

SECCONにおける新たな試み

アセンブラ短歌と
バイナリかるた

坂井弘亮
(KOZOSプロジェクト)

今年度のSECCONでは、セキュリティに関する低レイヤー教育の目的で、以下の試みを行いました

アセンブラ短歌(コンテスト)

バイナリかるた(競技)

アセンブラ短歌

アセンブラ短歌の目的

機械語 ... コンピュータが理解する最も低水準な言語
アセンブラ(アセンブリ言語) ... 機械語を人間にわかりやすい
シンボルで記述したもの

- セキュリティの根本を理解するためには, 機械語やアセンブラなどの低レイヤーの理解が重要
- しかしアセンブラ・プログラミングの分野は空洞化しており, 学習が困難
- 中高生や若年層が遊び感覚でアセンブラを学習するための題材を提供したい

アセンブラ短歌とは

5・7・5・7・7の機械語コードで短いプログラムを書いてみる

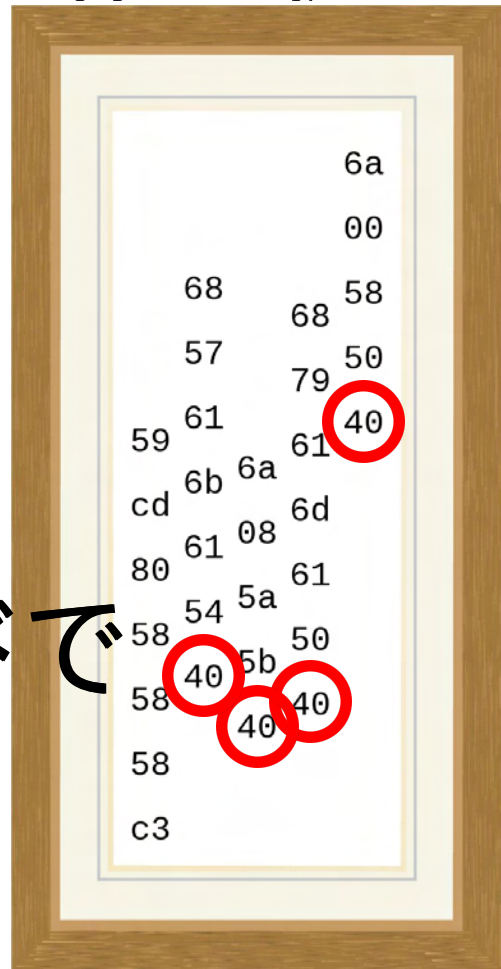
- 31バイトの限られた機械語コードでプログラミングする
- 決められた位置で区切られるようにプログラミングする
- 決まったバイトパターンを決まった位置に埋め込む(韻を踏む)
- あえて特定の命令を使って(もしくは使わずに)プログラミングする

シェルコードの理解に繋がる (攻撃から守るためには、まずはどのような攻撃があり得るのか、攻撃手法を理解することが必要)

アセンブラ短歌の作品例

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

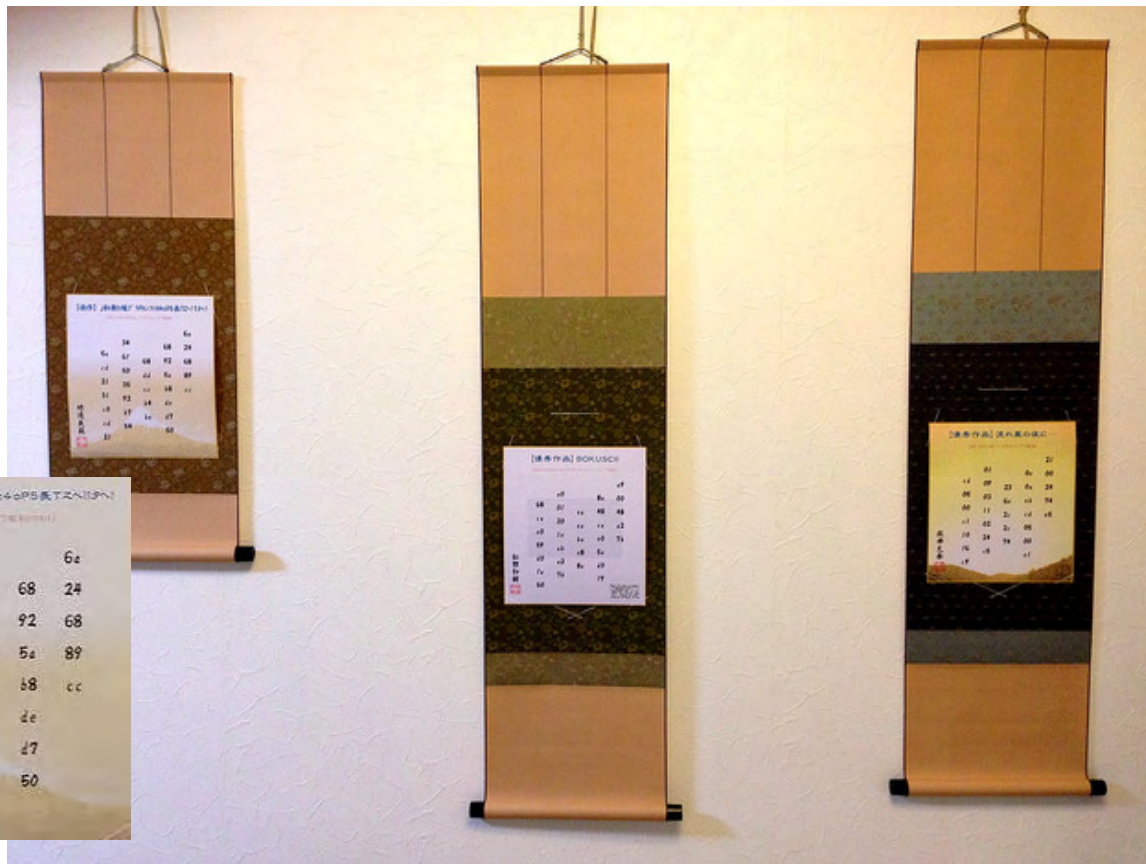
機械語コードで
韻をふむ



SECCONでのイベント実施

- **2013年10月**
長野大会でコンテストと品評会を実施
- **2014年3月**
全国大会でコンテストと品評会を実施予定

(長野大会) 優秀作品を掛軸にして展示



【作品名】3桁数字順ダウソフエセ49P5長アスヘUP2
2019年10月10日開催の「第10回長野県大会」にて出品された作品です。

				6e
	34		68	24
5a	67	68	92	68
cd	50	4d	5a	89
2l	35	cc	68	cc
3l	92	b4	2e	
c0	b7	be	27	
cd	54		50	
2l				

竹道 良範

【作品名】3桁数字順ダウソフエセ49P5長アスヘUP2
2019年10月10日開催の「第10回長野県大会」にて出品された作品です。

				6e
	34		68	24
5a	67	68	92	68
cd	50	4d	5a	89
2l	35	cc	68	cc
3l	92	b4	2e	
c0	b7	be	27	
cd	54		50	
2l				

【作品名】3桁数字順ダウソフエセ49P5長アスヘUP2
2019年10月10日開催の「第10回長野県大会」にて出品された作品です。

【作品名】BOKUSO

				6e
	34		68	24
5a	67	68	92	68
cd	50	4d	5a	89
2l	35	cc	68	cc
3l	92	b4	2e	
c0	b7	be	27	
cd	54		50	
2l				

【作品名】3桁数字順ダウソフエセ49P5長アスヘUP2
2019年10月10日開催の「第10回長野県大会」にて出品された作品です。

【作品名】流れる水

				27
	34		68	24
5a	67	68	92	68
cd	50	4d	5a	89
2l	35	cc	68	cc
3l	92	b4	2e	
c0	b7	be	27	
cd	54		50	
2l				

様々なアーキテクチャでの実施例

組込み機器も視野に入れ、PC以外の各種マイコン等でも実施

- **M32C(三菱)**
- **MN10300(パナソニック)**
- **RL78, RX (ルネサス)**
- **その他 ... Z80, 6502, 68HC11, VAX 等**

様々なプラットフォーム上で実施

- **Windows, Linux, FreeBSD, Mac OS X, MS-DOS**

普及のためには
入門書が必要

SECCON実行委員
メンバーにより執筆

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



バイナリかるた

バイナリかるたの目的

バイナリデータを目視で解析できる技術の育成 (ツールによる解析には限界がある)

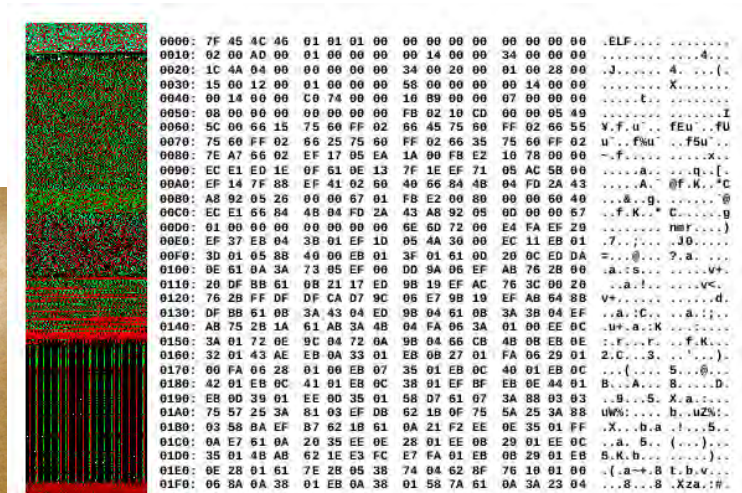
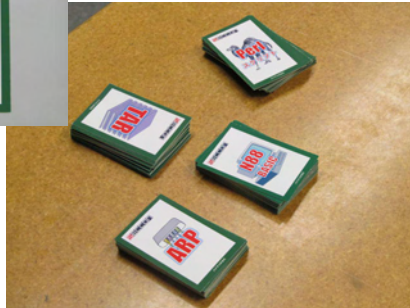
バイナリデータに関する理解を深める

- 初心者がゲーム感覚でバイナリ解析に慣れ親しむための題材を提供したい
- バイナリ解析に興味を持つためのきっかけと土壌を作りたい

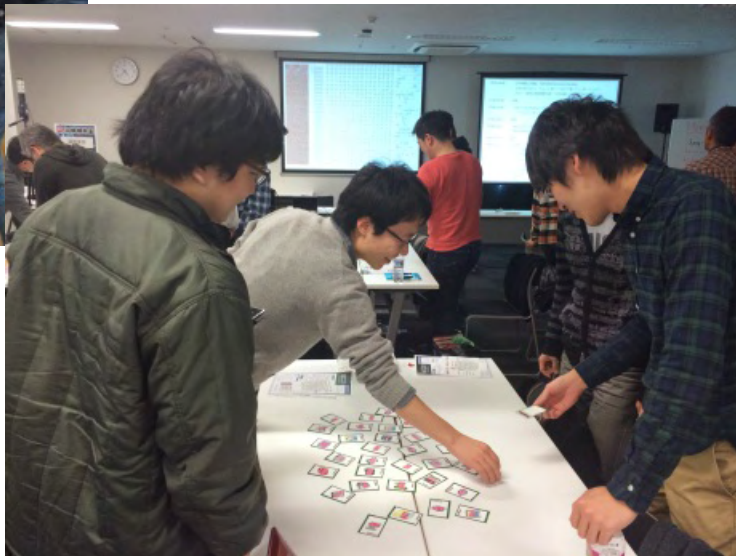
バイナリかるたとは

プロジェクトにバイナリダンプを投影し、対応するバイナリ・フォーマットの札をとるかるた競技

- ビットマップ画像, データ, ASCII文字から判断

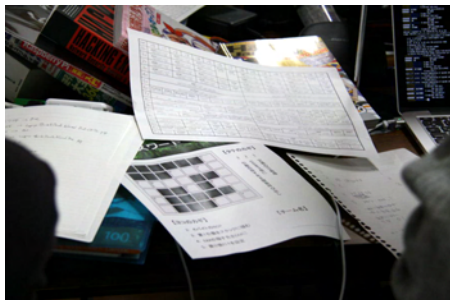


SECCONでの実施風景



低レイヤー教育の推進のためのその他の試み

- 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



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 10011	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	

終