別紙４

システム運用機器類の管理及び運用について

サイトの公開･運用などに必要なハードウェア、ソフトウェア、ネットワーク機器等について、委託者と協議の上、下記のとおり調達し、システムを構成し、管理・運用すること。

１　ドメイン名

使用ドメイン名は委託者と協議すること。

なお、使用ドメインは都で用意することを想定するが、使用ドメイン名の取得及びLGPKI Webサーバ証明書発行するまでの期間は、受託者の負担にて、SSL証明書適用（httpsによる暗号化通信）、不要なポートの全ての遮断、特定のIPアドレスのみからのアクセス許可等の対策を行い、十分なセキュリティ対策を施すこと。

また、以下の（１）～（２）を行うこと。

（１）lg.jpドメイン設定

①　都がサブドメインを申請するための様式に示す申請入力票の必要な項目を入力し、作成すること。また、CSRファイルを作成すること。

②　サブドメインのDNS設定を行うこと。

（２）LGPKI Webサーバ証明書のインストール

①　都がLGPKIを申請するための様式に示す申請入力票の必要な項目を入力し、作成すること。申請に必要なCSRファイルは、(1) で作成したものを兼ねることとする。

②　本サイトにLGPKI Webサーバ証明書をインストールすること。

２　システム運用機器類の構成

（１）サーバ（インターネット回線準備を含む。）

サーバは専用サーバとし、ホスティングサービスを前提とする。サーバの機能及びホスティングサービスの内容等詳細については下記のとおりとする。

①立地条件

東京都内もしくは隣接する県内であること。ただし、離島部を除く。

②設備条件

ア　耐震・免震性に優れた構造物で、震度７程度の地震にも耐えうる建設構造物であること。

イ　耐火設計構造であること。

ウ　電源は基幹の二重化による無停電対策を施し、自家発電設備あるいはUPS 設備を有すること。また、過電流対策を施すこと。

エ　空調設備が整備されており、室内温度・湿度が適正に管理されていること。

オ　消防設備は非水系消火設備をサーバ室に整備し、付属施設には消火栓など消防設備を整備していること。

カ　防水対策・漏水対策等の水害対策設備が整備されていること。

キ　通信設備

(ｱ)インターネット回線は100Mbps 以上のベストエフォートのものを提供すること。

(ｲ)IP アドレスは1 つ以上用意すること。

ク　防犯対策として、敷地内の通門管理、施設への入館管理、サーバ設置フロアへの入室管理、ラック開閉管理、サーバ操作管理がなされていること。

ケ　サーバ等の設置に際し、ラックへの収納や耐震ベルト・セキュリティーワイヤーの装備など、転倒防止策や持ち出し禁止策がとられていること。また、他顧客のサーバ担当者等が誤って操作しないよう、施錠管理などの対策を施すこと。

コ　パフォーマンス対策

サーバは、利用するユーザが快適にアクセスできるよう、十分な処理能力を有する占有環境とすること。また、急なトラフィック増等に対応し、CPU、メモリ、ディスク容量等のリソース追加に柔軟に対応できる環境とすること。

サ　共用サーバ（バックアップサーバ）の運用

専用サーバに重大な障害が生じた場合に備えて、バックアップを取得するための領域を確保するため、共用サーバ（バックアップサーバ）を運用すること。また、専用サーバ及び共用サーバ間でデータ同期を行うこと。

③運営管理条件

ア　サーバは24時間365日リモート監視が行われており、非常時には迅速な対応を図れること。

イ　運営内容

(ｱ)15 分毎以上の頻度でPing、http 確認監視を行うこと。

(ｲ)サーバ起動、終了、再起動を必要に応じて行い，リブート処理の処理結果を確認すること。

(ｳ)http、postgreSQL、Postfixの起動・再起動を必要に応じて行い、起動後の処理結果を確認すること。

(ｴ)障害時一時対応(通知、対応切り分け連絡)を行うこと。

(ｵ)監視周期15 分毎以上のログ監視を行うこと。

(ｶ)サービスレベルダウン及び障害を未然に防ぐアプリケーション監視等を行うこと。

(ｷ)サーバに不正侵入が発生した場合、警告メールを発信すること。

ウ　ＯＳ及びソフトウェアに重大なセキュリティホールが発見された場合、パッチ適用作業を行うこと。

エ　その他、盗聴・改ざん、攻撃等のリスクに関する情報を収集し、適宜対策を実施すること。

オ　サーバの運用維持に必要な定期保守を、委託者と協議の上適宜行うこと。
（四半期に１回以上）

カ　各種作業実施にあたっては、２人以上で実施し、作業ミスを防止すること。また、作業完了後は正常稼動の確認を行い、確認方法及び結果について委託者に報告すること。

キ　システム管理記録（保守作業記録等）、障害記録を作成し保管すること。また、委託者の求めに応じ、記録の提示及び内容説明を行うこと。

ク　時刻を保持する装置等については、正確な時刻を保つ対策を施すこと。

ケ　各種アクセスログ及び情報セキュリティの確保に必要な情報等の記録は3 か月間保持し、委託者の求めに応じて提出すること。また、窃取、改ざん及び誤消去等がなされないよう適切な対策を施すこと。

コ　サーバ及び本システムの運営管理を安全かつ安定した状態で運営するための体制を整えること。連絡及び対応時間は以下のとおりとする。

(ｱ)連絡先

連絡は、原則電話又はメールにて行う。システム担当者の電話番号・メールアドレスを提示し、連絡不可の状態を避けること。

(ｲ)対応時間

問い合わせは、原則として平日午前9 時から午後5 時まで対応可能であること。

④回線

本システムで使用するインターネット回線に係る仕様を以下に示す。

ア　DNSサーバを導入し、独自ドメイン（未定）を使用可能にすること。また、セカンダリDNSサーバを用意すること。DNS サービスはホスティングサービスを使用する。

イ　IPアドレス付与をはじめとした新規インターネット環境を構築する際に必要となる手続き等の初期費用も含む形とする。

■回線仕様

・帯域： 100Mbps 以上(ベストエフォート型)の帯域
・コンシューマ向けの回線と比べ、品質・信頼性の面で優れていること。
・故障時の復旧対応が24 時間サポートであること。
・固定IP アドレスが1 つ以上取得できること。

■DNS ホスティング仕様

・ホスティングサーバは1(1)②の条件を満たす、高水準のデータセンター内に設置され、機密性・安全性の面で優れていること。
・高い実績のあるサービスであること。
・設定の変更が容易に可能であること。

■ファイアウォール仕様

・本システムの使用に耐えうる処理能力を有するもの(100Mbps 以上)
・100～200 件程度の同時アクセスが可能であること。
・DoS/DDoS をはじめとしたサーバ攻撃並びに進入に対応する機能を有すること。
・IPアドレスによるパケットフィルタリング等の機能を提供すること。

3　セキュリティ対策等

（1）サーバは、ウィルス対策ソフトを導入し、加えて以下のいずれかのセキュリティ対策を講

じること。導入前に各対策を提案し、委託者の承認を得ること。

① 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か、IPS（不正侵入防御システム）を導入すること。

② 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。

（２）Webサイトの改ざん検知を行うこと。

（３）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。

（４）ウェブサイトに対する不正アクセスを防止するため、SQLインジェクション等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。