別紙1

ホームページ運営業務におけるセキュリティ要件

(1)ウェブサーバー等に対する接続制限

ウェブサーバー・CMS等のウェブサイトを構成する機器・サービスに対しては、通信(受託者にてリモートメンテナンスのために使用する通信も含む)の制限を行い、公衆インターネット回線からの不正アクセスに備えること。IPアドレスや電子証明書による認証が望ましい。

(2)パスワードポリシー

全ての管理者用アカウントに付与するパスワードは、[8文字以上、英字(大文字・小文字)・数字・記号混合]とすること。この基準を下回るパスワードに、一般ユーザー自らが設定・変更することは不許可とすること。

(3)認証制限(アカウントロック)

上記(1)のIPアドレスや電子証明書による認証を行うことが困難な環境では、ユーザー認証は、一定回数の失敗でロックをかけること。設定値は契約後に指示する。

(4)サービス不能攻撃対策

サービス不能攻撃と疑われる大量通信などによるサーバの稼働停止を検知できる体制を有すること。検知した際は、速やかに委託者に報告を行うとともに、対応方針を示し、協議を行うこと。サービス不能攻撃対策が施されたプラットフォームであれば、なお望ましい。

(5)脆弱性対応

受託者は、脆弱性に関する情報を収集するとともに、ウェブサイトを構成する環境に係る設定は定期的に点検し、インジェクション攻撃等を招くことがないよう、不必要なサービスについては制限・停止を行うこと。

また、ウェブサイトを構成する環境に脆弱性が発見され、対応が必要と区が判断した場合は、受託者はサービスの影響が最小となるよう対応計画案を策定し、区の承認を得た上で実施すること。

(6)常時SSL化について

本ページについては、常時SSL化対応とすること。台東区のサブドメインを採用するにあたり、SSL通信を採用していることから、SSLサーバ証明書の適用を実施すること。