シラバス － 情報セキュリティ応用 －

基本情報

学部	IT総合学部
科目	情報セキュリティ応用
教員名	鈴木 耕二
年度 / 学期	2025年度春学期
開講期間	2025/4/3 ～ 2025/8/7
科目履修区分	専門講義（選択）／専門応用（選択）／専門応用科目
単位	2
科目レベル	3
サンプル授業	再生 第１回１章を見る ※学習評価（ディベート、レポート、小テスト、期末試験、その他の配分）については、「シラバス」内の記載事項が最新情報となります。「サンプル授業」内での教員の説明と異なる場合がありますので、必ずシラバスで最新情報を確認の上、履修を検討してください。

↑ページの先頭へ戻る

科目概要

本科目では、通信の暗号化や匿名通信網を始めとするネットワーク・セキュリティ技術、量子コンピュータによる暗号解読法や量子暗号、ブロックチェーンを用いた暗号通貨など、情報セキュリティに関連する最新の技術動向を学習する。上述のセキュリティ関連技術の学習に加え、近年急速に拡充しつつあるセキュリティ社会制度基盤や、サイバー攻撃/犯罪に関連する社会問題についても学ぶ。これらの学習を通じて、情報セキュリティ技術が私達の社会・経済に及ぼす影響を理解し、状況に応じた適切な情報セキュリティ対策を講ずる上で必要とされる知識を修得する。

【科目コード】CS304

↑ページの先頭へ戻る

科目目標

・履修目標
①秘匿通信方式SSL/TLSのアルゴリズムの詳細を理解し、最新攻撃手法への対処法を説明できる
②暗号化メール方式の概要を理解し、説明できる
③匿名通信網Torの仕組みを理解し、これに依拠する闇市場などの社会的影響を説明できる
④二次ふるい法の原理とアルゴリズムを理解し、暗号の安全性との関係について説明できる
⑤量子コンピューティングの基本原理を理解し、説明できる
⑥量子鍵配送BB84の具体的な仕組みについて理解し、説明できる
⑦電子政府構想など、代表的なセキュリティ社会制度基盤の概要を理解し、これらが社会に与える影響を説明できる
⑧セキュリティ社会制度基盤を支えるICカード技術やブロックチェーン技術の概要を理解し、説明できる
⑨DDoS攻撃や標的型攻撃などの代表的なサイバー攻撃を理解し、それへの対処法を説明できる
⑩サイバー戦を中心とする近代戦争の動向を理解し、説明できる

・到達目標
①秘匿通信方式SSL/TLSの仕組みの概要を理解し、最新攻撃手法への対処法を説明できる
②暗号化メール方式の概要を理解し、説明できる
③匿名通信網Torの仕組みを理解し、これに依拠する闇市場などの社会的影響を説明できる
④素因数分解アルゴリズムの概要を理解し、暗号の安全性との関係について説明できる
⑤量子コンピューティングの概要を理解し、説明できる
⑥量子暗号の概要について理解し、説明できる
⑦電子政府構想など、代表的なセキュリティ社会制度基盤の概要を理解し、これらが社会に与える影響を説明できる
⑧セキュリティ社会制度基盤を支えるICカード技術やブロックチェーン技術の概要を理解し、説明できる
⑨DDoS攻撃や標的型攻撃などの代表的なサイバー攻撃を理解し、それへの対処法を説明できる
⑩サイバー戦を中心とする近代戦争の動向を理解し、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が、最低限身につける内容を表す到達目標のみ設定している科目もあります。
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

↑ページの先頭へ戻る

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

暗号理論・技術など、セキュリティ基本構成要素についての知見を持つことが望ましいが、予備知識を持たない受講者に配慮し、講義の中でこれらを簡単に復習する。また、講義では素因数分解問題やRSA暗号等に関連する数学を若干解説するが、ビジネスコース履修者に配慮し、小テスト・期末テスト・ディベートの内容に、高度な数学的能力を要する設問等は設けない。

※この科目は、実務経験のある教員による授業科目です。教員の経歴や補足説明は以下の通りです:
精密機器メーカーで研究開発・情報セキュリティ監査・品質保証業務などに従事。情報セキュリティと安全評価の領域を専門とする実務経験を活かし、実践的応用を視野に入れた講義としている。

↑ページの先頭へ戻る

関連するバッジ

セキュリティ

↑ページの先頭へ戻る

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

題名	著者	出版社	発行年	備考
サイバー攻撃 ネット世界の裏側で起きていること（ブルーバックス）	中島 明日香	講談社	2018.1	1000円（税別）附属図書館で提供している「Maruzen eBook Library」でも見ることができます。https://elib.maruzen.co.jp/elib/html/BookDetail/Id/3000057468
闇ウェブ	セキュリティ集団スプラウト	文藝春秋	2016.7	780円（税別）
量子コンピュータ―超並列計算のからくり（ブルーバックス）	竹内 繁樹	講談社	2005.2	940円（税別）附属図書館で提供している「Maruzen eBook Library」でも見ることができます。https://elib.maruzen.co.jp/elib/html/BookDetail/Id/3000028555

その他の資料

なし

↑ページの先頭へ戻る

期末試験実施方法について

Webテスト形式

↑ページの先頭へ戻る

授業時間外の学修と評価について

・シラバスや科目内で案内している学内で利用可能な電子書籍やその他の参考書、科目のお知らせで紹介する補足事項などを参照し、2時間程度の予習を行いましょう。
・各回の小テストを受験する前に、授業動画を繰り返し視聴したり、学習資料や学内で利用できる電子書籍やその他の参考書などを自習したり、あるいは科目のお知らせで紹介する補足事項などを参照して、2時間程度の復習を欠かさないようにしましょう。

【オフィスアワーについて】
Zoomで対応します。申込制のため、事前に「学生サポート」ページのオフィスアワー申込フォームから申し込んでください。
月曜　17:00～18:00
申込の際、相談内容について記載してください。

↑ページの先頭へ戻る

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 %	0 %	50 %	40 %	0 %	100 %

↑ページの先頭へ戻る

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: 本科目の概要と学習目標 2)学習目標: ・最新の情報セキュリティ技術を学ぶ意義について学習する ・暗号・電子署名・ハッシュ等、この科目を学ぶ上で基本となる、情報セキュリティ要素技術の概念について学習する ・本科目の体系と授業構成を学習する 3)目次: 第1章 オリエンテーション 第2章 暗号の概念 第3章 暗号関連技術の概念 第4章 本科目の学習体系と授業構成	・小テスト	

第2回	1)タイトル: ネットワーク・セキュリティ～SSL/TLS 2)学習目標: ・SSL/TLSの概要を学習する ・SSL/TLSのプロトコルを学習する ・SSL/TLSの安全性について学習する ・NSAのSSL/TLSに対する解読の試みとTLS1.3の概要について学習する 3)目次: 第1章 SSL/TLSの概要 第2章 SSL/TLSの仕組みとプロトコル 第3章 SSL/TLSの問題点 第4章 TLS1.3	・小テスト	
第3回	1)タイトル: ネットワーク・セキュリティ～IPsec, PGP, S/MIME 2)学習目標: ・IPsecの概要を学習する ・IPsecのプロトコルを学習する ・IPsecの安全性について学習する ・PGPとS/MIMEの概要を学習する 3)目次: 第1章 IPsecの概要 第2章 IPsecのプロトコル 第3章 IPsecの安全性 第4章 PGPとS/MIME	・小テスト	
第4回	1)タイトル: ネットワーク・セキュリティ～匿名通信Tor 2)学習目標: ・匿名通信技術の概要を学習する ・匿名通信技術Torの概要を学習する ・Torにおけるクライアントとサーバー双方の秘匿通信について学習する ・Torの安全性について学習する 3)目次: 第1章 匿名通信技術の概要 第2章 Torの秘匿通信手順 第3章 Tor秘匿サービス 第4章 Torの安全性	・小テスト	
第5回	1)タイトル: サイバー攻撃とサイバー戦争 I ～アノニマスとDDoS攻撃 2)学習目標: ・DDoS攻撃の概要を学習する ・アノニマスの概要を学習する ・DDoS攻撃の事例について学習する ・DDoS攻撃への対策について学習する 3)目次: 第1章 DDoS攻撃の概要 第2章 アノニマスの概要 第3章 DDoS攻撃の事例	・ディベート	

	第4章 DDoS攻撃の対策		
第6回	1)タイトル: 計算の原理とセキュリティ～素因数分解と暗号の安全性 2)学習目標: ・素因数分解問題の歴史を学習する ・RSA暗号の安全性と素因数分解問題との関係について学習する ・アルゴリズムとその計算量について学習する ・素因数分解の計算量について学習する 3)目次: 第1章 素因数分解問題の歴史とその重要性 第2章 RSA暗号と素因数分解問題 第3章 アルゴリズムの計算量 第4章 素因数分解の計算量	・小テスト	
第7回	1)タイトル: 計算の原理とセキュリティ～量子コンピュータ 2)学習目標: ・量子コンピュータの歴史とその計算原理について学習する ・量子チューリング・マシンの概要と動作原理について学習する ・量子アニーリング・マシンの概要と初の商用量子計算機D-Waveについて学習する ・量子鍵配送について学習する 3)目次: 第1章 量子コンピュータの概要と歴史 第2章 量子チューリング・マシン 第3章 量子アニーリングとD-Wave 第4章 量子鍵配送	・小テスト	
第8回	1)タイトル: 計算の原理とセキュリティ～量子計算と暗号の安全性 2)学習目標: ・量子ゲートの概要について学習する ・ショアのアルゴリズムの計算原理について学習する ・量子ゲートを用いたショアのアルゴリズムの構成法を学習する ・量子コンピュータの実現性と暗号の安全性に与える影響について学習する。 3)目次: 第1章 量子ゲートの基本 第2章 ショアのアルゴリズムの数学的原理 第3章 量子ゲートによる構成 第4章 量子ゲート型コンピュータの実現可能性	・小テスト	
第9回	1)タイトル: サイバー攻撃とサイバー戦争Ⅱ～標的型攻撃とサイバー犯罪 2)学習目標: ・標的型攻撃の概要を学習する ・標的型攻撃の事例を学習する	・小テスト	

	・急速に進化しつつある標的型攻撃の現状について学習する ・標的型攻撃に対する防御策について学習する 3)目次: 第1章 標的型攻撃の概要 第2章 標的型攻撃の事例 第3章 進化する標的型攻撃 第4章 標的型攻撃に対する防御策		
第10回	1)タイトル: 社会基盤とセキュリティ～セキュリティ社会制度 2)学習目標: ・セキュリティ社会基盤制度の概要について学習する ・セキュリティに関連する標準化団体について学習する ・暗号モジュール評価制度について学習する ・公的認証基盤と電子政府について学習する 3)目次: 第1章 セキュリティ社会基盤の概要 第2章 セキュリティ関連標準化団体 第3章 IPAと暗号モジュール評価制度 第4章 認証基盤と電子政府	・小テスト	
第11回	1)タイトル: 社会基盤とセキュリティ～CC認証とエントロピープール 2)学習目標: ・CC認証試験制度の概要について学習する ・CC認証試験制度の評価手順詳細について学習する ・乱数シードとエントロピーの関係について学習する ・ミニマムエントロピー法について学習する 3)目次: 第1章 CC認証制度の概要 第2章 CC認証制度の詳細 第3章 シードとエントロピー 第4章 ミニマムエントロピー法	・小テスト	
第12回	1)タイトル: 社会基盤とセキュリティ～情報インフラとしてのブロックチェーン 2)学習目標: ・ブロックチェーンの概要について学習する ・ブロックの更新手順について学習する ・ブロックチェーンのトランザクションについて学習する ・ブロックチェーンの安全性について学習する 3)目次: 第1章 ブロックチェーンの概要 第2章 ブロックの更新手順 第3章 トランザクションの仕組み 第4章 ブロックチェーンの安全性	・小テスト	
第13回	1)タイトル: 社会基盤とセキュリティ～ICカードの普及と安全性 2)学習目標:	・小テスト	

	・ICカードの構造と安全性（解析手法）に関して概要を学習する ・ICカード等におけるRSA暗号の実装方法について学習する ・破壊型解析とその対策について学習する ・サイドチャネル攻撃とその対策法について学習する 3)目次： 第1章 ICカードの構造と安全性 第2章 RSA暗号とべき乗剰余計算 第3章 破壊型解析と対策 第4章 サイドチャネル攻撃		
第14回	1)タイトル： サイバー攻撃とサイバー戦争Ⅲ～サイバー軍と諜報機関による攻撃 2)学習目標： ・サイバー戦争の概要について学習する ・スタックスネットについて学習する ・”ラザルス”が行う、国家支援の下でのサイバー犯罪について学習する ・デジタル・インフラへの攻撃と防御策について学習する 3)目次： 第1章 サイバー攻撃の概要 第2章 スタックスネット 第3章 国家が支援するサイバー犯罪 第4章 国家が支援するサイバー犯罪	・小テスト	
第15回	1)タイトル： セキュリティ人材育成と総括 2)学習目標： ・セキュリティ人材育成の概要について学習する ・ネットワーク・セキュリティについて復習する ・計算の原理とセキュリティ、およびサイバー攻撃とサイバー戦争について復習する ・社会基盤とセキュリティの関係について復習する 3)目次： 第1章 セキュリティ人材育成 第2章 ネットワーク・セキュリティの復習 第3章 計算原理とセキュリティ、サイバー攻撃と戦争の復習 第4章 社会基盤とセキュリティの復習	・小テスト	

↑ページの先頭へ戻る

ウィンドウを閉じる