

| | | | | | | | | | |
|---|----------------------------------|---------------------------------------|--------|----------------|-------------|------|------------|------|-----|
| 科目ナンバリング | | G-LAS12 80025 LJ10 G-LAS12 80025 LJ11 | | | | | | | |
| 授業科目名 <英訳> | 情報セキュリティ Information Security | | | 担当者所属 職名・氏名 | 非常勤講師 高倉 弘喜 | | | | |
| 群 | 大学院横断教育科目群 | | 分野(分類) | 統計・情報・データ科学系 | | 使用言語 | 日本語 | | |
| 旧群 | | 単位数 | 2単位 | 時間数 | 30時間 | 授業形態 | 講義(対面授業科目) | | |
| 開講年度・ 開講期 | 2026・ 前期集中 | | 曜時限 | 集中 金曜1・2限 | | 配当学年 | 修士課程 | 対象学生 | 全学向 |
| (情報学研究科の学生は、全学共通科目として履修登録できません。所属部局で履修登録してください。) | | | | | | | | | |
| 【授業の概要・目的】 | | | | | | | | | |
| IT化とネットワーク化が進行し、情報システムが企業活動・学術活動に不可欠になった現代において、そこに潜む脆弱性を狙ったサイバー攻撃により社会が大きな影響を受けることが問題となっている。本講義では、インターネットおよび組織内ネットワークを利用する際に知っておくべき知識、例えば、安全確保、攻撃からの防御と運用の継続、消されたデータの復旧、法制度などについて、システム管理者・利用者の視線に立ちながら最新技術を交えて講述する。 | | | | | | | | | |
| 【到達目標】 | | | | | | | | | |
| 情報システムを利用する上での危険性を認識するとともに、その対策の概要を知る。 | | | | | | | | | |
| 【授業計画と内容】 | | | | | | | | | |
| 開講日程： 5月8日(金)、15(金)、29日(金) 6月5(金)、12日(金)、19日(金)、26日(金) 各1-2限 期末試験・フィードバック： 7月3日(金) 1-2限 | | | | | | | | | |
| 【基礎技術】 ネットワークアーキテクチャ: IPv4、IPv6、TCP、UDP サイバー攻撃と防御技術: マルウェア、脆弱性攻撃、不正アクセス検知、アンチウィルス、ブロックチェーン、オニオンルーティング | | | | | | | | | |
| 【攻撃技術】 ソーシャルエンジニアリング 脆弱性探索: ペネトレーションテスト、倫理的ハッキング、レインボーテーブル 攻撃の自動化: AIによる脆弱性自動探索と攻撃プログラム自動作成 | | | | | | | | | |
| 【防御技術】 自動防御プログラム: 攻撃検知から防御プログラム生成 デジタルフォレンジックス: 消されたデータの復旧作業の手順と実態 サイバーインテリジェンスと状況把握: オープンソース情報、DarkWeb情報などの分析による状況把握 | | | | | | | | | |
| 【統合運用】 国内・国外の法制度: 著作権法、不正アクセス禁止法、IoT対策など サイバーにおけるグループ管理: インシデント発生時の危機管理 | | | | | | | | | |
| ----- 情報セキュリティ(2)へ続く ----- | | | | | | | | | |

情報セキュリティ(2)

[履修要件]

特になし

[成績評価の方法・観点]

講義でのディスカッション等への貢献度、講義終了後に提出されるレポートにより総合的に判断する。

[教科書]

特に定めない。必要な資料は講義において配布する。

[参考書等]

(参考書)

必要に応じて講義内で紹介する。

[授業外学修(予習・復習)等]

受講に際し特別の知識は必須ではないが、講義の効果を高めるため事前予習を課す場合がある。

[その他(オフィスアワー等)]

[主要授業科目(学部・学科名)]