新入社員等研修向け情報セキュリティマニュアル

有限責任中間法人 JPCERT コーディネーションセンター

2009 年 4 月 24 日

目次

はじめに

新年度を迎え、社会人研修や業務セミナーなどが活発になる時期ですが、電子メールやPC の利用に関するマナーやセキュリティ対策は、もはや新人研修には欠かせない項目となっています。この文書は、企業や組織の教育担当者や情報セキュリティ担当者に向けて、新入社員等に対して情報セキュリティに関する知識を教える際のガイドライン、研修資料のベースとなるような情報やトピックをまとめたものです。セキュリティ対策やインシデント対応に関する社内ルールの教育、研修等においてご参照いただければ幸いです。

なお、教育担当者や情報セキュリティ担当者向けのメッセージを**ゴシック体**で、新入社員向けのコンテンツとして参照いただきたい部分を明朝体で記載しています。

1　企業等における PC 端末利用者のための基本的な情報セキュリティ対策

個人情報の漏洩をはじめ、情報セキュリティ上の問題に関する報道が後を絶たない昨今、各企業においては、それぞれ情報セキュリティに関する社内ルールを定めたり、情報セキュリティの担当者を置いたりして対策を進めていらっしゃると思います。しかしながら、せっかくルールを周知しても、意義や目的の分からないルールは、忘れられたり、無視されたりすることが少なくありません。社内の情報セキュリティに関するルール等の徹底を図るためにも、どんな PC の使い方がセキュリティ上の問題事象を発生させるのか、またそのような情報セキュリティ上の問題が会社にどのような被害をもたらすか、そのような被害を発生させないためにはどう対処すれば良いのかといったことを新入社員の段階から周知しておくことは企業や組織にとってとても重要なことであるといえます。電話の応対やビジネスマナーを身につけることと同様に、セキュリティに関する正しい知識や対応方法を新入社員のうちから身につけてもらうようにしましょう。

1.1 発生し得る問題事象

セキュリティ上問題のある PC の利用や注意を欠いた PC の操作は、情報セキュリティ上の脅威になり得る事象（以下「インシデント」といいます。）を引き起こす可能性があります。

1.1.1　インシデントの例

○ 怪しい電子メールに添付されたファイルを開いてしまうことによる、ウイルス感染
○ ウェブサイト上の情報の安易なダウンロードによるウイルス感染
○ 修正しないまま放置したソフトウェアの脆弱性を第三者に攻撃されることによる、ウイルス感染、不正侵入
○ 安易な ID やパスワードを設定したり、不用意に公開してしまったりすることによる、第三者による不正侵入

1.1.2　インシデントの被害の例

ウイルス感染や不正侵入等のインシデントが発生した場合、以下のような被害が想定されます。

○ PC やネットワーク上のシステム内のデータが窃取されて悪用されたり（個人情報や企業秘密の漏洩）、破壊されたりする（業務の継続に支障）

○　コンピュータウイルスやスパイウェアなどの利用者の意図に反する動作を行わせる不正なプログラム（以下「マルウェア」といいます。）を勝手にインストールされ、将来にわたってデータを窃取され続けたり、または、他の PC に対する攻撃のための道具として利用されたりする
○　他の社員の PC やシステムにウイルス感染が拡大することにより、業務の継続が困難になる可能性がある

これらの情報漏洩などの問題が起きてしまった場合、その会社は、業務継続上の支障や復旧のためのコスト等の直接的な被害のみならず、取引先に対する信用の失墜やイメージダウンなど社会的評価の低下も招きます。あるいは、漏洩した情報が個人情報や取引先から提供を受けている秘密情報等であった場合には損害賠償責任などの甚大なダメージを受けてしまう可能性があります。例えば、企業がウイルス感染の被害を受けた場合、その損害額は中小企業で 1 社あたり平均 430 万円、大企業では 1 億 3000 万円にも上るという試算（※1）があります。

このような問題が不幸にして発生してしまった場合には、被害を最小化するために、社員が各社のルールに従って迅速かつ適切な対応を行う必要がありますが、対応ルールの周知が行われていない新入社員が初期の判断を誤ることで、関係部署への報告や組織的な対応が遅れてしまい、被害が拡大することも懸念されるところです。

※1：IPA - 2005 年 企業における情報セキュリティ事象被害額調査 -
http://www.ipa.go.jp/security/fy17/reports/virus-survey/documents/2005_model.pdf

1.2 インシデントの原因及び発生を抑止するための対策

上記のようなインシデントやそれによる被害が発生しないよう、事前に、新入社員に対して、インシデントの原因と発生を抑止するための対策に関する基本的な情報を周知しておくことが重要です。

1.2.1　全般的な原因と対策

➢　PC にインストールされているソフトウェアに関し、最新版へのアップデートを怠る――不正侵入・システム障害

PC にインストールされている OS・ソフトウェアについては、最新の修正プログラムを適用するなどして、セキュリティ上の弱点（以下「脆弱性」といいます。）が含まれるソフトウェアを使用しないようにしましょう。普段あまり使用しないソフトウェ

アについては、修正プログラムの適用の必要性を看過してしまいがちですから、適切なソフトウェア管理のために不要なソフトウェアを PC になるべくインストールしないようにするという配慮も大切です。

修正プログラムの適用は、業務を中断して行わなければならない場合もあるので、面倒と思われがちですが、脆弱性に関する情報が公開されると、その直後からその脆弱性を狙った攻撃が増えることが多いので、製品開発ベンダから修正プログラムが提供されたときは、なるべく早く適用するようこころがけましょう。

また、製品開発ベンダから修正プログラムが提供される以前から、対象となる脆弱性を狙う攻撃（以下「ゼロデイ攻撃」といいます。）が行われている場合もありますので、「すでに攻撃コードが出回っている」との情報が併せて公開されている場合には、修正プログラムの迅速な適用だけでなく、ウイルス対策ソフトを使用してスキャンを行う等、自らの PC が既に攻撃を受けていないか（その脆弱性を狙うウイルスに感染していないか）を確認するとよいでしょう。

なお、このようなソフトウェアの脆弱性や修正プログラムの適用が必要であること等の情報を各社員が個別に収集しなければならないとなると、重複した作業を大勢の社員に強いることになってしまうので、各組織における情報セキュリティ担当者やインシデントへの緊急対応を行う組織（CSIRT: Computer Security Incident Response Team）が関連する情報を収集し、自社の情報システムにとって対応が必要な情報か否かを判断した上で、所要の対応方法を社内に指示、周知するという対応がとられる場合が多いところです。上記のとおり、このような担当部署からの連絡には迅速に対応することが必要です。

また、これらの担当部署に無断で新たなソフトウェアのインストールを行うと、そのソフトウェアが管理対象からはずれているために（担当部署がそのソフトウェアに関する脆弱性情報を入手しても、社内で使用されているという事実を知らないために、社内での展開が不要であると判断してしまう可能性があります。）、修正プログラムの適用等の指示、周知が行われず、結果的に脆弱性のあるソフトウェアを使用し続けてしまい、ウイルスに感染してしまうという事態が生じる可能性があります。ソフトウェアの無断インストールの危険性については、後述の「ソフトウェアの無断インストール」の部分も参照してください。

- ウイルス対策ソフトを導入しただけ――ウイルス感染

ウイルス対策ソフトは、インストールしただけでは十分ではありません。ウイルス感染予防のためには、ウイルスパターンファイルを常に最新の状態に保つことが必要

です。また、ウイルスパターンファイルを最新の状態に保っていても、ゼロデイ攻撃によりウイルス対策ソフトによる検知をすり抜けて PC 内にウイルスが入り込んでいる場合もあり得ますから、ウイルス対策ソフトのスキャン（検索）機能を利用して、PC 内にウイルスが存在しないか定期的にスキャン（検索）するようにしましょう。

- 安易なパスワード――不正侵入・情報漏洩

  PC の起動やファイルへのアクセスを制限するためにパスワードの設定が求められる場合がありますが、このような場合には、他人に推測されにくいパスワードを設定しましょう。安易なパスワードは、盗まれなくても、総あたり攻撃（ブルートフォース攻撃：機械的な処理により可能な組み合わせすべてを試す攻撃方法）で破られてしまう可能性があります。総あたり攻撃を回避するためにパスワードを定期的に変更する運用が効果的であるとする見解もありますが、定期的にパスワードを変更するとなると、ついつい覚えやすい簡単なパスワードを設定するようになりがちです。そのようなことになると本末転倒といわざるをえませんので、注意が必要です。実際にどのようなパスワードを設定したら良いかについては、後述の「3.特に新入社員が起こしやすい問題への対応」の「安全なパスワードの作り方を知ろう」を参照してください。

- ソフトウェアの無断インストール――ウイルス感染・システム障害

  私用の PC の感覚で、便利そうだからという理由でシステム管理者や情報セキュリティ担当者等に断ることなく勝手にソフトウェアをインストールすることには危険が伴います。無料のセキュリティ対策ソフトを装ったマルウェアが増えているという報告もあります。また、悪意のないソフトウェアでも粗悪なものはシステムやネットワークに悪い影響を与えたり、セキュリティポリシーに反する処理をしたりするものもあります。

  さらに、脆弱性対策としてのソフトウェアの管理の観点からしても、社内で利用しているソフトウェアの脆弱性対応を行っている担当部署に無断で新たなソフトウェアのインストールを行うと、当該ソフトウェアに関する修正プログラムの適用等の指示、周知が行われず、結果的に脆弱性のあるソフトウェアを使用し続けてしまい、ウイルスに感染してしまうという事態が生じる可能性があります。

  ソフトウェアを無断でインストールしないこと等のルールが社内で定められている場合には、そのルールを順守しなければなりません。そのようなルールがない場合であっても、ソフトウェアを独自にインストールして利用する場合には、そのソフトウェアの脆弱性に関する情報は自ら注意を払って収集し、自ら適時に修正プログラムを適用する等の覚悟と責任をもって利用することが必要です。

  ソフトウェアは、最初にインストールした状態でずっと使い続けられるものではなく、脆弱性への対応のためのバージョンアップや修正プログラムの適用等のメンテナ

ンスを継続しながら使うものであることを、認識しましょう。便利そうだからという理由での安易なソフトウェアの利用によってリスクに曝されるのは、会社の情報資産であることを肝に銘じる必要があります。

- 離席時等に PC にロックをかけない――不正操作・情報漏洩

  見積書や請求書などを不用意に机の上に広げたまま放置しないのと同様に、PC の画面もそのままにして席をはずしたりしてはいけません。PC の前を離れる時には必ずログオフする、もしくはパスワード入力画面で PC をロックする習慣をつけるようにしましょう。Windows を使っている場合、Windows キー＋L で「コンピュータのロック」が簡単に行えます。

- USB メモリなどの外部記憶メディアの不用意な利用――情報漏洩、ウイルス感染

  自宅での作業や取引先とのデータ受け渡しなどのために、USB メモリなどにデータを保存して社外に持ちだすと、紛失や盗難により情報漏洩の可能性があります。組織で決められたデータの持ち出しやデータ消去のポリシーを理解し、不用意な外部記憶メディアの利用は控えるようにしましょう。

  また、最近では USB メモリを介したウイルス感染が拡大しています。管理の不明な USB メモリを会社の PC に接続したり、また逆に管理の不明な PC に、自分の USB メモリを接続したりしないようにしましょう。

1.2.2 ウェブサイトに関連する原因と対策

- ウェブブラウザの設定が安全ではない――ウイルス感染

  ウェブサイトの中には、知らないうちにマルウェアをダウンロードさせたり、そのような危険なサイトに誘導したりするものもありますので、ウェブブラウザのセキュリティ設定機能を利用して、そのような問題の発生をできるだけ抑止する取組みが重要です。ウェブブラウザのセキュリティ設定では以下のような項目について設定することができます。社内のポリシーに従って、適切な設定を維持しましょう（※2）。

  ●JavaScript、Java や ActiveX コントロールなどを無効にする
  ●ポップアップウィンドウをブロックする
  ●画像の自動読み込みを無効にする
  ●クッキーを無効にする

※2：JPCERT/CC - 安全な Web ブラウザの使い方（Version 1）-
https://www.jpcert.or.jp/ed/2008/ed080002_1104.pdf

企業や組織の業務の種類によっては、ウェブブラウザの設定を厳しくすることが難しい場合もありますし、必要以上に厳しい設定にすると業務に支障が出る等の理由で社員が勝手に設定のレベルを変更してしまう可能性もありますので、効率とリスクとのバランスを考えたポリシーに基づく、業務上最適なセキュリティ設定を行う必要があります。業務上、無効にできないサービスや機能がある場合は、その状態に対する危険性や注意点、運用のガイドラインなどを定め、周知を図るようにしましょう。

- 危険なサイトにアクセス――情報漏洩

  スパムメールに含まれている URL などを不用意にクリックすると、マルウェアをダウンロードさせる等の怪しいウェブサイトに誘導されることがあります。また、このようなサイトで、個人情報や ID パスワードその他の会社の情報などを入力してしまうと、その情報が悪意のある者の手に渡ってしまいます。

  会社の PC からは、業務上アクセスする必要がないサイトにはアクセスしないことが前提であると考えられますが、ウェブサイト上で、情報を入力したりする際には、そのサイトが SSL（https）による暗号化等の安全措置を使っているかを確かめるようにしましょう。

  最近では、正規サイトかどうか簡単に判別できないような精巧なフィッシングサイトや、正規のサイトが改ざんされる事例も発生しています。危険なサイトの見分け方は難しくなっていますが、「3. 特に新入社員が起こしやすい問題への対応」に参考となる簡単なチェックポイントを掲載しました。

1.2.3 電子メールに関連する原因と対策

- 不用意に添付ファイルを実行――ウイルス感染

  コンピュータウイルスが仕込まれた添付ファイルを実行させようとする電子メールの受信事例は、相変わらず後を絶ちません。見知らぬ人から送付された電子メールや、知っている人からの電子メールではあるが普段とは異なるアドレスから送付されている等の不審な点がある電子メールに添付されたファイルは、不用意に開いたりせず、削除するか、情報セキュリティ担当者に相談するようにしましょう。

なお、お客様相談窓口や営業の窓口等、業務上、見知らぬ人から送付されたメールの内容を確認しなければならない部署については、社内のネットワークから切り離された専用の環境を用意して添付ファイルの内容を確認する等、組織的にリスク回避のための措置を検討する必要があります。

- HTML 形式の電子メールを注意せず表示――ウイルス感染

  マルウェアの中には、HTML 形式のメールに仕込まれているものもあり、メールを閲覧するだけでマルウェアに感染するケースもあります。また、詐欺を目的とした迷惑メールなどにおいて HTML 形式のメールを悪用するケースも増えてきています。このため、HTML 形式メールについてはテキスト形式で表示するように電子メールクライアントの設定を変更しましょう。

- メールに電子署名をしない――「なりすまし」

  電子メールでは、送信元の表示を偽ることが容易にできてしまうため、「なりすまし」などの危険がつきまといます。差出人の表示が上司や取引先等であっても、それだけでは本当に本人が送った電子メールである証明にはなりません。

  自分が送信した電子メールが、本当に自分が送付したものであることを保証するためには、電子署名の技術の利用が有効です。

  電子署名を付すことは、客先等に対して自社の情報セキュリティに対する意識の高さを示したり、第三者になりすまされて客先に電子メールが送付された場合の問題の発生を最小化したりする効果もあります。会社のポリシーとして、電子メールに電子署名を付すべき場合が定められている場合には、会社の信用の維持のためにも、そのルールに従うことが重要です。

- 重要なメールを暗号化していない――盗聴・情報漏洩

  電子メールの情報は、基本的にテキスト形式でやりとりされているので、送受信の途中で第三者が不正な手段によってメールの内容を盗み見する可能性があります。重要な情報をメールでやりとりする場合には、必要に応じて暗号化して送信する必要があります。どのような内容の電子メールであれば暗号化が必要となるか、そもそも電子メールでそのような情報を送信してよいか等については、各会社のポリシーに従って判断することになります。

2　インシデント発生時における基本的な対応

情報セキュリティ対策をどんなに実施してもインシデントが発生する確率が 0%になることはありません。いざインシデントが発生してから、被害の拡大防止のための対応方法の調査、検討を始めるようでは、その間にも会社の情報が漏洩し続けたり、社内のシステムへのウイルス感染が拡大し続けたりしてしまって、取り返しのつかない事態を招くことになってしまいます。平時から、インシデントが発生した場合に各社員や担当部署がどのような対応を取るべきかについてのルールを定め、周知しておくことが重要です。

新入社員については、社内のシステムの平時の状況に関する知識が少ないために、インシデント等の異常な事態が発生していても、そのことにすぐには気付かないという問題もありそうですが、仮にインシデントの発生に気がついても、どう対処すればよいかを理解していないために自分で解決しようとして、必要な関係部署への連絡が遅れ、結果的に被害が拡大してしまうことが懸念されます。

ここでは、新入社員が理解しておくべき、インシデントへの一般的な対応手順をまとめました。併せて、セキュリティ担当者が取るべき一般的な対応についても整理していますが、なにより重要なことは、企業や組織のポリシーに従ったインシデントへの対応方法や報告ラインなどが組織として整備されていること、及び、それを新入社員に理解させ、実践させるための周知手段が整えられていることです。この機会に、自社のインシデント対応ポリシーおよびその周知、徹底の方法に問題がないか（組織の実態に合わないものになってしまってはいないか等）、確認されることを推奨します。

2.1 インシデントの発生に気がついた時、まずどうすればよいのか

(1) 冷静に対処する

まず、落ち着きましょう。冷静さを失ってしまったがために、インシデントの被害や影響範囲を拡大してしまうこともあります。落ち着いて、どのような「普段と違う異常なこと」が発生していて、今どのような状況なのかを把握しましょう。分かる範囲でメモを取りましょう。

(2) 手順の確認

セキュリティポリシーや作業マニュアルにより、すでに対応の手順がルール化されている場合は、その内容を確認し、従うようにしましょう。非常時に備え、セキュリティポリシーや作業マニュアルなど必要な資料は、すぐに参照できる場所に用意しておくようにしましょう。

(3) 責任者、担当者への連絡

新入社員含む一般社員がインシデントを発見した場合は、セキュリティポリシーや作業マニュアルなど事前に定められた連絡手順に従い、組織内の責任者やインシデント対応チーム（CSIRT）などの担当者に連絡し、その後の対応について指示を仰ぐようにしましょう。

新入社員などでなにが危険なのかがよく分かっていないような場合には、「分からなければ、放置するよりまず報告」を徹底させましょう。

(4) 作業記録の作成

時刻情報を含める形で自分が実施した作業や判断の内容を可能な限りすべて記録しておくようにしましょう。また、インシデント対応作業について以下の項目を記録するようにしましょう。これらの作業記録は、作業時の手順を後日評価する際の資料に用いられるだけでなく、作業中に副次的に障害が発生した場合などには、 作業手順のポリシーなどを見直すための重要な資料となります。

・インシデントの発見、発生日時
・発見者（通報者）
・インシデントの内容
・インシデントと疑った理由
・インシデントを発生直前から報告するまでの作業

2.2 セキュリティ担当者がとるべき一般的な対応

ここからは、システム管理者やインシデント対応チーム（CSIRT）など専門の担当者が行う作業になりますが、対応の全体を把握させ、なぜこのような処理が必要なのか理解させることも重要ですので、必要に応じて、対応のフローを一般社員に周知しておくことも有効であると考えられます。

(5) 事実の確認

どのようなインシデントが起こっているのか、事実関係や影響範囲などを確認するようにしましょう。場合によっては、発見者・報告者へのヒアリングも有効です。

(6) ネットワーク接続やシステムの遮断もしくは停止

被害が拡大する恐れがある場合には、ネットワークやシステムの全体もしくは一部を遮断または停止するといった対策が必要になるかもしれません。さらに、この後の調査に備えてシステムの状態を保存するようにしましょう。事業継続を考慮し、代替機を準備してインシデントが発生しているシステムと一時的に置き換える等の運用も有効です。ただし、代替機にも同様の問題が存在する場合は、同じインシデントが発生する可能性がありますので、代替機で一時的に運用する場合は監視体制を強化するなどの対策を行うようにしましょう。

(7) 要因の特定と対応方針の検討

インシデントの再発を防ぐための再発防止策について検討するために、インシデント

が発生した要因（原因）を特定するようにしましょう。また、特定した要因に対して、どのような対策が可能か検討するようにしましょう。

インシデントの原因の排除や対策の検討等のために、攻撃元その他の第三者に対して調整を行う必要がある場合には、JPCERT コーディネーションセンター（以下「JPCERT/CC」といいます。）に報告をして、攻撃元やインシデントの原因となっているサイト等に対する調整等の対応を依頼することができます。

(8) システムの復旧

システムへの侵入により管理者権限を取られた場合や何らかの改ざんやデータの破壊が行われた場合には、ウイルス対策ソフトなどが検知しないバックドアや別のプログラムを組み込まれている可能性もありますので、データのバクアップ、システムの OS を再インストールすることも検討してください。

(9) 作業結果の報告

作業終了後、記録に基づいて、インシデントの影響範囲や対応全般の作業内容、作業にかかったコスト（時間、費用など）、また（確認された範囲内での）損失、対応において発見した課題や問題点をまとめ、責任者に報告するようにしましょう。

(10) 作業の評価、ポリシー・運用体制・運用手順の見直し

作業報告に基づいて、必要に応じてポリシーを見直します。また、これまでの運用体制や運用手順、さらに今回実際に行ったインシデント対応作業に問題がなかったかどうかを確認するようにしましょう。

JPCERT/CC では、情報システムにおけるインシデントが発生した場合、その被害の拡大を最小限にするための「事後」対応として、国内外の関連組織と連携して、コンピュータセキュリティインシデントに係わる報告の受付や、攻撃元に対する調整等のインシデントへの対応の支援を行っています。また、国内外におけるインシデントの事例を収集し、国内において同様の被害が発生しないよう注意喚起等の啓発活動を行っています。JPCERT/CC が行っているインシデント対応をさらに詳しく知りたい方は以下のページを参考にしてください。

JPCERT/CC - はじめての JPCERT/CC(インシデント対応) -
https://www.jpcert.or.jp/about/brief/page1.html

なお、JPCERT/CC へのインシデント報告は、以下のページから行えます。

JPCERT/CC - インシデント報告の届出 -
https://www.jpcert.or.jp/form/

3　特に新入社員が起こしやすい問題への対策

ビジネス上の慣習と同様に、情報セキュリティ上の注意事項も、新入社員にとっては常識ではないことがあります。ここでは新人が起こしやすいと思われる問題を事例ベースで整理してみました。その問題に対する対処方法もあわせて記載していますので、「１．企業等における PC 端末利用者のための基本的な情報セキュリティ対策」と併せて、新人向けのセキュリティ研修の参考にしてください。

- P2P ファイル共有ソフトを使用しないようにしよう

  Winny や Share などのファイル共有ソフトは誤った設定で利用したり、ウイルスに感染したりすることによって、PC の中の大切なデータを流出させてしまうことがあります。

  業務用 PC はもちろん、個人所有の PC であっても会社の情報を扱う可能性が少しでもある場合には、Winny を始めとするファイル共有ソフトは絶対に入れないようにしましょう。会社の情報を扱わない場合であっても、いったんネットワーク上に流出してしまった情報を完全に消去することは不可能であり、個人の情報が流出してしまうことの被害は自分が思っているより深刻ですから、慎重に行動しましょう。

  自宅 PC については、家族で共同して利用していると、知らないうちに Winny 等がインストールされている場合があり得ます。

  企業側においても、業務データの持ち出しについては、検疫システムの導入や指定の PC にしかデータのコピーを認めないなどといったルールを定め、徹底することが重要です。

- 怪しいウェブサイトにアクセスしないようにしよう

  ウイルスなどが仕掛けられたサイト、架空請求を行うためのサイト、正規サイトを装って暗証番号など個人情報を取得するサイトなど、悪意のあるウェブページにアクセスしたがために、PC が停止する、データが窃取・破壊される、ウイルスの送信元にされてしまう、などの被害が発生することがあります。

  これらの問題への対策として、以下のような点に注意しましょう。

・迷惑メールや広告メールなど素性の知れないメールに含まれているリンクには絶対にアクセスしない
・掲示板やブログなど不特定多数の人が書き込める場所に張られているリンクにはアクセスしない
・フィッシングサイトの URL には、意図的に正規サイトのスペルミスを含ませ、正規サイトの検索結果に表示されるようにしたものがある。URL の綴りに不審点があるサイトにはアクセスしない

最近では、サーチエンジンの検索結果に、リンク先の URL や内容の一部が表示されることが多いため、これらの情報が危険のあるサイトかどうかの判断材料になることもあります。問題のあるサイトにアクセスしないよう怪しいサイトを見分ける目を持ちましょう。また、ちょっとした興味で怪しいサイトにアクセスした場合にリスクにさらされるのは、会社の情報資産であることを認識しましょう。

➢ 電子メールの宛先（To:）に多数の宛先を入れないにしよう

複数の相手に同時に電子メールを送る場合、宛先欄に多数のメールアドレスが記載されていると、直接の知り合いでない人同士に他人のメールアドレスを教えてしまうことになります。メールアドレスを個人情報として扱っている企業・組織の場合は、このような取扱いが個人情報保護ポリシー違反に該当してしまう可能性があります。また、宛先欄に多数のアドレスが記載してあるとスパムフィルタによってスパムメールと判断されることもあります。

多数の宛先に、電子メールを送る場合は、メーリングリストを作って送信するか、面倒でも一件ずつ送るようにしましょう。

➢ 業務に関する話をブログで公開しないようにしよう

業務時間内に業務と関係のないブログの書き込みを行うことは禁止されている場合が多いと思いますが、業務時間外だからといって仕事の内容や取引先についての書き込み、公開は問題ないわけではありません。ブログも検索エンジンの検索対象になっています。SNS もユーザ数が数十万、数百万という単位になれば、もはやクローズドなコミュニティとはいえないでしょう。ブログや SNS などに業務その他の企業活動に関する話が投稿されていると、その企業の情報管理のあり方が問われることになります。また、それらの情報を第三者が閲覧して、不正な目的（なりすましメールの送付等）のために利用する可能性があります。

類似の問題として、ウェブ上でのチャット、メッセンジャー、地図ツール、カレンダーツールなどの公開範囲の設定にも注意が必要です。

これらのサービスを業務上利用する場合は、企業側において、各サービスの利用方法に関するルールやマニュアルを組織的に整備することが必要でしょう。

- 電子メールの添付ファイルの取り扱いには気をつけよう

電子メールでは送信元の表示を偽ることが容易なため、たとえ送信元として表示されている人が信頼できる相手であったとしても、その電子メールが本人から送付されたものであると信用することはできないのです。このため、電子メールの添付ファイルを開く場合は、次のような手順を踏むようにしましょう。

1. ウイルス対策ソフトのパターンファイルが最新であることを確認する。
2. 添付ファイルを保存する。
3. 添付ファイルをウイルス対策ソフトで検査する。
4. ウイルスが検知された場合はメールを削除する。ウイルスが検知されなかった場合でも、件名や本文等から不審を感じた場合には送信者に確認したり、情報セキュリティ担当者に相談したりする。

- 安全なパスワードの作り方を知ろう

パスワードはあらゆるサービスの認証に使われるようになっています。サービスやシステムごとに異なるパスワードを管理するのは確かに煩雑ですが、あらゆるサービスに同じパスワードを利用していると、万が一、あるサービスを利用するためのパスワードが何らかの事情で漏洩した場合、すべてのサービスの利用が危険にさらされてしまいますから、使い分けを検討する必要があります。もっとも、多数のパスワードを管理しなければならないために、各パスワードが覚えやすい推測可能な安易なものになってしまうとパスワードを設定する意味がなくなってしまいますので、用途に応じた適切な設定を心がけましょう。

安全なパスワードのポイントを以下に示します。

・電話番号や誕生日など、個人情報を基にした文字列は使用しない
・日本語、英語に限らず、辞書に載っている単語を使用しない
・ユーザアカウントと同じ文字列を含めない
・アルファベットの大文字、小文字、数字、特殊記号を混ぜる
・パスワードの長さは 8 文字以上が望ましい
・同じパスワードを使い回さない

ここまで制限があると、どうパスワードを作成したらいいのかわからないという人も多いかと思います。以下に一例を示しますので、覚えやすく強度の高いパスワードの設定を心がけてください。

1. 8 文字以上で自分が覚えやすい文字列を考える（記号・数字が入るとよい）
2. 一部を意図的に大文字に置き換える
3. 意図的に誤植（自分で覚えやすいもの）を含める

自分が忘れさえしなければ、変換ルールは独自なものでかまいませんので、これらをうまく組み合わせて、パスワード条件を満たすフレーズを考えましょう。なお、以下のサイトで、作ったパスワードの強度を確認することができます。

Microsoft - パスワードチェッカー -
https://www.microsoft.com/japan/protect/yourself/password/checker.mspx

おわりに

この文書は、新入社員の入社が多く、情報セキュリティインシデントが発生しがちなこの時期に、企業や組織の教育担当者や情報セキュリティ担当者に向けて、組織内の PC 端末の利用に関する注意点を中心に、新入社員教育を行う場合の参考になることを期待して公開するものですが、併せて、この時期に各組織の情報セキュリティポリシーやインシデント対応ポリシーその他の情報セキュリティに関する社内ルールの点検や、社内への周知の再確認等を行っていただく契機になることを期待しています。

情報セキュリティ上の脅威は、日に日に変化するものであり、いったん定めた情報セキュリティに関するポリシーやルールがいつまでも有効であるというものではありません。また、各企業の業務実施のための IT 利用の実態も変化するでしょうから、定期的なポリシーの見直しは不可欠であるといえます。この機会に、セキュリティ対策やインシデント発生時の対応に関する社内ルールの見直し、周知の確認を行われてはいかがでしょうか。

■参考文献

・JPCERT/CC - はじめての JPCERT/CC(インシデント対応) -
https://www.jpcert.or.jp/about/brief/page1.html

・JPCERT/CC - インシデント報告の届出 -
https://www.jpcert.or.jp/form/

・JPCERT/CC - 技術メモ(コンピュータセキュリティインシデントへの対応) -
https://www.jpcert.or.jp/ed/2002/ed020002.txt

・NTT - NTT-CERT Security Tips(第 6 回インシデントへの対応) -
http://www.ntt.co.jp/journal/0604/files/jn200604068.pdf

・JPCERT/CC - 初心者のためのセキュリティ講座(インターネットでの不正行為その傾向と対策) -
https://www.jpcert.or.jp/magazine/security/im9801jc.pdf

・JPCERT/CC - 技術メモ(安全な Web ブラウザの使い方) -
https://www.jpcert.or.jp/ed/2008/ed080002_1104.pdf

・総務省 - 国民のための情報セキュリティサイト(事故・被害の事例)-
http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/jiko/jiko00.htm

・Microsoft - 強力なパスワード：その作り方と使い方 -
http://www.microsoft.com/japan/protect/yourself/password/create.mspx

・Microsoft - パスワードチェッカー -
https://www.microsoft.com/japan/protect/yourself/password/checker.mspx