

講義録レポート

講義録コード

04-63-1-102-01

講 座	応用情報技術者	科目①	講義編
目標年	2016年4月合格目標	科目②	基本講義 (セキュリティ基礎)
コース	本科生/A/B 本科生プラス/A/B	回 数	1 回
用 途	個別DVD ・ テープレクチャー ・ 集合ビデオ WEB ・ DVD通信 ・ 資料通信		

講師名	根岸 先生	講義録枚数	8 枚	※レポート 含まず
		補助レジュメ枚数	0 枚	サイズ (B5)
		その他	1 枚	

講義構成	前半講義 (72分) → 休憩 (10分) → 後半講義 (75分)		
使用教材	試験対策テキストⅡ P. 202～P. 232		
配付教材 (※個別DVD生)	【本科生/A/B】受講ガイド 日程表		
	【本科生プラス/A/B・本科生/A/B】 本試験問題集(平成26年秋期) 本試験問題集(平成27年春期)		
	試験対策テキストⅠver2.1 試験対策テキストⅡver3.1 試験対策テキストⅢver4.1		
	午前対策問題集ver3.1 実力テスト第1回問題/解答解説/マークシート		
	実力テスト第2回問題/解答解説/マークシート 実力テスト第3回問題/解答解説/マークシート		
備考	※補助レジュメは、講義録の最後に添付しております。 【教材配付のタイミングについて】 個別DVD生：上記配付教材覧に記載の回に配付となります。 Web/DVD通信生：日程表もしくは受講ガイド記載の日程で送付となります。		

T A C 情報処理講座

情報処理	講義録	コース・講義等	応用情報	科目	基本講義 セキュリティ基礎	回数	1
------	-----	---------	------	----	---------------	----	---

配布物	★テスト類 : []	★その他の配布物1 : []	★その他の配布物2 : []	講師	根岸 先生
-----	-------------	-----------------	-----------------	----	-------

黒 板 内 容

P.202~

情報セキュリティ

(参) 信頼性

JISQ

RASIS

定義 CIA → ISO27001

暗号技術

Confidentiality : 機密性

Integrity : 完全性 ... 改ざん されていない
破壊 されない

Availability : 可用性 ... DoS攻撃など

真正性 · 信頼性 を受けない

責任追跡性 → デジタルフォレンジック

否認防止

(P.203)

定義 CIA → ISO27001) ISMSの
要求事項

情報処理	講義録	応用情報	科目	基本講義 セキュリティ基礎	回数	1
------	-----	------	----	---------------	----	---

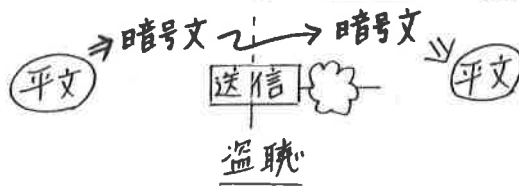
配布物	★テスト類： []	講師	根岸
	★その他の配布物1： []		
	★その他の配布物2： []		先生

黒板内容

P.209 p.209~213 リスクマネジメント → プログラム分野の
P.214 p.214 暗号技術 リスクマネジメントと同じ

平文 Plain text
暗号文 Cypher text
平文

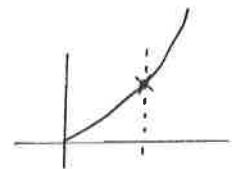
暗号化 encrypt
復号 decrypt



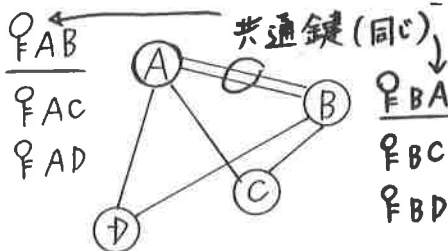
・共通鍵 (P.215~) 図4.5

暗号化・復号に同一の鍵を使う

- 処理 (暗号化/復号の) が速い
- × 鍵の個数が爆発的に増える



$$N \times N C_2 = \frac{N(N-1)}{2} \dots \text{全部で } 1 \text{人いくつ: } [N-1]$$



$$(N-1) \times N = 12 \times 11 = 132$$

$$132 \div 2 = 66$$

※ 全ての鍵が秘密

情報処理	講義録	コース講義等	応用情報	科目	基本講義 セキュリティ基礎	回数	1
------	-----	--------	------	----	---------------	----	---

配布物	★テスト類 []	★その他の配布物1 []	★その他の配布物2 []	講師	根岸 先生
-----	-----------	---------------	---------------	----	-------

黒板内容

公開鍵

秘密鍵

・ P で暗号化すると P のみ復号できる
 <機密性>

・ K " P "
 秘密鍵 公開鍵 <完全性>
 <署名>

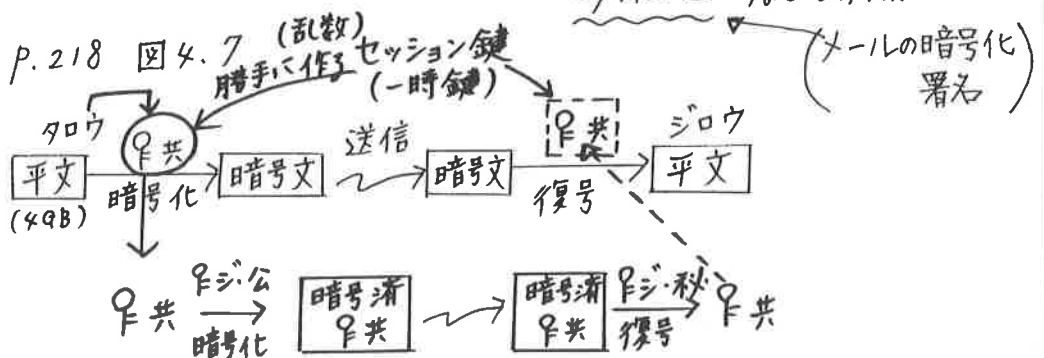
- 事前鍵交換が不要
 → 受信者から「公開鍵」を受取る
 受信者の公開鍵で暗号化
- 鍵の数が爆発的には増えない
 N 人 全部: $2N$ 1人あたり (2コ)

× 処理が遅い
 (暗号化・復号)

P.217 P.217 セッション鍵方式 → 共通鍵方式 公開鍵方式 の組み合わせ

- 処理が高速
- 事前鍵交換不要

※ SSL
 S/MIME など利用



情報処理	講義録	コース講義等	応用情報	科目	基本講義 セキュリティ基礎	回数	1
------	-----	--------	------	----	---------------	----	---

配布物	★テスト類 : []	★その他の配布物1 : []	★その他の配布物2 : []	講師	根岸 先生
-----	-------------	-----------------	-----------------	----	-------

黒板内容

暗号規格

鍵長 128, 256 bit

共通鍵方式 --- AES ~~DES, 3DES~~

公開鍵方式 --- RSA → 素因数分解の困難性を利用

DSA : 離散対数暗号

署名 [ECDSA : 楕円曲線暗号]

鍵長 2048 bit

384 bit

↓

RSAと比較して
短い鍵長で、同強度
が得られる

P.219 ~ P.219 ~ 認証 (主体)

(P.219 ~ P.224) [エンティティ] 認証 ... ユーザ認証などの本人確認

(P.224 ~ P.232) [メッセージ] 認証 ... 改ざんの有無のチェック ⇒ (署名)

(P.223) AAA制御 → アクセス制御に関する要素

認証 authentication

認可 authorization ... アクセス権を設定して
アクセスの許可/不許可を
コントロールする

責任追跡 accountable ... ログの取得

情報処理

講義録

応用情報

科目

基本講義 セキュリティ基礎

回数

1

配布物

- ★テスト類 : []
 ★その他の配布物1 : []
 ★その他の配布物2 : []

講師

根岸

先生

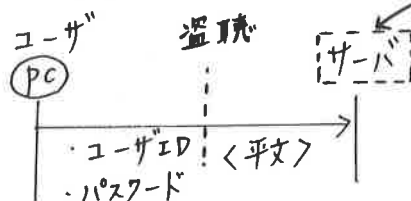
黒板内容

エンティティ認証

- ・パスワード認証
- ・バイOMETRICS認証
- ・所持品

○本人しか知り得ない
 持ち得ない

パスワード認証



偽サーバ
 (サーバのなりすまし)

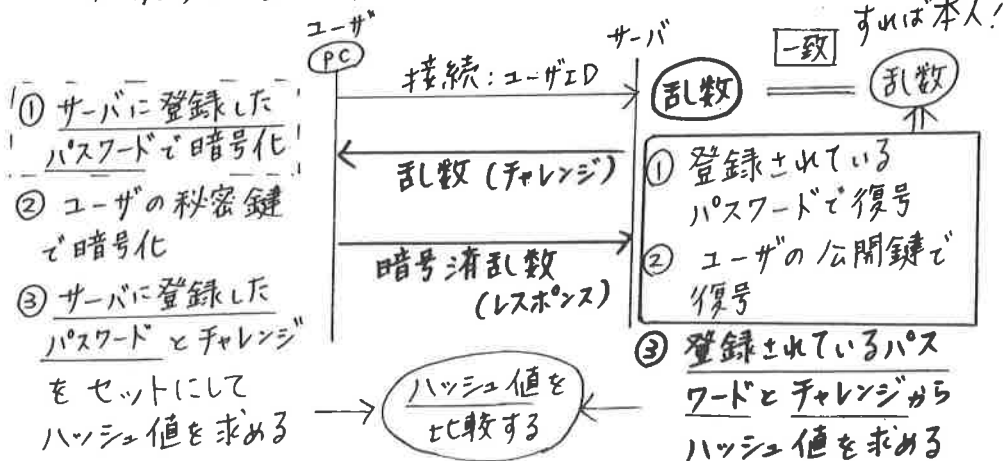
○SSL上で
 ↑使う

BASIC 認証
 PLAIN "
 USER/PASS"

P.221 チャレンジ・レスポンス認証

⇒ 相手に 直接 パスワードを送らない

③ ダイジェスト認証



情報処理 講義録	コース・講義等	応用情報	科目	基本講義 セキュリティ基礎	回数	1
----------	---------	------	----	---------------	----	---

配布物	★テスト類 : []	講師	根岸 先生
	★その他の配布物1 : []		
	★その他の配布物2 : []		

黒 板 内 容

攻撃: ・ 総あたり、ブルートフォース 攻撃
 ・ 辞書攻撃
 ・ パスワードリスト攻撃

アカウント
ロックアウト

侵入 → サイトA

→ サイトB

・ ユーザ
・ パスワード一覧

試す

事前入手したものを使う

P.220 バイオメトリクス認証

・ 本人拒否率 (FRR)
 ・ 他人受入率 (FAR)

↓
↓
好ましい
↓
実現は困難

FRR ↑ FAR ↓	↑ 厳
FRR ↓ FAR ↑	↓ ゆるい

判断基準

情報処理	講義録	コース 講義等	応用情報	科目	基本講義 セキュリティ基礎	回数	1

配布物	★テスト類	【	】	講師	根岸	先生
	★その他の配布物1	【	】			
	★その他の配布物2	【	】			

黒板内容

P.224

メッセージ認証

・デジタル署名

目的

・改ざんの有無のチェック

・署名者(本人)が作成したことの証明

・ハッシュ関数 / メッセージダイジェスト関数 (P.225)

(暗号学的な) P.225 × MD5
× SHA1
○ SHA2 (SHA-256)
SHA3

(本文)



指紋

・衝突困難性 ... 異なる入力から同じ

ハッシュ値は出ない

・原像計算困難性 ... ハッシュ値から元の
(一方向性) データは復元できない

・第二原像計算困難性 ... 同じハッシュ値をもつ
別データは作れない

署名 → ハッシュ値を署名者の秘密鍵で

暗号化したもの

↑
署名者にしか出来ない
ことをする

応用情報技術者 2016年4月合格目標 講義進度予定表

★休憩は適宜10分程度とします。

★分野別実践講義は本試験で選択される分野を中心に学習してください。

＜教室生の方へ＞分野別実践講義のうち組込みシステム開発/プロジェクトマネジメント①②/サービスマネジメント①②/システム監査①②はDVD受講となります。

	本 科 生 A	本 科 生 B	本 科 生 A	本 科 生 B	本 科 生 A	本 科 生 B	教室講座	個別DVD 視聴開始日	Web通信 配信開始日	DVD通信 DVD発送日	内容	使用テキスト
基本講義	■	■	■	■	■	■	11/15(日) 10:00～12:30 13:30～16:00	11/20(金)	11/24(火)	11/26(木)	基本講義①セキュリティ基礎 基本講義②データベース基礎 基本講義③ネットワーク基礎 基本講義④情報システム開発基礎	試験対策テキストⅡ 午前対策問題集
	■	■	■	■	■	■	11/22(日) 10:00～12:30 13:30～16:00	11/27(金)	11/29(日)	12/10(木)	基本講義⑤コンピュータシステム基礎① 基本講義⑥コンピュータシステム基礎②	
	■	■	■	■	■	■	11/29(日) 10:00～12:30 13:30～16:00	12/4(金)	12/6(日)		基本講義⑦コンピュータ科学基礎	
	■	■	■	■	■	■	12/6(日) 10:00～12:30 13:30～16:00	12/11(金)	12/13(日)	12/24(木)	基本講義⑧監査・マネジメント基礎① 基本講義⑨監査・マネジメント基礎② 基本講義⑩ストラテジ基礎	試験対策テキストⅠ 午前対策問題集
	■	■	■	■	■	■	12/13(日) 10:00～12:30 13:30～16:00	12/18(金)	12/20(日)			試験対策テキストⅢ 午前対策問題集
	■	■	■	■	■	■	12/20(日) 13:30～16:00		1/8(金)		セキュリティ①	試験対策テキストⅡ 午後対策問題集
	■	■	■	■	■	■	12/23(祝) 10:00～12:30 13:30～16:00	1/8(金)	1/10(日)	1/14(木)	セキュリティ② セキュリティ③	
	■	■	■	■	■	■	1/10(日) 10:00～12:30 13:30～16:00	1/15(金)	1/17(日)	1/28(木)	データベース① データベース② データベース③	
	■	■	■	■	■	■	1/17(日) 10:00～12:30 13:30～16:00	1/22(金)	1/24(日)		経営戦略/情報戦略① 経営戦略/情報戦略② 経営戦略/情報戦略③	試験対策テキストⅢ 午後対策問題集
	■	■	■	■	■	■	1/24(日) 10:00～12:30 13:30～16:00	1/29(金)	1/31(日)	2/4(木)	ネットワーク① ネットワーク② ネットワーク③	試験対策テキストⅡ 午後対策問題集
分野別実践講義	■	■	■	■	■	■	1/31(日) 10:00～12:30 13:30～16:00	2/5(金)	2/7(日)	2/18(木)	プログラミング(アルゴリズム)① プログラミング(アルゴリズム)② プログラミング(アルゴリズム)③	試験対策テキストⅠ 午後対策問題集
	■	■	■	■	■	■	2/7(日) 10:00～12:30 13:30～16:00	2/12(金)	2/14(日)		システムアーキテクチャ① システムアーキテクチャ②	試験対策テキストⅠ 午後対策問題集
	■	■	■	■	■	■	2/11(祝) 10:00～12:30 13:30～16:00	2/19(金)	2/21(日)	2/25(木)	情報システム開発① 情報システム開発②	試験対策テキストⅡ 午後対策問題集
	■	■	■	■	■	■	2/14(日) 10:00～12:30 13:30～16:00	2/19(金)	2/21(日)		組込みシステム開発 プロジェクトマネジメント① プロジェクトマネジメント②	試験対策テキストⅠ 午後対策問題集
	■	■	■	■	■	■	2/21(日) 10:00～12:30 13:30～16:00	2/26(金)	2/28(日)	3/3(木)	サービスマネジメント① サービスマネジメント②	試験対策テキストⅢ 午後対策問題集
	■	■	■	■	■	■		1/15(金)	1/17(日)	1/28(木)	システム監査① システム監査②	
	■	■	■	■	■	■	DVD受講 (要予約)	1/22(金)	1/24(日)	2/4(木)		
	■	■	■	■	■	■				2/18(木)		
	■	■	■	■	■	■						
	■	■	■	■	■	■						
	■	■	■	■	■	■						
	■	■	■	■	■	■						
	■	■	■	■	■	■						
	■	■	■	■	■	■						
直前期	■	■	■	■	■	■	2/28(日) 10:00～12:30 13:30～16:00	3/4(金)	3/6(日)	3/10(木)	午前総合① 午前総合②	午前演習レジュメ
直前期	■	■	■	■	■	■	3/6(日) 10:30～12:30 13:30～16:00		自宅演習		午後対策実力テスト 午後実力テスト解説	午後対策実力テスト 午後実力テスト/解答解説
	■	■	■	■	■	■		3/4(金)	3/4(金)	3/10(木)		
	■	■	■	■	■	■		公開模試 3/20(日) 9:30～15:30				
	■	■	■	■	■	■	DVD受講 (要予約)	3/21(月)	3/21(月)	3/17(木)	公開模試解説 午前 公開模試解説 午後① 公開模試解説 午後②	公開模試問題/解答解説

★公開模試は、通信生も書替手続を行なうことで会場受験に変更することができます。詳細のご案内は、1月15日～別途郵送にてお送りします。