IT 技術者を目指す人の

情報セキュリティ入門

松田勝敬 著

コロナ社

ま　え　が　き

現在の高度情報化社会において，情報システムは日常的に誰もが接しているものになった。携帯電話に始まりその発展したデバイスであるスマートフォンの普及により，ネットワークに接続されている情報端末を 1 人 1 台以上つねに身につけている状況である。また AI などのブームが再来し，国を挙げて DX（digital transformation）の推進もされている。

この状況を支えるべき IT 業界も人手不足で，多くの企業で IT 技術者や IT 技術者を目指す人を採用したいが人が集まらないという話を聞く。IT 技術者の募集要項には「学部学科不問」と記されていることをよく目にし，情報系の勉強を専門にしていなかった人も IT 技術者として働いている。

IT 業界は，電子計算機ができておよそ 80 年，インターネットができておよそ 50 年，と他の業界に比べると新しい業界といえる。現在では IT 業界（情報通信産業）は日本でも国内総生産の 1 割を占める業界となっている。

この IT 業界の特徴の一つは，国家資格などに制限されずに仕事に就けることである。不動産取引では宅地建物取引士，医者になるには医師免許，建物の設計では建築士など，特定の資格をもっていないと仕事ができないことがある業界が多いが，IT 業界は資格をもっていなくても IT 技術者としていろいろな仕事に就けるのである。

また IT 業界は同じ業界の中でも多種多様な業務内容があることも特徴である。一般的には IT 業界で働く人は，机に座ってパソコンに向かってプログラミングをする人を思い描く人が多いのではないだろうか。実際は IT 業界のすべての職種でプログラムを作るわけではなく，プログラムを作る人も他の業務をしている割合のほうが多かったりするのである。構築する情報システムも金融システムなのか，輸送管理システムなのか，組込みシステムなのか，スマー

トフォンのアプリなのか，ネットワークゲームなのか，Web アプリなのか，などさまざまである。プログラミング言語も COBOL なのか，Java なのか，C なのか，Kotlin なのか，Swift なのか，C# なのか，Java Script なのかなどいろいろある。ネットワーク構築では機器の設定はするが，プログラミングはしない職種もある。新人のときはプログラマーでも経験を積んでいくと Project Leader や，Project Manager と呼ばれる仕事をするようになり，プログラミングをする人たちの管理者になってしまう。元プログラマーが同じ職場で監督業になってしまい，プログラミングはまったくしなくなってしまう業界でもある。

このような業界でも必ず一定レベルの知識をもっていないといけないことは情報セキュリティについてである。本書では，IT 技術者を目指す人が勉強しておくと IT 業界で働いているといつかどこかで役に立つ情報セキュリティの内容を，著者の経験も踏まえて解説している。本書は入門書のため，取り上げた内容についてもっと深く学ぶには原典やその分野の専門書などをあたって勉強していただきたいが，IT 技術者としてある程度仕組みまで理解しておいたほうがよいことは少し詳しく解説している。また解説している内容が，IT 技術者になったときにどのように実務に関係してくるのか，少しでも見えやすくするように実例などを交えて解説した。

また，本書は理系の情報系の学科ではさまざまな授業で習っているであろう内容はある程度理解していることを前提に説明している。それらを勉強したことがない場合や忘れかけている場合は，その分野の専門書などである程度理解して本書に戻ってきてもらいたい。

本書で学んだ方が IT 業界で働くようになり，少しでも情報システムで不幸になる人が減ることを願っている。

2024 年 2 月

松田勝敬

目　　次

1. 情報セキュリティの概要

2. 情報システムに関する脅威

3. 暗 号

4. 認　　証

5. ネットワークセキュリティ

6. アプリケーションセキュリティ

7. 物理的なセキュリティ対策

8. 予 防 技 術

9. 情 報 漏 洩

10. セキュリティマネジメント

11. セキュリティ関連法規と標準

【本書ご利用にあたって】

・本文中に記載している会社名，製品名は，それぞれ各社の商標または登録商標です。本書では®や TM は省略しています。

1

情報セキュリティの概要

1.1　情報セキュリティとは

現在は情報システムが広く一般的に普及しており，全世界的に共通の仕組みがもとになって構成されている。そのため「情報セキュリティ」の定義についても国際機関や国際的な規格で記載されている。例えば経済協力開発機構（OECD）から 1992 年に出された「Guidelines for the Security of Information Systems[1)] †（情報システムのセキュリティに関するガイドライン）」にて定義されていたが，2002 年の改定で削除されている。現在は ISO/IEC 27000:2018[2)] の 3.28 information security に記載されている内容が情報セキュリティの定義とされている。

そこでは情報セキュリティとは，「preservation of confidentiality, integrity and availability of information」となっており，「情報の機密性，完全性，可用性を保全すること」である。さらに追加事項として「In addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved.」とあり，「情報の真正性，説明可能性，否認防止性，信頼性の保全も係ることがある」となっている。これらの特性が損なわれる事件や事故は「セキュリティインシデント」と呼ばれる。

1.1.1　情報セキュリティに関する特性

機密性とは秘匿性ともいわれ，認められて許可されたユーザーのみ情報にア

† 肩つき数字は巻末の引用・参考文献を示す。

クセスできるようにすることである。完全性とは一貫性ともいわれ，情報が改竄されないようにして，完全で正確であることを保護することである。可用性とは利用可能性ともいわれ，認められて許可されたユーザーの必要な情報へのアクセスを確実にすることである。

真正性とは，記録された情報に対しなりすましなどが行われておらず正しく記録されていることを保証できることである。説明可能性とは，動作や操作が記録などをもとに説明ができることである。否認防止性とは，ある動作や操作について後から否定できないようにすることである。信頼性とは，意図したとおりの動作や操作ができることである。意図した行動と結果が一貫していることともいえる。

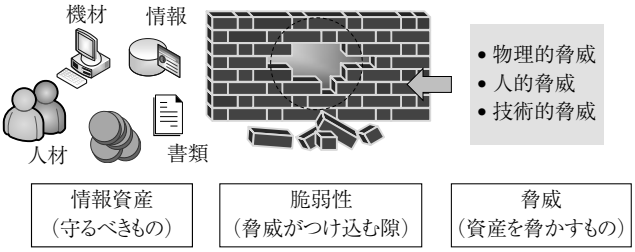
1.1.2　情報セキュリティ対策と利便性

情報システムのセキュリティ対策では，さまざまな技術を用いてこれらの特性を保全，維持する機能を実装することになる。そのような機能を実装すると，使いにくく手続きや操作が面倒になってしまうことが多い。情報セキュリティ対策をすることは，システムの利便性を低下させ，対策のためのコストも発生することが多い。

しかし，セキュリティ対策を怠るとインシデント発生時に大きな損害が発生することがある。実際の情報セキュリティ対策は，限られたコストの中で必要最低限の対策を施し，ある程度以上の脅威に対しては被害の発生も覚悟した内容となる。完全なセキュリティ対策を施すことは非常に難しいので，どこまで対策ができているか把握して，関係者に説明をしておくことが重要である。

1.2　セキュリティとリスク

リスクとは一般的に危険や将来的に被害や損失を与えるものである。情報セキュリティにおけるリスクは，情報資産，脆弱性，脅威を掛けたものであり，これら三つが存在することによって現れるものである（**図 1.1**）。



情報資産・脆弱性・脅威がそろうとリスクが顕在化（表面化）する

図 1.1 情報資産×脆弱性×脅威＝リスク

セキュリティとリスクはたがいにトレードオフの関係であり，どちらかが高まると一方は低くなる。情報セキュリティを高めることは，リスクを下げることで実現することができる。対策を施してセキュリティを高めることと，リスクを下げてセキュリティを高めることの両方から検討し，コストが低く実施しやすいことから取り組むとよい（**図 1.2**）。

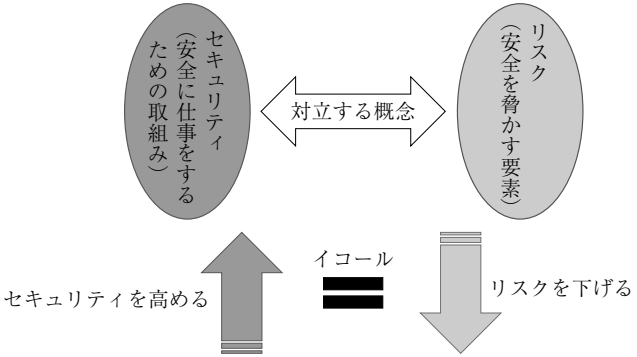


図 1.2 セキュリティとリスク

1.3 情 報 資 産

情報資産（information asset）とは，情報そのものや情報を記録したものなど，守るべきものである。コンピュータや記録媒体だけでなく，その他の機材や書類，人財なども含めて，失われたり損なわれたりすると損害が発生するも

のが情報資産である。

情報資産は有形資産と無形資産に分けることができる。

1.3.1 有 形 資 産

有形資産は情報を記録する記録媒体や記録媒体を読み込んだり書き込んだりする機器類，コンピュータやネットワークシステムの設備などである。コンピュータや通信機器などのハードウェアおよびソフトウェア，それらに関するマニュアルなどの文書なども有形資産である。さらに，これらが設置されている建物や部屋，電源設備や空調設備を含んだ建物なども有形資産となる。さらに，組織を構成する人材も有形資産に含まれる。

情報セキュリティというと，コンピュータやネットワークシステム，それらで用いるハードディスクやUSBメモリなどの記録媒体が思い浮かぶが，情報が書かれている紙やマイクロフィルムなども有形資産である。

IT業界はパソコンなどとそれらを設置する机などがおもな設備であることが多く，データセンターなどを除くと工場などの大規模な敷地や設備をもたない企業が多いことが特徴である。

1.3.2 無 形 資 産

無形資産は各種情報自体やプログラムなどである。学校であれば学生や生徒の成績などの情報，企業であれば顧客情報や経営情報である。さらに，組織のイメージや信頼，評判，知名度なども無形資産となる。研究成果や構成員の技術力，ノウハウなども無形資産に含まれる。

1.4 脆 弱 性

脆弱性（vulnerability，hazard）とは，安全を脅かす欠陥や，つけ込まれると被害が発生する弱いところである。脅威となるものが脆弱性を狙い資産を奪ったり，破壊したりする。情報システムは複雑なシステムであるので，脆弱

性をなくすことは非常に難しく，現実的ではない。当初はわからなかった脆弱性が，利用していたり時間が経過したりすると，表面化することもある。また，情報システムを利用する人や，構築や管理する人が脆弱性になることも多い。

情報システムやそれを構成するソフトウェア，ハードウェアの設計や構造上の欠陥やバグなどによる脆弱性を「セキュリティホール」と呼ぶ。セキュリティホールがあると，通常時は正常に動作しているが，ある状態や条件を満たすと不具合の発生や誤動作などの想定外の動作をする。セキュリティホールによる誤動作を利用して，不正アクセスなどを実現することもある。

ある程度の規模の情報システムではセキュリティホールを完全になくすことは難しいが，設計や構築時からセキュリティホールを作らないように考慮することが重要である。

1.5 脅　　威

脅威（threat，peril）とは，情報資産を脅かす存在である。悪意をもって資産を不正に取得したり，破壊したりするものだけでなく，悪意をもたない脅威も存在する。

情報セキュリティでは，セキュリティ対策機器の導入や災害対策など，技術的脅威や物理的脅威に対して備えるだけでなく，人的脅威に対する対策も重要である。特に悪意のない行為による脅威についても，システム設計時から考慮しておくことが重要である。悪意の有無にかかわらず情報セキュリティでは人が原因になることが多く，対策もとても難しい。組織全体で無知や技術力不足の状態になると改善されることがないため，現場の担当者だけでなく特に上司や管理，執行部などがある程度以上の知識や判断力をもつことが必要である。

1.5.1 脅威の分類

脅威はおもに「物理的脅威」，「技術的脅威」，「人的脅威」に分類することができる。また「自然災害による脅威」を加えた 4 種類に分類することもある。

索　　引

――著 者 略 歴――

1994 年　宇都宮大学工学部電気電子工学科卒業
1997 年　宇都宮大学大学院工学研究科博士前期課程修了（電気電子工学専攻）
2000 年　宇都宮大学大学院工学研究科博士後期課程修了（生産・情報工学専攻），博士（工学）
2001 年　宇都宮大学助教
2005 年　東北工業大学講師
2008 年　東北工業大学准教授
2021 年　東北工業大学教授
　　現在に至る

IT 技術者を目指す人の
情報セキュリティ入門

Introduction to Information Security for Aspiring IT Engineers　

2024 年 4 月 30 日　初版第 1 刷発行　★

検印省略

著　者　松田勝敬（まつだまさひろ）
発行者　株式会社　コロナ社
　　代表者　牛来真也
印刷所　壮光舎印刷株式会社
製本所　株式会社　グリーン

112−0011　東京都文京区千石 4−46−10
発 行 所　株式会社　**コ ロ ナ 社**
CORONA PUBLISHING CO., LTD.
Tokyo Japan
振替00140−8−14844・電話(03)3941−3131(代)
ホームページ　https://www.coronasha.co.jp

ISBN 978-4-339-02944-4　C3055　Printed in Japan　（齋藤）