【別紙２】

機能要件書

平成３０年４月１６日
小田原市

1　基本事項

次に掲げる事項を基本方針としてシステムの調達を行い、セキュリティ対策、本市職員の作業負担の軽減策等を講じ、業務継続性のある安定的かつ効率的な運用の実現を目指す。

(1)　作業負担の軽減

安全かつ最適な導入スケジュールを計画・立案し、データ登録等をできるかぎり作業負担の軽減ができる方法により実現する。

(2)　低廉及び効率的なシステムの導入

ア　本市の職員規模、端末の運用実績等を考慮し、システム利用期間中の円滑な運用を可能とする性能を最適なシステムを構築する。

イ　システムの導入費用のみでなく、運用管理経費を含めた総コストの低廉化を図る。

2　契約期間

平成３０年１０月１日から平成３５年９月３０日まで

3　二要素認証システム要件

(1)　二要素認証システムを利用する職員数・クライアント端末数

ア　Windows アカウント数　　８００ユーザ（うち２５ユーザは共有ユーザとして利用）

イ　IC カード数　　８００枚（FeliCa Lite カードを職員証として利用）

ウ　職員数　　８００人

エ　クライアント端末数　　３７０台

オ　クライアント端末オペレーティングシステム（以下、「OS」という。）

Windows7 enterprise(x64)、Windows7 professional、Windows7 professional(x64)
Windows8.1 pro(x64)、Windows 10 pro バージョン 1511、Windows10 pro(x64)
バージョン 1607、バージョン 1703

(2)　調達範囲

ア　生体情報認証装置　370 台

イ　IC カードリーダ　370 台

ウ　生体情報認証クライアントライセンス　370 台分

エ　生体情報認証管理サーバ等のハードウェア一式

オ　生体情報認証システムの稼動に必要なソフトウェア一式

カ　上記エのハードウェア一式をデータセンター(以下、「DC」という。)に設置する場合、本市と DC 間の回線

(3)　機能要件

ア　生体情報認証装置及び IC カード認証装置

(1)既設端末の USB インターフェース（USB2.0 準拠）にて外付け接続可能であり、接続可能な端末は、特定のベンダー、製品に依存しないこと。

(2)生体情報認証装置及び IC カード認証装置の本体に情報を保持しないこと。

イ　生体情報認証方式

(ｱ)静脈認証方式とする。(体表情報を用いるものは、対象外とする)

(ｲ)本市の個人番号利用事務系ドメイン環境下の端末 370 台を導入対象とする。

ウ　生体情報登録

(ｱ)事故や疾病、怪我等により認証に用いる部位の損失等に対する代替手段を考慮し、1 ユーザにつき異なる 2 箇所以上の生体情報を登録できること。(１：１認証)

(ｲ)アカウント、利用者情報等の一括登録機能等、効率的な登録が可能であること。

エ　生体認証精度

(ｱ)本人拒否率（FFR)：0.01％以下のとき、他人受入率（FAR)：0.001％以下を満たすこと。

(ｲ)肌表面の状態（乾燥、肌荒れ、水分付着など）にほぼ影響されずに生体情報認証が行えること。

(ｳ)成長等による認証に用いる部位の変化に影響を受けないこと。

(ｴ)万人不同性が証明されており、一卵性の双子の場合でも認証可能であること。

(ｵ)生体情報認証装置本体を接続している端末にて認証の判別結果を判別できること。

オ　ユーザ情報の登録

(ｱ)本システムの本稼動開始時や人事異動の際の大規模な新規登録および情報変更に対応するために、生体情報以外のユーザ情報については、一括処理が可能なこと。

(ｲ)数名規模の都度登録に対応するために個別の登録ができること。

カ　ユーザ情報の管理

(ｱ)生体情報を含むユーザ情報は管理サーバに一括管理をすること。

(ｲ)安定運用や将来的な保守性の観点から、本市の既存システムにソフトウェアのインストール等一切手を加えることなく認証システムを導入可能なこと。

(ｳ)いつ、誰が、どのアカウントでログインしたかのログが出力できること。

(ｴ)管理者操作（ユーザ情報の操作等）についてもログの出力ができること。

キ　非常時の認証

(ｱ)緊急時における対応のため、生体情報認証を回避するログイン方法を有すること。

(ｲ)管理サーバやネットワークの障害などにより、クライアント端末から管理サーバへの接続が不可となっても、同一端末において本システムが最後に認証したユーザの認証は継続できること。また、認証の継続が可能な日数を設定できること。

ク　管理サーバ

冗長構成とすること。

コ　OS 要件

認証装置・ソフトウェアともに上記３.(１).オに記載する OS に対応していること。また後継の OS バージョンに対応すること。

(4)　ソフトウェア要件

ア　認証情報をサーバ上で一元管理するために必要なソフトウェアを準備すること。

イ　認証情報は、暗号化して取り扱うことが可能であること。
ウ　認証結果のログが管理サーバで一元的に取得可能であること。

(5)　設置場所

管理サーバは原則十分なセキュリティ対策が図られた日本国内の DC または市役所の本庁舎に設置するものとする。なお、DC に設置する場合は市と DC 間の回線は、LGWAN 回線または IP-VPN 回線の閉域網とすること。IP-VPN 回線を利用する場合は、その DC がインターネット回線に直接接続されないこと。

(6)　成果物

ア　利用者用手順書
(ｱ)初回利用時の手順
(ｲ)その他、利用する職員が運用に必要な手順
イ　管理者用手順書
(ｱ)ユーザ登録方法
(ｲ)カード紛失時等の緊急認証方法
(ｳ)ログの確認方法
(ｴ)その他、システム管理者が運用に必要な手順

4　ネットワーク監視システム要件

(1)　監視対象数

ア　ネットワーク機器（スイッチや無線 AP 等）　300 台
イ　サーバ機器　30 台

(2)　調達範囲

ア　管理サーバのハードウェア一式
イ　本市に設置する監視用クライアント端末　１台
OS は windows10 Pro、また Microsoft Office Professional 2016 を有すること。
ウ　監視に必要なソフトウェア一式
エ　上記アのハードウェア一式をデータセンター(以下、「DC」という。)に設置する場合、本市と DC 間の回線

(3)　機能要件

ア　監視対象の生存監視を行い、不通及び再通時にシステム管理者に電子メールにより通報する機能を有すること。
イ　対象機器ごとに監視が不要な時間帯についてはシステム管理者に通報しない仕組みを提供すること。
ウ　監視対象の変更や監視時間帯の設定については、システム管理者が容易に設定できる仕組みとすること。

エ　ネットワーク機器については通信量を取得し、過去1年間分を閲覧できるようにすること。また、特定のSNMPトラップについてシステム管理者に通報すること。

オ　監視対象となるネットワーク機器と時刻同期を行うこと。なお、時刻は小田原市の指定するサーバと同期すること。

カ　監視対象機器ごとに通信量、PING応答時間を監視し記録すること。

キ　上記カで得た監視結果を本市に設置する端末から確認できること。

ク　上記カの監視状況を本市に設置する端末からリアルタイムで確認できること。

ケ　本市ネットワークはインターネットから分離されているため、通報については本市が有するメール転送システム（MTA）に送信すること。

(4)　設置場所

管理サーバは原則十分なセキュリティ対策が図られた日本国内のDCまたは市役所の本庁舎に設置するものとする。なお、DCに設置する場合は市とDC間の回線は、LGWAN回線またはIP-VPN回線の閉域網とすること。IP-VPN回線を利用する場合は、そのDCがインターネット回線に直接接続されないこと。

(5)　成果物

手順書

ア　監視対象の変更（追加及び削除）方法

イ　監視時間帯の変更方法

ウ　通信量の確認方法

エ　その他、システム管理者が運用に必要な手順

5　LGWAN接続システム要件

(1)　現行利用機種

LGWAN接続ルータ　Cisco社製　CiscolSR892J

LGWANファイアウォール　FortiGate社製FortiGate 40c

(2)　調達範囲

LGWAN接続ルータ及びLGWANファイアウォール

(3)　機能要件

ア　以下の機能を備えていること。

(ｱ)LGWANへの接続機能

(ｲ)LGWAN接続用ファイアウォール機能

(ｳ)LGWAN通信のウイルスチェック機能

(ｴ)ログ保存機能

イ　現在、LGWANを利用し稼働している本市の各業務システムが遅延なく継続して利用できるようにすること。

ウ　上記アの各機能について第三者からの不正アクセスを防止するための適切な処置を行うこと。

エ　上記ア(ｱ)(ｲ)の機能について、冗長化構成（ホットスタンバイ）として構築し、機器に障害があった場合の切り替え手順を記載した手順書を提供すること。

オ　上記ア(ｲ)の機能について本市の依頼があった場合に設定変更を行うこと。

カ　上記ア(ｳ)の機能についてウイルスチェックのパターンファイルが最新を保つように設定すること。

キ　上記ア(ｴ)の機能について次の要件を満たす仕組みを提供すること。

(ｱ)上記ア(ｱ)～(ｳ)の各機能のログを収集する仕組み

(ｲ)発注者のドメイン管理サーバの監査ログを収集する仕組み

(ｳ)職員がメールを外部に送信した履歴の一部を庁内に公開する仕組み

ク　上記ア(ｴ)の機能で収集したログを５年間保存し、本市の求めに応じて随時提供すること。また、各機能の設定情報も同様に引き渡すこと。

ケ　上記アの機能に障害が発生した場合は速やかに発注者に報告すること。

コ　業務期間完了後、上記３の各機能で用いたデータを消去し、復元できないように処理すること。

(4)　設置場所

小田原市本庁舎３階サーバ室内

6　構築スケジュール

平成３０年１０月１日にそれぞれのシステムの本稼働とする。それまでに必要なシステムの構築、データセットアップ、成果物の納品、職員への研修等を完了させるものとする。ただし、提案するスケジュールにより、これを変更することができるものとする。

7　サポート体制

(1)　問い合わせ、相談等への迅速かつ適切な対応ができること。

(2)　本市と協議した内容については記録した上で、適宜、報告書を本市に提出すること。

(3)　構築したシステムの操作方法等について、職員に対し充分に研修を行う。なお、研修に使用する資料は受注者が用意すること。

(4)　ハードウェアの故障等に関しては、速やかに交換等故障復旧作業を行うこと。

8　個人情報保護・情報セキュリティ

(1)　十分な情報セキュリティ対策が講じられており、安全に使用することができる環境を用意すること。

(2)　本件業務の従事者（再委託先を含む。）に対する個人情報保護・情報セキュリティに関する指導、研修等が確実に講じられていること。

９　導入実績

他自治体への導入実績（特に本市と同程度又は同程度以上の規模の自治体への導入実績）が豊富であり、信頼性が高く、かつ多くのユーザから評価されているシステムであること。

１０　その他の追加提案

本機能要件書は、現在、本市が必要と考えている機能について示したものであり、システムの構築及び運用管理にあたっては、本機能要件書に記載されている要件等及び受注者からの提案内容に基づき、本件業務に係る詳細設計及び仕様を確定する。

したがって、本プロポーザルでは、本件業務の履行にあたって、将来的な技術革新、社会情勢の変化等も踏まえ、専門的な立場から、本市が要求する機能要件以外で導入すべき効果的な機能、運用方法等について、企画提案書において積極的に提案すること。

以上