1．科目名（単位数）	情報セキュリティ　（2単位）	3．科目番号	EDIT3323
2．授業担当教員	里吉竜一		
4．授業形態	演習	5．開講学期	春期
6．履修条件・他科目との関係	情報科免許教諭必修科目 科目「コンピュータネットワーク 1」と「II」、「コンピュータサイエンス 1」と「II」を履修済みであることが望ましい。		
7．講義概要	本科目では、コンピュータシステムおよびデータのセキュリティとプライバシー保護について学ぶ。具体的には、システム保護、システムの信頼性、システムの欠陥への対処、データ保護と暗号、ハッキングとソーシャルエンジニアリングについて演習を通じて、かなり高度な内容にまで踏み込み、情報セキュリティに関する深い理解を図る。		
8．学習目標	技術の面、国際および国内規程の面からみた情報セキュリティの基礎を学ぶ。 ITに関しては、抽象的なことだけではなく、ハッカーの基本的技術を学び、また、今までの様々な事例を見ながら、情報システムの欠陥をどう探すか、どう防ぐかを考えることができる。 情報資産への脅威は、最近、ITが大部分を占めているが、IT以外にも多くのリスクが存在する。それらのリスクの分析、評価の方法についても考えることが出来るようになる。		
9．アサイメント（宿題）及びレポート課題	授業ごとに提出するレポートを作成して発表及びディスカッションを行うことで思考力及び表現力とコミュニケーション能力を身に付けることができます。最終課題は、これまでに学習した内容の要点を整理し、それらに対する自分の意見を発表して提出します。 ・レポート課題（各講義毎） ・最終課題（1回）		
10．教科書・参考書・教材	・教科書：中村行弘、若尾靖和、林静香『情報セキュリティ』技術評論社、2021。 ・副教材：西俊明『改訂6版ITパスポート最速合格術』技術評論社、2023。 ・参考書：講義の中で適宜紹介します		
11．成績評価の規準と評定の方法	○成績評価の規準 技術の面、国際および国内規程の面からみた情報セキュリティの基礎を学ぶことができたか。 ○評定の方法 1．授業ごとに提出されるレポート、小テスト、課題提出状況など70% 2．授業への積極的参加と受講態度30%		
12．受講生へのメッセージ	・教科「情報」教員免許を取得して学校現場で生徒を指導できるノウハウを身に付けることができます。 ・正解を事前に設定できない問題を科学的な根拠に基づいて解決し、生涯にわたって自ら学び続けられる素養を身に付けることができます。 ・Society5.0とGIGAスクール構想に対応した授業を設計するので各自パーソナルディバイス（スマホかタブレット）を準備してください。 ・質問はいつでも気軽にしてください。 ・欠席、遅刻、早退をする場合は連絡してください。 ・本学規定により3/4以上の出席が確認できない場合は単位の修得を認められないので注意してください。		
13．オフィスアワー	・面談や補講の希望者は事前にメール等で連絡してください。p-rysatoyo@ed.tokyo-fukushi.ac.jp		

14．授業展開及び授業内容

講義日程	授業内容	学習課題	
第1回	イントロダクションI 情報セキュリティの概要、ICT経験値に関するアンケート、アクティブ・ラーニング及び最終課題について等を確認して講義の導入とします。	事前学習	はしがきを読んでおく。
		事後学習	発表レジメの書き方や発表の方法等について理解した上で、最終課題発表の準備を始める。
第2回	情報セキュリティの基礎知識について講義します。	事前学習	情報セキュリティの基礎知識について復習しておく。
		事後学習	情報セキュリティの基礎知識の要点をまとめる。
第3回	根本的なセキュリティ対策について講義します。	事前学習	根本的なセキュリティ対策について調べておく。
		事後学習	根本的なセキュリティ対策の要点をまとめる。
第4回	第1章　セキュリティの概念と対策の方針	事前学習	教科書pp.9〜26を読んで要旨をドキュメントファイルにまとめて提出しておく。
		事後学習	セキュリティの概念と対策の方針の要点をまとめる。
第5回	情報セキュリティにおける「認証」の重要性	事前学習	情報セキュリティにおける「認証」の重要性をドキュメントファイルにまとめて提出しておく。
		事後学習	「認証」の重要性の要点をまとめる。
第6回	第2章　サイバー攻撃の手法①	事前学習	教科書pp.28〜60を読んで要旨をドキュメントファイルにまとめて提出しておく。
		事後学習	サイバー攻撃の手法の要点をまとめる。
第7回	第3章　サイバー攻撃の手法②_その1	事前学習	教科書pp.61〜89を読んで要旨をドキュメントファイルにまとめて提出しておく。

		事後学習	サイバー攻撃の手法②の要点をまとめる。
第８回	第３章　サイバー攻撃の手法②_その２	事前学習	教科書 pp.90～118 を読んで要旨をドキュメントファイルにまとめて提出しておく。
		事後学習	サイバー攻撃の手法②の要点をまとめる。
第９回	第４章　セキュリティ確保の基礎技術	事前学習	教科書 pp.119～144 を読んで要旨をドキュメントファイルにまとめて提出しておく。
		事後学習	セキュリティ確保の基礎技術の要点をまとめる。
第１０回	第５章　情報セキュリティの管理	事前学習	教科書 pp.145～166 を読んで要旨をドキュメントファイルにまとめて提出しておく。
		事後学習	情報セキュリティの管理の要点をまとめる。
第１１回	第６章　情報セキュリティ対策の基礎知識	事前学習	教科書 pp.167～212 を読んで要旨をドキュメントファイルにまとめて提出しておく。
		事後学習	情報セキュリティ対策の基礎知識の要点をまとめる。
第１２回	第７章　セキュリティの実装に関する知識	事前学習	教科書 pp.213～246 を読んで要旨をドキュメントファイルにまとめて提出しておく。
		事後学習	セキュリティの実装に関する知識の要点をまとめる。
第１３回	最終課題の作成と提出 これまでに学習したことを活用して最終課題を作成するために、「テーマ」「作成条件」「評価規準」を確認して評価方法、評価システム、教育的価値等を講義します。	事前学習	これまでの授業内容を復習しておく。
		事後学習	諸条件を確認して期末レポートを提出する。
第１４回	最終課題の発表 所定の場所に最終課題を提出して発表します。	事前学習	前回の授業内容の復習をしておく。
		事後学習	「評価規準」を確認して自己評価及び相互評価の教育的価値を考える。
第１５回	総合演習：自己評価と相互評価 学生自身が他者の成果物を評価するのと同じように客観的に自己の成果物も評価する実践を行います。自己の内面に向かう自己教育力の醸成を目的とします。	事前学習	最終課題を客観的に評価する意義を考えておく。
		事後学習	どうしたら客観的な自己評価ができるようになるかについての考察を深める。