

ホームページサーバ等確認チェックリスト(第2版)

ホームページタイトル	
URL(トップページ)	
所管局・部・課	
外部委託先事業者名	
担当者連絡先	

回答結果については取扱注意

※ 回答が「いいえ」になっている場合は、危険な状態です。早急に改善をお願いします。
 ※ 調査結果は所管課で確認し、回答内容はセキュリティ情報のため関係者以外には秘密にしてください。

※選択肢は、プルダウンメニューから選択してください

チェック項目	説明	
A. サーバで使用しているOS・ミドルウェア・ウェブアプリケーションの脆弱性の確認 (WAFやIPS等により脆弱性への攻撃に対する対応を別途行っている場合は、「はい」と回答しても構いません。)		
1	サーバで使用しているOSにセキュリティパッチを速やかに適用しているか(重要) (【いいえの場合】は非常に非常に危険です。)	OSの脆弱性を利用することにより、管理者権限を奪われ、サーバを乗っ取られたり、不正なプログラムが実行されます。セキュリティパッチは必ず実行するようにしてください。
2	サーバで使用しているミドルウェア(OS上で動作し、アプリケーションソフトに対してOSよりも高度で具体的な機能を提供するソフトウェア。OSとアプリケーションソフトの中間的な性格を持っている。)に速やかにセキュリティパッチを適用したり最新版にアップデートしているか(重要) (【いいえの場合】は危険です。)	ミドルウェアにも脆弱性が存在しており、脆弱性を放置しているとそれを利用したウェブサイトの改ざん等が行われる可能性が高まります。速やかにセキュリティパッチを実行したり、最新版へのアップデートを行ってください。 ※ミドルウェアの例 Struts, JBoss, ColdFusion, Tomcat, WebSphere, WebLogic, Joomla!, Apache HTTP Server, IIS
3	サーバで使用しているアプリケーションソフトに速やかにセキュリティパッチを適用したり最新版にアップデートしているか(重要) (【いいえの場合】は非常に危険です。)	アプリケーションソフトにも脆弱性が存在しており、脆弱性を放置しているとそれを利用したウェブサイトの改ざん等が行われる可能性が高まります。速やかにセキュリティパッチを実行したり、最新版へのアップデートを行ってください。
4～14については、別紙「ウェブアプリケーションのセキュリティ実装 チェックリスト(IPA作成)」でチェックを実施した上でご回答ください。 (別紙のチェックリストで未対策の項目にチェックが入っている場合に、いいえと回答してください) ウェブアプリケーションを使用していない場合は、該当なしと回答してください。		
4	SQLインジェクションに対する対策はできているか	「SQLインジェクション」とは、データベースと連携したウェブアプリケーションにおいて、SQL文(データベースへの命令文)の組み立て方法に問題があり、それを利用して不正にデータベースを利用しようとする攻撃のことを指します。 情報漏えいやデータベースの改ざんの他、不正ログイン等が行われる可能性があります。
5	OSコマンドインジェクションに対する対策はできているか	「OSコマンドインジェクション」とは、外部からウェブサイトへOSを操作するコマンドを含んだ要求を送ることにより、OSを不正に操作しようとする攻撃のことを指します。 情報漏えいやデータベースの改ざんの他、不正ログインやそのサーバを踏み台とした他のサーバへの攻撃等が行われる可能性があります。
6	ディレクトリトラバーサルに対する対策はできているか	「ディレクトリトラバーサル」とは、パラメータにファイル名を指定しているウェブアプリケーションで、ファイル名指定の実装に問題がある場合、それを利用して外部から任意のファイルを指定し、アプリケーションが意図しない操作をさせる攻撃のことを指します。 情報漏えいやデータベースの改ざん等が行われる可能性があります。
7	セッション管理の不備に対する対策はできているか	「セッション管理の不備」とは、セッションID(利用者を識別するための情報)を発行し、セッション管理を行っているウェブアプリケーションで、セッション管理に問題がある場合、それを利用してログイン中の利用者になりすます攻撃のことを指します。 情報漏えいやデータの改ざん等が行われる可能性があります。
8	クロスサイト・スクリプティングに対する対策はできているか	「クロスサイト・スクリプティング」とは、利用者の入力情報等を基にウェブページを作成するウェブアプリケーションで、ウェブページへの出力処理に問題がある場合、それを利用してウェブページへ不正なスクリプト(小さなプログラム)を埋め込む攻撃のことを指します。 ウェブサイト上への偽のページの作成やCookieの窃取等が行われる可能性があります。
9	クロスサイト・リクエスト・フォージェリに対する対策はできているか	「クロスサイト・リクエスト・フォージェリ」とは、ログイン機能の存在するウェブサイトで、ログインした利用者からのリクエストについて、その利用者が意図したリクエストであるかどうかを識別する仕組みを持たない場合、それを利用して利用者が予期しない処理を実行させる攻撃のことを指します。 情報漏えいやデータの改ざん等が行われる可能性があります。
10	HTTPヘッダ・インジェクションに対する対策はできているか	「HTTPヘッダ・インジェクション」とは、HTTPレスポンスヘッダの出力処理に問題があるウェブアプリケーションで、攻撃者が、レスポンス内容に任意のヘッダフィールドを追加したり、任意のボディを作成したり、複数のレスポンスを作り出すような攻撃のことを指します。 ウェブサイト上への偽のページの作成やCookieの窃取等が行われる可能性があります。
11	メールヘッダ・インジェクションに対する対策はできているか	「メールヘッダ・インジェクション」とは、利用者が入力した内容を、特定のメールアドレスに送信する機能を持つウェブアプリケーションに問題がある場合、攻撃者が、任意のメールアドレスを指定してメールを送信させる攻撃のことを指します。 迷惑メール等の送信が行われる可能性があります。
12	クリックジャッキングに対する対策はできているか	「クリックジャッキング」とは、ログインしている利用者のみが使用可能な機能がマウス操作のみで使用可能な場合、細工された外部サイトを閲覧し操作することにより、利用者が誤操作し、意図しない機能を実行させる攻撃のことを指します。 ログイン後の利用者のみが利用可能なサービスの悪用や設定の変更が行われる可能性があります。
13	バッファオーバーフローに対する対策はできているか	「バッファオーバーフロー」とは、プログラムが入力されたデータを適切に扱わない場合、プログラムが確保したメモリの領域を超えて領域外のメモリが上書きされ、意図しないコードを実行してしまう攻撃のことを指します。 プログラムの異常終了や任意のプログラムが実行されウイルス感染等が行われる可能性があります。
14	アクセス制御や認可制御の欠落に対する対策はできているか	「アクセス制御や認可制御の欠落」とは、パスワード等の秘密情報の入力が必要な認証機能やログイン中の利用者が他人になりすましてアクセスできないようにする機能が必要であるにも関わらず実装されていないことを指します。 情報漏えいやデータの改ざん等が行われる可能性があります。

チェック項目	説明
B. 更新のためのアカウント・パスワード等の確認	
15 更新方法にFTP (File Transfer Protocol) を使用していないか (重要) (FTPを使用している場合= [いいえの場合] は非常に危険です。)	FTP(ファイル転送プロトコル)は、ホームページデータをサーバにアップロードする際に、よく使用される仕組みですが、Gumblarなどウイルスに対して脆弱性があります。従来はこの仕組みが主流でしたが、項目16のとおり、できるだけ早く移行するかwebサービスの見直しをしてください。
16 更新方法にFTPを使用している場合、SFTP(Secure Copy Protocol)、SCP(SSSH File Transfer Protocol) その他暗号化による方法への移行ができるか	FTPは、データを暗号化せずに通信するため、IDやパスワードを盗まれる恐れがあります。SFTPやSCPの仕組みはデータを暗号化して通信するため、これらのリスクを低減できます。暗号化が困難な場合は、回線を通じて画面更新をせず、媒体を使う運用方法も考えられます。
17 FTPやSFTP、SSH等を使用している場合、ID、パスワードを定期的(6ヶ月に1回以上)に変更しているか	ID・パスワードを盗まれるリスクを考慮して、定期的(6ヶ月に1回以上)に変更することが推奨されます。
18 FTPやSFTP、SSH等を使用している場合、パスワードは、8桁以上の複雑なもの(少なくとも英数小文字大文字混合)にしているか	辞書攻撃による不正アクセスを防ぐためにも、複雑なパスワードにすることが推奨されます。
19 FTPやSFTP、SSH等を使用している場合、必要最低限のIDしか利用できないようにしているか	不要なIDが残っていると、それを利用して不正アクセスが行われることが考えられます。定期的に必要なIDをチェックし、削除することを推奨します。
C. その他項目の確認	
20 ウイルス対策ソフトの定義ファイルは最新状態か	ウイルス対策ソフトの定義ファイルの適用日付を確認してください。
21 サーバに接続(更新作業)できる発信元IPアドレスの制限はかけているか(重要) (制限していない場合= [いいえの場合] は非常に危険です。)	発信元IPアドレスを制限しないと、FTPのIP・パスワードが漏えいすることで、世界中からホームページを改ざんされる恐れがあります。必ず発信元IPアドレス制限は実施してください。但し、レンタルサーバ等を利用している場合でこの方法が技術的に困難な場合は、他の方法(特に項番14)でセキュリティを確保するようにして下さい。
22 サーバにおいて、必要のないサービスを稼働させていないか、また、必要なサービスであっても、それに対するアクセス権限を必要最低限に設定しているか	ウェブサイト運営に必要なサービスがウェブサーバ上で稼働している場合、そのサービスに対する管理が十分でなく、脆弱性が存在するバージョンをそのまま利用している可能性があるため、不要なサービスは稼働させず、必要な最低限のサービスのみ稼働させるようにして下さい。
23 ホームページの改ざんチェックができる仕組みを導入しているかもしくはサーバに不審なアクセスが行われていないか、また、不正なフォルダやファイル等が作成されていないか定期的に確認(1日1回以上)しているか	ホームページの改ざんチェックサービスを利用するなど、改ざんを検知できる仕組みが整っていることが望ましいですが、少なくとも、改ざんされていないか定期的に確認を行うことは必要です。
24 公開しているウェブサイトのデータを定期的にバックアップしているか	ウェブサイトのデータのバックアップがないと、サイトを復旧させる際に、再度データの作成から始めていかないといけなくなります。定期的に、ウェブサイトのデータのバックアップを取得しておきましょう。
25 ウェブサイト等の復旧手順が策定され、定期的に手順の確認を行っているか	事件・事故が発生した場合に備えて、復旧手順を策定し、手順を確認しておくことが必要です。