講義（野本）課題
E0427／S0501

班ごとに題材を選び（？）
パワポ1枚でまとめる
- 八重桜祭で掲示（組班のみ記載）
- 小学生でもわかる内容に
- 30秒で理解できるものを目指そう

ポイント
- 文章は必要最低限に
- 惹きつけるキャッチフレーズなど

1. ユーザビリティ
2. アクセシビリティ
3. 架空請求・ワンクリック詐欺
4. フィッシング
5. テクノストレス
6. メディア産業

事例やメリット・デメリットを

講義（野本）課題　提出方法
E0427／S0501

確認
- 1枚になってますか
- 組班は入っていますか
- 小学生が30秒で見られますか

提出
- pdfに印刷（Microsoft Print to PDF）
- ファイル名は
  理組班番情報システム日付.pdf
  （例）RNZ0情報システム04XX.pdf
  - 日付は課題が出た日
    - E0427／S0501
  - 「番」は今回提出される方ので

情報セキュリティ

高Ⅲ情報の科学（理系）

野本悠太郎

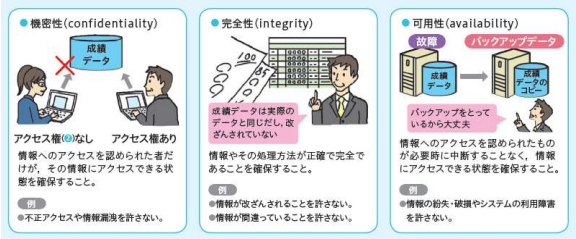
3. 情報セキュリティ

p.72

1. 情報セキュリティ技術

第3章第3節

情報セキュリティ
- 情報セキュリティに求められる3つの要素



3. 情報セキュリティ

p.73

1. 情報セキュリティ技術

第3章第3節

認証技術

「盗み見，聞き出し，重要な情報の入手」

3. 情報セキュリティ

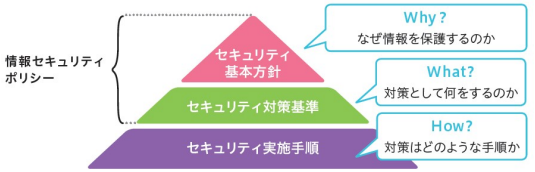
p.73

1. 情報セキュリティ技術

第3章第3節

情報セキュリティポリシー

- 情報セキュリティポリシー
  組織における情報資産のセキュリティ対策について，その基本的な考え方をとりまとめたもの。



情報セキュリティポリシーは，つねに評価・見直す必要がある。

3. 情報セキュリティ
マルウェア（悪いソフトウェアまとめ）

名称	内容
コンピュータウイルス	増殖し宿主となるソフトウェアが必要、不正プログラムを実行し他のプログラムへ
ワーム	増殖し宿主を必要とせず独立して動く、ネットワーク上で動くため感染力が強い
トロイの木馬	正常な文書ファイルなどに擬態、増殖せず基本的に他に感染しないため気付きにくい
スパイウェア	意図に反して個人情報などを収集し自動的に送信
キーロガー	キー入力を記憶、共用PCに取り付けてサイバー犯罪に利用されることも
ボット	リモート操作を可能にする、サイバー犯罪やスパムメールの大量送信に利用
Emotet	主にメールが感染経路となりアカウント情報やメール内容を盗み出し、それらを利用してさらに巧妙な偽装メールを作成

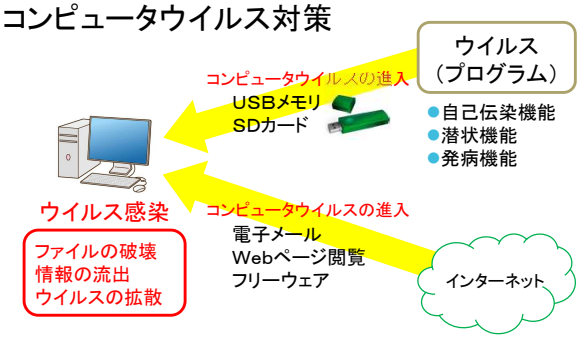
3. 情報セキュリティ

p.74

2. コンピュータウイルスとスパイウェア

第3章第3節

コンピュータウイルス対策



3. 情報セキュリティ

p.74

2. コンピュータウイルスとスパイウェア

第3章第3節

コンピュータウイルス対策

3. 情報セキュリティ

p.74

2. コンピュータウイルスとスパイウェア

第3章第3節

コンピュータウイルス対策

ウイルス感染

ウイルス対策ソフトウェア

● ウイルス定義ファイル
ウイルスに感染したファイルなどの特徴的なデータパターンが記述されたファイル。

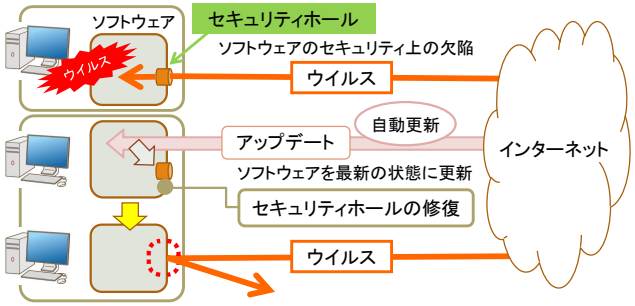
3. 情報セキュリティ

p.75

2. コンピュータウイルスとスパイウェア

第3章第3節

セキュリティホール



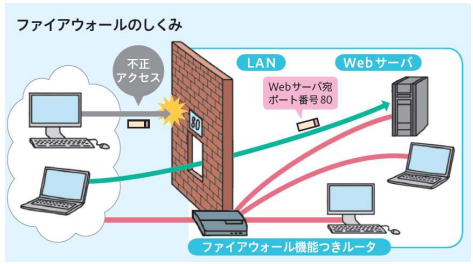
3. 情報セキュリティ

p.75

2. コンピュータウイルスとスパイウェア

第3章第3節

ファイアウォール



外部ネットワークからの不正な侵入を防ぐ技術

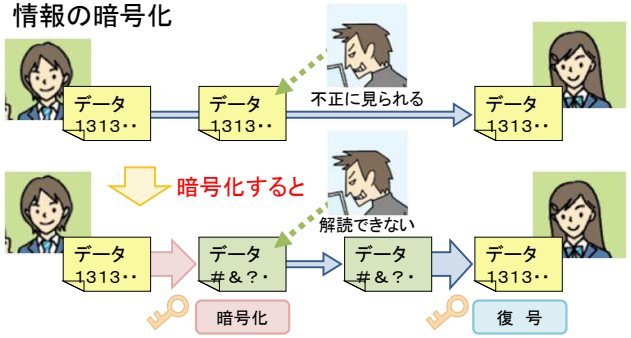
3. 情報セキュリティ

p.76

3. 情報の暗号化

第3章第3節

情報の暗号化



3. 情報セキュリティ

p.76

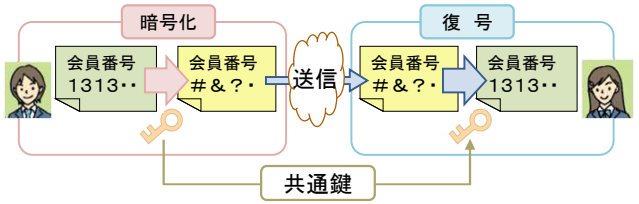
3. 情報の暗号化

第3章第3節

情報の暗号化

- 共通鍵暗号方式

暗号化鍵と復号鍵が同一の暗号方式。



共通鍵： 暗号化鍵と復号鍵が同一

3. 情報セキュリティ

p.76

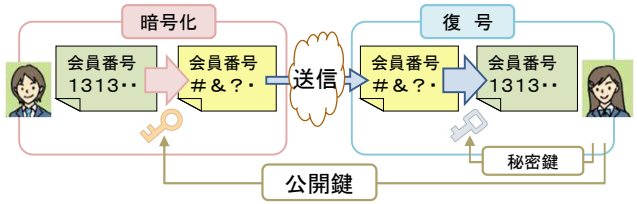
3. 情報の暗号化

第3章第3節

情報の暗号化

- 公開鍵暗号方式

暗号化鍵と復号鍵が異なる2つの対となる鍵を使用する暗号方式。



外部に公開

3. 情報セキュリティ

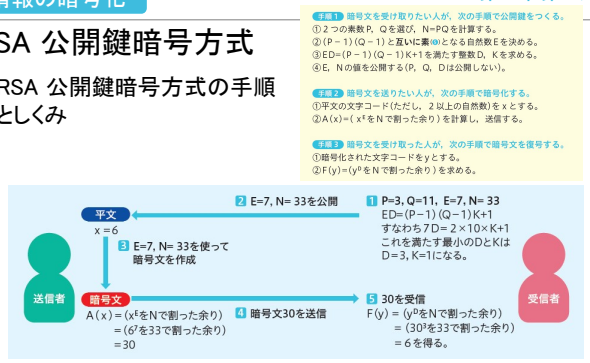
p.77

3. 情報の暗号化

第3章第3節

RSA 公開鍵暗号方式

- RSA 公開鍵暗号方式の手順としくみ



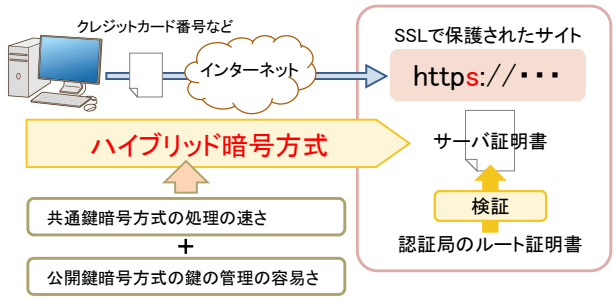
3. 情報セキュリティ

p.78

4. 暗号化と認証技術

第3章第3節

SSL



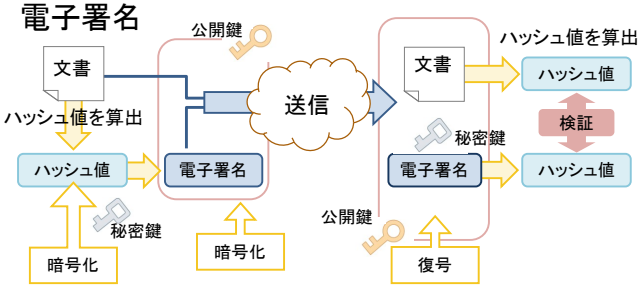
3. 情報セキュリティ

p.78

4. 暗号化と認証技術

第3章第3節

電子署名



- ハッシュ値：ファイルやメッセージなどから計算される値。

3. 情報セキュリティ

p.79

4. 暗号化と認証技術

第3章第3節

無線LANのセキュリティ技術

- 暗号化方式とセキュリティ強度

	暗号化なし	WEP	WPA (WPA－PSK)	WPA2 (WPA2－PSK)
特徴	暗号化なしの通信	アクセスポイントと端末間をWEPキー（秘密鍵）で暗号化して通信	WEP の改良版	WPA の改良版
暗号化方式	—	WEP	TKIP	AES
暗号化の強度	×	×（弱い）	△（脆弱性あり）	○（強い）

講義（野本）課題

E0508／S0515（回収は、、、）

班ごとに題材を選び
パワポ1枚でまとめる

- 八重桜祭で掲示（組班のみ記載）
- 小学生でもわかる内容に
- 30秒で理解できるものを目指そう

お好きな（？）
マルウェア
を1つ

ポイント

- 文章は必要最低限に
- 惹きつけるキャッチフレーズなど