大学生活と情報倫理

慶應義塾 CSIRT，慶應義塾ITC
（2023年度商学部導入教育情報リテラシー資料より一部抜粋）

Keio University
1858
CALAMVS GLADIO FORTIOR

情報倫理

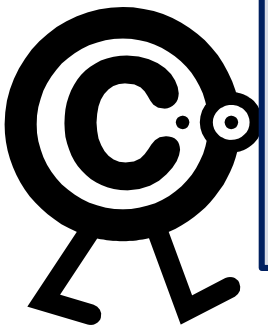
- 著作権の遵守
- セキュリティの対策
- インターネット利用時の注意

正しい知識、ルールとマナーが重要

著作権とは

- **著作物を創作した人（著作者）に発生する権利**
  - 著作者がその著作物の扱い方を決めることが可能

- **著作者に無断での複製・貸与・公衆送信などは法律によって禁止されている**



著作権を侵害すると「10年以下の懲役または1000万円以下の罰金」が科せられる

デジタル著作物の著作権(1/2)

デジタル技術への対応のため、著作権法は昨今頻繁に改正されている
（禁止事項を増やすだけではなく、新たに許可される事項もある）

□ 2012年

- コピーガードのあるDVD等のデータをPCへ取り込む行為の禁止
- 音楽や映像の海賊版のダウンロードの違法化
- コピー防止解除プログラムの作成禁止

□ 2018年

- 実情に応じた制限緩和
  - AI学習用途、キャッシュやバックアップへの保存、検索結果で表示されるコンテンツの一部
- 遠隔授業におけるコンテンツの利用に関する規定

デジタル著作物の著作権(2/2)

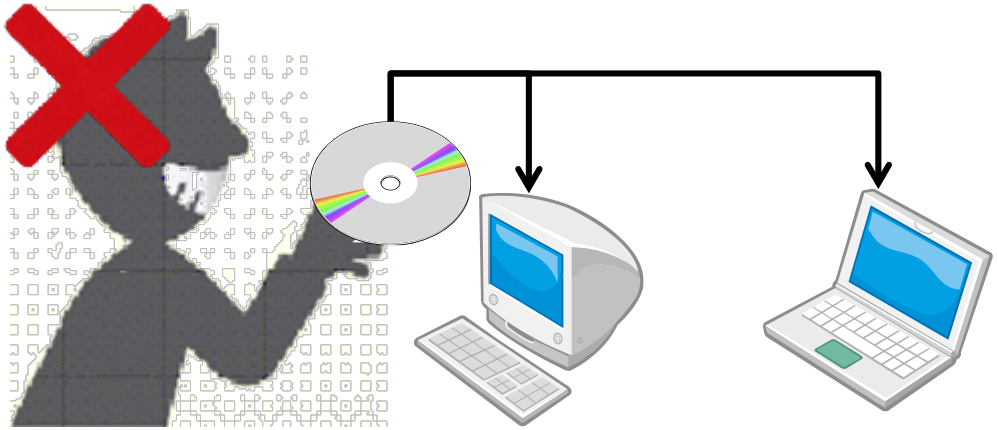
ロ 2020年

- 違法コンテンツへのリンクを集約したサイト（リーチサイト）の規制
- 書籍、漫画、論文、アプリなどの海賊版のダウンロードも違法化
- 不正シリアルコードによるアプリのアクティベーションの違法化

著作権への注意（貸し借り）

- **友人が購入したソフトウェア・映画DVD・音楽CD・書籍をコピーしてはならない**

※ 著作権上、現物の貸与は問題ないが、複製（コピー）は違法
※ 有償ソフトウェアの多くは、複数台のPCへのインストールを禁止している
※ 各ソフトウェアのライセンス事項を確認すること



著作権への注意（不正共有）

- **著作者に無断で音楽・動画ファイル、漫画、雑誌などをダウンロード・アップロードしてはならない**

  ※ 著作者に無許可でのアップロードは違法
  ※ Webに不正に公開されたコンテンツのダウンロードも違法
  (違法配信されたものであることを知りながらダウンロードする行為は刑罰の対象)

- **自分に著作権のない、または著作者に無断での配布を禁止されているデータを、P2Pファイル共有ソフトウェアなどを利用してダウンロード可能な状態にする行為も禁止**

P2Pファイル共有ソフトウェア

- インターネットを通じてファイルを不特定多数で共有することを目的としたソフトウェア
  - BitTorrent, Xunleiなど
  - 他人の著作物を無許可で共有すると、著作権侵害に該当する

https://www.hc.itc.keio.ac.jp/ja/file_sharing.html

著作権への注意（レポート）

- **レポート作成の際、書籍やWebの情報（文章や図表）を出典を記さずに参考・引用してはならない**
  - ※ 出典を明記しないと盗用もしくは不正行為と見なされる
  - ※ 引用は著作権法で認められている
  - ※ 必ず出典を明記すること

Webや書籍、他人のレポートをコピーしたり、参考や引用の出典を明記しなかった場合はカンニングと見なされ処分の対象になります

アカウント管理時の注意

ロ パスワード漏洩による危険性

- アカウント名とパスワードが分かれば
  アカウントの持ち主になりすますことが可能

ロ パスワード漏洩時の対処

- すぐにパスワードを変更し、すぐに管理者へ連絡
  - keio.jpアカウント、ITCアカウントの管理者はITCです。
    重要な問題ですので、直接ITC窓口までお越しください。
  - 日吉キャンパスのITC窓口：第七校舎地下一階

パスワードに関する注意

- 他サービスと同じパスワードを設定しない
- 他人に教えない
- 推測されにくいパスワードを設定する
- ショルダーハッキングにも注意
- パスワードマネージャの利用も一案

推測されやすいパスワード

- 自分や家族の誕生日/電話番号
- 辞書に載っている単語のみ
- ユーザ名やその主要部分と同じ文字列
- 数字、英字のみで短い
- 例：keiotaro, taro2001

推測されにくいパスワード

- 他人が見て意味が分からないもの
- 非常に長い文字列
- 大文字、小文字、数字、記号を含む
- パスワードマネージャが自動生成するもの
- 例：Xhx!s15$Rsk@, amsf elam kmea slfm plea

パスワードを盗まれると？

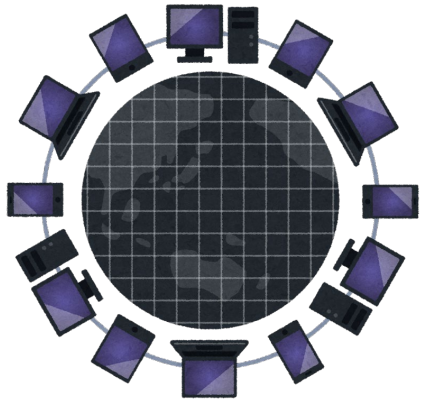
ロ 不正ログインされることで発生する不都合の例

- メールの送受信、閲覧をされる
  - マルウェア感染のためのメールに利用される
  - より「もっともらしい」フィッシングメールの素材にされる
- パスワードを勝手に変更され自分がアクセスできなくなる
- クラウドストレージの内容をコピー、改竄、消去される
- 履修申告等の重要な事務手続きを勝手にされる

ロ IDとパスワードが闇市場で販売される

- ソフトウェアや論文検索などを不正利用される
- 学内システムを攻撃するための経路として利用される
- 同じパスワードの他サービスも乗っ取られる

ダークウェブ
通常のブラウザなどではアクセスできない匿名性の高いネットワーク。違法な商品やサービスが売買される闇市場もある。



パスワード漏洩対策

- **推測されにくいパスワードをつけることは基本**
- **以降解説するこれらの対策は、パスワード漏洩に対しても非常に有効である**
  - フィッシング詐欺に気をつける
  - マルウェア対策を行う
  - 多要素認証を導入する

フィッシング詐欺への注意

ロ フィッシング詐欺

- 迷惑メールやWebサイトから利用者を誘導し、パスワードや個人情報、銀行・クレジットカード情報を打ち込ませて不正にアカウント情報を取得する詐欺
  - 特定の利用者に向けた詐欺メールも（標的型攻撃メール）

ロ 対策

- メール内のURLはクリックせず、
  必要に応じて正規の手順でパスワードを変更する
  など

フィッシングメールの例

From: keio.ac.jp <**********@gmail.com>
日付: 2016年8月22日 8:00
件名: Keio Admin

怪しい差出人

注意！！！
私たちの新しいウェブメールは、電子メールに速く利用、共有カレンダー、ウェブ文書や新2016アンチスパムバージョンを含む慶應義塾から新しいメッセージングシステムに改善されました。
この重要なアップデートに注意してください。
私たちの新しい慶應義塾改善されたメールボックスのためにあなたの更新を完了するために、次のリンクをご利用ください。

怪しいURL

http://logins.s*****.net/keio.ac.jp/SFC-CNS%20WebMail%20%20%20SFC-CNS%20WebMail.htmを更新する]をクリックします

http://www.hc.itc.keio.ac.jp/ja/news_20160822_email_phising_sfc.html より一部抜粋

偽サイトにアクセスし、フォームに慶應IDとパスワードを入力してしまった利用者は…

- 少なくとも、アカウントの名前が
  見知らぬ差出人名（政府組織（.gov）や海外の病院）に変更されていた。
- 新たな攻撃に使われそうだった？

マルウェアとは？

- **ウイルス、トロイの木馬、スパイウェア、ワーム等、システムに何らかの悪さをするプログラム**
  - データの破壊、個人情報の漏洩、遠隔制御など
  - 不正なWebページ、添付ファイル、USBメモリなどから感染することが多い
  - 近年はパスワードなどの認証情報を盗むことに特化したスティーラーと呼ばれる種類のマルウェアが大きな問題となっている

マルウェア対策(1/2)

- **OS・ソフトウェアのアップデートをこまめに適応し、最新の状態とする**
  - ただし最新の状態でも感染することはある(「ゼロデイ攻撃」など)
- **セキュリティソフトを利用する**
  - マルウェアなどを検知し防衛するソフトウェア
    - keio.jpから無料でセキュリティソフト(ESET)を入手・利用できる(1人につきPC1台まで)
    - Windows10以降なら標準のDefenderでも良い
  - ただしどんなセキュリティソフトも完璧ではない
    - 特に新種のマルウェアは検知をすり抜けることがある

PCでは必ずセキュリティソフトを使用すること

マルウェア対策(2/2)

ロ 不正コピーソフトやチートツール等の不審なソフトウェアを使わない

- 不正コピーのソフトウェアやゲームのチートツールなどには、スティーラーなどの悪質なマルウェアが含まれていることが多く、感染の主要原因の一つであることが知られている
- 不正コピーソフトなどの利用が違法なだけではなく、IDやパスワードなどが漏洩する原因となる

多要素認証とは？

- **パスワード（「知識情報」）だけではなく、「所持情報」や「生体情報」を組み合わせて認証すること**
  - 複数のパスワードを入力するのは多要素認証ではない
  - パスワードのみで読める可能性のあるメールアドレスに認証コードを送るのも多要素認証ではない
- **多要素認証の例**
  - パスワードとSMS（ショートメッセージ）を併用して認証
  - パスワードとスマートフォンの認証器アプリを併用して認証
  - パスワードとUSB認証キー、指紋認証、顔認証などを併用して認証

多要素認証のメリット

- **仮にフィッシングやスティーラーなどによってパスワードが漏洩しても、それだけではログインすることが困難**
  - 多要素認証を突破するための様々な手法が試みられ始めているが、それでも設定なしの状態と比べると非常に困難

FIDOデバイスの例

TOTP

keio.jpで利用可能な多要素認証の例

TOTP (Time-based One-Time Password)
スマートフォン上の認証器アプリ等で計算される数字を多要素認証で入力する

FIDO (Fast IDentity Online)
PCやスマートフォンの顔認証・指紋認証・パスコード認証や、USB認証キー等を多要素認証で利用可能

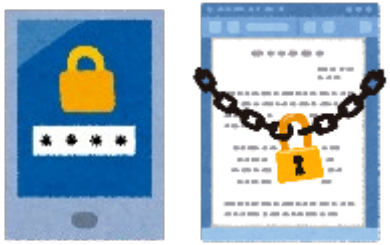
デバイスの紛失に関する注意

□ 紛失による個人情報の漏洩

- 携帯電話やスマートフォン、パソコンなど
  - 個人情報の宝庫（電話帳データ、アカウント情報など）
- USBメモリ
  - 多くの学生がレポートや名簿などを保存

□ 対策：端末のロック機能の利用、ディスクの暗号化

- ディスクだけでなく、通信自体の暗号化も重要



個人情報を含んでいる端末やファイルは
パスワードを必ず設定して管理をすること

SNSでの発言に関する注意

□ Social Networking Service (SNS)

- コミュニケーションや情報発信に欠かせないツール
  - Facebook, Twitter , Tiktokなど（ブログも例外ではない）

□ 注意して利用しないとトラブルを招く

- 全世界の不特定多数の人間が、あなたの投稿を閲覧できる
- 一度投稿した情報を完全に消し去ることは極めて困難
  - 迷惑メール・電話、誹謗中傷、ストーカー被害に発展する場合も
- 被害者にならないために、不用意に個人情報を記載しない
  - 本名, 住所, 電話番号, メールアドレス, 所属団体名など
- 加害者にならないために、他人の個人情報や誹謗中傷するような内容を投稿しない

・自分の発言には，しっかり責任を持つ
・発言の及ぼす影響について考えること

SNSトラブル事例集（1/2）

□　事例1

- A大学に合格した高校生がSNSで飲酒を自慢
- 某掲示板で炎上
  → 本人のプロフィールと写真が掲載される

□ 事例2

- 学部1年生がTwitterで飲酒運転をツイート
- Twitterで拡散後に某掲示板で炎上
  → 本人のプロフィールと写真が掲載される

SNSトラブル事例集（2/2）

□ 事例3

- 学部生が電車内で寝ている老人を撮影し、Twitterでその写真を公開
- 某掲示板で炎上
  → 本人のプロフィールや写真などが掲載される

□ 事例4

- 学部生がTwitterで不適切な内容を書き込む
- 某掲示板で炎上
  → 当事者には大学より無期限停学の処分

まとめ（情報倫理について）

☑ **著作権の遵守**

- 他人の著作物の扱いに注意
- レポート等を作成する時の参考・引用の出典を明記

☑ **セキュリティの対策**

- 利用するPCへセキュリティ対策ソフトをインストール
- OS・ソフトウェアの脆弱性修正プログラムをこまめに適応
- 個人情報を含む端末やファイルにはパスワードを設定

☑ **インターネット利用時の注意**

- SNSにおける発言の影響と責任を考慮
- 個人情報の慎重な取り扱い

参考：不正アクセス禁止法

- **IDやパスワードを盗まれないようにすることは重要ですが、逆に他人のIDやパスワードを盗んだり利用することは、不正アクセス禁止法で定められた犯罪です**
- **不正アクセス（三年以下の懲役又は百万円以下の罰金）とは？**
  - なりすまし：正当な理由なく他人のIDやパスワードでログインする行為
  - セキュリティホールの攻撃：特殊なプログラムやデータなどを用いてアクセス制御を回避する行為
- **その他不正アクセス禁止法で禁止されている行為の例**
  - 他人のパスワードを正当な理由なく、取得もしくは第三者に提供すること
  - 不正アクセスのためにパスワードを保管すること
  - フィッシングサイトなどでパスワードを騙し取ること

参考：慶應IDの取り扱い

- **慶應ID（keio.jpで利用されるID）の扱いに関してはkeio.jpの利用規定を参照**
  - ID等（ID・パスワードの組）を第三者に貸与、譲渡、売買、質入してはならない（第6条⑤）
  - ID等が第三者に漏洩や開示があった場合の不利益を理解し、自己の責任において厳重に管理・保障する（第6条⑥）
  - ID等の失念、第三者への漏洩や開示、第三者による利用が判明した場合は直ちに義塾に連絡する（第6条⑦）