

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で 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

1.1 情報セキュリティとは	1
1.1.1 情報セキュリティに関する特性	1
1.1.2 情報セキュリティ対策と利便性	2
1.2 セキュリティとリスク	2
1.3 情報資産	3
1.3.1 有形資産	4
1.3.2 無形資産	4
1.4 脆弱性	4
1.5 脅威	5
1.5.1 脅威の分類	5
1.5.2 災害	6
レポートワーク	6

2. 情報システムに関する脅威

2.1 人的脅威	7
2.1.1 攻撃の動機の変遷	7
2.1.2 人的脅威の種類	8
2.1.3 無知や技術力不足	9
2.1.4 ゼロトラスト	10
2.2 技術的脅威	11
2.3 マルウェア	12

2.3.1	コンピュータウイルス	12
2.3.2	ワーム	12
2.3.3	トロイの木馬	12
2.4	マルウェアの目的からの分類	13
2.4.1	スパイウェア	13
2.4.2	アドウェア	13
2.4.3	ランサムウェア	13
2.4.4	スケアウェア	14
2.4.5	マルウェアによる被害例	14
	レポートワーク	14

3. 暗 号

3.1	暗号技術	15
3.2	共通鍵暗号方式	16
3.3	公開鍵暗号方式	19
3.3.1	公開鍵暗号方式の流れ	20
3.3.2	公開鍵暗号方式の鍵数	21
3.3.3	ハイブリッド暗号システム	22
3.3.4	公開鍵暗号通信への中間者攻撃	23
3.4	PKI	24
3.4.1	PKIの構成	25
3.4.2	PKIにおける手続き	25
3.4.3	電子証明書の信頼性	26
3.4.4	SHA-1 ハッシュ関数の利用廃止とサーバ証明書の切り替え	27
3.5	電子署名	28
3.5.1	電子署名の仕組み	28
3.5.2	電子署名の応用	30
	レポートワーク	31

4. 認 証

4.1 認 証 技 術	32
4.1.1 知 識 情 報	33
4.1.2 生 体 情 報	35
4.1.3 所 持 情 報	36
4.2 認 証 シ ス テ ム	37
4.2.1 RADIUS (Remote Authentication Dial In User Service)	38
4.2.2 LDAP (Lightweight Directory Access Protocol)	38
4.2.3 AD (Active Directory)	38
4.2.4 IEEE802.1X 認 証	38
4.2.5 Shibboleth	39
4.3 パ ス ワ ー ド 認 証	39
4.3.1 パ ス ワ ー ド 認 証 の 例	40
4.3.2 パ ス ワ ー ド 認 証 の 変 化	41
4.3.3 パ ス ワ ー ド 認 証 へ の 攻 撃	43
4.4 認 証 処 理 の 一 元 化	46
4.4.1 認 証 シ ス テ ム の 統 合	46
4.4.2 シ ン グ ル サ イ ン オ ン	47
4.5 フ ェ デ レ ー シ ョ ン	48
4.5.1 SAML 認 証	49
4.5.2 Web API	51
4.5.3 OAuth	52
4.6 多 要 素 認 証	53
4.6.1 二 段 階 認 証	53
4.6.2 多 要 素 認 証	54
4.6.3 認 証 シ ス テ ム の 被 害 例	55
レポ ー ト ワ ー ク	56

5. ネットワークセキュリティ

5.1 ネットワークにおける脅威	57
5.1.1 不正アクセス	57
5.1.2 サービス拒否攻撃	59
5.2 防御システム	60
5.2.1 ファイアウォール	61
5.2.2 ファイアウォールの種類	63
5.2.3 IDS	66
5.2.4 IPS	66
5.2.5 WAF	67
5.2.6 マルウェア対策システム	68
5.3 予防技術	70
5.3.1 VPN	70
5.3.2 暗号化通信	71
5.4 無線 LAN	73
5.4.1 WEP	73
5.4.2 TKIP	74
5.4.3 AES	74
5.4.4 WPA	74
5.4.5 MAC 認証	75
5.4.6 IEEE802.1X	75
5.4.7 無線 LAN の運用	76
レポートワーク	77

6. アプリケーションセキュリティ

6.1 電子メールセキュリティ	78
6.1.1 電子メールシステム	78

6.1.2	電子メールシステムの暗号化	80
6.1.3	PPAP	81
6.1.4	迷惑メール対策	82
6.1.5	メールのブラックリスト	84
6.2	Web アプリケーションセキュリティ	86
6.2.1	WWW の仕組み	86
6.2.2	Web アプリケーションの構成	87
6.2.3	コードインジェクションとエスケープ処理	87
6.2.4	クロスサイトスクリプティング	90
6.2.5	リクエスト強要	92
6.2.6	SQL インジェクション	93
6.2.7	OS コマンドインジェクション	94
6.2.8	ハードコーディングによる脆弱性	96
6.2.9	セッション管理不備	96
	レポートワーク	98

7. 物理的なセキュリティ対策

7.1	物理的に実施するセキュリティ対策	99
7.1.1	ゾーニング	99
7.1.2	アンチパスバック機能	100
7.2	災害への対策	101
7.2.1	地震対策	103
7.2.2	水害対策	104
7.2.3	雷対策	105
7.2.4	火災対策	106
7.2.5	停電対策	106
	レポートワーク	108

8. 予 防 技 術

8.1	バックアップとリストア／リカバリ	109
8.1.1	情報システムのバックアップ	110
8.1.2	バックアップの種類	111
8.1.3	増分バックアップと差分バックアップの違い	113
8.1.4	スナップショット	115
8.1.5	バックアップのスケジュール	116
8.1.6	バックアップとリストア／リカバリの注意点	117
8.1.7	バックアップに関する事例	119
8.2	ストレージの保全技術	120
8.2.1	ストレージ	120
8.2.2	DAS	120
8.2.3	NAS	121
8.2.4	SAN	122
8.3	RAID	122
8.3.1	RAID0	123
8.3.2	RAID1	124
8.3.3	RAID0+1 と RAID1+0	125
8.3.4	RAID4	128
8.3.5	RAID5	128
8.3.6	RAID6	129
8.3.7	RAID システムの障害と選択	130
8.4	特 権 分 離	131
	レポートワーク	132

9. 情 報 漏 洩

9.1	情報漏洩とは	133
9.2	情報漏洩に関する攻撃と対策	134

9.2.1 盗聴・盗撮	134
9.2.2 ネットワークの盗聴	135
9.2.3 パスワードクラック	136
9.2.4 パスワードクラック対策	138
9.2.5 記録媒体の廃棄	139
9.2.6 パスワードロック	141
9.2.7 耐タンパ性	142
9.3 情報漏洩の事例	142
9.3.1 記録媒体からの漏洩の例	142
9.3.2 漏洩情報の公開の例	143
9.3.3 P2P ネットワークでの事例	144
9.3.4 対策不備による事例	145
9.3.5 匿名掲示板の情報流出	145
9.3.6 社員によるデータ持ち出しの例	146
9.4 情報漏洩の防止と対応	146
レポートワーク	147

10. セキュリティマネジメント

10.1 情報セキュリティマネジメントとは	148
10.2 情報セキュリティマネジメント体制	149
10.2.1 情報セキュリティポリシー	150
10.2.2 PDCA モデル	151
10.2.3 ISMS	152
10.2.4 プライバシーマーク制度	153
レポートワーク	154

11. セキュリティ関連法規と標準

11.1 セキュリティ関連法規	155
-----------------	-----

11.1.1	不正アクセス禁止法	155
11.1.2	不正指令電磁的記録に関する罪	156
11.1.3	電子署名法	156
11.1.4	e - 文書法	157
11.1.5	電子帳簿保存法	157
11.1.6	プロバイダ責任制限法	157
11.2	知的財産	158
11.2.1	知的財産権	158
11.2.2	著作権と著作者人格権	159
11.2.3	著作権法の改正	159
11.3	個人情報	160
11.3.1	個人情報とは	160
11.3.2	パーソナルデータの利活用	162
11.4	標準化組織と関連規格	163
11.4.1	国際組織	164
11.4.2	国内組織	166
	レポートワーク	166
	引用・参考文献	167
	索引	172

【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 27000:2018²⁾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。

2 1. 情報セキュリティの概要

ア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^{ざん}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ないか把握して、関係者に説明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）。

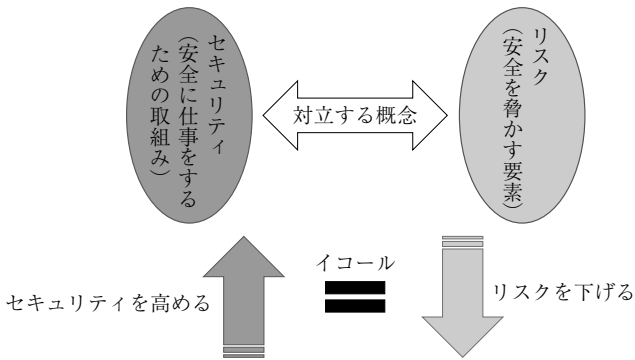


図 1.2 セキュリティとリスク

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

【あ】		【か】		【こ】	
アクセストークン	52	鍵数の問題	17	公開鍵	19
アクティブディレクトリ	38	鍵配送センター	18	公開鍵暗号方式	16
アドウェア	13	鍵配送問題	17, 18	工業的保護	158
アプライアンス	64	学術認証フェデレーション		公的個人認証サービス	30
暗号化	15		49	行動的特徴	35
暗号鍵	15	学 認	49	国際電気通信連合	164
暗号化通信	71	火災対策	106	国際電気標準会議	164
暗号技術	15	雷サージ	105	国際標準化機構	164
暗号文	15	雷対策	105	国税電子申告・	
暗号方式	15	仮名加工情報	163	納税システム	54
アンチパスバック機能	100	可用性	2	個人識別符号	161
		完全性	2	個人情報	160
				——の保護に関する法律	160
【い】		【き】			
育成者権	158	技術的脅威	6, 11	個人情報保護委員会	161
意匠権	158	機密性	1	個人情報保護関連法	160
意匠法	158	脅 威	2, 5	個人情報保護マネジメント	
一貫性	2	行政機関の保有する個人情		システム	153
一般データ保護規則	163	報の保護に関する法律	160	個人データ	161
違法ダウンロード	160	行政機関の保有する個人情		誤操作	8
		報保護法等の施行に伴う		コードインジェクション	87
		関連法律の整備等に関する		コンセントタップ型の	
		法律	160	盗聴器	135
		共通鍵暗号方式	15, 16	コンピュータウイルス	12
				——に関する罪	156
		【く】		【さ】	
		クロスサイト		災 害	6
		スクリプティング	90	サイバーテロ	8
		クロスサイトリクエスト		サービス拒否攻撃	59
		フォージェリ	92	サービス不能攻撃	59
		グローバルアンチパス		サブリカント	38
		バック	101	差分バックアップ	112
		【け】		サンドボックス	69
		経済協力開発機構	162		
		権限分離	131		
【お】					
追っかけ配信	160				
オフィスエリア	99				
オフライン	122				
オンライン	122				
オンライン識別子	163				
オンラインストレージ	120				

【し】

識 別 32
 識別符号 57
 辞書攻撃 137
 地震対策 103
 自然災害 6,101
 実用新案権 158
 実用新案法 158
 シボレス 39
 瞬 停 106
 商標権 158
 商標法 158
 商 法 158
 情報公開・個人情報保護
 審査会設置法 160
 情報資産 2,3
 情報セキュリティ 1
 情報セキュリティ基本方針 150
 情報セキュリティ実施手順 151
 情報セキュリティ対策基準 151
 情報セキュリティポリシー 150
 情報セキュリティマネジ
 メント 148
 情報セキュリティマネジ
 メントシステム 152
 情報セキュリティマネジ
 メント制度 152
 情報セキュリティマネジ
 メント体制 149
 情報漏洩 133
 初期バックアップ 111
 ジョークプログラム 7
 所持情報 33
 ショルダーハッキング 9
 人為的エラー 6
 人為的災害 6,101
 人 災 6,101
 真正性 2
 身体的特徴 35
 人的脅威 6,7
 侵入検知システム 66

侵入防衛システム 66
 信頼性 2

【す】

水害対策 104
 スキャベンジング 9
 スケアウェア 13
 ステートフルイン
 スペクション 65
 ストライピング 123
 ストレージ 120
 スナップショット 115
 砂 場 69
 スパイウェア 13

【せ】

脆弱性 2,4
 生体情報 33,35
 セキュリティインシデント 1
 セキュリティエリア 99
 セキュリティ関連法規 155
 セキュリティ対策 2
 セキュリティポリシー 150
 セキュリティホール 5
 セッションID 97
 セッション管理 96
 セッション管理不備 96
 説明可能性 2
 セーフティ 101
 ゼロトラスト 11

【そ】

増分バックアップ 112
 ソーシャル
 エンジニアリング 9
 ゴーニング 99
 ゾンビPC 60

【た】

対称鍵暗号方式 15,16
 耐タンパ機能 142
 耐タンパ性 142
 楯円曲線暗号 20
 多要素認証 46,53,54

【ち】

知識情報 33
 知的財産 158
 知的財産基本法 158
 知的財産権 158
 チャレンジレスポンス方式 44
 中間者攻撃 23
 著作権 158,159
 著作権法の改正 159
 著作人人格権 159
 著作物 159

【て】

定期的なパスワード変更 42
 定義ファイル 69
 停電対策 106
 ディフィー・ヘルマン
 鍵交換方式 18
 データ消去証明書 141
 電子計算機を使用して作成
 する国税関係帳簿書類の
 保存方法等の特例に関す
 る法律 157
 電子署名 28
 —及び認証業務に
 関する法律 28,156
 電子署名法 28,156
 電子帳簿保存法 157
 電磁的記録不正作出及び
 供用罪 156

【と】

透過性 70
 盗 撮 134
 同時配信 160
 盗 聴 134
 盗聴器検出器 135
 登録局 25
 匿名加工情報 163
 匿名掲示板 145
 独立行政法人の保有する個
 人情報の保護に関する法
 律 160
 トークン 45

特許権	158	パリティ	128	フルバックアップ	112
特許法	158			ブレースホルダ	94
特権分離	131	【ひ】		プロバイダ責任制限法	157
トラッキング	9	非対称鍵暗号方式	16	紛失	8
トロイの木馬	12	秘匿性	1	【ほ】	
【な】		否認防止性	2	ボット	60
なりすまし	9	非武装地帯	62	ホットスワップ	130
【に】		秘密鍵	19	【ま】	
ニアライン	122	ヒューリスティック方式	69	マイナンバーカード	30,37,55
二段階認証	53	標準化	163	マトリクス認証	34
日本規格協会	166	標準化組織	163	マルウェア	12
日本産業規格	166	平文	15	マルウェア対策システム	68
日本産業標準調査会	166	【ふ】		【み】	
認可	32,33	ファイアウォール	61	見逃し配信	160
認証	32	フィッシング	155	身代金	13
認証局	25	フィルタファイル	69	ミラーリング	124
認証システム	37	フィルタルール	61	民間事業者等が行う書面の 保存等における情報通信 の技術の利用に関する法 律	157
【は】		フェデレーション	48	——の施行に伴う関係法 律の整備等に関する法律	157
廃棄	139	復号	15	【む】	
廃棄証明書	141	不正アクセス	57	無形資産	4
ハイブリッド		不正アクセス禁止法	155	無方式主義	159
暗号システム	22	不正アクセス行為の禁止等 に関する法律	57,155	【め】	
バインド機構	94	不正競争防止法	158	メールソフト	43,53
バインド値	94	不正顕示機能	142	【ゆ】	
ハザードマップ	6	不正行為	8	有形資産	4
パスワード	39	不正司令電磁的記録	156	【ら】	
パスワードクラック	136	——に関する罪	156	ラックマウントサーバ	103
パスワードスプレー攻撃	138	不正指令電磁的記録供用・ 同未遂罪	156	ラディウス	38
パスワード認証	39	不正指令電磁的記録取得・ 保管罪	156	ランサムウェア	13
パスワードリスト攻撃	137	不正対抗機能	142	【り】	
パスワードロック	141	不正防護機能	142	リカバリ	110
パソコン遠隔操作事件	93	不正利用	8	リストレスト強要	92
パーソナルデータ	162	フタかぶせ	160		
パーソナル		物理的脅威	6		
ファイアウォール	64	プライバシー保護と個人デ ータの国際流通に関する ガイドライン	162		
破損	8	プライバシーマーク制度	153		
パターンマッチング方式	69	ブラウザ	86		
バックアップ	109	ブラックリスト	84		
——のスケジュール	116	ブルートフォースアタック			
ハードウェアトークン	36		136		
ハードコーディング	96				
ハードディスクドライブ	109				
パブリックエリア	99				

リスク 2 リストア 110 リソースサーバ 52 リプレイ (再生) 攻撃 43	【る】 【ろ】	【わ】 ワクチンソフト 68 ワーム 12 ワンタイムパスワード 44
	ルールデータベース方式 69 ローカルアンチバズバック 101	

【A】 Act 152 Active Directory 38 AD 38 Advanced Encryption Standard 17, 74 adware 13 AES 17, 74 Antinny 144 ARCFOUR Algorithm 17 ASIC 64	cyber-terrorism 8 【D】 DAS 120 Data Encryption Standard 17, 74 DDoS 60 De Militarized Zone 62 Denial of Service attack 59 DES 17, 74 dictionary attack 137 Diffie-Hellman 鍵交換方式 18 Direct Attached Storage 120 Distributed Denial of Service 59 DMZ 62 Do 152 DoS 攻撃 59 DRAGONBLOOD 75	【G】 GDPR 163 General Data Protection Regulation 163 【H】 hard coding 96 Hard Disk Drive 109 hazard 4 HDD 109 HTTPS 通信 22
【B】 back up 109 Bagle 7 bot 60 brute force attack 136 BS7799 153 BYOD 11	【E】 EAP 38 eduroam 49 ElGamal 暗号 20 e-Tax 54 EU データ保護指令 163 executive policy 150 Extensible Authentication Protocol 38 e-文書法 157	【I】 IdP 49 IDS 66 IEC 164 IEEE 165 IEEE802.1X 認証 38 IETF 165 IMAP 79 information asset 3 Information Security Management System 152 Institute of Electrical and Electronic Engineers 165 International Electrotechnical Commission 164 International Organization for Standardization 164 International Telecommunication Union 164 Internet Engineering Task Force 165 Intrusion Detection System 66 Intrusion Protection System 66
【C】 CA 25 C&C 14 Certification Authority 25 Check 152 CIFS 121 CMS 95 Code Red 7 Command and Control server 14 Common Internet File System 121 Contents Management System 95 Cross Site Request Forgery 92 Cross Site Scripting 90 CSRF 92	【F】 FCoE 122 Fiber Channel 122 Fiber Channel over Ethernet 122 fire wall 61	

IPS	66	MTA	78	POP	79
iSCSI	122	MUA	43, 78	PPAP	81
ISMS	152	MultiProtocol Label Switching	71	Pre-Shared Key	74
ISMS 審査機関	152			Pretty Good Privacy	80
ISMS 適合性評価制度	153			private key	19
ISMS 認証	153	[N]		privilege separated	131
ISO	164	NAS	121	procedure	151
ISO/IEC 27000	1	Network Attached Storage	121	Protocol Analyzer	135
ISO/IEC 27001	152			PSK	74
ITU	164	Network File System	121	public key	19
		NFS	121	Public Key Infrastructure	24
[J]		NIST	27		
Japanese Industrial Standards				[R]	
Committee	166	[O]		RA	25
Japanese Public Key		OASIS	165	RADIUS	38
Infrastructure	30	OAuth	52	RAID	122
Japanese Standards		OECD	162	RAID0	123
Association	166	One Time Password	44	RAID0+1	125
JIS	166	OPEN ID	49	RAID1	124
JISC	166	OpenID Connect	53	RAID1+0	125
JIS Q 15001	153	Organization for Economic		RAID10	126
JIS Q 27001	152	Co-operation and		RAID4	128
JPKI	30	Development	162	RAID5	128
JSA	166	Organization for the		RAID6	129
JSON	52	Advancement of Structured		ransom	13
		Information Standards	165	ransomware	13
[K]		OS command injection	94	RC4	17
key distribution center	18	OS コマンドインジェク		RC5	17
Key Reinstallation AttaCKs	74	ション	94	recovery	110
KRACK	74	OTP	44	Redundant Array of	
				Independent Disks	122
[L]		[P]		Redundant Array of	
LDAP	38	Packet Capture	135	Inexpensive Disks	123
Lightweight Directory Access		Padding Oracle On		Registration Authority	25
Protocol	38	Downgraded Legacy		Remote Authentication Dial	
		Encryption	72	In User Service	38
[M]		parity	128	restore	110
MAC	75	PDCA モデル	151	RFC6749	52
MAC 認証	75	peril	5	RFC6750	52
Mail Transfer Agent	78	PGP	80	Rivest Cipher or Ron's	
malware	12	phishing	155	Code 4	17
man in the middle attack	23	PIN コード	33	RSA 暗号	20
Media Access Control	75	PKI	24	RSA 暗号方式	28
Message User Agent	43, 78	Plan	152		
mirroring	124	policy standard	151	[S]	
MPLS	71	POODLE	72	SAE handshake	75

SAML	49	striping	123	Web API	51
SAN	122			Web Application Firewall	67
scareware	13	[T]		Web Authorization Protocol	
SCP	72	tamper resistance	142		52
SCSI	122	Temporal Key Integrity Protocol	74	Web Hypertext Application Technology Working Group	165
SCSI over IP	122	threat	5	Web アプリケーション	86
Secure CP	72	TKIP	74	WEP	73
Secure Shell	72	TLS	72	WHATWG	165
Secure Sockets Layer	71	Transport Layer Security	72	Wi-Fi Alliance	166
SE Linux	132	Trojan horse	12	Wi-Fi Protected Access	74
SHA-1	27	Trusted OS	132	Windy	144
SHA-1 broken	27			Wired Equivalent Privacy	73
SHA-2	27	[U]		World Wide Web	86
shadow ファイル	40	UBE	82	World Wide Web Consortium	165
Shibboleth	39	UCE	83	worm	12
Simple Mail Transfer Protocol	79	UDID	143	WPA	74
		Unique Device Identifier	143	WPA3	75
Single Sign On	47	Unsolicited Bulk Email	83	WWW	86
S/Key 方式	45	Unsolicited Commercial Email	83	WWW クライアント	86
Small Computer System Interface	122			WWW ブラウザ	86
SMTP	79	[V]			
SP	49	Virtual Private Network	70	[X]	
SPAM	83	virus	12	XML	52
spyware	13	VPN	70	XSS	90
SQL	93	vulnerability	4		
SQL インジェクション	93			[Z]	
SSH	72	[w]		ZIP ファイルフォーマット	81
SSL	71	W3C	165		
SSO	47	WAF	67		
storage	120	WannaCry	14		
Storage Area Network	122				

— 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 © Masahiro Matsuda 2024

2024年4月30日 初版第1刷発行



検印省略

著者 まつ だ まき ひろ 敬
松 田 勝 敬
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)



【JCOPY】 < 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@jcopy.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。