Web サイトに対して専用ツールによる脆弱性診断作業を実施

Webアプリケーション診断項目

準拠ガイドライン	対象項目
OWASP TOP10	A1:2017-インジェクション
	A2:2017-認証の不備
	A3:2017-機微な情報の露出
	A4:2017-XML 外部エンティティ参照(XXE)
	A5:2017-アクセス制御の不備
	A6:2017-不適切なセキュリティ設定
	A7:2017-クロスサイトスクリプティング(XSS)
	A8:2017-安全でないデシリアライゼーション
	A9:2017-既知の脆弱性のあるコンポーネントの使用

準拠ガイドライン	対象項目
IPA 安全なウェブサイトの作り方	SQL インジェクション
	OS コマンド・インジェクション
	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
	セッション管理の不備
	クロスサイト・スクリプティング
	CSRF（クロスサイト・リクエスト・フォージェリ）
	HTTP 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
	クリックジャッキング
	バッファオーバーフロー

※A10:2017 - 不十分なロギングとモニタリング は対象外

Copyright Cybertrust Japan Co., Ltd. All rights reserved.

OWASP アプリケーションセキュリティ検証標準 4.0対応状況サマリー(1/8)

項番	内容
2.1.1	ユーザが設定するパスワードは、最低12文字となっている。(C6)
2.1.2	64文字以上のパスワードが使用できる。(C6)
2.1.3	パスワードにスペースを含めることができ、切り捨てが行われない。任意で、連続した複数のスペースは1つにまとめてもよい。(C6)
2.1.4	パスワードにUnicode文字が使用できる。単一のUnicode符号点は文字と見なされるため、12文字の絵文字や64文字の漢字が有効に使用できる必要があります。
2.1.6	パスワード変更機能には、ユーザの現在のパスワードと新しいパスワードが必要とされる。
2.1.7	アカウント登録、ログインおよびパスワード変更中に送信されるパスワードが、ローカル（システムのパスワードポリシーに一致する上位1,000または10,000個の最も一般的なパスワードなど）または外部API を使用して、侵害されたパスワードと照合される。API を使用する場合は、平文のパスワードが送信されたりパスワードの侵害状況を確認する際に使用されたりしないように、ゼロ知識証明またはその他の仕組みを使用する必要があります。パスワードが侵害された場合、アプリケーションはユーザに新しい侵害されていないパスワードの設定を要求する必要があります。(C6)

項番	内容
2.1.9	使用可能な文字の種類を制限するパスワード規則がない。大文字、小文字、数字、特殊文字を要求する必要はない。(C6)
2.1.11	パスワード入力に対して、ペースト、ブラウザのパスワードヘルパー、および外部パスワードマネージャが使用できる。
2.2.1	耐自動化コントロールが流出したクレデンシャルテスト攻撃、ブルートフォース攻撃、およびアカウントロックアウト攻撃の軽減に効果的となっている。このようなコントロールには最も一般的な流出パスワードのブロック、ソフトロックアウト、レート制限、CAPTCHA、試行間の遅延増加、IP アドレスの制限、または場所、デバイスへの最初のログイン、アカウントロック解除の最近の試行などのリスクベースの制限があります。一つのアカウントで一時間あたり100 回以上の試行失敗が可能ではない。
2.5.2	パスワードのヒントや知識ベースの認証（いわゆる「秘密の質問」）が存在しない。
2.5.3	パスワードクレデンシャルのリカバリによって現在のパスワードが明らかにならない。(C6)
2.5.4	共有アカウントまたはデフォルトアカウントが存在しない（例えば "root", "admin", "sa"）。
3.1.1	アプリケーションがURL パラメータやエラーメッセージ内にセッショントークンを漏洩しない。

Copyright Cybertrust Japan Co., Ltd. All rights reserved.

OWASP アプリケーションセキュリティ検証標準 4.0対応状況サマリー(2/8)

項番	内容
3.2.1	アプリケーションがユーザ認証時に新しいセッショントークンを生成する。(C6)
3.2.2	セッショントークンに少なくとも64ビットのエントロピーがある。(C6)
3.2.3	適切に保護されたCookie(セクション3.4 を参照) やHTML 5 セッションストレージなどのセキュアな方法を使用して、アプリケーションがブラウザにセッショントークンのみを保存する。
3.3.1	「戻る」ボタンや下流の依拠当事者(Relying Parties)が、依拠当事者(Relying Parties)間を含め認証済みセッションを再開しないように、ログアウトおよび有効期限によってセッショントークンが無効になる。(C6)
3.4.1	クッキーベースのセッショントークンにSecure 属性が設定されている。(C6)
3.4.2	クッキーベースのセッショントークンにHttpOnly 属性が設定されている。(C6)
3.4.3	クロスサイトリクエストフォージェリ攻撃を抑制するために、クッキーベースのセッショントークンがSameSite 属性を利用している。(C6)
3.4.4	セッションクッキーの機密性を確保するために、クッキーベースのセッショントークンが"__Host-"プレフィックス（参考文献を参照）を使用している。

項番	内容
3.7.1	機密性の高いトランザクションやアカウントの変更を許可する前に、アプリケーションが完全で有効なログインセッションを確保していること、または再認証や二次検証を必要としている。
4.1.1	特に、クライアント側のアクセス制御が存在し、それが迂回される可能性がある場合には、アプリケーションは信頼できるサービスレイヤに対してアクセス制御ルールを適用する。
4.1.2	アクセス制御で使用されるすべてのユーザ属性とデータ属性およびポリシー情報は、特に認可されていない限りエンドユーザーによって操作されない。
4.1.3	最小権限の原則が導入されている。ユーザは認可されているものについてのみ、機能やデータファイル、URL、コントローラ、サービス、他のリソースにアクセスできる。これは、なりすましや権限昇格に対する防御となる。(C7)
4.1.4	デフォルト拒否の原則が存在する。これにより新規のユーザやロールは最小限の権限または権限なしで開始し、アクセスが明示的に割り当てられるまで新しい機能へのアクセスができません。(C7)
4.1.5	例外が発生した場合も含めて、アクセス制御がセキュアに失敗する。(C10) ○
3.7.1	機密性の高いトランザクションやアカウントの変更を許可する前に、アプリケーションが完全で有効なログインセッションを確保していること、または再認証や二次検証を必要としている。

Copyright Cybertrust Japan Co., Ltd. All rights reserved.

OWASP アプリケーションセキュリティ検証標準 4.0対応状況サマリー(3/8)

項番	内容
4.2.1	機密データおよびAPI が、他人のレコードの作成や更新、全員のレコードの閲覧、すべてのレコードの削除など、レコードの作成、読み取り、更新、削除を目的とするダイレクトオブジェクト攻撃に対して保護されている。
4.2.2	認証済みの機能を保護するために、アプリケーションやフレームワークが強力なCSRF 対策メカニズムを実施していること、および有効な自動化対策やCSRF 対策が未認証機能の保護を実施している。
4.3.2	ディレクトリリスティグは、意図して許可されない限り、無効となっている。また、ファイルやディレクトリのメタデータ(Thumbs.db、.DS_Store、.git、.svn フォルダなど) の検出や開示が許可されていない。
5.1.2	フレームワークが大量のパラメータ割り当て攻撃から保護している、またはフィールドを非公開にするなど安全でないパラメータの代入を防ぐための対策が行われている。(C5)
5.1.3	すべての入力データがバリデーションされている。入力データには、HTML のフォームのフィールド、REST 呼び出し、クエリパラメータ、HTTP ヘッダ、Cookie、バッチファイル、RSS フィードなども含む。バリデーションはホワイトリスト方式で行う。(C5)
5.1.4	構造化データが強く型付けされており、使用可能な文字、長さ、パターン等の定義されたスキーマに基づいてバリデーションされる。（例：クレジットカード番号や電話番号などのバリデーションや、地区名と郵便番号等2つの関連するフィールドのデータが妥当なことのバリデーション）(C

項番	内容
5.1.5	URLのリダイレクト先と転送先がホワイトリストに登録された宛先のみ許可されている、または信頼できない可能性のあるコンテンツにリダイレクトするときに警告を表示する。
5.2.1	WYSIWYG エディタ等から取得した信頼できないHTML入力が、HTMLサニタイザライブラリもしくはフレームワークの機能によって適切に無害化され、入力バリデーションやエンコードにより適切に処理されている。(C5)
5.2.2	非構造化データが無害化され、使用可能な文字や長さなど一般的な対策が適用されている。
5.2.3	SMTP またはIMAP インジェクションから保護するため、アプリケーションがメールシステムに渡す前にユーザ入力を無害化する。
5.2.4	eval()もしくは動的コード実行機能を使用しない。代替方法がない場合は、実行前に含まれるユーザ入力の無害化もしくはサンドボックス化する。
5.2.5	テンプレートインジェクション攻撃に対して、ユーザ入力の無害化もしくはサンドボックス化によってアプリケーションが保護されている。
5.2.6	信頼できないデータやファイル名やURL入力フィールドなどHTTPファイルメタデータのバリデーションまたは無害化や、プロトコル、ドメイン、パス、ポートにホワイトリストを使用することで、アプリケーションがSSRF攻撃から保護されている。

Copyright Cybertrust Japan Co., Ltd. All rights reserved.

OWASP アプリケーションセキュリティ検証標準 4.0対応状況サマリー(4/8)

項番	内容
5.2.7	ユーザの指定したSVGスクリプト化可能コンテンツ（特にXSSに関連するインラインスクリプトやforeignObject）に対して、アプリケーションが無害化またはサンドボックス化している。
5.2.8	ユーザ指定のMarkdown、CSS、XSLスタイルシート、BBCodeのようなスクリプト可能もしくは式のテンプレート言 語コンテンツに対して、アプリケーションが無害化、無効化またはサンドボックス化されている。
5.3.1	出力エンコーディングがインタプリタとコンテキストが要求するものに関連している。例えば特に信頼できない入力 ("ねこ" や"O'Hara" など、Unicode 文字やアポストロフィを含む名前など) に対して、HTML値、HTML属性、JavaScript、URLパラメータ、HTMLヘッダ、SMTP、その他コンテキストが必要とするものに対して個別のエンコードを使用する。(C4)
5.3.2	どのUnicode文字でも有効かつ安全に処理されるように、出力エンコーディングがユーザが選択した文字コードセット、ロケールが保持されている。(C4)
5.3.3	HTML や他のWeb クライアントコード中に存在するすべての文字列変数が、コンテキストに応じて適切に手動でエンコードされる、もしくはコンテキストに応じて自動的にエンコードを行うテンプレートを使用しており、アプリケーションが、反射型、格納型、およびDOMベースクロスサイトスクリプティング(XSS)攻撃の影響を受けない。(C4)

項番	内容
5.3.4	データ選択またはデータベースクエリ（例、SQL、HQL、ORM、NoSQL）がクエリのパラメータ化、ORM、エンティティフレームワークもしくは他の方法により保護されており、データベースインジェクション攻撃の影響を受けない。(C3)
5.3.5	パラメータ化もしくはより安全な機構が存在しない場合、SQLインジェクションから保護するためのSQLエスケープの使用など、コンテキスト固有の出力エンコーディングによりインジェクション攻撃から保護されている。(C3, C4)
5.3.6	eval攻撃、リモートJavaScriptインクルード、CSPバイパス、DOM XSS、JavaScriptの式の評価を含むJavaScriptもしくはJSONインジェクション攻撃からアプリケーションが保護されている。(C4)
5.3.7	アプリケーションがLDAP インジェクションの影響を受けない、またはセキュリティ管理策によってLDAP インジェクションが防止される。(C4)
5.3.8	OSコマンドインジェクションに対して保護していること、およびオペレーティングシステムコールがパラメータ化されたOSクエリを使用、もしくはコンテキストコマンドライン出力エンコーディングを使用する。(C4)
5.3.9	アプリケーションが、リモートファイルインクルード(RFI) やローカルファイルインクルード(LFI) の影響を受けない。

Copyright Cybertrust Japan Co., Ltd. All rights reserved.

OWASP アプリケーションセキュリティ検証標準 4.0対応状況サマリー(5/8)

項番	内容
5.3.10	アプリケーションがXPathインジェクション攻撃やXML インジェクション攻撃から保護されている。(C4)
5.5.1	シリアライズされたオブジェクトが整合性チェックを使用していること、または悪意のあるオブジェクトの作成やデータの改ざんを防ぐために暗号化されている。(C5)
5.5.2	アプリケーションがXMLパーサを可能な限り最も制限の厳しい構成のみを使用するように正しく制限し、外部エンティティの解決などの危険な機能を無効にしてXXEを防ぐようにしている。
5.5.3	信頼できないデータのデシリアライズが回避されている、またはカスタムコードとサードパーティのライブラリ（JSON、XML、YAMLパーサなど）の両方で保護されている。
5.5.4	ブラウザもしくはJavaScriptベースのバックエンドでJSON をパースするときはJSON.parse を使用する。eval() を使用しない。
6.2.1	すべての暗号化モジュールにおいて、処理に失敗した場合の安全対策が施されており、オラクルパディング攻撃を許さない方法でエラーが処理される。
8.2.1	最新のブラウザで機密データがキャッシュされないように、アプリケーションは十分なキャッシュ防止ヘッダを設定する。

項番	内容
8.2.2	クライアントの記憶域（HTML5 のローカルストレージ、セッションストレージ、IndexedDB、通常のCookie、FlashCookie など）に保存されるデータにセンシティブなデータやPII が含まれていない。
8.2.3	セッションの終了後、ブラウザのDOM など認証されたデータがクライアントの記憶域から消去される。
8.3.1	センシティブなデータがHTTP メッセージボディまたはヘッダでサーバに送信される。どんなHTTP verb のクエリストリングパラメータにもセンシティブなデータが含まれない。
9.1.1	安全なTLSがすべてのクライアント接続に使用されており、安全でないプロトコルや非暗号化プロトコルにフォールバックしない。(C8)
9.1.2	オンラインまたは最新のTLSテストツールを使用して、強力なアルゴリズム、暗号、プロトコルのみが有効であり、最も強力なアルゴリズムと暗号が優先的に設定されている。
9.1.3	古いバージョンのSSLやTLSプロトコル（SSLv2、SSLv3、TLS 1.0、TLS 1.1）、アルゴリズム、暗号および構成が無効になっている。最新バージョンのTLSを優先する暗号スイートに設定する。
10.3.2	アプリケーションで、コード署名やサブリソースの完全性などの保護が使用されている。加えて、信頼できない場所やインターネットから取得したモジュール、プラグイン、コード、ライブラリなどをロードまたは実行しない。

Copyright Cybertrust Japan Co., Ltd. All rights reserved.

OWASP アプリケーションセキュリティ検証標準 4.0対応状況サマリー(6/8)

項番	内容
10.3.3	期限切れドメイン名、期限切れDNS ポインタまたはCNAME、パブリックソースコードリポジトリでの期限切れプロジェクト、一時的なクラウドAPI、サーバレス機能、ストレージバケット（autogen-bucket-id.cloud.example.com）など、DNSエントリまたはDNS サブエントリに依存している場合、アプリケーションがサブドメイン奪取（subdomaintakeover）から保護されている。アプリケーションの保護は使用するDNS 名の有効期限または変更を定期的にチェックすることを含めます。
11.1.1	アプリケーションが同じユーザのビジネスロジックフローを手順通り、省略せずに処理する。
11.1.2	アプリケーションは、すべてのステップが人間の実際に処理する時間で処理されたビジネスロジックフローのみ処理する。（送信されるのが早すぎるトランザクションは処理されない。）
11.1.3	アプリケーションに適切な制限が実装されており、特定のビジネス活動やトランザクションに対し、ユーザごとに適用されている。
11.1.5	アプリケーションは脅威モデリング(threat modelling)または類似の方法を使用して特定されたビジネスリスクから保護するために、ビジネスロジックの制限またはバリデーションがある。
12.3.1	パストラバーサルから保護するために、ユーザが送信したファイル名のメタデータがシステムまたはフレームワークファイルやURL APIで直接使用されていない。

項番	内容
12.3.2	ローカルファイル（LFI）の漏えい、作成、更新、または削除を防止するために、ユーザが送信したファイル名のメタデータをバリデートもしくは無視する。
12.3.3	SSRFにも繋がる可能性があるリモートファイル(RFI)の漏えいまたは実行を防ぐために、ユーザが送信したファイル名のメタデータをバリデートもしくは無視する。✓
12.3.4	アプリケーションを反射型ファイルダウンロード（RFD）から保護するため、ユーザが送信したファイル名（JSON、JSONPまたはURLパラメータの中にある）をバリデートまたは無視し、レスポンスのContent-Type ヘッダはtext/plainに設定、およびContent-Disposition ヘッダは固定ファイル名を指定する。
12.3.5	OS コマンドインジェクションから保護するために、信頼できないファイルメタデータをシステムAPI またはライブラリで直接使用しない。
12.4.1	信頼できない場所から取得したファイルは、Webルート以外にパーミッションを制限した上で保存し、可能な限り厳密なバリデーションを行う。
12.4.2	信頼できない場所から取得したファイルが、アプリケーションが想定する種類であることを検証し、既知の悪性コンテンツがアップロードされるのを防止するためにアンチウイルスソフトで検査する。
12.5.1	意図しない情報やソースコードの漏えいを防ぐために、特定のファイル拡張子を持つファイルのみを処理するようにWeb層が構成されている。例えば、バックアップファイル（.bakなど）、一時作業ファイル（.swpなど）、圧縮ファイル（.zip、.tar.gzなど）およびエディタで一般的に使用されるその他の拡張子は、必要ない限り処理しない。

Copyright Cybertrust Japan Co., Ltd. All rights reserved.

OWASP アプリケーションセキュリティ検証標準 4.0対応状況サマリー(7/8)

項番	内容
12.5.2	アップロードされたファイルへの直接のリクエストがHTML/JavaScriptコンテンツとして実行されない。
12.6.1	Webサーバまたはアプリケーションサーバが、リクエストを送信したりデータ/ファイルをロードしたりできるように、リソースまたはシステムにホワイトリストが構成されている。
13.1.1	SSRF 攻撃やRFI 攻撃で使用される可能性があるような、異なるURI またはファイルのパーサを悪用する攻撃を回避するために、すべてのアプリケーションコンポーネントが同じエンコードおよびパーサを使用する。
13.1.2	Web サービスアプリケーション内の管理機能にアクセスできるのは、アクセスが許可された管理者のみとなっている。
13.1.3	API URL がAPI Key やセッショントークンなどの機密情報を公開していない。
13.2.1	保護されたAPI またはリソースに対して通常ユーザがDELETE または PUT を使用するのを防ぐなど、有効化されているRESTful HTTP メソッドが、ユーザまたはアクションにとって妥当となっている。
13.2.2	JSON スキーマバリデーションが設定され、入力を受け付ける前に確認されている。
13.2.3	Cookie を使用するRESTful Webサービスが、次のうち少なくとも1つ以上を使って、クロスサイトリクエストフォージェリから保護されている。三重または二重送信クッキーパターン（参考文献）、CSRFノンス、ORIGINリクエストヘッダのチェック。

項番	内容
13.3.1	適切に形成されたXML 文書を確保するために、XSD スキーマバリデーションに続いて、そのデータの処理が行われる前に各入力フィールドのバリデーションが実施されている。
14.2.1	すべてのコンポーネントが最新となっている。できればビルド時またはコンパイル時にディペンデンシチェッカを使用する。(C2
14.2.2	サンプルアプリケーション、プラットフォームのドキュメント、デフォルトまたはサンプルのユーザなど、不要な機能、ドキュメント、サンプル、コンフィギュレーションがすべて削除されている。
14.2.3	JavaScriptライブラリ、CSSスタイルシート、Webフォントなどのアプリケーション資産がコンテンツ配信ネットワーク（CDN）または外部プロバイダで外部的にホストされている場合、資産の整合性を検証するためにサブリソース完全性（SRI）が使用されている。
14.3.1	Webまたはアプリケーションサーバとフレームワークのエラーメッセージが、意図しないセキュリティ情報の開示を排除するために、ユーザが実行可能なカスタマイズされた応答を返すように構成されている。
14.3.2	Webまたはアプリケーションサーバとアプリケーションフレームワークのデバッグモードが運用環境で無効になっていることを確認して、OWASP アプリケーションセキュリティ検証標準4.089デバッグ機能、開発者コンソール、および意図しないセキュリティ開示を排除する。
14.3.3	HTTPヘッダまたはHTTPレスポンスの一部がシステムコンポーネントの詳細なバージョン情報を公開していない。

Copyright Cybertrust Japan Co., Ltd. All rights reserved.

OWASP アプリケーションセキュリティ検証標準 4.0対応状況サマリー(8/8)

項番	内容
14.4.1	すべてのHTTPレスポンスに、安全な文字セット（例：UTF-8、ISO 8859-1）を指定するコンテントタイプヘッダが含まれている。
14.4.2	すべてのAPIレスポンスにContent-Disposition:attachment; filename="api.json"が含まれている（または他のコンテントタイプの適切なファイル名）。
14.4.3	HTML、DOM、JSON、JavaScriptインジェクションの脆弱性などのXSS攻撃の影響を軽減するのに役立つContentSecurity Policy(CSPv2) が配置されている。
14.4.4	すべてのレスポンスにX-Content-Type-Options：nosniffが含まれている。
14.4.5	HTTP Strict Transport Securityヘッダがすべてのレスポンスとすべてのサブドメインに含まれている。例えば、Strict-Transport-Security：max-age = 15 724800;
14.4.6	「no-referrer」や「same-origin」のような、適切な「Referrer-Policy」ヘッダが含まれている。
14.4.7	サードパーティのサイトに埋め込むべきではないサイトで、適切なヘッダが（XFrame-OptionsまたはContent-Security-Policy：frame-ancestors）が、サイトで使用されている。
14.5.1	アプリケーションサーバが、pre-flight OPTIONSを含む、アプリケーションまたはAPIで使用されているHTTPメソッドのみを受け入れる。
14.5.2	提供されたOriginヘッダは、攻撃者によって簡単に変更できるため、認証やアクセス制御の判断に使用されていない。

項番	内容
14.5.3	オリジン間リソース共有（CORS）のAccess-Control-Allow-Originヘッダが信頼できるドメインの厳密なホワイトリストを使用して照合し、「null」オリジンをサポートしていない。

Copyright Cybertrust Japan Co., Ltd. All rights reserved.

Web サイトに対して専用ツールによる脆弱性診断作業を実施

ネットワーク診断項目

カテゴリ	対象項目
ポートスキャン	TCP（0～65535）/ UDP（主要ポート）のポートの状況調査
バナー調査	使用ソフトウェアの検出、バージョン情報の収集
稼働サービスの設定調査	稼働サービスの設定不備の調査 例）Telnet,FTP,SMTP等
アカウント調査	デフォルトアカウント調査、認証なしで利用できるサービスの調査

本サービスではWebアプリケーション(前頁)に対する診断に加え、
ネットワークスマート診断も標準でご提供させて頂きます。

Copyright Cybertrust Japan Co., Ltd. All rights reserved.