

1. 科目コード

1225

2. 科目名

情報セキュリティ

3. 担当教員

嶋 久登 (Hisato Shima)

4. 開講期

春2期

5. 履修要件(前提科目)

「1206 コンピュータシステム基礎論」を受講しているか同時に受講することが望ましい。

6. 科目の目的・概要

本科目では情報システムの企画・開発・運用に必要な情報セキュリティの技術と管理の基礎を学ぶことを目的とする。各種のセキュリティ事故や攻撃を理解したうえで、そのような事故を防止、検出、対応するための手法を学習する。さらに、セキュリティ機能を実現するために重要な暗号技術の応用方法を学習する。

7. 授業概要

- 1 情報セキュリティとは
- 2 人的セキュリティと組織としての対策
- 3 マルウェアによるセキュリティ脅威とその対策
- 4 サーバーに対するセキュリティ脅威と対策
- 5 セキュリティワークショップ(1)
- 6 セキュリティワークショップ(2)
- 7 Webサイトに対するセキュリティ脅威と対策
- 8 情報セキュリティのリスクマネジメント
- 9 情報セキュリティと暗号技術、共通鍵暗号
- 10 暗号演習と公開鍵暗号
- 11 データの正しさの検証とデジタル署名
- 12 公開鍵証明書とPKI
- 13 学生発表
- 14 学生発表
- 15 セキュリティインシデント対応、情報セキュリティまとめ
- 16

8. 教科書

なし

9. 参考書

情報セキュリティ読本 四訂版: IT時代の危機管理入門
独立行政法人 情報処理推進機構、監修 土居 範久
実業出版

新版 暗号技術入門－秘密の国のアリス
結城 浩
ソフトバンククリエイティブ

10. 科目の学習目標

- (1) 情報システムのセキュリティに対するさまざまな脅威と対策を説明できる。
- (2) セキュリティ事故が発生した場合の対応方法を説明できる。
- (3) 共通鍵暗号と公開鍵暗号の使い方について説明できる。
- (4) セキュリティについてチームで調査し、発表できる。
- (5)
- (6)
- (7)
- (8)

11. 本学の教育目標と科目の学習目標との対応

教育目標		学習目標	
高度ICT スキルの修得	基礎的素養 専門知識および業務応用力	(1)(2)(3)	
人間力 (=探究力) の修得	自ら強みを磨き続ける力		
	自ら社会における 課題を発見し、 解決する力	課題設定	
		仮説立案	
		仮説検証	
	実行		
社会人基礎力	前に踏出す力		
	考え抜く力	(4)	
	チームで働く力	(4)	
職業倫理の修得			

12. 評価方法と配点

学習目標	達成度評価方法と配点					
	期末試験	小テスト	レポート	発表	成果物	その他
(1)		○		○		
(2)		○				
(3)		○				
(4)				○		
(5)						
(6)						
配点		60		40		

13. 評価基準

期末試験	
小テスト	毎週の小テストでその週の授業のポイントを出題し、理解しているかどうかを評価する。
レポート	
発表	セキュリティに関して、グループで選択したテーマについて調査し発表した内容、発表資料とプレゼンについて学生通しのピアレビューで評価する。

成果物	
その他	

14. アクティブラーニング

授業時間全体に占めるアクティブラーニングの時間的な割合	30%
1 授業で得られた知識や技能を活用し、出題された問題を解いたり、課題に取り組むなど能動的学習を行う	B
2 グループワークで課題に取り組み、学生同士が自由に発言することで何らかの課題に取り組むなど能動的学習を行う	B
3 能動的学習の成果を発表し、そのフィードバックを得て自ら主体的に振り返り、学習効果を高める	B
4 学生自身が主体となって、授業における学習の方向性を定める	C

15. 備考

本授業では教科書を利用しないが、授業資料をMoodleにて公開する。

16. 授業計画

(注) 授業計画は、あくまでも予定であり、実施時に、適時、追加・変更・修正等が生じる場合があります。

第1回 情報セキュリティとは (講義 90分)

本授業の内容、進め方および成績評価理解をするとともに、情報セキュリティの各種の事故や事件の実例を通じて、情報セキュリティとは何かを学ぶ。

1. 情報セキュリティとは
2. 本講義の進め方(学習目標、成績評価、等)
3. 情報セキュリティの傾向と事故例
4. 情報セキュリティの3要素:機密性・完全性・可用性

第2回 人的セキュリティと組織としての対策 (講義 90分)

情報セキュリティ事件の人的側面と組織としての対策について学ぶ。

1. 情報セキュリティ対策の人的側面
2. 情報セキュリティマネジメントシステム (ISMS)
3. 情報セキュリティの社内体制
4. 情報セキュリティの社内規定と運用

第3回 マルウェアのセキュリティ脅威とその対策

(講義 90分)

マルウェア(コンピュータウイルス)によるセキュリティ脅威を理解し、その対策を考えます。

1. マルウェア(コンピュータウイルス)とは
2. マルウェアの侵入経路とその対策
3. スケアウェア、ランサムウェア

第4回 サーバーに対するセキュリティ脅威と対策

(講義 90分)

情報システムのサーバーに対するセキュリティ脅威を理解し、その対策を考えます。

1. サーバーのセキュリティ
2. ユーザー認証とパスワード
3. ネットワークの分離とファイヤーウォール
4. ネットワークの監視

第5回 セキュリティワークショップ(1)

(講義 30分 演習 60分)

不正ソフトが行うシステムへの侵入行為の流れを実習し、その対策について考えます。

1. ネットワークへの侵入と情報収集
2. ターゲット機器の発見
3. ターゲット機器への侵入

第6回 セキュリティワークショップ(2)

(講義 30分 演習 60分)

不正ソフトが行うシステムへの侵入行為の検出方法について実習を続ける。また不正侵入の検出方法について学ぶ。

1. 不正実行
2. ログの分析
3. ログサーバー

第7回 Webサイトに対するセキュリティ脅威と対策

(講義 60分 演習 30分)

Webサイトの利用や運営に関するセキュリティ脅威と対策について学ぶ。

1. Webサイトのなりすまし
2. Webアクセスの暗号化
2. SQLインジェクション
3. Dos攻撃

第8回 情報セキュリティのリスクマネジメント

(講義 90分)

製品やシステムのセキュリティリスクマネジメントの手法を学ぶ。

1. リスクマネジメントとは
 2. 情報資産の特定
 3. 脅威の洗い出しと評価
 4. リスクへの対応
-

第9回 情報セキュリティと暗号技術、共通鍵暗号

(講義 90分)

情報セキュリティを守るために必要な暗号技術を学ぶ。共通鍵暗号の特徴と技術について学習する。

1. 情報セキュリティと暗号
2. 古典的な暗号
3. 共通鍵暗号 (DES, AES)
4. ブロック暗号のモード

第10回 暗号演習と公開鍵暗号

(講義 45分、演習 45分)

共通鍵暗号の演習の後、公開鍵暗号について学ぶ。また公開鍵暗号が共通鍵暗号と組み合わせたハイブリッド暗号を理解します。

1. 共通鍵暗号演習
2. 共通鍵暗号における鍵配信の問題
3. 公開鍵暗号、RSA暗号
4. ハイブリッド暗号システム

第11回 データの正しさの検証とデジタル署名

(講義 60分、演習 30分)

データの完全性の検証方法について学びます。データの完全性の検証に使われるハッシュ関数やデジタル署名の技術について説明します。

1. 公開鍵暗号演習
2. データの改ざんの検出
3. ハッシュ関数とデジタル署名
4. ハッシュ関数とデジタル署名演習

第12回 公開鍵証明書とPKI

(講義 90分)

公開鍵の証明書と公開鍵認証基盤(PKI)について学ぶ。

1. 公開鍵への電子署名
2. 公開鍵認証局とPKI
3. 暗号技術の選定
4. 暗号技術まとめ

第13～14回 学生発表

(発表 180分)

学生がグループで選択したテーマについて調査、研究した結果を発表する。

第15回 セキュリティインシデント対応、情報セキュリティまとめ

(講義 90分)

セキュリティ事故が発生した時の対応方法について学ぶ。これまでに学んだ内容を振り返り復習する。

1. セキュリティインシデント対応チーム (CSIRT)
 2. セキュリティインシデント対応のやり方
 3. 情報セキュリティまとめ
-