Akamai

ホワイトペーパー

OWASP トップ 10

Akamai は一般的な脆弱性をどのように緩和するのか

概要

OWASP（Open Web Application Security Project）トップ 10 リストは、Web アプリケーションの最も一般的な脆弱性をまとめたものであり、そうした脆弱性に対する認知を高められるようにすることが狙いです。OWASP トップ 10 を最大限に活用するためには、セキュリティベンダーの支援によって、自社の開発業務のどの領域がどのような方法で、どの程度改善されるのかを把握する必要があります。以下の OWASP トップ 10 脆弱性の内訳では、それぞれの脆弱性の内容とともに、Akamai がエッジ・セキュリティ・ソリューション、マネージド型サービス、さらに世界最大級のインテリジェント・エッジ・プラットフォームを使用して組織の取り組みをどのようにサポートできるのかという観点から解説します。

Akamai 製品

OWASP トップ 10		Account Protector	Akamai Guardicore Segmentation	App & API Protector	Bot Manager	Enterprise Application Access	Enterprise Threat Protector	Identity Cloud	Managed Security Services	Akamai MFA	Page Integrity Manager
アクセス制御の不備	A01			✓	✓	✓		✓		✓	
暗号化の失敗	A02			✓		✓	✓				✓
インジェクション	A03			✓							
安全が確認されない不安な設計	A04			✓		✓					
セキュリティの設定ミス	A05		✓	✓	✓						
脆弱で古くなったコンポーネント	A06		✓	✓							✓
識別と認証の失敗	A07	✓		✓	✓	✓		✓		✓	
ソフトウェアとデータの整合性の不具合	A08		✓	✓			✓				✓
セキュリティログとモニタリングの失敗	A09		✓	✓		✓	✓		✓		
サーバーサイドリクエストフォージェリ（SSRF）	A10		✓	✓							

OWASP トップ 10 では、単独のリスクではなく、リスクのカテゴリーを挙げています。Akamai のソリューションは、こうしたリスクカテゴリーに複数の方法で対応します。詳細は Akamai のホワイトペーパーをご覧ください。

A01: アクセス制御の不備

> **「アクセス制御は、ユーザに対して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するものです。ポリシー適用の失敗により、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、またはユーザ制限から外れたビジネス機能の実行が引き起こされます。」**
>
> **— 出典：owasp.org**

Akamai による支援

この脆弱性に完全に対処できるよう、お客様側でアクセス制御モデルを修正していただくことが必要ですが、Akamai は、WAAP の専門知識を駆使して、このアクセス制御の不備の脆弱性を悪用しようとする攻撃ベクトルのいくつかを検知し、これらを防御することでサポートできます。

- **Enterprise Application Access** により、エンタープライズのユーザーには最小権限アクセスモデルが適用され、認証されたユーザーは権限のあるアプリケーションに限って表示とアクセスが許されることになり、ゼロトラスト・セキュリティ・モデルをサポートします。
- **Akamai MFA** は、フィッシング対抗の FIDO2 テクノロジー基準をベースとする認証サービスを提供します。
- **App & API Protector** — Akamai WAAP ソリューションは、「Referer」ヘッダーをチェックし、API に対する認証を強制して、Akamai API Gateway によるアクセス制御を強化することで、強力なブラウザー攻撃を阻止します。
- **Identity Cloud** は、エンドユーザーのデータに対してきめ細かいアクセス制御を提供し、内部ユーザーやシステムごとに最小限のアクセス権限を設定できます。
- **Bot Manager** は、自動化されたツール攻撃やログイン攻撃を阻止します。

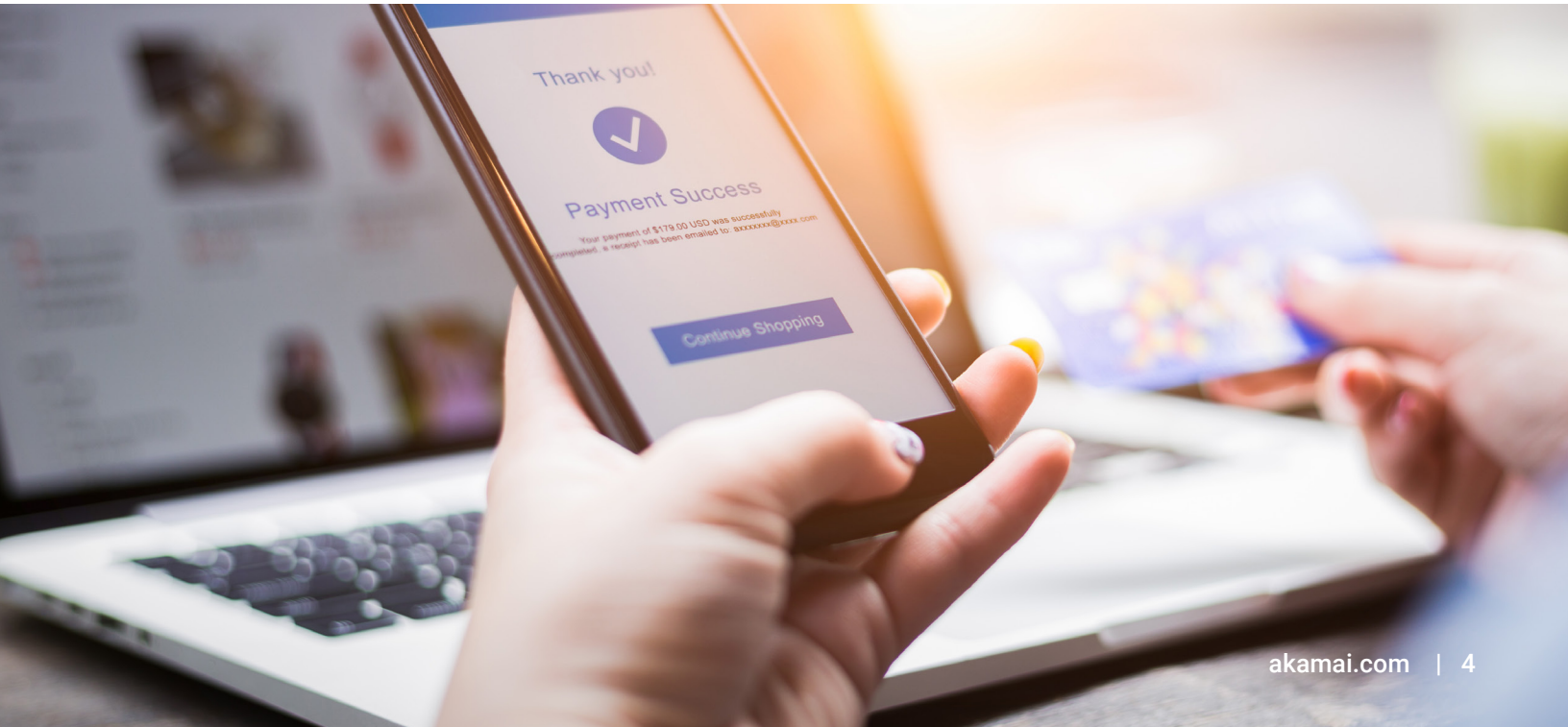
A02: 暗号化の失敗

> **「暗号化技術の不適切な使用、または暗号化の欠如に関連した幅広い障害に焦点を当てています。こうした障害は、時に機微な情報の露出を結果としてもたらします。… 例えば、パスワード、クレジットカード番号、健康記録、個人データやビジネス上の機密は特別な保護が必要になります。」**
>
> **— 出典：owasp.org**

Akamai による支援

単一のセキュリティソリューションでは、暗号化の失敗を完全に保護することはできません。ただし、さまざまなソリューションを組み合わせることで、この脆弱性のいくつかの側面に対応できます。以下に例を挙げます。

- **App & API Protector** は、最新バージョンの TLS と強力な暗号化により、伝送中の機微な情報を暗号化して保護します。また、次のような操作も支援します。
  - 安全な CDN のみからサービスを提供し、すべての主要 TLS 認証をサポートし、顧客の秘密鍵を保護することで、PCI 遵守が維持されるようにします。
  - ケージラックや動体検知など、運用上および物理的なセキュリティで保護される CDN を提供し、承認された人員のみがサーバーにアクセスできるようにします。
  - API による PII 学習で機微な情報の流出を特定し、回避します。
- **Enterprise Application Access** は、通信を暗号化し、機微な情報をネットワーク上の盗聴者から守ることで、リモートアクセスを保護します。
- **Enterprise Threat Protector** は、機微な情報の漏えいを回避できるように支援します。
- **Page Integrity Manager** は、暗号化の失敗に起因する JavaScript コードの悪用から生じる PII データ漏えいも検知します。



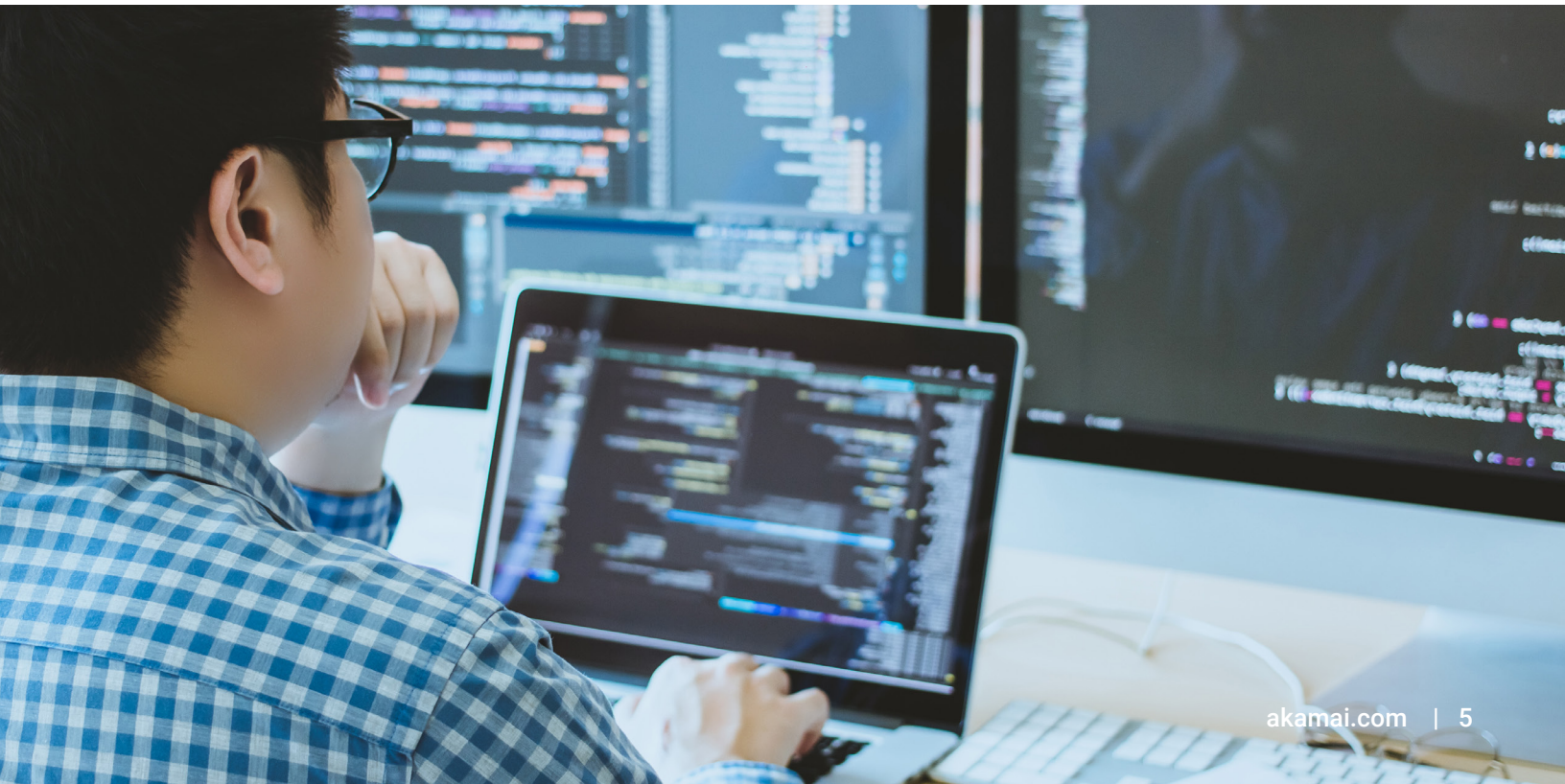
A03: インジェクション

> 「SQL、NoSQL、OS、LDAP インジェクションなどのインジェクションの欠陥は、信頼されていないデータがコマンドまたはクエリーの一部としてインタープリターに送信される際に発生します。攻撃者の悪性のデータは、インタープリターを騙すことで、意図しないコマンドの実行や適切な権限のないデータへのアクセスを達成します」
>
> — 出典：Akamai

Akamai による支援

WAAP を使用して、Web アプリケーションや API インジェクションの欠陥によるリスクを緩和できます。ただし、それぞれの開発ライフサイクルに基づいて、Web アプリケーションに脆弱性が発見されるたびに、パッチを適用する必要があります。

- **App & API Protector** は、業界トップラクスの WAAP ソリューションと Adaptive Security Engine（ASE）を提供し、そのまま適用できる既存のルールを使用してインジェクション攻撃に対する広範な保護をもたらします。ASE ペナルティボックスは、WAAP を使用してインジェクション攻撃を最近試みたクライアントからのすべてのトラフィックを一時的にブロックできます。
- カスタマイズされた WAF ルールに基づく仮想パッチは、アプリケーションにパッチが適用されるまでの間、新たなインジェクション脆弱性やアプリケーションの変更によって生じた脆弱性に対する迅速な対応を支援します。セキュリティ組織は、Akamai の API 機能を活用することで、仮想パッチを自動化して DevSecOps プロセスに統合することもできます。
- **Client Reputation** は、インジェクションベースの攻撃を検知してブロックできるように支援し、Web 攻撃者カテゴリーの非常にアクティブな悪性クライアントについてリスクスコアを提供します。



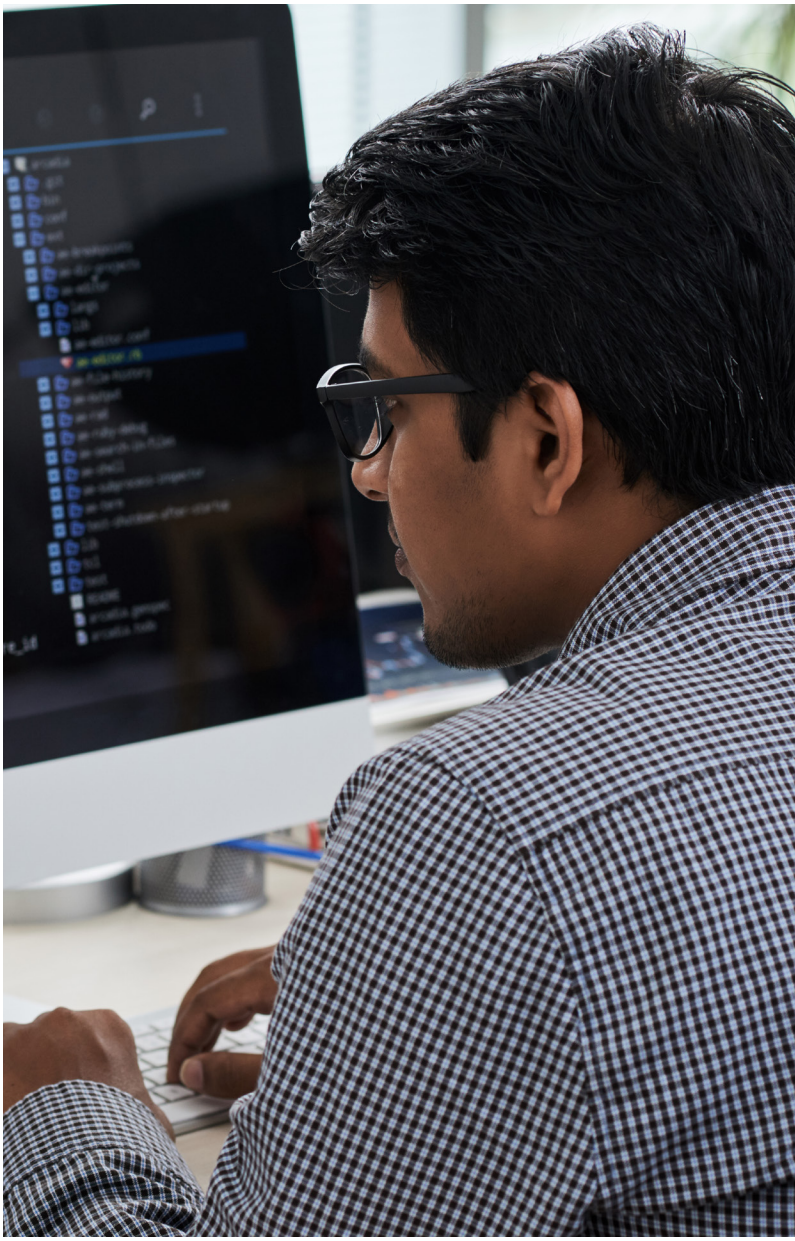
A04: 安全が確認されない不安な設計

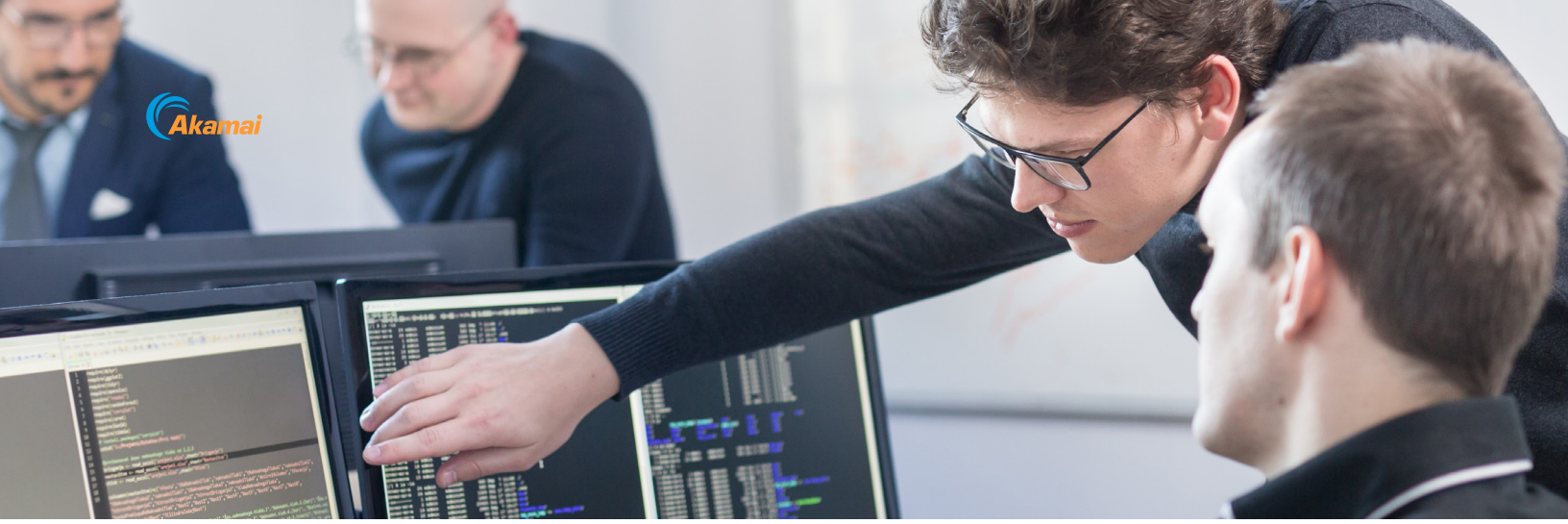
> **「安全が確認されない不安な設計とは、様々な脆弱性を表す広範なカテゴリーであり、「欠落した、あるいは不十分な制御設計」とも表されます。安全でない設計と安全でない実装は異なります。安全な設計であっても、実装上の欠陥があると、それが悪用される可能性のある脆弱性につながります。安全でない設計は、完璧な実装によって修正することはできません。というのも、定義上、特定の攻撃を防御するために必要なセキュリティ制御が作成されたことはないからです。」**
>
> **— 出典：owasp.org**

Akamai による支援

組織は、設計の最初期段階からセキュリティを統合する必要があります。ただし、セキュリティの組み込みが困難な場合、開発チームはセキュリティの統合に苦慮する可能性があります。Akamai 製品は、組織による迅速な「シフトレフト」を支援し、安全が確認されない不安な設計がアプリや API に影響するのを防ぎます。

- **App & API Protector** は、WAAP ソリューションと ASE を構成し、本番環境に影響する一部の設計上の欠陥を検知して修正することも可能です。さらに、自動化を利用して、日常的なタスクをオフロードしてシンプル化することもできます。ただし、人間による分析が必要な作業は、人間がそのまま担当します。この自動化には、自動更新、セルフチューニング、API ディスカバリー、プログラマビリティーのシンプル化、ユーザー体験などがあります。
- **Enterprise Application Access** は、認証されたユーザーのみがアプリケーションにアクセスできるようにします。VPN などのネットワーク・アクセス・ソリューションでは他のアプリケーションへのラテラルムーブメント（横方向の移動）が容易に発生しますが、この最小限の権限アプローチによってそれを阻止します。





A05: セキュリティの設定ミス

> **「アプリケーションの 90 %には何らかの設定ミスが確認され、平均発生率は 4 %であり、20 万 8 千以上の CWE が発生していました。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協調して繰り返すことができなければ、システムはより高いリスクにさらされます。」**
>
> **— 出典：owasp.org**

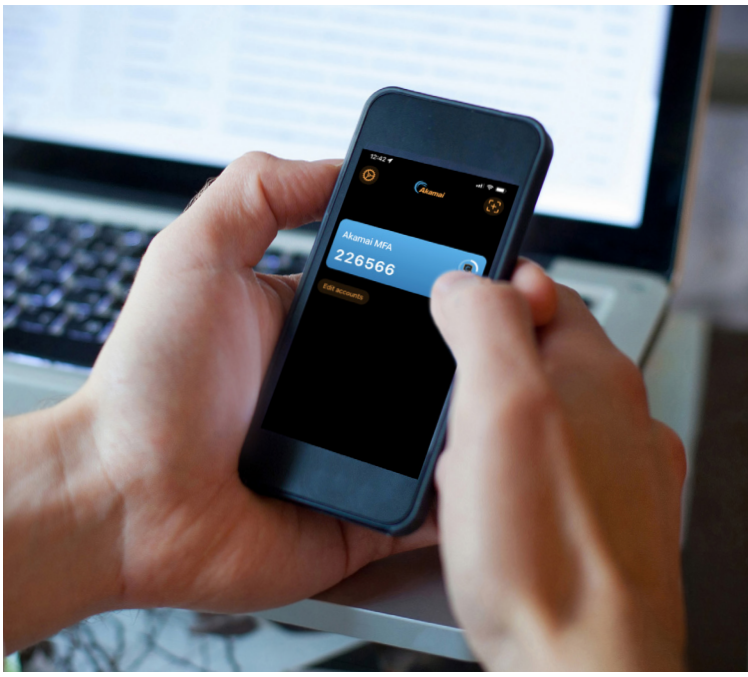
Akamai による支援

当然のことですが、セキュリティの設定ミスは、アプリケーションセキュリティの複数の側面に関連します。また、組織はセキュリティ制御を適切に設定する必要があります。Akamai の製品は次のようなサポートを提供します。

- 適切な設定に代わるものではありませんが、**App & API Protector** は次の機能で貢献します。
  1. アウトバウンド・アノーマリ・アタック・グループを使用して、セキュリティの設定ミスが原因で漏えいするソースコードだけでなくエラーコードによる情報漏えいを、追加設定なしですぐに検出します。
  2. XML パーサーが危険な外部エンティティを処理する前に XXE 攻撃を検知して阻止するルールを実装します。
  3. 開発者が残した既知の機微なファイルへのアクセスを検知できるルールを本番環境サーバーに実装します。
- **Akamai Guardicore Segmentation** は、アプリケーションとインターネット間の不正な通信や想定外の通信に対する可視性ときめ細かい制御を提供することで、不適切な設定によるデータ漏えいを阻止します。
- カスタマイズされたルールに基づく仮想パッチは、チームがアプリケーションにパッチを適用するまでの間、検知したデータ漏えいに対する迅速な対応を支援します。
- **App & API Protector** と **Bot Manager** により、デフォルトの認証情報を使用した総当たり攻撃をレート制御で防ぎます。
- Content-Security-Policy ヘッダーや他のセキュリティ関連 HTTP ヘッダーの脆弱なセキュリティ設定を、Akamai プラットフォームで強化できます。
- **App & API Protector** の API 自動検出により、API を自動的に検出してプロファイリング（エンドポイント、定義、リソースおよびトラフィック特性など）を実行できます。

A06: 脆弱で古くなったコンポーネント

> 「ライブラリー、フレームワーク、および他のソフトウェアモジュールなどのコンポーネントは、アプリケーションと同じ権限で実行されます。さらに、スクリプトは信頼できるアプリケーションリソースとして機能し、アプリケーションデータへのフルアクセスが可能です。脆弱なコンポーネントが悪用されると、攻撃によって深刻なデータ損失やサーバーの乗っ取りが生じる可能性があります」
>
> ― 出典：Akamai



Akamai による支援

自分たちのアプリケーションに存在するサードパーティコンポーネントを追跡できない組織は多く、セキュリティチームがこれらを全く認識していないこともよくあります。さらに、新たに発見された脆弱性に対して、サードパーティ側がどの程度速やかに対応するかについては、組織側で関与することができません。この可視性の欠如を緩和するためには、WAAP などのセキュリティソリューションや、以下のようなスクリプト保護を使用する必要があります。

- **App & API Protector** には既知の脆弱性向けに設計されたルールが複数含まれており、お客様独自のアプリケーション内、サードパーティのコンポーネント内のどちらの脆弱性にも対応できます。さらに、API 保護機能では、API に組み込まれているサードパーティコンポーネントが API を開いて悪用する場合も、API を保護します。
- **Akamai Guardicore Segmentation** の知見モジュールは、脆弱な可能性があるネットワークのアセットについてクエリーを送信できます。きめ細かい適用機能を駆使することで、パッチが適用されるまでの間、影響を受けるアセットを隔離できます。
- カスタマイズされたルールに基づく仮想パッチは、アプリケーションにパッチが適用されるまでの間、新しい脆弱性やアプリケーションの変更によって生じた脆弱性に対する迅速な対応を支援します。
- **Client Reputation** は、Web スキャニングカテゴリーにおける悪性クライアントについてリスクスコアを提供し、新しい脆弱性の悪用からの保護を支援します。
- **Page Integrity Manager** は、実ユーザーのセッションにおけるスクリプトの実行を継続的に分析し、疑わしいふるまいや明らかな悪性のふるまいを特定します。また、常に最新の Common Vulnerabilities and Exposures（CVE）データベースを使用して、既知の脆弱性を持つ URL に対するファーストパーティおよびサードパーティのスクリプトからのデータ窃盗を阻止します。

A07: 識別と認証の失敗

> **「認証とセッション管理に関連するアプリケーション機能は、適切に実装されていないことも多いため、攻撃者はパスワード、キー、またはセッショントークンを漏えいさせたり、他の実装の不備を悪用したりして、一時的または永続的に、他のユーザーアイデンティティになりすますことができます」**
>
> **― 出典：Akamai**

Akamai による支援

組織は、この脆弱性に完全に対応するために、過失を修正する必要があります。以下に挙げる Akamai ソリューションは、識別と認証の失敗を悪用しようとする多くの攻撃ベクトルを検知して防御できるように支援します。

- **Bot Manager** は、Credential Stuffing 攻撃で使用される自動化された攻撃を検知して緩和できます。
- **Account Protector** は、なりすましの犯罪者がユーザーアカウントへの不正アクセスを取得するためのアカウント乗っ取りの試みを緩和します。
- **Enterprise Application Access** は、「最小権限アクセスモデル」に基づいてアプリケーションへのプロキシアクセスを可能にすることで、アプリケーションのアタックサーフェス（攻撃の対象となり得る領域）を減らし、アクセスを強化します。
- **Akamai MFA** は、フィッシング対抗の FIDO2 テクノロジーを使用する強力な認証を提供します。
- **App & API Protector** にはレート制御機能があり、総当たり攻撃に対処できます。
- **Identity Cloud** では、2 要素認証とリスクベースの認証機能でエンドユーザー資格情報とプロファイル情報を保護し、安全に管理できます。

A08: ソフトウェアとデータの整合性の不具合

「ソフトウェアとデータの整合性の不具合は、コードやインフラストラクチャが整合性違反から保護されていないことに関連しています。例として、アプリケーションが信頼されていないソースに由来するプラグインやライブラリ、モジュール、コンテンツデリバリーネットワーク (CDNs) に依存している場合が挙げられます。安全でない CI/CD パイプラインも、権限のないアクセスや悪意のあるコード、システムののっとりの可能性を高めます。」

— 出典：owasp.org

Akamai による支援

組織は、WAAP を使用して、ソフトウェアとデータの整合性の不具合から Web アプリケーションと API を保護できます。ただし、開発ライフサイクルに基づいて、Web アプリケーションに脆弱性が発見されるたびに、パッチを適用する必要があります。

- **App & API Protector**
  - デシリアライゼーション攻撃に対して強力な保護を提供します。
  - 最新の TLS バージョンと強力な暗号を実装することで、データ整合性の問題の原因となるマシン仲介型攻撃を防ぎます。
  - DNSSEC と Edge DNS を導入することで、DNS レコードのデータオリジン認証とデータ整合性を確実に保護します。こうすることで、ユーザーを信頼できないソースへと導く DNS レコードの改ざんを防ぎます。
- **Akamai Guardicore Segmentation** の知見モジュールにより、破損した更新を受け取ったネットワークのアセットについてクエリーを送信できます。きめ細かい適用機能を駆使することで、修正版が作成されるまでの間、影響を受けるアセットを隔離できます
- **Enterprise Threat Protector** は、フィッシング攻撃を検知します。フィッシング攻撃はアプリケーションの管理者やスーパーバイザーを騙して、悪意のある環境や信頼されていないソースに導きます。
- 新たにデシリアライゼーションの欠陥が発見された場合、アプリケーションにパッチを適用できるようになるまでは、カスタムルールによる仮想パッチですぐに対応できます。
- **Page Integrity Manager** は、サードパーティスクリプトを検知し、その変更を監視して、不正アクセスされたスクリプトに対して対策を講じます。

A09: セキュリティログとモニタリングの失敗

「ロギングや検知、モニタリング、適時の対応が十分に行われないという状況は、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(dynamic application security testing) ツール（OWASP ZAP 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。」

— 出典：owasp.org

Akamai による支援

セキュリティログとモニタリングの失敗では、脆弱性に対処する組織の能力とそれらの脆弱性を悪用する試みの間にギャップが生じます。Akamai は、攻撃の可視化を強化する機能を、以下を含め複数ご用意しています。

- Akamai は、Akamai Control Center のグラフィカル・ユーザー・インターフェースを通じてダッシュボードとレポートツールを提供します。
- Akamai のアプリケーションセキュリティ製品は、組織の既存の SIEM インフラを統合し、Akamai が検知したイベントを他のセキュリティベンダーが検知したイベントと関連付けることができます。
- **Managed Security Service** では 24 時間体制で分析と対応の機能を提供します。
- **App & API Protector** には、ペナルティボックス機能があり、悪性または疑わしいふるまいの IP ロギングが増えると、詳細な分析を行うことができます。
- **Enterprise Application Access** は統合的なアイデンティティ管理ソリューションを提供し、すべてのエンタープライズアプリケーションに対するアクセスの認証と制御を可能にします。アイデンティティ認識型プロキシの機能と組み合わせることで、組織はユーザーの操作に対するきめ細かい可視性（すべての GET/POST アクションに対する可視性を含む）を得ることができます。
- **Enterprise Threat Protector** は、悪性かどうかにかかわらずエンタープライズからのすべての外部 DNS リクエストに対する完全な可視化を実現します。
- **Akamai Guardicore Segmentation** は、ネットワーク内の通信フローを詳細に可視化します。不正な通信や予期しない通信が発生するとアラートが起動し、プロセスまたはサービスレベルごとにセキュリティポリシーを適用して、その通信を制限できます。追加された侵害検知モジュールにより、潜在的な脅威を速やかに検知して修復できます。

A10: サーバーサイドリクエストフォージェリ（SSRF）

> **「SSRF の欠陥は、Web アプリケーション上からリモートのリソースを取得する際に、ユーザーから提供された URL を検証せずに使用することで発生します。ファイアウォールや VPN あるいはその他の種類のネットワークアクセス制御リスト (ACL) によってアプリケーションが保護されている場合であっても、SSRF によりアプリケーションに対して意図しない宛先へ細工されたリクエストを強制的に発行させることができます。」**
>
> **— 出典：owasp.org**

Akamai による支援

Akamai WAAP には、URL のインジェクションを検出するルールがあります。この機能により、攻撃者がサーバーに侵入して別の場所に移動したり、リクエストを送信する（セキュリティアナリストにとって正当なリクエストに見せかける）ことを阻止できます。

- **App & API Protector** ルールは、こうした不正リクエストが脆弱なサーバーに最初に到達するのを回避できます。
- **Akamai Guardicore Segmentation** は、予期しないアウトバウンドトラフィックをサーバーレベルで監視してブロックします。

結論

OWASP トップ 10 の脆弱性に対する最適な防御策を積み上げていくためには、組織とセキュリティベンダーが連携し、できるだけ速やかに脆弱性を特定し、解決策を適用して緩和する必要があります。Akamai のエッジ・セキュリティ・ポートフォリオの詳細をご確認ください。パートナーとして当社が貴社のビジネスに最善の保護をどのように確立できるかについて、詳しく検討されたい場合は、是非 Akamai の営業担当者にお問い合わせください。