※同封の「解答用紙」に解答いただき、「解答用紙」のみ年末調整書類と一緒に返送してください。

テクノウェイブでは「Pマーク」及び「ISMS」の認証を取得しており、最低年一回の社員教育を制定しております。つきましては、スタッフの皆様におかれましても本テキストによる教育へのご協力をお願いいたします。（テキスト確認後、**同封の「解答用紙」に解答お願いします。**）

Web でも受講できます。
Web で受講いただいた場合は同封の解答用紙の返送は必要ありません。

2026 年度・個人情報保護・情報セキュリティ教育テキスト

近年、デジタル化の進展や生成AIの普及により、業務効率化が進む一方で、情報漏えいリスクも高まっています。特に近年増加しているのが、

- **ランサムウェア攻撃**
- **フィッシングメール**
- **標的型メール攻撃**
- **クラウドサービスの設定不備による情報漏えい**
- **SNS投稿による機密情報の拡散**
- **生成AIへの機密情報入力による情報漏えい**

といった事例です。サイバー攻撃は大企業だけでなく、中小企業や派遣社員を含む個人も標的となっています。また、情報漏えいの原因は外部攻撃だけではありません。

- **メールの誤送信**
- **書類やPCの置き忘れ**
- **パスワード管理の不備**
- **業務ルールの未確認**
- **SNSへの不用意な投稿**

など人為的ミスによる事故も多く発生しています。情報漏えいは、会社だけでなくお客様や取引先にも大きな影響を与えます。その結果、多額の損害賠償や社会的信用の失墜につながる可能性があります。情報セキュリティを守る最後の砦は、一人ひとりの行動です。「自分は大丈夫」と考えるのではなく、**「自分の行動が会社やお客様を守る」**という意識を持って日常業務に取り組みましょう。このテキストでは、改めて「個人情報保護」と「情報セキュリティ」の基本を確認し、安全な業務遂行のために必要な知識とルールについて学んでいただきます。

① 個人情報とは

知っているようで、よくわかっていないなんてことはありませんか？

氏名、住所、電話番号、メールアドレス、社員番号、給与明細、お客様情報、写真、映像、音声、名刺等・・・これらの情報を、単独あるいは組み合わせる事で特定の個人を識別できるものです。もちろん、個人を識別できるDNAや指紋等の身体の一部の特徴情報、マイナンバー等の公的な番号も個人情報です。また、人種・信条・病歴・障害の有無・前科等は要配慮個人情報となり特に慎重な取り扱いが必要です。

② 個人情報保護法

個人情報を正しく扱わなければならないという法律があります。

2005年4月から「個人情報の保護に関する法律」が施行されています。また、2017年5月に「改正個人情報保護法」が施行され、更に情報の取り扱いには注意が必要です。この法律は会社等を対象とした法律ではありますが、事件や事故を起こした当人に対し、結果として損害賠償を請求されるということもありえます。個人情報は「知る必要のある人だけが利用する」という原則を徹底してください。

③ 就業先企業のルールを守ること

当たり前のことですが、とても大事なことです。

就業先によって異なりますが、就業先のルール(社風、服務規程、慣行、その他規程)を守らなければなりません。個人情報や情報全般の取扱いについても、就業先のセキュリティルールに従ってください。

④ 守秘義務

派遣の場合は更に重視されます。

仕事をするうえで知った情報を外部に漏らしてはなりません。また、就業期間が終了した後も同様です。

- 書類やUSBメモリ等記録媒体、モバイル機器等を勝手に持ち出さない。
- 机を離れるときや、退社するときは、書類などを出したままにしない。パソコンの画面も情報を表示したままにしない。
- 仕事で使った書類や記録媒体などは、もとの場所に戻す。不要なものは規定に従いシュレッダー等で破棄。
- 仕事上知った機密情報等を他人に漏らさない。
- **会社情報（会社での出来事、写真等を含む）を勝手に個人の SNS 等にアップしない。**

⑤ 常に漏洩への注意

「しゃべる情報」も重要な情報です。

仕事をする上で知った個人情報や機密情報を社外の人に口外したり、仕事以外の目的に利用してはいけません。特に、酒席での会話や喫煙場所での会話は要注意です。また、ビルのロビー、駅や電車内等公共の場でも同様の注意が必要です。

⑥ 紛失への注意

どんな状況でも危機管理意識の低下から紛失は起こります。

ノート PC やタブレット等モバイル機器の利用の増加に伴い、**紛失によるセキュリティ事故は年々増加傾向にあります。**忙しい時、集中している時、リラックスしている時、どんな状況でも紛失は起こり得ます。普段から危機管理の意識を高く保つように注意を怠らないでください。不安な場合はスマートフォンをストラップで身体につなぐ等の物理的な対策をして紛失を防ぐことも必要です。

特に飲みの席及びその帰路では注意が必要です。できるだけ情報は持ち歩かないことも重要です。

また、**紛失してしまった時は速やかに就業先のルールに従い関係各所へ連絡し、弊社の担当営業へも連絡してください。**

⑦ 保管・整頓

整理・整頓は仕事のキホンです。

就業先で仕事をする時は常に整理・整頓に心掛けましょう。書類や記録媒体等は就業先でそれぞれ保管場所が決まっているので就業先の責任者もしくは担当者に確認し、必ずそのルールに従い保管して下さい。

（例）「利用後は所定のキャビネットに保管して施錠する。

裏へ続く

⑧ PC の取扱い　　パソコンの取り扱いで被害が拡大します。

就業先の管理規程や運用規程に従い、管理を徹底して下さい。

- 利用しているパソコンから席を外す場合は画面のロック、また長時間席を外す時はログオフ又は電源を切ってなりすましによる利用を防ぐ。
- 就業先からパスワードが与えられた場合、絶対他人に教えない。
- パソコンから出力した書類は、速やかに回収し長時間放置しない。
- インターネット接続は、私的な目的に利用しない。
- 許可されていないソフトウェアを無断でインストールしない。
- 私有のノートパソコン等を無断で持ち込み、利用しない。業務上やむを得ず持ち込む時は、就業先の責任者もしくは担当者に確認し、承認を得る。
- Winny 等のファイル共有ソフトは情報漏洩の危険性がかなり高いので、職場や自宅に関わらず絶対使用しない。

⑨ 携帯電話（スマートフォン）の取扱い　　携帯電話(スマートフォン)は機密情報や個人情報が一杯です。

会社から貸与された携帯電話の取り扱いは会社の管理規程に従ってください。私有の携帯電話には許可がない限り、業務関わる情報を登録してはいけません。また、私有の携帯電話を業務で使用する事も原則禁止です。やむを得ず許可を得て使用した場合も、使用後直ちに発信記録・着信記録を消去して下さい。

⑩ 外部との通信について　　情報漏洩事故で一番多い原因です。

就業先から、業務用メールアドレスが与えられている場合、私的利用は厳禁です。業務での使用は就業先での管理規程や運用規程に従って下さい。重要な情報ではないと思っても、漏らしていけない機密情報である場合があります。

- 受信したメールの添付ファイルは必ず信頼のおける相手からのメールであることを確認した上で開封するようにしてく ださい。近年、取引先だと思わせる件名で確認をおろそかにさせる迷惑メールも増えています。本文内のURLリンクも同様です。
- 個人情報や企業情報等の機密情報をメールで送る時は、就業先の添付ファイルの取り扱い等のルールに従い、必要に応じて就業先の責任者あるいは担当者に確認し、判断を仰いで下さい。
- メールや FAX を送信する場合、**送信前に必ず宛先を確認**し、誤送信が無いように注意して下さい。
- 電話で社外あるいは社内から個人情報や機密情報の問合せがあった場合は、自分で判断せずに、必ず就業先の責任者あるいは担当者に判断を仰いで下さい。

⑪ オンライン（クラウド）サービス利用の注意　　オンライン＝漏洩リスクがあることを常に意識してください。

Googledrive や OneDrive、iCloud、Dropbox、GitHub 等、ファイル保存・共有系のオンラインサービスもよく問題になっています。とても便利ですが、使い方を間違えると大きなセキュリティ事故に発展する恐れがあります。基本的には客先が用意したサービス以外は利用しないようにしてください。勝手な業務利用はせず、必ず現場の責任者に相談してください。

⑫ SNS・動画配信系サービスの業務利用の注意　　本当にその情報はアップしてもいいの？！

LINE、X（旧 Twitter）、Facebook、Instagram、TikTok、Pinterest 等のSNS系サービスや、YouTubeやニコニコ動画等の 動画配信系サービスの利用についても細心の注意を払う必要があります。プライベートの個人アカウントに業務に関わる情報を無断で安易にアップしないようにしてください。派遣先が業務用に用意したサービス以外は利用しないでください。

⑬ 廃棄する情報について　　捨てたゴミからも情報漏洩します。

個人情報や企業情報等機密情報が記載された書類や記録媒体はそのままゴミ箱に捨ててはいけません。記載された文字などが読めなくなる様に処理を行う必要があります。具体的には、書類はシュレッダーによる裁断や焼却処分となりますが、詳しくは就業先の責任者もしくは担当者に確認し、ルールに従ってください。

⑭ セキュリティカード（入館証・ID カード等）の取り扱いについて　　とても重要な責務です。

セキュリティカードを就業先で貸与された場合は、責任をもって所持・管理し、業務終了後には速やかに返却してください。
紛失した場合は大きなペナルティが発生するとともに、派遣先及び就業先を含め多くの方に大変な迷惑をかけることとなりますので、取り扱いには十分注意してください。
「気付かないうちに ID カードがホルダーから落ちていた」といった報告も多く、ホルダーからIDカードが落ちないようにしっかり管理し、落ちやすいホルダーの場合は交換するか、テープ等で止める等落ちないように工夫して紛失を防いでください。
また、飲みの席や移動中は特に注意し、他人に預けたり網棚に乗せたりせず、身体から離さないように管理してください。
万が一紛失してしまった場合は“速やか”に派遣先・就業先のルールに従い報告すること。同時に弊社担当者へも連絡をして指示に従い適切に行動してください。

⑮ 生成AI利用時の注意

ChatGPT、Copilotなどの生成AIサービスは便利な反面、利用方法を誤ると重大な情報漏えい事故につながります。

注意事項

- 顧客情報や個人情報を入力しない
- 機密情報や社外秘情報を入力しない
- 開発ソースコードや設計資料を無断で入力しない
- AIの回答をそのまま信用せず必ず確認する
- 就業先が定める生成AI利用ルールに従う

生成AIは業務を支援するツールであり、情報管理の責任は利用者自身にあります。