2023 年度　長岡大学シラバス

授業科目名 科目コード	情報セキュリティ概論(Introduction to Information Security) 392078-14-700					担当教員	吉川　宏之 （ヨシカワ　ヒロユキ）		
科目区分	専門科目	必修・選択区分	選択	単位数	2	配当年次	2 年次	開講期	前期
科目特性	知識定着・確認型 AL								

① 授業のねらい・概要
コンピュータとインターネットは、今では欠かせないものです。しかし、コンピュータウイルス感染や詐欺、個人情報の流出などの様々な脅威にさらされています。 コンピュータウイルスやネットワークにおけるセキュリティの基本をふまえたうえで、一般利用者として必要なセキュリティ対策の基本を学んでいきます。
② ディプロマ・ポリシーとの関連
職業人として通用する能力／専門的知識・技能を活用する能力
③ 授業の進め方・指示事項
テキストに沿って行います。授業時は必ず参照できるようにすること。 授業内容を復習し、リスクとセキュリティ対策を理解すること。 各自の所有するパソコン、スマートフォン等に対策を行うこと。 情報セキュリティ関連の最近のニュースを調べること。
④ 関連科目・履修しておくべき科目
⑤ テキスト（教科書）
独立行政法人情報処理推進機構『情報セキュリティ読本 六訂版 -IT 時代の危機管理入門-』(実教出版株式会社)
⑥ 参考図書・指定図書
⑦ 評価 A に対応する具体的な学習到達目標の目安
コンピュータネットワークの利用について、以下の項目を目的とします。 （ｉ）どのようなリスクがあるのか理解する （ⅱ）被害を受けないためのセキュリティ対策の知識を持つ （ⅲ）被害を受けたときの対応を身につける

⑧　ルーブリック					
評価項目	評価基準				
	S 到達目標を越えたレベルを達成している	A 到達目標を達成している	B 到達目標達成にはやや努力を要する	C 到達目標達成には努力を要する	D 到達目標達成には相当の努力を要する
（ｉ）どのようなリスクがあるのか理解する。	外部のリスク要因、内部のリスク要因の最近の傾向を説明できる。	外部のリスク要因、内部のリスク要因の違いを説明できる。	外部のリスク要因を説明できる。	フィッシング詐欺、ワンクリック不正請求を説明できる。	マルウェアを説明できる。
（ⅱ）被害を受けないためのセキュリティ対策の知識を持つ。	被害を受けないために個人および組織が行うセキュリティ対策を説明できる。	被害を受けないために個人が行うセキュリティ対策を説明できる。	コンピュータウイルス感染などで起こる症状を説明できる。	パスワードなど個人認証の重要性を説明できる。	適切なパスワードを設定できる。
（ⅲ）被害を受けたときの対応を身につける。	被害を受けたときに組織が行うべき対応を順序付けて説明できる。	被害を受けたときに個人が行う対応を順序付けて説明できる。	被害を受けたときに個人が最初に行うべきことを説明できる。	重要なデータのバックアップを取ることができる。	情報機器をネットワークから切り離すことができる。

⑨　学習の到達目標（評価項目）とその評価の方法、フィードバックの方法								
学習到達目標（評価項目）	試験	小テスト	課題	レポート	発表・実技	授業への参加･意欲	その他	合計
総合評価割合	60%	20%				20%		100%
（ｉ）どのようなリスクがあるのか理解する	20%	7%				7%		34%
（ⅱ）被害を受けないためのセキュリティ対策の知識を持つ	20%	7%				7%		34%
（ⅲ）被害を受けたときの対応を身につける	20%	6%				6%		32%
フィードバックの方法	小テストの内容について解説を行い、間違いの多かった点は授業内で復習を行う。							

⑩　担当教員からのメッセージ（昨年度授業アンケートを踏まえての気づき等）
情報セキュリティ関連の最近のニュースを紹介することで、情報セキュリティが身近な出来事であることを実感させる。

⑪　授業計画と学習課題

回数	授業の内容	授業外の学習課題と時間（分） （※特別な持参物）	
1	授業の進め方 情報セキュリティにおける被害事例	1-1 情報セキュリティにおける被害事例の整理・復習	60 分
2	危険の認識と対策	1 章今日のセキュリティリスクの整理・復習	150 分
3	情報セキュリティとは 外部のリスク要因	2-1 情報セキュリティとは、2-2 外部のリスク要因の整理・復習	150 分
4	内部のリスク要因	2 章情報セキュリティの基礎の整理・復習	150 分
5	マルウェア	3-1 マルウェアの整理・復習	150 分
6	共通の対策	3-2 共通の対策の整理・復習	150 分
7	標的型攻撃と誘導型攻撃への対策	3-3 標的型攻撃と誘導型攻撃への対策の整理・復習	150 分
8	前半のまとめ	前半の復習	150 分
9	フィッシング詐欺への対策	3-4 フィッシング詐欺への対策の整理・復習	150 分
10	ワンクリック不正請求への対策	3-5 ワンクリック不正請求への対策の整理・復習	150 分
11	スマートフォンの脅威と対策	3-6 スマートフォンの脅威と対策の整理・復習	150 分
12	無線 LAN に潜む脅威とその対策	3 章見えない驚異とその対策の整理・復習	150 分
13	アカウント、ID、パスワード	5-1 アカウント、ID、パスワードの整理・復習	150 分
14	暗号とディジタル署名	5-5 暗号とディジタル署名の整理・復習	150 分
15	情報セキュリティ関連の法規	6-1 情報セキュリティ関連の法規の整理・復習。全体の振り返り。	90 分

⑫　アクティブラーニングについて
知識定着・確認型 AL を採用する。授業の終わりに演習問題を課し、回答を提出させることで、理解できていない部分を確認し、学修にフィードバックする。次回の始めに前回の演習問題の解説を行い、知識の定着をはかる。 6 回程度の小テストを行い、理解を深めるための解説を行う。

※以下は該当者のみ記載する。

⑬　実務経験のある教員による授業科目
実務経験の概要
実務経験と授業科目との関連性