はじめに

未来学者アルビン・トフラーが 1980 年に第 1 の波（農業革命），第 2 の波（産業革命）に続く第 3 の波（脱産業社会）として，情報化社会の到来を予言して以来ほぼ 40 年が経過し，コンピュータ，ネットワークを含む ICT の発展に伴い，インターネットは我々の日常生活を営むのに不可欠なものとなって久しい．インターネットが便利になりビジネスにも使われるインフラストラクチャとして確立すると，悪意を持った利用者がネットワーク経由でコンピュータに侵入する不正アクセスをはじめとする種々の脅威が頻繁に発生するようになった．甚大な被害を被る事例や国どうしの紛争の原因になる場合もあり，大きな社会問題として取り上げられるようになってきた．このため，ネットワークセキュリティは，現在の喫緊の課題となっている．社会の根幹に関わる問題の具体的な例として，公共施設などのシステムに侵入するサイバーテロ，電子マネーの偽造・不正使用による経済の混乱，著作権の侵害，不正・迷惑文書，プライバシー侵害など枚挙にいとまがない．

ネットワークセキュリティがやっかいで問題が収束しないのは，ICT が進展しそれらが情報システムに導入されると，新たに別の脅威を発生させる要因となる可能性があり，脅威と対策がモグラたたき状態で繰り返されているところにある．新しい技術を開発する際には十分注意してセキュリティに配慮したものになっているにもかかわらずこのような事態が発生するのは，守るより攻撃する方が有利という一般的な原則が成り立っているからであろう．

我々がインターネットを利用する上で，守るべき資源（コンピュータ，ネットワーク，データ，など），これらの資源に対する脅威，脅威から資源を守る技術とその限界を含めたネットワークセキュリティを学ぶことは今後 IoT を含む情報システムの研究・開発・実用化を行う上で必須になっている．

上記を踏まえ本書では，線形代数学，情報ネットワーク，アルゴリズムとデータ構造，オペレーティングシステムなどを履修した 3 年生を想定して，ネットワークセキュリティに関する基本的な知識を体系的に学習することを前提に構成してある．具体的には，第 1 章では，ネットワークセキュリティの背景となるインターネットの発展経緯と潜在する脅威について述べるとともに，脅威に対する対策技術の概要を解説する．また，本書で扱う主な技術，トピックスとともに脅威の具体例を解説している．

第 2〜5 章では，脅威を防御（情報を秘匿）するための基本技術である暗号について，基本的な概念や用語を示すとともに，暗号技術の発展経緯，古典的な暗号と，現代暗号である共通鍵暗号と公開鍵暗号について，それらの動作原理を解説する．また，実用例として共通鍵暗号と公開鍵暗号の短所を補完したハイブリッド暗号方式について解説する．さらに，公開鍵暗号の

応用として，デジタル署名と鍵の配送方式について解説する．

第 6 章では，通信相手が本人であるか否かを確認するユーザ認証技術について，認証に使用する情報の種類や脅威を含むその基本原理を解説する．

第 7 章では，組織内ネットワークを構築する際の具体的なセキュリティ対策として，ファイアウォールや侵入検知システムなどについてその動作原理について解説する．

第 8 章では，第 2〜6 章で述べた基本防御技術を使用した応用例として，安全に Web アクセス，電子メール，リモートアクセス，プライベートネットワークなどのアプリケーション実現方法と，その動作原理について解説する．

第 9 章では，情報システムを安全に維持管理するために必要な情報セキュリティマネジメントについて，その基本的な考え方，取り組み手順，取り組み内容について解説する．

第 10 章では，情報セキュリティのための法律や制度について，日本の情報セキュリティに関する法制度が準拠している国際的な取り組み状況について解説するとともに，国境を越えた法制度とその執行体制の重要性を解説する．

第 11 章では，国内における情報セキュリティに関する各種法律についてその制定経緯を含めて解説する．

本書は 11 の章からなる構成となっているが，各章末には参考の図書，文献を示している．各章の本文では理系・文系にかかわらず，いわゆる情報系の学科／コースで学ぶべき基本的な事項を取り上げているので，それらを基に必要に応じて技術の詳細や応用，法律などの運用・管理を補足して講義してもらうのがよい．また，前述した通りセキュリティに関する状況は，ICT が進展し情報システムの構築環境が変化するとそれに応じて新たな脅威が発生する可能性があり，常にアンテナを高くして新しい情報をキャッチアップしタイムリーなトピックとして講義の中で補足していただくのもよいと思う．以下に本書を用いて 1 セメスタ（15 回）の講義を実施する場合の指針の一例を示す．

第 1 回： 第 1 章　ネットワークセキュリティ序説
　　（1.1　インターネットの発展と潜在する脅威）
第 2 回： 第 1 章　ネットワークセキュリティ序説（1.2　具体的な脅威）
第 3 回： 第 2 章　古典的な暗号
第 4 回： 第 3 章　共通鍵暗号
第 5 回： 第 4 章　公開鍵暗号 (1)-基本的な考え方
第 6 回： 第 5 章　公開鍵暗号 (2)-デジタル署名と公開鍵の配送
第 7 回： 第 6 章　ユーザ認証
第 8 回： 第 7 章　組織内ネットワークのセキュリティ
　　（7.1　組織内ネットワーク，7.2　ネットワーク機器におけるセキュリティ対策，
　　7.3　ファイアウォールと侵入検知システム）
第 9 回： 第 7 章　組織内ネットワークのセキュリティ（7.4　無線 LAN のセキュリティ）

第 10 回： 第 8 章　インターネットのセキュリティ
（8.1　インターネットにおけるセキュリティ，8.2　Web におけるセキュリティ）
第 11 回： 第 8 章　インターネットのセキュリティ（8.3　電子メールにおけるセキュリティ，8.4　リモート接続におけるセキュリティ）
第 12 回： 第 8 章　インターネットのセキュリティ（8.5　仮想プライベートネットワーク）
第 13 回： 第 9 章　情報セキュリティマネジメント
第 14 回： 第 10 章　プライバシーの保護と情報セキュリティの確保
第 15 回： 第 11 章　日本の情報セキュリティ法，まとめ

ネットワークセキュリティのための基盤技術である暗号技術は，古代から使われてきており，インターネットの発展とともに進歩してきた．コンピュータを使ったからといえ，完全な防御技術が実現できているわけではない．たとえ完全な防御技術ができたとしても，完全なセキュリティが達成できるわけではない．そこには必ず人間（不完全な私たち）が介在するからであることを肝に銘じておきたい．

最後に，本書を執筆するにあたって，有益なコメントと遅々として進まない執筆作業に叱咤激励していただいた未来につながるデジタルシリーズの編集委員長の白鳥則郎先生，編集委員の水野忠則先生，岡田謙一先生，ならびに共立出版編集制作部の島田誠氏に深く感謝します．

2017 年 8 月

著者を代表して　高橋修