CONFIDENTIAL

SAMPLE

〇〇〇株式会社　御中

Web アプリケーション標準診断
（修正確認診断）
診断結果報告書

〇〇〇〇年〇月〇日

株式会社サイバーセキュリティクラウド

SAMPLE

【資料改編履歴】

日 付	内 容	承 認	作成/更新
○○○○年○月○日	第一版作成	○○	○○

目　　次

1　はじめに

本診断結果報告書は、Web アプリケーション標準診断において〇〇〇〇年△月△日に実施した修正確認診断の診断結果についてご報告するものです。

1－1　目的

本修正確認診断の目的は、前回（〇〇〇〇年◎月◎日）実施した Web アプリケーション標準診断により検出された脆弱性について、適切な対策が行われていることを確認することにあります。

1－2　診断期間および診断内容

本修正確認診断は、表 1-2-1 の日程で実施いたしました。

表 1-2-1　診断期間および診断内容

診断種別	診断期間	診断内容
リモート診断	〇〇〇〇年△月△日（10 時から 12 時まで）	リモートにて、前回検出された脆弱性への対策内容について手動による確認作業を実施しました。

1－3　診断対象

本修正確認診断における診断対象は以下の通りです。

〇〇〇サイト

	検出された脆弱性（診断項目）	危険度	確認対象画面／URL ※1
1	クロスサイトスクリプティング（クロスサイトスクリプティング）	High	2. 実行 https://www.example.com/Input
2			4. 実行 https://www.example.com/Show
3			6. 実行 https://www.example.com/InputBundle
4			（診断対象外） https://www.example.com/Update

	検出された脆弱性（診断項目）	危険度	確認対象画面／URL ※1
5	クロスサイトリクエストフォージェリ（クロスサイトリクエストフォージェリ）	Medium	9. 実行 https://www.example.com/Password
6		Low	10. 実行 https://www.example.com/ResetPassword
7	IP アドレスでアクセス可能（既知の脆弱性）	Low	https://192.168.1.1/Login 等
8	ディレクトリリスティングが有効（強制ブラウジング）	Low	https://www.example.com/icons/ 等
9	サンプルページの存在（強制ブラウジング）	Low	https://www.example.com/examples/ 等
10	マニュアルページの存在（強制ブラウジング）	Low	https://www.example.com/manual/ 等
11	アプリケーション標準エラーページの使用（サードパーティ製品の設定ミス）	Low	https://www.example.com/Show 等
12			https://www.example.com/examples/xxx 等
13	アプリケーションバージョンの出力（サードパーティ製品の設定ミス）	Low	https://www.example.com/examples/xxx 等
14			https://www.example.com/manual/ 等

※1　POST パラメータの記述については、割愛させていただいております。

2　診断結果

2－1　総合評価

今回実施した修正確認診断の診断結果に基づき、弊社の評価基準に照合した総合評価を脆弱性診断に対して行いました。以下に評価クラスと評価の根拠となった診断結果を示します。

○○○サイト

A	前回確認された脆弱性について、全てが適切に対策が行われており、セキュリティ上問題がない状態です

- 「クロスサイトスクリプティング（危険度：High）」、および「クロスサイトリクエストフォージェリ（危険度：Medium/Low）」について、適切に対策が行われていることを確認しております。
- 前回の診断時に検出されていたな軽微な脆弱性（危険度:Low）についても、適切に対策が行われていることを確認しております。

参考までに、前回の脆弱性診断結果における総合評価を以下に示します。

C	危険性の高い脆弱性が確認されており、セキュリティ上問題のある状態です。

- 成りすましによる個人情報の漏洩等に繋がる可能性のある「クロスサイトスクリプティング」が確認されております
- ユーザの操作無しに仮登録メールを大量に送付することが可能な「クロスサイトリクエストフォージェリ」が確認されております
- サーバ設定に起因する軽微な問題が確認されております

評価基準につきましては、付録の「3－3　評価基準」として添付しておりますので、必要に応じてご参照下さい。

2－2　概要

本修正確認診断の診断対象範囲において検出された脆弱性を危険度別に集計したものを図 2-2-1 危険度別脆弱性検出数に、診断項目別に集計したものを図 2-2-2　診断項目別脆弱性検出数、表 2-2-1 診断項目別脆弱性検出数一覧に示します。

図 2-4-1　危険度別脆弱性検出数

図 2-4-2　診断項目別脆弱性検出数

表 2-2-1　診断項目別脆弱性検出数一覧

診断項目	危険度	○○○サイト	
		修正確認診断	前回
クロスサイトスクリプティング	High	0	4
ステルスコマンド	-	-	-
SQL インジェクション	-	-	-
バッファオーバーフロー	-	-	-
既知の脆弱性	Low	0	1
強制ブラウジング	Low	0	3
hidden フィールドの操作	-	-	-
サードパーティ製品の設定ミス	Low	0	4
バックアップファイルの検出	-	-	-
バックドア、デバッグオプション	-	-	-
HTML 中のコメント	-	-	-
ディレクトリトラバーサル	-	-	-
不適切なエラーハンドリング	-	-	-
パラメータの改竄	-	-	-
Web サービスの脆弱性	-	-	-
クロスサイトリクエストフォージェリ	Medium	0	1
	Low	0	1
セッション管理の脆弱性	-	-	-
合　計	Critical	0	0
	High	0	4
	Medium	0	1
	Low	0	9

また、本修正確認診断において確認された対策状況について表 2-2-2　確認結果一覧に示します。表中の対策状況欄は、〇が対策済、△が一部対策済、×が未対策を示します。

なお、背景がグレーになっている項目は、担当者様より今回の修正内容に含まれていないことを確認した項目を示しています。

表 2-2-2　確認結果一覧

	検出された脆弱性	危険度	対策状況
1	クロスサイトスクリプティング（クロスサイトスクリプティング）	High	〇
2			〇
3			〇
4			〇
5	クロスサイトリクエストフォージェリ（クロスサイトリクエストフォージェリ）	Medium	〇
6		Low	〇
7	IP アドレスでアクセス可能（既知の脆弱性）	Low	〇
8	ディレクトリリスティングが有効（強制ブラウジング）	Low	〇
9	サンプルページの存在（強制ブラウジング）	Low	〇
10	マニュアルページの存在（強制ブラウジング）	Low	〇
11	アプリケーション標準エラーページの使用（サードパーティ製品の設定ミス）	Low	〇
12			〇
13	アプリケーションバージョンの出力（サードパーティ製品の設定ミス）	Low	〇
14			〇

本修正確認診断の結果より、前回確認された全ての脆弱性について、適切に対策が行われていることを確認しており、セキュリティ上の問題がない状態です。

今後の Web アプリケーションセキュリティへの対策としては、脆弱性が発生することを予防することも念頭に置き、以下のような対応の検討をお奨めします。

✓　開発当初からセキュリティを考慮した Web アプリケーションの実装の実施

開発時からセキュリティを考慮した実装を行うことにより、よりセキュリティ的に安全な Web アプリケーションを構築することが可能となります。通常の開発では開発者・開発会社によってセキュリティレベルが大きく変化することが予想されますが、開発指針・チェックリストを作成しておくことで最低限のセキュリティレベルを維持することが可能になると考えます。

✓ Web アプリケーションファイアウォールの導入による防衛

リリース前の脆弱性診断が難しいケースや、頻繁に Web サイトの更新を行うようなサイトでは、Web アプリケーションファイアウォールの導入が効果的です。クロスサイトスクリプティングや SQL インジェクション等多くの Web アプリケーション脆弱性に対して防衛することが可能です。

危険度につきましては、付録の「3－2　危険度の判定基準」として添付しておりますので、必要に応じてご参照下さい。

3　付録

3－1　危険度の判定基準

本報告書では検出された各脆弱性について、表 3-1-1 を基に危険度を判定し記載しています。

危険度は、検出された各脆弱性への対策の際に、どの脆弱性を優先的に修正すべきか判断するための目安として記載しているものです。

表 3-1-1　危険度の判定基準

危険度	判定基準
Critical	直接的に深刻な被害を及ぼすことが懸念される脆弱性。 SQL インジェクション等が該当します。
High	フィッシング詐欺等、受動的な攻撃により個人情報等の重要な情報を奪われるような被害が想定される重大な脆弱性。 Critical との違いは、Critical は攻撃者が能動的に攻撃を行うことが可能な脆弱性を対象としているのに対し、High はユーザが罠にかかるのを待つような受動的な手法が採られる脆弱性を対象としています。 クロスサイトスクリプティング等が該当します。
Medium	他の脆弱性と組み合わせることによって被害を受けることが想定される脆弱性。ディレクトリリスティングなどが該当します。
Low	Medium 以上に該当せず、被害を受ける可能性が低いと考えられる脆弱性。サードパーティ製品の設定ミスなどが該当します。

判定基準はあくまでも目安であり、脆弱性の検出された箇所・内容等により判定基準とは異なる危険度を脆弱性に与えることもありますので、ご了承下さい。

3－2　評価基準

本報告書における総合評価は、表 3-2-1 に規定される絶対評価と、診断対象の環境を考慮して評価される相対評価によるものです。

絶対評価は、A、B、C、D のいずれかのアルファベット 1 文字で表記され、診断結果を絶対評価の評価基準に照合し適合するクラスが評価として与えられます。

表 3-2-1　絶対評価の評価基準

クラス	評価基準
A	脆弱性が検出されていない。
B	システム情報の漏洩を始めとした、単体では被害を受ける可能性が低いと考えられる脆弱性のみ検出されている。
C	危険性の高い脆弱性が検出されており、被害を受ける可能性がある。
D	個人情報の漏洩に繋がる深刻な脆弱性が検出されている。または、検出されている複数の脆弱性を組み合わせることで個人情報の漏洩に繋がることが懸念される状態である。

相対評価は、絶対評価では表すことが出来ない診断対象の環境やリスト対象等、外的要因について考慮されて評価されるものであり、＋（プラス；より安全）、－（マイナス；より安全でない）を絶対評価に付与することで表されます。

なお、上記評価基準は、弊社の診断実績を基に、診断結果を簡潔に表現するために作成された、弊社独自基準になります。上記評価基準による評価は、あくまでも診断結果を簡潔に表現するためのものであり、弊社は評価に対しての保証や責任は負いかねますのでご了承下さい。

以上