資料５－２

総務省ＬＡＮシステムの更新整備及び運用管理業務

民間競争入札実施要項（案）

総務省大臣官房企画課情報システム室

【更新履歴】

No.	更新の概要	更新責任者	更新日付
1			
2			
3			
4			
5			
6			

目次

1　趣旨

「競争の導入による公共サービスの改革に関する法律」（平成 18 年法律第 51 号。以下「法」という。）に基づく競争の導入による公共サービスの改革については、公共サービスによる利益を享受する国民の立場に立って、公共サービスの全般について不断の見直しを行い、その実施について、透明かつ公正な競争の下で民間事業者の創意と工夫を適切に反映させることにより、国民のため、より良質かつ低廉な公共サービスを実現することを目指すものである。

上記を踏まえ、総務省は、「公共サービス改革基本方針」（平成 23 年 7 月 15 日閣議決定）別表において民間競争入札の対象として選定された「総務省ＬＡＮシステムの更新整備及び運用管理業務」（以下「総務省ＬＡＮ構築等請負業務」という。）について、公共サービス改革基本方針に従って、本実施要項を定めるものとする。

２　総務省ＬＡＮの構築等請負業務の詳細な内容及びその実施に当たり確保されるべき対象公共サービスの質に関する事項

（１）総務省ＬＡＮの構築等請負業務の業務内容

ア　総務省ＬＡＮの概要

総務省においては、「総務省情報ネットワーク（共通システム）最適化計画」（平成 17 年６月 29 日総務省行政情報化推進委員会決定平成 23 年８月 26 日改定）に基づき、総務省職員が行政の組織活動を実施するための基盤システムとなる「総務省ネットワーク基盤（ＬＡＮ）」（以下「総務省ＬＡＮ」という。）を整備し、平成 21 年度には総務省全体のＬＡＮを完全統合（旧総務庁、旧郵政省、旧自治省の９のＬＡＮ）するなど、最適化に取り組んできている。

現行の総務省ＬＡＮは、第３期システムとして平成 24 年度に構築、平成 28 年度まで運用することとしており、次期総務省ＬＡＮは平成 28 年度に設計・構築し、平成 29 年度から運用開始する必要がある。

イ　次期総務省ＬＡＮの整備方針

次期総務省ＬＡＮでは、「経済財政運営と改革の基本方針 2015」（平成 27 年６月閣議決定）、「『日本再興戦略』改訂 2015」（平成 27 年６月閣議決定）、「世界最先端ＩＴ国家創造宣言」（平成 25 年 6 月閣議決定、平成 27 年 6 月変更閣議決定）、「首都直下地震緊急対策推進基本計画」（平成 27 年３月閣議決定）や「サイバーセキュリティ戦略」（平成 27 年９月閣議決定）等の政府方針に基づき、サイバーセキュリティ対応能力及び基盤の強化を図るとともに、行政のＩＴ化と業務改革、働き方改革の実行・実現を推進するための基盤環境の整備や情報システムの事業継続性を向上し、安全性と信頼性を確保するための業務継続性を考慮したディザスタリカバリサイト（以下「ＤＲサイト」という。）の整備を図ることが急務となっている。

ウ　総務省ＬＡＮの提供する機能等

総務省ネットワーク基盤は、総務省職員であるユーザ（以下「ユーザ」という。）がＬＡＮ端末等を用いて電子メールや電子掲示板、ファイル共有等の職員向けサービスを提供するとともに、高い安定性と安全性を同時に実現し、信頼性の高い基盤機能を提供するものである。

次期総務省ＬＡＮの提供する機能等を図２-１　次期総務省ＬＡＮが提供する機能等の概要、表２-１　次期総務省ＬＡＮが提供する機能等の概要一覧に示す。

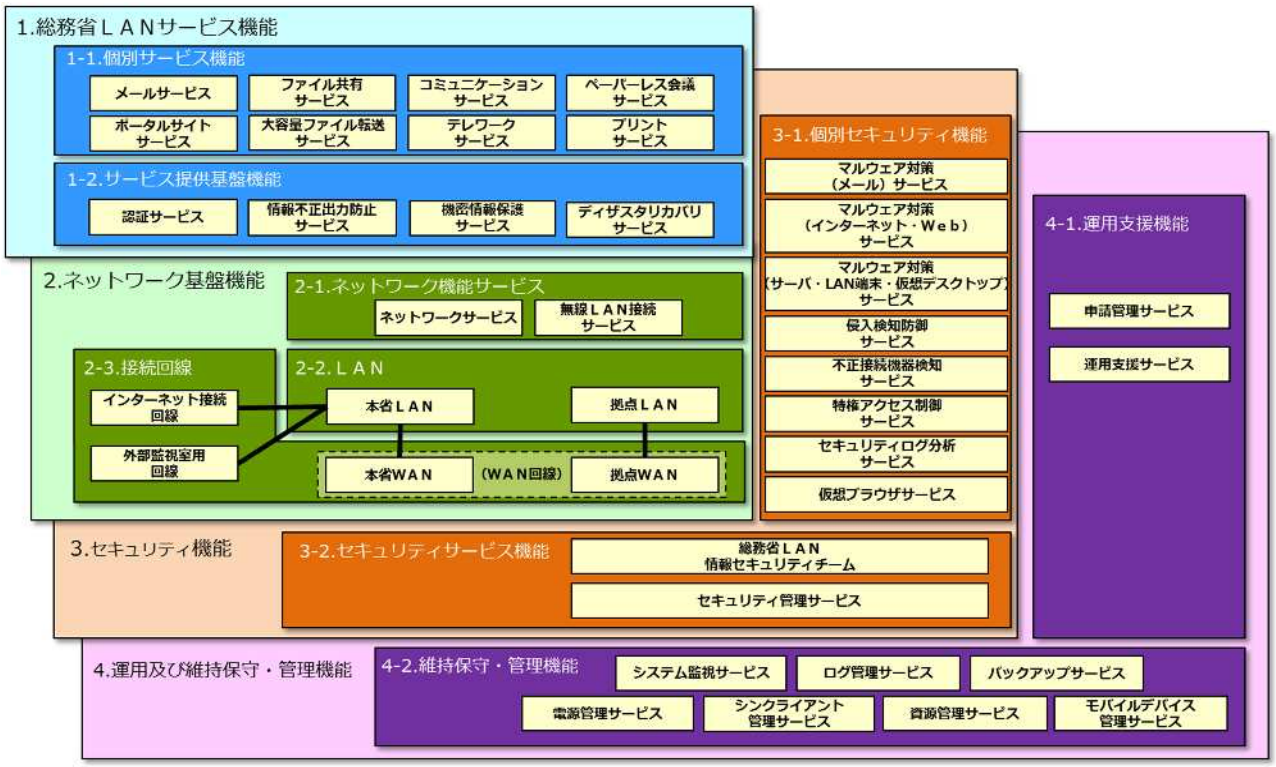


図２-１　次期総務省ＬＡＮが提供する機能等の概要

表２-１　次期総務省ＬＡＮが提供する機能等の概要一覧

機能等の名称	機能等の概要
１．総務省ＬＡＮサービス機能	
１－１．個別サービス機能	
メールサービス	総務省職員が省内外との連絡手段として電子メールを用いるため、メールサービスを提供する。
ポータルサイトサービス	総務省職員が円滑に業務を遂行するため、ポータルサイトサービス（電子掲示板、電子会議室、設備予約、アンケート、スケジューラ、幹部出退表示等）を提供する。
ファイル共有サービス	総務省職員間で電子データを共有・活用し、円滑に業務を進めるため、ファイル共有サービスを提供する。
大容量ファイル転送サービス	総務省職員と省外の関係者間で安全に情報を交換するため、大容量ファイル共有サービスを提供する。
コミュニケーションサービス	メッセージの送受信・在席管理・Ｗｅｂ会議等を用いてコミュニケーションを円滑にし、ワークスタイル変革を推進するため、コミュニケーションサービスを提供する。
テレワークサービス	総務省職員の多様で柔軟な働き方を可能にし、ワーク・ライフ・バランスを推進するため、テレワークサービスを提供する。
ペーパーレス会議サービス	会議室内での電子データの資料共有・閲覧を可能にし、業務効率を向上させるため、ペーパーレス会議システムサービスを提供する。

機能等の名称	機能等の概要
プリントサービス	電子データを紙資料として印刷する際、不用意な印刷による情報の漏えいを防ぐため、認証機能を有するプリントサービスを提供する。
１－２．サービス提供基盤機能	
認証サービス	総務省職員のアカウント情報を一元管理し、各サービス利用時の認証及びアクセス権の付与を行うため、認証サービスを提供する。
情報不正出力防止サービス	電磁的記憶媒体による総務省ＬＡＮ外部への電子データ入出力を制限することで情報の不正出力を防止するため、情報不正出力防止サービスを提供する。
機密情報保護サービス	暗号化専用フォルダへファイルを保存することで自動的に暗号化し、機密性の高い情報の流出を防止するため、機密情報保護サービスを提供する。
ディザスタリカバリサービス	大規模災害の発生等により本省から提供されるサービスが停止した際に、ＤＲサイトで総務省ＬＡＮの主要サービスを提供し、業務継続性を確保するため、ディザスタリカバリサービスを提供する。
２．ネットワーク基盤機能	
２－１．ネットワーク機能サービス	
ネットワークサービス	総務省職員がネットワークを介した各種サービス（ＤＨＣＰ、ＤＮＳ、ＮＴＰ、プロキシ、負荷分散装置等）を利用するため、ネットワークサービスを提供する。
無線ＬＡＮ接続サービス	端末の設置場所を固定せず、利用場所にとらわれないネットワーク接続環境を実現するため、無線ＬＡＮ接続サービスを提供する。
２－２．ＬＡＮ	
本省ＬＡＮ	総務省ＬＡＮ全体にネットワークサービスを提供し、総務省職員が総務省ＬＡＮサービスを利用するため、本省ＬＡＮを提供する。
拠点ＬＡＮ	総務省職員が外部拠点、地方支分部局の各拠点において総務省ＬＡＮサービスを利用するため、拠点ＬＡＮを提供する。
２－３．接続回線	
インターネット接続回線	総務省職員が行政事務を遂行する際の情報収集及び情報交換を行うため、インターネット接続回線を提供する。
本省ＷＡＮ	本省、外部拠点、地方支分部局の各拠点及びＤＲサイトで相互に通信を行うため、本省ＷＡＮ（本省側における総務省ＷＡＮへの接続回線）を提供する。
拠点ＷＡＮ	本省、外部拠点、地方支分部局の各拠点及びＤＲサイトで相互に通信を行うため、拠点ＷＡＮ（拠点側における総務省ＷＡＮへの接続回線）を提供する。
外部監視室用回線	構築や移行の際、外部に設置した機器と本省に設置した機器間で必要なデータの転送を行うため、外部監視室用回線を提供する。
３．セキュリティ機能	
３－１．個別セキュリティ機能	
マルウェア対策（メール）サービス	メールを侵入経路とするマルウェア等の侵入を早期に検知・駆除するため、マルウェア対策（メール）サービスを提供する。
マルウェア対策（インターネット・Ｗｅｂ）サービス	インターネットを介したＷｅｂ閲覧を侵入経路とするマルウェアの侵入を早期に検知・駆除するため、マルウェア対策（インターネット・Ｗｅｂ）サービスを提供する。

機能等の名称	機能等の概要
マルウェア対策（サーバ・ＬＡＮ端末・仮想デスクトップ）サービス	サーバ、ＬＡＮ端末及び仮想デスクトップにマルウェアが侵入した際、早期に検知・駆除するため、マルウェア対策（サーバ・ＬＡＮ端末・仮想デスクトップ）サービスを提供する。
侵入検知防御サービス	インターネット及び政府共通ネットワークから省内への不正侵入を防ぐため、侵入検知防御サービスを提供する。
不正接続機器検知サービス	総務省ＬＡＮに不正に接続された端末等による情報漏えいの防止や、ウイルス感染から保護するため、不正接続機器検知サービスを提供する。
特権アクセス制御サービス	機器に対する不正な管理操作を防止するため、特権アクセス制御サービスを提供する。
セキュリティログ分析サービス	ゼロデイ攻撃の回避や、検知回避技術を活用した攻撃を早期に検知するため、セキュリティログ分析サービスを提供する。
仮想ブラウザサービス	マルウェアが直接ＬＡＮ端末に侵入するリスクを低減するために、総務省職員がインターネットへの Web アクセスを行う専用ブラウザ環境として、仮想ブラウザサービスを提供する。
３－２．セキュリティサービス機能	
総務省ＬＡＮ情報セキュリティチーム	政府全体の動向及び総務省の状況を反映し、専門的な知見をもってセキュリティ対策に当たるため、総務省ＬＡＮ情報セキュリティチームにより対応する。
セキュリティ管理サービス	ＯＳやミドルウェアに潜むぜい弱性や運用におけるセキュリティの問題等を検証・評価するため、セキュリティ管理サービスを提供する。
４．運用及び維持保守・管理機能	
４－１．運用支援機能	
申請管理サービス	ヘルプデスクで処理する各種申請の運用負荷を軽減するため、申請管理サービスを提供する。
運用支援サービス	総務省ＬＡＮに関する問い合わせを一元管理し、進捗状況の確認や問題の分析を可能とするため、運用支援サービスを提供する。
４－２．維持保守・管理機能	
システム監視サービス	管理対象機器の障害等を迅速に検知しシステムの可用性を維持する。また、定型的な業務を自動化することで運用負荷を軽減するため、システム監視サービスを提供する。
ログ管理サービス	収集したログ（認証ログ、アクセスログ、セキュリティログ、利用状況ログ、ＬＡＮ端末の操作ログ等）について、迅速に検索、閲覧及び分析を可能とするため、ログ管理サービスを提供する。
バックアップサービス	障害発生、災害発生、操作ミス等によりファイルが消失又は破損した場合に当該ファイルの復旧を可能とするため、バックアップサービスを提供する。
電源管理サービス	電源障害・法定停電・災害時等に、電源の切断順序に依存関係のある機器を安全に停止するため、電源管理サービスを提供する。
資源管理サービス	不要なアプリケーションのインストール防止、不正な操作や設定等を禁止するため、資源管理サービスを提供する。
モバイルデバイス管理サービス	モバイルデバイスについて、不要なアプリケーションのインストール防止、不正な操作や設定等を禁止するため、モバイルデバイス管理サービスを提供する。
シンクライアント管理サービス	テレワークで利用するシンクライアントのイメージの管理、セットアップ処理を行うため、シンクライアント管理サービスを提供する。

エ　総務省ＬＡＮの構成概要

総務省ＬＡＮの概要図を図２-２　総務省ＬＡＮシステム概要図に示す。

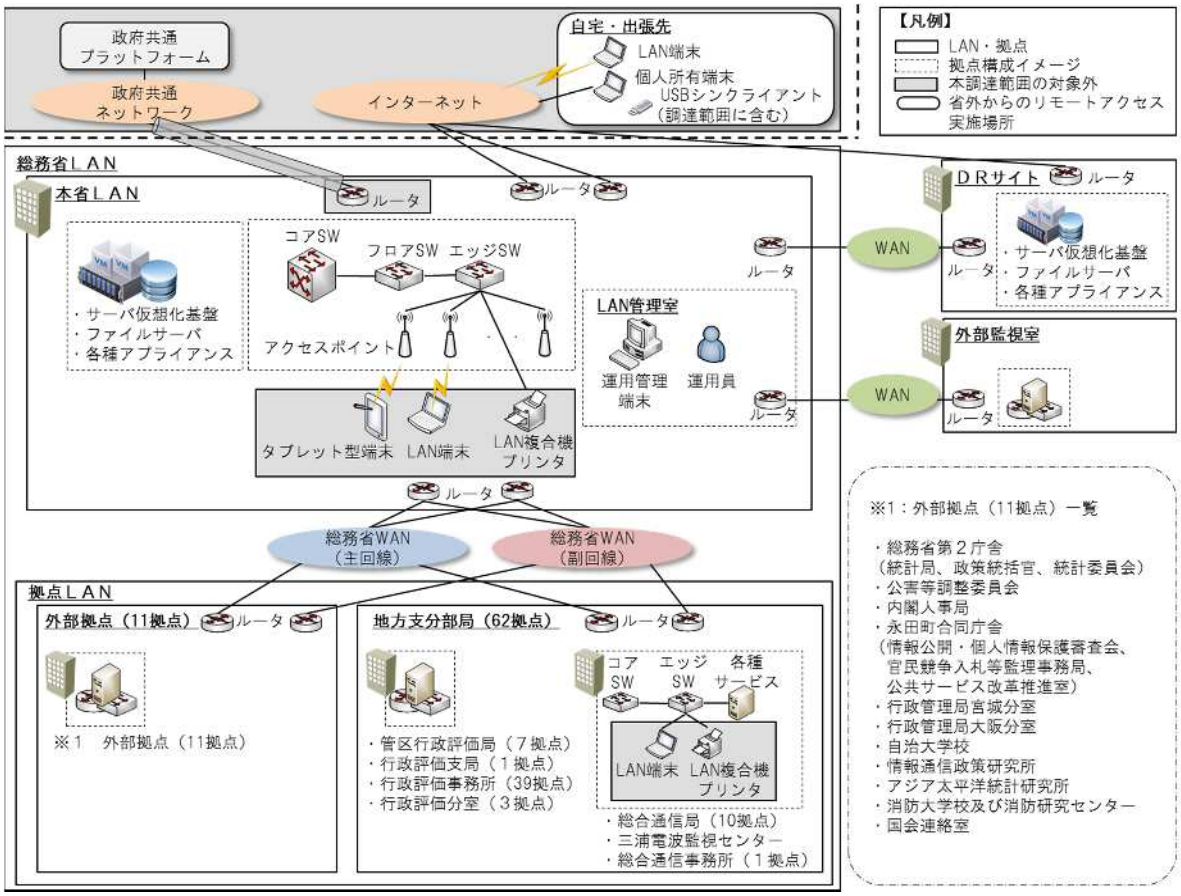


図２-２　総務省ＬＡＮシステム概要図

各構成要素の概要を以下に示す。

（ア）本省ＬＡＮ

本省ＬＡＮは、職員向けサービスである電子メールや電子掲示板、ファイル共有サーバ、Ｗｅｂ会議やテレワーク等のサービスを提供するとともに、それらサービスを利用するためのＬＡＮ基盤を提供する。

職員向けサービスは、主に本省に設置されるサーバ・ストレージ機器、情報セキュリティ対策機器及びＬＡＮ基盤を構成するためのネットワーク機器により提供される。また、政府共通ネットワーク（以下「政府共通NW」という。）やインターネットへの接続、政府共通NWを経由した政府共通プラットフォーム（以下「政府共通ＰＦ」という。）や府省共通システムへの接続機能を提供する。

（イ）拠点ＬＡＮ

拠点ＬＡＮは、主に本省ＬＡＮに整備された職員向けサービスを利用するために外部拠点、地方支分部局に構築され、各拠点のＬＡＮ基盤を提供する。

（ウ）外部拠点

外部拠点は、都内にある総務省第２庁舎（統計局、政策統括官、統計委員会）、公害等調整委員会、内閣人事局、永田町合同庁舎（情報公開・個人情報保護審査会、官民競争入札等監理事務局、公共サービス改革推進室）、行政管理局宮城分室、行政管理局大阪分室、自治大学校、情報通信政策研究所、アジア太平洋統計研修所、消防大学校及び消防研究センター、国会連絡室の 11 拠点を指す。

（注）平成 28 年 4 月に内閣官房・内閣府の組織の見直しで編入予定の拠点を含む。このうち、永田町合同庁舎の配置組織は現時点の情報であり、変更されることがある。

（エ）地方支分部局

地方支分部局は、全国に点在する総合通信局、総合通信事務所、管区行政評価（支）局、行政評価事務所及び行政評価分室の 62 拠点を指す。

（オ）ディザスタリカバリサイト

ディザスタリカバリサイト（以下「ＤＲサイト」という。）は、大規模災害等の有事や障害時の際に総務省ＬＡＮの提供するサービスの一部を代替して提供し、かつ、総務省ＬＡＮの設定情報や職員の作成する電子データをバックアップする機能を有する拠点を指す。

（カ）総務省ＷＡＮ

総務省ＷＡＮは、本省ＬＡＮと拠点ＬＡＮを相互に接続するための広域ネットワークを指す。

（キ）外部監視室

運用業務時間外等、総務省ＬＡＮをリモート監視するための施設を指す。次期総務省ＬＡＮに移行する際、本省に設置するサーバ等の機器を一時的に収容し、構築・試験・運用を行う施設としても利用する。

オ　総務省ＬＡＮの特性

（ア）システム規模

総務省ＬＡＮは、ユーザにより、原則として 24 時間 365 日利用されるシステムである。ユーザアカウント数、クライアント端末数及び拠点数を以下に示す。

（平成 27 年 7 月現在）

ユーザアカウント数		約 16,000 個
	ユーザアカウント数	約 7,000 個
	非ユーザアカウント数 （共有メールアカウント、動作確認用アカウント等）	約 5,000 個
	一時保管アカウント	約 4,000 個
クライアント端末数		約 7,000 台
拠点数	外部拠点	11 拠点
	地方支分部局	62 拠点
	ＤＲサイト	１拠点
	外部監視室	１拠点

（イ）安定性と信頼性

総務省ＬＡＮは、ユーザが業務を円滑に行うためのシステム基盤であり、高い安定性と信頼性が同時に求められる。

（ウ）情報セキュリティ

総務省ＬＡＮは、ユーザが業務を行うに当たり、要機密情報、要保全情報及び要安定情報を取り扱う必要があることから、高い安全性が求められるため、各種ガイドライン等に基づいた情報セキュリティ対策の導入を基本とし、更なる安全性を高めるための対策が求められる。

カ　構築等請負業務の内容

次期総務省ＬＡＮの構築等請負業務は、①総務省ＬＡＮの設計・構築を行う更新整備業務、②システムの稼働状態を維持し機能維持や品質維持等設計された仕様どおりにシステムを動作させることを目的とした運用及び維持保守・管理等のシステム維持業務であり、その詳細は、別添１「総務省ＬＡＮ構築等請負　調達仕様書」に従うものとする。

（ア）統制作業

請負者は、総務省ＬＡＮ構築等請負業務全体に係る作業管理、進捗管理、変更管理、リスク管理、課題管理、品質管理、各種技術支援、報告支援等を行う。

（イ）設計・構築

請負者は、総務省ＬＡＮ構築等請負業務のうち設計・構築業務について、調達仕様書、提案書に基づき、設計・構築実施計画書及び設計・構築実施要領を作成し、主管課の承認を得る。

請負者は、設計・構築の開始前に、主管課、工程管理支援事業者、ＰＭＯ等と調整し、調達時の請負者の提案内容等を踏まえ、「政府情報システムの整備及び管理に関する標準ガイドライン」（平成 26 年 12 月３日各府省情報化統括責任者（ＣＩＯ）連絡会議決定。以下「標準ガイドライン」という。）に基づく第二

次工程レビューを受け、要件を確定する。

請負者は、承認された設計・構築実施計画書及び設計・構築実施要領に基づき、設計、構築、試験、受入試験の実施支援、移行及び教育訓練を実施する。各作業の概要を表２-２　設計・構築作業の概要に示す。

表２-２　設計・構築作業の概要

作業	概要
設計・構築実施計画書等の作成	「プロジェクト計画書」及び「プロジェクト管理要領」と整合をとりつつ、主管課の指示に基づき、工程管理支援事業者と調整の上、「設計・構築実施計画書」及び「設計・構築実施要領」を作成し、主管課の承認を受ける。
設計	入札公告時の調達仕様書及び要件定義書に対して、主管課の合意のもと、調達時の請負者の提案内容に基づき変更を行い、ＰＭＯによる第二次工程レビューを受け、要件定義書を確定させる。 確定された要件を実現するために必要となる設計を行い、基本設計書、詳細設計書、ファシリティ設計書及び回線導入計画書等を作成し、主管課の承認を得る。
構築	設計作業において作成された設計書や計画書等に基づき、機器等について、稼働に必要なソフトウェア製品のインストールや設定を実施し、所定の場所へ搬入の上、設置調整等の構築作業を実施する。
試験	試験実施計画書、試験仕様書を作成し、主管課の承認を得た上で、構築したシステムが全ての要件を満たすことを請負者自ら確認し、試験結果報告書により報告する。
受入試験の実施支援	受入試験実施計画書、受入試験仕様書を作成し、主管課に提示する。 承認を得た受入試験実施計画書、受入試験仕様書に基づき、主管課が実施する受入試験の実施を支援する。
移行	移行実施計画書、展開実施計画書等を作成し、計画の妥当性について主管課の承認を得た上で、同計画書に基づく具体的な作業内容、移行判定項目や移行判定基準、不具合が発生した際の切戻し手順等を記載した移行設計書、移行手順書等を作成する。 移行手順書等に基づき、総務省ＬＡＮの安全かつ確実な移行を行い、その結果について報告する。
教育訓練	教育訓練実施計画書、教育訓練教材を作成し、主管課の承認を得た上で、部局運用担当者、主管課に教育訓練を実施する。 ユーザ向けには、教育訓練教材をポータルサイトに公開する。

（ウ）運用及び維持保守・管理

請負者は、総務省ＬＡＮ構築等請負業務のうち運用及び維持保守・管理業務について、第二次工程レビューで確定した要件に基づき、サービスレベル合意書（以下「ＳＬＡ」という。）（案）、運用・保守要領（案）、運用・保守実施計画書を作成し、主管課の承認を得る。

請負者は、承認された運用・保守実施計画書に基づき、運用及び維持保守・管理業務を実施する。また、総務省の重要通信基盤システムである総務省ＬＡＮにおける当該業務は、システムの機能及び品質の維持等情報システムを設計仕様どおりに動作させることを目的とした維持保守業務が主となるため、請負者内で設計・構築に携わった要員と密接に連携し、対応を行う。申請業務対応及び運用支援業務について、その対応を行う。運用及び維持保守・管理業務の内容について、よりシステムの安全性を高め、効率的な業務が実施できるよう運用改善を行う。なお、申請業務対応のうち例外申請に係る受付及び内容審査は、主管課が行う。

各作業の概要を表２-３　運用及び維持保守・管理作業の概要に示す。

表２-３　運用及び維持保守・管理作業の概要

作業	概要
運用・保守要領等の作成	運用を開始するに当たり、運用・保守を行う上での指針・基準となる項目を記載した「運用・保守要領」、具体的な作業内容や実施時間、実施サイクル等に関する内容を取りまとめた「運用・保守実施計画書」を作成する。 また、運用及び維持保守・管理期間中に計画的に発生する作業内容、想定される発生時期等を取りまとめた中長期運用・保守作業計画を作成する。なお、中長期運用・保守作業計画には、総務省ＬＡＮのライフサイクルを通じた運用及び維持保守・管理に係る作業の内容を記載する。
平常時対応	運用・保守実施計画書に基づき、対象となる機器等や監視等の方法を記載した運用・保守設計書、操作手順や解説等を記載した運用・保守手順書を作成し、運用及び維持保守・管理業務を行う。
申請業務対応	総務省ＬＡＮ運用管理規程に基づく約 30 種類の申請書について、その受付、内容確認、対応等を行う。また、これら手続のうち、誤って削除したファイルの復旧や権限設定の変更等例外的な申請については、主管課がその受付及び審査を担当する。
運用支援業務	職員からの電話照会を一元的に受付・管理及び対応を行うヘルプデスク業務を行う。また、その進捗状況の確認や問題の分析を行うため、各種集計業務を行う。各種集計業務は、継続的な改善により自動化がなされるなど効率的に行う。

作業	概要
障害発生時対応	総務省ＬＡＮに障害や不具合等が発生又は発生が予測される場合や情報セキュリティに係る事故が疑われる場合には、速やかに主管課に報告するとともに、その緊急度及び影響度を判断の上、適切な一次対応を行う。一次対応を行った後、原因調査、復旧措置、確認作業を行い、一連の作業の報告書を作成し、主管課に報告する。
情報システムの現況確認支援	年１回、主管課の指示に基づき、ＯＤＢ格納データと情報システムの現況との突合・確認（以下「現況確認」という。）の実施を支援する。現況確認の結果、ＯＤＢの格納データと情報システムの現況との間の差異がみられる場合は、「運用・保守要領」に定める変更管理方法に従い、差異を解消する。また、ライセンス許諾条件が合致しない場合や、サポート切れのソフトウェア製品の仕様が明らかになった場合は、当該条件への適合可否や更新の可否、条件等について、更新した場合の影響の有無を含め、主管課に報告する。
主管課等支援業務	総務省ＬＡＮへの接続、政府共通ＰＦへの移行等、主管課、部局担当者等からの各種照会に対し、要望確認のためのヒアリング等を実施し、適宜技術的観点からの支援を行う。
構成管理	総務省ＬＡＮ全体の構成、各機器等の設定やインストールされているソフトウェア製品とそのバージョン及びライセンス、ＩＰアドレスの割当などの構成情報を最新の状態に管理する。
変更管理	構成管理を行う情報に変更がある場合には、必要性や変更した場合の影響等を精査し、主管課に変更の承認を得た上で作業を実施する。
現況管理	サーバのＣＰＵや通信回線の性能管理、サーバやストレージ等のディスク容量、通信回線の利用率、システムの設定情報やユーザの作成した電子ファイル等のバックアップなどに係る資源管理を行う。
情報セキュリティ管理	ウイルスやマルウェア等への感染、不正アクセス等の有無についての監視を行う。監視の結果、情報セキュリティに影響する事象が確認又は疑われる場合には、関連する機器等のログを収集し、相互分析・調査を行い、速やかに必要な措置を行う。また、脆弱性情報に基づいたセキュリティパッチの適用を行う。
ＳＬＡ管理	ＳＬＡに基づく達成率の確認、傾向分析、未達成が継続した場合の改善策等、サービスレベルの維持・改善に向けた管理を行う。
定期報告	システムの操作や監視状況、障害発生・対応の状況、サービス指標の実績値等を日次、週次、月次及び年次で適宜報告する。

作業	概要
運用及び維持保守・管理業務の改善提案	日次、週次、月次及び年次で報告される運用及び維持保守・管理業務の内容について、請負者の知見を活かし、よりシステムの安全性を高め、かつ、より効率的な業務を実施するために有益と考えられる提案を積極的に行う。

（２）本請負業務の引継ぎ

ア　現行請負者からの引継ぎ

総務省は、当該引継ぎが円滑に実施されるよう、現行請負者及び本請負者に対して必要な措置を講ずるとともに、引継ぎが完了したことを確認する。本業務を新たに実施することとなった請負者は、本業務の開始日までに、業務内容を明らかにした書類等により、現行請負者から業務の引継ぎを受けるものとする。なお、その際の引継ぎに必要となる経費は、現行請負者の負担とすること。

イ　本請負期間満了の際の引継ぎ

総務省は、当該引継ぎが円滑に実施されるよう、本請負者及び次回請負者に対して必要な措置を講ずるとともに、引継ぎが完了したことを確認する。

本業務の請負期間満了の際には、本請負者は、次回業務の開始日までに、業務内容を明らかにした書類等により、次回請負者に対し、引継ぎを行うものとする。引継ぎが円滑に実施されなかったことにより次回請負業務の遂行に支障が出た場合には、改善されるまで支援を行うこと。なお、その際の引継ぎに必要となる経費は、本請負者の負担とすること。

（３）確保されるべき対象業務の質

本業務は、「総務省設置法」（平成 11 年法律第 91 号）第４条に規定された総務省の所管事務を円滑に遂行するための情報基盤を更新整備するものであるため、総務省ＬＡＮの利用者への継続的、かつ、安定的なサービスの円滑な提供に資するものである必要がある。このため、上記「２（１）総務省ＬＡＮの構築等請負業務の業務内容」に示した業務を実施するに当たり、請負者が確保すべき対象業務の質は、次のとおりとする。

ア　対象業務内容

「２（１）カ　構築等請負業務の内容」に示す運用及び維持保守・管理業務について、以下に示す水準以上の質を確保すること。

イ　総務省ＬＡＮの稼働率

稼働率は、99.90%以上とする。ただし、拠点のプリントサービス、ファイル共有サービス及びコミュニケーションサービス、ディザスタリカバリサービス、運用管理サービス並びに無線ＬＡＮ接続サービスは稼働率を 99.00%以上とする。稼働率は以下の計算式で計算する。

総務省ＬＡＮの稼働率（%）
=｛1 - （a÷b）｝×100

ａ：１か月の停止時間
ｂ：１か月の稼働予定時間
※１か月の稼働予定時間＝（24 時間×１か月の日数）-計画停電等により停止する時間（ただし、拠点の各種サービスにおいては、１か月の稼働予定時間は、（８時間×１か月のうち、開庁日の日数）-計画停電等により停止する時間）

なお、本サービスの運用及び維持保守・管理業務を実施しなければならない時間は、調達仕様書の記載のとおりとする。

ウ　セキュリティ上の重大障害

個人情報、施設等に関する情報その他の契約履行に際し知り得た情報漏えいの件数は０件であること。

エ　システム運用上の重大障害の件数

長期にわたり正常に稼働できない事態、状況及び保有するデータの喪失等により、業務に多大な支障が生じるような重大障害の件数は０件であること。

オ　総務省ＬＡＮの利用に関する満足度アンケート調査結果

業務開始後、年に１回の割合で総務省ＬＡＮの利用に関して、部局運用担当者及び主管課に対して､次の項目の満足度についてアンケートを実施(回収率は 70%以上）し、その結果の基準スコア（75 点以上）を維持すること。

・問い合わせから回答までに要した時間
・回答又は手順に対する説明の分かりやすさ
・回答又は手順に対する結果の正確性
・担当者の対応（言葉遣い、親切さ、丁寧さ等）

各質問とも､「満足」(配点 100 点)､「ほぼ満足」(同 80 点)､「普通」(同 60 点)､「やや不満」(同 40 点)､「不満」(同０点）で採点し、各利用者の４つの回答の平均スコア（100 点満点）を算出する。

（４）創意工夫の発揮可能性

本業務を実施するに当たっては、以下の観点から請負者の創意工夫を反映し、公共サービスの質の向上（包括的な質の向上、効率化の向上、経費の削減等）に努めるものとする。

ア　総務省ＬＡＮ構築等請負業務の実施全般に対する提案

請負者は、別添２「総務省ＬＡＮ構築等請負業務の総合評価基準書」に従い、総務省ＬＡＮ構築等請負業務の実施全般に係る質の向上の観点から取り組むべき事項等の提案を行うこととする。

イ　事業内容に対する改善提案

請負者は、事業内容に対し、改善すべき提案（コスト削減に係る提案を含む）がある場合は､別添２｢総務省ＬＡＮ構築等請負業務の総合評価基準書｣に従い、具体的な方法等を示すとともに、従来の実施状況と同等以上の質が確保できる根拠等を提案すること。

（５）契約の形態及び支払

ア　契約の形態は、業務請負契約とする。

イ　総務省は、業務請負契約に基づき、請負者が実施する本業務について、契約の履行に関し、別添１「総務省ネットワーク基盤（ＬＡＮ）の構築等の請負調達仕様書」に定めた内容に基づく監督・検査を実施するなどして適正に実施されていることを確認した上で、適正な支払請求書を受領した日から 30 日以内に、毎月、契約金額を支払うものとする。平成 28 年度においては、契約金額のうち、設計・構築費に相当する額（ただし、契約金額の１／10 を上限とする。）を、平成 29 年度以降においては、毎月、契約金額から設計・構築費を差し引いた額に運用期間の全月数で除した額を請求者に支払うこととする。確認の結果、確保されるべき対象業務の質が達成されていないと認められる場合、総務省は、確保されるべき対象業務の質の達成に必要な限りで、請負者に対して本業務の実施方法の改善を行うよう指示することができる。請負者は、当該指示を受けて業務の実施方法を改善し、業務改善報告書を速やかに総務省に提出するものとする。業務改善報告書の内容が、確保されるべき対象業務の質が達成可能なものであると認められるまで、総務省は、請負費の支払を行わないことができる。なお、請負費は、本件業務開始以降のサービス提供に対して支払われるものであり、請負者が行う引継ぎや準備行為等に対して、請負者に発生した費用は、請負者の負担とする。

（６）法令変更による増加費用及び損害の負担

法令の変更により事業者に生じた合理的な増加費用及び損害は、アからウに該当する場合には総務省が負担し、それ以外の法令変更については請負者が負担する。

ア　本業務に類型的又は特別に影響を及ぼす法令変更及び税制度の新設

イ　消費税その他類似の税制度の新設・変更（税率の変更含む）

ウ　上記ア及びイのほか、法人税その他類似の税制度の新設・変更以外の税制度の新設・変更（税率の変更含む）

３　実施期間に関する事項

本請負契約の契約期間は、平成 28 年４月から平成 33 年３月 31 日までとする。

なお、設計・構築の期間は、平成 28 年４月から平成 29 年３月まで、運用及び維持保守・管理の期間は、平成 29 年４月から平成 33 年３月までとする。

総務省ＬＡＮの全体スケジュール（想定）を図３-１に示す。

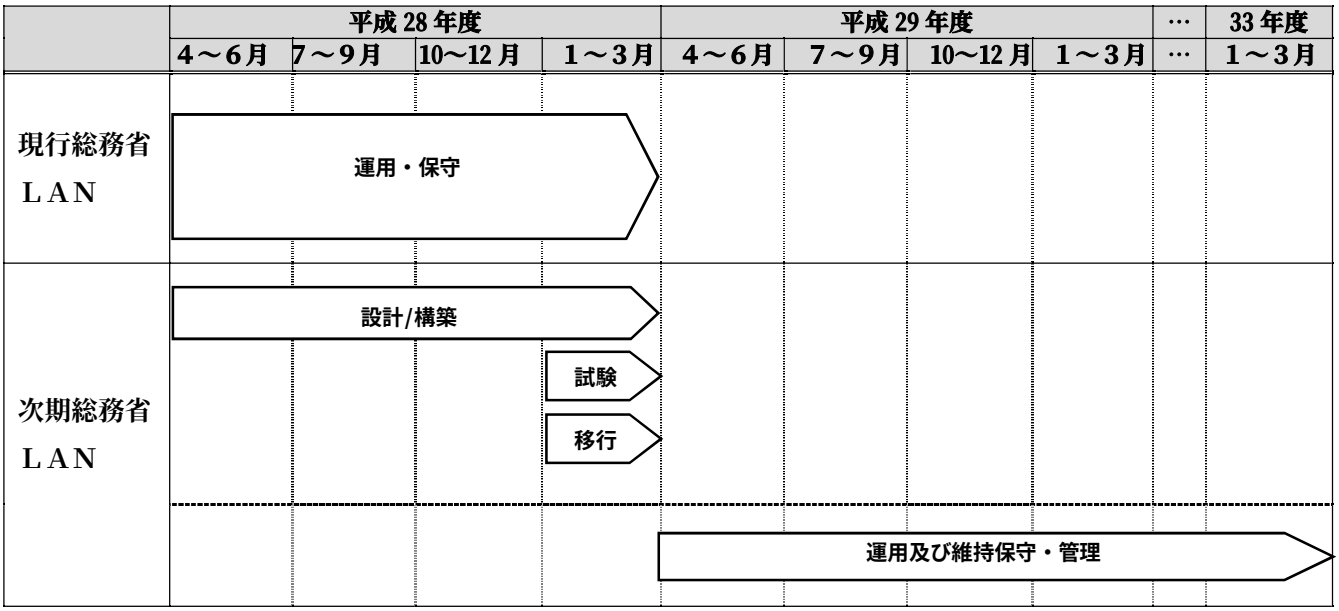


図３-１　全体スケジュール（想定）

４　入札参加資格に関する事項

（１）法第 15 条において準用する法第 10 条各号（第 11 号を除く。）に該当する者でないこと。

（２）予算決算及び会計令（昭和 22 年勅令第 165 号）第 70 条の規定に該当しない者であること。なお、未成年者、被保佐人又は被補助人であって、契約締結のために必要な同意を得ている者は、同条中、特別な理由がある場合に該当する。

（３）予算決算及び会計令第 71 条の規定に該当しない者であること。

（４）平成 25・26・27 年度総務省競争参加資格（全省庁統一資格）の「役務の提供等」Ａ及びＢの等級に格付けされ、関東・甲信越地域の競争参加資格を有する者であること（「役務の提供等」の営業品目④情報処理、⑥ソフトウェア開発又は⑮その他に登録しているものであること。）。

（５）法人税並びに消費税及び地方消費税の滞納がないこと。

（６）労働保険、厚生年金保険等の適用を受けている場合、保険料等の滞納がないこと。

（７）総務省及び他府省等における物品等の契約に係る指名停止措置要領に基づく指名停止を受けている期間中でないこと。

（８）次の事業者（再委託先等を含む。）及びこの事業者の「財務諸表等の用語、様式及び作成方法に関する規則」（昭和 38 年 11 月 27 日大蔵省令第 59 号）第８条に規定する親会社及び子会社、同一の親会社を持つ会社並びに委託先事業者等の緊密な利害関係を有する事業者は、入札には参加できない。

ア　「次期総務省ＬＡＮに係る調達支援業務の請負」の受注事業者

イ　「次期総務省ＬＡＮに係る工程管理支援業務の請負」の受注事業者

（９）調達仕様書の妥当性確認及び入札事業者の審査に関する業務を行うＣＩＯ補佐官及びその支援スタッフ等の属する又は過去２年間に属していた事業者でないこと。または、ＣＩＯ補佐官等がその職を辞職した後に所属する事業者の所属部門（辞職後の期間が２年に満たない場合に限る。）でないこと。

（１０）単独で対象業務を行えない場合は、又は、単独で実施するより業務上の優位性があると判断する場合は、適正に業務を実施できる入札参加グループを結成し、入札に参加することができる。その場合、入札書類提出時までに入札参加グループを結成し、入札参加資格の全てを満たす者の中から代表者を定め、他の者は構成員として参加するものとする。また、入札参加グループの構成員は、上記（１）から（９）までの資格を満たす必要があり、他の入札参加グループの構成員となり、又は、単独で参加することはできない。なお、入札参加グループの代表者及び構成員は、入札参加グループの結成に関する協定書（又はこれに類する書類）を作成し、提出すること。

（１１）本請負業務を統括管理する部門は、IS09001 認証を取得していること。

（１２）本請負業務を統括管理する部門は、IS027001 認証を取得していること。

（１３）財団法人日本情報経済社会推進協会のプライバシーマーク制度の認定を受けていること。

（１４）建築業法（昭和 24 年５月 24 日法律第 100 号）に基づく電気通信工事業及び電気工事業の許可を受けていること。

（１５）請負者は、本総務省ＬＡＮと同等又は類する全国規模のネットワークシステムの設計・構築の実績を有すること。ただし、設計・構築の実績については請負者自身のものであり、再委託等を受けた実績は含まないものとする。

５　入札に参加する者の募集に関する事項

（１）スケジュール

ア　パブリックコメント及び意見招請	平成 27 年	10 月下旬
イ　資料閲覧（第１回目）		11 月上旬
ウ　入札公示（官報掲載）		12 月下旬
エ　入札説明会	平成 28 年	１月上旬
オ　本省サーバ室の現地確認		１月中旬
カ　資料閲覧（第２回目）		１月中旬
キ　質問受付期限		２月上旬
ク　入札書（提案書）提出期限		２月下旬
ケ　入札参加者によるプレゼンテーション		３月上旬
コ　提案書の審査		３月中旬
サ　開札及び落札予定者の決定		３月下旬
シ　契約締結		４月上旬

（２）入札書類

入札参加者は、次に掲げる書類を入札説明会において説明された期日及び方法により提出すること。

ア　入札説明後の質問受付

入札公告以降、総務省において入札説明会に参加した者は、本実施要項の内容や入札に係る事項について、入札説明会後に、総務省に対して質問を行うことができる。質問は原則として電子メールにより行い、質問内容及び総務省からの回答は原則として入札説明会に参加したすべての者に公開することとする。ただし、民間事業者の権利や競争上の地位等を害するおそれがあると判断される場合には、質問者の意向を聴取した上で公開しないよう配慮する。

イ　提案書等

別添２「総務省ネットワーク基盤（ＬＡＮ）の構築等の請負総合評価基準書」に示した各要求項目について具体的な提案（創意工夫を含む。）を行い、各要求項目を満たすことができることを証明する書類

ウ　下見積書

人件費の単価証明書及び物件費の価格証明書を含んだ下見積書

ただし、契約後に発生する経費のみとする。

エ　入札書

入札金額（契約期間内の全ての請負業務に対する報酬の総額の 108 分の 100 に相当する金額）を記載した書類。

オ　委任状

代理人に委任したことを証明する書類

ただし、代理人による入札を行う場合に限る。

カ　競争参加資格審査結果通知書の写し

　平成 25・26・27 年度総務省競争参加資格（全省庁統一資格）「役務の提供等」Ａ及びＢ等級に格付けされた（関東・甲信越地域の）競争参加資格を有する者であること（「役務の提供等」の営業品目④情報処理、⑥ソフトウェア開発又は⑮その他に登録している者であること。）を証明する審査結果通知書の写し

　ただし、電子入札システムにより入札を行う場合は不要。

キ　理由書

　電子入札システムにより入札を行うことができない旨の理由を示した書類

　ただし、官側の事情で電子入札システムを用いた入札を行わない場合には不要。

ク　法第 15 条において準用する法第 10 条に規定する欠格事由のうち、暴力団排除に関する規程について評価するために必要な書類

ケ　法人税並びに消費税及び地方消費税の納税証明書（直近のもの）

コ　主たる事業概要、従業員数、事業所の所在地、代表者略歴、主要株主構成、他の者との間で競争の導入による公共サービス改革に関する法律施行令（平成 18 年７月５日政令第 228 号）第３条に規定する特定支配関係にある場合は、その者に関する当該情報

サ　共同事業体による参加の場合は、共同事業体内部の役割分担について定めた協定書又はこれに類する書類

シ　指名停止等に関する申出書

　各府省庁から指名停止を受けていないことを確認する書類

ス　誓約書

　本請負を完了できることを証明する書類

６　総務省ＬＡＮの構築等請負業務を実施する者を決定するための評価の基準その他本請負業務を実施する者の決定に関する事項

以下に本業務を実施する者の決定に関する事項を示す。

なお、詳細は別添２「総務省ネットワーク基盤（ＬＡＮ）の構築等の請負総合評価基準書」（以下「総合評価基準書」という。）を基本とする。

（１）評価方法

本業務を実施する者の決定は、総合評価落札方式によるものとする。

また、総合評価は、価格点（入札価格の得点）に技術点（総合評価基準書による加点）を加えて得た数値（以下「総合評価点」という。）をもって行う。

価格点と技術点の配分 **価格点の配分：技術点の配分 ＝ １：１**

総合評価点 ＝ 価格点（1,100 点満点） ＋ 技術点（1,100 点満点）

（２）合否決定方法

ア　調達仕様書及び要件定義書において必須と定められた要求要件を全て満たしている場合に「合格」とし、１つでも欠ける場合は「不合格」とする。

（３）総合評価点

ア　価格点

価格点は、入札価格を予定価格で除して得た値を１から減じて得た値に入札価格に対する得点配分を乗じて得た値とする。

価格点＝（１－入札価格÷予定価格）×1,100 点

イ　技術点

技術点の評価方法は以下のとおりとする。

（ア）全ての仕様を満たし、「合格」したものに「基礎点」として 100 点与える。

（イ）「合格」した提案書について、提案書審査委員会の委員ごとに「加点」部分の評価を行う。総務省にとって有益な提案があった場合に、別紙２「総合評価基準及び対応表」の評価ポイントに基づき、「加点」を与えるものとし、各委員の採点結果を委員会で確認し、事実誤認等があれば各委員において訂正する。なお、各委員が行う「加点」部分の評価は、以下の評価基準に基づき点数化する。確定した各委員の採点結果について、その平均値を算出し、「加点」とする。

評価	評価基準	配点比率
A	評価方針にのっとっており、提案内容が総務省ＬＡＮの質の向上や効率的な業務の実施に資することが具体的に示され、かつ、客観的な指標を用いて提案されている。	100%
B	評価方針にのっとっており、提案内容が総務省ＬＡＮの質の向上や効率的な業務の実施に資することが具体的に示され、提案されている。	40%
C	評価方針にのっとっていない、提案内容が不十分又は総務省ＬＡＮの質の向上や効率的な業務の実施について具体的に示されていない。	0%

（ウ）評価は、以下の方針に基づき判断する。

・ 総務省ＬＡＮの経緯等を十分に把握し有益な提案となっているか。
・ 実現性が十分に担保されていると判断できるか。
・ 提案者の実績や知見に基づく創意工夫が盛り込まれているか。

（エ）「基礎点」と「加点」の合計点を「技術点」とする。

技術点 ＝ 基礎点（100 点） ＋ 加点（1,000 点）

（４）落札者の決定

ア　総合評価基準書に示す全ての要求要件を満たし、入札者の入札価格が予算決算及び会計令第 79 条の規定に基づいて作成された予定価格の制限の範囲内であり、かつ、「総合評価落札方法」によって得られた総合評価点の最も高い者を落札者とする。ただし、予算決算及び会計令第 84 条の規定に該当する場合は、予算決算及び会計令第 85 条の基準（予定価格に 10 分の６を乗じて得た額）を適用するので、基準を下回る金額による入札が行われた場合は入札の結果を保留する。この場合、入札参加者は総務省の行う事情聴取等の調査に協力しなければならない。

イ　調査の結果、会計法（昭和 22 年法律第 35 号）第 29 条の６第１項ただし書きの規定に該当すると認められるときは、その定めるところにより、予定価格の制限の範囲内で次順位の者を落札者とすることがある。

ウ　落札者となるべき者が２人以上あるときは、直ちに当該入札者にくじを引かせ、落札者を決定するものとする。また、入札者又は代理人がくじを引くことができないときは、入札執行事務に関係のない職員がこれに代わってくじを引き、落札者を決定するものとする。

エ　契約担当官等は、落札者を決定したときに入札者にその氏名（法人の場合はその名称）及び金額を口頭で通知する。ただし、上記イにより落札者を決定する場合には別に書面で通知する。また、落札できなかった入札者は、落札の相対的な

利点に関する情報（当該入札者と落札者のそれぞれの入札価格及び技術点）の提供を要請することができる。

（５）落札決定の取消し

次の各号のいずれかに該当するときは、落札者の決定を取り消す。ただし、契約担当官等が、正当な理由があると認めたときはこの限りでない。

ア　落札者が、契約担当官等から求められたにもかかわらず契約書の取り交わしを行わない場合

イ　入札書の内訳金額と合計金額が符合しない場合

落札後、入札者に内訳書を記載させる場合がある。内訳金額が合計金額と符合しないときは、合計金額で入札したものとみなすため、内訳金額の補正を求められた入札者は、直ちに合計金額に基づいてこれを補正しなければならない。

（６）落札者が決定しなかった場合の措置

初回の入札において入札参加者がなかった場合、必須項目を全て満たす入札参加者がなかった場合又は再度の入札を行っても、なお、落札者が決定しなかった場合、原則として、入札条件等を見直した後、再度公告を行う。

なお、再度の入札によっても落札者となるべき者が決定しない場合又は本請負業務の実施に必要な期間が確保できないなどやむを得ない場合は、その理由を民間競争入札等監理委員会に報告するとともに公表するものとする。

7　総務省ＬＡＮの構築等請負業務に関する従来の実施状況に関する情報の開示に関する事項

（１）開示情報

対象業務に関して、以下の情報は別紙１「従来の実施状況に関する情報の開示」のとおり開示する。

ア　従来の実施に要した経費

イ　従来の実施に要した人員

ウ　従来の実施に要した施設及び設備

エ　従来の実施における目標の達成の程度

オ　従来の実施方法等

（２）資料の閲覧

前項オ「従来の実施方法等」の詳細な情報は、４「入札参加資格に関する事項」の要件を満たす民間競争入札に参加する予定の者から要望があった場合、現行総務省ＬＡＮに係る設計書等の納入成果物等について、所定の手続を踏まえた上で閲覧可能とする。閲覧可能な資料一覧を含め、詳細は別紙６「資料閲覧要領」に従うものとする。

また、民間競争入札に参加する予定の者から追加の資料の開示について要望があった場合は、総務省は、法令及び機密性等に問題のない範囲で適切に対応するよう努めるものとする。

8　総務省ＬＡＮの構築等請負業務の請負業者に使用させることができる国有財産に関する事項

（１）国有財産の使用

請負者は、本請負業務の遂行に必要な施設、設備等として、次に掲げる施設、設備等を適切な管理の下、無償で使用することができる。

ア　業務に必要な電気設備

イ　別紙１「従来の実施状況に関する情報の開示」の「３　従来の実施に要した施設及び設備」に記載されている設備及び主な物品

ウ　その他、総務省と協議し承認された業務に必要な施設、設備等

（２）使用制限

ア　請負者は、本請負業務の実施及び実施に付随する業務以外の目的で使用し、又は利用してはならない。

イ　請負者は、あらかじめ総務省と協議した上で、総務省の業務に支障を来さない範囲内において、施設内に本請負の実施に必要な設備等を持ち込むことができる。

ウ　請負者は、設備等を設置した場合は、設備等の使用を終了又は中止した後、直ちに、必要な原状回復を行う。

エ　請負者は、既存の建築物及び工作物等に汚損・損傷等を与えないよう十分に注意し、損傷（機器の故障等を含む。）が生じるおそれのある場合は、養生を行う。万一損傷が生じた場合は、請負者の責任と負担において速やかに復旧するものとする。

9　総務省ＬＡＮの構築等請負業務の請負業者が、総務省に対して報告すべき事項、秘密を適正に取り扱うために必要な措置その他の本請負業務の適正かつ確実な実施の確保のために本業務請負者が講じるべき措置に関する事項

（１）本業務請負者が総務省に報告すべき事項、総務省の指示により講じるべき措置

ア　報告等

（ア）請負者は、別添１「総務省ネットワーク基盤（ＬＡＮ）の構築等の請負調達仕様書」に規定する業務を実施したときは、当該仕様書に基づく各種報告書を総務省に提出しなければならない。

（イ）請負者は、請負業務を実施又は完了に影響を及ぼす重要な事項の変更が生じたときは、直ちに総務省に報告するものとし、総務省と請負者が協議するものとする。

（ウ）請負者は、契約期間中において、（イ）以外であっても、必要に応じて総務省から報告を求められた場合は、適宜、報告を行うものとする。

イ　調査

（ア）総務省は、本請負業務の適正かつ確実な実施を確保するために必要があると認めるときは、法第 26 条第１項に基づき、請負者に対し必要な報告を求め又は総務省の職員が事務所に立ち入り、当該業務の実施の状況又は記録、帳簿書類その他の物件を検査し、又は関係者に質問することができる。

（イ）総務省の職員が立入検査等を行う場合には、当該検査が法第 26 条第１項に基づくものであることを請負者に明示するとともに、その身分を示す証明書を携帯し、関係者に提示するものとする。

ウ　指示

総務省は、本請負業務の適正かつ確実な実施を確保するために必要と認めるときは、請負者に対し、必要な措置を採るべきことを指示することができる。

（２）秘密を適正に取り扱うために必要な措置

ア　請負者は、本業務の実施に際して知り得た総務省の情報等（公知の事実等を除く）を、第三者に漏らし、盗用し、又は請負業務以外の目的のために利用してはならない。これらの者が秘密を漏らし、又は盗用した場合は、法第 54 条により罰則の適用がある。

イ　請負者は、本業務の実施に際して得られた情報処理に関する利用技術（アイデア又はノウハウ）については、請負者からの文書による申出を総務省が認めた場合に限り、第三者へ開示できるものとする。

ウ　請負者は、総務省から提供された個人情報及び業務上知り得た個人情報について、個人情報の保護に関する法律（平成 15 年法律第 57 号）に基づき、適切な管理を行わなくてはならない。また、当該個人情報については、本業務以外の目的のために利用してはならない。

エ　請負者は、総務省の情報セキュリティに関する規程等に基づき、個人情報等を

取り扱う場合は、①情報の複製等の制限、②情報の漏えい等の事案の発生時における対応、③請負業務終了時の情報の消去・廃棄（復元不可能とすること。）及び返却、④内部管理体制の確立、⑤情報セキュリティの運用状況の検査に応じる義務、⑥請負者の事業責任者及び請負業務に従事する者全てに対しての守秘義務及び情報セキュリティ要求事項の遵守に関して、別紙５「機密保持に関する誓約書」を契約後速やかに総務省に提出しなければならない。

オ　アからエまでのほか、総務省は、請負者に対し、本請負業務の適正かつ確実な実施に必要な限りで、秘密を適正に取り扱うために必要な措置を採るべきことを指示することができる。

（３）契約に基づき請負者が講じるべき措置

ア　請負業務開始

請負者は、本業務の開始日から確実に業務を開始すること。なお、更新整備は、平成 29 年３月末までに完了し、運用開始は、平成 29 年４月から開始すること。

イ　権利の譲渡

請負者は、債務の履行を第三者に引き受けさせ、又は契約から生じる一切の権利若しくは義務を第三者に譲渡し、承継せしめ、若しくは担保に供してはならない。ただし、書面による総務省の事前の承認を得たときは、この限りではない。

ウ　権利義務の帰属等

（ア）本請負業務の実施が第三者の特許権、著作権その他の権利と抵触するときは、請負者は、その責任において、必要な措置を講じなくてはならない。

（イ）請負者は、本請負業務の実施状況を公表しようとするときは、あらかじめ、総務省の承認を受けなければならない。

エ　瑕疵担保責任

（ア）総務省は、成果物の引渡し後に発見された瑕疵について、引渡し後１年間は、請負者に補修を請求できるものとし、補修に必要な費用は、全て請負者の負担とする。

（イ）成果物の瑕疵が請負者の責めに帰すべき事由によるものである場合は、総務省は、前項の請求に際し、これによって生じた損害の賠償を合わせて請求することができる。

オ　再委託

（ア）本請負業務の請負者は、業務を一括して又は主たる部分を再委託してはならない。

（イ）請負者における遂行責任者を再委託先事業者の社員や契約社員とすることはできない。

（ウ）請負者は再委託先の行為について一切の責任を負うものとする。

（エ）再委託を行う場合、再委託先が４（８）に示す要件を満たすこと。

（オ）再委託先における情報セキュリティの確保については請負者の責任とする。

（カ）本請負業務の実施の一部を合理的な理由及び必要性により再委託する場合に

は、あらかじめ再委託の相手方の商号又は名称及び住所並びに再委託を行う業務の範囲、再委託の必要性及び契約金額等について記載した別添の再委託承認申請書を総務省に提出し、あらかじめ承認を受けること。

（キ）前項による再委託の相手方の変更等を行う必要が生じた場合も、前項と同様に再委託に関する書面を総務省に提出し、承認を受けること。

（ク）再委託の相手方が更に委託を行うなど複数の段階で再委託が行われる場合（以下「再々委託」という。）には、当該再々委託の相手方の商号又は名称及び住所並びに再々委託を行う業務の範囲を書面で報告すること。

（ケ）再委託先において、本調達仕様書に定める事項に関する義務違反又は義務を怠った場合には、請負者が一切の責任を負うとともに、総務省は、当該再委託先への再委託の中止を請求することができる。

カ　契約内容の変更

総務省及び請負者は、本請負業務の質の確保の推進、またはその他やむをえない事由により本契約の内容を変更しようとする場合は、あらかじめ変更の理由を提出し、それぞれの相手方の承認を受けるとともに法第 21 条の規定に基づく手続を適切に行わなければならない。

キ　契約の解除

総務省は、請負者が次のいずれかに該当するときは、請負者に対し請負費の支払を停止又は契約を解除若しくは変更することができる。この場合、請負者は総務省に対して、契約金額から消費税及び地方消費税を差し引いた金額の 100 分の 10 に相当する金額を違約金として支払わなければならない。その場合の算定方法については、総務省の定めるところによる。ただし、同額の超過する増加費用及び損害が発生したときは、超過分の請求を妨げるものではない。

また、請負者は、総務省との協議に基づき、本請負業務の処理が完了するまでの間、責任を持って当該処理を行わなければならない。

（ア）法第 22 条第１項イからチまで又は同項第２号に該当するとき。

（イ）暴力団員を、業務を統括する者又は従業員としていることが明らかになった場合。

（ウ）暴力団員と社会的に非難されるべき関係を有していることが明らかになった場合。

（エ）再委託先が、暴力団若しくは暴力団員により実質的に経営を支配される事業を行う者又はこれに準ずる者に該当する旨の通知を、警察当局から受けたとき。

（オ）再委託先が暴力団又は暴力団関係者と知りながらそれを容認して再委託契約を継続させているとき。

ク　談合等不正行為

請負者は、談合等の不正行為に関して、総務省が定める「談合等の不正行為に関する特約条項」に従うものとする。

ケ　損害賠償

　請負者は、請負者の故意又は過失により総務省に損害を与えたときは、総務省に対し、その損害について賠償する責任を負う。また、総務省は、契約の解除及び違約金の徴収をしてもなお損害賠償の請求をすることができる。

　なお、総務省から請負者に損害賠償を請求する場合において、原因を同じくする支払済の違約金がある場合には、当該違約金は原因を同じくする損害賠償について、支払済額とみなす。

コ　不可抗力免責、危険負担

　総務省及び請負者の責に帰すことのできない事由により契約期間中に物件が滅失又は毀損し、その結果、総務省が物件を使用することができなくなったときは、請負者は、当該事由が生じた日の翌日以後の契約期間に係る代金の支払を請求することができない。

サ　金品等の授受の禁止

　請負者は、本請負業務の実施において金品等を受け取ること又は与えることをしてはならない。

シ　宣伝行為の禁止

　請負者及び本請負業務に従事する者は、本請負業務の実施に当たっては、自ら行う業務の宣伝を行ってはならない。また、本請負業務の実施をもって、第三者に対し誤解を与えるような行為をしてはならない。

ス　法令の遵守

　請負者は、本請負業務を実施するに当たり適用を受ける関係法令等を遵守しなくてはならない。

セ　安全衛生

　請負者は、本請負業務に従事する者の労働安全衛生に関する労務管理については、責任者を定め、関係法令に従って行わなければならない。

ソ　記録及び帳簿類の保管

　請負者は、本請負業務に関して作成した記録及び帳簿類を、本請負業務を終了し、又は中止した日の属する年度の翌年度から起算して５年間、保管しなければならない。

タ　契約の解釈

　契約に定めのない事項及び契約に関して生じた疑義は、総務省と請負者との間で協議して解決する。

１０総務省ＬＡＮの構築等請負業務の請負業者が本業務を実施するに当たり、第三者に損害を加えた場合において、その損害の賠償に関し契約により請負者が負うべき責任に関する事項

本請負業務を実施するに当たり、請負者又はその職員その他の本請負業務に従事する者が、故意又は過失により、本請負業務の受益者等の第三者に損害を加えた場合は、次のとおりとする。

（１）総務省が国家賠償法（昭和 22 年法律第 125 号）第１条第１項等に基づき当該第三者に対する賠償を行ったときは、総務省は請負者に対し、当該第三者に支払った損害賠償額（当該損害の発生について総務省の責めに帰すべき理由が存する場合は、総務省が自ら賠償の責めに任ずべき金額を超える部分に限る。）について求償することができる。

（２）請負者が民法（明治 29 年法律第 89 号）第 709 条等に基づき当該第三者に対する賠償を行った場合であって、当該損害の発生について総務省の責めに帰すべき理由が存するときは、請負者は総務省に対し、当該第三者に支払った損害賠償額のうち自ら賠償の責めに任ずべき金額を超える部分を求償することができる。

１１総務省ＬＡＮの構築等請負業務に係る法第７条第８項に規定する評価に関する事項

（１）本業務の実施状況に関する調査の時期

総務省は、本業務の実施状況について内閣総理大臣が行う評価の時期（平成 31 年５月を予定）及び本業務の本格運用開始時期（平成 29 年度）を踏まえ、平成 29 年度以降各年の 12 月末日時点における状況を調査する。

（２）調査項目及び実施方法

ア　総務省ＬＡＮの稼働率

業務報告書等により調査

イ　セキュリティ上の重大障害

業務報告書等により調査

ウ　システム運用上の重大障害の件数

業務報告書等により調査

エ　総務省ＬＡＮ利用に関する満足度アンケート調査結果

各年度において、総務省ＬＡＮの利用者に対する年１回のアンケート（総務省ＬＡＮ利用に関する満足度アンケート調査）の実施結果により調査

（３）意見聴取等

総務省は、必要に応じ、請負者から意見の聴取を行うことができるものとする。

（４）実施状況等の提出時期

総務省は、平成 31 年５月を目途として、本業務の実施状況を内閣総理大臣及び民間競争入札等監理委員会へ提出する。

なお、調査報告を内閣総理大臣及び民間競争入札等監理委員会に提出するに当たり、総務省ＣＩＯ補佐官の意見を聴くものとする。

１２その他業務の実施に関し必要となる事項

（１）総務省ＬＡＮ構築等請負業務の実施状況等の民間競争入札等監理委員会への報告

総務省は、法第 26 条及び第 27 条に基づく報告徴収、立入検査、指示等を行った場合には、その都度、措置の内容及び理由並びに結果の概要を民間競争入札等監理委員会へ報告することとする。

（２）総務省の監督体制

本契約に係る監督は、総務省主管課が自ら立会い、指示その他の適切な方法によって行うものとする。

本請負業務の実施状況に係る監督は以下のとおり。

監督職員：総務省大臣官房企画課情報システム室情報システム第三係長

検査職員：総務省大臣官房企画課情報システム室課長補佐

（３）本業務請負者の責務

ア　請負者は、刑法（明治 40 年法律第 45 号）その他の罰則の適用について、法令により公務に従事する職員とみなされる。

イ　請負者は、法第 54 条の規定に該当する場合は、１年以下の懲役又は 50 万円以下の罰金に処される。

ウ　請負者は、法第 55 条の規定に該当する場合は、30 万円以下の罰金に処されることとなる。なお、法第 56 条により、法人の代表者又は法人若しくは人の代理人、使用人その他の従業者が、その法人又は人の業務に関し、法第 55 条の規定に違反したときは、行為者を罰するほか、その法人又は人に対して同条の刑を科する。

エ　請負者は、会計検査院法（昭和 22 年法律第 73 号）第 23 条第１項第７号に規定する者に該当することから、会計検査院が必要と認めるときには、同法第 25 条及び第 26 条により、同院の実地の検査を受けたり、同院から直接又は総務省に通じて、資料又は報告等の提出を求められたり、質問を受けたりすることがある。

（４）著作権

ア　請負者は、本業務の目的として作成される成果物に関し、著作権法第 27 条及び第 28 条を含む著作権の全てを当省に無償で譲渡するものとする。

イ　請負者は、成果物に関する著作者人格権（著作権法第 18 条から第 20 条までに規定された権利をいう。）を行使しないものとする。ただし、当省が承認した場合は、この限りではない。

ウ　ア及びイに関わらず、成果物に請負者が既に著作権を保有しているもの（以下「請負者著作物」という。）が組み込まれている場合は、当該請負者著作物の著作権についてのみ、請負者に帰属する。

エ　提出される成果物に第三者が権利を有する著作物が含まれる場合には、請負者が当該著作物の使用に必要な費用の負担及び使用許諾契約等に係る一切の手続きを行うものとする。

（５）総務省ＬＡＮ構築等請負業務の調達仕様書

本請負業務を実施する際に必要な仕様は、別添１「総務省ネットワーク基盤（ＬＡＮ）の構築等の請負調達仕様書」に示すとおりである。

１３別添一覧

別紙１「従来の実施状況に関する情報の開示」
別紙２「運用管理の業務フロー」
別紙３「組織図」
別紙４「総務省ＬＡＮの利用に関する満足度アンケート調査」
別紙５「機密保持に関する誓約書」
別紙６「資料閲覧要領」
別紙７「資料閲覧申込書」
別紙８「質問票」

別添１「総務省ネットワーク基盤（ＬＡＮ）の構築等の請負調達仕様書」
別添２「総務省ネットワーク基盤（ＬＡＮ）の構築等の請負総合評価基準書」

別紙１

従来の実施状況に関する情報の開示

１　従来の実施に要した経費

（単位：千円）

			平成 24 年度	平成 25 年度	平成 26 年度
総務省情報ネットワークの構築等の請負業務					
	人件費	常勤職員	-	-	-
		非常勤職員	-	-	-
	物件費		0	0	0
	請負費	役務（運用員）	-	288,540	296,784
		機器・回線リース料	-	1,069,583	1,100,142
		設計・構築費	563,010	-	-
		その他	-	-	-
計(a)			563,010	1,358,123	1,396,926
参考値(b)	減価償却費		-	-	-
	退職給付費用		-	-	-
	間接部門費		-	-	-
(a)＋(b)			563,010	1,358,123	1,396,926

（注記事項）

平成 25 年度：運用期間 12 月
平成 26 年度：運用期間 12 月

設計・構築期間：平成 24 年７月～平成 25 年３月

なお、現行システムの構築に係る当時の作業スケジュール・実績等の納入成果物は、民間競争入札に参加する予定の者から閲覧の要望があった場合には、所定の手続きを踏まえた上で、別紙５「機密保持に関する誓約書」へ署名し、遵守することで閲覧可能である。

2　従来の実施に要した人員

（単位：人）

	平成 24 年度	平成 25 年度	平成 26 年度
(運用業務従事者)			
ＬＡＮ管理室（運用責任者、維持保守管理、セキュリティ、インフラ対応）	0	17	17

（業務従事者に求められる知識・経験等）

運用に係る要員（運用責任者、維持保守管理、セキュリティ、インフラ対応）は、運用業務遂行に当たり十分な技能と経験、資格を有すること。

なお、総務省ＬＡＮ情報セキュリティチームについては、以下の項目を実施することのできる知識・経験等を有すること。

・定常的な分析監視を行うこと。
・政府の情報セキュリティ方針や施策、総務省の情報セキュリティポリシ等を理解し、総務省 LAN の情報セキュリティ対策との適合性を把握すること。
・総務省 LAN の構成や状態を詳細に把握し、主管係や関係各所との協議や調整において、具体的な情報の提示や施策の可否等を迅速に判断できること。
・定期的にリソースやトラフィックの状況・内容を監視し、傾向分析やログの相関分析等を行い、異常検知を行うこと。
・ログ分析のための定義、検索のロジック、相関分析手法の考え方を明示すること。
・セキュリティインシデント発生時には情報の収集、分析、問題の特定、解析、対策案の検討、協議、（運用員に対する）被害拡大防止策の指示、その他対応の指示、対応の状況確認、報告等を行うこと。また、十分な体制を組むこと。
・セキュリティインシデント発生後には各種証跡を分析し、発生源や影響範囲等の調査、外への影響や潜在的な危険性等を報告すること。
・振る舞い検知技術やファイル評価検知技術等を活用した、異常動作の迅速な把握をすること。
・マルウェア感染の疑いがあるファイル（検体）の特定を行うこと。
・内閣官房セキュリティセンター（NISC）等、関係機関からの調査依頼や対応要請への支援を行うこと。
・定期的に総務省 LAN の脆弱性を診断し、総務省 LAN におけるセキュリティ課題の提示と対策の検討、実施を行うこと。
・運用員やヘルプデスク要員と連携できるよう、日常的にコミュニケーションとりつつ運用の状況を把握しておくこと。

（業務の繁閑の状況とその対応）

平成 25・26 年度の運用及び維持保守・管理業務の主な対応状況は、以下のとおり。

実施要項２(1)カ「（ウ）運用及び維持保守・管理」の表２－３「運用及び維持保守・管理作業の概要」に示す作業の件数を以下に示す。

申請受付・審査（総務省職員が対応）

・平成 25 年度

	4 月	5 月	6 月	7 月	8 月	9 月	10 月	11 月	12 月	1 月	2 月	3 月	合計(件)
受付件数	20	4	5	9	6	10	7	2	7	3	5	5	83

・平成 26 年度

	4 月	5 月	6 月	7 月	8 月	9 月	10 月	11 月	12 月	1 月	2 月	3 月	合計(件)
受付件数	9	8	7	2	15	1	6	3	3	7	2	2	65

利用者からの申請・操作方法等の問合せ対応、申請に基づく設定変更、LAN 端末の動作不良、ウイルス感染等の対応

・平成 25 年度

	4 月	5 月	6 月	7 月	8 月	9 月	10 月	11 月	12 月	1 月	2 月	3 月	合計(件)
受付件数	900	576	665	791	620	615	514	420	516	545	443	664	7,269

・平成 26 年度

	4 月	5 月	6 月	7 月	8 月	9 月	10 月	11 月	12 月	1 月	2 月	3 月	合計(件)
受付件数	922	633	567	574	599	754	715	564	637	638	472	633	7,708

※ 利用者からの申請や操作方法の問合せ対応は、総務省職員が原則対応。

※ 申請に基づく設定変更や LAN 端末の動作不良、ウイルス感染等の対応は、請負事業者が原則対応。

障害発生対応

・平成 25 年度

	4 月	5 月	6 月	7 月	8 月	9 月	10 月	11 月	12 月	1 月	2 月	3 月	合計(件)
サーバ対応件数	2	4	0	4	0	0	3	1	2	3	0	2	21
ネットワーク機器対応件数	0	3	2	0	0	2	1	2	0	0	0	0	10
LAN 端末対応件数	5	3	4	2	6	2	1	0	5	4	2	3	37

・平成 26 年度

	4 月	5 月	6 月	7 月	8 月	9 月	10 月	11 月	12 月	1 月	2 月	3 月	合計(件)
サーバ対応件数	0	1	0	5	0	3	0	1	1	4	1	2	18
ネットワーク機器対応件数	0	0	2	0	2	0	0	2	1	0	0	0	7
LAN 端末対応件数	1	2	3	3	3	3	4	4	6*	0	2	3	34

* 複合機２件を含む。

情報セキュリティ対応

・平成 25 年度

	4 月	5 月	6 月	7 月	8 月	9 月	10 月	11 月	12 月	1 月	2 月	3 月	合計(件)
情報セキュリティ対応（不審メール対応件数、不正接続機器対応件数、LAN 端末検知ウイルス対策）	55	35	44	46	55	114	165	117	142	114	113	129	1,129

・平成 26 年度

	4 月	5 月	6 月	7 月	8 月	9 月	10 月	11 月	12 月	1 月	2 月	3 月	合計(件)
情報セキュリティ対応（不審メール対応件数、不正接続機器対応件数、LAN 端末検知ウイルス対策）	147	152	137	129	150	126	161	255	133	130	192	160	2,660

※ 不審メール対応件数：職員から提出された不審メールの対応件数。

情報セキュリティ管理（セキュリティパッチの適用）

・平成 25 年度

	4 月	5 月	6 月	7 月	8 月	9 月	10 月	11 月	12 月	1 月	2 月	3 月	合計(件)
サーバ対応件数	0	0	0	0	8	0	3	0	0	8	13	4	36
ネットワーク機器対応件数	0	0	0	0	2	0	0	0	0	0	1	1	4
LAN 端末対応件数	20	16	14	14	15	33	19	24	19	10	25	18	227

・平成 26 年度

	4 月	5 月	6 月	7 月	8 月	9 月	10 月	11 月	12 月	1 月	2 月	3 月	合計(件)
サーバ対応件数	0	0	0	9	4	0	0	0	8	0	9	4	34
ネットワーク機器対応件数	2	7	0	5	2	5	5	0	5	0	0	0	31
LAN 端末対応件数	14	25	16	23	21	8	24	17	16	13	31	36	244

（注記事項）

3　従来の実施に要した施設及び設備

(本省)
【施設】
施設名称：中央合同庁舎第２号館
使用場所：地下１階サーバ室及びＬＡＮ管理室

【設備及び主な物品】
総務省貸与：
　サーバラック 23 台
　内線電話 29 台（固定電話８台、PHS21 台)、机８台、袖机６台、椅子 20 脚、ロッカー６本、鍵収納庫１台、キャビネット 14 台、パソコンラック７台、光ディスク破壊装置１台、台車２台

請負者所有：
　プリンタ２台、FAX・コピー統合機１台、シュレッダ１台、会議卓１台、机 13 台、長机７台、折り畳み机１台、袖机 12 台、椅子 50 脚、ワゴン１台、キャビネット 11 本、書庫１本、ロッカー３本、パーティション９個、ホワイトボード４台他

(外部拠点)
【施設】
施設名称：「拠点情報一覧」を参照のこと
使用場所：「拠点情報一覧」を参照のこと

【設備及び主な物品】
種類：サーバラック
使用数量：71 台

（注記事項）

・本請負業務を実施する上で必要となる電源は、総務省が指定した分電盤に工事を施すことにより使用可能とする。

・本請負業務を実施する上で必要となる局舎建物の一部については主管課が無償で使用させるものとし、光熱費、電話回線使用料も総務省が負担するものとする。なお、請負者はこれらを本件業務以外の目的に使用してはならない。

・本請負業務を実施する上で必要となる機器等で、現に総務省が保有するもの以外（運用及び維持保守・管理業務上使用する事務機器、消耗品等）は請負者において準備することとし、その所要経費は契約金額に含めるものとする。

・隣接するサーバ室に打合せスペースがある。

・拠点情報一覧（平成 27 年７月 15 日現在）

拠点	郵便番号	住所
本省	100-8926	東京都千代田区霞が関２-１-２ 中央合同庁舎第２号館
ＤＲサイト	－	－
総務省第２庁舎	162-8668	東京都新宿区若松町１９-１
中央合同庁舎４号館 （公害等調整委員会）	100-0013	東京都千代田区霞が関３-１-１
中央合同庁舎８号館 （行政管理局）	100-8914	東京都千代田区永田町１-６-１
行政管理局宮城分室	－	宮城県仙台市内
行政管理局大阪分室	－	大阪府豊中市内
自治大学校	190-0014	東京都立川市緑町３５９１
情報通信政策研究所	185-8795	東京都国分寺市泉町２-１１-１６
アジア太平洋統計研修所	261-8787	千葉県千葉市美浜区若葉３-２-２

消防大学校　及び 消防研究センター	182-8508	東京都調布市深大寺東町４-３５-３
国会連絡室	100-0014	東京都千代田区永田町１-７-１ 参議院別館
北海道管区行政評価局	060-0808	北海道札幌市北区北８条西２-１-１ 札幌第１合同庁舎　（北海道総合通信局と同じ）
函館行政評価分室	040-0032	北海道函館市新川町２５-１８ 函館地方合同庁舎
旭川行政評価分室	078-8501	北海道旭川市大町３条４丁目 北海道管区行政評価局旭川行政評価分室ビル
釧路行政評価分室	085-0022	北海道釧路市南浜町５-９ 釧路港湾合同庁舎
東北管区行政評価局	980-0014	宮城県仙台市青葉区本町３-２-２３ 仙台第２合同庁舎　（東北総合通信局と同じ）
青森行政評価事務所	030-0801	青森県青森市新町２-４-２５ 青森合同庁舎
岩手行政評価事務所	020-0045	岩手県盛岡市内丸７-２５ 盛岡合同庁舎第２号館
秋田行政評価事務所	010-0951	秋田県秋田市山王７-１-３ 秋田合同庁舎
山形行政評価事務所	990-0041	山形県山形市緑町１-５-４８ 山形地方合同庁舎
福島行政評価事務所	960-8021	福島県福島市霞町１-４６ 福島合同庁舎
関東管区行政評価局	330-9717	埼玉県さいたま市中央区新都心１-１ さいたま新都心合同庁舎１号館
茨城行政評価事務所	310-0061	茨城県水戸市北見町１-１１ 水戸地方合同庁舎
栃木行政評価事務所	320-0043	栃木県宇都宮市桜５-１-１３ 宇都宮地方合同庁舎
群馬行政評価事務所	371-0026	群馬県前橋市大手町２-３-１ 前橋地方合同庁舎
千葉行政評価事務所	260-0024	千葉県千葉市中央区中央港１-１１-３ 千葉地方合同庁舎
東京行政評価事務所	169-0073	東京都新宿区百人町３-２８-８ 新宿地方合同庁舎
神奈川行政評価事務所	231-0023	神奈川県横浜市中区山下町３７-９ 横浜地方合同庁舎
新潟行政評価事務所	950-8628	新潟市中央区美咲町１-１-１ 新潟美咲合同庁舎第１号館
山梨行政評価事務所	400-0031	山梨県甲府市北口１-２-１９ 甲府地方合同庁舎
長野行政評価事務所	380-0846	長野県長野市旭町１１０８ 長野第１合同庁舎　（信越総合通信局と同じ）
中部管区行政評価局	460-0001	愛知県名古屋市中区三の丸２-５-１ 名古屋合同庁舎第２号館
富山行政評価事務所	930-0856	富山県富山市牛島新町　１１-７ 富山合同庁舎
石川行政評価事務所	920-0962	石川県金沢市広坂２-２-６０ 金沢広坂合同庁舎　（北陸総合通信局と同じ）
岐阜行政評価事務所	500-8114	岐阜県岐阜市金竜町５-１３ 岐阜合同庁舎
静岡行政評価事務所	420-0853	静岡県静岡市葵区追手町９-５０ 静岡地方合同庁舎
三重行政評価事務所	514-0033	三重県津市丸之内２６-８ 津合同庁舎
近畿管区行政評価局	540-0008	大阪府大阪市中央区大手前４-１-６７ 大阪合同庁舎第２号館７階
福井行政評価事務所	910-0859	福井県福井市日之出３-１４-１５　福井地方合同庁舎
滋賀行政評価事務所	520-0044	滋賀県大津市京町３-１-１ 大津びわ湖合同庁舎
京都行政評価事務所	604-8482	京都府京都市中京区西ノ京笠殿町３８ 京都地方合同庁舎

兵庫行政評価事務所	650-0024	兵庫県神戸市中央区海岸通２９　神戸地方合同庁舎
奈良行政評価事務所	630-8213	奈良県奈良市登大路町８１　奈良合同庁舎
和歌山行政評価事務所	640-8155	和歌山県和歌山市九番丁１１
中国四国管区行政評価局	730-0012	広島県広島市中区上八丁堀６-３０　広島合同庁舎第４号館
鳥取行政評価事務所	680-0845	鳥取県鳥取市富安２-８９-４　鳥取第１地方合同庁舎
島根行政評価事務所	690-0841	島根県松江市向島町１３４-１０　松江地方合同庁舎
岡山行政評価事務所	700-0984	岡山県岡山市北区桑田町１-３６　岡山地方合同庁舎
山口行政評価事務所	753-0088	山口県山口市中河原町６-１６　山口地方合同庁舎第１号館
四国行政評価支局	760-0088	香川県高松市松島町１-１７-３３　高松第２地方合同庁舎
徳島行政評価事務所	770-0851	徳島県徳島市徳島町城内６-６　徳島地方合同庁舎
愛媛行政評価事務所	790-0808	愛媛県松山市若草町４-３　松山若草合同庁舎
高知行政評価事務所	780-0870	高知県高知市本町４-３-４１　高知地方合同庁舎
九州管区行政評価局	812-0013	福岡県福岡市博多区博多駅東２-１１-１　福岡合同庁舎
佐賀行政評価事務所	840-0041	佐賀県佐賀市城内２-１０-２０　佐賀合同庁舎
長崎行政評価事務所	852-8106	長崎県長崎市岩川町１６-１６　長崎合同庁舎
熊本行政評価事務所	860-0047	熊本県熊本市西区春日２-１０-１　熊本地方合同庁舎　B棟
大分行政評価事務所	870-0016	大分県大分市新川町２-１-３６　大分合同庁舎
宮崎行政評価事務所	880-0805	宮崎県宮崎市橘通東　３-１-２２　宮崎合同庁舎
鹿児島行政評価事務所	892-0816	鹿児島県鹿児島市山下町１３-２１　　鹿児島合同庁舎
沖縄行政評価事務所	900-0006	沖縄県那覇市おもろまち２-１-１ 那覇第２地方合同庁舎１号館
北海道総合通信局	060-8795	北海道札幌市北区北８条西２-１-１　札幌第１合同庁舎
東北総合通信局	980-0014	宮城県仙台市青葉区本町３-２-２３　仙台第２合同庁舎
関東総合通信局	102-0074	東京都千代田区九段南１-２-１　九段第３合同庁舎
関東総合通信局 （三浦電波監視センター）	238-0115	神奈川県三浦市初声町高円坊１６９１
信越総合通信局	380-8795	長野県長野市旭町１１０８　長野第１合同庁舎
東海総合通信局	461-8795	愛知県名古屋市東区白壁１-１５-１　名古屋合同庁舎第３号館
北陸総合通信局	920-8795	石川県金沢市広坂２-２-６０　金沢広坂合同庁舎
近畿総合通信局	540-8795	大阪府大阪市中央区大手前１-５-４４　大阪合同庁舎第１号館
中国総合通信局	730-8795	広島県広島市中区東白島町１９-３６
四国総合通信局	790-8795	愛媛県松山市宮田町８-５
九州総合通信局	860-8795	熊本県熊本市西区春日２-１０-１　熊本地方合同庁舎
沖縄総合通信事務所	900-8795	沖縄県那覇市旭町１-９　カフーナ旭橋Ｂ-１街区
外部監視室	―	―

4　従来の実施における目標の達成の程度

SLA 達成率	平成 24 年度		平成 25 年度		平成 26 年度	
	目標	実績	目標	実績	目標	実績
総務省 LAN の稼働率	-	-	99.90%	99.996%	99.90%	100.000%
セキュリティの重大障害の件数	-	-	0 件	0 件	0 件	0 件
システム運用上の重大障害の件数	-	-	0 件	0 件	0 件	0 件
アンケート調査	-	-	75 点	85.90 点	75 点	84.57 点

（注記事項）

総務省ＬＡＮの利用満足度調査（別紙４「総務省 LAN の利用に関する満足度アンケート調査」を用いてアンケート形式で調査を実施）は、平成 25 年度分を平成 26 年５月 14 日(水)～同年５月 23 日(金)、平成 26 年度分を平成 27 年４月 28 日(火)～同年５月 20 日(水)の期間に実施した。平成 25 年度分は回答者数 61 人（回収率 70%）、平成 26 年度は回答者数 87 人（回収率 99%）であった。当該調査は、回答までに要した時間、説明の分かりやすさ、回答・手順の正確性、担当者の対応について、満足 100 点、やや満足 80 点、普通 60 点、やや不満 40 点、不満 0 点として回答してもらい、各調査対象者がアンケートに回答した結果の全体の平均点を算出した。

5　従来の実施方法等

従来の実施方法（業務フロー図等）

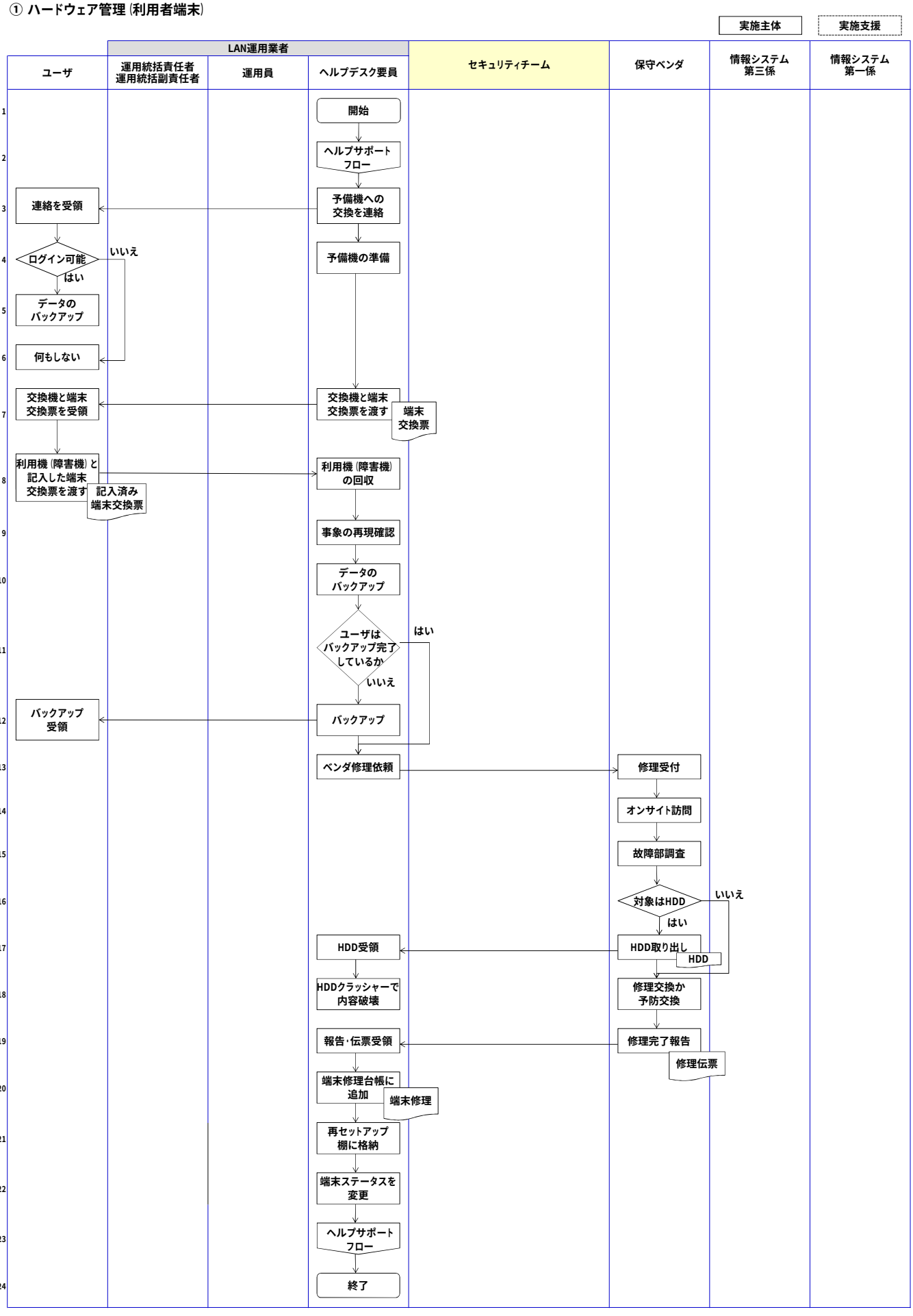
別紙２のとおり。

（注記事項）

・現行総務省 LAN の運用及び維持保守・管理に関する詳細な情報は、別紙６「資料閲覧要領」に基づき所定の手続を経て、応札を希望する事業者に開示する。

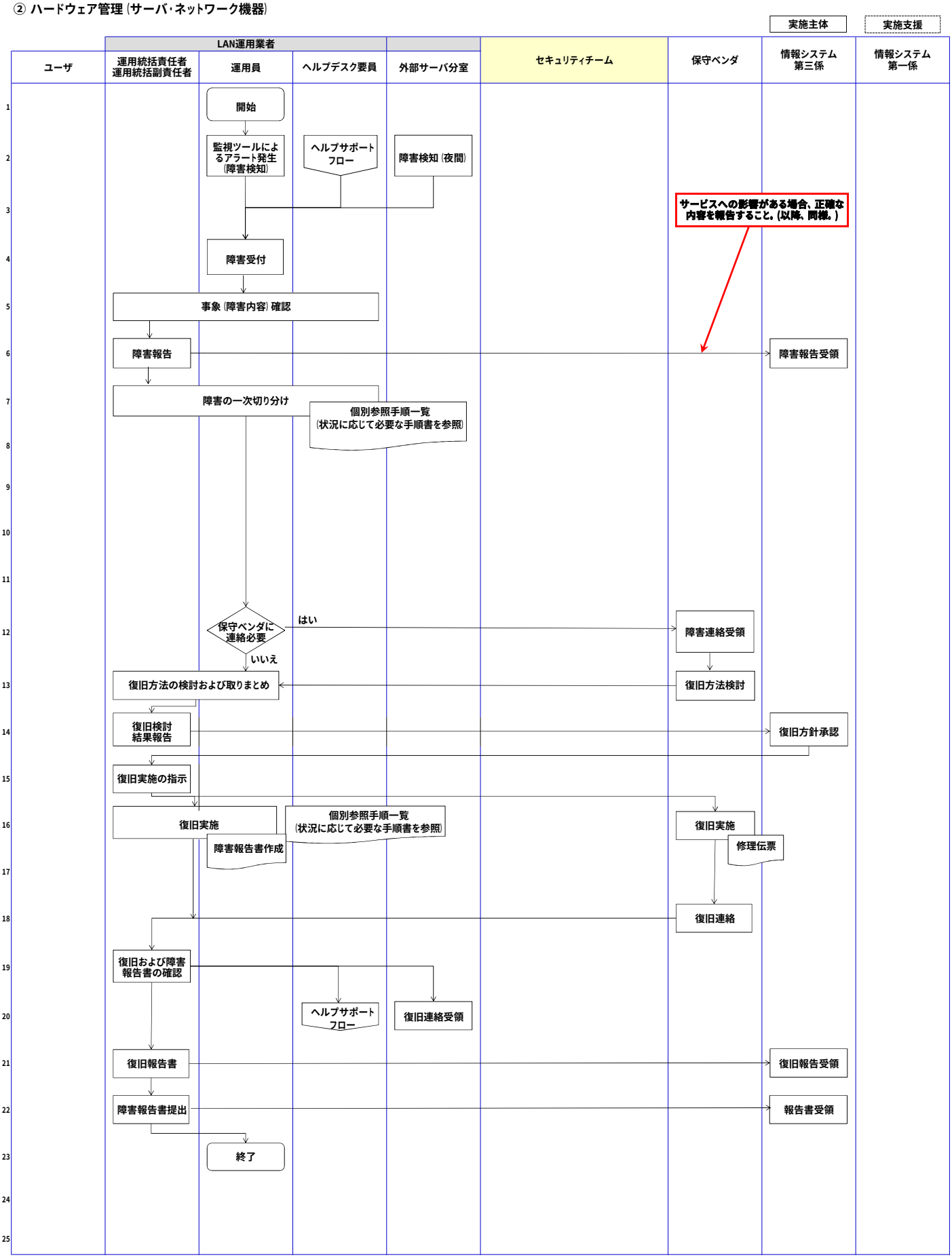
別紙2

① ハードウェア管理（利用者端末）



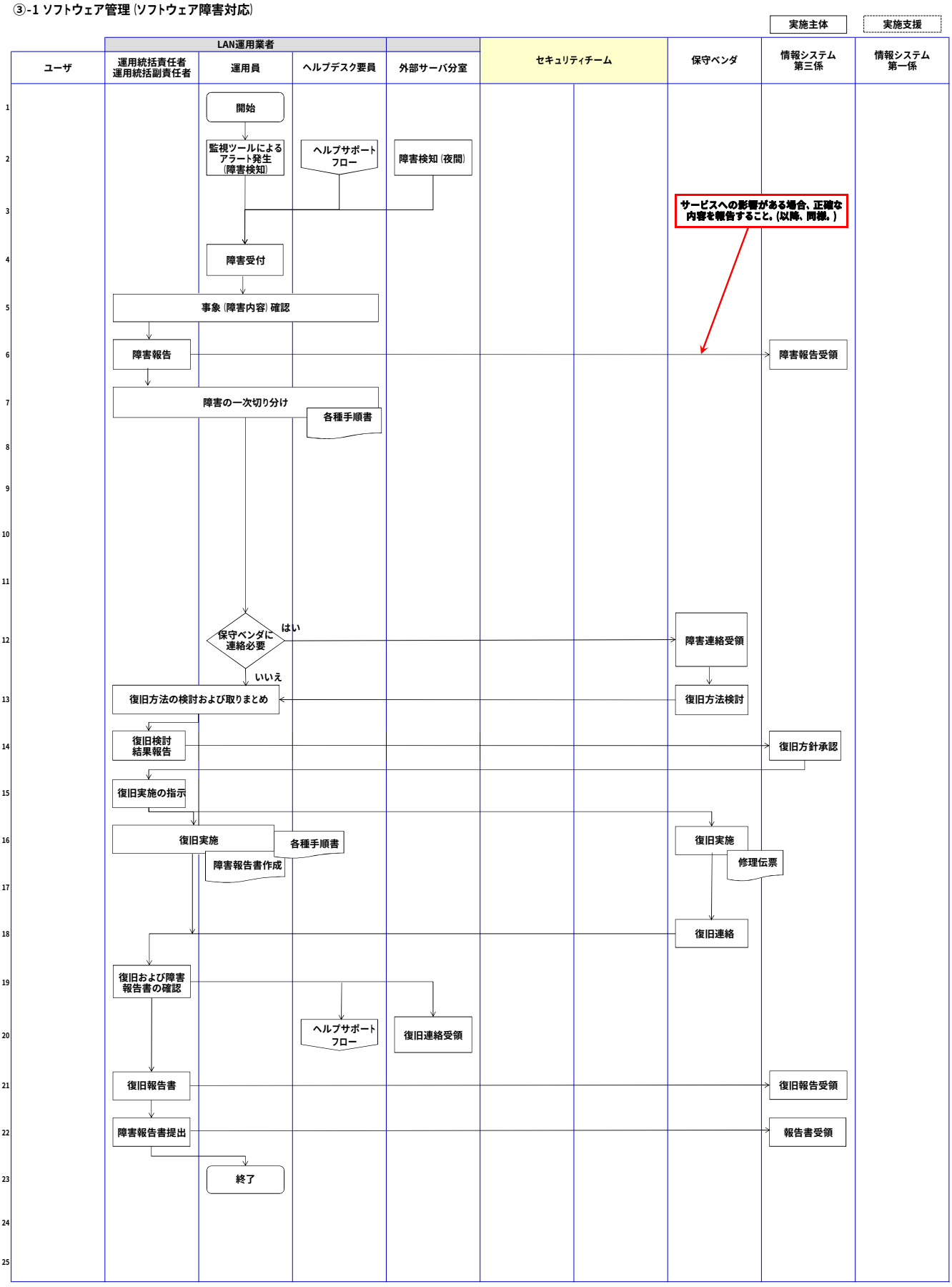
別紙2

② ハードウェア管理（サーバ・ネットワーク機器）



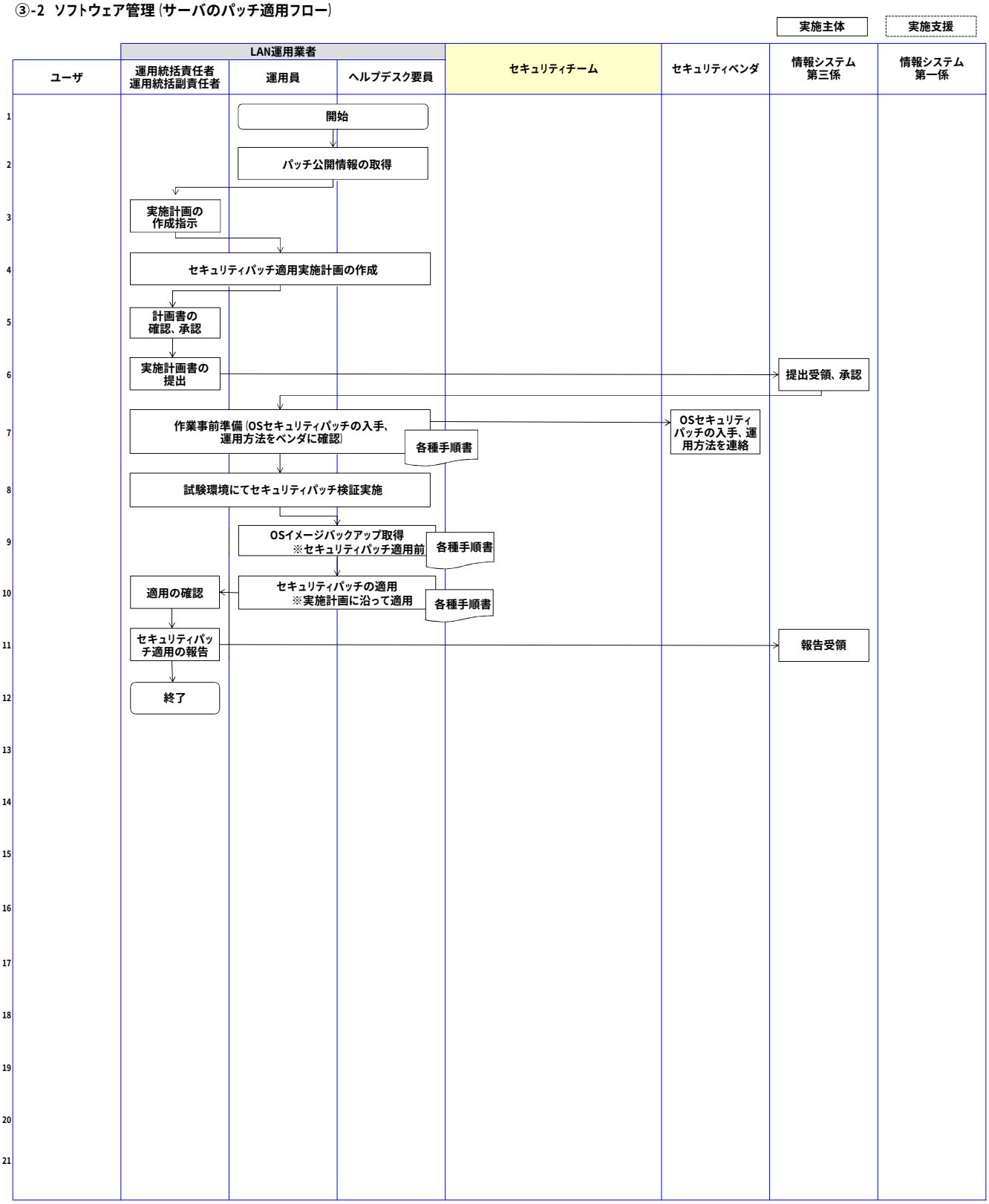
別紙2

③-1 ソフトウェア管理（ソフトウェア障害対応）



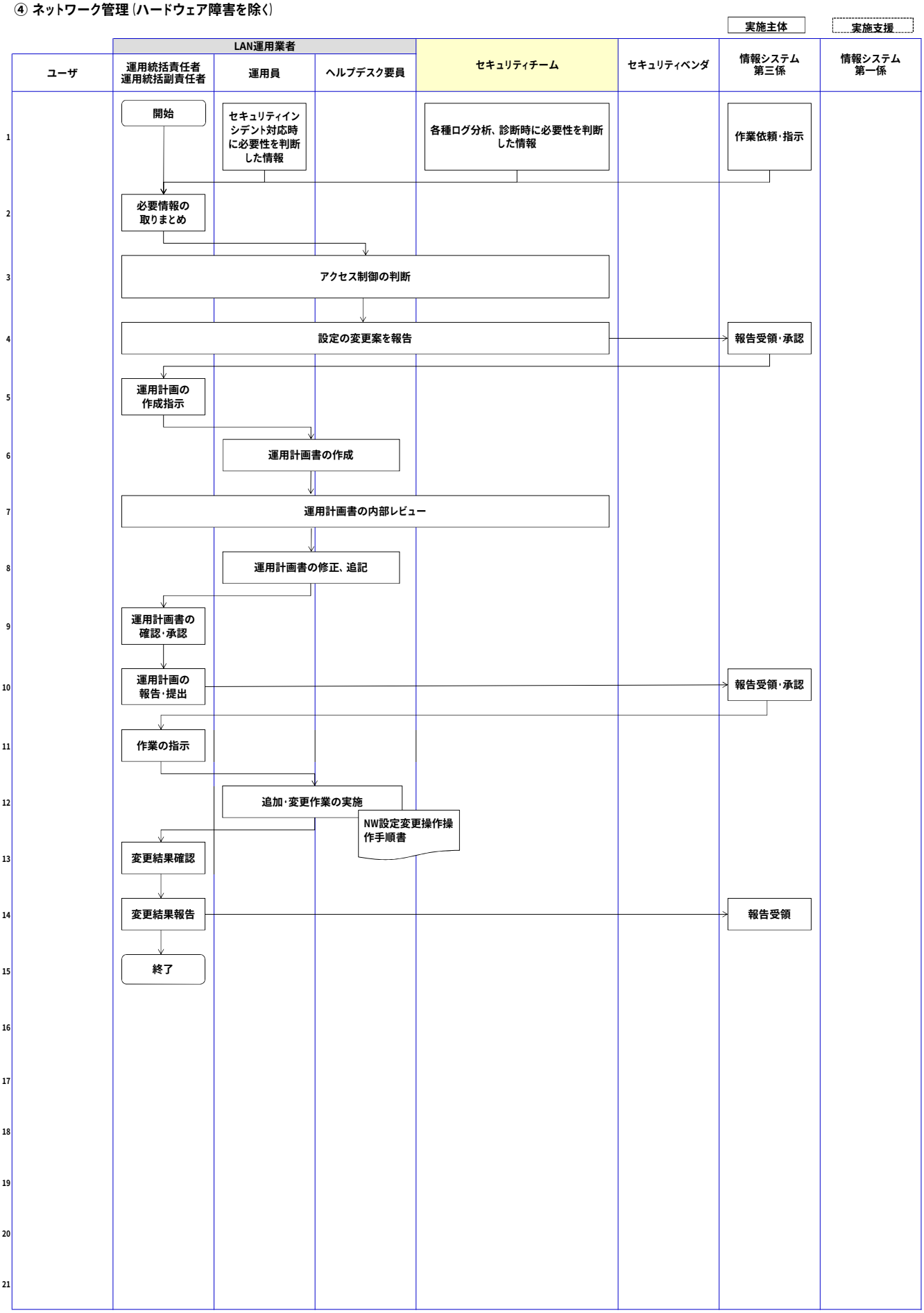
別紙2

③-2 ソフトウェア管理（サーバのパッチ適用フロー）



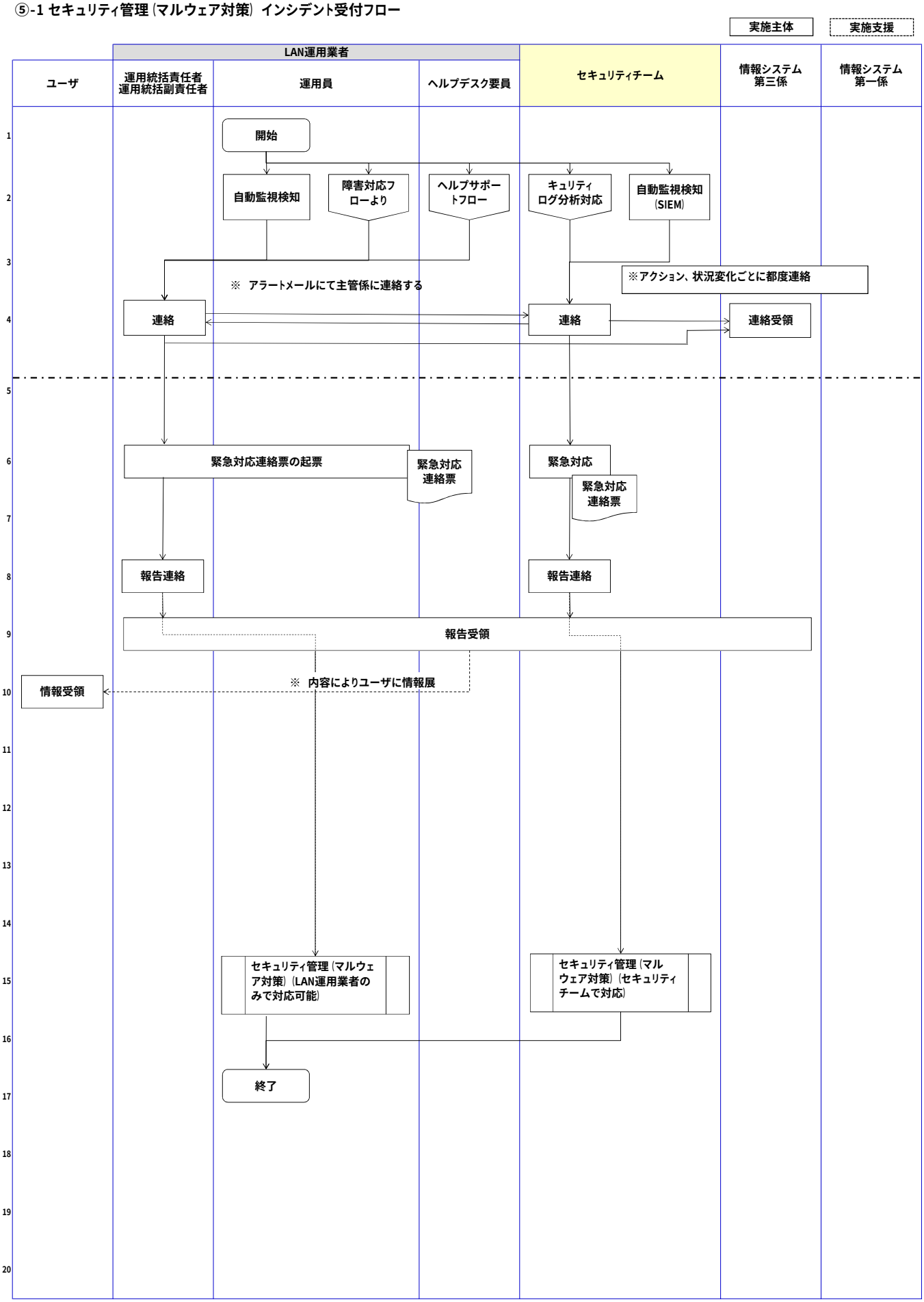
別紙2

④ ネットワーク管理（ハードウェア障害を除く）



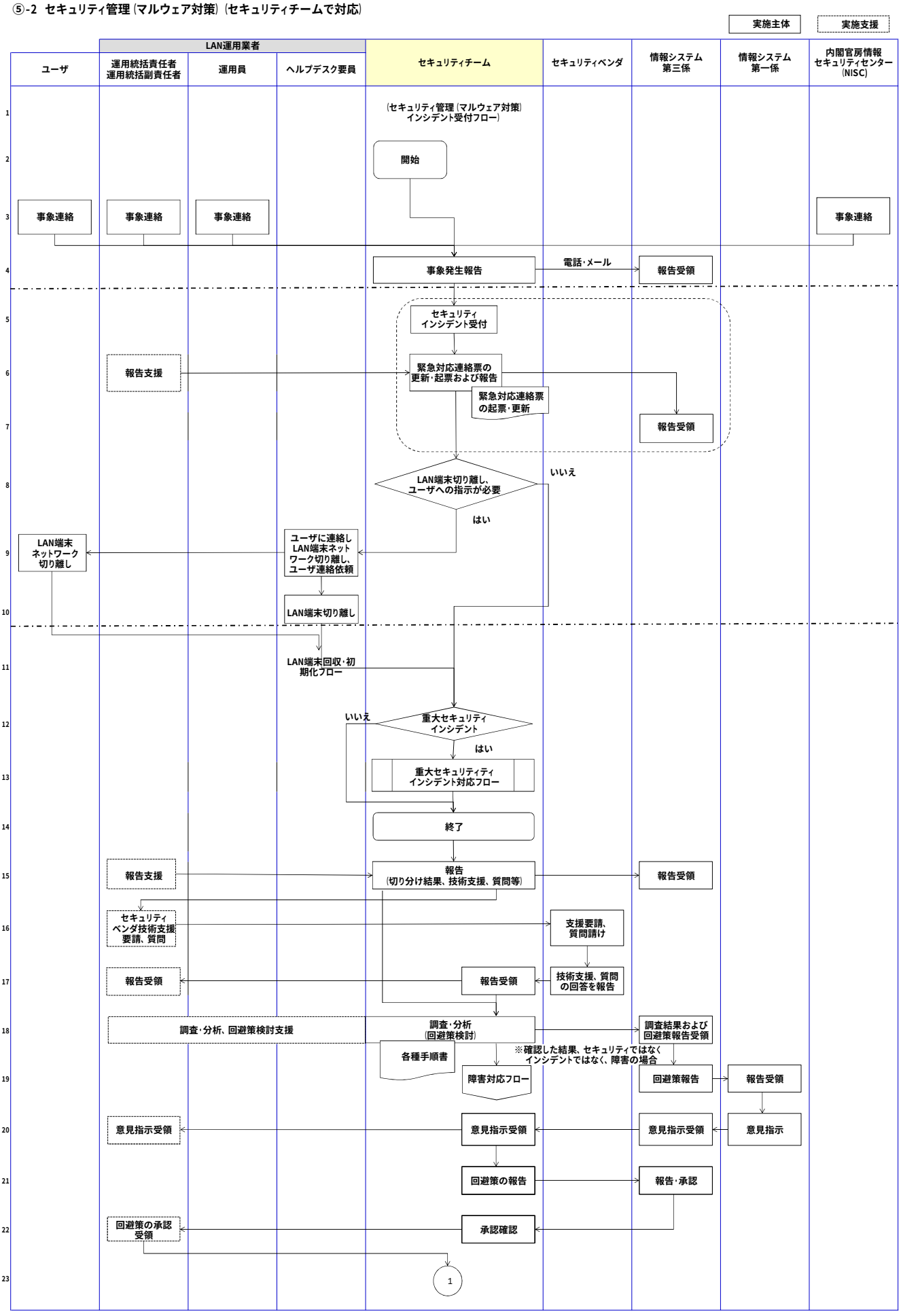
別紙2

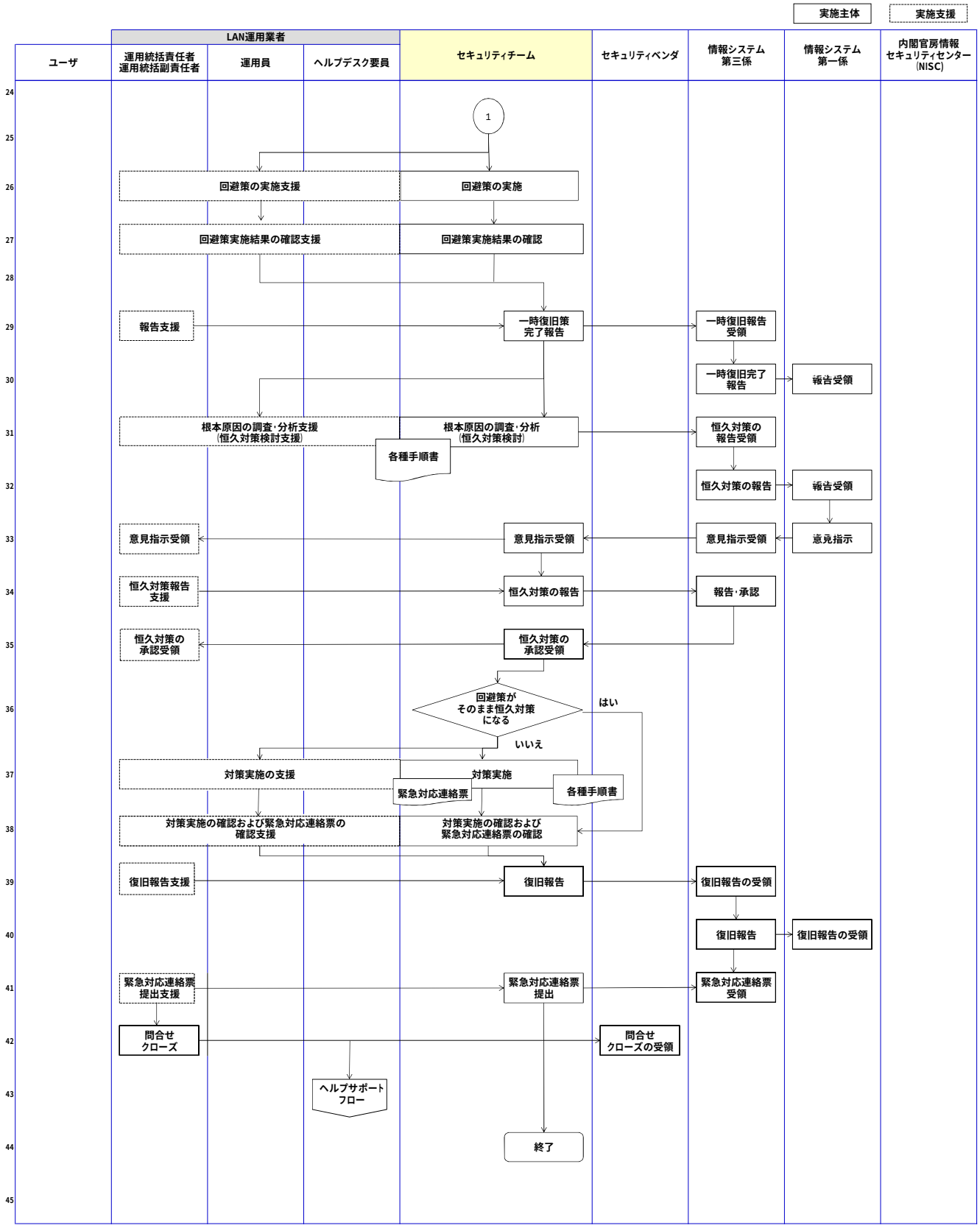
⑤-1 セキュリティ管理（マルウェア対策）インシデント受付フロー



別紙2

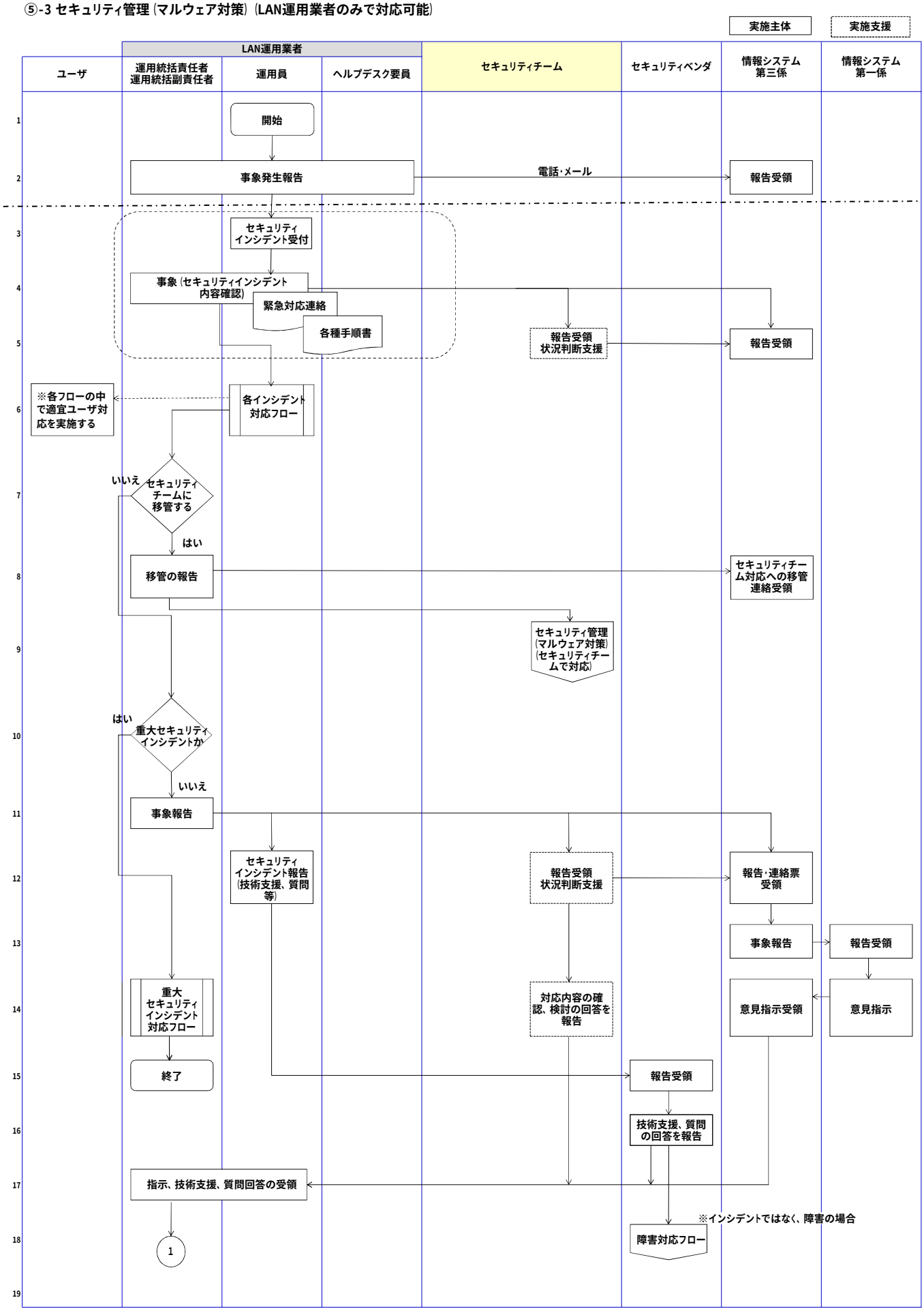
⑤-2 セキュリティ管理（マルウェア対策）（セキュリティチームで対応）

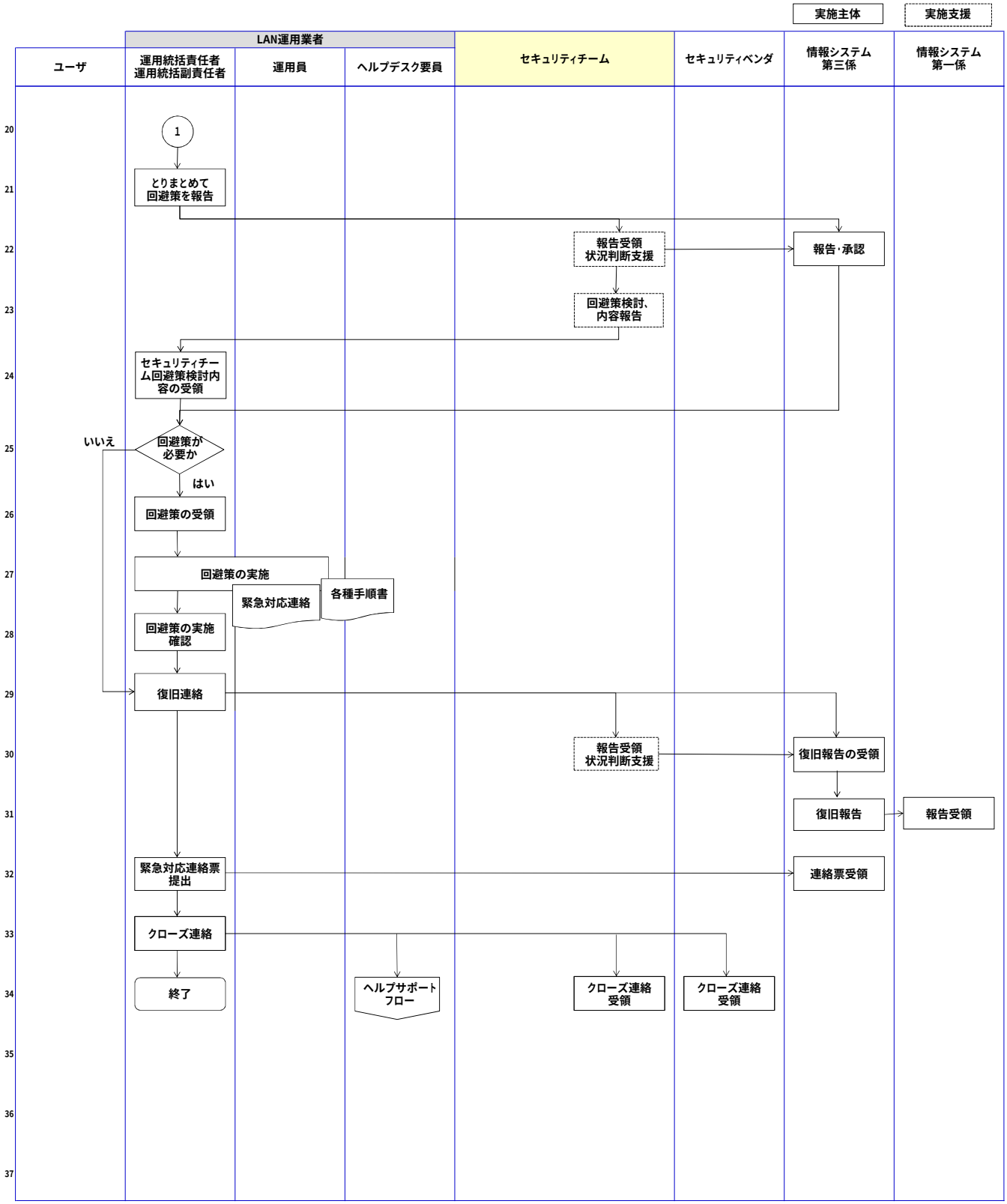



実施主体
実施支援
LAN運用業者
ユーザ
運用統括責任者
運用統括副責任者
運用員
ヘルプデスク要員
セキュリティチーム
セキュリティベンダ
情報システム
第三係
情報システム
第一係
内閣官房情報
セキュリティセンター
(NISC)
1
回避策の実施支援
回避策の実施
回避策実施結果の確認支援
回避策実施結果の確認
報告支援
一時復旧策
完了報告
一時復旧報告
受領
一時復旧完了
報告
報告受領
根本原因の調査・分析支援
(恒久対策検討支援)
根本原因の調査・分析
(恒久対策検討)
各種手順書
恒久対策の
報告受領
恒久対策の報告
報告受領
意見指示受領
意見指示受領
意見指示受領
意見指示
恒久対策報告
支援
恒久対策の報告
報告・承認
恒久対策の
承認受領
恒久対策の
承認受領
回避策が
そのまま恒久対策
になる
はい
いいえ
対策実施の支援
対策実施
緊急対応連絡票
各種手順書
対策実施の確認および緊急対応連絡票の
確認支援
対策実施の確認および
緊急対応連絡票の確認
復旧報告支援
復旧報告
復旧報告の受領
復旧報告
復旧報告の受領
緊急対応連絡票
提出支援
緊急対応連絡票
提出
緊急対応連絡票
受領
問合せ
クローズ
問合せ
クローズの受領
ヘルプサポート
フロー
終了

別紙2

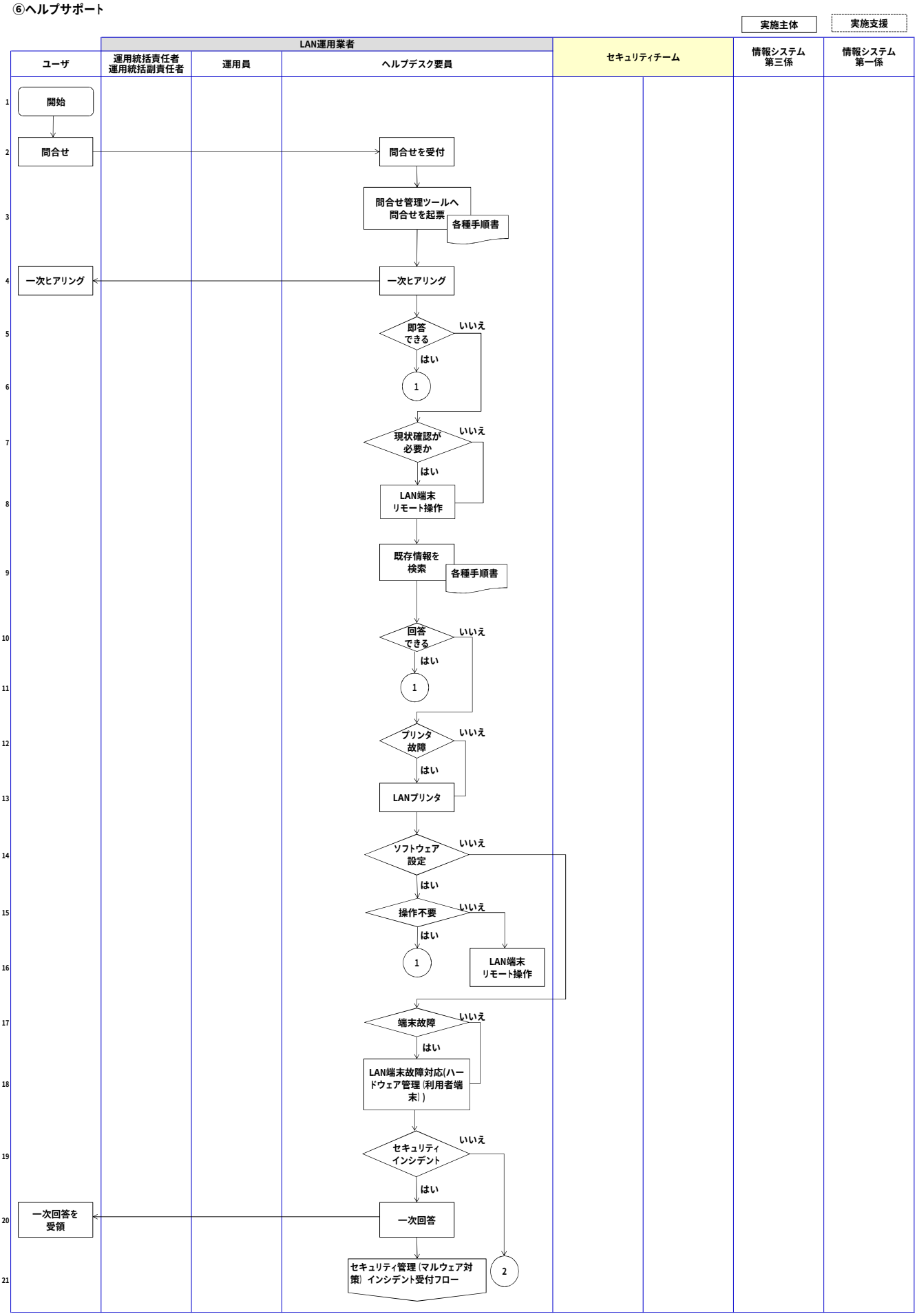
⑤-3 セキュリティ管理（マルウェア対策）（LAN運用業者のみで対応可能）

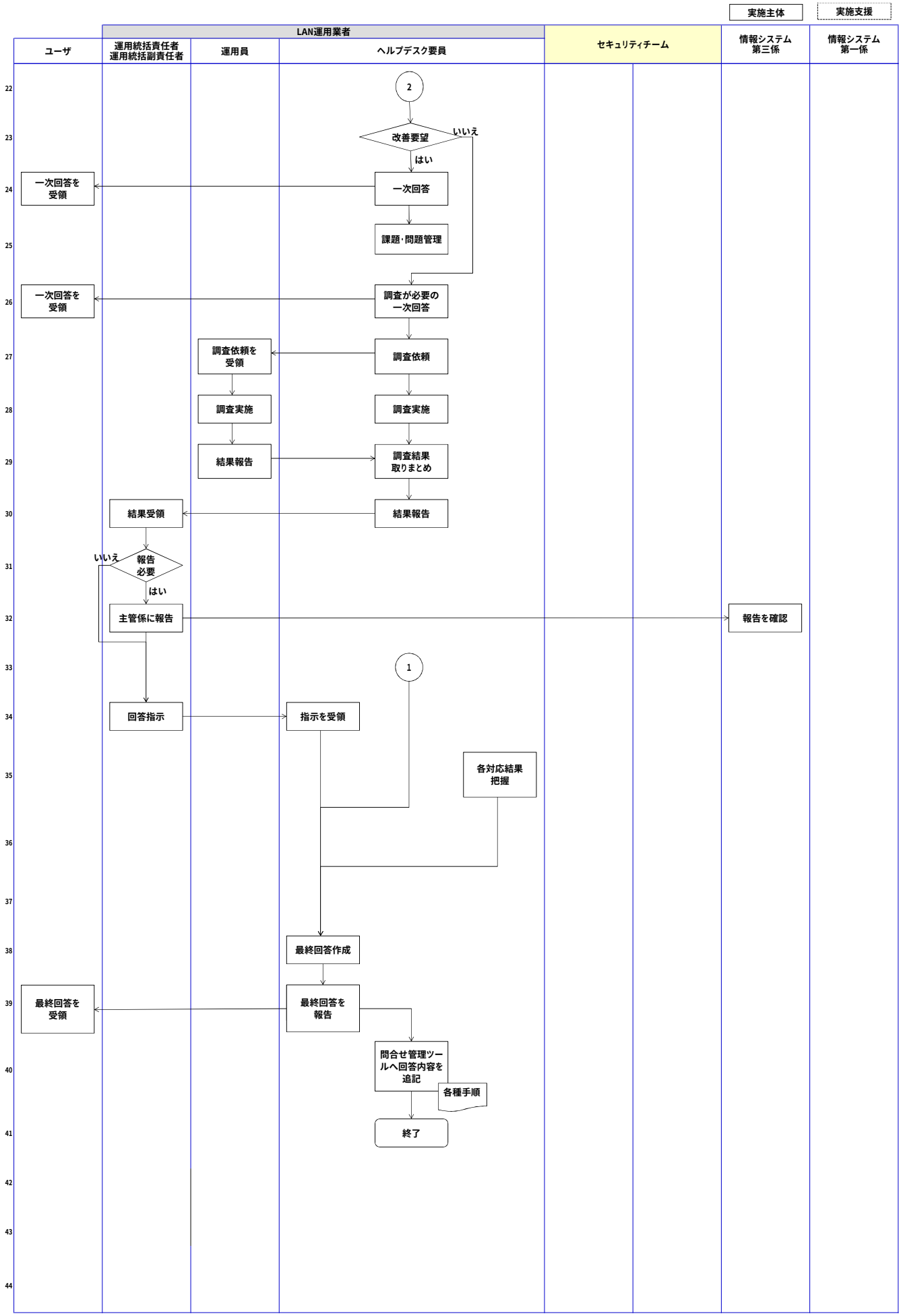



実施主体
実施支援
LAN運用業者
ユーザ
運用統括責任者
運用統括副責任者
運用員
ヘルプデスク要員
セキュリティチーム
セキュリティベンダ
情報システム
第三係
情報システム
第一係
1
とりまとめて
回避策を報告
報告受領
状況判断支援
報告・承認
回避策検討、
内容報告
セキュリティチー
ム回避策検討内
容の受領
いいえ
回避策が
必要か
はい
回避策の受領
回避策の実施
緊急対応連絡
各種手順書
回避策の実施
確認
復旧連絡
報告受領
状況判断支援
復旧報告の受領
復旧報告
報告受領
緊急対応連絡票
提出
連絡票受領
クローズ連絡
終了
ヘルプサポート
フロー
クローズ連絡
受領
クローズ連絡
受領

別紙2

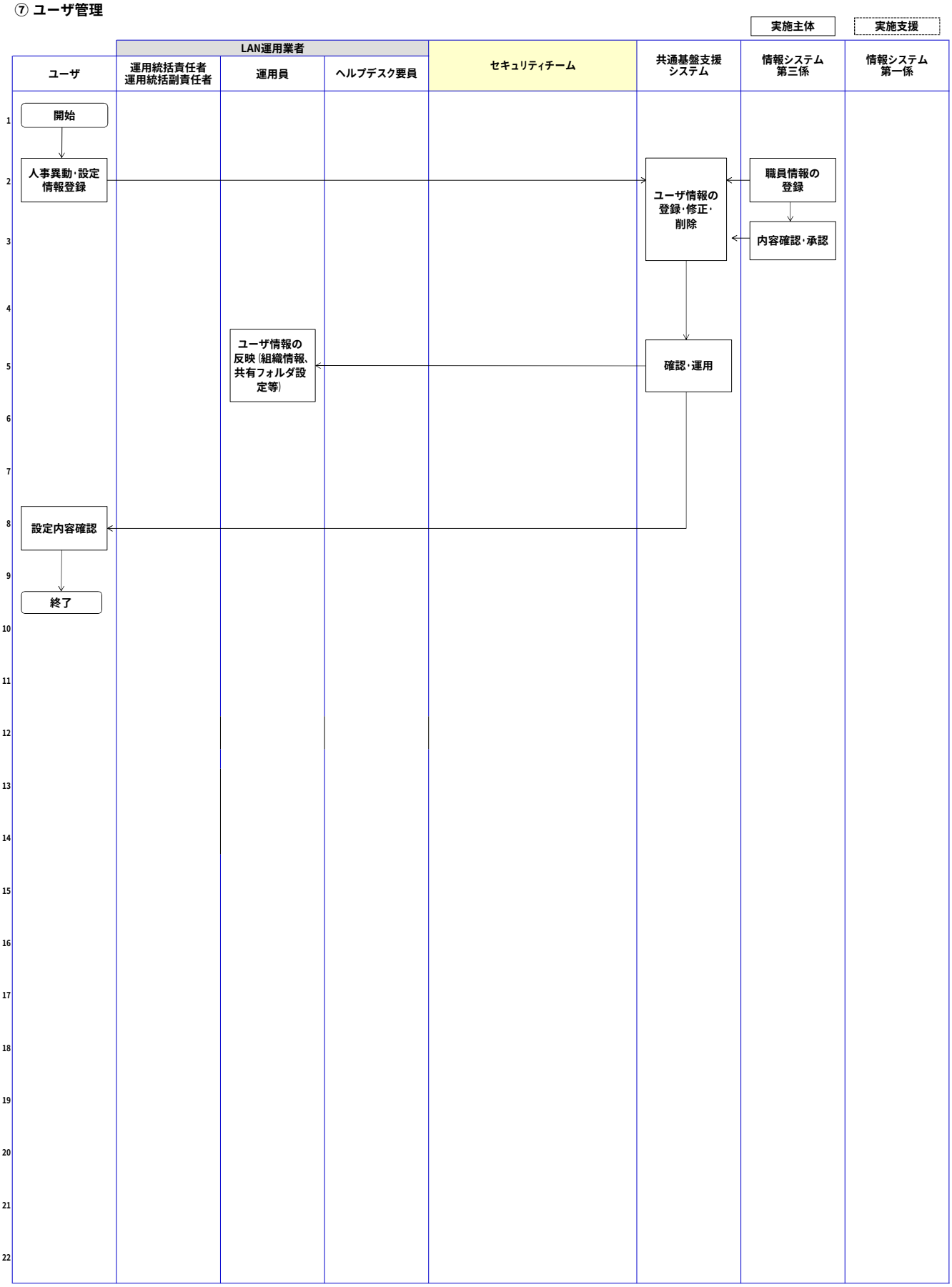
⑥ヘルプサポート




実施主体
実施支援
LAN運用業者
ユーザ
運用統括責任者
運用統括副責任者
運用員
ヘルプデスク要員
セキュリティチーム
情報システム
第三係
情報システム
第一係
2
改善要望
いいえ
はい
一次回答を
受領
一次回答
課題・問題管理
一次回答を
受領
調査が必要の
一次回答
調査依頼を
受領
調査依頼
調査実施
調査実施
結果報告
調査結果
取りまとめ
結果受領
結果報告
いいえ
報告
必要
はい
主管係に報告
報告を確認
1
回答指示
指示を受領
各対応結果
把握
最終回答作成
最終回答を
受領
最終回答を
報告
問合せ管理ツー
ルへ回答内容を
追記
各種手順
終了

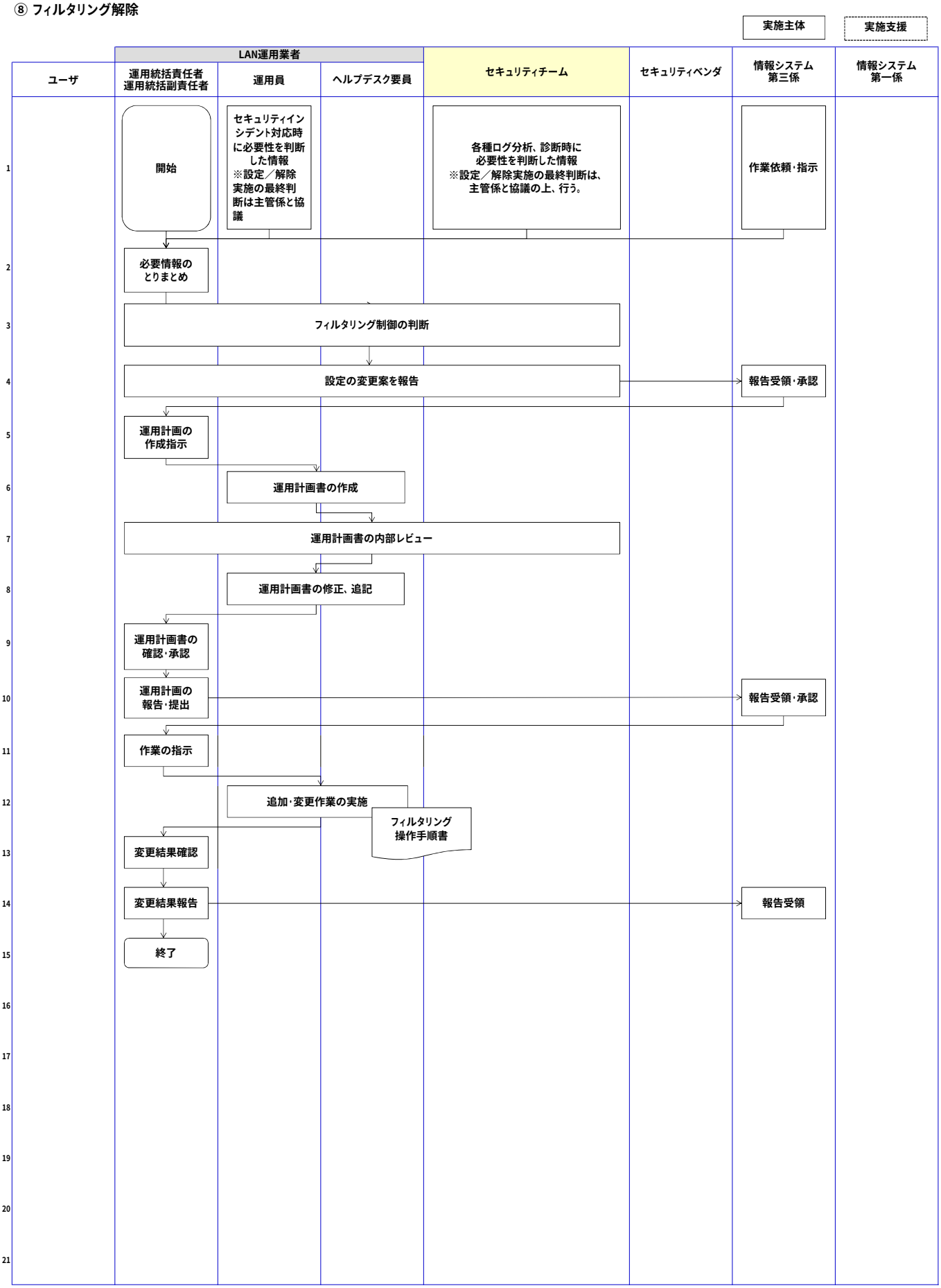
別紙2

⑦ ユーザ管理


実施主体
実施支援
LAN運用業者
ユーザ
運用統括責任者
運用統括副責任者
運用員
ヘルプデスク要員
セキュリティチーム
共通基盤支援システム
情報システム第三係
情報システム第一係
開始
人事異動・設定情報登録
職員情報の登録
ユーザ情報の登録・修正・削除
内容確認・承認
ユーザ情報の反映（組織情報、共有フォルダ設定等）
確認・運用
設定内容確認
終了

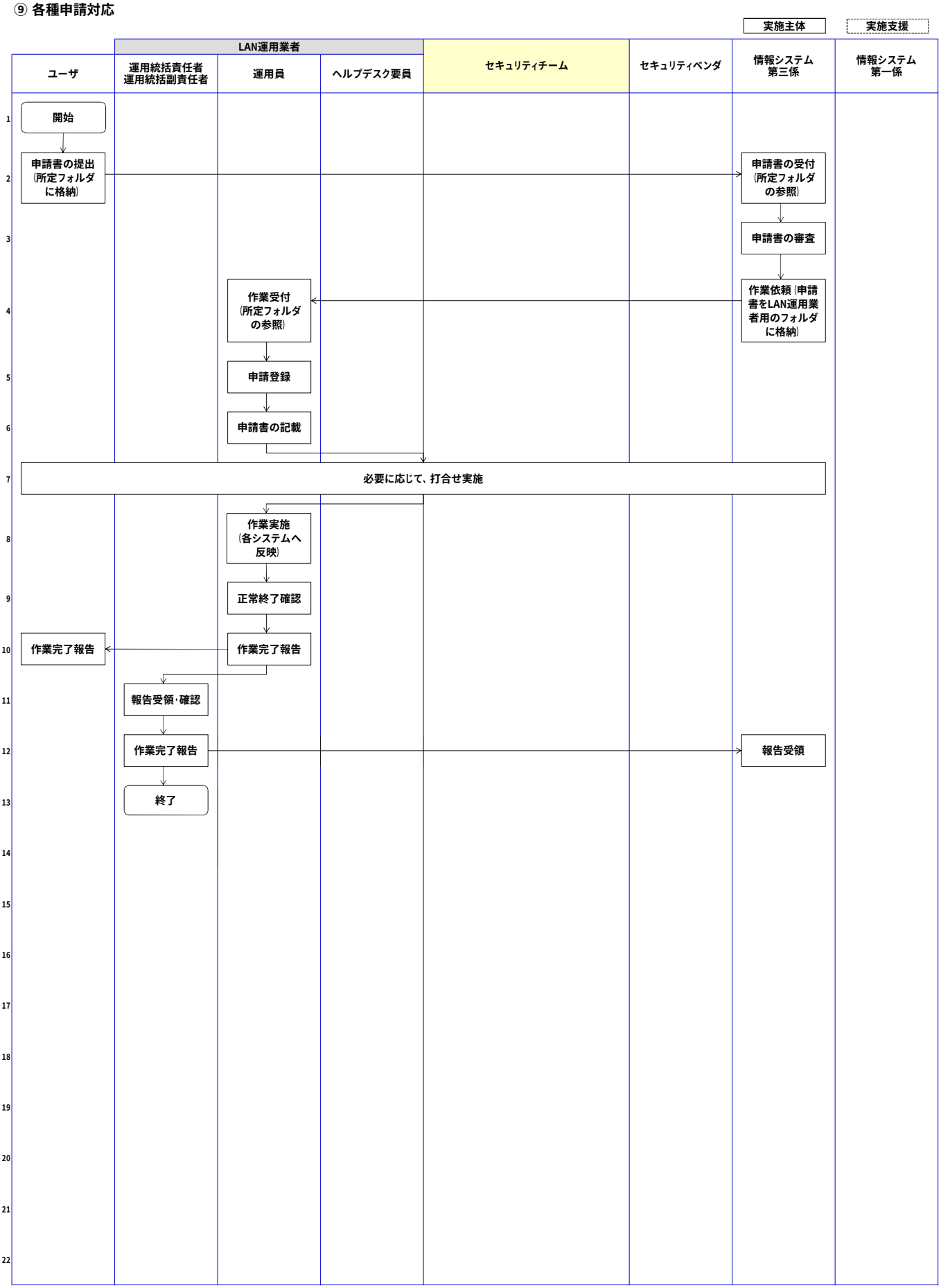
別紙2

⑧ フィルタリング解除



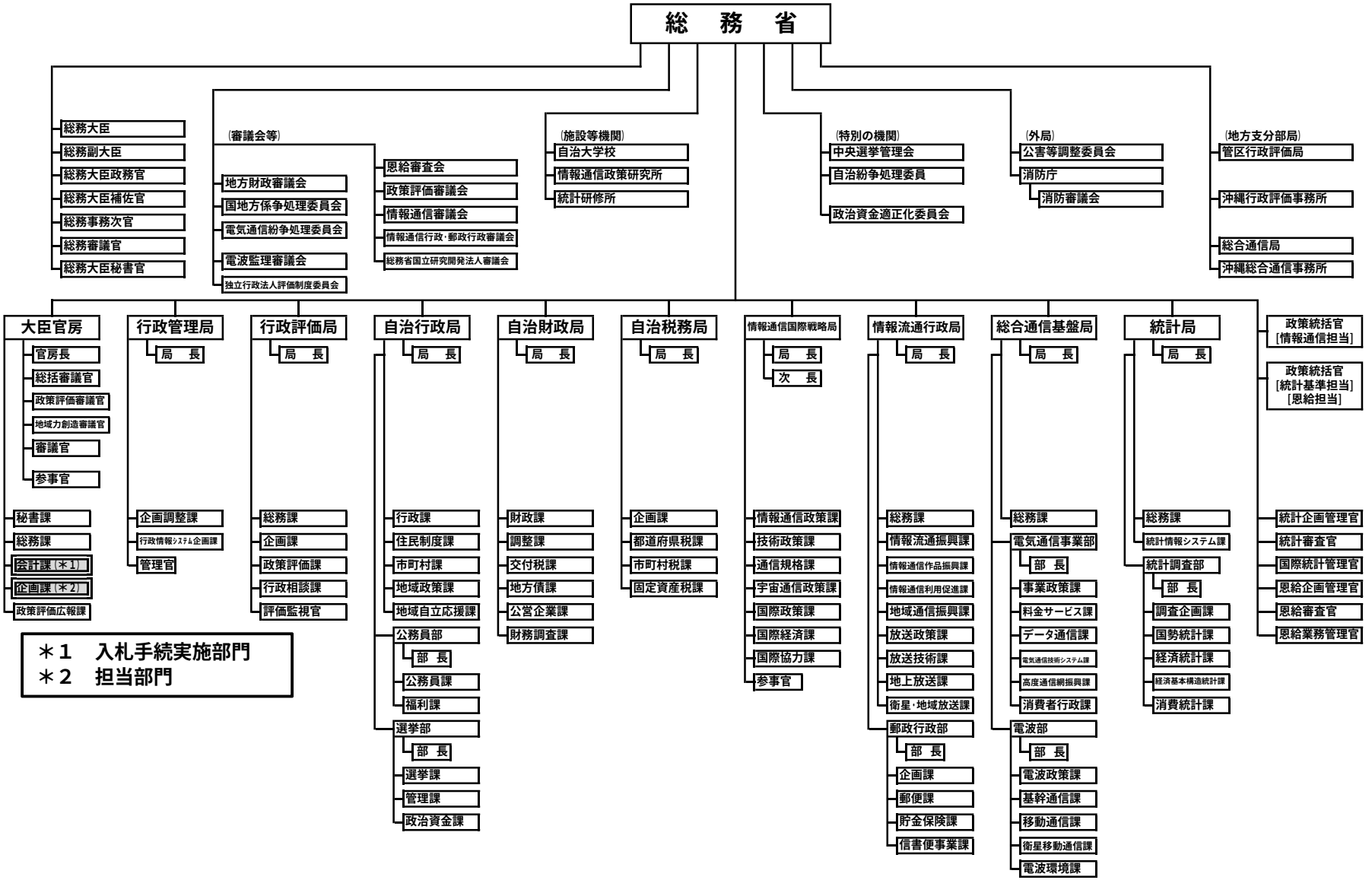
別紙2

⑨ 各種申請対応


実施主体
実施支援
LAN運用業者
ユーザ
運用統括責任者
運用統括副責任者
運用員
ヘルプデスク要員
セキュリティチーム
セキュリティベンダ
情報システム
第三係
情報システム
第一係
開始
申請書の提出
(所定フォルダ
に格納)
申請書の受付
(所定フォルダ
の参照)
申請書の審査
作業受付
(所定フォルダ
の参照)
作業依頼(申請
書をLAN運用業
者用のフォルダ
に格納)
申請登録
申請書の記載
必要に応じて、打合せ実施
作業実施
(各システムへ
反映)
正常終了確認
作業完了報告
作業完了報告
報告受領・確認
作業完了報告
報告受領
終了
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22

総務省の組織 (平成27年度)

別紙3



(注1) 政令職以上の組織を掲げた。

【別紙４】
平成○○年○○月○○日

総務省ＬＡＮの利用に関する満足度アンケート調査

このアンケートは、総務省 LAN について、確保されるべきサービスの質を検討するため、職員利用者を対象に利用満足度を調査するものです。

つきましては、次の４つの質問に対して、それぞれ「満足」から「不満」までのいずれかに該当する□にレ印を記入してください。

１　お問合せから回答までに要した時間について満足されましたか。

□満足　□ やや満足　□普通　□やや不満　□不満

２　回答又は手順に対する説明の分かりやすさについて満足されましたか。

□満足　□ やや満足　□普通　□やや不満　□不満

３　回答又は手順に対する結果の正確性について満足されましたか。

□満足　□ やや満足　□普通　□やや不満　□不満

４　担当者の対応（言葉遣い、親切さ、丁寧さ等）について満足されましたか。

□満足　□ やや満足　□普通　□やや不満　□不満

＜ ご意見等 ＞

ご協力ありがとうございました。

別紙５

総務省大臣官房企画課長　殿

機 密 保 持 に 関 す る 誓 約 書

「総務省ＬＡＮシステムの更新整備及び運用管理業務民間競争入札実施要項」７（２）による従来の当該業務に係る各種書類を閲覧するに当たり、同 ４に記載の入札参加資格に関する事項を全て満たした上で資料閲覧の申込みを行い、かつ、下記の事項を厳守することを、ここにお誓い致します。

記

１　総務省の情報セキュリティに関する規程等を遵守し、総務省が開示した情報（公知の情報等を除く）を本件調達の目的以外に使用又は第三者に開示若しくは漏えいしないものとし、そのために必要な措置を講ずることを約束致します。

２　１に違反して、情報の開示、漏えい若しくは使用した場合、法的な責任を負うものであることを確認し、これにより総務省が被った一切の損害を賠償することを約束致します。

平成　　年　　月　　日
住　　所
会 社 名
代表者名　　印

総務省ＬＡＮシステムの更新整備及び運用管理業務

民間競争入札実施要項（案）

別紙６　資料閲覧要領

総務省大臣官房企画課情報システム室

【更新履歴】

No.	更新の概要	更新責任者	更新日付
1			
2			
3			
4			
5			
6			

目次

１　本文書の位置付け

本文書は、「総務省ネットワーク基盤（ＬＡＮ）の構築等の請負」の調達において、応札を希望する事業者が提案書を作成するに当たり、参考となる資料（プロジェクト計画書、遵守するべき規程、各種設計書等）の閲覧要領を示したものである。

２　資料閲覧要領

(１)閲覧場所

総務省大臣官房企画課情報システム室内

(２)閲覧期間及び時間

第１回目　平成 27 年 11 月２日、４日～６日　10 時～17 時

第２回目　平成 28 年 １月中旬～下旬

(３)閲覧手続

応札希望者の商号、連絡先、閲覧希望者氏名等を別紙７「資料閲覧申込書」に記載の上、閲覧希望日の５日前までに提出すること。また、閲覧日当日までに別紙５「機密保持に関する誓約書」に記載の上、提出すること。

(４)閲覧時の注意

閲覧にて知り得た内容については、提案書の作成以外には使用しないこと。また、本調達に関与しない者等に情報が漏えいしないように留意すること。閲覧資料の複写等による閲覧内容の記録は行わないこと。

(５)連絡先

総務省大臣官房企画課情報システム室情報システム第三係

電話 03－5253－5159

3　事業者が閲覧できる資料一覧表

応札を希望する事業者は、本要領で示す手順に従って、現行総務省ＬＡＮの納入成果物であるプロジェクト計画書、遵守するべき規程、各種設計書等を閲覧することができる。

閲覧対象の文書を、「表 3-1　閲覧対象文書の一覧」に示す。

表 3-1　閲覧対象文書の一覧（現行総務省ＬＡＮの納入成果物）

No	分類	完成図書名	内容	資料閲覧での閲覧対象	
				第１回目	第２回目
1	プロジェクト管理	プロジェクト計画書	プロジェクト実施に当たっての目的、前提、体制、全体スケジュール、連絡体制、会議計画、コミュニケーション方法等を記載した文書。プロジェクト運営に当たって要となる文書。		○
2		情報管理計画書	情報の取扱者、情報の保護・管理のための教育・周知の計画内容、情報の取扱い要領、作業場所における情報セキュリティ確保のための措置、情報セキュリティが損なわれた場合の対応計画について記載した文書。		○
3		情報管理簿	主管課から貸与を受けた各種ドキュメント、電子データ類の授受方法、保管場所、保管方法、使用場所、使用目的等取扱い方法を明確に記載した文書。		○
4		スケジュール表	プロジェクト全体のマイルストーンや日程の全体規模感を記載した全体スケジュールと、各フェーズでの詳細作業を記載した詳細スケジュールのこと。	○	○

No	分類	完成図書名	内容	資料閲覧での閲覧対象	
				第１回目	第２回目
5		ＷＢＳ	プロジェクトで実施すべきすべての作業を、適切なワークパッケージに分解して階層的に表した文書。		○
6		課題管理表	各種課題の管理を行うため、課題の内容、対処方法、対応担当者、実施時期等について記録した文書。		○
7		リスク管理表	プロジェクト実施に当たってのリスクの管理を行うため、リスクの内容、対処方法、対応担当者、実施時期等について記録した文書。		○
8		変更管理表	プロジェクト実施中に変更になった事項について管理を行うため、変更の内容、対処予定、実施時期等を記録した文書。		○
9		品質管理報告書	本調達で作成する総務省ＬＡＮサービス一式及び完成図書の品質管理を行うためのレビュー実施記録を記載した文書。		○
10		会議アジェンダ	会議の議題一覧を記載した文書。		○
11		会議議事録	会議の議事録を記載した文書。		○
12		プロジェクト完了報告書	プロジェクト中の各作業の実施日時や内容及び結果を記載した文書。		○
13	設計・構築	設計・構築計画書	設計・構築実施に当たっての体制、詳細スケジュール、作業内容等を記載した文書。		○

No	分類	完成図書名	内容	資料閲覧での閲覧対象	
				第１回目	第２回目
14		システム概要説明資料	主管課が総務省ＬＡＮのシステム概要を把握するための提供サービス内容、規模感、拠点情報、運用情報等を記載した文書。	○	○
15		基本設計書	本調達の提供するサービス全体の設計内容を記載した文書。	○	○
16		詳細設計書	各サービス提供で必要となる詳細な設計を記載した文書。パラメータ等も含む。		○（＊）
17		回線導入計画書	インターネット回線やＷＡＮ回線の導入に当たっての体制、詳細スケジュール、作業内容等を記載した文書。		○
18		回線一覧	インターネット回線やＷＡＮ回線の回線速度や種別の一覧を記載した文書。		○
19		回線導入報告書	回線導入の結果や報告を記載した文書。		○
20		ファシリティ設計書	ラック構成等のファシリティの設計内容を記載した文書。		○
21	試験	試験実施計画書	単体・結合・総合試験実施に当たっての体制、詳細スケジュール、試験環境等を記載した文書。		○
22		試験仕様書	単体・結合・総合試験実施計画に基づき、試験方針、試験項目、試験方法、合否判定基準を定めた文書。		○（＊）
23		試験結果報告書	単体・結合・総合試験の各結果及び全体の報告、統計的な分析を行った結果を記載した文書。		○（＊）

No	分類	完成図書名	内容	資料閲覧での閲覧対象	
				第１回目	第２回目
24		受入試験実施計画書	受入試験実施に当たっての体制、詳細スケジュール、試験環境等を記載した文書。		○
25		受入試験仕様書	受入試験実施計画に基づき、試験方針、試験項目、試験方法、合否判定基準を定めた文書。		○（＊）
26	移行・教育訓練	移行実施計画書	移行の体制、方針、詳細スケジュール、移行環境、移行方法等を記載した文書。		○
27		展開実施計画書	展開の体制、方針、詳細スケジュール、展開方法等を記載した文書。		○
27		展開事前調査報告書	本省及び各拠点の展開に必要な情報を記載した文書。配線、ラック等の状況をまとめたもの。		○
29		工事前調査報告書	工事実施に当たって、工事に必要な情報を記載した文書。ＬＡＮ敷設、電源敷設用の設計図等をまとめたもの。		○
30		移行設計書	移行実施に当たって、対象データ範囲や整備方法、具体的な作業内容を設計した文書。移行判定項目や移行判定基準等も含む。		○
31		移行手順書	作業体制、連絡先一覧とバックアップ等準備作業、移行・導入作業、事後作業等の作業項目、操作対象、操作方法を記載した文書。想定時間等を明確したタイムチャートやトラブル発生時の切戻し（フォールバック）手順を含む。		○（＊）

No	分類	完成図書名	内容	資料閲覧での閲覧対象	
				第１回目	第２回目
32		展開手順書	機器設置や展開作業を行うための手順が記載された文書。展開が正しく行われたことの確認手順も含む。		○
33		ユーザ移行手順書	移行実施に当たってユーザが実施する作業手順をまとめた文書。		○
34		移行結果報告書	移行作業について、移行実施設計書に記載の判定項目・判定基準に沿った結果を記載した文書。		○
35		教育訓練実施計画書	教育訓練実施に当たっての体制、詳細スケジュール、訓練環境及び訓練方法等を記載した文書。		○
36		教育訓練用教材	現行総務省ＬＡＮサービスの利用方法をユーザに教育訓練するため、手順や解説等が記載された文書。本文書はユーザが総務省ＬＡＮを使うマニュアルとなる。		○
37		教育訓練実施報告書	教育訓練作業の実施日時や内容・結果、教育訓練の習熟度分析等を記載した文書。		○
38	運用・保守	サービスレベル合意書	総務省側と請負者側の責任分解点や役割を明確にし、必要な管理項目とサービスレベル管理指標の保証値等について記載した文書。	○	○
39		運用・保守要領	運用・保守を行う上での指針・基準となる項目を記載した文書。	○	○
40		運用・保守実施計画書	システム運用の実施に当たっての体制、詳細スケジュール、作業内容等を記載した文書。	○	○

No	分類	完成図書名	内容	資料閲覧での閲覧対象	
				第１回目	第２回目
41		運用・保守設計書	システム運用・保守の対象や方法について記載した文書。	○（＊）	○（＊）
42		運用・保守手順書	運用要員が運用・保守を行う上での手順や解説等を記載した文書。		○
43		運用報告書	システム操作や監視の実施状況、障害状況、サービス指標実績値、ヘルプデスク運用状況の報告や分析等の運用状況を記載した文書。	○（＊）	○（＊）
44		保守報告書	ハードウェアの定期点検やソフトウェアの脆弱性対策等の保守状況を記載した文書。		○（＊）
45		セキュリティ報告書	セキュリティ監視、分析、対策状況等を記載した文書。		○（＊）
46		ＳＬＡ報告書	ＳＬＡの達成率や状況の分析、未達成が継続された場合は改善策等のＳＬＡ管理状況を記載した文書。		○（＊）
47		ハードウェア管理台帳	各サーバ・端末・ネットワーク機器の機種名や型番等の情報を記載した文書。		○
48		ソフトウェア管理台帳	各サーバ・端末・ネットワーク機器にインストールされているソフトウェアの名称、バージョン、メーカ名等の情報を記載した文書。		○
49		ライセンス管理台帳	現行総務省ＬＡＮで管理するすべてのライセンスの名称や期限等の利用状況を一覧にして記載した文書。		○
50		ネットワーク構成情報管理台帳	ＩＰアドレス、ＭＡＣアドレス、ホスト名等、サーバ及び端末に係るネットワーク情報を管理した文書。		○（＊）

No	分類	完成図書名	内容	資料閲覧での閲覧対象	
				第１回目	第２回目
51		フロアレイアウト図	フロア内の機器の場所や機器の配置状況のわかる写真等をまとめた文書。		○
52		課題管理表	システム運用時に発生した課題の内容、対処方法、対応担当者、実施時期等について記録した文書。		○（＊）
53		運用管理用文書	上記資料以外で運用管理上、必要となる文書。 ・運用計画書（個別の作業を記録） ・入退室管理表 等		○
54		変更管理台帳	運用実施に際し変更が生じた資料の変更履歴を示す文書。		○（＊）
55		情報システム運用継続計画	総務省ＬＡＮにおける情報システム運用継続計画を記載した文書。		○（＊）
56	その他 会議資料	全体定例会資料 個別会議資料 分科会会議資料	各種会議資料		○
57	調査･研究時の資料		平成 26 年度に実施した次期総務省ＬＡＮに係る調査･研究業務の納入成果物のうち、要件定義の前提となる文書。		○（＊）

（＊）開示することを前提とするが、情報セキュリティや個人を特定できる機微情報に関わるものについては、項目のみ、黒塗り、抜粋などを行った上で閲覧可能とする。

別紙７

平成　　年　　月　　日

資料閲覧申込書

会社名		
部署名		
担当者名		
電話番号		
E-mail アドレス		
閲覧希望日時	第一希望	第二希望
閲覧者人数 （最大５名まで）		
閲覧者氏名		

調達件名　：　総務省ネットワーク基盤（ＬＡＮ）の構築等の請負

提 出 日	
会 社 名	
代表者名	
部 署 名	
担当者名	
住　　所	
電話番号	
ＦＡＸ番号	
E-mail	

質問の総数	

項	頁番号	行番号	項 目	種 別	質　　問　　等	理　　由
1						
2						
3						

〔別紙8〕質問票

項	頁番号	行番号	項 目	種 別	質　　問　　等	理　　由
4						
5						
6						
7						

注）１．種別欄には、質問の種類を以下から選択して、その番号を記載すること。
　　［１．調達仕様書に対する質問等。　２．証明書作成要領に対する質問等。　３．その他］
　２．質問等及び、理由は、明確かつ簡潔に記載すること。
　３．本様式の変更は、行わないこと。

別添１

総務省ネットワーク基盤（ＬＡＮ）の
構築等の請負
調達仕様書

（案）

総務省大臣官房企画課情報システム室

－ 目 次 －

第１　調達案件の概要に関する事項

１　調達件名

総務省ネットワーク基盤（ＬＡＮ）の構築等の請負

(Construction of MIC's computer-network infrastructure.)

２　調達の背景

総務省においては、「総務省情報ネットワーク（共通システム）最適化計画」（平成17年６月29日総務省行政情報化推進委員会決定平成23年８月26日改定）に基づき、総務省職員が行政の組織活動を実施するための基盤システムとなる「総務省ネットワーク基盤（ＬＡＮ）」（以下「総務省ＬＡＮ」という。）を整備し、現在稼働中の総務省ＬＡＮ（以下「現行総務省ＬＡＮ」という。）が第３期ＬＡＮとして平成25年４月から運用を開始しているところである。

平成29年４月から運用開始を予定している総務省ＬＡＮ（以下「次期総務省ＬＡＮ」という。）では、「経済財政運営と改革の基本方針2015」（平成27年６月閣議決定）、「『日本再興戦略』改訂2015」（平成27年６月閣議決定）、「世界最先端IT国家創造宣言」（平成25年６月閣議決定、平成27年６月変更閣議決定）、「首都直下地震緊急対策推進基本計画」（平成27年３月閣議決定）、「サイバーセキュリティ戦略」（平成27年９月閣議決定）等の政府方針に基づき、サイバーセキュリティ対応能力及び基盤の強化を図るとともに、行政のＩＴ化と業務改革、働き方改革の実行・実現を推進するための基盤環境の整備や情報システムの事業継続性を向上し安全性と信頼性を確保するための業務継続性を考慮したディザスタリカバリサイト（以下「ＤＲサイト」という。）の整備を図ることが急務となっている。

３　目的及び期待する効果

本システムの整備によって、基盤システムの安定性と信頼性を向上させ、公務におけるワークスタイル変革、業務処理の電子化・共通化、職員の多様で柔軟な働き方を推進し公務の生産性を高めるとともに、大規模災害時における行政運営の継続性を確保する。また、情報セキュリティ対策を強化し、安全・安心なＩＣＴ環境の下で、総務省職員が行政の組織活動をコミュニケーション良く効率的・生産的に行える環境を整備するものである。

４　用語の定義

本調達仕様において使用する用語を表１-１に示す。

表１-１　用語の定義

No.	用語	定義
1	総務省ＬＡＮ	総務省職員が行政の組織活動を実施するための基盤システム。
2	現行総務省ＬＡＮ	平成25年４月から運用している現行の総務省ＬＡＮ。
3	次期総務省ＬＡＮ	平成29年４月から運用開始を予定している総務省ＬＡＮ。

No.	用語	定義
4	政府共通ネットワーク	政府機関内における情報の円滑な流通、情報共有等を図るため、各利用機関のＬＡＮを相互に接続する政府専用のネットワーク。総務省行政管理局が運営・管理を行う。
5	政府共通プラットフォーム	政府情報システムの統合・集約化の基盤及びデータ連携の基盤。総務省行政管理局が運営・管理を行う。政府情報システム改革ロードマップに基づき、総務省の各部局が運用している個別業務システムが順次、政府共通プラットフォームに移行する。
6	個別業務システム	各部局がその所掌する業務を遂行するために個別に設置しているシステムの総称。
7	総務省共通基盤支援システム	府省共通の情報システム（一元的な文書管理システム、職員等利用者共通認証基盤（ＧＩＭＡ)及び省内の各種情報システム(総務省ＬＡＮ、個別業務システム)と総務省職員情報の連携やシングルサインオンを行うためのシステム。
8	職員等利用者共通認証基盤（ＧＩＭＡ）	各府省の業務・システムを利用する際の本人性確認等に必要な利用者認証情報及びユーザ認証機能を一元的に管理・提供する認証基盤であり、総務省共通基盤支援システムがＧＩＭＡと情報連携を行っている。
9	仮想デスクトップ環境	タブレット型端末等で、デスクトップ仮想化用サーバにログオンすることにより総務省ＬＡＮの各種サービスを利用可能となる環境。タブレット型端末等にはデスクトップ仮想化用サーバの画面情報だけが表示されるため、総務省ＬＡＮのデータはタブレット型端末等に残らない。
10	サーバＯＳ環境	サーバに対して、ＷｉｎｄｏｗｓＳｅｒｖｅｒ等のサーバＯＳの導入が可能となる環境。
11	申請アプリケーション	職員又は部局の申請が許可された後に、個別に導入されるアプリケーション。
12	ローカルバックアップ	同一筐体内又は冗長機器内でデータをバックアップする方式。
13	遠隔地バックアップ	総務省ＷＡＮを経由した別拠点においてデータをバックアップする方式。
14	ＬＡＮ端末	総務省大臣官房企画課情報システム室が各部局に配備し、執務室において業務を行うための端末。ＬＡＮ端末は、本調達とは別に調達を実施している。なお、次期ＬＡＮで動作させるための再設定等は、調達範囲である。
15	タブレット型端末	ペーパーレス会議で利用するタブレット型端末と、テレワークで利用するタブレット型端末の２種類がある。ペーパーレス会議用のタブレット型端末は、本調達とは別に調達を実施する。なお、次期ＬＡＮで動作させるための再設定等は、調達範囲である。

No.	用語	定義
16	ウイルスチェック用端末	外部から、電磁的記憶媒体による電子データの受取りを行う場合に、ウイルスチェックを行う端末。ウイルスチェック用端末から総務省ＬＡＮに接続することは原則禁止としている。なお、ウイルスチェック用端末は既存流用可であるが、次期ＬＡＮで動作させるための再設定等は、調達範囲である。
17	シンクライアントデバイス	個人所有端末へ接続することで、総務省省外から省内の仮想デスクトップ環境にアクセスが可能となるデバイス。
18	ＬＡＮ複合機・プリンタ	総務省ＬＡＮで管理されている複合機及びプリンタ。ＬＡＮ複合機・プリンタは、本調達とは別に調達を実施している。なお、次期ＬＡＮで動作させるための再設定等は、調達範囲である。
19	コアスイッチ	本省ＬＡＮにおいて各セグメントのスイッチを集約し、拠点ＬＡＮでは、エッジスイッチとフロアスイッチを集約するスイッチ。拠点ＬＡＮに関しては、ＬＡＮ端末やＬＡＮ複合機・プリンタを集約する際に利用する場合もある。
20	フロアスイッチ	同一フロア内にあるエッジスイッチを集約するスイッチ。ＬＡＮ端末やＬＡＮ複合機・プリンタを集約する際に利用する場合もある。
21	エッジスイッチ	ＬＡＮ端末、ＬＡＮ複合機・プリンタを集約するスイッチ。
22	総務省公開サーバ	総務省が外部向けに公開しているＷｅｂサイト等の情報が格納されたサーバ。なお、Ｗｅｂサイトの管理は本調達に含まない。また、次期ＬＡＮで動作させるための再設定等は、調達範囲である。
23	ユーザ管理ＤＢサーバ	ユーザアカウントのＩＤ、パスワード等の情報が格納されたデータベースサーバ。
24	ＵＳＢデバイス	ＵＳＢ接続により利用する機器全般。
25	システム室ＵＳＢメモリ	ウイルスチェック用端末で行ったウイルスチェックにおいて、問題が発生しなかった電子データをＬＡＮ端末へ移動するためのセキュリティ機能付きＵＳＢデバイス。
26	外部記憶デバイス	ＬＡＮ端末で電子データの読み取り又は書き込みすることで、電子データの移動を行うためのデバイス。
27	外部拠点	総務省第２庁舎（統計局、政策統括官、統計委員会）、公害等調整委員会、内閣人事局、永田町合同庁舎（情報公開・個人情報保護審査会、官民競争入札等管理事務局、公共サービス改革推進室）、行政管理局宮城分室、行政管理局大阪分室、自治大学校、情報通信政策研究所、アジア太平洋統計研修所、消防大学校及び消防研究センター、国会連絡室の 11 拠点を指す。
28	地方支分部局	全国に点在する総合通信局、総合通信事務所、管区行政評価(支)局、行政評価事務所及び行政評価分室の 62 拠点を指す。

No.	用語	定義
29	外部監視室	運用業務時間外等、総務省ＬＡＮをリモート監視するための施設を指す。次期総務省ＬＡＮに移行する際、本省に設置するサーバ等の機器を一時的に収容し、構築・試験・運用を行う施設としても利用する。なお、外部監視室は、本調達の一環として借上げを行う。
30	ＤＲサイト	大規模災害等の有事や障害時の際に総務省ＬＡＮの提供するサービスの一部を代替して提供し、かつ、総務省ＬＡＮの設定情報や職員の作成する電子データをバックアップする機能を有する拠点。なお、ＤＲサイトとして利用する施設は、本調達の一環として借上げを行う。
31	本省サーバ室	本省地下１階にあるサーバ室。
32	主管課	総務省大臣官房企画課情報システム室。
33	ユーザ	総務省ＬＡＮを利用する利用者。
34	職員	総務省の職務を担当する者。
35	兼務職員	総務省の複数の職務を担当する者。
36	ユーザアカウント	ユーザに割り当てられたアカウント。
37	職員アカウント	総務省の職員に割り当てられた個別のアカウント。
38	共有アカウント	複数のユーザに割り当てられた共有のアカウント。
39	請負者	本仕様書に基づき次期総務省ＬＡＮの構築等を請け負う事業者。
40	運用担当者	主管課及び総務省ＬＡＮの構築等を請け負う事業者の運用責任者、サービス保守要員、ヘルプデスク要員。
41	ＬＡＮ管理室	本省サーバ室と隣接する常駐室。ただし、常駐する運用責任者、サービス保守要員、ヘルプデスク要員の総称のことも指す。

5　業務・情報システムの概要

（1）システム概要

総務省ＬＡＮの概要図について、図１-１に示す。

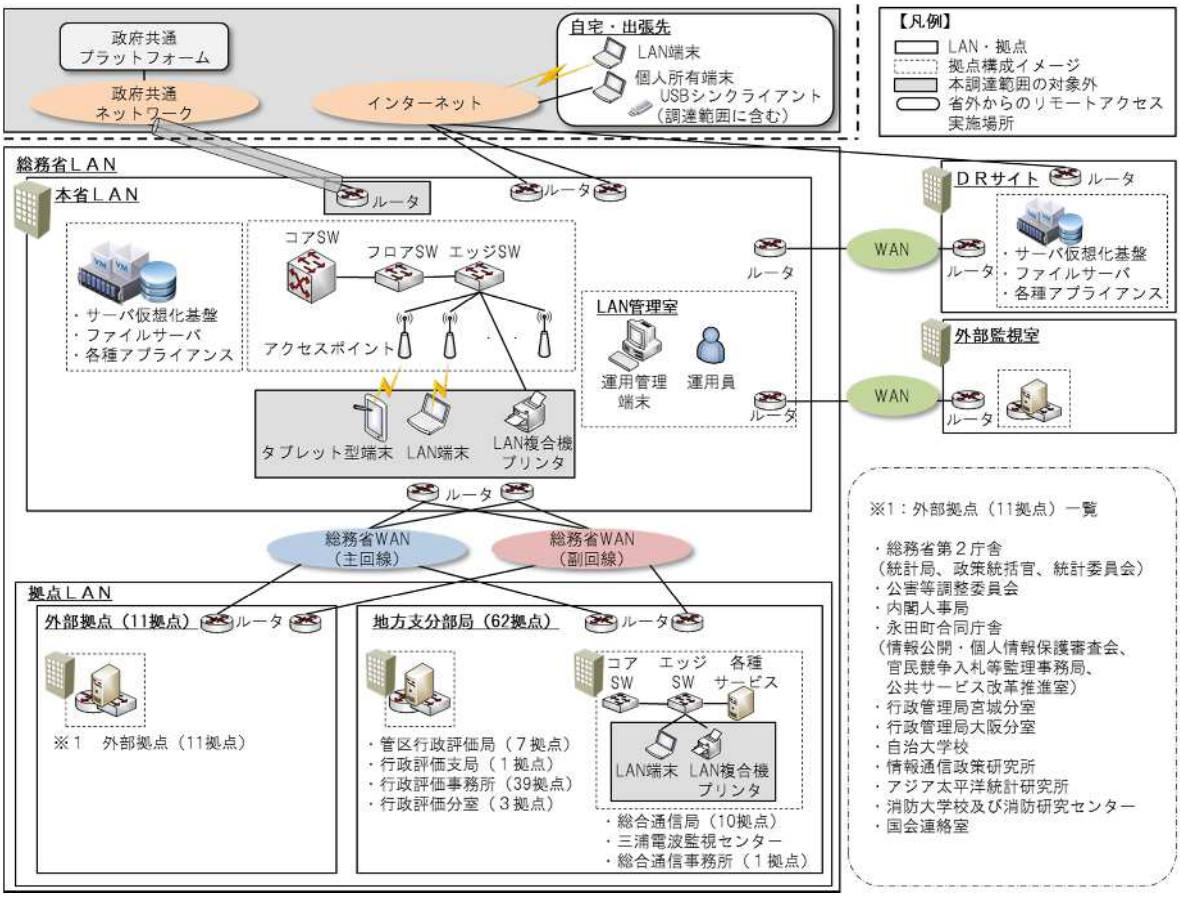


図１-１　総務省ＬＡＮシステム概要図

（2）システム構成

総務省ＬＡＮは、以下に示す要素から構成される。

ア　本省ＬＡＮ

本省ＬＡＮは、職員向けサービスである電子メールや電子掲示板、ファイル共有サーバ、Ｗｅｂ会議やテレワーク等のサービスを提供するとともに、それらサービスを利用するためのＬＡＮ基盤を提供する。

職員向けサービスは、主に本省に設置されるサーバ・ストレージ機器、情報セキュリティ対策機器及びＬＡＮ基盤を構成するためのネットワーク機器により提供される。また、政府共通ネットワークやインターネットへの接続、政府共通ネットワークを経由した政府共通プラットフォームや府省共通システムへの接続機能を提供する。

イ　拠点ＬＡＮ

拠点ＬＡＮは、主に本省ＬＡＮに整備された職員向けサービスを利用するために外部拠点、地方支分部局に構築され、各拠点のＬＡＮ基盤を提供する。

（ア）外部拠点

外部拠点は、都内にある総務省第２庁舎（統計局、政策統括官、統計委員会）、公害等調整委員会、内閣人事局、永田町合同庁舎（情報公開・個人情報保護審査会、官民競争入札等監理事務局、公共サービス改革推進室）、行政管理局宮城分室、行政管理局大阪分室、自治大学校、情報通信政策研究所、アジア太平洋統計研修所、消防大学校及び消防研究センター、国会連絡室の 11 拠点を指す。

（注）平成 28 年４月に内閣官房・内閣府の組織の見直しで編入予定の拠点を含む。このうち、永田町合同庁舎の配置組織は現時点の情報であり、変更されることがある。

（イ）地方支分部局

地方支分部局は、全国に点在する総合通信局、総合通信事務所、管区行政評価（支）局、行政評価事務所及び行政評価分室の 62 拠点を指す。

（ウ）ＤＲサイト

ＤＲサイトは、大規模災害等の有事や障害時の際に総務省ＬＡＮの提供するサービスの一部を代替して提供し、かつ、総務省ＬＡＮの設定情報や職員の作成する電子データをバックアップする機能を有する拠点を指す。

ウ　総務省ＷＡＮ

総務省ＷＡＮは、本省ＬＡＮと拠点ＬＡＮを相互に接続するための広域ネットワークを指す。

エ　外部監視室

運用業務時間外等、総務省ＬＡＮをリモート監視するための施設を指す。次期総務省ＬＡＮに移行する際、本省に設置するサーバ等の機器を一時的に収容し、構築・試験・運用を行う施設としても利用する。

（３）提供する機能等

総務省ＬＡＮが提供するサービスと機能の概要を図１-２、表１-２に示す。

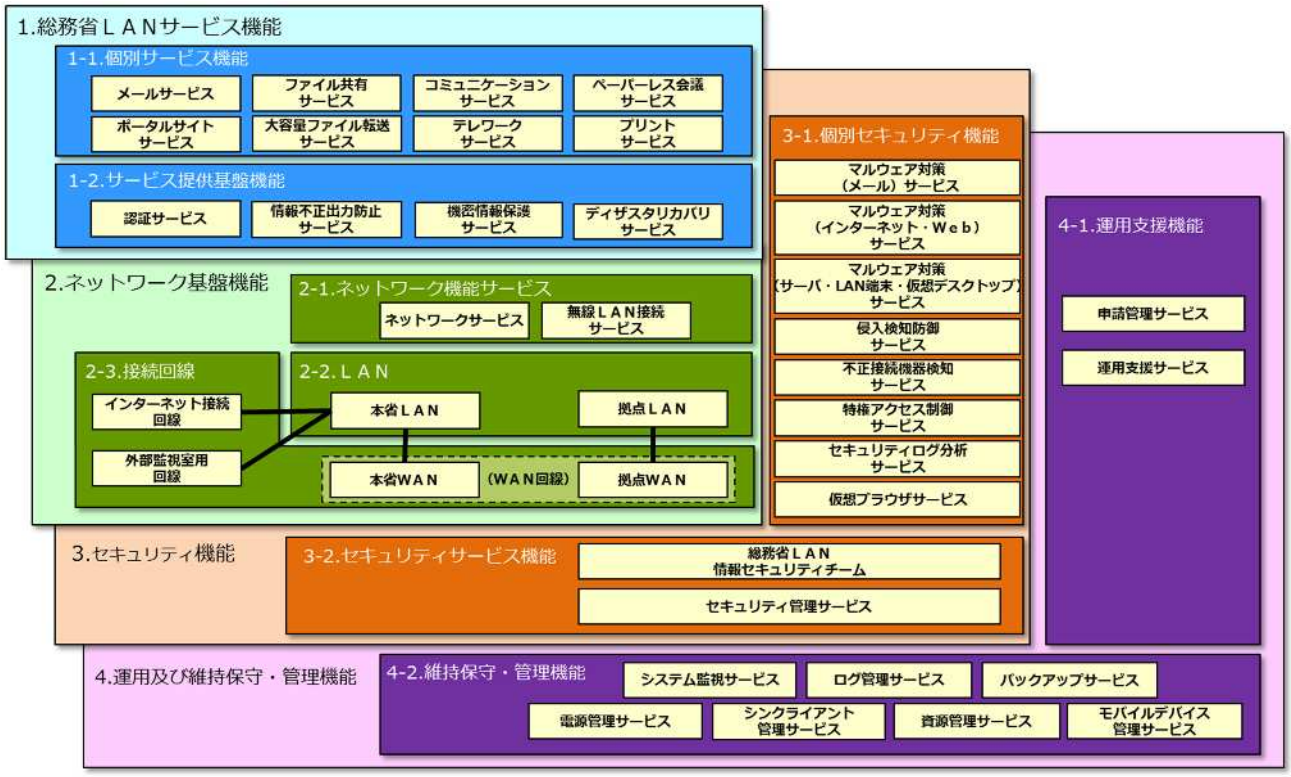


図１-２　次期総務省ＬＡＮが提供する機能等の概要

表１-２　次期総務省ＬＡＮが提供する機能等の概要一覧

機能等の名称	機能等の概要
１．総務省ＬＡＮサービス機能	
１－１．個別サービス機能	
メールサービス	総務省職員が省内外との連絡手段として電子メールを用いるため、メールサービスを提供する。
ポータルサイトサービス	総務省職員が円滑に業務を遂行するため、ポータルサイトサービス（電子掲示板、電子会議室、設備予約、アンケート、スケジューラ、幹部出退表示等）を提供する。
ファイル共有サービス	総務省職員間で電子データを共有・活用し、円滑に業務を進めるため、ファイル共有サービスを提供する。
大容量ファイル転送サービス	総務省職員と省外の関係者間で安全に情報を交換するため、大容量ファイル共有サービスを提供する。
コミュニケーションサービス	メッセージの送受信・在席管理・Ｗｅｂ会議等を用いてコミュニケーションを円滑にし、ワークスタイル変革を推進するため、コミュニケーションサービスを提供する。
テレワークサービス	総務省職員の多様で柔軟な働き方を可能にし、ワーク・ライフ・バランスを推進するため、テレワークサービスを提供する。
ペーパーレス会議サービス	会議室内での電子データの資料共有・閲覧を可能にし、業務効率を向上させるため、ペーパーレス会議システムサービスを提供する。
プリントサービス	電子データを紙資料として印刷する際、不用意な印刷による情報の漏えいを防ぐため、認証機能を有するプリントサービスを提供する。

機能等の名称			機能等の概要
	１－２．サービス提供基盤機能		
		認証サービス	総務省職員のアカウント情報を一元管理し、各サービス利用時の認証及びアクセス権の付与を行うため、認証サービスを提供する。
		情報不正出力防止サービス	電磁的記憶媒体による総務省ＬＡＮ外部への電子データ入出力を制限することで情報の不正出力を防止するため、情報不正出力防止サービスを提供する。
		機密情報保護サービス	暗号化専用フォルダへファイルを保存することで自動的に暗号化し、機密性の高い情報の流出を防止するため、機密情報保護サービスを提供する。
		ディザスタリカバリサービス	大規模災害の発生等により本省から提供されるサービスが停止した際に、ＤＲサイトで総務省ＬＡＮの主要サービスを提供し、業務継続性を確保するため、ディザスタリカバリサービスを提供する。
２．ネットワーク基盤機能			
	２－１．ネットワーク機能サービス		
		ネットワークサービス	総務省職員がネットワークを介した各種サービス（ＤＨＣＰ、ＤＮＳ、ＮＴＰ、プロキシ、負荷分散装置等）を利用するため、ネットワークサービスを提供する。
		無線ＬＡＮ接続サービス	端末の設置場所を固定せず、利用場所にとらわれないネットワーク接続環境を実現するため、無線ＬＡＮ接続サービスを提供する。
	２－２．ＬＡＮ		
		本省ＬＡＮ	総務省ＬＡＮ全体にネットワークサービスを提供し、総務省職員が総務省ＬＡＮサービスを利用するため、本省ＬＡＮを提供する。
		拠点ＬＡＮ	総務省職員が外部拠点、地方支分部局の各拠点において総務省ＬＡＮサービスを利用するため、拠点ＬＡＮを提供する。
	２－３．接続回線		
		インターネット接続回線	総務省職員が行政事務を遂行する際の情報収集及び情報交換を行うため、インターネット接続回線を提供する。
		本省ＷＡＮ	本省、外部拠点、地方支分部局の各拠点及びディザスタリカバリサイトで相互に通信を行うため、本省ＷＡＮ（本省側における総務省ＷＡＮへの接続回線）を提供する。
		拠点ＷＡＮ	本省、外部拠点、地方支分部局の各拠点及びディザスタリカバリサイトで相互に通信を行うため、拠点ＷＡＮ（拠点側における総務省ＷＡＮへの接続回線）を提供する。
		外部監視室用回線	構築や移行の際、外部に設置した機器と本省に設置した機器間で必要なデータの転送を行うため、外部監視室用回線を提供する。
３．セキュリティ機能			
	３－１．個別セキュリティ機能		
		マルウェア対策（メール）サービス	メールを侵入経路とするマルウェア等の侵入を早期に検知・駆除するため、マルウェア対策（メール）サービスを提供する。
		マルウェア対策（インターネット・Ｗｅｂ）サービス	インターネットを介したＷｅｂ閲覧を侵入経路とするマルウェアの侵入を早期に検知・駆除するため、マルウェア対策（インターネット・Ｗｅｂ）サービスを提供する。
		マルウェア対策（サーバ・ＬＡＮ端末・仮想デスクトップ）サービス	サーバ、ＬＡＮ端末及び仮想デスクトップにマルウェアが侵入した際、早期に検知・駆除するため、マルウェア対策（サーバ・ＬＡＮ端末・仮想デスクトップ）サービスを提供する。

機能等の名称			機能等の概要
		侵入検知防御サービス	インターネット及び政府共通ネットワークから省内への不正侵入を防ぐため、侵入検知防御サービスを提供する。
		不正接続機器検知サービス	総務省ＬＡＮに不正に接続された端末等による情報漏えいの防止や、ウイルス感染から保護するため、不正接続機器検知サービスを提供する。
		特権アクセス制御サービス	機器に対する不正な管理操作を防止するため、特権アクセス制御サービスを提供する。
		セキュリティログ分析サービス	ゼロデイ攻撃の回避や検知回避技術を活用した攻撃を早期に検知するため、セキュリティログ分析サービスを提供する。
		仮想ブラウザサービス	マルウェアが直接ＬＡＮ端末に侵入するリスクを低減するために、総務省職員がインターネットへのＷｅｂアクセスを行う専用ブラウザ環境として、仮想ブラウザサービスを提供する。
	３－２．セキュリティサービス機能		
		総務省ＬＡＮ情報セキュリティチーム	政府全体の動向及び総務省の状況を反映し、専門的な知見をもってセキュリティ対策に当たるため、総務省ＬＡＮ情報セキュリティチームにより対応する。
		セキュリティ管理サービス	ＯＳやミドルウェアに潜むぜい弱性や運用におけるセキュリティの問題等を検証・評価するため、セキュリティ管理サービスを提供する。
４．運用及び維持保守・管理機能			
	４－１．運用支援機能		
		申請管理サービス	ヘルプデスクで処理する各種申請の運用負荷を軽減するため、申請管理サービスを提供する。
		運用支援サービス	総務省ＬＡＮに関する問い合わせを一元管理し、進捗状況の確認や問題の分析を可能とするため、運用支援サービスを提供する。
	４－２．維持保守・管理機能		
		システム監視サービス	管理対象機器の障害等を迅速に検知しシステムの可用性を維持する。また、定型的な業務を自動化することで運用負荷を軽減するため、システム監視サービスを提供する。
		ログ管理サービス	収集したログ（認証ログ、アクセスログ、セキュリティログ、利用状況ログ、ＬＡＮ端末の操作ログ等）について、迅速に検索、閲覧及び分析を可能とするため、ログ管理サービスを提供する。
		バックアップサービス	障害発生、災害発生、操作ミス等によりファイルが消失又は破損した場合に当該ファイルの復旧を可能とするため、バックアップサービスを提供する。
		電源管理サービス	電源障害・法定停電・災害時等に、電源の切断順序に依存関係のある機器を安全に停止するため、電源管理サービスを提供する。
		資源管理サービス	不要なアプリケーションのインストール防止、不正な操作や設定等を禁止するため、資源管理サービスを提供する。
		モバイルデバイス管理サービス	モバイルデバイスについて、不要なアプリケーションのインストール防止、不正な操作や設定等を禁止するため、モバイルデバイス管理サービスを提供する。
		シンクライアント管理サービス	テレワークで利用するシンクライアントのイメージの管理、セットアップ処理を行うため、シンクライアント管理サービスを提供する。

（４）システム規模

総務省ＬＡＮは、総務省の職員により、原則として 24 時間 365 日利用するシステムである。ユーザアカウント数、ＬＡＮ端末数及び拠点数を以下に示す。総務省ＬＡＮの設計・構築に当たっては、本調達仕様書及び別紙１「要件定義書」（別紙１－１「要件定義書（システム全般）」から別紙１－４「要件定義書（運用及び維持保守・管理）」までを含む。以下同じ。）を満たすものであること。

（平成 27 年 7 月現在）

ユーザアカウント数		約 16,000 個
	ユーザアカウント数	約 7,000 個
	非ユーザアカウント数 （共有メールアカウント、動作確認用アカウント等）	約 5,000 個
	一時保管アカウント	約 4,000 個
ＬＡＮ端末数		約 7,000 台
拠点数	外部拠点	11 拠点
	地方支分部局	62 拠点
	ＤＲサイト	１拠点
	外部監視室	１拠点

（５）信頼性等及び情報セキュリティの確保

総務省ＬＡＮは、総務省の職員が組織活動及び業務を円滑に行う上でのシステム基盤である。そのため、総務省ＬＡＮは、安定的に稼働する必要がある。また、業務を遂行するに当たり、要機密情報、要保全情報及び要安定情報（以下「要保護情報」という。）を取り扱う。要保護情報を的確に取り扱うためには、十分なセキュリティ対策を施す必要がある。総務省ＬＡＮの設計・構築、運用及び維持保守・管理に当たっては、本調達仕様書及び別紙１「要件定義書」を満たすものであること。

また、運用及び維持保守・管理においては、システムの信頼性と情報セキュリティを確保するために、決められた業務のみを行うのではなく、サイバー攻撃のトレンド情報を踏まえ、その対応について設計・構築担当、運用及び維持保守・管理担当、セキュリティ担当が一体となって検討し、必要な対策等を行うなど、常に高度化・複雑化する新たな攻撃手法に対応していく必要がある。

６　本調達の範囲

（１）本調達の対象範囲

総務省ＬＡＮの更改により表１-２に記載の全てのサービス・機能の提供を受けるため、サービス・機能の設計・構築、機器等の借入、運用及び維持保守・管理等を調達の対象範囲とするものである。なお、総務省ＬＡＮを構成する要素のうち、ＬＡＮ端末、端末ソフトウェア（詳細は、別紙３「ソフトウェア一覧」の「１　総務省ＬＡＮ保有ソフトウェアライセンス一覧」を参照すること。）及び複合機は、別途

調達している。総務省ＬＡＮが提供するサービス・機能の実現に向け、端末ソフトウェアは、総務省の有するライセンスを活用することも可能である。

（２）作業内容

本調達の作業内容を以下に示す。

作業に当たっては、「政府情報システムの整備及び管理に関する標準ガイドライン」（平成 26 年 12 月３日各府省情報化統括責任者(ＣＩＯ）連絡会議決定)に基づき、以下のとおり行うこと。

ア　統制作業

イ　設計・構築

（ア）設計・構築実施計画書等の作成

（イ）進捗管理

（ウ）要件定義書の確定

（エ）設計の実施

（オ）構築の実施

（カ）試験の実施

（キ）受入試験の実施支援

（ク）移行の実施

（ケ）引継ぎの実施

（コ）教育訓練の実施

（サ）ＯＤＢ登録用シートの提出

ウ　運用及び維持・保守管理

（ア）運用・保守要領の作成

（イ）中長期運用・保守作業計画の作成

（ウ）運用・保守実施計画書の作成

（エ）平常時対応

（オ）障害発生時対応

（カ）情報システムの現況確認支援

（キ）主管課等業務支援

（ク）運用業務及び保守作業の改善提案

（ケ）引継ぎ

（コ）ＯＤＢ登録用シートの提出

エ　ＯＤＢ登録用シートのその他事項に係る提出

（３）総務省ＬＡＮを構成する機器等

総務省ＬＡＮを構成する機器等の要件は、「第４　満たすべき要件に関する事項」のとおりとすること。

7　契約期間

平成 28 年４月から平成 33 年３月まで

8　作業スケジュール

総務省ＬＡＮの設計・構築における全体スケジュールを表１-３、図１-３に示す。

表１-３　全体作業スケジュール

フェーズ	期間（想定）	備考
設計・構築	平成 28 年４月～平成 28 年 12 月	
試験	平成 29 年１月～平成 29 年３月	
移行	平成 29 年１月～平成 29 年３月	
稼働	平成 29 年４月～	外部監視室を設置する場所での稼働を想定
移設	平成 29 年５月	総務省サーバ室での稼働に向けて移設を想定
運用	平成 29 年４月～平成 33 年３月	
保守	平成 29 年４月～平成 33 年３月	

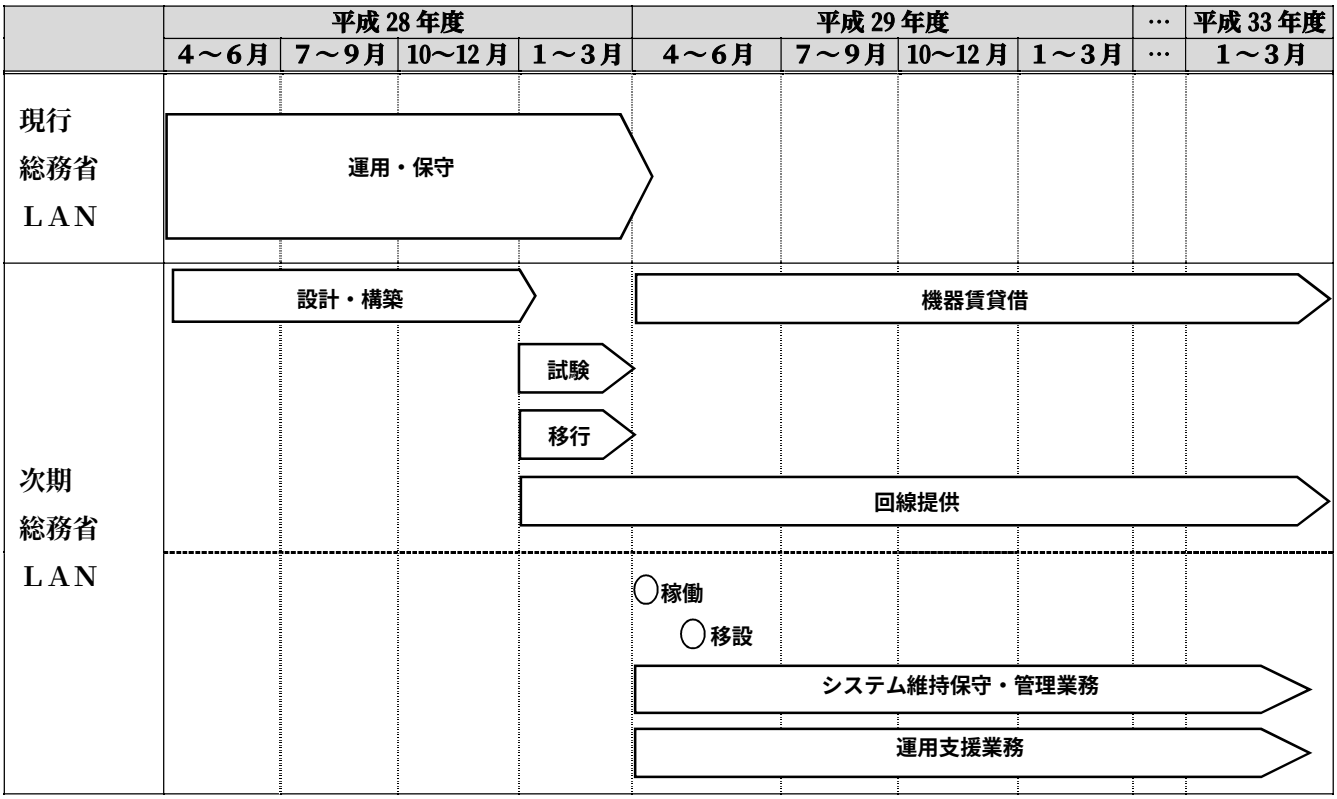


図１-３　想定スケジュール

第２　調達案件及び関連調達案件の調達単位、調達の方法等に関する事項

１　調達案件及びこれと関連する調達案件の調達単位、調達の方式、実施時期

関連する調達案件について、総務省ＬＡＮの全体スケジュールを図２-１に、調達単位、調達の方式、実施時期を表２-１に示す。

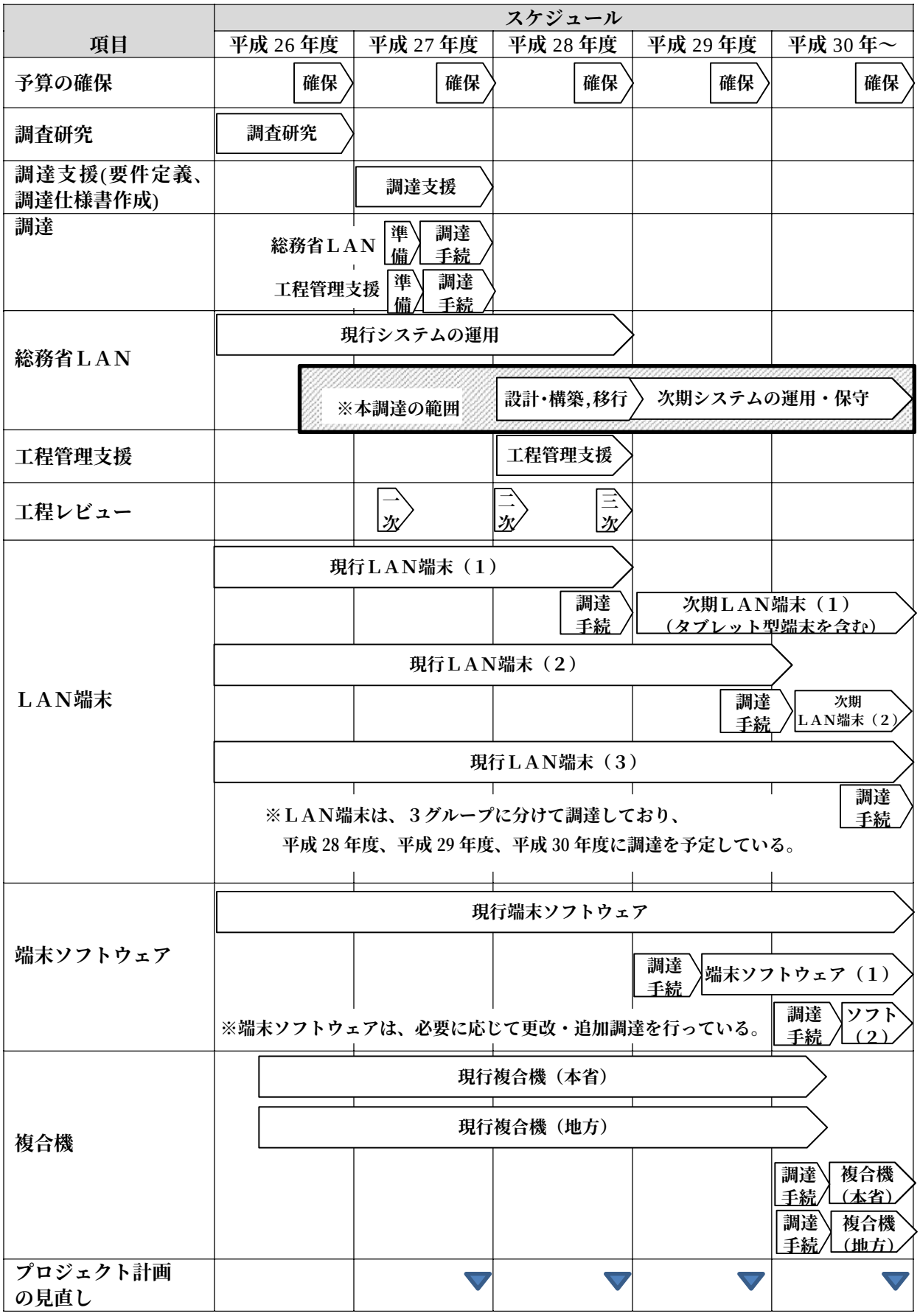


図２-１　総務省ＬＡＮ全体スケジュール

表２-１　関連する調達案件

No.	調達案件名	調達の方式	実施時期
1	総務省ネットワーク基盤（ＬＡＮ）の構築等の請負 （本調達）	一般競争入札 （総合評価落札方式）	意見招請（官報公示）： 平成 27 年 10 月下旬 入札公告（官報公示）： 平成 27 年 12 月下旬 落札者決定： 平成 28 年４月上旬
2	次期総務省ＬＡＮに係る調達支援業務の請負 （調達支援）	一般競争入札 （最低価落札方式）	入札公告（官報公示）： 平成 27 年３月４日 落札者決定： 平成 27 年５月 13 日
3	次期総務省ＬＡＮに係る工程管理支援業務の請負 （工程管理支援）	一般競争入札 （最低価落札方式）	入札公告（官報公示）： 平成 28 年１月中旬 落札者決定： 平成 27 年３月下旬
4	ＬＡＮ端末(１)の賃貸借・保守	一般競争入札 （総合評価落札方式）	（H28 年度）
5	ＬＡＮ端末(２)の賃貸借・保守	一般競争入札 （総合評価落札方式）	（H29 年度）
6	ＬＡＮ端末(３)の賃貸借・保守	一般競争入札 （総合評価落札方式）	（H30 年度）
7	端末ソフトウェア(１)	一般競争入札 （総合評価落札方式）	（H30 年度）
8	端末ソフトウェア(２)	一般競争入札 （総合評価落札方式）	（H31 年度）
9	複合機(本省)の賃貸借・保守	一般競争入札 （総合評価落札方式）	（H30 年度）
10	複合機(地方)の賃貸借・保守	一般競争入札 （総合評価落札方式）	（H30 年度）

２　調達案件間の入札制限

相互牽制の観点から、「次期総務省ＬＡＮに係る調達支援業務の請負」の受注事業者及び「次期総務省ＬＡＮに係る工程管理支援業務の請負」の受注事業者は、入札制限の対象とし、本調達の請負者となることはできない。

3　関連事業者との作業範囲

総務省ＬＡＮに係る調達範囲別の作業項目及び関連事業者との業務分担を表２-２に示す。

表２-２　関連事業者との業務分担

調達範囲別の作業項目 ＼ 関連事業者		工程管理支援	総務省ＬＡＮの構築等（請負者）	ＬＡＮ端末の賃貸借・保守	端末ソフトウェア	複合機の賃貸借・保守
総務省ＬＡＮの構築等（本請負業務）	作業統制	●	－	－	－	－
	設計	－	●	－	－	－
	構築／導入	－	●	－	－	－
	移行	－	●	－	－	－
	運用	－	●	－	－	－
	保守	－	●	－	－	－
ＬＡＮ端末の賃貸借・保守	作業統制	●※1	●※2	－	－	－
	設計	－	－	●	－	－
	構築／導入	－	－	●	－	－
	移行	－	▲	●	－	－
	運用	－	●	▲	－	－
	保守	－	－	●	－	－
端末ソフトウェア	作業統制	－	●	－	－	－
	設計	－	－	－	●	－
	構築／導入	－	－	－	●	－
	移行	－	▲	－	●	－
	運用	－	●	－	▲	－
	保守	－	－	－	●	－
複合機の賃貸借・保守	作業統制	－	●	－	－	－
	設計	－	－	－	－	●
	構築／導入	－	－	－	－	●
	移行	－	▲	－	－	●
	運用	－	●	－	－	▲
	保守	－	－	－	－	●

●：業務の主担当、▲：業務の連携・調整先

※１：平成 28 年度内、※２：平成 29 年度以降

第３　作業の実施内容に関する事項

１　作業の内容

（１）統制作業

請負者は、契約期間を通じて、総務省ＬＡＮ全体に対し、以下の統制作業を行うこと。なお、初年度（平成 28 年度）における統制作業は、別途調達する工程管理支援事業者が実施する。

ア　作業管理、進捗管理

契約期間中に発生する他の調達等に対し、総務省ＬＡＮ全体の統制を確保するために主管課が行う作業（作業管理、進捗管理等）について、作業の実施を支援すること。

イ　変更管理

契約期間中に発生する総務省ＬＡＮの変更に対し、変更影響の分析、変更内容の管理等、変更管理作業の実施を支援すること。

ウ　リスク管理

契約期間中に発生する総務省ＬＡＮのリスクに対し、リスク影響の分析、リスク対応方針の検討等、リスク管理作業の実施を支援すること。

エ　課題管理

契約期間中に発生する総務省ＬＡＮの課題に対し、課題の影響分析、課題解決案の立案、課題への対応状況の管理等、課題管理作業の実施を支援すること。

オ　品質管理

契約期間中に発生する総務省ＬＡＮの機能追加や機能変更に関し、全体の品質を管理するため、機能追加や機能変更に伴う成果物の整合性確認及び修正、機能追加や機能変更を実施する受注事業者の作業品質報告の確認等、品質管理作業の実施を支援すること。

カ　各種技術支援、報告支援

契約期間中、主管課からの求めにより、技術的な確認への回答や問題点・課題の解決案提示等の各種技術支援を実施すること。また、主管課が総務省ＬＡＮについて対外的に報告する際、報告書類の作成等の支援を行うこと。

（２）設計・構築

総務省ＬＡＮの設計・構築に当たっては、以下に示す作業を行うこと。

ア　設計・構築実施計画書等の作成

請負者は、「プロジェクト計画書」及び「プロジェクト管理要領」と整合をとりつつ、主管課の指示に基づき、工程管理支援事業者と調整の上、「設計・構築実施計画書」及び「設計・構築実施要領」を作成し、主管課の承認を受けること。

イ　進捗管理

請負者は、設計・構築に当たって、適切に進捗の管理を行い、原則週次で主管課に進捗状況を報告すること。

ウ　要件定義書の確定

請負者は、主管課、工程管理支援事業者、ＰＭＯ等と調整し、入札公告時の調達仕様書及び要件定義書に対して、調達時の請負者の提案内容に基づき変更を行い、主管課の合意のもと要件定義書を確定させること。

エ　設計の実施

請負者は、基本設計、詳細設計、移行設計及び運用設計を行い、成果物として各種設計書や各種規程、要領、操作マニュアル等を作成し、その内容について主管課の承認を得ること。詳細の要件として、別紙１「要件定義書」を満たすこと。

オ　構築の実施

請負者は、「エ　設計の実施」で実施する設計に基づき、サーバ機器、ストレージ機器、メールサービス、ポータルサイトサービス、ファイル共有サービス、大容量ファイル転送サービス、コミュニケーションサービス、テレワークサービス、認証サービス、ペーパーレス会議サービス、プリントサービス、情報不正出力防止サービス、機密情報保護サービス、ディザスタリカバリサービス、ネットワークサービス、無線ＬＡＮ接続サービス、本省ＬＡＮ、拠点ＬＡＮ、インターネット接続回線、本省ＷＡＮ、拠点ＷＡＮ、外部監視室用回線、マルウェア対策（メール）サービス、マルウェア対策（インターネット・Ｗｅｂ）サービス、マルウェア対策（サーバ・ＬＡＮ端末・仮想デスクトップ）サービス、侵入検知防御サービス、不正接続機器検知サービス、特権アクセス制御サービス、セキュリティログ分析サービス、仮想ブラウザサービス、セキュリティ管理サービス、申請管理サービス、運用支援サービス、システム監視サービス、ログ管理サービス、バックアップサービス、電源管理サービス、資源管理サービス、モバイルデバイス管理サービス、シンクライアント管理サービス、検証環境、運用業務環境、ＫＶＭ、ＵＰＳ、ＬＡＮ端末マスタ、仮想デスクトップマスタその他総務省ＬＡＮの稼働に必要な機能やサービスを構築すること。詳細の要件として、別紙１－２「要件定義書（サービス・機器）」中に示す各構築要件を満たすこと。

カ　試験の実施

請負者は、総務省ＬＡＮが求める要件を確実に満たしていることを確認するため、単体試験、結合試験、総合試験その他総務省ＬＡＮの稼働に必要な試験を計画し、計画に基づいて試験を実施すること。なお、それぞれの試験計画、試験結果について主管課の承認を受けること。詳細の要件として、別紙１－１「要件定義書（システム全般）」の「第４　構築・試験」を満たすこと。

キ　受入試験の実施支援

主管課は、総務省ＬＡＮの構築が完了する前に、求めている要件を満たしているか確認するため、受入試験を実施する。請負者は、受入試験の計画策定、受入試験の実施を支援すること。また、受入試験の結果、サービス・機能等を満たしていない点や不具合が発生した場合、改修のための計画を策定し、速やかに取り組むこと。詳細の要件として別紙１－１「要件定義書（システム全般）」の「第５

受入試験支援」を満たすこと。

ク　移行の実施

請負者は、総務省ＬＡＮの安全かつ確実なシステムの切り替えのため、移行計画の策定、移行設計、移行手順の作成、リスクの識別・コンティンジェンシープランの作成、移行判定基準の作成、移行計画に基づいた移行を実施すること。詳細の要件として、別紙１－１「要件定義書（システム全般）」の「第６　情報システムの移行」を満たすこと。

ケ　引継ぎの実施

請負者は、現行総務省ＬＡＮの現行請負者から業務内容を明らかにした書類等により引継ぎを受けること。なお、その際の引継ぎに必要となる経費は、現行請負者の負担とする。

また、請負者は、本請負業務を終える前に、次々期総務省ＬＡＮの請負者に対して引継ぎを実施すること。引継ぎが円滑に実施されなかったことにより次々期総務省ＬＡＮの請負者の業務遂行に支障が出た場合には、改善されるまで支援を行うこと。なお、その際の引継ぎに必要となる経費は、請負者の負担とすること。詳細の要件として、別紙１－１「要件定義書（システム全般）」の「第７　引継ぎ」を満たすこと。

コ　教育訓練の実施

請負者は、業務運用の継続性を担保するためにユーザ・部局運用担当者に対する教育を行うこと。詳細の要件として、別紙１－１「要件定義書（システム全般）」の「第８　教育」を満たすこと。

サ　ＯＤＢ登録用シートの提出

請負者は、「政府情報システムの整備及び管理に関する標準ガイドライン実務手引書（第３編第６章　調達）」（平成 27 年３月 19 日内閣官房情報通信技術（ＩＴ）総合戦略室。総務省行政管理局。）における「第６章２．１）ウ２（１）ア（キ）ＯＤＢ登録用シートの提出」に基づき、以下に掲げる事項について記載したＯＤＢ登録用シートを提出すること。

（ア）ハードウェアの管理
（イ）ソフトウェアの管理
（ウ）回線の管理
（エ）外部サービスの管理
（オ）施設の管理
（カ）公開ドメインの管理
（キ）取扱情報の管理
（ク）情報セキュリティ要件の管理
（ケ）指標の管理

（３）運用及び維持保守・管理

総務省ＬＡＮの運用及び維持・保守管理に当たっては、以下に示す作業を行うこ

と。

ア　運用・保守要領の作成

請負者は、運用を開始するに当たり、「運用・保守要領」を作成し、主管課の承認を受けること。

イ　中長期運用・保守作業計画の作成

請負者は、「運用・保守要領」に基づき、運用期間中に計画的に発生する作業内容、その想定される時期等を取りまとめた「中長期運用・保守作業計画」を作成すること。「中長期運用・保守作業計画」には、情報システムの構成やライフサイクルを通じた運用業務及び保守作業の内容について記載すること。

ウ　運用・保守実施計画書の作成

請負者は、具体的な作業内容や実施時間、実施サイクル等に関する内容を取りまとめた「運用・保守実施計画書」を作成し、主管課の承認を受けること。

エ　平常時対応

請負者は、総務省ＬＡＮの安定性、安全性を維持するため、構成管理、変更管理、インシデント管理、問題管理、サービスレベル管理、キャパシティ管理、可用性管理、情報セキュリティ管理、継続的なサービス改善等の運用業務を行うこと。情報セキュリティ管理については、サイバー攻撃に関するトレンド情報を入手し、総務省ＬＡＮにおいて可能な防御策を確認の上、必要な機器の設定変更等を迅速かつ適切に行うこと。

また、運用支援業務として、職員からの電話照会を一元的に受付・管理及び対応を行うヘルプデスク業務を行うこと。なお、運用支援業務のうちＬＡＮ端末の操作方法、利用申請の手続等に関する問い合わせ対応業務、総務省ＬＡＮ管理規程で定める申請書の受付・審査等業務は、主管課が行う。

請負者は、総務省ＬＡＮの安定性、安全性を維持するため、ソフトウェア保守、ハードウェア保守等の保守業務を行うこと。詳細の要件として、別紙１－４「要件定義書（運用及び維持保守・管理）」を満たすこと。

オ　障害発生時対応

請負者は、情報システムの障害発生時（又は発生が見込まれる時）には、速やかに主管課に報告するとともに、その緊急度及び影響度を判断の上、障害発生箇所の切り分け、復旧作業、復旧確認作業に対応すること。また、請負者は、情報セキュリティインシデントの発生時（又は発生が見込まれる時）も同様に、感染や被害の状況を的確に把握し、その緊急度及び影響度を判断の上、被害の拡大を防止するための緊急対策、根本原因の究明と機器の設定変更を含む恒久対策を行うこと。詳細の要件として、別紙１－４「要件定義書（運用及び維持保守・管理）」を満たすこと。

カ　情報システムの現況確認支援

請負者は、年１回、主管課の指示に基づき、ＯＤＢ格納データと情報システムの現況との突合・確認（以下「現況確認」という。）の実施を支援すること。現況

確認の結果、ＯＤＢの格納データと情報システムの現況との間の差異がみられる場合は、「運用・保守要領」に定める変更管理方法に従い、差異を解消すること。また、ライセンス許諾条件が合致しない場合や、サポート切れのソフトウェア製品の仕様が明らかになった場合は、当該条件への適合可否や更新の可否、条件等について、更新した場合の影響の有無を含め、主管課に報告すること。

キ　主管課等業務支援

請負者は、総務省ＬＡＮへの接続、政府共通ＰＦへの移行等、主管課、部局担当者からの各種照会に対し、要望確認のためのヒアリング等を実施し、適宜技術的観点から主管課等への支援を行うこと。

ク　定期報告

システムの操作や監視状況、障害発生・対応の状況、サービス指標の実績等を日次、週次、月次及び年次で適宜報告すること。

ケ　運用業務及び保守作業の改善提案

請負者は、年度末までに年間の運用実績及び保守作業を取りまとめるとともに、必要に応じて「運用・保守要領」、「中長期運用・保守作業計画」及び「運用・保守実施計画書」に対する改善提案や、総務省ＬＡＮ構築等請負業務の実施全般に係る質の向上の観点から取り組むべき事項等の提案を行うこと。

また、特に情報セキュリティに関する点については、平常時及び障害発生時のみならず、脆弱性やサイバー攻撃の事例とその対策等を調査の上、機器の設定変更等、必要な対策を適切に実施することができるよう、継続的な改善提案を行うこと。

コ　引継ぎ

請負者は、本業務の開始日までに、業務内容を明らかにした書類等により現行請負者から業務の引継ぎを受けること。なお、その際の引継ぎに必要となる経費は、現行請負者の負担とする。また、本業務の終了に伴い、請負者は、当該業務の開始日までに、業務内容を明らかにした書類等により次々期受注事業者に対し、引継ぎを行うこと。引継ぎが円滑に実施されなかったことにより次々期受注事業者の業務遂行に支障が出た場合には、改善されるまで支援を行うこと。なお、その際の引継ぎに必要となる経費は、請負者の負担とすること。

サ　ＯＤＢ登録用シートの提出

請負者は、請負者は、「政府情報システムの整備及び管理に関する標準ガイドライン実務手引書（第３編第６章　調達）」における「第６章２．１）ウ２（１）ウ（ク）ＯＤＢ登録用シートの提出」に基づき、以下に掲げる事項について記載したＯＤＢ登録用シートを提出すること。

（ア）各データの変更管理

（イ）作業実績等の管理

（４）ＯＤＢ登録用シートのその他記載事項に係る提出

ア　請負者は、「政府情報システムの整備及び管理に関する標準ガイドライン」にお

ける別紙２「情報システムの経費区分」に基づき区分等した契約金額の内訳を記載した「ＯＤＢ登録用シート」を契約締結後速やかに提出すること。

イ　請負者は、主管課から求められた場合は、スケジュールや工数等の計画値及び実績値について記載した「ＯＤＢ登録用シート」を提出すること。

２　成果物の範囲、納品期日等

（１）成果物、内容、納品数量、納品期日

本業務の成果物を表３-１に示す。

表３-１　成果物一覧

No.	分類	成果物	内容	提出時期
1	プロジェクト管理	設計・構築実施計画書	本構築作業実施に当たって、目的・対象範囲・目標・体制・実施計画・その他の事項を記載した基本となる文書。体制の詳細は別紙として添付する。	契約締結後２週間以内
2		設計・構築実施要領	本構築作業実施に当たって、コミュニケーション管理・工程管理・リスク管理・課題管理・変更管理、文書管理等の実運用を規定する文書。	契約締結後２週間以内
3		情報管理計画書	情報の取扱者、情報の保護・管理のための教育・周知の計画内容、情報の取扱い要領、作業場所における情報セキュリティ確保のための措置、情報セキュリティが損なわれた場合の対応計画について記載した文書。	契約締結後１週間以内
4		情報管理簿	主管課から貸与を受けた各種ドキュメント、電子データ類の授受方法、保管場所、保管方法、使用場所、使用目的等取扱い方法を明確に記載した文書。	主管課から貸与を受けて１週間以内 完成図書納入時に更新の上、最終版を納品
5		スケジュール表	プロジェクト全体のマイルストーンや日程の全体規模感を記載した全体スケジュールと、各フェーズでの詳細作業を記載した詳細スケジュールのこと。	契約締結後１週間以内
6		ＷＢＳ	プロジェクトで実施すべき全ての作業を、適切なワークパッケージに分解して階層的に表した文書。	契約締結後１週間以内
7		進捗管理表	スケジュールの進捗をＥＶＭにより管理する文書。	設計・構築実施計画書の承認後、進捗報告時に毎回

No.	分類	成果物	内容	提出時期
8		課題管理表	各種課題の管理を行うため、課題の内容、対処方法、対応担当者、実施時期等について記録した文書。	設計・構築実施計画書の承認後、進捗報告時に毎回
9		リスク管理表	プロジェクト実施に当たってのリスクの管理を行うため、リスクの内容、対処方法、対応担当者、実施時期等について記録した文書。	設計・構築実施計画書の承認後、進捗報告時に毎回
10		変更管理表	プロジェクト実施中に変更になった事項について管理を行うため、変更の内容、対処予定、実施時期等変更履歴を記録した文書。	設計・構築実施計画書の承認後、変更をするとき
11		品質管理報告書	本調達で作成する総務省ＬＡＮサービス一式及び完成図書の品質管理を行うためのレビュー実施記録を記載した文書。	対象作業・文書の完了時
12		会議アジェンダ	会議の議題一覧を記載した文書。	プロジェクト開始後の会議実施時に毎回
13		会議議事録	会議の議事録を記載した文書。	会議実施後、４営業日以内
14		プロジェクト完了報告書	プロジェクト中の各作業の実施日時や内容及び結果を記載した文書。	設計・構築の完了時（平成29年５月31日）
15		ＯＤＢ登録用シート	政府における情報システムに関係する情報を一元的に管理するためのデータベースへの各種登録情報（構築規模、ハードウェア情報、ソフトウェア情報等）をまとめたシート。	（平成29年５月31日）
16	設計・構築	設計・構築計画書	設計・構築実施に当たっての体制、詳細スケジュール、作業内容等を記載した文書。	（平成28年４月30日）
17		システム概要説明資料	主管課が総務省ＬＡＮのシステム概要を把握するための提供サービス内容、規模感、拠点情報、運用情報等を記載した文書。	（平成28年６月30日）
18		基本設計書	本調達の提供するサービス全体の設計内容を記載した文書。	（平成28年５月から平成28年８月まで）
19		詳細設計書	各サービス提供で必要となる詳細な設計を記載した文書。パラメータ等も含む。	（平成28年７月から平成28年10月まで）
20		回線導入計画書	インターネット回線やＷＡＮ回線の導入に当たっての体制、詳細スケジュール、作業内容等を記載した文書。	（平成28年８月31日）
21		回線一覧	インターネット回線やＷＡＮ回線の回線速度や種別の一覧を記載した文書。	（平成28年８月31日）

No.	分類	成果物	内容	提出時期
22		回線導入報告書	回線導入の結果や報告を記載した文書。	（平成 29 年 1 月 31 日）
23		ファシリティ設計書	ラック構成等のファシリティの設計内容を記載した文書。	（平成 28 年 9 月 30 日）
24	試験	試験実施計画書	単体･結合･総合試験実施に当たっての体制、詳細スケジュール､試験環境等を記載した文書。	（平成 28 年 10 月 31 日）
25		試験仕様書	単体・結合・総合試験実施計画に基づき、試験方針、試験項目、試験方法、合否判定基準を定めた文書。	（平成 28 年 12 月 20 日）
26		試験結果報告書	単体・結合・総合試験の各結果及び全体の報告､統計的な分析を行った結果を記載した文書。	（平成 29 年 3 月 31 日）
27		受入試験実施計画書	受入試験実施に当たっての体制､詳細スケジュール、試験環境等を記載した文書。	（平成 29 年 1 月 31 日）
28		受入試験仕様書	受入試験実施計画に基づき、試験方針、試験項目､試験方法､合否判定基準を定めた文書。	（平成 29 年 2 月 28 日）
29	移行･教育訓練	移行実施計画書	移行の体制、方針、詳細スケジュール、移行環境、移行方法等を記載した文書。	（平成 28 年 10 月 31 日）
30		展開実施計画書	展開の体制、方針、詳細スケジュール、展開方法等を記載した文書。	（平成 28 年 10 月 31 日）
31		展開事前調査報告書	本省及び各拠点の展開に必要な情報を記載した文書。配線、ラック等の状況をまとめたもの。	（平成 28 年 12 月 20 日）
32		工事前調査報告書	工事実施に当たって､工事に必要な情報を記載した文書。ＬＡＮ敷設、電源敷設用の設計図等をまとめたもの。	（平成 28 年 12 月 20 日）
33		移行設計書	移行実施に当たって､対象データ範囲や整備方法、具体的な作業内容を設計した文書。移行判定項目や移行判定基準等も記載する。	（平成 28 年 11 月 30 日）
34		移行手順書	作業体制、連絡先一覧、バックアップ等準備作業、移行・導入作業、及び事後作業等の作業項目､操作対象､操作方法を記載した文書。想定時間等を明確したタイムチャートやトラブル発生時の切戻し（フォールバック）手順を含む。	（平成 28 年 12 月 20 日）

No.	分類	成果物	内容	提出時期
35		展開手順書	機器設置や展開作業を行うための手順が記載された文書。展開が正しく行われたことの確認手順も含む。	（平成 28 年 11 月 30 日）
36		ユーザ移行手順書	移行実施に当たって、ユーザが実施する作業手順をまとめた文書。	（平成 29 年 1 月 31 日）
37		移行結果報告書	移行作業について、移行実施設計書に記載の判定項目・判定基準に沿った結果を記載した文書。	（平成 29 年 5 月 31 日）
38		教育訓練実施計画書	教育訓練実施に当たっての体制、詳細スケジュール、訓練環境、訓練方法等を記載した文書。	（平成 28 年 12 月 20 日）
39		教育訓練用教材	次期総務省ＬＡＮサービスの利用方法をユーザに教育訓練するため、手順や解説等が記載された文書。本文書は、ユーザが総務省ＬＡＮを利用する際のマニュアルとなる。	（平成 28 年 12 月 20 日）
40		教育訓練実施報告書	教育訓練作業の実施日時や内容・結果、教育訓練の習熟度分析等を記載した文書。	（平成 29 年 3 月 31 日）
41	運用・保守	サービスレベル合意書	総務省側と請負者側の責任分界点や役割を明確にし、必要な管理項目とサービスレベル管理指標の保証値等について記載した文書。	（平成 29 年 3 月 31 日）
42		運用・保守要領	運用・保守を行う上での指針・基準となる項目を記載した文書	（平成 28 年 12 月 20 日）
43		運用・保守実施計画書	システム運用の実施に当たっての体制、詳細スケジュール、作業内容等を記載した文書。	（平成 29 年 1 月 31 日）
44		中長期運用・保守作業計画	運用期間中に計画的に発生する作業内容、その想定される時期等を取りまとめた中長期運用・保守作業計画。	（平成 29 年 1 月 31 日）
45		運用・保守設計書	システム運用・保守の対象や方法について記載した文書。	（平成 29 年 1 月 31 日）
46		運用・保守手順書	運用要員が運用・保守を行う上での手順や解説等を記載した文書。	（平成 29 年 3 月 31 日）
47		情報システム運用継続計画	総務省ＬＡＮにおける情報システム運用継続計画を記載した文書。	（平成 29 年 3 月 31 日）
48		運用報告書	システム操作や監視の実施状況、障害状況、サービス指標実績値、ヘルプデスク運用状況の報告、分析等の運用状況を記載した文書。	平成 29 年 4 月以降、項目に応じ日時、週次、月次、年次で報告

No.	分類	成果物	内容	提出時期
49		保守報告書	ハードウェアの定期点検やソフトウェアの脆弱性対策等の保守状況を記載した文書。	平成 29 年４月以降、項目に応じ日時、週次、月次、年次で報告
50		セキュリティ報告書	セキュリティ監視、分析、対策状況等を記載した文書。	平成 29 年４月以降、項目に応じ日時、週次、月次、年次で報告
51		ＳＬＡ報告書	ＳＬＡの達成率や状況の分析、未達成が継続された場合は改善策等のＳＬＡ管理状況を記載した文書。	平成 29 年４月以降、項目に応じ月次、年次で報告
52		ハードウェア管理台帳	各サーバ・端末・ネットワーク機器の機種名、型番等の情報を記載した文書。	（平成 29 年３月 31 日）更新の都度
53		ソフトウェア管理台帳	各サーバ・端末・ネットワーク機器にインストールされているソフトウェアの名称、バージョン、メーカ名等の情報を記載した文書。	（平成 29 年３月 31 日）更新の都度
54		ライセンス管理台帳	次期総務省ＬＡＮで管理する全てのライセンスの名称や期限等の利用状況を一覧にして記載した文書。	（平成 29 年３月 31 日）更新の都度
55		ネットワーク構成情報管理台帳	ＩＰアドレス、ＭＡＣアドレス、ホスト名等、サーバ及び端末に係るネットワーク情報を管理した文書。	（平成 29 年３月 31 日）更新の都度
56		フロアレイアウト図	フロア内の機器の場所や機器の配置状況のわかる写真等をまとめた文書。	（平成 29 年３月 31 日）更新の都度
57		課題管理表	システム運用時に発生した課題の内容、対処方法、対応担当者、実施時期等について記録した文書。	平成 29 年４月以降、週次で報告
58		運用管理用文書	上記資料以外で運用管理上、必要となる文書。 （例） ・作業管理表 ・入退室管理表 等	文書ごとに主管課と協議の上、提出時期を決定し、提出
59		変更管理台帳	運用実施に際し変更が発生した資料について、変更した内容を示す文書。	変更した文書ごとに項目を追加し、提出

（注）提出時期欄の括弧書きについては、予定年月日を示し、請負者が主管課と協議の上、設計・構築実施計画書等に規定するものとする。

（２）納品方法

ア　成果物は、全て日本語で作成すること。
イ　用字・用語・記述符号の表記については、「公用文作成の要領（昭和 27 年４月４日内閣閣甲第 16 号内閣官房長官依命通知）」を参考にすること。
ウ　情報処理に関する用語の表記については、日本工業規格（ＪＩＳ）の規定を参考にすること。
エ　成果物は紙媒体及び電磁的記録媒体により作成し、総務省から特別に示す場合を除き、原則紙媒体は正１部・副１部、電磁的記録媒体は１部を納品すること。
オ　紙媒体による納品について、用紙のサイズは、原則として日本工業規格Ａ列４番とするが、必要に応じて日本工業規格Ａ列３番を使用すること。
カ　電磁的記録媒体による納品について、Ｍｉｃｒｏｓｏｆｔ Ｏｆｆｉｃｅ（Ｗｏｒｄ、Ｅｘｃｅｌ及びＰｏｗｅｒＰｏｉｎｔ）又はＰＤＦのファイル形式で作成し、ＤＶＤの媒体に格納して納品すること。また、図表等の元データも併せて納品すること。
キ　成果物の作成に当たって、特別なツールを使用する場合は、担当職員の承認を得ること。
ク　成果物が外部に不正に使用されたり、納品過程において改ざんされたりすることのないよう、安全な納品方法を提案し、成果物の情報セキュリティの確保に留意すること。
ケ　電磁的記録媒体により納品する場合は、不正プログラム対策ソフトウェアによる確認を行うなどして、成果物に不正プログラムが混入することのないよう、適切に対処すること。

（３）納品場所

請負者は、納入成果物に示した完成図書一式を本省に納品すること。また、総務省ＬＡＮサービス一式は、それぞれ表３-２に示す各拠点に納品すること。詳細は、主管課の指示によるものとする。

表３-２　拠点一覧

No.	拠点名	郵便番号	所在地
1	本省	100-8926	東京都千代田区霞が関２－１－２　中央合同庁舎第２号館
2	ＤＲサイト	－	－
3	総務省第２庁舎	162-8668	東京都新宿区若松町 19－１
4	公害等調整委員会	100-0013	東京都千代田区霞が関３－１－１ 中央合同庁舎第４号館
5	内閣人事局	100-8914	東京都千代田区永田町１－６－１
6	情報公開・個人情報保護審査会及び官民競争入札等監理事務局	100-0014	東京都千代田区永田町１－11－39
7	行政管理局宮城分室	－	宮城県仙台市内

No.	拠点名	郵便番号	所在地
8	行政管理局大阪分室	－	大阪府豊中市内
9	自治大学校	190-8581	東京都立川市緑町 10－１
10	情報通信政策研究所	185-8795	東京都国分寺市泉町２－11－16
11	アジア太平洋統計研修所	261-8787	千葉県千葉市美浜区若葉３－２－２ 日本貿易振興会アジア経済研究所ビル４階
12	消防大学校及び 消防研究センター	182-8508	東京都調布市深大寺東町４－35－３
13	国会連絡室	100-0014	東京都千代田区永田町１－７－１　参議院別館４階
14	北海道管区行政評価局	060-0808	北海道札幌市北区北８条西２丁目　札幌第１合同庁舎７階
15	函館行政評価分室	040-0032	北海道函館市新川町 25－18　函館地方合同庁舎６階
16	旭川行政評価分室	078-8501	北海道旭川市宮前通東 4155－31　旭川合同庁舎西館５階
17	釧路行政評価分室	085-0022	北海道釧路市南浜町５－９　釧路港湾合同庁舎３階
18	東北管区行政評価局	980-0014	宮城県仙台市青葉区本町３－２－23 仙台第二合同庁舎 10 階、11 階
19	青森行政評価事務所	030-0801	青森市新町２－４－25　青森合同庁舎４階
20	岩手行政評価事務所	020-0045	岩手県盛岡市盛岡駅西通１－９－15 盛岡第２合同庁舎４階
21	秋田行政評価事務所	010-0951	秋田県秋田市山王７－１－３　秋田合同庁舎４階
22	山形行政評価事務所	990-0041	山形県山形市緑町１－５－48　山形地方合同庁舎３階
23	福島行政評価事務所	960-8021	福島県福島市霞町１－46　福島合同庁舎３階
24	関東管区行政評価局	330-9717	埼玉県さいたま市中央区新都心１－１ さいたま新都心合同庁舎１号館 19 階
25	茨城行政評価事務所	310-0061	茨城県水戸市北見町１－11　水戸地方合同庁舎２階
26	栃木行政評価事務所	320-0043	栃木県宇都宮市桜５－１－13　宇都宮地方合同庁舎３階
27	群馬行政評価事務所	371-0026	群馬県前橋市大手町２－３－１　前橋地方合同庁舎６階
28	千葉行政評価事務所	260-0024	千葉県千葉市中央区中央港１－11－３ 千葉地方合同庁舎７階
29	東京行政評価事務所	169-0073	東京都新宿区百人町３－28－８　新宿地方合同庁舎２階
30	神奈川行政評価事務所	231-0023	神奈川県横浜市中区山下町 37－９　横浜地方合同庁舎３階
31	新潟行政評価事務所	950-8628	新潟市中央区美咲町１－１－１ 新潟美咲合同庁舎第１号館７階
32	山梨行政評価事務所	400-0031	山梨県甲府市丸の内１－１－18　甲府合同庁舎９階
33	長野行政評価事務所	380-0846	長野県長野市旭町 1108　長野第１合同庁舎
34	中部管区行政評価局	460-0001	愛知県名古屋市中区三の丸２－５－１ 名古屋合同庁舎第２号館４階
35	富山行政評価事務所	930-0856	富山県富山市牛島新町 11－７　富山合同庁舎５階

No.	拠点名	郵便番号	所在地
36	石川行政評価事務所	920-0024	石川県金沢市西念３－４－１　金沢合同庁舎４階
37	岐阜行政評価事務所	500-8114	岐阜県岐阜市金竜町５－13　岐阜合同庁舎２階
38	静岡行政評価事務所	420-0853	静岡県静岡市葵区追手町９－50　静岡地方合同庁舎５階
39	三重行政評価事務所	514-0033	三重県津市丸之内 26－８　津合同庁舎３階
40	近畿管区行政評価局	540-8533	大阪府大阪市中央区大手前４－１－67 大阪合同庁舎第２号館７階
41	福井行政評価事務所	910-0859	福井県福井市日之出３－14－15　福井地方合同庁舎２階
42	滋賀行政評価事務所	520-0044	滋賀県大津市京町３－１－１　大津びわ湖合同庁舎７階
43	京都行政評価事務所	604-8482	京都府京都市中京区西ノ京笠殿町 38 京都地方合同庁舎４階
44	兵庫行政評価事務所	650-0024	兵庫県神戸市中央区海岸通 29　神戸地方合同庁舎２階
45	奈良行政評価事務所	630-8213	奈良県奈良市登大路町 81　奈良合同庁舎４階
46	和歌山行政評価事務所	640-8155	和歌山県和歌山市九番丁 11
47	中国四国管区行政評価局	730-0012	広島県広島市中区上八丁堀６－30 広島合同庁舎第４号館 13 階
48	鳥取行政評価事務所	680-0845	鳥取県鳥取市富安２－89－４　鳥取第１地方合同庁舎３階
49	島根行政評価事務所	690-0841	島根県松江市向島町 134－10　松江地方合同庁舎
50	岡山行政評価事務所	700-0984	岡山県岡山市桑田町１－36　岡山地方合同庁舎３階
51	山口行政評価事務所	753-0088	山口県山口市中河原町６－16 山口地方合同庁舎１号館２階
52	四国行政評価支局	760-0068	香川県高松市松島町１－17－33 高松第２地方合同庁舎４階
53	徳島行政評価事務所	770-0851	徳島県徳島市徳島町城内６－６　徳島地方合同庁舎５階
54	愛媛行政評価事務所	790-0808	愛媛県松山市若草町４－３　松山若草合同庁舎４階
55	高知行政評価事務所	780-0870	高知県高知市本町４－３－41　高知地方合同庁舎
56	九州管区行政評価局	812-0013	福岡県福岡市博多区博多駅東２－11－１ 福岡合同庁舎（本館）８階
57	佐賀行政評価事務所	840-0041	佐賀県佐賀市城内２－10－20　佐賀合同庁舎３階
58	長崎行政評価事務所	852-8106	長崎県長崎市岩川町 16－16　長崎合同庁舎５階
59	熊本行政評価事務所	860-0047	熊本県熊本市西区春日２－10－１ 熊本地方合同庁舎Ｂ棟４階
60	大分行政評価事務所	870-0016	大分県大分市新川町２－１－36　大分合同庁舎４階
61	宮崎行政評価事務所	880-0805	宮崎県宮崎市橘通東３－１－22　宮崎合同庁舎４階
62	鹿児島行政評価事務所	892-0816	鹿児島県鹿児島市山下町 13－21 鹿児島合同庁舎３階（黎明館前）

No.	拠点名	郵便番号	所在地
63	沖縄行政評価事務所	900-0006	沖縄県那覇市おもろまち２－１－１ 那覇第２地方合同庁舎１号館４階
64	北海道総合通信局	060-8795	北海道札幌市北区北８条西２－１－１　札幌第１合同庁舎
65	東北総合通信局	980-8795	宮城県仙台市青葉区本町３－２－23　仙台第２合同庁舎
66	関東総合通信局	102-8795	東京都千代田区九段南１－２－１ 九段第３合同庁舎 22 階、23 階
67	関東総合通信局 （三浦電波監視センター）	238-0115	神奈川県三浦市初声町高円坊 1691
68	信越総合通信局	380-8795	長野県長野市旭町 1108　長野第１合同庁舎
69	北陸総合通信局	920-8795	石川県金沢市広坂２－２－60　金沢広坂合同庁舎６階
70	東海総合通信局	461-8795	愛知県名古屋市東区白壁１－15－１ 名古屋合同庁舎第３号館
71	近畿総合通信局	540-8795	大阪府大阪市中央区大手前１－５－44 大阪合同庁舎第１号館４階
72	中国総合通信局	730-8795	広島県広島市中区東白島町 19－36
73	四国総合通信局	790-8795	愛媛県松山市宮田町８－５ 日本郵政グループ松山ビル６階 ※庁舎移転の予定あり ・平成 30 年度 第１四半期（５～６月頃）回線の配線工事 第２四半期（７月頃）庁舎移転
74	九州総合通信局	860-8795	熊本県熊本市西区春日２－10－１ 熊本地方合同庁舎Ａ棟 11 階
75	沖縄総合通信事務所	900-8795	沖縄県那覇市旭町１－９　カフーナ旭橋Ｂ－１街区５階
76	外部監視室	－	－

（４）作業窓口

総務省大臣官房企画課情報システム室第三係

第４　満たすべき要件に関する事項

１　調達仕様書記載の要件

本業務の実施に当たっては、本調達仕様書の記載事項の内容を理解した上で、全ての要件を満たすこと。

２　要件定義書記載の要件

（１）「システム全般」の要件

ア　規模・性能

本業務の実施に当たって、共通方針、規模・性能要件を理解した上で、全ての要件を満たすこと。なお、詳細な要件は、別紙１－１「要件定義書（システム全般）」の「第１　規模・性能」を参照すること。

イ　信頼性等

本業務の実施に当たって、信頼性要件、拡張性要件、上位互換性要件、システム中立性要件、事業継続性要件を理解した上で、全ての要件を満たすこと。なお、詳細な要件は、別紙１－１「要件定義書（システム全般）」の「第２　信頼性等」を参照すること。

ウ　情報セキュリティ

本業務の実施に当たって、情報セキュリティ対策、本調達の遂行等に係る情報セキュリティ対策を理解した上で、全ての要件を満たすこと。なお、詳細な要件は、別紙１－１「要件定義書（システム全般）」の「第３　情報セキュリティ」を参照すること。

エ　構築・試験

本業務の実施に当たって、試験要件、試験場所を理解した上で、全ての要件を満たすこと。なお、詳細な要件は、別紙１－１「要件定義書（システム全般）」の「第４　構築・試験」を参照すること。

オ　受入試験支援

本業務の実施に当たって、受入試験支援を理解した上で、全ての要件を満たすこと。なお、詳細な要件は、別紙１－１「要件定義書（システム全般）」の「第５　受入試験支援」を参照すること。

カ　情報システムの移行

本業務の実施に当たって、移行に係る要件、移行作業の進め方を理解した上で、全ての要件を満たすこと。なお、詳細な要件は、別紙１－１「要件定義書（システム全般）」の「第６　情報システムの移行」を参照すること。

キ　引継ぎ

本業務の実施に当たって、業務運用開始時の引継ぎ、業務終了時の引継ぎを理解した上で、全ての要件を満たすこと。なお、詳細な要件は、別紙１－１「要件定義書（システム全般）」の「第７　引継ぎ」を参照すること。

ク　教育

本業務の実施に当たって、教育に係る要件を理解した上で、全ての要件を満たすこと。なお、詳細な要件は、別紙１－１「要件定義書（システム全般）」の「第８　教育」を参照すること。

ケ　施設・設備

本業務の実施に当たって、本省サーバ室、ディザスタリカバリサイト、外部監

視室、工事に係る要件を理解した上で、全ての要件を満たすこと。なお、詳細な要件は、別紙１－１「要件定義書（システム全般）」の「第９　施設・設備」を参照すること。

（２）「サービス・機器」の要件

ア　調達機器の共通事項

総務省ＬＡＮとして提供する全てのサービスは、セキュリティの担保上の理由から、原則として全て、オンプレミスで提供を行うこと。なお、詳細な要件は、別紙１－２「要件定義書（サービス・機器）」の「第１　調達機器の共通事項」を参照すること。

イ　共用サーバ・ストレージ

（ア）サーバ機器

本省及びディザスタリカバリサイトにおいて、各サービス機能、セキュリティ機能、運用管理機能を構築するためのサーバ機器を提供すること。なお、詳細な要件は、別紙１－２「要件定義書（サービス・機器）」の「第２　１　サーバ機器」を参照すること。

（イ）ストレージ機器

本省・ディザスタリカバリサイトにおいて、サーバ機能、セキュリティ機能、運用管理機能のストレージ機器を提供する。ストレージ機能として、スナップショット、仮想マシンバックアップ、リストア、レプリケーション、重複排除、仮想クローン、読み取りを有すること。なお、詳細な要件は、別紙１－２「要件定義書（サービス・機器）」の「第２　２　ストレージ機器」を参照すること。

ウ　総務省ＬＡＮサービス

（ア）メールサービス

総務省職員が省内外との連絡手段として電子メールを用いるため、メールサービスを提供する。メールサービスには、メール送受信、インターネットメール中継、政府共通ネットワークメール中継、メールストア、メーリングリスト、メールマガジン配信、メールアーカイブ及びアドレス帳機能等が含まれる。なお、詳細な要件は、別紙１－２「要件定義書（サービス・機器）」の「第３　１　メールサービス」を参照すること。

（イ）ポータルサイトサービス

総務省職員が円滑に業務を遂行するため、ポータルサイトサービスを提供する。ポータルサイトには、総務省ＬＡＮの利用規定・ＦＡＱ、インターネット・イントラネット・政府共通ネットワークのＷｅｂサイト等の情報を公開する。また、電子掲示板、電子会議室、設備予約、アンケート及びスケジューラ等が含まれる。なお、詳細な要件は、別紙１－２「要件定義書（サービス・機器）」の「第３　２　ポータルサイトサービス」を参照すること。

（ウ）ファイル共有サービス

総務省職員が円滑に業務情報を交換・記録するため、ファイル共有サービスを提供する。２種類の共有フォルダ（組織用・個人用）を提供する。組織用共有フォルダは、職員が所属する部署によりアクセス権が設定される。なお、詳細な要件は、別紙１－２「要件定義書（サービス・機器）」の「第３　３　ファイル共有サービス」を参照すること。

（エ）大容量ファイル転送サービス

総務省職員と省外の関係者間において、メール添付では扱えない大容量ファイルの送受信を行うために大容量ファイル転送サービスを提供する。なお、詳細な要件は、別紙１－２「要件定義書（サービス・機器）」の「第３　４　大容量ファイル転送サービス」を参照すること。

（オ）認証サービス

総務省職員等のアカウント情報を一元管理し、各サービスへの接続時に認証及びアクセス権の付与を行うため、認証サービスを提供する。生体認証サービスを利用することにより、パスワードの入力が不要になる。各種サービスにおいて利用する証明書を発行する。なお、詳細な要件は、別紙１－２「要件定義書（サービス・機器）」の「第３　５　認証サービス」を参照すること。

（カ）テレワークサービス

総務省職員の多様で柔軟な働き方を可能にし、ワーク・ライフ・バランスを実現するため、テレワークサービスを提供する。在宅業務、出張、災害時において、ＬＡＮ端末・タブレット型端末・シンクライアントを利用した個人所有端末からサービスを利用できる。通常時は本省へアクセス、災害発生時はディザスタリカバリサイトへアクセスする。なお、詳細な要件は、別紙１－２「要件定義書（サービス・機器）」の「第３　６　テレワークサービス」を参照すること。

（キ）コミュニケーションサービス

メッセージ交換、在席管理、Ｗｅｂ会議を用いてコミュニケーションを円滑にし、ワークスタイル変革を推進するため、コミュニケーションサービスを提供する。なお、詳細な要件は、別紙１－２「要件定義書（サービス・機器）」の「第３　７　コミュニケーションサービス」を参照すること。

（ク）ペーパーレス会議サービス

会議室内での電子データの資料共有・閲覧を可能にし、業務効率を向上させるため、ペーパーレス会議サービスを提供する。タブレット型端末からＷｅｂブラウザ又は専用ソフトウェアを介して、会議資料を共有・閲覧する。なお、詳細な要件は、別紙１－２「要件定義書（サービス・機器）」の「第３　８　ペーパーレス会議サービス」を参照すること。

（ケ）プリントサービス

プリントサービスは、職員がＬＡＮ端末から任意の印刷機器を指定し印刷を

行う「プリント機能」と、印刷機器からのプリントアウト時にＩＣカードによる認証が必要な「認証プリント機能」を提供するサービスである。放置された資料からの情報漏えいを防ぐため、国家公務員身分証明証として用いる個人番号カード及びＦｅｌｉＣａカードによって認証することで、印刷できるようにする。プリントサービスは、全てのＬＡＮ複合機、ＬＡＮプリンタで利用できるものとする。なお、詳細な要件は、別紙１－２「要件定義書（サービス・機器）」の「第３　９　プリントサービス」を参照すること。

（コ）情報不正出力防止サービス

情報不正出力防止サービスは、電磁的記憶媒体による総務省ＬＡＮ外部への電子データ入出力を制限し、情報の不正出力を防止する環境を提供する。職員は、総務省ＬＡＮ外部から電磁的記憶媒体による電子データの受取りを行う場合は、ウイルスチェック用端末でウイルスチェックを行い、ＬＡＮ端末に接続許可された USB デバイスを利用してＬＡＮ端末に電子データを移動する。ＬＡＮ端末では、電磁的記録媒体の制限をかけてあり、許可された電磁的記憶媒体しか利用できない。なお、詳細な要件は、別紙１－２「要件定義書（サービス・機器）」の「第３　10　情報不正出力防止サービス」を参照すること。

（サ）機密情報保護サービス

機密情報保護サービスは、ＬＡＮ端末から機微度の高い情報の不正な閲覧を防止するために、ファイルを暗号化専用フォルダに移動することにより自動的に暗号化して保存し、事前に許可を得た職員のみが閲覧・編集・印刷等の機能を制御可能とするサービスである。職員は、ＬＡＮ端末上で作成したファイルを暗号化専用フォルダに移動することにより、ファイルを暗号化できる。職員は、自身のアクセス権に基づき、暗号化されたファイルを「読込」「書込」「編集」「印刷」することができる。なお、詳細な要件は、別紙１－２「要件定義書（サービス・機器）」の「第３　11　機密情報保護サービス」を参照すること。

（シ）ディザスタリカバリサービス

大規模災害発生等の有事の際においても総務省ＬＡＮの主要サービスを提供し、業務継続性を確保するため、ディザスタリカバリサービスを提供する。執務場所に参集できない場合は、テレワークサービスを利用して総務省ＬＡＮの主要サービスを利用する。ディザスタリカバリサービスで提供するサービスには、メールサービス、ポータルサイトサービス、ファイル共有サービス、認証サービス、テレワークサービス、コミュニケーションサービス、プリントサービス、ネットワークサービス、無線ＬＡＮ接続サービス、システム監視機能が含まれる。なお、詳細な要件は、別紙１－２「要件定義書（サービス・機器）」の「第３　12　ディザスタリカバリサービス」を参照すること。

エ　セキュリティサービス

（ア）マルウェア対策（メール）サービス

メールを侵入経路とするマルウェア等の侵入を早期に検知・駆除するため、

マルウェア対策（メール）サービスを提供する。インターネット及び政府共通ネットワークと本省間のメール通信のマルウェア検査・検知を行う。インターネットと本省間のメール通信に対しては、振る舞い検知型のマルウェア検査を行う。迷惑メール判定を行い、迷惑メールを防御する。ドメイン認証やレピュテーション情報を用いて、不審なメールから防御する。なお、詳細な要件は、別紙１－２「要件定義書（サービス・機器）」の「第４　１　マルウェア対策（メール）サービス」を参照すること。

（イ）マルウェア対策（インターネット・Ｗｅｂ）サービス

インターネット及び政府共通ネットワークを経由したＷｅｂ閲覧を侵入経路とするマルウェアの侵入を早期に検知・駆除するため、マルウェア対策（インターネット・Ｗｅｂ）サービスを提供する。インターネット及び政府共通ネットワークと本省間のＷｅｂ通信のマルウェア検査・検知を行う。インターネットと本省間のＷｅｂ通信に対しては、振る舞い検知型のマルウェア検査を行う。レピュテーション情報等を用いて、不審なＷｅｂサイトへのアクセスを防止する。なお、詳細な要件は、別紙１－２「要件定義書（サービス・機器）」の「第４　２　マルウェア対策（インターネット・Ｗｅｂ）サービス」を参照すること。

（ウ）マルウェア対策（サーバ・ＬＡＮ端末・仮想デスクトップ）サービス

サーバ、共有フォルダ及びＬＡＮ端末、仮想デスクトップにマルウェアが侵入した際、早期に検知・駆除するため、マルウェア対策（サーバ・ＬＡＮ端末・仮想デスクトップ）サービスを提供する。サーバ及び共有フォルダ、ＬＡＮ端末のマルウェア検査・検知を行う。サーバ及びＬＡＮ端末では、ホスト間の通信の制御を行う。ＬＡＮ端末では、振る舞い検知型のマルウェア検査を行う。なお、詳細な要件は、別紙１－２「要件定義書（サービス・機器）」の「第４　３　マルウェア対策（サーバ・ＬＡＮ端末・仮想デスクトップ）サービス」を参照すること。

（エ）侵入検知防御サービス

インターネット及び政府共通ネットワークから省内への不正侵入を防ぐため、侵入検知防御サービスを提供する。サイバー攻撃などの総務省ＬＡＮへの不正なアクセスに対して、アクセス制御・侵入検知を行う。総務省ＬＡＮの各セグメント間のアクセス制御を行う。なお、詳細な要件は、別紙１－２「要件定義書（サービス・機器）」の「第４　４　侵入検知防御サービス」を参照すること。

（オ）不正接続機器検知サービス

総務省ＬＡＮに不正に接続された機器に起因したウイルス感染から総務省ＬＡＮを保護するため、不正接続機器検知サービスを提供する。総務省ＬＡＮに接続可能な機器を事前に登録し、限定する。未登録の機器が総務省ＬＡＮに接続された際に、接続通知・通信の遮断を行う。なお、詳細な要件は、別紙１－２「要件定義書（サービス・機器）」の「第４　５　不正接続機器検知サービス」

を参照すること。

（カ）特権アクセス制御サービス

総務省ＬＡＮを構成する各機器に対する不正な管理操作を防止するため、特権アクセス制御サービスを提供する。管理目的のアクセス及び操作を、許可された専用端末のみに限定する。また、管理目的のアクセス及び操作のログを収集し、記録する。なお、詳細な要件は、別紙１－２「要件定義書（サービス・機器）」の「第４　６　特権アクセス制御サービス」を参照すること。

（キ）セキュリティ管理サービス

ＬＡＮ端末及びＷｉｎｄｏｗｓサーバ、Ｌｉｎｕｘサーバのセキュリティポリシー遵守状況を確認するため、セキュリティ管理サービスを提供する。ポリシーテンプレートを作成し、ＬＡＮ端末、Ｗｉｎｄｏｗｓサーバ、Ｌｉｎｕｘサーバが本ポリシーに準拠しているか確認する。監査に必要なログを収集し、保全する。なお、詳細な要件は、別紙１－２「要件定義書（サービス・機器）」の「第４　７　セキュリティ管理サービス」を参照すること。

（ク）セキュリティログ分析サービス

セキュリティインシデントの兆候を早期に検知するため、セキュリティログ分析サービスを提供する。複数のセキュリティログやイベントを用いて相関分析を実施することで、早期検知を実現する。検知したイベントの詳細を調査するため、関連するログを検索、分析する。なお、詳細な要件は、別紙１－２「要件定義書（サービス・機器）」の「第４　８　セキュリティログ分析サービス」を参照すること。

（ケ）仮想ブラウザサービス

マルウェアが直接ＬＡＮ端末に侵入するリスクを低減するために、総務省職員がインターネットへのＷｅｂアクセスを行う専用ブラウザ環境として、仮想ブラウザサービスを提供する。インターネットにアクセスする際は、ＬＡＮ端末のブラウザを利用せずに、本サービスからアクセスする。なお、詳細な要件は、別紙１－２「要件定義書（サービス・機器）」の「第４　９　仮想ブラウザサービス」を参照すること。

オ　運用管理サービス

（ア）申請管理サービス

申請管理サービスは、職員から受け付けた総務省ＬＡＮサービスに関する申請依頼を一元管理し、申請内容に応じて、総務省ＬＡＮサービスと連携するサービスである。職員は、申請書を申請管理サービスを介して提出し、主管課に承認依頼を行う。主管課は、職員からの申請に対して承認又は拒否を行い、運用要員に承認した申請の対応を依頼する。運用要員は、運用管理端末から申請管理サービスに接続し、申請内容を登録する。申請管理サービスは、登録された申請内容に応じて該当するサービスと連携する。なお、詳細な要件は、別紙１－２「要件定義書（サービス・機器）」の「第５　１　申請管理サービス」を

参照すること。

（イ）運用支援サービス

運用支援サービスは、総務省ＬＡＮに関する問い合わせを一元管理し、進捗状況の確認や問題分析のための情報収集する環境を提供するサービスである。問い合わせとイベントをインシデントとして登録し、一次対処、復旧までの調査・回答の進捗管理を運用員内で共有できるようにする。なお、詳細な要件は、別紙１－２「要件定義書（サービス・機器）」の「第５　２　運用支援サービス」を参照すること。

（ウ）システム監視サービス

システム監視サービスは、システムの可用性を維持するため、総務省ＬＡＮのサービスを提供する機器の障害検知やリソース監視、トラフィック監視、その報告を行うためのサービスである。サーバ、ネットワーク機器及びアプライアンス機器の状態を取得し、基準値から外れるものに対し、警告を発生させる。サーバのシステムログを収集し、エラー発生時に警告を発生させる。運用要員が、発生したアラートの内容を確認することができる。なお、詳細な要件は、別紙１－２「要件定義書（サービス・機器）」の「第５　３　システム監視サービス」を参照すること。

（エ）ログ管理サービス

ログ管理サービスは、総務省ＬＡＮサービスを構成する機器が出力したログ（認証ログ、アクセスログ、セキュリティログ、利用状況ログ、ＬＡＮ端末の操作ログ等）を収集し、運用保守及びインシデント対応時に、検索、閲覧及び分析するためのサービスである。運用要員は、運用保守及びインシデント対応時に、必要な各種総務省ＬＡＮサービスのログ（認証ログ、アクセスログ、セキュリティログ、利用状況ログ、ＬＡＮ端末の操作ログ等）の情報を収集、検索、分析する。各種ログを自動的に収集し、一定期間保管する。なお、詳細な要件は、別紙１－２「要件定義書（サービス・機器）」の「第５　４　ログ管理サービス」を参照すること。

（オ）バックアップサービス

総務省ＬＡＮの可用性を維持するために、バックアップサービスを提供する。障害発生や操作ミス等でデータが消失又は破損した場合に復旧可能とし、また、災害発生時にサービスを継続利用可能とする。自動でバックアップを取得し、一定期間保管する。なお、詳細な要件は、別紙１－２「要件定義書（サービス・機器）」の「第５　５　バックアップサービス」を参照すること。

（カ）電源管理サービス

電源障害・法定停電・災害時等に機器を安全に停止しかつ機器の起動制御を行うため、電源管理サービスを提供する。自動でシステム停止・起動を行う。なお、詳細な要件は、別紙１－２「要件定義書（サービス・機器）」の「第５　６　電源管理サービス」を参照すること。

（キ）資源管理サービス

資源管理サービスは、管理対象機器のハードウェア情報、ソフトウェア情報、ライセンス情報等の情報収集や、ソフトウェア配付、セキュリティパッチ等の配付、ＬＡＮ端末接続デバイスの制御、各種設定情報の変更等を一括管理するサービスである。ＬＡＮ端末にソフトウェア（セキュリティパッチ等）をインストールする必要が発生した場合、ソフトウェア（セキュリティパッチ等）の配信を制御できる。職員は、クライアント資源管理サービスを利用し、業務に必要なソフトウェアを任意にＬＡＮ端末にインストールすることができる。総務省が配備した記憶媒体（ＤＶＤ、セキュリティＵＳＢメモリ）以外の記憶媒体をＬＡＮ端末に接続した際に、利用制限できる。なお、詳細な要件は、別紙１－２「要件定義書（サービス・機器）」の「第５　７　資源管理サービス」を参照すること。

（ク）モバイルデバイス管理サービス

モバイルデバイス管理サービスは、職員が省内外で利用するタブレット型端末のハードウェア情報、ソフトウェア情報、利用状況を自動で収集することにより、運用要員が一元的に管理を行うためのサービスである。タブレット型端末に盗難や紛失が発生した場合には、リモートワイプを実行することにより情報漏えいを防ぐ。また、ＯＳやアプリケーションの導入や更新の作業にも利用する。なお、詳細な要件は、別紙１－２「要件定義書（サービス・機器）」の「第５　８　モバイルデバイス管理サービス」を参照すること。

（ケ）シンクライアント管理サービス

シンクライアント管理サービスは、テレワークで利用するシンクライアントのイメージの管理、セットアップ処理を行うサービスである。なお、詳細な要件は、別紙１－２「要件定義書（サービス・機器）」の「第５　９　シンクライアント管理サービス」を参照すること。

カ　その他機器基盤

（ア）検証環境

サーバ、ストレージ、ネットワーク機器の保守作業や障害の原因調査作業を実施する際に、総務省ＬＡＮに及ぼす影響とその手順を確認するため、検証環境を提供する。なお、詳細な要件は、別紙１－２「要件定義書（サービス・機器）」の「第６　１　検証環境」を参照すること。

（イ）運用業務環境

運用業務環境は、運用要員が日常の運用業務に使用する設備環境である。運用要員は、利用する機能ごとの個別環境を利用する。個別環境には、一般執務環境、サーバ接続用環境、遠隔操作用環境がある。運用要員の共有環境として、メンテナンス用端末、地方監視用サーバ、キッティングサーバがある。なお、詳細な要件は、別紙１－２「要件定義書（サービス・機器）」の「第６　２　運用業務環境」を参照すること。

（ウ）ＫＶＭ

サーバ等の機器に対しコンソールからの操作を可能とするため、操作環境を提供する。なお、詳細な要件は、別紙１－２「要件定義書（サービス・機器）」の「第６　３　ＫＶＭ」を参照すること。

（エ）ＵＰＳ

機器に安定した電源を供給し、電源供給が途絶えた際に一定時間電源を供給するため、ＵＰＳを準備する。また、停電の際安全に機器を停止するため、電源管理機能と連携する。なお、詳細な要件は、別紙１－２「要件定義書（サービス・機器）」の「第６　４　ＵＰＳ」を参照すること。

（オ）ＬＡＮ端末マスタ

ＬＡＮ端末マスタは、総務省ＬＡＮ端末をキッティングする際に基となるイメージであり、総務省職員が通常業務で利用するソフトウェアから構成される。ＬＡＮ端末の機種ごとに準備されていること。なお、詳細な要件は、別紙１－２「要件定義書（サービス・機器）」の「第６　５　ＬＡＮ端末マスタ」を参照すること。

（カ）仮想デスクトップマスタ

仮想デスクトップマスタは、仮想デスクトップを複製する際の基となるイメージであり、総務省職員が通常業務で利用するソフトウェアから構成される。仮想デスクトップの環境ごとに準備されていること。なお、詳細な要件は、別紙１－２「要件定義書（サービス・機器）」の「第６　６　仮想デスクトップマスタ」を参照すること。

キ　ネットワーク基盤

（ア）本省ＬＡＮ

本省ＬＡＮは、総務省ＬＡＮ全体にネットワークサービスを提供し、総務省職員が総務省ＬＡＮサービスを利用するため、本省ＬＡＮを提供する。なお、詳細な要件は、別紙１－２「要件定義書（サービス・機器）」の「第７　１　本省ＬＡＮ」を参照すること。

（イ）拠点ＬＡＮ

拠点ＬＡＮは、総務省職員が各拠点において総務省ＬＡＮサービスを利用するため、拠点ＬＡＮを提供する。なお、詳細な要件は、別紙１－２「要件定義書（サービス・機器）」の「第７　２　拠点ＬＡＮ」を参照すること。

（ウ）ネットワークサービス

総務省職員がネットワークを介した各種サービス（ＤＨＣＰ、ＤＮＳ、ＮＴＰ、プロキシ）を利用するため、ネットワークサービスを提供する。なお、詳細な要件は、別紙１－２「要件定義書（サービス・機器）」の「第７　３　ネットワークサービス」を参照すること。

（エ）無線ＬＡＮ接続サービス

端末の設置場所を固定せず、執務場所にとらわれないネットワーク接続環境

を実現するため、無線ＬＡＮ接続サービスを提供する。ペーパーレス会議システムを行う際に、無線ＬＡＮ接続サービスを提供する。なお、詳細な要件は、別紙１－２「要件定義書（サービス・機器）」の「第７　４　無線ＬＡＮ接続サービス」を参照すること。

（オ）インターネット接続回線

総務省職員が業務を遂行する際の情報収集及び情報交換を行うため、インターネット接続回線を提供する。なお、詳細な要件は、別紙１－２「要件定義書（サービス・機器）」の「第７　５　インターネット接続回線」を参照すること。

（カ）本省ＷＡＮ

本省、各地方拠点及びディザスタリカバリサイトで相互に通信を行い、総務省ＬＡＮサービスを利用するため、本省ＷＡＮ（本省側におけるネットワーク及び回線）を提供する。閉域網を使用した通信環境を提供する。なお、詳細な要件は、別紙１－２「要件定義書（サービス・機器）」の「第７　６　本省ＷＡＮ」を参照すること。

（キ）拠点ＷＡＮ

本省、各地方拠点及びディザスタリカバリサイトで相互に通信を行うため、拠点ＷＡＮ（拠点側におけるネットワーク及び回線）を提供する。閉域網を使用した通信環境を提供する。なお、詳細な要件は、別紙１－２「要件定義書（サービス・機器）」の「第７　７　拠点ＷＡＮ」を参照すること。

（ク）外部監視室用回線

構築や移行の際、外部に設置した機器と本省に設置した機器間で必要なデータの転送を行うため、外部監視室用回線を提供する。なお、詳細な要件は、別紙１－２「要件定義書（サービス・機器）」の「第７　８　外部監視室用回線」参照すること。

（３）「回線」の要件

ア　インターネット接続回線

本業務の実施に当たって、本省、ディザスタリカバリサイトのインターネット接続回線要件を理解した上で、全ての要件を満たすこと。なお、詳細な要件は、別紙１－３「要件定義書（回線）」の「インターネット接続回線」を参照すること。

イ　ＷＡＮ回線

本業務の実施に当たって、本省、外部拠点、地方支分部局、ディザスタリカバリサイト、外部監視室のＷＡＮ回線要件を理解した上で、全ての要件を満たすこと。なお、詳細な要件は、別紙１－３「要件定義書（回線）」の「ＷＡＮ回線」を参照すること。

ウ　監視用回線他

本業務の実施に当たって、本省、外部監視室の監視用回線要件を理解した上で、全ての要件を満たすこと。なお、詳細な要件は、別紙１－３「要件定義書（回線）」

の「監視用回線他」を参照すること。

（４）「運用及び維持保守・管理」の要件

ア　全体概要

本業務の実施に当たって、運用設計要件、全体要件の内容を理解した上で、全ての要件を満たすこと。なお、詳細な要件は、別紙１－４「要件定義書（運用及び維持保守・管理）」の「第１　全体概要」を参照すること。

イ　サービスストラテジ

本業務の実施に当たって、事業関係管理の内容を理解した上で、全ての要件を満たすこと。なお、詳細な要件は、別紙１－４「要件定義書（運用及び維持保守・管理）」」の「第２　サービスストラテジ」を参照すること。

ウ　サービスデザイン

本業務の実施に当たって、デザイン・コーディネーション、サービスカタログ管理、サービスレベル管理、キャパシティ管理、ＩＴサービス継続性管理、可用性管理、情報セキュリティ管理、サプライヤ管理の内容を理解した上で、全ての要件を満たすこと。なお、詳細な要件は、別紙１－４「要件定義書（運用及び維持保守・管理）」の「第３　サービスデザイン」を参照すること。

エ　サービストランジション

本業務の実施に当たって、移行の計画立案及びサポート、変更管理、リリース管理及び展開管理、サービス資産管理及び構成管理の内容を理解した上で、全ての要件を満たすこと。なお、詳細な要件は、別紙１－４「要件定義書（運用及び維持保守・管理）」の「第４　サービストランジション」を参照すること。

オ　サービスオペレーション

本業務の実施に当たって、イベント管理、インシデント管理、要求実現、問題管理、アクセス管理の内容を理解した上で、全ての要件を満たすこと。なお、詳細な要件は、別紙１－４「要件定義書（運用及び維持保守・管理）」の「第５　サービスオペレーション」を参照すること。

カ　継続的サービス改善

本業務の実施に当たって、継続的サービス改善の内容を理解した上で、全ての要件を満たすこと。なお、詳細な要件は、別紙１－４「要件定義書（運用及び維持保守・管理）」の「第６　継続的サービス改善」を参照すること。

キ　サービスデスク

本業務の実施に当たって、サービスデスクの内容を理解した上で、全ての要件を満たすこと。なお、詳細な要件は、別紙１－４「要件定義書（運用及び維持保守・管理）」の「第７　サービスデスク」を参照すること。

ク　ソフトウェア保守要件

本業務の実施に当たって、ソフトウェア保守要件の内容を理解した上で、全ての要件を満たすこと。なお、詳細な要件は、別紙１－４「要件定義書（運用及び

維持保守・管理)」の「第８　ソフトウェア保守要件」を参照すること。

ケ　ハードウェア保守要件

本業務の実施に当たって、ソフトウェア保守要件の内容を理解した上で、全ての要件を満たすこと。なお、詳細な要件は、別紙１－４「要件定義書（運用及び維持保守・管理)」の「第９　ハードウェア保守要件」を参照すること。

3　その他満たすべき要件

本業務の実施に当たっては、別紙２から別紙５までの内容を理解した上で、全ての要件を満たすこと。

第５　作業の実施体制・方法に関する事項

1　作業実施体制

プロジェクトの推進体制及び本件請負者に求める作業実施体制を図５-１、表５-１に示す。請負者内のチーム編成については、設計・構築担当、運用及び維持保守・管理担当、セキュリティ担当などを想定しており、特にシステムの信頼性向上や情報セキュリティの確保について、これらのチームが一体となって継続的な改善活動を行う必要がある。

なお、請負者の情報セキュリティ対策の管理体制については、作業実施体制とは別に作成する。

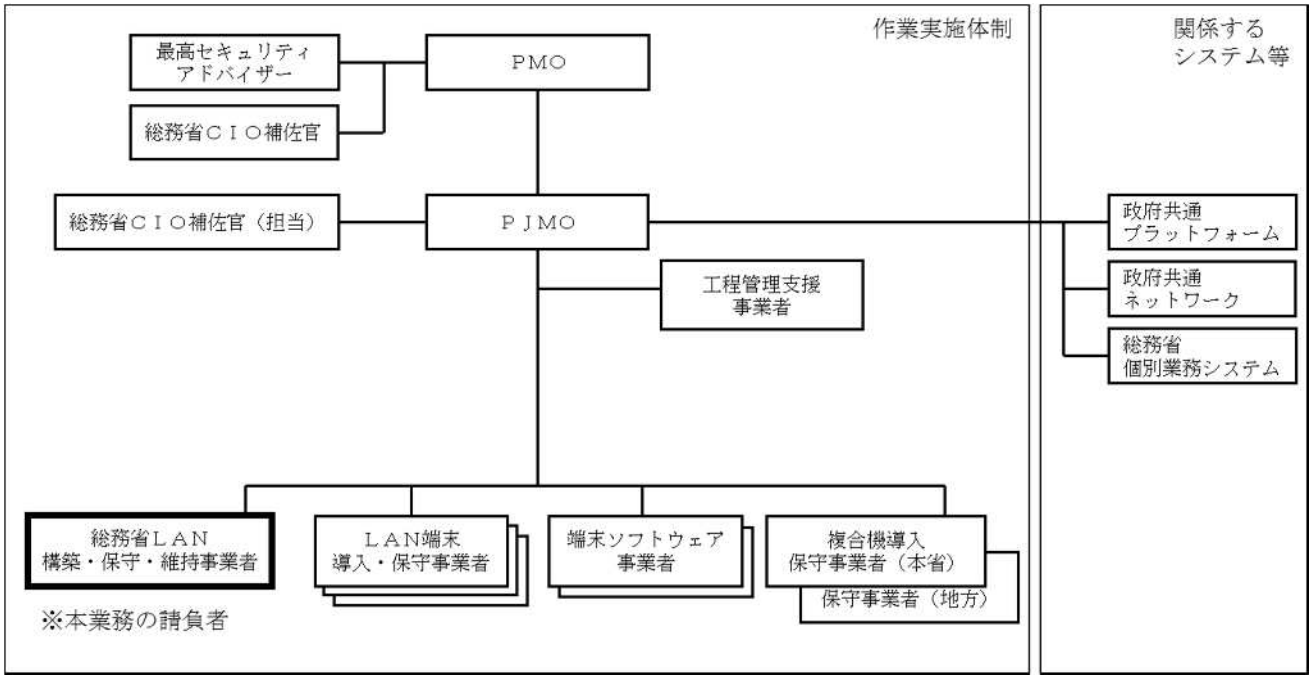


図５-１　プロジェクト実施体制

表５-１　組織・事業者の役割

No.	組織・事業者	役割

No.	組織・事業者	役割
1	ＰMO	総務省のＩＴ施策に関する全体管理の機能を担う組織。
2	ＰＪMO	プロジェクトを遂行し、その進捗等を管理する機能を担う組織。
3	最高セキュリティアドバイサー	総務省最高セキュリティ責任者が任命する、情報セキュリティに関する専門的な知識及び経験を有した専門家。
4	総務省ＣＩＯ補佐官	総務省において、各府省情報化統括責任者（ＣＩＯ）を補佐する者。
5	総務省ＣＩＯ補佐官（担当）	本請負業務に対し、主担当となる総務省ＣＩＯ補佐官
6	政府共通プラットフォーム	クラウドコンピューティング技術等を活用し、各府省別々に構築・運用している政府情報システムの段階的な統合・集約化を図るために整備された共通基盤。
7	政府共通ネットワーク	政府共通プラットフォームとの整合性を確保した政府専用の情報通信ネットワーク基盤。
8	総務省個別業務システム	総務省において、個別の業務を遂行するために整備されたシステム。
9	工程管理支援事業者	総務省ＬＡＮの更改に際し、工程管理を支援する事業者。
10	総務省ＬＡＮ構築・保守・維持事業者	総務省ＬＡＮの更改に際し、構築・保守・維持を担当する事業者。本請負者。
11	ＬＡＮ端末導入・保守事業者	総務省ＬＡＮにおいて、ユーザが使用する端末の導入・保守を担当する事業者。
12	端末ソフトウェア事業者	総務省ＬＡＮにおいて、ＬＡＮ端末上で動作する端末ソフトウェアの開発・保守を担当する事業者。
13	複合機導入保守事業者（本省）	総務省ＬＡＮにおいて、ユーザが印刷等の用途で使用する複合機を総務省本省に導入し、保守を担当する事業者。
14	複合機導入保守事業者（地方）	総務省ＬＡＮにおいて、ユーザが印刷等の用途で使用する複合機を総務省本省以外に導入し、保守を担当する事業者。

２　作業要員に求める資格等の要件

（１）本プロジェクトの統括責任者は、システム計画の立案、プロジェクト管理、システム設計・構築等の実務経験が通算して 10 年以上有する者であること。また、本プロジェクト専任として、支援業務を一貫して実施することができる者であること。ただし、他の兼業しているプロジェクトの業務内容、役割や関与の割合などを客観的に明らかにした上で提案がなされ、総務省の承認が得られた場合はこの限りでは

ない。

（２）本プロジェクトの統括責任者は、「情報処理の促進に関する法律」（昭和 45 年法律第 90 号）に基づき実施される情報処理技術者試験のうち、プロジェクトマネージャ試験の合格者又は「技術士法」（昭和 58 年法律第 25 号）第 32 条に規定する技術士（情報工学部門）若しくは技術士（総合技術監理部門（情報工学を選択科目とする者））の登録を行っている者であること。ただし、当該資格保有者等と同等の能力を有することが経歴等において明らかな者については、これを認める場合がある（その根拠を明確に示し、総務省の理解を得ること。）。

（３）本プロジェクトの統括責任者、担当の作業リーダー又は作業担当者は、情報処理に係る高度な知識を有する者として、以下の資格のうち、アからエまでを有する者を含めること（アからエまでの全てを有する者１名でも可とする。）。

なお、当該資格を有する者については、資格保有後に継続した５年以上の当該資格に関係する業務経験を持つ者であることとする。

ア　プロジェクトマネージャ（独立行政法人情報処理推進機構）、プロジェクトマネジメント・プロフェッショナル（米国ＰＭＩ）、ＩＴストラテジスト（独立行政法人情報処理推進機構）のいずれか

イ　ネットワークスペシャリスト（独立行政法人情報処理推進機構）又はこれと同等以上の資格であることが証明できる資格

ウ　情報セキュリティスペシャリスト（独立行政法人情報処理推進機構）、ＣＩＳＳＰ（（ＩＳＣ）２～ＩＮＴＥＲＮＡＴＩＯＮＡＬ　ＩＮＦＯＲＭＡＴＩＯＮ　ＳＹＳＴＥＭＳ　ＳＥＣＵＲＩＴＹ　ＣＥＲＴＩＦＩＣＡＴＩＯＮ　ＣＯＮＳＯＲＴＩＵＭ）又はこれらと同等以上の資格であることが証明できる資格

エ　ＩＴサービスマネージャ（独立行政法人情報処理推進機構）、ＩＴＩＬ（ＩＮＦＯＲＭＡＴＩＯＮ　ＴＥＣＨＮＯＬＯＧＹ　ＩＮＦＲＡＳＴＲＵＣＴＵＲＥ　ＬＩＢＲＡＲＹ）ＶＥＲＳＩＯＮ２／３　ＦＯＵＮＤＡＴＩＯＮ以上（ＥＸＩＮ）又はこれらと同等以上の資格であることが証明できる資格

３　作業場所

本業務の作業場所及び作業に当たり必要となる設備、備品及び消耗品等については、請負者の責任において用意すること。また、必要に応じて、担当職員が現地確認を実施することができるものとする。

4　作業の管理に関する要領

（1）請負者は、「設計・構築実施要領」に基づき、設計・構築業務に係るコミュニケーション管理、体制管理、工程管理、品質管理、リスク管理、課題管理、システム構成管理、変更管理、情報セキュリティ対策を行うこと。

（2）請負者は、「運用・保守要領」に基づき、運用及び維持・保守管理業務に係るコミュニケーション管理、体制管理、作業管理、リスク管理、課題管理、システム構成管理、変更管理、情報セキュリティ対策を行うこと。

第6　作業の実施に当たっての遵守事項

1　機密保持、資料の取扱い

本調達に係る業務を実施するために扱う情報は、別紙5「情報保護・管理要領」に従い、十分な管理を行うこと。

2　法令等の遵守

当該調達案件の業務遂行に当たっては、「民法」（明治 29 年法律第 89 号）、「刑法」（明治 40 年法律第 45 号）、「私的独占の禁止及び公正取引の確保に関する法律」（昭和 22 年法律第 54 号）、「著作権法」（昭和 45 年法律第 48 号）、「不正アクセス行為の禁止等に関する法律」（平成 11 年法律第 128 号）、「行政機関の保有する個人情報の保護に関する法律」（平成 15 年法律第 58 号）、「行政手続における特定の個人を識別するための番号の利用等に関する法律」（平成 25 年法律第 27 号）等の関連法規を遵守すること。また、総務省が定めた「情報保護・管理要領」（別紙5として添付）及び「総務省情報セキュリティポリシー」（平成 27 年3月 27 日総務省行政情報化推進委員会決定）を遵守すること。なお、「総務省情報セキュリティポリシー」は、落札後に請負者に対し必要に応じて主管課から開示する。

3　その他文書、標準への準拠

（1）プロジェクト計画書

当該調達案件の業務遂行に当たっては、「プロジェクト計画書」との整合を確保して行うこと。

（2）プロジェクト管理要領

当該調達案件の業務の管理に当たっては、「プロジェクト管理要領」との整合を確保して行うこと。

第7　成果物の取扱いに関する事項

1　知的財産権の帰属

（1）本業務における納品物の原著作権及び二次的著作物の著作権（「著作権法」第 21 条から第 28 条に定める全ての権利を含む。）は、請負者が本調達の実施の従前から権利を保有していた等の明確な理由によりあらかじめ提案書にて権利譲渡不可能と示されたもの以外は、全て総務省に帰属するものとする。

（2）総務省は、納品物について、自由に複製し、改変等し、及びそれらの利用を第三

者に許諾することができるとともに任意に開示できるものとする。また、「産業技術力強化法」（平成 12 年法律第 44 号）の趣旨に鑑み、総務省による権利の行使に支障が生じない範囲で、請負者も、成果物を利用することができる。

（３）本件プログラムに関する権利（「著作権法」第 21 条から第 28 条に定める全ての権利を含む。）及び成果物の所有権は、総務省から請負者に対価が完済されたとき請負者から総務省に移転するものとする。

（４）納品される成果物に第三者が権利を有する著作物（以下「既存著作物等」という。）が含まれる場合には、請負者は、当該既存著作物等の使用に必要な費用の負担及び使用許諾契約等に関わる一切の手続を行うこと。この場合、本業務の請負者は、当該既存著作物の内容について事前に総務省の承認を得ることとし、総務省は、既存著作物等について当該許諾条件の範囲で使用するものとする。

（５）請負者は総務省に対し、一切の著作者人格権を行使しないものとし、また、第三者をして行使させないものとする。

２　瑕疵担保責任

（１）請負者は、本調達について検収を行った日を起算日として１年間、成果物に対する瑕疵担保責任を負うものとする。その期間内において瑕疵があることが判明した場合には、その瑕疵が総務省の指示によって生じた場合を除き（ただし、請負者がその指示が不適当であることを知りながら、又は過失により知らずに告げなかったときはこの限りでない。）、請負者の責任及び負担において速やかに修正等を行い、指定された日時までに再度納品するものとする。なお、修正方法等については事前に総務省の承認を得てから着手するとともに、修正結果等についても総務省の承認を受けること。

（２）前項の瑕疵担保期間経過後であっても、成果物等の瑕疵が請負者の故意又は重大な過失に基づく場合は、本調達について検収を行った日を起算日として４年間はその責任を負うものとする。

（３）総務省は、前各項の場合において、瑕疵の修正等に代えて、当該瑕疵により通常生ずべき損害に対する賠償の請求を行うことができるものとする。また、瑕疵を修正してもなお生じる損害に対しても同様とする。

３　検収

（１）本業務の請負者は、成果物等について、納品期日までに総務省に内容の説明を実施して検収を受けること。

（２）検収の結果、成果物等に不備又は誤り等が見つかった場合には、直ちに必要な修正、改修、交換等を行い、変更点について総務省に説明を行った上で、指定された日時までに再度納品すること。

第８　入札参加資格に関する事項

1　入札参加要件

（1）競争参加資格

ア　競争の導入による「公共サービスの改革に関する法律」（平成 18 年6月2日法律第 51 号）第 10 条各号（第 11 号を除く。）に該当する者でないこと。

イ　「予算決算及び会計令」（昭和 22 年勅令第 165 号）第 70 条の規定に該当しない者であること。なお、未成年者、被保佐人又は被補助人であって、契約締結のために必要な同意を得ている者は、同条中、特別な理由がある場合に該当する。

ウ　「予算決算及び会計令」第 71 条の規定に該当しない者であること。

エ　平成 25・26・27 年度総務省競争参加資格（全省庁統一資格）「役務の提供等」Ａ及びＢの等級に格付けされ関東・甲信越地域の競争参加資格を有する者であること（「役務の提供等」の営業品目④情報処理、⑥ソフトウェア開発」又は⑮その他に登録している者であること。）。

（2）公的な資格や認証等の取得

請負者は、以下の内容を証明する資料を提出すること。

ア　本業務を統括管理する部門は、IS09001 認証を取得していること。

イ　本業務を統括管理する部門は、IS027001 認証を取得していること。

ウ　請負者は、一般財団法人日本情報経済社会推進協会のプライバシーマーク制度の認定を受けていること。

エ　請負者は、建設業法に基づく電気通信工事業及び電気工事業の許可を受けていること。

（3）受注実績

請負者は、本総務省ＬＡＮと同等又は類する全国規模のネットワークシステムの設計・構築の実績を有すること。ただし、設計・構築の実績については請負者自身のものであり、再委託等を受けた実績は含まないものとする。

（4）複数事業者による共同提案

ア　複数の事業者が共同提案する場合、その中から全体の意思決定、運営管理等に責任を持つ共同提案の代表者を定めるとともに、本代表者が本調達に対する入札を行うこと。

イ　共同提案を構成する事業者間においては、その結成、運営等について協定を締結し、業務の遂行に当たっては、代表者を中心に、各事業者が協力して行うこと。事業者間の調整事項、トラブル等の発生に際しては、その当事者となる当該事業者間で解決すること。また、解散後の瑕疵担保責任に関しても協定の内容に含めること。

ウ　共同提案を構成する全ての事業者は、本入札への単独提案又は他の共同提案への参加を行っていないこと。

2　入札制限

（1）総務省ＬＡＮに関係する他の調達の受注事業者

次の事業者（再委託先等を含む。）及びこの事業者の「財務諸表等の用語、様式及

び作成方法に関する規則」（昭和 38 年 11 月 27 日大蔵省令第 59 号）第８条に規定する親会社及び子会社、同一の親会社を持つ会社並びに委託先事業者等の緊密な利害関係を有する事業者は、入札には参加できない。

ア　「次期総務省ＬＡＮに係る調達支援業務の請負」の受注事業者

イ　「次期総務省ＬＡＮに係る工程管理支援業務の請負」の受注事業者

（２）ＣＩＯ補佐官及びその支援スタッフの属する事業者

調達仕様書の妥当性確認及び入札事業者の審査に関する業務を行うＣＩＯ補佐官及びその支援スタッフ等の属する又は過去２年間に属していた事業者でないこと。または、ＣＩＯ補佐官等がその職を辞職した後に所属する事業者の所属部門（辞職後の期間が２年に満たない場合に限る。）でないこと。

第９　再委託に関する事項

１　再委託の制限及び再委託を認める場合の条件

（１）本業務の請負者は、業務を一括して又は主たる部分（設計・構築業務、運用業務、保守業務等）を再委託してはならない。

（２）請負者における遂行責任者を再委託先事業者の社員や契約社員とすることはできない。

（３）請負者は再委託先の行為について一切の責任を負うものとする。

（４）再委託を行う場合、再委託先が「第８　２　入札制限」に示す要件を満たすこと。

（５）再委託先における情報セキュリティの確保については、請負者の責任とする。

２　承認手続き

（１）本業務の実施の一部を合理的な理由及び必要性により再委託する場合には、あらかじめ再委託の相手方の商号又は名称及び住所並びに再委託を行う業務の範囲、再委託の必要性及び契約金額等について記載した別添の再委託承認申請書を総務省に提出し、あらかじめ承認を受けること。

（２）前項による再委託の相手方の変更等を行う必要が生じた場合も、前項と同様に再委託に関する書面を総務省に提出し、承認を受けること。

（３）再委託の相手方が更に委託を行うなど複数の段階で再委託が行われる場合（以下「再々委託」という。）には、当該再々委託の相手方の商号又は名称及び住所並びに再々委託を行う業務の範囲を書面で報告すること。

３　再委託先の契約違反等

再委託先において、本調達仕様書に定める事項に関する義務違反又は義務を怠った場合には、請負者が一切の責任を負うとともに、総務省は、当該再委託先への再委託の中止を請求することができる。

第１０その他特記事項

１　前提条件及び制約条件

（１）本件は、平成 28 年度の予算成立を条件とする。平成 28 年▲月▲日以前に平成 28

年度予算が成立していない場合には、契約の中止等を行う可能性がある。

（２）本件受注後に調達仕様書（別紙１「要件定義書」を含む。）の内容の一部について変更を行おうとする場合、その変更の内容、理由等を明記した書面をもって総務省に申し入れを行うこと。双方の協議において、その変更内容が軽微（委託料、納期に影響を及ぼさない）かつ許容できると判断された場合は、変更の内容、理由等を明記した書面に双方が記名捺印することによって変更を確定する。

第１１附属文書

１　要件定義書は、以下の全ての文書を指す。

・別紙１「要件定義書」

別紙１－１「要件定義書（システム全般）」

別紙１－２「要件定義書（サービス・機器）」

別紙１－３「要件定義書（回線）」

別紙１－４「要件定義書（運用及び維持保守・管理）」

２　本調達において、参照すべき内容を含む文書を以下に示す。

・別紙２「次期総務省ＬＡＮ構成イメージ」

・別紙３「ソフトウェア一覧」

・別紙４「機器数量一覧」

・別紙５「情報保護・管理要領」

３　提案書等の審査要領は、別添２「総務省ネットワーク基盤（ＬＡＮ）の構築等の請負総合評価基準書（案）」に示すとおりである。

４　本調達に参加する予定の者から要望があった場合、現行総務省ＬＡＮに係る設計書等の納入成果物等について、所定の手続を踏まえた上で閲覧可能とする。閲覧可能な資料一覧を含め、詳細は、「総務省ＬＡＮシステムの更新整備及び運用管理業務民間競争入札実施要項」の別紙６「資料閲覧要領」に従うものとする。また、本調達に参加する予定の者から追加の資料の開示について要望があった場合は、総務省は、法令及び機密性等に問題のない範囲で適切に対応するよう努めるものとする。

別紙１

総務省ネットワーク基盤（ＬＡＮ）の構築等の請負
要件定義書

総務省大臣官房企画課情報システム室

－ 目 次 -

第１　本文書の位置づけ

本文書は、総務省職員が行政の組織活動を実施するための基盤システムとなる「総務省ネットワーク基盤（ＬＡＮ）」（以下「総務省ＬＡＮ」という。）について、平成29年４月から運用開始を予定している総務省ＬＡＮ（以下「次期総務省ＬＡＮ」という。）の導入において満たすべき要件を記載するものである。

第２　要件定義内容

１　要件定義書の構成

要件定義書は、本文書のほか、別紙に詳細な個別の要件を取りまとめている。要件定義書（本文書及び別紙）の構成は、以下のとおり。

別紙１　要件定義書
- 別紙１－１　要件定義書（システム全般）
- 別紙１－２　要件定義書（サービス・機器）
- 別紙１－３　要件定義書（回線）
- 別紙１－４　要件定義書（運用及び維持保守・管理）

２　記載内容

各別紙の記載内容について、「表２-１　要件定義の個別の記載内容」に示す。

表２-１　要件定義の個別の記載内容

別紙番号	資料名	記載内容
別紙１－１	要件定義書（システム全般）	次期総務省ＬＡＮのシステム全般について満たすべき要件を記載
別紙１－２	要件定義書（サービス・機器）	次期総務省ＬＡＮのサービス・機器について満たすべき要件を記載
別紙１－３	要件定義書（回線）	次期総務省ＬＡＮの回線について満たすべき要件を記載
別紙１－４	要件定義書（運用及び維持保守・管理）	次期総務省ＬＡＮの運用及び維持保守・管理について満たすべき要件を記載

第３　添付資料

別紙１－１　要件定義書（システム全般）
別紙１－２　要件定義書（サービス・機器）
別紙１－３　要件定義書（回線）
別紙１－４　要件定義書（運用及び維持保守・管理）

別添１　拠点回線・機器一覧表
別添２　現行総務省ＬＡＮにおけるサービスレベル一覧

別添２

総務省ネットワーク基盤（ＬＡＮ）の
構築等の請負
総合評価基準書

総務省大臣官房企画課情報システム室

- 目　次 -

1　はじめに

本書は「総務省ネットワーク基盤（ＬＡＮ）の構築等の請負」に関する評価基準を取りまとめた総合評価基準書である。

2　評価基準

（1）評価方法

本業務を実施する者の決定は、総合評価落札方式によるものとする。

また、総合評価は、価格点（入札価格の得点）に技術点（総合評価基準書による加点）を加えて得た数値（以下「総合評価点」という。）をもって行う。

価格点と技術点の配分 価格点の配分：技術点の配分 ＝ １：１

総合評価点 ＝ 価格点（1,100 点満点） ＋ 技術点（1,100 点満点）

（2）合否決定方法

ア　調達仕様書及び要件定義書において必須と定められた要求要件を全て満たしている場合に「合格」とし、１つでも欠ける場合は「不合格」とする。

（3）総合評価点

ア　価格点

価格点は、入札価格を予定価格で除して得た値を１から減じて得た値に入札価格に対する得点配分を乗じて得た値とする。

価格点＝（１－入札価格÷予定価格）×1,100 点

イ　技術点

技術点の評価方法は以下のとおりとする。

（ア）全ての仕様を満たし、「合格」したものに「基礎点」として 100 点を与える。

（イ）「合格」した提案書について、提案書審査委員会の委員ごとに「加点」部分の評価を行う。総務省にとって有益な提案があった場合に、別紙２「総合評価基準及び対応表」の評価ポイントに基づき、「加点」を与えるものとし、各委員の採点結果を委員会で確認し、事実誤認等があれば各委員において訂正する。なお、各委員が行う「加点」部分の評価は、以下の評価基準に基づき点数化する。確定した各委員の採点結果について、その平均値を算出し、「加点」とする。

評価	基準	配点比率
A	評価方針にのっとっており、提案内容が総務省ＬＡＮの質の向上や効率的な業務の実施に資することが具体的に示されており、かつ、客観的な指標を用いて提案されている。	100%
B	評価方針にのっとっており、提案内容が総務省ＬＡＮの質の向上や効率的な業務の実施に資することが具体的に示され、提案されている。	40%
C	評価方針にのっとっていない、提案内容が不十分又は総務省ＬＡＮの質の向上や効率的な業務の実施について具体的に示されていない。	0%

（ウ）評価は以下の方針に基づき判断する。

・総務省ＬＡＮの経緯等を十分に把握し有益な提案となっているか。

・実現性が十分に担保されていると判断できるか。

・提案者の実績や知見に基づく創意工夫が盛り込まれているか。

（エ）「基礎点」と「加点」の合計点を「技術点」とする。

技術点＝基礎点（100 点）＋加点（1,000 点満点）

（４）落札者の決定方法

ア　総合評価基準書に示す全ての要求要件を満たし、入札者の入札価格が予算決算及び会計令第 79 条の規定に基づいて作成された予定価格の制限の範囲内であり、かつ、「総合評価落札方法」によって得られた総合評価点の最も高い者を落札者とする。ただし、予算決算及び会計令第 84 条の規定に該当する場合は、予算決算及び会計令第 85 条の基準（予定価格に 10 分の６を乗じて得た額）を適用するので、基準を下回る金額による入札が行われた場合は入札の結果を保留する。この場合、入札参加者は総務省の行う事情聴取等の調査に協力しなければならない。

イ　調査の結果、会計法（昭和 22 年法律第 35 号）第 29 条の６第１項ただし書きの規定に該当すると認められるときは、その定めるところにより、予定価格の制限の範囲内で次順位の者を落札者とすることがある。

ウ　落札者となるべき者が２人以上あるときは、直ちに当該入札者にくじを引かせ、落札者を決定するものとする。また、入札者又は代理人がくじを引くことができないときは、入札執行事務に関係のない職員がこれに代わってくじを引き、落札者を決定するものとする。

エ　契約担当官等は、落札者を決定したときに入札者にその氏名（法人の場合はその名称）及び金額を口頭で通知する。ただし、上記イにより落札者を決定する場合

には別に書面で通知する。また、落札できなかった入札者は、落札の相対的な利点に関する情報（当該入札者と落札者のそれぞれの入札価格及び技術点）の提供を要請することができる。

（５）落札決定の取消し

次の各号のいずれかに該当するときは、落札者の決定を取り消す。ただし、契約担当官等が、正当な理由があると認めたときはこの限りでない。

ア　落札者が、契約担当官等から求められたにもかかわらず契約書の取り交わしを行わない場合

イ　入札書の内訳金額と合計金額が符合しない場合

落札後、入札者に内訳書を記載させる場合がある。内訳金額が合計金額と符合しないときは、合計金額で入札したものとみなすため、内訳金額の補正を求められた入札者は、直ちに合計金額に基づいてこれを補正しなければならない。

（６）落札者が決定しなかった場合の措置

初回の入札において入札参加者がなかった場合、必須項目を全て満たす入札参加者がなかった場合又は再度の入札を行っても、なお、落札者が決定しなかった場合、原則として、入札条件等を見直した後、再度公告を行う。

なお、再度の入札によっても落札者となるべき者が決定しない場合又は本請負業務の実施に必要な期間が確保できないなどやむを得ない場合は、その理由を民間競争入札等監理委員会に報告するとともに公表するものとする。

3　提出書類及び様式

提案者は以下の内容の提案書を提出すること。

（1）表紙記載事項

提案書の表紙には、以下の事項を明記すること。

ア　表題は「総務省ネットワーク基盤（ＬＡＮ）の構築等の請負　提案書」とすること。

イ　提案者の住所、名称、代表者名及び社印

ウ　連絡担当者の所属、氏名及び電話番号

エ　提案書の提出日

オ　構成及び記載事項

（ア）共通事項

提案書は該当ページの右端に連番等を記述した索引を用いて、要求要件との対応が分かるように工夫すること。

（イ）基礎点相当記載事項

「別紙１　機能証明書」（別紙１－１から別紙１－４までを含む。以下同じ。）に沿って、要件を理解かつ適合していることを示すこと。また、提案内容を簡潔明瞭に記載し、要求要件を満たしていることを評価者である総務省職員が客観的に判断できるように証明すること。補足資料を用いて証明する際は、提案内容補足資料欄及び記載個所欄に補足資料との対応関係を明示し、補足資料の添付順序は、原則として「別紙２　総合評価基準及び対応表」の順番のとおりとすること。

ハードウェア、ソフトウェアの機能証明は、原則としてメーカカタログ等を補足資料として添付し、対応関係を明示すること。その際、補足資料においては、要求要件を満たすことを証明する該当箇所を蛍光ペン等でマーキングすること。

全ての補足資料は、「別紙１　機能証明書」との対応が分かるように該当ページの右端に連番等を記述した索引を用いること。

（ウ）加点項目記載事項

「別紙２　総合評価基準及び対応表」に沿って、要件を理解かつ適合していることを具体的に示すこと。具体的に示された提案内容が要件を満たした上で簡潔明瞭に記載され、本調達における評価ポイントに対して有益と評価者である提案書審査委員会の委員が客観的に判断できる場合は加点する。補足資料を用いて明示する際は、提案内容補足資料欄及び記載個所欄に補足資料との対応関係を明示し、補足資料の添付順序は、原則として「別紙２　総合評価基準及び対応表」の順番のとおりとすること。

全ての補足資料は、「別紙２　総合評価基準及び対応表」との対応が分かるように該当ページの右端に連番等を記述した索引を用いること。

カ　書式

（ア）日本語、Ａ４縦版横書き（ただし、図表などについては必要に応じてA3縦版または横版を用いてもよい。）、上部余白25㎜、下部余白20㎜、左右余白20㎜、ヘッダー部15㎜、フッター部17.5㎜とし、上質紙に12ポイント以上の文字で作成すること。原則として文書はＷｏｒｄで作成し、図表はＥｘｃｅｌ又はＰｏｗｅｒＰｏｉｎｔで作成すること。

キ　項番

（ア）項番の付番については、下記の基準に従うこと。項目を更に細分化する必要等から下記の付番以下のレベルが必要となった場合は、適宜追加設定すること。また、図表番号については、章内での一連番号とし、併せて図表題名を付すこと。

見出し種類	項番表示
見出し1	１、２、３、・・・
見出し2	(１)、(２)、(３)、・・・
見出し3	ア、イ、ウ、・・・
見出し4	(ア)、(イ)、(ウ)、・・・
見出し5	Ａ、Ｂ、Ｃ、・・・
見出し6	(A)、(B)、(C)、・・・
見出し7	ａ、ｂ、ｃ、・・・
見出し8	(a)、(b)、(c)、・・・

４　プレゼンテーション

（１）提案者はプレゼンテーション形式による提案書の説明を行うこと。

（２）提案書の説明は、別途説明資料の作成も可とする。

（３）出席者は最大で▲名とする。

（４）プレゼンテーションは、原則本プロジェクトのプロジェクトマネージャが行うこと。ただし、セキュリティや運用に係る対応能力や経験等についても評価対象とするため、該当部分の説明は上級セキュリティエンジニア及び運用責任者が行うことも可能とする。

（５）プレゼンテーション時間は、原則として１時間以内とする。なお、１時間を超える説明時間が必要な場合には、事前に主管課に申し出を行い、許可を得ること。

（６）実施日時等、詳細は提出期限以降に連絡する。

５　提案書の提出

（１）提出期限

平成 28 年２月▲▲日（▲）午後▲時

（郵送による場合は、必着のこと。）

（２）提出場所

総務省大臣官房会計課契約第２係

東京都千代田区霞が関２丁目１番２号　中央合同庁舎第２号館

Tel:　03-5253-5132

（３）提出部数

書面▲部（うち社名・ロゴ等をマスキングしたものを▲部)、電子媒体（CD-ROM）２式

（４）提出方法

提案書の提出は、直接持参又は郵便（書留郵便に限る。）とすること。

郵便の場合には、「総務省ネットワーク基盤（ＬＡＮ）の構築等の請負　提案書在中」と朱書きすること。

（５）照会先

提案書作成要領等配布物に関し、照会事項がある場合は、下記の照会先に電子メールにて照会を行うとともに、電話にて連絡すること。

総務省大臣官房企画課情報システム室情報システム第三係

TEL：　03-5253-5159

Mail:　j3.kikakuka@soumu.go.jp

（６）その他

ア　分かりやすい日本語で記述すること。

イ　必要に応じて確認及び追加資料の提出を求めることがあるので、提案者はその内容についての説明及び資料提出を行うこと。

ウ　応募に要する経費は、提案応募者の負担とする。

エ　応募された提案書は、返却しない。

オ　提出された提案書等は、当該調達選定のためだけに使用する。

別紙１　機能証明書

項番号	内容	提案内容	提案内容 補足資料	記載箇所
第１	調達案件の概要に関する事項			
１	調達件名			
２	調達の背景			
３	目的及び期待する効果			
４	用語の定義			
５	業務・情報システムの概要			
（１）	システム概要			
（２）	システム構成			
ア	本省ＬＡＮ			
イ	拠点ＬＡＮ			
(ア)	外部拠点			
(イ)	地方支分部局			
(ウ)	ＤＲサイト			
ウ	総務省ＷＡＮ			
エ	外部監視室			
（３）	提供する機能等			
（４）	システム規模			
	総務省ＬＡＮは、総務省の職員により、原則として24時間365日利用するシステムである。ユーザアカウント数、ＬＡＮ端末数及び拠点数を以下に示す。総務省ＬＡＮの設計・構築に当たっては、本調達仕様書及び別紙１「要件定義書」（別紙１－１「要件定義書（システム全般）」から別紙１－４「要件定義書（運用及び維持保守・管理）」までを含む。以下同じ。）を満たすものであること。 （平成27年7月現在） ユーザアカウント数 約16,000個 ユーザアカウント数 約7,000個 非ユーザアカウント数 （共有メールアカウント、動作確認用アカウント等） 約5,000個 一時保管アカウント 約4,000個 ＬＡＮ端末数 約7,000台 拠点数 外部拠点 11拠点 地方支分部局 62拠点 ＤＲサイト １拠点 外部監視室 １拠点			
（５）	信頼性等及び情報セキュリティの確保			
	総務省ＬＡＮは、総務省の職員が組織活動及び業務を円滑に行う上でのシステム基盤である。そのため、総務省ＬＡＮは、安定的に稼働する必要がある。また、業務を遂行するに当たり、要機密情報、要保全情報及び要安定情報（以下「要保護情報」という。）を取り扱う。要保護情報を的確に取り扱うためには、十分なセキュリティ対策を施す必要がある。総務省ＬＡＮの設計・構築、運用及び維持保守・管理に当たっては、本調達仕様書及び別紙１「要件定義書」を満たすものであること。 また、運用及び維持保守・管理においては、システムの信頼性と情報セキュリティを確保するために、決められた業務のみを行うのではなく、サイバー攻撃のトレンド情報を踏まえ、その対応について設計・構築担当、運用及び維持保守・管理担当、セキュリティ担当が一体となって検討し、必要な対策等を行うなど、常に高度化・複雑化する新たな攻撃手法に対応していく必要がある。			
６	本調達の範囲			
（１）	本調達の対象範囲			
	総務省ＬＡＮの更改により表１　２に記載の全てのサービス・機能の提供を受けるため、サービス・機能の設計・構築、機器等の借入、運用及び維持保守・管理等を調達の対象範囲とするものである。なお、総務省ＬＡＮを構成する要素のうち、ＬＡＮ端末、端末ソフトウェア（詳細は、別紙３「ソフトウェア一覧」の「１　総務省ＬＡＮ保有ソフトウェアライセンス一覧」を参照すること。）及び複合機は、別途調達している。総務省ＬＡＮが提供するサービス・機能の実現に向け、端末ソフトウェアは、総務省の有するライセンスを活用することも可能である。			

別紙１　機能証明書

項番号	内容	提案内容	提案内容 補足資料	記載箇所
（２）	作業内容			
	作業に当たっては、「政府情報システムの整備及び管理に関する標準ガイドライン」（平成26年12月３日各府省情報化統括責任者(ＣＩＯ）連絡会議決定)に基づき、以下のとおり行うこと。 ア 統制作業 イ 設計・構築 （ア）設計・構築実施計画書等の作成 （イ）進捗管理 （ウ）要件定義書の確定 （エ）設計の実施 （オ）構築の実施 （カ）試験の実施 （キ）受入試験の実施支援 （ク）移行の実施 （ケ）引継ぎの実施 （コ）教育訓練の実施 （サ）ＯＤＢ登録用シートの提出 ウ 運用及び維持・保守管理 （ア）運用・保守要領の作成 （イ）中長期運用・保守作業計画の作成 （ウ）運用・保守実施計画書の作成 （エ）平常時対応 （オ）障害発生時対応 （カ）情報システムの現況確認支援 （キ）主管課等業務支援 （ク）運用業務及び保守作業の改善提案 （ケ）引継ぎ （コ）ＯＤＢ登録用シートの提出 エ ＯＤＢ登録用シートのその他事項に係る提出			
（３）	総務省ＬＡＮを構成する機器等			
	総務省ＬＡＮを構成する機器等の要件は、「第４　満たすべき要件に関する事項」のとおりとすること。			
7	契約期間			
	平成28年４月から平成33年３月まで			
8	作業スケジュール			
	総務省ＬＡＮの設計・構築における全体スケジュールを表１－３、図１－３に示す。 表１－３　全体作業スケジュール フェーズ　期間（想定）　備考 設計・構築　平成28年４月～平成28年12月 試験　平成29年１月～平成29年３月 移行　平成29年１月～平成29年３月 稼働　平成29年４月～　外部監視室を設置する場所での稼働を想定 移設　平成29年５月　総務省サーバ室での稼働に向けて移設を想定 運用　平成29年４月～平成33年３月 保守　平成29年４月～平成33年３月			
第２	調達案件及び関連調達案件の調達単位、調達の方法等に関する事項			
１	調達案件及びこれと関連する調達案件の調達単位、調達の方式、実施時期			
	関連する調達案件について、総務省ＬＡＮの全体スケジュールを図２－１に、調達単位、調達の方式、実施時期を表２－１に示す。			

別紙１　機能証明書

項番号	内容	提案内容	提案内容 補足資料	記載箇所
2	調達案件間の入札制限			
	相互牽制の観点から、「次期総務省ＬＡＮに係る調達支援業務の請負」の受注事業者及び「次期総務省ＬＡＮに係る工程管理支援業務の請負」の受注事業者は、入札制限の対象とし、本調達の請負者となることはできない。			
3	関連事業者との作業範囲			
	総務省ＬＡＮに係る調達範囲別の作業項目及び関連事業者との業務分担を表２－２に示す。			
第３	作業の実施内容に関する事項			
1	作業の内容			
（1）	統制作業			
	請負者は、契約期間を通じて、総務省ＬＡＮ全体に対し、以下の統制作業を行うこと。なお、初年度（平成28年度）における統制作業は、別途調達する工程管理支援事業者が実施する。			
ア	作業管理、進捗管理			
	契約期間中に発生する他の調達等に対し、総務省ＬＡＮ全体の統制を確保するために主管課が行う作業（作業管理、進捗管理等）について、作業の実施を支援すること。			
イ	変更管理			
	契約期間中に発生する総務省ＬＡＮの変更に対し、変更影響の分析、変更内容の管理等、変更管理作業の実施を支援すること。			
ウ	リスク管理			
	契約期間中に発生する総務省ＬＡＮのリスクに対し、リスク影響の分析、リスク対応方針の検討等、リスク管理作業の実施を支援すること。			
エ	課題管理			
	契約期間中に発生する総務省ＬＡＮの課題に対し、課題の影響分析、課題解決案の立案、課題への対応状況の管理等、課題管理作業の実施を支援すること。			
オ	品質管理			
	契約期間中に発生する総務省ＬＡＮの機能追加や機能変更に関し、全体の品質を管理するため、機能追加や機能変更に伴う成果物の整合性確認及び修正、機能追加や機能変更を実施する受注事業者の作業品質報告の確認等、品質管理作業の実施を支援すること。			
カ	各種技術支援、報告支援			
	契約期間中、主管課からの求めにより、技術的な確認への回答や問題点・課題の解決案提示等の各種技術支援を実施すること。また、主管課が総務省ＬＡＮについて対外的に報告する際、報告書類の作成等の支援を行うこと。			
（2）	設計・構築			
	総務省ＬＡＮの設計・構築に当たっては、以下に示す作業を行うこと。			
ア	設計・構築実施計画書等の作成			
	請負者は、「プロジェクト計画書」及び「プロジェクト管理要領」と整合をとりつつ、主管課の指示に基づき、工程管理支援事業者と調整の上、「設計・構築実施計画書」及び「設計・構築実施要領」を作成し、主管課の承認を受けること。			
イ	進捗管理			
	請負者は、設計・構築に当たって、適切に進捗の管理を行い、原則週次で主管課に進捗状況を報告すること。			
ウ	要件定義書の確定			
	請負者は、主管課、工程管理支援事業者、ＰＭＯ等と調整し、入札公告時の調達仕様書及び要件定義書に対して、調達時の請負者の提案内容に基づき変更を行い、主管課の合意のもと要件定義書を確定させること。			

別紙１　機能証明書

項番号	内容	提案内容	提案内容 補足資料	記載箇所
エ	設計の実施			
	請負者は、基本設計、詳細設計、移行設計及び運用設計を行い、成果物として各種設計書や各種規程、要領、操作マニュアル等を作成し、その内容について主管課の承認を得ること。詳細の要件として、別紙１「要件定義書」を満たすこと。			
オ	構築の実施			
	請負者は、「エ　設計の実施」で実施する設計に基づき、サーバ機器、ストレージ機器、メールサービス、ポータルサイトサービス、ファイル共有サービス、大容量ファイル転送サービス、コミュニケーションサービス、テレワークサービス、認証サービス、ペーパーレス会議サービス、プリントサービス、情報不正出力防止サービス、機密情報保護サービス、ディザスタリカバリサービス、ネットワークサービス、無線ＬＡＮ接続サービス、本省ＬＡＮ、拠点ＬＡＮ、インターネット接続回線、本省WAN、拠点WAN、外部監視室用回線、マルウェア対策（メール）サービス、マルウェア対策（インターネット・Ｗｅｂ）サービス、マルウェア対策（サーバ・ＬＡＮ端末・仮想デスクトップ）サービス、侵入検知防御サービス、不正接続機器検知サービス、特権アクセス制御サービス、セキュリティログ分析サービス、仮想ブラウザサービス、セキュリティ管理サービス、申請管理サービス、運用支援サービス、システム監視サービス、ログ管理サービス、バックアップサービス、電源管理サービス、資源管理サービス、モバイルデバイス管理サービス、シンクライアント管理サービス、検証環境、運用業務環境、ＫＶＭ、ＵＰＳ、ＬＡＮ端末マスタ、仮想デスクトップマスタその他総務省ＬＡＮの稼働に必要な機能やサービスを構築すること。詳細の要件として、別紙１－２「要件定義書（サービス・機器）」中に示す各構築要件を満たすこと。			
カ	試験の実施			
	請負者は、総務省ＬＡＮが求める要件を確実に満たしていることを確認するため、単体試験、結合試験、総合試験その他総務省ＬＡＮの稼働に必要な試験を計画し、計画に基づいて試験を実施すること。なお、それぞれの試験計画、試験結果について主管課の承認を受けること。詳細の要件として、別紙１－１「要件定義書（システム全般）」の「第４　構築・試験」を満たすこと。			
キ	受入試験の実施支援			
	主管課は、総務省ＬＡＮの構築が完了する前に、求めている要件を満たしているか確認するため、受入試験を実施する。請負者は、受入試験の計画策定、受入試験の実施を支援すること。また、受入試験の結果、サービス・機能等を満たしていない点や不具合が発生した場合、改修のための計画を策定し、速やかに取り組むこと。詳細の要件として、別紙１－１「要件定義書（システム全般）」の「第５　受入試験支援」を満たすこと。			
ク	移行の実施			
	請負者は、総務省ＬＡＮの安全かつ確実なシステムの切り替えのため、移行計画の策定、移行設計、移行手順の作成、リスクの識別・コンティンジェンシープランの作成、移行判定基準の作成、移行計画に基づいた移行を実施すること。詳細の要件として、別紙１－１「要件定義書（システム全般）」の「第６　情報システムの移行」を満たすこと。			
ケ	引継ぎの実施			
	請負者は、現行総務省ＬＡＮの現行請負者から業務内容を明らかにした書類等により引継ぎを受けること。なお、その際の引継ぎに必要となる経費は、現行請負者の負担とする。また、請負者は、本請負業務を終える前に、次々期総務省ＬＡＮの請負者に対して引継ぎを実施すること。引継ぎが円滑に実施されなかったことにより次々期総務省ＬＡＮの請負者の業務遂行に支障が出た場合には、改善されるまで支援を行うこと。なお、その際の引継ぎに必要となる経費は、請負者の負担とすること。詳細の要件として、別紙１－１「要件定義書（システム全般）」の「第７　引継ぎ」を満たすこと。			
コ	教育訓練の実施			
	請負者は、業務運用の継続性を担保するためにユーザ・部局運用担当者に対する教育を行うこと。詳細の要件として、別紙１－１「要件定義書（システム全般）」の「第８　教育」を満たすこと。			

別紙１　機能証明書

項番号	内容	提案内容	提案内容 補足資料	記載箇所
サ	ＯＤＢ登録用シートの提出			
	請負者は、「政府情報システムの整備及び管理に関する標準ガイドライン実務手引書（第３編第６章　調達）」（平成27年３月19日内閣官房情報通信技術（ＩＴ）総合戦略室。総務省行政管理局。）における「第６章２．１）ウ２（１）ア（キ）　ＯＤＢ登録用シートの提出」に基づき、以下に掲げる事項について記載したＯＤＢ登録用シートを提出すること。 (ア) ハードウェアの管理 (イ) ソフトウェアの管理 (ウ) 回線の管理 (エ) 外部サービスの管理 (オ) 施設の管理 (カ) 公開ドメインの管理 (キ) 取扱情報の管理 (ク) 情報セキュリティ要件の管理 (ケ) 指標の管理			
（３）	運用及び維持・保守管理			
	総務省ＬＡＮの運用及び維持・保守管理に当たっては、以下に示す作業を行うこと。			
ア	運用・保守要領の作成			
	請負者は、運用を開始するに当たり、「運用・保守要領」を作成し、主管課の承認を受けること。			
イ	中長期運用・保守作業計画の作成			
	請負者は、「運用・保守要領」に基づき、運用期間中に計画的に発生する作業内容、その想定される時期等を取りまとめた「中長期運用・保守作業計画」を作成すること。「中長期運用・保守作業計画」には、情報システムの構成やライフサイクルを通じた運用業務及び保守作業の内容について記載すること。			
ウ	運用・保守実施計画書の作成			
	請負者は、具体的な作業内容や実施時間、実施サイクル等に関する内容を取りまとめた「運用・保守実施計画書」を作成し、主管課の承認を受けること。			
エ	平常時対応			
	請負者は、総務省ＬＡＮの安定性、安全性を維持するため、構成管理、変更管理、インシデント管理、問題管理、サービスレベル管理、キャパシティ管理、可用性管理、情報セキュリティ管理、継続的なサービス改善等の運用業務を行うこと。情報セキュリティ管理については、サイバー攻撃に関するトレンド情報を入手し、総務省ＬＡＮにおいて可能な防御策を確認の上、必要な機器の設定変更等を迅速かつ適切に行うこと。 また、運用支援業務として、職員からの電話照会を一元的に受付・管理及び対応を行うヘルプデスク業務を行うこと。なお、運用支援業務のうちＬＡＮ端末の操作方法、利用申請の手続等に関する問い合わせ対応業務、総務省ＬＡＮ管理規程で定める申請書の受付・審査等業務は、主管課が行う。 請負者は、総務省ＬＡＮの安定性、安全性を維持するため、ソフトウェア保守、ハードウェア保守等の保守業務を行うこと。詳細の要件として、別紙１－４「要件定義書（運用及び維持保守・管理）」を満たすこと。			
オ	障害発生時対応			
	請負者は、情報システムの障害発生時（又は発生が見込まれる時）には、速やかに主管課に報告するとともに、その緊急度及び影響度を判断の上、障害発生箇所の切り分け、復旧作業、復旧確認作業に対応すること。 また、請負者は、情報セキュリティインシデントの発生時（又は発生が見込まれる時）も同様に、感染や被害の状況を的確に把握し、その緊急度及び影響度を判断の上、被害の拡大を防止するための緊急対策、根本原因の究明と機器の設定変更を含む恒久対策を行うこと。詳細の要件として、別紙１－４「要件定義書（運用及び維持保守・管理）」を満たすこと。			
カ	情報システムの現況確認支援			
	請負者は、年１回、主管課の指示に基づき、ＯＤＢ格納データと情報システムの現況との突合・確認（以下「現況確認」という。）の実施を支援すること。現況確認の結果、ＯＤＢの格納データと情報システムの現況との間の差異がみられる場合は、「運用・保守要領」に定める変更管理方法に従い、差異を解消すること。また、ライセンス許諾条件が合致しない場合や、サポート切れのソフトウェア製品の仕様が明らかになった場合は、当該条件への適合可否や更新の可否、条件等について、更新した場合の影響の有無を含め、主管課に報告すること。			

別紙１　機能証明書

項番号	内容	提案内容	提案内容 補足資料	記載箇所
キ	主管課等業務支援			
	請負者は、総務省ＬＡＮへの接続、政府共通ＰＦへの移行等、主管課、部局担当者からの各種照会に対し、要望確認のためのヒアリング等を実施し、適宜技術的観点から主管課等への支援を行うこと。			
ク	定期報告			
	システムの操作や監視状況、障害発生・対応の状況、サービス指標の実績等を日次、週次、月次及び年次で適宜報告すること。			
ケ	運用業務及び保守作業の改善提案			
	請負者は、年度末までに年間の運用実績及び保守作業を取りまとめるとともに、必要に応じて「運用・保守要領」、「中長期運用・保守作業計画」及び「運用・保守実施計画書」に対する改善提案や、総務省ＬＡＮ構築等請負業務の実施全般に係る質の向上の観点から取り組むべき事項等の提案を行うこと。 また、特に情報セキュリティに関する点については、平常時及び障害発生時のみならず、脆弱性やサイバー攻撃の事例とその対策等を調査の上、機器の設定変更等、必要な対策を適切に実施することができるよう、継続的な改善提案を行うこと。			
コ	引継ぎ			
	請負者は、本業務の開始日までに、業務内容を明らかにした書類等により現行請負者から業務の引継ぎを受けること。なお、その際の引継ぎに必要となる経費は、現行請負者の負担とする。また、本業務の終了に伴い、請負者は、当該業務の開始日までに、業務内容を明らかにした書類等により次々期受注事業者に対し、引継ぎを行うこと。引継ぎが円滑に実施されなかったことにより次々期受注事業者の業務遂行に支障が出た場合には、改善されるまで支援を行うこと。なお、その際の引継ぎに必要となる経費は、請負者の負担とすること。			
サ	ＯＤＢ登録用シートの提出			
	請負者は、請負者は、「政府情報システムの整備及び管理に関する標準ガイドライン実務手引書（第３編第６章　調達）」における「第６章２．１）ウ２（１）ウ（ク）ＯＤＢ登録用シートの提出」に基づき、以下に掲げる事項について記載したＯＤＢ登録用シートを提出すること。 (ア) 各データの変更管理 (イ) 作業実績等の管理			
（４）	ＯＤＢ登録用シートのその他記載事項に係る提出			
	ア 請負者は、「政府情報システムの整備及び管理に関する標準ガイドライン」における別紙２「情報システムの経費区分」に基づき区分等した契約金額の内訳を記載した「ＯＤＢ登録用シート」を契約締結後速やかに提出すること。			
	イ 請負者は、主管課から求められた場合は、スケジュールや工数等の計画値及び実績値について記載した「ＯＤＢ登録用シート」を提出すること。			
２	成果物の範囲、納品期日等			
（１）	成果物、内容、納品数量、納品期日			
	本業務の成果物を表３－１に示す。			
（２）	納品方法			
	ア 成果物は、全て日本語で作成すること。			
	イ 用字・用語・記述符号の表記については、「公用文作成の要領（昭和27年４月４日内閣閣甲第16号内閣官房長官依命通知）」を参考にすること。			
	ウ 情報処理に関する用語の表記については、日本工業規格（ＪＩＳ）の規定を参考にすること。			
	エ 成果物は紙媒体及び電磁的記録媒体により作成し、総務省から特別に示す場合を除き、原則紙媒体は正１部・副１部、電磁的記録媒体は１部を納品すること。			
	オ 紙媒体による納品について、用紙のサイズは、原則として日本工業規格Ａ列４番とするが、必要に応じて日本工業規格Ａ列３番を使用すること。			

別紙１　機能証明書

項番号	内容	提案内容	提案内容 補足資料	記載箇所
	カ 電磁的記録媒体による納品について、Ｍｉｃｒｏｓｏｆｔ Ｏｆｆｉｃｅ（Ｗｏｒｄ、Ｅｘｃｅｌ及びＰｏｗｅｒＰｏｉｎｔ）又はＰＤＦのファイル形式で作成し、ＤＶＤの媒体に格納して納品すること。また、図表等の元データも併せて納品すること。			
	キ 成果物の作成に当たって、特別なツールを使用する場合は、担当職員の承認を得ること。			
	ク 成果物が外部に不正に使用されたり、納品過程において改ざんされたりすることのないよう、安全な納品方法を提案し、成果物の情報セキュリティの確保に留意すること。			
	ケ 電磁的記録媒体により納品する場合は、不正プログラム対策ソフトウェアによる確認を行うなどして、成果物に不正プログラムが混入することのないよう、適切に対処すること。			
（３）	納品場所			
	請負者は、納入成果物に示した完成図書一式を本省に納品すること。また、総務省ＬＡＮサービス一式は、それぞれ表３－２に示す各拠点に納品すること。詳細は、主管課の指示によるものとする。			
（４）	作業窓口			
	総務省大臣官房企画課情報システム室第三係			
第４	満たすべき要件に関する事項			
１	調達仕様書記載の要件			
	本業務の実施に当たっては、本調達仕様書の記載事項の内容を理解した上で、全ての要件を満たすこと。			
２	要件定義書記載の要件			
（１）	「システム全般」の要件			
ア	規模・性能			
	本業務の実施に当たって、共通方針、規模・性能要件を理解した上で、全ての要件を満たすこと。なお、詳細な要件は、別紙１－１「要件定義書（システム全般）」の「第１　規模・性能」を参照すること。			
イ	信頼性等			
	本業務の実施に当たって、信頼性要件、拡張性要件、上位互換性要件、システム中立性要件、事業継続性要件を理解した上で、全ての要件を満たすこと。なお、詳細な要件は、別紙１－１「要件定義書（システム全般）」の「第２　信頼性等」を参照すること。			
ウ	情報セキュリティ			
	本業務の実施に当たって、情報セキュリティ対策、本調達の遂行等に係る情報セキュリティ対策を理解した上で、全ての要件を満たすこと。なお、詳細な要件は、別紙１－１「要件定義書（システム全般）」の「第３　情報セキュリティ」を参照すること。			
エ	構築・試験			
	本業務の実施に当たって、試験要件、試験場所を理解した上で、全ての要件を満たすこと。なお、詳細な要件は、別紙１－１「要件定義書（システム全般）」の「第４　構築・試験」を参照すること。			
オ	受入試験支援			
	本業務の実施に当たって、受入試験支援を理解した上で、全ての要件を満たすこと。なお、詳細な要件は、別紙１－１「要件定義書（システム全般）」の「第５　受入試験支援」を参照すること。			
カ	情報システムの移行			
	本業務の実施に当たって、移行に係る要件、移行作業の進め方を理解した上で、全ての要件を満たすこと。なお、詳細な要件は、別紙１－１「要件定義書（システム全般）」の「第６　情報システムの移行」を参照すること。			

別紙１　機能証明書

項番号	内容	提案内容	提案内容 補足資料	記載箇所
キ	引継ぎ			
	本業務の実施に当たって、業務運用開始時の引継ぎ、業務終了時の引継ぎを理解した上で、全ての要件を満たすこと。なお、詳細な要件は、別紙１－１「要件定義書（システム全般）」の「第７　引継ぎ」を参照すること。			
ク	教育			
	本業務の実施に当たって、教育に係る要件を理解した上で、全ての要件を満たすこと。なお、詳細な要件は、別紙１－１「要件定義書（システム全般）」の「第８　教育」を参照すること。			
ケ	施設・設備			
	本業務の実施に当たって、本省サーバ室、ディザスタリカバリサイト、外部監視室、工事に係る要件を理解した上で、全ての要件を満たすこと。なお、詳細な要件は、別紙１－１「要件定義書（システム全般）」の「第９　施設・設備」を参照すること。			
（２）	「サービス・機器」の要件			
ア	調達機器の共通事項			
	総務省ＬＡＮとして提供する全てのサービスは、セキュリティの担保上の理由から、原則として全て、オンプレミスで提供を行うこと。なお、詳細な要件は、別紙１－２「要件定義書（サービス・機器）」の「第１　調達機器の共通事項」を参照すること。			
イ	共用サーバ・ストレージ			
（ア）	サーバ機器			
	本省及びディザスタリカバリサイトにおいて、各サービス機能、セキュリティ機能、運用管理機能を構築するためのサーバ機器を提供すること。なお、詳細な要件は、別紙１－２「要件定義書（サービス・機器）」の「第２　１　サーバ機器」を参照すること。			
（イ）	ストレージ機器			
	本省・ディザスタリカバリサイトにおいて、サーバ機能、セキュリティ機能、運用管理機能のストレージ機器を提供する。ストレージ機能として、スナップショット、仮想マシンバックアップ、リストア、レプリケーション、重複排除、仮想クローン、読み取りを有すること。なお、詳細な要件は、別紙１－２「要件定義書（サービス・機器）」の「第２　２　ストレージ機器」を参照すること。			
ウ	総務省ＬＡＮサービス			
（ア）	メールサービス			
	総務省職員が省内外との連絡手段として電子メールを用いるため、メールサービスを提供する。メールサービスには、メール送受信、インターネットメール中継、政府共通ネットワークメール中継、メールストア、メーリングリスト、メールマガジン配信、メールアーカイブ及びアドレス帳機能等が含まれる。なお、詳細な要件は、別紙１－２「要件定義書（サービス・機器）」の「第３　１　メールサービス」を参照すること。			
（イ）	ポータルサイトサービス			
	総務省職員が円滑に業務を遂行するため、ポータルサイトサービスを提供する。ポータルサイトには、総務省ＬＡＮの利用規定・ＦＡＱ、インターネット・イントラネット・政府共通ネットワークのＷｅｂサイト等の情報を公開する。また、電子掲示板、電子会議室、設備予約、アンケート及びスケジューラ等が含まれる。なお、詳細な要件は、別紙１－２「要件定義書（サービス・機器）」の「第３　２　ポータルサイトサービス」を参照すること。			
（ウ）	ファイル共有サービス			
	総務省職員が円滑に業務情報を交換・記録するため、ファイル共有サービスを提供する。２種類の共有フォルダ（組織用・個人用）を提供する。組織用共有フォルダは、職員が所属する部署によりアクセス権が設定される。なお、詳細な要件は、別紙１－２「要件定義書（サービス・機器）」の「第３　３　ファイル共有サービス」を参照すること。			
（エ）	大容量ファイル転送サービス			
	総務省職員と省外の関係者間において、メール添付では扱えない大容量ファイルの送受信を行うために大容量ファイル転送サービスを提供する。なお、詳細な要件は、別紙１－２「要件定義書（サービス・機器）」の「第３　４　大容量ファイル転送サービス」を参照すること。			

別紙１　機能証明書

項番号	内容	提案内容	提案内容 補足資料	記載箇所
（オ）	認証サービス			
	総務省職員等のアカウント情報を一元管理し、各サービスへの接続時に認証及びアクセス権の付与を行うため、認証サービスを提供する。生体認証サービスを利用することにより、パスワードの入力が不要になる。各種サービスにおいて利用する証明書を発行する。なお、詳細な要件は、別紙１－２「要件定義書（サービス・機器）」の「第３　５　認証サービス」を参照すること。			
（カ）	テレワークサービス			
	総務省職員の多様で柔軟な働き方を可能にし、ワーク・ライフ・バランスを実現するため、テレワークサービスを提供する。在宅業務、出張、災害時において、ＬＡＮ端末・タブレット型端末・シンクライアントを利用した個人所有端末からサービスを利用できる。通常時は本省へアクセス、災害発生時はディザスタリカバリサイトへアクセスする。なお、詳細な要件は、別紙１－２「要件定義書（サービス・機器）」の「第３　６　テレワークサービス」を参照すること。			
（キ）	コミュニケーションサービス			
	メッセージ交換、在席管理、Ｗｅｂ会議を用いてコミュニケーションを円滑にし、ワークスタイル変革を推進するため、コミュニケーションサービスを提供する。なお、詳細な要件は、別紙１－２「要件定義書（サービス・機器）」の「第３　７　コミュニケーションサービス」を参照すること。			
（ク）	ペーパーレス会議サービス			
	会議室内での電子データの資料共有・閲覧を可能にし、業務効率を向上させるため、ペーパーレス会議サービスを提供する。タブレット型端末からＷｅｂブラウザ又は専用ソフトウェアを介して、会議資料を共有・閲覧する。なお、詳細な要件は、別紙１－２「要件定義書（サービス・機器）」の「第３　８　ペーパーレス会議サービス」を参照すること。			
（ケ）	プリントサービス			
	プリントサービスは、職員がＬＡＮ端末から任意の印刷機器を指定し印刷を行う「プリント機能」と、印刷機器からのプリントアウト時にICカードによる認証が必要な「認証プリント機能」を提供するサービスである。放置された資料からの情報漏えいを防ぐため、国家公務員身分証明証として用いる個人番号カード及びＦｅｌｉＣａカードによって認証することで、印刷できるようにする。プリントサービスは、全てのＬＡＮ複合機、ＬＡＮプリンタで利用できるものとする。なお、詳細な要件は、別紙１－２「要件定義書（サービス・機器）」の「第３　９　プリントサービス」を参照すること。			
（コ）	情報不正出力防止サービス			
	情報不正出力防止サービスは、電磁的記憶媒体による総務省ＬＡＮ外部への電子データ入出力を制限し、情報の不正出力を防止する環境を提供する。職員は、総務省ＬＡＮ外部から電磁的記憶媒体による電子データの受取りを行う場合は、ウイルスチェック用端末でウイルスチェックを行い、ＬＡＮ端末に接続許可されたUSBデバイスを利用してＬＡＮ端末に電子データを移動する。ＬＡＮ端末では、電磁的記録媒体の制限をかけてあり、許可された電磁的記憶媒体しか利用できない。なお、詳細な要件は、別紙１－２「要件定義書（サービス・機器）」の「第３　10　情報不正出力防止サービス」を参照すること。			
（サ）	機密情報保護サービス			
	機密情報保護サービスは、ＬＡＮ端末から機微度の高い情報の不正な閲覧を防止するために、ファイルを暗号化専用フォルダに移動することにより自動的に暗号化して保存し、事前に許可を得た職員のみが閲覧・編集・印刷等の機能を制御可能とするサービスである。職員は、ＬＡＮ端末上で作成したファイルを暗号化専用フォルダに移動することにより、ファイルを暗号化できる。職員は、自身のアクセス権に基づき、暗号化されたファイルを「読込」「書込」「編集」「印刷」することができる。なお、詳細な要件は、別紙１－２「要件定義書（サービス・機器）」の「第３　11　機密情報保護サービス」を参照すること。			

別紙１　機能証明書

項番号	内容	提案内容	提案内容 補足資料	記載箇所
（シ）	ディザスタリカバリサービス			
	大規模災害発生等の有事の際においても総務省ＬＡＮの主要サービスを提供し、業務継続性を確保するため、ディザスタリカバリサービスを提供する。執務場所に参集できない場合は、テレワークサービスを利用して総務省ＬＡＮの主要サービスを利用する。ディザスタリカバリサービスで提供するサービスには、メールサービス、ポータルサイトサービス、ファイル共有サービス、認証サービス、テレワークサービス、コミュニケーションサービス、プリントサービス、ネットワークサービス、無線ＬＡＮ接続サービス、システム監視機能が含まれる。なお、詳細な要件は、別紙１－２「要件定義書（サービス・機器）」の「第３　12　ディザスタリカバリサービス」を参照すること。			
エ	セキュリティサービス			
（ア）	マルウェア対策（メール）サービス			
	メールを侵入経路とするマルウェア等の侵入を早期に検知・駆除するため、マルウェア対策（メール）サービスを提供する。インターネット及び政府共通ネットワークと本省間のメール通信のマルウェア検査・検知を行う。インターネットと本省間のメール通信に対しては、振る舞い検知型のマルウェア検査を行う。迷惑メール判定を行い、迷惑メールを防御する。ドメイン認証やレピュテーション情報を用いて、不審なメールから防御する。なお、詳細な要件は、別紙１－２「要件定義書（サービス・機器）」の「第４　１　マルウェア対策（メール）サービス」を参照すること。			
（イ）	マルウェア対策（インターネット・Ｗｅｂ）サービス			
	インターネット及び政府共通ネットワークを経由したＷｅｂ閲覧を侵入経路とするマルウェアの侵入を早期に検知・駆除するため、マルウェア対策（インターネット・Ｗｅｂ）サービスを提供する。インターネット及び政府共通ネットワークと本省間のＷｅｂ通信のマルウェア検査・検知を行う。インターネットと本省間のＷｅｂ通信に対しては、振る舞い検知型のマルウェア検査を行う。レピュテーション情報等を用いて、不審なＷｅｂサイトへのアクセスを防止する。なお、詳細な要件は、別紙１－２「要件定義書（サービス・機器）」の「第４　２　マルウェア対策（インターネット・Ｗｅｂ）サービス」を参照すること。			
（ウ）	マルウェア対策（サーバ・ＬＡＮ端末・仮想デスクトップ）サービス			
	サーバ、共有フォルダ及びＬＡＮ端末、仮想デスクトップにマルウェアが侵入した際、早期に検知・駆除するため、マルウェア対策（サーバ・ＬＡＮ端末）サービスを提供する。サーバ及び共有フォルダ、ＬＡＮ端末のマルウェア検査・検知を行う。サーバ及びＬＡＮ端末では、ホスト間の通信の制御を行う。ＬＡＮ端末では、振る舞い検知型のマルウェア検査を行う。なお、詳細な要件は、別紙１－２「要件定義書（サービス・機器）」の「第４　３　マルウェア対策（サーバ・ＬＡＮ端末・仮想デスクトップ）サービス」を参照すること。			
（エ）	侵入検知防御サービス			
	インターネット及び政府共通ネットワークから省内への不正侵入を防ぐため、侵入検知防御サービスを提供する。サイバー攻撃などの総務省ＬＡＮへの不正なアクセスに対して、アクセス制御・侵入検知を行う。総務省ＬＡＮの各セグメント間のアクセス制御を行う。なお、詳細な要件は、別紙１－２「要件定義書（サービス・機器）」の「第４　４　侵入検知防御サービス」を参照すること。			
（オ）	不正接続機器検知サービス			
	総務省ＬＡＮに不正に接続された機器に起因したウイルス感染から総務省ＬＡＮを保護するため、不正接続機器検知サービスを提供する。総務省ＬＡＮに接続可能な機器を事前に登録し、限定する。未登録の機器が総務省ＬＡＮに接続された際に、接続通知・通信の遮断を行う。なお、詳細な要件は、別紙１－２「要件定義書（サービス・機器）」の「第４　５　不正接続機器検知サービス」を参照すること。			
（カ）	特権アクセス制御サービス			
	総務省ＬＡＮを構成する各機器に対する不正な管理操作を防止するため、特権アクセス制御サービスを提供する。管理目的のアクセス及び操作を、許可された専用端末のみに限定する。また、管理目的のアクセス及び操作のログを収集し、記録する。なお、詳細な要件は、別紙１－２「要件定義書（サービス・機器）」の「第４６　特権アクセス制御サービス」を参照すること。			

別紙１　機能証明書

項番号	内容	提案内容	提案内容 補足資料	記載箇所
（キ）	セキュリティ管理サービス			
	ＬＡＮ端末及びＷｉｎｄｏｗｓサーバ、Ｌｉｎｕｘサーバのセキュリティポリシー遵守状況を確認するため、セキュリティ管理サービスを提供する。ポリシーテンプレートを作成し、ＬＡＮ端末、Ｗｉｎｄｏｗｓサーバ、Ｌｉｎｕｘサーバが本ポリシーに準拠しているか確認する。監査に必要なログを収集し、保全する。なお、詳細な要件は、別紙１－２「要件定義書（サービス・機器）」の「第４　７　セキュリティ管理サービス」を参照すること。			
（ク）	セキュリティログ分析サービス			
	セキュリティインシデントの兆候を早期に検知するため、セキュリティログ分析サービスを提供する。複数のセキュリティログやイベントを用いて相関分析を実施することで、早期検知を実現する。検知したイベントの詳細を調査するため、関連するログを検索、分析する。なお、詳細な要件は、別紙１－２「要件定義書（サービス・機器）」の「第４　８　セキュリティ分析サービス」を参照すること。			
（ケ）	仮想ブラウザサービス			
	マルウェアが直接ＬＡＮ端末に侵入するリスクを低減するために、総務省職員がインターネットへのＷｅｂアクセスを行う専用ブラウザ環境として、仮想ブラウザサービスを提供する。インターネットにアクセスする際は、ＬＡＮ端末のブラウザを利用せずに、本サービスからアクセスする。なお、詳細な要件は、別紙１－２「要件定義書（サービス・機器）」の「第４　９　仮想ブラウザサービス」を参照すること。			
オ	運用管理サービス			
（ア）	申請管理サービス			
	申請管理サービスは、職員から受け付けた総務省ＬＡＮサービスに関する申請依頼を一元管理し、申請内容に応じて、総務省ＬＡＮサービスと連携するサービスである。職員は、申請書を申請管理サービスを介して提出し、主管課に承認依頼を行う。主管課は、職員からの申請に対して承認又は拒否を行い、運用要員に承認した申請の対応を依頼する。運用要員は、運用管理端末から申請管理サービスに接続し、申請内容を登録する。申請管理サービスは、登録された申請内容に応じて該当するサービスと連携する。なお、詳細な要件は、別紙１－２「要件定義書（サービス・機器）」の「第５　１　申請管理サービス」を参照すること。			
（イ）	運用支援サービス			
	運用支援サービスは、総務省ＬＡＮに関する問い合わせを一元管理し、進捗状況の確認や問題分析のための情報収集する環境を提供するサービスである。問い合わせとイベントをインシデントとして登録し、一次対処、復旧までの調査・回答の進捗管理を運用員内で共有できるようにする。なお、詳細な要件は、別紙１－２「要件定義書（サービス・機器）」の「第５　２　運用支援サービス」を参照すること。			
（ウ）	システム監視サービス			
	システム監視サービスは、システムの可用性を維持するため、総務省ＬＡＮのサービスを提供する機器の障害検知やリソース監視、トラフィック監視、その報告を行うためのサービスである。サーバ、ネットワーク機器及びアプライアンス機器の状態を取得し、基準値から外れるものに対し、警告を発生させる。サーバのシステムログを収集し、エラー発生時に警告を発生させる。運用要員が、発生したアラートの内容を確認することができる。なお、詳細な要件は、別紙１－２「要件定義書（サービス・機器）」の「第５　３　システム監視サービス」を参照すること。			
（エ）	ログ管理サービス			
	ログ管理サービスは、総務省ＬＡＮサービスを構成する機器が出力したログ（認証ログ、アクセスログ、セキュリティログ、利用状況ログ、ＬＡＮ端末の操作ログ等）を収集し、運用保守及びインシデント対応時に、検索、閲覧及び分析するためのサービスである。運用要員は、運用保守及びインシデント対応時に、必要な各種総務省ＬＡＮサービスのログ（認証ログ、アクセスログ、セキュリティログ、利用状況ログ、ＬＡＮ端末の操作ログ等）の情報を収集、検索、分析する。各種ログを自動的に収集し、一定期間保管する。なお、詳細な要件は、別紙１－２「要件定義書（サービス・機器）」の「第５　４　ログ管理サービス」を参照すること。			
（オ）	バックアップサービス			
	総務省ＬＡＮの可用性を維持するために、バックアップサービスを提供する。障害発生や操作ミス等でデータが消失又は破損した場合に復旧可能とし、また、災害発生時にサービスを継続利用可能とする。自動でバックアップを取得し、一定期間保管する。なお、詳細な要件は、別紙１－２「要件定義書（サービス・機器）」の「第５　５　バックアップサービス」を参照すること。			

別紙１　機能証明書

項番号	内容	提案内容	提案内容 補足資料	記載箇所
（カ）	電源管理サービス			
	電源障害・法定停電・災害時等に機器を安全に停止しかつ機器の起動制御を行うため、電源管理サービスを提供する。自動でシステム停止・起動を行う。なお、詳細な要件は、別紙１－２「要件定義書（サービス・機器）」の「第５　６　電源管理サービス」を参照すること。			
（キ）	資源管理サービス			
	資源管理サービスは、管理対象機器のハードウェア情報、ソフトウェア情報、ライセンス情報等の情報収集や、ソフトウェア配付、セキュリティパッチ等の配付、ＬＡＮ端末接続デバイスの制御、各種設定情報の変更等を一括管理するサービスである。ＬＡＮ端末にソフトウェア（セキュリティパッチ等）をインストールする必要が発生した場合、ソフトウェア（セキュリティパッチ等）の配信を制御できる。職員は、クライアント資源管理サービスを利用し、業務に必要なソフトウェアを任意にＬＡＮ端末にインストールすることができる。総務省が配備した記憶媒体（ＤＶＤ、セキュリティＵＳＢメモリ）以外の記憶媒体をＬＡＮ端末に接続した際に、利用制限できる。なお、詳細な要件は、別紙１－２「要件定義書（サービス・機器）」の「第５　７　資源管理サービス」を参照すること。			
（ク）	モバイルデバイス管理サービス			
	モバイルデバイス管理サービスは、職員が省内外で利用するタブレット型端末のハードウェア情報、ソフトウェア情報、利用状況を自動で収集することにより、運用要員が一元的に管理を行うためのサービスである。タブレット型端末に盗難や紛失が発生した場合には、リモートワイプを実行することにより情報漏えいを防ぐ。また、ＯＳやアプリケーションの導入や更新の作業にも利用する。なお、詳細な要件は、別紙１－２「要件定義書（サービス・機器）」の「第５　８　モバイルデバイス管理サービス」を参照すること。			
（ケ）	シンクライアント管理サービス			
	シンクライアント管理サービスは、テレワークで利用するシンクライアントのイメージの管理、セットアップ処理を行うサービスである。なお、詳細な要件は、別紙１－２「要件定義書（サービス・機器）」の「第５　９　シンクライアント管理サービス」を参照すること。			
カ	その他機器基盤			
（ア）	検証環境			
	サーバ、ストレージ、ネットワーク機器の保守作業や障害の原因調査作業を実施する際に、総務省ＬＡＮに及ぼす影響とその手順を確認するため、検証環境を提供する。なお、詳細な要件は、別紙１－２「要件定義書（サービス・機器）」の「第６　１　検証環境」を参照すること。			
（イ）	運用業務環境			
	運用業務環境は、運用要員が日常の運用業務に使用する設備環境である。運用要員は、利用する機能ごとの個別環境を利用する。個別環境には、一般執務環境、サーバ接続用環境、遠隔操作用環境がある。運用要員の共有環境として、メンテナンス用端末、地方監視用サーバ、キッティングサーバがある。なお、詳細な要件は、別紙１－２「要件定義書（サービス・機器）」の「第６　２　運用業務環境」を参照すること。			
（ウ）	ＫＶＭ			
	サーバ等の機器に対しコンソールからの操作を可能とするため、操作環境を提供する。なお、詳細な要件は、別紙１－２「要件定義書（サービス・機器）」の「第６　３　ＫＶＭ」を参照すること。			
（エ）	ＵＰＳ			
	機器に安定した電源を供給し、電源供給が途絶えた際に一定時間電源を供給するため、ＵＰＳを準備する。また、停電の際安全に機器を停止するため、電源管理機能と連携する。なお、詳細な要件は、別紙１－２「要件定義書（サービス・機器）」の「第６　４　ＵＰＳ」を参照すること。			
（オ）	ＬＡＮ端末マスタ			
	ＬＡＮ端末マスタは、総務省ＬＡＮ端末をキッティングする際に基となるイメージであり、総務省職員が通常業務で利用するソフトウェアから構成される。ＬＡＮ端末の機種ごとに準備されていること。なお、詳細な要件は、別紙１－２「要件定義書（サービス・機器）」の「第６　５　ＬＡＮ端末マスタ」を参照すること。			

別紙１　機能証明書

項番号	内容	提案内容	提案内容 補足資料	記載箇所
（カ）	仮想デスクトップマスタ			
	仮想デスクトップマスタは、仮想デスクトップを複製する際の基となるイメージであり、総務省職員が通常業務で利用するソフトウェアから構成される。仮想デスクトップの環境ごとに準備されていること。なお、詳細な要件は、別紙１－２「要件定義書（サービス・機器）」の「第６　６　仮想デスクトップマスタ」を参照すること。			
キ	ネットワーク基盤			
（ア）	本省ＬＡＮ			
	本省ＬＡＮは、総務省ＬＡＮ全体にネットワークサービスを提供し、総務省職員が総務省ＬＡＮサービスを利用するため、本省ＬＡＮを提供する。なお、詳細な要件は、別紙１－２「要件定義書（サービス・機器）」の「第７　１　本省ＬＡＮ」を参照すること。			
（イ）	拠点ＬＡＮ			
	拠点ＬＡＮは、総務省職員が各拠点において総務省ＬＡＮサービスを利用するため、拠点ＬＡＮを提供する。なお、詳細な要件は、別紙１－２「要件定義書（サービス・機器）」の「第７　２　拠点ＬＡＮ」を参照すること。			
（ウ）	ネットワークサービス			
	総務省職員がネットワークを介した各種サービス（ＤＨＣＰ、ＤＮＳ、ＮＴＰ、プロキシ）を利用するため、ネットワークサービスを提供する。なお、詳細な要件は、別紙１－２「要件定義書（サービス・機器）」の「第７　３　ネットワークサービス」を参照すること。			
（エ）	無線ＬＡＮ接続サービス			
	端末の設置場所を固定せず、執務場所にとらわれないネットワーク接続環境を実現するため、無線ＬＡＮ接続サービスを提供する。ペーパーレス会議システムを行う際に、無線ＬＡＮ接続サービスを提供する。なお、詳細な要件は、別紙１－２「要件定義書（サービス・機器）」の「第７　４　無線ＬＡＮ接続サービス」を参照すること。			
（オ）	インターネット接続回線			
	総務省職員が業務を遂行する際の情報収集及び情報交換を行うため、インターネット接続回線を提供する。なお、詳細な要件は、別紙１－２「要件定義書（サービス・機器）」の「第７　５　インターネット接続回線」を参照すること。			
（カ）	本省ＷＡＮ			
	本省、各地方拠点及びディザスタリカバリサイトで相互に通信を行い、総務省ＬＡＮサービスを利用するため、本省ＷＡＮ（本省側におけるネットワーク及び回線）を提供する。閉域網を使用した通信環境を提供する。なお、詳細な要件は、別紙１－２「要件定義書（サービス・機器）」の「第７　６　本省ＷＡＮ」を参照すること。			
（キ）	拠点ＷＡＮ			
	本省、各地方拠点及びディザスタリカバリサイトで相互に通信を行うため、拠点ＷＡＮ（拠点側におけるネットワーク及び回線）を提供する。閉域網を使用した通信環境を提供する。なお、詳細な要件は、別紙１－２「要件定義書（サービス・機器）」の「第７　７　拠点ＷＡＮ」を参照すること。			
（ク）	外部監視室用回線			
	構築や移行の際、外部に設置した機器と本省に設置した機器間で必要なデータの転送を行うため、外部監視室用回線を提供する。なお、詳細な要件は、別紙１－２「要件定義書（サービス・機器）」の「第７　８　外部監視室用回線」参照すること。			
（３）	「回線」の要件			
ア	インターネット接続回線			
	本業務の実施に当たって、本省、ディザスタリカバリサイトのインターネット接続回線要件を理解した上で、全ての要件を満たすこと。なお、詳細な要件は、別紙１－３「要件定義書（回線）」の「インターネット接続回線」を参照すること。			

別紙１　機能証明書

項番号	内容	提案内容	提案内容 補足資料	記載箇所
イ	WAN回線			
	本業務の実施に当たって、本省、外部拠点、地方支分部局、ディザスタリカバリサイト、外部監視室のWAN回線要件を理解した上で、全ての要件を満たすこと。なお、詳細な要件は、別紙１－３「要件定義書（回線）」の「WAN回線」を参照すること。			
ウ	監視用回線他			
	本業務の実施に当たって、本省、外部監視室の監視用回線要件を理解した上で、全ての要件を満たすこと。なお、詳細な要件は、別紙１－３「要件定義書（回線）」の「監視用回線他」を参照すること。			
（４）	「運用及び維持保守・管理」の要件			
ア	全体概要			
	本業務の実施に当たって、運用設計要件、全体要件の内容を理解した上で、全ての要件を満たすこと。なお、詳細な要件は、別紙１－４「要件定義書（運用及び維持保守・管理）」の「第１　全体概要」を参照すること。			
イ	サービスストラテジ			
	本業務の実施に当たって、事業関係管理の内容を理解した上で、全ての要件を満たすこと。なお、詳細な要件は、別紙１－４「要件定義書（運用及び維持保守・管理）」」の「第２　サービスストラテジ」を参照すること。			
ウ	サービスデザイン			
	本業務の実施に当たって、デザイン・コーディネーション、サービスカタログ管理、サービスレベル管理、キャパシティ管理、ＩＴサービス継続性管理、可用性管理、情報セキュリティ管理、サプライヤ管理の内容を理解した上で、全ての要件を満たすこと。なお、詳細な要件は、別紙１－４「要件定義書（運用及び維持保守・管理）」の「第３　サービスデザイン」を参照すること。			
エ	サービストランジション			
	本業務の実施に当たって、移行の計画立案及びサポート、変更管理、リリース管理及び展開管理、サービス資産管理及び構成管理の内容を理解した上で、全ての要件を満たすこと。なお、詳細な要件は、別紙１－４「要件定義書（運用及び維持保守・管理）」の「第４　サービストランジション」を参照すること。			
オ	サービスオペレーション			
	本業務の実施に当たって、イベント管理、インシデント管理、要求実現、問題管理、アクセス管理の内容を理解した上で、全ての要件を満たすこと。なお、詳細な要件は、別紙１－４「要件定義書（運用及び維持保守・管理）」の「第５　サービスオペレーション」を参照すること。			
カ	継続的サービス改善			
	本業務の実施に当たって、継続的サービス改善の内容を理解した上で、全ての要件を満たすこと。なお、詳細な要件は、別紙１－４「要件定義書（運用及び維持保守・管理）」の「第６　継続的サービス改善」を参照すること。			
キ	サービスデスク			
	本業務の実施に当たって、サービスデスクの内容を理解した上で、全ての要件を満たすこと。なお、詳細な要件は、別紙１－４「要件定義書（運用及び維持保守・管理）」の「第７　サービスデスク」を参照すること。			
ク	ソフトウェア保守要件			
	本業務の実施に当たって、ソフトウェア保守要件の内容を理解した上で、全ての要件を満たすこと。なお、詳細な要件は、別紙１－４「要件定義書（運用及び維持保守・管理）」の「第８　ソフトウェア保守要件」を参照すること。			
ケ	ハードウェア保守要件			
	本業務の実施に当たって、ソフトウェア保守要件の内容を理解した上で、全ての要件を満たすこと。なお、詳細な要件は、別紙１－４「要件定義書（運用及び維持保守・管理）」の「第９　ハードウェア保守要件」を参照すること。			

別紙1　機能証明書

項番号	内容	提案内容	提案内容 補足資料	記載箇所
3	その他満たすべき要件			
	本業務の実施に当たっては、別紙２から別紙５までの内容を理解した上で、全ての要件を満たすこと。			
第５	作業の実施体制・方法に関する事項			
1	作業実施体制			
	プロジェクトの推進体制及び本件請負者に求める作業実施体制を図５－１、表５－１に示す。請負者内のチーム編成については、設計・構築担当、運用及び維持保守・管理担当、セキュリティ担当などを想定しており、特にシステムの信頼性向上や情報セキュリティの確保について、これらのチームが一体となって継続的な改善活動を行う必要がある。 なお、請負者の情報セキュリティ対策の管理体制については、作業実施体制とは別に作成する。			
2	作業要員に求める資格等の要件			
	（１）本プロジェクトの統括責任者は、システム計画の立案、プロジェクト管理、システム設計・構築等の実務経験が通算して10年以上有する者であること。本プロジェクト専任として、支援業務を一貫して実施することができる者であること。ただし、他の兼業しているプロジェクトの業務内容、役割や関与の割合などを客観的に明らかにした上で提案がなされ、総務省の承認が得られた場合はこの限りではない。			
	（２）本プロジェクトの統括責任者は、「情報処理の促進に関する法律」（昭和45年法律第90号）に基づき実施される情報処理技術者試験のうち、プロジェクトマネージャ試験の合格者又は「技術士法」（昭和58年法律第25号）第32条に規定する技術士（情報工学部門）若しくは技術士（総合技術監理部門（情報工学を選択科目とする者））の登録を行っている者であること。ただし、当該資格保有者等と同等の能力を有することが経歴等において明らかな者については、これを認める場合がある（その根拠を明確に示し、総務省の理解を得ること。）。			
	（３）本プロジェクトの統括責任者、担当の作業リーダー又は作業担当者は、情報処理に係る高度な知識を有する者として、以下の資格のうち、アからエまでを有する者を含めること（アからエまでの全てを有する者１名でも可とする。）。 　なお、当該資格を有する者については、資格保有後に継続した５年以上の当該資格に関係する業務経験を持つ者であることとする。 ア プロジェクトマネージャ（独立行政法人情報処理推進機構）、プロジェクトマネジメント・プロフェッショナル（米国ＰＭＩ）、ＩＴストラテジスト（独立行政法人情報処理推進機構）のいずれか イ ネットワークスペシャリスト（独立行政法人情報処理推進機構）又はこれと同等以上の資格であることが証明できる資格 ウ 情報セキュリティスペシャリスト（独立行政法人情報処理推進機構）、ＣＩＳＳＰ（（ＩＳＣ）2～ＩＮＴＥＲＮＡＴＩＯＮＡＬ ＩＮＦＯＲＭＡＴＩＯＮ ＳＹＳＴＥＭＳ ＳＥＣＵＲＩＴＹ ＣＥＲＴＩＦＩＣＡＴＩＯＮ ＣＯＮＳＯＲＴＩＵＭ）又はこれらと同等以上の資格であることが証明できる資格 エ ＩＴサービスマネージャ（独立行政法人情報処理推進機構）、ＩＴＩＬ（ＩＮＦＯＲＭＡＴＩＯＮ ＴＥＣＨＮＯＬＯＧＹ ＩＮＦＲＡＳＴＲＵＣＴＵＲＥ ＬＩＢＲＡＲＹ）ＶＥＲＳＩＯＮ2／3 ＦＯＵＮＤＡＴＩＯＮ以上（ＥＸＩＮ）又はこれらと同等以上の資格であることが証明できる資格			
3	作業場所			
	本業務の作業場所及び作業に当たり必要となる設備、備品及び消耗品等については、請負者の責任において用意すること。また、必要に応じて、担当職員が現地確認を実施することができるものとする。			
4	作業の管理に関する要領			
	（１）請負者は、「設計・構築実施要領」に基づき、設計・構築業務に係るコミュニケーション管理、体制管理、工程管理、品質管理、リスク管理、課題管理、システム構成管理、変更管理、情報セキュリティ対策を行うこと。			
	（２）請負者は、「運用・保守要領」に基づき、運用及び維持・保守管理業務に係るコミュニケーション管理、体制管理、作業管理、リスク管理、課題管理、システム構成管理、変更管理、情報セキュリティ対策を行うこと。			
第６	作業の実施に当たっての遵守事項			
1	機密保持、資料の取扱い			
	本調達に係る業務を実施するために扱う情報は、別紙５「情報保護・管理要領」に従い、十分な管理を行うこと。			

別紙１　機能証明書

項番号	内容	提案内容	提案内容 補足資料	記載箇所
2	法令等の遵守			
	当該調達案件の業務遂行に当たっては、「民法」（明治29年法律第89号）、「刑法」（明治40年法律第45号）、「私的独占の禁止及び公正取引の確保に関する法律」（昭和22年法律第54号）、「著作権法」（昭和45年法律第48号）、「不正アクセス行為の禁止等に関する法律」（平成11年法律第128号）、「行政機関の保有する個人情報の保護に関する法律」（平成15年法律第58号）、「行政手続における特定の個人を識別するための番号の利用等に関する法律」（平成25年法律第27号）等の関連法規を遵守すること。また、総務省が定めた「情報保護・管理要領」（別紙５として添付）及び「総務省情報セキュリティポリシー」（平成27年３月27日総務省行政情報化推進委員会決定）を遵守すること。なお、「総務省情報セキュリティポリシー」は、落札後に請負者に対し必要に応じて主管課から開示する。			
3	その他文書、標準への準拠			
（1）	プロジェクト計画書			
	当該調達案件の業務遂行に当たっては、「プロジェクト計画書」との整合を確保して行うこと。			
（2）	プロジェクト管理要領			
	当該調達案件の業務の管理に当たっては、「プロジェクト管理要領」との整合を確保して行うこと。			
第７	成果物の取扱いに関する事項			
1	知的財産権の帰属			
	（１）本業務における納品物の原著作権及び二次的著作物の著作権（「著作権法」第21条から第28条に定める全ての権利を含む。）は、請負者が本調達の実施の従前から権利を保有していた等の明確な理由によりあらかじめ提案書にて権利譲渡不可能と示されたもの以外は、全て総務省に帰属するものとする。			
	（２）総務省は、納品物について、自由に複製し、改変等し、及びそれらの利用を第三者に許諾することができるとともに任意に開示できるものとする。また、「産業技術力強化法」（平成12年法律第44号）の趣旨に鑑み、総務省による権利の行使に支障が生じない範囲で、請負者も、成果物を利用することができる。			
	（３）本件プログラムに関する権利（「著作権法」第21条から第28条に定める全ての権利を含む。）及び成果物の所有権は、総務省から請負者に対価が完済されたとき請負者から総務省に移転するものとする。			
	（４）納品される成果物に第三者が権利を有する著作物（以下「既存著作物等」という。）が含まれる場合には、請負者は、当該既存著作物等の使用に必要な費用の負担及び使用許諾契約等に関わる一切の手続を行うこと。この場合、本業務の請負者は、当該既存著作物の内容について事前に総務省の承認を得ることとし、総務省は、既存著作物等について当該許諾条件の範囲で使用するものとする。			
	（５）請負者は総務省に対し、一切の著作者人格権を行使しないものとし、また、第三者をして行使させないものとする。			
2	瑕疵担保責任			
	（１）請負者は、本調達について検収を行った日を起算日として１年間、成果物に対する瑕疵担保責任を負うものとする。その期間内において瑕疵があることが判明した場合には、その瑕疵が総務省の指示によって生じた場合を除き（ただし、請負者がその指示が不適当であることを知りながら、又は過失により知らずに告げなかったときはこの限りでない。）、請負者の責任及び負担において速やかに修正等を行い、指定された日時までに再度納品するものとする。なお、修正方法等については事前に総務省の承認を得てから着手するとともに、修正結果等についても総務省の承認を受けること。			
	（２）前項の瑕疵担保期間経過後であっても、成果物等の瑕疵が請負者の故意又は重大な過失に基づく場合は、本調達について検収を行った日を起算日として４年間はその責任を負うものとする。			
	（３）総務省は、前各項の場合において、瑕疵の修正等に代えて、当該瑕疵により通常生ずべき損害に対する賠償の請求を行うことができるものとする。また、瑕疵を修正してもなお生じる損害に対しても同様とする。			
3	検収			
	（１）本業務の請負者は、成果物等について、納品期日までに総務省に内容の説明を実施して検収を受けること。			
	（２）検収の結果、成果物等に不備又は誤り等が見つかった場合には、直ちに必要な修正、改修、交換等を行い、変更点について総務省に説明を行った上で、指定された日時までに再度納品すること。			

別紙１　機能証明書

項番号	内容	提案内容	提案内容 補足資料	記載箇所
第８	入札参加資格に関する事項			
1	入札参加要件			
（1）	競争参加資格			
	ア 競争の導入による「公共サービスの改革に関する法律」（平成18年６月２日法律第51号）第10条各号（第11号を除く。）に該当する者でないこと。			
	イ 「予算決算及び会計令」（昭和22年勅令第165号）第70条の規定に該当しない者であること。なお、未成年者、被保佐人又は被補助人であって、契約締結のために必要な同意を得ている者は、同条中、特別な理由がある場合に該当する。			
	ウ 「予算決算及び会計令」第71条の規定に該当しない者であること。			
	エ 平成25・26・27年度総務省競争参加資格（全省庁統一資格）「役務の提供等」Ａ及びＢの等級に格付けされ関東・甲信越地域の競争参加資格を有する者であること（「役務の提供等」の営業品目④情報処理、⑥ソフトウェア開発」又は⑮その他に登録している者であること。）。			
（2）	公的な資格や認証等の取得			
	請負者は、以下の内容を証明する資料を提出すること。			
	ア 本業務を統括管理する部門は、IS09001認証を取得していること。			
	イ 本業務を統括管理する部門は、IS027001認証を取得していること。			
	ウ 請負者は、一般財団法人日本情報経済社会推進協会のプライバシーマーク制度の認定を受けていること。			
	エ 請負者は、建設業法に基づく電気通信工事業及び電気工事業の許可を受けていること。			
（3）	受注実績			
	請負者は、本総務省ＬＡＮと同等又は類する全国規模のネットワークシステムの設計・構築の実績を有すること。ただし、設計・構築の実績については請負者自身のものであり、再委託等を受けた実績は含まないものとする。			
（4）	複数事業者による共同提案			
	ア 複数の事業者が共同提案する場合、その中から全体の意思決定、運営管理等に責任を持つ共同提案の代表者を定めるとともに、本代表者が本調達に対する入札を行うこと。			
	イ 共同提案を構成する事業者間においては、その結成、運営等について協定を締結し、業務の遂行に当たっては、代表者を中心に、各事業者が協力して行うこと。事業者間の調整事項、トラブル等の発生に際しては、その当事者となる当該事業者間で解決すること。また、解散後の瑕疵担保責任に関しても協定の内容に含めること。			
	ウ 共同提案を構成する全ての事業者は、本入札への単独提案又は他の共同提案への参加を行っていないこと。			
2	入札制限			
（1）	総務省ＬＡＮに関係する他の調達の受注事業者			
	次の事業者（再委託先等を含む。）及びこの事業者の「財務諸表等の用語、様式及び作成方法に関する規則」（昭和38年11月27日大蔵省令第59号）第８条に規定する親会社及び子会社、同一の親会社を持つ会社並びに委託先事業者等の緊密な利害関係を有する事業者は、入札には参加できない。 ア 「次期総務省ＬＡＮに係る調達支援業務の請負」の受注事業者 イ 「次期総務省ＬＡＮに係る工程管理支援業務の請負」の受注事業者			
（2）	ＣＩＯ補佐官及びその支援スタッフの属する事業者			
	調達仕様書の妥当性確認及び入札事業者の審査に関する業務を行うＣＩＯ補佐官及びその支援スタッフ等の属する又は過去２年間に属していた事業者でないこと。または、ＣＩＯ補佐官等がその職を辞職した後に所属する事業者の所属部門（辞職後の期間が２年に満たない場合に限る。）でないこと。			

別紙１　機能証明書

項番号	内容	提案内容	提案内容 補足資料	記載箇所
第９	再委託に関する事項			
１	再委託の制限及び再委託を認める場合の条件			
	（１）本業務の請負者は、業務を一括して又は主たる部分（設計・構築業務、運用業務、保守業務等）を再委託してはならない。			
	（２）請負者における遂行責任者を再委託先事業者の社員や契約社員とすることはできない。			
	（３）請負者は再委託先の行為について一切の責任を負うものとする。			
	（４）再委託を行う場合、再委託先が「第８　２　入札制限」に示す要件を満たすこと。			
	（５）再委託先における情報セキュリティの確保については、請負者の責任とする。			
２	承認手続き			
	（１）本業務の実施の一部を合理的な理由及び必要性により再委託する場合には、あらかじめ再委託の相手方の商号又は名称及び住所並びに再委託を行う業務の範囲、再委託の必要性及び契約金額等について記載した別添の再委託承認申請書を総務省に提出し、あらかじめ承認を受けること。			
	（２）前項による再委託の相手方の変更等を行う必要が生じた場合も、前項と同様に再委託に関する書面を総務省に提出し、承認を受けること。			
	（３）再委託の相手方が更に委託を行うなど複数の段階で再委託が行われる場合（以下「再々委託」という。）には、当該再々委託の相手方の商号又は名称及び住所並びに再々委託を行う業務の範囲を書面で報告すること。			
３	再委託先の契約違反等			
	再委託先において、本調達仕様書に定める事項に関する義務違反又は義務を怠った場合には、請負者が一切の責任を負うとともに、総務省は、当該再委託先への再委託の中止を請求することができる。			
第１０	その他特記事項			
１	前提条件及び制約条件			
	（１）本件は、平成28年度の予算成立を条件とする。平成28年▲月▲日以前に平成28年度予算が成立していない場合には、契約の中止等を行う可能性がある。			
	（２）本件受注後に調達仕様書（別紙１「要件定義書」を含む。）の内容の一部について変更を行おうとする場合、その変更の内容、理由等を明記した書面をもって総務省に申し入れを行うこと。双方の協議において、その変更内容が軽微（委託料、納期に影響を及ぼさない）かつ許容できると判断された場合は、変更の内容、理由等を明記した書面に双方が記名捺印することによって変更を確定する。			
第１１	附属文書			
	１　要件定義書は、以下の全ての文書を指す。 ・別紙１「要件定義書」 　別紙１－１「要件定義書（システム全般）」 　別紙１－２「要件定義書（サービス・機器）」 　別紙１－３「要件定義書（回線）」 　別紙１－４「要件定義書（運用及び維持保守・管理）」			
	２　本調達において、参照すべき内容を含む文書を以下に示す。 ・別紙２「次期総務省ＬＡＮ構成イメージ」 ・別紙３「ソフトウェア一覧」 ・別紙４「機器数量一覧」 ・別紙５「情報保護・管理要領」			
	３　提案書等の審査要領は、別添２「総務省ネットワーク基盤（ＬＡＮ）の構築等の請負総合評価基準書（案）」に示すとおりである。			

別紙１　機能証明書

項番号	内容	提案内容	提案内容 補足資料	記載箇所
	４　本調達に参加する予定の者から要望があった場合、現行総務省ＬＡＮに係る設計書等の納入成果物等について、所定の手続を踏まえた上で閲覧可能とする。閲覧可能な資料一覧を含め、詳細は、「総務省ＬＡＮシステムの更新整備及び運用管理業務民間競争入札実施要項」の別紙６「資料閲覧要領」に従うものとする。また、本調達に参加する予定の者から追加の資料の開示について要望があった場合は、総務省は、法令及び機密性等に問題のない範囲で適切に対応するよう努めるものとする。			

別紙1－1　要件定義書（システム全般）

項番号	内容	提案内容	提案内容 補足資料	記載箇所
第1　規模・性能				
1　共通方針				
	①　規模要件を参考に、賃貸借期間満了時である4年後も利用に耐えうる性能を有すること。			
	②　各サービスにおける処理のピーク時でもレスポンスやスループットの極端な低下を招かないよう、十分な処理性能を確保するための設計を行うこと。			
	③　各サービスの処理内容や量に応じた適切な性能を確保するために、負荷分散等の対策を行うこと。			
	④　本仕様書で記載した機能は、すべて利用可能な状態で納品すること。なお、各機器の設計は主管課と協議の上で行うこと。			
	⑤　システム全体が円滑に動作し、各サービスの性能が十分に活用できること。			
2　規模・性能要件				
(1) ユーザ数				
	①　ユーザ数は約7000（端末数と同数）である。			
(2) アカウント数				
	①　4年間で使用するアカウント数の総数は約16,000となり、内訳や用途は以下のとおり。 ・ユーザアカウント　:約7,000 ・非ユーザアカウント　:約5,000（共有メールアカウント、動作確認用アカウント等） ・一時保管用アカウント　:約4,000			
	②　ユーザアカウント及び非ユーザアカウントは、総務省LANの利用及び運用において、恒常的に必要となるアカウントである。			
	③　一時保管用アカウントは、異動した職員等の情報を一時的に保持するためのアカウントである。			
(3) 機器数				
	①　端末数、プリンタ数などは以下のとおり。 ・LAN端末数　:7,000 台 ・ウィルスチェック用端末数　:140 台 ・タブレット型端末　:220台 ・LANプリンタ数　:300 台 ・直接利用プリンタ数　:250 台 ・LAN複合機　:600 台			
(4) 拠点数				
	①　本省以外の拠点数は以下のとおり。 ・外部拠点　:11 拠点 ・地方支分部局　:62 拠点 ・外部監視室　:1 拠点 ・DRサイト　:1 拠点			
(5) 総務省LANサービス				
ア　メールサービス				
	①　メール送受信数、迷惑メール数、ボックスサイズ、アーカイブ期間は以下のとおり。 ・送受信数　:1,000 万通/月 ・総務省内メール　:750 万通/月 ・政府共通ネットワーク経由　:100 万通/月 ・インターネット経由　:150 万通/月 ・上記以外迷惑メール数　:1000 万通/月 ・メールボックスサイズ　:ユーザアカウント　10GB以上/人 ・メールボックスサイズ　:共有メールアカウント　2GB以上/人 ・メールアーカイブ期間　:12ヶ月以上			

別紙1－1　要件定義書（システム全般）

項番号	内容	提案内容	提案内容 補足資料	記載箇所
イ　ポータルサイトサービス				
①	電子掲示板への書き込みは、平均約200 件/月である。			
ウ　ファイル共有サービス				
①	割り当てフォルダ領域は以下のとおり。 ・個人別割り当てフォルダ領域　：10GB以上/人 ・組織別割り当てフォルダ領域　：26GB以上/人 組織数については以下のとおり。 組織数：761 ※局、部、課、室(それぞれ相当組織を含む)			
エ　大容量ファイル転送サービス				
①	利用登録者数は7000人とする。			
オ　認証サービス				
①	共通基盤支援システムからユーザ情報を受け取った後、2時間以内にサービスのユーザ環境作成を完了すること。			
②	パスワード情報変更は情報を受け取った後10分以内にサービスに反映すること。			
③	大規模な人事異動期には、0時から6時までに最大6000人の職員情報の異動処理を行う性能を有すること。			
④	すべての総務省アカウント数（ユーザアカウント数：約7,000個）に対し生体認証機能を提供できること。			
⑤	新規で利用を開始する大量の利用者に対する登録（ユーザIDやアクセス権などの初期登録）に対応できる、十分な性能を有すること。			
⑥	認証のピーク時間（9:00～10:00）においても、1分未満でユーザ認証を完了できる性能を有すること。			
カ　テレワークサービス				
①	リモートアクセスによるテレワークサービスの登録者数は5,000人であり、同時接続数は1000以上を可能とする。			
②	デスクトップ仮想化によるテレワークサービスのために、シンクライアントデバイスを1,550以上用意すること。また、同時接続数は650以上を可能とすること。			
③	リモートアクセスとデスクトップ仮想化を合わせた同時接続数は1,500以上を可能とする。			
キ　コミュニケーションサービス				
①	登録者数は7,000人である。			
②	同時接続ユーザ数は1,000以上であり、1会議あたりの参加者数は100を可能とする。同時接続ユーザ数の内訳は、以下とすること。 ・HD画質（1280×720 ピクセル） 本省内　670 インターネット回線経由　80 総務省WAN回線経由　110 ・HD画質以下 総務省WAN回線経由　140			
ク　ペーパーレス会議サービス				
①	同時接続ユーザ数は200以上であり、1会議あたりの参加者数は100を可能とする。			
ケ　プリントサービス				
①	業務繁忙等により印刷要求が増加する月でも印刷処理が可能な性能を有すること。 ・印刷枚数　：平均約600万枚/月			
コ　情報漏えい対策サービス				
①	別途調達のシステム室USBメモリ1,300本及び別途調達のウイルスチェック用端末に対応すること。			
②	機密情報保護を行うに当たり、対象ユーザ数は250 名とする。			

別紙1－1　要件定義書（システム全般）

項番号	内容	提案内容	提案内容 補足資料	記載箇所
サ　ディザスタリカバリサービス				
	複製されたデータを1世代以上保管できる領域を有し、発動時に利用できること。 ①・大規模災害時・非常時の運用可能期間が1ヶ月以上であること。 ・主管課の連絡を受けてから、3時間以内に切替えが実施できること。 ・テレワークサービスに関しては、同時接続750以上で提供できること。			
(6) セキュリティサービス				
ア　マルウェア対策（メール）サービス				
	① 一月あたり約1000万通以上の迷惑メールを処理可能な性能を有すること。			
	② 総務省LANのメール送受信数に対してウイルスメールを検知、処理可能な性能を有すること。			
イ　マルウェア対策（インターネット・Web）サービス				
	① Webコンテンツフィルタリングは、Web閲覧同時接続ユーザ数7,000人を踏まえた性能を担保すること。			
	② Web閲覧を行う際のブラウザは、IE11を使用する事を想定し、性能を担保すること。			
ウ　マルウェア対策（サーバ・LAN端末・仮想デスクトップ）サービス				
	① 管理を行うLAN端末数は7000 台となり、加えて導入サーバ（Windows Linuxを含み、アプライアンスを除く）、テレワークサービスの仮想デスクトップ環境も対象とする。			
エ　侵入検知防御サービス				
	インターネット接続回線の帯域を踏まえ、性能を担保すること。 ① ・ファイアウォール性能　：1 Gbps 以上 ・不正侵入検知（IPS）性能　：1 Gbps 以上			
オ　不正接続機器検知サービス				
	以下の機器を管理すること。 ① ・管理端末数　：7000 台 ・管理複合機・プリンタ数　：約1000 台 ・タブレット型端末　：220台 ・総務省LANサービス提供機器			
カ　特権アクセス制御サービス				
	以下の機器へのアクセス制御を実現すること。 ① ・総務省LANサービス提供サーバ ・総務省LANネットワーク機器 ・総務省LANセキュリティ機器			
キ　セキュリティ管理サービス				
	以下の機器へのセキュリティ監査を実現すること。 ① ・管理端末数 7000 ・導入サーバ（Windows Linuxを含み、アプライアンスを除く） ・テレワークサービスの仮想デスクトップ環境			
ク　セキュリティログ分析サービス				
	① 50,000eps以上の処理性能を有すること。			
ケ　仮想ブラウザサービス				
	① 同時利用者数7000 以上を考慮した性能を担保すること。			
(7) 運用管理サービス				
ア　運用支援サービス				
	① 問い合わせ件数につき、1,000件以上 /月の受付を行っている。			
	② 申請対応件数につき、750件以上 /月の対応を行っている。			
イ　システム監視サービス				
	① 導入機器の監視等統合的管理を行う上で十分な性能を有すること。			
ウ　ログ管理サービス				
	① 収集ログ保存期間は12ヶ月以上を可能とする。			
エ　バックアップサービス				
	① システムのバックアップ及びファイル共有サービスのバックアップは、ローカルバックアップ、遠隔地バックアップを合せて12時間以内に完了できること。			

別紙1－1　要件定義書（システム全般）

項番号	内容	提案内容	提案内容 補足資料	記載箇所
オ　電源管理サービス				
①	全拠点で、電源の管理を提供すること。			
カ　資源管理サービス				
①	全拠点の導入機器のハードウェア管理が行える性能を有すること。			
②	全拠点のサーバ・LAN端末のソフトウェア管理が行える性能を有すること。			
③	全拠点のサーバ・LAN端末へソフトウェア配布、セキュリティパッチ等の配布を行える性能を有すること。			
キ　モバイルデバイス管理サービス				
①	管理対象数は以下のとおり。 ・省外利用端末　：20 台 ・省内利用端末　：200 台			
ク　シンクライアント管理サービス				
①	管理対象数は以下のとおり。 ・平常利用シンクライアントデバイス　：1350 台 ・緊急時利用シンクライアントデバイス　：200 台			
(8) その他機器基盤				
ア　検証環境				
①	実運用の環境で動作するサーバの検証が行える環境を準備すること。			
イ　運用業務環境				
①	運用要員人数分及び構築時必要となる台数を準備すること。			
ウ　KVM				
①	提供サーバ台数が接続可能であること。			
エ　UPS				
①	電源容量は、給電停止から5分間経過後、安全にシャットダウンできるために十分な容量であること。			
オ　LAN端末マスタ				
①	既存のLAN端末数のキッティングを行うこと。			
カ　仮想デスクトップマスタ				
①	仮想デスクトップ用のキッティングを行うこと。			
(9) ネットワーク基盤				
ア　本省LAN				
①	本省LANにおける各帯域は以下のとおり。 ・バックボーン回線速度（コアスイッチ間及びコアスイッチ、サーバスイッチ間）　：10 Gbps ・コアネットワーク回線速度　：1 Gbps ・エッジ回線速度　：100 Mbps			
イ　拠点LAN				
①	拠点LANにおける各帯域は以下のとおり。 ・コアネットワーク回線速度　：1 Gbps又は100Mbps（拠点による） ・エッジ回線速度　：100 Mbps			

別紙1－1　要件定義書（システム全般）

項番号	内容	提案内容	提案内容 補足資料	記載箇所
ウ　ネットワークサービス				
	① 全省DNS問い合わせ性能は、50,000 qps以上を有すること。			
	② 全省DHCP性能は、300 lease/sec以上を有すること。			
	③ インターネット接続回線の帯域を踏まえ、以下の性能を担保すること。 Web閲覧同時接続数 ：7,000以上			
エ　無線LANサービス				
	① 提供する範囲は、本省及び外部拠点、各管区行政評価（支）局、各総合通信局（沖縄通信事務所含む）とする。			
	② 各拠点での提供スペースは、会議室、及び打合せスペース等とする。			
	③ 会議室の収容人数は、20名～40名程度とする。			
	④ 接続クライアント数は7200とする。			
第2　信頼性等				
1　信頼性要件				
	① 総務省LANは安定性を最も重視するため、以下の要件を満たすこと。また必要に応じて要件に記載されている以外の信頼性向上施策を提案すること。			
	② 耐障害性や可用性を重視して信頼性の高い構成とすること。			
	③ 十分に実績のある機器を選定すること。			
	④ サーバ、ネットワーク機器共に原則として冗重化して信頼性を高めること。			
	⑤ エッジスイッチ等冗長化できない機器は実績のある機器を選定した上で、MTBF値等を根拠に信頼性を担保すること。			
	⑥ 切り替え、切り戻しのロジックをしっかり担保し、片方の機器に障害が発生しても他の機器で通常通り業務が継続できること。			
	⑦ 各種保存データや設定ファイル等は情報が正確に記録又は保存されること。			
	⑧ 24時間365日の稼働に耐えうる製品を選定すること。			
	⑨ 本調達で導入するサーバ製品等は、装置購入後5年間以上の部品保守が可能であること。			
	⑩ ユーザが直接利用し、障害が直ちにサービス停止に結びつき業務影響を与えるサーバ、アプライアンス機器は冗長化すること。			
	⑪ 停電発生時や非常用電源故障時において、自動的かつ安全にシャットダウンが可能な構成とすること。			
	⑫ 正式なメーカサポートのないオープンソースソフトウェア等の製品を利用する場合は、十分な品質を保証するためのサポート体制や組織を有すること。また、サポート体制や対応方針を明示すること。			
	⑬ メーカ又は同等のオンサイトサポートが対応可能であること。			
2　拡張性要件				
	① ハードウェア、ソフトウェア共にリソース面で契約期間である4年を見越した最適な拡張性を保持すること。			
	② 追加要件が発生しても柔軟に対応できる設計とすること。			
	③ 追加要件が発生した場合でも、各機器のCPUやメモリ、ポート等のスケールアップやスケールアウト型の拡張に対応できること。			
	④ ストレージのディスク増設時は既存ファイルを待避させることなくディスクの増設が行えること。ディスク増設時は、モジュールやブレード等の追加によって拡張可能なこと。			
	⑤ サービスに著しく影響を与えない範囲で拡張が可能であること。			
3　上位互換性要件				
	① OS及び各種ソフトウェアについて、修正プログラムの適用又はバージョンアップにより、大幅な構成変更や利用方法の変更が見込まれる場合は、主管課に通知し、詳細内容や手法を説明した上で承諾を受けること。			
	② サーバ・ネットワーク機器・アプライアンス・LAN端末等のOS・ミドルウェアを含むソフトウェア環境は統一し、常に適切なバージョンを維持すること。バージョンアップは、請負者の責任と負担で対応すること。			
	③ LAN端末のマスタ媒体作成を年に1回行い、地方拠点を含むLAN端末への展開作業を、請負者の責任と負担で対応すること。ただし、更改するLAN端末の地方展開はLAN端末導入事業者が行う。（LAN端末の更改は平成29年4月に約1,900台、平成30年6月に約2,350台、平成31年4月に約2,750台行う予定）			
	④ バージョンアップに技術的な問題等がある場合は主管課と協議し、その指示に従うこと。			
	⑤ バージョンアップ実施後に、設定やプロトコル等を引き継ぐことが可能な製品であること。引き継ぎが困難な場合は主管課と協議し、適切な対応を実施すること。			

別紙1－1　要件定義書（システム全般）

項番号	内容	提案内容	提案内容 補足資料	記載箇所
	⑥ マネージャやエージェントによって構成される製品で、機器の追加等の発生によりバージョンの差異が発生した際でも、導入時の設計を引き継いだ形で運用が可能なこと。			
	⑦ 請負者は、現行利用中の「Microsoft Windows 7」の後継OSに関して、導入時期、導入バージョンを主管課と協議の上決定し、バージョンアップを行うこと。なお、バージョンアップ作業には総務省LANサービスの動作検証、LAN端末導入ソフトウェアの動作検証、マスタ媒体の作成、展開作業と展開作業に付随する作業等を含む。			
4　システム中立性要件				
	① 特定の事業者・製品に依存することなく、引き継ぐことが可能なシステム構成であること。			
	② ハードウェア及びソフトウェア等には、オープンな規格（原則として、①開かれた参画プロセスの下で合意され、具体的仕様が実装可能なレベルで公開されていること、②誰もが採用可能であること、③技術標準が実現された製品が市場に複数あることのすべてを満たしている技術標準をいう。）に基づいた技術や製品を導入しシステム中立性を確保すること。			
	③ 今後の調達における導入機器との相互接続性を確保するため、原則として国際規格や日本工業規格等のオープンな規格に準拠した製品が選定されていること。			
5　事業継続性要件				
	① 大規模災害時・非常時に災害を受けていない各拠点から、ユーザがディザスタリカバリサービスを利用し、総務省LANの主要サービスを利用可能であること。			
	② 大規模災害時・非常時にユーザの業務が停滞しないよう、主要なサービスのデータがディザスタリカバリサービスとしてバックアップされており業務継続を可能とすること。			
	③ 大規模災害時・非常時にディザスタリカバリサイトの運用へ切り替わった場合、1ヶ月程度の運用を可能とすることとし、具体的な運用内容に付いては、主管課と別途協議して策定すること。			
	④ 現行総務省LANでは「総務省LANにおける情報システム運用継続計画」を策定している。請負者は、次期総務省LANに適合する形で本計画を同等内容で再作成すること。また本計画は年に一回以上、見直しや修正を行い主管課の承認を得ること。			
第3　情報セキュリティ				
1　情報セキュリティ対策				
(1) 共通方針				
	① 情報セキュリティ対策の共通方針として、以下の方針に従い総務省LAN全体の情報セキュリティ対策を具体的に明示すること。対策は「総務省情報セキュリティポリシー」等に準拠して行うこと。			
	② セキュリティ対策は、政府の情報セキュリティ対策方針（「政府機関の情報セキュリティ対策のための統一基準（平成26年度版）」）に示されるセキュリティ対策事項を実現する上で必要となる対策を、網羅的に実施すること			
	③ 調達時点で、実現可能な対策であること。			
	④ セキュリティ対策製品は、定義ファイルやバージョンアップ等の継続的な更新を行うための仕組みを構築すること。			
	⑤ 総務省LAN稼働時点の機能に加え、稼働期間中に継続的なセキュリティレベル向上のための仕組みを構築すること。			
	⑥ セキュリティパッチ等は、最新かつ日本語環境下で実証済みの上、遅延なく適用可能であること。			
	⑦ 内閣サイバーセキュリティセンター、総務省等が別途実施する第三者機関等によるセキュリティ監査への対応を実施し、監査の結果改善の必要性が指摘された場合には、速やかに総務省と対応を協議すること。			
	⑧ 管理者権限を持つアカウントを利用する場合には、管理者としての業務遂行時に限定して利用すること。また管理者権限で実行できる範囲を、該当する管理作業に必要な最小の範囲に制限すること。			
	⑨ ユーザに付与したアカウントを、その後別のユーザに付与しないこと。ただし、共有メールアカウントは除く。			
	⑩ ネットワークは各種サービスと運用管理のセグメントを分離して、適切なアクセス制御を行うこと。			
	⑪ 証跡ログを1年以上保管し、必要に応じてログの調査が可能であること。			
	⑫ 主管課の指示に基づいて、内閣サイバーセキュリティセンターから提供されるセキュリティ対策に関する情報の調査や対応を行うこと。			
	⑬ セキュリティ関係の設計・運用は主管課及び関係部署と調整すること。			
	⑭ セキュリティインシデントの状況を正確に把握できるよう、適切に分類し報告を行うこと。			
	⑮ 情報漏えいが発生した場合、流出経路の特定等の調査を行い、対策を講じられるようにすること。			
	⑯ 不要な通信は抑制すること。			

別紙1－1　要件定義書（システム全般）

項番号	内容	提案内容	提案内容 補足資料	記載箇所
	⑰ 証跡ログは標準的な形式（テキストファイル等）で出力でき、次々期総務省LANに引き継げること。			
	⑱ 内閣サイバーセキュリティセンターが設置するGSOCセンサーの対応を踏まえること。			
(2) リスクと対策				
	① 各サービスのセキュリティリスクとそれに対する対応策を明示すること。			
(3) 脆弱性対策				
	① 総務省LANの稼働で利用しないプロセス、サービス等は原則停止すること。			
	② メーカから脆弱性に関する情報が公開された場合、当該脆弱性がもたらすリスクを確認した上で主管課へ報告すること。			
	③ 脆弱性対策を行う場合は、メーカより入手したセキュリティパッチやファーム等のリリース情報を基に十分に検証した上で本番環境へ適用すること。			
	④ セキュリティパッチ、ファームの適用状況を管理すること。			
(4) 暗号技術				
	① 「電子政府における調達のために参照すべき暗号のリスト（CRYPTREC暗号リスト）」（平成25年3月1日 総務省 経済産業省）等を参照し、最適な方式を選定して提案すること。			
	② 暗号アルゴリズムやハッシュアルゴリズムへの危殆化への対応を行うこと。			
	③ インターネット経由のリモートアクセス、WAN及び無線LANの通信路は暗号化すること。			
(5) 総務省LAN情報セキュリティチーム				
	① 総務省LAN情報セキュリティチームは、運用員とは独立した複数名の要員で構成すること。具体的には、セキュリティに精通した要員（以下、上級セキュリティエンジニアという）、上級セキュリティエンジニアの指示に従い、ログ分析を実施する要員（以下、「ログ分析要員」という。）及びそれらの要員の統括者において構成すること。			
	② 総務省LAN情報セキュリティチームは、必ずしも常駐は必要としないが、日次でセキュリティに関するログの分析監視を行うこと。			
	③ 上級セキュリティエンジニアは、以下の要件を満たすものとする。 ・上級セキュリティエンジニアは、「本調達の遂行等に係る情報セキュリティ対策」の項に記載の「重大インシデント」に対応可能なように複数名の体制を想定する。 ・上級セキュリティエンジニアの中心的役割を担う者は、総務省LANと同等規模の組織（利用者数5000名程度以上）の基幹LANシステムにおける未知のウイルス感染事案への緊急対応経験を有すること。また、情報漏えい事案の緊急対応経験を有すること。ただし、緊急対応経験は、平成23年以降の経験であること。なお、当該者が、原則、重大インシデント対応の際の応答や助言等を行うこと。 ・上級セキュリティエンジニアの中心的役割を担う者は、政府機関において、別紙1-2_要件定義書（サービス・機器）の「第4　セキュリティサービス」「8 セキュリティログ分析サービス」に示すものと同等なログ解析機器（以下、「SIEM（Security Information and Event Management）システム」という。）を用いたログの分析監視経験を1年以上有すること。なお、当該者が、原則、月次の報告会に出席し、セキュリティに関するログの分析監視状況について説明を行うこと。 ・上級セキュリティエンジニアは、以下のいずれかの資格を有するか、または、セキュリティコンサルティング業務の経験を5 年以上有していること。 SANS GIAC Certified Forensics Analyst SANS GIAC Certified Incident Handler 情報システムセキュリティ専門家（CISSP） 情報セキュリティマネージャ（CISM） 情報セキュリティ監査人（CAIS） 情報システム監査人（CISA）			
	④ 上級セキュリティエンジニアは、政府の情報セキュリティ方針や施策、総務省の情報セキュリティポリシー等を理解し、総務省LANの情報セキュリティ対策との適合性を把握すること。具体的には、本調達のシステム導入時にセキュリティ関連のサービス等につき、セキュリティ対策との適合状況のレビューを実施すること。運用期間において、情報セキュリティ対策が変更となる場合、あるいは、システム変更が加わる場合に、レビューを実施することにより適合性を把握するものとする。			
	⑤ 上級セキュリティエンジニアは、1年につき1回、総務省LANのリスク分析を実施し、総務省LANにおけるセキュリティ課題の提示と対策の検討及び対策案の提示を行うこと。リスク分析は、本調達の設計・構築時に実施した上で、分析結果を設計・構築内容に反映するとともに、運用開始時おいても残留リスクを提示すること。			
	⑥ 上級セキュリティエンジニアは、総務省LANの構成や状態を詳細に把握し、主管課や総務省情報セキュリティ班(情報システム第1係、最高情報セキュリティアドバイザ等)、他関係各所との協議や調整において、具体的な情報の提示や施策の可否等を迅速に判断できること。			

別紙1－1　要件定義書（システム全般）

項番号	内容	提案内容	提案内容 補足資料	記載箇所
⑦	上級セキュリティエンジニアは、本調達で導入する各種セキュリティ機能の活用を念頭に、ログ分析のためのルール定義、検索のロジック、相関分析手法等セキュリティのログ分析の考え方を明示すること。また、ログ分析の手法を本調達で導入するSIEMシステムへ実装する方法を提示すること。			
⑧	上級セキュリティエンジニアは、運用期間中は、特に政府機関のセキュリティに関する最新情報を日常的に入手し、新たなリスクに対しては、対応する分析手法およびSIEMシステムへの実装方法について、検討・提示及び実装支援を実施すること。			
⑨	上級セキュリティエンジニアは、内閣サイバーセキュリティセンター（NISC）等、関係機関からの調査依頼や対応要請への支援を行うこと。また、必要に応じて、セキュリティ機器やSIEMシステムへの当該情報の投入を運用員に依頼すること。			
⑩	ログ分析要員は、以下の要件を満たす複数名で構成するものとする。 ・別紙1-2「要件定義書（サービス・機器）」における「第3　総務省LANサービス」の「5　認証サービス」や「第4　セキュリティサービス」の「4　侵入検知防御サービス」、「第7　ネットワーク基盤」の「3　ネットワークサービス」等のサービス内容及び各サービスが出力するログについて、理解する能力を有すること。 ・上記ログから、マルウェアの活動の疑いのあるイベントを抽出するため、SIEMシステムを用いて、各ログを月次・週次で分析可能な能力を有すること。			
⑪	ログ分析要員は、ログ分析の結果、不審な通信や不審操作の疑いのあるイベントを発見した場合、速やかに上級セキュリティエンジニアに報告すること。			
⑫	総務省LAN情報セキュリティチームの統括者は、以下の要件を満たすものとする。 ・総務省LANにおけるセキュリティの課題管理、主管課とのコミュニケーションを含むチームの管理業務を実施できること。 ・上記管理のために必要な一定程度のセキュリティスキルを有すること。 ・本調達で導入する総務省LANのシステム構成やセキュリティ対策状況、また、その変化について、常時詳細に把握しておくこと。 なお、統括者は、上級セキュリティエンジニアが上記要件を充足できる場合には、兼任を可とする。			
⑬	総務省LAN情報セキュリティチームは、運用員と連携できるよう、日常的にコミュニケーションをとりつつ運用の状況を把握しておくこと。			
⑭	総務省LAN情報セキュリティチームは、運用員と連携し、日常的に、リソースやトラフィックの状況把握、複数ログの相関分析、レピュテーション情報との照合等を実施し、異常検知を行うこと。			
⑮	上級セキュリティエンジニアは、ログ分析要員からの報告を含むセキュリティのログ分析の中で、不審な通信ログや不審な操作ログ等をもとに、マルウェア感染の疑いがあるファイル（検体）について、ファイル名及び格納場所の特定を行うこと。また、当該検体について、本要件定義書の「2. 本調達の遂行等に係る情報セキュリティ対策」に従い、解析を実施すること。			
⑯	上級セキュリティエンジニアは、情報セキュリティインシデント発生時には情報の収集、分析、問題の特定、解析、対策案の検討、協議、（運用員に対する）被害拡大防止策の指示、その他対応の指示、対応の状況確認、報告等を行うこと。			
⑰	また、インシデントの収束に向け、必要に応じて情報セキュリティインシデント対応の専門技術者の起用を可能にする等、あらかじめ十分な体制を組んでおくこと。			
⑱	上級セキュリティエンジニアは、情報セキュリティインシデント発生確認後には、主管課と協議し、必要に応じて各種証跡を分析し、発生源や影響範囲等の調査、外部への影響や潜在的な危険性等を1時間以内に報告すること。			
⑲	上級セキュリティエンジニアは、月次で主管課および総務省情報セキュリティ班への報告会を実施し、セキュリティログ相関分析、本調達で導入する各セキュリティサービスの状況分析、分析の中で不審と疑われるイベントの調査、に関する報告、ウイルス対策ソフトの検知アラート対応等の情報セキュリティインシデント対応状況の報告、総務省ＬＡＮにおけるセキュリティ課題の提示及び解決案の提示、一般的なセキュリティ情報の提供を行うこと。			
⑳	上級セキュリティエンジニアは、世界規模でセキュリティに係る情報を収集し、解析する能力があるセキュリティ専門のメーカー等に所属しており、それらの情報を活用できる能力を持っていること。			
㉑	上級セキュリティエンジニアは、総務省情報セキュリティ班(情報システム第1係、最高情報セキュリティアドバイザ等）と面談を実施し、その能力や実績を証明すること。			

別紙1－1　要件定義書（システム全般）

項番号	内容	提案内容	提案内容 補足資料	記載箇所
2　本調達の遂行等に係る情報セキュリティ対策				
(1) 情報セキュリティ侵害が発生した場合の対処				
	① 情報セキュリティに関する事故又は障害が発生した場合に備え、連絡体制・対応手順等を明示して主管課に承認を得ること。			
	② 情報セキュリティ侵害が発生した場合又はその恐れがある場合には、速やかに主管課に報告すること。 本内容に該当する事象として以下も含めて考慮すること。 ・請負者に提供する総務省の情報の外部漏えい及び目的外利用 ・請負者による総務省のその他の情報へのアクセス			
(2) セキュリティインシデントへの対応				
	① 情報セキュリティインシデントに関する問い合わせについて、24時間365日受付可能とすること。問い合わせには、LAN端末やタブレット、USBシンクライアントの紛失等を含むものとする。			
	② 情報セキュリティインシデントの中でも、大規模なウイルス感染や情報漏洩等、緊急で対応が必要となるインシデント（以下、「重大インシデント」という。）発生時は、主管課の指示に基づき、24時間365日対応可能なように十分な体制を組んでおくこと。			
	③ 重大インシデント以外の情報セキュリティインシデントについては、別途定める運用業務の提供時間内において、対応すること。ただし、業務時間内に確認されたインシデントに関しては、重大インシデントの判断がつくまで対応すること。			
	④ 重大インシデントは、請負期間中、年1回までは想定内として対応すること。			
	⑤ 重大インシデントの具体的な定義については、別途主管課と協議の上決定すること。			
	⑥ 想定回数を超える重大インシデントが発生した際の対応については、主管課と協議し、別途契約の上、実施すること。			
	⑦ マルウェア感染の疑いがあるファイル（検体）の解析及び応急的なパターンファイル提供は、原則として検体提供後から2時間以内に行われること。			
	⑧ また、原則として、専門に設けたサポート担当者が当省との対応窓口となること。			
	⑨ 検体の解析については、1年につき、300回を想定する。想定回数を超える場合は、主管課と協議し、別途契約の上、実施すること。			
	⑩ 重大インシデント対応時は、定期的及び必要に応じて主管課と情報交換や問題解決の打ち合わせを実施すること。			
	⑪ また、対応の迅速性を優先し、総務省外部での調査が効率的である場合は、あらかじめ主管課と合意したセキュリティ措置を施した上でディスクイメージやログを総務省外部に持ち出し、調査を実施すること。			
(3) セキュリティ監査				
	① 総務省LANの稼働前に全サービスのセキュリティ診断を実施し、OSやミドルウェアの導入や設定に伴う脆弱性が無いことを確認すること。インターネット接続が発生する環境は特に重点的な監査を行うこと。			
	② セキュリティ診断により検出された脆弱性の説明、対処方法、証跡等がまとめられた診断結果レポートを提供すること。			
	③ セキュリティ診断の結果、修正を要する場合は必要な対応処置を行うこと。			
(4) 機密保持				
	① 総務省から請負者に提供するすべての情報及び資料等は、本契約期間中の如何を問わず、第三者に開示、漏えい又は他の目的に使用しないこと。ただし、第三者に開示の必要性がある場合は、開示方針や漏えいの防止策を明示し主管課に承認を得ること。			
	② 総務省LANへのデータ持ち込み、持ち出し等機密保持に係る対応は、別紙5「情報保護管理要領」に準拠すること。			
(5) 入退室管理				
	① 請負者が作業する場所では、入退室記録を取得し不正な入退室が無いよう管理すること。			
	② 請負者の作業場所では、主管課の許可なく請負者以外の入退室ができないよう施錠管理を行うこと。			
	③ 要員に変更がある場合は、当該変更内容を体制表に反映させ主管課に承認を得ること。			
(6) セキュリティ教育				
	① 請負者は、本調達業務に関わる者すべてに対して情報の漏えい、消去、不正アクセス、不正利用等の防止を目的としセキュリティ教育を実施すること。また、その結果を証跡として取得すること。			

別紙1－1　要件定義書（システム全般）

項番号	内容	提案内容	提案内容 補足資料	記載箇所
(7) データ管理				
①	本調達で利用及び作成するデータ等は、一元的に管理を行うこと。また、作業従事者の権限に応じたアクセス権を設定しデータの漏えい等が無いよう対応すること。			
(8) 端末管理				
①	請負者の作業端末は定期的にセキュリティチェックを行い、セキュリティ上の問題が無いことを確認すること。			
(9) その他				
①	上記以外でセキュリティ品質を向上させる対応策がある場合は提案すること。			
第4　構築・試験				
1　試験要件				
①	作業を実施するにあたっては、以下の内容を含む「試験実施計画書」を速やかに作成し、主管課の承認を得ること。また、各作業項目単位の試験終了後は、各試験の証跡及び「試験結果報告書」を提出し主管課の承認を得ること。記載事項は次のとおり。 ・試験目的・方針 ・試験体制と役割 ・試験スケジュール ・詳細な試験作業内容 ・制限・条件 ・合否判定基準 ・試験環境、試験シナリオ ・試験方法（単体試験、結合試験、総合試験、受入試験支援） ・試験ツール ・インターネット接続前検査 ・試験結果の証跡			
②	インターネットに接続する部分は接続実施前に第三者による脆弱性評価又は脆弱性確認ソフトウェアによる脆弱性評価を行い、問題がないことを確認すること。主管課にその確認結果を提示し、承認を受けた上で接続すること。			
③	構築作業場所から移設した際は、移設後の動作確認として必ず総合試験を実施すること。試験内容は内容とレベルを精査し、主管課と協議の上、決定すること。			
④	試験実施時は、1つの試験を2名体制で行う等、品質を確保した環境を整備して実施すること。また、試験結果は責任者が責任を持って内容の確認を行うこと。特に現行運用環境と連携が必要になる場合は、稼働中のサービスに影響を与えることのないよう、試験実施規定を必ず定め、主管課の承認を得ることとし、万全の作業体制のもと試験を実施すること。			
⑤	定常時の試験だけではなく、異常時、障害発生時の切り替り動作及び障害発生からの切り戻り動作等の試験を必ず実施し、正常性を確保すること。切り替え・切り戻し試験は移行時にしか行えないため、総合試験時に必ず行うこと。			
2　試験種類				
①	請負者は以下の各試験の「試験実施計画書」を提出し、主管課の承認を得ること。また、試験終了後は各試験の「試験結果報告書」を提出し、主管課の承認を得ること。			
(1) 単体試験				
①	単体試験は各機能を試験の単位とし、全項目の試験を実施すること。なお、試験内容が担保できるのであれば、試験単位の変更は可能とする。			
(2) 結合試験				
①	結合試験は、連携して機能するシステムの試験である。当該試験は、本省と外部拠点及び地方支分部局等間、本省とディザスタリカバリサイト、外部監視室間の疎通に係る試験も含まれる。結合試験は、移行前に実施すること。			
(3) 総合試験				
①	総合試験は、運用業務の遂行を想定した総合的な機能試験及び非機能試験（性能の確認、障害対応、バックアップ／リストア等）を行うものとする。また、当該試験では、インターネット回線、政府共通ネットワーク、WAN回線の疎通、停電停止処理に係る試験も含まれる。運用に必要なジョブやスクリプト、ツール等がある場合は、それらも試験に含むこと。			
②	本運用系とディザスタリカバリサービス系の切り替え、切り戻しの確認を行い、ディザスタリカバリサービスで提供するサービスが実際に利用可能であることを検証すること。また、検証に際しては切り替え、切り戻しに要した時間を記録しておくこと。			

別紙1－1　要件定義書（システム全般）

項番号	内容	提案内容	提案内容 補足資料	記載箇所
3　試験場所				
①	試験を実施するにあたっては、原則として請負者が試験を実施する場所を用意すること。			
第5　受入試験支援				
1　受入試験支援				
(1) 受入試験支援				
①	受入試験は、現行総務省LANから次期総務省LANへの移行可否を最終的に判断するものである。そのため、移行可否を最終的に判断するための具体的な受入試験内容を提案し、主管課が「受入試験実施計画書」を作成する支援を実施すること。			
②	受入試験を実施するに当たり、請負者は主管課の受入試験実施の支援を行うこと。なお、以下に受入試験で、請負者が対応すべき内容を示す。 ・可能な限り本番環境に近い試験環境の提供を行うこと。 ・可能な限り本番データに近い試験データの提供を行うこと。 ・十分な試験時間を確保すること。 ・ユーザの積極的な参画のための企画及び支援を行うこと。			
(2) 受入試験を踏まえた改修				
①	受入試験の結果サービス要件を満たしていない点や不具合が発生した場合、改修のための計画を策定し速やかに取り組むこと。			
第6　情報システムの移行				
1　移行に係る要件				
(1) 移行の基本方針				
①	次期総務省LANへの移行作業はユーザの業務に影響がないよう、現行総務省LANで稼働中のサービスについては無停止での作業を行うこと。ただし、主管課が承認したシステムや日時は除く。			
②	ネットワーク及びシステムの停止を伴う作業が避けられない場合は、ユーザへの影響を最小限に抑えるため、基本的に平日勤務時間外の他、土日及び休日の作業とし、事前時に主管課の承認を得ること。また、各執務室内への機器の搬入及び設置・調整も、ユーザの業務に支障を与えないよう同様の対応とすること。			
③	次期総務省LANへの移行に当たり、現行総務省LANで保存されているデータの移行を行うこと。			
④	現行総務省LANで保存されているログデータを移行し、次期総務省LANで検索・閲覧できるようにすること。			
⑤	請負者がユーザに移行・導入のための作業を依頼する場合は、当該ユーザ以外では実施不可能と判断した必要最低限の作業にとどめること。			
⑥	請負者がユーザに移行・導入のための作業を依頼する場合は、ユーザの負担をできる限り軽減できる方策を検討の上で、「ユーザ移行手順書」やツールを必要部数作成し、作業方法の説明を行うこと。			
⑦	現行総務省LAN上で稼働している各業務システムの移行は、移行に伴いユーザに影響を与えることのないよう、各業務システム接続セグメントの設計及び接続試験期間を留意すること。			
⑧	政府共通ネットワーク、政府共通プラットフォームとの連携を考慮すること。			
⑨	主管課より指示があった場合は、現行総務省LANで使用している機器類を取り外し、指定した場所へ移動すること。			
⑩	移行・導入を行う当日に、障害発生等により作業が中断した場合、迅速にその原因を明らかにし、作業を再開できるようにすること。			
⑪	移行・導入の実施前に請負者は、現行総務省LANのデータのバックアップを必ず取得すること。			
⑫	移行・導入のために必要な追加機器は、移行期間中は請負者が提供し、作業終了後に撤去すること。			
⑬	業務の引継ぎ及びシステム切り替え作業に関わる協力依頼等、請負者が現行受注事業者（現行ネットワーク回線事業者などを含む）と調整が必要になる場合、原則業者間で調整業務を行い主管課に報告を行うこと。			
⑭	現行受注事業者との引き継ぎ内容を遅滞なく正確に実施できるよう、請負者は現行運用事業者から提供される「引き継ぎ資料」を基に引き継ぎを行い、その結果を報告すること。			
⑮	本省サーバ室に設置してある現行総務省LAN機器の撤去が終了次第、外部監視室に設置した機器を本省サーバ室へ移設する。当該作業にあたっては、「移行実施計画書」を作成するとともに、当該計画に基づき移設作業を実施すること。			
⑯	移行で利用できる本省サーバ室のスペースが極少であり、移行期間に全ての機器の併設ができない。そのため、省スペースを考慮した移行を行うこととし、機器を併設する期間もできる限り短くすること。			
⑰	本省サーバ室にすべての機器が移設できるまで、外部監視室を用意しサービスを提供することとし、当該運用で発生する経費は請負者で負担するものとする。			

別紙1－1　要件定義書（システム全般）

項番号	内容	提案内容	提案内容 補足資料	記載箇所
⑱	本省サーバ室に設置済みの19インチラック等のうち、設置条件によって再利用ができない物に関しては、請負者の負担で撤去し、新しく設置を行うこと。			
(2) 移行作業の進め方				
ア 移行計画の策定				
①	移行開始までに「移行実施計画書」を策定し、主管課と協議の上、承認を得ること。移行計画では、現行総務省LAN及び業務の継続に影響がないよう考慮すること。			
イ 移行設計				
①	移行に係る設計として、システム移行及びデータ移行の設計を行うこと。システム移行設計には、ハードウェア、ミドルウェア、ネットワーク、プログラム資源、及び環境設定等を含むこと。			
ウ 移行手順の作成				
①	システム移行、機器の設置、導入・移行及び検証に係る「移行手順書」を作成し、主管課の承認を得ること。「移行手順書」には、作業体制、連絡先一覧とバックアップ等準備作業、移行・導入作業、及び事後作業等の作業項目、操作対象、操作方法、想定時間等を明確したタイムチャートを含むこと。			
②	トラブル発生時の切戻し（フォールバック）手順を作成すること。			
エ リスクの識別・コンティンジェンシープランの作成				
①	リスクを組織的にマネジメントし、リスクの発生源・発生原因、損失等回避、転嫁、又はそれらの低減等を計画すること。			
②	移行作業に係るリスクを明らかにした上で、コンティンジェンシープランを作成、「移行実施計画書」に記述し、主管課と協議の上、承認を得ること。			
オ 移行判定基準の作成				
①	移行・導入作業の実行是非の判断基準として、移行判定基準を作成し、移行判定時の予定値を定めること。この移行判断基準は可能な限り定量的なものとし、「移行設計書」に記述し主管課と協議の上承認を得ること。			
カ 移行手順の検証				
①	移行手順書、タイムチャート、作業体制図、連絡先一覧、及び資源管理一覧が適切であることを検証すること。検証結果に基づき、必要に応じて移行手順書を修正すること。			
キ 移行リハーサルの実施				
①	「移行実施計画書」に基づき、主管課、現行受注事業者等の関係者と調整の上、可能な限り、本番移行作業を模した条件下で、個別サービス単位の移行リハーサルを実施すること。リハーサルの実施結果は、移行リハーサル実施報告書にまとめ主管課に報告すること。			
ク 移行判定				
①	移行判定基準の各確認項目の実績値を報告し、主管課から移行・導入作業実施の承認を得ること。			
ケ 移行・導入作業の実施				
①	請負者は、「移行実施計画書」、「移行設計書」及び「移設手順書」等を作成し、主管課の承認を得た上で、現行総務省LANから次期総務省LANへの移行・切り替えを実施すること。移行・切り替えにあたっては、ユーザ及び業務システムに与える影響を十分に考慮し、特に業務システムの停止は主管課と協議の上最小限にとどめるよう、調整すること。			
②	次期総務省LANへの移行は各拠点の機器・回線、本省の各フロア、回線、各種サーバシステムの切り替えが必要である。切り替え方法や切り替えスケジュールは、ユーザの業務影響がなく、期間内に終了するよう検討すること。			
③	移行作業時には複数個所の同時期の移行に対応するため、ファシリティ担当を分けること。			
④	移行作業時は、端末展開作業全般を管理する作業管理者を置くこと。			
⑤	移行時の現行総務省LANと次期総務省LANが並行稼動する期間は、移行用ヘルプデスクを用意すること。			

別紙1－1　要件定義書（システム全般）

項番号	内容	提案内容	提案内容 補足資料	記載箇所
	⑥ 移行対象データは以下を対象に含むこと。 ・メールデータ ・メールマガジン登録ユーザデータ ・メーリングリストデータ ・ポータルサイトコンテンツデータ ・グループウェアデータ ・ディレクトリデータベース ・移動ユーザプロファイルデータ ・ユーザ情報管理データ ・申請管理データ ・DNSゾーン設定 ・ファイル共有サーバデータ及びアクセス権 （自動暗号化フォルダー及び、配下ファイルを含む） ・LAN端末上のユーザデータ、メールデータ、ローカルアドレス帳 ・メールアーカイブデータ　：1年間分 ・現行総務省LANで保存されている各種ログデータ			
	⑦ 展開の基本方針として、搬入・据付・設置などの次期総務省LANの機器展開作業は、ユーザの業務に影響がないよう、主管課とスケジュールを調整し対応すること。			
	⑧ 次期総務省LANの機器展開作業の「展開実施計画書」を策定し、主管課と協議の上、承認を得ること。			
	⑨ 本省及び各拠点において展開作業に係る事前調査を行い「展開事前調査報告書」を作成し、主管課の承認を得ること。「展開事前調査報告書」は、原則、現地調査実施のもと作成すること。なお、事前調査の際の調査項目は予め提出すること。			
	⑩ 事前調査を行うに当たり、流用する配線・ラック等の設備状況の確認は必ず行い、導入後障害等が発生した際対応できるよう、内容の把握を責任を持って行うこと。			
	⑪ 機器設置、LAN端末展開作業を対象とした「展開手順書」を作成すること。展開作業の手順には、各作業が正しく行われていることの確認を含めること。			
	⑫ 事前調査結果を基に、機器設置場所への電源、LANケーブル、回線の敷設等の工事作業を実施し、適切な環境整備を行うこと。			
	⑬ フロアレイアウト、ラック搭載図、LAN敷設、電源敷設等の工事に係る情報を取りまとめ、「工事前調査報告書」を作成し報告すること。			
	⑭ 請負者は利用した総務省の施設・設備を含むすべてのファシリティの状態を把握した上で作業を行うこと。			
	⑮ 敷設した各種ケーブルには敷設元及び敷設先が判断可能となるラベルを貼付すること。			
	⑯ 必要に応じ展開する機器の転倒防止対策を行うこと。			
	⑰ 展開計画で策定したスケジュールを基に、本省及び拠点で機器設定の追加・変更作業を行うこと。			
	⑱ 搬入、搬出に際して発生する各種申請手続きは請負者が行うこと。養生が必要な場合、実施すること。			
	⑲ 梱包資材は請負者が撤去を行うこと。			
	⑳ 進捗管理を行い、主管課の要求に応じた適切な報告が可能な体制をとること。			
	㉑ 移行作業を実施した翌開庁日は現地立会いや本省でのモニタリング等、システムの稼働状況を把握するとともに、ユーザからの問い合わせ及びトラブル対応を迅速に実施できる体制を確保すること。			
	㉒ 次期総務省 LAN 上では現行総務省LAN の複数機種のLAN 端末が稼働するよう、LAN 端末のシステムの再作成（マスタ媒体の作成、既存LAN 端末へのインストール、環境設定、動作確認等）及び管理サーバ等への登録確認を行うこと。			
	㉓ LAN 端末の機種は複数存在しているため、機種ごと及び利用用途別のマスタ作成を行うこと。マスタ媒体作成後、マスタとして問題が無いか主管課の試験を経て承認を得ること。また、主管課の試験を支援すること。			
	㉔ 別途調達する LAN 端末が、次期総務省LAN 環境下で稼働するために必要となるマスタ媒体を作成すること。別途調達する LAN 端末は、LAN 端末納入事業者が設置及び動作確認等の作業を行うため、連携して作業を行うこと。			
	㉕ LAN 端末のマスタ作成に当たり、別途調達済みの複合機、プリンターの利用を考慮すること。なお、展開作業において印刷確認を実施すること。			

別紙1－1　要件定義書（システム全般）

項番号	内容	提案内容	提案内容 補足資料	記載箇所
	㉖ 現行総務省 LAN端末 のユーザデータの退避・復元が可能となるよう移行用の環境及び手順書を提供すること。			
	㉗ システム再構成を行った LAN 端末とシステム再構成を行っていないLAN 端末が並行して稼働する期間でも総務省LANのサービスが利用できるよう配慮すること。			
コ 特別運用体制の維持				
	① 移行・導入作業実施後は、トラブル報告・問い合わせが多く発生することが想定されるため、通常時より多くの要員、対応時間を確保すること。発生したトラブル報告、問い合わせ等は課題管理として管理すること。また、トラブル数等を定量的に確認できる報告を行うこと。			
	② 移行時の現行総務省LANと次期総務省LANが並行稼動する期間は、移行用ヘルプデスクを用意し、現行受注事業者と連携をとりトラブルや問い合わせに対応する体制を保持すること。ヘルプデスクは運営場所を確保し、インターネットや電話等の通信環境を用意すること。ヘルプデスク要員は次期総務省LANの教育を受けた人員を用意すること。			
	③ 大規模なトラブル等により本番稼働への影響が大きい場合には、現行総務省LANへの切り戻しを行うこと。切り戻し作業は、請負者の責任と負担により実施し、切り戻したことにより発生する諸費用はすべて請負者で負担すること。			
第7　引継ぎ				
1　業務運用開始時の引継ぎ				
	① 本業務の運用開始に当たり、運用要員への情報の引継ぎを行うこと。			
	② 請負者は、「運用保守要領」「運用保守実施計画書」「運用保守設計書（運用フロー等含む）」及び「運用保守手順書」等を作成し、主管課の承認を得ること。			
	③ 請負者は、構築・試験時に主管課と協議した内容等を運用員と共有すること。			
2　業務終了時の引継ぎ				
	① 本業務の契約期間が終了する際は次々期総務省LAN受注事業者への情報の引継ぎを行うこと。			
	② 情報引継ぎは、次々期総務省LAN受注事業者と打ち合わせを行い、引き継ぐ情報と作業内容を明らかにすること。			
	③ 総務省LANの運用情報の提供に協力すること。			
	④ データ移行に際しては現行データの提供のため、数回程度の打ち合わせに協力すること。			
	⑤ 運用業務の引継ぎのため、次々期総務省LAN受注事業者の訓練に協力すること。			
	⑥ 請負者が合同庁舎2号館に持ち込んだ機器・設備等は主管課が指定する時期までに撤去し、次々期受注事業者が作業開始できるスペースを用意すること。			

別紙1－1　要件定義書（システム全般）

項番号	内容	提案内容	提案内容 補足資料	記載箇所
第8　教育				
1　教育に係る要件				
(1) 教育要件				
	請負者は業務運用の継続性を担保するためにユーザ・運用担当者に対する教育訓練として以下の項目を含む「教育訓練実施計画書」を作成し、主管課に承認を取った上で作業を進めること。 教育訓練実施後には、「教育訓練実施報告書」を作成すること。記載事項は次のとおり。 ① ・教育・研修目的と対象 ・教育・研修訓練実施体制と役割 ・教育・研修訓練作業内容 ・教育・研修訓練スケジュール ・教育・研修訓練環境 ・教育・研修内容（教育・研修用教材）			
(2) 教育・研修				
	① 教育・研修を実施するに当たり、「教育訓練実施計画書」を作成し主管課の承認を得ること。			
	② 教育・研修対象者への教育・研修を行う講師はシステムを、平易な言葉で説明できること。			
	③ 教育・研修対象者は、各部局の担当者・運用員・ヘルプデスク要員等とする。			
	④ 実施形式は基本的に集合研修で行うこととするが、e-ラーニングでも研修できるように準備すること。			
	⑤ 総務省LAN運用開始初年度は各部局の担当者を対象として5日/年程度の教育・研修を行うこと。次年度以降は2日/年程度の教育・研修を行うこと。			
	⑥ 教育・研修実施後は対象者の理解度を測り主管課に報告すること。			
	⑦ 教育・研修実施後は「教育訓練実施報告書」を提出し、主管課の承認を得ること。			
	⑧ 運用員・ヘルプデスク要員の交代、補充を行う場合は、次期総務省LANに対する教育を受講させてから業務に就かせること。			
	⑨ 請負者は社内で情報セキュリティの教育を実施していること。運用員・ヘルプデスク要員はこのセキュリティの教育を受講していること。			
第9　施設・設備				
1　本省サーバ室				
(1) 設備要件				
ア　スペース				
	① 本省サーバ室では19 インチラック23 本分のスペースが利用できる。			
イ　19 インチラック				
	① ラックは高さ 2,200mm 以下の19 インチラックとすること。			
	② 個別に施錠できること。			
	③ 耐震設置とすること。			
	④ 既存の 19 インチラックを流用することは可能である。			
ウ　耐荷重				
	① 床荷重は500kg/㎡以上であること。			
エ　電源				
	① 単相 100V 及び単相200Vを満たすこと。			
	② 必要に応じて分電盤の工事をすること。			
(2) LAN 管理室				
	① 17名程度が常駐可能なスペースを、LAN 管理室としてサーバ室とは別に利用することは可能である。			

別紙1－1　要件定義書（システム全般）

項番号	内容	提案内容	提案内容 補足資料	記載箇所
(3) その他				
	① 請負者の執務場所は本省とする。ただし、障害復旧等のため外部拠点及び地方支分部局等、本省以外の場所で業務を行う場合がある。			
	② 運用業務を行う上で必要となる事務機器及び消耗品（什器、備品、コピー機、FAX、PC、プリンタ、トナー、テープ媒体等）は、請負者が準備すること。なお、運用業務で使用する内線電話機は総務省が無償で提供する。			
	③ 本省サーバ室に置く各種物品は整理すること。本省サーバ室に置く物は必要最小限とし、不要不急な物は置かないこと。			
	④ 重要な機器や資料は必ず施錠する等、厳重に管理すること。なお、書類は可能な限り電子データで管理することが望ましい。			
	⑤ 配線は安全上、また外観を考慮して整線し、19 インチラックの扉が閉まること。（サーバ室以外も同様とする）			
2 ディザスタリカバリサイト				
(1) 設備要件				
ア 耐震性				
	① 震度6 弱に耐えうる耐震又は免震構造であること。			
イ 消火設備				
	① 現行の建築基準法に規定する耐火性能を満たすこと。			
	② 消火設備は水を使用しないガス消火方式であること。			
	③ 煙検知装置が設置され、火災の早期発見が可能なこと。			
ウ 電源設備				
	① 異なる変電所からの2 系統の受電設備があること。			
	② 法定点検実施時でも停電対応をとる必要がないこと。			
	③ 停電時に十分な電力供給が可能な非常用発電機が設置されていること。			
	④ 電源設備として発電用設備を有し、その発電用設備は無給油で連続24 時間以上、さらに給油を行うことで連続2 日以上、安定的に電力を供給できること。			
	⑤ 停電時に非常用発電機が起動するまでの間、瞬断することなく十分な電力が供給可能なUPSが設置されていること。			
エ 空調設備				
	① 空調設備は24 時間365 日の連続運転が可能であり、機器室が適温、適切な湿度にコントロールされていること。			
	② 電源系統を含めて冗長構成であり、主機器が故障した場合でも必要な冷房能力を確保できること。			
	③ 空調設備に水冷式を採用している場合は、補給水を24 時間以上備蓄していること。			
オ フロア				
	① 二重床で50cm 以上の高さがあること。			
	② フロア強度が500Kg/㎡以上あること。			
カ 19 インチラック				
	① EIA 規格準拠であること。			
	② 最大積載量が200Kg 以上であること。			
	③ 耐震設置であること。			
キ 通信				
	① キャリアフリーであること、又はインターネット接続、広域LAN サービス等通信サービスが構内で直接接続できること。			
ク 入館				
	① 24 時間365 日入館可能であること。			
ケ セキュリティ				
	① 生体情報、IC カード等認証による入退室管理が実施されていること。			
	② 入退館は警備員が駐在又は遠隔監視により24 時間警備が実施されていること。			
	③ 19 インチラックを個別施錠できること。			
	④ 19 インチラック間の監視カメラでフロアを監視していること。			
	⑤ 19 インチラックの設置場所は、死角のない監視カメラにより監視されていること。			

別紙1－1　要件定義書（システム全般）

項番号	内容	提案内容	提案内容 補足資料	記載箇所
コ　その他				
	① 一時的に利用可能な他とは区切られた作業スペースを同一建物内に確保可能なこと。			
	② 機器操作が可能な技術員が常駐していること。			
(2) 資格要件				
	① 当該設備を管理する組織は「情報セキュリティマネジメントシステム(ISMS)適合評価制度」を取得していること。			
(3) 立地要件				
	① 総務省庁舎（東京都千代田区霞が関2-1-2）より直線距離で300km 以上はなれた日本国内の場所かつ、総務省庁舎を午前9 時から午後7 時の間に出発した際に、公共交通機関（航空機等）の利用及び徒歩で平均して360 分以内で到着可能な範囲にあること。			
	② 中央防災会議（内閣府）が設置した首都直下地震対策専門調査会の報告で、震度6 弱以上の地震動が予測される市区町村以外であること。			
	③ 国土交通省告示により定められる地域別地震係数が 0.8 以下であること。			
3　外部監視室				
(1) 設備要件				
ア　耐震性				
	① 震度6 弱に耐えうる耐震又は免震構造であること。			
イ　消火設備				
	① 現行の建築基準法に規定する耐火性能を満たすこと。			
	② 消火設備は水を使用しないガス消火方式であること。			
	③ 煙検知装置が設置され、火災の早期発見が可能なこと。			
ウ　電源設備				
	① 2 系統の受電設備があること。			
	② 法定点検実施時でも停電対応をとる必要がないこと。			
	③ 停電時に十分な電力供給が可能な非常用発電機が設置されていること。			
	④ 電源設備として発電用設備を有し、その発電用設備は無給油で連続24 時間以上、さらに給油を行うことで連続2 日以上、安定的に電力を供給できること。			
	⑤ 停電時に非常用発電機が起動するまでの間、瞬断することなく十分な電力が供給可能なUPS が設置されていること。			
エ　空調設備				
	① 空調設備は24 時間365 日の連続運転が可能であり、機器室が適温、適切な湿度にコントロールされていること。			
	② 電源系統を含めて冗長構成であり、主機器が故障した場合でも必要な冷房能力を確保できること。			
	③ 空調設備に水冷式を採用している場合は、補給水を24 時間以上備蓄していること。			
オ　フロア				
	① 二重床で25cm 以上の高さがあること。			
	② フロア強度が500Kg/㎡以上あること。			
カ　19 インチラック				
	① EIA 規格準拠であること。			
	② 最大積載量が200Kg 以上であること。			
	③ 耐震設置であること。			

別紙1－1　要件定義書（システム全般）

項番号	内容	提案内容	提案内容 補足資料	記載箇所
キ　通信				
①	キャリアフリーであること、又はインターネット接続、広域LAN サービス等通信サービスが構内で直接接続できること。			
ク　入館				
①	24 時間365 日入館可能であること。			
ケ　セキュリティ				
①	生体情報、IC カード等認証による入退室管理が実施されていること。			
②	入退館は警備員が駐在又は遠隔監視により24 時間警備が実施されていること。			
③	19 インチラックを個別施錠できること。			
④	19 インチラック間の監視カメラでフロアを監視していること。			
⑤	19 インチラックの設置場所は、死角のない監視カメラにより監視されていること。			
コ　その他				
①	一時的に利用可能な他とは区切られた作業スペースを同一建物内に確保可能なこと。			
②	作業スペースを同一建物内に確保できない場合は、上記セキュリティレベルを担保した作業スペースを確保すること。			
(2) 資格要件				
①	当該設備を管理する組織は「情報セキュリティマネジメントシステム(ISMS)適合評価制度」を取得していること。			
(3) 立地要件				
①	公共交通機関を使用して、本省から2 時間以内に到着可能な範囲にあること。			
4　工事				
(1) 配線工事				
ア　本省				
①	本省サーバ室の配線工事・整線を行うこと。			
②	無線LANアクセスポイントに接続するケーブルは、既存を流用する事を可とする。			
イ　拠点				
①	拠点のケーブルは原則流用すること。ただし、移行の際に必要な線や不足分、断線等で不調なものはケーブルを準備し、配線すること。			
(2) 電源工事				
ア　本省				
①	本省サーバ室の分電盤工事を行うこと。			
②	現行の電源が利用できるのであれば流用も可能とする。			
イ　拠点				
①	拠点の分電盤工事を行うこと。			
②	現行の電源が利用できるのであれば流用も可能とする。			
(3) 敷設工事				
ア　本省				
①	本省サーバ室の19 インチラックの敷設、ラックへの各機器への敷設工事を行うこと。			
②	無線LANアクセスポイントの設置については、原則として天井設置とすること。			
イ　拠点				
①	各拠点に19 インチラックの敷設、ラックへの各機器への敷設工事を行うこと。			
②	各拠点に無線LANアクセスポイント、及び接続ケーブルの設置、敷設を行うこと。			
③	無線LANアクセスポイントの設置については、原則として天井設置とすること。			

別紙1－2　要件定義書（サービス・機器）

項番号	内容	提案内容	補足資料	記載箇所
第1　調達機器の共通事項				
1　概要				
	総務省LANとして提供する全てのサービスは、セキュリティの担保上の理由から、原則として全て、オンプレミスで提供を行うこと。			
2　ハードウェア				
	① ハードウェアの選定方針を明示すること。			
	② 機器選定は、可能な限り同じメーカの機種を採用する等、運用保守業務の負荷を軽減すること。			
	③ 選定に当たっては、国等による環境物品等の調達推進等に関する法律（グリーン購入法）や RoHS 指令など環境要件に配慮すること。			
	④ 複数のハードウェア要件を統合することも可能とする。その場合は全要件を満たした上で、統合の内容と根拠、性能を記載すること。			
	⑤ サーバラックに収納されたサーバ機器を操作するコンソール（統合的にサーバの操作が行えるディスプレイ及びキーボード等）を必要数用意すること。			
	⑥ 調達する機器は新品であること。			
	⑦ 省電力に配慮した提案をすること。			
	⑧ システムを構成するに当たり、必要なケーブル等の物品は請負者の責任で用意すること。			
	⑨ サーバラック、サーバルームの電源設備等、ファシリティに係る工事も本調達の範囲内とする。なお、詳細情報は、落札後開示する。			
	⑩ システムで必要なディスク容量は、基本的な考え方、拡張性等を考慮して提案すること。なお、データ種別の明示とそれらに対する考え方を明らかにすること。			
	⑪ 以下に導入が想定される機器を記載するが、その他必要と思われる機器を準備すること。提案時には、最適な機器台数で提案を行うこと。ただし、「別紙1-1_要件定義書（システム全般）」における「第2　信頼性等　1　信頼性要件」を遵守すること。			
3　ソフトウェア				
	① ソフトウェアの選定方針を明示すること。			
	② 必要なライセンス数を明示すること。			
	③ 可能な限り開発は行わず、汎用的なパッケージ製品を主体に構成すること。			
	④ 使用するソフトウェアは、可能な限り統一して運用業務の負荷を軽減すること。			
	⑤ 下記に記載する各要件で、提案するソフトウェアの選定根拠、実績等を明示すること。			
	⑥ オープンソースソフトウェアやフリーソフトウェアを採用する際は、合理的な選定理由、著作権等法的な制約、最低でも運用開始から4年間の保守等継続性等を明示すること。			
	⑦ 調達するソフトウェアは、必要なライセンス及び、インストールメディアを用意すること。			
	⑧ ソフトウェアは、過去に出荷及び稼働した実績を持ち、十分に高い信頼性を有し、かつ原則最新のバージョンのものを提案すること。			
第2　共用サーバ・ストレージ				
1　サーバ機器				
(1) 概要				
	本省及びディザスタリカバリサイトにおいて、後述する各サービス機能、セキュリティ機能、運用管理機能を構築するためのサーバ機器を提供する。 具体的要件について、以下に記載する。			
(2) 構築要件				
	① サーバ機器として、後述する各サービス及び各機能に関して、問題なく動作するサーバ構成とすること。			
	② サーバ機器として、動作する各サービスのリソース使用ピーク時が重なった場合を考慮して適切なサイジングを行うこと。			

別紙1－2　要件定義書（サービス・機器）

項番号	内容	提案内容	補足資料	記載箇所
	③ サーバ機器は、ブレード型サーバ上で実現すること。また、システム監視サービスによるハードウェア監視が可能なこと。			
	④ サーバ機器は、セキュリティを考慮して、必要に応じて物理的に分けて構成すること。			
	⑤ 仮想基盤環境を物理的に分ける又はサービス固有の物理サーバを使用する場合は、各サービスの要件に合わせ最適なサイジングを行い、必要な機器を提案すること。			
(3) 機器等要件				
ア ブレード型サーバ				
ソフトウェア要件				
	① ハイパーバイザ型の仮想化基盤を採用すること。			
	② ゲストOSとして、Microsoft Windows Server 2012 R2、RedHat EnterpriseLinux 6及び7が動作可能であること。			
ハードウェア要件				
	① 24時間365日の連続稼働に対応していること。			
	② 温度は10～35℃、湿度は20～80%RH以内（結露がないこと）で動作可能であること。			
	③ 1Gbps以上のLANポートを4個以上又は10Gbps以上のLANポートを4個以上実装可能であり、構成によって選定を行うこと。			
	④ サーバのLANポートは冗長化構成とすること。			
	⑤ 各サーバは最低でも Intel Xeon E5-2697v3（2.60GHz/14コア/35MBキャッシュ）以上のCPUを2個以上搭載し、メモリ容量は128GB以上とすること。			
	⑥ ハードディスクやメモリ等の障害検知が可能であること。			
	⑦ ファイバチャネルを利用する場合は、8Gbps以上のファイバチャネルポートが実装可能であること。実装する場合は冗長化構成を採用すること。			
	⑧ iSCSIを利用する場合は、10GbpsのLANポートを実装すること。			
	⑨ 後述する各サービス及び各機能を満たすのに十分なサーバ台数を用意すること。			
イ ブレード型サーバ収容シャーシ				
ソフトウェア要件				
	① マネジメントモジュールとの接続は、SSHに対応していること。			
ハードウェア要件				
	① 19インチラックに搭載可能であること。			
	② 24時間365日の連続稼働に対応していること。			
	③ 温度は10～35℃、湿度は20～80%RH以内（結露がないこと）で動作可能であること。			
	④ 省電力を目的としたモジュールを有しており、それを実装すること。			
	⑤ シャーシ当たり8台以上のブレードサーバが搭載可能であること。			
	⑥ マネジメントモジュールをシャーシ内部又は外部に実装すること。			
	⑦ サーバブレードと外部との通信を行うモジュールをシャーシ内部又は外部に実装すること。			
	⑧ 40Gbps Ethernet を2ポート以上実装可能であること。			
	⑨ 10Gbps Ethernet を8ポート以上実装可能であること。			
	⑩ 1Gbps Ethernet を12ポート以上実装可能であること。			
	⑪ 8Gbp FibreChannel を8ポート以上実装可能であること。			
	⑫ 電源モジュール、ファンが活性交換可能であること。			

別紙1－2　要件定義書（サービス・機器）

項番号	内容	提案内容	補足資料	記載箇所
2　ストレージ機器				
(1) 概要				
	本省・ディザスタリカバリサイトにおいて、後述するサーバ機能、セキュリティ機能、運用管理機能のストレージ機器を提供する。 ストレージ機能として、スナップショット、仮想マシンバックアップ、リストア、レプリケーション、重複排除、仮想クローン、読み取りを有すること。 具体的要件について、以下に記載する。			
(2) 構築要件				
	① 後述する各サービス及び各機能等に対して、統合的なストレージを提供すること。			
	② ディザスタリカバリサイトと定期的に連携し、必要データのミラーリングを行うこと。			
	③ ディザスタリカバリサイトでも同様のストレージサービスを提供すること。			
	④ CIFS、NFSといったファイル共有プロトコルに対応しモジュールやライセンスを追加することで、iSCSI、FC接続にも対応可能な構成とすること。 ただし、利用するプロトコルは、設計段階で選定すること。			
	⑤ ストレージの割り当て容量が不足した際は、ストレージの未使用領域を利用することで、必要容量の増加に柔軟に対応すること。			
	⑥ 管理ポートを構成し、リモートからコマンドラインの操作が可能になるように構成すること。			
	⑦ 各用途・要件に応じた最適なボリュームを構成すること。			
	⑧ ストレージ機器は、認証サービスと連携すること。			
	⑨ メインストレージとバックアップストレージは別筐体で構築すること。			
	⑩ 本省において、拠点内のバックアップストレージを構築すること。			
	⑪ バックアップストレージはバックアップサービス用の専用領域として使用すること。			
	⑫ コントローラはHAクラスタ構成（Active/Active）とし、電源、ディスク、ファンも冗長化構成とすること。			
	⑬ メインストレージではストレージ階層化機能を有効化すること。			
	⑭ ストレージ機器は、セキュリティを考慮して、必要に応じて物理的に分けて構成すること。			
	⑮ ストレージを物理的に分ける場合は、各サービスの要件に合わせ最適なサイジングを行い、必要な機器、性能及び容量を提案すること。			
(3) 機器等要件				
ア　本省メインストレージ				
ソフトウェア要件				
	① 本体の機能で、本省内及びWAN回線経由の別筐体に対してブロックレベルでの差分レプリケーションを行い、複数世代管理可能であること。			
	② 別筐体から差分データを受け取り、ディスクに書き込む機能を有すること。			
	③ 別筐体に対して差分データをミラーリングする機能を有し、スケジュール設定が可能であること。			
	④ ファイル破損時等において、スナップショット領域からリストアする際に数分で復旧が可能であること。			
	⑤ 重複したブロックをまとめる重複排除機能を有し、効率的なディスク容量の活用を実現すること。また、手動コマンド実行や自動スケジューリングで実行可能であること。			
	⑥ サービスを中断することなく、ボリュームの増減を適時行える機能を有すること。			
	⑦ ストレージの未使用領域を利用することで、ディスク容量の増加に柔軟に対応可能であること。			
	⑧ ストレージ装置は、汎用OSではなく、専用のOSを搭載していること。			
	⑨ 255世代以上のスナップショットを作成できること。ただし、保存世代は、用途に合わせた形で適切な数を構成すること。			
	⑩ コマンド操作でスナップショットからファイルシステム全体又はデータボリュームのリストアを実施できる機能を有すること。			

別紙1－2　要件定義書（サービス・機器）

項番号	内容	提案内容	補足資料	記載箇所
	⑪ 仮想化基盤のスナップショット機能と連携し、仮想マシンを高速にバックアップ、リストアできる機能を有すること。			
	⑫ 書き込み可能な仮想マシンイメージを、フルコピー時に発生するオーバーヘッドなしに、瞬時に複製する機能を有すること。			
	ハードウェア要件			
	① 温度は10～35℃、湿度は20～80%RH以内（結露がないこと）で動作可能であること。			
	② コントローラ当たり1TB以上のリードキャッシュを有すること。			
	③ NFSv3/v4、CIFS、iSCSI及びファイバチャネル接続が提供可能なユニファイドストレージであること。			
	④ 10Gbps以上のLANポートをコントローラごとに2個以上実装可能であり、構成によって選定を行うこと。			
	⑤ コントローラはHAクラスタ構成（Active/Active）とし、電源、ディスク、ファンが冗長化されていること。			
	⑥ ディスクドライブ数480以上、物理容量で2,880TB以上が搭載可能な筐体であること。ただし、ディスクは、利用用途に合わせた形で適切な種別及び数を構成すること。			
	⑦ 2.5インチのSSD及びSASディスクが搭載可能であること。			
	⑧ 3.5インチのニアラインSAS又はSATAディスクが搭載可能であること。			
	⑨ パフォーマンスへの影響を最小限に抑えつつ、二重ディスク障害からデータを保護できること。			
	⑩ 別の専用装置などを用いず、ブロックレベルの重複排除機能を有効化できること。			
	⑪ ファイルへのアクセスを高速化する手段として、フラッシュメモリ等を搭載し、ストレージへの読み取り要求をキャッシュできる機能を有すること。			
	⑫ ファイルへのアクセスを高速化する手段として、SSD等を搭載し、ストレージへの読み書き要求をキャッシュできる機能を有すること。			
	⑬ 後述する各サービス及び各機能を満たすのに十分なストレージ性能、容量及び台数を用意すること。			
	イ　本省バックアップストレージ			
	ソフトウェア要件			
	① 本体の機能で、本省内及びWAN回線経由で別筐体に対してブロックレベルでの差分レプリケーションを行い、複数世代管理可能であること。			
	② 別筐体から差分データを受け取り、ディスクに書き込む機能を有すること。			
	③ 別筐体に対して差分データをミラーリングする機能を有し、スケジュール設定が可能であること。			
	④ ファイル破損時等において、スナップショット領域からリストアする際に数分で復旧が可能であること。			
	⑤ 重複したブロックをまとめる重複排除機能を有し、効率的なディスク容量の活用を実現すること。また、手動コマンド実行や自動スケジューリングで実行可能であること。			
	⑥ サービスを中断することなくボリュームの増減を適時行える機能を有すること。			
	⑦ ストレージの未使用領域を利用することで、ディスク容量増加に柔軟に対応可能であること。			
	⑧ ストレージ装置は、汎用OSではなく、専用のOSを搭載していること。			
	⑨ 255世代以上のスナップショットを作成できること。ただし、保存世代は、用途に合わせた形で適切な数を構成すること。			
	ハードウェア要件			
	① 温度は10～35℃、湿度は20～80%RH以内（結露がないこと）で動作可能であること。			
	② NFSv3/v4、CIFS、iSCSI及びファイバチャネル接続が提供可能なユニファイドストレージであること。			
	③ 10Gbps以上のLANポートをコントローラごとに2個以上が実装可能であり、構成によって選定を行うこと。			
	④ コントローラはHAクラスタ構成（Active/Active）とし、電源、ディスク、ファンが冗長化されていること。			
	⑤ ディスクドライブ数480以上、物理容量で2,880TB以上が搭載可能な筐体であること。ただし、ディスクは、バックアップ用途に合わせた形で適切な種別及び数を構成すること。			
	⑥ 2.5インチのSSD及びSASディスクが搭載可能であること。			
	⑦ 3.5インチのニアラインSAS又はSATAディスクが搭載可能であること。			

別紙1－2　要件定義書（サービス・機器）

項番号	内容	提案内容	補足資料	記載箇所
	⑧ パフォーマンスへの影響を最小限に抑えつつ、二重ディスク障害からデータを保護できること。			
	⑨ 別の専用装置などを用いず、ブロックレベルの重複排除機能を有効化できること。			
	⑩ 後述する各サービスのバックアップを取得するために十分なストレージ性能、容量及び台数を用意すること。			
ウ ディザスタリカバリサイト用ストレージ				
ソフトウェア要件				
	① 本体の機能で、本省内の別筐体に対してブロックレベルでの差分レプリケーションを行い、複数世代管理可能であること。			
	② 別筐体から差分データを受け取り、ディスクに書き込む機能を有すること。			
	③ 別筐体に対して差分データをミラーリングする機能を有し、スケジュール設定が可能であること。			
	④ ファイル破損時等において、スナップショット領域からリストアする際に数分で復旧が可能であること。			
	⑤ 重複したブロックをまとめる重複排除機能を有し、効率的なディスク容量の活用を実現すること。また、手動コマンド実行や自動スケジューリングで実行可能であること。			
	⑥ サービスを中断することなくボリュームの増減を適時行える機能を有すること。			
	⑦ ストレージの未使用領域を利用することで、ディスク容量増加に柔軟に対応可能であること。			
	⑧ ストレージ装置は、汎用OSではなく、専用のOSを搭載していること。			
	⑨ 255世代以上のスナップショットを作成できること。ただし、保存世代は、用途に合わせた形で適切な数を構成すること。			
	⑩ コマンド操作でスナップショットからファイルシステム全体又はデータボリュームのリストアを実施できる機能を有すること。			
	⑪ 仮想化基盤のスナップショット機能と連携し、仮想マシンを高速にバックアップ、リストアできる機能を有すること。			
	⑫ 書き込み可能な仮想マシンイメージを、フルコピー時に発生するオーバーヘッドなしに、瞬時に複製する機能を有すること。			
ハードウェア要件				
	① 温度は10～35℃、湿度は20～80%RH以内（結露がないこと）で動作可能であること。			
	② コントローラ当たり1TB以上のリードキャッシュを有すること。			
	③ NFSv3/v4、CIFS、iSCSI及びファイバチャネル接続が提供可能なユニファイドストレージであること。			
	④ 10Gbps以上のLANポートをコントローラごとに2個以上実装可能であり、構成によって選定を行うこと。			
	⑤ コントローラはHAクラスタ構成（Active/Active）とし、電源、ディスク、ファンが冗長化されていること。			
	⑥ ディスクドライブ数480以上、物理容量で2,880TB以上が搭載可能な筐体であること。ただし、ディスクは、各サービスの利用用途に合わせた形で適切な種別及び数を構成すること。			
	⑦ 2.5インチのSSD及びSASディスクが搭載可能であること。			
	⑧ 3.5インチのニアラインSAS又はSATAディスクが搭載可能であること。			
	⑨ パフォーマンスへの影響を最小限に抑えつつ、二重ディスク障害からデータを保護できること。			
	⑩ 別の専用装置などを用いず、ブロックレベルの重複排除機能を有効化できること。			
	⑪ ファイルへのアクセスを高速化する手段として、フラッシュメモリ等を搭載し、ストレージへの読み取り要求をキャッシュできる機能を有すること。			
	⑫ ファイルへのアクセスを高速化する手段として、SSD等を搭載し、ストレージへの読み書き要求をキャッシュできる機能を有すること。			
	⑬ 後述する各サービス及び各機能を満たすのに十分なストレージ性能、容量及び台数を用意すること。			

別紙1－2　要件定義書（サービス・機器）

項番号	内容	提案内容	補足資料	記載箇所
第3 総務省LANサービス				
1 メールサービス				
(1) 概要				
	総務省職員が省内外との連絡手段として電子メールを用いるため、メールサービスを提供する。 メールサービスには、メール送受信、インターネットメール中継、政府共通ネットワークメール中継、メールストア、メーリングリスト、メールマガジン配信、メールアーカイブ及びアドレス帳機能等が含まれる。 具体的要件について、以下に記載する。			
(2) 構築要件				
	① インターネット、政府共通ネットワーク、総務省LAN内でsoumu.go.jpドメインによるメールサービスを提供すること。			
	② インターネット、政府共通ネットワーク、総務省LAN内それぞれに対して、適切な振り分け機能が利用できること。			
	③ ユーザ宛のメールはディザスタリカバリサービス用に複製し、バックアップすること。また、バックアップしたメールの閲覧が可能であること。			
	④ メールは、送受信ログを1年以上保存し、また、監査用アーカイブとして職員が省外に送信したメールを2年以上保存できること。また、検索、閲覧を行う機能を提供すること。			
	⑤ IMAP4によるメールの取得を実施すること。			
	⑥ ユーザが利用するメールソフトウェアは、Outlook2013を必須とすること。また、複数のメールクライアントでも利用できること。			
	⑦ メールボックスは、容量超過した際に通知や自動削除等が可能となるよう構成すること。			
	⑧ メールアカウントは、職員アカウント及び共有メールアカウントを提供すること。			
	⑨ 兼務職員は、本務のメールアカウントと同じメールボックスを利用できるように提供すること。			
	⑩ 省内外に対して、メールマガジン・メーリングリスト機能を提供すること。			
	⑪ 職員アカウントは、総務省の組織階層構造に準拠して、組織及び職員の構成を自動で反映する階層型のアドレス帳を提供すること。 ・ 省内の組織を階層表示し、組織を選択することで、所属職員が一覧表示されること。 ・ 表示する組織と職員の情報は、総務省LANの「認証サービス」と連携すること。			
	⑫ インターネットメールは、IPv4/IPv6のサービスを提供すること。			
	⑬ 認証サービスと連携したアカウント管理が利用できること。			
	⑭ テレワークサービス利用時に、メール閲覧、送受信、削除の各機能が利用できること。			
	⑮ メールアカウント当たり10GB以上のメールボックスが利用可能であること。			
	⑯ 仮想環境での動作を可とする。			
(3) 機器等要件				
ア メール送受信機能				
ソフトウェア要件				
	① 規模・性能要件に記載したメール流量を処理可能となるよう構成すること。			
	② 2万人以上の規模において稼働実績があること。			
	③ SMTPによるメール配送機能を有すること。			
	④ 人事異動における他省庁への出向を考慮し、受信したメールを他ドメイン向けに自動転送する機能を有すること。			
	⑤ メール配送ログの取得が可能なこと。			
	⑥ メール送受信数、メール送受信容量（KB）は、一定間隔で集計やドメイン別のランキング等のレポーティングが可能なこと。			
	⑦ メールの平均サイズや添付ファイルの平均サイズのレポーティングが可能なこと。			

別紙1－2　要件定義書（サービス・機器）

項番号	内容	提案内容	補足資料	記載箇所
	⑧ メール中継のプロセス数、キュー数やディレクトリの空き容量等の稼働状況を収集し、レポーティングが可能なこと。			
	ハードウェア要件			
	① ハードウェア要件は、本要件定義書の第2－2 ストレージ機器を参照すること。			
イ	インターネットメール中継機能			
	ソフトウェア要件			
	① 規模・性能要件に記載したメール流量を処理可能となるよう構成すること。			
	② 2万人以上の規模において稼働実績があること。			
	③ SMTPによるメール配送機能を有すること。			
	④ メール配送ログの取得が可能なこと。			
	⑤ メール送受信数、メール送受信容量（KB）は、一定間隔における集計やドメイン別のランキング等のレポーティングが可能なこと。			
	⑥ メール中継のプロセス数、キュー数やディレクトリの空き容量等の稼働状況をレポーティングが可能なこと。			
	ハードウェア要件			
	① ハードウェア要件は、本要件定義書の第2－2 ストレージ機器を参照すること。			
ウ	政府共通ネットワークメール中継機能			
	ソフトウェア要件			
	① 規模・性能要件に記載したメール流量を処理可能となるよう構成すること。			
	② 2万人以上の規模において稼働実績があること。			
	③ SMTPによるメール配送機能を有すること。			
	④ メール配送ログの取得が可能なこと。			
	⑤ メール送受信数、メール送受信容量（KB）は、一定間隔における集計やドメイン別のランキング等のレポーティングが可能なこと。			
	⑥ メールの平均サイズや添付ファイルの平均サイズのレポーティングが可能なこと。			
	⑦ メール中継のプロセス数、キュー数やディレクトリの空き容量等の稼働状況をレポーティングが可能なこと。			
	ハードウェア要件			
	① ハードウェア要件は、本要件定義書の第2－2 ストレージ機器を参照すること。			
エ	メールストア機能			
	ソフトウェア要件			
	① ユーザ1人当たり最低10GB以上のメールボックスの利用が可能であること。			
	② 2万人以上の規模において稼働実績があること。			
	③ ユーザごとにメールボックスの容量制限が可能なこと。			
	④ ユーザのメールボックスが制限値を超過した場合、警告メール等の通知が可能なこと。			
	⑤ メールクライアントでのメール受信時に、ID/パスワードによる利用者認証を行うこと。			
	⑥ メールクライアントとのメール受信プロトコルは、IMAP4を使用すること。			
	⑦ 認証サービスとアカウント連携が可能なこと。			
	⑧ 通信経路が暗号化されていること。			
	ハードウェア要件			
	① ハードウェア要件は、本要件定義書の第2－2 ストレージ機器を参照すること。			
オ	メーリングリスト機能			
	ソフトウェア要件			
	① メーリングリストでメールを配信する機能を有すること。			
	② メーリングリストの登録、変更、削除を行う機能を有すること。			

項番号	内容	提案内容	補足資料	記載箇所
	③ 登録メーリングリストや登録ユーザアカウントの一覧を参照、設定する機能を有すること。			
	④ システム管理用インターフェースとしてCLI及びGUIを提供すること。			
	⑤ 他ドメインのユーザも利用が可能なこと。			
	⑥ メーリングリストへの登録が一括で登録が可能なこと。			
	ハードウェア要件			
	① ハードウェア要件は、本要件定義書の第2－2 ストレージ機器を参照すること。			
	カ　メールマガジン配信機能			
	ソフトウェア要件			
	① 配信ログの取得が可能なこと。			
	② データベースやファイルからデータを取り込むことが可能なこと。			
	③ メール業務に支障を与えないよう、メール送信容量の制御が可能なこと。			
	④ データを一元管理し、複数名・複数LAN端末での操作が可能なこと。			
	⑤ ファイルの添付が可能なこと。			
	ハードウェア要件			
	① ハードウェア要件は、本要件定義書の第2－2 ストレージ機器を参照すること。			
	キ　メールアーカイブ機能			
	ソフトウェア要件			
	① 規模・性能要件に記載したメール流量を処理可能となるよう構成すること。			
	② アーカイブされたメールの検索、閲覧機能を有すること。			
	③ メールを2年間以上アーカイブすること。			
	④ 指定期間が経過したメールを自動で削除が可能なこと。			
	⑤ 当サービスに障害が発生した場合もメールサービスを継続可能となるよう構成すること。			
	⑥ 検索を容易かつ直感的に実施するため、専用のGUI管理画面を有すること。			
	⑦ 検索、閲覧に必要なユーザの作成、削除が可能なこと。			
	⑧ 指定条件により特定のメールをアーカイブしない設定が可能なこと。			
	⑨ 本文、添付ファイルの内容のコンテンツ検索が可能なこと。			
	⑩ 作成したユーザに権限を付与して検索、閲覧できる範囲の限定が可能なこと。			
	ハードウェア要件			
	① ハードウェア要件は、本要件定義書の第2－2 ストレージ機器を参照すること。			
	ク　アドレス帳機能			
	ソフトウェア要件			
	① メールクライアントで、ユーザの氏名、役職名でメールアドレス帳の検索が可能なこと。			
	② メールクライアントで、総務省の組織を組織構成に従って階層的に表示し、組織のユーザ一覧から所定のユーザをメール送信先に指定することが可能なこと。			
	ハードウェア要件			
	① ハードウェア要件は、本要件定義書の第2－2 ストレージ機器を参照すること。			
2　ポータルサイトサービス				
(1) 概要				
	総務省職員が円滑に業務を遂行するため、ポータルサイトサービスを提供する。 ポータルサイトには、総務省LANの利用規定・FAQ、インターネット・イントラネット・政府共通ネットワークのWebサイト等の情報を公開するほか、電子掲示板、電子会議室、設備予約、アンケート及びスケジューラ等が含まれる。 また、大臣以下本省内幹部の出退庁情報をリアルタイムに、幹部用表示専用ディスプレイに表示し、総務省LAN端末から閲覧する。 具体的要件について、以下に記載する。			

別紙1－2　要件定義書（サービス・機器）

項番号	内容	提案内容	補足資料	記載箇所
(2) 構築要件				
	① 省内ポータル（MICNET）のコンテンツ作成し、提供すること。			
	② 職員に対して、電子掲示板、電子会議室、設備予約、アンケート、スケジューラのグループウェアサービスを提供すること。			
	③ LAN端末で使用するWebブラウザ（現在はInternetExplorer11、Firefox）でサービスを利用可能にすること。			
	④ グループウェアはパッケージ製品をベースとし、現行の運用や利用状況に応じたカスタマイズすること。			
	⑤ アクセスログは、1年以上保存すること。			
	⑥ 省内ポータル（MICNET）に総務省LANに関する資料（総務省LANの利用規定類、FAQ）へのリンクを掲載すること。			
	⑦ 省内ポータル（MICNET）に電子掲示板、共通基盤支援システム等の各種システムへのリンクを掲載すること。			
	⑧ 省内ポータル（MICNET）に総務省の関係部局が管理するリンクを掲載すること。			
	⑨ 省内ポータル（MICNET）には、イントラネット等の業務に必要な Web サイトへのリンクを掲載すること。			
	⑩ 複数の階層構造の掲示板機能を提供すること。組織階層構造に合わせて階層的に作成できること。			
	⑪ スケジュールは、省・局・部・課・室・個人に対して提供し、組織階層構造に準拠した表示を実現すること。			
	⑫ 大臣以下本省内幹部の出退庁情報をリアルタイムに、幹部用表示専用ディスプレイ及び総務省LAN端末に更新・表示すること。			
	⑬ 省内幹部出退庁情報表示は、専用ソフトをインストールせずに、LAN端末にインストールされているWebブラウザ（Internet Explorer 11）で利用できるように構成すること。			
	⑭ 省内幹部出退庁情報表示は、次のとおり構成すること。 ・名札一覧は、一画面で最大60名分を複数画面表示すること。 ・ログインユーザの区分により、一般用、秘書用、管理用の3種類とすること。 ・最大200人同時接続しても安定して稼働すること。			
	⑮ 幹部個室に幹部用表示専用ディスプレイを設置し、省内幹部出退庁情報表示を行うこと。 幹部用表示専用ディスプレイは、画面比率4:3の19型TFTカラー液晶ディスプレイとし、電源スイッチは有線型とすること。リモコン型の電源スイッチは不可とする。 設置にあたっては、壁面を加工すること無く、既存設置場所と同箇所・同位置に設置すること。なお、既存のものは木目家具調壁面への埋め込み型となっている。			
	⑯ 省内幹部出退庁情報表示の導入場所に設置されている既存表示機器は、設置工事時に撤去し、適切に処分すること。			
	⑰ 幹部用表示専用装置及び幹部用表示専用ディスプレイは、下記の場所に36台（予備機4台含む）設置すること。 11階　局長級幹部室　2台 10階　局長級幹部室　1台 9階　局長級幹部室　3台 7階　上級幹部室　10台、秘書室　5台、局長級幹部室　3台 6階　局長級幹部室　2台 5階　局長級幹部室　1台 4階　局長級幹部室　3台 3階　上級幹部室　2台 予備　4台			
	⑱ 幹部用表示専用装置及び幹部用表示専用ディスプレイの電源操作を行うため、電源スイッチを用意すること。			
	⑲ 電源スイッチの設置場所は、幹部用表示専用ディスプレイと同室内を前提とし、詳細は別途、主管課と協議の上、決定すること。			
	⑳ 電源スイッチの設置及びそれに伴う配線等は、景観を配慮し実施すること。			

項番号	内容	提案内容	補足資料	記載箇所
	㉑ 省内幹部出退庁情報表示に対してセキュリティパッチ適用等メンテナンスを行う時は、閉庁日に作業を実施すること。			
(3) 機器等要件				
ア 省内ポータル機能				
ソフトウェア要件				
	① 総務省のイントラネットホームページサービスを提供し、Webブラウザ起動時の初期画面として表示が可能なこと。			
	② デザインやコンテンツを更新する機能を有すること。			
ハードウェア要件				
	① ハードウェア要件は、本要件定義書の第2－2 ストレージ機器を参照すること。			
イ グループウェア機能				
ソフトウェア要件				
	① それぞれの掲示板には適切なアクセス権の設定が可能なこと。			
	② 電子掲示板はユーザ自身が記事掲載期間を指定でき、情報の登録・修正・削除が可能なこと。			
	③ 掲載期間が経過した電子掲示板の情報は、他のユーザからは見えなくなり、ユーザの設定により参照が可能なこと。			
	④ 電子会議室は特定のグループ内での議論（電子会議）ができるよう、適切なアクセス権が設定が可能なこと。			
	⑤ 電子会議室は管理者が承認した議題のみを公開できる機能を有すること。			
	⑥ 設備予約ができる期間と予約可能な最大時間の設定が可能なこと。			
	⑦ それぞれの設備に対して、予約可能な組織グループ割り当てが可能なこと。			
	⑧ 特定のユーザ又は全体に対して、アンケートを発行する機能を有すること。			
	⑨ アンケートは無記名での回答が可能なこと。			
	⑩ アンケートの回収期限が設定が可能なこと。			
	⑪ アンケートの発行者がアンケートの結果確認、集計を行う機能及びCSV形式等でダウンロードできる機能を有すること。			
	⑫ ToDoリスト機能と連携してユーザが各自のToDoの登録、変更、削除、状況の参照を行う機能を有すること。			
ハードウェア要件				
	① ハードウェア要件は、本要件定義書の第2－2 ストレージ機器を参照すること。			
ウ 幹部出退勤表示機能				
ソフトウェア要件				
	① 省内幹部出退庁情報表示の一般ユーザ用機能は、閲覧のみとし、自動ログインが可能なこと。			
	② 省内幹部出退庁情報表示の秘書用機能は、一般ユーザ用の機能に加え、特定幹部の登退庁情報が更新できること。			
	③ 省内幹部出退庁情報表示の管理用機能は、一般ユーザ用及び秘書用に加え、ユーザIDの管理、画面レイアウト変更のシステム管理が可能なこと。			
	④ 省内幹部出退庁情報表示の画面表示は、FlashPlayerに対応していること。			
ハードウェア要件				
	① 幹部用表示専用装置は、ファンレスタイプであること。			
	② 幹部用表示専用装置は、バックアップ用リチウム一時電池の寿命は5年以上であること。			
	③ 幹部用表示専用装置は、1000BASE-Tのネットワークインタフェースを1ポート以上有すること。			
	④ 幹部用表示専用装置は、VGA又はDVI出力端子を有すること。			
	⑤ 幹部用表示専用ディスプレイは、1,280×1024ドット以上の解像度を有すること。			
	⑥ 幹部用表示専用ディスプレイは、VGA又はDVI入力端子を有すること。			

別紙1－2　要件定義書（サービス・機器）

項番号	内容	提案内容	補足資料	記載箇所
3　ファイル共有サービス				
（1）概要				
	総務省職員が円滑に業務情報を交換・記録するため、ファイル共有サービスを提供する。 2種類の共有フォルダ（組織用・個人用）を提供する。 組織用共有フォルダは、職員が所属する部署によりアクセス権が設定される。 具体的要件について、以下に記載する。			
（2）構築要件				
	① 省・局・部・課・室・個人及び任意に指定された組織に対して、ファイル共有サービスを提供すること。			
	② ログオンユーザの所属組織に応じたドライブマップを実現すること。			
	③ 認証サービスと連携した認証・アクセス権の管理を実施すること。			
	④ 職員に対して、組織用共有フォルダとして26GB以上/人の領域を確保すること。			
	⑤ 職員に対して、個人用共有フォルダとして10GB以上/アカウントの領域を確保すること。			
	⑥ 組織用共有フォルダのデータはディザスタリカバリサービスにより複製し、バックアップすること。			
	⑦ ファイル共有サービスは、本省又はディザスタリカバリサイトで提供すること。			
	⑧ ユーザの利用する領域とは別にスナップショット領域を確保し、複数世代管理を実施すること。			
	⑨ 組織用共有フォルダ、個人用共有フォルダへのアクセスのログを3年以上、保存すること。			
	⑩ 各サービスがシステム上、必要とする共有フォルダを本サービスで提供することを可とする。ただし、職員が利用する領域とは別に準備すること。			
	⑪ アクセス負荷等を考慮し、組織用共有フォルダ及び個人用共有フォルダの配置を実施すること。			
	⑫ スナップショットは、7世代以上保存すること。また、スナップショット用の領域を考慮した上でサイジングを行うこと。			
（3）機器等要件				
ア　ファイル共有（個人用）機能				
ソフトウェア要件				
	① 各フォルダに対して、アクセス権の設定が可能であること。また、アクセス権限は認証サービスと連携できること。			
	② 各共有フォルダに対して容量制限が行えること。			
	③ Windows及びLinuxからのファイル共有が可能であること。			
	④ 個人領域として10GB/人以上の領域を確保した構成とすること。			
	⑤ 容量超過時にメール通知が可能であること。			
	⑥ 十分なスナップショット領域を確保し、90世代管理可能であること。			
	⑦ スナップショット領域はユーザの閲覧可否の設定が可能であること。			
	⑧ データ領域の効率的利用を目的とし、LAN端末がアクセスする領域に対し、ブロックレベルの重複排除機能を実装すること。			
	⑨ 本体の機能で、本省内の別筐体に対してブロックレベルでの差分レプリケーションを行い、複数世代管理可能であること。			
ハードウェア要件				
	① ハードウェア要件は、本要件定義書の第2－2 ストレージ機器を参照すること。			
イ　ファイル共有（組織用）機能				
ソフトウェア要件				
	① 各フォルダに対して、アクセス権の設定が可能であること。また、アクセス権限は、認証サービスと連携できること。			
	② 各共有フォルダに対して、容量制限が行えること。			
	③ Windows及びLinuxからのファイル共有が可能であること。			

別紙1－2　要件定義書（サービス・機器）

項番号	内容	提案内容	補足資料	記載箇所
	④ 組織領域として26GB/人以上の領域を確保した構成とすること。			
	⑤ 容量超過時にメール通知が可能であること。			
	⑥ 十分なスナップショット領域を確保し、90世代管理可能であること。			
	⑦ スナップショット領域はユーザの閲覧可否の設定が可能であること。			
	⑧ データ領域の効率的利用を目的とし、LAN端末がアクセスする領域に対して、ブロックレベルの重複排除機能を実装すること。			
	⑨ 本体の機能で、本省内及びWAN回線経由の別筐体に対してブロックレベルでの差分レプリケーションを行い、複数世代管理可能であること。			
	⑩ 主管課が指示する一部の兼務職員に対して、本務組織に加え、兼務組織に紐付く組織用共有フォルダに、再ログオンすることなくアクセス可能な環境を準備すること。なお、兼務組織に紐付く組織用共有フォルダへのアクセスを許可する期間については、任意に設定可能であること。			
	ハードウェア要件			
	① ハードウェア要件は、本要件定義書の第2－2 ストレージ機器を参照すること。			
4	**大容量ファイル転送サービス**			
(1)	**概要**			
	総務省職員と省外の関係者間において、メール添付では扱えない大容量ファイルの送受信を行うために大容量ファイル転送サービスを提供する。 具体的要件について、以下に記載する。			
(2)	**構築要件**			
	① 総務省LANにおいて、通信の暗号化等安全に大容量ファイルの受け渡しが可能な環境の設計・構築を行うこと。			
	② 職員の利用するLAN端末、デスクトップ仮想化環境、省外の関係者の利用するPC環境から大容量ファイル転送サービスが利用できるように構成すること。			
	③ 省外の関係者が大容量ファイル転送サービスを利用する際には、職員がファイルのアップロードや受取り用のフォルダを用意する等、必ず総務省職員がやり取りの起点となるように構成すること。			
	④ 省外の関係者からのWebアクセスを処理するための公開サーバをDMZに配置し、インターネットから直接、省内に侵入できないように構成すること。			
	⑤ 省内から大容量ファイル転送サービスを利用するためのアカウントは、セキュリティに配慮したものとすること。			
	⑥ アカウントのパスワードには、一定期間で変更が要求されるようなパスワードポリシーを設定すること。			
	⑦ 公開サーバと端末との間の通信は暗号化すること。			
	⑧ 公開サーバにアクセスする際の公開URLは、ランダムなものが生成されるように構成すること。			
	⑨ 省外の関係者によるファイルダウンロード及びファイルアップロードに当たっては、職員が独自に回数の制限や公開期間を設定できるように構成すること。			
	⑩ 本サービスの操作ログ、アクセスログを1年以上保存すること。			
	⑪ ファイルのアップロード時には、ウィルスチェックが実行されること。			
	⑫ 省内へのファイルダウンロード時には、マルウェア対策（インターネット・Web）サービスが実行されるように構成すること。			
(3)	**機器等要件**			
ア	大容量ファイル転送機能			
	ソフトウェア要件			
	① Webブラウザを介して、ファイルの送受信が可能であること。			
	② ファイルの送信先には、受信に使用するURLをメールで通知が可能なこと。この受信に使用するURLは、受信者以外にはわからないURLであること。また、ファイルのダウンロードの際は、パスワード認証を行うことが可能であること。			

別紙1－2　要件定義書（サービス・機器）

項番号	内容	提案内容	補足資料	記載箇所
	③ 登録されたユーザは、所属するフォルダに対し、ファイルのアップロード及びダウンロードが行えること。			
	④ 複数のファイルをアップロード可能であること。また、複数の宛先に対して送信可能であること。			
	⑤ アップロードされたファイルを複数選択又は全選択して削除する操作が可能であること。			
	⑥ ファイルのアップロード時にウイルスチェックを行う機能を有すること。			
	⑦ ファイルのアップロード時に、ダウンロード期間とダウンロード可能回数を設定でき、超過した場合は自動削除可能であること。また、システム管理者が初期値と上限値をそれぞれ設定可能であること。			
	⑧ SSL通信が可能であること。			
	⑨ ユーザが連続してログオンに失敗した場合に、ユーザのアカウントをロックする機能を有すること。また、アカウントのロックを自動解除することが可能であること。			
	⑩ ユーザ管理画面を有し、手動操作によりユーザの登録・変更・削除が可能であること。			
	⑪ ユーザの登録情報をCSV形式でエクスポート可能であること。			
	⑫ CSV形式によりユーザのインポート（一括登録・変更・削除）が可能であること。			
	⑬ 転送するファイルを格納するフォルダごとに、アップロードやダウンロードなどのアクセス権をユーザ単位で設定可能であること。			
	⑭ ユーザやグループ、フォルダごとに利用可能容量制限（クォータ）を設定可能であること。			
	⑮ アップロード可能なファイルの拡張子を設定可能であること。			
	⑯ システムが発信する通知メールの定型文書を管理者が任意に設定する機能を有すること。また、通知メール文書は、ユーザにより修正可能であること。			
	⑰ ログオン画面及び操作画面の説明や画像を変更する機能を有すること。			
	⑱ システムの利用状況や統計情報を参照可能であること。			
	⑲ ファイル転送履歴を参照可能であること。また、履歴は画面表示及びCSVファイルでの出力が可能であること。			
	⑳ 最大で20,000ユーザに対応できること。			
	㉑ Internet ExplorerとFirefoxから利用可能であること。			
	㉒ ストレージ接続プロトコルとして、iSCSI、NFSに対応していること。			
	ハードウェア要件			
	① ラックマウント型のアプライアンス製品であること。			
	② EIA規格19インチラックに搭載可能であり、2U以下であること。			
	③ 4TB以上のディスク容量を有すること。			
	④ 1000BASE-Tのネットワークインタフェースを1ポート以上有すること。			
	⑤ 電源は、AC100V（標準周波数50Hz）で動作可能であること。			
	⑥ 装置の冗長化が可能であること。			
5　認証サービス				
(1) 概要				
	総務省職員等のアカウント情報を一元管理し、各サービスへの接続時に認証及びアクセス権の付与を行うため、認証サービスを提供する。 生体認証サービスを利用することにより、パスワードの入力が不要になる。 各種サービスにおいて利用する証明書を発行する。 具体的要件について、以下に記載する。			
(2) 構築要件				
	① 認証基盤として、ユーザやコンピュータを一元管理すること。			
	② 指紋、静脈などの生体認証により個人を識別し、認証・権限付けを行えること。			
	③ 認証の履歴を1年以上保存すること。			
	④ ユーザやコンピュータを組織に紐づいたポリシーに基づき管理できること。			

別紙1－2　要件定義書（サービス・機器）

項番号	内容	提案内容	補足資料	記載箇所
	⑤ 共通基盤支援システムからユーザ情報及びパスワード情報等を定期的に取得し、関連するサービスに各種情報を配付・連携すること。			
	⑥ ディザスタリカバリサービス用のディレクトリ機能と相互にレプリケーションを行うこと。			
	⑦ ディレクトリ機能の情報を利用し、シングルサインオン機能を提供すること。			
	⑧ 国家公務員身分証明証として用いる個人番号カードの情報をディレクトリ機能に登録すること。			
	⑨ 部課室に別途調達されているLAN複合機のコピー用として払い出しているカードの認証機能を提供すること。			
	⑩ ディレクトリ機能と連携するプライベート認証局機能を提供すること。			
	⑪ ユーザアカウント、システム用アカウント及び管理者用アカウントを区別し、適正に管理を行うこと。			
	⑫ 職員に対して、共有メールアカウントのパスワードを変更できる環境を提供すること。			
(3) 機器等要件				
ア ディレクトリ機能				
ソフトウェア要件				
	① LAN端末から総務省LANにアクセスする際のユーザ単位での認証を提供すること。			
	② ユーザアカウントは、組織ごとの階層管理を行えること。			
	③ ユーザアカウントをまとめてグループとして管理が可能であること。			
	④ LAN端末から総務省LANにアクセスする際にユーザとグループ単位でのアクセス管理可能であること。			
	⑤ ユーザ認証の履歴の記録、管理が可能であること。			
	⑥ 人事異動やユーザからの申請等に応じ、ユーザやグループの作成・変更・削除が可能であること。			
	⑦ 特定のグループにのみ個別のパスワードルールを適応できること。			
ハードウェア要件				
	① ハードウェア要件は、本要件定義書の第2－2 ストレージ機器を参照すること。			
イ 総務省LANユーザ情報管理機能				
ソフトウェア要件				
	① 総務省の総務省共通基盤支援システムから職員情報を受け取り、以下のサービスとの間で必要であれば、アカウントやアクセス権を付与・設定すること。 ・申請管理サービス ・生体認証サービス ・ディレクトリ機能 ・メールサービス ・ポータルサイトサービス ・ファイル共有サービス ・コミュニケーションサービス ・階層アドレス帳 ・メールプロファイル ・大容量ファイル転送サービス ・インシデント管理機能 ・災害時掲示板 ・認証プリントサービス ・上記サービスのうち、ディザスタリカバリサイトで公開されるサービス			
	② 適切な猶予期間を設けて、不要となったアカウント、アクセス権、関連するリソースを削除すること。			
	③ 何らかの原因で処理が途中停止した場合でも、速やかに整合をとるための再実行機能を有すること。			
	④ 6000人分の設定変更処理を6時間以内に終了できるパフォーマンスを持つこと。			
	⑤ 平常時の更新は、2時間で終了できるパフォーマンスを持つこと。			
	⑥ パスワード更新は、10分で終了できるパフォーマンスを持つこと。			
	⑦ 共有メールアカウントのパスワードを変更するインターフェースを持つこと。			

項番号	内容	提案内容	補足資料	記載箇所
	⑧ 共有メールアカウントのパスワード変更を行う場合は、総務省職員IDでログオンを行うこと。			
	⑨ 主管課がすべての共有メールアカウントのパスワード初期化を行う機能を持つこと。			
	⑩ 共有メールアカウントのパスワード変更履歴が保存されること。			
	⑪ それぞれの情報の整合性がとれていること。			
	ハードウェア要件			
	① ハードウェア要件は、本要件定義書の第2－2 ストレージ機器を参照すること。			
ウ 生体認証機能				
	ソフトウェア要件			
	① 生体情報による認証により、ログオン認証、スクリーンセーバロック解除、及びアプリケーションログオン等の認証ができること。			
	② 生体情報は、暗号化され集中管理されていること。			
	③ 生体情報の登録・削除・変更機能を有すること。			
	④ 利用者ログ及び管理者ログを取得することが可能であること。			
	⑤ 生体認証が行えない場合、一時的にID、パスワードによる代替認証も可能であること。			
	ハードウェア要件			
	① 全LAN端末で生体認証を利用可能であること。			
エ 認証局機能				
	ソフトウェア要件			
	① ディレクトリ機能と連携し、証明書を発行する機能を有すること。			
	② SHA-2以上、2048ビット以上の証明証のみ発行すること。			
	③ サービス提供期間を超える証明書が発行できること。			
	④ 目的により、証明書テンプレートを準備できること。			
	ハードウェア要件			
	① 特に規定しない。			
6 テレワークサービス				
(1) 概要				
	総務省職員の多様で柔軟な働き方を可能にし、ワーク・ライフ・バランスを実現するため、テレワークサービスを提供する。 在宅業務、出張、災害時において、LAN端末・タブレット型端末・シンクライアントを利用した個人所有端末からサービスを利用できる。 通常時は本省へアクセス、災害発生時はディザスタリカバリサイトへアクセスする。 具体的要件について、以下に記載する。			
(2) 構築要件				
	① 省外からインターネット経由で安全なアクセスを実現すること。			
	② 外部接続を処理するための公開サーバをDMZに配置し、外部からのアクセスに対してインターネットから直接省内に侵入できないように構成すること。			
	③ 仮想デスクトップ環境で使用するシンクライアントデバイスは、個人所有端末上のOSを流用せず、別途シンクライアント専用のOSを準備すること。			
	④ 接続時の認証は、二要素認証を実施すること。			
	⑤ 接続に関するアクセスログを1年以上保存すること。			
	⑥ 紛失時の情報漏えいを防止するため、シンクライアントデバイスの記憶領域は暗号化されていること。			
	⑦ LAN端末・タブレット型端末・個人所有端末からインターネットを経由して、総務省LANの各種サービス（メール、ファイル共有、Web接続、コミュニケーションサービス、オフィス製品の利用、業務システムの利用）を提供すること。			
	⑧ LAN端末では、リモートアクセス機能での総務省LANへのアクセス環境を提供すること。			

別紙1－2　要件定義書（サービス・機器）

項番号	内容	提案内容	補足資料	記載箇所
	⑨ タブレット型端末、個人所有端末は、デスクトップ仮想化機能で総務省LANへのアクセス環境を提供すること。			
	⑩ 本省とディザスタリカバリサイトの双方に仮想デスクトップ環境を構築し、通常時は本省へアクセス、災害発生時はディザスタリカバリサイトへアクセスする環境を構築すること。			
	⑪ 総務省LANへの不正な接続を検知するため、シンクライアントデバイスから総務省LANに接続された際に、予め登録された複数のメールアドレスに通知される環境を構築すること。			
	⑫ 総務省LANへの接続の際に、LAN端末に対して、セキュリティパッチの適用状況を確認すること。			
	⑬ システム領域を占有する仮想デスクトップ環境を利用している場合、申請アプリケーションがインストール可能であること。			
	⑭ デスクトップ仮想化環境はドメインに参加した環境で利用可能であり、総務省LANと同一の認証方式を利用して構築すること。			
	⑮ テレワークサービス全体としては、本省では最大同時接続で1500人の職員にサービスを提供する規模で環境を構築すること。また、ディザスタリカバリサービス利用時に必要な最大同時接続数は、その半分（750）とする。			
	⑯ 仮想デスクトップ環境の本省構成において、システム領域を占有する仮想デスクトップ環境を50台分用意すること。			
	⑰ 仮想デスクトップ環境の本省構成において、システム領域を共有する仮想デスクトップ環境を、ユーザプロファイルが保持可能な構成で約5,000ユーザ分用意すること。			
	⑱ 仮想デスクトップ環境のディザスタリカバリ構成において、システム領域を共有する仮想デスクトップ環境を、ユーザプロファイルが保持可能な構成で約5,000ユーザ分用意すること。			
	⑲ テレワークサービスで、コミュニケーションサービス（メッセージ交換、在席管理、Web会議）が利用できること。			
（3）機器等要件				
ア　リモートアクセス機能				
ソフトウェア要件				
	① 総務省LANへの接続の際に、端末のOSパッチの適用状況、ウイルスチェックソフトのパターン更新状況、端末の固有情報等をチェックし、条件を満たさない場合は総務省LAN内部ネットワークへ接続できないこと。			
	② LAN端末から外部ネットワークを経由して、総務省LANの各種サービス（メール、ファイル共有、Web接続、コミュニケーションサービス、オフィス製品の利用、対応した業務システムの利用）を提供すること。			
	③ 内部のメールサービスが利用できること。			
	④ システム管理用インターフェースとして、CLI及びGUIを提供すること。			
	⑤ 接続時の認証、通信路の暗号化、接続記録の保持等十分なセキュリティ対策を施すこと。			
	⑥ 認証方式として、ワンタイムパスワード又は生体認証が行えること。			
	⑦ リモートアクセス経由でアクセス可能なネットワーク及び使用可能なアプリケーションを限定する機能を有すること。			
	⑧ 利用できるサービスは、ポリシーによる制御を実現すること。			
ハードウェア要件				
	① 本省に設置するサーバおいては、最大接続数が1,000以上に耐える構成とすること。また、ディザスタリカバリサイトに設置するサーバにおいては、最大接続数が500以上に耐える構成とすること。			
	② 有線LAN及び無線LANに接続したLAN端末から、リモートアクセス機能が利用可能なこと。			

別紙1－2　要件定義書（サービス・機器）

項番号	内容	提案内容	補足資料	記載箇所
イ	デスクトップ仮想化機能			
	ソフトウェア要件			
①	個人所有端末から外部ネットワークを経由して、総務省LANの各種サービス（メール、ファイル共有、Web接続、コミュニケーションサービス、オフィス製品の利用、対応した業務システムの利用）を提供すること。			
②	内部のメールサービスが利用できること。			
③	システム管理用インターフェースとして、CLI及びGUIを提供すること。			
④	認証方式として、ワンタイムパスワード又は生体認証が行えること。			
⑤	利用できるサービスは、ポリシーによる制御を実現すること。			
⑥	シンクライアントは、転送された画面上で操作が可能なリモートデスクトップ接続機能を有すること。			
⑦	総務省LANで管理しているアカウントと連携して、VPN接続が可能なこと。			
⑧	OSの起動時には、パスワード認証が必要となる設定が可能であること。			
⑨	パスワードを設定回数以上間違えると自動的にパスワードがロックされる機能を有すること。			
⑩	シンクライアントデバイスに保存される情報は、総務省LANとの接続に必要な設定等に限定され、任意のデータの記録ができないこと。			
⑪	総務省外から外部接続環境に接続する際には、通信を暗号化したVPN接続を行うこと。			
⑫	事前に許可された端末のみ、本環境への接続を許可すること。			
⑬	ユーザ認証においては、ユーザID、パスワードに加え、ワンタイムパスワード等のセキュリティ強化の施策を導入すること。			
⑭	ユーザID及びパスワードは通常使用しているアカウントとし、総務省LANと同期できること。			
⑮	総務省LANサービス（メール、インターネット、掲示板、ファイルサービス等）が利用できること。			
⑯	ICA、PCoIP等の画面転送プロトコルに対応していること。			
	ハードウェア要件			
①	ハードウェア要件は、本要件定義書の第2－2 ストレージ機器を参照すること。			
②	本省に設置するサーバ及びストレージは、最大同時接続数が650以上に耐える構成とすること。また、ディザスタリカバリサイトに設置するサーバ及びストレージは、最大同時接続数が300以上に耐える構成とすること。			
③	シンクライアント専用OSが入ったシンクライアントデバイスは、Microsoft社におけるWindows To Goデバイスとして認定を受けていること。			
④	シンクライアント専用OSが入ったシンクライアントデバイスは、ファームウエアの更新の際、デジタル証明での改ざん防止機能を有すること。			
⑤	シンクライアント専用OSが入ったシンクライアントデバイスは、システム領域を占有する仮想デスクトップ環境用に50台分、システム領域を共有する仮想デスクトップ環境用に1,300台分を用意すること。また、災害時用に200台分を用意すること。			
⑥	災害時用の200台分は、自治大学校、情報通信政策研究所にそれぞれ100台分配備すること。			
⑦	シンクライアントデバイスには、総務省LANとの接続に必要な機能に限定された専用のOSが搭載されていること。			
⑧	運用及びセキュリティ上の問題がないように、シンクライアント専用OSに適切にパッチを適用すること。			
⑨	シンクライアントデバイスの記憶領域は暗号化されていること。			
⑩	タブレット型端末20式は、9.7インチ（対角）LEDバックライトマルチタッチディスプレイを搭載すること。			
⑪	解像度は、2,048 x 1,536ピクセル以上であること。			
⑫	内蔵ディスク容量は16GB以上であること。			
⑬	ネットワークはWi-Fi及び携帯電話回線が利用可能であること。			
⑭	カメラを搭載していること。			
⑮	機能制限等のプロファイルを適用できること。			

別紙1－2　要件定義書（サービス・機器）

項番号	内容	提案内容	補足資料	記載箇所
	⑯ 覗き見防止フィルタ、保護ケース、タッチペンを本体台数分添付すること。			
7 コミュニケーションサービス				
(1) 概要				
	メッセージ交換、在席管理、Web会議を用いてコミュニケーションを円滑にし、ワークスタイル変革を推進するため、コミュニケーションサービスを提供する。 具体的要件について、以下に記載する。			
(2) 構築要件				
	① 総務省LAN内でメッセージ交換、在席管理、Web会議が行えるように構成すること。			
	② 認証サービスと連携し、ユーザ管理や利用時の認証を行うこと。			
	③ メッセージ交換機能を利用したメッセージの内容及び誰と誰が利用したかの履歴を1年以上保存すること。			
	④ テレワークサービスと連携し、省外からコミュニケーションサービス（メッセージ交換、在席管理、Web会議）が利用できるように構成すること。			
	⑤ 別途調達の共用webカメラ・共用マイク等を用いて、複数人がWeb会議を行えるよう構成すること。			
	⑥ LAN端末及びタブレット型端末から安全に利用できる環境の設計・構築を行うこと。また、セキュリティ面については、外部ユーザ（職員以外）の端末からの利用を十分考慮した設計・構築を行うこと。			
	⑦ 現行システムではVPN経由で総務省LANに接続しコミュニケーション・ツールを利用しているが映像・音声が利用できない課題に対応するため、総務省職員が省外からWeb会議に参加する際は、VPN経由ではなく外部ユーザ（職員以外）として利用させる等の運用設計を行うこと。			
	⑧ システム上の保存データ（アーカイブ系データベース）とロギングデータ（監視系データベース）のそれぞれについて、障害からの復旧を容易にするためのバックアップを取得するよう構成すること。			
	⑨ 在席管理機能では、職員の内線番号を表示すること。			
	⑩ 総務省の組織階層構造に準拠した組織及び職員の構成を自動で反映する階層型のアドレス帳を提供すること。 ・省内の組織を階層表示し、組織を選択することで、所属職員が一覧表示されること。 ・職員を氏名の一部で検索できること。 ・表示する組織と職員の情報は、総務省LANの「認証サービス」と連携すること。			
	⑪ 職員がログインした記録を1年以上保存すること。			
	⑫ web会議機能は、複数の会議室を提供可能であること。また、複数の会議室の会議参加者の合計は、ネットワーク（インターネット回線及び総務省WAN回線）の利用帯域が逼迫している場合を除き、1000名以上とする。			
	⑬ web会議の会議室の予約は、LAN端末で使用するWebブラウザ（現在はInternetExplorer11、Fireiox）から可能であること。			
	⑭ 省外の関係者は、Webブラウザ又はモバイル端末アプリケーションを用いて会議に参加できるように構成すること。			
	⑮ 省外の関係者が会議に参加する場合には、職員の承認が必要となるように構成すること。			
	⑯ 省外の関係者からは、会議の開催はできないように構成すること。			
	⑰ 省外の関係者との間では、資料の受け渡しができないように構成すること。			
	⑱ Web会議機能では、会議参加者、会議開催時間、会議内での資料共有の有無等の利用状況のログを取得できるようにすること。			
	⑲ 省外の関係者からのweb会議参加を処理するための公開サーバをDMZに配置し、外部からのアクセスに対してインターネットから直接、省内に侵入できないように構成すること。			
(3) 機器等要件				
ア メッセージ交換機能				
ソフトウェア要件				
	① リアルタイムに文字ベースでユーザ間で会話できる機能を有すること。			

項番号	内容	提案内容	補足資料	記載箇所
	② 在席管理機能を利用して、連絡可能なユーザとの会話を容易に開始できること。			
	③ 在席管理機能を利用して、ユーザを会話に招待することができること。			
	④ 在席管理機能を利用して、複数のユーザと会話することができること。			
	⑤ 会話中の相手にファイルを送信することができること。			
	⑥ サーバにメッセージの記録が残せること。			
	ハードウェア要件			
	① ハードウェア要件は、本要件定義書の第2－2 ストレージ機器を参照すること。			
	イ 在席管理機能			
	ソフトウェア要件			
	① 連絡先ユーザが連絡可能な状態にあるか把握することができる機能を有すること。			
	② アイコンと文字の情報を使って、視覚的にわかりやすく表示されること。			
	③ ユーザの状態は、「連絡可能」、「取り込み中」、「応答不可」、「一時退席中」、「業務時間外」等、状況を的確に反映できる数種類以上の表示が可能であること。			
	④ ユーザの状態は、PCの稼働状態やユーザの操作状況から自動的に変化させることができること。			
	⑤ ユーザの状態は、手動で変更することも可能であること。			
	⑥ 在席表示されているユーザをクリックすることで、メッセージ交換サービスを起動できること。			
	⑦ 頻繁に連絡をとるユーザ等をひとまとめにして情報共有しやすくするために、グループを作成する機能を有すること。			
	ハードウェア要件			
	① ハードウェア要件は、本要件定義書の第2－2 ストレージ機器を参照すること。			
	ウ Web 会議機能			
	ソフトウェア要件			
	① カメラとマイクを追加することにより、Web会議を開催できる機能を有すること。			
	② 在席表示されているユーザをクリックすることで、Web会議サービスを起動できること。			
	③ 会議参加者全員が閲覧、書き込みが行えるホワイトボード機能を有すること。			
	④ 会議参加者全員がファイルを展開、共有、閲覧する機能を有すること。			
	⑤ 会議画面解像度は最大1920×1080（ピクセル）であること。			
	⑥ 会議開催中にメッセージ交換サービスが利用できること。			
	⑦ 会議開催中に参加者間で資料の受け渡しが可能なこと。			
	⑧ ブラウザ（Internet Explorer及びFirefox）から会議室の予約が可能であること。			
	⑨ 会議開催中にメッセージ交換機能が利用できること。			
	⑩ 会議開催中に参加者間で資料の受け渡しができること。			
	⑪ すべてのユーザに会議を主催できる個別のIDを付与できること。			
	⑫ 会議の開催及びメンバの指定・招集等を実施できること。			
	⑬ 利用状況のログを月ごとに取得できること。			
	⑭ 機器性能（WAN回線帯域を考慮しない状況）としては、会議同時開催が1,000以上実施できること。			
	ハードウェア要件			
	① ハードウェア要件は、本要件定義書の第2－2 ストレージ機器を参照すること。			
8 ペーパーレス会議サービス				
(1) 概要				
	会議室内での電子データの資料共有・閲覧を可能にし、業務効率を向上させるため、ペーパーレス会議サービスを提供する。 タブレット型端末からWebブラウザ又は専用ソフトウェアを介して、会議資料を共有・閲覧する。 具体的要件について、以下に記載する。			

別紙1－2　要件定義書（サービス・機器）

項番号	内容	提案内容	補足資料	記載箇所
(2) 構築要件				
	① 総務省LANの無線LAN環境を利用して、タブレット型端末を用いたペーパーレス会議サービスを構築すること。			
	② 別途調達するiOS搭載のタブレット型端末を用いること。			
	③ 認証サービスと連携し、会議参加者の登録及び利用時の認証を行うよう構成すること。			
	④ 省外からの参加者は、「認証サービス」上でペーパーレス会議システム専用の一時的なユーザとして管理すること。			
	⑤ 参加者を登録する際、総務省の組織階層構造に準拠した組織及び職員の構成を自動で反映する階層型のアドレス帳を提供すること。 ・省内の組織を階層表示し、組織を選択することで、所属職員が一覧表示されること。 ・職員を氏名の一部で検索できること。 ・表示する組織と職員の情報は、総務省LANの「認証サービス」と連携すること。			
	⑥ サービス提供サーバとタブレット型端末間の通信は、総務省LANにおける無線LANインフラのLAN端末とは異なるセグメントを用いて実現すること。			
	⑦ サービス提供サーバとタブレット型端末間の通信は、暗号化されるよう構成すること。			
	⑧ 複数会議の合計で同時に200台のタブレット型端末から利用可能であること。			
	⑨ 1会議に100台のタブレット型端末が同時に参加可能であること。			
	⑩ 会議の開催準備及び会議後のメモデータ回収等の際には、データのアップロード及びダウンロードのために、LAN端末からもアクセスできるように構成すること。			
	⑪ ペーパーレス会議で使用する資料等は、会議が始まる前にタブレット型端末へダウンロードできる構成とすること。			
(3) 機器等要件				
ア　ペーパーレス会議機能				
ソフトウェア要件				
	① サーバにアップロードした会議資料を、タブレット型端末で閲覧できること。			
	② 会議資料や参加者等のデータの保管、画面や状態の制御は、専用のサーバにより実現されること。			
	③ タブレット型端末の操作においては、スワイプ、ピンチ、フリック等、スマートデバイス特有のジェスチャーが有効に利用できること。			
	④ 最大で 200台の端末から同時に利用可能であること。			
	⑤ 1つの会議に最大 100台の端末が参加可能であること。			
	⑥ サーバと端末間の暗号化通信機能を有すること。			
	⑦ 会議開催者が会議データを作成し、会議参加者を登録、削除できること。			
	⑧ 会議主催者及び登録された会議参加者が会議資料を登録、削除できること。			
	⑨ 会議資料として、次に挙げるファイル形式のものが登録可能であること。 ・PDF ・Microsoft Word（doc、docx） ・Microsoft Power Point（ppt、pptx） ・JPEG ・PNG ・TIFF ・Windowsビットマップ（bmp） ・GIF ・テキスト（txt）			
	⑩ 会議開催中であっても、会議参加者及び会議資料の登録と削除が可能なこと。			

別紙1－2　要件定義書（サービス・機器）

項番号	内容	提案内容	補足資料	記載箇所
⑪	会議資料及び参加者情報を含む会議データは、会議開催後、所定の日数経過後に自動的にサーバ上から削除されること。			
⑫	ユーザ名とパスワードを用いたログイン機能を有すること。			
⑬	ログイン認証は、認証サービスと連携して実行可能であること。			
⑭	システムにログインした際、参加可能な会議の一覧が表示され、任意の会議を選択して参加できること。			
⑮	会議選択後、当該会議に登録された資料の一覧が表示され、任意の資料を選択して閲覧できること。			
⑯	資料閲覧画面において、スワイプ操作により資料のページ送りができること。			
⑰	資料閲覧画面において、資料の縮小表示（サムネイル）から任意のページを選択して移動できること。			
⑱	資料閲覧画面において、ピンチ操作により表示中のページを拡大・縮小して表示できること。			
⑲	資料閲覧画面において、拡大表示中であってもページ移動できること。			
⑳	資料閲覧画面において、任意のページ番号を指定して移動できること。			
㉑	資料閲覧画面において、閲覧中の資料から、同一会議内の他の資料に表示の切り替えができること。			
㉒	会議に登録した参加者情報をコピーすることにより、新たな会議で利用できること。			
㉓	参加者は、それぞれの端末上で個々にマーキングやメモを作成することができ、サーバ上に個別に保存できる機能を有すること。			
㉔	会議中に作成したマーキングやメモの情報は、会議終了後に会議主催者及び参加者がサーバからダウンロードして個々の端末に保存できる機能を有すること。			
㉕	すべての参加者又は一部の参加者が自ら操作することにより、システム上で発表者となることができる機能を有すること。			
㉖	発表者の端末上で表示した資料ページは、自動的に他の参加者の端末上に反映される機能を有すること。			
㉗	発表者の端末上でのポインタ操作やマーキング操作を行える機能を有し、その軌跡が参加者の端末上の資料にも表示される機能を有すること。			
㉘	会議参加者の誤操作等で発表者にならないよう、発表者になることに対して確認を求める画面を表示する機能を有すること。			
㉙	会議中に無線LAN等の影響を受けずに安定的に動作させるため、あらかじめ資料をタブレット型端末にダウンロードして会議進行することが可能な機能（オフライン動作モード）を有すること。			
㉚	オフライン動作モードで会議を開催する際には、次の機能は無効としてよい。 ・ログイン認証時の認証サービスとの連携 ・会議中の資料と参加者の登録、削除 ・発表機能			
㉛	会議資料を事前にダウンロードする際には、暗号化してタブレット型端末に保存すること。			
㉜	タブレット型端末にダウンロードした資料は、会議開催後一定時間内に自動的に消去されること。			
㉝	オフライン動作モードでの会議開催時にタブレット型端末に作成したメモは、事後ネットワークに再接続 したときにサーバ上に回収され、オンラインでの会議開催の場合と同様にサーバからダウンロードできること。			
ハードウェア要件				
①	ハードウェア要件は前項イ「ソフトウェア要件」を参照すること。			
9　プリントサービス				
(1) 概要				
	プリントサービスは、職員がLAN端末から任意の印刷機器を指定し印刷を行う「プリント機能」と、印刷機器からのプリントアウト時にICカードによる認証が必要な「認証プリント機能」を提供するサービスである。放置された資料からの情報漏えいを防ぐため、国家公務員身分証明証として用いる個人番号カード及びFeliCaカードによって認証することで、印刷できるようにする。プリントサービスは、全てのLAN複合機、LANプリンタで利用できるものとする。 具体的要件について、以下に記載する。			

別紙1－2　要件定義書（サービス・機器）

項番号	内容	提案内容	補足資料	記載箇所
(2) 構築要件				
ア　プリント機能				
①	別途調達のLAN複合機、LANプリンタ等を用いて、LAN端末からプリントサーバ経由で印刷物の出力を行える構成とすること。			
②	LAN端末からのプリント要求に対する応答時間を考慮してプリントサーバを構成すること。			
③	LAN複合機、LANプリンタ納入業者から受領したプリンタドライバ等の最新版を管理すること。			
④	主管課の指示に基づき、LAN複合機、LANプリンタをプリントサービスに登録すること。			
⑤	LAN端末のログオン時に職員の所属組織に基づいたLAN複合機・LANプリンタを割り当てること。また、主管課から指示に基づき、LAN複合機・LANプリンタを割り当てられること。			
⑥	ユーザがプリントサービスを利用した際の状況を調査できるようプリントログを出力すること。			
⑦	印刷日時、枚数、印刷指示を出した端末の情報等をプリントログとして3年以上保存すること。			
イ　認証プリント機能				
①	認証サービスと連携し、職員が使用している国家公務員身分証明証として用いる個人番号カード及びFeliCaカードを用いて個人認証を行うこと。			
②	ICカード情報の読み取りは、LAN複合機、LANプリンタに設置済みの既存ICカードリーダを利用すること。			
③	プリントサーバで個人認証を行わず、LAN複合機、LANプリンタから印刷物の出力を許可することも可能な構成とすること。			
④	サービスが稼働するサーバは、使用するLAN複合機、LANプリンタやドライバを管理する機能を保有すること。			
⑤	クライアントからの要求に対して、所定の応答性を確保できる台数のサーバを用意し、配置すること。			
⑥	LAN端末で特定の出力機器を指定せずに専用のプリンタドライバに対して印刷指示を行い、ICカードリーダ等によりユーザ認証を行ったLAN複合機、LANプリンタから印刷できる機能を有すること。また、この専用のプリンタドライバで、部数・片面/両面・ホッチキス等の指定が行えること。			
⑦	兼務者など一人の職員が複数のユーザアカウント名を利用している場合は、主務用のユーザアカウントで個人認証を行うこと。			
⑧	ディレクトリサーバ及びユーザ管理DBサーバとの通信が遮断された場合でも、プリント機能が利用できること。			
⑨	原則として、各拠点にプリントサーバを提供すること。ただし、回線帯域及びプリントサーバの性能に余剰を設ける等総務省LANサービスに影響を与えない場合は、プリントサーバを設置しない方法を認める場合もある。			
⑩	職員に対して、個人認証後に印刷物の出力を許可する構成とすること。			
⑪	LAN複合機利用者カードの新規発行を行える環境を構成すること。			
(3) 機器等要件				
ア　プリント機能				
ソフトウェア要件				
①	LAN端末へのプリンタドライバ自動更新に対応すること。			
②	ユーザがプリントサービスを利用した際の状況を調査できるようプリントログを出力すること。			
ハードウェア要件				
①	ハードウェア要件は、本要件定義書の第2－2 ストレージ機器を参照すること。			
イ　認証プリント機能				
ソフトウェア要件				
①	一定時間以上出力されなかったプリントジョブが自動的にキャンセルされる機能を有すること。			
②	出力機器のメーカに依存することなく利用できること。			
③	プリントジョブをLAN端末の操作で削除できる機能を有すること。			
④	LAN複合機においては、LAN複合機のパネル上の操作でプリントジョブを削除できること。			

項番号	内容	提案内容	補足資料	記載箇所
	⑤ LAN端末で特定の出力機器を指定せずに専用のプリンタドライバから印刷を実行し、ICカードリーダ等によりユーザ認証を行った出力機器から印刷できる機能を有すること。また、この専用のプリンタドライバで、部数・片面/両面・ホッチキス等の指定できること。出力機器のメーカに依存することなく利用できること。			
	⑥ LAN複合機のパネル上の操作で、部数、片面/両面、フィニッシャー（ホッチキス・パンチ等）の設定変更が行えること。また、複数ジョブを一括で同じ設定に変更指定が行えること。			
	⑦ カード認証後印刷できること。			
	⑧ LAN複合機・LANプリンタのプリント/コピー/スキャン等のログを3年間保持すること。			
	⑨ 本システムが稼働するために必要なWebサーバが稼働し、複合機制御用のWebサーバ機能を有すること。			
	⑩ 管理サーバ上のデータベースリカバリ用にバックアップファイルを格納すること。			
	⑪ 職員が使用している国家公務員身分証明証として用いる個人番号カードにより個人認証できること。なお、ICカードリーダは、既存の物を利用すること。			
	⑫ 既存のFeliCaカードを500枚と連携すること。必要に応じて、設定を行うこと。			
	⑬ ユーザが無断でプリンタドライバをインストールした場合でも、その出力機器からプリントができないように制御ができること。ただし、ユーザ認証を行わずプリントできる出力機器を指定できること。			
	⑭ ユーザ又はユーザのグループ別にプリント可能な出力機器を設定できること。			
	⑮ 複数メーカのLAN複合機のログを一元管理できる機能を有し、複数メーカのプリンタのログが同一システムで一元管理できること。複合機においては、コピー・スキャンのログも管理できること。また、このログを集計及び分析するレポート機能を有すること。取得するログはドキュメント名やユーザ名等を想定しているが、別途、主管課と協議の上、決定すること。			
	⑯ 削除されたカードを含めて、認証プリントサービスのデータベースと認証サービスとで同期すること。			
	⑰ LAN複合機でICカード認証されたユーザ毎のスキャン設定を統一管理できること。			
	⑱ スキャン設定は、複数メーカのLAN複合機パネル上で共通のスキャン操作ができること。			
	⑲ LAN複合機を入れ替えてもスキャンの設定データを引き継ぐことができること。			
	⑳ メーカー及び機種に依存することなく、個人単位のスキャン操作設定ができること。			
	ハードウェア要件			
	① LAN複合機数　670台、LANプリンタ数 330台、LAN端末数 7,000台、一日当たりの平均印刷枚数 650,000枚の処理に耐えられること。			
10　情報不正出力防止サービス				
（1）概要				
	情報不正出力防止サービスは、電磁的記憶媒体による総務省LAN外部への電子データ入出力を制限し、情報の不正出力を防止する環境を提供する。 ・職員は、総務省LAN外部から電磁的記憶媒体による電子データの受取りを行う場合は、ウイルスチェック用端末でウイルスチェックを行い、LAN端末に接続許可されたUSBデバイスを利用してLAN端末に電子データを移動する。 ・LAN端末では、電磁的記録媒体の制限をかけてあり、許可された電磁的記憶媒体しか利用できない。 具体的要件について、以下に記載する。			
（2）構築要件				
ア　情報不正出力防止機能				
	① 資源管理サービスと連携し、総務省LANに接続可能な外部記憶デバイスは官房企画課情報システム室所有のUSBメモリのみを可能とし、これ以外の外部記憶デバイスは利用できないようにすること。			
	② 官房企画課情報システム室所有のUSBメモリ1,300本及び別途調達のウイルスチェック用端末に対応すること。			
	③ ウィルスチェック用端末は、他の総務省機器とは別のドメインを利用すること。			
	④ ウイルスチェック用端末のマスタ作成、ウイルスチェック用端末のキッティングを行うこと。			
	⑤ ウイルスチェック用端末と総務省LANのネットワークを分離し、相互にアクセスはできない構成とすること。			

項番号	内容	提案内容	補足資料	記載箇所
	⑥ ウイルスチェック用端末のアンチウイルスパターンファイル及びセキュリティパッチは、総務省LANと連携し自動更新を行い、最新の状態を保つこと。			
	⑦ ウイルスチェック用端末は、端末起動時にキッティング終了時の初期状態に毎回戻すこと。			
	⑧ ウイルスチェック用端末は、セキュリティアップデート等一部の通信を除きインターネット、イントラネット等、端末以外の通信させないこと。			
	⑨ ウイルスチェック用端末は、ユーザアプリケーションのインストールを実行できない環境とすること。			
	⑩ ウイルスチェック用端末は、外部から持ち込まれたデータのウィルスチェックを自動的に実行すること。			
	⑪ ウイルスチェック用端末を集中管理するためのネットワークサービス（Active Directory、DNS等）を構築すること。			
	⑫ ウイルスチェック用端末の端末管理は、他のLAN端末と同等に管理できること			
	⑬ Windowsインストーラによるインストールを禁止すること。			
	⑭ ウイルスチェック用端末のハードディスクドライブへのユーザアカウントによる書き込みは、ユーザフォルダ以外禁止とすること。			
	⑮ 外部から持ち込むデータ、外部へ持ち出すデータの情報を1年以上保存すること。			
（3）機器等要件				
ア　情報不正出力防止機能				
ソフトウェア要件				
	① ウイルスチェック用端末は、端末起動時に初期状態に戻せること。			
	② ウイルスチェック用端末は、Word、Excel、PowerPoint、一太郎で作成したファイルとPDFを閲覧のみ可能なこと。			
	③ ウイルスチェック用端末は、インターネットへのアクセスするOS標準ツールがアンインストールできること。			
	④ ウイルスチェック用端末は、総務省LANへの接続を禁止できること。			
	⑤ ウイルスチェック用端末は、インターネットへ接続せずに、アップデートを行えること。			
ハードウェア要件				
	① ハードウェア要件は前項イ「ソフトウェア要件」を参照すること。			
11　機密情報保護サービス				
（1）概要				
	機密情報保護サービスは、LAN端末から機微度の高い情報の不正な閲覧を防止するために、ファイルを暗号化専用フォルダに移動することにより自動的に暗号化して保存し、事前に許可を得た職員のみが閲覧・編集・印刷等の機能を制御可能とするサービスである。 ・職員は、LAN端末上で作成したファイルを暗号化専用フォルダに移動することにより、ファイルを暗号化できる。 ・職員は、自身のアクセス権に基づき、暗号化されたファイルを「読込」「書込」「編集」「印刷」することができる。 具体的要件について、以下に記載する。			
（2）構築要件				
ア　機密情報保護機能				
	① ファイル共有サービスと連携し、250人の利用を想定し、組織用フォルダ内に利用権限ポリシー設定を行った暗号化専用フォルダを作成すること。			
	② Microsoft Office製品（Word、Excel、PowerPoint）について、「読込」「書込」「編集」「印刷」「コピー＆ペースト」の機能制限を可能とした上で、自動的に暗号化すること。			
	③ Adobe　PDFドキュメントを「読込」「印刷」の機能制限を可能とした上で、自動的に暗号化すること。			
	④ Microsoft　Office製品（Word、Excel、PowerPoint）、Adobe　PDFドキュメント以外のファイルを自動的に暗号化すること。			
	⑤ ファイルの格納時に、ファイルの暗号化が即時に開始される専用フォルダを提供すること。			

項番号	内容	提案内容	補足資料	記載箇所
	⑥ 暗号化は、「電子政府における調達のために参照すべき暗号のリスト（CRYPTREC暗号リスト）」にある電子政府推奨暗号リストに記載された方式以上の強度で行えること。			
	⑦ 暗号化、閲覧、復号は、認証サービスと連携し、利用者がパスワードの入力を行うことなくできること。			
	⑧ 総務省LANに接続していない状態では、暗号化したファイルの閲覧及び復号ができないこと。			
	⑨ 閲覧対象者の制限ができる構成とすること。			
	⑩ 暗号化ファイルに対するユーザの閲覧の成功と失敗に関するアクセス履歴を取得すること。			
	⑪ 暗号化ファイルへのアクセスログは、1年以上保存すること。			
（3）機器等要件				
ア　機密情報保護機能				
ソフトウェア要件				
	① Microsoft　Office製品（Word、Excel、PowerPoint）について、「読込」「書込」「編集」「印刷」「コピー＆ペースト」の機能制限を可能とした上で、自動的に暗号化できること。			
	② Adobe　PDFドキュメントを「読込」「印刷」の機能制限を可能とした上で、自動的に暗号化できること。			
	③ Microsoft　Office製品（Word、Excel、PowerPoint）、Adobe　PDFドキュメント以外のファイルを自動的に暗号化できること。			
	④ ファイルの格納時に、ファイルの暗号化が即時に開始される専用フォルダを提供すること。			
	⑤ 暗号化は、「電子政府における調達のために参照すべき暗号のリスト（CRYPTREC暗号リスト）」にある電子政府推奨暗号リストに記載された方式以上の強度で行えること。			
	⑥ 暗号化、閲覧、復号は、認証サービスと連携し、利用者がパスワードの入力を行うことなくできること。			
	⑦ 総務省外の環境では、暗号化ファイルの閲覧及び復号ができないこと。			
	⑧ 予め利用権限ポリシー設定を行った対象フォルダへ保存することで、自動的に暗号化される機能を有すること。また、ファイル単体を手動で暗号化できる機能を併せ持つこと。			
	⑨ 閲覧対象者の制限機能を有すること。			
	⑩ ファイルの格納するとともに、自動的に暗号化される専用フォルダへ準備すること。暗号化は、格納後即時に開始されること。			
	⑪ 暗号化ファイルに対するユーザの閲覧の成功と失敗に関するアクセス履歴が取得できること。			
	⑫ 暗号化ファイルへのアクセスログは、1年以上保管すること。			
	⑬ 暗号化ファイルは、適切な権限を有した利用者のみが利用できること。			
	⑭ 総務省LANに接続していない状態では、暗号化されたファイルの閲覧及び復号ができないよう構成すること。			
	⑮ 対象ユーザは250アカウントとする。			
ハードウェア要件				
	① ハードウェア要件は、本要件定義書の第2－2 ストレージ機器を参照すること。			

別紙1－2　要件定義書（サービス・機器）

項番号	内容	提案内容	補足資料	記載箇所
12　ディザスタリカバリサービス				
（1）概要				
	大規模災害発生等の有事の際においても総務省LANの主要サービスを提供し、業務継続性を確保するため、ディザスタリカバリサービスを提供する。 執務場所に参集できない場合は、テレワークサービスを利用して総務省LANの主要サービスを利用する。 ディザスタリカバリサービスで提供するサービスには、メールサービス、ポータルサイトサービス、ファイル共有サービス、認証サービス、テレワークサービス、コミュニケーションサービス、プリントサービス、ネットワークサービス、無線LAN接続サービス、システム監視機能が含まれる。 具体的要件について、以下に記載する。			
（2）構築要件				
	① ディザスタリカバリサービスには、メールサービス、ポータルサイトサービス、ファイル共有サービス、認証サービス、テレワークサービス、コミュニケーションサービス、プリントサービス、ネットワークサービス、無線LAN接続サービス、システム監視機能について、以下の要件を満たすよう構成すること。（本省での提供機能と比べ、一部縮退等有）			
	② 災害時においても、主管課からの連絡を受けられる窓口を準備すること。			
	③ 主管課から指示を受けてから、3時間以内に切替えを完了できること。			
	④ インターネット、総務省LAN内でsoumu.go.jpドメイン又はdr.soumu.go.jpドメインによるメールサービスを提供すること。			
	⑤ バックアップしたメールの閲覧が可能であること。			
	⑥ 災害時に利用する電子掲示板を準備すること。			
	⑦ 省、局、部、課、室、個人及び任意に指定された組織に対して、ファイル共有サービスを提供すること。			
	⑧ ログオンユーザの所属組織に応じたドライブマップを実現すること。			
	⑨ バックアップしたファイル共有（組織用）領域を読み取り可能な構成で提供すること。			
	⑩ ユーザは、通常時と同一のアカウントを利用した認証が可能であること。			
	⑪ 認証・アクセス権の管理が可能なこと。			
	⑫ 生体認証機能を提供すること。			
	⑬ 災害時用のテレワークサービスを提供すること。			
	⑭ 災害時用のコミュニケーションサービスを提供すること。			
	⑮ LAN端末がプリントサーバ経由でLANプリンタを利用できるようにすること（プリントサービス）。認証プリントサービスの導入は必須としない。			
	⑯ ネットワークサービスを提供すること。			
	⑰ 被災拠点を除いた拠点で、無線LANサービスを継続利用できること。			
	⑱ ディザスタリカバリサービスを構成する各機器の死活監視、障害監視ができること。			
	⑲ LAN端末では、リモートアクセス機能での総務省LANへのアクセス環境を提供すること。			
	⑳ タブレット型端末、個人所有端末は、デスクトップ仮想化機能で総務省LANへのアクセス環境を提供すること。			
（3）機器等要件				
ア　メール送受信機能				
ソフトウェア要件				
	① 規模・性能要件に記載したメール流量を処理可能となるよう構成すること。			
	② 2万人以上の規模において稼働実績があること。			
	③ SMTPによるメール配送機能を有すること。			
	④ 人事異動における他省庁への出向を考慮し、受信したメールを他ドメイン向けに自動転送する機能を有すること。			
	⑤ メール配送ログの取得が可能なこと。			

別紙1－2　要件定義書（サービス・機器）

項番号	内容	提案内容	補足資料	記載箇所
	⑥ メール送受信数、メール送受信容量（KB）は、一定間隔で集計やドメイン別のランキング等のレポーティングが可能なこと。			
	⑦ メールの平均サイズや添付ファイルの平均サイズのレポーティングが可能なこと。			
	⑧ メール中継のプロセス数、キュー数やディレクトリの空き容量等の稼働状況を収集し、レポーティングが可能なこと。			
	ハードウェア要件			
	① ハードウェア要件は、本要件定義書の第2－2 ストレージ機器を参照すること。			
イ インターネットメール中継機能				
	ソフトウェア要件			
	① 規模・性能要件に記載したメール流量を処理可能となるよう構成すること。			
	② 2万人以上の規模において稼働実績があること。			
	③ SMTPによるメール配送機能を有すること。			
	④ メール配送ログの取得が可能なこと。			
	⑤ メール送受信数、メール送受信容量（KB）は一定間隔における集計やドメイン別のランキング等のレポーティングが可能なこと。			
	⑥ メール中継のプロセス数、キュー数やディレクトリの空き容量等の稼働状況をレポーティングが可能なこと。			
	ハードウェア要件			
	① ハードウェア要件は、本要件定義書の第2－2 ストレージ機器を参照すること。			
ウ メールストア機能				
	ソフトウェア要件			
	① ユーザ1人当たり最低10GB以上のメールボックスの利用が可能であること。			
	② 2万人以上の規模において稼働実績があること。			
	③ ユーザごとにメールボックスの容量制限が可能なこと。			
	④ ユーザのメールボックスが制限値を超過した場合、警告メール等の通知が可能なこと。			
	⑤ メールクライアントでのメール受信時に、ID/パスワードによる利用者認証を行うこと。			
	⑥ メールクライアントとのメール受信プロトコルは、IMAP4を使用すること。			
	⑦ 認証サービスとアカウント連携が可能なこと。			
	⑧ 通信経路が暗号化されていること。			
	ハードウェア要件			
	① ハードウェア要件は、本要件定義書の第2－2 ストレージ機器を参照すること。			
エ 省内ポータル機能				
	ソフトウェア要件			
	① 総務省のイントラネットホームページサービスを提供し、Webブラウザ起動時の初期画面として表示が可能なこと。			
	② デザインやコンテンツを更新する機能を有すること。			
	ハードウェア要件			
	① ハードウェア要件は、本要件定義書の第2－2 ストレージ機器を参照すること。			
オ グループウェア機能				
	ソフトウェア要件			
	① 複数の階層構造の掲示板機能を提供すること。組織階層構造に合わせて階層的に作成できること。			
	② それぞれの掲示板には、適切なアクセス権の設定が可能なこと。			
	③ 電子掲示板はユーザ自身が記事掲載期間を指定でき、情報の登録・修正・削除が可能なこと。			

別紙1－2　要件定義書（サービス・機器）

項番号	内容	提案内容	補足資料	記載箇所
	④ 掲載期間が経過した電子掲示板の情報は、他のユーザからは見えなくなり、ユーザの設定により参照が可能なこと。			
	⑤ 電子会議室は、特定のグループ内での議論（電子会議）ができるよう、適切なアクセス権が設定が可能なこと。			
	⑥ 電子会議室は、管理者が承認した議題のみを公開できる機能を有すること。			
	⑦ 設備予約ができる期間と予約可能な最大時間の設定が可能なこと。			
	⑧ それぞれの設備に対して、予約可能な組織グループ割り当てが可能なこと。			
	⑨ 特定のユーザ又は全体に対して、アンケートを発行する機能を有すること。			
	⑩ アンケートは、無記名での回答が可能なこと。			
	⑪ アンケートの回収期限が設定が可能なこと。			
	⑫ アンケートの発行者がアンケートの結果確認、集計を行う機能及びCSV形式等でダウンロードできる機能を有すること。			
	⑬ ToDoリスト機能と連携して、ユーザが各自のToDoの登録、変更、削除、状況の参照を行う機能を有すること。			
	⑭ スケジュールは、省・局・部・課・室・個人に対して提供し、組織階層構造に準拠した表示を実現すること。			
	⑮ 幹部職員等のスケジュール情報に対して、代理入力ができるように特定ユーザ（秘書等）にアクセス権の付与が可能なこと。			
	ハードウェア要件			
	① ハードウェア要件は、本要件定義書の第2－2 ストレージ機器を参照すること。			
カ ファイル共有機能				
	ソフトウェア要件			
	① 組織ファイル共有（組織用）機能を利用できること。			
	② 各フォルダに対して、アクセス権の設定が可能であること。また、アクセス権限は、認証サービスと連携できること。			
	③ 各共有フォルダに対して容量制限が行えること。			
	④ Windows及びLinuxからのファイル共有が可能であること。			
	⑤ 組織領域として、26GB/人以上の領域を確保した構成とすること。			
	⑥ 容量超過時にメール通知が可能であること。			
	⑦ 十分なスナップショット領域を確保し、90世代管理可能であること。			
	⑧ スナップショット領域は、ユーザの閲覧可否の設定が可能であること。			
	⑨ データ領域の効率的利用を目的とし、LAN端末がアクセスする領域に対して、ブロックレベルの重複排除機能を実装すること。			
	ハードウェア要件			
	① ハードウェア要件は、本要件定義書の第2－2 ストレージ機器を参照すること。			
キ ディレクトリ機能				
	ソフトウェア要件			
	① LAN端末から総務省LANにアクセスする際のユーザ単位での認証を提供すること。			
	② ユーザアカウントは、組織ごとの階層管理を行えること。			
	③ ユーザアカウントをまとめてグループとして管理が可能であること。			
	④ LAN端末から総務省LANにアクセスする際に、ユーザとグループ単位でのアクセス管理可能であること。			
	⑤ ユーザ認証の履歴の記録、管理が可能であること。			
	⑥ 特定のグループにのみ個別のパスワードルールを適応できること。			
	ハードウェア要件			
	① ハードウェア要件は、本要件定義書の第2－2 ストレージ機器を参照すること。			

別紙1－2　要件定義書（サービス・機器）

項番号	内容	提案内容	補足資料	記載箇所
ク	生体認証機能			
	ソフトウェア要件			
①	生体情報による認証により、ログオン認証、スクリーンセーバロック解除、及びアプリケーションログオン等の認証ができること。			
②	生体情報は、暗号化され集中管理されていること。			
③	生体情報の登録・削除・変更機能を有すること。			
④	利用者ログ及び管理者ログを取得することが可能であること。			
⑤	生体認証が行えない場合、一時的にID、パスワードによる代替認証も可能であること。			
	ハードウェア要件			
①	ハードウェア要件は、本要件定義書の第2－2 ストレージ機器を参照すること。			
ケ	リモートアクセス機能			
	ソフトウェア要件			
①	総務省LANへの接続の際に、端末のOSパッチの適用状況、ウイルスチェックソフトのパターン更新状況、端末の固有情報等をチェックし、条件を満たさない場合は総務省LAN内部ネットワークへ接続できないこと。			
②	LAN端末から外部ネットワークを経由して、総務省LANの各種サービス（メール、ファイル共有、Web接続、コミュニケーションサービス、オフィス製品の利用）を提供 すること。			
③	内部のメールサービスが利用できること。			
④	システム管理用インターフェースとして、CLI及びGUIを提供すること。			
⑤	接続時の認証、通信路の暗号化、接続記録の保持等十分なセキュリティ対策を施すこと。			
⑥	認証方式として、ワンタイムパスワード又は生体認証が行えること。			
⑦	リモートアクセス経由でアクセス可能なネットワーク及び使用可能なアプリケーションを限定する機能を有すること。			
⑧	利用できるサービスは、ポリシーによる制御を実現すること。			
	ハードウェア要件			
①	最大接続数が500以上に耐える構成とすること。			
②	有線LAN及び無線LANに接続したLAN端末から、リモートアクセス機能が利用可能なこと。			
コ	デスクトップ仮想化機能			
	ソフトウェア要件			
①	個人所有端末から外部ネットワークを経由して、総務省LANの各種サービス（メール、ファイル共有、Web接続、コミュニケーションサービス、オフィス製品の利用）を提供すること。			
②	内部のメールサービスが利用できること。			
③	システム管理用インターフェースとして、CLI及びGUIを提供すること。			
④	認証方式として、ワンタイムパスワード又は生体認証が行えること。			
⑤	利用できるサービスは、ポリシーによる制御を実現すること。			
⑥	シンクライアントは、転送された画面上で操作が可能なリモートデスクトップ接続機能を有すること。			
⑦	総務省LANで管理しているアカウントと連携して、VPN接続が可能なこと。			
⑧	OSの起動時にはパスワード認証が必要となる設定が可能であること。			
⑨	パスワードを設定回数以上間違えると自動的にパスワードがロックされる機能を有すること。			
⑩	シンクライアントデバイスに保存される情報は、総務省LANとの接続に必要な設定等に限定され、任意のデータの記録ができないこと。			
⑪	総務省外から外部接続環境に接続する際には、通信を暗号化したVPN接続を行うこと。			
⑫	事前に許可された端末のみ、本環境への接続を許可すること。			

別紙1－2　要件定義書（サービス・機器）

項番号	内容	提案内容	補足資料	記載箇所
	⑬ ユーザ認証においては、ユーザID、パスワードに加え、ワンタイムパスワード等のセキュリティ強化の施策を導入すること。			
	⑭ ユーザID及びパスワードは通常使用しているアカウントとし、総務省LANと同期できること。			
	⑮ 総務省LANサービス（メール、インターネット、掲示板、ファイルサービス等）が利用できること。			
	⑯ ICA、PCoIP等の画面転送プロトコルに対応していること。			
	ハードウェア要件			
	① ハードウェア要件は、本要件定義書の第2－1サーバ機器及び第2－2 ストレージ機器を参照すること。			
	② 最大接続数300以上に耐えられる構成とすること。			
	③ シンクライアント専用OSが入った媒体は、ディザスタリカバリサービス用に200個準備すること。			
	④ シンクライアントデバイスは、総務省LANとの接続に必要な機能に限定された専用のOSが搭載されていること。			
	⑤ 紛失時の情報漏えいを防止するため、シンクライアントデバイスの記憶領域は暗号化されていること。			
サ	メッセージ交換機能			
	ソフトウェア要件			
	① リアルタイムに文字ベースでユーザ間で会話できる機能を有すること。			
	② 在席管理機能を利用して、連絡可能なユーザとの会話を容易に開始できること。			
	③ 在席管理機能を利用して、ユーザを会話に招待することができること。			
	④ 在席管理機能を利用して、複数のユーザと会話することができること。			
	⑤ 会話中の相手にファイルを送信することができること。			
	⑥ サーバにメッセージの記録が残せること。			
	ハードウェア要件			
	① ハードウェア要件は、本要件定義書の第2－2 ストレージ機器を参照すること。			
シ	在席管理機能			
	ソフトウェア要件			
	① 連絡先ユーザが連絡可能な状態にあるか把握することができる機能を有すること。			
	② アイコンと文字の情報を使って、視覚的にわかりやすく表示されること。			
	③ ユーザの状態は、「連絡可能」、「取り込み中」、「応答不可」、「一時退席中」、「業務時間外」等、状況を的確に反映できる数種類以上の表示が可能であること。			
	④ ユーザの状態は、PCの稼働状態やユーザの操作状況から自動的に変化させることができること。			
	⑤ ユーザの状態は、手動で変更することも可能であること。			
	⑥ 在席表示されているユーザをクリックすることで、メッセージ交換サービスを起動できること。			
	⑦ 頻繁に連絡をとるユーザ等をひとまとめにして情報共有しやすくするために、グループを作成する機能を有すること。			
	ハードウェア要件			
	① ハードウェア要件は、本要件定義書の第2－2 ストレージ機器を参照すること。			
ス	Web 会議機能			
	ソフトウェア要件			
	① カメラとマイクを追加することにより、Web会議を開催できる機能を有すること。			
	② 在席表示されているユーザをクリックすることで、Web会議サービスを起動できること。			
	③ 会議参加者全員が閲覧、書き込みが行えるホワイトボード機能を有すること。			
	④ 会議参加者全員がファイルを展開、共有、閲覧する機能を有すること。			
	⑤ 会議画面解像度は最大1920×1080（ピクセル）であること。			
	⑥ 会議開催中にメッセージ交換サービスが利用できること。			
	⑦ 会議開催中に参加者間で資料の受け渡しが可能なこと。			

別紙1－2　要件定義書（サービス・機器）

項番号	内容	提案内容	補足資料	記載箇所
	⑧ ブラウザ（Internet Explorer及びFirefox）から会議室の予約が可能であること。			
	⑨ 会議開催中にメッセージ交換機能が利用できること。			
	⑩ 会議開催中に参加者間で資料の受け渡しができること。			
	⑪ すべてのユーザに会議を主催できる個別のIDを付与できること。			
	⑫ 会議の開催及びメンバの指定・招集等を実施できること。			
	⑬ 利用状況のログを月ごとに取得できること。			
	ハードウェア要件			
	① ハードウェア要件は、本要件定義書の第2－2 ストレージ機器を参照すること。			
セ	プリント機能			
	ソフトウェア要件			
	① LAN端末からの印刷要求に対して、印刷処理を行えること。			
	② LAN端末へのプリンタドライバ自動更新に対応すること。			
	③ ユーザがプリントサービスを利用した際の状況を調査できるようプリントログを出力すること。			
	ハードウェア要件			
	① ハードウェア要件は、本要件定義書の第2－2 ストレージ機器を参照すること。			
ソ	DNS 機能			
	ソフトウェア要件			
	① 大規模災害発生時において、総務省LANの機器に関するホスト名とIPアドレスの名前解決を行うこと。			
	② 内部とDMZにDNSサービスを提供し、本省と同じ構成をとること。			
	③ 総務省LANの機器に関するホスト名とIPアドレスの名前解決を行うこと。			
	④ DHCP機能と連携し、DNS情報の動的更新を行うこと。			
	⑤ インターネット上の公開DNSと通信し、総務省ドメイン以外のドメインの名前解決を行うこと。			
	⑥ 内部からの問い合わせと外部からの問い合わせを区別し、対応する情報も分離して管理すること。			
	⑦ SPFに対応できること。			
	⑧ 本省のDNSサービスと連携し、ホスト名、IPアドレスを統合管理すること。			
	⑨ 大規模災害発生時、本省においてDNSサービスが提供できない場合、ディザスタリカバリサイトのDNSサービスに切り替わること。			
	⑩ DNS問い合わせ及びゾーン転送を許可するIPアドレス範囲を指定できること。			
	⑪ 本省にある全省DNSサービスにDNS情報を複製すること。			
	ハードウェア要件			
	① 100BASE-TX/1000BASE-Tのポートを2ポート以上有すること。			
	② DNSの問い合わせ性能として、24,000qps以上有すること。			
タ	DHCP 機能			
	ソフトウェア要件			
	① 大規模災害発生時において、LAN端末に対して、IPアドレス、ネットワーク情報（デフォルトゲートウェイ、サブネットマスク、ドメイン名、DNSサービスのIPアドレス）の自動割り当てを行うこと。			
	② IPアドレスの割り当て期間を制御できること。			
	③ IPアドレスの割り当てる範囲を指定できること。			
	④ DHCPの利用状況（日時、IPアドレス、MACアドレス、コンピュータ名等）を記録すること。			
	⑤ セキュリティ及び証跡管理を考慮して、特定端末などにDHCP環境でも特定のIPアドレスを割り当てることができること。			
	⑥ 端末のMACアドレスによって、DHCPでのIPアドレス割り当てを許可するかどうか設定する機能を有すること。			
	⑦ MACアドレスを登録し、登録されたMACのみに特定のDHCPレンジからIPアドレスを払いだせること。			
	⑧ システム管理用インターフェースとして、WebベースのGUIを提供すること。			

別紙1－2　要件定義書（サービス・機器）

項番号	内容	提案内容	補足資料	記載箇所
	⑨ クライアントに割り当てるデフォルトルータ、ブロードキャストアドレス、サブネットマスク、リース時間をDHCPレンジごとに指定できること。			
	⑩ 本省の全省DHCPサービスと併せて一元管理すること。			
	⑪ 大規模災害発生時において、リース情報を本省から引き継げること。			
	ハードウェア要件			
	① 100BASE-TX/1000BASE-Tのポートを2ポート以上有すること。			
	② DHCP性能として、150lease/sec以上有すること。			
チ NTP 機能				
	ソフトウェア要件			
	① 大規模災害発生時において、時刻を同期させる機能を有すること。			
	② 総務省LANに接続された機器に対して、NTPによる時刻提供サービス機能を有すること。			
	③ NTPの利用状況（設定日時、上位NTPサービスのIPアドレス、オフセット時間）の記録機能を有すること。			
	④ LAN端末、サーバ、ネットワーク機器等からの時刻同期において、適切な構成をとること。			
	ハードウェア要件			
	① 特に規定しない。			
ツ プロキシ機能				
	ソフトウェア要件			
	① 大規模災害発生時において、プロキシサービスを提供できること。			
	② 内部とDMZにプロキシサービスを提供し、本省と同じ構成をとること。			
	③ HTMLコンテンツや画像データ等のWebコンテンツのキャッシュ機能を有すること。			
	④ 利用状況（アクセス元LAN端末等のIPアドレス、アクセス先URL等、アクセス制御（許可、拒否）、日時）の記録機能を有すること。			
	⑤ 連携したサービスにより、Webアンチウイルスを実現すること。			
	⑥ IPv4、IPv6のデュアルスタックに対応すること。			
	⑦ Web画面上でプロキシの統計情報の閲覧できる機能を有すること。			
	⑧ NTLM、LDAP、Active Directory、RADIUS等と連携した認証が可能であること。			
	⑨ 通過プロトコルとして、HTTP、HTTPS、FTPに対応すること。			
	⑩ システム管理用インターフェースとして、WebベースのGUIを提供すること。			
	⑪ イベントログをSyslogや電子メールで転送する仕組みを有すること。			
	ハードウェア要件			
	① 100BASE-TX/1000BASE-Tのポートを2ポート以上有すること。			
テ メールウイルス対策機能				
	ソフトウェア要件			
	① ウイルスやスパイウェアといった電子メールを介して、ネットワークから侵入する不正プログラムを隔離又は削除できること。			
	② 添付ファイル、メッセージ本文を含むメッセージからウイルスを検出し、駆除できること。			
	③ システム管理用インターフェースとして、Webベース等のGUIを利用できること。			
	④ 圧縮されたファイルを自動解凍して、ウイルスを検出できること。			
	⑤ ウイルス対策結果のログが記録できること。			
	⑥ ウイルスメールと判定されたメールの件数や検知されたウイルスの情報を収集し、ランキング表示等の表示が可能であること。			
	ハードウェア要件			
	① 特に規定しない。			

別紙1－2　要件定義書（サービス・機器）

項番号	内容	提案内容	補足資料	記載箇所
ト	メール検索機能			
	ソフトウェア要件			
	① 宛先、送信元IPアドレス、件名、本文で送信メールの検索ができること。			
	② 添付ファイルメールの件数や添付ファイルのタイプの情報を収集し、ランキング形式でレポーティング可能であること。			
	ハードウェア要件			
	① 特に規定しない。			
ナ	迷惑メール対策機能			
	ソフトウェア要件			
	① イメージスパムやPDFスパム、日本語スパムに対応していること。			
	② IPアドレス、メールアドレス、ドメインで迷惑メールの判定が可能であること。			
	③ 件名、本文内のキーワードで迷惑メールの判定が可能であること。			
	④ 迷惑メールの判定結果によって排除、隔離が可能であること。			
	⑤ 迷惑メールと判定されたメールの送信元や受信数の情報を収集し、ランキング形式でレポーティング可能であること。			
	⑥ 省内に侵入する迷惑メールの量を大幅に削減するため、迷惑メール送信元のIPアドレスをブロックするための仕組みに対応すること。			
	⑦ DoS攻撃やDHAへの対応を考慮していること。			
	⑧ スパム判定エンジンによる迷惑メールの判定は、内容や言語ではなく、フィンガープリント解析やスパムらしさ判定等迷惑メール特有の特徴を基に行うこと。			
	⑨ SPF及びDKIMがサポートされていること。			
	⑩ 2万人以上の規模において稼働実績があること。			
	⑪ フリーメール等受信時に当該メールに注意喚起メッセージを挿入できること。			
	ハードウェア要件			
	① 特に規定しない。			
ニ	インターネットウイルス対策機能			
	ソフトウェア要件			
	① ハードウェア要件を参照すること。			
	ハードウェア要件			
	① インターネット接続セグメントとサーバセグメントに製造業者の異なる2段階ウイルス対策サーバ又はウイルスゲートウェイを設置すること。			
	② ディザスタリカバリサイトサーバセグメントにおいて、ICAPによる連携等プロキシサービスと連携したウイルス対策に対応すること。			
	③ 受信トラフィックと送信トラフィックの両方を分析するように設定できること。			
	④ ウイルス検出時は、削除、通知ができること。			
	⑤ 最新のウイルスのパターンファイルを自動的にダウンロードし、更新できること。			
	⑥ 監視対象のプロトコルはFTP、HTTP、HTTPSとする。			
	⑦ システム管理用インターフェースとして、Webベース等のGUIを提供すること。			
	⑧ ネットワークパフォーマンスを低下させることなく、転送ファイル、Webトラフィックからのウイルスやワーム、スパイウェア等に対して防御できること。			
	⑨ 100BASE-TX/1000BASE-Tのポートを4ポート以上有すること。			
	⑩ アンチウイルススループットは、500Mbps以上であること。			

別紙1－2　要件定義書（サービス・機器）

項番号	内容	提案内容	補足資料	記載箇所
ヌ	Web ウイルス対策機能			
	ソフトウェア要件			
	① ハードウェア要件を参照すること。			
	ハードウェア要件			
	① プロキシキャッシュと連携し、ウイルススキャンの最適化が可能であること。			
	② 15分おきのパターンファイル・アップデートで、常に最新の脅威を防御できること。			
	③ ファイルサイズやコンテンツタイプの制限に加え、拡張子による許可、拒否リストが適用可能であること。			
	④ Webベース等のGUIで設定が可能であること。			
	⑤ 100BASE-TX/1000BASE-Tのポートを2ポート以上有すること。			
	⑥ プロキシサービスと連携することで、高速なウイルススキャンが実現可能であること。			
ネ	無線LAN管理機能			
	ソフトウェア要件			
	① 最大で1000のアクセスポイントの管理が可能であること。			
	② 電子政府推奨暗号に対応していること。			
	③ RADIUS認証/アカウンティング機能を有すること。			
	④ 管理インターフェースとして、HTTPS、SSH、シリアル接続が可能であること。			
	⑤ 外部LDAPサーバとの認証連携が可能であること。			
	⑥ コントローラによる構成定義の一元管理を行えること。			
	⑦ アクセスポイントとコントローラ間の通信を暗号化する機能を有すること。			
	⑧ 不正なアクセスポイントを検出する機能を有すること。			
	⑨ アクセスポイントは、コントローラによる、チャネル、電波強度、セキュリティ設定等の制御が可能であること。			
	⑩ 電波干渉源監視のための専用機器を必要としないこと。			
	ハードウェア要件			
	① ボックス型筐体であること。			
	② 10Gbpsのポートを4ポート以上有すること。			
	③ 電源部の冗長化が可能であること。			
ノ	システム監視機能			
	ソフトウェア要件			
	① サーバ、ネットワーク機器、アプライアンス機器を含めたシステム稼働状況（死活監視、イベント監視等）を監視する機能を実装すること。			
	② ハードウェア、ソフトウェア、アプリケーションプログラムのプロセス及びサービスも監視すること。			
	③ イベント発生時に、メール自動発信等複数の方法で運用員に対して通知可能であること。			
	④ 監視機器が追加になる場合においても、既に導入済みの機器と同様にメッセージ通知や性能の監視ができるように、ポリシーテンプレートの配布が可能であること。			
	⑤ 管理GUI上で異常が発生したサーバを特定可能であること。また、その画面からハードウェア管理ツール等を起動可能であること。			
	⑥ OS異常時、サーバ停止時でもメール、トラップ通知が可能であること。			
	ハードウェア要件			
	① ハードウェア要件は、本要件定義書の第2－2 ストレージ機器を参照すること。			

別紙1－2　要件定義書（サービス・機器）

項番号	内容	提案内容	補足資料	記載箇所
第4　セキュリティサービス				
1　マルウェア対策（メール）サービス				
（1）概要				
	メールを侵入経路とするマルウェア等の侵入を早期に検知・駆除するため、マルウェア対策（メール）サービスを提供する。インターネット及び政府共通ネットワークと本省間のメール通信のマルウェア検査・検知を行う。インターネットと本省間のメール通信に対しては、振る舞い検知型のマルウェア検査を行う。迷惑メール判定を行い、迷惑メールを防御する。ドメイン認証やレピュテーション情報を用いて、不審なメールから防御する。 具体的要件について、以下に記載する。			
（2）構築要件				
	① インターネット経由で送られてくる迷惑メールを件名・送信元アドレス等の条件により判定し、隔離、削除又は当該メールへの注意喚起文の挿入を実施すること。			
	② Webブラウザ等を用い、迷惑メールとして隔離されたメールを確認・操作できる構成とすること。			
	③ インターネット経由で送られてくるウイルスメールは、ユーザのメールボックスで受信する前に検知・駆除すること。			
	④ 総務省LANで送受信されるメールは、すべてマルウェア検査される構成とすること。ただし、インターネット経由で送受信するメールは、異なるベンダの製品により多段でマルウェア検査を実施すること。			
	⑤ インターネット経由で送受信するメールに対しては、振る舞い型のマルウェア検査を行い、検知時は当該メールを隔離又は削除するよう構成すること。			
	⑥ インターネット経由で受信したメールは、ドメインによる認証を実施すること。			
	⑦ 職員が主として利用するメールクライアントには、職員が不審メールを受信した際に、運用員にその旨を通知するためのしくみを構成すること。			
	⑧ マルウェア判定された場合は、運用員に通知するよう構成すること。			
	⑨ インターネット経由で送られてくるメールの送信元IPアドレスを評価（レピュテーション）すること。また、判定結果に応じて、メールの受信動作の制御を実施すること。			
	⑩ 圧縮された添付ファイルを自動解凍し、ウイルスを検知すること。			
（3）機器等要件				
ア　メールウイルス対策機能				
ソフトウェア要件				
	① ウイルスやスパイウェアといった電子メールを介して、ネットワークから侵入する不正プログラムを隔離又は削除できること。			
	② 添付ファイル、メッセージ本文を含むメッセージからウイルスを検出し、駆除できること。			
	③ システム管理用インターフェースとして、Web ベース等の GUI を利用できること。			
	④ 圧縮されたファイルを自動解凍して、ウイルスを検出できること。			
	⑤ ウイルス対策結果のログが記録できること。			
	⑥ ウイルスメールと判定されたメールの件数や検知されたウイルスの情報を収集し、ランキング表示等の表示が可能であること。			
ハードウェア要件				
	① 特に規定しない。			
イ　メール検索機能				
ソフトウェア要件				
	① 宛先、送信元IPアドレス、件名、本文で送信メールの検索ができること。			
	② 添付ファイルメールの件数や添付ファイルのタイプの情報を収集し、ランキング形式でレポーティング可能であること。			

別紙1－2　要件定義書（サービス・機器）

項番号	内容	提案内容	補足資料	記載箇所
	ハードウェア要件			
	① 特に規定しない。			
ウ	迷惑メール対策機能			
	ソフトウェア要件			
	① イメージスパムやPDFスパム、日本語スパムに対応していること。			
	② IPアドレス、メールアドレス、ドメインで迷惑メールの判定が可能であること。			
	③ 件名、本文内のキーワードで迷惑メールの判定が可能であること。			
	④ 迷惑メールの判定結果によって排除、隔離が可能であること。			
	⑤ 迷惑メールと判定されたメールの送信元や受信数の情報を収集し、ランキング形式でレポーティング可能であること。			
	⑥ 省内に侵入する迷惑メールの量を大幅に削減するため、迷惑メール送信元のIPアドレスをブロックするための仕組みに対応すること。			
	⑦ DoS攻撃やDHAへの対応を考慮していること。			
	⑧ スパム判定エンジンによる迷惑メールの判定は、内容や言語ではなくフィンガープリント解析やスパムらしさ判定等、迷惑メール特有の特徴を基に行うこと。			
	⑨ SPF及びDKIMがサポートされていること。			
	⑩ 2万人以上の規模において稼働実績があること。			
	⑪ フリーメール等受信時に当該メールに注意喚起メッセージを挿入できること。			
	ハードウェア要件			
	① 特に規定しない。			
エ	不審メール通報機能			
	ソフトウェア要件			
	① メールクライアントから直接操作し、通報できること。			
	② 通報先として任意のメールアドレスを設定できること。			
	ハードウェア要件			
	① 特に規定しない。			
オ	標的型攻撃対策（メール）機能			
	メールマルウェア検出装置			
	ソフトウェア要件			
	① ハードウェア要件を参照すること。			
	ハードウェア要件			
	① 100BASE-TX/1000BASE-Tの検査用ポートを2つ以上持つこと、また、100BASE-TX/1000BASE-Tの管理用ポートを2つ以上持つこと。			
	② 1日あたり平均750,000通のメールの添付ファイルを検査可能であること。			
	③ アプライアンス内の仮想化環境で添付ファイルの動作の解析が可能であること。			
	④ 添付ファイルは、exe、dll、pdf、Office、swf、RealPlayer のファイル形式を解析可能であること。			
	⑤ C&Cサーバ定義情報により、メールに記載されているURLがマルウェア配布サイトであるかの検知が行えること。			
	⑥ 検知したマルウェアを解析し、接続しうるC&Cサーバの情報を取得できること。			
	⑦ 総務省ＬＡＮ上の端末がEmail経由のマルウェアに感染したこと又は感染した疑いがあることを検知できること。			
	⑧ マルウェアの検知状況やコールバック先などのレポートを作成する機能を有すること。			
	⑨ C&Cサーバ定義情報をインターネット経由で自動及び手動の両方で更新できること。			
	⑩ ディスクはRAID1で冗長化すること。			

別紙1－2　要件定義書（サービス・機器）

項番号	内容	提案内容	補足資料	記載箇所
2　マルウェア対策（インターネット・Web）サービス				
（1）概要				
	インターネット及び政府共通ネットワークを経由したWeb閲覧を侵入経路とするマルウェアの侵入を早期に検知・駆除するため、マルウェア対策（インターネット・Web）サービスを提供する。インターネット及び政府共通ネットワークと本省間のWeb通信のマルウェア検査・検知を行う。インターネットと本省間のWeb通信に対しては、振る舞い検知型のマルウェア検査を行う。レピュテーション情報等を用いて、不審なWebサイトへのアクセスを防止する。 具体的要件について、以下に記載する。			
（2）構築要件				
	① インターネット経由及び政府共通ネットワーク経由のWebアクセスのマルウェア検査を実施すること。			
	② インターネット経由及び政府共通ネットワークのWebアクセスに対しては、異なるベンダの製品により多段でマルウェア検査を実施すること。			
	③ 業務に無関係なサイトや悪意あるサイトへのアクセスをブロックすること。ブロック対象のサイトを設定・変更できるインターフェースを提供すること。			
	④ レピュテーション情報を用いて、不審サイトへのアクセスをブロックすること。			
	⑤ マルウェア判定された場合、又は、悪意あるサイトへのアクセスがあった場合は、必要に応じて運用員に通知するよう構成すること。			
	⑥ Webアクセス時に認証サービスと連携して、ユーザ認証するよう構成すること。			
	⑦ SSL通信（個別業務システム含む）については、デコードしたうえでマルウェア検査を実施すること。			
	⑧ インターネット経由でのWebアクセスに対しては、振る舞い型のマルウェア検査を実施すること。また、マルウェア検知されたアクセス先への次回以降のアクセスを、一定期間ブロックすること。			
（3）機器等要件				
ア　インターネットウイルス対策機能				
ソフトウェア要件				
	① ハードウェア要件を参照すること。			
ハードウェア要件				
	① 転送ファイル、Webアクセスからのスパイウェア、ウイルス等に対しての防御が可能であること。			
	② ウイルスを確認するポート（管理用ポートを除く）は、IPアドレスを割り振る必要なく接続できること。			
	③ 特定のファイルのダウンロード、アップロードが制限可能であること。			
	④ WebベースのGUIで設定が可能であること。			
	⑤ 受信トラフィックと送信トラフィックの両方を分析するように設定できること。			
	⑥ ウイルス検出時は、削除、通知ができること。			
	⑦ 最新のウイルスのパターンファイルを自動的にダウンロードし、更新できること。			
	⑧ 複数の通信プロトコルにおいて、ウイルス対策が可能であること。			
	⑨ システム管理用インターフェースとして、Webベース等のGUIを提供すること。			
	⑩ 100BASE-TX/1000BASE-Tのポートを4ポート以上有すること。			
	⑪ アンチウイルススループットは、500Mbps以上であること。			
イ　Web ウイルス対策機能				
ソフトウェア要件				
	① ハードウェア要件を参照すること。			
ハードウェア要件				
	① プロキシキャッシュと連携し、ウイルススキャンの最適化が可能であること。			
	② 15分おきのパターンファイル・アップデートで、常に最新の脅威を防御できること。			
	③ ファイルサイズやコンテンツタイプの制限に加え、拡張子による許可、拒否リストが適用可能であること。			
	④ Webベース等のGUIで設定が可能であること。			

別紙1－2　要件定義書（サービス・機器）

項番号	内容	提案内容	補足資料	記載箇所
	⑤ 100BASE-TX/1000BASE-Tのポートを2ポート以上有すること。			
	⑥ プロキシサービスと連携することで、高速なウイルススキャンが実現可能であること。			
ウ Webコンテンツフィルタリング機能				
ソフトウェア要件				
	① 業務に無関係なサイトや悪意あるサイトへのアクセスをブロック、許可、警告する機能を有すること。また、この設定はカテゴリごとに可能であること。			
	② 部や課等の単位でグループが設定可能であり、そのグループごとにフィルタリングポリシーを設定できること。			
	③ 手動でブラックリスト、ホワイトリストの設定が可能であること			
	④ 特定のWebサイト（掲示板等）への書き込みを禁止する機能を有すること。			
	⑤ プロキシサービスや認証サービスと連携して、シングルサインオンが可能であること。			
	⑥ システム管理用インターフェースとして、Webベース等のGUIを提供すること。			
	⑦ フィルタリングデータベースの自動更新及び手動更新が可能であること。			
	⑧ ブロックログ、POSTログの記録、グラフ表示等のレポーティング機能を有すること。			
	⑨ 掲示板等への書き込んだ内容のログ取得が可能であること。			
	⑩ 現行運用でフィルタリングされているルールを引き継ぐことができること。			
	⑪ ユーザ別又はアクセス元IPアドレス等で閲覧許可ポリシーを制御可能なこと。			
	⑫ Webコンテンツフィルタリングのログは1年以上保存し、検索、閲覧を行う機能を有すること。			
ハードウェア要件				
	① 特に規定しない。			
エ 標的型攻撃対策（Web）機能				
Webマルウェア検出装置				
ソフトウェア要件				
	① ハードウェア要件を参照すること。			
ハードウェア要件				
	① 100BASE-TX/1000BASE-Tのポートを4つ以上持つこと。			
	② 250Mbps以上のトラフィックを検査可能であること。			
	③ アプライアンス内の仮想化環境でダウンロードファイルの動作の解析が可能であること。			
	④ ネットワークにおけるボットによる不正な活動を検知できること。			
	⑤ マルウェアの検知状況やコールバック先などのレポートを作成する機能を有すること。			
	⑥ C&Cサーバ定義情報をインターネット経由で自動及び手動の両方で更新できること。			
3 マルウェア対策（サーバ・LAN端末・仮想デスクトップ）サービス				
（1）概要				
	サーバ、共有フォルダ及びLAN端末、仮想デスクトップにマルウェアが侵入した際、早期に検知・駆除するため、マルウェア対策（サーバ・LAN端末）サービスを提供する。サーバ及び共有フォルダ、LAN端末のマルウェア検査・検知を行う。 サーバ及びLAN端末では、ホスト間の通信の制御を行う。LAN端末では、振る舞い検知型のマルウェア検査を行う。 具体的要件について、以下に記載する。			
（2）構築要件				
	① 最新のパターンファイルをインターネット経由で自動及び手動の両方で更新できるよう構成すること。			
	② マルウェア検知・駆除を一括で管理できるよう構成すること。			
	③ Windowsサーバ、Linuxサーバ及びLAN端末のマルウェア検査を実施すること。			
	④ ファイル共有サーバに格納されているファイルのマルウェア検査を実施すること。			
	⑤ マルウェア検査方式として、パターンマッチングによる検査を提供すること。			
	⑥ ホストベースのファイアウォール機能を導入し、サーバ、及びLAN端末、テレワークサービスの仮想デスクトップ環境のホスト間の通信を制御し、可能な限りリアルタイム検知が可能なこと。			

別紙1－2　要件定義書（サービス・機器）

項番号	内容	提案内容	補足資料	記載箇所
	⑦ LAN端末におけるマルウェア検査には、振る舞い型のマルウェア検査を提供すること。			
	⑧ LAN端末で検知したマルウェアが他のLAN端末に存在しないか確認できる機能を提供すること。			
	⑨ LAN端末で検知したマルウェアの感染経路を確認できるよう機能を提供すること。			
	⑩ マルウェアに感染したファイルを隔離する機能を提供すること。			
	⑪ マルウェア判定された場合は、運用員に通知するよう構成すること。			
	⑫ マルウェア検査対象機器にエージェントの導入が必要な場合は、エージェントを管理サーバで全て管理できるよう構成すること。			
	⑬ マルウェアは、可能な限りリアルタイムで検知できる構成とすること。			
(3) 機器等要件				
ア　ウイルス対策（ファイル共有）機能				
ソフトウェア要件				
	① スケジュール設定により定時スキャンが可能であること。			
	② リアルタイムスキャンが可能であること。			
	③ 圧縮及び多重圧縮したファイルのマルウェア検知・駆除が可能であること。			
	④ マルウェア等の検出時に通知を行う機能を有すること。			
	⑤ システム管理用インターフェースとして、Web ベース等の GUI を提供すること。			
	⑥ バックアップ領域を除き CIFS でアクセス可能な領域すべてをスキャン可能であること。			
ハードウェア要件				
	① ハードウェア要件は、本要件定義書の第2－2 ストレージ機器を参照すること。			
イ　ウイルス対策（サーバ）機能				
ソフトウェア要件				
	① Windows及びLinuxサーバに対するマルウェア対策が可能であること。			
	② スケジュール設定により定時スキャンが可能であること。			
	③ リアルタイムスキャンが可能であること。			
	④ 圧縮及び多重圧縮したファイルのマルウェア検知・駆除が可能であること。			
	⑤ マルウェア等の検出時に通知を行う機能を有すること。			
	⑥ システム管理用インターフェースとして、Webベース等のGUIを提供すること。			
ハードウェア要件				
	① ハードウェア要件は、本要件定義書の第2－2 ストレージ機器を参照すること。			
ウ　ウイルス対策（LAN端末）機能				
ソフトウェア要件				
	① LAN端末に対して、マルウェア等の不正プログラムの検出、自動駆除、隔離等の一元的な管理が可能であること。			
	② LAN端末間の通信をポートベースで制御することが可能なこと。			
	③ LAN端末及びテレワークサービスの仮想デスクトップ環境においても、適切にマルウェア対策が可能であること。			
	④ スケジュール設定により定時スキャンが可能であること。			
	⑤ リアルタイムスキャンが可能であること。			
	⑥ マルウェア等の検出時に通知を行う機能を有すること。			
	⑦ システム管理用インターフェースとして、WebベースのGUIを提供すること。			
ハードウェア要件				
	① ハードウェア要件は、本要件定義書の第2－2 ストレージ機器を参照すること。			

別紙1－2　要件定義書（サービス・機器）

項番号	内容	提案内容	補足資料	記載箇所
エ　端末マルウェア検知機能				
ソフトウェア要件				
①	ハッシュ値や、IOC（複数のソースからのイベントデータ（侵入イベントとマルウェアイベントなど）を相互に関連付ける機能）、Yaraなどの手法を用いた検査が可能であること。			
②	サンドボックス等でマルウェアと疑わしいファイルの挙動を確認可能であること。			
③	サンドボックス等でのファイル解析においては、複数のファイル形式での解析が可能であること。			
④	LAN端末で検知したマルウェアが他のLAN端末に存在しないか確認できること。			
⑤	管理サーバ、サンドボックス等については、オンプレミス型で提供すること。			
ハードウェア要件				
①	特に規定しない。			
オ　端末インシデント対応機能				
ソフトウェア要件				
①	LAN端末内のマルウェアの感染経路を管理画面（GUI）で確認ができること。			
②	LAN端末内のマルウェアが組織内のネットワーク上でどのように広がっていくかを分析できること。			
ハードウェア要件				
①	特に規定しない。			
4　侵入検知防御サービス				
(1) 概要				
	インターネット及び政府共通ネットワークから省内への不正侵入を防ぐため、侵入検知防御サービスを提供する。サイバー攻撃などの総務省LANへの不正なアクセスに対して、アクセス制御・侵入検知を行う。総務省LANの各セグメント間のアクセス制御を行う。 具体的要件について、以下に記載する。			
(2) 構築要件				
①	総務省LANとインターネット間、総務省LANと政府共通ネットワーク間の接続に対するアクセス制御を行うこと。			
②	総務省LANとインターネット間のアクセス制御は、異なるベンダの製品により多段防御構成で行うこと。			
③	総務省LANとインターネット間のアクセス制御では、通過するパケットの中身を判別し、通過・拒否（破棄）等の制御を行うこと。			
④	インターネットからのDoS/DDoS攻撃を防御すること。			
⑤	通過・拒否（破棄）するパケットのログを取得すること。また、ログの保存期間は1年以上とすること。			
⑥	総務省LAN内において、本省と外部監視室間の接続に対するアクセス制御を行うこと。			
⑦	総務省LAN内において、サーバセグメントと端末セグメントを分離し、これらセグメント間の接続に対するアクセス制御を行うこと。			
⑧	総務省LAN内において、サービス系のセグメントと管理系のセグメント間の接続に対するアクセス制御を行うこと。			
⑨	政府共通ネットワーク接続ネットワーク内の複数の業務システムを集約し、それぞれに対してアクセス制御を行うこと。			
⑩	業務システム接続ネットワーク内の複数の業務システムを集約し、それぞれに対してアクセス制御を行うこと。			
(3) 機器等要件				
ア　侵入検知防御機能				
ソフトウェア要件				
①	インラインモード、パッシブモードに対応すること。			
②	IPv4/IPv6によるアクセス制御や攻撃の検知、防御が行えること。			
③	通過するIPパケット、ポート番号、プロトコルのアクセス制御（許可、拒否（破棄）等）ができること。			

別紙1－2　要件定義書（サービス・機器）

項番号	内容	提案内容	補足資料	記載箇所
	④ 通過するパケットの中身を判別し、中身に応じた制御ができること。			
	⑤ インターネットからの分散サービス拒否（DoS/DDoS）攻撃を防御できること。			
	⑥ 不正侵入検知シグネチャをインターネット経由で自動及び手動の両方で更新できること。			
	⑦ 通過・拒否（破棄）するパケットのログが取得できること。また、ログの保存期間は1年以上とし、検索、閲覧を行う機能を有すること。			
	⑧ シグネチャ、アノーマリ双方の検知メカニズムを搭載していること。			
	⑨ アノーマリ検知のためのパラメータは、動的に学習可能であること。			
	⑩ オンラインでシグネチャファイルの更新が可能であること。もしくは、シグネチャファイルに相当する情報の更新が可能であること。			
	⑪ 1,000以上のアプリケーションを識別できること。もしくは、同等以上の検出、防御機能を有すること。			
	⑫ 不正アクセスの検知をSNMPTrap、電子メール等で通知する機能を有すること。			
	⑬ 通過する通信のパケットのIPアドレス、プロトコル、TCP/UDPポート番号の組み合わせ等、予め決められたルールに基づき通信の許可及び拒否の制御ができること。			
	⑭ 通信フローのログを表示できること。			
	⑮ システム管理用インターフェースとして、WebベースのGUIを提供すること。			
	⑯ 予め設定されたイベントを検出した場合、通知する機能を有すること。			
	⑰ 不正アクセスをリアルタイムに検知し、防御する機能を有すること。			
	⑱ トラフィックのパターンを分析し、マルウェアによる攻撃、DoS/DDoS攻撃、アプリケーションやサーバの脆弱性を狙う攻撃等の悪意又は異常な通信の排除ができること。			
	⑲ ポートやプロトコルに関わらず全てのトラフィックをモニタし、ボットネット感染が疑われる端末をリストアップする機能を有すること。			
	⑳ シグネチャ情報は、常に最新の状態に保つこと。			
	㉑ 総務省情報セキュリティポリシーに適合するようにシグネチャのチューニングが可能であること。			
	㉒ 管理用端末からシグネチャ等の更新及びログの検索等ができること。			
	㉓ 通信量の統計情報を元に、宛先/送信元の国別で通信量を世界地図など視覚的に表示できること。			
	㉔ 検出/防御した脅威の統計情報を元に、宛先/送信元の国別で脅威の発生状況を世界地図など視覚的に表示できること。			
	㉕ 40以上の事前に定義されたレポートテンプレート及びカスタムレポート機能を有し、それらをPDF形式にして設定されたスケジュールで自動メール送信可能なこと。			
	ハードウェア要件			
	① 100BASE-TX/1000BASE-T のポートを 4 ポート以上有すること。			
	② 消費電力が 450W 以下であること。			
	③ 侵入検知防御（IPS）スループットは、1Gbps 以上であること。			
イ	外部監視室接続侵入検知防御機能			
	ソフトウェア要件			
	① IPv4及びIPv6のルーティングに対応すること。また、IPv4のIPSecによる暗号化機能もサポートしていること。			
	② アドレス変換機能（NAT）やTCPポート番号変換機能（NAPT）を有すること。			
	③ ステートフルインスペクション機能を有すること。			
	④ WebベースのGUIとCLIで設定が可能であること。また、CLIでは、SSHをサポートすること。			
	ハードウェア要件			
	① ボックス型筐体であること。			
	② 消費電力が150W以下であること。			

別紙1－2　要件定義書（サービス・機器）

項番号	内容	提案内容	補足資料	記載箇所
ウ	仮想ブラウザネットワーク接続侵入検知防御機能			
	ソフトウェア要件			
①	アドレス変換機能（NAT）やTCPポート番号変換機能（NAPT）を有すること。			
②	IPv4/IPv6通信のアクセス制御が可能であること。			
③	トラブル解決を迅速にするために、ネットワークトレース（TCP dump相当）機能をサポートし、パケットキャプチャ等で解析ができること。			
④	設定内容の世代管理を行えること。			
⑤	WebベースのGUIとCLIで設定が可能であること。また、CLIでは、SSHをサポートすること。			
	ハードウェア要件			
①	100BASE-TX/1000BASE-Tのポートを8ポート以上有すること。			
②	消費電力が350W以下であること。			
③	ファイアウォールスループットは、1Gbps以上であること。			
④	同時セッション数は、128,000以上であること。			
エ	政府共通ネットワーク接続侵入検知防御機能（内）			
	ソフトウェア要件			
①	アドレス変換機能（NAT）やTCPポート番号変換機能（NAPT）を有すること。			
②	IPv4/IPv6通信のアクセス制御が可能であること。			
③	トラブル解決を迅速にするために、ネットワークトレース（TCP dump相当）機能をサポートし、パケットキャプチャ等で解析ができること。			
④	設定内容の世代管理を行えること。			
⑤	WebベースのGUIとCLIで設定が可能であること。また、CLIでは、SSHをサポートすること。			
	ハードウェア要件			
①	100BASE-TX/1000BASE-Tのポートを8ポート以上有すること。			
②	消費電力が350W以下であること。			
③	ファイアウォールスループットは、1Gbps以上であること。			
④	同時セッション数は、128,000以上であること。			
オ	政府共通ネットワーク用侵入検知防御機能			
	ソフトウェア要件			
①	総務省LANの業務システムに対し、仮想ファイアウォールを各々稼働可能なこと。			
②	20台分の仮想ファイアウォールが構成できる機能を有すること。なお、現在の業務システムは9システムある。			
③	アドレス変換機能(NAT)や TCP ポート番号変換機能(NAPT)を有すること。			
④	IPv4/IPv6通信のアクセス制御が可能であること。			
⑤	トラブル解決を迅速にするために、ネットワークトレース(TCP dump 相当)機能をサポートし、パケットキャプチャ等の解析が可能であること。			
⑥	設定内容の世代管理を行えること。			
⑦	Web ベースの GUI と CLI の設定が可能であること。また、CLI では、SSH をサポートすること。			
	ハードウェア要件			
①	冗長化構成を組むことが可能であること。			
②	100BASE-TX/1000BASE-T のポートを 8 ポート以上有すること。			
③	消費電力が350W以下であること。			
④	ファイアウォールスループットは、1Gbps 以上であること。			
⑤	同時セッション数は、500,000 以上であること。			

別紙1－2　要件定義書（サービス・機器）

項番号	内容	提案内容	補足資料	記載箇所
カ	インターネット接続侵入検知防御機能（外）			
	ソフトウェア要件			
①	アプリケーションレベルのアクセスを制御する機能を有すること。			
②	アドレス変換機能（NAT）やTCPポート番号変換機能（NAPT）を有すること。			
③	IPv4/IPv6通信のアクセス制御が可能であること。			
④	トラブル解決を迅速にするために、ネットワークトレース（TCP dump相当）機能をサポートし、パケットキャプチャ等の解析が可能であること。			
⑤	設定内容の世代管理を行えること。			
⑥	WebベースのGUIとCLIで設定が可能であること。また、CLIでは、SSHをサポートすること。			
	ハードウェア要件			
①	100BASE-TX/1000BASE-Tのポートを8ポート以上有すること。			
②	消費電力が450W以下であること。			
③	ファイアウォールスループットは、1Gbps以上であること。			
④	同時セッション数は、250,000以上であること。			
キ	インターネット接続侵入検知防御機能（内）			
	ソフトウェア要件			
①	アドレス変換機能（NAT）やTCPポート番号変換機能（NAPT）を有すること。			
②	IPv4/IPv6通信のアクセス制御が可能であること。			
③	トラブル解決を迅速にするために、ネットワークトレース（TCP dump相当）機能をサポートし、パケットキャプチャ等の解析が可能であること。			
④	設定内容の世代管理を行えること。			
⑤	WebベースのGUIとCLIの設定が可能であること。また、CLIでは、SSHをサポートすること。			
	ハードウェア要件			
①	100BASE-TX/1000BASE-Tのポートを8ポート以上有すること。			
②	消費電力が150W以下であること。			
③	ファイアウォールスループットは、1Gbps以上であること。			
④	同時セッション数は、128,000以上であること。			
ク	業務システム用侵入検知防御機能			
	ソフトウェア要件			
①	総務省LANの業務システムに対し、仮想ファイアウォールを各々稼働可能なこと。			
②	50台分の仮想ファイアウォールが構成できる機能を有すること。なお、現在の業務システムは18システムある。			
③	アドレス変換機能(NAT)や TCP ポート番号変換機能(NAPT)を有すること。			
④	IPv4/IPv6通信のアクセス制御が可能であること。			
⑤	トラブル解決を迅速にするために、ネットワークトレース(TCP dump 相当)機能をサポートし、パケットキャプチャ等の解析が可能であること。			
⑥	設定内容の世代管理を行えること。			
⑦	Web ベースの GUI と CLI の設定が可能であること。また、CLI では、SSH をサポートすること。			
	ハードウェア要件			
①	冗長化構成を組むことが可能であること。			
②	100BASE-TX/1000BASE-T のポートを 8 ポート以上有すること。			
③	消費電力が 125W 以下であること。			
④	ファイアウォールスループットは、1.5Gbps 以上であること。			
⑤	同時セッション数は、750,000 以上であること。			

別紙1－2　要件定義書（サービス・機器）

項番号	内容	提案内容	補足資料	記載箇所
ケ	管理LAN侵入検知防御機能（本省）			
	ソフトウェア要件			
	① アドレス変換機能（NAT）やTCPポート番号変換機能（NAPT）を有すること。			
	② IPv4/IPv6通信のアクセス制御が可能であること。			
	③ トラブル解決を迅速にするために、ネットワークトレース（TCP dump相当）機能をサポートし、パケットキャプチャ等の解析が可能であること。			
	④ 設定内容の世代管理を行えること。			
	⑤ WebベースのGUIとCLIの設定が可能であること。また、CLIでは、SSHをサポートすること。			
	ハードウェア要件			
	① 100BASE-TX/1000BASE-Tのポートを8ポート以上有すること。			
	② 消費電力が150 W以下であること。			
	③ ファイアウォールスループットは、3.5Gbps 以上であること。			
	④ 同時セッション数は、1,000,000以上であること。			
コ	インターネット接続侵入検知防御機能（ディザスタリカバリサイト）			
	ソフトウェア要件			
	① ハードウェア要件を参照すること。			
	ハードウェア要件			
	① アプリケーションレベルのアクセスを制御する機能を有すること。			
	② アドレス変換機能（NAT）やTCPポート番号変換機能（NAPT）を有すること。			
	③ IPv6通信のアクセス制御が可能であること。			
	④ トラブル解決を迅速にするために、ネットワークトレース（TCPdump相当）機能をサポートし、パケットキャプチャ等の解析が可能であること。			
	⑤ 設定内容の世代管理を行えること。			
	⑥ WebベースのGUIとCLIで設定が可能であること。また、CLIでは、SSHをサポートすること。			
	⑦ 100BASE-TX/1000BASE-Tのポートを8ポート以上有すること。			
	⑧ 消費電力が450W以下であること。			
	⑨ ファイアウォールスループットは、1Gbps以上であること。			
	⑩ 同時セッション数は、250,000以上であること。			
サ	管理LAN侵入検知防御機能（ディザスタリカバリサイト）			
	ソフトウェア要件			
	① アドレス変換機能（NAT）やTCPポート番号変換機能（NAPT）を有すること。			
	② IPv4/IPv6通信のアクセス制御が可能であること。			
	③ トラブル解決を迅速にするために、ネットワークトレース（TCP dump相当）機能をサポートし、パケットキャプチャ等の解析が可能であること。			
	④ 設定内容の世代管理を行えること。			
	⑤ WebベースのGUIとCLIの設定が可能であること。また、CLIでは、SSHをサポートすること。			
	ハードウェア要件			
	① 100BASE-TX/1000BASE-Tのポートを8ポート以上有すること。			
	② 消費電力が150 W以下であること。			
	③ ファイアウォールスループットは、3.5Gbps以上であること。			
	④ 同時セッション数は、1,000,000以上であること。			

別紙1－2　要件定義書（サービス・機器）

項番号	内容	提案内容	補足資料	記載箇所
5　不正接続機器検知サービス				
（1）概要				
	総務省LANに不正に接続された機器に起因したウイルス感染から総務省LANを保護するため、不正接続機器検知サービスを提供する。総務省LANに接続可能な機器を事前に登録し、限定する。未登録の機器が総務省LANに接続された際に、接続通知・通信の遮断を行う。 具体的要件について、以下に記載する。			
（2）構築要件				
	① 未登録機器が接続された場合、接続されたことを検知し、その通信を遮断すること。			
	② 総務省LANに接続された機器の固有情報を収集・管理できるよう構成すること。			
	③ 総務省LANに接続を許可する機器の固有情報を取得・登録できるよう構成すること。			
	④ 総務省LANへの接続を許可されたデバイスのみ、総務省LANへの接続を許可すること。			
（3）機器等要件				
ア　不正接続機器検知機能				
ソフトウェア要件				
	① 総務省LANに接続された機器の固有情報を収集・管理できること。			
	② 総務省LANに接続を許可する機器の固有情報を登録できること。			
	③ 未登録機器を検出し、通知する機能を有すること。			
	④ 管理外の LAN 端末等が接続した場合、接続を抑止する機能を有すること。			
	⑤ Webインターフェースの管理画面を有すること。			
ハードウェア要件				
	① 特に規定しない。			
6　特権アクセス制御サービス				
（1）概要				
	総務省LANを構成する各機器に対する不正な管理操作を防止するため、特権アクセス制御サービスを提供する。管理目的のアクセス及び操作を、許可された専用端末のみに限定する。また、管理目的のアクセス及び操作のログを収集し、記録する。 具体的要件について、以下に記載する。			
（2）構築要件				
	① 総務省LANを構成する各機器への特権ID操作（管理的アクセス）は、専用端末からのみ可能となるように構成し、LAN端末からはアクセスできないよう設計・設定をすること。			
	② LAN端末ではディレクトリ機能の管理者権限でのログオンが不可となるよう構成すること。			
	③ 特権ID操作を許可する専用端末では、ディレクトリ機能の管理者権限アカウントのキャッシュを無効化すること。			
	④ ディレクトリ機能の管理者権限でのログオン失敗を検知すること。			
	⑤ ソフトウェアインストール申請時は、ディレクトリ機能の管理者権限アカウントではなく、ソフトウェアインストールに必要な権限のみをもったアカウントを発行すること。			
	⑥ LAN端末のローカル管理者権限のパスワードを端末ごとに異なるものにすること。			
	⑦ Windowsサーバでは不要なポート宛の通信を拒否するよう構成し、必要最小限のポートを開放すること。			
	⑧ 特権IDによる操作ログを取得すること。また、ログの保存期間は1年以上とし、検索、閲覧を行う機能を有すること。			
（3）機器等要件				
ア　特権アクセス制御機能				
ソフトウェア要件				
	① 端末側にエージェントを導入することなく、導入可能であること。			
	② 接続元端末のIPアドレスを限定できること			

項番号	内容	提案内容	補足資料	記載箇所
	③ 操作ログの検索が可能なこと。			
	④ 操作ログは、暗号化して保存可能なこと。			
	⑤ 外部システム（LDAP、パスワード管理システム）と連携可能なこと。			
	⑥ 複数のプロトコルでアクセス制御が可能なこと。			
	ハードウェア要件			
	① 特に規定しない。			
7　セキュリティ管理サービス				
（1）概要				
	LAN端末及びWindowsサーバ、Linuxサーバのセキュリティポリシー遵守状況を確認するため、セキュリティ管理サービスを提供する。ポリシーテンプレートを作成し、LAN端末、Windowsサーバ、Linuxサーバが本ポリシーに準拠しているか確認する。監査に必要なログを収集し、保全する。 具体的要件について、以下に記載する。			
（2）構築要件				
	① サーバ、LAN端末及びテレワークサービスの仮想デスクトップ環境に対して、定期的にセキュリティポリシーの遵守状況を確認すること。			
	② ファイル属性、ファイルアクセス権、パッチ適用状況、パスワード強度、システム監査設定、起動サービスの監査が可能な環境を構成すること。			
	③ セキュリティ監査対象機器との通信は、全て暗号化されていること。			
	④ ポリシー及び監査項目の設定、検査の実行及び結果レポートを集中管理できる構成とすること。			
	⑤ 総務省が年に一回実施するセキュリティ監査時に本サービスが利用できるようにすること。			
	⑥ 総務省情報セキュリティポリシーに準拠したポリシーテンプレートを作成できる機能を提供すること。			
	⑦ 総務省LANを構成するサーバ、ネットワーク機器、アプライアンス機器の監査ログを自動的に取得・保全すること。			
	⑧ LAN端末の操作ログを取得・保全すること。			
	⑨ ログデータは、1年以上保管すること。			
	⑩ 管理コンソールでポリシー及び監査項目の設定、検査の実行及び結果レポートを一元管理すること。			
（3）機器等要件				
ア　セキュリティ監査機能				
	ソフトウェア要件			
	① 本省、拠点のサーバ、LAN端末及びテレワークサービスの仮想デスクトップ環境に対して監査条件の配布、監査の実行指示及び結果の収集が可能である等、セキュリティ監査に耐えうる情報の収集が可能であること。また、日時及び周期等を指定し、自動的に処理できること。			
	② LAN 端末及びサーバの OS に対応していること。			
	③ 管理コンソールでポリシー及び監査項目の設定、検査の実行及び結果レポートを一元管理できること。			
	④ 監査結果のスコア表示等ポリシー遵守状況を可視化できること。			
	⑤ 項目を選択して監査結果の表示及び印刷ができること。			
	⑥ 管理画面及び結果レポートは、主管課が分かりやすいよう日本語化されていること。			
	⑦ アカウントの整合性、ログインパラメータ、パスワードの強度、ネットワーク整合性、オブジェクト整合性、OS パッチ、システム監査、レジストリの監査ができること。			
	⑧ ISO/IEC 17799 に沿った監査項目に対応していること。			
	⑨ 現行のセキュリティポリシーの移行が可能であること。			
	⑩ ポリシテンプレートをベースにカスタマイズが可能であること。			
	⑪ 保管したログは検索、閲覧が可能なこと。			
	ハードウェア要件			
	① ハードウェア要件は、本要件定義書の第2－2 ストレージ機器を参照すること。			

項番号	内容	提案内容	補足資料	記載箇所
イ	ログアーカイブ機能			
統合ログ収集装置				
ソフトウェア要件				
①	総務省LANを構成するサーバ、ネットワーク機器、アプライアンス機器のログ情報を自動的に収集・保存すること。また、これらの機器のログ収集に必要な台数のサーバを構成すること。			
②	収集したログ情報は閲覧や検索ができること。			
③	ログデータは、1年間以上の長期保管ができること。			
④	収集したログから、日、週、月ごと等でレポートを出力することが可能であること。			
⑤	集計した結果は、PDF、HTML、CSV形式等主管課がわかりやすい形式で提出されること。			
⑥	正規表現を用いたログの検索が可能であること。			
ハードウェア要件				
①	ハードウェア要件は、本要件定義書の第2－2 ストレージ機器を参照すること。			
8　セキュリティログ分析サービス				
(1) 概要				
	セキュリティインシデントの兆候を早期に検知するため、セキュリティログ分析サービスを提供する。複数のセキュリティログやイベントを用いて相関分析を実施することで、早期検知を実現する。検知したイベントの詳細を調査するため、関連するログを検索、分析する。 具体的要件について、以下に記載する。			
(2) 構築要件				
①	総務省LANを構成する各機器のログ・イベントのうち、セキュリティインシデントの兆候を掴むために必要なものを取得・保全すること。			
②	ログは1年以上保管すること。			
③	過去のログ・イベントに遡って相関分析を実施できるように構成すること。			
④	セキュリティインシデント調査等の際に、過去のログ・イベントを検索できるよう構成すること。			
⑤	収集されたログを単一のコンソールから確認できるよう構成すること。			
⑥	収集されたログを様々な条件での検索やフィルタリングして確認できるよう構成すること。			
⑦	イベント発生状況をグラフィカルなレポートとして提供できるよう構成すること。			
⑧	収集したログ・イベントを用いて、イベントの種類・時間・発生頻度等の情報を基にして正常ではない振る舞いを検出可能なルール（相関分析ルール）を作成し、本ルールを用いてログの自動分析を行うこと。			
⑨	収集したログ・イベントをパーシングし、正規化すること。			
⑩	セキュリティインシデントの兆候等をつかんだ場合は、アラートを通知すること。			
⑪	相関分析ルールは必要に応じて見直しができるよう構成とすること。			
(3) 機器等要件				
ア	セキュリティログ解析機能			
ソフトウェア要件				
①	ハードウェア要件を参照すること。			
ハードウェア要件				
①	専用OSを搭載したアプライアンス製品であること。			
②	総務省LAN内で発生するログを取りこぼすことなく収集できる性能を有すること。（ピーク時には50,000EPS以上）			
③	収集したログデータを内部で集計し、同様なイベントのログを集約して解析データ格納に必要なディスク容量を削減する機能を有すること。			
④	ログファイルは圧縮して保管し、ログ保管のために必要なディスク容量を削減できること。			
⑤	最低1年間のログを格納できること。			
⑥	イベント発生状況をグラフィカルなレポートとして提供する機能を有すること。			

別紙1－2　要件定義書（サービス・機器）

項番号	内容	提案内容	補足資料	記載箇所
	⑦ ドリルダウン操作によって、イベントの詳細な分析が実行できること。			
	⑧ セキュリティの観点から、ログファイルの転送を暗号化して行う機能を有すること。			
	⑨ イベント解析処理に特化した専用のDBを利用し、高速な処理が可能であること。			
	⑩ 統合ログ管理機能を有し、集約されたログを単一のコンソールから確認できること。			
	⑪ Webブラウザで操作が可能であり、1画面中にすべての機能が統合されていること。			
	⑫ インタフェースは、完全日本語対応であること。			
	⑬ 自動ベースライン機能により、長期間保存したログに対して、選択した期間に応じて自動的に平均値を算出してグラフ化し、平均と異なる傾向を把握できること。			
	⑭ 長期間のログに対して、様々な条件での検索やフィルタリングが実行できること。			
	⑮ ログ解析には、傾向分析だけではなく、相関分析のルールを利用できること。			
	⑯ セキュリティベンダが提供する最新の脅威情報や攻撃手法に関する情報を自動的に取り込み、相関分析のルールに加えることが可能であること。			
	⑰ 1つのログでは確認できないセキュリティインシデントに対して、イベントの種類・時間・発生頻度等の情報を基にして正常ではない振る舞いを検出可能であること。			
	⑱ リアルタイムの振る舞い検知だけでなく、過去データの振る舞い検知が可能であること。			
	⑲ 新しい攻撃のシナリオを想定して対応するルールを作成した場合、過去のログに遡って当該シナリオの発生有無を確認することが可能であること。			
	⑳ ログの相関分析だけではなく、ログの変化量の相関分析が可能であること。（例えば、侵入検知により何らかの攻撃イベントを検出した後に、通常時よりもログ量が増減するといった事象を抽出するためのルールを作成できること。）			
	㉑ ログ変化量や、外向のパケット数が一定値を超えた等といった異常状態を検知するためのルールを作成できること。			
	㉒ IPアドレスを有する全てのログに関してIP Reputationリストとマッチングし、不正な通信を検出できること。また、最新のIP Reputationリストを生成できること。			
9　仮想ブラウザサービス				
（1）概要				
	マルウェアが直接LAN端末に侵入するリスクを低減するために、総務省職員がインターネットへのWebアクセスを行う専用ブラウザ環境として、仮想ブラウザサービスを提供する。 インターネットにアクセスする際は、LAN端末のブラウザを利用せずに、本サービスからアクセスする。 具体的要件について、以下に記載する。			
（2）構築要件				
	① Internet Explorerを利用したインターネットへのWebアクセス機能を提供すること。			
	② LAN端末及びテレワークサービスの仮想デスクトップ環境からhttp、https以外のプロトコルを用いて本サービスにアクセスできる構成とすること。			
	③ インターネットからダウンロードしたデータを格納する領域を提供すること。			
	④ インターネットからダウンロードしたデータをLAN端末に移動する手段を提供すること。また、データ移動時にはマルウェア検査を実施すること。			
	⑤ 本サービスが万一マルウェア感染した際には、影響範囲を最小限にとどめ、感染拡大を抑止すること。			
	⑥ 仮想ブラウザサービスを提供するネットワークは、他のネットワークとの境界にファイアウォールを設置すること。			
	⑦ 仮想ブラウザサービスは、同時7,000ユーザが利用可能な構成とすること。			

別紙1－2　要件定義書（サービス・機器）

項番号	内容	提案内容	補足資料	記載箇所
(3) 機器等要件				
ア　仮想ブラウザ機能				
ソフトウェア要件				
	① RDP又はICAあるいはPCoIPを用いて、アクセスできること。			
	② 仮想ブラウザ環境のプロファイルを一元管理できること。			
	③ 細かなセキュリティポリシーを適用するために、アクセス制御用のファイアウォールサービスが、仮想サーバ単位で提供可能なこと。			
	④ LAN端末のブラウザのお気に入りなどに登録した外部サイトを閲覧する場合、外部サイトの URL が仮想ブラウザに転送され、自動的に仮想ブラウザが起動し外部サイトを閲覧できること。			
	⑤ 内部サイトやメール本文内に記載されている外部サイトを閲覧する場合、外部サイトの URL が仮想ブラウザに転送され、自動的に仮想ブラウザが起動し外部サイトを閲覧できること。			
	⑥ 高パフォーマンスを提供するために、ファイアウォールがハイパーバイザー内のカーネルで処理されること。			
	⑦ 同一セグメント上の仮想サーバ間のトラフィックにファイアウォールの動作を設定できること。			
ハードウェア要件				
	① ハードウェア要件は、本要件定義書の第2－2 ストレージ機器を参照すること。			
イ　仮想ブラウザ用ファイルマルウェア対策機能				
ソフトウェア要件				
	① 特に規定しない。			
ハードウェア要件				
	① 検査対象は仮想ブラウザサービス用のファイルサーバとし、当該サーバを検査可能なセグメントに本システムを導入すること。			
	② 装置の製造元が集収した不正プログラムの情報を自動的にダウンロードし、検出精度を高める機能を有すること。			
	③ 不正プログラムの判定はファイルのシグネチャマッチングに加え、装置に搭載した複数の仮想環境上で当該ファイルを読み込み実行し、挙動を解析することにより実現すること。			
	④ 実行するOS、アプリケーションをファイルタイプ毎に複数指定できること。			
	⑤ ファイルサーバとの通信は、CIFS,NFS,SMBをサポートすること。			
	⑥ 指定したファイルサーバのフォルダ内のファイルを定期的かつ自動的に解析できること。			
	⑦ 160,000ファイルオブジェクト/日程度の解析が可能なこと。			
	⑧ 解析の結果を管理端末からGUIで確認できること。			
	⑨ 装置で検知した情報を自動的に製造元へ提供する機能を持たないこと。			
	⑩ 暗号化及びパスワードロックがかかっていない解析可能な複数の圧縮ファイル形式に対応すること。			
ウ　アプリケーション不正動作検知機能				
ソフトウェア要件				
	① 本サービス内で利用できるアプリケーションをホワイトリスト方式で制限できること。			
ハードウェア要件				
	① ハードウェア要件は、本要件定義書の第2－2 ストレージ機器を参照すること。			
エ　仮想ブラウザ用ファイル共有機能				
ソフトウェア要件				
	① 特に規定しない。			
ハードウェア要件				
	① ハードウェア要件は、本要件定義書の第2－2 ストレージ機器を参照すること。			

別紙1－2　要件定義書（サービス・機器）

項番号	内容	提案内容	補足資料	記載箇所
第5　運用管理サービス				
1　申請管理サービス				
(1) 概要				
	申請管理サービスは、職員から受け付けた総務省LANサービスに関する申請依頼を一元管理し、申請内容に応じて、総務省LANサービスと連携するサービスである。 ・職員は、申請書を申請管理サービスを介して提出し、主管課に承認依頼を行う。 ・主管課は、職員からの申請に対して承認又は拒否を行い、運用要員に承認した申請の対応を依頼する。 ・運用要員は、運用管理端末から申請管理サービスに接続し、申請内容を登録する。申請管理サービスは、登録された申請内容に応じて該当するサービスと連携する。 具体的要件について、以下に記載する。			
(2) 構築要件				
	① 認証サービスと連携し、ユーザ認証を行うこと。			
	② 権限を持つものだけが、承認できるよう構成すること。			
	③ 申請の処理状況を管理し、ユーザと承認者へ通知すること。			
	④ 申請内容の整合性チェックを行うこと。			
	⑤ 申請の履歴を保存し、確認できるよう構成すること。			
	⑥ 貸出用機器の在庫管理を行うこと。			
	⑦ 職員以外のユーザアカウント管理機能を持つこと。			
	⑧ 以下の各種申請フォーマットを作成すること。 ・共有メールアカウント申請（メールサービス） ・電子メール自動転送申請（メールサービス） ・メーリングリスト設定申請（メールサービス） ・LAN端末新規配備申請（ネットワークサービス） ・LAN端末移設申請（ネットワークサービス） ・LAN 端末撤去申請（ネットワークサービス） ・LANプリンタ・LAN複合機移設申請　（認証サービス、ネットワークサービス、プリントサービス） ・ソフトウェアインストール申請（認証サービス） ・機器接続申請（ネットワークサービス） ・インフォメーションフォルダ設定申請　（ポータルサイトサービス） ・電子会議室設定申請　（ポータルサイトサービス） ・設備予約設定申請（ポータルサイトサービス） ・訓令通達登録申請（大臣官房）（ポータルサイトサービス） ・迷惑メール対策除外設定申請（セキュリティサービス） ・外部接続システム環境利用申請（認証サービス） ・LAN端末期間限定配備申請（ネットワークサービス） ・LAN端末期間限定移設申請（ネットワークサービス） ・LANプリンタ期間限定移設申請（認証サービス、ネットワークサービス、プリントサービス） ・DNS 設定申請（ネットワークサービス） ・業務システム用アカウント設定申請（認証サービス） ・会議用タブレット型端末貸出申請（ネットワークサービス） ・シンクライアント貸出申請（テレワークサービス） ・タブレット型端末外部利用申請（テレワークサービス） ・2号館会議室予約設定申請書（ポータルサイトサービス） ・第2庁舎会議室予約設定申請　（ポータルサイトサービス） ・会議室予約アカウント設定申請（ポータルサイトサービス） ・その他提案に合わせた申請			
(3) 機器等要件				
ア　申請管理機能				
	① 過去の申請情報を表示可能であること。			

項番号	内容	提案内容	補足資料	記載箇所
	② 申請処理の完了後には、申請者に通知されること。			
	③ 申請情報を一元管理すること。			
	④ 利用期限の通知機能を有すること。			
	⑤ ハードウェア要件は、本要件定義書の第2－2 ストレージ機器を参照すること。			
2 運用支援サービス				
(1) 概要				
	運用支援サービスは、総務省LANに関する問い合わせを一元管理し、進捗状況の確認や問題分析のための情報収集する環境を提供するサービスである。 問い合わせとイベントをインシデントとして登録し、一次対処、復旧までの調査・回答の進捗管理を運用員内で共有できるようにする。 具体的要件について、以下に記載する。			
(2) 構築要件				
	① インシデント管理機能を活用し、効率的に情報共有や履歴管理、主管課への報告を行えるようにすること。			
	② インシデント対応や操作説明のため、特定のLAN端末を遠隔操作できること。			
	③ インシデント管理機能は、運用期間中に十分対応できるよう構成すること。			
(3) 機器等要件				
ア インシデント管理機能				
ソフトウェア要件				
	① ユーザからの問い合わせを管理できること。			
	② 問い合わせ実績の検索ができること。			
	③ 障害の対応状況の管理ができること。			
	④ 日次、週次、月次単位でレポート出力が可能であること。			
	⑤ 一定時間に対応が完了していない問い合わせに対してメール通知等の督促手段を提供すること。			
	⑥ ITIL Version3に沿った機能を備えること。			
	⑦ WEB上で複数人による操作、編集作業が可能であること。			
ハードウェア要件				
	① ハードウェア要件は、本要件定義書の第2－2 ストレージ機器を参照すること。			
イ LAN端末リモート操作機能				
ソフトウェア要件				
	① LAN端末に対してリモートで操作できること。			
	② ユーザ側でリモート操作の承認を行い、許可された場合のみ操作できること。			
	③ ユーザの操作画面を共有して操作ができること。			
	④ 運用者によりGUIで操作が可能であること。			
	⑤ リモートで操作指導等が実施可能であること。			
	⑥ ユーザが支援を必要とする場合、ホスト招待メッセージを送信する等、リモート操作の認証方法には複数の方式が利用可能であること。			
	⑦ リモート操作端末とLAN端末間でファイルコピーやクリップボードの共有等が可能であること。			
	⑧ リモート操作画面は、全画面表示が可能であること。			
ハードウェア要件				
	① ハードウェア要件は、本要件定義書の第2－2 ストレージ機器を参照すること。			

別紙1－2　要件定義書（サービス・機器）

項番号	内容	提案内容	補足資料	記載箇所
3　システム監視サービス				
（1）概要				
	システム監視サービスは、システムの可用性を維持するため、総務省LANのサービスを提供する機器の障害検知やリソース監視、トラフィック監視、その報告を行うためのサービスである。 ・サーバ、ネットワーク機器及びアプライアンス機器の状態を取得し、基準値から外れるものに対し、警告を発生させる。 ・サーバのシステムログを収集し、エラー発生時に警告を発生させる。 ・運用要員が、発生したアラートの内容を確認することができる。 具体的要件について、以下に記載する。			
（2）構築要件				
	① 管理対象機器の一元的な監視を行い、効率的な管理を行うこと。			
	② 本調達で導入する機器の稼働状況をグラフィカルに表示し、異常が発生した場合には関係者が遅滞なく対応できるようにすること。			
	③ 監視対象機器のリソース状況・性能情報を取得し、適切な資源配分、異常検知等が行えること。			
	④ 定期ジョブを一元管理（スケジュール、実行、連携、記録、結果確認）できること。			
	⑤ 重大な問題や緊急の問題を検知した場合、パトランプ、警告音及びメール等で運用要員に通知すること。			
（3）機器等要件				
ア　システム監視機能				
ソフトウェア要件				
	① 総務省LANを構成するサーバ、ネットワーク機器、アプライアンス機器を含めたシステム稼働状況（死活監視、イベント監視等）を監視する機能を実装すること。			
	② ハードウェア、ソフトウェア、アプリケーションプログラムのプロセス及びサービスも監視すること。			
	③ イベント発生時に、メール自動発信等複数の方法で運用員に対して通知可能であること。			
	④ 外部監視室でも、機器の稼働状況（死活監視、ログ監視等）を監視できること。			
	⑤ 監視機器が追加になる場合においても、既に導入済みの機器と同様にメッセージ通知や性能の監視ができるように、ポリシーテンプレートの配布が可能であること。			
	⑥ 管理GUI上で異常が発生したサーバを特定可能であること。また、その画面からハードウェア管理ツール等を起動可能であること。			
	⑦ OS異常時、サーバ停止時でもメール、トラップ通知が可能であること。			
	⑧ 外部拠点サーバにおいては、保守性の向上のため、サーバ本体の状態（BIOS画面、ハング状態等）に依存せず監視や操作が可能であり、画面キャプチャーが可能な構成とすること。			
ハードウェア要件				
	① ハードウェア要件は、本要件定義書の第2－2 ストレージ機器を参照すること。			
イ　リソース管理機能				
ソフトウェア要件				
	① 管理対象機器のCPU使用率、メモリ使用率、ディスクビジー率、ページフォルト数、ネットワーク等の性能情報を取得できること。			
	② 性能異常を検知した際に、グラフ等で可視化できる機能を有すること。			
	③ CPU、メモリ、ディスク等のサーバ性能情報を監視すること。また、閾値を超えた場合に管理者に通知が可能であること。			
ハードウェア要件				
	① ハードウェア要件は、本要件定義書の第2－2 ストレージ機器を参照すること。			

別紙1－2　要件定義書（サービス・機器）

項番号	内容	提案内容	補足資料	記載箇所
ウ	ネットワーク資源管理機能			
	ソフトウェア要件			
①	NetFlowやsFlow等のプロトコルを利用し、トラフィックの測定ができること。			
②	500以上のセンサーをサポートすること。			
③	HTML及びPDFフォーマットでレポート出力ができること。			
④	システム管理用インターフェースとして、WebベースのGUIを提供すること。			
⑤	HTTPやFTP等のプロトコル単位で性能情報を採取できること。			
⑥	障害を検出した場合、電子メール等でアラームを送信できること。			
⑦	定期的（毎日、週1回、月1回）に、またいつでも実行できるレポートタスク機能を有すること。			
	ハードウェア要件			
①	ハードウェア要件は、本要件定義書の第2－2 ストレージ機器を参照すること。			
エ	ジョブ管理機能			
	ソフトウェア要件			
①	各種ジョブに関して、スケジュールの登録及び管理機能を有すること。			
②	ジョブの再実行、強制終了、保留等のジョブ操作が可能であること。			
③	スケジュールに基づいたジョブの自動実行結果を監視する機能を有すること。			
④	CSV 形式等でジョブの一括登録が可能であること。			
⑤	サーバ間におけるジョブの連携が可能であること。			
⑥	複数ジョブの連携が可能であること。			
⑦	ジョブの分岐処理が可能であり、前段ジョブの実行結果に伴った後続ジョブを設定できること。			
⑧	複数のサーバに分散されているスケジュール実行状況を一つの監視画面で監視できること。			
⑨	ジョブの開始及び終了が遅延した場合に検知して通報できること。			
⑩	ハードウェア要件は、本要件定義書の第2－2 ストレージ機器を参照すること。			
	ハードウェア要件			
①	ソフトウェア要件を参照すること。			
4	ログ管理サービス			
(1)	概要			
	ログ管理サービスは、総務省LANサービスを構成する機器が出力したログ（認証ログ、アクセスログ、セキュリティログ、利用状況ログ、LAN端末の操作ログ等）を収集し、運用保守及びインシデント対応時に、検索、閲覧及び分析するためのサービスである。 ・運用要員は、運用保守及びインシデント対応時に、必要な各種総務省LANサービスのログ（認証ログ、アクセスログ、セキュリティログ、利用状況ログ、LAN端末の操作ログ等）の情報を収集、検索、分析する。 ・各種ログを自動的に収集し、一定期間保管する。 具体的要件について、以下に記載する。			
(2)	構築要件			
①	運用保守・セキュリティ等の面から必要と思われるログを取得・保全すること。			
②	ログは、1年以上保管すること。			
③	保管したログは、検索、閲覧が可能なこと。			
④	画面から容易に各種ログの検索が行え、誤操作によるファイル削除やウイルス感染の原因を前後の操作を確認できること。			

別紙1－2　要件定義書（サービス・機器）

項番号	内容	提案内容	補足資料	記載箇所
(3) 機器等要件				
ア　統合ログ収集機能				
ソフトウェア要件				
①	総務省 LAN を構成するサーバ、ネットワーク機器、アプライアンス機器のログ情報を自動的に収集・保存すること。また、これらの機器のログ収集に必要な台数のサーバを構成すること。			
②	収集したログ情報は、閲覧や検索ができること。			
③	ログデータは、1年間以上の長期保管ができること。			
④	収集したログから、日、週、月ごと等でレポートを出力することが可能であること。			
⑤	集計した結果は、 PDF、HTML、CSV 形式等主管課がわかりやすい形式で提出されること。			
⑥	正規表現を用いたログの検索が可能であること。			
ハードウェア要件				
①	ハードウェア要件は、本要件定義書の第2－2 ストレージ機器を参照すること。			
イ　LAN 端末操作ログ収集機能				
ソフトウェア要件				
①	全 LAN 端末の操作ログ、印刷ログ、ファイルの利用状況、アプリケーションの稼働状況等を収集、検索、分析可能であること。			
②	誤操作によるファイル削除やウイルス感染の原因を前後の操作から確認できること。			
③	ファイル共有サービスの利用情報から不正なファイルアクセスを管理できること。ファイルのオープン・クローズも記録できること。			
④	LAN 端末によるドメインへのログオン・ログオフの管理ができること。			
ハードウェア要件				
①	ハードウェア要件は、本要件定義書の第2－2 ストレージ機器を参照すること。			
5　バックアップサービス				
(1) 概要				
	総務省LANの可用性を維持するために、バックアップサービスを提供する。障害発生や操作ミス等でデータが消失又は破損した場合に復旧可能とし、また、災害発生時にサービスを継続利用可能とする。自動でバックアップを取得し、一定期間保管する。 具体的要件について、以下に記載する。			
(2) 構築要件				
①	各種サーバのバックアップは、ローカルバックアップ、遠隔地バックアップともに実施すること。			
②	組織用ファイル共有サービスのデータは、ローカルバックアップ、遠隔地バックアップを行うこと。			
③	個人用ファイル共有サービスのデータは、ローカルバックアップを行うこと。			
④	バックアップ格納媒体は、バックアップの速度、データ量、セキュリティ、リカバリ等を考慮すること。			
⑤	バックアップは、障害の種類（大規模災害含む）、地域、データ量、通信回線、復旧方法等、様々な側面を考慮すること。			
⑥	バックアップの間隔・世代管理・ディザスタリカバリとの連携に当たり、データの種類と特性を考慮すること。ただし、以下の要件を満たすよう構成すること。 ・ファイル共有サービスのバックアップは、毎日行い、7世代分保有すること。 ・各種サーバのバックアップは、毎週行い、7世代分保有すること。			
⑦	バックアップ運用を自動的に制御すること。			
⑧	システム領域のリストアは、OSの再セットアップすることなく復旧を可能となるよう構成すること。			
⑨	ファイル単位のリストアを可能となるよう構成すること。			
⑩	遠隔地にバックアップデータを送る場合は、総務省LANサービスへの影響を考慮し、バックアップ方法を検討すること。			

別紙1－2　要件定義書（サービス・機器）

項番号	内容	提案内容	補足資料	記載箇所
(3) 機器等要件				
ア　バックアップ機能				
ソフトウェア要件				
①	ハードウェア要件を参照すること。			
ハードウェア要件				
①	システムバックアップ及びデータバックアップを取得することが可能であること。			
②	Linux/Windows/仮想マシンのバックアップを実現すること。			
③	拠点を除きバックアップは、データの格納されているストレージ装置とは別の外部筐体（別シャーシ等）に行うこと。			
④	差分ブロック転送によるバックアップが可能であること。			
⑤	重複排除されたデータをバックアップできること。			
⑥	ハードウェア要件は、本要件定義書の第2－2 ストレージ機器を参照すること。			
6　電源管理サービス				
(1) 概要				
	電源障害・法定停電・災害時等に機器を安全に停止しかつ機器の起動制御を行うため、電源管理サービスを提供する。自動でシステム停止・起動を行う。 具体的要件について、以下に記載する。			
(2) 構築要件				
①	停電発生時にシステムを安全に停止する機能の実装を行うこと。			
②	物理サーバ、仮想サーバ、ネットワーク、アプライアンス製品等の安全な停止・起動を実現すること。			
③	LAN端末の省電力対策を実現するため、電源設定（電源ON、OFF、再起動、スリープスタンバイ、休止状態等）が可能であること。スケジュールによる実行も含め管理できること。			
(3) 機器等要件				
ア　電源管理機能				
ソフトウェア要件				
①	リモートから電源使用量の監視が可能であること。			
②	電流の閾値が超過又は復旧した場合、運用管理サービスやメールサービスと連携し、管理者へ通知を行うことが可能であること。			
③	サーバ機器の消費電力監視機能を有し、過去1ヶ月以上のデータをグラフ表示できること。			
④	サーバ機器の電力の閾値監視や動的な電力制御を行う機能が搭載されていること。			
⑤	スケジュールシャットダウンに対応した機能を有すること。			
ハードウェア要件				
①	経年劣化によるバッテリーの容量低下を管理者に通知する機能を有すること。			
②	稼働中に自己診断を行い、異常の際は、管理者に通知する機能があること。			

別紙1－2　要件定義書（サービス・機器）

項番号	内容	提案内容	補足資料	記載箇所
7　資源管理サービス				
(1) 概要				
	資源管理サービスは、管理対象機器のハードウェア情報、ソフトウェア情報、ライセンス情報等の情報収集や、ソフトウェア配付、セキュリティパッチ等の配付、LAN端末接続デバイスの制御、各種設定情報の変更等を一括管理するサービスである。 ・LAN端末にソフトウェア（セキュリティパッチ等）をインストールする必要が発生した場合、ソフトウェア（セキュリティパッチ等）の配信を制御できる。 ・職員は、クライアント資源管理サービスを利用し、業務に必要なソフトウェアを任意にLAN端末にインストールすることができる。 ・総務省が配備した記憶媒体（DVD、セキュリティUSBメモリ）以外の記憶媒体をLAN端末に接続した際に、利用制限できる。 具体的要件について、以下に記載する。			
(2) 構築要件				
	① 各種サーバ、ネットワーク機器、LAN端末等のインベントリ情報、ライセンス等の資源管理を一元的に行うこと。			
	② 各種サーバ、LAN端末及びテレワークサービスの仮想デスクトップ環境に対し、ソフトウェア配付、セキュリティパッチ等の配付、LAN端末接続デバイスの制御、各種設定情報の変更等を一括管理して行うこと。			
	③ セキュリティパッチ等の適用状況を確認し、ポリシー違反を含む情報を検索できること。			
	④ LAN端末のアプリケーションの稼働状況やサーバへのアクセス情報を一元的に管理すること。			
	⑤ セキュリティパッチのダウンロードを行う場合、外部サイトに接続できること。			
	⑥ ソフトウェア、セキュリティパッチ配布は、サーバ及びネットワークの負荷を軽減させる構成とすること。			
(3) 機器等要件				
ア　資源管理機能				
ソフトウェア要件				
	① 規模・性能要件に記載したLAN端末数、プリンタ数を管理可能であること。外部接続端末等の機器も含めて管理できること。			
	② 1万台の機器を管理できる構成とすること。			
	③ 職員が資源管理サービスを利用し、業務に必要なソフトウェアをインストールできること。			
	④ ソフトウェア配布の中継機能を有すること。			
	⑤ コンピュータ名、CPU情報、メモリ容量、ハードディスク容量、ハードディスク空き容量、IPアドレス、MACアドレス等のハードウェアやOS、ソフトウェア情報を自動収集する機能を有すること。本要件はサーバも対象となるため、対応すること。			
	⑥ アプリケーションのインストール数を把握して、ライセンス管理を行える機能を有すること。			
	⑦ ハードウェア、ソフトウェア、ライセンス管理用に取得した情報やその他任意項目等を持つ台帳作成機能を有すること。			
	⑧ アプリケーションの稼働状況を把握するために、各LAN端末の稼働状況の記録（コンピュータ名、ユーザ名、アプリケーション名等）を自動収集し、端末や部署別に集計する機能を有すること。			
	⑨ 業務に必要のないアプリケーションの起動やインストールを禁止する機能を有すること。			
	⑩ 収集情報に対して、管理者用のレポート作成機能や資産管理データを検索する機能を有すること。			
	⑪ LAN端末ごとに、記憶媒体（CD、DVD、FD、USBメモリ等）を禁止する機能を有すること。また、読み込みのみ許可する設定が可能であること。			
	⑫ 運用上のルール（禁止アプリケーション起動、禁止デバイスの使用等）に違反した場合、違反内容を管理者や該当するLAN端末に通知する機能を有すること。			
	⑬ 検索を行う際には複数の条件を一度に指定して検索ができること。			
	⑭ ポリシー違反の情報だけを検索できること。			
	⑮ ソフトウェアの配布実行は、強制実行、LAN端末の使用者による実行のどちらも設定できること。			

項番号	内容	提案内容	補足資料	記載箇所
	⑯ セキュリティ傾向を把握できるようにするため、登録したポリシーに基づき、セキュリティ違反数等の推移を集計しまとめて表示できること。			
	ハードウェア要件			
	① ハードウェア要件は、本要件定義書の第2－2 ストレージ機器を参照すること。			
8	モバイルデバイス管理サービス			
(1)	概要			
	モバイルデバイス管理サービスは、職員が省内外で利用するタブレット型端末のハードウェア情報、ソフトウェア情報、利用状況を自動で収集することにより、運用要員が一元的に管理を行うためのサービスである。 タブレット型端末に盗難や紛失が発生した場合には、リモートワイプを実行することにより情報漏えいを防ぐ。 また、OSやアプリケーションの導入や更新の作業にも利用する。 具体的要件について、以下に記載する。			
(2)	構築要件			
	① 省内及び省外から安全に総務省LANのサービスを利用できるよう構成すること。			
	② タブレット型端末を220台以上管理できる構成とすること。			
	③ タブレット型端末の利用状況やポリシー遵守の状況が得られるように構成すること。			
	④ 盗難や紛失等の事故が発生した際には、速やかにリモートワイプを実行できるよう構成すること。			
	⑤ 初期の導入設定に加え、故障交換や構成見直し等による設定作業を容易にかつ画一的に行えるよう構成すること。			
	⑥ 管理用機器を準備すること。			
(3)	機器等要件			
ア	モバイルデバイス管理機能			
	ソフトウェア要件			
	① 複数の端末に対して、一括でアカウントやポリシーの設定を行う機能を有すること。			
	② プロファイルを適用することにより、端末上で利用可能な機能やアプリケーションを制限する機能を有すること。			
	③ プロファイルやアプリケーションは遠隔からタブレット型端末に投入できること。			
	④ 端末のリモートワイプ、リモートロックが可能であること。			
	⑤ ユーザ自身からもリモートワイプ、リモートロックが可能であること。			
	⑥ 端末の状態や利用状況、コンプライアンス遵守の状況を取得する機能を有すること。			
	⑦ Jailbreak端末の発見が可能であること。			
	⑧ コンプライアンス違反の端末に対して、通知やワイプ等のアクションを設定することが可能であること。			
	⑨ 端末の所在確認のための位置情報を提示する機能を有すること。			
	⑩ 位置情報を時系列的に表示することにより、端末の移動履歴を確認することが可能であること。			
	⑪ 端末の位置情報に基づいて、適切なプロファイルを切り替えて適用できる機能を有すること。			
	⑫ 利用する組織、グループ、ユーザを登録し、対象とする端末や適用するポリシー等と結び付けられること。			
	⑬ ログインするユーザに応じて環境を切り替えることで、複数のユーザが端末を共有できること。			
	⑭ タブレット型端末上で稼働するMDMエージェントと管理サーバ間の通信は暗号化されること。			
	⑮ Apple社の提供する構成ユーティリティツール又は構成ユーティリティプログラムと関連付けられること。			
	⑯ 次の条件を満たす場合、SaaS型のサービス提供も可とする。 ・日本国内データセンタを利用しており、利用データは全て国内に保存されること。 ・広域災害を想定した設備を有しており、各データセンタは350km以上離れた場所にあること。 ・データセンタに格納するデータは暗号化すること。			
	⑰ ポリシー遵守の状態を逐次監視し、ポリシー違反を検出したときには速やかにアラートを発する機能を有すること。			
	⑱ 端末側から削除できない固定の初期プロファイルをインストールする機能を有すること。			
	⑲ 管理を容易にするために、連続する番号を自動的に振り、連番を含む名前を設定する機能を有すること。			

別紙1－2　要件定義書（サービス・機器）

項番号	内容	提案内容	補足資料	記載箇所
	⑳ 端末の管理情報として、シリアル番号、ハードウェアID、MACアドレス等の情報をファイルに書き出す機能を有すること。			
	㉑ 端末を初期化する機能を有すること。			
	㉒ 情報漏えい防止のために、管理対象の端末を特定のコンピュータ以外に接続できなくする機能を有すること。			
	㉓ 指定以外のアプリケーションをタブレット型端末にインストールできないようにする機能を有すること。			
	㉔ 同時に複数の端末に対して、OSのアップデートやアプリケーションのインストールを行う機能を有すること。			
	㉕ 端末のバックアップを取得し、端末に復元する機能を有すること。			
	㉖ 端末にiOSの監視モードを設定できること。			
	ハードウェア要件			
	① 管理用機器は、上記ソフトウェア要件を満たすものを用意すること。			
9　シンクライアント管理サービス				
（1）概要				
	シンクライアント管理サービスは、テレワークで利用するシンクライアントのイメージの管理、セットアップ処理を行うサービスである。 具体的要件について、以下に記載する。			
（2）構築要件				
	① シンクライアントのイメージを管理を一元的に管理できること。			
	② シンクライアントへのイメージ展開を自動的に実施できること。			
	③ イメージへのアップデートの適用が管理できること。			
	④ セットアップと同時に暗号化処理を行うことができること。			
（3）機器等要件				
ア　シンクライアント管理機能				
	ソフトウェア要件			
	① シンクライアントの情報を管理できること。			
	② 管理用のGUIインターフェースを備えること。			
	③ サービス提供以外の機器からアクセスが可能であること。			
	ハードウェア要件			
	① ハードウェア要件は、本要件定義書の第２－２ ストレージ機器を参照すること。			
第６　その他機器基盤				
1　検証環境				
（1）概要				
	サーバ、ストレージ、ネットワーク機器の保守作業や障害の原因調査作業を実施する際に、総務省LANに及ぼす影響とその手順を確認するため、検証環境を提供する。 具体的要件について、以下に記載する。			
（2）構築要件				
	① 検証環境のバックアップを取得可能な構成であること。			
	② サーバ用のOS環境を容易に作成可能であり、有効活用できるように構成されていること。			
	③ 総務省LANの検証が実施できる環境を準備すること。			
（3）機器等要件				
（ア）コアスイッチ(検証用)要件				
	ソフトウェア要件			
	① レイヤ 2 及びレイヤ 3 のスイッチングを行えること。また、ハードウェアによる IPv4及び IPv6 のルーティングに対応すること。			
	② DHCP リレー機能を有すること。			

別紙1－2　要件定義書（サービス・機器）

項番号	内容	提案内容	補足資料	記載箇所
	③ スパニングツリー機能として、IEEE802.1d、IEEE802.1s、IEEE802.1w 又はこれらと同等の機能を有すること。			
	④ IEEE802.1p の COS、TOS 及び DSCP の書換え、書き込み、DSCP に基づく優先制御が可能であること。			
	⑤ ACL 又は同等の方式によるアクセス制限が行えること。			
	⑥ 信頼できない DHCP メッセージをフィルタリングできる機能を有すること。			
	⑦ IEEE802.1x に準拠した認証が行えること。			
	⑧ IEEE802.3ah/UDLD により、片方向リンクを検出することが可能であること。			
	⑨ データフローの送信元 IP アドレスと送信先 IP アドレスに基づいた統計情報、プロトコル情報を収集することが可能であること。			
	⑩ ポートに対しての自動障害検知機能及び自動復帰機能を有すること。			
	⑪ 指定したイベントが発生した際に、電子メールの通知等が自動で行えること。			
	⑫ ブロードキャスト及びマルチキャストの流量を制限する機能を持つこと。			
	ハードウェア要件			
	① シャーシ型筐体又はボックス型筐体であること。			
	② 消費電力が 110W 以下であること。			
	③ 90Gbps 以上のスイッチング容量を有すること。			
	④ 65.5Mpps 以上のパケット処理能力を有すること。			
	⑤ 100BASE-TX／1000BASE-T を 24 ポート以上有すること。			
	⑥ 拡張により、1000BASE の SFP を 4 ポート以上、又は、10GBASE の SFP を 2 ポート以上搭載できること。			
	（イ） エッジスイッチ(検証用)要件			
	ソフトウェア要件			
	① ボックス型筐体であること。			
	② 消費電力が40W以下であること。			
	③ 16Gbps 以上のスイッチング容量を有すること。			
	④ 6.5Mpps 以上のパケット処理能力を有すること。			
	⑤ 100BASE-TX を 24 ポート以上有すること。			
	⑥ 100BASE-TX／1000BASE-T と SFP の排他ポートを 2 ポート以上有すること。			
	ハードウェア要件			
	① レイヤ 2 のスイッチングを行えること。			
	② スパニングツリー機能として、IEEE802.1d、IEEE802.1s、IEEE802.1w 又はこれらと同等の機能を有すること。			
	③ IEEE802.3ah/UDLD により、片方向リンクを検出することが可能であること。			
	④ ポートに対しての自動障害検知機能及び自動復帰機能を有すること。			
	⑤ ブロードキャスト及びマルチキャストの流量を制限する機能を持つこと。			
	（ウ） ブレード型サーバ(検証用)要件			
	ソフトウェア要件			
	① Microsoft Windows Server 2012 R2、RedHat EnterpriseLinux 6及び7が動作可能であること。			
	② 仮想化を行う場合は、ハイパーバイザ型の仮想基盤を採用すること。			
	③ 検証作業が実施できるようライセンスを適切に準備すること。			
	ハードウェア要件			
	① 本番機と同様のスペックを持つシャーシによって構成すること。			
	② 本番機と同様のスペックを持つブレード3枚以上によって構成すること。			
	③ 1Gbpsのインターフェイスを12個以上有すること。			
	④ 10Gbpsのインターフェイスを16個以上有すること。			

別紙1－2　要件定義書（サービス・機器）

項番号	内容	提案内容	補足資料	記載箇所
	（エ）　回線シミュレータ要件			
	ソフトウェア要件			
	① WebUIを用いた設定機能を有すること。			
	ハードウェア要件			
	① 遅延の発生やパケットロスを再現する機能を有すること。			
	② IPv6に対応していること。			
2 運用業務環境				
（1）概要				
	運用業務環境は、運用要員が日常の運用業務に使用する設備環境である。 運用要員は、利用する機能ごとの個別環境を利用する。 個別環境には、一般執務環境、サーバ接続用環境、遠隔操作用環境がある。 運用要員の共有環境として、メンテナンス用端末、地方監視用サーバ、キッティングサーバがある。 具体的要件について、以下に記載する。			
（2）構築要件				
ア　個別環境				
	① 運用要員が日常業務で使用するためのアプリケーションを導入した一般執務環境を準備すること。			
	② 一般執務環境は、インターネット閲覧、メールの機能を利用できるよう構成すること。			
	③ サーバに接続するためのサーバ接続用環境を準備すること。インターネット閲覧、メールは利用不可とし外部へのアクセスを制限すること。			
	④ 運用支援サービスの一環として、職員のLAN端末へリモート接続するための遠隔操作用環境を準備すること。遠隔操作用環境では、リモート接続のみ許可すること。			
	⑤ 外部監視室オペレータが操作を行うための環境を準備すること。			
	⑥ DRオペレータが操作する環境を準備すること。			
	⑦ 運用のための情報を格納する共有ファイル領域を準備すること。			
イ　共有環境				
	① ストレージ又はスイッチをメンテナンスするために、対象機器と端末をシリアルケーブルで接続するメンテナンス用端末を準備すること。			
	② 地方の機器の死活監視や定時通知のために、地方監視サーバを準備すること。監視状況をディスプレイに表示すること。			
	③ LAN端末の再セットアップに必要となるキッティングサーバを準備すること。			
	④ キッティングサーバは、冗長構成とすること。			
	⑤ 監視状況を運用員全員がすぐに確認できるような環境を準備すること。			
（3）機器等要件				
ア　個別環境				
	ソフトウェア要件			
	① Windows 8.1以上のOSであること。			
	② Microsoft Office 2013以上が利用可能なこと。			
	③ Adobe Acrobatを利用可能なこと。			
	④ USB機器の使用禁止設定が可能なセキュリティソフトを添付していること。			
	⑤ 資源管理サービスの管理クライアントが動作すること。			
	ハードウェア要件			
	① フルHD以上の解像度で表示可能なこと。			
	② CPUは2.4GHz 4コア以上とする。			
	③ メインメモリは、8GB以上とする。			
	④ 記憶領域は、250GB以上とする。			

項番号	内容	提案内容	補足資料	記載箇所
	⑤ 共有ファイル領域は、3TB以上とする。			
	イ　共有環境（メンテナンス用端末）			
	ソフトウェア要件			
	① メンテナンス用端末は、Windows 7以上のOSであること。			
	ハードウェア要件			
	① メンテナンス用端末には、RS-232Cシリアル接続可能なインターフェースを持つこと。			
	② メンテナンス用端末は、ノート型であり、本体重量は1.2kg以下であること。			
	ウ　共有環境（地方監視用サーバ）			
	ソフトウェア要件			
	① 地方監視用サーバは、Windows Server 2012 R2 以上のOSであること。			
	ハードウェア要件			
	① 地方監視用サーバは、XEON E5 2630v3以上の性能を持つこと。			
	② 地方監視用サーバは、メインメモリを32GB以上搭載すること。			
	③ 地方監視用サーバは、記憶領域を1TB以上持つこと。			
	エ　共有環境（キッティングサーバ）			
	ソフトウェア要件			
	① キッティングサーバは、Windows Server 2012 R2 以上のOSであること。			
	ハードウェア要件			
	① キッティングサーバは、1000Base-Tポートを2つ以上装備していること。			
	② キッティングサーバは、XEON E5 2630v3以上の性能を持つこと。			
	③ キッティングサーバは、メインメモリを32GB以上搭載すること。			
	④ キッティングサーバは、記憶領域を2TB以上持つこと。			
3	KVM			
(1)	概要			
	サーバ等の機器に対しコンソールからの操作を可能とするため、操作環境を提供する。 具体的要件について、以下に記載する。			
(2)	構築要件			
	① 全サーバ機器に対して準備すること。			
	② 本省・ディザスタリカバリサイトは必要台数を用意し、その他の拠点においては各拠点1台ずつ配備すること。			
	③ KVMスイッチで、統合管理を可とする。			
	④ KVMスイッチが必要な場合は、KVMケーブルも含めて必要台数用意すること。			
(3)	機器等要件			
	ソフトウェア要件			
	① KVMスイッチは、切替時の表示名をサーバ名に変更することが可能であること。			
	ハードウェア要件			
	① 1U以内であること。			
	② キーボードは日本語配列であること。			
	③ ポインティングデバイスを有すること。			
	④ 17インチ以上のモニタを有すること。			
	⑤ モニタはSXGA以上の解像度を有すること。			
	⑥ USB接続が可能であること。			

別紙1－2　要件定義書（サービス・機器）

項番号	内容	提案内容	補足資料	記載箇所
4　UPS				
(1) 概要				
	機器に安定した電源を供給し、電源供給が途絶えた際に一定時間電源を供給するため、UPSを準備する。 また、停電の際安全に機器を停止するため、電源管理機能と連携する。 具体的要件について、以下に記載する。			
(2) 構築要件				
	① 電源保護対象は、本調達のサーバ、ストレージ、ネットワーク、セキュリティ、運用管理機器とすること。			
	② 電源容量は、給電停止から5分間経過後、安全にシャットダウンできるために十分な容量であること。			
	③ リモートでUPSの状態が確認・制御できるよう構成すること。			
(3) 機器等要件				
	ソフトウェア要件			
	① 電源管理機能と連携可能であること。			
	② ネットワーク経由でアクセスできること。			
	ハードウェア要件			
	① 常時インバータタイプであること。			
	② バッテリモジュールの活性交換が可能であること。			
	③ 本省では、単相AC100V及び単相AC200Vの入力機器を接続できること。			
	④ 拠点では、単相AC100V、周波数は50/60Hzに対応すること。			
	⑤ 経年劣化によるバッテリーの容量低下を管理者に通知する機能を有すること。			
	⑥ 稼働中に自己診断を行い、異常の際は、管理者に通知する機能があること。			
	⑦ LANインターフェースを有すること。			
5　LAN端末マスタ				
(1) 概要				
	LAN端末マスタは、総務省LAN端末をキッティングする際に基となるイメージであり、総務省職員が通常業務で利用するソフトウェアから構成される。 LAN端末の機種ごとに準備されていること。 具体的要件について、以下に記載する。			
(2) 構築要件				
	① 既存のLAN端末のマスタを作成し、対象となる全LAN端末に導入すること。			
	② 拠点に設置されているLAN端末に対しては、現地に赴き展開作業を行うこと。			
	③ LAN端末マスタのOSは、Microsoft Windows 7 Enterprise 64bit とする。ただし、業務システム都合により、別のOSが必要な場合は、これを準備すること。			
	④ LAN端末マスタの導入作業時に、ユーザデータを移行するための環境を提供すること。			
	⑤ テレワーク用として総務省外へ持ち出して利用する場合を考慮した構成とすること。			
	⑥ LAN端末に対して提供される総務省LANの全てのサービスが利用できること。			
	⑦ LAN端末の記憶領域は、現行と同等以上の強度で暗号化すること。			
	⑧ 業務システムで導入が必要ソフトウェアについては、業務システム担当者及び現行運用業者と調整すること。			
(3) 機器等要件				
	ソフトウェア要件			
	① 本調達によって必要となるソフトウェアを導入すること。			
	② Microsoft Office 2013 が動作すること。			
	③ その他、現行のソフトウェアの導入要否を検討すること。			

別紙1－2　要件定義書（サービス・機器）

項番号	内容	提案内容	補足資料	記載箇所
	④ OS及びOSの基本機能はサポート期間内のものを選定すること。			
	⑤ できる限りWindows 7 Enterprise 64bitに対応したソフトウェアを選定すること。Windows 7 Enterprise 64bitで動作しないソフトウェアを利用する場合は、個別に検討すること。			
	ハードウェア要件			
	① 端末本体については、別調達のため、本項に記載しない。			
6　仮想デスクトップマスタ				
(1) 概要				
	仮想デスクトップマスタは、仮想デスクトップを複製する際の基となるイメージであり、総務省職員が通常業務で利用するソフトウェアから構成される。 仮想デスクトップの環境ごとに準備されていること。 具体的要件について、以下に記載する。			
(2) 構築要件				
	① 仮想デスクトップのマスタを仮想デスクトップ環境ごとに作成し、必要数分複製すること。			
	② 仮想デスクトップマスタのOSは、Microsoft Windows 7 Enterprise 64bit とする。ただし、業務システム都合により、別のOSが必要な場合は、これを準備すること。			
	③ マスタの導入作業時に、ユーザデータを移行するための環境を提供すること。			
	④ LAN端末と同様に、総務省LANの全てのサービスが利用できること。			
	⑤ 業務システムで導入が必要なソフトウェアについては、業務システム担当者及び現行運用業者と調整すること。ただし、システム領域を占有する仮想デスクトップに限る。			
(3) 機器等要件				
	ソフトウェア要件			
	① 本調達によって必要となるソフトウェアを導入すること。			
	② Microsoft Office 2013 が動作すること。			
	③ その他、現行のソフトウェアの導入要否を検討すること。			
	④ OS及びOSの基本機能はサポート期間内のものを選定すること。			
	⑤ できる限りWindows 7 Enterprise 64bitに対応したソフトウェアを選定すること。Windows 7 Enterprise 64bitで動作しないソフトウェアを利用する場合は、個別に検討すること。			
	ハードウェア要件			
	① ハードウェア要件は、本要件定義書の第2－1 サーバ機器及び第2－2 ストレージ機器を参照すること。			
第7　ネットワーク基盤				
(1) 概要				
	ネットワーク基盤は、次の区分によって構成される。 1. 本省LAN: 2. 拠点LAN 3. ネットワークサービス 4. 無線LAN 5. インターネット接続回線 6. 本省WAN 7. 拠点WAN 8. 外部監視室用回線			

別紙1－2　要件定義書（サービス・機器）

項番号	内容	提案内容	補足資料	記載箇所
1　本省LAN				
(1) 概要				
	本省LANは、総務省LAN全体にネットワークサービスを提供し、総務省職員が総務省ＬＡＮサービスを利用するため、本省ＬＡＮを提供する。 具体的要件について、以下に記載する。			
(2) 構築要件				
ア　共通				
	① バックボーンネットワーク、フロアネットワーク、サーバネットワーク、監視ネットワーク、運用ネットワーク、業務システム接続ネットワーク、総務省WAN接続ネットワーク、インターネット接続ネットワーク、政府共通ネットワーク接続ネットワーク、仮想ブラウザネットワークを構成すること。			
	② 利用用途に応じて、以下のネットワーク設計を行うこと。 ・ルーティング設定 ・アドレス空間設計 ・VLAN設計 ・セキュリティ設計 ・可用性設計			
	③ L2ループやブロードキャストストームによるサービス障害が発生しないよう考慮した設計とすること。			
イ　バックボーンネットワーク				
	① バックボーンネットワークは、総務省LANにおける基幹となるネットワークとして、他のネットワークを相互接続する役割を持つ。			
	② コアスイッチは、2台以上導入し、冗長構成とすること。			
	③ コアスイッチ内の制御用モジュール及びインターフェースモジュールを冗長構成とすること。なお、冗長構成は複数スイッチの仮想化を利用してもよい。			
	④ コアスイッチへの接続はすべて冗長接続とすること。			
	⑤ コアスイッチ間は、40Gbps以上で接続すること。			
	⑥ 冗長化されている部分は、ケーブルや機器等障害による通信断時に自動的に切換え可能な構成とすること。			
	⑦ コアスイッチは、中央合同庁舎第2号館B1F総務省サーバ室に設置すること。			
	⑧ コアスイッチは、将来の拡張を考慮し、ポート数に余裕を持たせること。			
	⑨ コアスイッチの制御機能は冗長化を実施し、障害時は自動切り替えとすることで、可能な限りサービスを継続できる構成とすること。			
ウ　フロアネットワーク				
	① フロアネットワークは、フロアスイッチと、配下に接続されるエッジスイッチにより構成され、LAN端末やプリンタ等を収容する役割を持つ。			
	② フロアスイッチは、2台以上導入し、冗長構成とすること。			
	③ エッジスイッチはシングル構成とし、経路冗長で構成すること。			
	④ コアスイッチとフロアスイッチの間は2Gbps以上の多重リンクとすること。また、将来のトラフィック増加を想定し、10Gbps以上にも対応できるようにすること。			
	⑤ フロアスイッチとエッジスイッチの間は2Gbps以上の多重リンクとすること。			
	⑥ フロアスイッチは、将来の拡張を考慮し、ポート数に余裕を持たせること。			
	⑦ フロアスイッチは、中央合同庁舎第2号館3F～11F東西EPS及びB1F総務省サーバ室に設置すること。			
	⑧ エッジスイッチは、中央合同庁舎第2号館1F西EPS及び3F～11F東西EPSに設置すること。なお、1F西EPSへは3F西EPSから接続すること。			

別紙1－2　要件定義書（サービス・機器）

項番号	内容	提案内容	補足資料	記載箇所
エ　サーバネットワーク				
	① サーバネットワークは、総務省LANのサービスを提供するための主要なサーバ機器を接続する役割を持つ。			
	② サーバネットワークは、コアスイッチと20Gbps以上で接続すること。			
	③ サーバネットワークを構成するネットワーク機器は、冗長化すること。			
	④ 仮想化するサーバ等との接続は10Gbps以上とし、冗長化すること。			
	⑤ 物理サーバやアプライアンス製品との接続は、1Gbps以上とし、冗長化すること。			
	⑥ 冗長化されている部分は、ケーブルや機器等障害による通信断時に自動的に切換え可能な構成とすること。			
	⑦ サービスごとに適切な負荷分散を実施できるよう負荷分散装置を導入すること。			
オ　監視ネットワーク				
	① 監視ネットワークは、総務省LAN の運用を行うための機器を接続し、原則としてサービスを提供するためのネットワークを介さずに主要なネットワーク機器、サーバ機器の監視及びログの収集等を行う役割を持つ。			
	② 監視ネットワークは、コアスイッチと2Gbps以上で接続すること。			
	③ 管理LANスイッチは、冗長構成とすること。			
	④ 冗長化されている部分は、ケーブルや機器等障害による通信断時に自動的に切換え可能な構成とすること。			
	⑤ 管理LANスイッチ～監視スイッチ間は2Gbps以上で接続する。また、将来のトラフィック増加を想定し、10Gbps以上にも対応可能なこと。			
	⑥ LANを制御する管理LANスイッチは、将来の拡張を考慮し、ポート数に余裕を持たせること。			
	⑦ 外部監視室との接続点では、アクセス制御を行うこと。			
カ　運用ネットワーク				
	① 運用ネットワークは、運用員がサーバ・ネットワーク機器へ運用管理上のアクセスを行うための端末を収容する役割を持つ。			
	② 運用ネットワークは、サーバスイッチと2Gbps以上で接続すること。			
	③ 運用スイッチは、冗長構成とすること。			
	④ 冗長化されている部分は、ケーブルや機器等障害による通信断時に自動的に切換え可能な構成とすること。			
	⑤ 将来の拡張を考慮し、ポート数に十分な余裕を持たせること。			
キ　業務システム接続ネットワーク				
	① 業務システム接続ネットワークは、共通基盤支援システム、電気通信行政情報システム（STARS）等の業務システムを収容する役割を持つ。			
	② 業務システム接続ネットワークは、コアスイッチと2Gbps以上で接続すること。			
	③ 現行接続されている業務システムを、継続して利用可能とすること。			
	④ 業務システム接続ネットワークを構成するネットワーク機器は、冗長化すること。			
	⑤ 冗長化されている部分は、ケーブルや機器等障害による通信断時に自動的に切換え可能な構成とすること。			
	⑥ 業務システムの接続は、将来的に二重化接続することを可能とすること。			
	⑦ 複数の業務システムを集約し、それぞれに対してアクセス制御を実施できるよう業務システム用ファイアウォールを導入すること。			
	⑧ 将来的な業務システムの増加にも対応できること。			

別紙1－2　要件定義書（サービス・機器）

項番号	内容	提案内容	補足資料	記載箇所
ク	総務省 WAN 接続ネットワーク			
①	総務省WAN接続ネットワークは、外部拠点、地方支分部局等及びディザスタリカバリサイトと接続する回線を収容した上で本省LANと接続する役割を持つ。			
②	総務省WAN接続ネットワークは、コアスイッチと2Gbps以上で接続すること。			
③	総務省WAN接続ネットワークを構成するネットワーク機器は、冗長化すること。			
④	冗長化されている部分は、ケーブルや機器、WAN等障害による通信断時に自動的に切換え可能な構成とすること。			
⑤	本省WAN接続スイッチは、将来の拡張を考慮し、ポート数に余裕を持たせること。			
ケ	インターネット接続ネットワーク			
①	インターネット接続ネットワークは、総務省LANとインターネットを接続する役割を持つ。			
②	インターネット接続ネットワークは、コアスイッチと2Gbps以上で接続すること。			
③	インターネット接続ネットワークを構成するネットワーク機器は、冗長化すること。			
④	冗長化されている部分は、ケーブルや機器、インターネット等障害による通信断時に自動的に切換え可能な構成とすること。			
⑤	異なる製造者の製品を用いた2段階のアクセス制御を行うこと。			
⑥	インターネット接続DMZスイッチは、将来の拡張を考慮し、ポート数に余裕を持たせること。			
⑦	DMZ内にあるサービスごとに適切な負荷分散を実施できるよう負荷分散装置を導入すること。			
コ	政府共通ネットワーク接続ネットワーク			
①	政府共通ネットワーク接続ネットワークは、総務省LANと政府共通プラットフォームを接続するための役割を持つ。			
②	政府共通ネットワーク接続ネットワークは、コアスイッチと2Gbps以上で接続すること。			
③	政府共通ネットワーク接続ネットワークを構成するネットワーク機器は、冗長化すること。			
④	冗長化されている部分は、ケーブルや機器、政府共通ネットワーク回線二重化サービス等の障害による通信断時に自動的に切換え可能な構成とすること。			
⑤	政府共通ネットワーク接続ネットワークは、政府共通ネットワークが設置するWAN回線接続ルータと政府共通ネットワーク接続スイッチで接続すること。			
⑥ ⑦	現行接続されている業務システムを、継続して利用可能とすること。 将来的に新たな業務システムが接続されることを想定し、拡張性を持たせること。			
⑧	政府共通ネットワークDMZスイッチは、将来の拡張を考慮し、ポート数に余裕を持たせること。			
⑨	政府共通ネットワーク接続,ネットワーク内の業務システムの接続は、二重化することを可能とすること。			
サ	仮想ブラウザネットワーク			
①	仮想ブラウザネットワークは、サーバセグメントと仮想ブラウザネットワークを接続するための役割を持つ。			
②	仮想ブラウザネットワークは、サーバ接続スイッチと1Gbps以上で接続すること。			
③	仮想ブラウザネットワークを構成するネットワーク機器は、冗長化すること。			
④	冗長化されている部分は、ケーブルや機器等障害による通信断時に自動的に切換え可能な構成とすること。			
⑤	仮想ブラウザネットワークで使用するスイッチは、提案する仮想ブラウザサービスの環境に合わせ、適切なポート数、性能を持った機器を提案、導入すること。			
(3)	機器等要件			
ア	共通			
	ソフトウェア要件			
①	ネットワークトポロジーを自動的に検出し、機器の IP アドレスやホスト名、接続機器名等の情報を取得できること。			

別紙1－2　要件定義書（サービス・機器）

項番号	内容	提案内容	補足資料	記載箇所
	ハードウェア要件			
	① 19 インチラックに搭載できること。			
	(ア) コアスイッチ要件			
	ソフトウェア要件			
	①「別添1 拠点回線・機器一覧表」 ④コアスイッチスペック要件一覧のType Ⅰを参照すること。			
	ハードウェア要件			
	①「別添1 拠点回線・機器一覧表」 ④コアスイッチスペック要件一覧のType Ⅰを参照すること。			
	(イ) フロアスイッチ要件			
	ソフトウェア要件			
	①「別添1 拠点回線・機器一覧表」 ⑤フロアスイッチスペック要件一覧のType Ⅰを参照すること。			
	ハードウェア要件			
	①「別添1 拠点回線・機器一覧表」 ⑤フロアスイッチスペック要件一覧のType Ⅰを参照すること。			
	(ウ) エッジスイッチ要件			
	ソフトウェア要件			
	①「別添1 拠点回線・機器一覧表」 ⑥エッジスイッチスペック要件一覧のType Ⅰを参照すること。			
	ハードウェア要件			
	①「別添1 拠点回線・機器一覧表」 ⑥エッジスイッチスペック要件一覧のType Ⅰを参照すること。			
	(エ) サーバ接続スイッチ要件			
	ソフトウェア要件			
	① レイヤ2及びレイヤ3のスイッチングを行えること。また、ハードウェアによるIPv4及びIPv6のルーティングに対応すること。			
	② スパニングツリー機能として、IEEE802.1d、IEEE802.1s、IEEE802.1w又はこれらと同等の機能を有すること。			
	③ IEEE802.1pのCOS、TOS及びDSCPの書換え、書き込み、DSCPに基づく優先制御が可能であること。			
	④ ACL又は同等の方式によるアクセス制限が行えること。			
	⑤ IEEE802.3ah/UDLDにより、片方向リンクを検出することが可能であること。			
	⑥ ポートに対しての自動障害検知機能及び自動復帰機能を有すること。			
	⑦ 指定したイベントが発生した際に、電子メールの通知等が自動で行えること。			
	⑧ ブロードキャスト及びマルチキャストの流量を制限する機能を持つこと。			
	ハードウェア要件			
	① シャーシ型筐体又はボックス型筐体であること。			
	② 電源ユニットを冗長化すること。また、活性交換できること。			
	③ 消費電力が350W以下であること。			
	④ 1.28Tbps以上のスイッチング容量を有すること。			
	⑤ 960Mpps以上のパケット処理能力を有すること。			
	⑥ SFP＋とSFPの排他ポートを48ポート以上、搭載可能であること。			
	(オ) 管理 LAN スイッチ要件			
	ソフトウェア要件			
	① レイヤ2及びレイヤ3のスイッチングを行えること。また、ハードウェアによるIPv4及びIPv6のルーティングに対応すること。			
	② スパニングツリー機能として、IEEE802.1d、IEEE802.1s、IEEE802.1w又はこれらと同等の機能を有すること。			
	③ IEEE802.1pのCOS、TOS及びDSCPの書換え、書き込み、DSCPに基づく優先制御が可能であること。			
	④ ACL又は同等の方式によるアクセス制限が行えること。			
	⑤ IEEE802.3ah/UDLDにより、片方向リンクを検出することが可能であること。			
	⑥ ポートに対しての自動障害検知機能及び自動復帰機能を有すること。			

別紙1－2　要件定義書（サービス・機器）

項番号	内容	提案内容	補足資料	記載箇所
	⑦ 指定したイベントが発生した際に、電子メールの通知等が自動で行えること。			
	⑧ ブロードキャスト及びマルチキャストの流量を制限する機能を持つこと。			
	ハードウェア要件			
	① シャーシ型筐体又はボックス型筐体であること。			
	② 電源ユニットを冗長化すること。また、活性交換できること。			
	③ 消費電力が350W以下であること。			
	④ 1.28Tbps以上のスイッチング容量を有すること。			
	⑤ 960Mpps以上のパケット処理能力を有すること。			
	⑥ SFP＋とSFPの排他ポートを48ポート以上、搭載可能であること。			
	(カ) 監視スイッチ要件			
	ソフトウェア要件			
	① レイヤ2のスイッチングを行えること。			
	② スパニングツリー機能として、IEEE802.1d、IEEE802.1s、IEEE802.1w又はこれらと同等の機能を有すること。			
	③ IEEE802.1pのCOS、DSCPの書き換え、書き込み及びDSCPに基づく優先制御が可能であること。			
	④ ACL又は同等の方式によるアクセス制限が行えること。			
	⑤ IEEE802.3ah/UDLDにより、片方向リンクを検出することが可能であること。			
	⑥ ポートに対しての自動障害検知機能及び自動復帰機能を有すること。			
	⑦ ブロードキャスト及びマルチキャストの流量を制限する機能を持つこと。			
	ハードウェア要件			
	① ボックス型筐体であること。			
	② 消費電力が37.1W以下であること。			
	③ 108Gbps以上のスイッチング容量を有すること。			
	④ 71.4Mpps以上のパケット処理能力を有すること。			
	⑤ 100BASE-TX/1000BASE-Tを24ポート以上有すること。			
	⑥ 10GBASEのSFP+を2ポート以上有すること。			
	(キ) 業務システム接続スイッチ要件			
	ソフトウェア要件			
	① レイヤ2及びレイヤ3のスイッチングを行えること。また、ハードウェアによるIPv4及びIPv6のルーティングに対応すること。			
	② スパニングツリー機能として、IEEE802.1d、IEEE802.1s、IEEE802.1w又はこれらと同等の機能を有すること。			
	③ IEEE802.1pのCOS、TOS及びDSCPの書換え、書き込み、DSCPに基づく優先制御が可能であること。			
	④ ACL又は同等の方式によるアクセス制限が行えること。			
	⑤ IEEE802.3ah/UDLDにより、片方向リンクを検出することが可能であること。			
	⑥ ポートに対しての自動障害検知機能及び自動復帰機能を有すること。			
	⑦ 指定したイベントが発生した際に、電子メールの通知等が自動で行えること。			
	⑧ ブロードキャスト及びマルチキャストの流量を制限する機能を持つこと。			
	ハードウェア要件			
	① シャーシ型筐体又はボックス型筐体であること。			
	② 消費電力が200W以下であること。			
	③ 160Gbps以上のスイッチング容量を有すること。			
	④ 101.2Mpps以上のパケット処理能力を有すること。			
	⑤ 100BASE-TX/1000BASE-Tを48ポート以上有すること。			
	⑥ 拡張により、1000BASEのSFPを4ポート以上又は10GBASEのSFPを2ポート以上搭載できること。			

別紙1－2　要件定義書（サービス・機器）

項番号	内容	提案内容	補足資料	記載箇所
	(ク) メディアコンバータ要件			
	ソフトウェア要件			
	① 1000BASE-Tと1000BASE-SXの変換機能を有すること。			
	② 全ての接続機器が通信可能な状態である場合にのみリンクを確立する機能を有すること。			
	ハードウェア要件			
	① ボックス型筐体であること。			
	② 消費電力が3.3W以下であること。			
	③ 9KByte以上のパケット転送能力を有すること。			
	④ 1000BASE-Tを1ポート以上有すること。			
	⑤ 1000BASE-SX（SCコネクタ、マルチモードファイバ）を1ポート以上有すること。			
	(ケ) 負荷分散装置要件			
	ソフトウェア要件			
	① 同一機能を持つ複数台のサーバに対して、様々なプロトコルを用いた通信の振り分けが可能であること。			
	② ラウンドロビン方式、最小コネクション方式、最小応答時間方式等の分散方式に対応すること。			
	③ サーバ障害時には、負荷分散対象から自動的に除外する機能を有すること。			
	④ 送信元IPやSSLセッションID、Cookie等の情報を利用したパーシステンス機能を有すること。			
	⑤ NAT、ソースNAT機能を有すること。			
	⑥ SSLアクセラレータ機能を有すること。			
	⑦ L3、L4、及びL7レベルのヘルスチェック機能を有すること。			
	⑧ IPv4及びIPv6のデュアルスタックに対応し、IPv6の通信の負荷分散が可能であること。			
	⑨ WebベースのGUIとCLIで設定が可能であること。また、CLIでは、SSHをサポートすること。			
	⑩ プログラミングを用いたL7パケットの振り分けルール作成機能を有すること。			
	ハードウェア要件			
	① 1000BASE-Tのポートを8ポート以上有すること。			
	② 消費電力が350W以下であること。			
	③ 負荷分散時のスループットは、4Gbps以上であること。			
2 拠点LAN				
(1) 概要				
	拠点LANは、総務省職員が各拠点において総務省ＬＡＮサービスを利用するため、拠点ＬＡＮを提供する。 具体的要件について、以下に記載する。			
(2) 構築要件				
ア 共通				
	① 拠点LANは、既存の配線、ラック等の流用を可とする。			
イ 総務省第2庁舎				
	① LAN端末が設置できるネットワークを設計・構築すること。			
	② コアスイッチ、フロアスイッチ、エッジスイッチで構成すること。			
	③ コアスイッチに政策統括官（恩給担当）室のエッジスイッチを接続すること。			
	④ コアスイッチ及びフロアスイッチは、冗長構成とすること。			
	⑤ 冗長化されている部分は、ケーブルや機器等障害による通信断時に自動的に切換え可能な構成とすること。			
	⑥ コアスイッチは、将来の拡張を考慮し、ポート数に余裕を持たせること。			
ウ 公害等調整委員会				
	① LAN端末が設置できるネットワークを設計・構築すること。			
	② エッジスイッチで構成すること。			

別紙1－2　要件定義書（サービス・機器）

項番号	内容	提案内容	補足資料	記載箇所
	③ 冗長化されている部分は、ケーブルや機器等障害による通信断時に自動的に切換え可能な構成とすること。			
エ 自治大学校				
	① LAN端末が設置できるネットワークを設計・構築すること。			
	② コアスイッチ、エッジスイッチで構成すること。			
	③ 冗長化されている部分は、ケーブルや機器等障害による通信断時に自動的に切換え可能な構成とすること。			
オ 情報通信政策研究所				
	① LAN端末が設置できるネットワークを設計・構築すること。			
	② コアスイッチ、エッジスイッチで構成すること。			
	③ 冗長化されている部分は、ケーブルや機器等障害による通信断時に自動的に切換え可能な構成とすること。			
	④ コアスイッチは将来の拡張を考慮し、ポート数に余裕を持たせること。			
カ 消防大学校及び消防研究センター				
	① LAN端末が設置できるネットワークを設計・構築すること。			
	② コアスイッチ、エッジスイッチで構成すること。			
	③ 冗長化されている部分は、ケーブルや機器等障害による通信断時に自動的に切換え可能な構成とすること。			
キ アジア太平洋統計研修所、国会連絡室				
	① LAN端末が設置できるネットワークを設計・構築すること。			
	② エッジスイッチで構成すること。			
	③ 冗長化されている部分は、ケーブルや機器等障害による通信断時に自動的に切換え可能な構成とすること。			
ク 総合通信局及び沖縄総合通信事務所				
	① LAN端末が設置できるネットワークを設計・構築すること。			
	② コアスイッチ、エッジスイッチで構成すること。			
	③ コアスイッチは、冗長構成とすること。			
	④ 冗長化されている部分は、ケーブルや機器等障害による通信断時に自動的に切換え可能な構成とすること。			
ケ 三浦電波監視センター				
	① LAN端末が設置できるネットワークを設計・構築すること。			
	② エッジスイッチで構成すること。			
	③ 冗長化されている部分は、ケーブルや機器等障害による通信断時に自動的に切換え可能な構成とすること。			
コ 管区行政評価（支）局、行政評価事務所、行政評価分室、内閣人事局及び永田町合同庁舎				
	① LAN端末が設置できるネットワークを設計・構築すること。			
	② エッジスイッチで構成すること。			
	③ 冗長化されている部分は、ケーブルや機器等障害による通信断時に自動的に切換え可能な構成とすること。			
サ 総合通信局と同建屋の行政評価局及び行政評価事務所				
	① LAN端末が設置できるネットワークを設計・構築すること。			
	② コアスイッチは、総合通信局に設置されるものを利用すること。			
	③ 各総合通信局～管区行政評価局、行政評価事務所間の接続は冗長化すること。			

項番号	内容	提案内容	補足資料	記載箇所
シ	行政管理局宮城分室、行政管理局大阪分室			
①	LAN端末が設置できるネットワークを設計・構築すること。			
②	エッジスイッチで構成すること。			
③	冗長化されている部分は、ケーブルや機器等障害による通信断時に自動的に切換え可能な構成とすること。			
ス	ディザスタリカバリサイト			
①	コアスイッチ、サーバスイッチ、監視スイッチで構成すること。			
②	コアスイッチ、サーバスイッチは冗長構成とすること。			
③	冗長化されている部分は、ケーブルや機器等障害による通信断時に自動的に切換え可能な構成とすること。			
(3)	**機器等要件**			
ア	総務省第二庁舎			
(ア)	コアスイッチ要件			
	ソフトウェア要件			
①	「別添1 拠点回線・機器一覧表」 ④コアスイッチスペック要件一覧のType　IIを参照すること。			
	ハードウェア要件			
①	「別添1 拠点回線・機器一覧表」 ④コアスイッチスペック要件一覧のType　IIを参照すること。			
(イ)	フロアスイッチ要件			
	ソフトウェア要件			
①	「別添1 拠点回線・機器一覧表」 ⑤フロアスイッチスペック要件一覧のType　IIIを参照すること。			
	ハードウェア要件			
①	「別添1 拠点回線・機器一覧表」 ⑤フロアスイッチスペック要件一覧のType　IIIを参照すること。			
(ウ)	エッジスイッチ①要件			
	ソフトウェア要件			
①	「別添1 拠点回線・機器一覧表」 ⑥エッジスイッチスペック要件一覧のType　IIIを参照すること。			
	ハードウェア要件			
①	「別添1 拠点回線・機器一覧表」 ⑥エッジスイッチスペック要件一覧のType　IIIを参照すること。			
(エ)	エッジスイッチ②要件			
	ソフトウェア要件			
①	「別添1 拠点回線・機器一覧表」 ⑥エッジスイッチスペック要件一覧のType　IVを参照すること。			
	ハードウェア要件			
①	「別添1 拠点回線・機器一覧表」 ⑥エッジスイッチスペック要件一覧のType　IVを参照すること。			
(オ)	エッジスイッチ（政策統括官（恩給担当）室）要件			
	ソフトウェア要件			
①	レイヤ2のスイッチングを行えること。			
②	スパニングツリー機能として、IEEE802.1d、IEEE802.1s、IEEE802.1w又はこれらと同等の機能を有すること。			
③	IEEE802.1pのCOS、DSCPに基づく優先制御が可能であること。			
④	IEEE802.3ah/UDLDにより、片方向リンクを検出することが可能であること。			
⑤	ポートに対しての自動障害検知機能及び自動復帰機能を有すること。			
⑥	ブロードキャスト及びマルチキャストの流量を制限する機能を持つこと。			
	ハードウェア要件			
①	ボックス型筐体であること。			
②	消費電力が37.1W以下であること。			
③	108Gbps以上のスイッチング容量を有すること。			

別紙1－2　要件定義書（サービス・機器）

項番号	内容	提案内容	補足資料	記載箇所
	④ 71.4Mpps以上のパケット処理能力を有すること。			
	⑤ 100BASE-TX/1000BASE-Tを24ポート以上有すること。			
	⑥ SFPを2ポート以上有すること。			
イ	公害等調整委員会			
(ア)	エッジスイッチ要件			
	ソフトウェア要件			
	①「別添1 拠点回線・機器一覧表」 ⑥エッジスイッチスペック要件一覧のType　IIを参照すること。			
	ハードウェア要件			
	①「別添1 拠点回線・機器一覧表」 ⑥エッジスイッチスペック要件一覧のType　IIを参照すること。			
ウ	自治大学校			
(ア)	コアスイッチ要件			
	ソフトウェア要件			
	①「別添1 拠点回線・機器一覧表」 ④コアスイッチスペック要件一覧のType　IIIを参照すること。			
	ハードウェア要件			
	①「別添1 拠点回線・機器一覧表」 ④コアスイッチスペック要件一覧のType　IIIを参照すること。			
(イ)	エッジスイッチ要件			
	ソフトウェア要件			
	①「別添1 拠点回線・機器一覧表」 ⑥エッジスイッチスペック要件一覧のType　IIIを参照すること。			
	ハードウェア要件			
	①「別添1 拠点回線・機器一覧表」 ⑥エッジスイッチスペック要件一覧のType　IIIを参照すること。			
エ	情報通信政策研究所			
(ア)	コアスイッチ①要件			
	ソフトウェア要件			
	①「別添1 拠点回線・機器一覧表」 ④コアスイッチスペック要件一覧のType　IIIを参照すること。			
	ハードウェア要件			
	①「別添1 拠点回線・機器一覧表」 ④コアスイッチスペック要件一覧のType　IIIを参照すること。			
(イ)	コアスイッチ②要件			
	ソフトウェア要件			
	①「別添1 拠点回線・機器一覧表」 ④コアスイッチスペック要件一覧のType　IVを参照すること。			
	ハードウェア要件			
	①「別添1 拠点回線・機器一覧表」 ④コアスイッチスペック要件一覧のType　IVを参照すること。			
(ウ)	エッジスイッチ①要件			
	ソフトウェア要件			
	①「別添1 拠点回線・機器一覧表」 ⑥エッジスイッチスペック要件一覧のType　IIを参照すること。			
	ハードウェア要件			
	①「別添1 拠点回線・機器一覧表」 ⑥エッジスイッチスペック要件一覧のType　IIを参照すること。			
(エ)	エッジスイッチ②要件			
	ソフトウェア要件			
	①「別添1 拠点回線・機器一覧表」 ⑥エッジスイッチスペック要件一覧のType　IIIを参照すること。			
	ハードウェア要件			
	①「別添1 拠点回線・機器一覧表」 ⑥エッジスイッチスペック要件一覧のType　IIIを参照すること。			

別紙1－2　要件定義書（サービス・機器）

項番号	内容	提案内容	補足資料	記載箇所
	オ　消防大学校及び消防研究センター			
	(ア) コアスイッチ①要件			
	ソフトウェア要件			
	①「別添1 拠点回線・機器一覧表」 ④コアスイッチスペック要件一覧のType　IIIを参照すること。			
	ハードウェア要件			
	①「別添1 拠点回線・機器一覧表」 ④コアスイッチスペック要件一覧のType　IIIを参照すること。			
	(イ) コアスイッチ②要件			
	ソフトウェア要件			
	①「別添1 拠点回線・機器一覧表」 ④コアスイッチスペック要件一覧のType　IVを参照すること。			
	ハードウェア要件			
	①「別添1 拠点回線・機器一覧表」 ④コアスイッチスペック要件一覧のType　IVを参照すること。			
	(ウ) エッジスイッチ要件			
	ソフトウェア要件			
	①「別添1 拠点回線・機器一覧表」 ⑥エッジスイッチスペック要件一覧のType　IIを参照すること。			
	ハードウェア要件			
	①「別添1 拠点回線・機器一覧表」 ⑥エッジスイッチスペック要件一覧のType　IIを参照すること。			
	カ　アジア太平洋統計研修所、国会連絡室			
	(ア) エッジスイッチ要件			
	ソフトウェア要件			
	①「別添1 拠点回線・機器一覧表」 ⑥エッジスイッチスペック要件一覧のType　IIIを参照すること。			
	ハードウェア要件			
	①「別添1 拠点回線・機器一覧表」 ⑥エッジスイッチスペック要件一覧のType　IIIを参照すること。			
	キ　総合通信局及び沖縄総合通信事務所			
	(ア) コアスイッチ要件			
	ソフトウェア要件			
	①「別添1 拠点回線・機器一覧表」 ④コアスイッチスペック要件一覧のType　Vを参照すること。			
	ハードウェア要件			
	①「別添1 拠点回線・機器一覧表」 ④コアスイッチスペック要件一覧のType　Vを参照すること。			
	(イ) フロアスイッチ要件			
	ソフトウェア要件			
	①「別添1 拠点回線・機器一覧表」 ⑤フロアスイッチスペック要件一覧のType　IIを参照すること。			
	ハードウェア要件			
	①「別添1 拠点回線・機器一覧表」 ⑤フロアスイッチスペック要件一覧のType　IIを参照すること。			
	(ウ) エッジスイッチ①要件			
	ソフトウェア要件			
	①「別添1 拠点回線・機器一覧表」 ⑥エッジスイッチスペック要件一覧のType　IIを参照すること。			
	ハードウェア要件			
	①「別添1 拠点回線・機器一覧表」 ⑥エッジスイッチスペック要件一覧のType　IIを参照すること。			
	(エ) エッジスイッチ②要件			
	ソフトウェア要件			
	①「別添1 拠点回線・機器一覧表」 ⑥エッジスイッチスペック要件一覧のType　IIIを参照すること。			
	ハードウェア要件			
	①「別添1 拠点回線・機器一覧表」 ⑥エッジスイッチスペック要件一覧のType　IIIを参照すること。			

別紙1－2　要件定義書（サービス・機器）

項番号	内容	提案内容	補足資料	記載箇所
	（オ）メディアコンバータ要件			
	ソフトウェア要件			
	① 1000BASE-Tと1000BASE-SXの変換機能を有すること。			
	② 全ての接続機器が通信可能な状態である場合にのみリンクを確立する機能を有すること。			
	ハードウェア要件			
	① ボックス型筐体であること。			
	② 消費電力が3.3W以下であること。			
	③ 9KByte以上のパケット転送能力を有すること。			
	④ 1000BASE-Tを1ポート以上有すること。			
	⑤ 1000BASE-SX（SCコネクタ、マルチモードファイバ）を1ポート以上有すること。			
	ク　三浦電波監視センター			
	（ア）エッジスイッチ①要件			
	ソフトウェア要件			
	①「別添1 拠点回線・機器一覧表」 ⑥エッジスイッチスペック要件一覧のType　IIを参照すること。			
	ハードウェア要件			
	①「別添1 拠点回線・機器一覧表」 ⑥エッジスイッチスペック要件一覧のType　IIを参照すること。			
	（イ）エッジスイッチ②要件			
	ソフトウェア要件			
	①「別添1 拠点回線・機器一覧表」 ⑥エッジスイッチスペック要件一覧のType　IIIを参照すること。			
	ハードウェア要件			
	①「別添1 拠点回線・機器一覧表」 ⑥エッジスイッチスペック要件一覧のType　IIIを参照すること。			
	ケ　管区行政評価（支）局、行政評価事務所、行政評価分室、内閣人事局、情報公開・個人情報保護審査会（永田町合同庁舎）、官民競争入札等監理事務局（永田町合同庁舎）			
	（ア）エッジスイッチ①要件			
	ソフトウェア要件			
	①「別添1 拠点回線・機器一覧表」 ⑥エッジスイッチスペック要件一覧のType　IIを参照すること。			
	ハードウェア要件			
	①「別添1 拠点回線・機器一覧表」 ⑥エッジスイッチスペック要件一覧のType　IIを参照すること。			
	（イ）エッジスイッチ②要件			
	ソフトウェア要件			
	①「別添1 拠点回線・機器一覧表」 ⑥エッジスイッチスペック要件一覧のType　IIIを参照すること。			
	ハードウェア要件			
	①「別添1 拠点回線・機器一覧表」 ⑥エッジスイッチスペック要件一覧のType　IIIを参照すること。			
	コ　行政管理局宮城分室、行政管理局大阪分室			
	（ア）エッジスイッチ要件			
	ソフトウェア要件			
	①「別添1 拠点回線・機器一覧表」 ⑥エッジスイッチスペック要件一覧のType　IIIを参照すること。			
	ハードウェア要件			
	①「別添1 拠点回線・機器一覧表」 ⑥エッジスイッチスペック要件一覧のType　IIIを参照すること。			
	サ　ディザスタリカバリサイト			
	（ア）コアスイッチ要件			
	ソフトウェア要件			
	①「別添1 拠点回線・機器一覧表」 ④コアスイッチスペック要件一覧のType　Vを参照すること。			

別紙1－2　要件定義書（サービス・機器）

項番号	内容	提案内容	補足資料	記載箇所
	ハードウェア要件			
	① 「別添1 拠点回線・機器一覧表」 ④コアスイッチスペック要件一覧のType　Vを参照すること。			
	(イ) サーバ接続スイッチ要件			
	ソフトウェア要件			
	① レイヤ2及びレイヤ3のスイッチングを行えること。また、ハードウェアによるIPv4及びIPv6のルーティングに対応すること。			
	② スパニングツリー機能として、IEEE802.1d、IEEE802.1s、IEEE802.1w又はこれらと同等の機能を有すること。			
	③ IEEE802.1pのCOS、TOS及びDSCPの書換え、書き込み、DSCPに基づく優先制御が可能であること。			
	④ ACL又は同等の方式によるアクセス制限が行えること。			
	⑤ IEEE802.3ah/UDLDにより、片方向リンクを検出することが可能であること。			
	⑥ ポートに対しての自動障害検知機能及び自動復帰機能を有すること。			
	⑦ 指定したイベントが発生した際に、電子メールの通知等が自動で行えること。			
	⑧ ブロードキャスト及びマルチキャストの流量を制限する機能を持つこと。			
	ハードウェア要件			
	① シャーシ型筐体又はボックス型筐体であること。			
	② 電源ユニットを冗長化すること。また、活性交換できること。			
	③ 消費電力が350W以下であること。			
	④ 1.28Tbps以上のスイッチング容量を有すること。			
	⑤ 960Mpps以上のパケット処理能力を有すること。			
	⑥ SFP＋とSFPの排他ポートを48ポート以上、搭載可能であること。			
	(ウ) 監視スイッチ要件			
	ソフトウェア要件			
	① レイヤ2のスイッチングを行えること。			
	② スパニングツリー機能として、IEEE802.1d、IEEE802.1s、IEEE802.1w又はこれらと同等の機能を有すること。			
	③ IEEE802.1pのCOS、DSCPに基づく優先制御が可能であること。			
	④ IEEE802.3ah/UDLDにより、片方向リンクを検出することが可能であること。			
	⑤ ポートに対しての自動障害検知機能及び自動復帰機能を有すること。			
	⑥ ブロードキャスト及びマルチキャストの流量を制限する機能を持つこと。			
	ハードウェア要件			
	① ボックス型筐体であること。			
	② 消費電力が37.1W以下であること。			
	③ 108Gbps以上のスイッチング容量を有すること。			
	④ 71.4Mpps以上のパケット処理能力を有すること。			
	⑤ 100BASE-TX/1000BASE-Tを24ポート以上有すること。			
	⑥ SFPを2ポート以上有すること。			
3 ネットワークサービス				
(1) 概要				
	総務省職員がネットワークを介した各種サービス（DHCP、DNS、NTP、プロキシ）を利用するため、ネットワークサービスを提供する。 具体的要件について、以下に記載する。			
(2) 構築要件				
ア　DNS・DHCP・NTPサービス要件				
	① DNS・DHCP・NTPの機能を提供すること。			
	② IPv4/IPv6いずれのレコードの管理（登録・変更・削除等）も容易に行う機能を提供すること。			

別紙1－2　要件定義書（サービス・機器）

項番号	内容	提案内容	補足資料	記載箇所
	③ 全LAN端末及びタブレット型端末に対するIPアドレスの配付・管理機能を提供すること。			
	④ 固定IPアドレスを含めたIPアドレス、MACアドレス、名前管理が行えること。			
	⑤ DNSキャッシュポイズニング対策を考慮した構成をとること。			
（ア）全省DNSサービス要件				
	① インターネット接続セグメントDNSと通信し、インターネット上の名前解決を行うこと。			
	② ディザスタリカバリサイトのDNS機能と連携し、ホスト名、IPアドレスを統合管理可能であること。			
	③ 総務省LAN内から、インターネット・政府共通ネットワーク・総務省LAN内の名前解決を行えること。			
	④ 名前管理・IPアドレス管理・MACアドレス管理は本省とディザスタリカバリサイトで同期し、いずれの機器からでもサービス提供が行えること。			
	⑤ 本省のDNSサーバは冗長化すること。			
（イ）インターネット接続DNSサービス要件				
	① インターネット上の公開DNSと通信し、総務省ドメイン以外のドメインの名前解決を行うこと。			
	② インターネットから、総務省公開サーバの名前解決を行えること。			
	③ インターネットからの問合せに対する総務省ドメインの名前解決の可用性を担保すること。			
	④ インターネット向けDNS情報は独立して管理すること。			
	⑤ 内部からの問い合わせと外部からの問い合わせを区別し、対応する情報を独立して管理すること。			
	⑥ 「soumu.go.jp」並びに「総務省.jp」ドメインを提供すること。			
（ウ）政府共通ネットワーク接続DNSサービス要件				
	① 政府共通ネットワークが提供するDNSサービスと連携し、政府共通ネットワークドメインの名前解決を行うこと。			
（エ）全省DHCPサービス要件				
	① 全LAN端末及びタブレット型端末に対して、IPアドレス、ネットワーク情報（デフォルトゲートウェイ、サブネットマスク、ドメイン名、DNSサービスのIPアドレス）の自動割り当てを行うこと。			
	② DHCP機能は冗長構成とし、リース情報の引継ぎを行えること。			
	③ 全省DHCPサービスを一元管理すること。			
（オ）NTPサービス要件				
	① インターネットに接続されていない環境でも、時刻同期を行うこと。			
	② 各種サーバ、ネットワーク機器、LAN端末に対して時刻同期を提供すること。配信する時刻は、主管課の指定するNTPサーバと同期を取ること。			
イ　プロキシサービス要件				
	① インターネット・政府共通ネットワーク・総務省LAN内に対してのWebアクセスは原則としてプロキシサービス経由で行えるよう構成すること。また、特定の総務省LAN内のWebアクセスは、直接アクセスするための仕組みを備えること。			
	② インターネットとのWebアクセス通信に対して、プロキシサービスはHTTPS（SSL通信）の復号化を行うこと。			
	③ プロキシサービスの利用状況（接続元IPアドレス、アクセス先URL、日時、バイト数、プロトコル等）を記録し、3年以上保管すること。			
	④ 標的型攻撃対策（インターネット・Web）サービスと連携すること。			
	⑤ 認証サービスと連携し、ユーザ認証を行うこと。			
（ア）全省プロキシサービス要件				
	① インターネット及び政府共通ネットワークへのWebアクセスを中継すること。			
（イ）インターネット接続プロキシサービス要件				
	① 全省プロキシサービスからのインターネットアクセスを中継すること。			

項番号	内容	提案内容	補足資料	記載箇所
	（ウ）政府共通ネットワーク接続プロキシサービス要件			
	① 全省プロキシサービスからの政府共通ネットワークアクセスを中継すること。			
（3）機器等要件				
ア 全省 DNS 機能				
	ソフトウェア要件			
	① IPアドレスとドメイン名やホスト名の名前解決機能を有すること。			
	② 名前解決に当たっては、正引き及び逆引きに対応すること。			
	③ 上位のDNSサーバと連携する機能を持つこと。			
	④ 端末や他のサーバからの上位に対して応答できる性能を有すること。			
	⑤ DNSの運用がWebベースのGUIで設定が可能であること。			
	⑥ 総務省LANの機器に関するホスト名とIPアドレスの名前解決を行うこと。			
	⑦ DHCP機能と連携し、DNS情報の動的更新を行うこと。			
	⑧ インターネット接続セグメントDNSと通信し、インターネット上の名前解決を行うこと。			
	⑨ 政府共通ネットワーク接続セグメントDNSと通信し、政府共通ネットワーク内の名前解決を行うこと。			
	⑩ システム管理用インターフェースとして、WebベースのGUIを提供すること。			
	⑪ ディザスタリカバリサイトのDNSサービスと連携し、ホスト名、IPアドレスを統合管理可能であること。			
	⑫ ディザスタリカバリサイトのDNSサービスにDNS情報を複製すること。			
	ハードウェア要件			
	① 100BASE-TX/1000BASE-Tのポートを2ポート以上有すること。			
	② DNSの問い合わせ性能として、36,000qps以上有すること。			
イ インターネット接続 DNS 機能				
	ソフトウェア要件			
	① インターネット上の公開DNSと通信し、総務省ドメイン以外のドメインの名前解決を行うこと。			
	② インターネットからの問合せに対し、総務省ドメインの機器の名前解決を行うこと。			
	③ インターネットサービスプロバイダのセカンダリDNSサービスに総務省のドメイン情報を提供すること。			
	④ DNS問い合わせ及びゾーン転送を許可するIPアドレス範囲を指定できること。			
	⑤ 総務省内部向けDNS情報とインターネット向けDNS情報は、分離して管理すること。			
	⑥ IPv6レコードの登録、並びにIPv6の問い合わせに対応できること。			
	⑦ 内部からの問い合わせと外部からの問い合わせを区別し、対応する情報も分離して管理すること。			
	⑧ SPFに対応できること。			
	ハードウェア要件			
	① 特に指定しない。			
ウ 政府共通ネットワーク接続 DNS 機能				
	ソフトウェア要件			
	① 政府共通ネットワークが提供するDNSサービスと連携し、政府共通ネットワークドメインの名前解決を行うこと。			
	② IPv6レコードの登録、並びにIPv6の問い合わせに対応可能であること。			
	ハードウェア要件			
	① 特に指定しない。			
エ 全省 DHCP 機能				
	ソフトウェア要件			
	① DHCPの運用がWebベースのGUIで設定が可能であること。			
	② 全クライアント端末に対して、IPアドレス、ネットワーク情報（デフォルトゲートウェイ、サブネットマスク、ドメイン名、DNSサービスのIPアドレス）の自動割り当てを行うこと。			

項番号	内容	提案内容	補足資料	記載箇所
	③ IPアドレスの割り当て期間を制御できること。			
	④ IPアドレスの割り当てる範囲を指定できること。			
	⑤ セキュリティ及び証跡管理を考慮して、特定端末などにDHCP環境でも特定のIPアドレスを割り当てることができること			
	⑥ MACアドレスを登録し、登録されたMACのみに特定のDHCPレンジからIPアドレスを払いだせる事。			
	⑦ クライアントに割り当てるデフォルトルータ、ブロードキャストアドレス、サブネットマスク、リース時間をDHCPレンジごとに指定できる事。			
	⑧ DHCPの利用状況（日時、IPアドレス、MACアドレス、コンピュータ名等）を記録すること。			
	⑨ 端末のMACアドレスによって、DHCPでのIPアドレス割り当てを許可するかどうか設定する機能を有すること。			
	⑩ 全省DHCPサービスを一元管理すること。			
	⑪ システム管理用インターフェースとしてWebベースのGUIを提供すること。			
	⑫ 障害が発生した場合においても、リース情報が引き継げること。			
	ハードウェア要件			
	① 100BASE-TX/1000BASE-Tのポートを2ポート以上有すること。			
	② DHCP性能として、225lease/sec以上有すること。			
オ　NTP 機能				
	ソフトウェア要件			
	① 時刻を同期させる機能を有すること。			
	② 総務省LANに接続された機器に対して、NTPによる時刻提供サービス機能を有すること。			
	③ NTPの利用状況（設定日時、上位NTPサービスのIPアドレス、オフセット時間）の記録機能を有すること。			
	④ インターネットが接続されていない環境でも、時刻同期が行えること。			
	ハードウェア要件			
	① 特に指定しない。			
カ　全省プロキシ機能				
	ソフトウェア要件			
	① インターネット及び他省庁へのWebアクセスが中継可能であること。			
	② HTTP、HTTPS、FTPリクエストの中継機能を有すること。			
	③ HTTP1.1に対応したHTTPリクエストの中継機能を有すること。			
	④ WebベースのGUI又はCLIで設定が可能であること。CLIではSSHをサポートすること。			
	⑤ クライアント端末等からの省内及び省外へのWebアクセスは、原則全省プロキシサービス経由で行うこと。			
	⑥ HTMLコンテンツや画像データ等のWebコンテンツのキャッシュ機能を有すること。			
	⑦ 利用状況（アクセス元クライアント端末等のIPアドレス、アクセス先URL等、アクセス制御（許可、拒否）、日時）の記録機能を有すること。			
	⑧ 省内のWebアクセスは、除外設定する機能を有すること。			
	⑨ IPv4、IPv6のデュアルスタックに対応すること。			
	⑩ システム管理用インターフェースとして、WebベースのGUIを提供すること。			
	⑪ Web画面上でプロキシの統計情報の閲覧できる機能を有すること。			
	⑫ 本省の全ユーザが外部に対するWebアクセスにおいて、プロキシサービスを経由するため、これを処理可能な構成とすること。			
	ハードウェア要件			
	① 100BASE-TX/1000BASE-T のポートを 4 ポート以上有すること。			

別紙1－2　要件定義書（サービス・機器）

項番号	内容	提案内容	補足資料	記載箇所
キ	インターネット接続プロキシ機能			
	ソフトウェア要件			
①	インターネット及び他省庁へのWebアクセスが中継可能であること。			
②	HTTP、HTTPS、FTPリクエストの中継機能を有すること。			
③	HTTP1.1に対応したHTTPリクエストの中継機能を有すること。			
④	WebベースのGUI又はCLIで設定が可能であること。CLIではSSHをサポートすること。			
⑤	全省プロキシサービスからのインターネットアクセスを中継すること。			
⑥	HTMLコンテンツや画像データ等のWebコンテンツのキャッシュ機能を有すること。			
⑦	NTLM,LDAP,ActiveDirectory,RADIUS等と連携した認証が可能であること。			
⑧	利用状況（アクセス元クライアント端末等のIPアドレス、アクセス先URL等、アクセス制御（許可、拒否）、日時）の記録機能を有すること。			
⑨	省内のWebアクセスは、除外設定する機能を有すること。			
⑩	IPv4、IPv6のデュアルスタックに対応すること。			
⑪	イベントログをSyslogや電子メールで転送する仕組みを有すること。			
⑫	システム管理用インターフェースとして、WebベースのGUIを提供すること。			
⑬	Web画面上でプロキシの統計情報の閲覧できる機能を有すること。			
	ハードウェア要件			
①	100BASE-TX/1000BASE-T のポートを 4 ポート以上有すること。			
ク	政府共通ネットワーク接続プロキシ機能			
	ソフトウェア要件			
①	全省プロキシサービスからの政府共通ネットワークアクセスを中継すること。			
②	通過プロトコルとして、HTTP、HTTPS、FTPに対応すること。			
③	HTMLコンテンツや画像データ等のWebコンテンツのキャッシュ機能を有すること。			
④	利用状況の記録機能を有すること。			
	ハードウェア要件			
①	100BASE-TX/1000BASE-Tのポートを4ポート以上有すること。			
4	**無線LAN接続サービス**			
(1)	**概要**			
	端末の設置場所を固定せず、執務場所にとらわれないネットワーク接続環境を実現するため、無線ＬＡＮ接続サービスを提供する。 ペーパーレス会議システムを行う際に、無線LAN接続サービスを提供する。 具体的要件について、以下に記載する。			
(2)	**構築要件**			
①	事前に許可されたLAN端末、タブレット型端末（ペーパレス会議システム用）に対してのみ、無線LAN接続環境を提供すること。			
②	無線LANアクセスポイントの固定的な設置場所は、以下とすること。 ・全ての会議室、執務室、打ち合わせスペース等（本省、総務省第2庁舎） ・会議室及び災害対策室等（自治大学校、情報通信政策研究所） ・会議室及び打合せスペース等（設置個所は任意で数か所） （管区行政評価（支）局、総合通信局、沖縄通信事務所、公害等調整委員会（4号館）、内閣人事局（8号館）、情報公開・個人情報保護審査会及び官民競争入札等監理事務局（永田町合同庁舎）、行政管理局、アジア太平洋統計研修所、消防大学校及び消防研究センター、国会連絡室）			
③	アクセスポイントを原則として天井に設置すること。			
④	アクセスポイントの設置場所は落下防止の措置を行い、固定すること。			

項番号	内容	提案内容	補足資料	記載箇所
	⑤ 無線LANアクセスポイントの設置時は事前に電波状況を調査し、干渉や他の通信機器への影響を配慮すること。また、設置後に電波状況を調査し、設計通りに設置されているか確認すること。			
	⑥ 無線LANアクセスポイントの設置後も電波干渉源（Wi-Fi、非Wi-Fi）を監視し、干渉が発生した場合は自動で回避させること。			
	⑦ 定期的な電波品質の調査をし、品質を評価するために、SN比や受信信号強度等を元に一元的な評価値を提供できること。			
	⑧ 無線LANアクセスポイントは、集中管理可能な構成とすること。また、集中管理に必要なライセンス等調達を行うこと。			
	⑨ 認証サービスと連携してユーザを識別し、利用権限に合わせた動的なセグメント管理を行うこと。			
	⑩ 認証や通信路の暗号化等、十分なセキュリティ対策を行うこと。			
	⑪ 1台のアクセスポイントが故障した場合にも、他のアクセスポイントが自動的に送信出力を上げることで、影響範囲を狭めることが可能であること。			
	⑫ タブレット型端末の無線LAN接続及び通信が、LAN端末の無線LAN接続及び通信により妨げられないよう構築すること。			
	⑬ 高密度環境（会議室等の狭いエリアに多数の職員が集う等）においても安定した無線LANシステムを提供すること。			
	⑭ タブレット型端末専用のVLANを作成し、許可された通信のみが利用できるようネットワーク上でアクセス制御を行うこと。			
	⑮ 会議室、執務室における無線電波状況や、干渉源、不正アクセスポイントの状況を可視化し、遠隔地から解析できること。			
（3）機器等要件				
ア　無線アクセスポイント管理機能				
ソフトウェア要件				
	① 最大で1000のアクセスポイントの管理が可能であること。			
	② 電子政府推奨暗号に対応していること。			
	③ RADIUS認証/アカウンティング機能を有すること。			
	④ 管理インターフェースとして、HTTPS、SSH、シリアル接続が可能であること。			
	⑤ 外部LDAPサーバとの認証連携が可能であること。			
	⑥ コントローラによる構成定義の一元管理を行えること。			
	⑦ アクセスポイントとコントローラ間の通信を暗号化する機能を有すること。			
	⑧ 不正なアクセスポイントを検出する機能を有すること。			
	⑨ アクセスポイントは、コントローラによるチャネル、電波強度、セキュリティ設定等の制御が可能であること。			
	⑩ 電波干渉源監視のための専用機器を必要としないこと。			
ハードウェア要件				
	① ボックス型筐体であること。			
	② 10Gbpsのポートを4ポート以上有すること。			
	③ 電源部の冗長化が可能であること。			
イ　無線LANアクセスポイント				
ソフトウェア要件				
	① 無線LANコントローラによる一括管理が可能であること。			
	② 802.11i規格のWPA2、WPAに準拠していること。			
	③ 電子政府推奨暗号に対応していること。			
	④ 802.1X認証に対応していること。			

項番号	内容	提案内容	補足資料	記載箇所
	⑤ 以下のEAPタイプに対応していること。 ・EAP-TLS ・EAP-TTLSorMSCHAPv2 ・PEAPv0orEAP-MSCHAPv2 ・EAP-FAST ・PEAPv1orEAP-GTC ・EAP-SIM			
	ハードウェア要件			
	① PoE、ローカル電源（AC100V）のどちらでも動作可能であること。			
	② 有線インターフェースが100BASE-TX/1000BASE-Tを1ポート以上有すること。			
	③ アクセスポイントの消費電力が17W以下であること。			
	④ アクセスポイント1台当たり50台程度のLAN端末が接続可能であること。			
	⑤ IEEE802.11a/b/g/n/ac機能を有すること。			
	⑥ IEEE802.11n/acでは、3X3以上のMIMO機能を有すること。			
	⑦ 802.11ac対応のLAN端末に対して機能を追加せずに、ビームフォーミング技術等により通信の信頼性とRFのカバレージを改善する機能を有すること。			
	⑧ 802.11n対応のタブレット型端末、802.11ac対応のタブレット型端末に対して機能を追加せずに、ビームフォーミング技術等により通信の信頼性とRFのカバレージを改善する機能を有すること。			
5　インターネット接続回線				
（1）概要				
	総務省職員が業務を遂行する際の情報収集及び情報交換を行うため、インターネット接続回線を提供する。 具体的要件について、以下に記載する。			
（2）構築要件				
ア　インターネット回線（本省）				
	① ベストエフォート型（2回線）及び帯域確保型（2回線）の回線を利用し、冗長化すること。			
	② IPv4/IPv6デュアルスタックに対応すること。			
	③ 総務省DNSのセカンダリサービスを提供すること。			
	④ 送信元IPアドレスの正当性を確認し、偽装された送信元IPアドレスを利用した通信を遮断する仕組みを導入していること。			
	⑤ 機器障害又は回線障害等により1系統の回線が切断された場合でも、総務省LANのサービスに影響を与えることなく通信経路及び帯域を確保すること。			
	⑥ 回線負荷分散機能を導入し、全ての回線を効率よく使用すること。			
	⑦ 帯域確保型の2回線は、異なる通信事業者の回線を準備すること。ベストエフォート型の2回線は、同一の通信事業者の回線であってもかまわない。			
	⑧ 冗長化する回線は、各々異なる局舎に収容されていること。			
	⑨ ベストエフォート型は1回線当たり1Gbps以上、帯域確保型は1回線当たり200Mbps以上、もう1回線当たり300Mbps以上を提供すること。			
	⑩ IPv4グローバルアドレス及びIPv6グローバルユニキャストアドレスは、必要数準備すること。			
イ　インターネット回線（ディザスタリカバリサイト）				
	① ベストエフォート型（1回線）及び帯域確保型（1回線）の回線を利用すること。			
	② IPv4/IPv6デュアルスタックに対応すること。			
	③ 総務省DNSのセカンダリサービスを提供すること。			
	④ 送信元IPアドレスの正当性を確認し、偽装された送信元IPアドレスを利用した通信を遮断する仕組みを導入していること。			

項番号	内容	提案内容	補足資料	記載箇所
	⑤ ベストエフォート型と帯域確保型それぞれで異なる通信事業者の回線を準備すること。			
	⑥ ベストエフォート型は1Gbps以上、帯域確保型は200Mbps以上を提供すること。			
	⑦ IPv4グローバルアドレス及びIPv6グローバルユニキャストアドレスは必要数準備すること。			
(3) 機器等要件				
ア インターネット回線（本省）				
(ア) インターネット回線接続ルータ要件				
ソフトウェア要件				
	①「別添1 拠点回線・機器一覧表」 ②回線接続ルータスペック要件一覧のType Ⅰを参照すること。			
ハードウェア要件				
	①「別添1 拠点回線・機器一覧表」 ②回線接続ルータスペック要件一覧のType Ⅰを参照すること。			
(イ) インターネット回線接続スイッチ要件				
ソフトウェア要件				
	① レイヤ2のスイッチングを行えること。			
	② スパニングツリー機能として、IEEE802.1d、IEEE802.1s、IEEE802.1w又はこれらと同等の機能を有すること。			
	③ IEEE802.1pのCOS、DSCPの書き換え、書き込み及びDSCPに基づく優先制御が可能であること。			
	④ ACL又は同等の方式によるアクセス制限が行えること。			
	⑤ IEEE802.3ah/UDLDにより、片方向リンクを検出することが可能であること。			
	⑥ ポートに対しての自動障害検知機能及び自動復帰機能を有すること。			
	⑦ ブロードキャスト及びマルチキャストの流量を制限する機能を持つこと。			
ハードウェア要件				
	① ボックス型筐体であること。			
	② 消費電力が40W以下であること。			
	③ 10Gbps以上のスイッチング容量を有すること。			
	④ 11.9Mpps以上のパケット処理能力を有すること。			
	⑤ 100BASE-TX/1000BASE-Tを8ポート以上有すること。			
	⑥ 100BASE-TX/1000BASE-TとSFPの排他ポートを1ポート以上有すること。			
(ウ) インターネット接続スイッチ要件				
ソフトウェア要件				
	① レイヤ2のスイッチングを行えること。			
	② スパニングツリー機能として、IEEE802.1d、IEEE802.1s、IEEE802.1w又はこれらと同等の機能を有すること。			
	③ IEEE802.1pのCOS、DSCPの書き換え、書き込み及びDSCPに基づく優先制御が可能であること。			
	④ ACL又は同等の方式によるアクセス制限が行えること。			
	⑤ IEEE802.3ah/UDLDにより、片方向リンクを検出することが可能であること。			
	⑥ ポートに対しての自動障害検知機能及び自動復帰機能を有すること。			
	⑦ ブロードキャスト及びマルチキャストの流量を制限する機能を持つこと。			
	⑧ セキュリティ監視の目的のため、トラフィックを分岐するためのミラーポートを1ポート設定すること。			
ハードウェア要件				
	① ボックス型筐体であること。			
	② 消費電力が30W以下であること。			
	③ 10Gbps以上のスイッチング容量を有すること。			
	④ 11.9Mpps以上のパケット処理能力を有すること。			
	⑤ 100BASE-TX/1000BASE-Tを8ポート以上有すること。			
	⑥ 100BASE-TX/1000BASE-TとSFPの排他ポートを1ポート以上有すること。			

別紙1－2　要件定義書（サービス・機器）

項番号	内容	提案内容	補足資料	記載箇所
	(エ) インターネット接続 DMZ スイッチ要件			
	ソフトウェア要件			
	① レイヤ2及びレイヤ3のスイッチングを行えること。また、ハードウェアによるIPv4及びIPv6のルーティングに対応すること。			
	② スパニングツリー機能として、IEEE802.1d、IEEE802.1s、IEEE802.1w又はこれらと同等の機能を有すること。			
	③ IEEE802.1pのCOS、TOS及びDSCPの書換え、書き込み、DSCPに基づく優先制御が可能であること。			
	④ ACL又は同等の方式によるアクセス制限が行えること。			
	⑤ IEEE802.3ah/UDLDにより、片方向リンクを検出することが可能であること。			
	⑥ ポートに対しての自動障害検知機能及び自動復帰機能を有すること。			
	⑦ 指定したイベントが発生した際に、電子メールの通知等が自動で行えること。			
	⑧ ブロードキャスト及びマルチキャストの流量を制限する機能を持つこと。			
	⑨ セキュリティ監視の目的のため、トラフィックを分岐するためのミラーポートを1ポート設定すること。			
	ハードウェア要件			
	① シャーシ型筐体又はボックス型筐体であること。			
	② 消費電力が200W以下であること。			
	③ 160Gbps以上のスイッチング容量を有すること。			
	④ 101.2Mpps以上のパケット処理能力を有すること。			
	⑤ 100BASE-TX/1000BASE-Tを48ポート以上有すること。			
	⑥ 拡張により、1000BASEのSFPを4ポート以上又は10GBASEのSFPを2ポート以上搭載できること。			
	(オ) インターネット接続セグメント負荷分散装置			
	ソフトウェア要件			
	① 同一機能を持つ複数台のサーバに対して、様々なプロトコルを用いた通信を振り分けできること。			
	② ラウンドロビン方式、最小コネクション方式、最小応答時間方式等の分散方式に対応すること。			
	③ サーバ障害時には、負荷分散対象から自動的に除外する機能を有すること。			
	④ 送信元IPやSSLセッションID、Cookie等の情報を利用したパーシステンス機能を有すること。			
	⑤ NAT、ソースNAT機能を有すること。			
	⑥ SSLアクセラレータ機能を有すること。			
	⑦ L3、L4、及びL7レベルのヘルスチェック機能を有すること。			
	⑧ IPv4及びIPv6のデュアルスタックに対応し、IPv6の通信の負荷分散が可能であること。			
	⑨ WebベースのGUIとCLIで設定が可能であること。また、CLIでは、SSHをサポートすること。			
	⑩ プログラミングを用いたL7パケットの振り分けルール作成機能を有すること。			
	ハードウェア要件			
	① 1000BASE-Tのポートを8ポート以上有すること。			
	② 消費電力が200W以下であること。			
	③ 負荷分散時のスループットは、4Gbps以上であること。			
	(カ) 回線負荷分散装置要件			
	ソフトウェア要件			
	① アウトバウンド/インバウンドの双方向でインターネット回線の回線負荷分散機能を有すること。			
	② ラウンドロビン、最小コネクション方式等の分散方式に対応すること。			
	③ 一方のISPで障害が発生した場合に、他方のISPにトラフィックを振り分ける機能を有すること。			
	④ WebベースのGUIとCLIで設定が可能であること。また、CLIでは、SSHをサポートすること。			
	⑤ プログラミングを用いたL7パケットの振り分けルール作成機能を有すること。			

別紙1－2　要件定義書（サービス・機器）

項番号	内容	提案内容	補足資料	記載箇所
	ハードウェア要件			
	① 100BASE-TX/1000BASE-Tのポートを4ポート以上有すること。			
	② 消費電力が200W以下であること。			
	③ 負荷分散時のスループットは、1Gbps以上であること。			
イ	インターネット回線（ディザスタリカバリサイト）			
	(ア) インターネット回線接続ルータ要件			
	ソフトウェア要件			
	①「別添1 拠点回線・機器一覧表」 ②回線接続ルータスペック要件一覧のType Ⅰを参照すること。			
	ハードウェア要件			
	①「別添1 拠点回線・機器一覧表」 ②回線接続ルータスペック要件一覧のType Ⅰを参照すること。			
	(イ) インターネット回線接続スイッチ要件			
	ソフトウェア要件			
	① レイヤ2のスイッチングを行えること。			
	② スパニングツリー機能として、IEEE802.1d、IEEE802.1s、IEEE802.1w又はこれらと同等の機能を有すること。			
	③ IEEE802.1pのCOS、DSCPの書き換え、書き込み及びDSCPに基づく優先制御が可能であること。			
	④ ACL又は同等の方式によるアクセス制限が行えること。			
	⑤ IEEE802.3ah/UDLDにより、片方向リンクを検出することが可能であること。			
	⑥ ポートに対しての自動障害検知機能及び自動復帰機能を有すること。			
	⑦ 指定したイベントが発生した際に、電子メールの通知等が自動で行えること。			
	ハードウェア要件			
	① ボックス型筐体であること。			
	② 消費電力が40W以下であること。			
	③ 10Gbps以上のスイッチング容量を有すること。			
	④ 11.9Mpps以上のパケット処理能力を有すること。			
	⑤ 100BASE-TX/1000BASE-Tを8ポート以上有すること。			
	⑥ 100BASE-TX/1000BASE-TとSFPの排他ポートを1ポート以上有すること。			
	(ウ) インターネット接続DMZスイッチ要件			
	ソフトウェア要件			
	① レイヤ2及びレイヤ3のスイッチングを行えること。また、ハードウェアによるIPv4及びIPv6のルーティングに対応すること。			
	② スパニングツリー機能として、IEEE802.1d、IEEE802.1s、IEEE802.1w又はこれらと同等の機能を有すること。			
	③ IEEE802.1pのCOS、TOS及びDSCPの書換え、書き込み、DSCPに基づく優先制御が可能であること。			
	④ ACL又は同等の方式によるアクセス制限が行えること。			
	⑤ IEEE802.3ah/UDLDにより、片方向リンクを検出することが可能であること。			
	⑥ ポートに対しての自動障害検知機能及び自動復帰機能を有すること。			
	⑦ 指定したイベントが発生した際に、電子メールの通知等が自動で行えること。			
	ハードウェア要件			
	① シャーシ型筐体又はボックス型筐体であること。			
	② 消費電力が150W以下であること。			
	③ 160Gbps以上のスイッチング容量を有すること。			
	④ 101.2Mpps以上のパケット処理能力を有すること。			
	⑤ 100BASE-TX/1000BASE-Tを48ポート以上有すること。			
	⑥ 拡張により、1000BASEのSFPを4ポート以上又は10GBASEのSFPを2ポート以上搭載できること。			

別紙1－2　要件定義書（サービス・機器）

項番号	内容	提案内容	補足資料	記載箇所
6　本省WAN				
（1）概要				
	本省、各地方拠点及びディザスタリカバリサイトで相互に通信を行い総務省LANサービスを利用するため、本省WAN（本省側におけるネットワーク及び回線）を提供する。 閉域網を使用した通信環境を提供する。 具体的要件について、以下に記載する。			
（2）構築要件				
ア　本省WAN回線				
	① WAN回線には主回線と副回線を準備し、主回線は帯域確保型（1回線）、副回線は帯域確保型（1回線）とベストエフォート型（1回線）の回線を利用し、冗長化すること。			
	② WAN回線は、各々独立した閉域網であること。			
	③ WAN回線の網内は、冗長構成をとること。			
	④ 主回線と副回線で通信事業者を分けること。また、主回線及び副回線を収容する機器及び局舎は分離すること。			
	⑤ 主回線、副回線ともにIPネットワーク上で利用できるすべてのプロトコルを利用可能な回線を提供すること。また、ルーティングプロトコルの使用に制限がないこと。			
	⑥ 帯域確保型の回線については、回線終端装置を除いたアクセス回線を含む網内の月間稼働率が99.99%以上であること。また、本要件がWeb等公開情報に提示されていること。			
	⑦ 主回線および副回線（帯域確保型の回線)については、網内遅延時間がIPパケットの往復転送時間の月間平均値が35ミリ秒以内であること。また、本要件がWeb等公開情報に提示されていること。			
	⑧ 帯域確保型の回線については、回線障害時、1時間以内に再び利用できる状態に回復できること。また、本要件がWeb等公開情報に提示されていること。			
	⑨ 回線終端装置とのインターフェースは、イーサネットインタフェースで提供すること。			
	⑩ 主回線は、500Mbps以上で接続し、全ての帯域で速度を確保するものとする。			
	⑪ 帯域確保型の副回線は、600Mbps以上で接続し、全ての帯域で速度を確保するものとする。			
	⑫ ベストエフォート型の副回線は、1Gbps以上で接続するものとする。			
	⑬ WAN回線を通る通信は暗号化すること。			
	⑭ 帯域確保型の回線は、主回線と副回線の合計帯域が1.1Gbps以上を満たす場合、主副それぞれの帯域変更を可とする。ただし、コミュニケーションサービスやファイル共有サービスの通信に影響がないよう考慮すること。			
（3）機器等要件				
（ア）総務省 WAN 回線接続ルータ要件				
ソフトウェア要件				
	①「別添1 拠点回線・機器一覧表」 ②回線接続ルータスペック要件一覧のType　IIを参照すること。			
ハードウェア要件				
	①「別添1 拠点回線・機器一覧表」 ②回線接続ルータスペック要件一覧のType　IIを参照すること。			
（イ）総務省 WAN 回線接続スイッチ要件				
ソフトウェア要件				
	① レイヤ2及びレイヤ3のスイッチングを行えること。また、ハードウェアによるIPv4及びIPv6のルーティングに対応すること。			
	② スパニングツリー機能として、IEEE802.1d、IEEE802.1s、IEEE802.1w又はこれらと同等の機能を有すること。			
	③ IEEE802.1pのCOS、TOS及びDSCPの書換え、書き込み、DSCPに基づく優先制御が可能であること。			
	④ ACL又は同等の方式によるアクセス制限が行えること。			

別紙1－2　要件定義書（サービス・機器）

項番号	内容	提案内容	補足資料	記載箇所
	⑤ IEEE802.3ah/UDLDにより、片方向リンクを検出することが可能であること。			
	⑥ ポートに対しての自動障害検知機能及び自動復帰機能を有すること。			
	⑦ 指定したイベントが発生した際に、電子メールの通知等が自動で行えること。			
	⑧ ブロードキャスト及びマルチキャストの流量を制限する機能を持つこと。			
	ハードウェア要件			
	① シャーシ型筐体又はボックス型筐体であること。			
	② 消費電力が110W以下であること。			
	③ 90Gbps以上のスイッチング容量を有すること。			
	④ 65.5Mpps以上のパケット処理能力を有すること。			
	⑤ 100BASE-TX/1000BASE-Tを24ポート以上有すること。			
	⑥ 拡張により、1000BASEのSFPを4ポート以上又は10GBASEのSFPを2ポート以上搭載できること。			
	(ウ) 政府共通ネットワーク回線接続スイッチ要件			
	ソフトウェア要件			
	① レイヤ2のスイッチングを行えること。			
	② スパニングツリー機能として、IEEE802.1d、IEEE802.1s、IEEE802.1w又はこれらと同等の機能を有すること。			
	③ IEEE802.1pのCOS、DSCPの書換え、書き込み、DSCPに基づく優先制御が可能であること。			
	④ ACL又は同等の方式によるアクセス制限が行えること。			
	⑤ IEEE802.3ah/UDLDにより、片方向リンクを検出することが可能であること。			
	⑥ ポートに対しての自動障害検知機能及び自動復帰機能を有すること。			
	⑦ ブロードキャスト及びマルチキャストの流量を制限する機能を持つこと。			
	ハードウェア要件			
	① ボックス型筐体であること。			
	② 消費電力が30W以下であること。			
	③ 10Gbps以上のスイッチング容量を有すること。			
	④ 11.9Mpps以上のパケット処理能力を有すること。			
	⑤ 100BASE-TX/1000BASE-Tを8ポート以上有すること。			
	⑥ 100BASE-TX/1000BASE-TとSFPの排他ポートを1ポート以上有すること。			
	(エ) 政府共通ネットワークDMZスイッチ要件			
	ソフトウェア要件			
	① レイヤ2及びレイヤ3のスイッチングを行えること。また、ハードウェアによるIPv4及びIPv6のルーティングに対応すること。			
	② スパニングツリー機能として、IEEE802.1d、IEEE802.1s、IEEE802.1w又はこれらと同等の機能を有すること。			
	③ IEEE802.1pのCOS、TOS及びDSCPの書換え、書き込み、DSCPに基づく優先制御が可能であること。			
	④ ACL又は同等の方式によるアクセス制限が行えること。			
	⑤ IEEE802.3ah/UDLDにより、片方向リンクを検出することが可能であること。			
	⑥ ポートに対しての自動障害検知機能及び自動復帰機能を有すること。			
	⑦ 指定したイベントが発生した際に、電子メールの通知等が自動で行えること。			
	⑧ ブロードキャスト及びマルチキャストの流量を制限する機能を持つこと。			
	ハードウェア要件			
	① シャーシ型筐体又はボックス型筐体であること。			
	② 消費電力が110W以下であること。			
	③ 90Gbps以上のスイッチング容量を有すること。			
	④ 65.5Mpps以上のパケット処理能力を有すること。			

別紙1－2　要件定義書（サービス・機器）

項番号	内容	提案内容	補足資料	記載箇所
	⑤ 100BASE-TX/1000BASE-Tを24ポート以上有すること。			
	⑥ 拡張により、1000BASEのSFPを4ポート以上又は10GBASEのSFPを2ポート以上搭載できること。			
	（オ）政府共通ネットワーク業務システム接続スイッチ要件			
	ソフトウェア要件			
	① レイヤ2のスイッチングを行えること。			
	② スパニングツリー機能として、IEEE802.1d、IEEE802.1s、IEEE802.1w又はこれらと同等の機能を有すること。			
	③ IEEE802.1pのCOS、DSCPに基づく優先制御が可能であること。			
	④ IEEE802.3ah/UDLDにより、片方向リンクを検出することが可能であること。			
	⑤ ポートに対しての自動障害検知機能及び自動復帰機能を有すること。			
	ハードウェア要件			
	① ボックス型筐体であること。			
	② 消費電力が37.1W以下であること。			
	③ 108Gbps以上のスイッチング容量を有すること。			
	④ 71.4Mpps以上のパケット処理能力を有すること。			
	⑤ 100BASE-TX/1000BASE-Tを24ポート以上有すること。			
	⑥ SFPを2ポート以上有すること。			
7　拠点WAN				
（1）概要				
	本省、各地方拠点及びディザスタリカバリサイトで相互に通信を行うため、拠点WAN（拠点側におけるネットワーク及び回線）を提供する。 閉域網を使用した通信環境を提供する。 具体的要件について、以下に記載する。			
（2）構築要件				
ア　総務省第2庁舎				
	① WAN回線は、主/副の冗長構成とすること。また、副回線も通常時、利用可能な構成とすること。ただし、L3SWが導入されていない拠点については、その必要性を考慮して構成すること。			
	② WAN回線は、各々独立した閉域網であること。			
	③ WAN回線の網内は、冗長構成をとること。			
	④ アクセス回線も併せて、主回線と副回線で通信事業者を分けること。また、主回線及び副回線を収容する機器及び局舎（ビル）は分離すること。			
	⑤ 主回線、副回線ともにIPネットワーク上で利用できるすべてのプロトコルを利用可能な回線を提供すること。また、ルーティングプロトコルの使用に制限がないこと。			
	⑥ 主回線は、回線終端装置を除いたアクセス回線を含む網内の月間稼働率が99.99%以上であること。また、本要件がWeb等公開情報に提示されていること。			
	⑦ 主回線の網内遅延時間は、IPパケットの往復転送時間の月間平均値が35ミリ秒以内であること。また、本要件がWeb等公開情報に提示されていること。			
	⑧ 帯域確保型の回線については、障害発生時、1時間以内に再び利用できる状態に回復できること。また、本要件がWeb等公開情報に提示されていること。			
	⑨ 回線終端装置のとのインターフェースは、イーサネットインタフェースで提供すること。			
	⑩ 他の拠点に影響を及ぼすことなく、当該対象拠点の移転、増速、廃止が可能であること。			
	⑪ 主回線は、200Mbps以上で接続し、全ての帯域で速度を確保するものとする。			
	⑫ 副回線は、1Gbps以上で接続すること。ただし、帯域の速度はベストエフォート型を利用してもよい。			
	⑬ WAN回線を通る通信は暗号化すること。			

別紙1－2　要件定義書（サービス・機器）

項番号	内容	提案内容	補足資料	記載箇所
イ	公害等調整委員会（4号館）、自治大学校、情報通信政策研究所、消防大学校及び消防研究センター			
①	WAN回線は、主/副の冗長構成とすること。また、副回線も通常時、利用可能な構成とすること。ただし、L3SWが導入されていない拠点については、その必要性を考慮して構成すること。			
②	WAN回線は、各々独立した閉域網であること。			
③	WAN回線の網内は、冗長構成をとること。			
④	アクセス回線も併せて、主回線と副回線で通信事業者を分けること。また、主回線及び副回線を収容する機器及び局舎（ビル）は分離すること。			
⑤	主回線、副回線ともにIPネットワーク上で利用できるすべてのプロトコルを利用可能な回線を提供すること。また、ルーティングプロトコルの使用に制限がないこと。			
⑥	主回線は、回線終端装置を除いたアクセス回線を含む網内の月間稼働率が99.99%以上であること。また、本要件がWeb等公開情報に提示されていること。			
⑦	主回線の網内遅延時間は、IPパケットの往復転送時間の月間平均値が35ミリ秒以内であること。また、本要件がWeb等公開情報に提示されていること。			
⑧	帯域確保型の回線については、障害発生時、1時間以内に再び利用できる状態に回復できること。また、本要件がWeb等公開情報に提示されていること。			
⑨	回線終端装置のとのインターフェースは、イーサネットインタフェースで提供すること。			
⑩	他の拠点に影響を及ぼすことなく、当該対象拠点の移転、増速、廃止が可能であること。			
⑪	主回線は、100Mbps以上で接続し、全ての帯域で速度を確保するものとする。			
⑫	副回線は、1Gbps以上で接続すること。ただし、帯域の速度はベストエフォート型を利用してもよい。			
⑬	WAN回線を通る通信は暗号化すること。			
ウ	アジア太平洋統計研究所、国会連絡室、内閣人事局、情報公開・個人情報保護審査会及び官民競争入札等監理事務局（永田町合同庁舎）			
①	WAN回線は、主/副の冗長構成とすること。また、副回線も通常時、利用可能な構成とすること。ただし、L3SWが導入されていない拠点については、その必要性を考慮して構成すること。			
②	WAN回線は、各々独立した閉域網であること。			
③	WAN回線の網内は、冗長構成をとること。			
④	アクセス回線も併せて、主回線と副回線で通信事業者を分けること。また、主回線及び副回線を収容する機器及び局舎（ビル）は分離すること。			
⑤	主回線、副回線ともにIPネットワーク上で利用できるすべてのプロトコルを利用可能な回線を提供すること。また、ルーティングプロトコルの使用に制限がないこと。			
⑥	主回線は、回線終端装置を除いたアクセス回線を含む網内の月間稼働率が99.99%以上であること。また、本要件がWeb等公開情報に提示されていること。			
⑦	主回線の網内遅延時間は、IPパケットの往復転送時間の月間平均値が35ミリ秒以内であること。また、本要件がWeb等公開情報に提示されていること。			
⑧	帯域確保型の回線については、障害発生時、1時間以内に再び利用できる状態に回復できること。また、本要件がWeb等公開情報に提示されていること。			
⑨	回線終端装置のとのインターフェースは、イーサネットインタフェースで提供すること。			
⑩	他の拠点に影響を及ぼすことなく、当該対象拠点の移転、増速、廃止が可能であること。			
⑪	主回線は、100Mbps以上で接続すること。ただし、帯域のうち10Mbps以上の速度を確保すること。			
⑫	副回線は、1Gbps以上で接続すること。ただし、帯域の速度はベストエフォート型を利用してもよい。			
⑬	WAN回線を通る通信は暗号化すること。			

別紙1－2　要件定義書（サービス・機器）

項番号	内容	提案内容	補足資料	記載箇所
エ　総合通信局及び沖縄総合通信事務所				
①	WAN回線は、主/副の冗長構成とすること。また、副回線も通常時、利用可能な構成とすること。ただし、L3SWが導入されていない拠点については、その必要性を考慮して構成すること。			
②	WAN回線は、各々独立した閉域網であること。			
③	WAN回線の網内は、冗長構成をとること。			
④	アクセス回線も併せて、主回線と副回線で通信事業者を分けること。また、主回線及び副回線を収容する機器及び局舎（ビル）は分離すること。			
⑤	主回線、副回線ともにIPネットワーク上で利用できるすべてのプロトコルを利用可能な回線を提供すること。また、ルーティングプロトコルの使用に制限がないこと。			
⑥	主回線は、回線終端装置を除いたアクセス回線を含む網内の月間稼働率が99.99%以上であること。また、本要件がWeb等公開情報に提示されていること。			
⑦	主回線の網内遅延時間は、IPパケットの往復転送時間の月間平均値が35ミリ秒以内であること。また、本要件がWeb等公開情報に提示されていること。			
⑧	帯域確保型の回線については、障害発生時、1時間以内に再び利用できる状態に回復できること。また、本要件がWeb等公開情報に提示されていること。			
⑨	回線終端装置のとのインターフェースは、イーサネットインタフェースで提供すること。			
⑩	他の拠点に影響を及ぼすことなく、当該対象拠点の移転、増速、廃止が可能であること。			
⑪	主回線は、100Mbps以上で接続し、全ての帯域で速度を確保するものとする。			
⑫	副回線は、1Gbps以上で接続すること。ただし、帯域の速度はベストエフォート型を利用してもよい。			
⑬	WAN回線を通る通信は暗号化すること。			
オ　三浦電波監視センター				
①	WAN回線は、主/副の冗長構成とすること。また、副回線も通常時、利用可能な構成とすること。ただし、L3SWが導入されていない拠点については、その必要性を考慮して構成すること。			
②	WAN回線は、各々独立した閉域網であること。			
③	WAN回線の網内は、冗長構成をとること。			
④	アクセス回線も併せて、主回線と副回線で通信事業者を分けること。また、主回線及び副回線を収容する機器及び局舎（ビル）は分離すること。			
⑤	主回線、副回線ともにIPネットワーク上で利用できるすべてのプロトコルを利用可能な回線を提供すること。また、ルーティングプロトコルの使用に制限がないこと。			
⑥	主回線は、回線終端装置を除いたアクセス回線を含む網内の月間稼働率が99.99%以上であること。また、本要件がWeb等公開情報に提示されていること。			
⑦	主回線の網内遅延時間は、IPパケットの往復転送時間の月間平均値が35ミリ秒以内であること。また、本要件がWeb等公開情報に提示されていること。			
⑧	帯域確保型の回線については、障害発生時、1時間以内に再び利用できる状態に回復できること。また、本要件がWeb等公開情報に提示されていること。			
⑨	回線終端装置のとのインターフェースは、イーサネットインタフェースで提供すること。			
⑩	他の拠点に影響を及ぼすことなく、当該対象拠点の移転、増速、廃止が可能であること。			
⑪	主回線は、100Mbps以上で接続すること。ただし、帯域のうち10Mbps以上の速度を確保すること。			
⑫	副回線は、1Gbps以上で接続すること。ただし、帯域の速度はベストエフォート型を利用してもよい。			
⑬	WAN回線を通る通信は暗号化すること。			

別紙1－2　要件定義書（サービス・機器）

項番号	内容	提案内容	補足資料	記載箇所
カ	関東管区行政評価局、千葉行政評価事務所、東京行政評価事務所、神奈川行政評価事務所、中部管区行政評価局、近畿管区行政評価局、兵庫行政評価事務所、中国四国管区行政評価局、四国行政評価支局、九州管区行政評価局			
①	WAN回線は、主/副の冗長構成とすること。また、副回線も通常時、利用可能な構成とすること。ただし、L3SWが導入されていない拠点については、その必要性を考慮して構成すること。			
②	WAN回線は、各々独立した閉域網であること。			
③	WAN回線の網内は、冗長構成をとること。			
④	アクセス回線も併せて、主回線と副回線で通信事業者を分けること。また、主回線及び副回線を収容する機器及び局舎（ビル）は分離すること。			
⑤	主回線、副回線ともにIPネットワーク上で利用できるすべてのプロトコルを利用可能な回線を提供すること。また、ルーティングプロトコルの使用に制限がないこと。			
⑥	主回線は、回線終端装置を除いたアクセス回線を含む網内の月間稼働率が99.99%以上であること。また、本要件がWeb等公開情報に提示されていること。			
⑦	主回線の網内遅延時間は、IPパケットの往復転送時間の月間平均値が35ミリ秒以内であること。また、本要件がWeb等公開情報に提示されていること。			
⑧	帯域確保型の回線については、障害発生時、1時間以内に再び利用できる状態に回復できること。また、本要件がWeb等公開情報に提示されていること。			
⑨	回線終端装置のとのインターフェースは、イーサネットインタフェースで提供すること。			
⑩	他の拠点に影響を及ぼすことなく、当該対象拠点の移転、増速、廃止が可能であること。			
⑪	主回線は、100Mbps以上で接続し、全ての帯域で速度を確保するものとする。			
⑫	副回線は、1Gbps以上で接続すること。ただし、帯域の速度はベストエフォート型を利用してもよい。			
⑬	WAN回線を通る通信は暗号化すること。			
キ	北海道管区行政評価局、東北管区行政評価局、長野行政評価事務所			
①	北海道管区行政評価局：北海道総合通信局と共用			
②	東北管区行政評価局：東北総合通信局と共用			
③	長野行政評価事務所：信越総合通信局と共用			
ク	行政評価事務所（千葉行政評価事務所、東京行政評価事務所、神奈川行政評価事務所、長野行政評価事務所以外）及び行政評価分室			
①	WAN回線は、主/副の冗長構成とすること。また、副回線も通常時、利用可能な構成とすること。ただし、L3SWが導入されていない拠点については、その必要性を考慮して構成すること。			
②	WAN回線は、各々独立した閉域網であること。			
③	WAN回線の網内は、冗長構成をとること。			
④	アクセス回線も併せて、主回線と副回線で通信事業者を分けること。また、主回線及び副回線を収容する機器及び局舎（ビル）は分離すること。			
⑤	主回線、副回線ともにIPネットワーク上で利用できるすべてのプロトコルを利用可能な回線を提供すること。また、ルーティングプロトコルの使用に制限がないこと。			
⑥	主回線は、回線終端装置を除いたアクセス回線を含む網内の月間稼働率が99.99%以上であること。また、本要件がWeb等公開情報に提示されていること。			
⑦	主回線の網内遅延時間は、IPパケットの往復転送時間の月間平均値が35ミリ秒以内であること。また、本要件がWeb等公開情報に提示されていること。			
⑧	帯域確保型の回線については、障害発生時、1時間以内に再び利用できる状態に回復できること。また、本要件がWeb等公開情報に提示されていること。			
⑨	回線終端装置のとのインターフェースは、イーサネットインタフェースで提供すること。			
⑩	他の拠点に影響を及ぼすことなく、当該対象拠点の移転、増速、廃止が可能であること。			
⑪	主回線は、100Mbps以上で接続すること。ただし、帯域のうち10Mbps以上の速度を確保すること。			

別紙1－2　要件定義書（サービス・機器）

項番号	内容	提案内容	補足資料	記載箇所
	⑫ 副回線は、1Gbps以上で接続すること。ただし、帯域の速度はベストエフォート型を利用してもよい。			
	⑬ WAN回線を通る通信は暗号化すること。			
ケ 行政管理局宮城分室、行政管理局大阪分室				
	① WAN回線は、主/副の冗長構成とすること。また、副回線も通常時、利用可能な構成とすること。ただし、L3SWが導入されていない拠点については、その必要性を考慮して構成すること。			
	② WAN回線は、各々独立した閉域網であること。			
	③ WAN回線の網内は、冗長構成をとること。			
	④ アクセス回線も併せて、主回線と副回線で通信事業者を分けること。また、主回線及び副回線を収容する機器及び局舎（ビル）は分離すること。			
	⑤ 主回線、副回線ともにIPネットワーク上で利用できるすべてのプロトコルを利用可能な回線を提供すること。また、ルーティングプロトコルの使用に制限がないこと。			
	⑥ 主回線は、回線終端装置を除いたアクセス回線を含む網内の月間稼働率が99.99%以上であること。また、本要件がWeb等公開情報に提示されていること。			
	⑦ 主回線の網内遅延時間は、IPパケットの往復転送時間の月間平均値が35ミリ秒以内であること。また、本要件がWeb等公開情報に提示されていること。			
	⑧ 帯域確保型の回線については、障害発生時、1時間以内に再び利用できる状態に回復できること。また、本要件がWeb等公開情報に提示されていること。			
	⑨ 回線終端装置のとのインターフェースは、イーサネットインタフェースで提供すること。			
	⑩ 他の拠点に影響を及ぼすことなく、当該対象拠点の移転、増速、廃止が可能であること。			
	⑪ 主回線は、100Mbps以上で接続すること。ただし、帯域のうち10Mbps以上の速度を確保すること。			
	⑫ 副回線は、1Gbps以上で接続すること。ただし、帯域の速度はベストエフォート型を利用してもよい。			
	⑬ WAN回線を通る通信は暗号化すること。			
コ ディザスタリカバリサイト				
	① WAN回線は、主/副の冗長構成とすること。ただし、副回線も通常時、利用可能な構成とすること。			
	② WAN回線は、各々独立した閉域網であること。			
	③ WAN回線の網内は、冗長構成をとること。			
	④ アクセス回線も併せて、主回線と副回線で通信事業者を分けること。また、主回線及び副回線を収容する機器及び局舎（ビル）は分離すること。			
	⑤ 主回線、副回線ともにIPネットワーク上で利用できるすべてのプロトコルを利用可能な回線を提供すること。また、ルーティングプロトコルの使用に制限がないこと。			
	⑥ 主回線は、回線終端装置を除いたアクセス回線を含む網内の月間稼働率が99.99%以上であること。また、本要件がWeb等公開情報に提示されていること。			
	⑦ 主回線の網内遅延時間は、IPパケットの往復転送時間の月間平均値が35ミリ秒以内であること。また、本要件がWeb等公開情報に提示されていること。			
	⑧ 帯域確保型の回線については、障害発生時、1時間以内に再び利用できる状態に回復できること。また、本要件がWeb等公開情報に提示されていること。			
	⑨ 回線終端装置のとのインターフェースは、イーサネットインタフェースで提供すること。			
	⑩ 他の拠点に影響を及ぼすことなく、当該対象拠点の移転、増速、廃止が可能であること。			
	⑪ WAN回線の帯域は、ディザスタリカバリサービスの設計を踏まえた検討とすること。ただし、目安として主回線200Mbps以上、副回線300Mbps以上を想定している。			
	⑫ WAN回線を通る通信は暗号化すること。			
	⑬ 主回線と副回線の合計帯域が500Mbps以上を満たす場合、主副それぞれの帯域変更を可とする。ただし、コミュニケーションサービスやファイル共有サービスの通信に影響がないよう考慮すること。			

別紙1－2　要件定義書（サービス・機器）

項番号	内容	提案内容	補足資料	記載箇所
(3)	**機器等要件**			
ア	総務省第二庁舎			
(ア)	WAN回線接続ルータ要件			
	ソフトウェア要件			
	①「別添1 拠点回線・機器一覧表」 ②回線接続ルータスペック要件一覧のType IIIを参照すること。			
	ハードウェア要件			
	①「別添1 拠点回線・機器一覧表」 ②回線接続ルータスペック要件一覧のType IIIを参照すること。			
イ	公害等調整委員会			
(ア)	WAN回線接続ルータ要件			
	ソフトウェア要件			
	①「別添1 拠点回線・機器一覧表」 ②回線接続ルータスペック要件一覧のType IIIを参照すること。			
	ハードウェア要件			
	①「別添1 拠点回線・機器一覧表」 ②回線接続ルータスペック要件一覧のType IIIを参照すること。			
ウ	自治大学校			
(ア)	WAN回線接続ルータ要件			
	ソフトウェア要件			
	①「別添1 拠点回線・機器一覧表」 ②回線接続ルータスペック要件一覧のType IIIを参照すること。			
	ハードウェア要件			
	①「別添1 拠点回線・機器一覧表」 ②回線接続ルータスペック要件一覧のType IIIを参照すること。			
エ	情報通信政策研究所			
(ア)	WAN回線接続ルータ要件			
	ソフトウェア要件			
	①「別添1 拠点回線・機器一覧表」 ②回線接続ルータスペック要件一覧のType IIIを参照すること。			
	ハードウェア要件			
	①「別添1 拠点回線・機器一覧表」 ②回線接続ルータスペック要件一覧のType IIIを参照すること。			
オ	消防大学校及び消防研究センター			
(ア)	WAN回線接続ルータ要件			
	ソフトウェア要件			
	①「別添1 拠点回線・機器一覧表」 ②回線接続ルータスペック要件一覧のType IIIを参照すること。			
	ハードウェア要件			
	①「別添1 拠点回線・機器一覧表」 ②回線接続ルータスペック要件一覧のType IIIを参照すること。			
カ	アジア太平洋統計研修所、国会連絡室			
(ア)	WAN回線接続ルータ要件			
	ソフトウェア要件			
	①「別添1 拠点回線・機器一覧表」 ②回線接続ルータスペック要件一覧のType Vを参照すること。			
	ハードウェア要件			
	①「別添1 拠点回線・機器一覧表」 ②回線接続ルータスペック要件一覧のType Vを参照すること。			
キ	総合通信局及び沖縄総合通信事務所			
(ア)	WAN回線接続ルータ要件			
	ソフトウェア要件			
	①「別添1 拠点回線・機器一覧表」 ②回線接続ルータスペック要件一覧のType IIIを参照すること。			
	ハードウェア要件			
	①「別添1 拠点回線・機器一覧表」 ②回線接続ルータスペック要件一覧のType IIIを参照すること。			

別紙1－2　要件定義書（サービス・機器）

項番号	内容	提案内容	補足資料	記載箇所
	ク　三浦電波監視センター			
	（ア）WAN回線接続ルータ要件			
	ソフトウェア要件			
	①「別添1 拠点回線・機器一覧表」 ②回線接続ルータスペック要件一覧のType　Vを参照すること。			
	ハードウェア要件			
	①「別添1 拠点回線・機器一覧表」 ②回線接続ルータスペック要件一覧のType　Vを参照すること。			
	ケ　管区行政評価（支）局、行政評価事務所、行政評価分室、内閣人事局、情報公開・個人情報保護審査会及び官民競争入札等監理事務局（永田町合同庁舎）			
	（ア）WAN回線接続ルータ①要件			
	ソフトウェア要件			
	①「別添1 拠点回線・機器一覧表」 ②回線接続ルータスペック要件一覧のType　IIIを参照すること。			
	ハードウェア要件			
	①「別添1 拠点回線・機器一覧表」 ②回線接続ルータスペック要件一覧のType　IIIを参照すること。			
	（イ）WAN回線接続ルータ②要件			
	ソフトウェア要件			
	①「別添1 拠点回線・機器一覧表」 ②回線接続ルータスペック要件一覧のType　Vを参照すること。			
	ハードウェア要件			
	①「別添1 拠点回線・機器一覧表」 ②回線接続ルータスペック要件一覧のType　Vを参照すること。			
	コ　行政管理局宮城分室、行政管理局大阪分室			
	（ア）WAN回線接続ルータ要件			
	ソフトウェア要件			
	①「別添1 拠点回線・機器一覧表」 ②回線接続ルータスペック要件一覧のType　Vを参照すること。			
	ハードウェア要件			
	①「別添1 拠点回線・機器一覧表」 ②回線接続ルータスペック要件一覧のType　Vを参照すること。			
	サ　ディザスタリカバリサイト			
	（ア）WAN回線接続ルータ要件			
	ソフトウェア要件			
	①「別添1 拠点回線・機器一覧表」 ②回線接続ルータスペック要件一覧のType　IIを参照すること。			
	ハードウェア要件			
	①「別添1 拠点回線・機器一覧表」 ②回線接続ルータスペック要件一覧のType　IIを参照すること。			
8	外部監視室用回線			
(1)	概要			
	構築や移行の際、外部に設置した機器と本省に設置した機器間で必要なデータの転送を行うため、外部監視室用回線を提供する。 具体的要件について、以下に記載する。			
(2)	構築要件			
	ア　外部監視室用回線（構築時）			
	① 外部監視室用回線（構築時）は、主/副の冗長構成とすること。			
	② 外部監視室用回線（構築時）は、各々独立した閉域網であること。			
	③ 外部監視室用回線（構築時）の網内は、冗長構成をとること。			
	④ アクセス回線も併せて、主回線と副回線で通信事業者を分けること。また、主回線及び副回線を収容する機器及び局舎（ビル）は分離すること。			
	⑤ 外部監視室用回線（構築時）はIPネットワーク上で利用できるすべてのプロトコルを利用可能な回線を提供すること。また、ルーティングプロトコルの使用に制限がないこと。			

別紙1－2　要件定義書（サービス・機器）

項番号	内容	提案内容	補足資料	記載箇所
	⑥ 主回線は、回線終端装置を除いたアクセス回線を含む網内の月間稼働率が99.99%以上であること。また、本要件がWeb等公開情報に提示されていること。			
	⑦ 主回線の網内遅延時間は、IPパケットの往復転送時間の月間平均値が35ミリ秒以内であること。また、本要件がWeb等公開情報に提示されていること。			
	⑧ 外部監視室用回線（構築時）の障害発生時、1時間以内に再び利用できる状態に回復できること。また、本要件がWeb等公開情報に提示されていること。			
	⑨ 回線終端装置のとのインターフェースは、イーサネットインタフェースで提供すること。			
	⑩ 回線の帯域は、構築及び移行方式を踏まえた検討とすること。現行総務省LAN調達時の回線は、主回線1Gbps、副回線100Mbpsで接続していたため、同程度を想定している。			
	イ　外部監視室用回線（運用時）			
	① 外部監視室用回線（運用時）は、独立した閉域網であること。			
	② 外部監視室用回線（運用時）はIPネットワーク上で利用できるすべてのプロトコルを利用可能なこと。また、ルーティングプロトコルの使用に制限がないこと。			
	③ 外部監視室用回線（運用時）は、回線終端装置を除いたアクセス回線を含む網内の月間稼働率が99.99%以上であること。また、本要件がWeb等公開情報に提示されていること。			
	④ 外部監視室用回線（運用時）の網内遅延時間は、IPパケットの往復転送時間の月間平均値が35ミリ秒以内であること。また、本要件がWeb等公開情報に提示されていること。			
	⑤ 外部監視室用回線（運用時）の障害発生時、1時間以内に再び利用できる状態に回復できること。また、本要件がWeb等公開情報に提示されていること。			
	⑥ 回線終端装置のとのインターフェースは、イーサネットインタフェースで提供すること。			
	⑦ 回線の帯域は、運用要件の内容を踏まえ検討を行うこと。現行総務省LAN調達時の回線は、主回線100Mbpsで接続されている。			
	(3) 機器等要件			
	(ア) 外部監視室ルータ①要件			
	ソフトウェア要件			
	①「別添1 拠点回線・機器一覧表」 ②回線接続ルータスペック要件一覧のType　IIを参照すること。			
	ハードウェア要件			
	①「別添1 拠点回線・機器一覧表」 ②回線接続ルータスペック要件一覧のType　IIを参照すること。			
	(イ) 外部監視室ルータ②要件			
	ソフトウェア要件			
	①「別添1 拠点回線・機器一覧表」 ②回線接続ルータスペック要件一覧のType　IVを参照すること。			
	ハードウェア要件			
	①「別添1 拠点回線・機器一覧表」 ②回線接続ルータスペック要件一覧のType　IVを参照すること。			

別紙1－3　要件定義書（回線）

本資料は総務省が想定する最低帯域を記載している。想定最低帯域以上でより最適な帯域があれば提案すること。

内容					提案内容	補足資料	記載箇所
本省/地方拠点名	回線	回線種別	帯域	備考			
インターネット接続回線							
本省	インターネット回線1	ベストエフォート	1Gbps				
	インターネット回線2	帯域確保	200Mbps				
	インターネット回線3	ベストエフォート	1Gbps				
	インターネット回線4	帯域確保	300Mbps				
ディザスタリカバリサイト	インターネット回線1	帯域確保	200Mbps				
	インターネット回線2	ベストエフォート	1Gbps				
WAN回線							
本省	主回線	帯域確保	500Mbps				
	副回線	帯域確保	600Mbps				
	副回線	ベストエフォート	1Gbps				
総務省第2庁舎	主回線	帯域確保	200Mbps				
	副回線	ベストエフォート	1Gbps				
公害等調整委員会（4号館）	主回線	帯域確保	100Mbps				
	副回線	ベストエフォート	1Gbps				
内閣人事局（8号館）	主回線	一部帯域確保	100Mbps（10Mbps確保）				
	副回線	ベストエフォート	1Gbps				
情報公開・個人情報保護審査会及び官民競争入札等監理事務局（永田町合同庁舎）	主回線	一部帯域確保	100Mbps（10Mbps確保）	H28/4/1～			
	副回線	ベストエフォート	1Gbps				
行政管理局宮城分室	主回線	一部帯域確保	100Mbps（10Mbps確保）				
	副回線	ベストエフォート	1Gbps				
行政管理局大阪分室	主回線	一部帯域確保	100Mbps（10Mbps確保）				
	副回線	ベストエフォート	1Gbps				
自治大学校	主回線	帯域確保	100Mbps				
	副回線	ベストエフォート	1Gbps				
情報通信政策研究所	主回線	帯域確保	100Mbps				
	副回線	ベストエフォート	1Gbps				
アジア太平洋統計研修所	主回線	一部帯域確保	100Mbps（10Mbps確保）				
	副回線	ベストエフォート	1Gbps				
消防大学校及び消防研究センター	主回線	帯域確保	100Mbps				
	副回線	ベストエフォート	1Gbps				
国会連絡室	主回線	一部帯域確保	100Mbps（10Mbps確保）				
	副回線	ベストエフォート	1Gbps				
北海道管区行政評価局	主回線	-	-	北海道総合通信局と共用			
	副回線	-	-	北海道総合通信局と共用			
函館行政評価分室	主回線	一部帯域確保	100Mbps（10Mbps確保）				
	副回線	ベストエフォート	1Gbps				
旭川行政評価分室	主回線	一部帯域確保	100Mbps（10Mbps確保）				
	副回線	ベストエフォート	1Gbps				
釧路行政評価分室	主回線	一部帯域確保	100Mbps（10Mbps確保）				
	副回線	ベストエフォート	1Gbps				
東北管区行政評価局	主回線	-	-	東北総合通信局と共用			
	副回線	-	-	東北総合通信局と共用			
青森行政評価事務所	主回線	一部帯域確保	100Mbps（10Mbps確保）				
	副回線	ベストエフォート	1Gbps				
岩手行政評価事務所	主回線	一部帯域確保	100Mbps（10Mbps確保）				
	副回線	ベストエフォート	1Gbps				
秋田行政評価事務所	主回線	一部帯域確保	100Mbps（10Mbps確保）				
	副回線	ベストエフォート	1Gbps				
山形行政評価事務所	主回線	一部帯域確保	100Mbps（10Mbps確保）				
	副回線	ベストエフォート	1Gbps				

別紙1－3　要件定義書 (回線)

本資料は総務省が想定する最低帯域を記載している。想定最低帯域以上でより最適な帯域があれば提案すること。

内容					提案内容	補足資料	記載箇所
福島行政評価事務所	主回線	一部帯域確保	100Mbps（10Mbps確保）				
	副回線	ベストエフォート	1Gbps				
関東管区行政評価局	主回線	帯域確保	100Mbps				
	副回線	ベストエフォート	1Gbps				
茨城行政評価事務所	主回線	一部帯域確保	100Mbps（10Mbps確保）				
	副回線	ベストエフォート	1Gbps				
栃木行政評価事務所	主回線	一部帯域確保	100Mbps（10Mbps確保）				
	副回線	ベストエフォート	1Gbps				
群馬行政評価事務所	主回線	一部帯域確保	100Mbps（10Mbps確保）				
	副回線	ベストエフォート	1Gbps				
千葉行政評価事務所	主回線	帯域確保	100Mbps				
	副回線	ベストエフォート	1Gbps				
東京行政評価事務所	主回線	帯域確保	100Mbps				
	副回線	ベストエフォート	1Gbps				
神奈川行政評価事務所	主回線	帯域確保	100Mbps				
	副回線	ベストエフォート	1Gbps				
新潟行政評価事務所	主回線	一部帯域確保	100Mbps（10Mbps確保）				
	副回線	ベストエフォート	1Gbps				
山梨行政評価事務所	主回線	一部帯域確保	100Mbps（10Mbps確保）				
	副回線	ベストエフォート	1Gbps				
長野行政評価事務所	主回線	-	-	信越総合通信局と共用			
	副回線	-	-	信越総合通信局と共用			
中部管区行政評価局	主回線	帯域確保	100Mbps				
	副回線	ベストエフォート	1Gbps				
富山行政評価事務所	主回線	一部帯域確保	100Mbps（10Mbps確保）				
	副回線	ベストエフォート	1Gbps				
石川行政評価事務所	主回線	一部帯域確保	100Mbps（10Mbps確保）				
	副回線	ベストエフォート	1Gbps				
岐阜行政評価事務所	主回線	一部帯域確保	100Mbps（10Mbps確保）				
	副回線	ベストエフォート	1Gbps				
静岡行政評価事務所	主回線	一部帯域確保	100Mbps（10Mbps確保）				
	副回線	ベストエフォート	1Gbps				
三重行政評価事務所	主回線	一部帯域確保	100Mbps（10Mbps確保）				
	副回線	ベストエフォート	1Gbps				
近畿管区行政評価局	主回線	帯域確保	100Mbps				
	副回線	ベストエフォート	1Gbps				
福井行政評価事務所	主回線	一部帯域確保	100Mbps（10Mbps確保）				
	副回線	ベストエフォート	1Gbps				
滋賀行政評価事務所	主回線	一部帯域確保	100Mbps（10Mbps確保）				
	副回線	ベストエフォート	1Gbps				
京都行政評価事務所	主回線	一部帯域確保	100Mbps（10Mbps確保）				
	副回線	ベストエフォート	1Gbps				
兵庫行政評価事務所	主回線	一部帯域確保	100Mbps（10Mbps確保）				
	副回線	ベストエフォート	1Gbps				
奈良行政評価事務所	主回線	一部帯域確保	100Mbps（10Mbps確保）				
	副回線	ベストエフォート	1Gbps				
和歌山行政評価事務所	主回線	一部帯域確保	100Mbps（10Mbps確保）				
	副回線	ベストエフォート	1Gbps				
中国四国管区行政評価局	主回線	帯域確保	100Mbps				
	副回線	ベストエフォート	1Gbps				
鳥取行政評価事務所	主回線	一部帯域確保	100Mbps（10Mbps確保）				
	副回線	ベストエフォート	1Gbps				

別紙1－3　要件定義書 (回線)

本資料は総務省が想定する最低帯域を記載している。想定最低帯域以上でより最適な帯域があれば提案すること。

内容					提案内容	補足資料	記載箇所
島根行政評価事務所	主回線	一部帯域確保	100Mbps (10Mbps確保)				
	副回線	ベストエフォート	1Gbps				
岡山行政評価事務所	主回線	一部帯域確保	100Mbps (10Mbps確保)				
	副回線	ベストエフォート	1Gbps				
山口行政評価事務所	主回線	一部帯域確保	100Mbps (10Mbps確保)				
	副回線	ベストエフォート	1Gbps				
四国行政評価支局	主回線	帯域確保	100Mbps				
	副回線	ベストエフォート	1Gbps				
徳島行政評価事務所	主回線	一部帯域確保	100Mbps (10Mbps確保)				
	副回線	ベストエフォート	1Gbps				
愛媛行政評価事務所	主回線	一部帯域確保	100Mbps (10Mbps確保)				
	副回線	ベストエフォート	1Gbps				
高知行政評価事務所	主回線	一部帯域確保	100Mbps (10Mbps確保)				
	副回線	ベストエフォート	1Gbps				
九州管区行政評価局	主回線	帯域確保	100Mbps				
	副回線	ベストエフォート	1Gbps				
佐賀行政評価事務所	主回線	一部帯域確保	100Mbps (10Mbps確保)				
	副回線	ベストエフォート	1Gbps				
長崎行政評価事務所	主回線	一部帯域確保	100Mbps (10Mbps確保)				
	副回線	ベストエフォート	1Gbps				
熊本行政評価事務所	主回線	一部帯域確保	100Mbps (10Mbps確保)				
	副回線	ベストエフォート	1Gbps				
大分行政評価事務所	主回線	一部帯域確保	100Mbps (10Mbps確保)				
	副回線	ベストエフォート	1Gbps				
宮崎行政評価事務所	主回線	一部帯域確保	100Mbps (10Mbps確保)				
	副回線	ベストエフォート	1Gbps				
鹿児島行政評価事務所	主回線	一部帯域確保	100Mbps (10Mbps確保)				
	副回線	ベストエフォート	1Gbps				
沖縄行政評価事務所	主回線	一部帯域確保	100Mbps (10Mbps確保)				
	副回線	ベストエフォート	1Gbps				
北海道総合通信局	主回線	帯域確保	100Mbps				
	副回線	ベストエフォート	1Gbps				
東北総合通信局	主回線	帯域確保	100Mbps				
	副回線	ベストエフォート	1Gbps				
関東総合通信局	主回線	帯域確保	100Mbps				
	副回線	ベストエフォート	1Gbps				
関東総合通信局 (三浦電波監視センター)	主回線	一部帯域確保	100Mbps (10Mbps確保)				
	副回線	ベストエフォート	1Gbps				
信越総合通信局	主回線	帯域確保	100Mbps				
	副回線	ベストエフォート	1Gbps				
北陸総合通信局	主回線	帯域確保	100Mbps				
	副回線	ベストエフォート	1Gbps				
東海総合通信局	主回線	帯域確保	100Mbps				
	副回線	ベストエフォート	1Gbps				
近畿総合通信局	主回線	帯域確保	100Mbps				
	副回線	ベストエフォート	1Gbps				
中国総合通信局	主回線	帯域確保	100Mbps				
	副回線	ベストエフォート	1Gbps				
四国総合通信局	主回線	帯域確保	100Mbps				
	副回線	ベストエフォート	1Gbps				
九州総合通信局	主回線	帯域確保	100Mbps				
	副回線	ベストエフォート	1Gbps				

別紙1－3　要件定義書（回線）

本資料は総務省が想定する最低帯域を記載している。想定最低帯域以上でより最適な帯域があれば提案すること。

内容					提案内容	補足資料	記載箇所
沖縄総合通信事務所	主回線	帯域確保	100Mbps				
	副回線	ベストエフォート	1Gbps				
ディザスタリカバリサイト（移行時）	主回線	ベストエフォート	100Mbps				
	副回線	ベストエフォート	100Mbps				
ディザスタリカバリサイト	主回線	帯域確保	200Mbps				
	副回線	帯域確保	300Mbps				
外部監視室（移行時）	主回線	帯域確保	1Gbps				
	副回線	帯域確保	100Mbps				
監視用回線他							
監視用回線（本省）	主回線	帯域確保	100Mbps				
監視用回線（外部監視室）	主回線	帯域確保	100Mbps				

別紙１－４ 要件定義書（運用及び維持保守・管理）

項番号	内容	提案内容	補足資料	記載箇所
第1　全体概要				
	① 総務省LANサービスを円滑に運用するため、各種運用設計を行い、運用手順書に基づいて運用を行うこと。			
	② 運用範囲は、「別紙1-2　要件定義書（サービス・機器）」に基づき提供されるサービス全般とする。			
	③ LAN 端末、タブレット型端末、シンクライアントの運用は、運用範囲に含まれる。			
	④ 既存流用した機器、配線、19 インチラック、電源設備等の保守は、本調達の範囲に含まない。 ただし、流用した機器、配線及び設備等は、状態や利用状況を図面におこして把握し管理すること。			
	⑤ 本仕様書に示す以外で、運用・保守業務を円滑に行うために必要となる作業があれば請負者が行うこと。			
1　運用設計要件				
	① 請負者は、「運用・保守要領」を策定し、主管課の承認を得ること。			
	② 請負者は、「運用・保守要領」に基づき「運用・保守設計書」を作成し、主管課の承認を得ること。			
	③ 請負者は、「運用・保守設計書」に基づき「運用・保守手順書」を作成し、主管課の承認を得ること。			
	④ 連絡体制及び連絡手順を明確にし、主管課及びLAN 管理室等の関係者への連絡を円滑かつ迅速に行える仕組みを構築すること。			
	⑤ サポートを行う窓口を一元化し、ユーザの利便性向上を図ること。			
	⑥ 標準化されたルール及び手順に基づき、均一なサポートを提供すること。			
	⑦ ITILv3 に準拠した運用設計を行うこと。			
	⑧ 主管課の業務負荷の軽減に配慮した運用設計を行うこと。			
	⑨ 請負者は、サービスレベル目標値と測定対象・測定方法を提案し、その詳細を落札後に主管課と調整し、承認を得ること。			
	⑩ 請負者は、運用要員の行う詳細な業務プロセス、役割分担等を提案すること。			
2　全体要件				
	① システム運用に必要な消耗品は、請負者の負担において準備すること。			
	② 24 時間365 日の運用を基本とすること。また、保守による停止が必要な際は、ユーザの利便性を損なわないよう配慮し作業を行うこと。			
	③ 日本語による円滑なコミュニケーションができること。			
	④ 情報を一元的に管理するための仕組みを活用し、サポートのノウハウ蓄積、品質の向上、及び効率化を図ること。			

別紙１－４ 要件定義書（運用及び維持保守・管理）

項番号	内容	提案内容	補足資料	記載箇所
(1) 運用・保守要領				
①	「政府情報システムの整備及び管理に関する標準ガイドライン」（平成26年12月3日各府省情報化統括責任者(CIO)連絡会議決定)に基づき、継続的・安定的なサービスをユーザに提供するため、以下の内容を含めた「運用・保守要領」を策定すること。 ・コミュニケーション管理 ・体制管理 ・作業管理 ・進捗管理 ・リスク管理 ・課題・問題管理 ・システム構成管理 ・変更管理 ・情報セキュリティ管理 ・文書管理 ・システム操作管理 ・サービスレベル管理 ・性能管理 ・データ管理 ・設備管理 ・障害対策管理 ・運用・保守要領の改訂手順 等			
(2) 定期報告				
①	主管課に対して、総務省ＬＡＮの運用・保守業務の報告を定期的に行うこと。			
②	運用業務報告として、総務省ＬＡＮの運用・保守全般における作業内容及び管理状況を報告すること。			
③	運用業務報告として、障害及びセキュリティインシデントに関する対応状況、対応結果を報告すること。			
④	総務省LAN情報セキュリティチームと連携し、各セキュリティサービスにおけるセキュリティログの集計・分析・評価の結果を報告すること。			
⑤	報告の機会は、定期報告（日次、週次、月次、年次）、緊急、随時とすること。			

別紙1－4 要件定義書（運用及び維持保守・管理）

項番号	内容	提案内容	補足資料	記載箇所
ア 日次報告				
①	以下の内容を報告すること。 ・ヘルプデスクへの問い合わせ状況 ・ヘルプデスク業務の実施状況 ・障害の対応状況 ・運用業務の実施状況			
②	その他、必要に応じて項目を追加すること。			
イ 週次報告				
①	以下の内容を報告すること。 ・システム稼動実績 ・ヘルプデスク問い合わせ実績 ・申請対応業務実績 ・障害対応実績 ・セキュリティ管理実績 ・資源・性能管理実績 ・構成管理実績 ・ユーザ支援業務実績 ・システム変更作業実績 ・課題管理進捗状況報告 ・その他作業実績			
②	その他、必要に応じて項目を追加すること。			
ウ 月次報告				
①	下記の内容を報告すること。 ・サービス稼動実績 ・システム稼動実績 ・SLA 管理 ・ヘルプデスク問い合わせ実績 ・申請受付実績 ・障害対応実績 ・セキュリティ管理実績 ・資源・性能管理実績 ・構成管理実績 ・ユーザ支援業務実績 ・システム変更作業実績 ・その他作業実績			
エ 年次報告				
①	1年間の運用業務を整理した総合的な報告書を提出すること。			

別紙１－４ 要件定義書（運用及び維持保守・管理）

項番号	内容	提案内容	補足資料	記載箇所
(3) 運用体制				
ア 体制				
(ア) 運用責任者				
①	運用業務全体を管理すること。(1名以上)			
②	原則として、運用業務時間内は LAN 管理室に常駐し、業務を行うこと。			
③	要員のシフト管理、出退勤管理等を行い、万全の体制で業務を遂行できる状態とすること。			
④	運用管理業務の実施内容は各報告書にまとめ、定期的に主管課に報告すること。			
(イ) サービスレベルマネージャ				
①	運用責任者とは別に、サービスレベルマネージャを配置すること。(1名以上)			
②	サービスレベルマネージャは、運用業務の品質を維持するために業務に対する監査を定期的に行うこと。			
(ウ) サービス保守要員				
①	サービス保守業務を担当する。(リーダ1 名、メンバ6 名以上)			
②	うち 2 名は、総務省LAN を運用する上で必要となる全てのサービス領域に関して技術的な助言を行えること。			
③	うち 2 名は、総務省LAN のファシリティに関して助言を行えること。			
④	運用業務時間内は、LAN 管理室に常駐し業務を行うこと。			
(エ) ヘルプデスク要員				
①	ヘルプデスク業務を担当する。(リーダ1 名、メンバ7 名以上)			
②	運用業務時間内は、LAN 管理室に常駐し業務を行うこと。			
イ 資格等				
①	運用に係る要員は、運用業務遂行に当たり十分な技能と経験、資格を有すること。			
ウ 教育				
①	請負者は、年1回、運用要員に対してセキュリティ教育を行うこと。			
②	運用要員の交代、補充を行う場合は、次期総務省LAN及び本業務に関する教育を受けること。			
(4) 業務時間				
(ア) サービス保守要員				
①	サービス保守業務は、以下の時間で行うこと。 ・開庁日 8:00 ～ 20:00 ・閉庁日 9:00 ～ 17:00			
(イ) ヘルプデスク要員				
①	ヘルプデスク業務は、以下の時間で行うこと。 ・開庁日 8:30 ～ 20:00 ・閉庁日 9:00 ～ 17:00			
(ウ) その他				
①	重大インシデント発生時は、主管課と協議の上、対応すること。			
②	平常時間外に対応する窓口を準備すること。			
③	大規模な人事異動の際は、深夜・休日においても対応すること。			

別紙１－４ 要件定義書（運用及び維持保守・管理）

項番号	内容	提案内容	補足資料	記載箇所
第2　サービスストラテジ				
1　事業関係管理				
(1) 概要				
	主管課及びユーザと良好な関係を築き、顧客満足度の高いサービスを提供すること。			
(2) ユーザ利用満足度調査				
	①　運用開始後、毎年ユーザに対する満足度調査をアンケート方式で実施すること。また、基準スコア（75 点）に満たない場合は、必要な改善を行うこと。 ・問い合わせから回答までに要した時間 ・回答又は手順に対する説明の分かりやすさ ・回答又は手順に対する結果の正確性 ・担当者の対応（言葉遣い、親切さ、丁寧さ等）			
	② 調査項目の詳細及び配点方法については、主管課と協議の上、決定すること。			
第3　サービスデザイン				
1　デザイン・コーディネーション				
(1) 概要				
	総務省LANに対して、一貫した設計のもとサービスの変更及び追加が行われるようにする。			
2　サービスカタログ管理				
(1) 概要				
	ユーザに対して、総務省LANサービスに関する最新の情報を公開する。			
(2) 運用要件				
	① ユーザ向けのサービス情報をまとめた文書を作成すること。			
	② サービスの利用手順を含め、ポータルサイトに掲載すること。			

別紙１－４ 要件定義書（運用及び維持保守・管理）

項番号	内容	提案内容	補足資料	記載箇所
3	サービスレベル管理			
(1)	概要			
	達成可能なSLA（Service Level Agreement：サービスレベル合意書）について主管課と調整し、合意する。 合意したSLAが満たされるような体制を整え、運用計画を準備する。 主管課に対し、月次単位でSLAの達成状況の報告を行い、未達の場合は改善に向けた活動を実施する。			
(2)	サービスレベルの評価			
	① サービスレベルは、運用開始後から測定すること。ただし、移行開始後1 か月間の評価は、主管課と調整すること。			
	② 総務省ＬＡＮのサービス、回線、運用業務、セキュリティ管理に関してサービスレベル目標値を定め、SLAとして文書化し、主管課と合意すること。			
	③ SLAで定めた項目及び目標値に対する実績、達成状況を月次単位で主管課に報告し、分析・評価・改善を行うこと。			
	④ 未達のサービスレベル項目に対して原因究明を行い、対策を検討・報告すること。			
	⑤ サービスレベル目標（稼働率、復旧時間等）については、「別添2 現行総務省LANにおけるサービスレベル一覧」を参照すること。			
	⑥ SLA未達の場合、総務省は月額役務費用に5%を乗じて得た額（1円未満切捨）を1か月ごとに請負者に支払う役務費用から減額して支払うものとする。ただし、請負者の責めに帰すべき理由によりSLAが未達であった場合に限る。なお、サービス提供時間及び正常稼働時間の実績値は、仕様書に基づき請負者が作成し総務省に提出した各種報告書の記載内容を踏まえて総務省が判断するものとする。			
	⑦ 天変地異等、通常の予測を超えた事態が発生した場合は、SLA の範囲外とする。			
ア	SLA等評定会議の実施			
	① SLAに関する達成状況及びITIL®に則した評価を月次単位で報告すること。			
(3)	運用計画			
ア	年次計画			
	① 作業の年次計画を次年度開始の1 か月前までに策定し、主管課の承認を得ること。年次計画には、以下の内容を含むこと。 ・法定停電（中央合同庁舎第２号館） ・防災訓練 ・LAN 端末の更新 ・業務システムの導入 ・各種修正プログラムの適用 ・各種修正プログラム群の適用 ・ソフトウェアアップデートの適用 等			
イ	月次計画			
	① 年次計画に基づき月次計画を作成し、主管課の承認を得ること。なお、月次計画には、以下の内容を含めること。 ・稼動計画（目的、作業内容、時間帯及び影響等を含めた計画停止の内容を含む） ・要員計画			
ウ	計画の変更			
	① 年次計画、月次計画に変更が生じた場合は、速やかに主管課に報告・調整し、承認を得ること。			

別紙１－４ 要件定義書（運用及び維持保守・管理）

項番号	内容	提案内容	補足資料	記載箇所
4　キャパシティ管理				
(1) 概要				
	性能劣化や資源枯渇等の問題を未然に防ぐため、提供する各種サービスのキャパシティを管理し、調整すること。			
(2) 運用要件				
ア　サービスキャパシティ管理（SCM）				
①	ユーザの利用に関する特徴、傾向及びシステムの特徴等を勘案し、性能監視を実施すること。			
②	提供する各種サービスの性能レベルを保持するため、性能情報を定期的に収集し、分析結果を報告すること。			
③	サービスの性能低下や障害を未然に防ぐため、性能の傾向を収集・分析し、改善が必要な場合は改善案を主管課に提案し、協議の上、必要な対応を行うこと。			
④	性能低下が発生した場合は、原因について分析を行い、対応を行うこと。			
イ　リソースキャパシティ管理（RCM）				
①	ファイル共有サービスは、個々のユーザ・組織単位で使用量を把握すること。			
②	ファイル共有サービス（個人用）は、状況に応じてユーザへ使用容量削減依頼を行うこと。			
③	ファイル共有サービス（組織用）は、状況に応じて主管課と協議の上、ディスク領域の変更等の必要な対応を行うこと。			
④	提供する各種サービスの資源の枯渇を防止するため、資源情報を定期的に収集・分析し、改善が必要な場合は改善案を主管課に提案し、協議の上、必要な対応を行うこと。			
5　ITサービス継続性管理				
(1) 概要				
	深刻な影響を与える可能性があるリスクを管理する。 リスクを許容可能なレベルにまで低減し、復旧に対する計画を立案することによって、事前に取り決めた合意済みのサービスレベルを、常に確実に満たせるようにする。			
(2) ディザスタリカバリ管理				
①	現行総務省LANでは「総務省LANにおける情報システム運用継続計画」を策定している。請負者は、次期総務省LANに適合する形で本運用継続計画を見直し、再作成すること。また、本運用継続計画は、年に一回以上見直し等を行い、主管課の承認を得ること。			
②	ディザスタリカバリサイトへのサービス切替えに関する計画の見直しや修正を行う場合は、切替試験を実施すること。			
③	本省へのサービスの切戻しに関する計画の見直しや修正を行う場合は、切戻試験を実施すること。			
④	緊急事態が発生した場合の緊急連絡手段や備蓄等、態勢を準備すること。			
⑤	1年に1回以上、ディザスタリカバリサイトを利用した防災訓練を実施すること。防災訓練を実施するに当たり、訓練目的やディザスタリカバリサイトへの切り替え試験を踏まえた計画書及び手順書を作成し、主管課の承認を得ること。防災訓練の実施後は報告書により主管課に報告し、訓練時に発見した改善点や見直し項目の確認を行い、改善策を実施すること。			
(3) バックアップ				
①	設計内容に基づいたバックアップが行われていることを確認すること。			
②	システムに変更を行う場合は、原則として作業前にバックアップを取得すること。			

別紙１－４ 要件定義書（運用及び維持保守・管理）

項番号	内容	提案内容	補足資料	記載箇所
6 可用性管理				
(1) 概要				
	総務省LANが提供する各サービスの停止を未然に防ぐため、可用性を管理する。			
(2) 運用要件				
	① サービスレベル管理プロセスで定義したサービスレベル目標値が達成されるよう、冗長構成を維持管理すること。			
ア 可用性管理				
(ア) サーバ・アプライアンス				
稼動監視				
	① 運用管理サービス等を活用し、稼働監視、サービス監視、プロセス監視、障害監視等を24時間365日対応で実施すること。異常が検知された場合には、適宜対応すること。			
停電対応				
	① 計画停電時には、事前に電源管理サービス等を活用し、安全にシステムを停止させること。			
(イ) LAN端末				
	① LAN 端末の故障時は、予備機を払い出し、業務への影響を最小限にすること。			
(ウ) 共通				
修正プログラム管理				
	① 既知の障害を回避するため、各サーバ・アプライアンス・LAN 端末等に対する修正プログラム等を適用すること。			
7 情報セキュリティ管理				
(1) 概要				
	総務省LANで取り扱う情報の機密性、完全性、可用性を担保すること。			
(2) 運用要件				
ア セキュリティ管理要件				
	① 総務省情報セキュリティポリシーをもとに、総務省LANサービスの情報セキュリティ管理を行うこと。			
	② 情報セキュリティ管理の要件は、主管課と十分に検討し合意すること。			
	③ 総務省LAN情報セキュリティチームと連携し、対応を行うこと。			
イ セキュリティチェック				
	① セキュリティサービスにおけるウイルス対策定義ファイル、シグネチャ・パターンファイルが最新であるか日次で確認すること。			
	② セキュリティインシデントの発生を確認すること。			
	③ セキュリティパッチが公開された際には、サービス提供機器、LAN端末に適用すること。			
	④ 年1回、サービス提供機器、LAN端末に対してセキュリティポリシーの遵守状況を確認するための情報を収集すること。また、主管課と協議の上、是正措置を行うこと。			

別紙１－４ 要件定義書（運用及び維持保守・管理）

項番号	内容	提案内容	補足資料	記載箇所
ウ	セキュリティインシデント対応			
①	マルウェア感染が疑われるLAN端末については回収し、予備機を払い出すこと。また、回収した端末は初期化を行うこと。			
②	セキュリティインシデント又は各種ログ分析・診断作業において、主管課がサービスへの影響を考慮し対応が必要と判断した場合、対象機器についてフィルタリング又はアクセス制御ルールの追加・変更を行うこと。			
③	セキュリティインシデントの内容の緊急度及び業務への影響度に応じて優先度を割り当てること。			
④	不審メール通報機能によりユーザから申告のあった不審メールに対して、調査を行うこと。			
⑤	各機器のID及びパスワードは、サービス運用に影響がでないよう厳格に管理すること。			
⑥	ウイルス対策定義ファイル、シグネチャ・パターンファイルの自動更新において、エラー又は異常終了が発生した場合には、手動更新を行うこと。			
エ	セキュリティ管理			
①	無許可ソフトウェアのインストール状況の調査を実施すること。			
オ	証明書			
①	証明書の期限切れによるセキュリティ低下を招かないように、証明書の管理を行うこと。			
カ	入退室管理			
①	本省サーバ室・LAN 管理室への入退室管理（受付、退室確認）を実施すること。			
②	LAN管理室から退室する際に、データの持ち出し有無について確認すること。			
キ	外付けUSBデバイス			
①	外付けDVDドライブを利用できるように設定したソフトウェアインストールアカウントを発行すること。			
②	LAN端末更改時及び大規模人事異動時（年2回程度）に外付けDVDドライブが利用できるようにすること。ただし、セキュリティには万全を期すこと。			
8	サプライヤ管理			
(1)	概要			
	サプライヤが契約上の義務を果たすよう管理する。			
(2)	運用要件			
①	サービス提供機器の保守契約の管理を行うこと。			
②	問合せ先や対応時間については、一元的に管理を行い、迅速に連絡がとれるようにしておくこと。			

別紙１－４ 要件定義書（運用及び維持保守・管理）

項番号	内容	提案内容	補足資料	記載箇所
第4　サービストランジション				
1　移行の計画立案及びサポート				
（1）概要				
	運用中に追加される新規サービスの導入を支援し、必要となるリソースを調整する。			
2　変更管理				
（1）概要				
	変更のライフサイクルをコントロールし、正確な変更業務を実施する。			
（2）運用要件				
	① 原則として、総務省ＬＡＮのすべての変更に標準化した手続きを適用し、総務省ＬＡＮの変更を正確に実施すること。			
	② インシデント管理プロセス、問題管理プロセス、セキュリティ管理プロセスから提出された変更要求の内容（変更提案者、変更対象となるサービス、変更概要、変更理由、変更しない場合の影響）を変更管理台帳で管理すること。			
	③ 運用要員が実施した変更作業については、設計・構築ドキュメント類や各種運用ドキュメント等に反映し、これを最新の状態に保つこと。			
	④ プログラムの修正が必要となる場合は、テスト実施の後にリリース(環境の変更を含む)の可否を判定すること。			
	⑤ 本番環境への変更実施が決定された場合は、リリース管理にリリース要求を発行し、リリースを実施すること。			
	⑥ リリース終了後、変更内容の判定及び結果の分析を行い、変更完了を変更管理台帳に記載すること。			
	⑦ リリース終了後、一定期間経過後に変更作業の評価を行い、レビューを実施すること。また、レビュー結果は、主管課に報告すること。			
	⑧ 業務システムを総務省 LAN に接続する際、主管課の調整業務の支援を行い、業務システム開発事業者と必要な調整を行うこと。			
	⑨ 業務システムを政府共通ＰＦに移行する際、主管課の調整業務の支援を行い、政府共通PF関係者及び、業務システム開発事業者と必要な調整を行うこと。			

別紙１－４ 要件定義書（運用及び維持保守・管理）

項番号	内容	提案内容	補足資料	記載箇所
3 リリース管理及び展開管理				
(1) 概要				
	変更管理により本番環境への変更が決定された作業について、手順の策定を経て変更を実施する。 リリースの構築、テスト、展開を計画立案、スケジューリング、コントロールする。 また、既存サービスの完全性を保護しながら、総務省LANが要求する新しい機能性を提供する。			
(2) 運用要件				
	① 変更管理プロセスで認可を受けた変更内容に対して、技術面及び非技術面の両方から保証をすること。			
	② 変更管理プロセスで認可を受けた変更内容に対して、検証環境で動作をテストすること。また、テストでは、有用性（変更要求通りの機能が提供できるか）、保証（可用性、キャパシティは保証できるか）、リリース手順（変更手順の明確化、切り戻しは機能するか）等を検証すること。			
	③ 業務への支障を最小化する方式で、リソースなどの投入計画を立案し、主管課と調整を行うこと。			
	④ リリースに伴う情報を総務省ＬＡＮポータルサイトサービスに掲載し、ユーザに周知を行うこと。			
	⑤ 投入計画に従い、変更を実施すること。			
ア リリース管理				
	① リリース要求に従い、リリース計画を策定し、主管課の承認を受けること。			
	② リリース計画の策定に当たっては、サービス及び業務システムへの影響やシステム稼働の安定性の担保に十分留意すること。			
	③ リリース作業に際して、手順書やチェックリストを作成し、必要に応じて検証環境でリハーサルを実施すること。			
	④ リリース作業の手順に問題がないことを確認の上、リリース計画に従ってリリース資源の配布や環境変更を実施すること。			
	⑤ リリース作業実施の際は、ユーザを含む関係者への周知連絡を徹底するとともに、各運用担当者が密に連携し、作業計画の遵守に努めること。			
	⑥ リリース作業の履歴管理を行うこと。			
	⑦ リリース終了後、リリース結果を確認し、主管課の承認を受けること。			
	⑧ 主管課の承認をもってリリース作業完了とし、変更管理に通知すること。			

別紙１－４ 要件定義書（運用及び維持保守・管理）

項番号	内容	提案内容	補足資料	記載箇所
4	サービス資産管理及び構成管理			
(1)	概要			
	サービスを提供するために必要な資産が適切にコントロールされるようにする。 また、資産に関する情報を正確に管理する。			
(2)	運用要件			
①	総務省ＬＡＮを構成する要素（サービス提供機器及びＬＡＮ端末のハードウェア、ソフトウェア、ライセンス情報、ユーザのアカウント情報等）を明確にし、構成管理台帳により管理すること。			
②	変更管理プロセス、リリース管理及び展開管理プロセスと連携し、構成要素を最新に保つこと。			
③	構成管理台帳の整合性を定期的に確認すること。			
ア	要員管理			
①	要員稼働計画を立案し、運用・保守業務を遂行する上で必要な要員をシフト管理表で管理すること。			
イ	機器管理			
(ア)	LAN 端末管理（本省）			
①	運用要員は、ユーザの申請に基づき必要な設定を行い、ユーザに引き渡すこと。			
(イ)	LAN 端末管理（本省以外）			
①	運用要員は、ユーザの申請に基づき必要な設定を行い、各拠点に送付すること。			
(ウ)	LAN端末			
①	運用要員は、以下に示す資産管理、構成管理を行うこと。 ・LAN 端末の配備先及びユーザとの対応管理 ・予備機の管理 ・人事異動等に伴う新規及び臨時の配備 ・マスタのキッティング手順の確立と LAN 端末納入事業者への引き継ぎ ・一定期間使用されていない LAN 端末の管理（原則主管課と調整の上、回収） ・全 LAN 端末のハードウェア及びソフトウェアの構成管理（ソフトウェアライセンスの保有数及び使用状況の把握等） ・LAN 端末の環境（OS のパッチレベル、使用ソフトウェアのバージョン等）の統一			
(エ)	タブレット型端末			
①	運用要員は、ユーザの申請に基づき必要な設定を行い、ユーザに引き渡すこと。			
②	運用要員は、返却予定日までにユーザからのタブレット型端末返却を受け、欠品がないことを確認して保管すること。			
③	運用要員は、保管している端末に対して、次の貸出しまでにモバイルデバイス管理サービスを用いて端末の初期化等を行うこと。			
④	運用要員は、以下に示す資産管理、構成管理を行うこと。 ・タブレット型端末の管理 ・適宜オペレーティングシステムやアプリケーションの更新、構成プロファイルの見直し			
(オ)	シンクライアント			
①	運用要員は、ユーザの申請に基づき、必要な設定を行いユーザに引き渡すこと。			
②	運用要員は、返却予定日までにユーザからのシンクライアントの返却を受け、欠品がないことを確認して保管すること。			
③	運用要員は、下記資産管理、構成管理を行うこと。 ・シンクライアントの管理 ・適宜オペレーティングシステムやアプリケーションの更新、構成プロファイルの見直し			

別紙１－４ 要件定義書（運用及び維持保守・管理）

項番号	内容	提案内容	補足資料	記載箇所
5 ナレッジ管理				
(1) 概要				
	知識及び有益な情報を共有し、それらを適切に公開する。			
(2) 運用要件				
	① 情報セキュリティ管理プロセスにおける調査と診断から導いた暫定策をナレッジ管理台帳に登録し、運用要員が参照できるようにすること。			
	② インシデント管理プロセスにおける調査と診断から導いた暫定策をナレッジ管理台帳に登録し、運用要員が参照できるようにすること。			
	③ 問題管理プロセスにおける調査と診断から導いた恒久策をナレッジ管理台帳に登録し、運用要員が参照できるようにすること。			
	④ 総務省ＬＡＮのサービスに関する利用マニュアル、Ｑ＆Ａ等のユーザ向けドキュメントをポータルサイトに掲示し、ユーザが参照できるようにすること。			
	⑤ 主管課からの指示に基づき、ポータルサイトのコンテンツの情報更新を行うこと。			
	⑥ ポータルサイトの作成、変更、修正、更新等の維持管理を行うこと。			
	⑦ ポータルサイトの作成は、ユーザにとって分かりやすく、利便性の高い内容であること。			
	⑧ 総務省 LAN のシステム情報やFAQ を掲載し、必要に応じて適宜更新を行うこと。			

別紙１－４ 要件定義書（運用及び維持保守・管理）

項番号	内容	提案内容	補足資料	記載箇所
第5 サービスオペレーション				
1 イベント管理				
(1) 概要				
	総務省LANで発生するイベントをモニタリングし、障害などの例外状況を検出した場合にはエスカレーションを行う。			
(2) 運用要件				
	① 総務省ＬＡＮの各サービスのイベントをシステム監視サービスを用いて検知、確認すること。			
	② 本省サーバ室及びディザスタリカバリサイトに設置した管理対象機器を日次で目視確認し、イベントを検知、確認すること。			
	③ 運用要員が受け付けるユーザからの問い合わせを通じて、イベントを検知、確認すること。			
	④ 主管課・関係者からのイベントの発見連絡、調査依頼等を通じて、イベントを検知、確認すること。			
	⑤ 運用要員が受け付ける主管課からの申請対応業務サービスに関する作業依頼をイベントとして検知、確認すること。			
	⑥ 検知したイベントを障害インシデント、セキュリティインシデント、問合せインシデント、申請インシデントに分類し、インシデント管理プロセス、情報セキュリティ管理プロセス、要求実現プロセス、アクセス管理プロセスにエスカレーションすること。			
ア 稼動監視				
	① 総務省LAN の稼動品質を担保するため、サービス及び機器等の稼動状況を24 時間365 日監視し、各種のインシデントに確実に対応すること。 なお、本省以外の場所で監視業務を行う場合、迅速な連携を行えること。			
	② ハードウェア障害等の機器交換が必要な作業については、本省は主管課と、第2庁舎、外部拠点、地方拠点はLAN運営担当者と連携し対処を行うこと。			
	③ 本省においての交換作業時間は、主管課と調整すること。			
	④ 第2庁舎、外部拠点、地方拠点においての交換作業時間は、原則平日9時～17時内とすること。			
2 インシデント管理				
(1) 概要				
	サービスに対する計画外の中断や品質の低下をインシデントとして管理する。 インシデント発生時は、ユーザに対する運用を可能な限り迅速に回復させることに焦点をあてる。			
(2) 運用要件				
	① イベント管理プロセスからエスカレーションされた障害インシデントの内容（発見者、発見日時、関連するサービス、障害状況等）をインシデント管理台帳で管理すること。			
	② インシデントの内容の緊急度及び業務への影響度に応じて優先度を割り当てること。			
	③ ユーザからの問い合わせは、インシデント管理台帳に登録すること。			

別紙１－４ 要件定義書（運用及び維持保守・管理）

項番号	内容	提案内容	補足資料	記載箇所
(3) 障害対応				
(ア) LAN端末・タブレット型端末・シンクライアント				
①	短時間での復旧ができない場合、予備機と交換すること。			
②	中央合同庁舎第2号館以外の拠点では、当該部局担当者が予備機を払い出す際の支援をすること。障害が発生した端末は回収し、対応完了後、再セットアップを行い、当該部局へ送付すること。			
③	ハードウェア障害等の場合は、機器の保守窓口に修理を依頼すること。			
④	部品交換などで、ハードディスク等の外部記憶媒体を総務省外へ搬出する際には、データの流出がないように処置を講じること。処置については、総務省情報セキュリティポリシーに則り、主管課の承認を得ること。			
⑤	障害の原因究明及び対応の妥当性を検証すること。また、障害が再発しないことを確認すること。			
(イ) サービス提供機器				
①	障害等が発生した場合は、主管課と協議し迅速に対応すること。			
②	請負者は一次切り分けを行い主管課へ第一報を行うとともに、主管課と連携し、原因の切分け及び復旧等の作業を実施すること。			
③	障害復旧後は速やかに主管課へ報告書を提出すること。			
④	政府共通ネットワーク並びに業務システムと総務省LANの間に跨って発生した障害は、関係者と共同で原因箇所の切分け及び復旧等を図ること。			
(ウ) システム保守対応時間				
①	本省、本省サーバ室、外部監視室並びにディザスタリカバリサイトは、原則24 時間365日オンサイト保守が実施可能であること。			
②	それ以外の拠点は、原則平日9 時～17 時のオンサイト保守を実施すること。			
3 要求実現				
(1) 概要				
	予期しないサービスの遅延や中断に起因するインシデントを除いた、顧客やユーザからの要求を処理する。			
(2) 運用要件				
①	要求実現の範囲については調達仕様書の範囲とし、依頼方法、対応手順については、主管課と協議すること。			

別紙１－４ 要件定義書（運用及び維持保守・管理）

項番号	内容	提案内容	補足資料	記載箇所
4	問題管理			
(1)	概要			
	イベント及びインシデントの根本原因を特定し、解決する。 将来発生する可能性があるインシデント及び問題を防止し、インシデントが発生した場合に迅速な診断と解決を可能にするため、既知のエラーの作成、ワークアラウンドの提供を行う。			
(2)	運用要件			
①	インシデント管理からエスカレーションされた事象を問題として登録し、影響度と緊急度により優先順位を決め、問題原因の特定を行うこと。			
②	早急に根本的解決ができない場合には、一時的な解決策を策定すると同時に、更に問題の原因調査、分析を実施し、恒久的な解決策の策定を行うこと。また、必要に応じて、主管課、関連事業者へエスカレーションを行うこと。			
③	管理された問題は、定期報告の内容として報告を実施すること。			
④	発生したインシデントに関して傾向を分析し、発生頻度の高いインシデントを優先的に対応すること。また、傾向分析の結果から更なるインシデントの発生を予測し、未然に防ぐための手立てを検討すること。			
5	アクセス管理			
(1)	概要			
	ユーザにサービスを使用できる権利を与えるとともに、データの機密性、可用性、完全性の確保を実現する。			
(2)	運用要件			
①	総務省ＬＡＮユーザ情報管理機能によるユーザアカウントのパスワード変更、ユーザ情報改廃の自動処理の結果、処理件数を日次で確認し、記録すること。			
ア	ユーザアカウント情報管理			
①	自動処理状況を確認し、実行結果を管理すること。			
②	大規模な人事異動の際は、深夜・休日においても対応すること。			
③	自動処理にミス等が発生した場合は、安全確実に修正を行うこと。			
イ	管理者アカウント管理			
①	特権管理アカウントの作成は、主管課の承認を受けること。			
②	特権管理アカウントでLAN端末へログオンができないようにすること。			
③	管理者アカウントは、一元的に管理すること。			

別紙１－４ 要件定義書（運用及び維持保守・管理）

項番号	内容	提案内容	補足資料	記載箇所
第6　継続的サービス改善				
（1）概要				
	PDCAサイクルに則り、運用改善活動を行う。			
（2）運用要件				
	① 運用管理業務をPDCAサイクルにより継続的に見直すこと。			
	② 改善に関する事項は随時提案し、主管課と協議の上、実施すること。			
	③ 改善活動は、内部プロセス、運用サービス内容等運用品質の向上につながる内容とすること。			
	④ 業務品質及びユーザ満足度を念頭に業務を遂行すること。また、積極的な業務改善の提案を実施し、安定稼動及びユーザサービスレベルの向上に努めること。			
第7　サービスデスク				
（1）概要				
	ユーザとの窓口を一元的に提供する。 インシデント、サービス要求、標準的な変更を管理し、ユーザとの連絡を処理する。			
（2）運用要件				
ア　問い合わせ対応				
	① 総務省LAN が提供するサービスに係るユーザからの問合せを電話又はメールで受け付けること。			
	② 必要に応じてLAN 端末の遠隔操作を活用して状況把握を行い、ユーザ業務の早期再開に向けて迅速に対応すること。			
	③ 必要に応じユーザの執務場所で問題解決の支援を行うこと。			
	④ ヘルプデスク要員は、サービス保守要員と綿密な連携をとり、ユーザの問い合わせに迅速に対応すること。			
イ　窓口業務				
	① LAN端末、タブレット型端末、シンクライアントの貸し出し、返却処理をサービス資産管理に従い実施すること。			
ウ　カード管理業務				
	① LAN複合機利用者カードの新規発行を行うこと。			
	② 50枚/月を目安とし、LAN複合機利用者カードの回収、発行、更新を行うこと。			
エ　盗難紛失対策				
	① LAN端末、タブレット型端末、シンクライアントの盗難紛失時受付及び対応は、24時間365日で行うこと。			
	② タブレット型端末及びシンクライアントの盗難、紛失が発生した場合は、総務省ＬＡＮサービスの利用ができないようにすること。			

別紙１－４ 要件定義書（運用及び維持保守・管理）

項番号	内容	提案内容	補足資料	記載箇所
第８　ソフトウェア保守要件				
（１）基本方針				
	① 保守対象ソフトウェアは、本調達で納入するすべてのソフトウェアとする。			
	② 日本語での対応ができること。			
	③ 保守は、万全な体制を確保すること。なお、連絡体制は、具体的な資料を提出すること。			
	④ 受注期間中の保守の実施は、追加費用が発生することなく、受注金額内で対応すること。			
	⑤ 通常の使用状態で障害があった場合、作業費用、出張費用等の追加費用が発生しないこと。			
	⑥ 平成33年４月から最大で１年間の契約延長が可能なこと。			
（２）体制と役割				
	① ソフトウェア保守の体制と役割を提案すること。			
（３）対応業務				
ア　ソフトウェア保守				
	① 次期総務省ＬＡＮの運用開始から撤去までの期間中、ファームウェア及びソフトウェアの不具合、セキュリティ上の不具合に対応する修正プログラムの適用を行うこと。			
イ　ソフトウェア障害対応				
	① ソフトウェアに障害があった場合、運用員による障害箇所の特定・原因調査・復旧作業の切り分けを実施し、復旧対応は必要な技術情報の提供等の支援を行うこと。			
	② 障害対応終了後、障害内容、原因及び対応内容等を主管課に作業報告を行うこと。			
	③ 保守期間は、本稼働から4年間とすること。			

別紙１－４ 要件定義書（運用及び維持保守・管理）

項番号	内容	提案内容	補足資料	記載箇所
第9　ハードウェア保守要件				
（1）基本方針				
	① 保守対象ハードウェアは、本調達で納入するすべてのハードウェアとする。			
	② 日本語での対応ができること。			
	③ 保守は、万全な体制を確保し、運用担当者に協力すること。なお、連絡体制は、具体的な資料を提出すること。			
	④ 本省及びディザスタリカバリサイトに導入する機器は、24時間365日の保守が行えること。			
	⑤ 本省及びディザスタリカバリサイト以外の拠点に導入する機器は、平日9時～17時の保守が行えること。			
	⑥ 現地対応体制は、障害発生時又は主管課の求めに応じて1時間以内を目標に対応を開始すること。			
	⑦ 受注期間中の保守の実施は、追加費用が発生することなく、受注金額内で対応すること。			
	⑧ 通常の使用状態で障害があった場合、作業費用、バッテリー等の消耗品の交換費用、出張費用等の追加費用が発生しないこと。			
	⑨ 1回/年以上のハードウェアの定期点検を実施し、その進捗及び実績の報告を行うこと。			
	⑩ 障害対応等でハードディスクを総務省外へ搬出する場合、総務省情報セキュリティポリシーによる適切な処置を講じること。			
	⑪ 平成33年4月から最大で1年間の契約延長が可能なこと。			
（2）体制と役割				
	① ハードウェア保守の体制と役割を提案すること。なお、保守体制として、全国各都道府県に保守拠点を有すること。			
（3）対応業務				
ア　ハードウェア保守				
	① 設置から撤去までの期間は、機器及びそれを構成する部品の調達が保証されること。			
	② 潜在的不具合がある場合は、機器に関する技術的な問題点の情報を無償で速やかに報告すること。また、主管課の指示に従い、機器への導入及び動作確認を行い、正常に動作することを保証すること。			
イ　ハードウェア障害対応				
	① 機器に障害があった場合は、障害箇所の特定・原因調査・復旧作業の切り分け、主管課との協議、復旧対応（部品の交換、修理等）等を速やかに行うこと。			
	② 障害対応終了後、障害内容、原因及び対応内容等を主管課に作業報告を行うこと。			
	③ 障害対応等によりハードディスクの交換が必要となった場合でも、故障したハードディスクにセキュリティ上の利用がある場合は、総務省外部へ持ち出さずに対応できる保守とすること。ハードディスクが取り出せない機器は、データ消去を行い、主管課の承認を得た上で障害対応を実施すること。			
	④ 保守期間は、本稼働から4年間とすること。			
ウ　機器の撤去				
	① 本調達の請負期間が完了後、機器の撤去を実施すること。機器撤去に際しては、主管課と日程等の調整を事前に実施しておくこと。また、データを保持している機器に関しては、主管課と協議の上、撤去前にデータ消去作業を実施し搬出すること。			

別紙2　総合評価基準及び対応表

1　必須項目

「調達仕様書」及び別紙1「要件定義書」（別紙1－1「要件定義書（システム全般）」から別紙1－4「要件定義書（運用及び維持保守・管理）」までを含む。以下同じ。）において「必須」と定められた要求要件であり、以下の表で「必須」欄に○がある事項に記載の要件を全て満たしたものを「合格」とする。

2　基礎点

「必須」項目の評価において「合格」となったものに「基礎点」として「100点」を与える。

3　加点項目

「合格」した提案書について、総合評価基準書に基づき、「加点」の評価を行う。「加点」の評価は、以下の観点を共通基準とした上で、各項目ごとに「評価ポイント」の観点から評価を行う。

・総務省ＬＡＮの経緯等を十分に把握し有益な提案となっているか。
・実現性が十分に担保されていると判断できるか。
・提案者の実績や知見に基づく創意工夫が盛り込まれているか。

No	評価項目（調達仕様書・要件定義書の項番に対応する）		必須	加点	加点配点	評価ポイント	提案内容	提案内容補足資料	記載箇所
1	調達仕様書	第１　調達案件の概要に関する事項	○	○		理解かつ適合していることを具体的に示すこと。 具体的に示された提案内容が要件を満たした上で、作業スケジュールは、次期総務省LANのサービスインに向けて現実的で実現性の高いものとなっていると客観的に判断される場合は加点する。また、総務省側のスケジュールを考慮し、効率的な提案であること。			
		第２　調達案件及び関連調達案件の調達単位、調達の方法等に関する事項	○	-		理解かつ適合していることを具体的に示すこと。			
		第３　作業の実施内容に関する事項	○	○		理解かつ適合していることを具体的に示すこと。 具体的に示された提案内容が要件を満たした上で、成果物は、文書体系が整理されたものであると客観的に判断される場合は加点する。また、運用時のマネジメントレビュー、修正・更新等を見越した構成、運用、品質管理方法が具体化されている提案であること。			
		第４　満たすべき要件に関する事項	-	-		-			
		１　調達仕様書記載の要件	○	-		理解かつ適合していることを具体的に示すこと。			
		２　要件定義書記載の要件	○	-		理解かつ適合していることを具体的に示すこと。			
		３　その他満たすべき要件	○	-	40	理解かつ適合していることを具体的に示すこと。			
		第５　作業の実施体制・方法に関する事項	○	○		理解かつ適合していることを具体的に示すこと。 具体的に示された提案内容が要件を満たした上で、作業実施体制は、大規模で複雑な総務省LANを再構築するのに十分な経験・知識・技能・実績・資格を持った作業要員が参画するものとし、適正な要員数にて編成していると客観的に判断される場合は加点する。 特にプロジェクトマネージャ・リーダがは、十分なコミュニケーション能力を持つだけでなく、適切な方法論、ツール等を用いて円滑・確実にプロジェクトを推進できると客観的に判断される場合は加点する。 なお、複数者、複数部門との連携がある場合、それぞれが十分な資格・実績を有し、本業務遂行に足る体制の提案であること。 作業の管理に当たってがは、体系的に整理されたプロジェクト管理手法を用いながらも、実践的で実現可能なプロジェクト管理を提案すると客観的に判断される場合は加点する。 なお、プロジェクト管理手法がは、教科書的な手法の羅列ではなく、実績や知見に基づいた現実的な手法を含む提案であること。			
-		第６　作業の実施に当たっての遵守事項	○	-	-	理解かつ適合していることを具体的に示すこと。	-	-	-
-		第７　成果物の取扱いに関する事項	○	-	-	理解かつ適合していることを具体的に示すこと。	-	-	-
-		第８　入札参加資格に関する事項	○	-	-	理解かつ適合していることを具体的に示すこと。	-	-	-
-		第９　再委託に関する事項	○	-	-	理解かつ適合していることを具体的に示すこと。	-	-	-
-		第１０　その他特記事項	○	-	-	理解かつ適合していることを具体的に示すこと。	-	-	-
-		第１１　附属文書	○	-	-	理解かつ適合していることを具体的に示すこと。	-	-	-

別紙2　総合評価基準及び対応表

No	評価項目（調達仕様書・要件定義書の項番に対応する）		必須	加点	加点配点	評価ポイント	提案内容	提案内容補足資料	記載箇所
-	別紙1－1要件定義書（システム全般）	第１　規模・性能	○	-	-	理解かつ適合していることを具体的に示すこと。	-	-	-
-		第２　信頼性等	○	-	-	理解かつ適合していることを具体的に示すこと。	-	-	-
2		第３　情報セキュリティ	○	○	100	理解かつ適合していることを具体的に示すこと。 具体的に示された提案内容が要件を満たした上で、総務省ＬＡＮ情報セキュリティチームは、調達対象の統合的な管理・運用を考慮した上で、日常的な情報セキュリティインシデントの確認が可能な体制の提案であると客観的に判断される場合は加点する。 また、情報セキュリティインシデント発生時に、総務省側と連携し、迅速かつ的確な対応の実現を考慮した提案であると客観的に判断される場合は加点する。			
3		第４　構築・試験	○	○	80	理解かつ適合していることを具体的に示すこと。 具体的に示された提案内容が要件を満たした上で、調達対象の構築を効率的に行える提案であると客観的に判断される場合は加点する。また、試験については、運用開始後の品質を十分に担保できる提案であると客観的に判断される場合は加点する。			
		第５　受入試験支援	○	○		理解かつ適合していることを具体的に示すこと。 具体的に示された提案内容が要件を満たした上で、受入試験の支援に当たっては、総務省側の負担を軽減しつつ、網羅的に機能、性能の確認が十分に行える質の高い支援が可能な提案であると客観的に判断される場合は加点する。			
		第６　情報システムの移行	○	○		理解かつ適合していることを具体的に示すこと。 具体的に示された提案内容が要件を満たした上で、総務省ＬＡＮの移行は、全国各地の拠点を対象とするため、経験に裏付けられた計画と実行力をもって、確実かつ迅速に行う必要がある。 移行に当たっては、具体的な方法論、手順、準備、実績等を踏まえた移行計画を含み、確実かつ迅速な移行が可能な提案であると客観的に判断される場合は加点する。 なお、無停止での移行を必要とする部署を考慮すること。			
		第７　引継ぎ	○	○		理解かつ適合していることを具体的に示すこと。 具体的に示された提案内容が要件を満たした上で、円滑で質の高い引き継ぎが行える提案であること。			
		第８　教育	○	○		理解かつ適合していることを具体的に示すこと。 具体的に示された提案内容が要件を満たした上で、円滑で質の高い教育が行える提案であると客観的に判断される場合は加点する。			
-		第９　施設・設備	○	-	-	理解かつ適合していることを具体的に示すこと。	-	-	-
-	別紙1－2要件定義書（サービス・機器）	第１　調達機器の共通事項	○	-	-	理解かつ適合していることを具体的に示すこと。	-	-	-
4		第２　共用サーバ・ストレージ	○	○	10	理解かつ適合していることを具体的に示すこと。 具体的に示された提案内容が要件を満たした上で、総務省ＬＡＮは、共用基盤として、各種サービスで利用するプラットフォームである。総務省ＬＡＮを構成する機器等は、十分な性能、信頼性が確保されているとともともに、総務省における運用に寄与する提案であると客観的に判断される場合は加点する。			
-		第３ 総務省LANサービス					-	-	-
5		1 メールサービス	○	○		理解かつ適合していることを具体的に示すこと。 具体的に示された提案内容が要件を満たした上で、メールサービスは、省内外への主要な通信手段であり、情報システムの中核である。 基本性能はもとより、利便性や信頼性、セキュリティが十分に確保された提案であると客観的に判断される場合は加点する。 特に、利便性については、総務省での組織形態や実運用に十分配慮した提案であると客観的に判断される場合は加点する。			
		2　ポータルサイトサービス	○	○		理解かつ適合していることを具体的に示すこと。 具体的に示された提案内容が要件を満たした上で、ポータルサイトサービスは、ユーザが業務を円滑に進めることができるよう、情報の提供や取得が分かりやすくかつ容易に行える提案であると客観的に判断される場合は加点する。 特に、利便性については、総務省での組織形態や実運用に十分配慮した提案であると客観的に判断される場合は加点する。 また、セキュリティに配慮した提案であること。			

No	評価項目（調達仕様書・要件定義書の項番に対応する）	必須	加点	加点配点	評価ポイント	提案内容	提案内容補足資料	記載箇所
	3　ファイル共有サービス	○	○	70	理解かつ適合していることを具体的に示すこと。 具体的に示された提案内容が要件を満たした上で、ファイル共有サービスは、省内の文書等成果物の保管場所であり、かつ作成場所として提供をする情報システムの中核である。 十分な性能・信頼性・容量・バックアップ環境が整っている提案であると客観的に判断される場合は加点する。 特に、共有可能なファイル容量については、大きな評価ポイントとなる。 また、利便性については、総務省での組織形態や実運用に十分配慮した提案であると客観的に判断される場合は加点する。さらに、セキュリティに配慮した提案であること。			
	4　大容量ファイル転送サービス	○	○		理解かつ適合していることを具体的に示すこと。 具体的に示された提案内容が要件を満たした上で、大容量ファイル転送サービスは、電子メールとともに、省内外で情報の交換を行う重要なサービスである。 転送可能なファイル容量とともに、総務省での運用を鑑みた利便性を提供し、かつセキュリティに配慮した提案であると客観的に判断される場合は加点する。			
	5　認証サービス	○	○		理解かつ適合していることを具体的に示すこと。 具体的に示された提案内容が要件を満たした上で、認証サービスは、総務省LANを構成する主要なサービスと連携をとり、一元的に認証を行うとともに、アカウントを管理する中核システムである。 各システムとの親和性を持ち、高い信頼性を有し、確実な処理を行える提案であると客観的に判断される場合は加点する。			
6	6　テレワークサービス	○	○	80	理解かつ適合していることを具体的に示すこと。 具体的に示された提案内容が要件を満たした上で、テレワークサービスは、総務省職員のテレワーク推進を支える上で、重要なサービスである。 省外での利用が中心となるため、セキュリティに関して十分に配慮するとともに、機動性、利便性等を確保した提案であると客観的に判断される場合は加点する。			
	7　コミュニケーションサービス	○	○		理解かつ適合していることを具体的に示すこと。 具体的に示された提案内容が要件を満たした上で、コミュニケーションサービスは、即時性のある多数参加型の双方向のコミュニケーション手段であり、組織生産性に寄与するサービスである。 ユーザの生産性向上に直結するため、利便性を十分に考慮した提案であると客観的に判断される場合は加点する。			
	8　ペーパーレス会議サービス	○	○		理解かつ適合していることを具体的に示すこと。 具体的に示された提案内容が要件を満たした上で、ペーパーレス会議システムサービスは、ワークスタイル変革を推進し、紙資源の削減に寄与するシステムである。 ユーザ以外の外部の参加者も利用するため、セキュリティと利便性が両立した提案であると客観的に判断される場合は加点する。 特に、利便性については、総務省における組織形態や実運用に十分配慮した提案であること。			
	9　プリントサービス	○	○		理解かつ適合していることを具体的に示すこと。 具体的に示された提案内容が要件を満たした上で、プリントサービスは、本省、外部各拠点のプリンタの管理を効率的かつユーザに利便性の高い形で提供できる提案であると客観的に判断される場合は加点する。			
	１０　情報不正出力防止サービス	○	○		理解かつ適合していることを具体的に示すこと。 具体的に示された提案内容が要件を満たした上で、情報不正出力防止サービスは、総務省における情報漏洩を防止し、セキュリティを向上する観点での提案であると客観的に判断される場合は加点する。			
	１１　機密情報保護サービス	○	○		理解かつ適合していることを具体的に示すこと。 具体的に示された提案内容が要件を満たした上で、機密情報保護サービスは、機微情報を扱うため、セキュリティが十分考慮されており、かつ総務省における利便性も同時に確保された提案であると客観的に判断される場合は加点する。			

No	評価項目（調達仕様書・要件定義書の項番に対応する）	必須	加点	加点配点	評価ポイント	提案内容	提案内容補足資料	記載箇所
7	１２　ディザスタリカバリサービス	○	○	40	理解かつ適合していることを具体的に示すこと。 具体的に示された提案内容が要件を満たした上で、ディザスタリカバリサービスは、総務省における業務の重要性を十分認識し、データの保全を考慮するとともに、本省の大規模障害時に拠点外のユーザに対して可能な限り高い性能で、使いやすいディザスタリカバリのサービスを提供できる提案であると客観的に判断される場合は加点する。また、想定される状況への対応や定期的な訓練等を十分に考慮した提案であること。			
-	第４　セキュリティサービス					-	-	-
8	1　マルウェア対策（メール）サービス	○	○	100	理解かつ適合していることを具体的に示すこと。 具体的に示された提案内容が要件を満たした上で、マルウェア対策（メール）サービスは、職員を対象とする迷惑メールやウイルス付メールに対して多層防御の考え方を持って的確・迅速な防御手段を講じ、安全なメール基盤を提供できる提案であると客観的に判断される場合は加点する。			
	2　マルウェア対策（インターネット・Web）サービス	○	○		理解かつ適合していることを具体的に示すこと。 具体的に示された提案内容が要件を満たした上で、マルウェア対策（インターネット・Ｗｅｂ）サービスは、外部とのWebアクセスに係る不正通信の検知・防御について、多層防御の考え方を持って、的確・迅速な防御手段を講じ、安全なWebアクセス基盤を提供できる提案であると客観的に判断される場合は加点する。			
	3　マルウェア対策（サーバ・LAN端末・仮想デスクトップ）サービス	○	○		理解かつ適合していることを具体的に示すこと。 具体的に示された提案内容が要件を満たした上で、マルウェア対策（サーバ・ＬＡＮ端末）サービスは、サーバやLAN端末において、適切にマルウェアの侵入を検知・防御する手段を講じており、かつ当該手段はユーザやシステムに与える影響が少なく、適正なプログラム・パターンファイル更新を考慮した統合的なマルウェア管理・対策の提案であると客観的に判断される場合は加点する。また、マルウェアの拡散防止の提案が具体的であること。			
	4　侵入検知防御サービス	○	○		理解かつ適合していることを具体的に示すこと。 具体的に示された提案内容が要件を満たした上で、侵入検知防御サービスは、外部ネットワークからの侵入や攻撃に対する有効かつ効果的なアクセス制御・侵入防御・証跡管理等を提供する提案であると客観的に判断される場合は加点する。			
	5　不正接続機器検知サービス	○	○		理解かつ適合していることを具体的に示すこと。 具体的に示された提案内容が要件を満たした上で、不正接続機器検知サービスは、総務省LANに接続する不正な端末の検知、防御を効果的かつ効率的に管理できる提案であると客観的に判断される場合は加点する。			
	6　特権アクセス制御サービス	○	○		理解かつ適合していることを具体的に示すこと。 具体的に示された提案内容が要件を満たした上で、特権アクセス制御サービスは、特権アクセス制限の方法を具体的に提示するとともに、管理目的のアクセス及び操作ログの収集・記録を含む提案であると客観的に判断される場合は加点する。			
	7　セキュリティ管理サービス	○	○		理解かつ適合していることを具体的に示すこと。 具体的に示された提案内容が要件を満たした上で、セキュリティ管理サービスは、「総務省情報セキュリティポリシー」に基づいて年一回実施されるセキュリティ監査（総務省LANを構成する各機器が、適正に設定・運用されているかを観点としている。）に対し、柔軟で素早い情報提供を可能とする提案であると客観的に判断される場合は加点する。			
	8　セキュリティログ分析サービス	○	○		理解かつ適合していることを具体的に示すこと。 具体的に示された提案内容が要件を満たした上で、セキュリティログ分析サービスは、マルウェア感染の徴候等を早期に検知することが可能な提案であると客観的に判断される場合は加点する。			
	9　仮想ブラウザサービス	○	○		理解かつ適合していることを具体的に示すこと。 具体的に示された提案内容が要件を満たした上で、仮想ブラウザサービスは、マルウェア感染防止のため、隔離した環境で実施するサービスである。本サービスの構成自体が感染しにくい構造であり、かつ感染時の対処が容易な提案であると客観的に判断される場合は加点する。			

No	評価項目（調達仕様書・要件定義書の項番に対応する）	必須	加点	加点配点	評価ポイント	提案内容	提案内容補足資料	記載箇所
-	第５　運用管理サービス					-	-	-
9	1　申請管理サービス	○	○	50	理解かつ適合していることを具体的に示すこと。 具体的に示された提案内容が要件を満たした上で、申請管理サービスは、分かりやすく、ユーザ負荷の少ない、総務省における利便性に富んだ提案であると客観的に判断される場合は加点する。			
	2　運用支援サービス	○	○		理解かつ適合していることを具体的に示すこと。 具体的に示された提案内容が要件を満たした上で、運用支援サービス、各サービスを安定的に効率よく運用するための提案であり、分析、運用改善に貢献すると客観的に判断される場合は加点する。 セキュリティ対策等を含む、統合的な運用提案であること。			
	3　システム監視サービス	○	○		理解かつ適合していることを具体的に示すこと。 具体的に示された提案内容が要件を満たした上で、システム監視サービスは、総務省LANが正常にかつ円滑に稼働していることを確認できることが重要である。 障害発生時には、迅速かつ正確に被疑部位を特定できるとともに、一次対応の指針となり得る提案であると客観的に判断される場合は加点する。			
	4　ログ管理サービス	○	○		理解かつ適合していることを具体的に示すこと。 具体的に示された提案内容が要件を満たした上で、ログ管理サービスは、システムの異常確認や、障害対処方法の指針を与えるための基礎情報となるだけでなく、ユーザの利用証跡管理も兼ねることから、ログを確実かつ効率的に保全する仕組みの提案であると客観的に判断される場合は加点する。			
	5　バックアップサービス	○	○		理解かつ適合していることを具体的に示すこと。 具体的に示された提案内容が要件を満たした上で、バックアップサービスは、WAN経由でディザスタリカバリサービスに対して行うため、回線帯域等を考慮するとともに、リカバリ時の運用を考慮した最適な提案とすると客観的に判断される場合は加点する。総務省の業務の重要性をを鑑みた事業継続の観点での提案であること。			
	6　電源管理サービス	○	-		理解かつ適合していることを具体的に示すこと。			
	7　資源管理サービス	○	○		理解かつ適合していることを具体的に示すこと。 具体的に示された提案内容が要件を満たした上で、資源管理サービスは、各サービス提供機器やLAN端末、プリンタ等の各種資源を統合的に管理し、効率的かつ確実に状態を把握できる提案であると客観的に判断される場合は加点する。			
	8　モバイルデバイス管理サービス	○	○		理解かつ適合していることを具体的に示すこと。 具体的に示された提案内容が要件を満たした上で、モバイルデバイス管理サービスは、ＬＡＮ端末側の運用やセキュリティに十分配慮した提案であると客観的に判断される場合は加点する。			
	9　シンクライアント管理サービス	○	-		理解かつ適合していることを具体的に示すこと。			
-	第６　その他機器基盤					-	-	-
10	1　検証環境	○	○	20	理解かつ適合していることを具体的に示すこと。 具体的に示された提案内容が要件を満たした上で、検証環境は、運用上の手順確認や動作確認、障害検証等に活用するものであり、総務省LANの安定稼働に寄与させるための提案であると客観的に判断される場合は加点する。			
	2　運用業務環境	○	-		理解かつ適合していることを具体的に示すこと。			
	3　KVM	○	-		理解かつ適合していることを具体的に示すこと。			
	4　UPS	○	-		理解かつ適合していることを具体的に示すこと。			
	5　LAN端末マスタ	○	○		理解かつ適合していることを具体的に示すこと。 具体的に示された提案内容が要件を満たした上で、ＬＡＮ端末マスタ及び仮想デスクトップマスタは、本調達に際し、全てのLAN端末のマスタが更新となることから、そのイメージが適正に作成でき、かつ迅速に導入、展開可能な提案であると客観的に判断される場合は加点する。			
	6　仮想デスクトップマスタ	○	○					

No	評価項目（調達仕様書・要件定義書の項番に対応する）		必須	加点	加点配点	評価ポイント	提案内容	提案内容補足資料	記載箇所
-		第７　ネットワーク基盤					-	-	-
11	別紙１－３（要件定義書（回線））	１　本省LAN	○	○	30	理解かつ適合していることを具体的に示すこと。 具体的に示された提案内容が要件を満たした上で、本省ＬＡＮは、ユーザが各サービスを利用するのに必要十分な処理能力、帯域・ポート数を有する機器を適正数配置し、高い信頼性と可用性を確保できる構成の提案であると客観的に判断される場合は加点する。 特に本省は様々な用途のネットワークを有するため、独立性、セキュリティに配慮した提案であること。			
		２　拠点LAN	○	○		理解かつ適合していることを具体的に示すこと。 具体的に示された提案内容が要件を満たした上で、拠点ＬＡＮは、ユーザが各サービスを利用するのに必要十分な処理能力、帯域・ポート数を有する機器を適正数配置し、高い信頼性と可用性を確保できる構成の提案であると客観的に判断される場合は加点する。			
		３　ネットワークサービス	○	○		理解かつ適合していることを具体的に示すこと。 具体的に示された提案内容が要件を満たした上で、ネットワークサービスは、総務省LANを利用する上で基本となる不可欠なサービスである。十分な可用性とセキュリティを考慮した構成の提案であると客観的に判断される場合は加点する。			
		４　無線LAN接続サービス	○	○		理解かつ適合していることを具体的に示すこと。 具体的に示された提案内容が要件を満たした上で、無線ＬＡＮ接続サービスは、無線LANの接続利便性を最大限に活かし、セキュリティや運用性を考慮した提案であると客観的に判断される場合は加点する。			
		５　インターネット接続回線	○	-		理解かつ適合していることを具体的に示すこと。			
		６　本省WAN	○	-		理解かつ適合していることを具体的に示すこと。			
		７　拠点WAN	○	-		理解かつ適合していることを具体的に示すこと。			
		８　外部監視室用回線	○	-		理解かつ適合していることを具体的に示すこと。			
12	別紙１－３（要件定義書（回線））	インターネット接続回線	○	○	30	理解かつ適合していることを具体的に示すこと。 具体的に示された提案内容が要件を満たした上で、インターネット接続回線は、総務省全体で利用することを踏まえた、高品質・広帯域の回線提案であること。			
		ＷＡＮ回線	○	○		理解かつ適合していることを具体的に示すこと。 具体的に示された提案内容が要件を満たした上で、本省ＷＡＮ及び拠点ＷＡＮは、各拠点が総務省LANサービスを快適に利用できる、高品質・広帯域の回線であること。全国に素早く展開し、運用時の拠点増減にも柔軟に対応できる提案であると客観的に判断される場合は加点する。			
		監視用回線他	○	-		理解かつ適合していることを具体的に示すこと。			
13	別紙１－４（要件定義書（運用及び維持保守・管理））	第１　全体概要	○	○	100	理解かつ適合していることを具体的に示すこと。 具体的に示された提案内容が要件を満たした上で、総務省ＬＡＮの運用及び維持保守・管理について、総務省LANの重要性を鑑み、必要十分なサービスレベルを提案であると客観的に判断される場合は加点する。その測定方法や測定点等も、継続する総務省LANの特性や運用を考慮した、現実的なPDCAサイクルの提案であること。 大規模・複雑な総務省LANを効率的に運用しながらもユーザ視点での質の高いサービス、主管課の負荷を減らせるよう、主体的に動ける要員と要員を適正に稼働させられるリーダシップ、組織体制の提案であること。総務省LANの各システムの稼働状況やリソースを適正に把握・管理し、性能を担保しつつ、能動的な運用を行える提案であると客観的に判断される場合は加点する。 また、本省はもちろんのこと、全国の拠点に対する迅速な保守が可能な保守拠点体制、部材確保、実績、対応時間等の提案であると客観的に判断される場合は加点する。			
		第２　サービスストラテジ	○	○					
		第３　サービスデザイン	○	○					
		第４　サービストランジション	○	○					
		第５　サービスオペレーション	○	○					
		第６　継続的サービス改善	○	○					
		第７　サービスデスク	○	○					
		第８　ソフトウェア保守要件	○	○					
		第９　ハードウェア保守要件	○	○					

別紙2　総合評価基準及び対応表

No	評価項目（調達仕様書・要件定義書の項番に対応する）		必須	加点	加点配点	評価ポイント	提案内容	提案内容補足資料	記載箇所
14	（追加提案）	全体構成	-	○	20	全体構成が、具体的な実運用イメージを持って設計され、かつ各サービス、各システム間で適切に連携し、また、全体としてバランスが取れた構成の提案であると客観的に判断される場合は加点する。			
15		追加提案	-	○	80	上記加点評価項目以外に、総務省LANを利用する上で有益な提案があったと客観的に判断される場合は加点する。			
16	（プレゼンテーション）	プロジェクトマネージャ	-	○	50	プロジェクトマネージャのプレゼンテーション能力、各種サービスに関する知識、プロジェクト推進のノウハウや経験があるかについて評価する。	-	-	-
17		上級セキュリティエンジニア	-	○	50	上級セキュリティエンジニアのセキュリティインシデントへの対応能力、最新のセキュリティに関する知識、過去のセキュリティ運用やインシデント対応に関するノウハウや経験があるかについて評価する。	-	-	-
18		運用責任者	-	○	50	運用責任者の実運用における運用統括能力、運用知識、経験、インシデント発生時の対応能力等を評価する。	-	-	-

加点合計　1000