資料１－２

総務省ＬＡＮシステムの更新整備及び保守・運用業務

民間競争入札実施要項

総務省大臣官房企画課サイバーセキュリティ・情報化推進室

【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」を、「総務省ＬＡＮシステムの更新整備及び保守・運用業務」（以下「更新整備及び保守・運用業務」という。）及び「総務省ＬＡＮシステムの運用管理及び受付窓口業務」（以下「運用管理及び受付窓口業務」という。）に分離、調達することによって、競争性を発揮できるよう考慮した。

このうち、更新整備及び保守・運用業務について、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。

なお、運用管理及び受付窓口業務については、令和２年度中に公共サービス改革基本方針に従って、別途実施要項を定めるものとする。

２　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質に関する事項

（１）更新整備及び保守・運用業務の業務内容

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た。

現行の総務省ＬＡＮは、第４期システムとして平成 28 年度に構築、令和 3 年９月まで運用することとしており、次期総務省ＬＡＮは令和２年度中に更新整備を開始し、令和３年 10 月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、「デジタル・ガバメント実行計画」（令和元年 12 月 20 日改定閣議決定）、「デジタル・ガバメント推進標準ガイドライン」（令和２年３月 31 日最終改定各府省情報化統括責任者（ＣＩＯ）連絡会議決定）と関連する指針類等に係る文書体系（両者を併せて、以下「標準ガイドライン群」という。）、「政府情報システムにおけるクラウドサービスの利用に係る基本方針」（平成 30 年６月７日各府省情報統括化責任者（ＣＩＯ）連絡会議決定）、「政府機関等の情報セキュリティ対策のための統一基準（平成 30 年度版）」（平成 30 年７月 25 日サイバーセキュリティ戦略本部）等の政府方針やガイドラインに沿って検討を行い、総務省ＬＡＮの基盤システムとしての重要性を踏まえ、安定性と信頼性の更なる向上を図り、併せて、高度に複雑化するサイバー攻撃への情報セキュリティ対策を強化し、安全・安心な基盤システムを実現することを整備方針とする。

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、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。

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	
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を提供する。ポータルサイトは、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、電子掲示板機能、アンケート機能、会議室予約機能、スケジューラ（予定表）機能、設備予約機能、自動応答機能提供する。
ファイル共有サービス	総務省職員間が業務情報である電子データを保存・共有するため、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、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、大容量ファイル転送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。
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。
プリントサービス	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。
インターネット閲覧サービス	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環境として、インターネット閲覧サービスを提供する。
機密情報保護サービス	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、機密情報保護サービスを提供する。
2. サービス基盤	
認証サービス	総務省職員等のアカウント情報を管理し、各サービスへの接続時に認証及びアクセス権の付与、証明書の発行・配布やライセンス認証等を行う。
テレワークサービス	省外から LAN 端末を用いて、本省で利用する場合と同等のサービス・機能を利用できるリモートアクセス機能を提供する。省外から支給端末（Windows タブレット）及び私物端末（PC・モバイル）を用いて、本省内で LAN 端末を利用する場合と同等のサービス･機能を利用できる仮想デスクトップ機能を提供する。
私物等端末リモートアクセスサービス	省外から私物等端末（モバイル）を用いて、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を利用できる環境を提供する。
デバイス管理サービス	ペーパーレス会議サービスで利用するタブレット型端末及び省外で利用する支給端末（Windows タブレット）のハードウェア情報・ソフトウェア情報等の収集、ソフトウェア・プロファイルの配布等を行う。また、端末の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。
資源管理サービス	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収集や、ソフトウェア（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。

機能等の名称		機能等の概要
	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し、情報の不正出力を防止する環境を提供する。
3. ネットワーク基盤		
	本省 LAN	本省 LAN は、総務省職員が総務省 LAN サービスを利用するため、また、本省内に設置するサーバや、業務システム及び政府共通ネットワークと接続するためのネットワークを提供する。
	DR サイト LAN	DR サイト LAN は、DR サイト内に設置するサーバや政府共通ネットワークと接続するためのネットワークを提供する。
	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のネットワークを提供する。
	総務省 WAN	総務省 WAN は、総務省職員が総務省 LAN サービスを利用するため、本省、各地方拠点及び DR サイトを相互に接続するためのネットワークを提供する。
	外部監視室接続ネットワーク	外部から総務省 LAN を 24 時間 365 日監視するため、本省及び DR サイトと外部監視室を独立した閉域網で接続する。
	インターネット接続ネットワーク	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を本省及び DR サイトにて提供する。
	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。
	無線 LAN 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、LAN 端末に無線 LAN 接続サービスを提供する。また、ペーパーレス会議サービスのタブレット型端末と情報不正出力防止サービスのウイルスチェック用端末にも無線 LAN 接続サービスを提供する。
4. セキュリティサービス		
	マルウェア対策（メール）サービス	メールからのマルウェア等の感染を早期に検知・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。
	マルウェア対策（サーバ・端末）サービス	サーバ、LAN 端末、仮想デスクトップ、ウイルスチェック用端末、運用端末及びファイル共有領域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・端末）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。
	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。
	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。
	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。

機能等の名称	機能等の概要
5. 運用管理サービス	
申請管理サービス	受付窓口を通じて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 に関するユーザからの支援依頼内容を一元管理し、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。
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。
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、保守・運用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。
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、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。
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。

エ　総務省ＬＡＮの構成概要

総務省ＬＡＮの概要図を図２-１　総務省ＬＡＮシステム概要図に示す。

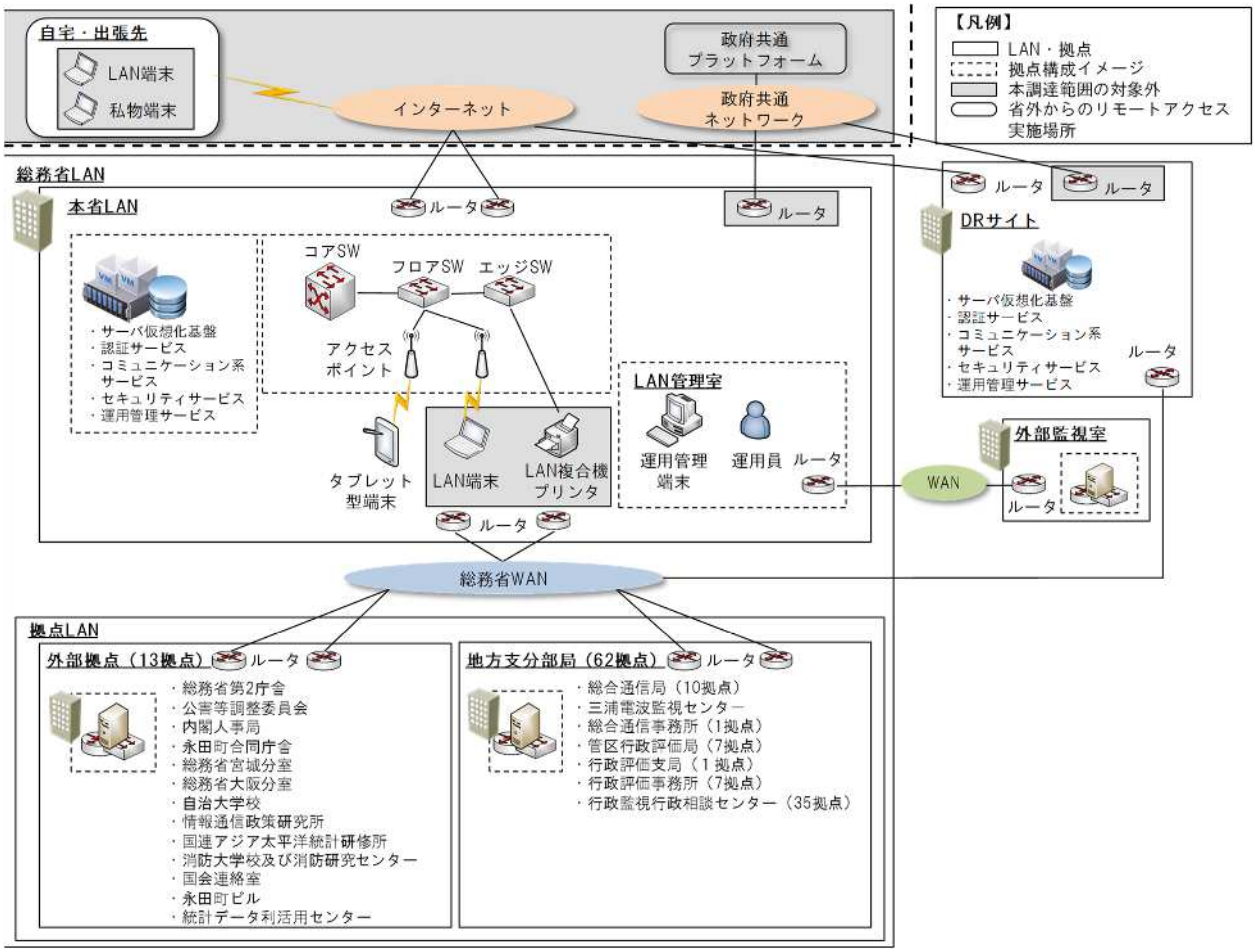


図２-１　総務省ＬＡＮシステム概要図

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。）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、総務省第２庁舎、公害等調整委員会、内閣人事局、永田町合同庁舎、総務省宮城分室、総務省大阪分室、自治大学校、情報通信政策研究所、国連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、永田町ビル、統計データ利活用センターの 13 拠点を指す。

（エ）地方支分部局

地方支分部局は、全国に点在する管区行政評価（支）局・行政評価事務所・行政監視行政相談センター及び総合通信局・総合通信事務所の 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、本省において大規模な災害や障害等が発生した際に、本省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。

（令和２年１月現在）

ユーザアカウント数		
	ユーザアカウント数	7,000 個
	一時保管アカウント	2,000 個
	共有アカウント	2,800 個
	保守・運用業務用アカウント	1,400 個
クライアント端末数		7,000 台
拠点数	外部拠点	13 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の更新整備及び保守・運用業務は、①総務省ＬＡＮの設計・構築を行う更新整備業務、②システムの機能維持、品質維持等、設計された仕様どおりに動作させることを目的とした保守業務、システムの稼働状態を維持することを目的とした運用業務である、その詳細は、「総務省ＬＡＮに係る更新整備及び保守・運用業務の請負　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）更新整備

請負者は、更新整備及び保守・運用業務のうち更新整備業務について、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、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、標準ガイドライン群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、テスト、受入テストの実施支援、移行及び教育訓練等を実施する。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	主管課及び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。
要件定義書の確定	主管課、工程管理事業者及びＰＭＯ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、ＰＭＯによる第二次工程レビューを受け、主管課の承認を得て、要件定義書を確定させること。
設計の実施	確定された要件定義書に基づき、要件を実現するために必要となる基本設計、詳細設計及び運用設計を行い、各種設計書や各種規程、要領、操作マニュアル等を作成し、主管課の承認を得ること。
構築の実施	作成された各種設計書や計画書等に基づき、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。
テストの実施	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、単体テスト、結合テスト、総合テスト、その他総務省ＬＡＮの稼働に必要なテスト計画を作成し、その計画に基づいてテストを実施すること。また、それぞれのテスト計画、テスト結果について主管課の承認を受けること。 なお、遅くとも総合テスト計画を確定するまでに、ＰＭＯによる第三次工程レビューを受けること。
受入テストの実施支援	主管課は、総務省ＬＡＮの構築が完了する前に、総務省ＬＡＮで求めている要件を満たしているか確認するため、受入テストを実施する。請負者は、受入テストの計画案の策定、受入テスト仕様書案の策定、受入テストの実施を支援すること。また、受入テストの結果、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。
移行の実施	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。

作業	概要
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。
教育訓練の実施	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。
ＯＤＢ登録用シートの提出	請負者は、「デジタル・ガバメント推進標準ガイドライン」における別紙３「調達仕様書に盛り込むべきＯＤＢ登録用シートの提出に関する作業内容」に基づき、必要な事項について記載したＯＤＢ登録用シートを提出すること。

（ウ）保守・運用

請負者は、更新整備及び保守・運用業務のうち保守・運用業務について、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）、保守・運用要領（案）、保守・運用実施計画書を作成し、主管課の承認を得る。

請負者は、承認された保守・運用実施計画書に基づき、保守・運用業務を実施する。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保守業務及び情報システムの稼働状態を維持することを目的とした運用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。保守・運用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。

各作業の概要を表２-３　保守・運用作業の概要に示す。

表２-３　保守・運用作業の概要

作業	概要
保守・運用要領等の作成	運用を開始するに当たり、「保守・運用要領」を作成し、主管課の承認を受けること。

作業	概要
中長期保守・運用作業計画の作成	「保守・運用要領」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「中長期保守・運用作業計画」を作成すること。「中長期保守・運用作業計画」には、情報システムの構成やライフサイクルを通じた保守作業及び運用業務の内容について記載すること。
保守・運用実施計画書の作成	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「保守・運用実施計画書」を作成し、主管課の承認を受けること。
平常時対応	保守・運用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保守・運用設計書、操作手順や解説等を記載した保守・運用手順書を作成し、保守・運用業務を行う。 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。 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、継続的なサービス改善等の運用業務を行うこと。 また、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。 その他、必要に応じ適宜「運用管理及び受付窓口業務」の請負者と連携し、対応すること。
障害発生時対応	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。

作業	概要
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、「保守・運用要領」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。
主管課等支援業務	総務省ＬＡＮへの接続、政府共通プラットフォームへの移行等、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。
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こと。
保守・運用業務の改善提案	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「保守・運用要領」、「中長期保守・運用作業計画」及び「保守・運用実施計画書」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。
ＯＤＢ登録シートの提出	「標準ガイドライン群」における別紙３「調達仕様書に盛り込むべきＯＤＢ登録シートの提出に関する作業内容」に基づき、必要な事項について記載したＯＤＢ登録用シートを提出すること。

（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）更新整備及び保守・運用業務の業務内容」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。

（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、「総務省ＬＡＮシステムの更新整備及び保守・運用業務の請負　総合評価基準書」に従い、更新整備及び保守・運用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、「総務省ＬＡＮシステムの更新整備及び保守・運用業務の請負　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、「総務省ＬＡＮシステムの更新整備及び保守・運用業務の請負　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。令和２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、令和３年度以降においては、契約金額から設計・構築費を差し引いた額に令和３年度以降の期間の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、令和２年 10 月から令和７年３月 31 日までとする。

なお、更新整備の期間は、令和２年 10 月から令和３年９月まで、保守・運用の期間は、令和３年 10 月から令和７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　全体スケジュール（想定）に示す。

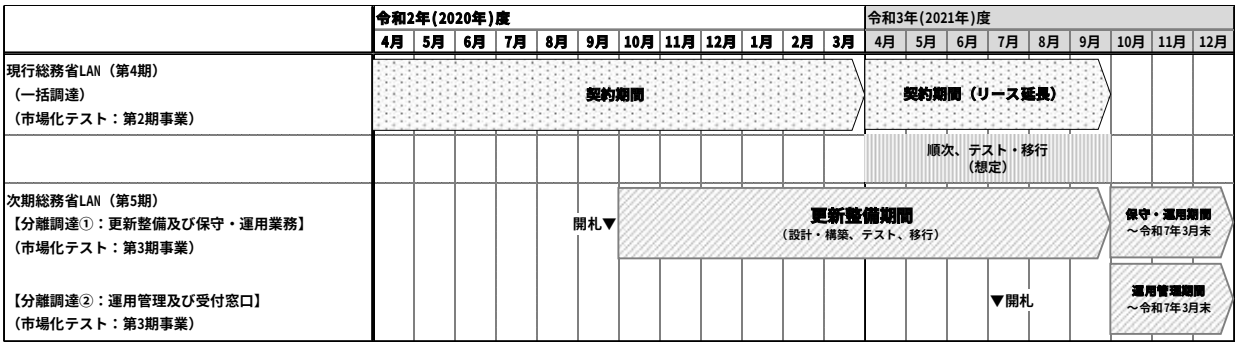


図３-１　全体スケジュール（想定）

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 31・32・33 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の調達支援及び計画・設計工程管理支援業務の請負」の受注事業者

ウ　「次期総務省ＬＡＮの調達支援及び構築、保守・運用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）建設業法（昭和 24 年法律第 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	令和２年	３月中旬
イ　資料閲覧（第１回目）		３月下旬
ウ　入札公示（官報掲載）		５月下旬
エ　入札説明会		６月中旬
オ　本省サーバ室の現地確認		６月中旬
カ　資料閲覧（第２回目）		６月中～下旬
キ　質問受付期限		７月下旬
ク　入札書（提案書）提出期限		８月上旬
ケ　入札参加者によるプレゼンテーション		８月上旬
コ　提案書の審査		８月中～下旬
サ　開札及び落札予定者の決定		９月上旬
シ　契約締結		９月下旬

（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

「総務省ＬＡＮシステムの更新整備及び保守・運用業務の請負　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 110 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 31・32・33 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　更新整備及び保守・運用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「総務省ＬＡＮシステムの更新整備及び保守・運用業務の請負　総合評価基準書」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 ＝ １：３**

総合評価点 ＝ 価格点（1,000 点満点） ＋ 技術点（3,000 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）×1,000 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４－２「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（300 点） ＋ 加点（2,700 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、その理由を官民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　更新整備及び保守・運用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　更新整備及び保守・運用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　更新整備及び保守・運用業務の請負者が、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業務の適正かつ確実な実施の確保のために本業務の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、「総務省ＬＡＮシステムの更新整備及び保守・運用業務の請負調達仕様書」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、令和３年９月末までに完了し、運用開始は、令和３年 10 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　契約不適合責任

（ア）総務省は、請負者に対し、引き渡された成果物が種類又は品質に関して契約の内容に適合しないものである場合（その不適合が総務省の指示によっ

て生じた場合を除き、請負者が当該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場合を含む。）において、その不適合を総務省が知った日から起算して 1 年以内にその旨の通知を行ったときは、その成果物に対する修補等による履行の追完を請求することができる。ただし、請負者は、総務省に不相当な負担を課するものでないときは、総務省が請求した方法と異なる方法による履行の追完をすることができる。

（イ）（ア）の場合において、総務省が相当の期間を定めて履行の催告をし、その期間内に履行の追完がないときは、総務省は、その不適合の程度に応じて代金の減額を請求することができる。

（ウ）（ア）又は（イ）の場合において、総務省は、損害賠償を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更新整備及び保守・運用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更新整備 及び 保守・運用業務に係る 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、総務大臣が行う評価の時期（令和５年２月を予定）及び本業務の本格運用開始時期（令和 3 年度）を踏まえ、令和４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

（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、令和５年２月を目途として、本業務の実施状況を総務大臣及び官民競争入札等監理委員会へ提出する。

なお、調査報告を総務大臣及び官民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）更新整備及び保守・運用業務の実施状況等の官民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官民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サイバーセキュリティ・情報化推進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サイバーセキュリティ・情報化推進室課長補佐

（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（昭和 45 年法律第 48 号）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）更新整備及び保守・運用業務の調達仕様書

本請負業務を実施する際に必要な仕様は、「総務省ＬＡＮシステムの更新整備及び保守・運用業務の請負　調達仕様書」に示すとおりである。

１３別紙一覧

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 システムの更新整備及び保守・運用業務の請負 総合評価基準書」
別紙４-２「総合評価基準及び対応表」
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 28 年度	平成 29 年度	平成 30 年度
総務省情報ネットワークの構築等の請負業務					
	請負費	役務（運用員）	－	119,337	119,337
		機器・回線リース料	－	1,513,009	1,513,009
		設計・構築費	1,470,616	－	－
		その他	－	－	－
計			1,470,616	1,632,346	1,632,346

（注記事項）

平成 29 年度：運用期間 12 月
平成 30 年度：運用期間 12 月

設計・構築期間：平成 28 年４月～平成 29 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 28 年度	平成 29 年度	平成 30 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 29・30 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。

障害発生対応

・平成 29 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)
LAN 端末障害	43	49	45	73	63	68	56	62	58	64	49	56	686
サーバ・ネットワーク障害	8	2	3	3	5	6	1	4	1	4	1	6	44

・平成 30 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)
LAN 端末障害	92	57	38	46	51	35	45	33	53	36	32	66	584
サーバ・ネットワーク障害	3	1	3	1	2	1	2	6	5	2	5	8	39

情報セキュリティ対応

・平成 29 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）	160	169	154	120	143	252	343	297	341	227	230	283	2719

・平成 30 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）	472	494	382	565	384	871	655	718	686	613	535	647	7022

※ 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 29 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)
LAN 端末対応件数	6	5	4	5	4	3	5	5	3	5	4	3	53
サーバ対応件数	274	60	216	192	264	240	318	343	301	378	368	298	3252
その他対応件数	1	0	0	5	0	0	2	4	0	7	0	0	19

・平成 30 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)
LAN 端末対応件数	5	4	5	6	8	5	6	7	4	3	7	2	62
サーバ対応件数	282	366	322	241	321	246	312	298	285	214	253	312	3452
その他対応件数	0	0	0	4	0	3	0	0	1	0	2	0	10

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（更新整備及び保守・運用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（令和２年１月 29 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（統計局、政策統括官（統計基準担当）、政策統括官（恩給担当））	162-8668	東京都新宿区若松町 19-1
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 10 階
内閣人事局	100-8914	東京都千代田区永田町 1-6-1 中央合同庁舎第 8 号館 5 階

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委員会、公共サービス改革推進室）	100-0014	東京都千代田区永田町 1-11-39
総務省宮城分室	－	宮城県仙台市内
総務省大阪分室	－	大阪府豊中市内
自治大学校	190-8581	東京都立川市緑町 10-13591
情報通信政策研究所	185-8795	東京都国分寺市泉町 2-11-16
国連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 日本貿易振興機構アジア経済研究所ビル 4 階
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 4 階
永田町ビル （電気通信紛争処理委員会･政治資金適正化委員会）	100-0014	東京都千代田区永田町 2-17-3 住友不動産永田町ビル 4 階
統計データ利活用センター	640-8203	和歌山県和歌山市東蔵前丁 3-17 南海和歌山市駅ビル 5 階
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
函館行政監視行政相談センター	040-0032	北海道函館市新川町 25-18 函館地方合同庁舎 6 階
旭川行政監視行政相談センター	078-8501	北海道旭川市宮前 1 条 3 丁目 3 番 15 号 旭川合同庁舎西館 5 階
釧路行政監視行政相談センター	085-0022	北海道釧路市南浜町 5-9 釧路港湾合同庁舎 3 階
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 10 階、11 階
青森行政監視行政相談センター	030-0801	青森県青森市新町 2-4-25 青森合同庁舎 4 階
岩手行政監視行政相談センター	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
秋田行政監視行政相談センター	010-0951	秋田県秋田市山王 7-1-3 秋田合同庁舎 4 階
山形行政監視行政相談センター	990-0041	山形県山形市緑町 1-5-48 山形地方合同庁舎 3 階
福島行政監視行政相談センター	960-8021	福島県福島市霞町 1-46 福島合同庁舎 3 階
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
茨城行政監視行政相談センター	310-0061	茨城県水戸市北見町 1-11 水戸地方合同庁舎 2 階
栃木行政監視行政相談センター	320-0043	栃木県宇都宮市桜 5-1-13 宇都宮地方合同庁舎 3 階
群馬行政監視行政相談センター	371-0026	群馬県前橋市大手町 2-3-1 前橋地方合同庁舎 6 階
千葉行政監視行政相談センター	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
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
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
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
山梨行政監視行政相談センター	400-0031	山梨県甲府市丸の内 1-1-181219 甲府合同庁舎 9 階
長野行政監視行政相談センター	380-0846	長野県長野市旭町 1108 長野第 1 合同庁舎 4 階
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

富山行政監視行政相談センター	930-0856	富山県富山市牛島新町 11-7 富山合同庁舎 5 階
石川行政評価事務所	920-0024	石川県金沢市西念 3-4-1 金沢駅西合同庁舎 4 階 2260
岐阜行政監視行政相談センター	500-8114	岐阜県岐阜市金竜町 5-13 岐阜合同庁舎 2 階
静岡行政監視行政相談センター	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
三重行政監視行政相談センター	514-0033	三重県津市丸之内 26-8 津合同庁舎 3 階
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
福井行政監視行政相談センター	910-0859	福井県福井市日之出 3-14-15　福井地方合同庁舎 2 階
滋賀行政監視行政相談センター	520-0044	滋賀県大津市京町 3-1-1 大津びわ湖合同庁舎 7 階
京都行政監視行政相談センター	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
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
奈良行政監視行政相談センター	630-8213	奈良県奈良市登大路町 81 奈良合同庁舎 4 階
和歌山行政監視行政相談センター	640-8143	和歌山県和歌山市二番丁 3 和歌山地方合同庁舎 3 階 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 13 階
鳥取行政監視行政相談センター	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
島根行政監視行政相談センター	690-0841	島根県松江市向島町 134-10 松江地方合同庁舎 2 階
岡山行政監視行政相談センター	700-0984	岡山県岡山市北区桑田町 1-36 岡山地方合同庁舎 3 階
山口行政監視行政相談センター	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 2 階
四国行政評価支局	760-0019	香川県高松市サンポート 3 番 33 高松サンポート合同庁舎南館 6 階
徳島行政監視行政相談センター	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
愛媛行政監視行政相談センター	790-0808	愛媛県松山市若草町 4-3 松山若草合同庁舎 4 階
高知行政監視行政相談センター	780-0870	高知県高知市本町 4-3-41 高知地方合同庁舎 2 階
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
佐賀行政監視行政相談センター	840-0041	佐賀県佐賀市城内 2-10-20 佐賀合同庁舎 3 階
長崎行政監視行政相談センター	852-8106	長崎県長崎市岩川町 16-16 長崎合同庁舎 5 階
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
大分行政監視行政相談センター	870-0016	大分県大分市新川町 2-1-36 大分合同庁舎 4 階
宮崎行政監視行政相談センター	880-0805	宮崎県宮崎市橘通東 3-1-22 宮崎合同庁舎 4 階
鹿児島行政監視行政相談センター	892-0812	鹿児島県鹿児島市浜町 2-5-11321 鹿児島港湾合同庁舎 5 階
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
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 12 階
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 12-15 階
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
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
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
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
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

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	愛媛県松山市味酒町 2-14-485
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
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
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 28 年度		平成 29 年度		平成 30 年度	
	目標	実績	目標	実績	目標	実績
総務省 LAN の稼働率	－	－	99.90%	99.998%	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	87 点	75 点	89 点

（注記事項）

総務省ＬＡＮの利用満足度調査（回答時間、平易な回答・説明、正確な回答・説明及び担当者の対応の４項目についてアンケート形式で調査を実施）は、平成 29 年度分を平成 30 年４月、平成 30 年度分を平成 31 年３月に実施した。平成 29 年度分は回答者数 89 人（回収率 100%）、平成 30 年度は回答者数 74 人（回収率 82%）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

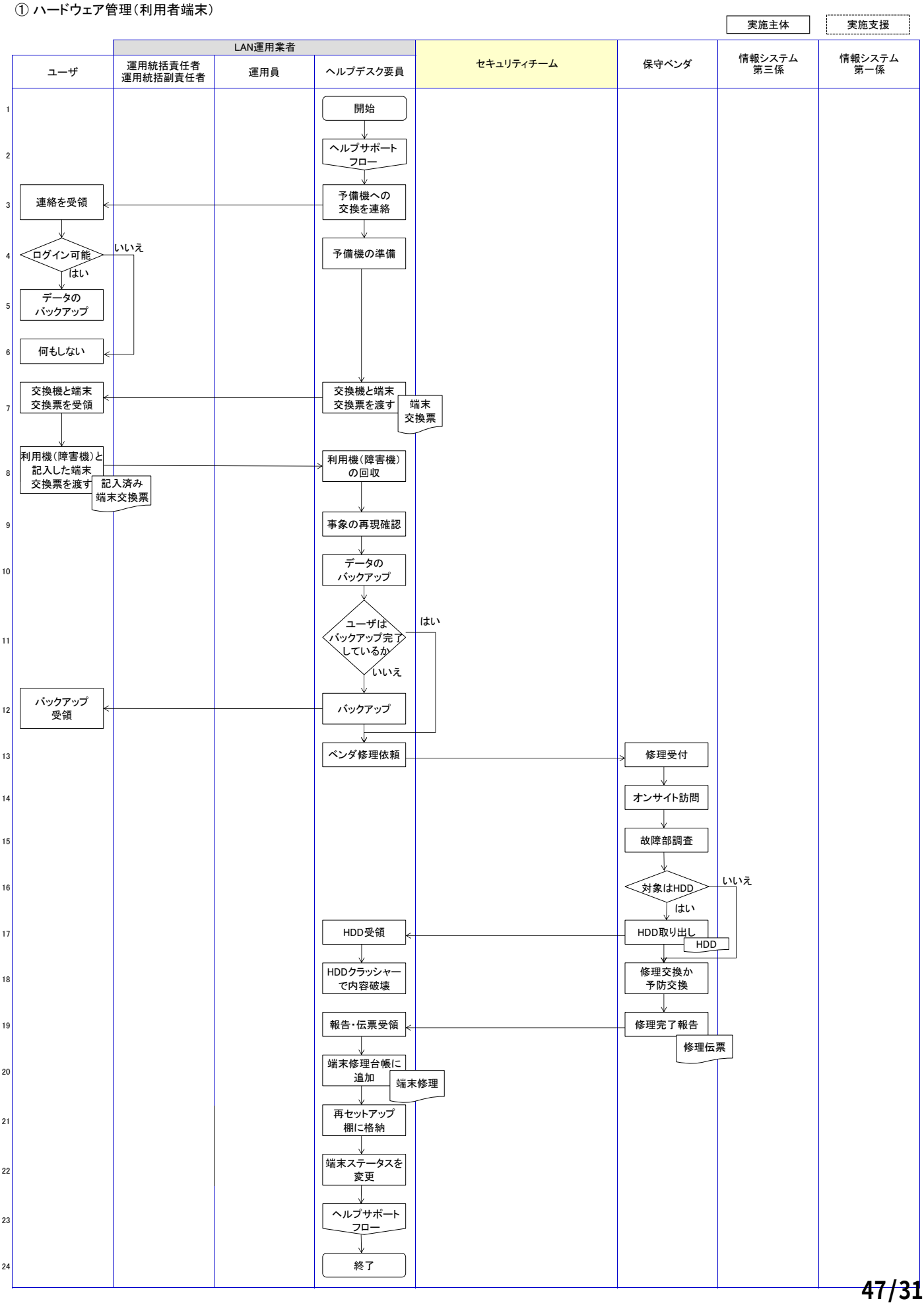
従来の実施方法（業務フロー図等）

別紙２のとおり。

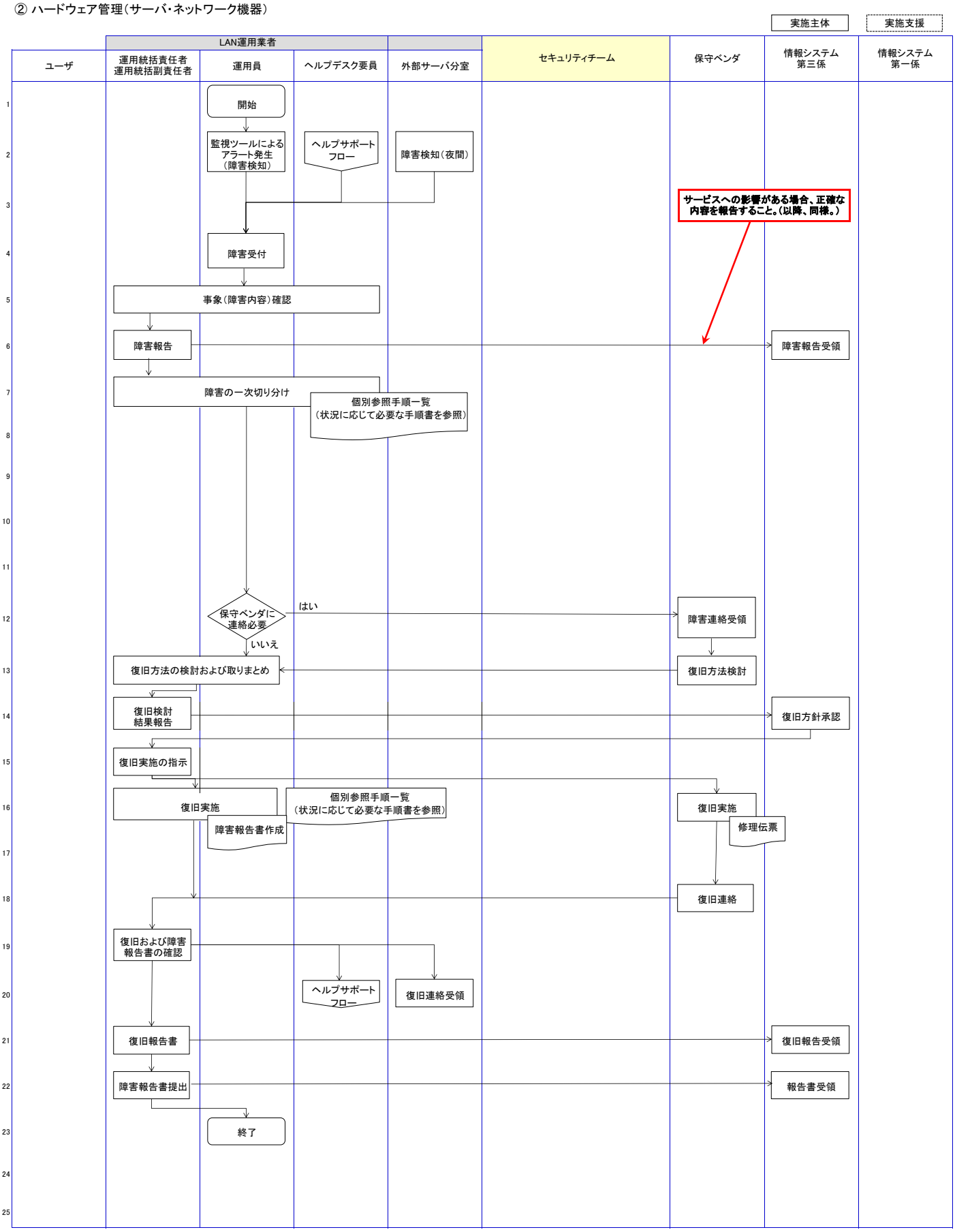
（注記事項）

・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。

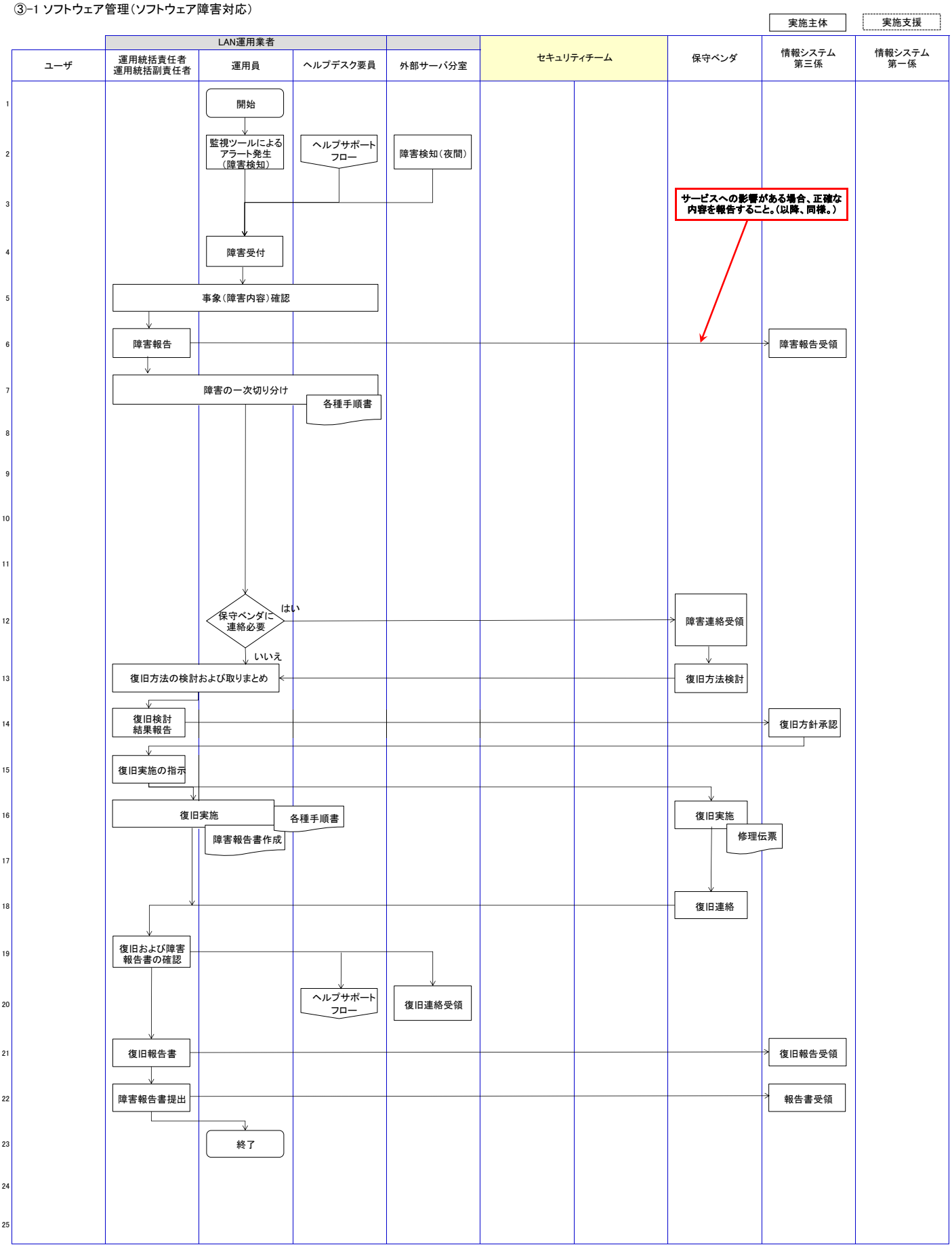
① ハードウェア管理（利用者端末）



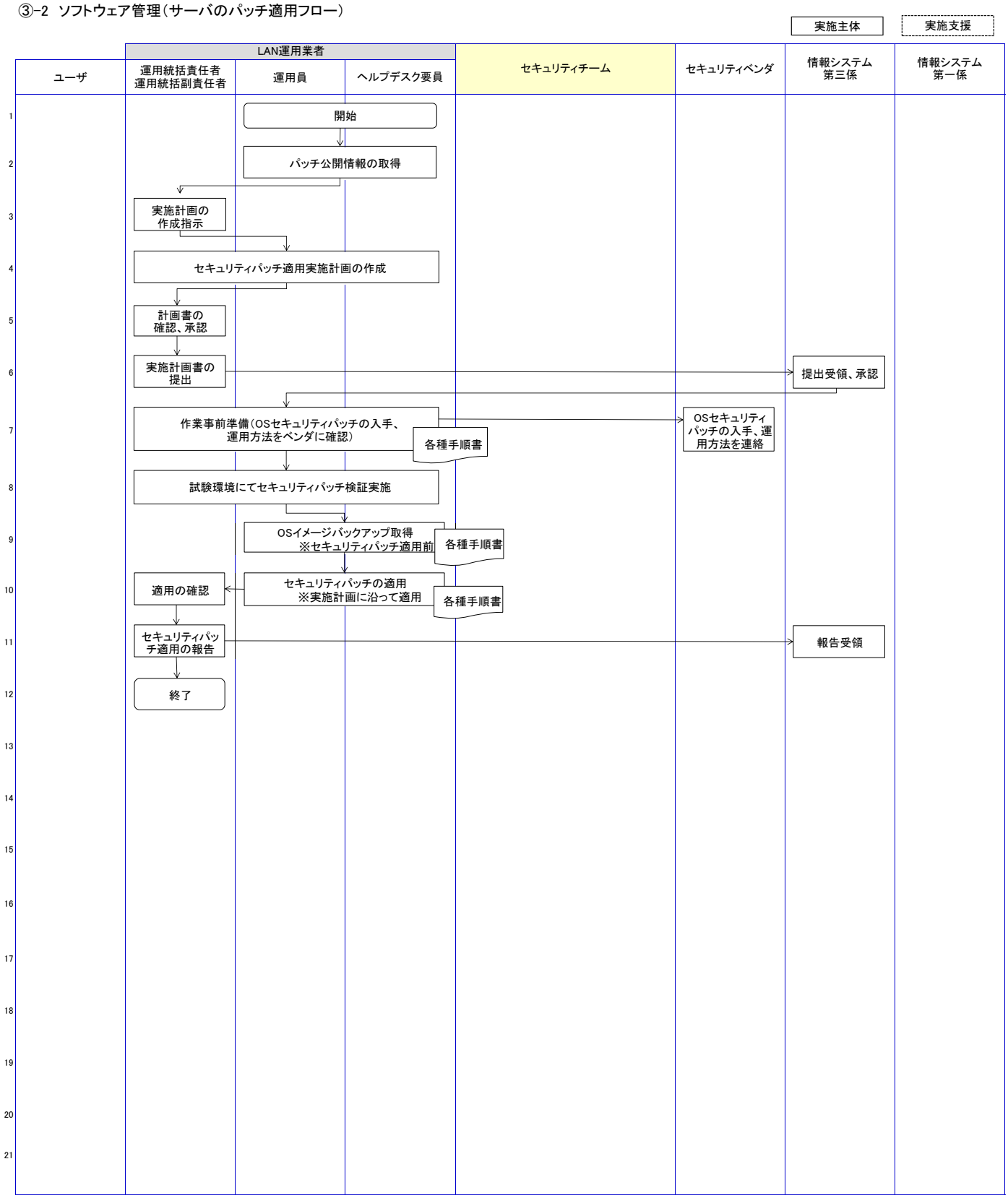
② ハードウェア管理（サーバ・ネットワーク機器）



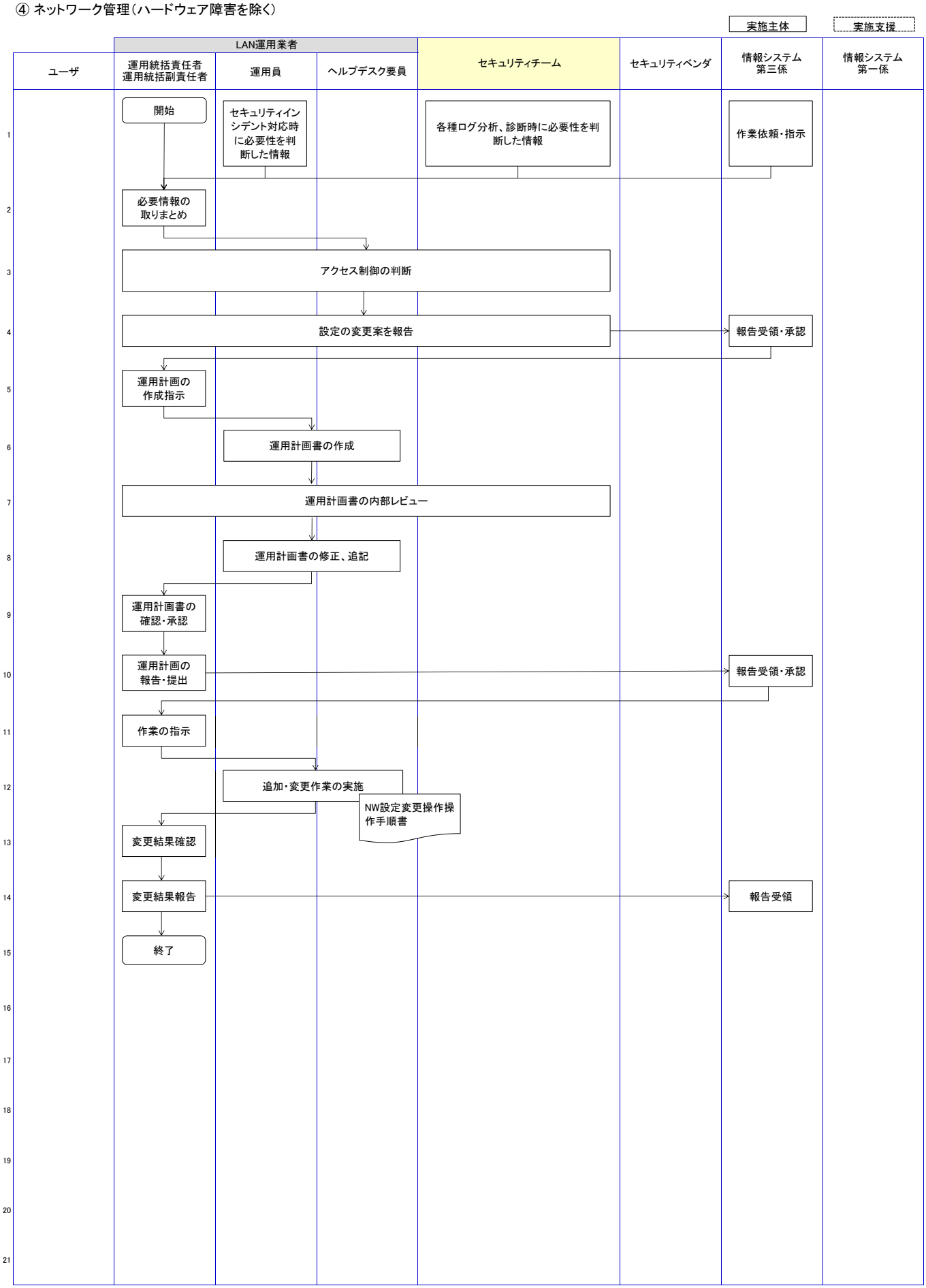
③-1 ソフトウェア管理（ソフトウェア障害対応）



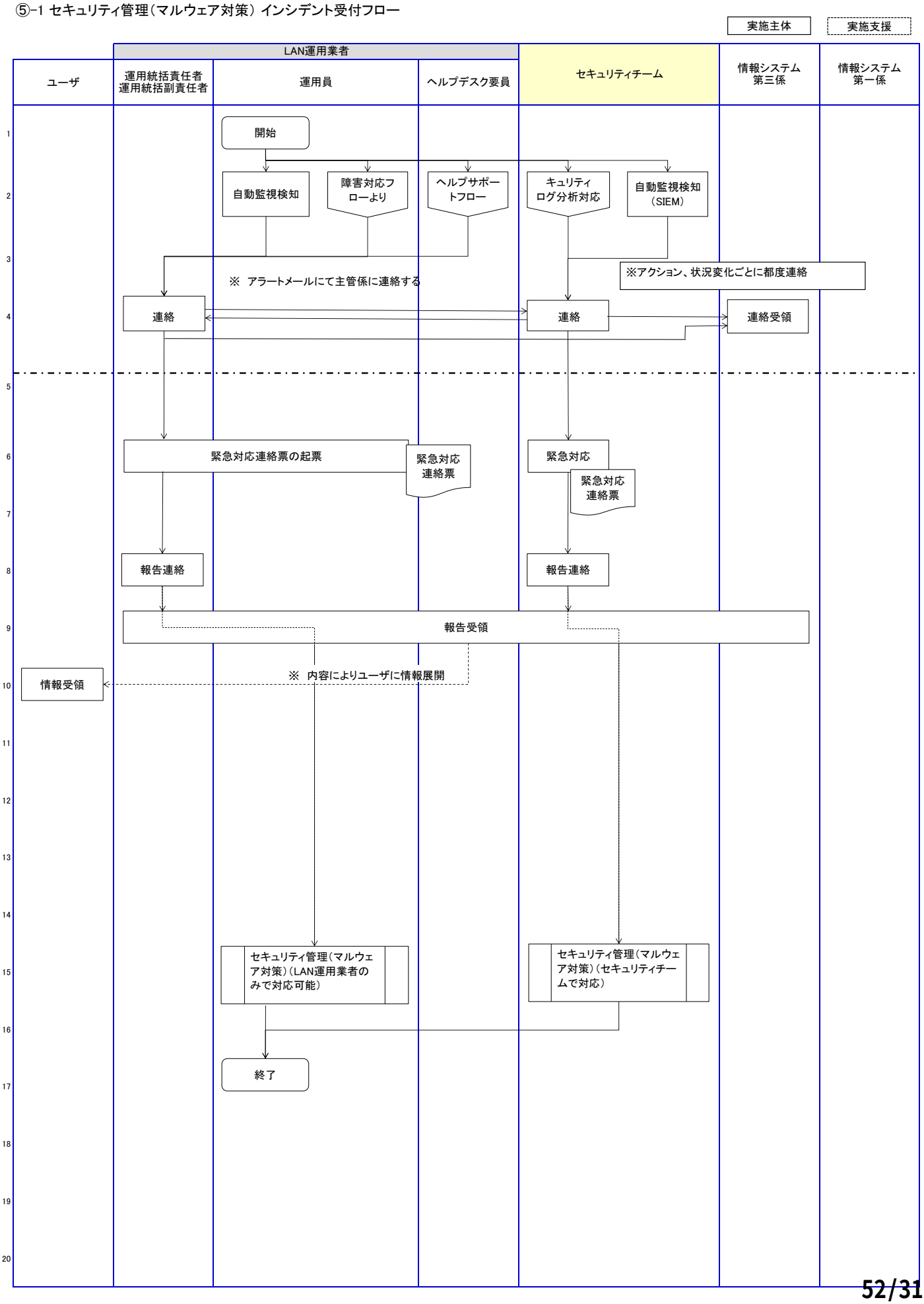
③-2 ソフトウェア管理（サーバのパッチ適用フロー）



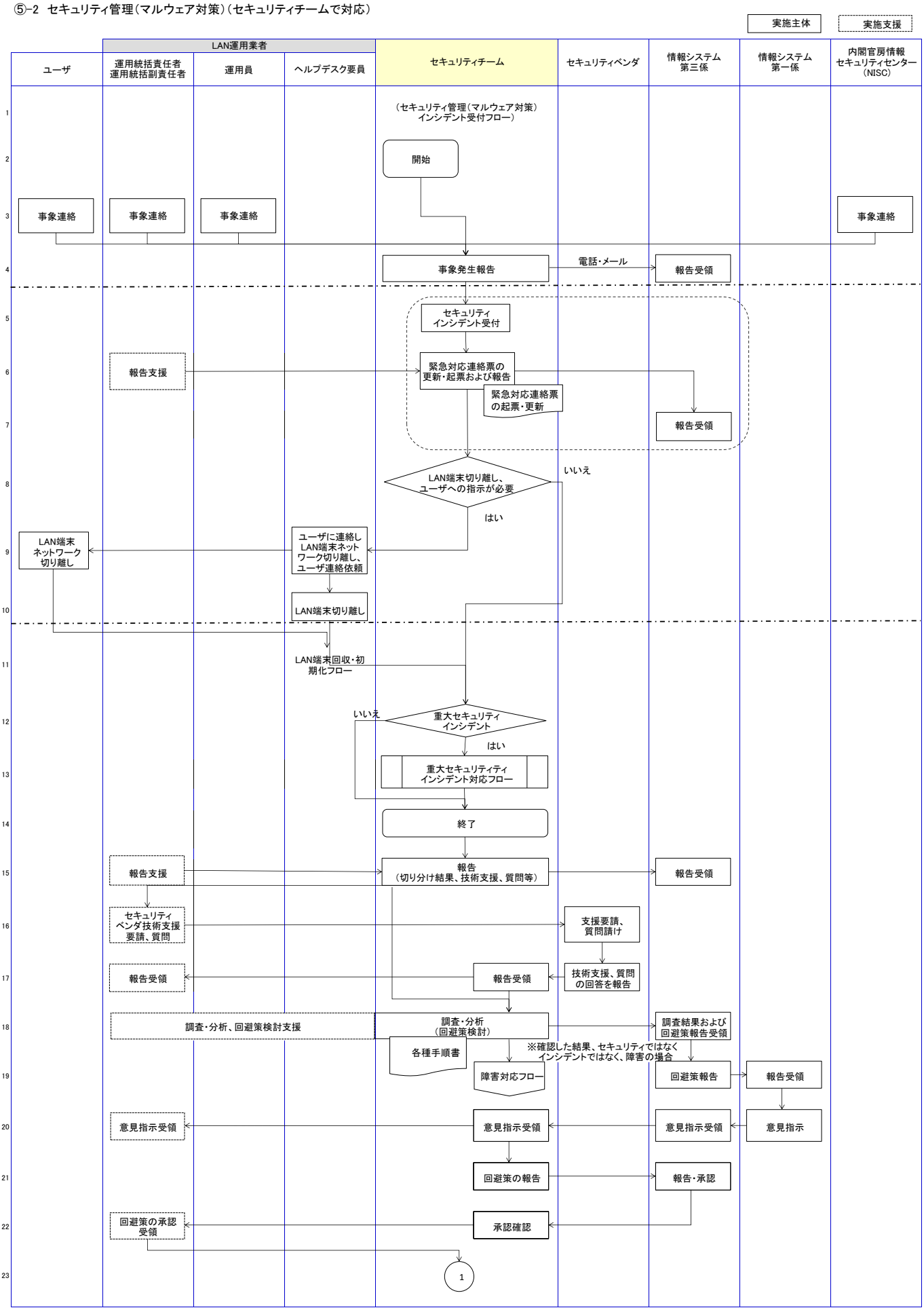
④ ネットワーク管理（ハードウェア障害を除く）

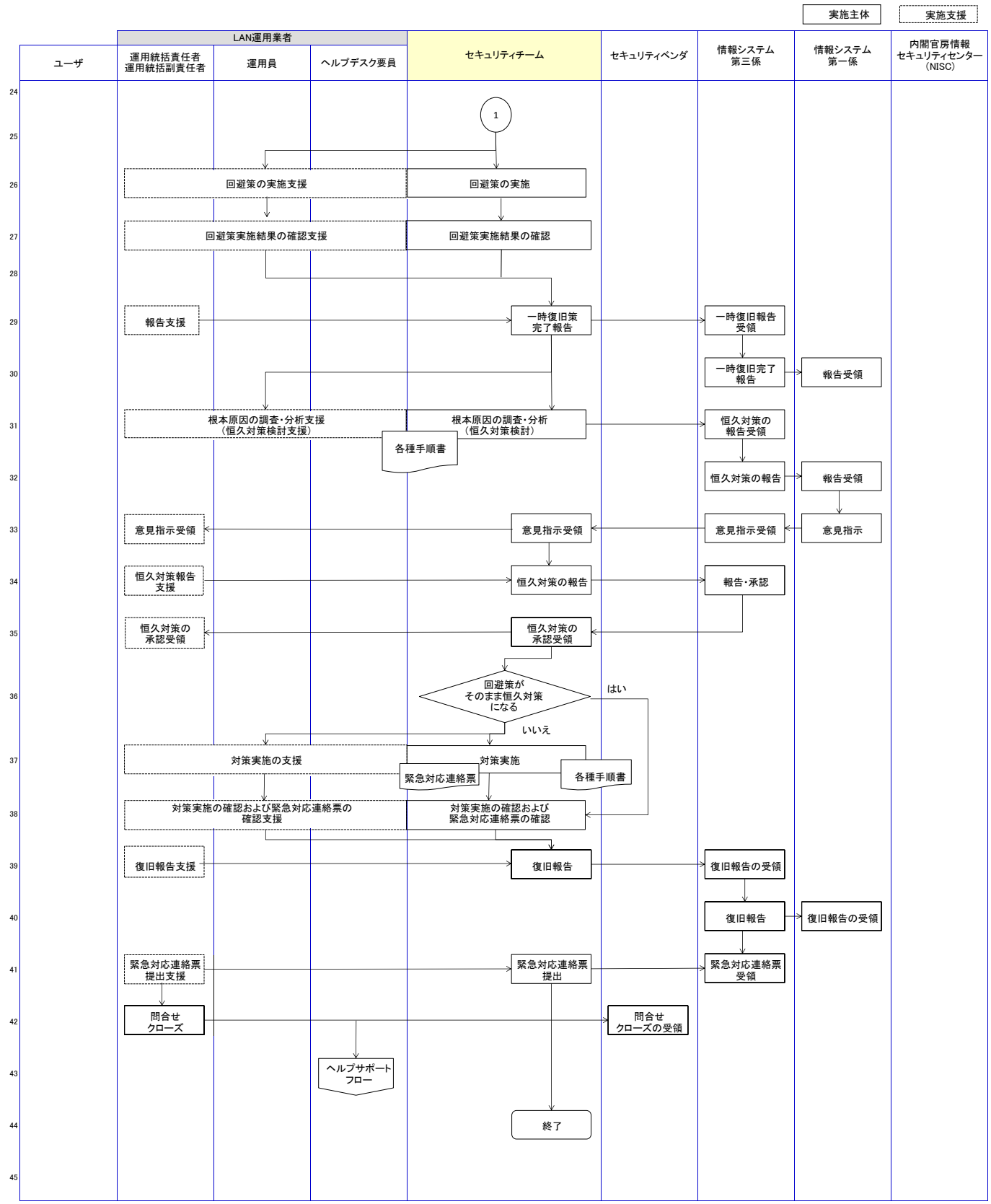


⑤-1 セキュリティ管理（マルウェア対策）インシデント受付フロー

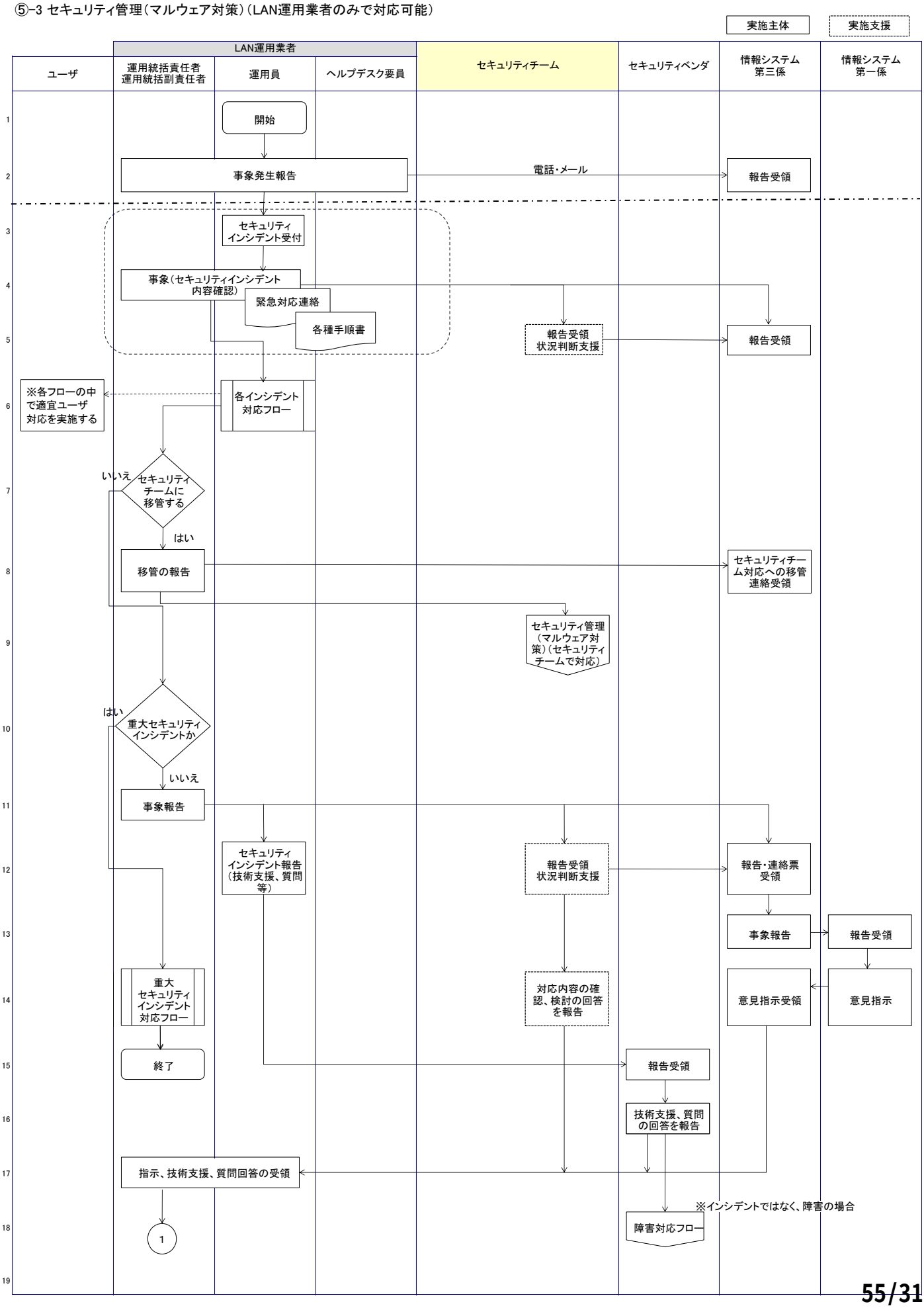


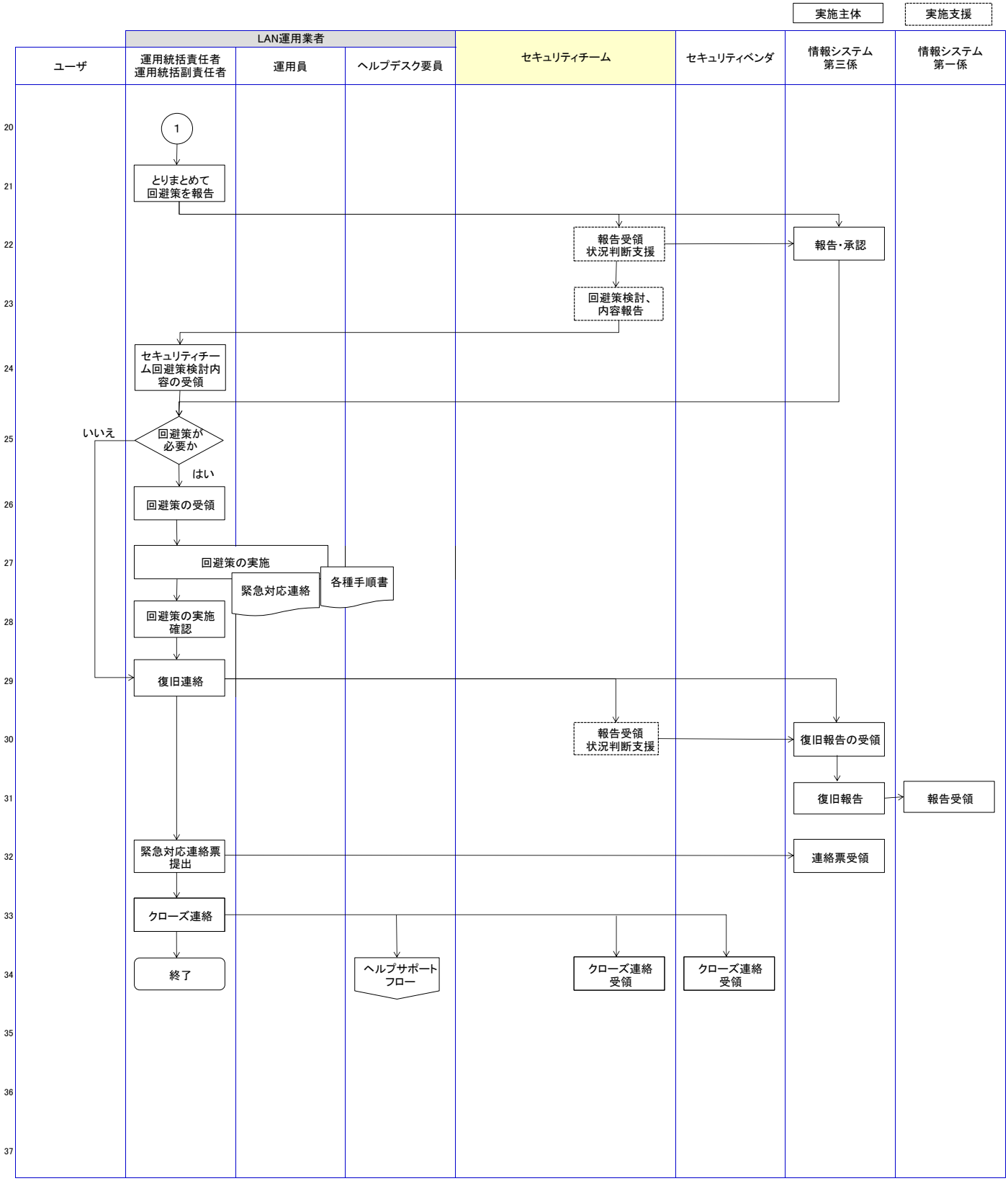
⑤-2 セキュリティ管理（マルウェア対策）（セキュリティチームで対応）



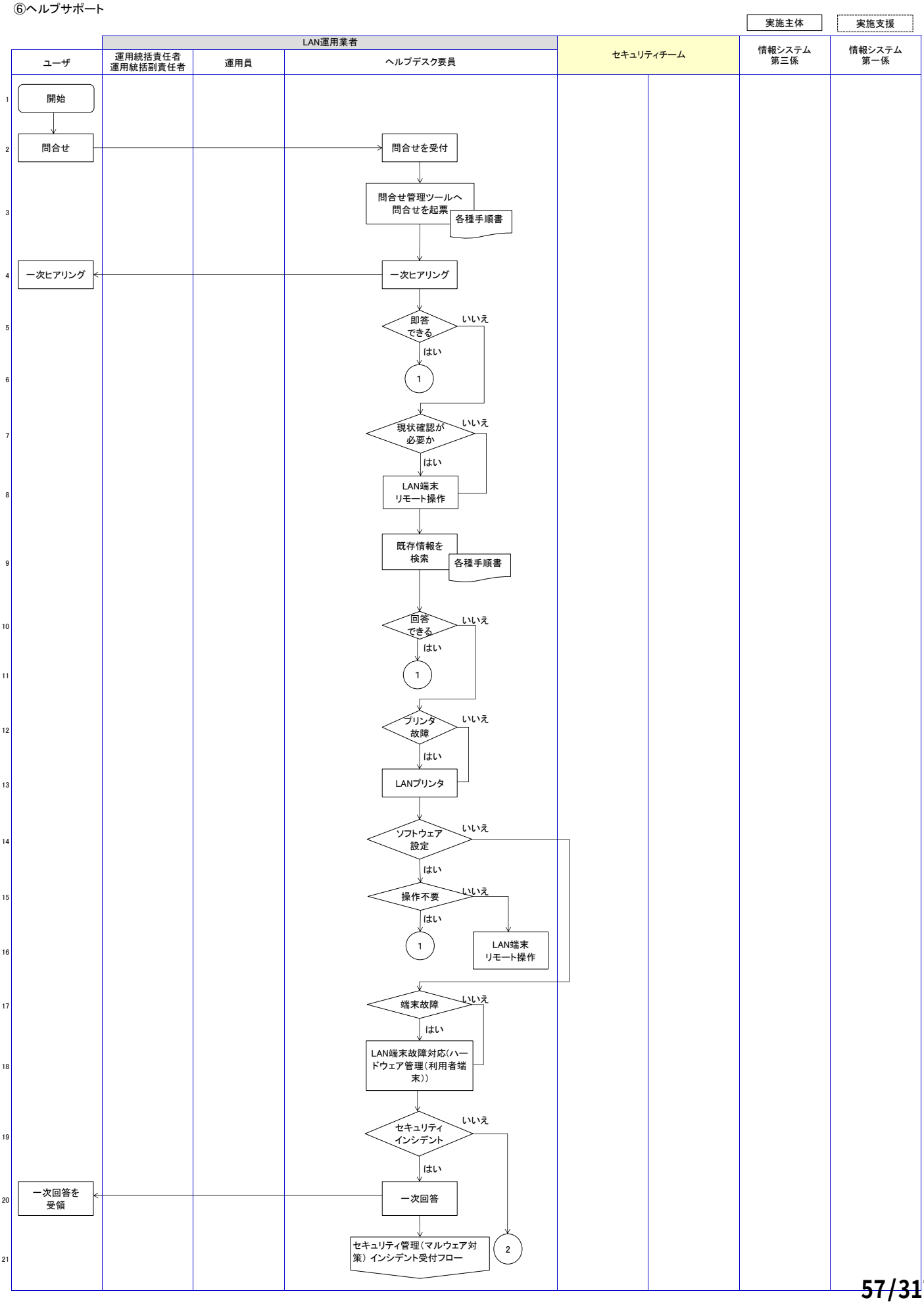

実施主体
実施支援
LAN運用業者
ユーザ
運用統括責任者
運用統括副責任者
運用員
ヘルプデスク要員
セキュリティチーム
セキュリティベンダ
情報システム
第三係
情報システム
第一係
内閣官房情報
セキュリティセンター
（NISC）
1
回避策の実施支援
回避策の実施
回避策実施結果の確認支援
回避策実施結果の確認
報告支援
一時復旧策
完了報告
一時復旧報告
受領
一時復旧完了
報告
報告受領
根本原因の調査・分析支援
（恒久対策検討支援）
根本原因の調査・分析
（恒久対策検討）
各種手順書
恒久対策の
報告受領
恒久対策の報告
報告受領
意見指示受領
意見指示受領
意見指示受領
意見指示
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

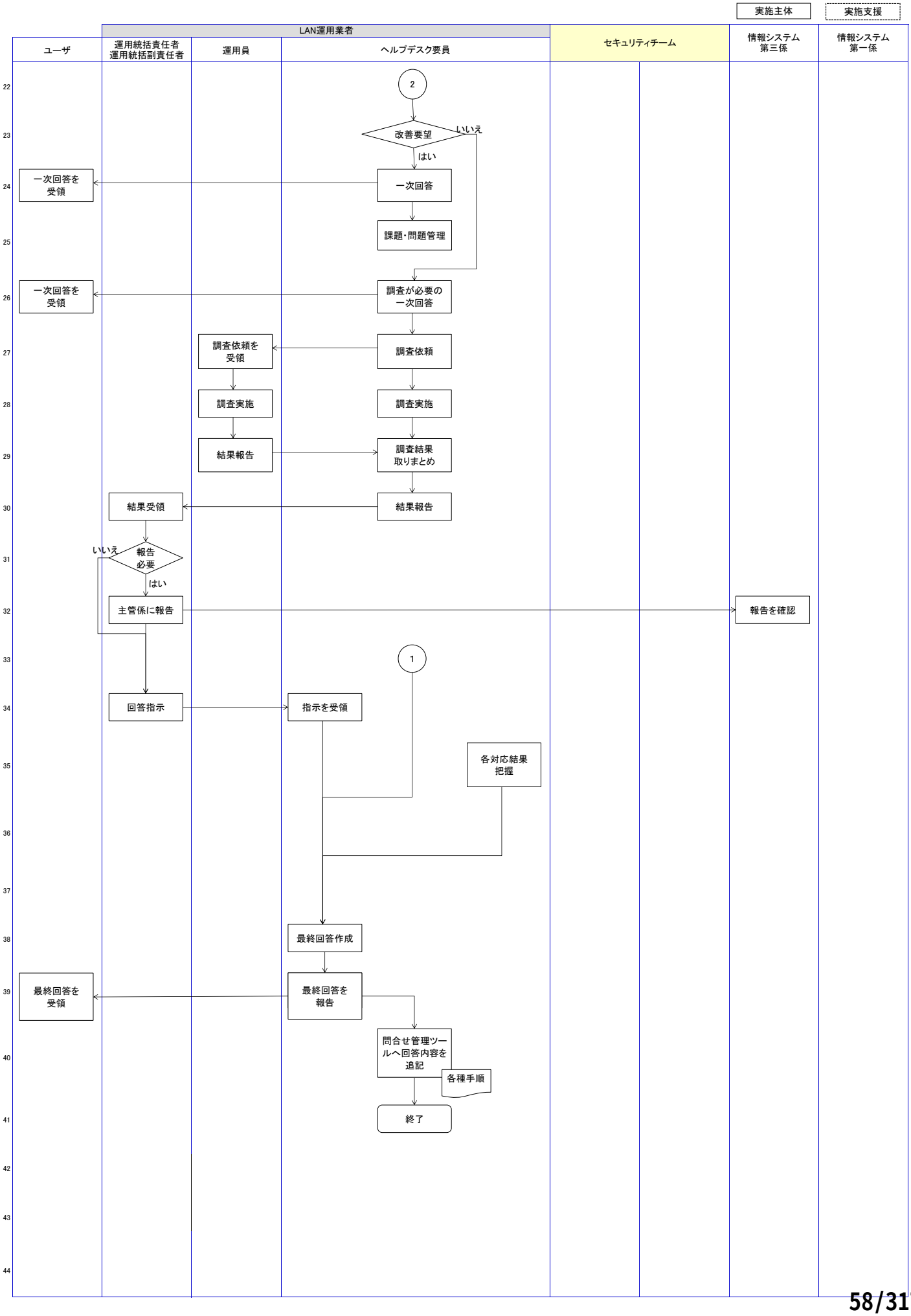
⑤-3 セキュリティ管理（マルウェア対策）（LAN運用業者のみで対応可能）



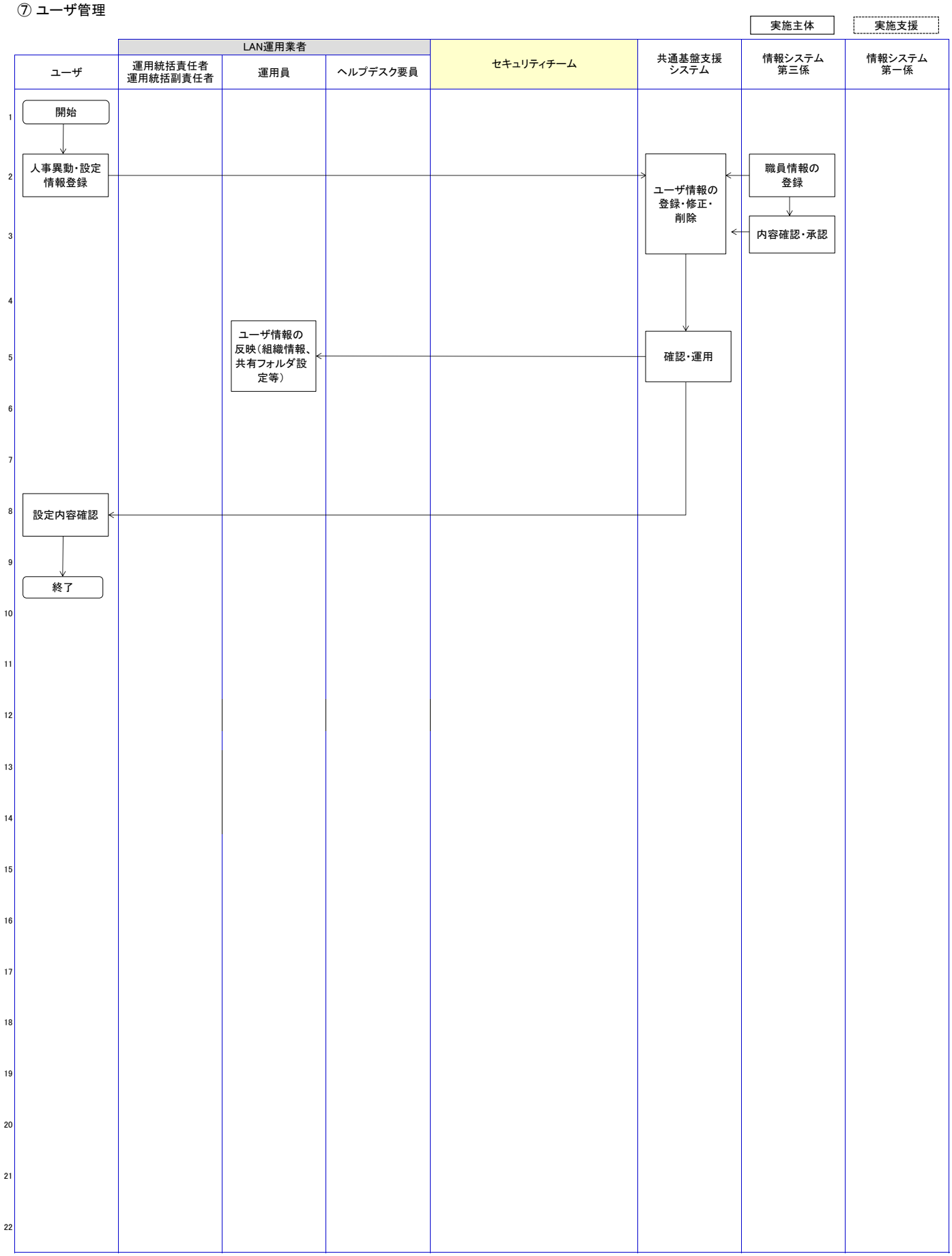

実施主体
実施支援
LAN運用業者
ユーザ
運用統括責任者
運用統括副責任者
運用員
ヘルプデスク要員
セキュリティチーム
セキュリティベンダ
情報システム
第三係
情報システム
第一係
1
とりまとめて
回避策を報告
報告受領
状況判断支援
報告・承認
回避策検討、
内容報告
セキュリティチー
ム回避策検討内
容の受領
いいえ
回避策が
必要か
はい
回避策の受領
回避策の実施
緊急対応連絡
各種手順書
回避策の実施
確認
復旧連絡
報告受領
状況判断支援
復旧報告の受領
復旧報告
報告受領
緊急対応連絡票
提出
連絡票受領
クローズ連絡
終了
ヘルプサポート
フロー
クローズ連絡
受領
ク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

⑥ヘルプサポート

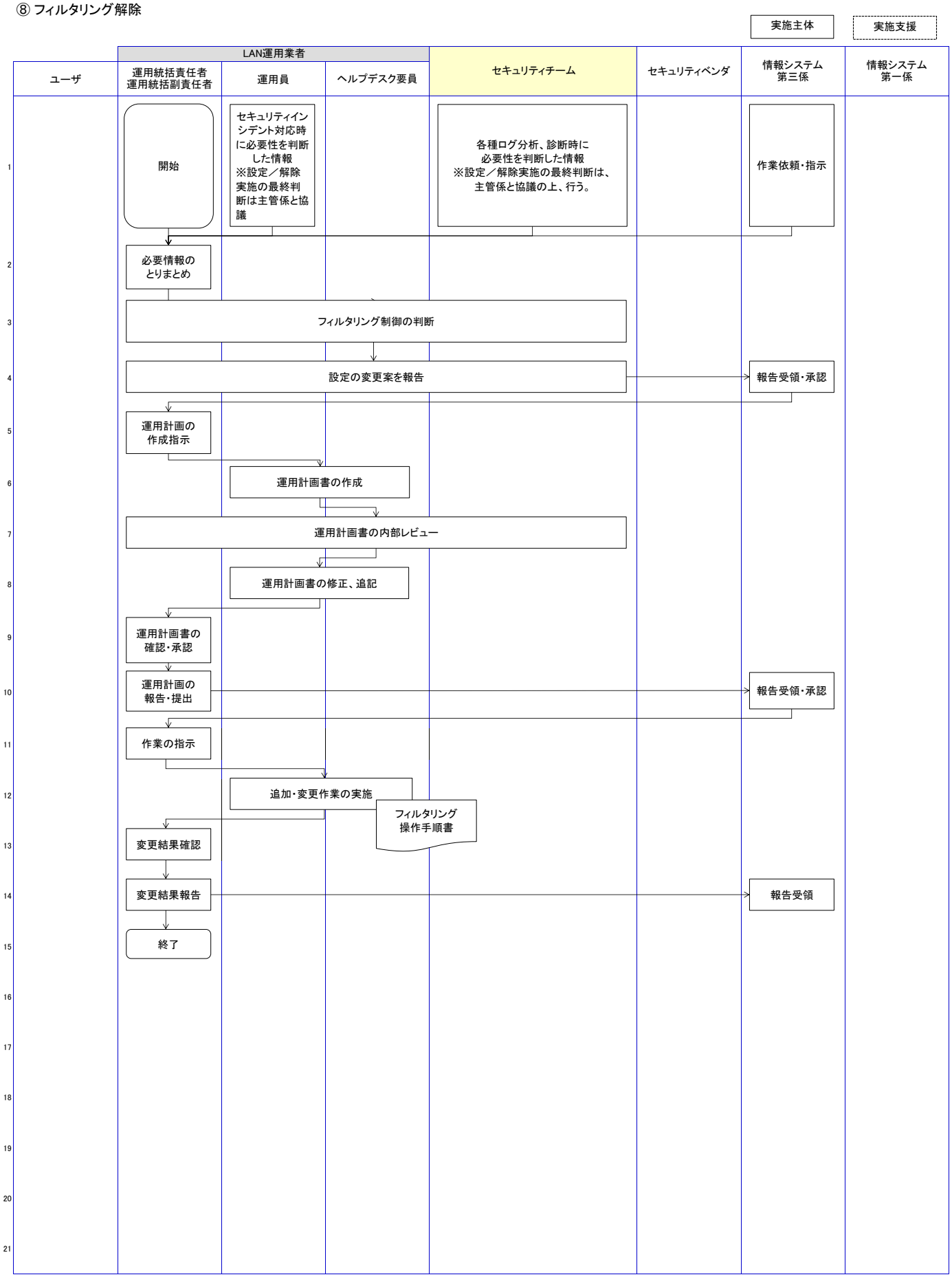

実施主体
実施支援
LAN運用業者
ユーザ
運用統括責任者
運用統括副責任者
運用員
ヘルプデスク要員
セキュリティチーム
情報システム
第三係
情報システム
第一係
開始
問合せ
問合せを受付
問合せ管理ツールへ
問合せを起票
各種手順書
一次ヒアリング
一次ヒアリング
即答
できる
いいえ
はい
1
現状確認が
必要か
いいえ
はい
LAN端末
リモート操作
既存情報を
検索
各種手順書
回答
できる
いいえ
はい
1
プリンタ
故障
いいえ
はい
LANプリンタ
ソフトウェア
設定
いいえ
はい
操作不要
いいえ
はい
1
LAN端末
リモート操作
端末故障
いいえ
はい
LAN端末故障対応(ハードウェア管理(利用者端末))
セキュリティ
インシデント
いいえ
はい
一次回答を
受領
一次回答
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
2


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

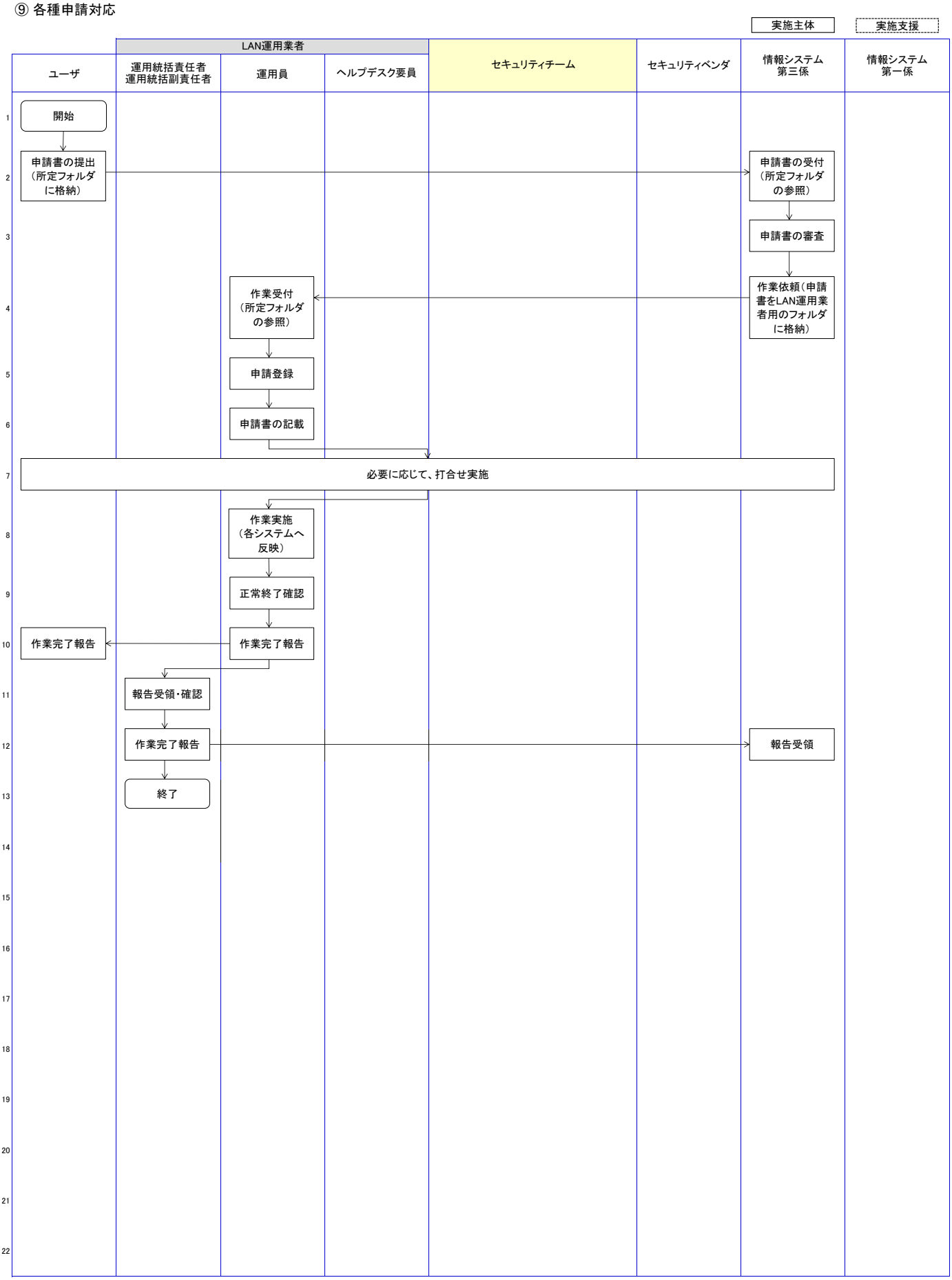
⑦ ユーザ管理


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
ユーザ情報の登録・修正・削除
職員情報の登録
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

⑧ フィルタリング解除


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
セキュリティインシデント対応時に必要性を判断した情報
※設定／解除実施の最終判断は主管係と協議
各種ログ分析、診断時に必要性を判断した情報
※設定／解除実施の最終判断は、主管係と協議の上、行う。
作業依頼・指示
必要情報のとりまとめ
フィルタリング制御の判断
設定の変更案を報告
報告受領・承認
運用計画の作成指示
運用計画書の作成
運用計画書の内部レビュー
運用計画書の修正、追記
運用計画書の確認・承認
運用計画の報告・提出
報告受領・承認
作業の指示
追加・変更作業の実施
フィルタリング操作手順書
変更結果確認
変更結果報告
報告受領
終了

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

総務省の組織

総　務　大　臣

総務副大臣(2)　総務大臣 政務官(3)　総務大臣補佐官

総務事務次官　　総務審議官(3)

施設等機関

自治大学校
情報通信政策研究所
統計研究研修所

特別の機関

中央選挙管理会
政治資金適正化委員会
[自治紛争処理委員]
※事件ごとに総務大臣が任命

審議会等

・地方財政審議会
・行政不服審査会
・情報公開・個人情報保護審査会
・官民競争入札等監理委員会
・独立行政法人評価制度委員会
・国地方係争処理委員会
・電気通信紛争処理委員会
・電波監理審議会
・統計委員会
・恩給審査会
・政策評価審議会
・情報通信審議会
・情報通信行政・郵政行政審議会
・国立研究開発法人審議会

地方支分部局

管区行政評価局(7)
四国行政評価支局
沖縄行政評価事務所
総合通信局(10)
沖縄総合通信事務所

（外局）

大臣官房

- 官房長
- 総括審議官(3)
- 政策立案総括審議官
- 公文書監理官
- サイバーセキュリティ情報化審議官
- 地域力創造審議官
- 審議官(14)
- 参事官(9)

秘書課
総務課
会計課（※１）
企画課（※２）
政策評価広報課
参事官

行政管理局

- 局長

企画調整課
行政情報システム企画課
管理官(10)

行政評価局

- 局長

総務課
企画課
政策評価課
行政相談企画課
行政相談管理官
評価監視官(7)

自治行政局

- 局長

行政課
住民制度課
市町村課
地域力創造グループ
地域政策課
地域自立応援課
公務員部
- 部長

公務員課
福利課
選挙部
- 部長

選挙課
管理課
政治資金課

自治財政局

- 局長

財政課
調整課
交付税課
地方債課
公営企業課
財務調査課

自治税務局

- 局長

企画課
都道府県税課
市町村税課
固定資産税課

国際戦略局

- 局長
- 次長

総務課
技術政策課
通信規格課
宇宙通信政策課
国際政策課
国際経済課
国際協力課

情報流通行政局

- 局長

総務課
情報通信政策課
情報流通振興課
情報通信作品振興課
地域通信振興課
放送政策課
放送技術課
地上放送課
衛星・地域放送課
参事官
郵政行政部
- 部長

企画課
郵便課
貯金保険課
信書便事業課

総合通信基盤局

- 局長

総務課
電気通信事業部
- 部長

事業政策課
料金サービス課
データ通信課
電気通信技術システム課
消費者行政第一課
消費者行政第二課
電波部
- 部長

電波政策課
基幹・衛星移動通信課
移動通信課
電波環境課

統計局

- 局長

総務課
事業所情報管理課
統計情報利用推進課
統計情報システム管理官
統計調査部
- 部長

調査企画課
国勢統計課
経済統計課
消費統計課

政策統括官

- 統計企画管理官
- 統計審査官(3)
- 国際統計管理官
- 恩給企画管理官
- 恩給業務管理官

サイバーセキュリティ統括官

参事官(3)

公害等調整委員会

- 委員長
- 委員(6)
- 事務局長
- 次長

総務課
審査官(9)

消防庁

- 長官
- 次長
- 審議官

総務課
消防・救急課
予防課
国民保護・防災部
- 部長

防災課
参事官(3)

施設等機関
消防大学校

審議会等
消防審議会

（※１）入札手続実施部門
（※２）担当部門

（注）組織図は政令以上で規定される主要組織のみを示している。(平成31年4月現在)

別紙４

総務省ＬＡＮシステムの更新整備
及び
保守・運用業務の請負
総合評価基準書

総務省大臣官房企画課サイバーセキュリティ・情報化推進室

- 目　次 -

1　はじめに

本書は「総務省ＬＡＮシステムの更新整備及び保守・運用業務の請負」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 ＝ １：３

総合評価点 ＝ 価格点（1,000 点満点） ＋ 技術点（3,000 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）×1,000 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４－２「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（300 点）＋加点（2,700 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ＬＡＮシステムの更新整備及び保守・運用業務の請負　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４－１　機能証明書」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４－２　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４－１　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４－２　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４－２　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４－２　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８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、該当部分の説明は各担当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

令和２年８月３日（月）午後５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６部（うち社名・ロゴ等をマスキングしたものを４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ＬＡＮシステムの更新整備及び保守・運用の請負　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サイバーセキュリティ・情報化推進室第三係

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「機能要件詳細」から別紙１－6「本省・DRサイト稼働サービス一覧」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」欄に〇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「300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。具体的に示された提案内容が要件を満たした上で、「評価ポイント」について客観的かつ合理的に示されていると評価できる場合は、加点する。

・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。

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
第１　調達案件の概要に関する事項	〇	〇		理解かつ適合していることを具体的に示すこと。 【加点項目】 ・作業スケジュールが、次期総務省LANの運用開始に向けて現実的で実現性の高いものとなっていること。また、総務省のスケジュールを考慮し、効率的なものであること。
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	〇	－		理解かつ適合していることを具体的に示すこと。
第３　満たすべき情報システムに求める要件に関する事項	〇	－		理解かつ適合していることを具体的に示すこと。
第４　作業の実施内容に関する事項	〇	〇		理解かつ適合していることを具体的に示すこと。 【加点項目】 ・作業内容が週次単位で分解され、各作業間の依存関係を明らかにし、簡潔明瞭に示されていること。 ・第二次工程レビュー及び第三次工程レビューを効果的かつ効率的に行う方法が示されていること。 ・成果物全体の文書体系を明らかにし、仕様書及び要件定義書に記載の要件と成果物の記載場所（想定）との関係が、簡潔明瞭に示されていること。 ・各成果物の構成が、保守・運用期間中の更新等を見越して、品質管理方法とともに示されていること。

別紙2　総合評価基準及び対応表

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
調達仕様書	第５　作業の実施体制・方法に関する事項	○	○	250	理解かつ適合していることを具体的に示すこと。 【加点項目】 ・作業実施体制は、大規模で複雑な総務省LANを再構築するために十分な実績・知識・技能・資格を有した業務従事者が参画し、適正な要員数で編成されていること。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。 ・プロジェクトの統括責任者及び作業リーダーは、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こと。 ・作業管理に当たっては、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、実践的で効果的なプロジェクト管理であること。なお、プロジェクト管理手法は、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。
	第１　業務要件	○	－	－	理解かつ適合していることを具体的に示すこと。
	第２　機能要件	○	－	－	理解かつ適合していることを具体的に示すこと。
	第３　非機能要件	－	－	－	
	1 ユーザビリティ及びアクセシビリティに関する事項	○	－	－	理解かつ適合していることを具体的に示すこと。
	2 システム方式に関する事項	○	－	－	理解かつ適合していることを具体的に示すこと。
	3 規模に関する事項	○	－	－	理解かつ適合していることを具体的に示すこと。
	4 性能に関する事項	○	○	150	理解かつ適合していることを具体的に示すこと。 【加点項目】 ・次期総務省LANの性能に係る考え方（目的及び方法）を明らかにした上で、当該性能の維持・向上のための施策が示されていること。
	5 信頼性に関する事項	○	○	150	理解かつ適合していることを具体的に示すこと。 【加点項目】 ・次期総務省LANの信頼性に係る考え方（目的及び方法）を明らかにした上で、当該信頼性の具体的な維持・向上のための施策が示されていること。

別紙2　総合評価基準及び対応表

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
【別紙1】要件定義書		6 拡張性に関する事項	○	○	60	理解かつ適合していることを具体的に示すこと。 【加点項目】 ・次期総務省LANの拡張性に係る考え方（目的及び方法）を明らかにした上で、当該拡張性の実現のための具体的な施策が示されていること。
		7 上位互換性に関する事項	○	○	60	理解かつ適合していることを具体的に示すこと。 【加点項目】 ・次期総務省LANの上位互換性に係る考え方（目的及び方法）を明らかにした上で、当該上位互換性の実現のための施策が示されていること。
		8 中立性に関する事項	○	－	－	理解かつ適合していることを具体的に示すこと。
		9 継続性に関する事項	○	○	150	理解かつ適合していることを具体的に示すこと。 【加点項目】 ・次期総務省LANの継続性に係る考え方（目的及び方法）を明らかにした上で、当該継続性の実現のための施策が示されていること。
		10 情報セキュリティに関する事項	○	－	－	理解かつ適合していることを具体的に示すこと。
		11 情報システム稼働環境に関する事項	○	－	－	理解かつ適合していることを具体的に示すこと。
		12 テストに関する事項	○	○	240	理解かつ適合していることを具体的に示すこと。 【加点項目】 ・次期総務省LANのテストに係る考え方（目的及び方法）が簡潔明瞭に示され、かつ、その予想効果が指標を用いて示されていること。
		13 移行に関する事項	○	○	240	理解かつ適合していることを具体的に示すこと。 【加点項目】 ・次期総務省LANの移行に係る考え方（目的及び方法）が簡潔明瞭に示され、かつ、その予想効果が指標を用いて示されていること。
		14 引継ぎに関する事項	○	－	－	理解かつ適合していることを具体的に示すこと。
		15 教育に関する事項	○	－	－	理解かつ適合していることを具体的に示すこと。
		16 運用に関する事項	○	○	240	理解かつ適合していることを具体的に示すこと。 【加点項目】 ・次期総務省LANの運用に係る考え方（目的及び方法）が簡潔明瞭に示され、かつ、その予想効果が指標を用いて示されていること。
		17 保守に関する事項	○	○	240	理解かつ適合していることを具体的に示すこと。 【加点項目】 ・次期総務省LANの保守に係る考え方（目的及び方法）が簡潔明瞭に示され、かつ、その予想効果が指標を用いて示されていること。
	第４　添付資料		－	－	－	

別紙2　総合評価基準及び対応表

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
【別紙1－1】機能要件詳細	第１　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。
	第２　総務省LANサービス	○	○	240	理解かつ適合していることを具体的に示すこと。 【加点項目】 ・利用者の生産性・利便性が必須要件又は現行システムより向上する提案であることが、指標を用いて示されていること。 ・次期総務省LANから提供を開始する新サービス及び新機能について、職員への利用促進や利便性向上を目的とした具体的なサービス提供方法が言及された提案であること。
	第３　サービス基盤	○	○	240	理解かつ適合していることを具体的に示すこと。 【加点項目】 ・認証サービスを中心とした他サービスとの連携及びシングルサインオンを実現する構成及び実現方法が具体的かつ図表等を用いて簡潔明瞭に示されている場合は加点する。併せて、アカウント情報を安全かつ適切に管理する方法も示されていること。 ・テレワークサービス・私物等端末リモートアクセスサービスの構成及び利用方法が具体的かつ図表等を用いて簡潔明瞭に示されていること。 ・セキュリティに十分に配慮するとともに、利用者の生産性・利便性・信頼性が必須要件より向上することが、指標を用いて示されていること。
	第４　ネットワーク基盤	○	○	150	理解かつ適合していることを具体的に示すこと。 【加点項目】 ・職員の総務省LAN利用における生産性や利便性の更なる向上のために、ネットワーク基盤での工夫された提案又は必須要件を上回る提案であることが、指標を用いて示されていること。 ・高い信頼性と可用性が確保できている構成の提案であることが、指標を用いて示されていること。
	第５　セキュリティサービス	○	○	240	理解かつ適合していることを具体的に示すこと。 【加点項目】 ・セキュリティ対策が必須要件より向上する提案であるとともに、利用者の利便性や次期総務省LANの信頼性を損なうことのない提案であることが、指標を用いて示されていること。
	第６　運用サービス	○	－	－	理解かつ適合していることを具体的に示すこと。
	第７　その他機器基盤	○	－	－	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】ルータ・スイッチ要件一覧		○	－	－	理解かつ適合していることを具体的に示すこと。
【別紙1-3】回線一覧		○	－	－	理解かつ適合していることを具体的に示すこと。
【別紙1-4】情報セキュリティ要件詳細		○	－	－	理解かつ適合していることを具体的に示すこと。
【別紙1-5】保守・運用要件詳細		○	－	－	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

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
【別紙1-6】本省・DRサイト稼働サービス一覧	○	－	－	理解かつ適合していることを具体的に示すこと。
ワーク・ライフ・バランス等の推進	－	○	50	理解かつ適合していることを具体的に示すこと。 【加点項目】 （複数の認定等に該当する場合は、最も配点が高い区分により加点を行う。） ・女性の職業生活における活躍の推進に関する法律（平成27年法律第64号）（女性活躍推進法）に基づく認定（えるぼし認定）を受けている場合、段階によって加点する。 １段階目（*1）15点 ２段階目（*1）35点 ３段階目　　50点 *1 労働時間等の働き方に係る基準は満たすこと。 ・女性の職業生活における活躍の推進に関する法律（平成27年法律第64号）（女性活躍推進法）に基づく行動計画を策定済みの場合、加点する。 行動計画（*2）10点 *2 女性活躍推進法に基づく一般事業主行動計画の策定義務がない事業主（常時雇用する労働者の数が300人以下のもの）に限る（計画期間が満了していない行動計画を策定している場合のみ） ・次世代育成支援対策推進法（平成15年法律第120号）（次世代法）に基づく認定（くるみん認定企業、プラチナくるみん認定企業）を受けている場合、加点する。 （くるみん認定企業・プラチナ認定企業） くるみん（旧基準）（*3）15点 くるみん（新基準）（*4）35点 プラチナくるみん　　50点 *3 旧くるみん認定マーク（次世代育成支援対策推進法施行規則等の一部を改する省令（平成29年厚生労働省令31号）による改正前の認定基準又は同附則第２条第３項の規定による経過措置により認定）。 *4 新くるみん認定マーク（次世代育成支援対策推進法施行規則等の一部を改正する省令（平成29年厚生労働省令31号）による改正後の認定基準により認定）。 ・青少年の雇用の促進等に関する法律（昭和45年法律第98号）（若者雇用促進法）に基づく認定を受けている場合、加点する。 ユースエール認定　50点
		加点合計	2700	

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保守・運用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。

令和　　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保守・運用業務

民間競争入札実施要項

別紙６　資料閲覧要領

総務省大臣官房企画課サイバーセキュリティ・情報化推進室

【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ＬＡＮシステムの更新整備及び保守・運用業務」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サイバーセキュリティ・情報化推進室内

(２)閲覧期間及び時間

第１回目　令和２年３月 16～23 日　10 時～17 時
第２回目　令和２年６月中～下旬　　10 時～17 時

(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サイバーセキュリティ・情報化推進室第三係
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表。	○	○

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 30 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

令和　　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ＬＡＮシステムの更新整備及び保守・運用業務

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						

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。

総務省 LAN システムの
更新整備及び保守・運用業務の請負
調達仕様書

総務省大臣官房企画課サイバーセキュリティ・情報化推進室

― 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 LAN システムの更新整備及び保守・運用業務の請負

(A LAN system construction, operation and maintenance for Ministry of Internal Affairs and Communications)

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、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 つの LAN）するなど、最適化に取り組んできた。

また、総務省 LAN は、第 3 期システムより「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（以下「市場化テスト」という。）の対象事業として選定されており、第 4 期システムである現行総務省 LAN の事業評価案の審議の結果、第 5 期システムである次期総務省 LAN においても引き続き市場化テストの対象とされることとなった。次期総務省 LAN においては、市場化テストの基本理念の実現に向け、従来一括調達してきたものを、「総務省 LAN に係る更新整備及び保守・運用業務」（以下「本調達」又は「更新整備及び保守・運用業務」という。）及び「総務省 LAN に係る運用管理及び受付窓口業務」（以下「運用管理及び受付窓口業務」という。）として分離調達することとした。

本調達に際しては、「デジタル・ガバメント実行計画」（令和元年 12 月 20 日改定閣議決定）、「デジタル・ガバメント推進標準ガイドライン」（令和 2 年 3 月 31 日最終改定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。）、「政府機関等の情報セキュリティ対策のための統一基準群（平成 30 年度版）」（平成 30 年 7 月 25 日サイバーセキュリティ戦略本部）（以下「統一基準群」という。）等の政府方針やガイドラインに沿って検討を行った結果、次期総務省 LAN を令和 3 年 10 月より運用開始することとした。

3　目的及び期待する効果

本調達では、総務省 LAN の基盤システムとしての重要性を踏まえ、安定性と信頼性の更なる向上を図り、併せて、高度に複雑化するサイバー攻撃への情報セキュリティ対策を強化し、安全・安心な基盤システムの実現を目的とする。

時間や場所にとらわれない円滑なコミュニケーション手段を安全に提供し、業務処理の電子化・共通化、職員の多様で柔軟な働き方などの推進によって、公務における働き方改革の実現に資するものとする。

4　用語の定義

本調達仕様書において使用する用語を別紙 8「用語の定義」に示す。

5　業務・情報システムの概要

(1)　次期総務省 LAN の概要

総務省 LAN の概要図について、図 1-1 に示す。

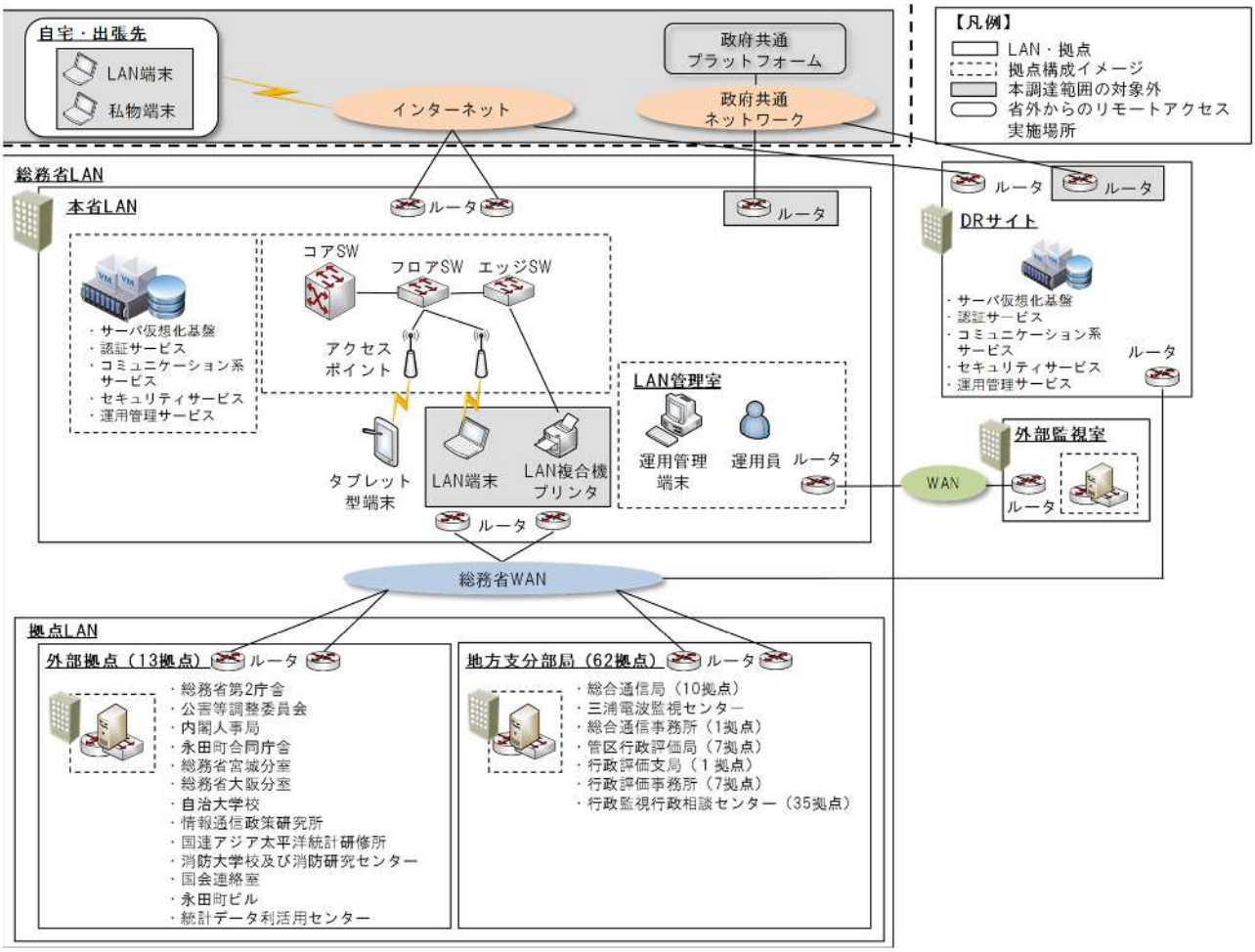


図 1-1　総務省 LAN システム概要図

(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　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。

オ　DR サイト

DR サイトは、本省において大規模な災害や障害等が発生した際に、本省 LAN の提供する一部サービスを代替して提供する拠点を指す。

(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表 1-1 に示す。

表 1-1　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		
	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を提供する。ポータルサイトは、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、電子掲示板機能、アンケート機能、会議室予約機能、スケジューラ（予定表）機能、設備予約機能、自動応答機能を提供する。
	ファイル共有サービス	総務省職員間が業務情報である電子データを保存・共有するため、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、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、大容量ファイル転送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。
	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。
	プリントサービス	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。
	インターネット閲覧サービス	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環境として、インターネット閲覧サービスを提供する。

機能等の名称		機能等の概要
	機密情報保護サービス	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、機密情報保護サービスを提供する。
2. サービス基盤		
	認証サービス	総務省職員等のアカウント情報を管理し、各サービスへの接続時に認証及びアクセス権の付与、証明書の発行・配布やライセンス認証等を行う。
	テレワークサービス	省外から LAN 端末を用いて、本省で利用する場合と同等のサービス・機能を利用できるリモートアクセス機能を提供する。省外から支給端末（Windows タブレット）及び私物端末（PC・モバイル）を用いて、本省内で LAN 端末を利用する場合と同等のサービス・機能を利用できる仮想デスクトップ機能を提供する。
	私物等端末リモートアクセスサービス	省外から私物等端末（モバイル）を用いて、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を利用できる環境を提供する。
	デバイス管理サービス	ペーパーレス会議サービスで利用するタブレット型端末及び省外で利用する支給端末（Windows タブレット）のハードウェア情報・ソフトウェア情報等の収集、ソフトウェア・プロファイルの配布等を行う。また、端末の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。
	資源管理サービス	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収集や、ソフトウェア（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。
	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し、情報の不正出力を防止する環境を提供する。
3. ネットワーク基盤		
	本省 LAN	本省 LAN は、総務省職員が総務省 LAN サービスを利用するため、また、本省内に設置するサーバや、業務システム及び政府共通ネットワークと接続するためのネットワークを提供する。
	DR サイト LAN	DR サイト LAN は、DR サイト内に設置するサーバや政府共通ネットワークと接続するためのネットワークを提供する。
	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のネットワークを提供する。
	総務省 WAN	総務省 WAN は、総務省職員が総務省 LAN サービスを利用するため、本省、各地方拠点及び DR サイトを相互に接続するためのネットワークを提供する。
	外部監視室接続ネットワーク	外部から総務省 LAN を 24 時間 365 日監視するため、本省及び DR サイトと外部監視室を独立した閉域網で接続する。
	インターネット接続ネットワーク	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を本省及び DR サイトにて提供する。
	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。
	無線 LAN 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、LAN 端末に無線 LAN 接続サービスを提供する。また、ペーパーレス会議サービスのタブレット型端末と情報不正出力防止サービスのウイルスチェック用端末にも無線 LAN 接続サービスを提供する。

機能等の名称	機能等の概要
4. セキュリティサービス	
マルウェア対策（メール）サービス	メールからのマルウェア等の感染を早期に検知･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。
マルウェア対策（サーバ・端末）サービス	サーバ、LAN端末、仮想デスクトップ、ウイルスチェック用端末､運用端末及びファイル共有領域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・端末）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。
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。
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。
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。
5. 運用サービス	
申請管理サービス	受付窓口を通じて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に関するユーザからの支援依頼内容を一元管理し、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。
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。
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、保守・運用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。
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、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。
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。

(4) システム規模

総務省LANは、職員が原則として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端末数及び拠点数の規模については、別紙1「要件定義

書」の「第 3　非機能要件 3 規模に関する事項」を参照すること。

(5)　信頼性等及び情報セキュリティの確保

総務省 LAN は、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ため、安定かつ安全にサービスを提供する必要がある。また、職員が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。）を取り扱うため、適切かつ十分な情報セキュリティ対策を施すこと。

保守・運用においては、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、あらかじめ決められた定型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、本調達における更新整備担当やセキュリティ担当、別途調達される運用管理及び受付窓口業務の担当が一体となって検討・対策を行うなど、高度化・複雑化する新たな攻撃手法に対応すること。

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 1-1「次期総務省 LAN が提供する機能等の概要一覧」に記載の全てのサービス・機能を提供するために必要となるサービス・機能の設計・構築、機器等の借入、保守・運用等を調達の対象範囲とする。

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「保有ライセンス・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、原則として総務省が保有するライセンスを活用すること。

なお、運用管理及び受付窓口業務は別調達とする。

(2)　作業内容

本調達の作業内容については、「第 4 作業の実施内容に関する事項」を参照すること。なお、作業に当たっては、「標準ガイドライン」に基づき、行うこと。

(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、別紙 1「要件定義書」の要件を満たすこと。

7　契約期間

令和 2 年 10 月から令和 7 年 3 月まで

8　作業スケジュール

総務省 LAN の更新整備における全体スケジュール（案）を表 1-2、図 1-2 に示す。なお、作業スケジュールについては主管課と協議の上、最終的な決定をすること。

また、現行総務省 LAN から次期総務省 LAN への移行期間中、本省サーバ室内に両シ

ステムの機器を併設することはラック設置スペース及び電源の制約から困難であるため、省外に次期総務省 LAN の構築拠点を設け、本省サーバ室へ移設を完了するまでの間、保守・運用すること。

表 1-2　全体作業スケジュール（案）

フェーズ	期間（想定）	備考
設計・構築	令和 2 年 10 月～令和 3 年 5 月	
テスト	令和 3 年 4 月～令和 3 年 8 月	
移行	令和 3 年 7 月～令和 3 年 9 月	
稼働	令和 3 年 10 月	構築拠点での稼働を想定
移設	令和 3 年 10 月（要調整）	本省サーバ室での稼働に向けて構築拠点から機器移設を行う
保守・運用	令和 3 年 10 月～令和 7 年 3 月	

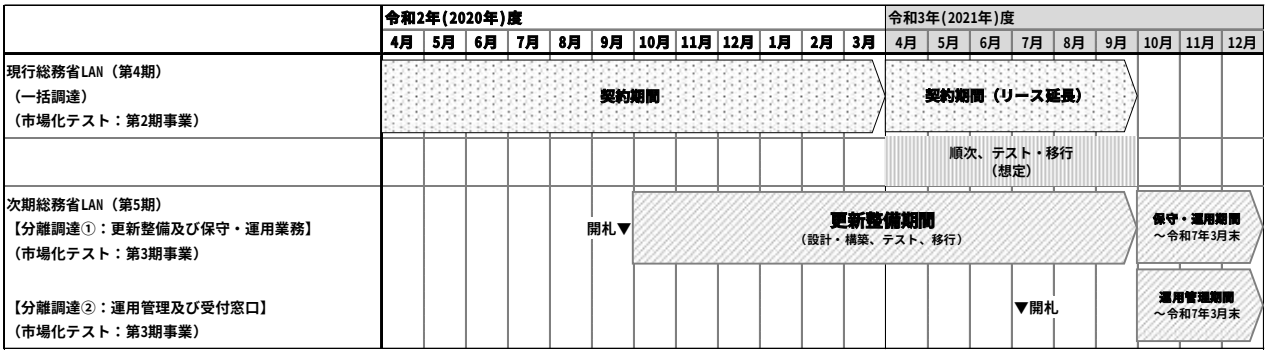


図 1-2　想定スケジュール（案）

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。

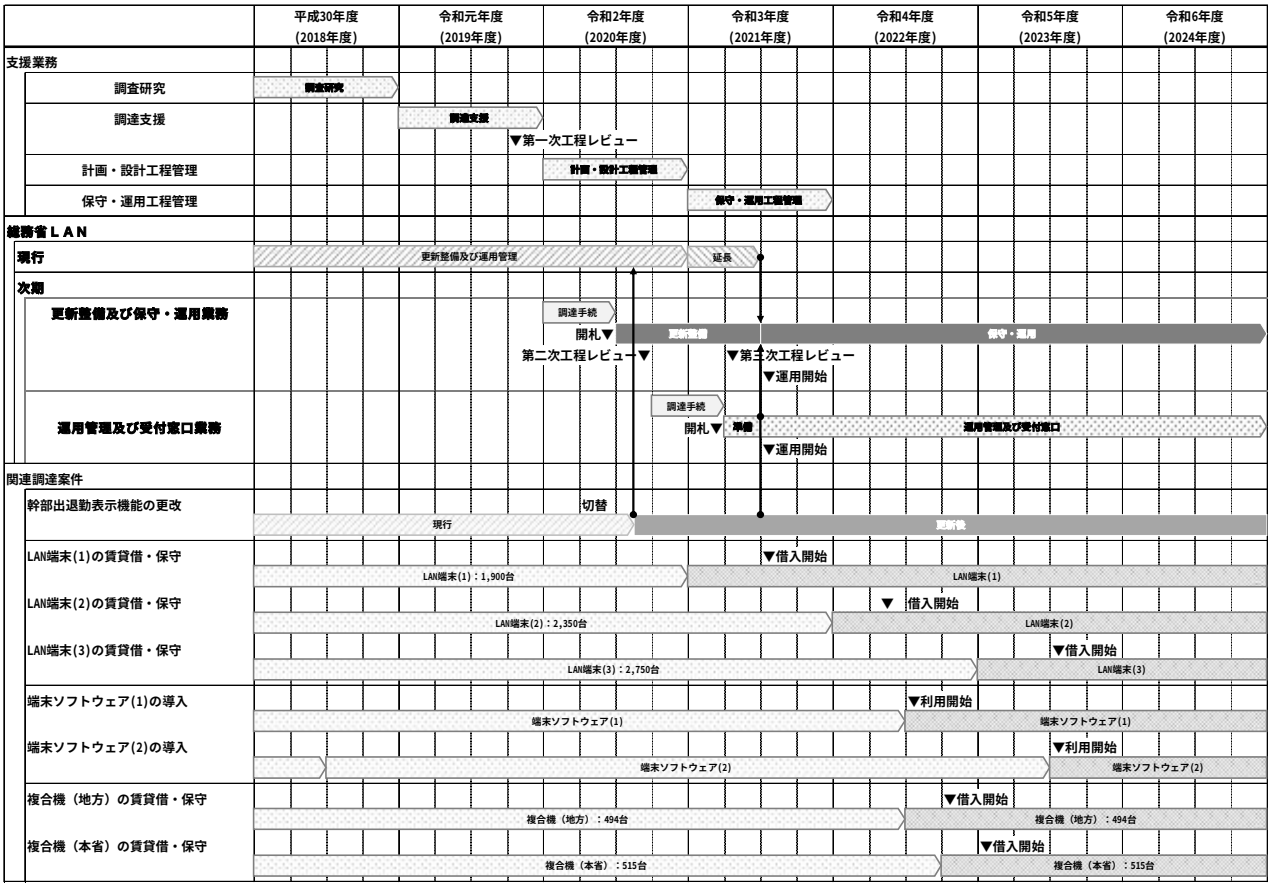


図 2-1　総務省 LAN 全体スケジュール

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	【調査・研究】（平成 30 年度） 次期総務省 LAN のあり方に関する調査研究作業の請負	一般競争入札 （最低価格落札方式）	入札公告：平成 30 年 5 月 14 日 落札者決定：平成 30 年 6 月 21 日
2	【調達支援】（令和元年度） 次期総務省 LAN に係る調達支援業務	一般競争入札 （最低価格落札方式）	入札公告：平成 31 年 1 月 25 日 落札者決定：平成 31 年 3 月 27 日
3	【計画・設計工程管理】（令和 2 年度） 次期総務省 LAN の調達支援及び計画・設計工程管理支援業務	一般競争入札 （最低価格落札方式）	入札公告：令和 2 年 1 月 23 日 落札者決定：令和 2 年 3 月 24 日

4	【保守･運用工程管理】(令和 3 年度) 次期総務省 LAN の調達支援及び構築、保守・運用工程管理業務	一般競争入札 （最低価格落札方式）	入札公告：令和 3 年 1 月頃 落札者決定：令和 3 年 3 月頃
5	**<本調達>** 【更新整備及び保守・運用業務】 総務省 LAN システムの更新整備及び保守・運用業務	一般競争入札 （総合評価落札方式） 市場化テスト対象	意見招請：令和 2 年 3 月 13 日 入札公告：令和 2 年 5 月 29 日 落札者決定：令和 2 年 9 月 7 日
6	【運用管理及び受付窓口業務】 総務省 LAN システムの運用管理及び受付窓口業務	一般競争入札 （総合評価落札方式） 市場化テスト対象	意見招請：令和 2 年 11 月頃 入札公告：令和 3 年 2 月頃 落札者決定：令和 3 年 6 月頃
7	総務省 LAN における幹部出退勤表示機能の更改に係る作業等	未定	入札公告：令和 2 年 7 月頃 落札者決定：令和 2 年 9 月頃
8	LAN 端末(1)の賃貸借・保守 1,900 台	一般競争入札 （総合評価落札方式）	入札公告：令和 3 年 1 月頃 落札者決定：令和 3 年 3 月頃
9	LAN 端末(2)の賃貸借・保守 2,350 台	一般競争入札 （総合評価落札方式）	入札公告：令和 4 年 1 月頃 落札者決定：令和 4 年 3 月頃
10	LAN 端末(3)の賃貸借・保守 2,750 台	一般競争入札 （総合評価落札方式）	入札公告：令和 5 年 2 月頃 落札者決定：令和 5 年 4 月頃
11	端末ソフトウェア(1)の借入	一般競争入札 （最低価格落札方式）	入札公告：令和 4 年 7 月頃 落札者決定：令和 4 年 9 月頃
12	端末ソフトウェア(2)の借入	一般競争入札 （最低価格落札方式）	入札公告：令和 5 年 7 月頃 落札者決定：令和 5 年 9 月頃
13	複合機（地方）の賃貸借・保守 494 台	一般競争入札 （総合評価落札方式）	入札公告：令和 4 年 6 月頃 落札者決定：令和 4 年 8 月頃
14	複合機（本省）の賃貸借・保守 515 台	一般競争入札 （総合評価落札方式）	入札公告：令和 4 年 9 月頃 落札者決定：令和 4 年 11 月頃

2　調達案件間の入札制限

相互牽制の観点から、表 2-1「No.2 調達支援」･「No.3 計画・設計工程管理」･「No.4 保守・運用工程管理」と「No.5 更新整備及び保守・運用業務」･「No.6 運用管理及び受付窓口業務」は、相互に入札制限の対象とする。

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	本調達(請負者)	運用管理及び受付窓口業務	幹部出退勤表示機能の更改	LAN 端末の賃貸借・保守	端末ソフトウェアの借入	複合機の賃貸借・保守
本調達 更新整備及び保守・運用	プロジェクト管理	▲	●	－	－	－	－	－
	設計	－	●	－	－	－	－	－
	構築／導入	－	●	－	－	－	－	－
	移行	－	●	－	－	－	－	－
	運用	－	●	－	－	－	－	－
	保守	－	●	－	－	－	－	－
運用管理及び受付窓口業務	プロジェクト管理	▲	▲	●	－	－	－	－
	管理設計	－	▲	●	－	－	－	－
	運用管理	－	▲	●	－	－	－	－
	受付窓口	－	▲	●	－	－	－	－
幹部出退勤表示機能の更改	環境設定	－	▲※	－	●	－	－	－
	運用	－	●	－	－	－	－	－
	保守	－	－	－	●	－	－	－
LAN 端末の賃貸借・保守	プロジェクト管理	▲	▲※	－	－	●	－	－
	マスタ作成	－	●※	－	－	▲	－	－
	マスタインストール	－	▲※	－	－	●	－	－
	展開作業	－	▲※	－	－	●	－	－
	運用	－	●	－	－	－	－	－
	保守	－	－	－	－	●	－	－
端末ソフトウェアの借入	提供	－	－	－	－	－	●	－
	環境設定	－	●	－	－	－	－	－
	運用	－	●	－	－	－	－	－
	QA 対応	－	●	－	－	－	－	－
複合機の賃貸借・保守	プロジェクト管理	－	▲※	－	－	－	－	●
	プリントサービス設計	－	●※	－	－	－	－	▲
	環境設定	－	▲※	－	－	－	－	●
	展開作業	－	▲※	－	－	－	－	●
	運用	－	●	－	－	－	－	－
	保守	－	－	－	－	－	－	●

●：業務の主担当、▲：業務の連携・調整先

※：総務省 LAN の更改に伴う幹部出退勤表示機能、賃貸借中の LAN 端末及び複合機

の設定変更等については、本調達の請負者が各事業者の作業費用を負担すること

第3　満たすべき情報システムに求める要件に関する事項

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)　機能要件

本業務の実施に当たっては、別紙 1「要件定義書」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。なお、機能要件の詳細は、別紙 1-1「機能要件詳細」、別紙 1-2「ルータ・スイッチ要件一覧」及び別紙 1-3「回線一覧」を参照すること。

(2)　非機能要件

本業務の実施に当たっては、別紙 1「要件定義書」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。なお、情報セキュリティ要件及び保守・運用要件の詳細は、別紙 1-4「情報セキュリティ要件詳細」、別紙 1-5「保守・運用要件詳細」及び別紙 1-6「本省・DR サイト稼働サービス一覧」をそれぞれ参照すること。

3　その他

本業務の実施に当たっては、以下の別紙 2 から別紙 8 までの内容を理解した上で、調達仕様書及び要件定義書記載の要件を満たすこと。

- 別紙 2「次期総務省 LAN 構成イメージ」
- 別紙 3「保有ライセンス・ソフトウェア一覧」
- 別紙 4「現行総務省 LAN におけるサービスレベル一覧」
- 別紙 5「拠点一覧」
- 別紙 6「成果物一覧」
- 別紙 7「情報保護・管理要領」
- 別紙 8「用語の定義」

第4　作業の実施内容に関する事項

1　作業の内容

(1)　プロジェクト管理

請負者は、契約期間を通じて、総務省 LAN 全体に対し、以下のプロジェクト管理を行うこと。なお、更新整備期間中である令和 2 年及び 3 年度におけるプロジェクト管理は、別途調達する工程管理支援事業者と調整の上、実施すること。

ア　コミュニケーション管理

契約期間中における主管課、工程管理支援事業者、関係事業者、関係機関、情報システム利用者等が認識を一致させ、調整事項や課題等を共有した上で合意形成を行うために、連絡調整や会議開催、情報共有等のコミュニケーション管理作業を実施すること。

イ　体制管理

契約期間中に発生する作業内容に合致した作業体制を構築・維持するため、体制管理作業を実施すること。

ウ　工程管理

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、工程管理支援事業者と調整の上、実施すること。また、更新整備に当たって、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。

エ　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、品質管理作業を実施すること。

オ　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、リスク管理作業を実施すること。

カ　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、課題管理作業を実施すること。

キ　システム構成管理

契約期間中において情報システムを構築・稼働するための環境は時系列で準備する必要があることを踏まえ、環境の過不足を無くすために、その構成要素や環境構築スケジュール等を意識したシステム構成の管理作業を実施すること。

ク　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、変更管理作業を実施すること。

ケ　情報セキュリティ対策

契約期間中、業務を遂行する上で情報セキュリティインシデントを発生させないために、情報セキュリティに対する基本方針の検討や情報セキュリティの管理作業を実施すること。

コ　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、報告書類の作成等を行うこと。

(2)　更新整備

総務省 LAN の更新整備に当たっては、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、主管課及び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　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。

また、PMO による第二次工程レビューを受けること。

ウ　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。

エ　構築の実施

請負者は、「ウ　設計の実施」で実施する設計に基づき、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。

オ　テストの実施

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、単体テスト、結合テスト、総合テスト、その他総務省 LAN の稼働に必要なテスト計画を策定し、その計画に基づいてテストを実施すること。なお、それぞれのテスト計画、テスト結果について主管課の承認を受けること。

また、遅くとも総合テスト計画を確定するまでに、PMO による第三次工程レビューを受けること。

カ　受入テストの実施支援

主管課は、総務省 LAN の構築が完了する前に、総務省 LAN で求めている要件を満たしているか確認するため、受入テストを実施する。請負者は、受入テストの計画案の策定、受入テスト仕様書案の策定、受入テストの実施を支援すること。また、受入テストの結果、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。

キ　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。

ク　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。

ケ　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。

コ　ODB 登録用シートの提出

請負者は、「標準ガイドライン」における別紙 3「調達仕様書に盛り込むべき ODB 登録用シートの提出に関する作業内容」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)　設計・構築規模の管理
(イ)　ハードウェアの管理
(ウ)　ソフトウェアの管理
(エ)　回線の管理
(オ)　外部サービスの管理
(カ)　施設の管理
(キ)　公開ドメインの管理
(ク)　取扱情報の管理
(ケ)　情報セキュリティ要件の管理
(コ)　指標の管理

(3)　保守・運用

総務省 LAN の保守・運用に当たっては、以下に示す作業を行うこと。

ア　保守・運用要領の作成

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

イ　中長期保守・運用作業計画の作成

請負者は、「保守・運用要領」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「中長期保守・運用作業計画」を作成すること。「中長期保守・運用作業計画」には、情報システムの構成やライフサイ

クルを通じた保守作業及び運用業務の内容について記載すること。

ウ　保守・運用実施計画書の作成

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「保守・運用実施計画書」を作成し、主管課の承認を受けること。

エ　平常時対応

（ア）運用業務

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、継続的なサービス改善等の運用業務を行うこと。

（イ）情報セキュリティ管理

請負者は、情報セキュリティ管理として、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。

（ウ）保守業務

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。

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。

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、「保守・運用要領」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、政府共通プラットフォームへの移行等、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　保守作業及び運用業務の改善提案

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「保守・運用要領」、「中長期保守・運用作業計画」及び「保守・運用実施計画書」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、本業務の運用開始までに、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、次々期総務省 LAN 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総務省 LAN の受注事業者に対し、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総務省 LAN の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、「標準ガイドライン」における別紙 3「調達仕様書に盛り込むべき ODB 登録用シートの提出に関する作業内容」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、「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」に基づき年度毎に分類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

本業務の成果物を別紙 6「成果物一覧」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、日本産業規格（JIS X 0001～0032）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1部、電磁的記録媒体は正1部・副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、原則として日本産業規格A列4番とするが、必要に応じて日本産業規格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、主管課の承認を得ること。

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、成果物一覧に示した完成図書一式を本省に納品すること。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サイバーセキュリティ・情報化推進室第三係

(5)　その他

別紙6「成果物一覧」に示された成果物のうち各種設計書については、調達仕様書（別紙1「要件定義書」を含む。）に示された各要件と当該設計書に記載の項目の関係を明らかにし、主管課が要件の実現を遺漏なく確認・検収できるよう、一覧で容易に確認できる資料を併せて納品すること。

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 に、各組織及び事業者の役割を表 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、保守・運用担当、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。

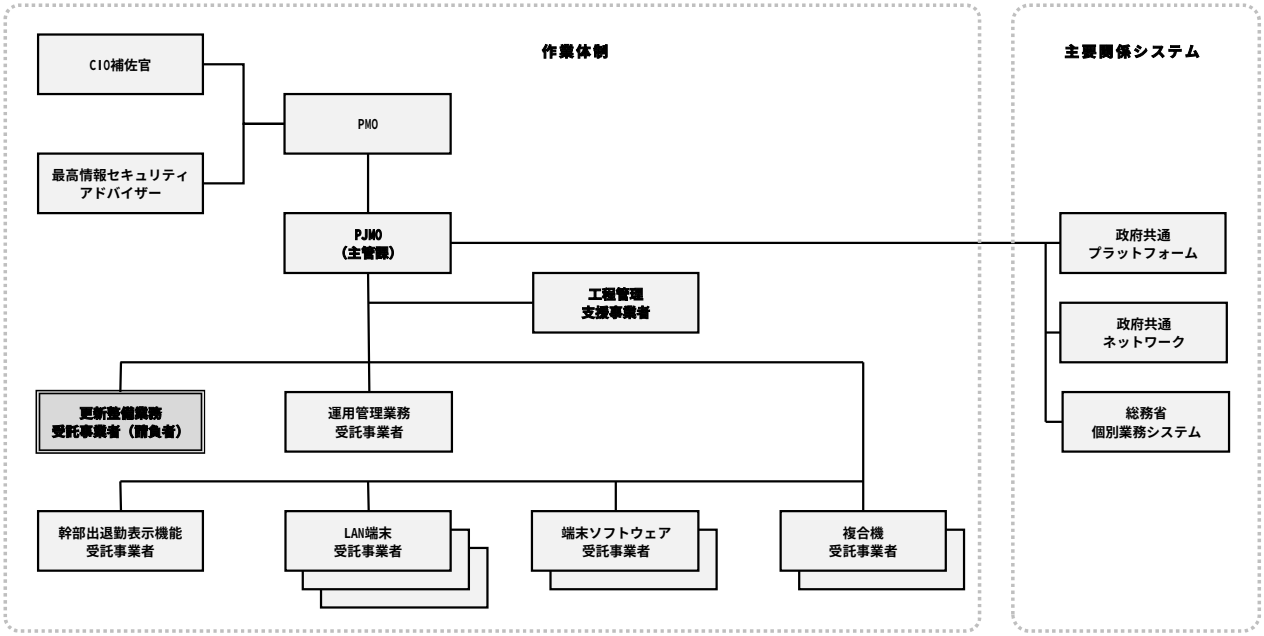


図 5-1　プロジェクト実施体制

表 5-1　組織・事業者の役割

No.	組織・事業者	役割
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（主管課）	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	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。
4	最高情報セキュリティアドバイザー	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。

No.	組織・事業者	役割
5	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。
6	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。
7	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。
8	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。
9	更新整備業務受託事業者（請負者）	総務省 LAN の更改に際し、更新整備及び保守・運用業務を担当する事業者。本請負者。
10	運用管理業務受託事業者	総務省 LAN の更改に際し、運用管理及び受付窓口業務を担当する事業者。
11	幹部出退勤表示機能受託事業者	総務省 LAN において、総務省本省幹部の出退勤を表示する機能を総務省本省に導入し、保守を担当する事業者。
12	LAN 端末受託事業者	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。
13	端末ソフトウェア受託事業者	総務省 LAN において、LAN 端末で利用する端末ソフトウェア・ライセンスを提供する事業者。
14	複合機受託事業者	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、総務省本省以外の拠点に導入し、保守を担当する事業者。

(1)　業務従事者の適格性の確保等

ア　請負者は、契約を履行する業務に従事する個人（以下「業務従事者」という。）として、本件業務を実施するに当たって必要な経験、資格、業績等を有する者を確保すること。

イ　業務従事者は、履行に必要若しくは有用な、又は背景となる経歴、知見、語学（母語及び外国語能力）、文化的背景（国籍等）を有すること。

(2)　情報保全の履行体制

ア　請負者は、この契約の履行に際し知り得た保護すべき情報（契約を履行する一環として請負者が収集、整理、作成等した情報であって、主管課が保護を要さないと確認したものを除く。）その他の非公知の情報（主管課から提供した情報を含む。以下「保護すべき情報等」という。）について、適切に管理するものとする。

イ　保護すべき情報等の取扱いについては、次の履行体制を確保し、これを変更した場合には、遅滞なく主管課に通知するものとする。

(ア) 主管課が保護を要さないと確認するまでは保護すべき情報として取り扱う履行体制
(イ) 主管課の同意を得て指定した取扱者以外の者に取扱わせない履行体制
(ウ) 主管課が許可した場合を除き、請負者に係る親会社や請負者に対して指導、監督、業務支援、助言、監査等を行う者を含む一切の請負者以外の者に対して伝達又は漏えいさせない履行体制

ウ 契約の履行中、履行後を問わず情報の漏洩等の事故や疑い、将来的な懸念の指摘があったときは、直ちに必要な措置等を講ずるとともに、主管課に報告すること。また、主管課から求められた場合は、情報の管理の履行状況等を報告するとともに、総務省による調査が行われる場合は、これに協力すること。

2 作業要員に求める資格等の要件

(1) 統括責任者

ア 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。

イ 本プロジェクトの統括責任者は、以下のいずれかの資格を有する者であること。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。）。

(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）
(イ) プロジェクトマネジメント・プロフェッショナル（米国 PMI）

(2) 作業リーダー・作業担当者

ア 本プロジェクト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) 情報処理安全確保支援士（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)Version3 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) 総務省 LAN 情報セキュリティチーム

ア 総務省 LAN 情報セキュリティチームは、サービス保守要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って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。

イ 上級セキュリティエンジニアは、別紙 1-4「情報セキュリティ要件詳細」の「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。

ウ 上級セキュリティエンジニアの中心的役割を担う者は、利用者数 5,000 名程度の基幹 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。又は、ウイルス感染事案等への対応を想定した最新のセキュリティ動向を踏まえたインシデント対応訓練等を継続的に受け、かつ、請負者が総務省 LAN における重大インシデント発生時の対応を確実に行うことができると合理的に説明できる者であること。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。

エ 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 1-1「機能要件詳細」の「セキュリティサービス」「セキュリティログ分析サービス」に示すものと同等のログ解析機器（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、当該者が原則として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。

オ 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。

(ア) SANS GIAC Certified Forensics Analyst
(イ) SANS GIAC Certified Incident Handler
(ウ) 情報システムセキュリティ専門家 （CISSP）
(エ) 情報セキュリティマネージャ （CISM）
(オ) 情報セキュリティ監査人 （CAIS）
(カ) 情報システム監査人 （CISA）

カ 総務省 LAN 情報セキュリティチームの統括者は、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。

キ　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。

ク　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。

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、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、主管課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、「保守・運用要領」に基づき、保守・運用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 7「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」（別紙として添付）及び「総務省情報セキュリティポリシー」（総務省情報セキュリティ委員会決定）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

当該調達案件の業務遂行に当たっては、「第 11 附属文書」に示す政府指針・ガイドライン等及び本省の指針等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　契約不適合責任

(1) 総務省は、請負者に対し、引き渡された成果物が種類又は品質に関して契約の内容に適合しないものである場合（その不適合が総務省の指示によって生じた場合を除き、請負者が当該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場合を含む。）において、その不適合を総務省が知った日から起算して 1 年以内にその旨の通知を行ったときは、その成果物に対する修補等による履行の追完を請求することができる。ただし、請負者は、総務省に不相当な負担を課するものでないときは、総務省が請求した方法と異なる方法による履行の追完をすることができる。

(2) (1)の場合において、総務省が相当の期間を定めて履行の催告をし、その期間内に履行の追完がないときは、総務省は、その不適合の程度に応じて代金の減額を請求することができる。

(3) (1)又は(2)の場合において、総務省は、損害賠償を請求することができる。

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　本件請負契約の仕様書に記載した実施体制を有する者であること。

イ　「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。

ウ　「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。

エ　「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。

オ　平成 31・32・33 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 304 情報処理、306 ソフトウェア開発」又は 305 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、ISO9001 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、ISO/IEC 27001 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

ア　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 の調達支援及び計画・設計工程管理支援業務の請負」の受注事業者

ウ　「次期総務省 LAN の調達支援及び構築、保守・運用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８２ 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「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。

(2) 調達仕様書（別紙 1「要件定義書」を含む。）に記載の要件は、目的を達成し、予算要求を行うための費用を算出するため、総務省の考える必要最低限の要件であり、更に効果的に目的を達成する方法がある場合には、客観的に合理的と認められる根拠を含め、積極的にその実現方法を提案すること。なお、提案の採否は、提案内容を踏まえ、総務省が総合的に判断するものとする。

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「機能要件詳細」
別紙 1-2「ルータ・スイッチ要件一覧」
別紙 1-3「回線一覧」
別紙 1-4「情報セキュリティ要件詳細」
別紙 1-5「保守・運用要件詳細」
別紙 1-6「本省・DR サイト稼働サービス一覧」

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「保有ライセンス・ソフトウェア一覧」
- 別紙 4「現行総務省 LAN におけるサービスレベル一覧」
- 別紙 5「拠点一覧」
- 別紙 6「成果物一覧」
- 別紙 7「情報保護・管理要領」
- 別紙 8「用語の定義」

3　提案書等の審査要領は、「総務省 LAN システムの更新整備及び保守・運用業務の請負総合評価基準書」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保守・運用業務民間競争入札実施要項」の「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。

5　参考とする政府指針・ガイドライン等及び本省の指針等を以下に示す。

- 政府情報システムにおけるクラウドサービスの利用に係る基本方針（平成 30 年 6 月 7 日 各府省情報化統括責任者（CIO）連絡会議決定）

- デジタル・ガバメント推進標準ガイドライン（2020 年 3 月 31 日 各府省情報化統括責任者(CIO）連絡会議決定）

- 公共サービス改革基本方針（令和元年７月９日改定 閣議決定）

- 世界最先端 IT 国家創造宣言・官民データ活用推進基本計画　（令和元年６月 14 日閣議決定）

- 政府共通プラットフォーム第二期整備計画（2019（平成 31）年 2 月 25 日 各府省情報化統括責任者（CIO）連絡会議決定）

- 総務省デジタル・ガバメント中長期計画（平成 30 年 6 月 22 日 総務省行政情報化推進委員会決定）

- 政府機関の情報セキュリティ対策のための統一基準群（平成 30 年度版）（平成 30 年 7 月 25 日サイバーセキュリティ戦略本部）

- 「高度標的型攻撃」対策に向けたシステム設計ガイド（平成 26 年 9 月 30 日 独立行政法人情報処理推進機構）

- テレワークセキュリティガイドライン（第 4 版）（2018 年 4 月 13 日 総務省 経済産業省）

- 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（平成 25 年 3 月 1 日 総務省 経済産業省）

- 総務省情報セキュリティポリシー（総務省情報セキュリティ委員会決定）

- 政府業務継続計画（首都直下地震対策）（平成 26 年 3 月 28 日 閣議決定）

- 中央省庁業務継続ガイドライン 第 2 版（首都直下地震対策）（平成 28 年 4 月 内閣府（防災担当））

- 総務省本省業務継続計画（令和元年 7 月 10 日 一部改定）

- 中央省庁における情報システム運用継続計画ガイドライン（平成 24 年 5 月改定 内閣官房情報セキュリティセンター）

日本産業規格 JIS X 8341-3:2016「高齢者・障害者等配慮設計指針－情報通信における機器，ソフトウェア及びサービス－第 3 部：ウェブコンテンツ」（2016 年 3 月版（2016 年 3 月 22 日公開） 情報通信アクセス協議会・ウェブアクセシビリティ基盤委員会）

別紙 1

総務省 LAN システムの更新整備及び保守・運用業務の請負 要件定義書

総務省大臣官房企画課サイバーセキュリティ・情報化推進室

－ 目 次 －

第1　業務要件

1　業務実施手順

総務省 LAN は総務省の業務全般を効率的に遂行する情報基盤であるため、特定の業務に対する業務実施手順は定義しない。

2　規模

ユーザアカウント数、機器数及び拠点数等の規模については、「第 3 非機能要件」の「3 規模に関する事項」を参照すること。

3　時期・時間

総務省 LAN は、原則として 24 時間 365 日稼働し、職員に対して各種サービスを提供するシステムであるため、それを理解した上で、「第 3 非機能要件」の「5 信頼性に関する事項」の要件を満たすこと。ただし、定期保守、法定停電等による停止時間を除く。

4　場所等

総務省 LAN は、本省を中心として、外部拠点（13 拠点）、地方支分部局（62 拠点）DR サイト、外部監視室で構成されている。各拠点の所在地については、調達仕様書の別紙 5「拠点一覧」を参照すること。

5　管理すべき指標

総務省 LAN において管理すべき指標（案）を以下に示す。具体的な指標及び測定方法については、主管課と協議の上、決定すること。

表 1-1　管理指標（案）

No.	視点	指標（案）
1	職員の利便性向上	・　職員のシステム満足度向上
2	働き方改革の推進	・　テレワーク利用率の向上 ・　Web 会議利用率の向上
3	安全性の確保	・　セキュリティインシデント発生数の軽減

6　情報システム化の範囲

総務省 LAN は、総務省の業務全般を効率的に遂行するための情報基盤であり、本調達における情報システムの範囲は、調達仕様書の別紙 2「次期総務省 LAN 構成イメージ」に示す範囲である。本調達における情報システムの範囲を理解した上で、全ての要件を満たすこと。

7　業務の継続の方針等

総務省 LAN では本省と同時に被災する可能性が低い遠隔地に DR サイトを構築し、本省で提供するサービスを代替して提供することにより、被災していない地方支分部局等間でのコミュニケーション系サービス（メール、Web 会議、チャット、ポータルサイト、ファイル共有）や政府共通ネットワーク等を利用した業務継続を想定している。そのため、本省が被災した場合においても業務継続に必要な機能・サービスが利用可能な構成とすること。

なお、総務省本省は「政府業務継続計画（首都直下地震対策）」（平成 26 年 3 月 28 日閣議決定）及び「中央省庁業務継続ガイドライン第 2 版（首都直下地震対策）」（平成 28 年 4 月内閣府（防災担当））に沿って作成された「総務省本省業務継続計画」（令和元年 7 月 10 日一部改定）において、発災から 1 週間程度の間、インターネットや地方支分部局等とのネットワークが維持され、非常用電源により総務省 LAN 機器を運用可能であることが記載されている。

8　情報セキュリティ

総務省職員は、「総務省情報セキュリティポリシー」（総務省情報セキュリティ委員会決定）及び情報セキュリティ関係規程に定められている事項を遵守している。そのため、遵守する上で必要となる機能・サービスを提供すること。なお、「総務省情報セキュリティポリシー」及び情報セキュリティ関係規程は、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。

第2　機能要件

1　機能に関する事項

総務省 LAN の各機能を満たすサービス・機器を提供すること。なお、詳細な要件は、別紙 1-1「機能要件詳細」の各章を参照すること。

2　画面に関する事項

画面については、特段要件を定義しないが、職員が利用する画面については可能な限り操作が容易であること。また、現行総務省 LAN で利用している機能を引き続き利用する場合は、可能な限り画面の変化を最小化すること。

3　帳票に関する事項

帳票については、特段要件を定義しない。

4　ファイルに関する事項

本システムにおいて入出力を行うファイルの形式については、別紙 1-1「機能要件詳細」の各章に示したファイル形式・拡張子の要件を考慮して最適なものを使用でき

るようにすること。

5　情報・データに関する事項

本システムにおいて取り扱われる情報・データについては、別紙 1-1「機能要件詳細」の各章に示した規模や容量の要件を参照すること。なお、情報・データの詳細については、資料閲覧の際に開示するものとする。

6　外部インタフェースに関する事項

現行総務省 LAN には各部局で調達している個別業務システムが約 80 システム接続されている。本調達においては、個別業務システムの接続及び切り離しに伴う各種支援を実施すること。なお、個別業務システムの詳細については、資料閲覧の際に開示するものとする。

第3　非機能要件

1　ユーザビリティ及びアクセシビリティに関する事項

(1)　情報システムの利用者の種類、特性

総務省 LAN の利用目的は行政事務であり、利用者は総務省等に所属する職員である。

(2)　ユーザビリティ要件

別紙 1-1「機能要件詳細」に示した機能・サービスの実装にあたってアプリケーションプログラムの開発を行う場合には、以下のユーザビリティ要件に配慮すること。また、ソフトウェアの選定にあたっては、以下のユーザビリティ要件に配慮したものを選定すること。なお、設計・構築時において、主管課と協議の上、最終的な決定をすること。

表 3-1　ユーザビリティ要件

No.	ユーザビリティ分類	ユーザビリティ要件
1	画面の構成	・ 何をすればよいかが見て直ちにわかるような画面構成にすること ・ 無駄な情報、デザイン及び機能を排し、簡潔でわかりやすい画面にすること ・ 十分な視認性のあるフォント及び文字サイズを用いること ・ 画面の大きさや位置の変更ができること

No.	ユーザビリティ分類	ユーザビリティ要件
2	操作方法のわかりやすさ	・ 無駄な手順を省き、最小限の操作、入力等で利用者が作業できるようにすること ・ 画面上で入出力項目のコピー及び貼付けができること ・ 業務の実施状況によっては、ショートカットや代替入力方法が用意されること（例えば、片手だけで主要な操作が完了することが求められたり、マウスを利用することが困難であったりする場合が考えられる）
3	指示や状態のわかりやすさ	・ 操作の指示、説明、メニュー等には、利用者が正確にその内容を理解できる用語を使用すること ・ 必須入力項目と任意入力項目の表示方法を変えるなど各項目の重要度を利用者が認識できるようにすること ・ システムが処理を行っている間、その処理内容を利用者が直ちにわかるようにすること
4	エラーの防止と処理	・ 利用者が操作、入力等を間違えないようなデザインや案内を提供すること ・ 入力内容の形式に問題がある項目については、それを強調表示する等、利用者がその都度その該当項目を容易に見つけられるようにすること ・ 電子申請等については、確認画面等を設け、利用者が行った操作又は入力の取消し、修正等が容易にできるようにすること ・ 重要な処理については事前に注意表示を行い、利用者の確認を促すこと ・ エラーが発生したときは、利用者が容易に問題を解決できるよう、エラーメッセージ、修正方法等について、わかりやすい情報提供をすること
5	ヘルプ	・ 利用者が必要とする際に、ヘルプ情報やマニュアル等を参照できるようにすること

(3) アクセシビリティ要件

別紙 1-1「機能要件詳細」に示した機能・サービスの実装にあたってウェブコンテ

ンツの作成を行う場合には、日本工業規格 JIS X 8341-3:2016「高齢者・障害者等配慮設計指針－情報通信における機器，ソフトウェア及びサービス－第 3 部：ウェブコンテンツ」のアクセシビリティ要件に配慮すること。

なお、設計・構築時において、主管課と協議の上、最終的な決定をすること。

2　システム方式に関する事項

(1)　システムアーキテクチャ

本システムのシステムアーキテクチャ（メインフレーム型／クライアントサーバ型／Web サーバ型／政府共通プラットフォーム利用型／外部サービス利用型／スタンドアロン型）は、別紙 1-1「機能要件詳細」の各章に示した要件を考慮して最適なものを組み合わせること。

(2)　アプリケーションプログラムの設計方針

別紙 1-1「機能要件詳細」に示した機能・サービスの実装にあたってアプリケーションプログラムの開発を行う場合には、システムを構成する各コンポーネント（ソフトウェアの機能を特定単位で分割したまとまり）間の疎結合、再利用性の確保を基本とすること。

(3)　ソフトウェア製品の活用方針

広く市場に流通し、利用実績を十分に有するソフトウェア製品を活用すること。また、アプリケーションプログラムの動作、性能等に支障を来たさない範囲において、可能な限りオープンソースソフトウェア(OSS)製品(ソースコードが無償で公開され、改良や再配布を行うことが誰に対しても許可されているソフトウェア製品）の活用を図ること。ただし、それらの OSS 製品のソフトウェア保守サポートが契約期間終了まで継続されていることを確認すること。

(4)　システム基盤の方針

次期総務省 LAN のシステム基盤は、オンプレミス環境とする。システムの概要については、調達仕様書の「第 1 調達案件の概要に関する事項」の「5 業務・情報システムの概要」を参照すること。

なお、サーバ等の機器は、可能な限り仮想化技術を利用し、スペースの圧縮や運用・管理面で工数の削減を図ること。

3　規模に関する事項

次期総務省 LAN のユーザアカウント数、機器数及び拠点数を以下に示す。以下の記載を理解した上で、「第 3 非機能要件」の「4 性能に関する事項」の要件を満たすこと。

表 3-2　ユーザアカウント数・機器数・拠点数

アカウント数	ユーザアカウント ※1	7,000 個
	一時保管アカウント　※2	2,000 個
	共有アカウント　※3	2,800 個
	保守・運用業務用アカウント　※4、※5	1,400 個
機器数	LAN 端末	7,000 台
	ウイルスチェック用端末	150 台
	ペーパーレス会議用タブレット型端末	300 台
	Windows タブレット型端末	10 台
	LAN プリンタ	232 台
	USB プリンタ	213 台
	LAN 複合機	564 台
拠点数	本省	1 拠点
	外部拠点	13 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

※1 職員が総務省 LAN の各種サービスを利用する際に用いるアカウント
※2 職員の異動や退職等で不要となったユーザアカウントを無効化した状態で一定期間保持しておくアカウント
※3 複数の職員が共有するメールアカウントやポータルサイトサービス等を利用するためのアカウント
※4 総務省 LAN の請負者と運用管理・受付窓口請負事業者が保守・運用等に利用するためのアカウント
※5 「保守・運用業務用アカウント」は、運用管理・受付窓口請負事業者が必要とするアカウント数 12 個を含む

4　性能に関する事項

本業務の実施に当たって、性能に係る要件を理解した上で、全ての要件を満たすこと。

① 規模要件を参考に、運用期間中の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。

5　信頼性に関する事項

本業務の実施に当たって、総務省 LAN は安定性を最も重視するため、信頼性に係る要件を理解した上で、以下全て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。

(1)　品質要件

① 十分に実績のある機器を選定すること。
② 24 時間 365 日の稼働に耐えうる製品を選定すること。
③ 本調達で導入するサーバ製品等は、契約開始後 60 か月は部品保守が可能であること。
④ メーカもしくはベンダによるオンサイトサポートが対応可能であること。
⑤ 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。

(2)　可用性要件

① 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。
② 対策により得られる効果と対策に要するコストの両面を考慮した、最適な対策を選択すること。
③ 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、平均故障間隔（MTBF）等を根拠に信頼性を担保すること。
④ 記憶装置、ネットワークインタフェース、電源及びファンについても、当該部品の障害に備え、同一機器内で冗長化すること。
⑤ 機器を冗長化構成とする場合、主系から副系への切替え、副系から主系への切戻しの際には、各サービスの停止時間を極少化し、業務継続に支障のないようにすること。
⑥ 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、ネットワーク機器、及びアプライアンス機器は冗長化し、信頼性を高めること。
なお、必要に応じて、負荷分散装置を利用した冗長化も可とする。
⑦ DR サイトへ設置する機器については、通常時でもサービス提供しているサーバやアプライアンス機器、その経路上にあるネットワーク機器については冗長化すること。本省のバックアップサービスとして待機している機器とその経路上にあるネットワーク機器についてはシングル構成でも可とする。
⑧ 停電発生時や非常用電源故障時において、自動的もしくは安全にシャットダウンが可能な構成とすること。

(3) 完全性要件

① 各種保存データや設定ファイル等の情報が正確に記録又は保存されること。
② 機器の故障に起因するデータの滅失や改変を防止する対策を講ずること。
③ 処理の結果を検証可能とするため、ログ等の証跡を残すこと。
④ データの複製や移動を行う際に、データが毀損しないよう、保護すること。

6 拡張性に関する事項

本業務の実施に当たって、拡張性に係る要件を理解した上で、全ての要件を満たすこと。

① ハードウェア、ソフトウェア共に契約開始後 60 か月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 リソース等を拡張する際は、サービスに与える影響を最小限に留めて実施できること。
⑥ ハードウェアの増設は、増加する利用者数、増加前の実使用量などを勘案の上、無駄のない構成とすること。

7 上位互換性に関する事項

本業務の実施に当たって、上位互換性に係る要件を理解した上で、全ての要件を満たすこと。

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、主管課に詳細な内容を説明した上で、実施手順の承諾を受けること。
② サーバ・ネットワーク機器・アプライアンス機器・LAN 端末等の OS・ミドルウェアを含むソフトウェア環境はバージョンを統一し、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 バージョンアップについて技術的な問題等がある場合は都度主管課と協議し、その指示に従うこと。
④ 旧バージョンで作成したファイルを新バージョンでも自由に扱うことができることを考慮すること。なお、本要件に合致しない場合は、代替案（旧バージョンで作成したファイルを新バージョンで利用可能な仕組み）を検討した上で、主管課の承認を得ること。
⑤ 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。

8　中立性に関する事項

本業務の実施に当たって、中立性に係る要件を理解した上で、全ての要件を満たすこと。

① ハードウェア及びソフトウェア等は、特定ベンダの技術に依存しない、オープンな技術仕様に基づくものとすること。

② ハードウェア及びソフトウェア等は、全てオープンなインタフェースを利用して接続又はデータの入出力が可能であること。

③ 導入するハードウェア及びソフトウェア等の構成要素は、標準化団体（ISO、IETF、IEEE、ITU、JISC 等）が規定または推奨する各種業界標準に準拠すること。

④ 次期総務省 LAN 更改の際に、データ移行の妨げとなることや、特定の装置や情報システムに依存することを防止するため、原則として情報システム内のデータ形式は XML、CSV 等の標準的な形式で取り出すことができるものとすること。

⑤ 特定の事業者や製品に依存することなく、他者にシステム導入時の設計情報を引き継げることが可能となるようなシステム構成とすること。

9　継続性に関する事項

本業務の実施に当たって、継続性に係る要件を理解した上で、全ての要件を満たすこと。

(1)　前提となる考え方

総務省は、「中央省庁における情報システム運用継続計画ガイドライン」に基づき、総務省 LAN において情報システム継続性を強化し、適切に維持管理していくための具体的な事項（対象範囲、事前対策計画、非常時の対応計画、教育訓練計画、維持改善計画）を「総務省 LAN 運用継続計画」として定めている。

また、「政府業務継続計画（首都直下地震対策）」等の資料群に基づき、総務省では「総務省本省業務継続計画」を定めており、次期総務省 LAN の構築は、これらの計画に着実に対応できるように、更なる対策の強化を進めていく必要がある。

なお、これらの資料については資料閲覧にて確認すること。

(2)　目標復旧時間と目標復旧時点

大規模災害時等の非常時において、以下に定める目標復旧時間及び目標復旧時点を満たすこと。

ア 目標復旧時間（RTO）

① 「総務省 LAN 運用継続計画」に従うこと。

② ディザスタリカバリ発動（主管課が保守運用事業者へ DR サイトの切替え指示を出すタイミング）から 30 分以内で、保守・運用事業者が切り替え作業等を実施

し、主管課へ対応の完了報告を行った上で、非常時優先業務として利用する総務省 LAN 提供サービスが開始できること。

イ 目標復旧時点（RPO）

① 保全対象のデータに対し、本省からの定期オンラインバックアップにて複数の世代管理で保全し、最低限 1 日前のデータを復元すること。

② バックアップデータの取得頻度、保持期間及び世代管理や、自動化の程度等については、対象とするデータの性質等に応じて、業務に影響を与えず、かつ費用対効果が高いものを選定すること。

ウ DR サイトの稼働条件

① 現行システムの DR サイトが提供するサービス・機能については、原則利用できること。詳細については、資料閲覧時において確認すること。

② 「【別紙 1-6】本省・DR サイト稼働サービス一覧」を参照し、①では提供されてないサービスも提供可能とすること。ただし、機能を縮退して提供する場合には、その内容を主管課と合意すること。

③ DR 発動後、本省から DR サイトに切り替えた際に、DR サイトからのインターネット接続、政府共通ネットワーク接続を可能にすること。

④ DR サイトでの運用は、1 か月程度は稼働し続けることを想定した運用体制を準備すること。また、リモートによる遠隔でも対応できるなど、DR サイト専属の要員は適切な人数で配置するように考慮すること。

エ その他

① 請負者は「総務省 LAN 運用継続計画」を次期総務省 LAN に適合する形で再作成すること。

② 本計画は年に一回以上、請負者が適切な見直しや修正を行い主管課の承認を得ること。

10 情報セキュリティに関する事項

本業務の実施に当たって、情報セキュリティ対策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「情報セキュリティ要件詳細」の情報セキュリティ要件を参照すること。

11 情報システム稼働環境に関する事項

本業務の実施に当たって、本省サーバ室、DR サイト、構築拠点、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。

(1) 本省サーバ室

ア 設備条件

① 本省サーバ室では既設 19 インチラック 23 本の流用が可能である。

② 42U ラック 1 本分の新設ラック設置スペースを総務省にて用意する。新設ラックを設置する場合は、主管課との協議の上、以下の要件に従って調達し、設置工事

を行うこと。

イ 既設ラック

① 個別に施錠可能な EIA 規格の 19 インチラックである。

② 耐震対策は実施済みである。

③ 自重 140kg、総耐荷重 500kg、マウント数 42U である。

④ 流用の際に、本省ラック設置の条件に当てはまらない状態（施錠不可、棚の破損等）が確認できた場合には、請負者によって新たに調達し交換設置すること。

ウ 床耐荷重

二重床の耐荷重は 500kg/㎡以下である。

エ UPS

① 現行機器では、7 台の大型 UPS（200V 20kVA UPSS-200X2）によって、各ラックへ電源供給しており、19 インチラック外に設置し、1 個所に集約している。

② 次期総務省 LAN でも適切な調達及び配置を行うこと。

オ 電源

① 分電盤（総務省 LAN 機器室サーバ分電盤×3 回路、自治省 LAN 機器室分電盤×2 回路、通信機械室 LAN 分電盤×2 回路）から UPS 集約場所まで、単相 100A/200V の既設電源ケーブル 7 本を流用することができる。

② 現行機器では、既設ラック 21 本分の供給までとしているため、22 本以上（最大 24 本まで）利用する場合には、主管課から指定された分電盤のブレーカから UPS までの電源ケーブル引き込み工事を行うこと。

③ 必要に応じて分電盤のブレーカ回路の変更をすることは可能であるが、電源容量の増設工事はできない。

カ 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すること。

キ LAN 管理室

① 3.8m×9.7m（36.86 ㎡）程度の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が可能である。

ク ログ監視室

① 2.0m×6.6m（13.6 ㎡）程度の常駐可能なスペースを、LAN 管理室とは別に利用す

ることが可能である。

(2) DR サイト

ア 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、機器の設置フロアが適温、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 二重床でスラブより 50㎝ 以上の高さがあること。

② 二重床の耐荷重は 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。

④ ハウジングサービスを利用する場合、上記①～③に適合したラックを調達し設置すること。

⑤ ロケーションサービスを利用する場合、上記①～③に適合しているラックであることを確認すること。

(キ) 通信

① インターネット接続、政府共通ネットワーク接続、WAN 等の通信サービスが、構

内で直接接続できること。
② 可能な限り、ISP との接続点（POI）は、データセンタと同じ建物内に用意されていること。
③ 通常時は DR サイトからインターネット接続や政府共通ネットワーク接続などが利用できないため、不必要な通信はできる限り遮断すること。

(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 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 機器操作が可能な技術員が常駐していること。

イ 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。

ウ 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 300㎞ 以上離れた日本国内であること。
② 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、公共交通機関の利用及び徒歩で平均して 6 時間以内で到着可能な範囲にあること。
③ 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。
④ 国土交通省や自治体が公開しているハザードマップ等の情報で危険地域と指定された場所にないこと。

(3) 構築拠点

次期総務省 LAN の調達機器を本省・DR サイト・各拠点へ本設置するまでの期間は、請負者にて以下の要件を満たす構築拠点を準備すること。

また機器の本設置をした後、構築拠点の有効活用として外部監視室としての利用を可とする。

ア 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、機器の設置フロアが適温、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 二重床でスラブより 25㎝ 以上の高さがあること。
② 二重床の耐荷重は 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 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。

イ 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。

ウ 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) 外部監視室

ア ネットワーク

① 運用業務時間外等、省外から総務省 LAN をリモート監視するための施設を設け、総務省 WAN とは異なるネットワーク網で構成すること。

イ 入館

① 24 時間 365 日入館可能であること。

ウ 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 監視カメラでフロアを監視していること。

エ 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。

オ 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。

カ 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。

(5) 工事

ア 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 フロアネットワークの幹線及び無線 LAN アクセスポイントに接続するケーブルは、既存の流用を可とする。ただし、移行の際に必要な分及び断線等で不調なも

のは新たにケーブルを準備し配線すること。また追加が必要な場合は、受託者の責任において敷設すること。

(イ) 拠点

① 拠点のケーブルは原則既存の流用を可とする。ただし、移行の際に必要な分及び断線等で不調なものは新たにケーブルを準備し配線すること。また追加が必要な場合は、受託者の責任において敷設すること。

イ 電源工事

(ア) 本省

① 必要に応じ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を可とする。

(イ) 拠点

① 必要に応じ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とする。

ウ 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し落下防止対策を行うこと。

(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。なお、拠点のラックは原則既存の流用を可とする。

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し落下防止対策を行うこと。

12 テストに関する事項

本業務の実施に当たって、テストに係る要件を理解した上で、全ての要件を満たすこと。

(1) テスト要件

① 作業を実施するにあたっては、以下の内容を含む「テスト実施計画書」を速やかに作成し、主管課の承認を得ること。また、各作業項目単位のテスト終了後は、各テストの証跡及び「テスト結果報告書」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。

・ テスト目的・方針
・ テスト体制と役割
・ テストスケジュール
・ テストを行う場所

・ 制限・条件
・ 合否判定基準
・ テストシナリオ
・ テスト環境
・ テスト方法（単体テスト、結合テスト、総合テスト、受入テスト支援）
・ テストツール
・ インターネット接続前検査
・ テスト結果の証跡

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。なお、回線事業者が約款等によって担保している項目に関しては、その旨を明示した上でテスト項目から除外することも可とする。

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テストを実施すること。テスト項目や手順を適切に精査し、主管課と協議の上、テスト内容を決定すること。

④ テスト実施時は、1 つのテストを確認者・実施者の 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、テスト結果は確認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、テスト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テストを実施すること。

⑤ 定常時のテストだけではなく、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テストを必ず実施し、正常性を確保すること。切り替え・切り戻しテストは移行時にしか行えないため、総合テスト時に必ず行うこと。

(2) テスト種類

① 単体テストは、機器の初期不良の検出及び機器単体レベルの設計内容の妥当性を確認すること。なお、テスト内容が担保できるのであれば、テスト単位の変更は可能とする。

② 結合テストは、機器相互間が連携して機能するシステムのテストである。当該テストは、本省と外部拠点及び地方支分部局等間、本省と DR サイト及び外部監視室間の疎通も含まれる。なお、結合テストは、移行前に実施すること。

③ 総合テストは、「表 12-1 総合テストにおけるテスト種別」に示す項目を考慮し、運用業務の遂行を想定した総合的な機能テスト及び非機能テスト（性能の確認、障害対応、バックアップ／リストア等）を行うこと。また、当該テストでは、インターネット回線、政府共通ネットワーク、WAN 回線の疎通及び停電停止処理に係るテストも含まれる。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、それらもテストに含むこと。

④ 本省と DR サイトの切り替え、切り戻しの確認を行い、DR サイト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。
⑤ 他システムとの接続試験を含める他、必要に応じて、脆弱性診断等を含めること。
⑥ 性能テスト、負荷テストにおいて、十分な性能を満たせない場合は、主管課と協議の上、速やかに性能改善に取り組むこと。

表 12-1　総合テストにおけるテスト種別

No	テスト種別	内容
1	機能テスト	要件定義で定めた機能要件に適合しているかを確認する。
2	負荷テスト	重い負荷をかけて、負荷のレベルに応じて想定どおりの動作をするか確認する。
3	大容量テスト	大容量のデータを取り扱い、想定どおりの動作をするか確認する。
4	性能テスト	性能に係る要件（応答時間、スループット等）に適合しているかを確認する。
5	信頼性テスト	信頼性に係る要件（平均復旧時間、エラー数の目標値等）に適合しているかを確認する。
6	障害回復テスト	ソフトウェア、ハードウェア、回線等について、障害発生時の処理を確認する。
7	保守性テスト	保守に関するツール（情報採取ツール、ダンププログラム、トレースプログラム等）が問題なく実行できるか確認する。
8	手順書テスト	手順書の内容に従って、総務省 LAN の利用者が操作を行うことができるか確認する。
9	ペネトレーションテスト	総務省 LAN に対する侵入、改ざん、情報漏えい等の不測の事故が発生しないように、あらかじめ対象システムに対して擬似的な侵入・攻撃等を仕掛けて、適切に対応できることを確認する。
10	脆弱性テスト	総務省 LAN にセキュリティホール（脆弱性）や設定ミスが残存していないかを確認する。
11	運用テスト	運用業務が適切に実施できるか、運用計画書及び運用手順書の妥当性を検証する。

(3)　テスト場所
① 原則として請負者が各種テストを実施する場所を用意すること。
② テストを行う場所については「テスト実施計画書」に記載し、主管課の承認を得

ること。

(4) 受入テスト支援

① 受入テストは、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、請負業者は移行可否を最終的に判断するための具体的な受入テスト内容を含む計画案を作成すること。また、主管課が「受入テスト実施計画書」を作成する支援を実施すること。

② 受入テストを実施するに当たり、請負者は主管課の受入テスト実施の支援を行うこと。なお、受入テストで請負者が対応すべき内容を以下に示す。

・ 可能な限り本番環境に近いテスト環境の提供を行うこと。
・ 可能な限り本番データに近いテストデータの提供を行うこと。
・ 十分なテスト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。

③ 受入テストの結果、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。

13 移行に関する事項

本業務の実施に当たって、移行に係る要件を理解した上で、全ての要件を満たすこと。

(1) 移行の進め方に係る要件

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。

② 移行作業に係るリスクを明らかにした上で、各リスク対策を「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。

③ 「移行実施計画書」に基づき、主管課、現行運用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。

④ 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、想定時間等を明確にしたタイムチャートを含むこと。

⑤ 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。

⑥ 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。

⑦ 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。
⑧ 請負者は、「移行実施計画書」、「移行設計書」及び「移行手順書」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。
⑨ 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。
⑩ 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。
⑪ 「展開実施計画書」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。
⑫ 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。
⑬ 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を確認し、導入後障害等が発生した際に適切に対応できるよう準備しておくこと。
⑭ 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。
⑮ 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。

(2) 移行対象に係る要件

① 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。
② 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。
③ 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。
④ 移行対象データは以下を対象に含むこと。1 年以上過去のデータについては、移行が必要な範囲を主管課と協議し、移行対象を決定すること。
なお、LAN 端末上のデータ移行作業は原則として利用者自身が実施することとし、移行を円滑に行うための作業手順書やツールを準備すること。
・ 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（グループウェア上のコンテンツ）
・ ポータルサイトコンテンツデータ（局部課が CMS で作成したコンテンツ）
・ ポータルサイトコンテンツデータ（局部課が独自に作成したコンテンツ）
・ グループウェアデータ（グループウェア上のスケジューラ、設備予約情報等）
・ ディレクトリデータベース
・ 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
・ 現行総務省 LAN で保存されている各種ログデータ

(3) LAN 端末の移行に係る要件

① 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。
② 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。
③ LAN 端末の機種と利用用途の組み合わせごとに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テストを経て承認を得ること。
④ 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。
⑤ 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。
⑥ 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。

(4) 移行計画・前提に係る要件

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停止時間を可能な限り短くすること。
② ネットワーク及びシステムの停止を伴う作業は、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 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。また、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」や作業簡易化のためのツール等を適宜準備し、作業の説明を行うこと。
④ 現行総務省 LAN 上で稼働している各業務システムの移行時に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テスト期間について十分留意すること。
⑤ 政府共通ネットワーク及び政府共通プラットフォームとの連携を考慮すること。
⑥ 次期総務省 LAN への移行は各拠点の機器及び回線、並びに本省の各フロア、回線、及び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。

(5) 移行作業時に係る要件
① 主管課より指示があった場合は、現行運用事業者と作業調整の上で、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。
② 工事前調査結果を基に、機器設置場所への電源、LAN ケーブル、及び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。
③ 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。
④ 移行・導入の実施前に請負者は、現行運用事業者と作業調整の上で、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。
⑤ 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。
⑥ 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、請負者が現行運用事業者（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。
⑦ 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。
⑧ 移行作業時には複数箇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。
⑨ 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。
⑩ 梱包資材は請負者が撤去を行うこと。

(6) 移行作業場所に係る要件
① 本省サーバ室にすべての機器が移設できるまで、構築拠点で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。
② 構築拠点での移行作業やサービス提供時に必要な WAN 回線帯域について検討を行い提案すること。また機器及び回線は冗長構成とすること。なお移行作業やサ

ービス提供時に不都合が生じた場合は、主管課と協議の上、増速等の対策を講じるものとする。

③ 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、構築拠点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。

④ 移行で利用できる本省サーバ室の余剰ラックと余剰スペースを考慮し、移行を行うこと。

⑤ 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、新しく調達したラックを設置すること。

⑥ 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。

⑦ 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。

⑧ 必要に応じ展開する機器の転倒防止対策を行うこと。

⑨ 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。

(7) 移行のトラブル対応に係る要件

① 現行総務省 LAN と次期総務省 LAN が並行稼働する移行期間中は、臨時の移行支援窓口を開設し、ユーザからの問い合わせやトラブル対応が行える体制を用意すること。また、現行運用事業者と連携をとり、移行に関わるトラブルやユーザからの問い合わせに対応できる体制を、次期総務省 LAN へ切り替わるまで保持すること。

② 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。なお、必要に応じて移行リハーサル等を適宜計画すること。

③ トラブル発生時の切り戻し（フォールバック）手順を作成すること。なお、手順には切り戻し実施の条件、連絡体制等も記載し、迅速に復旧できるように留意すること。

④ 移行・導入作業実施後は、職員からの問い合わせやトラブル報告など多く発生することが予想されるため、移行支援窓口は通常時より多くの要員、対応時間を確保し、迅速に対応できるように体制を準備すること。発生したトラブル報告、問い合わせ等は課題管理として記録し、必要に応じて受付窓口請負事業者と情報連携すること。また、トラブル数等を定量的に報告すること。

⑤ 移行期間中は本省の隣接地域に運営場所を確保し、インターネットや電話等の通信環境を用意すること。対応要員は次期総務省 LAN の教育を受けた人員を用意すること。

⑥ 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。
⑦ 現行総務省 LAN への切り戻しが発生した場合においても、全体としては遅滞なく移行が完了できるように、適切にスケジュール等を計画すること。
⑧ 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内容の支援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。

14 引継ぎに関する事項

本業務の実施に当たって、引継ぎに係る要件を理解した上で、全ての要件を満たすこと。

(1) 業務運用開始の引継ぎ

① 本業務の運用開始に当たり、運用要員は現行運用事業者から必要な情報の引継ぎを受けること。
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、設計・構築・テスト時に主管課と協議した内容等を運用員と共有すること。
④ 請負者は、現行運用事業者から幹部出退勤サービスについて必要な情報の引継ぎを受け、総務省 LAN 提供サービスの一部として運用保守を行うこと。現行における幹部出退勤サービスの機器等詳細については、「【別紙 3】保有ライセンス・ソフトウェア一覧」を参照すること。

(2) 業務運用中の引継ぎ

① 本業務の運用期間中、次々期総務省 LAN 更改に係る調達支援事業者及び設計・構築事業者に対し、以下の情報に対する引継ぎを行うこと。
- 設計・構築並びに保守・運用に係る各種資料・情報
- 課題、リスク等の引継ぎ事項
- システム特性に伴う個別引継ぎ事項
- 改善提案等の引継ぎ事項
- 政府方針や総務省内で新たに作成された規定等

② 主管課や次々期総務省 LAN 更改に係る各事業者の要求に応じて情報提供等を行えるように、引継ぎ内容は常に整理しておくこと。

(3) 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 の各種設計・運用情報等の提供に協力すること。
④ データ移行に際しては、現行データの提供作業、打ち合わせ等に最大限協力すること。
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。

15 教育に関する事項

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。

(1) 教育要件

① 請負者は業務運用の継続性を担保するために各部局の担当者・運用員・保守員等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。
- 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・研修の結果、受講者に求める理解度の水準や、水準達成までのスケジュールを定義し、「教育訓練実施計画書」に記載すること。
③ 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。
④ 教育・研修対象者は、各部局の担当者・運用員・保守員等とする。
⑤ 教育・研修は、総務省 LAN や他システム上のデータに影響を与えないように配慮して行うこと。
⑥ 実施形式は基本的に集合研修で行うこととする。集合研修に参加できない者に対しては個別研修を実施する等のフォローを行うこと。
⑦ 新たに利用するサービスに関しては、利用開始時のトラブルを最小限に留めるため、必要に応じて運用開始前から各部局の担当者に対して教育・研修を行うこと。

また、現行総務省 LAN から利用方法が変更されたサービスについても適宜教育を行うこと。

⑧ 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。

⑨ 教育・研修実施後は、アンケートやテスト等で対象者の理解度を測り、主管課に報告すること。

⑩ 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。

⑪ 対象者の理解度が一定の水準に達するまで、繰り返し教育・研修を実施すること。

⑫ 運用員・保守員の交代、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。

⑬ 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・保守員はこのセキュリティの教育を受講していること。

16 運用に関する事項

本業務の実施に当たって、運用設計要件、運用体制要件、各種管理要件等の内容を理解した上で、全ての要件を満たすこと。また、主体業務以外にも、別調達となる「運用管理・受付窓口請負事業者」の運用管理業務と受付窓口業務（以下「受付窓口」）との作業連携を行うこと。なお、詳細な要件は、別紙 1-5「保守・運用要件詳細」の運用要件を参照すること。

(1) 本調達における主体的な業務

- 総務省 LAN の稼働状態を維持することを目的とした業務の実施
- 主管課からの業務支援の対応

(2) 運用管理・受付窓口請負事業者と連携して行う主な業務

- 職員の申請依頼の対応作業
- 総務省 LAN の稼働状態に異常を検知した際の、状況とユーザへの影響や復旧への見通しなどの情報提供
- 受付窓口では対応できない主管課からの業務支援の対応

17 保守に関する事項

本業務の実施に当たって、ソフトウェア保守要件及びハード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。また、主体業務以外にも、別調達となる「運用管理・受付窓口請負事業者」の運用管理業務と受付窓口業務において、作業における相互連携を行うこと。なお、詳細な要件は、別紙 1-5「保守・運用要件詳細」の保守要件を参照すること。

(1) 本調達における主体的な業務

- 総務省 LAN の機能維持、品質維持、設計された仕様どおりに安定稼働させることを目的とした業務の実施

(2) 運用管理・受付窓口請負事業者と連携して行う主な業務

- 受付窓口を通じて職員からの技術的な問い合わせに対する支援や、LAN 端末の故障連絡における対応作業
- 保守作業において、総務省 LAN の利用に影響のある情報の公開依頼

第4 添付資料

別紙 1-1 機能要件詳細
別紙 1-2 ルータ・スイッチ要件一覧
別紙 1-3 回線一覧
別紙 1-4 情報セキュリティ要件詳細
別紙 1-5 保守・運用要件詳細
別紙 1-6 本省・DR サイト稼働サービス一覧

【別紙1-1】機能要件詳細

第1 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。 なお、仮想化を想定しているサービスのハードウェア要件については、原則として第1 共通事項 - 3 共有サーバ・ストレージの記載のとおりとする。ただし、これらのハードウェア要件に当てはまらない仮想アプライアンス製品の提案については、各サービスの規模・性能要件、拡張性を満たすことを前提に、これを妨げるものではない。
2 共通要件
(1) 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 職員用と運用管理用等も含めて必要なライセンス数を明示すること。なお職員用として必要なユーザアカウント数は、各サービスの要件に特段の断りが無い限り7,000とする。ただし、【別紙3】保有ライセンス・ソフトウェア一覧に記載しているライセンスについては、職員用として追加購入する必要はない。
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42ヶ月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、インストールに必要なファイルやソフトウェアを用意すること。
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。
(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、保守運用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 必要な性能に対して効率的かつ可能な限り省スペースにも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 本紙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。

【別紙1-1】機能要件詳細

3 共有サーバ・ストレージ
(1) サーバ機器
ア 概要
本省及びDR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。 また、アプライアンス製品については、2 共通要件 - (2) ハードウェアの各項目と、アプライアンス製品を導入する機能要件を満たしていることを前提とし、機器等要件は規定しない。
イ 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。
③ サーバ機器は、CPU及びメモリリソースが高密度に集約された製品を選定すること。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、可用性向上や機密性保持の観点を考慮して、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。
ウ 機器等要件
(ア) 省スペース型サーバ
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 2019、RedHat Enterprise Linux 8、Windows 10が動作可能であること。
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 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。
⑤ 機器管理用のLANポートを除くサーバのLANポートは冗長化構成とすること。
⑥ 各サーバは最低でも Intel Xeon Gold 6248（2.50GHz/20コア/28MB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。
⑦ 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。
⑧ 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。
⑨ iSCSIを利用する場合は、10Gbps以上のLANポートを実装すること。
⑩ 電源モジュールは活性交換可能であること。
⑪ 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。

(2) ストレージ機器

ア 概要

本省・DR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、仮想クローンを有すること。

イ 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 DR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 DR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 管理ポートを利用して、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 DRサイト用メインストレージとバックアップストレージはDRサイト内に構築すること。
⑫ 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。
⑬ 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。
⑭ メインストレージで複数種類の記憶媒体を利用する場合は、ストレージ階層化機能を有効化すること。
⑮ ストレージ機器は、格納するデータの重要性を考慮して、必要に応じて物理的に分けて構成すること。
⑯ 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。

ウ 機器等要件

(ア) 本省メインストレージ・本省バックアップ用ストレージ・DR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。 もしくはスケジュール機能を有した機器またはソフトウェアと連携して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。 もしくはスケジュール機能を有した機器と連携して自動スケジュール設定が可能であること。
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。 ただし、バックアップ用ストレージには不要とする。
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。 ただし、バックアップ用ストレージには不要とする。
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複製する機能を有すること。 ただし、バックアップ用ストレージには不要とする。

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。 ただし、バックアップ用ストレージには不要とする。
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	総務省LAN各サービス提供に必要なディスクドライブ本数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量を構成すること。
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。 ただし、オールフラッシュストレージ製品も可とする。
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。 ただし、オールフラッシュストレージ製品も可とする。
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	SAS、ニアラインSAS又はSATAディスクを搭載する場合には、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構成とすること。 ただし、バックアップ用ストレージには不要とする
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。 ただし、バックアップ用ストレージには不要とする。
⑬	ストレージを利用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1-1】機能要件詳細

第2 総務省LANサービス

1 概要

総務省LANサービスは、次の区分によって構成される。
1.メールサービス
2.ポータルサイトサービス
3.幹部出退勤表示サービス
4.ファイル共有サービス
5.大容量ファイル転送サービス
6.コミュニケーションサービス
7.ペーパーレス会議サービス
8.プリントサービス
9.インターネット閲覧サービス
10.機密情報保護サービス

2 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、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。
メールサービスの利用規模を以下に記載する。
・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　：1,000万通/月
・ユーザメールボックスサイズ　：10GB以上/人
・共有メールボックスサイズ　:10GB以上/1共有メールボックス
・省内メールアーカイブ期間　：12ヶ月以上
・省外送信メールアーカイブ期間　：24ヶ月以上
・省外受信メールアーカイブ期間　：12ヶ月以上

(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3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、省外から受信したメールを1年以上保存できること。 また、管理者や監査担当者が監査用アーカイブの検索、閲覧を行う機能を提供すること。
⑤ 利用するメールソフトウェアに対する適切な通信方式を選択し、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クライアントは原則としてOutlookとし、導入時点での最新バージョンが利用できること。また、Web版のメールインタフェースも利用可能な構成とすること。
⑦ メールボックスは、容量超過した際に、超過の通知やメールの削除など、速やかな継続利用が可能となる運用が行えるよう構成すること。
⑧ 職員個々のメールボックス及び共有メールボックスを提供すること。
⑨ 職員からの共有メールアカウント申請によって共有メールボックスの新規作成を行うこと。
⑩ 共有メールボックスごとに、共有するアカウントの参照及び追加・削除を職員自らが実施できるように構築すること。また、共有するアカウントの参照及び追加・削除が実施可能な職員を管理できること。
⑪ 兼務職員は、本務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。
⑫ 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。
⑬ メールマガジン機能及びメールアーカイブ機能については、DRサイトでの提供は不要とする。
⑭ 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。
⑮ 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。
⑯ 仮想環境での動作を可とする。
⑰ メール配送ログの取得が可能な構成とすること。
⑱ メール送受信数、メール送受信容量（KB）は、一定間隔でのメール総数の集計や、ドメイン別メール送受信数の集計が可能な構成とすること。
⑲ メールの平均サイズの収集・集計が可能な構成とすること。
⑳ 総務省の局部課等の組織情報を反映した階層型アドレス帳機能をOutlookクライアントのアドインで提供すること。Web版のメールインタフェースでの提供は不要とする。
㉑ 不審なメールを利用者自身が簡易に報告できる機能をOutlookのアドインで提供すること。Web版のメールインタフェースでの提供は不要とする。
㉒ メールを送信する際に、送信メールを一定時間保留する・宛先や文面、添付ファイル等の再確認を促す誤送信防止機能をOutlookのアドインで提供すること。Web版のメールインタフェースでの提供は不要とする。
(3) 機器等要件
ア インターネットメール中継機能
ソフトウェア要件
① メールサービスの概要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 STARTTLSなどセキュリティを考慮した通信方式によるメール配送機能を有すること。
④ メールの送受信は適切な暗号強度を持つアルゴリズムにより暗号化が可能なこと。
ハードウェア要件
① ハードウェア要件は、本書の第1 共通事項 - 3 共有サーバ・ストレージを参照すること。

【別紙1-1】機能要件詳細

イ 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 メールサービスの概要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 政府共通ネットワーク間及び、総務省LANネットワーク内部機器間におけるメールを中継し、宛先ごとに振り分け・配送する機能を有すること。
	④ メールの宛先から政府共通ネットワーク内にあるDNSサーバを参照し、存在しなければインターネット側へ配送するなど、適切な宛先へメールを振り分け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、本書の第1 共通事項 - 3 共有サーバ・ストレージを参照すること。
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な構成とすること。共有メールボックスについても同様の容量とすること。
	② 複数の利用者がOutlook上で同時に利用できる共有メールボックスの機能を有すること。
	③ 2万人以上の規模において稼働実績がある構成とすること。
	④ ユーザごとにメールボックスの容量制限が可能な構成とすること。
	⑤ メールボックス容量が不足している利用者に対して空き容量を割り当てることで、メールストア全体容量の有効活用ができること。 メールボックス容量拡張は、利用者によるメールボックス拡張申請によって設定が行えること。
	⑥ 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構成とすること。
	⑦ 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。 また、利用者による電子メール自動転送申請によって転送が設定できること。
	⑧ メールクライアントでのメールボックスアクセス時に利用者認証を行う構成とすること。
	⑨ 利用するメールクライアントに対して適切なプロトコルを選択し、メールの取得を実施すること。
	⑩ 認証サービスとアカウント連携が可能なこと。
	⑪ 通信経路を暗号化すること。
ハードウェア要件	
	① ハードウェア要件は、本書の第1 共通事項 - 3 共有サーバ・ストレージを参照すること。
エ メーリングリスト機能	
ソフトウェア要件	
	① ユーザがメーリングリストでメールを配信できること。
	② メーリングリストの新規作成や登録ユーザアカウントの変更は、利用者のメーリングリスト設定申請によって設定が行えること。
	③ メーリングリストに対してユーザに所有権を割り当て、メーリングリストの所有者がメンバーの登録・変更・削除を簡易的に行えること。
	④ ユーザが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できること。
	⑤ メーリングリスト管理用インタフェースとしてCLI及びGUIが利用できること。
	⑥ 総務省以外のドメインのメールアドレスもメーリングリストに含められること。
	⑦ メーリングリストは「ml.soumu.go.jp」のサブドメインで提供できること。
ハードウェア要件	
	① ハードウェア要件は、本書の第1 共通事項 - 3 共有サーバ・ストレージを参照すること。

オ メールマガジン配送機能

ソフトウェア要件

① 配信ログの取得が可能なこと。
② CSVファイルなどからデータを一括で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、メール送信容量又はメール送信通数の制御が可能なこと。
④ メールマガジン配信先、配信スケジュール、配信内容などのデータを一元管理できること。
⑤ メールマガジンの配送機能は、全職員が個々の端末上から利用できること。
⑥ メールマガジンにファイルの添付が可能なこと。
⑦ メールマガジン配送先件数に上限がなく、多数の宛先に配送する場合は自動的に同時送信件数を制御し、ネットワークに過剰な負荷を与えないこと。
⑧ メールマガジン件名や配送元名を日本語で登録・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、本書の第1 共通事項 - 3 共有サーバ・ストレージを参照すること。

カ メールアーカイブ機能

ソフトウェア要件

① メールサービスの概要に記載したメール流量を処理可能であること。
② アクセスを許可された監査担当者以外の一般利用者には閲覧、削除ができない監査用メールアーカイブを利用できること。
③ アクセスを許可された監査担当者が監査用にアーカイブされたメールを検索、閲覧できること。
④ 監査用メールアーカイブは、メール受信者のアカウントが削除されてもメールが閲覧できること。
⑤ 監査用として省外へ送信したメールを2年間以上、省外から受信したメールを1年間以上、省内間のメールを1年間以上アーカイブできること。
⑥ 指定期間が経過したアーカイブメールを自動で削除できること。
⑦ 検索を容易かつ直感的に実施するため、専用のGUI管理画面を提供すること。
または、監査担当者がメールクライアントから検索・閲覧が可能なこと。
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、添付ファイル内に含まれた文字列の検索が可能なこと。

ハードウェア要件

① ハードウェア要件は、本書の第1 共通事項 - 3 共有サーバ・ストレージを参照すること。

キ 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、本書の第1 共通事項 - 3 共有サーバ・ストレージを参照すること。

3 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、電子掲示板機能、電子会議室機能、アンケート機能、会議室予約機能、スケジューラ（予定表）機能、設備予約機能、自動応答機能を提供する。
スケジューラ（予定表）機能と設備予約機能は、Outlookから直接利用できるように構成するものとする。
なお、会議室予約機能については、現行で運用している会議室仮予約・予約キャンセル処理等を実現するため、既存グループウェア製品の設備予約機能等をカスタマイズして提供することも可とする。

【別紙1-1】機能要件詳細

(2) 構築要件	
	省内ポータル（MIC-net）のコンテンツを作成し、提供すること。 ① なお、現行のMIC-netは、グループウェア上のポータル作成機能で構築されたコンテンツと、コンテンツ管理システム（CMS）を用いて利用者が作成したコンテンツ、利用者自身がHTML等で作成したコンテンツで構成されている。
	② 利用者が簡易的に省内ポータルコンテンツを作成・更新できるコンテンツ管理システム（CMS）を提供すること。 なお、CMSはDRサイトでの提供は不要とする。
	③ 職員に対して、電子掲示板、電子会議室、会議室予約、アンケート、スケジューラ（予定表）、設備予約、自動応答のサービスを提供すること。
	④ LAN端末で使用するWebブラウザ（現在はInternet Explorer 11、Mozilla Firefox）でサービスを利用可能にすること。 スケジューラ（予定表）機能と設備予約機能については、Outlookから直接利用できるように構成すること。
	⑤ 電子掲示板、電子会議室、アンケート、会議室予約のサービスを提供するためにグループウェアを導入する場合は、原則として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をすること。
	⑥ 各機能のアクセスログは、3年以上保存すること。
	⑦ 省内ポータル（MIC-net）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。
	⑧ 省内ポータル（MIC-net）に電子掲示板、総務省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。
	⑨ 省内ポータル（MIC-net）に総務省の関係部局が管理するリンクを掲載すること。
	⑩ 省内ポータル（MIC-net）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。
	⑪ 省内ポータル（MIC-net）には、現行で運用している公開情報掲載用のサイトを作成すること。
	⑫ 省内ポータル（MIC-net）内コンテンツの拡張（局部課組織サイトの追加、各種ワーキンググループ発足等に伴う専用サイト追加など）を見据えたデザインであること。
	⑬ 省内ポータル（MIC-net）には、ファイル共有サービスで提供している各組織用フォルダの使用率を掲載すること。
	⑭ 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。
	⑮ スケジュールは、省・局・部・課・室・個人に対して提供すること。
	⑯ 省内ポータル内にFAQ情報や手順書・申請書情報等を格納またはリンクすること。格納した情報・ファイルはカテゴリごとに整理され、利用者が必要な情報にアクセスしやすいように構成すること。
	⑰ 各ページへのリンク、見出し、メニュー配置、文字の大きさや色など、重要な情報が目につきやすく、必要な情報が探しやすいように職員の利便性を考慮したサイトをデザインした上でポータルサイトを構成すること。
	⑱ 部局単位で公開可能なポータルの作成機能を提供すること。作成したポータルに対するアクセス権や、公開する範囲を任意に設定できること。
	⑲ ポータルサイトサービス内の以下機能等に対して、文書内のキーワード検索が可能な全文検索機能が利用できるよう構築すること。 (1)省内ポータルサイトに格納又はリンクされる、FAQ情報や手順書、申請書情報 (2)電子掲示板機能 (3)電子会議室機能 (4)アンケート機能 (5)会議室予約機能 ただし、(4)(5)に関しては添付ファイルの検索は対象外とする。
	⑳ 省内ポータル（MIC-net）に自動応答機能（チャットボット）を導入し、職員からの総務省LANに関する各種問い合わせへの回答を支援すること。
	㉑ DRサイトにおける省内ポータル（MIC-net）は、原則としてDRサイト上で提供していることが判別できる画面構成とすること。

- (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 利用者によって作成されたMIC-netのデザインやコンテンツに対して、利用者自身が簡易的に更新できる機能を有すること。
      - ③ 利用者によるポータルの作成・更新は、ポータル管理者アカウント設定申請によって権限を与えられたユーザが行えること。
    - ハードウェア要件
      - ① ハードウェア要件は、本書の第1 共通事項 - 3 共有サーバ・ストレージを参照すること。
  - イ 電子掲示板機能
    - 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を設定し、掲示情報の登録・修正・削除・公開対象ユーザを制御できること。
      - ② 投稿する記事はユーザ自身が記事掲載期間を指定でき、記事掲載期間に達していない記事は表示されず、掲載期間になった場合に表示されること。
      - 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 投稿された情報は新着記事として表示できること。
      - ⑤ 投稿された情報の未読・既読が判別できるように表示できること。
    - ハードウェア要件
      - ① ハードウェア要件は、本書の第1 共通事項 - 3 共有サーバ・ストレージを参照すること。
  - ウ 電子会議室機能
    - ソフトウェア要件
      - ① 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、適切なアクセス権の設定が可能なこと。
      - ② 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。
      - ③ 利用者による電子会議室新規作成申請によって電子会議室の設定ができること。
    - ハードウェア要件
      - ① ハードウェア要件は、本書の第1 共通事項 - 3 共有サーバ・ストレージを参照すること。
  - エ アンケート機能
    - ソフトウェア要件
      - ① 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。
      - ② アンケートは無記名での回答が可能なこと。
      - ③ アンケートは回収期限の設定が可能なこと。
      - ④ 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。
    - ハードウェア要件
      - ① ハードウェア要件は、本書の第1 共通事項 - 3 共有サーバ・ストレージを参照すること。

オ 会議室予約機能
ソフトウェア要件
① 総務省内の共通会議室と統計局の共通会議室を対象とした会議室の予約機能を提供すること。
② 会議室の予約が可能になる日時を管理者が任意に設定できること。（例えば、職員の勤務時間に合わせ、設備予約は利用90日前の10:00から可能にする等）
③ 会議室ごとに、仮予約に対するキャンセル待ちができる機能を追加すること。
④ 予約に対して、キャンセル待ちが最大5件まで可能とすること。
⑤ キャンセル待ちをする場合は通知用のメールアドレスを3件登録可能とし、繰り上げ等、キャンセル待ちの状態に変化があった場合には登録されたメールアドレスに通知すること。
⑥ 仮予約が本予約に変更された場合には、待機しているキャンセル待ちはすべて登録から抹消すること。
⑦ 会議室毎に本予約期限を指定可能とすること。
⑧ 本予約期限時に仮予約のままとなっていた場合には、仮予約を削除すること。
⑨ キャンセル待ちの状況を一覧表示や会議室ごとの表示などで確認可能とすること。
⑩ 会議室は作成権限を与えた利用者にて作成できること。
⑪ 会議室の予約にあたっては、課室単位で提供する予約用アカウントを利用できること。
⑫ CSVファイルによる予約の一括登録ができること。なお、登録の際には登録者を特定のユーザに指定できること
⑬ 一度に予約可能な連続時間の指定ができること。
ハードウェア要件
① ハードウェア要件は、本書の第1 共通事項 - 3 共有サーバ・ストレージを参照すること。
カ ポータルサイト全文検索機能
ソフトウェア要件
① ポータルサイトサービス内の以下機能等に対して、文書内のキーワード検索が可能な全文検索機能を有すること。 (1)省内ポータルサイトに格納又はリンクされる、FAQ情報や手順書、申請書情報 (2)電子掲示板機能 (3)電子会議室機能 (4)アンケート機能 (5)会議室予約機能 ただし、(4)(5)に関しては添付ファイルの検索は対象外とする。
② 全文検索は、or検索機能を有すること。
ハードウェア要件
① ハードウェア要件は、本書の第1 共通事項 - 3 共有サーバ・ストレージを参照すること。
キ スケジューラ（予定表）機能
ソフトウェア要件
① メールクライアントから他の利用者のスケジュール閲覧と、設備（局部課内の打合せスペース、備品など）の利用予約が可能なこと。 総務省内の共通会議室と統計局の共通会議室については、会議室予約機能にて管理することとする。
② アクセス権を付与することで、他の利用者のスケジュールの閲覧・登録・削除権限の制御が可能なこと。
③ 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。
④ 利用者の新規設備の登録・改廃申請によって、設備の登録・変更・削除が可能なこと。
ハードウェア要件
① ハードウェア要件は、本書の第1 共通事項 - 3 共有サーバ・ストレージを参照すること。

ク 自動応答機能

ソフトウェア要件

① チャットボットに登録するFAQはExcel形式で管理でき、1,000件以上登録できること。
② ユーザの過去の質問を踏まえた学習機能を有すること。
③ シナリオに沿ってユーザが質問を絞り込み、回答を得られること。加えて、自然言語での自由記述質問も可能なこと。
④ 類義語の定義が可能なこと。また、類義語の使用有無を設定により切り替えることが出来ること。
⑤ ユーザインタフェースをグループウェア機能のウィジェットとして提供できること。
⑥ ユーザ利用状況を分析できること。
⑦ インターネットに接続できない環境で動作可能であること。

ハードウェア要件

① ハードウェア要件は、本書の第1 共通事項 - 3 共有サーバ・ストレージを参照すること。

4 幹部出退勤表示サービス

(1) 概要

大臣以下本省内幹部の出退勤情報をリアルタイムに反映し、職員が閲覧できる機能を提供する。出退勤情報は省内各所に設置する幹部用表示専用ディスプレイに表示させ、総務省LAN端末のWebブラウザで閲覧できるように、ポータルサイトからリンクする。
なお、本サービスは現行運用中に別途調達した機器・ソフトウェアを継続利用すること。

(2) 構築要件

① 請負者は、本サービスの保守・運用を適切に行えるようにカスタマイズすること。

(3) 機器等要件

ソフトウェア要件

① 「【別紙3】保有ライセンス・ソフトウェア一覧」参照。

ハードウェア要件

① 「【別紙3】保有ライセンス・ソフトウェア一覧」参照。

【別紙1-1】機能要件詳細

5 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である電子データを保存・共有するため、以下の機能を有するファイル共有サービスを提供する。
・ファイル共有（組織用・個人用2種類の共有フォルダ）
・ファイル共有全文検索（組織用共有フォルダ対象）

(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40GB以上/アカウント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DRサイトで提供すること。
⑧ ファイル共有機能において、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。
⑬ 本省被災時においてもサービスを継続するため、DRサイトでもサービスを継続できるよう構成すること。
⑭ 組織用共有フォルダに対して、ファイル名及びフォルダ名だけでなく、ファイル内の文字列からキーワード検索が可能な全文検索機能を提供すること。
⑮ 全文検索サーバは、高速検索を実現するために複数台による分散構成とすること。また、ファイル共有サービスを提供するストレージと同じサイトに設置すること。

(3) 機器等要件

ア ファイル共有機能

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 容量超過時にメール通知が可能であること。
⑤ 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。
⑥ 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。
⑦ 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。
⑧ 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。

ハードウェア要件

① ハードウェア要件は、本書の第1 共通事項 - 3 共有サーバ・ストレージを参照すること。

イ ファイル共有全文検索機能	
ソフトウェア要件	
①	組織用共有フォルダに対して、ファイル名及びフォルダ名だけでなく、ファイル内の文字列（本文）からキーワード検索ができること。
②	Officeファイル（Word、Excel、PowerPoint）、PDFファイル、及びテキストファイルが検索対象であること。
③	あいまい検索（自然文検索）機能を有すること。
④	ファイルの種類や更新日付からの検索（属性検索）機能を有すること。
⑤	キーワード検索、あいまい検索、及び属性検索から、検索条件を任意に組合せることが可能であること。
⑥	検索結果を指定した条件で更にフィルタリングできること。
⑦	検索結果を任意のフィールドで並び替えできること。
⑧	検索対象のインデックス処理実行中においても、検索機能が利用できること。
⑨	全文検索機能の利用状況を可視化できる機能を有すること。
⑩	全文検索のログを集計し、レポートとして抽出できる機能を有すること。
⑪	検索結果をサムネイル表示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、本書の第1 共通事項 - 3 共有サーバ・ストレージを参照すること。
6 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で、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、大容量ファイル転送サービスを提供する。
(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、仮想デスクトップ環境、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け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、インターネット接続用ネットワークの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できること。
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	省外の関係者がファイルダウンロード及びファイルアップロードを行う際は、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3年以上保存すること。ただし他サービスにて実現することも可能とする。
⑪	ファイルのアップロード時には、ウイ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。
⑬	本省被災時においてもサービスを継続するため、DRサイトでもサービスを継続できるよう構成すること。

(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をメールにて通知することが可能なこと。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、パスワード認証ができること。
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できること。
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 ファイルのダウンロード時に振る舞い型マルウェアを検査できること。ただし、他サービスにて実現することも可能とする。
⑧ 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。
⑨ SSL通信が可能であること。
⑩ 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。
⑪ 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。
⑫ 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。
⑬ 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。
⑭ 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。
⑮ 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。
⑯ 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。
⑰ 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。
⑱ 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。
⑲ システムの利用状況や統計情報を参照可能であること。
⑳ 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。
㉑ 大容量ファイル転送サービスを利用する職員と省外の関係者を合わせて最大で20,000ユーザに対応できること。
㉒ Internet Explorer、Microsoft Edge、Google Chrome、Mozilla Firefox、Safariから利用可能であること。
㉓ ストレージ接続プロトコルとして、iSCSI、NFSに対応できること。
ハードウェア要件
① ハードウェア要件は、本書の第1 共通事項 - 3 共有サーバ・ストレージを参照すること。

【別紙1-1】機能要件詳細

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。
(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3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 総務省職員が、省外の関係者をWeb会議に招待できるように構成すること。
	⑥ 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。
	⑦ 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。
	⑧ Web会議において映像の表示・音声の出力が問題なく行えるように機器構成、ネットワーク構成、運用設計を行うこと。
	⑨ 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。
	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3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、1,000名以上とする。
	⑬ 一人が最大1,000名の参加者に対して音声と映像を発信する形態の大規模Web会議を行えるように構成すること。 大規模Web会議利用時においても通常のWeb会議機能を提供できること。
	⑭ Web会議の会議室の予約は、LAN端末で使用するWebブラウザ（Internet Explorer、Microsoft Edge、Google Chrome、Mozilla Firefox）から可能であること。
	⑮ 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。
	⑯ 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。
	⑰ 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。
	⑱ 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。
	⑲ 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。
	⑳ 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。
      - 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共有サービスを使ってファイルを共有することができること。
      - ⑥ 会話中の相手への直接ファイル添付を禁止できること。
      - ⑦ サーバに3年間以上メッセージの記録が残せること。
      - ⑧ メールサービスと連携して会話の履歴を残し、後から閲覧できること。
      - ⑨ 会話のトピックごとにチャットルームを作成できること。
また、利用者によるチャットルーム新規作成申請によって設定できること。
      - ⑩ 作成されたチャットルーム内で、さらに会話のトピックを細分化できること。
      - ⑪ チャットルームにアクセスできる利用者を制限できること。
      - ⑫ チャットルームに記録されたメッセージについては、別のユーザにアクセス権を与えて閲覧させられること。
    - ハードウェア要件
      - ① ハードウェア要件は、本書の第1 共通事項 - 3 共有サーバ・ストレージを参照すること。
  - 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、本書の第1 共通事項 - 3 共有サーバ・ストレージを参照すること。

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共有、閲覧する機能を有すること。
	⑤ 会議画面は1,920×1,080ピクセル以内で表示できること。
	⑥ 会議開催中にメッセージ交換機能が利用できること。
	⑦ 会議開催中に参加者間で資料の共有ができること。
	⑧ 総務省職員全員に会議を主催できる個別のIDを付与できること。
	⑨ 省内のメンバを指定してWeb会議が開催できること。
	⑩ 総務省職員が省外関係者のメンバを招待してWeb会議が開催できること。
	⑪ 利用状況のログを日、週、月ごとに取得できること。
	⑫ 1,000以上の会議を同時に開催できること。（WAN回線帯域を考慮しない状況）
	⑬ 一人が最大1,000名の参加者に対して音声と映像を発信する形態の大規模Web会議を行えること。
	ハードウェア要件
	① ハードウェア要件は、本書の第1 共通事項 - 3 共有サーバ・ストレージを参照すること。
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。 LAN端末及び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。
(2) 構築要件	
	① 総務省LANの無線LAN環境を利用して、LAN端末及び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 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サービス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 複数会議に対して同時に合計300台のタブレット型端末から利用可能であること。
	⑨ 1会議に対して100台のタブレット型端末が同時に利用可能であること。
	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。
	⑫ 資料閲覧画面において、画面のにじみ等の苦情があった場合は対策を行うこと。

(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	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。
⑤	会議開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。
⑥	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 Excel （xls、xlsx） ・ Microsoft PowerPoint （ppt、pptx） ・ JPEG ・ PNG ・ TIFF ・ Windowsビットマップ （bmp） ・ GIF ・ テキスト （txt）
⑦	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。
⑧	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。
⑨	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。
⑩	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。
⑪	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。
⑫	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。
⑬	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。
⑭	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。
⑮	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。
⑯	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。
⑰	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。
⑱	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。
⑲	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。
⑳	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。
㉑	会議中に作成したマーキングやメモの情報は、会議終了後に会議開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。
㉒	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。
㉓	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。
㉔	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。
㉕	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。

				㉖ 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。
				㉗ 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
				㉘ 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。
				㉙ 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。
				㉚ 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、本書の第1 共通事項 - 3 共有サーバ・ストレージを参照すること。
		イ タブレット型端末		
			ソフトウェア要件	
				① タブレット型端末のOSは、ペーパーレス会議サービスが問題なく利用できるバージョンであること。
			ハードウェア要件	
				① ペーパーレス会議サービスを利用するiOS搭載のタブレット型端末は、iPad 10.2インチを300台用意すること。
				② タブレット型端末のネットワークはWi-Fi（802.11a/b/g/n/ac）が利用可能であること。また、携帯電話機能を有しないこと。
				③ のぞき見防止フィルタを本体台数分添付すること。なお、のぞき見防止フィルタはタブレット型端末に貼付された状態で納品すること。
				④ タブレット型端末対応の保護ケースを本体台数分添付すること。なお、保護ケースはタブレット型端末に装着された状態で納品すること。
				⑤ タブレット型端末の収容ラックを用意すること。複数ラックを結合させることも可能とする。
				⑥ 複数のタブレット端末が同時に充電可能な収容ラックを用意すること。台数についてはペーパーレス会議の運用に支障がでないように必要な数を用意すること。
				⑦ タブレット型端末本体の故障時には引き取り修理を行うこと。ただし、保守はタブレット型端末メーカが対応可能な期間において実施するものとする。
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。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。

(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 ユーザは自身のLAN端末に割り当てたいLAN複合機・LANプリンタを自ら選択できること。なお、割り当てる際には、組織階層ごとにまとめられたLAN複合機・LANプリンタ一覧を表示し、必要なLAN複合機・LANプリンタにチェックを入れるなど、ユーザの操作が簡易となる構成とすること。
	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、原則、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。なお、既存ICカードリーダを利用しない場合は、主管課の承認を得た上で、請負者の責任と負担において機器等を準備すること。
	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可能とする構成とすること。
	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、業務に支障が出ない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 職員IDとICカードの識別情報を含むユーザ管理情報を、管理サーバ上のデータベースと認証サービスで同期すること。
	⑨ 認証サービス及びユーザ管理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。
	⑩ 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、本省と拠点間の回線帯域及び本省に設置するプリントサーバの性能に余剰を設ける等の対策を行い、他の総務省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。 なお、拠点にプリントサーバを設置する場合、同一筐体上で他のサービスを提供することも可能とする。
	⑪ 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。
	⑫ 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。 また、LAN複合機利用者カードの情報を変更・削除できること。
	⑬ LAN複合機及びLANプリンタの制御に係る各種設定を行うために、Webベースの操作画面を提供すること。
	⑭ 管理サーバ上のデータベースをリカバリ用にバックアップすること。
	⑮ 本省や拠点の被災時等、通常利用できない場合は、USBケーブル経由での印刷を行えること。

(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、本書の第1 共通事項 - 3 共有サーバ・ストレージを参照すること。
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 出力機器のメーカ及び機種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。
⑤ LAN端末で特定の出力機器を指定せずに印刷指示を行い、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。その際、部数・片面/両面・ホッチキス等を指定できること。 また、LAN複合機・LANプリンタのメーカと異なるプリンタドライバを利用する場合には、プリントサービスにて自動変換を行い出力が行える機能を有すること。
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 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。
⑩ 既存のFeliCaカードを利用できること。必要に応じて、設定を行うこと。
⑪ 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。
⑫ ユーザごとにプリント可能な出力機器を設定できること。
⑬ 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。
⑭ 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。
⑮ 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。
⑯ 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：本省 401台・地方拠点 395台、LANプリンタ数：本省 114台・地方拠点 99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。
② ハードウェア要件は、本書の第1 共通事項 - 3 共有サーバ・ストレージを参照すること。

【別紙1-1】機能要件詳細

10 インターネット閲覧サービス	
(1) 概要	インターネットへのWebアクセス時にLAN端末、業務システムセグメントの端末及び仮想デスクトップがマルウェアに感染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環境として、インターネット閲覧サービスを提供する。ユーザ数は7000人とする。 LAN端末及び業務システムセグメントの端末及び仮想デスクトップからインターネットにアクセスする際は、本サービスからアクセスする。
(2) 構築要件	
	① 総務省LAN内部からインターネット閲覧環境を分離し、インターネットへは通信できない構成とすること。
	② 本サービスを利用する端末から、Webアクセスが可能となる機能を提供すること。
	③ 本サービスを用いてインターネットへのWebアクセス時にインターネット閲覧環境側がマルウェア感染しても、本サービスを利用する端末は感染しないこと。
	④ 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。
	⑤ インターネットからダウンロードしたデータを本サービスを利用する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。
	⑥ インターネットからダウンロードしたデータは、ダウンロードを行った利用者のみがアクセスできること。
	⑦ インターネットからダウンロードしたデータにアクセスする際の認証は、シングルサインオンを行うこと。
	⑧ インターネット閲覧サービスはインターネット接続ネットワーク内のDMZ等の内部ネットワークとは分離されたネットワークに配置すること
	⑨ 同時利用者数7,000以上を考慮した性能を担保すること。
	⑩ ファイル共有領域は、インターネット閲覧サービスがアクセス可能な領域と、本サービスを利用する端末がアクセス可能な領域を別々の領域として提供すること。 また、それぞれ1TB以上の容量を確保すること。
	⑪ ファイル共有領域は、以下のディレクトリ構成とすること。 ・本サービスからアクセス可能なダウンロードファイル格納ディレクトリ ・本サービスからアクセス可能なアップロードファイル格納ディレクトリ ・本サービスを利用する端末からアクセス可能なダウンロードファイル格納ディレクトリ ・本サービスを利用する端末からアクセス可能なアップロードファイル格納ディレクトリ ・管理者のみアクセス可能な隔離ディレクトリ
	⑫ ファイルマルウェア対策機能は、インターネット閲覧サービス用のダウンロードファイル格納ディレクトリを定期的に検査し、格納されているダウンロードファイルの不正プログラム検出を行うこと。 また、不正プログラムが検出されなかったファイルを合格ファイルとし、本サービスを利用する端末用のダウンロードファイル格納ディレクトリに移動すること。

	⑬ ファイルマルウェア対策機能は、本サービスを利用する端末用のアップロードファイル格納ディレクトリを定期的に検査し、格納されているアップロードファイルの不正プログラム検出を行うこと。 また、不正プログラムが検出されなかったファイルを合格ファイルとし、インターネット閲覧サービス用のアップロードファイル格納ディレクトリに移動すること。
	⑭ ファイルマルウェア対策機能による検査で不合格となったファイルは、管理者がアクセスできる隔離用のディレクトリに移動すること。 また、不合格ファイルを検出した場合は、管理者宛に通知すること。
	⑮ インターネット閲覧サービスを用いたファイルダウンロード完了時に、コミュニケーションサービスと連携してユーザに通知すること。
	⑯ インターネット閲覧サービスはDRサイトでの提供を必須としない。ただし、DRサイトでもインターネットの閲覧は可能な構成とすること。
(3) 機器等要件	
ア インターネット閲覧機能	
ソフトウェア要件	
	① インターネット閲覧サービス起動時に、ID/パスワード等による認証ができること。なお、認証サービスと連携し、利用者がパスワード等の入力を行うことなく利用できること。
	② インターネット閲覧サービスで表示したWebページ内のコンテンツをコピーして、他のアプリケーションにペーストする操作を禁止できること。ただし、インターネット閲覧サービス内でのコピー及びペーストは許可できること。
	③ 他のアプリケーションとインターネット閲覧サービスとの間では、文字列のコピー及びペーストを許可できること。
	④ インターネット閲覧サービスはユーザ自身によるWebページのブックマーク登録を許可できること。
	⑤ インターネット閲覧サービスは、アプリの領域内にダウンロードした PDF ファイルや Microsoft Officeファイル（Word、Excel、PowerPoint ）を、別のアプリケーションに引き渡すことなく、インターネット閲覧サービスのファイルビューアーを用いて簡易表示できること。
	⑥ インターネット閲覧サービスで参照したファイルをプリンターを利用して印刷できること。
	⑦ インターネット閲覧サービスよりインターネット閲覧サービス用のファイル共有領域へアクセスし、ファイルの参照及び書き込みができること。
ハードウェア要件	
	① ハードウェア要件は、本書の第1 共通事項 - 3 共有サーバ・ストレージを参照すること。

イ ファイルマルウェア対策機能

ソフトウェア要件

①	検査対象はインターネット閲覧サービス用のファイル共有領域とし、当該領域を検査可能なセグメントに本機能を導入すること。
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、振る舞い検知として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できること。
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	ファイル共有領域との通信は、CIFS、NFS、SMBをサポートすること。
⑥	指定したファイル共有領域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	70,000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製造元へ提供する機能を持つ場合は、設定により無効化できること。
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。

ハードウェア要件

①	ハードウェア要件は、本書の第1 共通事項 - 3 共有サーバ・ストレージを参照すること。

11 機密情報保護サービス

(1) 概要

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、機密情報保護サービスを提供する。
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・印刷等の機能を利用できるよう制御する。

- 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。

(2) 構築要件

①	ストレージ機器と連携し、ファイル共有領域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。
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。
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3年以上保存し、検索、閲覧を行えるよう構成すること。 なお、他サービスにて実現することも可とする。
⑫	自動的に暗号化するファイルは、次の拡張子を持つものを対象とすること。 doc、docx、xls、xlsx、ppt、pptx、pdf、jtd、jtt、jtdc、jttc、txt、text、csv、gif、jpeg、jpg、jpe、jiff、jfi、png、tif、tiff、bmp、mp4、wmv、mp3、wma、dib。
⑬	機密情報保護を行うに当たり、対象ユーザ数は450 名とすること。
⑭	データベースに格納されているデータに対して暗号化を実施すること。なお、バックアップデータやトランザクションデータ等についても暗号化を実施すること。

(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 ファイルを格納するとともに、自動的に暗号化される専用フォルダを準備すること。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 暗号化ファイルは、適切な権限を有した利用者のみが利用できること。
	⑬ 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。
ハードウェア要件	
	① ハードウェア要件は、本書の第1 共通事項 - 3 共有サーバ・ストレージを参照すること。
第3 サービス基盤	
1 概要	
	サービス基盤は、次の区分によって構成される。 1.認証サービス 2.テレワークサービス 3.私物等端末リモートアクセスサービス 4.デバイス管理サービス 5.資源管理サービス 6.情報不正出力防止サービス

2 認証サービス	
(1) 概要	
	総務省職員等のアカウント情報を管理し、各サービスへの接続時に認証及びアクセス権の付与、証明書の発行・配布やライセンス認証等を行う。 認証サービスは以下の機能で構成されている。 ・総務省LANユーザ情報管理機能 ・ディレクトリ機能 ・生体認証機能 ・認証局機能 ・ライセンス認証機能 ・無線LAN認証機能 ・OTP認証機能 ・証明書認証機能 ・証明書配布機能
(2) 構築要件	
ア 総務省LANユーザ情報管理機能	
	総務省共通基盤支援システムから定期的に取得した情報、申請管理サービスから連携されたアカウント情報及びパスワード情報等を管理し、以下の関連するサービス又は機能に配付・連携すること。また、必要に応じて、その他のサービス又は機能にも各種情報を配付・連携すること。 ・ディレクトリ機能 ・生体認証機能 ・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 ・申請管理サービス ・会議室予約機能（ポータルサイトサービス） ・階層アドレス帳（メールサービス） ・プリントサービス ・大容量ファイル転送サービス ・インシデント管理機能（運用支援サービス）
①	
②	職員が共有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	職員が共有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によるユーザ認証を行うこと。
④	30日以上の猶予期間を設けて、不要となったアカウント情報及び組織情報を削除すること。また、関連するサービス・機能が有する、該当アカウントに係るリソースも併せて削除すること。
⑤	関連サービスとの連携処理が何らかの原因で途中停止した場合、再実行を行うことで情報の整合をとること。
⑥	姓名変更が発生したユーザアカウントの個人共有フォルダ名を変更すること。
⑦	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・削除すること。
⑧	本機能はDRサイトでの提供を必須としない。

【別紙1-1】機能要件詳細

イ ディレクトリ機能	
	① 認証基盤として、ユーザやコンピュータを一元管理し、各サービスを利用する際に本人を認証、アクセス権を付与する。
	② 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。
	③ 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。
	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。
	⑤ 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。
	⑥ 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アクセス管理を行うこと。
	⑦ ユーザアカウントは、組織ごとの階層管理を行うこと。
	⑧ 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・削除すること。
	⑨ 必要に応じて、特定のグループにのみ個別のパスワードルールを適応すること。
	⑩ 認証の履歴を3年以上保存すること。なお、他サービスにて実現することも可とする。
ウ 生体認証機能	
	① LAN端末でログオン認証する際、顔認証により個人を識別し、認証・権限付けを行えること。顔認証が利用できない場合には、例外的に別の認証で代替できること。
	② LAN端末が総務省LANのネットワークに接続していない場合、LAN端末に保存されている生体認証情報のキャッシュで端末にログオンすること。
	③ 総務省共通基盤支援システムから連携される（総務省LANユーザ情報管理機能を経由）情報に基づき、ID/パスワード認証を可能とすること。
	④ ディレクトリ機能の情報を利用し、LAN端末及び仮想デスクトップから総務省LANの各種サービス及び認証が必要な機器（プロキシ等）の接続時、シングルサインオンを行うこと。
	⑤ ディレクトリ機能の情報を利用し、LAN端末及び仮想デスクトップから以下の個別業務システムの利用時、シングルサインオンを行うこと。また、必要に応じて、その他の個別業務システムにも対応すること。 ・電気通信行政情報システム（STARS） ・職員等利用者共通認証基盤（GIMA） ・行政相談総合システム ・総務省共通基盤支援システム
	⑥ ユーザが所定の回数以上認証を失敗した場合、アカウントをロックすること。 また、ロックされたアカウントは、管理者によるロックの解除、または、所定の時間が経過することで再度利用可能となること。
	⑦ 認証の履歴を3年以上保存すること。なお、他サービスにて実現することも可とする。
エ 認証局機能	
	① 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。
	② ルート証明書の秘密鍵の侵害を防ぐよう、ルート認証局と下位認証局を構成すること。
	③ サーバ証明書及び無線LANサービスで利用する端末証明書を発行すること。
	④ 証明書の失効リストを管理すること。
	⑤ ルート認証局は本省でのみ提供すること。
オ ライセンス認証機能	
	① LAN端末・ウイルスチェック用端末のWindows及び各Windows ServerのOSライセンス認証、Microsoft Officeのライセンス認証を行うこと。
	② ライセンス認証サーバはMicrosoftからライセンス認証を受け、各種端末・各Windows Serverのライセンス認証を行うこと。

		カ 無線LAN認証機能	
			① 無線LANサービスと連携し、LAN端末、タブレット型端末（ペーパーレス会議システム用）、ウイルスチェック用端末が無線LANに接続した際の証明書認証を行うこと。
			② 無線LANアクセスポイントが設置された場所であれば、拠点を問わず総務省無線LANに接続可能であること。
			③ サーバ証明書を無線LAN認証サーバに保持することにより、偽のアクセスポイントへの接続を防止すること。
		キ OTP認証機能	
			① テレワークサービス（LAN端末テレワーク機能・仮想デスクトップ機能）・私物等端末リモートアクセスサービスと連携し、支給端末（LAN端末・Windowsタブレット）・私物等端末（PC・モバイル）が省外から総務省LANに接続した際、ワンタイムパスワード認証を行うこと。
			② 連携するサービスが提供する認証画面に、ワンタイムパスワード認証の入力欄を表示させること。
			③ 連携するサービスが提供する認証画面に、毎回異なる文字列を表示すること。表示された文字列から、ユーザが設定したPIN番号に対応する文字を確認し、ワンタイムパスワードとして入力すること。
			④ 連携するサービスが提供する認証画面に、ワンタイムパスワードに利用する文字列を表示できない場合、Eメールやソフトウェアトークン等でワンタイムパスワードをユーザに通知すること。
			⑤ 職員の1つの職員IDに対して、初期PINを付与すること。
			⑥ 初期PINを変更してからサービスを利用すること。
			⑦ 初期PINの変更は、LAN端末上のブラウザから、ポータルサイトにアクセスして初期PINを変更すること。
			⑧ ワンタイムパスワード認証を一定回数失敗した場合、アカウントをロックすること。
			⑨ ワンタイムパスワード認証を処理するサーバを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。 ただし、データベースは省内に配置すること。
		ク 証明書認証機能	
			① テレワークサービス（仮想デスクトップ機能）と連携し、支給端末（Windowsタブレット）・私物端末（PC）が省外から総務省LANに接続した際、証明書認証を行うこと。
		ケ 証明書配布機能	
			① 私物端末（PC）に対して証明書を配布すること。
			② ユーザが事前申請し、管理者が承認した上で、私物端末（PC）に安全かつ適切に証明書を配布すること。
			③ 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 総務省LANユーザ情報管理機能	
			ソフトウェア要件
			① 6200人分のアカウント情報の設定変更処理を6時間以内に終了できるパフォーマンスを持つこと。
			② 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。
			③ 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。
			④ 共有アカウントのパスワードを変更するGUIを持つこと。
			⑤ 主管課がすべての共有アカウントのパスワード初期化を行う機能を持つこと。
			⑥ 共有アカウントのパスワード変更履歴が保存されること。
			ハードウェア要件
			① ハードウェア要件は、本書の第1 共通事項 - 3 共有サーバ・ストレージを参照すること。

イ 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、本書の第1 共通事項 - 3 共有サーバ・ストレージを参照すること。

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ができること。
② 生体情報は暗号化され、安全かつ適切に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 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。
⑤ 管理者が操作した管理ソフトの操作ログを取得可能であること。
⑥ Webブラウザで提供されるサービスに対し、ユーザに代わってID/パスワードの入力を行えること。
ただし、インターネット閲覧サービスの専用ブラウザ上で提供されるWebサービスは除く。
⑦ 既存の全LAN端末で利用できること。

ハードウェア要件

① ハードウェア要件は、本書の第1 共通事項 - 3 共有サーバ・ストレージを参照すること。

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-256以上、鍵長2048ビット以上の証明書のみ発行すること。
③ 有効期限が10年以上の証明書を発行できること。
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 ハードウェア要件は、本書の第1 共通事項 - 3 共有サーバ・ストレージを参照すること。

オ ライセンス認証機能

ソフトウェア要件

① Windows 10・Windows Server 2019・Microsoft Officeのライセンス認証が行えること。

ハードウェア要件

① ハードウェア要件は、本書の第1 共通事項 - 3 共有サーバ・ストレージを参照すること。

カ 無線LAN認証機能

ソフトウェア要件

① 無線LANコントローラと連携し、証明書認証を行うこと。
② RADIUSサーバとして機能すること。

ハードウェア要件

① ハードウェア要件は、本書の第1 共通事項 - 3 共有サーバ・ストレージを参照すること。

キ OTP認証機能

ソフトウェア要件

① Windows 10のログオン認証画面にワンタイムパスワード認証の入力画面が表示できること。
② 省内でLAN端末を利用する場合には、ワンタイムパスワード認証を要求しない設定が可能であること。

ハードウェア要件

① ハードウェア要件は、本書の第1 共通事項 - 3 共有サーバ・ストレージを参照すること。

ク 証明書認証機能

ソフトウェア要件

① 認証に用いるアカウントは7,000以上登録できること。
② アカウントの管理は個別のほか、CSVファイルからの一括登録・変更・削除ができること。
③ テレワークサービス（仮想デスクトップ機能）で利用する支給端末（Windowsタブレット）・私物端末（PC）の端末数以上の証明書を発行できること。

ハードウェア要件

① ハードウェア要件は、本書の第1 共通事項 - 3 共有サーバ・ストレージを参照すること。

ケ 証明書配布機能

ソフトウェア要件

① 端末証明書を配布する際の外部公開インタフェースに、製品名や製品ベンダの名称等、製品を特定可能な情報が表示されないこと。

ハードウェア要件

① ハードウェア要件は、本書の第1 共通事項 - 3 共有サーバ・ストレージを参照すること。

3 テレワークサービス

(1) 概要

テレワークサービスは以下の機能で構成されている。
・LAN端末テレワーク機能
・仮想デスクトップ機能

(2) 構築要件

ア LAN端末テレワーク機能

① 省外からLAN端末を用いて、総務省LANサービス及び業務システムを利用できること。利用できないサービス・機能がある場合は、客観的かつ合理的な理由を添えて主管課に説明の上、承認を得ること。
② 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。
③ LAN端末が省外で接続していると判定した場合、自動で外部接続に係るサーバに接続すること。
④ LAN端末が省外で接続していると判定した場合、外部接続に係るサーバへの接続以外の通信を行わないこと。ただし、海外出張での利用時には、申請に基づきWeb認証等を伴う外部ネットワークへの接続も可能にすること。
⑤ ポリシーにより、利用できるサービス・機能を制御すること。
⑥ 端末ログオン時、生体認証を行うこと。
⑦ 総務省LANへの接続時、認証サービスと連携し、端末証明書認証・ワンタイムパスワード認証を行うこと。
⑧ 端末の盗難や紛失等の事故が発生した場合、端末証明書を失効にすることで、本サービスを利用できないよう構成すること。
⑨ 資源管理サービスと連携し、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。
また、適用状況がポリシーに違反している場合、LAN端末に通知し、必要に応じて特定の宛先とのみ通信可能とするよう制御すること。
⑩ 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。
⑪ 本省・DRサイトは、それぞれ最大同時接続で2,000人・1,500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。
⑫ 接続に関するログを3年以上保存すること。

【別紙1-1】機能要件詳細

イ 仮想デスクトップ機能	
①	仮想デスクトップ環境を用いて、総務省LANサービス及び業務システムを利用できること。利用できないサービス・機能がある場合は、客観的かつ合理的な理由を添えて主管課に説明の上、承認を得ること。 なお、現時点では、システム領域を共有する仮想デスクトップ環境の場合、機密情報保護サービス及び個別のアプリケーションをインストールする必要がある業務システムは利用できないことを理解している。
②	私物端末（PC・モバイル）及び支給端末（Windowsタブレット）上のOSから、総務省LAN上の仮想デスクトップ環境に接続すること。
③	利用可能な私物端末（PC）はWindows 10及びmacOS搭載の端末、私物端末（モバイル）はiOS及びAndroid搭載の端末とすること。
④	情報漏えいを防止するため、仮想デスクトップ環境と私物端末（PC・モバイル）及び支給端末（Windowsタブレット）のローカル環境間におけるデータの共有及びテキストのコピー＆ペースト、印刷を禁止すること。
⑤	私物端末（PC・モバイル）及び支給端末（Windowsタブレット）から、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。
⑥	ポリシーにより、利用できるサービス・機能を制御すること。
⑦	支給端末（Windowsタブレット）は仮想デスクトップ機能のみ利用可能とし、その他アプリケーションの利用及びローカル環境へのデータの保存を禁止すること。
⑧	総務省LANへの不正な接続を検知するため、仮想デスクトップに接続された際に、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。
⑨	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。
⑩	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ること。
⑪	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。
⑫	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2,000ユーザ分用意すること。
⑬	仮想デスクトップ環境のDRサイトにおいて、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2,000ユーザ分用意すること。
⑭	仮想デスクトップをホストする仮想基盤は、十分な性能を確保するために適切にサイジングを行うこと。また、システム領域用のディスクについては、SSDを採用すること。
⑮	認証サービスと連携し、通常使用しているアカウントのユーザID及びパスワードで認証すること。
⑯	認証サービスと連携し、パスワードを設定回数以上間違えた場合、自動的にアカウントをロックすること。
⑰	総務省外から外部接続環境に接続する際には、通信を暗号化した接続を行うこと。
⑱	ゲートウェイ装置への接続時、認証サービスと連携し、ID/パスワード認証・ワンタイムパスワード認証を行うこと。また、接続された端末を確認するために、端末証明書認証等を行うこと。
⑲	ゲートウェイ装置から仮想デスクトップに接続した際の認証は、シングルサインオンを行うこと。
⑳	端末の盗難や紛失等の事故が発生した場合、端末証明書の失効等を行うことで、本サービスを利用できないよう構成すること。
㉑	ゲートウェイ装置への接続の際に、私物端末（PC・モバイル）及び支給端末（Windowsタブレット）に対して、ポリシーの順守状況を確認すること。
㉒	ゲートウェイ装置を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。
㉓	本省は最大同時接続で1,200人、DRサイトは最大同時接続で1,000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。
㉔	接続に関するログを3年以上保存すること。
㉕	Windowsタブレットを20台手配すること。
㉖	Windowsタブレットで利用する携帯電話回線（データ通信容量が10GB以上/月）を端末の台数分手配すること。
㉗	一定期間利用していないユーザに対してメールで通知すること。更に一定期間利用していない場合はアカウントを停止すること。
㉘	ゲートウェイ装置は、サービス基盤の他サービスのゲートウェイ装置と共用してもよい。

- (3) 機器等要件
  - ア LAN端末テレワーク機能
    - ソフトウェア要件
      - ① 総務省外でLAN端末をインターネットに接続した場合、自動で総務省LANに接続できること。
      - ② 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。
      - ③ システム管理用インタフェースとして、CLI及びGUIを提供すること。
      - ④ 固定回線及びモバイル回線から利用可能なこと。
      - ⑤ 本省及びDRサイトに設置するサーバにおいては、それぞれ最大接続数が2,000以上・1,500以上に耐える構成とすること。
    - ハードウェア要件
      - ① ハードウェア要件は、本書の第1 共通事項 - 3 共有サーバ・ストレージを参照すること。
  - イ仮想デスクトップ機能
    - (ア)仮想デスクトップ
      - ソフトウェア要件
        - ① システム管理用インタフェースとして、CLI及びGUIを提供すること。
        - ② 私物端末（PC・モバイル）及び支給端末（Windowsタブレット）に転送された画面上で仮想デスクトップの操作が可能であること。
        - ③ 通信を暗号化して接続が可能なこと。
        - ④ 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。
        - ⑤ 仮想デスクトップ機能利用時には、私物端末（PC・モバイル）及び支給端末（Windowsタブレット）に保存される情報は総務省LANとの接続に必要な設定に限定され、任意のデータの記録ができないこと。
        - ⑥ メンテナンスやトラブルシューティングのため、各仮想デスクトップをリモートから操作する機能を持つこと。その際、ユーザの操作画面を共有して操作ができること。
        - ⑦ 各仮想デスクトップのプロセス単位で、リソースの負荷状況を確認でき、必要に応じて強制的にプロセスをダウンさせる事が出来ること。また、本機能の権限を持つ利用者を限定できること。
        - ⑧ ICA、PCoIP、Blast Extreme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、本書の第1 共通事項 - 3 共有サーバ・ストレージを参照すること。
    - (イ)ゲートウェイ装置
      - ソフトウェア要件
        - ① Windows・macOSの端末に対して、ウイルス対策製品の有無やOSの種類などのポリシー順守状況を確認できること。
        - ② iOS・Androidの端末に対して、root化・Jailbreakの有無などのポリシー順守状況を確認できること。
        - ③ ポリシー順守状況を確認するためのアプリケーションが必要な場合、ゲートウェイ装置に接続した際に、端末にダウンロードできること。
        - ④ PCoIPプロキシやBlast Extremeプロキシ、HTML5ゲートウェイ、VPN装置等として動作すること。
        - ⑤ 仮想デスクトップのコネクション数を基に接続先を振り分ける負荷分散機能を有すること。
        - ⑥ 仮想デスクトップ機能と連携し、仮想デスクトップ起動時のシングルサインオンが可能であること。
        - ⑦ Webベース等の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。
        - ⑧ 証明書認証機能（認証サービス）及びOTP認証機能（認証サービス）と連携し、証明書認証やOTP認証が可能であること。
        - ⑨ 暗号化通信を確立できること。
        - ⑩ 固定回線及びモバイル回線から利用可能なこと。
      - ハードウェア要件
        - ① 構築要件を踏まえた最適な機器を提案すること。

ウ Windowsタブレット	
ソフトウェア要件	
	① Windows 10を搭載していること。
	② 内蔵のHDD・SSDを暗号化する機能を搭載していること。
ハードウェア要件	
	① 画面のサイズは12インチ以上であること。
	② 端末の重量が約1,000g以下であること。
	③ 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。
	④ カメラを搭載していること。
	⑤ 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。
4 私物等端末リモートアクセスサービス	
(1) 概要	
	省外から私物等端末（モバイル）を用いて、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を利用できる環境を提供する。
(2) 構築要件	
ア 私物等端末リモートアクセス機能	
	① 省外から私物等端末（モバイル）を用いて、省内のポータルサイトの閲覧、メールサービスと連携して電子メールの閲覧及び送信、ファイル共有サービスと連携して共有フォルダのファイルの閲覧ができること。
	② アクセスできる範囲は、総務省LAN内部ネットワークのみとすること。
	③ メール本文のURLリンクによるWebサイトの閲覧ができること。また、省外サイトや特定サイトの閲覧を制限できること。
	④ ワンタイムパスワードによる認証を行うこと。
	⑤ 本サービスへのログイン時には、認証サービスと連携し、ID・パスワードによる認証を行うこと。
	⑥ 端末上のアプリ起動時及び休止状態からの復帰時に、暗証番号の入力を必要とすること。また、アプリ起動時の暗証番号入力に一定回数失敗した際に、本サービスへのアクセスに必要な設定情報が私物等端末（モバイル）から自動的に消去されること。
	⑦ 利用端末を申請システムで申請し、あらかじめ各端末固有の情報が登録された端末のみが本サービスを利用できるものとすること。登録方法については、別途主管課と協議すること。
	⑧ 利用可能な私物等端末（モバイル）は、iOS・iPadOS・Android搭載の端末とし、専用アプリからのみ本サービスを利用できること。
	⑨ セキュリティログ分析サービスでログの解析等ができるよう、ユーザアクセスに関するログを定期的に収集すること。
	⑩ 本サービスの利用にあたり、総務省LANの申請管理サービス及び認証サービスと連携して、利用者の登録及び管理等を行うこと。
	⑪ DMZにゲートウェイ装置を設置し、外部から不正に侵入できない構成であること。
	⑫ 本サービスを利用できる職員数は2,500人とする。また、同時接続数は、500人を目安とする。
	⑬ 部署に割り振られている共有アカウント宛のメールを閲覧できること。
	⑭ アドレス帳を利用して、全職員の連絡先を検索できること。また、選択した連絡先を個人アドレス帳に登録できること。
	⑮ 専用アプリ内でのコピー&ペーストを許可すること。その際、端末内部に保存するのではなく、セキュアな環境を用意すること。
	⑯ 特定条件の新着メールを受信した場合に、メールの受信通知を行うこと。また、特定条件はユーザが個別に設定できること。
	⑰ 一定期間利用していないユーザに対してメールで通知すること。更に一定期間利用していない場合はアカウントを停止すること。
	⑱ ゲートウェイ装置は、サービス基盤の他サービスのゲートウェイ装置と共用してもよい。

(3) 機器等要件

ア 私物等端末リモートアクセス機能

ソフトウェア要件

① 端末が一定時間操作されない場合は、端末をロック又は自動的にログアウトする機能を有すること。
② ユーザの登録・変更、操作履歴の閲覧等の管理機能を有すること。
③ 職員が公開マーケットから各自で専用アプリをインストールできること。
④ メールに添付されたテキスト、PDF、Word、Excel、PowerPoint及び一太郎の各ファイルを閲覧できること。
⑤ メールに添付されたパスワード付のZIP・7-zipファイルを展開できること。
⑥ 本サービスの利用にあたり、私物等端末（モバイル）に閲覧情報を残さないこと。
⑦ アプリ起動時及びアプリロック解除時のパスワード入力を指紋認証で代替可能であること。
⑧ root化やJailbreakがなされた端末では、専用アプリを利用できないこと。
⑨ iOS/iPadOS搭載の端末では、本サービス利用中の利用者によるスクリーンショットが使用された場合、使用を検知しログを保存するとともに、管理者への通知、当該利用者を強制ログアウト、次回以降のログインを不可とする機能を有すること。 Android搭載の端末では、本サービス利用中の利用者によるスクリーンショットを禁止できること。
⑩ 通信が暗号化されていること。
⑪ 管理者画面には、総務省LANからのみアクセスできること。
⑫ 認証に必要なパスワードの端末への保存及び自動ログインを禁止できること。
⑬ メール作成時や返信時に、端末内に保存された写真などファイル添付の許可、禁止できる機能を有すること。
⑭ ブラックリストで指定したアプリケーションがインストールされた端末のログインを防止することが可能なこと。
⑮ オートフィルイン機能（宛先欄に相手方のアドレスの頭文字を入力した際に、これまでにやりとりのあるアドレスを予測表示し、選択可能とする機能）を有していること。

ハードウェア要件

① ハードウェア要件は、本書の第1 共通事項 - 3 共有サーバ・ストレージを参照すること。

イ ゲートウェイ装置

ソフトウェア要件

① リバースプロキシとして動作すること。
② HTTPS（SSL通信）の暗号化・復号を行えること。
③ IPv4/IPv6デュアルスタックに対応すること。
④ Webベース等の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 OTP認証機能（認証サービス）と連携し、OTP認証が可能であること。
⑥ 暗号化通信を確立できること。
⑦ 固定回線及びモバイル回線から利用可能なこと。

ハードウェア要件

① 構築要件を踏まえた最適な機器を提案すること。

【別紙1-1】機能要件詳細

5 デバイス管理サービス

(1) 概要

ペーパーレス会議サービスで利用するタブレット型端末及び省外で利用する支給端末（Windowsタブレット）のハードウェア情報・ソフトウェア情報等の収集、ソフトウェア・プロファイルの配布等を行う。また、端末の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。

(2) 構築要件

ア タブレット型端末管理機能

① 省内から安全に総務省LANのサービスを利用できるよう構成すること。

② タブレット型端末の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・リモートロックを実行できるよう構成すること。

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 タブレット型端末のポリシー遵守の状況を逐次監視し、ポリシー違反を検出したときには管理者に通知すること。

⑤ プロファイルやアプリケーションを遠隔からタブレット型端末に投入すること。

⑥ タブレット型端末を300台以上管理できる構成とすること。

⑦ 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。

⑧ iPadの構成管理・監視設定を行う管理用機器を準備すること。

⑨ 情報漏えい防止のために、管理対象のタブレット型端末を特定のコンピュータ以外に接続できない構成とすること。

⑩ 省内において、職員以外もタブレット型端末を利用できるよう、サービスに係るライセンスはデバイスに帰属させること。

⑪ ログインするユーザに応じて環境を切り替えること。

(3) 機器等要件

ア タブレット型端末管理機能

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 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。

④ 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。

⑤ Jailbreak端末の発見が可能であること。

⑥ 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。

⑦ 端末のポリシー遵守状況等を取得する際の通信が暗号化されていること。

⑧ 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。

⑨ 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いること。
・データセンタに格納するデータは暗号化されていること。

⑩ 端末側から削除できない固定のプロファイルをインストールできること。

⑪ タブレット型端末の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。

⑫ 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。

⑬ 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。

⑭ 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できること。

⑮ 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。

⑯ 端末にiOS及びiPadOSの監視モードを設定できること。

ハードウェア要件

① ハードウェア要件は、本書の第1 共通事項 - 3 共有サーバ・ストレージを参照すること。

【別紙1-1】機能要件詳細

6 資源管理サービス	
(1) 概要	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収集や、ソフトウェア（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。 ・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、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ドライブ、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。
(2) 構築要件	
①	Windowsサーバ、Linuxサーバ、LAN端末、仮想デスクトップ、ウイルスチェック用端末及び運用業務に利用する端末のインベントリ情報、ライセンス等の資源管理を行うこと。
②	LAN端末及び仮想デスクトップに対し、ソフトウェアの配付、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	Windowsサーバ、LAN端末、仮想デスクトップ、ウイルスチェック用端末に対して、Microsoft Updateサービスが提供するソフトウェア及びセキュリティパッチ等を配付すること。配布は、管理者の承認により、資源管理用のサーバから実施されること。
④	Microsoft Updateサービスが提供するソフトウェア及びセキュリティパッチ等は外部サイトに接続して自動でダウンロードし、資源管理用のサーバで保管すること。
⑤	Linuxサーバの更新パッケージを外部サイトに接続して自動でダウンロードし、資源管理用のサーバで保管すること。
⑥	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。
⑦	LAN端末が省外から接続した場合、セキュリティパッチの適用状況を確認すること。その際、最新のセキュリティパッチが適用されていない場合は、適用を促すポップアップメッセージを表示すること。
⑧	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。
⑨	Windowsサーバ、Linuxサーバ、LAN端末及びウイルスチェック用端末及び運用業務に利用する端末に対して、セキュリティパッチを配付すること。
⑩	セキュリティパッチのダウンロードを行う場合、外部サイトに接続して自動でダウンロードし、管理者により承認されたセキュリティパッチを配布すること。
⑪	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つつ、速やかに配布する構成とすること。
⑫	マルウェア対策（エンドポイント・ファイル共有）サービスがLAN端末のマルウェアを検知した場合、端末情報を資源管理サービスに連携すること。
⑬	セキュリティパッチ等がLAN端末に適用されているかを定期的に確認し、未適用の場合は、指定した日時にLAN端末上に特定のメッセージを表示すること。また、適用されるまでの間、メッセージを繰り返し表示すること。
⑭	セキュリティパッチ等がLAN端末に適用・導入されているか定期的に確認し、未適用の場合は、指定した日時にLAN端末をネットワークから隔離すること。また、ネットワーク隔離後においても特定のサーバとは通信できるよう通信制御機能を具備すること。

(3) 機器等要件	
ソフトウェア要件	
	① 規模・性能要件に記載した数の各種サーバ、LAN端末、支給端末（Windowsタブレット）及び運用業務に利用する端末を管理可能であること。
	② 1万台以上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 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。
	⑤ ライセンス管理を行うために、アプリケーションのインストール状況を自動収集する機能を有すること。
	⑥ 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。
	⑦ LAN端末におけるアプリケーションの稼働状況の記録（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。
	⑧ 業務に必要のないアプリケーションをブラックリストとして指定し、起動を禁止する機能を有すること。
	⑨ 収集した情報を基にレポートを作成する機能や、情報を検索する機能を有すること。
	⑩ LAN端末ごとに、記憶媒体（CD、DVD、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。
	⑪ 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。
	⑫ 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。
	⑬ ポリシー違反の情報だけを検索できること。
	⑭ 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。
	⑮ 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。
	⑯ LAN端末の操作ログ、アプリケーションの稼働時間等を収集、検索可能であること。
	⑰ 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するために、ファイル操作の前後のログ取得できること。
	⑱ LAN端末によるドメインへのログオン・ログオフの時刻を収集できること。
	⑲ 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。
ハードウェア要件	
	① ハードウェア要件は、本書の第1 共通事項 - 3 共有サーバ・ストレージを参照すること。
7 情報不正出力防止サービス	
(1) 概要	
	電磁的記録媒体による総務省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外部から電磁的記録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セキュリティUSBメモリを利用して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、許可されたセキュリティUSBメモリしか利用できない。 ・配布媒体作成の際は、LAN端末よりセキュリティUSBメモリへ複写後、ウイルスチェック用端末にて、必要なメディアの作成を行う。

(2) 構築要件

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セキュリティ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。 例外措置とし、必要により特定の総務省LAN端末において個別にセキュリティUSBメモリ以外のデバイスが接続できる設定を可能とする。
②	セキュリティUSBメモリ1,300本及びウイルスチェック用端末150台を準備すること。
③	ウイ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。
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のアップデート等を行う場合には、同一ネットワーク内に管理サーバを配置し、管理サーバが総務省LANと連携して自動更新を行い、最新の状態を保つこと。 なお、本ネットワークと総務省LANのネットワーク間は、必要となる通信以外は通さないこと。
⑦	ウイルスチェック用端末は、セキュリティアップデートで変更が必要となる領域を除き、書き込みを不可とすること。
⑧	ウイルスチェック用端末は、インターネット、イントラネット等への通信をさせないこと。
⑨	ウイルスチェック用端末は、ユーザによる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イ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	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。
⑭	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2年以上保存すること。
⑮	セキュリティUSBメモリ内にウイルスが隔離されていた場合に、LAN端末及びウイルスチェック用端末で利用できないようにすること。
⑯	セキュリティUSBメモリへの記録は、一定のパスワードポリシーの元自動的に暗号化格納を行うこと。
⑰	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、PDFを閲覧可能とすること。
⑱	ウイルスチェック用端末は、インターネットへアクセスするOS標準ツールをアンインストールすること。
⑲	LAN端末と同様に、マルウェア対策・セキュリティ監査を実施すること。
⑳	無線LANに接続する構成とすること。

(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を、セキュリティアップデートで変更が必要となる領域を除き、書き込み不可にできること。
②	一時的にデータ保存可能なフォルダを作成・削除できること。
③	管理コンソールからウイルスチェック用端末のソフトウェアを管理できること。
④	ウイルスチェック用端末の利用ログを収集する機能を有すこと。
⑤	管理コンソールからソフトウェアの設定やアップデートを配信できること。

ハードウェア要件

①	ハードウェア要件は、本書の第1 共通事項 - 3 共有サーバ・ストレージを参照すること。

イ セキュリティUSBメモリ

ソフトウェア要件

①	セキュリティUSBメモリ本体内にハードウェア暗号化機能を有し、強制的に暗号化できること。
②	暗号化方式は、AES256bit相当以上であること。
③	パスワードを一定回数誤った場合、アクセスできなくなる機能を有すること。
④	管理者機能を具備し、パスワードポリシー（文字長、文字種、有効期限等）を設定可能なこと。
⑤	未フォーマット時容量として、32GB以上のメモリを有すること。
⑥	アンチウイルス機能を内蔵すること。ただし、ウイルスチェック用端末にインストールされているアンチウイルスソフトとは別のメーカーであること。
⑦	アンチウイルス機能のライセンスは、5 年間とし自動でパターンファイルをアップデート可能なこと。
⑧	ウイルス感染被疑ファイルをUSBメモリ内に隔離する機能を有すること。
⑨	Microsoft Windows 10で利用可能なこと。
⑩	総務省LAN及び、LAN端末で利用中の各種ソフトウェアと相互に干渉しないこと。なお、利用中のソフトウェア群に関しては、セキュリティ上の理由から公表できない。よって、必要に応じて閲覧開示を受けること。
⑪	ファイルシステムはexFATでフォーマットされていること。

ハードウェア要件

①	スティック状の形状であり、紛失防止のためのストラップホールを有すること。
②	USB3.0及びUSB2.0の両方の規格で利用できること。
③	USBバスパワーで動作すること。
④	資源管理サービスと連携できること。

ウ ウイルスチェック用端末

ソフトウェア要件

①	Windows 10を有すること。
②	以下のファイルを閲覧できるソフトウェアをインストールすること。 ・Microsoft Office ・Adobe PDF ・一太郎

ハードウェア要件

①	15型ノート形式PCであること。
②	書き込み禁止化ソフトウェアが動作するCPU・メインメモリ・ディスクを有すること。
③	USB2.0以上のポートを3ポート以上内蔵すること。少なくとも2ポートはUSB3.0に対応し、1ポートはUSB3.1（Type-C）に対応すること。
④	100BASE-TX/1000BASE-Tに対応した有線LANポートを内蔵すること。
⑤	IEEE802.11a/b/g/n/acに対応した無線LANを内蔵すること。
⑥	DVDスーパーマルチドライブを内蔵すること。
⑦	マスターキー方式のセキュリティワイヤーを有すること。

【別紙1-1】機能要件詳細

第4 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．DRサイトLAN 3．拠点LAN 4．総務省WAN 5．インターネット接続ネットワーク 6．外部監視室接続ネットワーク 7．ネットワークサービス 8．無線LANサービス
2 本省LAN	
(1) 概要	
	本省LANは、総務省職員が本省内において総務省LANサービスを利用するため、また、本省内に設置するサーバや、業務システム及び政府共通ネットワークと接続するためのネットワークを提供する。
(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、管理ネットワーク、業務システム接続ネットワーク、政府共通ネットワーク接続ネットワークを構成すること。なおバックボーンネットワークは他に総務省WAN及びインターネット接続ネットワークとも接続するため、各項の要件についても確認すること。
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、本省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	バックボーンネットワークと他のネットワークはレイヤ3で接続する構成とすること。
③	コアスイッチは、2台以上導入し、冗長構成とすること。
④	他の機器と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、80Gbps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、主管課が指定する場所に設置すること。
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	コアスイッチは、2台のスイッチを論理的な1台のスイッチとして動作させ、単体障害時は自動的に1台のスイッチのみで可能な限りの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	フロアネットワークは基本的に現行ネットワークを置き換える構成を想定している。必要な要件及び台数は、【別紙1-2】ルータ・スイッチ要件一覧を参照すること。また現在のネットワーク構成等は資料閲覧にて確認し、その他必要と思われる機器がある場合はそれらを含め、最適な機器台数で提案を行うこと。なお有益な提案を行える場合は、提案すること。
③	フロアネットワークの幹線は流用可とする。但しその場合、光トランシーバの形状は配線されているケーブルに合わせて用意すること。また幹線の追加が必要な場合は、受託者の責任において敷設すること。
④	フロアスイッチは､2台のスイッチを論理的な1台のスイッチとして動作させ、単体障害時は自動的に1台のスイッチのみで可能な限りのサービスを継続できる構成とすること。ただしサーバ室に設置する低層棟/高層棟/LAN管理室/電算室フロアスイッチは現行どおりシングル構成でも可とする。
⑤	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。
⑥	コアスイッチとフロアスイッチの間は4Gbps以上の多重リンクとすること。ただしサーバ室に設置する低層棟/高層棟/LAN管理室/電算室フロアスイッチとコアスイッチの間は現行どおり2Gbps以上とする。
⑦	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。ただしサーバ室に設置する低層棟/高層棟/LAN管理室/電算室フロアスイッチとエッジスイッチの間は現行どおりシングル接続でも可とする。
⑧	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。
⑨	フロアスイッチは、中央合同庁舎第2号館3F～11F東西EPS及びサーバ室に設置すること。
⑩	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。
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内のネットワーク構成は定義しないので、提案するネットワーク構成を提案書にて具体的に記載すること。
③	サーバネットワークを構成する機器及び接続は、冗長構成とすること。
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	サーバネットワーク内のスイッチは、将来の拡張を考慮し、ポート数に余裕を持たせること。
⑧	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 管理ネットワーク	
①	管理ネットワークは、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運用業務を行う役割と運用員がサーバ・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	管理ネットワーク内のネットワーク構成は定義しないので、提案するネットワーク構成を提案書にて具体的に記載すること。
③	管理ネットワークは、管理LAN侵入検知防御装置と1Gbps以上で接続すること。
④	管理ネットワークを構成する機器のうち、監視業務を行う役割を提供する機器及び接続は冗長構成とすること。
⑤	管理LANネットワーク内のスイッチは、将来の拡張を考慮し、ポート数に余裕を持たせること。

カ 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、総務省共通基盤支援システム、電気通信行政情報システム（STARS）等の業務システムとの接続点を提供する役割を持つ。
	② 業務システム接続ネットワークは、現行と同様に業務システム接続スイッチと業務システム集約スイッチで構成すること。
	③ 業務システム接続ネットワークは、コアスイッチと4Gbps以上の多重リンクとすること。
	④ 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。
	⑤ 業務システム接続スイッチと業務システム集約スイッチは、それぞれ2台のスイッチを論理的な1台のスイッチとして動作させ、単体障害時は自動的に1台のスイッチのみで可能な限りのサービスを継続できる構成とすること。
	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 将来的な業務システムの増加にも対応できること。
キ 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、政府共通プラットフォームやLG-WAN等と通信するために、総務省LANと政府共通ネットワークを接続する役割を持つ。
	② 政府共通ネットワーク接続ネットワークは、政府共通ネットワーク接続侵入検知防御機能（内）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は、政府共通ネットワーク回線接続スイッチ、政府共通ネットワーク接続DMZスイッチ、政府共通ネットワーク業務システム接続スイッチで構成すること。
	④ 政府共通ネットワーク接続DMZスイッチと政府共通ネットワーク業務システム接続スイッチは、それぞれ2台のスイッチを論理的な1台のスイッチとして動作させ、単体障害時は自動的に1台のスイッチのみで可能な限りのサービスを継続できる構成とすること。
	⑤ 冗長化されている部分は、ケーブルや機器、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。
	⑥ 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回線接続スイッチで接続すること。
	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。
	⑧ 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。
	⑨ 政府共通ネットワーク接続ネットワークのスイッチは、将来の拡張を考慮し、ポート数に余裕を持たせること。
	⑩ 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。
(3) 機器等要件	
ア コアスイッチ要件	
ソフトウェア要件	
	① 【別紙1-2】ルータ・スイッチ要件一覧　④スイッチスペック要件一覧のコアスイッチType Ⅰの要件を満たすこと。
ハードウェア要件	
	① 【別紙1-2】ルータ・スイッチ要件一覧　④スイッチスペック要件一覧のコアスイッチType Ⅰの要件を満たすこと。
イ フロアスイッチ要件	
ソフトウェア要件	
	① 【別紙1-2】ルータ・スイッチ要件一覧　④スイッチスペック要件一覧のフロアスイッチType Ⅰの要件を満たすこと。
ハードウェア要件	
	① 【別紙1-2】ルータ・スイッチ要件一覧　④スイッチスペック要件一覧のフロアスイッチType Ⅰの要件を満たすこと。
ウ エッジスイッチ要件	
ソフトウェア要件	
	① 【別紙1-2】ルータ・スイッチ要件一覧　④スイッチスペック要件一覧のエッジスイッチType Ⅰ、エッジスイッチType Ⅱ、エッジスイッチType Ⅲ、エッジスイッチType Ⅳの要件を満たすこと。
ハードウェア要件	
	① 【別紙1-2】ルータ・スイッチ要件一覧　④スイッチスペック要件一覧のエッジスイッチType Ⅰ、エッジスイッチType Ⅱ、エッジスイッチType Ⅲ、エッジスイッチType Ⅳの要件を満たすこと。

【別紙1-1】機能要件詳細

エ サーバネットワーク内スイッチ要件
ソフトウェア要件
① 【別紙1-2】ルータ・スイッチ要件一覧　④スイッチスペック要件一覧のスイッチ共通要件を満たすこと。
ハードウェア要件
① 【別紙1-2】ルータ・スイッチ要件一覧　④スイッチスペック要件一覧のスイッチ共通要件を満たすこと。
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 スイッチング容量、必要なポート数、消費電力等は指定しないので、提案製品の仕様について提案書に具体的に記載すること。
オ 管理 LAN ネットワーク内スイッチ要件
ソフトウェア要件
① 【別紙1-2】ルータ・スイッチ要件一覧　④スイッチスペック要件一覧のスイッチ共通要件を満たすこと。
ハードウェア要件
① 【別紙1-2】ルータ・スイッチ要件一覧　④スイッチスペック要件一覧のスイッチ共通要件を満たすこと。
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 スイッチング容量、必要なポート数、消費電力等は指定しないので、提案製品について提案書に具体的に記載すること。
カ 業務システム接続スイッチ要件
ソフトウェア要件
① 【別紙1-2】ルータ・スイッチ要件一覧　④スイッチスペック要件一覧のスイッチ共通要件を満たすこと。
② IPルーティング・プロトコルとして、Static、RIPV1/V2、OSPFをサポートしていること。
③ 2台のスイッチを論理的に1台の仮想的なスイッチにクラスタ化する仮想化技術を有すること。
④ クラスタ化したスイッチで複数の筐体にまたがったイーサネットポートを論理的に1本に束ねることが可能なこと。
⑤ 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。
ハードウェア要件
① 【別紙1-2】ルータ・スイッチ要件一覧　④スイッチスペック要件一覧のスイッチ共通要件を満たすこと。
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200W以下であること。
④ 208Gbps以上のスイッチング容量を有すること。
⑤ 100BASE-TX/1000BASE-Tを48ポート以上有すること。
キ 業務システム集約スイッチ要件
ソフトウェア要件
① 【別紙1-2】ルータ・スイッチ要件一覧　スイッチスペック要件一覧のスイッチ共通要件を満たすこと。
② レイヤ2のスイッチングを行えること。
③ 2台のスイッチを論理的に1台の仮想的なスイッチにクラスタ化する仮想化技術を有すること。
④ クラスタ化したスイッチで複数の筐体にまたがったイーサネットポートを論理的に1本に束ねることが可能なこと。
ハードウェア要件
① 【別紙1-2】ルータ・スイッチ要件一覧　④スイッチスペック要件一覧のスイッチ共通要件を満たすこと。
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100W以下であること。
④ 104Gbps以上のスイッチング容量を有すること。
⑤ 100BASE-TX/1000BASE-Tを48ポート以上有すること。

【別紙1-1】機能要件詳細

ク 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 【別紙1-2】ルータ・スイッチ要件一覧　④スイッチスペック要件一覧のスイッチ共通要件を満たすこと。
② レイヤ2のスイッチングを行えること。
ハードウェア要件
① 【別紙1-2】ルータ・スイッチ要件一覧　④スイッチスペック要件一覧のスイッチ共通要件を満たすこと。
② 消費電力が20W以下であること。
③ 20Gbps以上のスイッチング容量を有すること。
④ 100BASE-TX/1000BASE-Tを8ポート以上有すること。
ケ 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 【別紙1-2】ルータ・スイッチ要件一覧　④スイッチスペック要件一覧のスイッチ共通要件を満たすこと。
② 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。
③ IPルーティング・プロトコルとして、Static、RIPV1/V2、OSPFをサポートしていること。
④ 2台のスイッチを論理的に1台の仮想的なスイッチにクラスタ化する仮想化技術を有すること。
⑤ クラスタ化したスイッチで複数の筐体にまたがったイーサネットポートを論理的に1本に束ねることが可能なこと。
ハードウェア要件
① 【別紙1-2】ルータ・スイッチ要件一覧　④スイッチスペック要件一覧のスイッチ共通要件を満たすこと。
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200W以下であること。
④ 208Gbps以上のスイッチング容量を有すること。
⑤ 100BASE-TX/1000BASE-Tを48ポート以上有すること。
コ 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 【別紙1-2】ルータ・スイッチ要件一覧　④スイッチスペック要件一覧のスイッチ共通要件を満たすこと。
② レイヤ2のスイッチングを行えること。
③ 2台のスイッチを論理的に1台の仮想的なスイッチにクラスタ化する仮想化技術を有すること。
④ クラスタ化したスイッチで複数の筐体にまたがったイーサネットポートを論理的に1本に束ねることが可能なこと。
ハードウェア要件
① 【別紙1-2】ルータ・スイッチ要件一覧　④スイッチスペック要件一覧のスイッチ共通要件を満たすこと。
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50W以下であること。
④ 56Gbps以上のスイッチング容量を有すること。
⑤ 100BASE-TX/1000BASE-Tを24ポート以上有すること。
サ メディアコンバータ要件
ソフトウェア要件
① 【別紙1-2】ルータ・スイッチ要件一覧　④スイッチスペック要件一覧のメディアコンバータ要件を満たすこと。
ハードウェア要件
① 【別紙1-2】ルータ・スイッチ要件一覧　④スイッチスペック要件一覧のメディアコンバータ要件を満たすこと。

シ 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ベース等の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 ポート数及びポート種別は指定しない。
	② 消費電力が330W以下であること。
	③ 負荷分散時のスループットは、30Gbps以上であること。
3 DRサイトLAN	
(1) 概要	
	DRサイトLANは、DRサイト内に設置するサーバや政府共通ネットワークと接続するためのネットワークを提供する。
(2) 構築要件	
ア 共通	
	① バックボーンネットワーク、サーバネットワーク、管理ネットワーク、政府共通ネットワーク接続ネットワークを構成すること。なおバックボーンネットワークは他に総務省WAN及びインターネット接続ネットワークとも接続するため、各項の要件についても確認すること。
	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。
	④ DRサイトLANにおいて、平常時からユーザにサービス提供を行うサービスの通信経路となるネットワークは、機器及び接続を冗長構成とすること。 なおDR発動時のみ提供するサービスのためのネットワークについてはシングル構成でも可とする。
	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。
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、DRサイト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 バックボーンネットワークと他のネットワークはレイヤ3で接続する構成とすること。
	③ 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 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内のネットワーク構成は定義しないので、提案するネットワーク構成を提案書にて具体的に記載すること。
	③ 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。
	④ 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。
	⑤ サーバネットワーク内のスイッチは、将来の拡張を考慮し、ポート数に余裕を持たせること。
	⑥ 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。
エ 管理ネットワーク	
	① 管理ネットワークは、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運用業務を行う役割と運用員がサーバ・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 管理ネットワーク内のネットワーク構成は定義しないので、提案するネットワーク構成を提案書にて具体的に記載すること。
	③ 管理ネットワークは、管理LAN侵入検知防御装置と1Gbps以上で接続すること。
	④ 管理LANネットワーク内のスイッチは、将来の拡張を考慮し、ポート数に余裕を持たせること。
オ 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、政府共通プラットフォームやLG-WAN等と通信するために、総務省LANと政府共通ネットワークを接続する役割を持つ。
	② 政府共通ネットワーク接続ネットワークは、政府共通ネットワーク接続侵入検知防御機能（内）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は、政府共通ネットワーク回線接続スイッチ、政府共通ネットワーク接続DMZスイッチで構成すること。
	④ 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回線接続スイッチで接続すること。
(3) 機器等要件	
ア コアスイッチ要件	
ソフトウェア要件	
	① 【別紙1-2】ルータ・スイッチ要件一覧　④スイッチスペック要件一覧のコアスイッチType Ⅱの要件を満たすこと。
ハードウェア要件	
	① 【別紙1-2】ルータ・スイッチ要件一覧　④スイッチスペック要件一覧のコアスイッチType Ⅱの要件を満たすこと。
イ サーバネットワーク内スイッチ要件	
ソフトウェア要件	
	① 【別紙1-2】ルータ・スイッチ要件一覧　④スイッチスペック要件一覧のスイッチ共通要件を満たすこと。
ハードウェア要件	
	① 【別紙1-2】ルータ・スイッチ要件一覧　④スイッチスペック要件一覧のスイッチ共通要件を満たすこと。
	② スイッチング容量、必要なポート数、消費電力等は指定しないので、提案製品の仕様について提案書に具体的に記載すること。
ウ 管理LANネットワーク内スイッチ要件	
ソフトウェア要件	
	① 【別紙1-2】ルータ・スイッチ要件一覧　④スイッチスペック要件一覧のスイッチ共通要件を満たすこと。
ハードウェア要件	
	① 【別紙1-2】ルータ・スイッチ要件一覧　④スイッチスペック要件一覧のスイッチ共通要件を満たすこと。
	② スイッチング容量、必要なポート数、消費電力等は指定しないので、提案製品の仕様について提案書に具体的に記載すること。

エ 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 本省LANの政府共通ネットワーク回線接続スイッチと同一要件を満たすこと。
ハードウェア要件
① 本省LANの政府共通ネットワーク回線接続スイッチと同一要件を満たすこと。
オ 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 本省LANの政府共通ネットワークDMZスイッチと同一要件を満たすこと。
ハードウェア要件
① 本省LANの政府共通ネットワークDMZスイッチと同一要件を満たすこと。
カ 負荷分散装置要件
ソフトウェア要件
① 本省LANの負荷分散装置と同一要件を満たすこと。
ハードウェア要件
① 本省LANの負荷分散装置と同一要件を満たすこと。

4 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のネットワークを提供する。
(2) 構築要件
ア 共通
① 拠点LANは基本的に現行ネットワークを置き換える構成を想定している。必要な台数及び要件は、【別紙1-2】ルータ・スイッチ要件一覧を参照すること。また現在のネットワーク構成等は資料閲覧にて確認し、提案時には、その他必要と思われる機器がある場合は含め、最適な機器台数で提案を行うこと。なお有益な提案を行える場合はこの限りではないので、提案すること。
② 職員の増減やフロアのレイアウト変更等により、機器の追加が発生する場合があるため、考慮すること。
③ コアスイッチ及びフロアスイッチは各拠点もしくは各フロアのレイヤ3を終端し、総務省WANへ配送する役割を持つため、レイヤ3で動作する構成とすること。
④ エッジスイッチのみの拠点のレイヤ3は、総務省WANルータで終端する構成とすること。
⑤ 拠点LANは、既存の配線、ラック等の流用を可とする。但し新規で追加が必要な場合は、受託者の責任において敷設するものとする。
イ 総務省第2庁舎
① 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。
② コアスイッチは、2台のスイッチを論理的な1台のスイッチとして動作させ、単体障害時は自動的に1台のスイッチのみで可能な限りのサービスを継続できる構成とすること。
③ 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。
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 コアスイッチ及びフロアスイッチは、将来の拡張を考慮し、ポート数に余裕を持たせること。
ウ 永田町合同庁舎
① コアスイッチ、エッジスイッチで構成すること。
② 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 コアスイッチ及びエッジスイッチは、将来の拡張を考慮し、ポート数に余裕を持たせること。
エ 自治大学校
① 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。
② 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 コアスイッチ及びフロアスイッチは、将来の拡張を考慮し、ポート数に余裕を持たせること。

オ 情報通信政策研究所	
	① コアスイッチ、エッジスイッチで構成すること。
	② コアスイッチは、2台のスイッチを論理的な1台のスイッチとして動作させ、単体障害時は自動的に1台のスイッチのみで可能な限りのサービスを継続できる構成とすること。
	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。
	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 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。
	② 複数の建屋に別れて接続している構成のため、留意すること。また効率的な接続構成に変更出来る場合は提案すること。
	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 コアスイッチ及びフロアスイッチは、将来の拡張を考慮し、ポート数に余裕を持たせること。
キ 総合通信局、沖縄総合通信事務所	
	以下を対象とする。 ① 北海道総合通信局、東北総合通信局、関東総合通信局、、信越総合通信局、北陸総合通信局、東海総合通信局、近畿総合通信局、中国総合通信局、四国総合通信局、九州総合通信局、沖縄総合通信事務所
	② 東海総合通信局を除く拠点はコアスイッチ、エッジスイッチで構成すること。東海総合通信局はコアスイッチ、フロアスイッチ、エッジスイッチで構成すること。
	③ 東北総合通信局、関東総合通信局、東海総合通信局、九州総合通信局ではメディアコンバータを提供すること。
	④ コアスイッチ及びフロアスイッチは、2台のスイッチを論理的な1台のスイッチとして動作させ、単体障害時は自動的に1台のスイッチのみで可能な限りのサービスを継続できる構成とすること。
	⑤ 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。
	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 コアスイッチ及びフロアスイッチは、将来の拡張を考慮し、ポート数に余裕を持たせること。
ク 総合通信局と同建屋の行政評価局及び行政監視行政相談センター	
	① 以下を対象とする。 北海道管区行政評価局、東北管区行政評価局、長野行政監視行政相談センター
	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 エッジスイッチのみで構成すること。なお北海道管区行政評価局では総合通信局のコアスイッチとの接続に中継用のスイッチが必要なため、現行と同様にエッジスイッチで中継を行うこと。
	④ 各総合通信局～管区行政評価局、行政監視行政相談センター間の接続は冗長化すること。
	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。
ケ その他外部拠点及び地方支分部局	
	① 【別紙1-2】ルータ・スイッチ要件一覧にて、エッジスイッチのみを設置する拠点（北海道管区行政評価局、東北管区行政評価局、長野行政監視行政相談センターを除く）を対象とする。
	② エッジスイッチのみで構成すること。
	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。
(3) 機器等要件	
ア 共通	
	① 各拠点で必要なスイッチタイプ及び光コンバータ等の台数は【別紙1-2】ルータ・スイッチ要件一覧　③コア・フロア・エッジスイッチ設置台数一覧を参照すること。
	② 各スイッチタイプ及びメディアコンバータの要件は、【別紙1-2】ルータ・スイッチ要件一覧　④スイッチスペック要件一覧を参照すること。

【別紙1-1】機能要件詳細

5 総務省WAN			
	(1) 概要		
			総務省WANは、総務省職員が総務省LANサービスを利用するため、本省、各地方拠点及びDRサイトを相互に接続するためのネットワークを提供する。
	(2) 構築要件		
		ア 拠点WAN回線要件	
			① 各拠点にWAN回線を主回線と副回線の2本提供すること。回線種別、帯域等は【別紙1-3】回線一覧のWAN回線を参照すること。なお【別紙1-3】回線一覧は想定する最低帯域を記載しているが、WAN全体の設計等からより最適な帯域等があれば具体的に提案すること。ただし回線帯域に不足が生じた場合は、主管課と協議の上、受託者の責任において対策を講じるものとする。
			② WAN回線は閉域網とし、主回線の閉域網と副回線の閉域網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。なお、局舎の立地条件等により分離が不可能な場合、合理的な理由を示し、主管課の承認を得られれば、同一局舎でも可とする。
			③ 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。
			④ 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。
			⑤ 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。
			⑥ 副回線用の閉域網はベストエフォート回線での構成を想定しているが、通信が集中する本省、DRサイト及び主要拠点においてはスループットに懸念がある。副回線で利用する通信の特性等を考慮し、最適な回線サービスの提案もしくは他の対策等を行うこと。
			⑦ 提供する回線の閉域網内は冗長構成がとられていること。また閉域網内での障害は、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。
			⑧ 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。
			⑨ 本省とDRサイトには、上記主回線及び副回線とは別で、本省とDRサイト間を直接接続する回線もしくは閉域網を提供すること。回線種別、帯域等は【別紙1-3】回線一覧のWAN回線を参照すること。また該当回線もしくは閉域網は、上記3から6の要件も満たすこと。
		イ WAN構成要件	
			① 各拠点にルータを2台設置し、2本の回線をそれぞれ収容すること。ただし北海道管区行政評価局、東北管区行政評価局、長野行政監視行政相談センターは同建屋内の総合通信局のルータ及び回線を利用するものとする。なお本省とDRサイトには、本省とDRサイトを直接接続する回線用にルータを別で1台用意し、合計3台設置すること。
			② WAN回線は主回線、副回線とも常時利用する構成とし、またどちらかの回線の障害時はもう一方の回線で通信を可能とすること。
			③ 主回線と副回線は、それぞれの特性を踏まえて、使い分けを提案すること。
			④ 必要な通信はルータにて優先制御や帯域制御を行い、回線逼迫時でも必要な通信が保護される構成とすること。
	(3) 機器等要件		
		ア 共通	
			① 各拠点で必要なルータタイプは【別紙1-2】ルータ・スイッチ要件一覧　①WAN・インターネット接続ルータ設置台数一覧を参照すること。
			② 各ルータタイプの要件は、【別紙1-2】ルータ・スイッチ要件一覧　②ルータスペック要件一覧を参照すること。

【別紙1-1】機能要件詳細

6 外部監視室接続ネットワーク	
(1) 概要	
	外部から総務省LANを24時間365日監視するため、本省及びDRサイトと外部監視室を独立した閉域網で接続する。
(2) 構築要件	
ア 外部監視室接続ネットワーク	
	① 外部監視室接続ネットワーク用回線は、総務省WANとは異なるネットワーク網を閉域網で構成すること。回線種別、帯域等は【別紙1-3】回線一覧の監視用回線を参照すること。
	② 外部監視室用回線は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。
	③ 必要な通信はルータにて優先制御や帯域制御を行い、回線逼迫時でも必要な通信が保護される構成とすること。
	④ 外部監視室接続ネットワーク用回線の回線帯域は1Gbpsベストエフォート、ネットワーク接続構成はシングル構成を想定しているが、運用要件の内容を踏まえ提案を行うこと。
(3) 機器等要件	
ア 外部監視室接続ルータ要件	
	ソフトウェア要件
	①【別紙1-2】ルータ・スイッチ要件一覧　②ルータスペック要件一覧のルータ共通要件を満たすこと。
	ハードウェア要件
	①【別紙1-2】ルータ・スイッチ要件一覧　②ルータスペック要件一覧のルータ共通要件を満たすこと。
7 インターネット接続ネットワーク	
(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を本省及びDRサイトにて提供する。
(2) 構築要件	
ア インターネット接続回線	
	① 本省及びDRサイトにインターネット回線を提供すること。なお回線種別、帯域等は【別紙1-3】回線一覧のインターネット回線を参照すること。
	② 回線負荷分散機能を導入して、利用するサービス等により回線を使い分けて全ての回線を効率よく使用すること。
	③ 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。なお帯域確保型回線の障害時にベストエフォート型回線を利用することによる通信の遅延については考慮しないものとする。
	④ 本省の帯域確保型回線はDDoS対策として、回線提供業者の網内で大量のトラフィックを検知した際に不正通信のみをブロックできるサービスに加入すること。 なおDDoS攻撃対策の検知条件は、トラフィック学習により得られたトラフィックパターンから決定すること。 またDDoS攻撃の検知及び収束時に、メール等で通知が行われること。
	⑤ IPv4/IPv6デュアルスタックに対応すること。
	⑥ 総務省DNSのセカンダリサービスを提供すること。
	⑦ 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。
	⑧ 帯域確保型の回線は、ベストエフォート型の2回線とは、別の通信事業者の回線で提供すること。
	⑨ 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。本省及びDRサイトにて構築すること。
② インターネット接続ネットワークは、インターネット回線接続ルータ、インターネット回線接続スイッチ、インターネット接続スイッチ、インターネット接続 DMZ スイッチ、負荷分散装置、回線負荷分散装置で構成すること。
③ インターネット接続ネットワークは、本省LAN及びDRサイトLANと4Gbps以上で接続すること。
④ インターネット接続ネットワークを構成する機器及び接続について、平常時にサービスを提供する本省では冗長構成とすること。DRサイトではDR発動時のみサービスを提供する想定のためシングル構成でも可とするが、平常時に何等かのサービスを提供する提案とする場合は冗長構成とすること。
⑤ 冗長するスイッチは、それぞれ2台のスイッチを論理的な1台のスイッチとして動作させ、単体障害時は自動的に1台のスイッチのみで可能な限りのサービスを継続できる構成とすること。
⑥ 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。
⑦ 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。
⑧ 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。
(3) 機器等要件
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 【別紙1-2】ルータ・スイッチ要件一覧　②ルータスペック要件一覧　インターネット接続ルータを参照すること。
ハードウェア要件
① 【別紙1-2】ルータ・スイッチ要件一覧　②ルータスペック要件一覧　インターネット接続ルータを参照すること。
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 【別紙1-2】ルータ・スイッチ要件一覧　④スイッチスペック要件一覧のスイッチ共通要件を満たすこと。
② レイヤ2のスイッチングを行えること。
ハードウェア要件
① 【別紙1-2】ルータ・スイッチ要件一覧　④スイッチスペック要件一覧のスイッチ共通要件を満たすこと。
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50W以下であること。
④ 56Gbps以上のスイッチング容量を有すること。
⑤ 100BASE-TX/1000BASE-Tを24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 【別紙1-2】ルータ・スイッチ要件一覧　④スイッチスペック要件一覧のスイッチ共通要件を満たすこと。
② レイヤ2のスイッチングを行えること。
ハードウェア要件
① 【別紙1-2】ルータ・スイッチ要件一覧　④スイッチスペック要件一覧のスイッチ共通要件を満たすこと。
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50W以下であること。
④ 56Gbps以上のスイッチング容量を有すること。
⑤ 100BASE-TX/1000BASE-Tを24ポート以上有すること。

【別紙1-1】機能要件詳細

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 【別紙1-2】ルータ・スイッチ要件一覧　④スイッチスペック要件一覧のスイッチ共通要件を満たすこと。
② 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。
③ IPルーティング・プロトコルとして、Static、RIPV1/V2、OSPFをサポートしていること。
ハードウェア要件
① 【別紙1-2】ルータ・スイッチ要件一覧　④スイッチスペック要件一覧のスイッチ共通要件を満たすこと。
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200W以下であること。
④ 208Gbps以上のスイッチング容量を有すること。
⑤ 100BASE-TX/1000BASE-Tを48ポート以上有すること。
オ 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ベース等の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 ポート数及びポート種別は指定しない。
② 消費電力が150W以下であること。
③ 負荷分散時のスループットは、6Gbps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 一方の回線で障害が発生した場合に、他方の回線にトラフィックを振り分ける機能を有すること。
④ Webベース等の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。
ハードウェア要件
① ポート数及びポート種別は指定しない。
② 消費電力が150W以下であること。
③ 負荷分散時のスループットは、6Gbps以上であること。

8 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。 なお本省とDRサイトに機器を設置し、DR発動時にもサービスを提供すること。 各サービスを構成する機器について、平常時にサービスを提供する本省では冗長構成とすること。DRサイトではDR発動時のみサービスを提供する想定のためシングル構成でも可とするが、平常時に何等かのサービスを提供する提案とする場合は冗長構成とすること。
(2) 構築要件
ア DNSサービス要件
① DNSサービスは、全省DNS機能、インターネット接続DNS機能、政府共通ネットワークDNS接続機能で構成されること。
② 全省DNS機能は本省LAN及びDRサイトLANのサーバネットワークに、インターネット接続DNS機能はインターネット接続ネットワークの本省及びDRサイトのDMZに、政府共通ネットワークDNS接続機能は本省LAN及びDRサイトLANの政府共通ネットワーク接続ネットワーク内のDMZにそれぞれ配置すること。
③ 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。
(ア)全省DNS機能要件
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 本省とDRサイトのDNS機能で連携し、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DR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。
(イ)インターネット接続DNS機能要件
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」及び「総務省.jp」ドメインを提供すること。
⑦ DNSキャッシュポイズニング対策のため、キャッシュサーバとコンテンツサーバは分離し、別々の筐体で構成すること。
⑧ DNSキャッシュポイズニング対策のため、DNSSECを利用すること。
⑨ ルートヒントファイル（DNSルートサーバの情報が登録されたファイル）の更新の有無を定期的に確認し、最新のDNSルートサーバの情報を維持すること。
(ウ)政府共通ネットワーク接続DNS機能要件
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 DNSキャッシュポイズニング対策のため、DNSSECを利用すること。
イ 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 冗長化した2台間及びサイト間でリース情報の引継ぎを行えること。
③ DHCPサービスを一元管理し、本省からDRサイトへDHCPサーバの切り替わりが発生した際にもIPアドレスのバッティングが発生しないよう構成すること。
ウ NTPサービス要件
① 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、政府共通ネットワーク上のNTPサーバと同期を取ること。と同期を取ること。
② 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。

エ 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	プロキシサービスは全省プロキシ機能、インターネット接続プロキシ機能、政府共通ネットワーク接続プロキシ機能で構成されること。
③	全省プロキシ機能は本省LAN及びDRサイトLANのサーバネットワークに、インターネット接続プロキシ機能はインターネット接続ネットワークの本省及びDRサイトのDMZに、政府共通ネットワーク接続プロキシ機能は本省LAN及びDRサイトLANの政府共通ネットワーク接続ネットワーク内のDMZにそれぞれ配置すること。
④	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。
⑤	マルウェア対策（インターネット・Web）サービスと連携すること。
⑥	認証サービスと連携し、ユーザ認証を行うこと。

(ア)全省プロキシ機能

①	インターネット閲覧サービスを経由する場合及び省内のサーバへアクセスする場合を除き、ユーザからの全てのWeb通信は、全省プロキシ機能が中継して通信する構成とすること。
②	インターネット宛はインターネット接続プロキシ機能、政府共通ネットワーク宛は政府共通ネットワーク接続プロキシ機能へ転送すること。

(イ)インターネット接続プロキシ機能

①	全省プロキシ機能及びインターネット閲覧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。
②	インターネット閲覧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。
③	プロキシサービスにてHTTPS（SSL通信）の復号を行うこと。また必要に応じて復号の除外指定ができること。

(ウ)政府共通ネットワーク接続プロキシ機能

①	全省プロキシ機能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	プロキシサービスにてHTTPS（SSL通信）の復号を行うこと。また必要に応じて復号の除外指定ができること。

(3) 機器等要件

ア DNSサービス要件

(ア)全省DNS機能要件

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ベース等の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フェースとして、Webベース等のGUIを提供すること。
⑪	DR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	DR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	DNSの問い合わせ性能として、45,000qps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 DNSの問い合わせ性能として、4,000qps以上有すること。
② DNSキャッシュポイズニング対策のため、キャッシュサーバとコンテンツサーバは分離し、別々の筐体で構成すること。
(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 DNSの問い合わせ性能として、4,000qps以上有すること。
イ DHCPサービス要件
ソフトウェア要件
① DHCPの運用がWebベース等の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。
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 MACアドレスを登録し、登録されたMACアドレスのみに特定のDHCPレンジからIPアドレスを払いだせる事。
⑥ 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。
⑦ 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。
⑧ 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。
⑨ 全省DHCPサービスを一元管理すること。
⑩ システム管理用インタフェースとしてWebベース等のGUIを提供すること。
⑪ 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 DHCP性能として、300lease/sec以上有すること。
② 全省DNSサーバと同一筐体でのサービス提供でも可とする。

ウ NTP サービス要件
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 全省DNSサーバと同一筐体でのサービス提供でも可とする。
エ プロキシサービス要件
(ア)全省プロキシ機能要件
ソフトウェア要件
① インターネット及び政府共通ネットワークへのWeb通信を、インターネット接続プロキシ機能及び政府共通ネットワーク接続プロキシ機能へ中継が可能であること。
② HTTP、HTTPS、FTPリクエストの中継機能を有すること。
③ HTTP1.1及びHTTP2.0に対応したHTTPリクエストの中継機能を有すること。
④ Webベース等の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 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。
⑥ NTLM、LDAP、Active Directory、RADIUS等と連携した認証が可能であること。
⑦ 認証サービス及び他のプロキシ機能と連携し、ユーザ認証を行うことが可能であること。
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フェースとして、Webベース等の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。
⑭ インターネット閲覧サービスを利用する場合を除き、基本的には全ユーザのWebアクセス通信が本プロキシ機能を経由するため、これを処理可能な構成とすること。
ハードウェア要件
① 1000BASE-T以上のポートを必要ポート数有すること。

【別紙1-1】機能要件詳細

(イ)インターネット接続プロキシ機能要件
ソフトウェア要件
① 全省プロキシ機能からのインターネット向けWeb通信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及びHTTP2.0に対応したHTTPリクエストの中継機能を有すること。
④ Webベース等の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 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。
⑥ NTLM、LDAP、Active Directory、RADIUS等と連携した認証が可能であること。
⑦ 認証サービス及び他のプロキシ機能と連携し、ユーザ認証を行うことが可能であること。
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フェースとして、Webベース等の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。
⑭ HTTPS（SSL通信）の復号が可能なこと。また必要に応じて復号の除外指定ができること。
⑮ 全ユーザのインターネット向けWeb通信が本プロキシ機能を経由するため、これを処理可能な構成とすること。
ハードウェア要件
① 1000BASE-T以上のポートを必要ポート数有すること。
(ウ)政府共通ネットワーク接続プロキシ機能要件
ソフトウェア要件
① 全省プロキシ機能からの政府共通ネットワーク向けWeb通信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及びHTTP2.0に対応したHTTPリクエストの中継機能を有すること。
④ Webベース等の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 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。
⑥ 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。
⑦ IPv4、IPv6のデュアルスタックに対応すること。
⑧ 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。
⑨ システム管理用インタフェースとして、Webベース等のGUIを提供すること。
⑩ 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。
⑪ HTTPS（SSL通信）の復号が可能なこと。また必要に応じて復号の除外指定ができること。
⑫ 全ユーザの政府共通ネットワーク向けWeb通信が本プロキシ機能を経由するため、これを処理可能な構成とすること。
ハードウェア要件
① 1000BASE-T以上のポートを必要ポート数有すること。

【別紙1-1】機能要件詳細

9 無線LAN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、LAN端末に無線LAN接続サービスを提供する。また、ペーパーレス会議システムのタブレット型端末と情報不正出力防止サービスのウイルスチェック用端末にも無線LAN接続サービスを提供する。 なお、本調達では有線LANも構築し職員等へ提供するが、無線LANの利用を推奨する方針とし、全ての端末が無線LANに接続可能なように高密度な人員配置も想定して、無線LANを提供すること。
(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（ペーパー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サービスは無線LANコントローラ、無線LANアクセスポイント、無線LAN管理サーバで構成し、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。
③	無線LANコントローラは本省とDRサイトに設置し、DR発動時にもサービスを提供すること。なお常時サービスを提供する本省では冗長構成とし、DRサイトではシングル構成でも可とする。
④	無線LAN管理サーバは本省にのみ設置し、シングル構成でも可とする。
⑤	通常時は本省の無線LANコントローラにて無線LANアクセスポイントを管理し、本省の冗長化した無線LANコントローラが全てダウンした場合、DRサイトの無線LANコントローラにて無線LANアクセスポイントが管理できること。
⑥	本省の無線LANアクセスポイントは、基本的にフロアスイッチと接続して給電を受けること。ただしフロアスイッチと接続が難しい場合はエッジスイッチとの接続とし、またその際は必要に応じて別途パワーインジェクタにて電力を供給すること。なお外部拠点の無線LANアクセスポイントは、基本的にパワーインジェクタでの電力供給を想定している。
⑦	現行から増加する無線LANアクセスポイントについて、接続先スイッチのポートが不足する場合は、必要に応じてスイッチを追加すること。なおその場合は、【別紙1-2】ルータ・スイッチ要件一覧　④スイッチスペック要件一覧のスイッチ共通要件を満たすこと。
⑧	無線LANコントローラは本省もしくはDRサイトにのみ設置する想定のため、外部拠点では無線LANの制御用通信以外（ユーザ通信等）は、無線LANコントローラを経由せずに通信すること。
⑨	同一拠点もしくは同一建屋内において無線LAN端末の持ち運びを行った際に、無線LANの再認証等が発生せずにローミングでき、また同一IPアドレスを保持し続ける構成とすること。
⑩	無線LANアクセスポイントは、全ての拠点にて、会議室、執務室、打ち合わせスペース等の業務において端末を利用するエリアで無線LANが提供できるように設置すること。ただしタブレット型端末は本省のみでの利用を予定している。 現行の無線APプロット図やフロア図、その他現行設計情報等を資料閲覧にて開示するので、AP必要台数の算出の参考とすること。なお大凡900台程度を想定している。
⑪	無線LANアクセスポイントを原則として天井に設置すること。
⑫	無線LAN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。
⑬	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、設計どおりに設置されているか確認すること。
⑭	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、自動で電波調整（チャネル変更）等を行い回避させること。
⑮	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。
⑯	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。
⑰	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。

	⑱ 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。
	⑲ タブレット型端末とウイルスチェック用端末の無線LAN接続用SSIDはそれぞれ、LAN端末の無線LAN接続用SSIDとは異なるSSIDにて構築すること。
	⑳ タブレット型端末専用とウイルスチェック用端末専用のVLANをそれぞれ作成し、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。
	㉑ 無線LAN管理サーバにて会議室、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LANコントローラ	
ソフトウェア要件	
	① 最大で1,000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。
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WPA、WPA2及びWPA3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。
	⑤ 以下のEAPタイプに対応していること。 ・EAP-TLS ・EAP-TTLSまたはMSCHAPv2 ・PEAP（EAP-MSCHAPv2）
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30W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 IEEE802.11acでは、4X4以上のMU-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。

ウ 無線LAN管理サーバ

ソフトウェア要件

① 管理している無線LANコントローラ(無線LANアクセスポイント)に接続している無線LANクライアントの一覧を表示可能なこと。

② 管理している無線LANコントローラ(無線LANアクセスポイント)で検出した不正アクセスポイントの一覧を表示可能なこと。

③ 各無線LANアクセスポイントにおける、時系列での無線LANクライアント接続数推移のグラフを表示することが可能なこと。ただし、ソフトウェアの機能として満たせなくても、運用の中で同等の内容の資料を提示可能であれば良い。

④ 無線LAN管理ソフトウェアにインポートしたMAP画面上に、管理している無線LANアクセスポイントの電波のカバレッジ状態を表示することが可能なこと。

⑤ 無線LAN管理ソフトウェアにインポートしたMAP画面上に、無線LANクライアントと不正アクセスポイントの位置推定表示が可能なこと。

⑥ 無線LANクライアントに対する簡易的なトラブルシューティング機能を有していること。

⑦ GUIは日本語対応していること。

ハードウェア要件

① ハードウェア要件は、本書の第1 共通事項 - 3 共有サーバ・ストレージを参照すること。

第5 セキュリティサービス

1 概要

セキュリティサービスは、次の区分によって構成される。
・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（エンドポイント・ファイル共有）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
・セキュリティ管理サービス
・セキュリティログ分析サービス

2 マルウェア対策（メール）サービス

(1) 概要

メールに含まれるマルウェア等を早期に検知・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総務省LAN間のメール通信のマルウェア検査・検知を行う。インターネットと総務省LAN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、迷惑メール判定を行い、迷惑メールを防御する。また、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。
また、不審メール通報機能及びメール誤送信対策機能については、Outlookクライアントのアドインとして提供すること。

(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管理者もしくは職員が確認・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、すべてメールウイルス対策機能によりマルウェア検査（アンチウイルス）される構成とすること。ただし、インターネット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（アンチウイルス）を実施すること。
⑤	インターネット及び政府共通ネットワーク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（SPF、DKIM、DMARC）を実施すること。
⑦	職員が不審メールを受信した際に、管理者にその旨を通知し、不審メール自体を提出するしくみを構成すること。 本機能はOutlookクライアントのアドインとして提供すること。
⑧	マルウェア判定された場合は、管理者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。
⑪	メール誤送信を防ぐ手段として、省外へのメール送信前に宛先アドレスを確認する機能、及びメール送信後に当該メールを一定時間滞留させる機能を提供すること。 本機能はOutlookクライアントのアドインとして提供すること。
⑫	インターネット経由で送受信するメールについて、実行可能ファイルが添付されたメールの中継を拒否すること。
⑬	本サービスは冗長構成とすること。
⑭	本省被災時においてもサービスを継続するため、DRサイトでもサービスを継続できるよう構成すること。なおDRサイトはシングル構成でも可とする。

(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。
⑦	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。

ハードウェア要件

①	消費電力が770W以下であること。
②	ディスクはRAID1で冗長化すること。

【別紙1-1】機能要件詳細

イ 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、DKIM及びDMARC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 消費電力が770W以下であること。
② ディスクはRAID1で冗長化すること。
ウ 不審メール通報機能
ソフトウェア要件
① 総務省職員が不審なメールを受信した場合に、当該メールを不審メールとして請負者の運用担当者に通報できること。
ハードウェア要件
① 本機能はOutlookクライアントのアドインとして提供を想定しているため、ハードウェア要件は規定しない。
エ メール誤送信対策機能
ソフトウェア要件
① 省外へのメール送信前に宛先アドレスの再確認ができること。
② 省外へのメール送信処理後、当該メールを一定時間滞留させてから送信すること。
ハードウェア要件
① 本機能はOutlookクライアントのアドインとして提供を想定しているため、ハードウェア要件は規定しない。

オ 標的型攻撃対策（メール）機能	
ソフトソフトウェア要件	
	① 1月あたり平均1,000万通のメールの添付ファイルを検査可能であること。
	② 振る舞い検知による不正プログラムの判定は、仮想環境上で添付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できること。
	③ 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。
	④ 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。
	⑤ 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。
	⑥ 総務省LAN上の端末がメール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。 なお、他サービスにて実現することも可とする。
	⑦ 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。
	⑧ 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。
	⑨ 攻撃者が頻繁に使用するパスワードや、パスワード付き圧縮ファイルが添付されているメールから抽出したパスワード候補にてパスワード付き圧縮ファイルの解凍を試み、解凍できた場合は圧縮ファイル内に格納されているファイルに対して動的解析を行えること。 ただし、多段マルウェア検査のうち全段で行う必要はない。
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。
	② ディスクはRAID1で冗長化すること。

3 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。
(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（アンチウイルス）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、必要に応じて管理者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、デコードした上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。
	⑨ インターネット閲覧サービスを介さないインターネットへのWebアクセスについては、一部の許可されたサイトを除き、原則、javaファイル（.jar/.class/.jnlp）、スクリーンセーバー（.scr）、Adobe Flash Player等のコンテンツへのアクセスをブロックすること。
	⑩ Webコンテンツフィルタリングのログは3年以上保存し、検索、閲覧を行えるよう構成すること。 なお、他サービスにて実現することも可とする。
	⑪ 本サービスは冗長構成とすること。
	⑫ 本省被災時においてもサービスを継続するため、DRサイトでもサービスを継続できるよう構成すること。なおDRサイトはシングル構成でも可とする。
	⑬ 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を踏まえた性能を担保すること。
	⑭ インターネットウイルス対策機能、Webコンテンツフィルタリング機能及び標的型攻撃対策（Web）機能はインターネット接続ネットワーク内のDMZに配置すること。
	⑮ 政府共通ネットワークウイルス対策機能は政府共通ネットワーク接続ネットワーク内のDMZに配置すること。
	⑯ Webウイルス対策機能は、インターネット接続ネットワーク内のDMZ及び政府共通ネットワーク接続ネットワーク内のDMZにそれぞれ配置すること。

- (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 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ベース等の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 1000BASE-T以上のポートを必要ポート数有すること。
      - ② アンチウイルススループットは、1Gbps以上であること。
  - イ 政府共通ネットワークウイルス対策機能
    - ソフトウェア要件
      - 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ベース等の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 1000BASE-T以上のポートを必要ポート数有すること。
      - ② アンチウイルススループットは、1Gbps以上であること。
  - ウ Webウイルス対策機能
    - ソフトウェア要件
      - 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 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。
    - ハードウェア要件
      - ① ハードウェア要件は、本書の第1 共通事項 - 3 共有サーバ・ストレージを参照すること。

エ 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、グラフ表示等の機能を有すること。
⑨ 現行運用でフィルタリングされているカスタムルールを引き継ぐことができること。
⑩ 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。
⑪ プロキシサービスと連携可能であること。

ハードウェア要件

① ハードウェア要件は、本書の第1 共通事項 - 3 共有サーバ・ストレージを参照すること。

オ 標的型攻撃対策（Web）機能

ソフトウェア要件

① 250,000オブジェクト/日程度の解析が可能なこと。
② 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。
③ 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。
④ マルウェアの検知状況についてレポートを作成する機能を有すること。
⑤ 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。

ハードウェア要件

① ハードウェア要件は、本書の第1 共通事項 - 3 共有サーバ・ストレージを参照すること。

4 マルウェア対策（エンドポイント・ファイル共有）サービス

(1) 概要

サーバ、LAN端末、仮想デスクトップ、ウイルスチェック用端末、運用端末及びファイル共有領域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・端末）サービスを提供する。サーバ、LAN端末、仮想デスクトップ、ウイルスチェック用端末、運用端末及びファイル共有領域のマルウェア検査・検知を行う。
サーバ、LAN端末、仮想デスクトップ、ウイルスチェック用端末及び運用端末では、ホスト間の通信の制御を行う。
サーバ及びLAN端末では、不正な挙動の検知、感染経路の特定を行う。
LAN端末では、振る舞い検知型のマルウェア検査を行う。

(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 各マルウェア対策機能及びLAN端末用未知マルウェア検知機能は、マルウェアの検知・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、ウイルスチェック用端末、運用端末及びLAN端末のマルウェア検査を実施すること。
④ ファイル共有領域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、LAN端末、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。
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 サーバ及び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、管理者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。
⑭ 以下の端末数に加えて、導入サーバ（Windows/Linuxを含み、アプライアンスを除く）及び運用端末の管理を行うことを踏まえた性能を担保すること。 ・LAN端末数　：7,000 台 ・ウイルスチェック用端末数　：150 台
⑮ サーバ及びLAN端末の挙動を監視し、不正な挙動を検知できる機能を提供すること。
⑯ LAN端末マルウェア対策機能によりファイルがマルウェアと判定された場合は、当該LAN端末及び仮想デスクトップを自動的にネットワークから遮断すること。
⑰ 本サービスは冗長構成とすること。ただし、ファイル共有マルウェア対策機能、サーバ（Windows/Linux）マルウェア対策機能、ウイルスチェック用端末マルウェア対策機能、運用端末マルウェア対策機能はシングル構成でも可とする。
⑱ 本省被災時においてもサービスを継続するため、DRサイトでもサービスを継続できるよう構成すること。なおDRサイトはシングル構成でも可とする。
(3) 機器等要件
ア ファイル共有マルウェア対策機能
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、本書の第1 共通事項 - 3 共有サーバ・ストレージを参照すること。

イ サーバ（Windows/Linux）マルウェア対策機能
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フェースとして、Webベース等のGUIを提供すること。
⑦ 通信をポートベースで制御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、本書の第1 共通事項 - 3 共有サーバ・ストレージを参照すること。
ウ LAN端末マルウェア対策機能
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フェースとして、Webベース等のGUIを提供すること。
⑧ LAN端末のOSや導入ソフトウェアの脆弱性に対応する正式なパッチが提供されるまでの期間、メーカが危険度や緊急度が高いと判断する脆弱性に対して、LAN端末に仮想パッチを適用し、暫定のセキュリティ対策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、本書の第1 共通事項 - 3 共有サーバ・ストレージを参照すること。
エ ウイルスチェック用端末マルウェア対策機能
ソフトウェア要件
① ウイルスチェック用端末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フェースとして、Webベース等のGUIを提供すること。
⑦ 通信をポートベースで制御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、本書の第1 共通事項 - 3 共有サーバ・ストレージを参照すること。

			オ 運用端末マルウェア対策機能	
				ソフトウェア要件
				① 各種運用端末端末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フェースとして、Webベース等のGUIを提供すること。
				⑦ 通信をポートベースで制御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、本書の第1 共通事項 - 3 共有サーバ・ストレージを参照すること。
			カ LAN端末用未知マルウェア検知機能	
				ソフトウェア要件
				① LAN端末マルウェア対策機能にて検知したマルウェアと疑わしいファイルを、複数の仮想環境上（サンドボックス等）で読み込み実行し、挙動を解析できること。
				② 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。
				ハードウェア要件
				① ハードウェア要件は、本書の第1 共通事項 - 3 共有サーバ・ストレージを参照すること。
			キ エンドポイント挙動監視・インシデント対応機能	
				ソフトウェア要件
				① サーバ及び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 サーバ及び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。
				③ 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。
				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 サーバ及びLAN端末の脆弱性を突く不審な動作を検知及び防御可能なこと。
				⑥ Windows PowerShell等を悪用するファイルレスマルウェアによる攻撃を検知できること。
				⑦ サーバ及びLAN端末内のマルウェア動作概要について、管理サーバ上で時系列で表示する機能を有すること。
				⑧ ファイルハッシュ（MD5/SHA1/SHA256）、ファイル名、アクセス先URLを用いて、それらに該当するサーバ及びLAN端末を管理サーバから検索できること。
				⑨ サーバ及びLAN端末から収集したフォレンジックデータを詳細解析する機能を有すること。
				⑩ マルウェアに感染したサーバ及びLAN端末を手動で隔離する機能を提供すること。
				⑪ LAN端末隔離時に、LAN端末使用者に通知できること。
				⑫ システム管理用インタフェースとして、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、本書の第1 共通事項 - 3 共有サーバ・ストレージを参照すること。

【別紙1-1】機能要件詳細

5 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。

(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が取得できること。また、ログは3年以上保存し、検索、閲覧を行えるよう構成すること。なお、他サービスにて実現することも可とする。
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、これらホス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。
⑪ 総務省LANと政府共通ネットワーク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。
⑫ 総務省LANと政府共通ネットワーク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。
⑬ 総務省LANとインターネット間のインスタントメッセンジャー通信及びTor通信をブロックすること。
⑭ 本サービスは冗長構成とすること。ただし、外部監視室接続侵入検知防御機能はシングル構成でも可とする。
⑮ 本省被災時においてもサービスを継続するため、DRサイトでもサービスを継続できるよう構成すること。ただし、政府共通ネットワーク業務システム接続侵入検知防御機能及び業務システム接続侵入検知防御機能はDRを構成しなくてもよい。なおDRサイトはシングル構成でも可とする。
⑯ ネットワークの帯域を踏まえ、性能を担保すること。
⑰ 外部監視室接続侵入検知防御機能は、本省、DRサイト、外部監視室に導入すること。
⑱ インターネット接続侵入検知防御機能（外）及びインターネット接続侵入検知防御機能（内）はインターネット接続ネットワーク内のDMZに配置すること。
⑲ 政府共通ネットワーク接続侵入検知防御機能（外）、政府共通ネットワーク接続侵入検知防御機能（内）及び政府共通ネットワーク業務システム接続侵入検知防御機能は政府共通ネットワーク接続ネットワーク内のDMZに配置すること。
⑳ 設定内容の世代管理を行うこと。

(3) 機器等要件

ア 外部監視室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 ステートフルインスペクション機能を有すること。
④ Webベース等の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180W以下であること。
③ 1000BASE-T以上のポートを必要ポート数有すること。

イ 政府共通ネットワーク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 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 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 インラインモード、パッシブモードに対応すること。
⑥ 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。
⑦ 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。
⑧ 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。
⑨ 政府共通ネットワークからの分散サービス拒否（DoS/DDoS）攻撃を防御できること。
⑩ シグネチャファイルもしくは、シグネチャファイルに相当する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。
⑪ 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、ログは3年以上保存し、検索、閲覧を行えるよう構成すること。 なお、他サービスにて実現することも可とする。
⑫ 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。
⑬ アノーマリ検知のためのパラメータを設定可能であること。
⑭ 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。
⑮ 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。
⑯ 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。
⑰ 通信フローのログを表示できること。
⑱ 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。
⑲ 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。
⑳ 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。
㉑ 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。
㉒ シグネチャ情報は、常に最新の状態に保つこと。
㉓ 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。
㉔ 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。
㉕ 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。
㉖ 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。
㉗ 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 1000BASE-T以上のポートを必要ポート数有すること。
② 消費電力が500W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、192,000 以上であること。
⑤ 不正侵入検知（IPS）スループットは、780Mbps以上であること。

ウ 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 Webベース等の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 1000BASE-T以上のポートを必要ポート数有すること。
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。
⑤ インターネット接続侵入検知防御機能（内）と同一筐体での提供を可とする。
エ 政府共通ネットワーク業務システム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 Webベース等の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 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。
⑥ シグネチャファイルもしくは、シグネチャファイルに相当する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。
⑦ 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。
⑧ 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。
⑨ 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、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。
⑩ シグネチャ情報は、常に最新の状態に保つこと。
⑪ 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。
⑫ 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。
ハードウェア要件
① 1000BASE-T以上のポートを必要ポート数有すること。
② 消費電力が 250W 以下であること。
③ ファイアウォールスループットは、1.5Gbps以上であること。
④ 同時セッション数は、750,000 以上であること。
⑤ 不正侵入検知（IPS）スループットは、900Mbps以上であること。

オ 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によるアクセス制御や攻撃の検知、防御が行えること。
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 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。
⑥ 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。
⑦ 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。
⑧ 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。
⑨ シグネチャファイルもしくは、シグネチャファイルに相当する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 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、ログは3年以上保存し、検索、閲覧を行えるよう構成すること。 なお、他サービスにて実現することも可とする。
⑪ 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。
⑫ アノーマリ検知のためのパラメータを設定可能であること。
⑬ 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。
⑭ 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。
⑮ 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。
⑯ 通信フローのログを表示できること。
⑰ 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。
⑱ 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。
⑲ 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。
⑳ 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。
㉑ シグネチャ情報は、常に最新の状態に保つこと。
㉒ 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。
㉓ 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。
㉔ 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。
㉕ 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。
㉖ 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 1000BASE-T以上のポートを必要ポート数有すること。
② 消費電力が1200W以下であること。
③ ファイアウォールスループットは、6Gbps以上であること。
④ 同時セッション数は、1,500,000以上であること。
⑤ 不正侵入検知（IPS）スループットは、6Gbps以上であること。

カ 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で解析ができること。
	④ Webベース等の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 1000BASE-T以上のポートを必要ポート数有すること。
	② 消費電力が400W以下であること。
	③ ファイアウォールスループットは、8Gbps以上であること。
	④ 同時セッション数は、1,500,000以上であること。
	⑤ 政府共通ネットワーク接続侵入検知防御機能（内）と同一筐体での提供を可とする。
キ 業務システム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 Webベース等の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 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。
	⑥ シグネチャファイルもしくは、シグネチャファイルに相当する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。
	⑦ 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。
	⑧ 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。
	⑨ 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、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。
	⑩ シグネチャ情報は、常に最新の状態に保つこと。
	⑪ 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。
	⑫ 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。
ハードウェア要件	
	① 1000BASE-T以上のポートを必要ポート数有すること。
	② 消費電力が 250W 以下であること。
	③ ファイアウォールスループットは、1.5Gbps以上であること。
	④ 同時セッション数は、750,000 以上であること。
	⑤ 不正侵入検知（IPS）スループットは、900Mbps以上であること。

ク 管理LAN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 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 ステートフルインスペクション機能を有すること。

ハードウェア要件

① 1000BASE-T以上のポートを必要ポート数有すること。
② 消費電力が180W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。

6 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。

(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 本サービスは以下の機器を管理すること。
・LAN端末数　：7,000 台
・ウイルスチェック用端末数　：150 台
・管理複合機・プリンタ数　：約1,000 台
④ 本省被災時においてもサービスを継続するため、DRサイトでもサービスを継続できるよう構成すること。

(3) 機器等要件

ア 不正接続機器検知

ソフトウェア要件

① 未登録機器を検出し、通知する機能を有すること。
② 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。
③ 管理可能な専用のインタフェースを有すること。

ハードウェア要件

① ハードウェア要件は、特に規定しない。

7 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。
(2) 構築要件
① 総務省LANを構成する各機器及びサービスへの特権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 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による操作ログを操作証跡として録画保存すること。また、録画データは装置内に1年以上保管し、管理画面から検索、閲覧を行う機能を有すること。
⑨ LAN端末、サーバ（Windows/Linuxを含み、アプライアンスを除く）及びネットワーク機器の運用管理者アカウントに対し、定期的なパスワード変更を行うこと。
⑩ 本省被災時においてもサービスを継続するため、DRサイトでもサービスを継続できるよう構成すること。
⑪ 以下の機器へのアクセス制御を実現すること。 ・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
(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 操作ログの検索が可能なこと。
② 操作ログは、暗号化して保存可能なこと。
③ LAN端末のローカル管理者アカウントパスワード変更が、認証サービスのディレクトリ機能と連携して行えること。
④ 各サーバに対してリモートで管理者パスワードの変更が行えること。
⑤ 各サーバ及びネットワーク機器に対してリモートで管理者パスワードの変更が行えること。
ハードウェア要件
① ハードウェア要件は、特に規定しない。

【別紙1-1】機能要件詳細

8 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。
(2) 構築要件
① サーバ（Windows/Linuxを含み、アプライアンスを除く）、LAN端末、ウイルスチェック用端末及び運用端末に対して、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 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。
⑧ 監査に必要なログは、セキュリティログ分析サービスにて取得・保全されているログデータを利用すること。
(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 レポートを日本語で出力可能なこと。
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 現行のセキュリティポリシーの移行が可能であること。
⑨ ポリシー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。
⑩ 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、本書の第1 共通事項 - 3 共有サーバ・ストレージを参照すること。

【別紙1-1】機能要件詳細

9 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。
(2) 構築要件	
	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・イベント情報を自動的に取得・保全すること。
	② ログは3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・イベントを閲覧や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すること。
	⑫ 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。
	⑬ レポートは、PDF、CSV形式等主管課がわかりやすい形式で出力可能であること。
	⑭ 正規表現を用いたログの検索が可能であること。
	⑮ 本サービスは冗長構成とすること。
	⑯ 本省被災時にサービス提供を行わない構成も可とするが、本省復旧後に、本省が被災してから復旧するまでの期間のログを遡って収集できるよう構成すること。
	⑰ 相関分析ルールは、既存の内容を踏襲せず、受託者が提案するシステム構成に対応するよう、新規設計を行うこと。
	⑱ 1日あたりの総ログ量128GB/日以上を考慮した性能を担保すること。

(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 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30,000EPS以上）
② 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。
③ 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。
④ 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。
⑤ 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。
⑥ 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。
⑦ 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。
⑧ 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。
⑨ 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。
⑩ インタフェースは、完全日本語対応であること。
⑪ 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。
⑫ 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。
⑬ 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。
⑭ 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。
⑮ 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。
⑯ 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。
⑰ 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。
⑱ 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。）
⑲ 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。
⑳ 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。
㉑ 収集したログデータに対してハッシュ値等を利用した改ざん検知を自動的に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、本書の第1 共通事項 - 3 共有サーバ・ストレージを参照すること。

【別紙1-1】機能要件詳細

第6 運用サービス

1 概要

運用サービスは、次の区分によって構成される。
1.申請管理サービス
2.運用支援サービス
3.システム監視サービス
4.ログ管理サービス
5.バックアップサービス
6.電源管理サービス
7.ディザスタリカバリサービス

2 申請管理サービス

(1) 概要

申請管理サービスは、受付窓口を通じて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、各種申請をWeb画面で入力し、申請管理サービスを介して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、受付窓口に承認した申請の対応を依頼する。
・運用要員は、受付窓口と連携し申請された内容を確認し、運用管理端末から申請管理サービスへ接続し申請に基づいた作業を行う。
・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。
・現行システムで稼働しているWeb画面を用いた申請処理の機能と処理方式、及び利便性については基本的に引き継ぐこととする。
・原則、DRサイトでも提供する。ただし、有事の際に提供できない機能については、提案時に主管課と協議の上決定すること。

(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、受付窓口へ通知すること。
④	申請内容と実施作業の整合性チェックを行うこと。
⑤	申請内容と実施作業の履歴を保存し、運用要員がいつでも確認・共有できるよう構成すること。 また、必要に応じて受付窓口でも共有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。 在庫情報は、受付窓口からでも参照できる構成とすること。
⑦	職員以外のユーザアカウント管理機能を持つこと。
⑧	現行総務省LANにおける申請届出の実績を参考とし、以下の各種申請フォーマットを提案し、主管課と合意すること。 01　共有メールアカウント申請 02　電子メール自動転送申請(異動用) 03　メーリングリスト設定申請 04　ソフトウェアインストール申請 05　迷惑メール対策無効化申請 06　DNS設定申請 07　ペーパーレス会議利用申請 08　電子会議室新規作成申請 09　ポータル管理者アカウント設定申請 10　チャットルーム新規作成申請 11　LAN端末新規配備・移設・撤去申請 12　LAN端末期間限定配備申請 13　Web認証利用申請(海外出張用) 14　兼務先組織フォルダ利用申請 15　会議室予約アカウント設定申請 16　業務システム用アカウント設定申請 17　タブレット端末外部利用申請 18　タブレット端末外部利用申請書(業務システム用) 19　LAN複合機利用申請書 20　新規設備の登録・改廃申請 21　メールボックス拡張申請 22　共有フォルダ拡張申請 23　仮想デスクトップ利用申請 24　私物等端末リモートアクセス利用申請 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	
				ソフトウェア要件
				① 過去の申請情報を表示可能であること。
				② 申請処理の完了後には、受付窓口に作業完了の通知をすること。
				③ 申請管理サービスにて、受付窓口からの申請情報を一元管理すること。
				④ 受付窓口へ利用期限の通知機能を有すること。
				⑤ 過去の申請情報を利活用できるようにし、省入力により利便性と申請業務の効率化を図ること。 ただし、利活用する情報は、そのまま申請できないように対応（完全複製禁止等の対応）すること。
				⑥ ペーパーレス会議利用申請においては、機材の空き状況等を受付窓口も確認できる仕組みを提供すること。
				⑦ ペーパーレス会議システムを利用したことのあるユーザ及び利用したことのないユーザを判別し、自動的に適切な情報を提示すること。
				⑧ 各共有メールボックスを扱える職員が把握できること。
				ハードウェア要件
				① ハードウェア要件は、本書の第1 共通事項 - 3 共有サーバ・ストレージを参照すること。
			イ カード管理業務	
				ソフトウェア要件
				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。
				ハードウェア要件
				① ハードウェア要件は、特に規定しない。
	3 運用支援サービス			
		(1) 概要		
				運用支援サービスは、総務省LANに関するユーザからの支援依頼内容を一元管理し、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。 受付窓口からの作業依頼内容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。 また、ユーザに関わる情報については、受付窓口にも提供できるようにする。 原則、DRサイトでも提供する。ただし、有事の際に提供できない機能については、提案時に主管課と協議の上決定すること。
		(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を行い、主管課へ報告ができること。
				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、運用期間中に十分な対応ができるよう構成すること。
				④ インシデント管理機能に登録されている情報は、必要に応じて受付窓口からでも共有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 受付窓口と連携し、主管課も含め適宜ユーザからの問い合わせ内容を参照できること。
② 運用支援サービスにて問い合わせ実績を管理し検索ができること。 また、必要に応じて受付窓口や主管課からも参照できる構成とすること。
障害の対応状況の管理ができること。 ③ 対応状況については、適切なタイミングで受付窓口と連携し、必要に応じて受付窓口にてポータルサイト等に掲示できるようにすること。
日次、週次、月次単位でレポート出力が可能であること。 ④ レポート結果を取り纏め、集計結果やトピック、問い合わせランキングなどを主管課へ月次・年次で報告すること。 なお、詳細な報告内容については主管課と協議し、決定すること。
⑤ 一定時間内に対応が完了していない問い合わせ対応については、受付窓口に対してメール通知等の督促手段を提供すること。
⑥ ITIL Incident Management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、本書の第1 共通事項 - 3 共有サーバ・ストレージを参照すること。
イ LAN端末リモート操作機能
ソフトウェア要件
① LAN端末及び仮想デスクトップに対してリモートで操作できること。
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、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。 ② なお、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。
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 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。
⑦ 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、本書の第1 共通事項 - 3 共有サーバ・ストレージを参照すること。

【別紙1-1】機能要件詳細

4 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。
・原則、DRサイトでも提供できるようにする。

(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 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、本書の第1 共通事項 - 3 共有サーバ・ストレージを参照すること。

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、本書の第1 共通事項 - 3 共有サーバ・ストレージを参照すること。

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フェースとして、Webベース等の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し可視化できること。
	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、本書の第1 共通事項 - 3 共有サーバ・ストレージを参照すること。
エ ジョブ管理機能	
ソフトウェア要件	
	① 各ジョブをスクリプトやシェルなどで連接し、依存関係を組んでいる場合は、必要に応じ以下のジョブ管理要件を満たすこと。 ・自動実行可能なジョブに対して、スケジュールの登録及び管理機能を有すること。 ・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。 ・スケジュールに基づいたジョブの自動実行結果が確認できること。 ・重要度の高いジョブの開始及び終了が遅延した場合に、発見が速やかにできること。
ハードウェア要件	
	① ハードウェア要件は、本書の第1 共通事項 - 3 共有サーバ・ストレージを参照すること。
5 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）を本省サイトにて一元的に収集し、保守・運用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、保守・運用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。 ・各種ログは原則自動的に収集し、一定期間保管する。 ・DR発動時から本省復旧完了までの間は、DRサイトで一元的に収集し、本省復旧後に転送すること。
(2) 構築要件	
	① 保守・運用、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、3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。 DRサイトにおいては、検索・分析機能については必須とはしない。
	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。

		(3) 機器等要件	
			ア 総合ログ収集機能
				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、3年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、本書の第1 共通事項 - 3 共有サーバ・ストレージを参照すること。
				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、本書の第1 共通事項 - 3 共有サーバ・ストレージを参照すること。
	6 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。 自動で本省・DRサイトの相互バックアップを取得し、一定期間保管する。
		(2) 構築要件	
			① 各種サーバ・ネットワーク機器・アプライアンス機器等のバックアップは、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。
			⑦ バックアップは適切なタイミングで行い、7世代分保有すること。
			⑧ バックアップ運用を自動的に制御すること。
			⑨ 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。
			⑩ 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。
			⑪ 遠隔地にバックアップデータを送る際は、WANのネットワーク負荷及び総務省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。

(3) 機器等要件

ア バックアップ機能

ソフトウェア要件

① ソフトウェア要件は、特に規定しない。

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/ネットワーク機器/アプライアンス機器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、本書の第1 共通事項 - 3 共有サーバ・ストレージを参照すること。

7 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。
DRサイトについては、必須とはしない。

(2) 構築要件

① 停電発生時にシステムを停止させる必要がある場合には、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、ネットワーク機器、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。

8 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。
【別紙1-6】本省・DRサイト稼働サービス一覧を参考にし、本省で提供されてるサービスを可能な限りDRサイトでもサービスの提供を行えるよう提案すること。
本省・DRサイトへの端末接続は、自動的に切り替わる仕組みとすること。
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の提供サービスが利用できること。

【別紙1-1】機能要件詳細

(2) 構築要件	
①	インターネット接続、政府共通NW接続、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、システム監視機能などについて、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と連絡手段を準備すること。
③	ディザスタリカバリ発動（主管課から保守運用事業者へDRサイトの切替え指示が出るタイミング）から30分以内で、非常時優先業務として利用する総務省LAN提供サービスが開始でき、3時間以内にDRサイトへの切り替えが完了できること。
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）領域をアクセス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	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。
⑭	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。
⑮	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。
⑯	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。
⑰	私物端末（PC）及び支給端末（Windowsタブレット）は、仮想デスクトップ機能で総務省LANへのアクセス環境を提供すること。
⑱	本省設置で構成しているサービス提供機器のうち、Activeで稼働しているものはDRサイトではシングル構成にて設置する。 また、DRサイト設置で構成しているサービス提供機器のうち、Activeで稼働しているものは本省ではシングル構成にて設置する。
⑲	DRサイトにおけるネットワーク要件については、「第4 ネットワーク基盤」を参照のこと。
⑳	DRサイトで提供されるサービスに付随するセキュリティサービスを1式設置し、本省と同等のセキュリティを担保すること。
㉑	サーバ、ネットワーク機器、アプライアンス機器におけるソフトウェア類、環境設定ファイル、セキュリティ情報は、常に本省と同じバージョンを維持・管理すること。
㉒	本省においてDNSサービスが提供できない場合、DRサイトのDNSサービスに切り替わること。
㉓	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。
㉔	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。
㉕	DR発動時において、職員の利用する端末に対して、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）の自動割当てを行い、再ログイン時には、接続先が自動的に切り替わること。
㉖	広域負荷分散装置等を導入する場合、インターネットに公開しているDNSゾーン及び内部ネットワークのDNSゾーンに対しても、広域負荷分散機能を提供すること。
㉗	広域負荷分散装置等を導入する場合、本省サイト、DRサイトのDMZ及び内部ネットワークに各1式導入し、広域負荷分散が実現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 広域負荷分散装置等を導入する場合は、以下の要件に対応していること。
② 本省・DRサイトへの通信の振り分けが可能であること。
③ 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。
④ 本省の総務省LANサービス全てが利用できなくなった場合、自動的にDRサイトへ切り替わること。
⑤ 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。
⑥ NAT、ソースNAT機能を有すること。
⑦ SSLアクセラレータ機能を有すること。
⑧ L3、L4、及びL7レベルのヘルスチェック機能を有すること。
⑨ 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。
⑩ Webベース等の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。
⑪ 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 広域負荷分散装置等を導入する場合は、以下の要件に対応していること。
② グローバルサーバロードバランシングの機能を有すること。
③ アプリケーションスループットを5Gbps以上有すること。
④ ポート数及びポート種別は指定しない。
⑤ 消費電力が330W以下であること。

第7 その他機器基盤

1 概要

その他の機器基盤として、以下の要件に沿った環境及び機器等を提供する。
1.保守・検証環境
2.運用業務環境
3.KVM
4.UPS
5.LAN端末マスタ

【別紙1-1】機能要件詳細

2 保守・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。
(2) 構築要件	
	① 本番環境に適用する前に、受託者において稼働中の機器やサービスに悪影響を与えないことが確認できる専用環境を準備すること。
	② 保守・検証環境の構築は本省設置の本番環境とは別の環境として構築すること。 ハードウェア構成及びネットワークは受注者の提案により構築を行うこと。
	③ 保守・検証環境は本省に設置すること。 ただし、DRサイトの設置場所を効果的に利用する場合は、本省からリモートで検証できる機器等とし、本省設置スペースと利便性を考慮した提案をすること。
	④ 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。
	⑥ セキュリティレベル改善のために実施されるOSやソフトウェア等のパッチ適用の影響による不具合の有無を検証できる環境とすること。
	⑦ 認証機能を実装し、無権限者の利用が排除できること。
	⑧ 仮想環境の活用により、1つの物理環境内に複数環境を保持する機能を有すること。
	⑨ 仮想環境を用いずに構築する場合は、本番環境と同レベルのデータ量、負荷を使って、性能テスト、負荷テスト等を実施できる機能を有すること。
	⑩ 不正アクセスや情報漏えい、設定改ざん等、セキュリティ上のリスクに対応できるよう考慮すること。
	⑪ 本番環境の機能強化、バージョンアップに伴い、処理能力の柔軟な増強ができる構成とすること。
	⑫ 対象とするシステムや保管するコンテンツの増加に伴い、処理能力の柔軟な増強ができる構成とすること。
	⑬ 保守・検証環境を教育訓練に活用することにより、システム利用者が本番環境で実施できない更新処理を伴うユーザ教育を実施できる機能を有していること。
	⑭ 保管データ及び、環境のバックアップを取得できること。
	⑮ 保守・検証環境専用のネットワークを構築すること。
	⑯ 保守・検証環境は物理的なネットワーク分離、VLAN等の活用により、本番環境と切り離されていること。
	⑰ 保守・検証環境と本番環境との間には、スイッチ、ルータ等の通信機器が配置され、許可された端末、サーバ間以外の通信は行えないこと。
	⑱ インターネットに接続するには、本番環境とは別に回線を用意すること。
	⑲ ルータ、スイッチ等のIPフィルタリング機能等により、保守・検証環境と本番環境との通信が制御されること。
	⑳ DRサイトの設置機器（待機系）を保守・検証環境として有効利用する場合には、その目的と本省設置要件とのメリット・デメリットを明らかにし、非常時における職員の業務継続に影響がないよう考慮した内容を提案書にて詳細に示すこと。
	㉑ DRサイトを有効利用する場合には、本省には必要以上の保守・検証用機器は設置しないこと。
	㉒ 得られる効果と要するコストの両面を考慮し、請負事業者にて適切な構成を提案すること。
(3) 機器等要件	
	ソフトウェア要件
	① ソフトウェア要件は、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、特に規定しない。

- 3 運用業務環境
  - (1) 概要
    - 運用業務環境とは、運用要員が日常の運用業務に使用する設備環境であり、利用する機器ごとの個別環境を準備し利用する。
      個別環境には、必要に応じて一般執務環境、サーバ接続用環境、遠隔操作用環境に分離する。
      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を準備する。
  - (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端末や仮想デスクトップ環境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 10 64bit OSであること。
        - ② Microsoft Office 2019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。
        - ⑥ セキュリティ監査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Intel core i5 又はAMD Ryzen5 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。
        - ⑤ 共有ファイル領域は、4TB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 10 64bit 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フェースを持つこと。
        - ② メンテナンス用端末は、基本的にノート型であり、本体重量は1.3kg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 2019 以上のOSであること。
			ハードウェア要件
			① ハードウェア要件は、本書の第1 共通事項 - 3 共有サーバ・ストレージを参照すること。
		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 2019以上のOSであること。
			ハードウェア要件
			① ハードウェア要件は、本書の第1 共通事項 - 3 共有サーバ・ストレージを参照すること。
	4 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。
		(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・DRサイトは必要台数を用意し、その他のサーバを設置する拠点においては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。

5 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。

(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。なお、拠点に設置するUPSについては、ラインインタラクティブ方式でも可とする。
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インタフェースを有すること。

6 LAN端末マスタ

(1) 概要

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。

(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。
尚、タスクシーケンスによるキッティングでの管理も可とする。
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 10 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 2019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 10 Enterprise 64bitに対応したソフトウェアを選定すること。Windows 10 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。

7 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。
	(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 10 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 2019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 10 Enterprise 64bitに対応したソフトウェアを選定すること。Windows 10 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、本書の第1 共通事項 - 3 共有サーバ・ストレージを参照すること。

【別紙1-2】ルータ・スイッチ要件一覧
①WAN・インターネット接続ルータ設置台数一覧

項番	拠点名称	WANルータ		インターネット接続ルータ	外部監視室接続ルータ	合計台数
		Type Ⅰ	Type Ⅱ			
1	本省	3		3	1	7
2	DRサイト	3		2	1	6
3	総務省第2庁舎（統計局、政策統括官（統計基準担当）、政策統括官（恩給担当））		2			2
4	公害等調整委員会		2			2
5	内閣人事局		2			2
6	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委員会、公共サービス改革推進室）		2			2
7	総務省宮城分室		2			2
8	総務省大阪分室		2			2
9	自治大学校		2			2
10	情報通信政策研究所		2			2
11	国連アジア太平洋統計研修所		2			2
12	消防大学校及び消防研究センター		2			2
13	国会連絡室		2			2
14	永田町ビル（電気通信紛争処理委員会・政治資金適正化委員会）		2			2
15	統計データ利活用センター		2			2
16	北海道管区行政評価局　※1					0
17	函館行政監視行政相談センター		2			2
18	旭川行政監視行政相談センター		2			2
19	釧路行政監視行政相談センター		2			2
20	東北管区行政評価局　※2					0
21	青森行政監視行政相談センター		2			2
22	岩手行政監視行政相談センター		2			2
23	秋田行政監視行政相談センター		2			2
24	山形行政監視行政相談センター		2			2
25	福島行政監視行政相談センター		2			2
26	関東管区行政評価局		2			2
27	茨城行政監視行政相談センター		2			2
28	栃木行政監視行政相談センター		2			2
29	群馬行政監視行政相談センター		2			2
30	千葉行政監視行政相談センター		2			2
31	東京行政評価事務所		2			2
32	神奈川行政評価事務所		2			2
33	新潟行政評価事務所		2			2
34	山梨行政監視行政相談センター		2			2
35	長野行政監視行政相談センター　※3					0
36	中部管区行政評価局		2			2
37	富山行政監視行政相談センター		2			2
38	石川行政評価事務所		2			2
39	岐阜行政監視行政相談センター		2			2
40	静岡行政監視行政相談センター		2			2
41	三重行政監視行政相談センター		2			2
42	近畿管区行政評価局		2			2
43	福井行政監視行政相談センター		2			2
44	滋賀行政監視行政相談センター		2			2
45	京都行政監視行政相談センター		2			2
46	兵庫行政評価事務所		2			2
47	奈良行政監視行政相談センター		2			2
48	和歌山行政監視行政相談センター		2			2
49	中国四国管区行政評価局		2			2
50	鳥取行政監視行政相談センター		2			2
51	島根行政監視行政相談センター		2			2
52	岡山行政監視行政相談センター		2			2
53	山口行政監視行政相談センター		2			2
54	四国行政評価支局		2			2
55	徳島行政監視行政相談センター		2			2
56	愛媛行政監視行政相談センター		2			2
57	高知行政監視行政相談センター		2			2
58	九州管区行政評価局		2			2
59	佐賀行政監視行政相談センター		2			2
60	長崎行政監視行政相談センター		2			2
61	熊本行政評価事務所		2			2
62	大分行政監視行政相談センター		2			2
63	宮崎行政監視行政相談センター		2			2
64	鹿児島行政監視行政相談センター		2			2
65	沖縄行政評価事務所		2			2
66	北海道総合通信局		2			2
67	東北総合通信局		2			2
68	関東総合通信局		2			2
69	関東総合通信局（三浦電波監視センター）		2			2
70	信越総合通信局		2			2

【別紙1-2】ルータ・スイッチ要件一覧
①WAN・インターネット接続ルータ設置台数一覧

項番	拠点名称	WANルータ		インターネット接続ルータ	外部監視室接続ルータ	合計台数
		Type Ⅰ	Type Ⅱ			
71	北陸総合通信局		2			2
72	東海総合通信局		2			2
73	近畿総合通信局		2			2
74	中国総合通信局		2			2
75	四国総合通信局		2			2
76	九州総合通信局		2			2
77	沖縄総合通信事務所		2			2
78	外部監視室				1	0
	タイプ別台数合計	6	144	5	3	150

※1　北海道総合通信局へ回線収容し接続
※2　東北総合通信局へ回線収容し接続
※3　信越総合通信局へ回線収容し接続

【別紙1-2】ルータ・スイッチ要件一覧
②ルータスペック要件一覧

機器タイプ	ルータスペック要件	
	ハードウェア要件	ソフトウェア要件
ルータ 共通要件	① 19インチラックに搭載できること。	① IPv4及びIPv6のルーティングに対応すること。
	② 設定情報の更新/動作状況の確認を行うためのコンソールポートを有すること。	② IPルーティング・プロトコルとして、Static、RIPV1/V2、OSPF、BGP4をサポートしていること。
	③ 光ファイバーケーブルでの接続を行うための、SFPトランシーバを必要個数搭載すること。	③ ポリシーベースルーティングが可能であること。
		④ ネットワークのパフォーマンスを監視/測定するモニタリング機能を有し、その結果により自動で経路切替が可能であること。
		⑤ トラフィックの優先度処理を行うため、QoS機能をサポートしていること。
		⑥ 複数のポリシーレベルで優先度処理を可能とするために階層型QoSをサポートし、トラフィックシェーピングを指定の値で設定可能であること。
		⑦ ACL又は同等の方式によるアクセス制限をサポートしていること。
		⑧ IPSecによる暗号化機能（DES、3DES、AES128、AES256）をハードウェアにてサポートすること。
		⑨ 冗長化機能のため、VRRP（RFC2338）に対応していること。
		⑩ 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。
		⑪ NTP機能による時刻同期をサポートしていること。
		⑫ 運用監視のため、SNMPエージェント機能をサポートしていること。
		⑬ SYSLOG機能をサポートし、ログ転送が可能であること。
		⑭ リモート保守を行うため、SSH機能をサポートしていること。
WANルータ TypeⅠ	① ルータ共通要件を満たすこと。	① ルータ共通要件を満たすこと。
	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。	② 複数のイーサネットポートを論理的に1本に束ねることが可能なこと。
	③ 消費電力が450W以下であること。	
	④ 4Gbps以上のスループットを提供できること。	
	⑤ 拡張性を考慮しインタフェースモジュールの搭載が行えること。	
	⑥ 10BASE-T/100BASE-TX/1000BASE-Tを4ポート以上有すること。	
	⑦ 10BASE-T/100BASE-TX/1000BASE-TとSFPの排他ポートを4ポート以上有すること。	
WANルータ TypeⅡ	① ルータ共通要件を満たすこと。	① ルータ共通要件を満たすこと。
	② 消費電力が100W以下であること。	② スイッチポートはスパニングツリー機能として、IEEE802.1d、IEEE802.1s、IEEE802.1w またはこれらと同等の機能を有し、VLAN ごとに STP を実行可能なこと。
	③ 1.5Gbps以上のスループットを提供できること。	③ スイッチポートはIEEE802.1Q準拠のタグVLAN及びポートベースVLANに対応していること。
	④ 10BASE-T/100BASE-TX/1000BASE-Tのルーテッドポートを2ポート以上有すること。	
	⑤ 10BASE-T/100BASE-TX/1000BASE-Tのスイッチポートを8ポート以上有すること。	
	⑥ 10BASE-T/100BASE-TX/1000BASE-TとSFPの排他ポートを1ポート以上有すること。	
インターネット 接続ルータ	① ルータ共通要件を満たすこと。	① ルータ共通要件を満たすこと。
	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。	② 複数のイーサネットポートを論理的に1本に束ねることが可能なこと。
	③ 消費電力が450W以下であること。	
	④ 4Gbps以上のスループットを提供できること。	
	⑤ 拡張性を考慮しインタフェースモジュールの搭載が行えること。	
	⑥ 10BASE-T/100BASE-TX/1000BASE-Tを4ポート以上有すること。	
	⑦ 10BASE-T/100BASE-TX/1000BASE-TとSFPの排他ポートを4ポート以上有すること。	

【別紙1-2】ルータ・スイッチ要件一覧
③コア・フロア・エッジスイッチ設置台数一覧

項番	拠点名称	コアスイッチ			合計台数	フロアスイッチ				合計台数	エッジスイッチ				合計台数	SFP（1000Base-sx）	メディアコンバータ
		Type Ⅰ	Type Ⅱ	Type Ⅲ		Type Ⅰ	Type Ⅱ	Type Ⅲ	Type Ⅳ		Type Ⅰ	Type Ⅱ	Type Ⅲ	Type Ⅳ			
1	本省	2			2	37				37	129	3	5	2	139	149	11
2	DRサイト		2		2					0					0		
3	総務省第2庁舎（統計局、政策統括官（統計基準担当）、政策統括官（恩給担当））			2	2			5		5	2	51	4	1	58	9	
4	公害等調整委員会				0					0	3				3		
5	内閣人事局				0					0	2				2		
6	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委員会、公共サービス改革推進室）			1	1					0		3			3	4	
7	総務省宮城分室				0					0		1			1		
8	総務省大阪分室				0					0		1			1		
9	自治大学校			1	1				1	1		6	2	2	10	16	
10	情報通信政策研究所			2	2					0	11	3		1	15		
11	国連アジア太平洋統計研修所				0					0		1			1		
12	消防大学校及び消防研究センター　※1			1	1		1		1	2	19				19	20　※2	
13	国会連絡室				0					0		1			1		
14	永田町ビル（電気通信紛争処理委員会・政治資金適正化委員会）				0					0	1				1		
15	統計データ利活用センター				0					0		1			1		
16	北海道管区行政評価局				0					0	4		2	1	7		
17	函館行政監視行政相談センター				0					0	1				1		
18	旭川行政監視行政相談センター				0					0	1				1		
19	釧路行政監視行政相談センター				0					0	1				1		
20	東北管区行政評価局				0					0	4				4		
21	青森行政監視行政相談センター				0					0	1				1		
22	岩手行政監視行政相談センター				0					0	1				1		
23	秋田行政監視行政相談センター				0					0	1				1		
24	山形行政監視行政相談センター				0					0	1				1		
25	福島行政監視行政相談センター				0					0	1				1		
26	関東管区行政評価局				0					0	4				4		
27	茨城行政監視行政相談センター				0					0	1				1		
28	栃木行政監視行政相談センター				0					0	1				1		
29	群馬行政監視行政相談センター				0					0	1				1		
30	千葉行政監視行政相談センター				0					0	1				1		
31	東京行政評価事務所				0					0	1				1		
32	神奈川行政評価事務所				0					0	4				4		
33	新潟行政評価事務所				0					0	1				1		
34	山梨行政監視行政相談センター				0					0	1				1		
35	長野行政監視行政相談センター				0					0	1				1		
36	中部管区行政評価局				0					0	4				4		
37	富山行政監視行政相談センター				0					0	1				1		
38	石川行政評価事務所				0					0	1				1		
39	岐阜行政監視行政相談センター				0					0	1				1		
40	静岡行政監視行政相談センター				0					0	1				1		
41	三重行政監視行政相談センター				0					0	1				1		
42	近畿管区行政評価局				0					0	4				4		
43	福井行政監視行政相談センター				0					0	1				1		
44	滋賀行政監視行政相談センター				0					0	1				1		
45	京都行政監視行政相談センター				0					0	1				1		
46	兵庫行政評価事務所				0					0	1				1		
47	奈良行政監視行政相談センター				0					0	1				1		
48	和歌山行政監視行政相談センター				0					0	1				1		
49	中国四国管区行政評価局				0					0	4				4		
50	鳥取行政監視行政相談センター				0					0	1				1		
51	島根行政監視行政相談センター				0					0	1				1		
52	岡山行政監視行政相談センター				0					0	1				1		

【別紙1-2】ルータ・スイッチ要件一覧
③コア・フロア・エッジスイッチ設置台数一覧

項番	拠点名称	コアスイッチ			合計台数	フロアスイッチ				合計台数	エッジスイッチ				合計台数	SFP（1000Base-sx）	メディアコンバータ
		Type Ⅰ	Type Ⅱ	Type Ⅲ		Type Ⅰ	Type Ⅱ	Type Ⅲ	Type Ⅳ		Type Ⅰ	Type Ⅱ	Type Ⅲ	Type Ⅳ			
53	山口行政監視行政相談センター				0					0	1				1		
54	四国行政評価支局				0					0	4				4		
55	徳島行政監視行政相談センター				0					0	1				1		
56	愛媛行政監視行政相談センター				0					0	1				1		
57	高知行政監視行政相談センター				0					0	1				1		
58	九州管区行政評価局				0					0	3				3		
59	佐賀行政監視行政相談センター				0					0	1				1		
60	長崎行政監視行政相談センター				0					0	1				1		
61	熊本行政評価事務所				0					0	1				1		
62	大分行政監視行政相談センター				0					0	1				1		
63	宮崎行政監視行政相談センター				0					0	1				1		
64	鹿児島行政監視行政相談センター				0					0	1				1		
65	沖縄行政評価事務所				0					0	2				2		
66	北海道総合通信局			2	2					0	6				6	4	
67	東北総合通信局			2	2					0	8				8	8	4
68	関東総合通信局			2	2					0	11	2			13	2	2
69	関東総合通信局（三浦電波監視センター）				0					0	1	1			2		
70	信越総合通信局			2	2					0	4				4	4	
71	北陸総合通信局			2	2					0		6			6		
72	東海総合通信局			2	2		6			6		19			19	8	4
73	近畿総合通信局			2	2					0	4				4		
74	中国総合通信局			2	2					0	6				6	4	
75	四国総合通信局			2	2					0		12			12		
76	九州総合通信局			2	2					0		14		1	15	8	4
77	沖縄総合通信事務所			2	2					0		5			5		
78	外部監視室				0					0					0		
	タイプ別台数合計	2	2	29	33	37	7	5	2	51	284	130	13	8	435	216	25

※1　現行ではコアスイッチが複数台あるが、コアスイッチは拠点内で1台（1セット）とし、他はフロアスイッチとして換算
※2　消防大学校及び消防研究センターでは、「1000BASE-SX」SFP20個とは別に「1000BASE-LX」SFPが1個必要（メディアコンバータ等での対応でも可）

【別紙1-2】ルータ・スイッチ要件一覧
④スイッチスペック要件一覧

機器タイプ	スイッチスペック要件	
	ハードウェア要件	ソフトウェア要件
スイッチ 共通要件	① 19インチラックに搭載できること。	① スパニングツリー機能として、IEEE802.1d、IEEE802.1s、IEEE802.1wまたはこれらと同等の機能を有し、VLANごとにSTPを実行可能なこと。
	② 設定情報の更新/動作状況の確認を行うためのコンソールポートを有すること。	② IEEE802.1pのCOS、TOS及びDSCPの書き換え、書き込み、DSCPに基づく優先制御が可能であること。
	③ 光ファイバーケーブルでの接続を行うための、光トランシーバ（SFP/SFP+等）を必要個数搭載すること。	③ ACL又は同等の方式によるアクセス制限が行えること。
	④ 光ファイバーケーブルを流用する場合は、配線されているケーブルの形状に合わせて光トランシーバ（SFP/SFP+等）を用意すること。	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 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。
		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有すること。
		⑧ NTP機能による時刻同期をサポートしていること。
		⑨ 運用監視のため、SNMPエージェント機能をサポートしていること。
		⑩ SYSLOG機能をサポートし、ログ転送が可能であること。
		⑪ リモート保守を行うため、SSH機能をサポートしていること。
コアスイッチ Type Ⅰ	① スイッチ共通要件を満たすこと。	① スイッチ共通要件を満たすこと。
	② シャーシ型筐体であること。	② 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。
	③ 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 IPルーティング・プロトコルとして、Static、RIPV1/V2、OSPFをサポートしていること。
	④ 消費電力が4,000W以下であること。	
	⑤ 2Tbps以上のスイッチング容量を有していること。	
	⑥ フロアスイッチとの接続用に1000BASE-SXが48ポート以上のインタフェースモジュールを搭載すること。	
	⑦ UTPでの接続用に100BASE-TX/1000BASE-Tが48ポート以上のインタフェースモジュールを搭載すること。	
	⑧ 上記⑥⑦以外にネットワーク構成上必要なモジュールがあれば搭載した上で、インタフェースモジュール拡張用の空きスロットが1つ以上あること。	
コアスイッチ TypeⅡ	① スイッチ共通要件を満たすこと。	① スイッチ共通要件を満たすこと。
	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。	② 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。
	③ 500Gbps以上のスイッチング容量を有すること。	③ IPルーティング・プロトコルとして、Static、RIPV1/V2、OSPFをサポートしていること。
	④ ポート種別及びポート数は指定しない。	
コアスイッチ TypeⅢ	① スイッチ共通要件を満たすこと。	① スイッチ共通要件を満たすこと。
	② 消費電力が110W以下であること。	② 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。
	③ 112Gbps以上のスイッチング容量を有すること。	③ IPルーティング・プロトコルとして、Static、RIPV1/V2、OSPFをサポートしていること。
	④ 100BASE-TX/1000BASE-Tを24ポート以上有すること。	④ DHCPリレー機能を有すること。
	⑤ 1000BASEのSFPを4ポート以上搭載できること。	⑤ 2台のスイッチを論理的に1台の仮想的なスイッチにクラスタ化する仮想化技術を有すること。
		⑥ クラスタ化したスイッチで複数の筐体にまたがったイーサネットポートを論理的に1本に束ねることが可能なこと。

【別紙1-2】ルータ・スイッチ要件一覧
④スイッチスペック要件一覧

機器タイプ	スイッチスペック要件	
	ハードウェア要件	ソフトウェア要件
フロアスイッチ Type I	① スイッチ共通要件を満たすこと。	① スイッチ共通要件を満たすこと。
	② 消費電力が715W以下であること。	② 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。
	③ 112Gbps以上のスイッチング容量を有すること。	③ IPルーティング・プロトコルとして、Static、RIPV1/V2、OSPFをサポートしていること。
	④ 100BASE-TX/1000BASE-Tを24ポート以上有すること。	④ DHCPリレー機能を有すること。
	⑤ 100BASE-TX/1000BASE-TのポートはPoE+に対応し、300W以上の給電が可能であること。	⑤ 2台のスイッチを論理的に1台の仮想的なスイッチにクラスタ化する仮想化技術を有すること。
	⑥ 1000BASEのSFPを4ポート以上搭載できること。	⑥ クラスタ化したスイッチで複数の筐体にまたがったイーサネットポートを論理的に1本に束ねることが可能なこと。
フロアスイッチ TypeII	① スイッチ共通要件を満たすこと。	① スイッチ共通要件を満たすこと。
	② 消費電力が110W以下であること。	② 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。
	③ 112Gbps以上のスイッチング容量を有すること。	③ IPルーティング・プロトコルとして、Static、RIPV1/V2、OSPFをサポートしていること。
	④ 100BASE-TX/1000BASE-Tを24ポート以上有すること。	④ DHCPリレー機能を有すること。
	⑤ 1000BASEのSFPを4ポート以上搭載できること。	⑤ 2台のスイッチを論理的に1台の仮想的なスイッチにクラスタ化する仮想化技術を有すること。
		⑥ クラスタ化したスイッチで複数の筐体にまたがったイーサネットポートを論理的に1本に束ねることが可能なこと。
フロアスイッチ TypeIII	① スイッチ共通要件を満たすこと。	① スイッチ共通要件を満たすこと。
	② 消費電力が200W以下であること。	② 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。
	③ 176Gbps以上のスイッチング容量を有すること。	③ IPルーティング・プロトコルとして、Static、RIPV1/V2、OSPFをサポートしていること。
	④ 100BASE-TX/1000BASE-Tを48ポート以上有すること。	④ DHCPリレー機能を有すること。
	⑤ 1000BASEのSFPを4ポート以上搭載できること。	⑤ 2台のスイッチを論理的に1台の仮想的なスイッチにクラスタ化する仮想化技術を有すること。
		⑥ クラスタ化したスイッチで複数の筐体にまたがったイーサネットポートを論理的に1本に束ねることが可能なこと。
フロアスイッチ TypeIV	① スイッチ共通要件を満たすこと。	① スイッチ共通要件を満たすこと。
	② 消費電力が100W以下であること。	② 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。
	③ 24Gbps以上のスイッチング容量を有すること。	③ IPルーティング・プロトコルとして、Static、RIPV1/V2、OSPFをサポートしていること。
	④ 1000BASEのSFPを必要ポート数搭載できること。なお1台での構成が難しい場合は、2台での構成も可とする。	④ DHCPリレー機能を有すること。
		⑤ 複数のイーサネットポートを論理的に1本に束ねることが可能なこと。
エッジスイッチ Type I	① スイッチ共通要件を満たすこと。	① スイッチ共通要件を満たすこと。
	② 消費電力が60W以下であること。	② レイヤ2のスイッチングを行えること。
	③ 100Gbps以上のスイッチング容量を有すること。	
	④ 100BASE-TX/1000BASE-Tを48ポート以上有すること。	
	⑤ 1000BASEのSFPを2ポート以上搭載できること。	

【別紙1-2】ルータ・スイッチ要件一覧
④スイッチスペック要件一覧

機器タイプ	スイッチスペック要件	
	ハードウェア要件	ソフトウェア要件
エッジスイッチ TypeⅡ	① スイッチ共通要件を満たすこと。	① スイッチ共通要件を満たすこと。
	② 消費電力が50W以下であること。	② レイヤ2のスイッチングを行えること。
	③ 52Gbps以上のスイッチング容量を有すること。	
	④ 100BASE-TX/1000BASE-Tを24ポート以上有すること。	
	⑤ 1000BASEのSFPを2ポート以上搭載できること。	
エッジスイッチ TypeⅢ	① スイッチ共通要件を満たすこと。	① スイッチ共通要件を満たすこと。
	② 消費電力が20W以下であること。	② レイヤ2のスイッチングを行えること。
	③ 20Gbps以上のスイッチング容量を有すること。	
	④ 100BASE-TX/1000BASE-Tを8ポート以上有すること。	
	⑤ 1000BASEのSFPを2ポート以上搭載できること。	
エッジスイッチ TypeⅣ	① スイッチ共通要件を満たすこと。	① スイッチ共通要件を満たすこと。
	② 消費電力が250W以下であること。	② レイヤ2のスイッチングを行えること。
	③ 20Gbps以上のスイッチング容量を有すること。	
	④ 100BASE-TX/1000BASE-Tを8ポート以上有すること。	
	⑤ 100BASE-TX/1000BASE-TのポートはPoE+に対応し、180W以上の給電が可能であること。	
	⑥ 1000BASEのSFPを2ポート以上搭載できること。	
メディア コンバータ	① ボックス型筐体であること。	① 1000BASE-Tと1000BASE-SXの変換機能を有すること。
	② 1000BASE-Tを1ポート以上有すること。	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。
	③ 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。	

【別紙1-3】回線一覧

拠点名称	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	帯域確保	1Gbps	DDoS対策要件あり
	インターネット回線2	ベストエフォート	1Gbps	
	インターネット回線3	ベストエフォート	1Gbps	
DRサイト	インターネット回線1	帯域確保	1Gbps	
	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	1Gbps	
	副回線	ベストエフォート	1Gbps	
	本省DRサイト接続回線	帯域確保	1Gbps	
DRサイト	主回線	帯域確保	1Gbps	
	副回線	ベストエフォート	1Gbps	
	本省DRサイト接続回線	帯域確保	1Gbps	
総務省第2庁舎（統計局、政策統括官（統計基準担当）、政策統括官（恩給担当））	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	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	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	
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委員会、公共サービス改革推進室）	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	
総務省宮城分室	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	
総務省大阪分室	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	
国連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	
永田町ビル（電気通信紛争処理委員会・政治資金適正化委員会）	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	
統計データ利活用センター	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	
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	-	-	
函館行政監視行政相談センター	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	
旭川行政監視行政相談センター	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	
釧路行政監視行政相談センター	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	
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	-	-	
青森行政監視行政相談センター	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	
岩手行政監視行政相談センター	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	
秋田行政監視行政相談センター	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	
山形行政監視行政相談センター	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	
福島行政監視行政相談センター	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	
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	
茨城行政監視行政相談センター	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	
栃木行政監視行政相談センター	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	
群馬行政監視行政相談センター	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	
千葉行政監視行政相談センター	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	

【別紙1-3】回線一覧

拠点名称	回線	回線種別	帯域	備考
山梨行政監視行政相談センター	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	
長野行政監視行政相談センター	主回線	-	-	信越総合通信局と共用
	副回線	-	-	
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	
富山行政監視行政相談センター	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	
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	
岐阜行政監視行政相談センター	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	
静岡行政監視行政相談センター	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	
三重行政監視行政相談センター	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	
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	
福井行政監視行政相談センター	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	
滋賀行政監視行政相談センター	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	
京都行政監視行政相談センター	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	
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	
奈良行政監視行政相談センター	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	
和歌山行政監視行政相談センター	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	
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	
鳥取行政監視行政相談センター	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	
島根行政監視行政相談センター	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	
岡山行政監視行政相談センター	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	
山口行政監視行政相談センター	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	
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	
徳島行政監視行政相談センター	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	
愛媛行政監視行政相談センター	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	
高知行政監視行政相談センター	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	
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	
佐賀行政監視行政相談センター	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	
長崎行政監視行政相談センター	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	
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	
大分行政監視行政相談センター	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	
宮崎行政監視行政相談センター	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	
鹿児島行政監視行政相談センター	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	
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	

【別紙1-3】回線一覧

拠点名称	回線	回線種別	帯域	備考
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	
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	
監視用回線				
本省	監視用回線	ベストエフォート	1Gbps	
DRサイト	監視用回線	ベストエフォート	1Gbps	
外部監視室	監視用回線	ベストエフォート	1Gbps	

【別紙1-4】情報セキュリティ要件詳細

第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、統一基準群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もの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 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。
		⑤ 脆弱性監査について、主管課から協力要請があった場合、これに応じること。
		⑥ 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。
		⑦ 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。
		⑧ 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。
		⑨ 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。
		⑩ 不要な通信は抑制すること。
		⑪ 内閣サイバーセキュリティセンターが設置するGSOCセンサーについて、必要となる対応を行うこと。
		⑫ 総務省LANのリスク分析を実施し、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。
		⑬ 受託者は、本調達における納入機器等について、設計書、仕様書、操作マニュアル等の運用管理に必要となる文書を作成すること。また、当該機器の設計や仕様、操作方法等に変更が発生した場合は、これらの文書を適時更新すること。
	2 主体認証	
		① 総務省LANでは、ユーザがシステムを利用する際、アカウントの共有による不正利用やなりすましを防止するため、生体認証を利用すること。
		② 生体認証が使えない場合も想定し、アカウント名、パスワードを用いた主体認証も併せて行うこと。
		③ 運用担当者がサーバやネットワーク機器にログオンする際においても主体認証を行うこと。
		④ システムや機器の種類に応じて、適切な認証方式（ダイジェスト認証、ワンタイムパスワード、多要素認証等）を採用すること。なお、多要素（複合）主体認証方式については、SMSを用いた認証を避けること。
		⑤ パスワード盗用のリスクを下げる為、パスワード長（10桁以上かつ20桁以下）、文字種別の指定（英大文字・英小文字・数字・記号より3種類以上）、同一パスワードの禁止等の機能を有すること。
		⑥ 不正にログオンしようとする行為を検知又は防止する機能を有すること。
		⑦ リモートアクセス（外部からLAN端末及び私物端末を用いた総務省LANへの接続）時はワンタイムパスワードを用いて認証を行い、認証通信は暗号化を施すこと。

	⑧ 管理者権限を持つ識別コードを共用する場合には、当該識別コードでログインする前に個別の識別コードによりログオンする機能を有すること。
	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。
	⑩ 主体認証情報を保存する場合は、暗号化する、アクセス制限を用いるなどの方法を用いて適切に管理すること。
	⑪ 利用者が主体認証情報を定期的に変更しているか否かを確認する機能、又は利用者が定期的に主体認証情報を変更しなければ情報システムの利用を継続させない機能を有すること。
	⑫ 主体認証情報及び対応する識別コードの利用を停止する機能を有すること。
	⑬ 主体認証情報を用いる場合に、利用者が自らの主体認証情報を設定する機能を有すること。
	⑭ 以前に設定したパスワードと同じものを再設定することを防止する機能を有すること。
3 アクセス制御・権限管理	
	① ユーザアカウントはシステムにおける作業者の役割ごと（各種システム操作を含む）に作成し、作業に必要な権限のみの付与等、目的に応じた適切なアクセス制限、権限管理及び設定を行うこと。
	② アクセス制御は拒否を前提とし、必要な通信のみを許可する方針とすること。
	③ アクセス制御は、IPアドレス単位かつポート単位で実施すること。
	④ 総務省LAN内のネットワークを用途ごとにセグメント分けし、必要に応じてセグメント間の通信経路を分離すること。
	⑤ 各種サービスと運用管理のセグメントは通信経路を分離し、適切なアクセス制御を行うこと。
	⑥ 総務省LANからインターネットへの接続に関しては適切なアクセス制御を行うこと。
	⑦ 総務省LANからインターネットコンテンツへの適切なフィルタリングを実施すること。
	⑧ 情報システムに保存される機微度の高い情報について、権限のある職員のみがアクセスできるようにするため、機密情報保護サービスを導入すること。
	⑨ 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。
	⑩ 管理者権限による操作は、特定の環境でのみ実施可能なように限定し、当該環境において操作ログを取得すること。
	⑪ 運用管理者が変更になった場合やシステム変更等の理由で不要となった運用管理者等のアカウントは、即時アカウントを削除し、使い回すことのないようにすること。
	⑫ 総務省LANへのアクセスは主管課が認める者に限ること。
	⑬ LAN端末から特権アクセス権限を用いた機器アクセスが行えないこと。
	⑭ サーバやデータへのアクセスについてはアクセス権限を適切に設定すること。
	⑮ 職員のアカウントは、「総務省共通基盤支援システム」により発行されたものを総務省LANに連携し、総務省LANでは1アカウントが1職員に対応するように運用すること。

		⑯ 不正アクセスのリスクに繋がる不要なアカウントを定期的に抽出し、必要に応じて削除できる対策を講ずること。
		⑰ 異動や退職等で不要となった職員のアカウントは、一時保管用アカウントとして無効化した状態で30日間以上保持すること。
		⑱ システム操作（移行等の作業におけるシステム操作を含む）に際しては主体認証を行い、認証通信は暗号化を施すこと。
		⑲ 主体認証情報の再発行を自動で行う機能を有すること。
	4 ログの取得・管理	
		① 提供するサービスにおける証跡ログ等を収集し、必要な証跡に対して分析する機能を有すること。なお、ログの取得・管理に関しては、統一基準群に準拠すること。
		② 総務省LANにおいて、職員へ提供するサービス（アプリケーション）、サーバ、LAN端末、ネットワーク機器、アプライアンスの証跡ログを収集すること。
		③ 収集する証跡ログは以下に示すものを想定している。具体的な収集情報については、主管課と協議の上で決定すること。 ・システム監査ログ（管理者による操作、設定変更等） ・ユーザ認証ログ ・ファイルの操作ログ ・メールの送受信ログ（メールジャーナル） ・プロセス起動／停止ログ ・ログオン／ログオフログ ・ウイルスを含むマルウェア及び脅威の検知ログ ・ウェブアクセスログ ・DNSクエリーログ ・チャットやWeb会議の発着信履歴 ・その他主管課が必要と認めた情報
		④ 証跡ログには、日時、ユーザ名、事象の種類（ファイルへのアクセス、ウェブサイトへのアクセス、ログオン及びログオフ等）、事象の対象（アクセスしたファイル名及びファイル操作内容、アクセスしたURL、ログインしたアプリケーション等）等に関する認証情報を収集できること。証跡情報は一元管理できること。
		⑤ 証跡ログは3年間以上保管し、必要に応じてログの調査が可能であること。証跡ログは、次々期総務省LANに引き継げること。
		⑥ 証跡ログは原則、CSV形式等の標準的な形式で保存すること。又は、証跡ログを平易にCSV形式等の標準的な形式に変換できること。
		⑦ 証跡ログは、主管課が指定する外部環境等に転送可能なこと。
		⑧ 内部からの不正操作、ユーザの誤操作等による情報セキュリティ上の脅威に対応する為、管理者権限操作を含めた証跡ログを取得すること。
		⑨ 取得した証跡ログを用いて、必要に応じて点検及び分析を行いその結果をもって対策の要否とリスクの有無を判断して報告すること。また、リスクのあった事象については、他の環境においても同様の対応を行うこと。
		⑩ 証跡ログは適切な権限を有した主管課及び本調達事業者のみ閲覧できるよう権限を付与すること。
		⑪ 証跡ログは完全性を保つ為、収集サーバの管理者を他のサーバ等の管理者と異なる者とする等、改ざん防止の対策を講ずること。
		⑫ 総務省LANに対する不正の検知、発生原因の特定に用いるために、総務省LANの利用記録、例外的事象の発生に関する証跡を蓄積し、保管すること。証跡の不当な消去や改ざんを防止する為、証跡に関するアクセス制御機能を備えること。

【別紙1-4】情報セキュリティ要件詳細

		⑬ 不正行為の追跡や情報セキュリティ侵害時において証跡の解析等を容易にする為、システム内の機器を正確な時刻に同期する機能を備えること。
		⑭ 提供するサービスについては、認証ログ、アクセスログ及びアプリケーションログ等の証跡情報を保管すること。
		⑮ 監視対象の機器等の状態を変更する操作（シャットダウン、リブート等）は証跡情報として記録すること。
		⑯ LAN端末については、ログオン、ログオフ及びファイル操作の証跡情報を保管すること。
		⑰ 端末操作の証跡ログについて、ファイル名を起点とした流出経路のトレースが可能なこと。
		⑱ メール送受信やウェブアクセスの証跡情報を保管すること。
		⑲ インターネットを対象としたWeb閲覧の通信を復号し証跡を取得すること。
		⑳ 証跡が取得できなくなった場合及び取得できなくなるおそれがある場合、これらに対処するための機能を有すること。
		㉑ 各サーバやセキュリティ機器から収集された証跡情報を基に相関分析等をすることにより、不審な動作を検出可能とすること。また、相関分析等により、情報セキュリティ侵害の可能性を示す事象を検知した場合に、管理者にその旨を即時に通知する機能を有すること。
	5 暗号・電子署名	
		① 総務省LANから外部に送信するデータについては暗号化を行うことで個人情報や機密情報が保護されるように対策を講ずること。暗号化の方式、適用範囲等に関しては、主管課と協議の上、決定すること。
		② 暗号及び電子署名のアルゴリズムについては、運用期間中に強度の高いアルゴリズムへ従来方式との互換性を確保しつつ移行することを想定した上で、設計・構築を実施すること。
		③ 暗号及び電子署名のアルゴリズムについては、「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）（平成25年3月1日総務省・経済産業省策定）」に記載されたものを使用すること。
		④ 情報システムのコンポーネントとして、暗号化モジュールを交換することが可能なこと。
		⑤ 複数のアルゴリズムを選択可能なこと。
		⑥ 暗号化された情報の復号又は電子署名の付与に用いる鍵を、耐タンパ性を有する暗号モジュールへ格納すること。
		⑦ 暗号モジュールテスト及び認証制度による認証取得製品を選択すること。
		⑧ インターネット経由のリモートアクセス及び無線LANの通信経路は暗号化すること。

【別紙1-4】情報セキュリティ要件詳細

6 ソフトウェアに関する脆弱性対策	
	① 本調達において導入する全てのファームウェア、ソフトウェア等に関連するセキュリティホール情報は公開され次第入手する体制を整えること。
	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 セキュリティホール対策の実施に際しては、事前に総務省LAN運用環境への影響検討、検証作業等を実施し、それらの結果を踏まえて主管課との協議により対応方針を決定すること。
	④ セキュリティパッチ等の提供情報は公表後速やかに主管課に報告し、主管課の承認の上、迅速かつ適切な対策を講ずること。
	⑤ ファイアウォール等のセキュリティ機器は適切なセキュリティ設定を維持すること。
	⑥ 機器やソフトウェアはアカウント、パスワード等を初期設定値の状態で運用しないこと。また、推察されやすい安易なユーザアカウント、パスワード等を設定しないこと。
	⑦ セキュリティ上の脆弱性が発見され、対策用パッチが利用可能になった場合、日本語環境下で動作確認を実施した上で速やかに更新すること。また、パッチ等の適用状況を管理すること。
	⑧ 利用者への提供及び運用に用いるものを除く、不要なプロセス、サービス等は原則停止すること。
	⑨ インターネットからのアクセスに対し、システムを構成するソフトウェアのバージョンを取得されない設定を行うこと。
	⑩ インターネットからのアクセスに対し、エラーを返す際に、OSやサービスのバージョンが表示されない対策をとること。
	⑪ 利用するソフトウェアは、ソフトウェア保守サポートが契約期間終了まで継続されるもののみを利用すること。
	⑫ 総務省LANを構成するファームウェア及びソフトウェアの脆弱性を悪用した不正を防止する為、設計・構築時に脆弱性の有無を確認の上、運用上対処が必要な脆弱性は全て対応の上で導入すること。
	⑬ 運用開始後、新たに発見される脆弱性を悪用した不正を防止する為、総務省LANを構成するファームウェア及びソフトウェアの更新を効率的に実施する機能を備えると共に、総務省LAN全体の更新漏れを防止する機能を備えること。
	⑭ 定期的に実施される脆弱性の診断を含むセキュリティ監査等に対して、主管課からの指示により、必要な情報の提示、書類の作成、システム開示対応等を行うこと。
	⑮ 受託者は、本調達における納入機器等のうち、脆弱性対策が必要となるそれぞれの機器について、機種並びに機器が利用しているソフトウェアの種類及びバージョンを記載した書面を作成すること。また、機能向上や脆弱性対策等によるソフトウェアのバージョンアップを実施する場合は、これらの書面を適時更新すること。なお、上記情報の収集に当たっては、自動でソフトウェアの種類やバージョン等を管理する機能を有するIT資産管理ソフトウェアを導入するなどにより、これら情報を効率的に収集する手法を決定すること。

【別紙1-4】情報セキュリティ要件詳細

7 不正プログラム対策	
(1) 基本要件	① 提供するサービスにおける証跡ログ等を収集し、必要な証跡に対して相関分析する機能を有すること。なお、証跡管理に関しては、統一基準等に準拠すること。
	② 本調達において導入する全てのサーバ及び端末について、既知及び未知の不正プログラムの検知及びその実行の防止の機能を有する、利用するOSごとに適合した不正プログラム対策ソフトウェアを導入すること。ただし、当該電子計算機で動作可能な不正プログラム対策ソフトウェアが存在しない場合を除く。
	③ 不正プログラム対策ソフトウェアが定義ファイルを用いる場合、当該定義ファイル更新は、インターネット経由で当該ファイル更新情報を自動で取得し、自動更新が可能なこと。
	④ 不正プログラム対策ソフトウェア等に係る当該ソフトウェア本体及び定義ファイル等のうち、オンラインで提供されるものは常に最新の状態に維持すること。
	⑤ 独自OSを搭載したアプライアンス製品を除き、不正プログラムに感染した場合、リアルタイム、スケジュール設定及び手動検索により隔離、又は駆除が行われ、他のサーバや端末に影響を及ぼさないこと。
	⑥ 常に不正プログラム対策ソフトウェアの製造元から、最新の脅威に関する拡散情報、注意喚起情報等が提供されること。
	⑦ 不正プログラム対策ソフトウェアの動作により、関係するサーバ及び端末に著しい遅延が発生しないこと。
	⑧ 本調達において導入する全てのサーバ及び端末において、不正プログラム対策ソフトウェアを利用した定期的なチェックが自動的にできること。なお、当該装置において、不正プログラム対策ソフトウェアが存在しない場合、又は不正プログラム対策ソフトウェアがインストール不可能な場合は主管課との協議により対応方針を決定すること。
	⑨ マルウェア（ウイルス、ワーム、ボット等）及びスパイウェア（キーロガー、アドウェア等）といった不正なプログラムに対する検出機能及び削除機能を有すること。
	⑩ マルウェアによる脅威に備える為、マルウェアの感染を防止する機能を備えると共に、新たに発見されるマルウェアに対応するために機能の更新が可能なこと。
	⑪ 定義ファイルの配信及び感染端末等の管理ができること。
	⑫ メール送受信経路上でメールの不正プログラム対策を実施すること。
	⑬ インターネット上のコンテンツへ通信する場合は、原則、プロキシサービスを経由し、プロキシサービスにおいて不正プログラム対策を実施すること。
	⑭ 脆弱な端末の総務省LANへの接続を防止するため、不正端末の接続制御を行うこと。
	⑮ 不正プログラムを検知した場合、管理者へ通知できること。
	⑯ 受託者は、不正な変更が加えられた機器等を調達することを防止するため、当該機器等を製造する企業及び製造国が確認できる書面を提出すること。
	⑰ 受託者は、納入する機器等の一覧をあらかじめ総務省に提出するとともに、総務省から代替品選定やリスク低減対策等の指示があった場合は、総務省からの指示を受け、必要な対応を実施すること。
	⑱ 受託者は、納入した機器等に不正な変更が発見された場合の対応として、総務省と連携を図りながら製造元への問合せや調査依頼等、不正な変更が加えられた理由や原因等の調査に必要な対応を実施すること。

【別紙1-4】情報セキュリティ要件詳細

(2) サーバにおける対策	
①	導入する全てのサーバに対して、不正プログラム対策機能をインストールすること。独自OSを搭載したアプライアンス製品の場合は除いてよいが、ファイルサーバの場合については、独自OSを搭載したアプライアンス製品であってもファイルサーバ上の共有ファイルを不正プログラム対策の対象とすること。
②	各サーバは不正プログラム対策管理サーバに総務省LAN経由でアクセスし、あらかじめ指定したスケジュールにより定義ファイルを自動的に実行・更新できること。
③	総務省LAN内部へマルウェア・スパイウェア等の不正プログラムが侵入した場合に備え、サーバ上での検知、当該プログラムの実行防止、一時的な通信制限の適用等、標的型攻撃への対策を行うこと。
(3) LAN端末における対策	
①	LAN端末に対して、不正プログラム対策機能をインストールすること。
②	LAN端末は不正プログラム対策管理サーバに総務省LAN経由でアクセスし、あらかじめ指定したスケジュールにより定義ファイルを自動的に実行・更新できること。
③	総務省LAN内部へマルウェア・スパイウェア等の不正プログラムが侵入した場合に備え、エンドポイント上での検知、当該プログラムの実行防止、一時的な通信制限の適用等、標的型攻撃への対策を行うこと。
④	インターネット上のコンテンツへ通信する場合は、インターネット閲覧サービスを利用すること。
⑤	LAN端末上のブラウザからは、一部の許可されたコンテンツを除き、原則、インターネットへ通信できないようにすること。
⑥	LAN端末に接続可能な外部記憶デバイスは、セキュリティUSBメモリのみとし、これ以外の外部記憶デバイスは利用できないよう構成すること。
⑦	LAN端末とは隔離されたセグメントにウイルスチェック用端末を設置し、外部記憶デバイスを用いて外部から持ち込むデータは、ウイルスチェック用端末においてウイルスチェックを実施した後、LAN端末に取り込むこと。
(4) 感染拡大防止機能	
①	不正プログラムの実行を検知した場合、当該プログラムの実行阻止、関連するプロセスの停止及び端末の通信制限等により感染拡大を防止する機能を有すること。
②	総務省LAN内のネットワークを用途ごとにセグメント分けし、必要に応じてセグメント間の通信を制御すること。
③	サーバ及び端末のパーソナルファイアウォール機能を利用し、ホスト間の通信を必要最小限に制限すること。
④	パーソナルファイアウォールのログを相関分析等の対象とすることにより不正な通信の発生を検出可能とすること。
(5) 未知の不正プログラムへの対応	
①	既知の不正プログラムの亜種及び新たな脆弱性を突く不正プログラム等、未知の不正プログラムの検知及び感染防止のための機能を有すること。
②	証跡ログ等を監視及び分析し、内部に侵入した未知の不正プログラムを早期に検知すること。

【別紙1-4】情報セキュリティ要件詳細

8 サービス不能攻撃対策	
	① フラッディング攻撃（Syn Flood、UDP Flood、ICMP Flood等）を検知し、攻撃とみなされた通信を廃棄可能なこと。フラッディング攻撃とみなされる通信のログを取得可能なこと。
	② 接続元コネクション数制限、接続先コネクション数制限が可能なこと。
	③ 攻撃種別ごとにしきい値の設定が行え、しきい値を超えた場合に攻撃と検知可能なこと。
	④ 不正元を特定する為、ホワイトリストに一致しないアプリケーションを検出した場合やブラックリストに一致したアプリケーションを検出した場合にログ採取可能で、収集したログの分析を実施し、主管課との協議により、対象の通信を許可する設定、対象の通信を拒否する設定が可能なこと。
	⑤ 上記以外の新たな攻撃の兆候に対して、必要となる対策を検討し対応すること。
	⑥ 分散サービス不能攻撃を検知及び収束を確認した場合、管理者へ通知できること。
9 標的型攻撃対策	
	① 標的型攻撃等の対策の詳細内容については、設計段階において、主管課との調整や協議の上、決定すること。なお、運用中において、日々変化する攻撃手法に対して対策内容の見直し・改善を適宜実施すること。
	② 外部から総務省LAN内部への標的型攻撃による侵入を低減する対策（入口対策）を講ずること。
	③ 総務省LAN内部における、侵入した攻撃の早期検知、感染拡大の防止や、外部への不正通信を検知して対処する対策（内部対策）を講ずること。対策に当たっては定義ファイルによるパターンマッチング、振る舞い検知機能、サンドボックス技術（仮想解析）等、異なる技術を複数用いることで検知精度の向上を図ること。

【別紙1-4】情報セキュリティ要件詳細

第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おそれがある場合には、速やかに主管課に報告すること。
	③ 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。 ・受託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 ・受託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、タブレット型端末及び私物端末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えい等、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 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 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 総務省LANの稼働後は年次にてセキュリティ診断を実施すること。

【別紙1-4】情報セキュリティ要件詳細

4 機密保持	
	① 総務省から受託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、調達仕様書の別紙7「情報保護管理要領」に準拠すること。
5 入退室管理	
	① 受託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 受託者の作業場所では、主管課の許可なく受託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 受託者は、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。
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 受託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。

【別紙1-5】保守・運用要件詳細

第1 運用
1 全体概要
(1) 設計要件
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。
② 運用範囲は、「【別紙1-1】機能要件詳細」に基づき提供されるサービス全般とする。
③ 別調達である運用管理・受付窓口請負事業者の受付窓口から連携されたユーザ問い合わせの対応支援を行うこと。 また、運用管理・受付窓口請負事業者との間で、認識齟齬や問い合わせ対応などにおける情報連携ミスなど発生しないように対策すること。
④ 受付窓口からのリモートアクセス（LAN端末やタブレット端末）については、運用管理・受付窓口請負事業者と協議の上、主管課へ報告し対応すること。
⑤ 主管課が別途調達しているLAN端末、LAN複合機・プリンタ、ソフトウェアの運用は、本調達で設計した内容に対しては運用範囲に含まれること。
⑥ 既存流用した機器、配線、19インチラック、電源設備（この項では資材という）等の保守は、本調達の範囲に含まない。 ただし、既存流用した資材に対し、資材の管理責任者、利用状況、状態等を資料化して把握し、管理すること。 既存流用した資材に対する保守依頼の一次窓口は受託者が対応し、保守作業については、管理責任者と協議の上、適切な対応を行うこと。
⑦ 本仕様書に示す以外で、保守・運用業務を円滑に行うために必要となる作業があれば受託者が行うこと。
⑧ 本省が被災し、本省LAN管理室での保守・運用サービスが行えない場合、受託者は数日以内（目標3日以内）に適切な要員を揃え、総務省LAN保守・運用事業者の代替施設からDRサイトへリモートアクセスし、保守・運用サービスの対応を行うこと。 なお、総務省LAN保守・運用事業者の代替施設については、提案の上、主管課の承認を得ること。
⑨ 受託者は、国際規格であるISO/IEC 20000 Part1,Part2（国内規格はJIS Q20000）に基づいて、ITサービスを提供する受託者のITサービスマネジメントが適切であるかどうかを評価するため、認証基準であるITSMS（ITサービスマネジメントシステム）が構築・運用されているかを、信頼できる第三者からの評価を得ていること。
⑩ 受託者は、「【別紙1】要件定義書」、「【別紙1-1】機能要件詳細」を基に、提案書、運用計画書、保守作業計画書の案を踏まえ、定常時及び障害時において想定される運用体制、保守体制、実施手順等を取りまとめた「運用手順書」及び「保守作業手順書」の案を作成し、主管課の承認を受けること。
(2) 全体要件
① システム運用に必要な消耗品は、受託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 受付窓口と連携し、ナレッジ管理・インシデント管理・申請管理などの情報を共有し、ユーザへの技術的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。
⑤ ユーザに業務影響を与える障害等が発生した場合は、受託者が主体となって対応措置を行う。 その際、決められた範囲での対応のみを行うのではなく、状況に応じて受付窓口と協力し、一体となって検討し早期解決を行うこと。

【別紙1-5】保守・運用要件詳細

ア 保守・運用要領	
	① 「標準ガイドライン 」、ITIL V3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「保守・運用要領」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 ・保守・運用要領の改訂手順 等
イ 定期報告	
	① 主管課に対して、総務省LANの保守・運用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の保守・運用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1-5】保守・運用要件詳細

(ア) 日次報告
① 現行の報告を踏襲すること。 例として、資料閲覧時に以下の内容を確認すること。 1.受付窓口からの支援作業の報告 ・問い合わせ対応件数 ・問い合わせ内訳 2.障害報告 ・発生障害件数 ・障害状況 ・ウイルス対応状況 3.日次作業報告 ・確認事項 ・申請処理進捗 ・LAN端末追加モジュール適用 4.特記事項 ・セキュリティインシデント対応
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 現行の報告を踏襲すること。 例として、資料閲覧時に以下の内容を確認すること。 1.システム稼働状況 2.個別障害発生状況 3.セキュリティ管理実績 ・パッチの状況 ・ウイルス検知 4.運用状況 ・受付窓口からの作業依頼実績 ・申請対応業務実績 5.変更管理 6.運用改善案 7.作業予定、実績 8.業務システム 9.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。

【別紙1-5】保守・運用要件詳細

(ウ) 月次報告
① 現行の報告を踏襲すること。 例として、資料閲覧時に以下の内容を確認すること。 ・サービス稼動実績 ・システム稼動実績 ・SLA管理（サービス、回線、運用業務、セキュリティ管理） ・受付窓口からの作業依頼実績 ・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 ・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。
ウ 運用体制
(ア) 体制
① 受託者は、保守・運用における体制図を提案すること。 また、提案した体制図については、受注後、各種計画書等に明記した上で、主管課と調整・協議の上で承認を得ること。
② 設計・開発工程における知見に基づき、適切な保守・運用を遂行するために、設計・開発工程の経験を有する要員を主要なポストに配置すること。
③ 情報セキュリティに関係する体制は、保守及び運用の体制とは独立した複数名の要員で構成すること。
④ 本調達に係る「【本紙】総務省LANシステムの更新整備及び保守・運用業務の請負調達仕様書」「【別紙1】要件定義書」を参照し、保守・運用に係る適切な要員数の体制を構築すること。
⑤ 情報セキュリティインシデント等の緊急事態が発生した際に、迅速に行動を実施できるよう指揮命令系統を明確にすること。
⑥ 本調達の履行に当たり、作業体制には、原則として契約期間を通して変更することなく、作業体制を組むこと。 ただし、主管課の了承を得た場合は、この限りではない。 また、本調達を遂行する上で適切なスキルを有する要員を十分な人数、配置すること。
⑦ 提案した体制図については、受注後、各種計画書等に明記した上で、主管課との調整・協議の上で承認を受けること。

【別紙1-5】保守・運用要件詳細

(イ) 運用要員
① 「【別紙1-1】機能要件詳細」に基づき提供されるサービス全般に係る運用支援を担当する要員を配置すること。
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 運用要員が直接ユーザへサービス提供する主な作業内容と作業量（目安）を以下に示す。 ・申請対応　20件～40件/日（受付窓口からの作業依頼） ・LAN端末キッティング、故障対応 故障対応　2台/日・平均（約40台/月） 新規配備　3台/日・平均（約90台/月） ・iPadキッティング　280台/週（ペーパーレス会議の貸し出し申請、準備） ・Windowswタブレットパッチ適用　10台/月（VDI接続専用決裁端末） ・LAN複合機利用者カードの新規発行　20枚/月（繁忙期で150枚/月）
(ウ) 運用責任者
① 運用業務全体を管理する要員を配置すること。
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。
(エ) 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。
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。

【別紙1-5】保守・運用要件詳細

(オ) サービス保守要員
① サービス保守業務を担当する要員を配置し、要員の中からリーダーを選出すること。
② サービス保守要員の中から、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要員を選出すること。
③ サービス保守要員の中から、総務省LANのファシリティに関して助言を行える要員を選出すること。
④ 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。
⑤ サービス保守要員の主な作業内容と作業量（目安）を以下に示す。 ・パッチ適用 LAN端末7,000台に対し、3回/月配信 サーバ機器に対し、1回/月 アプライアンス機器に対し、1回/3ヶ月 ・セキュリティインシデントの発生を確認　50件/日 ・総務省LANの各サービスのイベント確認　100件/日 ・受付窓口からの問い合わせ内容に関するユーザへの確認　5件/日 ・ハードウェア障害等の機器交換　2件/月 ・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確認　3件/月 ・障害発生対応（機器やソフトウェアに障害があった場合、障害箇所の特定・原因調査・復旧作業の切り分けを実施）　3件/月
(カ) 総務省LAN情報セキュリティ要員
① 総務省LAN情報セキュリティチームは、適切な人数の常駐要員を配置し、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。
② 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、セキュリティ関連サービス等のセキュリティ対策について、総務省情報セキュリティポリシーとの適合状況のレビューを実施すること。また、運用期間中に情報セキュリティ対策を変更・追加する場合やシステム構成を変更する場合には、レビューを実施し適合性を把握すること。
③ 上級セキュリティエンジニアは、年次計画等で設定した適切なタイミングで総務省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その対策の検討及び対策案について主管課と最高情報セキュリティアドバイザへ提示すること。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、運用開始時においても残留リスクを最高情報セキュリティアドバイザ及び主管課のサイバーセキュリティ対策担当者等へ主管課を通じ提示すること。
④ 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、最高情報セキュリティアドバイザ及び主管課のサイバーセキュリティ対策担当者等、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。
⑤ 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システム等へ実装させる方法について最高情報セキュリティアドバイザ及び主管課のサイバーセキュリティ対策担当者等へ主管課を通じ提示すること。
⑥ 上級セキュリティエンジニアは、運用期間中、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、対応する分析手法及びSIEMシステム等への実装方法を検討し、最高情報セキュリティアドバイザ及び主管課のサイバーセキュリティ対策担当者等へ主管課を通じ提示すること。 また、実装支援を行うこと。

【別紙1-5】保守・運用要件詳細

⑦ 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サービス保守要員に依頼すること。
⑧ 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し、以下に示す者をログ分析要員に含めること。 ・「【別紙1-1】機能要件詳細」における「第3 サービス基盤」の「認証サービス」や「第4 ネットワーク基盤」の「8 ネットワークサービス」、「第5 セキュリティサービス」の「5 侵入検知防御サービス」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。
⑨ 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。
⑩ 総務省LAN情報セキュリティチームは、サービス保守要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。
⑪ 総務省LAN情報セキュリティチームは、サービス保守要員と連携し、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。
⑫ 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発見した不審な通信ログや操作ログ等を基に、マルウェア感染の疑いがあるファイル（検体）の特定（ファイル名及び格納場所）を行うこと。また、当該検体について、「【別紙1-4】情報セキュリティ要件詳細」の「第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。
⑬ 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、（サービス保守要員に対する）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。
⑭ 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。
⑮ 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。
⑯ 上級セキュリティエンジニアは、月次で主管課及び総務省情報セキュリティ班(サイバーセキュリティ対策担当、最高情報セキュリティアドバイザ等)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。
⑰ 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。
⑱ 上級セキュリティエンジニアは、総務省の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1-5】保守・運用要件詳細

(キ) 教育
① 受託者は、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、新しく加わった運用要員に対して総務省LAN及び本業務に関する教育を受けさせること。
エ 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) 運用要員
① 運用支援サービス業務は、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 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 法定停電時における時間外にも対応すること。
オ 外部監視室
(ア) 監視要件
① 本省のサービス保守対応時間外における総務省LANの監視を行うために、外部監視室より監視を行うこと。
② 本省が被災しDRが発動された場合、DRサイトで業務継続を実施するため、外部監視室はDRサイトの監視を行うこと。
③ 外部監視室が被災し使用できない場合は、受託者によって速やかに現状復旧の対応を行うこと。

【別紙1-5】保守・運用要件詳細

カ ログ監視室
(ア) 監視要件
① 定常的な分析監視を行うこと。
② 政府の情報セキュリティ方針や施策、総務省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。
③ 総務省LANの構成や状態を詳細に把握し、主管課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。
④ 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、異常の検知を行うこと。
⑤ 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。
⑥ 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。
⑦ 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。
⑧ 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。
⑨ 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。
⑩ 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。
⑪ 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。
⑫ 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。
2 サービスストラテジ
(1) 事業関係管理
ア 概要
主管課及びユーザと良好な関係を築き、利用者満足度の高いサービスを提供する。
イ 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。 ・ユーザに向けた回答の内容又は手順に対する説明の分かりやすさ、その結果の正確性 ・ユーザとの直接対応の際における担当者の対応（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。

【別紙1-5】保守・運用要件詳細

3 サービスデザイン
(1) デザイン・コーディネーション
ア 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
ア 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受付窓口と連携し公開する。
イ 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。
(3) サービスレベル管理
ア 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。
イ 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、「【別紙4】現行総務省LANにおけるサービスレベル一覧」を参照し、現行の目標値を下回らないよう提案すること。
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か月ごとに受託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、受託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、仕様書に基づき受託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。
⑧ サービスレベル目標値は、本省とDRサイトの両方をそれぞれで設定すること。なお、DRサイトの待機系機器等については、DR発動時等における切替開始後から本省への切戻し完了までをSLAの対象とし、受託者より提案すること。

【別紙1-5】保守・運用要件詳細

ウ 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。
例として、資料閲覧時に以下の内容（現行の報告）を確認すること。
・大規模人事異動対応
・セキュリティ監査対応
・テレワーク・デイズ対応
・法定停電（中央合同庁舎第2号館）
・防災訓練
・システムで利用する各種カレンダーの更新
・各種管理台帳の突合
・LAN端末導入ソフトウェア調査
・長期ログオン端末調査
・未使用LAN端末調査
・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、速やかに主管課と協議し、承認を得ること。

(4) キャパシティ管理

ア 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。

イ 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。

【別紙1-5】保守・運用要件詳細

(イ) リソースキャパシティ管理（RCM）

① 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

ア 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。

イ ディザスタリカバリ管理

① 現行総務省LANでは「総務省LAN運用継続計画」を策定している。受託者は、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1回以上見直し等を行い、主管課の承認を得ること。

② DR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際の非常時体制、非常時連絡網・連絡手段、指示命令系統等を主管課と調整し、総務省LAN運用継続計画に明記すること。

⑤ 1年に1回以上、DR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DRサイトへの切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。

ウ 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。

(6) 可用性管理

ア 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。

イ 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。

ウ サーバ・アプライアンス・ネットワーク

(ア) 稼動監視

① 運用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。

(イ) 停電対応

① 計画停電時において、システムを停止させる必要がある場合には、事前に電源管理サービス等を活用し、停止させること。

【別紙1-5】保守・運用要件詳細

(ウ) 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。
エ 共通
(ア) 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
ア 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。 「【機2】調達等における情報セキュリティ対策手順書」に従い、総務省LANの情報セキュリティ対策を実施する。
イ 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 サービス保守要員は総務省LAN情報セキュリティチームと連携し、SIEMでのログ解析や監視状況の報告、セキュリティパッチ等の対応を行うこと。
(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を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。
(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。 なお、回収した端末は完全にセキュリティの脅威が払拭されない限り、基本的に再利用はしない。 そのため、予備機が不足する可能性がある場合には、主管課と協議の上、適切な対応を行うこと。
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。

【別紙1-5】保守・運用要件詳細

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。
⑦ タブレット型端末及び証明書をインストールした私物端末の盗難、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。
⑧ LAN端末、タブレット型端末、証明書をインストールした私物端末の盗難又は紛失した際には、発覚してから3時間以内にセキュリティインシデントとして運用管理責任者へ報告すること。 報告を受けた運用管理責任者は、速やかに主管課へ報告すること。 セキュリティインシデントに対する緊急受付対応は、24時間365日で行えるよう準備すること。
(エ) セキュリティ管理
① LAN端末、タブレット型端末に対し、定期的に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。
② 端末にインストールできるソフトウェアを一元管理すること。 管理の対象は、主管課と調整し、「総務省LANとして保守の管理対象にする」と決定したソフトウェアとする。
③ 申請管理サービスにより認可されたソフトウェアは、総務省LANで利用できるソフトウェアとしてユーザに提供できること。 なお、認可されたソフトウェアの事前検証やバージョン管理は、主管課と受託者で協議の上、決定すること。
④ 総務省LANのサービス保守対象と認められないソフトウェアの場合は、申請者がバージョン管理や脆弱性等の維持管理を行うこととする。 なお、格納場所については受託者が管理を行うこと。
⑤ 資源管理ツール等で対象とするソフトウェアの名称とバージョン、管理者（申請者）を部局ごとに出力し、各部局のLAN運営担当者に適切な周期で通知すること。
(オ) 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。
(カ) 外付けUSBデバイス
① デバイス制御で使用を認められた外付けUSBデバイス以外は利用不可とすること。
(キ)総務省情報セキュリティ対策
a セキュリティ監視
① 受託者は、不正侵入やサービス不能攻撃等を監視するため、以下を遵守すること。 ・不正侵入を受けるおそれのあるサーバ装置、端末、通信回線装置又は通信回線から監視対象を特定し、監視すること。 ・サービス不能攻撃を受けるおそれのあるサーバ装置、端末、通信回線装置又は通信回線から監視対象を特定し、監視すること。 ・インターネットに接続している通信回線を提供している事業者とサービス不能攻撃発生時の対処手順や連絡体制を整備すること。 ・監視ログは取得後3年間以上保管すること。保管期間経過後は、速やかに消去すること。
b 不正プログラム対策
① 受託者は、次期総務省LANの保守・運用において、当該情報システムに導入されているアンチウイルスソフトウェアを最新の状態に維持するとともに、アンチウイルスソフトウェアを使用した不正プログラムの自動的な検査及び週一回の全ファイル検査を実施すること。

【別紙1-5】保守・運用要件詳細

c 脆弱性対策

① 受託者は、次期総務省LANの保守・運用において、対象機器及びソフトウェアについて、公表される脆弱性情報を常時把握すること。脆弱性情報が公表された場合は、脆弱性の内容の分析及び推奨されている対処の検証を行うこと。
・把握した脆弱性情報について、対処の要否、可否につき主管課と協議し、決定すること。決定した対処又は代替措置を実施すること。
・把握した脆弱性情報について、対処の要否、可否を判断した際に、対処したものに関して対処方法、対処しなかったものに関してその理由、代替措置及び影響を主管課に報告すること。

d 情報セキュリティインシデント対応

① 受託者は、次期総務省LANの保守・運用において、情報セキュリティインシデント（以下、機密性、完全性、可用性が侵害される事象を指す。）の発生を認知した場合には、直ちに、主管課に、口頭にてその旨第一報を入れること。主管課への第一報は、情報セキュリティインシデントの発生を認知してから遅くとも1時間以内に行われるように留意して行うこと。
当該第一報が行われた後、発生した日時、場所、発生した事由、関係する受託者の作業者を明らかにし、平日の8時から20時の間は1時間以内に、それ以外の時間帯は3時間以内に、または主管課からの求めに応じて主管課に報告すること。

e 作業の記録

① 受託者は、不正な行為及び意図しない情報システムへのアクセス等の事象が発生した際に追跡できるように、情報システムの保守・運用に係る作業についての記録を管理すること。

f データ保護

① 受託者は、情報システムで取扱うデータを保護するため、以下を遵守すること。
・暗号化が必要なデータをネットワーク上にて送受信する場合、盗聴による情報漏えいを防止するため、TLS（SSL）、IPsec等により通信を暗号化すること。また、主体認証情報を通信する場合には、その内容も暗号化を行うこと。
・機密性を確保するため、情報システムに保存したデータへのアクセスは識別コード及び主体認証情報等により制限し、当該データへのアクセスが必要と認められるものに限定すること。また、付与するアクセス権は必要最小限に留めること。
・完全性を確保するため、情報システムに保存したデータのバックアップを取得すること。
・職務上不要となったデータは、速やかに消去すること。またこのうち、電磁的記録媒体に保存されたデータは、当該記録媒体内にデータが残留した状態とならないよう、データ抹消ソフトウェアによるファイルの抹消、消磁装置によるデータの抹消、当該記録媒体の物理的破壊等の方法により抹消すること。なお、データ抹消ソフトウェアによりファイルを抹消する場合は、以下のいずれかの方式を用いること。

書込み方式　書込み最低回数
・ゼロ書込み方式（ゼロ値で書込み）3
・乱数書込み方式（乱数値で書込み）2
・乱数+ゼロ書込み方式（乱数値で書込み後、ゼロ値で書込み）2
・米国国家安全保障局（NSA）方式 （方式の定めによる）
・米国国防省（DoD5220.22-M）方式 （方式の定めによる）
・米国陸軍方式 （方式の定めによる）
・米国海軍方式 （方式の定めによる）
・米国空軍方式 （方式の定めによる）
・北大西洋条約機構方式 （方式の定めによる）
・米国コンピュータセキュリティセンター方式 （方式の定めによる）
・グートマン（Gutmann）方式 （方式の定めによる）

【別紙1-5】保守・運用要件詳細

g 物理対策

① 総務省は、情報システムを物理的に保護するため、以下の対策を実施している。
・生体認証デバイスにて、LAN管理室へ入室できる者を制限。
・LAN管理室とサーバ室の物理的な隔離。
・LAN管理室とサーバ室には、監視カメラと集音装置が設置され、主管課が監視。
これらの物理対策を踏まえ、受託者は常時入室が許可されていない者への入室については、事前に入室申請を受領するとともに、入退室の際には記録簿へ必要事項を記入させ、申請と一致していることを確認すること。

h 構成情報の管理

① 受託者は、情報セキュリティインシデント発生時の対応を適切に実施するため、以下を遵守すること。
・電子計算機及び通信回線装置に係る構成情報として、以下の文書を整備すること。また、構成情報は適宜確認し、許可なく変更されていないことを確認すること。
－情報システムを構成する電子計算機の管理簿
－情報システムを構成する通信回線装置の管理簿
－情報システム構成図
－通信回線構成図
－情報システムを構成する電子計算機及び通信回線装置で使用するソフトウェアの名称及びバージョン
・情報システムの可用性を高めるため、情報セキュリティインシデント検知時の対応フローや対応手順等を整備すること。
・総務省において事業継続計画（BCP）が発動した場合、当該計画の遂行を支援するため、主管課の指示事項に対応すること

I サービスレベルの保障

① 本業務の実施に当たっては、当省と受託者との間で、SLA（Service Level Agreement：サービスレベル合意書）を締結すること。サービスレベル評価項目と要求水準については、当仕様書に記載している要件を基本として、締結前に、当省と受託者との協議により決定するが、協議の前提として「サービスレベル評価項目と要求水準」「サービスレベル評価方法」及び「未達成時のサービス改善計画」について具体的に提案すること。
なお、当省にて現在盛り込むことを想定している要件の一部は以下のとおりであり、これらも踏まえて提案すること。
・脆弱性対策に関して、その公表から対応策の決定及び実施までの期間の目標
・当該情報システムの稼働率等、可用性に関する目標

j 監査対応

① 受託者は、情報システムに対する監査を適切に実施するため、以下を遵守すること。
・ネットワーク、Webサーバ、Webアプリケーション等の脆弱性を評価するための監査（脆弱性監査）について、主管課から協力要請があった場合、これに応じること。
・総務省情報セキュリティポリシーへの情報システムの適合状況を評価するための監査（運用準拠性監査）について、主管課から協力要請があった場合、これに応じること。
・その他、主管課から情報システムに関する監査について協力要請があった場合、これに応じること。

k 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。

(8) サプライヤ管理

ア 概要

サプライヤが契約上の義務を果たすよう管理する。

イ 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1-5】保守・運用要件詳細

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
ア 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
ア 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。
イ 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。調整結果に基づき、総務省LAN機器への設定が必要な場合は実施すること。
⑨ 業務システムを政府共通プラットフォームに移行する際、主管課の調整業務の支援を行い、政府共通プラットフォーム関係者及び、業務システム開発事業者と必要な調整を行うこと。調整結果に基づき、総務省LAN機器への設定が必要な場合は実施すること。
(3) リリース管理及び展開管理
ア 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。

【別紙1-5】保守・運用要件詳細

イ 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（変更要求どお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 受付窓口と連携し、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へ掲載し、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、ユーザや受付窓口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。
(4) サービス資産管理及び構成管理
ア 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かつ一元的に管理する。
イ 運用要件
① 総務省LANを構成する要素（サービス提供機器、LAN端末のハードウェア、タブレット型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。

【別紙1-5】保守・運用要件詳細

(ア) 要員管理
① 要員稼働計画を立案し、保守・運用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
a LAN端末管理（本省）
① 運用要員は、受付窓口からのユーザ申請に基づき必要な設定を行い、ユーザに引き渡すこと。
b LAN端末管理（本省以外）
① 運用要員は、受付窓口からの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。
c LAN端末
① 運用要員は、以下の必要なる資産管理、構成管理を適切に行うこと。 ・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
d タブレット型端末（ペーパーレス会議用、Windowsタブレット）
① 運用要員は、受付窓口からのユーザ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
(5) ナレッジ管理
ア 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。

【別紙1-5】保守・運用要件詳細

イ 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 上記①～③の情報は、必要に応じて主管課及び受付窓口と情報共有を行うこと。
⑤ 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受付窓口と連携し、ポータルサイトへ掲示しユーザが参照できるようにすること。
⑥ 受付窓口からの作業依頼より、ポータルサイトのコンテンツの情報更新を行うこと。 なお、主管課はコンテンツ情報の更新を依頼する際には、受付窓口へ作業依頼申請を行うこと。
⑦ 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。
⑧ 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。
⑨ 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。
5 サービスオペレーション
(1) イベント管理
ア 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。
イ 運用要件
① システム監視サービスを用いて、総務省LANの各サービスのイベントを検知、確認すること。
② 本省サーバ室及びDRサイトに設置した管理対象機器の稼働状況及び障害発生状況を日次で目視確認し、イベントを検知、確認すること。
③ ユーザから受付窓口への問い合わせを通じて調査依頼を受け、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 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、受付窓口を通じて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。

【別紙1-5】保守・運用要件詳細

ウ 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（外部監視室等）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。
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時とすること。
(2) インシデント管理
ア 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。
イ 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 運用要員は、受付窓口よりインシデント発生連絡を受けたら、インシデント管理システムに登録すること。 インシデント管理システムに登録した情報は、Excelなどで可読性に考慮した出力を可能とすること。
④ 対応時間外において、ユーザから直接時間外連絡先（公開している時間外連絡先）へ問い合わせをしてきた場合は、応対者は運用要員と連携をし保守・運用関係者へエスカレーションすること。 また運用要員は、インシデント発生状況を把握し、インシデント管理システムに登録すること。
ウ 障害対応
(ア) LAN端末・タブレット型端末
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 LAN端末やプリンタなどの調達範囲外のハードウェア障害（ファームウェア、BIOSなども含む）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。

【別紙1-5】保守・運用要件詳細

(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 受託者は障害の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、原因の切り分け及び復旧等の作業を実施すること。 一次切り分けの結果、運用の範囲外における機器やソフトウェアが原因である場合は、その所管と連携し障害復旧の支援をすること。
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り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、外部監視室及びDR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
ア 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、ユーザからの要求（受付窓口への申請に基づくもの等）を処理する。
イ 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。
(4) 問題管理
ア 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。
イ 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、受付窓口、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。

【別紙1-5】保守・運用要件詳細

(5) アクセス管理
ア 概要
ユーザにサービスを利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。
イ 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、安全に、かつ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、運用管理責任者が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。
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。

【別紙1-5】保守・運用要件詳細

第2 保守
1 ソフトウェア保守
(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、万全な体制を確保し、運用担当者及び運用管理・受付窓口請負事業者に協力すること。 なお、連絡体制は、具体的な資料を提出すること。
④ 総務省LANの利用に影響のある保守作業については、受付窓口へ事前に連携しユーザに向けた情報を提供すること。
⑤ 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。
⑥ 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。
⑦ 令和7年4月から原則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。 なお、運用管理・受付窓口請負事業者との作業連携も考慮すること。
(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、サービス保守要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、受付窓口からの依頼については、受付窓口へ作業報告を行うこと。 自検知においては、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報告し、受付窓口には情報連携を行うこと。

【別紙1-5】保守・運用要件詳細

2 ハードウェア保守	
(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、運用担当者及び運用管理・受付窓口請負事業者に協力すること。 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DR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 総務省LANの利用に影響のある保守作業については、受付窓口へ事前に連携しユーザに向けた情報を提供すること。
	⑥ 本省及びDR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。
	⑦ 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。
	⑧ 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。
	⑨ 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。
	⑩ 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。
	⑪ 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。
	⑫ 令和7年4月から原則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、運用管理・受付窓口請負事業者との作業連携も考慮すること。

【別紙1-5】保守・運用要件詳細

(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 潜在的な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 ハードウェア障害対応手順書（マニュアル）を作成し、主管課に承認を得ること。 手順書には、障害の切り分けにおいて、調達機器範囲外での要因も考慮し、エスカレーション等の手順を示しておくこと。
② 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。
③ 障害対応終了後、受付窓口からの依頼については、受付窓口へ作業報告を行うこと。 自検知においては、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報告し、受付窓口には情報連携を行うこと。
④ ハードウェア交換が必要となる場合は、ハードウェア障害対応手順書に基づき、修理・交換などの作業を行うこと。
⑤ 保守期間は、本稼働から原則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。

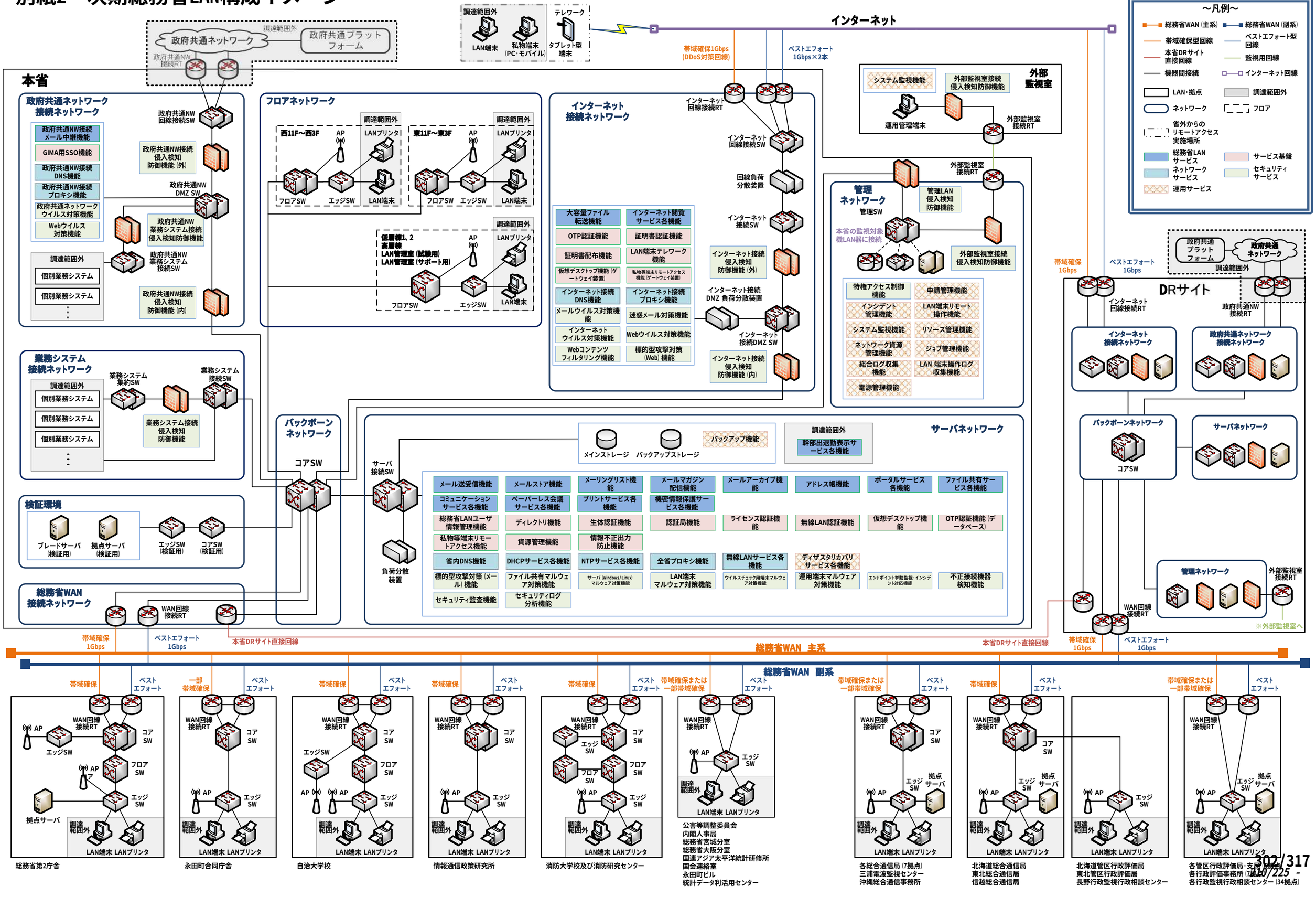
【別紙1-6】本省・DRサイト稼働サービス一覧

#	提供サービス名	設置場所		備考
		本省	DRサイト	
1	総務省LANサービス			
2	メールサービス	○	○	
3	ポータルサイトサービス	○	○	
3	幹部出退勤表示サービス	○	×	現行運用中に別途調達した機器・ソフトウェアを継続利用する
4	ファイル共有サービス	○	○	
5	大容量ファイル転送サービス	○	○	
6	コミュニケーションサービス	○	○	
7	ペーパーレス会議サービス	○	×	
8	プリントサービス	○	○	
9	インターネット閲覧サービス	○	×	
10	機密情報保護サービス	○	○	
11	サービス基盤			
12	認証サービス	○	○	
13	テレワークサービス	○	○	
14	私物等端末リモートアクセスサービス	○	○	
15	デバイス管理サービス	○	×	
16	資源管理サービス	○	×	
17	情報不正出力防止サービス	○	○	
18	ネットワーク基盤			
19	本省LAN	○	－	
20	DRサイトLAN	－	○	
21	拠点LAN	－	－	拠点のネットワーク基盤であるため除外
22	総務省WAN	○	○	

【別紙1-6】本省・DRサイト稼働サービス一覧

#	提供サービス名		設置場所		備考
			本省	DRサイト	
23		インターネット接続ネットワーク	○	○	
24		外部監視室接続ネットワーク	○	○	
25		ネットワークサービス	○	○	
26		無線LANサービス	○	○	
27	セキュリティサービス				
28		マルウェア対策（メール）サービス	○	○	
29		マルウェア対策（インターネット・Web)サービス	○	○	
30		マルウェア対策（エンドポイント・ファイル共有）サービス	○	○	
31		侵入検知防御サービス	○	○	
32		不正接続機器検知サービス	○	○	
33		特権アクセス制御サービス	○	○	
34		セキュリティ管理サービス	○	×	
35		セキュリティログ分析サービス	○	×	
36	運用サービス				
38		申請管理サービス	○	○	
39		運用支援サービス	○	○	
40		システム監視サービス	○	○	
41		ログ管理サービス	○	○	
42		バックアップサービス	○	○	
43		電源管理サービス	○	×	
44		ディザスタリカバリサービス	―	―	機器設置はないため除外
45	その他機器基盤				
46		保守・検証環境	○	×	原則、DRサイトへは設置しない
47		運用業務環境	○	○	

別紙2　次期総務省LAN構成イメージ



【別紙3】保有ライセンス・ソフトウェア一覧

1　総務省保有ソフトウェアライセンス等一覧

1-1. 以下のライセンスは現行総務省LANで利用中（令和2年4月時点）であり、次期総務省LANでも継続利用及び継続契約が可能である。

区分	ソフトウェア名称	型番	数量	期間	備考
CAL	CoreCALBridge0365FromSA ALNG SubsVL MVL Pltfrm PerUsr	AAA-12417	6,100	平成30年10月から 令和4年9月末まで	
OS	WinE3perUserFromSAALNG SubsVL MVL Pltfrm PerUsr	AAA-10777	6,100	平成30年10月から 令和4年9月末まで	
オフィスソフトウェア	O365E3FromSA ShrdSvr ALNG SubsVL MVLGov GovOnly PerUsr	AAA-10757	6,000	平成30年10月から 令和4年9月末まで	
	O365E5FromSA ShrdSvr ALNG SubsVL MVL GovGovOnly PerUsr	SZ7-00001	100	平成30年10月から 令和4年9月末まで	
	JUST Government4	E241790	6,200	令和元年10月から 令和5年9月末まで	
その他ソフトウェア	Adobe Acrobat Pro	-	6,200	令和元年10月から 令和5年9月末まで	
その他ソフトウェア	CACHATTO 5,000ユーザー帯 初年度パック（10ユーザー毎）	CAV1204500S	500	平成29年4月から 令和4年3月末まで	初年度分、10ユーザパック×500式
その他ソフトウェア	CACHATTO 5,000ユーザー帯 継続パック（10ユーザー毎年額）	CAV1204500N	2,000		次年度以降4年分
その他ソフトウェア	スタンバイ機ライセンス（CACHATTOサーバ毎）	CMS1204999S	2	平成29年4月から 令和4年3月末まで	CACHATTO
その他ソフトウェア	一太郎オプション	CIC170900SA	3	平成31年4月から 令和4年3月末まで	CACHATTO
セキュリティソフトウェア	※資料閲覧時に確認すること	-	-	-	

1-2. 以下のライセンスは今後調達予定（令和2年4月時点）であり、調達された場合、次期総務省LANでも継続利用及び継続契約が可能である。

区分	ソフトウェア名称	型番	数量	期間	備考
CAL	CoreCALBridge0365 ALNG SubsVL MVL PerUsr	AAA-12414	100	令和2年10月から 令和4年9月末まで	
OS	WinE3 ALNG SubsVL MVL PerUsr	AAA-10787	100	令和2年10月から 令和4年9月末まで	
オフィスソフトウェア	O365E3 ShrdSvr ALNG SubsVL MVL GovOnly PerUsr	AAA-10841	100	令和2年10月から 令和4年9月末まで	
幹部出退勤表示用ソフトウェア	スマートサインN@vi	-	1	令和2年12月から 令和7年3月末まで	

1-3. 以下の機器は今後調達予定（令和2年4月時点）であり、調達された場合、次期総務省LANでも継続利用及び継続契約が可能である。

区分	機器名称	型番	数量	期間	備考
幹部用表示専用装置	ボックスPC	BX-U200-W19M01M03	39	-	令和2年12月納品予定
幹部用表示専用ディスプレイ	ディスプレイ	未定	40	-	令和2年12月納品予定

【別紙4】現行総務省LANにおけるサービスレベル一覧

サービスレベル目標				計算方法	
分類	評価項目	目標値	内容	式	補足
サービス	稼働率	99.90%以上	以下のサービスの稼働率 ・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 ・テレワークサービス ・プリントサービス（本省） ・認証サービス ・仮想ブラウザサービス	■DRサービス以外 稼働率（%） =(1- b÷c)×100 ■DRサービス 稼働率（%） =(1- f÷g)×100	■DRサービス以外 ・サービス停止による影響量 a ：サービス停止時間×影響を受けたユーザ数 b ：上記aをサービスごとに、サービス停止の都度算出し、その1ヶ月分の合計 ・稼働予定量　c = d + e d ：本省分　= 24時間×1ヶ月の日数×ユーザ数 e ：拠点分　= 8時間×1ヶ月の開庁日の日数×ユーザ数 ※法定点検による停電時間、サービスの計画停止時間は除く。 ■DRサービス ・サービス停止時間 f ：サービス停止時間の1ヶ月分の合計 ・1ヶ月の稼働予定時間 g ：　24時間×1ヶ月の日数 ※法定点検による停電時間、サービスの計画停止時間は除く。
		99.00%以上	以下のサービスの稼働率 ・ポータルサイトサービス（幹部出退勤） ・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 ・ペーパーレス会議サービス ・プリントサービス（拠点） ・情報不正出力防止サービス ・機密情報保護サービス ・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 ・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 ・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 ・不正接続機器検知サービス		
	サービス停止時の 緊急連絡	99.90%以上	LAN運用業者がサービスの停止を検知してから5分以内(開庁日)、30分以内(閉庁日)に主管課へ報告する。	実施率（%） =(a÷b)×100	a：サービス停止検知から5分以内に連絡した件数 b：サービス停止を検知した総数
回線	稼働率	99.99%以上	総務省WANの稼働率。	稼働率（%） =(1-a÷b)×100	a：1ヶ月の障害復旧時間 b：1ヶ月の稼働予定時間（24時間×1ヶ月の日数） ※法定点検による停電時間、サービスの計画停止時間は除きます。
	回線障害時の 緊急連絡	99.90%以上	総務省WAN又はインターネット回線の回線障害をLAN運用業者が検知してから10分以内に主管課へ報告する。	実施率（%） =(a÷b)×100	a：回線障害検知から10分以内に連絡した件数 b：回線障害を検知した総数

【別紙4】現行総務省LANにおけるサービスレベル一覧

サービスレベル目標				計算方法	
分類	評価項目	目標値	内容	式	補足
	網内遅延時間	35ミリ秒以内	総務省WAN のIPパケットの往復転送時間の月間平均値。	網内遅延時間	IPパケットの往復転送時間の全測定点の月間平均値。
	障害復旧時間	1時間以内	総務省WANの回線障害発生から復旧までの時間。	障害復旧時間 =b-a	a：回線障害発生時刻 b：障害復旧時刻
運用業務	申請依頼業務	99.99%以上	LAN運用業者が申請書を受領し、主管課の作業指示後、全作業を翌々開庁日の執務時間開始までに完了させた実施率。	サービス実施率 （%） =(a÷b)×100	ａ：所定の期日までに完了した件数 ｂ：申請書受領件数
	ヘルプデスク回答	95.00%以上	翌開庁日内までに問い合わせ内容の把握、状況の確認、対応の方針等を主管課又はユーザに対して報告した実施率。	ヘルプデスク回答率 （%） =(a÷b)×100	ａ：1開庁日（翌開庁日）以内に回答した件数 ｂ：問い合わせの総数
セキュリティ管理	セキュリティインシデントの検知時間 （日勤帯）	検知してから30分以内に報告	製品によるパターンマッチングでインシデントを検知し、LAN端末隔離等の対処を自動で実施した場合の主管課へ報告するまでの時間。	検知時間 =b-a	a：発生時刻 b：検知時刻
	セキュリティインシデントの検知時間 （夜間帯）	翌日9時30分迄に報告		検知時間 =b-a	a：発生時刻 b：検知時刻
	セキュリティインシデントの報告時間	検知してから30分以内	SIEM情報に基づき上級セキュリティエンジニアが分析・判断によりインシデントを検知し、主管課へ報告するまでの時間。	報告時間 =b-a	a：検知時刻 b：報告時刻
	セキュリティインシデントへの対応時間	検知してから3時間以内	セキュリティインシデントの発生の報告後からネットワーク遮断等の回避策を実施完了するまでの時間。	対応時間 =b-a	a：検知時刻 b：対応完了時刻 ※未知のマルウェアに対する回避策検討、報告に要した時間は除外。 ※セキュリティベンダーへのファイル(検体)提供からパターンファイル提供までの時間は除外。

【別紙5】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（統計局、政策統括官（統計基準担当）、政策統括官（恩給担当））	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10階
5	内閣人事局	100-8914	東京都千代田区永田町1-6-1 中央合同庁舎第8号館5階
6	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委員会、公共サービス改革推進室）	100-0014	東京都千代田区永田町1-11-39
7	総務省宮城分室	-	宮城県仙台市内
8	総務省大阪分室	-	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	国連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 日本貿易振興機構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	永田町ビル（電気通信紛争処理委員会・政治資金適正化委員会）	100-0014	東京都千代田区永田町2-17-3 住友不動産永田町ビル4階
15	統計データ利活用センター	640-8203	和歌山県和歌山市東蔵前丁3-17 南海和歌山市駅ビル5階
16	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
17	函館行政監視行政相談センター	040-0032	北海道函館市新川町25-18 函館地方合同庁舎6階
18	旭川行政監視行政相談センター	078-8501	北海道旭川市宮前1条3丁目3番15号 旭川合同庁舎西館5階
19	釧路行政監視行政相談センター	085-0022	北海道釧路市南浜町5-9 釧路港湾合同庁舎3階
20	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10階、11階
21	青森行政監視行政相談センター	030-0801	青森県青森市新町2-4-25 青森合同庁舎4階
22	岩手行政監視行政相談センター	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
23	秋田行政監視行政相談センター	010-0951	秋田県秋田市山王7-1-3 秋田合同庁舎4階
24	山形行政監視行政相談センター	990-0041	山形県山形市緑町1-5-48 山形地方合同庁舎3階
25	福島行政監視行政相談センター	960-8021	福島県福島市霞町1-46 福島合同庁舎3階
26	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
27	茨城行政監視行政相談センター	310-0061	茨城県水戸市北見町1-11 水戸地方合同庁舎2階
28	栃木行政監視行政相談センター	320-0043	栃木県宇都宮市桜5-1-13 宇都宮地方合同庁舎3階
29	群馬行政監視行政相談センター	371-0026	群馬県前橋市大手町2-3-1 前橋地方合同庁舎6階
30	千葉行政監視行政相談センター	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
31	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
32	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
33	新潟行政評価事務所	950-8628	新潟県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
34	山梨行政監視行政相談センター	400-0031	山梨県甲府市丸の内1-1-18 甲府合同庁舎9階
35	長野行政監視行政相談センター	380-0846	長野県長野市旭町1108 長野第1合同庁舎4階
36	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
37	富山行政監視行政相談センター	930-0856	富山県富山市牛島新町11-7 富山合同庁舎5階
38	石川行政評価事務所	920-0024	石川県金沢市西念3-4-1 金沢駅西合同庁舎4階
39	岐阜行政監視行政相談センター	500-8114	岐阜県岐阜市金竜町5-13 岐阜合同庁舎2階
40	静岡行政監視行政相談センター	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
41	三重行政監視行政相談センター	514-0033	三重県津市丸之内26-8 津合同庁舎3階
42	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
43	福井行政監視行政相談センター	910-0859	福井県福井市日之出3-14-15 福井地方合同庁舎2階
44	滋賀行政監視行政相談センター	520-0044	滋賀県大津市京町3-1-1 大津びわ湖合同庁舎7階
45	京都行政監視行政相談センター	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
46	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
47	奈良行政監視行政相談センター	630-8213	奈良県奈良市登大路町81 奈良合同庁舎4階
48	和歌山行政監視行政相談センター	640-8143	和歌山県和歌山市二番丁3 和歌山地方合同庁舎3階
49	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
50	鳥取行政監視行政相談センター	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
51	島根行政監視行政相談センター	690-0841	島根県松江市向島町134-10 松江地方合同庁舎2階
52	岡山行政監視行政相談センター	700-0984	岡山県岡山市北区桑田町1-36 岡山地方合同庁舎3階
53	山口行政監視行政相談センター	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
54	四国行政評価支局	760-0019	香川県高松市サンポート3番33 高松サンポート合同庁舎南館6階
55	徳島行政監視行政相談センター	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
56	愛媛行政監視行政相談センター	790-0808	愛媛県松山市若草町4-3 松山若草合同庁舎4階
57	高知行政監視行政相談センター	780-0870	高知県高知市本町4-3-41 高知地方合同庁舎2階
58	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
59	佐賀行政監視行政相談センター	840-0041	佐賀県佐賀市城内2-10-20 佐賀合同庁舎3階
60	長崎行政監視行政相談センター	852-8106	長崎県長崎市岩川町16-16 長崎合同庁舎5階
61	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
62	大分行政監視行政相談センター	870-0016	大分県大分市新川町2-1-36 大分合同庁舎4階
63	宮崎行政監視行政相談センター	880-0805	宮崎県宮崎市橘通東3-1-22 宮崎合同庁舎4階
64	鹿児島行政監視行政相談センター	892-0812	鹿児島県鹿児島市浜町2-5-1 鹿児島港湾合同庁舎5階
65	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
66	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12階
67	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12階～15階
68	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
69	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
70	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
71	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
72	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

【別紙5】拠点一覧

No.	拠点名	郵便番号	所在地
73	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
74	中国総合通信局	730-8795	広島県広島市中区東白島町19-36
75	四国総合通信局	790-8795	愛媛県松山市味酒町2-14-4
76	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
77	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
78	外部監視室	-	-

【別紙6】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
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、テスト、移行・展開の完了時
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。	（令和3年9月）
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。	（令和2年10月）
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。	（令和2年12月）
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。	（令和3年2月）
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。	（令和3年3月）
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。	（令和3年2月）
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。	（令和3年2月）
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。	（令和3年7月）
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。	（令和3年3月）
24	テスト	テスト実施計画書	単体・結合・総合テスト実施に当たっての体制、詳細スケジュール、テスト環境等を記載した文書。	（令和3年4月）
25		テスト仕様書	単体・結合・総合テスト実施計画に基づき、テスト方針、テスト項目、テスト方法、合否判定基準を定めた文書。	（令和3年6月）
26		テスト結果報告書	単体・結合・総合テスト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。	（令和3年9月）
27		受入テスト実施計画書	受入テスト実施に当たっての体制、詳細スケジュール、テスト環境等を記載した文書。	（令和3年7月）

【別紙6】成果物一覧

No.	分類	成果物	内容	提出時期
28		受入テスト仕様書	受入テスト実施計画に基づき、テスト方針、テスト項目、テスト方法、合否判定基準を定めた文書。	（令和3年8月）
29	移行・展開	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。	（令和3年4月）
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。	（令和3年4月）
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。	（令和3年6月）
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。	（令和3年6月）
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。	（令和3年5月）
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。	（令和3年6月）
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。	（令和3年5月）
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。	（令和3年7月）
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。	移行の完了時
38	教育訓練	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。	（令和3年6月）
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。	（令和3年6月）
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。	（令和3年9月）
41	保守・運用	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。	（令和3年9月）
42		保守・運用要領	保守・運用を行う上での指針・基準となる項目を記載した文書。	（令和3年6月）
43		保守・運用実施計画書	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。	（令和3年7月）
44		中長期保守・運用作業計画	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保守・運用作業計画。	（令和3年7月）
45		保守・運用設計書	システム保守・運用の対象や方法について記載した文書。	（令和3年7月）
46		保守・運用手順書	運用要員が保守・運用を行う上での手順や解説等を記載した文書。	（令和3年9月）
47		総務省LAN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。	（令和3年9月）
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。	令和3年10月以降、項目に応じ日次、週次、月次、年次で報告
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。	令和3年10月以降、項目に応じ日次、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。	令和3年10月以降、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。	令和3年10月以降、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。	（令和3年9月） 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。	（令和3年9月） 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。	（令和3年9月） 更新の都度

【別紙6】成果物一覧

No.	分類	成果物	内容	提出時期
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。	（令和3年9月） 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。	（令和3年9月） 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。	令和3年10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
60		情報返却等計画書	情報管理簿に記載した全ての情報の返却、消去、廃棄等の処理を行う際に、その処理について方法、日時、場所、立会人、作業責任者等の事項を網羅した文書。	情報管理簿に記載した情報の返却、消去、廃棄等の処理を行う都度に提出

（注）提出時期欄の括弧書きは予定時期を示し、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。

【別紙 7】

情報保護・管理要領

1　目的

本契約に係る作業において取り扱う各種情報について、適正な保護・管理方策について明確にすることを目的とする。

2　適用範囲

本契約に係る作業で取り扱う主管課が交付又は使用を許可した全ての情報（電子データ、印刷された情報を含む。）を対象とする。

3　本契約を受託する者が遵守すべき事項

請負者は、本契約の履行に関して、以下の項目を全て遵守すること。

(1)　作業開始前の遵守事項

請負者は以下のアからオまでの各項目に定める事項を定め、その結果を取りまとめた「情報管理計画書」を作成し、契約締結後１週間以内に主管課の承認を受けること。また、役務内容を一部再委託する場合は、カに定める事項に必要な情報を主管課に提供し、主管課の承認を受けること。

ア　情報取扱者等の指定

「適用範囲」に定める情報を取り扱う者（以下、「情報取扱者」という。）を指定すること。また、情報取扱者のうち、情報取扱者を統括する立場にある者一名を情報取扱責任者として指定すること。なお、情報取扱者及び情報取扱責任者（以下、「情報取扱者等」という。）は、守秘義務等の情報の取り扱いに関する社内教育又はこれに準ずる講習等（以下、「社内情報セキュリティ教育」という。）を受講した者とすること。

なお、「情報管理計画書」には、上記に従って指定した情報取扱者等の所属、役職、氏名及び社内情報セキュリティ教育の受講状況を明記すること。

イ　情報取扱者等への教育・周知の計画策定

情報取扱者等を対象に実施する本契約での各情報の取り扱いや漏えい防止等の教育・周知に関する計画を策定すること。

ウ　情報の取り扱いに関する計画策定

本契約の作業に係る情報の取り扱いに関し、情報の保存、運搬、複製及び破棄において実施する措置を情報セキュリティ確保の観点から定めること。また、情報の保管場所を変更する場合における取り扱いについても定めること。

上記の情報の取り扱いに関して定める措置には、以下に示す措置を含めること。

（ア） 本契約の作業に係る情報を取り扱うサーバ、PC、モバイル端末について、脅威に関する最新の情報を踏まえた不正プログラム対策及び脆弱性対策を行うこと。

（イ） 総務省が「要保護情報」に指定した情報の取り扱いに、総務省又は請負者のいずれかの管理下にない情報システム等（作業従事者の個人所有物である PC 及びモバイル端末を含む）を用いることを原則として禁止し、必要がある場合は主管課の許可を得て用いること。

（ウ） 総務省が「要保護情報」に指定した情報の保存に、総務省又は請負者のいずれかの管理下にない情報システム等又は電磁的記録媒体（作業従事者が私的に契約しているサービス及び作業従事者の個人所有物である電磁的記録媒体を含む。）を用いることを原則として禁止し、必要がある場合は主管課の許可を得て用いること。

（エ） 総務省が「要保護情報」に指定した情報を電子メールにて送信する場合には、暗号化を行うこと。

エ 作業場所の情報セキュリティ確保のための措置の決定

総務省又は総務省が指定する場所以外の作業場所において本契約に係る作業を行う場合は、情報に係るセキュリティ確保のために、作業場所の環境、作業に使用する情報システム等に講ずる措置を定めること。

上記の情報に係るセキュリティ確保のために定める措置には、以下に示す措置を含めること。

（ア） 総務省の情報システムにアクセス（一般向けに提供されているウェブページへのアクセスを除く。）する作業は、請負者の管理下にあり、部外者の立入りが制限された場所において行うこと。

（イ） 本契約の作業に係る情報を取り扱う PC、モバイル端末等について、盗難、紛失、表示画面ののぞき見等による情報漏えいを防ぐための措置を講ずること。また、それらの措置を講じていない PC、モバイル端末等を用いた作業を制限すること。

オ 情報セキュリティが侵害された又はそのおそれがある場合の対処手順等の策定

本契約に係る業務の遂行において情報セキュリティが侵害された又はそのおそれがある場合に備え、事前に連絡体制を整備し、主管課に提示すること。

本契約に係る業務の遂行において情報セキュリティが侵害された場合又はそのおそれがある場合の対処手順を定めること。対処手順には、以下に示す対処を含めること。

（ア） 作業中に、情報セキュリティが侵害された又はそのおそれがあると

判断した場合には、直ちに、主管課に、口頭にてその旨第一報を入れること。主管課への第一報は、情報セキュリティインシデントの発生を認知してから遅くとも１時間以内に行われるように留意して行うこと。

（イ） 当該第一報が行われた後、発生した日時、場所、発生した事由、関係する請負者の作業者を明らかにし、平日の 9 時から 18 時の間は 3 時間以内に、それ以外の時間帯は翌開庁日に主管課に報告すること。また、当該報告の内容を記載した書面を遅延なく主管課に提出すること。

（ウ） 主管課の指示に基づき、対応措置を実施すること。

（エ） 主管課が指定する期日までに、発生した事態の具体的内容、原因、実施した対応措置を内容とする報告書を作成の上、主管課に提出すること。

（オ） 再発を防止するための措置内容を策定し、主管課の承認を得た後、速やかにその措置を実施すること。

本契約の業務が国の安全に関する重要な情報の取り扱いを含む場合は、上記に加えて、以下に示す対処を対処手順に含めること。

（ア） 情報セキュリティの侵害による被害の程度を把握するために必要となる記録類を作成又は取得すること。これらの記録類は契約終了時まで保存すること。

（イ） 総務省の求めに応じてこれらの記録類を総務省に引き渡すこと。

なお、ここでいう「情報セキュリティが侵害された又はそのおそれがある場合」には、以下の事象を含む。

（ア） 不正プログラムへの感染（受託者におけるものを含む。）

（イ） サービス不能攻撃によるシステムの停止（受託者におけるものを含む。）

（ウ） 情報システムへの不正アクセス（受託者におけるものを含む。）

（エ） 書面又は外部電磁的記録媒体の盗難又は紛失（受託者におけるものを含む。）

（オ） 要機密情報の流出・漏えい・改ざん（受託者におけるものを含む。）

（カ） 異常処理等、予期せぬ長時間のシステム停止（受託者におけるものを含む。）

（キ） 総務省が受託者に提供した又は受託者にアクセスを認めた総務省の情報の目的外利用又は漏えい

（ク） アクセスを許可していない総務省の情報への受託者によるアクセス

（ケ） 意図しない不正な変更等が発見された場合

カ　再委託に係る情報セキュリティの確保

事前に主管課の承認を得た上で、本契約の役務内容を一部再委託する場合、請負者自体が業務を実施する場合に求められる水準と同一水準の情報セキュリティ対策を再委託先においても確保させる必要があり、再委託先における情報セキュリティの十分な確保を請負者が担保するとともに、再委託先の情報セキュリティ対策の実施状況を確認するために必要な情報を主管課に提供し、主管課の承認を受けること。

(2)　請負作業中の遵守事項

ア　「情報管理計画書」に基づく情報セキュリティ確保

「情報管理計画書」に記載した、情報取扱者等への教育・周知、情報の取り扱い及び作業場所等の情報セキュリティ確保のための措置を実施すること。

イ　「情報管理簿」の作成

主管課から貸与を受けた各種ドキュメント、電子データ類又は本契約に係る作業を実施するに当たり作成されたドキュメント、電子データについて、授受方法、保管場所、保管方法、作業場所、使用目的等を含む取扱方法を明確にするため、「情報管理簿」を作成すること。

ウ　「情報管理計画書」の変更に関する報告

本契約に基づく請負作業中に、作業開始前に提出した「情報管理計画書」の内容と異なる措置を実施する場合は、以下の手続を行うこと。

（ア）　情報取扱者等の異動を行う場合は、事前にその旨を主管課に報告し承認を得ること。また、承認された異動の内容を記録し保存すること。

（イ）　「情報管理計画書」に記載した情報取扱者等に対する教育・周知の計画を変更する場合は、当該個所を変更した「情報管理計画書」を主管課に提出し承認を得ること。

（ウ）　「情報管理計画書」に記載した情報の取り扱いに関する計画又は作業場所等の情報セキュリティ確保のための措置を変更する場合は、当該箇所を変更した「情報管理計画書」を主管課に提出し承認を得ること。

（エ）　一時的に「情報管理計画書」に記載した情報の取り扱いに関する計画又は作業場所等の情報セキュリティ確保のための措置とは異なる措置を実施する場合は、原則として事前にその旨を主管課に報告し承認を得ること。

エ　作業場所への監査の受け入れ

総務省以外の作業場所において本契約に係る作業を行っている場合

に、主管課がその施設及び設備に関し、請負者が「情報管理計画書」に記載した作業場所等の情報セキュリティ確保のため措置が実施されていることを監査する旨申し出たときは、これを受け入れること。

オ　情報セキュリティ対策の履行が不十分であった場合の対応

本契約に係る作業における情報セキュリティ対策の履行が不十分であると主管課が判断した場合、主管課と協議の上、必要な是正措置を講ずること。また、是正措置の内容を「情報管理計画書」に反映させること。

(3)　請負作業完了時の遵守事項

ア　情報返却等処理

本契約に係る作業完了時に上記(2)イで作成した「情報管理簿」に記載されている全ての情報について、返却、消去、廃棄等の処理を行うこと。

なお、その処理について方法、日時、場所、立会人、作業責任者等の事項を網羅した「情報返却等計画書」を事前に主管課に提出し、承認を得ること。

処理の終了後、その結果を記載した「情報管理簿」を主管課に提出すること。

イ　情報セキュリティ侵害の被害に関する記録類の引渡し

本契約の業務が国の安全に関する重要な情報の取り扱いを含む場合であって、業務遂行中に情報セキュリティが侵害された又はそのおそれがある事象が発生した場合、上記（１）オに基づいて取得し保存している記録類を引き渡すこと。

【別紙8】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29年4月から運用している第4期の総務省LAN。
3	次期総務省LAN	令和3年10月から運用開始を予定している第5期の総務省LAN。
4	次々期総務省LAN	令和7年4月から運用開始を予定している第6期の総務省LAN。
5	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・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。
6	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。「総務省デジタル・ガバメント中長期計画（平成30年6月22日 総務省行政情報化推進委員会決定）」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。
7	個別業務システム	総務省の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。
8	総務省共通基盤支援システム	府省共通の情報システム（一文（一元的な文書管理システム）、GIMA（職員等利用者共通認証基盤））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。
9	GIMA （職員等利用者共通認証基盤）	各府省の業務・システムを利用する際の本人確認等に必要な利用者認証情報及び利用者認証機能を一元的に管理・提供する認証基盤。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。
10	一文 （一元的な文書管理システム）	行政文書の起案・登録から廃棄・移管までのライフサイクルを電子的に管理するシステム。行政文書の保存・管理機能及び電子決裁機能を有する。
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サイバーセキュリティ・情報化推進室が各部局に配備し、業務を行うための端末。LAN端末の調達は、本調達には含まれない。ただし、次期総務省LANで動作させるための再設定等は、本調達の範囲である。
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、その他用途で利用するタブレット型端末の2種類がある。タブレット型端末は、いずれも本調達の範囲である。
16	ウイルスチェック用端末	外部から、電磁的記憶媒体に記録された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。ウイルスチェック用端末は、本調達の範囲である。
17	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・プリンタの調達は、本調達には含まれない。ただし、次期総務省LANで動作させるための再設定等は、本調達の範囲である。
18	コアスイッチ	本省LANでは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。なお、拠点LANでは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。
19	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。なお、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	エッジスイッチ	LAN端末及びLAN複合機・プリンタを集約するスイッチ。
21	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。サーバの調達及びWebサイトの管理は本調達に含まない。
22	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。
23	USBデバイス	USB接続により利用する機器全般。
24	セキュリティ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。
25	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をすることで、電子データの移動を行うためのデバイス。
26	外部拠点	総務省第2庁舎（統計局､政策統括官（統計基準担当）､政策統括官（恩給担当））、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委員会、公共サービス改革推進室）、総務省宮城分室、総務省大阪分室、自治大学校、情報通信政策研究所、国連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、永田町ビル（電気通信紛争処理委員会･政治資金適正化委員会）、統計データ利活用センターの13拠点を指す。
27	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、及び行政監視行政相談センターの62拠点を指す。
28	外部監視室	運用業務時間外等に、総務省LANをリモート監視するための場所。なお、外部監視室の借上げは本調達の範囲である。
29	DRサイト （Disaster Recovery Site）	大規模災害等の有事や障害の際に、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サイトの借上げは、本調達の範囲である。
30	本省サーバ室	総務省本省にあるサーバ室。
31	主管課	総務省大臣官房企画課サイバーセキュリティ・情報化推進室。

【別紙8】用語の定義

No.	用語	定義
32	ユーザ	総務省LANの利用者。
33	職員	総務省の職務を担当する者。
34	兼務職員	総務省の複数の職務を担当する者。
35	ユーザアカウント	ユーザに割り当てられたアカウント。
36	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。
37	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。
38	運用管理・受付窓口請負事業者	別途調達する「総務省LANシステムの運用管理及び受付窓口業務」を請け負う事業者。
39	LAN管理室	本省サーバ室と隣接する場所。ここに常駐する運用責任者、サービス保守要員、及びヘルプデスク要員の総称を指す場合もある。
40	ODB （政府情報システム管理データベース）	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、総務省行政管理局において整備及び管理し、各府省の用に供する政府情報システム管理データベース。