科目名	情報セキュリティ							年度	2025
英語科目名	Information Security							学期	前期
学科・学年	ＩＴスペシャリスト科 ２年次	必／選	必	時間数	30	単位数	2	種別※	講義
担当教員	東堂隼平		教員の実務経験		有	実務経験の職種		システムエンジニア	

【科目の目的】

本講義を受講する学生は、ネットワークを介した不正攻撃、コンピュータウイルスの仕組みや対策、ファイアウォールの原理などのネットワークセキュリティ、共通鍵暗号、公開鍵暗号、ハッシュなどの暗号技術、暗号理論を応用した認証技術、電子透かし技術、セキュリティ監査およびセキュリティの標準、法規についての知識を身に着け、セキュリティマネジメント手法や対策など実学に基づく専門能力として社会で活用できるようになることを目的とする。

【科目の概要】

本講義では、セキュリティ技術の基本を学び、管理策（マネジメント手法）についても学び、社会で活用できるようにする。また、近年のサイバー攻撃事例の調査、発表を行う。学生が主体的に学ぶことができるよう、グループワークを採り入れる。他人が発する情報をどのように受けとめ、理解するか、さらにそれをどのように伝えていくかを意識しながら、講義を進める。

【到達目標】

セキュリティ技術の基本として暗号化、フィルタリングなどの知識を深め、セキュリティマネジメント、セキュリティ対策等の応用や活用例を知り、実社会において理解、活用ができるようになることを目標とする。また、近年のサイバー攻撃事例を学び、セキュリティに関連する話題、ニュース記事を理解し、興味を持ち、常にセキュリティ関連のトレンドを追いかけることができるようにする。

【授業の注意点】

本講義では学生の主体性を重視し、定期的に課題の提出を実施する。また、グループで考え、発表する作業があるため全員が積極的に参加し、時間内で効果的に作業を進める意識が肝要である。パソコン、教科書を忘れずに持参すること。授業時数の４分の３以上出席しない者は定期試験を受講することができない。

評価基準＝ルーブリック

ルーブリック 評価	レベル1 優れている	レベル2 ふつう	レベル3 要注意
到達目標 A	機密性、完全性、可用性などの要素とそれらの関係性について明確な理解を示し、適切に説明ができる	基本的なセキュリティ概念についての理解があるが、正確な定義や関連性の説明が一貫していない	基本的なセキュリティ用語や要素について理解できていない
到達目標 B	パスワード管理、セキュアな通信の確立などのセキュリティプラクティスを実践することができる	セキュリティプラクティスについての理解があるが、実践に十分な注意を払っておらず、改善の余地がある	基本的なセキュリティプラクティスを理解できていない
到達目標 C	セキュリティリスクの特定と評価を行い、リスクの優先順位付けや適切な対策の計画を行うことができる	セキュリティリスクの特定と評価を行えるが、リスクの優先順位付けや適切な対策の計画はできない	キュリティリスクの特定や評価方法に関する理解ができていない

【教科書】

【参考資料】

【成績の評価方法・評価基準】

試験・課題、小テスト、レポート、平常点

※種別は講義、実習、演習のいずれかを記入。

科目名		情報セキュリティ				年度	2025	
英語表記		Information Security				学期	前期	
回数	授業テーマ	各授業の目的		授業内容	到達目標＝修得するスキル		評価方法	自己評価
1	情報セキュリティ基礎①	情報セキュリティの重要性を理解する	1 2 3	セキュリティの三要素、攻撃の種類、セキュリティポリシー	セキュリティの基本概念を説明し、情報資産の保護の重要性を理解できる		1	
2	情報セキュリティ基礎②	サイバー攻撃手法を理解する	1 2 3	情報セキュリティ10大脅威	主要なサイバー攻撃手法について理解し、それらに対抗するための対策や防御方法を理解できる		1	
3	情報セキュリティ基礎③	暗号化技術、認証技術を理解する	1 2 3	暗号化技術、認証技術	暗号化技術と認証技術の基本的な概念と原則を理解し、それらのセキュリティ手法の実際の適用方法を理解できる		1	
4	情報セキュリティ基礎④	利用者認証・生体認証、公開鍵基盤を理解する	1 2 3	用者認証・生体認証、公開鍵基盤	利用者認証、生体認証、および公開鍵基盤の原則と適用方法を理解し、セキュリティ強化に寄与する方法を理解できる		1	
5	情報セキュリティ管理①	情報セキュリティマネジメントを理解する	1 2 3	情報セキュリティ管理、諸規程、ISMS	情報セキュリティの基本的な管理手法や法的要件、ISMSの概念を理解し、組織内のセキュリティ実践を支援することができる		1	
6	情報セキュリティ管理②	リスク分析と評価を理解する	1 2 3	情報資産、リスクの種類、アセスメント、リスク対応	情報資産の価値やリスクの種類を認識し、リスクアセスメントとリスク対応のプロセスを理解し、情報セキュリティを強化することができる		1	
7	情報セキュリティ管理③	情報セキュりティの取組みを理解する	1 2 3	セキュリティ組織・機関、セキュリティ評価	セキュリティ組織や機関の役割、セキュリティ評価の重要性を理解し、組織内でのセキュリティの効果的な管理と評価方法を理解できる		1	
8	情報セキュリティ対策①	人的、技術的対策を理解する	1 2 3	クラッキング・不正アクセス	クラッキングと不正アクセスの概念を理解し、その手法と対策について学び、情報セキュリティを向上させることができる		1	
9	情報セキュリティ対策②	技術的対策を理解する	1 2 3	マルウェア・不正プログラム、携帯・無線、証拠保全	マルウェアや不正プログラムの性質と影響を理解し、セキュリティ管理能力を向上させることができる		1	
10	情報セキュリティ対策③	物理的対策、セキュリティ実装技術	1 2 3	スマートカード、生体認証のアクセス制御	物理的なセキュリティ対策の重要性を理解し、さまざまなセキュリティ実装技術について知識を持ち、物理的セキュリティの設計と実装を理解できる		1	
11	法務	情報セキュリティに関する法務を理解する	1 2 3	情報セキュリティ関連法規、ガイドライン・倫理、標準化	情報セキュリティに関連する法規制、ガイドラインと倫理、標準化の重要性を理解し、これらの要素を組織内で適切に遵守することができる		1	
12	マネジメント	情報セキュリティとマネジメントの関連性を理解する	1 2 3	マネジメント、システム監査	情報セキュリティとマネジメントの相互関係と重要性を理解し、組織内での情報セキュリティマネジメントの実践方法を理解することができる		1	
13	テクノロジ	情報セキュリティとテクノロジの関連性を理解する	1 2 3	コンピュータシステム、データベース、ネットワーク	情報セキュリティとテクノロジの密接な関連性を理解することができる		1	
14	ストラテジ	情報セキュリティとストラテジの関連性を理解する	1 2	システム戦略、システム企画、企業活動	情報セキュリティとストラテジの密接な関連性を理解することができる		1	

		を理解する	3				
15	まとめ・試験	総合的に情報セキュリティマネジメントを理解する	1 2 3	総合復習	総合的に情報セキュリティマネジメントを理解できる	1	
評価方法：1.小テスト、2.パフォーマンス評価、3.その他							
自己評価：S：とてもよくできた、A：よくできた、B：できた、C：少しできなかった、D：まったくできなかった							
備考 等							