中部学院大学・中部学院大学短期大学部

個人情報保護に関する
ICTガイドブック
（教職員編）

Ver 1.02　（2023年7月4日更新）

ガイドブックについて

この「個人情報保護に関するICTガイドブック」、大学業務における個人情報保護の安全管理を図る上で必要な事項をまとめています。本ガイドブックは、今後も必要に応じて改定していく予定です。ガイドブックに記載の無い事項であっても個人情報保護に向けて必要な事項は積極的に取り入れて下さい。また、個人情報が漏えいする等の問題が生じる可能性が少しでもある場合は、より慎重に個人情報を取り扱うように心がけましょう。特に、業務の進め方、個人情報の管理等に関して、各自で判断せず、適時に所属長等に相談・報告して下さい。本学の全ての教職員が個人情報保護の重要性を強く認識し、社会から信頼される組織・環境を目指しましょう。

目次

事故の発生や異常に気付いたら

個人情報に関する事故が発生した場合やその可能性がある場合、速やかに報告して下さい。

◆速やかな報告が大切です！

（まずは「一報」を入れて、その後、詳細を確認する）

◆ あなたの上司・同僚の取扱の場合も、事故が発生した可能性があれば、迷わず報告する。

◆ 事故が発生する可能性を予見した場合、不安な点があれば、同様に報告・相談する。

下記の事案が発生した場合は、速やかに報告を

1）個人情報(教員、職員、学生等)の漏えい等が疑われる場合

2）コンピューターウィルス等の感染が疑われる場合（※）

3）その他、個人情報保護及び情報セキュリティ上、問題と思われること。

※コンピューターウィルス等の感染が疑われる場合は、P11の操作を行った後、速やかに報告して下さい。

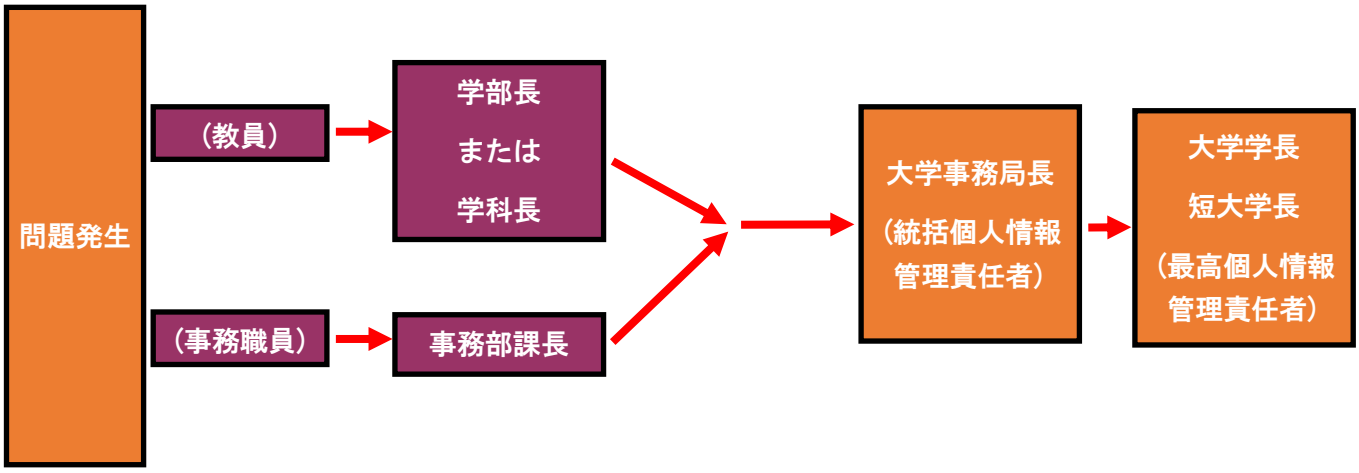
速やかに報告を

報告先

教員：所属学部長または学科長(*学科に属さない教員については総務部長)

職員：所属事務部課長

緊急時の報告経路



個人情報の保護に関するお願い

教職員の皆様へ

少なくとも年間1回は、次のような機会を学科・事務課室で設けて下さい。

①本ガイドブックや本学関連規程に目を通す。

※ガイドブック・規程は適時に改定されます。最新の情報を確認しましょう。

②学科・事務課室内で個人情報・情報セキュリティの取扱を点検し、業務の改善方法について話し合う。

※複数の関係者(学科教員や課内)で話し合いましょう。

個人情報の取扱について、不明な点、曖昧になっている点等があれば、所属長に相談・報告しましょう。

中部学院大学・中部学院大学短期大学部セキュリティポリシー

岐阜済美学院の個人情報保護基本方針

学校法人岐阜済美学院（以下「学院」という。）は、個人情報が個人の人格尊重の理念のもとに慎重に取り扱われるべきものであることを深く認識し、個人情報の保護に関する法律が定める個人情報を適正に取り扱うため、次のように基本方針を定めます。

1 教職員その他学院の業務に従事する者（以下「従業者」という。）は、個人情報の取り扱いに当たっては、個人情報保護法及び関係法令並びに学院が制定する諸規程（以下「法令等」という。）を遵守し、個人情報の保護に努める。

2 従業者は、個人情報の収集、利用及び提供を行う場合には、法令等に基づき、安全かつ厳正な管理に努める。

3 従業者は、個人情報への不正アクセス、個人情報の漏洩、滅失、毀損及び改ざんの予防並びに是正に努める。

4 従業者は、収集した個人情報は、あらかじめ定める利用目的の範囲内でのみ利用する。

5 個人情報保護の取り組みは、継続的に見直しを行い、改善を図る。

6 個人情報の保護に関しては、学院の設置する大学・短期大学、高等学校及び幼稚園毎に規程を整備する。

中部学院大学・中部学院大学短期大学部個人情報保護に関する規程 (抜粋)

第1章 総則

（目 的）

第1条 中部学院大学・中部学院大学短期大学部（以下「本学」という。）は、個人情報（個人情報データベースを含む。以下「個人情報」という。）の保護が、人格の尊厳に由来する基本的人権の保障に係る問題であることを深く認識し、本学が保有する個人情報の取扱いに関する基本事項を定める。

（用語の定義）

第2条 この規程において、「学生」とは次の各号によるものとし、「教職員」とは専任の教職員及び本学の業務に直接かかわりがあり、又はかかわりがあった者をいう。

（1）「本学において教育を受けている者」で在学生、科目等履修生や聴講生など

（2）「本学において教育を受けようとする者」で受験生、入学前の合格者、オ ープンキャンパスへの参加者など

（3）「過去において、本学において教育を受けた者」で卒業生、中途退学者、転学した者など

（4）「過去において、本学において教育を受けようとした者」で不合格者や入学辞退者など

2 この規程において、「個人情報」とは次の各号によるものとする。

（1）氏名、住所、生年月日、電話番号により、又はこれらの組合せにより特定の個人が識別されるもの

（2）映像、デジタル記録等により特定の個人が識別されるもの

（3）学籍番号、IPアドレス等個人を特定できないものであっても学内で対応付けられた個人情報がある場合のもの

（4）教職員が業務上取得又は作成した情報（文書、写真、フィルム、電磁的記 録その他これらに類するものに記録されたものを含む。）

（5）個人識別符号（身体の一部の特徴を電子計算機用に変換した符号、又はカ ードその他の書類等に対象者ごとに異なるものとなるように記載等された公的な符号のうち、個人情報保護法施行令（以下「政令」という。）で定めるものをいう。）が含まれるもの

3 この規程において「要配慮個人情報」とは、本人の人種、信条、社会的身分、病歴、犯罪の経歴、犯罪による被害の事実その他本人に対する不当な差別、偏見その他の不利益が生じないようにその取扱いに特に配慮を要するものとして政令で定める記述等が含まれる個人情報をいう。

4 この規程において「個人情報データベース」とは、個人情報が含まれる情報の集まりで、検索できる情報のものであって、ユーザーIDとユーザーが記録されているログ情報ファイル、紙による文書の住所録や名刺など整理されて検索できる利用可能な情報のデータベース（利用方法からみて個人の権利利益を害するおそれが少ないものを除く。）をいう。

（責 務）

第3条 学長は、この規程の目的を達成するため、個人情報の保護に関し次の各号に対する必要な措置を講じなければならない。

（1）利用目的の特定と公表

（2）適正管理、利用及び第三者への提供

（3）本人の権利と関与

（4）本人の権利への対応

（5）苦情の処理

2 教職員は、業務上知り得た個人情報をみだりに他人に知らせ、又は不当な目的に使用してはならない。

3 教職員は、個人情報保護の重要性を認識し、本規程によって学生個人の権利・利益を侵害しないように努めなければならない。

第2章 個人情報の収集及び利用目的の特定、公表等

（中略）

（個人情報の適正管理）

第5条 学長は、個人情報の保護のため、次の各号に掲げる事項について、適正で安全な措置を講じなければならない。

（1）紛失、滅失、毀損、破損その他の事故の防止

（2）改ざん及び漏洩の防止

（3）個人情報の正確性及び最新性の保持

（4）不用となった個人情報の速やかな廃棄又は消去

（個人情報保護委員会）

第6条 学長は、個人情報の保護に関する重要事項を審議するため、個人情報保護委員会（以下「委員会」という。）を置く。

2 委員会は、次の事項について審議する。

（1）個人情報の保護についての基本的施策に関する事項

（2）個人情報の保護に関する取扱いに係る疑義事項

（3）個人情報の保護に関する不服申立て

（4）その他個人情報の保護に関する重要事項

3　委員会の構成、運営等に関しては、次の各号の通りとする。

（1）委員会は大学評議会をもって充てる。

（2）委員会の委員長は大学学長とし、副委員長は短期大学部学長とする。

（3）委員会に関する事務は大学事務局総務課において処理する。

（最高個人情報保護管理責任者等）

第7条 本規程に基づく業務を適切に執行するため、最高統括個人情報保護管理責任者（以下、「最高管理責任者」という。）を置き、大学学長及び短期大学部学長も って充てる。

2 最高統括管理責任者は、本学の個人情報保護に関する全ての権限と責任を掌握し、本学における個人情報の保護に関する一切の業務を統括する。

3　最高管理責任者は、本規程に基づく業務の適切な執行を補助させるため、統括個人情報保護管理責任者（以下、「統括管理責任者」という。）を置き、大学事務局長をもって充てる。

4 統括管理責任者は、その権限と責任を分担させるため、業務毎に個人情報保 護管理責任者を置き、大学学部長、短期大学部学科長及び各課長又は室長をもって充てる。

5 統括管理責任者は、次の各号に掲げる組織的、人的、物的、技術的その他の広範囲な安全対策措置を講ずるものとする。

（1） 組織的安全管理措置

ア. 個人情報保護管理責任者の設置、組織体制の整備

イ. 学内諸規制の整備と運用

ウ. 個人情報取扱い台帳の整備

エ. 安全管理措置の評価、見直し、改善

オ. 事故又は違反への対処

（2） 人的安全管理措置

ア. 雇用時や契約時において非開示契約を締結

イ. 教職員に対する教育・訓練の実施

（3） 物理的安全管理措置

ア. 入退室管理

イ. 盗難対策

ウ. 機器、装置等の物理的な保護

（4） 技術的安全管理措置

ア. 個人情報へのアクセス認証・制御・記録・権限管理

イ. 不正ソフトウェア対策

ウ. 移送、通信時の対策

エ. 動作確認時の対策

オ. 情報システムの監視

（5） その他重要事項

ア. 個人情報を閲覧できる教職員の限定

イ. 個人情報の持ち出し制限

ウ. 外部からの個人情報への不正アクセス防止策の導入

エ. 教職員に対する個人情報保護研修の実施

6 統括管理責任者は、業務に関係する教職員に対する情報セキュリティ対策と して、個人情報に対するアクセス制限、アクセス管理及び監視を行うものとする。

7 統括管理責任者は、業務マニュアルを定め、持ち出し制限や移動時の取り決め、暗号化等のプロセスを決め、全て申請・承認によって処理することを定めて、守らせるものとする。

8 統括管理責任者は、業務に関係する教職員に個人情報を取り扱わせるに当っては、当該個人情報の安全管理が図られるよう、当該教職員に対する必要かつ適切な監督を行わなければならない。

9 統括管理責任者は、業務に関係する個人情報の取扱いの全部又は一部を委託する場合は、その取扱いを委託された個人情報の安全管理が図られるよう、委託を受けた者に対する必要かつ適切な監督を行わなければならない。

10 統括管理責任者は、次条に掲げる場合を除くほか、あらかじめ本人の同意を得ないで個人情報を第三者に提供してはならない。

（個人情報の利用制限）

第8条 教職員は、業務上収集した個人情報をその目的以外のために利用又は提供してはならない。ただし、次の各号のいずれかに該当するときはこの限りで ない。

（1）本人の同意があるとき

（2）個人の生命、身体、健康に対する急迫の危険を避けるために止むを得ないと認められるとき

（3）教員及び保護者の教育上、特段の必要性があるとき

（4）法の定めがあるとき

（5）最高管理責任者又は統括管理責任者が必要と認めたとき

2 前項各号の一に該当して個人情報を利用又は提供する場合、又は緊急に対応 した場合は、当該教職員は速やかに統括管理責任者に届け出なければならない。

（個人情報に関する業務の学外委託）

第9条 個人情報に関する業務を学外に委託するときは、教職員は統括管理責任 者の指導のもと委託業者との間で個人情報の保護に関する必要な措置をとらなければならない。

（中略）

第5章　事故等への対応

（事故等が発生した場合の対応）

第16条　本学の教職員は、個人情報等の漏えい、滅失又は毀損による事故（以下「漏えい事案等」という。）が発生した場合又はその可能性が高いと判断したときは、速やかに統括管理責任者に報告しなければならない。

2　統括管理責任者は、漏えい事案等が発生したと判断した場合は、速やかに最高管理責任者に報告する。併せて、漏洩事案等が発生した原因を分析し、再発防止に向けた対策を講ずるとともに、その事実を本人に通知し、関係法令等の定めに従い適切に対応する。

（事故等再発防止委員会）

第17条　最高管理責任者は、漏えい事案等が発生したと判断した場合は、事故等再発防止委員会（以下「再発防止委員会」という。）を必要に応じて設置するものとする。

2　再発防止委員会は、次の事項について審議する。

（1）漏えい事案等の発生原因の分析

（2）再発防止に向けた対策の策定

（3）その他必要とされる事項

3　再発防止委員会は、次の各号によって構成し、学長が委員長を指名する。

（1）学長が指名した教育職員　3名以内

（2）個人情報保護に関わる有識者　2名以内

（3）事務局長が指名した事務職員　2名以内

（4）上記の他、学長が必要に応じて指名する者　2名以内

（中略）

附　則［2022年5月　　日理事会議決］（*2022年5月改正予定）

この規程は、2022年5月　　日から施行する。

（以下省略）

パソコン利用時における「個人情報」の取り扱い

パソコンの設定等

◆パソコンへの適切なパスワード設定

●パソコンサインインに必要なパスワードは、**8桁以上で推測されにくいパスワード**を設定しましょう。

●パスワードは、大文字、小文字、数字、記号の内から３種類以上を織り交ぜましょう。

●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は避けましょう。

●パスワードの取扱いには注意し、パスワードを書いたメモなどを見える場所に貼ったり、他人に教えないようにしましょう。。

●パスワードを保存（キャッシュ）できるシステム(コラム参照)は、自分以外は使用できないパソコンのみで使用し、第三者に不正利用されないよう注意しましょう。

◆離席時は、ロックやログオフを実施

●パソコンを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設定しましょう。

●パソコン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。【原則として事務職員は外出先での使用は不可。】

◆パソコンへの個人情報の保存

●パソコンへ個人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。

●個人情報が保存されたファイルは、利用後、速やかに完全消去しましょう。

◆記録媒体(USBメモリ等)への個人情報の保存

●原則として、記録媒体(USBメモリ・ポータブルHDD/SSD等)に個人情報を保存しないで下さい。ただし、致し方無い理由で、個人情報を保存する必要がある場合は、万一に備え、暗号化の上、保存しましょう。

◆盗難、紛失及びデータの消去

●大学内で施錠できない部屋のパソコン等は、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。

● HDD・SSD等の保存された情報を完全に削除するには特別な対応が必要です（コラム参照）。各自で対応できない場合は、教育研究支援課に相談しましょう。

パソコン利用時における「個人情報」の取り扱い

◆Webサービスなどインターネット利用時の注意点

●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か確認しましょう。

※アクセス先が（https://）（注：httpではく、httpsであり、「S」がある）（コラム参照）であること。

●大学メールアドレスは、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。

●公共機関や商業施設で利用できるフリーWi-Fiは、不特定多数の人が使用するためセキュリティ上の課題があります。大学業務で使用は避けて下さい。

◆情報が記憶された媒体、機器の持運びや輸送について

●個人情報が記録された媒体、機器を持ち運ぶ時は、紛失、盗難、破損に十分注意してください。

●学内で個人情報が記録された媒体、機器等を受渡する際は、直接、担当者(責任者)に手渡しして下さい。

●輸送の場合は、書留郵便や配達記録が残る方法を利用しましょう。

◆大学外での管理について

●原則として、自宅等、学外で個人情報を取り扱う事はできません。

●教育職員の内、致し方ない理由により個人情報を学外で管理しなければならない場合は、万一に備え暗号化して保護した後、保存しましょう。

●個人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。

●共同研究室や学生が使用するパソコン等、複数人でパソコンを利用する場合は、個人情報をパソコン内に保存しないで下さい。

◆個人情報を暗号化するパスワードについて

●個人情報を暗号化する場合のパスワードも、パソコンサインインのパスワード設定と同様に推測されにくいものを適切に使用しましょう。

コラム

データの完全消去について

ー削除したと思っても削除されていない？ー

HDD・SSD等の記憶媒体は、ファイルを削除(「ゴミ箱」に捨てて「ゴミ箱を空にする」場合を含む。)やHDD・SSDを初期化してもデータを“完全には”消去できません。これらの作業は、管理情報を変更して、ファイルが“見えなくなっている”だけだからです。データ本体は、HDDやSSD内に残っているため、特殊なソフトウェアを使えば容易に復元できます。

電子メールの設定等

◆電子メール利用時の注意事項

●メールアドレスに入力間違いがないか、十分に確認しましょう。

●To、Cc、Bccを適切に使い分けましょう。ToやCcに複数のメールアドレスを入力した場合、受信者全員が当該メールアドレスを知ることとなり、場合によっては、情報漏えいに繋がります。

TO	Toはメールの送り先を示します。	Toに指定したメールアドレスは、Cc･Bccで送信したすべての受信者に表示されます。
CC	Toと同一の内容を送信することができます。ただし、Toの場合と異なりメインでやりとり(返信等)しないこと想定しています。	Ccに指定されているメールアドレスは、To･Bccで送信したすべての受信者に表示されます。
BCC	Ccのように同一の内容のメールを送信することができます。なお、他の送り先にアドレスが表示されないことが特徴です。	他にも受信者がいることを隠したい場合や、受信者のメールアドレスを明かすことなく送信したい場合に有効です。

●複数の対象者に送信し、本人以外の送付先が知られてはいけない場合、Bccを利用しましょう。

●個人情報を含む添付ファイルの送信は、必要最低限の範囲とし、送信する場合には添付ファイルに必ずパスワードを付けましょう。

●上記のパスワードは別便で送信しましょう。

●ファイル送信を行う際には、次の対策を実施することを推奨します。

・事務局は、職員の個人メールアドレスではなく、部署の代表メールアドレスを使用する。

・送信前に複数人で確認を行う等の方法により、誤送信防止に努める。

ー注意ー

送信するファイルが個人情報に該当するか否か、判断に迷う場合は、所属長(学科長･所属課長)に事前に相談しましょう。

なお、今後、本ガイドブックの改訂版において、個人情報の該当事例を掲載する予定です。

電子メールの設定等

◆電子メールで送信できないもの

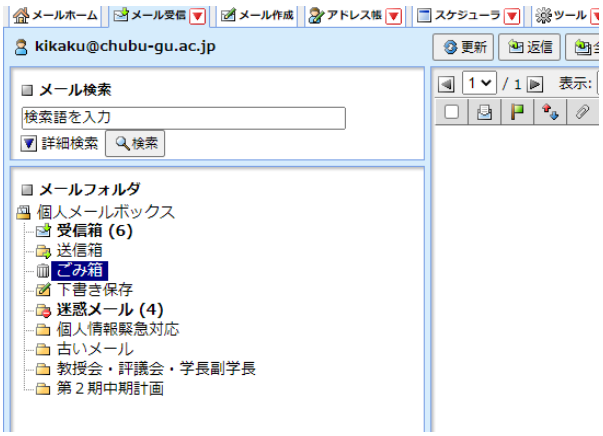
- 私的な利用に関すること。
- 性的な画像や文章を送信すること。
- 差別的な画像や文章を送信すること。
- 事実が確認されていない情報に基づく内容を送信すること。
- 他者の名誉・信用を傷つけるおそれのある内容を送信すること。
- プライバシーを侵害するおそれのある内容を送信すること。
- 本学の信用・品位を傷付けるおそれのある内容を送信すること。
- 不正なネットワークを経由したメールを送信すること。

コラム

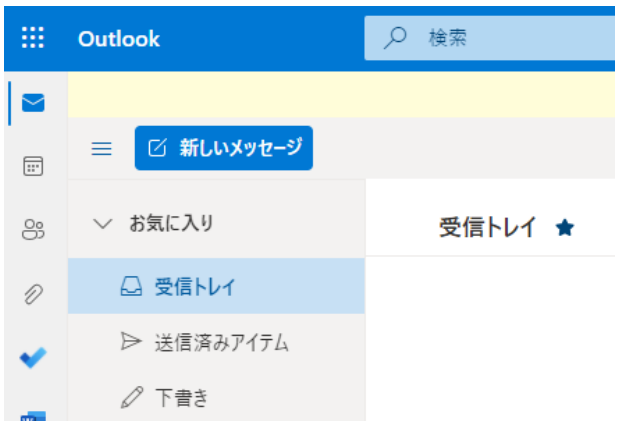
「教職員メール」と「Office365」の2つのメールアドレス

ー上手に使い分けしましょうー

教職員 メール



Office365メール



本学では、全ての教職員に対して、2つのメールアカウントを付与しています。

「教職員メール」(画像上段)は、大学における事務手続や研究活動に活用することを想定しています。

一方、「Office365メール」は、学生に貸与しているメールアドレスです。

今後は「教職員メール」を事務・研究用として活用し、「Office365メール」は、学生指導用に使い分ける方法が想定されます。

＜教職員メール＞

abcdef@chubu-gu.ac.jp

<Office365メール>

abcdef@st.chubu-gu.ac.jp

パソコン利用時における「個人情報」の取り扱い

パソコンの管理

◆OS・アプリケーションのアップデート

•OSやアプリケーションは、セキュリティの観点からは、最新版に更新することが望ましいでしょう。

・ただし、OS・アプリケーションを更新すると、アプリケーションや周辺機器の不具合が発生する場合があります。十分に注意して下さい。

・事務局パソコンは、年次計画に即して、適時、OS・アプリケーションのアップデートを行っています。※原則として事務職員の作業は不要です。

・教育職員パソコンは、都度、最新版のOS・アプリケーションへの更新をライセンス元から促されます。その際、各自でご判断でOS・アプリケーションを更新して下さい。※原則として教育職員が自ら操作する必要があります。

◆ウィルス感染等の対応

・大学貸与のパソコンや個人研究費で購入したパソコン(大学内ネットワークを使用するパソコン)には、本学導入のセキュリティソフト(ESET)がインストール済みです。

•ESETは、ネットワークに接続していれば、自動的にウィルス定義が最新版に更新されます。

・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、教育研究支援課まで速やかに報告して下さい。

・ウイルス感染の兆候は、コラムを参照して下さい。

•ウイルス感染は、パソコンの不具合と見分けがつきにくいものです。おかしいと思ったら、教育研究支援課に相談して下さい。

コラム

ウィルス検出が表示されたら。

ー下記の操作をしつつ、速やかに教育研究支援課へ連絡ー

コンピュータウィルスが検出されたと表示されたら次の3つの操作を行って下さい。

①LANケーブルを取り外す　又は、Wi-FiをOFFにする。

②電源をOFF(シャットダウン）する。

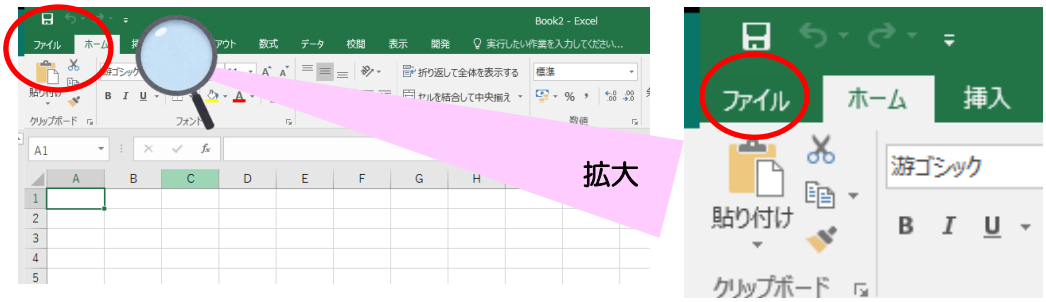
③速やかに教育研究支援課へ連絡する。

コラム

「Excel」ファイルにパスワード設定

― 設定したパスワードを忘れないようにしましょう。―

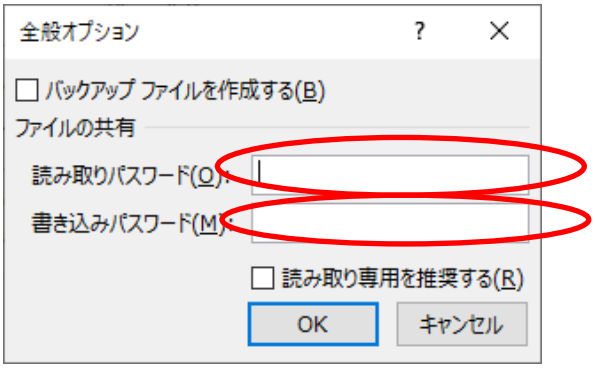
①[ファイル]をクリック



②[名前を付けて保存]をクリック

③[ツール]→[全般オプション]をクリック

④[読み取りパスワード]・[書き込みパスワード]を入力



読み取りパスワードと書き込みパスワード

「読み取りパスワード」を設定することで、パスワードを入力しなければ、ファイルの中身を参照することができなくなります。機密性の高いファイルにはパスワードを設定しましょう。

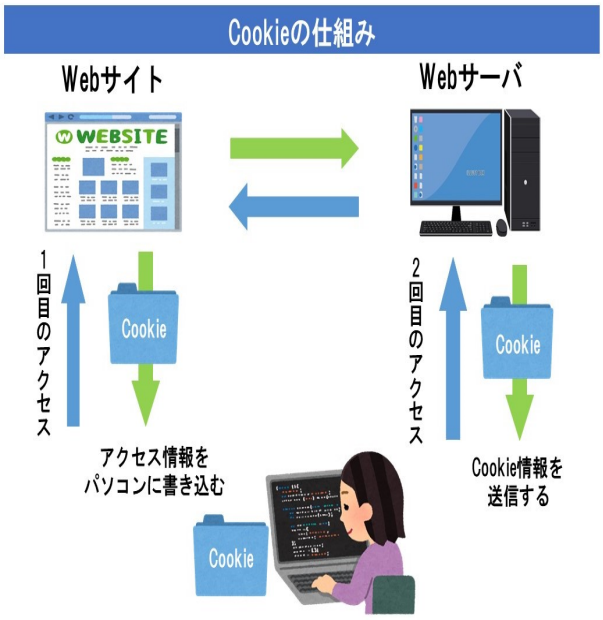
「書き込みパスワード」は、ファイルの「書き込み」(編集)を行うためのパスワード設定です。

このパスワードを設定することで、「データの書替」を防止することができます。

コラム

クッキー？？　いえ、「Cookie」です！

ーパスワードを保存（キャッシュ）できるシステムー



「Cookie」とは、Webサイトを訪れたユーザー情報を一時的に保存する仕組み。

例えば、閲覧中のWebサイトを訪れた日時や訪問回数、ログインIDやパスワードなどの情報が記録される。

「Cookie」に情報が保存されることで、ログイン(サインイン)が必要なWEBサービス等に一度ログインすれば、再度同じIDやパスワードを入力してログインする必要がない。

このように「Cookie」機能によりWebサイトがを快適に利用できる。

ただし、家族共用のパソコンで大学の業務を行ったり、業務を行ったパソコンを紛失した場合は、「Cookie」で保存されたIDやパスワードが漏えいしてしまい非常に危険な状態になる。

このため不特定多数の人が使うパソコンでは必ず「Cookie」を削除しておく必要がある。

コラム

ソフトウェアの利用には「ライセンス」が必要です。

ー違法コピーは、「犯罪」ですー

コンピュータソフトウェア（プログラム）は、原則として、著作権法によって保護された著作物。

そのため、大学教職員がソフトウェアのインストール（コピー）を行うには、著作権者(ソフトウェアの制作者）からの使用の許諾・許可が必要。

この許諾・許可は「ライセンス」と呼ばれており、ライセンスで認められたインストール可能台数の範囲を超えたインストールは不正コピーであり、著作権侵害となる。

したがって、ライセンスが無いソフトウェアをインストールした場合は、使用許諾契約違反に加えて、著作権法違反となる可能性がある。また、不正コピーが明るみに出ることで、社会的な信用を損なうことになる。

＜事例１＞　新規購入したパソコンにこれまで使用していたソフトウェアをインストールし直した。この際、これまで使用していたパソコンのソフトウェアは、アンインストール（削除）していない。

⇒この状態では、これまで使用していたパソコンを使用していない(又は廃棄した場合)であっても、ソフトウェアは、2台分の使用と見なされます。ソフトウェアの「ライセンス」が1台分であれば、不正コピーに該当します。

＜事例２＞　インターネットオークションやファイル共有ソフト等などから「海賊版」(正規ライセンスの無いソフトウェア)を購入してインストールした。

⇒ネットオークションやネットショップでは、ソフトウェアが、正規販売店よりも格安で販売されるケースが散見されます。絶対に「海賊版」のソフトウェアの購入はしないで下さい。

コラム

コンピューターウィルスに感染した兆候

ー次の兆候が現れたたウィルスに感染した可能性があります。ー

□全体的に作動が遅くなる。

□メモリ不足と表示される。

□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

□ 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が表示される。

□ 身に覚えのないファイルが作成されたり、増殖している

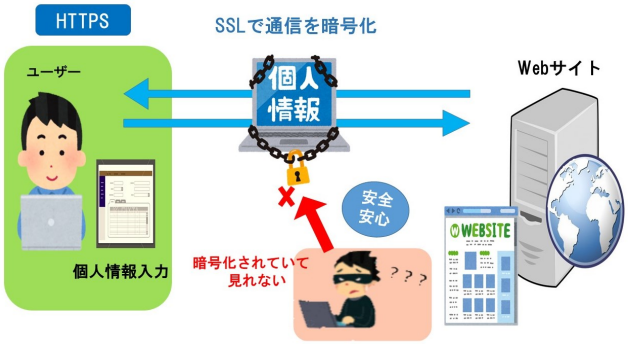
□ファイルサイズが大きくなったり、破壊されたり、解除できない暗号化がされている

□メールの送受信記録に覚えの無いものがある

コラム

「S」は大切なキーワード！

ー HTTP：// と　HTTPS：// のWEBサイトの違い

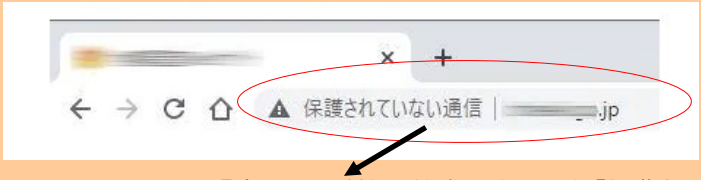


HTTPと、HTTPSはホームページ通信手段に関する取り決め。

URLの始まりが「https://」のようにhttpの後に「S」があるものは、通信内容が暗号化される。一方、「http://」の場合は、暗号化はない。

このためWEBサイトは、「https://」から始まるサイトの方がより安全と言われており、現在では、多くが「https://」が導入されている。

なお、ChromeやFirefoxでは、「http://」から始まるサイトを閲覧しようとすると下記のような警告が表示される。



Chromeの場合、http://から始まるサイトは「保護されていない通信」と表記される。

コラム

本学では、次を標準としています。

ーOS（基本ソフト）、アプリケーション　他ー

	教育職員	事務職員	学生
OS(基本ソフト)	Windows10／11	Windows10	Windows10
Office	Office2016以上	Office2016以上	Microsoft 365 Apps for enterprise
ウイルス対策ソフト	ESET	ESET	Windows Defender

＊上記は、2022年4月1日現在。最新の情報は、最新の本ガイドブックを参照下さい。更新版のガイドブックは、グループウェア　⇒　文書管理　⇒　研究支援課　⇒　情報支援　を参照ください。