島根県立大学・島根県立大学短期大学部
松江キャンパス

情報ネットワークシステム
利用の手引

2026年4月

目 次

第１章　　情報ネットワークシステムの利用にあたって

■ユーザー名とパスワードの管理を確実に行ってください

ユーザー名・メールアドレスは、基本的に変更できません。パスワードは学内システム共通で、個人で管理します。また、自分のユーザー名（やメールアドレス）とパスワードを使ってシステム上で行われた行為には責任がありますので、ユーザー名とパスワードを他人に使用させたり、知らせたりしないでください。もし悪意ある第三者へユーザー名とパスワードが知られた場合、本人に加えて大学全体に被害が及ぶリスクがあります。さらに、外部社会への攻撃の踏み台に使われた場合は加害者の立場になり、社会からの信頼を損なうことになります。ついては、万一、パソコン（以降 PC）やスマートフォン（以降スマホ）の紛失など漏洩がありえる事態の際は、管理課へ急ぎご相談ください。

■PC やスマホにはセキュリティソフトを使ってください

授業や学内サービスを利用するパソコン・スマートフォンには、ウイルス対策ソフトを必ず入れてください。未導入の場合、ウイルス感染や情報漏えい、不正利用の危険が高まります。これらの問題は、本人だけでなく学内ネットワーク全体に影響することがあります。なお、有料ソフトでなくても、Defender などの標準機能でも問題ありません。

■メールの宛先を必ず確認しましょう

悪意の第三者による漏洩よりも発生リスクが高いのは、メールなどでの宛先間違えによる情報漏洩です。メールソフトは、アドレスの一部や名前の一部を入力すると候補を出す仕組みがありますが、同姓の方もいますので、送りたい相手かどうか、学籍番号やフルネームで必ず確認をしてください。本手引の参考資料内『島根県立大学電子メール利用ガイドライン（P54）』を参照し、適切に利用してください。

■規則の順守をお願いします

すべての情報システム利用者は、本学が決めるセキュリティポリシーを順守しなければなりません。参考資料（P40～）をつけていますのでご一読ください。松江キャンパスでのシステム管理は管理課が行っています。

・各種情報システムは学外からも利用可能（一部機能制限あり）ですが、セキュリティの観点から、信頼性が低い情報端末（ネットカフェなど多数のユーザーが利用する端末等）からのアクセスは行わないこと。
・共用パソコンなど複数人で使用するパソコンで、ユーザー名、パスワードを誤って保存した場合は、P37『９.５　ブラウザの履歴について』をご確認ください。

第２章　　情報ネットワークシステムの概要

２.１　主な情報システム・ネットワーク

■学内トップページ（学内 LAN 接続時のみ）

学内専用のホームページ（http://mhome/）です。主要システムへの入口を用意していますので、ブラウザのホーム画面やお気に入りへの登録をお勧めします。「学生情報システム（略称：ユニパ）」、「メール」、「図書館」や、教員の学内、学外の出退状況が確認できる「出退表示システム」などへのリンクがあります。

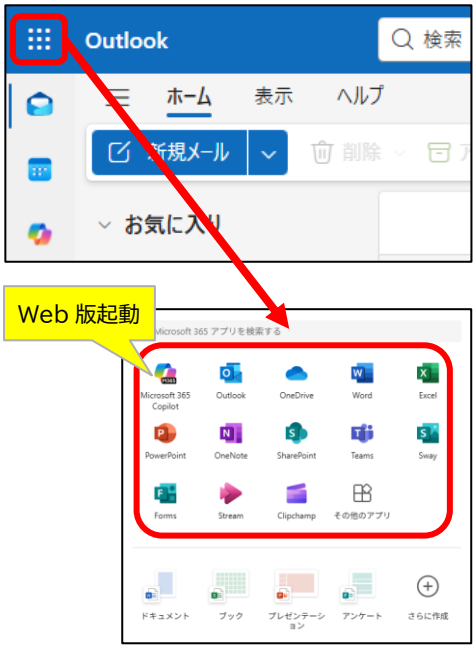
■学生情報システム（UNIPA／ユニパ）

履修登録、時間割、教室予約情報、各種お知らせが掲載される掲示板など、学生生活の中心になるシステムです。ログイン情報はメールアドレス・パスワード＋多要素認証です。前項の学内トップのリンクや、学外 HP ヘッダーのバナーをクリックしてサインインしてください。(スマホは、アプリをインストールしなくても利用できます)

PC 版
https://unipa-web.u-shimane.ac.jp/uprx/ShibbolethAuthServlet
スマホ版（Web）
https://unipa-web.u-shimane.ac.jp/uprx/MobileShibbolethAuthServlet

スマホ用 QR

■Outlook（メール）ほか、Microsoft365 ソフト



システム利用者には、メールアドレス（以降メアド）が与えられます。メアドは「ユーザー名@u-shimane.ac.jp」で、学外からも利用可能です。また、スマホからも見ることができます。ログイン情報は、メアド・パスワード＋多要素認証です。

word などの他ソフトも左上のタイルメニューから起動（Web 版）もしくは、インストール（アプリ版）ができます。

Outlook　https://outlook.office.com/owa/

■大学 PC 設置演習室および自習室

当手引で説明するマルチメディア・第２PC 演習室には、大学のデスクトップ PC が配置され、印刷もできます。ユーザー名・パスワードでサインインできます。これら２つの演習室では、教材の配布やファイル共有の機能があり、効果的な授業が行われるとともに、空き時間には自習もできます。他 PC の設置場所は当手引内コンピューターマップを参照してください。また、３号館自習室とオロリンひろばには、自分の PC で利用できるプリンタがあります。

■図書館

図書館では、OPAC（オパック：蔵書検索）やマイライブラリ（図書館用の個人ページ）のほか、ILL（アイエルエル：図書館間相互貸借サービス）により、他キャンパスや他大学図書館の図書を取り寄せるサービスなどを提供しています。

マイライブラリのログイン情報は、ユーザー名・パスワードです。

OPAC・マイライブラリ　https://opac.u-shimane.ac.jp/

■無線 LAN

キャンパス内のほぼ全ての館内で学内無線 LAN に接続できます（当手引内コンピューターマップ参照）。無線名は「kendai」、ログイン情報は、ユーザー名とパスワードです。個人の PC・スマホともに接続できますのでご利用ください。なお、松江キャンパスでは個人の機器は有線 LAN への接続はできません。

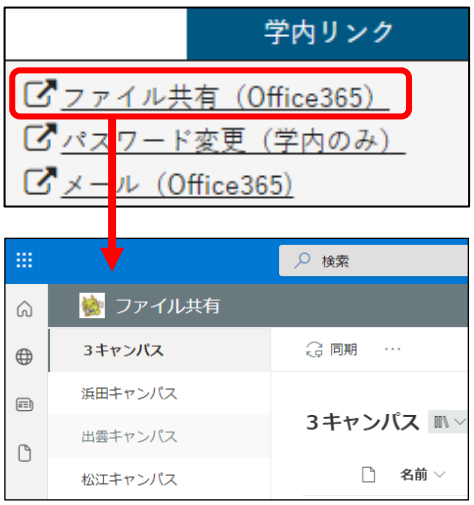
■ファイル共有（Microsoft365）

３キャンパス内の学生・教職員向けの共有ファイルがあるクラウド（インターネット）上の保管場所です。下記 URL を指定、もしくは学生情報システム（ユニパ）トップページの左下にある学内リンク欄内から接続します。

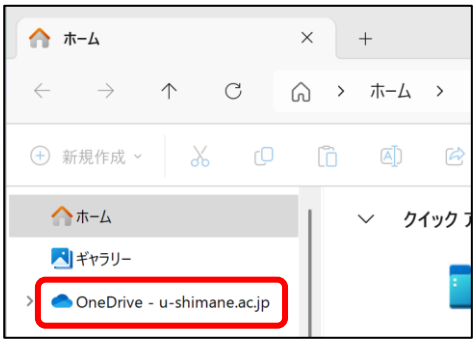
「３キャンパス」「松江キャンパス」に関連資料があります（文書名の検索も可）。ログイン情報は、メアド・パスワード＋多要素認証です。

ファイル共有
https://ushimaneacjp.sharepoint.com/pub

ユニパトップページの左下　学内リンク欄



OneDrive（Microsoft365）



Microsoft365 サービスの一つで、クラウド上の個人別保管場所です。大学用として一人当たり１TB の容量がありますので、PC ローカルデータのバックアップ場所としても利用できます。また、共有機能もあるので、特定の学内・学外者とファイル共有できます。但し、インターネット上の保存場所ですので、万が一の操作ミスや不正アクセスにご注意ください。

なお、個人で同サービスを契約されている場合は、大学用と個人用のどちらにアクセスしているか確認のうえご利用ください。

アクセス方法は、前ページメールの項で紹介したとおりです。ほか、エクスプローラーからも接続（上記画像参照）でき、ローカル PC 内のフォルダと同様の使い方でアクセスすることもできます。

2.2 システム管理者

松江キャンパスシステム管理者（管理課の情報担当者。以下、「システム管理者」という）は、以下の管理業務を担当しています。システムの安全な運用のために、利用者にメールなどで緊急連絡することがあります。また、全学的な情報については、浜田キャンパスの図書情報課や情報基盤推進室より提供されることもあります。

① 利用者の ID・パスワードの割り当てと、登録・変更・廃止手続き
② 本学が策定したセキュリティ方針にもとづく、情報セキュリティの管理
③ 定期的なメンテナンスの実施と障害発生時の復旧および事後報告
④ ネットワークサービス事業者・ハードウェアソフトウェア供給者との技術連絡
⑤ システム利用者へのシステム停止の事前連絡（可能な限り２週間前まで）
⑥ システム利用者へのセキュリティ管理に関する情報提供
⑦ その他、システム監視上必要な業務

2.3 施設利用上の注意

飲食物の持ち込みについて

重要

大学 PC 設置場所での飲食や飲食物持込は、
PC などに支障を与えるおそれがありますので基本 NG ですが、
脱水予防のためフタ付きの飲み物のみ可とします。

■大学 PC 設置演習室（マルチメディア、第２PC の各演習室）および自習室

- 演習室の空き時間は学生の自由利用を認めます。授業中か自由利用かは、時間割やユニパの施設予約で確認してください。平日の利用には特に届出は必要ありません。
- ３号館 1 階の自習室は、平日は８時から 21 時まで自由に利用できます。
  ※３号館自習室を休日に自習で使用する学生は、警備員室に口頭で届け出てください。
- 授業で習得した機器管理の手順を守り、自主的に利用してください。教室で機器に障害が発生した場合は、管理課にすぐに知らせてください。放置したままにしておくと、後の授業に差し支えます。夜間で管理課職員がいない場合は、警備員室に翌日管理課職員に知らせるよう添えて障害内容を伝言してください。

■図書館

図書館の PC、iPad は蔵書検索専用です。質問があればカウンターの司書におたずねください。

■各学科の演習室や資料室

各学科演習室や資料室にある PC やコピー機の利用方法は各学科で規則をつくります。利用方法については各学科の教員に問い合わせてください。

２.４　もっと知りたいとき・困ったときは

■相談・質問先

本学では、規程やマニュアル類をまとめたクラウド型共有フォルダ「ファイル共有（Microsoft365）」（ushimaneacjp.sharepoint.com/pub/）を設置しています。

Microsoft 365 をはじめ、各種ソフトウェアの操作方法に関するマニュアルも掲載していますので、利用方法に迷ったときや機能の詳細を確認したいときには、ぜひ「ファイル共有」をご参照ください。

① 所属学科の教員：アプリの使い方や設定などは、所属する学科の先生に聞いてみましょう。
② 管理課 情報担当：ネットワークに接続できないなどは、情報担当へお声かけください。
（事務室窓口、メールなど）

■個人 PC 修理中の代替機

個人 PC 修理期間中は、期間中の代替機として貸出するノート PC を用意しています。申請が必要ですので、貸出期間の見通しや、学生証をお持ちのうえ、管理課へお越しください。

2.5 パスワードの変更手順

「ファイル共有（Microsoft365）」（ushimaneacjp.sharepoint.com/pub/）に各種マニュアルがありますので、そちらをご確認ください。

① 学内の大学 PC に大学ユーザー名でログインしている時

（ファイル共有＞３キャンパス＞I_学生・教職員共有＞03_Microsoft365 関連＞
m365_学内アカウントパスワードの変更方法（学内で行う場合）.pdf）
※右記 QR コードからもご確認いただけます。

② 自分の PC から変更する時

（ファイル共有＞３キャンパス＞I_学生・教職員共有＞03_Microsoft365 関連＞
m365_学内アカウントパスワードの変更方法.pdf）
※右記 QR コードからもご確認いただけます。

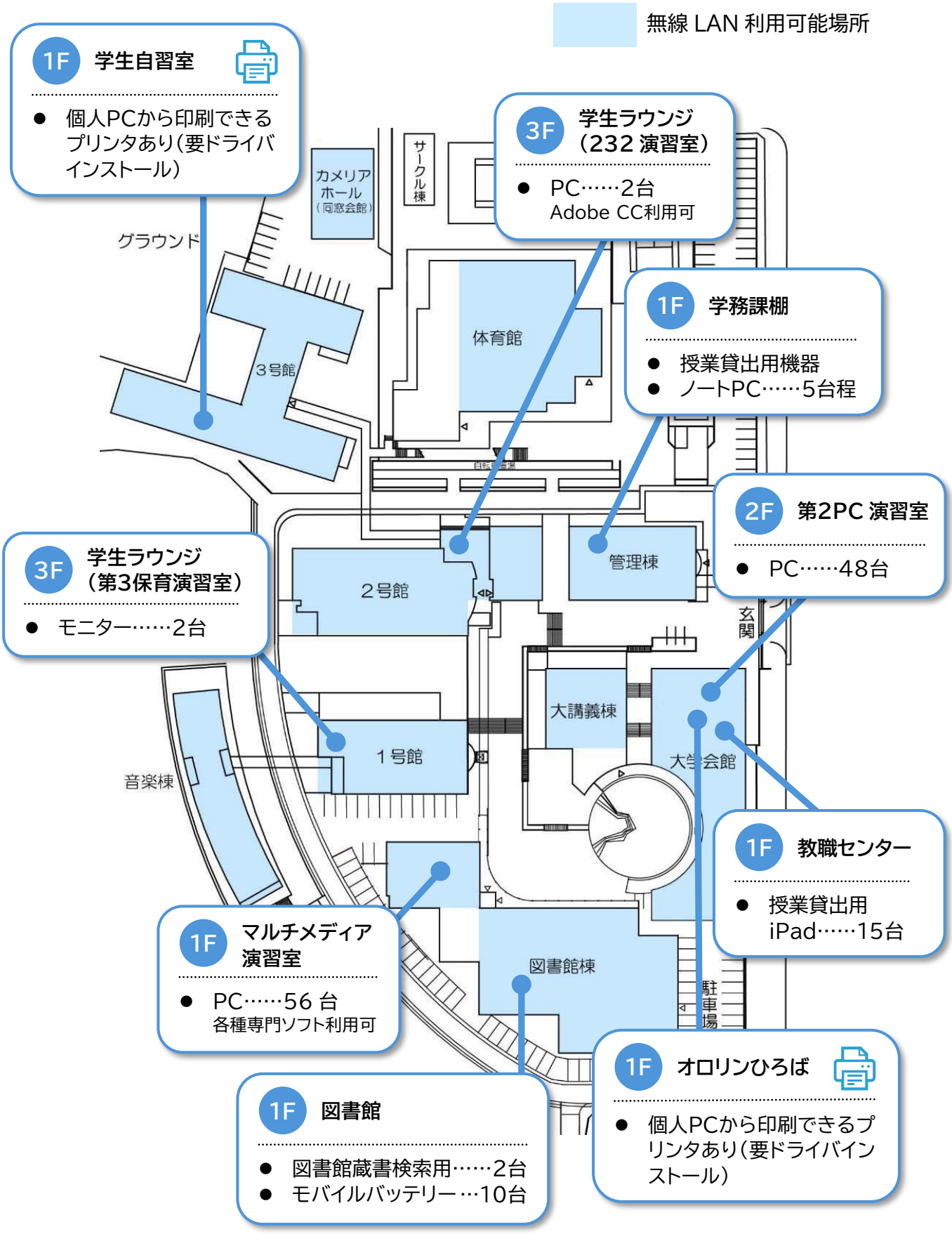
2.6 各室の利用時間およびコンピューターマップ

■各施設の利用時間・管理方法

部　屋　名 （PC設置台数）		学生の利用時間		端末責任者
		平　日	休　日	
図書館棟 IF	マルチメディア演習室 （56）	8:00～21:00 **（授業優先※1）**	使用不可 ✕	システム 管理者
大学会館 2F	第2PC演習室 （48）	8:00～21:00 **（授業優先※1）**	使用不可 ✕	システム 管理者
3号館 IF	学生自習室 （プリンタのみ）	8:00～21:00	使用可※2	システム 管理者
各学科	各学科演習室	8:00～21:00	各学科教員に 確認すること	各学科が決める 端末責任者

※１：授業で使用していない時間は、学生の自由利用を認める。教室入り口で授業での使用状況を確認すること。
※２：自習室を休日利用の際は、警備員室に声をかけること。

コンピューター配置＆無線 LAN マップ



第３章　　大学 PC 設置演習室（マルチ・第 2PC）の共通手順

大学の PC が設置されている２つの演習室は、いずれも授業が行われていない時間は、自由に使って構いません。ただし、授業以外で使う場合は、時間割を確認し、演習室が空いていることを確認してから入室するようにしましょう。みんなで使う部屋です。後に使う人のことを考えて、故障した場合などは放置しないようにしてください。

３.１　PC の起動と終了（共通）

■電源オンとシステムへのサインイン

各 PC 実習室に大学が設置する PC を使うために最初に行う作業が、電源ボタンを押して PC を起動し、システムに［サインイン］することです。

PC 本体の電源ボタンを押すと本体の電源が入り、画面（モニター・ディスプレイ）も自動的に電源が入ります（入らない場合は、モニターの電源ボタンに触れてオンにしてください）。画面には、メーカーロゴ表示ののち、パソコンの OS（オペレーティングシステム）である Windows１１ が起動し、サインイン画面が表示されます。

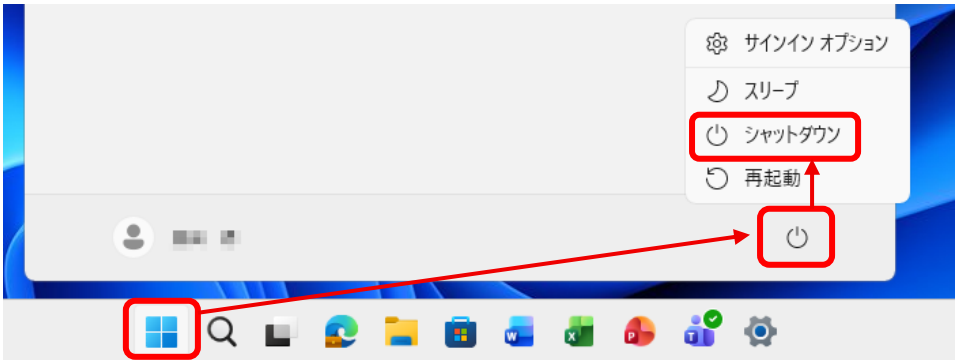
各自の［ユーザー名］と［パスワード］を正しく入力し、→ ボタンを押してください。

ユーザー名	パスワード
e＋ 学籍番号 （例）学籍番号が XXXXXXX ならユーザー名は eXXXXXXX	自分で決めた 10 文字以上のランダムな英数字

■終了（シャットダウン）

PC の利用を終了し電源オフにする作業を［シャットダウン］と呼びます。このシャットダウン操作をせずに本体の電源ボタンを押して切ることはしないでください（故障の原因になります）。

① 作業していたアプリケーションソフト（Word など）をすべて終了してください。
② 画面下の（ウィンドウズ）ボタンをクリックし、現れたメニューの中から（電源）ボタンをクリックし、さらに表示されたメニューから「シャットダウン」を選択してください。
③ これでシャットダウン完了です。正常に終了処理がなされれば、PC 本体（およびディスプレイや周辺機器）の電源は自動的に切断されます。



3.2 プリンタとスキャナの利用（PC 演習室 共通）

各演習室には、プリンタが設置されていますので、その使い方を説明します。

■基本的な使い方

各 PC には初期プリンタ（デフォルトプリンタ）が指定されていますので、原則そのプリンタを利用してください。

室内の他のプリンタに変更して印刷することもできます。デフォルトプリンタが印刷不能の際などに変更してください。プリンタ名は当手引のレイアウト図か、プリンタ本体のシールで確認をしてください。

プリンタで印刷するとユーザー名（学籍番号）もヘッダーに印刷されますので、自他の印刷物を見分ける手がかりとし、他の人の印刷物と間違えないように気をつけてください。

用紙やトナーは大学が用意しています。必要な範囲・部数で印刷すること、モノクロ（白黒）でよいものは、モノクロで印刷するよう心がけ、用紙やトナーの効果的な利用にご協力をお願いします。

職員が適宜補充していますが、不足・不明の際は、管理課までご連絡ください。

■プリンタ名と種別

プリンタ名は、以下の規則で命名され、本体にシールが貼られています。プリンタを指定する際の参考にしてください。

XXXX-〇〇△△

演習室名	プリンタ台数	プリンタ名		
		ＸＸＸＸ その演習室を示す文字列	○○ CP：カラー	△△ プリンタNo.
マルチメディア	４台	MMUL	CP	０１～０４
第２PC	２台	MPC	CP	０１・０２

共用プリンタ利用心得

● ３大エラーとその対応方法を知ろう

見分け方：プリンタ本体の状態確認ボタン（下記写真①）を押す

No	エラー	対応方法
1	紙切れ	紙を補給してください。部屋に紙の在庫ない時は管理課へ連絡。
2	サイズ誤り	そのデータをプリンタ本体で削除してください。 （プリンタにない紙サイズのデータは印刷されません）
3	紙詰まり	プリンタ本体画面の指示に従って用紙を取るか、管理課へ連絡。 （湿気の多い時期に頻度上昇）
番外	トナー切れ	３大エラーが表示されていない場合は稀に原因になっているので、管理課へ連絡。（交換が近い旨の表示は詰まりの原因ではありません）

● 出力されなかったときは、プリンタ本体でデータ削除してから退室しよう

印刷ボタンを押したら、そのプリンタから印刷されるまで自分のデータはプリンタ本体にずっと保管されているものと思ってください。プリンタの詰まり解消後に、保管されていたデータが印刷され、自分の個人情報やレポートなどが、教室に長時間放置され、他の人に見られる恐れもあります。共用プリンタ利用者のマナーとして、また、個人情報保護の点や省資源の点からも、後始末の習慣をぜひつけてください。

■データ削除方法：（一例）

① プリンタ本体の状態確認ボタンを押す
② 画面上部のタブ「実行中ジョブ」を押す
③ プリンタ本体にあるデータ（他の方のも）の一覧が表示される
④ ファイル名から自分のデータを特定し、選択、予約削除を押す

※次ページは留意点の詳細版です。

共用プリンタ利用の留意点

出力先を選ぼう。すでにエラーが出ているプリンタに出力すべからず

赤ランプ点灯時は、状態確認ボタンを押すとエラーの詳細がわかります。
- 用紙切れは室内に紙在庫があれば補充。放置データがあり、削除可能な場合はデータ削除
- 紙詰まりは、管理課へ連絡。これらの結果、状態が「印刷可能」となればよいです

※トナーやドラム交換は目立って表示されても警告期間が長く、印刷できることが多いです

データ側とプリンタ側の用紙サイズを一致させよう

プリンタには、A４・A３の用紙がセットされています。データ側で他サイズの用紙が指定されていると、プリンタに送られてから用紙サイズエラーとなり印刷されません。プリンタ本体でデータ削除をする等で、プリンタにデータが残らないようにしてください。

印刷範囲をプレビューで一度は確認しよう。かさばらない省資源印刷も活用しよう

- 印刷前はプレビュー画面を表示し、印刷内容を確認してください
- ページや画面上での選択範囲のみ等の指定ができますので、適切に印刷範囲を指定してください
- 両面印刷や、集約印刷（2 in 1 等）で用紙使用量が片面印刷に比較し、半分や 1/4 になります

白黒でもよいときはモノクロ印刷を指定しよう

同じプリンタで印刷しても、モノクロか、カラーかで、印刷コストが数倍違います。 下書き段階ではモノクロで印刷して内容を確認し、完成間近から提出物印刷の際のみカラーとする等、コスパの高い印刷にご協力をお願いいたします。

印刷ボタンは連打すべからず

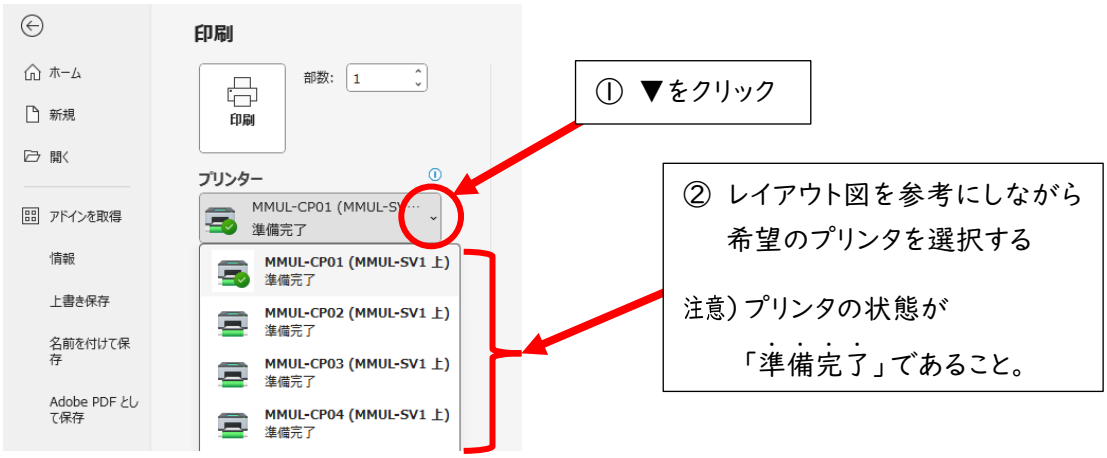
プリンタはすぐには反応しません。少し待っても印刷が始まらないときは、上記の原因（用紙やトナー切れ・紙詰まり・用紙サイズエラー等）で印刷が止まっているか、プリンタの指定誤りで室内の他のプリンタに印刷されている可能性がありますので、プリンタ本体で確認をしてください。

プリンタが PC 上にないときは、PC に再サインイン。５分程度なにもせずに待とう

共用 PC のある演習室のプリンタは自動でパソコンが認識して使えるようになっています。しかし、時にそれがうまくできず、プリンタがパソコンから選べないという時が稀にあります（特にマルチメディア演習室）。その時は、自分でプリンタを探す、設定するのではなく、PC から一度サインアウトし、再サインイン後、５分程度何もせずに待ってみてください。

■任意のプリンタへの出力

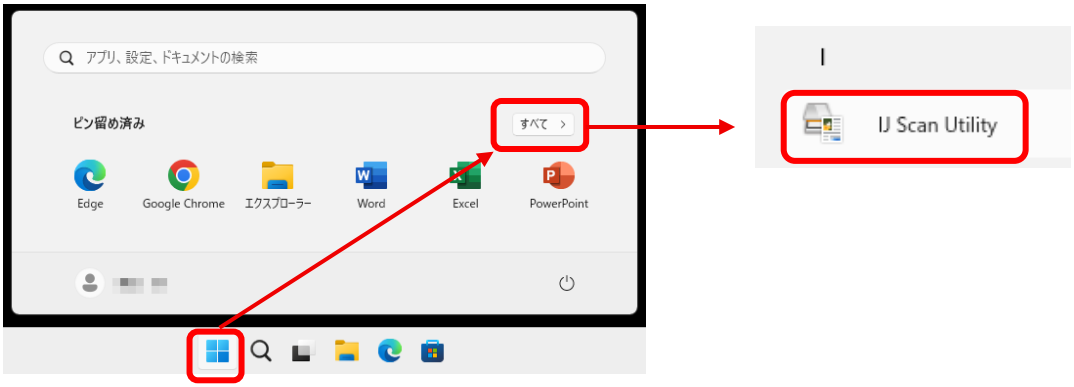
デフォルトプリンタ以外から出力したいときには、印刷プレビューボタンやメニューから[印刷]を選んでください。以下のような印刷設定画面が現れますので、プリンタを変更して印刷ボタンを押してください。



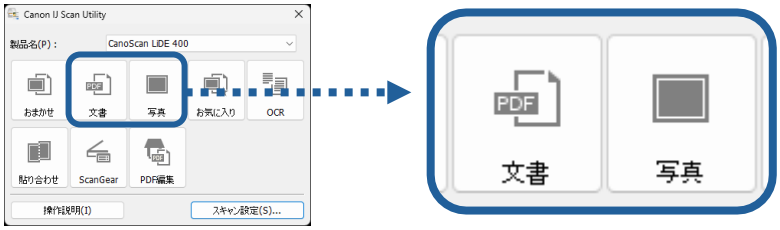
■イメージスキャナの利用

マルチメディア演習室は、PC２台に１台の割合でスキャナが設置されています。
【収納箇所】　マルチメディア演習室：PC 本体の棚の最下段

① 原稿をスキャナにセット
② 「IJ Scan Utility」を起動します。(Windows ボタン ＞ すべて ＞ IJ Scan Utility)



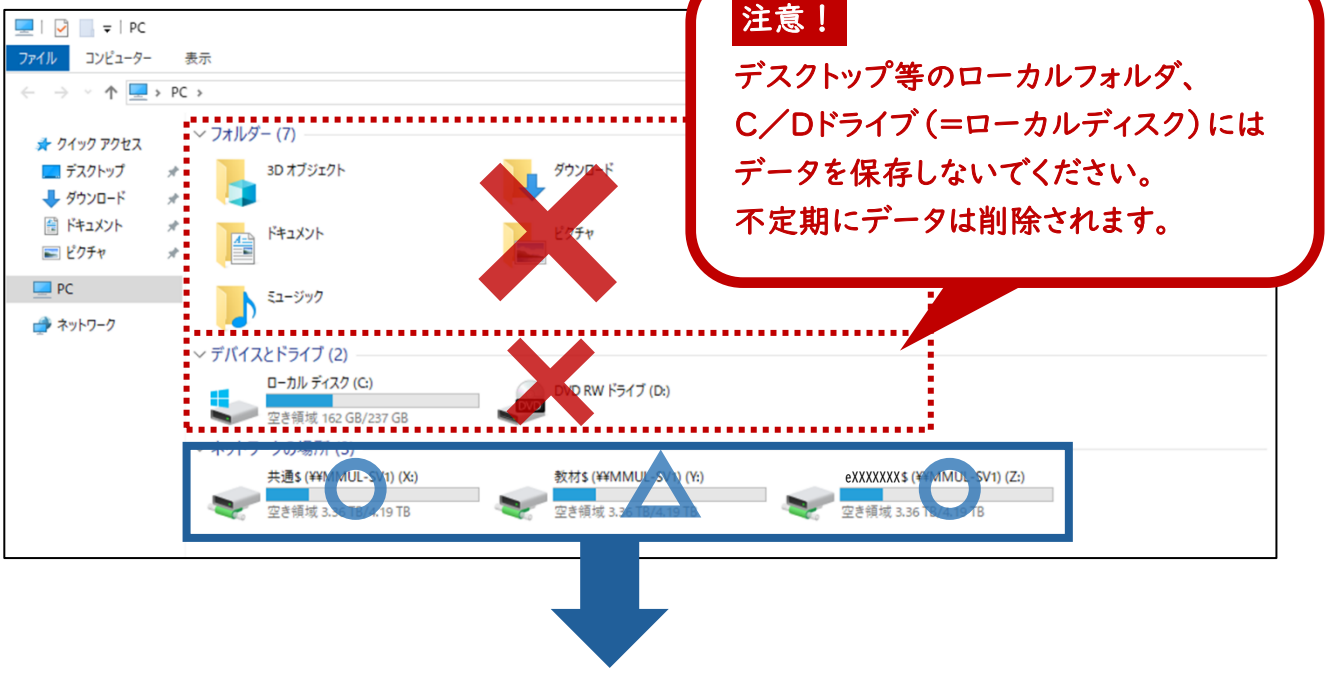
③ PDF でスキャンしたい場合は「文書」、画像の場合は「写真」をクリックします。



④ スキャンが始まると『スキャン中』の画面が表示されます。
⑤ 各ユーザーの「ドキュメントフォルダ」に PDF データが保存されます。

3.2 コンピュータのドライブ構成とファイルの保存（PC 演習室共通）

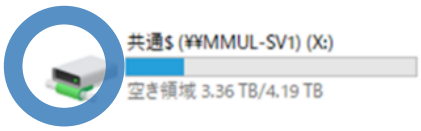
デスクトップの左上にある［PC］と書いてあるアイコン  をダブルクリックしてください。下のような画面が表示されます。



注意！

デスクトップ等のローカルフォルダ、
C／Dドライブ（=ローカルディスク）には
データを保存しないでください。
不定期にデータは削除されます。

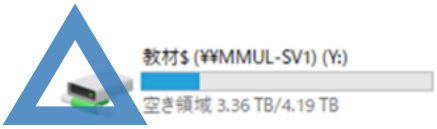
共通ドライブ（X:）（各演習室共通）



サーバ上の共通ドライブです

誰もが読み書き可能

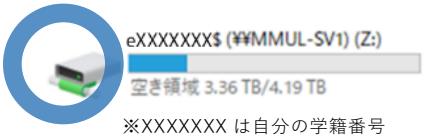
教材ドライブ（Y:）（各演習室共通）



サーバ上の教材ドライブです

【学生】読み**のみ**　【教員】読み書き可

個人ドライブ（Z:）（各演習室共通）



※XXXXXXX は自分の学籍番号

サーバ上の個人用ドライブです

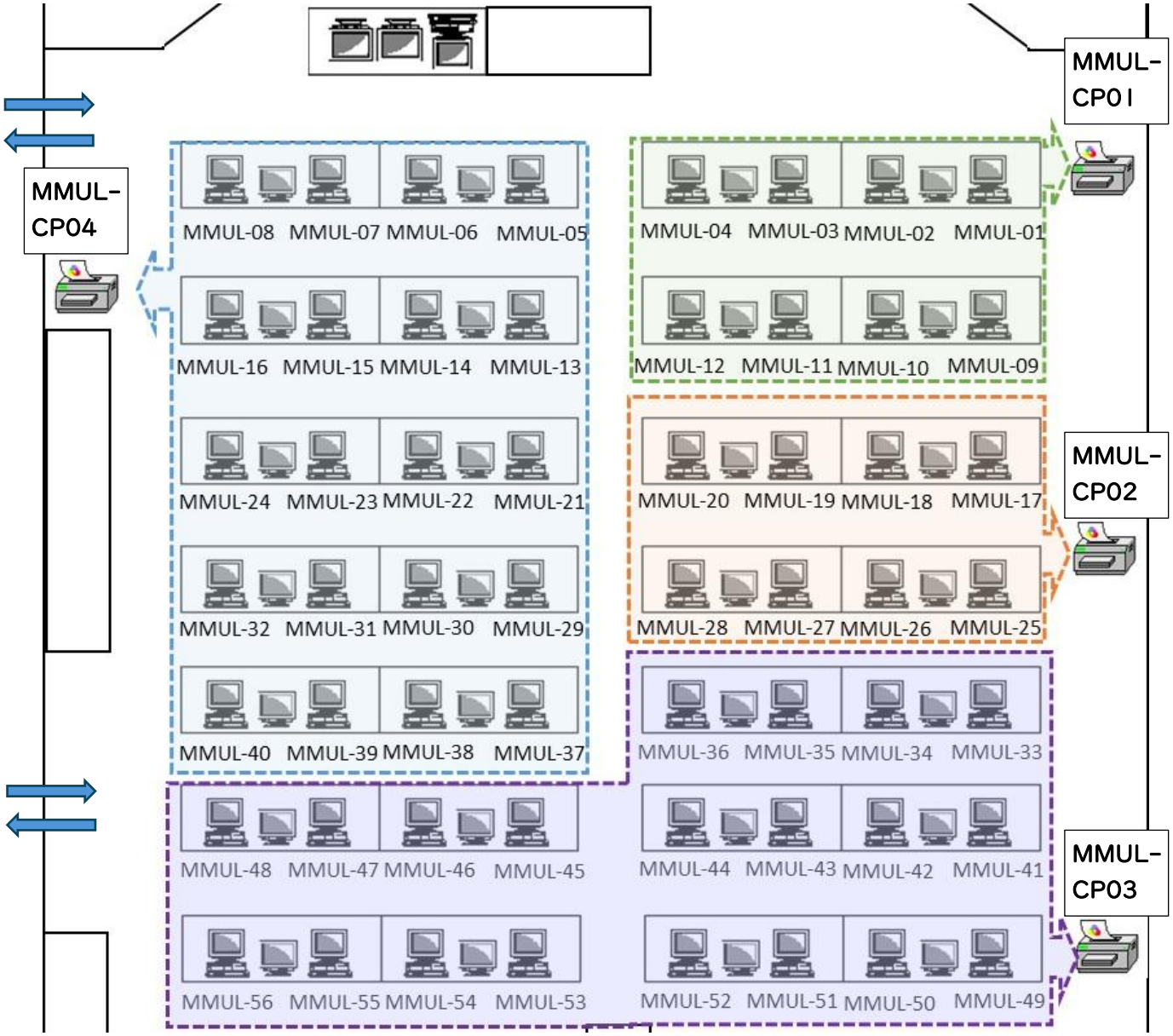
各自読み書き可能

第４章　　マルチメディア演習室の利用

図書館棟　１Ｆ

４.１　レイアウトと、デフォルトプリンタグループ

マルチメディア演習室には教師機が１台、学生機が 56 台あります。



●最寄りのプリンタ（デフォルトプリンタ）：上記図の点線に対応

ＰＣ名（MMUL-△△）	プリンタ名	備　　考
０１～０４・０９～１２	MMUL-CP０１	カラーレーザー
１７～２０・２８～２５	MMUL-CP０２	カラーレーザー
３６～５６	MMUL-CP０３	カラーレーザー
０５～０８・１３～１６・２１～２４・２９～３２・３７～４０	MMUL-CP０４	カラーレーザー

4.2 アプリケーションソフトについて

マルチメディア演習室のコンピュータには、次の表に示すようなさまざまなアプリケーションソフトがインストールされており、授業や自習などで利用することができます。

アプリケーションソフトの中には、演習室内の全てのコンピュータに入っている(インストールされている)ものもあれば、一部のコンピュータにだけインストールされているものもあります。

分　類	アイコン	備　考
統合ソフト (MS-Office Pro Plus 2024)	Word Excel PowerPoint Microsoft Teams etc.	全台 （Word、Excel、PowerPoint など）
インターネットブラウザ (Google Chrome、Microsoft Edge)	Google Chrome Microsoft Edge	全台
Creative Cloud コンプリート (Photoshop、Illustrator、InDesign など)	Adobe Photoshop 2025 Adobe Illustrator 2025 Adobe InDesign 2025 Adobe Premiere Pro 2025 etc.	MMUL-01～40
Media Player Classic - Black Edition	MPC-BE x64	全台

各PCモニターの台座に、そのPCで利用可能なソフトウェアを示すシールを貼付しています。(上表のうち、台数限定のソフトウェアが対象)

Adobe Creative Cloud の利用について

Adobe Creative Cloud を利用する際には、ユーザー認証が必要になります。

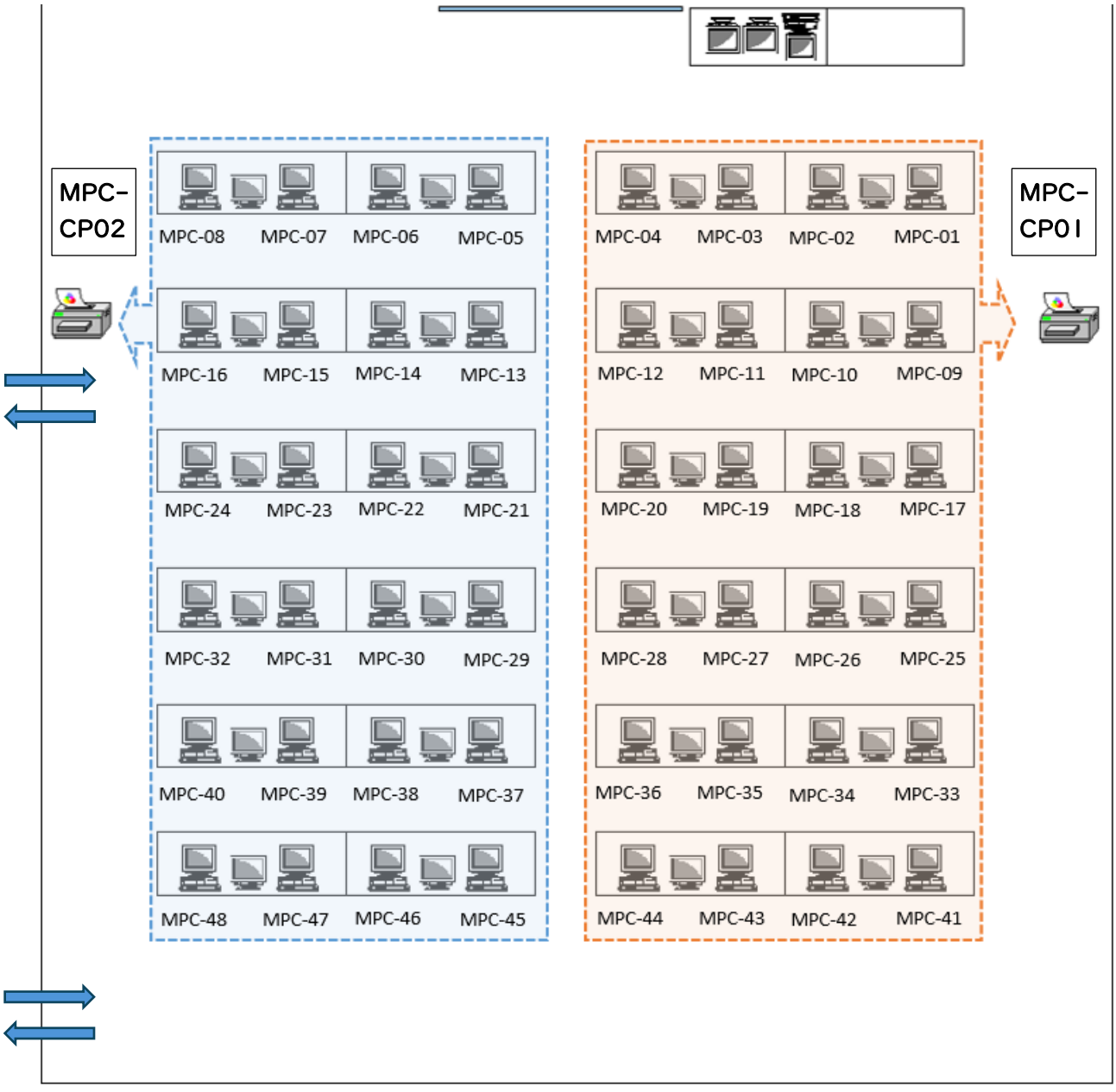
ソフトウェアを起動すると以下の画面が表示されますので、**学内メールのアドレスとパスワードを入力**し、認証を行ってください（Office365 にサインインする時と同様に多様素認証を求められます）。認証完了後、ソフトウェアが利用できるようになります。

第５章　　第２PC 演習室の利用

大学会館 2F

５.１　レイアウトとデフォルトプリンタグループ

第２PC 演習室には教師機が１台、学生機が 48 台あります。

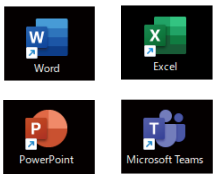
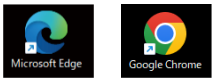


●最寄りのプリンタ（デフォルトプリンタ）：上記図の点線に対応

クライアント（MPC-△△）	最寄りのプリンタ	備　　考
教卓に向かって右手半分の PC	MPC-CP01	カラーレーザー
教卓に向かって左手半分の PC	MPC-CP02	カラーレーザー

5.2 アプリケーションソフトについて

第２PC 演習室のコンピュータには、次の表に示すようなアプリケーションソフトがインストールされており、授業や自習などで利用することができます。

分　類	アイコン	備　考
統合ソフト (MS-Office Pro Plus 2024)	 etc.	全台 （Word、Excel、PowerPoint など）
インターネットブラウザ (Google Chrome、Microsoft Edge)		全台
IBM SPSS Statistics Ver30		全台

第６章　　自習室の利用

自習室にはプリンタが設置されています。

６.１　３号館自習室

無線 LAN 接続が可能な自習室です。プリンタが２台あり、無線 LAN を経由して自分のパソコンから印刷することが可能です。印刷をするためには、パソコンにプリンタドライバのインストールが必要ですので、自習室に掲示してある設定方法を確認し利用してください。

■３号館自習室のプリンタ（カラープリンタ　１台、モノクロプリンタ　１台）

プリンタ	備　　考
JISCP1	カラーレーザー
JISPRT1	モノクロレーザー

※印刷時にプリンタの選択を間違えないように注意してください。
※プリンタドライバダウンロードやインストールの際に、PC が警告を出すことがありますが、安全なファイルなので、拒否せず先に進んでください。

■自分のパソコンから印刷する方法

「ファイル共有（Microsoft365）」（ushimaneacjp.sharepoint.com/pub/）にマニュアルがありますので、そちらをご確認ください。

（ファイル共有＞松江キャンパス＞1_学生・教職員共有＞
管理課より＞３号館１Ｆ学生自習室｜プリンタ利用方法＞
３号館プリンタ利用手順_20250220.pdf）
※右記 QR コードからもご確認いただけます。

大学会館学生ラウンジ（オロリンひろば）にも**モノクロプリンタが１台（LOUNGEPRT1）**設置してあります。こちらも自分のパソコンから印刷することが可能です。
プリンタのドライバとインストールマニュアルが「ファイル共有（Microsoft365）」にありますので、そちらをご確認ください。

（ファイル共有＞松江キャンパス＞1_学生・教職員共有＞
管理課より＞オロリンひろば｜プリンタ利用方法）
※右記 QR コードからもご確認いただけます。

第７章　　松江キャンパス学内無線 LAN（kendai）接続方法

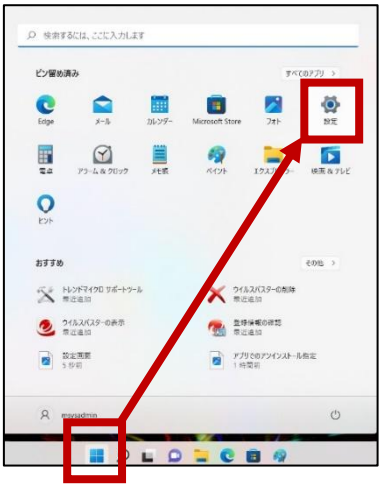
以下の方法で、各自所有のパソコン、スマートフォン等を学内無線 LAN（kendai）へ接続できます。ご使用の端末の OS のバージョンの違いなどにより設定方法が異なる場合もありますので、解説を参考にして各自設定を行うようにしてください。

対象エリア：コンピュータ MAP 参照（P９）
対　象　者：在学生、教職員（本学より学内 ID を発行された者）
重　　要：使用する機器（PC・スマホ・タブレットいずれも）には、ウイルス対策ソフトを必ず導入してください。下記設定は、上記対象エリア内で実施してください。

７.１　パソコンの接続方法（例：Windows１１）

①設定画面から、「ネットワークとインターネット」の画面を開く

画面中央左下の をクリックし、開いた画面内から （設定）をクリック。
展開した設定画面の左メニューから「ネットワークとインターネット」をクリック。



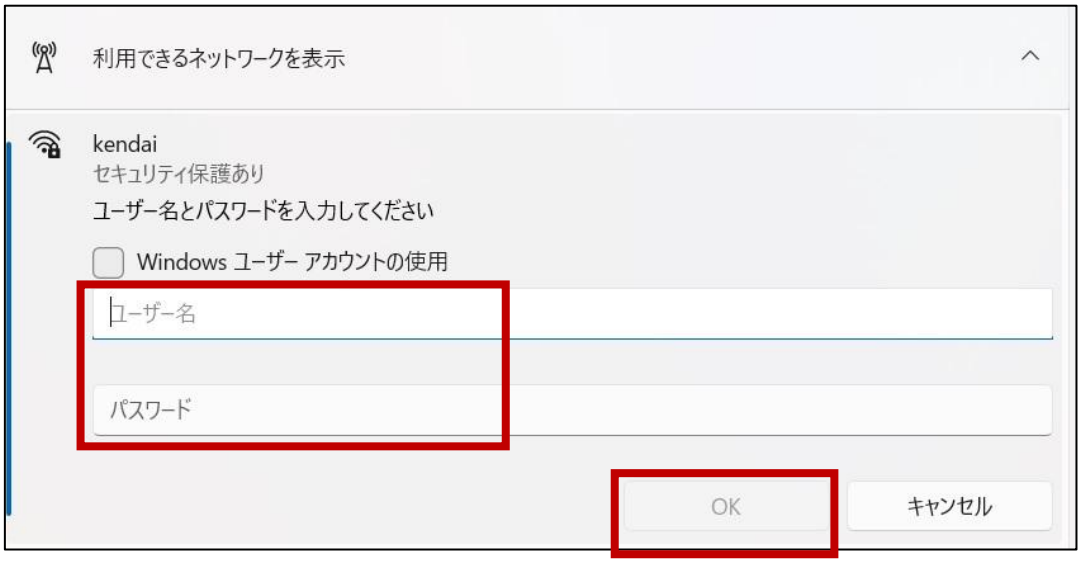
②kendai 無線の接続画面まで移動する

「ネットワークとインターネット」画面から
右メニュー　「Wi-Fi」→「利用できるネットワークを表示」→表示された「kendai」をクリック。

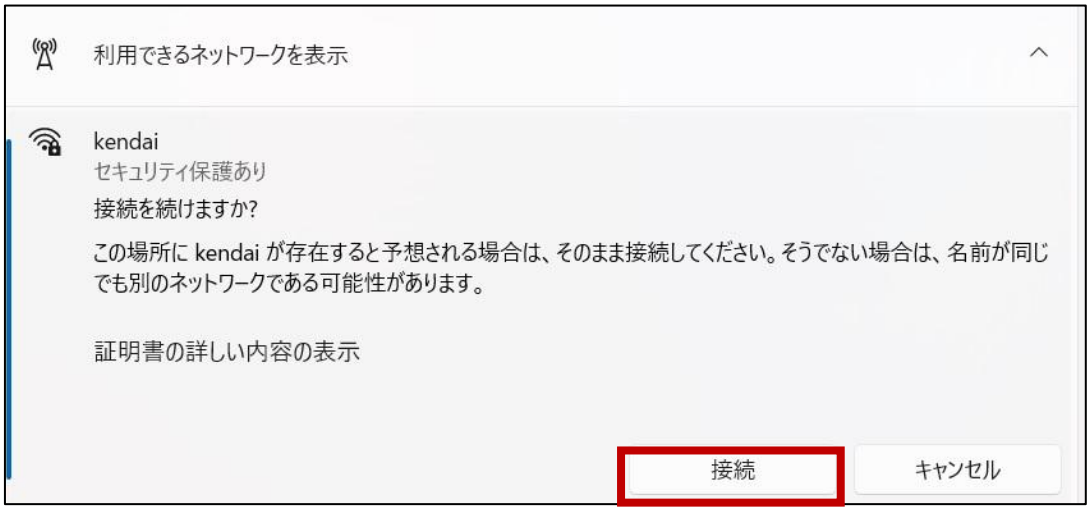
※Wi-Fi がオフの場合は、オンにすること。（自動的に接続にチェックありのほうが便利）

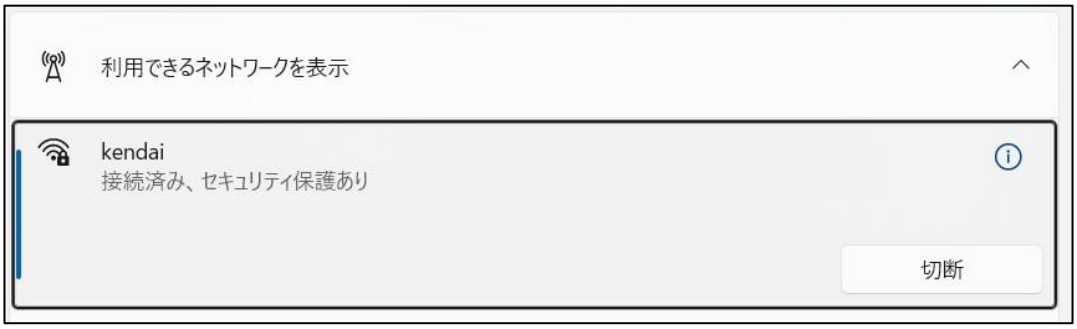
③認証画面になったら、大学のユーザーID（e＋学籍番号）とパスワードを入力し、OK ボタンを押す

※Windows ユーザーアカウントの使用 はチェックしない。



④接続継続の画面が出る際は、「接続」ボタンを押して処理継続し、接続済み表示を確認する





7.2 スマートフォン、タブレットの接続方法

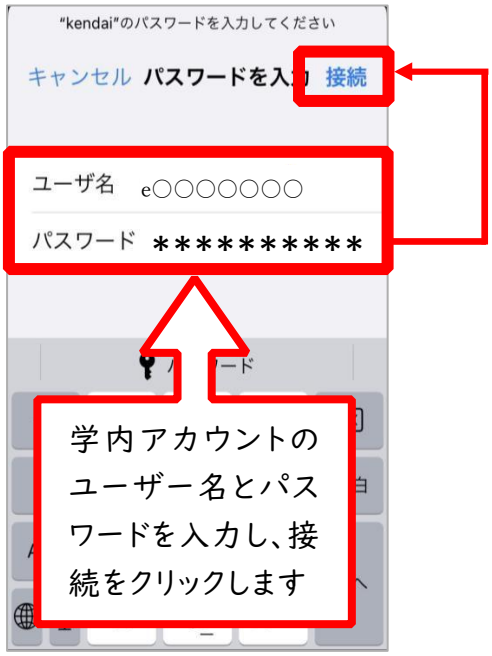
学内ネットワーク接続方法［iPhone］

①

②

③

④

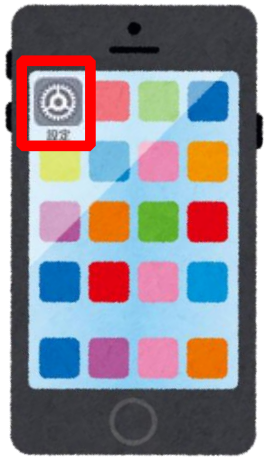


⑤

⑥

学内ネットワーク接続方法［Android］

①

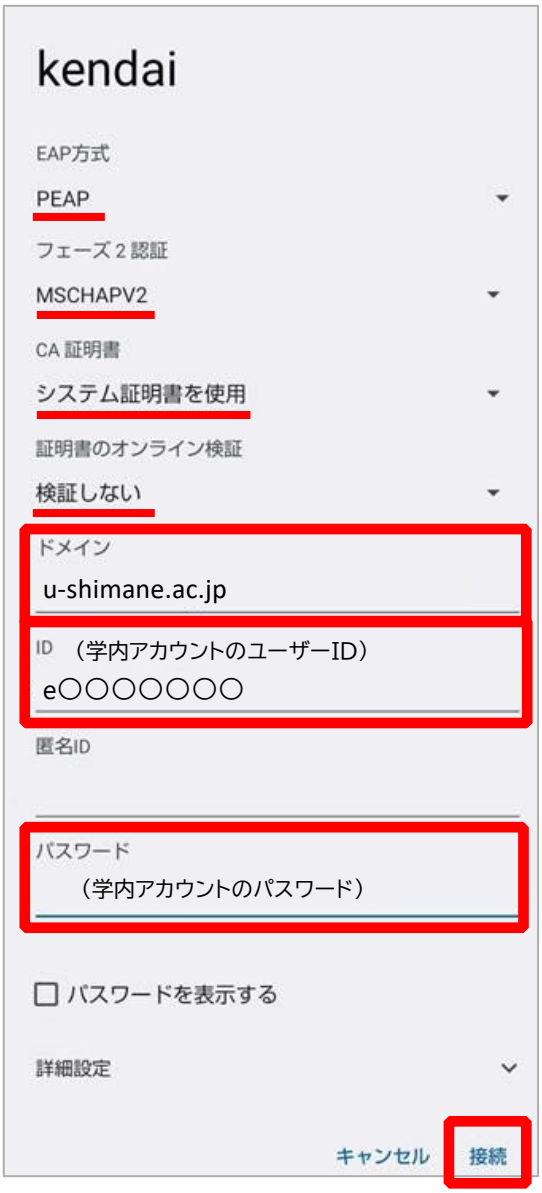


②

③

④

⑤



⑥

第８章　　Microsoft365 利用マニュアル

「ファイル共有（Microsoft365）」（ushimaneacjp.sharepoint.com/pub/）に各種マニュアルがありますので、そちらをご確認ください。

■Microsoft365　多要素認証設定

（ファイル共有＞３キャンパス＞I_学生・教職員共有＞03_Microsoft365 関連＞
Microsoft365_多要素認証設定手順.pdf）
※下記 QR コードからもご確認いただけます。

■Outlook 版 学内メール基本操作

（ファイル共有＞３キャンパス＞I_学生・教職員共有＞03_Microsoft365 関連＞
学内メール（Outlook）＞Office365_学内メール基本操作編.pdf）
※下記 QR コードからもご確認いただけます。

■Teams 活用マニュアル

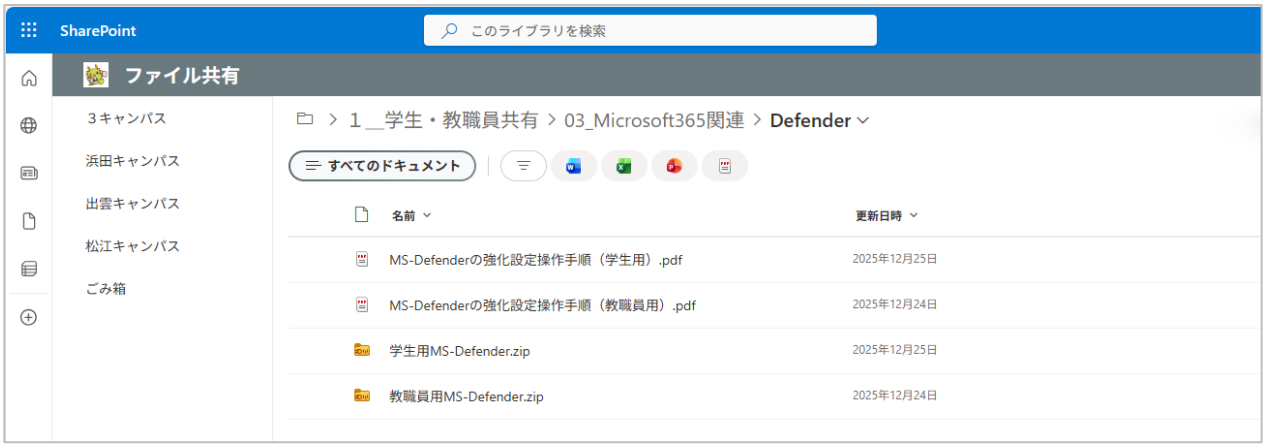
（ファイル共有＞３キャンパス＞I_学生・教職員共有＞03_Microsoft365 関連＞
Teams&Stream＞MicrosoftTeams 活用マニュアル_学生用.pdf）
※下記 QR コードからもご確認いただけます。

第９章　　その他必要事項

９．１　Microsoft Defender の強化設定

Windows１１に標準搭載されている Microsoft Defender は、初期状態では簡易的な設定のみが有効になっています。「ファイル共有（Microsoft 365）」内にある Microsoft Defender の強化設定操作手順をご確認のうえ、Microsoft 365 の有償セキュリティ機能を有効化し、ご自身の PC をマルウェアやネットワーク上の脅威からより強固に保護してください。

以下からご確認いただけます。
（ファイル共有＞３キャンパス＞１_学生・教職員共有＞03_Microsoft365 関連＞Defender）

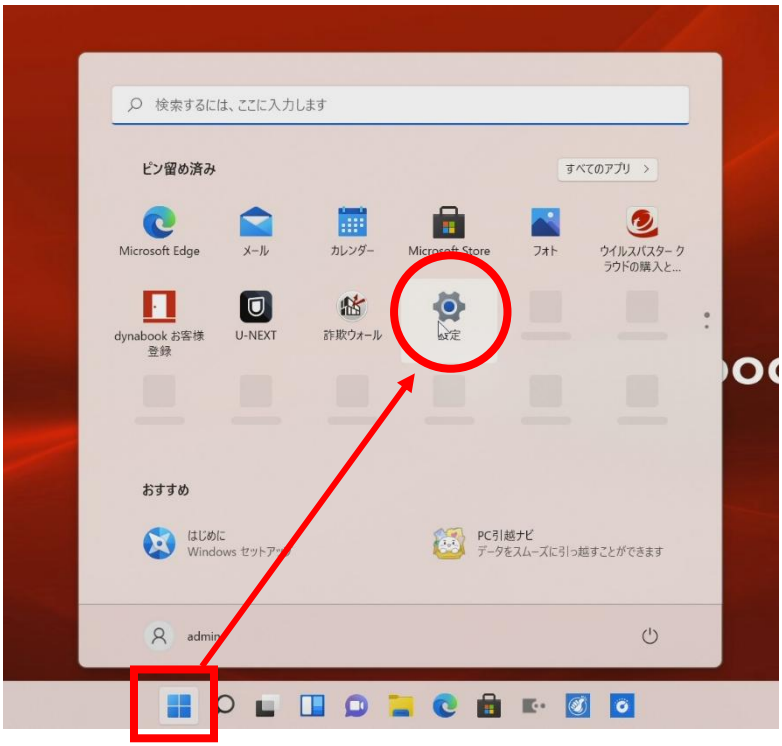


※右記 QR コードからもご確認いただけます。

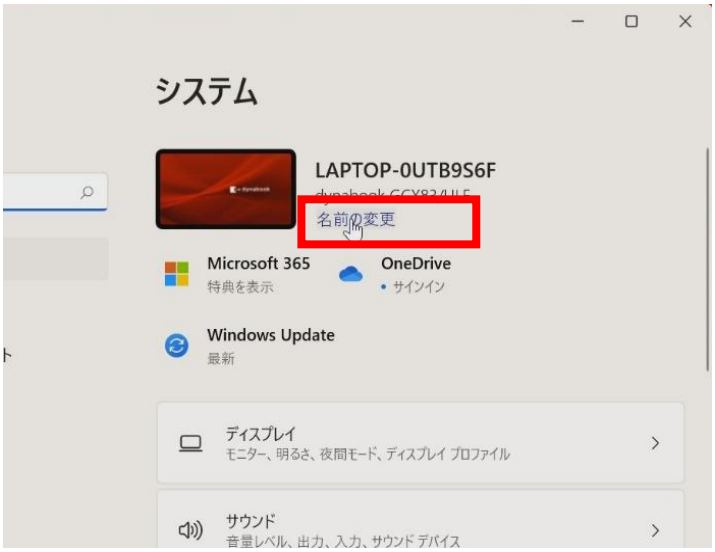
9.2 個人 PC のコンピューター名変更方法

セキュリティ対策の一環として、大学のネットワークをどなたの機器が使っているか早めに把握できるようにするため、大学の無線 LAN に接続する個人の PC について、下記により、コンピューター名をご自身の大学ユーザー名「e＋学籍番号」に変更をお願いいたします。

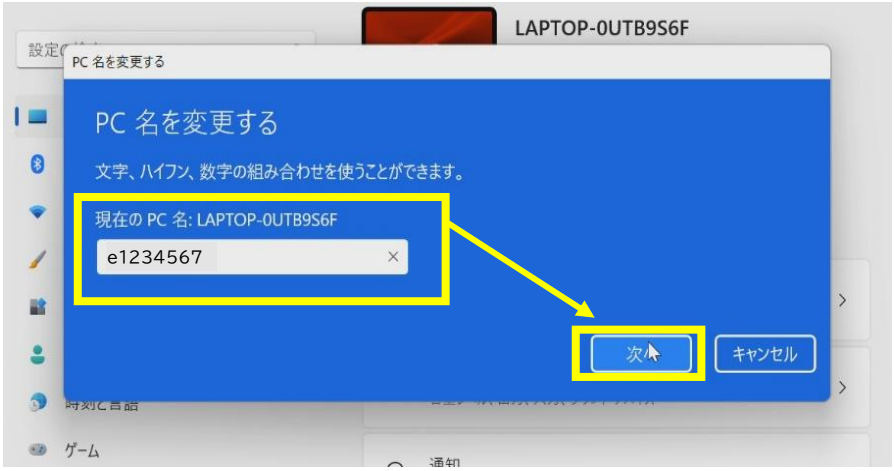
① Windows メニューを開き、【設定】をクリックする。



② 【名前の変更】をクリックする。



③　大学のユーザー名「e＋学籍番号」を入力し、【次へ】をクリックする。（例：e1234567）



④　【今すぐ再起動】をクリックする。

9.3 USB メモリについて

≪重要≫ USB メモリについての注意点

■個人情報の保護について

近年 USB メモリからの情報流出が多発しています。本学でも紛失や学内のパソコンに挿し忘れ、机に置いたままの USB メモリの届け出がたくさんあります。くれぐれも個人情報などが記載されたものを保存した USB メモリは扱いに注意してください。

■USB メモリを媒体としたコンピュータウイルスについて

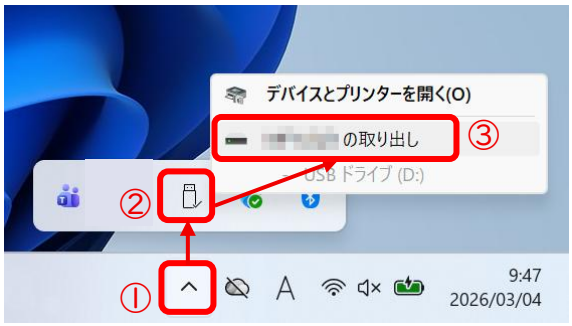
USB メモリから感染するコンピュータウイルスが、流行しています。このウイルスは感染したパソコンに USB メモリを挿すと即座に感染し、さらに感染した USB メモリを他のパソコンに挿した瞬間、そのパソコンにも感染するという仕組みです。ウイルスに感染したパソコンは、データを盗みとられたり、不正サイトに誘導されたりと様々な危険があります。

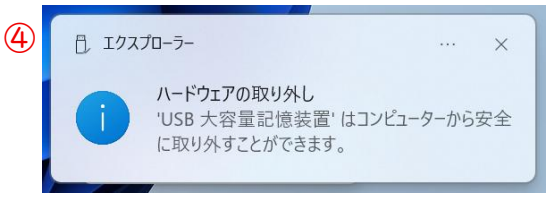
大学のパソコンには全台ウイルス対策ソフトが導入されていますので、ウイルス感染した USB メモリを挿入すると検知しますが、感染元を駆除しなければ、ウイルスを巻き散らす感染源になってしまいます。自宅・個人用のパソコンにもウイルス対策ソフトは必ず導入してください。

■USB メモリの取り外しについて

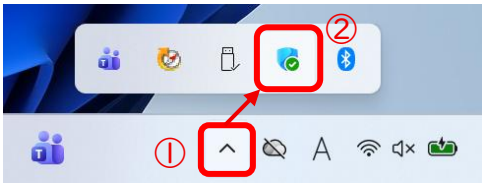
USB メモリにデータを読み書きしている時に本体から抜いてしまうと、関係ないファイルまで破損したり、USB メモリ自体が壊れてしまいます。そこで、安全に取り外すための方法を以下にご紹介します。

① パソコンの右下の∧ボタンをクリックします。
② 「ハードウェアの安全な取り外しアイコン」をクリックします。
③ ハードウェアの安全な取り外し項目が表示されるので、取り外したい USB を選択します。
④ 「コンピュータから安全に取り外すことができます」と表示が出れば本体から抜いてください。





■USB メモリのスキャン方法について

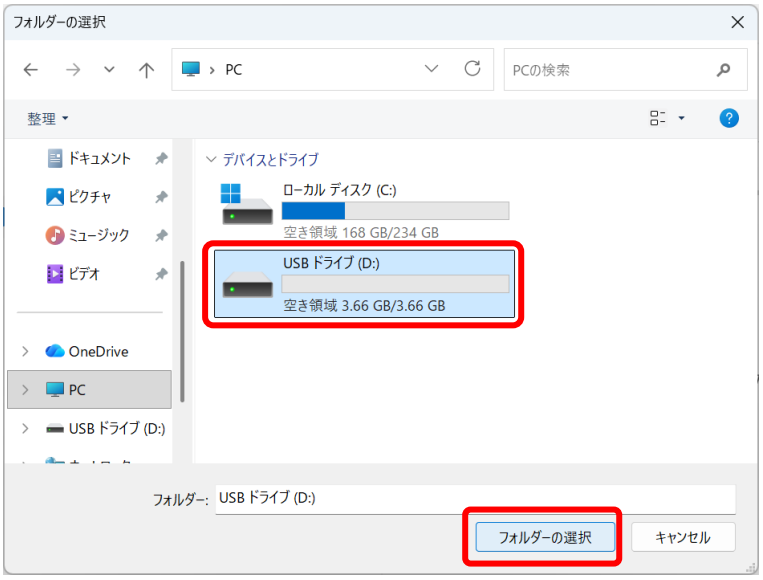


① パソコンの右下の∧ボタンをクリックします。
② 「Windows セキュリティ」をクリックします。
③ 「ウイルスと脅威の防止」をクリックします。

④ 画面を下にスクロールし、「スキャンのオプション」をクリックします。

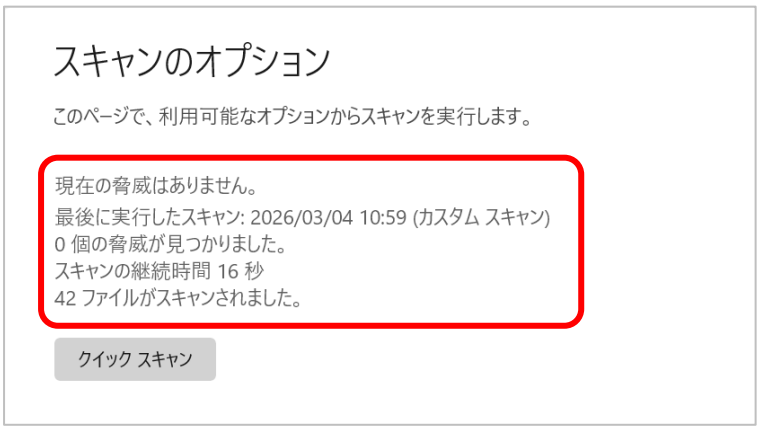
⑤ 「カスタムスキャン」をクリックして、「今すぐスキャン」をクリックします。

⑥ スキャンしたい USB メモリをクリックし、「フォルダーの選択」をクリックします。



⑦ スキャンが開始されるので、終了するまでしばらく待ちます。

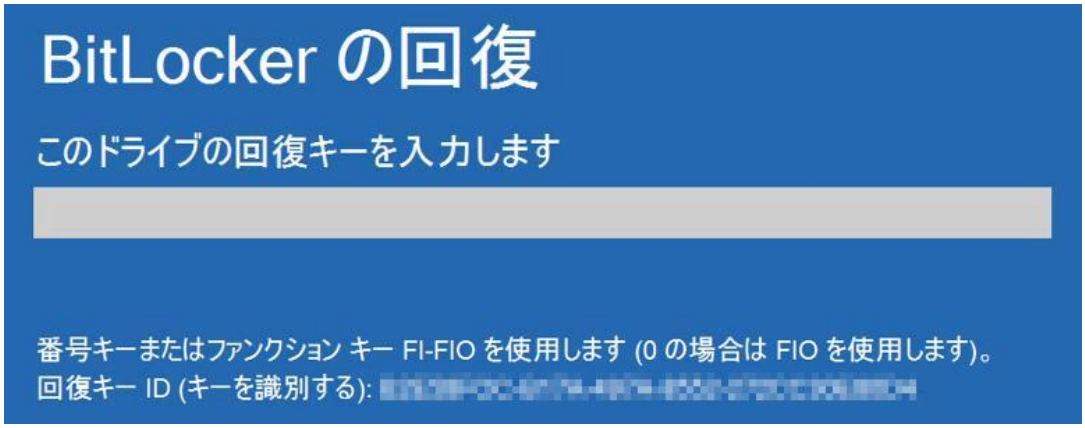
⑧ スキャンが終了すると結果が表示されます。以下の画面が表示されれば完了です。



9.4 BitLocker 回復キーのバックアップ方法について

パソコンに不具合が生じたときに、以下のような BitLocker の回復キーの入力を求められる場合があります。このとき、回復キーがわからないと、パソコンを初期化する必要があります。

そのため、以下の手順を行い、回復キーを Microsoft365 上にバックアップしておいてください。

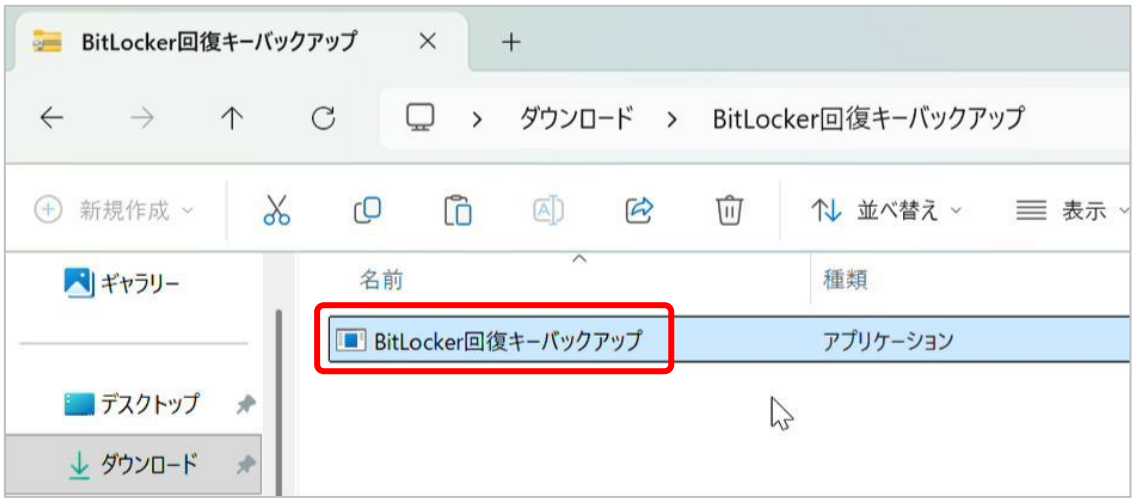


■回復キーのバックアップ

① 「ファイル共有（Microsoft365)」(ushimaneacjp.sharepoint.com/pub/）から【3 キャンパス ＞ I_学生･教職員共有 ＞ 03_Microsoft365 関連 ＞ Microsoft 365 Apps ＞ BitLocker 回復キーバックアップ.zip】をダウンロードしてください。

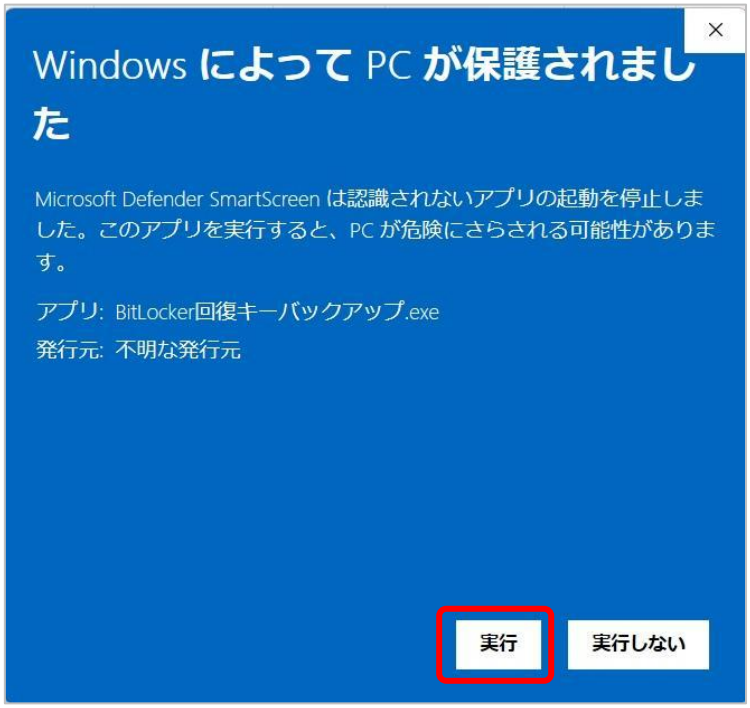
② ダウンロード後、「ファイルを開く」をクリックします。

③　「BitLocker 回復キーバックアップ」をダブルクリックして実行します。



④　次の画面が表示された場合は、「詳細情報」をクリックします。

⑤　「実行」をクリックします。



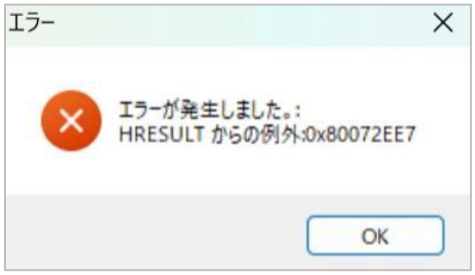
⑥　「はい」をクリックします。

⑦　「バックアップ成功： C:」と表示されれば完了です。「OK」をクリックしてください。

もし、エラーが出る場合は、以下の点を確認して、「BitLocker 回復キーバックアップ」を実行してみてください。

・インターネットに接続されていること。

・Teams アプリを起動し、自分のユーザーでサインインできること。

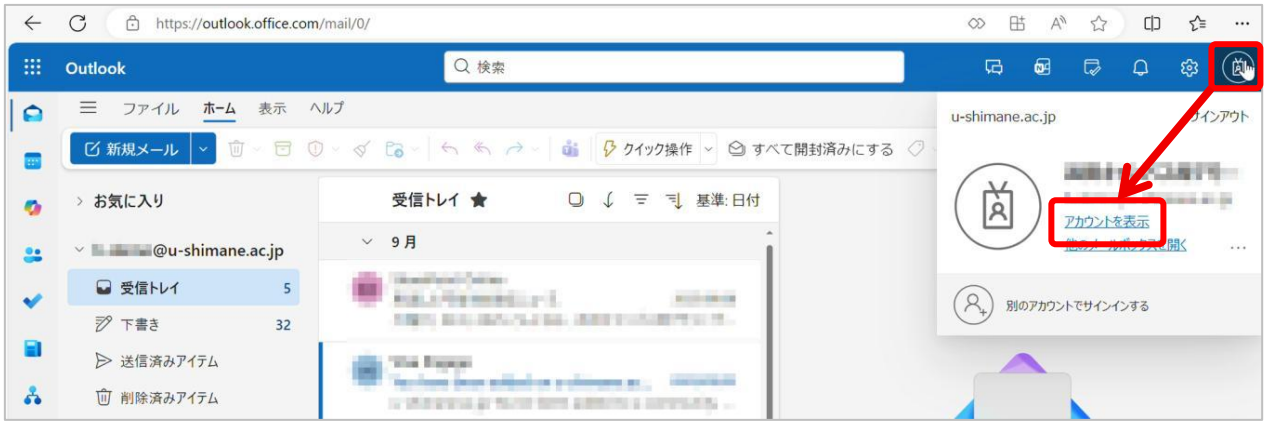


もし以下のエラーが表示された場合は、各キャンパスのシステム管理者までお問合せください。

バックアップした回復キーの確認

取得した回復キーは以下の手順で確認することができます。

① 学内メールを開きます。
画面右上のアカウントのアイコンをクリックし、「アカウントを表示」をクリックします。



② 「デバイス」をクリックします。

③ 利用しているパソコン名の右にある「v」をクリックします。

④　「BitLocker のキーの表示」をクリックします。

⑤　「回復キーを表示する」をクリックします。

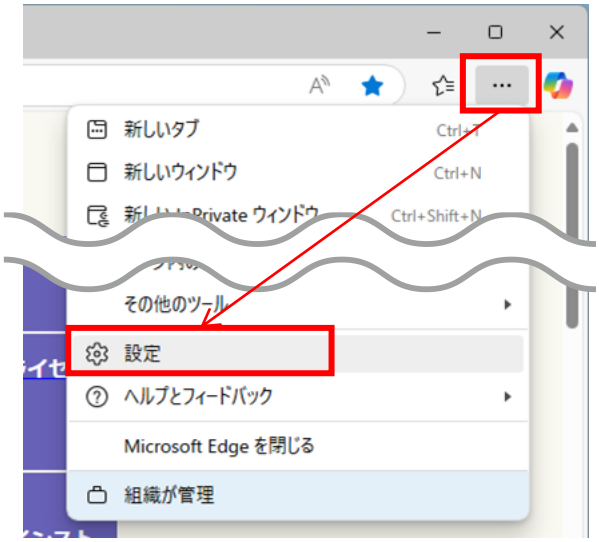
⑥　回復キーが表示されます。
もし、パソコンに不具合が生じて、回復キーを入力する必要になった場合は、別のパソコン等でこの画面を開き、この回復キーを確認してください。

９.５　ブラウザの履歴について

学校やネットカフェなど、複数の人で共用するパソコンを利用するときは、ログイン情報などの個人情報を残さないようにしましょう。不特定多数の人にメールなどの個人データを見られたり、データの複製、削除や、あなたに成りすまして情報を利用される危険性があります。

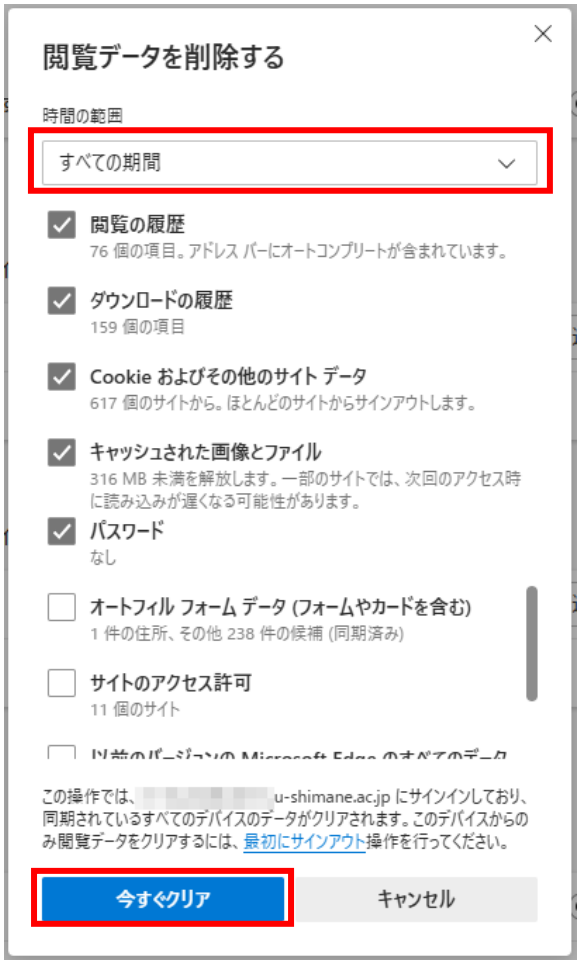
■ブラウザの履歴やログ、保存してしまったパスワードを消す方法（Microsoft Edge）

① ブラウザ右上の【…】を押し【設定】を選択する



② 左サイドメニューの【プライバシー、検索、サービス】を選択し、【閲覧データを削除する】の今すぐ閲覧データをクリアの【クリアするデータの選択】を押す

③ 時間の範囲を【すべての期間】とし、【閲覧の履歴／ダウンロードの履歴／ Cookie およびその他のサイトデータ／キャッシュされた画像とファイル／パスワード】にチェックを入れ【今すぐクリア】を選択し、終わったらブラウザを閉じる



第 10 章　情報ネットワーク利用上の規則

学内のパソコン等を利用する際は、公立大学法人島根県立大学として定める以下のガイドラインに従い、情報の取り扱いには十分注意するとともに、マナーにも気を付けること。

ガイドラインの内容は【参考資料】を参照すること。

参考資料

島根県立大学情報取扱ガイドライン

1　目的

情報の不適切な取扱いにより、情報の漏えいや改ざん等が生じた場合は、社会的信用が失墜し教育研究活動の停止も起こり得る。このガイドラインは、「公立大学法人島根県立大学情報取扱規程（平成 27 年規程第 75 号）」（以下「取扱規程」という。）に基づき、このようなリスクを回避し、情報の適切な取扱いに資することを目的とする。

2　対象

（1）対象者

このガイドラインは、公立大学法人島根県立大学が設置する島根県立大学及び島根県立大学短期大学部（以下「本学」という。）の教育研究活動及びそれに伴う諸業務（以下「大学活動」という。）に係る情報を取り扱うすべての役員及び教職員等を対象とする。

3　情報の取扱いに関する全般的な注意事項

（1）大学活動の遂行以外の目的での情報の作成、入手及び利用禁止

① 大学活動の遂行以外の目的で、情報の作成、入手又は利用を行わないこと。

② ゼミ活動、インターンシップ、実習等、学外の組織における大学活動の中で重要情報を扱う場合は、別途学部若しくは受入先の組織が定める規則に従わなければならない。

（2）情報の分類及び取扱制限に応じた取扱い

① 重要情報を自ら作成又は入手した者（以下「担当者」という。）は、当該情報について、分類及び取扱制限を文書に明示しておくこと。

② 教職員等は、明示された取扱制限に従い、当該情報をこのガイドラインに定めるとおりに取り扱うこと。

4　情報の分類及び取扱制限

（1）分類及び取扱制限の指定

① 情報の分類は次のとおりとする。

ア　重要情報

イ　一般情報

② 取扱制限は次のとおりとする。印刷、修正等の可否に関するその他の項目は必要に応じて加えてよい。

ア　共有の範囲

イ　アクセス権限（印刷／修正等の可否）

（2）分類及び取扱制限の明示方法

① 紙媒体において重要情報であることの明示等は、公立大学法人島根県立大学文書管理規程（平成 23 年規程第 37 号。以下、「文書管理規程」と言う。）の定めに従う。

② 電磁的に記録される重要情報については、参照、印刷時に分類及び取扱制限が分かるように、文章のヘッダにおいて各ページに明記すること。（記載例を参照。）

（記載例）【重要情報：○○課限り、課長以外修正不可、印刷不可】

③ 電磁的に記録される重要情報のファイル名、及び、当該ファイルを直下に持つフォルダ名は、「文

書管理規程」第6条第1項第2号、及び、第27条第3号に準じ、"【秘】"を先頭に付けること。(記載例を参照。)

（記載例）　【秘】ファイル（フォルダ）名

④　書類の特性あるいは、ソフトウェアの制限等により、上記各号を満たすことができない場合は、他の適切な方法で分類及び取扱制限を明示すること。

（3）分類及び取扱制限の変更

担当者は、次の場合に、分類及び取扱制限を変更するとともに、その内容を関係者に周知すること。

ア　元の情報への修正、追加、削除、時間の経過等により、情報の分類及び取扱制限を再指定する必要があると判断した場合。

イ　元の情報の分類及び取扱制限がその時点で不適当であり、情報の分類及び取扱制限を見直す必要があると判断した場合。

5　情報の保存と保護

（1）情報の保存における注意事項

①　ファイルサーバへ保存される情報は、公立大学法人島根県立大学文書管理規程（平成23年規程第37号）に定める「ファイル管理表」と同等に分類・整理されていなければならない。

②　滅失、消失又は改ざんにより業務の遂行に影響を与える可能性が高いと判断される情報については、バックアップ又は複写を取得すること。

ただし、定常的にバックアップされているファイルサーバ等に保存している場合は、この限りでない。

③　バックアップ又は複写された情報は、元の情報と同等に管理すること。

④　暗号化又はパスワード（以下「暗号化等」という）により情報を保護する場合は、システム管理者（基盤管理者）の指定した方法によって行うこと。

⑤　暗号化等で用いる暗号化キー又はパスワードについては、別に定める「利用者パスワードガイドライン」に従うこと。

（2）ファイルサーバや情報端末などを含む情報システムへ情報を保存する場合の保護方法

①　重要情報を保存する場合は、他の権限を持たない者が当該情報を参照、変更、削除などできないようにアクセス制御すること。

（3）外部記録媒体へ情報を保存する場合の保護方法

①　重要情報が保存された外部記録媒体は、施錠可能な所定の保管庫等に保管すること。

②　重要情報を持出しやバックアップ等の目的で外部記録媒体に保存する場合は、当該情報を暗号化等により保護すること。

③　事務職員が、外部記録媒体に情報を保存する場合は、当該機器を予め図書情報課又は管理課に登録すること。特にUSBメモリに情報を保存する場合は、当該情報が一般情報か重要情報かに関わらず、強制暗号化機能の付いた製品を使用すること。

④　教員が、USBメモリに重要情報を保存する場合は、強制暗号化機能の付いた製品を使用すること。

（4）重要情報が記載された書類の保管方法

重要情報が記載された書類を保管する場合は、施錠可能な所定の保管庫等に保管すること。

6　情報の利用

（1）情報の利用に関する注意事項

①　重要情報が保存された外部記録媒体を利用する場合は、紛失及び盗難を防止するために、必要時以外は机上等に放置しないこと。

② 必要時以外は、重要情報が記載された書類を机上等に放置しないこと。
③ 重要情報が記載された書類をプリンタ等印刷した場合は、出力トレイに放置せずに、速やかに回収すること。
④ 重要情報が記載された書類又はこれが含まれる電磁的記録を、必要以上に複製又は配付しないこと。

7 情報の提供

（1）情報の提供における注意事項
① 提供する情報及び提供先を必要最小限にとどめること。
② 電磁的記録の提供に際しては、原則 PDF 化すること。また、可能であれば、取扱い制限に応じたセキュリティ措置を施すこと。
③ 電磁的記録には、プロパティ等に作成者名、組織名、作成履歴等が残されている可能性があり、これら付加情報から情報が漏えいする場合がある。当該付加情報に不要な情報が含まれていないか確認すること。

（2）情報の提供に関する手続
① 事務職員が重要情報を学外の者に提供する場合は、当該情報を所管する所属の定めに従った上で、所定の様式により課長等の責任者に申請し、許可を得ること。教員の場合は、自らが管理する教育研究事務に関する重要情報については責任者として判断し、その他の重要情報については当該情報を所管する所属の定めに従うこと。
② 重要情報を学外の者に提供する場合は、提供先において、当該情報が、本学が付した情報の分類に準じて適切に取り扱われるよう、注意事項の伝達、適切な管理のための取決め等の措置を講じておくこと。
③ 重要情報を提供するために当該情報を持ち出す場合は、「８ 情報の持ち出し及び送信」に従うこと。

8 情報の持ち出し及び送信（以下、「持ち出し等」と言う。）

（1）情報の持ち出し等における注意事項
① 大学活動の遂行以外の目的で、情報の持ち出し等をしないこと。
② 持ち出し等をする情報は必要最低限にとどめること。
③ 持出先においても慎重に情報を取り扱い、本人の責任において適切に管理すること。

（2）情報の持ち出しに関する手続き
事務職員が重要情報を持ち出す場合は、持出先が学内・学外に関わらず、当該情報を所管する所属の定めに従った上で、所定の様式により課長等の責任者に申請し、許可を得ること。教員の場合は、自らが管理する教育研究事務に関する重要情報については責任者として判断し、その他の重要情報については当該情報を所管する所属の定めに従うこと。

（3）情報端末、外部記録媒体及び書類を持ち出す場合の保護方法
① 重要情報が保存された情報端末及び外部記録媒体（以下「情報端末等」という。）を持ち出す場合は、暗号化等により情報を保護すること。
② 重要情報が保存された情報端末等又は記載された書類を持ち出す場合は、安全確保のため、外見から機密性の高い情報であることが判からないようにする。
③ 郵便、信書便等によって、重要情報が保存された情報端末等又は記載された書類を学外に輸送する場合は、書留で送付する。
④ 重要情報が保存された情報端末等又は記載された書類を携行する場合は、封筒、書類鞄等に収め、

置き忘れ等に注意する。

（4）電磁的記録を送信する場合の保護方法

① 重要情報である電磁的記録を送信する場合は、宛先が学内・学外に関わらず、暗号化等を用いて保護すること。

② ①におけるパスワードを送信先に通知する際は、電話を利用するなど当該の電磁的記録を送った方法とは別の方法で行うこと。ただし、緊急の場合等別の方法による通知が困難な場合はこの限りではない。

③ 電磁的記録を送信する場合は、必要に応じて情報のバックアップを取得すること。

（5）法人の契約するクラウドストレージの利用

① 重要情報を学外へ持ち出し等する場合は（3）（4）の規定にかかわらず、原則として法人の契約するクラウドストレージを利用して行うこと。ただし、これによりがたい事情がある場合はこの限りではない。

② ①による場合（ただし書による場合を含む）は、当該情報を暗号化等により保護すること。

③ クラウドストレージを利用して情報を提供するときは、アクセス権限を誤って設定しないよう、十分に確認をすること。また、期間を限定して提供し、用途が済み次第、速やかに提供を終了すること。

9 情報の廃棄及び消去

（1）外部記録媒体及び書類の廃棄方法

① 外部記録媒体を譲渡、又は廃棄する場合は、図書情報課又は管理課に届け出ること。図書情報課又は管理課は、記録されていたデータが復元されることのないように、データ消去ソフトウェア又はデータ消去装置（以下、消去ツールと言う。）を用いて消去すること。消去が困難な場合は、媒体を物理的に破壊すること。（注1）

② 重要情報が記録された文書を廃棄する場合は、焼却又はシュレッダーを利用すること。

（2）情報端末に保存した情報の消去方法

情報端末と一体となった記憶装置を廃棄、若しくは他者に譲渡する場合は、図書情報課又は管理課に届け出ること。図書情報課又は管理課は、消去ツールを用いて、当該記憶装置に保存されている情報を復元が困難な状態にすること。

（3）業務委託による廃棄又は消去

図書情報課又は管理課は、情報端末等を廃棄又は情報の消去をする際、専門の業者との契約により廃棄又は消去を委託することも可能とする。

10 事務及び相談窓口

このガイドラインに関する事務及び相談窓口は、図書情報課又は管理課が取り扱う。

附 則

このガイドラインは、平成27年4月1日から実施する。

附 則

このガイドラインは、平成29年4月1日から実施する。

附 則

このガイドラインは、平成30年4月1日から実施する。

附 則

このガイドラインは、平成31年4月1日から実施する。

附 則

このガイドラインは、令和5年12月1日から実施する。

（注１）情報が保存された外部記録媒体を廃棄する場合は、次のとおり外部記録媒体を物理的に破壊する等、読取装置を利用して当該外部記録媒体から情報が読み出せない状態にすること。

① フロッピーディスク等の磁気媒体の場合は、当該媒体を折り曲げる、切断する等して情報を記録している内部の円盤を破壊する。

② CD-R/RW、DVD-R/RW等の光学媒体の場合は、カッター等を利用してラベル面側から同心円状に多数の傷を付け、情報を記録している記録層を破壊する。

③ テープ媒体の場合は、テープをカートリッジから取り出し、はさみ、カッター等で物理的に細断することで記録層を破壊する。

島根県立大学情報端末取扱ガイドライン

1　目的

このガイドラインは、「公立大学法人島根県立大学情報システム利用規程（平成 27 年規程第 76 号）」に基づき、情報及び情報機器の保護の観点から、島根県立大学・島根県立大学短期大学部（以下「本学」という。）のネットワークに接続して利用されるパーソナルコンピュータ・モバイル機器等（以下「情報端末」という。）の利用に関する取扱手順を示し、情報端末の安全な利用・運用に資することを目的とする。

2　定義

このガイドラインにおける用語の意義は、次のとおりとする。

（1）　共用情報端末

講義室、演習室、共同研究室、実習室等に法人が設置した情報端末。

（2）特権アカウント

アプリケーションのインストールやシステム設定の変更、全データへのアクセスなど、システムに対して高いレベルの権限を持ったアカウント。本学では、教職員個人に貸与する情報端末については、各教職員に特権アカウントが付与されるが、サーバ類や共用情報端末等については、システム管理者（基盤管理者）だけに付与されている。

3　対象者

このガイドラインは、本学が管理する情報端末及び情報ネットワークに接続する情報端末を利用・運用するすべての者を対象とする。

4　管理者の指定

学内のすべての情報端末について、当該情報端末の管理者を次のとおりとする。

① 共用情報端末については教育研究支援部長又は事務部長を管理者とする。

② 研究室、及び事務局に法人が個々の教職員用に設置した情報端末については、当該教職員を管理者とする。

③ その他、課又は室が独自に導入配備した情報端末については、特定の個人が利用する場合はその者を、共用の場合は当該課室の責任者を管理者とする。

④ 一時的に教職員及び学生に貸し出された情報端末については、貸出期間内においては、貸出しを受けている者を管理者とする。

⑤ 教職員・学生が持ち込み、本学情報ネットワークに接続する個人所有の情報端末については、持ち込んだ者を管理者とする。

5　利用者の遵守事項

（1）物理的損傷行為の禁止

利用者は、情報端末を物理的に損傷する可能性のある行為をしてはならない。

（2）ネットワーク帯域占有の禁止

利用者は、高い頻度で問い合わせパケット等を送出するソフトウェアの使用等ネットワーク帯域を占有する行為をしてはならない。

（3）コンピュータウィルスへの対応

利用者は、情報端末の利用において、ウィルス等への感染及び他への拡散を防ぐため、以下の各号を遵守しなければならない。

① 利用者は、情報端末にウィルス対策を講じること。

② ウィルス対策ソフトウェアにより情報端末内のすべての電子ファイルに対して、定期的にウィルス感染の有無を確認すること。

③ 外部からデータやソフトウェアを情報端末に取り込む場合又は外部にデータやソフトウェアを提供する場合は、ウィルス感染の有無を確認すること。

④ ウィルス等を検知した場合は、その実行形式のファイルを実行したり、データファイルをアプリケーション等で開いたりせず、ウィルスを駆除又はファイル自体を削除すること。

（4）外部記録媒体への注意事項

利用者は、CD-ROM や DVD-ROM、USB メモリ等の外部記録媒体を利用する場合は、以下の各号を遵守しなければならない。

① 利用者のファイルを保存した外部記録媒体を放置しないこと。

② 放置してある、又は出所が定かでない外部記録媒体を情報端末に挿入しアクセスしてはならない。そのような媒体を発見した場合は、図書情報課又は管理課に届け出ること。

③ 使用済みの外部記録媒体を譲渡、又は廃棄する場合は、別に定める「情報取扱ガイドライン」に従うこと。

（5）重要情報の取扱い

利用者は、重要情報を情報端末、又は外部記憶装置に保管する場合は、別に定める「情報取扱ガイドライン」に従うこと。

（6）共用情報端末利用上の遵守事項

利用者は、共用情報端末を利用する場合は、次の各号を遵守しなければならない。

① 自分で追加したファイルは必ず削除すること。

② 自分の ユーザ ID でログインした場合には、必ずログアウトを行うこと。

③ 設定変更を行った場合には、必ず変更前の状態に戻すこと。

④ 印刷物は放置しないこと。

⑤ 共有情報端末の異常を認めた場合は、図書情報課又は管理課に報告すること。

（7）情報端末利用上の遵守事項

利用者は、自身が管理者となっている情報端末を利用する際には、次の各号を遵守しなければならない。

① 情報端末に対し、強固な認証システムとログ機能が動作するよう設定すること。

② ウィルス対策ソフトウェアは、その機能を最新にした上で、システムを保護可能な状態に保つこと。

③ 情報端末の画面を他者から見える状態で利用しないこと。他者から見える怖れのある場合は、レイアウトを変更する、プライバシーフィルタを装着する等の措置を講じること。

④ 離席時には必ず情報端末のロックを行い、他者が支配又は操作可能な状態にしないこと。

⑤ 情報端末を情報ネットワークに接続する場合は、接続の直後にウィルス対策ソフトウェア等でスキャンを実行し、ウィルス等が検出されないことを確認すること。

⑥ 事務職員が、図書情報課又は管理課に登録されていない外部記録媒体に保存されたデータを利用する場合は、検閲用パソコンにてウィルス等が検出されないことを確認すること。

⑦ 本学が所有する情報端末及び重要情報を含む情報端末の紛失及び盗難があった場合は、速やかに図書情報課又は管理課に報告すること。

ただし、課又は室で導入配備したものについては、当該課室の責任者に報告すること。

⑧ 事務職員は、法人又は課室が設置した情報端末以外の情報端末から、非公開のサーバにアクセスしてはならない。

（8）学外からの利用における遵守事項

利用者は、学外のネットワークから学内の情報システム（不特定多数に公開されている Web サービスなどを除く）にアクセスする場合は、次の各号を遵守しなければならない。

① アクセスの際に必要となる認証情報（パスワードや秘密鍵）が漏えいしないように細心の注意を払うこと。

万一、認証情報が漏えいした場合、又はその可能性がある場合は、速やかに図書情報課又は管理課に連絡し、指示に従うこと。

② 不正利用対策が実施されていない情報端末、信頼性が保証できない情報端末（インターネットカフェの情報機器等）からのアクセスを行わないこと。

（9）セキュリティ上の問題箇所発見時の対応

利用者は、次に掲げる事項を発見したときは、速やかに図書情報課又は管理課、あるいは総務課に連絡すること。

① 情報端末の OS やアプリケーション又は学内に設置されているサーバコンピュータやネットワーク機器等について、セキュリティ上の脆弱性など不具合を発見した場合。

② 学内のサーバ上に、著作権を侵害するおそれのあるコンテンツや、重要情報、個人情報等が公開されていることを発見した場合。

③ 学外のサーバで、本学の重要情報若しくは構成員の権利を侵害するおそれのある情報等が公開されている場合、又は本学が権利を有するコンテンツが無断で使用されていることを発見した場合。

6 特権アカウント利用者の遵守事項

（1）ソフトウェアのインストール及び使用

特権アカウント利用者は、本学所有の情報端末にソフトウェアをインストールし、使用する場合は、次の各号を遵守しなければならない。

① 以下のソフトウェアのインストール及び使用を禁止する。

・教育・研究目的に合致しないソフトウェア
・不正なソフトウェア
・出所の定かでないソフトウェア
・その他、本学のネットワークやシステムに悪影響を及ぼす恐れのあるソフトウェア

② ソフトウェアの利用条件に従うこと。

③ 管理する情報端末について、インストール管理台帳を作成するなど、ソフトウェアライセンスの適正管理に、十分に注意すること。

（2）情報漏えいに関わる遵守事項

特権アカウント利用者は、自らが管理する情報端末に関して、次の各号を遵守しなければならない。

① 利用者が情報端末を認証なしで利用できないようにすること。情報端末が認証機能を有さない場合は、あらかじめ許可された者のみが利用できるように手段を講じること。

② ネットワークを経由した情報端末へのアクセスを認める場合は、セキュリティ対策に注意すること。

③ 管理者が特に認める場合を除いて、当該情報端末のアカウントを有さない者に使用させないこと。

④　アカウントを有さない者が情報端末に物理的にアクセスできないよう、短時間であっても情報端末を放置しないこと。設置場所・保管場所に施錠等の措置をとるとともに、必要に応じて機器にワイヤーロック等の盗難防止措置をとること。

⑤　情報端末を学外に持ち出す可能性がある場合は、盗難及び紛失に備えて、情報端末の内蔵ストレージを暗号化すること。

⑥　情報端末を廃棄又は譲渡する場合は、重要な情報が残留することのないように、専用ツールを用いて完全に消去するか、物理的に破壊すること。

7　事務及び相談窓口

このガイドラインに関する事務及び相談窓口は、図書情報課又は管理課が取り扱う。

附 則

このガイドラインは、平成27年4月1日から実施する。

附 則

このガイドラインは、平成29年4月1日から実施する。

附 則

このガイドラインは、平成31年4月1日から実施する。

附 則

このガイドラインは、令和5年12月1日から実施する。

島根県立大学ウェブブラウザ利用ガイドライン

1　目的

このガイドラインは、「公立大学法人島根県立大学情報システム利用規程（平成 27 年規程第 76 号)」に基づき、ウェブブラウザの利用におけるリスクの軽減、情報資産の保護、並びにウェブの安心・安全な利用に資することを目的とする。

2　対象

このガイドラインは、島根県立大学・島根県立大学短期大学部（以下「本学」という。）の情報ネットワークに接続された情報端末でウェブブラウザを利用するすべての利用者（以下「利用者」という。）を対象とする。

3　ウェブの利用に係る全般的な注意事項

（1）目的外利用の禁止

利用者は、教育研究及び事務利用等、本学で活動する上で必要な範囲以外でウェブサイトを閲覧してはならない。

（2）ウィルスチェックの実施

① 本学では、通信経路にファイアウォールを設置しているが、閲覧が可能なコンテンツであっても、常にウィルス感染等の脅威があることを認識して利用すること。

② ウィルスチェック機能により閲覧が制限されているウェブサイトを閲覧することが必要な場合は、図書情報課又は管理課に連絡・相談すること。

（3）外部のウェブサイトで提供されているサービスの利用等の注意事項

① 学外の掲示板、ブログ等への書き込み、ウェブメールの利用等を行う場合は、情報漏えいに注意すること。

② 学内から任意のウェブサイトを閲覧することにより、閲覧先のサーバに本学のドメイン名及び IP アドレス等が記録されることに注意すること。

③ 公序良俗に反する書き込みや利用を行わないこと。他人への誹謗中傷と誤解されるような記事、プライバシー及び著作権等の侵害と疑われかねない書き込みを行わないこと。

④ 不正なソフトウェアをダウンロードさせることを目的としたリンク、及び不正なサイトへの誘導を狙ったリンクがインターネット上に多数存在するため、不用意にリンクをクリックしないこと。

（4）証跡の取得

システム管理者（基盤管理者）は、ウェブ利用の証跡を取得及び保存し、必要に応じて点検及び分析を行うことができる。

4　ウェブサイトの閲覧

（1）ウェブサイト閲覧時の一般的な注意事項

① ウェブサイトの情報には、偽情報や誤情報が含まれている可能性があるため、その内容に注意すること。

② 検索サイトでは、検索結果に有害なウェブサイトへのリンクが含まれている可能性があるため注意すること。

③ バナー広告等には、有害なサイトやウィルスダウンロードサイトへのリンクが設定されていることがあるため、安易にクリックしないこと。

④ 成りすましサイト又はワンクリック詐欺サイトへの誘導、フィッシング（注１）被害につながることがあるため、電子メール内のリンクを安易にクリックしないこと。

⑤ ウィルス感染及び不正なソフトウェアをインストールさせられる可能性があるため、ウェブページ閲覧時にソフトウェアのダウンロードを求められても安易に実行しないこと。

⑥ 中継サイトを経由したデータの詐取、並びに認証情報の漏えいを防止するため、目的とするウェブサイトの URL を直接入力することを推奨する。

⑦ サービス不能攻撃（DoS 攻撃、サービスに不要な通信を起こさせて、サービスの質の低下を狙った攻撃）と見なされ、アクセスがブロックされる可能性があるため、次の行為は実施しないこと。

（a）ウェブページの再読込を短時間に繰り返すこと。

（b）オンラインジャーナルの大量一括ダウンロードを行うこと。

（2）SSL/TLS 通信の確認

SSL/TLS 通信とは、通信内容の暗号化及び通信相手の成りすまし防止を目的とした安全な通信であり、重要な情報等を送受信するウェブサイトで標準的に利用されている技術である。利用者は、個人情報、重要な情報等を送受信する場合は、SSL/TLS 通信が利用されており、サーバ証明書が正当なものであることを確認すること。

（3）確認・警告等のダイアログへの対応

セキュリティ機能に係る設定等により確認のためのダイアログ等が表示される可能性がある。当該ダイアログ等に関して安易に ActiveX、Java 等のスクリプトの実行を許可すると、不正プログラムの感染、情報漏えい等の危険性があるため、利用者は、確認用のダイアログ等が表示された場合は、中身を確認せずに安易に実行しないこと。

（4）ウェブブラウザの設定変更を要求するウェブサイトの閲覧

ウェブブラウザのセキュリティ水準が低下し、不正プログラムに感染する危険性が高まるため、ウェブサイトからブラウザの設定変更を要求されても、安易に実行しないこと。

5．ウェブサイト上のファイル利用

（1）ダウンロード

① ウェブサイト上に配置されたプログラムや文書ファイル等を利用する場合は、ウェブブラウザから直接実行したり開くのではなく、情報端末に一旦保存することが望ましい。

② WEB サイト上からダウンロードしたファイルは、実行したり開く前にウィルスチェック機能で安全を確認することが望ましい。

③ 保存したファイルに不正プログラムが含まれていることが判明した場合は、当該ファイルを実行又は特定のソフトウェアにより開かずに削除すること。

④ 保存したファイルについて電子署名により配布元が確認できる場合は、配布元が適切な組織であることを確認すること。

（2）不正プログラムに感染した時の対処

ダウンロードしたファイルを実行又は開くことにより、不正プログラムに感染又は感染の疑いがある場合は、直ちに当該情報端末を情報ネットワークから切り離した後、図書情報課又は管理課に連絡し、指示に従うこと。

6　事務及び相談窓口

このガイドラインに関する事務及び相談窓口は、図書情報課又は管理課が取り扱う。

附 則

このガイドラインは、平成 27 年 4 月 1 日から実施する。

附 則

このガイドラインは、平成 29 年 4 月 1 日から実施する。

附 則

このガイドラインは、平成 31 年 4 月 1 日から実施する。

（注 1）フィッシング

フィッシング（phishing）とは、たとえばオークションサイトと類似の画面を持った成りすましサイトに利用者を誘導しユーザ ID やパスワードを盗み出すような行為である。偽のサイトには、電子メール等で HTML メールのリンクから誘導する。

島根県立大学利用者パスワードガイドライン

1　目的

このガイドラインは、「公立大学法人島根県立大学情報システム利用規程（平成 27 年規程第 76 号）」に基づき、公立大学法人島根県立大学が設置する島根県立大学及び島根県立大学短期大学部（以下「本学」という。）情報システムのアカウントを利用する際のパスワードを、利用者が適切に管理することを目的とする。

2　定義　〔削除〕

3　対象

このガイドラインは、本学情報システムを利用するすべての利用者を対象とする。

4　パスワードに係る全般的な注意事項

（1）初期パスワードの変更

利用者は、新たなアカウントの発行を受けた後、速やかに初期パスワードを変更すること。初期パスワードのまま情報システムの利用を継続してはならない。

（2）パスワードに使用する文字列

① 利用者が設定するパスワード文字列は、10 文字以上であって、次のア、イ及びウの文字集合からそれぞれ最低1文字以上を含むこと。

ア　英大文字（A～Z）

イ　英小文字（a～z）

ウ　数字（0～9）

② 次の文字列は容易に推測可能であるため、パスワードとして設定してはならない。

ア　利用者のアカウント情報から推測できる文字列（名前、ユーザ ID 等）

イ　アの文字列を並べ替えたもの、又は当該文字列に数字や記号を追加したもの

ウ　辞書の見出し語、又は著名人の名前等

（3）パスワードの変更

① [削除]

② アカウント管理責任者からパスワード変更の指示を受けた場合は遅滞なくパスワードを変更すること。

③ パスワードを変更する際、変更前のパスワードと類似の文字列は使用しないこと。

④ アカウント管理責任者は、システム管理者（基盤管理者）に命じて、次のアカウントに対して停止措置をとることができる。

ア　[削除]

イ　アカウント管理責任者からのパスワード変更指示に従わない利用者のアカウント

ウ　セキュリティの侵害又はその可能性があるアカウント

（4）パスワードの管理

① パスワードは他者に洩れないように厳重に管理すること。

② 他の者にパスワードを教えないこと。

③ パスワードが他の者に知られないよう注意すること。

④ 他のサービスとの使い回しをしないこと。

⑤ その他、パスワードの漏えいのおそれがある行為を行わないこと。

5　パスワードに関する各種手続き

（1）パスワードを忘れた場合

パスワードを忘れた場合は、当該アカウント管理責任者に、身分証（学生証もしくは教職員証等）を持参の上、パスワードの再発行を申請すること。再発行後は、速やかに新しいパスワードに変更すること。

（2）アカウント停止となった場合

前条（3）④によりアカウント停止措置を受けた場合は、身分証（学生証もしくは教職員証等）を持参の上、当該アカウント管理責任者に対しパスワードの再発行を申請すること。再発行後は、速やかに新しいパスワードに変更すること。

（3）パスワードの事故の報告

アカウントを他者に使用された場合又はその可能性が疑われる場合、直ちにパスワードを変更したうえで、当該情報システムのアカウント管理責任者にその旨を報告しなければならない。

6　事務及び相談窓口

このガイドラインに関する事務及び相談窓口は、図書情報課又は管理課が取り扱う。

附 則

このガイドラインは、平成27年4月1日から実施する。

附 則

このガイドラインは、平成29年4月1日から実施する。

附 則

このガイドラインは、平成30年4月1日から実施する。

附　則

このガイドラインは、平成31年4月1日から施行する。

附　則

このガイドラインは、令和2年4月1日から施行する。

島根県立大学電子メール利用ガイドライン

1　目的

このガイドラインは、「公立大学法人島根県立大学情報システム利用規程（平成 27 年規程第 76 号)」に基づき、公立大学法人島根県立大学が設置する島根県立大学及び島根県立大学短期大学部（以下「本学」という。）における情報資産を保護し、電子メールの安全な利用に資することを目的とする。

2　対象者

このガイドラインは、本学ドメイン（u-shimane.ac.jp）に属するメールドメインにて電子メールを利用するすべての利用者（以下「利用者」という。）を対象とする。本学が提供する電子メールシステム（以下「本学メールシステム」という。）のほか、外部プロバイダ、学部・研究科・センター等、及び教員個人が運用する電子メールの利用者についても、このガイドラインに準じることとする。

3　本学メールシステムの設定

（1）電子メール受信に係る設定

① ウィルス対策ソフトウェア等を利用し、ウィルス対策を行うこと。

② 〔削除〕

（2）電子メール送信に係る設定

① 〔削除〕

② 本学メールシステムでは、受信した電子メール自体の自動転送を認めていない。

4　電子メールに係る全般的な注意事項

（1）利用目的

利用者は、本学メールシステムを教育研究活動及び活動支援のために使用すること。

（2）証跡の取得

本学は、本学メールシステム全般の利用について、証跡を取得及び保存し、必要に応じて点検及び分析を行うことがある。

（3）ウィルス対策、迷惑メール対策

本学は、電子メールに対し、ウィルス対策及び迷惑メール対策を行っているが、対策により電子メールの送受信に支障がある場合は、図書情報課又は管理課に相談すること。

（4）ユーザ ID 及び電子メールアドレスの管理

① 他人のアカウント及び電子メールアドレスを使用してはならない。

② アカウント及び電子メールアドレスを他人と共用しないこと。

③ 利用者は、電子メールを利用する必要がなくなった場合は、図書情報課又は管理課に届け出ること。なお、離籍した者に対しては、その都度アカウントの廃止を行う。

④ 特定のサービス、職位、部門単位に付与されるアカウント及び電子メールアドレスのように、複数の関係者が共用したり、担当を引き継いで使用する必要がある場合、利用者は、許可及び設定について所属責任者から説明を受けること。

5　パスワードの管理

別に定める「利用者パスワードガイドライン」に従うこと。

6　電子メールの受信

（1）電子メールの受信確認

利用者は、定期的に電子メールの受信確認を行うこと。

（2）電子メールを受信した場合のウィルスチェック

① ウィルス対策ソフトウェアによる自動ウィルスチェックを実施すること。

② 電子メール利用によって、ウィルスに感染又は感染の疑いがある場合は、直ちに当該 PC をネットワークから切り離した後、図書情報課又は管理課に連絡すること。

③ その他、電子メールに関連したウィルス対策において緊急対応が必要な場合は、図書情報課又は管理課の指示に従うこと。

（3）あて先間違いの電子メールを受信したときの対応

あて先間違いの電子メールを受信し、その内容から、送信者から正しい受信者へ再度送信する必要があると判断した場合は、可能な範囲で、送信者へあて先が間違っていたことを通知すること。通知した後は当該メールを削除すること。

（4）不審な電子メールを受信したときの対応

① 不審な電子メールを受信した場合は、開かずに削除すること。

② 電子メールに不審なファイルが添付されていた場合は、当該ファイルを開かずに削除すること。

③ 上記の２項に関わらず、受信した不審な電子メール又は添付ファイルの参照が必要な場合は、削除する前に図書情報課又は管理課に相談すること。

（5）迷惑メールの対応

① 必要以上に電子メールアドレスを公表又は通知しないこと。

② 電子メールアドレスを開示又は通知する場合は、自動収集されないように、工夫を施すこと。(画像情報で貼付する、意図的に全角文字で表示する、無駄な文字列を前後に接続する等)

③ 受信した迷惑メールに対しては、これを無視すること。送信者へ停止要求を出すと、その電子メールアドレスが使用されている事実を伝えてしまう結果となるため返信しないこと。

7 電子メールの作成と送信

（1）To、Cc 及び Bcc の利用

① To（あて先）、Cc（カーボンコピー）及び Bcc（ブラインドカーボンコピー）の総あて先件数は必要最小限とすることし、送信先に間違いがないか十分確認してから送ること。

② 意図せず他人の電子メールアドレスを公開することを避けるため、同時に多数の人へ電子メールを送信するときは、Bcc を利用する、又は各自に個別送信すること。

③ 受信者全てのメールアドレスが既に共有されていても、受信者に機微な内容の返信を求める場合は、受信者が誤操作によって全員に返信することを避けるため、 Bcc を利用する、又は各自に個別送信すること。

（2）電子メール１件当たりのファイル容量の制限

① 電子メール本文と添付ファイルを含めた容量が 10M バイトを超えないこと。

② 電子メール本文と添付ファイルを含めた容量が 10M バイトを超える場合は、別手段による提供や分割送信などの方法を採ること。

③ メーリングリストを使用するなどして同時に多数の相手に送信する場合は、総容量が大きくなるのを防ぐため、ファイル添付をなるべく避け、ファイルサーバでの共有やグループウェアの機能（お知らせや掲示板等）を利用すること。

（3）受信確認について

電子メールは、相手に必ず届くことが保証されているシステムではない。重要な事項をメールにて送った場合は、電話等電子メール以外の方法により、相手が受け取ったかどうか確認をすることが望まし

い。

（4）誤送信時の対応

電子メールを誤って送信したときは、相手先（受信者）への対応は発信者が責任を持って行うこと。システムに送信取り消し機能が備わっている場合は、予め利用設定をしておくことが望ましい。

（5）ウィルスを送信したときの対応

誤ってウィルスを送信したことが判明したときは、直ちに相手先へ通知するとともに、図書情報課又は管理課へ連絡すること。

（6）その他、電子メール作成及び送信時の留意事項

① 重要情報を電子メールを用いて送信するときは、別に定める「情報取扱ガイドライン」に基づく安全措置を講じること。

② 他人になりすまして電子メールを送信しないこと。

③ 電子メールを転送するときに、作成者の許可なく内容の変更をしないこと。

④ 個人情報やプライバシーの保護に配慮すること。

（7）電子メールを送信するときの注意事項

① チェーンメール（同じ内容の電子メールを別の人に転送するように要請するもの等）の送信・転送を行わないこと。

② スパムメール（ダイレクトメール等営利目的を主とした無差別に発信された電子メール）、ジャンクメール（役に立たない情報が書かれている電子メール）等を送信しないこと。

③ 電子メールに題名を付けること。また、題名は電子メールの内容が分かるように具体的かつ簡潔に書くこと。

④ 俗語的表現やあらかじめ定められていない省略語を使用しないこと。

⑤ 環境依存文字は使用しないことが望ましい。（次表の例参照）

（表　環境依存文字の例）

①	②	③	④	⑤	⑥	⑦	⑧	⑨	⑩	⑪	⑫	⑬	⑭	⑮	⑯
⑰	⑱	⑲	⑳	Ⅰ	Ⅱ	Ⅲ	Ⅳ	Ⅴ	Ⅵ	Ⅶ	Ⅷ	Ⅸ	Ⅹ		㍉
㌔	㌢	㍍	㌘	㌧	㌃	㌶	㍑	㌦	㌍	㌦	㌣	㌫	㍊	㌻	㎜
㎝	㎞	㎎	㎏	㏄	㎡									平成	
〝	〃	№	㏍	℡	㊤	㊥	㊦	㊧	㊨	㈱	㈲	㈹	明治	大正	昭和
≒	≡	∫	∮	∑	√	⊥	∠	∟	⊿	∵	∩	∪			

⑥ メール本文は、読み易さを考慮して適宜改行を入れながら作成すること。一行の目安は、全角 30～35 文字程度である。

8　電子メールの保存・削除

（1）メールボックス（サーバ側）における電子メールの保存・削除

必要な電子メールは適宜情報端末に保存するとともに、不要な電子メールや一定期間を経過した電子メールは削除し、メールボックスにおける長期保存は行わないこと。

（2）メールボックス（情報端末側）における電子メールの保存・削除

本文や添付ファイルに重要情報が含まれている電子メールを削除する場合は、「ごみ箱」に入れるのではなく完全に削除すること。

9　事務及び相談窓口

このガイドラインに関する事務及び相談窓口は、図書情報課又は管理課が取り扱う。

附 則

このガイドラインは、平成27年4月1日から実施する。

附 則

このガイドラインは、平成29年4月1日から実施する。

附 則

このガイドラインは、平成30年4月1日から実施する。

附　則

このガイドラインは、平成31年4月1日から施行する。

附 則

このガイドラインは、令和2年4月1日から実施する。

手引やマニュアルの電子データ（最新版）について

本手引をパソコン等でも参照できるよう電子データ（PDF）を公開しています。内容に変更があった場合、修正し公開していきますのでご確認ください。また、手引未収録の全学マニュアル（例: OneDrive や Teams でのファイルや動画の共有方法等）もありますので、必要に応じて参照してください。参照方法は以下のとおりです。

■ 共通

① 以下 URL（https://ushimaneacjp.sharepoint.com/pub）を指定、もしくは学生情報システム（UNIPA）トップページの左下にある『ファイル共有（Office365）』のリンクをクリックしてください。

■ 当手引の電子データを参照する方法

② 『松江キャンパス』→『1_学生・教職員共有』→『管理課より』を選択します。
『情報ネットワーク利用の手引』のフォルダに電子データ（PDF）が格納してあります。

QR コードからも
ご確認できます

■ Microsoft365など、全学共通マニュアルを参照する方法

② 『3キャンパス』→『1_学生・教職員共有』を選択します。
各フォルダに電子データ（PDF）やインストーラーなどが格納してあります。

QR コードからも
ご確認できます

島根県立大学・島根県立大学短期大学部

松江キャンパス

情報ネットワークシステム
利用の手引

2026年4月　発行