



# 情報セキュリティについて

2020年4月3日  
情報基盤センター

質問があるときは:

情報基盤センター利用者窓口(情報基盤センター棟2F)へ

場所が分からないときは:

学生便覧の後ろの方に地図があるので見てください

# アカウントとサービス

自分のノートパソコンを使って大学で学習・研究・生活するために

- 九工大ID(オリエンテーション時に配布)
  - ネットワーク接続サービス
    - 学内無線LANサービス, 全学VPNサービス
  - 学習教育センター学習支援サービスMoodle
  - 教務情報システム(Live Campus)
  - 九工大メールサービス(認証ゲートウェイ)
  - 学認が提供するサービス(<https://www.gakunin.jp/>)
    - 電子ジャーナルも使えます
  - eduroam認証連携IDサービス
    - 他大学や海外での無線接続利用可能(別アカウントの発行が必要)
- 九工大メールアドレス(オリエンテーション時に配布)
  - 九工大メールサービス(Office365)
  - Office 365(Word, Excel, Powerpoint等)

# ネットワーク接続サービス

- 情報コンセントサービス (**学内無線LAN**)
  - キャンパス内に無線LANアクセスポイント設置
    - SSID: **KIT-IA, KIT-IB, KIT-EDU**
      - **九工大ID**での認証
    - SSID: **eduroam**
      - **他大学や海外での無線接続利用可能**
- 遠隔接続サービス (**全学VPN**)
  - 学外から学内のサービスを利用可能
  - **九工大ID**での認証
  - 情報基盤センター (ISC) オンラインガイド  
ホーム > VPN接続サービスの利用方法

# 大学包括ライセンス

- 学生の個人ノートパソコンでも利用可能
  - ウィルス対策ソフトウェア(トレンドマイクロ)
    - 大学のネットワークに接続する場合は  
ウィルス対策ソフトウェアを必ずインストールすること!
    - 窓口: 附属図書館情報工学部分館(学部1~3年生)
  - マイクロソフト教育機関向けライセンスプログラム  
(Office 365: Word, Excel PowerPoint等)
    - 詳しくはISCオンラインガイドへ
  - 数値解析ソフトウェアMATLAB
    - 詳しくは情報工学研究院 情報基盤室サイトへ  
<http://www.kiban-i.kyutech.ac.jp/matlab/>

# 九州工業大学情報システム利用規程

- インターネットで全世界とつながる便利と**危険**
- **九州工業大学情報システム利用規程**
  - アカウント管理, 制限事項, 禁止事項, 安全管理義務など。以下を参照のこと (新入生キットに封入)
    - 「ネットワークをよりよく安全に使うために」
    - 「情報基盤センターをはじめて使う人へ」
- **罰則あり**
  - 結果的に留年・退学も
- **コンピュータネットワーク利用に関する他規則**
  - 九州工業大学における情報セキュリティ・不正アクセス防止に関する規則

# 情報セキュリティとは

- 情報の機密性, 完全性, 可用性を確保すること
  - 情報の機密性  
アクセスが認められた人だけが, その情報にアクセスできる
  - 情報の完全性  
情報が破壊, 改ざん又は消去されていない
  - 情報の可用性  
情報へのアクセスが認められた人が, 必要時に中断することなく, その情報にアクセスできる
- 自分のパソコンやデータだけでなく, まわりの人や組織のものにも被害を生じさせないようにすること
  - 具体的にはどうすればよい?

# システムを最新に保つ **必**

- セキュリティソフトを導入して守りを固める
  - **トレンドマイクロ ウィルスバスター**
- パソコン本体とセキュリティの状態を最新に保つ
  - 本体のファームウェア, OSのバージョンアップ
  - アプリケーションやセキュリティソフトのアップデート
- スマホやネットワーク機器も最新に保つ
  - Wifiルータ, ネットワーク対応のプリンタやカメラも
- ソフトやアプリは**原則公式ストア**から, 権限にも気を付ける
  - **フリーソフトウェアにウィルスが入っている事がある**

# バックアップを定期的に取り取る

- パソコンが故障したり，データが失われたりしても，バックアップがあれば(少し)安心
- Windows10標準機能「バックアップと復元」
- Mac標準機能「Time Machine」
  - バックアップを取ったときのパソコンの状況に戻すことができる
  - 外部の記憶メディア(USBメモリや外付けハードディスク等)にバックアップすること
- **定期的**にバックアップする習慣を身につけよう
  - もしもの時に，数年前のバックアップしかなかったら？



# 安全なパスワードを設定する(1)

- パスワードは金庫の鍵と同じです
- 簡単なパスワードは総当たり攻撃や辞書攻撃ですぐに破られます
- 安全なパスワード文字列は？
  - 名前などの個人情報から推測できないこと
  - 英単語を使用していないこと
  - アルファベットと数字が混在していること
  - 適切な長さであること
  - 類推しやすい並び方ではないこと

# 安全なパスワードを設定する(2)

- パスワードは金庫の鍵と同じです
  - 書かない
    - パスワードが書いてあるものを放置しない
    - 電子メールでやりとりしない
  - 言わない
    - 人に教えない
  - 忘れない
  - 使いまわししない

# 何が問題か？

- 想定される二次被害（漏洩したアカウント情報を用いた攻撃）
  - 迷惑メール送信
  - 架空請求
  - リスト攻撃

大学がセキュリティ機器を用いて学内システム・データを守っていても、外部サービスを利用して漏洩する可能性がある。

パスワードを使い回しすると、アカウントを不正利用される確率があがる。

自分が送受信したメールを用いてアドレス帳を使った標的型攻撃の送信元となる（加害者となる）

# 不確かな情報源は信用しない

- メールやブラウザ内のリンクを安易にクリックしない
  - メールリンク機能は便利だが、不審なサイトへの誘導も
  - URLが正規のものであるかを確認してからクリックする
- メールの添付ファイルを安易に開かない
  - 添付ファイルを開く(=実行)とマルウェアに感染することも
  - 見知らぬ他人からの添付ファイルは決して開かない
  - 差出人が詐称されている場合もあるので、たとえ知人であってもタイトルや本文が不審なものは開かない
  - 添付ファイルを開いたのと同じことになるので、メールのプレビュー機能は使わない
- メールの真偽は確かな情報源で確認
  - メール本文に記載されている連絡先に連絡したり、届いたメールへ返信して問い合わせはしない

# 無線LANを安全に利用する

- 識別名「**SSID**(Service Set Identifier)
  - アクセスポイント名
  - 信用できる組織が提供しているSSIDにしか接続しないこと！
- 通信内容を暗号化するための「**暗号化方式**」
  - なし, WEP, WPA-PSK, WPAパーソナル, WPAエンタープライズ等
  - 暗号化方式が「なし」は情報ダダ洩れ. 危険なので接続しないこと
- 暗号化のための鍵となる「**暗号キー**」
  - 機器に接続するためのパスワード的にも使われる

# 知的所有権を侵害しない**必**

- ソフトウェアを利用するとき
  - 特定の条件下で、ソフトウェアを使用する権利（使用権）  
← 所有権を持っているわけではない
    - × 複数台のパソコンにインストールしたり、コピーして他の人に渡す行為
- 画像や音楽を利用するとき
  - × 雑誌や本に載っている画像をスキャナで取り込んで権利者に無断でWebページに乗せる行為
  - × 音楽CDからパソコンに取り込んでWebページのBGMに使用する行為
  - × 無償の共有ストレージに公開されていたコミックのzipファイルをダウンロードする行為

# 不正アクセスの禁止 **必**

- 不正アクセス行為を行ったもの【第3条】
  - 3年以下の懲役又は100万円以下の罰金
- 他人のID・パスワードを不正に取得する行為【第4条】
  - 1年以下の懲役又は50万円以下の罰金
- 他人のID・パスワードを提供する行為【第5条】
  - 相手に不正アクセス行為をする目的があったことを知っていた場合
    - 1年以下の懲役又は50万円以下の罰金
  - 相手に不正アクセス行為をする目的があったことを知らなかった場合
    - 30万円以下の罰金
- 他人のID・パスワードを不正に保管する行為【第6条】
  - 1年以下の懲役又は50万円以下の罰金
- ID・パスワードの入力を不正に要求する行為(フィッシング行為)【第7条】
  - 1年以下の懲役又は50万円以下の罰金

# 有害サイトへのアクセスの禁止 **必**

- 仮想通貨のマイニング
- ポルノ, アダルト, 危険薬物
- スпам, フィッシングサイト

## 通信をブロックしています

- ! おいしい話には必ず裏がある!
- ! 危険なサイトには近づかない!
- ! 個人情報 はむやみやたらに公開しない





# 誹謗・中傷してはいけない **必**

## • 名誉棄損罪

- 公然と事実を摘示し、人の名誉を毀損したもの
- **3年以下の懲役もしくは禁錮又は50万円以下の罰金**

ホームページの伝言板に、他人の名前を使って「恋人募集中」という内容を掲示したり、性的な中傷を行うなど、他人の名誉を傷つけた場合、**名誉毀損罪**等に問われることもあります。

【平成28年6月検挙：福岡】

被疑者は、インターネット掲示板に被害者の名前をかたって「お金を盗んだり、いじめを楽しんでいる・・・」などといったウソの書き込みをして、名誉を毀損したもの

[http://www.police.pref.fukuoka.jp/seian/seikei/cyokukennhouihan\\_2.html](http://www.police.pref.fukuoka.jp/seian/seikei/cyokukennhouihan_2.html)

福岡県警 サイバー犯罪対策課より

# SNSで気を付ける**必**

- 個人情報 は 基本的に 公開しない
- 個人が 特定 できる 情報は 投稿しない
- 他人が 映っている 写真を 勝手に 投稿しない
- 会った ことが ない 人と むやみに 友達 にならない
- 現実世界で 会おうと する 人を 警戒 する。 出会い系 に 近づかない
- 存在 する データ は 必ず 流出 すると 考える

インターネットに拡散した情報のすべてを消し去ることはできず、人生の節目であなたを苛むかもしれません

# 必須の対策

- パスワードの使いまわしはしない
- OSのバージョンは最新にする
- ウィルス対策ソフトウェアのシグネチャは最新にする
  - Windowsの場合はdefenderでも無いよりはまし
  - 「高いから」「買ってない」はインターネットに繋げてはダメ
  - Macだからと言って安心してはダメ
- 不審なメールは開かない
  - 開いてしまったら管理者へ連絡
- バックアップは定期的にする
  - もしランサムウェアに感染したら大事なデータが。。。。
- フリーソフトを無暗にインストールしない
  - 動画変換ソフトウェア・動画再生ソフトウェア・ダウンロード自動ツール
  - おまけでマルウェアが付いてきます
- ポップアップは要注意
- 事故を起こさないように→事故が起きても大丈夫なように



不審なメールの  
添付ファイルを  
開いたり、URL  
をクリックした  
場合は。

パソコン画面もそのままにして。

まずは

**「情報基盤運用室」**

に連絡！

外線093-884-3011

内線87-3011

E-mail [op-members@kiban.kyutech.ac.jp](mailto:op-members@kiban.kyutech.ac.jp)