

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

編集委員長

博士（情報理工学） 浅見 徹（東京大学）

編集委員

（五十音順）

博士（理学） 河野 健二（慶應義塾大学）

博士（情報学） 五島 正裕（国立情報学研究所）

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

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ジタルメディアに書き込まれるようになってきている。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

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^{ちゆう}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

1 章 情報セキュリティの基本

1.1	基本要素	2
1.1.1	守秘性	2
1.1.2	完全性	3
1.1.3	可用性	4
1.1.4	信頼関係	5
1.2	管理サイクル	6
1.2.1	計画段階	6
1.2.2	実施段階	7
1.2.3	評価検証段階	8
1.2.4	処置改善段階	9
1.3	三原則	10
1.3.1	明示性の原則	10
1.3.2	首尾一貫性の原則	12
1.3.3	動機付け支援の原則	13
1.4	ベストプラクティス	17
1.4.1	アドレス確認	17
1.4.2	任務の分離	18
1.4.3	最小権限への制限	18
1.4.4	ルーチン化	19
1.4.5	情報セキュリティポリシー	20

1.5	安全性評価	20
1.5.1	計算量的安全性	24
1.5.2	情報理論的安全性	24
1.5.3	形式検証	26
1.5.4	経験的安全性	29
	演習問題	30

2 章 暗 号

2.1	暗号の使い方	33
2.2	共通鍵暗号	35
2.2.1	DES	36
2.2.2	差分攻撃	39
2.2.3	ブロック暗号の動作モード	41
2.3	暗号学的ハッシュ関数	45
2.3.1	機能と性質	45
2.3.2	Merkle-Damgård 構成	50
2.4	公開鍵暗号	59
2.4.1	数論の基礎	59
2.4.2	教科書的 RSA 暗号	69
2.4.3	公開鍵暗号スキームへの安全性強化	73
2.4.4	KEM-DEM	78
2.5	電子署名	80
2.5.1	安全性定義	80
2.5.2	教科書的 RSA 署名	82
2.5.3	電子署名スキームへの安全性強化	82
2.5.4	否認不可	85
	演習問題	85

3 章 ネットワークセキュリティ

- 3.1 ファイアウォール 89
 - 3.1.1 達成度 90
 - 3.1.2 攻撃モデル 91
 - 3.1.3 静的な基本設定 92
 - 3.1.4 動的な設定表への拡張 95
 - 3.1.5 ネットワークアドレス変換 96
 - 3.1.6 攻撃モデルへの対応 98
 - 3.1.7 パケットフィルタリングの限界 99
 - 3.2 仮想専用線 101
 - 3.2.1 鍵共有 101
 - 3.2.2 カプセル化 109
 - 3.2.3 ローミング 111
 - 3.3 TLS と Web セキュリティ 118
 - 3.3.1 TLS 118
 - 3.3.2 インジェクション攻撃 121
 - 3.3.3 標的型攻撃 122
 - 3.4 情報セキュリティの基盤 123
 - 3.4.1 認証基盤 123
 - 3.4.2 情報共有基盤 128
- 演習問題 130

4 章 コンピュータセキュリティ

- 4.1 アクセス制御 133
 - 4.1.1 枠組み 133
 - 4.1.2 認証と認可 134
 - 4.1.3 モデル 136
 - 4.1.4 異常対応 138

4.2	個人認証	139
4.2.1	個人認証の基礎	139
4.2.2	パスワード認証	142
4.2.3	生体認証	145
4.2.4	多要素認証とユーザブルセキュリティ	151
4.3	マルウェア	155
	演習問題	160

5 章 応用例と社会

5.1	匿名通信システム	163
5.1.1	匿名通信の基本概念	163
5.1.2	オニオンルーティング	164
5.1.3	安全性	170
5.2	分散台帳	174
5.2.1	ブロックチェーン	174
5.2.2	プロトコル式	179
5.2.3	仮想通貨	179
5.2.4	安全性	180
5.2.5	スケーラビリティ	181
5.3	情報セキュリティと社会	182
5.3.1	行動と経済学	182
5.3.2	情報セキュリティ倫理	188
	演習問題	191

引用・参考文献	193
演習問題解答例	194
索引	206

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、端的に言えば、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る。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

【あ】		一方向性 one-wayness 22	鍵管理 key management 3
アクセス制御 access control 133		(ハッシュ関数の部分的な) 一方向性破り partial hash inversion 178	鍵共有ペイロード key-agreement payload 165
アクセス制御行列 access-control matrix 137		移動通信機器 mobile node 112	鍵スケジューリング key scheduling 36
アクセス制御リスト access-control list 135		入口番人 entry guard 164	鍵生成の種 pre-master secret 120
アドウェア adware 156		インジェクション攻撃 injection attack 121	拡大転置 expansion permutation 36
暗号化 encryption 33		インターネット鍵交換 Internet Key Exchange 104	確率過程 stochastic process 48
暗号化オラクル encryption oracle 21		インターネットプロトコル Internet Protocol 91	仮想通貨 virtual currency 5
暗号化鍵 encryption key 33		【う】	
暗号学的ハッシュ関数 cryptographic hash function 46		ウルフ wolf 141	カプセル化セキュリティ ペイロード encapsulated security payload 110
暗号プリミティブ cryptographic primitive 35		ウルフ攻撃率 wolf-attack probability 141	可用性 availability 2
暗号文 ciphertext 21, 33		【お】	
暗号文空間 ciphertext space 33		オイラーのファイ関数 Euler's phi function 62	環境税 environmental tax 15
暗号文単独攻撃 ciphertext-only attack 21		オニオンルーティング onion routing 164	完全性 integrity 2
暗号モジュール試験および 認証制度 Japan cryptographic module validation program 130		【か】	
安全性定義 security notion 20		解釈作業 interpretation 5	【き】 偽陰性率 false negative rate 31
【い】		外部性 externality 13	気付けアドレス Care-of Address 112
異常対応 failure mode 4		外部不経済 external diseconomies 13	(法のもとの) 逆数 modular inverse 60
位数 order 64		鍵カプセル化機構 key-encapsulation mechanism 78	逆トンネリング reverse tunneling 113
			キャプチャ Completely Automated Public Turing tests to tell Computers and Humans Apart 144

教科書的 RSA 暗号
textbook RSA encryption 69

強制アクセス制御
mandatory access control 136

偽陽性率
false positive rate 31

共通鍵暗号
symmetric-key encryption 33

許可者限定チェーン
permitted chain 181

許可不要チェーン
permissionless chain 181

【く】

クエリ
query 21

クッキー
Cookie 108

【け】

計画段階
Plan 6

経験的安全性
heuristic security 29

経験的論証
heuristic argument 29

形式検証
formal verification 27

形式的手法
formal method 26

ケイバビリティ
capability 137

経路最適化
route optimization 114

結果レベルの統合
decision-level fusion 153

ケルクホフスの原則
Kerckhoffs' principle 10

権限
privilege 18

原始根
primitive root 66

検証者
verifier 139

健全性
soundness 39

【こ】

公開鍵
public key 33

公開鍵暗号
public-key encryption 33

公開鍵基盤
public-key infrastructure 124

公開鍵証明書
public-key certificate 120

公平な交換
fair exchange 180

個人認証
personal authentication 3

コンセンサスアルゴリズム
consensus algorithm 178

コンピュータウイルス
computer virus 156

【さ】

採掘
mining 178

採掘者
miner 176

再送攻撃
replay attack 110

サイドチャネル攻撃
side-channel attack 173

サービス妨害攻撃
Denial-of-Service attack 4

差分攻撃
differential attack 40

参照モニタ
reference monitor 133

サンドボックス
sandbox 159

【し】

識別不可能性
indistinguishability 22

辞書攻撃
dictionary attack 143

時相論理
temporal logic 27

実現値
occurrence 48

実験の評価
experimental evaluation 29

実施段階
Do 7

シビル攻撃
Sybil attack 170

社会関係資本
social capital 16

受信者動作特性
receiver operating characteristic 149

受信者匿名性
recipient anonymity 163

首尾一貫性の原則
consistency principle 10

守秘性
confidentiality 2

状態あり検査
stateful inspection 96

衝突
collision 46

情報共有分析組織
information sharing and analysis center 128

情報セキュリティ投資による純利益の期待値
Expected Net Benefit from an investment in Information Security 185

情報セキュリティの相互依存性
interdependency of information security 14

情報セキュリティポリシー information security policy 20	スマート契約 smart contract 3	ソルティング salting 144
情報セキュリティマネジメン トシステム information security management system 30	【せ】	ソルト salt 144
情報通信技術 information and commu- nication technology 2	生成元 generator 66	存在的偽造不可能性 existential unforgeability 81
証明者 prover 139	生体検知 liveness detection 140	【た】
証明書失効リスト certificate revocation list 124	生体認証 biometric authentication または biometrics authentication 145	対向機器 correspondent node 112
初期転置 initial permutation 37	静的解析 static analysis 159	タイミング攻撃 timing attack 172
初期ベクトル initial vector 42	制度設計 mechanism design 15	ただ乗り問題 free-riding problem 14
処置改善段階 Act 9	製品認証 product validation 129	他人受入率 false-acceptance rate 141
人工知能 artificial intelligence 191	責任ある開示 responsible disclosure 189	他人分布 impostor distribution 148
真正性 authenticity 3	セキュリティ・バイ・デザ イン security by design 189	多要素認証 multi-factor authentication 151
信頼関係 trust relationship 2	セキュリティマネジメント security management 6	単純セキュリティ特性 simple security property 27
信頼できる第三者機関 trusted third party 24	ゼロデイ攻撃 zero-day attack 92	誕生日攻撃 birthday attack 50
【す】	選択暗号文攻撃 chosen-ciphertext attack 21	誕生日パラドックス birthday paradox 50
数論 number theory 59	選択文書攻撃 chosen-message attack 47	【ち】
スキーム scheme 74	選択平文攻撃 chosen-plaintext attack 21	チャレンジ challenge 34
スコアレベルの統合 score-level fusion 153	専用ハッシュ関数 dedicated hash function 50	中央処理装置 central processing unit 158
ストリーム暗号 stream cipher 35	【そ】	中間者攻撃 man-in-the-middle attack 104
スパイウェア spyware 156	送受信者リンクの匿名性 unlinkability of sender and recipient 163	中間中継者 middle relay 164
スプーフィング spoofing 94	送信者匿名性 sender anonymity 163	(Tor の) 中継者 Tor relay あるいは 単に relay 164

【て】

デジタルフォレンジック	
digital forensic	19
定理証明	
theorem prover	27
適応的選択暗号文攻撃	
adaptive chosen-ciphertext attack	21
適応的選択文書攻撃	
adaptive chosen-message attack	81
適応的選択平文攻撃	
adaptive chosen-plaintext attack	21
出口中継者	
exit relay	164
出口フラグ	
exit flag	165
データカプセル化機構	
data-encapsulation mechanism	78
デフォルト棄却	
default deny	95
電子証拠物	
digital evidence	48
転置	
permutation	36
テンプレート	
template	145
【と】	
動機付け支援の原則	
incentive-mechanism principle	10
統合	
fusion	151
動作モード	
mode of operation	42
同定	
identification	140
同定誤り率	
identification-error rate	142

動的解析	
dynamic analysis	159
登録更新	
binding update	114
特徴量レベルの統合	
feature-level fusion	154
ドメインネームシステム	
Domain Name System	91
トロイの木馬	
Trojan horse	156
トンネリング	
tunneling	113

【な】

内閣サイバーセキュリティセンター	
National center of Incident readiness and Strategy for Cybersecurity	20

【に】

二重使用	
double spending	5
任意アクセス制御	
discretionary access control	136
認可	
authorization	135
認証	
authentication	140
認証局	
certificate authority	121
任務の分離	
separation of duties	18

【ね】

ネットワークアドレス変換	
network address transform	96
ネットワーク侵入検知システム	
network intrusion detection system	90

【は】

バイオメトリックス	
biometrics	145
ハイブリッド暗号	
hybrid encryption	78
バックアップ認証	
backup authentication	7
ハッシュ関数	
hash function	46
パッド	
pad	8
バッファオーバーフロー	
buffer overflow	157
パディング	
padding	8
バーナム暗号	
Vernam cipher	25
ハニーポット	
honeypot	160
番人フラグ	
guard flag	164
番人ローテーション	
guard rotation	165

【ひ】

ビットごとの排他的論理和	
bitwise exclusive OR	25
人の誤り	
human error	3
否認不可	
non-repudiation	85
非武装地帯	
demilitarized zone	89
秘密鍵	
secret key あるいは private key	33
評価検証段階	
Check	8
標的型攻撃	
targeted attack	122

【ふ】			
ファイアウォール firewall	4, 89	本人拒否率 false-rejection rate	142
フィッシング phishing	17	本人分布 genuine distribution	147
フォールバック認証 fallback authentication	7	【ま】	
フォワードセキュリティ forward security	102	マスク生成関数 mask generation function	78
復号 decryption	21, 33	マルウェア malicious software	3, 155
復号オラクル decryption oracle	21	マルチモーダル生体認証 multi-modal biometrics	151
復号鍵 decryption key	33	【め】	
ブロック暗号 block cipher	35	明示性の原則 explicitness principle	10
ブロックチェーン blockchain	3	メッセージ認証 message authentication	3
プロトコル一式 protocol suite	174	メッセージ認証子 message authentication code	47
分散台帳 distributed ledger	174	【も】	
【へ】		モダリティ modality	145
閉塞対策トークン anti-clogging token	107	モデル検査 model checking	27
平文 plaintext	21, 33	【ゆ】	
平文空間 plaintext space	33	ユーザブルセキュリティ usable security	139
【ほ】		【よ】	
ボット bot	91	要求者 claimant	139
本拠地アドレス Home Address	112	【ら】	
本拠地代理人 home agent	112	ラウンド round	37
		ラム lamb	160
		ランサムウェア ransomware	157
		ランダムオラクル random oracle	74
		ランダムオラクルモデル random-oracle model	75
		【り】	
		利己の採掘 selfish mining	204
		リスク中立性 risk neutrality	184
		利便性 usability	4
		【る】	
		ルートキット rootkit	156
		【れ】	
		レインボー攻撃 rainbow attack	145
		レインボーテーブル rainbow table	144
		レスポンス response	34
		連結 concatenation	37
		【ろ】	
		ローミング roaming	112
		【わ】	
		ワーム worm	156
		ワンタイムパッド one-time pad	25

[A]

ACL
access-control list 135

ACMA
adaptive chosen-message
attack 81

AES
advanced encryption
standard 37

AI
artificial intelligence 191

[B]

BU
binding update 114

[C]

CA
certificate authority 121

CAPTCHA
Completely Automated
Public Turing tests to tell
Computers and Humans
Apart 144

CBC
cipher block chaining 43

CFB
cipher feedback 44

CN
correspondent node 112

CoA
Care-of Address 112

CPU
central processing unit
158

CRL
certificate revocation list
124

[D]

DAC
discretionary access
control 136

DEM
data-encapsulation
mechanism 78

DES
data encryption
standard 36

Diffie-Hellman 鍵共有
Diffie-Hellman key
agreement 103

DMZ
demilitarized zone 89

DNS
Domain Name System 91

DoS 攻撃
Denial-of-Service attack 4

DV
domain validation 125

[E]

ECB
electronic codebook 42

ENBIS
Expected Net Benefit
from an investment in
Information Security 185

ESP
encapsulated security
payload 110

EUf
existential unforgeability
81

EV
extended validation 125

[F]

f 関数
f function 37

FAR
false-acceptance rate 141

FNR
false negative rate 31

FPR
false positive rate 31

FRR
false-rejection rate 142

[G]

Gordon-Loeb モデル
Gordon-Loeb model 184

[H]

HA
home agent 112

HoA
Home Address 112

[I]

ICT
information and commu-
nication technology 2

IER
identification-error rate
142

IKE
Internet Key Exchange 104

IP
Internet Protocol 91

ISAC
information sharing and
analysis center 128

ISMS
information security
management system 30

【J】

JCMVP
Japan cryptographic
module validation
program 130

【K】

KEM
key-encapsulation
mechanism 78

KEM-DEM の枠組み
KEM-DEM framework 79

【M】

MAC
mandatory access control 136

MAC
message authentication
code 47

MAC アドレス
media access control
address 127

malware
malicious software 3, 155

Merkle-Damgård 構成
Merkle-Damgård
construction 54

MGF
mask generation function 78

MIM
man-in-the-middle attack 104

MN
mobile node 112

【N】

NAT
network address
transform 96

NIDS
network intrusion
detection system 90

NISC
National center of Inci-
dent readiness and Strat-
egy for Cybersecurity 20

NRU
no read-up 28

NWD
no write-down 28

【O】

OAEP
optimal asymmetric
encryption padding 76

OFB
output feedback 42

OV
organization validation 125

【P】

PDCA サイクル
Plan-Do-Check-Act cycle 6

PKI
public-key infrastructure 124

PMS
pre-master secret 120

PSS
probabilistic signature
scheme 83

【R】

ROC
receiver operating
characteristic 149

RSA 暗号
RSA encryption 69

RSA 合成数
RSA composite 70

RSA 問題
RSA problem 72

【S】

S 箱
S-box または substitution
box 38

SSL
secure sockets layer 119

【T】

TCB
trusted computing base 134

TLS
transport layer security 119

Tor
the onion routing 164

TTP
trusted third party 24

【v】

VPN
virtual private network 101

【w】

WAP
wolf-attack probability 141



【記号】

*-特性 27
*-property

— 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

© Kanta Matsuura 2019

2019年3月18日 初版第1刷発行

検印省略

著者 ^{まつ}松 ^{うら}浦 ^{かん}幹 ^た太
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)



JCCOPY <出版者著作権管理機構 委託出版物>

本書の無断複製は著作権法上での例外を除き禁じられています。複製される場合は、そのつど事前に、出版者著作権管理機構（電話 03-5244-5088, FAX 03-5244-5089, e-mail: info@jccopy.or.jp）の許諾を得てください。

本書のコピー、スキャン、デジタル化等の無断複製・転載は著作権法上での例外を除き禁じられています。購入者以外の第三者による本書の電子データ化及び電子書籍化は、いかなる場合も認めていません。落丁・乱丁はお取替えいたします。