セキュリティ

情報の科学　第3回

情報セキュリティ

情報セキュリティとは…？

悪意ある行為や突発的事故からコンピュータを守ること

以下の性質が守られなければならない

機密性	許可された人だけが情報にアクセスできること
完全性	情報が破壊されていたり、誤っていたりしていないこと
可用性	情報を使いたいときいつでも使えること
真正性	情報やユーザが本物であると確認できること
責任追跡性	何が起こったかを後から追跡できること
信頼性	想定した通りの結果が得られること
否認防止性	情報システム上あることが起きたことを、後になって否認されないように証明できること

ユーザ認証

① **ユーザID**…あなたは誰ですか？
② **パスワード**…証拠を見せてください
③ **バイオメトリクス**…本人の特徴を利用

パスワードに関する注意（復習）

ダメなパスワード
① 名前・誕生日・電話番号など類推されるもの
② 地名・辞書にある言葉・有名な固有名詞など

良いパスワード
1. 大文字・小文字・記号・数字などを混ぜる
2. いろいろなところで同じパスワードを使わない
3. パスワードは定期的に変えると良い

暗号

暗号…情報を特定の人にしかわからない形にしたもの
※他の人が見てもわからないから情報が守られる！
IAAHGRSI

暗号

暗号…情報を特定の人にしかわからない形にしたもの
※他の人が見てもわからないから情報が守られる！
IAAHGRSI→IAAH→
GRSI

暗号

暗号…情報を特定の人にしかわからない形にしたもの
※他の人が見てもわからないから情報が守られる！
IAAHGRSI→IAAH→IGARSHI　転置法…一定の規則で並べ替える
GRSI

暗号

暗号…情報を特定の人にしかわからない形にしたもの
※他の人が見てもわからないから情報が守られる！
IAAHGRSI→IAAH→IGARSHI　転置法…一定の規則で並べ替える
GRSI
JHBSBTIJ

暗号

暗号…情報を特定の人にしかわからない形にしたもの
※他の人が見てもわからないから情報が守られる！
IAAHGRSI→IAAH→IGARSHI　転置法…一定の規則で並べ替える
GRSI
JHBSBTIJ→IGARASHI　換字法…文字を別な文字にかえる
→シーザー暗号…文字をずらす

秘密鍵暗号と公開鍵暗号

① 秘密鍵暗号
暗号のルール(鍵)を秘密に共有
※鍵を渡すときが危険
② 公開鍵暗号
1. **受け手が公開鍵を公開**
2. **送り手が公開鍵で暗号化**
3. **暗号化された文章を送る**
4. **受け手は秘密鍵で複合化**

ディジタル署名とディジタル証明書

①ディジタル署名
公開鍵暗号を署名に利用したもの

② ディジタル証明書
なりすまして公開鍵を作られると困る
→公開鍵を第三者に認証してもらう

ソーシャルエンジニアリング

他人のコンピュータに不正侵入する手がかりを得ること

なりすまし (Masquerade)	○○へアクセスするパスワードを忘れてしまった。今すぐ必要なので教えてほしいなどと、本人になりすまして電話するなどして、情報を入手する。
ピギーバック (Piggybacking)	鍵のかかった建物や権限に、関係者、業者、同伴者などを装って侵入する。
ショルダーサーフィン (Shoulder Surfing)	コンピュータを操作している者の肩越しにのぞき込みをして、パスワードや暗証番号などの情報を盗み見る。
ゴミ箱あさり (Trashing,Dumpster Diving)	ゴミ箱をあさって、捨てられた機密情報を探します。
廃棄データ探索 (Data Salvage)	シュレッダーなどで細断された書類や廃棄されたディスク、コンピュータ、SDカード、携帯電話などから情報を収集する。

ソーシャルエンジニアリング

他人のコンピュータに不正侵入する手がかりを得ること

対策として…
①パスワードは人目に付くところに置かない
②人がいるときは重要な画面を開かない
③知人の個人情報をきかれても教えない
④情報を破棄するときは物理的に！

暗号のルールを調べて紹介しよう！

紹介する暗号のルールを決める
見た人が暗号をすぐ作れるようにパワポを作る
（授業で扱っていても、新しいものでも良いです）
（授業で扱ったものはより詳しくなるように！）
（そこまで行ければ）グループで紹介しあう

課題

本日のファイルをメールに添付して提出

宛先：五十嵐(e160189@gakushuin.ac.jp)

Cc：宅原先生(e080254@gakushuin.ac.jp)

件名とファイル名はクラス文理出席番号班番号氏名タイトル

- **クラスは東E西W中C南S北Nのアルファベット半角**
- **文理は文系B理系Rのアルファベット半角**
- **出席番号と班番号も半角（1桁の場合は0を補う）、空白無し**

（例）「東組理系45番1班五十嵐聡」の場合

件名・ファイル名 ： ER4501五十嵐聡自己紹介