電子通信情報系コアテキストシリーズ C-2

情報セキュリティ基礎講義

松浦 幹太
著

コロナ社

電子通信情報系コアテキストシリーズ
編集委員会

2017 年 3 月現在

刊行のことば

産業革命には，エネルギーを基軸に段階分けする立場と，産業のインフラ要素から情報化を含めて段階分けする立場がある。1860 年代から始まったとされる第 2 次産業革命はエネルギー源としての「電気」を基軸に置く議論が一般的である。ところが，明治政府はそのような分類学を超越し，電気の効能は通信にあると見切っていた。実際，明治 4 年（1871 年）には東京・ロンドン間で電信網を完成させ，その開発・運用に必要な技術者養成を目指して，明治 6 年に工部省工学寮電信科を創設している。本シリーズのテーマである電気・電子，通信と情報に関する日本最初の学校である。東京に電灯が灯ったのが 1882 年であるから，その 10 年以上前に通信網を完成していたわけである。一方，ケンブリッジ大学は 1871 年に電磁気現象に物理学の未来を夢見てキャヴェンディッシュ研究所を設立している。今から考えると，どちらの「電気」の見方も正しかったが，より産業的な実利を得たのは日本だったといえよう。現代は第 4 次産業革命のただ中にあるといわれ，日本の立ち遅れを叱責する声が大きい。ただし，そのように外国がやっていることをただ真似るのだとしたら，明治政府は物理学研究所を作っていたはずである。彼らは，後世にいわれるほど西洋の物まねに機械的に熱中していたわけではない。彼らなりの戦略眼があったと見るべきである。

電気・電子，通信そして情報は，以来，工学の主要な分野を形作ってきたが，特に第 2 次世界大戦後は，電子工学に代表される工業製品や生産設備の刷新を経て，1990 年代以降の情報通信社会を導いている。これはコンピュータの性能の急速な向上と，光通信に代表される通信網の急速な高速化に支えられたイ

ンターネットの出現に負うところが大きい。太平洋横断海底通信ケーブルを例にとると最初の光ケーブルだった TPC-3（1989 年）の 560 Mbps と比較して FASTER（2016 年）の 60 Tbps では約 11 万倍の高速化が達成されている。この結果，全世界の情報を一瞬に集め，これまでにない速度で処理する，いわゆるビッグデータの時代が到来している。今や，SNS (Social Networking Service) などに代表されるように，我々の活動は様々なディジタルメディアに書き込まれるようになっている。我々は梅棹忠夫が数十年前に予想した情報環境の中で生活するようになったともいえる。20 世紀までの歴史研究の「書物」がそうであったように，ディジタルメディアに堆積された「情報」こそ，これからの歴史を語る際の基本資料であるといえる。

そこで今回，これから技術者を目指す電気・電子・情報系学部生また高専生向けの教科書シリーズ「電子通信情報系コアテキストシリーズ」を立ち上げた。本シリーズは，電気・電子分野（A），通信分野（B）そして情報分野（C）と三つの分野に分け，多くの大学で講義されている科目を厳選し，実際に講義を担当している先生を執筆者とし，これからの教育現場に合った教科書を目指している。

本シリーズで勉強した学生が，若者の目で，上記のような 2010 年代における価値観から技術を再整理する一助になれば幸いである。

2017 年 5 月

編集委員長　浅見　徹

まえがき

本書は，東京大学工学部の電気系学科 4 年生を対象とした講義「情報セキュリティ (information security)」の内容がベースとなっている。筆者が 2009 年に同講義を始めるまで，学科に情報セキュリティ専門の講義はなく，通信や計算機関係の講義の一部で情報セキュリティに触れられる程度であった。講義が始まってしばらくは試行錯誤が続いたが，試行錯誤するまでもなく自明なことがあった。半年間の一コマの講義で教えるには，情報セキュリティの内容はあまりにも多く，時間が大幅に不足していた。

そう，情報セキュリティ分野は，広く，深いのである。

情報セキュリティだけでも一つの学科が成り立つといっても過言ではなく，最初から，網羅的な内容は考えられなかった。そこで，情報セキュリティ分野を支える重要な考え方をまとめ，それらの考え方を学ぶ上で適切な素材を厳選し，必要に応じて簡略化あるいは一般化などの変更を加えた上で基礎講義として形作ってきた。脆弱(ぜいじゃく)性が除去されていない段階の技術を選び，そこから学ぶことを狙ったものもある。丁寧過ぎるほど細かく説明する内容と自習を促す内容を使い分けることも工夫し，効果を見ながら改善を積み重ねた。各論で暗号を学ぶよりも早く，序論段階で暗号分野の概念をいくつか学ぶという順序も，最終的な効果を重視した結果である。今回，教科書としてまとめ直すにあたって，「情報セキュリティ分野は，広く，深い」という原点に立ち返り，その理由を分析した結果に基づいてアレンジを加えた。

情報セキュリティ分野は，なぜ，広く，深いのか。

一つには，商用化されている最終製品やサービスで，情報通信技術 (ICT:

information and communication technology) を利用していないものはまれだからである。その製造工程や流通過程も含めて考えればなおさらである。ICT を利用する限り，情報セキュリティと無縁ではいられない。したがって，情報セキュリティを学ぶことは，理工学の多くの教育課程において，有意義である。特に，ICT 分野では必要不可欠である。したがって，本書は，ICT を大学教育レベルで学ぶが情報セキュリティに携わるとは限らない幅広い人々を読者として想定し，執筆した。

もう一つには，技術だけで話が閉じないからである。情報セキュリティは，最終的には人の問題という見方も多い。「問題が発生すれば，最終的には司法の判断やお金による解決に頼る」という見方もある。これらは，学術的には人文社会科学の範疇（ちゅう）である。したがって，本書は，技術的でない素材もやや多く内容に含めて執筆した。

ユーザとして ICT を使うことは，いまやオフィスワークから家庭生活に至るまで，広く浸透している。基礎という看板を掲げるならば，大学教育を受けない人々をも対象として執筆したい気持ちもあった。しかし，残念ながら筆者の力量では，最低限の数学（大学の教養課程レベルの確率統計と微積分）と情報学（エントロピーと条件付きエントロピーなど）やインターネット工学（インターネットプロトコルの基礎など）を含む素養を，読者に求めなければならなかった。また，本書自体，最初から通読することを前提としている。より一般の読者を対象とし，ある程度断片的にも読みやすい縦書きの解説については，他書を参照していただきたい。拙著の範囲では，現時点では，「サイバーリスクの脅威に備える――私たちに求められるセキュリティ三原則――化学同人 (2015)」が最もその役割に近い。

最後に，本書執筆のきっかけを与えていただいた東京大学の坂井修一教授，そして，本書の草稿に貴重なコメントをいただいた産業技術総合研究所の大畑幸矢博士および本書担当編集委員に，深く感謝の意を表するしだいである。

2019 年 1 月

松浦 幹太

目　次

1章　情報セキュリティの基本

3章　ネットワークセキュリティ

4章　コンピュータセキュリティ

1章 情報セキュリティの基本

◆本章のテーマ

「そもそも情報セキュリティを確保するとはいかなることか」という問から始めて，情報セキュリティにおける着眼点や，安全性評価の枠組みを示す。本章の目的は，情報セキュリティに取り組む心構えを知り，ベストプラクティスにも目を向け，情報セキュリティ分野におけるセキュリティマネジメントの基礎を理解することにある。

◆本章の構成（キーワード）

1.1 基本要素
　守秘性，完全性，可用性，信頼関係

1.2 管理サイクル
　PDCA サイクル，セキュリティマネジメント，脅威分析，異常対応

1.3 三原則
　ケルクホフスの原則，明示性，首尾一貫性，相互依存性

1.4 ベストプラクティス
　アドレス確認，任務の分離，最小権限への制限，ルーチン化，情報セキュリティポリシー

1.5 安全性評価
　計算量的安全性，情報理論的安全性，形式検証，経験的安全性

◆本章を学ぶと以下の内容をマスターできます

- ☞ 情報セキュリティで着目する性質
- ☞ 情報セキュリティの手順
- ☞ 情報セキュリティに取り組む心構え
- ☞ 情報セキュリティのベストプラクティス
- ☞ 情報セキュリティのモデル

1.1 基 本 要 素

「情報セキュリティの確保[†1]」とは，端的にいえば，情報セキュリティの基本要素に関する品質管理を徹底することである。基本要素としては，少なくとも，**守秘性** (confidentiality)，**完全性** (integrity)，そして**可用性** (availability) を考える必要があり，これら三つをまとめて **CIA** と呼ぶ。さらに，**情報通信技術** (**ICT**: information and communication technology) を活用したサービスを考える時には，そのサービスに固有の**信頼関係** (trust relationship) も基本要素に含める。

攻撃や誤操作などのように，情報セキュリティを論じる対象の要素技術，システム，あるいは組織などに危害を与える原因となり得るものを**脅威**という。また，それらの要素技術，システム，あるいは組織などに内在し，脅威の影響を左右する弱さ（狭義には，具体的な欠陥そのもの）を**脆弱性**という[†2]。われわれは，脅威にさらされ，また，脅威が進化する中で，基本要素に関する品質管理に取り組むことになる。

1.1.1 守 秘 性

守秘性は，**秘匿性**あるいは**機密性**とも呼ばれる。ある情報の「守秘性を守る」とは，その情報を知らせてはならない主体にその情報を知られないようにすることであり，守ったままに保つ期間は技術によりさまざまである。

守秘性を守る技術として，**暗号技術**を考えよう。例えば，パスワードを元に生成した鍵による電子ファイルの暗号化は身近であろう。鍵の生成手法や暗号化のアルゴリズムは，その電子ファイルを処理するアプリケーションソフトウェアに実装されているとする。もし，暗号化のアルゴリズムに脆弱性があれば，攻撃

[†1] 必ずしも明確に定義されてはいないが，サイバー空間との関わりを強く意識する時には「サイバーセキュリティの確保」ともいう。

[†2] 脅威がもたらす危害を経済的な損失と解釈して定量的な議論をするために，脅威を「損失につながり得る原因が生起する確率」，脆弱性を「その原因が生起した際に，生起したという条件のもとで，実際に損失が生じる（例えば攻撃が生起した場合には，その攻撃が成功する）条件付き確率」と定義する場合もある（5 章の 5.3.1 項参照）。

者が，その脆弱性を突くツールで電子ファイルの内容を見るかもしれない。これは，暗号技術の問題である。一方，パスワードを知らせるべきでない相手にパスワードを知らせてしまうと，暗号技術に問題がなくとも守秘性が守られない。これは，**鍵管理** (key management) の問題である。また，そもそもパスワードで保護する作業を忘れたまま放置してしまう場合もあろう。だからといって即座に電子ファイルの内容を盗み見られるとは限らないが，守秘性は脅威にさらされる。これは，**人の誤り** (human error) の問題である。

守秘性を守る防御の焦点は情報にあり，脅威の源は多岐にわたる。

1.1.2 完 全 性

完全性は，**一貫性**とも呼ばれる。人や情報が想定しているとおりの本物である性質を**真正性** (authenticity) と呼んで，完全性と区別する場合もある。ある情報の「完全性を保つ」とは，その情報の不正な変更や詐称（改ざんや破壊など）を防止することである。より広義には，ICT に関するリソース（例えばメモリやソフトウェアのように，情報通信システムの動作を担う資源）や処理方法の不正な変更を防止することなども，完全性の観点で論じる。例えば，**ブロックチェーン** (blockchain) を利用した**スマート契約** (smart contract) では，契約した処理方法自体を，完全性検証できる仕組みで保管する。

完全性が保たれていることを確認する代表的な技術として，認証技術を考えよう。完全性を議論する対象の情報が文書である場合には**メッセージ認証** (message authentication)，個人を特定する身元情報である場合には**個人認証** (personal authentication) という。これらが脅威にさらされると，文書や身元情報を用いた処理に影響が出る。処理に用いるという観点で，文書や身元情報にもリソースとしての性格がある。一方，計算機プログラムなどのより一般的なリソースの完全性を保つことができない場合もある。例えば，不正なソフトウェアである**マルウェア** (**malware**: malicious software) に感染すると，多方面に影響が出かねない。

完全性を保つ防御の焦点にはリソースが加わり，影響の範囲（インパクト）は

多岐にわたる。

認証技術を用いて完全性が保たれていることを確認できても，完全性が保たれていないと判明した場合に元に戻す術(すべ)がなければ，完全性を保つことは難しい。処理を止めるなどの対応をとれば影響を軽微にとどめることはできるかもしれないが，根本的な解決にはならない。完全性に関する情報セキュリティ対策では，問題がある場合の対応すなわち**異常対応** (failure mode) が重要である。ブロックチェーンの場合，自律分散的に数多く存在するノードにすべてのブロックを保管すれば，異常対応時に規定通りに復元する機能も実現できる可能性がある。

1.1.3 可　用　性

あるリソースの「可用性を守る」とは，そのリソースが必要な時に十分な品質で利用できるようにすることである。利用できなければ不便なので，可用性を**利便性** (usability) の尺度と見なす場合もある。

可用性を守る代表的な技術として，ネットワークセキュリティ技術を考えよう。例えば，サーバをダウンさせるために大量の接続要求を送りつける**サービス妨害攻撃**（**DoS 攻撃**: Denial-of-Service attack）は，可用性に対する脅威である。サービス妨害攻撃は，そのオペレーションの単純さ故，攻撃ツールが出回った場合に素人が興味本位で使ってしまうリスクも高い。ネットワーク上の他人の言動に煽(あお)られて，あるいは，踏み台として乗っ取られた計算機を介して同時多発的に発生すれば，攻撃の威力は増大する。**ファイアウォール** (firewall) などのネットワークセキュリティ技術で攻撃を検知してブロックするという対策は，常時稼働を旨として講じるべきである。

攻撃ではない正当な通信も，可用性低下の原因となり得る。例えば，人気の高いイベントの参加申込受付開始時に，申込用 Web サイトの混雑で接続できない場合がある。また，事前の予測が難しい天変地異や社会的事件が引き起こすパニックによる可用性低下も，サービスの品質を大きく左右する。これらの影響を低減するために常時稼働の情報セキュリティ対策を緩めると，その時に到

来した攻撃が被害をもたらす確率が高まる。パニックが意図的な虚言やほかの情報セキュリティインシデント†によって起きたものである場合には，いくつかの準備行動や攻撃を組み合わせたハイブリッドな攻撃の可能性もある。

あるシステム内の情報やプログラムなどが改ざんされたり破壊されたりすると，そのシステムは思い通りに使えないかもしれない。しかし，直接的な改ざんや破壊がなくとも，可用性が脅かされることはあり得る。

可用性を守る防御の焦点にはサービスが加わり，脅威の伝搬経路は多岐にわたる。

1.1.4 信 頼 関 係

アプリケーション固有の「信頼関係を守る」とは，時空間的に離れた事象に関する主張を，必要な時に必要な場所で，確実に成り立たせることである。

信頼関係を守る代表的な技術として，ブロックチェーンを利用した**仮想通貨** (virtual currency) を考えよう。その額面の価値を持つということと**二重使用** (double spending) ではないということを主張する場合，額面の価値は入手時の行為に関連し，二重使用の有無は過去の使用行為すべてと関連する。ブロックチェーンでは，それらの行為に関する電子的な証拠を生成したり検証したりするメカニズムを備え，信頼関係を守ろうとする。ただし，額面価値を主張時のレートや環境のもとで変換した実質価値（例えば，現実通貨に換算した価値）は，変換作業を実行する場所や主体によって異なる場合がある。額面に，仮想通貨の単位で表した数値だけでなくほかの補助的な情報（例えば有効期間）も記されている場合，変換作業は外貨両替のように単純なものではなく，複雑な**解釈作業** (interpretation) になり得る。

信頼関係を守る防御の焦点は主張にあり，解釈は多岐にわたる。

† 情報セキュリティに関する事故や事件。情報セキュリティに関するということが文脈から明らかな場合には，単に**インシデント**ともいう。

索　　引

―― 著 者 略 歴 ――

1992年　東京大学工学部電気工学科卒業
1994年　東京大学大学院工学系研究科修士課程修了（電子工学専攻）
1997年　東京大学大学院工学系研究科博士課程修了（電子工学専攻），博士（工学）
1997年　東京大学助手
1998年　東京大学講師
2002年　東京大学助教授
2007年　東京大学准教授
2014年　東京大学教授
　　現在に至る

情報セキュリティ基礎講義

Lecture on Fundamentals of Information Security

2019 年 3 月 18 日　初版第 1 刷発行

検印省略

著　　者　松浦幹太（まつうらかんた）
発 行 者　株式会社　コロナ社
　　代 表 者　牛来真也
印 刷 所　三美印刷株式会社
製 本 所　有限会社　愛千製本所

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　http://www.coronasha.co.jp

ISBN 978–4–339–01934–6　C3355　Printed in Japan　（齋藤）