

脆弱性診断士に!!!  
俺はなるっ!!!!

JNSA ISOG-J WG1リーダー  
株式会社トライコーダ  
上野 宣



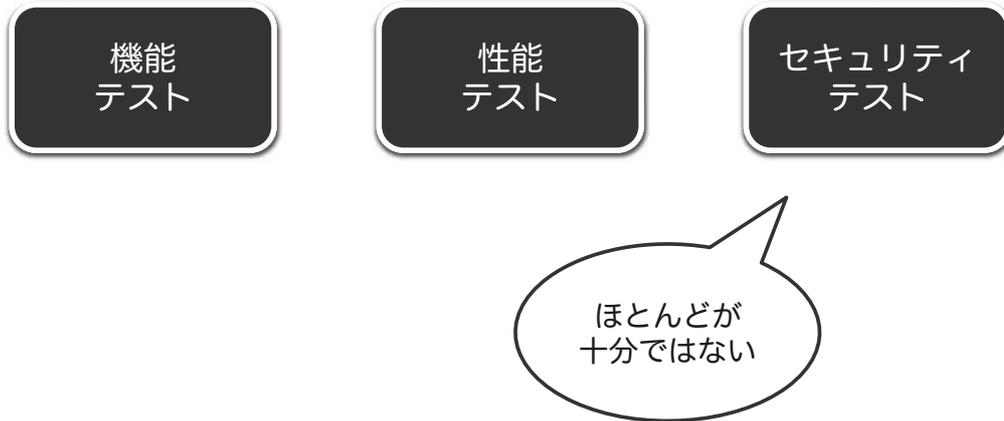
## 上野 宣 : Sen UENO

- 株式会社トライコーダ 代表取締役
  - 企業や官公庁向けにサイバーセキュリティ教育やトレーニング、ネットワーク/Webアプリケーション脆弱性診断などを提供
  - 奈良先端科学技術大学院大学で情報セキュリティを専攻、eコマース開発ベンチャーで東証マザーズ上場などを経て、2006年に株式会社トライコーダを設立
- 独立行政法人情報処理推進機構(IPA)セキュリティセンター研究員
- 情報セキュリティ専門誌 ScanNetSecurity 編集長
- OWASP Japan Chapter リーダー
- JNSA ISOG-J セキュリティオペレーションガイドラインWGリーダー
- セキュリティキャンプ講師主査
- SECCON 実行委員、Hardening Project 実行委員 など
- 主な著書
  - HTTPの教科書、図解HTTP (簡体字)
  - めんどくさいWebセキュリティ
  - 今夜わかるシリーズ (TCP/IP, HTTP, メール)
  - 平成27年度情報セキュリティスペシャリスト試験によくできる午前・午後問題集、他多数



# Webの世界は？

”十分な”テストが行われているのか？



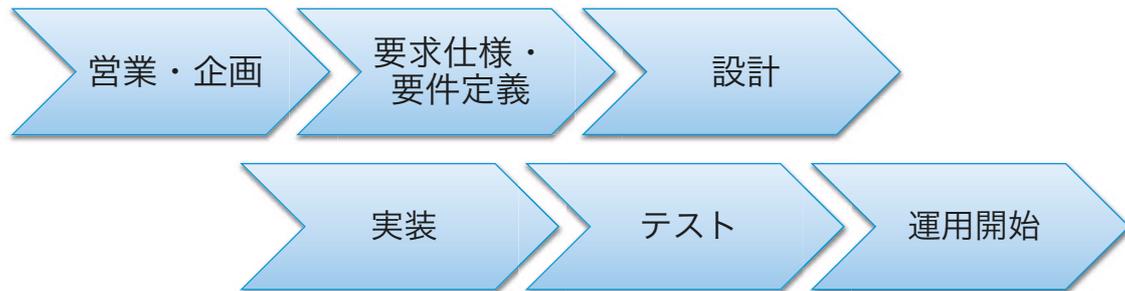
# Webサイト上には



盗まれても、破壊されても、  
改ざんされても、妨害されても困るはず

# Webサイトの開発

- セキュリティ要件（たぶん？あるはず）
- そのセキュリティ要件通りか確認するのがテスト（脆弱性診断）の工程



(c) 2015 Tricorder Co.Ltd.

5

## 開発の工程は十分だろうか？

- ちゃんとテスト分の工数は足りているか？テストにコストを支払っているか？

### 開発に必要な工数の目安（割合）

要求仕様作成、設計	1/3
実装（コーディング）	1/6
単体テスト	1/4
統合テスト	1/4

時間も予算も  
足りないって？  
何を削ろうか



参考：『人月の神話—狼人間を撃つ銀の弾はない (Professional Computing Series)』

(c) 2015 Tricorder Co.Ltd.

6

## 開発者の多くは脆弱性診断ができない

- 攻撃技術・脆弱性を知らない
- テスト方法を知らない
- テスト仕様書を作れない
- どこを診断して良いか判らない
- 脆弱性判定の基準が判らない
- 報告書の書き方が判らない



## 脆弱性診断はどうしてるの？

- **脆弱性診断サービスを提供する業者に外注**
  - コストは決して安くない
- **脆弱性診断の自動ツールを利用**
  - 自動ツールには得意分野と不得意分野があり、自動ツールだけでは完結しない
  - コストも決して安くない
- **開発者自身が実施**
  - 十分なスキルがある？

実施していない  
こともあるかも。

## 脆弱性診断サービスの問題点

### 顧客には品質の違いがわからない

- 各社の診断サービスには品質にばらつきがある
  - 特にWebアプリケーション脆弱性診断
- 自動ツールだけ？手動の品質は？
  - そもそも品質があるとか知らないかもしれない
- 利用者にはもっとわからない
  - 安全なWebサイトかどうか判別がつかない

## 脆弱性診断の品質は

### 会社で決まる？診断する個人で決まる？

- 診断技術は個人スキルに大きく依存する
  - 顧客からの指名買いがあることも



しかし、技術レベルの  
可視化が行われていない

# そこで

## 脆弱性診断士 (Webアプリケーション) スキルマップ

作りました！



## 脆弱性診断士 (Webアプリケーション) スキルマップ

- 脆弱性診断を行う**個人**の技術的な能力を具体的にすることが目的
- 「脆弱性診断士(Webアプリケーション)スキルマッププロジェクト2014」で作成
  - JNSA ISOG-JセキュリティオペレーションガイドラインWG(WG1)とOWASP Japan主催の共同ワーキンググループ
  - <http://isog-j.org/output/2014/pentester-web-skillmap-201412.pdf>

## 問題解決に必要なもの

- 品質の良いサービスが選べない  
→ **品質の良い脆弱性診断を選べる基準作り**
- 必要な技術や知識を明確にしたい  
→ **スキルマップ、シラバス**
- 技術力の向上や人材育成  
→ **ガイドライン**

## 脆弱性診断士

- 高い倫理を持ち、適切な手法で IT システムの脆弱性診断を行える者
- 求める技術や知識をスキルマップ化
- Webアプリケーションの脆弱性診断にフォーカスした内容



# 想定している利用用途

## 人事関連分野

- 採用基準、能力判定、人事評価基準、セキュリティエンジニアの人材育成

## 開発関連分野

- リリース前の要件、システムの品質向上

## 発注関連分野

- 入札仕様、診断サービス依頼先の選定

# 「脆弱性診断士」 ランク

## 2つのランクを定義

- Silver ランク
  - 脆弱性診断業務に従事する者が全員知って
  - おくべき技能
- Gold ランク
  - 単独で診断業務を行うために必要な技能



# 各ランクの詳細

	 <b>Silver</b>	 <b>Gold</b>
対象者像	<ul style="list-style-type: none"> <li>● 自社の Web アプリケーションの脆弱性診断（受入れ検査）を行う方</li> <li>● 脆弱性診断業務の従事を目指す方（学生など）</li> </ul>	<ul style="list-style-type: none"> <li>● Web アプリケーションの脆弱性診断（受入れ検査）を行う方</li> <li>● 脆弱性診断をサービスとして提供する業務に従事する方</li> </ul>
業務と役割	<ul style="list-style-type: none"> <li>● Gold ランクの者の指示の下、脆弱性診断を行う</li> <li>● 自社 IT システムの脆弱性診断を行う</li> </ul>	<ul style="list-style-type: none"> <li>● 脆弱性診断業務を管理し、診断方針の決定、作業指示の実施、診断結果の精査および評価を行うことができる</li> <li>● 脆弱性診断の報告書を作成し、技術的な説明ができる</li> </ul>
期待する技術水準	<ul style="list-style-type: none"> <li>● IT システムを診断する上で（最低限）必要な技術や知識を保有</li> </ul>	<ul style="list-style-type: none"> <li>● 脆弱性診断サービスを提供するのに必要十分な技術や知識を保有</li> </ul>

# スキルマップ

分野	大分類	中分類	小分類	Silver	Gold	備考	
基礎知識（技術）	標準的なプロトコルと技術	プロトコル	IP	○	○		
			TCP	○	○		
			UDP	○	○		
			DNS	○	○		
			SSL/TLS	○	○		
			Web Socket	×	○		
			IPv6	×	○		
		名前解決	トップレベルドメイン(TLD)	○	○		
			ICANN	×	○		
			DNS /etc/hosts	○	○		
			レジストラ	×	○		
		文字コード		○	○		
		メール		○	○		
		セキュリティ技術	暗号	共通鍵暗号		○	○
					○	○	
	暗号学的ハッシュ				○	○	
					○	○	
	PKI		認証局	○	○		
			証明書	○	○		
			認証	○	○		
ネットワーク	ファイアウォール		○	○			
	IDS/IPS		×	○			
	WAF		○	○			
認証		パスワード認証	○	○			

## 今後

- 今後はシラバス、ガイドラインを出す予定
- プラットフォーム診断も取組中
- 資格化できるかな？
  - 開発者が自分たちで診断ができる時代がくる
  - 診断会社のレベルが上がり、可視化できる
  - 入札時や発注時の要件として盛り込める