国民のための
サイバーセキュリティサイト

総務省

事前対策

（セキュリティ事故を未然に防ぐためには）

システムを“利用”する人向けの対策

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があります。社員・職員の一人ひとりが、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。

多くの企業や組織では、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。その場合には、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。

目次

ソフトウェアの最新化

パソコンやスマートフォン・タブレット端末などのコンピュータは、キーボードなどから入力した情報を、内部のソフトウェアが処理することで動いています。

こうしたソフトウェアには、オペレーティング・システム（OS）と呼ばれる、コンピュータを動かす基本的なソフトウェアや、ホームページを閲覧するときに使う Web ブラウザ、メールを送受信するときに使うメールソフトなど、利用目的に合わせたさまざまな種類のものがあります。

今では、パソコンやスマートフォンに限らず、多くの機器にコンピュータが搭載され、ソフトウェアで動いています。その点ではパソコンやスマートフォンと同じです。

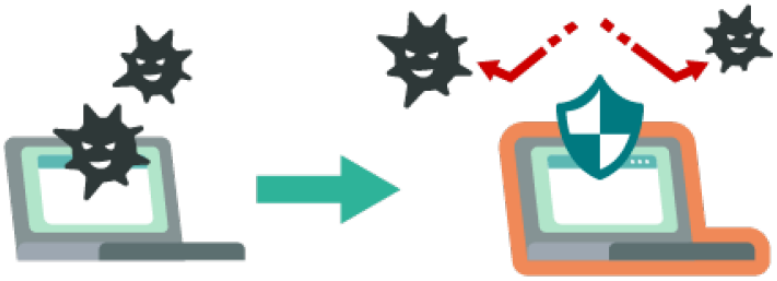
しかし、こうしたソフトウェアには、時間の経過とともに、脆弱性（ぜいじゃくせい）と呼ばれる不具合が発見されることがあります。脆弱性は、プログラムの不具合や設計ミスに起因して起こるものですが、それらが発見されるたびに、それを修正するための修正プログラムが、メーカーから配布されています。代表的なソフトウェアでは、最近は、「アップデートの準備ができました」などの形で通知が表示されることが多くなっています。

ソフトウェアのアップデートを
知らせるアイコンとメッセージ

脆弱性を残しておくことは、さまざまな攻撃のきっかけを与えてしまうことになりますので、通知が来たら、面倒がらずに毎回更新することが重要です。

パソコンやスマートフォン以外の、インターネットに接続された機器（家電製品やカーナビゲーションなど）も、ソフトウェアの更新が提供されることがあります。多くは自動的に

更新されるようになっているので、その機能を無効にしないよう留意しましょう。



マルウェア（ウイルス等）対策

マルウェア（ウイルス等）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、まずマルウェアへの適切な対策が必要です。最近のマルウェアは、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。

マルウェア感染の予防対策としては、まず OS やソフトウェアを更新して最新の状態に保つことが大切です。併せて、マルウェア対策ソフトをインストールした場合は、パターンファイルを常に最新のものに更新しておくことも大切です。

次に、情報システム部門などからのマルウェアに関する連絡に注意を払い、怪しい電子メールが届いたときは、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 ブラウザについても最新のバージョンのブラウザを使用したり、サポートされていないブラウザを利用しないようにしたりすることも大切です（例：Microsoft 社の Internet Explorer は 2022 年 6 月にサポートが終了しています）。

しかし、ここに挙げたマルウェア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。マルウェアは、日々新しいものが出回っており、OS のアップデートやマルウェア対策ソフトでは対応しきれないことがあるからです。

もし、マルウェアに感染してしまった場合は、会社のルールに従い対応するようにしましょう。一般的な対応としては、企業や組織全体にマルウェアを蔓延させないためにも、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が多いです。
困った際には、社内の情報システム担当者や情報システム部門等に連絡しましょう。

■　マルウェア対策ソフトの確認

最近の OS はマルウェアのスキャン、簡易ファイアウォールなどセキュリティ機能が充実しています。通常の使用であれば OS を最新の状態に保つことで十分ですが、さらにマルウェア対策ソフトを導入することで安全性を高められます。

マルウェア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マルウェア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、マルウェア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マルウェア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。

■　パターンファイルの更新

マルウェア対策ソフトが新しいマルウェアに対応するためには、常にパターンファイルを最新のものに更新しておかなければなりません。パソコンにマルウェア対策ソフトがインストールされていても、パターンファイルが古いままでは、かえって脆弱で危険な状態になりかねないので注意が必要です（マルウェア対策ソフトの導入により、OS 自身のセキュリティ機能が無効となっている場合があるからです）。

自分のパソコンのマルウェア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、新規にマルウェア対策ソフトを購入しなければなりません。一般的なマルウェア対策ソフトでは、契約期間が設定されているため、パターンファイル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。

パターンファイルは、マルウェア対策ソフトによって、マルウェア検知用データ、マルウェア定義ファイルなどの名前でも呼ばれています。

■　定期的なマルウェアスキャンの実行

マルウェア対策を万全にするためには、マルウェア対策ソフトを導入して、パターンファイルを更新するだけでなく、定期的なマルウェアスキャンを実行することが大切です。ほとんどのマルウェア対策ソフトでは、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マルウェア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 メモリを介したマルウェア感染への対策

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マルウェアも存在します。これらへの対策として、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マルウェア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。

■　マルウェア添付メールへの対応

パソコンのサイバーセキュリティ対策が不十分だった場合、受け取ったメールの形式によってはメールまたは添付ファイルを開くだけで感染する可能性があります。

ソフトウェアを最新にしていれば、リスクの高いファイルを開こうとしたときに警告を表

示するものも多いので、安易に続行しないで判断することが大切です。

コラム：ランサムウェア対策

マルウェア感染による被害が後を絶ちません。とりわけ企業にとって、重大な脅威のひとつにランサムウェアがあります。ランサムウェアとは、PC 上に保存しているファイルを暗号化して使用できない状態にしたり PC をロックしたりするなどして、復旧させることと引き換えに身代金を要求するマルウェアです。ランサムウェアに感染した場合、パソコンやサーバ内のデータが暗号化されてしまうため復旧にはバックアップが欠かすことができません。業務継続性を確保するために、定期的かつ適切な方法でバックアップを実施することが求められます。

特にランサムウェア対策としては、バックアップデータが暗号化されることも想定し、保存時にはネットワークから切り離されたストレージやメディアを利用するようにしましょう。

また、これまでは暗号化して身代金を要求するケースが多かったものの、攻撃者が「より手軽に」身代金を得るため、「暗号化」を行わず、盗み取ったデータの公開を対価に身代金を要求する「ノーウェアランサム」攻撃による被害も増加しています。

安全な無線 LAN の利用

無線 LAN は、ケーブルの代わりに無線を利用するという性質上、通信内容が傍受（盗聴）される危険性があります。そのため、無線 LAN を使ってユーザ ID やパスワードなどのログイン情報、クレジットカード番号のほか、プライバシー性の高い情報をやり取りする場合には、自分と相手先との間で通信が暗号化されていることを確認しましょう。

公共の場で無線 LAN を利用するときに、ファイル共有機能が有効になっていると、他人からパソコンやスマートフォン内のファイルが読み取られたり、ウイルスなどの不正なファイルを送りこまれたりすることがあります。公共の場で無線 LAN を利用する際には、必ずファイル共有機能を解除しましょう。

一方で、自宅内などに自分で無線 LAN のアクセスポイントを設置して利用する場合には、アクセスポイントで暗号化の設定を行ってください。現時点では、WPA2 方式または WPA3 方式による暗号化を推奨します。WPA3 の方が、より強固な暗号化方式を利用できます。旧来から WEP という暗号化方式もありましたが、WEP は短時間で解読される方法が発見され、安全な方式とは言えなくなっていますので、使用は推奨しません。

また、アクセスポイントに設定する管理パスワードや、認証・暗号化のための共有鍵は、単純なものや、無線 LAN のネットワーク識別子である SSID から類推できるものにしないよう、注意が必要です。一般的に SSID は公開されて使用されるため、SSID と似たパスワードを設定していると、第三者に類推されてしまう可能性があるからです。共有鍵が知られると、第三者がアクセスポイントに接続できたり、通信内容が容易に解読できたりします。

安全なパスワードの設定に関しては、下記のリンクを参照してください。

さらに、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、そのような機器を積極的に利用することをお勧めします。

コラム： 企業向けの Wi-Fi セキュリティ方式

一般利用向けの Wi-Fi セキュリティ方式である WPA2 パーソナル（WPA2-PSK）方式や WPA3 パーソナル（WPA3-personal）などに対して、企業向けの Wi-Fi セキュリティ方式として WPA2 エンタープライズ（WPA2-EAP）・WPA3 エンタープライズ（WPA3-enterprise）などがあります。

企業向けの Wi-Fi セキュリティ方式は、共通のパスワードを利用する一般利用向けの Wi-Fi セキュリティ方式とは異なり、利用者ごとに ID 等を設定し、接続の際に利用者側とアクセスポイント側で相互に認証する方式となります。認証の際に暗号鍵も個別に設定されます。利用者からアクセスポイントに対する認証も行うため、偽のアクセスポイントへ接続してしまう心配がありません。

標的型攻撃への対策

近年、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メール内のリンクをクリックしたり、添付ファイルを開いたりするなどして、ウイルスに感染するように巧妙に作り込まれたメールです。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りしただけでも、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ような新種（未知）の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、ソフトウェアの更新を必ず行い、最低限、既知のマルウェアに感染することを防ぐために、マルウェア（ウイルス等）対策ソフトを利用することも有効な対策となります。

万が一、被害を受けてしまった場合にはすぐに、情報セキュリティポリシーなどで定められている組織内の連絡先に報告をしましょう。報告が遅れることで被害が拡大してしまう可能性があります。

悪意のある Web サイトへの対策

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。また必要に応じて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。

安全なパスワードの設定・管理

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設定

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。

理想的には、ある程度長いランダムな英数字の並びが好ましいですが、覚えなければならないパスワードの場合は、英語でも日本語（ローマ字）でもよいので無関係な（文章にならない）複数の単語をつなげたり、その間に数字列を挟んだりしたものであれば、推測されにくく、覚えやすいパスワードを作ることができます。
近年では、スマートフォンやＷｅｂブラウザの標準機能として、パスワード生成機能があるものもありますので、そういったものをうまく活用しましょう。

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。このような危険なパスワードが使われていないかどうか、チェックをするようにしましょう。

(1) ID と同じ文字列
(2) 自分や家族の名前、電話番号、生年月日
　　yamada、tanaka、taro、hanako（名前）
　　09011112222（電話番号）
　　19960628、h020315（生年月日）
　　tokyo、kasumigaseki（住所）
　　3470、1297（車のナンバー）
(3) 辞書に載っているような一般的な英単語ひとつだけ
　　password、baseball、soccer、monkey、dragon
(4) 同じ文字の繰り返しやわかりやすい並びの文字列
　　aaaa、0000（同じ文字の組み合わせ）

abcd、123456、200、abc123（安易な数字や英文字の並び）
asdf、qwerty（キーボードの配列）

(5) 短すぎる文字列
gf、ps

この他、電話番号や郵便番号、社員コードなど、他人から類推しやすい情報やユーザ ID と同じものなどは避けましょう。

また、組織の情報セキュリティポリシーでパスワードポリシーが定められている場合もあります。その場合は上記の注意点と合わせて情報セキュリティポリシーに則るようにパスワードを作成しましょう。

■ 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、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特に留意が必要です。

・ パスワードは、同僚等の第三者に教えずに、秘密にすること
・ パスワードを電子メールでやりとりしないこと
・ パスワードのメモをディスプレイなど他人の目に触れる場所に貼ったりしないこと
・ やむを得ずパスワードをメモなどで記載した場合は、鍵のかかる机や金庫など安全な方法で保管すること

なお、各サービスごとに異なる充分に安全なパスワードを覚えておくのは大変なので、パスワードを覚える必要のない、パスワード管理ツールを使うことも推奨されます。スマートフォンや Web ブラウザ標準機能、あるいは専用のアプリケーションのパスワード保存機能を活用しましょう。 これらのツールやサービスは、マスターパスワード（覚えられる充分に安全なもの）や、利用デバイス（スマートフォンなど）のロック（生体認証など）で守る必要があります。

なお、利用にあたっては、企業ごとに決まりを定めていることもあるので、情報システム担当者に相談・確認しましょう。

■ パスワードを複数のサービスで使い回さない（定期的な変更は不要）

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。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る等のサービス側から流出した事実がない場合は、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）インターネットの安全・安心ハンドブック Ver 5.00 p.114
https://security-portal.nisc.go.jp/guidance/handbook.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。

■ 多要素認証の活用

多要素認証とは、認証の 3 要素である「知識情報」「所持情報」「生体情報」のうち、2 つ以上を組み合わせて認証することを指し、多要素認証の中でも 2 つの要素を使う認証のことを 2 要素認証と呼びます。

多要素認証の具体例としては、ID・パスワード（知識情報）で認証した後に、ユーザが持っている機器（所持情報）にショートメッセージで送ったパスコードを入力させたり、指紋や顔（生体情報）などを用いた認証と組み合わせたりするなどです。

多要素認証を用いることでセキュリティレベルを高めることができます。利用するシステムで多要素認証の設定が可能な場合は積極的に利用しましょう。

電子メールの誤送信対策

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、送信方法の間違い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：）が自分の意図した通りになっているか、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。

データの保護・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。業務で通常使用するパソコンでは、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。

バックアップの方法や頻度等は、企業ごとにルールやポリシーで定められているため、そのルールやポリシーに従う必要があります。
一般的なやり方としては、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、Blu-ray Disc 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。

■ 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。

■ 外付けのハードディスク（SSD）

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。

■ 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、片面一層で 4.7GB、片面二層で 8.5GB、両面一層で 9.4GB、両面二層で 17GB 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。

■ Blu-ray Disc

DVD の後継にあたる光ディスクであり、一般に BD という略称で呼ばれています。DVD と同様に 12cm のディスクでありながら 1 層で 25GB と DVD の 5 倍以上（2 層のものは 50GB 保存可能）のファイルを保存することができます。BD-ROM は再生専用ディスクで

データを書き換えることはできませんが、データを一度だけ書き込める BD-R や複数回書き込める BD-RE といった書き換え可能ディスクもあります。

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。

データ持ち出し時の対策

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。

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。

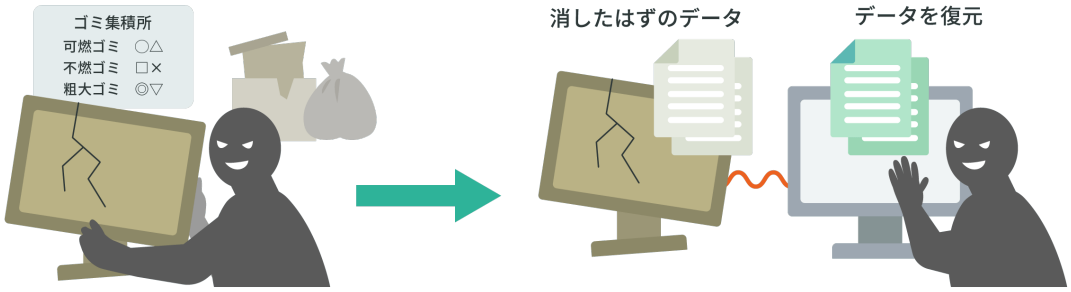
これらの持ち運び可能なメディアを外部へ持ち出した際には、カバンの置き忘れなどによる紛失と情報漏洩、自宅や外出先のパソコンからウイルス感染し、会社内のネットワークにも感染を広げてしまうなどの危険性が考えられます。これらのリスクを軽減するためには、次のような対策が考えられます。

- 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恐れがあるため、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。

安全なデータの廃棄

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や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。



捨てられたコンピュータを持ち出す　　コンピュータからデータを取り出す

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りしただけで、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。なお、SSD についてはその特性からハードディスク用のデータ消去ソフトでは完全に消去できない場合があるので、専用のソフトを使用するか物理的な破壊などを検討しましょう。
- 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。

- 「暗号化消去」を行う。
  ハードディスクや SSD へ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して読み出し不能とすることで、消去と同じ効果が得られます。

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、携帯電話・スマートフォン、CD-ROM や CD-R、DVD、USB メモリ、SD メモリカードといった記憶媒体、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。

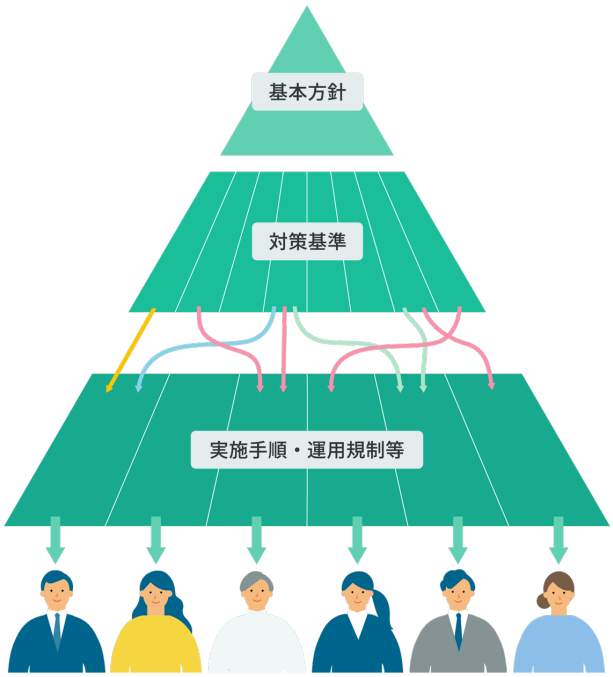
■ ごみ箱を漁る（トラッシング）

廃棄時に狙われる情報は電子データのみではありません。攻撃者は、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紙の資料から、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、溶解したりする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

情報セキュリティポリシーの順守

情報セキュリティポリシーとは、企業や組織において実施する情報セキュリティ対策の方針や行動指針のことです。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、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。



情報セキュリティ対策は画一的なものではなく、企業や組織の持つ情報や組織の規模、体制によって、大きく異なります。つまり、業務形態、ネットワークやシステムの構成、保有する情報資産などを踏まえた上で、その内容に見合った情報セキュリティポリシーを作成しなければなりません。

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の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、取引先や顧客からの信頼性の向上といった二次的なメリットを得ることもできます。

情報セキュリティポリシーを整備する上で大切なことは、情報セキュリティ担当者だけが

ネットワークやパソコンなどに対する情報セキュリティ対策を心がければよいというものではないという点です。情報資産を共有するすべての社員や職員が適切な情報セキュリティ意識を持たなければ、ウイルス、情報漏洩（ろうえい）などから組織を防御することは困難です。

情報セキュリティポリシーの内容に疑問がある場合や、行おうとしている行動にセキュリティ面での不安がある場合には、情報管理担当者に相談するようにしましょう。

SNS の正しい利用

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。
- 発信内容が著作権や肖像権の侵害に該当しないようにする。

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。