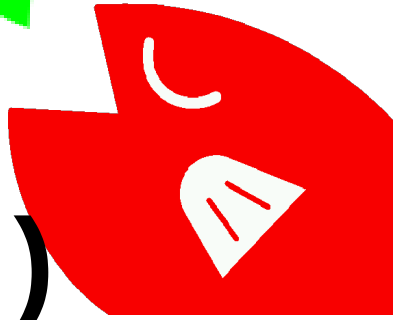
バイナリで遊ぼう

坂井弘亮
(KOZOSプロジェクト)



まずは報告

フィーリングで読む
アセンブラ入門

フィーリングで読むアセンブラ入門とは何か？

.

多種類のアセンブラをフィーリングでパッと読んでみようという
現代の草食な若者向けの
アセンブラ本

当初の予定

.

５種類くらいのアーキテクチャを
見比べながら軽く読んでみる
200ページくらいの薄い本

できあがったもの

.

40種類のアーキテクチャを
見比べながら軽く読んでみる
800ページの薄くない本

アーキテクチャ一覧

Alpha ARC ARM AVR CRIS FR30
FR-V H8/300 PA-RISC x86 i960
IA-64 M32R 68HC11 68000
M・CORE MIPS MIPS64 MMIX
MN10300 PDP-11 PowerPC
PowerPC64 S/390 SH SH64 SPARC
StrongARM V850 VAX x86-64
XScale Xstormy16 Xtensa
Thumb AVR(8bit) H8/300H
68HC11(16bit) MIPS16

熱血！
アセンブラ入門

熱血！アセンブラ入門

坂井弘亮［著］

秀和システム

三省堂の
コンピュータ書籍売場が
たいへんなことに

熱血!
アセンブラ入門
やらなければ、
一生
わからん!!

もうひとつ
報告

アセンブラ短歌

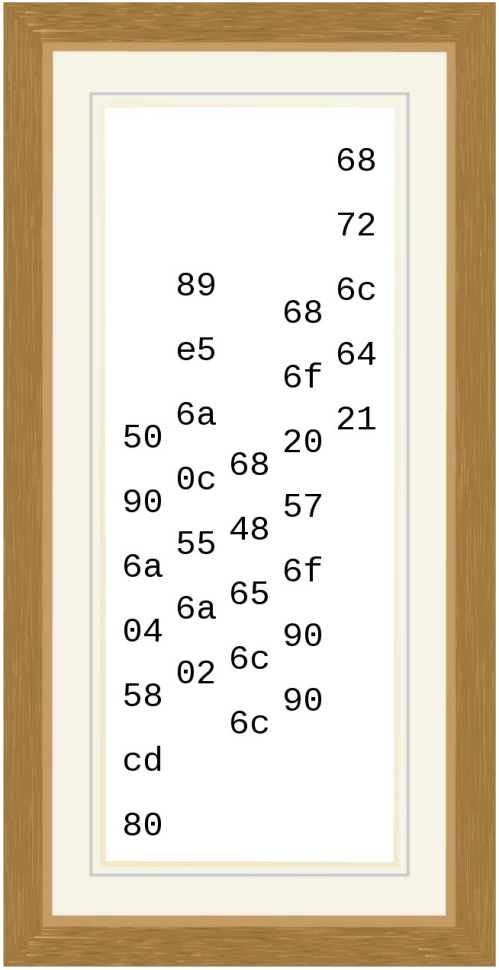
アセンブラ短歌とは

5・7・5・7・7の機械語
コードでプログラムを
書いてみるという
近未来の文化的趣味

こんな感じです

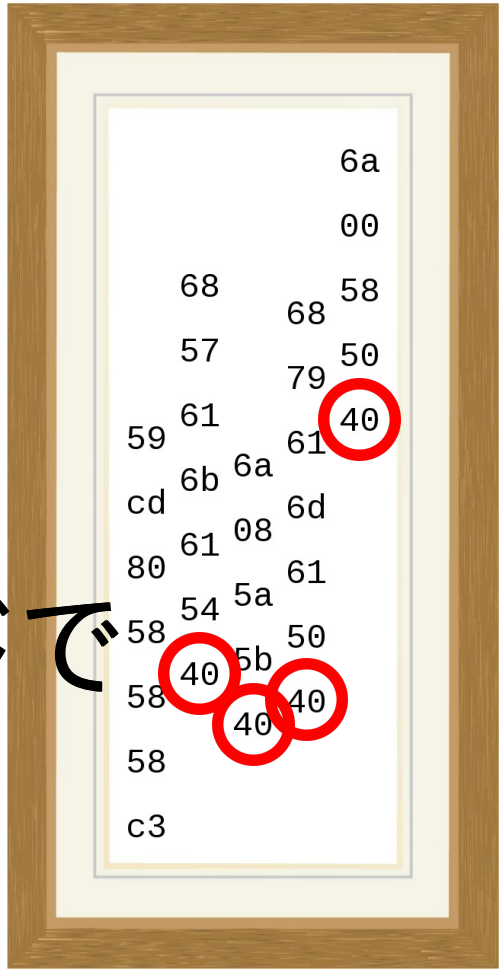
```
68 72 6c 64 21
68 6f 20 57 6f 90 90
68 48 65 6c 6c
89 e5 6a 0c 55 6a 02
50 90 6a 04 58 cd 80
```

札に詠むと
こんな感じ



アセンブラ短歌の作品例

```
6a 00 58 50 40
68 79 61 6d 61 50 40
6a 08 5a 5b 40
68 57 61 6b 61 54 40
59 cd 80 58 58 58 c3
```



機械語コードで
韻をふむ

そんなアセンブラ短歌
ですが

掛軸になったり

【最優秀作品】虹(93 F8)
79 FA B8 00 4C CD 21
B0 07 FD 04 20 AA 4F
D3 EF 83 C7 17
93 F8 B1 04 BF 93 F8
BB 00 A2 8E C3
大坪雄平

本になったり

31バイトでつくる
アセンブラプログラミング
アセンブラ短歌の世界

歌人(Tankists)

坂井 弘亮 (白樺派)
愛甲 健二 (新思潮派)
松田 和樹 (明星派)
坂井 丈泰 (アララギ派)
竹迫 良範 (アララギ派)

Tankable Architectures

x86(Intel) M32C(三菱)
MN10300(松下)
RL78(ルネサス) RX(ルネサス)

さて本題

KOZOSプロジェクトの最近の活動

SECCONにコミットしています

SECCONとは何か

セキュリティ競技のコンテストです

SECCONで行われている競技・コンテストなど

CTF

バイナリかるた

アセンブラかるた

アセンブラ・クロスワード

バイナリカレンダー

なぜ低レイヤー？

セキュリティ分野では
アセンブラ・バイナリ解析の
技術は超重要

本日はこれらの中から
いくつかを紹介します

バイナリかるた

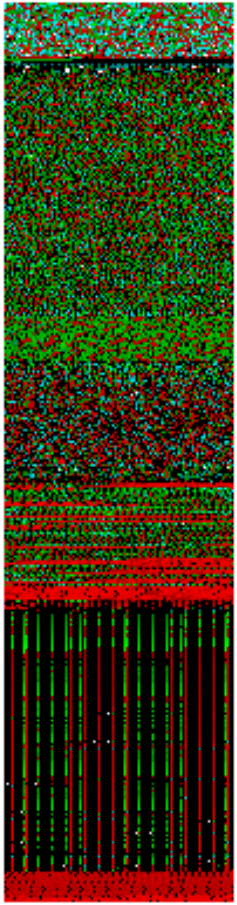
バイナリかるた
とは何か？

ルールは
超簡単

まず，こんなかるた札を
用意して机に並べます

SECCON
TCP
バイナリかるた
SECCON
ZIP
バイナリかるた
SECCON
JPEG
バイナリかるた
SECCON
FAT16
バイナリかるた
SECCON
Linux/x86
実行ファイル
バイナリかるた
SECCON
EXE
バイナリかるた

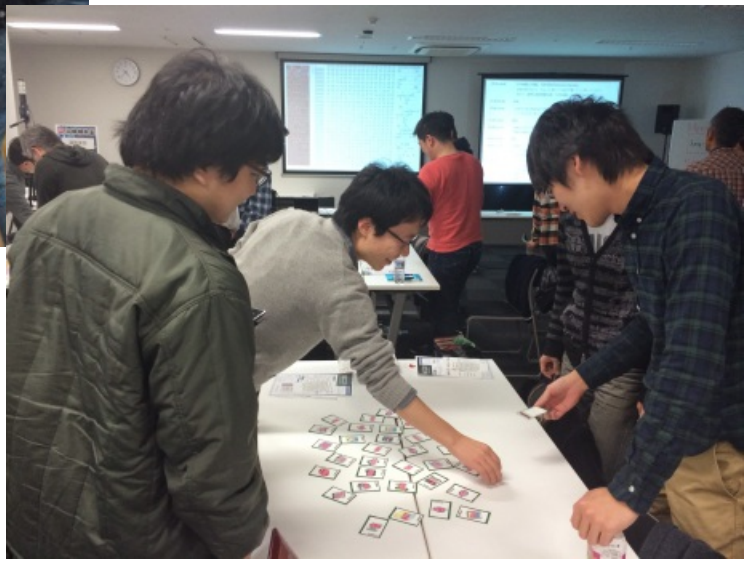
こんなデータを
プロジェクタで映します



```
0000: 7F 45 4C 46  01 01 01 00  00 00 00 00  00 00 00 00  .ELF.... ........
0010: 02 00 AD 00  01 00 00 00  00 14 00 00  34 00 00 00  ........ ....4...
0020: 1C 4A 04 00  00 00 00 00  34 00 20 00  01 00 28 00  .J...... 4. ...(.
0030: 15 00 12 00  01 00 00 00  58 00 00 00  00 14 00 00  ........ X.......
0040: 00 14 00 00  C0 74 00 00  10 B9 00 00  07 00 00 00  .....t.. ........
0050: 08 00 00 00  00 00 00 00  FB 02 10 CD  00 00 05 49  ........ .......I
0060: 5C 00 66 15  75 60 FF 02  66 45 75 60  FF 02 66 55  ¥.f.u`.. fEu`..fU
0070: 75 60 FF 02  66 25 75 60  FF 02 66 35  75 60 FF 02  u`..f%u` ..f5u`..
0080: 7E A7 66 02  EF 17 05 EA  1A 00 FB E2  10 78 00 00  ~.f..... .....x..
0090: EC E1 ED 1E  0F 61 0E 13  7F 1E EF 71  05 AC 5B 00  .....a.. ...q..[.
00A0: EF 14 7F 88  EF 41 02 60  40 66 84 4B  04 FD 2A 43  .....A.` @f.K..*C
00B0: A8 92 05 26  00 00 67 01  FB E2 00 80  00 00 60 40  ...&..g. ......`@
00C0: EC E1 66 84  4B 04 FD 2A  43 A8 92 05  0D 00 00 67  ..f.K..* C......g
00D0: 01 00 00 00  00 00 00 00  6E 6D 72 00  E4 FA EF 29  ........ nmr....)
00E0: EF 37 EB 04  3B 01 EF 1D  05 4A 30 00  EC 11 EB 01  .7..;... .J0.....
00F0: 3D 01 05 8B  40 00 EB 01  3F 01 61 0D  20 0C ED DA  =...@... ?.a. ...
0100: 0E 61 0A 3A  73 05 EF 00  DD 9A 06 EF  AB 76 2B 00  .a.:s... .....v+.
0110: 20 DF BB 61  0B 21 17 ED  9B 19 EF AC  76 3C 00 20   ..a.!.. ....v<.
0120: 76 2B FF DF  DF CA D7 9C  06 E7 9B 19  EF AB 64 8B  v+...... ......d.
0130: DF BB 61 0B  3A 43 04 ED  9B 04 61 0B  3A 3B 04 EF  ..a.:C.. ..a.:;..
0140: AB 75 2B 1A  61 AB 3A 4B  04 FA 06 3A  01 00 EE 0C  .u+.a.:K ...:....
0150: 3A 01 72 0E  9C 04 72 0A  9B 04 66 CB  4B 0B EB 0E  :.r...r. ..f.K...
0160: 32 01 43 AE  EB 0A 33 01  EB 0B 27 01  FA 06 29 01  2.C...3. ..'...).
0170: 00 FA 06 28  01 00 EB 07  35 01 EB 0C  40 01 EB 0C  ...(.... 5...@...
0180: 42 01 EB 0C  41 01 EB 0C  38 01 EF BF  EB 0E 44 01  B...A... 8.....D.
0190: EB 0D 39 01  EE 0D 35 01  58 D7 61 07  3A 88 03 03  ..9...5. X.a.:...
01A0: 75 57 25 3A  81 03 EF DB  62 1B 0F 75  5A 25 3A 88  uW%:.... b..uZ%:.
01B0: 03 58 BA EF  B7 62 1B 61  0A 21 F2 EE  0E 35 01 FF  .X...b.a .!...5..
01C0: 0A E7 61 0A  20 35 EE 0E  28 01 EE 0B  29 01 EE 0C  ..a. 5.. (...)...
01D0: 35 01 4B AB  62 1E E3 FC  E7 FA 01 EB  0B 29 01 EB  5.K.b... .....)..
01E0: 0E 28 01 61  7E 2B 05 38  74 04 62 8F  76 10 01 00  .(.a~+.8 t.b.v...
01F0: 06 8A 0A 38  01 EB 0A 38  01 58 7A 61  0A 3A 23 04  ...8...8 .Xza.:#.
```

スパーン！
みたいな感じです

SECCONでの実施風景



アセンブラかるた

アセンブラかるたとは何か？

ルールは
超簡単

まず，こんなかるた札を
用意して机に並べます

c9
94
90
92
99
53
5e
5c
4c
46
4e
5a
51
56
42
52
45

例えばこんな命令を
読み上げます

NOP

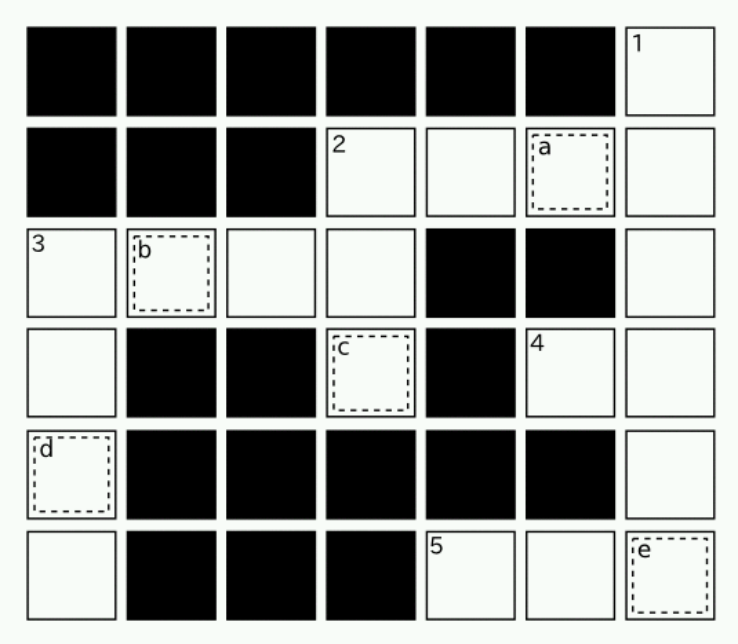
HALT

RET

PUSH EAX

スパーン！
みたいな感じです

アセンブラ・クロスワード



縦のカギ
1: 定番の**EIP**取得
2: EAXを３倍に
3: 引数の指す先を
関数呼び出し

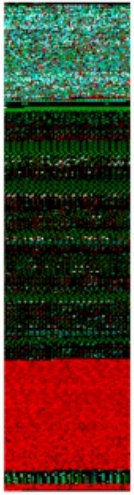
横のカギ
2: ４バイトの**NOP**
3: 第1引数をスタックに積む
4: EAXの指す先を**EAX**に
5: 戻り値に1を設定

解答

						[1] E8
			[2] 8D	74	26	00
[3] FF	74	24	04			00
54			40		[4] 8B	00
24						00
04				[5] 6A	01	58

SECCON会場で配布した記念品

バイナリカレンダー



```
0000: 7F 45 4C 46  01 01 01 09  00 00 00 00  00 00 00 00  .ELF.... ........
0010: 02 00 03 00  01 00 00 00  00 84 04 08  34 00 00 00  ........ ....4...
0020: 64 3E 02 00  00 00 00 00  34 00 20 00  01 00 28 00  d>...... 4. ...(.
0030: 0C 00 09 00  01 00 00 00  00 00 00 00  00 80 04 08  ........ ........
0040: 00 80 04 08  2C 85 00 00  A0 C9 00 00  07 00 00 00  ....,... ........
0050: 00 10 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ........ ........
0060: 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ........ ........
0070: 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ........ ........
... Skipped same lines ...
0400: BC A0 49 05  08 E8 17 01  00 00 50 E8  00 00 00 00  ..I..... ..P.....
0410: B8 01 00 00  00 EB 1C B8  03 00 00 00  EB 15 B8 04  ........ ........
0420: 00 00 00 EB  0E B8 05 00  00 00 EB 07  B8 06 00 00  ........ ........
0430: 00 EB 00 52  51 53 50 8B  54 24 1C 8B  4C 24 18 8B  ...RQSP. T$..L$..
0440: 5C 24 14 8B  44 24 10 52  51 53 50 8B  44 24 10 F8  ¥$..D$.R QSP.D$..
0450: CD 80 73 07  83 F8 00 7E  02 F7 D8 5B  5B 5B 5B 5B  ..s....~ ...[[[[[
0460: 5B 59 5A C3  83 EC 18 FF  74 24 1C E8  A0 FF FF FF  [YZ..... t$......
0470: 83 EC 10 FF  74 24 1C FF  74 24 1C FF  74 24 1C E8  ....t$.. t$..t$..
0480: 93 FF FF FF  83 C4 1C C3  83 EC 10 FF  74 24 1C FF  ........ ....t$..
0490: 74 24 1C FF  74 24 1C E8  82 FF FF FF  83 C4 1C C3  t$..t$.. ........
04A0: 83 EC 10 FF  74 24 1C FF  74 24 1C FF  74 24 1C E8  ....t$.. t$..t$..
04B0: 71 FF FF FF  83 C4 1C C3  83 EC 18 FF  74 24 1C E8  q....... ....t$..
04C0: 68 FF FF FF  83 C4 1C C3  83 EC 10 6A  3C 6A 00 FF  h....... ...j<j..
04D0: 74 24 20 E8  C8 00 00 00  B8 00 00 00  00 83 C4 1C  t$ ..... ........
04E0: C3 8B 44 24  08 C3 A1 04  FC 04 08 8B  54 24 04 01  ..D$.... ....T$..
04F0: C2 89 15 04  FC 04 08 C3  B8 01 00 00  00 C3 83 EC  ........ ........
0500: 10 B8 9C 45  05 08 2D 40  05 05 08 50  6A 00 68 40  ...E..-@ ...Pj.h@
0510: 05 05 08 E8  88 00 00 00  B8 00 00 00  00 83 C4 1C  ........ ........
0520: C3 83 EC 0C  E8 D5 FF FF  FF 83 EC 10  E8 08 00 00  ........ ........
0530: 00 89 04 24  E8 2F 00 00  00 55 89 E5  83 EC 08 83  ...$./.. .U......
0540: E4 F0 83 EC  14 68 A0 F3  04 08 FF 35  00 FC 04 08  .....h.. ...5....
0550: 68 AC F3 04  08 E8 EA 00  00 00 C7 04  24 00 00 00  h....... ....$...
0560: 00 E8 02 00  00 00 00 00  55 89 E5 53  83 EC 0C 6A  ........ U..S...j
```

October 0x7DE

Sun	Mon	Tue	Wed	Thu	Fri	Sat
			01 00001	02 00010	03 00011	04 00100
05 00101	06 00110	07 00111	08 01000	09 01001	0A 01010	0B 01011
0C 01100	0D 01101	0E 01110	0F 01111	10 10000	11 10001	12 10010
13 10011	14 10100	15 10101	16 10110	17 10111	18 11000	19 11001
1A 11010	1B 11011	1C 11100	1D 11101	1E 11110	1F 11111	

ところで前述
したように

私はアセンブラとかの
一般ウケを狙った本を
多く書いているのですが

これらのネタでも
書いてみました

バイナリで遊ぼう！

Binary | Assembly Language | Machine Language
0と1のコンピュータ世界
バイナリで遊ぼう！
［バイナリを読むことは、楽しい！］

著者陣(Binarists)

坂井 弘亮
坂井 丈泰
愛甲 健二
竹迫 良範
松田 和樹

目的

現代の草食な若者の間で
近年流行しているバイナリ解析
なるものの, 正しい楽しみかたを
一般に伝えなければ

書籍中で
紹介している
バイナリ遊び

バイナリかるた
アセンブラかるた
などの他に

バイナリ体操
バイナリけんけんぱ
バイナリ鑑賞

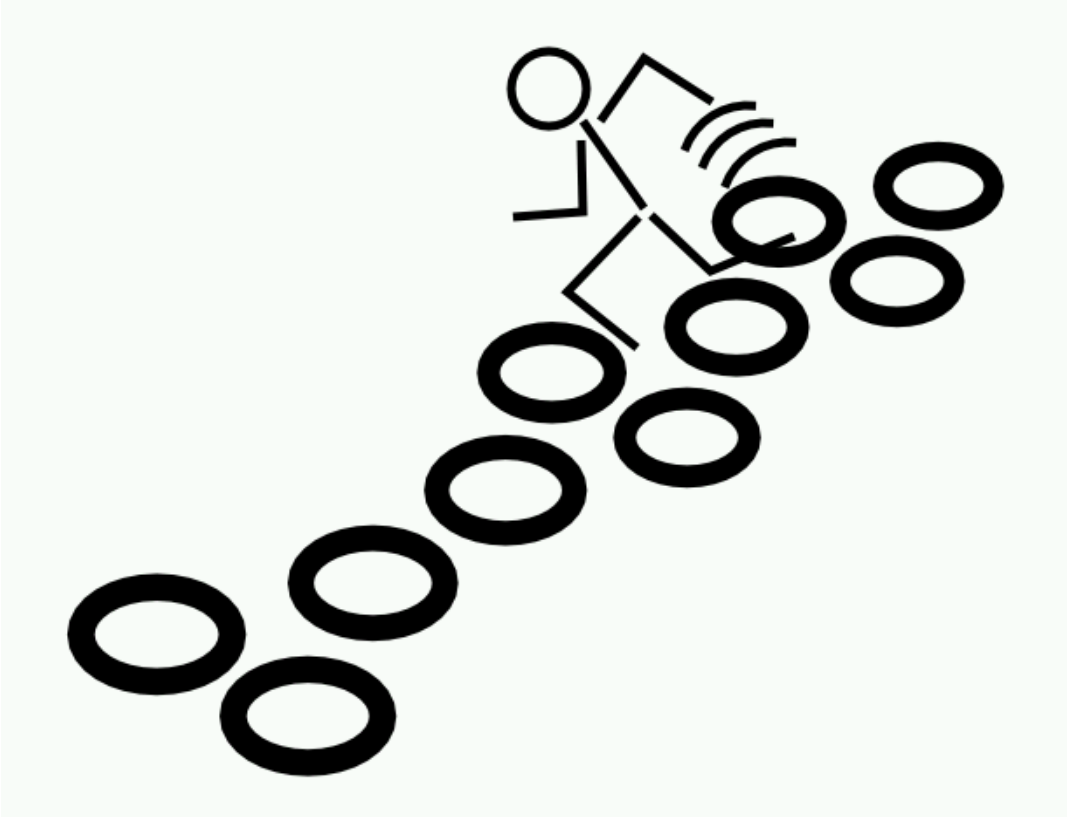
「そんなこと言っても
２進数が苦手です」

「ていうかそもそも
バイナリって何？」

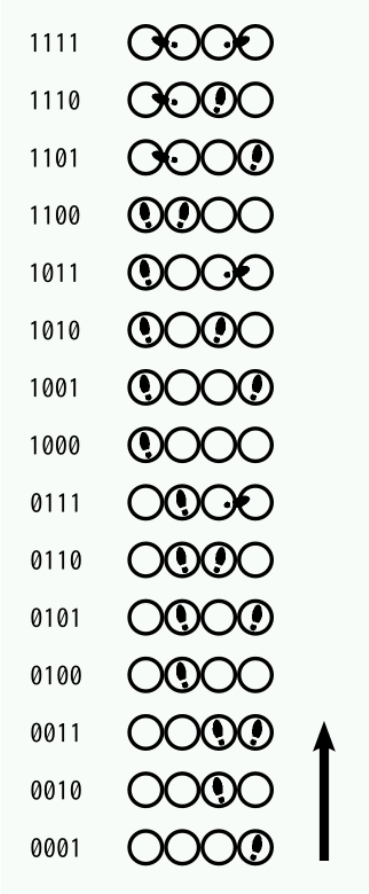
そんなあなたのために

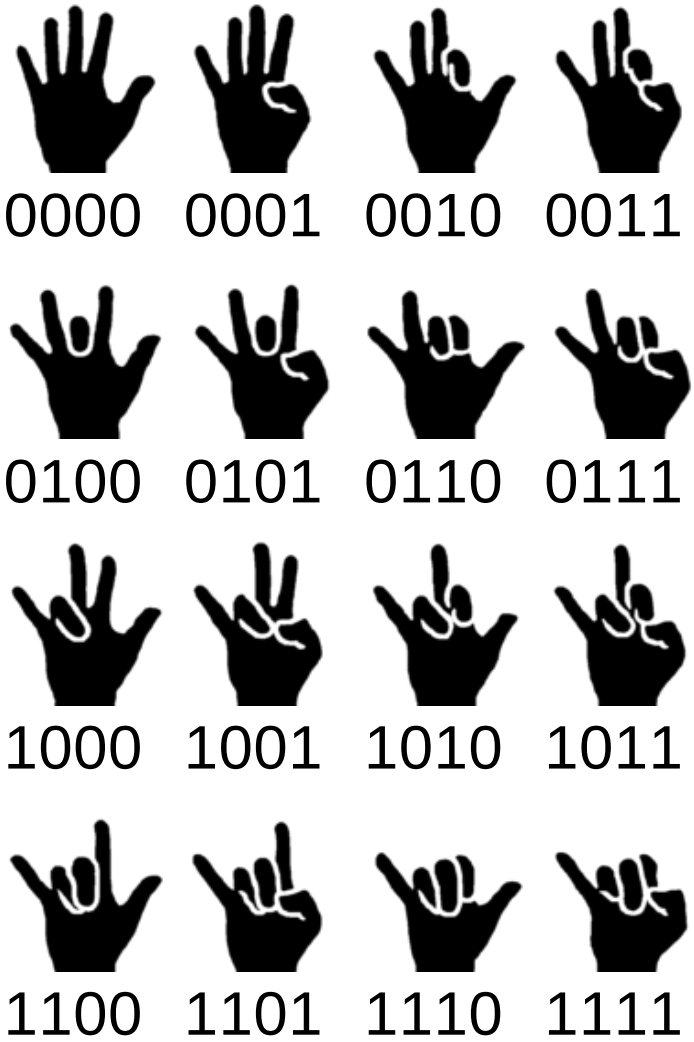
書籍中で紹介している
２進数に慣れ親しむ
方法を紹介

普通のけんけんぱ



バイナリけんけんぱ


1111
1110
1101
1100
1011
1010
1001
1000
0111
0110
0101
0100
0011
0010
0001


0000 0001 0010 0011
0100 0101 0110 0111
1000 1001 1010 1011
1100 1101 1110 1111

どうもありがとう
ございました