(*)は任意記入事項（省略可能）

〇開講科目名
セキュリティ基礎論I
〇開講科目名（英）
Foundations of Security I
〇対象所属(*)

〇担当教員
宮地 充子, 松井 充(三菱電機)

〇開講言語
日本語

〇授業の目的・概要
セキュリティ分野を垂直な2軸で網羅的にカバーすることを目的とします。
具体的には、"共通鍵暗号解析"から"マルウェア解析"及び"基盤理論"から"実用技術・標準化"という2軸により、
セキュリティの基盤理論、暗号理論、実用化から標準化技術など最先端のセキュリティ技術までを守備した講義内容となります。

【代数学から構築する実践セキュリティ技術】（担当：宮地 充子）
代数学における各種定理が, セキュリティ技術の基本原理, 手法, 安全性証明,
計算の効率化などに応用されている.
代数学がどのように情報セキュリティ技術に実践的に活用されているのか,
複雑な代数学の各種定理を実学に適用する手法を習得することで, 新たな
セキュリティ技術の構築を可能にする代数学の実践的な習得を目指す.

【共通鍵暗号】（担当：松井 充）
暗号は見えないけれど現代社会は暗号なくして一日も成り立たない。
本講義では、このようなディジタル社会を支える暗号技術が私達の
身近なところでどのように利用されているかを、実例を示して説明
するとともに、共通鍵暗号を中心にそのアルゴリズムと利用方法な
らびに安全性について解説する。

【セキュリティ技術の標準化】
セキュリティ技術の普及には標準化が必須である。セキュリティ技術をどのように標準化するのかについて、具体的な事例を用いて習得する。

〇学習目標
【代数学から構築する実践セキュリティ技術】（担当：宮地 充子）
代数的諸概念として、整数論、環、体、群を理解するとともに、
暗号理論、数論アルゴリズムへの応用方法を習得する。さらに各種アルゴリズムの評価
方法について学習する。

【共通鍵暗号】（担当：松井 充）
暗号技術によってディジタル社会のどのような課題が解決できるのか
（できないのか）を理解するとともに、共通鍵暗号の正しい使い方を
学習することにより、暗号技術を中心とした情報セキュリティ技術を
今後みずから学習できる能力をみにつける。

【セキュリティ技術の標準化】
セキュリティ技術をどのように標準化するのかについて、具体的な事例を用いて
習得する。

〇履修条件・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。

【数理モデルから紐解く暗号理論】（担当：河内 亮周）
【代数学から構築する実践セキュリティ技術】（担当：宮地 充子）
アルゴリズム、群論、線形代数の基礎的な知識

【マルウェア解析入門】（担当：新井 悠）
Pythonによるプログラミング技能

〇授業計画

【代数学から構築する実践セキュリティ技術】（担当：宮地 充子）
【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、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、べき演算

【第2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
具体的な公開鍵暗号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：公開鍵暗号，安全性，

【第3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，

【共通鍵暗号】（担当：松井 充）
【第１回　暗号技術の実用例】
暗号技術が実社会でどのように利用されているかを、いくつかの
実例で示すとともに暗号技術の法的・政治的課題などにもふれる。
さらに共通鍵暗号の定義とその使い方について学習する。
【知識単位】暗号の実用例、共通鍵暗号、ブロック暗号

【第２回　共通鍵暗号のアルゴリズム】
現在利用されている、あるいは歴史的に重要ないくつかの共通鍵
暗号アルゴリズムを紹介する。特にＡＥＳ暗号については、その
仕様とともにソフトウエアによる高速化手法について学習する。
【知識単位】ＤＥＳ暗号、ＡＥＳ暗号、ソフトウエア実装

【第３回　共通鍵暗号の安全性】
暗号の安全性と暗号解読との関係を述べるとともに、暗号解読に
いたるいくつかのシナリオを説明する。続いて共通鍵暗号とその
利用モードに対する具体的な暗号解読の例を学習する。
【知識単位】暗号の安全性、暗号解読

【セキュリティ技術の標準化】
セキュリティ技術をどのように標準化するのかについて、具体的な事例を用いて
紹介する。

〇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）。

〇教科書・教材(*)
【代数学から構築する実践セキュリティ技術】（担当：宮地 充子）
宮地充子著，「代数学から学ぶ暗号理論」，日本評論社

〇参考文献(*)
【共通鍵暗号】（担当：松井 充）
結城浩著　暗号技術第３版　秘密の国のアリス

〇成績評価［評価方法・割合の記載は必須］
[評価の観点] 講義内容の理解度
[評価方法] レポート提出
[評価基準] レポート課題

〇オフィスアワー(*)

〇コメント(*)

〇特記事項(*)
講義の一部にプログラミング演習を含むのでノートPCを所有している学生は持参すること。
大阪大学のBasic SecCapに関する詳細については、ウェブページを参照：
https://cy2sec.comm.eng.osaka-u.ac.jp/miyaji-lab/basic-seccap/index-jp.html