情報セキュリティプロ人材育成
短期 集中プログラム［ProSec］

ProSec × 大阪大学 OSAKA UNIVERSITY

安全なデータ利活用のための
プロフェッショナル人材育成コース

― コース案内 ―

大阪大学大学院工学研究科
宮地研究室

Brush up Program
for professional

情報セキュリティプロ人材育成 短期 集中プログラム（ProSec）

安全なデータ利活用のための
プロフェッショナル人材育成コース

— コース案内 —

大阪大学大学院 工学研究科
宮地研究室

はじめに

情報セキュリティは，技術部門の問題ではなく，今や，情報セキュリティガバナンスという用語にみられるように組織全体で取り組むものです．一方，ビットコインにみられるように，情報セキュリティ技術は経済活動にも大きな影響を与えます．

様々な業務で情報利活用が必要となる社会人を対象として立ち上げた「情報セキュリティプロ人材育成短期集中プログラム（ProSec）」では，データを利活用するために必要なサイバーセキュリティ，リスクマネジメント，法制度，暗号技術の応用，ビットコイン・ブロックチェーン・IoTなどの最新技術から，実務を支える理論として数学，アルゴリズム，暗号理論などのセキュリティの基盤技術までを幅広くカバーしており，社会システムにセキュリティ技術を安全に適用できる知識の獲得と現場知識の涵養を目指します．

なお，講義は遠隔配信に加えてビデオによる視聴も可能です．場所や時間の制約を超えて，ご希望の場所と時間での受講が可能です．土日に開催される課題解決型演習（PBL）では，社会人と大学院生から構成されるグループで協力し，課題解決に臨みます．セキュリティソリューションの習得に加えて，コミュニケーション力，ダイバーシティ力，協働力，プロジェクト実行力の向上も目指すことができます．

本プログラムは，「職業実践力育成プログラム（BP）」として認定されています．

「職業実践力育成プログラム（BP）」とは，大学・大学院・短期大学・高等専門学校におけるプログラムの受講を通じた社会人の職業に必要な能力の向上を図る機会の拡大を目的として，大学等における社会人や企業等のニーズに応じた実践的・専門的なプログラムとして文部科学大臣が認定するものです．

また，本プログラム修了者には，大阪大学より科目等履修生高度プログラムの修了認定及び，文部科学省「Society5.0 に対応した高度技術人材育成事業」に選定された「情報セキュリティプロ人材育成短期集中プログラム（ProSec）」における取得単位に応じたコース修了の認定書が授与されます．

Brush up Program
for professional

コース長

宮　地　充　子（大阪大学）

情報セキュリティはソーシャルな問題を解決する学問であり，その対象はサイバー攻撃に見られるように日々手法が強度化され, 更新されます．一方, 情報セキュリティは離散数学, 確率統計, 計算量理論, 情報理論などを学問的基盤とし，学際的･包括的に構成される総合科学です．このような，情報セキュリティの学際的な特徴を鑑みて，日々対象が変わる環境においても常に最新の情報セキュリティに携わる人材の育成には，現在の課題を対象としたアドホック的な教育は不十分です．

つまり，離散数学，確率統計，計算量理論，情報理論という基盤理論の確固たる知識の習得に加えて，それらの基盤理論を道具として活用し，新たな攻撃のモデル化，防御手法，新規の暗号構築ができる力を教育することが重要です．理論習得に加えて，ソーシャルな課題を対象とした実装を組み合わせたバランスの取れた教育の構築が重要である．実際，理論研究と実験や実装の両者は密接に関係しており，理論結果を実験あるいは実装することで理論の理解を深め，周辺知識の習得ができるし，逆に新たな問題を発見し，その問題を理論にフィードバックすることで新しい理論が生まれる可能性もあります．

本コースはそのような考えで構成されました．セキュリティのみならず，問題発見能力，解決能力など考える力を育成するコースです．また，世代，職業を超えた人たちが同窓生になることで，その力はより強く育成されると思います．

[経歴]

1990年 パナソニック株式会社入社.
1998年 北陸先端科学技術大学院大学 准教授.
2002-2003年 カリフォルニア大学デービス校 客員研究員.
2007-現在 北陸先端科学技術大学院大学 教授.
2008-2012年 同附属図書館長.
2015-現在 大阪大学大学院 教授.
2016-現在 独立行政法人 情報処理推進機構 監事.

[受賞歴]

- 平成4年度 SCIS93若手論文賞.
- 平成9年度 科学技術庁注目発明賞.
- 平成13年度 坂井記念特別賞（情報処理学会）.
- 平成14年度 標準化貢献賞（情報処理学会）.
- 平成17年度 功労感謝状（電子情報通信学会）.
- 平成18年度 情報セキュリティ文化賞.
- 平成19-22，24，28，30年度　国際規格開発賞（情報処理学会）.
- 平成19年度 国際標準化奨励者表彰（産業技術環境局長表彰）.
- 平成19年度 編集活動感謝状（電子情報通信学会）
- 平成20年度 ドコモ・モバイル・サイエンス賞.
- The 6th International Conference on Advanced Data Mining and Applications（ADMA 2010）最優秀論文賞.
- 平成24年度 基礎・境界ソサイエティ功労賞（電子情報通信学会）.
- 平成26年度 科学技術分野の文部科学大臣表彰科学技術賞.
- International Conference on Applications and Technologies in Information Security（ATIS 2016）最優秀論文賞.
- 平成29年度 電子情報通信学会マイルストーン認定証.
- The 16th IEEE International Conference on Trust，Security and Privacy in Computing and Communications（TrustCom 2017）最優秀論文賞.
- The 14th Asia Joint Conference on Information Security（AsiaJCIS2019）最優秀論文賞.
- Information Security Applications - 20th International Conference（WISA）（WISA 2020）Best Paper Gold Award.
- 令和2年度　日本ソフトウェア科学会　第7回実践的IT教育シンポジウムrePiT2021最優秀論文賞.

目　次

1. スケジュール

○申込期間

◆春～夏学期に開講される科目（通年科目を含む）

2月

◆秋～冬学期に開講される科目（通年科目を含む）

7月

○出願受付期間

◆春～夏学期に開講される科目（通年科目を含む）

内諾許可後～2月末

◆秋～冬学期に開講される科目（通年科目を含む）

内諾許可後～7月末

○入学手続期間

◆春～夏学期に開講される科目（通年科目を含む）

3月上旬

◆秋～冬学期に開講される科目（通年科目を含む）

9月下旬

講義時間

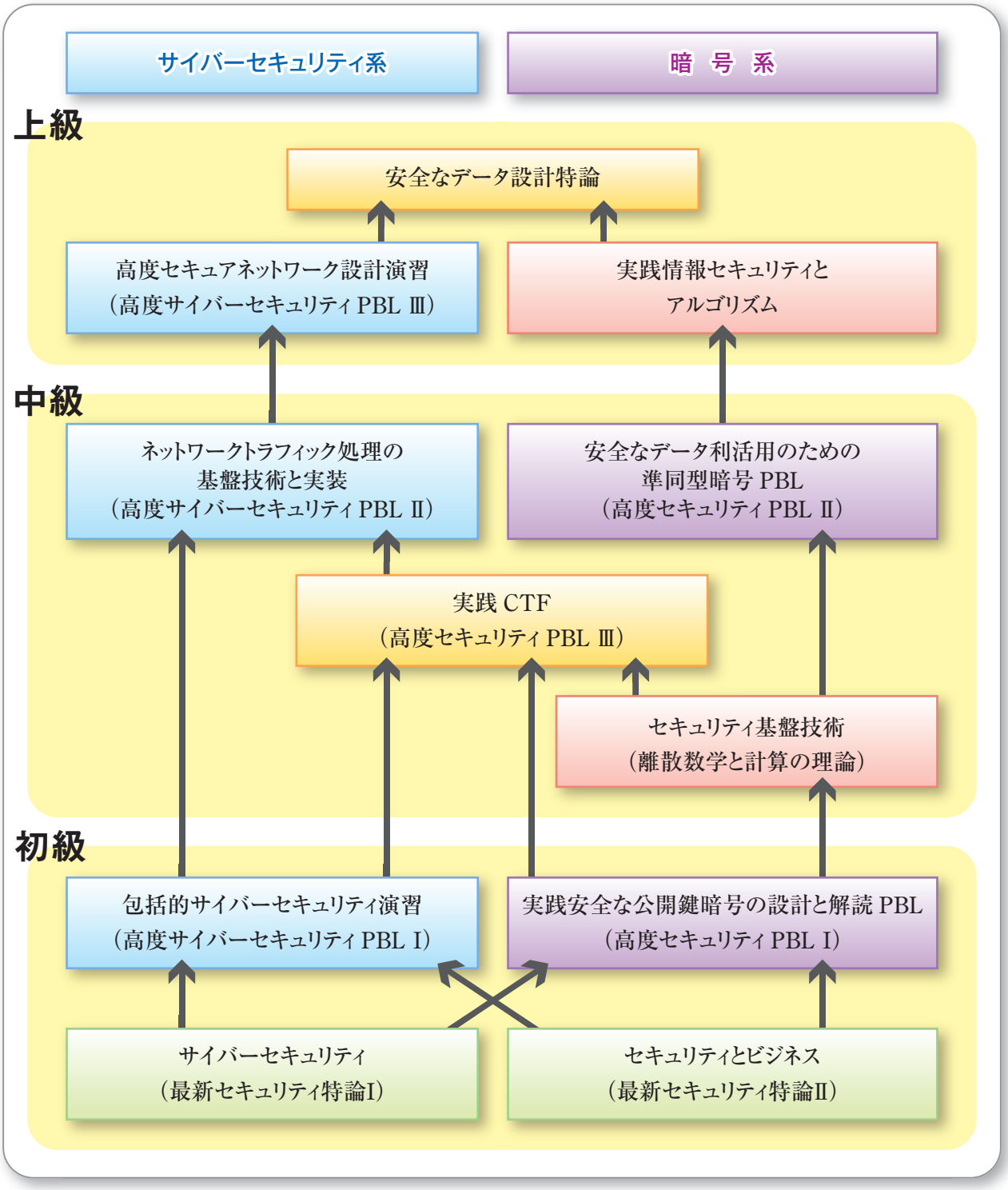
第1時限　8:50 ～ 10:20　第2時限 10:30 ～ 12:00　第3時限 13:30 ～ 15:00

第4時限 15:10 ～ 16:40　第5時限 16:50 ～ 18:20　第6時限 18:30 ～ 20:00

2. 各講義の関係

各講義の関連は次のようになります．矢印に沿って受講することが望ましいですが，各受講者の知識に応じて選択してください．

表1. 各講義の関連図



オプション科目

情報ネットワーク経済学

3. 各講義の知識マップ

各講義, 演習で習得される知識となります. 受講の判断にご利用ください.

表2. 知識マップ

	導　入			発　展
サイバーセキュリティ	・ISMS ・ソフトウェア脆弱性	・リスクアセスメント ・Web アプリケーション脆弱性	・CSIRT ・ログ監査	・ディザスタリカバリ ・メモリフォレンジック
セキュリティとビジネス	・IoT 市場の概要 ・暗号危殆化 ・国際標準の役割 ・不正競争防止法	・製造・開発・運用の実態 ・OAuth 認証 ・不正アクセス禁止法	・ブロックチェーン技術 ・仮想通貨 ・個人情報保護法	・IoT 業界将来の可能性やリスク ・ICO ・EU のデータ保護指令 ・アメリカの経済スパイ法
セキュリティ基盤技術（離散数学）	・整数 ・最大公約数	・ユークリッドの互除法 ・中国人の剰余定理	・初等整数論	・群・環・有限体
セキュリティ基盤技術（計算の理論）	・命題論理	・一階述語論理 ・形式的証明	・停止問題 ・チューリングマシンとλ計算	・不完全性定理 ・型システム
実践情報セキュリティ	・暗号用数学	・公開鍵暗号 ・ディジタル署名	・暗号の実装方法	・ハイブリッド暗号（TLS）
実践アルゴリズム	・型付きλ計算	・線形型システム	・エフェクト型システム ・リージョン推論	・形式手法 ・モデル検査
実践安全な公開鍵暗号の設計と解読 PBL	・2 進法 ・逆元演算	・べき乗演算の実装	・公開鍵暗号 ・ElGamal 暗号	・解読
安全なデータ利活用のための準同型暗号 PBL	・整数 ・モジュラー演算	・準同型暗号（理論）	・準同型暗号（実装）	・解読 ・電子投票
実践 CTF	・ファイルの分別	・XSS	・コマンドインジェクション ・Web 脆弱性	・リバースエンジニアリング
包括的サイバーセキュリティ演習	・コンピュータネットワーク ・UNIX	・パケットフィルタ ・ファイアウォール ・異常検知 ・検疫ネットワーク		
ネットワークトラフィック処理の基盤技術と実装		・抽象レジスタマシンの実装 ・パケットフィルタ ・カーネルバイパス技術	・バイトコードインタプリタ ・レジスタマシン ・オートマトン ・正規表現	・パケットフィルタ
高度セキュアネットワーク設計演習			・コンピュータネットワーク	・多層防御 ・セキュリティアプライアンス ・ファイアウォール ・NFV
安全なデータ設計特論			・セキュリティの課題発見	・セキュアシステム設計

4. 受講者タイプ別推奨講義プラン

受講者を5タイプに分類し，各タイプのモデル受講プランを記載します．各タイプの説明や時間数は表3の後に記載しています．

表3. モデル受講プラン

	講義（配信有） 演習	単位数	管理職 ユーザー系	教育関係者	開発系	学びなおし	セキュリティ 技術者
サイバー セキュリティ	講義（配信有）	1	✔	✔	✔	✔	✔
セキュリティと ビジネス		1	✔	✔	✔	✔	✔
セキュリティ 基盤技術 （離散数学）	講義（配信有）	2		✔		✔	✔
セキュリティ 基盤技術 （計算の理論）				✔		✔	✔
実践情報 セキュリティ	講義（配信有）	2		✔	✔	✔	✔
実践 アルゴリズム				✔	✔	✔	✔
実践安全な 公開鍵暗号の 設計と解読 PBL	演習	1	✔	✔	✔	✔	✔
安全なデータ 利活用のための 準同型暗号 PBL	演習	1			✔		✔
実践 CTF	演習	1	✔	✔	✔	✔	✔
包括的 サイバー セキュリティ演習	演習	1	✔	✔	✔	✔	✔
ネットワーク トラフィック処理の 基盤技術と実装	演習	1			✔	✔	✔
高度セキュア ネットワーク 設計演習	演習	1					✔
安全なデータ 設計特論	演習	1		✔	✔	✔	✔

受講者のタイプ別プランをご紹介します．受講する講義を決定いただく際の参考にしてください．

① ユーザー系及び管理職

学部卒以上と同等の知識を有する方を想定しています．

講義はサイバーセキュリティ（90分×8回），セキュリティとビジネス（90分×6回）の座学講義があります．なお，これら90分×14回の講義は遠隔配信，講義録画を行いますので，自宅・職場での受講が可能です．

演習は実践安全な公開鍵暗号の設計と解読PBL（2日），実践CTF（2日），包括的サイバーセキュリティ演習（2日）の合計6日の課題解決型演習があります．

修得単位数は5単位です．

講義の選択例

春入学

1年目（2単位）

・サイバーセキュリティ（1単位）（春～夏学期）

・実践安全な公開鍵暗号の設計と解読PBL（1単位）（夏学期）（集中）

2年目（3単位）

・包括的サイバーセキュリティ演習（1単位）（春～夏学期）（集中）

・セキュリティとビジネス（1単位）（秋～冬学期）

・実践CTF（1単位）（秋～冬学期，集中）

秋入学

1年目（2単位）

・セキュリティとビジネス（1単位）（秋～冬学期）

・実践CTF（1単位）（秋～冬学期，集中）

2年目（3単位）

・サイバーセキュリティ（1単位）（春～夏学期）

・包括的サイバーセキュリティ演習（1単位）（春～夏学期）（集中）

・実践安全な公開鍵暗号の設計と解読PBL（1単位）（夏学期，集中）

② 教育関係者

学部卒以上と同等の知識を有し，情報系あるいは数学系の教育に携わる方を想定しています.

講義はセキュリティ基盤技術 (90分×16回), 実践情報セキュリティとアルゴリズム (90分×16回), サイバーセキュリティ (90分×8回)，セキュリティとビジネス（90分×6回）の座学講義があります. なお，これら90分×46回の講義は遠隔配信，講義録画を行いますので，自宅・職場での受講が可能です.

演習は実践安全な公開鍵暗号の設計と解読PBL（2日），実践CTF（2日）包括的サイバーセキュリティ演習（2日）の合計6日の課題解決型演習があります.

修得単位数は9単位です.

講義の選択例

春入学

1年目（4単位）

・包括的サイバーセキュリティ演習（1単位）（春～夏学期）（集中）
・実践安全な公開鍵暗号の設計と解読PBL（1単位）（夏学期）（集中）
・実践情報セキュリティとアルゴリズム（2単位）（秋～冬学期）

2年目（5単位）

・サイバーセキュリティ (1単位)（春～夏学期）
・セキュリティ基盤技術（2単位）（春～夏学期）
・セキュリティとビジネス（1単位）（秋～冬学期）
・実践CTF（1単位）（秋～冬学期）（集中）

秋入学

1年目（3単位）

・セキュリティとビジネス（1単位）（秋～冬学期）
・実践情報セキュリティとアルゴリズム（2単位）（秋～冬学期）

2年目（6単位）

・実践CTF（1単位）（秋～冬学期，集中）
・サイバーセキュリティ (1単位)（春～夏学期）
・セキュリティ基盤技術（2単位）（春～夏学期）
・包括的サイバーセキュリティ演習（1単位）（春～夏学期）（集中）
・実践安全な公開鍵暗号の設計と解読PBL（1単位）（夏学期）（集中）

③ 開発系

理系学部卒以上と同等の知識を有し，システムあるいはソフトウェアの開発に携わる方を想定しています.

講義は実践情報セキュリティとアルゴリズム（90分×16回），サイバーセキュリティ(90分×8回)，セキュリティとビジネス（90分×6回）の座学講義があります．なお，これら90分×30回の講義は遠隔配信，講義録画を行いますので，自宅・職場での受講が可能です.

演習は実践安全な公開鍵暗号の設計と解読PBL（2日），安全なデータ利活用のための準同型暗号PBL（2日），実践CTF（2日），包括的サイバーセキュリティ演習（2日），ネットワークトラフィック処理の基盤技術と実装（2日）の合計10日の課題解決型演習があります.

修得単位数は9単位です.

講義の選択例

春入学

1年目（5単位）

・包括的サイバーセキュリティ演習（1単位）（春～夏学期）（集中）
・サイバーセキュリティ(1単位)（春～夏学期）
・実践安全な公開鍵暗号の設計と解読PBL（1単位）（夏学期）（集中）
・実践情報セキュリティとアルゴリズム（2単位）（秋～冬学期）

2年目（4単位）

・セキュリティとビジネス（1単位）（秋～冬学期）
・安全なデータ利活用のための準同型暗号PBL（1単位）（秋～冬学期）（集中）
・実践CTF（1単位）（秋～冬学期，集中）
・ネットワークトラフィック処理の基盤技術と実装（1単位）（春～夏学期）（集中）

秋入学

1年目（4単位）

・セキュリティとビジネス（1単位）（秋～冬学期）
・実践情報セキュリティとアルゴリズム（2単位）（秋～冬学期）
・実践CTF（1単位）（秋～冬学期）（集中）

2年目（5単位）

・実践安全な公開鍵暗号の設計と解読PBL（1単位）（夏学期）（集中）
・サイバーセキュリティ(1単位)（春～夏学期）
・安全なデータ利活用のための準同型暗号PBL（1単位）（秋～冬学期）（集中）
・包括的サイバーセキュリティ演習（1単位）（春～夏学期）（集中）
・ネットワークトラフィック処理の基盤技術と実装（1単位）（春～夏学期）（集中）

④ 学びなおし

学部卒以上と同等の知識を有し，セキュリティの基礎から応用まで幅広く学びたい方を想定しています.

講義はセキュリティ基盤技術（90分×16回），実践情報セキュリティとアルゴリズム（90分×16回），サイバーセキュリティ（90分×8回），セキュリティとビジネス（90分×6回）の座学講義があります. なお，これら90分×46回の講義は遠隔配信，講義録画を行いますので，自宅・職場での受講が可能です.

演習は実践安全な公開鍵暗号の設計と解読PBL（2日），実践CTF（2日），包括的サイバーセキュリティ演習（2日），高度セキュアネットワーク設計演習（2日）の合計8日の課題解決型演習があります.

修得単位数は10単位です.

講義の選択例

春入学

1年目（5単位）

・包括的サイバーセキュリティ演習（1単位）（春～夏学期）（集中）
・実践安全な公開鍵暗号の設計と解読PBL（1単位）（夏学期，集中）
・実践情報セキュリティとアルゴリズム（2単位）（秋～冬学期）
・セキュリティとビジネス（1単位）（秋～冬学期）

2年目（5単位）

・サイバーセキュリティ（1単位）（春～夏学期）
・セキュリティ基盤技術（2単位）（春～夏学期）
・実践CTF（1単位）（秋～冬学期，集中）
・高度セキュアネットワーク設計演習（1単位）（秋～冬学期）（集中）

秋入学

1年目（4単位）

・実践情報セキュリティとアルゴリズム（2単位）（秋～冬学期）
・セキュリティとビジネス（1単位）（秋～冬学期）
・実践CTF（1単位）（秋～冬学期，集中）

2年目（4単位）

・高度セキュアネットワーク設計演習（1単位）（秋～冬学期）（集中）
・サイバーセキュリティ（1単位）（春～夏学期）
・包括的サイバーセキュリティ演習（1単位）（春～夏学期）（集中）
・実践安全な公開鍵暗号の設計と解読PBL（1単位）（夏学期，集中）

3年目（2単位）

・セキュリティ基盤技術（2単位）（春～夏学期）

⑤ セキュリティ技術者

理系学部（情報系）卒以上と同等の知識を有し，セキュリティあるいはデータ利活用の業務に携わる方を想定しています.

講義はセキュリティ基盤技術（90分×16回），実践情報セキュリティとアルゴリズム（90分×16回），サイバーセキュリティ（90分×7回），セキュリティとビジネス（90分×6回）の座学講義があります. なお，これら90分×45回の講義は遠隔配信，講義録画を行いますので，自宅・職場での受講が可能です.

演習は実践安全な公開鍵暗号の設計と解読PBL（2日），安全なデータ利活用のための準同型暗号PBL（2日），実践CTF（2日），包括的サイバーセキュリティ演習（2日），ネットワークトラフィック処理の基盤技術と実装（2日），高度セキュアネットワーク設計演習（2日）の合計12日の課題解決型演習があります.

修得単位数は12単位です.

講義の選択例

春入学

1年目（5単位）

- 包括的サイバーセキュリティ演習（1単位）（春～夏学期）（集中）
- 実践安全な公開鍵暗号の設計と解読PBL（1単位）（夏学期，集中）
- 実践情報セキュリティとアルゴリズム（2単位）（秋～冬学期）
- セキュリティとビジネス（1単位）（秋～冬学期）

2年目（7単位）

- セキュリティ基盤技術（2単位）（春～夏学期）
- サイバーセキュリティ（1単位）（春～夏学期）
- 実践CTF（1単位）（秋～冬学期，集中）
- 高度セキュアネットワーク設計演習（1単位）（秋～冬学期）（集中）
- 安全なデータ利活用のための準同型暗号PBL（1単位）（秋～冬学期，集中）
- ネットワークトラフィック処理の基盤技術と実装（1単位）（春～夏学期）（集中）

秋入学

1年目（3単位）

- 実践情報セキュリティとアルゴリズム（2単位）（秋～冬学期）
- セキュリティとビジネス（1単位）（秋～冬学期）

2年目（6単位）

- サイバーセキュリティ（1単位）（春～夏学期）
- 実践CTF（1単位）（秋～冬学期，集中）
- 包括的サイバーセキュリティ演習（1単位）（春～夏学期）（集中）
- 実践安全な公開鍵暗号の設計と解読PBL（1単位）（夏学期，集中）
- 高度セキュアネットワーク設計演習（1単位）（秋～冬学期）（集中）
- ネットワークトラフィック処理の基盤技術と実装（1単位）（春～夏学期）（集中）

3年目（3単位）

- セキュリティ基盤技術（2単位）（春～夏学期）
- 安全なデータ利活用のための準同型暗号PBL（1単位）（秋～冬学期，集中）

5. 各コース

各講義・演習の受講パターンとコース名をご紹介します.

科目名＼コース名	メインコース（8 単位以上）			クイックコース（5 単位以上）				
	セキュリティ	暗号	サイバー	セキュリティ	暗号	サイバー	暗号実践	実践サイバー・セキュリティ・
最新セキュリティ特論 I, II	必修	必修	必修	必修		必修	選択 D	選択 D
離散数学と計算の理論	選択 A	必修	選択 A		必修		選択 A	
実践情報セキュリティとアルゴリズム	選択 A	必修	選択 A		必修		選択 A	
高度セキュリティ PBL I	選択 B	選択 B		必修	選択 B		選択 E	選択 F
高度セキュリティ PBL II	選択 B	選択 B			選択 B		選択 E	選択 F
高度セキュリティ PBL III	必修	選択 B	必修	必修			選択 E	選択 F
高度サイバーセキュリティ PBL I	選択 C		必修	必修		必修	選択 E	選択 F
高度サイバーセキュリティ PBL II	選択 C		必修			必修	選択 E	選択 F
高度サイバーセキュリティ PBL III	選択 C		必修			必修	選択 E	選択 F
安全なデータ設計特論	選択 G			選択 G			選択 G	

【必修】必修科目

【選択A】講義科目から選択（2単位以上選択）

【選択B】高度セキュリティ PBL科目から選択（1単位以上選択）

【選択C】高度サイバーセキュリティ PBL科目から選択（1単位以上選択）

【選択D】講義科目から選択（1単位以上選択）

【選択E】PBL科目から選択（3単位以上選択）

【選択F】PBL科目から選択（4単位以上選択）

【選択G】履修条件：クイックコースを1コース以上修了していること

※ 選択Gの単位取得済みかつコースを修了した場合，各コースのアドバンスドの修了となる.

例：暗号メインコース+選択G→アドバンスド暗号メインコース

6. 教員紹介

高野 祐輝（大阪大学）

2011年3月 北陸先端科学技術大学院大学 情報科学研究科 博士後期課程修了. 博士（情報科学）.

2011年4月～2012年3月に北陸先端科学技術大学院大学
高信頼ネットワークイノベーションセンターにて研究員を務め，堅牢なネットワークシステムの研究に従事．2012年4月～2018年9月，情報通信研究機構にてサイバーセキュリティ関連の研究開発に従事．2018年10月より大阪大学にて特任講師，2019年8月より特任准教授.

[受賞歴]

- 2005年3月，平成16年度優秀学生賞 受賞，情報処理学会北陸支部.
- 2013年，インターネットコンファレンス 2013 論文賞 受賞.
- 2014年，WIDE Project 2014年春のWIDE研究会 ポスター賞 受賞.
- 2014年，Interop Tokyo 2014，Best of Show Award，ShowNet デモンストレーション部門 審査員特別賞 受賞，“インタラクティブな無線メッシュネットワーク計画”.
- 2015年，Interop Tokyo 2015，Best of Show Award，ShowNet デモンストレーション部門 審査員特別賞 受賞，“CHAKRA: ソフトウェアベースL7解析器によるビッグデータビジュアライゼーション”.
- 2016年，Interop Tokyo 2015，Best of Show Award，サイエンス部門 グランプリ 受賞，“SF-TAP: Scalable and Flexible Traffic Analysis Platform”，2015・DICOMO.
- 2016年，野口賞技術賞，“次世代サイバー演習環境に向けて”.
- 2017年，MWS 2017 ベストプラクティカル研究賞 受賞，“サイバー攻撃誘引基盤STARDUST”.
- 2018年，情報通信研究機構，成績優秀賞 受賞.

奥村 伸也（大阪大学）

2015年 九州大学大学院数理学府数理学専攻博士後期課程修了. 博士(数理学). 九州大学マス・フォア・インダストリアル研究所 学術研究員,（公財）九州先端科学技術研究所情報セキュリティ研究室 研究員，大阪大学 大学院工学研究科特任助教を経て，現在2018年より大阪大学 大学院工学研究科 助教．主な研究分野は耐量子暗号，数論アルゴリズム.

[受賞歴]

- 2016年，CANDAR 2016，Outstanding Paper Award.
- 2016年，電子情報通信学会基礎・境界ソサイエティ 2016年度 情報セキュリティ研究奨励賞.
- 2016年，日本応用数理学会 2016年度若手優秀講演賞.

明石 邦夫（東京大学）

2017年9月 北陸先端科学技術大学院大学 情報科学研究科 博士後期課程修了．博士（情報科学）．東京大学 情報理工学系研究科 情報理工学教育研究センター助教．

2013年より Interop Tokyo にて ShowNet NOC チームメンバーとして参加し，イベントネットワークの構築を行う．2017年10月より国立研究開発法人 情報通信研究機構 オープンイノベーション推進本部 ソーシャルイノベーションユニット 総合 テストベッド研究開発推進センター研究員，2021年4月より現職．データセンタネットワーク，ストレージの研究に従事．

[受賞歴]

- 2015年，Interop Tokyo 2015，Best of Show Award，ShowNet デモンストレーション部門 審査員特別賞 受賞，“CHAKRA: ソフトウェアベースL7解析器によるビッグデータビジュアライゼーション”．
- 2015年，Interop Tokyo 2015，Best of Show Award，サイエンス部門 グランプリ 受賞，“SF-TAP: Scalable and Flexible Traffic Analysis Platform”．
- 2018年，Interop Tokyo 2018，Best of Show Award，デモ部門 グランプリ 受賞，“JAIan: Syslog，xFlow 配信/記録システム”．

新井 悠（株式会社エヌ・ティ・ティ・データ）

2000年に情報セキュリティ業界に飛び込み，株式会社ラックにてSOC事業の立ち上げやアメリカ事務所勤務等を経験．その後情報セキュリティの研究者としてWindowsやInternet Explorerといった著名なソフトウェアに数々の脆弱性を発見する．ネットワークワームの跳梁跋扈という時代の変化から研究対象をマルウェアへ照準を移行させ，著作や研究成果を発表した．よりマルウェア対策に特化した仕事をしたいという想いから2013年8月にトレンドマイクロ株式会社に活躍の場を移す．平成29年度より大阪大学非常勤講師．CISSP．

[著書]

- アナライジング・マルウェア ―フリーツールを使った感染事案対処（Art Of Reversing）（著）新井 悠，岩村 誠
- ソフトウェアの匠Ⅱ（著）新井 悠，飯田 貴光
- ネットワーク攻撃詳解―攻撃のメカニズムから理解するセキュリティ対策
  （著）三輪 信雄，新井 悠

猪俣 敦夫（大阪大学）

北陸先端大（JAIST）情報科学研究科博士後期課程修了．博士（情報科学）．独立行政法人科学技術振興機構（JST），奈良先端科学技術大学院大学（NAIST）准教授，を経て，現在，東京電機大学教授，大阪大学特任教授，一般社団法人公衆無線LAN認証管理機構代表理事，一般社団法人JPCERTコーディネーションセンター理事，奈良県警サイバーセキュリティ対策アドバイザー他．専門は暗号の高速実装に関する研究開発のほか，IPAセキュリティキャンプ全国大会講師，NICT CYDER，SecHack365実行委員等，若手情報セキュリティ人材育成に努める．

[受賞歴]

− 2014年，(ISC)^2 Asia-Pacific Information Security Leadership Achievement 受賞．

[著書]

− サイバーセキュリティ入門 私たちを取り巻く光と闇（共立出版），（著）猪俣 敦夫 等

岩佐 琢磨（株式会社Shiftall）

1978年生まれ，立命館大学大学院理工学研究科修了．2003年からパナソニックにてネット接続型家電の商品企画に従事．2008年より，ネットワーク接続型家電の開発・販売を行なう株式会社Cerevoを立ち上げ，20種を超える自社開発IoT製品を世界70の国と地域に届けた．2018年にハードウェアを開発・製造・販売するCerevoの子会社として設立した株式会社Shiftallの代表取締役CEOに就任，4月2日付けでパナソニック株式会社の買収によってパナソニックのグループ会社として事業を開始．パナソニックが「くらしの統合プラットフォーム」として掲げる「HomeX」対応のタッチポイント機器第1弾となる「HomeX Display」の開発・製造や，パナソニックのデザインスタジオ「FUTURE LIFE FACTORY」が企画・デザインしたウェアラブル端末「WEAR SPACE」のクラウドファンディングおよび量産時の設計・製造・販売を担当．WEAR SPACEは1，500万円というクラウドファンディングとしては高額の目標を達成し，量産が決定した．2019年1月にラスベガスで開催される世界最大の家電見本市「CES2019」では，Shiftall独自ブランドの新製品を発表．

岩下 直行（京都大学）

1984年3月，慶應義塾大学経済学部卒業. 同年4月，日本銀行入行. 1994年7月，日本銀行金融研究所に異動し，以後約15年間，金融分野における情報セキュリティ技術の研究に従事．同研究所・情報技術研究センター長，下関支店長を経て，2011年7月，日立製作所に出向．2013年7月，日本銀行決済機構局参事役．2014年5月，同金融機構局審議役･金融高度化センター長．2016年4月，新設されたFinTechセンターの初代センター長に就任．2017年3月，日本銀行退職．同年4月，京都大学・公共政策大学院の教授に就任．同年6月，PwCあらた有限責任監査法人のスペシャルアドバイザー兼務，同年8月，金融庁参与兼務．金融審議会 金融制度スタディ・グループ（2017年～）．仮想通貨交換業等に関する研究会（2018年）に参加．2018年12月より，G20のエンゲージメントグループの一つであるT20（Think20）TF2「国際金融アーキテクチャー」で暗号資産（仮想通貨），FinTech担当のco-chairを務める．

[著書]

－「フィンテックは金融ビジネスを根底から変える」（文芸春秋，2018年3月）
－「ブロックチェーンの未来」（共著，日経新聞社，2017年9月）他

上原 哲太郎（立命館大学）

京都大学博士（工学）．立命館大学情報理工学部教授．京都大学大学院工学研究科助手，和歌山大学システム工学部講師，京都大学大学院工学研究科助教授，同学術情報メディアセンター准教授，総務省通信規格課標準化推進官を経て2013年より現職．現在は，NPOデジタル・フォレンジック研究会（IDF）副会長．和歌山県警察サイバー犯罪対策アドバイザー，京都府警察サイバー犯罪対策テクニカルアドバイザー，京都府警察サイバーセキュリティ戦略アドバイザー，滋賀県警察サイバーセキュリティ対策委員会アドバイザー．芦屋市最高情報統括責任者（CIO）補佐官を兼務．専門は情報セキュリティ，デジタル・フォレンジック，情報倫理教育，自治体情報システム．

[受賞歴]

－ 2015年，第11回情報セキュリティ文化賞.
－ 平成30年度，情報通信功績賞（総務省情報通信月間推進協議会会長表彰）.

[著書]

－ IT Text ネットワークセキュリティ（著）菊池 浩明，上原 哲太郎 オーム社
－ デジタル・フォレンジックの基礎と実践 佐々木 良一 編著，上原 哲太郎，櫻庭 信之，白濱 直哉，野﨑 周作

園田 道夫（情報通信研究機構）

中央大学大学院理工学研究科博士（工学）課程修了.
2004年より経済産業省，JIPDEC，IPA主催セキュリティキャンプに企画，講師，実行委員として携わる．2007年より白浜サイバー犯罪シンポジウム危機管理コンテスト審査委員，2012年よりSECCON実行委員（事務局長），2016年より国立研究開発法人情報通信研究機構セキュリティ人材育成研究センター長（2017年よりナショナルサイバートレーニングセンター長）.

[受賞歴]

- 2008年，経済産業省商務情報政局長表彰.
- 2012年,（ISC）2（R）第6回年次アジア・パシフィック情報セキュリティ・リーダーシップ・アチーブメント・プログラムにてSenior Information Security Professionalとして表彰.
- 2018年，情報セキュリティ文化賞表彰.

[著書]

- Winnyはなぜ破られたのか―P2Pネットワークをめぐる攻防,（著）園田 道夫
- ぼくのパソコンを守って,（著）根津 研介，宮本 久仁男，園田 道夫，武礼堂

苗村 博子（苗村法律事務所）

大阪大学法学部卒業，シカゴ大学ロースクール（LL.M.）卒業.
大江橋法律事務所勤務を経て，苗村法律事務所開設.
弁護士，弁護士法人苗村法律事務所 代表社員.

[著書]

- 企業活動における知的財産（共著，大阪大学出版会）
- 新・注解　不正競争防止法【新版】上下巻（共著，青林書院）　他

[主な活動]

－著作権法学会理事

[主な業務分野]

－国際取引に関する相談業務
－知的財産権に関する相談業務及び訴訟担当
－企業の経済犯罪についての対応（国際的なものも含む，反トラスト法，FCPA等捜査対応）
2018年9月に，フラダンスの振り付けに著作権を認めるとの判決を得る.

満永 拓郎（東洋大学）

京都大学大学院情報学研究科博士後期課程修了．博士（情報学）．
東洋大学情報連携学部准教授．独立行政法人情報処理推進機構産業サイバーセキュリティセンター専門委員．
民間企業，JPCERT/CC，東京大学情報学環での勤務を経て現職．サイバー攻撃防御手法の研究やセキュリティ人材育成，AI・DX（デジタルトランスフォーメーション）などの調査研究を行っている．

［著書］

- 制御システムセキュリティ入門 : Society 5.0/Industry 4.0時代に向けて社会インフラをいかに守るか（共著，NTT出版）
- はじめて学ぶバイナリ解析（共著，インプレスR&D）

7. 講義のシラバス

7.1 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] 春～夏学期

[担当教員]

猪俣 敦夫（大阪大学），上原 哲太郎（立命館大学），満永 拓邦（東洋大学），宮地 充子（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，その具体例として組織におけるCSIRT運用を取り上げる．

[学習目標]

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を目標とする．

[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

[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/IEC27001:2013（JIS Q 27001:2014）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．ISMS運用のための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を行う．

第2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．

[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/IEC27001

[準備学習等の具体的な指示]

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2019：IPA 独立行政法人 情報処理推進機構

[成績評価] レポートによる

[評価の観点] 教科書的知識のみならず自身の考え方がきちんと述べられていることをより評価する．

[評価方法] レポート成績

【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．

[学習目標]

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

[準備学習等の具体的な指示]

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

[成績評価] レポートによる

[評価の観点] 教科書的知識のみならず自身の考え方がきちんと述べられていることをより評価する．

[評価方法] レポート成績

【ログ分析・バイナリ解析】（担当：満永 拓邦）

[授業の目的・概要]

セキュリティインシデント発生時には，被害の局所化のために発生原因や影響範囲を調査する必要がある．本講義では技術的な観点から，インシデント発生時に必要な相関的なログ分析の手法や，不正なソフトウエアの挙動を分析する手法について取り上げる．

[学習目標]

相関的なログ分析手法やバイナリ解析を適切に理解し，インシデント発生時の原因調査や影響分析に必要な知識と技術を習得することを目標とする．

[知識単位]

NIST SP800-53，CSIRT，ログ分析，バイナリ解析

[講義計画]

第1回 ログ分析

インシデント発生時には，個別機器のログだけではなく，複数の器機で取得されるログを相関的に分析することにより，巨視的に攻撃手法や被害範囲を把握することができるようになる．この講義では高度なログの分析手法（ツールを用いた相関分析など）を通じて攻撃の痕跡を調査する方法を学ぶ．

- 分析ツールを用いたログの可視化および相関分析演習
- Windowsのイベントログ
- プロキシログ
- ファイアウォールログ
- OSINTを組み合わせたログ分析

第2回 バイナリ解析

コンピュータ上で不正なソフトウエアやマルウエアが実行された場合に，バイナリ解析を用いることで挙動を理解することができます．この講義ではバイナリ解析ついての理解を深め，バッファローオーバフローなどの攻撃の概要や解析手順を学びます．

- バイナリ解析の概要説明
- CPUとメモリの役割
- デバッガを用いたバイナリ分析演習
- 不正なソフトウエアへの対策

[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

[準備学習等の具体的な指示]

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]

はじめて学ぶバイナリ解析 -不正なコードからコンピュータを守るサイバーセキュリティ技術-

[成績評価] ログ分析の評価（50%），バイナリ解析の評価（50%）

[評価方法] 事前課題試験及びレポート成績

[評価基準] 事前課題（10%）及びレポート成績（90%）

7.2 セキュリティとビジネス

[開講科目名]

（授業科目）最新セキュリティ特論Ⅱ／(enPiT-Pro) セキュリティとビジネス

[単位数] 1単位

[開講日] 秋～冬学期

[担当教員]

苗村 博子（苗村法律事務所），岩下 直行（京都大学），岩佐 琢磨（㈱Shiftall），宮地 充子（大阪大学）

【情報の法的価値と法的規制】（担当：苗村博子）

[授業の目的・概要]

データ化された情報は，国境に関係なくやりとりされている．しかし，情報の価値とそれに見合った規制を行う法は，基本的に国や地域という単位で作られており，その国や地域の重視する価値観によってそれぞれに異なっている．日本の法だけにとらわれることなく，世界のトレンドを作り出している欧州連合（EU）のデータ管理や，アメリカでの情報規制にも触れつつ，情報の法的価値を探り，その保護のための規制とその規制に対応する為に普段必要な努力について理解してもらう．

[学習目標]

国境に関係なくやりとりされる情報の価値や規制について，各国の法的違いを学ぶことで，情報のグローバルな取り扱う能力を養成する．

[知識単位]

個人情報保護法，不正競争防止法，不正アクセス禁止法

EUのデータ保護指令，アメリカの経済スパイ法

[講義計画]

第1回 日本における情報に関する法律

個人情報保護法（ビッグデータの取扱の仕方を含む），不正競争防止法（営業秘密に関する部分），不正アクセス禁止法など，日本における情報を取り巻く法の紹介と法令に違反しないために行うべき日常業務での注意点を判例などに事例から学ぶ．

第2回 EU，アメリカにおける情報管理法

EUのデータ保護指令やアメリカの経済スパイ法などを概観し，保護方法の違いや内容を学び，違反した場合の日本に比較すると格段に厳しい法執行の現状について考える．

[履修条件・受講条件]

法律に精通している必要はなく，法律の世界では，正しい答えという考え方はなく，合理性，相当性といった多様な価値観に目配りして，その時々の最もバランスのとれた答えを得るという点を理解いただければよい．

[準備学習等の具体的な指示]

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）

[成績評価]

[評価の観点]

[評価方法] レポート成績

【金融業務における暗号技術の応用と国際標準化】（担当：岩下直行）

[授業の目的・概要]

DES暗号の開発に始まる現代暗号の進化には，金融業界という巨大なユーザーの存在があった．本授業では，1970年代に始まる銀行の巨大情報ネットワーク化と，そこで利用された暗号がムーアの法則に伴う暗号技術の危殆化の経験を経て，どのように進化を遂げたかを述べる．また，そうした技術の一つの応用事例として，仮想通貨とブロックチェーン技術を取り上げる．

[学習目標]

暗号技術がそのユーザーである金融業界とともに進化してきた歴史を学ぶとともに，今後も発生するであろう暗号危殆化に対処していく能力を養成する．また，暗号資産などの新しい応用事例の実態と，その原理を学ぶ．

[知識単位]

暗号危殆化，国際標準の役割，OAuth認証，ブロックチェーン技術，暗号資産，ICO，STO

[講義計画]

第1回 金融業務における暗号技術の応用の経緯

DES暗号の開発と金融業界における応用事例，国際標準との関わり

DES暗号の危殆化と金融業界の対応，3DESとAESの標準化

2010年，2回目の暗号危機と金融業界の対応

FinTechの発展と金融オープンAPIを巡る議論

第2回 ビットコインと暗号技術

ビットコインの誕生前史，ブロックチェーン技術の原理と課題

ビットコインがもたらしたもの，暗号資産ブームと相場急騰の背景

ブロックチェーン技術，DLTとその応用事例

ICO，STOを巡る動きと各国規制当局の動向

[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．

− 共通鍵暗号・公開鍵暗号に関する基礎的な知識

− 暗号的ハッシュ関数に関する基礎的な知識

[準備学習等の具体的な指示]

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]

1. 今井秀樹,『暗号のおはなし』，日本規格協会，2003年

2. ドン＆アレックス・タプスコット,『ブロックチェーン・レボリューション』，ダイヤモンド社，2016年

[成績評価] 授業時間内に理解度テストを実施．

[評価の観点] 授業への積極的な参加，および講義内容の正確な理解．

[評価方法] 質問等による授業への積極的な参加，および授業時間内に実施する理解度テスト．やむを得ない理由で理解度テストに参加できなかった者にはレポート課題等の救済措置を講じる．

【IoT先端技術とその展開】（担当：岩佐琢磨）

[授業の目的・概要]

IoTなどとも呼ばれる最先端のネット連携型家電製品や家庭用ロボット等.

これらをリードしているスタートアップ企業はなぜ少ない資金や人員で未だ世の中にないハードウェアを設計・製造できるのか．IoTを支えるソフトウェアだけでなくハードウェア技術の潮流にも触れながら，日本以外の国におけるトレンドを含めて学ぶ.

[学習目標]

IoTを構成するハードウェア的，ソフトウェア的な技術要素を理解し，これらがどのようにして最終製品として仕立て上げられるかのプロセスを理解する．また，ハードウェアスタートアップを取り巻く周辺環境について技術的側面のみならず，資金的側面や市場全体のなかでの必要性などについて理解することを目標とする.

[知識単位]

モジュール化，オープンソース，製造方法，オープンイノベーション，HaaS，スタートアップ

[講義計画]

第1回 IoT家電を構成する技術要素と製造プロセス

前半では過去20年ほどに遡り，IoTや家庭用ロボットをとりまく技術トレンドがどのように移り変わってきたのかを学ぶ．各技術の詳細を解説しつつ進める.

後半ではこういった機器はどのようにして製造されているのかを学ぶ.

第2回 家電スタートアップを取り巻くさまざまな情勢

世界各国の家電スタートアップの状況や，部品メーカーの姿勢，ベンチャーキャピタルやエンジェルの存在，オープンイノベーションの動向などを取り上げ，なぜスタートアップがハードウェアを作って世界で売っていくことができるようになったのかを解説.

[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.

- 現在販売されている最新のIoT家電が有する機能・性能についての知識（カタログに載っている情報程度で構わない）
- CES 2018で発表された最先端のConsumer Technologiesに関する知識（一般紙における記事を読む程度で構わない）

[準備学習等の具体的な指示]

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）

[成績評価]

[評価の観点]

[評価方法] レポート成績

7.3 セキュリティ基盤技術

[開講科目名]

（授業科目）離散数学と計算の理論／（enPiT-Pro）セキュリティ基盤技術

[開講科目名（英）]

Discrete Mathematics and Computational Theory

[単位数/時間数] 2.5単位/30時間

[開講日] 春～夏学期

[担当教員]

宮地 充子（大阪大学），高野 祐輝（大阪大学）

[授業の目的・概要]

（1）情報セキュリティにおいて必要となる離散的な構造に対する数学的諸概念や考え方に習熟し，数学の各種定理を応用する方法について理解する．

（2）数学的な証明とプログラミング言語の基礎となる論理と計算について理解する．

[学習目標]

(1) 離散的な構造に対する数学的諸概念として，群，環，体，初等整数論の概念を理解するとともに，各種数論的アルゴリズムを習熟し，それらの情報セキュリティへの応用方法を習得することを目標とする．

(2) 命題論理，述語論理の概念を理解し，多くの関数型プログラミング言語の基礎となっている λ 計算と型システムについて習熟することを目標とする．

[講義計画]

OH1回 本講義に必要な事前課題，事前準備の説明．講義の関係について紹介

OH2回 本講義の中間全内容までの関する質問

OH3回 本講義の全内容に関する質問

第1回 群（1）

置換群など非可換群から可換群の具体例とともに，生成元や有限生成群など群の諸性質について学ぶ．

知識単位（半群，モノイド，群の公理，部分群）

第2回 群（2）

剰余類，及び正規部分群について定義し，剰余類が群になる部分群の条件を明確にする．

知識単位（剰余類（Lagrange の定理），正規部分群，剰余群）

第3回 環

環の公理及び準同型写像，準同型定理，準同型写像の核，準同型写像の像，さらにイデアルについて説明する．

知識単位（環の公理，準同形写像（準同形定理），イデアル）

第4回 環・体

ユークリッド環，単項イデアル環の定義及び具体例，さらに，体の公理及び有限体について学ぶ．

知識単位（Euclid 環，体，有限体）

第5回 整数論（1）

整数及び多項式環を用いて，素数，除法の原理，Euclid の互除法について説明する．

知識単位（素数，除法の原理，Euclid の互除法）

第6回 整数論（2）

不定方程式の解の存在条件，解の求め方から，中国人の剰余定理について学ぶ．さらに，有限体を用いて，Lagrange の定理など，これまでに学んだ群・環・体の諸性質について理解を深める．

知識単位（不定方程式，合同式，中国人の剰余定理，平方剰余記号）

第7回 総合課題1（代数学1）

第8回 総合課題2（代数学2）

第9回 総合課題3（初等整数論）

第10回（離散数学）試験

第11回 命題論理

命題論論理について学習し，形式的証明を通して数学における証明について学ぶ．

それとともに，日常生活で必要な論理的な思考法についても習得する．

知識単位（命題論理，自然演繹法，命題論理の形式的証明）

第12回 述語論理

一階述語論理について学習し，数学の証明を行う上で必須の概念である述語や∀や∃といった限量子についてと，論理式の解釈とモデルについて学ぶ.

知識単位（限量子，解釈，モデル，述語論理の形式的証明）

第13回 計算可能性

チューリングマシンや原子帰納的関数といった計算モデルを利用して計算の仕組みについて学習し，その後に停止問題について学ぶ.

知識単位（停止問題，原始帰納的関数，チューリングマシン）

第14回 不完全性定理

健全性，完全性といった概念を学んだ後，算術の不完全性について学習する.

知識単位（健全性，完全性，算術の形式系，ペアノ算術，ゲーデル数，ゲーデルの不完全性定理）

第15回 λ計算

単純だが強力な計算モデルであるλ計算について学び，計算とは何かということを考える.

知識単位（α同値，β簡約，評価戦略，カリー化，不動点コンビネータ）

第16回 型システム

型付きλ計算について学習し，型による安全なプログラミングの基礎を学ぶとともに，数学の証明とプログラミングの型の構造が同一であることを学ぶ.

知識単位（型付きλ計算，カリー・ハワード同型対応，型検査，型推論）

第17回 プログラムの正当性

論理的な推論規則に基づいてプログラムの正当性を証明する方法について学習する.

知識単位（ホーア論理，不変条件，命令型プログラム，停止問題）

[準備学習等の具体的な指示]

事前課題を実施すること.

教育システムで提供される事前課題を行うことで，理解を深めること.

[教科書・教材]

1. 宮地充子著,「代数学から学ぶ暗号理論」，日本評論社
2. 萩谷昌己，西崎真也,「論理と計算のしくみ」，岩波書店

[参考文献]

1. James L.Hein,「独習コンピュータ科学基礎II 論理構造」，翔泳社
2. Benjamin C. Pierce,「型システム入門 プログラミング言語と型の理論」，オーム社

[成績評価]

[評価の観点] 情報セキュリティに必要な基礎知識及びセキュリティの理解度による.

[評価方法] 試験及びレポート成績

[評価基準] 中間試験（40%）及びレポート成績（10%），レポート（50%）

7.4 実践情報セキュリティとアルゴリズム

[開講科目名（英)]

Practical Information Security and Algorithms

[単位数/時間数] 2.5 単位/30時間

[開講日] 秋～冬学期

[担当教員]

宮地 充子（大阪大学），高野 祐輝（大阪大学）

[授業の目的・概要]

(1) RFIDタグや携帯端末等，IoT機器におけるデータ秘匿やデータの偽造を防ぐ技術として脚光を浴びている楕円曲線暗号について解説するとともに，その実装も行う．

(2) 高信頼なソフトウェアを設計・実装するための技術である，型システム，モデル検査について解説する．また，型付き λ 計算上への型システムの実装と，形式手法を用いたアルゴリズム・ソフトウェアの設計を行い，実践的なアルゴリズム・ソフトウェアの設計・実装手法について理解する．

[学習目標]

(1) 暗号理論と情報セキュリティの基盤技術およびその構成要素を理解し，暗号理論と情報セキュリティを応用するアプリケーションと適切な実装や応用ができるようになる．

(2) 型システムとモデル検査について理解し，高信頼なアルゴリズム・ソフトウェアを設計・実装できるようになる．

[講義計画]

OH1回 本講義に必要な事前課題，事前準備の説明．講義の関係について紹介

OH2回 本講義の中間全内容までの関する質問

OH3回 本講義の全内容に関する質問

第1回 公開鍵暗号の基礎知識

公開鍵暗号の基礎知識である離散数学及び初等整数論について理解する．ユークリッドの互除法，拡張ユークリッドの互除法，中国人の剰余定理，べき演算など．

知識単位：ユークリッドの互除法，拡張ユークリッドの互除法，中国人の剰余定理，べき演算

第2回 python の利用方法

数式処理ソフト python の利用方法，及び python を用いた離散数学，暗号処理，暗号解析の実装のために必要な方法を習得する．

第3回 楕円曲線１

楕円曲線は情報セキュリティ利用されるだけでなく，代数という観点でも，様々な性質を具現化する非常に興味深い理論である．本講義では，楕円曲線暗号のベースとなる楕円曲線の理論を紹介する．具体的には，同型写像，加法公式，j不変数などの楕円曲線の基礎的な定義，定理を具体例を含めて解説する．

知識単位：楕円曲線，同型写像

第4回 楕円曲線２

楕円曲線は計算量的安全性をもつ暗号から耐量子安全性を持つ暗号まで提案されている．本講義では，ハッセの定理，同種写像，各種座標系など，さらに進んだ楕円曲線の定義，定理を具体例を含めて解説する．

知識単位：楕円曲線，同種写像，ハッセの定理

第5回 公開鍵暗号

情報セキュリティの理論で最も重要な技術の一つである公開鍵暗号は現代暗号理論の基本概念であるとともに，秘匿・完全性・可用性を実現する情報セキュリティの基本概念である．公開鍵暗号の基本原理及び TLS などで利用される公開鍵暗号の概念について紹介するとともに，安全性の概念及び効率などの指標について紹介する．

知識単位：公開鍵暗号，安全性

第6回 楕円曲線暗号

情報セキュリティの理論で最も重要な技術の一つである公開鍵暗号の中で最も脚光を浴びているのが楕円曲線暗号である．本講義では，楕円曲線暗号について紹介し，その安全性，特徴，他の公開鍵暗号との違いを含めて解説する．

知識単位：公開鍵暗号，安全性，楕円曲線暗号

第7回 ディジタル署名

情報セキュリティの理論で最も重要な技術の一つであるディジタル署名は電子署名法を支える技術であるとともにディジタル認証に利用される基本技術である．本講義ではディジタル署名の基本原理の基本原理及びTLS などで利用される具体的なディジタル署名について紹介するとともに，その安全性の概念及び効率などの指標について紹介する．

知識単位：ディジタル署名，安全性

第8回 ハイブリッド暗号

公開鍵暗号・ディジタル署名を用いて，実際にデータ秘匿・完全性を実現する方法について紹介するとともに，その安全性の概念及び効率などの指標について紹介する．

さらに，ハイブリッド暗号を実際に実装することでその仕組みについて理解する．さらに実装を通して，公開鍵暗号の運用時の問題点について，理解する．

知識単位：ハイブリッド暗号，ディジタル署名，公開鍵暗号，安全性，楕円曲線暗号

第9回 楕円曲線暗号システム構築

python を用いて，楕円曲線暗号，楕円DSA署名を実装し，ハイブリッド暗号システムを実装する．さらに実装したシステムを用いて，相互秘匿通信を実験する．

知識単位：ハイブリッド暗号の効率，性能

第10回 総合課題1（セキュリティシステムの設計）

第11回 ソフトウェアテスト概論

ソフトウェアテストについて解説した後，動的解析，ダングリングポインタ，代数的データ型，参照カウンタ，ガベージコレクションなどの概念及びアルゴリズムについて説明する．

知識単位：ソフトウェアテスト，ガベージコレクション，代数的データ型

第12回 プログラミング言語Rust

部分構造型システムのアフィン型を適用したプログラミング言語の代表例としてRust言語の説明を行い，Rust言語の基礎的な文法とその安全性について理解する．

知識単位：Rust言語，部分構造型，代数的データ型

第13回 線形型システム

部分構造型システムのうち，特に型付き λ 計算上の線形型システムについて，文脈の分割，型付け規則などの理論的背景を解説する．

知識単位：型付き λ 計算，線形型システム，形式的証明

第14回 線形型システムの実装

Rust言語を用いて線形型システムの型検査アルゴリズムを実装することで，理論と実装の両面からRust言語の安全性について理解する．

知識単位：Rust言語，型付き λ 計算，線形型システム

第15回 並行プログラミング

アトミック命令，排他制御，スピンロックなどの基本的な同期処理機構について説明する．また，PthreadsとRust言語による並行プログラミング手法の紹介と比較を行い，並行プログラミングという側面から見たRust言語の安全について理解する．

知識単位：並行プログラミング，アトミック命令，同期処理，Rust言語，Pthreads

第16回 モデル検査

モデル検査の基本的な考え方を示した後，関係，制約，述語，アサーション，関数，ファクトといった基本的な概念について解説する．

知識単位：述語論理，形式手法，モデル検査

第17回 形式仕様記述

スピンロックを形式的に仕様記述する方法について解説する．その後Readers-writerロックアルゴリズムなどを示し，それらアルゴリズムをモデル検査によって検査する方法について説明する．また，食事する哲学者問題やデッドロック，ライブロック，飢餓といった並行プログラミングに関する諸問題について紹介する．

[準備学習等の具体的な指示]

事前課題を実施すること．

教育システムで提供される事前課題を行うことで，理解を深めること．

[教科書・教材]

1. 宮地充子著,「代数学から学ぶ暗号理論」，日本評論社
2. 宮地充子，菊池浩明編「IT Text 情報セキュリティ」，オーム社
3. Daniel Jackson，中島 震「抽象によるソフトウェア設計 Alloyではじめる形式手法」，オーム社
4. Benjamin C. Pierce編「Advanced Topics in Types and Programming Languages」，The MIT Press

[成績評価]

セキュリティ応用の評価（50%），暗号理論の評価（50%）

[評価方法] 事前課題試験及びレポート成績

[評価基準] 事前課題試験（10%）及びレポート成績（40%），レポート（50%）

7.5 実践安全な公開鍵暗号の設計と解読PBL（高度セキュリティ PBL I）

[開講科目名]

（授業科目）高度セキュリティ PBL Ⅰ／(enPiT-Pro）実践安全な公開鍵暗号の設計と解読PBL

[開講科目名（英)]

Advanced Security PBL I

[単位数/時間数] 1.5 単位/16時間

[開講日] 夏学期，集中

[担当教員]

宮地 充子

[開講言語]

英語

[授業の目的・概要]

本科目では公開鍵暗号を用いてモノのインターネット（IoT）のデータを保護する方法を学び，実際に実装する方法について習得する．

サイバーセキュリティの基礎である暗号には共通鍵暗号および公開鍵暗号の二種類がある．前者では各参加者は一つ以上の秘密鍵を事前に共有していることが仮定するので，n端末のネットワークではn^2個の鍵を管理する必要があり，IoTへの応用では現実的でない．一方，公開鍵暗号は，n端末のセキュアネットワークを1個の鍵で実現し，理論的に魅力的な解決方法を提供する．しかし，多くのIoT機器は計算・メモリ・通信能力が非常に限られおり，公開鍵暗号を利用することが容易ではない．さらに，多数のIoT機器を用いた攻撃も考えられる．

本PBL演習ではIoTのデータを保護する公開鍵暗号の実現方法から暗号解読手法まで，理論的なアルゴリズム習得から，実際に実装する手法まで習得することを目的とする．公開鍵暗号及びその解読手法を実装することで，暗号及び解読にかかる時間を実感することで，より深い理解を促すことを目的とする．

[学習目標]

現代の公開鍵暗号の背後にある理論，および資源に制約を持つIoT機器上で公開鍵暗号を実装する際に特有の課題について学ぶ．また，解読手法についても学ぶ．さらにIoTのための効率的な公開鍵暗号の実装方法とともに解読の実装方法や並列化手法についても学ぶ．

[講義計画]

OH1回 本講義に必要な事前課題，事前準備の説明．講義の関係について紹介

OH2回 本講義の中間全内容までの関する質問

OH3回 本講義の全内容に関する質問

第1回 python で数学を

python を用いて，初等整数論，統計解析などに応用する手法を学習する．

第2回 暗号の基礎となる整数論及び必要なアルゴリズムの紹介と実装

知識単位：ユークリッドの互除法，バイナリ法

第3回 サイドチャネル攻撃と初等整数論を応用した防御方法

実装による実験解析を実施する．

知識単位：サイドチャネル攻撃，フェルマーの小定理

第4回 公開鍵暗号の概念及びElGamal 暗号の紹介と実装

知識単位：公開鍵暗号の概念，ElGamal 暗号

第5回 公開鍵暗号の応用及びDH 鍵共有法の紹介

知識単位：鍵共有の概念，DH 鍵共有法，暗号の評価手法

第6回 典型的な解読方法ρ法とその実装，並列化

知識単位：ρ 法，指数計算法

第7回 ディジタル署名の概念及DSA署名の紹介と実装

知識単位：ディジタル署名の概念，DSA 署名

第8回 解読実験と課題発表

[履修条件・受講条件]

「離散数学と計算の理論」か「実践情報セキュリティとアルゴリズム」の受講が望ましい．

また，数学的素養およびプログラミングの基本技術を必要とする．

[準備学習等の具体的な指示]

教育システムで提供される事前課題を行うことで，理解を深めること．

[教科書・教材]

1. 宮地充子著,「代数学から学ぶ暗号理論」，日本評論社

[成績評価]

公開鍵暗号の概念と数論応用の手法の理解，さらに実装に必要な基礎知識

[評価方法] 事前課題試験及び演習課題，演習発表

[評価基準] 事前課題試験（20%）及びレポート成績（50%），演習発表（30%）

7.6 安全なデータ利活用のための準同型暗号PBL（高度セキュリティ PBL Ⅱ）

[開講科目名]

（授業科目）高度セキュリティ PBL Ⅱ／(enPiT-Pro）安全なデータ利活用のための準同型暗号PBL

[開講科目名（英)]

Advanced Security PBL Ⅱ

[単位数/時間数] 1.5 単位/16時間

[開講日] 秋～冬学期，集中

[担当教員]

宮地 充子（大阪大学），奥村 伸也（大阪大学）

[授業の目的・概要]

本科目では暗号化したまま統計処理などが可能な準同型暗号やその応用と課題を学び，実際に実装することで習得する．

情報化社会が進むにつれ大量のデータをクラウドに預ける企業などが急激に増えてきた．さらに，クラウドサーバーはそれ自体が高い演算処理能力のあるマシンであるから，預けたデータの統計処理等が可能であり，様々なアプリケーションを提供することができる．しかし，クラウドデータの漏洩や信用できないクラウド管理者への対策としてデータを暗号化した状態でクラウドに預けることが望ましいが，通常の暗号による暗号化では，暗号化データを処理してしまうと正しく復号できなくなってしまう，という問題がある．

そこで，暗号化データに対して暗号化した状態で特定の演算処理を行うことで，復号後に望んだ平文の処理結果を手に入れることができる，準同型暗号が非常に注目されている．

GentryやDijkらにより暗号化したまま加法と乗法両方の演算が可能な完全準同型暗号が提案されて以降，改良や応用に関する研究が活発に行われている．

本PBL演習では，暗号化されたデータを安全に利活用するための準同型暗号に関する理論・応用・安全性について，実際に実装することで習得する．

[学習目標]

準同型暗号の理論から応用・攻撃について学び，実際に実装することで習得すると共に，準同型暗号の有用性や実用化のための課題について体感する．

[講義計画]

(1) 数学と暗号理論からの準備
　知識単位：初等整数論，格子理論，暗号の構成要素，暗号の識別不可能性

(2) 準同型暗号に関する講義と準同型暗号の例
　知識単位：準同型暗号，RSA暗号，Paillier暗号，ElGamal暗号

(3) 準同型暗号の応用と実装1
　知識単位：電子投票（匿名性の確保のみ）

(4) 格子ベースの準同型暗号（構成と効率化のテクニック）
　知識単位：Learning With Errors（LWE）問題

(5) 格子ベースの準同型暗号の安全性と攻撃
　知識単位：最短ベクトル問題，最近ベクトル問題，Kannanの埋め込み法

(6) まとめと課題発表

[履修条件・受講条件]

「離散数学と計算の理論」か「実践情報セキュリティとアルゴリズム」の受講が望ましい．
また，数学的素養およびプログラミングの基本技術を必要とする．

[成績評価]

[評価の観点] 準同型暗号やその応用と課題について実装や説明ができるか
　学んだ準同型暗号の安全性について説明できるか

[評価方法] 課題と最終プロジェクト

[評価基準] 課題（60%）+ 最終プロジェクト（40%）

[備考]

人数多数の場合には履修条件を満たしている学生から優先します．

7.7 実践CTF（高度セキュリティ PBL Ⅲ）

[開講科目名]

（授業科目）高度セキュリティ PBL Ⅲ／(enPiT-Pro）実践CTF

[単位数/時間数] 1.5 単位/16時間

[開講日] 秋冬学期（集中講義）

[担当教員]

新井 悠（NTTデータ），中津留 勇（セキュアワークス），園田 道夫（NICT）

[授業の目的・概要]

本科目では情報セキュリティ分野における各種のカテゴリの習熟度を確認するための演習に取り組む．情報セキュリティ分野の技能検定については，筆記による情報処理試験やその他民間の試験がよく知られている．一方で，実践的技能を自ら主体的に判定する方法としてCapture The Flag方式の問題を実際にプログラム開発などを通じて解き，得点を獲得する手法がある．本科目においては，まずCTFに取り組むための基礎的な知識を演習形式で学習する．

その上で，CTF形式の演習に取り組むことで，参加者の実践的技能が十分に獲得できている科目と，そうでない科目を経験として得ることで，さらなる自らの技能向上に取り組むための一助とする．

[学習目標]

情報セキュリティ分野に関する実践的技能を自主的に向上させていく能力を養成する．

[講義計画]

OH1回 本講義に必要な事前課題，事前準備の説明．講義の関係について紹介

OH2回 本講義の中間全内容までの関する質問

OH3回 本講義の全内容に関する質問

第1回 CTF概要とウォーミングアップ問題

第2回 暗号問題

第3回 PWN問題

第4回 リバースエンジニアリング

第5回 リバースエンジニアリング

第6回 CTF実践

第7回 CTF実践

第8回 振り返りと問題解説

[知識単位]

CTF，バイナリ，ヘッダ，メタデータ，通信プロトコル，フォレンジック

[成績評価]

[評価の観点] 情報セキュリティへの学習意欲と実習の結果

[評価方法] CTFの結果で評価する

[評価基準] 演習課題（20%）と CTF（80%）

[備考]

演習機材の関係で人数を制限します．

7.8 包括的サイバーセキュリティ演習（高度サイバーセキュリティ PBL Ⅰ）

[開講科目名]

（授業科目）高度サイバーセキュリティ PBL Ⅰ／(enPiT-Pro）包括的サイバーセキュリティ演習

[開講科目名（英)]

Comprehensive Cyber Security Training

[単位数/時間数] 1.5 単位/16時間

[開講日] 春学期

[担当教員]

高野 祐輝，宮地 充子（大阪大学）

[授業の目的・概要]

一般的に，サイバー攻撃は，探索活動，侵入・感染，侵入・感染時攻撃，侵入・感染後攻撃と言うように，いくつかの段階を踏んで行われる事が多い．そのため，サイバー攻撃に適切に対処するためには，マルウェア解析や暗号技術といった要素技術の習得のみではなく，サイバー攻撃の各段階における手法と防御技術を系として捉え，包括的に理解し，適切なネットワーク設計をする必要がある．

そこで，本PBLでは，仮想エンタープライズネットワークを用いて，サイバー攻撃における各段階の手法を学習するとともに，ネットワークレベルでの対策手法とネットワーク設計の演習を行う．

[学習目標]

本PBLではネットワーク設計の基礎演習，境界型防御演習，検疫ネットワーク設計演習の3つを行い，さまざまな攻撃とその対策手法について習得する．

(1) ネットワーク設計の基礎演習

データリンク層とネットワーク層の基本を学び，仮想環境上にネットワークを構築する手法を習得する．

(2) 境界型防御演習

境界型防御演習では，OpenBSDのPF等に代表されるパケットフィルタリング機構を利用し，上記攻撃手法学習で学んだ攻撃手法に対するネットワークレベルでの対策手法を習得する．

(3) 検疫ネットワーク設計演習

検疫ネットワークの設計を行うことで，セキュアなネットワーク設計を行う方法を習得する．

[講義計画]

OH1回 本講義に必要となるLinux，UNIXの基本的な操作に関する事前課題の説明

OH2回 コンピュータネットワーク設計に関する質問

OH3回 本講義の全内容に関する質問

第1，2回 インターネットのアドレスとOSI参照モデル

物理層，データリンク層，インターネットの基礎的な動作について説明し，その原理を理解する．

第3，4回 仮想ネットワーク技術

VLANなどの仮想ネットワーク技術について説明し，先端のネットワーク設計手法について学習する．

第5回 トランスポート層，アプリケーション層

TCP，UDPのトランスポート層に説明する．特にTCPのコネクションについて理解を深める．また，DNSといったアプリケーション層で動作するプロトコルの解説も行う．

第6回 ファイアウォール

Radix Treeといったルーティング技術について説明し，pfやiptablesといったファイアウォール技術について解説する．

第7回 ネットワークスタックの実装と検疫ネットワーク

TCP/IPのネットワークスタックを実装する方法について説明する．また，高度なネットワーク防御手法である検疫ネットワークについても解説する．

第8回 ネットワーク設計演習と発表

仮想環境上にネットワークを構築し，ファイアウォール技術を用いたドメインの分離とフィルタリングを行う．また実際に作成した環境について発表し議論する．

[履修条件・受講条件]

特になし

[準備学習等の具体的な指示]

Linux，UNIXのシェルを利用できるように学習しておくこと．

[教科書・教材]

アンドリュー･S･タネンバウム，デイビッド･J･ウエザロール,「コンピュータネットワーク 第5版」,日経BP

Peter N. M. Hansteen,「The Book of PF: A No-nonsense Guide to the Openbsd Firewall」

[成績評価] 演習発表とレポートによる評価を行う．

[評価方法] 演習と発表50点，レポート50点

[評価基準]

優：ファイアウォール技術でDeMilitarized Zoneのあるネットワーク設計と構築を行うことができる

良：ファイアウォール技術で適切なネットワークアクセスコントロールができる

可：ネットワークのしくみを理解し説明することができる

7.9 ネットワークトラフィック処理の基盤技術と実装（高度サイバーセキュリティ PBL Ⅱ）

[開講科目名]

（授業科目）高度サイバーセキュリティ PBLⅡ／(enPiT-Pro) ネットワークトラフィック処理の基盤技術と実装

[開講科目名（英)]

Fundamental Technique and Implementation of Network Traffic Processing

[単位数/時間数] 1.5 単位/16時間

[開講日] 春学期

[担当教員]

高野 祐輝（大阪大学），宮地 充子（大阪大学）

[授業の目的・概要]

デバッガはネットワークソフトウェアのみならず，ソフトウェア解析全般の基本となる技術である．そこでPBLでは，システムソフトウェアについて概要を示した後，ptraceを用いたデバッガの実装を行う．これにより，コンピュータの基本的なしくみを理解できるようになる．

また，ネットワークフィルタリングで頻繁に用いられるフィルタリング技術についても学習する．例えば，BSDやLinuxなどのオペレーティングシステムでは，BSD Packet Filter（BPF）と呼ばれる疑似レジスタマシンが用いられ，また，正規表現を実装する方法の一つとして，非決定性有限オートマトンを模倣する疑似レジスタマシンが用いられる事もある．

そこで，本PBLでは，ネットワークトラフィックに対してパターンマッチを行うための疑似レジスタマシンの設計と実装を行い，ネットワークトラフィック処理技術について理解を深める．

[学習目標]

(1) システムソフトウェア理解

システムソフトウェアについて理解し，システムコール，プロセス，割り込みなどについてのしくみを習得する．

(2) デバッガの設計と実装

ソフトウェア解析の基本となるデバッガをptraceを用いて設計，実装し，コンピュータの原理から理解する．

(3) バイトコードインタプリタの設計と実装

BPFや正規表現のバイトコードインタプリタを設計・実装することで，パターンマッチングの基盤技術を習得する．

[講義計画]

OH1回 本講義に必要となる演習環境である仮想マシンの事前準備説明

OH2回 デバッガ、正規表現実装に関する質問

OH3回 本講義の全内容に関する質問

第1，2回 UNIX OSとコンピュータのしくみ

物理層，データリンク層，UNIX OSのとコンピュータの基本的なしくみについて理解し，システムソフトウェアの実装について学習する．

第3，4回 デバッガのしくみ

デバッガのしくみについて理解し，ptraceを用いた実装方法について学習する．

第5回 正規表現エンジン

正規表現エンジンの基本的な動作について理解し，疑似マシンを用いた実装方法について学習する．

第6回 LLVMを用いたコンパイラフロントエンド実装

コンパイラ基盤であるLLVMを用いて，コンパイラフロントエンドを設計，実装する方法を学ぶ．

第7，8回 デバッガと正規表現エンジンの実装と発表

学習した成果を元にデバッガと正規表現エンジンを実装し発表する．また，お互いに議論し合い互いの不足点を補う．

[履修条件・受講条件] 特になし

[準備学習等の具体的な指示]

C言語とポインタについて学習しておくこと．CPUの基礎について学習しておくこと．

[教科書・教材]

W. Richard Stevens，Stephen A. Rago,「詳解UNIXプログラミング 第3版」，翔泳社

[成績評価]

演習発表とレポートによる評価を行う．

[評価方法] 演習と発表50点，レポート50点

[評価基準]

優：デバッガと疑似マシンの実装を行いテストまで実施可能

良：デバッガと疑似マシンのしくみを説明可能

可：基本的なシステムソフトウェアのしくみを説明可能

7.10 高度セキュアネットワーク設計演習（高度サイバーセキュリティ PBL Ⅲ）

[開講科目名]

（授業科目）高度サイバーセキュリティ PBL Ⅲ／(enPiT-Pro) 高度セキュアネットワーク設計演習

[開講科目名（英)]

Advanced Secure Network Design Practice

[単位数/時間数] 1.5 単位/16時間

[開講日] 春学期

[担当教員]

高野 祐輝（大阪大学），宮地 充子（大阪大学）

[授業の目的・概要]

巧妙化するサイバー攻撃に対して，様々な防御手法を設けることで脅威に対するリスクを下げることができる．しかしながら，サイバー攻撃の巧妙化に加えて，サービスが多様化したことで対策するべき範囲が広がっている．そこで，様々なセキュリティ機器を組み合わせてインシデントの発生確率を下げる多層防御が用いられている．

本演習では，まず複数の特徴が異なるセキュリティアプライアンスを用いて，その動作を理解する．そして，これらのセキュリティアプライアンスを使用し多層防御の考え方，構築手法を習得することを目的とする．

[学習目標]

(1) 多層防御学習
　多層防御の考え方，及び必要性について学ぶ

(2) セキュリティアプライアンスを利用した演習
　実際の商用ネットワークで利用されている複数のセキュリティアプライアンスを利用し，セキュアなネットワーク運用を行うための基礎技術を習得する

(3) 多層防御的ネットワークの設計と構築演習
　複数のセキュリティアプライアンス正しく利用し，多層防御的なネットワークを設計し，構築できるようになる．

[講義計画]

OH1回 本講義に必要なる遠隔接続の説明

OH2回 多層防御に関する質問

OH3回 本講義の全内容に関する質問

第1回 UNIX OSとコンピュータのしくみ

物理層，データリンク層．

第2回 サイバーセキュリティ

サイバーセキュリティの基本的な概念を説明し，サイバー攻撃について最新の事例を紹介する．

第3，4回 ファイアウォール

商用のファイアウォール機器を用いた，ファイアウォールの基礎的な設定方法について説明する．

第5回 アプリケーション層でのセキュリティ

サンドボックスやスパムフィルタなど，アプリケーション層でのセキュリティ技術について解説

する.

第6回 監視

セキュリティ情報収集の基礎となるネットワーク監視技術について説明する.

第7，8回 演習と発表

実際のファイアウォール機器を用いたファイアウォール設定や，監視ソフトウェアを用いた監視の演習を行い発表する．また，それらについて議論することで，さらに理解を深める.

[履修条件・受講条件] 特になし

[準備学習等の具体的な指示]

基本的なUNIX OSの操作について学習しておくこと.

コンピュータネットワークについて基本を学習しておくこと.

[成績評価] 演習発表とレポートによる評価を行う.

[評価方法] 演習と発表50点，レポート50点

[評価基準]

優：ファイアウォール設計及び監視を協調した設計ができる

良：多層防御の考え方に基づいてファイアウォール設計ができる

可：多層防御の考え方を説明できる

7.11 情報ネットワーク経済学

[開講科目名]

情報ネットワーク経済学

[単位数] 2単位

[開講日] 夏学期

[担当教員]

新井 圭太（近畿大学），山口 弘純（大阪大学）

[授業の目的・概要]

講義を通じて, 情報ネットワークと経済学, 政策との関連を理解する．また, 近年の情報セキュリティ意識の高まりを受け，経済学の観点から情報セキュリティにかかるコストについて議論する．

[学習目標]

以下の学習を行い，情報ネットワークと経済学，政策との関連を理解できるようになることを目標とする．

1. 市場経済のメカニズム（Market Mechanism）
2. 経済システムと厚生（Economic System and Welfare）
3. 規制経済学（Regulatory Economics）
4. 情報経済学（Economics of Telecomuunication）
5. マクロ経済と情報通信（Macroeconomic perspective）

7.12 安全なデータ設計特論

[開講科目名]

安全なデータ設計特論

[開講科目名（英)]

Special Course of Secure Data Design

[単位数/時間数] 1.5 単位/16時間

[開講日] 秋冬学期

[担当教員]

宮地 充子

[開講言語]

日本語・英語

[授業の目的・概要]

安全安心便利なディジタル社会構築に向けた課題を明らかにし，その課題を解決するアプローチを設計する．また，提案アプローチを評価し，実現に必要なステップを明確にする．第一線で活躍する産官学のセキュリティ管理者，技術者，研究者のセミナーおよび現在の情報システムが抱える課題を議論することで，喫緊の課題や課題解決の方法，実現に必要な工数などを明確にし，セキュリティを社会に応用するシステム設計書を作成する．

[学習目標]

安全安心便利なディジタル社会構築に向けた課題を把握し，セキュリティを社会に応用するシステム設計について学習する．

[講義計画]

OH1回 本講義に必要な事前準備の説明

OH2回 安全なシステム設計書作成に関する質問

OH3回 本講義の全内容に関する質問

第1，2回 最新セキュリティセミナー

第一線で活躍される産官学のセキュリティ技術者，研究者による最新のディジタル社会の現状，各種課題，今後の進展についてのセミナー

第3，4，5回 課題抽出，解決方法検討

安全なシステム設計に向けた事例収集と課題解決手法やそのコストについて，議論する．

各受講者による事例紹介を実施する．

受講者の興味・知識に合わせたグループ分けを実施する．

第6，7，8回 安全なシステム設計発表

現在の情報システムが抱える課題，その課題解決の方法，実現に必要な工数などを明確にし，セキュリティを社会に応用するシステム設計書を作成する．

グループによるシステム設計書のプレゼンを実施し，課題の重要度，実現コスト，実現可能性について，議論する．

[履修条件・受講条件]

少なくともどれか一つのクイックコースを修了済みであること．

[準備学習等の具体的な指示]

職場や身近なディジタルシステムにおける課題の事例収集.

[教科書・教材]

1. 宮地充子著,「代数学から学ぶ暗号理論」, 日本評論社

[成績評価]

各種ディジタルシステムの知識, さらに課題解決手法の理解, さらに実装に必要な知識

[評価方法] セキュアなシステム設計書, 演習発表

[評価基準] システム設計書（50%）, 演習発表（50%）

8. 受講者の声

2018年以降の受講者の声を掲載します．各講義の受講を判断する基準にご利用ください．

8.1 離散数学と計算の理論

［離散数学］

・群の公理を限定した半群やモノイドの存在は本講義を通じて初めて学びました．定義したことのみを極力用いて証明を行う宮地先生の論理の進め方は非常にわかりやすく，自らも身に付けたいと感じました．

・群論は30年前の学生の頃に学んだはずでしたが，ほとんど忘れていました．基礎からきちんと説明して頂いてわかりやすかったです．

・部分群，剰余類，正規部分群などの定義や完全代表系を使った証明の方法，同値関係と剰余類で分割する意味が分かりました．

・準同型定理等，昔学習したはずですが，すべて学び直しでした．

・群や環，体は，対象を有限に落とし込んで研究しやすくするために使えることが分かりました．

・最大公約数，最小公倍数，素数の積，互いに素など定義や証明について理解できました．

・中国人の剰余定理（CRT）は応用分野が広いことが分かりました．

［計算の理論］

・形式的証明，記号や式の意味，証明の手順について理解できました．真理表で，AがFalseの場合，A->Bが常にTrueになる理由が分かりました．

・XORに関する内容は最も勉強になりました．多入力のXOR-GATEの奇妙な性質は何故かと考えて，最後は証明できるまで理解できて，勉強になりました．

・論理については高校数学の学習で身につく程度のものしか知らず，一部前提知識として身につけていたものもありましたが，きちんと体系的に学習したことがなく，非常に興味深かったです．形式的証明の例題として与えられている問を本講義を聞かずに解くことも十分可能であると思いますが，本講義により厳密に筋立てて証明できるようになったと感じます．

・RRR法を使用した形式的証明が分かりました．

・計算が関数の再帰で定義できることが分かりました．Haskellのプログラミングについて，原始帰納的関数を学んだことで理解できるようになりました．

・ゲーデルの不完全性定理はなんとなく知識として概要は知っていましたが，証明を聞いても難解すぎてついていくのが厳しかったです．

・ラムダ計算について，わかりやすい説明で自分でも手を動かして確認できるようになりました．

・LISPでLAMBA式で，束縛と解放の意味がよく分かりました．

8.2 実践情報セキュリティとアルゴリズム

[セキュリティ編]

- Pythonを使ってみたいとずっと思っていたのによくわからなかったので，環境設定から始めることができてよかったです.
- Pythonのパッケージは多数あり，書き方も色々あるので，どう書かれているのかの実例が参考になりました.
- Jupyter notebookというアプリを知らなかったので，便利なものがあるな，と思いました．基本的にコマンドラインでプログラミング等をしているので，こういう新しいツールを教えてもらうとありがたいです.
- 演習をつけていただいていたので，普段は使わない文法の部分の復習ができました.
- pythonでバイト列と文字列の変換を行うパッケージの使い方がわかりました.
- データ型で直積型と直和型という分類があるということは初めて知りました．Maybe型も使用したことがなかったので，勉強になりました．ガベージコレクションなども，具体的な仕組みは知らなかったので，勉強になりました.
- 群・環・体について，書籍では調べておりましたが授業を受けたのが初めてでしたので，考え方を教えていただいて勉強になりました.
- 離散数学の授業を欠席して，あやふやになっていた部分がある程度明確になった気がします.
- 逆元を求める手法やべき乗を効率よく行う方法など数学的に解決できる問題について勉強になりました.
- 群の位数の考え方が，少しあやふやだったのですが，具体的に計算してだいぶん理解できました．バイナリ法も復習できました．拡張ユークリッドの互除法は，行列を使った実装をやりたかったのですが，今回実装できてよかったです.
- j不変量が何かという確認と，楕円曲線の加法が直線と楕円曲線の交点で表されるということが理解できました.
- ElGamal暗号となぜ準同型性がないのかが理解できました.
- 暗号の解読（攻撃）の種類
- いつも鮮やかなご説明がありがとうございます．ざっとかんがえて高々●●倍，といった見込みを立てて進められていたことが良かったです.

[アルゴリズム編]

- GCや所有権を用いてメモリリークを防止する仕組みを知ることができました.
- F35戦闘機のメモリリークの話は聞いたことがありましたが，12時間が許容範囲というのは衝撃的でした．戦闘時間が長くなったらどうするだろうと思いました.
- ガベージコレクションまでは知っていましたが，コンパイル時に型を確認するRust言語などは初耳だったので，勉強になりました．またMaybe型という考えが新鮮でした.
- 並行プログラミングの要件定義をALLOYで可能なこと.

8.3 セキュリティとビジネス

[情報の法的価値と法的規制]

<2020年>

・個人情報は面倒だという認識しかありませんでしたが，今回の講義を受講して，日本の現状とEUの取り組みなどを知ることができました．また，普段は避けていた法律の世界に触れることができ，今後，業務で個人情報を扱う際に役立つ内容でした．

<2019年まで>

・GDPR違反の事例
・Googleがなぜ統一基準がよいといっているのかというのは，非常に勉強になりました．
・過去の事例をもとに説明をしてもらえたので，頭に入ってきやすかったです．
・GDPRは職場でも関心が高い内容のため，面白かったです．
・法律の域外適用といった本来なら適用されない他国での行為に対し，法律が適用される可能性があるとの内容が，最も参考になりました．
・GDPRの影響力と，グローバル企業がそれに違反した場合，どのぐらいの費用がかかっていたのか，規模感がとてもよく理解できました．
・カリフォルニア州やEUの個人情報保護の法令解釈だけでなく背景についても，実際のクライアントをかかえておられる先生ならではの迫力あるお話で，非常に勉強になりました．
・来年施行されるCCPAの内容が，新聞で見るよりも詳しく教えていただき，最も参考になりました．
・個人情報保護に関しては，ヨーロッパvsアメリカとばかり思っていましたが，アメリカ内部でもカリフォルニアとニューヨークでは考え方が全く異なるということは知りませんでした．また，産業スパイが意外に世界に多く，発覚している例もたくさんあるということも勉強になりました．

[金融業務における暗号技術の応用と国際標準化]

<2020年>

・ブロックチェーンの技術は以前少し勉強しましたが，岩下先生の講義では生い立ちから幾多の変遷，そして現在まで詳しくテキストに記載していただき，とても勉強になりました．ここまで全体的にまとめていただいた講義は初めてでした．
・金融ITと暗号技術の歴史はとても興味深かったです．暗号の書籍では，軍事関連の利用の話が多く，金融の話はあまり知らなかったので勉強になりました．

<2019年まで>

・金融について，暗号資産はたしかにセキュリティそのものだということを改めて認識しました．ありがとうございました．
・名前だけは知っていた共通鍵暗号や公開鍵暗号などの仕組みを理解できたのが参考になりました．
・金融業界というのは，インフラ業界に次いでセキュリティを考えないといけない産業だと思いますが，内部でどういった議論がされているかというのを全く知らなかったので，とても勉強になりました．
・ブロックチェーン技術の基礎から理解できたことが参考になりました．また，マイニングの電力消

費の問題も参考になりました.

・ブロックチェーンのイベントなどに行くと，この技術でサーバーレスな非中央集権的システムが実現すると，少し大げさに歌われていることが多いですが，ビットコインの運用の実例を示していただき，技術に疎い人にとっては，そこまで非中央集権的なシステムではないということが再確認できてよかったです．また，マイニングによる消費電力量が一国の消費電力量を上回っているということは，衝撃的でした.

[IoT先端技術とその展開]

<2020年>

・IoTビジネスの本質と課題，個人情報に関して，ベンチャー的な観点も踏まえてわかりやすく講義いただき，勉強になりました.

・IoTがネットワークにつながることで，今までになかった価値を生み出せる可能性が高まるこいうことを実例を交えて知ることができてよかったと思います.

・IoTについて講義形式で話を聴くことは多かったものの，実際にIoT製品を開発されている方からのお話を伺うことはなく，非常に良い経験となりました.

<2019年まで>

・IOTの機器自身も簡単にハッキングできるためセキュリティが必要ということ.

・刺激的で，とにかく面白かったです．自分が電機メーカーの社員で，しかもIoT関連のしかもセキュリティ担当であることから，身につまされるというか，勉強になりました．メルカリの偽装されたマルウェアつき商品は，今までの情報資産に対する脅威の中で最もばれにくく，悪質で，大きな脅威だと感じました．家の中には悪い人はいないと考えてはいけない，と，強く感じました.

・DMPの内容を理解できたのが，最も参考になりました．また，IoTビジネスのサービス維持運営コストの内容も参考になりました.

・ハードが触れると，そこからデータを盗聴するのは意外と簡単だということが，とても勉強になりました．また，DMPやsimのお話も勉強になりました.

8.4 高度セキュリティ PBL Ⅰ，Ⅱ，Ⅲ

[高度セキュリティ PBL Ⅰ]

・学部時代に数学や情報の科目を履修していましたが，今回の実習で，やっとその意味がわかってきました.

・純粋に楽しくプログラミングできました.

・数学やシステム自体が好きな方，技術の習得が目的で受講されている方，社会的にどう応用できるかということに興味を持たれている方などがいらっしゃるように感じました.

・懇親会や最後のプレゼン発表で，自由にお話や質問する時間を設けていただいておりましたが，そこで，どういった動機で授業に来て，自分にどのような目的があるかということに気づいて帰られた方も多かったのではと思います.

・一般的なセキュリティの講座や実装中心の学部などでは，数学の知識から実際の実装まで教えてい

ただけることは稀だと感じておりますが,（ほとんどの場合，実装だけか，言葉の説明だけかと思います.（例えば，公開鍵暗号方式の説明も，公開鍵があって秘密鍵があって…と言葉だけは教えてもらえますが，実際の実装時の鍵がどのようなもので，どう実装するのかという説明まではされない場合がほとんどです．情報系の国家資格なども同じレベルかと思います.））やはり，数学の部分を少しでも学んでおかないと，既存システムの枠を超えて柔軟に考えるということが難しくなってくると思いますので，このように統合的に知識を教えていただける実習は，セキュリティや開発を専門にやっていこうと思われている方の将来性を広げてくれるものだと思います.

・普段あまり使っていない数学の基礎知識から応用するまで，幅広いシラバスが提供されていますので，暗号化技術で必要な数学の知識を取得するのに最適な場だと思います.

・講義形式と実装演習形式両方行いながら理解していくのは楽しかったです．講義で自分が書いていたノートを読むと，すぐに忘れていて，書いている意味が分からないことが多くあります．それで，私は実装演習の時間を使って，理解不十分な内容をノートで修正し，それをすぐに実装することで，自分が修正していた内容を本当に理解しているかどうかを確認することができました．それでも分からないことがありましたら，教員だけではなく，チューターによる指導・課題の回答説明もしていただいたので，解決した課題をすぐにフィードバックすることができます.

・最初は二日間だけで，実際にメッセージを暗号化できるまでのソースを書けるとは思いませんでしたが，PBL形式で受講することにより，ソースコードを単に書けるだけではなく，暗号化は実際にどうやって行うかというところ（基礎的な部分）を数学的に説明できるようになれたと思います．また，理論的な内容だけではなく，実装の演習も行うことによって，開発現場で直面する問題の可能性も想定できると思います.

［高度セキュリティ PBL Ⅱ］

・暗号の講義は,“現代暗号の誕生と発展”岡本龍明著という本で網羅されている新しい暗号の話なので，興味深く聞くことができました.

［高度セキュリティ PBL Ⅲ］

<2020年>

・CTFとは何かから丁寧に説明して下さり，理解しやすかったです．Kali Linuxについても，まったく知識がなかったのですが，なんとか触ることができてよかったです．私は仕事では管理職で，自分では手を動かすことがほとんどないので，今回の実践は役に立ちました.

・バイナリ解析の進め方を理解しました.

・リバースエンジニアリングについて，概念は知っていましたが，実際にはこうやるというのを手を動かして体験できたのは貴重でした．多くのコードを全部を読まず，ほぼあたりをつけてそこを精査するという技術はすごいと思いました.

・マルウエアと脆弱性はサーバー攻撃として多くない氷山の一角であるということ，サイバーセキュリティの仕事は範囲が広く一人で全部網羅することができないこと，プログラム言語の壁，権利や法律関係，製品開発者と連携して，解析をすることがわかりました.

・CTF，Kali Linux，リバースエンジニアリングなど，具体的なセキュリティ解析の手法について，まず初歩を教えて頂き，さらに実践として実際に手を動かしてやってみるところまでできました．私は仕事では管理職なので普段はあまり手を動かすことはないのですが，実際にやってみるとこうなっているというのを経験してみることは大変有意義でした．CTFはチャレンジャブルな問題も多く，答えが出た時の嬉しさはひとしおで短時間でしたが充実した楽しい時間でした．

・社会人でセキュリティの仕事をしているのですが，CTFに自分が参加することは想像もしていなかったので，今回の2日間を通して，実践力をどうすれば身につくのか，きっかけを与えていただけたと思います．学生さんたちのような反射神経や瞬発力はありませんが，市場でよく起こるセキュリティ事故の実例などからくる直観はたぶん社会人のほうがあると思うので，ある程度の場数を踏めば，社会人もCTFで楽しめると思いました．

また，ツールや解き方を知っているか知らないか，あるいは，教えてくれるサイトを見たことがあるかないか，も，とても重要な武器だということもよくわかりましたので，若い人たちにゲーム感覚でセキュリティを学んでいただくいいきっかけになると思いました．

・最初に概要の説明がされた後に実習という形式で，しかも説明時もハンズオン形式だったので，理解が深まったのだと思います．とても勉強になりました．

・CTFはじめて体験して，久々に頭がフル回転してよかったです．時間制限ありでパズルを解くような感覚でバタバタしながら考えることが面白かったです．

<2019年まで>

・演習の内容が素晴らしいと感じました．実際に手を動かして学べるため，よい経験になったと思います．

・CTFはやっぱり面白かったです．初心者用のものを何個か紹介してもらったので，チャレンジしたいと思います．

8.5 高度サイバーセキュリティ PBLI，Ⅱ，Ⅲ

［高度サイバーセキュリティ PBL Ⅰ］

・TCP/IPモデルについて必修の授業でやる内容よりも深い知識が得られました．

・仮想ネットワークはほとんど知らない事ばかりで，難しかったが勉強になりました．

・効率的かつ安定した通信を行うためにパケットへの処理やネットワークの構造など様々な工夫が行われていることが分かりました．

・オーバーレイネットワークネットワーク系の知識がなかったため，全てを完全に理解，覚えられたわけではないですが，各用語やそもそもどうなっているのかといった根本的な部分から勉強できたことが最も良かった点です．

・Linuxサーバー上に仮想マシンを立てて利用したことが勉強になりました．OpenBSDに加えてvagrantの基本操作を数個覚えることができました．またルーティングテーブルの設定を通して「通信」をイメージしやすくなりました．

・Firewallは，なんとなくブロックするものという認識でしかなかったため，より詳しく知れたのが良かったです．

・ルーティングテーブルやFWの具体的な設定方法が，知見や経験がなかったため，もっとも勉強になりました.

[高度サイバーセキュリティ PBL II]

<2020年>

・デバッガをこれまで詳しく見たり触ったりしたことが無く，どのようなことが出来るのか学ぶとても良い機会になりました．レジスタ周りのことも改めて実践で知ることが出来たので良かったです.

・アセンブリやマシンコードは見たことがあった程度でしたが，実際に触って理解するのは初めてだったのでとても勉強になりました．自分で小さな正規表現検索を作れたのも良かったです.

・x-codeがLLVMになったと聞いた時から，いつかLLVMについて勉強しようと思っていましたが，今日やっと勉強することができました．自学では，なにから始めればいいかわかりませんでしたが，1日で全体像がわかって，続きを自分でできそうです.

<2019年まで>

・理解があやふやになっていたところ，また名前だけもしくはざっくりと聞いたことは深く理解できていないところに対する理解が深まった気がします.

・ニュースなどでも仮想化技術が流行っているという記事をよく見かけるのですが，実際の導入はニュースから想像するほど多くないようです.

・インフラの仮想化は，ちょうど知りたいと思っていた部分でした．大変勉強になりました.

[高度サイバーセキュリティ PBL III]

<2020年>

・一番勉強になったことは，セキュリティに対する考え方とそれぞれのlayerにおけるセキュリティ対策方法です．動作しているシステム・サービスに合わせて何（機密性，完全性，可用性）を重要視するかでセキュリティの組み方も大きく変わってくるというところです．また，多層防御の考え方で処理速度が遅いものを後回しにすることで負荷の少ない量で処理することができるのは効率が非常に良いと思いました．layerにおけるセキュリティ対策方法では，特にVRFというものは知らなかったので知ることができてとてもよかったです.

・講義の内容は，情報処理の試験を受験する際に勉強した内容に近いものでしたが，詳細が思い出せないことが多く，また，知らない内容もいくつかあり継続して学ぶ必要性を感じました．また，勘違いしていたことや試験勉強でわからなかったことが明確になりました．書籍で学ぶのとは違って，実際にネットワークを運用されている明石先生のお話を聞けて理解が深まりました.

・今日の講義で改めてL7のセキュリティを学習しました．ひとつひとつは聞いたことがありますが，全部まとめて整理して聞いたのは初めてでした.

<2019年まで>

・基本から最新の動向まで順を追って説明がありわかりやすかったです.

・SRXを設定するのは初めての経験だったため大変勉強になりました.

・今まで使ってはいるけれど自身で構築や設定を行なったことがなかった，WAF等の設定を自分で

行えたので，理解が深まりました．特にルータやファイヤーウォールについては，演習で行なった規模で自身で試してみることは難しいので体験できて良かったと思います．

・L4/L7のセキュリティについて，座学では知っていたものの実際に設定するのは初めてでした．わかってしまえば難易度は高くないものの，設定それぞれの関連性があり事前に設計するにはいろいろと留意することがあるのを体感できました．

・典型的なサイバー攻撃の手法と多層防御について整理が出来，実際のクライアントサーバとネットワーク機器の設定，動作がエミュレーション環境内で連携して学べたことが勉強になりました．

MiYaJi Laboratory

OSAKA UNIVERSITY ／ Miyaji Laboratory