Webアプリケーション脆弱性診断ガイドラインについて

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。

ISOG-J WG1とOWASP Japan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）のスキルマップと学習の指針となるシラバスを整備している。
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とシラバス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＆シラバス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とシラバスを明確にした。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

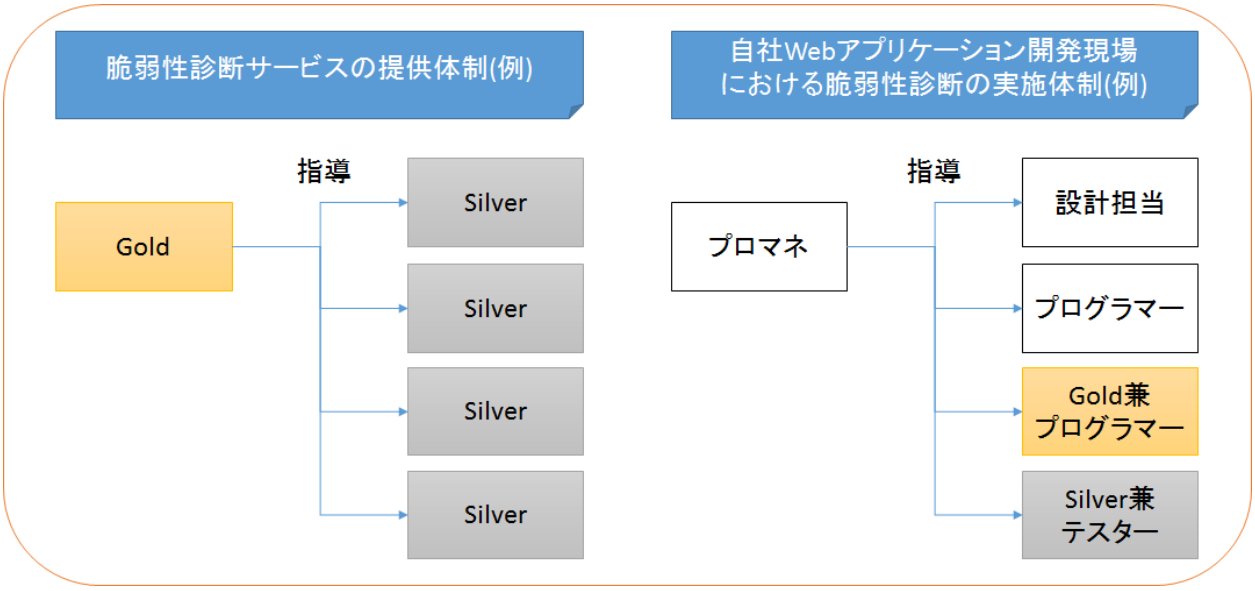
脆弱性診断の対象によって、脆弱性診断士に必要とされる技術、知識が異なるため、それぞれの対象をいくつかに分け、対象毎に脆弱性診断士を区分することとした。

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

「Webアプリケーション脆弱性診断ガイドライン」について

Webアプリケーションの脆弱性診断は、自動診断ツールを使った脆弱性診断だけでは十分な診断結果が得られないと本プロジェクトでは考えており、そのため手動診断補助ツールを使った手動診断を併用することが望ましいとしている。
しかし、手動診断は脆弱性診断士の経験やスキルによる診断能力の差違がある。そこで本プロジェクトでは、最低限必要な診断項目や手順を定義することで、一定レベルの手動診断による脆弱性診断を行うことができる「Webアプリケーション脆弱性診断ガイドライン」（以下、本ガイドライン）を作成し公開した。

本ガイドラインは「脆弱性診断士」における「脆弱性診断士（Webアプリケーション）」区分における「Silver」ランクで要求される内容としている。

執筆者(1.0,1.1版)

- 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 (三井物産セキュアディレクション株式会社)
- 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 (三井物産セキュアディレクション株式会社)
- 岩井 基晴 (株式会社イエラエセキュリティ)
- 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)
- 越智 勇貴
- 池田 雅一 (テクマトリックス株式会社)
- 東内 裕二 (NTTコミュニケーションズ株式会社)
- 伊藤 彰嗣 (サイボウズ株式会社)
- 阿部 真吾
- 藤本 万里子
- 野口 睦夫(日本電気株式会社)
- 八木橋 優(株式会社メルカリ)
- 原田 浩充(NTTデータ先端技術株式会社)
- 小武 裕也(NTTデータ先端技術株式会社)
- 大塚 淳平(NRIセキュアテクノロジーズ株式会社)
- 田中 悠一郎(NRIセキュアテクノロジーズ株式会社)

(順不同)

執筆者(1.2版)

- 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)
- 廣田 一貴 (三井物産セキュアディレクション株式会社)
- 西谷 完太 (株式会社イエラエセキュリティ)
- 渡部 裕(株式会社イエラエセキュリティ)
- 安達 智弘(株式会社神戸デジタル・ラボ)
- 林 義徳 (LINE株式会社)
- 米内貴志(株式会社Flatt Security)

(順不同)

レビュアー

- ISOG-J WG1 メンバーの方々
  http://isog-j.org/ OWASP Japan メンバー方々
  https://www.owasp.org/index.php/Japan

改定履歴

- 2014年12月8日 脆弱性診断士（Webアプリケーション）スキルマップ 第1.0版リリース
- 2016年3月7日 脆弱性診断士（Webアプリケーション）スキルマップ＆シラバス 第1.0版リリース
- 2018年5月18日　脆弱性診断士（Webアプリケーション）スキルマップ＆シラバス 第1.1版リリース
- 2022年3月1日　脆弱性診断士（Webアプリケーション）スキルマップ＆シラバス 第1.2版リリース

本プロジェクトに係わる組織について

NPO日本ネットワークセキュリティ協会（JNSA）について

NPO日本ネットワークセキュリティ協会は、ネットワーク・セキュリティ製品を提供しているベンダー、システムインテグレータ、インターネットプロバイダーなどネットワークセキュリティシステムに携わるベンダーが結集し、ネットワーク社会の情報セキュリティレベルの維持・向上及び日本における情報セキュリティ意識の啓発に努めるとともに、最新の情報セキュリティ技術及び情報セキュリティへの脅威に関する情報提供などを行うことで、情報化社会へ貢献することを目的としております。
http://www.jnsa.org/

日本セキュリティオペレーション事業者協議会（ISOG-J）について

日本セキュリティオペレーション事業者協議会（Information Security Operation providers Group Japan 略称: ISOG-J）は、セキュリティオペレーション技術向上、オペレータ人材育成及び関係する組織・団体間の連携を推進することによって、セキュリティオペレーションサービスの普及とサービスレベルの向上を促し、安全で安心して利用できるIT環境実現に寄与することを目的として設立されました。
http://isog-j.org/

OWASP Japanについて

OWASP（Open Web Application Security Project）は、Webを始めとするソフトウェアのセキュリティ環境の現状、またはセキュアなソフトウェア開発を促進する技術・プロセスに関する情報共有と普及啓発を目的としたプロフェッショナルの集まる、オープンソース・ソフトウェアコミュニティです。OWASP Japanは、その日本チャプターであり、数々のプロジェクトへの参画による貢献、日本語への翻訳、またプロジェクト設立なども行っています。
https://www.owasp.org/index.php/Japan

本プロジェクトに関するお問い合わせ先

脆弱性診断士スキルマッププロジェクト
https://www.owasp.org/index.php/Pentester_Skillmap_Project_JP