サイバーセキュリティへの確かな道標に寄せて

コーディネーター　井上克郎

ニュースでサイバーセキュリティに関する記事を目にしない日はない，今日このごろです．さまざまな組織において，その重要な情報が盗み出され，公開され，悪用されるなど，多大なダメージを受ける例が数多く見られます．また，国と国との間でネットワークを介した妨害や攻撃も実際に行われてきています．

現在，日本のみならず世界的に見て，このようなサイバーセキュリティに関する諸問題を理解し，対策を施して，解決に導く人材が非常に不足しています．サイバー空間に繋がる機器はますます増え，それらを利用する情報システムも複雑化し，高い社会的な価値を持つようになってきています．したがって，サイバー攻撃が成功した際の利益は，莫大なものになってきており，攻撃者には高いインセンティブが働いているものと思われます．次々と新たな攻撃手法が開発されるため，それに対して，高いサイバーセキュリティ技術と倫理観を持った人材が，各情報システムで迅速に対策を行わなければなりません．

サイバーセキュリティ技術者には，非常に幅広い基礎的な知識と，数多いケーススタディ学習や実例に裏付けられた経験が必要です．整数論を基礎とした暗号理論，通信機器のハードウェアとその上で動くソフトウェアやプロトコルなどのネットワーク技術，オペレーティングシステムやその上で動くツールやコマンドのシステムソフトウェア技術，各種サービスを提供するアプリケーションソフ

トウェアやその記述言語であるプログラミング技術などが基礎的な知識の例として挙げられます．これら個々の技術は，それぞれ非常に幅広い知識体系を背景に持っており，すべてを深く学ぶことは簡単ではありません．また，サイバーセキュリティに関するいろいろなインシデントを集めて分析するには大変な労力が必要となります．

本書は，これらサイバーセキュリティを学ぶ上で必要な基礎的な知識を，非常にバランスよく解説しています．大学の低学年学生や，意欲の高い高校生などが読んでもわかるよう，基礎的で重要な概念の説明が丁寧にされており，これからこの分野を学ぼうとする人にとって，非常に頼りになることと思います．また，過去のものから最新のものまでいろいろなインシデントの例を詳しく紹介しており，ケーススタディの学習にも非常に有益な一冊となっています．

具体的に紹介しますと，まず 1 章では，インターネットの仕組みについて，非常に初歩的なこと，基礎的なことから応用的なことまで，多くの実例や写真を用いて紹介されています．電話網とコンピュータネットワークとの類似性や違いなどを的確に説明に取り入れ，大変わかりやすくなっています．また，WEB システムやメールシステムがどのように動いているかが丁寧に紹介されています．これを読むだけで，インターネットの基礎を知ることができます．

2 章では，インターネット上を流れる情報やコンピュータの中に蓄積されたデータの安全を守るために用いられている暗号について説明されています．古代に使われた簡単な方式からより複雑で破られにくい近代的なものまで，歴史にそって，わかりやすく丁寧に紹介されています．特に近代的な暗号で用いる整数論やプロトコル，公開鍵暗号などのいろいろな知識や概念が，多くの例を用いて説明

されています．この章によって，コンピュータの進化とともに大きく変化する暗号の強度の考え方を理解できるようになります．

3章では，インターネット上でいかに安全で信頼性のあるデータ交換をするかについて，電子認証やそこで利用する暗号化技術，プロトコルの実装法について，例を用いて解説されています．インターネット上でいろいろなサービスを安全に行うためには，通信する相手が確かなもので，その相手と正しいデータのやり取りをしていることを保証する必要があります．ここで紹介する電子認証技術はそのために必須なもので，今後，ますます大きく発展する可能性を秘めています．

4章では，今，社会を揺るがしているサイバー攻撃について，多くの実例とその原理が紹介されています．マルウェア，DoS攻撃，標的型攻撃，そしてSQLインジェクションなど，日々多くの組織でこれらの問題が発生しており，その対策が急務になっています．この章を読むことで，さまざまな種類のサイバー攻撃に対して，どういう原理の攻撃か，攻撃されると何が起こるか，どうすれば防ぐことができるか，などの基礎的な知識が得られます．また，最近発覚し社会を大きく騒がせた遠隔操作ウイルス事件に関しても，その手口や原理の解説が詳しく行われており，同様な事件を防ぐためにもぜひ学ぶ必要があります．

5章では，ハードウェアの入出力や漏えい情報を利用した暗号解読手法，サイドチャネル攻撃について詳しく説明されています．暗号化のアルゴリズムやプロトコルをいかに強固にしたとしても，その情報を処理するハードウェアから漏れ出る微小な電力情報を得れば，暗号解読できる可能性があることが説明されています．コンピュータ画面を見ているだけでは想像もつかないところから，隠すべき情報が漏えいし，秘匿情報が解析されるという，驚くような手

法です．

最後の 6 章では，インターネットをより安全に利用できるようにするためのさまざまな活動，組織，法律など，技術以外の要素で，セキュリティ技術者が知っておくべきことが紹介されています．特に法律に関してはその条文や解説が詳しく書かれており，今後，この分野を目指す人々にとって必読の章です．

このように本著は，現在のインターネットセキュリティを初歩から最前線まで学ぶための最良のものとなっています．しかし，4 章，5 章で述べられているように，攻撃者は新たな攻撃方法を日々考案し，実際に挑戦してきています．過去には想像もつかなかった方法で，秘匿情報にたどり着くことができるようになることもあります．たとえば，コンピュータの能力が向上するとともに，その値段は非常に安価になっており，経済的な理由で現実的には計算できなかったものが計算できてしまうこともあります．また，安全が確立されている部分の外の情報，たとえばハードウェアの電力情報が攻撃されてしまうこともあります．

今後，今までとは違う新しい方式や考え方で，インターネットの攻撃が行われるかもしれません．しかし，本著で書かれている基礎的な知識や応用事例などをしっかり学んでおけば，ある程度，新たなものにも対処できるはずです．セキュリティ技術者としては，常に新たなものを学び，新しい対策を考える，という柔軟性と向学心は必須な心構えです．今後，末永く第一線で活躍するためには，新しいチャレンジを常にし続ける必要があります．

猪俣先生は，インターネットセキュリティの分野での第一人者で，日々，幅広い活動を精力的にされています．本著の中でも述べられていますが，enPiT-SecCap においては，奈良先端科学技術大学院大学，東北大学，情報セキュリティ大学院大学，慶應義塾大

学，北陸先端科学技術大学院大学の学生，そしてそれらと結びつきの深い他大学の学生に対して，サイバーセキュリティに関する授業や演習を行っています．猪俣先生は，この活動の中心となって非常に熱意を持って学生のチーム演習を牽引されています．確かな基礎的な知識をもとに，さまざまな経験やケーススタディを紹介して，学生の高い信頼を得られています．

このような実績をお持ちの猪俣先生が書く本著は，これからサイバーセキュリティを学習しようとしている方にとって非常に確かな道標となることでしょう．本書を通して，読者の方がサイバーセキュリティの基礎から最先端の知識までを身につけ，サイバー社会の安全がより高まることを強く期待します．