CONFIDENTIAL

SAMPLE

〇〇〇〇〇株式会社　御中

Web アプリケーション標準診断
診断実施計画書

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

【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　目的

本計画書の目的は、Web アプリケーション標準診断を実施するために必要な情報をまとめ、事前に内容を把握・確認を行い、円滑な診断作業を実現することにあります。

2　適用範囲

本計画書の適用範囲は、「３　診断概要」に示す Web アプリケーション標準診断に対するものとします。

3　診断概要

Web アプリケーション標準診断について、以下の内容で実施いたします。

3－1　診断日時

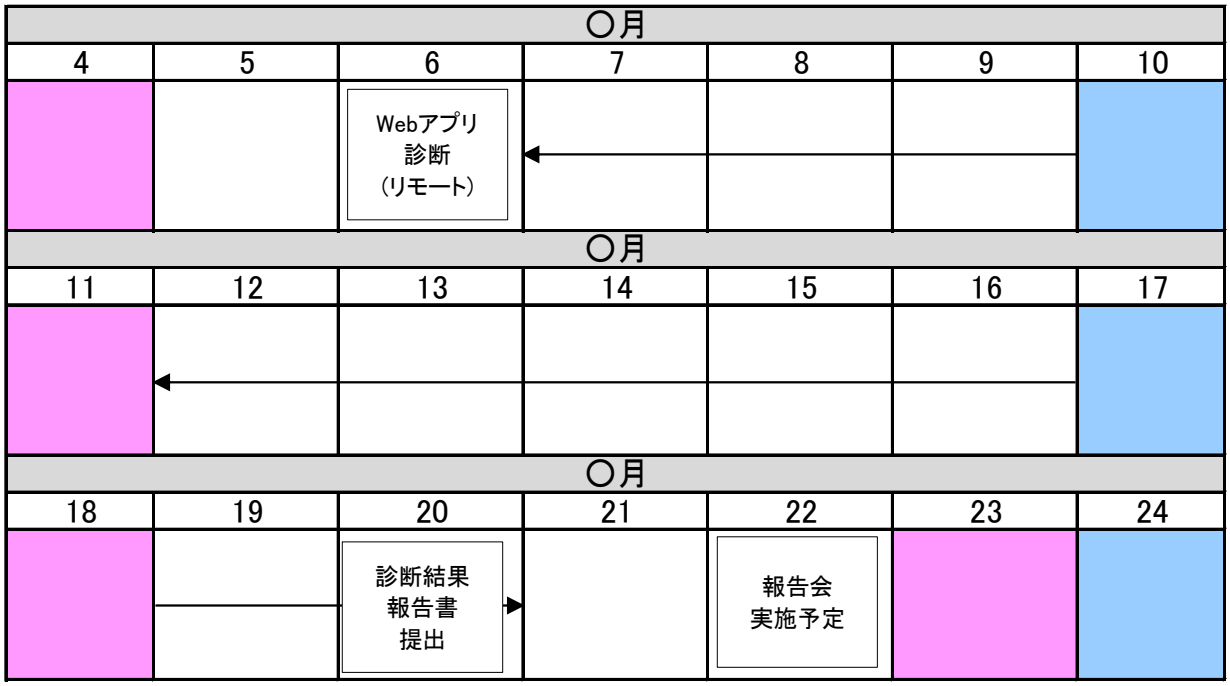
〇〇〇〇年〇月〇日（〇）　10：00～18：00

3－2　診断作業場所

株式会社サイバーセキュリティクラウド
診断指定エリア

3−3　診断スケジュール

全体スケジュール



作業当日スケジュール

作業項目	実施場所	〇/△							
		10	11	12	13	14	15	16	17
Webアプリケーション診断	サイバーセキュリティクラウド	事前準備	脆弱性診断						事後処理

※　診断状況によって診断時間の変更が必要な場合には、お電話等でご担当者と調整させていただく場合があります。

3－4　体制（連絡先）

○○○○○株式会社　様

ご担当者様：
○○○○○部
○○　○○様
電話連絡先　　：XX－XXXX－XXXX
メールアドレス　：XXXXXX@XXX.co.jp

・ 診断時の連絡
・ 緊急時における連絡

株式会社サイバーセキュリティクラウド

技術窓口：

●●　●●
電話連絡先　　：03－6416－9996
メールアドレス　：●●●●@cscloud.co.jp

●●　●●
電話連絡先　　：03－6416－9996
メールアドレス　：●●●●@cscloud.co.jp

営業窓口：

●●　●●
電話連絡先　　：03－6416－9996
メールアドレス　：●●●●@cscloud.co.jp

3－5　診断の流れ

3－5－1　診断開始日の前営業日

診断開始日の前営業日に、「3－4　体制（連絡先）」のご担当者様メールアドレス宛に本診断の事前確認のメールをお送り致します。

お手数をお掛け致しますが、ご確認下さいますよう宜しくお願い致します。

3－5－2　診断日当日（診断開始）

診断日当日、診断開始時間（10:00）の 10 分前（9:50 頃）に、「3－4　体制（連絡先）」のご担当者様メールアドレス宛に本診断の開始連絡のメールをお送り致します。

10:00 までに特にご返信・ご連絡が無ければ、予定通り 10:00 から診断を開始致します。

もし事前にお電話での開始・終了連絡のご希望を伺っていた場合は、「3－4　体制（連絡先）」のご担当者様お電話番号にお電話で開始連絡を入れさせて頂きます。

メールアドレス、お電話番号共に、必ず当日ご連絡が取れることをご確認下さいますよう宜しくお願い致します。

もしご担当者様が診断日当日にご不在の可能性がある場合には、当日ご対応が可能な別の方も追加でご担当者様としてご連絡下さいますよう宜しくお願い致します。

3－5－3　診断日当日（診断中）

診断中は、特に何も無ければご連絡することはございませんが、以下のような理由でご担当者様にご連絡させて頂くことがございますので、その際にはお手数をお掛け致しますがご対応下さいますよう宜しくお願い致します。

- 診断対象画面へのアクセス方法の確認

  アクセスできない画面がある等、診断対象画面へのアクセス方法の確認のために、ご担当者様にご確認のご連絡をさせて頂く場合がございます。

- 診断対象に関するトラブル発生時

  診断対象にアクセスできない、診断中にサーバからの応答が無くなった、等、システム上のトラブルが発生したと推測される場合には、ご担当者様にご連絡させて頂きます。

3－5－4　診断日当日（診断終了）

診断終了時間（18:00）後に、「3－4　体制（連絡先）」のご担当者様メールアドレス宛に本診断の終了連絡のメールをお送り致します。

もし事前にお電話での開始・終了連絡のご希望を伺っていた場合は、「3－4　体制（連絡先）」のご担当者様お電話番号にお電話で終了連絡を入れさせて頂きます。

4　診断内容

4−1　Web アプリケーション標準診断

4−1−1　診断概要

診断対象の Web アプリケーションに対してリモートより脆弱性診断を実施し、潜在している脆弱性を特定します。具体的には「4−2−6　診断時に使用する脆弱性診断ツール」に示す脆弱性診断ツールによる診断と、手動による診断を実施し、診断対象サイトに対するリスク評価を行います。

4−1−2　診断対象

○○○○　(20 画面)

	画面名称	URL ※1	備考
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			

	画面名称	URL ※1	備考
15			
16			
17			
18			
19			
20			

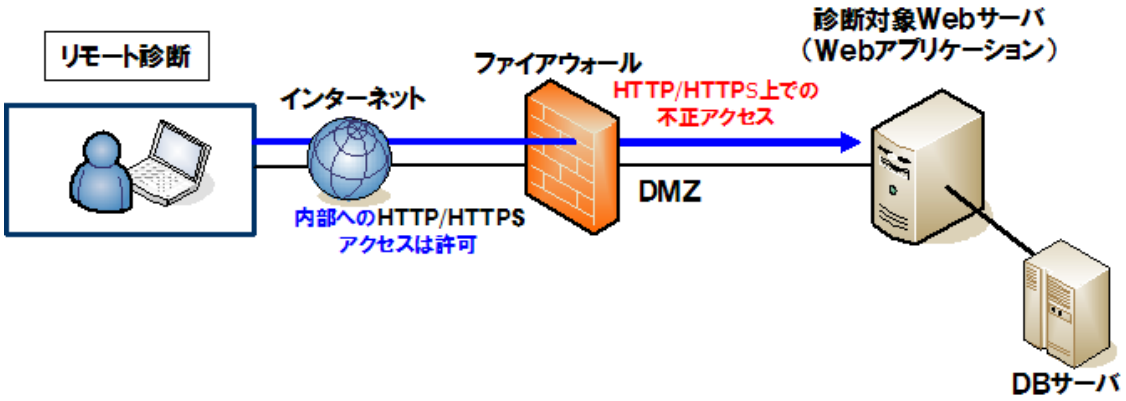
※1　URL については、診断実施時に確認させていただきます。

4－1－3　診断元 IP アドレス

以下の IP アドレスより診断を実施します。IDS 等の監視を行っている場合は、診断当日はこのアドレスからのアクセスについては、監視対象からの除外をお願い致します。

XXX.XXX.XXX.XXX

4－1－4　診断実施イメージ



4－1－5　診断項目

項目名	内容
クロスサイトスクリプティング	入力されたデータの内容を充分チェックせずに出力している HTML 内に JavaScript などの任意のコードが埋め込まれ、実行されてしまう脆弱性が存在するか診断を行います。
ステルスコマンド	外部から任意の OS のコマンドや SSI(サーバサイドインクルード)などの実行可能か診断を行います。
SQL インジェクション	SQL データベースに対し、外部から任意の SQL が実行可能か診断を行います。
バッファオーバーフロー	想定よりも長いデータを処理する際に、本来書き込まれるべきメモリ領域からデータが溢れ、本来書き込まれてはならない別のメモリ領域に書き込まれてしまうか診断を行います。
既知の脆弱性	OS や Web サーバ、アプリケーションサーバ、サードパーティ製ツールなどの持つ一般的に広く知られている脆弱性が存在しないか診断を行います。
強制ブラウジング	意図していないコンテンツが公開ディレクトリにあるために、第三者が URL を直接入力することでそれらのページやデータを取得できてしまう脆弱性が存在しないか診断を行います。
hidden フィールドの操作	hidden フィールドによって重要なデータをやり取りしている場合、アクセス制御をバイパスされたり、予期せぬ動作を引き起こしたりする脆弱性が存在しないか診断を行います。
サードパーティ製品の設定ミス	サードパーティ製品の設定が不適切でないか診断を行います。
バックアップファイルの検出	ファイルを編集した際に作成されるバックアップファイルがサーバ上に存在するか診断を行います。方法によっては、ソースコードが表示されてしまう可能性があります。
バックドア、デバッグオプション	アプリケーションの開発段階で使用されていたデバッグ用のオプションやバックドアがそのまま残されているか診断を行います。
HTML 中のコメント	HTML の中に、管理者のユーザ ID やパスワードの一部などの重要な情報がコメントとして書かれていないか診断を行います。
ディレクトリトラバーサル	Web サーバやアプリケーションサーバが通常表示させることの可能なルートディレクトリを越えて、他のディレクトリパスにアクセスが行えるか診断を行います。

項目名	内容
不適切なエラーハンドリング	Web アプリケーションのエラー処理を行う際の画面表示内容が、システム情報などの攻撃者にとって有効な情報が含まれていないか診断を行います。
パラメータの改ざん	Web アプリケーションが通常使用しているパラメータの値を不正な値に変更したり削ったりすることで、情報の漏洩やアクセス制御のバイパスが行えるか診断を行います。
Web サービスの脆弱性	XML 攻撃など、Web サービスに特化した脆弱性が存在しないか診断を行います。
クロスサイトリクエストフォージェリ	永続的な影響を与えるリクエストが発行されるページにおいて、意図しない商品の購入や記事の投稿等の被害が発生しないか診断を行います。
セッション管理の脆弱性	ログインユーザ毎に適切な識別が行われていない、あるいはアクセス制御が正常でないページが存在するなど、セッション管理に関する脆弱性が存在しないか診断を行います。

4－1－6　診断時に使用する脆弱性診断ツール

ツール名	概要
PortSwigger BurpSuite Professional	PortSwigger BurpSuite Professional は、Web アプリケーションに存在する脆弱性を検出する脆弱性診断ツールです。Web アプリケーションのフォーム変数に様々な値を設定し応答から脆弱性を診断する機能や、診断ツールが保持している Web アプリケーション脆弱性の診断項目データベースを元に診断する機能を備えています。 開発元サイト（〇〇年〇月〇日現在） https://portswigger.net/burp

5　依頼事項

ご連絡先のご確認

「3－5　診断の流れ」の事前確認や開始・終了連絡につきましては、「3－4　体制（連絡先）」のご担当者様へ行いますので、診断日当日にご連絡が取れることを予めご確認下さいますよう宜しくお願い致します。

もしご担当者様が診断日当日にご連絡が取れない可能性がある場合には、事前にご担当者様不在の場合のご連絡先をご連絡下さいますよう宜しくお願い致します。

また、開始・終了連絡につきましては、基本的にメールでのご連絡を行っておりますが、もしご希望がございましたらお電話でのご連絡も可能ですので、ご希望がありましたらその旨ご連絡下さいますよう宜しくお願い致します。

なお、お電話でのご連絡をご要望された場合に、もし当日連絡を取ることができないことがありますと、診断の開始ができない等の問題が発生することがございますので、必ず当日ご連絡を受けられる方のご連絡先をお伝え下さいますよう宜しくお願い致します。

アクセス情報のご確認

ログインパスワード等、診断対象へのアクセスの際に必要な情報につきましては、診断実施までにご用意下さいますよう宜しくお願い致します。

アクセス条件等のご用意

ご用意頂いたアカウントで診断対象の各画面にアクセスができるよう、Web アプリケーション側の設定やアクセス条件（入力値、選択肢等）のご用意・ご連絡をお願い致します。

なお、診断作業時にもアクセス方法の確認のため、ご担当者様へご連絡させて頂くことがございますので、その際にはお手数をお掛け致しますがご対応下さいますよう宜しくお願い致します。

アカウントロックアウト機能に対する対応

Web アプリケーションにより、同じアカウントで複数回ログインに失敗するとアカウントが使用不能になる場合があります。

実際の診断ではパラメータを変更して何度もアクセスを行うことから、ロックアウト機能を持った Web アプリケーションでは実際にロックアウトされる可能性が高くなります。

今回診断対象となる Web アプリケーションにロックアウト機能がある場合には、ロックアウト発生時に解除を依頼させて頂く可能性がございますので、あらかじめご了承下さい。

データベースに対するテストデータの混入の可能性

診断を行う際には、テストデータを登録フォームから登録することにより、データベースに対するテストデータの書き込みが発生します。

診断が終了した後でも、テストデータが残存する可能性がありますので、その場合は、診断後に書き込んだテストデータを削除いただくか、事前にお取りいただいたシステムバックアップからの書き戻しにより原状復帰していただくようご対応をお願い致します。

診断用 PC からアクセス可能な診断対象ページ

脆弱性診断を行う際には診断用ツールを使用する必要がありますので､診断用 PC から診断対象ページへアクセス可能な環境が前提となります。今回は「4-1-3　診断元 IP アドレス」に記載のアドレスからアクセスさせていただきますので、診断期間中はアクセス可能な環境の維持をお願いします。

Web アプリケーション診断によるメール送信・お問い合わせ・登録処理等における対応

Web アプリケーション診断では、Web アプリケーションの構成によって、診断中に大量のメールが管理者様のメールアドレスやテスト用アカウントに関連付けられたメールアドレス等に届く可能性があります。

また、お問い合わせフォームや登録処理が診断対象に入っている場合、診断では数回から数十回の試行を行うため、多数のお問い合わせや登録処理等が発生します。

メール送信に関しましては､診断に必要ないものについてはメール送信機能を停止していただくか､あるいは大量にメールが発生した場合でも問題にならないようご対応をお願い致します。

お問い合わせ・登録等の処理につきましては、特定のアカウントによる依頼については無視するよう、予め関係部署にご周知下さいますよう宜しくお願い致します。

Web サーバのアクセスログへの大量の書き込みにおける対応

診断を行う際には、Web サーバへの大量のアクセスが発生するため、アクセスログへの大量のログが記録されますので、その際にも問題にならないようご対応をお願い致します。

不正アクセス検出用システムに対する対応

脆弱性診断により、ファイアウォール（ネットワーク用/Web アプリケーション用）や侵入検知システム(IDS)等の不正アクセス検出用のシステムで多数の不正アクセスが検出される可能性があります。

設定によっては、診断元アドレスからのアクセス遮断や管理者様のメールアドレスに対する多数の警告メール送信等の影響が考えられます。

今回の診断環境が不正アクセス検出用のシステムの管理下にある場合には、診断元アドレスからのアクセスについては検出を抑制することをお願いします。

診断によるシステム・サービスの負荷増大、停止について

診断ツールが実施するスキャン診断により、診断対象サーバやネットワークに大きな負荷がかかることがあります。同じクラウド業者を利用する他社ユーザに影響が出ることは無いと思われますが、診断対象サーバにおいては稀に診断によってシステムやサービスが不安定となり、場合によってはシステム・サービスの停止へと繋がることもあります。

また、診断対象と同一サーバ上で稼動しているサービスや診断対象とシステム・データベース等を共有しているサービスが存在する場合には、診断対象での障害が他サービスに影響を及ぼすことがあります。

念のため事前に診断対象サーバのシステムやデータ、設定のバックアップを行うことを強く推奨致します。また、診断対象と関連のあるサービスについても合わせてバックアップを行うことを強く推奨いたします。

6　トラブル時の対応

トラブル回避のための対応

診断の際には、事前調査の結果、システムに影響を与える要因を可能な限り排除することで、トラブルの回避に努めます。

緊急連絡経路の確保

トラブル発生時に状況を報告する担当者様への連絡先を予めお知らせ下さい。診断現場から連絡可能な電話番号等をご用意いただくようお願い致します。

トラブル発生時の対応

診断の際には最大限トラブルの回避に努めますが、著しいシステム遅延や停止などが確認された場合は直ちに作業を停止致します。また、万が一プロセス及び OS が停止した場合は、ご担当者の方に再起動処理を行って頂く場合がございますので、予めご了承下さい。

7　診断結果報告書

簡易報告書

検出された脆弱性について、毎日の診断終了後に簡易報告書を提出致します。ご報告する内容は以下の通りです。

- 診断結果要約
- 検出された脆弱性一覧
- 診断時に検証を行った内容とその結果
- 脆弱性の対策方法の提示

診断結果報告書

検出された全ての脆弱性について診断終了後 10 営業日に診断結果報告書を提出致します。ご報告する内容は以下の通りです。

- 総合評価と概要
- 検出された脆弱性一覧
- 診断時に検証を行った内容とその結果
- 脆弱性の対策方法の提示
-

8　無料 Web アプリケーション修正確認診断

診断結果報告書の提出をもって、「Web アプリケーション標準診断サービス」が完了となりますので、その時点でご請求を行わせていただきます。

ご請求後のアフターサポートとして、「Web アプリケーション標準診断サービス」でご報告した脆弱性に対するお客様の修正作業が適切に実施されているかの確認を希望される場合は、修正確認診断を無料にて実施させていただきますので、別途ご連絡下さい。

修正確認診断の条件は以下の通りです。

1) 修正確認診断の実施期間は、ご請求後 1 ヶ月以内です
2) 修正確認診断の実施回数は、1 回です
3) 修正確認診断の実施後、修正確認診断報告書を提出致します
4) 報告会は実施致しません
5) オンサイトでの診断の場合は、オンサイト費用が別途必要となります
6) 修正確認診断の対象は、初回の診断で検出された脆弱性（報告書に記載された脆弱性）限定となります
7) プラットフォーム診断の修正確認診断は実施致しません

以上