ウェブ健康診断仕様

「安全なウェブサイトの作り方」別冊

注意事項

本診断は検査パターンを絞り込んだものです。安全宣言には繋がりません。

IPA 独立行政法人情報処理推進機構
セキュリティセンター

2012年12月

本書は、以下の URL からダウンロードできます。

「安全なウェブサイトの作り方」別冊
「ウェブ健康診断仕様」
http://www.ipa.go.jp/security/vuln/websecurity.html

目次

注意事項

- **「ウェブ健康診断仕様」は検査パターンを絞り込んだ診断です。**
- **「ウェブ健康診断仕様」で脆弱性が検出されなかった場合でも、検査パターンを絞り込んでいることから、安全宣言には繋がりません。**

1.はじめに

1.1. 本資料公開の経緯

本資料「ウェブ健康診断仕様」は、財団法人地方自治情報センター（LASDEC）が実施したウェブ健康診断事業における診断仕様の一部をまとめたものを、IPA（独立行政法人情報処理推進機構）が「安全なウェブサイトの作り方」の別冊として公開するものです。

■ 地方公共団体向けにまとめられた「ウェブ健康診断仕様」（平成 20 年度版、平成 22 年度版）

LASDEC では 2008 年から 2010 年まで、地方公共団体が運営するウェブサイトの改ざん防止等を目的とし、ウェブアプリケーションの脆弱性の有無を診断する「ウェブ健康診断事業」を実施しました。

同事業は、地方公共団体がウェブアプリケーションの脆弱性を身近な問題として認識することを目指したもので、地方公共団体が運営するウェブサイトに対して、基本的な脆弱性対策ができているかどうかを知るきっかけとしての診断を行いました。

その事業の中でまとめられた具体的な診断仕様が「ウェブ健康診断仕様」です。この仕様は有識者等による「ウェブ健康診断検討委員会」で検討され、仕様の一部は LASDEC から「ウェブ健康診断仕様」として 2009 年（平成 20 年度版）および 2011 年（平成 22 年度版）に公開されました[1]。

診断内容は、基本的な対策ができているかどうかを診断するものですので、一般にウェブアプリケーションの脆弱性診断サービスとして提供されているものよりも簡素です。しかしながらウェブ健康診断仕様の公開後、そのコンセプトによる診断は地方公共団体のみならず民間企業等多くの団体から反響があり、活用され始めました。

上記背景から、LASDEC はより広範囲に適切な活用がなされることを期待し、2012 年、同仕様の維持・発展に係る業務を IPA に移管しました。

■ より広い範囲での活用を目指し、IPA が公開する「ウェブ健康診断仕様」（本資料）

IPA は、地方公共団体だけではなく民間企業の中でも、ウェブアプリケーションの脆弱性を身近な問題として捉えていないところが少なくなく、特に中小企業では顕著だと考えています。IPA は今回、「ウェブ健康診断仕様」を公開することで、ウェブサイトを運営する多くの企業が診断を実施し、脆弱性を自社のウェブサイトに関わる問題として捉えるようになることを願っています。

さらに、具体的な対策に繋がるよう、「ウェブ健康診断仕様」を「安全なウェブサイトの作り方」の別冊としました。もし診断の結果、脆弱性が検出された場合、「安全なウェブサイトの作り方」に参考に対策を検討することができます。

なお、この「ウェブ健康診断仕様」の診断は、検査パターンを絞り込んだ診断ですので、脆弱性が検出されなかった場合でも、**安全宣言には繋がりません**。診断の結果を確認した後は、より詳細な診断を受けたり、「安全なウェブサイトの作り方」を参考に対策を実装することなどを、検討してください。

[1] ウェブ健康診断 - 財団法人 地方自治情報センター（LASDEC）
https://www.lasdec.or.jp/cms/12,1284.html

1.2. ウェブ健康診断とは

「ウェブ健康診断」とは、ウェブサイトを人間に例えるなら、その名のとおり「健康診断」にあたるような位置づけの診断です。人間ドックに比べると精密ではありませんが、LASDEC が平成 19 年度に実施した Web アプリケーション脆弱性診断結果等も考慮しながら重要な診断項目を検討し、改良を重ねたものです。

ウェブ健康診断は「基本的な対策が出来ているかどうかを診断するもの」とご理解ください。また、診断対象のウェブアプリケーションの全てのページを診断するものではなく、診断対象の規模にもよりますが、基本は抜き取り調査（診断）です。

1.3. 注意事項

本資料「ウェブ健康診断仕様」活用の際には、以下の点にご注意ください。

1. 「ウェブ健康診断仕様」**検査パターンを絞り込んだ診断**であり、**安全宣言には繋がりません**。
2. できるだけ低いコストで診断が実施できるように、**必要かつ最小限の診断項目、検査パターン**を採用した診断です。
3. 健康診断の結果、**脆弱性が検出された場合**は、**詳細な診断を行う、又は改修**を検討してください。
4. 健康診断の結果、脆弱性が検出されなかった場合でも、検査パターンを絞り込んだ診断であることから、**脆弱性が存在する可能性は残ります**。
5. 健康診断の結果、脆弱性が検出された場合でも、**実際には脆弱性ではない可能性**があります。
6. 健康診断を行うことにより、診断対象の**ウェブサイトが停止したり、ウェブサイトに意図しないデータが登録**される可能性があります。
7. ウェブサイトが停止する際は、診断対象のウェブサイトだけにとどまらず、インフラを共有している**別のウェブサイトにも影響が及ぶ可能性**があります。診断を行う際は必ず、サーバやデータセンター等、インフラ管理者の**許可を事前に得てください**。

2.ウェブ健康診断 診断内容

2.1. 診断対象脆弱性(診断項目)及びその選定理由

診断対象脆弱性(診断項目)は以下のとおりです。なお、本書では、診断項目を示す場合、記号(A)～(M)を付与しています。

項番	記号	診断項目(脆弱性名)	危険度	能動的攻撃/受動的攻撃	想定被害		
					情報漏洩	改ざん	妨害
1	(A)	SQL インジェクション	高	能動的	○	○	○
2	(B)	クロスサイト・スクリプティング	中	受動的	○	△	
3	(C)	CSRF(クロスサイト・リクエスト・フォージェリ)	中	受動的	△	○	○
4	(D)	OS コマンド・インジェクション	高	能動的	○	○	○
5	(E)	ディレクトリ・リスティング	低～高	能動的	○		
6	(F)	メールヘッダ・インジェクション	中	能動的			○
7	(G)	パス名パラメータの未チェック／ディレクトリ・トラバーサル	高	能動的	○	△	
8	(H)	意図しないリダイレクト	中	受動的	○		
9	(I)	HTTP ヘッダ・インジェクション	中	受動的	○	△	
10	(J)	認証	低～中	能動的	○	○	
11	(K)	セッション管理の不備	低～高	能動的／受動的	○	○	
12	(L)	認可制御の不備、欠落	高	能動的	○	○	
13	(M)	クローラへの耐性	低～中	能動的			○

上記診断項目の選定にあたっては、下記のものを選定の対象としました。

- 危険性の高い脆弱性(直接的な被害につながる可能性が高いもの)
- 平成 19 年度 Web アプリケーション脆弱性診断事業(LASDEC 実施)で検出数の多かったもの
- IPA「安全なウェブサイトの作り方 」に取り上げられているもの(届出の多いもの)
- 問題となるケースが多いもの(SQL インジェクション、クロスサイト・スクリプティング、CSRF)
- 社会問題にまで発展した事案の原因となったもの(クローラへの耐性)

2.2. 危険度基準

各脆弱性に付与している危険度のレベルは、以下の基準に則って提示しました。

危険度「高」	被害者ユーザの関与がなくても攻撃者が直接アプリケーションに対して攻撃可能である能動的な脆弱性。攻撃を受けると、大量の情報漏洩や改ざんの被害を生じる可能性がある。
危険度「中」	攻撃成功には被害者ユーザの関与（攻撃者の罠のリンクをクリックする等）が必要である受動的な脆弱性。若しくは能動的な脆弱性であっても大量の情報漏洩や改ざんにはつながりにくいもの。
危険度「低」	攻撃成功の確率が低い若しくは攻撃が成功しても被害が軽微であると考えられる脆弱性。ただし、確率は低いものの被害に遭う可能性はある。

2.3. 総合判定基準

脆弱性が発見された場合、「総合判定所見」が

- 「要治療・精密検査」
- 「差し支えない」
- 「異常は検出されなかった」

のいずれかとなります。いずれの「総合判定所見」になるかは、以下の基準に基づきます。

総合判定所見	**要治療・精密検査**
説明	危険度が「高」又は「中」の、明らかに危険な脆弱性が検出された。ウェブアプリケーションの改修等の措置を講じる必要がある。また、指摘箇所以外にも危険な脆弱性が発見される可能性が高い。
基準	脆弱性（A)～(M）の 13 項目のうち、1 つでも脆弱性が発見された場合。ただし、「差し支えない」の判定基準にある脆弱性以外のもの（危険性が高い脆弱性）

総合判定所見	**差し支えない**
説明	今回の診断では危険度が「低」の脆弱性のみが検出された。現状すぐに実被害に及ぶ可能性は低く、運用上は差し支えないと判断されるが、本件は注意が必要であり放置しない方がよい。
基準	下記 4 つの脆弱性（E)、(J)、(K)、(M）のみが検出された場合。 (E) ディレクトリ・リスティング（P.13 参照） ただし、重要な情報（個人情報の記載されたファイル等）が検出された場合は、既に危険な状態ということから、「要治療・精密検査」とします。 (J) 認証（P.16 参照） ただし、検出パターン 1 かつ 2 が検出された場合若しくは検出パターン 5 が検出された場合は、危険度が高いため「要治療・精密検査」とします。 (K) セッション管理の不備（P.18 参照）

	ただし、検出パターン 2 が検出された場合若しくは検出パターン 4 かつ 5 が検出された場合は、危険度が高いため「要治療・精密検査」とします。 (M) クローラへの耐性(P.21 参照) ただし、P.22 ⑥脆弱性の判定基準 にある条件 1)、2)、3)、4) だった場合は、危険度が高いため「要治療・精密検査」とします。

総合判定所見	**異常は検出されなかった**
説明	今回の診断では脆弱性は発見されなかった。**ただし、診断していない項目もあり、診断方法も限定しているので、「安全である」ことと同義ではない**。
基準	診断結果が「すべて正常」あるいは「該当なし」の場合。

2.4. 診断時に利用する診断項目毎の検出パターン（目安）、脆弱性有無の判定基準、及び対象画面について

各診断項目における検出パターン及び脆弱性有無の判定基準は以下のとおりです。なお、厳密な意味で言えば、ここでの基準で判定される挙動は、「当該脆弱性がある可能性が高い」ということになります（必ず当該脆弱性があることを 100%保証はしていません）。

また、表右端にある、「対象画面（機能）」 の詳細は P.24「2.6 診断対象画面（機能）とその定義について」を参照してください。

（A） SQL インジェクション				
検出パターン		脆弱性有無の判定基準	備考（脆弱性有無の判定基準詳細、その他）	対象画面（機能）
1	「'」（シングルクォート 1 つ）	エラーになる	レスポンスに DBMS 等が出力するエラーメッセージ（例：SQLException、Query failed 等）が表示された場合にエラーが発生したと判定します（※注 1）。	・ DB アクセス
2	「*検索キー*」と、 「*検索キー*'and'a'='a」 の比較	*検索キー*のみと同じ結果になる	HTTP ステータスコードが一致し、かつレスポンスの diff（差分）が全体の 6% 未満の場合、同一の結果と判定します。検査対象が検索機能の場合は、検索結果件数が同一の場合にも、同一の結果と判定します。	
3	「*検索キー(数値)*」と、 「*検索キー* and 1=1」 の比較	*検索キー*のみと同じ結果になる	同上（この検出パターンは検索キーが数値の場合のみ検査します。数値の場合は全ての検出パターンを検査し、数値以外の場合は検出パターン 1、2 のみ検査します）	

※ 注 1 DBMS のエラーメッセージと判断する基準は以下の通りとします。

- DBMS の製品名（Oracle、Microsoft SQL Server、IBM DB2、MySQL、PostgreSQL 等）の全て又は一部が表示される。
- SQL の一部が表示されている。
- シングルクォートが対応していない等、SQL の構文上の問題指摘が含まれている。
- 他のエラーメッセージとは明らかに異質なメッセージ、例えば、通常のエラーメッセージが日本語であるのに対し、英語のメッセージになっている等。

(A) SQL インジェクションの脆弱性ありと判定された時は

☞「安全なウェブサイトの作り方」中の「1.1 SQL インジェクション」を参考に、解決策を検討してください。

(B) クロスサイト・スクリプティング				
検出パターン		脆弱性有無の判定基準	備考（脆弱性有無の判定基準詳細、その他）	対象画面（機能）
1	「'>"><hr>」(※注 2)	エスケープ等されずに出力される	レスポンスボディーに検査文字列の文字列がエスケープ等されずに出力されると脆弱性ありと判定します。	・入力内容確認 ・エラー
2	「'>"><script>alert(document.cookie)</script>」(※注 2)	エスケープ等されずに出力される	同上	
3	「<script>alert(document.cookie)</script>」(※注 3)	エスケープ等されずに出力される	同上。http://www.example.jp/service/index.html という URL であった場合、「index.html」の部分に検査文字列をエンコードせずに挿入します。	
4	「javascript:alert(document.cookie);」 (※注 2)	href 属性等に出力される	レスポンスボディーの特定の URI 属性（src, action, background, href, content）や、JavaScript コード（location.href, location.replace）等に検査文字列が出力される場合、脆弱性ありと判定します。	

※ 注 2　検出パターン 1、2、4 は、GET 及び POST パラメータについて実施します。

※ 注 3　検出パターン 3 は、URL 中のファイル名部分について実施します。

(B) クロスサイト・スクリプティングの脆弱性ありと判定された時は

☞「安全なウェブサイトの作り方」中の「1.5 クロスサイト・スクリプティング」を参考に、解決策を検討してください。
（検出パターン 4 が検出された場合、特に 5-(ii) を参照してください）

（C） CSRF（クロスサイト・リクエスト・フォージェリ）				
検出パターン		脆弱性有無の判定基準	備考（脆弱性有無の判定基準詳細、その他）	対象画面（機能）
1	ログイン状態において、特定副作用を持つ画面に対して外部からパラメータを強制する（この際に、Referer が送出されないように抑止すること）	特定副作用（たとえば送金、商品購入、退会処理、パスワードや設定の変更など、ウェブサイトの利用者にとって重要で、取り消しできない処理）が実行される	特定副作用を持つ機能において、以下のいずれかを満たす場合に脆弱性ありと判定します。 ・トークン等のパラメータが存在しない ・トークン等を削除しても特定副作用が実行される ・トークン文字列の推測が可能 ・別ユーザのトークンが使用できる 特定副作用が実行されたかどうかは、画面に表示されるメッセージ等により判断します。	・パスワード変更 ・DB 更新 ・メール送信 （※注 4）

※ 注 4　メール送信機能における（C）CSRF（クロスサイト・リクエスト・フォージェリ）の検査については、ログイン後の状態でメール送信機能が利用可能な場合に限ります。

(C) CSRF（クロスサイト・リクエスト・フォージェリ）の脆弱性ありと判定された時は
☞「安全なウェブサイトの作り方」中の「1.6 CSRF（クロスサイト・リクエスト・フォージェリ）」を参考に、解決策を検討してください。

（D） OS コマンド・インジェクション				
検出パターン		脆弱性有無の判定基準	備考（脆弱性有無の判定基準詳細、その他）	対象画面（機能）
1	（UNIX 系 OS 向け） 「../../../../../../../bin/sleep 20|」を入力	20 秒レスポンスが遅くなる	―	・ファイル名 ・メール送信
2	（UNIX 系 OS 向け） 「;/bin/sleep 20」を入力	20 秒レスポンスが遅くなる	―	
3	（Windows 系 OS 向け） 「../../../../../../../windows/system32/ping -n 21 127.0.0.1|」を入力	20 秒レスポンスが遅くなる	―	
4	（Windows 系 OS 向け） 「&/windows/system32/ping -n 21 127.0.0.1」を入力	20 秒レスポンスが遅くなる	―	

(D) OS コマンド・インジェクションの脆弱性ありと判定された時は

☞「安全なウェブサイトの作り方」中の「1.2 OS コマンド・インジェクション」を参考に、解決策を検討してください。

(E) ディレクトリ・リスティング				
検出パターン		脆弱性有無の判定基準	備考（脆弱性有無の判定基準詳細、その他）	対象画面（機能）
1	URL をディレクトリまでで終端し HTTP リクエストを送信する	ディレクトリー覧が表示される。ファイルー覧の表示のみでは「低」危険度、重要情報があれば「高」危険度	URL の末尾のファイル名部分を削除して HTTP リクエストを送り、ファイルー覧がレスポンスされるか確認します。icons 等、明らかに無害なものは報告しません。抜き取り調査にて、一覧ファイル内のバックアップファイル等を探し、発見されたものを報告対象とします。	・任意の箇所（※注 5）

※ 注 5 (E) ディレクトリ・リスティングに関しては特に調査対象の基準を設けていないため、必要に応じて任意の箇所で診断を行います。

(F) メールヘッダ・インジェクション				
検出パターン		脆弱性有無の判定基準	備考（脆弱性有無の判定基準詳細、その他）	対象画面（機能）
1	Subject、From、To 欄に「%0d%0aTo:XXX@example.jp」（XXX は数値 2～3 桁）を入力することで、新たなあて先を指定できるか	新たなあて先を指定できる	改行文字の後に追加した To アドレス（XXX@example.jp のアドレス）にメールが届く場合に、新たなあて先を指定できたと判定します。	・メール送信
2	Subject、From、To 欄に「%0d%0a%0d%0akensa」を入力することで、本文内容を改ざんできるか	本文内容を改ざんできる	XXX@example.jp のアドレスに届いたメールの本文部分に「kensa」という文字列が含まれている場合、本文内容を改ざんできたと判定します。	

(F) メールヘッダ・インジェクションの脆弱性ありと判定された時は

☞「安全なウェブサイトの作り方」中の「1.8 メールヘッダ・インジェクション」を参考に、解決策を検討してください。

（G） パス名パラメータの未チェック／ディレクトリ・トラバーサル				
検出パターン		脆弱性有無の判定基準	備考（脆弱性有無の判定基準詳細、その他）	対象画面（機能）
1	（UNIX 系 OS 向け） 「../../../../../../../../../etc/hosts」	/etc/hosts が表示される	レスポンスに 127.0.0.1、localhost 等の文字列が含まれる場合、/etc/hosts が表示されたと判定します。	・ファイル名（※注 6）
2	（UNIX 系 OS 向け） 「../../../../../../../../../etc/hosts%00」	/etc/hosts が表示される	同上	
3	（Windows 系 OS 向け） 「../../../../../../../../../windows/win.ini」	win.ini が表示される	レスポンスに[extensions]等の文字列が含まれる場合、win.ini が表示されたと判定します。	
4	（Windows 系 OS 向け） 「../../../../../../../../../windows/win.ini%00」	win.ini が表示される	同上	

※ 注 6 （G）パス名パラメータの未チェック／ディレクトリ・トラバーサル に関しては、ファイルアクセスが想定される画面、ファイル名を想起させるパラメータがあった場合に診断します。

(G) パス名パラメータの未チェック／ディレクトリ・トラバーサルの脆弱性ありと判定された時は

☞「安全なウェブサイトの作り方」中の「1.3 パス名パラメータの未チェック／ディレクトリ・トラバーサル」を参考に、解決策を検討してください。

(H) 意図しないリダイレクト				
検出パターン		脆弱性有無の判定基準	備考（脆弱性有無の判定基準詳細、その他）	対象画面（機能）
1	クエリストリング等に URL を保持している場合に、URL を別ドメインのもの（http://www.example.jp/）に変更して HTTP リクエストを送信する	指定した別ドメインの URL に遷移させられる	Location ヘッダ、META タグの Refresh、JavaScript コード（location.href, location.assign, location.replace）によるリダイレクト部分に検査文字列が出力される場合にリダイレクト可能と判定します。ログイン機能以外でも脆弱性として判定します。（※注 7）	・リダイレクト

※ 注 7　リダイレクタがバナー広告の遷移専用の場合は、「差し支えない」判定とします（他に中危険度以上の指摘がない場合）。

(I) HTTP ヘッダ・インジェクション				
検出パターン		脆弱性有無の判定基準	備考（脆弱性有無の判定基準詳細、その他）	対象画面（機能）
1	Cookie に相当するパラメータに改行コードを入力 元の値%0d%0aSet-Cookie:xxxtest%3Dxxxxtest%3B	Set-Cookie ヘッダのパラメータに改行が挿入される	レスポンスヘッダに、xxxtest=xxxxtest という Set-Cookie ヘッダが存在する場合、改行が挿入されたと判定します。	・Cookie ・リダイレクト
2	リダイレクト先 URL に相当するパラメータに改行コードを入力 元の値%0d%0aSet-Cookie:xxxtest%3Dxxxxtest%3B	Location ヘッダのパラメータに改行が挿入される	同上	

(I) HTTP ヘッダ・インジェクションの脆弱性ありと判定された時は

☞「安全なウェブサイトの作り方」中の「1.7 HTTP ヘッダ・インジェクション」を参考に、解決策を検討してください。

(J) 認証				
検出パターン		脆弱性有無の判定基準	備考（脆弱性有無の判定基準詳細、その他）	対象画面（機能）
1	パスワード(※注 8)の最大文字数が 8 文字以上確保されているか	8 文字未満の場合	―	・ログイン ・ログアウト

2	パスワードの文字種が数字のみ、英字のみに限定されていないか	数字のみ、英字のみの場合	ー	
3	パスワードが入力時に伏字になっているか	伏字になっていない場合	ー	
4	パスワード間違いの際のメッセージは適切か	ユーザ ID とパスワードのどちらが間違いか分かるようなメッセージの場合	ー	
5	ログアウト機能はあるか、適切に実装されているか	ログアウト機能がない、あるいはログアウト後「戻る」ボタンでセッションを再開できる場合	ー	
6	意図的に 10 回パスワードを間違える	アカウントロックされない場合	ー	

※ 注 8　ユーザ ID 入力欄が存在せず、パスワード入力欄のみ存在する場合は、暗黙の固定ユーザ ID が想定されているとみなし、上記検出パターンを適用します。

(J) 認証の脆弱性ありと判定された時は

☞「安全なウェブサイトの作り方」中の「1.9 アクセス制御や認可制御の欠落」を参考に、解決策を検討してください。
（特に 9-(i) を参照してください）

（K） セッション管理の不備				
検出パターン		脆弱性有無の判定基準	備考（脆弱性有無の判定基準詳細、その他）	対象画面（機能）
1	ログインの前後でセッション ID が変化するか	セッション ID が変わらない場合	―	・ログイン ・ログアウト
2	言語・ミドルウェアの備えるセッション管理機構を使用せず手作りのセッション管理機構を使っていないか	手作りのセッション管理機構を使用している場合	セッション ID のパラメータ名等で、言語・ミドルウェアのセッション管理機構を使用しているかを判断します(※注 9)。 判断がつかない場合には、"手作りの疑いあり"として報告します。	
3	SSL を使用するサイトの場合、セッション ID を保持する Cookie にセキュア属性が付与されているか	Cookie のセキュア属性が付与されていない場合	―	
4	Cookie をオフにしてアクセスした場合、セッション ID が URL 埋め込みにならないか	セッション ID が URL 埋め込みの場合	リファラから漏洩するおそれがある場合にのみ、脆弱と判定します。（検出パターン 5 を参照）	
5	携帯電話向けサイト等でセッション ID を URL 埋め込みにしている場合、外部リンクから Referer 経由でセッション ID が漏洩しないか	Referer からセッション ID が漏洩する場合	PC/携帯サイト両方が対象。外部へのリンク（検査対象とは異なるホスト上のページへのリンク）が存在する場合にのみ脆弱と判定します。セッション ID の漏洩が問題とならない場合（認証等の機能が無いケースや、ワンタイムなセッション ID を使用しているケース）は報告から除外します。	

※ 注 9　言語・ミドルウェアのセッション管理機構とは、以下のセッション ID の場合とします。

- PHPSESSID
- JSESSIONID

・ ASPSESSIONIDxxxx（xxxx はランダムな英数字）

その他、検査実施者の既知のセッション ID を判断材料として加えてもよいこととします。

(K) セッション管理の不備の脆弱性ありと判定された時は

☞「安全なウェブサイトの作り方」中の「1.4 セッション管理の不備」を参考に、解決策を検討してください。

(L)　認可制御の不備、欠落				
検出パターン		脆弱性有無の判定基準	備考（脆弱性有無の判定基準詳細、その他）	対象画面（機能）
1	URL 操作により、現在のユーザでは実行権限のない機能が実行可能	実行可能の場合	貸与アカウントでは実行権限が無いと推測されるページ（管理者機能等）の URL が特定できる場合に、検査を実施します。権限が無いと推測されるページ（管理者向けメニュー等）が表示された時点で、脆弱性ありとして判定します。	・認可制御有
2	文書 ID、注文番号、顧客番号等がパラメータにより指定されている場合、その ID 類を変更して、元々権限のない情報を閲覧できるか	ID 類の変更により、閲覧権限のない情報が表示された場合	閲覧権限がない情報の ID 類が特定できる場合に検査を実施します。特定できない場合は、ID 類の末尾数値を操作する等の方法で、参照権限がないと推測される情報が表示されたら脆弱性ありと判定します。	
3	hidden, Cookie に現在権限が指定されており、その変更により現在のユーザでは実行権限のない機能が実行可能	実行可能の場合	「admin」等権限クラスを示すと推測されるパラメータが存在する場合に、検査を実施します。	

(L) アクセス制御の不備、欠落の脆弱性ありと判定された時は

☞「安全なウェブサイトの作り方」中の「1.9 アクセス制御や認可制御の欠落」を参考に、解決策を検討してください。
（特に 9-(ii) を参照してください）

(M)　クローラへの耐性

インターネットに公開されているホームページは通常の利用者（人間）によるアクセスだけではなく、「クローラ」と呼ばれる自動プログラムによるアクセスを受けています。この「クローラ」とは、主には検索エンジンの検索データベースを作成するために、ウェブページのデータを回収するプログラムのことです。

このクローラは、データの回収にあたって、ホームページへ連続的にアクセスをするのですが、そのようなクローラによるアクセスに耐えられないという欠陥を抱えるウェブシステムが一部にあることがわかりました。

クローラは既にインターネットにおいては検索エンジンをはじめたくさん利用されており、たとえば国立国会図書館でも、政府・地方公共団体等の公的機関を対象に、自動収集プログラム（クローラ）によるインターネットで公開されている資料の収集が実施されている状況です。

大半の一般的なウェブサーバ・ウェブアプリケーションはまず問題ありません。しかし万一、クローラによるアクセスに耐えられないシステムであった場合、クローラのアクセスによりサーバがエラーを出したり、レスポンスが極端に遅くなったり、最悪の場合、ウェブサーバが停止するといった不具合が発生し、利用者に不利益となる可能性があります（可用性が損なわれる）。

（M）クローラへの耐性の診断方法詳細は以下の通りです。

① アクセス方法

HTTP によるシリアルアクセス

HTTP リクエストを送信してから、HTTP レスポンスを受信するまでの間に、別の HTTP リクエストは送信しないアクセス方法です。なおこの診断では HTTP リクエストに Cookie は付加しないものとします。

② 負荷のかけ方

最大 0.5 秒に 1 回

ただし HTTP リクエストを送信し、その応答である HTTP レスポンスの受信を完了してからは、必ず 0.5 秒待機した後に、次の HTTP リクエストを送信するものとします。

③ 診断対象となるウェブページの選定方法

トップページ URL を起点として、そこから順次クローリングによってたどることが可能なウェブページ

ただしクローリングによって 1 度アクセスしたウェブページについては、以降の診断対象に含めません。なお、クローリングを行う際は、ウェブページ中の A タグから同一ドメイン内の URL を抽出するものとし、診断対象サイトのサブドメイン、別ドメインは原則として対象外とします。また、JavaScript、Java アプレット、Flash 等に含まれる URL 情報の収集や、手動入力を必要とするフォームによる遷移は行わないものとします。

④ 診断対象ページ数範囲

最小1ページから最大 4,800 ページ

⑤ 診断方法

トップページ URL を起点として、最大 0.5 秒間隔の HTTP によるシリアルアクセスで、順次クローリングを行ないます。仮に HTTP リクエストを送信してから、5 秒経過しても HTTP レスポンスの受信が完了しない場合は、HTTP 接続を一旦切断して 5 秒待機した後に HTTP によるシリアルアクセスを再開します。

なお、以下の診断終了条件のいずれかに該当した場合には、その時点で診断を終了とします。

1) クローリングによってたどることのできる全診断対象ページへのアクセスが完了した場合
2) 診断開始から 40 分が経過した場合
3) 「⑥ 脆弱性の判定基準」にある 1) ～ 6) のいずれかに該当した場合

⑥ 脆弱性の判定基準

診断の結果、次の 1) ～ 4) のいずれかの条件に該当する場合、以下の判定とします。

診断結果	「×異常」
危険度	「中」

診断の結果、次の 5) 又は 6) の条件に該当する場合は、以下の判定とします。

診断結果	「×異常」
危険度	「低」

診断の結果、次の 1）～ 6）の条件にいずれも該当しない場合は、以下の判定とします。

診断結果	「〇正常」

1） HTTP リクエストを送信してから、5 秒経過しても HTTP レスポンスの受信が完了しない状態が、5 回連続で発生した場合

2） HTTP リクエストを送信してから、5 秒経過しても HTTP レスポンスの受信が完了しない状態が、累計で 10 回発生し、かつ以下の計算式で算出される値が 10%以上であった場合

（計算式） 10 ÷ アクセスの総数 × 100%

3） HTTP レスポンスの HTTP ステータスコードにおいて、400 番台又は 500 番台のエラーが発生し、かつこの状態が、5 回連続で発生した場合

4） HTTP レスポンスの HTTP ステータスコードにおいて、400 番台又は 500 番台のエラーが発生する状態が、累計で 10 回発生し、かつ以下の計算式で算出される値が 10%以上であった場合

（計算式） 10 ÷ アクセスの総数 × 100%

5） HTTP リクエストを送信してから、5 秒経過しても HTTP レスポンスの受信が完了しない状態が、累計で 10 回発生し、かつ以下の計算式で算出される値が 10%未満であった場合

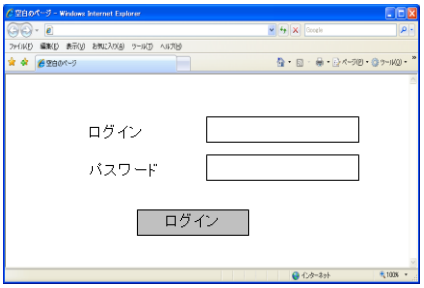
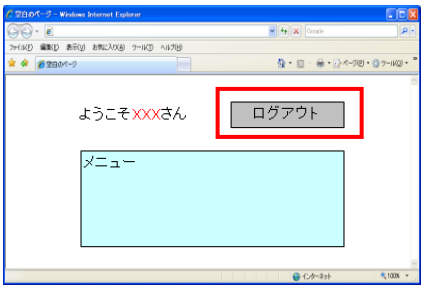
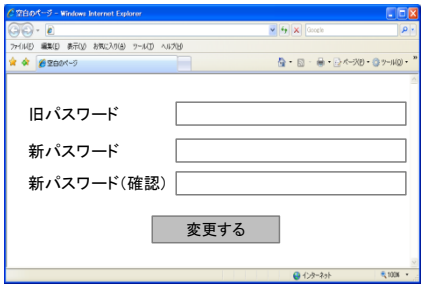
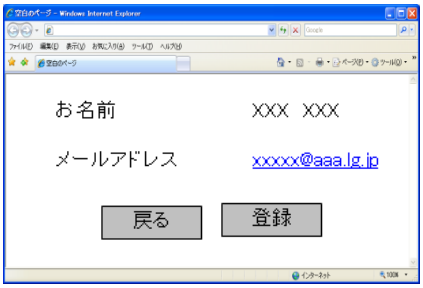
（計算式） 10 ÷ アクセスの総数 × 100%

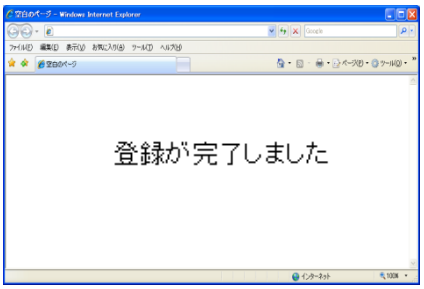
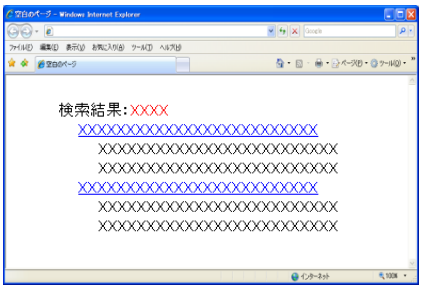
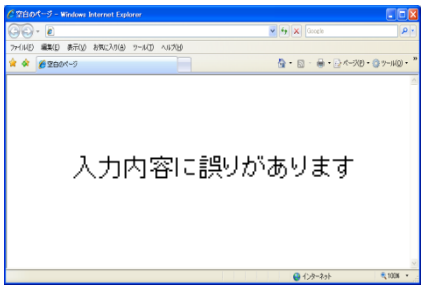
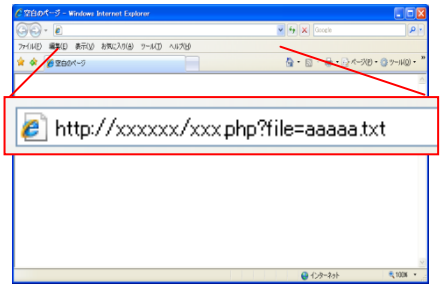
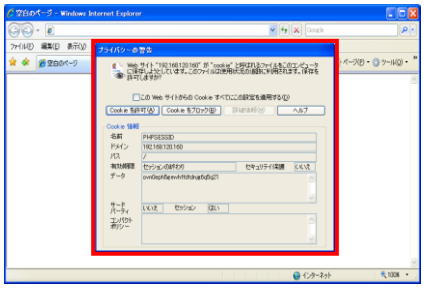
6） HTTP レスポンスの HTTP ステータスコードにおいて、400 番台又は 500 番台のエラーが発生する状態が、累計で 10 回発生し、かつ以下の計算式で算出される値が 10%未満であった場合

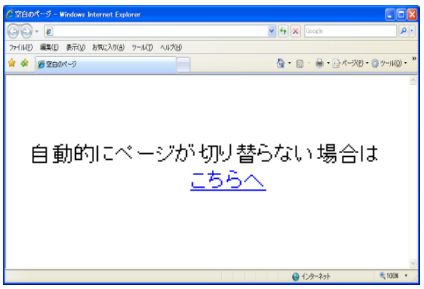
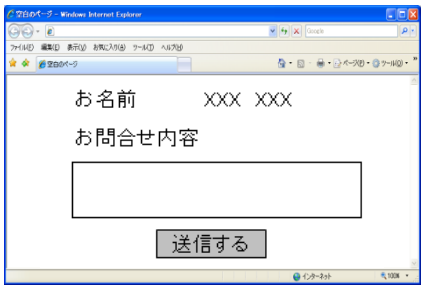
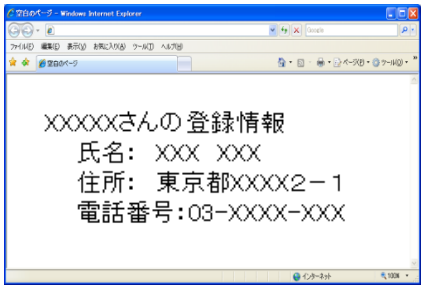
（計算式） 10 ÷ アクセスの総数 × 100%

2.5. 診断対象画面（機能）とその定義について

診断を実施するにあたっては、全ての画面（機能）を調査することが困難なウェブサイトもあるため、診断対象のページ数に上限を設け、診断対象となる画面（機能）の選定に関して以下のような定義を設けています。

診断対象画面（機能）名称	診断対象画面(機能)の定義／説明	診断対象画面（機能）イメージ
ログイン	ユーザ ID とパスワードを入力する等して認証を行う画面。 パスワードの代わりに「暗証番号」等の表記になっている場合もあります。	
ログアウト	認証状態を廃棄するための機能。 認証機能があれば、ログイン機能は必ずありますが、ログアウト機能を有しているとは限りません。ログアウトボタン等が見当たらない場合は、ログアウト機能が無いものと見なして構いません。	
パスワード変更	ユーザが自分のパスワードを変更する画面。	
入力内容確認	ユーザが入力した値を次の画面で表示し、確認できるようになっている画面。 一般的に、データ入力の画面は、「入力」→「確認」→「登録」の 3 画面構成になっていることが多く、その場合の 2 番目の画面を指します。なお、ウェブサイトによっては「入力」→「登録」という構成で「入力内容確認」がない場合もあります。	

診断対象画面（機能）名称	診断対象画面(機能)の定義／説明	診断対象画面（機能）イメージ
DB 更新	データの新規登録や変更により、データベースに更新処理を行っていると想定される画面。 実際に DB 更新を行っているかどうかは外部からは判別できないので、DB 更新と想定される画面を探します。	
DB アクセス	検索機能やデータ登録・参照機能等、SQL を利用していると想定される画面。 実際に SQL を使っているか、他の手段(ファイル、オブジェクト DB 等)を利用しているかは分からないので、通常 SQL を利用していると想定されるものを列挙します。	
エラー	エラー表示に特化した画面。 意図的にエラーを発生させることにより、エラーに特化した画面が現れるかどうかを確認します。ただし、そのようなエラー専用画面がない場合もあります。	
ファイル名	ファイル名と想定されるパラメータを引き回している画面。 xxxxx.txt 等拡張子が値に付与されている場合や、パラメータ名が xxxxfile、filexxxx 等、ファイル名を連想する命名になっていることにより見分けます。	
Cookie	Cookie 設定を行っている画面。 レスポンスヘッダを調べて、「Set-Cookie:」が発行されている画面を探します。特に、ミドルウェアの発行するセッション ID 以外の Cookie を優先して探します。	

診断対象画面（機能）名称	診断対象画面(機能)の定義／説明	診断対象画面（機能）イメージ
リダイレクト	Location ヘッダや「<meta http-equiv="Refresh" ...」により、他画面に遷移している画面。	
メール送信	アプリケーションがメールを送信している画面。 重要な処理(パスワード変更、申し込み処理等)の際に確認メールが送信される場合があります。そのような処理がないか探します。	
認可制御有	情報アクセスのための認可システムが実装されている箇所のことです。	

付録A. 用語対応表（平成 22 年度版から）

本資料「ウェブ健康診断仕様」は IPA が公開するものですが、それ以前に LASDEC が公開していました。今回「安全なウェブサイトの作り方」の別冊とするにあたっての整合をとる観点から、一部の用語の使い方を平成 22 年度版（LASDEC 公開）より変更しています。この付録では、変更した部分について、対応関係を記します。

平成 22 年度版（LASDEC 公開）	本資料（IPA 公開）
クロスサイト・スクリプティング（XSS）	クロスサイト・スクリプティング
クロスサイト・リクエスト・フォージェリ（CSRF）	CSRF（クロスサイト・リクエスト・フォージェリ）
メールヘッダインジェクション	メールヘッダ・インジェクション
パストラバーサル	パス名パラメータの未チェック／ディレクトリ・トラバーサル
アクセス制御	認可制御

著作・制作　独立行政法人情報処理推進機構（IPA）

編集責任　　小林 偉昭

※独立行政法人情報処理推進機構の職員については所属組織名を省略しました。

「安全なウェブサイトの作り方」別冊

ウェブ健康診断仕様

［発　　行］２０１２年１２月２６日　第１版　第１刷

［著作・制作］独立行政法人 情報処理推進機構 セキュリティセンター

情報セキュリティに関する届出について

IPA セキュリティセンターでは、経済産業省の告示に基づき、コンピュータウイルス・不正アクセス・脆弱性関連情報に関する発見・被害の届出を受け付けています。

ウェブフォームやメールで届出ができます。詳しくは下記のサイトを御覧ください。
URL: http://www.ipa.go.jp/security/todoke/

コンピュータウイルス情報

コンピュータウイルスを発見、またはコンピュータウイルスに感染した場合に届け出てください。

不正アクセス情報

ネットワーク(インターネット、LAN、WAN、パソコン通信など)に接続されたコンピュータへの不正アクセスによる被害を受けた場合に届け出てください。

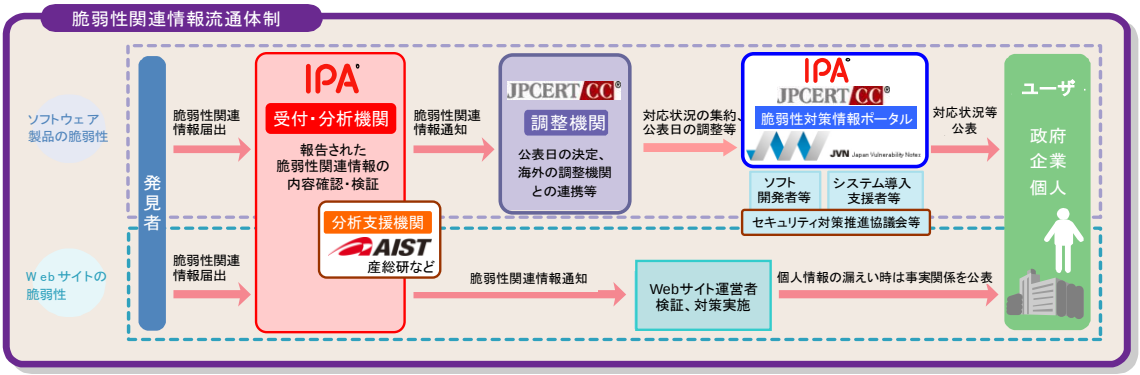
ソフトウエア製品脆弱性関連情報

OSやブラウザ等のクライアント上のソフトウエア、ウェブサーバ等のサーバ上のソフトウエア、プリンタやICカード等のソフトウエアを組み込んだハードウエア等に対する脆弱性を発見した場合に届け出てください。

ウェブアプリケーション脆弱性関連情報

インターネットのウェブサイトなどで、公衆に向けて提供するそのサイト固有のサービスを構成するシステムに対する脆弱性を発見した場合に届け出てください。

脆弱性関連情報流通の基本枠組み「情報セキュリティ早期警戒パートナーシップ」



※IPA:独立行政法人 情報処理推進機構、JPCERT/CC:一般社団法人 JPCERT コーディネーションセンター、産総研:独立行政法人 産業技術総合研究所

独立行政法人 情報処理推進機構
〒113-6591
東京都文京区本駒込二丁目28番8号
文京グリーンコートセンターオフィス16階
http://www.ipa.go.jp

セキュリティセンター
TEL: 03-5978-7527 FAX 03-5978-7518
http://www.ipa.go.jp/security/