情報セキュリティの基礎

アイ・エス・ケー株式会社

2012.03

◆情報資産とは

資産とは、企業の業務遂行の過程で生み出される価値あるもののことです。資産には、不動産や商品など目に見えるものもあれば、財務情報、人事情報、顧客情報、技術情報などの目に見えないものもあります。

これらのことを情報資産といい、情報セキュリティ上の脅威から守る必要があります。

企業には、多くの情報資産が蓄えられており、それらはコンピュータ、記憶媒体、紙、または人の記憶や知識など、様々な形態をとります。ITの普及に伴い、情報資産の価値は、ますます高まっているといえます。

◆情報セキュリティの三大要件

情報セキュリティとは、企業の情報システムを取り巻くさまざまな脅威から、情報資産を機密性・完全性・可能性（三大要件）の確保を行いつつ、正常に維持することです。

機密性の確保

情報資産を正当な権利を持った人だけが使用できる状態にしておくこと。

・情報漏えい防止、アクセス権の設定などの対策

完全性の確保

情報資産が正当な権利を持たない人により変更されていないことを確実にしておくこと。

・改ざん防止、検出などの対策

可能性の確保

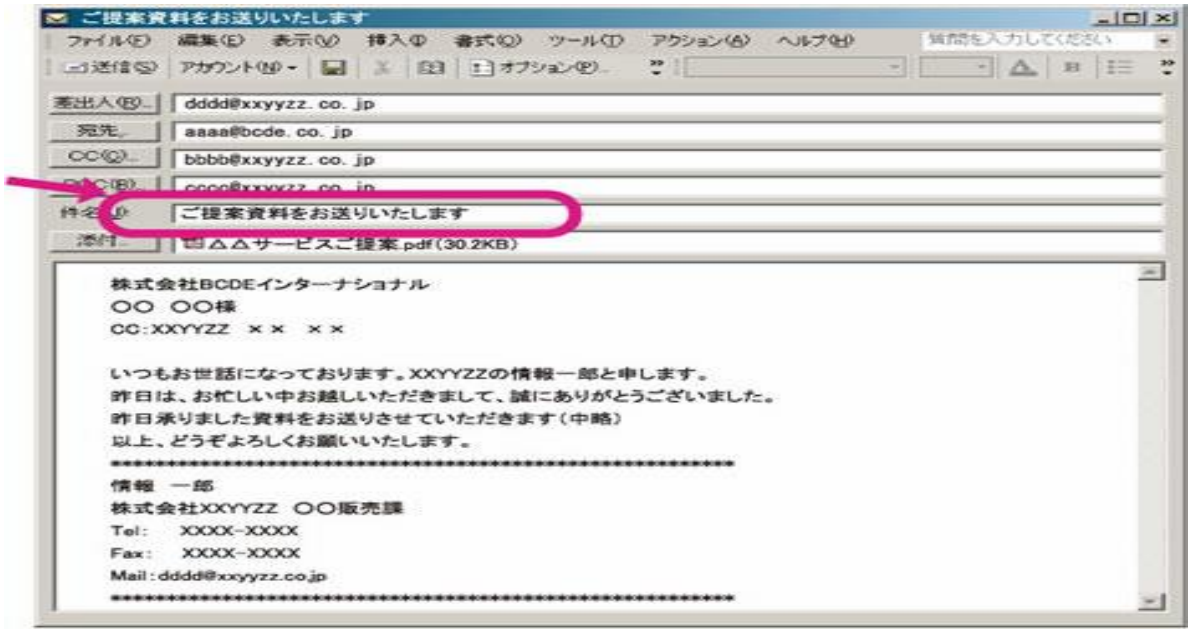
情報資産を必要なときに使用できること。

・電源対策、システムの二重化などの対策

◆メールのマナー

メールの標題は的確な表現で

標題（Subject）は、メールを読んでもらうための重要な要素です。以下の点に留意しましょう。



わかりやすい標題を心がける

本文を読まないと内容がわからない標題は、相手が多忙な場合、重要な用件でもかぐに読んでもらえない可能性がある。

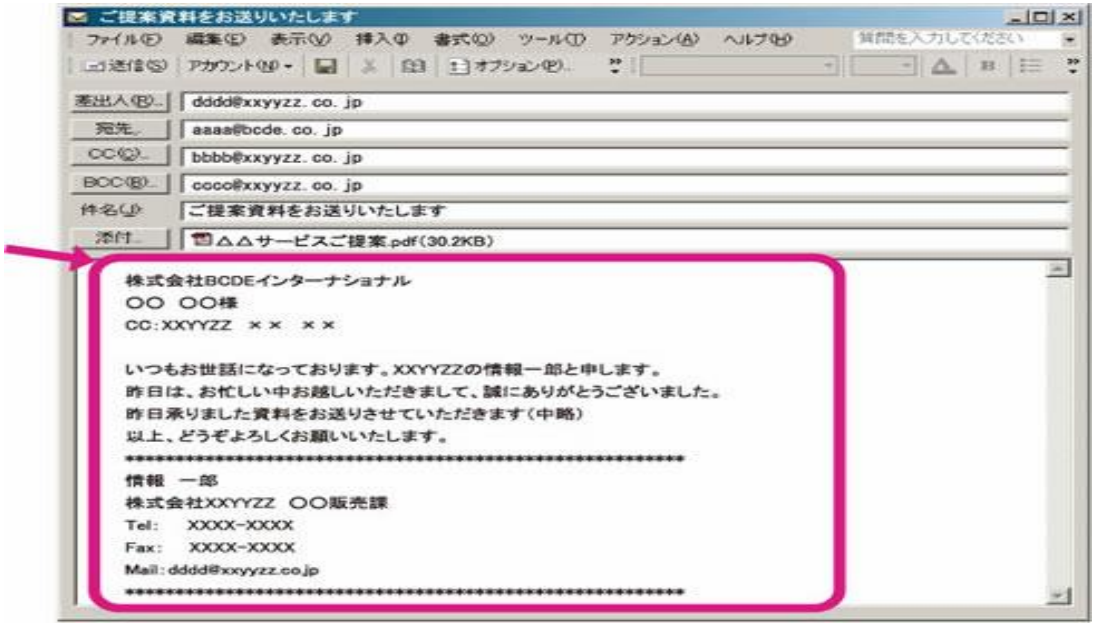
極端に長い標題も、よく読まないとわからないため不適切である。

誤解を受けないような標題にする

ウィルスなどの誤解を受けないために、空白や紛らわしい標題をつけないよう注意する（意味のある標題をつけるよう配慮する）

メール本文はていねいかつ簡潔に

メール本文の書き方は、基本的に手紙の書き方と同じです。ていねいな言葉づかいで、初めてのメール相手やお客様に失礼のないよう留意しましょう。



文字だけのコミュニケーションでは、こちらの意図する以上に強い調子や冷たい調子で伝わることがあります。できるだけ柔らかい表現を心がけ、感情的な文章を書かないようにしましょう。

そのほか、以下のような点に留意しましょう。

- ・業務にかかわりないメールは送らない
- ・機種依存文字や特殊文字を使わない
- ・海外へのメールは、相手側の環境に注意する
- ・極端に長い文章を避ける
- ・改行やスペースを適宜使用し、読みやすさを重視する
- ・メールの返信、転送に、先方のメールの文章を使用する場合、引用したことが明確になるよう、引用文字などを使用する

◆メールソフトのセキュリティ対策

メールソフト（Outlook Express、Windowsメール等）の各種セキュリティ機能を有効にするだけでも、メールによるウイルス感染を、未然に防ぐことが可能です。ここでは、その代表的な例を紹介します。

メールのプレビュー表示を行わない

受信したメールをプレビューしただけで感染するウイルスがあります。

メールの読み取りおよび送信をテキスト形式にする

HTMLメールに貼られたJavaスクリプトやActiveXコントロールの自動実行により、ウイルス感染かることがあります。

◆CC:、BCC:の誤使用による個人情報漏えい

多数の人に同一内容のメールを送りたい。

このような場合、宛先メールアドレスをCC:やBCC:に指定した一斉同報メールは非常便利です。

しかし、CC:、BCC:の使い方を適切に行わなかったことによるトラブルが多発しています。

事例

メール誤送信での個人情報漏えい（2008年12月）

子供向け番組を提供しているK社が、番組オーディションへの応募者に対して結果を発表するメールを送った際、誤ってアドレスが表示された状態となったことがわかった。誤送信が発生したのは、番組オーディションへの応募者に対し送られた結果発表に関するメールである。同社によれば、従業員が一斉送信した際、誤って応募者615人のメールアドレスが表示された状態になったという。

メールアドレスが第三者に流出するだけでなく、メールの内容によっては、プライバシーの漏えいにつながることもあります。

◆宛先指定ミスによる情報漏えい

メールは一度送信してしまうと取り消しができません。

CC:やBCC:の使い分けだけでなく、メールアドレスの指定に不備があると、以下のようなトラブルが起こる可能性があります。

指定したメールアドレスが存在しない場合

指定したメールアドレスが間違っていて、しかも存在しないアドレスである場合、メールは先方へ届かず、差し出し人にエラーメールが返ります。必要な相手に必要な情報が届かず、業務が滞る原因になります。

指定したメールアドレスが第三者のものであった場合

指定したメールアドレスが想定した相手のものとは違っていても、アドレスそのものが実在する場合、そのアドレスを所有している第三者にメールが届きます。

関係のない第三者にメールの内容を知られる

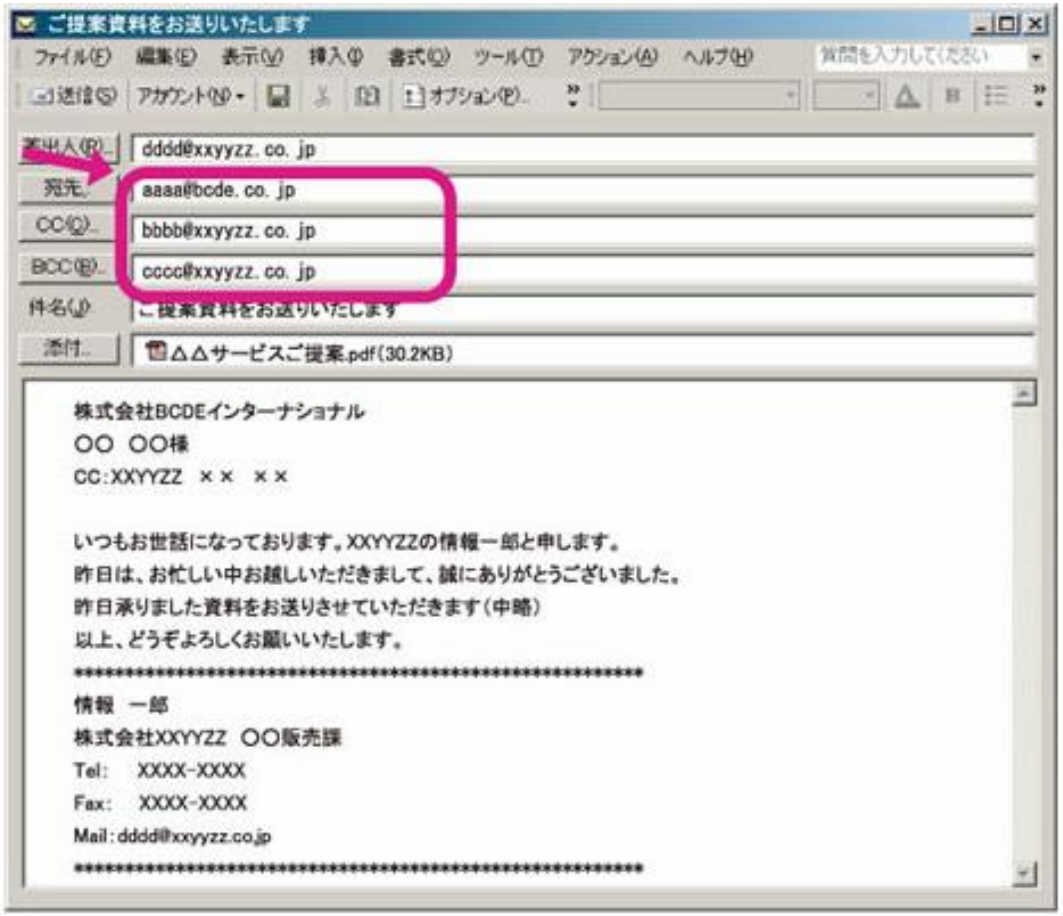
企業の機密情報がメールに記載されていた場合、機密情報が漏えいする

本文の内容によっては、本来の宛先となる人（お客様や取引先企業など）の個人情報が漏えいする

◆宛先の適切な指定方法

メールの一斉送信において、CC:、BCC:を適切に使い分ける

CC:、BCC:は、ともに同一内容の通信文を多数ユーザに配信する（一斉同報）ときに使用する機能ですが、違いをよく理解して、適切な指定を行うようにしましょう。

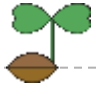


⇒ CC（カーボンコピー）は、受信側で、自分以外にメールを受け取った人が誰かということがわかる

⇒ BCC（ブラインドカーボンコピー）は、受信側で、自分以外の誰にこのメールが同報されているかわからない。したがって、メールによる情報提供サービスなど、お互いに面識のない複数の人にメールを一斉同報する場合、送信先となる相手の個人情報保護の観点から、すべてのメールアドレスをBCC:として指定することが望ましいといえる。

◆添付ファイルによるトラブル

メールの添付ファイルは、頻繁に使用される機能の一つですが、以下のようなトラブルが起きる可能性があります。



大容量ファイルの添付

企業によっては、「ネットワークのトラフィクを上げてしまう」などの理由で大きなサイズのメールを送受信しないよう、メールサーバを設定している場合があります。

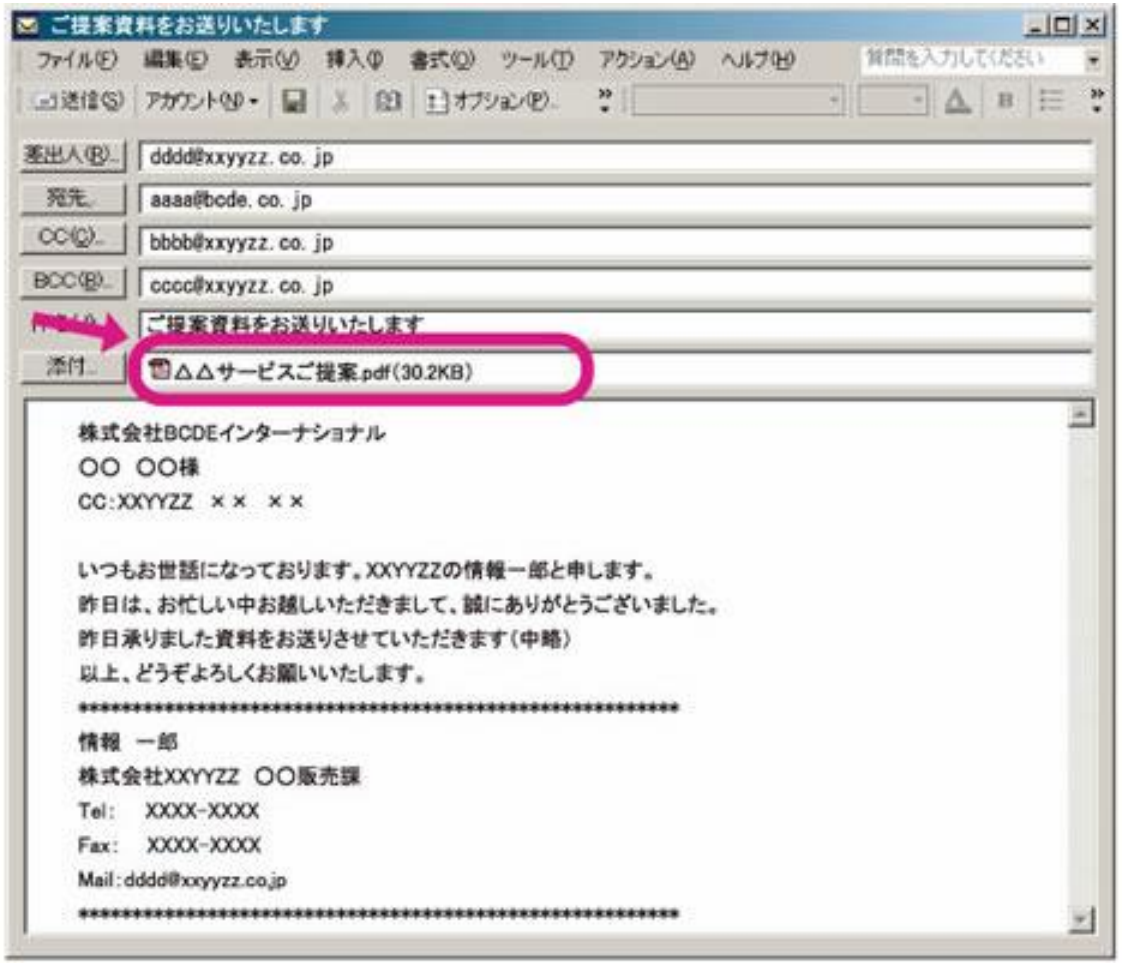
必要な情報が相手に届かない

ファイルサイズが大きくなればネットワーク負荷も高くなる

非常識なサイズのメールの送信は自社および相手先の業務妨害にもなりかねない

◆添付ファイルに気をつける

添付ファイルはメールの便利な機能の一つですが、添付ファイルについても注意事項があります。



添付ファイルの名前や拡張子に気をつける

⇒ ネットワークのルールで、特定の拡張子のファイルの送受信を拒否している場合があるため、先方にあらかじめ確認や了承を得ておく

⇒ 実行形式のファイルや、ウイルスなどと紛らわしい名前のファイル名を避ける（誤解を受けないため）

極端に大きなサイズのファイルを添付しない

⇒ 大きなサイズのファイルは圧縮してから添付するか、分割して送信する

⇒ 送信側または受信側のネットワークのルールで送受信できない場合もあるため、先方にあらかじめ受信の可否を確認する

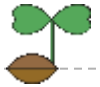
重要情報、機密情報を添付ファイルで送らない

⇒ 重要な内容でなくとも、取引先相手の企業名、個人名が記載されていれば個人情報になる

⇒ 添付ファイルのパスワード設定や暗号化を行う

◆減らない迷惑メール

迷惑メール（スパムメール）とは、広告や嫌がらせなどの目的で不特定多数に大量に送信されるメールのことです。最近では、詐欺やウイルス感染を目的とするものも多く、その扱いには注意が必要です。



迷惑メールによる被害

インターネット上に流れるメールの90%以上が迷惑メールであるという統計もあるぐらいに、大量の迷惑メールが日々配信されています。迷惑メールによって、以下のような被害が考えられます。

⇒ 迷惑メールの対応に時間が取られ、業務の妨げになる

⇒ 大量の迷惑メールに埋もれて重要なメールを見逃してしまう

⇒ ネットワークの負荷などによって、重要なメールの送受信が遅延する

⇒ ウイルスが添付された迷惑メールによって、受信したパソコンがウイルスに感染する

⇒ 迷惑メールの本文やリンク先によって、詐欺に巻き込まれてしまう

（フィッシング詐欺、ワンクリック不正請求　等）

【出典】情報セキュリティ白書2009（IPA)

◆迷惑メールへの対策

各企業にて行うべき迷惑メールへの主な対策は、以下のとおりです。

迷惑メールに反応しない

⇒ 迷惑メールに対して返信しない

⇒ 迷惑メールの本文に書かれたURLをクリックしない

興味本位に開かない

⇒ 迷惑メールは、興味本位で開かずに、そのまま削除する

⇒ 添付ファイルは絶対に開かない

⇒ メールソフトのプレビュー機能は使用しない

迷惑メールの数を減らす

⇒ プロバイダのブロックサービスを利用する

⇒ ウイルス対策ソフトの迷惑メール対策機能を利用する

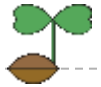
⇒ メールソフトの迷惑メール対策機能を利用する

◆増加する標的型攻撃メール

近年、特定の組織や個人を狙って情報窃取等を行う標的型攻撃が多くなっています。不特定多数に対する攻撃ではなく、ある特定の対象を狙って攻撃が行われることから、標的型攻撃の呼び名があります。中でもメールを使った標的型攻撃メールはソーシャルエンジニアリングの手口を使っており、だまされやすいため注意が必要です。

通常、迷惑メールの中でも悪意あるメールは、添付ファイルを開かせることでウイルスに感染させたり、特定のサイトに誘導することで気付かれないようにウイルスを送りつけることがあります。標的型攻撃メールでは、これと同様の攻撃パターンを含み、なおかつあたかも正当な業務や依頼であるかのように見せかける件名や本文でメールを送りつけ、受信者がだまされやすいような仕掛けをしています。特に昨今は、受信者に関係ある実在の発信元を詐称するケースが増えており、被害を受けやすくなっています。

このため、標的型攻撃メールに対しては、利用者は発信元に問い合わせるなどして受信したメールの信頼性を確認する、添付ファイルを開かない、リンク先を安易にクリックしないなど、十分な注意をはらう必要があります。



標的型攻撃メールによる被害

標的型攻撃メールによる被害は増加傾向にあります。標的型攻撃メールが送信される背景には、組織や個人の機密情報を盗み取ろうとする意図や、組織内ネットワークやシステムの最深部にたどり着くための踏み台（中継点）を確保しようとする意図、詐欺に巻き込もうとする意図などが考えられます。

標的型攻撃メールの受信により、次のような被害が発生することが考えられます。

⇒ 標的型攻撃メールの判定に時間を取られ、業務の妨げになる

⇒ ウイルスが添付された標的型攻撃メールの閲覧によって、受信したパソコンがウイルスに感染する

○ ウイルスの動作例：

- ネットワーク上において組織外部への接続口を勝手に開く
- 感染パソコン内の情報を収集して外部に送信する
- 感染パソコンが組織内ネットワークやシステムの最深部にたどり着くための踏み台（中継点）とされ、重要な機密情報を奪う足がかりとされる

⇒ 標的型攻撃メールの本文やリンク先のURLによって、ウイルスに感染させられたり、詐欺に巻き込まれたりしてしまう（フィッシング詐欺、ワンクリック不正請求等）

⇒ 標的型攻撃メールによる攻撃を受けたパソコン内部の情報が、次の標的型攻撃メールによる攻撃を成功させるための情報として悪用される（例：宛先、差出人、件名、本文、署名等への利用）

◆標的型攻撃メールへの対策

各企業にて行うべき標的型攻撃メールへの主な対策は、以下のとおりです。前述した迷惑メール対策に加えて、特に人的な対策を強化する必要があります。

基本的な対策

⇒ 迷惑メール対策を徹底する（標的型攻撃についても一定の効果が得られる場合がある）

標的型攻撃メールを開かない

⇒ 件名や内容が不自然なメールについては開封しない
（開封する際は、送信者に対してメール送信の事実があるかを確認する）

⇒ 不自然なメールが着信した際は、たとえ興味のある件名でも開封しない

標的型攻撃メールを開かせない

⇒ 利用者に対する教育を実施し、標的型攻撃メールの見分け方を訓練する

⇒ 標的型攻撃メールが着信した際は、システム管理者に対して着信の事実を通知し、組織内への注意喚起を依頼する

メールを開いた後で標的型攻撃と気づいた場合の対応

⇒ 添付ファイルは絶対に開かない

（ウイルス対策ソフトでは検出できない攻撃が仕組まれているケースも多い）

⇒ メールの本文に書かれたURLをクリックしない

⇒ システム管理者に対して着信の事実を通知し、組織内への注意喚起を依頼した後に、メールを速やかに削除する

◆オフィスにおける情報漏えい

社内には、さまざまな情報資産があります。その中には、社外に公開できない以下のような「機密情報」も多くあります。

⇒ 顧客や社員の個人情報

⇒ 開発中の新商品に関する情報

⇒ 社内での会議資料　　など

これらの情報を狙う第三者は、訪問者や清掃人、他支店の社員などを装ってオフィス内部に入り込み、以下のような方法で情報を盗みます。

⇒ 画面に表示された顧客情報などを盗み読む、隠し撮りする

⇒ 机の上に放置された書類や媒体、モバイルパソコンを持ち去る

⇒ 廃棄書類等を持ち出す　　など

デスクトップパソコンであっても、近年小型化しており、持ち去られる可能性は高くなっています。

◆身のまわりの情報漏えい

オフィスの中のさまざまな場所に情報資産が存在しています。部屋の中にあるからといって油断せず、以下の点に留意して情報資産を取り扱いましょう。

クリアデスクポリシー

常に、机の上の整理整頓を行いましょう。美観を損ねる、という理由ではなく、機密情報を印刷した書類や媒体などを目に付く場所に放置しないようにしたり、情報の紛失を防いだりするためにも必要なことです。）

クリアデスクポリシー

クリアスクリーンポリシーとは、パソコンなどの情報機器から離れる場合に、ディスプレイに情報が表示されないようにして、他人が容易に操作できない処置を行うことです。

⇒ システムからログオフする

⇒ 画面のロックを行う（パスワード付きスクリーンセイバーなど）

機密情報を表示したまま席を立ち、他人に盗み見されたり、情報を改ざんされたりするなどの事故を防ぐために重要な処置です。

◆PCや記録媒体（紙含む）の管理

パソコンの管理

⇒ クリアスクリーンポリシーを遵守する

⇒ 退社時は電源を落とし、他人に使われないようにする

⇒ メンテナンスや修理などで社外の業者へ一時的にパソコンを預ける場合、機密情報データは別途記録媒体に保存して、ハードディスクから完全消去しておくなどの対策を実行する

CD、DVD、USBメモリ、SDカードの管理

⇒ 廃棄の必要がある場合、媒体を初期化したうえで、破砕してから廃棄する

⇒ 管理者の許可なく、自宅へ持ち帰るなど社外に持ち出さない

⇒ 私用の記録媒体は持ち込ませない

機密情報を印刷した用紙の管理

⇒ 機密情報を印刷した用紙は、プリンタ、FAX、コピーなどで、裏紙として再利用しない

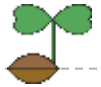
⇒ 機密情報を出力機器に印刷した場合、すみやかに文書を自席に持ち帰るようにする

⇒ 機密情報が印刷された用紙を廃棄する場合、細かく裁断し、鍵のかかるゴミ箱に入れ、溶解業者へ処理を依頼する

⇒ クリアデスクポリシーを遵守する

◆データのバックアップ管理

今やデータやプログラムは、企業にとって非常に重要な資産です。万が一、事故や障害により、データ等が破損・紛失してしまうと企業にとっては、大きな損失となってしまいます。そこで、定期的にデータやシステムを複製（バックアップ）し、きちんと管理する事が肝心です。



データの障害と復旧

データへの障害は、以下のように分類できます。

⇒ データ自体の障害

一番多い事柄は、管理者や利用者の操作ミスにより、必要なデータの削除、上書きをしてしまうことです。また、ウイルス感染による上書き（改ざん）が発生することもあります。
この対応には、データをいくつかの世代管理しておくことです。

⇒ 物理的な障害

データが保管されている装置（主にハードディスク）の障害であり、装置自体の故障、天災（地震、火災、水害）、盗難があります。
この対応には、データを別の場所、別媒体で保管しておくことです。

バックアップの方法

一般的には、以下の方法があり、組み合わせて管理しています。

⇒ 外部媒体（CD／DVD、フラッシュメモリ、ハードディスク、テープ）方式

低価格な機器、媒体でデータのバックアップがとれる。媒体は、ネットワークやPCと別の場所に保管したり、耐火金庫で保管する。

⇒ ネットワーク（ハードディスク、ストレージ、オンラインストレージ）方式

ネットワークを介して、バックアップを目的としたハードティスク、ストレージを用いたバックアップをとれる。最近では大容量のディスクを用いているため、複数世代のバックアップが可能となっている。また、深夜、休日での自動バックアップ作業ができるため、管理工数が削減できる。

バックアップの運用

バックアップの対象を決定させるためには、そのシステムの用途、重要度に加え、万が一障害が生じたとき復旧させるための費用を考慮して決定します。また、その運用管理としては、対象、保管種類、頻度、保存期間、保管場所　等を決めておく必要があります。

⇒ 対象

バックアップするデータ、プログラムのことである。

⇒ 保管種類

データを保管するために、フルバックアップ、差分バックアップ、増分バックアップの種類がある。

⇒ 頻度

バックアップの時間的間隔。毎日行う、１週間単位で行う、１ヶ月単位で行う等を決める必要がある。

⇒ 保存期間

データの保存する期間であり、頻度と世代管理に影響される。また、会計データ、財務データ、個人情報データ等、データ種類によっては、法的に保存期間が設定されている。

⇒ 保管場所

外部媒体により保管する時、その媒体の保管は、ネットワーク／サーバ管理部署と異なる施設に保管する事が望ましい。しかしながら、同一施設に保管せざるを得ない場合、耐火金庫等の設置が不可欠である。
ネットワーク方式の場合、ほとんどがサーバ設置場所と異なる施設となっているが、さらに地理的に離れている場所、安全な施設に預けたほうが良い。

◆モバイルパソコンの管理

社外でノートパソコンなどを持ち歩き、文書作成をしたり、スケジュール管理をしたり、お客様にプレゼンテーションを行ったりするなど、モバイルパソコンはさまざまな用途に利用できます。

しかし、モバイルパソコンは、「携帯に容易な、小型、軽量の機器である」という特性のため、携帯中に紛失、盗難の被害に遭う可能性が高いのです。モバイルパソコンに会社の機密情報が保存されていた場合、機密情報の漏えいにつながります。モバイルパソコンの取り扱いには十分注意しましょう。

⇒ 機密情報をむやみに保存しない

⇒ 外出先でモバイルパソコンを放置しない

⇒ 航空機、列車などでの移動中は、モバイルパソコンを手荷物として携帯する

⇒ 飲酒および、うたた寝をしない

⇒ バックアップを外部メディア（可搬型HDDを含む）に行う場合には、メディアの盗難対策を行うこと

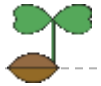
そのほか、外出先で作業中、画面に表示された情報を他人にのぞき見されないように注意することも重要です

◆ユーザーIDとパスワードの管理

パソコンからネットワークにログオンする場合、最初にユーザIDとパスワードを入力します。情報へアクセスするためには、ユーザIDとパスワードの入力の手続きを省略することはできません。

⇒ ユーザIDとパスワードの入力＝扉の鍵を開ける動作

⇒ 特に「鍵＝パスワード」の管理は重要である



推測されにくいパスワードを使う

パスワードが漏えいすると、悪意を持った他人が自分になりすまして情報にアクセスすることも可能になります。パスワード漏えいを防ぐための第一歩は、推測されにくいパスワードを用いることです。

⇒ パスワードの内容に、生年月日や名前（家族や友人、知人の名前も含む）、電話番号など、個人情報に類する情報を使わない

⇒ ８文字以上の長さにする

⇒ 大文字と小文字、数字や記号を混ぜる

⇒ 初期パスワードは必ず変更する（初期パスワードは社員番号や 生年月日など、便宜的に設定されるものが多いため）

⇒ 同じパスワードの使いまわしは避け、定期的にパスワードを変更する

パスワードの自己管理を適切に行う

推測されにくいパスワードでも、パスワードそのものを見られてしまえば意味がありません。パスワード入力に際しては、以下の点に留意しましょう。

⇒ パスワードを入力しているところを見られないようにする

⇒ パスワードをメモ書きして目に付くところへ貼ったりしない

⇒ パスワードの自動入力設定を行わない

⇒ パスワードを忘れないようにする

◆ファイルサーバーのセキュリティ対策

LAN上のファイルサーバは、日常業務に必要なさまざまなデータが蓄積されています。IDとパスワードが漏えいし、そのIDとパスワードを外部の第三者に悪用された場合、社内の機密情報を盗まれる可能性もあります。

IDとパスワードを適切に管理する

特に、パスワードは扉の鍵のようなものです。第三者に漏えいしないようにしましょう。

⇒ 決して口外しない

⇒ メモに書きとどめ、目立つ場所に貼ったりしない

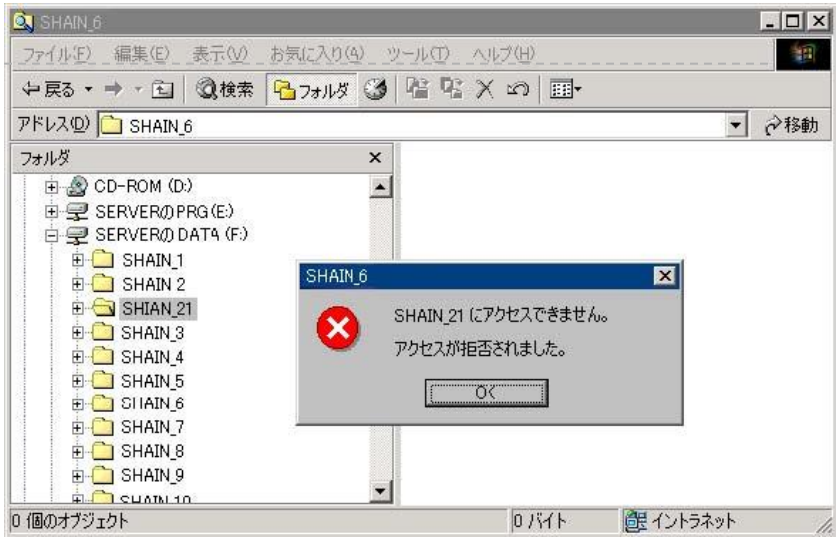
⇒ 初期パスワードはすみやかに変更する

そのほか、定期的にパスワードを変更することも効果的です。

アクセス権を適切に管理する

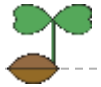
サーバの共有資源を、必要な人が必要な権限で使用できるように、アクセス権を適切に設定します。

アクセス権を設定した場合、自分にアクセス権が与えられていないフォルダは参照できません



◆wwwサーバーのセキュリティ対策

セキュリティ関連製品を導入し、技術面での対策を行うことも効果的ですが、WWWサーバの運用を適切に行うことも重要です。



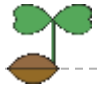
不正アクセスを許してしまう要因を減らす

⇒ セキュリティに関する最新情報を取得するよう、常に心がける

⇒ Webアプリケーションサーバのソフトウェアは常に最新バージョンを使用し、修正プログラムがあればインストールする

⇒ サーバの設定のままにせず、必要なサービスのみ有効にしておく

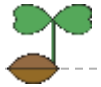
⇒ サーバ管理者以外によるシステムへのログインを制限する



情報漏えいにつながる要因を減らす

⇒ ホームページで個人情報を収集しているなどの場合、データは別のサーバ上で管理する

⇒ ホームページで収集した情報の取り扱いについて、社内のルールを明確にし、ルールを遵守する



不正アクセスを監視する

⇒ アクセスログを取り、不審なアクセスがないことを定期的にチェックする。および、アクセスログは一定期間（一年以上）、安全に保存管理しておくこと

⇒ 侵入検知ツールなど、専用のツールを導入する

◆ソーシャルエンジニアリングとは

ソーシャルエンジニアリングは、もともと日本語では「社会工学」と訳されており、学問の一つとして理解されてきました。「社会工学」は、人間の社会的行動を科学的に研究し、社会生活上の実際問題を解決する学問です。

不正アクセスの手段としてのソーシャルエンジニアリングを定義すると、おおよそ以下のとおりです。

⇒ **ソーシャルエンジニアリング**

ネットワークシステムへの不正侵入を達成するために、コンピュータの技術やネットワークの技術を利用するのではなく、侵入に必要なID、パスワードや、企業の機密情報などを、物理的手段（あるいは心理的な手段）によって獲得する行為

最近では、企業、個人を問わず、不正アクセスを目的とした第三者に、いつのまにか情報を収集されているケースが増えています。

ソーシャルエンジニアリングにはさまざまな手法があります。

巧妙な手法で目的の企業に入り込みます。

清掃員になりすまして構内侵入

◆構内侵入

「構内侵入」は、実際に建物内に侵入する行為です。以下のような方法でオフィスに侵入します。

⇒ 偽造または拾得したIDカードで社員として入る

⇒ カードリーダーなど機械によるチェックを行う扉の場合、他の社員の後ろに付いて一緒に入る

⇒ 清掃員や回収業者として（なりすます、実際に仕事に就くなど）入る

⇒ 他の用件で訪問したついでに、他の部署に入る

オフィスへの侵入に成功したあと、目的の情報を収集するため、ゴミ箱を探す、システムに不正侵入する、のぞき見をする・・・などの行動に移ります。

◆物理的セキュリティの強化

企業では社員の他にさまざまな訪問客に加え、派遣社員、アルバイト、パートなど、多様な勤務形態の従業員がオフィスを出入りします。オフィスへの入退管理を強化して、正当な用件のない部外者を社内へ不正に侵入させないようにしましょう。

⇒ オフィスの施錠管理を行う

⇒ 入退室の履歴を記録に残す（台帳記入など）

⇒ 身分証を発行し、従業員に携帯させる

⇒ 出入りが激しい場所については、不審者がいないかどうかを常に留意する

また、可能ならば、以下のような対策を実施すると、より効果的です。

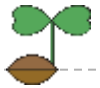
⇒ セキュリティカードなどで出入り口の制限を行う

⇒ 出入り口に守衛を配置したり、監視カメラを設置したりする

⇒ バイオメトリクス（生体認証）など、より強固なシステムを導入する

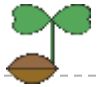
◆なりすまし

不正アクセスの標的となる部署や個人に電話をかけ、ユーザIDやパスワードを巧みに聞き出す行為です。



社員になりすます

社員を装ってシステム管理者に電話をかけ、
「パスワードを忘れてしまったので教えて欲しい」
「今日から出社した中途社員だがIDとパスワードがわからない」
などと言って聞き出します。

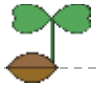


プロバイダなどのシステム管理者になりすます

⇒個人でプロバイダを利用しているユーザに電話をかけ、「システムのメンテナンスのためユーザIDとパスワードを確認させていただきます」などと言って聞き出す

⇒「御社の情報部門からの委託で社員番号とIDパスワードのチェックをおこなっている」などと言って聞き出す

システム管理者を名乗るだけで信用されやすい、という盲点を突いています。



企業のエグゼクティブになりすます

標的となる社員と面識のない役員が誰かを事前に調査し、その役員になりすまします。「ログインできない。急いでいるのでなんとかしろ。」など高圧的な態度で迫り、答えざるを得ない雰囲気を作って聞き出します。

手段は電話だけではない

電話だけでなく、さまざまな媒体が使用されます。

⇒葉書などでアンケートを装って情報を収集する

⇒メールのヘッダーを偽装し、なりすましメールを送ってだます

◆電話によるなりすましの対策

電話で、IDやパスワードなどに関する問い合わせを受けた場合、安易に教えないようにし、なりすましによる漏えいを防ぎましょう。

⇒折り返し連絡をし、本人確認を行ったうえで質問に答える

⇒公衆電話など、本人が特定できない電話からの問い合わせは答えない

上記のほか、情報セキュリティポリシーなどに、「ID、パスワードの再発行は、本人が直接システム担当部署に出向いて手続きを行う」などの規定をおこなっている企業もあります。オフィスのルールとして、電話対応での対策を徹底するようにしましょう。

◆のぞき見

オフィス内では、さまざまな場所に情報が露出しています。オフィスに入り込むことができれば、情報をのぞき見ることは容易です。よくある例は以下のとおりです。

⇒ディスプレイの周りに貼られている付箋やメモ

⇒キーボードで入力中のパスワード

⇒机の上に放置された情報

⇒FAX、プリンタに放置された印刷物

◆トラッシング

トラッシング（Trashing）は、ゴミとして廃棄されるなど、不要となったものの中から、目的とする情報を探し、取得する方法です。
スカビンジング（scavenging）ともいいます。

オフィスでこんなことはしていませんか。

⇒顧客リストを印刷したら、プリンタが紙詰まりしたので捨てた

⇒社外秘の内容の回覧を、部署内で回して終わったので捨てた

⇒使い古しのフロッピーディスクを捨てた

◆情報の機密性確保

トラッシングやのぞき見により、情報はどこから第三者に漏えいするかわかりません。油断は禁物です。

文書は機密性を考慮した廃棄を行う

⇒ 決められた箱の中に回収して、溶解処理業者へ

⇒ シュレッダー処理をする

媒体は破砕する（再読不可能な状態にする）

⇒ 物理的に叩いて壊す

⇒ 媒体用のシュレッダーを使用する

自席を離れるときも情報漏えい対策

⇒ ディスプレイの電源を落とす、画面をロックする、ログオフするなどの対策を行う（クリアスクリーンポリシー）

⇒ 書類などを放置しないよう、机の上を整頓する（クリアデスクポリシー）

◆ウイルス感染

ウイルス感染の兆候

このような場合は、ウイルス感染を疑ってください。

⇒ パソコンの起動に時間がかかるようになった、または、起動できなくなった

⇒ システムの動作速度が遅くなった、または、途中で動かなくなった

⇒ 画面上に、奇妙なメッセージが表示された、または、音楽が流れた

⇒ 突然データが消えた

⇒ 身に覚えのないメールを送信しているパソコンの動作が遅い

ウイルス感染の主な経路

ウイルスは、パソコンのあらゆる環境に潜んでいます。

⇒ **メールによる感染**

メールの添付ファイルからウイルス感染する場合があります。添付ファイルには、マイクロソフト社のOfficeアプリケーション（例えば、WORD、EXCEL）や、色々なプログラム（拡張子が．EXE など）が、多いといえます。また、メールのプレビューをしただけで感染するもの、メール本文がHTML形式で書かれたメールに感染している場合があります。

⇒ Webによる感染

HP（ホームページ）の閲覧によりウイルス感染する場合があります。これは、HP自体（図、写真、音楽）、または、ダウンロードしたプログラムにウイルスが埋め込まれている場合があります。また、HPを閲覧するWebブラウザにも、ウイルスが潜んでいる場合もあります。

⇒ ファイル共有ソフトからの感染

インターネットを利用して不特定多数のコンピュータ間でファイルの共有や交換を行うソフト(Winny、Share)があります。ファイル共有ソフトでやり取りされるファイルにはウイルス感染しているものが多く、このソフトを会社で利用していた場合、ウイルス感染の危険性が非常に高くなります。

⇒ USBメモリからの感染

USBメモリには、PCに接続したときに自動的に実行するプログラムを組み込むことができます。このプログラム（ウイルス）に感染すると、接続したPCや他のUSBメモリにも感染していきます。

⇒ CD(DVD)-ROM、フロッピーディスクからの感染

雑誌の付録、出所不明なCD、DVD、フロッピーディスクからも、ウイルスに感染することがあります。

メールを介したウイルス感染

特に目立つ被害が、メールを介した感染です。

⇒ メールの添付ファイルとしてパソコンに侵入する

⇒ メールのプレビューによりウイルスが実行される場合もある

⇒ 添付ファイルの実行により感染するが、感染したことに気付かない

⇒ パソコンに登録してあるメールアドレスに、自動的にウイルス付きメールが送信される

⇒ 送信されたウイルス付きメールは記録が残らないため気付かない場合がある

【事例】

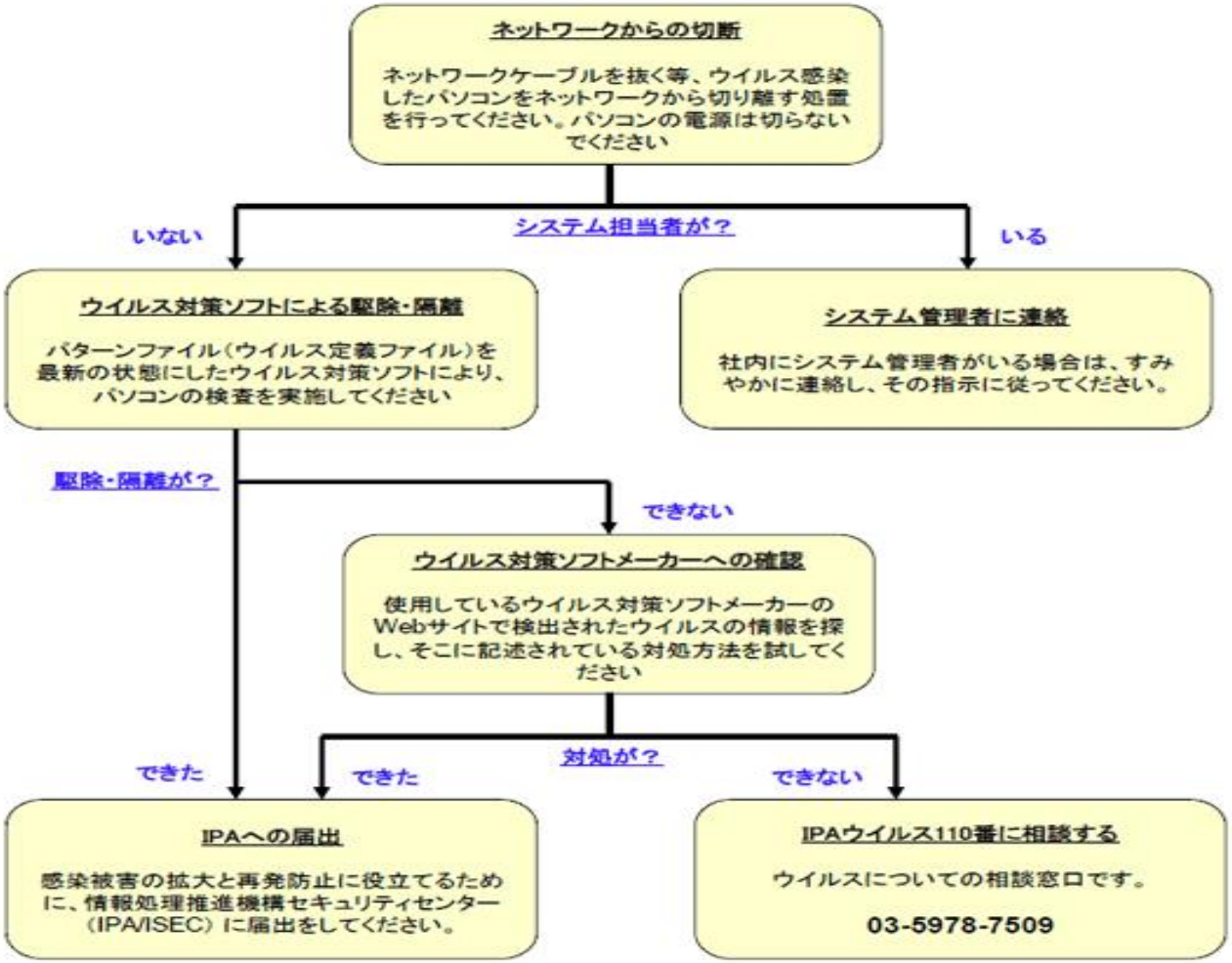
新型インフルエンザの注意喚起に便乗したウイルス（2009年4月）

情報処理推進機構（IPA）は、新型インフルエンザの話題に便乗したウイルスに対して注意を呼びかけている。IPAに寄せられた相談の中には、実在する研究機関を装った偽の注意喚起メールにウイルスを添付し、パソコンに感染させようとする事例もあった。今回のように世界中で注目されるニュース報道の直後は、それに便乗してウイルスを感染させようとする手口が多発するため、IPAでは、自分の身に覚えのないメールの添付ファイルは開かないように呼びかけている。

【出典】コンピュータウイルス・不正アクセスの届出状況について（IPA）

もしウイルスに感染していたら

ネットワークに接続されたパソコンでウイルス感染が発見された場合、既に他のパソコンにも感染している場合が多いため、自分勝手に対処することは危険です。以下のフロー図に従い、適切な対処をおこなってください。また、社内にシステム管理者がいる場合は、すみやかに連絡し、その指示に従ってください。



◆スパイウェア

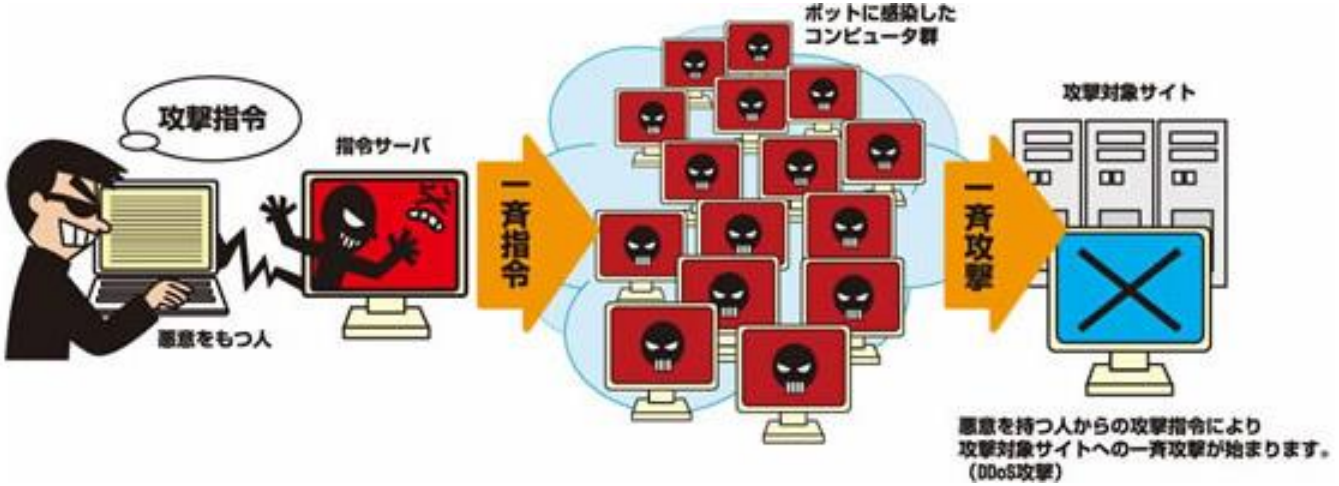
スパイウェアとは

スパイウェアとは情報を収集する不正なプログラムで、Webサイトの閲覧履歴、「ID・パスワード」などパソコンに入力した情報、コンピュータに保存されている情報を収集し、悪意のある第三者に送信してしまうものです。

◆ボット

ボットとは

ボットはユーザのコンピュータに侵入（感染）し、ネットワークを通じてこのコンピュータを外部から操る目的を持つ不正プログラムです。そして、感染してしまったコンピュータは被害者であると同時に加害者になってしまうという点も大きな問題と言えます。



【出典】
情報セキュリティ読本改訂版（IPA）
小規模企業のための情報セキュリティ対策（IPA）
対策のしおりシリーズ（IPA）

◆ウイルス対策（スパイウェア・ボット対策含む）

ウイルス対策ソフトを使う

ウイルス対策として最も効果的なのは、ウイルス対策ソフトを利用することです。
ウイルス対策ソフトは、常に進化しており、現在のウイルス対策ソフトはコンピュータウイルスだけではなく、新たな脅威への対策も含んだ「統合セキュリティ対策ソフト」に進化しています。

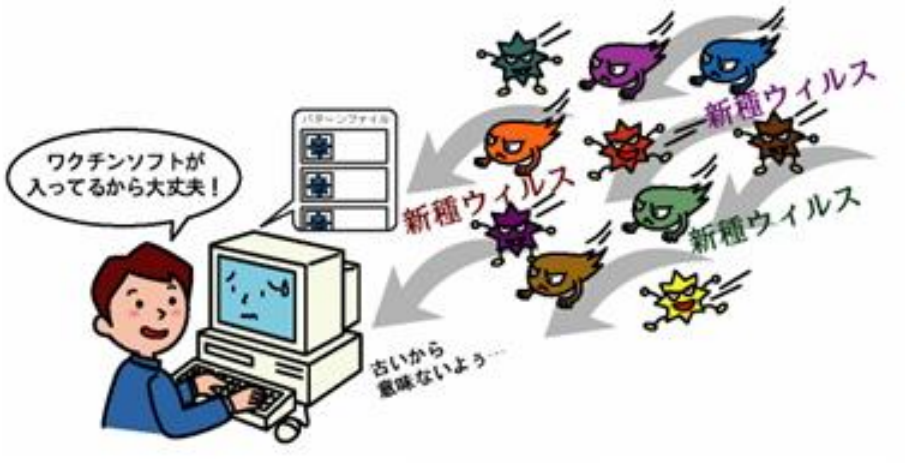
現在のウイルス対策ソフトはほぼ全自動で安全な状態を保ってくれますが、セキュリティに絶対はあり得ません。以下の点には注意が必要です。

⇒ パターンファイルを最新の状態に保つ

⇒ 出来るだけ最新のソフトウェアを使用する

⇒ 試用版ではなく製品版を利用する

⇒ ウイルス対策ソフトは、全社共通のものを使用する



OSやソフトウェアのアップデート

OSやブラウザ、メールソフトなどのソフトウェアは、メーカーによっては「セキュリティホール」を修正したり、セキュリティ上の問題を解決したり、ソフトウェアの不具合を解消したりするための修正プログラムが、インターネット経由で提供されることがあります。インターネットに接続されたコンピュータを利用する場合には、これらの修正プログラムを定期的に適用して、できる限りソフトウェアを最新の状態に保つように心がける必要があります。

このアップデートの代表的なものに、以下に説明する「Microsoft Update」があります。また、ワープロソフトや表計算ソフトなどその他のソフトウェアについても、情報セキュリティ上の問題などで修正プログラムが提供されることがあります。これらについても、コンピュータにインストールされているソフトウェアを確認して、それぞれのメーカーのWebサイトなどで定期的にチェックしてください。

また、最近ではソフトウェアのメーカーにユーザ登録をしておくと、プログラムが更新された場合にメールで連絡がくるサービスもあります。利用しているソフトウェアについては、必ずユーザ登録をしておきましょう。

Microsoft Update

Windows Vista やWindows XPなどのWindows系のOSでは、修正プログラムを自動的に適用するための「Microsoft Update」という機能が導入されています。タスクバーの右下に「アップデートの準備ができました」というメッセージが表示された場合は、自動的にアップデートする機能が準備されていることを表します。その場合には、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

重要！

パターンファイルが古ければ、ウイルス対策ソフトをインストールしていても、月に数百個のペースで生まれる新種のウイルスを発見することはできません。パターンファイルや検索エンジンの更新は、ウイルス対策ソフトの機能で、スケジュール設定での自動実行や、手動で実行することができるようになっています。ウイルス対策ソフトを常に最新の状態に保つことが重要です

◆フィッシング詐欺

フィッシング詐欺とは

巧妙な文面のメールなどを用い、実在する企業（金融機関、信販会社、オンラインショップなど）のWebサイトを装った偽のWebサイトにユーザを誘導し、クレジットカード番号、ID、パスワードなどを入力させて盗み取る不正行為です。

その典型的な手口は、以下のとおりです。

⇒ **ユーザを錯誤させるだましメール**

〇送信元がいかにも存在する企業のメールアドレスになっている

〇メール本文が真実味のある内容になっている

⇒ **本物に見間違えるような偽のWebサイト**

〇リンク先のWebサイトで、実在する企業名やロゴが使われている

〇実在のWebサイトと全く同じデザインになっている

⇒ **個人情報の入力を求める**

〇個人情報の入力を受け付けるフィールドが用意されている

フィッシング詐欺への対策

フィッシング詐欺は、ユーザをだますことによって成り立っています。したがって、怪しいメール、リンク先、Webサイトは、まず疑ってかかることが原則です。フィッシング詐欺の被害に遭わないためには、以下の点に注意しましょう。

⇒ メールの送信元（差出人）を安易に信用しない

⇒ メールの内容を安易に信用しない

⇒ リンクを安易にクリックしない

⇒ 入力前に本物のサイトかどうか確認する

〇アドレスバーに正しいURLが表示されているか確認する

〇SSL接続を示す錠アイコンがないWebサイトに個人情報を入力しない

◆ワンクリック不正請求

ワンクリック不正請求とは

出会い系サイト、アダルトサイト、投資関係サイト、ダウンロードサイトなどを装ってユーザが訪れるのを待ち、単にクリックをしただけで、入会金や登録料などの名目でユーザに料金の支払いを求める不正請求行為です。その典型的な手口は、以下のとおりです。

⇒ **個人が特定されているものと勘違いさせる**

〇パソコンでアクセスした場合、IPアドレス、接続プロバイダ名などが表示される

〇携帯電話でアクセスした場合、キャリア名、機種名などが表示される

⇒ **文言で不安をあおる**

〇「自宅や会社に回収へ行く」「法的な処置を行う」 等

ワンクリック不正請求への対策

⇒ **信頼できないWebサイトへはアクセスしない**

一般サイトを閲覧中にアダルトサイト等が表示されても、好奇心や興味本位でボタン等をクリックしないで、絶対にそれ以上先に進まないようにしてください。

⇒ **請求があっても、基本的には無視をする**

〇Webサイトの利用契約が成立するためには、料金が明示されたうえでの利用の意思確認が必要です

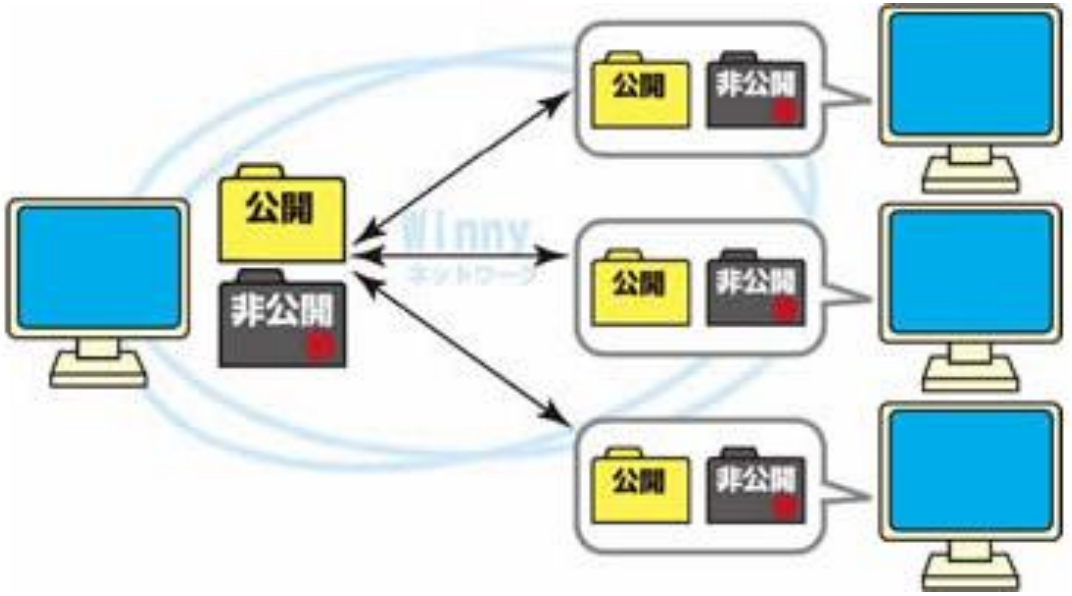
〇ワンクリックでは個人を特定する情報を、Webサイト側で把握することはできません

〇心配な場合は、最寄りの消費生活センターや国民生活センター等に問合せ、自分だけの判断で安易に入金しない

◆ファイル共有ソフト

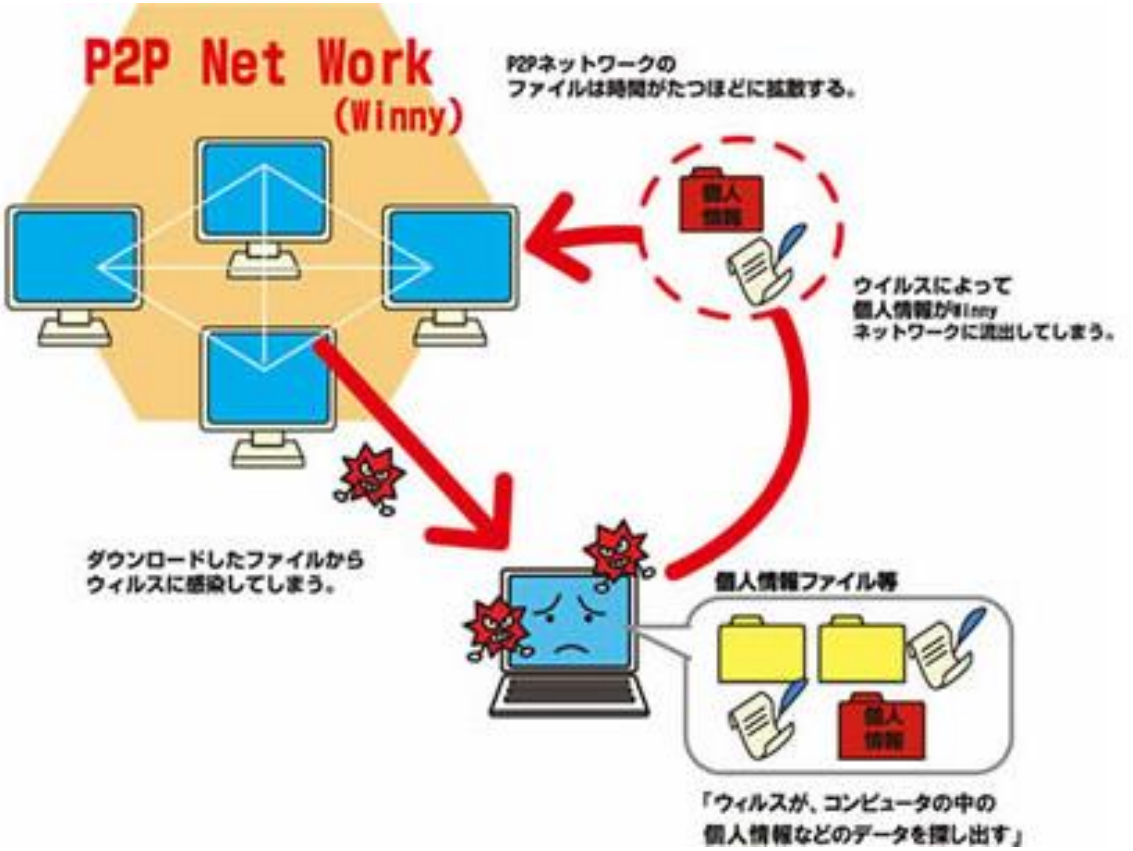
ファイル共有ソフトとは

インターネットを利用して不特定多数のコンピュータ間でファイルの共有や交換を行うソフトウェアのことです。代表的なものとして、Winny、Share、Cabos、LimeWire などがあります。これら多くのファイル共有ソフトでは、公開したいファイルを置くフォルダは、自分で設定します（下図を参考）。
つまり、利用者の操作ミスや設定の誤り一つで公開したくないファイルを公開してしまい、情報が漏えいする可能性があります。「公開」フォルダに置かれたファイルは、ファイル共有ソフトを利用している不特定多数のユーザ同士で共有されるため、その行き先がわからなくなってしまいます。そのうえ、ファイルが多くの利用者にダウンロードされてしまうと、回収が事実上不可能になってしまいます。
このように、ファイル共有ソフトの利用には多くの危険を伴います。よって、単なる興味本位で利用することは絶対に慎まなくてはなりません。



ファイル共有ソフトによる情報漏えい

ファイル共有ソフトを利用して情報を漏えいさせるウイルスの多くは、多数の人が興味を持つ単語を含むファイル名で出回っています。ユーザがファイル共有ソフトを利用してそれらのファイルをダウンロードし、ファイルを開くことにより、情報を漏えいさせるウイルスがユーザのパソコンに感染してしまいます。
パソコンに感染したウイルスは、パソコン内の各種の情報を一つのファイルとしてまとめ、公開フォルダにコピーしてしまいます。また、この過程でウイルス（自分自身）を紛れ込ませます。
こうして、ウイルスがパソコンの中から各種の情報をファイル共有ネットワークに流出させて情報漏えいが起きることになるとともに、情報を漏えいさせるウイルスもファイル共有ネットワークに広がっていきます。



ファイル共有ソフトからの情報漏えい対策

ファイル共有ソフトからの情報漏えいを防ぐには、次のような対策が考えられ、それらを組み合わせて実施することが有効と考えられます。

⇒ 職場のパソコンだけでなく、自宅のパソコンにもファイル共有ソフトはインストールしない

⇒ 職場のパソコンに許可なくソフトウェアを導入しない、または、できないようにする

⇒ 職場のネットワークに、私有パソコンを接続しない、または、できないようにする

⇒ 自宅に業務データを持ち帰らない

⇒ 職場のパソコンからUSBメモリやCD等の媒体に情報をコピーしない、または、できないようにする

⇒ 漏えいして困る情報をメールで送らない、または、送れないようにする

⇒ ウイルス対策ソフトを導入し、最新のパターンファイルで常に監視する

⇒ 不審なファイルは開かない

◆USBメモリ感染型ウイルス

USBメモリとは

USBメモリとは、USBコネクタに接続して使用する持ち歩き可能なフラッシュメモリのことです。最近は、大容量化と低価格化が進み、利用機会が増えていますが、USBメモリにおけるウイルス対策には、あまり意識が行き届いていないのが実情です。

USBメモリによるウイルス感染の仕組み

最近のパソコンにはUSB メモリが接続されると、そのUSBメモリの中に置かれたプログラムを自動的に実行する機能があります。USBメモリ感染型ウイルスは、この機能を悪用して感染活動を行います。
ウイルス感染したパソコンに、別の USB メモリを接続すると、その USB メモリにウイルスが感染し、USB メモリ感染型ウイルスが拡散していきます。

ウイルスの特徴

⇒ ウイルスファイル自身のアイコンや属性情報を偽装し、データファイルとして見える場合があります

⇒ 起動中のウイルス対策ソフトなどを強制終了させます

⇒ ウイルスの駆除や感染確認作業を妨害します

主な被害内容

⇒ Windows が正常に動作するために必要なシステムファイルが破壊される

⇒ 各種アカウント情報(ID やパスワード)が盗まれる

⇒ 他のウイルスをダウンロードさせられる

などの被害が発生することを確認しています。

USBメモリ感染型ウイルスへの基本的な対策

⇒　ウイルス対策ソフトのパターンファイルを常に最新の状態に更新して、リアルタイムのウイルス検知機能を有効にしておく

⇒　パソコンだけでなく、USB メモリに対しても定期的なウイルスチェックを行う

⇒　ぜい弱性を突かれてのウイルス感染を防ぐため、OS、アプリケーションを常に最新の状態に更新して、ぜい弱性を可能な限り解消する

USB メモリの使用における対策

⇒　自身が管理していない USB メモリや所有者の不明なUSBメモリは、自身のパソコンには接続しない

⇒　自身が管理していないパソコンや不特定多数が使用するパソコンには、自身の USB メモリを接続しない

⇒　自宅から職場にウイルスを持ち込んだりしないよう、個人所有の USB メモリを会社のパソコンに接続しない、また、会社所有の USB メモリを自宅のパソコンに接続しない

無線LAN

近年、無線LANが注目されています。配線を必要とせず、オフィスの中で手軽にネットワークを構築することができるためです。しかし、無線LANは、通信の特異性ゆえに情報を盗聴される危険性があります。

⇒ アクセスポイントをフレキシブルに設置できるため、設置場所によって屋外に情報が漏えいしやすくなる

⇒ LANケーブルなどの配線を必要としないため、クライアントとなるパソコンの移動が容易であり、盗難に遭いやすい

⇒ 盗まれたパソコンで屋外から不正アクセスされる危険性がある

⇒ 無線LANの利便性を追求するため、セキュリティ確保に対する意識が高まりにくい（セキュリティ技術を実装していないアクセスポイントが多いなど）

無線LANの情報セキュリティ対策

無線LANを利用する際は、以下のような設定を行うことにより、セキュリティを高めることが不可欠です。

⇒ **ESS-IDの設定**

無線LANは、アクセスポイントを中心にネットワークが構成されます。それぞれの無線LANを識別するために、アクセスポイントにはESS-ID（Extended Service Set ID）と呼ばれる識別子を設定します。無線LANを初めて利用するとき、アクセスポイントには、工場出荷時のデフォルトのESS-IDが設定されています。

⇒ **初期設定のままで使用しない**

〇機器や使用者を推測しにくい値に変更する

〇「ANY」または「空白」のESS-IDを設定したクライアントからの接続を拒否する設定に変更する

〇ESS-IDの通知を無効にする

◆クラウドサービス

クラウドサービスとは

「クラウドサービス」とは、利用者がコンピュータ処理を主にインターネット経由で利用する形態である「クラウドコンピューティング」で提供されるITに関するサービスのことです。企業や個人が個別にコンピュータやアプリケーションを所有して利用するのに比べて、ITに関する開発や調達や運用・保守の負担が軽減され、コスト削減にもなる技術、サービスとして注目されています。

クラウドサービス活用の利点

クラウドサービスでは、以下のような利点があると考えられています。

⇒ ITの調達に関わる負担からの解放または負担の軽減

⇒ ITの運用・保守の負荷からの解放または負荷の軽減

⇒ IT資源利用の柔軟性・拡張性の獲得

⇒ セキュリティ対策の負担と負荷からの解放または負担軽減

クラウドサービス利用上留意すべき事項

クラウドサービスの利用には、いくつかの懸念材料も指摘されています。

⇒ コンピュータシステムを自ら管理しないことによる制約

⇒ データを自らの管理範囲外に置く、あるいは社外に預ける不安や制約

⇒ 利用量・処理量の異常な増加や意図せぬ増大に伴う使用料の急増のリスク

⇒ 利用できるアプリケーションのカスタマイズの制約

⇒ アプリケーション間のデータ連携実現への制約やコスト増の可能性

これらの懸念材料については、各企業ごとの状況やクラウド事業者の情報を総合的に判断して、リスクを見極め、対策を施した上でクラウドサービスを利用する必要があります。

◆スマートフォン

スマートフォンは

「スマートフォン」は、従来の携帯電話機能に追加のソフトウェアをインストールすることで柔軟に機能が拡張できる携帯端末です。ここ1年ほどで急激に普及が進み、個人利用だけでなく、業務での利用も増えてきています。それに伴い、スマートフォンを狙った攻撃も多数確認されるようになってきました。

スマートフォンの更なる高機能化や利用者数の増加、想定される脅威等、今後の様々な状況を加味した対策と柔軟な運用が必要になります。

スマートフォンの主な脅威

主な脅威としては、紛失・盗難、社内ネットワークへの無許可接続、ウイルス感染、などがあります。

【紛失・盗難】

スマートフォンは、それ自体がデータを格納できるストレージになっているなど携帯電話よりも豊富な機能を持っているため、携帯電話の場合より大量でかつ機微な情報を保有している確率が高く、影響がより大きくなります。

【社内ネットワークへの無許可接続】

スマートフォンは従来の携帯電話方式での通信だけでなく、無線LANでの接続も可能な機種が多く、高速大容量の通信が行えることから、意図しない情報流出など、影響がより大きくなります。

【ウイルス感染】

OSに付属するウェブブラウザの脆弱性を悪用し、ウェブサイトを閲覧、またはファイルを開かせるなどして、スマートフォンに設定されているセキュリティ関連の制限を解除します。端末の制限が解除されることにより、攻撃による被害を受けやすい状態になります

また、正規のソフトウェアを装ったウイルスを端末にインストールさせるものもあります。スマートフォンのOSの脆弱性には関係なく、利用者が正規のソフトウェアを装ったウイルスのインストールを許可してしまった場合に被害を受けます。

スマートフォンのセキュリティ対策事情

PCに近い機能をもったスマートフォンですが、現時点ではOSに対するセキュリティパッチ提供までに時間がかかるなど、PCと同様のセキュリティ対策を実施することが難しい状況です。

利用者数の増加、柔軟な拡張性、不十分なセキュリティ対策等、悪意ある者が攻撃しやすい条件でもあるため、今後はさらに攻撃を受ける可能性が高まっていくと予想されます。このため、最低限のセキュリティ対策は実施する必要があります。

【最低限実施すべきセキュリティ対策】

⇒ 紛失・盗難時の対策

持ち運びが簡単であるがゆえに、紛失・盗難のリスクは高まります。そのため紛失や盗難に注意するだけでなく、もしもの時のために端末の利用ポリシーをMDM(Mobile Device Management)で一括設定し、リモートでの端末ロック・データ消去などが行えるようにしておきます。

⇒ 社内ネットワーク接続のための運用管理ルールと教育

組織においてスマートフォンを利用する場合は、運用管理ルールの策定はもちろんのこと、スマートフォンの利用者に、リスクとそのセキュリティ対策にどのようなものがあるかを理解させることが重要です。活用のためのリテラシー(基礎的な使いこなし能力)教育をすることが不可欠です。

⇒ ウイルス対策ソフトの使用

ウイルスの脅威に対応するため、いくつかのスマートフォン用のセキュリティ対策ソフトが提供されています。該当機種に合った対策ソフトを使用することで、最低限の対策は講じておきましょう。

◆ソーシャルメディア

ソーシャルメディアとは

「ソーシャルメディア」とは、インターネット技術を利用した、誰でも比較的簡単に情報発信などができるコミュニティサービスであり、SNSやブログなどの総称です。文字情報だけでなく写真や映像・音声を、それぞれのソーシャルメディアに所属している個人や組織に伝えることができ、多数の人々による双方向での対話ができるのが特徴です。

これにより従来、電子メールや掲示板などが中心であったインターネットでのコミュニケーションは、このソーシャルメディアに移りつつあり、ここ1～2年で日本での利用者は爆発的に増えています。また、個人だけでなく、官公庁や地方公共団体、企業において、これらのサービスを情報発信やプロモーション、マーケティングなどのビジネス目的で利用する機会が急増しています。今後ますます利用者が増えることでリスクも増大しますので、ソーシャルメディアを安心・安全に利用するためには、利用者とサイト運営者それぞれにおいて適切な対策を講じることが必要です。

ソーシャルメディアの主な脅威と対策

ソーシャルメディアの特徴を悪用し利用者を騙したり、ウイルスに感染させようとしたりする攻撃も増えています。それぞれの脅威に対して適切な対策を実施しましょう。

【外部サイトへの誘導】

利用者が興味を持つような内容を発信して、ウイルス感染を目的とした外部サイトに誘導しようとしたりします。その際には、長いURL文字列を短縮して一見しただけではどのようなウェブサイトかわからないくなっている「短縮URL」を使ったりしているものもあります。

⇒　このような被害に遭わないためには、短縮されたURLの上にマウスカーソルを合わせて、正式なURLを確認するなどします。

【公開する情報の管理】

ソーシャルメディアに入力するということは、その内容を公開するということですので注意が必要です。また、IDやパスワード等の管理を適切にすることも重要です。

⇒　個人情報などを書き込まないのはもちろん、不適切な発言に注意が必要

⇒　自分のアカウントの設定(ID、パスワード、アプリケーションの連携、プライバシー情報の公開範囲等)を確認する

【不正アプリへの対応】

ソーシャルメディアでは、利用者どうしが直接メッセージをやりとりしたり、アプリケーションを追加できる機能など豊富な機能があります。この機能を利用して、怪しいサイトに誘導するメッセージを送りつけたり、不正アプリなどの脅威が多数出現してきています。これらのアプリケーションをインストールしてしまうと、交流のある他の利用者に意図しないにもかかわらずどんどん拡散したり、登録してある自分のプライバシー情報を悪用されたりしてしまいます。

⇒ 怪しいユーザーやアプリケーションをソーシャルメディアの機能でブロックする

⇒ もしも、不正アプリをインストールしてしまった場合には、あわてず削除をする

上記に挙げたものの他にも、ソーシャルメディアは一般的なウェブアプリケーションとしての脆弱性も狙われる可能性があります。利用者はこのようなことを念頭に置いて利用すること、またウェブサイト運営者はウェブアプリケーションの脆弱性への対策をすることが必要となります。

【事例】

仕事で得た情報をソーシャルメディアで発信

最近はソーシャルメディアの普及で、情報の発信がインターネット経由で簡単にできるようになりました。仕事で知り得た情報を気軽に発信してしまう人がいるのも事実です。

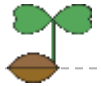
■ ホテルの従業員が有名人の宿泊を実名で発信して問題となった。

■ お店に来店した有名人のプライベートな内容を従業員が発信して問題になり、会社が公式に謝罪。

正しい情報を適正な方法で発信するのであれば法で守られますが、友人にメールをしている感覚でソーシャルメディアを使い、業務上知り得た内容をインターネットで発信するというのは、機密情報の漏えいとなり処罰の対象となる可能性があります。

◆事故が与える企業への影響

企業を取り巻くさまざまな脅威に対して、企業は関係する法律を遵守しつつ、十分な情報セキュリティ対策を施す必要があります。これらの情報セキュリティ対策は、企業の情報システムに携わる担当者だけの仕事というより、経営者が率先垂範し、会社全体として取り組む必要があります。万が一、情報セキュリティに関する事故、又は法令違反を生じさせると、企業にとって重大な経営的影響を与えられてしまいます。



情報セキュリティ事故が与える企業への影響

⇒ 行政からの指導

行政指導、業務停止、免許剥奪、刑事責任（懲役、罰金）、損害賠償責任

⇒ 社会的信用の低下

社会的信用・ブランドイメージの失墜、マーケットシェア低下、風評、株価暴落

⇒ 売上の減少

顧客からの取引停止、営業機会の損失

⇒ 対策費用の増大

見舞金・謝罪費、情報システムの改善費用

⇒ 社内のモラル低下

従業員の不安、不満、モラル低下

企業が知っておくべき関連法規

現在の日本は、ITによる社会基盤が整備され、ITに関する多くの法律が規定されているとともに、年々更新されています。企業においても、これらの法律を知らなかったとは言えず、自社の情報セキュリティ対策を実施する際に、関係する法律を遵守することは社会的責任として必要なことです。企業が最低限遵守すべきITや情報セキュリティに関する法律には、個人情報保護法、不正競争防止法、不正アクセス禁止法、及び著作権法等があります。これらの法制度を理解し、情報セキュリティ対策をはじめ、社内規程や各種契約書に反映させるには、知識と経験が必要となりますので、顧問弁護士やコンサルタントに相談すると良いかと思います。

⇒ 個人情報保護法

個人の権利や利益を保護するため、個人情報を取り扱う事業者に一定の義務を課した法律。事業者は、個人情報の利用目的を明確にし、適正に取得し、安全に管理しなくてはならない。

⇒ 不正競争防止法

企業の研究開発や業務活動の遂行の中で得られる新しい技術手法やノウハウを営業上の秘密として保護し、万が一その営業的秘密が盗まれた時に指し止め請求や損害賠償請求を行うことが出来る法律。

⇒ 不正アクセス禁止法

他人のIDやパスワードを無断使用やOSやソフトウェアの弱点の悪用により、コンピュータを不正に利用したり、保存してあるデータやプログラムを改ざんしたりする行為を禁止した法律。

⇒ 著作権法

第三者の著作物である音楽、画像、

プログラムやデータベースの無断使用を禁止する法律。

被害者が加害者に

不正アクセスの被害者は、不正アクセスを受けた結果、次の加害者になる可能性が高く、企業の社会的信用に大きな影響を与えることになります。

⇒ 不正アクセスを受けた企業の被害

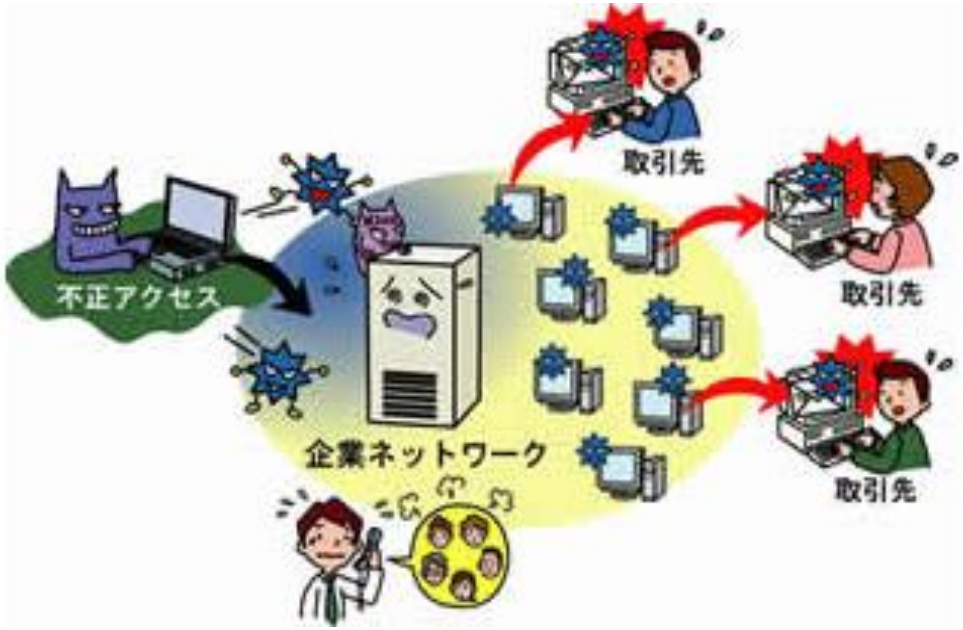
〇ネットワークの停止で業務が滞る

〇ウイルスの侵入や情報漏えい

⇒ 二次的な被害（被害者が加害者になる）

〇ウイルスに感染したメールなどを送信してしまい、顧客企業のネットワークに感染を広げてしまう

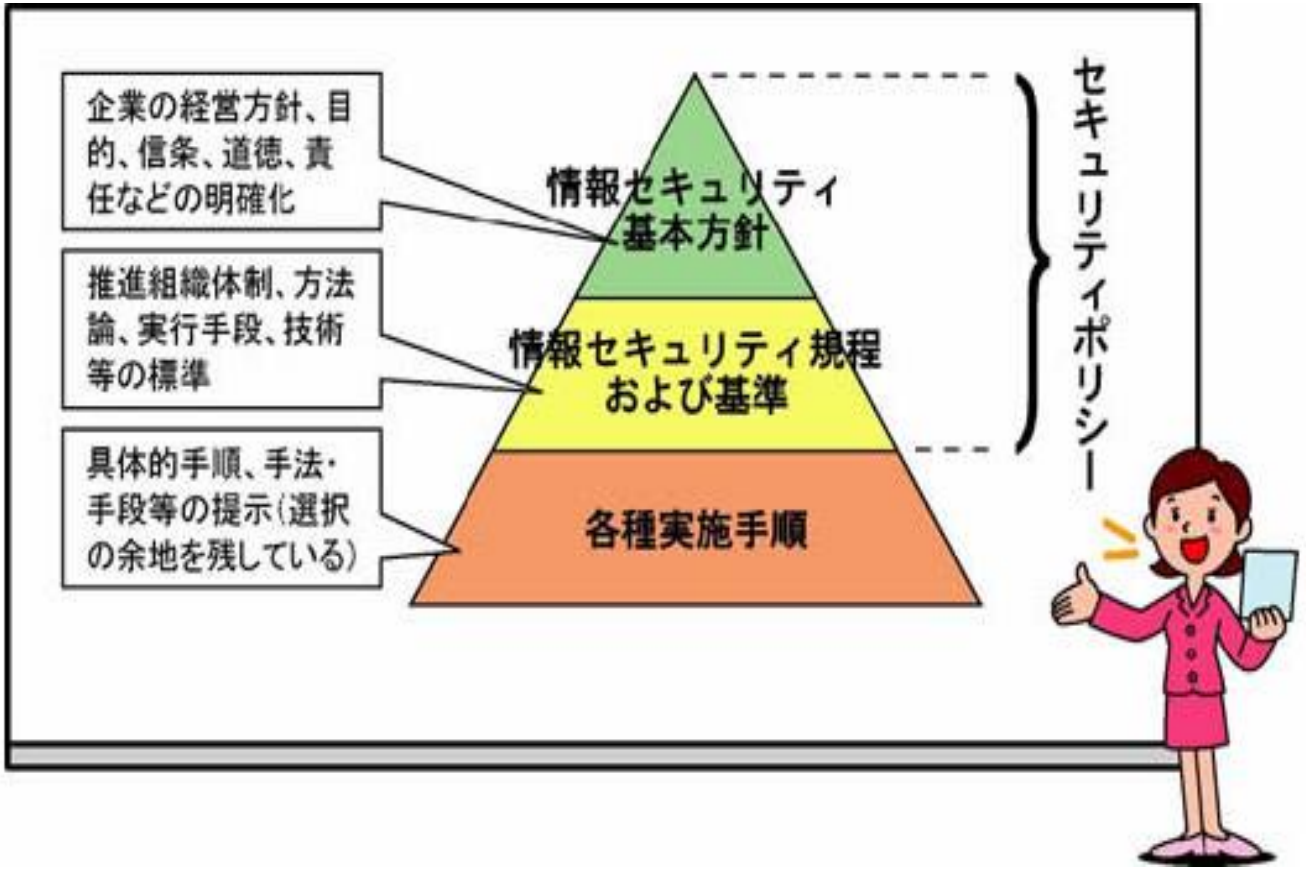
〇サーバが踏み台になり、迷惑メールなどの不正中継を許してしまう



◆セキュリティポリシー

セキュリティポリシーとは

セキュリティポリシーとは、企業の「情報資産」を守るための情報セキュリティ対策を具体的にまとめた社内ルールのことです。セキュリティポリシーの構成は、以下のようになります。



⇒ 情報セキュリティ基本方針

経営者の声明文であり、企業として情報セキュリティにどのように取り組むかを表明する文書です。企業の経営方針、目的、責任などを明確にします。

⇒ 情報セキュリティ規程

情報セキュリティ対策の全般にわたって必要な、適用範囲や定義、責任と要件、遵守義務などを規定する文書です。

⇒ 情報セキュリティ基準

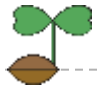
情報セキュリティ対策のための個別規程であり、情報セキュリティ対策の対象別の基準を規定します。「基準集」として1部の文書にまとめることも、各基準を別々の文書に分けることも、どちらも可能です。

主な基準

機密情報取り扱い基準 ・ ネットワーク管理基準 ・ ソフトウェア管理基準 ・
ユーザリテラシ管理基準 ・ 安全対策基準 ・ ウイルス対策基準 ・ ソフトウェア開発基準 など

◆社員への教育

長い時間をかけ、緻密にセキュリティポリシーを作成したとしても、社員が遵守しなければ意味がなくなってしまいます。社員への教育は、企業風土に合った方法で、継続的（1回／年程度）行うことが大切です。また、社員の立場に立ち、理解しやすい表現を用い、大きな負担をかけない気配りも必要です。



教育の方法

⇒ 集合研修

就労者に対し、一番最初に行う教育方法としては、大変効果的です。このため、新人・中途社員、パート、アルバイト、派遣社員が就労した時に、実施します。時間は、1時間から半日程度がよいでしょう。ただし、教育する場所（会議室、食堂等）を確保することが欠点です。

⇒ eラーニング（Webラーニングとも言う）

この教育は、インターネットを介しておこなう教育のため、いつでもどこからでも教育を受けられるメリットがあります。このため、年1回継続的に教育させる場合、又は就労先が遠隔地で集合教育の開催が出来かねる場合に大変効果的です。ただし、内容（コンテンツ）の開発費用、サーバの維持管理費等、経費がかかります。

⇒ パンフレット・チラシ

会社のセキュリティに対する考え方をまとめたパンフレット・チラシは、取引会社、顧客へ企業の経営姿勢を示すのに大変効果的です。特に、この説明には、社員自らがおこなうことが多く、社員の自覚を促すことにもつながります。

⇒ ポスター

定期的な教育は、その教育が終了すると、就労者はセキュリティに対する意識が薄れてきます。そこで、新入社員の入社時期、年始年末等、会社の催事に併せたポスターを作製し、普段からの啓蒙活動をすることは、セキュリティ意識を醸成する効果があります

◆委託先としての対応

企業は、日々の事業活動を行う中で、外部へ業務委託をする場合が多い。例えば、総務・営業部署は、清掃業者、警備会社、宅配業者、廃棄業者、DM業者等、情報システム部署は、ソフト開発業者、システムのアフターサポート業者等、工場は、人材派遣業者、配送業者等がある。これら業務委託する場合、企業のセキュリティポリシーや情報セキュリティ対策を理解してもらうことは勿論のこと、具体的な委託契約を締結しつつ、定期的な管理を行うことが必要です。また、委託される側の企業としても、預かった情報をしっかりと管理できる仕組みや対策を講じておくことが、仕事の受注にも影響するようになってきています。対外的なアピール材料としては、定期的に外部のセキュリティ監査を受け、監査報告を提示することや、プライバシーマークや「ISMS」等の情報セキュリティに関する第三者認証を取得するなどの方法があります。

委託契約書に盛り込むべき事項

⇒ 委託内容、範囲、責任の明確化

⇒ 委託契約期間

⇒ 守秘義務の取り決め

⇒ 委託契約終了後の情報の取り決め（返還・消去・廃棄等）

⇒ 再委託に関する取り決め

⇒ 委託業者の情報セキュリティ管理に対する内容

⇒ 契約内容を遵守していることの確認

⇒ 契約内容を違反した場合の措置

⇒ 契約内容を違反した場合の措置

◆事業継続計画（BCP）

企業では、事業の中断を引き起こすような地震等の災害等に対し、復旧を図り、早急に最低限の事業を継続していく必要があります。事業継続計画（Business Continuity Plan：BCP）とは、そのための計画を策定し、訓練をすることで、万一の災害等が発生した場合に、実際に事業の継続ができるよう備えを行います。

現実的な事業継続計画を策定し、これに沿って訓練を行うことはもちろん、災害・障害発生後に事業継続を行うためには、特に経営陣の強いリーダーシップが必要です。

事業の中断を引き起こす可能性のある事象

⇒ 地震・津波・火災のような自然災害

⇒ 電力・通信のような社会インフラの障害

⇒ 新型インフルエンザに代表される感染症の世界的な大流行（パンデミック）

⇒ 米国同時多発テロにみられるようなテロ攻撃

計画策定のポイント

可能性がある全ての災害・障害に対する事業継続計画を策定することは困難です。そのため、地震のような突発的に発生する事象と、計画停電やパンデミックのようにある程度の時間をかけて発生する事象を分けて、事業継続計画を策定することが望まれます。

事前の準備

⇒ データバックアップ

災害・障害発生時に情報が失われないように、情報のバックアップを取得しておくことが重要です。取得した情報は災害・障害で失われないように、別の場所にデータを保管します。さらに、災害・障害に強い場所のデータセンターにサーバを設置するなどします。

⇒ 就業場所の確保

業種によっては、別の場所で業務が継続できるようにオフサイト（遠隔地）のシステムや業務エリアを確保することも有効です。

⇒ 在宅勤務

業種にもよりますが、在宅勤務を取り入れ、万一の際に自宅から業務が継続できる仕組みも考えられます。在宅勤務は計画停電などの節電にも有効と考えられています

◆事件・事故の対応

前章まで説明してきた情報セキュリティに関する対策は、その脅威に対して直接的な対策を説明してきました。しかしながら、その対策が遅れた、対策は行ったがすでに情報資産が流出してしまったなど、情報漏えいの事件・事故が生じてしまった場合に企業としてすべき対応を、まとめました。
この対応方法は、IPA 「情報漏えい発生時の対応ポイント集」に、まとめられていますので、ご紹介いたします。
⇒ 「情報漏えい発生時の対応ポイント集」

1. 基本的な考え方
2. 情報漏えい対応の基本ステップ
3. 情報漏えいのタイプ別対応のポイント
    - 3-1 紛失・盗難の場合の対応
    - 3-2 誤送信・Webでの誤公開の場合の対応
    - 3-3 内部犯行の場合の対応
    - 3-4 Winny/Share等への漏えいの場合の対応
    - 3-5 不正プログラム（ウイルス、スパイウェア等）
    - 3-6 不正アクセスの場合の対応
    - 3-7 風評・ブログ掲載の場合の対応
4. 発見・報告におけるポイント
5. 通知・報告・公表等におけるポイント
6. 参考情報

◆点検と見直し

企業を取り巻く環境は、市場環境、顧客ニーズ、取引先との関係等により、日々変化しています。加えて、万が一、事件・事故が生じた場合、その原因究明と新たな情報セキュリティ対策を施すことにより、社内体制、社内規程の変更を行う必要があります。企業は、このような環境変化がある度、社内の情報セキュリティ対策の点検と改善を施し、情報セキュリティレベルを維持管理する事が肝心です。

点検が必要と思われる状況

⇒ 市場環境、顧客ニーズの変化

⇒ 取引先、委託業者の変更

⇒ 事件・事故への対応

⇒ 会社、委託元からの要望

⇒ 社内の情報インフラ、情報システムの追加、変更

⇒ 社内の組織、業務、運用の変更

点検方法

点検するためには、「点検リスト」があると大変便利です。

IPA 「5分でできる！中小企業のための情報セキュリティ自社診断」は、簡単な25項目のチェックリストに答えるだけで、企業の情報セキュリティ対策度合いを診断してもらえます。