椙山女学園パソコン等利用ガイドライン

平成１９年１０月２６日制定

（趣旨）

第１条　このガイドラインは、学校法人椙山女学園（以下「学園」という。）の個人情報を含む重要な電子情報を取り扱うパソコン（以下「PC」という。）及び電子情報媒体（以下「情報媒体」という。）の利用において、情報の安全管理を図るため、重要度に応じた取扱いを定めるものとする。

（用語の定義）

第２条　このガイドラインにおいて、次の各号に掲げる用語の意義は、当該各号に定めるところによる。

(1)　PC 等とは、デスクトップ型 PC、ノート型 PC、PDA、携帯電話等の情報機器をいい、学園の所有するものであるか否かは問わない。

(2)　利用者とは、PC 等及び情報媒体を利用して、学園の情報を取り扱う学園の構成員をいう。

(3)　情報記憶媒体とは、ハードディスク（HDD：内蔵型、外付型及び携帯型を含む。）、フロッピーディスク、CD、DVD、MO、ＵＳＢメモリ、メモリカード、磁気テープ等情報の書き込み、再生及び読み取りの可能なすべての電磁的、光学的記憶媒体で、学園の所有するものであるか否かは問わない。

(4)　情報通信媒体とは、電子メール、電子ニュース、Web システムなどのインターネットやサーバ等を使用する通信手段をいう。

(5)　情報媒体とは、情報記憶媒体及び情報通信媒体をいう。

(6)　ウイルス等とは、メッセージの表示、ファイルの破壊、重要情報の漏えい等を実行する機能を持った不正なコンピュータプログラムをいう。

(7)　完全消去とは、電子データを復元不可能な状態にして、二度と利用できない状態にすることをいう。

(8)　ファイル交換ソフトとは、Winny 等に代表されるネットワークを介して不特定多数のコンピュータの間で匿名性を確保しつつファイルを交換するソフトをいう。

(9)　保存とは、利用者が、情報を PC 等及び情報記憶媒体に記憶させること（プログラムの動作に伴う自動記憶は含まない。）をいう。

(10)　保管とは、情報を保存した PC 等及び情報記憶媒体を保持して管理することをいう。

（適用範囲）

第３条　椙山女学園電子情報資産区分ガイドライン第２条に規定する機密性レベル２以上の情報を扱うすべての PC 等及び情報媒体の利用行為を適用範囲とする。サーバについては、別に定める。

（組織体制）

第４条　情報を取り扱う PC 等及び情報媒体のセキュリティに関する責任者は、各部門の電子情報セキュリティ管理者（以下「管理者」という。）とする。

（事故発生時の対応）

第５条　利用者は、PC 等及び情報記憶媒体の紛失、盗難、第三者による不正使用並びに情報通信媒体の第三者による不正使用が発覚した場合、管理者に速やかに報告し、事故対応を行う。

２　管理者は、利用者に対応措置を指示するとともに、必要な場合は電子情報セキュリティ管理責任者に報告する。

（PC 等利用遵守事項）

第６条　利用者は、情報を取り扱う PC 等に関し次の各号に掲げる事項を遵守して管理し、同事項が遵守されていない、又は遵守されているかどうか不確かな PC 等（例えば、他の者の管理する PC 等、インターネットカフェ等で不特定の者が利用する PC 等）では、情報を取り扱ってはならない。

(1)　パスワードによる管理

ア　パスワードは、最低６桁以上の桁数（８桁以上が望ましい。）で､アルファベット、数字又は記号を２種類以上組み合わせ、推測されにくいものとし、定期的に更新するよう十分注意を払う。

　また、取り扱う情報の機密性レベルに応じて、機密性レベル３以上の情報を保存するファイルの暗号化に使用するパスワードは、定期的に変更し、機密性レベル４以上の場合は、他と異なるパスワードを使用し、８桁以上でアルファベット、数字及び記号の３種類を含む組合せで、推測されにくいものとする。

イ　パスワードは、それが保護する情報と等しい程度の重要性があることを認識し、重要度、使用場面

等を考慮して使い分ける。

ウ　パスワードは、他の者の耳目に触れることを避け、初期パスワードのように他の者があらかじめ知っている場合、他の者に知られた場合又は知られた可能性がある場合は、速やかにそのパスワードを変更する。

エ　パスワードに使用する文字列については、ユーザ ID と共通する文字列、自己及び身近な者の名前、電話番号、誕生日等の類推されやすい文字列、辞書に掲載されている単語、映画、テレビ、漫画、小説等に登場する固有名詞、キーボードのキー配列及びこれらと単純な数字との組合せによる文字列を使用しない。

オ　パスワードは、パスワードを保存できるシステムであっても、特別に認められたものを除き、保存しないように注意を払う。

(2)　クリアスクリーンによる管理

ア　離席時は、コンピュータのロック又はログオフを行い、不正な操作又は画面の盗み見を防止する。画面設定では、１５分以上放置するとパスワード付きスクリーンセーバが動作するように設定する。

イ　可搬な PC 等（ノート型 PC、PDA 等）を帯出して使用する場合は、第三者から盗み見が可能な環境では使用しない。

ウ　作業終了時は、使用した PC 等の電源をオフにする、又は利用再開時にパスワード等の認証が必要とされる状態に移行させる。

(3)　可搬な PC 等の保管

可搬な PC 等については、個室、ロッカー、引出し等の施錠可能な設備での施錠保管、盗難防止ワイヤー等での固定保管等、盗難対策を施す。

(4)　アカウントによる他の者の利用の制限

アカウント及びパスワードの設定を行い、他の者（学園構成員、家族等を含む。）に無断で利用されないようにする。また、他の者に利用させる場合は、他の者の管理者権限を有しないアカウントの作成等、適切な制限の下で利用させる。

(5)　インストール禁止のソフトウェア

ファイル交換ソフトウェア等学園がインストールを禁止したソフトウェア（以下「禁止ソフトウェア」という。）をインストールしてはならない。また、定期的に禁止ソフトウェアのリストを確認し、新たに追加された禁止ソフトウェアの有無について確認する。

(6)　時刻合わせ

ア　各種の記録等に利用するため、常に PC 等の時刻は正しく合わせる。

イ　ＰＣ等を学園ネットワークに常時接続する場合は、学園の推奨する時刻サーバに同期する時刻設定を行う。

(7)　携帯電話の取扱い

ア　機密情報を登録する携帯電話は、万が一に備えパスワードロック等の安全対策を施し、盗難又は紛失に十分注意を払う。

イ　盗難又は紛失が発生した場合は、携帯電話会社に直ちに連絡し、不正利用阻止の措置を講ずる。

（ウイルス対策）

第７条　利用者は、次のとおり、ウイルス対策を徹底しなければならない。

(1)　感染防止手順

ア　学園の推奨するウイルス対策ソフトウェアをインストールし、ウイルス対策が有効な状態で利用する。

イ　ネットワーク、情報媒体等により外部から入手するファイルに対しては、自動検知機能（リアルタイムスキャン）を有効にする。

ウ　ウイルス対策ソフトウェアの定義ファイルは、継続的に更新を行う。

エ　オペレーティングシステム等の修正プログラム（Windows Update 等）が頒布されている場合は、適宜これをインストールする。

(2)　ウイルス感染時の対応

ウイルス等の感染を発見した場合、又はウイルス対策ソフトウェアが不正なプログラムの除去・隔離に失敗した場合は、感染した PC 等を直ちにネットワークから物理的に切り離し、速やかに学園情報センターへ報告し、必要に応じて指示を求める。

（情報記憶媒体管理遵守事項）

第８条　利用者は、情報を保存した情報記憶媒体に関し次の各号に掲げる事項を遵守して管理する。

(1)　情報記憶媒体の保管を外部倉庫業者等に委託する場合は、安全管理の要求を十分に満たす業者を選定し、契約を締結した上で実施する。

(2)　情報記憶媒体を持ち運ぶときは、安全な入れ物又は包装を使用し、紛失、盗難、破損等から保護し、パスワードロック、暗号化等の安全策を施す等、十分注意を払う。

（情報通信媒体利用遵守事項）

第９条　利用者は、情報通信媒体に関し次の各号に掲げる事項を遵守して利用する。

(1)　Web 利用時

ア　Web サイトへ個人情報（メールアドレス、氏名、所属等）を入力するときは、通信の暗号化（https://）を確認する等、十分注意を払う。

イ　Web サイトには、ウイルス等を感染させる又はセキュリティ上危険なソフトウエアを実行させるものがあるため、ブラウザのセキュリティレベルを「中」以上に設定する等、その利用には十分注意を払う。

(2)　電子メール利用時

ア　電子メールのアドレスを入力するときは、宛先を十分確認し、送信前には、宛先、ｃｃ、ｂｃｃを必ず確認する。（ｃｃで送信する場合、受信者のアドレスが表示されるため、特に注意が必要。）

イ　機密性レベル４以上の情報を電子メールに添付して送信する場合、添付ファイルを強固な暗号化処理を施す。

（ファイルの暗号化）

第１０条　利用者は、ファイルの暗号化について、次のとおり取り扱う。

(1)　機密性レベル３以上の情報を学園内の施錠保管する場所以外に帯出するときは、帯出の方法によらず、情報保存時にそのファイルの暗号化を行う。

(2)　機密性レベル４以上の情報のファイルの暗号化を行うときは、学園情報センターが推奨するツール等を使用し、復号に必要なパスワードは、８桁以上及びその利用するツールの上限内の桁数で、アルファベット、数字又は記号を含む２種類以上の組合せで推測されにくいものとする。

（PC 等の廃棄等に係る情報消去）

第１１条　機密性レベル２以上の情報については、サーバに保存して利用するよう十分注意を払い、機密性レベル３以上の情報を PC 等に一時的に保存する必要がある場合は、利用後速やかに完全消去する。

２　機密性レベル３以上の情報が、現に保存されている、又は保存されて６ヶ月以内に消去された、若しくは保存されて６ヶ月より前に消去されたがその後稼動していない PC 等を廃棄、返却又は譲渡するときは、次のとおり対応を実施する。

(1)　PC 等の廃棄を行うときは、HDD の情報を完全消去し、又は HDD を物理的に破壊し（後者が望ましい。）管理者に報告する。

(2)　PC 等の返却又は譲渡を行うときは、HDD の情報を完全消去し、管理者に報告する。

(3)　PC 等の廃棄の委託又は返却若しくは譲渡に関し、相手先が HDD の情報の消去を保証している場合であっても、学園は、前２号の報告により完全消去を確認する。

(4)　PC 等の HDD の情報の消去を外部業者等へ委託するときは、守秘義務等の契約を締結した上で実施し、完全消去を保証する文書等の発行を依頼する。

(5)　PC 等の廃棄、返却又は譲渡において、自ら HDD の情報の完全消去が困難な場合は、学園情報センターに支援を要請し、学園情報センターが HDD の情報の完全消去を行う。その際、担当者は、必要最小限の人数で行うこととし、担当者の氏名を利用者に開示するものとする。また、担当者は、情報へのアクセスを必要最小限とし、知り得た情報を公開又は利用してはならない。

（PC 等の修理）

第１２条　機密性レベル３以上の情報が、現に保存されている、又は保存されて６ヶ月以内に消去された、若しくは保存されて６ヶ月より前に消去されたがその後稼動していない PC 等の修理を行うときは、次のとおり対応を実施する。

(1)　PC 等の修理のため外部業者に委託する場合、事前に学園情報センターに相談し、指示を仰ぐ。

(2)　HDD の情報は、必要な部分のバックアップを取った上で完全消去し、修理依頼を行う。

(3)　HDD の修理は、少なくとも守秘義務の契約が行われている業者に依頼し、管理者にこれを報告する。

（情報記憶媒体の保管、移送等）

第１３条　情報記憶媒体は、施錠可能なキャビネット等の設備に施錠保管し、移送及び情報の送信を行う場合は、次の対応を実施する。

(1)　情報記憶媒体の移送は、手渡しで行う、あるいは信頼できる輸送手段及び輸送会社を選定し、委託する。

(2)　情報記憶媒体の輸送を委託する場合は、郵便にあっては、書留郵便を、宅配便等にあっては、重要物運搬便等（集荷から配達までを記録し、紛失又は損失時に一定の保証があるもの）必ず輸送記録が可能なものを利用する。

(3)　輸送中の事故に備え、輸送する情報のバックアップを保管する。

(4)　電子メールで情報を送信する場合は、機密情報は本文中に含めず、そのファイルを暗号化して添付する。この際、復号に必要なパスワードは、別の手段で連絡する。

（情報記憶媒体の廃棄等）

第１４条　機密性レベル３以上の情報が、現に保存されている、又は保存されて６ヶ月以内に消去された、若しくは保存されて６ヶ月より前に消去されたがその後稼動していない情報記憶媒体を廃棄する場合は、情報の完全消去又は情報記憶媒体の破壊若しくは裁断処理を行い、返却又は譲渡する場合は、情報の完全消去を行う。

付　記

このガイドラインは、平成１９年１０月２６日から実施する