

講義録レポート

講義録コード

04-53-1-102-01

講 座	応用情報技術者	科目①	講義編
目標年	2015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 本科生プラス	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	9 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 (75分) → 休憩 (10分) → 後半講義 (73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】受講ガイド 日程表		
	【本科生プラス・本科生】 本試験問題集(平成25年秋期) 本試験問題集(平成26年春期)		
	試験対策テキストⅠ ver2. 1 試験対策テキストⅡ ver3. 1 試験対策テキストⅢ ver4. 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

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 P.202 情報セキュリティの定義
 ISO 27001 ISMSの要求事項

表4.1 CIA

- Confidentiality : 機密性] → 暗号技術
 Integrity : 完全性]
 Availability : 可用性 → アクセス制御技術
- ・ 真正性
 - ・ 責任追跡性 → デジタルフォレンジック
 - ・ 否認防止 → 署名
 - ・ 信頼性
- 証拠

- ・ インシデント ... 事象、コトガラ
- ・ 脅威
- ・ 脆弱性 ... 弱点
- ・ リスク

P.214 P.214 暗号技術 → 機密性、完全性を保つ技術

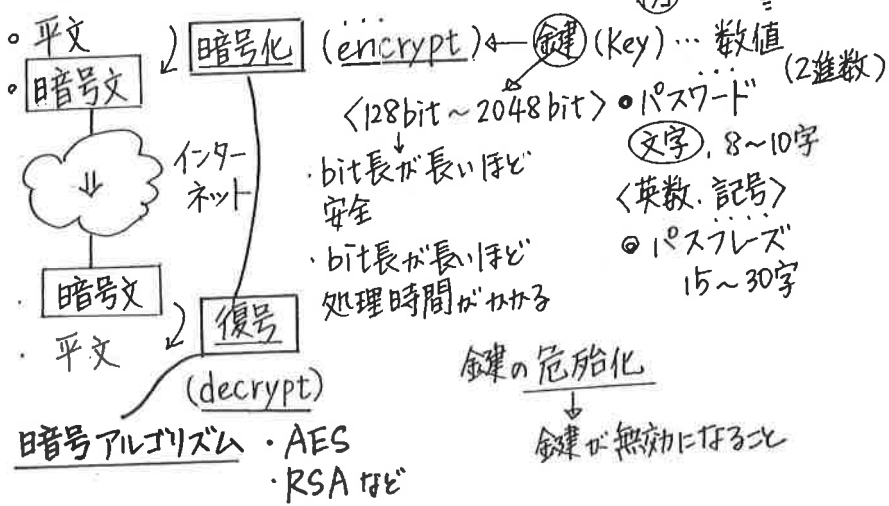
- 共通鍵方式
- 公開鍵方式
- ハイブリッド方式 / セッション鍵方式

情報処理 講義録	コース 講義等	応用情報	科目 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

図 4.3



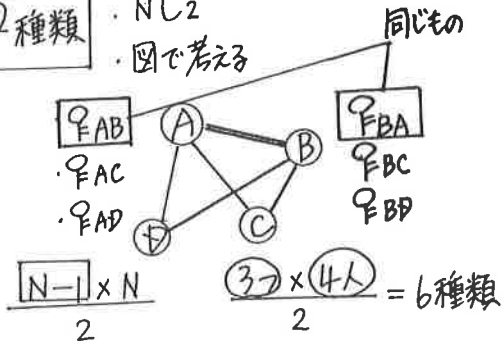
共通鍵方式

- 処理時間が短い (高速)
- × 管理する鍵の数が増える

$$N人 \rightarrow \frac{N(N-1)}{2} \text{種類}$$
 ・ $N C_2$
 ・ 図で考える

× 事前鍵交換が必要
 ↓

はじめて会った人
 どうしていきなり
 暗号通信できない!



情報処理 講義録	コース講義等	応用情報	科目 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

(機密) (署名)
 公開鍵 (public key) 秘密鍵
 ... ♀で暗号化すると、♂になる ♀のみ復号できる
 秘密鍵 (private key) 公開鍵
 ... ♂で暗号化すると、♀になる ♂のみ復号できる

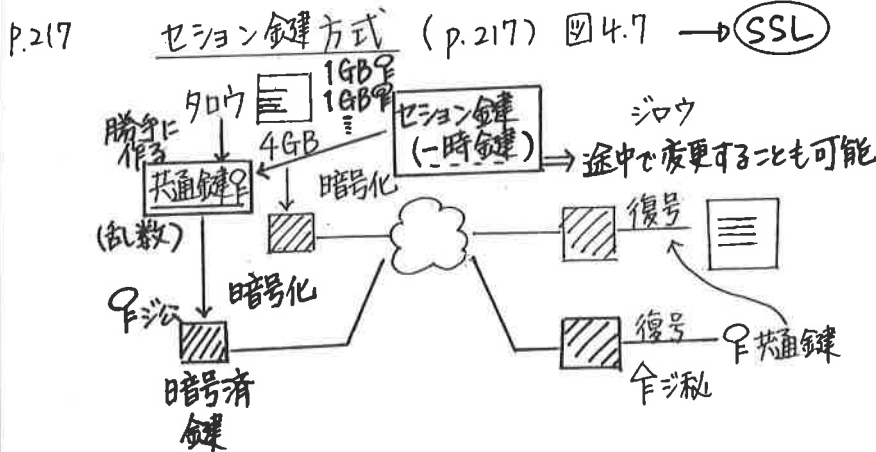
送信者の公開鍵
 送信者 → 受信者

送信者の秘密鍵
 送信者 → 受信者

送信者の秘密鍵
 送信者 → 受信者

送信者の秘密鍵
 送信者 → 受信者

送信者の秘密鍵
 送信者 → 受信者



情報処理 講義録	コース講義等	応用情報	科目	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.219 認証

- エンティティ認証 ... ユーザ、クライアント、サーバの真正性の確認
- メッセージ認証 ... 改ざんの有無の確認

P.225 P.225 図4.12

ハッシュ関数

→ データの格納用

Ⓢ セキュリティ用

<メッセージダイジェスト関数>

<暗号的なハッシュ関数>

○ 衝突困難性
別データなのに同じハッシュ値となることはない

データ

→

ハッシュ関数

→

結果

指紋: (ハッシュ値)

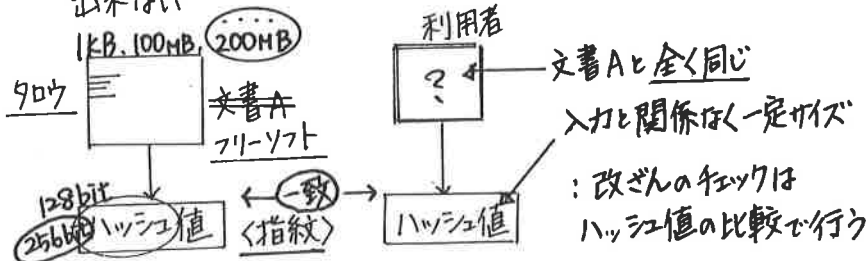
○ 原像計算困難性 (一方向性)

出力から入力値を求めることが出来ない

○ 第二原像計算困難性

同じハッシュ値を出す別の入力を作ることは

出来ない



情報処理 講義録	コース・講義等	応用情報	科目 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

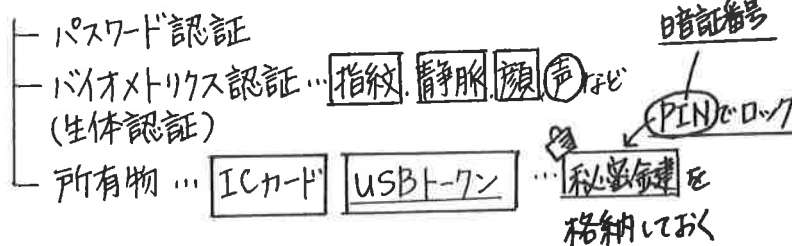
ハッシュ関数 (p.225)

× MD5

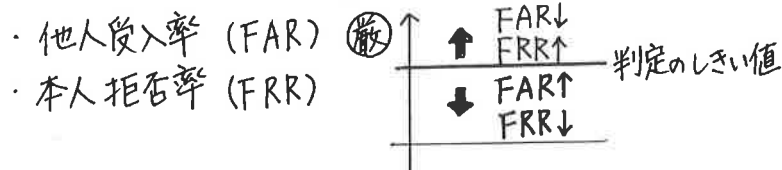
× SHA-1

推奨 ◎ SHA-2 (SHA-256)

p.219 ユーザ認証



- ・耐タンパ性 ... 物理的に分解したりして、動作を測定することで、秘密鍵を読み出す攻撃に対する耐性



情報処理

講義録

コース・講義等

応用情報

科目

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：[]

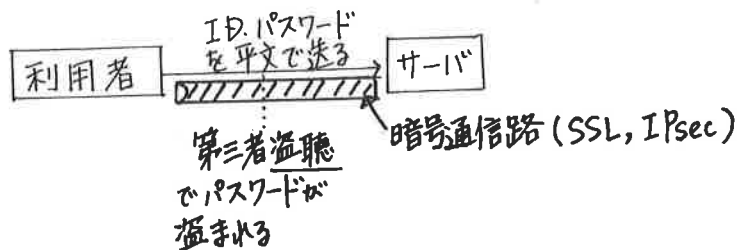
講師

根岸

先生

黒板内容

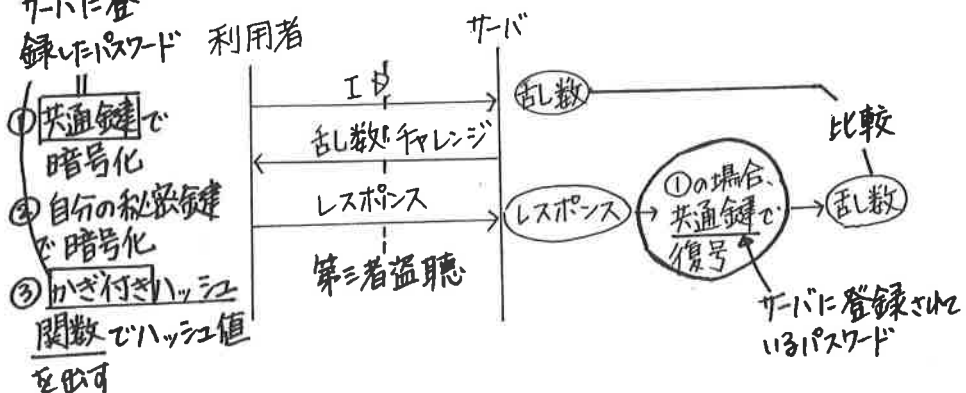
◎ パスワード認証のしくみ

・ 基本認証 (BASIC 認証, USR/PASS, PLAIN)

・ ダイジェスト認証 → ③のパターンでチャレンジ・レスポンス認証
 P.221 チャレンジ・レスポンス方式 (図4.8) をする

P.221

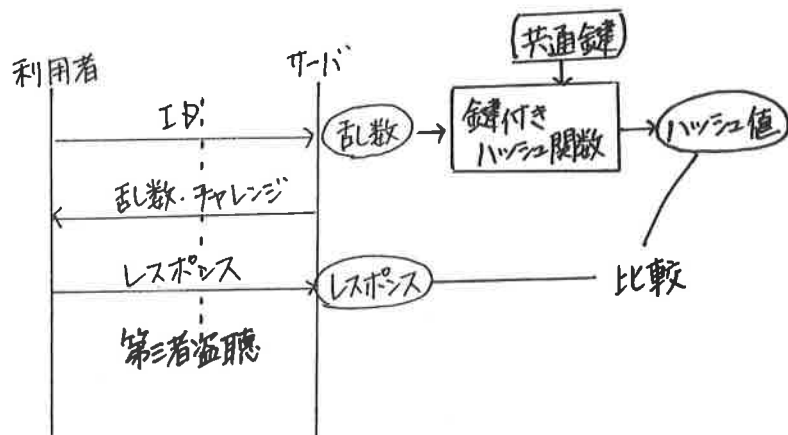
※ パスワードを直接相手に送らない!



情報処理 講義録	コース講義等	応用情報	科目 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



先生

応用情報技術者 2015年春期試験対策 講義進度予定表

★休憩は適宜10分程度とります。

★本科生/本科生プラス/上級コースの受講生は、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。

※＜個別DVD生の方へ＞分野別実践講義システムアーキテクチャ①②について、日程表に記載の視聴開始日は2/16(月)となっておりますが、2/17(火)に訂正いたします。

	本科生 プラス	本科生	上級	上級 A	上級 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	■	■	—	—	—	11/2(日) 10:00～12:30	11/7(金)	11/10(月)	11/13(木)	基本講義①セキュリティ基礎	試験対策テキストⅡ 午前対策問題集
	■	■	—	—	—	11/2(日) 13:30～16:00				基本講義②データベース基礎	
	■	■	—	—	—	11/9(日) 10:00～12:30	11/14(金)	11/16(日)		基本講義③ネットワーク基礎	
	■	■	—	—	—	11/9(日) 13:30～16:00			11/27(木)	基本講義④情報システム開発基礎	
	■	■	—	—	—	11/16(日) 10:00～12:30	11/21(金)	11/23(日)		基本講義⑤コンピュータシステム基礎①	試験対策テキストⅠ 午前対策問題集
	■	■	—	—	—	11/16(日) 13:30～16:00				基本講義⑥コンピュータシステム基礎②	
	■	■	—	—	—	11/23(日) 10:00～12:30	11/28(金)	11/30(日)		基本講義⑦プロジェクトマネジメント基礎	試験対策テキストⅢ 午前対策問題集
	■	■	—	—	—	11/23(日) 13:30～16:00			12/11(木)	基本講義⑧サービスマネジメント基礎	
	■	■	—	—	—	11/30(日) 10:00～12:30	12/5(金)	12/7(日)		基本講義⑨システム監査基礎	
	■	■	—	—	—	11/30(日) 13:30～16:00				基本講義⑩ストラテジ基礎	
分野別実践講義	■	■	■	■	■	12/7(日) 13:30～16:00	12/12(金)	12/15(月)		セキュリティ①	試験対策テキストⅡ 午後対策問題集
	■	■	■	■	■	12/14(日) 10:00～12:30	12/19(金)	12/21(日)	12/25(木)	セキュリティ②	
	■	■	■	■	■	12/14(日) 13:30～16:00				セキュリティ③	
	■	■	■	■	■	12/21(日) 10:00～12:30	12/26(金)	1/5(月)	1/8(木)	データベース①	
	■	■	■	■	■	12/21(日) 13:30～16:00				データベース②	
	■	■	■	■	■	12/23(火) 10:00～12:30	1/9(金)	1/11(日)		データベース③	
	■	■	■	■	—	12/23(火) 13:30～16:00				ネットワーク①	
	■	■	■	■	—	1/11(日) 10:00～12:30	1/16(金)	1/18(日)	1/22(木)	ネットワーク②	試験対策テキストⅢ 午後対策問題集
	■	■	■	■	—	1/11(日) 13:30～16:00				ネットワーク③	
	■	■	■	■	■	1/18(日) 10:00～12:30	1/23(金)	1/25(日)	2/5(木)	経営戦略/情報戦略①	
	■	■	■	■	■	1/18(日) 13:30～16:00				経営戦略/情報戦略②	
	■	■	■	■	■	1/25(日) 10:00～12:30	1/30(金)	2/2(月)		経営戦略/情報戦略③	試験対策テキストⅠ 午後対策問題集
	■	■	■	■	■	1/25(日) 13:30～16:00				経営戦略/情報戦略④	
	■	■	■	■	■	2/1(日) 10:00～12:30	2/6(金)	2/8(日)	2/19(木)	プログラミング(アルゴリズム)①	
	■	■	■	■	■	2/1(日) 13:30～16:00				プログラミング(アルゴリズム)②	
	■	■	■	■	■	2/8(日) 10:00～12:30	2/13(金)	2/15(日)		プログラミング(アルゴリズム)③	試験対策テキストⅡ 午後対策問題集
	■	■	■	■	■	2/8(日) 13:30～16:00				プログラミング(アルゴリズム)④	
	■	■	■	■	■	2/11(水) 10:00～12:30	2/17(火)※	2/18(水)	2/26(木)	システムアーキテクチャ①	
	■	■	■	■	■	2/11(水) 13:30～16:00				システムアーキテクチャ②	
	■	■	■	■	■	2/15(日) 10:00～12:30	2/20(金)	2/22(日)		情報システム開発①	試験対策テキストⅢ 午後対策問題集
	■	■	■	■	■	2/15(日) 13:30～16:00				情報システム開発②	
	■	■	■	■	■	DVD受講 (要予約)	12/26(金)	1/5(月)	1/8(木)	組込みシステム開発	試験対策テキストⅢ 午後対策問題集
	■	■	■	■	■					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	
	■	■	■	■	■					サービスマネジメント①	
	■	■	■	■	■		1/16(金)	1/18(日)	2/5(木)	サービスマネジメント②	試験対策テキストⅡ 午後対策問題集
	■	■	■	■	■					システム監査①	
直前演習	■	■	■	■	■	2/22(日) 10:00～12:30	2/27(金)	3/1(日)	3/5(木)	午前総合テクノロジ①	午前演習レジュメ
	■	■	■	■	■	2/22(日) 13:30～16:00				午前総合テクノロジ②	
	■	■	■	■	■	3/1(日) 10:00～12:30	3/6(金)	3/8(日)	3/12(木)	午前総合テクノロジ③	
	■	■	■	■	■	3/1(日) 13:30～16:00				午前総合ストラテジ・マネジメント	
直前期	■	■	■	■	■	3/8(日) 10:00～12:30	自宅演習			午後対策実カテスト	午後対策実カテスト
	■	■	■	■	■	3/8(日) 13:30～16:00	3/6(金)	3/8(日)	2/26(木)	午後実カテスト解説	午後実カテスト/解答解説
	■	■	■	■	■	公開模試 3/22(日) 9:30～15:30					
	■	■	■	■	■	DVD受講 (要予約)	3/23(月)	3/23(月)	3/19(木)	公開模試解説 午前 公開模試解説 午後	公開模試問題/解答解説 公開模試問題/解答解説

★公開模試は、通信生も書籍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22日～教材と同梱でお送りいたします。