
アクティブラーニングで学ぶ 情報リテラシー

宇田 隆哉 共著
井上 亮文



コロナ社

アクティブラーニングで学ぶ
情報リテラシー

宇田 隆哉 共著
井上 亮文

コロナ社

ま え が き

本書は、「情報リテラシー」というタイトルのもと、情報通信技術の原理的な側面と、それらがどのように現在およびこれからの社会に役立てられていくかをまとめたものである。

本書は、コンピュータやソフトウェアに関する最低限の利用方法を修得している学生を想定している。多くの場合、情報リテラシーといえば、コンピュータやソフトウェアの使い方、マナーの学習を指すことが多い。しかし、情報通信技術は猛烈な勢いで進化した、変化していく。昨日まで使っていたウェブサービスの画面や機能が翌日には一変していることが日常茶飯事な中では、そのような知識はすぐに陳腐化してしまう。

その一方、技術の基本原理は変わりにくい。たとえ変わったとしても、過去の知識を理解していれば、それをもとにして新しい仕組みを理解することに役立つ。また、情報通信技術はすでに社会に深く溶け込み、あつて当たり前の生活基盤である。現在の情報通信技術が社会に果たす役割を見ることは、未来の情報通信技術が支える社会を想像し、それに備えることにつながるであろう。

第I部では、情報通信技術の基本原理について扱う。インターネットの仕組みや動作原理だけでなく、セキュリティの基本原理にも触れることで安全に対する意識を啓発する。

第II部では、人や社会の側から見た情報通信技術のあり方について扱う。われわれの身近にあるサービスの原理や情報機器の仕組みを理解することで、情報技術が不可分となる社会で生きるための基礎的な素養を養う。

本書は、アクティブラーニング型の学習が行える書き方になっている。一般的な教科書では、一方的に解説をしてそれで終わりである。確かに、紙面を最大限有効に活用してなにかを解説するには、その解説に紙面のすべてを割り当

てることが最も適切である。しかし、概してこのような構成では、場合によっては読者は理解した気になっているだけか、読破による満足感に包まれているだけで学習が終了してしまう。本書では、読者が技術的な仕組みを理解して説明できることを目指している。別の言い方をすれば、技術的な仕組みを正確に理解していない読者に、理解していないことを気付かせ、それを理解せずにつきに進んではいけないことを認識させるようにするということであり、それがアクティブラーニングという形になっている。本書を読む際には、文字や図表を目で追うだけでなく、必ず手を動かし頭脳を働かせて、アクティブラーニングの問題に取り組んでほしい。本書のアクティブラーニングの問題は、暗記では答えられないものになっているし、数秒の思考で即答できるものでもない。アクティブラーニングの問題に答えられないときには、もう一度本書の説明を読み直してほしい。直前の説明を読んだだけでわからない場合には、さらにその前の説明に戻る必要がある。一部の問題に正解はなく、インターネット検索の結果も駆使して自分の考えをもつ必要がある。このようにして理解した内容は、実際に役立つ知識の一つとなり、さらに複雑な情報技術を学ぶ際の一助になるであろう。

最後に、本書を執筆するにあたってご支援とご助力を頂いたコロナ社の関係各位に深く感謝する。

2016年8月

宇田隆哉，井上亮文

目 次

第I部 情報通信技術の動作原理

1 インターネット

1.1 IP アドレス	1
1.2 NAT	3
1.3 DHCP	9
1.4 DNS の偽装	12
1.5 ハブ	15
1.6 OSI 参照モデル	20
理解度チェック	22

2 SSL (TLS)

2.1 前提知識	24
2.2 共通鍵暗号	26
2.3 公開鍵暗号	27
2.4 鍵交換	29
2.5 ハッシュ関数	31
2.6 デジタル署名	32
2.7 公開鍵証明書	34
2.8 SSL の仕組み	36

理解度チェック	39
---------	----

3 無 線 LAN

3.1 Wi-Fi	40
3.2 周波数による特性	42
3.3 Wi-Fi の 規 格	44
3.4 Wi-Fi のセキュリティ	47
理解度チェック	51

4 携帯電話と電子メール

4.1 携帯電話の通信方式	52
4.2 携帯電話に関する用語	55
4.2.1 プラチナバンド	55
4.2.2 SIM ロ ッ ク	55
4.2.3 ロ ー ミ ン グ	56
4.2.4 プリペイドSIM	56
4.2.5 NFC	56
4.2.6 WiMAX	57
4.2.7 LTE	57
4.3 電 子 メール	58
4.4 通信経路を暗号化する電子メール技術	60
4.5 暗号化と署名が行える電子メール技術	61
4.6 Web メール	62
理解度チェック	64

5 DNS

5.1 DNSの仕組み	65
5.2 正引きと逆引き	68
5.3 キャッシュと有効期限	71
5.4 ダイナミックDNS	73
理解度チェック	76

6 IP アドレス

6.1 IPアドレスの計算	77
6.2 セグメント	80
6.3 サブネットマスク	82
6.4 ブロードキャストアドレスとネットワークアドレス	87
理解度チェック	89

7 パケット通信

7.1 パケットの仕組み	90
7.2 MTU	92
7.3 MSS	93
7.4 TTL	95
7.5 パケット分割	96
理解度チェック	98

第II部 社会から見た情報通信技術

8 人と情報の接点としてのディスプレイ

8.1 液晶ディスプレイ	99
8.2 3D ディスプレイ	101
8.2.1 立体視の原理	101
8.2.2 フレームシーケンシャル方式	102
8.2.3 視差バリア方式	104
8.3 タッチスクリーン	105
8.3.1 抵抗膜方式	106
8.3.2 静電容量方式	107
理解度チェック	109

9 モノの認識技術

9.1 ユビキタスからモノのインターネットへ	110
9.2 バーコード	111
9.2.1 1次元コード	112
9.2.2 2次元コード	114
9.3 RFID	117
9.3.1 動作原理	117
9.3.2 バーコードとの比較	118
9.3.3 バーコードの代わりとしての利用	119
9.3.4 非接触型 IC カード	121
理解度チェック	122

10 仮想現実感

10.1 Virtual とは	123
10.2 仮想現実感に必要なもの	125
10.3 現実感はどこにあるか	126
10.4 仮想現実感を支えるインタフェース	127
10.4.1 視覚による没入感	127
10.4.2 聴覚による没入感	130
10.4.3 触覚による没入感	131
10.4.4 味覚による没入感	132
10.4.5 嗅覚による没入感	133
10.4.6 姿勢計測	134
10.5 クロスモーダル知覚	135
10.6 仮想現実感の応用	135
理解度チェック	137

11 拡張現実感

11.1 拡張現実感とは	138
11.2 拡張現実感に必要なもの	140
11.3 「窓」となるデバイス	140
11.3.1 光学透過型 HMD	141
11.3.2 ビデオ透過型 HMD	142
11.3.3 網膜走査型 HMD	143
11.4 現実世界の「認識技術」	144
11.5 拡張・増強される「価値」	146
理解度チェック	147

12 交通の情報化

12.1 ナビゲーションシステム	148
12.1.1 カーナビゲーションシステム	148
12.1.2 歩行者ナビゲーション	150
12.2 位置情報システム	150
12.2.1 GPS	151
12.2.2 無線 LAN	152
12.2.3 RFID	154
12.3 経路案内	155
12.3.1 ネットワークとグラフ	155
12.3.2 隣接行列	156
12.4 自動運転技術	158
12.4.1 車線逸脱の防止	158
12.4.2 衝突被害軽減（自動ブレーキ）システム	160
12.4.3 ディープラーニングによる画像認識	161
理解度チェック	162

13 コンピュータを介したコミュニケーション

13.1 ノンバーバルコミュニケーションとアウェアネス	163
13.2 電子メール	164
13.3 電子掲示板	165
13.4 チャット	166
13.5 プログラム	168
13.6 ソーシャルネットワーキングサービス	169

13.7 オンラインストレージサービス	171
13.8 目的に応じた使い分け	172
理解度チェック	175
引用・参考文献	176
索引	177

目次社

1

インターネット

本章では、インターネットにおいて人間が情報をやりとりする際の仕組みについて説明する。インターネットでは、インターネットプロトコル (Internet Protocol : IP) という通信の規約に従って、コンピュータ機器どうしが通信を行っている。IP は、国によってはバージョン 6 (IP version 6 : IPv6) が使用されているが、2016 年現在、日本国内では一般的にバージョン 4 (IPv4) が使用されている。

1.1 IP アドレス

インターネットに接続されているコンピュータ機器には、その機器のネットワーク上の位置を特定するためのアドレス (番地) が割り振られている。これを IP アドレスという。日本国内で一般的に使用されている IPv4 では、IP アドレスは 32 ビットのビット列で表現される。1 ビットは 0 か 1 の値をもっており、これが 32 個並んで一つの IP アドレスを表現しているのである。その値は、00000000000000000000000000000000 から 11111111111111111111111111111111 までの 2^{32} 通り、つまり 4 294 967 296 通り (約 43 億通り) である。

しかしながら、人間が眺めたとき、0 と 1 のみで構成されるビット列の表現は非常に読みにくく、一瞥して記憶することは困難である。そこで、インターネットの世界では、32 ビットの値を 8 ビットずつ四つのグループに区切り、それぞれの 8 ビットの値を 10 進数にしてピリオドで区切って表現する習慣がある。例えば、11000000101010000000101000000001 であれば、この 32 ビットを「11000000」「10101000」「00001010」「00000001」という四つのグループに分割し、それぞれを 2 進数から 10 進数に変換すると「192」「168」「10」「1」と

2 1. インターネット

なるため、この IP アドレスを「192.168.10.1」と表現するのである。なお、この変換方法については 6 章で詳述する。

IP アドレスのすべてがインターネットに接続されている機器に割り振られているわけではない。IP アドレスの中には、インターネット上に存在しないプライベート IP アドレスというものがある。プライベート IP アドレスの範囲を図 1.1 に示す。

クラス A	10.	0.0.0 ~	10.255.255.255
クラス B	172.	16.0.0 ~	172.31.255.255
クラス C	192.168.	0.0 ~	192.168.255.255

図 1.1 プライベート IP アドレス

プライベート IP アドレスには、クラスに応じて三つの範囲がある。クラスがなにを意味しているのかについては 6 章で詳述する。ここでは、この範囲の IP アドレスがプライベート IP アドレスであることを知ってもらいたい。

自宅で、インターネットに常時接続できる環境をもっている読者もいるであろう。自宅のネットワークとインターネットを接続するために、ブロードバンドルータというものを使用していると思う。ブロードバンドルータの IP アドレスは、購入時に 192.168.1.1 に設定されていることが多い。これは図のクラス C に書かれている範囲に含まれているプライベート IP アドレスである。

このように、プライベート IP アドレスは、家庭や職場のコンピュータ機器に自由に割り当ててよい。家庭のコンピュータにプライベート IP アドレスを割り当てると、それはあたかもインターネット上に存在する IP アドレスをもった機器のように感じられるが、じつはそうではない。ただし、プライベート IP アドレスも IP アドレスであることに違いはないため、IP を使用して通信することは可能である。つまり、その機器からインターネット上に存在する機器に対しては、IP を使用して情報を送信することができるが、その機器はインターネット上に存在しない IP アドレスを使用しているため、その機器宛ての情報をインターネット上の機器が送信することはできないのである。しかし、自宅のコンピュータがインターネット上の機器と通信していると反論する読者がい

るかもしれない。この仕組みについては次節にて解説する。

IP アドレスのうち、プライベート IP アドレスでないものをグローバル IP アドレスという。つまり、0.0.0.0～255.255.255.255 の中で、図 1.1 の範囲のアドレスを除いたものがグローバル IP アドレスである。グローバル IP アドレスが割り当てられた機器はインターネット上に存在し、その機器宛ての情報を受け取ることができる。

1.2 NAPT

プライベート IP アドレスが割り当てられた機器はインターネット上に存在しないことを前節で述べた。IP では、情報はパケット（小包という意味）という状態で送受信される。IP アドレスをもつ機器は IP を使用した通信が行える。しかし、プライベート IP アドレスはインターネット上に存在しないアドレスであるため、プライベート IP アドレスを送信先として IP を使用してパケットを送信しようとしても、インターネット上ではそのアドレスがどこにあるかだれも知らず、どこにも送ることができないのである。

それでは、自宅のブロードバンドルータを通して、プライベート IP アドレスをもつ機器はどうしてインターネットに接続できるのであろうか。ここで **NAT** (Network Address Translation) という技術を紹介する。図 1.2 に NAT を使用してプライベート IP アドレスをもつ機器とグローバル IP アドレスをもつサーバが通信する様子を示す。

ブロードバンドルータは、インターネット側にグローバル IP アドレス、LAN (Local Area Network: 自宅などのネットワーク) 側にプライベート IP アドレスと、1 台で二つの IP アドレスをもっているのが特徴である。まず、192.168.1.5 の機器（ここでは PC）から 1.2.3.4 のサーバにパケットを送る場合について見てみよう。パケットは 192.168.1.5 の PC から 192.168.1.1 のブロードバンドルータに送られる。このとき、IP の仕組みに則ってパケットは送信され、送信元は 192.168.1.5、送信先は 1.2.3.4 になっている。ブロードバンドルータは、

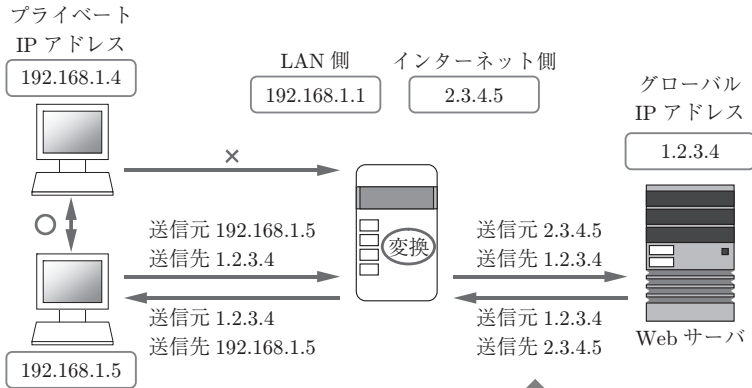


図 1.2 NAT

このパケットをインターネットに送る際、送信元を書き換えて 2.3.4.5 にする[†]。この書き換えられたパケットがサーバに到着すると、サーバは、2.3.4.5 の機器から自分宛にパケットが送られたと認識する。サーバが返信のパケットを送る場合、送信元は 1.2.3.4、送信先は 2.3.4.5 になる。このパケットは 2.3.4.5 の IP アドレスをもつブロードバンドルータに送られる。ブロードバンドルータはこのパケットを受け取ると、送信先を 192.168.1.5 に書き換えて LAN 側のネットワークに送信する。こうすることで、先ほどパケットを送信した PC は、送信元が 1.2.3.4、送信先が 192.168.1.5 のパケットを受信することができ、あたかもグローバル IP アドレスをもつ機器であるかのように、インターネット上の機器と通信が行えるのである。

前節で、IP アドレスは約 43 億通りであることを述べた。これは、最大でも 43 億個のコンピュータどうししか通信が行えないことを意味する。しかし、プライベート IP アドレスと NAT の仕組みを使えば、より多くの機器がインターネット上に存在しているように見せかけられるのである。

ここで、自宅のブロードバンドルータには、インターネット側のほうにもプライベート IP アドレスが割り当てられていると主張する読者もいるかもしれない。それは、インターネットサービスプロバイダ (Internet Service Provider :

[†] 「1.2.3.4」や「2.3.4.5」といった IP アドレスは、便宜上用いたものである。

ISP) のゲートウェイ (出入り口に相当する) にも同じ仕組みがあり, プライベート IP アドレスのネットワークが二重になっているのである。図 1.3 に, ブロードバンドルータにプライベート IP アドレスが割り当てられている場合の NAT の状態を示す。ISP のネットワークは LAN になっており, その LAN 内の機器どうしは通信が行える。このように NAT が何段階になっていても問題なく, インターネット上の機器とプライベート IP アドレスをもつ機器との間で通信は可能である。

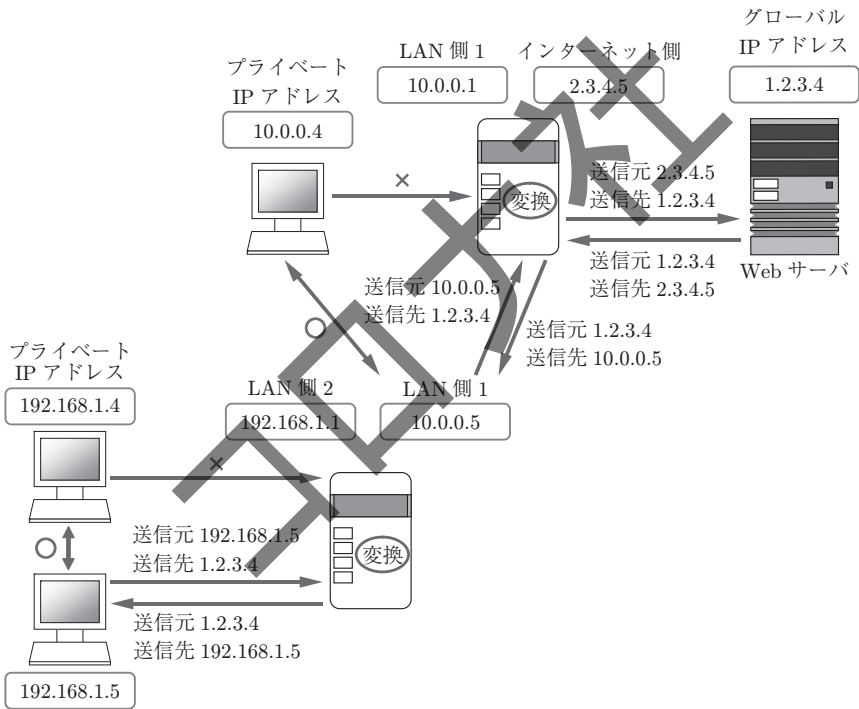


図 1.3 2 段階の NAT

図 1.2 において, 192.168.1.4 の PC がインターネット上の機器と通信できないことに気付いたであろうか。ブロードバンドルータは, インターネットから受信したパケットの送信先 IP アドレスをつねに 192.168.1.5 に変更してしまうため, これでは LAN 内にあるほかの PC はインターネット上の機器と通信で

索引

【あ】		【く】		【ち】	
アウェアネス	164	グラフ	155	チェックディジット	113
アプリケーション層	20	クロスモーダル知覚	135	チャット	166
歩きスマホ	150				
暗号化	25	【け】		【て】	
暗号文	25	検 証	33	抵抗膜方式	106
				デジタルデバインド	106
【い】		【こ】		ディープラーニング	161
インターネットプロトコル	65	公開鍵証明書	34	データリンク層	21
インターネット・		光学透過型 HMD	141	電子掲示板	165
プロトコル・スイート	22	五 感	126		
		コンテンツ管理システム	169	【と】	
【え】		【し】		同期型コミュニケーション	164
液晶ディスプレイ	99	視差バリア方式	104	頭部伝達関数	130
エッジ	156	車線維持支援システム	159	トランスポート層	21
		車線逸脱警報システム	158	トレーサビリティ	119
【お】		車線逸脱防止支援		トレースバック	119
オンラインストレージ		システム	159	トレースフォワード	119
サービス	171	受信信号強度	153		
		衝突被害軽減ブレーキ	160	【に】	
【か】		【す】		認 証	34
換字式暗号	26	スイッチ液晶	104	認証局	34
拡張現実感	138	スキミング	121		
カスケード接続	19			【ね】	
仮想現実感	123	【せ】		ネットワーク	155
カーナビゲーション		静電容量方式	107	ネットワーク層	21
システム	148	正引き	71		
		セッション層	21	【の】	
【き】		【そ】		ノード	156
基本味	132	ソーシャルネット		ノンバーバルコミュニ	
逆引き	71	ワーキングサービス	169	ケーション	163
嗅覚ディスプレイ	133				
共通鍵暗号	26				

【は】		フレームシーケンシャル 方式 102	【も】	
バーコード 111		ブログ 168	網膜走査型 HMD 143	
バーチャルリアリティ 123		【へ】	モノのインターネット 110	
【ひ】		ヘッドマウントディスプレイ プレイ 128	【ゆ】	
ビデオ透過型 HMD 142		ペルティエ素子 131	有向グラフ 156	
非同期型コミュニケーション ション 164		【ほ】	ユビキタス 110	
平文 24		歩行者ナビゲーション システム 148	【り】	
【ふ】		没入感 125	両眼視差 101	
復号 25		【む】	両耳間強度差 130	
輻輳角 101		無向グラフ 156	両耳間時間差 130	
物理層 21			隣接行列 157	
フルサービス・リゾルバ 71				
プレゼンテーション層 21				
◇				
【A】		【I】	POP 59	【Q】
AR 138		IID 130		QR コード 114
【B】		IoT 110		【R】
BBS 165		IP 65		RFID 117
【C】		IP アドレス 1		RSSI 153
CMS 169		ITD 130		【S】
【D】		【J】		SMTP 59
DNS 65		JAN コード 112		SNS 169
【G】		【N】		SNS 疲れ 170
GPS 151		NAPT 6		SSL 24
【H】		NAT 3		【T】
HRTF 130		【O】		TLS 24
		OSI 参照モデル 20		【V】
		【P】		VR 123
		PND 149		

— 著者略歴 —

宇田 隆哉 (うだ りゅうや)

1998年 慶應義塾大学理工学部計測工学
科卒業

2000年 慶應義塾大学大学院理工学研究
科前期博士課程修了(計測工学
専攻)

2002年 慶應義塾大学大学院理工学研究
科後期博士課程修了(開放環境
科学専攻)
博士(工学)

2002年 東京工科大学助手

2003年 東京工科大学講師
現在に至る

井上 亮文 (いのうえ あきふみ)

1999年 慶應義塾大学理工学部計測工学
科卒業

2001年 慶應義塾大学大学院理工学研究
科前期博士課程修了(計測工学
専攻)

2004年 東京工科大学助手

2005年 慶應義塾大学大学院理工学研究
科後期博士課程修了(開放環境
科学専攻)
博士(工学)

2010年 東京工科大学講師
現在に至る

アクティブラーニングで学ぶ 情報リテラシー

Information Literacy—An Active Learning Approach—

© Ryuya Uda, Akifumi Inoue 2016

2016年10月7日 初版第1刷発行



検印省略

著者 宇田 隆 哉

井上 亮 文

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

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 978-4-339-02860-7 (新井) (製本:愛千製本所)

Printed in Japan



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おります。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おりません。

落丁・乱丁本はお取替えいたします