GEAR-S

本チェックシートは、IPA（独立行政法人情報処理推進機構）のチェックリスト「安全なウェブサイトの作り方 改訂第7版」に基づき、
株式会社スカラコミュニケーションズが提供する クラウドサービス「GEAR-S SITEサービス」について、そのセキュリティ対策を記載したものです。
独自のセキュリティチェックシートへの回答をご希望の場合は、別途有償にてご対応とさせていただいております。詳細はお問い合わせください。

「安全なウェブサイトの作り方 改訂第7版」（チェックリスト）

■「GEAR-S SITEサービス」における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）

2022年10月19日現在

No	脆弱性の種類	対策の性質	チェック	実施項目	解説	GEAR-S SITE対応状況
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	【公開サイト】対応不要。静的ホスティング機能のみ提供しているためSQL は使用されません。 【管理サイト】対応不要。SQLは使用しておりません。
				□ 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	【公開サイト】対応不要。静的ホスティング機能のみ提供しているためSQL は使用されません。 【管理サイト】対応不要。SQLは使用しておりません。
		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はSQL文を直接指定しない。	1-(ii)	【公開サイト】対応不要。静的ホスティング機能のみ提供しているためSQL は使用されません。 【管理サイト】対応不要。SQLは使用しておりません。
		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)	【公開サイト】対応済。アクセス時にエラーが発生した場合は、あらかじめ用意されているエラーページが表示されます。 【管理サイト】対応済。詳細なエラーメッセージをブラウザに表示しておりません。
		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)	【公開サイト】対応不要。静的ホスティング機能のみ提供しているためSQL は使用されません。 【管理サイト】対応済。各プログラム(LambdaFunction）毎に最小限のDB権限を付与しております。
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。	2-(i)	【公開サイト】対応済。シェルを起動できる環境・コードは使用しておりません。 【管理サイト】対応済。シェルを起動できる環境・コードは使用しておりません。
		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)	【公開サイト】対応不要。シェルを起動できる環境・コードは使用しておりません。 【管理サイト】対応不要。シェルを起動できる環境・コードは使用しておりません。
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	【公開サイト】未対策。静的ホスティング機能を提供しているので、パスでファイル名を指定するようになっています。 【管理サイト】対応済。ファイル名を直接指定する実装をしていません。
				■ 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	【公開サイト】対応済。静的ホスティングによって公開しているファイルとそれ以外の非公開ファイルは、それぞれアクセス範囲の隔離されたストレージに保管しているため、公開していないファイルを外部から参照する事は出来ません。 【管理サイト】対応済。ファイル操作を実行するコードはございません。
		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)	【公開サイト】対応済。静的ホスティング用のストレージは、適切な権限を設定しています。 【管理サイト】対応済。ファイル操作を実行するコードはございません。
		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)	【公開サイト】対応不要。物理的に意図しないファイルへのアクセスを防いでいるためチェック機能は要ありません。 【管理サイト】対応済。ファイル操作を実行するコードはございません。
4	セッション管理の不備	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。	4-(i)	【公開サイト】対応済。セッションを使用しておりません。 【管理サイト】対応済。トークン認証(JSON Web Token）を使用の為、セッションIDは使用しておりません。
		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。	4-(ii)	【公開サイト】対応済。セッションを使用しておりません。 【管理サイト】対応済。トークン認証(JSON Web Token）を使用の為、セッションIDは使用しておりません。
		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。	4-(iii)	【公開サイト】対応済。セッションを使用しておりません。 【管理サイト】対応済。アプリケーションで使用しているCookieはすべてsecure属性を付与しております。
		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。	4-(iv)-a	【公開サイト】対応済。セッションを使用しておりません。 【管理サイト】対応済。トークン認証(JSON Web Token）を使用の為、セッションIDは使用しておりません。
				■ 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。	4-(iv)-b	【公開サイト】対応済。セッションを使用しておりません。 【管理サイト】対応済。トークン認証(JSON Web Token）を使用の為、セッションIDは使用しておりません。
		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。	4-(v)	【公開サイト】対応済。セッションを使用しておりません。 【管理サイト】対応済。トークン認証(JSON Web Token）を使用の為、セッションIDは使用しておりません。
		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。	4-(vi)	【公開サイト】対応済。セッションを使用しておりません。 【管理サイト】対応済。トークン認証(JSON Web Token）を使用の為、セッションIDは使用しておりません。

※ 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。

■「GEAR-S SITEサービス」における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	GEAR-S SITE対応状況
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)	【公開サイト】対応不要。サービスの機能として提供しているので対象外 【管理サイト】対応済。管理画面表示時に全表示項目をHTMLエスケープしております。
			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)	【公開サイト】対応不要。サービスの機能として提供しているので対象外 【管理サイト】対応済。URLを動的に表示する機能はございません。
			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)	【公開サイト】対応不要。サービスの機能として提供しているので対象外 【管理サイト】対応済。script タグを動的に生成する機能はございません
			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)	【公開サイト】対応不要。サービスの機能として提供しているので対象外 【管理サイト】対応済。スタイルシートを動的に取り込む機能はございません
			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)	【公開サイト】対応不要。サービスの機能として提供しているので対象外 【管理サイト】対応済。入力値ハエスケープしております。
		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)	【公開サイト】対応不要。サービスの機能として提供しているので対象外 【管理サイト】対応済。HTMLを動的に生成する機能はございません
			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)	【公開サイト】対応不要。サービスの機能として提供しているので対象外 【管理サイト】対応済。HTMLを動的に生成する機能はございません
		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)	【公開サイト】対応済。 【管理サイト】対応済。
			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。	5-(ix)	【公開サイト】対応不要。cookieを使用しません。 【管理サイト】未対策。TRACEメソッドを無効化については対応済ですが、管理サイトの機能実現の為、HttpOnly属性のみとする制限が行えないため未対策となります。
			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。	5-(x)	【公開サイト】対応済。 【管理サイト】対応不要。レガシーブラウザ向け対策であるXSS-Protectionは未出力ですが、上記クロスサイトスクリプティング対策済の為、本対策は対応不要といたします。
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	【公開サイト】対応不要。静的ホスティング機能のみ提供しておりAPI は提供していないため。 【管理サイト】対応済。管理側はTokenで保護されている為,CSRFによる投稿は不可となっております。
					□ 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)	【公開サイト】対応不要。静的ホスティング機能のみ提供しておりAPI は提供していないため。 【管理サイト】未対策。
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	【公開サイト】対応不要。静的ホスティング機能のみ提供しておりAPI は提供していないため。 【管理サイト】対応済。ヘッダの直接出力は行っておりません。
					□ 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	対応不要。上記根本的解決で対応済の為、本対策については対応不要といたします。
			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。	7-(ii)	対応不要。上記根本的解決で対応済の為、本対策については対応不要といたします。

※ 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。

■「GEAR−S SITEサービス」における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	GEAR−S SITE対応状況
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	【公開サイト】対応不要。メール送信機能はございません。 【管理サイト】対応不要。メール送信機能はございません。
				□ 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	【公開サイト】対応不要。メール送信機能はございません。 【管理サイト】対応不要。メール送信機能はございません。
		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)	【公開サイト】対応不要。メール送信機能はございません。 【管理サイト】対応不要。メール送信機能はございません。
		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。	8-(iii)	【公開サイト】対応不要。メール送信機能はございません。 【管理サイト】対応不要。メール送信機能はございません。
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。	9-(i)-a	【公開サイト】対応済。 【管理サイト】未対策。
				□ 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	【公開サイト】対応済。 【管理サイト】未対策。
		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)	【公開サイト】対応不要。上記根本的解決で対応済の為、本対策については対応不要といたします。 【管理サイト】未対策。
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。	10-(i)-a	対応不要。10-(i)-b で対応済。
				■ 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。	10-(i)-b	【公開サイト】対応不要。静的ホスティング機能のみ提供しているため。 【管理サイト】対応済。メモリにアクセスする機能は使用しておりません。
		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)	【公開サイト】対応不要。静的ホスティング機能のみ提供しており、ライブラリを使用していないため。 【管理サイト】対応済 2022/9/1時点で脆弱性のあるライブラリは使用しておりません。
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)	【公開サイト】対応済。基本的にはログイン機能はなし。任意ID/PWでフォームを保護する機能もありますが、その場合も対応済。 【管理サイト】対応済。ログイン認証については、トークン認証で保護しており、テナント間の保護や非公開データの保護はアプリケーションロジックで保護しております。ただしユーザーがアップロードした画像については非対応（非公開機能なし）。
		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。