情報セキュリティ教育テキスト
～情報資産と個人情報～
＋捕捉

1.個人情報保護の必要性について

１．個人情報保護の必要性について

「個人情報」はプライバシーの一つであり、本人のものです。

- 個人情報が漏洩することにより、悪徳業者に渡り見知らぬ架空請求や、悪質なメールの送信等実害も発生する可能性があります。個人のプライバシーを守ることはもとより、個人情報を適切に取り扱うことは企業として当然の社会的責務なのです。
  - **自分の個人情報（氏名、連絡先、学歴、健康状態、給与額等）がずさんな管理をされていて、見ず知らずの人に興味本位で見られていたり、社会に漏洩することで事件やトラブルにあったら！！　という意識を持って下さい。**

個人情報は本人の持ち物であり、私共はその持ち物を預かっているに過ぎません。

１．個人情報保護の必要性について

個人情報漏洩事件の例

– 過去にいくつもの個人情報漏洩事件が社会的問題となっていま

企業名	時期	内容
ベネッセコーポレーション	2014年7月	外部業者の派遣社員が顧客の大量の情報およそ760万件を圧縮ファイルで小分けにした上で持ち出した。営業秘密に当たる顧客の情報を流出させた不正競争防止法違反で逮捕。お客様へのお詫び対応として、200億円の原資を準備。 ベネッセは顧客情報に関するデータベースの運用や保守をグループ企業の「シンフォーム」に委託。同社はさらに複数の外部業者に分散して再委託していた。

２.情報資産とは？

情報資産とは？

極論を恐れずに単純に言うと「組織にとって”大事なモノ”」です。
どういう大事なものが情報資産になるかというと、次の3つの側面から考える事が出来ます。

・機密性（confidentiality）を維持する必要があるもの
・完全性（integrity）を維持する必要があるもの
・可用性（availavility）を維持する必要があるもの

・機密性とは・・・
許可されている人だけが情報にアクセスでき情報が外部に漏えいしないこと
・完全性とは・・・
情報が改ざんされたりせず整合性が取れて完全な状態であること
・可用性とは・・・
システムが安定運用されており必要なときに情報にアクセスできること

３.個人情報とは？

個人情報とは？

個人情報保護法における個人情報の定義

生存する個人に関する情報であって、当該個人情報に含まれる氏名、生年月日その他の記述などにより特定の個人を識別することができるもの

（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む）

JIS Q 15001における個人情報の定義

個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述などによって特定の個人を識別できるもの

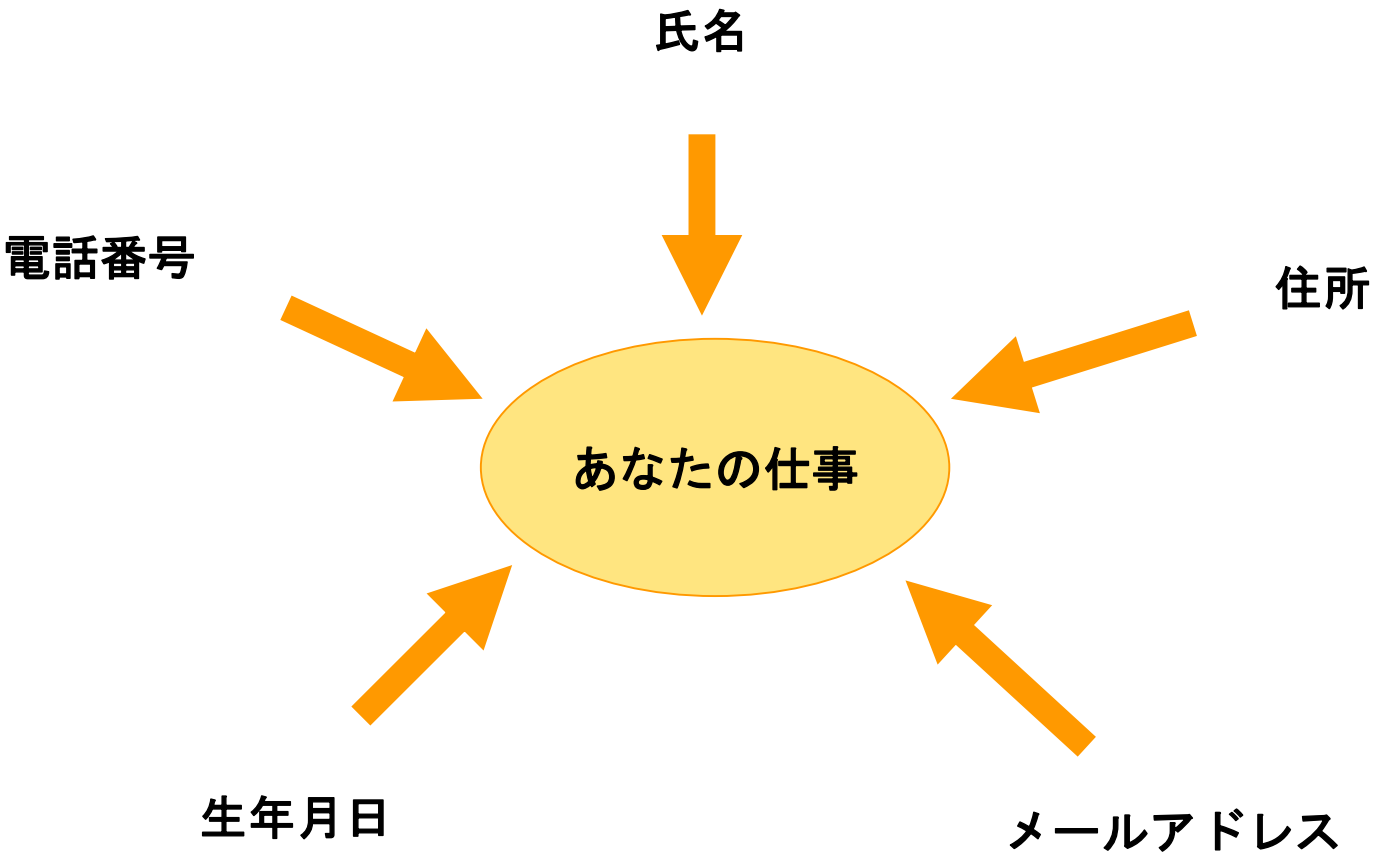
（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む）

個人情報とは？

特定の個人を識別できるもの

（例）
- 氏名
- 住所
- 電話番号
- メールアドレス
- 生年月日

あなたの仕事にも個人情報が含まれている



常に潜んでいるリスク

取扱いの各局面におけるリスク

- 漏えい（外に漏れること）
- 滅失（なくなってしまうこと）
- き損（壊れること、正確でなくなること）

結果として起こるリスク

- 関連する法令，国が定める指針その他の規範に対する違反
- 想定される経済的な不利益及び社会的な信用の失墜
- 本人への影響などのおそれ
- 業務停止をしなければならなくなる

番外. 第三者が他人の個人情報を公開しても良い場合とは？

- 生命・身体・財産の保護のために必要な場合
- 警察・裁判所による照会対応など法令に基づく要請

（個人情報の保護に関する法律　第二十七条より）

なぜこういったリスクが起こるのか？

ほとんどが規則を守らないことによる事故

例1）寝坊をして慌てていたため、会社のパソコンを電車に置き忘れてきてしまった。

例2）USBメモリに顧客情報を無断で写していたものをうっかり紛失してしまった。
ディーメイクは例外を除きリムーバブルディスクの使用は禁止です。（例外：デジカメ等）

例3）フリーソフトの無断ダウンロードが禁止されているにも関わらず、こっそりダウンロードをしてウィルス感染してしまった。

５.個人情報取り扱いによるリスク

もし事故を起こしてしまったら？

あなたや会社にこんなことが降りかかってくるかもしれません。

６.あなたにできることは？

あなたにできることは？

・規則を守る事

情報セキュリティポリシーを読みましょう。

・危ないと思ったら報告する事

社内にはインデント報告ルートが存在します。

６.あなたにできることは？

・規則を守る事

規則を理解し、遵守すれば、個人情報保護法に従った行動を行えます。

規則の例

・パスワードをメモした紙をパソコンに貼り付けないようにしましょう。
・会社のデータ情報などは持ち帰らないようにしましょう。
・未許可のサイトへのアクセスをしないようにしましょう。
・個人情報の含まれるメールは暗号化しましょう。
・帰宅時はパソコンの電源を必ずオフにしましょう。
・許可なくノート型パソコンを社外に持ち出さないようにしましょう。
・クリアデスク、クリアスクリーンを実施し、大事な物を出しっぱなしで席を離れないようにしましょう。

６.あなたにできることは？

・危ないと思ったら報告する事

事故ではないからと軽視をせず、危ないと思ったことを報告することで、
本当の大きな事故を防ぐことができます。

例えば、

・アドレス帳から違う人のメールアドレスを選択してしまっていた。
・FAX番号を押し間違えていたが、送信前に気づいた。
・個人情報の書かれた紙の裏を使った後、ゴミ箱に捨てそうだった。
・メールを送る時のBCC欄とCC欄を間違えていた。
・パスワードを書いたメモ紙が物を出した時に飛んでいった。
・友人との世間話で顧客情報を伝えてしまった。

7.まとめ

・まとめ

1.個人情報とは？

特定の個人を識別できるもの
あなたの仕事にも個人情報が含まれている
「氏名」「住所」「電話番号」「メールアドレス」
「生年月日」等

2.個人情報取り扱いによるリスク

取り扱いの各局面におけるリスク、結果として起こるリスク
リスクはほとんどが規則を守らないことにより起こる
もし事故を起こしてしまったら罰則がある可能性

3.あなたにできることは？

規則を守る事
危ないと思ったら上司に報告する事

8.ソーシャル・エンジニアリング

8.ソーシャル・エンジニアリング

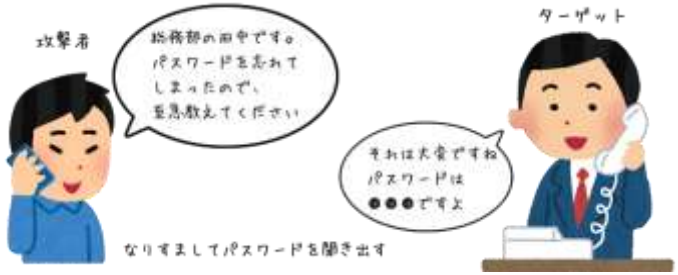
ソーシャル・エンジニアリングとは

- ソーシャル・エンジニアリングとは、情報セキュリティにおける「人間の心理的な隙」を突いて、機密情報やアクセス権を不正に入手する手法のことです。
- 技術的なハッキングではなく、人をだまして情報を引き出す「非技術的な攻撃手法」であり、情報漏洩や不正アクセスの原因となることがあります。

8.ソーシャル・エンジニアリング

■ 主なソーシャル・エンジニアリング手法

1. なりすまし
　信頼できる人物や組織（上司、社内IT担当、業者など）になりすまして情報を聞き出す。



2. フィッシング
　偽のメールやWebサイトでユーザーを誘導し、パスワードや個人情報を入力させる。

3. ショルダーハッキング
　他人がパスワードなどを入力する姿を背後から覗き見て盗み見る行為。

4. ゴミ漁り（ダンピング）
　ゴミ箱からメモや書類などの機密情報を探し出す。

5. 尋問・電話詐欺
　電話で相手の立場や状況を利用し、情報を自然に引き出す手法。

ソーシャル・エンジニアリングの対策

1. セキュリティ意識の向上
   定期的なセキュリティ教育や研修を実施する。自主的に学習する。

2. 情報取扱の明確化
   書類やメモは破棄する際にシュレッダーを使用。

3. パスワードの管理徹底
   ID・パスワードは絶対に第三者に伝えない。

4. 不審なメールや電話への対応
   不明な相手には情報を教えない。確認のプロセスを設ける。

- 5. ログイン・画面表示の注意
   外部の目を気にして操作する。画面ロックも徹底する。

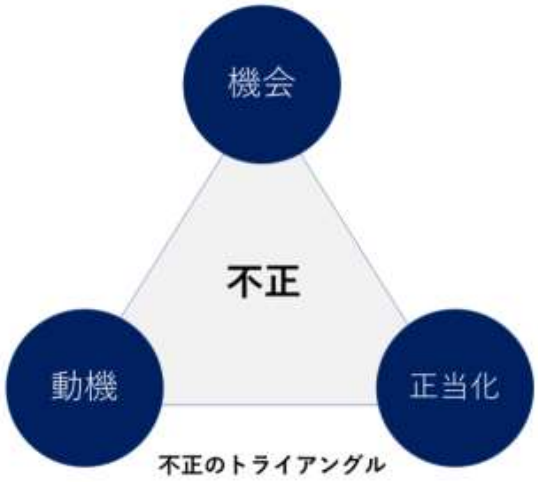
常に人の目を気にしましょう。

9.不正のトライアングル

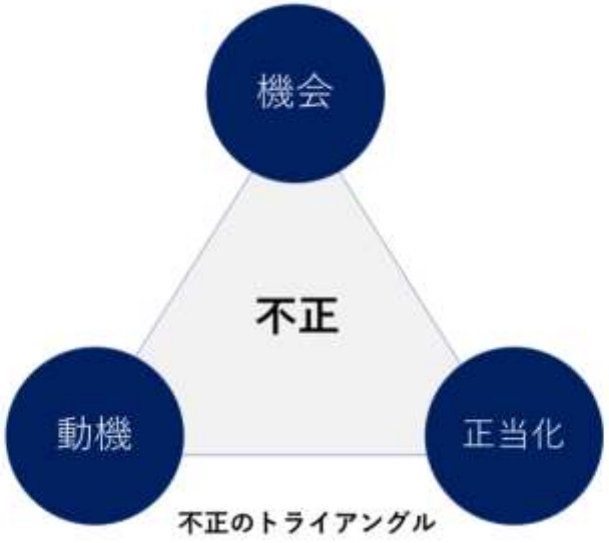
不正のトライアングル

- 不正のトライアングルとは？

不正トライアングルは、アメリカの犯罪学者である
ドナルド・R・クレッシー（Donald R. Cressey）が提唱した理論です。
不正行為が発生する要因を「動機」、「機会」、「正当化」の
3つの要素で説明しています。



不正のトライアングルの説明



不正のトライアングル

動機（Motive）：不正行為を行う理由や動機です。
たとえば、金銭的な困窮、職場での不満、過去の経験から来る報復心などが該当します。

機会（Opportunity）：不正行為を行うチャンスや機会が存在することです。
企業や組織内で、管理の甘さや監視の不十分さが原因で、不正を犯す機会が生じることがあります。

正当化（Rationalization）：自分の行動を正当化する考え方です。
不正行為に対して罪悪感を感じないよう、自分の行為を合理的に説明することで、
行動に対する心理的障壁が低くなります。

この3つの条件が揃う時、不正が起きやすくなると言われています。

不正のトライアングルの例

例えば大谷翔平選手の口座から巨額の現金資産を盗んでいた
水原一平容疑者の場合

- **動機**：彼は違法賭博による巨額の負債を抱えていたと報じられています。負債返済のプレッシャーが、不正行為を働く動機になった可能性があります。
- **機会**：通訳という立場上、大谷翔平の資金管理にある程度アクセスできる状況だったと考えられます。通訳以上の権限や彼との信頼のある立場が、不正の機会を生んだ可能性があります。
- **正当化**：「賭けに勝てば返済できる」「一時的に借りるだけ」「自分も苦しんでいる」「大谷はあれだけ稼いでいる」といった自己正当化の論理が働いていた可能性があります。

不正のトライアングルでは、こうした心理的なハードルの低下が、不正を引き起こす要因となります。

もしあなたが不正を犯したなら？

- 社内：就業規則内での各種懲戒行為にあたり、あなたは減給、解雇など社内罰則が適用される可能性が有ります。
- 社外：不正が外部に影響を及ぼす内容であった場合、会社の社会的信用は失墜します。

あなた自身も各種機関から刑事罰・民事訴訟などを受ける可能性があります。

法令違反に該当する場合

法令	罰則の例
個人情報の保護に関する法律	三年以下の懲役または百万円以下の罰金
不正アクセス行為の禁止等に関する法律	二年以下の懲役または百万円以下の罰金

当然ですが、不正を行うのはやめましょう。

会社側も労働環境の改善を逐次行っていますが、もし不満や困っている事があるのであれば、上司や各種相談窓口にまず相談をしてください。