| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 授　業<br>科目名 | 【Ｇ】　情報セキュリティⅡ<br>【Ｈ】　情報セキュリティⅡ | 区　　分<br>その他参照 | | 開講年次 | 【Ｇ】2<br>【Ｈ】2 | 単位数 | 【Ｇ】2<br>【Ｈ】2 |
| 科目区分 | 基本科目:【Ｇ･Ｈ】教科及び教科の指導法に関する科目（ー･ー･ー･情報） | | | | | | |
| 授業形態 | 対面授業 | | | | | | |
| 担当形態 | 単　独 | 【Ｇ】　教員の免許状取得のための　（ー･ー･ー･情報選択）科目 | | | | | |
| 施行規則に定める科目区分又は事項等 | | 教科に関する専門的事項:「情報通信ネットワーク（実習を含む）」（高一種免情報） | | | | | |
| サブ<br>タイトル | 情報セキュリティの人的要素と社会制度 | | | 担当者 | 谷津　貴久 | | |

| | | |
|---|---|---|
| 授業概要 | 【概要】 | 情報通信機器は人間が利用するために存在しています。そのため、情報通信機器に対する技術的な攻撃のほかに、人間の弱さを突く攻撃にも注意しなければなりません。また、個人が所属する組織で情報セキュリティを考えるときには組織での取り組みが必要となり、さらに上位の国家や国際的な組織による取り組みも必要となります。この講義では情報セキュリティの人的要素を主に取り上げて、私たちの社会に必要な対策について考えていきます。 |
| | 【到達目標】 | 情報セキュリティの人的要素とその対策にはどのようなものがあるのかが説明でき、私たちの国の情報セキュリティ関連制度についても説明できることを到達目標とします。 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| アクティブラーニングの方法 | 【 ー 】 | 事前学習型 | 【 ー 】 | 反転授業 | 【 ー 】 | 調査学習 | 【 ー 】 | フィールドワーク |
| | 【 ー 】 | 双方向アンケート | 【 ー 】 | グループワーク | 【 ー 】 | 対話･議論型授業 | 【 ー 】 | ロールプレイ |
| | 【 ー 】 | プレゼンテーション | 【 ー 】 | 模擬授業 | 【 ー 】 | PBL | 【 ー 】 | その他 |

| | | |
|---|---|---|
| ディプロマ･ポリシーとの関連性 | DP（ディプロマ･ポリシー）① | ー　（当てはまらない） |
| | DP（ディプロマ･ポリシー）② | ー　（当てはまらない） |
| | DP（ディプロマ･ポリシー）③ | ◎　（よく当てはまる） |
| | DP（ディプロマ･ポリシー）④ | ー　（当てはまらない） |

| | |
|---|---|
| 他科目との関連性 | 「情報セキュリティⅠ」と相補的関係にあります。 |
| 教科書 | 『図解入門 よくわかる 最新情報セキュリティの技術と対策』, 若狭直道著, 2021, 秀和システム, ISBN978-4-7980-6463-5 |
| 参考書 | 授業中に適宜紹介します。 |
| 評価方法 | 試験（80%）、授業への参加態度（20%）で評価します。 |
| フィードバック方法 | 試験の実施後に解説を行います。授業内に時間が取れなかったときには Google Classroom に掲載します。 |
| 評価基準 | 授業内容についてよく理解していると見なせた者にはその程度に応じてＳまたはＡ、一部不十分な箇所がある者についてはＢまたはＣとします。授業内容への理解自体が不十分な者については、その程度に応じてＤまたはＥとします。出席要件を満たさないなど評価不能の場合にはＦとします。 |

| 授　業<br>科目名 | 【Ｇ】<br>【Ｈ】 | 情報セキュリティⅡ<br>情報セキュリティⅡ | 区　　分<br>その他参照 | 開講年次 | 【Ｇ】2<br>【Ｈ】2 | 単位数 | 【Ｇ】2<br>【Ｈ】2 |
|---|---|---|---|---|---|---|---|

| 授業回数 | 授業内容 | | | |
|---|---|---|---|---|
| 1 | 情報資産と脅威 | | | |
| | 予習: | 教科書1-3, 1-4節を通読する(60分) | 復習: | 脅威と攻撃者についてまとめる(120分) |
| 2 | 脆弱性の種類 | | | |
| | 予習: | 教科書1-9節とp.61のコラムを通読する(60分) | 復習: | 物理的・人的脆弱性をまとめる(120分) |
| 3 | ソーシャルエンジニアリング | | | |
| | 予習: | 教科書1-11, 4-4節を通読する(60分) | 復習: | この攻撃手法の種類と対策をまとめる(120分) |
| 4 | リスクマネジメント | | | |
| | 予習: | 教科書1-6, 5-4節を通読する(120分) | 復習: | リスクの種類と評価方法をまとめる(60分) |
| 5 | 情報セキュリティポリシ (1) | | | |
| | 予習: | 教科書1-6, 4-10節を通読する(90分) | 復習: | 情報セキュリティポリシの種類をまとめる(90分) |
| 6 | 情報セキュリティポリシ (2) | | | |
| | 予習: | 教科書1-6, 4-10節を通読する(90分) | 復習: | 基本方針を遵守させるためのポイントを確認する(90分) |
| 7 | 情報セキュリティマネジメントシステム | | | |
| | 予習: | 教科書5-1から5-6節を通読する(120分) | 復習: | 関連する規格を確認する(60分) |
| 8 | 情報セキュリティ関連制度 | | | |
| | 予習: | 教科書5-15から5-18節を通読する(120分) | 復習: | 国内のガイドラインを確認する(60分) |
| 9 | セキュリティ対処の組織 | | | |
| | 予習: | 教科書4-10, 4-12節を通読する(60分) | 復習: | CSIRTの役割についてまとめる(120分) |
| 10 | 情報セキュリティ監査 | | | |
| | 予習: | 教科書5-10, 5-11節を通読する(90分) | 復習: | システム監査との違いを確認する(90分) |
| 11 | 人的・物理的対策 | | | |
| | 予習: | 教科書4-17, 4-18節を通読する(90分) | 復習: | 不正と対策についてまとめる(90分) |
| 12 | 知的財産権と個人情報保護 | | | |
| | 予習: | 教科書4-14, 5-14節を通読する(90分) | 復習: | 情報セキュリティとの関連を確認する(90分) |
| 13 | セキュリティ関連法規 | | | |
| | 予習: | 教科書1-2, 4-13, 5-13節を通読する(90分) | 復習: | 法規と実際の対策との関連を確認する(90分) |
| 14 | 外国の取り組み | | | |
| | 予習: | 教科書5-19から5-21節を通読する(90分) | 復習: | 諸外国と日本の違いを確認する(90分) |
| 15 | セキュリティを高める具体策 | | | |
| | 予習: | 教科書4-1から4-7節を通読する(120分) | 復習: | 日々の対策の重要性を考える(60分) |
| その他 | 特になし<br><br>※G・Hｶﾘ:法【選択】ｽﾎﾟ【選択】情【必修】 | | | |

科目コード　A930-3-Y　(科目一覧番号：42)