１０．情報セキュリティ対策ガイドライン

（1）趣旨

静岡産業技術専門学校（以下「本校」という。）の建学の精神を継承し、高度に情報化する社会における教育機関としての使命を果たし続けていくためには、コンピュータやネットワークなどで構成される情報処理環境を安全に利用し、それらを活用して情報を安全かつ的確に取り扱うことが不可欠です。情報通信技術の進展は早く、サイバー攻撃に代表される情報セキュリティの脅威が多様化し巧妙化する中で、本校の学生においては情報セキュリティに関する知識を有し、かつ組織的に統制のとれた対応方法を身につけることが必要不可欠です。

情報セキュリティの確保に向けて、学生のみなさん全員が統一したルールで情報セキュリティリスクを未然に防ぎ、やむを得ず情報セキュリティインシデントが発生した場合の損害を最小に抑え、セキュリティ対策を環境に合わせて改善していくことへの理解を趣旨とするものです。

本校におけるネットワークや共有サーバー、就活サイトなどの情報資産を利用する学生は、情報セキュリティの重要性を十分に認知し、これをを遵守しなければなりません。

（2）社会的動向（法令遵守）

１）個人情報保護

個人情報とは、当該情報に含まれる内容によって、個人が誰かを識別することができる情報のことを指します。個人情報保護法では、①個人情報の利用目的の明確化および目的外利用の制限、②個人情報の適正な取得と利用目的の通知、③個人情報のデータ内容の正確性の確保と安全管理措置、④従業者、委託先の監督および第三者提供の制限、⑤本人からの求めに応じた個人情報の開示、訂正、利用停止等について定められています。

２）著作権

授業内の利用であれば、著作権者の許諾なしで著作物を利用可能と思われがちですが、利用可能な範囲には制限があり、著作権者の利益を不当に害するような利用は認められていません。特にインターネット経由でコンテンツを配信する場合は、たとえ授業内であっても、特別な条件を満たさない限り、著作権者の許諾なしに著作物を利用することはできません。

２０１０年１月１日施行の改正著作権法において、違法にアップロードされた音楽・映像といったコンテンツを、それと知りながらダウンロードする行為自体も違法となりました。また２０１２年の改正では、違法ダウンロードに対する刑事罰が規定され、「２年以下の懲役もしくは２００万円以下の罰金」あるいはこの両方が科されることとなりました。

３）ソフトウェアの不正利用

学生が授業にて利用するソフトウェアは、すべて著作権や利用する上で遵守しなければならない使用許諾契約書が定められており、ソフトウェアを利用するすべての人には「 必ず正規品を購入し、正しく使用する 」という責任があります。ソフトウェアの不正利用は「犯罪行為」です。 個人個人がソフトウェアライセンスに関する知識と意識を深め、不正利用をしないよう、また、不正利用に加担することがないように十分注意する必要があります。

ソフトウェアの違法コピーにより、著作権を侵害する行為に対して刑事罰が規定され、「１０年以下の懲役もしくは１，０００万円以下の罰金」あるいはこの両方が科されることとなりました。

４）コンピュータウィルス感染の防止

コンピュータウィルスは、電子メールの受信（添付ファイルの開封）やホームページの閲覧（ダウンロード）、またUSBメモリなどの記憶媒体など様々な経路から感染する可能性があります。また、コンピュータウィルスに

感染すると、コンピュータシステムを破壊するものもあれば、他のコンピュータに感染を拡大したり、コンピュータにバックドアと呼ばれる不正な侵入口が仕掛けられて、パソコン内の情報が抜き出されたりすることがあります。さらに、オンラインゲームなどのソフトウェアに見られる表の動作の裏側でボットと呼ばれるプログラムがサイバー攻撃に加担し、あなたが被害者ではなく加害者になるような場合もあります。

（3）遵守事項

1）学内ネットワークの利用

個人アカウント（パスワード）は、自己責任において厳重に管理すること。また、これを他人に提供することはしないこと。また、コンピュータウィルスの感染により、感染したパソコンのみならず、他人のパソコンや学内その他の情報資産の可用性や完全性を損なうことを防止するため、コンピュータウィルスに感染することを予防しなければなりません。さらに、感染時の被害を最小化するための対応を実施しなければなりません。

2）ノートパソコンのセキュリティ対策

学内に持ち込む個人ノートパソコンには、コンピュータウィルス感染を防ぐために、本校で決められた指定のウィルス対策ソフトウェアを導入し常時動作しなければなりません。さらに、新種のウィルスに対応するために、ウィルス定義ファイルを常に最新の状態にアップデートするようにし、基本ソフト（OS）やその他ソフトウェアの更新プログラムの適用（セキュリティアップデート）も必要です。

3）ソフトウェアの利用

インターネットからソフトウェアをダウンロードしてインストールする場合には、ウィルス感染やスパイウェアによる情報漏えいの危険性に配慮する必要があります。また、実習室に常設されているパソコンや貸出用ノートパソコンに、私的利用ソフトウェアをインストールしないこと。さらに、正規に購入したソフトウェアの利用に対しては、予め決められたライセンスの範囲で利用すること。

（4）制限事項

情報セキュリティ確保のため、次の行為を禁止する。

1）インターネットサイトからの違法な音楽や映像といった著作物をダウンロードすること。

2）Webサイトなどインターネット上で見つけた他人の著作物を、自分の課題レポートや作品などに出所を明示しないで転用提出すること（このような行為は剽窃（盗用）にあたり著作権法に抵触します）。

3）電子メールにおいて添付ファイルをむやみにダブルクリックしない（開かない）。

送信元が出所不明であればもちろんのこと、知人からのメールであってもウィルス感染の危険があります。添付ファイルは必ずウィルス感染の検査を行ってから開くようにすること。

4）購入したソフトウェアを使用許諾範囲外の複数のPCにインストール利用しない。

下記のソフトウェア利用も違法行為となります。

ア）１ライセンスしかなく、すでに他のPCで利用しているソフトウェアを一時的に別のPCにインストールした。

イ）海賊版ソフトウェアを海賊版と承知した上でダウンロード（または購入）して利用した。

ウ）インターネットやファイル共有ソフトを通じて、他人が著作権を有するソフトウェアをダウンロードした。

エ）ファイル共有ソフト所定の共有フォルダやファイルサーバーに保存し、ファイル送信可能な状態にした。

5）Twitter、Facebook、LINEなどのソーシャルメディアに不適切な情報発信をしない。

個人アカウントによる私的利用であっても、インターネットでは不特定多数の利用者がアクセスでき、一旦発信した情報は拡散し削除することはできません。

（5）懲戒

上記事項に違反した学生は、本校学則第３７条に従って処分を受けることがあります。