1. 科目コード

1203

2. 科目名

情報セキュリティ基礎論 (Fundamentals of Information Security)

3. 担当教員

嶋　久登 (Hisato SHIMA)

4. 開講期

春 2 期　（昼）火曜 3-4 時限　（夜）火曜 6-7 時限

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。また、情報セキュリティに関するテーマについて学生がチームを組んで調査を行い、その内容をプレゼンテーションし、テーマの理解とコミュニケーション力の向上を図る。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) 情報セキュリティの事件を分析し、対策を考えることができる。
(3) セキュリティ事故発生の対応方法を説明できる。
(4) 共通鍵暗号と公開鍵暗号の使い方について説明できる。
(5) データの保護や署名、公開鍵認証の仕組みを説明できる。

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) (4) (5)
	専門知識および業務応用力		(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	(1) (2)
		仮説立案	(1) (2)
		仮説検証	
		実行	
	社会人基礎力	前に踏出す力	
		考え抜く力	(2) (3)
		チームで働く力	(2) (3)
職業倫理の修得			(2) (3)

8. 履修要件

「コンピュータシステム基礎論」を受講していることが望ましい

9. 教科書

なし

10.参考書

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

書籍名　：　新版　暗号技術入門－秘密の国のアリス
著者　：　結城　浩
出版社　：　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)		○				
配点		70		30		

12.備考

■ 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
4. 情報セキュリティと組織の責任

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3要素と基本用語を説明し、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.
3. ソーシャルエンジニアリングと内部犯罪
4. 情報セキュリティの3要素：機密性・完全性・可用性【C.I.A】.
5. 情報セキュリティに関する基本用語の説明（リスク、脆弱性、脅威、インシデント、対抗策など）

第3回　情報システムのセキュリティ脅威と対策（サーバ）　（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、その対策についてディスカッションを通して理解します。

1. サーバーを狙った攻撃とその対策
2. サービス中止を狙った攻撃
3. ウェブサイトを狙った攻撃とその対策
4. ネットワークのセキュリティ

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

情報システムのクライアント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、その対策についてディスカッションを通して理解します。

1. コンピュータウィルス
2. コンピュータういるうを送り込む方法とその防御

第5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. リスクマネージメントの進め方

第6回　リスクマネージメント演習　（演習 90 分）

具体的なシステム設計を想定しリスクマネージメントの手法を演習します。

1. 情報資産の洗い出しと整理
2. セキュリティリスクの特定と評価
3. リスク対応の選択

第7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。また、セキュリティの事故後の対応とセキュリティ監査の手法を学びます。

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ポリシー、対策基準、実施基準
4. セキュリティインシデント対応

第8回 セキュリティインシデント対応演習 （演習 90 分）

具体的な例をもとにセキュリティ事件が発生した時の対応方法について演習を通して学びます。

1. セキュリティインシデント対応チーム （CSIRT）
2. インシデント対応演習（グループワーク）

第9回 情報セキュリティと暗号技術 （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。

1. 安全な通信とは
2. 暗号とは
3. 古典的な暗号
4. 現代の暗号

第10回 共通鍵暗号と共通鍵暗号演習 （講義 45 分、演習 45 分）

暗号技術のうち、共通鍵暗号の特徴を理解します。共通鍵暗号として実際に広く使われている DES, AES と暗号利用モードについて学習します。

1. 共通鍵暗号とは
2. DES, Triple DES, AES
3. ブロック暗号のモード
4. 共通鍵暗号の演習

第11回 公開鍵暗号と暗号技術の選定 （講義 90 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。共通鍵暗号と公開鍵暗号の推奨リストを学びます。

1. 共通鍵暗号における鍵配信の問題
2. 公開鍵暗号とは
3. RSA 暗号
4. ハイブリッド暗号システム
5. 暗号技術に関する調達基準、推奨リスト

第12回 公開鍵暗号演習 **（演習 90 分）**

本授業では、公開鍵暗号とハイブリッド暗号を実際に使う演習を行います。

第13回 データの正しさの検証とデジタル署名 **（講義 45 分、演習 45 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．データの認証と完全性
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14回 公開鍵基盤(PKI) **（講義 45 分、演習 45 分）**

公開鍵暗号技術に使われる認証局と PKI について説明します。

1．公開鍵の正しさの認証
2．公開鍵認証局と PKI
3．PKI演習

第15回 テーマ発表プレゼンテーション **（プレゼンテーション 90 分）**

学生がグループでテーマを選択し調査した結果を発表し、その内容についてディスカッションします。