▼ 対応の優先度の定義

必須	現状発生している攻撃手段の直接の要因として可能性が高いもの
推奨	確認、対応を実施することで、リスクを軽減できるもの
状況により判断	カスタマイズ状況により対応判断を行うもの

▼各優先度とカテゴリ

必須
- 意図しないディレクトリ・ファイルが公開されていないか
- 過去の脆弱性を対応しているか(危険度：高)
- デバッグモードが無効になっているか
- SSLの導入状況

推奨
- 過去の脆弱性を対応しているか(危険度：中以下)
- ID/パスワードの管理
- 管理画面のアクセス制限
- ディレクトリ・ファイルの権限不備
- 利用しない機能の無効化
- 機能に関する操作ミス

状況により判断
- カスタマイズ・プラグインによる影響
- EC-CUBE外のプログラムの利用

▼ 対応の優先度の定義

更新日	対象	更新内容
2020/12/3	【チェックリスト_3.x】シート	カテゴリ：【過去の脆弱性への対応(危険度：中以下)】に対して、危険度中の脆弱性対応パッチのURLを2件追加しました。
	全バージョンのシート	昨今の攻撃のトレンドから、カテゴリ【管理画面のアクセス制限】に関する下記項目を【推奨】から【いずれか必須】に変更しました。 【チェックリスト_2.x】シート NO.11,12 【チェックリスト_3.x】シート NO.10,11 【チェックリスト_4.x】シート NO.10,11
2020/6/25	【チェックリスト_3.x】シート 【チェックリスト_4.x】シート	カテゴリ：【過去の脆弱性への対応(危険度：高)】、【過去の脆弱性への対応(危険度：中以下)の内容を更新しました。

EC-CUBE 2.x系 環境チェックリスト　v20201203

No.	更新日	対応優先度	カテゴリ	項目	確認方法	対応方法
1		必須	意図しないディレクトリ・ファイルの露出	data 以下のファイル、フォルダが公開されていないか	EC-CUBEのURL直下(例: https://example.com/path/to/ec-cube/data など)に data フォルダが公開されていないかご確認ください。 もしくは、 EC-CUBEの URL と同階層(例: https://example.com/path/to/ec-cube の場合 https://example.com/path/to/data) に data フォルダが公開されていないかご確認ください。 https://example.com/path/to/ec-cube/data/Smarty/templates/default/site_frame.tpl などにアクセスし、ファイルの中身が表示されないことをご確認ください。	data フォルダに .htaccess というファイル名で、以下の内容を保存してください。 order allow,deny deny from all 保存した後、ファイルの中身が表示されないことをご確認ください。
2		必須	意図しないディレクトリ・ファイルの露出	install 以下のファイル、フォルダが公開されていないか	EC-CUBEのURL直下(例: https://example.com/path/to/ec-cube/install など)に install フォルダが存在するかご確認ください。	通常の運用では使用しないプログラムが含まれています。 install フォルダを削除してください。
3		必須	意図しないディレクトリ・ファイルの露出	test 以下のファイル、フォルダが公開されていないか	EC-CUBEのURL直下(例: https://example.com/path/to/ec-cube/test など)に test フォルダが存在するかご確認ください。	通常の運用では使用しないプログラムが含まれています。 test フォルダを削除してください。
4		必須	意図しないディレクトリ・ファイルの露出	tests 以下のファイル、フォルダが公開されていないか	EC-CUBEのURL直下(例: https://example.com/path/to/ec-cube/tests など)に tests フォルダが存在するかご確認ください。	通常の運用では使用しないプログラムが含まれています。 tests フォルダを削除してください。
5		必須	意図しないディレクトリ・ファイルの露出	管理画面の URL を変更したにも関わらず、標準の admin フォルダが残存していないか	管理画面の URL を標準の admin から変更した場合、 admin フォルダが残っていないことをご確認ください。	admin フォルダが残っている場合 使用しなくなったプログラムが含まれています。 admin を削除してください。
6		必須	デバッグモードの無効化	デバッグモードが有効になっていないか	デバッグモードが有効になっていないかをご確認ください。	システム設定＞パラメータ設定より、DEBUG_MODEの値をfalseに設定してください。
7		必須	過去の脆弱性への対応(危険度：高)	公表された脆弱性のうち、危険度：高のものが修正されているか	https://www.ec-cube.net/info/weakness/index.php?level=3 にアクセスし、お使いのバージョンの危険度：高の脆弱性対応が済んでいるかご確認ください。 2020年01月30日現在 2.13.1 ~ 2.17.0 は確認されたすべての危険度高の脆弱性対応が完了しているバージョンとなります。	脆弱性に応じた修正をおこなってください。 カスタマイズ等をおこなっている場合は、委託先の制作会社・開発会社へご相談ください。
8		必須	SSLの導入	SSLが導入されているか	EC-CUBE に https:// からの URL でアクセスできるかご確認ください	https:// からの URL でアクセスできない場合 SSLを導入してください。
9		必須	SSLの導入	管理画面へのアクセスには常に SSL を利用している	管理画面へのアクセス時に、http://で表示されないことをご確認ください。	SSLの導入後に、システム設定＞管理画面設定より、SSLを強制するを設定してください。
10		必須	ID/パスワード管理	管理画面のユーザーID/パスワードが推測されやすいものになっていないか	ユーザーIDとパスワードが同じ ユーザーIDが admin など推測されやすいもの パスワードが8文字以下 パスワードが数字のみ、英字のみ など、推測されやすいIDパスワードになっていないかご確認ください	システム設定＞メンバー管理より、適切なパスワードを設定ください。
11	2020/12/3	いずれか必須(※)	管理画面のアクセス制限	管理画面が推測しやすい URL になっていないか	管理画面の URL が admin など推測しやすい URL になっていないことをご確認ください。 **変更後にNo.5のadminフォルダが残存していないかもめずご確認ください。**	システム設定＞セキュリティ設定より、admin 以外に変更してください。
12	2020/12/3	いずれか必須(※)	管理画面のアクセス制限	管理画面のIP制限は実施しているか	固定IPをお持ちの場合、管理画面へのアクセスを制限しているかをご確認ください	システム設定＞セキュリティ設定より、ipアドレスを設定してください。
13		推奨	過去の脆弱性への対応(危険度：中以下)	公表された脆弱性のうち、危険度：中以下のものが修正されているか	https://www.ec-cube.net/info/weakness/ にアクセスし、お使いのバージョンの危険度：中以下の脆弱性対応が済んでいるかご確認ください。 2020年01月31日現在 2.13.5、2.17.0 は確認されたすべての脆弱性対応が完了しているバージョンとなります。	脆弱性に応じた修正をおこなってください。 カスタマイズ等をおこなっている場合は、委託先の制作会社・開発会社へご相談ください。
14		推奨	SSLの導入	SSL Labs（https://www.ssllabs.com/ssltest/index.html）にて、SSL のランクが B以上だと表示される	SSL Labs（https://www.ssllabs.com/ssltest/index.html）にて、SSL のランクが B以上だと表示される	確認結果をもってサーバー管理者や委託先の制作会社・開発会社へご相談ください。
15		推奨	ディレクトリ・ファイルの権限不備	パーミッション777のファイル、フォルダが存在しないか	パーミッションが 777 となっているファイル、フォルダが存在しないことをご確認ください	パーミッション777のファイル、フォルダが存在する場合 ファイルは 604、 フォルダは 705 など、ご利用のサーバーでの適切なパーミッションに変更してください。 テンプレートや、画像フォルダなど、Webサーバーから書き込みが必要な場合は、ファイル: 606、フォルダ: 707など、書き込み許可が必要な場合があります。
16		推奨	ディレクトリ・ファイルの権限不備	パーミッション666のファイルが存在しないか	パーミッションが 666 となっているファイルが存在しないことをご確認ください	ファイルは 604 など、ご利用のサーバーでの適切なパーミッションに変更してください。 テンプレートなど、Webサーバーから書き込みが必要な場合は、606 など、書き込み許可が必要な場合があります。
17		推奨	利用しない機能の無効化	API が有効になっていないか	EC-CUBEのURL直下(例: https://example.com/path/to/ec-cube/api など)にアクセスし、ページが見つかりません もしくは、 API機能が無効です。 と表示されることをご確認ください。	API機能を利用しない場合は、html/api フォルダを完全に削除してください。
18		推奨	機能に関する操作ミス	user_data 以下に CSV ファイルが存在しないか	user_data フォルダ以下に CSV ファイルが存在しないかご確認ください。	存在する場合はファイルを削除してください
19		推奨	機能に関する操作ミス	upload 以下に CSV ファイルが存在しないか	upload フォルダ以下に CSV ファイルが存在しないかご確認ください	存在する場合はファイルを削除してください
20		推奨	意図しないディレクトリ・ファイルの露出	運用では利用しない開発用ファイルが公開されている	EC-CUBEのURL直下(例: https://example.com/path/to/ec-cube/composer.json など)に以下のファイルが存在するかご確認ください。 build.xml phpunit.xml.dist Gruntfile.js composer.json composer.lock package.json package-lock.json	通常の運用では使用しないプログラムが含まれています。 該当のファイルを削除してください。
21		状況により判断	EC-CUBE外のプログラムの利用	他の CMS バージョン(本体, プラグイン)は最新か	WordPress など利用している製品が最新バージョンが導入されているかご確認ください。	最新バージョンでは無い場合は、最新バージョンにバージョンアップしてください。 お使いのCMSによって異なりますので、詳しくはお使いのCMSの情報をご確認ください。
22		状況により判断	EC-CUBE外のプログラムの利用	他のフリーCGIを使用していないか	フリーで配布されている CGI を使用していないかご確認ください。	EC-CUBEは機密情報を扱いますので、フリーで配布されている CGI との同時利用はおすすめしません。 フリーで配布されている CGI を使用されている場合、ご利用の中止をご検討ください。
23		状況により判断	カスタマイズ・プラグインによる影響	独自テンプレートでエスケープ漏れなど無いか	フォームの input タグなどにエスケープ漏れが無いかご確認ください。 以下のようにタグのvalue 属性に h が付与されていることをご確認ください。 <input type="text" name="<!--{$key1}-->" value="<!--{$arrForm[$key1].value|h}-->" />	エスケープ漏れを確認した場合、value に h が付与する修正を行ってください。 サンプル： <input type="text" name="<!--{$key1}-->" value="<!--{$arrForm[$key1].value|h}--->" />
24		状況により判断	カスタマイズ・プラグインによる影響	独自カスタマイズ, プラグインで eval を使用している箇所は無いか	ソースを検索し、 eval 関数を使用している箇所は無いかご確認ください。	eval 関数の使用は推奨しませんので、その他の方法をご検討ください。
25		状況により判断	カスタマイズ・プラグインによる影響	独自カスタマイズ, プラグインで serialize/unserialize を使用している箇所は無いか	ソースを検索し、 serialize/unserialize 関数を使用している箇所は無いかご確認ください。	serialize/unserialize 関数の使用は推奨しませんので、その他の方法をご検討ください。
26		状況により判断	カスタマイズ・プラグインによる影響	独自カスタマイズ, プラグインで SQL を実行する際, プレースホルダを使用しているか	ソースを確認し、以下のようにプレースホルダ利用せずに、変数を直接 SQL に渡しているものが無いか確認してください。 $sql = "SELECT * FROM dtb_products WHERE product_id = '".$product_id."';";	プレースホルダを使用していないことが確認できた場合、修正を行ってください。

※ No. 11、No. 12の管理画面アクセス制御は、いずれか、もしくは両方の対応が必須となります。

EC-CUBE 3.x系 環境チェックリスト　v20201203

No.	更新日	対応優先度	カテゴリ	項目	確認方法	対応方法
1		必須	意図しないディレクトリ・ファイルの露出	app が公開されていないか	EC-CUBEのURL直下(例: https://example.com/path/to/ec-cube/app など)に app フォルダが公開されていないかご確認ください。 app/console などにアクセスし、ファイルの中身が表示されないことをご確認ください。	app フォルダに .htaccess というファイル名で、以下の内容を保存してください。 order allow,deny deny from all
2		必須	意図しないディレクトリ・ファイルの露出	vendor が公開されていないか	EC-CUBEのURL直下(例: https://example.com/path/to/ec-cube/vendor など)に vendor フォルダが公開されていないかご確認ください。 vendor/symfony/config/README.md などにアクセスし、ファイルの中身が表示されないことをご確認ください。	vendor フォルダに .htaccess というファイル名で、以下の内容を保存してください。 order allow,deny deny from all
3		必須	意図しないディレクトリ・ファイルの露出	インストール用のファイルが残されている	EC-CUBEのURL直下(例: https://example.com/path/to/ec-cube/install.php など)に以下のようなファイル が存在するかご確認ください。 install.php eccube_install.php eccube_install.sh	通常の運用では使用しないプログラムが含まれています。 install.php を削除してください。
4		必須	意図しないディレクトリ・ファイルの露出	tests 以下のファイル、フォルダが公開されていないか	tests 以下のファイル、フォルダが公開されていないか	通常の運用では使用しないプログラムが含まれています。 tests フォルダを削除してください。
5		必須	デバッグモードの無効化	デバッグモードが有効になっていないか	index_dev.phpにアクセスし、デバッグモードが有効になっていないことをご確認ください。	開発環境でのみindex_dev.php経由でのデバッグモードを利用し、本番環境では index_dev.phpを削除してください。
6	2020/6/25	必須	過去の脆弱性への対応(危険度：高)	公表された脆弱性のうち、危険度：高のものが修正されているか	https://www.ec-cube.net/info/weakness/index.php?level=3 にアクセスし、お使いのバージョンの危険度：高の脆弱性対応が済んでいるかご確認ください。 2020年06月22日 現在 3.0.4~3.0.18 は確認されたすべての危険度高の脆弱性対応が完了しているバージョンとなります。	脆弱性に応じた修正をおこなってください。 カスタマイズ等をおこなっている場合は、委託先の制作会社・開発会社へご相談ください。
7		必須	SSLの導入	SSLが導入されているか	EC-CUBE に https:// からの URL でアクセスできるかご確認ください	https:// からの URL でアクセスできない場合 SSLを導入してください。
8		必須	SSLの導入	管理画面へのアクセスには常に SSL を利用している	管理画面へのアクセス時に、http://で表示されないことをご確認ください。	SSLの導入後に、システム設定＞セキュリティ設定より、SSLを強制するを設定してください。
9		必須	ID/パスワード管理	管理画面のユーザーID/パスワードが推測されやすいものになっていないか	ユーザーIDとパスワードが同じ ユーザーIDが admin など推測されやすいもの パスワードが8文字以下 パスワードが数字のみ、英字のみ など、推測されやすいID/パスワードになっていないかご確認ください	システム設定＞メンバー管理より、適切なパスワードを設定ください。
10	2020/12/3	いずれか必須(※)	管理画面のアクセス制限	管理画面が推測しやすい URL になっていないか	管理画面の URL が admin など推測しやすい URL になっていないことをご確認ください。	システム設定＞セキュリティ設定より、admin 以外に変更してください。
11	2020/12/3	いずれか必須(※)	管理画面のアクセス制限	管理画面のIP制限は実施しているか	固定IPをお持ちの場合、管理画面へのアクセスを制限しているかをご確認ください	システム設定＞セキュリティ設定より、ipアドレスを設定してください。
12	2020/12/3	推奨	過去の脆弱性への対応(危険度：中以下)	公表された脆弱性のうち、危険度：中以下のものが修正されているか	https://www.ec-cube.net/info/weakness/ にアクセスし、お使いのバージョンの危険度：中以下の脆弱性対応が済んでいるかご確認ください。 2020年12月3日 現在 2020年6月17日、2020年12月3日に危険度中の脆弱性対応のため修正パッチを公開しております。 3系最終版 3.0.18をお使いの場合でも、パッチの適用が必要になります。 https://www.ec-cube.net/info/weakness/weakness.php?id=73 https://www.ec-cube.net/info/weakness/weakness.php?id=75 https://www.ec-cube.net/info/weakness/weakness.php?id=76	脆弱性に応じた修正をおこなってください。 カスタマイズ等をおこなっている場合は、委託先の制作会社・開発会社へご相談ください。
13		推奨	SSLの導入	SSL Labs（https://www.ssllabs.com/ssltest/index.html）にて、SSL のランクが B以上だと表示される	SSL Labs（https://www.ssllabs.com/ssltest/index.html）にて、SSL のランクが B以上だと表示される	確認結果をもってサーバー管理者や委託先の制作会社・開発会社へご相談ください。
14		推奨	ディレクトリ・ファイルの権限不備	パーミッション777のファイル、フォルダが存在しないか	パーミッションが 777 となっているファイル、フォルダが存在しないことをご確認ください	パーミッション777のファイル、フォルダが存在する場合 ファイルは 604、 フォルダは 705 など、ご利用のサーバーでの適切なパーミッションに変更してください。 テンプレートや、画像フォルダなど、Webサーバーから書き込みが必要な場合は、ファイル: 606、フォルダ: 707など、書き込み許可が必要な場合があります。
15		推奨	ディレクトリ・ファイルの権限不備	パーミッション666のファイルが存在しないか	パーミッションが 666 となっているファイルが存在しないことをご確認ください	ファイルは 604 など、ご利用のサーバーでの適切なパーミッションに変更してください。 テンプレートなど、Webサーバーから書き込みが必要な場合は、606 など、書き込み許可が必要な場合があります。
16		推奨	利用しない機能の無効化	利用していないAPIプラグインをインストールして、API が有効になっていないか	EC-CUBEのURL直下(例: https://example.com/path/to/ec-cube/api など)にアクセスし、ページが見つかりません もしくは、 API機能が無効です。 と表示されることをご確認ください。	API機能を利用しない場合は、APIプラグインをアンインストールしてください。

17		推奨	意図しないディレクトリ・ファイルの露出	運用では利用しない開発用ファイルが公開されている	EC-CUBEのURL直下(例: https://example.com/path/to/ec-cube/)に 以下のようなファイルが存在するかご確認ください。 composer.json composer.lock phpunit.xml.dist web.config.sample	通常の運用では使用しないプログラムが含まれています。 該当のファイルを削除してください。
18		推奨	機能に関する操作ミス	user_data 以下に CSV ファイルが存在しないか	user_data フォルダ以下に CSV ファイルが存在しないかご確認ください。	存在する場合はファイルを削除してください
19		推奨	機能に関する操作ミス	upload 以下に CSV ファイルが存在しないか	upload フォルダ以下に CSV ファイルが存在しないかご確認くださ	存在する場合はファイルを削除してください
20		状況により判断	EC-CUBE外のプログラムの利用	他の CMS バージョン(本体, プラグイン)は最新か	WordPress など利用している製品が最新バージョンが導入されているかご確認ください。	最新バージョンでは無い場合は、最新バージョンにバージョンアップしてください。 お使いのCMSによって異なりますので、詳しくはお使いのCMSの情報をご確認ください。
21		状況により判断	EC-CUBE外のプログラムの利用	他のフリーCGIを使用していないか	フリーで配布されている CGI を使用していないかご確認ください。	EC-CUBEは機密情報を扱いますので、フリーで配布されている CGI との同時利用はおすすめしません。 フリーで配布されている CGI を使用されている場合、ご利用の中止をご検討ください。
22		状況により判断	カスタマイズ・プラグインによる影響	独自テンプレートでエスケープ漏れなど無いか	テンプレートファイルを |raw で検索し、フォームの input タグなどに意図せず |raw と記載されている箇所がないかご確認ください。	意図せず利用している |raw を削除してください。
23		状況により判断	カスタマイズ・プラグインによる影響	独自カスタマイズ, プラグインで eval を使用している箇所は無いか	ソースを検索し、 eval 関数を使用している箇所は無いかご確認ください。	eval 関数の使用は推奨しませんので、その他の方法をご検討ください。
24		状況により判断	カスタマイズ・プラグインによる影響	独自カスタマイズ, プラグインで serialize/unserialize を使用している箇所は無いか	ソースを検索し、 serialize/unserialize 関数を使用している箇所は無いかご確認ください。	serialize/unserialize 関数の使用は推奨しませんので、その他の方法をご検討ください。
25		状況により判断	カスタマイズ・プラグインによる影響	独自カスタマイズ, プラグインで SQL を実行する際, プレースホルダを使用しているか	ソースを確認し、以下のようにプレースホルダ利用せずに、変数を直接 SQL に渡しているものが無いか確認してください。 $sql = "SELECT * FROM dtb_products WHERE product_id = '".$product_id."';";	プレースホルダを使用していないことが確認できた場合、修正を行ってください。

※ No. 10、No. 11の管理画面アクセス制御は、どちらか、もしくは両方の対応が必須となります。

EC-CUBE 4.x系 環境チェックリスト　　v20201203

No.	更新日	対応優先度	カテゴリ	項目	確認方法	対応方法
1		必須	意図しないディレクトリ・ファイルの露出	var が公開されていないか	EC-CUBEのURL直下(例: https://example.com/path/to/ec-cube/var など)に var フォルダが公開されていないかご確認ください。 var/cache/prod/annotations.map などにアクセスし、ファイルの中身が表示されないことをご確認ください。	var フォルダに .htaccess というファイル名で、以下の内容を保存してください。 order allow,deny deny from all
2		必須	意図しないディレクトリ・ファイルの露出	.env が公開されていないか	EC-CUBEのURL直下(例: https://example.com/path/to/ec-cube/.env など)に .env ファイルが公開されていないか、ファイルの中身が表示されないことをご確認ください。	EC-CUBE をインストールしたフォルダの .htaccess ファイルに以下の内容を追加し、保存してください。 <FilesMatch "^composer|^COPYING|^¥.env|^¥.maintenance|^Procfile|^app¥.json|^gulpfile¥.js|^package¥.json|^package-lock¥.json|web¥.config|^Dockerfile|¥.(ini|lock|dist|git|sh|bak|swp|env|twig|yml|yaml|dockerignore)$"> order allow,deny deny from all </FilesMatch>
3		必須	意図しないディレクトリ・ファイルの露出	vendor が公開されていないか	EC-CUBEのURL直下(例: https://example.com/path/to/ec-cube/vendor など)に vendor フォルダが公開されていないかご確認ください。 vendor/symfony/config/README.md などにアクセスし、ファイルの中身が表示されないことをご確認ください。	vendor フォルダに .htaccess というファイル名で、以下の内容を保存してください。 order allow,deny deny from all
4		必須	意図しないディレクトリ・ファイルの露出	codeception が公開されていないか	EC-CUBEのURL直下(例: https://example.com/path/to/ec-cube/codeception など)に codeception フォルダが存在するかご確認ください。	codeception フォルダが存在する場合 通常の運用では使用しないプログラムが含まれています。 codeception フォルダを削除してください。
5		必須	デバッグモードの無効化	デバッグモードが有効になっていないか	.env ファイルや、 .htaccess ファイルに設定されている APP_ENV の値が dev になっていないかご確認ください。	APP_ENV=dev になっている場合 開発用途で使用する設定になっています。 本番環境では、 APP_ENV を prod に設定してください。
6	2020/6/25	必須	過去の脆弱性への対応(危険度：高)	公表された脆弱性のうち、危険度：高のものが修正されているか	https://www.ec-cube.net/info/weakness/index.php?level=3 にアクセスし、お使いのバージョンの危険度：高の脆弱性対応が済んでいるかご確認ください。 2020年06月22日 現在 4.0系 では危険度高の脆弱性は確認されていません。	脆弱性に応じた修正をおこなってください。 カスタマイズ等をおこなっている場合は、委託先の制作会社・開発会社へご相談ください。
7		必須	SSLの導入	SSLが導入されているか	EC-CUBE に https:// からの URL でアクセスできるかご確認ください	https:// からの URL でアクセスできない場合 SSLを導入してください。
8		必須	SSLの導入	管理画面へのアクセスには常に SSL を利用している	管理画面へのアクセス時に、http://で表示されないことをご確認ください。	SSLの導入後に、システム設定＞セキュリティ設定より、SSLを強制するを設定してください。
9		必須	ID/パスワード管理	管理画面のユーザーID/パスワードが推測されやすいものになっていないか	ユーザーIDとパスワードが同じ ユーザーIDが admin など推測されやすいもの パスワードが8文字以下 パスワードが数字のみ、英字のみ など、推測されやすいIDパスワードになっていないかご確認ください	システム設定＞メンバー管理より、適切なパスワードを設定ください。
10	2020/12/3	いずれか必須(※)	管理画面のアクセス制限	管理画面が推測しやすい URL になっていないか	管理画面の URL が admin など推測しやすい URL になっていないことをご確認ください。	システム設定＞セキュリティ設定より、admin 以外に変更してください。
11	2020/12/3	いずれか必須(※)	管理画面のアクセス制限	管理画面のIP制限は実施しているか	固定IPをお持ちの場合、管理画面へのアクセスを制限しているかをご確認ください	システム設定＞セキュリティ設定より、ipアドレスを設定してください。
12	2020/6/25	推奨	過去の脆弱性への対応(危険度：中以下)	公表された脆弱性のうち、危険度：中以下のものが修正されているか	https://www.ec-cube.net/info/weakness/ にアクセスし、お使いのバージョンの危険度：中以下の脆弱性対応が済んでいるかご確認ください。 2020年06月22日 現在 4.0.4 は確認されたすべての脆弱性対応が完了しているバージョンとなります。	脆弱性に応じた修正をおこなってください。 カスタマイズ等をおこなっている場合は、委託先の制作会社・開発会社へご相談ください。
13		推奨	SSLの導入	SSL Labs（https://www.ssllabs.com/ssltest/index.html）にて、SSL のランクが B以上だと表示される	SSL Labs（https://www.ssllabs.com/ssltest/index.html）にて、SSL のランクが B以上だと表示される	確認結果をもってサーバー管理者や委託先の制作会社・開発会社へご相談ください。
14		推奨	ディレクトリ・ファイルの権限不備	パーミッション777のファイル、フォルダが存在しないか	パーミッションが 777 となっているファイル、フォルダが存在しないことをご確認ください	パーミッション777のファイル、フォルダが存在する場合 ファイルは 604、 フォルダは 705 など、ご利用のサーバーでの適切なパーミッションに変更してください。 テンプレートや、画像フォルダなど、Webサーバーから書き込みが必要な場合は、ファイル: 606、フォルダ: 707など、書き込み許可が必要な場合があります。
15		推奨	ディレクトリ・ファイルの権限不備	パーミッション666のファイルが存在しないか	パーミッションが 666 となっているファイルが存在しないことをご確認ください	ファイルは 604 など、ご利用のサーバーでの適切なパーミッションに変更してください。 テンプレートなど、Webサーバーから書き込みが必要な場合は、606 など、書き込み許可が必要な場合があります。

16		推奨	意図しないディレクトリ・ファイルの露出	運用では利用しない開発用ファイルが公開されている	EC-CUBEのURL直下(例: https://example.com/path/to/ec-cube/composer.json など)に以下のファイルが存在するかご確認ください。 Dockerfile composer.json composer.lock gulpfile.js package-lock.json package.json symfony.lock web.config	EC-CUBE をインストールしたフォルダの .htaccess ファイルに以下の内容を追加し、保存してください。 <FilesMatch "^composer|^COPYING|^¥.env|^¥.maintenance|^Procfile|^app¥.json|^gulpile¥.js|^package¥.json|^package-lock¥.json|web¥.config|^Dockerfile|¥.(ini|lock|dst|git|sh|bak|swp|env|twig|yml|yaml|dockerignore)$"> order allow,deny deny from all </FilesMatch>
17		推奨	機能に関する操作ミス	user_data 以下に CSV ファイルが存在しないか	user_data フォルダ以下に CSV ファイルが存在しないかご確認ください。	存在する場合はファイルを削除してください
18		推奨	機能に関する操作ミス	upload 以下に CSV ファイルが存在しないか	upload フォルダ以下に CSV ファイルが存在しないかご確認くださ	存在する場合はファイルを削除してください
19		状況により判断	EC-CUBE外のプログラムの利用	他の CMS バージョン(本体, プラグイン)は最新か	WordPress など利用している製品が最新バージョンが導入されているかご確認ください。	最新バージョンでは無い場合は、最新バージョンにバージョンアップしてください。 お使いのCMSによって異なりますので、詳しくはお使いのCMSの情報をご確認ください。
20		状況により判断	EC-CUBE外のプログラムの利用	他のフリーCGIを使用していないか	フリーで配布されている CGI を使用していないかご確認ください。	EC-CUBEは機密情報を扱いますので、フリーで配布されている CGI との同時利用はおすすめしません。 フリーで配布されている CGI を使用されている場合、ご利用の中止をご検討ください。
21		状況により判断	カスタマイズ・プラグインによる影響	独自テンプレートでエスケープ漏れなど無いか	テンプレートファイルを |raw で検索し、フォームの input タグなどに意図せず |raw と記載されている箇所がないかご確認ください。	意図せず利用している |raw を削除してください。
22		状況により判断	カスタマイズ・プラグインによる影響	独自カスタマイズ, プラグインで eval を使用している箇所は無いか	ソースを検索し、 eval 関数を使用している箇所は無いかご確認ください。	eval 関数の使用は推奨しませんので、その他の方法をご検討ください。
23		状況により判断	カスタマイズ・プラグインによる影響	独自カスタマイズ, プラグインで serialize/unserialize を使用している箇所は無いか	ソースを検索し、 serialize/unserialize 関数を使用している箇所は無いかご確認ください。	serialize/unserialize 関数の使用は推奨しませんので、その他の方法をご検討ください。
24		状況により判断	カスタマイズ・プラグインによる影響	独自カスタマイズ, プラグインで SQL を実行する際, プレースホルダを使用しているか	ソースを確認し、以下のようにプレースホルダ利用せずに、変数を直接 SQL に渡しているものが無いか確認してください。 $sql = "SELECT * FROM dtb_products WHERE product_id = '".$product_id."';";	プレースホルダを使用していないことが確認できた場合、修正を行ってください。

※ No. 10、No. 11の管理画面アクセス制御は、どちらか、もしくは両方の対応が必須となります。