シラバス – 認証システム論 –

基本情報 科目概要 科目目標 履修前提条件 関連するバッジ 授業教材
期末試験実施方法について 授業時間外の学修と評価について 評価配分
各回の授業内容（予定）

基本情報

学部	IT総合学部
科目	認証システム論
教員名	末永 光弘
年度 / 学期	2026年度秋学期
開講期間	2026/10/2 ～ 2027/2/4
科目履修区分	専門応用（選択）／専門応用科目
単位	2
科目レベル	4

科目概要

認証技術とは、サービスやシステムを使用する際にユーザ本人であることを確認する技術を指し、セキュリティ確保のために活用されている。本講義では、認証技術の幅広い知識の習得や適切な認証技術の選択、簡単な認証連携の実装ができるようになることを目標とする。また、様々な認証技術を取り上げ、それらの特性を学習するとともに、AIやブロックチェーンを利用する認証技術の動向を学び、社会・個人への影響を考察する。さらに、OAuthによる認証連携の実装方法を解説し、理論的な学びと実践的なスキルを結びつける。

【科目コード】CS361

科目目標

【履修目標】
①認証技術の基本概念を体系的に整理し、システム全体のセキュリティ設計における認証の役割と重要性を、多角的な視点から論理的に説明できる
②多様な認証技術の仕組みを深く理解した上で、それぞれの長所・短所を比較・分析し、特定のシステム要件に対して最適な手法を論理的に導き出せる
③最新の攻撃手法やセキュリティ脅威を考慮し、堅牢性とユーザーの利便性を両立させたセキュアな認証システムの構成を具体的に設計・提案できる
④複雑なビジネス要件や技術的制約下において、認証技術の特性（多要素認証、適応的認証等）を最大限に活かすための最適な技術選定と、その妥当性の根拠を提示できる
⑤認証技術の最新動向が、将来の社会やビジネスモデルにどのような変化や課題をもたらすかを独自の視点で考察

できる
⑥認証技術が及ぼす社会的影響を深く洞察し、技術者として配慮すべき倫理的課題と具体的な対策案を論じることができる
⑦認証連携技術において、安全なプロトコルシーケンスを詳細に理解し、実際の開発現場でセキュアな実装を設計・検証できる

【到達目標】
①認証技術の基礎知識を理解し、説明できる
②多様な認証技術の仕組みと特性を理解し、説明できる
③パスワードの安全な管理等に配慮したセキュアな認証システムの仕組みと設計を説明できる
④それぞれの認証技術に適した状況を理解し、適切な技術を選択できる
⑤認証技術の動向を理解し、説明できる
⑥認証技術の社会的・倫理的影響を考察できる
⑦基本的な認証技術の実装手順を理解し、正しい実装手順を説明できる

※授業科目間における成績評価基準の統一化と修得基準の明確化を目的に、科目目標を履修目標と到達目標に分けて設定しています。履修目標と到達目標の定義は以下の通りです。
履修目標：授業を履修した人が、授業で扱う内容を十分に身につけたことを表す水準です。履修目標を概ね達成すれば、成績はBに相当します。
到達目標：授業を履修した人が最低限身につける内容を表す目標です。履修目標を達成するには、さらなる学修が必要な水準です。到達目標を概ね達成すれば、成績はDに相当します。

この科目とディプロマポリシーとの対応はこちらのページから確認してください

履修前提条件

・情報セキュリティ入門
の単位を修得済みであること。

関連するバッジ

セキュリティ

授業教材

教科書　※購入必須

なし

ツール

なし
※大学の定める必要環境はご用意ください。

参考資料　※購入任意

なし

その他の資料

なし

期末試験実施方法について

Webテスト形式

授業時間外の学修と評価について

・前回の講義内容について繰り返し視聴を行って復習し、次回の学習資料を確認して予習を行ってください
・不明な専門用語については図書館の提供する電子記事サービスや技術系Webサイトなどを使って調べてください

・発展的学習として、授業内で紹介する技術文書や参考資料を閲覧し、理解を深めてください
※各回の授業に臨むにあたり、これらの予習・復習を合わせて4時間程度行ってください

【オフィスアワーについて】
水曜　18:00～20:00
本学は通信制のためZoomで対応します。事前にURLを連絡しますので、希望する方は「学生サポートページ」のオフィスアワーフォームからお知らせください。
メールでの相談も受け付けています。予約フォームで「メールでの相談を希望」を選択した上で、申し込んでください。

評価配分

ディベート	レポート	小テスト	期末試験	その他	合計
10 %	10 %	40 %	40 %	0 %	100 %

各回の授業内容

回	授業内容および目次	小テスト他	備考(教科書、参考資料等)
第1回	1)タイトル: 認証技術の基礎と概要 2)学習目標: ・認証技術の基本的な知識を理解して説明することができる ・認証技術の歴史を理解して説明することができる 3)目次: 第1章 認証技術の基本概念 第2章 認証の種類 第3章 認証と認可の違い 第4章 認証の歴史と進化	・小テスト	
第2回	1)タイトル: パスワード認証 2)学習目標: ・パスワード認証の仕組みとパスワードの管理について理解して説明することができる ・パスワードに対する攻撃と対策について理解して説明することができる ・パスワード認証の最新の動向を説明することができる 3)目次: 第1章 パスワード認証の仕組み 第2章 パスワードの安全な管理 第3章 パスワード攻撃の種類 第4章 パスワード認証の最新事例	・小テスト	
第3回	1)タイトル: 多要素認証 2)学習目標: ・多要素認証の重要性を理解して説明することができる ・適応的認証について理解して説明することができる ・パスワードレス認証と多要素認証の未来について理解して説明することができる	・小テスト	

	3)目次: 第1章 多要素認証の重要性 第2章 多要素認証の種類と実例 第3章 リアルタイムリスク評価と適応的認証 第4章 多要素認証の最新事例		
第4回	1)タイトル: 認証基盤 2)学習目標: ・認証基盤の概要と技術を理解して説明することができる ・認証基盤のセキュリティ対策について理解して説明することができる ・認証基盤の今後の発展について理解して説明することができる 3)目次: 第1章 認証基盤の概要と重要性 第2章 認証基盤の技術 第3章 セキュリティ脅威と対策戦略 第4章 認証基盤の未来と進化	・小テスト	
第5回	1)タイトル: 公開鍵暗号とデジタル証明書 2)学習目標: ・公開鍵暗号の基本概念を理解して説明することができる ・デジタル証明書と認証局について理解して説明することができる ・SSL/TLSとHTTPSの役割について理解して説明することができる 3)目次: 第1章 公開鍵暗号の基本的な概念 第2章 デジタル証明書と認証局 第3章 SSL/TLSとHTTPSの役割 第4章 公開鍵暗号とデジタル証明書の最新事例	・小テスト	
第6回	1)タイトル: セキュアなシステム設計と認証 2)学習目標: ・認証システムのセキュリティ強化について理解して説明することができる ・アイデンティティとアクセス管理(IAM)について理解して説明することができる ・パスワードリセットとアカウント回復のプロセスについて理解して説明することができる 3)目次: 第1章 セキュアな認証プロセスの設計 第2章 アイデンティティとアクセス管理 第3章 パスワードリセットとアカウント回復 第4章 セキュアなシステム設計の最新事例	・小テスト	
第7回	1)タイトル: ネットワーク認証 2)学習目標: ・ネットワーク認証技術を理解して説明することができる ・ネットワークのセキュリティリスクと対策について認識して説明することができる ・ネットワーク認証におけるセキュリティアプローチの適用や評価について説明することができる	・小テスト	

	3)目次: 第1章 ネットワーク認証の基礎 第2章 Wi-Fiの保護 第3章 VPNとリモートアクセスの認証 第4章 ネットワーク認証の最新事例		
第8回	1)タイトル: OAuthとOpenID 2)学習目標: ・OAuthとOpenIDの概要を理解して説明することができる ・トークンと認可グラントタイプについて理解して説明することができる ・OAuthとOpenIDにおけるセキュリティ対策について理解して説明することができる 3)目次: 第1章 OAuthとOpenIDの基本的な概念 第2章 ソーシャルログインと委任認証 第3章 トークンと認証・認可 第4章 採用事例とセキュリティ対策	・小テスト	
第9回	1)タイトル: SAMLとシングルサインオン 2)学習目標: ・SAMLとフェデレーションの概要を理解して説明することができる ・シングルサインオンのメリットとデメリットを理解して説明することができる ・SAMLやシングルサインオンの最新動向を理解して説明することができる 3)目次: 第1章 SAMLの基本的な概念 第2章 SSOのメリットとデメリット 第3章 フェデレーション認証 第4章 SAMLとSSOの最新事例	・レポート	
第10回	1)タイトル: 生体認証の最新動向 2)学習目標: ・生体認証の概要を理解して説明することができる ・生体認証における問題点を理解して説明することができる ・生体認証の最新動向を理解して説明することができる 3)目次: 第1章 生体認証技術の基本 第2章 プライバシーと個人識別情報(PII)の問題 第3章 進化する生体認証攻撃 第4章 新たな生体認証技術の最新事例	・小テスト	
第11回	1)タイトル: ブロックチェーンと認証 2)学習目標: ・ブロックチェーン認証の概要を理解して説明することができる ・ブロックチェーン認証の最新動向を理解して説明することができる 3)目次:	・小テスト	

	第1章 ブロックチェーンの基本的な概念 第2章 ブロックチェーンを用いた認証システムの設計 第3章 デジタルアイデンティティと自己主権型ID（SSI） 第4章 ブロックチェーンと認証の最新事例		
第12回	1)タイトル： AIと機械学習を用いた認証 2)学習目標： ・AIと機械学習の認証技術への適用について理解して説明することができる ・AIと機械学習の最新事例について理解して説明することができる 3)目次： 第1章 AIと機械学習の基礎 第2章 AIを用いた行動認証とリスクベースの認証 第3章 AIと生体認証の統合 第4章 AIと機械学習を用いた認証の最新事例	・小テスト	
第13回	1)タイトル： 認証技術の社会的影響 2)学習目標： ・認証とプライバシー保護の重要性について理解して説明することができる ・アイデンティティやデジタルディバイドにおける問題について理解して説明することができる ・認証技術による社会的影響について理解して説明することができる 3)目次： 第1章 デジタル認証とプライバシー 第2章 デジタルアイデンティティと不平等 第3章 デジタルディバイドとアクセシビリティ 第4章 認証技術の社会的影響に関する最新の議論	・ディベート	
第14回	1)タイトル： 認証技術の未来 2)学習目標： ・様々な新技術が認証に与える影響について理解して説明することができる ・予測される将来の認証技術について動向を理解して説明することができる 3)目次： 第1章 クォンタムコンピューティングと認証 第2章 ゼロトラストアーキテクチャ 第3章 パスワードレスの未来 第4章 認証技術の未来予測と最新の研究動向	・小テスト	
第15回	1)タイトル： 認証連携の実装および講義のまとめ 2)学習目標： ・本講義で学んだ内容を復習する ・簡単な認証連携の実装手順について理解する 3)目次： 第1章 これまでの授業の復習 第2章 最新の認証技術のニュースと事例の紹介 第3章 Google認証連携の基本的な実装方法1 第4章 Google認証連携の基本的な実装方法2	・小テスト	

Copyright © 2011 Cyber University Inc. All Rights Reserved.