セキュリティの人材育成について

園田道夫

自己紹介

- サイバー大学IT総合学部専任教授
- 国立高知工業高等専門学校客員教授
- 情報通信研究機構（NICT）セキュリティ人材育成研究センター長
- 独立行政法人情報処理推進機構（IPA）研究員
- NPO日本ネットワークセキュリティ協会（JNSA）研究員
- 経済産業省、IPAなど主催、セキュリティ（＆プログラミング）　キャンプ企画、講師、実行委員、トラックリーダー等
- 白浜サイバー犯罪シンポジウム危機管理コンテスト審査委員
- 2008年、経済産業省商務情報政局長表彰を受賞
- SECCON実行委員(事務局長)
- 2012年、SecureAsia@Tokyo 2012にてAsia-Pasific Information Security Leadership Achivements(ISLA) Senior Information Security Professional として表彰
- 会津IoTハッカソン審査委員
- 主な関係書籍「ブラウザハック」「ファジング」「ハニーネットプロジェクト」「実践パケット解析第一版」「実用SSH第二版」「暗号技術大全」「Snort2.0侵入検知」「アクセス探偵IHARA」「アクセスガール明日香危機一髪」「企業情報ネットワークの保護管理」「Winnyはなぜ破られたのか」等

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

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。」

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

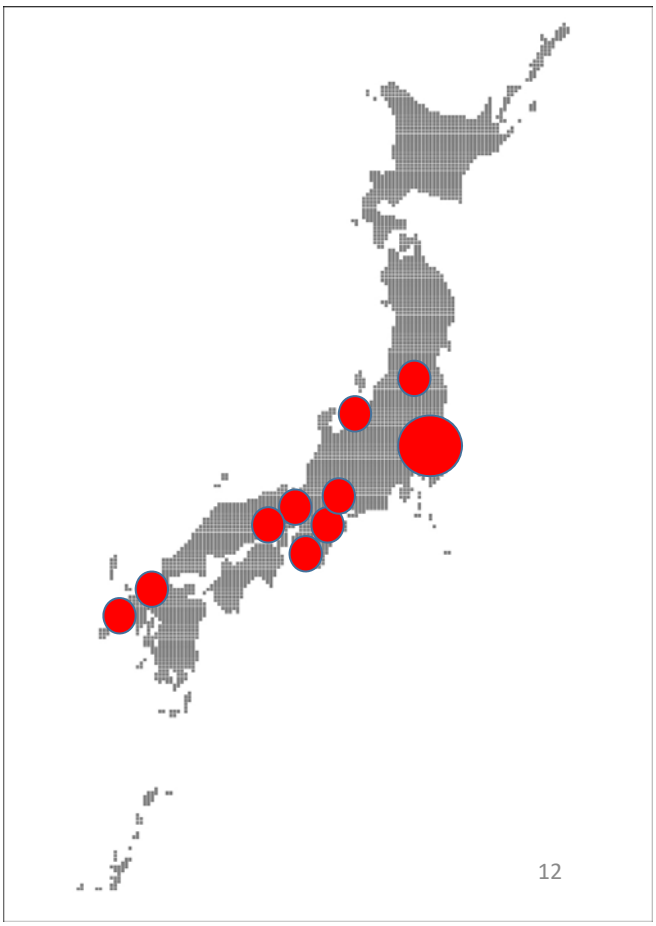
- 現状：次々襲い来るID、パスワード、データベース個人情報狙い、ウイルス植え付けなど
- →「情報セキュリティに関する知識・経験を含めてIT全般に関して基礎的な能力を有している」現場対応力を持つIT人材（notセキュリティ専門家）

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
- 神戸大
- 兵庫県立大（カーネギーメロン大）
- 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

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

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

pwn2own@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。

セキュリティ・キャンプ

- 2004年スタート
- 主催：セキュリティ・キャンプ実施協議会、情報処理推進機構
- 共催：経済産業省、後援：文部科学省
- 8月中旬に幕張にて開催、4泊5日の合宿研修
- セキュリティどっぷり
- 行き帰りの旅費、宿泊費、食費タダ！
- 超一流の講師陣

NICT　CYDER演習

- 1.5日の机上演習＋StarBED解析
- 全国11カ所30回＋中央省庁向け10回
- 1300人以上が参加
- レベル、規模を拡充予定

終