーバ上でデータを処理・保管しており、その画面を利用者の端末に転送して表示しているのです。

同じような仕組みに、仮想デスクトップがあります。仮想デスクトップは、仮想化技術を用いて、サーバ上で複数のデスクトップ環境を実行させる技術です。利用者はシンクライアント端末などから、ネットワーク経由で企業・組織のサーバに接続し、自分のデスクトップ画面を呼び出して利用します。

シンクライアントや仮想デスクトップ技術を使うことにより、社員や職員が使うパソコン本体に重要情報を保存しないようにすることができるため、紛失時などの情報漏洩（ろうえい）対策に効果的です。また、ソフトウェアをサーバ側で一元的に管理するため、更新などのメンテナンスが行き届くという点も、情報セキュリティ対策として有効です。

この他、社員・職員が業務でスマートフォンを利用する機会も増えてきました。スマートフォンは、パソコンに比べて紛失する危険性が高いため、紛失した場合のリスクに備えることがいっそう必要になっています。

企業・組織では、MDM（Mobile Device Management：モバイルデバイス管理）というシステムを使って、スマートフォンなどの携帯情報端末を効率的に管理する仕組みを導入することも有効な手段です。一般的にMDMでは、携帯情報端末のソフトウェアの更新を一元管理したり、端末で利用できる機能を制限するなどして情報セキュリティを強化しているほか、GPS機能を使ってスマートフォンの位置を検索したり、遠隔操作で端末のロックや内部データの消去などを行うことのできる機能も提供されています。

その他、テレワークにおけるセキュリティ対策については、こちらのサイトも参考にしてください。

テレワークにおけるセキュリティ確保
https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/index.html

【コラム】BIOSのパスワードとハードディスク・SSDの暗号化

BIOSとは、Basic Input Output Systemの略で、パソコンの電源を入れたときに最初に起動するプログラムです。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、パソコンの起動にパスワードが要求されます。パソコンにログインするためのパスワードとは別にパスワードが必要になるため、パソコンに不正にログインされる危険性を減らすことができます。ただし、BIOSのパスワードを忘れてしまった場合には、パソコン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・SSDの暗号化は、パソコンに内蔵されているハードディスク・SSD上のデータを暗号化する機能です。ハードディスク・SSDの暗号化を設定してしまえば、パソコンが分解されてハードディスク・SSDを抜き取られてしまっても、他のパソコンでデータを読み取ることは困難になります。

なお、これを採用した場合、将来ハードディスク・SSDを廃棄する際に、暗号化消去（後述）が利用できるようになります。

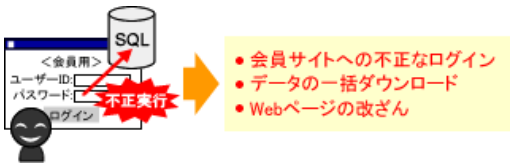
なお、BIOSのパスワードとハードディスク・SSDの暗号化については、使用するパソコンによって装備されていなかったり、機能が異なったりすることがありますので、パソコンの説明書やメーカーのホームページなどで確認してください。

SQLインジェクションへの対策

多くの企業や組織のホームページやショッピングサイトは、データベースを利用したWebアプリケーションが使われています。このような場合には、Webサーバ経由でのデータベース接続を利用した攻撃方法であるSQLインジェクションへの対策が必要です。

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、例えばログイ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い攻撃者が正当な利用者としてログインし、クレジットカード番号などの個人情報を窃取したりすることがあります。

また、別の方法によって、データベースに保存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（ろうえい）事件が相次いで発生しています。



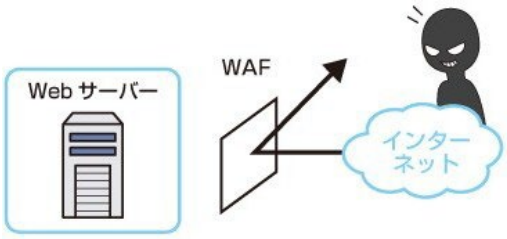
また、SQLインジェクションを利用した特殊な命令によって、サーバ上のファイルを書き換えることで、Webページが改ざんされてしまう事件も発生しています。書き換えられたWebページでは、多くの場合、訪問者には分からないような状態（表面上は正規サイトがそのまま表示される）で、利用者を悪質なWebサイトに誘導したり、iframeタグで埋め込んだ別のWebサイトからウイルスに感染させたりすることが多いようです。

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、開発担当者又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、最小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（ぜいじゃくせい）検査を行うこと。

また、ウェブアプリケーションファイアウォール（WAF）を利用するのも、有効なSQLインジェクション対策となります。

WAFは、Webアプリケーションのやり取りを把握・管理することによって不正侵入を防御することのできるファイアウォールのことで、従来のファイアウォールがネットワークレベルでの管理であるのに対し、WAFはWebアプリケーションのレベルで管理を行います。WAFでは、プログラムに渡される入力内容などを直接に検査することで、不正と見なされたアクセス要求を遮断することができます。Webブラウザと Webサーバを仲介するかたちで、Webブラウザとの直接的なやり取りをWAFが受け持つことで、SQLインジェクションなどの不正な要求に対して、「攻撃」と見なして通信を遮断することができます。



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したり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、新しい攻撃方法が公開された場合には、利用しているサーバで必要な対策を迅速に実施することです。

参照 事例8：SQLインジェクションでサーバの情報が・・・

標的型攻撃への対策

標的型攻撃は、機密情報を盗み取ることなどを目的として、特定の個人や組織を狙った攻撃です。業務関連のメールを装ったウイルス付きメール（標的型攻撃メール）を、組織の担当者に送付する手口が知られています。従来は府省庁や大手企業が中心に狙われてきましたが、最近では地方公共団体や中小企業もそのターゲットとなっています。

標的型攻撃は、狙われた組織向けに巧妙に作り込まれているため、完璧な防御対策を立てることは困難であるのが現状です。被害を最小限に抑えるためには、攻撃の侵入を防ぐための対策、侵入された場合にすばやく検知するための対策、検知した場合にすばやく対処するための対策をバランスよく行うことが重要です。以下で紹介するような、さまざまな対策を組み合わせて、多層的な対策を行うようにしましょう。

■ 入口対策（攻撃の侵入を防ぐ対策）

ウイルス付きのメールを入口段階で阻止し、情報システムを保護するには、まず基本の対策としてメールのフィルタリングサービスやウイルス対策ソフトを利用することが必要です。しかし、標的型攻撃メールに利用されるウイルスは、市販のフィルタリングサービスやウイルス対策ソフトなどに検知されないものも多く、それだけでは十分な対策とは言えません。

標的型攻撃に利用されるウイルスには、実行形式（拡張子が.exe）のものや、組織でよく利用されるソフトウェアの脆弱性を突くものが多いとされています。実行形式の添付ファイルは開かないなどのルールを組織全体で徹底することや、組織で利用するソフトウェアを常に最新の状態にしておくことが重要です。

一方で、昨今、ソフトウェアの脆弱性が発見されても、修正プログラムが作成されるまでに時間を要するケースが見受けられ、その間に未修正の脆弱性を狙った攻撃が行われることがあります。これは、ゼロデイ攻撃と呼ばれ、従来の手法では対応が困難な課題として認識されています。情報管理担当者は、常日頃からソフトウェア開発元や、国内外の調整機関の発表に注意し、最新のソフトウェアの脆弱性関連情報を入手できる状態を確保しましょう。未修正の脆弱性が発表された場合は、関係機関などが公表する一時的対策を適用するなどしながら、普段以上に、攻撃に対する警戒を怠らないようにしましょう。

最近では、未知のウイルスに対処するため、組織に送られたメールを別の安全な実行環境の中で実行してみて、そのふるまいの危険性を調べるセキュリティ製品なども提供されています。

また、こうしたシステム上の対策と同時に、後で述べる社員・職員の意識向上を通じて、不審なメールを見抜く対策も重要です。

■ 出口対策（侵入後に被害の発生を防ぐ対策）

入口段階で攻撃を防げず、組織にウイルスが侵入してしまった場合にも、組織内から重要な情報が外部に送信される段階で被害を食い止める対策（出口対策）を行うことが重要です。主な出口対策としては、ウイルス感染による外部への不審な通信を見つけて遮断する、サーバやWebアプリケーションなどのログを日常的に取得し、異常な通信を見つけるために定期的にチェックするといった対策があり、侵入の早期発見と迅速な対応のために有効です。特にログの取得は、侵入の発覚

後に被害内容の特定や原因の追及をするために重要な情報源となります。

さらに、万が一データが流出してしまっても、情報にアクセスできないようデータを暗号化しておくなどの対策も重要です。

■ 社員・職員への教育

標的型攻撃による被害を防止するためには、メールを受信する社員・従業員への教育が欠かせません。実際に想定される標的型攻撃のメール文を見せながら、典型的な手口や、開封してしまった場合の対応などを啓発するような教育が効果的です。最近では、社員や職員に擬似的な標的型攻撃メールを送り、教育の効果測定や標的型攻撃への意識向上を図るという方法も使われています。

また、最近の標的型攻撃メールは、フリーメールアドレスを利用して送信されることが増えているので、社員・職員への注意を促すため、フリーメールアドレスからのメールには、LANシステム側でヘッダや本文に注意を促す文言を挿入してから配送する対策も考えられます。

そのほか、送信ドメイン認証（SPF）の認証結果を利用できると、正規のドメインを詐称して送信された不審メールを特定するための手がかりになります。

■ 被害に気づいたときには

上述のような多層的な対策を行ったとしても、標的型攻撃を完全に防ぐことは難しいため、実際に被害を受けた際の対応についても想定しておくことが大切です。まずは、情報セキュリティポリシーなどの中で、社員・職員が異常に気づいた際に、組織内のどの部門に連絡するかなどを事前に決め、定期的に周知するようにしましょう。次に、連絡を受けた部門でも、適切かつ迅速な処理を行えるよう、あらかじめ初動対処について対応方策を定めておき、訓練などを通して事故にそなえるようにしましょう。

感染した端末の特定や流出した情報の確認など、被害状況の把握や、再発防止策の実施にあたっては、外部の専門機関に協力を求めることが必要な場合も多くあります。そのような専門機関との連絡方法についても、事前に初動対処の一環として検討しておくようにしましょう。

参照 標的型攻撃への対策（社員・職員全般の情報セキュリティ対策）

【コラム】送信ドメイン認証技術

迷惑メールや不審メールの多くは、送信元メールアドレスを詐称しています。この対策として考案された技術が、送信ドメイン認証です。送信ドメイン認証は、電子メールの送信者情報のうち、ドメイン部分の正当性確認を目的としています。

送信ドメイン認証技術は、現在は主にSPF(Sender Policy Framework)とDKIM(Domain Keys Identified Mail)の2種類の規格が知られています。SPFは電子メールの送信元のIPアドレスをもとに、DKIMは電子署名をもとに、メール送信者情報のドメインの正当性を評価します。この技術を導入することにより、受信者側はメールの送信者情報(From)やエンベロープ情報から送信元の正当性を確認することが可能になり、なりすましが行われた場合はそれを検出できることになります。

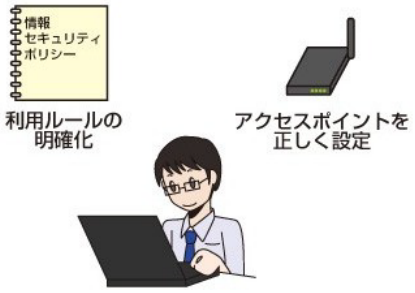
なお、DKIMは、署名するMTA(メール転送エージェント:Mail Transfer Agent)から検証するMTAまで、ほぼエンドツーエンドの完全性を提供します。多くの場合、署名するMTAが送信者に代わりDKIM署名ヘッダを追加し、また、検証するMTAがDNS問合せにより送信者の公開鍵を入手して署名の検証を行うことで、受信者に代わって受信したメールの正当性を確認します。

安全な無線LAN利用の管理

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、オフィスや一般家庭においても従来の有線LANを置き換える形で導入が進んでいます。また、最近では公衆無線LANサービスが普及し、公共施設、駅や空港、カフェやレストランなどでも利用できるようになっています。しかし、無線LANはその性質上、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などの危険性が存在します。

機密データや顧客データを持つ企業や組織で、無線LANを安全に利用するには、情報セキュリティポリシーや利用規定によって、ルールを明確化することが重要です。その上で、適切な情報セキュリティ対策を行った上で社員・職員に利用させることが求められます。

社内や組織内に無線LANのアクセスポイントを設置して運用する場合には、アクセスポイントで適切な暗号化を設定するようにします。現時点では、WPA2方式又はWPA3方式による暗号化が推奨されていますが、WPA3の方がより強固な暗号化方式を利用できます。また、かつて利用されていたWEPという暗号化方式は、脆弱性があるため、利用すべきではありません。



アクセスポイントに設定する管理パスワード、認証・暗号化のための共有鍵は、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安易なものにしないなど、注意が必要です。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。

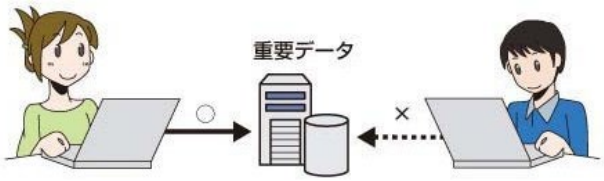
さらに、現在はIEEE802.1X認証への対応など、セキュリティ機能を強化した無線LAN機器が普及していますので、そのような機器を導入することも積極的に検討しましょう。

企業が守るべき無線LANの対策については、以下のリンクも参考にしてください。

参照 無線LANの仕組み（基礎知識）
安全な無線LANの利用（社員・職員全般の情報セキュリティ対策）
企業等が安心して無線LANを導入・運用するために

ユーザ権限とユーザ認証の管理

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、個々の利用者ごとに適切な権限を設定する必要があります。利用者に与える権限は、全ての利用者に全ての権限を与えるのではなく、最低限必要な利用者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。



たとえば、サーバに対しては、アドミニストレータ（管理者）権限やユーザ（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。ある程度の利用者数を持つネットワークの場合には、ユーザ権限を管理するための認証サーバを用意することで、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。

また、ユーザ名とパスワードによるユーザ認証以外に、ICカードによるユーザ認証や、指紋や網膜などのバイオメトリクス（生体情報）を使ったユーザ認証、これらを組み合わせた多要素認証も利用されています。

パスワード管理の推奨

社内の利用者に対して、アクセス権限に応じた個別のユーザアカウントを発行していたとしても、実際にそれぞれの利用者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。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全ての利用者に対して、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。

また、情報管理担当者として利用者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。

利用者数が多く、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、利用者が初めてログインした際に、サーバ側で利用者に強制的にパスワードを変更させるなどの方法を検討しましょう。

利用者からパスワードの再発行依頼があったときには、利用者の本人性の確認が必要になります。電話での問合せに対しそのまま電話で回答するというのでは、ソーシャルエンジニアリングの危険があります。問合せの受付は電子メールで、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。

参照 IDとパスワード（基礎知識）
安全なパスワード管理（社員・職員全般の情報セキュリティ対策）

バックアップの推奨

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、パソコン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の運用が要求されています。

企業や組織内の利用者が安全にパソコン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。クライアントのパソコンでは、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、電子メール、よく利用するホームページのURL、各種の設定などもバックアップさせる対象としておきましょう。

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、明確に記載しておきましょう。

なお、バックアップの方法や保管場所等については、トラブル発生時に復旧できることが重要です。ポリシー策定の際に留意する必要があります。

例えば、オンラインバックアップのみだったのでサイバー攻撃でバックアップも被害を受けてしまった、バックアップを同じサーバ室に保管していたら火災で全て焼失してしまった、などの事態があり得ます。

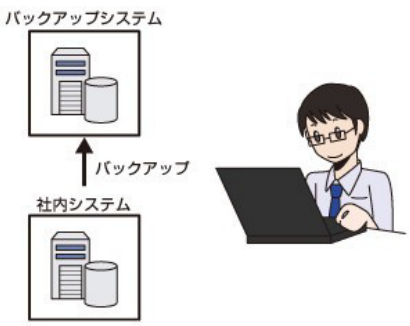
サイバー攻撃、災害等何がおきても、どれかひとつは残るようにするという考え方が重要です。

具体的なバックアップ方法の対策例として以下が挙げられます。

- 物理的な隔離
  オフラインバックアップであれば、バックアップ媒体を遠隔地に輸送して保管する。オンラインバックアップでは遠隔地にあるストレージにバックアップを実施する。これらの方法は特に災害リスクへの対策となります。
- 自動暗号化保存
  バックアップ先にクラウドサービスを利用する場合に、バックアップ先からの情報漏洩リスクを防ぎます。復号化に必要な鍵は安全に保管する必要があるのはもちろんです。
- ネットワーク上の隔離
  オンラインでバックアップを実施する場合は、サイバー攻撃リスクを考慮して、バックアップ先はネットワーク的に分離できることが重要です。安易に同一ネットワーク上にバックアップシステムを接続すると、共倒れのリスクが高まります。

これら以外の対策も含めて、企業・組織の実情に応じて複数のバックアップ手段を組み合わせて、リスク低減を図ることが重要です。

また、平時からバックアップを戻す訓練を実施しておくことも推奨されます。



サーバ上のデータのバックアップ

データベースサーバやファイルサーバに保存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。

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ソフトを利用します。なお、サーバのバックアップは、OSやバックアップソフトの持つスケジューリング機能を利用して、利用者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、組織内の利用者に対しても、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など）、使用するバックアップソフトや方法、バックアップの頻度など、各利用者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。

利用者がバックアップに外部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（ろうえい）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。

参照 バックアップ（社員・職員全般の情報セキュリティ対策）

セキュリティ診断

セキュリティ診断を実施することで、サーバやネットワークの持つ脆弱性（ぜいじゃくせい）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情報セキュリティ専門家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脆弱性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としていて、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の情報を情報セキュリティ専門家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、WebアプリケーションのSQLインジェクションの脆弱性や、セッションハイジャックの脆弱性の有無などを診断することで、設置したサーバ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、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、自分である程度のチェックを試みる方法もあります。

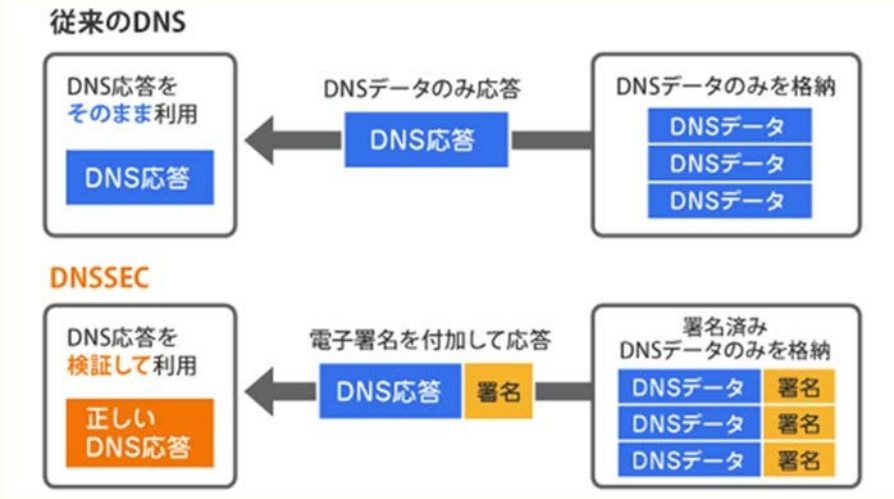
【コラム】DNSSEC

DNS(Domain Name System)は、インターネット上のホスト名とIPアドレスとの対応づけを管理するために使用されるプロトコルです。

DNSはドメイン名とIPアドレスの一意性を保つためにドメインツリー構造を取っています。Webサーバへのアクセスやメールの送受信など、インターネット上の多くのアプリケーションはDNSサービスの存在を前提としていることから、DNSはインターネットの基盤サービスとも言われています。

DNSにはキャッシュする情報を書き換えられる脆弱性（ぜいじゃくせい）があることが知られています。これが正規の通信を不正なコンピュータに誘導するために利用され、フィッシング詐欺などに悪用されることがあります。このような攻撃はDNSキャッシュが汚染されるということから「DNSキャッシュポイズニング」と呼ばれています。

DNSSEC（DNS Security Extensions）は、DNSのセキュリティを向上させるための拡張機能です。DNSSECは、ドメインの権威を持つDNSサーバの応答にデジタル署名を付加することで、正当な権威サーバによって生成された応答であること、また、応答内容が改ざんされていないことを保証します。



2010年7月15日には、世界各地のルートサーバでDNSSECの運用が開始されました。2011年1月からは、日本国内の.jp(ドット・ジェイピー)ドメインでも運用が始まっています。

まずは、自分たちの組織が利用しているインターネットサービスプロバイダやホスティングサービスが、DNSSECに対応しているかを確認しましょう。

ログの適切な取得と保管

外部からの不正アクセスやウイルス感染により、組織内部からの情報漏洩等の事故が発生してしまった場合、そのことにいち早く気づき、被害状況や影響範囲の調査などの事後対応を効果的に行うためには、ログ（通信記録）の取得と保管が重要になります。

そのときネットワークでどのような通信が行われていたか、情報システム内で何が起こっていたかなど、後から追跡調査を行う際にログの解析が役立ち、事故の原因究明や、事後の抜本的な対策を導き出すことにつながります。

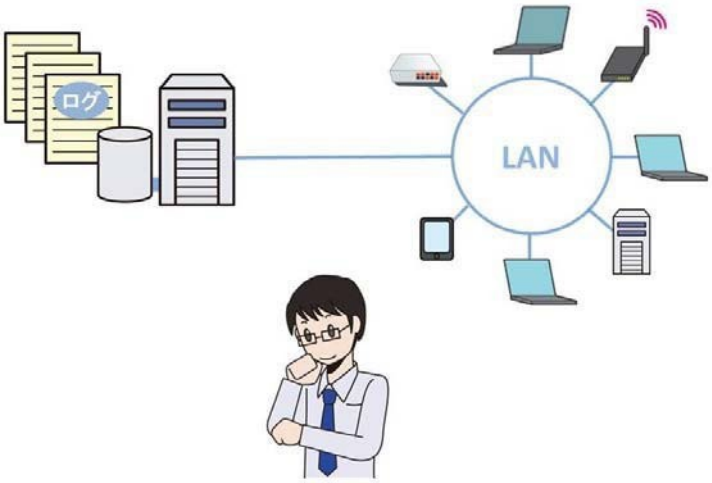
■ ログの種類と内容

ログの具体的な例としては次のものが挙げられます。

- ファイアウォールを通過した通信又は拒否された通信のログ
- 侵入検知システム（IDS）や侵入防止システム（IPS）が監視した通信のログ
- DHCPサーバがパソコンにIPアドレスを割り当てたログ
- ファイルサーバへのアクセスのログ
- ファイルの参照や編集などの成功や失敗のログ
- 情報システムへのログイン、ログアウトなど認証の成功や失敗のログ
- Webサーバへのアクセスのログ
- Webサーバが利用者から受け取った入力内容のログ
- Webプロキシサーバが中継した通信のログ
- データベースサーバへのアクセスのログ
- アプリケーションが出力する処理結果の正常終了、異常終了などのログ
- パソコンの監査のログ

それぞれのサーバやシステムが出力するログの内容は、通信やアクセスの送信元・送信先のIPアドレスを始めとして、通信に使用されるポート番号、命令の内容、通信データ自身など、さまざまなレベルがあります。出力されるログの詳細度は一般的には設定によって制御できますが、どのような内容のログを取得するべきかは、組織が扱うデータの性質や、システムの処理能力、ネットワーク構成などに大きく関係します。さらに、組織が受ける可能性があるネットワーク攻撃を事前に想定し、それを考慮したログの取得・管理方法を設計に反映することで、調査が必要になった場合に、より役に立つ情報を得られることが考えられます。

必要なログの種類と内容について、組織内で十分に検討を行い、適切なログを取得できるようにしましょう。



■ システムの時刻同期の必要性

ログを取得する場合、各コンピュータ間でシステムの時刻を一致させておく必要があります。この時刻の同期が不適切であると、ログに記録された時刻がずれてしまい、各システム間でログを相関的に分析することが困難になります。

システムの時刻を同期させる手段として、一般的にNTP（Network Time Protocol）が広く利用されています。実際にNTPが正しく設定され、正常に動作していることを確認しておくことが重要です。

■ ログの保管とバックアップ

ログは、収集した機器の本体内ではなく、ログ取得のために別途ログ管理システムなどを設計し、そこで保管を行うことが推奨されます。そうすることで、ログの改ざんなどの不正行為からの保護だけでなく、ログ解析プログラムによる可視化処理を行ったり、保存期間の制御なども行いやすくなります。

また、一定期間を経過したログの保管方法として、コストや保存期間を考慮し、外部記憶媒体等に保管する運用も検討しましょう。通常のデータのバックアップと同様に、ログのバックアップも重要になります。

■ ログの取り扱いの注意

ログには、誰と誰がいつどのような内容の通信を行ったか、という情報が記録されています。また、企業秘密に関する情報や、電子メールの内容、利用者が入力した個人情報などがそのまま含まれている場合もあります。ログは機密情報であるということを理解し、取扱いには十分な注意が必要です。

例えば、外部のセキュリティ調査会社にログを開示して調査を依頼する際には、ログの内容に関して秘密保持契約を結んだり、ログを外部に持ち出さなければならない際にはデータの暗号化を検討するなど、秘密の保全に関する対応が必要であることを理解しましょう。

サポート期間が終了するソフトウェアに注意

ソフトウェアを安全に利用するためには開発元や機器メーカーから配布される更新プログラムを早急に適用することが重要ですが、更新プログラム配布等のサポートは一定期間で終了するものがあります。サポート期間が切れたソフトウェアは脆弱性が発見された場合も修正されないといったセキュリティ上の懸念があります。

サポート期間を見逃し易いものとして、ソフトウェアの中にはソフトウェア単体で動作するものだけでなく、他のシステムやアプリケーションに使用されているものがあります。その場合、気づかないうちにソフトウェアのサポート期間が切れ、セキュリティ上のリスクを抱えるといったことが発生します。こうしたソフトウェアのサポート期間はソフトウェアの提供元があらかじめ公表しているものもあります。サポート終了時期を事前に把握しておき、計画的に更新を行いましょう。

■ ログの取り扱いの注意

Javaでアプリケーションを開発、実行するために必要なソフトウェア群であるJava Platform Standard Edition（以後JavaSE。現在は8が最新版）のうち一世代前のJavaSE7についてセキュリティの問題の修正等を行う無償サポートが2015年4月をもって終了します。組織内でJavaSE7を利用している場合は、システムや製品の提供元、保守ベンダーに相談する等、検討を行いましょう。

防御モデルの解説

■「防御モデルの解説」概要

「防御モデルの解説」では、巧妙化・複雑化し続けるサイバー攻撃（特に標的型攻撃）への対策として、官公庁・民間企業が具備することが推奨される機能群（以下「防御モデル」という。）を解説しています。この解説を通じて、サイバー攻撃への対応能力が向上することが目的とされています。

防御モデルは、人・組織対策と技術的対策から構成されており、前者ではインシデントレスポンスの計画と実行について、後者では事前対策・検知・事後対策について解説しています。

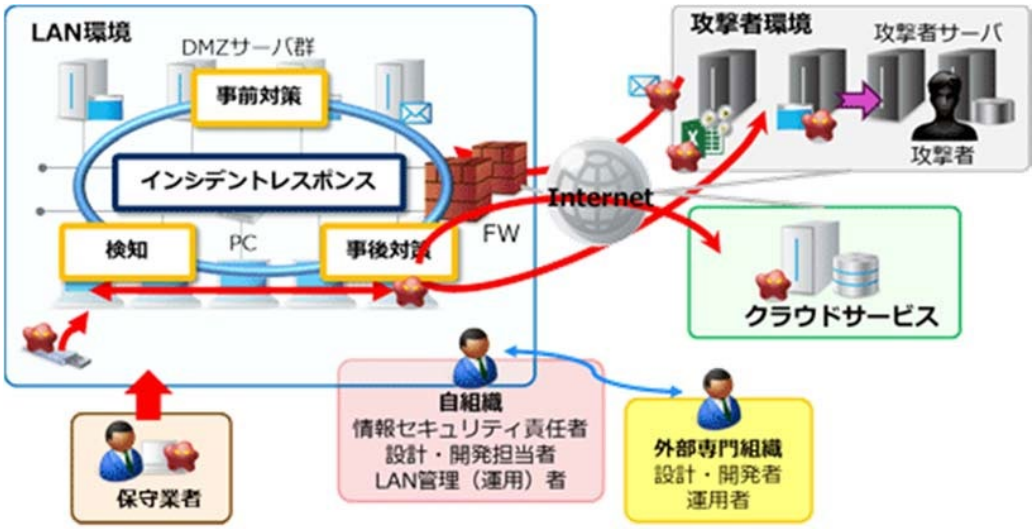
本解説書の想定読者は、各組織で標的型攻撃に対応する担当者や関係者の方々です。

＜本解説の読者について＞

想定読者		説明
自組織	情報セキュリティ責任者	自組織の情報セキュリティ責任者（CISOも含む）
	設計・開発担当	自組織の情報システムに関する設計・開発の担当者
	LAN管理者	自組織のLAN管理者
	LAN運用者	自組織のLAN運用者
外部専門組織	設計・開発者	自組織の設計・開発者からの依頼に基づき一部の設計・開発を行う外部専門組織の設計・開発者
	運用者	自組織のLAN管理者又はLAN運用者からの依頼に基づきLANの運用を行う外部専門組織の運用者

■防御モデルが対応するサイバー攻撃について

防御モデルは、「標的型メール」、「Drive-by-Download等のWebサイト」、「不正なプログラムを含むソフトウェア」、「USBメモリ」、「保守業者の持ち込んだ機器」、「クラウドサービス」を攻撃経路とするサイバー攻撃（標的型攻撃）を想定しています。



解説資料

- サイバー攻撃（標的型攻撃）対策防御モデルの解説（簡易版）（別紙2）
- サイバー攻撃（標的型攻撃）対策防御モデルの解説（詳細版）（別紙3）

付録

- 付録1_インシデントハンドリングフェーズの定義（別紙4）
- 付録2_システムログ一覧（別紙5）
- 付録3_暫定対処策一覧（別紙6）
- 付録4_システムログ一覧（証拠保全）（別紙7）

情報セキュリティポリシーの導入と運用

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、大きな利便性を与えるものでも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。
- 情報セキュリティ対策が「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」という対応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、「計画」、「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、社員や職員の教育、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を積極的に社員や職員に普及させ支援する、情報セキュリティポリシーが遵守され、有効に機能しているか、業務の妨げなどになっていないかなどを日常的にモニタリングする、情報セキュリティ対策の評価を行い、経営幹部へ報告を行うなど、情報セキュリティポリシーの導入だけでなく継続的に運用を行うことが必要です。

参照 情報セキュリティマネジメントとは（組織幹部のための情報セキュリティ対策）

ソーシャルエンジニアリングの対策

企業や組織の機密を狙ったソーシャルエンジニアリングの手法は、古くから存在しますが、その中でも、最近は、標的型攻撃の被害が深刻化していることとの関係で、再び注目を集めています。

ひとりの社員・職員の情報が漏洩（ろうえい）するということが、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。全ての社員・職員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。

社員・職員への研修にあたっては、実際にあったソーシャルエンジニアリングの手口を紹介したり、体験させる手法も有効です。

参照 ソーシャルエンジニアリングの対策（社員・職員全般の情報セキュリティ対策）

クラウドサービスを利用する際の情報セキュリティ対策

クラウドサービスとは、インターネットを通じてアプリケーションやストレージなどのさまざまなサービスの提供が受けられるサービスです。

企業や組織において、社内の情報資産をクラウドサービスに預けるという利用が進んでいます。クラウドサービスには、一般の企業や組織が共有して利用するパブリッククラウドサービスと、特定の企業・組織向けのプライベートクラウドサービスがあります。ここではおもにパブリッククラウドサービスを利用する際の注意点を説明します。

参照 クラウドサービスとは？（基礎知識）

クラウドサービスは、これまでのパッケージソフトや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を保管するということ、クラウドサービス事業者側に運用やデータ管理を依存するということです。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などのメリットがある一方で、情報セキュリティ対策をサービス事業者に大きく依存することになります。

そのため、クラウドサービスを利用する際には、事業者が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確認した上で選定する必要があります。

クラウドサービス事業者が行うべき主要な情報セキュリティ対策
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など）
データのバックアップ
ハードウェア機器の障害対策
仮想サーバなどのホスト側のOS、ソフトウェア、アプリケーションにおける脆弱性（ぜいじゃくせい）の判定と対策
不正アクセスの防止
アクセスログの管理
通信の暗号化の有無

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。利用するクラウドサービスのサービス条件などを、事業者との契約内容や規約で確認して、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。

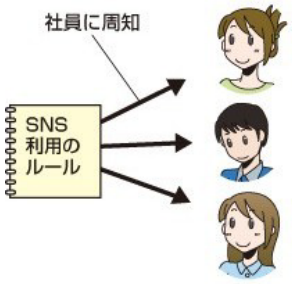
実際にクラウドサービスを利用するに際しては、情報セキュリティポリシーを整備し、バックアップやアカウント管理などの情報セキュリティ対策を十分にしておくこと、社員・職員にポリシーを遵守させることも重要です。クラウドサービスに限った話ではありませんが、社員・職員個人が勝手に利用したサービスからインシデントが発生する場合も少なくないので、利用可能なサービスをポリシーではっきり定める必要もあるでしょう。

参照 クラウドサービス利用上の注意点（社員・職員全般の情報セキュリティ対策）

SNSを利用する際の情報セキュリティ対策

SNSは、一般の利用者相互のコミュニケーションのために広く使われていますが、最近ではビジネスでの利用も進んできています。企業や組織の職員の多くが個人としてSNSを利用するようになり、また、企業や組織が広報戦略の一環としてSNSを積極的に活用する機会が増えています。

一方、SNSには社会的に不適切な内容の発言に対して激しい非難が浴びせられるなどの反応が起きることがあり、企業や組織にとってリスクとなっています。こうした発言による問題については、組織として、SNSの利用に関するルールを決め、社員・職員に周知をして守らせましょう。特に組織を代表する公式アカウントについては、アカウントや投稿内容などを十分に管理することが大切ですし、パスワードの管理も含めて利用状態を適切に把握し、しっかり管理するようにしましょう。



SNSでは本人以外が同一名称のアカウントを作成できる場合があり、そうしたなりすましアカウントで発言される内容も会社のブランドイメージに影響を与えます。こうしたなりすましの被害にあわないためにも、定期的に発言をチェックするなどの運用を検討しましょう。また、公式アカウントなどを取得できるSNSでは、企業・組織の正式な発信を区別するため、公式アカウントを取得することも一つの方策です。

参照 SNS利用上の注意点（社員・職員全般の情報セキュリティ対策）

社員の不正による被害と対策

外部からの不正アクセスに対して、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、全ての社員や職員に適切な権限を設定したユーザ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を防ぐためには、ノートパソコンやスマートフォン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したりするなどによって、電子データに対する情報管理の意識を高めることが大切です。許可なく社内のデータを外部に持ち出すことが違反行為であり、犯罪行為にもなり得るということをしっかりと教育することが重要となります。

廃棄するパソコンやメディアからの情報漏洩

廃棄した物品からの情報漏洩を防ぐには、パソコンや記憶媒体は、必ず情報管理担当者が取りまとめて適切な処理をした後で廃棄するなど、社内で統一の手順とルールを確立し、徹底することが重要です。

なお、パソコンなどをリースしていて期間終了に伴い返却する場合は、リース会社においても適切に処理されるよう、契約内容に含めることも重要です。

不要になったコンピュータのハードディスク・SSDや記憶媒体の処理方法には、次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

データ消去用のソフトウェアを利用すると、ハードディスクやメディアのファイルを無意味なデータで全て上書きするなどして、二度と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、SSDについてはその特性から完全に上書きされない場合があることには留意が必要です。

専門業者のデータ消去サービスを利用する

専門業者にデータ消去を依頼する場合には、消去する前の重要なデータをその業者に渡すことになります。依頼先の会社の実績や信頼度、さらに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業者を選定しましょう。

不適切な業者に委託したために、データ消去・廃棄されるはずのハードディスクが転売され、情報漏洩につながった事例もあるため、特に留意が必要です。

ハードディスクや記憶媒体を物理的に破壊する

ハードディスクについては、外側のケースを破壊しても、中にあるディスク自体が破損していない場合があります。このまま廃棄すると、ディスクを取り出してデータを復元できることもあるので、データが記録されているディスク面が確実に破壊されたことを確認しましょう。

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で粉砕しましょう。

「暗号化消去」を行う

ハードディスク・SSDの記録を暗号化していた場合は、復号に必要な鍵を確実に廃棄することにより、記録内容を読み出せなくする方法があります。これにより、上書き消去漏れ、物理的破壊漏れによるデータの復元リスクもなくせます。

例えば、WindowsOSにおいて利用可能なストレージ暗号化方式であるBitLockerの場合、保管している回復キーを確実に廃棄することで実現します。留意したいのは、回復キーを保存したデバイスと一緒に廃棄してしまうなど、第三者が回復キーを入手する可能性を排除することです。

暗号化消去は「政府機関等のサイバーセキュリティ対策のための統一基準群（令和3年度版）」で追加されました。

参照 廃棄するパソコンやメディアからの情報漏洩（社員・職員全般の情報セキュリティ対策）

持ち運び可能な記憶媒体や機器を利用する上での危険性と対策

小さくて持ち運びが楽なUSBメモリなどの記憶媒体は、紛失や盗難の危険性を伴います。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、社員や職員に順守させることも大切です。たとえば、以下のようなルールを検討してください。

- 外部に持ち出す記憶媒体や機器の利用は、十分な情報セキュリティ対策を施した、企業や組織が管理するものだけに制限し、個人所有の媒体や機器の使用は許可しない。
- 記憶媒体や機器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。
- 記憶媒体や機器の利用に何らかの制限をかける。BIOSの設定でUSB端子を使用できなくする、CD・DVDドライブなどの外部記憶媒体への書き込みを可能にする機器を取り除いたパソコンを使用させる、など。

以下の社員・職員全般の情報セキュリティ対策も参考にしてください。

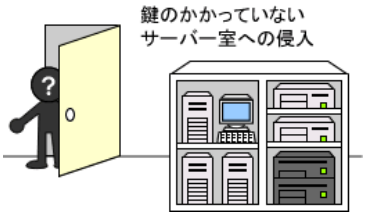
参照 持ち運び可能なメディアや機器を利用する上での危険性と対策（社員・職員全般の情報セキュリティ対策）

情報セキュリティポリシーの導入と運用（情報管理担当者の情報セキュリティ対策）

サーバの設置と管理

企業や組織内にサーバ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を直接操作されてしまったり、サーバの情報が盗み出されてしまったりする危険があるため、避けるべきです。

また、サーバの設置場所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。

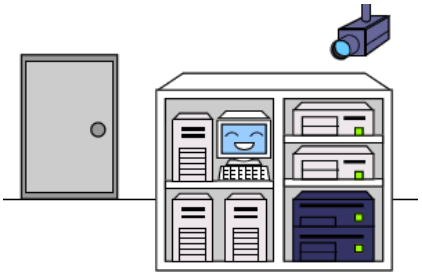


次に重要なこととして、サーバに適切なパスワードを設定した上で、常にログアウトした状態にしておくことです。短時間の内にログインするためのパスワードを見つけ出すということはとても困難であるため、サーバが不正に利用される可能性を減らすことにつながります。

サーバ室でサーバ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。

- 防犯カメラの設置や生体認証の導入など、他の執務エリアよりもセキュリティ対策を強化する。
- 鍵の管理や入退室時間を記録するなど、サーバ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）。
- サーバは、使用後に常にログアウトしておくようにルールを徹底する。



なお、これらのサーバ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しておきましょう。

最後に、地震などの天災からサーバを守るために、耐震などを考慮したサーバの設置を検討すべきです。専用のサーバラックにサーバを固定して、サーバ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

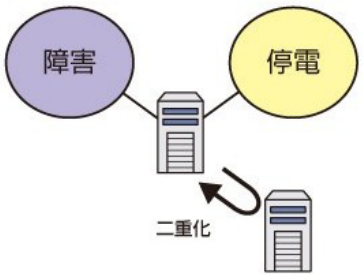
入を通して、情報セキュリティをさらに向上する効果も期待できます。最近では、インターネットデータセンターと呼ばれるサーバの管理を全て請負ってくれるサービスもありますので、社内に適切なサーバの設置場所が見つからない場合には、そのようなサービスを検討するのもよいでしょう。

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、電圧が低下したりしたときに、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、サーバに障害が発生したときのために、定期的にバックアップをとっておくことが大切です。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、あらかじめ全てのサーバの設定内容を安全に保管しておかなければなりません。社内の基幹サーバなどのように、サーバ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を用意しておくこともよいでしょう。交換用サーバ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、基幹サーバの可用性を高めることができます。



このテキストに関する問い合わせ先

総務省 サイバーセキュリティ統括官室
Email:kokumin-security@ml.soumu.go.jp

- 国民のためのサイバーセキュリティサイト
  https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/index.html
- キッズページ
  http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/kids/
- このテキストの利用規約
  https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/guide.html