教習所事業者情報セキュリティ規程

この規程は、教習所事業者　山晃有限会社（以下「教習所事業者」という。）が、その事業活動を通じ情報セキュリティを確保するために必要な事項を定めるものとする。

第 1 章　基本的対策

（脆弱性対策）

第 1 条　OS やソフトウェアを古いまま放置していると、セキュリティ上の問題点が解決されず、それを悪用したウイルスに感染してしまう危険性があることから、使用する OS やソフトウェアは、修正プログラムを適用する、又は最新版を使用するなどして、常に最新の状態にする。

（ウイルス対策）

第 2 条　ID・パスワードを盗んだり、遠隔操作を行ったり、ファイルを勝手に暗号化するウイルスが増えていることから、ウイルス対策ソフトを導入し、ウイルス定義ファイル（注 1）は常に最新の状態になるようにする。

（注 1）　コンピュータウイルスを検出するためのデータベースファイル。「パターンファイル」とも呼ばれる。

（パスワード管理）

第 3 条　パスワードが推測や解析されたり、ウェブサービスから流出した ID・パスワードが悪用されたりすることで、不正にログインされる被害が増えていることから、パスワードは、英数字記号を含めて 10 文字以上にするなど長く、複雑にして、また、使い回さないようにして強化する。

（機器の設定）

第 4 条　データ保管などのウェブサービスやネットワーク接続した複合機の設定を間違ったために、無関係な人に情報を覗き見られるトラブルが増えていることから、無関係な人が、ウェブサービスや機器を使うことができるような設定になっていないことを確認する。

（情報収集）

第 5 条　取引先や関係者と偽ってウイルス付のメールを送ってきたり、正規のウェブサイトに似せた偽サイトを立ち上げて ID・パスワードを盗もうとする巧妙な手口が増えていることから、脅威や攻撃の手口を知って対策をとる。

第 2 章　従業員としての対策

（電子メールのルール 1）

第 6 条　電子メールに添付されたファイルを開いたり、電子メール本文中に記載された URL リンクをクリックしたりすることでウイルス感染する事故が続いていることから、身に覚えのない電子メールの添付ファイルや URL リンクへのアクセスに気をつける。

（電子メールのルール 2）

第 7 条　電子メールや FAX の送り先を間違えて、他人に情報が漏えいしてしまう事故が続いていることから、電子メールや FAX は送り先を十分に確認するようにする。また、電子メールアドレスを誤って他人に伝えてしまうことも情報漏えいになることから、複数の送り先に送信する際には、送り先の指定方法を十分に確認する。

（電子メールのルール 3）

第 8 条　重要情報（注 2）を電子メールで送る場合は、電子メールの本文に書き込まず、文書ファイルなどに記載してパスワードで保護した後、メールに添付する。パスワードはその電子メールには書き込まず、電子メール以外の手段で通知する。

（注 2）　重要情報とは、営業秘密など事業に必要で組織にとって価値のある情報や、顧客や従業員の個人情報など管理責任を負う情報のことをいう。

（無線 LAN のルール）

第 9 条　適切なセキュリティ設定がされていない無線 LAN は、通信内容を読み取られたり、不正に接続されて犯罪行為に悪用されたりする被害を受ける可能性があることから、無線 LAN の盗聴や無断使用を防止するようにセキュリティ設定をする。

（インターネット利用のルール）

第 10 条　悪意あるウェブサイトやセキュリティ上の問題があるウェブサイトを閲覧することでウイルス感染する可能性がある。また、SNS や掲示板へ悪ふざけした画像を投稿したり、秘密情報を勝手に掲載して、教習所事業者に被害を及ぼすことがある。業務でのインターネット利用を制限する仕組みやルールにより、被害を防止する。

（バックアップのルール）

第 11 条　故障や誤操作、ウイルス感染などにより、パソコンやサーバーの中に保存したデータが消えてしまうことがある。このような不測の事態に備えて、バックアップを取得しておく。

（保管のルール）

第 12 条　机の上に放置された情報は、誰かに持ち去られたり、盗み見られたりする危険にさらされている。関係者以外が見たり、触れたりすることができないように、重要情報は放置せず、管理する必要があることから、保管場所を定め、作業に必要な場合のみ持ち出し、終了後に戻すことを励行する。

（持ち出しのルール）

第 13 条　重要情報を社外へ持ち出す場合、思わぬ盗難にあったり、うっかり紛失したりすることがある。ノートパソコンやスマートフォンの利用にあたってパスワードの入力を求めるように設定したり、データファイルを暗号化するなどの対策を事前に行うことで、盗難や紛失の際に情報を簡単に読み取られることができないようにする。

（事務所の安全管理 1）

第 14 条　パソコンを使用した作業の途中でそのまま席を離れたり、パスワードなしでログインできるパソコンなど、誰でも操作できる状態のパソコンは、不正に使用される可能性があることから、不正使用からパソコンを守るための対策を行う。

（事務所の安全管理 2）

第 15 条　関係者以外の事務所への立ち入りを制限しなければ侵入されてしまい、情報を盗み取られる危険性がある。特にサーバーや書庫・金庫など、重要な情報の保管場所の近くには無断で立ち入りができないようにする。

（事務所の安全管理 3）

第 16 条　ノートパソコンやタブレット端末、USB メモリなどは、手軽に持ち運べる便利さがある反面、盗難や紛失の危険性も高くなっていることから、利用しない場合は、施錠可能な引き出し等に保管するなどの対策を講じる。

（事務所の安全管理 4）

第 17 条　最終退出者と退出時間の記録を残すことは、最終退出者による施錠の責任意識を向上させることにも役立つことから、施錠と退出記録の管理をする。

（情報の安全な処分）

第 18 条　重要情報が記載された書類をゴミ箱にそのまま捨てると、関係者以外の目に触れてしまい、重大な漏えい事故を引き起こすことがある。また、電子機器・電子媒体に保存された情報は、ファイル削除の操作をしても復元されるおそれがある。重要情報を廃棄する場合は、シュレッダーや消去用ソフトウェアを利用するなど、媒体ごとに適切な処分をする。

第 3 章　組織としての対策

（守秘義務の周知）

第 19 条　就業規則などで定める従業員の守秘義務や機密保持について、どのような情報が秘密なのか、何をしたらいけないのかなどを、従業員に明確に説明する。

（従業員教育）

第 20 条　日々の仕事では常に様々な情報を取り扱うが、日常的であるがゆえに管理の意識がつい疎かになりがちであることから、従業員に対し繰り返し意識付けを行う。

（私物機器の利用）

第 21 条　個人所有のパソコンやスマートフォンを業務で使用する場合、管理が行き届かず、セキュリティの確保が難しくなることから、個人所有端末の業務利用の可否や業務利用のルールを定める。

（取引先管理）

第 22 条　取引先が情報の内容から判断して「当然秘密にしてくれるだろう」という一方的な期待は禁物であり、取引先に機密情報を提供する場合には、それを機密として取り扱ってもらうことを明確にする。

（外部サービスの利用）

第 23 条　クラウドサービスなど外部サービスをコスト優先で選んでしまうと、障害等でサービスが利用できなくなっても、補償を受けられない場合もあることから、外部サービスを利用する場合は、性能や信頼性、補償内容など十分に吟味する。

（事故への備え）

第 24 条　実際に事故が起きてからだと、冷静に対応する余裕がなくなってしまう。また、対応が後手に回り、それが原因でさらに深刻な事態になりがちである。報道されるセキュリティ事故などを参考に、「もし、同じことが自分の会社で起きたら…」を想定して、誰がいつ何をするのかをまとめておく。

附　則

（施行期日）

第 1 条　この規程は、令和４年１０月１日から施行する。