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

20240422-V41

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プログラム
コース案内

大阪大学
OSAKA UNIVERSITY

大阪大学大学院 工学研究科 宮地研究室


MiYaJi
Laboratory

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を育成するには，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になります．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．

2007-2023 年 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.
- 令和 3 年度 IPSJ(情報処理学会)　よりフェローとして認定
- 令和 3 年度 IEICE(電子情報通信学会)第 5 回歴代教育優秀賞受賞
- 令和 3 年度 第 7 回プライバシーワークショップ 2021PWS Cup 匿名ヘルスケアデータコンテスト総合優勝

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

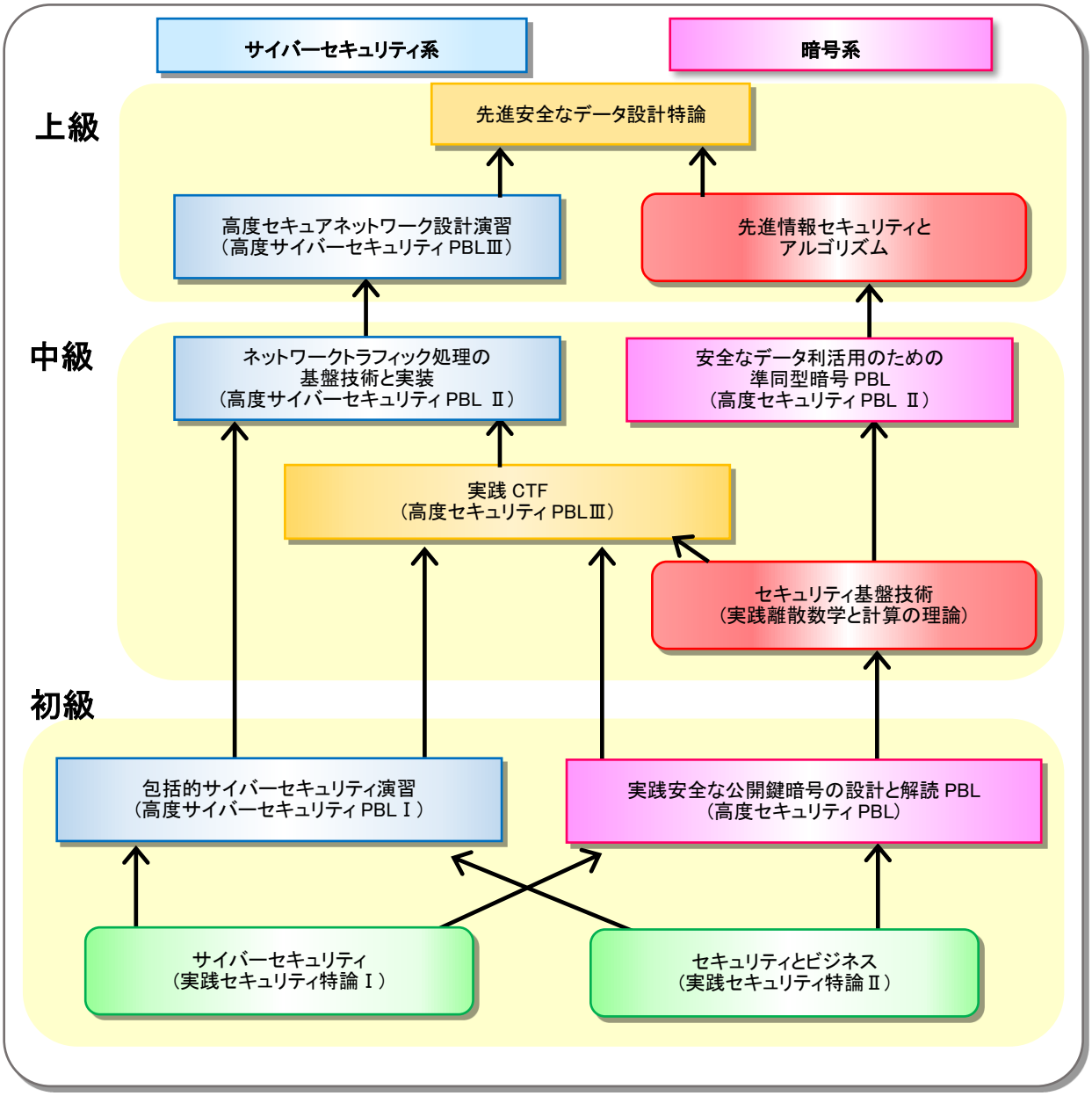
○受講の目安知識

大学教養レベルの数学やアルゴリズム・プログラミングに関する基礎知識を有することが望まれます.

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．

	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（実践離散数学と計算の理論）	・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
	・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
先進情報セキュリティとアルゴリズム	・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）
	・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
先進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

表 2. 知識マップ

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．講義・演習ともにオンライン参加が可能です．

表 3. モデル受講プラン

	講義・演習	春/秋	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	春	1.5	✔	✔	✔	✔	✔
セキュリティとビジネス	講義	秋	2	✔	✔	✔	✔	✔
セキュリティ基盤技術（実践離散数学と計算の理論）	講義	春	2.5		✔		✔	✔
先進情報セキュリティとアルゴリズム	講義	秋	2.5		✔	✔	✔	✔
実践安全な公開鍵暗号の設計と解読 PBL	演習	春	2	✔	✔	✔	✔	✔
安全なデータ利活用のための準同型暗号 PBL	演習	秋	1			✔		✔
実践 CTF	演習	秋	1	✔	✔	✔	✔	✔
包括的サイバーセキュリティ演習	演習	春	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	春	1			✔	✔	✔
高度セキュアネットワーク設計演習	演習	秋	1				✔	✔
先進安全なデータ設計特論	演習	秋	2		✔	✔	✔	✔
合計単位数			17.5	7.5	14.5	14	16.5	17.5

タイプ別受講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

インターネットを利用して情報収集あるいはデータの管理をされる方を想定しています. 学部卒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 x13 回), セキュリティとビジネス(90 分 x15 回)の座学講義があります. なお, これら 90 分 x28 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(3 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 7 日の課題解決型演習があります.

修得単位数は 5 科目(7.5 単位)です.

講義の選択例

春入学

1 年目 (5.5 単位)

・サイバーセキュリティ(1.5 単位)(春～夏学期)
・実践安全な公開鍵暗号の設計と解読 PBL(2 単位)(夏学期)(集中)
・セキュリティとビジネス(2 単位)(秋～冬学期)

2 年目 (2 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 CTF(1 単位)(秋～冬学期, 集中)

秋入学

1 年目 (5.5 単位)

・セキュリティとビジネス(2 単位)(秋～冬学期)
・サイバーセキュリティ(1.5 単位)(春～夏学期)
・実践安全な公開鍵暗号の設計と解読 PBL(2 単位)(夏学期, 集中)

2 年目 (2 単位)

・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)

② 教育関係者

学部卒同等の知識を有し，情報系，工学系あるいは理学系の教育に携わる方を想定しています.

講義は実践離散数学と計算の理論(90 分 x20 回)，先進情報セキュリティとアルゴリズム(90 分 x20 回)，サイバーセキュリティ(90 分 x13 回)，セキュリティとビジネス(90 分 x15 回)の座学講義があります. なお，これら 90 分 x68 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(3 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 7 日の課題解決型演習があります.

プロジェクト学習は先進安全なデータ設計特論(90 分 x15 回)があります. 遠隔配信を行いますので，自宅・職場での受講が可能です.

修得単位数は 8 科目(14.5 単位)です.

講義の選択例

春入学

1 年目(9 単位)

・サイバーセキュリティ(1.5 単位)(春～夏学期)
・実践離散数学と計算の理論(2.5 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(2 単位)(夏学期)(集中)
・セキュリティとビジネス(2 単位)(秋～冬学期)

2 年目(5.5 単位)

・先進情報セキュリティとアルゴリズム(2.5 単位)(秋～冬学期)
・実践 CTF(1 単位)(秋～冬学期)(集中)
・先進安全なデータ設計特論(2 単位)(秋～冬学期)

秋入学

1 年目(9 単位)

・セキュリティとビジネス(2 単位)(秋～冬学期)
・実践離散数学と計算の理論(2.5 単位)(春～夏学期)
・サイバーセキュリティ(1.5 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(2 単位)(夏学期)(集中)

2 年目(5.5 単位)

・実践 CTF(1 単位)(秋～冬学期，集中)
・先進情報セキュリティとアルゴリズム(2.5 単位)(秋～冬学期)
・先進安全なデータ設計特論(2 単位)(秋～冬学期)

③ 開発系

理系学部卒同等の知識を有し，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.

講義は先進情報セキュリティとアルゴリズム(90 分 x20 回)，サイバーセキュリティ(90 分 x13 回)，セキュリティとビジネス(90 分 x15 回)の座学講義があります．なお，これら 90 分 x 48 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(3 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 11 日の課題解決型演習があります.

プロジェクト学習は先進安全なデータ設計特論(90 分 x15 回)があります．遠隔配信を行いますので，自宅・職場での受講が可能です.

修得単位数は 9 科目（14 単位）です.

講義の選択例

春入学

1 年目(9 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(1.5 単位)（春～夏学期)
・実践安全な公開鍵暗号の設計と解読 PBL(2 単位)（夏学期)(集中)
・セキュリティとビジネス(2 単位)（秋～冬学期)
・先進情報セキュリティとアルゴリズム（2.5 単位)（秋～冬学期)

2 年目(5 単位)

・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)
・先進安全なデータ設計特論（2 単位)（秋～冬学期)

秋入学

1 年目(7.5 単位)

・セキュリティとビジネス(2 単位)（秋～冬学期)
・実践安全な公開鍵暗号の設計と解読 PBL(2 単位)（夏学期)(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)
・サイバーセキュリティ(1.5 単位)（春～夏学期)
・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)

2 年目(6.5 単位)

・先進情報セキュリティとアルゴリズム(2.5 単位)（秋～冬学期)
・実践 CTF(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)
・先進安全なデータ設計特論（2 単位)（秋～冬学期)

④ 学びなおし

学部卒同等の知識を有し，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．講義は実践離散数学と計算の理論(90 分 x20 回)，先進情報セキュリティとアルゴリズム(90 分 x20 回)，サイバーセキュリティ(90 分 x13 回)，セキュリティとビジネス(90 分 x15 回)の座学講義があります．なお，これら 90 分 x 68 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(3 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 11 日の課題解決型演習があります．プロジェクト学習は先進安全なデータ設計特論(90 分 x15 回)があります．遠隔配信を行いますので，自宅・職場での受講が可能です．

修得単位数は 10 科目（16.5 単位）です．

講義の選択例

春入学

1 年目（12.5 単位）

・サイバーセキュリティ(1.5 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(2 単位)（夏学期，集中）
・実践離散数学と計算の理論(2.5 単位)（春～夏学期）
・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 単位）（春～夏学期）
・先進情報セキュリティとアルゴリズム(2.5 単位)（秋～冬学期）
・セキュリティとビジネス(2 単位)（秋～冬学期）

2 年目（4 単位）

・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）
・先進安全なデータ設計特論（2 単位)（秋～冬学期）

秋入学

1 年目（10 単位）

・セキュリティとビジネス(2 単位)（秋～冬学期）
・実践離散数学と計算の理論(2.5 単位)（春～夏学期）
・サイバーセキュリティ(1.5 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）
・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 単位）（春～夏学期）
・実践安全な公開鍵暗号の設計と解読 PBL(2 単位)（夏学期，集中）

2 年目（6.5 単位）

・先進情報セキュリティとアルゴリズム(2.5 単位)（秋～冬学期）
・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）
・実践 CTF(1 単位)（秋～冬学期，集中）
・先進安全なデータ設計特論（2 単位)（秋～冬学期）

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.

講義は実践離散数学と計算の理論(90 分 x20 回)，先進情報セキュリティとアルゴリズム(90 分 x20 回)，サイバーセキュリティ(90 分 x13 回)，セキュリティとビジネス(90 分 x15 回)の座学講義があります. なお，これら 90 分 x 68 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(3 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 13 日の課題解決型演習があります.

プロジェクト学習は先進安全なデータ設計特論(90 分 x15 回)があります. 遠隔配信を行いますので，自宅・職場での受講が可能です.

修得単位数は 11 科目(17.5 単位)です.

講義の選択例

春入学

1 年目 (12.5 単位)

・サイバーセキュリティ(1.5 単位)(春～夏学期)
・実践離散数学と計算の理論(2.5 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)
・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)
・実践安全な公開鍵暗号の設計と解読 PBL(2 単位)(夏学期，集中)
・先進情報セキュリティとアルゴリズム(2.5 単位)(秋～冬学期)
・セキュリティとビジネス(2 単位)(秋～冬学期)

2 年目 (5 単位)

・先進安全なデータ設計特論(2 単位)(秋～冬学期)
・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)

秋入学

1 年目 (10 単位)

・セキュリティとビジネス(2 単位)(秋～冬学期)
・サイバーセキュリティ(1.5 単位)(春～夏学期)
・実践離散数学と計算の理論(2.5 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)
・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)
・実践安全な公開鍵暗号の設計と解読 PBL(2 単位)(夏学期，集中)

2 年目（7.5 単位）

・先進情報セキュリティとアルゴリズム(2.5 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)
・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)
・先進安全なデータ設計特論(2 単位)(秋～冬学期)

5. コースプラン

タイプ別受講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.

5－1. 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プログラム(暗号春/秋)

実践セキュリティ特論 I,II(4単位, 45h)＋実践離散数学と計算の理論(2.5 単位+30h)＋先進情報セキュリティとアルゴリズム(2.5 単位+30h)＋高度セキュリティ PBL, II,III(4 単位, 22.5+16+12h)
＝13 単位(155.5 時間)

春入学
1 年目(9 単位, 30*2+22.5*2=105h)
・サイバーセキュリティ(2 単位)(春～夏学期)
・実践離散数学と計算の理論(2.5 単位)(春～夏学期)
・セキュリティとビジネス(2 単位)(秋～冬学期)
・先進情報セキュリティとアルゴリズム(2.5 単位)(秋～冬学期)
2 年目(4 単位, 12+16+22.5=50.5h)
・実践安全な公開鍵暗号の設計と解読 PBL(2 単位)(夏学期)(集中)
・実践 CTF(1 単位)(秋～冬学期)(集中)
・高度セキュリティ PBL II(1 単位)(秋～冬学期)(集中)

秋入学
1 年目(6.5 単位, 22.5*2+30=75h)
・セキュリティとビジネス(2 単位)(秋～冬学期)
・実践離散数学と計算の理論(2.5 単位)(春～夏学期)
・サイバーセキュリティ(2 単位)(春～夏学期)
2 年目(6.5 単位, 22.5+12+30+16=80.5h)
・実践 CTF(1 単位)(秋～冬学期, 集中)
・先進情報セキュリティとアルゴリズム(2.5 単位)(秋～冬学期)
・高度セキュリティ PBLII(1 単位)(秋～冬学期)
・実践安全な公開鍵暗号の設計と解読 PBL(2 単位)(夏学期)(集中)

５－２. 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プログラム(サイバー春/秋)

特論 I,II(４単位, 45h)＋３サイバーPBL(3 単位+16*3=48h)＋PBLIII(1 単位, 12h)+ データ設計特論(2 単位, 22.5h)+ PBL(2 単位, 22.5h)＝12 単位（150.時間）

春入学

1 年目(8 単位, 16*2+22.5*3=99.5h)

・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(2 単位)(春～夏学期)
・実践安全な公開鍵暗号の設計と解読 PBL(2 単位)(夏学期)(集中)
・セキュリティとビジネス(2 単位)(秋～冬学期)
・高度サイバーセキュリティ PBL III(1 単位)(秋冬学期)

2 年目(4 単位, 12+16+22.5=50.5h)

・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)
・実践 CTF(1 単位)(秋～冬学期, 集中)
・先進安全なデータ設計特論（2 単位)(秋～冬学期)

秋入学

1 年目(7 単位, 22.5*2+16*2+12=89h)

・セキュリティとビジネス(2 単位)(秋～冬学期)
・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)
・サイバーセキュリティ(2 単位)(春～夏学期)
・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)

2 年目(5 単位, 22.5*2+16=61h)

・先進安全なデータ設計特論（2 単位)(秋～冬学期)
・高度サイバーセキュリティ PBLIII（1 単位)(秋冬学期)
・実践安全な公開鍵暗号の設計と解読 PBL(2 単位)(夏学期)(集中)

５－３. 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プログラム(セキュリティ春/秋)

特論 I,II(4単位, 45h))＋離散数学(2.5 単位+30h)＋先進情報セキュリティ(2.5 単位+30h)＋PBL(2 単位, 22.5h)＋サイバーPBLI or II(1 単位, 16h)+PBLIII(1 単位, 12h)＝13 単位(155.5 時間)

春入学

1 年目(11 単位, 30*2+22.5*3=127.5h)

・サイバーセキュリティ(2 単位)(春～夏学期)
・実践離散数学と計算の理論(2.5 単位)(春～夏学期)
・実践安全な公開鍵暗号の設計と解読 PBL(2 単位)(夏学期, 集中)
・先進情報セキュリティとアルゴリズム(2.5 単位)(秋～冬学期)
・セキュリティとビジネス(2 単位)(秋～冬学期)

2 年目 (2 単位, 12+16=28h)

・包括的サイバーセキュリティ演習(1 単位)(春～夏学期) (集中)
or 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)
・実践 CTF(1 単位)(秋～冬学期, 集中)

秋入学

1 年目 (8.5 単位, 22.5*3+30=113.5h)

・セキュリティとビジネス(2 単位)(秋～冬学期)
・サイバーセキュリティ(2 単位)(春～夏学期)
・実践離散数学と計算の理論(2.5 単位)(春～夏学期)
・実践安全な公開鍵暗号の設計と解読 PBL(2 単位)(夏学期, 集中)

2 年目 (4.5 単位, 30+12+16=58h)

・先進情報セキュリティとアルゴリズム(2.5 単位)(秋～冬学期)
・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)
or 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)

５－４. 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プログラム(総合春/秋)

全ての講義受講(データ設計特論, 特論, 離散と計算の理論, セキュリティとアルゴリズム, 6 PBL 科目)

特論 I,II(4単位, 45h)＋離散数学(2.5 単位+30h)＋先進情報セキュリティ(2.5 単位+30h)＋3PBL(4 単位, 22.5+16+12h)＋3 サイバーPBL(3 単位, 16*3=48h)+データ設計特論(2 単位, 22.5h)＝18 単位(226 時間)

春入学

1 年目(11 単位, 30*2+16*2+22.5*2=137h)

・サイバーセキュリティ(2 単位)(春～夏学期)
・実践離散数学と計算の理論(2.5 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)
・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)
・先進情報セキュリティとアルゴリズム(2.5 単位)(秋～冬学期)
・セキュリティとビジネス(2 単位)(秋～冬学期)

2 年目 (7 単位, 22.5*2+12+16*2= 89h)

・実践安全な公開鍵暗号の設計と解読 PBL(2 単位)(夏学期, 集中)
・先進安全なデータ設計特論(2 単位)(秋～冬学期)
・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)

秋入学

1 年目(9.5 単位, 22.5*2+12+30+16*2=119)

・セキュリティとビジネス(2 単位)(秋～冬学期)
・実践 CTF(1 単位)(秋～冬学期, 集中)
・サイバーセキュリティ(2 単位)(春～夏学期)
・実践離散数学と計算の理論(2.5 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)
・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)

2 年目 (8.5 単位, 30+16*2+22.5*2=107h)

・先進情報セキュリティとアルゴリズム(2.5 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)
・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)
・先進安全なデータ設計特論(2 単位)(秋～冬学期)
・実践安全な公開鍵暗号の設計と解読 PBL(2 単位)(夏学期, 集中)

6. 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.

コース名 / 科目名	メインコース(120 時間以上)				クイックコース(60 時間以上)				
	総合	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・
実践セキュリティ特論 I, II	必修	必修	必修	必修	必修		必修	選択 B	選択 B
実践離散数学と計算の理論	必修	必修	必修			必修		選択 E	
先進情報セキュリティとアルゴリズム	必修	必修	必修			必修		選択 E	
高度セキュリティ PBL	必修	必修	必修	必修	選択 C	選択 B		選択 C	選択 D
高度セキュリティ PBL II	必修		必修			選択 B		選択 C	選択 D
高度セキュリティ PBL III	必修	必修	必修	必修	選択 C			選択 C	選択 D
高度サイバーセキュリティ PBL I	必修	選択 A		必修	選択 C		必修	選択 C	選択 D
高度サイバーセキュリティ PBL II	必修	選択 A		必修			必修	選択 C	選択 D
高度サイバーセキュリティ PBL III	必修			必修			必修	選択 C	選択 D
先進安全なデータ設計特論	必修	選択 S		必修	選択 S			選択 S	
ネットワーク経済学	自由選択								

【必修】必修科目

【選択 A】高度サイバーセキュリティ PBL I or 高度サイバーセキュリティ PBL II から 1 単位選択

【選択 B】講義科目・PBL 科目から選択(1 単位以上選択)

【選択 C】PBL 科目から選択(2 単位以上選択)

【選択 D】PBL 科目から選択(4 単位以上選択)

【選択 E】講義科目から選択(2.5 単位以上選択)

【選択 S】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 S 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 S →アドバンスド暗号メインコース

・修了認定について

科目等履修生高度プログラムの履修可能期間での単位取得状況に応じて，修了認定します．
例えば，
+2022 年度春夏学期科目等履修生高度プログラムに入学の場合
2024 年度秋冬学期までの期間での単位取得状況に応じて認定し，その期間で暗号メインコースを修了された場合，2024 年度暗号メインコース認定となります．
+2022 年度秋冬学期科目等履修生高度プログラムに入学の場合
2024 年度春夏学期までの期間での単位取得状況に応じて認定し，その期間で暗号メインコースを修了された場合，2024 年度暗号メインコース認定となります．
　なお，先進安全なデータ設計特論の受講の条件は該当 2 年間にクイックコースを修了していることとなります．

・再受講

　講義の内容は毎年少しずつ更新されます．
一度認定されても新しい知識の習得のために，再受講していただくことをお勧めします．

再入学時には，その期間で修得した単位に応じて新たに認定書を授与します．

7. 教員紹介

樽谷　優弥(大阪大学)

2014 年 大阪大学大学院情報科学研究科情報ネットワーク学専攻博士後期課程修了. 博士(情報科学).

2014.10～2018.11 大阪大学サイバーメディアセンター 助教, 2018.12～2021.3 岡山大学大学院ヘルスシステム統合科学研究科 助教、2021.4～2024.3 岡山大学学術研究院ヘルスシステム統合科学学域 助教を経て、2024.4 より大阪大学大学院工学研究科 講師(現在に至る)。主な研究分野は情報ネットワーク, ネットワークセキュリティ、ネットワークシステムに関する研究に従事。

[受賞歴]

- 2019.9 FIT 奨励賞
- 2014.2, IEEE 関西支部学生研究奨励賞

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.

高野 祐輝(株式会社ティアフォー)

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～2022 年 3 月まで同学特任准教授として勤務. 2022 年 4 月より株式会社ティアフォーで勤務し自動運転の研究開発に従事. 2022 年 4 月より, 大阪大学 招へい准教授.

[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.

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 (パナソニック株式会社)

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

北条 孝佳（西村あさひ法律事務所・外国法共同事業）

電気通信大学大学院電気通信岳研究科博士前期課程修了。警察庁技官として 10 年以上多くのサイバー攻撃事案の解析、支援及び研究業務に従事。現在は、企業内における不祥事対応、危機管理対応等を中心に、様々なサイバーセキュリティ事案の調査・法的措置・再発防止策に関するアドバイスを実施。埼玉県警察本部・サイバー犯罪対策技術顧問、国立研究開発法人情報通信研究機構・招聘専門員、NPO デジタル・フォレンジック研究会・理事等、多くの顧問・理事等に就任。内閣サイバーセキュリティセンター、総務省、経産省等の委員にも歴任。警察大学校・都道府県警察本部の外部講師等も数多く担当。

[受賞歴]
-Microsoft MVP 受賞(2017 年-2023 年)

[近時の執筆参加著書]
-ランサムウェア攻撃に対する捜査ハンドブック(2024 年、立花書房)
-サイバーリスクマネジメントの強化書(2023 年、日刊工業新聞)
-情報刑法Ⅰ　サイバーセキュリティ関連犯罪(2022 年、弘文堂)
-法律実務のためのデジタル・フォレンジックとサイバーセキュリティ(2021 年、商事法務)
等、執筆多数。

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）

大塚　玲（情報セキュリティ大学院大学）

大阪大学大学院工学研究科博士前期課程修了．東京大学大学院工学研究科電子情報工学専攻博士課程修了．博士(工学)．
情報セキュリティ大学院大学情報科学研究科教授．

民間企業，東京理科大学，城西大学，北陸先端科学技術大学院大学の講師を経て現職．
情報セキュリティ，暗号プロトコル，機械学習（特にバイオメトリクス）のセキュリティの調査研究を行っている．

[著書]

- IT Text 情報セキュリティ（共著，オーム社）

8. 講義のシラバス

8.1 サイバーセキュリティ

[開講科目名]
(授業科目)実践セキュリティ特論Ⅰ／(enPiT-Pro)サイバーセキュリティ
[単位数/時間数] 1.5 単位/18 時間
[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)
[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.

【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ー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ー策定設計を行う..

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

[評価の観点] 教科書的知識のみならず自身の考え方を明確に述べ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

[評価の観点] 教科書的知識のみならず自身の考え方を明確に述べ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，不正なソフトウェアの挙動を分析する手法について取り上げる．

[授業の目標]

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 サイバー攻撃の動向概論

近年，サイバー攻撃の被害が増加しており，社会的な対策の必要性が高まっている．
どのような攻撃者が，どのような攻撃手法を使っているかなどについて対策と併せて紹介する．
- インシデント傾向 - サイバー攻撃の動向
- 組織におけるセキュリティ対策

第 2 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ります．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びます．
- 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

第 3 回　バイナリ解析(1)

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

第 4 回 バイナリ解析(2)

コンピュータ上で不正なソフトウェ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．

－ デバッガを用いたバイナリ分析演習　－ 不正なソフトウェアへの対策

[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

[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]

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－

[評価の観点] 教科書的知識のみならず自身の考え方を明確に述べることをより評価する．

[評価方法]　レポート成績

8.2 セキュリティとビジネス

[開講科目名]

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

[単位数/時間数] 2 単位/22.5 時間

[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 (パナソニック株式会社), 大塚 玲（情報セキュリティ大学院大学）, 宮地 充子(大阪大学)

[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.

【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 のデータ保護規則, カリフォルニア州消費者プライバシー保護法

[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 のデータ保護規則やアメリカのカリフォルニア州消費者プライバシー保護法などを概観し, 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）

[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）

[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

[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）

[評価の観点]

[評価方法] レポート成績

【ブロックチェーン理論】（担当：大塚 玲）

[授業の目的・概要]

ブロックチェーンを構成する諸理論を正しく理解する.

[授業の目標]

ブロックチェーンが実現する合意形成技術を基礎理論から理解することを通じて，現代社会に広がりつつある暗号通貨，スマートコントラクトの仕組みと安全性・リスクについての深い理解を得ることを目標とする.

[知識単位]

ブロックチェーン，暗号理論

[講義計画]

- Permissioned Blockchain
第 1 回 ブロックチェーンの基礎
第 2 回 コンセンサス
第 3 回 ビザンチン合意とブロードキャスト
- Permissionless Blockchain
第 4 回 結果整合性とビットコイン
第 5 回 Ethereum とスマートコントラクト
第 6 回 Selfish Mining と共通プレフィックス定理

[準備学習等の具体的な指示]

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.
- 暗号理論
- マルチパーティ計算

[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）

[教科書・教材]

Roger Watenhofer, Blockchain Science: Distributed Ledger Technology, Inverted Forest Publishing; 第 3 版 (2019/1/22).
大塚 玲，"ブロックチェーンを利用した暗号資産の安全性と匿名性：原理と限界，" 日本銀行金融研究所ディスカッションペーパーシリーズ（日本語版） 2021-J-4.

[評価の観点] ブロックチェーン理論の理解

[評価方法] レポート成績

8.3 実践離散数学と計算の理論

[開講科目名]

(授業科目)実践離散数学と計算の理論／(enPiT-Pro)実践離散数学と計算の理論

[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), 王 イントウ(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∀やヨ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

[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%)

8.4 先進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), 王 イントウ(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 を用いた実践離散数学, 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．
知識単位：並行プログラミング，モデル検査

[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. 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%)

8.5 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）

[開講科目名]

（授業科目）高度セキュリティ PBL／（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）]

High-Level Security PBL

[単位数/時間数] 2 単位/22.5 時間

[開講日] 夏学期

[担当教員]

宮地 充子

[開講言語]

日本語・英語

[授業の目的・概要]

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公開鍵暗号の各種応用についても学ぶ．

[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 グループ課題
第 8 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 9 回. 暗号プロトコルや署名の応用公開鍵暗号とディジタル署名で新たな方式を実現してみよう
知識単位:暗号プロトコル,
第 10 回 ハイブリッド暗号
知識単位:ハイブリッド暗号
第 11 回 ハイブリッド暗号の実装
知識単位:文字コード, 暗号と署名の組み合わせ, ハイブリッド暗号
第 12 回 最終課題発表

[履修条件・受講条件]

「実践離散数学と計算の理論」か「先進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

[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%)

8.6 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 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]

OH1 回 本講義に必要な事前課題, 事前準備の説明

OH2 回 本講義の中間内容までに関する質問.

OH3 回 本講義の全内容に関する質問.

第 1 回 準同型暗号の基礎及び Ring-LWE 導入のための数学の基礎

知識単位:準同型暗号, 多項式環の剰余環, 高速フーリエ変換による多項式の高速乗算, 数論変換

第 2 回 Python による剰余環, 数論変換, 数論変換による多項式の高速乗算の実装

第 3 回 LWE 問題, Ring-LWE 問題と Ring-LWE 問題に基づく制限付き準同型暗号

知識単位:LWE 問題, Ring-LWE 問題, BGV 方式, BFV 方式

第 4 回 Ring-LWE ベース準同型暗号(BGV 方式, BFV 方式)の実装

第 5 回 BGV 方式と BFV 方式のレベル付準同型暗号化
知識単位:鍵変更, モジュラス変更, 再線形化
第 6 回 鍵変更, モジュラス変更, 再線形化を適用した BGV・BFV 方式の実装
第 7 回 BGV・BFV 方式の比較実験及び成果発表準備
知識単位:BGV・BFV 方式の効率とノイズの増加率
第 8 回 成果発表とまとめ

[履修条件・受講条件]
「実践離散数学と計算の理論」か「先進情報セキュリティとアルゴリズム」,「高度セキュリティ PBL」を受講済みであることが望ましい. 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.

[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.

8.7 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 単位/12 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

[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．

8.8 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 単位/16 時間

[開講日] 春学期

[担当教員]

明石 邦夫（東京大学），高野 祐輝(ティアフォー)，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 回，第 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 回，第 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 等の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」

[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

8.9 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 単位/16 時間

[開講日]春学期

[担当教員]

高野 祐輝(ティアフォー), 宮地 充子(大阪大学)

[授業の目的・概要]

プログラミング言語 Rust は，型システムを適用して安全なソフトウェアを実装するのに適したプログラミング言語である．

本講義では，Rust を用いて，コンピュータの基礎となるデバッガとレジスタマシンの実装を行い，セキュリティの基礎技術を学ぶ．

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．

また，それらを Rust で実装する手法を学ぶ．

(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 UNIX OS とコンピュータのしくみ
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 回 プログラミング言語 Rust
プログラミング言語 Rust を用いて, 安全なシステムソフトウェア実装を行う手法を学習する.
第 4, 5 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 6, 7, 8 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て学習する.
第 9 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 10, 11 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]

クイックコースを修了済み, あるいは, メインコースを受講中であること.

[準備学習等の具体的な指示]

Rust とコンピュータでのメモリの扱い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
Jim Blandy, Jason Orendorff, Leonora F. S. Tindall,「プログラミング Rust 第 2 版」, オライリー・ジャパン
高野 祐輝,「並行プログラミング入門」, オライリー・ジャパン

[評価方法] 演習と発表 50 点, レポート 50 点

[評価基準]

優:Rust によるセキュアプログラミングについてついて十分に理解し, 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:Rust によるセキュアプログラミングについて理解し, 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

8.10 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 単位/16 時間

[開講日]春学期

[担当教員]

明石 邦夫（東京大学), 高野 祐輝(ティアフォー), 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．

[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

8.11 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/時間数] 2 単位/22.5 時間

[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）

8.12 先進安全なデータ設計特論

[開講科目名]

先進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] 2 単位/22.5 時間

[開講日] 秋冬学期

[担当教員]

宮地 充子, 王 イントウ, 奥村 伸也

[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.

第 2-5 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・知識に合わせたプロジェクト分けを実施する.

第 6-8 回 中間発表会

プロジェクト内での検討成果を発表する.

第 9－12 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. 各自の検討結果を定期的にグループ内でディスカッションを実施する.

第 13－15 回 最終発表会

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

[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%)

9. 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.

9. 1 離散数学と計算の理論

〈2021 年〉

[離散数学]

・1 回目

・部分群や有限群などについて, これまで知らなかった内容だったので, 新たな内容を学習でき, 勉強になりました.

・ある群の部分集合が部分群となるための証明の立て方について, 直前に示した内容を次示したいことに利用する手法.

・生成元関係の話はあまりわかっていなかったので勉強になった.

・半群, 単位元, 単位元の一意性, モノイド, 逆元, 群, 群の公理, 部分群, 有限群, 有限群, 生成元について整理出来た.

・有理数の考え方が群に繋がっているということ

・2 回目

・正規部分群の定義とその意味について, 学部時代のときはいまいちピンと来ていなかったが, そのときよりも理解が深まった.

・ラグランジュの定理はいまひとつ理解していなかったので勉強になった. 正規部分群なども知らない概念だったため勉強になった.

・同値, 同値類の考え方がわかった

・剰余類についての学びが勉強になりました

・3 回目

・環が今回出てきたが, 符号理論などとも関係してくる分野である一方, あまり理解していなかったので勉強になった.

・写像がまったくわからなかったのですが, 宮地先生にご説明いただいて, もう一度勉強したらわかる気がしてきました. ありがとうございます. あと些細なことで恐縮ですが, ζ の意味を調べなくてもいいですよ, といっていただいて, 非常に気分的に楽になりましたありがとうございます.

前回レポートでどう入力するかわからなくて, ものすごく苦労していました. (前回マスターできました)

・4 回目

・イデアルの復習, 整域, 体, 有限体, 単数群, 零因子

・well-defined(の理解)の重要性

・今回の授業では具体例が多く登場したので, 環や整域について理解が深まりました

・準同型を使うことで先生が言う「グローバル」と「ローカル」へ移った時の分析が対応できるようになるところ

・5 回目

・ユークリッドの互除法のアルゴリズムの本質について教えていただいたこと

・単数群の位数, 単数群の生成元

・中国人の剰余定理から，同型写像によって計算することなど今までの授業が繋がったところ
・基本的なところから教えていただいてはじめて CRT をどう使うのかがわかりました．ありがとうございます．
・同値類の同値関係など，あいまいに覚えていたことが明確になってよかったです．
事前の演習が予習となり，授業の内容が想像できたので分かり易かったです．
・演習
・ラグランジュの定理の理解が若干怪しかったため再確認できてよかった．
・補足部分の説明
・問題の解説を通して生成元や余剰群に関する理解が深まった．具体例の提示もしてくれたので助かった．
・ラグランジュの定理を使うところ
・可約，既約の考え方
・剰余群や環についての理解がより深まりました．
・多項式の問題がわからなくてものすごく悩んでいたので，そうやって解くのか・・と感動しました．ありがとうございます．よくわかりました．
・単数群の群構造，単数群の生成元，中国人剰余定理による計算量削減，オイラー関数
・生成元の個数， U(Z/8Z)が生成元を2個持つこと CRT
・問題の解き方についてよく分かり，より授業の内容が理解出来ました．
・オイラー数を使い，問を解くこと
・U(Z/nZ)の部分群の数の解説が参考になりました．試験の事前に練習問題を作成して頂いたので対策になりました．
・課題の説明がとても丁寧にご説明いただきました．

[計算の理論]

・1 回目
・形式的な証明の具体的な記述方法は知らなかったため，とても勉強になった．
また，コンピュータ上での応用も具体例が少し紹介されていたので具体的なイメージが湧きやすくなった．
・部分証明を用いた証明
・推論規則，形式的証明の概念を知ることができた
・論理的な考え方．今までなんとなくしていた作業が明らかになって面白かったです．
・2 回目
・述語論理，実体化規則，汎化規則
・限量子は今までなんとなく使っていたことがあったが，厳密な書き方等は知らなかったため，勉強になった．
・自然言語をどのようにして論理式と対応させるかについて．
・規則の誤った適用の，なぜ失敗になるかの説明
・「ある」や「全て」の記号の使い方や述語論理の形式化について勉強になりました． - ∀やヨを，∧ や∨ に置き換えた時の表現
・3 回目
・原始帰納的関数などは完全初見で勉強になった
・Coq を通してコンピュータでどのように計算が定義されているかを学べたことです．
・帰納的関数の考え方について分かりました．

・チューリングマシンについての説明がきけたこと

・4 回目

・健全性，完全性，無矛盾性，素朴集合論，ラッセルのパラドックス，ペアノの公理

・ゲーテルの不完全性定理

・いわゆる「証明」について厳密には知らなかったため勉強になった

・不完全性定理が何を示すための定理なのかがわかった．

・ゲーデルの不完全性定理を理解するための重要な定理や公理等を理解出来ました．

・5 回目

・λ 計算はプログラミングでもよく使っており，由来や実際の動作はあまり 知らなかったので勉強になった．

・カリー化について

・評価戦略という概念が勉強になりました

・6 回目

・静的型付けと動的型付け

・型推論の流れはとても勉強になった

・型付き λ 計算の例についての解説

・7 回目

・ホーアの 3 つ組は全く知らなかったので勉強になった．

・証明の流れについてよく分かりました．

・ホーアの三つ組みの話をていねいに教えていただいたこと

・ゲーデル不完全定理のところが，色々な本読めたので勉強になりました．COQ は，優しいですが RUST のプログラムは難しいです．

＊講義全体に関する意見

・数学の講義は受動的な講義が一般的ですが，課題による演習が多く手を動かして学んでいくので，去年と比べて内容もグレードアップして理解度があがったと思います．計算の理論の講義で COQ，ホーア論理が追加されています．私はできるだけ教室で受講するようにしましたが，感染対策の為オンラインで受講する方が多かったように思えます．どちらか選んで受講できるので，途切れずに続けることができたと思います．

・非常にていねいな授業と後から見直すことのできる環境をご用意いただき，リモートの環境下でありながら非常に助かりました．ありがとうございました．質問に対しても迅速，かつていねいにいつも答えていただき大変感謝しています．今年は，大学の数学の教科書を取り寄せて勉強しなおしながら受講しましたので，先生方の授業の理解が進みました．

〈2020 年まで〉

・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．
・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は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．

９．２実践情報セキュリティとアルゴリズム

〈2021 年〉

[セキュリティ編]

・1 回目
  ・昨年度も受講しましたが，最後まで終わらなかったので学び直しとして受講しています．群・環・体と Euclid の互除法の基礎からの復習になりました．
  ・計算時間のようなサイドチャネル攻撃等に利用可能な情報を与えてしまう可能性について学べた．
  ・拡張 Euclid 互除法を行列で表すことが出来る事
  ・基礎から学べたので，わかりやすかった．
  ・高校でも微分積分と行列を触り程度に習った程度で大学では数学を履修していなかった為，殆ど全てが新しい概念でとても勉強になりました．
  ・フェルマーの小定理と拡張ユークリッドの互除法では，計算プログラムの視点から考えると，計算コストが異なるということ．
  ・整数だけでなく，正則行列も環となるところ．
  ・群，環，体に関する基本的な知識の復習
  ・離散数学の復習だったので特にないです．
  ・群，環，体について改めて整理できた
  ・剰余環，体，フェルマーの小定理について

・拡張ユークリッドの互除法で逆元が求まる仕組みを理解することができた．拡張ユークリッドの互除法とフェルマーの小定理で逆元を求めることができることは知っており，逆元を求める際は拡張ユークリッドの互除法が使われる(計算量の面で)と思っておりましたが，攻撃者へのヒントを与えることになるという理由でフェルマーの小定理もありというのは新たな視点だった．

・2 回目

・同種写像の具体的な作り方の説明がわかりやすかったです．事前の予習では結果はわかってもなぜそうなるか理解できていませんでした．

・同種写像の定義

・楕円曲線の加法の仕組み

・楕円曲線上の演算

・楕円曲線の性質についてよく分かりました．

・3 回目

・j 不変量が一致しても元の個数が一致しない例を，事前課題で自分で確かめることができてよかったです．実例があるととてもわかりやすかった．

・前期の授業では理解できなかった型システムについて，少し理解できたような気がします．

・jacobian 座標系について

・4 回目

・公開鍵暗号の基礎からの説明で，わかりやすかったです．

・暗号化と復元の仕方について分かりました．

・有限体上の暗号と楕円曲線暗号について

・5 回目

・楕円曲線暗号については理解出来ました．

・(演習)

・問題演習を通して前回の授業内容が理解出来ました．

・mod の性質について

・オイラー関数を使うと，位数 N となる元の個数を求めることができる

・python での無限遠点の扱い方でした．自分では省略して実装していました．

・有限体上の楕円曲線の公式の利用の仕方について分かりました．

・演習 3.1 の(X, Y, Z)=(X*t^2, Y*t^3, Z*t)となる t を求めるプログラムが自分で作ったものはとても処理が遅かった (t の約数で順番に計算していたので)のですが，X, Y, Z の最大公約数を求めればよいと説明されて，なるほどその方法があったか，と勉強になりました．

・いつもコードが長くなっていたので短くなるような工夫の仕方が分かりました．

[アルゴリズム編]

・1 回目

・型検査とエラーハンドリングの重要性について．

・rust 言語の概要

・メモリ管理について，参照カウンタや循環参照などで起きるバグについて具体的に知ることが出来，とても勉強になりました．また大学院で情報処理やセキュリティの難しい講義を受けることでエッセンシャルなシステムを構

築出来る人材になれるという説明は大学院で学習していくモチベーションになりました.

・参照カウンタの仕組みが，例を用いて実際に各段階に挙動を見せながら説明してもらえて，とても分かりやすかった.

・Rust が Python などと比べて，何故安全な実装をしやすいのか

・作るプログラムによって，言語の向き不向きがあるということ．暗号の実装に安全性の高い言語を使ったほうがいい，などは初めて聞いたのでとても参考になった.

・参照について具体例を示してくれたので理解しやすかったです.

・python 等がアプリケーションを作るために使いやすい言語ではあるが，セキュリティ面で脆弱性が生まれてしまう可能性がある危険な言語であるため，重大な責任が伴うシステムを設計する場合は Rust などの安全な言語を使用するようにするという点が勉強になりました.

・普段プログラムを書くときには意識していなかったが，裏でメモリの管理が行われていること

・直積型と直和型の違い 直和型については普段意識したことがなかったため．GC の種類について 参照型，Mark and Sweep に関するスライドが非常に分かり易かった.

・型安全な言語という概念

・Option 型などを用いることで型検査をしていることを理解することができた．GC がメモリ管理を行うものであることは知っていたが，どのように管理しているかは知らなかったので，参照カウンタや mark and sweep の話はとても面白かった.

・2 回目

・昨年度秋も受講し，今回再受講です．ここまではわかりやすいです.

所有権と借用がでてきたので，そろそろ難しい（従来の言語にはなじみが薄い）ところに入るので，基礎から復習します.

・借用の簡易モデル

・Option 型と Result 型の使い方（パターンマッチ） 借用時の変数の変数の状態の簡易モデルの説明

・3 回目

・線形型システム全般

・論理学自体あまり触れたことが無い学問でしたが，リソースの消費を示す事が出来る線形論理は面白いなと感じました.

・難しかったですが，証明図の流れは少し理解しました.

・型付け規則に線形論理が使われていること

・線形論理

・4 回目

・線形システムについてまだイメージだけですが，何となく掴めた気がします.

・rust での型環境の実装や型付けについて

・5 回目

・並行プログラミング，メモリバリア

・型計算

〈2020 年まで〉

［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．

9．3 サイバーセキュリティ

＜2021 年＞

[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]

・セキュリティはガバナンスから取り組むことが重要であること．
・セキュアな情報システムを構築するには，上流工程である要求定義からセキュリティを意識することが大事であること．システムの安定化を計画する際に重要となるのは，平均故障間隔・平均修理時間ではなく，効率低下率と修理時間を抑えることである．
・ これまで習った技術がどのようにセキュリティに関連するかを学ぶことができたことが最も勉強になった点です．

・インシデント対応（入念に偵察されて組織ぐるみで波状攻撃されると防御側は厳しい）
・Secure by Design について具体的なバグの例，レジリエンスの考え方
・もっとも勉強になったのは，公開鍵暗号などの暗号理論だけでなくセキュリティ全般に，「全くミスがない」ことではなく，「やられても大丈夫」(暗号なら公開鍵を知られても大丈夫，共通鍵ならバレたら終わり)という前提で対策を練る考えを重視しているように感じたことである．
・″セキュリティにとっては故障間隔 F より効率低下 I と修理時間 R を抑える方が大切″という点が，システムの構築以外の分野でも似たような考え方に使えそうだと思った．
・元々セキュリティという分野自体，開発の下流工程(実装的部分)に近い側面でしか知らなかったため，上流工程でのセキュリティは自分にとって未知の観点であったため，勉強になった．
・ウイルスソフトが万能ではないということ
・不正アクセス等，情報システムが悪用されるまでの仕組みがよく分かりました．
・セキュリティ要求工学という分野の存在を知らなかったので，その存在や要素，具体的な手法について知ることができ，勉強になりました．
・具体的なセキュリティの問題，それを解決するための具体策とその歴史について．
・スタックオーバーフローの危険性 授業で C 言語を扱っている際に何度も起こしたことがあり，身近な内容だった．これがセキュリティを脅かす理由がわかり勉強になった． 自分で開発をする際に C を選ばないようにしようと思った．
・「セキュリティ要求工学」を初めて知り，設計をセキュアにという考え・手法がとても勉強になりました．
ほかにも，具体的なセキュリティリスクをご紹介いただき，システムの運用計画にセキュリティの要素を入れる（特に，平時正常に動作しているかを「能動的に」チェックする）ことも勉強になり，普段の実務に活かしていきたいと思いました．
・セキュリティフレームワーク
・基本的な用語の定義（システム，情報，情報システムなど）
・境界線防御，ゼロトラスト，NIST の基準書，ICMP の悪用
・今回の講義内容はかなり具体的な処理が多く，全体的に勉強になった．
特にファイアウォールは当たり前のように使用している一方，細かい仕組みは知らなかったので理解は深まった．また，思ったより簡易的な構造であるにも関わらず境界を敷くには十分で興味深いと感じた．
・情報システムの防衛の仕方についてよく分かりました．
・FW について詳しく知ることができた． 利用方法や FW が有効な攻撃がより具体的にイメージできるようになった．SQL インジェクションはエスケープで対処すると，教科書で学んでいたので，エスケープでは逃げ切るのが困難なケースもあることを学ぶことができて有益であった．
・ファイアウォールの重要性（Fail safe），実例，Stateful なファイアウォールと， NAT も状態管理が必要で定期的に通信させておくこと，LAN を細かく分離する（LAN どうしを通信させない）こと，ZeroTrustNetwork がもっとも勉強になりました
・FAT，NTFS，SED，ライブフォレンジック
・ライブフォレンジック
・HDD やメモリの仕組みやファイルシステムについてよく分かりました．
・デジタル・フォレンジックという言葉と，それに関する知識．

・横浜 CSRF 事件，証拠の真正性が裁判で争われることがあること，ファイルシステムの構造，データを復元できない確実な方法，ライブフォレンジック，今後話題になるであろうメディア・フォレンジック．
・FS の様々な種類

[リスクマネジメント・インシデント対応]

・セキュリティのインシデントの約 7 割が人的ミスによるという事実を知り，人に対するシステムの重要性を再認識した．（社外に PC,USB 持ち出し禁止等）
・ソーシャルエンジニアリング攻撃の具体的な名称（ネームドロップ，テクニカルワードなど），インシデント事例の半分は人的ミスであること，信頼性・責任追跡性・真正性，JIS Q 27000
・ソーシャルエンジニアリング（注意が必要なメールの見分け方等）・ISMS，情報セキュリティポリシーについて
・情報セキュリティのポリシー作成に 3 段階の基本構造を持たせるのが basic な手法であるということ．
・インシデントの発生理由のうち紛失や誤操作のような人為的なミスが思っていたよりも多いこと．ここまでとは思っていなかった．また旧姓や生年月日といった「変えられない情報」に価値があるという視点は持っていなかった．
・ソーシャルエンジニアリングによる情報流出の割合が高いということ
・ソーシャルエンジニアリング攻撃の様々な実例から概要を理解出来ました．
・情報セキュリティの3大要素
・CIA の概要と実例
・ちゃんとタイムスタンプ付きでログを取っていても，そのログが正しいものと証明するのは難しいという事．情報漏洩の一番の原因が人的要因であること 実際に起こったインシデントの話
・情報セキュリティが技術だけでなく，心理学，経済学など多岐にわたる点や，企業の IR にも関わることを具体例でよく分かりました．また，約8割がサイバーセキュリティ以外のインシデントだということも勉強になり，「情報は消えない」という怖さから，リスク低減のための情報セキュリティ教育を普段から実施していこうと考えさせられました．
・組織としてのセキュリティポリシーとその歴史
・情報セキュリティポリシー
・ISMS の取得
・実際に ISMS を取るまでの流れなど
・練習問題を通じて，ISMS やトップマネジメントについて理解することが出来ました．
・組織の経営層がいかにセキュリティの意識と責任をもつかということ． ISMS の認定は多くの項目があり，容易に取得できないということ．
・セキュリティポリシーについて
・ISMS について，特に組織にその考えを浸透させているか，トップマネジメント（リーダーシップとコミットメント）がもっとも勉強になりました．千葉大学やベネッセ，資料に記載されていない，講義でご説明いただいた事例など，とてもためになりました．
・組織目標としてのセキュリティポリシー
・ISMS の歴史

[ログ分析・バイナリ解析]

・ログ解析の実践演習，相関分析
・さまざまなログから不正な接続先，被害を受けた端末などを調べることができること，また，その方法を知ることができてよかったです．

・プロキシログ分析など，説明は聞いたことがあるもののあまり具体的なイメージができておらずCTF を通じて十分理解できるようになってよかった．実際にはここまできれいに見つけられるものではないのかもしれないが，原因を突き止められるのは気持ちよさがあった．特に共通ユーザーエージェントから不正な操作を導き出すところなどはより実践的なように思えた．
・実際に手を動かしたので，不正なアドレス等を検知する仕組みが分かった．
・実戦形式でログを検索したところ．ログを取っておくことの大切さと，原因追及の難しさを身をもって体感できた
・プロキシログは内→外を，FW ログは内→内を，AD ログはアカウント←→端末を，相関分析は内→内→外を分析するということ．あと，演習の目的が原因の追究方法を理解し，インシデント対応の勘所をつかむということで，プロキシログの送信元と送信先が重要，またユーザーエージェントがヒントになることがあるということが良く分かりました．－ 演習による各種ログ（AD，Proxy，FW）の解析方法
・プログラムとハードを関連させて理解できたこと（メモリのどこを書き換えているのか？レジスタとメモリの違い等）
・Buffer Overflow が起きる仕組み
・デバッガ―の使い方，バッファオーバーフローの演習，カナリヤ
・バッファオーバーフローによるプログラム書き換えの仕組みを詳しく説明してくださったのが印象に残りました．
・スタックオーバーフローによる攻撃が実際にどのように行われるか，利用されているかを知ることができた．
・アドレスの書き換えなどを実際のマシンで試したことはなかったので参考になった
・データの書き換えについて具体例を交えてくれてかなり分かりやすかったです．
・バッファオーバーフローの攻撃手法の流れ．
・メモリとスタック領域，EIP，バッファオーバーフローによるリターンアドレスの書き換え．
・ポインタ書き換えの実践
・バッファオーバーフローや，リターンアドレスの書き換えなどの仕組みは知っていたつもりでしたが，プログラム上でそれらの動作をトレースすることができ，より理解を深めることができました．
〈2020 年まで〉
・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．
・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アウォールについては，演習で行なった規模を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.

9．4セキュリティとビジネス

〈2021 年〉

[情報の法的価値と法的規制]

・データを取り扱う上での「個人情報」「仮名加工情報」「匿名加工情報」の分類が勉強になりました.

・「個人情報である仮名加工情報」と「個人情報でない仮名加工情報」

・個人情報などの法律関係は，法律関係の仕事を行う人だけが詳しく知ってある必要があると思ったが，事業者あるいは会社員までもが把握していなければ，重大なリスクがあるということ. システム開発一つにしても，個人情報の法律を考慮した仕様にしなければならなく，ビジネスの設計にも大きく影響を与える存在であるということが勉強になりました.

・個人情報に関する法律についてよく分かりました.

・他国の個人情報保護法，他国との個人情報保護法の域外適用（サーバーをどこに置くかによってどの国の法律が適応されるのか）について. 個人情報保護法の改正に至る事件や経緯について.

・GDPR，破産者マップ事件を受けて不当な目的で利用できなくすること，死んだら個人情報を保護されないこと，個人情報の「保護」と「利用」のバランスの難しさ.

・各国の個人情報の取り扱いの話が面白かったです.

・違反，執行理由が「法的根拠が十分でない」と知り，驚愕です. そして 1 億円の平均課徴金額. 問われてからでは手遅れで，個人データの管理，処理を取り行う前から様々な観点において，「こんなケースは大丈夫だろうか？」と考えておかないといけないのですね.

・GDPR の存在・内容，適用対象について

・個人データの管理者(Manager)と処理者(Processor)，保護される個人データの地理的範囲

[金融業務における暗号技術の応用と国際標準化]

・金融と暗号の関係関係

・日本に暗号が普及した理由，技術面ではなく，普及しない理由

・セキュリティ関連の歴史的背景についてよく分かりました.

・暗号技術が金融業界と密接に関係していたこと，むしろ金融業界から暗号技術が始まったという歴史を知り大変興味深いお話でした.

・日銀が暗号のパイオニアであること，暗号の強度低下・耐用年数，ムーアの法則

・金融業務による認証方式の変遷について

・暗号資産の目的と危うさ

・ブロックチェーンの取り扱い方法二つ（オフチェーン取引とオンチェーン取引）の実態

・暗号資産の値上がり値下がりの要因などが分かりました.

・ビットコイン技術は昔から研究されていた暗号資産であることを知りました（ブロックチェーン技術よりも）．もともとは取引の匿名化をするためのものであったにもかかわらず，現状はまた違った使われ方をしていてこの先どうっていくのか気になります．
・ビットコインや仮想通貨業界の歴史
・ビットコインの仕組み（センターをもたず二重使用を防ぐ仕組み）オンチェーン取引とオフチェーン取引の違い．
・暗号資産の概要を理解するのにブロックチェーンの基礎が最も勉強になった．

［IoT 先端技術とその展開］

・大企業は 1→100 にするのは得意だが，0→1 は苦手としている． 一方でベンチャーは 0→1 が得意である．
・VR のデモがとても興味深いものでした．
・身の回りのあらゆる製品が，IOT 化することによって，新たな価値が 生まれてくるということが具体的によくわかりました．そして，新製品を生み出す原動力に遊び心とでもいえるものがあると いうことがイメージできました．
・IoT 機器のインターネットへの接続方法として主に3つあり（スマホ経由，直接（Wi-Fi），直接（3G,4G,5G）の3パターン），その中で，最も直接（Wi-Fi）のセキュリティ的に危険度が高く，直接（3G,4G,5G）は危険度がそこまで高くないということ
・IoT を活用した様々な製品が見れて良かったです．
・0 から 1 を生み出すことがいかに大変なことが勉強になりました．
・IoT が Wifi 等直接サーバー側に繋がっているとセキュリティリスク大，メタバース×AI が熱いこと，IoT のすぐ裏にデータビジネスがあること．
・多種多様な IoT 機器とその利活用
・IoT のビジネスとしての難しさ
・大変興味深いお話を聞かせていただいてありがとうござ いました． お話を聞いて，いくつものひらめきが得られました．自分も起業を考えているので，大いに刺激になりました． 是非また，いろいろなお話を聞かせていただきたいと思っています．
・IoT 機器ビジネスを継続することの難しさ．想像以上に管理コストがかかるなと思いました．
・cookie に関する話は面白かったです．
・ニッチな分野の IoT のお話など，とてもおもしろかったです．
・ プライバシー・セキュリティの問題が予想以上に大きく，IoT 業界の課題であること．
・SaaS + a Box，ブラウザと Cookie，情報収集タグが貼られていること，メタバースとセキュリティ
・3rd Patty Cookie の仕組みについて

〈2020 年まで〉

［情報の法的価値と法的規制］

・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．
・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 年まで〉

・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.
・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 年まで〉

・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.
・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．

9．5 高度セキュリティ PBL Ⅰ，Ⅱ，Ⅲ

［高度セキュリティ PBL Ⅰ］

〈2021 年〉

・ElGamal 暗号の特徴について．乱数 r の情報がなくとも復号を行えるのは非常に良い仕組みだと感じました．

・バイナリユークリッド互除法

・暗号化の概略について知りました

・群・環・体や有限体の演算と，実際に鍵を共有する流れが理解できました

・DH 鍵共有法,Elgamal,DH と DSA 署名の詳細が理解できました．

・バイナリユークリッドの互除法，ゼロ知識証明，離散対数問題解読は今回の講義で初めて聞きました．

・初等整数論の暗号技術への応用．（ユークリッド互除法，バイナリ法，DH 鍵共有法）

・セキュリティ自体が新たな分野だったので，素数と情報でどれほどのセキュリティ対策ができるかが勉強になった．後で TA にも聞いたが，1024bit の暗号化がそのままパケット通信の暗号化にも適用ができ，HDD のクラスターを 1024bit などの単位としていたことなどとも結びつき，コンピュータが身近なものになった経験だった．

・ρ 法，ゼロ知識証明，共有鍵の保有，GOOGLE ドライブで共有ファイルが複数人で書き込み出来ること，ハッシュ関数のビット長調整

・理論と実装の両方を学べたこと．特に GH 鍵共有法と ELGamal 暗号に関しては，今までに少し知っていたので，深い理解へつなげることができた．

・ρ 法の考え方についてよく分かりました．

・暗号かぎの受け渡しが裏でどんな計算が行われているかを知ることが出来たのと，どのようにセキュリティを確保しているのかを学べてよかった

・DSA 暗号化では理論的には問題ありませんでした．実装では，メッセージのエンコード方法やハッシュの方法など仕様が明確に決まっていないと，メッセージの送信者と受信者でうまくやりとりができないことがわかりました．実装レベルで仕様を明確にしておく必要性を感じました．

・乗算アルゴリズムにおいて，MOD をとりアルゴリズムを最適化することで，計算時間を大きく短縮することができる点．

＊PBL 全体に関する意見

・PBL いきなりでは全く分からなかったことを，事前課題を通して Python 基礎と初等整数論基礎を学ぶことで，本番でも講義と演習に取り組むことができました．内容も難しくかつスピードも速いため，とても疲れましたが，心地よさや達成感，満足感もふりきってます．暗号技術，数学，プログラミング，アルゴリズムなどを学ぶだけでなく

実装することで，モノクロの資格試験も少し楽しくなり何となくカラフルになりました．

〈2020 年まで〉

・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］

〈2021 年〉

＊講義で最も勉強になったこと

・多項式環の数学,RING-LWE のプログラム演習が理解できました

・格子理論と FFT,NTT が勉強になりました．多項式の乗算って面倒だなあと思っていましたが，FFT,NTT という理論・手法があることは初めて知り，勉強になりました．

・多項式，剰余環の数学的な知識 演習問題を解いて，数式を描き証明しないと身につかないです．

・LWE 問題を用いた暗号システムを実装するのが初めてだったのでそこが良い勉強になった．（効率性の悪さを体感できた）

・Ring-LWE 方式に基づく準同型暗号に BGV 方式, FV 方式といった亜種があることを知れて良かった.
・発表検討と発表（準同型暗号の応用など）は色々意見交換できてよかったです.
＊PBL 全体に関する意見
・多項式環なので数学はついていけたのですが, 格子の理論など事前に勉強しておけば理解が進んだと思います. コーディングに落とし込むのは難しかった.
〈2020 年まで〉
・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］

〈2021年〉
・リバースエンジニア アセンブリコードの読解
・逆コンパイルや逆アセンブルを行えるソフトの中に無償版も存在するという事実
・リバースエンジニアリングの実践, IDA の使い方
・バイナリ解析, 具体的なツールの使い方など実際ハンズオンで試してみることで理解が深まりました.
CTF について書籍などは読むだけで, 実際に書籍の内容を試してみる環境を整えようと思ってもうまくいかずなかなかハードルが高かったので, 実際に体験ができて良かったと思います.
・CTF とは, CTF 実例, Kali Linux の存在, Linux コマンド, シーザー暗号・ROT-13, リバースエンジニアリングとは, レジスタとスタック, IDA と逆アセンブリ
・体系的, 実践的にリバースエンジニアリングの知識を修得でき, 職務に直結する内容で有意でした.
・CTF の実践, デバッガの使い方
・実際に CTF を体験しながら, 過去に合ったセキュリティインシデントの事例を知ることができたと思う
・バッファオーバーフロー, 実践 CTF
・以前参加した CTF の講座のフォレンジック系は問題が多く, バイナリファイルや Windows のレジストリ等ひたすら検索と言う感じであまり興味がわきませんでした. 今回, バイナリ解析やリターンアドレス書き換え, Python でプログラムを作成してサーバからフラグを得るなど楽しい内容が多く, 熱中するあまり, 後半のサービス問題に辿りつかないぐらいでした. ただ, 講義で説明していただいた難易度の高い内容はかなり解けたので充実した2日間になりました.
・スタックの動き, バッファオーバーフローの利用の詳細, CTF 実践
・職場において職員に対する CTF を企画したり, 問題に触れることはありましたが自らが解答するのは初めてで知識のみならず解答の当たりをつけたりセンスが必要であると体感でき, 職務に直結する有意なものでした.
＊PBL 全体に関する意見
・集中して CTF の問題解けたので楽しかったです. 簡単な問題から解いていって時間配分もうまくいきました.
CTF の問題は幅広いです今回取り上げた問題以外も幅を広げてほしいと思います. アタック＆ディフェンスは難しいのでジョパディ形式で ネットワークのパケット分析, XSS, エクスプロイトのコーディングの問題とかもやりたいです.
・座学と演習の流れが素晴らしい PBL でした. 具体的には, 初めに CTF の概要を学び, 暗号・リバースエンジニアリング・PWN 問題を座学とウォーミングアップ問題で準備してから, 2 日目の後半で CTF 実践の流れ. CTF 実

践は，対抗戦ということもあり燃えます． 実践後には，CTF のフィードバックで答え合わせやヒントの時間があり，優勝者の表彰では和やかな空気になりました．ランチミーティングも，講師の方々と学生，社会人のつながりが生まれてひとつの魅力です．

〈2020 年まで〉

・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．

・マルウチ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．

・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．

8．6 高度サイバーセキュリティ PBL Ⅰ， Ⅱ， Ⅲ

［高度サイバーセキュリティ PBL Ⅰ］

〈2021 年〉

・OSI モデルとその各層の基本的な特徴が非常に復習になりました．とくに，IP アドレスと MAC アドレスにおける計算が異常に勉強になりました．

・ネットワークに関する知識や基本構造について勉強できました.
・仮想ネットワーク, VLAN に関しては事前知識が概要しかもっていなかったので勉強になりました.
・ルーティングテーブルの計算方法
・アドレス変換, 仮想ネットワーク
・仮想ネットワーク技術 名前は聞いたことはあってもどのような技術なのか理解することは難しく, 今回の講義は為になった.
・理解できた中ではネットワークの階層の内容ではあるが, 完全な理解にはまだ至っていないものの, 仮想ネットワークの内容は非常に勉強になったと思う.
・私は現在情報通信基礎Ⅱという講義を受講していますがその中でも OSI 参照モデルをやっているので今回の講義と重ねる部分がありました. しかし例えば同じデータリンク層でも初めて聞いた部分があったりして, より深く OSI 参照モデルについて知ることができたことが最も勉強になりました.
・実際にネットワークコマンドを用いてファイアウォールを設計することで かなり曖昧なままだったネットワーク関係の知識がきちんと定着させられて勉強になった.
・仮想ネットワークの仕組み ・ルーティングテーブル
・明石先生の講義の中での MPLS のお話が最も興味深く勉強になりました. MPLS については名前を聞いたことがある程度だったので, MPLS がの仕組みやスイッチング技術として使われなくなった理由, VPN の技術として使われるようになった理由などすべてが新鮮でしたし, 一度使われなくなった技術が別の形で使われるようになったということにひかれたというのもあると思います.
・インターネットの技術の標準化の細かい話などが聞けて興味深かった.
・仮想ネットワーク
・IPv4 では延命のために複雑な処理が行われていたこと
・どのようにデータがやり取りされているかがいままで曖昧でしたが, どのようなものかつかむことができたと思います.
・ARP やアドレスについてよく分かりました.
・ルーティングテーブル・NAT など, 各レイヤでのパケットの移動の仕組みに関すること.
・講義の合間に少し出た QUIC やプロトコル仕様を決める時の会議の雰囲気の話が初日は最も印象に残りました. また明石先生の後半のスライドの内容が, 一般ユーザーはおおよそ触れることのできない技術でとても勉強になりました.
・VPN の仕組みについて
・TCP/IP の 4 階層モデルについて深く知ることができました. 実践を通して, ルーティングテーブルを理解し, 普段使っているネットワークがどのように構成され, 接続されているかを知ることができました.
・明石先生の仮想ネットワークのお話はほとんど初めて聞くような内容だったためとても勉強になったと思う.
・オーバーレイネットワーク等, 仮想ネットワークの最新技術
・仮想環境でルーティングテーブルの作成が一番勉強になりました.
・vargrant を扱うことができてとても勉強になりました.
・ネットワークの仕組み全般, TCP ハンドリングの流れ
・ファイアウォールとはどのような仕組みなのかをしれて良かった.
・実際にコンピュータをさわって, ルーティングテーブルの設計やファイアウォールの設定が非常に勉強になった.

・サイバーセキュリティの仕組みが一体どうなっているかということに興味があり実際にネットワークアドレスでブロックしたりとファイアウォールのプログラムングを見て概要を知ることができたこと.
・ネットワーク関係のコマンドを実機で扱えたのは極めて実践的で勉強になった.
・Vagrant を使って実際に環境を構築し，ルーティングテーブルを設定することができ，実践的なことが学べたので良かった.
・ネットワークに関して基礎的な知識から実践的な部分を学ぶことができました.
・Vagrant の使い方. 大変便利なツールであることがわかりました.
・Linux におけるファイアウォールの設定方法
＊PBL 全体に関する意見
・普段学部の授業より実践的な内容で，非常に勉強になりました.
〈2020 年まで〉
・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］

〈2021 年〉
・UNIX OS の仕組みについて，おおよそは理解しているつもりだったが，fork，signal，debugger など改めて勉強になった.　デバッガを作ったことはなかったので演習は難しいけど楽しいです.
・CPP のプログラミング ELF，DWARF LLVM の環境，LLVM コード生成
・主に 1 日目の内容が勉強になった. デバッガは使用している IDE にデフォルトで搭載されているため機能としては知っていたものの，使い方や動作原理はイマイチわかってなかったためかなり勉強になった. またシステムコールについても学部の授業で習ったものの，実際コンピュータ上で動かして動作確認する機会等はなかったため，かなり勉強になった. また 2 日目についても，LLVM はライブラリのインストールの際などにキーワードとして知っていたもののそれが何なのかは全く知らなかったため勉強になった.
・Docker の使い方から C，C++を使ったプロセス・メモリ・レジスタ操作方法
・アセンブリを書いた事. デバッガの仕組みを学べたこと.　全体を通して，実際に体験しながら授業を理解できたこと
・C++からの LLVM への変換が簡単なコードは変換できるが複雑な構文であると変換できない. 変換しやすい構文にしてコーディングする必要がある. LLVM のプロジェクトの今後の活動に期待します.

〈2020 年まで〉

・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，どのようなことができ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．

・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］

〈2021 年〉

・ゼロトラストの正式な概念と juniperOS の機能

・JuniperOS の操作．実務と違う環境を実際に操作することができて，知見が広まった

＊PBL 全体に関する意見

〇最新セキュリティ特論 I

＊講義全体に関する意見

・情報セキュリティの基礎を学ぶのに最適な講義内容でした．今回全ての講義をオンラインで受講しましたが，充実した教材と講師の方々の配慮により，特に違和感なく講義に集中することができました．

・情報セキュリティの最先端で活躍されている先生方から，知識だけでなく，実際にあったインシデント事例の紹介やその考察などを学べました．座学形式の講義でありながらも，中には演習さながらの講義もあり，手を動かすことでさらに習得できたように思いました．

・情報処理試験での基礎的な内容をしっかりと押さえながら（基本情報処理試験の内容については復習になりました），最新のセキュリティの状況やトレンドなどの内容をしっかり取り入れられており，「現状」を伝えてくださったので非常に勉強になりました．それと同時に，情報セキュリティを学ぶ上で自分の学習や知識が足りていない部分というのもたくさん見つかりましたので，いただいた講義資料やビデオなどでさらに理解を深めたいと思います．

10. 認定者の声

10. 1 2020 年度認定

・ご指導ありがとうございました．今まで深く理解していないまま活用していた内容に関する理解が深まったように感じています．受講した内容が直接業務に役立つわけではないですが，本カリキュラムを通じて 学んだことを業務に生かしていければと考えています．このような学びの機会を与えていただけたことに非常に感謝しています．

2020 年 3 月修了 株式会社エヌ・ティ・ティ・データ・イントラマート 中嶋基喜

・私は業務系のエンジニアをしておりますが，昨今のセキュリティの状況から，もう少し勉強する必要があるのではないかと感じておりました．宮地先生の Prosec のカリキュラムは，暗号の基礎となる代数や解析学の基本的な知識から，インフラ設定，プログラム言語の基礎となったチューリングマシンの考え方など，幅広く扱われており，今までよりも，IT やシステム開発の技術の大局観が掴みやすくなりました．また，様々な現場のプロフェッショナルの先生方から，生の声を聞くことができ，大変勉強になりました．仕事をする際も，以前より方針などを立てやすくなったように感じます．一緒に勉強させていただいた学生の皆さんにも，大変親切にしていただき感謝しております．皆様の益々のご活躍を心よりお祈りしております．私も頑張ってまいりたいと思います．

（株）ハンド 中谷恭子

10．2 2021 年度認定

・2年間多くの分野の先生方の授業を受けさせていただき，視野が広がりました．ありがとうございました．秋学期から入学した最初のころは，暗号の本質が数学だということがわかっていなかったので，毎週土日に終日勉強していましたが，2 年目はわからないところを質問させていただくことで理解が早くなりました．コロナ前は，出張先で業務を終えた後に受講する機会が多かったので，出張先で WiFi 環境を探して受講していました．いつもは優しい宮地先生が学生さんたちに社会人の方は仕事を終えてから，この講義を受けているのだから，学生たちはがんばらないといけないよ，と言ってくださったときは，励ましていただいた気持ちになりました．高野先生から，質問してくださいねとメールをいただいたこと．奥村先生がわたしの全く的外れな質問にも，夜遅い時刻にも何度も答えてくださったこと．苗村先生の迫力ある GDPR の授業，上原先生の最新の動向を踏まえた授業，猪股先生の緻密な情報セキュリティの授業，興味深かった岩佐先生，いつの間にか使えるようになった Python の演習・・・先生方の素晴らしい授業，励ましとご指導なくしては修了することはできませんでした．感謝でいっぱいです．今後も勉強を続けます．どうぞ今後ともご指導賜りたく，よろしくお願いいたします．

パナソニック株式会社　黒田 園子

・技術革新の速い IT 業界において，基礎原理の理解と手を動かして学ぶことの重要性を再認識しました．年度ごとにコース内容も刷新され，学びの多い講座です．学生の方はもちろん業務上では学べない気づきも多いので社会人の方に是非受講してもらいたいです．

富士通株式会社 宮本 明宜

・ほとんどの講義が，理系学部教養程度の知識があれば，段階的に理解できるように工夫されているところがいいと思います．学んだ内容がすぐにいかせるわけではないのですが，情報セキュリティについての解像度が上がった気がします．全ての講義がリモートで受講可能，社会人が受講しやすいスケジュール，授業のアーカイブがある等，仕事をしながら受講できる環境だと思います．ただし，完全に社会人向けではなく，大学生も受講する講座なので，社会人向けの教養講座や，セミナーとは異なり，自ら学ぶ姿勢とある程度まとまった時間が必要です．時間をかけるだけの価値のある講座だと思います．

有限会社 平成 河原 章

・実践と講義を組み合わせる事で，自分の得意/不得意が鮮明になって良かった．またリモートで講義を受けられるのは，社会人の学び直しという意味で非常に助かった．

パナソニック株式会社 成岡 秀真

・最新セキュリティ特論 Ⅰ(サイバーセキュリティ):たくさんの専門家の先生に色々と教えていただき，有意義な講座だと思います．高度セキュリティ PBL Ⅰ(実践安全な公開鍵暗号の設計と解読 PBL):普段利用している暗号技術について，具体的なプログラミングをすることで詳細が理解できました．何気なく使っている裏側を理解できた気がします．高度セキュリティ PBLⅢ(実践 CTF):CTF を実施する前に，バイナリ解析の講座をしていただき実際に体験したことが非常に記憶に残っています．また，CTF も初めてだったので，非常に楽しかったです．

日本アイ・ビー・エム・サービス株式会社 山口 隆博

10. 3 2022 年度認定

・学びと成長する機会を与えていただき、また分かりやすく丁寧にご指導くださり心より感謝申しあげます。

(講義感想) 上原先生は情報セキュリティリテラシーのみならずアメリカでの実体験やフォレンジックを教えてくださり、猪俣先生はセキュリティインシデント(当時はカプコン)の対応などとても興味深い話をしてくださりました。また、情報処理安全確保支援士試験の問題など講義テキストで実際の問題に触れることで情報セキュリティの知識を得ながら自身の IPA 試験受験にも活用することができました。満永先生の講義は1回目 30 分座学、後半は実技のかたちだったのを覚えています。座学で学んだことをヒントに実技に活用する流れで 2 回目のバッファオーバーフローの講義は次回機会に、是非とも実技演習を受けたいです。苗村先生は個人情報と GDPR についてお話してくださりパワフルでバイタリティに溢れている印象を受けました。岩下先生からはフィンテックやブロックチェーン理論を学び、オンライン講義後の小テストも他の講義にはなかったためとても良いやり方でだと感じました。 岩佐先生からは土曜オンライン講義で、「アカウント管理」「パッチ適用」「ログ管理」と、「製品の説明書どおりに利用する」話が印象に残っています。ニッチな IoT 製品の紹介も楽しかったです。PBL1 は事前課題→講義で、Python、数学、暗号理論を学び実装することで暗号の実装方法が習得できました(講義後の課題も含めて)。チームに迷惑をかけまいと 1 日目は徹夜したのちに早朝に起きて演習に励んだことを覚えています。久しぶりに頭をフルで使い気持ちのいい疲労感を体験しました(課題はあまりできていませんでした)。 PBLⅡは理論が非常に難しく進むにつれて理解が追いつきませんでしたが、Python で実装することで理論の部分も少し理解することができました。「練習問題3は手を動かしてから、練習問題4は自由に」と言われたとおり手を動かし、練習問題4については 1 頁のレポートですが書きたかったことをかたちにできたと思います。 PBLⅢは座学で学んだことを 2 日目の CTF で実践するという貴重な体験をさせていただきました。CTF では基礎的な部分もできなかったので復習しました。ネットワークを学んだり仕事等で実践したことがなかったりしたことから高度サイバーセキュリティ PBL1～Ⅲは講義も課題も非常に難しく感じました。高野先生や明石先生が詳しく教えてくださったことでできていないながらも課題をやり遂げました。全体を通してもっと積極的に先生方へ質問をしたり学生や社会人の皆さまともっとやり取りをしたりしておくべきだったとあとになって後悔しています。これから学ぶ方は是非実践してほしいと思います。

(コメント)本プログラムの出願要項に「大学教養レベルの数学やアルゴリズム・プログラミングに関する基礎知識を有することが望ましい」とあったため、出願までの半年間、基礎的なことを学ぶため IPA 情報処理推進機構の情報処理試験資格と数学とプログラミングに関する民間資格を取得して本プログラムに臨みました。科目等履修生として入学し大学院生も受講する講義を受けるため、アルゴリズムやプログラミング特に数学の講義が社会人にとっては難しいと感じました。基礎的なことからと整数・論理、集合についての高校数学参考書を学び数学は楽しいと認識し続けるために「はじめアルゴリズム」という漫画を通勤中に何度も読み返して、講義前後に教科書を学習する習慣となっていました。手を動かすことで、脳と体に憶えさせる講義ノートをとることの大事さも感じまし

た。暗号の基盤となる数学は、「最初はわからなくても継続していたらわかってくる」という宮地先生の言葉を信じて続けたことにより最後まであきらめずに学ぶことができました。Python の演習・実装をすることで数学やアルゴリズムを少しずつ理解できる場面もあり数学がわかってくることで暗号や情報セキュリティもわかって学習が楽しくなりました。2年目後期は、土日の仕事と課題レポートに追われ、末年始の帰省・帰阪時の電車の中でも数学とプログラミングをやっていたことを思い出します。セキュリティ関連の仕事に携わらなくても、学んだことが間接的に技術者等の生産性向上にも寄与でき、技術の進展に貢献できることも教わりました。仕事に活かしつつ学ぶことを継続し周りの方にも学び直しの大切さを発信し企業や社会に活力を与えるよう努めてまいります。

新家工業株式会社　與倉 正治

・最初の半年はかなり苦労しました。講義は大学院生や、週末の集中講義では他専攻や他大学の方も参加していることもあり、負けないように頑張りすぎたかもしれません。理解できなかった講義については、再履修に挑みましたが、実務に追われる毎日の中では頭を切り替えて最初の1年のような緊張感がなかなか取り戻せませんでした。PBL では、週末にむけて予習して備えていても、ちょっとしたところで躓き、土曜日の夜は追いつくために深夜まで取り組んだこともありました。丁度、この2年間コロナ渦で東京からのオンラインでの受講しか出来ませんでしたが、機会を見つけて残った単位は現地参加で再履修したいと思っています。

株式会社 IHI　山本顕弘

10. 4 2023 年度認定

・明石先生のネットワーク演習は、会社でも調達が難しい規模のサーバー台数のテスト環境で演習ができるのは、研究のインフラが活用できるからと思います。猪俣先生の病院のセキュリティ事故、岩佐先生の IoT の製品開発、大塚先生のブロックチェーンのビザンチン合意など実践的な授業が多いです。離散数学では、講義だけでなく事前課題のクイズと試験があり、学生と一緒に教室で受けました。先進情報セキュリティとアルゴリズムは、授業のペースが速いので事前に PYTHON の関数を作成しないと厳しかったです。先進情報セキュリティとアルゴリズムの RUST の課題や、論理式を使った証明、不完全定理は勉強になりました。安全なデータ設計特論では、提案したテーマを大学院生と一緒に議論しながら課題を解決し発表することができました。宮地研究室でミーティングし、研究室の熱い雰囲気に接することができてよかったです。特に、PBL では、学生と社会人とチームを組むこともあり垣根が低く良い刺激になると思いました。コース終了後、セキュリティ関係で交流している受講生もあり、人脈も広げることができてよかったです。

シャープジャスダロジスティクス株式会社 児玉修一

・2 年間、貴重な学びの機会をいただき、ありがとうございました。プログラミング（Python や Rust も！）、ネットワーク（仮想アプライアンスを使った FW 構築）や数学、暗号、バイナリ解析等様々なカテゴリを体験できた上に、第一線で活躍される弁護士の方や経営者の方のお話を伺い、自分の知らない世界を見ることができる楽しみな時間でした。さすがに大学院の講義内容でしたので、理解するだけでも精一杯でしたが、頂いた課題を、考えに考えてレポートにまとめる中で、考える力が身についたと考えております。2 年間の ProSec を修了したことで、現業のシステム管理にも自信を持って取り組めるようになりました。そして、ProSec で視野が広がったがゆえに、更に知りたいことも増えてしまい、引き続き学習を進めています。機会があれば、知識のアップデートのために、また ProSec に参加させていただきたいと考えております。今後とも、どうぞよろしくお願い致します。

名古屋記念財団 安立 征大

・2 年間の ProSec プログラムでは、サイバーセキュリティを暗号理論、ネットワーク技術、法制度の 3 つの側面で、

体系的かつ実践的に学ぶことができました。先生方のご指導に感謝いたします。講義をリモートで受講できる環境や週末土日の PBL 演習は、社会人の学びにとっては非常にありがたいです。また、社会人だけでなく探究心旺盛な大学院生と一緒に学ぶことは、とても刺激的でした。暗号理論の基礎である離散数学や Python でのアルゴリズム演習は、初学者の私にはハードルが高かったものの、先生方への質問や Moodle でのオンライン学習システム、講義のアーカイブなどを活用することで、着実に力をつけることができたと思います。ProSec を修了することは容易ではありませんでしたが、先生方の熱心な指導と様々な学習支援の仕組みがサポートしてくれました。ProSec では、多様な角度からサイバーセキュリティの知識・スキルを修得できます。セキュリティ分野でスキルを高めたい社会人の方に、おすすめのプログラムです。

りそなアセットマネジメント株式会社　IT戦略部　毛海 健雄

・金融系の業務システムの開発者からセキュリティ関連の企業に転職した私は、自身の専門知識の乏しさを少しでも補うべく、Prosec に応募いたしました。初めて暗号を中心に専門的な講義を受講しましたが、「セキュリティ」に関連した先進の知見を俯瞰的に教えていただき、こちらのプログラムでしか得られない貴重な学びを得る事ができました。私のようにセキュリティ分野の初学者の方であっても、きっとその方にとっての特別な学びを必ず獲得できるプログラムだと思います。私が履修させていただいた分野は、実践離散数学と暗号、サイバーセキュリティ、各種特論（様々な脅威関連、攻撃手法、法律、ビジネス…） などなど、実に多彩なプログラムでした。いずれの講義も初学者の自分にとってはレベルが高く、毎回必死で宿題と格闘しておりましたが、少しだけ理解が進みささやかでも進捗が実感できた時は、達成感がありました。暗号の講義では、離散数学など全く自信がなかったのですが、先生方が各々のレベルに見合った到達点を定めてくださり、本当にきめ細やかにご指導いただきました。講義のテキストや、証明、試験前の模試問題などは宝物です。実践的な演習群は、実践的な環境で手を動かす事ができる充実した内容でした。演習用の環境構築テクニックからして早速実務に応用が利きそうなヒントにあふれていて、技術的な学びがありました。私にとって特に印象的だった安全な公開鍵暗号実装のサマースクールでは、安直な API ではなく 0 からコードを組み、衝突や性能試験といった評価の設計・手法まで教えていただき、開発→検証→技術を応用した設計案、まで一通り経験する事ができました。チームで実践的で内容の濃い課題に取り組み、チーム対抗戦をした経験は、興奮と感動しきりでした。素晴らしい思い出を贈ってくださった、先生方と留学生・学生・院生の研究者スタッフの皆様に心から感謝しています。一緒に手を動かして同じ課題に取り組んで共に発表してくださった皆様方の背中から、学問や研究に向き合う上で最も大事にしなければならない事を学ばせていただいたのだと思います。宮地先生をはじめ、皆様にいつも励まされた事で、学習を続ける勇気をいただきました。今後も、今回のプログラムで得た知識を業務に活かし、未熟でも一歩ずつ「セキュリティエンジニア」として、学びと成長を続けていきたいと思います。本当にどうもありがとうございました。

NTT セキュリティ株式会社　　矢田部　小百合

11. 認定書

2021 年までの各コースの認定者数です.

	総合コース	メインコース	クイックコース	高度プログラム修

	総合	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	セキュリティ・サイバー実践	了
2020 春修了		0								
2020 秋修了		1	1	1	1	1	1	1		2
2021 春修了		1	1	1	2	1	1		1	2
2021 秋修了		3	1	2	3	1	3	3	4	3
2022 春修了		3	2	3	3	3	3	4	4	4

MiYaJi Laboratory

OSAKA UNIVERSITY ／ Miyaji Laboratory