中央大学　多摩 IT センター
2025 年 5 月 12 日作成

情報セキュリティの基本的な留意事項

1. 情報機器に関する留意事項

① 盗難防止のため、施錠可能な棚やラック等に保管する、あるいは肌身離さず保持すること。

② 離席する場合には、他人に悪用されないよう、端末をロックすること。

③ 飲み会等紛失のリスクが高い場面においては、端末を持ちださないこと。

④ システムがマルウェアに感染することを防止するため、それらを構成する情報機器やソフトウェアに対してはセキュリティパッチを適用すること。

⑤ 出所が明らかではないソフトウェアや配信元が明確でなく怪しい Web ページは利用しないこと。

⑥ ウイルス対策ソフト（※）や OS 等から更新が求められた場合には、更新作業を行うこと。

⑦ 端末やその他電子記録媒体を廃棄・譲渡する場合には、適切な方法でデータを消去した上で、廃棄・譲渡すること。

※本学では、教職員・学生向けのセキュリティソフトとして、ESET Endpoint Security を提供しております。

2. ファイル・資料管理に関する留意事項

【電子ファイルの取扱い】

① 学生の個人情報等機密情報（学生の成績情報、入試や試験問題等学内の一部の者のみが閲覧可能な情報、以下同様）については、他の一般の情報とは分別した上で、指定された利用者でなければ利用できないよう、必ずファイルにパスワードを付すこと。

② 端末に保存されているファイルについて、必要性がなくなった時点で、速やかに端末上より削除すること。

【紙媒体の取扱い】

① 学生の個人情報等機密情報が記録された資料等は、机上等の人目に触れる場所には放置しないこと。

② 学生の個人情報等機密情報が記載された紙媒体を廃棄する場合、ごみ箱やごみ集積所で拾得されることによる情報漏洩を防止するため、廃棄前には必ずシュレッダーにかけること。

3. パスワード管理に関する留意事項

① パスワードを設定する際は、下記に注意すること。

・他人から推測されやすい文字列を使用しない（自分や家族の名前、電話番号、生年月日、英単語など）

・アルファベットの大文字、小文字、数字、記号を混ぜた 10 文字以上で構成する

・様々なサービスで同じパスワードを使わない

② 端末に対して ID/パスワードを記載した紙を付すなど、ID/パスワードが人目に触れることの無いようにすること。

③ パソコンやシステム利用にあたって用いている自分の ID を他人に貸さないこと。また、他人に対して自らの ID/パスワード情報を伝えないこと。

4. その他

① 身に覚えのないメールを受信した場合には不用意にメールの開封及び添付ファイルや本文上の URL にはアクセスしないこと。また、悪意のある不審メールを受け取った方場合は、IT センター㊢に対して報告を行うこと。

② 生成 AI を利用する際には、「中央大学における「生成系 AI」についての基本的な考え方（https://www.chuo-u.ac.jp/aboutus/efforts/generative_ai/thinking/）」等を参照の上、生成 AI のリスクを十分に理解したうえで利用すること

③ 本学のセキュリティ関連の案内（https://itc.r.chuo-u.ac.jp/com/security/index.htm）を踏まえ、適切に管理・対応すること

インシデント発生時の対応について

1. インシデントの定義

セキュリティインシデントとは、情報の「機密性」、「完全性」、「可用性」のいずれかを侵害した事象、あるいは侵害した可能性のあった事象を指す。

セキュリティインシデントの具体例を以下に示す。

① 機密性の侵害例（適切な人以外が情報にアクセスできてしまう）

- 他の教授の個人情報や学生の成績情報が含まれる資料等機密性の高い情報を、意図しない宛先に送ってしまった。
- 講義資料や研究データが保存されたUSBメモリを紛失し、第三者がデータにアクセスできる状態になった。

※機密性の高い情報とは、学生の成績情報、入試や試験問題等学内の一部の者のみが閲覧可能な情報を指す

② 完全性の侵害例（情報が不正確である、改ざんされてしまった）

- 学生の成績データが第三者によって書き換えられた。
- ウイルス感染によって講義資料の一部が意図せず書き換えられた。

③ 可用性の侵害例（許可された利用者が情報にアクセスできない）

- 講義資料のフォルダを誤って削除または移動し、学生が必要なタイミングで利用できなくなった。
- 誤って古いファイルで新しいデータを上書き保存してしまい、必要な情報にアクセスできなくなった。

2. 発生時の報告の実施

セキュリティインシデントを発見又は疑いを持った場合、認知者はできるだけ速やかに本学事務職員に口頭又は電話で報告すること。

なお、セキュリティインシデントに該当するか判断に迷うような場合も必ず報告を行い、判断を仰ぐこと。

3. 協力要請

セキュリティインシデントの関係者となった場合に、本学が実施する外部機関への報告や原因究明、被害範囲の確認等を行うために、インシデント発生時の状況の報告や端末のログ提供等協力を求める場合があるため、その際には本学の求めに応じ、協力すること。

以上