

ISOG-Jの2017年度 成果物あれこれ

日本セキュリティオペレーション事業者協議会

WG4リーダー： 阿部 慎司 (NTTセキュリティ・ジャパン)

WG6リーダー： 武井 滋紀 (NTTテクノクロス)



リーダー: 上野 宣 (トライコーダ)

脆弱性診断士スキルマッププロジェクト

- ✓ Webアプリケーション脆弱性診断ガイドライン
- ✓ 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
- ✓ 脆弱性診断 初心者ハンズオントレーニング

(OWASP Japanとの共同WG)



Log in Request account

Page Discussion Read View source View history Search

Pentester Skillmap Project JP

脆弱性診断士スキルマッププロジェクト

特定非営利活動法人日本ネットワークセキュリティ協会(JNSA)の日本セキュリティオペレーション事業推進委員会(JNSA-PO)の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「脆弱性診断士スキルマッププロジェクト (以下「スキルマップ」)」では、脆弱性診断を行う個人の技術的能力を具体的に示すべく、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、脆弱性診断を行うためのガイドラインを整理しています。

本ワーキンググループに関心のある方は、Project leader: Sen UENO まで

Webアプリケーション脆弱性診断ガイドライン

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う脆弱性診断だけでは十分なプロジェクトではおえず、そのために手動診断ツールを使う手動診断を併用することが、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が大きい。そこで本委員会では手動や半自動を定義することで、一定レベルの手動診断による脆弱性診断を行うことが可能な脆弱性診断ガイドライン (以下、本ガイドライン) を作成し公開します。

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)」で要求される内容としています。

Download

2018年5月18日リリース版

- Webアプリケーション脆弱性診断ガイドライン (PDF版) [ダウンロード](#)
- Webアプリケーション脆弱性診断ガイドライン (PDF版) [ダウンロード](#)
- Webアプリケーション脆弱性診断ガイドラインについて [ダウンロード](#)
- Webアプリケーション脆弱性診断ガイドライン (PDF版) [ダウンロード](#)

脆弱性診断 初心者ハンズオントレーニング



20180513-HandsOn

すべてダウンロード

名前 ↑

 HTTP基礎入門 2018/5/13 脆弱性診断士スキルマッププロジェクト 1320_HTTP基礎入...	 Burp Suiteの使い方 2018/5/13 脆弱性診断士スキルマッププロジェクト 1340_Burpの使い...	 ガイドラインの説明 (見方の説明) 2018/5/13 脆弱性診断士スキルマッププロジェクト 1420_ガイドライ...	 Badstoreでの診断実践編 SQL Injection & XSS 2018/5/13 Burp Suite Japan User Group 1450_SQLI.XSS.2...
 Badstoreでの診断実践編 SQL Injection & XSS 実習課題(4)解答編 2018/5/13 Burp Suite Japan User Group 1450_SQLI.XSS解...	 アクセス制御系の話 2018/5/13 脆弱性診断士スキルマッププロジェクト 1550_認可制御不...		

脆弱性診断士スキルマッププロジェクト



リーダー: 川口 洋 (ラック)

セキュリティ技術者交流の場を提供

- ✓ 参加企業持ち回りで開催
- ✓ セキュリティトレンド、研究、SOC見学、人材育成など幅広いジャンルで交流
- ✓ 会合後の懇親会で繋がりを深めるのが大切



リーダー: 阿部 慎司 (NTTセキュリティ・ジャパン)

セキュリティオペレーションの普及啓発

- ✓ セキュリティ対応組織成熟度 (ISOMM) 調査タスクフォースの立ち上げ
- ✓ 他の組織・団体との連携
- ✓ 普及啓発のための講演、イベントの企画

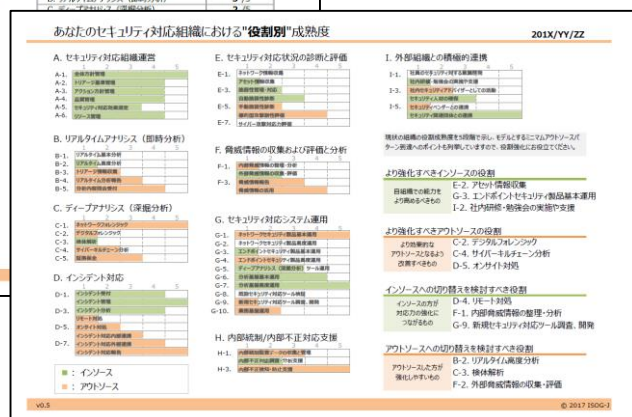
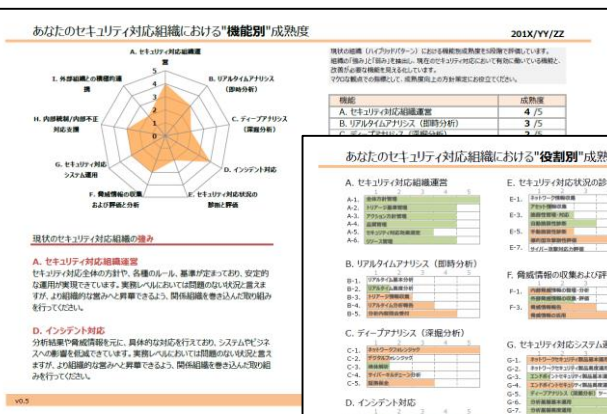
セキュリティ対応組織成熟度 (ISOMM) の普及

ISOG-J事業者連絡会の企画

毎年約120名の
会員が参加



2018年で
10周年！



講演

- Network Security Forum (JNSA)
 - セキュリティ対応組織力を上げるコツ～成熟度の可視化と、情報共有の心得～
- 関西情報セキュリティ合同セミナー (JASA)
- デジタル・フォレンジック・コミュニティ (IDF)
 - セキュリティオペレーションとインシデントレスポンスの蜜月



リーダー: 佳山 こうせつ (富士通)

セキュリティに関する世界動静を可視化

- ✓ 1年での短期集中プロジェクト
- ✓ セキュリティに関する、ニュース、イベント、事件などを月ごとにまとめ変化を可視化

グローバル動静共有プロジェクト



セキュリティ動静マップ2017年まとめ

(以下は2017年11月の例)





リーダー: 武井 滋紀 (NTTテクノクロス)

セキュリティオペレーションを徹底議論

- ✓ セキュリティ対応組織(SOC,CSIRT)の教科書 v2.0
- ✓ セキュリティ対応組織 (SOC,CSIRT)強化に向けたサイバーセキュリティ情報共有の「5W1H」v1.0
- ✓ Six Ws on cybersecurity information sharing for enhancing SOC/CSIRT v1.0

- 毎月定例会を開催
- セキュリティの運用や対処に関する課題を議論し、公開できる成果物は公開を行う
- 成果物、発表
 - 10/3,「セキュリティ対応組織(SOC,CSIRT)の教科書 v2.0」公開
 - 10/27,「セキュリティ対応組織 (SOC,CSIRT)強化に向けたサイバーセキュリティ情報共有の「5W1H」 v1.0」公開
 - 11/28, InternetWeek 2017 での発表「今求められる SOC,CSIRTの姿とは」
 - 2/20,「Six Ws on cybersecurity information sharing for enhancing SOC/CSIRT v1.0」公開

セキュリティ対応組織 (SOC,CSIRT)の教科書 v2.0

- 2017/10/3にV2.0に改版
 - 2018/4/9にV2.1にさらに改版
- 9つの機能と54の役割について、インシデント時のフローを追加！
- 何もない時に何をすべきか、平時の対応についても追加！
- 「成熟度チェックリスト」を新たに追加！
 - 通称ISOMM : ISOG-J SOC,CSIRT Maturity Model
- 全国のいろいろな組織での成熟度を図りたいので、タスクフォースを立ち上げました！
- JNSA各社の皆さんも成熟度を測ってデータをください！
- 今どのくらいできている、どんな組織が多いのかを分析します！

セキュリティ対応組織(SOC,CSIRT)強化に向けたサイバーセキュリティ情報共有の「5W1H」

- いま課題の多い情報共有について課題を分析し、なぜ問題になっているかをまとめました。
- 公開からすぐにダウンロード数が急増！人気コンテンツです。
- 人気のので英語版もできました！「6Ws」
 - IIIのもいさんがFIRST TC カトマンドウで発表し、海外で紹介されています

- 今年も発表しました！
- 2015年から3年連続3回目です！
- 6/1にInternet Week ショーケース in 広島で広島の皆さんに披露しました



- SOC,CSIRTの成熟度チェックリスト(通称:ISOMM)の各地での説明と展開、データ収集、分析
- 「マネージドセキュリティサービス選定ガイド v1.0」(2010年発表)の更改に向けた議論
- 「セキュリティ対応組織 (SOC,CSIRT)強化に向けたサイバーセキュリティ情報共有の「5W1H」 v1.0」の更改に向けた議論
- 次世代エンドポイントセキュリティ製品に関する議論(非公開予定)
- InternetWeek 2018 における発表

- ISOG-J成果物に対するご意見、ご要望お待ちしております！

<https://jp.surveymonkey.com/r/W9HCMFP>

- 常時受け付けております
- 匿名での投稿が可能です



ISOG-J

日本セキュリティオペレーション事業者協議会 (ISOG-J) アンケート

ISOG-J成果物に対するフィードバック

* 日本セキュリティオペレーション事業者協議会 (ISOG-J) が作成した成果物についてご意見、ご要望などございましたらこちらにご記入ください。

フィードバックは次の成果物の内容にいかしていきます。ご協力よろしくお願いします。

成果物名：

*コメント：

* 成果物に対する評価：

送信する