シラバス参照

タイトル「**2022年度危機管理学部(公開)**」、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 | RMGT2602 | | |
| 科目名 | 危機管理基礎演習Ⅱ | | |
| 担当教員 | 美濃輪　正行 | | |
| 対象学年 | 2年,3年,4年 | 開講学期 | 後期 |
| 曜日・時限 | 火２ | | |
| 講義室 | 1316 | 単位区分 | 必 |
| 授業形態 | 演習 | 単位数 | 1 |
| 科目大分類 | 専門 | | |
| 科目中分類 | 演習・ゼミナール等 | | |
| 科目小分類 | - | | |
| 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<br>　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。<br>　ＤＰ３－Ｈ［論理的思考力］　理路整然とした思考を備えつつ、偏りを排除するための内省をもって、問題・課題を合理的に解決することができる。<br>　ＤＰ４－Ｉ［理解力・分析力］文章表現、数値データを適切に扱いつつ、情報の収集と取捨選択、分析と加工を有効かつ円滑に行い、課題の解決につなげることができる。<br>　ＤＰ４－Ｌ［協働力・牽引力］集団的に課題解決を行う際に、自己の立場や責任を認識し、互いに集団の連帯を強めることができる。<br>　ＤＰ６－Ｋ［表現力・対話力］文章及び口頭で、自らの考えを的確に表現し、他者に過不足なく伝達することができる。<br>■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<br>　ＣＰ４－　Ｉ１　理解・分析と読解（３０%）<br>　ＣＰ３－　Ｈ１　論理的思考（１５%）<br>　ＣＰ４－　Ｌ１　チームワーク（２０%）<br>　ＣＰ１－Ｅ１　学識と専門技能（２０%）<br>　ＣＰ４－Ｉ３　情報分析（１０%）<br>　ＣＰ６－Ｋ２　オーラルコミュニケーション（５%） | | |
| 教員の実務経験 | 担当教員は、当大学着任前に情報サービスを提供する民間企業で勤務しておりました。本講義で取り扱う内容は、情報セキュリティの知見を深めるために必要とされるものです。情報セキュリティは応用分野であり，技術的な知識の記憶ではなく、包括的な視点からの考察が求められます。担当教員は情報サービスを直接提供する立場で様々な経験を積んでおり、これらの知見を講義に活かす所存です。（第7/11/13/14回） | | |
| 成績ターゲット区分 | ■ 成績ターゲット　能力開発の目標ステージとの対応<br>２進行期～３発展期 | | |
| 科目概要・キーワード | 危機管理に関するサイバー犯罪の事例を取り上げて、危機管理に関する基礎的な演習を行います。情報セキュリティ領域の教員が担当し、この研究領域における研究の手法について指導します。ここの学びが、３年次以降のゼミナールや危機管理特殊研究でのより深化した研究活動へと発展します。本科目では、専門的研究のテーマに基づいて、自ら問題を策定・分析して、その結果のプレゼンテーションを実施します。授業形態は演習形式により行います。なお、対応するコンピテンスに基づき効果的な授業方法として、又は各授業を補完・代替するためオンライン授業を一部取り入れる場合があります。<br>（キーワード）危機管理　集団的検討　危機管特殊研究への橋渡し | | |

| | |
|---|---|
| 授業の趣旨 | ■副題<br>サイバー犯罪のケーススタディ<br>■授業の目的<br>情報技術の世界は日々進歩しており、それを活用したサイバー犯罪の形態も進化しつつあります。本講義では、これらを技術的、社会的の両面で理解を深め、事案に対する個人の理解や認識を形成し、更には将来、包括的な理解に発展させるものです。サイバー犯罪に対して自然科学分野の学術的視点では技術的な理解に終始する考え方も存在しますが、危機管理の視点では、事案が発生するに至る複数の要素を考慮した上で、それらに対応することが求められます。技術的要素以外にもシステムを管理する人間系、犯罪を誘発する社会的背景、等が該当しますが、本講座ではこれらも取り扱います。サイバー犯罪において実践的な技術や知識を習得するための基礎となる概念を形成することを目的とします。<br>■授業のポイント<br>危機管理に関する諸問題の内容とその経緯の理解、集団的な検討手法の会得、研究成果の発表の各過程を通じて、①協働力・牽引力、②学識・専門技能、③論理的思考力・批判的思考力、④理解力・分析力、⑤表現力・対話力の各コンピテンスの開発を行います。将来のキャリアを見据えた学びにおいて、⑥自己の特性を理解し社会に貢献しようとする姿勢、⑦倫理観と公共心、⑧省察力の各観点について自覚を持つことも望まれます。 |
| 総合到達目標 | ■ サイバー犯罪に関する問題を詳細に分析して結果と原因の因果関係を考察することにより、問題分析能力を習得するための基本的な素養を身に付ける。<br>■ 具体的な指標としては次の通り。<br>・受講生が与えられた教材を読解して、適切な問題意識を持つ。<br>・問題発生の背景，根本的な原因を訴求する論理思考力を高める。<br>・各自の成果を他者に理解できるよう適切に表現することができるようになる。<br>・事例を通して技術情報を咀嚼する知識を体得する。 |
| 成績評価方法 | ■ チームディスカッション資料作成 1回（２０%）：適用ルーブリック　Ｉ１・Ｈ１・Ｌ１・Ｅ１・Ｉ３<br>（評価の観点）<br>受講生は与えられたケーススタディ資料を各自が的確に読み取り内容を理解・分析し、チーム内での意見を交わし、結果を発表資料にまとめます。時間相応の分析結果と知見が含まれているか、チームの運営が効率的になされたか、技術的な知識が活用されたものか、について評価します。<br>（フィードバックの方法）<br>プレゼンテーション資料作成時の個人ごとの活動レポートを評価して、採点結果を公開します。<br>■ チームディスカッション発表　1回（１０%）：適用ルーブリック　Ｋ２・Ｌ１<br>（評価の観点）<br>受講生は前述のケーススタディの資料をチーム毎に発表します。発表の内容、チーム内での協力について評価します。<br>（フィードバックの方法）<br>チーム別のプレゼンテーションの内容を相互に評価して、採点結果を公開します。<br>■ 個人レポート作成 6回（６０%）：適用ルーブリック　Ｉ１・Ｈ１・Ｌ１・Ｅ１・Ｉ３<br>（評価の観点）<br>受講生は前述のプレゼンテーション資料を適宜見直し修正して提出します。成果物は、要求条件を適切に満たしているか、技術的な知識が活かされたものか、及び有用性について評価します。<br>（フィードバックの方法）<br>講義中に解答例を提示して、採点結果を公開します。<br>■ 授業参加度（１０%）：適用ルーブリック　Ｉ１・Ｈ１・Ｃ１<br>（評価の観点）<br>受講生は講義中の問いかけに対して解答を記述して講義後に提出します。提出頻度、解答内容について評価します。<br>（フィードバックの方法）<br>出欠情報としてポータルシステムに公開します。 |
| 履修条件 | 特になし。ただし、記事・資料を読みこなす読解力が前提となります。講義内容は、情報セキュリティ以外の領域にも渡ります。 |
| 履修上の注意点 | |
| 授業内容 | |

| 回 | 内容 |
|---|---|
| 1 | ①授業テーマ<br>ガイダンス<br>②授業概要 |

| | |
|---|---|
| | 講義の重要な点を理解するために、その目的、講義の構成、スケジュール、評価方法について説明します。情報セキュリティの要素について解説、受講生はいくつかの事案に対応づけて考察します。（I1）<br>③復習（240分）<br>情報セキュリティの要素について講義資料で復習し、具体的な事案を紐付けて考えること。 |
| 2 | ①授業テーマ<br>情報システムの基礎知識①<br>②授業概要<br>サイバー犯罪を理解するために必要となる情報システムを構成するコンピュータの基礎について説明します。これらの知識は以後の講義の前提となります。講義後は、情報システムの概要について、情報セキュリティの視点からいくつかの要因を示すことができるようになります。(E1)<br>③予習（120分）<br>コンピュータ・情報リテラシの教科書 第1章を精読しておくこと。<br>④復習（120分）<br>授業説明資料を復習すること。 |
| 3 | ①授業テーマ<br>情報システムの基礎知識②<br>②授業概要<br>サイバー犯罪を理解するために必要となるネットワークの基礎について説明します。これらの知識は以後の講義の前提となります。講義後は、情報システムの概要について、情報セキュリティの視点からいくつかの要因を示すことができるようになります。(E1)<br>③予習（120分）<br>コンピュータ・情報リテラシの教科書 第３章を精読しておくこと。<br>④復習（120分）<br>授業説明資料を復習すること。 |
| 4 | ①授業テーマ<br>情報システムの基礎知識③<br>②授業概要<br>サイバー犯罪を理解するために必要となる情報システムの運用管理の基礎について説明します。これらの知識は以後の講義の前提となります。講義後は、情報システムの概要について、情報セキュリティの視点からいくつかの要因を示すことができるようになります。(E1)<br>③予習（120分）<br>情報システムの運用管理にはどのような作業があるかインターネットで調べること。<br>④復習（120分）<br>授業説明資料を復習すること。 |
| 5 | ①授業テーマ<br>情報セキュリティの基礎知識<br>②授業概要<br>情報セキュリティの基礎とサイバー犯罪の概要について説明します。講義後は、情報セキュリティの基本特性とサイバー犯罪のいくつかの手口について説明できるようになります。(E1/H1/I3)<br>③予習（240分）<br>ケース資料を精読して、技術的な観点で意味が不明な点を講義までに挙げておくこと。 |
| 6 | ①授業テーマ<br>ケーススタディ（全体概要）<br>②授業概要<br>1件の具体的事案について、サイバー犯罪とはどのようなものか、犯行内容、被害内容、被害者、対応の経緯について解説します。尚、ケーススタディの初回であることに考慮して、資料の読み取り方や調査の留意点についても触れます。この回はチームディスカッションを含みます。講義後は、サイバー犯罪事案のいくつかの技術要素とその関連性について説明できるようになります。(E1/H1/I3)<br>③予習（240分）<br>ケース資料を精読して、技術的な観点で意味が不明な点を講義までに挙げておくこと。 |
| 7 | ①授業テーマ<br>ファシリテーション技法<br>②授業概要 |

| | |
|---|---|
| | ファシリテーションについて、その経緯や基本的な技法について解説した後、チーム内でディスカッションします。この回はチームディスカッションを含みます。チームワークの重要ポイントを理解し、チーム内の議論が効率的に進行することにより、チームディスカッションで適切にチームを運営し、チーム内のメンバーで円滑にコミュニケーションして意見を取りまとめることができるようになります。(LI/H1)　担当教員の実務経験を踏まえ、実務で有効な技術の習得を目指します。<br>③復習（240分）<br>チームのディスカッションを活発にするために、何をすれば良いか、自分でできること、チームのルールとして必要なことについて次回のディスカッションまでに考案してくること。 |
| 8 | ①授業テーマ<br>ケーススタディ（時系列の考察）<br>②授業概要<br>当該ケースを時系列で捉えるため、チーム内でケーススタディについて各自の意見を交換します。但し、前回のファシリテーションで学んだことを活用してディスカッションします。チーム内の状況に応じて議論の方向性を考えながら議論を進めて、他のメンバーの意見を傾聴し、自らの考えと融和を図ります。議論の成果は、後続回の内容と関連するもので、発生事象の関連性を捉えることが求められます。(ＬI/K2/I1/I3)<br>③復習（240分）<br>前回のファシリテーションで学んだことを有効活用できたか振り返ること。満足がいかない点の改善策を考えること。 |
| 9 | ①授業テーマ<br>ケーススタディ（技術的な視点）<br>②授業概要<br>前述の事案について、システム環境を技術的視点から更に深度を上げて考察します。受講生は当事案の複数の構成の関連性を捉えることを目標にチームでディスカッションします。講義後は、サイバー犯罪事案のいくつかの技術要素とその関連性について説明できるようになります。(EI/H1)<br>③復習（240分）<br>ケーススタディについて技術的な視点からはどの様な原因が考えられ、それらの因果関係がどの様に繋がっているのか考察すること。 |
| 10 | ①授業テーマ<br>ケーススタディ（人的管理の視点）<br>②授業概要<br>前述の事案について、人的システム管理の視点から更に深度を上げて解説します。受講生は組織の取組みがどのようにサイバー犯罪の解決に影響するか、チームでディスカッションします。講義後は、サイバー犯罪事案のいくつかの人的管理に起因する要素とその課題点について説明できるようになります。(EI/H1)<br>③復習（240分）<br>ケーススタディについてシステム管理の観点からどの様な原因が考えられ、それらの因果関係がどの様に繋がっているのか考察すること。 |
| 11 | ①授業テーマ<br>ロジカルシンキング技法<br>②授業概要<br>ロジカル・シンキングについて、その経緯や基本的な技法について解説します。これにより、受講生は論理的に思考を展開する技法を理解し、これを講義の中や実生活で活用することが期待されます。この回はチームディスカッションを含みます。講義後はサイバー犯罪事案の考察において論理的思考を意識できるようになります。(H1/I1)　担当教員の実務経験を踏まえ、実務で有効な技術の習得を目指します。<br>③復習（240分）<br>ケーススタディについて情報流出が発生した理由にはどの様なカテゴリが考えられるか、個運限的な理由には何が考えられるのか、ロジカルシンキングの技法を使って考察すること。 |
| 12 | ①授業テーマ<br>ケーススタディ（事象間の因果関係）<br>②授業概要<br>前述の事案について、サイバー攻撃に対してシステム構成や組織の行動がどの様に影響して被害に及ぶか、考察します。受講生は各要因間の関係性及び因果関係をチームでディスカッションします。講義後は、いくつかの重要な要因を導出する技術を習得することができるようになります。(EI/H1/F2)<br>③復習（240分） |

| | | |
|---|---|---|
| | | 取り上げているケーススタディについてどの様な犯罪に発展する可能性があるのか、別のサイバー犯罪の事案ではどの様な影響が予想されるか考察すること。 |
| | 13 | ①授業テーマ<br>リスク考察とプレゼンテーション準備<br>②授業概要<br>危機管理の観点から情報セキュリティに関するリスクの特性を考察します。担当教員の実務経験を踏まえ、問題解決の実践的な対応力について説明します。(E1/H1/L1) この回では，プレゼンテーションの条件を説明、チーム毎に活動計画を立案します。<br>③予習（120分）<br>前回までのディスカッションの結果を振り返ること。<br>④復習（240分）<br>発表までの段取りを各チームで合意して、プレゼンテーションに向けて準備すること。 |
| | 14 | ①授業テーマ<br>成果発表１<br>②授業概要<br>ディスカッションの成果物としての発表資料をチーム毎に発表します。発表後はチーム間で相互にコメントを出し合い、多様な意見を認識し、自らのセキュリティ管理に関する見識を再考します。(E1/H1/L1)　担当教員の実務経験を踏まえ、実践的能力の強化を意識してアドバイスします。<br>③予習（120分）<br>自チームの発表の段取りを事前に整えること。<br>④復習（120分）<br>発表後のコメントを受けて適宜修正してレポートとして提出すること。 |
| | 15 | ①授業テーマ<br>総括<br>②授業概要<br>本コース全体を通して、学んできたこと、不足していることについて再考します。講義の中で取り扱うことができなかったケースや今後のサイバー犯罪事情の予想等についてコメント及びフリーディスカッションとします。(E1/H1)<br>③復習（240分）<br>本コース全般を通して情報セキュリティについて履修した内容を配布教材を参照しながら再考すること。 |
| 関連科目 | 情報技術と社会(未定)、サイバーセキュリティ論(RMGT 3573)、デジタルフォレンジック(RMGT 3577)、情報法(RMGT 3471) 、危機管理特殊講義２（デジタルリスク） (02060024) が関連します。 | |
| 教科書 | 特にありません。講義で使用する資料は教員から提供します。 | |
| 参考書・参考ＵＲＬ | 講義中に適宜紹介します。 | |
| 連絡先・オフィスアワー | ■連絡先<br>開講時に公開します。<br>■オフィスアワー<br>火曜５限を予定しています。 | |
| 研究比率 | ■ 危機管理四領域との対応<br>情報セキュリティ：100%<br>■ 危機管理と法学との割合<br>危機管理：95% 法学：5% | |

戻る