

第1部 サイバー犯罪理解のための 基礎知識

第1章 インターネット時代の新しい道具たち

I スマートフォン	2
1 はじめに	2
2 スマートフォンとは	3
3 スマートフォンの商標登録	4
4 代表的なスマートフォン	6
5 スマートフォンの機能	6
〔コラム〕 スマートフォン誕生の足どり／8	
6 わが国におけるスマートフォンの現況	10
(1) 概況	10
(2) 日本で発売されているスマートフォン	11
(3) スマートフォンのセキュリティ	12
(4) Apple社に対抗する包囲網	12
〔コラム〕 オバマ大統領のスティーブ・ジョブズ氏への弔辞／13	
〔コラム〕 携帯電話を悪用した京都大学入試カンニング事件／13	
II 電子マネー	14
1 はじめに	14
2 電子マネーとは	15

3	電子マネーの方式	16
4	電子マネーの種類・特徴	16
	〈表1〉 電子マネーの種類・特徴／16	
5	電子マネー端末	19
6	電子マネーに関する不正行為と規制法	19
7	電子マネーに関する統計	20
	〈表2〉 電子マネーの市場規模／21	
	〈表3〉 電子マネーの市場規模予測／21	
8	電子マネーと地域通貨	22
III	電子書籍	23
1	電子書籍とは	23
2	電子ブックリーダー	24
3	出版業界、通信業界、電機メーカー、電子書籍ストアの動き	25
4	電子書籍をめぐる問題	28
	(1) 著作権の侵害	28
	(2) 情報の格差	28
	(3) 収益の配分	29
	(4) 電子化の権利	29
	(5) 電子書籍端末	29
	(6) 米アマゾン社の対日進出	29
5	わが国の出版関連業界の市場規模等	29
6	電子書籍作成代行業者の誕生	30
IV	IC (Integrated Circuit)	31
1	ICとは	31
2	ICチップの動力源	31
3	ICカードと電子マネー	32
4	IC読み取り端末	32

目次

5 ICチップのセキュリティ	33
〈表4〉 ICカードとMTカードのセキュリティ比較	33
6 無線通信技術の国際規格	34
7 非接触型ICカードの技術方式	35
(1) NFC	35
(2) Felica	36
(3) MIFARE	37
〔コラム〕 Google Walletとおサイフケータイ	38

第2章 インターネット上の取引と決済

I 電子商取引の決済	39
1 電子商取引（インターネット・ショッピング、インターネット・オークション）	39
2 インターネット・ショッピング、オークションの決済方法	40
3 インターネット・バンキング	41
(1) インターネット・バンキングとは	41
(2) メガバンク3行の新サービス	42
(3) インターネット・バンキングをめぐる法規制	42
(4) インターネット・バンキングのセキュリティ対策	43
(5) インターネット・バンキング不正利用の手口	45
(6) インターネット・バンキング不正利用による被害	45
(7) 電子貿易決済にかかわる国際基準づくり	46
(8) 新規参入のインターネット銀行	46
4 電子ウォレット	49
5 フェイスブックの活用	50
6 インターネット決済代行業者の誕生	50
7 ペイジー（Pay-easy）	51

<表5> ペイジーのシステム利用件数および利用金額／51	
8 スマートフォン決済の安全基準等に関する基本的な考え方	52
II PCIDSS	52
1 はじめに	52
2 PCIDSS とは	54
3 PCIDSS の弱点	56
4 PCIDSS の管理団体、準拠認証機関等	56
III 電子決済代行業者	57
1 決済代行業者とは	57
2 インターネットに関連した決済代行業者の動き	57
3 決済代行業者の不正行為	58
(1) 具体例	58
(2) 対抗策	59
4 決済代行業者に対する消費者庁の動き	59

第3章 インターネット上の不正行為

I コンピュータ・ウイルス	61
1 コンピュータ・ウイルスとは	61
2 コンピュータ・ウイルスに関する法律	63
3 コンピュータ・ウイルスに関する基礎知識と名称	63
(1) コンピュータ・ウイルスの歴史	63
(2) コンピュータ・ウイルス作成者の逮捕事例	64
(3) その他の知識	65
<表6> コンピュータ・ウイルスを悪用する不正行為者の名称／65	
<表7> コンピュータ・ウイルスや社会問題となったソフト／66	
II サイバー攻撃、ソニーのデータ流出事件、ウイキリークス	76
1 サイバー攻撃	77

目次

(1) 概要	77
(2) サイバー攻撃者の動機と犯人像	77
(3) サイバー攻撃の方法	78
(4) サイバー攻撃の目標	79
(5) サイバー攻撃の発信元	79
(6) サイバー攻撃への対策	79
(ア) 米国の対策	80
(イ) 日本の対策	80
(ウ) 個人の対策	82
(7) ロンドン・サイバー国際会議	82
(8) サイバー攻撃による被害額	83
2 ソニーのデータ流出事件	83
3 ウイキリークス	83
(1) 概要	83
(2) ウイキリークスが引き起こした問題	84
〔コラム〕 サイバー攻撃とアノニマス	85
4 サイバー攻撃、ソニーのデータ流出事件とウイキリークスの関連性	85
5 浮き彫りになった日本の問題点	86
III インターネットを利用した悪徳商法	88
1 はじめに	88
2 悪徳商法の手口と対策	88
(1) インターネット通信販売	88
(2) インターネット・オークション（チャリンカー詐欺）	89
(3) オンラインショッピング	89
(4) オンライン SOHO	90
(5) アフィリエイト広告、ドロップ SHIPPING	90

(6) ID・パスワードの窃取	90
(7) インターネットを通じた個人間の売買	91
(8) 悪質な出会い系サイト	91
(9) ねずみ講メール	92
(10) インターネット・バンキング	92
(11) 児童買春、児童ポルノ	93
(12) 振り込め詐欺	93
(13) やらせ請負業（ステルス・マーケティング）	93
(14) ソーシャル・ネットワーク（SNS）を悪用したフィッシング	93
〔コラム〕 インターネット関連事業のニューフェイス	93

第2部 サイバー犯罪の実情と対策

第1章 サイバー犯罪の種類と手口

I サイバー犯罪の定義	98
1 不正アクセス犯罪	99
2 コンピュータ・電磁的記録対象犯罪	100
3 コンピュータネットワーク利用犯罪	101
II サイバー犯罪の特徴	102
III サイバー犯罪の事例	102
1 不正アクセス禁止法違反	103
2 コンピュータ・電磁的記録対象犯罪	105
(1) 電子計算機損壊等業務妨害	105

目次

(2) 電磁的記録不正作出・供用	106
(3) 不当指令電磁的記録作成・提供等	106
3 コンピュータ・ネットワーク利用犯罪	107
(1) 窃盗	107
(2) 詐欺	107
(ア) 主な事例	107
(イ) 新しい詐欺の手口	108
(3) 著作権法違反	110
(4) 犯罪収益移転防止法違反	110
(5) 電気通信事業法違反	111
(6) 国際的な協力の下に規制薬物に係る不正行為を助長する行為等の防止を図るための麻薬及び向精神薬取締法等の特例等に関する法律違反	112
(7) 器物損壊	112
(8) 出会い系サイト規制法違反	112
(9) 児童ポルノ法違反	113
IV サイバー犯罪に用いられる手口	113
1 攻撃型の不正行為	113
2 ID・パスワードの窃取の手口	114
3 詐欺行為	116
4 電子マネー関連	116
5 その他	116
V サイバー犯罪による情報漏えいの実情	117
<表8> 情報漏えい件数の推移	118
VI サイバー犯罪関連の統計	118
<表9> サイバー犯罪の検挙件数の内訳	119
<表10> サイバー犯罪の罪名別割合	120

〈表11〉 サイバー犯罪等に関する相談件数の推移／120
〈表12〉 PIO-NET、インターネット通販相談件数／120
〈表13〉 ネットバンキング犯罪状況／121
〈表14〉 コンピュータウイルス被害届出件数／121
〈表15〉 インターネット・バンキングによる預金等不正払戻し被害発生状況／121
〈表16〉 偽造キャッシュカード等による被害発生等の状況／122
〈表17〉 偽造キャッシュカード等による平均被害額／122
〈表18〉 出会い系サイト被害児童数／122
〈表19〉 インターネット利用人口普及率／122

第2章 サイバー犯罪対策をめぐる関係機関の 取組み

I 第二東京弁護士会消費者問題対策委員会にみる法律実務家の 考え方	123
1 インターネットを利用したオークション・買物のトラブル	124
2 インターネット上の名誉毀損等	124
3 インターネット上の悪徳商法、広告等	124
4 身に覚えのない請求	125
5 その他	125
II 電子商取引及び情報財取引等に関する準則（経済産業省） にみる考え方	125
1 電子商取引	126
(1) オンライン契約の申込みと承諾	126
(ア) 契約の成立時期／126	
(イ) 消費者の操作ミスによる錯誤／126	
(ウ) インターネット通信販売におけるわかりやすい申込画面の設定義務／127	
(エ) ワンクリック請求と契約の履行義務／127	

目次

(2) オンライン契約の内容	128
(ア) ウェブサイトの利用規約の契約への組入れと有効性	128
(イ) 価格誤表示と表意者の法的責任	128
(ウ) 管轄合意条項の有効性	129
(エ) 仲裁合意条項の有効性	129
(3) なりすまし	130
(ア) 「なりすまし」による意思表示のなりすまされた本人への効果帰属	130
(イ) 「なりすまし」が生じた場合の認証期間の責任	130
(4) 未成年者による意思表示	130
(5) 電子商店街（ネットショッピングモール）運営者の責任	131
(6) インターネット・オークション	131
(ア) オークション事業者の利用者に対する責任	133
(イ) オークション利用者（出品者・落札者）間の法的責任	133
(ウ) インターネット・オークションにおける売買契約の成立時期	133
(エ) 「ノークレーム・ノーリターン」特約の効力	133
(オ) インターネット・オークションと特定商取引法	134
(カ) インターネット・オークションと景品表示法	134
(キ) インターネット・オークションと電子消費者契約法	134
(ク) インターネット・オークションと古物営業法	134
(7) インターネット上で行われる懸賞企画の取扱い	135
2 インターネット上の情報の掲示・利用等	135
(1) CGM サービス提供事業者の違法情報媒介責任	135
(2) 他人のホームページにリンクを張る場合の法律上の問題点	136
(3) P2P ファイル共有ソフトウェアの提供	136
(4) ウェブ上の広告	136
(ア) 景品表示法による規制	136
(イ) 特定商取引法による規制	137

(ウ) 薬事法・健康増進法による規制／137	
(ク) 貸金業法による規制／138	
(5) ドメイン名の不正取得等	138
(6) インターネット上への商品情報の掲示と商標権侵害	139
(7) ID・パスワード等のインターネット上での提供	139
(8) インターネットを通じた個人情報の取得	139
(9) 肖像の写り込み	140
(10) インターネットと著作権	140
(ア) インターネット上の著作物の利用／140	
(イ) サムネイル画像と著作権／140	
(ウ) 著作物の写り込み／141	
(ク) e-ラーニングにおける他人の著作物の利用／141	
3 情報財の取引等	142
(1) ライセンス契約の成立とユーザーの返品可否	142
(ア) 情報財が媒介を介して提供される場合／142	
(イ) 情報財がオンラインで提供される場合／143	
(ウ) 重要事項不提供の効果／143	
(2) ライセンス契約中の不等条項	144
(3) ライセンス契約の終了	144
(ア) 契約終了時におけるユーザーが負う義務の内容／144	
(イ) 契約終了時の担保措置の効力／144	
(4) ベンダーが負うプログラムの担保責任	145
(5) SaaS・ASPのためのSLA	145
(6) ソフトウェアの使用許諾が及ぶ人的範囲	145
(7) ユーザーの知的財産権譲受人への対抗	146
(8) ソフトウェア特許権の行使と権利濫用	146
(9) 使用機能、使用期間等が制限されたソフトウェアの制限解除	

目次

方法を提供した場合の責任	146
(10) データベースから取り出された情報・データの取扱い	147
4 国境を越えた取引等	147
(1) 国際裁判管轄と準拠法	147
(2) 2011年改正民事訴訟法による国際裁判管轄	148
(3) 準拠法とウィーン売買条約	149
(4) 準拠法の取決めがないとき	150
(5) インターネット上の取引における消費者契約と準拠法	150
(6) インターネット上の名誉・信用の毀損と準拠法	150
III インターネット消費者取引研究会（消費者庁）にみる考え方	150
1 決済代行業者とクレジットカード決済	151
2 連鎖販売	151
3 ドロップシッピング内職	152
4 インターネット上の情報商材の販売	152
5 インターネット・オークションサイトへの連絡不能	152
6 インターネット上のフリーマーケット	152
7 オンラインゲーム	152
8 出会い系サイト、アダルトサイト	153
9 インターネット・ショッピングサイト	153
10 継続的サービスの自動更新	153
IV PIO-NET（国民生活センター）にみる考え方	154
1 インターネット・ショッピング	154
(1) 契約の成立時期	154
(2) 錯誤による申込みの無効	154
(3) 表示義務	155
(4) 詐欺の疑い	155
2 インターネット・オークション	156

(1) 不実告知もしくは詐欺	156
(2) 落札者のキャンセル	156
(3) オークション外取引	156
(4) ペニーオークション	157
3 出会い系サイト	158
(1) 有料サイトへの誘導	158
(2) 無料サイト利用停止中のサーバー利用料金	158
(3) 詐欺の疑い	158
4 迷惑メール	158
5 オンラインゲーム	159
(1) 禁止事項への抵触	159
(2) アイテムの未到着	159
(3) 個人情報の流失	159
6 その他	160
(1) ワンクリック詐欺	160
(2) 宅配ビデオレンタルサービス	160
(3) アフィリエイト、ドロップシッピング	161
(4) メール交換サイト	162
(5) アダルトサイトの料金請求	162

第3章 ネットセキュリティによるサイバー犯罪 対策

I ネットセキュリティとは	164
II ネットセキュリティの2つの局面	165
1 技術的手段——コンピュータアクセス制御	165
2 暗号 (AES・DES・SSL)	167
(1) 暗号の定義	167

目次

(2) 暗号の種類と作成方法	168
<表20> サイファ通信の表記法	169
(3) 暗号の解読法	169
〔コラム〕 いまだに解読できない暗号文	170
〔コラム〕 暗号作成に使用された道具	171
(4) 暗号を理解するために最小限知っておきたい言葉	171
(5) 暗号方式	172
<表21> 暗号にかかわる技術・システムの用語等	172
III 不正ウイルス対策ワクチン (Anti Virus Vaccine)	175
IV フィルタリングとブロッキング	176
1 サイトとは	176
(1) 定義と種類	176
(2) サイトの閲覧手順	177
(3) 有害サイト	177
2 フィルタリングとは	177
3 ブロッキングとは	178
(1) 概要	178
(2) 仕組み・手法	179
(ア) DNS ブロッキングによるアクセス遮断	179
(イ) パケットドロップによるアクセス遮断	179
(ウ) URL フィルタリングによるアクセス遮断	179
(エ) ハイブリッドフィルタリングによるアクセス遮断	180
4 フィルタリングとブロッキングの相違	180
V セキュリティに関する政府・各省庁、警察庁の動き	181
VI セキュリティ関連団体等	184
VII 相談窓口・機関	189
VIII 一般消費者による具体的な対処法	190

1 パソコンの不正操作、覗き見を防ぐには	190
2 クラッカーに攻撃された場合	191
3 フィッシング詐欺対策	191
4 SNS を利用したネットゲームのトラブルを避けるには.....	192
5 その他、日頃から気をつけておくべきこと	192
参考資料1 インターネット関連用語の基礎知識	194
参考資料2 インターネット関連法と裁判例	219
【著者紹介】	267