脆弱性診断士（Web アプリケーション）スキルマップについて

はじめに

近年、IT システムのさらなる普及に伴い、様々なシステムに対する攻撃に起因する情報漏えいや経済的損失などの被害が発生していることを受け、システムのリリース前に脆弱性の有無を調査する脆弱性診断を行い、問題点を修正するという脆弱性診断の一連の営みに関する重要性が高まっている。
脆弱性診断を行うためにはソフトウェアやネットワークなどの基本的な素養にはじまり、各種脆弱性診断ツールの使用手順や最新の技術動向へのキャッチアップなど、多岐に渡るスキルが必要とされる。
しかし、IT システムの中でも Web アプリケーションの脆弱性診断については、保有すべき具体的なスキルマップが関係者間で統一されていない。そのため、脆弱性診断を行う技術者やサービス事業者の技術力には差違が見られる。一方で、その差違は脆弱性診断サービスを利用する利用者には判りづらく、事業者も可視化することが難しい状況である。

日本セキュリティオペレーション事業者連絡会（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である「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」では、脆弱性診断を行う個人の技術的な能力を具体的にすべく、脆弱性診断を行う技術者（以下、脆弱性診断士）のスキルマップを整備している。
まず、脆弱性診断の中でも早急な整備が必要な領域は Web アプリケーションであるとして、「脆弱性診断士（Web アプリケーション）」 についてのスキルマップの作成を下記の方針に基づいて行った。

- 脆弱性診断業務に必要な技術的な能力を対象とする
- マネージメントスキルやコミュニケーションスキルは対象外とする
- 脆弱性診断士に必要なスキルを明確化する
- 特定の脆弱性診断ツールや環境に依存しないようにする
- 現在必要だと考えられる技術水準を基に作成する
- 脆弱性診断士が持つべきスキルの指標とするものであり、各社が提供する脆弱性診断サービスの品質については対象外とする

「脆弱性診断士」について

脆弱性診断士は、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であり、脆弱性診断士スキルマップで求める技術や知識を保有している者に対して与えられる呼称である。

脆弱性診断士の業務に係わる各分野で使用できるようにスキルマップを明確にした。以下のような分野/用途を想定しているがこれに限定するものではない。

- 人事関連分野の用途
    - 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
- 開発関連分野の用途
    - リリース前の要件、システムの品質向上
- 発注関連分野の用途
    - 入札仕様、診断サービス依頼先の選定

これらを通じて、脆弱性診断士の地位向上、待遇改善、給与向上につながることを目指している。また、脆弱性診断士が魅力ある職業として認知されることにより、セキュリティ事業を志す優秀な人材が増えることを期待しており、就職活動、教育活動を行なう上で基礎を規定する役割の一端を担うことも目指している。

「脆弱性診断士」区分

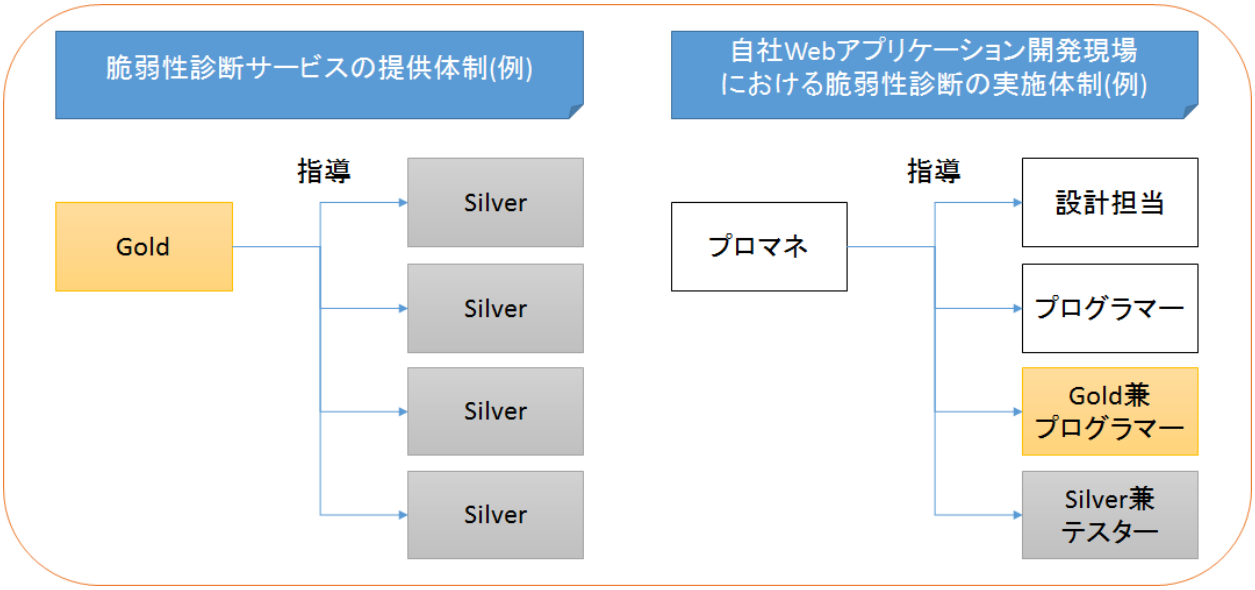
脆弱性診断の対象によって、脆弱性診断士に必要とされる技術、知識が異なるため、それぞれの対象をいくつかに分け、対象毎に脆弱性診断士を区分することとした。

脆弱性診断士(Web アプリケーション)

Web アプリケーション/Web システムに対する脆弱性診断を行う者を対象に「脆弱性診断士(Web アプリケーション)」という区分を設ける。
この脆弱性診断士の対象者像としては、Web アプリケーション/Web システムの脆弱性診断を必要とする者、Web アプリケーション/Web システムの開発者、運用者を想定する。

「脆弱性診断士」ランク

脆弱性診断士のランクを定義するにあたっては、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（ Silver ランク）と、単独で診断業務を行うために必要な技能（ Gold ランク）を定義した２つのランクに分けた。



Silver ランクは Gold ランクの者から指導を受けた上で診断サービスを提供する、もしくは、自社向けに脆弱性診断を実施するための必要スキルとして設定した。
Gold ランクは業務としての脆弱性診断サービスを提供するチームにおいて、最低限 1 名以上メンバーに加えるべきスキルとして設定した。

Silver

対象者像	• 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 • 脆弱性診断業務の従事を目指す方（学生など）
業務と役割	• Gold ランクの者の指示の下、脆弱性診断を行う • 自社 IT システムの脆弱性診断を行う
期待する技術水準	• 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

Gold

対象者像	• Web アプリケーションの脆弱性診断（受入れ検査）を行う方 • 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
業務と役割	• 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 • 脆弱性診断の報告書を作成し、技術的な説明ができる
期待する技術水準	• 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

脆弱性診断のスキルマップ

脆弱性診断士(Web アプリケーション)

スキルマップの構成は下表の通りである。詳細は別紙「脆弱性診断士（Web アプリケーション）スキルマップ」を参照のこと。

分野	大分類
基礎知識（技術）	標準的なプロトコルと技術
	セキュリティ技術
	WWW
	その他
基礎知識（脆弱性）	Web アプリケーションの脆弱性
	Web アプリケーションの動作環境への診断項目
基礎知識（診断業務）	診断前・準備
	診断実査
	診断実施後・アフターサポート
診断技術（自動診断ツール）	自動診断ツールの特徴
	ツール使用時の注意事項
	自動診断の準備
	実施の準備、設定
	スキャン実行
	診断結果の精査
	その他ツールの機能

診断技術（手動診断で使うツール）	手動診断補助ツールの機能
	手動診断の準備
	診断を効率化するツール
レポーティング・リスク算出	リスク算出方法
	報告書の種類
	報告書に記載する内容
法律	法律や犯罪
	診断時のルール・倫理
	セキュリティに関する基準

執筆者

- 上野 宣（ISOG-J WG1 リーダー、OWASP Japan Leader、株式会社トライコーダ）
- 国分 裕（ISOG-J WG1 サブリーダー、三井物産セキュアディレクション株式会社）
- 洲崎 俊（ソフトバンクモバイル株式会社）
- 山崎 圭吾（株式会社ラック）
- 吉田 聡（株式会社ラック）
- 亀田 勇歩（SCSK 株式会社）
- 小河 哲之（セコムトラストシステムズ株式会社）
- 岩井 基晴（NTT データ先端技術株式会社）
- 松本 悦宜（JPCERT/CC）
- 高橋 宗昭（日本アイ・ビー・エム株式会社）
- 今野 俊一（日本電信電話株式会社）
- 富居 姿寿子（日本電信電話株式会社）
- 池田 雅一（テクマトリックス株式会社）

レビュアー

- 日本セキュリティオペレーション事業者連絡会（ISOG-J）セキュリティオペレーションガイドライン WG (WG1) メンバー
  http://isog-j.org/
- OWASP Japan メンバー
  https://www.owasp.org/index.php/Japan
- 徳丸 浩（HASH コンサルティング株式会社）
  https://www.hash-c.co.jp/

改定履歴

- 2014 年 12 月 19 日 第 1.0 版リリース