講義のシラバス

6.1 サイバーセキュリティ

［開講科目名］

（授業科目）最新セキュリティ特論Ⅰ／（enPiT-Pro）サイバーセキュリティ

[単位数] 1 単位

［開講日］

大阪大学中之島センター

4/26 (金)上原 1. 講義室 302 18:00～19:30

4/27 (土)河野 1. 講義室 302 10:30～12:00

4/27 (土)河野 2. 講義室 302 13:00～14:30

5/10 (金)猪俣 1. 講義室 302 18:00～19:30

5/17 (金)上原 2. 講義室 302 18:00～19:30

6/14 (金)猪俣 2. 講義室 302 18:00～19:30

6/21 (金)上原 3. 講義室 302 18:00～19:30

7/19 (金)猪俣 3. 講義室 302 18:00～19:30

［担当教員］

猪俣 敦夫(東京電機大学), 上原 哲太郎(立命館大学), 河野 省二(日本マイクロソフト株式会社),
宮地 充子(大阪大学), 河内 亮周(大阪大学)

【リスクマネジメント・インシデント対応】(担当:猪俣敦夫)

[授業の目的・概要]

今や守るべき資産は目に見える有価物だけでなくデータそのものが重要な資産である. 組織が何らかの情報(データ)を管理し, それらを保護するための秘匿技術は数多く存在するが, 技術だけで情報が完全に保護できるわけでなく, それらの技術を適正に運用・維持することが重要である. 本講義では情報セキュリティマネジメントの基本である ISMS を中心とした, 組織における体系的な情報セキュリティリスクマネジメント手法について学ぶとともに, 実際に備えておくべきインシデント対応として幅広い視野を考慮し, その具体例として CSIRT, 事業継続計画(BCP)について触れる.

[授業の目標]

情報セキュリティマネジメントシステム(ISMS)を適切に理解し, 自分自身で情報セキュリティポリシを策定することができ, 様々なインシデントに対するリスクアセスメントが行えるための豊富な知識を得ることが目標である.

[知識単位]

ISMS, BS7799, ISO/IEC17799, ISO/IEC27001, JIS Q 27001, リスクアセスメント, PDCA, NIST SP800-53, CSIRT, JPCERT/CC, BCP(事業継続計画), ディザスタリカバリ, ISO/IEC17025, 制御システム

[講義計画]

第 1 回 情報セキュリティマネジメントシステム(ISMS)基礎

ISMS の歴史的背景として BS7799, ISO/IEC17799 を概観し, 組織の ISMS 構築, 運用に関する第 3 者認証の規格である ISO/IEC27001:2005 Information technology - Security techniques - Information security management systems - Requirements を学ぶ. さらに政府等における情報セキュリティ管理策として NIST SP ドキュメントにも触れる.

第 2 回 情報セキュリティポリシ策定とリスクアセスメント

ISMS を適正に運用するためには, 1. 情報セキュリティポリシの意識付け, 2. セキュリティ情報の収集と分析, 3. 実装した情報セキュリティ対策の日常的な監視, 4. 定期的な情報セキュリティ監査, 5. 見直しと改善, という流れが重要である. そこでケーススタディを提示し, 実際の情報セキュリティポリシ策定設計の演習を行う. この演習ではリスクへの対応として情報資産の価値, 脅威の視点からリスクアセスメントもあわせて行う.

第 3 回 CSIRT 設計と運用

情報セキュリティに関わる全ての組織においては CSIRT(Computer Security Incident Response Team)と名付けられた体制やグループを構築し, 運用していくことが求められる時代である. しかしながら, CSIRT を構築しただけの「名ばかり CSIRT」も多数存在するのが現状である. そこで CSIRT の基本として, 体制構築, 運用などのノウハウを学ぶ. また, グループごとにケーススタディをもとにした CSIRT 演習もあわせて行う.

第 4 回 国際規格とディザスタリカバリ

我が国では想定外の大規模な災害に見舞われた過去がある． このような災害時においては自助，共助，公助が重要な役割を担うが，これらを補完するのが情報システムと通信ネットワークである． これらのおかげで例えば道路が寸断されたエリアからの情報をいち早く受け取ることができる可能性がある． しかしながら平常時には利用しないシステムやネットワークが非常時に適正かつ迅速に動作する保証はない． そこで BCP の視点から様々なディザスタリカバリの技術を紹介する． さらに組織で適正に運用するための国際規格である ISO/IEC17025 について触れるとともに今後の制御システムセキュリティのあり方についても言及する．

［履修条件・受講条件］

特に事前知識は仮定しないが，下記があるとより理解が深まる．

－ ISO/IEC17799

［授業外における学習］

演習課題（教育システムで提示）

テキストの予習及び演習課題（教育システムで提示）

テキストの予習（教育システムで提示）

［参考文献］

情報セキュリティ白書 2017：IPA 独立行政法人 情報処理推進機構

【システムとネットワークのセキュリティ・フォレンジックス】(担当:上原　哲太郎)

[授業の目的・概要]

情報システムの設計・導入・運用・事故対応に際し，セキュリティ確保のために必要な知識を習得する．　セキュアなシステムを調達導入し，可能な限り低いコストでセキュリティ事故を素早く見つけ出す体制を構築して運用し，事故発生時に適切に対応するためのさまざまな知識を習得する．

[授業の目標]

情報システムの設計・導入・運用・事故対応にかかるセキュリティの課題を概観することでセキュアな情報システムの導入運用と事故発生時への適切かつ迅速な対応能力を養成する．

[知識単位]

セキュリティ要求，ソフトウェア脆弱性，ログ監査，ファイアウォール，Web アプリケーション脆弱性，DDoS 攻撃，証拠保全，メモリフォレンジック，削除ファイル復活

[講義計画]

第 1 回 システム管理とセキュリティ

システムの導入設計開発または調達と運用にかかるセキュリティについて学ぶ．

特にシステム設計時に必要な要求工学とシステム脆弱性の原理，システムの運用計画について述べる．

第 2 回 ネットワークセキュリティ

ネットワークレイヤにおけるセキュリティ確保に必要な機器の原理・機能と利用法，

ネットワークによる攻撃，Web セキュリティの基本について学ぶ．

第 3 回 デジタル・フォレンジックス

インシデントレスポンスに必要なデジタル・フォレンジックの知識，特に証拠保全の手順と手法，技術と課題また証拠分析技法の基礎について学ぶ．

[履修条件・受講条件]

特に事前知識は仮定しないが，下記があるとより理解が深まる．

- コンピュータアーキテクチャ
- プログラミング言語
- ネットワークプロトコル

[授業外における学習]

演習課題(教育システムで提示)

テキストの予習及び演習課題(教育システムで提示)

テキストの予習(教育システムで提示)

[参考文献]

菊池浩明，上原哲太郎「IT TEXT ネットワークセキュリティ」，オーム社

佐々木良一ほか「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