Sugiyama
人間になろう

電子情報セキュリティ
ガイドブック
（教職員編）

ガイドブックについて

　この情報セキュリティガイドブックは、個人情報を含む重要な電子情報を取扱うパソコンや情報媒体の利用において、情報の安全管理を図っていただくため作成しました。
　最低限守って欲しいことを中心にまとめていますが、情報の重要度や性質によっては、一層慎重に取扱うことが必要な場合もあります。適切な取扱いによって自身で事故を起こさず、周囲にも起こさせないよう注意しましょう。

　業務に従事する全ての人が情報セキュリティの重要性を強く認識し、社会から信頼される教育研究機関を築いていきましょう。

目次

椙山女学園情報セキュリティポリシー

平成１９年　４月２７日

学校法人椙山女学園（以下「学園」という。）は、「人間になろう」という教育理念の達成や、グローバル情報社会の一員として情報活用を促進するとともに、社会からの厚い信頼に応えるため、学園内外と安全に情報交換できる環境を構築することを目指し、教育研究機関にふさわしい情報セキュリティポリシーをここに策定する。

1. 学園の教育事業運営における情報セキュリティの重要性を正しく認識し、学園の学生生徒等を含む構成員に対して基本的事項の理解及び適切な行動を促すように努める。

2. 学園における情報セキュリティ適用範囲及び境界を定義し、管理対象を明確にすることで、適切な管理体系を構築する。

3. セキュリティ目標を設定する。設定目標は、達成可能なものであり客観的に評価可能なものとする。

4. 学園に、前項の目標を達成するために必要な組織及び規則を整備する。

5. 情報セキュリティ事項を周知徹底するため、学園の職員等に対して適切な研修及び啓発活動を実施する。学生生徒等に対しては、情報セキュリティポリシーの遵守は情報化社会における重要な責務であることを認識するよう、教育及び啓発に努める。

6. 情報セキュリティの適正な運用及び有効性を維持するために、定期的に監査を実施する。

電子情報セキュリティ運営組織

電子情報セキュリティの推進体制は以下のとおりです。

〔運営組織〕電子情報セキュリティ管理者会議

電子情報セキュリティ管理責任者

電子情報セキュリティ管理者

- 事務局
- 学園情報センター企画課

部門		電子情報セキュリティ管理者
事務局	総務部	総務部長
	企画広報部	企画広報部長
	財務管財部	財務管財部長
	学務部	学務部長
総合クリエイティブセンター		企画課長
オープンカレッジセンター		企画課長
学園情報センター		ネットワーク主幹及び企画課長
椙山人間学研究センター		企画課長
食育推進センター		企画課長
歴史文化館		企画課長
大学	研究科	研究科長
	学部	学部長
	入学センター	入学センター長
	図書館	図書館長
	国際交流センター	国際交流センター長
	大学情報教育開発センター	大学情報教育開発センター長
	キャリア育成センター	キャリア育成センター長
	社会連携センター	社会連携センター長
	学生相談室	学生相談室長
	臨床心理相談室	臨床心理相談室長
高等学校		教頭
中学校		教頭
小学校		教頭
幼稚園		教頭
こども園		副園長
保育園		園長

事故の発生や異常に気付いたら

情報セキュリティ事故に関する被害の拡大を食い止めるためには、**速やかな報告**が欠かせません！！
事故の発生や異常の兆候に気付いたら、**学園情報センター及び電子情報セキュリティ管理者**に報告しましょう。

- 見て見ぬ振りはしない！！
- 隠すことが問題を大きくする！！
- 嘘を付かないこと！！
- 正確性よりもスピード重視！！

発見者の対応によって変わる！

報告・連絡する事故等

- コンピュータウイルス等の感染
- データの破壊・改ざん・紛失
- スマートフォン/パソコン等や情報記憶媒体※1の紛失、盗難
- 情報通信媒体※2の不正使用
- 情報（機密性レベル２以上）の紛失、盗難
- 個人情報（教員、職員、学生）の漏えい、紛失、盗難※3
- 情報セキュリティ上、重要と思われること

※１　HD、USBメモリ、CD、DVD、BD等の電磁的・光学的記憶媒体
※２　電子メール、電子ニュース、Webシステム、SNSなど
　　インターネットを介してサーバ等を使用する通信手段
※３　個人情報の拡散など、自身では制御が不可能な場合も含む

<<学園情報センター>>

星が丘キャンパス　メディア棟３階
代表メールアドレス　jyoho@sugiyama-u.ac.jp
TEL　０５２－７８１－１０８８

事故の発生や異常に気付いたら

事故の発生や兆候を発見した時は、表に従い対応しましょう。

<table>
<tr><td colspan="2">被害レベル</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td></tr>
<tr><td colspan="2">最終的に被害がおよぶ範囲</td><td>被害にまでは至らないが被害が発生する可能性があった事象（インシデント）、又は将来において被害が発生する可能性がある事象（兆候）が発見されたとき</td><td>所属内個人の業務遂行に被害が及ぶとき</td><td>所属内の業務遂行に被害が及ぶとき</td><td>学園全体の業務遂行に被害が及ぶとき</td><td>外部に被害が及ぶとき</td></tr>
<tr><td>区分</td><td>連絡先ルート
意味</td><td>構成員
↓
学園情報センター</td><td>構成員
↓
学園情報センター</td><td>構成員
↓
電子情報セキュリティ管理者
学園情報センター</td><td>構成員
↓
電子情報セキュリティ管理者
学園情報センター
↓
電子情報セキュリティ管理責任者</td><td>構成員
↓
電子情報セキュリティ管理者
学園情報センター
↓
電子情報セキュリティ管者責任者</td></tr>
<tr><td>①情報破壊</td><td>情報資産の破壊、破損、喪失</td><td rowspan="7">発見次第、発生の可能性がある被害を学園情報センターへ通知する。</td><td>・原因の特定、応急処置を実行する。
・バックアップによる復旧、又は再作成を実行する。
・原因対策を実施する。
※原因が特定できない場合は、学園情報センターに相談する。</td><td rowspan="2" colspan="2">・発見した事実をできるだけ速やかに電子情報セキュリティ管理者及び学園情報センターに連絡する。</td><td rowspan="2">・発見した事実を即座に電子情報セキュリティ管理者及び学園情報センターに連絡する。</td></tr>
<tr><td>②情報改ざん</td><td>情報資産の意図しない悪影響のある修正、変更</td><td rowspan="2">・原因の特定、応急処置、今後の予防策を実行する。
※原因の特定、応急処置、今後の予防策が不明だったり、個人で実行不可能な場合は、学園情報センターに相談する。</td></tr>
<tr><td>③情報漏洩</td><td>情報資産に対する不正な複製、流出、学外紛失</td><td rowspan="2">・発見した事実をできるだけ速やかに電子情報セキュリティ管理者及び学園情報センターに連絡する。</td><td rowspan="2">・発見した事実を即座に電子情報セキュリティ管理者及び学園情報センターに連絡する。</td></tr>
<tr><td>④不正アクセス</td><td>情報資産への許可されない者のアクセス</td></tr>
<tr><td>⑤ウイルス感染</td><td>ウイルス、ワームなどの悪意のあるソフトウエアの侵入、感染</td><td colspan="3">・ネットワークから切断するため、LANケーブルを抜く、無線LAN（Wi-Fi）をオフにする</td></tr>
<tr><td>⑥サービス停止</td><td>情報資産が必要な時に利用不可になること</td><td>・原因の特定、応急処置、今後の予防策を実行する。
※原因の特定、応急処置、今後の予防策が不明だったり、個人で実行不可能な場合は、学園情報センターに相談する。</td><td>・発見した事実をできるだけ速やかに電子情報セキュリティ管理者及び学園情報センターに連絡する。</td><td>・発見した事実を即座に電子情報セキュリティ管理者及び学園情報センターに連絡する。</td></tr>
</table>

パソコン/スマホ等の利用時に注意すること

パスワード管理

◆適切なパスワード設定

- 学園で使用するパスワードは、12桁以上で推測されにくいパスワードが求められます。アルファベット大文字・小文字・数字・記号の内から3種類以上が必要です。
- 一般的にパスワードは、自分や身近な人の名前、誕生日、電話番号、辞書に載っている単語など推測されやすいものは使用してはいけません。
- 設定可能なら英単語を組合せて30文字程度にしたパスフレーズを定期変更無しで用いるという考え方もあります。

◆適切なパスワード管理

パスワードの取扱いには注意しましょう。

- 他人に教えないようにしましょう。入力は見られないように、他人の入力時は目をそらすなど配慮しましょう。
- 忘れないようにしましょう。メモするときは見える場所に書いてはいけません。
- パスワードを保存（キャッシュ）できるシステムは、自分以外は使用できないパソコン、スマホのみで使用し、第三者に不正利用されないよう注意しましょう。

◆多要素認証を使用しましょう！

- 学園では、Microsoft365のログイン時に、スマートフォンアプリでの認証や送付コードの入力を必須化しています。他システムへも順次拡大予定です。
- 各種アカウントを使用するにあたり、パスワードの漏えい対策として、「なりすまし」「のっとり」を防止できる有効な対策です。

離席時の対応・機器の管理

◆離席時は、ロックやログオフを実施

- パソコンやスマホは、使用していない際に自動的にロックするよう設定しましょう。Windows10は初期設定でスリープし、再開時はパスワードが要求されます。スマホもキーコード、指紋、顔認証を設定しましょう。
- 長時間使用しない場合は電源をオフ、又は再開時にパスワード等の認証を必須にしましょう。
- パソコンやスマホを外出先で使用する場合は、第三者から盗み見されないよう注意しましょう。

◆盗難、紛失に注意

- 学園内で施錠できない部屋のパソコン、ＤＶＤ、ＵＳＢメモリ等は、個室、ロッカー、引き出し等に施錠保管するか、盗難防止ワイヤー等で固定しましょう。
- 機密情報を保存する場合は、万が一の盗難、紛失に備え、ファイルの読取り等に対して、パスワードロック等の対策をしましょう。
- 盗難にあったり、紛失した場合は、スマホの場合は警察以外にも携帯電話会社へ連絡し不正利用阻止の措置を依頼しましょう。
- 万が一に備えて、「端末を探す」設定をしておくことも大切です。過信は禁物ですが遠隔操作で、スマートフォンの位置を特定したり、中のデータを消去できる場合もあります。

他者利用の制限

◆他者による無断利用、および供与の禁止

- 学園構成員や家族、または第三者に無断で利用されないよう、上記の対応をとりましょう。
- 家族共用パソコンの業務利用は避けましょう。
- 研究室や学生が使用するものなど、複数人で利用するパソコン、スマホ等では、管理者権限を有しないアカウントを作成するとともに、個々人のデータについては、パソコン内に保存しないなど適切な運用をしましょう。

パソコン/スマホ等の利用時に注意すること

ソフトウエアの利用について

◆学園が禁止するソフトウエアはインストールしない
- P2Pファイル共有ソフト（Winny、PerfectDark、Share）等は、インストールしてはいけません。

◆正規ライセンスの利用

- コピーされたソフトウェアの使用は禁止です。またソフトウェアを利用する権利の貸与や譲渡を認めていない場合があります。
  ソフトウェアの貸し借りや、パソコンを譲ってもらった場合には気を付けましょう。
- 正規ライセンスがあるソフトウェアであっても、インストールできるパソコンや台数が制限されている場合があります。よく確認の上で違反の無いようにしましょう。

セキュリティ対策

◆セキュリティ被害の防止
- OSやアプリケーションは、アップデートを行い常に最新にしましょう。
- セキュリティ対策ソフトを導入し、継続的に更新しましょう。
  - 購入時に付属しているセキュリティ対策ソフトは、有効期間を確認しましょう。
    期間が切れていると、内容が更新されず危険です。契約更新（有償）が必要です。
  - Windows10/11は、無償で添付されたWindows Defenderを使用することができます。

◆Webサービスなどインターネット利用時の注意点
- 利用者の意図しない危険なソフトウエアを実行させるサイトがあります。実行に制限をかけるためインターネットエクスプローラーのインターネット向けのセキュリティレベルは「中」以上に設定しましょう。
  何らかの指定が無い限りは、基本設定の「中高」のまま使うか、Chrome、Firefox、Safariなど、最新ブラウザを利用することを推奨します。
- 個人情報（メールアドレス、氏名、所属等）を入力する時は、通信が暗号化されていることが必要です。アクセス先が（https://）であることを確認しましょう。
- 学園のメールアドレスは業務用途以外の使用、特にWebサービスへの登録は避けてください。スパムメールや標的型攻撃の的になってしまいます。
- フリーWi-Fiや、学園内無線ＬＡＮサービスの利用時は、不特定多数の人が使用する環境になります。特にセキュリティ対策やアップデートが必須です。

◆ウィルス感染等の対応
- ウイルス検出など、セキュリティに関するメッセージが表示された時は、表示を読み、その内容を理解した後、一旦ネットワークから物理的に切り離し、原因の駆除、隔離など処置を行いましょう。
- 速やかに感染した内容を学園情報センターに報告しましょう。
- ウイルス感染の兆候は次のようなものがあります。
  ハードウェアやソフトウェアのトラブルと見分けがつきにくいものです。おかしいなと思ったら、ウイルス対策ソフトでウイルスチェックをするようにしましょう。

□ 動作
- 全体的に遅くなる
- メモリ不足になる
- プログラムが起動しなくなる
- キーやタッチ入力ができなくなる
- 勝手にWebサイトに接続されている
- 普段使っている接続先が偽Webに変更されている

□ 見た目
- アイコンが変更されたり、覚えのないものが増えている
- 画面上に心当たりの無いメッセージ、絵、図形等が表示されたり表示がくずれる

□ファイル等
- 覚えのないファイルが作成されたり、増殖している
- ファイルサイズが大きくなったり、破壊されたり、解除できない暗号化がされている
- メールの送受信記録に覚えの無いものがある

情報媒体の利用時に注意すること

情報通信媒体の利用

◆掲示板・SNS（Twitter・Line等）の利用時の注意

- 教職員、学生の個人情報の扱いは、各自で慎重に考えて責任を持って行動しましょう。
  個人情報の公開については、自身のWebページ、Twitter、Facebook等、記載先や閲覧者を想定して、内容が適正か、写真等の掲載許諾が必要か等、十分検討してからにしましょう。
- 誹謗中傷や公序良俗に反した書込みはしないようにしましょう。
- セキュリティ上の問題を確認した場合は、電子情報セキュリティ管理者に報告しましょう。

◆電子メール利用時の注意事項

- メールアドレスの入力間違いがないか十分確認しましょう。
- 送信前には、To、Cc、Bccを必ず確認しましょう、送信後は取消せません。
  Microsoft365は送信までの猶予時間を設定できるため、不安な場合は設定し活用しましょう。
- 宛先間違いは、当人にその気がなくても情報漏洩につながります。またToやCcに複数のメールアドレスを入力した場合、受信者全員が送付先を確認できます。
  他者に送付先が知られてはいけない場合、Bccを利用してください。
- 添付ファイルは、電子情報セキュリティ区分（P.１１参照）に基づき、送付先の選択、暗号化等を行いましょう。
- 大学からパスワードの再設定や、ログインを促す内容は、メールで送信しません！
  うっかり自分のユーザーID、パスワードを促されるまま入力しないようにしましょう。
  Microsoft365の乗っ取り被害が他大学で発生しています。

◆その他留意点

- □ 学園提供システムの私的利用
- □ 性的な画像や文章
- □ 差別的なもの
- □ 虚偽のもの

- □ 名誉・信用を傷つけるおそれのあるもの
- □ プライバシーを侵害するおそれのあるもの
- □ 学園の信用・品位を傷付けるおそれのあるもの
- □ 不正なネットワークの使用

Webサイト（ホームページ）の注意事項

◆Webサイトの作成・管理

- 作成
  - ➢ 情報通信媒体であることを理解し、作成する内容に注意しましょう。
  - ➢ 著作物を権利者の許諾を得ないで複製したり、ホームページ上に掲載し誰でもアクセスできる状態にすることなどは、著作権の侵害にあたりますので行わないよう注意が必要です。
- 管理

  - ➢ Webサーバー自体を運用する、レンタルしている、Webサイト開設サービスを利用している、いずれにおいてもWebサイトを作った人は管理者です。管理用ユーザーID、パスワードの漏えいは、第三者による改ざんの危険等が極めて高くなるため注意しましょう。可能であれば、より安全性のある多要素認証の仕組みを導入、利用しましょう。
  - ➢ 個人が管理するWebサーバーでは、セキュリティを高めるサーバ設定、不要なサービスやスクリプトの削除、随時のセキュリティホール対応、ウイルス対策、修正プログラムの適用、ログ確認による不正侵入や異常の早期発見に留意しましょう。
  - ➢ 第三者にWebサーバーを利用させる場合は、利用者のパスワード管理に注意が必要です。当ガイドブックの内容をはじめとした、注意事項を利用者にも周知しましょう。
  - ➢ 掲示板やコメント投稿機能があるWebサイトは、嫌がらせ、広告、個人情報の拡散に利用されることがあります。『迷惑行為の禁止』や『不適当と思われる書込みは削除します』といった旨の規約を明記し、管理者の責任と権限に基づき不適当なものは、速やかに削除などの対応を取る必要があります。
  - ➢ 迷惑行為を受けた場合は、電子掲示板、コメント等のログから、投稿日時、投稿者のリモートホスト名、ＩＰアドレス、投稿内容の情報を抜粋して保管しておくようにしましょう。行為が継続される際は該当のログ内容に基づき、プロバイダに行為者の情報開示を要請するなどの対応も必要になります 。

情報媒体の利用時に注意すること

学園Webシステムの利用

学園では、S*mapやMicrosoft365等へのログインを、まとめて一回で可能なシステム（シングルサインオン）が使われています。パスワードの漏えいは全てを乗っ取られる危険があるため、取り扱いに注意するとともに、多要素認証（P.6参照）を使用するなどセキュリティ強化に努めましょう。

また、電子情報セキュリティ区分（P.１１参照）に基づいた、情報共有先の制御をしましょう。

◆Microsoft365 利用時の注意事項

Microsoft365には、OneDriveをはじめ、様々なアプリケーションがあります。設定を間違えると、想定しない相手にも情報やファイルの共有をしてしまうため、以下の点には注意しましょう。

- 「OneDrive」はクラウドストレージです。インターネット上にファイルを保存し、さらにインターネットURLを作成し、それを知っている人に対して、ファイルやフォルダを共有（公開）することが可能です。
- 公開範囲は「意図的な世間一般への公開」を除いて、次の範囲に「リンクの設定」を設定するなど気を付けましょう。
  - 特定のユーザー
    生成されたリンク（URL）を知っている指定したメールアドレスを持つユーザーに共有します。
    大学内、大学外のメールアドレスが指定可能です。
  - リンクを知っている学校法人椙山女学園のユーザー
    生成されたリンク（URL）を知っているMicrosoft365を利用可能な学生教職員に共有します。
- 「Teams」や「SharePoint」は、チャットとWebサイト等を介して情報共有が可能です。アクセス許可については取り扱うファイルの内容に応じて、しっかり判断してください。

◆Gmail （Google G-suite）の共有に関する注意事項

G-suiteには、Gmailをはじめ、様々なアプリケーションがあります。設定を間違えると、想定しない相手にも情報やファイルの共有をしてしまうため、以下の点には注意しましょう。

- 「ドライブ」はクラウドストレージです。インターネット上にファイルの保存ができます。インターネットURLを作成し、それを知っている人に対して、ファイルやフォルダを共有（公開）することが可能です。
- 公開範囲は「意図的な世間一般への公開」を除いて、次の範囲に「リンクの共有」を設定するなど気を付けましょう。
  - オフ - 特定のユーザー
    生成されたリンク（URL）を知っている指定したメールアドレスを持つユーザーに共有します。
    大学内、大学外のメールアドレスが指定可能です。
  - オン - リンクを知っている椙山女学園の全員
    生成されたリンク（URL）を知っているG-suiteを利用可能な学生教職員に共有します。
- 「フォト」は、写真に特化したクラウドストレージです。共有をかけた場合、生成されたリンク（URL）を知っているユーザーのみに共有します。

情報媒体の利用時に注意すること

Microsoft365の利用方法 OneDrive

◆ OneDrive へのファイル保存

「OneDrive」へのファイル保存には、方法が複数あります。2019年3月現在可能な方法を幾つか紹介します。OneDriveアプリの入手方法は、OfficeProPlus、Microsoft365をインストール、または、個別にインストールする等複数ありますので、やり易い方法で実施してください。

また、暗号化を行いたいファイルは、OneDriveへアップロードする前に、パソコン上で暗号化してください。

1. Microsoft365経由

① Outlookを使用する要領で、Microsoft365へログインしてください。
https://sitec.sugiyama-u.ac.jp/uploads/Web-Outlook_manual.pdf

② アプリのOneDriveを選択します。

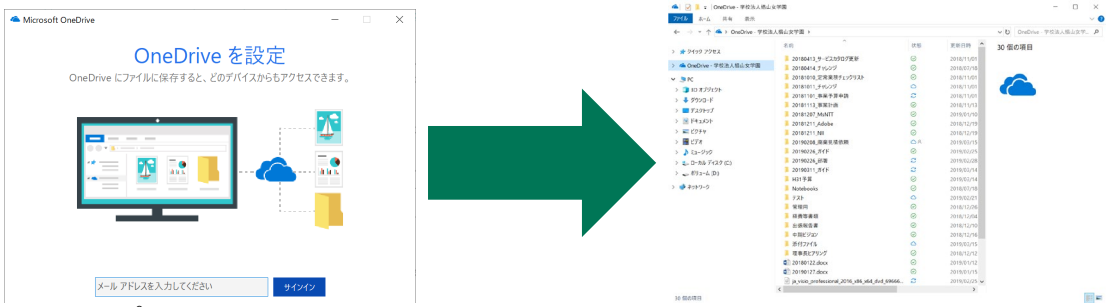
③ パソコン上のファイルをドラッグ＆ドロップする。アップロードボタンから、パソコン上のファイルを選択する等で、ファイルをクラウドへアップロードします。

2. OneDrive アプリ経由

① Microsoft OneDrive アプリをインストールしておきます。アプリ起動時に「サインイン」が必要です。
Microsoft365で使用しているメールアドレスを入力し、「サインイン」してください。

② 以降の操作は、上記１－①と同じになりますので、割愛します。

③ OneDriveは、使用しているパソコンと、クラウド上のOneDrive間で基本的にはファイルを同期します。
例：パソコン側　C:¥Users¥user-rei1¥OneDrive - 学校法人椙山女学園
　　クラウド側　user-rei1@sugiyama-u.ac.jp のOneDrive

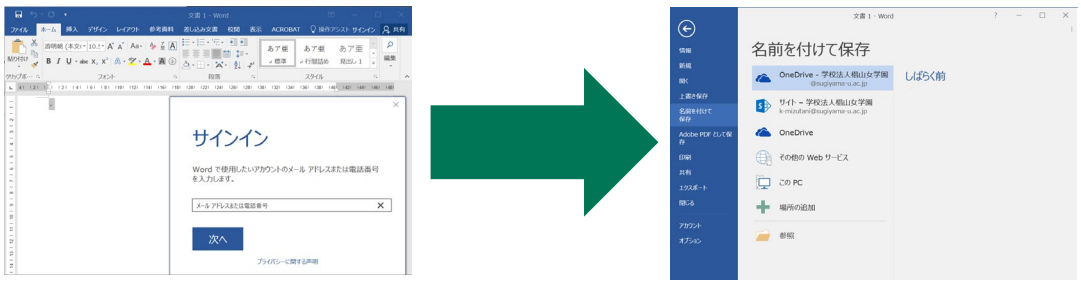


3. Microsoft アプリ経由

① Office2016以降、Microsoft365で、アプリケーションを起動します。

② アプリケーション右上の、サインインから、Microsoft365へログインします。
ログイン方法は、２－①②と同じになります。

③ ログイン済みのソフトからは、保存先にOneDriveが選択できます。



電子情報の区分について

「椙山女学園電子情報資産区分ガイドライン、平成１９年１０月２６日制定」より抜粋。

補足説明欄は、本書用に付け加えた機密性、完全性、可用性に関するレベル判断の説明となります。

（趣旨）

第１条　このガイドラインは、椙山女学園電子情報セキュリティ規程（平成１９年規程第１８号）第２条第１号の規定に基づき、情報資産の重要度に応じた適切な管理を行うため、情報資産区分（以下「情報資産区分」という。）に関して必要な事項を定めるものとする。

（情報資産区分）

第２条　情報資産は、次に規定する機密性及び完全性・可用性の各レベルにより区分する。

（１）機密性レベル基準 ―――― 補足説明

レベル	機密性	判断基準
1	漏洩・流出による影響なし。	一般公開可
2	漏洩・流出により、個別業務に影響する。 又は、学園イメージが低下する。	社外秘 組織内にのみ開示可能な情報
3	漏洩・流出により、広い範囲の業務に影響する。 又は、学園イメージや信頼が大きく低下する。	秘密 特定の関係者のみ開示可能
4	漏洩・流出により、全ての業務に影響がでる。 又は、学園イメージや信頼が非常に大きく低下し、受験者減少等の問題が発生する。	極秘 極一部向けのみ開示可能な情報
5	漏洩・流出により、事業継続に影響を与え、学園の存続に関わる甚大な損害が発生する。	極秘 極一部向けのみ開示可能な情報

備考　機密性レベル判定補足事項

1. 住所、電話番号等を含む個人情報は、レベル３以上として取扱う。
2. 試験解答などは、レベル３以上として取扱う。但し、個人を特定できない状態で管理する場合はレベル２とする。
3. 個人情報を含まない個人の研究データは、学園の管理対象外とし、自身の責任で管理する。
4. 入試問題は、漏洩等の影響が多大なため、作成途中も含めレベル４とする。
5. 機密性レベル５の情報は、一般にはその存在も知りえないレベルの情報が対象となる。

（２）完全性・可用性レベル基準 ―――― 補足説明

レベル	完全性・可用性	判断基準
1	改ざん、誤記等により、特に業務には影響しない。 長期間利用できない状態が発生しても特に影響はない。	左記は、一行目が完全性、二行目が可用性の基準となります。 本基準での完全性とは、元の状態に対し現状がどれ程同一であるかを示します。 また可用性は、その情報を使用できること、もしくは使用できないことによる影響の度合いを示します。 起こる影響の度合いに応じて、レベルを示すものです。
2	改ざん、誤記等により、一部の業務に影響する。 1週間を超えて利用できない状態が発生すると、一部の業務に影響する。	
3	改ざん、誤記等により、部門の業務に影響する。 １日利用できない状態が発生すると、部門の業務に影響する。	
4	改ざん、誤記等により、学園全体の業務に影響する。 業務時間中に利用できない状態が発生すると、学園全体の業務に影響する。	
5	改ざん、誤記等により、学園の存続に関し影響する。 業務時間中利用できない状態が発生すると、学園の存続に関し影響する。	

備考　完全性・可用性レベル判定補足事項

1　ホームページのトップページは、完全性レベル４とする。
2　ホームページの入試合格情報等は、完全性レベル４とする。
3　ホームページの学部トップページは、完全性レベル３以上として取扱う。
4　通常業務で使用しているファイルサーバは、可用性レベル３以上として取扱う。

高レベル機密情報の取扱い

高レベル機密情報の暗号化について

◆機密情報を暗号化するパスワードについて
- 暗号化に使用するパスワードも、適切なパスワード設定（P.６参照）に基づいて推測されにくいものを使用しましょう。

◆学園情報センターが推奨するツール
- 少なくともMicrosoft365アプリ標準のセキュリティ機能を使用しましょう。セキュリティ機能はファイルにパスワードをかける方法（P.１３参照）に基づき設定しましょう。
- クラウドサービスの利用の拡大に伴い、機能拡張、操作手順、画面構成の変更頻度が高まっています。そのため、学園から手順書を提供することは極めて困難です。
  随時サービスが提供するヘルプ等を参照して使い方を把握するように努めましょう。

入試問題の取扱い注意事項

入試問題関連情報は、機密性レベル４に該当します。次の事項に注意し取り扱いましょう。

◆保存方法
- 第一に、パソコン、クラウドサービスなど保存先へのアクセス方法について、これまでの記述に基づきセキュリティを担保しましょう。また、万が一に備えて、ファイル自体を暗号化し保存しましょう。
- 暗号化に用いたパスワードは、他のファイル暗号化や、ログインパスワード等に使いまわしをせず、個々に異なるものを使用しましょう。

◆電子メールの利用
- 添付ファイルとして送付する際は必ず暗号化が必要ですが、復号に必要なパスワードは添付したメールそのものには記載せず、必ず別の手段（電話等）で連絡しましょう。
- メールの件名、本文は、入試情報に関するものと判読されないような内容で作成するよう気をつけましょう。
- メールは、添付間違いや誤送信の際に、取消ができないため、学園Webシステムの利用（P.9参照）にあるクラウドサービスによる受け渡しも検討しましょう。

個人情報の取扱い時の注意事項

◆情報の消去
- 個人情報は、機密性の高いファイルサーバへ保存しましょう。パソコン等インターネットに直接接続する環境は、共有の環境では原則保存せず、一時的に保存した場合は、利用後速やかに完全消去しましょう。

◆情報が記憶された媒体、機器の持運びや輸送について
- 持ち運びや輸送時は、紛失、盗難、破損に十分注意し、万一に備え暗号化して保護しておきましょう。
- 学内で受渡をする際は、複数人の手を経由せず手渡ししましょう。
- 輸送の場合は、信頼のおける業者で輸送記録（書留郵便、集荷→配達まで一定の保証あるもの）を利用しましょう。

◆媒体、機器の持運び廃棄、返却、譲渡
- ＨＤＤ等の処分が難しい機器に保存された情報は、全データ保存領域に0を上書きして完全消去するか、物理的に破壊し管理者に報告しましょう。自分で処理できない時は、学園情報センターに相談しましょう。

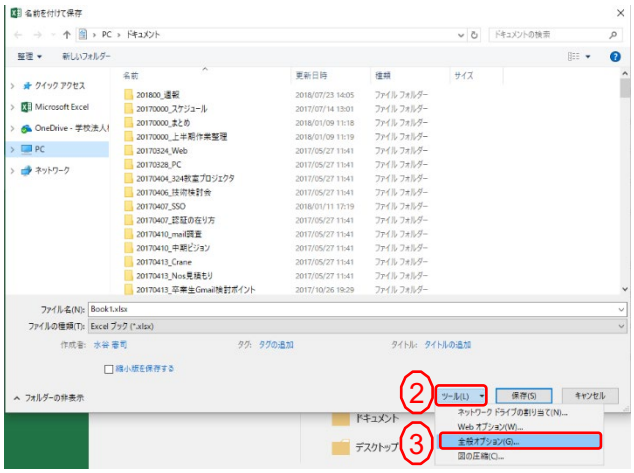
◆学園外での管理について
- 自宅に保存する際は、学園内と同様に施錠保管し、万一の盗難対策をしておきましょう。
- 自宅のパソコンでは、原則個人情報を扱わないようにしましょう。使用しなければならない場合は、セキュリティ対策を適切に実施するとともに、クラウドサービス上で作業を完結させるなど、情報を保存しない工夫をしましょう。
- 情報が保存されたパソコン等は、原則家族と共用してはいけません。情報を事前に削除し、他者用に管理者権限を有しないアカウントを作成するなど適切な使い方をしましょう。

高レベル機密情報のパスワード設定方法

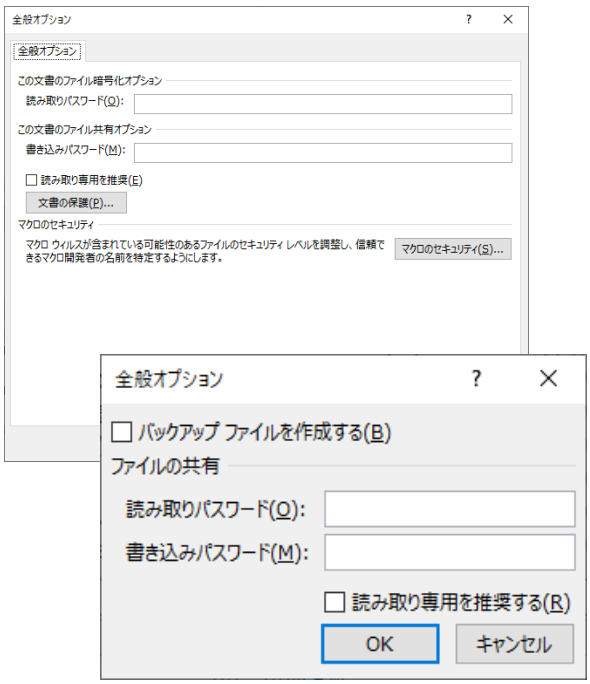
機密性レベル３以上の情報は、パスワードで保護しましょう

◆Microsoft365アプリのファイルにパスワードをかける方法

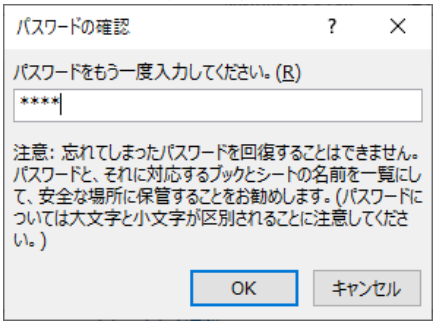
1. [ファイル]メニューから、[名前を付けて保存]をクリック
2. 保存先を指定するウィンドウ中の[ツール]をクリック
3. 表示されたメニューの[全般オプション]をクリック



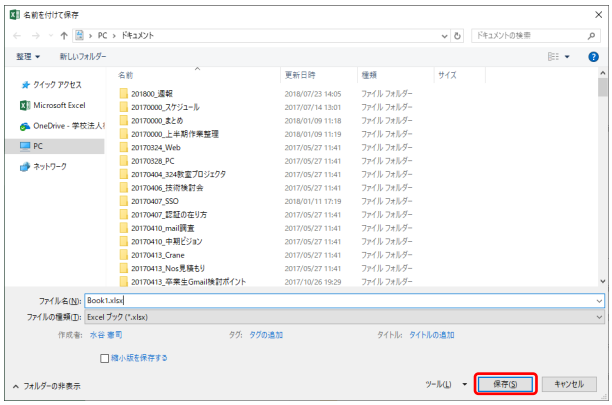
4. [読み取りパスワード]欄に、設定したいパスワードを入入力
〔上：Excel、PowerPoint、下：Word〕



5. 確認に再度パスワード入力を求められる、パスワードを入力



6. 通常の[名前を付けて保存]ウィンドウに戻る任意のファイル名を付け[保存]をクリック



- パスワードをかけていない元のファイルと同じ名前にすれば、パスワードをかけたファイルで上書きされる。
- ファイルを一旦閉じて開き直し、パスワード入力を求められることを確認する。
- 元のファイルが残っている場合は、必ず削除する。必要なら別メディアに保存する。

参考情報

1. 個人情報の保護に関する法律

本人の意図しない個人情報の不正な流用や、個人情報を扱う事業者がずさんなデータ管理をしないように、一定数以上の個人情報を取り扱う事業者を対象に義務を課す法律のこと。2005年4月より施行されている。次の5つの原則から成り立っています。

- 利用目的による制限 （利用目的を本人に明示）
- 適正な取得 （利用目的の明示と本人の了解を得て取得）
- 正確性の確保 （常に正確な個人情報に保つ）
- 安全管理の処置 （流出や盗難、紛失を防止する）
- 透明性の確保 （本人が閲覧可能なこと、本人に開示可能であること、本人の申し出により訂正を加えること、同意なき目的外利用は本人の申し出により停止できること）

この法律によって、本人の了解なくして個人情報の流用や売買、譲渡は規制されます。国の定める一定数以上の個人情報を持つ団体などは、この法律の適用対象となり守らない場合、本人の届け出や訴えにより、最高で事業者に刑罰（6ヶ月以下の懲役又は30万以下の罰金）が科されるという実効性を持つ法律です。

2. 不正アクセス禁止法

不正アクセス禁止法とは、「ID・パスワードの不正な使用」や「そのほかの攻撃手法」によってアクセス権限のないコンピュータ資源へのアクセスを行うことを犯罪として定義するものです。
この法律は、「ネットワークを利用してほかの端末に不正行為が行われることを防止したり、アクセス制御を越えて権限のないコンピュータ資源へアクセスするなど、ハッキングに代表される行為を犯罪として定義し、罰することを規定することで秩序を守り、それがネットワーク社会の正常な発展につながる」ことを目的としています。

不正アクセス禁止法において犯罪と定義されるのは、次のような行為です。

- 他人のID・パスワードを奪取・盗用して、その者になりすましてアクセス認証を越える行為
- なりすまし以外の攻撃手法を用いて、認証サーバをだまし、それに従属する目標の端末を利用可能にする行為
- 目標の端末を利用可能にするために、その端末の属するネットワークのゲートウェイ端末のアクセス認証をだまして、その内部ネットワークの目的端末を利用可能にしてしまう行為

上記3つの犯罪の場合、罰則は1年以下の懲役または50万円以下の罰金を科されます。
また、特定のアクセス制御を有する端末に関する認証情報（ID・パスワードなど）を、その端末利用者や管理者以外の人間に漏らしたり流布してはいけない、ということも規定されており、これは「不正アクセスを助長する行為」として犯罪とされ、本法により罰せられます。 この場合の刑は30万円以下の罰金刑になります。

3. その他、情報セキュリティに関わる法律

- IT基本法
  （高度情報通信ネットワーク社会形成基本法）（平成12年12月6日法律第144号）
- 著作権法
  （昭和45年 5月6日法律第48号）（最終改正：平成22年12月3日法律第65号）
- 刑法・コンピュータ犯罪
  （明治40年 4月24日法律第45号）（最終改正：平成23年6月24日法律第74号）
- 不正競争防止法
  （平成5年 5月19日法律第47号）（最終改正：平成30年5月30日法律第33号）
- 電気通信事業法
  （昭和59年12月25日法律第86号）（最終改正：平成30年5月23日法律第24号）
- 電波法
  （昭和25年 5月2日法律第131号）（最終改正：平成30年12月14日法律第102号）
- サイバーセキュリティ基本法
  （平成26年11月12日法律第104号）（最終改正：平成30年12月12日法律第91号）

Sugiyama
人間になろう

変更履歴

Ver 1.0	2007年10月26日	新規発行
Ver 2.0	2012年 4月 1日	改訂
Ver 3.0	2019年 4月 1日	改訂
Ver 3.1	2023年 4月 1日	改訂

発　行
学校法人椙山女学園
電子情報セキュリティ委員会