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学期

5. 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。
本科目では、情報セキュリティ対策のセキュリティポリシー策定や体制づくりなど「文系的」対策と、技術的なセキュリティ対策や暗号技術などの「理系的」対策の両方をカバーする。

6. 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. 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		(1)(2)(3)
	専門知識および業務応用力		
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			

8. 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。

9. 教科書

なし

10. 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ーティブ

11. 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		

12. 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。

13. 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 情報セキュリティの概要　(講義 90分)

まず、本授業の内容、進め方および成績評価を説明します。情報セキュリティの各種の事故や事件の実例を通じて、本授業の目的を理解します。

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. 情報セキュリティ事故例から学ぶ

第2回　情報セキュリティの考え方と人的セキュリティ　(講義 90分)

情報セキュリティ事件の傾向から特にセキュリティ対策のうち人的側面について学びます。また情報セキュリティの基本用語を説明し、情報セキュリティの考え方に親しみます。

1. 情報セキュリティ事件の傾向と対策
2. 情報セキュリティ対策の人的側面
4. 情報セキュリティの3要素:機密性・完全性・可用性

第3回　情報システムのセキュリティ脅威と対策（Part1）　（講義 90分）

情報システムのクライアント（パソコン、スマホなど）に対してどのようなセキュリティ脅威があるかを説明し、その対策について理解します。

1．コンピュータウィルスとは
2．メールやWebサイトを使った感染
3．ソーシャルエンジニアリング

第4回 情報システムのセキュリティ脅威と対策（Part2）　（講義 90分）

情報システムのサーバーに対してどのようなセキュリティ脅威があるかを説明し、その対策について理解します。

1．アドレススキャン、ポートスキャン
2．ユーザー認証とパスワード

第5回 情報システムのセキュリティ脅威と対策（Part3）　（講義 90分）

情報ネットワークに対してどのようなセキュリティ脅威があるかを説明し、その対策について理解します。

1．ネットワーク通信の監視
2．ファイヤーウォールとネットワークの分離
3．成りすまし、盗聴とSSL/TLS
4．無線LANのセキュリティ

第6回 情報システムのセキュリティ脅威と対策（Part4）　（講義 90分）

ネットワークサービスに対してどのようなセキュリティ脅威があるかを説明し、その対策について理解します。

1．Dos攻撃
2．Webサイトのセキュリティ
3．情報システムのセキュリティ脅威と対策のまとめ

第7回 情報セキュリティのリスクマネージメント　（講義 90分）

製品やシステムのセキュリティを強化するために必要なリスクマネージメントの手法を学びます。

1．リスクマネージメントとは
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8回 組織としてのセキュリティ対策　（講義 90分）

組織全体のセキュリティを強化するためのセキュリティポリシーの策定、体制作り、社内規定などの考え方を学びます。

1．情報セキュリティマネジメントシステム（ISMS）
2．情報セキュリティの体制作り
3．情報セキュリティの社内規定と運用

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とはどういうものかを理解します。共通鍵暗号の特徴を理解し、実際に広く使われているDES, AESについて学習します。

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 公開鍵暗号と暗号演習 （講義 45分、演習 45分）

暗号技術のうち、公開鍵暗号を実際に広く使われているRSAを使って説明します。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. 共通鍵暗号における鍵配信の問題
2. 公開鍵暗号、RSA暗号
3. ハイブリッド暗号システム
4. 暗号演習

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. データの改ざんの検出
2. ハッシュ関数
3. 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)について説明します。

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 テーマ発表 （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 60分、演習 30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びます。

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. インシデント対応演習
4. 情報セキュリティまとめ