IPA（独立行政法人情報処理推進機構） 安全なウェブサイトの作り方チェックリスト（改訂第7版）

2025年7月1日

Office Hub

アートメタバースランド株式会社

■ ウェブアプリケーションのセキュリティ実装 チェックリスト（1/3）

No	脆弱性の種類	対策の性質	チェック	実施項目	解説
1	SQLインジェクション	根本的解決	※ ■ 対応済 □ 未対策 □ 対応不要	■ SQL文の組み立ては全てプレースホルダで実装する。	1-(i)-a
				■ SQL文の構成を文字列連結により行う場合は、アプリケーションの変数をSQL文のリテラルとして正しく構成する。	1-(i)-b
		根本的解決	■ 対応済 □ 未対策 □ 対応不要	ウェブアプリケーションに渡されるパラメータにSQL文を直接指定しない。	1-(ii)
		保険的対策	■ 対応済 □ 未対策 □ 対応不要	エラーメッセージをそのままブラウザに表示しない。	1-(iii)
		保険的対策	■ 対応済 □ 未対策 □ 対応不要	データベースアカウントに適切な権限を与える。	1-(iv)
2	OSコマンド・インジェクション	根本的解決	□ 対応済 □ 未対策 ■ 対応不要	シェルを起動できる言語機能の利用を避ける。 Office Hubは、AWS上に構築されているためOSコマンド・インジェクションは発生しません。	2-(i)
		保険的対策	□ 対応済 □ 未対策 ■ 対応不要	シェルを起動できる言語機能を利用する場合は、その引数を構成する全ての変数に対してチェックを行い、あらかじめ許可した処理のみを実行する。	2-(ii)
3	パス名パラメータの未チェック／ディレクトリ・トラバーサル	根本的解決	※ ■ 対応済 □ 未対策 □ 対応不要	■ 外部からのパラメータでウェブサーバ内のファイル名を直接指定する実装を避ける。	3-(i)-a
				■ ファイルを開く際は、固定のディレクトリを指定し、かつファイル名にディレクトリ名が含まれないようにする。	3-(i)-b
		保険的対策	■ 対応済 □ 未対策 □ 対応不要	ウェブサーバ内のファイルへのアクセス権限の設定を正しく管理する。	3-(ii)
		保険的対策	■ 対応済 □ 未対策 □ 対応不要	ファイル名のチェックを行う。	3-(iii)
4	セッション管理の不備 当社のメタバースOffice Hubは、従来のセッションIDを用いた認証方式ではなく、モダンなWebアプリケーションに適したトークンベース認証方式を採用しております。 これにより、セッションIDの盗難や固定化によるリスクを排除し、より高いセキュリティレベルとスケーラビリティを確保しています。	根本的解決	□ 対応済 □ 未対策 ■対応不要	セッションIDを推測が困難なものにする。 セッションIDを使用しておらず、全てのAPI通信においてトークンベースの認証（アクセストークン＋リフレッシュトークン）を採用しています。トークンは十分なランダム性と暗号学的安全性を有する方式で生成されており、推測は困難です。	4-(i)
		根本的解決	□ 対応済 □ 未対策 ■ 対応不要	セッションIDをURLパラメータに格納しない。 セッションIDは使用しておらず、トークンはHTTPヘッダ（Authorizationヘッダ）に格納されるため、URLに含まれることはありません。	4-(ii)
		根本的解決	□ 対応済 □ 未対策 ■ 対応不要	HTTPS通信で利用するCookieにはsecure属性を加える。 トークンはCookieではなく、HTTP Authorizationヘッダで管理されているため、Cookieのsecure属性は使用していません。また、すべての通信はHTTPSで暗号化され保護されています。	4-(iii)
		根本的解決	※ □ 対応済 □ 未対策 ■ 対応不要	ログイン成功後に、新しくセッションを開始する。 □ セッションの概念がなく、ログイン成功時にアクセストークンとリフレッシュトークンが発行されます。これにより、再認証やトークン更新によりセキュリティが担保され、セッションフィクセーションのリスクを排除しています。	4-(iv)-a
				ログイン成功後に、既存のセッションIDとは別に秘密情報を発行し、ページの遷移ごとにその値を確認する。 □ サーバ側のセッションIDやページ遷移ごとのトークン照合は行っておりません。アクセストークンはJWT形式で署名されており、各APIリクエストにおいて認証トークンの整合性と有効性が確認されるため、同様のセキュリティ効果を実現しています。	4-(iv)-b
		保険的対策	□ 対応済 □ 未対策 ■ 対応不要	セッションIDを固定値にしない。 セッションIDは使用していません。アクセストークンはランダム性を持つものであり、一定時間で失効する短期トークンです。固定的なIDにはなりません。	4-(v)
		保険的対策	□ 対応済 □ 未対策 ■ 対応不要	セッションIDをCookieにセットする場合、有効期限の設定に注意する。 Cookieによるセッション管理を行っていません。アクセストークンの有効期限は短く、リフレッシュトークンにより更新する構成です。	4-(vi)

※ このチェック項目の「対応済」のチェックは、実施項目のいずれかを実施した場合にチェックします。

■ ウェブアプリケーションのセキュリティ実装 チェックリスト（2/3）

No	脆弱性の種類		対策の性質	チェック	実施項目	解説
5	クロスサイト・スクリプティング	HTMLテキストの入力を許可しない場合の対策	根本的解決	■ 対応済 □ 未対策 □ 対応不要	ウェブページに出力する全ての要素に対して、エスケープ処理を施す。	5-(i)
			根本的解決	■ 対応済 □ 未対策 □ 対応不要	URLを出力するときは、「http://」や「https://」で始まるURLのみを許可する。	5-(ii)
			根本的解決	■ 対応済 □ 未対策 □ 対応不要	<script>…</script> 要素の内容を動的に生成しない。	5-(iii)
			根本的解決	■ 対応済 □ 未対策 □ 対応不要	スタイルシートを任意のサイトから取り込めるようにしない。	5-(iv)
			保険的対策	■ 対応済 □ 未対策 □ 対応不要	入力値の内容チェックを行う。	5-(v)
		HTMLテキストの入力を許可する場合の対策	根本的解決	■ 対応済 □ 未対策 □ 対応不要	入力されたHTMLテキストから構文解析木を作成し、スクリプトを含まない必要な要素のみを抽出する。	5-(vi)
			保険的対策	■ 対応済 □ 未対策 □ 対応不要	入力されたHTMLテキストから、スクリプトに該当する文字列を排除する。	5-(vii)
		全てのウェブアプリケーションに共通の対策	根本的解決	■ 対応済 □ 未対策 □ 対応不要	HTTPレスポンスヘッダのContent-Typeフィールドに文字コード（charset）の指定を行う。	5-(viii)
			保険的対策	□ 対応済 □ 未対策 ■ 対応不要	Cookie情報の漏えい対策として、発行するCookieにHttpOnly属性を加え、TRACEメソッドを無効化する。 当社システムではセッション管理にCookieを使用しておらず、すべてのAPI通信においてアクセストークンとリフレッシュトークンを含むトークンベース認証を採用しています。そのため、HttpOnly属性の付与対象となるCookieは発行されておらず、本項目は該当しません。また、TRACEメソッドは無効化済です。	5-(ix)
			保険的対策	■ 対応済 □ 未対策 □ 対応不要	クロスサイト・スクリプティングの潜在的な脆弱性対策として有効なブラウザの機能を有効にするレスポンスヘッダを返す。 Office Hubでは、クロスサイト・スクリプティング（XSS）対策として、ブラウザのセキュリティ機能を有効化するレスポンスヘッダの付与を、AWS CloudFront の機能により実装しています。また、AWSのCloudFrontのレスポンスヘッダー設定機能を用いて、以下のようなセキュリティヘッダーを追加しています： ・Content-Security-Policy（CSP）によるスクリプト制御 ・X-Content-Type-Options: nosniff ・X-XSS-Protection: 1; mode=block （※一部ブラウザで非推奨であることを認識のうえ設定） これによりウェブアプリケーションにおけるXSS脆弱性のリスクを低減しています。	5-(x)
6	CSRF （クロスサイト・リクエスト・フォージェリ）		根本的解決	※ ■ 対応済 □ 未対策 □ 対応不要	■ 処理を実行するページを POST メソッドでアクセスするようにし、その「hidden パラメータ」に秘密情報が挿入されるよう、前のページを自動生成して、実行ページではその値が正しい場合のみ処理を実行する。	6-(i)-a
					■ 処理を実行する直前のページで再度パスワードの入力を求め、実行ページでは、再度入力されたパスワードが正しい場合のみ処理を実行する。	6-(i)-b
					■ Refererが正しいリンク元かを確認し、正しい場合のみ処理を実行する。	6-(i)-c
			保険的対策	■ 対応済 □ 未対策 □ 対応不要	重要な操作を行った際に、その旨を登録済みのメールアドレスに自動送信する。	6-(ii)
7	HTTPヘッダ・インジェクション		根本的解決	※ ■ 対応済 □ 未対策 □ 対応不要	■ ヘッダの出力を直接行わず、ウェブアプリケーションの実行環境や言語に用意されているヘッダ出力用APIを使用する。	7-(i)-a
					■ 改行コードを適切に処理するヘッダ出力用APIを利用できない場合は、改行を許可しないよう、開発者自身で適切な処理を実装する。	7-(i)-b
			保険的対策	■ 対応済 □ 未対策 □ 対応不要	外部からの入力の全てについて、改行コードを削除する。 HTTPヘッダ・インジェクション対策として、外部から受け取るすべての入力値に対し、改行コード（CRLF：0x0d、0x0a）の除去またはエスケープ処理を実施しています。加えて、サーバ側でHTTPレスポンスヘッダを構成する際には、ヘッダフィールドへの動的挿入を最小限にし、ヘッダ操作は信頼できる静的値または厳格に検証された値に限定しています。また、HTTPレスポンスはAWS CloudFrontおよびバックエンドAPIにより生成され、各層でセキュリティ対策を講じています。	7-(ii)

※ このチェック項目の「対応済」のチェックは、実施項目のいずれかを実施した場合にチェックします。

■ ウェブアプリケーションのセキュリティ実装 チェックリスト（3/3）

No	脆弱性の種類	対策の性質	チェック	実施項目	解説
8	メールヘッダ・インジェクション	根本的解決	※ ■ 対応済 □ 未対策 □ 対応不要	■ メールヘッダを固定値にして、外部からの入力はすべてメール本文に出力する。	8-(i)-a
				■ ウェブアプリケーションの実行環境や言語に用意されているメール送信用APIを使用する（8-(i) を採用できない場合）。	8-(i)-b
		根本的解決	■ 対応済 □ 未対策 □ 対応不要	HTMLで宛先を指定しない。	8-(ii)
		保険的対策	■ 対応済 □ 未対策 □ 対応不要	外部からの入力の全てについて、改行コードを削除する。 当社システムでは、問い合わせフォームや通知メールなど、メール送信機能において外部入力がメールヘッダに影響を及ぼすことがないよう、以下の対策を講じています。 ・外部入力値からCRLF（¥r、¥n）を除去または無害化処理を行っています。 ・メールヘッダに挿入する値（宛名・件名など）は、ホワイトリスト検証および最大長制限を実施しています。 ・メール送信処理にはサニタイズ済み値を用いて生成したテンプレートを使用し直接連結によるヘッダ構築は行っておりません。 以上により、メールヘッダ・インジェクションのリスクは回避されています。	8-(iii)
9	クリックジャッキング	根本的解決	※ ■ 対応済 □ 未対策 □ 対応不要	■ HTTPレスポンスヘッダに、X-Frame-Optionsヘッダフィールドを出力し、他ドメインのサイトからのframe要素やiframe要素による読み込みを制限する。 Office Hubは、AWSのCloudFrontサービスを利用しクリックジャッキングを防止しています。	9-(i)-a
				□ 処理を実行する直前のページで再度パスワードの入力を求め、実行ページでは、再度入力されたパスワードが正しい場合のみ処理を実行する。	9-(i)-b
		保険的対策	■ 対応済 □ 未対策 □ 対応不要	重要な処理は、一連の操作をマウスのみで実行できないようにする。	9-(ii)
10	バッファオーバーフロー	根本的解決	※ □ 対応済 □ 未対策 ■ 対応不要	直接メモリにアクセスできない言語で記述する。 □ Office HubはNginxを使用しており、client_max_body_size や header_buffer_size などのリクエスト制限設定により、異常なリクエストを制御する仕組みを持っています。	10-(i)-a
				直接メモリにアクセスできる言語で記述する部分を最小限にする。 □ Office HubはNginxを使用しており、client_max_body_size や header_buffer_size などのリクエスト制限設定により、異常なリクエストを制御する仕組みを持っています。	10-(i)-b
		根本的解決	■ 対応済 □ 未対策 □ 対応不要	脆弱性が修正されたバージョンのライブラリを使用する。	10-(ii)
11	アクセス制御や認可制御の欠落	根本的解決	■ 対応済 □ 未対策 □ 対応不要	アクセス制御機能による防御措置が必要とされるウェブサイトには、パスワード等の秘密情報の入力を必要とする認証機能を設ける。	11-(i)
		根本的解決	■ 対応済 □ 未対策 □ 対応不要	認証機能に加えて認可制御の処理を実装し、ログイン中の利用者が他人になりすましてアクセスできないようにする。	11-(ii)

※ このチェック項目の「対応済」のチェックは、実施項目のいずれかを実施した場合にチェックします。