シラバス参照

タイトル「**2021年度危機管理学部(公開用_コロナ対策版)**」、フォルダ「**危機管理学部**」
シラバスの詳細は以下となります。

戻る

科目ナンバー	RMGT3573		
科目名	サイバーセキュリティ論		
担当教員	藤井　秀之		
対象学年	3年,4年	開講学期	前期
曜日・時限	木４		
講義室	オンライン	単位区分	選必
授業形態	講義	単位数	2
科目大分類	専門科目		
科目中分類	専門展開		
科目小分類	専門・危機管理		
科目の位置付け（開発能力）	■ＤＰコード-学修のゴールを示すディプロマポリシーとの関連 DP1-E [学識・専門技能]専門分野にかかる理論知と実践知を獲得し利用することができる DP4-F[探求力・課題解決力]問を設定し又は論点を特定し、それに対する答・結論・判断を合理的に導くために、論拠の収集と分析を体系的に行うとともに、オープンエンドな問題・課題に答えるための方略をデザインし、検証し実行することができる。 ■ＣＲコード-学修を通じて開発するマインドセット・ナレッジ・スキルを示すコモンルーブリック（ＣＲ）との関連 C1倫理的思考・社会認識ー10% E1学識と専門技能ー30% F1探求と論拠ー10% G1状況把握ー10% H1論理的思考ー20% I3情報分析ー20%		
教員の実務経験	セキュリティコンサルタントとしてセキュリティ領域に関わる多種多様なコンサルティング・調査業務経験を踏まえ、デジタル化・ネットワーク化・グローバル化等の観点から、サイバーセキュリテイの現実的課題を具体的に提示し、体系的な理解と問題意識を醸成します。 (授業回：第1回～第15回)		
成績ターゲット区分	3発展期～4定着期		
科目概要・キーワード	現代社会は、インターネットやイントラネットのような様々な通信技術をもちいて構成されたネットワークに依存しています。こうしたネットワークによって構成されるサイバー空間において様々な社会活動が執り行われていますが、このネットワークやサイバー空間が攻撃を受けることで、現代社会において政治的、経済的、文化的な面で被害が発生するようになりました。ネットワークやサイバー空間をこうした外部の攻撃から守るためのサイバーセキュリティのあり方について、理論的かつ具体的に考察しながら、サイバーセキュリティに関する総合的な理解を深めることを目的とします。マルウェアやハッキングなどに対する技術的対策や、そのために必要とされる法制度や社会政策について考察します。 なお、授業の一部を補完するため、あるいは代替するためにディスタンスラーニング（講義動画のオンデマンド配信等）を取り入れる予定です。 （キーワード）サイバー攻撃 、サイバー犯罪、サイバーセキュリティ政策		
授業の趣旨	■副題 サイバーセキュリティを守るための技術・運用・制度 ■授業の目的 サイバーセキュリティに関する脅威、技術、運用、制度の動向を学び、サイバーセキュリティに関する諸問題を、論理的に分析・対処する考え方を身につける。 ■授業のポイント		

	現代社会ではサイバー空間において様々な社会活動が執り行われています。このサイバー空間が攻撃を受けることで、現実社会の政治的、経済的、文化的な面で被害が発生するようになっています。こうした攻撃に代表されるサイバーセキュリティに関する脅威や、関連する技術・制度の動向を学ぶ。コンピュータ・ネットワークの利用が飛躍的に増大したことで、サイバーセキュリティの重要性も高まっています。特に、クラウドやスマートホン、タブレット端末が急速に普及し、インターネットがビジネスや日常生活に欠かせないものになっているなかで、セキュリティ上の脅威もより深刻になっています。情報セキュリティ（Information Security）は、「情報の機密性，完全性及び可用性を維持すること」と定義されることが多いです。現実の世界で重要なものの安全を確保するには、例えば金庫に入れて外部から遮断し、出入りを厳重に管理し、不純物が入り込まないようにする、といった対策がとられます。サイバーセキュリティは、デジタルネットワークおいて、こうした対策を実現するものです。しかし、デジタル情報については、金庫のような単純な手段では、利便性を損なわずに十分な安全を確保することができません。その特性をよく理解し、保護するための手段やそれを支える制度について正しい知識を持つことが不可欠です。この講義では、デジタル情報とサイバーセキュリティに関する問題について、脅威、技術、制度の動向を解説しながら検討します。その上で、サイバーセキュリティに関する諸問題を論理的に分析し、問題の所在と課題への対処のあり方について、自ら説明できるだけの能力を身につけることを目的とします。
総合到達目標	■サイバーセキュリティに関する脅威、技術、制度の状況を理解し、サイバーセキュリティ対策に必要な基本的知識を習得し、問題とそれへの対処のあり方について、自分なりの視点から論ずることができるようになる。
成績評価方法	■リアクションペーパー：13回（65%） （評価の観点）講義内容を理解しているか、学んだ内容を自分の言葉で説明できているかを評価します。 適用ルーブリック：C1（10%）、E1（30%）、F1（10%）、G1（10%）、H1（20%）、I3（20%） （フィードバックの方法）各回授業内に解説を行う。 ■レポート：1回（35%） （評価の観点）講義内容を踏まえ、与えられた設問に対して、的確かつ論理的に答えているかどうかを評価します。 適用ルーブリック：C1（10%）、E1（30%）、F1（10%）、G1（10%）、H1（20%）、I3（20%） （フィードバックの方法）授業（第15回）で解説を行う。 ※成績評価における各方法の比率は、授業形態によって変更となる場合があります。詳細は初回ガイダンスで説明します。
履修条件	特にありません
履修上の注意点	特にありません
授業内容	

回	内容
1	①授業テーマ ガイダンス（全体テーマおよび進め方の説明） ②授業概要 授業のテーマや内容、スケジュール、評価方法と、サイバーセキュリティ論の学習方法や研究方法について説明し、受講生が授業の準備を具体的に行えるようにする（適用ルーブリックーC1：10%、E1：30%、F1：10%、G1：10%、H1：20%、I3：20%）。 セキュリティコンサルタントとしてセキュリティ領域に関わる多種多様なコンサルティング・調査業務経験を踏まえ、デジタル化・ネットワーク化・グローバル化等の観点から、サイバーセキュリテイの現実的課題を具体的に提示し、体系的な理解と問題意識を醸成する。 ③予習（120分） シラバスの内容をよく読み、教科書を入手して「はじめに」を読む。 ④復習（120分） 講義ノートを確認して、自分の学習計画と他の履修科目との関係について検討する。
2	①授業テーマ 情報セキュリティとは（総論） ②授業概要 情報セキュリティのリスクと情報セキュリティが確保すべき要素とされているCIA（Confidentiality, Integrity, Availability）について学び、受講者がそれについて説明できるようにする（適用ルーブリックーC1：10%、E1：30%、F1：10%、G1：10%、H1：20%、I3：20%）。

	セキュリティコンサルタントとしてセキュリティ領域に関わる多種多様なコンサルティング・調査業務経験を踏まえ、デジタル化・ネットワーク化・グローバル化等の観点から、サイバーセキュリテイの現実的課題を具体的に提示し、体系的な理解と問題意識を醸成する。 ③予習（120分） 教科書『図解まるわかりセキュリティの仕組み』（翔泳社、2018年）の「第１章　セキュリティの基本的な考え方」を読み、情報セキュリティとは何かについて理解する。 ④復習（120分） 講義ノートを確認して、情報セキュリテイとは何かについて、自分なりの説明をまとめる。
3	①授業テーマ 情報セキュリティのインシデント ②授業概要 情報セキュリティに関する脅威や、最新技術とセキュリティのリスク（スマートフォン、SNS、クラウド、IoT等）について実際のインシデント事例を通して学び、受講者がそれについて説明できるようにする（適用ルーブリックーC1：10%、E1：30%、F1：10%、G1：10%、H1：20%、I3：20%）。 セキュリティコンサルタントとしてセキュリティ領域に関わる多種多様なコンサルティング・調査業務経験を踏まえ、デジタル化・ネットワーク化・グローバル化等の観点から、サイバーセキュリテイの現実的課題を具体的に提示し、体系的な理解と問題意識を醸成する。 ③予習（120分） 教科書『図解まるわかりセキュリティの仕組み』（翔泳社、2018年）の「第３章　ウイルスとスパイウェア」を読み、情報セキュリティのインシデントの種類等について考察する。 ④復習（120分） 講義ノートを確認して、情報セキュリティに関する脅威や、最新技術とセキュリティのリスクについて、自分なりの説明をまとめる。
4	①授業テーマ 情報セキュリティ対策の基本的考え方と情報セキュリティ技術 ②授業概要 サイバー攻撃の典型的な技術である不正アクセス、DDoS攻撃、コンピュータウィルス、マルウェア等の、攻撃手法の概要と防護について学び、受講者がそれについて説明できるようにする（適用ルーブリックーC1：10%、E1：30%、F1：10%、G1：10%、H1：20%、I3：20%）。 セキュリティコンサルタントとしてセキュリティ領域に関わる多種多様なコンサルティング・調査業務経験を踏まえ、デジタル化・ネットワーク化・グローバル化等の観点から、サイバーセキュリテイの現実的課題を具体的に提示し、体系的な理解と問題意識を醸成する。 ③予習（120分） 教科書『図解まるわかりセキュリティの仕組み』（翔泳社、2018年）の「第２章　ネットワークを狙った攻撃」及び「第４章　脆弱性への対応」を読み、一般的なネットワークセキュリティや脆弱性対策について理解する。 ④復習（120分） 講義ノートを確認して、インターネットで情報がやりとりされる基本的な仕組みや、パスワードの基本等について、自分なりの説明をまとめる。
5	①授業テーマ 暗号と認証 ②授業概要 情報システムを防護するうえで欠かせない技術である暗号と認証について学び、受講者がそれについて説明できるようにする（適用ルーブリックーC1：10%、E1：30%、F1：10%、G1：10%、H1：20%、I3：20%）。 セキュリティコンサルタントとしてセキュリティ領域に関わる多種多様なコンサルティング・調査業務経験を踏まえ、デジタル化・ネットワーク化・グローバル化等の観点から、サイバーセキュリテイの現実的課題を具体的に提示し、体系的な理解と問題意識を醸成する。 ③予習（120分） 教科書『図解まるわかりセキュリティの仕組み』（翔泳社、2018年）の「第５章　暗号/署名/証明書とは」を読み、暗号技術等について理解する。 ④復習（120分） 講義ノートを確認して、暗号技術や証明書等の概念やその内容について、自分なりの説明をまとめる。

6	①授業テーマ 情報セキュリティマネジメントとリスクアセスメント ②授業概要 サイバーセキュリテイ確保のためのリスクマネジメントの基本的な考え方について学び、受講者がそれについて説明できるようにする（適用ルーブリックーC1：10%、E1：30%、F1：10%、G1：10%、H1：20%、I3：20%）。 セキュリティコンサルタントとしてセキュリティ領域に関わる多種多様なコンサルティング・調査業務経験を踏まえ、デジタル化・ネットワーク化・グローバル化等の観点から、サイバーセキュリテイの現実的課題を具体的に提示し、体系的な理解と問題意識を醸成する。 ③予習（120分） 教科書『図解まるわかりセキュリティの仕組み』（翔泳社、2018年）の「第６章　組織的な対応」を読み、情報セキュリティ確保のための組織的な対応としてどのような対策があるかについて理解する。 ④復習（120分） 講義ノートを確認して、情報セキュリティに関するリスクマネジメントのあり方について、自分なりの説明をまとめる。
7	①授業テーマ サイバーセキュリティの最新動向・事例① ②授業概要 直近のサイバーセキュリティに関連するニュースや政策動向等を踏まえ、授業で学んだ内容を踏まえた解説、紹介を行う。場合によっては、当該分野に精通する専門家をゲストとして招く場合もある。（適用ルーブリックーC1：10%、E1：30%、F1：10%、G1：10%、H1：20%、I3：20%）。 セキュリティコンサルタントとしてセキュリティ領域に関わる多種多様なコンサルティング・調査業務経験を踏まえ、デジタル化・ネットワーク化・グローバル化等の観点から、サイバーセキュリテイの現実的課題を具体的に提示し、体系的な理解と問題意識を醸成する。 ③予習（120分） 事前に提示された参考資料等を読み、自分なりの理解や確認事項を明確にしておく。 ④復習（120分） 講義ノートを確認して、自分なりの説明をまとめる。
8	①授業テーマ 前半のまとめと質疑応答 ②授業概要 第７回までの授業で学んだ内容について質問や意見を受け付けそれに対する回答を行うとともに、前半の授業に関する補足とまとめを行う（適用ルーブリックーC1：10%、E1：30%、F1：10%、G1：10%、H1：20%、I3：20%）。 セキュリティコンサルタントとしてセキュリティ領域に関わる多種多様なコンサルティング・調査業務経験を踏まえ、デジタル化・ネットワーク化・グローバル化等の観点から、サイバーセキュリテイの現実的課題を具体的に提示し、体系的な理解と問題意識を醸成する。 ③予習（120分） これまでの講義を通して、自分の疑問に思った点、理解が難しかった点等をまとめておく。 ③復習（120分） 講義ノートを確認して、自分の疑問点が解決したかどうか、新たな疑問が生じていないかどうかを考察する。
9	①授業テーマ サイバーセキュリティ基本法と重要インフラ防護 ②授業概要 わが国におけるサイバーセキュリティに関する政策や国家戦略の概要と重要インフラの情報システムに関する防護の状況と課題について学び、受講者がそれについて説明できるようにする（適用ルーブリックーC1：10%、E1：30%、F1：10%、G1：10%、H1：20%、I3：20%）。 セキュリティコンサルタントとしてセキュリティ領域に関わる多種多様なコンサルティング・調査業務経験を踏まえ、デジタル化・ネットワーク化・グローバル化等の観点から、サイバーセキュリテイの現実的課題を具体的に提示し、体系的な理解と問題意識を醸成する。 ③予習（120分） 事前に提示された参考資料等を読み、自分なりの理解や確認事項を明確にしておく。 ④復習（120分） 講義ノートを確認して、サイバーセキュリティに関する政策や国家戦略の概要と重要イ

	ンフラの情報システムに関する防護の状況と課題について、自分なりの説明をまとめる。
10	①授業テーマ サイバー犯罪と法 ②授業概要 サイバーセキュリティ上の脅威となりうる攻撃等に関して、法律上どのような禁止規定が定められているのかについて学び、受講者がそれについて説明できるようにする（適用ルーブリックーC1：10%、E1：30%、F1：10%、G1：10%、H1：20%、I3：20%）。 セキュリティコンサルタントとしてセキュリティ領域に関わる多種多様なコンサルティング・調査業務経験を踏まえ、デジタル化・ネットワーク化・グローバル化等の観点から、サイバーセキュリテイの現実的課題を具体的に提示し、体系的な理解と問題意識を醸成する。 ③予習（120分） 事前に提示された参考資料等を読み、自分なりの理解や確認事項を明確にしておく。 ④復習（120分） 講義ノートを確認して、サイバーセキュリティに関する禁止規定について、自分なりの説明をまとめる。
11	①授業テーマ 個人情報保護と安全管理措置 ②授業概要 サイバーセキュリティ上の脅威にさらされる情報に関して、法律上どのような保護がなされているのかについて学び、受講者がそれについて説明できるようにする（適用ルーブリックーC1：10%、E1：30%、F1：10%、G1：10%、H1：20%、I3：20%）。 セキュリティコンサルタントとしてセキュリティ領域に関わる多種多様なコンサルティング・調査業務経験を踏まえ、デジタル化・ネットワーク化・グローバル化等の観点から、サイバーセキュリテイの現実的課題を具体的に提示し、体系的な理解と問題意識を醸成する。 ③予習（120分） 事前に提示された参考資料等を読み、自分なりの理解や確認事項を明確にしておく。 ④復習（120分） 講義ノートを確認して、個人情報保護と安全管理措置の関係性について、自分なりの説明をまとめる。
12	①授業テーマ プラットフォーム事業者と法 ②授業概要 今日のネット社会においてプラットフォーム事業者が深く関与している構造について理解した上で、フェイクニュースやSNS上での誹謗中傷、忘れられる権利などの概要と、その法的位置づけについて理解する。（適用ルーブリックーC1：10%、E1：30%、F1：10%、G1：10%、H1：20%、I3：20%）。 セキュリティコンサルタントとしてセキュリティ領域に関わる多種多様なコンサルティング・調査業務経験を踏まえ、デジタル化・ネットワーク化・グローバル化等の観点から、サイバーセキュリテイの現実的課題を具体的に提示し、体系的な理解と問題意識を醸成する。 ③予習（120分） 事前に提示された参考資料等を読み、自分なりの理解や確認事項を明確にしておく。 ④復習（120分） 講義ノートを確認して、情報管理者の法的責任について、自分なりの説明をまとめる。
13	①授業テーマ サイバーセキュリティの国際政治 ②授業概要 諸外国のサイバーセキュリティ政策の動向や国際政治におけるサイバーセキュリティに関する議論の動向について学び、受講者がそれについて説明できるようにする（適用ルーブリックーC1：10%、E1：30%、F1：10%、G1：10%、H1：20%、I3：20%）。 セキュリティコンサルタントとしてセキュリティ領域に関わる多種多様なコンサルティング・調査業務経験を踏まえ、デジタル化・ネットワーク化・グローバル化等の観点から、サイバーセキュリテイの現実的課題を具体的に提示し、体系的な理解と問題意識を醸成する。 ③予習（120分） 事前に提示された参考資料等を読み、自分なりの理解や確認事項を明確にしておく。米国や中国等のサイバーセキュリティに関する政策や法制度等について調べてみて、各国の取組みの違いやその背景について考察する。 ④復習（120分）

		講義ノートを確認して、諸外国のサイバーセキュリティに関する政策の違いやその背景等について、自分なりの説明をまとめる。
	14	①授業テーマ サイバーセキュリティの最新動向・事例② ②授業概要 直近のサイバーセキュリティに関連するニュースや政策動向等を踏まえ、授業で学んだ内容を踏まえた解説、紹介を行う。場合によっては、当該分野に精通する専門家をゲストとして招く場合もある。（適用ルーブリックーC1：10%、E1：30%、F1：10%、G1：10%、H1：20%、I3：20%）。 セキュリティコンサルタントとしてセキュリティ領域に関わる多種多様なコンサルティング・調査業務経験を踏まえ、デジタル化・ネットワーク化・グローバル化等の観点から、サイバーセキュリテイの現実的課題を具体的に提示し、体系的な理解と問題意識を醸成する。 ③予習（120分） 事前に提示された参考資料等を読み、自分なりの理解や確認事項を明確にしておく。 ④復習（120分） 講義ノートを確認して、自分なりの説明をまとめる。
	15	①授業テーマ まとめ ②授業概要 計14回の授業の内容を総括しサイバーセキュリティ論に関するまとめを行う（適用ルーブリックーC1：10%、E1：30%、F1：10%、G1：10%、H1：20%、I3：20%）。また、レポート課題について解説する。 セキュリティコンサルタントとしてセキュリティ領域に関わる多種多様なコンサルティング・調査業務経験を踏まえ、デジタル化・ネットワーク化・グローバル化等の観点から、サイバーセキュリテイの現実的課題を具体的に提示し、体系的な理解と問題意識を醸成する。 ③予習（120分） 講義ノート全体と教科書の該当部分（講義で取り上げた部分）を読みなおし、各回のテーマについて自分の考えをもとに論じられるように準備する。 ④復習（120分） 授業の内容を振り返り、自分の考えを再検証するとともに、今後の学習方針を考える。
関連科目		情報管理論（RMGT 3571）、情報法（RGMT 3471）、プライバシーと法（RGMT 3472）、デジタル・フォレンジック（RGMT 3577）
教科書		増井敏克『図解まるわかりセキュリティの仕組み』（翔泳社、2018年）
参考書・参考ＵＲＬ		増島雅和、蔦大輔「事例に学ぶサイバーセキュリティ」（経団連出版、2020年）、小向太郎『情報法入門（第5版）デジタル・ネットワークの法律』（NTT出版、2020年）
連絡先・オフィスアワー		授業内で共有する。
研究比率		ｻｲｶﾞｲﾏﾈｼﾞﾒﾝﾄ10%：ﾊﾟﾌﾞﾘｯｸｾｷｭﾘﾃｨ10%：ｸﾞﾛｰﾊﾞﾙｾｷｭﾘﾃｨ10%：情報ｾｷｭﾘﾃｨ70% 危機管理学50%：法学50%

戻る