東京ITスクール
TOKYO IT SCHOOL

情報セキュリティ

目次

1. はじめに

本資料では、インターネットやコンピュータを安心して使い続けられるように、大切な情報が外部に漏れたり、ウィルスに感染してデータが壊されたりしないために対策やリスクマネジメントについて紹介します。

2. 情報セキュリティ

1. 情報セキュリティとは

情報セキュリティとは情報の機密性、可用性、完全性を維持するものであり、JIS 規格(日本工業規格)に定められています。情報の機密性、完全性、可用性それぞれの定義は以下に示す通りです。

名称	意味
機密性	情報へのアクセスを認められた者だけが、その情報にアクセス出来る状態を確保すること
可用性	情報へのアクセスを認められた者だけが、必要時に中断することなく、情報及び関連資産にアクセス出来る状態を確保すること
完全性	情報が破壊、改ざんまたは消去されていない状態を確保すること

機密性が確保されていない場合、顧客情報など、保護しなければいけない情報に誰でもアクセスすることができてしまいます。可用性が確保できなければ、情報にアクセスするのに莫大な時間が要求される、またはアクセスできません。完全性が確保できない場合は、アクセスした情報が正しい保証が一切なくなってしまいます。

2. 情報の重要性

1990 年代中頃より爆発的にインターネットが普及し、情報化社会という言葉が日常的に使用されるようになりました。情報化社会とは、情報が諸資源と同等の価値を有し、それらを中心として機能する社会を意味します。ここで言う諸資源とは、市場経済を支える企業の経営資源となっているヒト、モノ、カネを指します。

企業は製品の企画や製造、販売、サービスの提供等を行い、その対価を顧客から得ることで成り立っています。売れる製品を販売するには顧客のニーズや市場の動向はおろか、コスト管理や競合他社の戦略等、様々な情報を扱う必要があります。

すなわち情報は、**企業の根幹を成す非常に重要な経営資源**であるということがお分かりいただけるでしょう。

3. 情報モラル

近年、社会のどの場面においても IT 化が急速に進められています。このような情報社会を生きるために必要な態度や考え方を情報モラルと言います。自分自身の身を守り、他人に迷惑をかけないことが大切になります。

インターネットの普及によって、誰もが手軽に様々な情報を受発信できるようになり、とても便利である一方、うその情報や犯罪、迷惑行為があるという闇の部分もあります。このようなインターネット社会の特性をよく理解して行動できるようになりましょう。

① 情報発信時の注意点

・一度ネットワーク上に発信された情報は完全に削除することはできないため、安易な情報発信はしない。

・ネット上でも実社会と同様に、ルールやマナーに注意をはらい発言等に責任を持つ。

② 情報受信時の注意点

・インターネット上には有益な情報が多数あり、中には誤った情報や、偏った情報が含まれている可能性もあるため、確かな情報かを調べる。

・Web サイトで名前やメールアドレスなどを入力する際は、利用目的を確認し、個人情報が不正に利用されないようにする。怪しいと思ったらクリックしたり個人情報を入力しない。

4. 情報セキュリティの必要性

情報セキュリティの必要性が訴えられるようになった背景は、次に示す通りです。

① 外部環境の変化

上記にも記載した通り、インターネットの普及に伴い、社会を取り巻く外部環境に変化が生じました。例えば、電子データで受発注を行う電子商取引等のサービスが生み出されたのも、その 1 つです。電子商取引では顧客の個人情報を扱う必要がありますが、情報が漏洩した場合の賠償請求等の訴訟リスクが付き纏います。

② 多発するセキュリティ事故

外部環境の変化に応じて対策を講じなければ、当然セキュリティ事故が発生します。例えば、2016 年 12 月度に発生した個人情報の漏洩事件だけでもこれだけの量となります。

公表日	内容	当事者
2016/12/22	中学校で個人情報含む USB メモリが所在不明	○○市
2016/12/22	学生の個人情報含むノート PC を紛失	○○大学
2016/12/21	入試問題案や個人情報含む USB メモリを紛失	○○大学
2016/12/21	生徒の個人情報含む PC を一時紛失	○○高専
2016/12/20	メール誤送信で関係者のメアド流出	○○クラブ
2016/12/19	県立高校で生徒情報を紛失	○○県
2016/12/19	顧客情報記載の書類が所在不明	○○販売
2016/12/16	セキュリティコード含むクレカ情報流出	○○通販サイト
2016/12/16	放送事業者向け情報提供メールで誤送信	○○省
2016/12/15	中学校内で車上荒らし、成績情報が盗難	○○市
2016/12/13	療養費データ 12.7 万人分のデータが所在不明	○○国保連
2016/12/13	自動車重量税納付書を誤廃棄	○○省
2016/12/12	会員向けサイトで個人情報を誤表示	○○会
2016/12/09	ホール予約状況案内メールを誤送信、メアド流出	○○フォーラム
2016/12/09	原子力損害賠償の請求書を紛失	○○電力
2016/12/09	全児童の個人情報含む USB メモリが所在不明	○○市
2016/12/07	不正アクセスでクレカ情報流出	○○通販サイト
2016/12/06	中学校で誤って作製した成績資料を紛失	○○市
2016/12/05	委託先が求人情報メールを誤送信	○○県
2016/12/02	クレカ情報 5.6 万件含む個人情報 42 万件が流出	株式会社○○
2016/12/02	薬剤科見学会参加者への連絡メールを誤送信	○○病院
2016/12/01	不正アクセスでクレカなど個人情報流出	○○通販サイト

セキュリティ事故の規模にもよりますが損害賠償額は非常に膨大であり、115 万人分の個人情報が流出した事例では 5 億 7500 万円、451 万人分の個人情報が流出した事例では 22 億 5500 万円もの損害賠償額が支払われたとも言われています。

そのため、情報セキュリティは、企業が存続していく上でも、無くてはならないもの となります。このような背景から、徐々に重要視されるようになったのです。

3. セキュリティ事故の事例

この章ではこれまでの内容を踏まえ、実際に起こったセキュリティ事故の事例を元に、再度情報セキュリティの重要性について理解を深めていきましょう。人的な脅威を抑制するには、個々のセキュリティ意識の高さが何よりも必要不可欠となります。

それでは、次のようなセキュリティ事故に対して、どのような対策を立てればよいでしょうか。以下の流れで、グループワークを行いましょう。

1. 具体的な対策を個々人で考えてみましょう。(3 分間)
2. グループ内で個々が考えた意見を交換しましょう。(5 分間)

グループワーク①「スマートフォンを紛失した事例」

> ○○は、取引先関係者の個人情報や業務情報が保存されたスマートフォンを、従業員が帰宅途中の電車内で紛失したことを公表した。
> 翌日、警察や交通機関に届け出たが見つかっていない。
>
> 紛失したスマートフォンには、取引先約 200 人の氏名や電話番号、メールアドレス、及び業務情報等が記録されていた。

グループワーク②「コンピュータウィルスに感染した事例」

> ○○は、同社の端末がコンピュータウィルスに感染し、顧客情報等が外部に流出した可能性があることを明らかにした。
> 同社が調査を行ったところ、同端末から不正サイトへアクセスした形跡を確認した。端末に脆弱性が存在し、更に添付ファイルを開いたことでコンピュータウィルスへ感染したという。
> 同社では 7 月 4 日より情報流出の可能性について外部へ調査を依頼していたが、影響はわかっていない。ファイルの精査により対象顧客の特定作業を 6 月 29 日より進めていたが、8 月 16 日に終えたとしている。
> 流出の可能性があるのは、顧客 211 件の氏名と住所。そのうち 1 件についてはメールアドレスも含まれる。また同社の職員名簿についても流出したおそれがある。
> 今回の問題を受けて、同社では対象となる顧客へ事情を説明し、謝罪する書面を送付。

4. コンピュータウィルス

1. コンピュータウィルスとは

コンピュータウィルスとは、第三者のプログラムやデータベースに対して意図的に何らかの被害を及ぼすように作られたプログラムです。それは、次の機能を一つ以上有するものを指します。

名称	意味
自己伝染機能	自らの機能によって他のプログラムに自らをコピー、またはシステムの機能を利用して自らを他のシステムにコピーすることにより、他のシステムに伝染する機能
潜伏機能	発病するための特定時刻、一定時間、処理回数等の条件を記憶させ、発病するまで症状を出さない機能
発病機能	プログラムやデータ等の破壊といった、設計者の意図しない動作をする等の機能

ユーザの気づかないうちに外部から侵入し、内部で増殖して被害を及ぼす点がウィルスと似ていることから、この名称が付けられました。また、コンピュータウィルスには様々な種類のものがあります。以下に示します。

名称	説明	例
ファイル伝染型	アプリケーション等の実行型ファイルに感染する。	W32/Marburg
ブートセクタ感染型	OS を起動するためのプログラムが書き込まれているブートセクタに感染する。	Swiss－BOOT
マクロウィルス	表計算ソフト等のマクロ機能を悪用したもので、データファイル経由で感染する。	W97M/Melissa
トロイの木馬	本来の仕様通りに機能させながら、データの不正コピー、改ざん等を行う。	W32/Gaobot
ワーム	ネットワーク経由で PC 間を自己複製しながら移動、増殖し、破壊を行う。	W32/Mydoom

2. コンピュータウィルスの感染予防策

IPA(独立行政法人情報処理推進機構)に届けられたウィルス感染の経路として、最も多い割合を占めているのが電子メールの添付ファイルです。

予防策として次のような対策を講じる必要があります。

① ウィルス対策ソフトをインストールし、常時稼働させておく。
② 日々新種のウィルスが発見されるため、ウィルス対策ソフトのウィルス定義ファイルは常に最新の状態にしておく。
③ OS や Web ブラウザ、メールソフト等の修正プログラムを定期的にチェックし、常に最新の状態にしておく。
④ ウィルス対策ソフトを用い、定期的にウィルススキャンを行う。
⑤ ウィルス対策ソフトを使ってもウィルスを完全に駆除できない場合があるため、日頃からデータのバックアップを作成しておく。
⑥ メールの添付ファイルやインターネットからダウンロードしたファイル等、外部から持ち込んだデータは必ずウィルスチェック後に使用する。
⑦ マクロウィルスへの感染を防ぐため、マクロ機能の自動実行は行わないようにする。

3. コンピュータウィルス感染時の対処

しかし、予防策を取っていたにも関わらず、ウィルスに感染してしまうことがあります。その場合は、次のような手順で対処します。

なおこれは一般論であり、当研修においては下記①の手順を取った後、速やかにサポーターへ報告して下さい。

① ネットワークを経由して他の PC に感染する可能性があるため、感染したコンピュータをネットワークから切り離す。
② PC の電源を切り、メモリを初期化することでメモリ内のウィルスを消去する。
③ 駆除作業では、ウィルスに感染していない OS 起動ディスクを使用し、ブートセクタからの伝染を回避する。
④ ウィルス対策ソフトを使って、ウィルスチェックをする。
⑤ ウィルスが発見された場合、速やかに情報セキュリティ管理者に報告する。
⑥ 情報セキュリティ管理者は、他の関連部署にも連絡しウィルスチェックをしてもらう。
⑦ 情報セキュリティ管理者は、ウィルス感染の必要情報を IPA(独立行政法人情報処理推進機構)に報告する。

5. ネットワークセキュリティ

1. ネットワークセキュリティとは

ネットワークセキュリティとは、ネットワークからアクセス可能な情報資産を守るために、導入されるインフラに関する規定や方針を意味します。社内のネットワークからインターネットを経由し、外部へアクセス出来ることは、反対に外部からインターネットを経由し社内のネットワークへ不正アクセスされる危険性を孕んでいます。

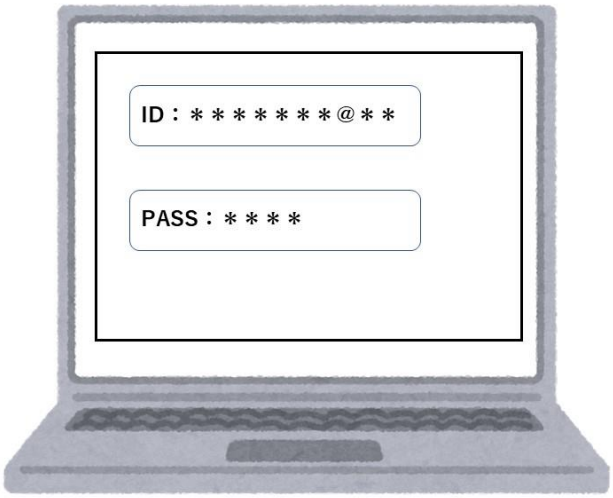
これまでにご紹介したセキュリティ上の問題を防止するためにも、ネットワークセキュリティは必要となります。
ここでは、ネットワークに関する脅威へのセキュリティ対策について見ていきましょう。

2. ネットワークセキュリティ対策

代表的なネットワークセキュリティ対策の手法としては、以下の３つが挙げられます。

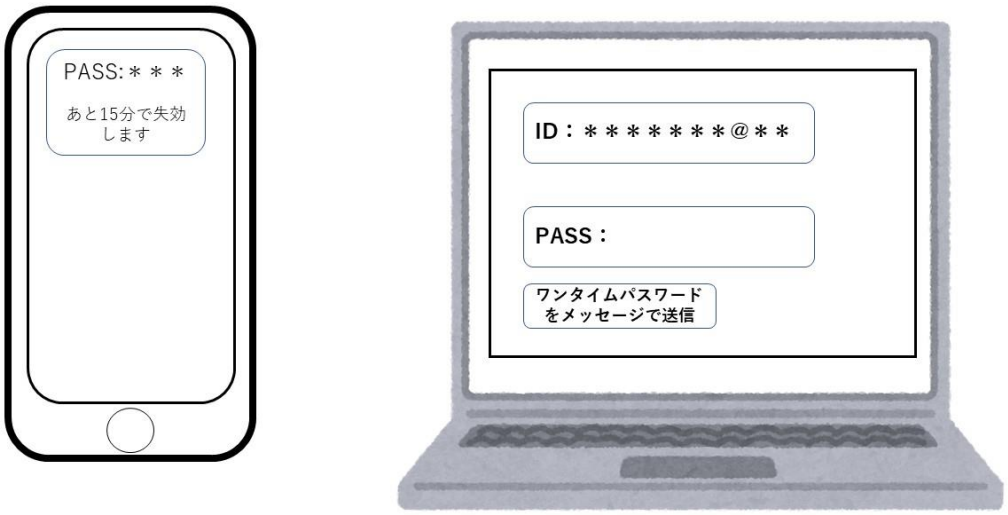
① ユーザ認証

社内のネットワークやサーバにアクセスする際に、事前に発行された ID、パスワードの入力を求める手法です。これによりアクセス権を持つ PC であることを確認することが出来ます。



② ワンタイムパスワード

上記の手法をより強固にしたもので、一度しか使用出来ない使い捨てのパスワードを都度発行し、アクセス権を持つ端末であることを確認する手法です。



③ ファイアウォール

ファイアウォールには防火壁という意味があり、社内のネットワークとインターネットの間に配置し、外部からの不正アクセスを防ぐ役割があります。