

EC-CUBE セキュリティガイドラインプラグイン チェックシート Version 1.0

2-1. プラグインプログラム全体

- | | | | |
|--|-----------------------------|------------------------------|------------------------------|
| ・EC-CUBE のコーディング規則に準じている。(プログラムのコーディング上の注意) | はい ☐ | いいえ ☐ | 対象外 ☐ |
| ・セキュリティ上の脅威が無い事を利用者や第三者が確認しやすいプラグインプログラムとしている。(プログラムのコーディング上の注意) | はい ☐ | いいえ ☐ | 対象外 ☐ |
| ・EC-CUBE のプラグインコーディング規則に準じている。(プラグインのコーディング上の注意) | はい ☐ | いいえ ☐ | 対象外 ☐ |
| ・セキュリティ上の脅威が無い事を利用者や第三者が確認しやすいプラグインプログラムとしている。(プラグインのコーディング上の注意) | はい ☐ | いいえ ☐ | 対象外 ☐ |
| ・命名規則やファイル構成、展開方法について規約に準拠している。(プラグインのコーディング上の注意) | はい ☐ | いいえ ☐ | 対象外 ☐ |
| ・プラグインプログラムの利用に関するマニュアルを提供している。(マニュアルの提供) | はい ☐ | いいえ ☐ | 対象外 ☐ |
| ・ファイルリストを用意している。(ファイル構成) | はい ☐ | いいえ ☐ | 対象外 ☐ |
| ・プラグインの機能によりファイルを複製して、公開ディレクトリ側に呼出プログラムファイル等を設置する場合は、そのプログラムファイルを明示している。(ファイル構成) | はい ☐ | いいえ ☐ | 対象外 ☐ |
| ・むやみに公開側ディレクトリにファイルを設置せず、必要最低限のファイル複製している。(ファイル構成) | はい ☐ | いいえ ☐ | 対象外 ☐ |
| ・設置内容をファイルリストで明らかにすることで関連するファイルの状態などを容易に確認出来る状態を作っている。(ファイル構成) | はい ☐ | いいえ ☐ | 対象外 ☐ |
| ・プラグインファイル自体は EC-CUBE のプラグインパッケージ仕様により展開されることを前提とした構成としている。(ファイル構成) | はい ☐ | いいえ ☐ | 対象外 ☐ |
| ・外部とデータを交換する為に公開側ディレクトリ設置するプログラムが存在する場合、その呼出用プログラムファイルの明示を行っている。(公開されるポイントの明確化) | はい ☐ | いいえ ☐ | 対象外 ☐ |
| ・プログラムファイルが通信相手として想定している相手方を明示している。(公開されるポイントの明確化) | はい ☐ | いいえ ☐ | 対象外 ☐ |
| ・公開されるポイントに対して、「公開／管理者／その他」と分類・明示している。(公開されるポイントの明確化) | はい ☐ | いいえ ☐ | 対象外 ☐ |
| ・公開されるポイントに対して、アクセス上の規制をどのように施しているかを明示している。(公開されるポイントの明確化) | はい ☐ | いいえ ☐ | 対象外 ☐ |
| ・「その他」の相手が決まっている場合を想定し、何らかの規制をかけている（またはかけるべき）部分を明らかとしている。(公開されるポイントの明確化) | はい ☐ | いいえ ☐ | 対象外 ☐ |

2-2. パラメーターの安全性確保

- | | | | |
|---|-----------------------------|------------------------------|------------------------------|
| ・ EC-CUBE のフォームパラムクラス (SC_FormParam) を使用し、適切な入力フォームデータの正規化とチェック処理を行っている。(入力フォームの正規化とエラーチェック) | はい ☐ | いいえ ☐ | 対象外 ☐ |
| ・ また、エラーチェック処理を必ず呼び出すようにする。(入力フォームの正規化とエラーチェック) | はい ☐ | いいえ ☐ | 対象外 ☐ |
| ・ 追加のパラメーター値を追加したい場合には SC_FormParam へのパラメーター追加機能を用いている。(フォームパラメーターの拡張による処理) | はい ☐ | いいえ ☐ | 対象外 ☐ |
| ・ プログラム内ではグローバル変数である\$_POST 変数や\$_GET 変数、\$_REQUEST 変数、\$_COOKIE などを直接参照せず、フォームパラムクラスを通してデータを扱っている。(グローバル変数の直接参照の制限) | はい ☐ | いいえ ☐ | 対象外 ☐ |
| ・ \$_GLOBAL 変数を使っていない。(グローバル変数の直接参照の制限) | はい ☐ | いいえ ☐ | 対象外 ☐ |
| ・ \$_COOKIE 変数および Cookie データ、UserAgent などに依存した確認を用いていない。(利用出来る変数の制限) | はい ☐ | いいえ ☐ | 対象外 ☐ |
| ・ 表示に用いる部分には、データそのものや変数そのまま、または HTML コードを直接プログラムから出力、または変数に HTML コードそのままを入れて出力していない。(表示をする場合には Smarty のテンプレート処理を通して表示を行う) | はい ☐ | いいえ ☐ | 対象外 ☐ |
| ・ 変数から表示するデータは必ず表示時には Smarty のエスケープ処理を行っている。(入力を受け付けたデータは必ずエスケープ処理をして表示をする) | はい ☐ | いいえ ☐ | 対象外 ☐ |

2-3. プラグインが扱うデータについて

- | | | | |
|---|-----------------------------|------------------------------|------------------------------|
| ・ EC-CUBE 以外の部分と通信するためにデータ等を出力または加工して提供やデータ交換する場合には、通信先を明らかにした上で交換するデータを明示している。(外部向けに提供するデータの明確化と利用の制限) | はい ☐ | いいえ ☐ | 対象外 ☐ |
| ・ EC-CUBE 内のデータを EC-CUBE 以外に渡すまたは提供する場合には、予めプラグインの説明や設定画面に EC-CUBE 以外に渡すデータの内容を明示し、利用者に事前の確認と了承を得ている。(外部向けに提供するデータの明確化と利用の制限) | はい ☐ | いいえ ☐ | 対象外 ☐ |
| ・ 個人情報などを EC-CUBE 以外に渡すまたは提供する場合には、必ずプラグインの設定画面等で確認と了承を管理者に事前に行った上で有効化されている。(外部向けに提供するデータの明確化と利用の制限) | はい ☐ | いいえ ☐ | 対象外 ☐ |
| ・ 管理者が顧客に対して EC-CUBE 以外に対して提供されるデータの内容について周知を行うようマニュアル等に明記している。(外部向けに提供するデータの明確化と利用の制限) | はい ☐ | いいえ ☐ | 対象外 ☐ |

- ・プラグインの目的以外に不要なデータをプラグイン内で扱っていない。(外部向けに提供するデータの明確化と利用の制限) はい ☐ いいえ ☐ 対象外 ☐
- ・EC-CUBE 以外の部分と通信する場合には、必ず通信先を明らかにした上でのログを残している。(ログの記録の徹底) はい ☐ いいえ ☐ 対象外 ☐
- ・EC-CUBE のログ用関数を利用して記録することで、日時とリクエスト元 (ブラウザ等での参照元) プログラムと、そのリクエスト者 IP が正しく記録されている。(ログの記録の徹底) はい ☐ いいえ ☐ 対象外 ☐
- ・プラグインが扱うデータとして個人情報に属するものを、プラグインにおいて独自に EC-CUBE 内または EC-CUBE 配下のデータベース内ならびに他のサーバーやファイル等に保存していない。(個人情報の保持の制限) はい ☐ いいえ ☐ 対象外 ☐
- ・個人情報を扱う場合には、符号化 (ハッシュ) や、番号化 (ID)、またはステータスなどの間接情報のみを扱い、直接保存していない。(個人情報の保持の制限) はい ☐ いいえ ☐ 対象外 ☐
- ・プラグインが生成または設置または一時的にでも取り扱うデータのファイルについて、公開ディレクトリ側に設置していない。() はい ☐ いいえ ☐ 対象外 ☐
- ・CSV ファイルの生成やアップロード時の保存先指定として、公開ディレクトリ側に設置した場合、本当に公開して良いファイル類のみを設置している。(生成ファイルの設置・保存場所の隠蔽) はい ☐ いいえ ☐ 対象外 ☐

2-4. プラグインが行うプログラム介入について

- ・画面表示に関わる部分に対して追加の表示を行う場合は、プラグインが独自に行っていない。(テンプレート利用の徹底) はい ☐ いいえ ☐ 対象外 ☐
- ・プラグインが用いる独自のテンプレート変数など他でも参照・代入が出来る変数は、プラグインの名前を付与して固有の変数名としている。(変数名の固有化) はい ☐ いいえ ☐ 対象外 ☐
- ・必要以上の介入処理を行わず、必要なタイミングのみ介入とデータ操作を行っている。(不要な加入をしない) はい ☐ いいえ ☐ 対象外 ☐