



**OWASP**

The Open Web Application Security Project

06/09

# OWASP Application Security Verification Standard 2009

– Web Application Standard

# release



**日本語版**  
Japanese Version



Creative Commons (CC) Attribution Share-Alike  
Free version at <http://www.owasp.org>



この冊子では、アプリケーションレベルの Web アプリケーションセキュリティ検査を 4 つのレベルに分類しています。アプリケーションレベルのセキュリティとは、the Open Systems Interconnection Reference Model (OSI Model) で定義づけられるアプリケーションレイヤーのコンポーネントの分析を指し、その他の実行中の OS やネットワークの分析とは異なります。各検査レベルにおいて、Web アプリケーションを保護するセキュリティ対策の有効性を検査する要件を設定しています。

なおこの要件は下記の目的で設定しました。

- 数値評価のため - アプリケーションの開発者やアプリケーションの運営者が、自身の Web アプリに対する資産評価や信頼度の指標として
- ガイダンスのため - セキュリティ管理者・セキュリティ管理業者が、アプリケーションセキュリティの要件を満たすためのガイダンスとして
- 購買・調達において - 契約文書においてアプリケーションセキュリティの検査に関する要件を定義する基礎として<sup>1</sup>

当要件は、上記の目的のために設計され、セキュリティ対策の設計・実装・（アプリケーションによる）運用についての確認を行います。この要件では、セキュリティ対策が 1) deny-by-default の原則を用いているか、2) 集中管理されているか、3) サーバサイドで行われているか、4) 全てが適切な箇所で実施されているかという 4 点を確認します。<訳者注：deny-by-default の原則とは、セキュリティ対策を指定した部分のみ除外するという原則で、除外対象のリストはホワイトリストで作成します。>

Copyright © 2008 - 2009 The OWASP Foundation.



This document is released under the Creative Commons Attribution ShareAlike 3.0 license. For any reuse or distribution, you must make clear to others the license terms of this work.

<sup>1</sup> For more information about using ASVS in contracts, see the *Contract Annex* (OWASP, 2009).



## 目次

はじめに .....	1
手法 .....	1
謝辞 .....	3
アプリケーションセキュリティ検査レベル .....	4
Level 1 - 自動検査 .....	4
Level 1A - 動的スキャン（半自動検査） .....	6
Level 1B - ソースコードスキャン（半自動検査） .....	7
Level 2 - 手動検査 .....	7
Level 2A - セキュリティテスト（半手動検査）	
Level 2B - コードレビュー（半手動検査） .....	10
Level 3 - 設計に関する検査 .....	10
Level 4 - 内部検査 .....	13
要件の解釈と参考例について .....	15
検査に関する詳細要件 .....	16
V1 - セキュリティアーキテクチャの文書化に関する要件 .....	17
V2 - 認証に関する検査要件 .....	18
V3 - セッション管理に関する検査要件 .....	19
V4 - アクセスコントロールに関する検査要件 .....	20
V5 - 入力のバリデーションに関する検査要件 .....	22
V6 - 出力のエンコード／エスケープに関する検査要件 .....	22
V7 - 暗号化に関する検査要件 .....	24
V8 - エラー処理及びログ記録に関する検査要件 .....	25
V9 - データの保護に関する検査要件 .....	26
V10 - 通信のセキュリティに関する検査要件 .....	27
V11 - HTTP のセキュリティに関する検査要件 .....	28
V12 - セキュリティ設定に関する検査要件 .....	29
V13 - 悪意のあるコードに関する検査要件 .....	29
V14 - 内部セキュリティに関する検査要件 .....	30
検査報告書に関する要件 .....	31
R1 - イントロダクション .....	31
R2 - アプリケーションに関する記載 .....	31
R3 - アプリケーションのセキュリティ設計 .....	31
R4 - 検査結果 .....	32
用語解説 .....	36



## 図

図 1 - OWASP ASVS のレベル .....	1
図 2 - SDLC に検査実施を導入する一例 .....	2
図 3 - OWASP ASVS レベル 1, 1A 及び 1B .....	5
図 4 - OWASP ASVS レベル 1 セキュリティアーキテクチャの例 .....	6
図 5 - OWASP ASVS レベル 2, 2A, 及び 2B .....	7
図 6 - OWASP ASVS レベル 2 セキュリティアーキテクチャの例 .....	9
図 7 - OWASP ASVS レベル 3 .....	11
図 8 - OWASP ASVS レベル 3 セキュリティアーキテクチャの例 .....	12
図 9 - OWASP ASVS レベル 4 .....	13
図 10 - OWASP ASVS レベル 4 未検査のコード例 .....	15
図 11 - 報告書の内容 .....	31

## 表

表 1 - OWASP ASVS セキュリティアーキテクチャの文書化に関する要件(V1) .....	17
表 2 - OWASP ASVS 認証に関する検査要件 (V2) .....	18
表 3 - OWASP ASVS セッション管理に関する検査要件 (V3) .....	19
表 4 - OWASP ASVS アクセスコントロールに関する検査要件 (V4) .....	21
表 5 - OWASP ASVS 入力のバリデーションに関する検査要件(V5) .....	22
表 6 - OWASP ASVS 出力のエンコード／エスケープに関する検査要件(V6) .....	23
表 7 - OWASP ASVS 暗号化に関する検査要件 (V7) .....	24
表 8 - OWASP ASVS エラー処理及びログ記録に関する検査要件 (V8) .....	25
表 9 - OWASP ASVS データの保護に関する検査要件 (V9) .....	26
表 10 - OWASP ASVS 通信のセキュリティに関する検査要件 (V10) .....	27
表 11 - OWASP ASVS HTTP のセキュリティに関する検査要件 (V11) .....	28
表 12 - OWASP ASVS セキュリティ設定に関する検査要件 (V12) .....	29
表 13 - OWASP ASVS 悪意のあるコードに関する検査要件 (V13) .....	29
表 14 - OWASP ASVS 内部セキュリティに関する検査要件 (V14) .....	30
表 15 - OWASP ASVS 検査報告書の記載内容 .....	32



## はじめに

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。全ての OWASP のツール、文書、フォーラム、各支部は、アプリケーションセキュリティの向上に関心を持つあらゆる人に無料で公開されています。最も効果的なアプリケーションセキュリティの向上とは、人、プロセス、技術という 3 点全ての改善であり、我々もこれら 3 点を課題としてアプリケーションセキュリティにアプローチすることを提唱しています。詳細は [www.owasp.org](http://www.owasp.org) を参照下さい。

OWASP は新しい種類の組織です。商業的な圧力が無い中、偏見無く現実的で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のコミュニティと同様に、OWASP もまたオープンな方法で様々なドキュメントを共同で作成しています。The OWASP Foundation はこの OWASP が長期的視点で成功することを目指す非営利組織です。

OWASP アプリケーションセキュリティ検査標準(Application Security Verification Standard (以下、ASVS とします))のプロジェクトの主な目的は、商用利用出来るオープンな標準として、市場で提供できるような現実的な検査の厳密性及び検査範囲に標準を設けることです。当標準は、クロスサイトスクリプティング (XSS) や SQL インジェクションなどの脆弱性に対する保護が必要なアプリケーションとその環境に対する技術的なセキュリティ対策のテストの基礎となります。またこの標準は、Web アプリケーションのセキュリティレベルを各レベル毎に達成する際にも用いる事が出来ます。<sup>2</sup>

## 手法

The OWASP ASVS では、検査と報告書の要件を網羅性と厳密性を基に設定しています。標準は下図の通りレベルを 4 つの階層に分けています（例：レベル 2 はレベル 1 に比して高い網羅性と厳密性を求めています）。

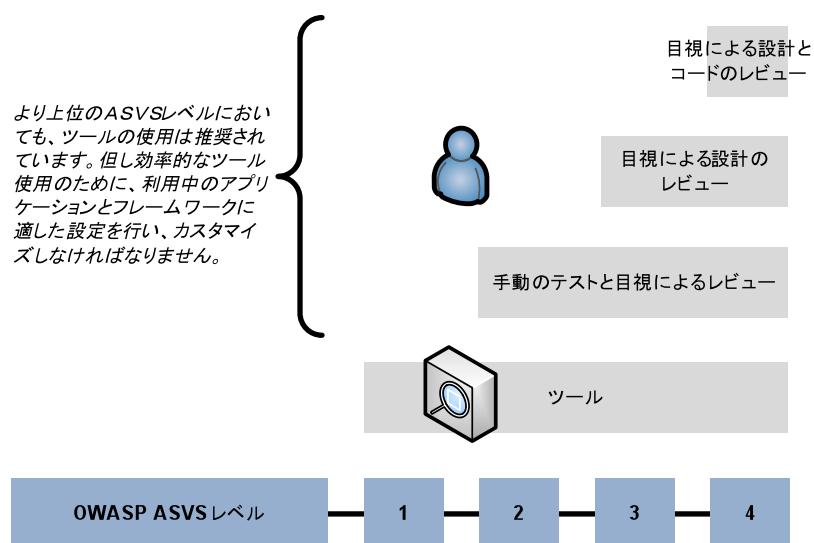


図 1 - OWASP ASVS のレベル

<sup>2</sup> For more information about common Web application vulnerabilities, see the OWASP Top Ten (OWASP, 2007).



Web アプリケーションのセキュリティ検査は、対象となるアプリケーションの入出力のパスを論理的視点から巡回（又は巡回することを企図）して、それらパスを解析することで実施します（なお、対象となるアプリケーションについては TOV (Target of Verification)と呼ぶこととします）。アプリケーションが複雑になると、一般的には解析にそれだけ長い時間とコストがかかります。アプリケーションの複雑さは、コードの行数だけが決定要素ではなく、様々な技術要素を採用している場合は様々な解析が必要となります。単純なアプリケーションはライブラリとフレームワークだけで構成されているでしょうが、若干複雑なアプリケーションは Web1.0 のアプリケーションが含まれていると思います。複雑なアプリケーションには、Web 2.0 のアプリケーションを含み、最新の技術や独特的の技術を活用している場合があります。

ASVS のレベル 1 及びレベル 2 ではさらに詳細な構成要素を持っています（レベル 1 の検査においては、レベル 1A 及び 1B の要件を満たしている必要があります）。例えば、レベル 1 ではなくレベル 1A 又は 1B のみに準拠しているという証明は、レベル 1 に準拠しているよりも弱い証明となります。ASVS では検査と報告の要件は、概要要件、詳細要件及び報告要件という 3 タイプの要件で定義されています。詳細要件は、low-level アプリケーションの実装と検査対象・内容に関するものです。報告の要件は、OWASP ASVS に基づいたアプリケーション検査の結果をどのように文書化すべきかという点に関するものです。

OWASP は、ASVS を初めとする膨大な情報を提供し、組織の安全なアプリケーション開発・運用を支援しています。OWASP ASVS、OWASP Contract Annex,<sup>3</sup> そして OWASP ESAPI<sup>4</sup> (Enterprise Security API) によって、ソフトウェア開発のライフサイクルをサポートします（下図参照）。

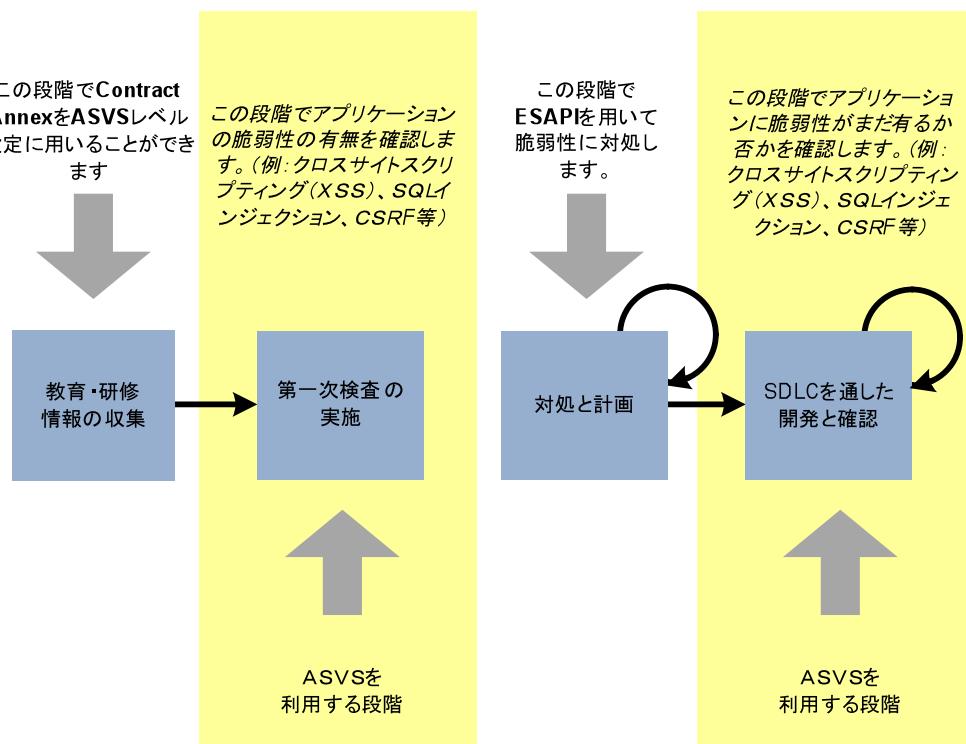


図 2 - 各自の SDLC に検査実施を導入する一例<sup>5</sup>

<sup>3</sup> For information about how to specify an ASVS level in a contract, see the OWASP Contract Annex.

<sup>4</sup> For more information about how to ESAPI-Enable (ES-Enable) your application, see the OWASP ESAPI project (OWASP 2009).



## 謝辞

We thank the OWASP Foundation for sponsoring the OWASP Application Security Verification Standard Project during the OWASP Summer of Code 2008.

Project Lead:<sup>6</sup> Mike Boberski (Booz Allen Hamilton)

Authors:<sup>7</sup> Mike Boberski (Booz Allen Hamilton), Jeff Williams (Aspect Security), Dave Wichers (Aspect Security)

Project Sponsors:



Booz | Allen | Hamilton

Acknowledgement is given for the contributions of: Pierre Parrend, who acted as an OWASP Summer of Code 2008 Reviewer; Andrew van der Stock (Aspect Security); Nam Nguyen (Blue Moon Consulting); John Martin (Boeing); Gaurang Shah (Booz Allen Hamilton); Theodore Winograd (Booz Allen Hamilton); Stan Wisseman (Booz Allen Hamilton); Barry Boyd (CGI Federal); Steve Coyle (CGI Federal); Paul Douthit (CGI Federal); Ken Huang (CGI Federal); Dave Hausladen (CGI Federal); Mandeep Khera (Cenzic); Scott Matsumoto (Digital); John Steven (Digital); Stephen de Vries (Corsaire); Dan Cornell (Denim Group); Shouvik Bardhan (Electrosoft), Dr. Sarbari Gupta (Electrosoft); Eoin Keary (Ernst & Young); Richard Campbell (Federal Deposit Insurance Corporation); Matt Presson (FedEx); Jeff LoSapio (Fortify Software); Liz Fong (National Institute of Standards and Technology); George Lawless (Noblis); Dave van Stein (ps\_testware); Terrie Diaz (SAIC); Ketan Dilipkumar Vyas (Tata Consultancy Services); Bedirhan Urgun (TURKCELL); Dr. Thomas Braun (United Nations); Colin Watson (Watson Hall); Jeremiah Grossman (WhiteHat Security); and finally, thanks are given to the application security verification community and others interested in trusted Web computing for their enthusiastic advice and assistance throughout this effort.

<sup>5</sup> For more information about introducing security-related activities into your existing SDLC, see the OWASP CLASP (OWASP 2008) or OWASP SAMM Projects (OWASP 2009).

<sup>6</sup> Email: mike.boberski@owasp.org

<sup>7</sup> Email: jeff.williams@owasp.org, dave.wichers@owasp.org



## アプリケーションセキュリティ検査レベル

The ASVS は 4 つのレベルがあり、検査深度と検査範囲が向上するごとに、数字が上がります。検査範囲は宣言されたセキュリティ要件、検査深度は手法と各セキュリティ検査に必要とされる厳密性によって設定されます。ツールは ASVS の各レベルにおいて重要な位置を占めます。高いレベルにおいてもツールの使用が奨励されますが、効果的な使用のために、検査対象のアプリケーションとフレームワークに合わせて、入念にカスタマイズ設定しなければなりません。また、全レベルにおいて、ツールの結果には目視確認が必要です。

レビューで設定したレベルの全要件を検査対象が満たしているかどうかを決定するのは、検査者の責任です。アプリケーションが設定したレベルの全要件を満たした場合、OWASP ASVS の該当レベルであるとみなすことができます。アプリケーションがある特定のレベルの全要件を満たすことはできなかったものの、1 段階低いレベルの全要件を満たした場合は、1 段階低いレベルの検査を通過したと見なすことができます。なお、本標準では、「検査者」という用語は、要件に対してアプリケーションをレビューする個人又はチームを指します。

アプリケーションのスペックとして、OWASP ASVS のある特定レベルに達することが必要な場合に、更に詳細要件設定が一部必要となる場合もあります。そのような場合にはさらに高い ASVS レベルの要件が含まれる場合があります。例えば、金融機関において、OWASP ASVS レベル 2 に適合する検査に加えて、悪意のあるコードの存否確認が必要なる場合があります（この存否確認はレベル 4 でのみ必要とされています）。その他の組織や業務でも同様の状況にあると思われます。ある特定の情報セキュリティポリシーや法的規制へのコンプライアンスなどがその例です。

レベル 0 はありません。  
また、レベル認定のためには、脆弱性が解消又は回避され、再確認されている必要があります。

### レベル 1 自動検査

レベル 1（「自動検査」）は、セキュリティ対策の適正な運用をある程度確認しなければならないアプリケーションに有効です。このレベルでのセキュリティ上の脅威は、ウィルスとワームです。攻撃対象は広範囲にわたるスキャンによって無作為に選ばれ、最も脆弱な対象に攻撃を加えます。検査対象には、アプリケーション構築のために開発・改修されたソースコードが含まれます。

レベル 1 の検査では、自動化ツールを使用し、目視確認で検査内容を強化します。このレベルの検査は、アプリケーションセキュリティの範囲としては部分的なものです。また目視確認は、ツールの検出結果が正確で、誤検知では無いことを確認することのみを企図しており、検査を完璧にすることを目的としていません。

レベル 1 は、2 つの要素で構成されています。レベル 1A は脆弱性スキャン（動的解析）の自動化ツール活用に関するものであり、レベル 1B はソースコードスキャン（静的解析）の自動化ツールに関するものです。検査は、どちらか一方の診断でも良いですし、2 種類の検査を統合することも可能です。このレベルの構造は下図の通りです。

レベル 1A または 1B どちらか一方の標準を満たすということは可能ですが、どちらか一方のレベルを満たすだけでは、レベル 1 の標準である網羅性又は厳密性を満たすことはできません。レベル 1 の標準を満たすには、レベル 1A 及び 1B 両方の要件を満たす必要があります。

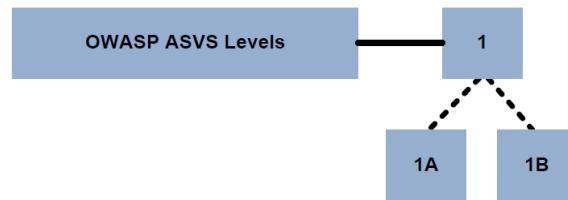


図 3 - OWASP ASVS レベル 1, 1A, 及び 1B

以下は、レベル 1、1A 又は 1B に達するための最小限の概要要件です。

#### 検査対象

L1.1 検査対象には、アプリケーション構築のために開発・改修されたソースコードを含む。

#### セキュリティ対策の決定に関する要件

無し レベル 1 では、アプリケーションセキュリティ対策の決定方法についての要件はない。

#### セキュリティ対策の利用に関する要件

無し レベル 1 のアプリケーションでは、アプリケーションセキュリティ対策が実施箇所についての要件はない。

#### セキュリティ対策の実装に関する要件

無し レベル 1 では、セキュリティ対策の実装方法についての要件は無い。

#### セキュリティ対策の検査に関する検査要件

L1.2 「検査に関する詳細要件」の章に記載されているレベル 1A の要件に則って、動的なスキャンが行われている。

L1.3 「検査に関する詳細要件」の章に記載されているレベル 1B の要件に則って、静的なソースコードスキャンが行われている。

レベル 1においてどちらか一方の検査手法だけで満たすことのできる要件は、どちらか一方の手法で検査すれば要件を満たしたことになります。また、検査者が選択したツールでは、ある特定の検査要件を満たすには不十分である場合、検査者はツールの不十分な部分に手動検査を採用することが出来ます。<sup>8 9</sup>

<sup>8</sup> For more information about performing manual verification by performing manual penetration testing, see the *OWASP Testing Guide* (OWASP, 2008).

<sup>9</sup> For more information about performing manual verification by performing a manual code review, see the *OWASP Code Review Guide* (OWASP, 2008).



## 報告に関する要件

L1.4 検査レポートには各コンポーネントを列挙してアプリケーションのセキュリティアーキテクチャを詳しく記述し、「報告に関する詳細要件」の章の要件に則った検査結果を記載する。

レベル 1 では、アプリケーションのコンポーネントとは、ソースファイル、ライブラリー、実行ファイルを指します（下図参照）。各コンポーネントがアプリケーションの一部なのかもっと広い IT 環境の一部なのかという区別は必要ですが、さらに細かい分類を行う必要はありません。したがってアプリケーションは、複数のコンポーネントを持つ単一の存在として扱われます。利用者が送るリクエストパスを、個別に確認したり文書化する必要はありません。

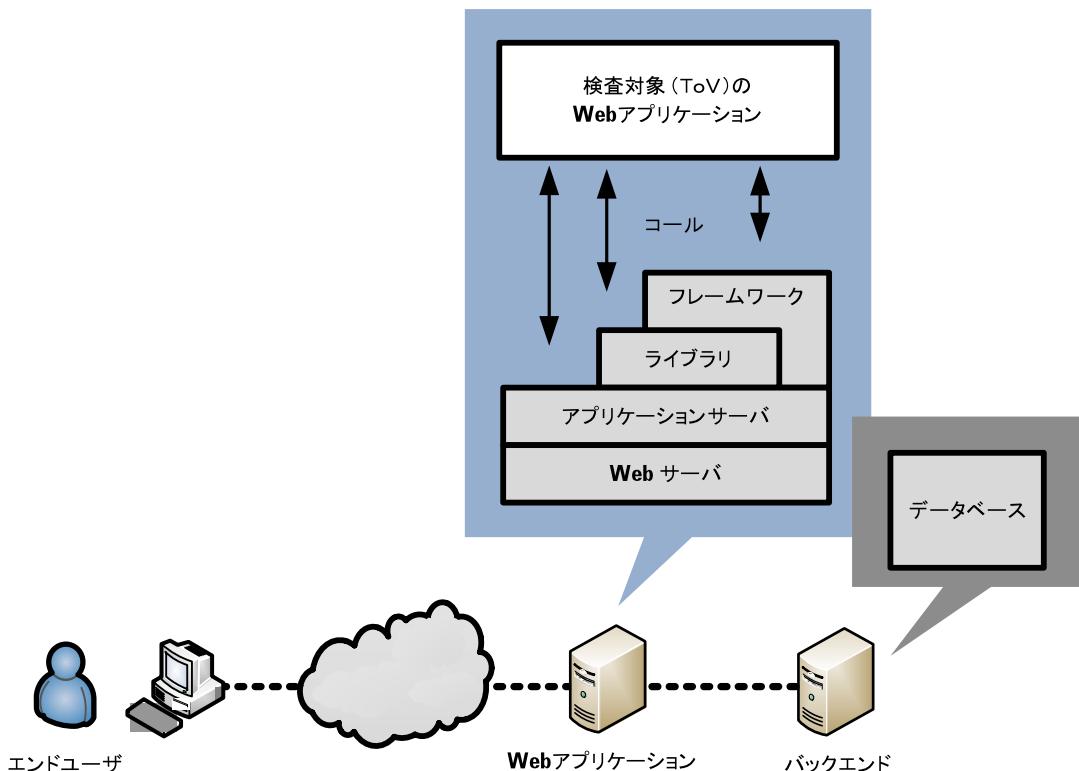


図 4 - OWASP ASVS レベル 1 セキュリティアーキテクチャの例

## レベル 1A - 動的スキャン(半自動検査)

### 動的スキャンによるセキュリティ対策検査に関する要件

動的スキャン（アプリケーション脆弱性スキャン）は、アプリケーションのセキュリティ上の脆弱性を検出するため、自動スキャンツールを用いて稼働状態にあるアプリケーションのインターフェースからアクセスする検査手法です。この手法では、設計・運用・セキュリティ対策の使用を十分に確認できませんが、レベル 1 の検査としては有用です。検査対象はこのレベルのセキュリティアーキテクチャの要件により設定されます。

L1A.1 「検査に関する詳細要件」の章に記載されているレベル 1A の要件に則って、動的なスキャンが行われている。



L1A.2 動的スキャンによる全結果が手動のペネトレーションテスト又は目視によるコードレビューにより確認されている。自動スキャンの結果が手動確認されていない場合は、確認がされていないと判断され、レベル 1 の要件達成には不十分である。

ツールが検出した脆弱性が、発現原因箇所が同一であり、脆弱性のカテゴリが一種類に集約できる場合、単一の検出結果とします。

## レベル 1B - ソースコードスキャン (半自動検査)

### ソースコードスキャンによるセキュリティ対策検査に関する要件

ソースコードスキャン（静的解析）では、自動スキャンツールを用いてソースコード内に含まれる脆弱なパターンを検知します。この手法では、設計・運用・セキュリティ対策の使用を十分に確認できませんが、レベル 1 の検査としては有用です。検査対象はこのレベルのセキュリティアーキテクチャの要件により設定されます。

- L1B.1 「検査に関する詳細要件」の章に記載されているレベル 1B の要件に則って、静的なソースコードスキャンが行われている。
- L1B.2 ソースコードスキャンによる全結果が手動のペネトレーションテスト又は目視によるコードレビューにより確認されている。自動化されたスキャンの結果が未確認の場合、何らかの保証を提供することは考えにくく、レベル 1 の品質には不十分である。

ツールが検出した脆弱性が、発現原因箇所が同一であり、脆弱性のカテゴリが一種類に集約できる場合、単一の検出結果とします。

## Level 2 - 手動検査

レベル 2（手動検査）は、一般的に、消費者決済や法人間決済、クレジットカード情報の取扱、個人情報を取り扱うアプリケーションに適したレベルです。レベル 2において確認出来るのは、適切なセキュリティ対策が立てられており、それが正しく機能しているということです。このレベルでのセキュリティ上の脅威は、ウィルス、ワーム、初歩的なオポチュニスト（訳注：script kiddie のような攻撃者）であり、例えば有償またはオープンソースの攻撃ツールを用いる攻撃者などが含まれます。検査対象には、アプリケーション構築のために開発・改修された全てのソースコードとアプリケーションに対してセキュリティ機能を提供するサードパーティのセキュリティが含まれます。レベル 2 では 2 つの構成要素があります（下図参照）。

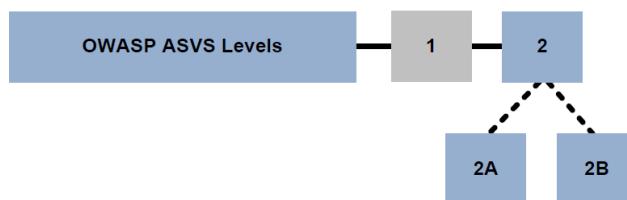


図 5 - OWASP ASVS レベル 2, 2A, 及び 2B

レベル 2A 又は 2B のどちらか一方の要件を満たしても、どちらか一方だけではレベル 2 の網羅性と厳密性を備えていることにはなりません。また、レベル 2 はレベル 1 よりも上位レベルですが、レベル 2 には自動化ツールを用いるという要件はありません。検査者は全要件を満たすために手動検査の手法のみを利用するという選択も可能です。自動ツールの結果を活用できる場合は、検査者はその結果を解析に用いることは出来ます。しかし、自動化ツールだけではレベル 2 の要件を満たしていると



いう十分な確証がなされないため、レベル1の要件を満たせば自動的にレベル2の同一要件を満たしているということにはなりません。

手動検査の手法においてもツール利用が想定されています。使用ツールには、レベル1で用いられる自動化ツールをはじめとして、あらゆる種類のセキュリティ解析ツール・検査ツールが含まれます。ただし、ツールはあくまでも検査対象の問題検出とセキュリティ対策評価を行う検査者の補助に留まります。また、ツールにアプリケーションの脆弱性を自動検出するロジックが含まれているか否かは問いません。

以下は、レベル2、2A又は2Bの最小限の概要要件です。

#### 検査対象

- L2.1 アプリケーション構築のために開発・改修された全てのソースコードを含む（レベル1からの継続要件）
- L2.2 サードパーティ製フレームワーク、ライブラリ、サービスで、アプリケーションのセキュリティ機能を担う全てのソースコード（レベル2での新規追加要件）。

#### セキュリティ対策の決定に関する要件

- L2.3 セキュリティチェックに関する技術的セキュリティ対策は、全てホワイトリストによって決定されている（レベル2での新規追加要件）。
- L2.4 「検査に関する詳細要件」の章で規定されているレベル2Aと2Bの要件に則って、セキュリティチェック及びセキュリティ実施効果をもたらすセキュリティ対策を必ず実施する（レベル2での新規追加要件）。

#### セキュリティ対策の利用に関する要件

- L2.5 「検査に関する詳細要件」の章で規定されているレベル2の要件に則って、サーバサイドにおいて、セキュリティ対策が必要な箇所に適切にたてられ、実装はアプリケーション内で集中管理されている（レベル2での新規追加要件）。

#### セキュリティ対策の実装に関する要件

- 無し レベル2では、セキュリティ対策の実装方法についての要件は無い

#### セキュリティ対策の検査に関する要件

- L2.6 「検査に関する詳細要件」の章で規定されているレベル2Aの要件に則って、アプリケーションに対して手動のペネトレーションテストを実施する（レベル2での新規追加要件）。
- L2.7 「検査に関する詳細要件」の章で規定されているレベル2Bの要件に則って、アプリケーションに対して手動でソースコードレビューを実施する（レベル2での新規追加要件）。

レベル2においてどちらか一方の検査手法だけで満たすことのできる要件は、どちらか一方の手法で検査すれば十分です。

検査者はレベル2の検査過程において、自動スキャンツールやコード解析ツールを用いることができますが、自動検査はレベル2の各要件における目視によるレビューの代替はできません。スキャンの結果が検査者の作業をより迅速に進め、目視によるレビューの結果を強化するのであれば、レベル2の検査実施においてツールは補助として利用することができます。



## 報告における要件

L2.8 各コンポーネントを概要要件に沿って整理してアプリケーションのセキュリティ構造を詳しく記述し、「報告に関する要件」の章の要件に則った検査結果を記載した検査報告書を作成する（レベル1からの継続要件）。

レベル2では、アプリケーションのコンポーネントとは、ソースファイル、ライブラリー、Model-View-Controller (MVC)のような、より上位のアーキテクチャに統合されている実行ファイル、ビジネスロジックやデータレイヤーのコンポーネント）を指します。例えば、下図のように、MVC構造に則ってグループ化されたサーバ側アプリケーション、アプリケーションサーバとして動作するアプリケーション、カスタムコード、ライブラリ、データベースアプリケーションから成るアプリケーションです。レベル2では、エンドユーザによって送信された各リクエストパスは、下図の様に文書化する必要がありますが、全パスを精査する必要はありません。

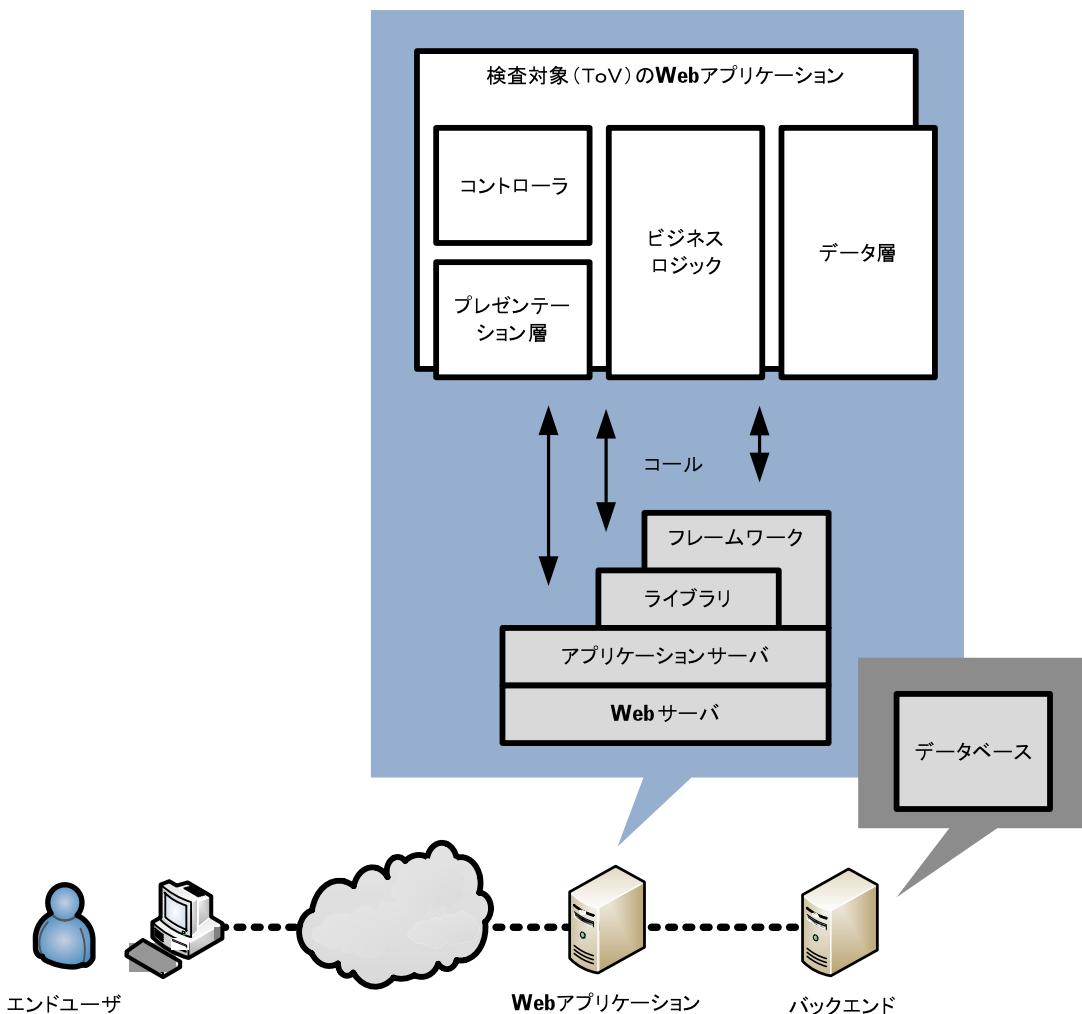


図 6 - OWASP ASVS レベル 2 セキュリティアーキテクチャの例



## レベル 2A セキュリティテスト（半手動検査）

### 手動のペネトレーションテストに関するセキュリティ対策要件

手動によるセキュリティテストは、アプリケーションの設計・実装・セキュリティ対策の利用を確認する動的テストで構成されています。検査対象は、このレベルにおけるセキュリティアーキテクチャの要件によって規定されます。

L2A.1 「検査に関する詳細要件」の章に記載されているレベル 2A の要件に則って、手動のセキュリティテストが行われている（レベル 2 での新規追加要件）。

検査者は、セキュリティ対策の効果的な利用を確立するため、サンプリング手法を用いることができます。検査者は、検出脆弱性について、ソフトウェアのベースラインにおける当該脆弱性を非公開にして検出し改修出来るように、文書化することを選択できます。また、検出された脆弱性が、発現原因箇所が同一であり、脆弱性のカテゴリが一種類に集約できる場合、単一の検出結果として統合すべきです。

## レベル 2B コードレビュー（半手動検査）

### 目視によるコードレビューに関するセキュリティ対策要件

目視によるコードレビューは、アプリケーションの設計・実装・セキュリティ対策の利用を確認するため、ソースコードの目視探索と手動解析で構成されています。ツールの使用については、ソースコードエディタや IDE の様な一般的に入手可能なツールを想定します。検査対象は、このレベルのセキュリティアーキテクチャの要件によって規定されます。

L2B.1 「検査に関する詳細要件」の章に記載されているレベル 2B の要件に則って、目視によるコードレビューが行われている（レベル 2 での新規追加要件）。

検査者は、セキュリティ対策の効果的な利用を確立するため、適切なサンプリング手法を用いることができます。検査者は、検出脆弱性について、ソフトウェアのベースラインにおける当該脆弱性を非公開にして検出し改修出来るように、文書化することを選択できます。また、検出された脆弱性が、発現原因箇所が同一であり、脆弱性のカテゴリを一種類に集約できる場合、単一の検出結果として統合します。

## レベル 3 - 設計に関する検査

レベル 3（設計検査）は、大規模な法人間取引を行うアプリケーションに適切な検査です。例えば、保健医療情報、重要な又は機密性の高い業務、機密性の高い資産を扱うアプリケーション等です。脅威としては、ウィルス、ワーム、オポチュニスト、さらには狙いを最初から定めている攻撃者（ターゲットを特定して、技術レベルもモチベーションも高い攻撃者で、目的に合わせて構築したスキャンツールなどを用いている攻撃者）が挙げられます。

検査対象には、構築又は改変された全ソースコードに加えて、セキュリティ機能を備えたサードパーティ製の全コンポーネントが含まれます。レベル 3 ではセキュリティ対策が正常に機能しているか、セキュリティ対策がアプリケーション固有のポリシー実施に適切な箇所で使われているかを確認します。レベル 3 はレベル 1 及び 2 と違い、構成要素は單一です（下図参照）。



図 7 - OWASP ASVS レベル 3

以下は、レベル 3 の最小限の概要要件です。

#### 検査対象

- L3.1 検査対象は、アプリケーション構築のために開発・改修された全てのソースコードを含む（レベル 1 からの継続要件）。
- L3.2 検査対象は、サードパーティ製フレームワーク、ライブラリ、サービスで、アプリケーションのセキュリティ機能を担う全てのソースコード（レベル 2 からの継続要件）。
- L3.3 検査対象は、サードパーティ製フレームワーク、ライブラリ、サービスで、アプリケーション全てのソースコード（レベル 3 での新規追加要件）。

#### セキュリティ対策の決定に関する要件

- L3.4 セキュリティチェックに関する技術的セキュリティ対策は、全てホワイトリストによって決定されている（レベル 2 からの継続要件）。
- L3.5 「検査に関する詳細要件」の章で規定されているレベル 2A と 2B の要件に則って、セキュリティチェック及びセキュリティ実施効果をもたらすセキュリティ対策を必ず実施する（レベル 2 からの継続要件）。

#### セキュリティ対策の利用に関する要件

- L3.6 「検査に関する詳細要件」の章で規定されているレベル 2 の要件に則って、サーバサイドにおいて、セキュリティ対策が必要な箇所に適切に用いられており、実装が集中管理されている（レベル 2 からの継続要件）。

#### セキュリティ対策の実装に関する要件

- 無し レベル 3 では、セキュリティ対策の実装方法についての要件は無い。

#### セキュリティ対策の検査に関する要件

- L3.7 「検査に関する詳細要件」の章で規定されているレベル 3 の要件に則って、アプリケーションに対して手動のペネトレーションテストを実施する（レベル 2 からの継続要件）。
- L3.8 セキュリティ設計の文書化を行い、設計と脅威モデリング（訳注）によるセキュリティ対策が適切に行われているかを同文書によって確認する（レベル 3 からの新規追加要件）。

#### 報告における要件

- L3.9 各コンポーネントを整理してアプリケーションのセキュリティ構造を詳しく記述し、脅威モデリング情報を含むより上位のアーキテクチャ内に「報告に関する要件」の章の要件に則った検査結果を記載した検査報告書を作成する（レベル 2 からの継続要件）。



レベル3では、アプリケーションのコンポーネントとは、ソースファイル、ライブラリー、より上位のアーキテクチャにグループ分けされる実行ファイル（例：Model-View-Controller (MVC)、ビジネスロジックやデータレイヤーのコンポーネント）として定義します。レベル3においては、脅威エンジニア（訳注：広い意味で脅威を与える人、集団、もの）及び資産に関する脅威モデル情報をサポートすることが追加されています。エンドユーザのリクエストによるアプリケーションのパスをアプリケーション概要として文書化します。またレベル3ではアプリケーション概要で確認出来る全てのパスを精査する必要があります。

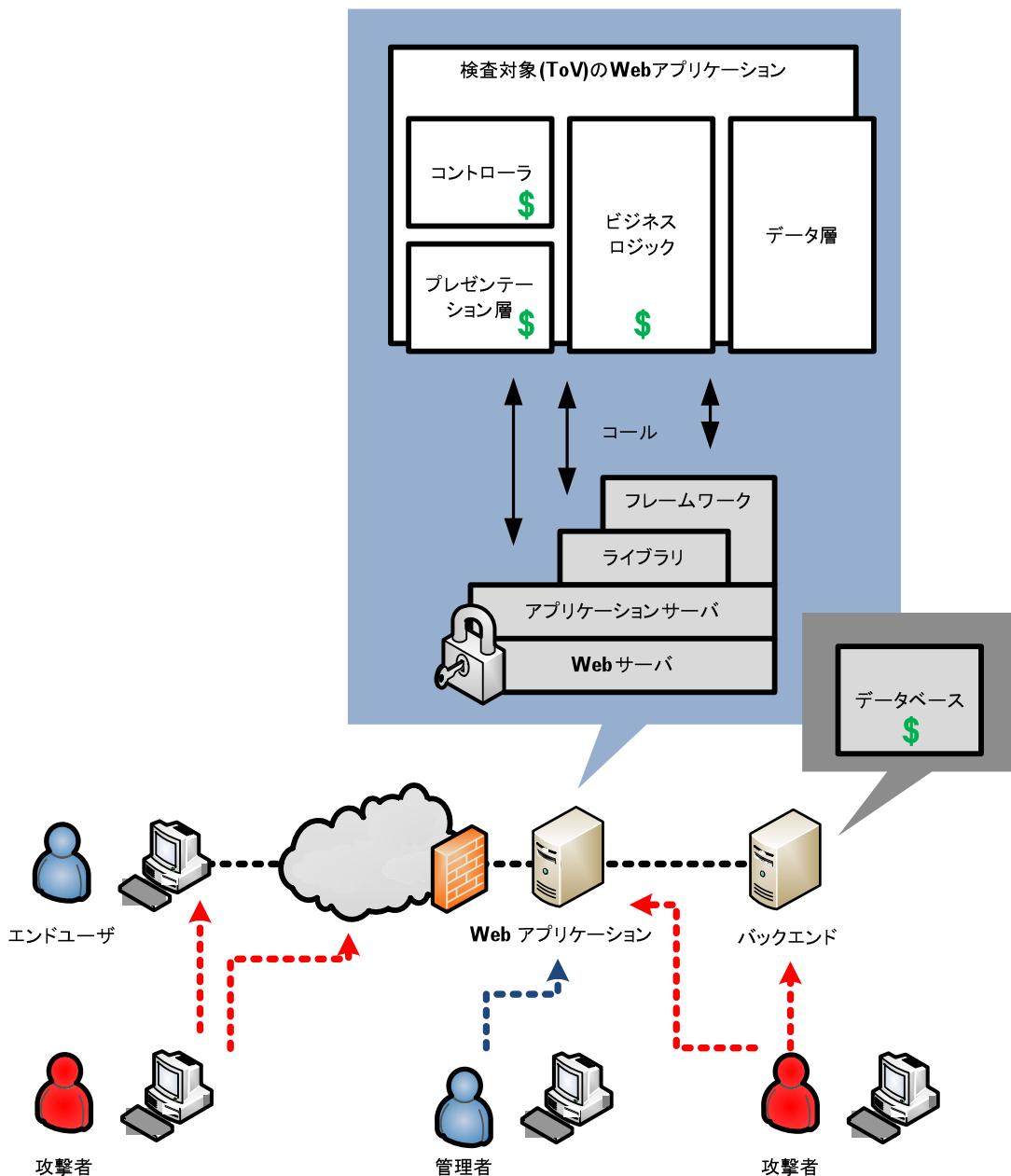


図 8 - OWASP ASVS レベル 3 セキュリティアーキテクチャの例<sup>10</sup>

<sup>10</sup> Dollar signs indicate assets in the diagram.



## Level 4 - 内部検査

レベル4（内部検査）は、人命・安全、重要なインフラ、安全保障を守る非常に重要なアプリケーションに対して適用されます。レベル4はまたは、機密資料・重要な資産を取り扱うアプリケーションにも適用されます。レベル4では、セキュリティ対策自体が正常に稼働しているか、セキュリティ対策がアプリケーション固有のポリシー実施に適切な箇所で使われているか、そしてセキュアコーディングが実施されているかどうかを確認します。脅威としては、狙いを最初から定めている攻撃者（ターゲットを当初より特定し、技術を備え、モチベーションの十分に高い攻撃者で、攻撃対象に合わせて構築したスキャンツールなどを用いている攻撃者）が挙げられます。

検査対象には、レベル3の対象に加えて、アプリケーション全コードが含まれます。レベル4は単一の構成要素です（下図参照）。



図 9 - OWASP ASVS レベル4

以下は、レベル4の要件の最低限の標準です。

### 検査対象

- L4.1 アプリケーション構築のために開発・改修された全てのソースコード（レベル1からの継続要件）。
- L4.2 検査対象は、サードパーティ製フレームワーク、ライブラリ、サービスで、アプリケーションのセキュリティ機能を担う全てのソースコード（レベル2からの継続要件）
- L4.3 サードパーティ製フレームワーク、ライブラリ、アプリケーションのサービス全てのソースコード（レベル3からの継続要件）。
- L4.4 アプリケーションに関連づけられている残り全てのソースコード、フレームワーク、ライブライバー、ランタイム実行環境、開発ツール、ビルドツール、デプロイ用ツールを含む。なお対象には、公的な精査を十分に受けているため、プラットフォームとなるソフトウェア（アプリケーションサーバ、データベースサーバ、バーチャルマシン、OSは含まれない（レベル4での新規追加要件）。

### セキュリティ対策の決定に関する要件

- L4.5 セキュリティチェックに関する技術的セキュリティ対策は、全てホワイトリストを用いた明示的な手法により決定されている（レベル2からの継続要件）。
- L4.6 「検査に関する詳細要件」の章で規定されているレベル2Aと2Bの要件に則って、セキュリティチェック及びセキュリティ実施効果をもたらすセキュリティ対策を必ず実施する（レベル2からの継続要件）。



### セキュリティ対策の利用に関する要件

- L4.7 「検査に関する詳細要件」の章で規定されているレベル4の要件に則って、サーバサイドにおいて、セキュリティ対策が必要な箇所に適切に用いられており、実装が集中管理されている（レベル3からの継続要件）。

### セキュリティ対策の実装に関する要件

- L4.8 「検査に関する詳細要件」の章で規定されているレベル4の要件に則って、アプリケーションに悪意のあるコードが存在しないことを検査する（レベル4での新規追加要件）

### セキュリティ対策の検査に関する要件

- L4.9 「検査に関する詳細要件」の章で規定されているレベル4の要件によって、アプリケーションが手動で検査されている（レベル3の要件を強化した要件）。
- L4.10 セキュリティアーキテクチャの文書化を行い、設計と脅威モデリングによるセキュリティ対策が適切に行われているかを同文書によって確認する（レベル3からの継続要件）
- L4.11 「検査に関する詳細要件」の章で規定されているレベル4の要件に則って、製造・改修された全ソースコードにおいて悪意のあるコードが含まれていないかどうかを目視でレビューする（レベル4での新規追加要件）。

### 報告における要件

- L4.12 レベル3の要件に則ってアプリケーションのセキュリティ対策を記述する報告書を作成する。報告書には、全ソースコードを記述し、「報告に関する要件」の章の要件に則った検査結果を記載する（レベル3の要件を強化した要件）。

レベル4では、アプリケーションのアーキテクチャの定義はレベル3と同一です。レベル4ではそれに加えて、レベル3では明確に精査対象となっていないコードを含む全アプリケーションコードが検査対象に含まれます（下図参照）。このコードには、全ライブラリ、フレームワーク、アプリケーションが依拠する補助的なコードを含みます。コンポーネントに対して以前に行った検査は、次の検査において再利用できます。OS、バーチャルマシン、バーチャルマシンのコアライブラリ、Webサーバ、アプリケーションサーバなどのプラットフォームに関わるコードはレベル4では含まれません。例えば、Javaランタイムに関連づけられているライブラリはレベル4では対象となりません。

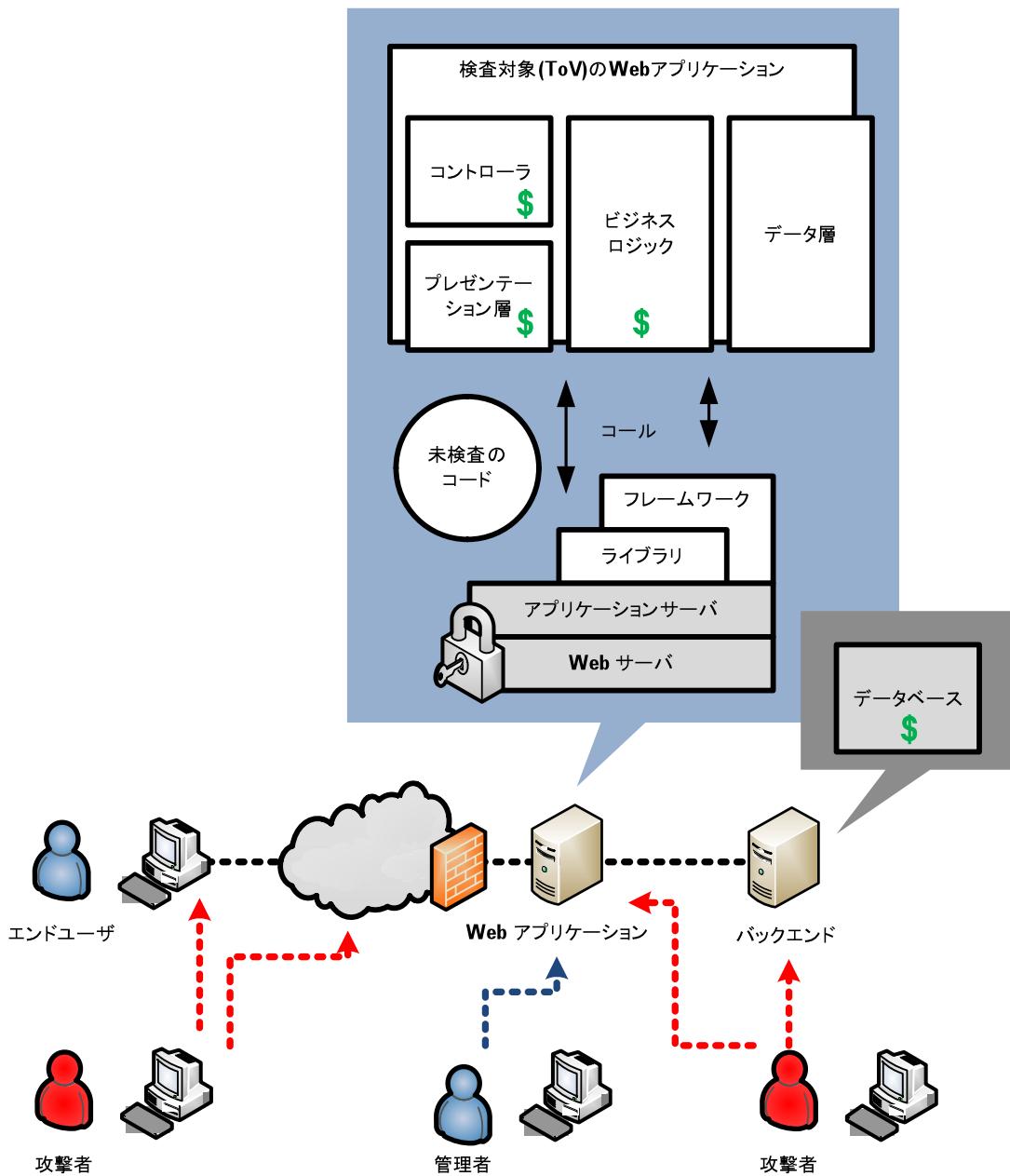


図 10 - OWASP ASVS レベル 4 未検査のコード例

### 要件の解釈と参考例について

OWASP ASVS は常に改善される文書です。この標準によってアプリケーションセキュリティの検査を実施する場合、下記の OWASP ASVS プロジェクトのページの記事を必ず確認して下さい。  
[http://www.owasp.org/index.php/ASVS#Articles\\_Below\\_-\\_More\\_About\\_ASVS\\_and\\_Using\\_It](http://www.owasp.org/index.php/ASVS#Articles_Below_-_More_About_ASVS_and_Using_It) . OWASP ASVS プロジェクトのページでは、要件の説明、実例における要件の評価、有用なヒントなどの記事を掲載しています。



## 検査に関する詳細要件

この章では、OWASP アプリケーションセキュリティ検査標準（Application Security Verification Standard (ASVS)）の検査に関する詳細要件を定義しています。これら詳細要件は、各レベルの概要要件を基にして定義されています。下記の各セクションは、関連エリアによってグループ分けされた検査に関する詳細要件を定義しています。

ASVS では下記範囲の要件を設定しています。

- V1. セキュリティ設計 Security Architecture
- V2. 認証 Authentication
- V3. セッション管理 Session Management
- V4. アクセス制御 Access Control
- V5. 入力のバリデーション Input Validation
- V6. 出力のエンコーディング／エスケープ Output Encoding/Escaping
- V7. 暗号化 Cryptography
- V8. エラー処理及びログ記録 Error Handling and Logging
- V9. データ保護 Data Protection
- V10. 通信のセキュリティ Communication Security
- V11. H T T P のセキュリティ HTTP Security
- V12. セキュリティ関連の設定 Security Configuration
- V13. 悪意のあるコードの検出 Malicious Code Search
- V14. 内部のセキュリティ Internal Security

上記各エリアにおいて、各レベル毎の検査要件は下記の通りです。

### Level 1: 自動検査

- Level 1A - 動的スキャン (部分的な自動化検査)
- Level 1B - ソースコードスキャン (部分的な自動検査)

### Level 2: 手動検査

- Level 2A - セキュリティテスト (部分的な手動検査)
- Level 2B - コードレビュー (部分的な手動検査)

### Level 3: 企画設計の検査

### Level 4: 内部の検査



## V1 - セキュリティアーキテクチャの文書化に関する要件

全 ASVS のレベルにおいて、基本的なセキュリティ設計情報を文書化することが、実施したセキュリティ検査の網羅性と正確性（及び対処策が必要な場合は再現性）を確定する上で必要です。分析は手順に沿って管理され、結果はアプリケーションのセキュリティ面の上位レベルのアーキテクチャへ遡ることが出来ます。セキュリティアーキテクチャの基本的なレベルから始めて、レベルが上がるごとに詳細な内容を文書化していきます。各レベル毎ごとの要件は下表の通りです。

Table 1 - OWASP ASVS セキュリティアーキテクチャに関する要件 (V1)

検査要件	Level 1A	Level 1B	Level 2A	Level 2B	Level 3	Level 4
V1.1 アプリケーションの全てのコンポーネント（ソースファイル、ライブラリー、実行ファイル）は個別に確認している。	✓	✓	✓	✓	✓	✓
V1.2 アプリケーションの一部ではないが、アプリケーションが参照するコンポーネントを個別に確認する。			✓	✓	✓	✓
V1.3 アプリケーションの概要アーキテクチャが定義づけられている。 <sup>11</sup>			✓	✓	✓	✓
V1.4 全てのコンポーネントが業務上の機能又はセキュリティ上の機能によって定義づけられている。					✓	✓
V1.5 アプリケーションの一部ではないが、アプリケーションが参照するコンポーネントが業務上の機能又はセキュリティ上の機能によって定義づけられている。					✓	✓
V1.6 脅威モデルの情報が提供されている。					✓	✓

<sup>11</sup> The verifier may create or document a high-level design if the application developer does not provide one.



## V2 - 認証に関する検査要件

認証に関する検査要件とは、アカウント情報が安全に生成・処理されているかを確認する要件です。各レベルごとの要件は下表の通りです。

表 2 - OWASP ASVS 認証に関する要件 (V2)

検査要件	Level 1A	Level 1B	Level 2A	Level 2B	Level 3	Level 4
V2.1 自由なアクセスを意図していない全てのページ及びリソースに認証がかかっている。	✓	✓	✓	✓	✓	✓
V2.2 パスワードフィールドにはユーザのパスワードがそのまま表示されない設定になっている。また、パスワードフィールドとそれを含むフォームの両方のオートコンプリート機能がオフになっている。	✓	✓	✓	✓	✓	✓
V2.3 許可された認証回数の上限を超えた場合に、ブルートフォース攻撃を防止できる期間、アカウントロックがかかる	✓		✓	✓	✓	✓
V2.4 全ての認証管理がサーバ側で行われる。			✓	✓	✓	✓
V2.5 外部認証サービスを利用しているライブラリを含む全ての認証制御が集中実装されている。				✓	✓	✓
V2.6 認証失敗の場合の安全対策を施している。			✓	✓	✓	✓
V2.7 実働環境における典型的な脅威に対して、認証の証明が十分な対策を施している			✓	✓	✓	✓
V2.8 全てのアカウント管理機能は、基礎的な認証メカニズムとしての機能を備えており攻撃に耐えうる			✓	✓	✓	✓
V2.9 ユーザが認証情報を変更する機能は、基礎的な認証メカニズムとしての機能を備えており攻撃に耐えうる。			✓	✓	✓	✓
V2.10 個々のアプリケーションが重要情報を扱う処理を行う際には、認証を再度行う。			✓	✓	✓	✓



V2.11 管理者が設定した期間を過ぎた認証証明は、確実に失効している。			✓	✓	✓	✓	✓
V2.12 全ての認証関連の処理が記録されている。				✓	✓	✓	✓
V2.13 アカウントのパスワードは salt 化し、各 salt にはそのアカウント固有のものを利用する (例：内部ユーザ ID とアカウント生成)。さらに保管する前にハッシュ化する。				✓	✓	✓	✓
V2.14 外部サービスにアクセスする認証証明は暗号化されて、ソースコードではなく、安全対策の施された環境で保管されている。				✓	✓	✓	✓
V2.15 実行される全ソースコード及び認証機能は悪意のあるコードの影響を受けない。							✓

### V3 - セッション管理に関する検査要件

セッション管理に関する検査要件は、セッションの管理を適切に行うための、HTTP リクエスト・レスポンス、セッション、クッキー、ヘッダー、ログ記録の安全な使用を確認する要件です。各レベルごとの要件は下表の通りです。

表 3 - OWASP ASVS セッション管理に関する要件 (V3)

Verification Requirement	Level 1A	Level 1B	Level 2A	Level 2B	Level 3	Level 4
V3.1 フレームワークがデフォルトとして持っているセッション管理機能をアプリケーションが実行している。	✓		✓	✓	✓	✓
V3.2 ログアウト時にセッションを無効化している。	✓		✓	✓	✓	✓
V3.3 ある一定の期間でセッションがタイムアウトする。	✓		✓	✓	✓	✓
V3.4 管理者が設定した時間になると、利用者がログイン状態であってもセッションタイムアウトとなる機能（絶対タイムアウト機能）を備えている。					✓	✓
V3.5 認証が必要となる全ページに、ログアウトのリンクがある。	✓		✓	✓	✓	✓



V3.6	クッキーのヘッダ以外ではセッション ID は非表示にする。特に URL、エラーメッセージ、ログでの非表示を確認する。セッションのクッキーによる URL リライティングをサポートしない。		✓		✓	✓	✓
V3.7	セッション ID はログインのたびに変更される。			✓	✓	✓	✓
V3.8	セッション ID は再度認証を行う際に変更される。			✓	✓	✓	✓
V3.9	セッション ID はログアウトの際には変更するか消去する。			✓	✓	✓	✓
V3.10	アプリケーションのフレームワークで生成したセッション ID のみを有効と認識する。			✓		✓	✓
V3.11	認証されたセッショントークンは、実働環境に対する一般的な攻撃に対して十分に耐えうるように、長さとランダムさを備えている。					✓	✓
V3.12	認証されたセッショントークン/ID を含むクッキーは、該当サイトのみに限定されたドメインとパスを適切に設定して保持する。					✓	✓
V3.13	実装された全ソースコード及びセッション管理機能は悪意のあるコードの影響を受けない。						✓

#### V4 - アクセスコントロールに関する検査要件

アクセスコントロールに関する検査要件は、アプリケーションのアクセスコントロールの安全性を確認する要件です。一般的にアクセス制御は、様々なアプリケーションレイヤーでそれぞれ違う場所で実施しています。この要件は、URL、業務上の機能、データ、サービス、ファイルに対するアクセスコントロールに関する検査要件です。各レベルごとの要件は下表の通りです。



表 4 - OWASP ASVS アクセス制御に関する要件 (V4)

検査要件	Level 1A	Level 1B	Level 2A	Level 2B	Level 3	Level 4
V4.1 ユーザは、認証されていない機能にはアクセスできない。	✓	✓	✓	✓	✓	✓
V4.2 ユーザは、認証されていない URL にはアクセスできない。	✓		✓	✓	✓	✓
V4.3 ユーザは、認証されていないデータファイルにはアクセスできない。	✓		✓	✓	✓	✓
V4.4 直接的なオブジェクト参照は、認証されたオブジェクトだけに各ユーザがアクセスできるように保護されている。	✓		✓	✓	✓	✓
V4.5 直接ブラウジング（ディレクトリ一覧表示）は、意図的な許可が無い限り、不可能な状態となっている。	✓		✓		✓	✓
V4.6 ユーザは、認証されていないサービスにはアクセスできない。			✓	✓	✓	✓
V4.7 ユーザは、認証されていないデータにはアクセスできない。			✓	✓	✓	✓
V4.8 アクセス制御に失敗した場合に安全な処理が施されている。			✓	✓	✓	✓
V4.9 プレゼンテーション層と同じアクセス制御がサーバサイドで実行される。			✓	✓	✓	✓
V4.10 アクセス制御で利用している全ユーザー属性・データ属性及びポリシー情報をエンドユーザは特別の許可無く変更できない。			✓	✓	✓	✓
V4.11 全てのアクセス制御がサーバサイドで実施されている。			✓	✓	✓	✓
V4.12 保護されているリソースへのアクセス保護のための集中管理するメカニズムを備える。これには外部認証サービスを利用するライブラリも含む。				✓	✓	✓
V4.13 業務上規定されている入力及びアクセス制限を超えることは出来ない（例：1日の取引制限やタスクの順序変更など）			✓	✓	✓	✓
V4.14 アクセスの制御及び制御失敗が記録されている。				✓	✓	✓



V4.15 実行される全ソースコード及びアクセス制御は悪意のあるコードの影響を受けない。							✓
--	--	--	--	--	--	--	---

## V5 - 入力のバリデーションに関する検査要件

入力のバリデーション（検証）に関する検査要件は、入力値がアプリケーションにおいて安全に処理するための入力値確認に関する要件です。各レベルごとの要件は下表の通りです。

表 5 - OWASP ASVS 入力のバリデーションに関する検査要件 (V5)

検査要件	Level 1A	Level 1B	Level 2A	Level 2B	Level 3	Level 4
V5.1 ランタイム環境がバッファオーバーフローの影響をうけにくい。又はバッファオーバーフローの対策を持っている。	✓	✓	✓	✓	✓	✓
V5.2 全入力値に対してポジティブバリデーションが定義され、適用されている。	✓	✓	✓	✓	✓	✓
V5.3 全てのバリデーションが失敗した場合は、入力を拒否又は無害化する。	✓		✓	✓	✓	✓
V5.4 全ての入力ソースは、キャラクタセットを指定する（例：UTF-8）。			✓	✓	✓	✓
V5.5 全ての入力のバリデーションはサーバサイドで実施する。			✓	✓	✓	✓
V5.6 許可されるデータタイプ各々に対して、適切な入力バリデーション制御を個別に用いる。				✓	✓	✓
V5.7 全ての入力バリデーションの失敗は記録される。				✓	✓	✓
V5.8 全ての入力データは、バリデーションに先だって行われるデコードやインタープリタに引き渡す前に正規化されている。					✓	✓
V5.9 実行される全てのバリデーション制御は悪意のあるコードの影響を受けない。						✓

## V6 - 出力のエンコード／エスケープに関する検査要件



出力のエンコード／エスケープの検証に関する要件は、アプリケーションの出力を外部のアプリケーションで安全に用いるために、出力が適切に行われているかを確認する要件です。各レベルごとの要件は下表の通りです。

表 6 - OWASP ASVS 出力のエンコード／エスケープに関する検査要件 (V6)

検査要件	Level 1A	Level 1B	Level 2A	Level 2B	Level 3	Level 4
V6.1 HTML に出力される信頼性の低いデータは、HTML 要素、HTML 属性、JavaScript のデータ値、CSS のプロック、URI 属性等のコンテキストに合った適切なエスケープ処理を行う。		✓	✓	✓	✓	✓
V6.2 出力のエンコード／エスケープに関する全制御がサーバサイドに実装されている。			✓	✓	✓	✓
V6.3 出力のエンコード／エスケープに関する制御が、利用するインターフリタにおいて安全性を保証できない全ての文字をエンコードしている。				✓	✓	✓
V6.4 SQL のインターフリタに出力される信頼性の低い全データは、パラメータ化されたインターフェースか prepared statement を用いるか、又は適切なエスケープ処理をしている。				✓	✓	✓
V6.5 XML に出力される信頼性の低いデータは、パラメータ化されたインターフェースを用いるか適切なエスケープ処理をしている。				✓	✓	✓
V6.6 LDAP クエリーで用いられる信頼性の低いデータは、適切なエスケープ処理をしている。				✓	✓	✓
V6.7 OS のコマンドパラメータに含まれる信頼性の低いデータは、適切にエスケープ処理している。				✓	✓	✓
V6.8 V6.4～6.7 に含まれていない全てのインターフリタに引き渡される信頼性の低いデータは、適切にエスケープ処理している。				✓	✓	✓
V6.9 アプリケーションによる出力のエンコード／エスケープ処理が、それぞれの出力先に合わせた単一のセキュリティ制御を実施している。					✓	✓



V6.10 出力のバリデーション制御に用いられている全てのコードは悪意のあるコードの影響を受けない。							✓
--	--	--	--	--	--	--	---

## V7 - 暗号化に関する検査要件

暗号化に関する検査要件は、アプリケーションの暗号化、鍵の管理、乱数化、ハッシュ処理に関する要件です。アプリケーションは必ず FIPS140-2 の承認を受けた暗号化モジュール又は同等の標準により承認を受けたモジュールを使用しなければなりません（例：米国以外の標準等）。各レベルごとの要件は下表の通りです。

表 7 - OWASP ASVS 暗号化に関する検査要件 (V7)

検査要件	Level 1A	Level 1B	Level 2A	Level 2B	Level 3	Level 4
V7.1 ユーザから送られた機密情報の暗号化はサーバサイドに実装されている。			✓	✓	✓	✓
V7.2 全ての暗号化モジュールは、処理失敗の場合には安全に対処出来るように対策が立てられている。			✓	✓	✓	✓
V7.3 認証を通っていないアクセスからマスターの機密へのアクセスは許可されない。マスターの機密とは、セキュリティの設定情報へのアクセスを制御するディスク上にプレインテキストとして保存されているアプリケーションの認証情報を言う。				✓	✓	✓
V7.4 パスワードを生成する際には、ハッシュして salt 化する。				✓	✓	✓
V7.5 暗号化モジュールの失敗は記録しておく。				✓	✓	✓
V7.6 全ての乱数、乱数化されたファイル名や GUID、乱数化された記号文字列は、攻撃者から推測されないことを意図している場合、暗号化モジュールが許可した乱数ジェネレータを用いて乱数を生成する。				✓	✓	✓
V7.7 アプリケーションが使用する暗号化モジュールは FIPS140-2 又は同等の標準で承認されたモジュールを使用する（下記 URL を参照）。 <a href="http://csrc.nist.gov/groups/STM/cmvp/validation.html">http://csrc.nist.gov/groups/STM/cmvp/validation.html</a>					✓	✓
V7.8 暗号化モジュールがセキュリティポリシーに則って活用されている（下記 URL 参照）。 <a href="http://csrc.nist.gov/groups/STM/cmvp/validation.html">http://csrc.nist.gov/groups/STM/cmvp/validation.html</a>					✓	✓
V7.9 暗号鍵の管理運営について明確なポリシーが規定されており（例：生成、提供、廃棄、無効など）、正しく実施されている。					✓	✓



V7.10 暗号化モジュールをサポート又は利用している全ソースコードが悪意あるコードの影響を受けない。							✓
---	--	--	--	--	--	--	---

## V8 - エラー処理及びログ記録に関する検査要件

エラー処理及びログ記録に関する検査要件は、セキュリティ関連のイベント及び攻撃確認のトラッキングに関する要件です。各レベルごとの要件は下表の通りです。

表 8 - OWASP ASVS エラー処理及びログ記録に関する検査要件 (V8)

検査要件	Level 1A	Level 1B	Level 2A	Level 2B	Level 3	Level 4
V8.1 攻撃に利用される可能性のある機密データをエラーメッセージやスタッフトレースに表示しない（データ例：セッション ID や個人情報）。	✓	✓	✓	✓	✓	✓
V8.2 サーバサイドのエラーはサーバサイドで処理されている。			✓	✓	✓	✓
V8.3 ログ記録に関する制御はサーバで行っている			✓	✓	✓	✓
V8.4 セキュリティに関連したエラー処理に関するロジックへのアクセスがデフォルトで許可されていない。			✓	✓	✓	✓
V8.5 セキュリティに関するログ記録では、セキュリティに関わるイベントであれば、成功・失敗両方のログを記録できるように設定する。				✓	✓	✓
V8.6 イベントログには下記を含む： 1. 信頼できるソースからのタイムスタンプ 2. イベントの深刻度レベル 3. セキュリティに関するイベントか否かの表示 4. イベントを起こしたユーザの確認（ユーザが存在する場合） 5. イベントに関連づけられるリクエストのソース IP アドレス 6. イベントの成功または失敗 7. イベントの内容				✓	✓	✓
V8.7 信頼性の低いデータを含む全てのイベントは、ログ閲覧ソフトでのコードとして実行しない。.				✓	✓	✓



V8.8	セキュリティログは認証されていないアクセスや変更から保護されている。				✓	✓	✓
V8.9	アプリケーションに実装するログ記録は単一にする。				✓	✓	✓
V8.10	セッション ID や個人情報・機密情報は攻撃者にとって有益な情報となり得る、アプリケーション特有のデータをアプリケーションが記録しない。				✓	✓	✓
V8.11	ログ記録のフォーマットの全項目で、ログイベントを複合検索条件で検索出来るログ分析ツールを分析者が使用出来るようにする。				✓	✓	✓
V8.12	エラー処理とログ記録制御を行う全ソースコードが悪意あるコードの影響を受けない。						✓

## V9 - データの保護に関する検査要件

データ保護に関する検査要件は、機密データの保護確認に関する要件です。機密データとは、クレジットカード番号、パスポート番号、個人を特定出来る情報などです。各レベルごとの要件は下表の通りです。

表 9 - OWASP ASVS データ保護に関する検査要件 (V9)

検査要件	Level 1A	Level 1B	Level 2A	Level 2B	Level 3	Level 4
V9.1 機密情報を扱う全てのフォームがクライアントサイドでのキャッシュ（オートコンプリート機能を含む）を許可していない。	✓	✓	✓	✓	✓	✓
V9.2 アプリケーションにより処理される機密データのリストが特定されており、これら機密データへのアクセス制御に関するポリシーが明文化されており、さらにこのデータが、送信中・保存中を問わず暗号化されている。さらに、このポリシーが適切に実施されている。				✓	✓	✓
V9.3 機密データを送信するのに URL のパラメータを使用しておらず、全データを HTTP のメッセージボディでサーバに送信している。			✓		✓	✓



V9.4	クライアントに送られた機密データのキャッシュ又は一時的なコピーは、認証されていないアクセスから保護されるか、あるいは認証されたユーザが機密データにアクセスした後は無効化または除去する（例：Cache-Control headers がキャッシュの許可をしないように設定されている）。				✓	✓	✓
V9.5	サーバに保存されている機密データのキャッシュ又は一時的なコピーは、認証されていないアクセスから保護され、認証されたユーザが機密データにアクセスした後は無効化または除去する。				✓	✓	✓
V9.6	保存期間の過ぎた機密データがアプリケーションから除去されるメソッドが存在する。					✓	✓

## V10 - 通信のセキュリティに関する検査要件

通信の安全性に関する検査要件は、アプリケーションの行う全通信の保護の適切さを確認する要件です。各レベルごとの要件は下表の通りです。

表 10 - OWASP ASVS 通信のセキュリティに関する検査要件 (V10)

検査要件	Level 1A	Level 1B	Level 2A	Level 2B	Level 3	Level 4
V10.1 パスが、信頼できる CA から各 TLS (Transport Layer Security) サーバ認証を経る。また各々のサーバ認証が有効である。	✓		✓	✓	✓	✓
V10.2 TLS 通信が失敗した場合も、安全性の低い通信にフォールバックしない。			✓		✓	✓
V10.3 認証処理や、機密情報・機密機能を処理する通信は、外部通信及びバックエンド方式による通信を含めて全て TLS を使用する。				✓	✓	✓
V10.4 バックエンド TLS 通信が失敗した場合は記録する。				✓	✓	✓
V10.5 認証のパスは、トラストアンカーと失効情報を用いて、クライアント証明書を確認する。				✓	✓	✓



V10.6 機密情報・機密機能を含む外部システムとの通信には認証を用いる。				✓	✓	✓
V10.7 機密情報・機能を含む外部システムとの通信では、アプリケーション使用のための必要最小限の権限のみを持つアカウントを用いる。				✓	✓	✓
V10.8 Approved mode of operation で機能するように構成されたアプリケーションがあり、そのアプリケーションが使用する標準 TSL が実装されている（下記 P D F を参照 <a href="http://csrc.nist.gov/groups/STM/cmvp/documents/fips140-2/FIPS1402IG.pdf">http://csrc.nist.gov/groups/STM/cmvp/documents/fips140-2/FIPS1402IG.pdf</a> ）。					✓	✓
V10.9 全通信で、特定のキャラクタエンコーディングを指定している（例：UTF-8）。					✓	✓

## V11 - HTTP セキュリティに関する検査要件

HTTP セキュリティに関する検査要件は、HTTP のリクエスト、レスポンス、セッション、クッキー、ヘッダー、ログ記録のセキュリティを検査する要件です。各レベルごとの要件は下表の通りです。

表 11 - OWASP ASVS HTTP のセキュリティに関する検査要件 (V11)

検査要件	Level 1A	Level 1B	Level 2A	Level 2B	Level 3	Level 4
V11.1 リダイレクトは必ずバリデイトする。	✓	✓	✓	✓	✓	✓
V11.2 アプリケーションは定義された HTTP リクエストメソッド（例：GET と POST）のみを受け付ける。	✓	✓	✓	✓	✓	✓
V11.3 全ての HTTP レスポンスに安全なキャラクタセットを指定したコンテンツタイプヘッダを含んでいる（例：UTF-8）。	✓	✓	✓	✓	✓	✓
V11.4 JavaScript からのアクセスを必要としない全てのクッキーで、HTTPOnly フラグがたてられている。			✓	✓	✓	✓
V11.5 セッションクッキーなど機密情報を含む全てのクッキーにセキュアフラグがたてられている。			✓	✓	✓	✓



V11.6 リクエスト・レスポンス両方の HTTP ヘッダに印刷可能な ASCII キャラクタが使用されている。			✓	✓	✓	✓
V11.7 機密データに関する全リンクとフォームの一部として、アプリケーションが強力な乱数性を持つトークンを生成し、さらに、実際のユーザのリクエストを処理する際に、ユーザの属性値の存在を確認する。 <sup>12</sup>					✓	✓

## V12 - セキュリティ設定に関する検査要件

セキュリティの設定に関する検査要件は、アプリケーションのセキュリティに関する処理を決める全設定情報を保存する際の安全性を確認する要件です。設定情報の保護は、アプリケーションの安全なオペレーションに不可欠です。各レベルごとの要件は下表の通りです。

表 12 - OWASP ASVS セキュリティ設定に関する検査要件 (V12)

検査要件	Level 1A	Level 1B	Level 2A	Level 2B	Level 3	Level 4
V12.1 セキュリティに関する全ての設定情報が、認証の無いアクセスから保護された場所で保存されている。				✓	✓	✓
V12.2 セキュリティの設定情報にアクセス出来ない場合は、アプリケーションに対する全てのアクセスを拒否する。				✓	✓	✓
V12.3 アプリケーションによるセキュリティ設定の全変更が、セキュリティイベントログに記録保存されている。					✓	✓
V12.4 保存されている設定が、監査を容易にするために、人間が読解可能な形で出力できる。						✓

## V13 - 悪意のあるコードの探索に関する検査要件

レベル 4 では、レベル 3 までの要件では調査されていない全ソースコードを対象として、悪意のあるコードを探索する必要があります。各レベルごとの要件は下表の通りです。

表 13 - OWASP ASVS 悪意のあるコードの探索に関する検査要件 (V13)

<sup>12</sup> This requirement describes the mechanism required to defend against Cross Site Request Forgery (CSRF) attacks.



検査要件	Level 1A	Level 1B	Level 2A	Level 2B	Level 3	Level 4
V13.1 アプリケーション構築において、開発または改修された全てのコードに悪意のあるコードが含まれていない。 <sup>13</sup>						✓
V13.2 インターブリタされたコード、ライブラリ、実行ファイル、設定ファイルがチェックサム又はハッシュで確認する。						✓

## V14 - 内部セキュリティに関する検査要件

内部セキュリティに関する検査要件は、実装上の不備に対するアプリケーション自身の保護・対策を検査する要件です。各レベルごとの要件は下表の通りです。

表 14 - OWASP ASVS 内部セキュリティに関する検査要件 (V14)

検査要件	Level 1A	Level 1B	Level 2A	Level 2B	Level 3	Level 4
V14.1 アプリケーションが、ユーザとそのユーザに属するデータ及びアクセス制御に関するポリシー情報を認証されていないアクセス又は改ざんから保護する。					✓	✓
V14.2 セキュリティ制御のインターフェースは、開発者が簡単に正確に使用できるように、扱いやすいものである。						✓
V14.3 アプリケーションが、不適切な並行アクセスから共有変数及び共有リソースを保護する。						✓

<sup>13</sup> E.g. examine system clock calls to look for time bombs, functions unrelated to business requirements for back doors, execution paths for Easter eggs, financial transactions for incorrect logic that may indicate a salami attack, other types of malicious code.



## 検査報告書に関する要件

OWASP ASVS の報告書には、OWASP ASVS の要件によって解析されたアプリケーションに関して記載されます。また、検出された脆弱性に対する対処方法を含めて、解析結果も記載します。

ASVS の報告書に関する要件は、報告書の各種記載事項を要件として設定しています。当要件では、構造やフォーマットなどについては規定していません。また、追加の情報を記載することを除外することもありません。

ASVS の検査報告書に関する要件に含まれる情報の種類は、認証側の要件に応じて、名前、フォーマット、構成手法が違う場合もあります。当要件では、情報が存在すれば良いのです。報告書には、解析内容とその結果を読み手が理解し易くするための全内容が含まれます。記載内容には、報告書の概要を作成する際に用いる可能性のある設定情報やコードスニペット等も含まれます（右図参照）。

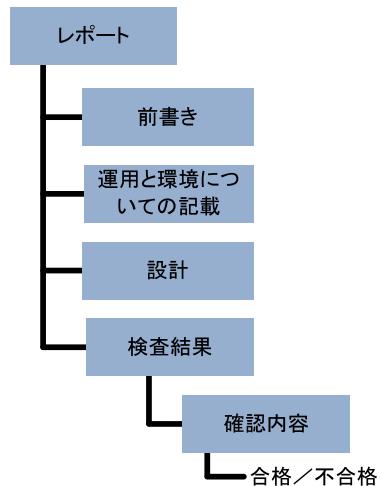


図 11 - 報告書の内容

### R1 - イントロダクション

- R1.1 報告書の対象となるアプリケーションと報告書自体の情報を記載する。
- R1.2 アプリケーションのセキュリティという観点から見た信頼性について要約する。
- R1.3 アプリケーションの運営上存在する主要な業務上のリスクを明確にする。
- R1.4 検査に当たって同意した契約上の規則及び検査対象に制約を加えることとなったものについて明記する。

### R2 - アプリケーションに関する記載

- R2.1 アプリケーションに関しては、アプリケーションの運用内容とその運用環境について十分に理解出来るように記載する。

### R3 - アプリケーションのセキュリティ設計

- R3.1 アプリケーションのセキュリティ設計については、解析が完結しており正確であることを読み手が理解する第一歩として、アプリケーションの詳細についての情報を追記する。この章で、解析の背景・状況を記載する。この章での記載事項は、現状と設計上の不一致を明確にする。また、この章における記載詳細は、ASVS の設定レベルによって記載内容は変化する。



## R4 - 検査結果

R4.1 検査要件の章に則って実施された解析結果及び検出脆弱性の対処方法を記載する。詳細は下記の通り

表 15 - OWASP ASVS 検査報告書の記載内容

Level	脆弱性の検出が無い場合	脆弱性を検出した場合
Level 1 Results	<ul style="list-style-type: none"><li>判断・評価</li><li>ツール設定（ツールがチェック可能であった場合）又は評価の正当性に関する説明（完全性と正確性の論拠、特定の事実）</li><li>検査要件詳細において自動化ツールが適用できた範囲のマッピング</li><li>ツール設定内容及び報告書の容器細事高としてのツールの適用範囲に関するマッピング</li></ul>	<ul style="list-style-type: none"><li>判断・評価</li><li>場所 (URL とパラメータ・ソースファイルのパス、名前、行番号)</li><li>解説（必要な場合は設定情報）</li><li>リスク評価<sup>14</sup></li><li>リスクの正当性に関する説明</li></ul>
ツール設定及びツール適用範囲		
Levels 2 - 4 Results	<ul style="list-style-type: none"><li>評価</li><li>評価の正当性に関する説明（完全性と正確性の論拠、特定の事実）</li></ul>	<ul style="list-style-type: none"><li>評価</li><li>場所 (URL とパラメータ・ソースファイルのパス、名前、行番号)</li><li>解説（アプリケーションコンポーネントのパス及び再現の手順）</li><li>リスク評価（OWASP Risk Rating Methodology 参照）</li><li>リスクの正当性に関する説明</li></ul>

<sup>14</sup> For more information about identifying risks and estimating risks associated with vulnerabilities, see the *Testing Guide* (OWASP, 2008).



## 用語解説

(訳注1：本標準本文では、原文の意図を正確にくみ取りつつ自然な日本語の文章にするために、一語一句の置き換えを避けました。しかし用語解説では、原著者の意図にフィルタをかけないためと、自然な日本語にするために書き直すと日本語でゼロから書き直すことと変わらなくなってしまうため、一語一句を極力はみ出さない直訳に近い文章にしました。固有名詞以外のほとんどの用語は、日常的な技術用語かインターネットで簡単に解説をみつける事ができる用語です)

(訳注2：原文にはありませんが、下記解説の用語の中で本用語解説で解説が行われている用語については下線を引きました)

**アクセス制御 (Access Control)** - ファイル、参照された機能、URL、データへのアクセスを属するグループ又は個人確認によって制限する手段。

**アプリケーションコンポーネント (Application Component)** - 検査者によって特定のアプリケーションとして確認された複数又は単一のソースファイル、ライブラリ、実行ファイル。

**アプリケーションセキュリティ - OS やネットワークよりも Open Systems Interconnection Reference Model (OSI Model) のアプリケーション層を構成しているコンポーネントの分析に重点をおくセキュリティ。**

**アプリケーションセキュリティ検査 - OWASP ASVS** に沿ったアプリケーションの技術的な評価

**アプリケーションセキュリティ検査報告書 (Application Security Verification Report)** - 特定のアプリケーションに対して検査者が行った分析と全体の結果を文書化した報告書

**アプリケーションセキュリティ検査標準 (Application Security Verification Standard (ASVS)) - OWASP の標準で、アプリケーションのセキュリティ検査を 4 レベルに定義している。**

**認証 (Authentication)** - アプリケーションのユーザによって要求された本人確認の検査。

**自動検査 (Automated Verification)** - 脆弱性のシグネチャを用いて問題点を検出する自動化ツールの使用。ツールは動的解析、静的解析、その両方の出来るものを含む。

**バックドア (Back Doors)** - アプリケーションの承認されていないアクセスを許す悪意のあるコード

**ブラックリスト (Blacklist)** - 許可されていない操作またはデータのリスト（例：入力データとして許可されていない文字のリスト）。

**コモンクライテリア、IT セキュリティ評価基準 (Common Criteria (CC))** - IT 製品のデザインや設置の評価確認に用いられる、様々なパートを持つ標準。

**通信のセキュリティ (Communication Security)** - アプリケーションコンポーネント間、クライアントとサーバ間、外部システムとアプリケーション間でのデータの交信におけるデータ保護

**デザイン検査 (Design Verification)** - アプリケーションのセキュリティ設計に関する技術的評価

**内部検査 (Internal Verification)** - OWASP ASVS で定義されているアプリケーションのセキュリティアーキテクチャの特定の側面に関する技術的評価



**暗号化モジュール** *Cryptographic module* - 暗号のアルゴリズムの実装・暗号鍵の生成を行うハードウェア・ソフトウェア・ファームウェア。

**DOS 攻撃** *(Denial of Service (DOS) Attacks)* - アプリケーションの許容量以上のリクエストを行う事によりオーバーフローさせる攻撃

**動的検査** *(Dynamic Verification)* - アプリケーションを実行して脆弱性のシグネチャを用いて問題点を検出する自動化ツールの利用する検査

**イースターエッグ** *(Easter Eggs)* - 悪意あるコードの一種で、ある特定の入力イベントが行われるまで実行されない。

**外部システム** *(External Systems)* - アプリケーションの一部ではないサーバサイドのアプリケーションまたはサービス

**FIPS 140-2 - 暗号化モジュール**の設計及び実装の検査の基礎として用いられる標準

**入力のバリデーション** *(Input Validation)* - 信頼されていないユーザからの入力の検証とカノニカル化（正規化）

**悪意のあるコード、マルコード** *(Malicious Code)* - アプリケーションの真の所有者に知らないよう アプリケーションに導入されたコードで、そのアプリケーションに設定されたセキュリティをかいくぐる。ウィルスやワームのようなマルウェアとは違う。

**マルウェア** *(Malware)* - アプリケーションに導入された実行コードで、アプリケーションの所有者や管理者に知られることなく実行される。

**オープン Web アプリケーションセキュリティプロジェクト** *(Open Web Application Security Project (OWASP))* - The Open Web Application Security Project (OWASP) は、アプリケーション・ソフトウェアのセキュリティ向上に重点を置いた自由で公開されたコミュニティです。OWASP のミッションは、人々・団体がアプリケーションセキュリティのリスクに関して見識を持って決断を下すことが出来るように、アプリケーションセキュリティを「目に見える」ものにすることです。詳細は [www.owasp.org](http://www.owasp.org) を参照下さい。

**出力のバリデーション** *(Output Validation)* - Web ブラウザや外部システムへの出力を正規化・検証すること。

**OWASP エンタープライズセキュリティ API** *(OWASP Enterprise Security API (ESAPI))* - 開発者がセキュアな Web アプリケーションを構築する上で必要とする、無料でオープンな一連のセキュリティ手法。 詳細は <http://www.owasp.org/index.php/ESAPI> を参照下さい。

**OWASP リスク評価手法** *(OWASP Risk Rating Methodology)* - アプリケーションセキュリティにカスタマイズされたリスクの評価手法詳細は、  
[http://www.owasp.org/index.php/How\\_to\\_value\\_the\\_real\\_risk](http://www.owasp.org/index.php/How_to_value_the_real_risk) を参照下さい。

**OWASP テストガイド** *(OWASP Testing Guide)* - テストのプログラムを組織で理解することを意図した文書。 詳細は [http://www.owasp.org/index.php/Category:OWASP\\_Testing\\_Project](http://www.owasp.org/index.php/Category:OWASP_Testing_Project) を参照下さい。

**OWASP トップ 10** *(OWASP Top Ten)* - Web アプリケーションセキュリティの深刻な欠陥について幅広いコンセンサスをまとめた文書。 詳細は <http://www.owasp.org/index.php/Top10> を参照下さい。

**ポジティブ** *(Positive)* - 「ホワイトリスト」の項を参照のこと。



**サラミ攻撃 (Salami Attack)** - 悪意のあるコードの一種で、検知されないほどの少額の決済を行い金銭を移転させる。

**セキュリティ アーキテクチャ (Security Architecture)** - セキュリティ制御の手法と実装箇所を記述・確認するアプリケーションのデザインの抽象化で、同時にアプリケーションと利用者に関するデータの場所とその重要度も記述・確認する。

**セキュリティコントロール、セキュリティ制御 (Security Control)** - セキュリティチェックを行う機能やコンポーネント（例：アクセスコントロールのチェック）又はセキュリティに影響する結果を呼び出す機能やコンポーネント（例：監査記録の生成）。

**セキュリティ設定 (Security Configuration)** - セキュリティ制御の利用に影響するアプリケーションのランタイム設定

**静的検査 (Static Verification)** - アプリケーションのソースコードの問題点を脆弱性のシグネチャを用いて検知する自動化ツールの利用

**検査対象 (Target of Verification (TOV))** - OWASP ASVS の要件に則ってアプリケーションのセキュリティ検査を行う際に、検査対象となる特定のアプリケーション。TOV とも略す。

**脅威モデリング (Threat Modeling)** - 脅威エージェント、セキュリティゾーン、セキュリティ制御、重要な技術的・事業的な資産を確認するセキュリティアーキテクチャを構築していくことからなる手法。

**「時限爆弾」 (Time Bomb)** - 予め設定されて時刻または経過時間になるまで動作しない悪意あるコード

**検査者 (Verifier)** - OWASP ASVS の要件に沿ってアプリケーションをレビューする個人又はグループ。

**ホワイトリスト (Whitelist)** - 許可されているデータ又は操作のリスト（例：入力のバリデーションで許可されている文字のリスト）





## さらにセキュリティのレベルを上げるために

OWASP は Web アプリケーションセキュリティの分野で著名なサイトです。OWASP では多くのプロジェクト、フォーラム、ブログ、プレゼンテーション、ツール、論文を扱っています。さらに OWASP では、年に 2 回、Web アプリケーションセキュリティに関する会議を開催しており、その他 80 を超える支部があります。OWASP ASVS プロジェクトのページは <http://www.owasp.org/index.php/ASVS> です。

下記の OWASP プロジェクトは、この標準の利用者・適用者にとって有用なプロジェクトです。

- OWASP Top10 プロジェクト [http://www.owasp.org/index.php/Top\\_10](http://www.owasp.org/index.php/Top_10)
- OWASP コードレビューガイド - [http://www.owasp.org/index.php/Category:OWASP\\_Code\\_Review\\_Project](http://www.owasp.org/index.php/Category:OWASP_Code_Review_Project)
- OWASP テストガイド - [http://www.owasp.org/index.php/Testing\\_Guide](http://www.owasp.org/index.php/Testing_Guide)
- OWASP エンタープライズセキュリティ API (ESAPI) プロジェクト - <http://www.owasp.org/index.php/ESAPI>
- OWASP 法務プロジェクト - [http://www.owasp.org/index.php/Category:OWASP\\_Legal\\_Project](http://www.owasp.org/index.php/Category:OWASP_Legal_Project)

同様に、下記の Web サイトも有用です。

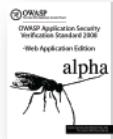
- OWASP - <http://www.owasp.org>
- MITRE - 一般的な弱点の一覧- 脆弱性のトレンド, <http://cwe.mitre.org/documents/vuln-trends.html>
- PCI セキュリティ標準委員会 PCI 標準の作成団体で、クレジットカードの処理・保持に関連する全ての組織に関連します <https://www.pcisecuritystandards.org>
- PCI データセキュリティ標準(DSS) v1.1 - [https://www.pcisecuritystandards.org/pdfs/pci\\_dss\\_v1-1.pdf](https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf)

THE BELOW ICONS REPRESENT WHAT OTHER VERSIONS ARE AVAILABLE IN PRINT FOR THIS TITLE BOOK.

**ALPHA:** "Alpha Quality" book content is a working draft. Content is very rough and in development until the next level of publication.

**BETA:** "Beta Quality" book content is the next highest level. Content is still in development until the next publishing.

**RELEASE:** "Release Quality" book content is the highest level of quality in a books title's lifecycle, and is a final product.



**ALPHA**  
PUBLISHED



**BETA**  
PUBLISHED



**RELEASE**  
PUBLISHED

YOU ARE FREE:



to **share** - to copy, distribute and transmit the work



to **Remix** - to adapt the work

UNDER THE FOLLOWING CONDITIONS:



**Attribution.** You must attribute the work in the manner specified by the author or licensor (but not in any way that suggests that they endorse you or your use of the work).



**Share Alike.** - If you alter, transform, or build upon this work, you may distribute the resulting work only under the same, similar or a compatible license.



The Open Web Application Security Project (OWASP) is a worldwide free and open community focused on improving the security of application software. Our mission is to make application security "visible," so that people and organizations can make informed decisions about application security risks. Everyone is free to participate in OWASP and all of our materials are available under a free and open software license. The OWASP Foundation is a 501c3 not-for-profit charitable organization that ensures the ongoing availability and support for our work.

On the cover: Braconid wasps are beneficial parasites. Braconids parasitize a broad range of hosts: caterpillars, flies, wasps, beetles, and aphids. After a female injects an egg into a host, the larva feeds slowly on that single host. By the time the host dies, the larva is fully grown. It pupates inside or near the dead host, sometimes in a silken cocoon, to emerge later as an adult wasp.