総務省 安心してインターネットを使うために
国民のための情報セキュリティサイト

社員・職員全般の情報セキュリティ対策

ここでは、企業や組織の一員である社員・職員に必要となる情報セキュリティ対策について説明します。

企業や組織においては、たった一人の不注意が、ウイルスへの感染や情報漏洩（ろうえい）といった脅威につながることもあります。社員・職員の一人一人が、情報セキュリティ対策の必要性を理解し、自覚をもって取り組むことが必要です。

多くの企業や組織において、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が策定されています。所属する企業や組織において、情報セキュリティポリシーが策定されている場合には、以下の内容も参照しながら、企業や組織の情報セキュリティポリシーに従ってください。

社員・職員全般の情報セキュリティ対策

安全なパスワード管理 2
ソフトウェアの情報セキュリティ対策 4
ウイルス対策 5
電子メールの誤送信 8
標的型攻撃への対策 10
悪意のあるホームページ 12
バックアップ 13
安全な無線 LAN の利用 15
廃棄するパソコンやメディアからの情報漏洩（ろうえい） 16
外出先で業務用端末を利用する場合の対策 17
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 19
ソーシャルエンジニアリングの対策 21
クラウドサービス利用時の注意点 23
SNS 利用上の注意点 24

企業・組織におけるパスワードは、ユーザ名と組み合わせることで企業・組織内の情報資産へのアクセスの可否を決める重要なものです。パスワードの重要性を再認識して、適切なパスワード管理を心がけましょう。

他人に自分のユーザアカウントを不正に利用されないようにするには、推測されにくい安全なパスワードを作成し、他人の目に触れないよう適切な方法で保管することが大切です。

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、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。

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

インターネットなどで配布されているツールの中には、パスワードクラッカーと呼ばれる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。このパスワードクラッカーには、パスワードでよく使われる単語が辞書として登録されており、この辞書に載っている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、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

安全なパスワードの作成だけでなく、他人に知られないよう、かつ自分でも忘れてしまうことがないように管理をしましょう。自分で忘れてしまわぬようにメモを作成した場合は、それが他人に見られることのないよう、肌身離さず持ち歩くなど、厳重に保管をするよう心がけましょう。

パスワードを複数のサービスで使いまわさない(定期的な変更は不要)

また、パスワードはできる限り、複数のサービスで使い回さないようにしましょう。あるサービスから流出したアカウント情報を使って、他のサービスへの不正ログインを試す攻撃の手口が知られています。もし、重要情報を利用しているサービスで、他のサービスからの使い回しのパスワードを利用していた場合、他のサービスから何らかの原因でパスワードが漏洩してしまえば、第三者に重要情報にアクセスされてしまう可能性があります。

なお、利用するサービスによっては、パスワードを定期的に変更することを求められることもありますが、実際にパスワードを破られアカウントが乗っ取られたり、サービス側から流出した事実がなければ、パスワードを変更する必要はありません。むしろ定期的な変更をすることで、パスワー

ドの作り方がパターン化し簡単なものになることや、使い回しをするようになることの方が問題となります。定期的に変更するよりも、機器やサービスの間で使い回しのない、固有のパスワードを設定することが求められます。

これまでは、パスワードの定期的な変更が推奨されていましたが、2017年に、米国国立標準技術研究所（NIST）からガイドラインとして、サービスを提供する側がパスワードの定期的な変更を要求すべきではない旨が示されたところです（※1）。また、日本においても、内閣サイバーセキュリティセンター（NISC）から、パスワードを定期変更する必要はなく、流出時に速やかに変更する旨が示されています（※2）。

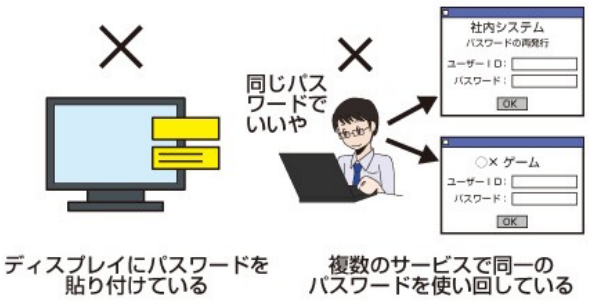
（※1）NIST SP800-63B（電子的認証に関するガイドライン）

（※2）https://www.nisc.go.jp/security-site/handbook/index.html

パスワードの活用

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、離席中に不正な利用者がそのパソコンを操作することを防ぐことができるようになります。ただし、スクリーンセーバーが起動するには一定の時間が必要です。

さらに情報セキュリティを強化するためには、離席する際にログアウトを行い、パスワードを入力してログインしなければパソコンを操作できないようにするなど、利用者が自発的にロックする方法が有効です。



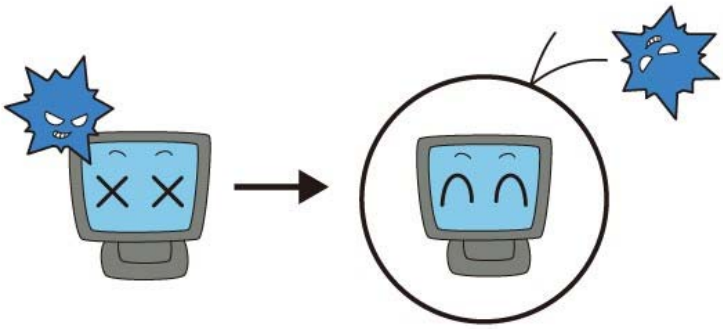
参照 IDとパスワード（基礎知識）

ソフトウェアの情報セキュリティ対策

Webブラウザや電子メールソフト、OS、Officeアプリケーションなどのソフトウェアには、時間の経過とともに、脆弱性（ぜいじゃくせい）と呼ばれる不具合が発見されることがあります。

脆弱性を放置していると、たとえウイルス対策ソフトを入れて、最新版のウイルス検知用データに更新していたとしても、ウイルスに感染してしまったり、ウイルス付きの電子メールが他の人に自動的に送られてしまったり、悪意のあるホームページを見ただけでパソコンの中のシステムが破壊されてしまったりすることがあります。

脆弱性は、プログラムの不具合や設計ミスなどに起因するものですが、それらを修正するための修正プログラムがメーカーから配布されています。



最近は、パッケージソフトなどの利用者の多いソフトウェアを始めとして、修正プログラムの有無を定期的に確認したり、自動的に適用したりするための自動アップデート機能が導入されることが増えてきました。このような自動アップデート機能を利用すると、修正プログラムの適用を忘れてしまうことがなくなります。自動アップデート機能を利用できる場合には、「アップデートの準備ができました」などのメッセージが表示されるため、そのメッセージをクリックして、画面上の指示に従って操作してください。

また、情報セキュリティ対策としては、企業や組織で許可されていないソフトウェアをパソコンにインストールしないことも大切です。インターネットなどからダウンロードできるソフトウェアの中には、悪意のあるプログラムが含まれているものや、脆弱性が存在しているものがあります。業務の都合上、許可されていないソフトウェアをインストールする必要がある場合は、事前に情報システム部門などに申告し、許可を得てから行うようにしましょう。

参照 ソフトウェアを最新に保とう（一般利用者のためのセキュリティ対策）

ウイルス対策

自分のパソコンや社内のネットワークを防御するためには、まずウイルスへの適切な対策が必要です。最近のウイルスは、電子メールをプレビューしたり、Webブラウザでホームページを閲覧したりするだけで感染するなど、多様かつ巧妙なものになってきており、以前に比べて被害の内容や規模が急速に拡大してきています。

ウイルス感染の予防対策としては、まずパソコンに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を常に最新のものに更新しておくことが大切です。併せて、OSやソフトウェアを更新しておくことも大切です。

次に、企業や組織での情報システム部門などからのウイルスに関する連絡に注意を払い、怪しい電子メールが届いた場合は、情報システム部門などにすぐに連絡することです。また、Webブラウザの設定についても、適切な設定に変更することも大切です。

しかし、ここに挙げたウイルス対策を十分に実施していたとしても感染してしまうことがあります。ウイルスは、日々新しいものが出回っており、それをウイルス対策ソフトで見つけられないことがあるからです。

もし、ウイルスに感染してしまった場合は、パソコンのLANケーブルを抜く、無線LANのスイッチを切るなどの方法で、社内のネットワークからパソコンを切り離すことを心がけてください。ネットワークにつながったままにしていると、企業や組織全体にウイルスを蔓延させてしまうこともあるためです。その上で社内の情報システム部門などに連絡しましょう。

ウイルス対策ソフトの確認

ウイルス対策ソフトがパソコンにインストールされている場合には、通常、パソコンのタスクバーと呼ばれる領域にウイルス対策ソフトが動作していることを示すアイコンが表示されます。または、パソコンのプログラムの一覧で、ウイルス対策ソフトが含まれているかどうかを確認するという方法もあります。

自分の使用しているパソコンにウイルス対策ソフトがインストールされていない場合には、情報管理担当者に確認してみましょう。

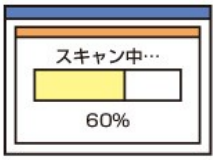
ウイルス検知用データの更新

ウイルス対策ソフトが新しいウイルスに対応するためには、常にウイルス検知用データを最新のものに更新しておかなければなりません。パソコンにウイルス対策ソフトがインストールされていても、ウイルス検知用データが古いままでは、新しいウイルスに感染してしまう危険性があります。

自分のパソコンのウイルス対策ソフトがどのような契約内容になっているかということを確認し、契約が切れてしまっている場合には、新たに契約を延長するか、新規にウイルス対策ソフトを購入しなければなりません。一般的なウイルス対策ソフトでは、契約期間が設定されているため、ウイルス検知用データの更新や契約方法について、確認して利用するようにしましょう。

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も呼ばれています。

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、ウイルス対策ソフトを導入して、ウイルス検知用データを更新するだけでなく、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（ただし、その時刻にパソコンの電源が入っていない場合には実行されません）。お昼休みや定例の会議の時間など、自分の予定に合わせて、スケジュールを設定しておくとよいでしょう。

USB媒介ウイルスへの対策

USB媒介ウイルスは、USBメモリなど記憶媒体の自動実行機能を利用して、パソコンに差し込んだだけで感染するウイルスです。USB媒介ウイルスへの対策として、許可されていない記憶媒体や持ち主の分からないものを使用しないようにしてください。また、記憶媒体を差し込んだときには、フォルダやファイルを開く前に必ずウイルスチェックを行うようにするとよいでしょう。パソコンの設定を変更して、自動再生機能を停止しておくと、さらに安心して利用できるようになります。

参照 ウイルスとは？（基礎知識）
ウイルスの感染経路と主な活動（基礎知識）
ウイルス対策をしよう（一般利用者の対策）

電子メールの誤送信

電子メールは、企業や組織において、日常的にもっとも利用するツールの1つですが、宛先アドレスの間違いや、メールアドレスの表示方法の誤操作といったミスによる情報漏洩（ろうえい）が頻繁に発生しています。

宛先アドレスを誤って入力してしまう原因の1つとして、オートコンプリートと呼ばれる自動補完機能によるアドレスの誤入力があります。オートコンプリートは、文字入力を補助する機能の一つで、過去の入力履歴を参照して次の入力内容を予想し、候補を表示してくれます。電子メールでは、メールアドレスの先頭の部分を入力するだけで自動的に全部の文字列が入力される便利な機能です。しかし、この機能で表示されたメールアドレスをよく確認せず、間違った宛先を指定して送信してしまうというケースがあるので、注意が必要です。

また、よくある誤送信の例としては、TO：、CC：、BCC：の使い方の誤りによるものがあります。電子メールの宛先欄には、この3つの種類がありますが、それぞれ目的に応じて使い分けます。

まず、TO：（宛先)には、メールを送る主体の相手のメールアドレスを入力します。

次に、CC：はカーボン・コピー（Carbon Copy）の略で、宛先の相手へ送った内容について、他の人にも知らせたい、という場合に使います。

BCC：は、ブラインド・カーボン・コピー（Blind Carbon Copy）の略で、CC：と同様に宛先の相手へ送った内容について、他の人にも知らせたい場合に使いますが、ここに入力されたメールアドレスは受信者には表示されません。他の受信者がいることや、他の受信者のメールアドレスをわからないようにしたい場合は、BCC：を使用します。

よくある誤りが、CC：と BCC：の取り違いです。本来は、BCC：で送るべきところを CC：で送ってしまったことにより、受信者に他のすべての受信者のメールアドレスがわかってしまう、という事例が多く発生しています。電子メールを送る際は、宛先のメールアドレスと送信欄（TO：、CC：、BCC：）が自分の意図したとおりになっているか、確認をしてから送るようにしましょう。

さらに、メールの誤送信の影響が大きくなるのは、多くの宛先に対して同時にメールを送信したいときです。この場合、宛先欄に大量のメールアドレスを入力することになりますが、途中で TO：、CC：、BCC：欄を取り違えて入力してしまい、そのままメールを送信して情報漏洩（ろうえい）となる事例が多く見られます。
このようなときには、通常利用しているメールソフトは使用せず、通信事業者が提供する専用の同報メールサービスを利用することなども検討し、誤送信による事故を起こさないようにしましょう。

参照 電子メールの仕組み（基礎知識）
メールの誤送信（一般利用者の対策）

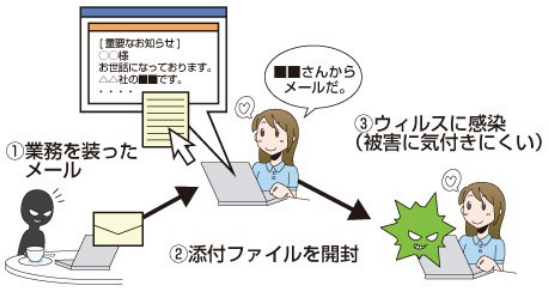
標的型攻撃への対策

最近、特定の企業や組織を狙った標的型攻撃メールにより、重要な情報が盗まれる事件が頻発しています。標的型攻撃メールとは、不特定多数の対象にばらまかれる通常の迷惑メールとは異なり、対象の組織から重要な情報を盗むことなどを目的として、組織の担当者が業務に関係するメールだと信じて開封してしまうように巧妙に作り込まれたウイルス付きのメールのことです。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。

企業や組織の中のたった1人の社員や職員が、標的型攻撃メールの添付ファイルを開封したり、リンクをクリックしただけでも、情報を盗み出すウイルスに感染し、機密情報が漏洩（ろうえい）する事態に陥ることがあります。特に、標的型攻撃メールのウイルスは、ウイルス対策ソフトでは検出 されないものが多いため感染に気づきにくく、知らぬ間に被害が拡大しているケースがあり、深刻な問題となっています。

標的型攻撃を一つの手段で防ぐことは困難ですが、社員・職員の対策としては、標的型攻撃メールの手口をよく知り、そのようなメールが届いても添付されたファイルを開封したり、リンクをクリックしたりしないようにすることが大切です。

標的型攻撃メールの文面は、業務でやりとりしているメールの送信者、よく使われているメールの件名やあて先、内容、添付ファイルの形式、署名などを真似て、受信側をだまそうとするものが主流です。一見して不審な点があまりなく、気がつきにくいのが特徴です。また、メールの件名や内容を、「緊急」や「重要」など、受信側の興味を引いたり、読まなければならないと思わせたりするような細工がされています。



このようなメールが標的型攻撃メールであることを見抜くためには、最近のメールのやりとりなどから判断をすることが重要です。たとえば、最近やりとりがなかったのに、突然メールが届いた、最近のやりとりの内容と全く脈絡のない内容のメールが届いた、などの場合は注意が必要です。このような疑わしいメールを受け取った場合は、情報管理者にすぐに報告・相談するようにしましょう。

その他、最近の標的型攻撃メールは、誰でも取得可能なフリーメールアドレスを利用して添付ファイルにマルウェアを仕込んで送信されることが増えていますので、フリーメールアドレスから送られてきたメールには特に注意が必要です。

また、送信者のメールアドレスを正規のドメインに詐称して攻撃メールが送られてくることもあります。この場合は、メールの送信者アドレスに注意し、送信ドメイン認証の機能を利用してメールが正しい送信元から送られてきているかどうかを確認することで、不審なメールを特定する手がかりになります。

また、一般的にウイルスに感染する危険性を小さくするために、ウイルス対策ソフトの利用とソフトウェアの更新を欠かさずにしておくことも最低限必要な対策となります。

参照 ウイルスの感染経路と主な活動（基礎知識）
ウイルスに感染しないために（基礎知識）

悪意のあるホームページ

インターネットにはさまざまなホームページが公開されていますが、それらの中には個人情報を収集することや、いやがらせが目的のものもあります。また、ホームページによっては、閲覧しただけで、ウイルスに感染したり、パソコンを破壊されたりしてしまうものもあります。

まず心がけなければならないのは、悪意を持ったホームページが存在するということを認識し、怪しいホームページはできる限り近寄らないようにするなどの対策が必要です。

このようなホームページの被害を受けないために、まずはOSやWebブラウザなどを最新の状態に更新しておくことが大切です。またウイルス対策ソフトを利用するようにしてください。

また、Webブラウザの設定を見直すことも大切です。悪意のあるスクリプトが自動的に実行されないようにするには、Webブラウザの設定を変更して、JavaScriptの実行時に警告を出すようにする、もしくは信頼できるWebサイト（信頼済みサイト）以外ではJavaScriptを実行させないといった対策が考えられます。実際には、組織の情報セキュリティポリシーに沿った対応を行って下さい。

参照 ウイルスに感染しないために（基礎知識）
インターネットの安全な歩き方（基礎知識）
ウイルス対策をしよう（一般利用者の対策）

バックアップ

安全にパソコンを利用するためには、定期的なバックアップが不可欠です。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、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などの情報も、バックアップしておかなければなりません。

バックアップには、ファイルサーバやインターネット上のオンラインストレージ、外付けのハードディスクにコピーする方法、CD-RやDVDメディアなどの外部の記憶媒体を利用する方法などがあります。

CD-R

1枚のメディアに、640MB以上のファイルを保存することができます。ただし、一度書き込むと、後からファイルを追加することはできますが、書き換えることができません（CD-RWというメディアでは、繰り返し書き換えて利用することが可能です）。書き込んだCD-Rメディアは、大部分のCD-ROMドライブで読み出すことができるため、ほとんどの場合、他のコンピュータへの復元がもっとも簡単です。

DVD-R、DVD+R

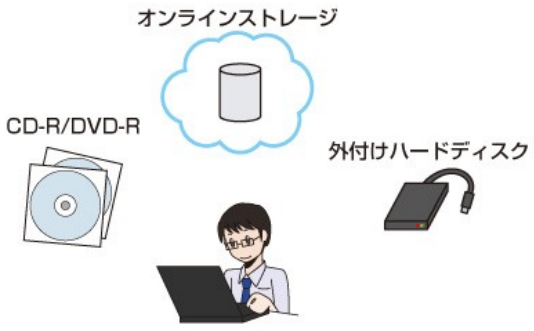
一度だけ書き込むことができるDVDメディアです。現在普及している規格では、片面で4.7GBのファイルを保存することができます。DVD-RやDVD+Rは追記型のメディアであるため、一度書き込んだデータを消去することはできませんが、DVD-RAM、DVD-RW、DVD+RWといった書き換え可能なDVDメディアもあります。

外付けのハードディスク

外付けのハードディスクをバックアップ用のデバイスとして使用する方法もあります。他のメディアに比べて高速であるということと、必要に応じた容量のハードディスクを選択できるというメリットがあります。

オンラインストレージ

オンラインストレージは、インターネット上で利用できるファイル保管用サービスです。Webブラウザや専用のソフトウェアを利用して、インターネット上の領域とクライアントのディスクとの間でデータをやり取りすることができます。複数の利用者でファイルを共有化できるサービスもあります。



まず、どのようなバックアップ方法を推奨しているかということを、情報管理担当者や情報システム部門などに確認するか、情報セキュリティポリシーや社内ルールで確認した上でバックアップ方法を決定してください。

なお、外部の記憶媒体にバックアップされた情報は、たとえ個人のパソコン内の情報だからといって外に持ち出したり、机の上に放置したりす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、適切な保管方法をとるべきです。

最近は機密情報や個人情報の漏洩（ろうえい）を防止するため、情報セキュリティポリシーで、個人による外部の記憶媒体の利用を禁止または制限している企業が増えてきています。バックアップ用に外部の記憶媒体を利用する場合には、事前に情報管理担当者や情報システム部門などに相談するか、情報セキュリティポリシーをよく確認してから行うようにしてください。

参照 機器の廃棄（一般利用者の対策）

安全な無線LANの利用

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。また、最近では公衆無線LANサービスが普及し、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。

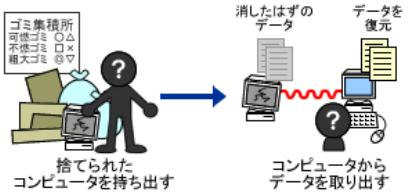
しかし、無線LANは電波を利用する通信であるという性質上、他人から通信内容を盗聴される危険性があります。また、公共の場でのパスワード等の入力を必要とせずに誰でもアクセスできる無線LANの場合には、無線LAN自体が悪意ある第三者により設置されている可能性もあるので、信頼できるものかどうか確認してからアクセスすることを心がけましょう。

その他、無線LANの利用にあたっては、社内や組織内で定められた情報セキュリティポリシーを遵守するようにしましょう。

参照 無線LANの仕組み（基礎知識）
無線LANの安全な利用（一般利用者の対策）

廃棄するパソコンやメディアからの情報漏洩（ろうえい）

企業や組織の重要情報が漏洩するのは、ネットワーク経由とは限りません。パソコンを廃棄したり、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なメディアから情報が漏洩する可能性があります。中古のパソコン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パソコン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、保存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、パソコン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。

不要になったパソコン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。
  市販されてい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。
- 専門業者のデータ消去サービスを利用する。 ただし、依頼先の会社の信頼度も考慮して業者を選定しましょう。
- パソコン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。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。

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て、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、CD-ROMやCD-R、DVD、USBメモリといった記憶媒体、外付けのハードディスクなどを廃棄する場合にも、同様の処理をしなければなりません。

また、パソコン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廃棄してから依頼するようにしましょう。

なお、情報セキュリティポリシーに廃棄の規定が定められている場合は、あらかじめ情報セキュリティポリシーを確認しておきます。また、組織内に情報管理担当者がいる場合には、パソコンを廃棄する前に、不明な点や廃棄方法を相談するようにしてください。

参照 機器の廃棄（一般利用者の対策）

外出先で業務用端末を利用する場合の対策

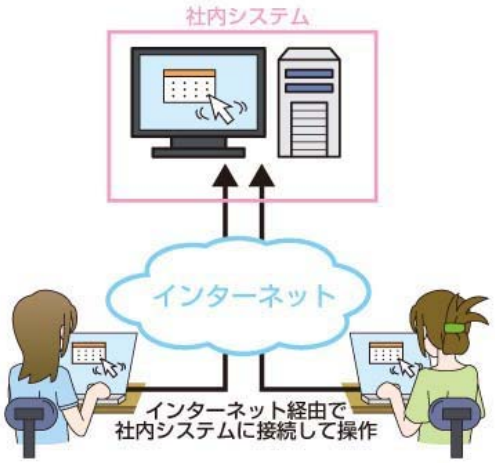
外出先でも業務用のノートパソコンやタブレット端末を利用するケースが増えてきています。しかし、外部に持ち出した業務用端末の情報セキュリティ対策を怠っていたがために、情報漏洩（ろうえい）を起こしてしまった事例が多数報告されています。

外部にノートパソコンなどを持ち出した場合には、電車内などへの置き忘れによる紛失や盗難、自宅や外出先でインターネットに接続することによるウイルス感染などの危険性があります。これらの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、個人情報は保存しない。
- 容易に推測されにくいログイ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。（指紋認証などの生体認証付きの端末を使用するのもよい）
- ハードディスクを暗号化して利用する。
- 持ち出し用の端末も、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。
- 持ち出し用の端末が入った鞄を電車の網棚などに置かない。鞄から目を離さない。
- 持ち出し用の端末にパスワードを書いた紙などを貼り付けない。

ただし、これらの対策はいずれも情報漏洩（ろうえい）に対するリスクを軽減するだけのものです。外部に業務用端末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常に念頭に置くことが大切です。

最近では、企業内のサーバ上でOSやソフトウェア、データを集中管理し、職員側は入力・表示などの最低限の機能に絞ったシンクライアント端末を利用して、ネットワークを通じてこれらのサーバに接続し、業務を行うという業務形態も徐々に広まっています。このような業務形態は、端末内に重要な情報が保存されない、ソフトウェアのメンテナンスが情報管理担当者により一元的に行われるという点から、外出先での端末利用に関する情報セキュリティ対策としても有効です。



スマートフォンを業務で利用する機会も増えています。スマートフォンは携帯電話と比較すると、紛失・盗難の場合の影響が格段に大きくなります。常に持ち歩く、どこかに置いたまま放置しないなど、紛失・盗難のリスクを最小限にするよう努めましょう。また、スマートフォンでは、紛失した場合に備え、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技術が、セキュリティ対策ソフトや、企業向けの携帯情報端末管理システムなどにより提供されています。

外出先で無線LANを利用してインターネットに接続する場合には、信頼できるアクセスポイントを選ぶこと、適切な暗号化などの設定を行うことも重要です。

参照 暗号化の仕組み（基礎知識）

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

最近、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、パソコンのUSB端子に接続するだけで手軽に利用でき、多くの利用者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（ろうえい）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、DVD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。

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、カバンの置き忘れなどによる紛失と情報漏洩、自宅や外出先のパソコンからウイルス感染し、会社内のネットワークにも感染を広げてしまうなどの危険性が考えられます。これらの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、個人情報は保存しない。
- ファイルは暗号化して保存する。
- セキュリティ機能つきのUSBメモリや外付けハードディスクを利用する。
- パソコンの設定を変更して、自動再生機能を停止する。ファイルを開く前に必ずウイルスチェックを行う。
- ウイルスに感染しているおそれがあるため、個人所有のUSBメモリや持ち主の分からないUSBメモリを使用しない。

最近は機密情報や個人情報の漏洩を防止するため、情報セキュリティポリシーで、個人による外部の記憶媒体の利用を禁止または制限している企業が増えてきています。外部の記憶媒体を利用する場合には、事前に情報管理担当者や情報システム部門などに相談するか、情報セキュリティポリシーをよく確認してから行うようにしてください。

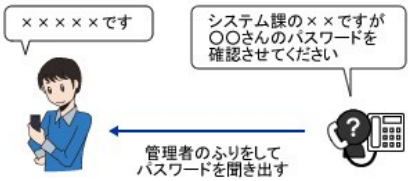
ソーシャルエンジニアリングの対策

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重要な情報を、情報通信技術を使用せずに盗み出す方法です。その多くは人間の心理的な隙や行動のミスにつけ込むものです。

ソーシャルエンジニアリングにはさまざまな方法がありますが、ここでは代表的なものとその対策を紹介します。

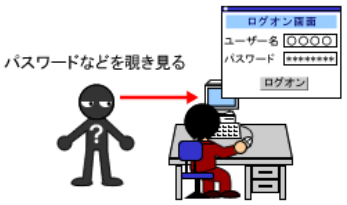
電話でパスワードを聞き出す

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名を入手したら、その利用者のふりをして、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、直接利用者に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。



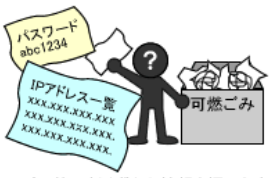
肩越しにキー入力を見る（ショルダハッキング）

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、事前の情報収集として行われることが多いのがトラッシングです。不正アクセス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（紙や記憶媒体）から、サーバやルータなどの設定情報、ネットワーク構成図、IPアドレスの一覧、ユーザ名やパスワードといった情報を探し出します。これらの対策としては、廃棄をする際に紙や記憶媒体にある情報を読み取られることがないよう、シュレッダにかけたり、溶解したりなどの処理をすることが重要になります。



ごみ箱の紙くずから情報を探し出す

最近では、特定の組織を狙った標的型攻撃メールにおいて、業務上のメールを装うなど、ソーシャルエンジニアリングの手法が用いられることが多くなっています。

企業や組織の重要情報が漏洩（ろうえい）するということは、組織全体のセキュリティを脅かすということをきちんと認識して、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）

クラウドサービス利用時の注意点

最近、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。一方で、利用者のIDやパスワードなどのアカウント情報の管理不備などが原因で、不正アクセスによる情報漏洩（ろうえい）などの事故が多く発生しています。クラウドサービスでは、誰もがどこからでも情報にアクセスしやすいことが利点ですが、場合によってはこのことがセキュリティ上の脅威にもなり得るのです。正しい利用者のみが許可された操作が行えるように、アカウントの管理には細心の注意が必要です。

また、クラウドサービスでは、データの保存場所がどの範囲の対象者からアクセス可能かを意識する必要があります。仮に外部に公開しているクラウドサーバに、公開するための情報に交じって、公開する予定ではなかったデータまで掲載してしまったとしたら、情報漏洩（ろうえい）の事故となり得ます。

さらに、クラウドサービスでは、業者側での障害や運用の不備などが原因で、システム上に置いたデータが消えてしまったり、サービス自体が使えなくなってしまったりという事態も発生しています。

万が一、クラウドサービスで障害が発生し、データが消えてしまった場合のことも想定し、データのバックアップを取得しておく必要があります。また、サービスが使えなくなった時のために、代替の手段やサービスを用意しておくことも検討する必要があります。組織のルールや情報の取り扱いポリシーを遵守し、公開範囲を意識した設定のしかたを確認した上で、適切に利用するようにしましょう。

参照 クラウドサービス利用上の注意点（一般利用者の対策）

SNS利用上の注意点

社員・職員は、個人として会社の名前を明らかにした上でSNSを利用する場合と、SNSを業務で利用する際にそれぞれ留意すべき点があります。

個人としてSNSを利用する場合には、個人の不用意な発言により、他の利用者から集中的な非難などを浴びる現象が起きることがあります。その影響は所属する企業や組織にまで及び、ブランドイメージを損なうというリスクもあるため、発言には十分に留意する必要があります。

また、業務でSNSを使用した情報発信を行う場合には、企業や組織の情報セキュリティポリシーに従い、以下のようなことに注意をしましょう。

- 企業や組織のブランドイメージを損なう発言をしない。
- 第三者にアカウントを乗っ取られないよう、アカウント情報(IDやパスワードなど)の適切な管理を行う。
- 利用するサービスの規約を遵守する。
- メンテナンスなどで、サービスが利用できない場合の運用を決めておく。

企業や組織の公式アカウントを担当している利用者は、よりいっそうの注意が必要になります。公式アカウントでの投稿は企業や組織を代表するものと受け取られます。また、このアカウントの管理が不十分なために不正行為による被害にあった場合は、企業や組織のブランドイメージを大きく損なうことになる可能性があります。

参照 SNS(ソーシャルネットワーキングサービス)の仕組み(基礎知識)
SNS利用上の注意(一般利用者の対策)
IDとパスワード(基礎知識)
情報発信の際の注意(一般利用者の対策)

このテキストに関する問い合わせ先

総務省 情報流通行政局 サイバーセキュリティ課
Email:　kokumin-security@ml.soumu.go.jp

○ 国民のための情報セキュリティサイト
http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/

○ 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
http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/guide.html