

初めての情報セキュリティ 対策のしおり

新入社員の皆さん
「情報セキュリティ対策」って
知っていますか？



IPA

独立行政法人 情報処理推進機構
セキュリティセンター

<http://www.ipa.go.jp/security/>

初めての情報セキュリティ対策

リテラシーという言葉があります。リテラシーとは元々「言語により読み書きできる能力」をさす言葉でしたが、最近では、自分が身につけた知識や技術を使って、事象を理解・整理し活用する能力のことをさすようです。

情報化社会においては、コンピュータの利用技術を持つか否かによって個人の可能性が大きく左右することから、情報リテラシーやコンピューターリテラシーなどが重要であるといわれています。

情報セキュリティ対策は、まさにこういったリテラシーをもって実施されるものと言われる所以(ゆえん)です。

しかしながら、リテラシーといった言葉を使う以前に、セキュリティに対する意識がなければ、情報セキュリティ対策は実施できません。



一昔前までは、自分のコンピュータを守ることがセキュリティ対策であると言われていました。コンピュータウイルス対策、脆弱性の解消、情報の暗号化、情報のバックアップ、企業内ネットワークで言えば、**(これは皆さんは覚える必要はありませんが)**ファイアウォールやIDS(侵入検知システム)/IPS(侵入防止システム)の設置、プロキシサーバにおけるネットワーク監視・制御等々、いわゆる物理的な対策が主(メイン)でした。

ところが、個人情報保護法と呼ばれる法律が2005年4月に施行されて以来、個人情報の漏えい問題が大きく取り沙汰されるようになりました。

そして、この個人情報の概念から、企業においては企業情報や機密情報といった情報も、企業として守るべきものであることが重要となってきました。これもセキュリティ対策であるとし、情報セキュリティ対策やマネジメントといった言葉が前面に出てきたわけです。

さらに、企業で取り扱う情報を守るためには、それらの情報を管理するためのコンピュータやネットワークの物理的なセキュリティ対策も当然必要ですが、それだけではなく、「人のセキュリティ対策」も重要になってきています。

ここで言う「人のセキュリティ対策」とは、いわゆるセキュリティ対策ルールや体制を決め、それを守ることです。



では、人のセキュリティ対策について、身近な問題を取り上げて説明することにしてしまおう。

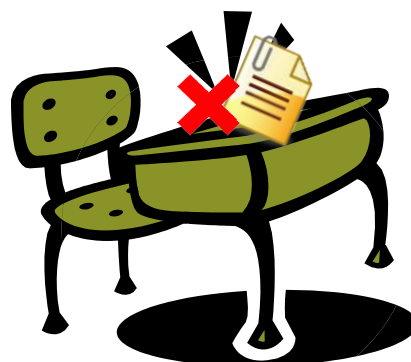
対策1: 企業にとって重要な情報って…

企業にとってその情報が企業外に漏れる(漏えいする)と、**企業の事業運営上で重大な問題を引き起こす可能性のある情報**を、重要な(あるいは守るべき)情報と呼びます。例えば、お客様から預かっているお客様の個人情報、企業で働く従業員の個人情報、企業運営のための企業情報およびノウハウなどの機密(秘密)情報等がそういった情報と言えます。

何が重要な情報か理解し、守ることが情報セキュリティ対策の第一歩と言えます。

対策2: 事務所の中の自分の(事務)机の上は…

机の上に放置した情報は、誰かに持ち去られる危険にさらされています。関係者以外が見たり触れたりできないよう、重要情報は**放置せず**、管理および保護する必要があります。



事務所の中に、関係者以外の方が出入りする場合があります。その際、机の上に重要な資料などがそのまま置かれていたり、内容を盗み見されたり、持ち去られたりすることがあります。そのためにも、机の上はいつも整理しておき、重要な情報が放置された状態にならないように注意する必要があります。さらに、机の上に資料を山積みにしておくと、重要な資料がどこにあるのか分からなくなる場合もあるようです。情報の整理および管理は重要なセキュリティ対策といえます。

対策3: 知らない人が事務所に入ってきたら…

関係者以外の社内への立ち入りを制限していないと、情報を盗み取られる危険性があります。特にサーバや書庫・金庫などの近くには無許可の人が近づいたり、操作できたりしないようにしましょう。

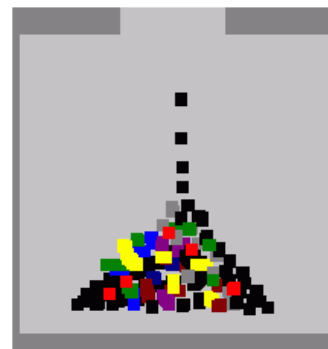
対策2とセットの対策となります。



対策 4: 重要な情報が記載された資料や、それらが格納された電子媒体が不要になった際の処分方法は…

重要な資料などを廃棄する場合は、シュレッダーで裁断するなどのように、**重要情報が読めなくなるような処分**が必要です。同じように、重要情報の入ったパソコンや記憶媒体を廃棄する場合は、消去ソフトを利用したり、業者に消去を依頼したりするなどして、電子データが読めなくなるような処分が必要です。

重要な情報が記載された資料や、それらが格納された電子媒体を廃棄する場合に、単にゴミ箱に捨てたり、廃品回収に出してしまうのは情報漏えい事故の典型的な事例となります。重要な情報が読めないようにする対策は必須の情報セキュリティ対策です。



こんな事例があります。

事例: 一般家庭ゴミ?

会社で終わらない仕事を自宅に持ち帰り、そのときに使用した重要な情報が記載されていた書類を、不要になったので一般家庭ゴミの回収に出した。その資料が地方自治体の住民情報だったので、回収業者はビックリして自治体に報告し、大騒ぎになった。情報漏えいはしなかったけれど…



この事件(事故)を起こした職員のいる企業は、その地方自治体から訴えられ、しばらくの間、仕事ももらえなくなりました。信用回復には長い時間と多大なコスト(セキュリティ対策費用や信用失墜による利益損失など)が掛かったようです。

対策 5: 重要な情報は企業の外に持ち出して良いの…

重要な情報を会社の外へ持ち出す場合は、上司に確認を仰ぎ、さらに持ち出し記録を残す必要があります。自分勝手な情報の持ち出しは、会社に対する犯罪行為となる場合もあるようです。

持ち出した情報は、思わぬ盗難にあったり、うっかり紛失したりすることがあります。情報が格納された携帯電話やパソコンの



起動やデータファイルにパスワードを設定するなどの対策を事前に行っておけば、盗難・紛失時に情報を簡単に見られないようにすることもできます。

情報の社外への持ち出しにおいては、「**そもそもこの情報は持ち出して良いのか**」を確認する必要があります。それが会社にとって重要な情報で、業務上しかたなく持ち出す必要がある場合は、上司の許可が必要でしょうし、紛失・盗難があった際に、流出した情報を特定するためにも、持ち出し記録は残す必要があります。重要な情報のこれらのような管理は、情報セキュリティ対策の基本です。

さらに、情報の持ち出し方法について考えると、パソコンだけでなくスマートフォンや携帯電話、CD や DVD、各種の電子メモリが考えられますが、これらの記憶媒体には、紛失・盗難に備えたしっかりとした物理的なセキュリティ対策が必要です。

例えば、



物理的な話がでてきたので、そちらに話を移します。物理的対策も、ルールとして運用され、それを守ることが人のセキュリティ対策となります。

対策 6: パソコンは…

重要な情報を扱うパソコンでは、トラブルが発生すると業務が出来なくなるだけでなく、場合によっては情報漏えいが発生することもあります。コンピュータウイルスに感染したり、外部からの不正アクセスあるいは単なる故障によっても業務が停滞したりします。そのため、常日頃のメンテナンスやセキュリティ対策が重要となります。

- ② 脆弱性の解消
- ② コンピュータウイルス対策
- ② 業務に関係のないアプリケーションはインストールしない(使わない)
- ② 私物パソコンは業務では使わない
- ② 業務情報のバックアップ

(1) 脆弱性の解消

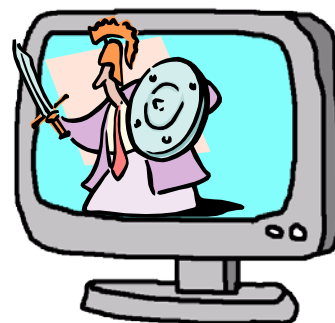
- ・ Microsoft 社 Windows の場合
Microsoft(Windows) Update の実施(毎月定例)
- ・ Apple 社の Mac の場合
定期的なセキュリティ更新の適用
- ・ パソコン上で利用するアプリケーション
常に最新のバージョンあるいはセキュリティ更新を適用する



セキュリティホールと呼ばれる安全上の欠陥(脆弱性)を放置していると、それを悪用したウイルスに感染してしまう危険性があります。お使いの OS やソフトウェアには、修正プログラムを適用するもしくは最新版を利用するようにしましょう。

(2) コンピュータウイルス対策

- セキュリティ(ウイルス)対策ソフトを利用する
- ウイルス定義ファイル(パターンファイル)は常に最新にする(自動更新)
- セキュリティ機能は安易に止めない
- ウイルスを発見したら駆除して報告

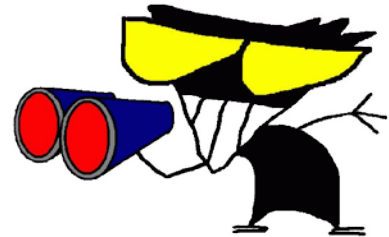




参考までに: 最近のコンピュータウイルスの紹介

スパイウェア

スパイウェアは、利用者の意図に関わらず勝手にパソコンに入り込み(感染)、パソコン内の情報や利用者の操作を記録し、必要に応じて外部に送信する行為を行うウイルスです。利用者の操作を記録するものとしてはキーロガーと呼ばれる利用者のキーボードでの操作を記録するツールが有名です。また、インターネット参照の履歴なども利用者の操作を記録したものとして奪取される場合があります。



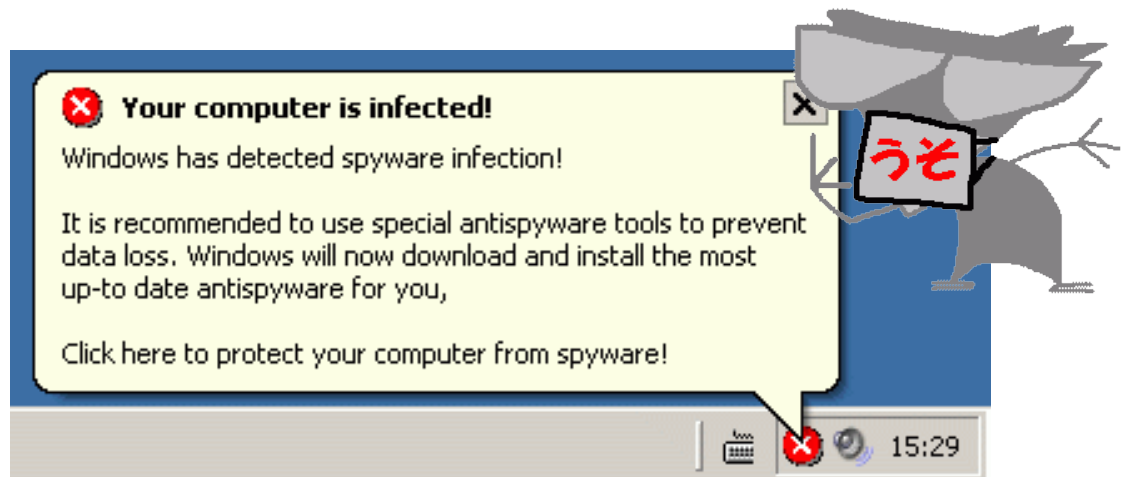
もともとは、インターネットを通じたマーケティングのための情報表示(商業表示)・収集(利用者の嗜好分析)活動、いわゆるアドウェアから発生したものと考えられ、その活動が過激になったものがスパイウェアであるともいわれています。

暴露ウイルス

ファイル交換ソフトを介した情報流出を行うウイルス(Antinny ウイルス等)や、利用者のパソコンを勝手にインターネットに向け公開された Web サイトにしてパソコンの内容をインターネットに晒してしまうウイルス(山田ウイルス等)を、情報を暴露するものとして暴露ウイルスと呼ぶ場合があります。これらも、前述のスパイウェアの一種といえます。

スケアウェア

スケアウェアは、読んで字のごとく脅迫するウイルスです。『あなたのパソコンはウイルスに感染しています』と偽の情報を表示し(自作自演のウイルス騒ぎ)、偽ウイルス対策ソフトの購入を促す詐欺を行うものなどがあります。



ランサムウェア

ランサムは身代金のことで、ランサムウェアはパソコンに格納された特定のファイルやフォルダを勝手に暗号化などし、『戻すためのパスワードを知りたければ金を出せ』などと脅迫するものです。たいていの場合は、お金を払っても人質は解放されないようです。リアルな世界の犯罪と同じようなことが、インターネットを介したネットワーク上のバーチャルな世界でも発生しているわけです。



ボット

ボットとは、パソコンに感染し、そのパソコンをネットワーク(インターネット)を通じて外部から操ることを目的として作成されたプログラムです。感染すると、外部からの指示を待ち(指令サーバとの通信を一定間隔で実施する)、与えられた指示に従って内蔵された処理を実行します。この動作が、ロボットに似ているところから、ボットと呼ばれています。最近流行のスマートフォンに感染するボットウイルスも確認されているので注意が必要です。

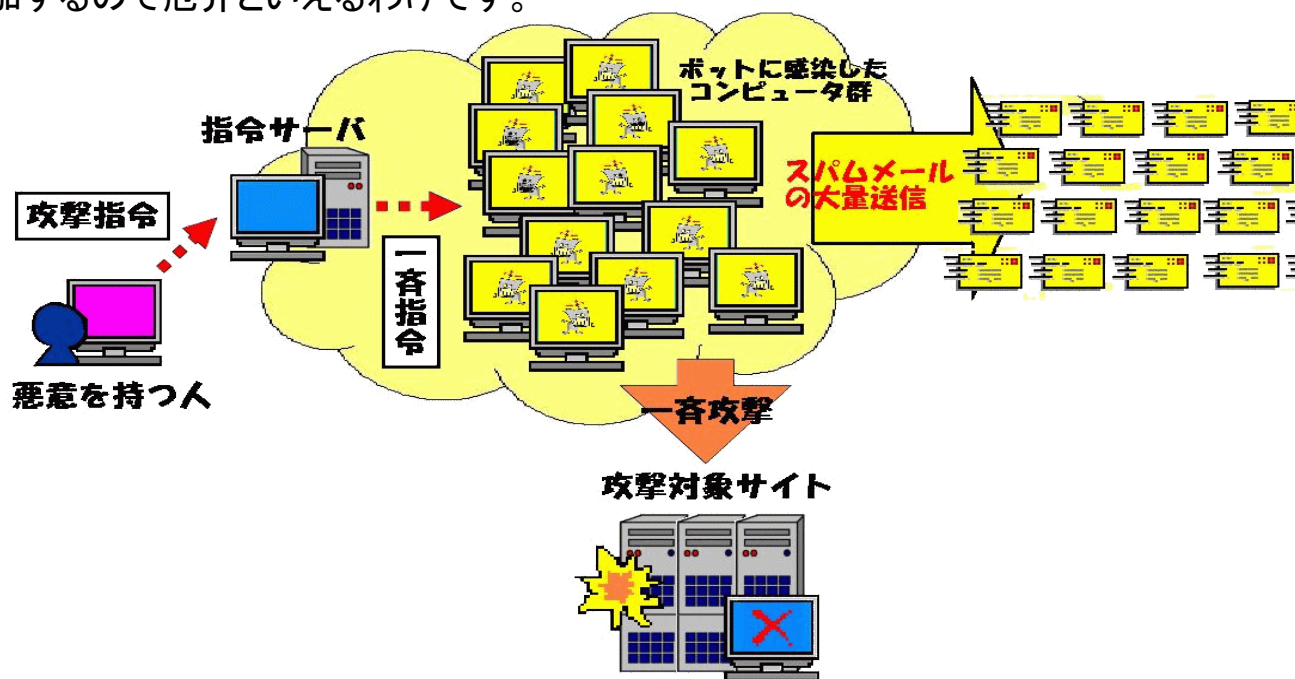


内蔵された処理の例

- ・ スпамメール送信活動(多量のスパムメールを送信する)
- ・ DoS 攻撃などの攻撃活動(特定のサイトへのサービス妨害攻撃を行う)
- ・ ネットワーク感染活動(コンピュータの脆弱性を狙った不正アクセスによる感染活動)

- ・ ネットワークスキャン活動（感染対象や脆弱性を持つコンピュータの情報を集める）
- ・ 自分自身のバージョンアップや指令サーバの変更
- ・ スパイ活動（感染したコンピュータ内の情報を外部へ送信）

ボットが厄介な点は、ボットに感染したパソコンが多数集まるとそれらが指令サーバを介してネットワーク(ボットネットワーク)を構成することです。これらのボットネットワークは数百から数十万台のパソコンで構成される場合もあり、それらから一斉にスパムメールが発信されたり、特定の攻撃先を一斉に DoS 攻撃したりする場合があります。ボットネットワークが大きければ大きいほど攻撃などの効力が増加するので厄介といえるわけです。



ボットネットワークを悪用された場合の脅威

トロイの木馬

ギリシャ神話である「トロイの木馬」の話はご存知でしょうか？相手(利用者)を騙し信用させ贈り物と称して木馬を場内へ入れさせる。木馬の中には城を内部から攻撃する兵隊を忍ばせておく話です。トロイの木馬型ウイルスは、この話と同じように、パソコン内に潜伏させ、必要に応じていろいろな悪さを行うウイルスです。一般的にはスパイウェアやスケアウェア、ランサムウェアといった区分けとは違った分類ですが、以下に示すような悪さを行うものです。

- バックドアの設置
インターネット(ネットワーク)を介して外部からパソコンを操作させるための裏口(バックドア)を作成する。このバックドアを通じて、パソコンの外部から侵入し、いろいろな操作を行うことができるようになる。非常に危険な状態といえます。

- 不正なプログラムのダウンロード
パソコンの利用者が意識することなく、不正なプログラム等をインターネットからダウンロードし実行します。
- 利用者パソコンの情報収集
いわゆるスパイウェアの行為を行います。
- 攻撃の踏み台(攻撃の中継等)
ボットと同じように攻撃(攻撃の中継)行為を行います。

ワーム

ワームとは、一般的な狭義のウイルスのような他のプログラムやファイルに感染(寄生)するタイプではなく、パソコンにインストールされ実行される自己完結型のプログラムで、自分自身の複製を作成(コピー)することで感染(自己増殖)活動を行います。昔ながらの狭義のウイルスと区別するために付けられた名前(種類)ですが、単独でパソコン内で破壊活動や感染(自己増殖)活動などの悪さをするためにうごめく様から、ミミズやウジのようなのでワームと呼ばれています。

実はこのタイプのウイルスが最も簡単に作成できるため、種類や亜種が多く出現しています。前述のスパイウェアやスケアウェア、さらにはランサムウェアやボットもこのタイプのウイルスといえます。昔ながらのウイルスは減っているということになります。

プログラミングができる人であれば誰でも作成できるものですが、普通はパソコン利用者により起動してもらう必要があるので、利用者にとって有用なプログラムを装って実行させたり、パソコンの脆弱性を利用して実行させたりするものがほとんどです。

(3) 業務に関係のないアプリケーションはインストールしない(使わない)

ファイル交換ソフトに代表される利用すると情報漏えいする可能性のあるアプリケーションは企業内のパソコンでは使用してはいけません。自宅からゲームソフトを持ち込むのも、業務に関係ないのでNG。

この問題の大きな理由は、それらのアプリケーションが脆弱性を持っていたり、提供元から何らのサポートも受けられなかったり等、保証がないためです。さらに、それらのアプリケーションがウイルス等の不正プログラムを誘引する可能性があるためです。そもそも、仕事で使う道具で遊ぶのは、どうでしょう…

ファイル交換ソフトからの情報漏えい

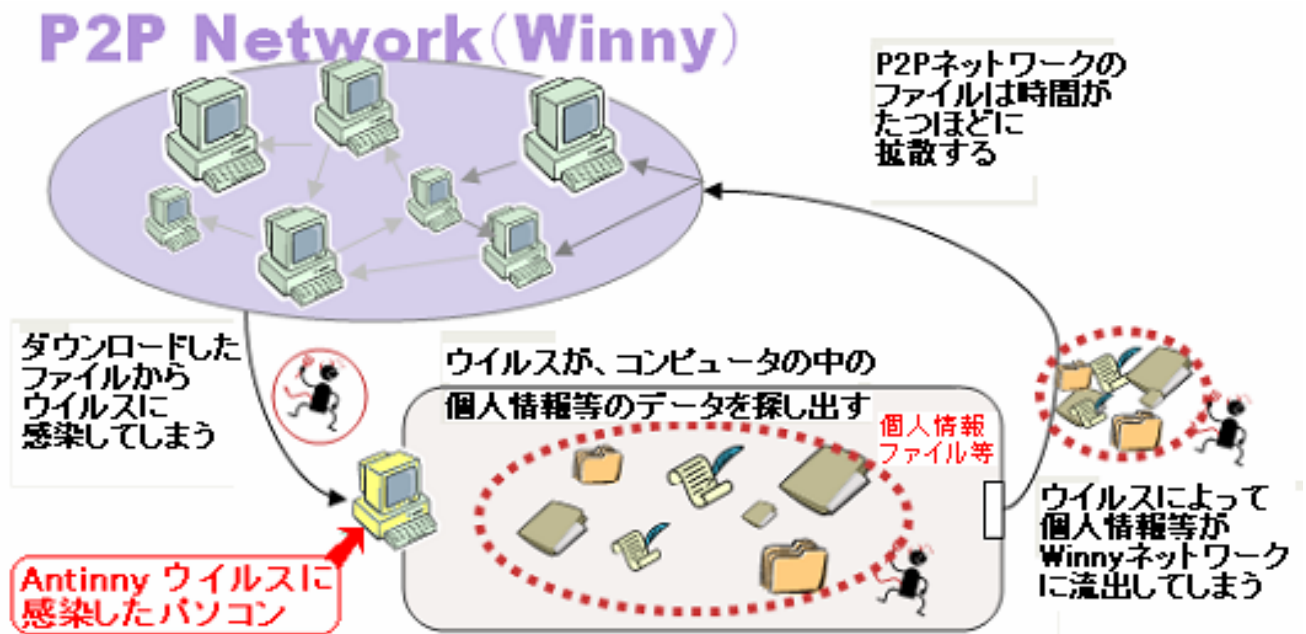


図 ファイル交換ソフトから情報流出する仕組み

実際にあったお粗末な事例

- 仕事中にアダルトサイトを訪問
- ワンクリック詐欺に引っ掛かり・・・
- 請求書がパソコンの画面から消えない!!
- これもウイルスの仕業・・・
- 恥ずかしくて、仕事ができませんか?
- 上司にバレないように、パソコンが壊れたと報告した!?
- この人の業務停止?



(4) 私物パソコンは業務では使わない

「業務に関係のないアプリケーションは使わない」と同じ理由で、私物パソコンは業務で使わないことが望ましいです。どうしても必要な場合は、上司の許可をとってから、十分なセキュリティ対策を施してから利用することになります。しかしながら、私物パソコンは企業として十分に管理できないので、原則として業務には使わないことを推奨します。

(5) 業務情報のバックアップ

故障や誤操作などにより、パソコンの中に保存したデータが、消えてしまうことがあります。定期的にバックアップを取得しておけば、このような不測の事態に備えることができます。

対策 7: パスワード…

パスワードは重要です。対策 5 でもパスワードの話はしましたが、パソコンやスマートフォン、携帯電話を利用する際のログインパスワードや暗証番号だけでなく、インターネットを利用していると多くのパスワードが必要になってきます。

みなさんもパスワードの重要性は理解されていると思いますが、インターネットなどでは、安易なパスワードやパスワードの使いまわしなど、パスワードの運用・管理上危険な取り扱いを多く見受けられます。

インターネットサービスを利用するためのパスワードが推察され、悪用されるといった事例が確認されています。この原因のひとつとして、名前や誕生日のように簡単なパスワードを設定していたケースがあります。パスワードを推察されると、本人に成りすまして不正利用されてしまうこととなります。大文字・小文字・数字・記号を組み合わせた複雑なパスワードを設定するとともに、定期的にパスワードを変更することで、被害を防ぐことができます。

特に業務で使うのであれば、しっかりとした管理のもと、次に示すようなパスワードのおきてを守ってください。

パスワードの掟(おきて)

- 他人に推測されやすいパスワード(ニックネームや誕生日等)は使わない
 - ☑ 大文字・小文字・数字・記号の組み合わせ
 - ☑ 長いパスワード(推奨は8桁以上)
 - ☑ 推測しづらく自分が忘れないパスワード等
- 他人の目に触れるような場所に、パスワードを残さない



- 定期的に変更する

パスワードを忘れそうなら、紙に書いて金庫にしまうなどのように、必要なときに取り出せるセキュアな管理ができれば OK です。パスワードを忘れたために、業務に支障をきたす場合もあるようですから…

対策 8: 電子メール…

業務における電子メールの利用は、やり取りする内容自体が重要な情報なので、宛先を間違えるなどの誤送信は、絶対にあってはなりません。

誤送信を防ぐためには、例えば以下のような対策が必要です。

- 送信前に宛先と内容の再確認
- 重要な情報はメール本文ではなく暗号化された添付ファイルに…
- 同時に多くの宛先に送信(同報メール)する場合は、To や CC でいいのか BCC にすべきなのか良く考えること

同報メールの送信方法を間違えて、個人情報としてのメールアドレスを漏えいさせたといった事故が多発しています。これは、ほとんどの場合、CC と BCC の使い方を間違えたことに起因しているようです。

対策 9: 守秘義務って何…

対策1で企業にとって重要な情報は何か示しましたが、こういった情報は従業員であれば、対外的に秘密としなければなりません。それが守秘義務です。一般的には、採用の際に守秘義務があることを知らせるなどのように、企業は従業員に秘密を守らせています。

ところで、こんな事故(事件)がありました。

事例:

東京のある著名なホテルで、ホテル内の飲食店のアルバイト店員が、有名スポーツ選手と女性タレントがプライベートで来店していたことを Twitter に投稿した。以前からこのアルバイト店員はこういった暴露情報をつぶやいていたようだが、この内容をみた Twitter 利用者の中で、著名人の情報を暴露したことに対する批判が相次ぎ、いわゆる“お祭り”騒ぎとなり、アルバイト店員の個人情報まで他のネット掲示板上で特定されるなどした。

ホテル側では、社員・アルバイトの区別なく、顧客情報の守秘義務に関する研修を実施したり、守秘義務の誓約書にも署名させたりしている。

まとめ

企業に入って業務を遂行するにあたっては、インターネットを利用するケースが増えてきます。最近では普段の生活でもインターネットを利用することは多いと思いますが、企業としての重要な情報を扱っていることを常に意識していないと、どんなところから情報漏えいなどの事故を起こすか分かりません。

安全にインターネットを利用していくにあたり、自分だけで判断するのが難しい状況も発生しています。金銭目的のサイバー犯罪者が増加しており、例えば、フィッシング詐欺や情報搾取を目的としたコンピュータウイルスなどがあります。また、特定の組織や企業を狙った標的型攻撃もあります。

自らの怠慢や過失によって、重大な事故を起こさないように、普段からセキュリティ意識を持つこと、それから企業が決めたセキュリティルールを守ることが重要です。

「自分の身は自分で守る」だけでなく、「会社の身は私が守る」ぐらいの気構えを持ってこれからの社会人としての活動をしていただきたいと思います。



参考情報

<知る>

- [これだけはやろう！セキュリティ対策](http://www.ipa.go.jp/security/personal/base/)
- [ウイルス感染を防ぐためのポイント](http://www.ipa.go.jp/security/personal/know/virus.html)
- [情報漏えいを防ぐためのポイント](http://www.ipa.go.jp/security/personal/know/leakage.html)
- [侵入を防ぐためのポイント](http://www.ipa.go.jp/security/personal/know/invasion.html)

<守る>

- [ウイルス対策](http://www.ipa.go.jp/security/personal/protect/antivirus.html)
- [ファイル交換ソフトによる情報漏えい対策](http://www.ipa.go.jp/security/personal/protect/leakage.html)
- [パソコンユーザのためのスパイウェア対策 5 箇条](http://www.ipa.go.jp/security/antivirus/spyware5kajyou.html)
- [フィッシング \(Phishing\)対策](http://www.ipa.go.jp/security/personal/protect/phishing.html)
- [メールに関わるトラブルについて](http://www.ipa.go.jp/security/ciadr/mailtrbl.html)
- [身に覚えのない請求などの防止](http://www.ipa.go.jp/security/personal/protect/oneclick.html)

<学習ツール>

- [5分でできる！情報セキュリティポイント学習
～事例で学ぶ中小企業のためのセキュリティ対策～](http://www.ipa.go.jp/security/vuln/5mins_point/)

IPA 対策のしおり シリーズ

<http://www.ipa.go.jp/security/antivirus/shiori.html>

- IPA 対策のしおり シリーズ(1) ウイルス対策のしおり
- IPA 対策のしおり シリーズ(2) スパイウェア対策のしおり
- IPA 対策のしおり シリーズ(3) ボット対策のしおり
- IPA 対策のしおり シリーズ(4) 不正アクセス対策のしおり
- IPA 対策のしおり シリーズ(5) 情報漏えい対策のしおり
- IPA 対策のしおり シリーズ(6) インターネット利用時の危険対策のしおり
- IPA 対策のしおり シリーズ(7) 電子メール利用時の危険対策のしおり
- IPA 対策のしおり シリーズ(8) スマートフォンのセキュリティ対策のしおり
- IPA 対策のしおり シリーズ(9) 初めての情報セキュリティ対策のしおり
- IPA 対策のしおり シリーズ(10) 標的型攻撃メール対策のしおり



IPA

独立行政法人 情報処理推進機構
セキュリティセンター

〒113-6591 東京都文京区本駒込2丁目28番8号
(文京グリーンコートセンターオフィス16階)

URL <http://www.ipa.go.jp/security/>

【情報セキュリティ安心相談窓口】

URL <http://www.ipa.go.jp/security/anshin/>

E-mail anshin@ipa.go.jp