**生産管理システム**

**セキュリティ仕様書**

**2020年　7月 (初版発行)**

はじめに

本仕様書は、ケービーソフトウェア（株）のパッケージソフトである 『生産管理システム』のセキュリティの仕様について纏めたものである。

参考文献：

　　・独立行政法人　情報処理推進機構

「安全なSQLの呼び出し方.pdf」

「安全なウェブサイトの作り方.pdf」

**目　次**

[2020年　7月 (初版発行) 0](#_Toc45627901)

[第１章 SQLインジェクション対策 3](#_Toc45627902)

[第１節 クエリビルダの使用 3](#_Toc45627903)

[第２節 DBエラーメッセージ 3](#_Toc45627904)

[第２章 OSコマンドインジェクション対策 4](#_Toc45627905)

[第１節 OSコマンドの使用時の注意点 4](#_Toc45627906)

[第３章 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 5](#_Toc45627907)

[第１節 Webサーバ内のファイル名の取り扱い 5](#_Toc45627908)

[第４章 セッション管理の不備 6](#_Toc45627909)

[第１節 セッションID 6](#_Toc45627910)

[第２節 セッションIDの再発行 6](#_Toc45627911)

[第５章 クロスサイト・スクリプティング 7](#_Toc45627912)

[第１節 エスケープ処理 7](#_Toc45627913)

[第２節 HTMLタグ 7](#_Toc45627914)

[第３節 <script>要素 7](#_Toc45627915)

[第４節 文字コードの指定 7](#_Toc45627916)

[第５節 7](#_Toc45627917)

[第６章 クロスサイト・リクエスト・フォージェリ 8](#_Toc45627918)

[第１節 秘密情報の一致による確認 8](#_Toc45627919)

[第７章 HTTPヘッダ・インジェクション 9](#_Toc45627920)

[第１節 header関数の使用 9](#_Toc45627921)

[第８章 メールヘッダ・インジェクション 10](#_Toc45627922)

[第１節 対象外 10](#_Toc45627923)

[第９章 クリックジャッキング 11](#_Toc45627924)

[第１節 X-Frame-Options ヘッダフィールド 11](#_Toc45627925)

[第１０章 バッファオーバーフロー 12](#_Toc45627926)

[第１節 対象外 12](#_Toc45627927)

[第１１章 アクセス制御や認可制御の欠落 13](#_Toc45627928)

[第１節 ログイン 13](#_Toc45627929)

[第２節 アクセス権 13](#_Toc45627930)

[第１２章 改定履歴 14](#_Toc45627931)

# SQLインジェクション対策

## クエリビルダの使用

* 自動でバインドする仕組みがある為、Laravelのクエリビルダを使用すること。
* rowメソッドや、whereRowメソッドはバインドされない為、使用しない。

→　やむを得ず使用する必要がある場合は、KBSプロジェクトリーダの許可を得ること。

　　　（whereRowメソッドであれば、第二引数を使うと安全に値をバインドできる）

## DBエラーメッセージ

* DBエラーのメッセージを、そのままブラウザに表示しないようにする。

# OSコマンドインジェクション対策

## OSコマンドの使用時の注意点

* 危険を及ぼす可能性のある関数（「exec」「system」「passthru」「proc\_open」「shell\_exec」「popen」）を

使用する場合、ユーザが入力した値を、パラメータに使用しない。

# 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

## Webサーバ内のファイル名の取り扱い

* Hiddenやリクエストパラメータで、ファイル名を直接指定しない。
* URLではファイル名を指定しない。
* ファイルを開く際は、固定のディレクトリを指定し、ファイル名を動的に指定する場合は、ディレクトリ名が含まれないか

チェックする。

# セッション管理の不備

## セッションID

* セッションIDは推測が困難なものにする。（自前でセッションIDを生成しない）
* セッションIDをURLパラメータに格納しない。（Cookieに格納）

Laravelの.envファイルのSESSION\_DRIVERをcookie に変更する。

* 念のため、php.iniの以下の設定も確認する。

　　　　　session.sid\_length = 32

　　　　　session.use\_cookies = 1

　　　　　session.use\_only\_cookies = 1

## セッションIDの再発行

* ログイン成功後に、セッションIDの再発行を行う。（Laravelのregenerateメソッドを使用する）

# クロスサイト・スクリプティング

## エスケープ処理

* Laravelのエスケープ処理機能（{{}}で要素をくくる）を使用し、出力する全ての要素に対して

エスケープ処理をする。

## HTMLタグ

* HTMLタグを出力する場合は、その属性値を「“」ダブルコーテーションで囲むようにすること。

## <script>要素

* <script></script>要素の内容を動的に生成しない。

## 文字コードの指定

* 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。

Laravelのミドルウェアで対応する。

## 表示メッセージ

* ユーザの入力値をwindow.alert、confirmに使用しない

# クロスサイト・リクエスト・フォージェリ

## 秘密情報の一致による確認

* Laravelのビューのformタグでは、リクエストを送るとき「@csrf」を記述すること。

※POST、PUT、DELETEリクエストが対象（記述しないとエラーになります）

# HTTPヘッダ・インジェクション

## header関数の使用

* HTTPレスポンスヘッダの出力は直接行わず、「header」関数を使用する。

# メールヘッダ・インジェクション

## 対象外

* メールを使用する予定はないので対象外。（使用する場合は、ここに記載する）

# クリックジャッキング

## X-Frame-Options ヘッダフィールド

* HTTPレスポンスヘッダに、X-Frame-Options ヘッダフィールドを出力する。

Laravelのミドルウェアで対応する。

* iframeの使用が必要な場合は、「SAMEORIGIN」を設定する。

# バッファオーバーフロー

## 対象外

* PHPは直接メモリを操作できない為、対象外。

# アクセス制御や認可制御の欠落

## ログイン

* Windowsログイン時のユーザIDを使用して、シングルサインオンとする。

## アクセス権

* Windowsログイン時のユーザIDにて、ユーザマスタを照会し、使用できる機能を制限する。
* ユーザが画面表示権限のない画面を表示した場合、トップ画面に戻るようにする。

# 改定履歴

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ＮＯ | 内 容 | 承認 | 担当 | 日付 |
| ０ | 初版発行 |  | 西田 | 2020-7-1 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |