セキュリティの人材育成について

園田道夫

攻撃は絶えず

- 「2013年に発生した政府機関に対する攻撃は約508万件。設置したセンサーで検知した脅威の件数を取りまとめたもので、約6秒に1回の割合で発生していた。2012年度の約108万件から4.7倍へと急増し、2011年度の66万件と比較すると、約7.7倍の水準に上昇した。」
- http://www.security-next.com/050390

最近の被攻撃事例

標的型攻撃でマルウェア感染、個人情報が流出 – JETRO	2015/02/20
朝日新聞子会社に海外から不正アクセス – 購読者情報の流出については調査中	2015/02/20
「MongoDB」を探索する不審アクセスが増加	2015/02/24
マルウェアで金融機関に侵入、ATM乗っ取りや不正送金 – 被害は10億ドル超か	2015/02/19
世界女子カーリング大会のサイトが改ざん – 閲覧でマルウェア感染の可能性	2015/02/18
NASが踏み台となりスパム10万件を配信 – 首都大学東京	2015/02/03
Flash Playerへのゼロデイ攻撃 – 人気動画サイト経由で誘導 – 1月中旬ごろより発生か	2015/02/03
三菱東京UFJ銀を騙るフィッシング –「個人情報漏洩が起きた」と騙す手口	2015/01/23
朝日新聞のPC17台がマルウェア感染 – 11月より情報流出か	2015/01/20
女子プロゴルフ協会のサーバに不正アクセス – 選手や記者の写真データが流出	2015/01/19
釜石の老舗料理店に不正アクセス – プログラム改ざんでカード情報流出	2015/01/16
ゲーム開発用サーバに不正アクセス、DoS攻撃の踏み台に – KADOKAWA	2015/01/15

http://www.security-next.comより引用

今もなおSQLi

- 「不正アクセスによるお客様の情報流出に関するお知らせとお詫び」2013年6月
  - http://www.first-jp.com/articleinfo/detail.php?id=360
  - 「SQLインジェクションの脆弱性を利用したWEBアプリケーションの管理者権限の不正取得、不正取得された権限によるバックドアプログラムの設置、バックドアプログラムを利用したアプリケーションの改ざん痕跡が発見されました。」

多様な攻撃パターン

- 手法：何でもアリ
- 対象：誰でも狙われる
  - 「サーバーなどの管理者じゃないから」
  - 「重要な情報資産持っていないから」
  - 「ウチなんて狙われるはずないから」
- 「最弱のリンク」が狙われる
- ホットな脆弱性が狙われる

多様化は市場確立のおかげ

- 昔：クラッカーが仲間でなければ、ウイルスも作れなかった
- 今：クラッカーはウイルス作成ツール、攻撃ツールを作ってブラックマーケットで売り、犯罪者はそれを買って攻撃する
- ツールのサポートサービスもある
- ゼロデイ情報も高く売れる

SQLインジェクション判例

- SQLインジェクション脆弱性が原因でクレジットカード情報が漏洩した事件につき、ショップ側が開発会社を相手取り損害賠償請求の裁判を起こし、ショップ側が勝訴した
- 認められた脆弱性：
  - システム管理機能のIDとパスワードがadmin/password であった
  - 個人情報が記載されたお問い合わせログファイルの閲覧が可能（ディレクトリリスティングと意図しないファイル公開）
  - SQLインジェクション
  - クロスサイトスクリプティング
  - ログにカード情報が保存されていた
  - DBに保存されたカード情報にはセキュリティコードも含まれていた
- IPAのWebセキュリティコンテンツくらいのことはやっとけ（by裁判所）

http://blog.tokumaru.org/2015/01/sql.htmlより引用

セキュリティ人材の質と量の不足

- IT（ICT）人材：106万人（SE80万人）
- 情報セキュリティ人材：26.5万人
  - 質的不足：16万人
  - 26.5万人ではまだ8万人程度ニーズを満たせていない

- なぜ足りないのか？

教育や進路の問題

- 教科「情報」のセキュリティ濃度？
- トレーナーが居ない
- 試す場が無い
- 動機付けもない
- おもしろそうだと気づいていても、乗り出せない
- 待遇もあまり良くない（これまでは）

足りないセキュリティ人材

- 足りないセキュリティ人材とは？
  - 経営型
  - セキュリティを知るIT人材

経営型セキュリティ人材

- 現状：予算上の制約があるがゆえに情報セキュリティ対策のために必要な資源を確保できていない
- 現状：新しい攻撃手法に対する理解が無い、浅い
- →起きている事象（サイバー攻撃等）を把握し、必要な予算をつける権限と眼力を持つ人材
- セキュリティリスクも経営リスクの一つ

セキュリティを知るIT人材

- 現状：次々襲い来るID,パスワード、データベース個人情報狙い、ウイルス植え付けなど
- →「情報セキュリティに関する知識・経験を含めてIT全般に関して基礎的な能力を有している」現場対応力を持つIT人材（notセキュリティ専門家）

セキュリティの専門家

- 引き抜き合戦（笑）
- →新しい脅威に対抗し得る、新たな対策を創造する人材が不足
- →研究的素材を現場に落とし込める人材が不足
  - 研究は存在するが、実装されていない（死屍累々）
  - テストデータも「独自」というのが多い…

大学の試み

- 早稲田大＋NTT「サイバー攻撃対策講座」
- 東京電機大CySec
- 北陸先端大＋NEC
- 奈良先端大
- enPiT
- 会津大＋シマンテック
- （SFC）
- 名古屋大
- 立命館大＋京都府警
- 和歌山大＋白浜危機管理コンテスト
- 情報セキュリティ大
- 筑波大
- 新潟大
- 九州大（一般講座として⇒専門講座）
- 長崎県立大（セキュリティ学科新設）
- サイバー大学もよろしくお願いします

Capture The Flag

- グループ対抗旗取り合戦（子供の遊び）
- サーバーに「旗を立てる」攻防戦
- 攻防の部分練習：クイズ戦

防御・解析と攻撃技術の両方を学ぶ実践的な場

- DEFCON（アメリカ：本家）
- pCTF（アメリカ）
- ghost in the shellcode（アメリカ）
- CSAW CTF（アメリカ）
- CODEGATE（韓国）
- Hacker’s Dream（韓国）
- secuinside CTF（韓国）
- HITCON（台湾）
- HITB CTF（オランダ,マレーシア）
- RuCTF（ロシア）
- PHDays CTF（ロシア）
- Nuit De Hack（フランス）
- PoliCTF（イタリア）
- ENOWAR（ドイツ）
- rwthCTF（ドイツ）
- OWASP CTF（世界各国）
- 他多数

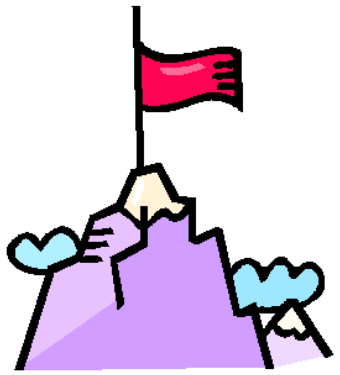
攻防戦

- 自分たちの脆弱なサーバーを破られないように運営する
- 他チームの脆弱なサーバーを攻める

フェイズ	必要な知識・スキル
守り：脆弱性解析	ファイル解析、ソフトウエア解析、メモリ管理、Webアプリ
守り：運用監視	ログ解析、パケット解析、侵入検知、攻撃妨害、フォレンジックス
攻め：脆弱性攻撃	ファジング、バッファオーバーフロー、Webアプリ攻撃、シェルコード作成

King of the hill形式

- 攻防戦と同じスキルセットが必要
- まず旗獲りを目指す
- 旗を獲ったら他のチームが旗を獲れないように妨害・防御する
- 旗獲りによる得点と、サービス（旗）維持による得点（単独もしくは複数で分け合う）を競う



クイズ戦

- 攻防戦の部分練習
- カテゴリーは多様：
  Web、パケット解析、ファイル解析、OS、ハードウエア、フォレンジックス、暗号、トリビアなど
- DEFCON予選、SECCON予選等、採用するCTF多数

世界のCTF分類（2014）

形態	採用大会
攻防	DEF CON CTF、RuCTFE2014（online）、HITB2014KUL Capture the Flag: Age of Extinction、VolgaCTF Finals、Nuit du Hack CTF Finals、PHD Finals、RuCTF Finals（計7大会）
King of the hill	SECCON Final、No cON Name CTF Finals
Hack quest	NorthSec
クイズ	31C3、Ghost in the Shellcode Teaser 2015、SECCON、9447、CSCAMP Finals、Defcamp Finals、CSCAMP Quals、CSAW Final Round、QIWI、Hackfest、MalCon、Hack.lu、UConn CyberSEED Competition、Defcamp Qualification、ASIS Finals、MalCon Quals、if(is)、Sharif University Quals、CSAW Qualification Round、CSAW Qualification Round、WaspNest CTF – AppSecUSA、No cON Name CTF Quals、HITCON、APAIUT-CERT Quals、OpenCTF、SECUINSIDE Finals、Pwnium、HitbSecConf、DEF CON Qualifier、ASIS Quals、NotSoSecure、PlaidCTF、Nuit du Hack Quals、Codegate Finals、VolgaCTF Quals、backdoorCTF、Insomni ‘hack、RuCTF Quals、DEFKTHON、Boston Key Party、Codegate Preliminary、RootedArena、Olympic Sochi、PHD Quals、HackIM、Ghost in the Shellcode2014、Break In、Ghost in the Shellcode Teaser 2014（計50大会）

注：http://ctftime.orgに登録された大会で2014年開催のもの

比較表

形態	メリット	デメリット
攻防	技の総合デパート 応用力、実戦経験	ワヤになりがち プレイヤーvs運営
King of the hill	トラブル少なめで プレイに専念 防御、妨害という視点 応用力、実戦経験	知恵比べ、ハックの余地は狭まる
クイズ	入門向き 実施規模のコントロールが容易 課題復習向き	実戦経験にはなりにくい？

日本のCTF、コンテスト

秋の大運動会(終了)	オープン	日本最初のCTF,攻防戦
セキュリティスタジアム(終了)	オープン	運動会の後継、攻防戦
SecSunbath	オープン	錦糸町ローカル(笑)、攻めオンリー
白浜情報危機管理コンテスト(2006～)	学生	専守防衛
Hardening(2013～)	オープン	専守防衛
MWS cup(2008～)	オープン	情報処理学会、マルウェア解析
セキュリティキャンプCTF(2010～)	学生	四日目の演習総仕上げ
SECCON(2012～)	オープン	CTF+コンテスト
オンラインCTF	オープン	多数

その昔のCTFは・・・

- フルパッチOS入りボックスを渡されてよーいどん！で脆弱性を探していた
  - 今はそんなに簡単には見つからない？
- pwn2own＠CanSecWest（http://cansecwest.com/）はガチのブラウザ脆弱性探しコンテスト
  - ガチのポリシーは難しい＠google離脱事件
- 会津の医療系ソフトウエアハックコンテスト（http://health2con.jp/hackathon/）
  - ガチでも良いよ！という対象を探すのが大変

pwn20wn@Japan

- Webブラウザのガチ脆弱性発掘コンテストが日本でも開催（初開催）
- 賞金総額3000万円
- http://www.itmedia.co.jp/enterprise/articles/1309/13/news044.html
- 標的となる端末は、「Nokia Lumia 1020」（Windows Phone）、「Microsoft Surface RT」（Windows RT）、「Samsung Galaxy S4」（Android）、「Apple iPhone 5」（iOS）、「Apple iPad mini」（iOS）、「Google Nexus 4／7／10」（Android）、「BlackBerry Z10」（BlackBerry 10）。エントリー登録の際にこの中から自分が挑戦する対象を選ぶ。OSのバージョンなどは登録者との間で調整する。

cybozu.com Security Challenge

- 賞金300万円（評価ポイントに応じて）
- 2013 年 11 月 11 日 午前 11 時 11 分 ～ 11 月 25 日 午後 6 時
- http://2013.seccon.jp/cybozucom-security-challenge.html
- お客様がご利用中の環境とは別の、コンテスト専用の検証環境にて、オンラインで実施
- サイボウズのクラウドサービスに存在する未知の脆弱性を見つけ出す能力を競います。参加者が脆弱性を検出し、脆弱性として認定されると、評価ポイントを手に入れます。より多くの評価ポイントを取得した参加者が、優勝者となります。

cybozu.com Security Challenge 結果

開催期間	2013年11月11日～ 11月25日
申し込み人数	95名
参加人数	75名
脆弱性の報告者	14名
発見された脆弱性	19件

cybozu.com Security Challenge結果順位

順位	名前	評価ポイント	報奨金	賞金	合計獲得賞金
1	Masato Kinugawa	43.5	¥522,000	¥516,960	¥1,038,960
2	@ren_hx	37.9	¥454,800	¥229,760	¥684,560
3	ビバップ	36.8	¥441,600	¥114,880	¥556,480
4	niwasaki	27.1	¥325,200		¥325,200
5	bbr_bbq	11	¥132,000		¥132,000
6	tkishiya	6	¥72,000		¥72,000

http://developer.cybozu.co.jp/tech/?p=6911より引用

cybozu.comバグハンター合宿

- http://togetter.com/li/704143
- 2日で53件見つかりました
- 最初は牽制、最後は協力＆和気藹々
- 技術や知見の共有
- http://itpro.nikkeibp.co.jp/atcl/column/14/346926/091700055/

バウンティプログラム

プログラム	プログラム内容
bugcrowd	93。1万人登録。平均241ドル、最高額は13500ドル。他にプライベートペネトレなども有り
HackerOne	パブリック73。
CrowdCurity	パブリック71。
Securiteam	ブローカー仲介。100件実績有り。5000～10万ドル

http://www.atmarkit.co.jp/ait/articles/1408/29/news011_2.htmlなどによる。プログラム数の数字は現在のもの。

SECCON 2012 開催実績

- 学生限定（Challenge Japanあったし）

2012/02	福岡大会
2012/05	つくば大会
2012/11	奈良大会
2012/12	横浜大会
2012/02	全国大会

参加チーム数は延べ38チーム、参加者数は延べ160人。

SECCON2013開催実績

	開催日程	開催地域	チーム数	参加人数	会場	併催コンテスト・講習会
1	8月22日～23日	関東（横浜）	100	100	パシフィコ横浜（CEDEC CHALLENGE)	早押しクイズ、バイナリかるた等
2	10月5日～6日	九州（福岡）	10	36	九州工業大学 情報工学部	スコアサーバ ハッカソン
3	10月5日～6日	甲信越（長野）	9	36	信州大学 工学部 SASTec	アセンブラ短歌コンテスト
4	10月20日	四国（香川）	9	28	香川大学 総合情報センター	CTF予選のみ開催
5	11月9日～10日	東北（福島）	10	36	會津藩校 日新館	CTFトライアスロン合宿（省エネ）
6	11月30日～12月1日	北海道（札幌）	10	32	札幌市産業振興センター	Wiresharkパケットコンテスト
7	11月30日～12月1日	北陸（富山）	11	43	インテックビル「タワー111」スカイホール	cybozu.com Security Challenge
8	12月14日～15日	関西（大阪）	14	53	マイドームおおさか	x86 Shellcoder's Challenge
9	12月14日～15日	東海（名古屋）	12	45	ウインクあいち	CTF入門、Python勉強会
10	1月25日～26日	オンライン予選	324	910	インターネット（情報セキュリティ大学院大学）	オンラインCTF予選（日本語）
		累計	509	1319		
11	3月1日～2日	全国大会（東京）	20	80	東京電機大学（東京千住）1号館 1F	King of the Hillによる決勝大会
12	3月1日～2日	カンファレンス	-	315	東京電機大学（東京千住）1号館 2F	各コンテスト優勝者による講演会

SECCON 2014 開催実績

	日程	開催大会	人数	会場	競技内容
1	6/29	CTF for GIRLS	70	六本木ヒルズ森タワー	女性向けCTFワークショップ
2	7/19	オンライン予選（日本語）	1267	インターネット	オンラインCTF予選（日本語）
3	8/6-8/7	cybozu.com バグハンター合宿	18	リフレフォーラム（東大島）	リアル製品の脆弱性発見
4	8/30-8/31	SANS NETWARS Tournament（連携大会）	100	秋葉原UDX	ワークショップ＋CTF大会
5	9/2-9/4	SECCON 2014 横浜大会	51	パシフィコ横浜	CEDEC CHALLENGE
6	9/27-9/28	SECCON 2014 長野大会	47	信州大学工学部	DNS Security Challenge
7	10/22-10/24	MWS Cup 2014（連携大会）	84	札幌コンベンションセンター	マルウェア解析、攻撃解析
8	10/25-10/26	SECCON 2014 札幌大会	37	札幌市産業振興センター	ARP Spoofing Challenge
9	11/9	SECCON 2014 大阪大会	52	グランフロント大阪	x86 Remote Exploit Challenge
10	12/6-12/7	オンライン予選（英語・日本語）	2555	インターネット	オンラインCTF予選（国際化）
		小計	4281		
11	2/7-2/8	SECCON 2014 CTF 決勝大会	(96)	東京電機大学	King of the Hill形式の決勝戦
12	2/7-2/8	SECCON 2014 全国大会カンファレンス	(300)	東京電機大学	カンファレンス同時開催

※1. 他社主催の「CTF Tournament」東京CTF大会で優秀な成績を収めたチームに対して、SECCON全国大会のCTF決勝戦へご招待。
※2. 情報処理学会コンピュータセキュリティ研究会MWS組織委員会主催「MWS Cup 2014」の成績優秀チームと、SECCON成績優秀チームの人材交流のため相互招待。

入門！

- CTF For GIRLS
  - ワークショップ
  - 過去2回開催
- CTF for Biginners
  - 勉強会＋ミニCTF
  - 過去2回開催＋広島、横浜開催予定

コンテスト＋CTF

- 幅広い技術分野に長けた人にCTFに参入してきて欲しい！
- 従来CTFの技術知見だけでは勝てない≒セキュリティ技術者の得意分野、対応可能領域を拡大（その逆も）
  - プログラミング、システムやネットワークの構築、運用＋セキュリティ

コンテストいろいろ

- アセンブラ短歌
- Wiresharkパケットコンテスト
- スコアサーバーハッカソン
- Cybozu.com Security Challenge
- Shellcoder’s Challenge
- DNS Security Challenge
- ARP Spoofing Challenge

攻撃検知コンテスト

- 機械学習（に限らず）アルゴリズム、プログラムを持ち寄って競技
- 学習用データセットを事前公開
- 本番用データセット（3回戦）で学習能力、精度を競う
- 二回開催済み。これまでのテーマはSQLインジェクション攻撃

機械学習とセキュリティ

- 自然言語解析、画像認識、音声認識、文字認識などで応用が進む
- セキュリティ分野？
- 大量データとは無縁？
  ＞セキュリティ

検知エンジンを開発して参加

- 依拠する手法は何でも良い
- サーバーGET型はターゲットの文字列をWebサーバーからbodyでGET
  - ExcelVBAのI/F（サンプルプログラム）有り
  - サンプルプログラムのアーキテクチャ部分を書き換えるだけ
- ファイルI/O型VBAは攻撃リストのテキストファイルを置くだけ

第一回静岡大会結果

- 台風直撃につき、急遽オンライン参加も
- SQLiデータと正常が混ざったものを100件→検知→再学習を3サイクル

検知率

1	FGLCT	73%
2	Oosawa	71%
3	中央1	65%
3	kanatoko	65%
5	中央2	55%
6	kawaguchi	33%

最終成績

1	Oosawa	81.5pt
2	FGLCT	75pt
3	中央1	66pt
4	kanatoko	65pt
5	中央2	56.5pt
6	kawaguchi	35pt

第二回東京大会結果

- 前回同様対象はSQLi

検知率

1	FGLCT3	98%
2	FGLCT4	97%
3	FGLCT6	96%
3	FGLCT5	94%
5	FGLCT7	93%
5	Oosawa	93%
7	中央	92%
8	FGLCT2	65%
9	FGLCT1	35%

最終成績

1	Oosawa	2066pt
2	FGLCT6	2065pt

検知サンプルの例（攻撃）

```
%5DSELECT+CHR%2865%29%7C%7CCHR%2866%29%3B
%22SELECT%20%2A%20FROM%20dblink%28%27host%3Dput.your.hostname.here%20user%3Dsomeuser%20dbnam
e%3Dsomedb%27%2C%20%20%27SELECT%20version%28%29%27%29%20RETURNS%20%28result%20TEXT%29%3B
1--
UNION ALL SELECT ID, Username, Email FROM [User]WHERE ID = 1 AND ISNULL(ASCII(SUBSTRING((SELECT TOP 1
name FROM sysObjects WHERE xtYpe=0x55 AND name NOT IN(SELECT TOP 0 name FROM sysObjects WHERE
xtYpe=0x55)),1,1)),0)<89--
%5BSELECT%20%2A%20FROM%20Table1%20WHERE%20id%20%3D%20-
1%20UNION%20ALL%20SELECT%20null%2C%20null%2C%20NULL%2C%20NULL%2C%20convert%28image%2C1%29
%2C%20null%2C%20null%2CNULL%2C%20NULL%2C%20NULL%2C%20NULL%2C%20NULL%2C%20NULL%2C%20NUL
L%2C%20NULL%2C%20NULl%2C%20NULL--
UNION ALL SELECT CONCAT(login, password) FROM members
 query.php?user=1+union+select+benchmark(500000,sha1
(0x414141)),1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1
%2B%20%27test
%40SELECT%20substr%28%27abcd%27%2C%203%2C%201%29%20FROM%20dual%3B
'SELECT 0x50 + 0x45
%7EIF+EXISTS+%28SELECT+%2A+FROM+users+WHERE+username+%3D+%27root%27%29+BENCHMARK%28100000
0000%2CMD5%281%29%29
%60BEGIN+DECLARE+%40rt+varchar%288000%29+SET+%40rd%3D%27%3A%27+SELECT+%40rd%3D%40rd%2B%27+
%27%2Bname+FROM+syscolumns+WHERE+id+%3D%28SELECT+id+FROM+sysobjects+WHERE+name+%3D+%27ME
MBERS%27%29+AND+name%3E%40rd+SELECT+%40rd+AS+rd+into+TMP_SYS_TMP+end%3B--
|SELECT CHAR(0x66)
```

検知サンプルの例（正常）

>|aa| テキスト ||<
((テキスト))
>< テキスト ><
[tex:テキスト]
[uke:テキスト]
http://d.hatena.ne.jp/sonodam
mailto:vp5m-snd@asahi-net.or.jp
[niconico:sm22019321]
[google:テキスト]
[google:image:テキスト]
[google:news:テキスト]
map:x132.45y87.56(:map)
[map:テキスト]
twitter:sonodam:tree
[twitter:@hatenadiary]
[http://twitter.com/sonodam/status/390078520786825216:twitter:title]
[] はてな記法 []
[graph:id:テキスト:テキスト(:image)]
<!-- テキスト -->
<ins> テキスト </ins>
表'ここ10年の平均値'
'S Wonderful

Do Androids Dream of Electric Sheep?
M. Sonoda
’赤い夕焼け
₤2,200
30℃
√2
ゑゐもせず
ΓΔΘ
λ
ⓒMichio Sonoda
Ä
´音声記号類
Ű
対応する“ダブルクォート”
¦罫線引き文法¦
２ ｃ ｈ 強 調 文
A Select Employee Group is a business partner of The Tennessee Credit Union that secures credit union membership eligibility for its employees at no cost and without the administrative responsibility of starting up a credit union on its own.
Please insert coin. It's a credit of "HARM".
{"request_key": "Zkk46eYme", "real_owner": "3526", "ft": "request_carpflag", "method": "request_carpflag", "ct": "rsa"}

機械学習を応用中

- Exact Soft Confidence-Weight Learning(SCW)
- Confidence-Weighted Algorithm(CW)
- 主成分分析(PCA)
- Support Vector Machine(SVM)
- ゼータ関数の応用
- N-gram系列
- K-means法
- その他

- 1. Takeshi Matsuda: Solution Space of Non Negative Matrix Factorization and Consideration of Feature Extraction on Web Application Attacks, 2014 International Conference on Information Science, Electronics and Electrical Engineering, pp. 892-896 (2014)
- 2. Takeshi Matsuda: Feature Extraction of Web Application Attacks Based on Zeta Distribution, World Congress on Internet Security (WorldCIS-2013), CD-ROM (2013)
- 3. Takeshi Matsuda: Learning Support System Based on Stochastic Model and Real Data of Users, 2013 International Conference on Active Media Technology (AMT'13) (2013)
- 4. Takeshi Matsuda: Desingularization of Mixture Tetranomial Distributions and Its Application for the Detection of Web Application Attacks, The 13th International Conference on Mathematics and Applications (2013)
- 5. Takeshi Matsuda: Estimation of SQL Injection Attacks Based on Single Character, The 2012 International Conference on Applied and Theoretical Information Systems Research, CD-ROM (2012)
- 6. Takeshi Matsuda: On Upper and Lower Boundaries of Real Log Canonical Threshold and Free Energy, The 7th International Conference on Mathematics, Statistics and its Applications (ICMSA 2011), pp.226-235, (2011)

- (共著)
- 1. Takeshi Matsuda, Daiki Koizumi, Michio Sonoda: Cross site scripting attacks detection algorithm based on the appearance position of characters, 2012 International Conference on Communications, Computers and Applications (MIC-CCA), pp. 65-70 (2012)
- 2. Daiki Koizumi, Takeshi Matsuda, Michio Sonida: On the automatic detection algorithm of Cross Site Scripting (XSS) with the non-stationary Bernoulli distribution, 2012 International Conference on Communications, Computers and Applications (MIC-CCA)pp. 131-135 (2012)
- 3. Daiki Koizumi, Takeshi Matsuda, Michio Sonoda, Shigeichi Hirasawa: A Learning Algorithm of Threshold Value on the Automatic Detection of SQL Injection Attack, The 2012 International Conference on Parallel and Distributed Processing Techniques and Applications, Vol.2012-MPS-89 No.10, pp.1-6 (2012)
- 4. Takeshi Matsuda, Daiki Koizumi, Michio Sonoda, Shigeichi Hirasawa: Predictive distribution of SQL Injection attacks Detection Model, 11th World Meeting of the International Society for Bayesian Analysis 2012
- 5. Michio Sonoda, Takeshi Matsuda, Daiki Koizumi, Shigeich Hirasawa: Markov Chain Monte Carlo method Simulation of SQL injection attack detection, 11th World Meeting of the International Society for Bayesian Analysis 2012
- 6. Michio Sonoda, Takeshi Matsuda, Daiki Koizumi, Shigeichi Hirasawa: On automatic detection of SQL injection attacks by the feature extraction of the single character, Proceedings of the 4th international conference on Security of information and networks (SIN2011), pp.1722-1727 (2011)
- 7. Takeshi Matsuda, Daiki Koizumi, Michio Sonoda, Shigeichi Hirasawa: On Predictive Errors of SQL Injection Attack Detection by the Feature of the Single Character, Proceedings of The 2011 IEEE International Conference on Systems, Man, and Cybernetics, pp.1722-1727 (2011)

- 口頭発表(査読無)
- 1. 園田道夫, 松田健, 小泉大城, 趙 晋輝: 主成分分析を用いた分類器によるSQLインジェクション攻撃の自動検出法, FIT2013 第12回情報科学技術フォーラム, 第4分冊, pp.187-192 (2013)
- 2. 松田健: ゼータ分布を利用したSQLインジェクション攻撃の特徴抽出について, FIT2013 第12回情報科学技術フォーラム, 第1分冊, pp.183-184 (2013)
- 5. 園田道夫, 松田健, 小泉大城, 平澤茂一, 辻井重男: 攻撃文字列の特徴抽出とWebアプリケーションの自動検出へのアプローチ, 情報処理学会第74回全国大会講演論文集, pp.3-557-558 (2012)
- 6. 松田健,: SQLインジェクション攻撃自動検出支援モデルと予測誤差,"
- 情報処理学会研究報告. MPS, 数理モデル化と問題解決研究報告 2012-MPS-87(14), pp.1-6 (2012)
- 8. 園田道夫, 松田健, 小泉大城, 平澤茂一: 文字単位の特徴抽出によるSQLインジェクション攻撃検出手法について, 情報処理学会研究報告. CSEC, [コンピュータセキュリティ] 2011-CSEC-52(49), pp.1-7 (2011)

- 学生の研究指導(卒業研究を含む)による学会発表
- 3. 前田すみれ, 園田道夫, 松田健, 趙　晋輝: ゼータ分布を用いたSQLインジェクション攻悟方法について, 情報処理学会第76回全国大会 (2013)
- 4. 佐野綾子, 松田健, 園田道夫, 趙　晋輝: SQLインジェクション攻撃に含まれる文字の出現頻度とその関連性の解析による攻撃検出方法の提案, 情報処理学会第76回全国大会 (2013)

キャンプでCTFやってみた結果・・・

- 競技性による熱中度の向上
- 記銘効果
  - 問題＝感情と結びつけて記憶する
  - 相互補完的な教え合いによる記銘効果も
- 講義・演習の総仕上げとして最適
  - 「わかったつもり」の排除

ゲーミフィケーション

- 「課題の解決や顧客ロイヤリティの向上に、ゲームデザインの技術やメカニズムを利用する活動全般」

課題	クエスト、ミッション、ランキング、難易度設定など
報酬	バッジ、経験値、レベルアップ、クーポン、ポイントなど
交流	チャット、対戦、アバター、ソーシャル、アンケート、GMなど

ゲーミフィケーション

- 「課題の解決や顧客ロイヤリティの向上に、ゲームデザインの技術やメカニズムを利用する活動全般」

課題	攻守の対象：サーバーの脆弱性 謎解き、解析クイズなど
報酬	フラグ（の代わりのファイル）を置く、 得点など
交流	チーム内コミュニケーション、チーム 間交流イベントなど

金銭的評価は一定の効果しかない

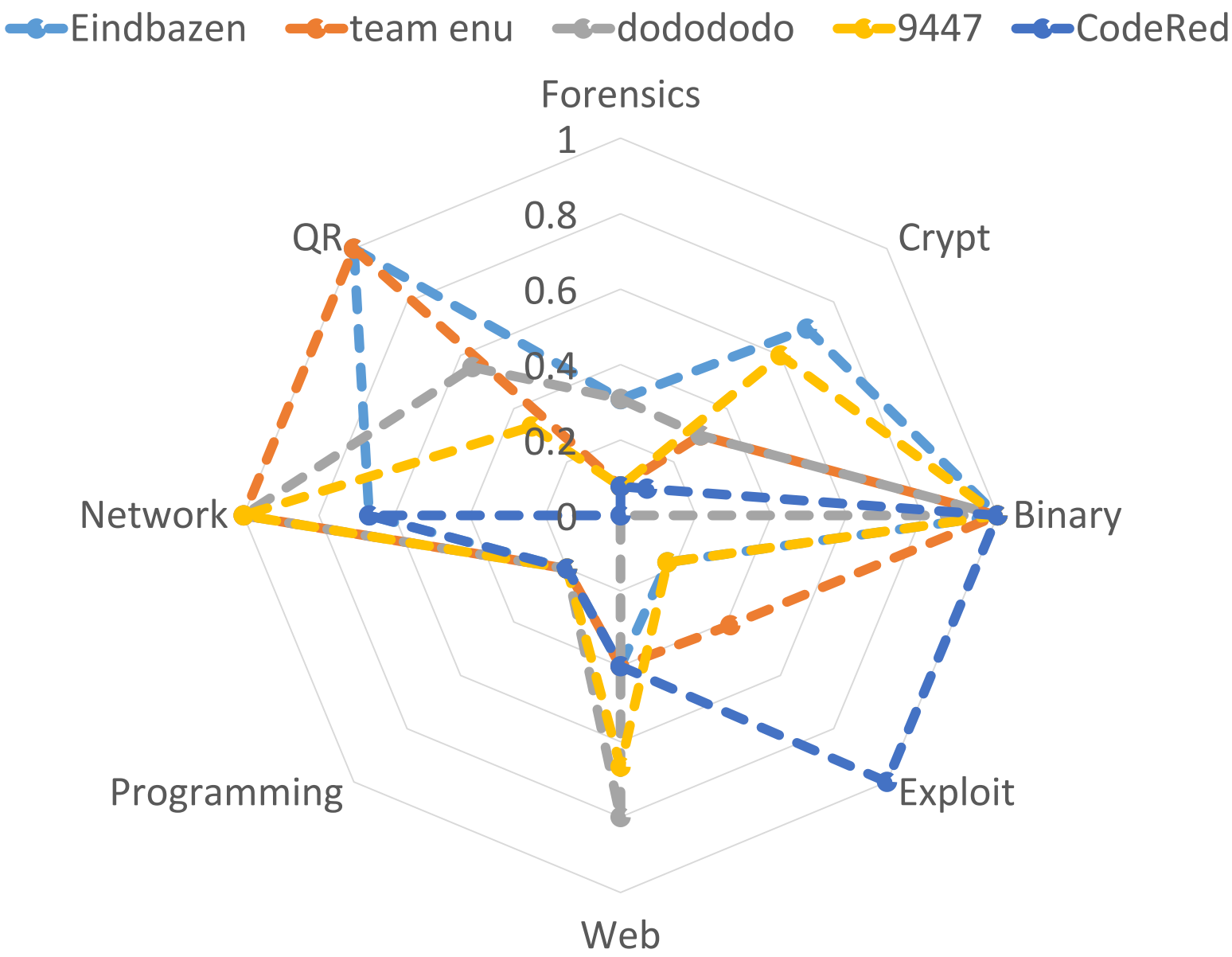
- 単純作業の場合、金銭的評価によってやる気が向上する
- 知的作業、複雑な作業の場合、やる気は一定以上向上しない
- ゲーム的要素を導入すると、勝手にのめり込み、勝手に工夫して効率を向上させ、勝手に必要な知見を学習する
- CTFで勝つために、評価されるために勉強・実験・工夫する！

攻めと守りに必要な能力

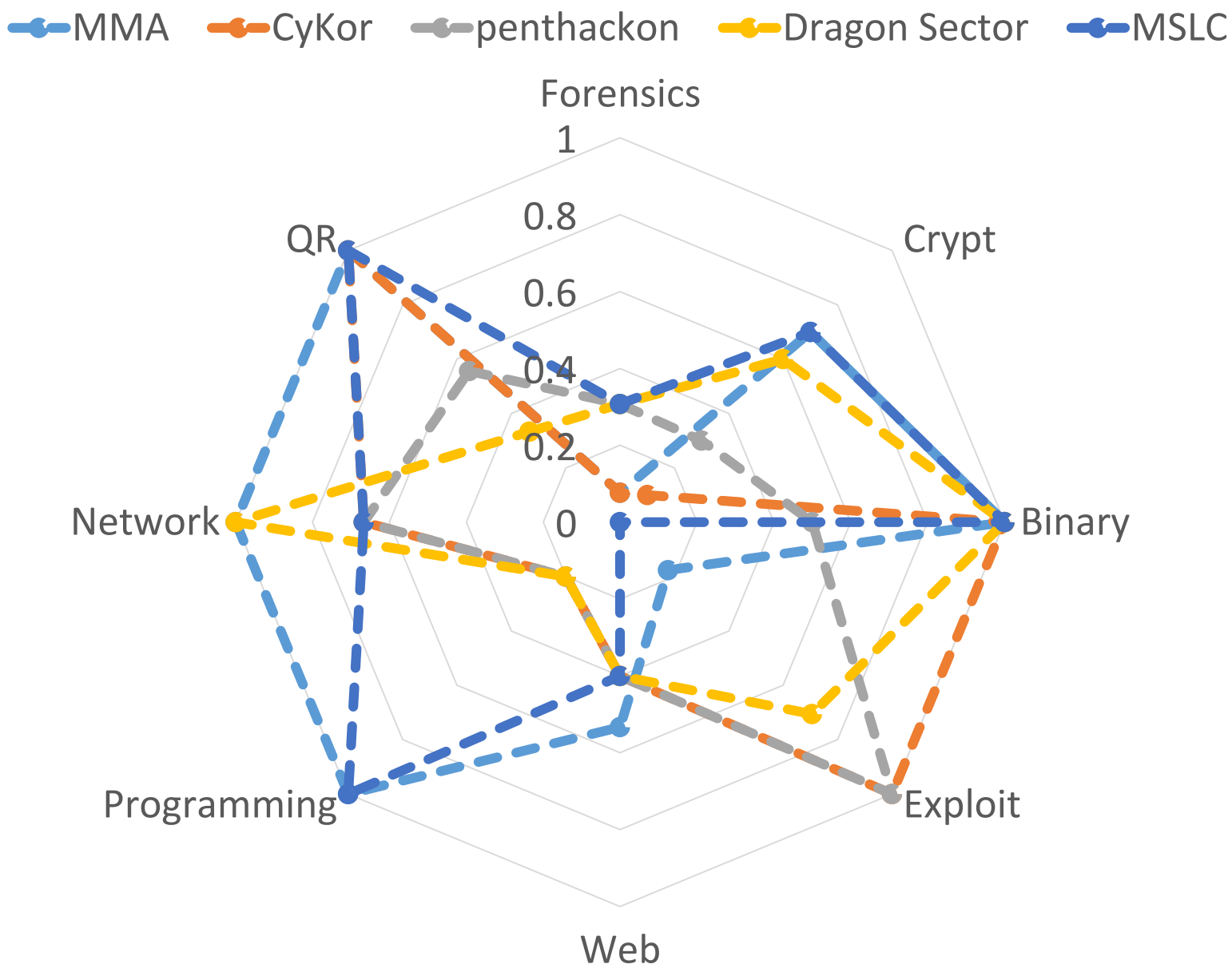
- テスト技法やソフトウエア解析技法を駆使し、脆弱性を突き止める能力
- 脆弱性を悪用するシナリオを考えつく能力
- 攻撃コードを作成し脆弱性を攻撃する能力
- メモリパッチ、侵入検知などの技法を用いて、脆弱性を暫定的に防護できる能力
- 脆弱性を修正する能力

現在の日本の弱点

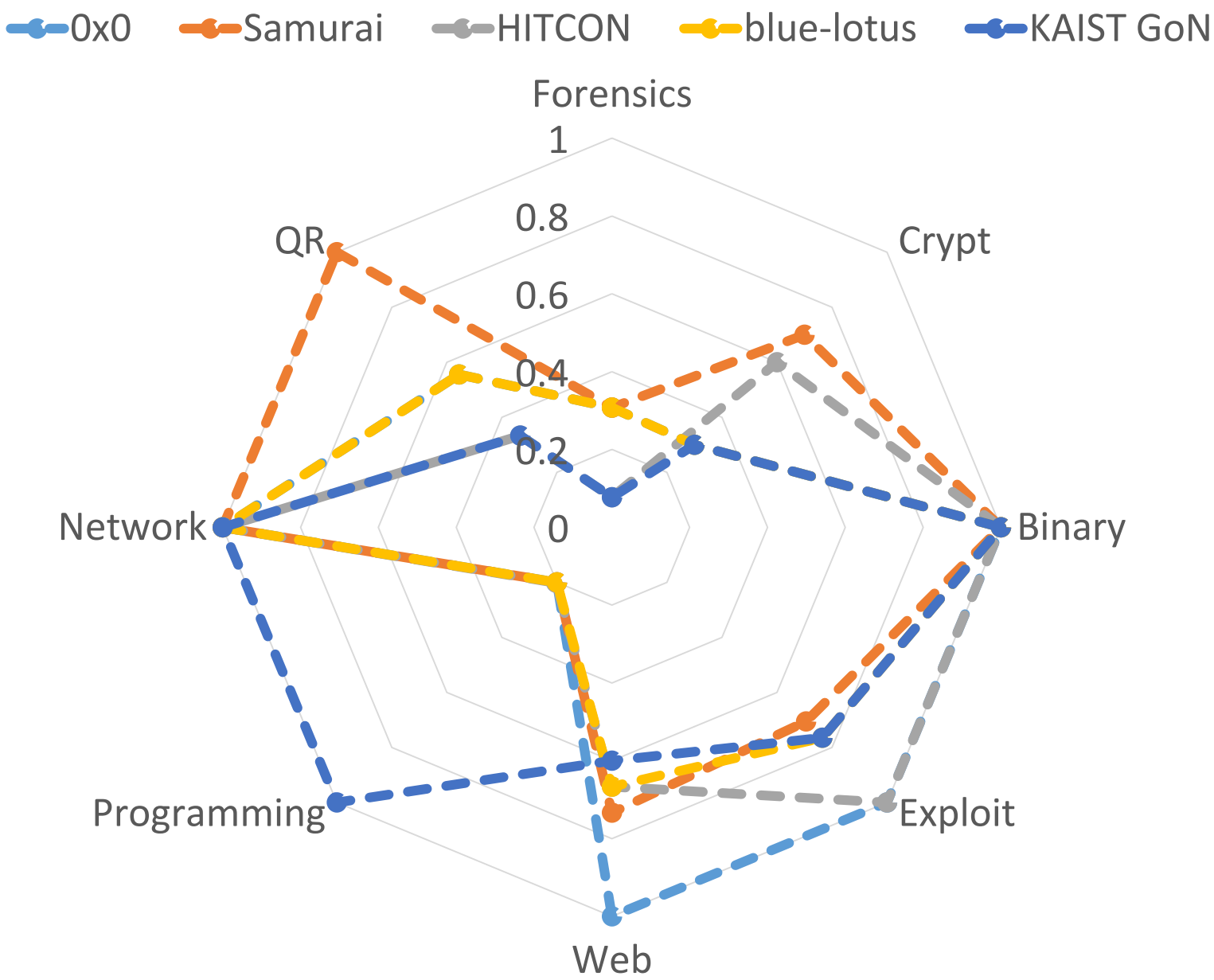
16位～20位


Eindbazen
team enu
dododododo
9447
CodeRed
Forensics
1
0.8
0.6
0.4
0.2
0
Crypt
Binary
Exploit
Web
Programming
Network
QR

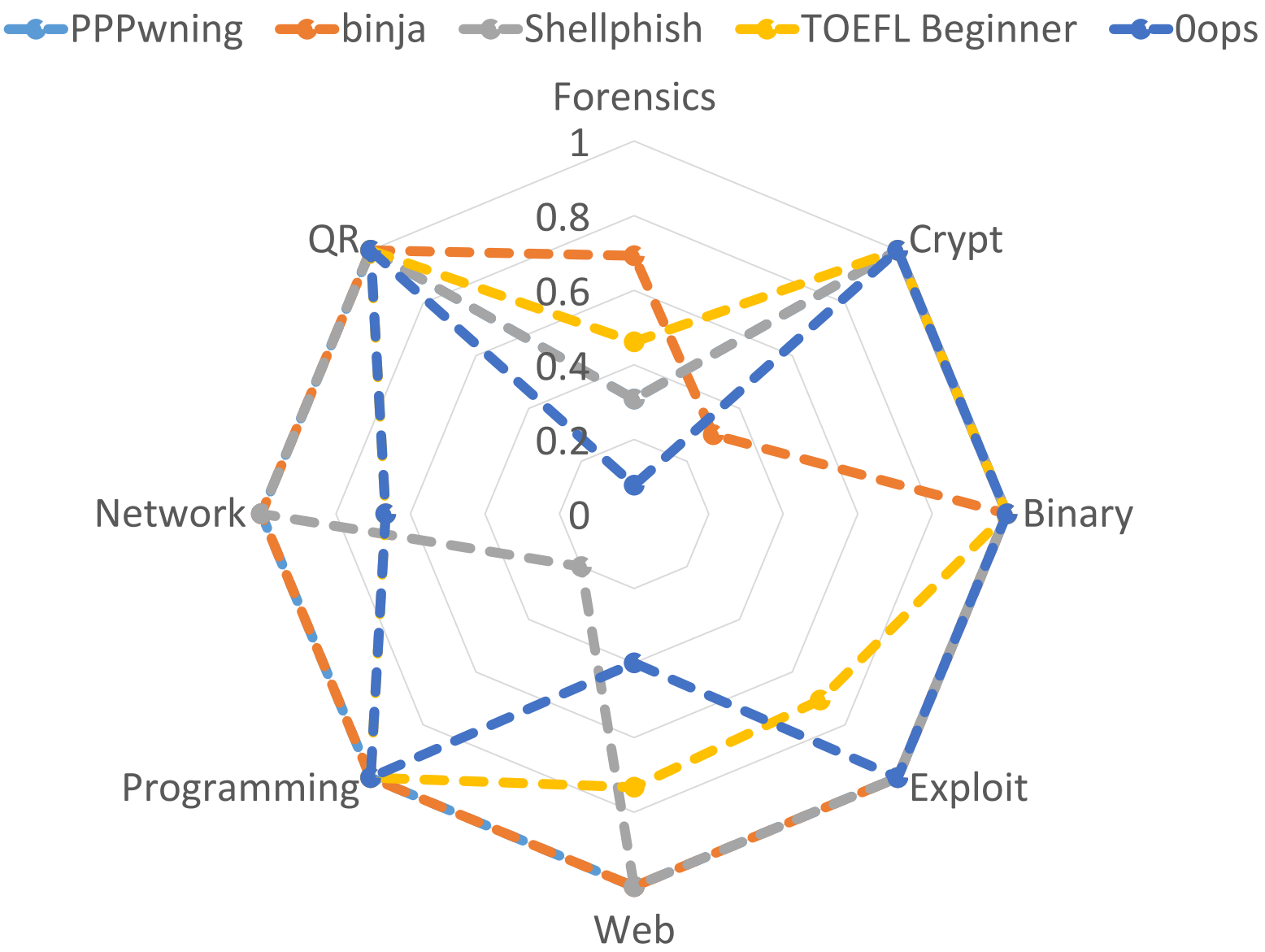
11位～15位


MMA
CyKor
penthackon
Dragon Sector
MSLC
Forensics
1
0.8
0.6
0.4
0.2
0
Crypt
Binary
Exploit
Web
Programming
Network
QR

6位～10位


0x0
Samurai
HITCON
blue-lotus
KAIST GoN
Forensics
1
0.8
0.6
0.4
0.2
0
Crypt
Binary
Exploit
Web
Programming
Network
QR

1位～5位


PPPwning
binja
Shellphish
TOEFL Beginner
0ops
Forensics
1
0.8
0.6
0.4
0.2
0
Crypt
Binary
Exploit
Web
Programming
Network
QR

弱点の克服

- ＝アメリカにいろいろ握られている現状を打破したい
- 自前で何とかできる環境、人材層を実現したい
- 攻撃者を先回りする発想を生み出したい
- そのためには攻撃の研究！

攻めと守りの切磋琢磨

- 攻撃を上回る防御、防御を上回る攻撃
  - WindowsOSなどの切磋琢磨の歴史
  - DEP、ASLR、NXビット等
  - 「攻め」も知らないと上回れない
- 攻撃側のコストを上げるには？
  - ウイルス対策＝防御側のコストが高い
  - SQLインジェクション攻撃はツールでほいほい→SQL文特有の記号を特徴とすれば検知ほいほいで攻撃は大変になる

負け戦を逆転するために

- セキュリティ＠日本には今、良いプログラマーが居ない
- プログラマーにセキュリティを考えてもらう＝セキュリティ要素を劇的に採り入れることが可能
- 安全なものを作るためのフレームワーク、ツール、環境を作る
  - 教育よりも効果的でコストがかからない
  - IT現場は成果物を使いこなせればいい

経産省的人材像とはちょっと違う望ましい人材像

- IT的イノベーションを起こせる人材の発掘
  - セキュリティを学習しなくてもセキュアに
- 実践的な技術力を持った人材の育成
  - 将来ありうる、新たな攻撃に備える
- もちろん予算は要るけど、イノベーションに予算は付いてくる（楽観

機械学習、ビッグデータ解析

- 機械学習を使う、人工知能を援用するにしても、まだまだ人間が経験知を言語化し、アルゴリズムに落とし込む必要がある
  - ≒人間のフィルタが無ければ望ましい動作ができない
- 防御だけでなく、攻撃の経験知、経験則も必要
- セキュリティは特徴づけられていない分野
- 職人＋機械学習が最強

おわり

Thanx for photos by tessy, Yuichi Hattori, Hiroshi Koide, Tomohiro Hanada@SECCON.