外部公開サイト構築・運用のセキュリティに関する仕様書

1　インシデント対応体制

(1)　セキュリティインシデント、セキュリティポリシーの違反等により情報資産に対するセキュリティ侵害が発生又は発生するおそれがある場合に、速やかに適切な対応がとれるよう、緊急時の対応計画を定めるとともに、夜間休日を含めた緊急時の連絡体制を構築すること。

(2)　緊急時の対応計画には、以下の内容を含めること。

ア　インシデント対応に係る報告窓口、必要な連絡先のリスト、情報共有手段の確保

イ　インシデントの発見及び報告、初動対応、告知、抑制措置と復旧、事後対応などの対応フロー

(3)　インシデント発生前の準備として、委託者及び受託者間の連絡手段について、疎通確認を実施すること。また、委託者と協議の上、インシデント対応訓練の実施に協力すること。

2　構築時の対策

(1)　ネットワークにファイアウォールを導入し、フィルタリング及びルーティング等により、適切なアクセス制御を施すこと。

(2)　Web サイトで機密情報又は個人情報を扱う場合は、以下のいずれかの対応を行うこと。

ア　IDS(不正侵入検知システム)を導入し、セキュリティ検知内容を監視するとともに、常時対応できる体制をとること。

イ　IPS（不正侵入防御システム）を導入すること。

ウ　WAF（ウェブアプリケーションファイアウォール）を導入すること。

(3)　Web サイトの改ざん検知を行うこと。なお、委託者が提供する改ざん検知サービスを利用することも可能であるが、その場合は委託者に依頼すること。

(4)　盗聴防止のため通信経路を暗号化すること。システム保守作業用の通信も含む。

(5)　外部からの侵入を防ぐため、保守作業用の通信は専用のネットワークとする又は通信可能な相手先を委託業者のネットワークに限定する等のアクセス制限をすること。

(6)　サーバの保守作業のために SSH を利用する場合は、公開鍵認証又は電子証明書による認証にすること。また、SSH の公開ポートをデフォルトポートから変更すること。

(7)　OS、アプリケーションは既知の脆弱性情報が公開されていないバージョンを採用し、最新のパッチを適用すること。

(8)　サーバで定期的にウイルススキャン（フルスキャン）を実施すること。

(9)　Web サイトの公開に不要なポートをすべて閉じること。

(10)　Web サイトの公開に不要なサービスを停止すること。

(11)　サーバへの外部からのアクセスに対して、利用ソフトウェア及びそのバージョンが推測できないようにすること。

(12)　構築時に使用したが運用の際には使用しないアプリケーションを含め、不要なアプリケーションを削除すること。

(13)　個人情報及び機微情報を保存する際は、暗号化すること。

(14) サーバまたはソフトウェアに登録するユーザについて、運用に必要な最小の権限設定とすること。また、登録されているユーザが把握できるよう管理を徹底すること。

(15) 必要のないアカウントは無効にすること。

(16) 複数職員等による同一アカウント(ID/パスワード)の共用を禁止すること。

(17) 利用者用アカウントおよび保守用アカウントなどを含めて、すべてのアカウントのパスワードが以下の基準を満たしていること。

ア パスワードは 10 文字以上とすること。

イ 英大文字小文字が混在していること。

ウ 1文字以上の数字が含まれること。

エ 1文字以上の記号が含まれること。

(18) Web サイト利用者がログインに失敗した場合に表示するエラーメッセージは、認証に失敗した理由を ID が存在しないか、パスワードが正しくないかのどちらかを特定できないようにすること。

(19) Web サイト利用者のパスワード変更の際に、変更前と変更後のパスワードを入力させるなど、第三者にパスワードを変更されないような対策を講ずること。

(20) Web サイト利用者のパスワード再発行の際は、パスワードリセット用の URL を登録済みのメールアドレスに送信するなど、変更後のパスワードを第三者に推測されにくい方法を採用すること。

(21) ウェブサイトに対する不正アクセスを防止するため、以下の攻撃及び脆弱性を回避するための情報セキュリティ対策を実施すること。

ア SQL インジェクション

イ OS コマンド・インジェクション

ウ 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

エ セッション管理の不備

オ クロスサイト・スクリプティング

カ CSRF(クロスサイト・リクエスト・フォージェリ

キ HTTP ヘッダ・インジェクション

ク メールヘッダ・インジェクション

ケ クリックジャッキング

コ バッファオーバーフロー

サ アクセス制御や認可制御の欠落

(22) 運用を開始する前に、「別紙 運用開始時のチェックリスト」を用いて構築時のセキュリティ対策について報告し、委託者の承認を得ること。なお、委託者より対策状況の証跡を求められた場合は、提出すること。

3 運用保守

(1) OS、アプリケーションに最新のパッチを適用するとともに、最新の状態を常に保つ体制をとること。

(2)　週1回以上の頻度で定期的に脆弱性情報を確認し、緊急時には即時対応とすること。
(3)　委託者から脆弱性情報の提供があった場合は、該当の有無と影響を確認し、委託者に報告すること。
(4)　利用する機器及びソフトウェアに関連する脆弱性情報を入手した場合又は脆弱性対策が講じられてない状態が確認できた場合は、委託者に報告するとともに、最新のセキュリティパッチの適用又はソフトウェアバージョンアップ等によるシステムへの影響を考慮した上で、脆弱性対策を講じること。
(5)　保守用アカウントの情報は外部流出等による不正使用防止の観点から適切に管理すること。
(6)　保守作業を実施する際は詳細なオペレーション記録を保守操作ログとして記録し、保管すること。
(7)　リモートアクセスによるシステムの改修や保守を実施する場合には、必ずアクセスログを取得し保管すること。
(8)　Web サイトのコンテンツが外部から不正に改ざんされた場合や、外部からの攻撃又はランサムウェアによりサーバ上のデータが破壊された場合等において、システムを迅速に復旧できるよう、システム及びデータについて定期的にバックアップを取得すること。

4　ログの管理
(1)　ネットワーク機器、サーバ及びウェブアプリケーション等のログ（アクセスログ、認証ログ、各ユーザのコマンド履歴、システムエラーログ等）を取得し、不正な通信や異常がないか、定期的に内容を確認すること。また、確認結果を報告すること。
(2)　アクセスログ等の整合性を保つため、サーバの正確な時刻設定及びサーバ間の時刻同期ができる措置を講ずること。
(3)　ログの履歴は窃取、改ざん、誤消去等をされない措置を講ずること。
(4)　ログの履歴を管理し、1 年間以上保管すること。また、委託完了時に納品すること。

5　本特記仕様書に係る納品物
(1)　システム構成、サーバ構成及びネットワーク構成が分かる資料
(2)　緊急時の対応計画及び連絡体制（委託開始時）
(3)　運用開始時のチェックリスト（運用開始時）
(4)　各種ログ（委託完了時）

6　本委託納品物の納品方法
(1)　本特記仕様書で定義する納品物に限らず、本委託の一切の納品物（Web サイトデータを含む）については、受託者でウイルスチェックを行った上で納品すること。

Web サイト構築・運用のセキュリティに関する特記仕様書 別紙　運用開始時のチェックリスト

項番	内容	受託業者確認 結果記載欄
2－ (1)	ネットワークにファイアウォールを導入し、フィルタリング及びルーティング等により、適切なアクセス制御を施すこと。	□対応済
2－ (2)	Web サイトで機密情報又は個人情報を扱う場合は、以下のいずれかの対応を行うこと。 ・IDS(不正侵入検知システム)を導入し、セキュリティ検知内容を監視するとともに、常時対応できる体制をとること。 ・IPS（不正侵入防御システム）を導入すること。 ・WAF（ウェブアプリケーションファイアウォール）を導入すること。	□対応済 対応内容 （ ）
2－ (3)	Web サイトの改ざん検知を行うこと。なお、委託者が提供する改ざん検知サービスを利用することも可能であるが、その場合は委託者に依頼すること。	□対応済
2－ (4)	盗聴防止のため通信経路を暗号化すること。システム保守作業用の通信も含む。	□対応済
2－ (5)	外部からの侵入を防ぐため、保守作業用の通信は専用のネットワークとする又は通信可能な相手先を委託業者のネットワークに限定する等のアクセス制限をすること。	□対応済
2－ (6)	サーバの保守作業のために SSH を利用する場合は、公開鍵認証又は電子証明書による認証にすること。また、SSH の公開ポートをデフォルトポートから変更すること。	□対応済
2－ (7)	OS、アプリケーションは既知の脆弱性情報が公開されていないバージョンを採用し、最新のパッチを適用すること。	□対応済
2－ (8)	サーバで定期的にウイルススキャン（フルスキャン）を実施すること。	□対応済
2－ (9)	Web サイトの公開に不要なポートをすべて閉じること。	□対応済
2－ (10)	Web サイトの公開に不要なサービスを停止すること。	□対応済
2－ (11)	サーバへの外部からのアクセスに対して、利用ソフトウェア及びそのバージョンが推測できないようにすること。	□対応済
2－ (12)	構築時に使用したが運用の際には使用しないアプリケーションを含め、不要なアプリケーションを削除すること。	□対応済
2－ (13)	個人情報及び機微情報を保存する際は、暗号化すること。	□対応済

項番	内容	受託業者確認結果記載欄
2－(14)	サーバまたはソフトウェアに登録するユーザについて、運用に必要な最小の権限設定とすること。また、登録されているユーザが把握できるよう管理を徹底すること。	□対応済
2－(15)	必要のないアカウントは無効にすること。	□対応済
2－(16)	複数職員等による同一アカウント（ID/パスワード）の共用を禁止すること。	□対応済
2－(17)	利用者用アカウントおよび保守用アカウントなどを含めて、すべてのアカウントのパスワードが以下の基準を満たしていること。 ・パスワードは 10 文字以上とすること。 ・英大文字小文字が混在していること。 ・１文字以上の数字が含まれること。 ・１文字以上の記号が含まれること。	□対応済
2－(18)	Web サイト利用者がログインに失敗した場合に表示するエラーメッセージは、認証に失敗した理由を ID が存在しないか、パスワードが正しくないかのどちらかを特定できないようにすること。	□対応済
2－(19)	Web サイト利用者のパスワード変更の際に、変更前と変更後のパスワードを入力させるなど、第三者にパスワードを変更されないような対策を講ずること。	□対応済
2－(20)	Web サイト利用者のパスワード再発行の際は、パスワードリセット用の URL を登録済みのメールアドレスに送信するなど、変更後のパスワードを第三者に推測されにくい方法を採用すること。	□対応済
2－(21)	ウェブサイトに対する不正アクセスを防止するため、以下の攻撃及び脆弱性を回避するための情報セキュリティ対策を実施すること。 ・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 ・アクセス制御や認可制御の欠落	本項目については、IPA（独立行政法人情報処理推進機構）「安全なウェブサイトの作り方 改訂第 7 版 セキュリティ実装チェックリスト」を活用して報告すること。