シラバス参照

タイトル「**2023年度危機管理学部(公開用)**」、フォルダ「**実務経験のある教員による科目**」
シラバスの詳細は以下となります。

戻る

科目ナンバー	RMGT3577		
科目名	デジタル・フォレンジック		
担当教員	野﨑　周作		
対象学年	3年,4年	開講学期	前期
曜日・時限	木２		
講義室	1309	単位区分	選
授業形態	講義	単位数	2
科目大分類	専門		
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 市民的素養を基礎として、法学と危機管理に関する高度な学識と技能（リーガルマインド、リスクリテラシー）を運用する能力 DP4 問題を探求し、状況を的確に分析する能力 ■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 E1　学識・専門技能　（70%） I3　情報分析　（30%）		
教員の実務経験	2004年デジタル・フォレンジック専門企業であるFRONTEO社に入社。以来、企業のコンプライアンス支援として、デジタルフォレンジックを活用した機密情報漏えいや不正会計などの内部不正調査・監査のためのソリューションを提供してきました。また、その知識と経験をもとに、米国をはじめとする国際訴訟に必要な証拠開示（eディスカバリ）に関する支援を行っています。本授業ではデジタル・フォレンジックの手順やフローに関して実務上の知見と経験を活かして講義を行います。(第４回～第６回、第８回～第１０回) 特定非営利活動法人デジタル・フォレンジック研究会　幹事。		
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比 3　発展期　～　4　定着期		
科目概要・キーワード	■科目概要 犯罪、サイバーテロ、国際訴訟、企業内不正などの危機事案が発生した際、どのようなリスクや被害があるか正確に把握する事が生じる損害や障害を最小化する為に必要であり、また現代のICT化社会においては、それらの情報は多くはデジタル機器に記録されている。 デジタル・フォレンジックとは，犯罪や法的紛争が発生した際，その捜査や原因究明に必要なコンピュータなどのデジタル機器やデータ，電子的記録を収集・分析し，その解決のために法的証拠を発見して活用するための手段や技術のことである。デジタル・フォレンジックは一般犯罪においても，企業内不正においても現代の犯罪捜査や法的対応調査に不可欠であり，そのデジタル・フォレンジックの基本的な手順や技術の概要を理解するとともに、それらをめぐる法制度や社会政策について考察する。 授業形態は講義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。 ■キーワード ・フォレンジック　・インシデントレスポンス　・ディスカバリ　・リーガルマインド		
授業の趣旨	■副題 あらゆるモノがコンピュータ化する社会においてデジタルデータの性質やそこに残る痕跡を証		

<table>
<tr><td></td><td>拠化する仕組みを学び情報化時代に強い危機管理担当者になりましょう。
■授業の目的
デジタル・フォレンジックの歴史や必要とされる分野を体系的に理解するとともに、デジタル機器や電子データの法的証拠として取り扱いといった基本的な手続きを理解する事を目的とする。また、デジタル・フォレンジックの最新技術を用いる事により、解析対象となるデジタル機器から得られる証拠となり得る情報の種類や、大容量データの効率的な解析手法を理解する事を目的とする。
■授業のポイント
法科学（ほうかがく、英: Forensic Science、フォレンジック・サイエンス）とは、犯罪捜査などにおいて事件の解決と刑事訴訟・民事訴訟の法廷における立証を目的として用いられる応用科学であり、科学的方法を用い、司法の原則に則り「法廷で認められる」証拠分析を行う事、及びその手続のことを言う。その中でデジタル分野に対する領域をデジタル・フォレンジックと呼ぶ。デジタルデータには筆跡のようなものはなくかつ簡単に改ざんが可能である為、記録されている情報の真正性を証明するためには適切な取り扱いが必要となる。分かりやすい例で示すと、証拠となるコンピュータ等の電子機器に直接アクセスしてしまうとそれによりデータが書き換わってしまう可能性があり、それは殺人現場に落ちている血の付いたナイフに素手で触る行為に等しい。 デジタル・フォレンジック自体は専門性の高い分野であるが、デジタルデータを証拠として取り扱うための基本的な考え方を理解しておくことは情報セキュリティ領域にとどまらずあらゆる危機管理領域にとって重要である。本授業ではデジタル・フォレンジックの手続きや解析で分かる事、デジタル・フォレンジックが活用されている事例など広く網羅します。</td></tr>
<tr><td>総合到達目標</td><td>１）デジタル・フォレンジックに関する基礎的な考え方や手続きを説明できる。
２）危機事案の発生時におけるデジタル機器や電子データの法的証拠としての取り扱う上での注意点を説明できる。
３）デジタル機器から得られる証拠となり得る情報に関して説明することができる。
４）社内不正調査や米国民事訴訟におけるeディスカバリ（電子情報開示）への活用事例を理解し、説明できる。</td></tr>
<tr><td>成績評価方法</td><td>以下の方法で総合的に評価する。
（適用ルーブリック：割合）
E1：70%　I3：30%
（成績評価手段）
授業参加度　：　40%
小テスト：　30%
（評価の観点）データ収集（証拠保全）、復元までの理解度をはかります。
（フィードバック方法）授業時間中に解説を行います。
授業内テスト：　30%
（評価の観点）当該単元の理解度をはかります。
（フィードバック方法）授業時間中に解説を行います。</td></tr>
<tr><td>履修条件</td><td>特にありません。</td></tr>
<tr><td>履修上の注意点</td><td>PC（特にWindows）の基本的なオペレーションを理解していることが望ましい。</td></tr>
<tr><td>授業内容</td><td>
<table>
<tr><th>回</th><th>内容</th></tr>
<tr><td>1</td><td>(授業テーマ)デジタル・フォレンジック序論
(授業概要)デジタル・フォレンジックの歴史を知るうえで必要なコンピュータ技術の歴史や、セキュリティに関連する技術・事件の歴史について国内及び海外の事例をもとに理解する事を目的とする。また、デジタル・フォレンジックが使用されている分野の体系を理解する事を目的とする。（E1）
（運営方法）講義
（予・復習）
予習（120分）　：　デジタル・フォレンジックとは何かについて説明したWEBサイトなどを読んで要点をまとめて持参する。
復習（120分）　：　講義を振り返り、デジタル・フォレンジックが使用された最近のニュースを１つ選び出して読んでみる。</td></tr>
<tr><td>2</td><td>(授業テーマ)デジタル・フォレンジック基礎
(授業概要)デジタルデータとはどのようなものか、その性質や、ビット（binary digit,bit）とバイト（byte）といった電子情報を扱う上での最小単位、ハードディスクドライブの種類や情報が記録される仕組みを理解する事を目的とする。また、初動対応（インシデントレスポンス）－証拠保全－解析－報告というデジタル・フォレンジックの基本的な手続き・フローを理解する事を目的とする。（E1）
（運営方法）講義
（予・復習）
予習（120分）　：　ビットとバイトの違い及びセクタとクラスタの違いを調べてお</td></tr>
</table>
</td></tr>
</table>

		く。 復習（120分）　：　講義資料を読み返しておく。
	3	(授業テーマ)パーソナルコンピュータにおけるフォレンジック基礎 (授業概要)デジタル・フォレンジックの中で最も調査対象となる事の多いパーソナルコンピュータによって記録される情報について理解する事を目的とする。また、NTFSやFATといったファイルシステムの役割を理解し、コンピュータ上に情報が記録される仕組みを理解する事を目的とする。（E1） （運営方法）講義 （予・復習） 予習（120分）　：　パーソナルコンピュータのOSの種類とファイルシステムの関係について調べておく。 復習（120分）　：　講義資料を読み返しておく。
	4	(授業テーマ)デジタル・フォレンジック実務　初動対応（インシデントレスポンス） (授業概要)デジタルデータは揮発性の高い情報である為、初動対応時に適切に調査対象デバイスの取り扱いを行わないと失われてしまう情報も多い。担当者の実務経験を踏まえて、一番初めに行うべき事前準備とインシデント発生時におけるインシデントレスポンスの重要性と注意点について、調査対象デバイスの種類やインシデントの状況に応じて適切に対応する為のポイントを講義する。（E1） （運営方法）講義 （予・復習） 予習（120分）　：　インシデントレスポンスついて調べておく。 復習（120分）　：　講義資料を読み返しておく。
	5	(授業テーマ)デジタル・フォレンジック実務　証拠保全 (授業概要)担当者の実務経験を踏まえて、デジタル・フォレンジックにおいて調査対象デバイスの100%物理コピー（フォレンジックコピー）を作成する証拠保全作業について、ハードウェアとソフトウェアを使用した証拠保全のそれぞれの特徴について講義する。また、調査対象デバイスにパスワードや暗号化等のセキュリティが設定されている場合の証拠保全に関して、最適な対応を理解する事を目的とする。（E1） （運営方法）講義 （予・復習） 予習（120分）　：　証拠原本と保全されたコピーとの同一性証明に用いられるハッシュ値（ハッシュ関数）について調べておく。 復習（120分）　：　講義資料を読み返しておく。
	6	(授業テーマ)デジタル・フォレンジック実務　データ復元 (授業概要)デジタル・フォレンジック調査において削除されているデータの復元は調査目的を問わず重要である。本授業では担当者の実務経験を踏まえて、デジタル・フォレンジック技術により証拠保全されたデータを解析し、どのようにデータが復元されるのか、複数のデータ復元手法を講義する。また、合わせてデータ復元が困難になるデータ消去の方法についても理解する事を目的とする。（E1） （運営方法）講義 （予・復習） 予習（120分）　：　第3回の講義資料を読み返し、ファイルシステム（NTFS、FAT）の働きに関して理解を深めておく。 復習（120分）　：　講義資料を読み返しておく。
	7	(授業テーマ)デジタル・フォレンジック実務　実習（証拠保全・データ復元） (授業概要)デジタル・フォレンジックのハードウェアやソフトウェアを使用し、実際に証拠保全作業を経験する事で証拠保全作業に関する理解を深める事を目的とする。証拠保全時おいて調査対象デバイスの原本と証拠保全によって作成された複製のハッシュ値を算出し、証拠として取り扱う為に必要となる原本と複製の同一性の検証を実習を通して確認するとともに、保管の継続性を証明する為のCOC（Chain of Custody）の書類の書き方も理解する事を目的とする。（I3） （運営方法）実習（WindowsPC使用） （予・復習） 予習（120分）　：　第5回、第6回の講義資料を読み返し、証拠保全、データ復元に関して理解を深めておく。 復習（120分）　：　実習で行った事を再度自分で行ってみる。
	8	(授業テーマ)デジタル・フォレンジック実務　解析① (授業概要)デジタル・フォレンジックを行う上で、調査対象デバイスにおいて、いつどのような事が行われたか履歴を調査する事は重要である。本授業では担当者の実務経験を踏まえて、Windows OSに記録されるレジストリやイベントログといったシステムファイルから取得できる行動履歴やファイルのタイムスタンプから取得できる行動履歴などをタイムラインで総合的に解析し、調査対象コンピュータ内でいつ・どのような事が

	行われたのか解析していく調査手法を講義する。（I3） （運営方法）講義 （予・復習） 予習（120分）　：　第３回の講義資料より、パーソナルコンピュータの機能と特徴について整理しておく。 復習（120分）　：　講義資料を読み返しておく。
9	(授業テーマ)デジタル・フォレンジック実務　解析② (授業概要)デジタル・フォレンジックを行う上で、膨大なデータの中から必要な情報を効率的に探し出す事は重要である。本授業では担当者の実務経験を踏まえて、日本語を含むアジア言語のキーワード検索に必要な技術や、類似データの検索技術、人工知能応用技術を用いた調査手法などを用いて、効率的に証拠を見つけ出す調査手法を講義する。また、アプリケーションファイルに付随するメタデータやWEBの閲覧履歴に関する調査手法を理解する事を目的とする。（I3） （運営方法）講義 （予・復習） 予習（120分）　：　人工知能技術にはどのようなものがあるか調べておく。 復習（120分）　：　講義資料を読み返しておく。
10	(授業テーマ)デジタル・フォレンジック実務　解析③ (授業概要)デジタル・フォレンジック調査を行う上で障害となる不正の証拠を残さない、証拠隠滅する行為や技術をアンチフォレンジックと呼ぶ。犯罪者や不正行為者は証拠を残さないようにするためにアンチフォレンジック行為を行う事が予想される。担当者の実務経験を踏まえて、予想されるアンチフォレンジック行為とそれによるデジタル・フォレンジック調査に対する障害の程度を講義する。本授業内にて小テストを実施する。（I3） （運営方法）講義 （予・復習） 予習（120分）　：　アンチフォレンジックにはどのようなものがあるか調べておく。 復習（120分）　：　講義資料を読み返しておく。
11	(授業テーマ)デジタル・フォレンジック実務　実習（解析） (授業概要)デジタル・フォレンジックの解析ソフトウェアを使用し、証拠保全したデータの解析実習を行う。第８回～第10回の内容を実習を通じて理解を深める事を目的とする。（I3） （運営方法）実習（WindowsPC使用） （予・復習） 予習（120分）　：　第8回～第10回の講義資料を読み返し、解析に関して理解を深めておく。 復習（120分）　：　実習で行った事を再度自分で行ってみる。
12	(授業テーマ)モバイル端末におけるフォレンジック基礎 (授業概要)デジタル・フォレンジックにおいて今後更に重要となるスマートフォンやタブレット端末等の種類や機能を理解するとともに、通信機器としての取り扱いの注意点や、iOS及びAndroid OSといったモバイル端末向けOS毎のデジタル・フォレンジックを行う上で必要となる特徴について理解する事を目的とする。（E1） （運営方法）講義 （予・復習） 予習（120分）　：　スマートフォンとOSの種類と関係性について調べておく。 復習（120分）　：　講義資料を読み返しておく。
13	(授業テーマ)企業内におけるフォレンジック調査（国内訴訟事例） (授業概要)企業内で発生し得る様々な危機事案（機密情報の情報漏えいや購買不正といった内部不正、標的型攻撃やウィルス感染といった外部からの脅威）に関して、初動対応から証拠保全、解析に至るまで、どのようにデジタル・フォレンジックを活用すべきか、実際の案件事例を通して理解する事を目的とする。（E1） （運営方法）講義 （予・復習） 予習（120分）　：　過去の情報漏えい事案のニュースを読みデジタル・フォレンジック活用事案を調べておく。 復習（120分）　：　講義資料を読み返しておく。
14	(授業テーマ)国際訴訟におけるeディスカバリ（国際訴訟事例） (授業概要)デジタル・フォレンジックは米国民事訴訟におけるeディスカバリにも使用されている技術であり、eディスカバリは大容量データから証拠となり得る情報を精査するベストプラクティスとして、米国をはじめとする海外司法当局の捜査や第三者委員会の調査などにも広く活用されている。本講義ではEDRM（The Electronic Discovery Reference Model）と最新の技術トレンドを実際の案件事例を通して理解する事を目的

		とする。（E1） （運営方法）講義 予習（120分）　：　EDRM（The Electronic Discovery Reference Model）について調べておく。 復習（120分）　：　講義資料を読み返しておく。
	15	(授業テーマ)デジタル・フォレンジックのまとめ (授業概要)14回の講義及び実習で学んできたことを総括し、デジタル・フォレンジックのまとめと今後のデジタル・フォレンジックの在り方や課題について考察する。授業内テストを実施する。（E1） （運営方法）講義 （予・復習） 予習（120分）　：　講義資料及び講義ノートの全体を読み直すこと。 復習（120分）　：　デジタル・フォレンジックを今後の自身のキャリア選択、領域選択にどのように生かせるか検討する。
関連科目		RMGT 3571 情報管理論 RMGT 3573 サイバーセキュリティ論 RMGT 3576 情報システム論
教科書		特になし。毎回レビュメ及び資料を配布する。
参考書・参考ＵＲＬ		安冨潔、上原哲太郎（編著）『基礎から学ぶデジタル・フォレンジック～入門から実務の対応まで～』（日科技連出版社）。 佐々木良一編著『デジタル・フォレンジックの基礎と実践』（東京電機大学出版局）。 羽室英太郎、國浦淳（編著）『デジタル・フォレンジック概論～フォレンジックの基礎と活用ガイド～』（東京法令出版）。 守本正宏『日本企業のディスカバリ対策 世界と対等に戦うためのeディスカバリの正しい手順』（グローバルトライ）。 佐々木良一監修『改訂版　デジタル・フォレンジック事典』（日科技連出版社）。
連絡先・オフィスアワー		■連絡先　授業前後の時間で質問に対応
研究比率		災害マネジメント0%：パブリックセキュリティ10%：グローバルセキュリティ10%：情報セキュリティ80% 危機管理学70%：法学30%

戻る

Copyright (c) 2016 NTT DATA KYUSHU CORPORATION. All Rights Reserved.