

愛媛大学情報セキュリティ対策ガイドライン

1

最新の状態

パソコンやスマートデバイスのOSとソフトウェアは、常にセキュリティ更新を行い最新の状態で利用する。

2

ウイルス対策

ウイルス対策ソフトを必ずインストールして、常に最新のウイルス定義ファイルに更新する。

3

電子メール

標的型攻撃に注意し、怪しく感じるメールの添付ファイルや本文中のリンク URL を開かない。

4

パスワード

パスワードは英数・記号を混ぜた堅牢なものを使用し、他人には教えない。使い回しをしない。

5

ファイル共有

ファイル共有設定はアクセス権を限定するなど情報漏洩対策を行う。共有する必要がなくなった場合は、速やかに共有を解除する。

守ってね!



愛媛大学マスコットキャラクター「えみか」

6

バックアップ

故障や誤動作などで重要情報が消失しないようにデータのバックアップを定期的に行い、不測の事態に備える。

7

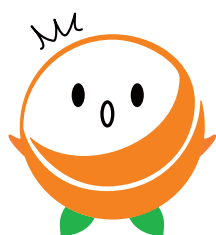
情報の管理

重要情報は机上に放置しない。個人情報など重要情報の入った端末やUSBメモリ等を学外に持ち出さない。

8

情報の廃棄

重要書類はシュレッダーする。パソコンや記憶媒体を廃棄する場合は、完全消去ソフトを利用したり専門業者に依頼する。



あれ?
おかしいな
と思ったら

- ① 学内ネットワークから切り離す
- ② 総合情報メディアセンター窓口 to 連絡 (内線 8803)

愛媛大学情報セキュリティ対策ガイドラインのチェックシート

1. 最新の状態

- ☐ パソコンもスマートデバイスも、OS・ソフトウェアは常にセキュリティ更新が必要です。最新の状態にしてください。
- ☐ 更新を怠った状態の機器は、脆弱性を悪用するマルウェアの感染を防げないので、利用しないで下さい。

2. ウイルス対策

- ☐ 怪しい Web サイトやメールを介したウイルスからパソコンを守るため、ウイルス対策ソフトをインストールして下さい。
- ☐ ウイルス対策ソフトのウイルス定義ファイルが古いままだと正常に動作しません。常に最新のウイルス定義ファイルに更新されていることを確認して下さい。

3. 電子メール

- ☐ 電子メールを送る前に、宛先の送信ミスを防ぐため、目視にて送信先アドレスを確認して下さい。
- ☐ 本人の許可を得ずに第三者に電子メールアドレスを伝えてしまうことも情報漏えいになります。お互いのメールアドレスを知らない複数人にメールを送る場合は、Bcc に記入して送信して下さい。
- ☐ 重要情報はメールで送信しないでください。
- ☐ メールアドレスのスペル違いにより、@以降が本物に酷似した宛先（ドッペルゲンガードメイン）へ誤送信され、情報漏えいが発生する恐れがあります。メールアドレスに誤りが無いかよく確認してください。
- ☐ 電子メール経由の標的型攻撃が多数発生しています。不審な発信者や内容かどうかにかかわらず、正しい電子メールを装った攻撃でないかどうかを念の為に疑って下さい。怪しく感じる場合は、添付ファイルやメール本文中のリンク URL を開かないで、メール本体を削除して下さい。

4. パスワード

- ☐ パスワードは自分の名前や誕生日などを避け、英数字・記号の組合せで、他人に推測されにくい堅牢なものに設定してください。パスワードは同じものを使い回さないで下さい。
- ☐ パスワードを他人が見えるような場所に貼らないで下さい。他人に教えたり、わからないように管理してください。
- ☐ ルータや複合機など、ネットワークに接続される機器において、管理者パスワードを出荷時の初期状態で利用すると不正アクセスされる恐れがあるため、パスワードを変更してから利用して下さい。

5. ファイル共有

- ☐ メール添付によるファイル送信は情報漏洩のおそれがあります。愛媛大学アカウントを用い、Microsoft365 の OneDrive・Group・Teams や Nii FileSender を利用して、適宜暗号化（パスワード保護等）し共有して下さい。

6. バックアップ

- ☐ 故障や誤操作などにより、パソコンやサーバの中に保存したデータが消えてしまうことがあります。また、データを勝手に暗号化してしまい、復号化するための代金を要求する「ランサムウェア」ウイルスも存在しますので、データのバックアップを定期的に行い、このような不測の事態に備えるようにして下さい。

7. 情報の管理

- ☐ 机上に放置された情報は、誰かに持ち去られたり、盗み見られたりする危険にさらされています。重要情報は放置せず、保管場所を定めて、鍵付き書庫等に保管して下さい。また、オフィスの戸締まりにも注意して下さい。
- ☐ ノートパソコンやタブレット端末、USB メモリ等は気軽に持ち運べる便利さがある一方で、盗難の危険性も高くなっています。重要情報が入った機器は学外に持ち出さないで下さい。

8. 情報の廃棄

- ☐ 重要情報が記載された書類をゴミ箱にそのまま捨てると、関係者以外の目に触れてしまい、重大な漏洩事故を引き起こすことがありますので、シュレッダーで裁断のうえ、廃棄して下さい。
- ☐ パソコン・記憶媒体を廃棄する場合は、削除操作をしても復元される恐れがあります。処分するときは、完全消去用ソフトを用いたり、専門業者に消去を依頼して、情報が復元出来ないように加工した上で廃棄して下さい。