福山大学
FUKUYAMA UNIVERSITY

情報セキュリティパンフレット

ICT は大学生活を支えるものです。授業、自宅学習、大学からのお知らせの確認、さまざまな手続きなど、あらゆる場面で活用します。入学時に配布される ID と自身で設定するパスワードの管理、およびマルウェア（コンピュータウイルスなど）への対策が求められます。大学からの通知を受け取るため、ご自身のスマートフォンに転送設定を行ってください。これ以降では、安全な ICT 利用のための情報セキュリティについて説明します。

１．なぜ情報セキュリティが大切なのか

大学では、自分専用のアカウント（大学の ID・パスワード）が発行される。履修登録、成績確認、レポート提出、大学からの通知確認など、大学生活のあらゆる場面でこのアカウントを使用する。このアカウントが他人に悪用されると、個人情報の流出、他人へのなりすましといった被害が生じうる。

その他、「フィッシングによる個人情報等の詐取」、「インターネット上のサービスへの不正ログイン」、「不正アプリによるスマートフォン利用者への被害」。「ネット上の誹謗・中傷・デマ」などから自分を守り、他の人に迷惑をかけないための情報セキュリティが大切である。

２．パスワード管理と認証

パスワードは、福山大学の情報通信機器やさまざまな情報サービスを利用する際に、本人確認に使用する情報である。

パスワード設定の基準

- 12 文字以上の英数字記号を組み合わせて設定する（推奨）
- 生年月日や電話番号、辞書に載っている単語など、推測されやすいものは避ける
- 覚えやすく長いパスフレーズ（例：HaruHaSakura#2004）を活用する方法もある

パスワード利用上の注意

- **大学のパスワードは、他のサービス（例：Gmail、LINE）で使い回さない**
- 自分が利用する情報通信機器（ノートパソコン、スマートフォンなど）には、パスワードまたは指紋認証等を設定する
- **パスワードは他の人に教えてはいけない**
- **大学のパソコンを使用した後は、必ずログオフしてから席を離れること**

多要素認証の活用

多要素認証とは、パスワードに加え、認証アプリや確認コードなど複数の要素で本人確認を行う仕組みであり、パスワードが漏洩しても不正ログインを防ぐ効果がある。

3．フィッシング詐欺・サポート詐欺への対策

フィッシング詐欺

フィッシングとは、実在する組織（銀行、通販サイト、大学事務局など）を装った電子メールやショートメッセージで偽サイトに誘導し、ID・パスワード・クレジットカード情報などを入力させる手口である。身近な具体例を以下に示す。

- 宅配便の不在通知を装ったショートメッセージ
- SNS のダイレクトメッセージで「あなたが写っている写真がある」としてリンクを送る手口
- 通販サイトや決済サービスを装い「アカウントが停止されます」と緊急性を強調する電子メール

見分け方と対処法

- 送信元の電子メールアドレスのドメイン（@以降の部分）が正規のものか確認する
- **「24 時間以内に対応しないとアカウントが停止されます」のように緊急性を強調する表現には警戒する**
- **リンクをクリックせず、自分で公式サイトを検索して正規の窓口に問い合わせる**
- 不審に感じたら、ICT サービスセンターや信頼できる人に確認する

サポート詐欺（偽警告）

Web ページの閲覧中に、突然「ウイルスに感染しました」という偽の警告画面が表示され、警告音が鳴ることがある。画面に表示された電話番号に電話をかけさせ、「復旧」を名目に金銭をだまし取ったり、マルウェアをインストールさせたりする手口である。

対処法

- 偽の警告画面が表示されても、落ち着いて対処する。表示された時点では実害は発生していない
- **表示された電話番号には電話しない**

4．マルウェア対策

マルウェアは、パソコンやスマートフォンなどに感染し、被害を与える有害なプログラムの総称である。コンピュータウイルスはその代表例である。電子メール、Web ページ、アプリなど、さまざまな経路で感染し、「ここをクリックするとプレゼント！」「添付の PDF ファイルは重要情報！」のような誘導文句で感染を促す手口がある。

電子メールを介した感染への注意

- 電子メールの送信者が有名人や知人の名前であっても、実際には別の人が送信している可能性がある
- 添付ファイルを開くときや、電子メール内の「会員登録」「抽選に応募」などのリンクをクリックするときは注意が必要である

マルウェアからの防御

- Web ページで「ここをクリック！」とあっても、安易にクリックせず、本当にクリックする必要があるかを落ち着いて判断する
- 情報通信機器には、標準のセキュリティ対策機能（例：Windows Defender）を有効化するか、ウイルス対策ソフトウェアをインストールする
- **スマートフォンのアプリは、公式ストア（App Store、Google Play）からインストールする**

5．情報通信機器とデータの管理

OS とアプリのアップデート

パソコンのオペレーティングシステムやアプリは常に最新版に保つか、自動アップデートを有効にする。アップデートには、セキュリティ上の欠陥（脆弱性）を修正する役割がある。

公衆 Wi-Fi 利用時の注意

カフェ、駅、商業施設などでの無料 Wi-Fi（パスワード無しで誰でも利用できる Wi-Fi）では、通信内容が傍受される可能性がある。ログインや決済などの操作は無料 Wi-Fi では行わない。

※ 大学の無線 LAN（Wi-Fi）は暗号化されている。名称は「Zelkova」である。

データバックアップ

- レポートや写真などのデータは、USB メモリや SD カードなどに複製（バックアップ）して保管すること
- OneDrive（Microsoft 365 で利用可能）などのクラウドストレージも活用できる。自動バックアップを設定しておくと、機器の故障や紛失時にもデータを復旧できる

紛失・盗難への注意

ノートパソコン、携帯電話、USB メモリ、SD カードなどには個人情報が保存されている。紛失・盗難に備え、以下の対策を講じておく。

- 機器にはパスワードまたは指紋認証等を設定する
- スマートフォンでは、紛失時に端末を遠隔でロックまたはデータ消去できる機能（iPhone の「探す」、Android の Google デバイスを探す機能など）を有効にする

6．SNS での情報発信と個人情報の保護

インターネット上での情報発信

SNS（LINE、Instagram、X（旧 Twitter）など）に書き込んだ情報は、世界中の人の目に触れる可能性がある。一度書き込んだ情報を他の人がコピーして配布することもある。**インターネット上に公開された情報は、完全には消去できない（デジタルタトゥー）。**投稿前に「将来にわたって残っても問題ないか」を確認する習慣が望ましい。

情報発信における注意事項

- 秘密にすべき情報をインターネット上で書き込まない
- 住所、免許証や履歴書のコピーなど、プライバシーに関わる個人情報は書き込まない
- 自宅周辺の写真は住所が特定される材料となるため、投稿を控える

SNS アカウントの保護

- SNS の公開範囲の設定を確認し、限定された範囲にのみ情報を公開する
- プロフィール情報（本名、所属学部、顔写真）、位置情報付きの投稿、時間割の写真投稿などから個人が特定される場合がある
- SNS アカウントが乗っ取られると、友人にフィッシングリンクが送信されるなどの連鎖被害が発生する。多要素認証の設定と、不審なダイレクトメッセージのリンクを開かないことが対策となる

他者への配慮

- 家族、友人、知り合いのことをインターネットに書き込むときは、その人たちのプライバシーや感情に配慮する
- その場の感情で書き込まず、落ち着いた気持ちで書き込む

業務・社会活動上の言動への注意

アルバイト、インターンシップなど、社会の一員として活動する際に、仕事を通じて知り得た情報を漏らすことや、不満や悪口を発信することは避ける。匿名であっても発信者は特定されうる。軽い気持ちでの投稿が重大な結果になることもある。

7．AI の適切な利用

AI（ChatGPT など）は、対話的に質問や相談ができるシステムであり、学修、思考の深まり、問題解決、インターネット情報の検索などに活用できる。ただし、課題での利用は授業担当教員の指示に従うこと。

活用できる用途

文章の校正・言い換え・要約・翻訳、調査・研究のヒント、予習・復習の補助、インターネット検索など。

利用上の注意点

- **AI の回答をそのまま課題として提出したり、SNS に投稿したりしてはいけない**（自作でないものを自作と偽ることは、マナーに反する）
- AI の回答は不正確な場合があるため、根拠を確認する習慣を持つ
- **個人情報や機密情報（研究データ等）は AI に入力してはいけない。**入力した情報が AI 事業者のサーバに保存される場合がある

8．著作権と法令の遵守

剽窃や著作権侵害の防止

- 他の人が作成した情報（文章や写真など）を丸ごとコピーしたり、一部を切り取ったりして、自分のものとして発表してはいけない
- 授業でのレポート作成、ブログや掲示板での情報発信において注意が必要である

違法コピーの禁止、違法コンテンツ利用の禁止

ソフトウェアやコンテンツ（映画、音楽など）の違法なダウンロード・コピーは法律で禁止されている。販売などで利益を得ることは、より重い違法行為となる。

公序良俗に反する行為の禁止

情報通信機器を悪用した詐欺・嫌がらせ・不正アクセスなど、公序良俗に反する行為は行わない。法的責任を問われる場合がある。

9．セキュリティ問題の発見と対応

セキュリティ問題の兆候

以下の状況はセキュリティ上の問題が発生している可能性がある：

- 見覚えのないウィンドウが突然表示される
- データが不自然に消失している
- スマートフォンやパソコンの動作が急に遅くなる
- 「あなたのアカウントから不審なメールが届いた」と友人から連絡があった

些細な疑いでも放置せず、早期に相談することが被害を抑える。**1 人で悩まず、すぐに相談すること。大学での相談先：ICT サービスセンター（未来創造館 1 階）**

インシデント発生時の対応手順

まず、その場ですべきこと：

- **インターネットケーブルを外す、Wi-Fi をオフにする（被害拡大防止のため）**
- 機器の電源は切らない（証拠保全・状況把握のため）
- ICT サービスセンター（未来創造館 1 階）へ連絡
  電子メール ictservice@fukuyama-u.ac.jp

ICT サービスセンターの指示に基づき対応する：

- 関係するアカウントのパスワードを変更する
- 不審な表示や電子メールのスクリーンショットを保存する（証拠として活用できる）
- 貴重なデータを別の媒体にコピーして保存する

不審な表示への対応

脅迫めいた表示（「現金を振り込め！」「電話しろ！」「１週間以内に振り込まなければ」など）が現れても、慌てずに信頼できる人に相談する。

１０．歩きスマホの禁止

歩行中にスマートフォンなどを操作することは危険であり、転倒や衝突事故を引き起こす可能性がある。周囲の人を巻き込む場合もあり、入院や死亡事故につながった事例もある。**車両（自転車、バイク、自動車）運転中の携帯機器の使用は法律で禁止されている。**

福山大学 ICT システムのまとめ

① **大学の ID とパスワード**：入学時に配布される ID と仮パスワードを使って、自身でパスワードを設定します。これらの情報は厳重に管理し、他人に教えないでください。
② **Zelkova（ゼルコバ）**：学生ポータルシステムです。大学からのお知らせの確認、履修登録、成績確認、シラバス閲覧などができます。
③ **Cerezo（セレッソ）**：学修支援システムです。授業資料、小テスト、レポート提出、出席確認、アンケートなどの授業活動をオンラインで行う学修基盤です。予習・復習にも利用できます。
④ **Microsoft 365**：Word・Excel・PowerPoint などのオフィスソフト、電子メールシステム、OneDrive クラウドストレージが大学内外から無償で利用できます。
⑤ **大学メールとその転送設定**：大学は Microsoft 365 のメールサービスを使用しています。大学からの通知を受け取るために、スマートフォンへの転送設定を行ってください。
⑥ **キャンパス無線 LAN**：全講義室に Wi-Fi スポットを整備しています。大容量回線ですが、利用者が多い時間帯は接続しにくい場合があります。講義室での学修のために整備しているものです。
⑦ **情報漏洩対策**：自分が利用する情報通信機器には、パスワードまたは指紋認証を設定すること。
⑧ **マルウェア対策**：標準のセキュリティ対策機能（例：Windows Defender）を有効化するか、ウイルス対策ソフトウェアをインストールすること。
⑨ **ICT サービスセンター（未来創造館 1 階）**：平日 10:00～13:00、15:00～17:00 に無線 LAN 設定、パソコン操作、情報セキュリティなどのサポートを実施しています。困ったときは早めに相談してください。

⑩ **学生用貸出ノートパソコン**：授業では BYOD（Bring Your Own Device：授業に自分のデバイスを持参して使用する方式）を実施しています。自分の PC 故障時には未来創造館 1 階で IC 学生証による貸出が可能です。当日返却、学外持出不可が原則です。

入学直後の確認チェックリスト

☐ 大学アカウントのパスワードを 12 文字以上で設定した
☐ 利用可能なサービスで多要素認証を有効にした
☐ スマートフォンへの大学メール転送設定を行った
☐ パソコン・スマートフォンの OS とアプリを最新版に更新した
☐ 情報通信機器にパスワードまたは指紋認証等を設定した
☐ SNS の公開範囲を確認した

困ったとき、相談したいときは

情報セキュリティに関して困ったこと、相談したいことがある場合は、ICT サービスセンターへ連絡してください。

ICT サービスセンター

場所　　未来創造館 1 階
開設時間　　平日 10:00～13:00、15:00～17:00（大学指定の休日を除く）
電話　　4403、4404、4405
電子メール　ictservice@fukuyama-u.ac.jp
※ 相談内容の秘密は厳守している

謝辞

このパンフレットでは「かわいいフリー素材集 いらすとや」のイラストを使用しています。

情報セキュリティパンフレット
編集・発行：　福山大学共同利用センターＩＣＴサービス部門
発行日：　２０１５年８月（２０２６年３月に最新改訂）