情報資産と個人情報を適切に管理するために

情報セキュリティ兼個人情報保護教育テキスト

はじめに

ISMSとPマークでは年に1回の教育を義務付けています。

今回の教育の中で、ただ、テキストを見るというのではなく皆さんのお仕事上でもどういうことに気を付けるべきなのか？

自分の身近に起こりうる事例を含めて気を付けていただきたい点を改めて共有いたします。

他人事ではなく、自分自身に置き換えて情報漏洩の事故や事件が起こらないように、気を引き締める意味合いで今回の教育の受講をお願いいたします。

目次

ISOの定義

ISO=国際標準化機構（International Organization for Standardization）

「世界中で同じルールでやり取りするための国際物差し」のことです。

例えば・・・💡

「非常口の表示が国ごとに違ったら困る」のと同じで、
世界共通のルールを作ろう！というのがISOの考え方です。

ISMSとは

ISMS=Information Security Management System の略。
ISOの中の情報セキュリティにおけるルール(規格)です。

ISMSの規格で守るべきものを“情報資産”と言います

✎情報資産とは：会社が保有する「価値のある情報」すべてです！

社内外における
“個人情報”

取り扱っている
業務データ

ソフトウエア

クラウドサービス

ハードウエア

etc

✎個人情報とは：生存する個人に関する情報で、特定の個人を「識別できる」ものです！

💡例えば・・・
・氏名
・生年月日
・住所
・顔写真
・会社名
・マイナンバー(個人番号)　など

<u>これらの情報が2つ以上組み合わさると、特定の個人を「識別できるもの」になります！</u>

例) 株式会社テクノエージェント　山田 花子
　　東京都新宿区○○-○○在住　山田 花子

※「氏名だけ」「住所だけ」では、“個人情報”とはなりません。

✎個人情報にも：日本国内においての規格があります！

Pマークとは=プライバシーマーク制度の略。
日本国内限定の制度です。

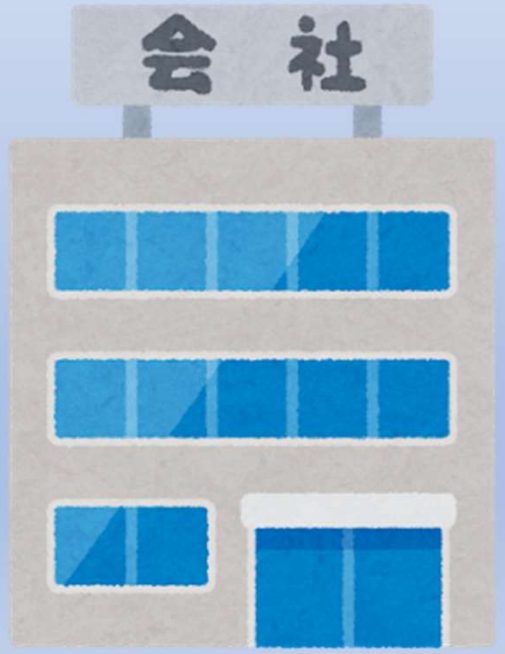
※引用元
一般財団法人日本情報経済社会推進協会
https://privacymark.jp/

当社はこの認定も取得しています！

✎ISMSとPマークを持っていることのメリット

💡 ISMSとPマークを持っていると

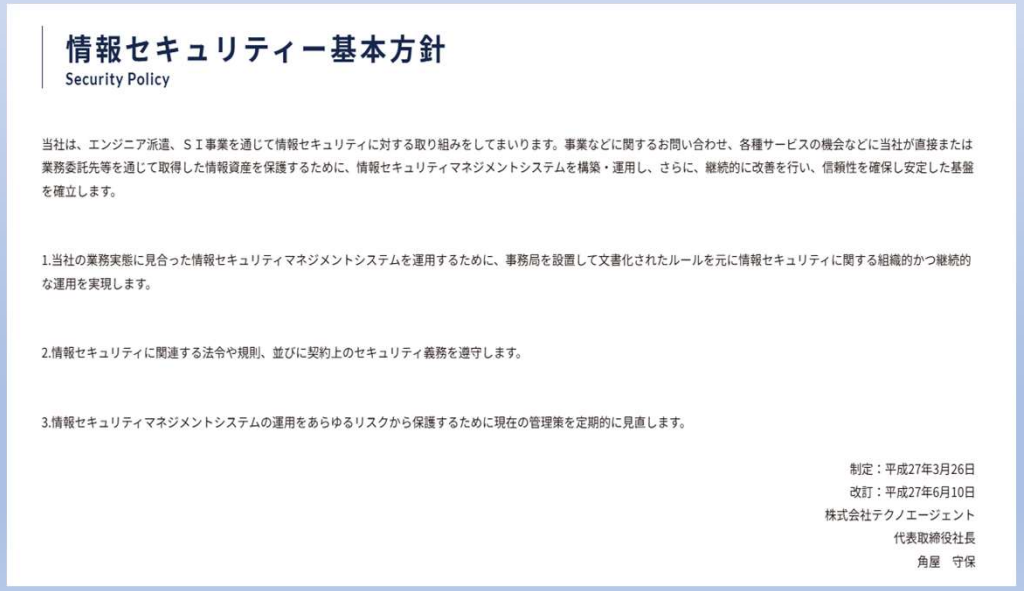
取引先や社会からの信用を得ることができ、会社の利益につながります！



✎ISMSとPマークの当社の方針

💡 ISMSとPマーク方針の掲載場所

当社HPに掲載しています！



情報セキュリティー基本方針
Security Policy

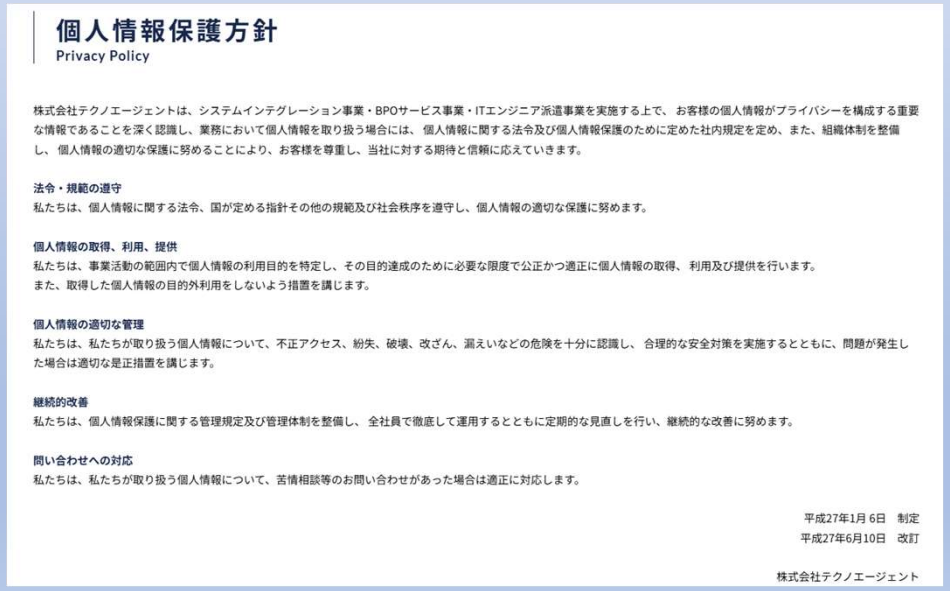
当社は、エンジニア派遣、ＳＩ事業を通じて情報セキュリティに対する取り組みをしてまいります。事業などに関するお問い合わせ、各種サービスの機会などに当社が直接または業務委託先等を通じて取得した情報資産を保護するために、情報セキュリティマネジメントシステムを構築・運用し、さらに、継続的に改善を行い、信頼性を確保し安定した基盤を確立します。

1.当社の業務実態に見合った情報セキュリティマネジメントシステムを運用するために、事務局を設置して文書化されたルールを元に情報セキュリティに関する組織的かつ継続的な運用を実現します。

2.情報セキュリティに関連する法令や規則、並びに契約上のセキュリティ義務を遵守します。

3.情報セキュリティマネジメントシステムの運用をあらゆるリスクから保護するために現在の管理策を定期的に見直します。

制定：平成27年3月26日
改訂：平成27年6月10日
株式会社テクノエージェント
代表取締役社長
角屋　守保



個人情報保護方針
Privacy Policy

株式会社テクノエージェントは、システムインテグレーション事業・BPOサービス事業・ITエンジニア派遣事業を実施する上で、お客様の個人情報がプライバシーを構成する重要な情報であることを深く認識し、業務において個人情報を取り扱う場合には、個人情報に関する法令及び個人情報保護のために定めた社内規定を定め、また、組織体制を整備し、個人情報の適切な保護に努めることにより、お客様を尊重し、当社に対する期待と信頼に応えていきます。

法令・規範の遵守
私たちは、個人情報に関する法令、国が定める指針その他の規範及び社会秩序を遵守し、個人情報の適切な保護に努めます。

個人情報の取得、利用、提供
私たちは、事業活動の範囲内で個人情報の利用目的を特定し、その目的達成のために必要な限度で公正かつ適正に個人情報の取得、利用及び提供を行います。
また、取得した個人情報の目的外利用をしないよう措置を講じます。

個人情報の適切な管理
私たちは、私たちが取り扱う個人情報について、不正アクセス、紛失、破壊、改ざん、漏えいなどの危険を十分に認識し、合理的な安全対策を実施するとともに、問題が発生した場合は適切な是正措置を講じます。

継続的改善
私たちは、個人情報保護に関する管理規定及び管理体制を整備し、全社員で徹底して運用するとともに定期的な見直しを行い、継続的な改善に努めます。

問い合わせへの対応
私たちは、私たちが取り扱う個人情報について、苦情相談等のお問い合わせがあった場合は適正に対応します。

平成27年1月 6日　制定
平成27年6月10日　改訂

株式会社テクノエージェント

参照：https://technoagent.co.jp/

✎ISMSやPマークのルールに違反した際に予想される結果💀

社会的な信用の失墜

- 顧客や取引先の信用を失う
- 企業ブランドのイメージダウン

経済的な損失

- 再発防止策への投資
- 本人への補償
- 業務の停止（営業機会の損失）
- 信用回復の投資

事業継続へのダメージ

- 株価の下落
- 取引の減少
- 経営状況の悪化

従業員が違反した場合

- 減給
- 罰金
- 解雇

※自社の罰則に関する規程に準ずる

✎直近で発生した実際の個人情報の事故事例を見てみましょう

事例 ①

なりすましメールによる個人情報漏洩事件

A社従業員のメールアドレス宛に、A社社長よりメールを受信しました。
内容を確認すると「今日は出社していますか？」という確認メールでした。
その日、社長は出社していなかったため、確認したいことがあるのだろうと、送信元のアドレスを確認せず、出社している旨をメールで返信しました。
やり取りを重ねていくうちに、「うちの会社の銀行口座の番号を教えてほしい。」と連絡があったため、取り急ぎそのメールに口座番号を記載し、送信してしまいました。
翌日、社長が出社した際、そのようなメールは送っていないことが発覚し、個人情報や口座番号の漏洩事件となりました。

■漏洩した個人情報
会社名、担当者名、連絡先、口座番号など

■原因
従業員のメールアドレスの漏洩、送信先の確認漏れ

■今後の対策
・取引明細の確認、暗証番号の変更(一時的対応)
・送信元のアドレスの確認、ダブルチェック
・メールで会社の機密情報は送らない

✎直近で発生した実際の個人情報の事故事例を見てみましょう

事例 ②

退職した従業員が顧客リストを不正に持ち出し

2025年8月、A社を退職した社員が、A社の顧客リストを不正に持ち出し、営業活動を行っていました。
事態が発覚後、A社代表は退職した社員に対し、訴訟を起こしました。
※A社勝訴

■漏洩した個人情報
A社で管理しているすべての顧客分のリスト

■原因
顧客リスト閲覧権限者の管理不足：全員が閲覧できるスプレッドシートにて管理しており、
スプレッドシートのURLをコピペすると、誰でも
持ち出せる状態にしていた。

■今後の対策
・閲覧権限者の棚卸
・必要最低限の従業員への展開
・入退職時の誓約書にて同意を交わす

✎2025年以降の傾向

脅威はより巧妙に、被害はより甚大に

不注意誤送信　　高度な攻撃　　内部不正

単なる不注意（メール誤送信）よりも、高度なサイバー攻撃や内部不正による被害額・影響範囲が急速に拡大しています。いまや「自分には関係ない」と言える時代ではありません。

✎情報資産や個人情報を守るためにできること

ちょっとの気の緩み、これくらいならいいか…　から事故は発生します。
この教育を機会に、実際に下記の項目が守れているか確認してみましょう。

事務所編

☑一番最初に事務所についた人、最終退出者は時間等の記録を残しているか？
☑来訪者が事務所に入る場合は「来訪者記録」を書いてもらっているか？
☑印刷したものは複合機に置いたままにせずに、すぐ回収しているか？
☑クリアデスクになっているか、名刺などを机に置いたまま離席していないか？
☑デスクに個人情報やPCのパスワードなど付箋が貼ってないか？
☑個人情報が記載されている紙をシュレッダーにかけ、廃棄しているか？

PC編

☑PCのパスワードは英数含む8桁以上か？
☑スクリーンセーバーは10分以内で設定されているか？
☑ウイルス対策ソフトが入っているか？
☑OSのアップデートは最新または会社から指示されているバージョンか？
☑業務に使わない、不要なアプリがダウンロードされていないか？
☑個人情報が保存されたPCなどは許可なく社外への持ち出しをしていないか？
☑許可なくPC、USBメモリを家に持ち帰っていないか？

✎情報資産や個人情報を漏洩しないためにできること　～報告･連絡･相談～

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・連絡・相談を行うことで、本当に起きてはならないような、大きな漏洩事故を未然に防ぐことに繋がります。

💡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、送信前に気づくことができた。

・電車を降りる時にノートPCを置き忘れそうになった。

・個人情報の書かれた紙の裏を使った後、ゴミ箱に捨ててしまいそうだった。

・メールを送る時のBCC欄とCC欄を間違えて送りそうになっていた。

✎まとめ

・他人事ではなく、皆さんがお仕事される中で、**一人一人の会社の定めたルールを守ろうという意識が、漏洩事故を防ぐ**ことになります。

・何か疑問や、少しでも不安・怪しいと感じた事象があれば、そのままにするのではなく**すぐに上司に報告**をするようにしましょう。

1.ISMSとは？
情報セキュリティにおけるルールのことです。

2.個人情報とは？
生存する個人に関する情報で、
特定の個人を「識別できる」ものです。

3. 情報資産取り扱いによるリスク
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

4.あなたにできることは？
規則を守る事
危ないと思ったら報告、連絡、相談する事