触媒としてのセキュリティコンテスト

～ SECCONの現在までの取組とこれからの展望

竹迫 良範（SECCON実行委員長 / サイボウズ・ラボ）

寺島 崇幸 a.k.a. tessy（AVTokyo/sutegoma2）

宮本 久仁男（NTTデータ / 情報セキュリティ大学院大学）

坂井 弘亮

ハッカー vs. クラッカー

- 悪いハッカー
  - インターネット経由で機密情報を盗む人？
  - テロリスト？（ハリウッド映画の影響？）
  - 高度な技術力を駆使してコンピュータシステムに不正侵入する人？
  - 不正アクセス行為をして逮捕される人？
- 良いハッカー
  - ホワイトハッカー？
  - 善玉ハッカー？　正義のハッカー？

世界で一番有名な日本人ハッカー?

1995: Kevin Mitnickの逮捕に協力

U.S. Department of Justice
United States Marshals Service

WANTED
BY U.S. MARSHALS

NOTICE TO ARRESTING AGENCY: Before arrest, validate warrant through National Crime Information Center (NCIC).

United States Marshals Service NCIC entry number: (NIC/ W721460021).

NAME: .....MITNICK, KEVIN DAVID

AKS (S): .....MITNIK, KEVIN DAVID
MERRILL, BRIAN ALLEN

DESCRIPTION:

Sex: .....MALE
Race: .....WHITE
Place of Birth: .....VAN NUYS, CALIFORNIA
Date(s) of Birth: 08/06/63; 10/18/70
Height: .....5'11"
Weight: 190
Eyes: .....BLUE
Hair: .....BROWN
Skintone: .....LIGHT
Scars, Marks, Tattoos: .....NONE KNOWN
Social Security Number (s): 550-39-5695
NCIC Fingerprint Classification: ...DOPM20PM13DIPM19PM09

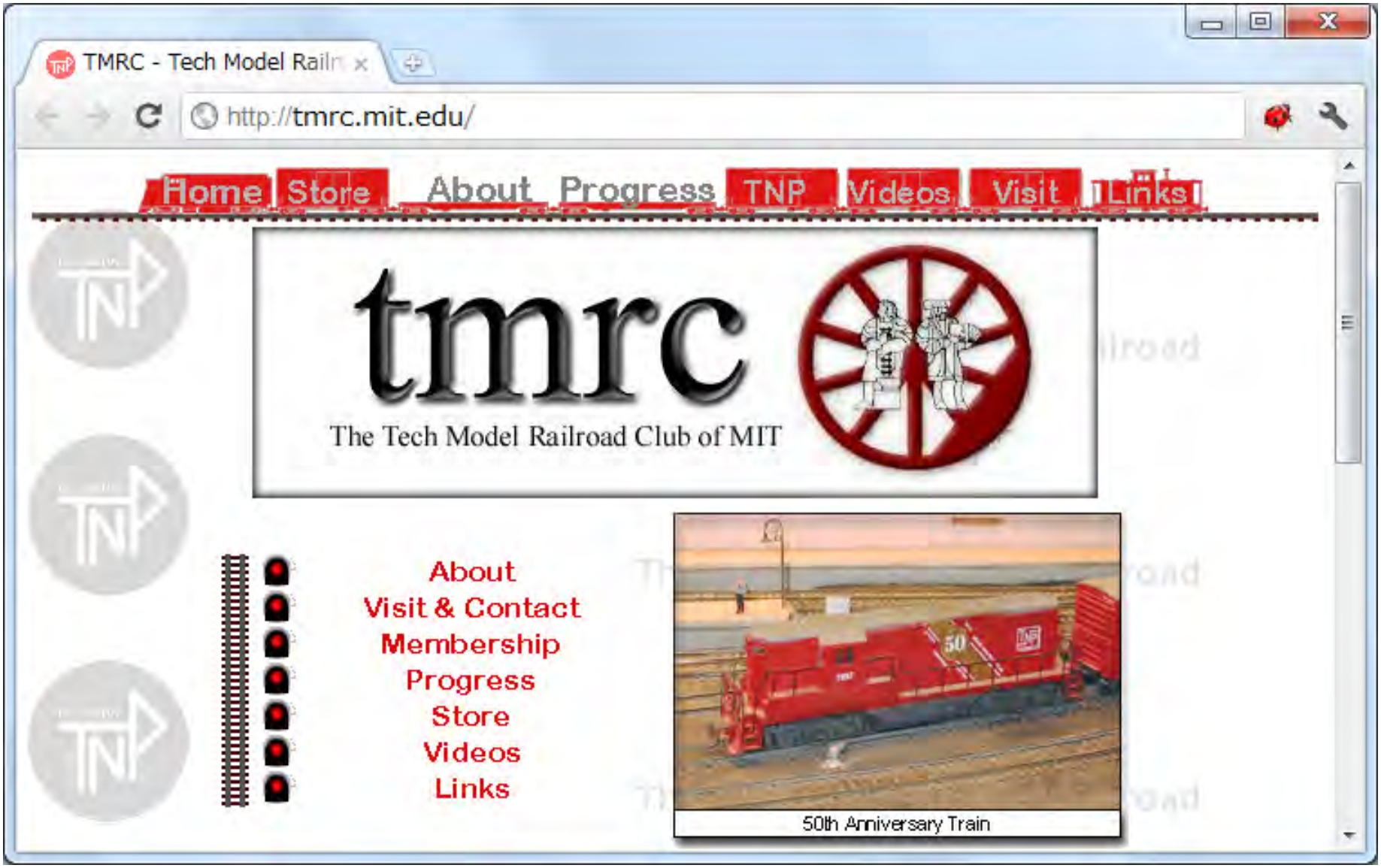
「Take down」
映画化
「ザ・ハッカー」

ハッカーとは

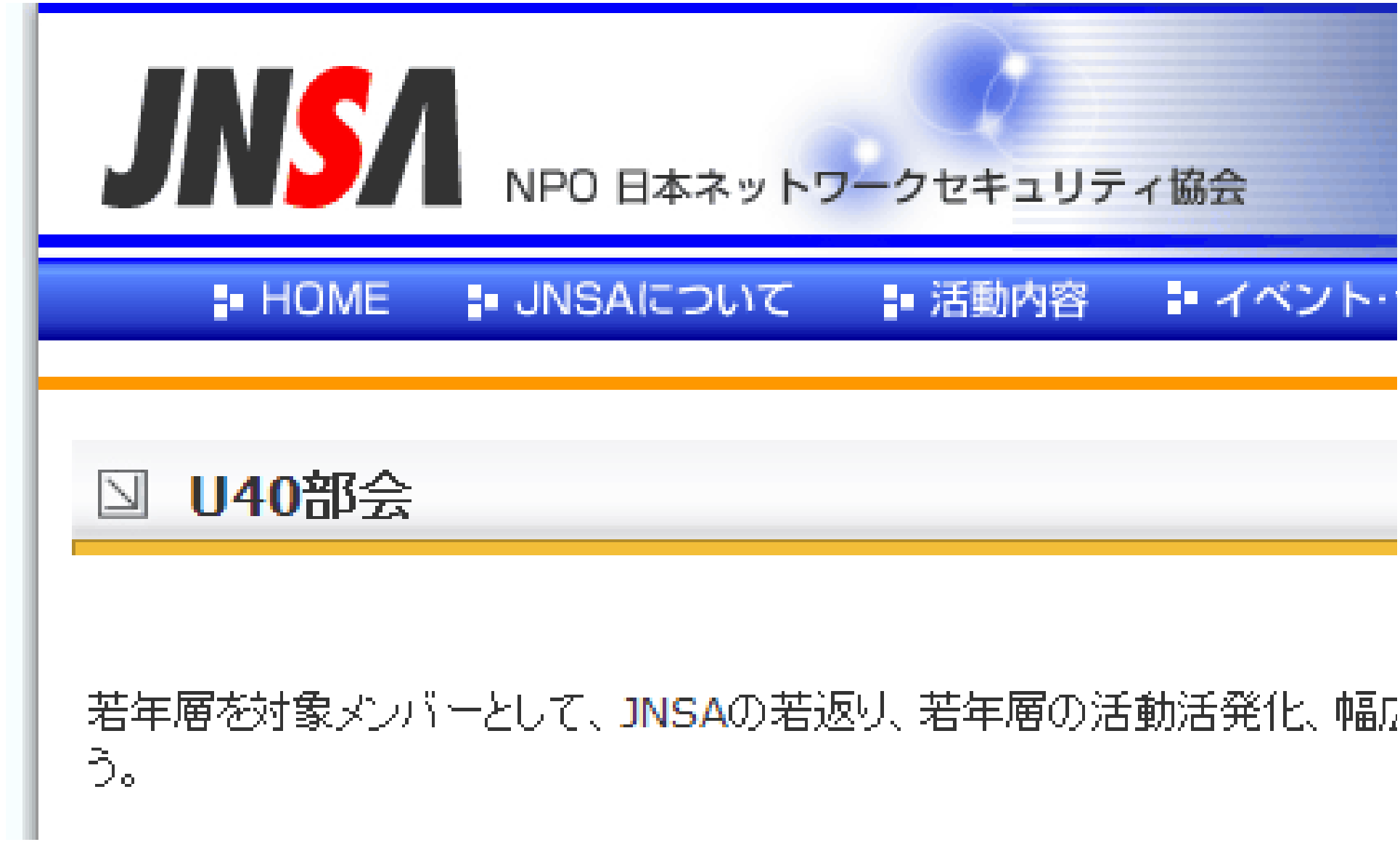
- コンピュータについて
  - 常人より深い技術的知識を持ち
- その知識を利用して
  - 技術的な課題に対して
  - 最小限の手間で
  - 最大の効果を生み出す人々

日本語版 Wikipedia より

ハッカーの誕生場所


TMRC - Tech Model Railr
http://tmrc.mit.edu/
Home
Store
About
Progress
TNP
Videos
Visit
Links
tmrc
The Tech Model Railroad Club of MIT
About
Visit & Contact
Membership
Progress
Store
Videos
Links
50th Anniversary Train

日本の若手セキュリティ人材



日本のセキュリティコンテスト

大会名	主催者	参加対象	競技形式	
セキュリティキャンプ	セキュリティキャンプ実施協議会（IPA）	22歳以下の学生	問題回答型	研修の1パートとして実施
SECCON CTF	SECCON 実行委員会（JNSA）	学生もしくは22歳以下	問題回答型	日本で初めての本格的なCTF大会
危機管理コンテスト	情報危機管理コンテスト運営委員会	博士後期課程を除く学生	トラブル対応型	白浜シンポジウムの一部として実施
IT Keys	IT Keys運営委員会	特定大学の学生	演習科目	京大、阪大、北陸先端、奈良先端の4大学を中心とした育成プログラムの一部
MWS Cup	MWS実行委員会	情報処理学会加入メンバー	問題回答型（マルウェア解析）	情報処理学会主催のイベントの一部
Hardening Zero	Hardening Zero 実行委員会	制約なし	攻防型（防御のみ）	
CTFチャレンジジャパン 2012	経済産業省（2012年度委託事業）	社会人（23歳以上の学生可）	フラッグ取得型問題回答型	

海外での取組み事例　（米国）

- DEFCON：年1回 ラスベガス
  - 世界各国から予選を通過した20チームが参加
  - 2012年の優勝チームは80人体制（会場に入れるのは8人）
  - 2012年が20回目の開催
  - セキュリティ技術者の発掘の場として注目
- NetWars：年数回 ワシントンDC、ラスベガス他
  - SANSトレーニングの一環として、1500人規模のイベントに併設で開催
  - 1回の参加人数は200人程度で世界最大級
- US CyberChallenge
  - 学生向けの人材発掘目的
  - 優秀者はインターンシップや奨学金が授与される（マイクロソフトなどがスポンサー）
- そのほか8つ程度のCTF大会が継続開催されており、地区大会・州大会も無数に存在

DEFCON終了後の意見交換

NetWarsの実施風景

CTF (Capture The Flag)

- グループ対抗の旗取り合戦
  - もともとは欧米の子供の遊び
- 仮想サーバーに「旗を立てる」
  - 「旗を立てさせない」攻防戦
- 日本語で言うと「サイバー騎馬戦」!?

防御・解析と攻撃技術
の両方を学ぶ
実践的な場

2012年度のCTF開催実績（日本国内）

- SECCON CTF（日本ネットワークセキュリティ協会）
  - 参加チーム：38（160人）※学生あるいは22歳以下
    - 九州大会：2012年 2月　7 チーム
    - 関東大会：2012年 5月　13チーム
    - 関西大会：2012年11月　5 チーム
    - 横浜大会：2012年12月　13チーム
  - 全国大会：2013年2月　地方大会の上位10チームを招待
- CTFチャレンジジャパン2012（経済産業省委託事業）
  - 参加チーム：46 （166人）※社会人および23歳以上の学生
    - 福岡予選会：2012年11月　11チーム
    - 大阪予選会：2012年11月　6 チーム
    - 東京予選会：2012年12月　22チーム
    - 仙台予選会：2012年12月　9 チーム
  - 決勝大会　：2013年2月 予選会の上位9チームを招待

SECCON CTF 参加校（2012年度）

■ 大学院（7校）：
岡山大学大学院
慶應義塾大学大学院
情報セキュリティ大学院大学
奈良先端科学技術大学院大学
名古屋大学大学院
筑波大学大学院
東北大学大学院

■ 大学（16校）：
会津大学
東北大学
福岡大学
法政大学
香川大学
九州工業大学
京都大学
慶應義塾大学
信州大学
筑波大学
電気通信大学
東京工科大学
東京電機大学
名古屋大学
大阪大学
明治大学

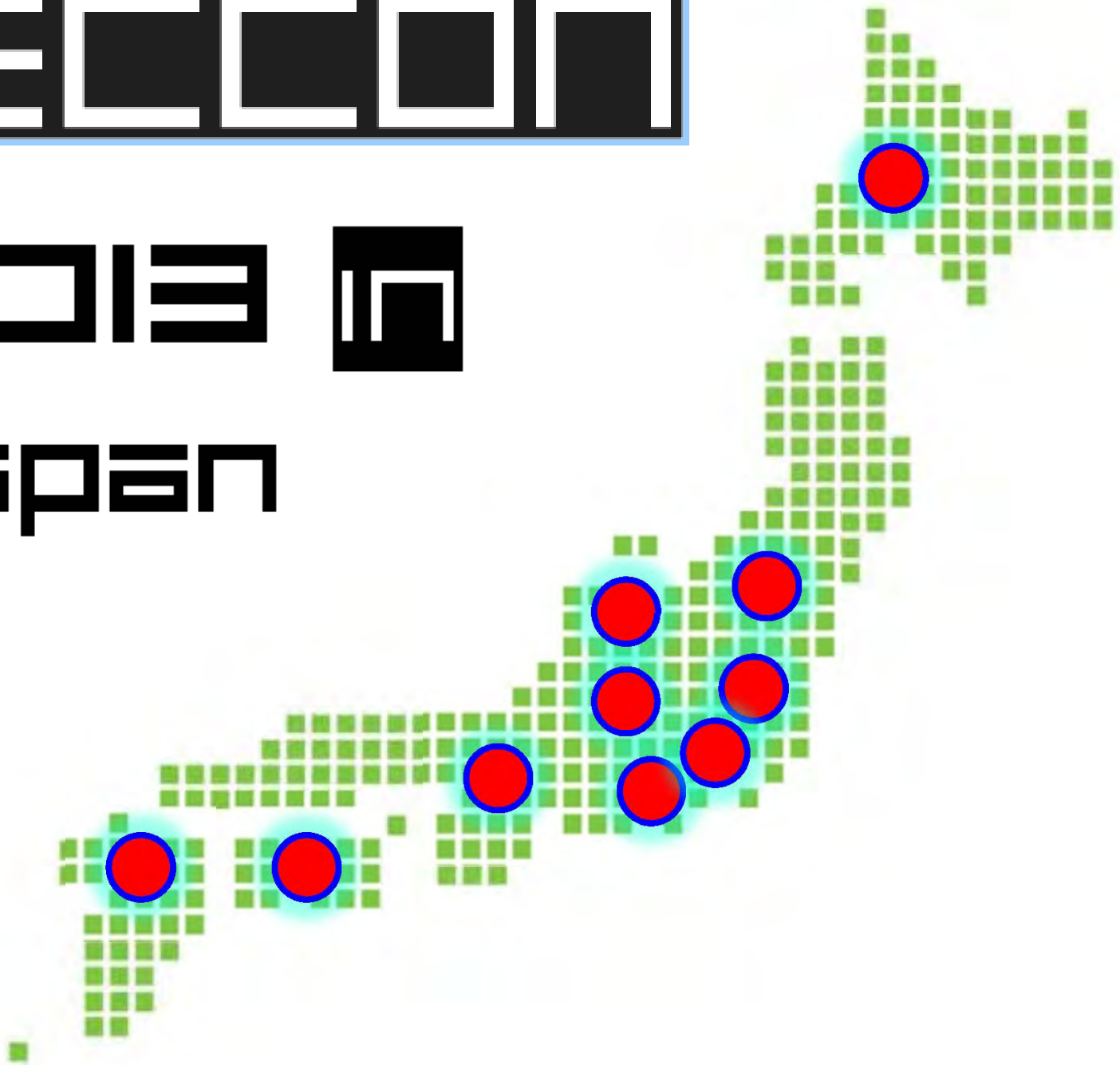
■ 専門学校（5校）：
HAL東京
日本工学院八王子専門学校
国立東京工業高等専門学校
情報科学専門学校
船橋情報ビジネス専門学校

■ 高等専門学校（3校）：
東京高等専門学校
熊本高等専門学校
沼津工業高等専門学校

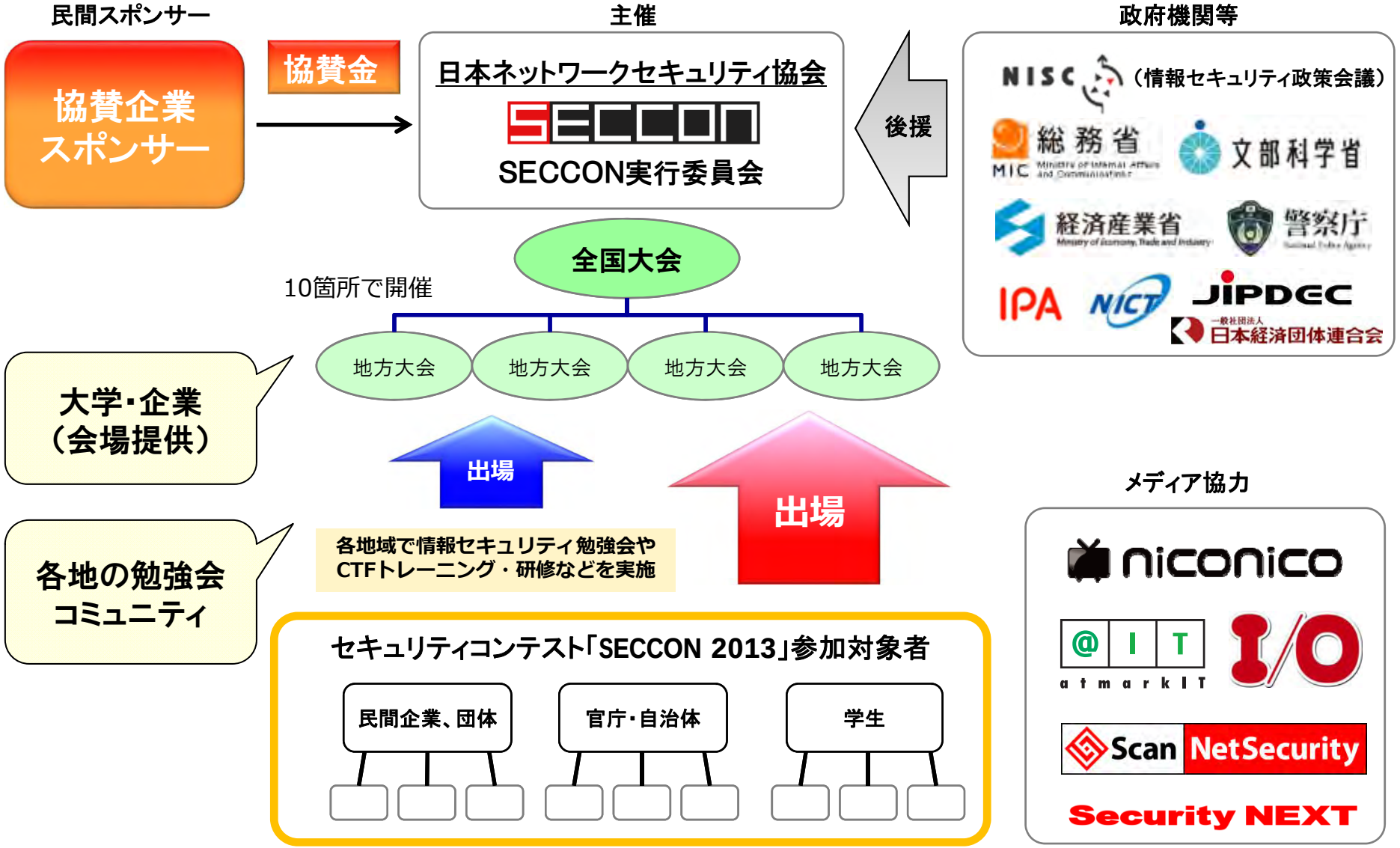
■ 高校（10校）：
小山工業高等学校
千葉県立京葉工業高校
愛媛県私立愛光高校
愛知県立五条高等学校
筑波大学附属駒場高等学校
灘高校
山形県立長井高等学校
新潟高等学校
海城高校
群馬県立高崎工業高校

■ 中学（1校）：
灘中学

SECCON 2013 in Japan



SECCON 2013 実施図



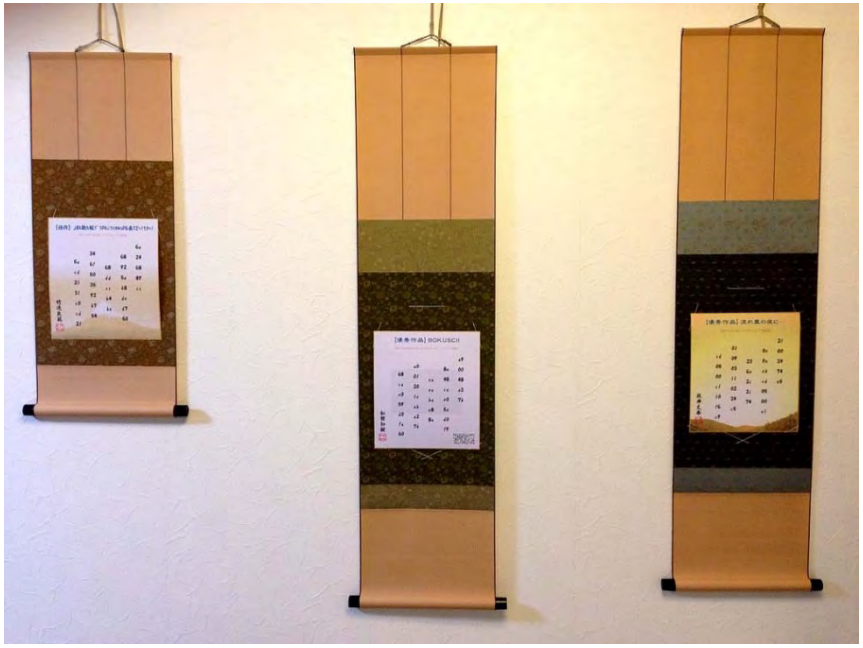
SECCON 2013 開催スケジュール

回数	日程	開催地域	会場
1	8月22日～23日	関東（横浜）	パシフィコ横浜 （CEDEC 2013）
2	10月5日～6日	甲信越（長野）	信州大学工学部
3	10月5日～6日	九州（福岡）	九州工業大学情報工学部
4	10月20日	四国（香川）	香川大学総合情報センター
5	11月9日～10日	東北（福島）	会津藩校 日新館
6	11月30日～12月1日	北海道（札幌）	札幌市
7	11月30日～12月1日	北陸（富山）	インテックビル「タワー111」
8	12月14日～15日	東海（名古屋）	ウインクあいち
9	12月14日～15日	関西（大阪）	マイドームおおさか
10	1月25日～26日	オンライン予選	情報セキュリティ大学院大学
11	**3月1日～2日**	**全国大会**	**東京電機大学**

SECCON 2013 協賛企業

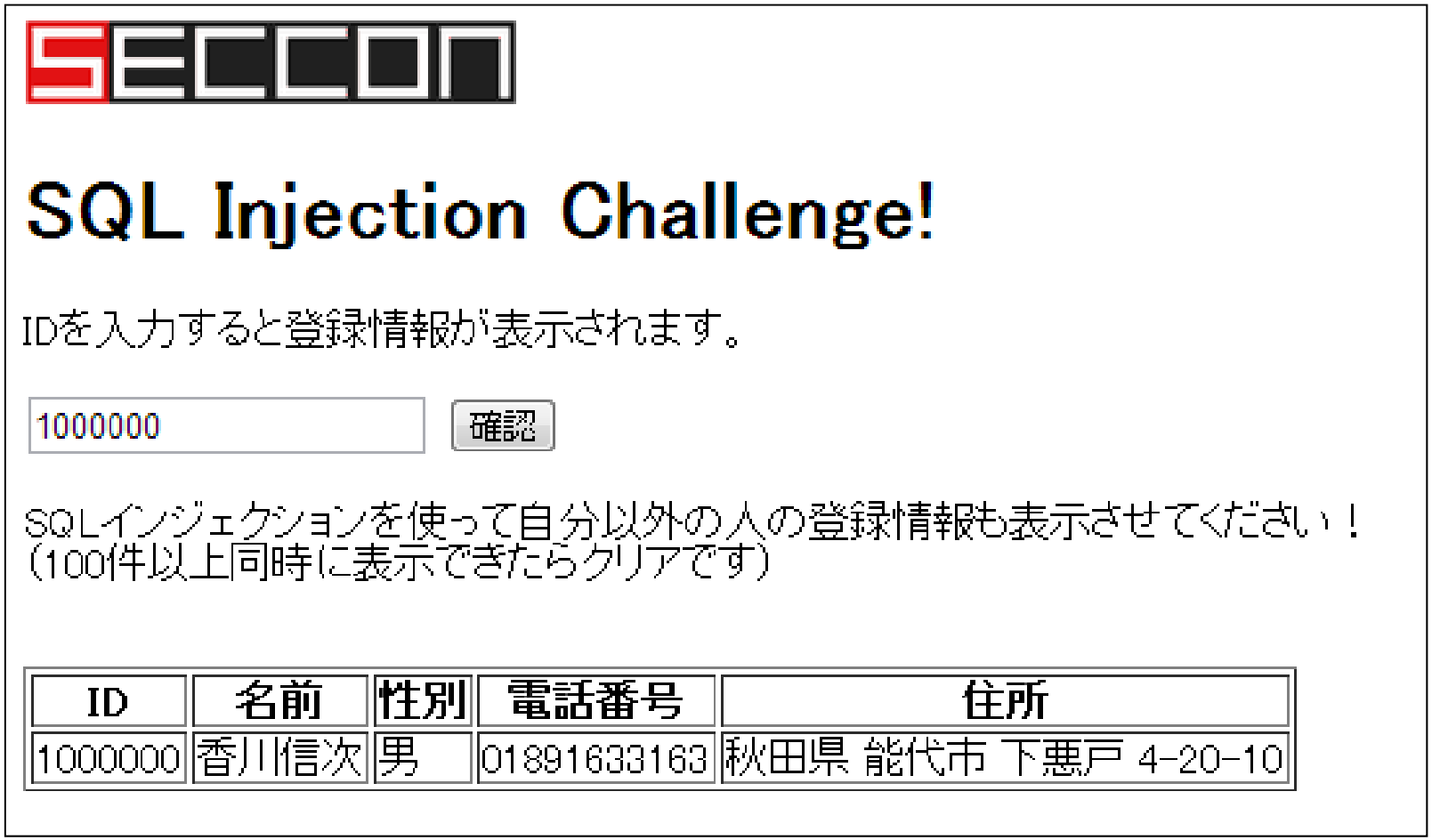
CTF以外の様々なコンテストも併催

- サイボウズSecurity Challenge（賞金300万円）
- Wireshark パケット・コンテスト
- Shellcoder’s Challenge
- アセンブラ短歌（5･7･5･7･7機械語）



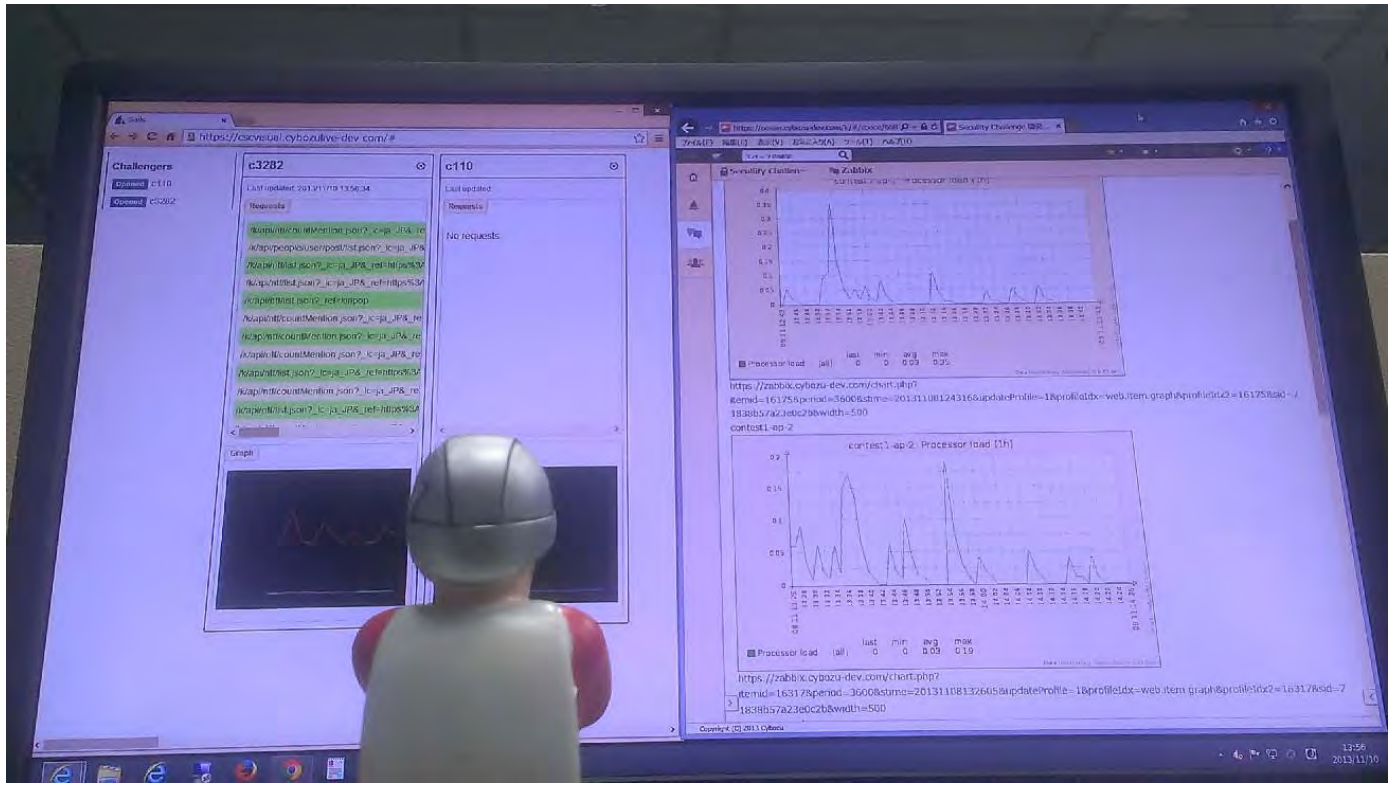
SQLインジェクションチャレンジ

■体験サーバの提供



Cybozu.com Security Challenge

■賞金総額 300万円の脆弱性発見大会

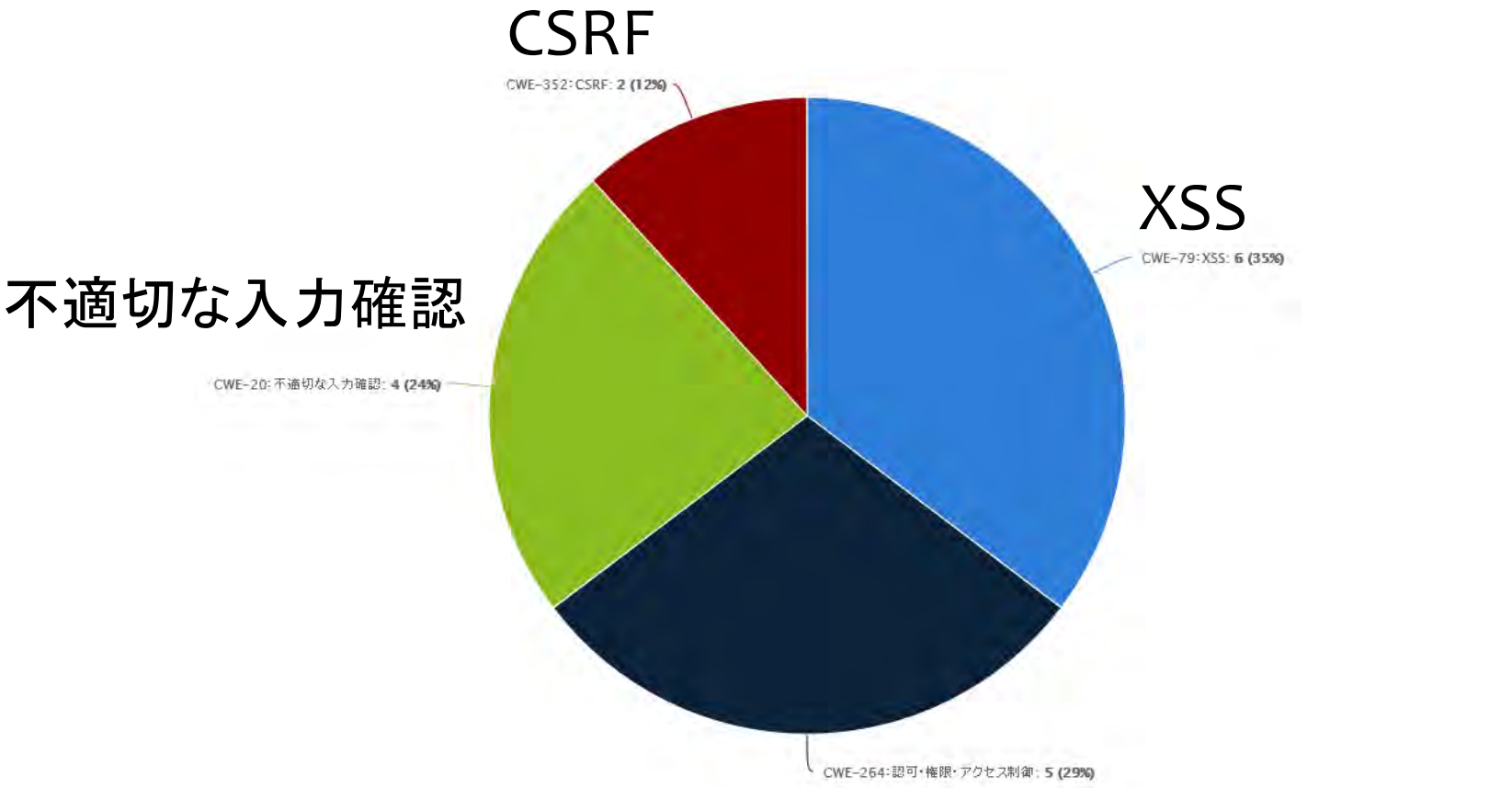


Security Challenge の攻撃者をリアルタイム監視してみた

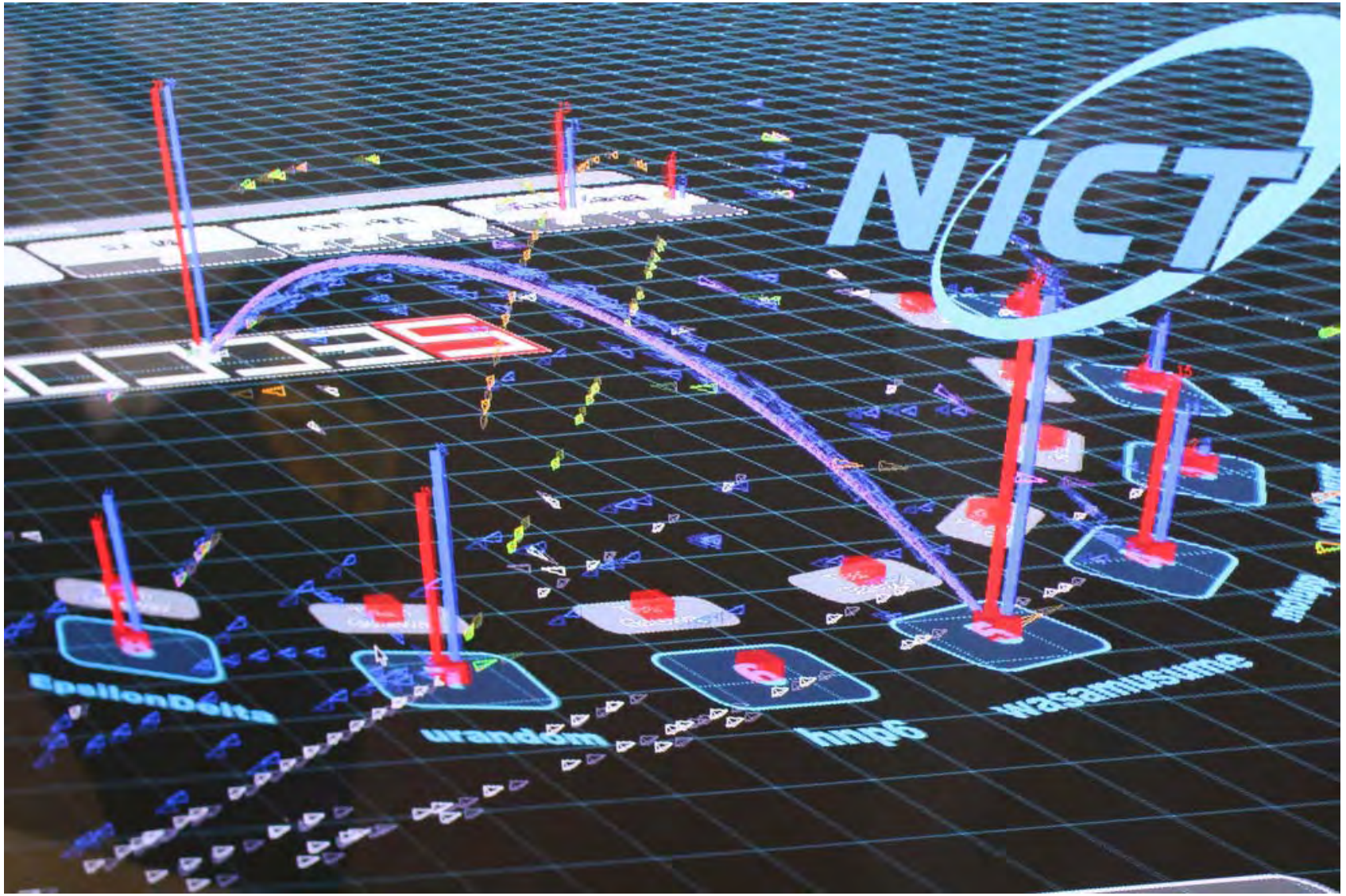
http://developer.cybozu.co.jp/tech/?p=6397

ご報告いただいた脆弱性情報 20件

■申込人数 95 名 / 参加人数 75 名



SECCON 攻防戦の可視化 (協力:NICT)

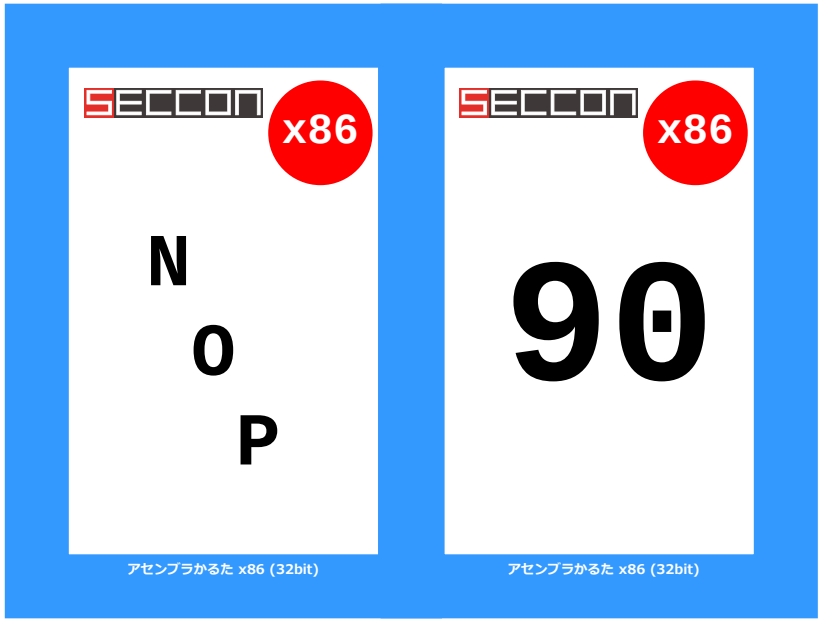


セキュリティ早押しクイズ

- セキュリティやゲームやインターネットに関する問題を早押しで解答する競技

アセンブラかるた（x86）

- アセンブラの命令が読み上げられたら、その機械語命令に対応する16進数の札を早く取る競技



x86 アセンブラ暗記表 (@a4lg)

insr.	x0	x1	x2	x3	x4	x5	x6	x7	x8	x9	xA	xB	xC	xD	xE	xF
0x	ADD (byte | word) reg/mem ← reg		ADD (byte | word) reg/mem → reg		ADD (byte | word) AL | eAX ← imm		PUSH ES | SS	POP ES | SS	OR (byte | word) reg/mem ← reg		OR (byte | word) reg/mem → reg		OR (byte | word) AL | eAX ← imm		PUSH CS | DS	⊕ 0F xx →
1x	ADC (byte | word) reg/mem ← reg		ADC (byte | word) reg/mem → reg		ADC (byte | word) AL | eAX ← imm				SBB (byte | word) reg/mem ← reg		SBB (byte | word) reg/mem → reg		SBB (byte | word) AL | eAX ← imm			POP DS
2x	AND (byte | word) reg/mem ← reg		AND (byte | word) reg/mem → reg		AND (byte | word) AL | eAX ← imm		seg.ES Prefix	DAA ⊕	SUB (byte | word) reg/mem ← reg		SUB (byte | word) reg/mem → reg		SUB (byte | word) AL | eAX ← imm		seg.CS Prefix	DAS ⊕
3x	XOR (byte | word) reg/mem ← reg		XOR (byte | word) reg/mem → reg		XOR (byte | word) AL | eAX ← imm		seg.SS Prefix	AAA ⊕	CMP (byte | word) reg/mem ← reg		CMP (byte | word) reg/mem → reg		CMP (byte | word) AL | eAX ← imm		seg.DS Prefix	AAS ⊕
4x	INC (word) eAX | eCX | eDX | eBX | eSP | eBP | eSI | eDI								DEC (word) eAX | eCX | eDX | eBX | eSP | eBP | eSI | eDI							
5x	PUSH (word) eAX | eCX | eDX | eBX | eSP | eBP | eSI | eDI								POP (word) eAX | eCX | eDX | eBX | eSP | eBP | eSI | eDI							
6x	PUSHA eAX → eDI	POPA eDI → eAX	BOUND ⊕	ARPL ⊕	seg.FS Prefix	seg.GS Prefix	o.size Prefix	o.addr Prefix	PUSH imm	IMUL (w) r/m*imm	PUSH imm8	IMUL (w) r/m*imm8	INSB byte | word [eDI] ← DX	INS	OUTSB byte | word [eSI] → DX	OUTS
7x	Jcc (short) O	NO	B/NAE/C	NB/AE/NC	Z/E	NZ/NE	BE/NA	NBE/A	S	NS	P/PE	NP/PO	L/NGE	NL/GE	LE/NG	NLE/G
8x	Immediate Group 1 r/m ← imm8 | imm		r/m ← imm8 | imm8		TEST (byte | word) reg/mem ↔ reg		XCHG (byte | word) reg/mem ↔ reg		MOV (byte | word) reg/mem ← reg		MOV (byte | word) reg/mem → reg		MOV (16) r/m ← sreg	LEA reg ← mem	MOV (16) r/m → sreg	Grp.1A Insr. Group
9x	XCHG eAX, reg (word) eAX (NOP)	eCX	eDX	eBX	eSP	eBP	eSI	eDI	CBW or CWDE	CWD or CDQ	CALL far	FWAIT or WAIT	PUSHF eFLAGS	POPF	SAHF AH ↔ eFLAGS	LAHF
Ax	MOV (byte | word) AL | eAX ← ptr[imm]		MOV (byte | word) AL | eAX → ptr[imm]		MOVSB byte | word [eDI] ← [eSI]	MOVS	CMPSB byte | word [eSI] ← [eDI]	CMPS	TEST (byte | word) AL | eAX ↔ imm		STOSB byte|word[eDI] ← AL|eAX	STOS	LODSB byte|word[eSI] → AL|eAX	LODS	SCASB AL|eAX ← byte|word[eDI]	SCAS
Bx	MOV (byte) AL | CL | DL | BL | AH | CH | DH | BH ← imm								MOV (word) eAX | eCX | eDX | eBX | eSP | eBP | eSI | eDI ← imm							
Cx	Shift Grp.2 byte | word ← imm8		RET (near) imm16	0	LES ⊕	LDS ⊕	Grp.11 (MOV) byte | word ← imm		ENTER ⊕	LEAVE	RET (far) 0	imm16	INT 3 (#BP)	imm8	INTO	IRET
Dx	Shift Grp.2 byte | word ← 1		Shift Grp.2 byte | word ← CL		AAM ⊕	AAD ⊕	SALC Undoc.	XLAT or XLATB	FPU Instructions 8087 Instruction Group							
Ex	LOOPNE	LOOPE	LOOP	JeCXZ short jump (imm8)		IN (imm8: byte | word) reg/mem ← I/O		OUT (imm8: byte | word) reg/mem → I/O	CALL near	JMP near	JMP far	JMP short	IN (DX: byte | word) reg/mem ← I/O		OUT (DX: byte | word) reg/mem → I/O	
Fx	LOCK Prefix	ICEBP Undoc.	REPNE Prefix	REPE or REP	HLT	CMC	Unary Grp.3 (b | w) r/m = ⊕(reg/mem)		CLC eFLAGS.CF ← 0 | 1	STC	CLI eFLAGS.IF ← 0 | 1	STI	CLD eFLAGS.DF ← 0 | 1	STD	Grp.4 INC/DEC	Grp.5 INC/DEC/...

http://d.hatena.ne.jp/a4lg/20120225/1330180431

Author: @a4lg

アセンブラ・クロスワードパズル(x86)

[Down]

1: mov EAX, EIP

2: EAX = EAX × 3

3: call [ESP+4]

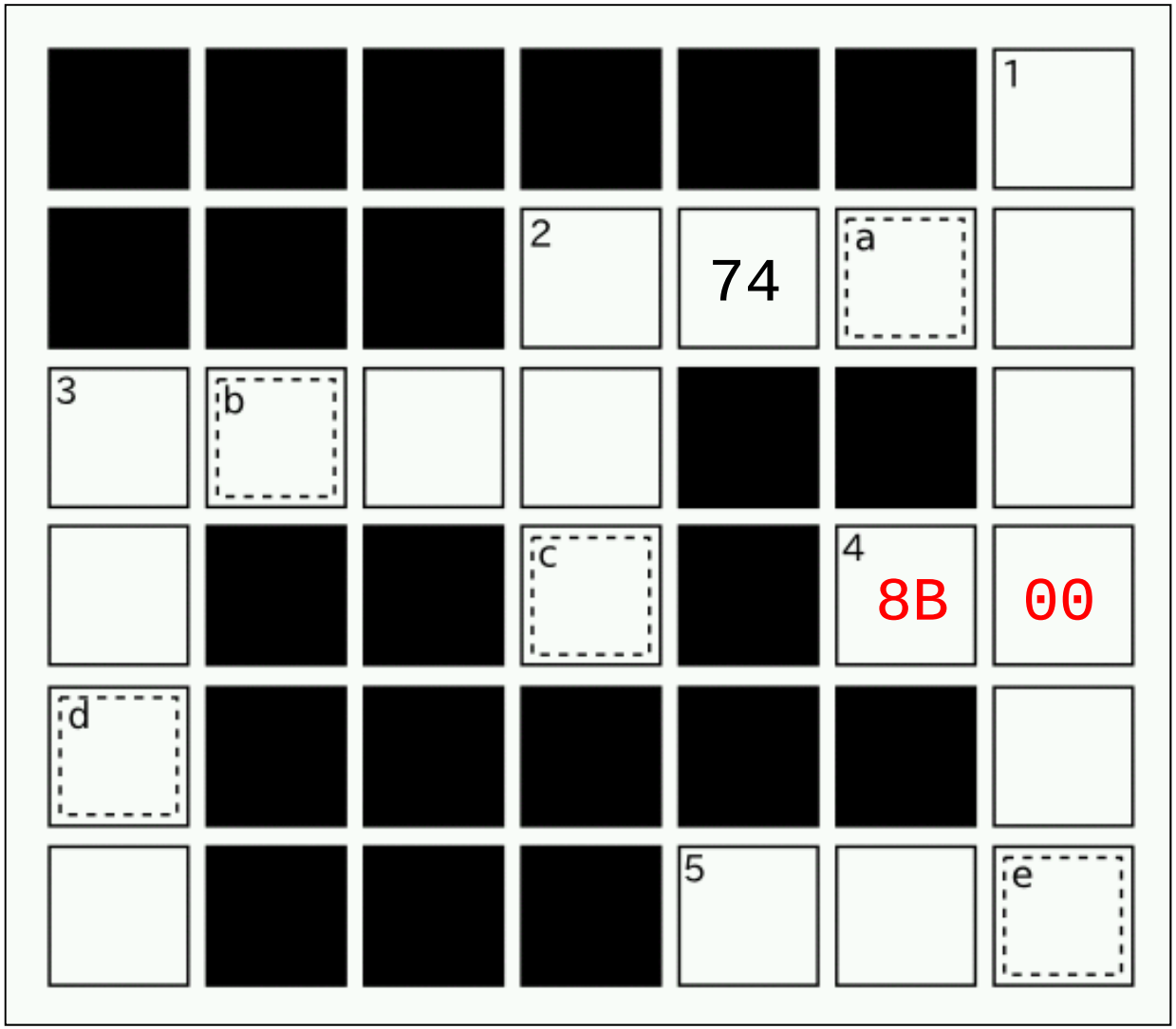
[Across]

2: NOP (4 bytes)

3: push [ESP+4]

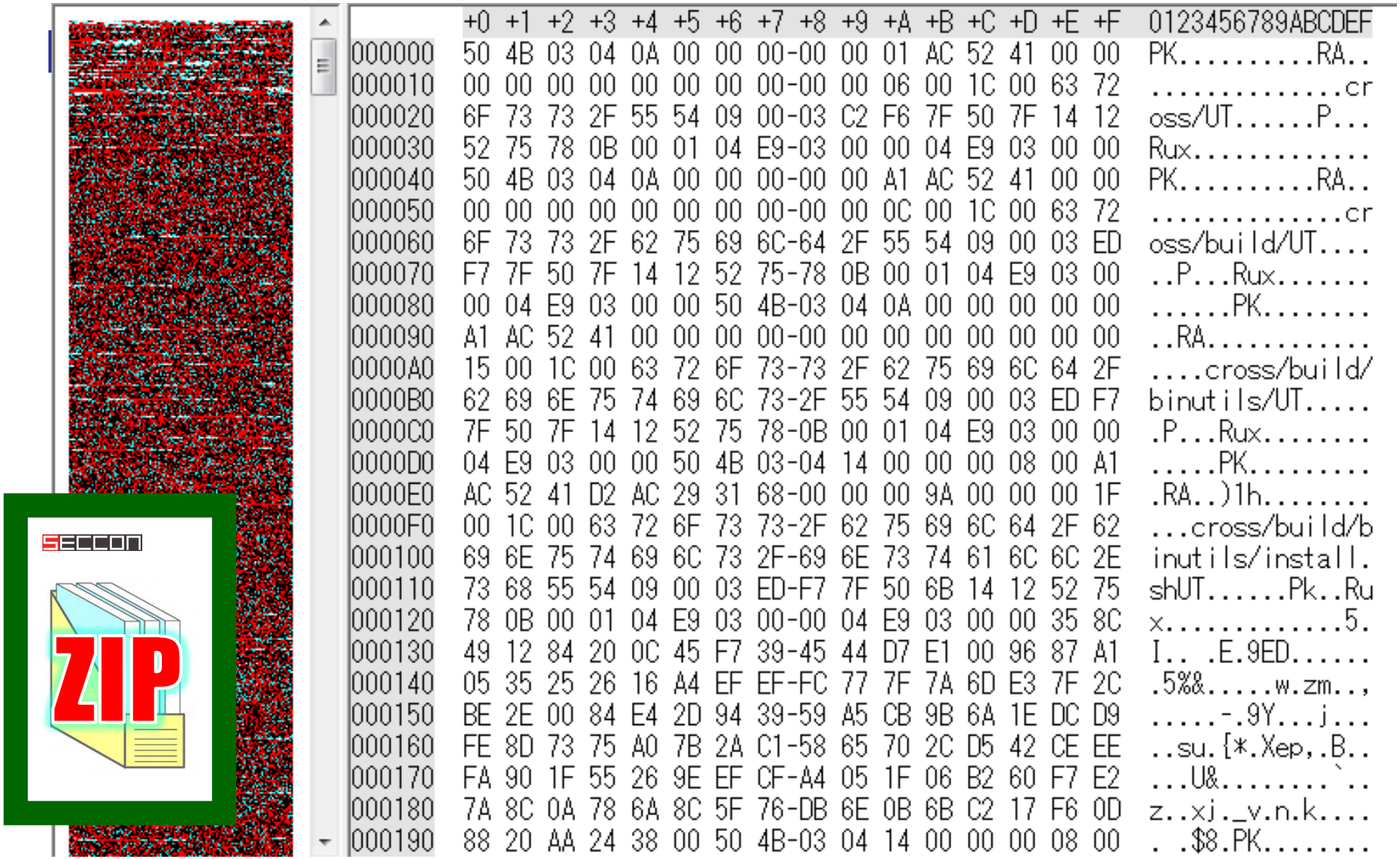
4: mov [EAX], EAX

5: return 1; //32bit



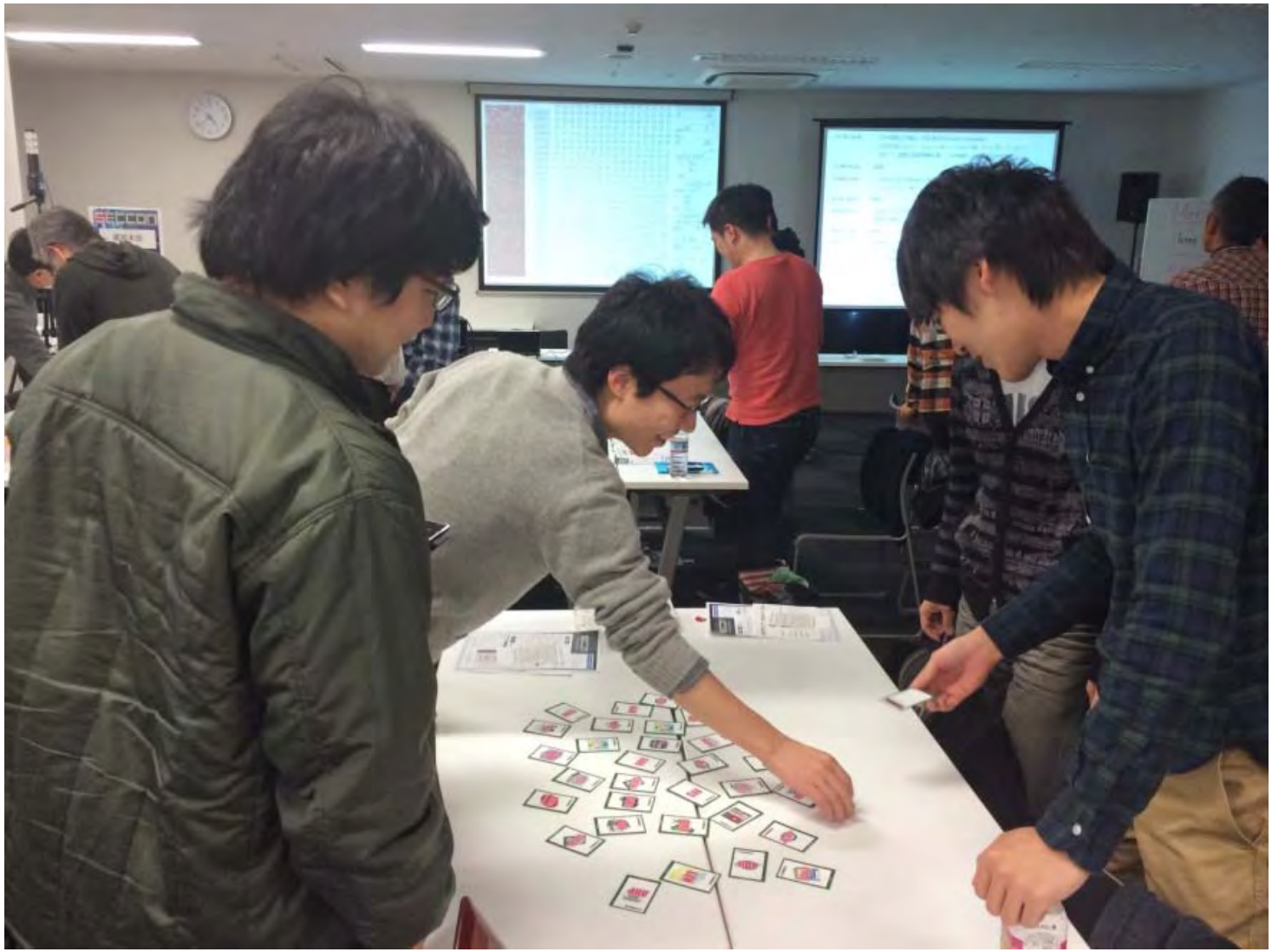
Author: Sakai Hiroaki

バイナリかるた（目grep対決）



	+0	+1	+2	+3	+4	+5	+6	+7	+8	+9	+A	+B	+C	+D	+E	+F	0123456789ABCDEF
000000	50	4B	03	04	0A	00	00	00	00	00	01	AC	52	41	00	00	PK.....RA..
000010	00	00	00	00	00	00	00	00	00	00	06	00	1C	00	63	72	.....cr
000020	6F	73	73	2F	55	54	09	00	03	C2	F6	7F	50	7F	14	12	oss/UT.....P...
000030	52	75	78	0B	00	01	04	E9	03	00	00	04	E9	03	00	00	Rux.....
000040	50	4B	03	04	0A	00	00	00	00	00	A1	AC	52	41	00	00	PK.....RA..
000050	00	00	00	00	00	00	00	00	00	00	0C	00	1C	00	63	72	.....cr
000060	6F	73	73	2F	62	75	69	6C	64	2F	55	54	09	00	03	ED	oss/build/UT....
000070	F7	7F	50	7F	14	12	52	75	78	0B	00	01	04	E9	03	00	..P...Rux.....
000080	00	04	E9	03	00	00	50	4B	03	04	0A	00	00	00	00	00	......PK.....
000090	A1	AC	52	41	00	00	00	00	00	00	00	00	00	00	00	00	..RA.....
0000A0	15	00	1C	00	63	72	6F	73	73	2F	62	75	69	6C	64	2F	....cross/build/
0000B0	62	69	6E	75	74	69	6C	73	2F	55	54	09	00	03	ED	F7	binutils/UT.....
0000C0	7F	50	7F	14	12	52	75	78	0B	00	01	04	E9	03	00	00	.P...Rux.....
0000D0	04	E9	03	00	00	50	4B	03	04	14	00	00	00	08	00	A1	.....PK.....
0000E0	AC	52	41	D2	AC	29	31	68	00	00	00	9A	00	00	00	1F	.RA..)1h.....
0000F0	00	1C	00	63	72	6F	73	73	2F	62	75	69	6C	64	2F	62	...cross/build/b
000100	69	6E	75	74	69	6C	73	2F	69	6E	73	74	61	6C	6C	2E	inutils/install.
000110	73	68	55	54	09	00	03	ED	F7	7F	50	6B	14	12	52	75	shUT.....Pk..Ru
000120	78	0B	00	01	04	E9	03	00	00	04	E9	03	00	00	35	8C	x.....5.
000130	49	12	84	20	0C	45	F7	39	45	44	D7	E1	00	96	87	A1	I.. .E.9ED.....
000140	05	35	25	26	16	A4	EF	EF	FC	77	7F	7A	6D	E3	7F	2C	.5%&.....w.zm..,
000150	BE	2E	00	84	E4	2D	94	39	59	A5	CB	9B	6A	1E	DC	D9	.....-.9Y...j...
000160	FE	8D	73	75	A0	7B	2A	C1	58	65	70	2C	D5	42	CE	EE	..su.{*.Xep,.B..
000170	FA	90	1F	55	26	9E	EF	CF	A4	05	1F	06	B2	60	F7	E2	...U&.....`..
000180	7A	8C	0A	78	6A	8C	5F	76	DB	6E	0B	6B	C2	17	F6	0D	z..xj._v.n.k....
000190	88	20	AA	24	38	00	50	4B	03	04	14	00	00	00	08	00	. .$8.PK.....

バイナリかるたワークショップ



コンテスト出場者のその後

■SECCON出場者 ⇒ 協賛企業に新卒採用

2012年2月 CTF 福岡大会（九州工業大学）

2013年4月 C社 新卒採用

マレーシアのCTF世界大会で優勝した日本人技術者を
協賛企業A社が自社のセキュリティ向上の目的のため
採用した過去の事例もあり （社会人 2012年）

日本のセキュリティのこれから

- 攻撃を受けた後に初めて対応を考える
  - では、もう遅い？
  - 「情報」は１度漏れてしまうと取り返せない性質
- CTF は攻防戦を含んだ実践的な体験場
  - 「攻撃」と「防御」と「監視」のスキルが必要
  - どのようなシチュエーションで攻撃されるのか
  - 具体的な攻撃の被害の影響について知る
    - OJTで経験を積むのは難しい（インシデント発生）
- 攻撃者よりも「先回り」して防御の対策をしたい（攻撃を知らなければ防御できない）

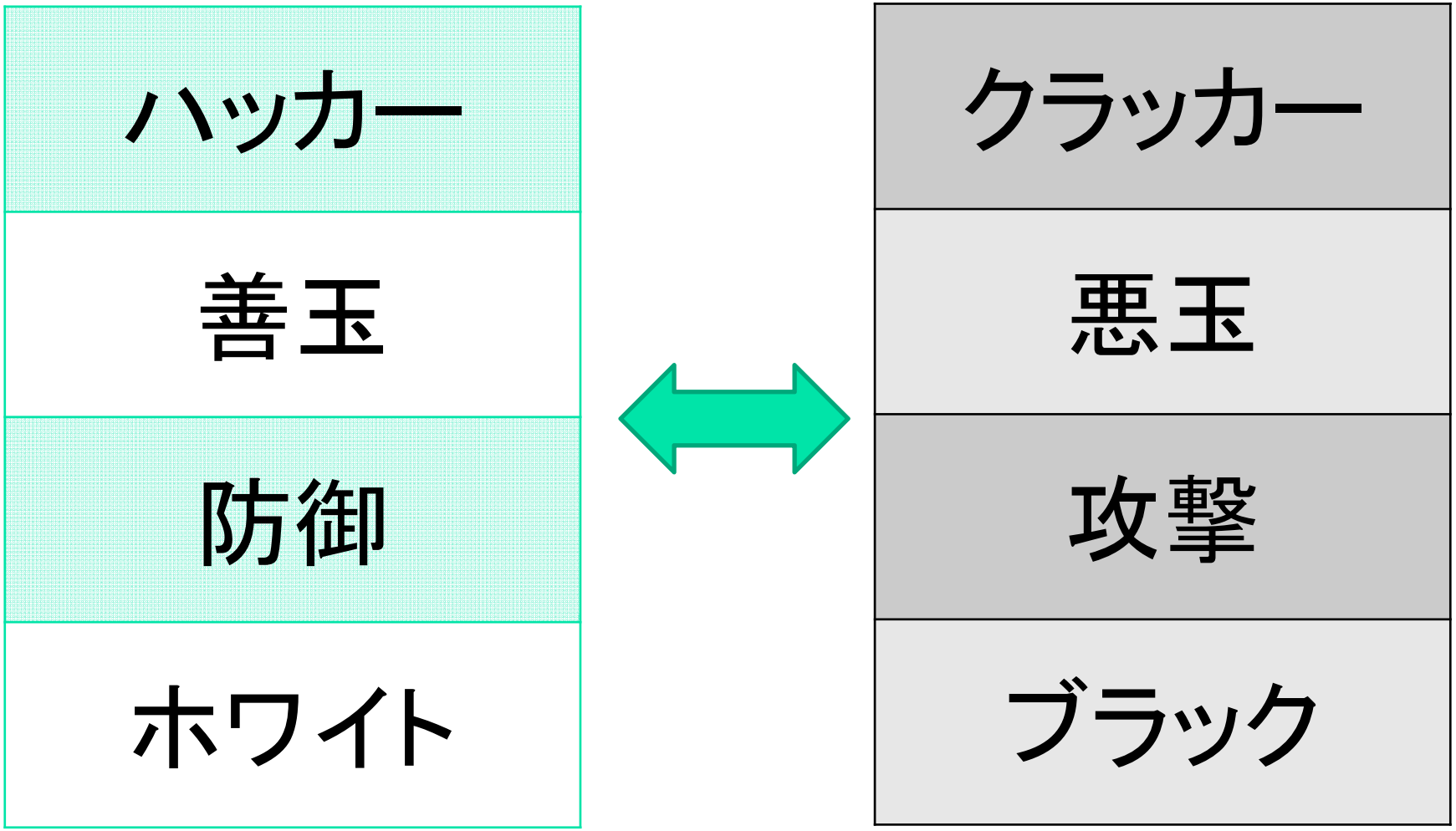
スポーツの世界をみると・・・

- 野球＆サッカーでは世界に通じる優秀な人材を輩出
  - 甲子園予選やアマチュアスポーツ大会など
    多くの地方大会が盛んに行われている
  - 全国の学校に野球グラウンド,サッカーコートがある
- 工業/電子系で見ると、日本国内には…
  - **技能五輪**、高専**ロボコン**、各種プロコン等
  - 競技プログラミングの土壌は既に根付いている
- **セキュリティはまだこれから**
  - 土壌を整備する段階
  - 各学校にクラブ活動ができて欲しい
    - 例：セキュリティ部活動、ハッカーサークル…

技能五輪(技能オリンピック)40種目

- 決められた時間内に正確に工作する競技
  - 熟練技術師のワザを若者に継承する場にも
    - 技術の空洞化を防ぐ（スキルトランスファー）

ハッキング技術の使い方



ハッカーの力を正しい道に導く

触媒としてのセキュリティコンテスト

- ITインフラの動作原理・原則を学ぶ
  - コンピュータ・インターネットの仕組み
  - トラブルが起きた時の問題解決能力
- ハッカーになるためには？
  - 人から一々教えられてなるものではない
  - 歴史を知り先代の技術を会得し、越える
  - 自分でセキュリティを学ぶ場を提供する
    - セキュリティコンテスト SECCON の実施
    - チーム結成による地域コミュニティ促進