シラバス － 暗号技術と情報セキュリティ －

基本情報

学部	IT総合学部
科目	暗号技術と情報セキュリティ
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、古代から近代までの暗号技術の変遷から、暗号ビジネスへの諜報機関による関与、政府による規制など、情報セキュリティの社会的背景や歴史を辿りながら、暗号技術の発展と実装、関連法を展望する。技術面では情報セキュリティ技術の基本構成要素である共通鍵暗号・公開鍵暗号・ハッシュ・乱数などの概念や基本的な仕組みを中心に学習する。特に公開鍵暗号の技術標準であるRSA暗号については実際の計算例を交えて詳しく取り扱うとともに、暗号等に関連するプログラムを実装する上での留意事項についても理解する。

【科目コード】CS305

↑ページの先頭へ戻る

科目目標

・履修目標
①サイバーセキュリティに関する歴史を理解し、これを踏まえた今後の技術動向を説明できる
②共通鍵暗号AESの具体的な仕組みを理解し、その知識をプログラミングに活かすことができる
③公開鍵暗号のデファクトであるRSA暗号の暗・復号手順、鍵生成手順を正確に理解し、具体的な計算を実施できる
④電子署名の仕組みの概要を理解し、その知識をプログラミングに活かすことができる
⑤ハッシュ関数の仕組みの概要を理解し、その知識をプログラミングに活かすことができる
⑥擬似乱数生成法の具体的手順を理解し、その知識をプログラミングに活かすことができる
⑦暗号・ハッシュ・乱数など、情報セキュリティ技術の構成要素に対する基本的な攻撃法と安全性を正確に理解し、現行の攻撃法の発展手法を理解できる
⑧外為法や電子署名法における暗号技術に関連する条文の内容を正確に理解し、これらの法律に対して正しく対処できる

・到達目標
①サイバーセキュリティに関する歴史を理解し、これを踏まえた今後の技術動向を説明できる
②共通鍵暗号の概念を理解し、説明できる
③公開鍵暗号のデファクトであるRSA暗号の概要を理解し、説明できる
④電子署名の仕組みの概要を理解し、その知識をプログラミングに活かすことができる
⑤ハッシュ関数の仕組みの概要を理解し、その知識をプログラミングに活かすことができる
⑥擬似乱数の概念を理解し、説明できる
⑦暗号・ハッシュ・乱数など、情報セキュリティ技術の構成要素に対する基本的な攻撃法と安全性を正確に理解し、現行の攻撃法の発展手法を理解できる
⑧外為法や電子署名法における暗号技術に関連する条文の内容を正確に理解し、これらの法律に対して正しく対処できる

※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（旧：情報セキュリティマネジメント入門）
の単位を修得済みであること。
また、
・Pythonプログラミング入門（旧：ソフトウェア開発論Ⅰ）
・情報処理のための基礎知識
の単位を修得していることが望ましい。

講義では暗号等に関連するプログラミングの注意点も解説するが、ビジネスコース履修者のプログラミング・スキルを配慮し、小テスト・期末テスト・レポート・ディベートの内容にプログラミング・スキルを要する設問等は設けない。
暗号技術を理解するためには、ある程度数学を扱う必要がある。専門基礎科目「情報処理のための基礎知識」の単位を修得済か、同等の知識を有することが望ましい。

※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
現代暗号入門　いかにして秘密は守られるのか	神永 正博	講談社	2017.10	980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/3000057459
暗号解読［上］	サイモン・シン	新潮文庫	2007.6	670円（税別）
暗号解読［下］	サイモン・シン	新潮文庫	2007.6	710円（税別）

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: 情報セキュリティ技術の概要 2)学習目標: ・暗号技術と現代の情報化社会との関係について学習する ・暗号の概念を学習する ・ハッシュ・電子署名等の暗号関連技術の概念について学習する ・暗号技術の歴史・社会的背景や、暗号技術に関する規制・法律を学ぶことの意義を学習する 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: サイバーセキュリティの歴史Ⅰ～古典暗号の時代から米NSA誕生まで 2)学習目標:	・ディベート	

	・古典から近代までの暗号技術の変遷とその解読の歴史を学習する ・英政府 暗号学校、米NSAなど、暗号技術・情報セキュリティ技術を担う政府機関の誕生とその発展の歴史を学習する ・エニグマ暗号の構造・アルゴリズムとその解読手法の概略を学習する 3)目次: 第1章 古典暗号 第2章 暗号学校の誕生 第3章 エニグマの解読 第4章 米NSAの誕生		
第3回	1)タイトル: 共通鍵暗号の標準技術 2)学習目標: ・共通鍵暗号の概念を復習し、共通鍵暗号の分類、および共通鍵暗号のアルゴリズムなどを理解するのに必要な数学(排他的論理和)について学習する ・共通鍵暗号の技術標準の変遷を学習する ・共通鍵暗号の以前の技術標準であるDESの概要を学習する ・DESに対する代表的な攻撃法の概略を学習する 3)目次: 第1章 概念(復習)と準備 第2章 共通鍵暗号の分類とワンタイムパッド暗号 第3章 標準技術の変遷 第4章 DESアルゴリズムと安全性	・小テスト	
第4回	1)タイトル: 共通鍵暗号AES 2)学習目標: ・共通鍵暗号AESのアルゴリズムを学習する ・AESの安全性について学習する ・AES等のブロック暗号で使用される暗号利用モードについて学習する ・AES等のブロック暗号に関連する実装上の注意点を学習する 3)目次: 第1章 AESのアルゴリズム 第2章 AESの安全性 第3章 暗号利用モード 第4章 実装上の注意点	・小テスト	
第5回	1)タイトル: 公開鍵暗号のデファクトRSA 2)学習目標: ・公開鍵暗号の概念を復習し、公開鍵暗号の発展の歴史を学習する ・RSA暗号を理解するのに必要な整数論の基礎を学習する 3)目次: 第1章 概念の復習と公開鍵暗号の歴史 第2章 整数論の基礎 第3章 法(モジュロ)とべき乗剰余計算	・小テスト	

	第4章 フェルマーの小定理とその系		
第6回	1)タイトル: RSA暗号のアルゴリズム 2)学習目標: ・公開鍵暗号を理解するのに必要な整数論を復習する ・RSA暗号のアルゴリズムを学習する ・データ・サイズと計算量について学習する ・RSA暗号の安全な鍵長のサイズについて学習する 3)目次: 第1章 整数論基礎の復習とRSA暗号の数学的基礎 第2章 RSA暗号の暗・復号化手順 第3章 データ・サイズと計算量 第4章 RSA暗号の安全な鍵長	・小テスト	
第7回	1)タイトル: RSAの安全性と実装に関する留意点 2)学習目標: ・RSA暗号の暗・復号化手順の計算例を復習する ・RSA暗号の安全性について学習する ・離散対数問題について学習する ・ElGamal暗号と楕円曲線暗号について学習する 3)目次: 第1章 RSA暗号における暗・復号化手順の計算例 第2章 RSA暗号の安全性と実装上の留意点 第3章 離散対数問題と群 第4章 ElGamal暗号と楕円曲線暗号	・小テスト	
第8回	1)タイトル: サイバーセキュリティの歴史Ⅱ～諜報機関とサイファーパンクの闘い 2)学習目標: ・DESの標準化におけるNSAの関与の経緯について学習する ・公開鍵暗号の真の開発の歴史を学習する ・鍵預託機能付き暗号化チップのクリッパーチップについて学習する ・暗号輸出規制を中心に、暗号技術を巡る利害の対立について学習する 3)目次: 第1章 DESの標準化におけるNSAの関与 第2章 公開鍵暗号発明の真の歴史 第3章 クリッパーチップ問題 第4章 暗号技術を巡る利害の対立	・小テスト	
第9回	1)タイトル: 安全性の定義 2)学習目標: ・統計的な相関が安全性にどのように関わっているかを学習する ・情報理論と安全性の関わりを学習する ・最良の解読アルゴリズムの計算量と安全性の関わりについて学習する ・理論的な安全性指標である識別不可能性に基づく安	・小テスト	

	全性について学習する 3)目次: 第1章 統計的な相関と安全性 第2章 情報理論的安全性 第3章 計算量的安全性 第4章 識別不可能性による安全性		
第10回	1)タイトル: 電子署名 2)学習目標: ・電子署名の概念を復習し、電子署名にどのような意義があるかを学習する ・RSA署名のアルゴリズムを学習する ・RSA署名の問題点について学習する ・RSA署名の技術標準を学習する 3)目次: 第1章 電子署名の概念 第2章 RSA署名のアルゴリズム 第3章 RSA署名に対する攻撃法 第4章 RSA署名の規格	・小テスト	
第11回	1)タイトル: PKIと認証技術 2)学習目標: ・PKI(公開鍵暗号基盤)の概念を学習する ・認証局の役割について学習する ・PKIを用いた暗号化通信を学習する ・電子署名法に基づくPKIの運用について学習する 3)目次: 第1章 PKIの概念 第2章 認証局の役割の詳細 第3章 PKIを利用した暗号化通信 第4章 PKIの運用と問題点	・小テスト	
第12回	1)タイトル: ハッシュ関数 2)学習目標: ・一般的なハッシュ関数の概念について復習する ・暗号学的ハッシュ関数の概念について学習する ・暗号学的ハッシュ関数の攻撃法と安全性について学習する ・暗号学的ハッシュ関数の標準技術を学習する 3)目次: 第1章 ハッシュの概念の復習 第2章 暗号学的ハッシュの概念 第3章 暗号学的ハッシュの安全性 第4章 暗号学的ハッシュの標準技術	・小テスト	
第13回	1)タイトル: 擬似乱数 2)学習目標: ・乱数の概念について復習する	・小テスト	

	・計算量的安全擬似乱数の概念について学習する ・計算量的安全擬似乱数の標準技術を学習する ・擬似乱数に関連した攻撃法とシステムの安全性について学習する 3)目次: 第1章 乱数の概念の復習 第2章 計算量的安全擬似乱数の概念 第3章 計算量的安全擬似乱数の標準技術 第4章 擬似乱数に関連した攻撃事例		
第14回	1)タイトル: サイバーセキュリティの歴史Ⅲ～大量監視時代 2)学習目標: ・米NSAによる大量監視の実態について学習する ・告発者たちによる諜報機関の違法行為告発の実態について学習する ・米NSAに対するIT企業の協力活動について学習する ・諜報機関によって仕掛けられたバック・ドアの影響について学習する 3)目次: 第1章 大量監視の始まり 第2章 告発者たちによる暴露 第3章 NSAとIT業界 第4章 危険なバックドア	・小テスト	
第15回	1)タイトル: 関連法とまとめ 2)学習目標: ・暗号技術に関連する法令について学習する ・暗号技術の分類と共通鍵暗号について復習する ・RSA暗号について復習する ・暗号関連技術について復習する 3)目次: 第1章 暗号関連法令 第2章 暗号技術の分類と共通鍵暗号の総括 第3章 RSA暗号の総括 第4章 暗号関連技術の総括	・小テスト	

↑ページの先頭へ戻る

ウィンドウを閉じる