科目名
情報セキュリティ実践的教育

学習概要

・情報セキュリティの重要性と基礎的な技術について理解する。
・リスクを見出す問題発見の重要性について理解する。

前提知識・準備学習

・プログラミングの基礎
・情報科学の基礎(データ構造とアルゴリズム、ネットワーク基礎、OS 基礎、データベース基礎)

到達目標

・ネットワーク社会で起きている問題を知るとともに情報セキュリティの基本的な概念と必要性について、基礎知識を理解する。
・認証、暗号利用技術、アクセス制御等情報セキュリティに必要な基礎技術を理解する。
・ネットワークを構築、運用する際に必要なセキュリティ技術の基礎知識を理解する。
・Web アプリケーションとサーバ・デスクトップアプリケーションを例にソフトウェアセキュリティ対策を理解する。
・情報セキュリティマネジメントの重要性と必要性について理解する。

課題

・チームは、教員１名に対し最大３０名の学生を目安とし、１チーム４～５名程度の複数チーム編成を想定とする。
・課題テーマは、いずれも学生にとって理解しやすい、身近な事例を取り扱う。

評価方法と評価基準

評価方法：
・授業における個人ワーク演習課題とチーム演習課題、およびテスト
・授業終了後の受講レポート課題
評価基準：
※評価基準は、別紙ティーチングガイドを参照のうえ開示内容および開示可否を決定してください。

授業進行計画	
パッケージ 1：「ネットワーク社会の脆弱性と脅威」	
教育目標： 現在、ネットワーク社会で起きている問題を知るとともに情報セキュリティの基本的な概念と必要性について、基礎知識を理解する。	
第 1 回	テーマ：情報セキュリティの必要性と定義
	授業目標： 1. 安心・安全なネットワーク社会における情報セキュリティの必要性と重要性を理解する。 2. 情報資産における機密性・完全性・可用性の確保と維持を理解する。 3. 情報セキュリティのリスクに対する主な対策を理解する。
	授業内容： 現在、ネットワーク社会で起きている問題を知るとともに、情報セキュリティの基本的な概念と必要性について、基礎知識を講義およびグループ演習を通じて学習する。
第 2 回	テーマ：情報セキュリティの脅威と対策
	授業目標： 1. 情報セキュリティの人的脅威と対策を理解する。 2. 情報セキュリティの技術的脅威と対策を理解する。 3. 情報セキュリティの物理的脅威と対策を理解する。
	授業内容： 情報セキュリティにおける身近な脅威について、講義およびグループ演習を通じて学習する。
パッケージ 2：「情報セキュリティ基礎技術」	
教育目標： 認証、暗号利用技術、アクセス制御等情報セキュリティに必要な基礎技術を理解する。	
第 3 回	テーマ：情報セキュリティの要素技術（認証、アクセス制御、ソフトウェアのセキュリティ）
	授業目標： 1. 情報セキュリティ技術の全体像を理解する。 2. 認証・アクセス制御技術を理解する。 3. ソフトウェアのセキュリティを確保するための技術を理解する。
	授業内容： 情報セキュリティの技術的対策に必要な認証・アクセス制御、ソフトウェアのセキュリティ確保の基礎技術ついて、講義を通じて学習する。
第 4 回	テーマ：情報セキュリティの要素技術（暗号、ログ管理）
	授業目標： 1. 暗号利用のための基礎技術を理解する。 2. PKI と暗号通信を理解する。 3. ログ管理の必要性と技術を理解する。
	授業内容： 情報セキュリティの技術的対策に必要な暗号利用とログ管理の技術について、講義を通じて学習する。

授業進行計画	
パッケージ 3：「ネットワークセキュリティ」	
教育目標： ネットワークを構築、運用する際に必要なセキュリティ技術の基礎知識を理解する。	
第 5 回	テーマ：ネットワークの基本的な構成、ネットワークの脆弱性とリスク
	授業目標： 1. ネットワーク社会におけるネットワークの位置づけと利便性について理解する。 2. ネットワークの基本的な構成について理解する。 3. ネットワークの課題とリスクを理解する。 4. ネットワークの代表的な脅威と対策について理解する。
	授業内容： ネットワークセキュリティを学習する上で必要なネットワークの基本的な構成と、ネットワークの脆弱性について講義を通して学習する。
第 6 回	テーマ：情報セキュリティにおけるファイアウォールの位置づけと機能
	授業目標： 1. 情報セキュリティ対策の価値を理解する。 2. ネットワーク環境での主な脅威/攻撃について理解する。 3. ファイアウォールの役割と仕組みについて理解する。
	授業内容： 情報セキュリティにおけるファイアウォールの位置づけと機能について講義を通して学習する。
第 7 回	テーマ：ネットワークセキュリティを構成する要素技術
	授業目標： 1. ファイアウォールを構築するうえでの考慮点を理解する。 2. NAT 機能、VPN 機能の役割と仕組みについて理解する。 3. IDS/IPS の役割と仕組みについて理解する。
	授業内容： ネットワークセキュリティを構成する要素技術について講義を通して学習する。
第 8 回	テーマ：無線 LAN 環境（規格、暗号化、認証、その他の機能など）
	授業目標： 1. 無線 LAN の利便性と問題点について理解する。 2. 無線 LAN の規格と構成について理解する。 3. 無線 LAN で使用されるセキュリティ技術の仕組みと必要性を理解する。 4. 有線 LAN との違いを理解する
	授業内容： 無線 LAN 環境におけるネットワークセキュリティについて講義を通して学習する。

授業進行計画	
パッケージ 4：ソフトウェア脆弱性（Ⅰ）（Web アプリケーションセキュリティ）	
教育目標： Web アプリケーションを例にソフトウェアセキュリティ対策を理解する。	
第 9 回	テーマ：Web アプリケーションセキュリティ
	授業目標： 1. Web アプリケーションにおけるセキュリティを理解する。 2. Web アプリケーションの仕組みを理解する。 3. Web アプリケーションのセキュリティ対策の概要を理解する。
	授業内容： Web アプリケーションの現状として、どのようなところで使われているか、セキュリティが考慮されていないアプリケーションにはどのような危険性があるのか学習する。 Web アプリケーションの仕組み、クライアント・サーバマシンごとに考慮が必要なセキュリティ対策について学習する。
第 10 回	テーマ：Web アプリケーションに対する代表的な攻撃、 SQL インジェクション攻撃
	授業目標： 1. Web アプリケーションに対する代表的な攻撃を理解する。 2. SQL インジェクション攻撃を理解する。
	授業内容： Web アプリケーションの脆弱性をついた代表的な攻撃としてどの様な攻撃が存在するかを学習する。 脆弱性体験学習ツール AppGoat を用いて、SQL インジェクション攻撃の脅威・脆弱性・対策を学習する。
11 回	テーマ：クロスサイト・スクリプティング攻撃、Web アプリケーション開発時の対策
	授業目標： 1. クロスサイト・スクリプティング攻撃を理解する。 2. Web アプリケーションにおける設計・実装時の対策を理解する。
	授業内容： 脆弱性体験学習ツール AppGoat を用いて、クロスサイト・スクリプティング攻撃の脅威・脆弱性・対策を学習する。 Web アプリケーション開発における設計・実装時の対策、考慮すべき点について学習する。

授業進行計画	
パッケージ 5：ソフトウェア脆弱性（Ⅱ）（サーバ・デスクトップアプリケーションセキュリティ）	
教育目標： サーバ・デスクトップアプリケーションを例にソフトウェアセキュリティ対策を理解する。	
第 12 回	テーマ： バッファオーバーフローによるデータ破壊の危険性
	授業目標： 1. サーバ・デスクトップアプリケーションにおけるセキュリティを理解する。 2. C 言語、C++言語の概要、現状を理解する。 3. バッファオーバーフローの危険性を理解する。
	授業内容： サーバ・デスクトップアプリケーションの現状として、どのようなところで使われているか、セキュリティが考慮されていないアプリケーションにはどのような危険性があるのか学習する。 C 言語、C++言語について、歴史や特性、脆弱性の例について講義形式で学習する。 脆弱性体験学習ツール AppGoat を用いて、バッファオーバーフローの脆弱性について、事例を基に学習する。
第 13 回	テーマ： リソースリークによるサービス機能低下の危険性
	授業目標： 1. リソースリークの危険性を理解する。 2. サーバ・デスクトップアプリケーションの脆弱性について危機意識を持ち、脆弱性を防ぐための、設計時や実装時の留意点を理解する。
	授業内容： 脆弱性体験学習ツール AppGoat を用いて、リソースリーク脆弱性について、事例を基に学習する。 サーバ･デスクトップアプリケーション開発におけるセキュリティ面での脆弱性を防ぐ設計時や実装時の留意点を講義形式で行う。
パッケージ 6：「情報セキュリティマネジメント 」	
教育目標： 情報セキュリティマネジメントの重要性と必要性について理解する。	
第 14 回	テーマ：情報セキュリティマネジメントシステムの基礎知識
	授業目標： 1. 情報セキュリティにおけるマネジメントの基礎知識と情報セキュリティポリシーの役割を理解する。 2. リスクマネジメントを活用した情報セキュリティポリシーの策定方法を理解する。 3. 情報セキュリティ対策の有効性評価および適合性の維持活動を理解する。
	授業内容： 情報セキュリティマネジメントの重要性と必要性、および仕組みについて講義を通じて学習する。

授業進行計画	
パッケージ 7：「チーム演習」	
教育目標： 学習した内容について総合的なチーム演習を行い、情報セキュリティの重要性を理解する。	
第 15 回	テーマ：情報セキュリティにおけるリスクアセスメントとリスク対応（総合演習）
	授業目標： 1. 情報セキュリティにおける情報資産の特定および分類とその価値を理解する。 2. 情報資産に対するさまざまな脅威の特定と対策方法の有効性を理解する。 3. 情報活用の効率性と情報セキュリティ対策のバランスを理解する。
	授業内容： 情報セキュリティの対策を効果的に導入および実践するため、リスクアセスメントとリスク対応方法について演習を通じて学習する。

授業進行計画	
OPTION	テーマ：ネットワークの基礎
	授業目標： 1. 社会におけるネットワークの位置づけについて理解する。 2. ネットワーク通信を実現する要素を理解する。 3. ネットワーク通信の流れを理解する。 4. 代表的な通信サービスの仕組みについて理解する。
	授業内容： 情報セキュリティを学習するうえで必要なネットワークの要素について講義を通して学習する。

教科書・教材等
情報セキュリティ実践教育コンテンツ【テキスト、演習課題、演習課題解答例】

参考文献
「情報セキュリティ読本 四訂版 -IT 時代の危機管理入門-」実教出版 「マスタリング TCP/IP　入門編」オーム社

備考