

## 情報数理学統論 B

担当：面和成

### 概要：

情報セキュリティは工学全般の分野において必須の技術である。情報セキュリティで重要となるネットワークセキュリティ及び暗号技術を主な対象として、その基本と応用について幅広く説明する。

### 目的・目標：

情報セキュリティの知識を幅広く習得することが目的である。そのための具体的な目標は次の3つである。(1) ネットワークシステムに潜む脅威と脆弱性を理解する。(2) ネットワークセキュリティ及び暗号技術の基礎を習得する。(3) 情報セキュリティの応用技術を習得する。

### 授業計画・授業内容：

1. 脅威と脆弱性
2. 暗号の基本技術
3. 認証の基本技術
4. ブロックチェーン技術(1)
5. ブロックチェーン技術(2)
6. ネットワークセキュリティ(1)
7. ネットワークセキュリティ(2)
8. 試験

### キーワード：

マルウェア、標的型攻撃、暗号、デジタル署名、認証、暗号資産、ブロックチェーン、ファイアウォール、Virtual Private Network (VPN)

### 教科書・参考書：

『入門 サイバーセキュリティ 理論と実験 ～暗号技術・ネットワークセキュリティ・ブロックチェーンから Python 実験まで～』（著者：面和成）

### 評価方法・基準：

出席、適宜出される課題、及び試験により総合的に評価する。