セ キ ュ リ テ ィ 研 修

アジェンダ

1. 情報セキュリティとは
2. 個人情報と機密情報
3. セキュリティ事故のインパクト
4. 情報漏洩の影響
5. メール誤送信例
6. IDカード・入館証紛失事例
7. IDカード・入館証の取り扱いに注意
8. 事故発生時の対応の重要性
9. パソコン使用における取り扱い注意点
10. 情報セキュリティルール①～④

1. 情報セキュリティとは

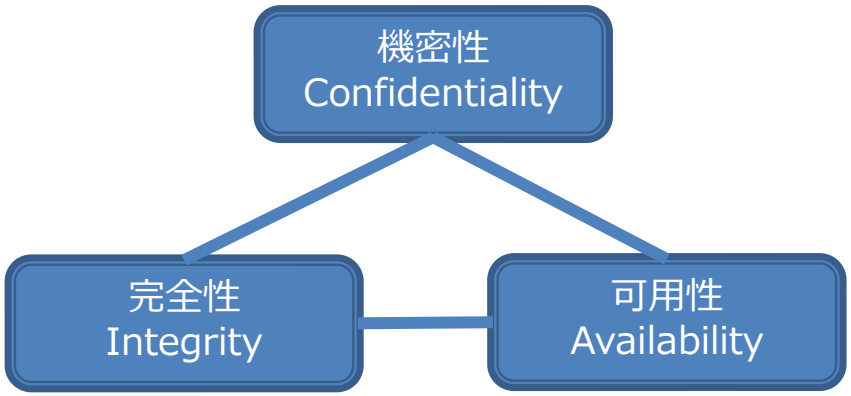
■ 情報セキュリティとは

企業が保有する情報資産（データやドキュメント、PCやサーバ、ソフトウェア、サービス）の機密性・完全性・可用性を維持すること

機密性：許可された者だけが情報にアクセスできるようにすること

完全性：情報が正確で完全であること

可用性：いつでも利用可能な情報であること



■情報セキュリティ・マネジメントシステム（ISMS）

組織のマネジメントとして、自らのリスクアセスメントにより必要なセキュリティレベルを決め、プランを持ち、資源を配分して、システムを運用することである。

要約すると、保有している情報資産を安全に管理すること。

2.　個人情報と機密情報について

個人情報とは・・

機密情報のうち、氏名・住所・写真など、

個人を特定できる情報

機密情報とは‥

会社経営上重要で機密を保つ必要がある情報

一般的に、極秘・部外秘・社外秘などに区分される

お客様先で業務上知り得た情報も対象となる！

3. セキュリティ事故のインパクト

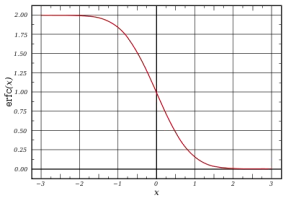
セキュリティ事故

- 情報紛失・流出
- ウイルス感染
- 不正アクセス
- システム停止
- 情報の改ざん

お客様・スタッフ・社員・社会への被害

- 社会に対する信用度失墜
- 損害賠償、取引停止
- 懲戒処分
- 業務遂行に支障 コスト増大

業績悪化



4. 情報漏洩の影響

【過去の事例より】

No.	内容	影響
1	ファイル転送サービス「宅ふぁいる便」より、約480万件の顧客情報が流出。 本来存在しない不正なファイルを同サービスのサーバ内で発見。調査を進めるなか、不審なアクセスログを確認	顧客情報約480万件の流出を確認。流出したデータには、同サービスの利用者に関する氏名や都道府県、生年月日、性別、業種、職種、メールアドレス、ログイン用のパスワードなどが含まれる。アカウント情報を変更するよう呼びかけをした。
2	人材派遣事業のスタッフサービスの元従業員が登録者に関する個人情報を在職中に外部に持ち出し、1万5368名分の情報漏洩となった。	流出したのは、1万5368人分の登録者情報で、氏名や住所、電話番号、メールアドレスなどが含まれる。既に回収済みと説明はあったが性別や時給金額、企業名などの営業情報も流失していた。
3	JTBのネットサービスで海外からの不正アクセスにより約７９３万人分の個人情報が流出。取引先を装ってウイルス感染させる「標的型メール」が原因。	流出した個人情報の中にはパスポート番号や外国人顧客なども一部含まれていた。流出問題があった翌月は予約サイトでの販売額が1割減であった。
4	日本年金機構がサイバー攻撃を受けて個人情報約１２５万件が流出した。	流出した個人情報は基礎年金番号、氏名、生年月日、住所の４種類。４種類すべてが含まれるのは約５万２千件。情報が漏れた受給者と加入者には謝罪文書を送付した。
5	ベネッセコーポレーションにおいて、データベースを管理していた担当者が、生活苦からお客様の個人情報を名簿業者に売却した。	発覚から2ヶ月後、ベネッセは記者会見を開き、顧客情報漏洩件数を3504万件と公表、個人情報漏洩被害者へ補償として金券500円を用意するとし、35社が漏洩した個人情報を利用していたため事業者に対して情報の削除を求めるなど利用停止を働きかけた。

5. メール誤送信事例

＜社内事例①＞

協力会社宛てにメールを送信する際、Ccに「山田太」さんを設定するはずが、「山田太郎」さんを選択して送信してしまった。（※文中の氏名は仮名です。）

【事故の原因】

宛先選択時、アドレス帳を利用せず、且つメールアドレスを十分に確認しなかったため誤送信となった。

宛先確認時は必ずアドレス帳を利用する、アドレス帳には氏名をフルネームで登録するなど、誤送信リスク対策の徹底をしてください！

＜社内事例②＞

そもそも送られてきたメールのアドレスが間違っていたが、そのメールを「全員返信」でメールを作成し返信してしまった。

【事故の原因】

送信する際、宛先に入っているメールアドレスを信用してしまい、そのまま全員に返信してしまった。

送信時はアドレス全てが適切なものか、機能に惑わされずに確認の徹底をしてください。

＜社内事例③＞

お客様から送られてきたメールを社内へ転送する際、誤って返信を選択してしまい、社内のやりとりがお客様にも送られてしまった。

【事故の原因】

繁忙期でスピードを重視したため、送信する際に改めて宛先に入っているメールアドレスを確認しなかった。

忙しい時ほどメールの送信は慎重に！送信前には再度、宛先を確認して下さい。

6. IDカード・入館証紛失事例

◆終業後、IDカードをぶら下げたまま就業先を出て、地下鉄の入口でIDカードを鞄にしまおうと思った所、ケースにIDカードが入っていなかった。今通った道を探し回ったが発見できず、就業先の警備室に確認すると届けられていた。その後すぐに一時紛失した事を報告した。

社員証は最後に提示した“その場所“で、鞄にしまう。IDカードケースが劣化していたらすぐに交換！紛失した場合は、探す前に報告！

◆業務後に飲食店に立ち寄り飲酒後、帰宅途中にお客様からの貸与品である
入館証をいれた鞄を紛失　飲酒起因事故による発生確率高し。

情報セキュリティ物品をもっている際は、常に携帯を意識すべし！
飲むなら持つな、飲んだら酔うな！

◆電車の網棚に置き忘れ、**社員証を入れていた鞄を紛失**

カバンは網棚には乗せないこと！

7. IDカード、入館証の取扱いに注意！

◆引越し時の紛失は過去にも多く発生しています。
貴重品などと同様に厳重に管理してください。

◆セキュリティカードにはストラップを付け、移動時は身体や鞄に固定してください。シャツや背広の胸ポケットに入れただけでは落下のリスクを避けられません。
また鞄に入れる場合は、必ず立ち止まるなど他の作業を中止し、しまったことを確認して下さい。鞄はチャック等の付いたポケットにしまうか、ストラップで鞄の金具等に固定して下さい。
鞄の中に無造作に入れてしまうと、鞄から財布などを取り出す時に一緒に落下する危険性があります。

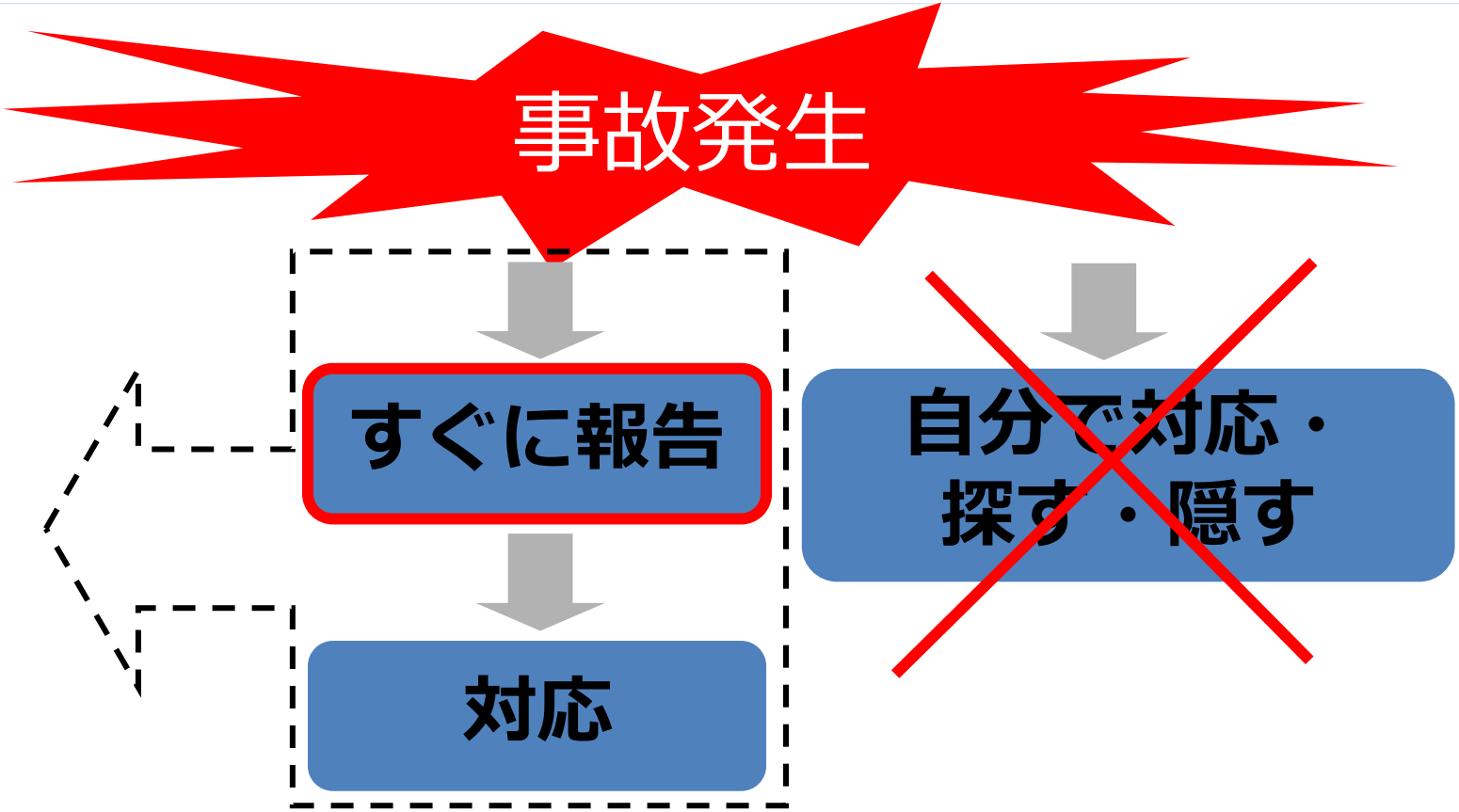
◆ストラップとカードケースの接続部分に十分な強度があるか確認してください。外れそうな場合は、早急に新しいものと交換してください。

◆休日等利用しない場合は持ち歩かないようにしてください。

万が一紛失した場合は、探す前に速やかに報告！

8. 事故発生時の対応の重要性

ここのスピードがお客様からの信用につながる



事故事件が発生した場合！

- ◆指示された緊急連絡先に基づき、上長に報告
- ◆業務時間外・休日・深夜に関わらず**直ちに報告・連絡をする**こと
- ◆自分一人だけで対処しようとしないこと

9. パソコン使用における取り扱い注意点

- 必要外のWebサイト閲覧はしない
  - 業務に必要のないサイトへのアクセスはしないこと
  - 許可無くアクセスしたサイトでの書き込みやダウンロードはしないこと
- 常に情報セキュリティ対策をとる（Windows Updateなど）
  - ウィルス感染防止のソフトウェア導入
  - ソフトウェアの更新
- 個人所有機器（USBなど）の業務利用は原則禁止とする
  - USBメモリ等の許可されていない機器使用禁止
  - 業務外のタブレット、スマホの使用禁止
- 許可されていないソフトウェアは導入しない
- 他人に利用されないような対策をする
  - 離席時の画面ロック
  - パスワード管理

セキュリティ事件・事故は、取引停止や莫大な損害賠償が発生する可能性があります。

情報セキュリティに対する意識を向上させ、

①お客様先・プロジェクトルール

②情報セキュリティルール

を遵守し、セキュリティ事件・事故防止に努めて下さい。

お客様の信頼を維持・向上させるのは、
みなさん一人一人の行動が重要です

10. 情報セキュリティルール①

【基本姿勢】

1. 情報セキュリティ基本方針、個人情報保護に対する基本方針を理解し、遵守する。
2. お客様先のセキュリティポリシーを理解し、遵守する。
3. 自社及びお客様からの貸与品である身分証明書(ID カード)やお客様先入館証、携帯 電話やスマートフォンは以下の紛失・盗難対策を行う。
   - ① 職場内では、ネックストラップ等で常時身につける。
   - ② 移動時はネックストラップ等で身体に固定するか、鞄のチャックの付いたポケットにしまう等、紛失・盗難に細心の注意を払う。
   - ③ 紛失・盗難に早く気付き適切な対処を行うために、出勤時及び帰宅時に必ず保持確認を行う。
   - ④ 紛失・盗難時は警察や交通機関に届出るとともに、機能停止の手続きを行う。
   - ⑤ 携帯電話やスマートフォンは、指紋認証やパスワードで情報を保護する。
   - ⑥ 携帯電話やスマートフォンに保存される機密情報を含むメールは、不要となったら直ぐに削除する。
   - ⑦ 携帯電話やスマートフォンに、SD カード等の外部メモリを装着することは禁止とする
4. 業務上知り得た情報は公開しない。
   - ① 不特定多数が閲覧できるサイト（個人ホームページ、ブログ、電子掲示板､ツイッター等のＳＮＳ）への書込みを行わない。
   - ② 業務上知り得た情報について、社外（通勤途中、飲食店、自宅等）でむやみに口にしない。
5. 職場内での個人所有機器（PC、タブレット、スマートフォン、USB 等）の業務利用は、やむを得ない事由を除き、禁止とする。

10.情報セキュリティルール②

【情報のライフサイクルにおける取り扱い】

【取得・入力】

1. 情報は不正に取得しない。また業務遂行に必要のない情報は取得しない。
2. 個人情報や機密情報（極秘・部外秘・社外秘）をシステム等へ入力する際は、その情報が正確であるように努める。

【移送・送信】

1. 電子メールや FAX、郵便で個人情報や機密情報を送信する際は、以下の誤送信防止対策を行う。
   - ① 電子メールや FAX、郵便の送信時は、宛先と内容が一致しているか出来る限り複数人で確認する。
   - ② FAX の場合、送信後には受け取り確認を行い、確実に相手先に届いていることを可能な限り確認する。
   - ③ 電子メールや FAX の場合、必要のない宛先が含まれていないか確認する。
   - ④ 電子メールの場合、機密情報や個人情報は本文に記載せずfileforce や OneDrive などで共有をする
   - ⑤ 電子メールの場合、メールソフトの環境設定にてメール送信時に一定時間送信されない設定とし、送信前に再度確認する。
   - ⑥ 電子メールの場合、宛先選択ミスを防止するためにアドレス帳には会社名や部署名を登録するなど工夫し、また定期的なメンテナンスを行う。
   - ⑦ 個人情報や機密情報の授受は原則としてファイルサーバを利用し、電子メール添付での情報送付は避ける。

10.情報セキュリティルール③

2. 個人情報や機密情報を含むドキュメントや情報機器を持ち出す場合は、以下の情報漏洩対策を行う。
   ① 情報が入った鞄は肌身離さず所持し、電車の網棚に載せない。
   ② 飲酒厳禁。
   ③ 情報セキュリティ推進責任者の承認の上、「持ち出し管理簿」にて管理する。
   ④ PC の場合、BIOS の他 HDD パスワードを設定し、暗号化ソフトを導入する。
   ⑤ USB 等の可搬記憶媒体は、暗号化できるものを利用する。

【利用・加工】

1. 業務中に取扱う情報は業務目的のみに使用し、適切に管理する。
2. 業務利用する PC には、以下の情報セキュリティ対策を行う。
   ① BIOS パスワードを設定する。
   ② Windows パスワードは推測されにくい英数混合 8 桁以上に設定し、90 日毎に変更する。
   ③ スクリーンセーバの起動を 5 分以内とし、パスワードロックの設定にする。
   ④ オートコンプリート機能は利用しない。
   ⑤ OS のアップデート（WindowsUpdate）の実施状況を、月 1 回手動にて確認する。
   ⑥ ウイルス対策ソフトの定義ファイルが最新化となっていることを、月 1 回手動にて確認する。
   ⑦ 認められていないファイル交換ソフトはインストールしない。
   ⑧ 許可されていないソフトウエアはインストールしない。

10.情報セキュリティルール④

【保管・バックアップ】

1. 個人情報や機密情報を含むドキュメントや情報機器は施錠管理、電子データはアクセス制御された安全なサーバに保管し、業務用 PC 内に個人情報や機密情報を保管しない。
2. 個人所有機器や個人契約（登録）のクラウド型ストレージサービスへの個人情報や機密情報の保管は禁止とする。

【廃棄・消去】

1. 個人情報や機密情報を含むドキュメントの廃棄は、シュレッダー又は溶解処理とする。
2. 情報機器や電子媒体は、物理的に破壊した上で廃棄する。
3. 退職時には、全ての情報を返却する。
4. プロジェクト終了後は、全ての情報をお客様に返却する。

【セキュリティ事件・事故発生時】

1. 事件・事故発生時及びその恐れがある場合は、直ちに上長に報告する。
2. 紛失・盗難の場合は警察や交通機関への届出を行う。
3. 事件・事故発生に備え、緊急連絡先を確認しておく。

10.情報セキュリティルール⑤

【個人所有機器から Microsoft 365 への接続】

（1）個人所有機器から Microsoft 365 に接続する際は、セキュリティ基準を満たすものを利用し、以下の情報漏洩対策を講ずる。

①個人所有機器には、認められていないファイル共有ソフトをインストールしない。
②スマートフォンやタブレット、携帯電話には指紋認証やパスワードを設定の上、会社貸与品に準じた対策を行う。

③Microsoft 365 へ接続する際には閲覧のみとし、データのダウンロード及び保管は原則禁止とする。なお、部門長の承諾による指示によりダウンロードが必要な場合は、作業完了後には速やかにデータを完全に削除する。

④ネットカフェ、ホテル等公共の場所に設置されている PC の利用は基本的に禁止とする。

⑤個人所有機器からのお客様先システムへの接続は禁止とする。

10.情報セキュリティルール⑥

＜使用可能な Web ブラウザおよびそれぞれのセキュリティ設定＞
貸与品のタブレット、スマートフォンについては OS 標準のブラウザを利用すること。

使用可能な Web ブラウザ	セキュリティ対策
Internet Explorer 最新バージョン Microsoft Edge(Chromium 版) 最新バージョン Google Chrome 最新バージョン Firefox 最新バージョン Safari 最新バージョン	【OS】 指定されたブラウザの動作が可能な OS を利用し、常に最新の状態にアップデートする。 【ウイルス対策ソフト】 有償・無償を問わずウイルス対策ソフトをインストールし、最新の定義ファイルにする。 （Windows Defender、マカフィー、ノートン、ウィルスバスター、ESET 等）

※上記以外の Web ブラウザを使用する際は、事前にシステム担当者に報告する。
※会社貸与 PC の利用者は、インターネットは、業務以外の目的に利用してはならない。信頼できない Web サイトには原則としてアクセスしてはならない。業務上必要な場合は、システム担当者へ報告し、指示に従う。

お客様先では、「必ず」ルールに従って情報セキュリティを守ってください。

よろしくお願いいたします。