情報セキュリティ研修テキスト

２０２２年7月

株式会社フリースタイル

1. 情報セキュリティ対策は、なぜ必要？

情報セキュリティ対策とは？

会社では、業務上で多くの情報を取り扱うことになります。
その中でも大きく分けて下記の2種類の情報が存在します。

個人情報
　個人情報とは「個人情報保護法」により定められた情報
　※詳しくは「個人情報保護研修テキスト」を参照

その他の情報
　個人情報以外の情報。
　例えば、企業で保有している経営情報・営業情報・人事情報・採用情報、
　および開発に関する情報などがあります。

これらの機密情報が外部に漏れないように対策を行うことが
情報セキュリティ対策となります。

情報セキュリティ対策はなぜ必要？

機密情報が外部に漏れると企業にとって
大きな損失を招く恐れがあります。

例えば、新製品の開発情報が他社に漏れる

↓

他社が先に製品化

↓

自社開発ならば
利益損失

お客様からの委託業務ならば
損害賠償

↓

信用の失墜：今後の業務への影響あり

情報セキュリティ対策はなぜ必要？

情報セキュリティ対策を行っている理由は・・・

- お客様からの委託開発(ゲーム開発、アプリ開発他)を行うため
- お客様先で委託業務を行うため

取引先のセキュリティが安全でないと被害を被ることになるため
多くの企業で取引先のセキュリティの安全性確認が行われている。

PマークやISMS（ISO２７００１）の取得は、セキュリティの一定の基準を満たしていることの証明となるため、取引先から取得の有無を確認される場合もある。

2. .情報漏洩はどのようにして起こるのか

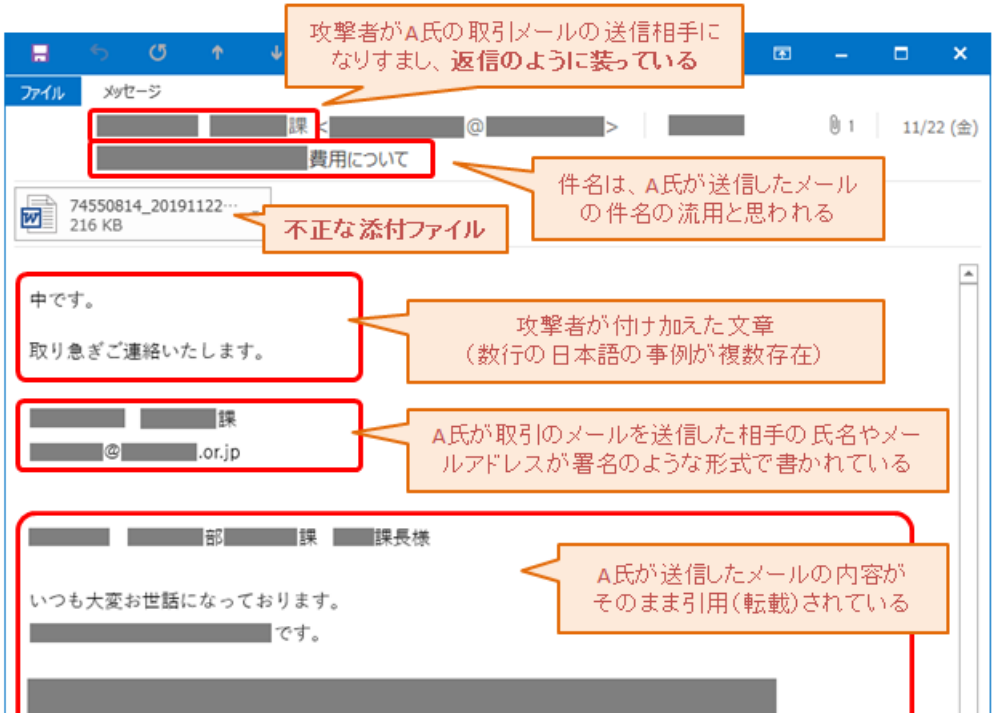
情報持ち出しによる漏洩

情報漏洩が発生する要因の一つに情報の持ち出しを行うことで漏れるケースがあります。過去事例として多いのは、USBフラッシュメモリやスマートフォンを利用して、故意にデータを盗み出すケースが多くありますが、意図せずに漏洩してしまうケースも多く存在します。

- PCを電車の棚やタクシーでおいてきてしまった
- USBフラッシュメモリを紛失してしまった
- USBフラッシュメモリのデータを他のPCで開きデータを残してしまった
- PCやUSBフラッシュメモリ等を盗まれた

ウィルス感染による漏洩

ウィルス感染による不正処理でPC等に入っているデータが漏洩するケースもあります。
最近多いのはメールにて展開されているEmotetというマルウェアに感染する事例がニュースでも取り上げられています。
Emotetは過去のメールの履歴から情報を採取し、大量の不正メールを送付します。



メール誤送信（FAX・郵送）

重要なデータ等をお客様などへ送付した際に、宛先間違いにより情報漏洩するケースもあります。
これはメールに限らず、FAXや郵便でも同様です。

廃棄方法による漏洩

個人のPCやスマートフォンを廃棄する場合にも注意が必要です。
データが残った状態で廃棄・売却等をすると、情報漏洩が発生するリスクが上がります。

また、データを削除しても、ツールを利用することで、ファイルを復元することが出来てしまうためHDDを廃棄する場合はドリル等で穴をあける等の作業が必要となってきます。

一部電化製品屋や情報機器の廃棄を専門に行っている業者に任せて廃棄することで、情報漏洩を防ぐことも可能です。
その際には必ずデータを削除する旨の書類をもらいましょう。

社外でのPC利用

社外でのPC利用にも注意が必要です。
喫茶店などではまわりに多くの人がいる為、画面を盗み見られるケースが多い為、漏洩のリスクは非常に高いと言えます。

公衆wifiに接続することも避けるようにしましょう。
公衆wifiに接続することで、PCにアクセスされる可能性が高まる為、Wifiを利用する際は、独自のパスワードをかけられるwifi（かかった個人wifiやテザリング）を利用することである程度抑止が可能です。

会話による漏洩

情報漏洩はPCや機器のみで発生するわけではありません。
公衆の場での会話や電話は、誰が聞いているかわからない為、注意が必要です。どうしても必要な場合は場所を選んで話をしましょう。

また、よくあるのは居酒屋や飲食店などで客先の話をすることがあります。
こちらも上記と同じで誰が聞いているかわかりません。
話しをしている対象のお客様が聞いていた場合信用の失墜につながることもあるので、話す場所にも意識を向けるように努力が必要です。

3.情報セキュリティ対策

機器の取り扱いについて

私物のPCやネットワーク機器（スマホ含む）、またUSBやHDDといった記憶媒体をPCへ接続することは禁止となります。
外部からのウィルス感染を抑止する目的とともに、機密情報の持ち出しをできないようにする為となります。

USBなどの記憶媒体については、社用の媒体がありますので、必要な場合はシステム管理責任者へ相談をお願いします。

業務に関係ないWEBサイト閲覧

業務に関係のないWEBサイトへアクセスすることは、ウィルス感染のリスクを高めることになる為禁止となります。
業務に関係のある場合でもウィルス感染の危険性はあります。
特に海外のサイト等は危険な為注意が必要です。

離席時のPC状態

離席時には必ず画面ロックまたはログアウトをするようにしてください。
離席中に画面が表示されていると機密情報を見られる可能性があります。

OS標準の設定でスクリーンセーバーの設定があるので、スクリーンセーバー起動時に画面ロックを行うようにすることで、画面ロックのし忘れを抑止できます。

ウィルス感染時の対処

ウィルスに感染した、またはPCの挙動がおかしいと感じた際は、LANケーブルを抜く又はwifiを切断するようにしてください。
問題を解決しようとしていろいろ設定をいじる人がいますが、
それにより悪化する可能性もありますので、余計なことはせずに、
システム管理者の指示を仰ぎましょう。

※感染が疑われた際にPCをシャットダウンする人がいますが、これも誤りです。
シャットダウンにより動作するウィルスがある為です。

メール誤送信対策

メール誤送信は昔から多く発生しているセキュリティ事故でもあります。
メール誤送信により、本来送ってはならない相手に情報が送られてしまい、問題となるケースが多発しています。

メール送信の際には送信先に誤りがないか確認したり、ソフトウェアを利用して、再確認するなどの抑止策を取る必要が有ります。

また、誤送信はメールに限った話ではありません。
FAXや郵便も送り先を誤ると誤送信としてセキュリティ事故となりますので注意しましょう。

スパムメールの対処

近年感染が拡大しているEMOTETというマルウェアが存在します。
特徴として、メールの履歴情報を奪い、それを元にあたかも知り合いからメールが送られてきたと誤認させウィルス感染する添付ファイルを開かせるマルウェアとなります。

対処としては送信者のアドレスや本文に間違いや違和感がないか確認することで、ある程度抑止が可能です。

下記点に注意し対応しましょう
- 送信元アドレスに身の覚えがない
- 添付ファイル名が英名等、ウイルスファイルの可能性がある

Cookieへの情報保持

cookieは閲覧した際の情報をPCに残しておく仕組みです。ショッピングサイト等で再度訪れるとカートの中身が残っているのもcookieを利用している為です。

cookieのデータが残っていることで、そのデータを元に悪用されるケースがある為、cookieへ個人情報を残さないようにしましょう。