

システム保守業務に対する運用基盤要件

(1) ネットワーク

利用者とシステム間の接続は、インターネットを利用すること。

(2) 利用規模・拡張性

以下の利用規模（ピーク時のアクセス量も含む。）を想定すること。

ア 会員数

単年度登録1,750名程度、同時アクセス6割程度

※登録開始2年目（令和7年度）は最大3,000名程度

イ 管理者

10名程度

(3) システム運用時間

24時間365日 ※計画停止、定期保守を除く。

(4) サーバ

ア 政府情報システムのためのセキュリティ評価制度（ISMAP）に登録されたクラウドサービスであること。

イ サーバ調達は、ホスティングベンダーが提供するホスティングサービスの利用可。ただし、共同利用は行わないこと。また、サーバ設置場所は、ICカード等による入退室管理、停電時の補助電源設備、空調設備、火災・地震・水害等の災害対策、耐震構造を備え、24時間365日監視体制のセキュリティが十分確保された日本国内データセンターとすること。さらに、入退室記録の管理を行うこと。

ウ 国内法を適用するため、国内にサーバが設置されていること。

エ ウェブサーバ、データベースサーバは、OSレベルで独立したものとする。

オ サーバを物理的に独立させるほか、同一筐体内に複数の仮想サーバを持つ構成も可とする。

カ ハードウェア故障の発生時等に停止することなく運用又はシステムの停止時間を可能な限り少なくするため、サーバ設備やネットワークの冗長化について必要な箇所に対策を行うこと。

キ 個人情報を含む情報資産を取り扱うサーバ等を設置した区域に機器を搬入する場合は、この区域（施設・設備）とは隔離された区画に納品場所・一時保管場所を指定する。又は、受託者が同行することにより監視・監督を行うこと。

ク 時刻同期に対応すること。

(5) セキュリティ

項目	要件
サーバ環境	<ul style="list-style-type: none"> ・セキュリティホールやバグを発生させないサーバの環境設定を行うこと。また、セキュリティパッチ適用等、脆弱性修正措置が必要になった場合、同一サーバ上の他システムの影響を受けることなく速やかに対応できること。 ・IPA 掲載の「安全なウェブサイトの作り方」に準拠すること。（https://www.ipa.go.jp/security/vuln/websecurity/）
ウイルス対策	<ul style="list-style-type: none"> ・適切なウイルス対策を行うこと。必要に応じたウイルスチェックができること。ウイルス対策ソフトを導入する場合、常に最新のパターンファイルを適用すること。 ・端末及びサーバの定期的なウイルスチェックを実施すること。 ・メール受信を行う場合、メールサーバでのウイルス対策（ゲートウェイソフトウェアの導入）を実施すること。
不正アクセス・改ざん対策	<ul style="list-style-type: none"> ・ファイアウォールを設置し、運用に必要な通信ポート及びIPアドレスを制限し、不正アクセスから保護すること。改ざん対策を行うこと。 ・WAF(Web Application Firewall)やIPS/IDSを導入し、脆弱性を突いた攻撃に対する対策を行うこと。
暗号化通信	利用者の端末とサーバ間は、SSL (Secure Socket Layer) / TLS (Transport Layer Security)による暗号化通信を行うこと。
利用者認証	多要素認証又はID/パスワードによる認証で、パスワードは英数字記号16文字以上とすること。
ログ	アクセスログを1年以上保存すること。必要に応じ、調査・分析を行うことができるように各利用者のログ記録（アクセス、操作、エラー）を取得できること。
その他	<ul style="list-style-type: none"> ・本業務に基づくシステム構築が影響する範囲について、第三者による脆弱性診断や脆弱性診断ツール等を用いて脆弱性診断を行い、結果を書面にて報告すること。脆弱性が発見された場合は速やかに対策を行うこと。 ・パスワード不正利用防止のため、パスワードをデータベースに保存する場合は暗号化を行うこと。 ・個人情報保護及び情報漏洩対策を行うこと。 ・OSやソフトウェアのバージョンアップ、セキュリティパッチ適用等について、システム運用に支障がないようにすること。