Web システム／Web アプリケーションセキュリティ要件書について

Ver.3.1
March 2021

1. Web システム／Web アプリケーションセキュリティ要件書について

1.1. 本ドキュメントについて

Web システム／Web アプリケーションセキュリティ要件書（以下、本ドキュメント）は、安全な Web アプリケーションの開発に必要なセキュリティ要件書です。発注者、開発者、テスト実施者、セキュリティ専門家、消費者が活用することで、以下のことを達成することを目的としています。

- 開発会社・開発者に安全な Web システム／Web アプリケーションを開発してもらうこと
- 開発会社と発注者の瑕疵担保契約の責任分解点を明確にすること
- 要求仕様や RFP（提案依頼書）として利用し、要件定義書に組み込むことができるセキュリティ要件として活用していただくこと

1.2. 本ドキュメントがカバーする範囲

本ドキュメントでは Web システム／Web アプリケーションに関して一般的に盛り込むべきだと考えられるセキュリティ要件について記載しています。また、開発言語やフレームワークなどに依存することなくご利用いただけます。ただし、ネットワークやホストレベル、運用などに関するセキュリティ要件については記載していません。

対象とする Web システム／Web アプリケーションは、インターネット・イントラネット問わず公開するシステムで、特定多数または不特定多数のユーザーが利用するシステムを想定しています。この中でも特に認証を必要とするシステムが、本ドキュメントの主なターゲットとなっています。

本ドキュメントは、セキュリティ要件としての利用しやすさを優先して記載しているため、一般的であろうというシステムを想定し、例外の記載を少なくしたセキュリティ要件となっています。そのため具体的な数値や対策を指定していることもありますが、要件定義書に記載する内容は開発者と折衝してください。

2. about OWASP

2.1. OWASP について

The Open Web Application Security Project (OWASP) は、信頼できるアプリケーションの開発・購入・運用の推進を目的として設立されたオープンなコミュニティです。OWASP では、以下をフリーでオープンな形で提供・実施しています。 (https://www.owasp.org/)

- アプリケーションセキュリティに関するツールと規格
- アプリケーションセキュリティ検査、セキュア開発、セキュリティ・コードレビューに関する網羅的な書籍
- 標準のセキュリティ制御とライブラリ
- 世界中の支部
- 先進的な研究
- 世界中での会議
- メーリング・リスト

全ての OWASP のツール、文書、フォーラム、および各支部は、アプリケーションセキュリティの改善に関心を持つ人のため、無料で公開されています。アプリケーションセキュリティに対する最も効果的なアプローチとして、我々は人、プロセス、技術という 3 つの課題から改善することを提唱しています。

OWASP は新しい種類の組織です。商業的な圧力が無い中、アプリケーションセキュリティに対して、偏見無く実用的かつコスト効果の高い情報の提供を行っています。OWASP はいかなる IT 企業の支配下にもありませんが、商用のセキュリティ技術の活用を支持しています。他のオープンソース・ソフトウェアプロジェクトと同様に、OWASP も協同かつオープンな形で多様な資料を作成しています。

The OWASP Foundation は、このプロジェクトの長期的な成功を目指す非営利組織です。OWASP 理事会、グローバル委員会、支部長、プロジェクトリーダー、プロジェクトメンバーを含む、OWASP の関係者はほとんどボランティアです。革新的なセキュリティ研究に対して、助成金とインフラの提供で支援しています。

2.2. OWASP Japan について

主に日本で活動している OWASP メンバーによる日本支部です。OWASP の膨大なドキュメントやツール類の日本語化を初めとして、日本からのセキュリティ情報の発信を行っています。是非ご参加下さい。
https://owasp.org/www-chapter-japan/

Web システム／Web アプリケーションセキュリティ要件書

制作：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の日本セキュリティオペレーション事業者協議会（ISOG-J）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》

Ver.3.1 執筆メンバー：
上野 宣 (ISOG-J WG1 リーダー／OWASP Japan Chapter 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)
池田 雅一 (テクマトリックス株式会社)
大塚 淳平 (NRI セキュアテクノロジーズ株式会社)
小河 哲之 (三井物産セキュアディレクション株式会社)
洲崎 俊 (三井物産セキュアディレクション株式会社)
関根 鉄平 (株式会社エーアイセキュリティラボ)
野口 睦夫 (NEC ソリューションイノベータ株式会社)
廣田 一貴 (三井物産セキュアディレクション株式会社)
松本　悦宜 (Capy 株式会社)
水戸部 一貴 (富士ソフト株式会社)
吉田 聡 (株式会社ラック)

3. 改訂履歴

株式会社トライコーダ版
Ver.1.0　　初版（2009 年 3 月 17 日）
Ver.1.1　　2009 年 4 月 22 日改訂

OWASP 版
Ver.1.0　　初版（2013 年 11 月 1 日）
Ver.2.0　　2015 年 10 月 13 日改訂
Ver.3.0　　2019 年 1 月 15 日改訂
Ver.3.1　　2021 年 3 月改訂