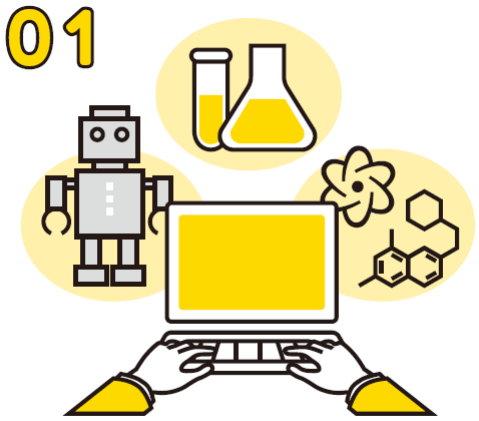
JAISTセキュリティ研修

2024年度版

JAIST CSIRT

あなたの生活や研究を守り、
安全で充実したJAIST生活をおくるために

情報環境の基本的な考え方



■ 教育・研究・事務処理等の業務に利用

- 情報環境に接続した個人所有の情報機器を含む
  - 学生寮・教員宿舎・VPNによる学外からの接続等
- 業務目的とは？
  - それぞれの業務内容に依存
  - 業務目的の利用であると説明できること
  - 判断に迷う場合は教職員やセンターに相談
  - 情報セキュリティポリシー・ガイドライン：
    https://www.jaist.ac.jp/member/personal/security.html

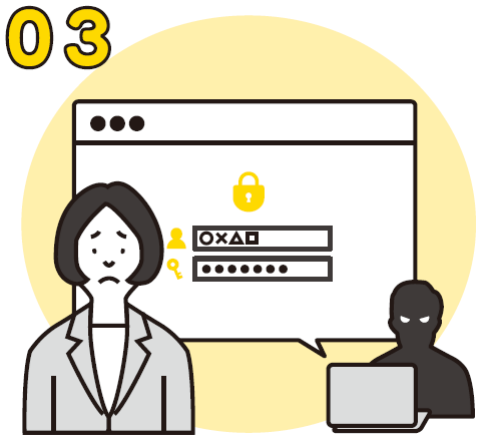
02

パスワードの重要性

■ パスワードを知られること ≒ 全ての情報を奪われること

- 他人が推測することが難しい複雑さに設定すること
  - 10文字以上，大小文字・記号・数字 / 推測されにくいもの
- 学外サービスのパスワードを使い回ししないこと
  - パスワード管理ソフトなどを活用
- パスワードは他人に教えないこと
  - 本学職員がパスワードの開示を求めることは絶対にありません
- パスワード変更：リセットアドレス登録後，変更ページで
  - https://www.jaist.ac.jp/iscenter/useraccount/password/

不正アクセスの禁止



■ 様々な不正アクセス行為

- 許可されていないシステムへの不正侵入
  - セキュリティホールの利用など
- 他人のユーザ名 / パスワードを利用した成りすまし
- 同一ページへの執拗なアクセスによるサービス妨害

■ 刑事・民事責任を問われる場合も

ウィルス対策(1)

■ コンピュータウィルス →
ソフトウェアの欠陥を悪用して感染

- 最新の修正プログラムの定期的な適用
  - Windows: Windows Update
  - Macintosh: ソフトウェア・アップデート
  - その他のOS: 最新状態を維持
- 最新のセキュリティパッチが自動適用される設定を推奨
- PC以外の機器の最新版への更新
  - スマートフォン, ネットワーク機器，IoT機器など

ウィルス対策(2)

■ マルウェア → 様々な経路から感染

- アンチウィルスソフトウェアの導入
  - 第三者団体の認定を受けたもの
    www.av-test.org
    www.av-comparatives.org
  - ウィルス定義ファイルの定期的な更新
  - 構成員向けにWindows/Macintosh用を配布
    ESET Endpoint Protection
    https://www.jaist.ac.jp/iscenter/software/eset/

フィッシングメール対策

■ フィッシングメール → 個人情報の詐取

- 誘導されたWebフォーム等でユーザ名と
  パスワードを入力しないこと
  - JAISTではhttpsを用いない学外サイトでユーザ名＋パスワードを
    入力させることはない (https://web-mail.jaist.ac.jp など)

■ 不審なWebサイトにアクセスしない

- マルウェア感染や不法行為で処罰される可能性
  - 海賊版ソフトウェア
  - 著作権上問題のある動画 / 音楽 / 漫画
  - 違法な薬物 / 武器 / ポルノ / 個人情報の販売 etc.

07

重要な情報の保護

- ■ 個人情報：個人を識別できる情報
  - 本学の個人情報保護についての情報
    - JAIST規則集（以下URL）で「個人情報」を検索
      - https://education.joureikun.jp/jaist/aggregate/catalog/index.htm
- ■ 研究データ：成果発表に用いたデータやノート
  - 安全保障に関わるものは国外への持ち出し制限も
  - 格付けガイドラインに従った適切な取り扱い
    - https://www.jaist.ac.jp/member/data/personal/rating-guideline.pdf
    - 電子メール等での宛先間違いや誤操作にも注意

著作権の順守

08

■ 著作物の対象
- 書籍・論文・レポート・音楽・映像
- Webページの文章や画像，ソフトウェア， etc.

■ 注意すべき行為
- 著作物の複製やネットワークで閲覧可能にすることは違法
  - 著作権者の許諾がある場合や法律で許可されている範囲を除く
- 著作権が侵害された音楽や映像のダウンロードも違法
- 誰もが著作物を作る(著作権を持つ)立場に

SNSの利用

■ インターネット上の不適切な発言や振る舞い

- 安易な書き込みによるトラブル
- 機密情報や公序良俗に反する内容の書き込み

  → 本学や本学構成員の良識が疑われる事態
- JAIST ソーシャルメディアガイドライン
  - https://www.jaist.ac.jp/member/personal/snsguideline.html
  - SNSにおける基本的な心得を理解すること

ネットワークの適切な利用

- 学外者に有線 / 無線LANを利用させない
  - 学内限定情報やサービスがアクセス可能
  - eduroamやゲスト利用が可能なものを除く
- 通信匿名化アプリケーションやVPNの私的使用
  - 世界中のユーザが学内に接続可能になるリスク
  - 研究等で必要な場合は所定の手続きに従うこと
    - ファイアウォール設定変更申請
      https://www.jaist.ac.jp/iscenter/security/firewall/

アプリケーションの適切な利用

- 仕組みや評判をよく調べて利用
  - 意図しない不法行為に加担しないために
  - 必要に応じて教職員やセンターに相談
- セキュリティの脅威となるアプリケーション例
  - 通信匿名化 / VPN / 通信制限迂回アプリケーション
    - VPNgate, Tor, Hotspot Shield, SpotFlux, Hola Unblocker, Mobility XE, Freenet 等
  - 自動公衆送信機能を持つファイル共有アプリケーション
    - Xunlei, LimeWire, Cabos, Winny, WinMX, Share, eMule, Perfect Dark 等

困ったときには…

■ トラブルを発見した場合には
- トラブルの種類・日時・ホスト名・場所
  - マルウェア等への感染
  - セキュリティ上の脆弱性や不具合
  - 著作権の侵害や機密情報の漏洩
  - 学外のシステム上での機密情報の公開 等
- JAIST CSIRT (sec-incident@ml.jaist.ac.jp)に報告
  - https://www.jaist.ac.jp/iscenter/security/hotline/
- 緊急避難措置として情報環境から切り離す場合も

最後に

- 少数のスタッフで運営，みなさんの協力が必要不可欠.
- ユーザの利便性を最大限考慮した運用・管理：適切な利用を.
- 無知からくるインターネットの被害者 / 犯罪者にならないように.
- 情報環境の詳細は https://www.jaist.ac.jp/iscenter/
- 問い合わせは isc-query@ml.jaist.ac.jp or 情報II棟2階のセンターまで.
- 情報セキュリティポリシー・ガイドライン：
  https://www.jaist.ac.jp/member/personal/security.html

安全で充実したJAIST Lifeを！