資料１－２

宮内庁共通基盤システムの整備・保守及び宮内庁 NWS の運用管理業務に係る民間競争入札

実施要項（案）

宮内庁

令和元年〇月

目　次

【資料一覧】

◆ 「宮内庁共通基盤システムの整備・保守及び宮内庁 NWS の運用管理業務に係る民間競争入札実施要項」
- 別紙 1「宮内庁 NWS 設置拠点・設置場所等」
- 別紙 2「従来の実施状況に関する情報の開示」
- 別紙 2 附属資料「運用管理の業務フロー」
- 別紙 3「談合等不正行為に関する特約条項」
- 別紙 4「暴力団排除に関する特約条項」
- 別紙 5「暴力団排除に関する誓約事項」
- 別紙 6「利用満足度調査」

◆ 別添 1 「宮内庁共通基盤システムの整備・保守及び宮内庁 NWS の運用管理業務に係る民間競争入札調達仕様書」
- 別紙 1「資料閲覧願い」及び「機密保持に関する誓約書」
- 別紙 2 宮内庁 NWS 設置拠点・設置場所等
- 別紙 3 各フロア配線，必要ポート数状況
- 別紙 4 本調達機器及び各事業者の役割範囲
- 別紙 5 運用・保守のフロー

◆ 別添 2 「宮内庁共通基盤システムの整備・保守及び宮内庁 NWS の運用管理業務に係る民間競争入札総合評価基準書」
- 別紙 評価基準表

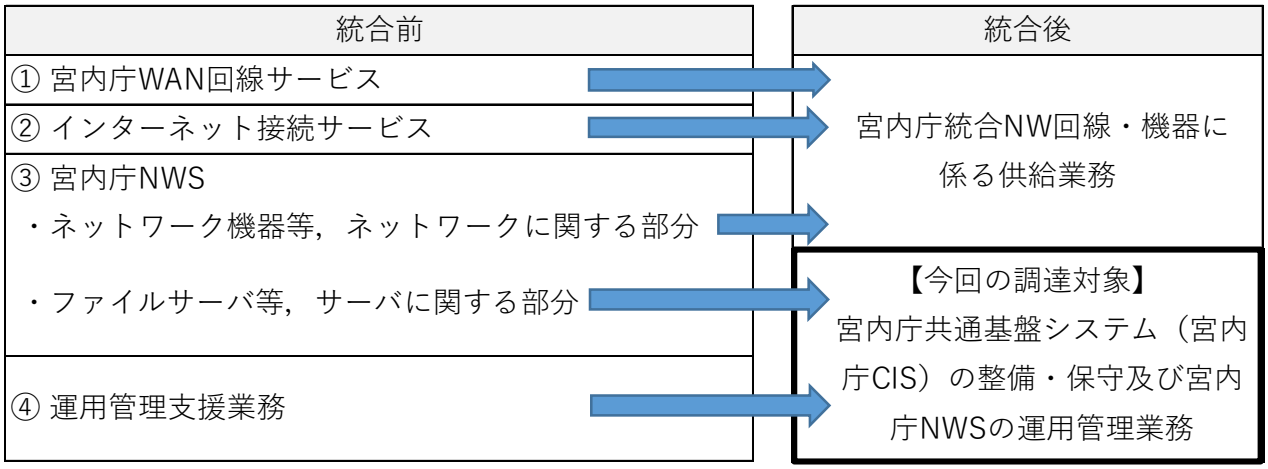
1. 趣旨

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，宮内庁（以下「当庁」という。）は「公共サービス改革基本方針」（平成 24 年 7 月 20 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「宮内庁ネットワーク運用管理支援業務」（調達名は「宮内庁共通基盤システムの整備・保守及び宮内庁 NWS の運用管理業務」）について，公共サービス改革基本方針に従って，民間競争入札実施要項を定めるものとする。

注：これまで「宮内庁ネットワークシステムの運用管理支援業務」の調達については，宮内庁 NWS の整備・保守に係る調達とは別の調達として行っていたが，今回，宮内庁 NWS の整備・保守に係る調達について，基盤サーバ群に係るものとネットワーク機器・回線等に係るものとに分離した上で，運用管理支援業務の調達については，その業務の対象が主に基盤サーバ群に係るものであるということから，基盤サーバ群の整備・保守に係る調達と統合して行うこととした。

そのため，調達名は「宮内庁共通基盤システムの整備・保守及び宮内庁 NWS の運用管理業務」となり，本業務を落札した民間事業者（以下「請負者」という。）の業務には宮内庁共通基盤システムの整備・保守も含まれることになる。



（本実施要項13ページ「図１：全体日程」を参照。）

【注】

- **宮内庁共通基盤システムの整備・保守及び宮内庁NWSの運用管理業務 → 基盤サーバ群の整備・保守と運用管理業務の調達**
- **宮内庁統合NW回線・機器に係る供給業務 → ネットワークインフラ（回線及びネットワーク機器）に係る調達**

2. 用語の定義

本実施要項における用語については，別添１「宮内庁共通基盤システムの整備・保守及び宮内庁 NWS の運用管理業務に係る民間競争入札調達仕様書（案）（以下「仕様書」という。）」の「1.3.用語の定義」を参照すること。

3. 本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

3.1.本業務の概要

現在，宮内庁 NWS は，皇居内に設置された構内ネットワーク（本庁 LAN）と，皇居外に所在する当庁の各部署それぞれに設置された構内ネットワーク（拠点 LAN）と，それら全ての LAN（宮内庁 LAN）を IP－VPN 回線で相互に接続し統合した広域拠点間ネットワーク（宮内庁 WAN）とで構成されており，一府省庁一ネットワークの体制になっている。この宮内庁 NWS においては，グループウェア（電子メール機能等），ファイルサーバ，インターネット接続，正倉院宝物管理等各種システムのネットワーク情報サービスが提供されている。

請負者の運用管理業務は，宮内庁 NWS の運用，管理等を行うことにより，宮内庁職員等（以下「ユーザ」という。）に対して宮内庁 NWS が有する機能を安定的に供給することである。

また，本業務では，日常的に使用する基盤サーバ群を始めとした宮内庁 CIS の整備，移行作業，サービスの提供及びそれに伴う保守も請負者の業務としている。これにより，情報システム障害対応等の迅速化も可能となり，利用者であるユーザの業務への影響，とりわけ情報システムを正常に利用できないことによる業務遅延などを最小化し，より効果的な IT マネジメントの実施を目指すものである。

3.2.宮内庁 NWS 等の概要

3.2.1. 概要

宮内庁 NWS は，ユーザが端末やプリンタ等の情報機器を利用し，電子メールの送受信，インターネット等のサービスの利用及び作成した情報資産を管理・共有するネットワークシステムであり，当庁の基幹システムとなっている。主な機能等は以下のとおり。

なお，本調達の運用期間中にクライアント端末，プリンタ及び複合機の増設が生じた場合でも，本調達の範囲内として運用対象とすること。

① 構成

・クライアント端末 約 1,200 台
・プリンタ 約 140 台
・複合機 約 110 台

② オペレーティングシステム

③ 業務のための各種アプリケーションソフトウェア

④ グループウェアシステム

グループウェアを利用することにより，スケジュール管理，会議室の予約等の各機能を有し，また，庁内間及びインターネット経由での民間との電子メールの送受信が可能となっている。

⑤ 霞が関の各府省庁を専用線で繋いだ広域ネットワークである「政府共通ネットワーク」と接続されており，インターネットを介さずに他省庁等との電子メールの送受信を含む情報交換が可能となっている。

⑥ ユーザ管理機能によりアカウント管理を行い，ユーザの人事異動情報を容易に各担当者が入力できるようになっている。

⑦ 宮内庁 NWS からネットワークを介して利用されるシステム

○ 宮内庁公開システム（情報システム IDA000771）
以下の３システムから構成されている。

・　宮内庁ホームページ
　宮内庁ホームページは，平成 9 年度に開設し，現在では皇室の様々な御活動を始め，参観申込要領，職員採用，報道発表資料（御動静及び御会見等）等を情報発信している。

・　皇居等参観受付システム
　当該システムは，平成 15 年度に導入されたシステムであり，皇居を始め京都御所等における参観業務のデータを一元的に管理し，インターネットで全国どこからでも参観申込みができるよう整備したものである。
　なお，同システムの管理端末は，本調達における運用管理業務の対象に含まれている。

・　情報公開関係システム
　当該システムは，平成 17 年度に導入されたシステムであり，職場や自宅の端末からインターネットを通じて情報公開法に基づく開示請求ができるよう整備したものである。

○　ＣＡＤシステム（情報システム ID A000782）
　宮内庁施設の図面の作成及び管理等の業務を電子化・データベース化して関係部局が共有することにより，事務の効率化を図るため，平成 12 年度に導入したシステムである。
なお，同システムに係るバックアップ役務作業は，本調達における運用管理業務の対象に含まれている。

○　正倉院宝物公開管理システム（情報システム ID A000793）
　正倉院宝物の画像・資料等のデータの蓄積及び宮内庁ホームページを通じて一般に公開するために平成14年度に開設されたシステムである。
　なお，同システムの管理端末は，本調達における運用管理業務の対象に含まれている。

○　図書寮文庫所蔵資料目録画像公開システム(情報システム ID A016231)
　宮内庁書陵部が所蔵する図書の適切な保存及びインターネットを通じて目録情報などを広く一般の利用者に供するため平成 25 年度に導入したデジタルアーカイブ・システムである。

○　標的型攻撃対策システム（情報システム ID A000760（宮内庁 NWS と同一））
　標的型メール（なりすまし）等によるサイバー攻撃の脅威からの防御や検知，情報セキュリティ強化のため平成 25 年度に導入したシステムである。

3.2.2.　機器構成

宮内庁 NWS 構成図及び機器は，別添 1 仕様書における別途閲覧（別紙 1「資料閲覧願い」）に供するので確認すること。

3.2.3.　利用特性

ユーザ約 1,200 名，クライアント端末約 1,200 台により，原則として 24 時間 365 日利用される。

3.2.4.　設置拠点

宮内庁 NWS の設置拠点は，別紙 1「宮内庁 NWS 設置拠点」に示す。

3.3.本業務の内容

請負者は，主に以下の内容の業務を行う。その詳細は仕様書に示す。

(1) 統括管理

本業務全体に係る作業実施計画作成，体制整備，進捗管理及び課題管理等を行う。

(2) 設計

仕様書，提案書及び各種ドキュメントに基づき，宮内庁 NWS のサーバ群等の機器に関する設計，移行業務及び運用管理業務の計画作成等を行う。

宮内庁統合 NW でなされた全体ネットワーク設計方針を前提とし，調達仕様書，提案書及び各種ドキュメントに基づき，宮内庁 LAN 基盤サーバ群等の機器に関する設計，移行業務及び運用管理業務の計画作成等を行う。設計に当たっては，宮内庁統合 NW 側の方針を精読し，設計方針に則って必要な作業を実施する。

(3) 構築

各種設計書及びドキュメントに基づき，機器等について，稼働に必要なソフトウェアのインストールや設定等を実施して指定の場所に搬入し，設置調整等の構築作業を行い，必要十分な機能を確実に動作させる。

(4) テスト

各種テストの計画書を作成し，テストを実施する。

なお，当庁担当者が主体となって実施する受入テストの支援を行う。

(5) 移行

各種設計書及び移行実施計画書に基づき，現行システムから次期システムへの移行を行い，宮内庁 NWS を用いたユーザ業務の継続性を保つ。

(6) 保守

宮内庁 LAN 基盤サーバ群等の機器障害発生時における連絡調整，障害機器等への対応及び保守業務結果に関する報告等を行う。

(7) 運用管理業務

運用管理業務は，日々の運用の中で，ユーザの異動，情報セキュリティ対策の導入などの要因に基づく宮内庁 NWS の変更管理が軸となる。主な内容は以下のとおりである。

① 運用管理手順書等の整備

・運用管理に係る既存の手順書等を適切に整理し，本業務を実施していく中で，より実態に即したものとなるよう，継続的に改善を行う。

・運用管理を実施していく中で，当庁と請負者にとって有益な手順を新たに案出した際には，それらの文書化を図る。

② 資産管理

・資産管理台帳，論理構成図，物理構成図，機器配置図，ライセンス契約管理，配線図，その他必要な文書の作成，管理を行う。

③ データ管理

・機器等データのバックアップ，バックアップログの確認，バックアップ媒体の保存，集配，交換を行う。

④ ネットワーク管理

・ネットワークセグメント及び各機器の死活，サーバの重要プロセス及びサービス稼働状況，サーバのシステムログに出力された障害情報，機器等及びサーバのリソース，パフォーマンス状況，メールログ，プロキシログ，さらには端末の操作ログ等の監視を行う。

・ネットワーク上のコンピュータの IP アドレス，ホスト名の台帳管理を行う。

・資産管理ソフトウェアによるインベントリ管理を行う。

・機器等の設定変更を行う。

⑤　ユーザ管理

・アカウント管理，パスワード管理，ファイルサーバへのアクセス権の管理を行う。

⑥　情報セキュリティ管理

・「仕様書における別途閲覧（別紙 1)」に供する当庁の情報セキュリティポリシーに則り，サーバ（Linux サーバを含む)，クライアント端末，貸出用端末，地方サーバ及び各業務システムに対しウイルス対策ソフトウェアを最新に維持する（※）とともに，ウイルス情報収集及び対策立案を行う。

※　最新に維持する対象は，パターン定義ファイル，検索エンジン及び一斉配信できるソフトウェアのマイナーバージョンアップなどとし，ソフトウェアのメジャーバージョンアップは含まないものとする。

⑦　障害対応と保守

・ハードウェア・ソフトウェアの障害発生時における一次切り分け，原因分析，復旧，ステータス管理，事後管理を迅速に行う。

⑧　性能管理

・ハードウェア・ソフトウェアの安定的かつ正常な稼働を保つ観点で，当庁が指定するサーバに対して，当庁が規定した項目に沿ったハードウェアの外観点検，システム稼働状態，トラフィック，サーバ室温度管理を行う。

⑨　個別システム運用管理

・宮内庁 NWS において提供されているグループウェアを始めとする個別システムに係るシステム監視，バックアップ処理の支援，セキュリティアップデート，個別システム保守業者，メーカー等保守契約の関係者による復旧作業に対し，適切な情報提供等の支援，復旧後の動作確認を行う。

⑩　予備機器，消耗品等の管理

・端末，HUB，UTP ケーブル，デジタル周辺機器等の予備機の管理を行う。

⑪　定例会議

・毎週，当庁において開催する運用管理会議において，運用報告を行うこと。

⑫　機器等変動に関する支援

・本業務請負期間中において機器等に変動があった場合には，助言，支援及び必要な資料の提供，作成を行う。

⑬　計画停電

・1 年に 1 回実施される法定停電において，サーバ及び機器等の停止，起動，起動後の確認の対応を行う。

⑭　ヘルプデスク

・各種アカウントの管理及びユーザが利用するハードウェア・ソフトウェア等に関する問合せ，申請に対し迅速に対応を行う。

3.4.運用管理業務の引継ぎ

(1)　現行運用管理支援業者（以下「現行業者」という。）から運用管理業務の開始日までに運用管理手順書等を使用して必要な事務引継ぎを受けなければならない。

なお，その際の事務引継ぎに必要となる経費は，現行業者の負担となるが，請負者の責任において発生した経費は請負者の負担とする。

⑵　請負者は，次期運用管理業者への引継ぎにおいては，本業務の内容及び課題事項等，運用管理業務を遂行するために必要な情報を取りまとめた資料等を作成し，次期運用管理業者に対し適切な説明を実施し，引継ぎの内容に関する質問にも適宜対応すること。

なお，次期運用管理業者の責任において発生した経費を除いて，引継ぎに必要となる経費は請負者の負担とする。

⑶　当庁は，運用管理業務の引継ぎが円滑に実施されるよう，現行業者及び請負者に対して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。

3.5.確保されるべき本業務の質

3.5.1.　業務の内容

仕様書に示す業務を適切に実施すること。

3.5.2.　宮内庁 NWS の稼働率

稼働率は 99.7%以上とし，以下の計算式により算出する。

○ 稼働率（%）＝｛1 －（1 か月の停止時間）÷（1 か月の稼働予定時間)｝× 100

※　停止時間の計測方法については，サービス停止の範囲及びユーザへの影響度等を考慮し，落札後に当庁と協議の上，決定すること。

※　稼働予定時間は，計画停電等（停電，メンテナンス等）により停止する時間を除く。

3.5.3.　サービスレベルアグリーメント（SLA）の締結

⑴ 運用管理業務の効率化と品質向上並びに円滑化を図るため，以下に示す指標に対してサービスレベルアグリーメント（SLA）を締結すること。

①　運用管理業務の一次回答時間

（ア）　ユーザからの質問等に対する一次回答時間は，1 時間以内とすること。回答時間は以下の計算式による。

（請負者がユーザに回答した時刻）－（ユーザが請負者に対して質問等した時刻）

（ただし，17 時 45 分以降の質問については，翌営業日の 9 時 30 分までに回答すること。）

②　運用管理業務の解決時間

（ア）　ユーザからの質問等に対する解決時間は，2 営業日以内とすること。解決時間は以下の計算式による。

（ユーザの質問等が解決した日時）－（ユーザが請負者に対して質問等した日時）

（イ）　請負者の作業範囲外のものについてはサービスレベルの対象外とする。ただし，この場合においても質問等の解決に向けて協力すること。

③　障害報告時間

（ア）　各システム又は外部監視等により検出された 3.2.1.に示す機器等の障害について，30 分以内に当庁担当者に対し報告すること。障害報告時間は以下の計算式による。

（請負者が当庁担当者に報告した時刻）－（障害確認時刻）

（ただし，17 時 45 分以降の障害発生については，翌営業日の 9 時までに報告すること。）

④　障害解決時間

（ア）　各システム又は外部監視等により検出された機器等の障害について，1 営業日以内に解

決させること。障害解決時間は以下の計算式による。

（障害が解決した日時）－（障害確認日時）

（イ） 請負者の作業範囲外のものについてはサービスレベルの対象外とする。ただし，この場合においても障害の解決に向けて協力すること。

⑤ 運用要領・運用計画の遵守

（ア） 運用要領・運用計画の遵守状況に関して，当庁から指摘された改善要求件数は，0 件であること。

(2) サービスレベルの遵守状況については，月 1 回開催の SLA 報告会議において報告し，当庁の承諾を得ること。

(3) 当庁の要求水準は，「上記(1)①から⑤全ての遵守率について 99%以上であること」とする。ただし，請負者の作業範囲外のもの，又はやむを得ない事情によるものであることを当庁が承諾したものについてはサービスレベル測定の対象外とする（例えば当庁担当者と連絡がつかない，地方部局とのやり取りなど。）。

(4) (3)で要求した水準を満たせなかった場合，具体的な解決策を検討し，(2)の報告時に合わせて報告すること。

(5) 3 か月連続して(3)の要求水準を満たせなかった場合，運用体制の強化，若しくは「仕様書 5.4.作業実施体制」の変更を指示することがあるが，(3)の要求水準を満たせるまでの期間において，請負者は本契約の範囲内でこれに対応すること。

3.5.4. ヘルプデスク利用者満足度調査の結果

ヘルプデスク業務の利用者に対して，次の項目の満足度についてアンケートを実施し，その結果の基準スコア（75 点以上）を維持又は向上すること。

- 問合せから回答までに要した時間
- 回答又は手順に対する説明の分かりやすさ
- 回答又は手順に対する結果の正確性
- 担当者の対応

各項目とも，「満足」（配点 100 点），「ほぼ満足」（同 80 点），「普通」（同 60 点），「やや不満」（同 40 点），「不満」（同 0 点）で回答させ，各利用者の 4 つの回答平均スコア（100 点満点）を算出する。

3.5.5. ハードウェアの保守サービスレベル

請負者がハードウェアをオンプレミス型で提供する場合，各ハードウェアの保守サービスレベルについては，原則 24 時間×7 日間／週のオンサイト保守対応とすること。

3.5.6. ソフトウェアの保守サービスレベル

請負者は，ソフトウェアに対する修正パッチ・修正モジュール又はマイナーアップデートが製造業者等から提供された際，それらが提供された日から起算して原則 2 日（休日を除く。）以内に当庁へ報告し，適用要否の協議を実施すること。ただし，重大かつ緊急性を有する修正パッチ・修正モジュール又はマイナーアップデートについては，可能な限り遅滞なく当庁へ報告し，適用要否の協議を実施した上で適用作業を実施すること。

3.5.7. セキュリティ上の重大障害の件数

個人情報，施設等に関する情報その他の契約の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。

3.5.8. 宮内庁 NWS 運用上の重大障害件数

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。

3.6.創意工夫の発揮

本業務を実施するに当たっては，以下の観点から提案を行い，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。

(1) 宮内庁 NWS の運用管理業務に対する提案

請負者は，運用管理業務の実施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。

(2) 運用管理業務以外に対する改善提案

請負者は，運用管理業務以外に関して，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，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。

3.7.契約の形態及び支払

(1) 契約の形態は，業務請負契約とする。

(2) 当庁は，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，本業務の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。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，又は達成できないおそれがある場合，当庁は，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当庁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，当庁は，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，請負者の負担となる。

(3) 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，以下①から③に該当する場合には当庁が負担し，それ以外の法令変更については請負者が負担する。

① 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

② 消費税その他類似の税制度の新設・変更（税率の変更含む）

③ 上記①及び②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）

4. 実施期間に関する事項

(1) 全体工程

実施期間全体に係る日程を「図１.全体日程」に示す。

(2) 契約期間

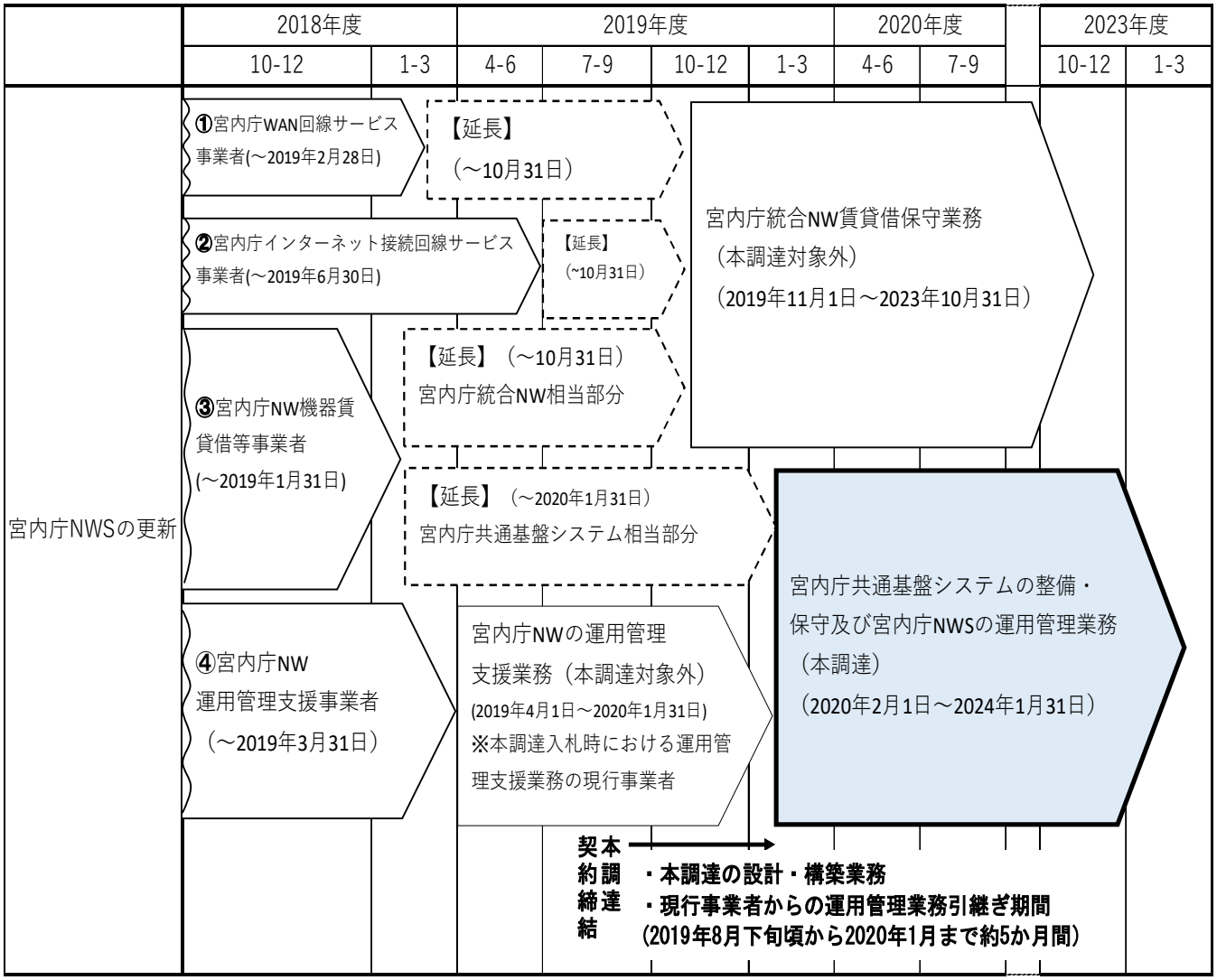
① 設計・構築業務

契約締結日（2019 年 8 月中旬～下旬頃）から 2020 年 1 月 31 日まで

② 運用管理・保守業務

2020 年 2 月 1 日から 2024 年 1 月 31 日までの 48 か月

※ 本業務の現行運用管理支援業者（以下「現行業者」という。）からの引継ぎ期間は，契約締結日（2019 年 8 月中旬～下旬頃）から 2020 年 1 月 31 日までを予定している。



注：①～④は，本実施要項５ページ「趣旨」の図の番号に対応

図１．全体日程

5. 入札参加資格に関する事項

5.1.入札参加資格

(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。以下「予決令」という。）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) 予決令第 71 条の規定に該当しない者であること。

(4) 平成 31・32・33 年度内閣府競争参加資格（全省庁統一資格）「役務の提供等」の「A」又は「B」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。

(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) 当庁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) 本仕様書の作成に直接関与した事業者及びその関連事業者（「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子会社並びに緊密な利害関係を有する事業者をいう。）ではないこと。

(9) 調達計画書及び仕様書の妥当性確認並びに入札事業者の審査に関する業務を行う宮内庁 CIO 補佐官及びその支援スタッフ等（常時勤務を要しない官職を占める職員，「一般職の任期付職員の採用及び給与の特例に関する法律」（平成 12 年 11 月 27 日法律第 125 号）に規定する任期付職員及び「国と民間企業との間の人事交流に関する法律」（平成 11 年 12 月 22 日法律第 224 号）に基づき交流採用された職員を除く。）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，宮内庁 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。

（注）入札参加グループとは本業務の実施を目的に複数の事業者が組織体を構成し，本業務の入札に参加する者のことを指す。

(11) 本業務の実施予定組織・部門は，品質管理体制として ISO9001:2015 又は，組織能力成熟度の CMMI レベル３以上のどちらかの認証を取得しているか，同等の品質管理体制を構築できていることを必要十分に証明することが可能な資料を提出すること。

(12) 本業務の実施予定組織・部門は，プライバシーマーク付与認定，又は ISO/IEC27001 認証（国際標準）若しくは JIS Q 27001 認証（日本工業標準）のいずれかを取得していること。

(13) 本業務の実施予定部門が ISO14001 の認証を取得しており，環境マネジメントを適確に行う体制が整備されていることを証明すること。

(14) 過去５年以内に，本件と同等規模以上の情報システム構築（設計，開発及び導入）及び保守運用を請け負った実績を有すること。ただし，ヘルプデスクのみの実績は認めない。

(15) 資本関係・役員等の情報，受託作業の実施場所に関する情報，受託業務の従事者の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績及び国籍に関する情報を提案書とともに提出すること。

(16) 保守性を高めるためにベンダーロックインとならないよう，システムの設計において属人性を排除しつつ標準化を図り，オープンな技術やフレームワークによるシステム構築が可能であること。

5.2.運用管理責任者（個人）の実績・資格

(1) 請負者は，本業務の円滑な実行や，運用作業員のみでは対処できない技術的な問題を解決するため，運用管理責任者（1 名以上配置すること。）を設け，運用作業員のサポートを行わせること。

なお，運用管理責任者は，1 週間のうち休日を除く平日の 60%以上，1 名が情報管理室に勤務することとし，運用管理責任者は以下の実績・資格を有することとする。ただし，運用管理責任者を複数配置する場合において，以下の③，④については，同一の者が両方を満たす必要はなく，運用管理責任者全体で③及び④を満たせばよいこととする。その場合には，運用管理責任者同士が密に連携をとって業務に臨むこと。

① 過去 5 年以内に実施された「宮内庁 NWS 同等以上システム」において，システム設計，構築，運用等の責任者を務めた経験を有すること。また，受注実績を示す文書を提出すること。

なお，「宮内庁 NWS 同等以上」とは，「3.2.宮内庁 NWS 等の概要」記載の構成及び別紙 2「従来の実施状況に関する情報の開示」（業務の繁閑の状況とその対応）記載の対応件数と同等以上であることとする。

② システム設計・構築・運用等の業務経験を 5 年以上有すること。

③ 「IT スキル標準 V3 2011」の IT サービスマネジメントの専門分野のうち，オペレーション，運用管理，システム管理又はサービスデスクのいずれか一つで達成度指標及びスキル熟達度ともにレベル 4 以上に相当する実務上の知識・経験を有すること。

④ 「情報処理促進法」に基づいて行われる情報処理技術者試験のうち，ネットワークスペシャリスト試験の合格者及び又は「情報処理促進法」第 15 条の規定に基づく情報処理安全確保支援士の登録を受けている者（又は同等の資格を有する者）であるか，又は「IT スキル標準 V3 2011」の IT スペシャリストのいずれかの専門分野で達成度指標及びスキル熟達度ともにレベル 4 に相当する実務上の知識・経験を有すること。

5.3.運用作業員（個人）の実績・資格

(1) 運用作業員（常駐者（1 名以上配置すること。）及び代替者）は，以下の実績・資格を有すること。

① 「宮内庁 NWS 同等以上システム」の企画，設計・開発，運用に関する業務に 3 年以上従事した経験を有すること。ヘルプデスク業務のみの実績は認めない。

なお，「宮内庁 NWS 同等以上」とは，「3.2.宮内庁 NWS 等の概要」記載の構成及び別紙 2「従来の実施状況に関する情報の開示」（業務の繁閑の状況とその対応）記載の対応件数と同等以上であることとする。

② 「IT スキル標準 V3 2011」（平成 24 年 3 月 26 日　独立行政法人 情報処理推進機構）（http://www.ipa.go.jp/jinzai/itss/download_V3_2011.html）における，「IT サービスマネジメ

ント」の専門分野「オペレーション」で達成度指標及びスキル熟達度ともにレベル３に相当する知識・経験を有すること。

③　IT ガバナンスのフレームワークの知識を有することを証明するため，ITIL Foundation 以上の資格を有し，証明できること。

④　Windows サーバ及びクライアント端末，Linux サーバ，それらを接続するネットワーク機器についての運用経験を有しており，業務上必要なシェル・コマンドの操作，スクリプト及びバッチファイルの作成と正常動作確認ができる能力を有していること。

⑤　当庁で現在利用している汎用ソフトウェアや汎用ミドルウェア全般についての専門知識と操作経験を有しており，迅速なヘルプデスク業務が実施可能な能力を有していること。

⑥　業務遂行において，ユーザや既存各システムの構築・保守業者と日本語により円滑で適切なコミュニケーションが図れること。

5.4.リモートで運用作業員のサポートを行う場合の要件

リモートにより，運用作業員のサポートを実施する（以下，「サポート業務」という。）には，セキュリティが確保された体制となっているか，サポート人員の実績・資格等が運用作業員と同等以上であるかなどの条件を満たす必要があり，情報管理室での勤務するのと遜色ないサービスレベルが維持されることを前提に認めることは，あり得る。

サポート業務の遂行に当たっては，請負者が保有する運用拠点からリモートで運用作業を行うことを可とするが，当庁内の機器に対しオペレーションを伴う作業を行う場合においては，以下の要件を遵守すること。

なお，運用拠点及び運用業務を行う居室（以下，「運用居室」という。）について，要件遵守の確認のため，当庁が立ち入りを求めた場合は，入室を許可すること。

5.4.1.基本要件

(1)　当庁より受領した情報については厳重に管理を行い，サポート業務遂行以外の目的に利用してはならない。

(2)　記録された映像やログ等は，当庁からの求めがあった場合は，速やかに提供すること。

5.4.2.ネットワーク接続形態要件

(1)　運用管理支援業務をリモートで行うに当たって宮内庁 NWS に接続を行う場合は，以下(2)の条件を満たす閉域等されたネットワーク（以下，「閉域等NW」という。）にて接続を行うこと。

(2)　接続される閉域等NWについて，インターネットを介した VPN を用いる場合には，OSI 階層モデルのネットワーク層以下での経路の暗号化手続きを行う通信経路上のセキュリティを配慮した方式であるか，又は，インターネットを介さない閉域網（専用線，閉域 IP 通信（IP-VPN）等）の利用とする。

(3)　該当の閉域等NWには，あらかじめ当庁に申請し許可を得た端末以外の端末は接続できない措置を講じること。

(4)　閉域等NWを利用して接続を行う場合は，当庁内に設置する機器等も含めその設営等に係る費用は，すべて請負者が負担すること。

5.4.3.運用拠点要件

(1) 運用拠点は，公共交通機関を利用して，当庁へ 2 時間を目途に到着できる場所に存在すること。
(2) 運用拠点には，運用管理責任者を配置すること。
(3) 運用拠点は，防火構造，空調設備を備えた建物であること。
(4) 運用拠点は，免震ないしは耐震構造建物となっており，震度 6 相当の地震にも耐えうること。
(5) 運用拠点には，常時安定した電力供給ができるほか，電力の瞬間停電等の際も，連続的な運転を可能にする措置が講じられていること。
(6) 運用拠点には，機械的に判別できる本人認証技術を用いた入場制限がなされており，受託者関係者以外の人員が出入りできない措置が講じられていること。
(7) 運用拠点への出入りは，監視カメラにより撮影され，その映像は記録されていること。記録した映像の保管・管理は，両者協議の上で決定すること。

5.4.4.運用居室要件

(1) 運用居室は，他の居室と壁で完全に仕切られているなど独立した居室であること。
(2) 運用居室は原則としてサポート業務専用の居室とすること。やむを得ず他業務と共有をする場合は，共有期間を明示した上で他業務内容及びその必要性についてあらかじめ当庁にその理由を記した書面を提出し承諾を得ること。
(3) 運用居室内には，あらかじめ当庁が承諾し登録された人員以外が出入りできない措置が講じられていること。
(4) 運用居室には，機械的に判別できる本人認証技術を 2 種類以上用いた入場制限がなされていること。
(5) 運用居室内に入室可能な人員は，あらかじめ当庁に書面にて名簿を提出し承諾を得ること。この人員を変更する場合は，その都度変更した名簿を当庁に提出して承諾を得ること。
(6) 運用居室への入退室は，人員ごとに入室時刻及び退室時刻を自動的に記録（ログ等）ができるものとし，当庁がこの記録を求めた場合は，即座に提出すること。また，この記録は，意図的な改ざんが不可能であること。
(7) 運用居室内では，原則として宮内庁 NWS に接続する閉域等NW以外の他回線の引き込みを行わないこと。やむを得ず他回線の引き込みを行う場合は，あらかじめ当庁にその理由を記した書面を提出し承諾を得ること。
(8) 運用居室内に人員が滞在している間は，常時監視カメラにより撮影され，その映像は記録されていること。
(9) 監視カメラで撮影される範囲は，死角がないように居室全体とすること。
(10) 監視カメラには，同カメラ自体に撮影を妨げる行為があった場合，それを検知し，その記録（ログ等）を保存できること。
(11) 監視カメラで記録した映像及びログ等は，少なくとも 1 年保存・管理すること。詳細については，両者協議の上で決定すること。

5.4.5.運用端末要件

(1) 運用端末は本業務を行うための専用端末とし，他の用途には使用しないこと。
(2) 運用端末の操作は，あらかじめ登録されている人員のみとし，登録されているどの人員が，いつ，

どんな操作をしたのか記録等（ログ等）をすること。また，運用端末を操作する際にコンピュータ・ネットワークを利用する人を識別するための番号であるユーザ ID を使用する場合は，総務省「国民のための情報セキュリティサイト」を踏まえ，次のルールを遵守すること。

【ユーザ ID 及びパスワードのルール】

① パスワードの長さ

管理者権限ユーザの場合は 13 桁以上，一般権限ユーザの場合は 8 桁以上とすること。

② パスワードは，数字，アルファベット大文字と小文字及び記号の 4 つの文字種を組み合わせること。

③ 数字の単なる羅列など，他人に推測されやすいパスワードやデフォルト（製品の初期値等）のパスワードは速やかに本ルールに沿って変更すること。

④ 本業務の運用端末操作ためのユーザ ID 及びパスワードは，他の業務の端末操作等では使用しないこと。

⑤ 運用作業員ごとの個別ユーザ ID で，作業すること。

※［参考］総務省 国民のための情報セキュリティサイト

http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/basic/privacy/01.html

(3) 運用端末は，宮内庁 NWS 以外に接続を行わないこと。また，運用端末を誤って他のネットワークに接続した場合は，外部との通信ができないような仕組みを講じること。

(4) 運用端末は，セキュリティワイヤー等で什器等固定物に繋げ，施錠等し，持ち出しができない措置を講じること。

(5) 運用端末に，USB メモリ等の外部電磁的記録媒体を接続し，データの取り込み，書き込み及び持ち出しができない措置を講じること。やむを得ず運用端末に外部電磁的記録媒体を接続する必要が生じる場合は，あらかじめ当庁にその理由を記した書面を提出し承諾を得ること。また，承諾を得た後，外部電磁的記録媒体を運用端末へ接続する直前には，必ずウイルス検査を行い，ウイルスが存在していないことを確認した上で接続すること。

(6) 運用端末のハードディスクは，暗号化される措置を講じること。

(7) 運用端末に保管するファイルは，自動的に暗号化される措置を講じること。

(8) 運用端末は，ウイルス対策ソフトがインストールされており，常に最新の状態でウイルス対策ができる措置を講じること。

(9) 運用端末の OS 及び各種ソフトウェア等の脆弱性情報を常に確認し脆弱性対策を講じること。

(10) 万一，運用端末がマルウェアに感染した場合又は感染のおそれがあると判断した場合は，当該端末を即座に宮内庁 NWS から切り離し，速やかに当庁に書面による報告を行うこと。感染原因の追及に当たっては，セキュリティオペレーションセンター等の支援を得て，受託者の負担においてフォレンジック調査等を行い，侵入経路，感染ルート等の原因調査を行い，その結果及び今後の防止対策を講じた上で，当庁に説明を行うこと。

(11) 運用管理支援業務の契約期間満了後には，速やかに運用端末内で保管・管理されている当庁に関する一切の情報が残らない（復元を不可能とする）措置をとり，データ消去証明書を当庁提出すること。

なお，データ消去に当たっては，当庁が定めた「情報処理及び情報システムについての対策規程（平成 27 年 3 月 10 日 統括情報セキュリティ責任者決定）」を遵守すること。

6. 入札に参加する者の募集に関する事項

6.1.入札手続（スケジュール）

(1) 入札公示：官報公示	2019 年 6 月中旬頃
(2) サーバ室閲覧及び資料閲覧	2019 年 6 月中旬～7 月上旬頃
(3) 質問受付期限	2019 年 7 月上旬頃
(4) 適合証明書（提案書）の提出期限	2019 年 7 月中旬頃
(5) 適合証明書の合否回答	2019 年 8 月上旬頃
(6) 入札書の提出期限	2019 年 8 月上旬～中旬頃
(7) 開札及び落札予定者の決定	2019 年 8 月中旬頃
(8) 契約締結	2019 年 8 月中旬～下旬頃
(9) 引継ぎ期間	契約締結日から 2020 年 1 月末日

6.1.1. サーバ室閲覧及び資料閲覧並びに質問受付

本業務の入札説明会は実施しないが，個別にサーバ室閲覧及び資料閲覧並びに質問受付の場を設けることにより，必要な情報は提供する。

本業務実施場所（サーバ室）及び本業務関係資料等の閲覧を希望する場合は，必ず資料閲覧可能期間に，以下の連絡先にあらかじめ連絡の上，仕様書別紙 1「資料閲覧願い」に記載し，閲覧日及び閲覧希望資料を調整すること。

資料閲覧可能期間：2019 年 6 月中旬から 7 月上旬頃までの予定（土日祝日を除く）
〒100-8111　東京都千代田区千代田 1-1（皇居内）
電 話 番 号：03-3213-1111（内線 3231）
ＦＡＸ 番 号：03-5220-1221
担当係：宮内庁長官官房調査企画室秘書課情報係

本件入札に関する質問は，2019 年 6 月中旬から 7 月上旬頃まで受け付ける予定である。

6.2.入札書類

入札参加者は，次に掲げる書類を別に定める「入札説明書」及び「宮内庁競争入札心得」に記載された期日及び方法等により提出すること。入札説明書等は，入札公告以降に当庁において交付する。

(1) 代表者の証明する適合証明書及び適合証明書の付随資料
(2) 提案書
(3) 入札書及び委任状
(4) 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定について評価するために必要な書類。（落札予定者となった者のみ提出。）

7. 本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業務を実施する者の決定に関する事項

以下に本業務を実施する者の決定に関する事項を示す。なお，詳細は別添２「宮内庁共通基盤システムの整備・保守及び宮内庁 NWS の運用管理業務総合評価基準書（以下「総合評価基準書」という）」に

示す。

7.1.評価方法

本業務を実施する者（以下「落札者」という。）の決定は，総合評価落札方式によるものとする。なお，技術の評価に当たっては，入札プロセスの中立性，公正性等を確保するため，宮内庁の CIO 補佐官に意見を聴くものとする。また，総合評価は，価格点（入札価格の得点）に技術点（総合評価基準書による加点）を加えて得た数値（以下「総合評価点」という。）をもって行う。

価格点と技術点の配分

価格点の配分：技術点の配分 ＝ 1 ： 1

総合評価点 ＝ 価格点（4,000 点満点） ＋ 技術点（4,000 点満点）

7.2.決定方法

総合評価基準書の評価項目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，一つでも欠ける場合は「不合格」とする。

7.3.総合評価点

(1) 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）× 4,000 点

(2) 技術点の評価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 500 点与える。

イ 「合格」した提案書について総合評価基準書に基づき，加点を行う。

(3) 「基礎点」と「加点」の合計点を「技術点」とする。

技術点 ＝ 基礎点（500 点） ＋ 加点（3,500 点）

7.4.落札者の決定

(1) 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決令第 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」によって得られた数値の最も高い者を落札者とする。ただし，予決令第 84 条の規定に該当する場合は，予決令第 85 条の基準を適用するので，基準に該当す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，入札参加者は当庁の行う事情聴取等の調査に協力しなければならない。

(2) 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。

（会計法第 29 条の 6 第 1 項ただし書き抜粋） 相手方となるべき者の申込みに係る価格によっては，その者により当該契約の内容に適合した履行がされないおそれがあると認められるとき，又はその者と契約を締結することが公正な取引の秩序を乱すこととなるおそれがあって著しく不適当であると認められるとき

(3) 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。

(4) 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(2)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性能等の得点）の提供を要請することができる。

7.5.落札者の取消し

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。

7.6.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は，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再度の入札公告によると本業務の実施の準備に必要な期間が確保できない等のやむを得ない事情がある場合には，入札対象事業を自ら実施すること等ができる。この場合において，当庁はその理由を官民競争入札等監理委員会（以下，「監理委員会」という。）に報告するとともに公表する。

8. 運用管理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

運用管理業務に関して，以下の情報は，別紙 2「従来の実施状況に関する情報の開示」のとおり開示する。

(1) 従来の実施に要した経費

(2) 従来の実施に要した人員

(3) 従来の実施に要した施設及び設備

(4) 従来の実施における目標の達成の程度

(5) 従来の実施方法等

「従来の実施方法等」の詳細な情報は，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，仕様書，各種運用ドキュメント及び各種報告書等について，所定の手続を踏まえた上で閲覧可能とする。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，当庁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。

9. 請負者に使用させることができる国有財産に関する事項

(1) 請負者は，次のとおり国有財産を使用することができる。

① 国有財産の使用

(ア) 請負者は，本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。

・ 業務に必要な電気設備

・ その他，当庁と協議し承諾された業務に必要な施設，設備等

② 国有財産の使用制限

(ア) 請負者は，本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，あらかじめ当庁と協議した上で，当庁の業務に支障を来さない範囲内において，施設内に本業務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。

10. 請負者が，当庁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講じるべき措置に関する事項

10.1. 請負者が当庁に報告すべき事項，当庁の指示により講じるべき措置

10.1.1. 報告等

(1) 請負者は，仕様書に規定する業務を実施したときは，仕様書に基づく各種報告書を当庁に提出しなければならない。

(2) 請負者は，本業務を実施し，完了に影響を及ぼす重要な事項の変更が生じたときは，直ちに当庁に報告するものとし，当庁と請負者が協議するものとする。

(3) 請負者は，契約期間中において，(2)以外であっても，必要に応じて当庁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。

10.1.2. 調査

(1) 当庁は，運用管理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，又は当庁の職員が請負者の事務所に立ち入り，本業務の実施の状況若しくは記録，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。

(2) 立入検査をする当庁の職員は，検査等を行う際には，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。

10.1.3. 管理者用ＩＤ・パスワードの取扱い

請負者は，管理者用ＩＤ・パスワードの取扱いについて，以下の事項を遵守すること。

(1) 当庁の指定する設定条件に基づき申請を行い，当庁より付与を受けること。

(2) 管理者用ＩＤの使用状況については，当庁の指示に基づき，定期的に報告すること。

(3) その他，管理者用ＩＤ・パスワードの管理，変更，削除等について，当庁の指示に従うこと。

10.1.4. 指示

当庁は，本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。

10.2. 秘密を適正に取り扱うために必要な措置

(1) 請負者は，本業務の実施に際して知り得た当庁の情報等（公知の事実等を除く）を，第三者に漏らし，盗用し，又は本業務以外の目的のために使用してはならない。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。

(2) 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当庁が認めた場合に限り，第三者へ開示できるものとする。

(3) 請負者は，当庁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ければならない。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。

(4) 請負者は，本業務の開始時に本業務に係る情報セキュリティ確保のための措置を講じ，実施方法及び管理体制について当庁に書面提出しなければならない。

(5) 請負者は，当庁から要機密情報が提供された場合には，当該情報の機密性の格付けに応じて適切に取り扱うための措置を講じること。また，本業務において請負者が作成する情報については，当庁からの指示に応じて適切に取り扱わなければならない。

(6) 請負者は，次のいずれかに該当するときは当庁の行う情報セキュリティ対策に関する監査を受け入れなければならない。

① 本業務に係る情報セキュリティ確保のための措置が不十分とみなされるとき。

② 請負者において本業務に係る情報セキュリティ事故が発生したとき。

③ 当庁が定期的に実施している情報セキュリティ監査を行うとき。

④ その他，当庁が必要と認めるとき。

(7) 請負者は，当庁から提供された要機密情報が業務終了等により不要になった場合には，確実に返却し，又は破棄すること。また，本業務において請負者が作成した情報についても，当庁からの指示に応じて適切に破棄しなければならない。

(8) 請負者は，当庁の情報セキュリティに関する規定等に基づき，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，仕様書別紙「機密保持に関する誓約書」への署名を遵守しなければならない。

(9) (1)から(8)までのほか，当庁は，請負者に対し，本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。

10.3. 契約に基づき請負者が講じるべき措置

10.3.1. 本業務の開始

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。

10.3.2. 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，書面により当庁の事前の承諾を得たときは，この限りではない。

10.3.3. 権利義務の帰属等

(1) 本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。

(2) 請負者は，本業務の実施状況を公表しようとするときは，あらかじめ，当庁の承認を受けなければならない。

10.3.4. 瑕疵担保責任

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

(2) 成果物の瑕疵が請負者の責に帰すべき事由によるものである場合は，当庁は，前項の請求に際し，これによって生じた損害の賠償を併せて請求することができる。

10.3.5. 再委託

(1) 請負者は，本業務の実施に当たり，その全部を一括又は主たる部分を再委託してはならない。

(2) 請負者は，本業務の実施に当たり，その一部について再委託する場合には，原則として，あらかじめ提案資料において，再委託先に委託する業務の範囲，再委託を行うことの合理性及び必要性，再委託先の履行能力並びに報告徴収，個人情報の管理その他の運営管理の方法について記載しなければならない。

(3) 請負者は，契約締結後やむを得ない事情により再委託する場合には，(2)に準じて当庁の承諾を得なければならない。

(4) 請負者は，(2)又は(3)により再委託を行う場合には，請負者が当庁に対して負う義務を適切に履行するため，再委託先の事業者に対し「10. 2. 秘密を適正に取り扱うために必要な措置」及び「10. 3. 契約に基づき請負者が講じるべき措置」に規定する事項その他の事項について，必要な措置を講じさせるとともに，再委託先から必要な報告を聴取することとする。

(5) (2)及び(3)に基づき，請負者が再委託先の事業者に義務を実施させる場合は，全て請負者の責任において行うものとし，再委託先の事業者の責に帰すべき事由については，請負者の責に帰すべき事由とみなして，請負者が責任を負うこととする。また，再委託先については，請負者と同等の義務を負わせるものとする。

(6) 仕様書に基づく作業に関し，第三者との間に著作権に係る権利侵害の紛争等が生じた場合は，当該紛争の原因が専ら当庁の責めに帰す場合を除き，請負者の責任と負担において一切の処理をすること。

10.3.6. 契約内容の変更

当庁及び請負者は，本業務の質の確保の推進，またはその他やむを得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。

10.3.7. 機器更新等の際における民間事業者への措置

当庁は，次のいずれかに該当するときは，請負者にその旨を通知するとともに，請負者と協議の上，契約を変更することができる。

(1) ハードウェアの更新，撤去又は新設，サポート期限が切れるソフトウェアの更新等に伴い運用管理対象機器の一部に変更が生じるとき

(2) セキュリティ対策の強化等により業務内容に変更が生じるとき

(3) 当庁の組織変更や人員増減に伴うシステム利用者数の変動等により業務量に変動が生じるとき

10.3.8. 契約の解除

当庁は，請負者が以下に該当するときは，請負者に対し請負費の支払を停止し，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，請負者は当庁に対して，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，当庁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，当庁との協議に基づき，本業務の処理が完了するまでの間，責任をもって当該処理を行わなければならない。

① 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。

② 契約内容の履行に関し，請負者，請負者の代理人又は使用人等に不正の行為があったとき。

③ 請負者が解約を申し出たとき。

④ 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。

⑤ 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。

⑥ 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。

⑦ 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。

10.3.9. 談合等不正行為

請負者は，談合等の不正行為に関して，別紙 3「談合等の不正行為に関する特約条項」に従うものとする。

10.3.10. 暴力団排除

請負者は，別紙 4「暴力団排除に関する特約条項」に従うものとし，入札書又は見積書の提出をもって，別紙 5「暴力団排除に関する誓約事項」に誓約等したものとする。

10.3.11. 損害賠償

請負者は，請負者の故意又は過失により当庁に損害を与えたときは，当庁に対し，その損害について

賠償する責任を負う。また，当庁は，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，当庁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。

10.3.12. 不可抗力免責・危険負担

当庁及び請負者の責に帰すことができない事由により契約期間中に物件が滅失し，又は毀損し，その結果，当庁が物件を使用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降の契約期間に係る代金の支払いを請求することができない。

10.3.13. 金品等の授受の禁止

請負者は，本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。

10.3.14. 宣伝行為の禁止

請負者及び本業務に従事する者は，本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。

10.3.15. 法令の遵守

請負者は，本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。

10.3.16. 安全衛生

請負者は，本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。

10.3.17. 記録及び帳簿類の保管

請負者は，本業務に関して作成した記録及び帳簿類を，本業務を終了し，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い。

10.3.18. 契約の解釈

(1) 本契約について，協議が必要なものにつき協議が整わないとき，又は紛争が生じたときは，当庁と請負者が協議して解決するものとする。

(2) 本契約に関して疑義が生じたとき，又は契約に定めのない事項については，当庁と請負者が協議して定めるものとする。

11. 請負者が，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負うべき責任に関する事項

本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業務に従事する者が，故意又は過失により，本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) 当庁が国家賠償法（昭和 22 年法律第 125 号）第 1 条第 1 項等の規定に基づき当該第三者に対する賠償を行ったときは，当庁は請負者に対し，当該第三者に支払った損害賠償額（当該損害の発生

について当庁の責めに帰すべき理由が存する場合は，当庁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 条等の規定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当庁の責めに帰すべき理由が存するときは，請負者は当庁に対し，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。

12. 本業務に係る法第７条第８項に規定する評価に関する事項

12.1.本業務の実施状況に関する調査の時期

当庁は，本業務の実施状況について，総務大臣が行う評価の時期（2022 年 4 月以降を予定）を踏まえ，本業務に係る運用が開始される 2019 年度以降，各年度末時点における状況を調査する。

12.2.調査項目及び調査方法

(1)　本業務の内容

各種報告書により調査

(2)　宮内庁 NWS の稼働率

各種報告書により調査

(3)　運用管理業務の一次回答時間

各種報告書により調査

(4)　運用管理業務の解決時間

各種報告書により調査

(5)　障害報告時間

各種報告書により調査

(6)　障害解決時間

各種報告書により調査

(7)　運用要領・運用計画の遵守

各種報告書により調査

(8)　運用管理業務のユーザ利用満足度調査の結果

各年度において，ユーザに対する年１回のアンケート別紙 6「利用満足度調査」の実施結果により調査

(9)　ハードウェアの保守サービス状況

各種報告書により調査

(10)　ソフトウェアの保守サービス状況

各種報告書により調査

(11)　セキュリティ上の重大障害の件数

各種報告書により調査

(12)　宮内庁 NWS 運用上の重大障害の件数

各種報告書により調査

12.3.実施状況等の提出

(1)　当庁は上記調査項目に関する内容を報告様式に従い取りまとめた本業務の実施状況等について，12.1 の評価を行うために 2022 年 4 月以降を目処に総務大臣及び監理委員会へ提出するものとする。

　また，当庁は，本業務の実施状況等の提出に当たり，宮内庁 CIO 補佐官及び外部有識者の意見を聴くものとする。

(2)　法第 45 条に基づき監理委員会から求められた場合には，本業務の実施状況等について監理委員会へ報告又は資料の提出を行うこととする。

(3)　当庁は必要に応じ本業務請負者から意見の聴取を行うことができるものとする。

13. その他の業務に関し必要な事項

13.1.本業務の実施状況等の監理委員会への報告

　当庁は，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監理委員会へ報告する。

13.2.当庁の監督体制

(1)　本契約に係る監督及び検査は，支出負担行為担当官が自ら又は補助者を命じて，立会い，指示その他の適切な方法において行うものとする。

(2)　本業務の実施状況に係る監督及び検査は以下の職員が行う。

①　監督職員：宮内庁長官官房秘書課調査企画室情報係長

②　検査職員：宮内庁長官官房秘書課調査企画室室長補佐

13.3.請負者の責務

(1)　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は，法令により公務に従事する職員とみなされる。

(2)　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。

(3)　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。

(4)　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，同院から直接又は当庁を通じて，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。

13.4.著作権

(1)　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庁に無償で譲渡するものとする。

(2)　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，当庁が承諾した場合は，この限りではない。

(3) (1)及び(2)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。
(4) 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。

13.5.本業務の詳細仕様

本業務を実施する際に必要な詳細仕様は，別添１「宮内庁共通基盤システムの整備・保守及び宮内庁NWSの運用管理業務に係る民間競争入札調達仕様書」に示すとおりである。

別紙１　宮内庁ＮＷ設置拠点・設置場所等

・御移居に伴い該当施設の名称が変更となる可能性があるので，留意すること。

拠点情報					事務，CAD端末概数（※１）	タブレット端末（※２）	システム関連端末（※３）	回線情報			備考
番号	拠点名１	拠点名２	郵便番号	住所				種別	帯域確保	帯域	
1	宮内庁本庁		100-8111	東京都千代田区千代田1番1号	E	◆	●	光	有	100Mbps	
2	宮内庁本庁（バックアップ回線）							光	有	10Mbps	
3	東宮御所		107-0051	東京都港区元赤坂2丁目1-8	D			光	有	100Mbps	
4	東宮御所（バックアップ回線）							光	有	10Mbps	
5	秋篠宮邸		詳細は契約締結後に開示します。		D			光		100Mbps	
6	常陸宮邸				A			光		100Mbps	
7	三笠宮邸				B			光		100Mbps	
8	三笠宮東邸				A			光		100Mbps	
9	高円宮邸				A			光		100Mbps	
10	高輪皇族邸				A			光		100Mbps	
11	三番町分庁舎		102-0075	東京都千代田区三番町2-18 宮内庁分庁舎	A			モバイルLTE		-	通信容量は7G以上とすること
12	埼玉鴨場		343-0021	埼玉県越谷市大字大林39	A			光		100Mbps	
13	新浜鴨場		272-0136	千葉県市川市新浜2-5-1	A			光		100Mbps	
14	多摩陵墓監区事務所	多摩部	193-0824	東京都八王子市長房町1833	A			光		100Mbps	
15	多摩陵墓監区事務所	豊島岡部	112-0012	東京都文京区大塚5-39-1	A			光		100Mbps	
16	多摩陵墓監区事務所	真野部	952-0313	新潟県佐渡市真野457	A			光		100Mbps	
17	桃山陵墓監区事務所	桃山部	612-0831	京都府京都市伏見区桃山町古城山	B			光		100Mbps	
18	桃山陵墓監区事務所	深草部	612-0871	京都府京都市伏見区深草坊町63-4	A			光		100Mbps	
19	桃山陵墓監区事務所	宇治部	611-0002	京都府宇治市木幡中村65	A			光		100Mbps	
20	桃山陵墓監区事務所	田邑部	616-8202	京都府京都市右京区宇多野馬場町1-1	A			光		100Mbps	
21	桃山陵墓監区事務所	嵯峨部	616-8382	京都府京都市右京区嵯峨天竜寺角倉町3077	A			光		100Mbps	
22	桃山陵墓監区事務所	金原部	617-0002	京都府向日市寺戸町大牧35	A			光		10Mbps	
23	桃山陵墓監区事務所	三島部	567-0018	大阪府茨木市太田3-10-3	A			光		100Mbps	
24	桃山陵墓監区事務所	可愛部	895-0065	鹿児島県薩摩川内市宮内町字脇園1935-1	A			光		10Mbps	
25	桃山陵墓監区事務所	高屋部	899-6404	鹿児島県霧島市溝辺町麓3392	A			光		100Mbps	
26	桃山陵墓監区事務所	吾平部	893-1101	鹿児島県鹿屋市吾平町上名字吾平山	A			モバイルLTE		-	通信容量は7G以上とすること
27	月輪陵墓監区事務所	月輪部	605-0977	京都府京都市東山区泉涌寺山内町34-2	B			光		100Mbps	
28	月輪陵墓監区事務所	山科部	607-8425	京都府京都市山科区御陵上御廟野町52	A			光		100Mbps	
29	月輪陵墓監区事務所	神楽岡部	606-8224	京都府京都市左京区北白川追分町57-1	A			光		100Mbps	
30	月輪陵墓監区事務所	北山部	603-8373	京都府京都市北区衣笠北高橋町1-1	A			光		100Mbps	
31	月輪陵墓監区事務所	大原部	601-1241	京都府京都市左京区大原勝林院町34-2	A			光		100Mbps	
32	月輪陵墓監区事務所	長等部	520-0037	滋賀県大津市御陵町3-2	A			ADSL		100Mbps	
33	畝傍陵墓監区事務所	畝傍部	634-0061	奈良県奈良市橿原市大久保町509	B			光		100Mbps	
34	畝傍陵墓監区事務所	奈良部	630-8236	奈良県奈良市下三条町47	A			光		100Mbps	
35	畝傍陵墓監区事務所	佐紀部	631-0803	奈良県奈良市山陵町325	A			光		100Mbps	
36	畝傍陵墓監区事務所	山辺部	632-0052	奈良県天理市柳本町1876	A			光		100Mbps	
37	畝傍陵墓監区事務所	忍坂部	633-0005	奈良県桜井市大字忍阪556	A			光		100Mbps	
38	畝傍陵墓監区事務所	傍丘部	639-0264	奈良県香芝市今泉1	A			光		10Mbps	
39	畝傍陵墓監区事務所	掖上部	634-0144	奈良県高市郡明日香村大字平田1658-1	A			ADSL		47Mbps	
40	畝傍陵墓監区事務所	吉野部	639-3115	奈良県吉野郡吉野町大字吉野山1023	A			ADSL		8Mbps	
41	古市陵墓監区事務所	古市部	583-0857	大阪府羽曳野市誉田6-11-3	B			光		100Mbps	
42	古市陵墓監区事務所	藤井寺部	583-0024	大阪府藤井寺市藤井寺4-764	A			光		100Mbps	
43	古市陵墓監区事務所	磯長部	583-0991	大阪府南河内郡太子町大字春日1532	A			光		100Mbps	
44	古市陵墓監区事務所	百舌鳥部	590-0035	大阪府堺市堺区大仙町7-1	A			光		100Mbps	
45	古市陵墓監区事務所	高野山部	648-0211	和歌山県伊都郡高野町大字高野山	A			ADSL		47Mbps	
46	那須御用邸管理事務所		329-3200	栃木県那須郡那須町大字湯本207	A			光		100Mbps	
47	須崎御用邸管理事務所		415-0014	静岡県下田市須崎字嵐の尾1206-1	A			光		100Mbps	
48	葉山御用邸管理事務所		240-0111	神奈川県三浦郡葉山町一色2038-1	A			光		100Mbps	
49	正倉院事務所		630-8211	奈良県奈良市雑司町129	B		★	光		100Mbps	
50	御料牧場		329-1224	栃木県塩谷郡高根沢町上高根沢6020	C			光		100Mbps	
51	京都事務所		602-8611	京都市上京区京都御苑3番	D		▲	光	有	100Mbps	
52	京都事務所（バックアップ回線）							光	有	10Mbps	
53	桂離宮		615-8014	京都府京都市西京区桂御園1-1	A			光		10Mbps	
54	修学院離宮		606-8052	京都府京都市左京区修学院藪添1-2	A			光		100Mbps	

※１　A：１個以上～10個未満，B：10個以上～30個未満，C：30個以上～50個未満，D：50個以上～100個未満，E：100個以上

※２　◆：タブレット端末

※３　●：統合運用管理端末，★：正倉院宝物管理端末，▲参観受付システム用端末

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27年度	平成28年度	平成29年度
	人件費	常勤職員	－	－	－
		非常勤職員	－	－	－
	物件費		－	－	－
	請負費等	役務	19,052	19,052	19,052
		機器・回線等料	0	0	0
		その他	0	0	0
計(a)			19,052	19,052	19,052
参考値(b)	減価償却費		－	－	－
	退職給付費用		－	－	－
	間接部門費		－	－	－
(a)＋(b)			19,052	19,052	19,052

（注意事項）

1. 宮内庁では，民間競争入札の対象である運用管理支援業務の全部を請負契約により実施している。
2. なお，支払い金額は，一般競争入札の落札額である。
3. 請負契約のため，費用の詳細な内訳の開示は受けられない
4. 24年度においては，予算決算及び会計令第86条の規定に基づく調査のうえ落札者を決定した。
5. 本項は運用管理のみの経費である。

2. 従来の実施に要した人員

（単位：人）

	平成27年度	平成28年度	平成29年度
（請負者における運用業務従事者）			
運用管理責任者（非常勤）	1	1	1
運用作業員（常勤）	2	2	2

（請負者における業務従事者に求められる知識・経験等）

1. 共通要件

(1) 作業要員は，別添1「宮内庁共通基盤システムの整備・保守及び宮内庁NWSの運用管理業務民間競争入札による調達仕様書」に示した業務内容を円滑に遂行できる能力を有すること。

(2) 作業要員は，宮内庁NWSを構成するハードウェア，ソフトウェアに関する知識及び操作技術を有すること。

(3) 「宮内庁NWS」と同等以上のシステム企画，設計・開発，運用に関する業務に3年以上従事した経験を有すること。
ヘルプデスク業務のみの実績は認めない。

(4) 「ITスキル標準V3 2011」（平成24年3月26日　独立行政法人 情報処理推進機構）「ITサービスマネジメント」の専門分野「オペレーション」で達成度指標およびスキル熟達度ともにレベル３に相当する知識・経験を有すること。

(5) ITガバナンスのフレームワークの知識を有することを証明するため，ITIL（Information Technology Infrastructure Library）Foundation 以上の資格を有し，証明できること。

(6) Windowsサーバ及びクライアント，Linuxサーバ，それらを接続するネットワーク機器についての運用経験を有しており，業務上必要なシェル・コマンドの操作，スクリプト及びバッチファイルの作成と正常動作確認ができる能力を有していること。

(7) 宮内庁で現在利用している汎用ソフトウェアや汎用ミドルウェア全般についての専門知識と操作経験を有しており，迅速なヘルプデスク業務が実施可能な能力を有していること。

(8) 業務遂行においてユーザや既存システムの構築・保守業者等と日本語により円滑で適切なコミュニケーションが図れること。

2. 運用管理責任者に関する要求要件

(1) 過去5年以内に実施された「宮内庁NWS」と同等以上のシステムにおいて，プロジェクトマネージャを務めた経験を有すること。

(2) システム設計・構築・運用等の業務経験を5年以上有すること。

(3) プロジェクトマネージメント協会のプロジェクトマネージメントプロフェッショナル（PMP）又は「情報処理の促進に関する法律（昭和45年法律第90号。以下「情報処理促進法」という。）」に基づいて行われる情報処理技術者試験のうちのプロジェクトマネージャ試験の合格者であること。

(4) 「情報処理促進法」に基づいて行われる情報処理技術者試験のうち，ネットワークスペシャリスト試験の合格者及び同法第15条の規定に基づく情報処理安全確保支援士の登録を受けている者（又は同等の資格を有する者）であること。

（業務の繁閑の状況とその対応）

1.　問合せ件数

平成27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)
対応件数	178	77	84	85	65	72	53	82	75	56	58	78	963

平成28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)
対応件数	107	53	63	90	52	45	91	54	57	68	79	100	859

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)
対応件数	168	103	101	141	118	81	85	73	55	73	76	71	1,145

上記の内訳及構成割合(%)

問合せ区分		割　合	概　　要
ユーザ等対応	ソフトウェア関連	22	ソフトウェアの使用方法，設定，障害に関するもの。
	アカウント	22	パスワード忘失に係る初期化依頼等に関するもの。
	パソコン等	15	パソコン・プリンタ等の使用方法，設定に関するもの。
	システム関連	41	宮内庁NWを始め個別システムに関する問合せ，使用方法，障害等に関するもの。

2.　皇居外でのオンサイト件数

○平成27年度 0件　　○平成28年度 0件　　○平成29年度 0件

3.申請件数

平成27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)
対応件数	350	58	115	92	110	64	68	92	87	58	78	129	1,301

平成28年度　(件)

	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)
対応件数	391	50	65	78	57	59	60	52	44	21	24	55	956

平成29年度　(件)

	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)
対応件数	390	51	44	104	48	37	41	26	16	24	22	61	864

上記の内訳及構成割合

申請業務区分	割　合	概　　要
ソフトウェア等インストール申請	9	業務上必要なソフトウェア等をクライアントPCにインストールするもの。
アカウント登録・変更申請	43	人事異動等に伴う職員のユーザIDの登録，変更，修正に関するもの。
パソコン・プリンタ障害申請等	14	パソコン・プリンタ等の障害にかかるもの。
宮内庁NWシステム障害申請等関連	1	宮内庁NWを始め個別システムに関する障害申請，セキュリティパッチ適用に関するもの。
不審メール調査・ウィルス駆除等	33	不審メールの調査及びウィルス感染に伴うウィルス駆除等に関するもの。

4.セキュリティパッチ適用件数

平成27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)
対応件数	5	4	4	4	6	6	6	5	9	9	8	6	72

平成28年度　(件)

	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)
対応件数	4	3	3	6	7	9	8	7	5	8	0	6	66

平成29年度　(件)

	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)
対応件数	7	5	5	10	8	7	7	7	5	9	7	7	84

（注意事項）

1.平成27年度運用期間:平成27年4月～平成28年3月（8:30～17:45） 2名/12か月

2.平成28年度運用期間:平成28年4月～平成29年3月（8:30～17:45） 2名/12か月

3.平成29年度運用期間:平成29年4月～平成30年3月（8:30～17:45） 2名/12か月

4.毎年度，4月に申請件数が多いのは，人事異動に伴うアカウント申請に伴うものである。人事異動が集中する4月1日前後が繁忙となる。

従来の実施状況に関する情報の開示

3. 従来の実施に要した施設及び設備

（施設）

施 設 名 称 ： 宮内庁本庁舎

使 用 場 所 ： 長官官房秘書課情報管理室

（設備）

宮内庁貸与

事務机×２脚，事務用回転椅子×２脚，鋼製棚×４個，パーソナルコンピュータ×２個，パソコン用プリンタ×１個

電話×２個（内線用×１，外線用×１）

（注意事項）

1. 本業務を実施する上で，必要な庁舎建物の一部及び物品については，宮内庁が無償で使用させるものとし，光熱費及び電話回線使用料についても宮内庁が負担するものとする。なお，請負者は，これらを本業務以外の目的に使用してはならない。
2. 本業務を実施する上で必要となる機器等で，現に宮内庁が所有するもの以外（運用業務上使用する事務機器及び消耗品等）は請負者において準備する。

4. 従来の実施における目標の達成の程度

		平成27年度	平成28年度	平成29年度
（SLA達成率）				
一時回答時間	目　標	1時間以内	1時間以内	1時間以内
	実　績	100%	100%	100%
	達成/受付	963/963	859/859	1,145/1,145
質問に対する解決時間	目　標	2営業日以内	2営業日以内	2営業日以内
	実　績	100%	100%	100%
	達成/受付	963/963	859/859	1,145/1,145
障害発生報告時間	目　標	30分以内	30分以内	30分以内
	実　績	100%	100%	100%
	達成/受付	10/10	3/3	0/0
障害解決時間	目　標	1営業日以内	1営業日以内	1営業日以内
	実　績	100%	100%	100%
	達成/受付	10/10	3/3	0/0
運用要領・運用計画の遵守	目　標	0件	0件	0件
	実　績	0件	0件	0件
アンケート調査		－	－	実施（全ての項目において基準スコアを上回った。）

（注意事項）

1. 一次回答時間とは，運用管理支援業務の一時回答時間であり，当庁職員等からの質問等に対する一時回答時間が1時間以内，17時45分以降の質問については翌営業日の9時30分まで
2. 質問等に対する解決時間とは，当庁職員等からの質問等に対する解決時間であり，当庁職員等からの質問等に対する解決時間が2営業日以内に回答されたもの。
3. 障害発生報告時間とは，システム又は外部監視等により検出された機器等の障害について，30分以内，17時45分以降の障害発生については，翌営業日の9時までに報告されたもの。
4. 障害解決時間とは，システム又は外部監視等により検出された機器等の障害について，1営業日以内に解決されたもの。
5. 運用要領・運用計画の遵守とは，宮内庁から改善要求を指摘された件数である。

従来の実施状況に関する情報の開示

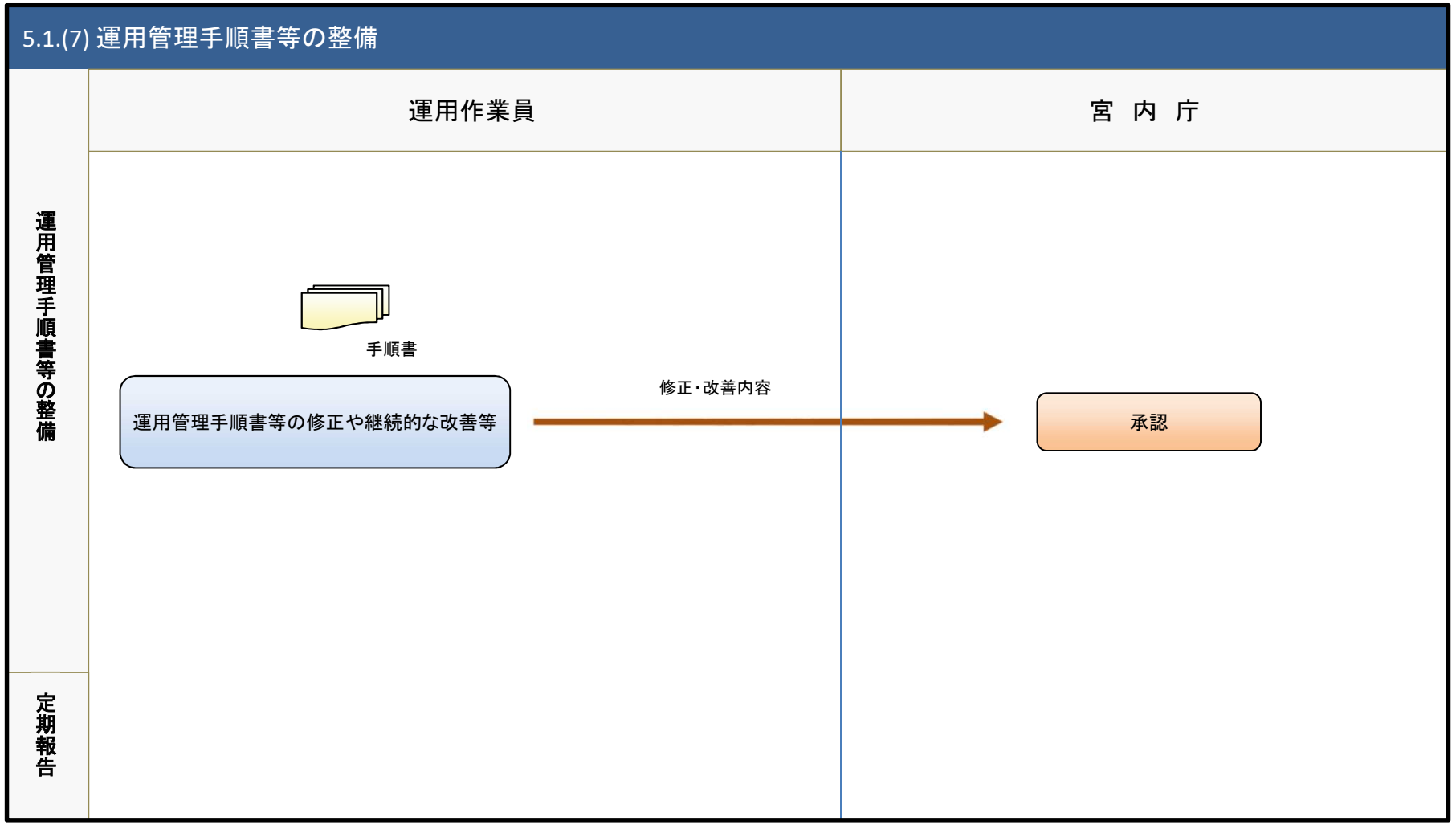
5.従来の実施方法等

1.　従来の実施方法等

付属資料　運用管理の業務フローのとおり

（注意事項）

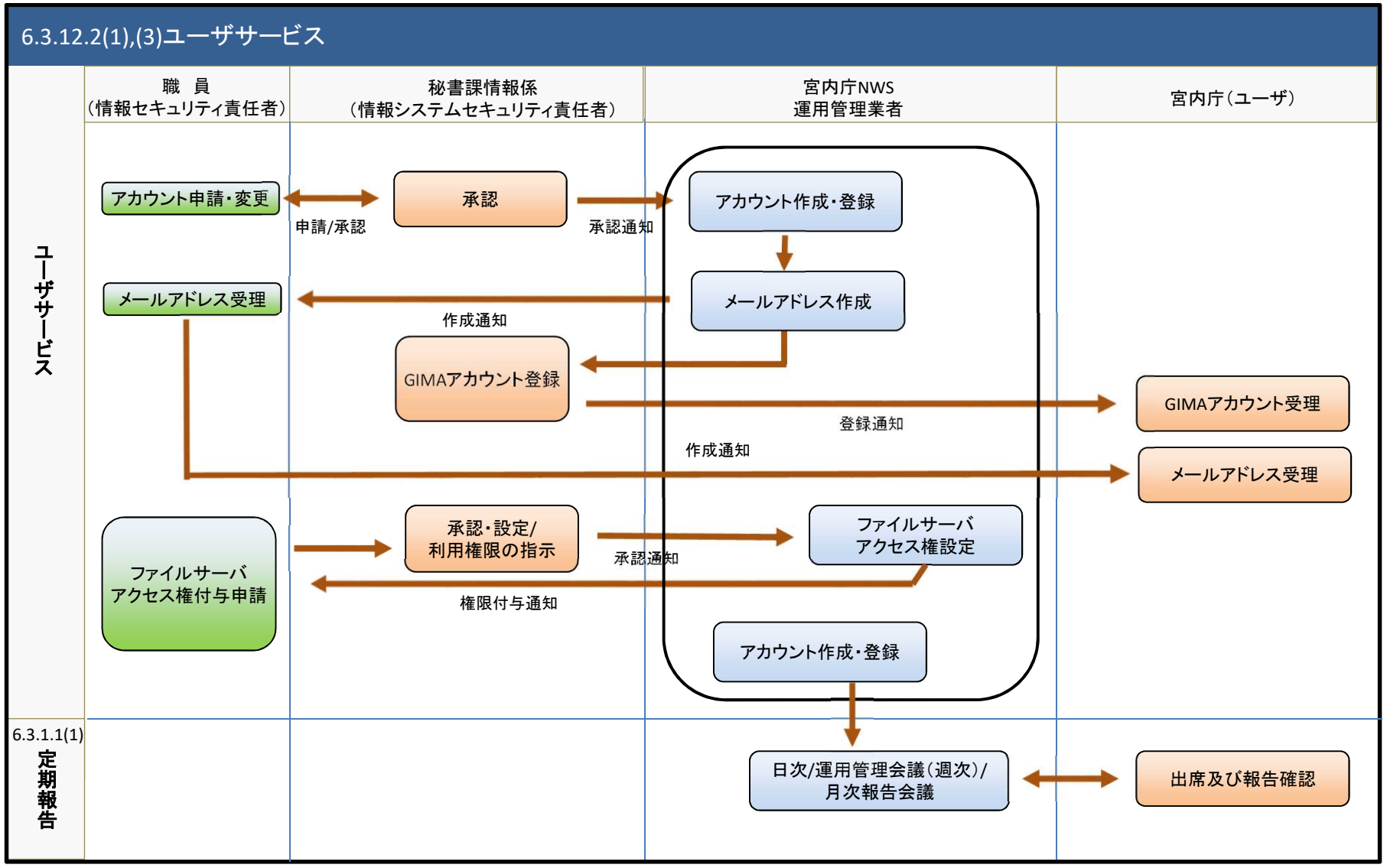
1.　現行宮内庁ネットワークシステムの運用管理支援業務に関する詳細な情報は，別途情報開示を行う。
なお，閲覧可能な資料は調達仕様書，各種運用ドキュメント及び各種報告書とする。
2.　詳細な実施方法等については，「3.4.運用管理業務の引継ぎ」により契約後速やかに説明する。
3.　１に示す資料のほか，情報セキュリティに関わる情報は，契約後速やかに開示する。



※項番は,「実施要項　別添1.宮内庁共通基盤システムの整備・保守及び宮内庁NWSの運用管理業務民間競争入札による調達仕様書」と同じ。

必須作業要件

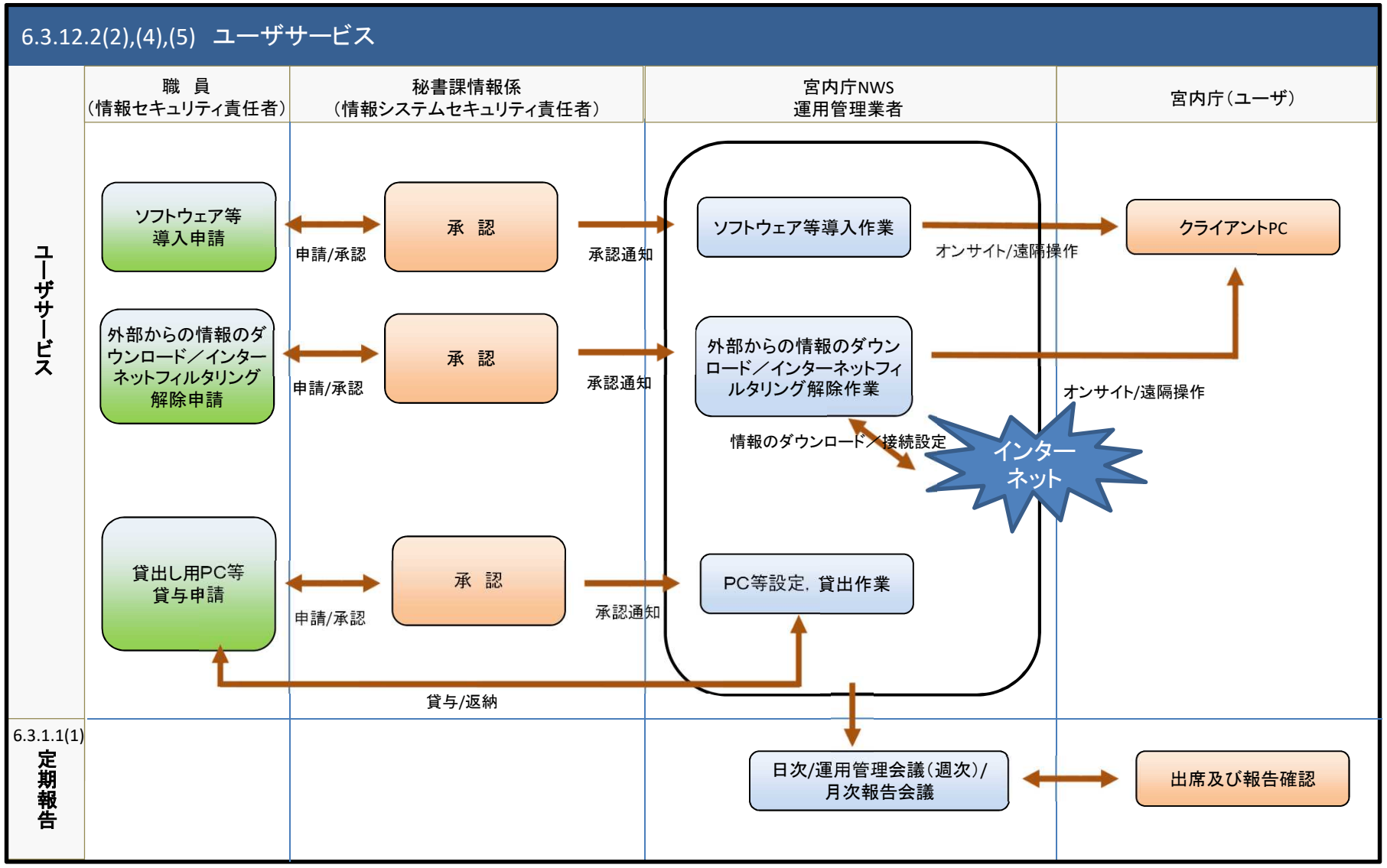
任意作業要件



※項番は,「実施要項　別添1.宮内庁共通基盤システムの整備・保守及び宮内庁NWSの運用管理業務民間競争入札による調達仕様書」と同じ。

必須作業要件

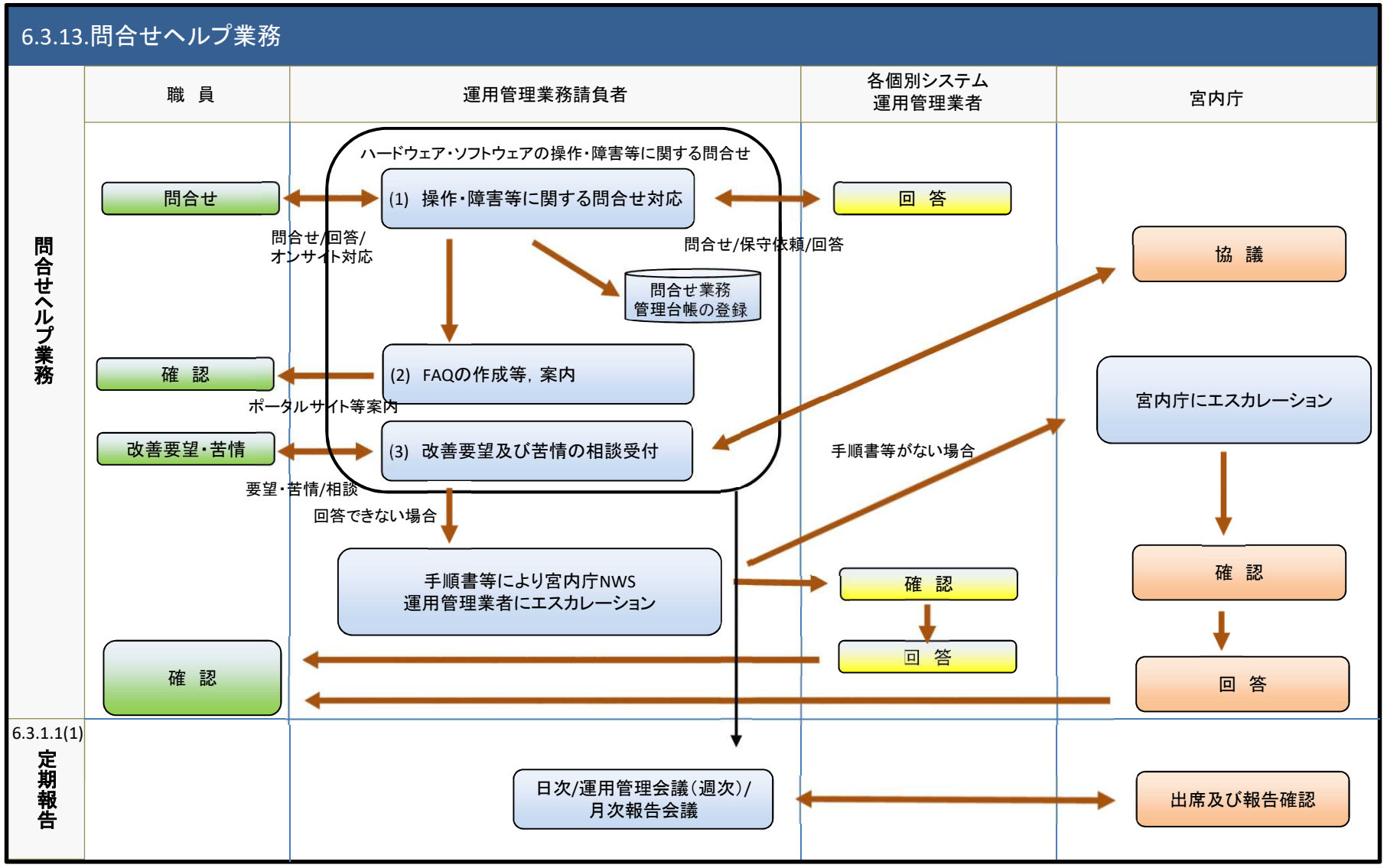
任意作業要件



※項番は，「実施要項　別添1.宮内庁共通基盤システムの整備・保守及び宮内庁NWSの運用管理業務民間競争入札による調達仕様書」と同じ。

必須作業要件

任意作業要件

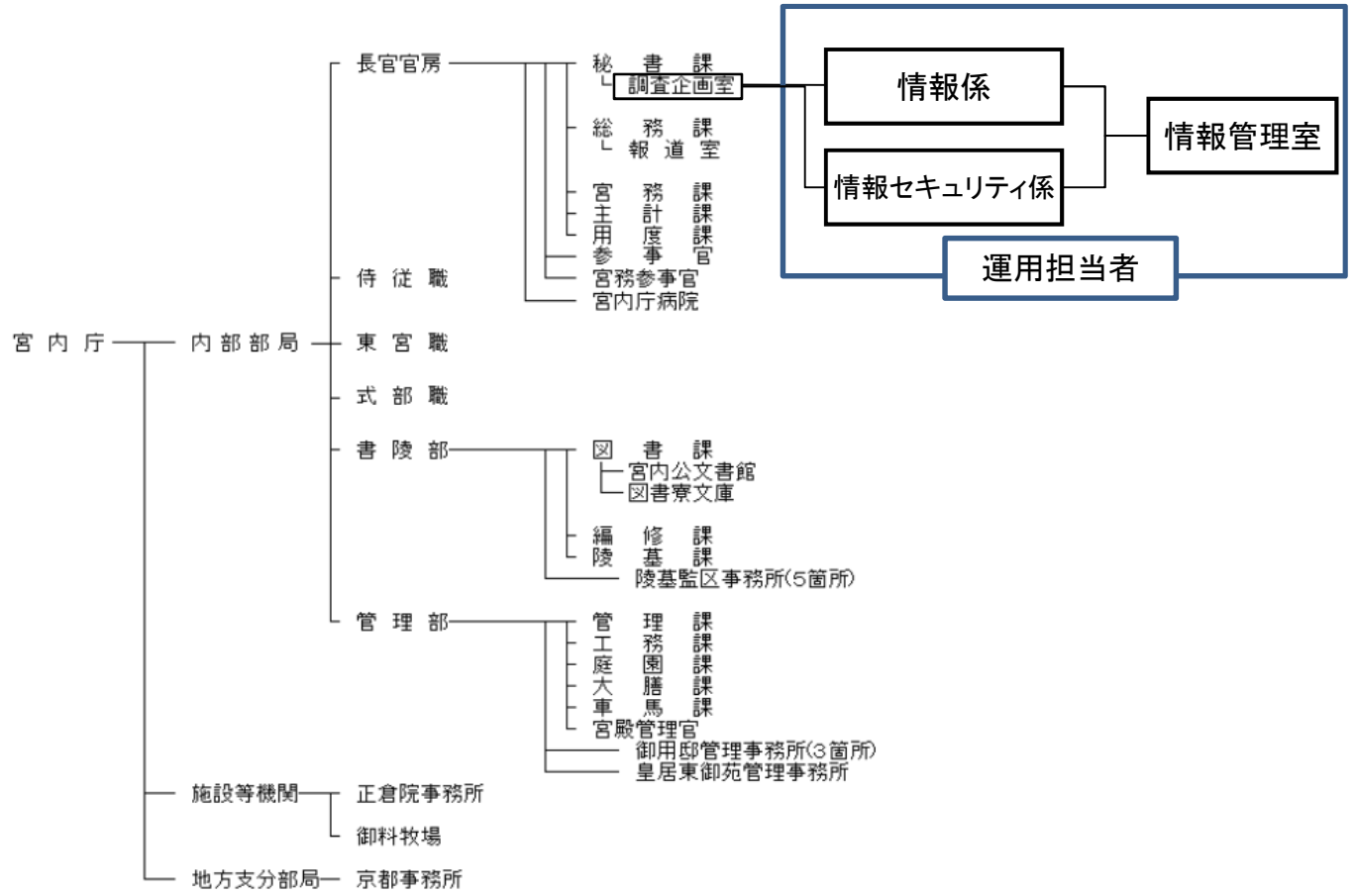


※項番は，「実施要項　別添1.宮内庁共通基盤システムの整備・保守及び宮内庁NWSの運用管理業務民間競争入札による調達仕様書」と同じ。

必須作業要件

任意作業要件

宮内庁組織図（平成31年2月1日現在）



【別紙３】

談合等不正行為に関する特約条項

（談合等の不正行為に係る解除）

第１条　甲は，本契約に関して，乙等が次の各号の一に該当するときは，本契約の全部又は一部を解除することができる。

(1)　公正取引委員会が，乙等又は乙等の代理人（乙又は乙の代理人が法人の場合にあっては，その役員又は使用人。以下同じ。）に対し，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。以下「独占禁止法」という。）第７条又は同法第８条の２（同法第８条第１号若しくは第２号に該当する行為の場合に限る。）の規定による排除措置命令を行ったとき，同法第７条の２第１項（同法第８条の３において読み替えて準用する場合を含む。）の規定による課徴金の納付命令を行ったとき，又は同法第７条の２第 18 項若しくは第 21 項の規定による課徴金の納付を命じない旨の通知を行ったとき。

(2)　乙等又は乙等の代理人が刑法（明治 40 年法律第 45 号）第 96 条の 6 若しくは同法第 198 条又は独占禁止法第 89 条第１項若しくは第 95 条第１項第１号の規定による刑の容疑により公訴を提起されたとき（乙の役員又はその使用人が当該公訴を提起されたときを含む。）。

２　乙等は，本契約に関して，乙等又は乙等の代理人が独占禁止法第７条の２第 18 項又は第 21 項の規定による通知を受けた場合は，速やかに当該通知文書の写しを甲に提出しなければならない。

（談合等の不正行為に係る違約金）

第２条　乙等は，本契約に関し，次の各号の一に該当するときは，甲が本契約の全部又は一部を解除するか否かにかかわらず，違約金（損害賠償金の予定）として，甲の請求に基づき，契約金額の 100 分の 10 に相当する額を甲が指定する期日までに支払わなければならない。

(1)　公正取引委員会が，乙等又は乙等の代理人に対し，独占禁止法第７条又は同法第８条の２（同法第８条第１号若しくは第２号に該当する行為の場合に限る。）の規定による排除措置命令を行い，当該排除措置命令が確定したとき。

(2)　公正取引委員会が，乙等又は乙等の代理人に対し，独占禁止法第７条の２第１項（同法第８条の３において読み替えて準用する場合を含む。）の規定による課徴金の納付命令を行い，当該納付命令が確定したとき。

(3)　公正取引委員会が，乙等又は乙等の代理人に対し，独占禁止法第７条の２第 18 項又は第 21 項の規定による課徴金の納付を命じない旨の通知を行ったとき。

(4)　乙等又は乙等の代理人が刑法第 96 条の６若しくは同法第 198 条又は独占禁止法第 89 条第１項若しくは第 95 条第１項第１号の規定による刑が確定したとき。

２　乙等は，前項第４号に規定する場合に該当し，かつ次の各号の一に該当するときは，前項の契約金額の 100 分の 10 に相当する額のほか，契約金額の 100 分の５に相当する額を違約金として甲が指定する期日までに支払わなければならない。

(1)　公正取引委員会が，乙等又は乙等の代理人に対し，独占禁止法第７条の２第１項（同法第８条の３において読み替えて準用する場合を含む）及び第７項の規定による納付命令を行い，当該納付命令が確定したとき。

(2)　当該刑の確定において，乙等が違反行為の首謀者であることが明らかになったとき。

(3)　乙等が甲に対し，独占禁止法等に抵触する行為を行っていない旨の誓約書を提出しているとき。

３　乙等は，契約の履行を理由として，前各項の違約金を免れることができない。

４　第１項及び第２項の規定は，甲に生じた実際の損害の額が違約金の額を超過する場合において，甲がその超過分の損害につき賠償を請求することを妨げない。

（違約金に関する遅延利息）

第３条　乙等が前条に規定する違約金を甲の指定する期日までに支払わないときは，乙等は当該期日を経過した日から支払をする日までの日数に応じ，年５パーセントの割合で計算した額の遅延利息を支払わなければならない。

【別紙４】

暴力団排除に関する特約条項

（属性要件に基づく契約解除）

第１条　甲(発注者をいう。以下同じ。)は，乙(契約の相手方をいう。以下同じ。)が次の各号のいずれかに該当すると認められるときは，何らの催告を要せず，本契約を解除することができる。

(1)　法人等(個人，法人又は団体をいう。)の役員等(個人である場合はその者，法人である場合は役員又は支店若しくは営業所(常時契約を締結する事務所をいう。)の代表者，団体である場合は代表者，理事等，その他経営に実質的に関与している者をいう。以下同じ。)が，暴力団(暴力団員による不当な行為の防止等に関する法律(平成３年法律第 77 号)第２条第２号に規定する暴力団をいう。以下同じ。)又は暴力団員(同法第２条第６号に規定する暴力団員をいう。以下同じ。)であるとき

(2)　役員等が，自己，自社若しくは第三者の不正の利益を図る目的又は第三者に損害を加える目的をもって，暴力団又は暴力団員を利用するなどしているとき

(3)　役員等が，暴力団又は暴力団員に対して，資金等を供給し，又は便宜を供与するなど直接的あるいは積極的に暴力団の維持，運営に協力し，若しくは関与しているとき

(4)　役員等が，暴力団又は暴力団員であることを知りながらこれを不当に利用するなどしているとき

(5)　役員等が，暴力団又は暴力団員と社会的に避難されるべき関係を有しているとき

（行為要件に基づく契約解除）

第２条　甲は，乙が自ら又は第三者を利用して次の各号のいずれかに該当する行為をした場合は，何らの催告を要せず，本契約を解除することができる。

(1)　暴力的な要求行為

(2)　法的な責任を超えた不当な要求行為

(3)　取引に関して脅迫的な言動をし，又は暴力を用いる行為

(4)　偽計又は威力を用いて甲又はその職員の業務を妨害する行為

(5)　その他前各号に準ずる行為

（表明確約）

第３条　乙は，前２条各号のいずれにも該当しないことを表明し，かつ，将来においても該当しないことを確約する。

２　乙は，前２条各号のいずれかに該当する者(以下「解除対象者」という。)を下請負人等(下請が数次にわたるときは，全ての下請負人を含む。)及び再受託者(再委託以降の全ての受託者を含む。)並びに乙，下請負人又は再受託者が当該契約に関して個別に契約する場合の当該契約の相手方をいう。以下同じ。)としないことを確約する。

（下請負契約等に関する契約解除）

第４条　乙は，契約後に下請負人等が解除対象者であることが判明したときは，直ちに当

該下請負人等との契約を解除し，又は下請負人等に対し契約を解除させるようにしなければならない。

２　甲は，乙が下請負人等が解除対象者であることを知りながら契約し，若しくは下請負人等の契約を承認したとき，又は不当な理由がないのに前項の規定に反して当該下請負人等との契約を解除せず，若しくは下請負人等に対し契約を解除させるための措置を講じないときは，本契約を解除することができる。

（損害賠償）

第５条　甲は，第１条，第２条及び前条第２項の規定により本契約を解除した場合は，これにより乙に生じた損害について，何ら賠償ないし補償することは要しない。

２　乙は，甲が第１条，第２条及び前条第２項の規定により本契約を解除した場合において，甲に損害が生じたときは，その損害を賠償するものとする。

（不当介入に関する通報・報告）

第６条　乙は，自ら又は下請負人等が，暴力団，暴力団員，暴力団関係者等の反社会的勢力から不当要求又は業務妨害等の不当介入(以下「不当介入」という。)を受けた場合は，これを拒否し，又は下請負人等をして，これを拒否させるとともに，速やかに不当介入の事実を甲に報告するとともに，警察への通報及び捜査上必要な協力を行うものとする。

【別紙５】

暴力団排除に関する誓約事項

当社(個人である場合は私，団体である場合は当団体)は，下記事項について入札書又は見積書の提出をもって誓約します。

この誓約が虚偽であり，又はこの誓約に反したことにより，当方が不利益を被ることとなっても，異議は一切申し立てません。

また，貴庁の求めに応じて当方の役員名簿(有価証券報告書に記載のもの(生年月日を含む。)ただし，有価証券報告書を作成していない場合は，役職名，氏名，性別及び生年月日の一覧表)等を提出すること,及び当該名簿に含まれる個人情報を警察に提供することについて同意します。

記

１　次のいずれにも該当しません。また，当該契約満了まで該当することはありません。

(1)　契約の相手方として不適当な者

ア　法人等(個人，法人又は団体をいう。)の役員等(個人である場合はその者，法人である場合は役員又は支店若しくは営業所(常時契約を締結する事務所をいう。)の代表者，団体である場合は代表者，理事等，その他経営に実質的に関与している者をいう。以下同じ。)が，暴力団(暴力団員による不当な行為の防止等に関する法律(平成３年法律第 77 号)第２条第２号に規定する暴力団をいう。以下同じ。)であるとき

イ　役員等が，自己，自社若しくは第三者の不正の利益を図る目的，又は第三者に損害を加える目的をもって，暴力団又は暴力団員を利用するなどしているとき

ウ　役員等が，暴力団又は暴力団員に対して，資金等を供給し，又は便宜を供与するなど直接的あるいは積極的に暴力団の維持，運営に協力し，若しくは関与しているとき

(2)　契約の相手方として不適当な行為をする者

ア　暴力的な要求行為を行う者

イ　法的な責任を超えた不当な要求行為を行う者

ウ　取引に関して脅迫的な言動をし，又は暴力を用いる行為を行う者

エ　偽計又は威力を用いて甲又はその職員の業務を妨害する行為を行う者

オ　その他前各号に準ずる行為を行う者

２　暴力団関係業者を下請負又は再委託の相手方としません。

３　下請負人等(下請負人(一次下請以降の全ての下請負人を含む。)及び再受託者(再委託以降の全ての受託者を含む。)並びに自己，下請負人又は再受託者が当該契約に関して個別に締結する場合の当該契約の相手方をいう。)が暴力団関係業者であることが判明したときは，当該契約を解除するため必要な措置を講じます。

４　暴力団員等による不当介入を受けた場合，又は下請負人等が暴力団員等による不当介入を受けたことを知った場合は，警察への通報及び捜査上必要な協力を行うとともに，発注元の契約担当官等へ報告を行います。

宮内庁 NWS の運用管理業務に関する満足度アンケート調査

このアンケートは，宮内庁 NWS の運用管理業務（ヘルプデスク）について，確保されるべきサービスの質を検討するため，職員利用者を対象に利用満足度を調査するものです。

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

１　お問合せから回答までに要した時間について満足されましたか。
□　満足　　□　やや満足　　□　普通　　□　やや不満　　□　不満

２　回答又は手順に対する説明の分かりやすさについて満足されましたか。
□　満足　　□　やや満足　　□　普通　　□　やや不満　　□　不満

３　回答又は手順に対する結果の正確性について満足されましたか。
□　満足　　□　やや満足　　□　普通　　□　やや不満　　□　不満

４　担当者の対応（言葉遣い，親切さ，丁寧さ等）について満足されましたか。
□　満足　　□　やや満足　　□　普通　　□　やや不満　　□　不満

＜ご意見等＞

ご協力ありがとうございました。

【別添１】

宮内庁共通基盤システムの整備・保守及び宮内庁 NWS の運用管理業務に係る民間競争入札

調達仕様書（案）

宮内庁

令和元年〇月

＜一般的な略語　アルファベット順＞

○ AD…Active Directory
○ ARP…Address Resolution Protocol
○ BCP…Business Continuity Plan
○ BPDU…Bridge Protocol Data Unit
○ CAD…Computer Aided Design
○ CAL…Client Access License
○ CCRA…Common Criteria Recognition Arrangement
○ CIO…Chief Information Officer
○ CIS…Common Infrastructure System
○ CISSP…Certified Information Systems Security Professional
○ CLI…Command Line Interface
○ CMMI…Capability Maturity Model Integration
○ CoS…Class of Service
○ CPU…Central Processing Unit
○ CSV…Cluster Shared Volume
○ DKIM…Domain Keys Identified Mail
○ DMARC…Domain-based Message Authentication，Reporting & Conformance
○ DMZ…DeMilitarized Zone
○ DSCP…Differentiated Services Code Point
○ DR…Disaster Recovery
○ EAL…Evaluation Assurance Level
○ FAQ…Frequently Asked Questions
○ FQDN…Fully Qualified Domain Name
○ GEPS…Government Electronic Procurement System
○ GUI…Graphical User Interface
○ HDD…Hard Disk Drive
○ HLS…High Level Structure
○ HTTPS…Hypertext Transfer Protocol Secure
○ IC…Integrated Circuit
○ IDM…Identity Manager
○ IEC…International Electrotechnical Commission
○ IP…Internet Protocol
○ IPA…Information-technology Promotion Agency，　Japan
○ IP-VPN…Internet Protocol-Virtual Private Network
○ ISO…International Organization for Standardization
○ ISP…Internet Service Provider
○ ITIL…Information Technology Infrastructure Library
○ JC3…Japan Cybercrime Control Center
○ JEITA…Japan Electronics and Information Technology Industries Association

○ JIS…Japan Industrial Standard
○ JPCERT/CC…Japan Computer Emergency Response Team Coordination Center
○ JVN…Japan Vulnerability Notes
○ KMS…Key Management Service
○ KVM…Keyboard Video Mouse switch
○ LAN…Local Area Network
○ LED…Light Emitting Diode
○ MSS…Management System Standards
○ NISC…National center of Incident readiness and Strategy for Cybersecurity
○ NOC…Network Operations Center
○ NTP…Network Time Protocol
○ NW…Net Work
○ NWS…Net Work System
○ ODB…Official information system total management Database
○ OS…Operating System
○ OSI…Open Systems Interconnection
○ OSPF…Open Shortest Path First
○ PC…Personal Computer
○ PCAP…Packet Capture
○ PDCA…Plan, Do, Check, Action
○ PDSA…Plan, Do, Study, Action
○ PDU…Professional Development Unit
○ PMBOK…Project Management Body of Knowledge
○ PMI…Project Management Institute
○ PMP…Project Management Professional
○ PPTP…Point-to-Point Tunneling Protocol
○ SaaS…Software as a Service
○ SAC…Semi-Annual Channel
○ SLA…Service Level Agreement
○ SMTP…Simple Mail Transfer Protocol
○ SOC…Security Operation Center
○ SPF…Sender Policy Framework
○ RFC…Request For Comments
○ RMON…Remote network MONitoring
○ TCP…Transmission Control Protocol
○ TLS…Transport Layer Security
○ TTL…Time To Live
○ UDP…User Datagram Protocol
○ UEBA…User and Entity Behavior Analytics
○ UPS…Uninterruptible Power Supply

○ URL…Uniform Resource Locator
○ UTP…Unshielded Twist Pair cable
○ VESA…Video Electronics Standards Association
○ WaaS…Windows as a Service
○ WAN…Wide Area Network
○ WBS…Work Breakdown Structure
○ WSUS…Windows Sever Update Service

【資料一覧】

□　別紙 1「資料閲覧願い」及び「機密保持に関する誓約書」

□　別紙 2「宮内庁ＮＷ設置拠点・設置場所等」

□　別紙 3「各フロア配線，必要ポート数状況」

□　別紙 4「本調達機器及び各事業者の役割範囲」

□　別紙 5「保守・運用フロー」

1. 一般的事項

1.1.件名

宮内庁共通基盤システムの整備・保守及び宮内庁 NWS の運用管理業務に係る民間競争入札

1.2.適用範囲

本調達仕様書（案）は，宮内庁 LAN の基盤サーバ群の構築，これらが正常に機能するための周辺機器や付属品を含めた物の搬入，ケーブル敷設，据付，設定，調整，動作確認，テスト（単体・結合・統合テストを含む。ただし，受入テストは支援まで。），保守業務及び運用管理業務に係る受託者が実施する全ての事項に適用する。

1.3.用語の定義

本調達における技術上の基準については，工業標準化法第 67 条に従い，日本工業規格（以下「JIS」という。）を尊重する。また，マネジメントに関する用語は，原則として，ISO マネジメントシステム規格（ISO MSS）の MSS の上位構造（HLS），共通テキスト（要求事項）及び共通用語・定義に従うものとする。ただし，運用管理業務に係るサービスマネジメントの用語は JIS Q 20000-1：2012 (ISO/IEC 20000-1：2011)又は ITIL2011，事業継続及び社会セキュリティに係る用語は JIS Q 22300：2013(ISO 22300：2012)，情報セキュリティに関する用語は JIS Q 27001：2014 (ISO/IEC 27001：2013)に従うものとする。JIS 等に定義されている用語であっても，本調達において特に注意すべき用語については抜粋し，次の表の中に記載している。

なお，調達に関する用語のうち，下記の表中以外の用語については，次の政府電子調達(GEPS)の用語集に従う。 https://www.geps.go.jp/glossary/nyusatsu

NO.	用語	定義
1	本業務	「宮内庁共通基盤システムの整備・保守及び宮内庁 NWS の運用管理業務に係る民間競争入札による調達仕様書（案）」で規定された調達業務。
2	本整備業務	本調達仕様書（案）の構築及び整備に係る業務のこと。
3	本保守業務	本調達仕様書（案）の保守に係る業務のこと。
4	本運用管理業務	本調達仕様書（案）の運用管理に係る業務のこと。
5	甲	宮内庁のこと。
6	甲担当者	甲の長官官房秘書課調査企画室の職員。
7	ユーザ	宮内庁職員のこと。
8	応札者	本調達の競争入札に対し，応札する意思がある者。
9	乙	本調達の競争入札の開札の結果，落札し，宮内庁の支出負担行為担当官と契約した者で受託者のこと。
10	ODB	政府情報システム管理データベース（Official information system total management Database）の略称。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，総務省において整備及び管理し，各府省の用に供するデータベースのこと。
11	情報システム ID	ODB に登録された情報システム毎にユニークに付与される管理用 ID のこと。

12	製造事業者等	製造物責任法（平成 6 年法律第 85 号）の第 2 条第 3 項に従う。
13	プロジェクト	PMI が発行するプロジェクトマネジメント知識体系ガイド（PMBOK ガイド）の最新版でのプロジェクトの定義に従う。 なお，プロジェクトに関係するハイレベルな概念については，PMBOK ガイドや他の規格をまとめた ISO 21500 と可能な限り整合性を図る。
14	本プロジェクト	「宮内庁共通基盤システムの整備・保守及び宮内庁 NWS の運用管理業務に係る民間競争入札による調達仕様書」の「1.2.背景と目的」に示した目的を達成するために遂行されるプロジェクト全体のこと。 なお，計画的な事前試験のことを「テスト」という。
15	休日	行政機関の休日に関する法律（昭和 63 年法律第 91 号）第 1 条第 1 項各号に掲げる日をいう。
16	IT ガバナンス	JIS Q 38500：2015(ISO/IEC 38500)の定義に従い，本調達でも「組織の IT の現在及び将来の利用を指示し，管理するシステム。IT ガバナンスは，組織を支援するために IT の利用を評価すること及び指示すること，並びに計画を遂行するためにこの IT 利用をモニタすることに関係する。これには組織における IT の利用に関する戦略及び方針を含む。」とする。
17	情報セキュリティ	JIS Q 27000：2014(ISO/IEC 27000)の定義に従い，本調達でも「情報の機密性，完全性及び可用性を維持すること。」とする。
18	情報セキュリティガバナンス	JIS Q 27014：2015 (ISO/IEC 27014：2013)の定義に従い，本調達でも「組織の情報セキュリティ活動を指導し，管理するシステム。」とする。
19	情報セキュリティインシデント	JIS Q 27000：2014 (ISO/IEC 27000) の定義に従い，本調達でも「望ましくない単独若しくは一連の情報セキュリティ事象，又は予期しない単独若しくは一連の情報セキュリティ事象であって，事業運営を危うくする確率及び情報セキュリティを脅かす確率が高いもの。」とする。また，情報セキュリティインシデント管理とは，情報セキュリティインシデントを検出し，報告し，評価し，応対し，対処し，更にそこから学習するためのプロセスのことを指す。
20	情報セキュリティインシデント管理	JIS Q 27000：2014 (ISO/IEC 27000) の定義に従い，本調達でも「情報セキュリティインシデントを検出し，報告し，評価し，応対し，対処し，更にそこから学習するためのプロセスのことを指す。」とする。
21	資源	JIS Q 38500：2015(ISO/IEC 38500 :2008)の定義に従い，本調達でも「人々，手順，ソフトウェア，情報，装置，消耗品，基盤，資金及び運用ファンド，並びに時間。」とする。
22	リスク	JIS Q 27000：2014 (ISO/IEC 27000) の定義に従い，本調達でも「目的に対する不確かさの影響。」とする。 なお，リスクがつく用語については，全て JIS Q 27000：2014 (ISO/IEC 27000) の定義に従う。
23	リスクマネジメント	JIS Q 38500：2015(ISO/IEC 38500 :2008)の定義に従い，本調達でも「リスクに関して組織を指揮し管理する調整された活動」とする。

24	ステークホルダー	JIS Q 38500：2015(ISO/IEC 38500:2008)の定義では「意思決定又は活動に影響を与え得る，影響され得る又は影響されると認知している，あらゆる個人，団体，又は組織。」となっているが，本調達では，宮内庁 NWS に間接的又は直接的に関与し，影響を与える又は受ける個人又は法人・団体のこととする。
25	関東エリア	宮内庁本庁，赤坂御用地内，多摩陵墓監区事務所，那須御用邸管理事務所，須崎御用邸管理事務所，葉山御用邸管理事務所，御料牧場等・・・ユーザ数 約 950 名。
26	関西エリア	桃山陵墓監区事務所，月輪陵墓監区事務所，畝傍陵墓監区事務所，古市陵墓監区事務所，京都事務所，正倉院事務所・・・ユーザ数 約 250 名。
27	端末	パーソナルコンピュータのこと。
28	一般事務用端末	平成 28 年度「パーソナルコンピュータ及びサーバ等の賃貸借及びサーバ等保守」で調達した一般事務用の端末であり，現行の宮内庁 NWS に含まれる。ただし，平成 30 年度「パーソナルコンピュータの購入及び構築」で調達した一般事務用の端末は「追加一般事務用端末」という。ODB 上の情報システム ID は，宮内庁 NWS と同一。
29	CAD 用端末	平成 28 年度「パーソナルコンピュータ及びサーバ等の賃貸借及びサーバ等保守」で調達した CAD 用の端末であり，現行の宮内庁 NWS に含まれる。ODB 上の情報システム ID は，宮内庁 NWS と同一。
30	参観受付システム用端末	平成 27 年度「宮内庁公開システムの賃貸借及び保守運用業務」で調達し，参観受付システムで使用しているデスクトップ端末（9 式）を指す（「別紙 2 宮内庁 NW 設置拠点・設置場所等」を参照）。
31	統合運用管理端末	平成 26 年度「宮内庁情報ネットワークシステム機器の賃貸借及び保守」で調達し，宮内庁情報ネットワークシステムで使用しているデスクトップ端末（2 式）及び本調達の端末を指す（「別紙 2 宮内庁 NW 設置拠点・設置場所等」を参照）。
32	宝物管理システム用端末	平成 26 年度「正倉院宝物公開管理システム機器の賃貸借及び保守等」で調達し，正倉院宝物管理公開システムで使用しているデスクトップ端末（2 式）を指す（「別紙 2 宮内庁 NW 設置拠点・設置場所等」を参照）。
33	タブレット端末	タブレット PC(10 式）を指す（「別紙 2 宮内庁 NW 設置拠点・設置場所等」を参照)。
34	クライアント端末	本表の NO.28 から 33 の端末を指す。
35	宮内庁 NWS	宮内庁情報ネットワークシステム全体の略。甲が業務を遂行するために使用する，甲の各拠点等に設置された情報通信機器等とそれらを繋ぐネットワークにより構成され，宮内庁 LAN，宮内庁 WAN とインターネット接続回線サービス，グループウェア，クライアント端末及びプリンタに大きく分類される。また，宮内庁 NWS の情報セキュリティ対策の強化として追加で調達を行った機器，ソフトウェア及びサービスも含む。ODB 上の情報システム ID は，A000760。
36	宮内庁 LAN	宮内庁構内ネットワークの略。皇居内に設置された構内ネットワーク（以

		下「本庁 LAN」という。），皇居外に所在する宮内庁の各拠点それぞれに設置された構内ネットワーク（以下「拠点 LAN」という。）の総称。ODB 上の情報システム ID は，宮内庁 NWS と同一。
37	宮内庁 WAN	本庁 LAN 及び各拠点 LAN を IP－VPN 回線で相互に接続し統合したネットワーク。ODB 上の情報システム ID は，宮内庁 NWS と同一。
38	端末資産管理システム	平成 28 年度「パーソナルコンピュータ及びサーバ等の賃貸借及びサーバ等保守」で調達したシステム全体を指し，現行の宮内庁 NWS に含まれる。ODB 上の情報システム ID は，宮内庁 NWS と同一。
39	端末賃貸借保守事業者	平成 28 年度「パーソナルコンピュータ及びサーバ等の賃貸借及びサーバ等保守」の受注事業者のこと。
40	プリンタ等調達各事業者	平成 28 年度「パソコン用プリンタ（インクジェットカラー）の購入」，「パソコン用プリンタ（モノクロ）の賃貸借及び保守」，「カラー複合機賃貸借」及び「CAD 用プリンタの賃貸借及び保守」の各落札事業者
41	出力機器管理システム	宮内庁ＮＷＳの仮想サーバ内で稼働している平成 25 年度に調達したカラープリンタの出力ログを取得するためのシステム。
42	現行宮内庁 LAN	平成 26 年度「宮内庁情報ネットワークシステム機器の賃貸借及び保守」で調達したシステム全体を指し，現行の宮内庁 NWS に含まれる。ODB 上の情報システム ID は，宮内庁 NWS と同一。
43	現行宮内庁 LAN 賃貸借保守事業者	平成 26 年度「宮内庁情報ネットワークシステム機器の賃貸借及び保守」の受注事業者のこと。
44	現行宮内庁 WAN サービス	平成 26 年度「宮内庁ＷＡＮの通信回線サービスの更新に係る調達仕様書」で調達した通信回線サービスのこと。
45	現行宮内庁インターネット接続サービス	平成 27 年度「インターネット接続回線サービス調達仕様書」で調達したインターネット接続回線サービスのこと。
46	GW システム	平成 29 年度「グループウェアシステムの賃貸借及び保守」で調達したシステム全体を指し，現行の宮内庁 NWS に含まれる。ODB 上の情報システム ID は，宮内庁 NWS と同一。
47	標的型攻撃対策システム	平成 29 年度「標的型攻撃対策システムの賃貸借及び保守」で調達したシステム全体を指し，現行の宮内庁 NWS の情報セキュリティ対策の強化に含まれる。ODB 上の情報システム ID は，宮内庁 NWS と同一。
48	WEB 無害化システム	平成 29 年度「WEB 閲覧の無害化機能賃貸借及び保守」で調達したシステム全体を指し，現行の宮内庁 NWS の情報セキュリティ対策の強化に含まれる。ODB 上の情報システム ID は，宮内庁 NWS と同一。
49	ファイル自動暗号化システム	平成 29 年度「電子ファイルの暗号化及びアクセス制御機能の賃貸借及び保守」で調達したシステム全体を指し，現行の宮内庁 NWS の情報セキュリティ対策の強化に含まれる。ODB 上の情報システム ID は，宮内庁 NWS と同一。
50	宮内庁公開システム	平成 27 年度「宮内庁公開システム政府共通プラットフォームへの移行等業務」で総務省が構築及び運用保守を行っている政府共通プラットフ

		ォーム（以下「政府共通 PF」という。）上に移行した皇居等参観受付システム，情報公開システム，ホームページ公開システムの 3 システムの全体を指す。ODB 上の情報システム ID は，A000771。
51	正倉院宝物公開管理システム	平成 26 年度「正倉院宝物公開管理システム機器の賃貸借及び保守等」で調達したシステム全体を指す。ODB 上の情報システム ID は，A000793。
52	書陵部所蔵資料目録・画像公開システム	平成 29 年度「図書寮文庫所蔵資料目録・画像公開システムの賃貸借及び保守」で調達したシステム全体を指す。ODB 上の情報システム ID は，A016231。
53	CAD システム	平成 29 年度「CAD システムの賃貸借及び保守」で調達したシステム全体を指す。ODB 上の情報システム ID は，A000782。
54	個別システム	ODB 上の情報システム ID が，宮内庁 NWS のシステム ID と異なるシステム又はシステム ID が無いシステムの全体を指す。
55	関係事業者	本表の No.35～54 での各現行システムに関係する事業者の全体を指す。
56	運用管理支援事業者	平成 31 年度「宮内庁ネットワークシステムの運用管理支援業務」の受託事業者で，宮内庁に常駐している（夜間，休日を除く。）。
57	宮内庁統合 NW	平成 31 年度「宮内庁統合ネットワーク回線・機器に係る供給（設計・構築，テスト，移行，運用等）業務一式」にて調達する予定。ODB 上の情報システム ID は，宮内庁 NWS と同一。
58	宮内庁統合 NW 受託者	平成 31 年度「宮内庁統合ネットワーク回線・機器に係る供給（設計・構築，テスト，移行，運用等）業務一式」の受託事業者のこと。
59	電気通信	電気通信事業法第 2 条の定義に従い，本調達においても「電気通信」とは，有線，無線その他の電磁的方式により，符号，音響又は影像を送り，伝え，又は受けることをいう。
60	電気通信設備	電気通信事業法第 2 条の定義に従い，本調達においても「電気通信設備」とは，電気通信を行うための機械，器具，線路その他の電気的設備をいう。
61	電気通信回線設備	電気通信事業法第 9 条の定義に従い，本調達においても「電気通信回線設備」とは，送信の場所と受信の場所との間を接続する伝送路設備及びこれと一体として設置される交換設備並びにこれらの附属設備をいう。
62	クラウドサービス	事業者によって定義されたインタフェースを用いた，拡張性，柔軟性を持つ共用可能な物理的又は仮想的なリソースにネットワーク経由でアクセスするモデルを通じて提供され，ユーザによって自由にリソースの設定・管理が可能なサービスであって，情報セキュリティに関する十分な条件設定の余地があるもの。
63	クラウドサービス事業者	クラウドサービスを提供する事業者又はクラウドサービスを用いて政府機関の情報システムを開発・運用する事業者
64	クラウドサービスプロバイダ	クラウドサービス事業者のうち，クラウドサービスを提供する事業者。
65	クラウドサービス	クラウドサービス事業者のうち，クラウドサービスを用いて政府機関の

	ブローカ	情報システムを開発・構築等する事業者。※本調達においては乙に該当する。
66	SaaS	アプリケーションやデータベースをサービスとして提供するクラウドサービス。
67	クラウド環境	クラウドサービス上で構築した情報システムが動作する環境。
68	オンプレミス	情報システムをユーザ自身が管理する設備内に導入，設置して運用する利用形態。また，その情報システムは，そのユーザにより占有され利用されることが可能。
69	運用コスト	「政府情報システムの整備及び管理に関する標準ガイドライン」（平成26年12月3日第58回各府省情報化統括責任者（CIO）連絡会議決定）の最新版（以下「管理標準ガイドライン」という。）で定義されている情報システムの経費区分のうち，運用等経費のことを指す。運用等経費には，システム運用経費，業務運用支援経費，操作研修等経費，ヘルプデスク経費，コールセンター経費，アプリケーション保守経費，ハードウェア保守経費，ソフトウェア保守経費，監査経費，情報セキュリティ検査経費，ハードウェア借料，ソフトウェア借料，サービス利用料，通信回線料，施設利用等経費，その他運用等経費を含む。
70	インシデント	JIS Q 22300：2013(ISO 22300：2012)では「中断・阻害，損失，緊急事態又は危機になり得る又はそれらを引き起こし得る状況。」と定義されている。また，JIS Q 20000-1：2012 (ISO/IEC 20000-1：2011)では「サービスに対する計画外の中断，サービスの品質の低下，又は顧客へのサービスにまだ影響していない事象。」と定義されている。本調達仕様書（案）では，それらの定義を包含したものをインシデントと定義する。 また，インシデント管理は，通常のサービス運用にできるだけ早く回復させ，業務への悪影響を最小化することを目的とする。
71	インシデント対応	JIS Q 22300：2013(ISO 22300：2012)の定義に従い，本調達でも「差し迫ったハザードの原因を食い止めるため，及び不安定又は中断・阻害を引き起こす可能性のある事象の結果を軽減し，正常な状況に復旧するために講じる措置。」とする。
72	問題	JIS Q 20000-1：2012 (ISO/IEC 20000-1：2011) の定義に従い，本調達でも「一つ以上のインシデントの根本原因。問題の記録が作成された時点では，通常はその根本原因は不明であり，問題管理プロセスは更なる調査に対して責任をもつ。」とする。また，問題管理は，インシデントの根本原因の除去とワークアラウンドの提供によって，インシデント発生による業務への悪影響を最小化することを目的とする。
73	既知の誤り	JIS Q 20000-1：2012 (ISO/IEC 20000-1：2011) の定義に従い，本調達でも「根本原因が特定されているか，若しくは回避策によってサービスへの影響を低減又は除去する方法がある問題。」とする。
74	アクセス制御	JIS Q 27000：2014 (ISO/IEC 27000) の定義に従い，本調達でも「資産へのアクセスが，事業上及びセキュリティの要求事項に基づいて認可及

		び制限されることを確実にする手段。」とする。
75	攻撃	JIS Q 27000：2014 (ISO/IEC 27000) の定義に従い，本調達でも「資産の破壊，暴露，改ざん，無効化，盗用，又は認可されていないアクセス若しくは使用の試み。」とする。
76	可用性	JIS Q 27000：2014 (ISO/IEC 27000) の定義に従い，本調達でも「認可されたエンティティが要求したときに，アクセス及び使用が可能である特性。」とする。 なお，エンティティは，“実体”，“主体”などともいう。情報セキュリティの文脈においては，情報を使用する組織及び人，情報を扱う設備，ソフトウェア及び物理的媒体などを意味する。
77	機密性	JIS Q 27000：2014 (ISO/IEC 27000) の定義に従い，本調達でも「認可されていない個人，エンティティ又はプロセスに対して，情報を使用させず，また，開示しない特性。」とする。
78	完全性	JIS Q 27000：2014 (ISO/IEC 27000) の定義に従い，本調達でも「正確さ及び完全さの特性。」とする。
79	信頼性	JIS Q 27000：2014 (ISO/IEC 27000) の定義に従い，本調達でも「意図する行動と結果とが一貫しているという特性」とする。
80	有効性	JIS Q 27000：2014 (ISO/IEC 27000) の定義に従い，本調達でも「計画した活動を実行し，計画した結果を達成した程度。」とする。
81	要求事項	JIS Q 27000：2014 (ISO/IEC 27000) の定義に従い，本調達でも「明示されている，通常暗黙のうちに了解されている又は義務として要求されている，ニーズ又は期待。」とする。
82	適合	JIS Q 27000：2014 (ISO/IEC 27000) の定義に従い，本調達でも「要求事項を満たしていること」とする。
83	不適合	JIS Q 27000：2014 (ISO/IEC 27000) の定義に従い，本調達でも「要求事項を満たしていないこと」とする。
84	脅威	JIS Q 27000：2014 (ISO/IEC 27000) の定義に従い，本調達でも「システム又は組織に損害を与える可能性がある，望ましくないインシデントの潜在的な原因。」とする。
85	脆弱性	JIS Q 27000：2014 (ISO/IEC 27000) の定義に従い，本調達でも「一つ以上の脅威によって付け込まれる可能性のある，資産又は管理策の弱点。」とする。
86	妥当性確認	JIS Q 27000：2014 (ISO/IEC 27000) の定義に従い，本調達でも「客観的証拠を提示することによって，特定の意図された用途又は適用に関する要求事項が満たされていることを確認すること。」とする。
87	検証	JIS Q 27000：2014 (ISO/IEC 27000) の定義に従い，本調達でも「客観的証拠を提示することによって，規定要求事項が満たされていることを確認すること。」とする。
88	ISP	インターネット接続の電気通信役務を 提供する組織のこと。

89	NOC	通信ネットワークを管理，運用するために設けられた施設のこと。
90	SOC	SOC とは，標的型攻撃対策装置などの機器のセキュリティログを一元的に監視，分析し対策及び通知を行う組織（セキュリティオペレーションセンタ）のこと。
91	特権 ID	情報システムの維持・管理のために利用する ID であり，情報システムの利用目的（業務目的）以外で利用する全ての ID。
92	政府共通ネットワーク	政府機関内における情報の円滑な流通，情報共有等を図るため，全府省，独立行政法人，日本銀行及び国会等のほか，府省共通システム，総合行政ネットワーク（LGWAN）を相互に接続する政府専用のネットワーク基盤（以下「政府共通 NW」という。）のこと。
93	センドバック保守	故障した製品を製造事業者等や販売店の窓口に送ると，修理若しくは代替品と交換して送り返してくれるサービスのこと。
94	先出しセンドバック	先に販売側が(故障の連絡を受けて)代替品を発送し，利用者が代替品と入れ替わりに故障品を製造事業者等へ送り返す方式のこと。
95	後出しセンドバック	先に利用者が故障品を発送し，販売側がこれを修理・交換して送り返す方式のこと。
96	オンサイト保守	IT 機器などの故障の際に，現地に出張して修理を行うサービスのこと。
97	スポット保守	IT 機器などの保証期間が終了，保守契約などを結んでいない顧客に対して，求めに応じて提供する保守サービス。作業の内容に応じてその都度，代金を請求・精算する。

1.4.背景と目的

甲は，行政事務を行う上で必要となる文書作成，情報伝達等の基盤として宮内庁 NWS をこれまで整備し，運用を行ってきた。宮内庁 NWS は，宮内庁 LAN と宮内庁 WAN とで構成されており，一府省庁一ネットワークの体制になっている。また，インターネット接続回線サービスを本庁だけに集約し，各拠点は，WAN を介してインターネット接続を行っている。

甲は，「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（平成 30 年 6 月 15 日　閣議決定）（以下「創造宣言」という。）」において「平成 30 年度までにシステム数の半減（平成 24 年度（1450 システム）比），平成 33 年度を目途に運用コストの３割削減（平成 25 年度（約 4000 億円）比）を目指すため，引き続き達成に向けた取組を着実に実施」すること等が目標として掲げられていることを踏まえ，これまで，宮内庁本庁サーバ及び地方サーバ（正倉院事務所，御料牧場，京都事務所に設置されている）（以下「地方サーバ」という。）の集約化を始め，情報システム構成及び運用の効率化・合理化を図るとともに，安全性，信頼性及び可用性並びに柔軟性が確保されたネットワーク環境を構築するにあたり，機器・ソフトウェア等を刷新し，ネットワークの再構築と高速化を推進してきた。

また，「デジタル・ガバメント実行計画（平成 30 年 7 月 20 日改定　デジタル・ガバメント閣僚会議決定）」においてマネジメント及びプロセスの強化として，政府情報システム改革の着実な推進，情報利活用と情報セキュリティの一体的推進，標準ガイドライン群の充実・拡充・定着が求められている。宮内庁においては，デジタル・ガバメント実行計画に基づき，「宮内庁デジタル・ガバメント中長期計画（平成 30 年 6 月 22 日　行政情報化推進委員会決定）」を策定した。

本調達では，これまでのそれらの取組を踏まえ，次の事項を更に推進し，宮内庁デジタル・ガバメント中長期計画の着実な実施を目的とする。

(1) 情報セキュリティ対策の更なる向上
(2) 情報システムの運用コストの削減
(3) 情報システムにおけるユーザの利便性の向上
(4) 情報システム構成及び運用の効率化・合理化
(5) 業務継続性の向上

現行の宮内庁 NWS は構築・保守業務と運用管理業務の調達を分けてきたが，日常的に利用する基盤サーバ群の運用管理業務と次期宮内庁 NWS の中核となる宮内庁共通基盤システム（以下「宮内庁 CIS」という。）の構築・保守業務の一体的な作業による効率化だけでなく，情報セキュリティインシデント及び情報システム障害対応の迅速化によって，利用者であるユーザの業務への影響，とりわけ情報システムを正常に利用できないことによる業務遅延などを最小化し，構築・保守業務と運用管理業務を一体的に行い，より効果的な IT マネジメントを図ることを目指す。そのため，本調達では，宮内庁 CIS の構築・保守だけでなく，競争の導入による公共サービスの改革に関する法律（以下「公共サービス改革法」という。）及び公共サービス改革基本方針の趣旨・目的に基づいた次期宮内庁 NWS の運用管理業務の調達を含めるため，官民競争入札・民間競争入札（いわゆる市場化テスト）を活用し，次期宮内庁 NWS の運用管理業務の実施については，「宮内庁共通基盤システムの整備・保守及び次期宮内庁 NWS の運用管理業務に係る民間競争入札実施要項（以下「実施要項」という。）」を基本とする。また，公共サービス改革法の第 1 条に基づき，民間事業者の創意と工夫を活用することにより，より良質かつ低廉な次期宮内庁 NWS の運用管理業務を実現し，IT ガバナンス及び情報セキュリティガバナンスの強化を図るとともに，継続的改善活動（PDSA サイクル）の徹底により，内的要因（ユーザニーズ）や外的要因（サイバー攻撃）が変化した場合でも，それらに柔軟に対応し，適切なサービスを継続的に提供することが本調達の第二の目的となる。本調達仕様書（案）は，甲が受注者となる民間事業者に請け負わせる，次期宮内庁 NWS の運用管理業務について適用する。

1.5.宮内庁における情報システムの概要

1.5.1.宮内庁における情報システム等

甲が利用する情報システム等について，以下のとおり示す。応札者は，以下について十分に把握し，必要ならば，甲担当者への確認を行うか，「13.資料閲覧」時に確認するなどし，宮内庁における情報システムとその利用実態について十分な理解に努めた上で，本調達の二つの目的を達成する提案を行うこと。

(1) 宮内庁が調達した情報システムの一覧

NO.	情報システム名 ［情報システム ID］	調達件名	契約の相手方	調達年度	備考

1	宮内庁情報ネットワークシステム（宮内庁 NWS）[A000760]	宮内庁情報ネットワークシステム機器の賃貸借及び保守	新日鉄住金ソリューションズ株式会社	平成 26 年	主なサーバ機器等は宮内庁 CIS での調達へ，運用管理は，宮内庁 NWS の運用管理業務に含める。ネットワーク機器の一部は，宮内庁統合 NW での調達へ。
		宮内庁 WAN の通信回線サービスの更新に係る調達	エヌ・ティ・ティ・コミュニケーションズ株式会社	平成 26 年	宮内庁統合 NW での調達へ。
		インターネット接続回線サービス	エヌ・ティ・ティ・コミュニケーションズ株式会社	平成 27 年	宮内庁統合 NW での調達へ。
		パーソナルコンピュータ及びサーバ等の賃貸借及びサーバ等保守	株式会社日立システムズ	平成 28 年	運用管理については，宮内庁 NWS の運用管理業務に含める。 なお，クライアント端末の保守は，スポット保守となる。ただし，サーバ（資産管理サーバ，KMS サーバ）については保守契約有。
		パソコン用プリンタ（インクジェットカラー）の購入	沖電気工業株式会社	平成 28 年	ドライバのインストール等は，宮内庁 NWS の運用管理業務に含める。保守は，都度のスポット保守にて対応。
		パソコン用プリンタ（モノクロ）の賃貸借及び保守	NEC ネクサソリューションズ株式会社	平成 28 年	ドライバのインストール等は，宮内庁 NWS の運用管理業務に含める。
		カラー複合機の賃貸借	富士ゼロックス株式会社	平成 28 年	ドライバのインストール等は，宮内庁 NWS の運用管理業務に含める。
		カラー複合機の保守	富士ゼロックス株式会社	平成 28 年	

		グループウェアシステムの賃貸借及び保守	新日鉄住金ソリューションズ株式会社	平成 29 年	運用管理については，宮内庁 NWS の運用管理業務に含める。
		標的型攻撃対策システムの賃貸借及び保守	エヌ・ティ・ティ・コミュニケーションズ株式会社	平成 29 年	宮内庁に設置した機器等の運用管理については，宮内庁 NWS の運用管理業務に含める。ただし，簡易 SOC サービスの運用管理については，標的型攻撃対策システムの賃貸借及び保守の宮内庁統合 NW 受託者が行う。
		Web 無害化機能の賃貸借及び保守	エヌ・ティ・ティ・コミュニケーションズ株式会社	平成 29 年	運用管理については，宮内庁 NWS の運用管理業務に含める。
		電子ファイルの暗号化及びアクセス制御機能の賃貸借及び保守	新日鉄住金ソリューションズ株式会社	平成 29 年	運用管理については，宮内庁 NWS の運用管理業務に含める。
		インターネットアクセス用セキュリティ機器の購入及び導入作業	新日鉄住金ソリューションズ株式会社	平成 29 年	買取機器。運用管理については，本調達に含む。
		宮内庁統合ネットワーク回線・機器に係る供給（設計・構築，テスト，移行，運用等）業務一式調達	未定（平成 31 年度に行う別調達であるため。）	平成 31 年	宮内庁 LAN のネットワークの定常的な運用管理については，宮内庁ＮＷＳの運用管理業務に含める。
		宮内庁共通基盤システムの整備・保守及び宮内庁 NWS の運用管理業	未定（本調達であるため）	平成 31 年	

		務に係る民間競争入札による調達			
2	正倉院宝物公開管理システム [A000793]	正倉院宝物公開管理システム機器賃貸借及び保守	新日鉄住金ソリューションズ株式会社	平成 26 年	端末はオンサイト保守を実施しているが，次期更新分からは，スポット保守とする予定。
3	宮内庁公開システム [A000771]	宮内庁公開システム政府共通 PF への移行等業務	スリーハンズ株式会社	平成 27 年	総務省の政府共通 PF 上に移行した。
		宮内庁公開システム賃貸借及び保守運用業務	株式会社セック	平成 27 年	端末はオンサイト保守を実施しているが，次期更新分からは，スポット保守とする予定。
4	CAD システム [A000782]	CAD システムの賃貸借及び保守	新日鉄住金ソリューションズ株式会社	平成 28 年	運用管理については，本調達に含む。
5	書陵部所蔵資料目録・画像公開システム [A016231]	書陵部所蔵資料目録・画像公開システムの賃貸借及び保守	株式会社ムサシ	平成 29 年	民間クラウド上で稼働している。

(2) 宮内庁が利用している主な府省共通システム

・官庁会計システム（ADAMSⅡ）　財務省

・国家公務員 IC カード身分証発行管理システム　内閣官房

・電子調達システム（GEPS）　総務省

・人事・給与システム（人給システム）　人事院

・政府共通 NW（G-Net）　総務省

・政府共通 PF　総務省

・旅費，謝金・諸手当及び物品管理の各業務・システム（SEABIS）　経済産業省

(3) その他

・セキュア USB メモリ

・USB 接続式 DVD-RAM ドライブなど

1.5.2.宮内庁 NWS の概要

現在，宮内庁 NWS は，ユーザが業務を遂行するために使用する，宮内庁の各拠点等に設置された情報通信機器等とそれらを繋ぐネットワークにより構成され，宮内庁 LAN，宮内庁 WAN とインターネット接続回線サービス，グループウェア，クライアント端末及びプリンタ等に大きく分類され，本調達仕様書（案）「1.5.1.宮内庁における情報システム等」の(1)に示した表中のとおりである。また，

ネットワーク機器を設置している主な拠点は次のとおりである。

なお，御移居に伴い該当施設の名称が変更となる可能性があるので留意すること。

(1)　宮内庁本庁

①　本庁サーバ室（本庁舎内）

②　各課室 19 インチラック内

③　各課室（本庁舎内と本庁舎以外の御所，書陵部，三の丸尚蔵館を含む）

(2)　東宮御所

①　東宮御所内サーバ室

②　各課室

(3)　宮邸

①　秋篠宮邸

②　常陸宮邸

③　三笠宮邸

④　三笠宮東邸

⑤　高円宮邸

(4)　その他

高輪皇族邸

(5)　御用邸

①　那須御用邸管理事務所

②　須崎御用邸管理事務所

③　葉山御用邸管理事務所

(6)　陵墓監区事務所

①　多摩陵墓監区事務所

②　桃山陵墓監区事務所

③　月輪陵墓監区事務所

④　畝傍陵墓監区事務所

⑤　古市陵墓監区事務所

(7)　京都事務所

①　京都事務所内サーバ室

②　各課室

(8)　正倉院事務所

①　正倉院事務所内サーバ室

②　各課室

(9)　御料牧場

①　御料牧場内サーバ室

②　各課室

宮内庁 NWS においては，ユーザ管理機能，グループウェア（電子メール機能，スケジュール機能等），標的型攻撃対策を中心としたネットワーク情報セキュリティ対策機能などのネットワーク情報サービスが提供されている。

次期宮内庁 NWS の中核である本調達は，ユーザが業務を遂行する上で重要な基盤となるが，操作性の向上など業務の更なる効率化と利用状況の向上，並びに近年，「標的型メール」攻撃を始めとする不正アクセスやウイルス感染による情報漏えいのリスク・脅威は増大していることから，情報セキュリティ対策の更なる向上を目的の一つとしてシステムの更改並びに見直しを実施するものである。

なお，別途調達される宮内庁統合 NW では，ネットワークに関する部分，現行宮内庁 LAN のネットワーク部分，現行宮内庁 WAN 及び現行インターネット接続回線サービスを同一調達内で行い，さらにその調達内で新たに統合 SOC サービスを加えてネットワーク全体でのシームレスな情報セキュリティ対策の強化を図ることとなる。

また，宮内庁 WAN の回線は，平成 26 年度の「宮内庁 WAN の通信回線サービスの調達仕様書」に基づく調達において，それ以前までメタル回線であった地方拠点（ただし，高野山部，吉野部，掖上部を除く），正倉院事務所や御料牧場などでの光回線化を行い，ネットワークの帯域幅増加による高速化と電磁ノイズ対策強化による安定化を図ったことから，クライアント端末上のソフトウェアのパッチの配信やリモートでの運用管理などが効率的に行うことができるようになった。現行の宮内庁 WAN の回線種別を別紙 2 に示す。ただし，宮内庁 WAN は，本調達の公示時点では宮内庁統合 NW の一部として構築中であるため，本調達の応札者は，提案に際して甲に確認すること。

1.5.3.運用管理業務の軽減に関するこれまでの主な取組

甲が取り組み，実現してきた宮内庁 NWS の運用管理業務の効率化について，次のとおり示す。応札者は，次について十分に把握し，必要ならば，甲担当者への確認を行うか，「13.資料閲覧」時に確認するなどし，宮内庁における情報システムについて十分な理解に努めた上で，より一層の宮内庁 NWS の運用管理業務の効率化に資する提案を行うこと。

1.5.3.1　宮内庁 WAN の光回線化によるネットワーク高速化

宮内庁 WAN の回線は，平成 26 年度の「宮内庁 WAN の通信回線サービスの調達仕様書」に基づく調達において，それ以前までメタル回線であった地方拠点，正倉院事務所や御料牧場などでの光回線化を行い，ネットワークの帯域幅増加による高速化と電磁ノイズ対策強化による安定化を図ったことから，クライアント端末上のソフトウェアのパッチの配信やリモートでの運用管理などが効率的に行うことができるようになった。現行の宮内庁 WAN の回線種別を別紙 2 に示す。

1.5.3.2　サーバの集約化による運用管理業務の軽減

宮内庁 WAN の光回線化により，地方拠点に点在していたサーバ機能及びその物理的なハードウェアを含めて本庁及び京都事務所へ集約化を行った結果，サーバについて現行宮内庁 NWS としての運用管理業務を軽減できた。具体的には，平成 26 年度の「宮内庁情報ネットワークシステム機器の賃貸借及び保守調達仕様書」に基づく調達において，それ以前の宮内庁 NWS における地方 3 拠点（正倉院事務所，御料牧場，京都事務所）に設置されていた各サーバは，次のサーバ機能を有していた。

(1)　ディレクトリ（AD: Active Directory）サーバ機能
(2)　ファイルサーバ機能
(3)　プリントサーバ機能
(4)　ウイルス対策サーバ機能

上記のサーバ機能を有するサーバ機器等は，それぞれ，本庁及び御料牧場を始めとする関東エリア

については，本庁のサーバ室へ集約し，京都事務所及び正倉院事務所を始めとする関西エリアについては，京都事務所のサーバ室へ集約した。

さらに，同時に仮想化技術を採用することにより，サーバの物理的なハードウェアの台数を削減し，ハードウェアに関する運用管理業務を軽減できた。

1.5.3.3　バックアップの集約化による運用管理業務の軽減

宮内庁 WAN の光回線化により，地方拠点に点在していたサーバを宮内庁本庁及び京都事務所へ集約化を行った結果，正倉院事務所と御料牧場のサーバ機器等を撤去したことから，バックアップに関する現行宮内庁 NWS としての運用管理業務を軽減できた。また，業務継続計画の実効性をより高めるため，平常時の情報システム設置拠点と同時被災しないことが想定される場所にバックアップシステムを確保する等の措置として，本庁サーバ室のリモート・バックアップシステム拠点を京都事務所とし，京都事務所サーバ室のリモート・バックアップ拠点は本庁サーバ室とする，宮内庁 WAN を介したネットワークによる計画的な自動リモート・バックアップを，現行宮内庁ＮＷＳでは実現している。

1.5.3.4　宮内庁公開システムの政府共通 PF への移行に伴う運用管理業務の軽減

平成 27 年度の「宮内庁公開システム政府共通 PF への移行等業務調達仕様書」に基づく調達により，皇居等参観受付システム，情報公開システム，ホームページ公開システムの 3 システムのサーバ機器等については，総務省が構築及び運用保守を行っている政府共通 PF 上のものに移行したことから，本庁・京都事務所・データセンタ設置機器の稼働監視などの現行宮内庁 NWS としての運用管理業務を軽減できた。

1.5.3.5　国家公務員 IC カード身分証等発行管理システムの廃止に伴う運用管理業務の軽減

創造宣言において，マイナンバーカードの普及・活用に関して「特に国家公務員における身分証としての活用は，重点的かつ計画的に実施する必要があるため，各省庁で導入計画を作成させ，引き続き順次移行を促進。」と示されたことに伴い，甲においても自治体が発行したマイナンバーカードを身分証としたため，国家公務員 IC カード身分証等発行管理システムを利用した身分証の発行がなくなり，同システムの廃止となったことから，これに関連する現行宮内庁 NWS としての運用管理業務を軽減できた。

1.5.3.6　ユーザ管理の集約化による運用管理業務の軽減

平成 29 年 8 月末までの現行宮内庁 NWS におけるユーザ管理は，平成 26 年度の「宮内庁情報ネットワークシステム機器の賃貸借及び保守」の調達で構築を行った，ユーザ管理用サーバとディレクトリサーバが中心となっていたが，グループウェアシステムのユーザ管理とは別体系となっており，ユーザ管理が重複し，運用管理業務が非効率であった。平成 29 年度の「グループウェアシステムの賃貸借及び保守調達仕様書」に基づく調達により，現行のグループウェアシステムにおいては，AD を中心とした設計となり，ユーザ管理の集約化を図ったことから，ユーザ管理に関する現行宮内庁 NWS としての運用管理業務を軽減できた。

1.5.3.7　グループウェアシステムのクラウドサービス利用による運用管理業務の軽減

創造宣言において，クラウド・バイ・デフォルト原則の導入が示されたことに伴い，平成 29 年度の「グループウェアシステムの賃貸借及び保守調達仕様書」に基づく調達において，情報セキュリティ対策を十分に求めた上で，オンプレミス型とクラウドサービス型の両方の提案を可能とする仕様としたが，入札の結果，クラウドサービス型の提案を行った事業者が受注した。これにより，現行のグループウェアシステムを構成するメール機能やスケジュール管理機能等のサーバ機器の保守やソフトウェアのパッチ適用等の運用管理業務は，クラウドサービスプロバイダが行っているため，現行宮内庁 NWS としての運用管理業務を軽減できた。

1.5.3.8　庁内ポータルサイトの集約化による運用管理業務の軽減

平成 29 年 9 月まで庁内には，Notes サーバによる掲示板と Web サーバによる職員情報ボードの 2 つのポータルサイトが存在したが，平成 29 年度の「グループウェアシステムの賃貸借及び保守調達仕様書」に基づく調達の結果，それ以前のグループウェアシステムに含まれていた Notes サーバによる掲示板を廃止した。それに伴い，庁内ポータルサイトが職員情報ボードへ一つに集約され，宮内庁 NWS としての運用管理業務を軽減できた。

1.5.3.9　資産管理サーバとクライアント端末の自動連携による運用管理業務の軽減

平成 28 年度の「パーソナルコンピュータ及びサーバ等の賃貸借及びサーバ等保守調達仕様書」に基づく調達及び現行宮内庁 NWS の設定変更により，クライアント端末上のウイルス対策ソフトで検知した情報を資産管理サーバに自動的に共有し，当該クライアント端末を自動的にネットワークから遮断する機能を実装したことにより，検知からネットワーク遮断に至るまでの人による運用管理業務が省略可能となり，かつ，迅速かつ適切な対応が可能となったため，現行宮内庁 NWS としての運用管理業務を軽減できた。

1.5.3.10　簡易 SOC サービス導入による運用管理業務の軽減

平成 29 年度の「標的型攻撃対策システムの賃貸借及び保守調達仕様書」に基づく調達の結果，標的型攻撃対策システムで検知したものの分析及び判断が明確化した。それ以前は，検知内容を運用管理支援事業者又は甲担当者が手作業で調査を行いつつ様式への記入等を行うなどの管理工数が発生していただけでなく，検知した内容が判明するまで時間がかかり，その間の対応の緊急性を高い状態に保つ必要があり，他の業務の進捗に影響を与えていた。簡易 SOC サービス導入以前のように，検知案件の内容確認からの事後処理（報告の作成など）がなくなったことから，プロセスに費やす時間が大幅に減り，かつ，初動対応の迅速化が可能となったため，現行宮内庁 NWS としての運用管理業務を軽減できた。

1.6.業務内容

1.6.1.調達範囲

本調達における主な調達区分は次のとおりとなる。各調達の詳細な範囲は次項以降を参照すること。

(1) 統括管理

本業務全体に係る作業実施計画作成，体制整備，進捗管理及び課題管理等を行う。

(2) 設計

調達仕様書，提案書及び各種ドキュメントに基づき，宮内庁 LAN 基盤サーバ群等の機器に関する設計，移行業務及び運用管理業務の計画作成等を行う。

宮内庁統合 NW でなされた全体ネットワーク設計方針を前提とし，調達仕様書，提案書及び各種ドキュメントに基づき，宮内庁 LAN 基盤サーバ群等の機器に関する設計，移行業務及び運用管理業務の計画作成等を行う。設計に当たっては，宮内庁統合 NW 側の方針を精読し，設計方針に則って必要な作業を実施する。

(3) 構築

各種設計書及びドキュメントに基づき，機器等について，稼働に必要なソフトウェアのインストールや設定等を実施して指定の場所に搬入し，設置調整等の構築作業を行い，必要十分な機能を確実に動作させる。

(4) テスト

各種テストの計画書を作成し，テストを実施する。

なお，甲担当者が主体となって実施する受入テストの支援を行う。

(5) 移行

各種設計書及び移行実施計画書に基づき，現行システムから次期システムへの移行を行い，宮内庁 NWS を用いたユーザの業務の継続性を保つ。

(6) 保守

宮内庁 LAN 等の機器障害発生時における連絡調整，障害機器等への対応及び保守業務結果に関する報告等を行う。

(7) 運用管理業務

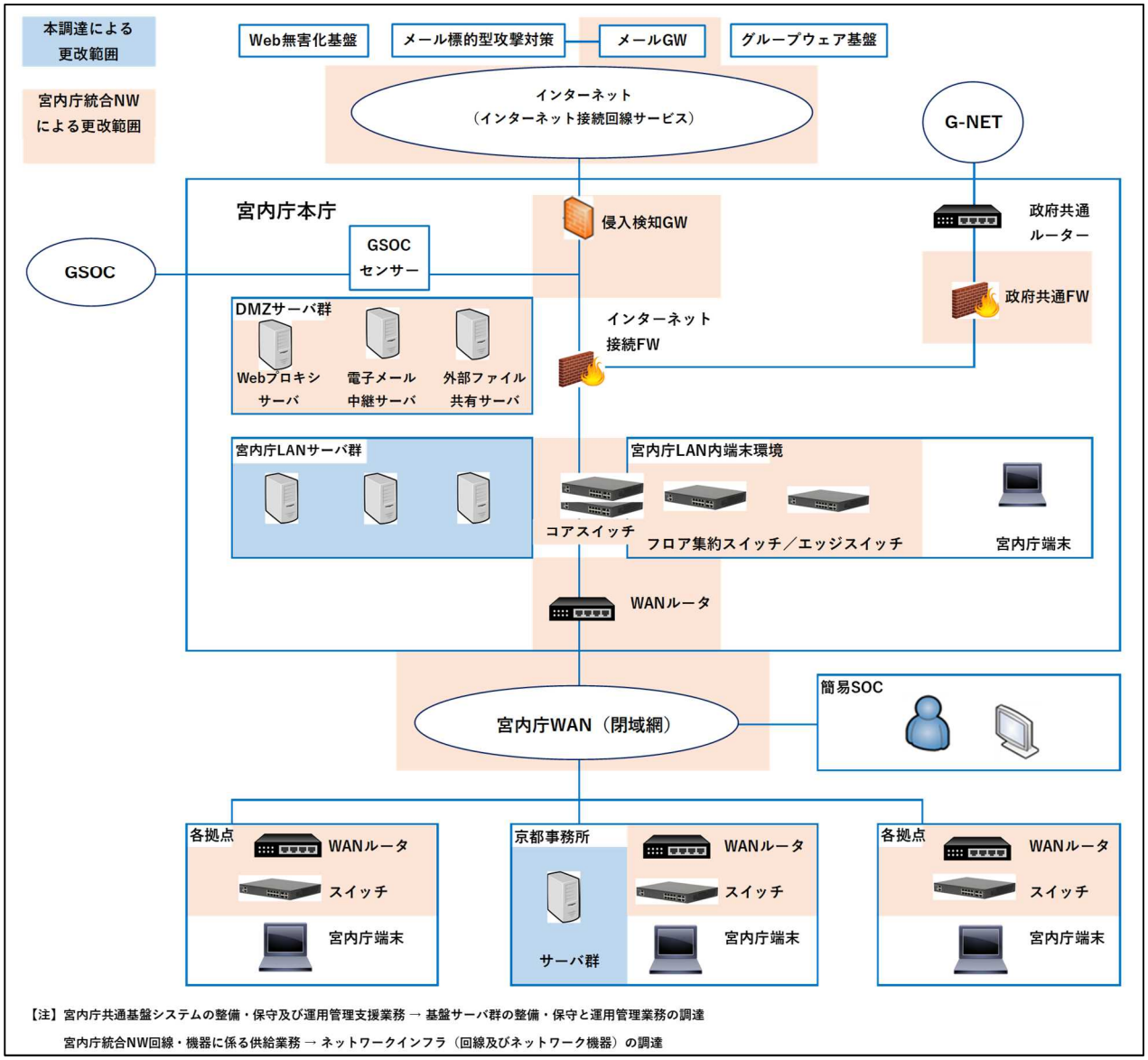
運用管理に係る手順書の整備，各種管理，定例会議での報告，機器等変動に関する支援，計画停電対応及びヘルプデスク業務等を行う。運用管理業務は，日々の運用の中で，ユーザの異動，情報セキュリティ対策の導入などの要因に基づく宮内庁 NWS の変更管理が軸となる。

1.6.2.現行宮内庁 NWS 構成

以下に現状の宮内庁ＮＷＳの構成及び，機器の更改範囲について示す。

詳細な現状構成については，閲覧資料を参照の上，詳細なシステム構成を把握すること。

【現行】



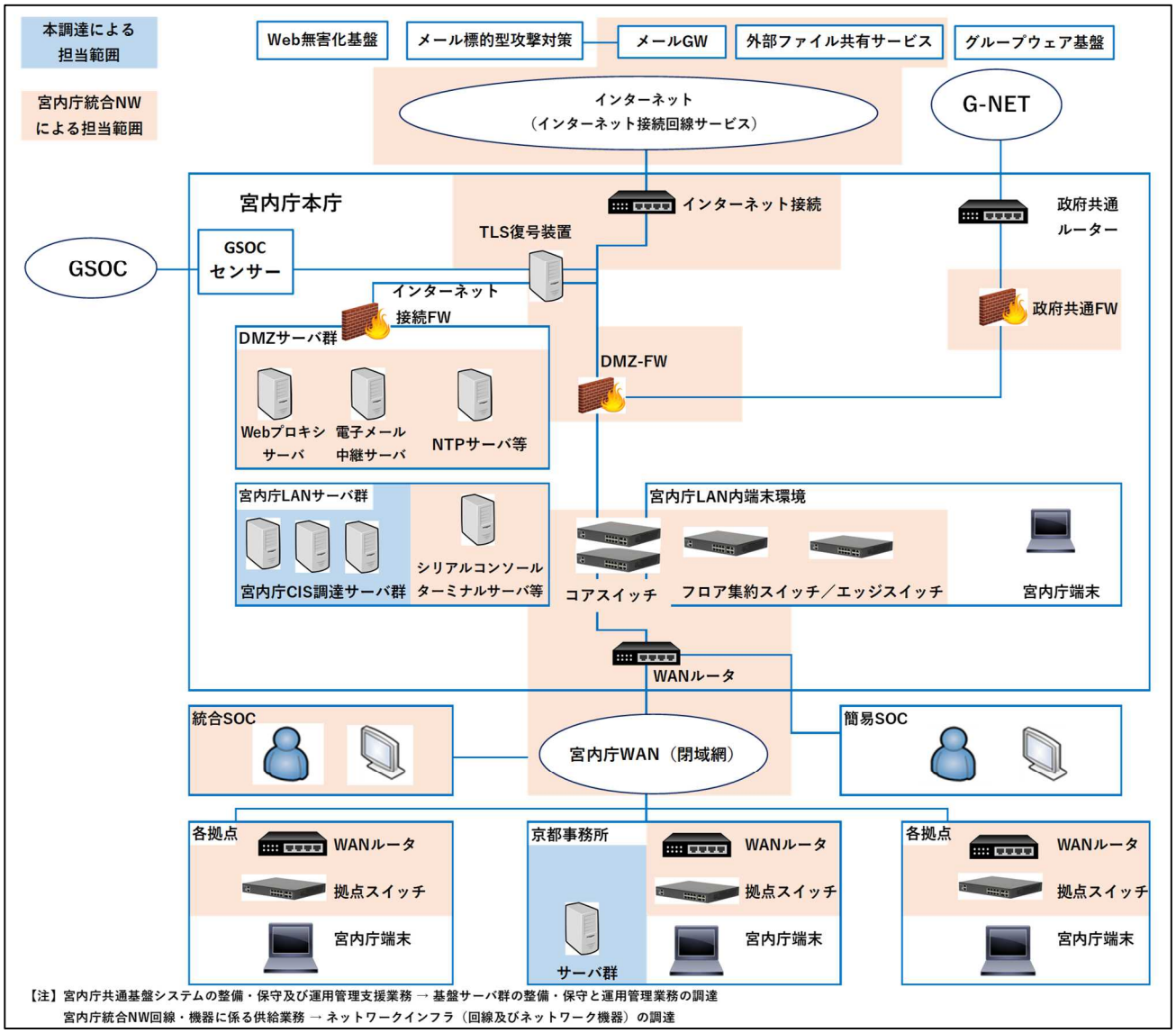
上に示す機器更改範囲を対象として，必要な機器群の更改を行うとともに，機器更改対象範囲ではない部分においても，移行期間中及び次期宮内庁 NWS 全体が正常に動作するように本受託者は適切な設計を行うこと。また，更改に当たって連携する周辺システムへの設計に関する変更が必要となる場合は，受託者の負担の下，次期宮内庁 NWS 全体が正常に稼働するよう作業を行うこと。

IP アドレス設計，セグメント設計，通信フロー設計，バックアップ設計など宮内庁ＮＷＳとして統一的な設計及び運用が求められる事項については，本調達仕様書（案）で定める会議体又は甲を通じて宮内庁統合 NW 受託者と協議を行った上で進めていくこと。

1.6.3.次期宮内庁 NWS 概要

次期宮内庁 NWS についてのシステム構成の全体概要は次のとおり。

【次期】



次期宮内庁 NWS における現行システムとの主要な変更点は次のとおりとなる。

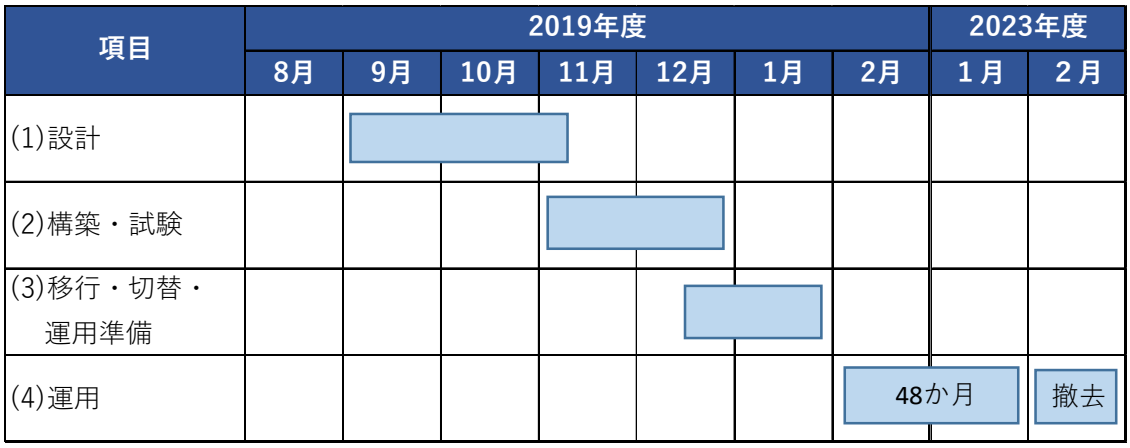
(1) 特権 ID 管理機能の導入

(2) ログ収集機能サーバの導入

(3) 振る舞いログ分析（UEBA）サーバの導入

1.6.4.スケジュール（案）

乙は次のスケジュール（案）を参考にし，各作業における WBS のクリティカルパスを明確にした上で，遅延なきよう各作業の進め方を工夫すること。また，宮内庁 CIS の構築は，宮内庁統合 NW の構築期間と並行して行われるが，本調達の目的を達成するため，宮内庁 NWS 全体として機能するよう双方で協力しながら設計・構築を行うこと。本調達の各作業内容については，次項を参照すること。



1.6.5.業務内容及び各事業者との役割範囲

本受託にて実施する業務内容について記載する。

現行各システム事業者，次期運用管理事業者（宮内庁 CIS 受託者），運用管理支援事業者及び各事業者等との役割分担については，別紙 4 を参照すること。作業及びシステム実装に求められる各要件については「3.システム要件」に記載されている詳細な要件を参照のこと。

1.7.契約期間

契約期間は，契約日から 2024 年 1 月 31 日までとする。その詳細は以下のとおり。

(1)　設計・構築業務

契約締結日から 2020 年 1 月 31 日まで

(2)　運用管理・保守業務

2020 年 2 月 1 日から 2024 年 1 月 31 日までの 48 か月

なお，賃貸借している機器については，契約期間終了後に再賃貸借又は買取をする場合がある。

1.8.納入

(1)　納入は，甲担当者の指示を受けてから行うこととし，乙側責任者は，作業開始の連絡及び作業終了の報告の上，確認を受けること。

(2)　納入時は，既設建物，特に室内の床板，敷物及びカーテン等の室内装飾を汚損又は破損しないように細心の注意を払うこと。

(3)　納入時に生じた梱包箱等不要物は適切に処分すること。

(4)　別途配線等工事が必要な場合は，事前に甲担当者の了承を受け，乙の負担で実施すること。

(5)　甲及び関係事業者との調整で発生する費用は，乙の負担で実施すること。

1.8.1.納入条件

(1)　本調達仕様書（案）に明示された機能，性能及びその他の条件を全て満たしていること。

(2)　提供予定の内容を示したネットワーク図（様式適宜），機器類明細書を提出すること。

(3)　本調達仕様書（案）に記載している事項及びそれらに付随して発生する費用を全て負担すること。

乙は本調達で導入する機器の設計・構築，インストール・アンインストール及び環境設定，現行データの移行，動作確認・テストを納入期限までに完了の上設置し，契約開始日から完全に利用可能な状

態にし，サービスを開始できる体制とすること。

なお，サービス利用開始日において全部又は一部が利用できない場合は，代替措置を乙の責任と負担で提供すること。

(4) 搬入，据付，配線，調整，既設設備との接続に要する全ての費用及び契約期間中の保守費用は，本調達に含まれる。

(5) 機器等については，原則，「国等による環境物品等の調達の推進等に関する法律(グリーン購入法)に基づく「環境物品等の調達の推進に関する基本方針（平成 30 年 2 月 9 日変更閣議決定)」に規定された製品については判断基準を満たすものとすること。

(6) 本調達が正常に稼働するために必要となる機器及び役務等については，甲担当者に報告の上，乙の責任において供給，実施すること。

(7) その他，納入に関する不明な点は甲乙協議の上，実施すること。

1.8.2.納入期限

2020 年 1 月 31 日

1.8.3.納入場所

支出負担行為担当官の指定する場所（「別紙 2 宮内庁 NW 設置拠点・設置場所等」参照）

1.8.4.納入検査

納入検査は，乙側責任者及び甲が指定する甲検査職員立会いの上行い，不合格品の生じた場合には，新規取替え等甲担当者の指示に基づき必要な処置をとること。

1.9.納入後に求める環境配慮（温室効果ガスの排出抑制のための取組要件）

本調達に際して，「宮内庁環境配慮の方針」（平成 19 年 3 月 14 日宮内庁環境配慮の方針推進委員会決定）の内，「２．(2)③温室効果ガスの排出抑制のための取組」について，助言等を行うこと。

（参考）宮内庁の環境配慮について

http://www.kunaicho.go.jp/kunaicho/shiryo/kankyo/kankyou-hairyo.html

1.10.保証

現場に搬入・設置等，搬入過程における傷・損傷等及び納入検査後に発覚した初期不良やユーザによる故意ではない見え隠れする部分の不具合等については，乙は直ちに新規取替え又は補修を行い，納入後 1 年間の保証義務を負うこと。

なお，それ以上の保証期間の明記があるものは，その期間の保証義務を負うこと。

1.11.成果物

本調達の成果物は，次の表のとおり実施前又は実施後に甲担当者に提出すること。

次の表に明記のない，各成果物の詳細な内容や提出期限は，甲担当者と協議の上決定すること。

成果物の形態は，次のとおりとする。

(1) 成果物は，主として日本語表記とすること。

(2) 情報処理に関する用語の表記は，JIS の規定に従うこと。

(3) 成果物は，紙媒体及び電磁的記録媒体（以下「電子媒体」という。）により作成し，2 部提出すること。紙媒体はファイル等にまとめ，各項目にはインデックスを貼付すること。

(4) 電子媒体は，甲担当者の端末にて読み取り可能な形式（マイクロソフト社の Word2016 ，Excel2016 ，PowerPoint2016 並びに Adobe 社の AcrobatReaderDC を標準）で電子媒体（CD-R 又は DVD-R 等）に納め，2 部提出すること。

(5) 成果物に修正等があった場合，紙媒体は，更新履歴と修正ページ，電子媒体は，更新履歴と修正後の全編を速やかに提出すること。

(6) 納品後，甲担当者において改変が可能となるよう，図表等の元データも併せて編集可能な形式で提出すること。

本整備業務管理文書

NO.	成果物	内容
1	作業実施計画書	本業務に係る全体の管理について，工程表や作業体制等を明記した作業実施計画書等をまとめた文書。契約締結後 10 日以内（休日を除く。）に作成し，甲担当者の承諾を得ること。工程に変更が生じた場合は，甲担当者と協議の上，新規工程表をその都度作成すること。
2	進捗管理報告書	本業務に係る作業全体の進捗報告を原則として週毎に作成すること。
3	移行実施計画書	端末，ネットワーク，サーバの移行計画を作成すること。
4	展開作業計画書	移行実施計画で作成する工程表を基に各設置場所へ機器を展開する計画を作成すること。
5	課題管理表	各工程において，検討，決定すべき課題や業務実施上の課題等を整理し一覧表を作成すること。様式については甲担当者と協議すること。
6	情報セキュリティ管理計画書	情報セキュリティを確保するための実施内容及び管理体制についてまとめた計画を作成すること。内容に変更が生じた場合は甲担当者と協議の上，都度計画書を修正すること。
7	打合せ資料	打合せ資料を作成すること。
8	議事録	打合せした内容を記した議事録を作成すること。

環境構築・運用管理文書

NO.	成果物	内容
1	基本設計書	本調達の要求事項を踏まえ，本調達機器の仕様と概略設計等（ハードウェア・ソフトウェア構成図，機能設計，データ設計等）を作成すること。 契約締結日から起算して 15 日（休日を除く。）以内で甲に提出し，甲の確認を得ること。甲の確認を得た日から起算して 3 日（休日を除く。）以内に甲と協議の上で承諾を受け，最終確定とすること。
2	詳細設計書	基本設計書に基づき，ハードウェア・ソフトウェア及びアプリケーションの実現内容（設定パラメータ・設定ルール等）を詳細に作成すること。 本表の NO.1 の最終確定をした日から起算して 25 日（休日を除く。）以内で甲に案を提出し，甲の確認を得ること。甲の確認を得た日から起算して 5 日（休日を除く。）以内に甲と協議の上で承諾を受け，最終確定とする

		こと。
3	ODB 登録用シート	管理標準ガイドラインに基づく ODB（政府情報管理システムデータベース）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）をまとめたシートについて，次の対応を実施すること。 ① 管理標準ガイドラインに記載されている「別紙 2 情報システムの経費区分」に基づき区分した契約金額の内訳を記載した「契約額内訳入力用 Excel シート」を契約締結後速やかに作成すること。 ② 導入したハードウェアの情報を記載した「ハードウェア情報入力用 Excel シート」及びソフトウェアの情報を記載した「ソフトウェア情報入力用 Excel シート」を作成すること。 ③ 上記①及び②以外においても甲担当者の求めに応じ，ODB 登録用シートを作成すること。
4	テスト計画書	各テスト（単体，結合，総合）の項目，実施方法，判定基準等を記した文書を作成すること。 なお，受入テストに当たっては，甲担当者の実施を支援するよう分かりやすい内容でテスト項目を作成すること。 本表の NO.1 の最終確定をした日から起算して 30 日（休日を除く。）以内で甲に案を提出し，甲の確認を得ること。本表の NO.3 の最終決定した日から起算して 15 日（休日を除く。）以内に甲と協議の上で承諾を受け，最終確定とすること。
5	テスト結果報告書	テスト計画書に基づいた各テストの結果を記した文書を作成すること。 なお，受入テストの結果を本報告書に含めること。
6	運用管理設計書（案）	必要に応じて本表の NO.1～6 を基に，宮内庁 CIS の運用管理に必要十分な管理項目，監視設計，バックアップ設計，障害設計などについて文書を作成すること。
7	運用管理手順書（案）	運用管理設計書（案）との内容の整合性を図りつつ，運用管理業務に従事する者（以下「運用管理従事者」という。）向けの運用管理手順書の案を作成すること。 また，この手順書（案）は，次期宮内庁 NWS の運用管理業務の手順書（案）となる。 ① 日々の運用，障害等発生時，バックアップ及びパッチ適用等の際に最低限必要と考えられる項目に対して参照可能な内容とすること。 ② 障害等発生時の一次切り分けの際に使用できる内容であること。 ③ 故障時の連絡先（役割分担，連絡先等）を作成すること。
8	甲担当者向け停電時復旧手順書(案)	運用管理設計書（案）及び運用管理手順書（案）との内容の整合性を図りつつ，勤務時間外に停電が発生し，サーバ等がシャットダウンされた状況を想定し，復電した際に，甲担当者がサーバ等の復旧作業ができるわかりやすい内容の復旧手順書及び復旧作業フロー図を作成すること。 おって，この手順書（案）は，次期運用管理事業者（宮内庁 CIS 受託者）にて運用する次期宮内庁NWSの運用管理業務向け停電時復旧手順書の基となる。

9	情報セキュリティインシデント対応手順書（案）	甲担当者と協議の上必要と判断された成果物は，運用管理設計書（案）及び運用管理手順書（案）との内容の整合性を図りつつ，別途，手順書の案を作成すること。情報セキュリティインシデントが発生した場合の甲及び次期運用管理事業者（宮内庁 CIS 受託者）向け対応手順書を作成すること。また，この手順書（案）は，次期運用管理事業者（宮内庁 CIS 受託者）にて運用する次期宮内庁 NWS の運用管理業務の情報セキュリティインシデント対応手順書の基となる。
10	ユーザ手順書(案)	クライアント端末を使用するユーザ向けの操作手順書の案を作成すること。また，この手順書（案）は，宮内庁 NWS の運用管理業務のユーザ手順書の基となる。
11	運用管理計画書（案）	必要に応じて本表の NO.6～10 を基とし，宮内庁 CIS の日々の安定稼働を確保することを目的とした計画書の案を作成すること。また，この計画書（案）は，次期運用管理事業者（宮内庁 CIS 受託者）にて運用する宮内庁 NWS の運用管理業務の運用管理計画書の基となる。
12	その他	甲担当者と協議の上必要と判断された成果物は，別途作成すること。

保守文書

NO.	成果物	内容
1	保守計画書	宮内庁 CIS に関する保守の実施計画及び作業体制等の実施内容を作成し，甲担当者の承諾を得ること。変更が生じた場合は，変更計画書を作成し，甲担当者の承諾を得ること。
2	保守手順書	宮内庁 CIS に関する事前準備，保守運用作業及び検証の手順等を作成し，甲担当者の承諾を得ること。変更が生じた場合は変更手順書を作成し，甲担当者の承諾を得ること。
3	保守結果報告書	宮内庁 CIS に関する保守を行った場合，速やかに結果をまとめ報告し，甲担当者の承諾を得ること。
4	データ消去証明書	宮内庁 CIS の利用期間満了に伴い実施する本調達機器のデータ消去に関し，全てのデータの完全な消去作業を確実に行ったことを証明する書類（作業実施者及び責任者，作業日，作業内容などを記載したもの）を作成し，甲担当者の承諾を得ること。

1.12.契約期間終了後の引取り

(1) 契約終了後の機器等の引取りは，全て乙の責任と負担において実施するものとする。また，実施に当たり甲及び関係事業者との調整に伴い発生する費用は，乙が負担すること。

(2) 機器等の引取りは，甲担当者の指示により行い，乙側責任者は，作業の開始及び終了時に甲担当者に報告の上，確認を受けてから行うこと。その際，既設建物，特に室内の床板，敷物及びカーテン等の室内装飾を汚損又は破損しないように細心の注意を持って行うこと。引取り時に生じた梱包箱等不要物は適切に処分すること。

(3) 機器等の引取りの際は，搭載されている HDD 等の補助記録装置内の情報が残らない（復元を不可能とする）措置を宮内庁庁舎内で講ずること。対応できないことがある場合は，事前にこの根拠を明

確にした文書を作成し，甲と協議の上で承諾を受けた後，適切な対応を行うこと。

なお，データ消去作業後は，データ消去証明書を作成し，甲担当者の承諾を得ること。

1.13.指示等の書面主義

本調達の具体的な指示，報告，申出，質問，回答及び協議等は，原則文書で行う。ただし，緊急又はやむを得ない場合は口頭で行うことができるが，事後必ずその内容を記した文書を取り交わすこと。

1.14.役務作業要件

(1) 乙は，契約開始日までに事前準備として必要なハードウェア及びソフトウェアは乙の負担で準備すること。

(2) 乙は，本業務の事前稼働検証，機器等の導入・設置，設計・構築・各種ソフトウェアのインストール及び環境設定，動作確認，現行のデータ移行手順書等の作成及び教育等を行うに当たり，当該各作業の実施前には，十分な時間的余裕をもって甲と調整し，各作業工程表を提出し，甲の承諾を得ること。

(3) 本業務の実施に当たり，各現行システムの業務に影響を与えないこと。また，ユーザ端末のデータ移行・切替えに当たり，ユーザの負担を軽減する方策を検討すること。

(4) 本業務の実施に当たり，関係事業者の協力を得る必要がある場合は，協力が必要となる日の原則 10 日（休日を除く。）前までに乙が文書にて甲へ具体的に説明して甲の承諾を得た上で，甲及び関係事業者と協議して合意を得ること。合意を得た場合には，原則として，乙の負担において関係事業者から協力を得ること。

(5) 本調達の目的の達成に必要な機器及び消耗品等は，全て乙の責任と負担において用意すること。

(6) 本業務の実施に当たり，乙は，業務全般を掌握し，かつ，本業務を指揮監督する業務管理責任者及びこれを補佐する者(以下「業務管理責任者等」という。）を選任し，業務管理責任者等の資格，経験及び国籍を証明する文書を提出の上，契約日から起算して 5 日（休日を除く。）以内に甲の承諾を得ること。

なお，業務管理責任者等を変更する場合は，原則として変更予定日の 10 日（休日を除く。）前までに前述の資格等証明文書を提出の上，甲の承諾を得ること。

(7) 業務管理責任者等は，業務の進捗状況全体を把握し，甲に対して内容及び結果を定期的に報告すると共に各工程の終了時には，その結果報告を提出し甲の承諾を得ること。また，甲からの本業務等に関する問合せに対しては，問合せを行った日から起算して原則 2 日（休日を除く。）以内に回答すること。ただし，甲が問合せ時に回答期限を設定した場合には，これに従うこと。

(8) 甲から乙に対する指示，協議申し出は，業務管理責任者等を通じて行うものとする。

(9) 本業務の実施に当たり，乙の故意又は過失により稼働中の各現行システムに対して不具合や問題を生じさせた場合は，乙の責任と負担において適切に対処し，正常化すること。

(10) ユーザの作業が発生する場合は，作業が必要となる日の 10 日（休日を除く。）前までに乙が作業内容について文書にて甲へ具体的に説明して協議の上，承諾を得ること。

(11) 本システムの導入日は，原則として，平日の業務時間（8:30～17:45）に実施すること。ただし，サーバ等各現行システムに影響を与える作業の場合は，ユーザの業務が停止しないよう，原則として，休日又は平日の業務時間（8:30～17:45）以外を利用し，実施すること。

(12) 本業務に当たり，現行環境の設定変更，ソフトウェアのインストール・アンインストールが必要

となる場合には，関係事業者への設計・設定変更依頼書にて甲及び関係事業者に依頼すること。

(13) (12)の作業に伴い，本調達以外の機器が必要な場合は，乙の責任と負担において適切な情報セキュリティ対策を機器に対して施した上で安全に導入すること。

(14) 本業務の実施に当たり，納入する機器等は，本調達仕様書（案）を満たす増設機器（メモリ（以下「主記憶装置」という。）及びハードディスク等（以下「補助記憶装置等」））を全て取り付けた形で，正常動作の確認を行った上で納入すること。

(15) 本業務の実施に当たり，導入する宮内庁 CIS の動作が正常であることを確認すること。

(16) 本業務を遂行するに当たり，宮内庁 CIS で新規に導入した機器等に必要な情報（政府共通 NW やインターネット等を介して利用するユーザの宮内庁 NW のシステム環境等）は，本業務の契約締結後に甲担当者より提示する。

(17) 乙は，マルチベンダ構成により調達を行う場合，納入及び運用を確実に実現するため，事前に関係事業者との間で必要な書類等を取り交わす等，十分な合意を得るとともに，その実施のための体制を整備した計画を作成し，甲に提出し，承諾を得ること。

(18) 関係事業者の各種調整などで生じた作業は，あらかじめ甲の承諾を得た上で乙の責任と負担において実施することとし，本業務に当たり，その調整等による不都合，負荷などができる限り発生しないようにすること。

(19) 機器の設定ファイル等は，一般的なテキスト・エディタ等での可読なファイルフォーマットで保存の上，時系列での保守ができるように構成管理し，変更があるときはその都度提出すること。

(20) 本調達機器等を甲が管理するための情報資産台帳に必要事項（ホスト名，IP アドレスなどのネットワーク設定の情報）を記入し，提出すること。

なお，IP アドレスの払い出しやネットワーク設定等は，甲を介して現行運用管理支援事業者及び宮内庁統合 NW の保守・運用事業者と必要な調整を行い，甲の承諾を得た上で，乙の責任と負担において実施すること。

(21) 本調達機器に関しては，現行機器の設定情報等を提供するので，その設定情報を活用し，効率的な設計・設定を行うこと。

(22) 本業務は，次の標準ガイドライン群の各文書を十分に理解した上で，記載内容に準じて実施すること。

（参考）「デジタル・ガバメント推進標準ガイドライン」（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）に関連する指針類等に係る文書体系を以下「標準ガイドライン群」という。
https://cio.go.jp/guides

1.15.情報セキュリティ対策

1.15.1.情報セキュリティの確保

情報セキュリティを確保するために応札者は以下の作業を実施することとし，発生する費用は本調達に含まれるものとする。また，その実施内容及び管理体制についてまとめた情報セキュリティ管理計画書を提出すること。

(1) 本業務の実施において，情報セキュリティを確保するための体制を整備すること。

(2) 秘密保持等のため次の項目を遵守すること。

① 取り扱う情報は甲の情報処理業務にのみ使用し，他の目的には使用しないこと。

② 取り扱う情報は甲の情報処理業務を行う者以外には秘密とすること。

③　取り扱う情報を甲の指定した場所から持ち出さないこと。

④　当該情報を甲の許可なく複製しないこと。

⑤　当該情報は，業務終了時に，返却，消去又は廃棄を確実に行うこと。

(3)　甲が定める「宮内庁情報セキュリティポリシー」を遵守すること。また，「政府機関の情報セキュリティ対策のための統一基準群（内閣サイバーセキュリティセンター（以下「NISC」という。））」の最新版を遵守すること。ただし，遵守のために別途，ソフトウェア又はハードウェアの機能やモジュール等の追加購入及びセットアップ作業が必要となる場合，又は現行システムに対する大幅な設計変更が必要となる場合には，必要となる費用の概算や作業内容等を可能な限り甲担当者へ提供し，甲担当者の検討に協力すること。

(4)　本調達においては，外部からの攻撃に対する情報セキュリティ対策のみでなく，内部での情報セキュリティ対策，外部の情報システムに対して悪影響を与えないための情報セキュリティ対策等，総合的な情報セキュリティ対策を講じること。

(5)　総合的な情報セキュリティ対策を講じる上で，宮内庁統合 NW，標的型攻撃対策システム，クライアント端末，資産管理サーバ，KMS サーバなどと連携して機能する対策については，連携する各システムの設計書や機器上の設定内容等を十分に確認し，理解すること。

なお，連携する各システムの機器上の設定の変更が必要となる場合には，甲を介して各システムの保守事業者，現行運用管理支援事業者と必要な調整を行い，設定変更の内容（変更前と変更後の差分等）を明らかにし，甲の承諾を得た上で，乙の責任と負担において具体的な設定変更の作業依頼書を作成すること。ただし，作業実施予定日の 10 日（休日を除く。）前までに乙が作業内容（設定，手順等）について文書にて甲へ具体的に説明した上で，通常の保守業務又は運用管理業務の範囲内の作業と認められる場合には，甲を介し，甲の指示として当該作業を関係事業者に通常業務として依頼することができる。

(6)　本調達システム内部への侵害拡大を防止するため，独立行政法人情報処理推進機構（以下「IPA」という。）の「『高度標的型攻撃』対策に向けたシステム設計ガイド」の最新版（以下「高度標的型攻撃対策ガイド」という。）のシステム設計対策セットを十分に理解した上で，各対策セットの適用を検討し，攻撃者が侵入しづらく，内部侵害拡大がしづらいシステム設計を行うこと。また，その設計内容を各機器等の設定に対して確実に反映し，機能させること。

(7)　高度標的型攻撃対策ガイドを十分に理解した上で，ネットワークの設計については，次の表で例示するネットワークセグメントの分離単位を基本とし，適切な設計を行うこと。ただし，現行宮内庁 NWS においては，ハートビート・CSV 用セグメント，ライブ・マイグレーション用セグメントもある。各セグメント間を行き来する通信は，原則不可とし，ユーザが利用する機能又は受けるサービスを滞りなく提供するために必要な通信などについては，必要最小限にするアクセス制御を施すこと。

なお，ネットワークセグメントの分離単位及びアクセス制御の設定内容については，あらかじめ甲と協議の上，決定すること。

NO.	ネットワークセグメント	内容
1	ユーザセグメント	ユーザが利用するクライアント端末が接続されているセグメントのこと。ただし，ユーザセグメントは単一のセグメントではなく，ユーザの所属組織（課室レベル）又は場所や執務室の位置を十分に顧慮してセグメント分けを検討し，情報セキュリティインシデントなどが発生した場合には，封じ込めや侵害を

		最小化できるような設計とする。 原則としてユーザセグメントは，インターネットと直接のリーチャビリティを持たない設計とし，新設する DMZ セグメントを経由して，アクセスを行うネットワーク体系とする。
2	サーバセグメント	各サーバが接続され，ユーザが，ユーザセグメントからクライアント端末を利用し，各サーバ上で動作している各サービスやアプリケーション等を利用することが可能なセグメントのこと。 原則として，各サーバセグメントのサーバ群はインターネットと直接のリーチャビリティを持たない設計とし，宮内庁統合 NW にて新設する DMZ セグメントを経由して，アクセスを行うネットワーク体系とする。
3	運用管理セグメント	運用管理セグメント用端末を接続して運用管理を行うための運用管理専用のセグメントのこと。また，ユーザセグメントからアクセスできないようにアクセス制限を施し，システム管理者のみが使用できる専用ネットワークとし，ユーザ（甲担当者は除く）には公開しない設計とする。運用管理セグメントの構築方法としては，サーバセグメントに接続されている物理的な LAN ポートとは別の LAN ポートからネットワークを構築する方法がある。 なお，現行システムでは，情報システム全体をコントロールできる管理者権限の悪用を防止するため，管理者権限を行使できる端末を統合運用管理端末に限定するため，運用管理セグメントを構築し，他セグメントと分離したネットワークとしている。 なお，運用管理セグメントは，本庁以外にもバックアップサイトとして機能する京都事務所にも存在する。京都事務所に存在する運用管理セグメントについても，運用管理ＷＡＮを設ける，ないしは VPN 装置などで，本庁内の運用管理セグメントと接続し，サービス経路を利用しないよう適切に他のセグメントから隔離を行うこと。

(8) ユーザが利用する業務やアプリケーション，宮内庁 CIS のネットワークの制御及び運用などで不要な通信プロトコル，通信ポート，ソフトウェア上の機能又はサービスを明らかにしてから甲と協議し，甲の承諾を得た上で，停止やブロックするなどの不要な機能を利用不可とする設計を適切に行うこと。

(9) ネットワークスイッチ等のネットワーク機器は，前項(8)で示した不要機能をあらかじめ排除した OS 又はファームウェアを採用し，ユーザの業務が滞りなく遂行でき，宮内庁 CIS のネットワークの制御及び運用などが適切に行うことが可能な必要最低限の機能が実装されたものとすること。

(10) 本調達で導入する HDD 等の補助記憶装置を搭載する機器が，故障・障害等により乙が新規交

換した場合，情報漏出防止のため，交換された HDD 等は甲が処分できること（本号を前提とした契約が可能であること）。

ただし，やむを得ない事情により交換された HDD 等の返却が必要な場合は，事前に甲の承諾を得た上で，甲の立ち会いの下，記録されているデータを完全に消去し，データ消去証明書を提出すること。

(11) 本調達における全ての機器に搭載されるオペレーティングシステム（以下「OS」という。）及びソフトウェアは，次の情報セキュリティに関する情報提供サイト等を参考にし，納入期限までに指摘されている脆弱性やセキュリティホール等に対して修正モジュールの導入など適切な処理を施し，安全なシステムの構築を行うこと。

① NISC から発出される情報
https://twitter.com/nisc_forecast

② 警察庁から発出される情報
https://www.npa.go.jp/cyberpolice/

③ IPA から発出される情報
http://www.ipa.go.jp/security/index.html
http://jvndb.jvn.jp/index.html

④ JPCERT/CC から発出される情報
https://www.jpcert.or.jp/

⑤ JC3 から発出される情報
https://www.jc3.or.jp/info/index.html

(12) 本調達で導入する機器のうち「ウイルス対策機能」を有することが機能要件に含まれる場合には， 以下を満たすこと。

① ウイルス対策ルール（又はパターンファイル）は，自動的に更新されること。

② ウイルススキャンのエンジンは，サーバ機器とクライアント端末とでは異なる製造業者の製品を採用し，ウイルス対策ルール又はパターンファイルの公開時期のずれなどによる対策の遅れを吸収するため，多層型防御による情報セキュリティ対策の強化が可能なこと。

(13) 本業務の実施に当たり，乙又はその従業員，本調達の役務内容の一部を請負等する先，若しくはその他の者により意図せざる変更が加えられないための管理体制が整備されていること。

(14) 乙の資本関係・役員等の情報，受注作業の実施場所に関する情報，受注業務の従事者の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績及び国籍に関する情報を提供すること。

(15) 乙は，受注業務の一部を請負等する場合は，あらかじめ情報セキュリティ管理計画書に相手方を含めた管理体制を記載の上，提出し，甲の承諾を受けること。また，再請負の相手方から更に第三者に請負が行われる場合においても同様とする。

なお，再委託先の変更等を行う必要が生じた場合は，情報セキュリティ管理計画書の該当部分を変更の上，甲に提出し，承諾を受けること。

(16) 情報セキュリティインシデントへの対処方法が確立されていること。

(17) 情報セキュリティ対策その他の契約の履行状況を定期的に確認し，甲へ報告すること。

(18) 乙の講ずる情報セキュリティ対策が甲の所有するポリシー等の基準を満たしていない場合には，乙は，甲と協議の上で追加的なセキュリティ対策を講ずること。

(19) 本調達に係る業務の遂行における情報セキュリティ対策の履行状況を確認するために，甲が情

報セキュリティ監査の実施を必要と判断した場合は，甲がその実施内容（監査内容，対象範囲，実施等）を定めて，情報セキュリティ監査を行う（甲が選定した事業者による監査を含む。）。また，乙は自ら実施した外部監査についても甲へ報告すること。

情報セキュリティ監査の実施については，これらに記載した内容を上回る措置を講ずることを妨げるものではない。

(20) JPCERT/CC「攻撃者が悪用する Windows コマンド(2015-12-02)」を参考にして，ユーザのクライアント端末に必要のない Windows コマンドを，AppLocker やソフトウェア制限ポリシー等を使用して制限することで，攻撃者による悪用を低減すること。

https://www.jpcert.or.jp/magazine/acreport-wincommand.html

制限するコマンドの選定は，契約後，甲担当者と協議の上，決定する。

1.15.2.情報セキュリティが侵害された場合の対応

(1) 情報セキュリティインシデントが発生した場合に備え，連絡・報告フロー，体制，対応手順等を明示した提出成果物を提出の上，甲担当者の承諾を得ること。また，提出成果物には，次の項目を記載することとし，その他必要と考えられる項目も記載すること。

(ア) 標的型攻撃

(イ) 不正アクセス

(ウ) 情報漏えい

(エ) 未知のマルウェア感染

(オ) 既知のマルウェア感染

(2) 本調達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又はそのおそれがある場合には，速やかに甲担当者へ報告し，甲担当者と協議を行いつつ対応を行うこと。これに該当する場合には，次の事象を含む。また，甲担当者が必要とする情報を開示すること。

(ア) 乙に提供し，又は乙によるアクセスを認める甲の情報の外部への漏えい及び目的外利用

(イ) 乙による甲のその他の情報へのアクセス

1.15.3.その他

その他，情報セキュリティ対策について，本調達仕様書（案）「1.2.背景と目的」の実現のために有効かつ必要な提案を具体的に行うこと。

1.16.宮内庁 NWS の運用管理業務

宮内庁 NWS の運用管理業務は，公共サービス改革法の「官民競争入札対象公共サービス」に該当する。また，乙は，公共サービス改革法の「公共サービス実施民間事業者」に該当する。

1.16.1.運用管理業務開始時期

乙は，宮内庁 NWS の運用管理業務は，2020 年 2 月 1 日から開始すること。

なお，乙は，2020 年 2 月 1 日から円滑に滞りなく宮内庁 NWS の運用管理業務が開始できるよう，宮内庁 CIS の構築期間中から宮内庁 NWS の運用管理業務に必要となる事項の洗い出しを行い，それらに対して必要な対策を事前に講じ，十分に準備を行うこと。

1.16.2.実施

1.16.2.1 実施

(1)　乙は，公共サービス改革法の第 24 条に基づき，宮内庁 NWS の運用管理業務を実施しなければならない。

(2)　乙は，公共サービス改革法の第 25 条に基づき，秘密保持義務等を負う。

1.16.2.2 実施場所

運用管理を行う主な実施場所は，東京都千代田区千代田 1-1　宮内庁庁舎内情報管理室（以下「情報管理室」という。）とする。

1.16.3.成果物

(1)　乙は，以下の成果物を納品すること。ただし，それぞれの納品時期については，契約締結後速やかに甲と乙が協議し，甲が承諾した上で定めるものとする。ただし，①，②については，契約締結後，運用管理業務開始 10 日（休日を除く）前までに遅滞なく提出すること。

①　運用管理計画書

②　サービスレベル合意書(SLA)

③　サービスレベル報告書

④　運用管理報告書（週次，月次）

⑤　改善提案書

⑥　その他，運用管理作業において作成・更新した各種資料

(2)　成果物は全て日本語表記とし，紙媒体及び甲の指示する電子媒体をそれぞれ 2 部ずつ作成すること。

1.17.創意工夫の発揮

本業務を実施するに当たっては，以下の観点から提案を行い，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。

(1)　宮内庁 NWS の運用管理業務に対する提案

乙は，運用管理業務の実施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。

(2)　運用管理業務以外に対する改善提案

乙は，運用管理業務以外に関して，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，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。

2.　特記事項

2.1.基本事項

(1)　本調達仕様書（案）「1.4.背景と目的」に沿い，本調達の設計・構築・稼働・運用に必要と認められる事項については，本調達仕様書（案）に記載なき事項であっても，具体的に提案を行うこと。

(2)　創造宣言に基づき，宮内庁 NWS の運用コストについて，平成 25 年度に比して 3 割削減達成を目指し，宮内庁 CIS の保守及び運用効率の最大化を図ることを設計段階から考慮しつつ，本調達仕

様書（案）「1.11.成果物」の各文書に適切に反映することにより，本調達仕様書（案）「1.4 背景と目的」における各目的の実現を達成すること。

(3) 本調達システムでは，次の事項に基づきつつ，宮内庁 NWS の全体最適に資する設計を行うこと。

① 現行宮内庁 NWS に導入されているサーバについて，「13.資料閲覧」時に，これまでの各リソースの使用状況（平均，ピーク，時間変化）等を把握し，CPU，メモリ等の主記憶装置，HDD 等の補助記憶装置，外部インタフェースの種類やポート数等の拡張余地（上限値）に係るハードウェア仕様が，アプリケーションプログラムの機能要件やユーザの業務量に照らして，過大となっていないか，サーバのハードウェアのグレードが適正な範囲に収まっているかを確認した上で，定量的かつ具体的に根拠を示しつつ本調達におけるサーバリソースのサイジングの実施及び全体最適な情報システムの設計を行うこと。

なお，ハイパースレッディングや仮想化技術を用いる場合には，用いない場合と比較して CPU 使用率の表示の特異性を考慮した上でサイジング及び設計を行うこと。

② 次に例示する情報に留まらず，最新の技術及び製品の動向を十分に調査した上で，前項①と相まってハードウェアのコスト削減を図ること。「平成 27 年版　情報通信白書（総務省）」によれば，次のとおり。

ア　データ伝送速度が指数関数的に向上し，固定ネットワーク，モバイルネットワークともにあらゆるデータが瞬時に共有可能な状況になってきている。

イ　コンピューティング分野は，いわゆる「ムーアの法則」に従い CPU 等の計算能力が指数関数的に向上するとともに，データを蓄積するストレージの大容量化も進んできた。

ウ　ムーアの法則：世界最大の半導体製造業者 Intel 社の創設者の一人であるゴードン・ムーア博士が 1965 年に経験則として提唱した「半導体の集積密度は 18～24 か月で倍増する」という法則。

エ　HDD やフラッシュメモリ，光ディスクなどに代表されるデータの記憶・保存に係る記憶装置等の製品においても同様の変化がみられる。2000 年以降は，面積あたりの記憶機密度は年率 30%～50%の増加率で向上しており，これに伴い記憶装置の単価の減少が続いている。市販の HDD の GB あたり単価に換算すると，1985 年から 30 年間で約 100 万分の 1 まで下がっている。

オ　Less’s Law：ムーアの法則と対比させ Less’s Law として，ストレージは 12 か月でコストが半減し，同時に容量が 2 倍になるという法則として言及されることがある。

(4) 本調達で要求する機能要件及び性能要件を満たし，宮内庁統合 NW の技術的仕様及び設計・設定内容を十分に理解した上で，1，200 名規模で利用するのに十分な処理性能を提供するため，本調達仕様書（案）に記載する機器等以外の新たなハードウェア又はソフトウェアの追加あるいは構成を変更しても構わない。その場合，新たに追加したハードウェア又はソフトウェアの製品資料及び機能証明書を提出し，その機能を採用する理由及び効果を提案書に具体的に記載すること。

2.2.機器等の選定

2.2.1.オンプレミス

宮内庁 CIS で導入されるオンプレミスの機器について記載する。

(1) 本調達機器等は中古品でないものとする。

(2) ネットワークの管理やアプリケーション等での通信に利用される，OSI 参照モデルのデータリンク層より上位（レイヤ 3 以上）の通信プロトコルは，IPv4(RFC 791)及び TCP(RFC 793)又は UDP(RFC

768)（以下「TCP/IP」という。）を基本とする。

なお，レイヤ 3 以上で，コスト削減及び運用管理業務の効率化の実現が可能な通信プロトコルを採用するのであれば，TCP/IP 以外の通信プロトコルを基盤として採用を阻害するものではない。ただし，TCP/IP 以外の通信プロトコルを基盤として採用した場合であったとしても，インターネット接続を可能とし，サーバ機器及びクライアント端末などが TCP/IP での通信が可能なこと。

(3) 本調達機器等の構成について，構成品一覧を提示し甲の承諾を得ること。（製造事業者等の製品型番が分かる品目表を提出すること）。

(4) 同一の種類の機器に関しては，オーバースペックにならないよう適材適所での設計に配慮し，保守性を高める観点から，可能な限り機種又はシリーズを揃えること。

(5) 同一種類のソフトウェアについては，可能な限りバージョンを統一すること。

(6) 本調達機器等は省スペース設計であること。

(7) 本調達機器等は省電力設計であること。

なお，提案を行う各ハードウェアの消費電力を示す資料を添付し，最大消費電力を具体的に示すこと。

(8) 本調達及びその構成，配置については，運用管理環境を考慮して，最適化を図るとともに，最新の技術を採用すること。

(9) ハードウェア及びソフトウェアは，製造事業者等による製品の動作が保証又は確認されたものであること。ただし，製造事業者等による製品の動作の保証又は確認ができない場合には，提案書の提出時までに応札者の検証環境での結果又は過去の実績から動作の証明が可能であるならば，その証跡を提出すること。

(10) 本調達で採用するソフトウェアのバージョン確定に当たっては，甲と協議すること。また，バージョン確定後から納入期限までにバージョンアップ又はパッチ適用の必要性があることが確認された場合には，動作確認が済んでいるものに限り，甲の承諾を得た後，最新バージョンとすること。

(11) 納入期限までに発見された本調達機器等の不具合や問題については，乙の責任と負担において迅速に対応すること。

(12) 本調達機器等に欠陥があった場合は，迅速に物品交換等の対応をとること。

(13) 本調達機器等に搭載されるハードウェア及びソフトウェアについて，納入期限までに指摘されているセキュリティホール等に関して，修正モジュールの導入など，適切な処理を施すこと。

(14) サポートライフサイクルポリシーが公表されているハードウェア及びソフトウェアについては，本調達の賃貸借期間終了まで対策用ファイルの提供が継続されると見込まれるハードウェア及びソフトウェアを選定すること。また，適宜入手したサポートライフサイクルポリシーの情報から必要と判断した場合は，後継となるハードウェア及びソフトウェアへの更新等の計画を策定すること。

(15) サポートライフサイクルポリシーが公表されていないハードウェア及びソフトウェアについては，後継となるハードウェア及びソフトウェアの有無や販売等開始からの経過年数等を考慮するなどして，本調達の賃貸借期間終了まで対策用ファイルの提供が継続されると見込まれるハードウェア及びソフトウェアを選定すること。また，後継となるハードウェア及びソフトウェアの販売等に関する情報を適宜入手し，当該情報を考慮して，後継となるハードウェア及びソフトウェアへの更新等の計画を策定すること。

(16) 本調達機器等の設置及び導入後の基本動作確認は，乙の責任と負担において対応すること。

(17) 納入するハードウェアの設置・接続に必要な接続器具やケーブル等は，乙の負担において必要数

供給すること。

(18) 本仕様を満たす機器等は，仕様を満たす増設機器として，メモリ等主記憶装置及びハードディスク等補助記憶装置等を全て取り付けた形で，正常動作の確認を行った上で納入すること。

なお，LAN ケーブル等の既設の接続方法を継続使用可能なものについては，原則として既設の接続方法を使用するものとする。

(19) 本調達機器等は，人体に危険がないものであること。

(20) 本調達機器等は，原則として単相 100V 商用電源を使用するものであること。

(21) 本調達機器等は，原則として特別な空調設備を必要とせず，支出負担行為担当官の指定する場所に設置可能であること。

(22) 本調達機器等は，ハードウェア，ソフトウェアともに，原則として日本語対応のものであること。

(23) 導入する機器は ISO9001 を取得した組織にて製造された製品であること。

(24) 導入する機器を構成するハードウェア及び実装されるソフトウェアのうち，JIS 等の国内規格，ISO 等の国際規格に定めのある製品については，当該規格に準拠していること。

(25) 各種災害(地震等)対策等を十分に考慮し，安全かつ信頼性のあるシステムを構築し，可用性と保守性の高い運用管理を可能にすること。

(26) 将来におけるハードウェア，ソフトウェアの増強，ネットワークの拡大，接続機器の増設及び拡張のため，互換性，移植性，接続性を確保でき，柔軟に対応できるよう標準化が考慮されていること。

(27) 甲においては，「電子政府システムの IPv6 対応に向けたガイドライン（平成 19 年 3 月 30 日総務省）http://www.kantei.go.jp/jp/singi/it2/cio/dai24/24siryou4-2.pdf」により，宮内庁 NWS に含まれる他のシステムとの運用管理面での整合性を保ちつつ，IPv6 対応を進めることとし，当面は IPv4 を念頭にシステムの稼働を行う。

なお， ネットワーク機器については，RFC 8200 を基本仕様とした IPv6 に対応済み，若しくは，将来的にソフトウェアのバージョンアップ等により IPv6 に対応できる機器を選定すること。また，その他の機器についても，可能な限り IPv6 に対応できる機器を選定することとする。

(28) ネットワークは，OSI 参照モデルの物理層（レイヤ 1）及びデータリンク層（レイヤ 2）は，IEEE 802.3 ETHERNET WORKING GROUP (http://grouper.ieee.org/groups/802/3/)にて標準化された技術を基本とする。

(29) 調達するソフトウェアは，原則として日本語に対応していること。ただし，日本語に対応していない場合には，利用，運用，管理，保守を行うのに必要十分な手順書等を乙が日本語で提供すること。また，乙が提供する日本語手順書等については，利用実態及び製造事業者等の提供する手順書等の変更にあわせ，必要に応じて修正を行うこと。

(30) 応札者が提案するソフトウェアについては，製造事業者等が提供する政府・公共機関を対象としたプログラムを適用し，ソフトウェアライセンス管理の集約化による負荷の軽減及び投資対効果の向上を図ること。導入予定のソフトウェアについて，甲のライセンスの保有状況を確認し，ライセンスを保有している場合には，既存ライセンスを最大限有効活用し，コスト削減を図ること。

2.2.2.クラウドサービス

本調達において，クラウドサービスを採用する場合は，次に示す要件を満たすこと。また，本調達における契約期間終了後も，本調達において利用するクラウド環境を契約期間終了前に契約の延長手続き

等を実施することにより，そのまま継続利用することが可能なこと。

(1) 日本国内に物理的に設置され，運用されていること。

(2) 準拠法を日本の法律とすること。

(3) 管轄裁判所を日本国内の裁判所とすること。

(4) ISO/IEC 27001 に準拠し，ISMS 審査機関による認証を証明できること。

(5) IaaS サービスを提供する場合は ISO27017 に準拠していること。

(6) 「クラウドサービス利用のための情報セキュリティマネジメントガイドライン（2013 年度版経済産業省）http://www.meti.go.jp/press/2013/03/20140314004/20140314004-2.pdf」に対し，乙は主に「クラウド事業者の実施が望まれる事項」について可能な限り遵守すること。

なお，遵守することができない内容については，甲に対してあらかじめ該当箇所を示した上で理由の詳細と可能な限り代替策等を報告すること。

(7) 情報資産の所有権がクラウドサービス事業者に移管されるものではないこと。したがって，甲担当者が要求する任意の時点で情報資産を他の環境に移管させることができること。

(8) 採用するクラウドサービスを選定する際には，事前にクラウドサービスプロバイダに第三者へのクラウド環境の引継ぎ等の手続きについて確認した上で，乙，運用管理事業者及び甲へのクラウド環境の引継ぎに遺漏が無いよう，クラウドサービスプロバイダとの契約内容や引継ぎ手順等を整備しておくこと。

(9) 法令や規制に従って，クラウドサービス上の記録を保護すること。

(10) 情報資産が残留して漏えいすることがないよう，必要な措置を講じること。

(11) 自らの知的財産権についてクラウド利用者に利用を許諾する範囲及び制約を，契約の締結前に甲担当者に対して正確に説明し，確認を行うこと。

(12) インターネット回線接続サービス及び宮内庁 WAN の通信回線接続サービスの技術的仕様及び設計・設定内容を十分に考慮した上で，クラウドサービスを 1,200 名規模で利用するのに十分な処理性能を提供し，ユーザの業務遂行が効率的かつ確実に可能なこと。

(13) クラウドサービスへのアクセス制限を指定した IP アドレス等に基づいて可能なこと。また，アクセス制御の設定を適切に行い，情報セキュリティ対策を確実に行うこと。

(14) 業務継続性を確保するため，本調達においてバックアップサイトをクラウドサービス型で提供する場合は，バックアップサイトについても上記(1)～(13)を満たすこと。

なお，バックアップサイトをクラウドサービス型で提供する場合は，本調達のメインシステムが物理的に設置された場所と異なる同時被災しない場所に設置され，運用されていること。

2.2.3.データセンタ仕様

本調達にオンプレミスの機器を宮内庁の外部のデータセンタに設置して提供する場合は，次の仕様を満たすこと。また，本調達における契約期間終了後も，本調達において利用するデータセンタ環境を契約期間終了前に契約の延長手続き等を実施することにより，そのまま継続利用することが可能なこと。

(1) 日本国内に物理的に設置され，運用されていること。

(2) 当庁から 50Km 以内の距離に存在し，必要に応じて駆けつけが可能なこと。

(3) データセンタ専用の建物であり制震又は免震構造であること。

(4) データセンタ設置エリアは活断層及び航空機発着航路に設定されていないこと。

(5) データセンタ専用の自家発電設備を有し，48 時間以上の無給油発電が可能なこと。

(6) データセンタのルーム内への入室には 2 種類以上の認証装置を経由し，生体認証等による入室制限を行うことが可能なこと。

(7) データセンタの入口，サーバ室への入室扉前には，監視カメラが設置されており，常時監視されていること。

(8) データセンタのラックは，当庁専用のラックとし他と共用しないこと。

(9) 可能な限り，甲からの書面等の申請に応じて，甲担当者が入室することが可能なこと。

(10) データセンタは，データセンタ運営・維持管理業務において，事業継続の国際規格 ISO22301 を取得した事業者が提供していること。

(11) データセンタへ設置した機器に対する運用管理業務が，情報管理室から十分に情報セキュリティ対策を施した上でリモートで実施できること。

2.3.オペレーティングシステムの集約化

2.3.1.クライアント端末

(1) 本調達で調達するクライアント端末の OS（以下「クライアント OS」という。）は，業務継続性，宮内庁 NWS の運用効率性及び安定性の観点から現行 OS に準拠したマイクロソフト社製 Windows 10 Enterprise 64bit 又はこれと同等以上の性能・機能を有する製品を搭載すること。

(2) クライアント OS は，全て同一のエディション及びバージョンで揃えること。

(3) クライアント OS の品質や機能等が起因となった障害が発覚した場合に，その製造事業者等が責任をもって迅速に対処できること。

(4) クライアント OS において脆弱性が発覚した場合に，その製造事業者等が責任をもって迅速に対策パッチの提供を行い，この周知を遅滞なく実施可能なこと。

(5) JPCERT/CC「ログを活用した Active Directory に対する攻撃の検知と対策」36 頁「Active Directory に対する攻撃の対策」の表の予防策を実施すること。

2.3.2.サーバ

(1) 原則として，本調達システムで採用するサーバの OS は，Windows 系 OS のうちサーバ用として 1 種類，UNIX 及び UNIX の派生 OS，又は Linux を含む UNIX に類似したシステム体系を持った OS(以下「UNIX 系 OS」という)のうち 1 種類とを合わせて，計 2 種類(以下「標準サーバ OS」という)に集約し，保守及び運用の効率化を図ること。ただし，提供される機能に特化したアプライアンス型のサーバについては，この限りではない。また，現行アプリケーションを動作させる上でやむを得ない理由がある場合に限り，甲の承諾を得た後，別バージョンを導入することを可とする。

(2) ライセンス料金体系及びその制約条件やライフサイクルなどを十分に理解し，サーバ・ハードウェアのサイジングと合わせ，全体最適かつ本調達システムが安定稼働するのに必要な設計となるライセンス数を過不足なく用意すること。

(3) 標準サーバ OS のうち，Windows 系 OS の場合は，次の条件を満たすこと。

現行宮内庁 NWS の構成を参考にしつつ，本調達仕様書（案）における課題の解決，要件を満たす上で必要となる数量の CAL も調達すること。

(4) 標準サーバ OS のうち，UNIX 系 OS の場合は，次の条件を満たすこと。

（ア） ユーザ数と同規模以上の組織・団体における情報システムにおいて，十分な利用実績があること。

（イ） ISO/IEC15408 の評価保証レベル（EAL）において，EAL4 以上の認証を取得している（IPA または CCRA のポータルサイト等で確認が可能である），あるいは今までに EAL4 以上の認証を取得した実績のある OS の後継 OS であること。

(5) 標準サーバ OS の品質や機能等が起因となった障害が発覚した場合に，その製造業者が責任をもって迅速に対処できること。

(6) 標準サーバ OS において脆弱性が発覚した場合に，その製造業者が責任をもって迅速に対策パッチの提供を行い，この周知を遅滞なく実施可能なこと。

(7) 仮想化技術を採用する場合には，次のことを満たすこと。

（ア） 保守・運用性の向上を図るため，仮想化技術として採用するハイパー・バイザの種類は，一つだけとすること。

（イ） ハイパー・バイザ上で，標準サーバ OS 及びクライアント OS がゲスト OS として正常に動作することの確認がとれていること。

（ウ） 異なるサーバ・ハードウェア間で，同一製造業者のハイパー・バイザであれば，仮想マシンのインポート又はエクスポートによる容易なサーバ・ハードウェアの移行が可能なこと。

（エ） 異なるサーバ・ハードウェア間で，同一製造業者のハイパー・バイザであれば，仮想マシンを停止させることなく，別のサーバ・ハードウェアへ移動することが可能なこと。

（オ） 業務継続性の向上の観点から，本調達システムの運用開始後，拠点間でのクラスタ構成が可能なこと。

（カ） 投資対効果を最大化するため，本調達システムの運用開始後，ハイパー・バイザを搭載するサーバ・ハードウェアの CPU，メモリ等の主記憶装置，HDD 等の補助記憶装置及び外部インタフェース等のリソースの使用状況の実測値を監視し，必要に応じて設定変更を行い，最適なリソースの割当てが可能なこと。

（キ） 投資対効果を最大化するため，本調達システムの運用開始後，ハイパー・バイザを搭載するサーバ・ハードウェアの CPU，メモリ等の主記憶装置，HDD 等の補助記憶装置及び外部インタフェース等のリソースの使用状況に余裕（以下「余裕リソース」という。）がある場合，この余裕リソースに対して新たな仮想マシンの割当てが可能なこと。

(8) 標準サーバ OS 及びハイパー・バイザは，本調達時点で販売されており，かつ本調達システムの賃貸借期間内において，ソフトウェアのアップデート（サービスパック及びセキュリティパッチ）の提供等販売元からのサポートが保証されていること。

2.3.3.ネットワークスイッチ

(1) 本調達で調達するネットワークスイッチのファームウェアは，業務継続性，システムの運用効率性の観点から，管理手段として，可能な限り同様なコマンド操作が可能なインタフェース（CLI）又は Web インタフェースを実装した製品で揃えること。

(2) 本調達で調達するネットワークスイッチのファームウェアの品質や機能等が起因となった障害が発覚した場合に，その製造事業者等が責任をもって迅速に対処できること。

(3) 本調達で調達するネットワークスイッチのファームウェアにおいて脆弱性が発覚した場合に，その製造事業者等が責任をもって迅速に対策パッチ又は対処済みファームウェアの提供を行い，この周知を遅滞なく実施可能なこと。

2.4.サーバ機器の集約化

宮内庁 CIS においては，現行宮内庁 NWS よりサーバの物理的台数を集約化し，ハードウェアリソースをより効率的に利用することにより，コスト削減を実現すること。

なお, 宮内庁 CIS を構成するサーバ, アプライアンス機器等の集約化に当たっては, 現行宮内庁 NWS の構成の見直しを行っても構わないとする。ただし，サーバ機器の集約化に当たっては，集約化後の構成でも現行宮内庁 NWS と同等以上の実効性能とし，宮内庁 CIS の契約期間中を考慮した実効性能を有すること。

3. システム要件

3.1.サーバ機能共通要件

各サーバ機能の共通仕様を以下に示す。

3.1.1.共通仕様

(1) サーバ用 OS の選択は，本調達仕様書（案）「2.3.オペレーティングシステムの集約化」に従い，また，以下を満たすこと。

① Windows 系のサーバ用 OS を採用する場合には, Windows Server 2016 以降であること。また，この場合のサーバを，以下「Windows 系サーバ」という。

② UNIX 系のサーバ用 OS を採用する場合には， Linux kernel のバージョンは 3.10 以降であること。

③ 仮想化技術を採用する場合には, 前項①と②のサーバ用 OS がゲスト OS として正常に動作することの確認がとれていること。

なお，本調達仕様書（案）「1.5.3.2 サーバの集約化による運用管理業務の軽減」に示したとおり，現行宮内庁 NWS では仮想化技術を採用している。

(2) 本調達仕様書（案）「3.12.1.機能要件」を満たすウイルス対策機能を有すること。

(3) バックアップサーバ機能と連携する場合には，システムを停止することなく，OS を含むシステムエリア，ユーザデータエリアのデータバックアップが可能なこと。障害時にはバックアップしたデータからリカバリが可能なこと。

(4) NTP 又は SNTP による時刻同期が可能なこと。

(5) ログレポート機能として，HTTP，Syslog， SNMP，SMTP メールのいずれかに対応していること。

(6) Windows 系のサーバ用 OS を採用する場合には，タスクスケジューラのログをレポート可能なこと。

(7) UPS の管理機能を有し，停電を検出した場合にはシステムを自動的にシャットダウンできること。

(8) 設定管理（コンソール）機能は，本調達仕様書（案）「3.1.3. コンソール（キーボード・ディスプレイ・マウス）機器要件」への接続，又はネットワークを介して使用できること。

3.1.2.サーバ機器構成要件

(1) 本調達システムの各サーバ機能を実現するためのサーバ機器は，それぞれ，「別紙 4 本調達機器及び各事業者の役割範囲」に示された現行宮内庁 NWS における各サーバの構成要素（CPU，メモリ，HDD 等の補助記憶装置，データ通信用ネットワーク・インタフェース等）以上の性能

及び容量又は数量を有し，本調達システムの契約期間中の利用率変化（利用推移）をあらかじめ考慮した構成とすること。

(2) 本調達仕様書（案）「2.4.サーバ機器の集約化」に従い，各サーバ機器の集約化を行う場合には，以下の要件を満たすこと。

① 集約化後のサーバ機器上の全てのサーバ機能が，同時に，現行宮内庁 NWS における各サーバ機能を実装したサーバ機器の CPU，メモリの最大リソース量と同等程度のリソース消費をそれぞれ発生させたとしても，ユーザの業務に支障なく，集約化後のサーバ機器が安定稼働可能となる性能の CPU，メモリを有すること。

② 集約化後のサーバ機器上の全てのサーバ機能が，同時に，現行宮内庁 NWS における各サーバ機能を実装したサーバ機器上のディスク I/O（Input/Output），データ通信用ネットワークの最高データ転送速度（最大帯域幅）と同等程度のデータ転送量をそれぞれ発生させたとしても，ユーザの業務に支障なく，集約化後のサーバ機器が安定稼働可能となる性能の HDD 等の補助記憶装置，データ通信用ネットワーク・インタフェースを有すること。

③ 集約化後のサーバ機器に搭載される HDD 等の補助記憶装置の容量は，サーバ機器を集約したことによるディスク利用率が向上するような設計を行い，本調達システムの契約期間を考慮した構成とすること。

④ 仮想化技術を採用した場合の要件を以下に示す。

- 各サーバ機能の冗長化や連携が有効に働くよう考慮した設計とすること。
- 仮想化技術で集約化されたサーバ機器が停止した際，他の物理的に異なるサーバ機器で，その停止した仮想化されたサーバ機能を収容し，自動的に再起動することにより，業務継続性を向上させる機能を有すること。同様に，一つの仮想化されたサーバ機能が停止した場合においても同様な機能を提供可能なこと。

(3) 補助記憶装置は耐障害性や性能を考慮し，RAID1/1+0/5/6 等から適切な構成とすること。

(4) 補助記憶装置はホットプラグ対応であること。

(5) DVD スーパーマルチ 2 層対応ドライブ（8 倍速以上の DVD-R，4 倍速以上の DVD-RW，24 倍速以上の CD-R，10 倍速以上の CD-RW）を有すること。

なお，同等の機能を有する外付け DVD スーパーマルチ 2 層対応ドライブを用いることも可とする。

(6) 管理用ネットワーク・インタフェースとして，IEEE802.3 規格に準拠した 10BASE-T/100BASE-TX のポートを 2 つ以上有すること。

(7) データ通信用ネットワーク・インタフェースとして，IEEE802.3 規格に準拠した 1000BASE-T のポートを 2 つ以上有すること。

なお，各サーバ機能のサーバ機器の集約化を行う場合には，本調達仕様書（案）3.1.2.(2)を満たすためのポート数を有すること。

(8) USB2.0 又は USB3.0 のポートを 2 つ以上有すること。

(9) EIA 規格準拠 19 インチラックに搭載可能なこと。また，サーバ機器の盗難及び不正な持ち出しを防止するため，盗難を防止可能な措置を実施すること。防止策は、筐体本体及びディスク等データの格納されている領域に対する措置を実施すること。

(10) 電源装置が冗長化されていること。

(11) 電源装置はホットプラグ対応であること。

(12) 冷却ファンが冗長化されていること。
(13) 本調達仕様書（案）「3.2.無停電電源装置（UPS)」の要件を満たし，応札者が提案するサーバ機器の電源容量及び台数に適した UPS を過不足なく用意すること。
(14) 本調達仕様書（案）「3.1.3. コンソール（キーボード・ディスプレイ・マウス）機器要件」を満たした機器と接続可能かつ操作可能なこと。
(15) HDD 等の補助記憶装置が故障等により交換が必要になった場合には，本調達仕様書（案）「1.15.1 情報セキュリティの確保(10)」を満たす対応が可能なこと。

3.1.3.コンソール（キーボード・ディスプレイ・マウス）機器要件

(1) 一つの拠点にて複数台のサーバ機器を設置する場合には，サーバ機器の設定管理の作業を効率的に行うため，KVM スイッチを用意することにより，キーボード，ディスプレイ（ビデオ），マウスを共有して使用できること。
(2) KVM スイッチを用いる場合には，サーバ機器台数以上の KVM スイッチのポートの数を用意し，各サーバ機器と KVM スイッチの接続に必要となるケーブルを過不足なく用意すること。
(3) ディスプレイは液晶 15 インチ以上，解像度 1024×768 以上であること。
(4) キーボードは，OADG 標準又は JIS 標準配列に準拠若しくは同等品であること。
(5) キーボード，ディスプレイ，マウスのそれぞれの数は，サーバ機器の台数及び KVM スイッチの有無を考慮し，過不足なく用意すること。
(6) EIA 規格準拠 19 インチラックに搭載可能なこと。

3.2.無停電電源装置（UPS）

本調達仕様書（案）の各サーバ機能を搭載したサーバ機器に接続する UPS の標準仕様を，以下に示す。

(1) サーバ機器等で電源を二重化した機器については，UPS を複数台準備し，異なる UPS に接続すること。
(2) UPS に接続するサーバ機器の定格電流・電圧及び電源プラグ（入力端子）の形状に適合すること。
(3) 停電時，自動的にバックアップ電源に切り替わり，接続している全てのサーバを自動的かつ安全にシャットダウンさせる機能を有すること。
(4) 瞬間的な停電，及び短時間（1～2 分程度）の停電時においても，バックアップ電源に切り替り給電できること。
(5) 指定時刻に自動的に電源投入・切断可能なカレンダー機能を有すること。
(6) 復電時，UPS に接続されている機器を自動復旧させる機能を有すること。
(7) IEEE802.3 規格に準拠した 10BASE-T/100BASE-TX の管理用ポートを一つ以上持つこと。
(8) EIA 規格準拠 19 インチラックに搭載可能なこと。

3.3.サーバセグメント用サーバ・ネットワークスイッチ

サーバセグメント用のサーバ・ネットワークスイッチとして，次の機能及び仕様を満たし，かつ，宮内庁統合 NW にて調達を行ったコア・ネットワークスイッチと接続して機能するものを冗長構成にて

提供すること。

3.3.1.一般機能要件

(1) 96Gbps 以上のスイッチファブリックを実装する固定ボックス型のレイヤ 2 以上に対応したスイッチ製品であること。
(2) レイヤ 3 パケット転送能力として 70Mpps 以上を有すること。
(3) IEEE802.1q VLAN Tagging に準拠していること。
(4) STP として，IEEE802.1d，IEEE802.1w，IEEE802.1s にそれぞれ準拠したスパニングツリー機能を有すること。
(5) IEEE802.1x に準拠した認証機能を有すること。
(6) IEEE 802.3x に準拠した全二重イーサネットにおけるフロー制御機能を有すること。
(7) IEEE 802.3ad Link Aggregation 機能を有すること。
(8) IEEE802.1p の優先制御機能を有すること。
(9) Round Robin 又は Strict Priority Queuing 等の QoS に対応していること。
(10) トラフィックの流量を制限（Rate Limit）する機能を有すること。
(11) DHCP リレー機能を有すること。
(12) 送信元及び受信元の MAC アドレス及び IP アドレス，TCP/UDP ポート番号，又はこれらのフィールドの任意の組み合わせに基づくパケットフィルタ機能を有すること。
(13) ポリシーベースルーティング機能を有すること。
(14) VLAN ID は，4,000 以上利用可能であること。
(15) 9,000Byte 以上のジャンボフレームに対応していること。
(16) 10,000 以上の MAC アドレスに対応していること。
(17) IPv4 ルーティングテーブル数が 11,000 以上に対応していること。
(18) ハードウェアで 1 ポートあたり 4 つ以上のキューに対応していること。

3.3.2.インタフェース仕様

(1) IEEE802.3 規格に準拠した 10BASE-T/100BASE-TX/1000BASE-T インタフェースを有し，SFP インタフェースを有すること。
(2) SFP インタフェースは，IEEE802.3 規格に準拠した 1000BASE-SX/LX に対応可能であること。
(3) EIA 規格準拠 19 インチラックに搭載可能であること。

3.3.3.セキュリティ機能要件

(1) 予期していないポートで BPDU を受信した際，ループを防ぐためにそのポートを自動的にダウンする機能を有すること。
(2) スイッチの追加等により期待されていない BPDU を受けルートブリッジが変更されてしまう事態を防止する機能を有すること。
(3) 光ファイバやツイストペアケーブルの単一方向リンク（片対障害）検出機能を有すること。
(4) ポートごとに通信可能な MAC アドレス，又は MAC アドレス数を制限する機能を有すること。

(5)　MAC アドレスと IP アドレスのマップをスイッチ上で管理することによって偽造 ARP による不正な通信盗聴（ARP スプーフィング）を防止する機能を有すること。

(6)　特定のポートの DHCP スヌーピングを介して取得した IP アドレスのみを許可することで，不正な接続（IP スプーフィング）を防止する機能を有すること。

(7)　不正な DHCP サーバの接続や DHCP メッセージを使った DoS 攻撃を防止する機能を有すること。

3.3.4.ネットワーク管理機能要件

(1)　シリアル接続によるコンソールポートを有すること。

(2)　Telnet / SSH によるリモート・コンソール機能を有すること。

(3)　トラフィック解析のためポートのミラーリング機能を有し，同一筐体内のみならず，他の筐体のポートもリモート・ミラーリングできる機能を有すること。

(4)　ソフトウェア及び設定情報を TFTP にてアップロード及びダウンロードする機能を有すること。

(5)　NTP 又は SNTP による時刻同期が可能なこと。

(6)　DNS を参照し IP アドレスの代わりにホスト名を使用できる機能を有すること。

(7)　Syslog サーバにメッセージを送信する機能を有することこと。

(8)　SNMP による管理機能を有すること。

(9)　SSHv1/v2 機能を有すること。

(10)　RMON を使った管理機能を有すること。

(11)　隣接するデバイスとの間で，トポロジの管理を行う機能を有すること。

(12)　近隣ノードの自動検知が可能な IEEE 802.1ab LLDP に対応し，ネットワーク管理の効率化が可能なこと。

3.3.5.信頼性要件

(1)　電源部を冗長化し，一方に障害が発生した場合にも機体が通常どおり稼動できること。
なお，電源部の冗長化の方法は，スイッチ筐体の内部と外部のどちらでも構わない。

(2)　動作温度が 0℃～40℃に対応していること。

(3)　動作湿度が 10%～90%に対応していること。

(4)　VCCI クラス A に準拠していること。

(5)　起動時に POST 等の自己診断プログラムによる自己診断機能を有すること。

3.3.6.構成要件

(1)　応札者が提案する宮内庁本庁及び京都事務所での各サーバの構成及びサーバセグメントの設計にあわせつつ，宮内庁 NWS が適切に機能するために十分なポート数を用意し，必要に応じて適切な SFP トランシーバのメディアタイプを過不足なく用意すること。
なお，未使用となるポート数は，スイッチに搭載されている全てのポート数に対して 40%以下とすること。

(2)　サーバスイッチとコアスイッチとの間は，リンクアグリゲーションプロトコル（IEEE 802.3ad）を使用し，実効スループットで 4Gbps 以上の帯域まで利用できること。

(3)　ホットスタンバイによる冗長構成とし，冗長経路において物理的なネットワークのループが構成される場合には，論理的にイーサネットフレームのループでのやり取りが発生しないような対策を講じ，高い耐障害性を確保すること。

3.4.運用管理セグメント用サーバスイッチ

運用管理セグメント用のサーバスイッチとして，次の機能及び仕様を満たすものを提供すること。

3.4.1.一般機能要件

(1)　固定ボックス型のレイヤ 2 以上に対応したスイッチ製品であること。

(2)　IEEE802.1q VLAN Tagging 機能を有すること。

3.4.2.インタフェース仕様

(1)　IEEE802.3 規格に準拠した 1000BASE-SX/LX， 100BASE-FX，10BASE-T/100BASE-TX/1000BASE-T の各インタフェースに対応可能であること。

なお，物理ポートの故障に備え，運用に支障の無い程度の予備ポートを有すること。

(2)　EIA 規格準拠 19 インチラックに搭載可能なこと。

3.4.3.セキュリティ機能要件

(1)　送信元/受信元 MAC アドレスに基づいたフィルタ機能を有すること。

3.4.4.ネットワーク管理機能要件

(1) シリアル接続によるコンソールポートを有すること。

(2) Telnet / SSH によるリモート・コンソール機能を有すること。

(3)　設定情報をクライアント端末上の標準的なテキスト編集ソフトウェア等で読み込み及び編集可能な形式で保存可能なこと。

(4) ソフトウェア及び設定情報を TFTP にてアップロード及びダウンロードする機能を有すること。

(5) NTP 又は SNTP による時刻同期が可能なこと。

(6) Syslog サーバにメッセージを送信する機能を有すること。

(7) SNMP による管理機能を有すること。

(8) SSHv1/v2 機能を有すること。

(9)　管理用の RADIUS ユーザ認証機能を有し，管理者以外が設定情報を参照，変更できないような機能を有すること。

3.4.5.信頼性要件

(1) 動作温度は 0℃～40℃に対応していること。

(2) 筐体の動作湿度が 20%～70%に対応していること。

3.4.6.機器構成要件

詳細な接続形態及び接続帯域，必要ポート数及び速度については，「別紙 3 各フロア配線，必要ポー

ト数状況」を参照した上で次のとおりとすること。

(1)　宮内庁 NWS の運用管理セグメントの設計を十分に理解した上で，応札者が提案する各サーバの構成に合わせ，宮内庁 NWS を適切に機能させるための運用管理を実現するために十分なポート数を用意し，必要に応じて適切な SFP トランシーバのメディアタイプを過不足なく用意すること。

なお，未使用となるポート数は，スイッチに搭載されている全てのポート数に対して 40%以下とすること。

(2)　乙が宮内庁本庁用及び京都事務所用にあらかじめ用意した予備機各 1 台によるコールドスタンバイでの冗長構成とする。本番機の構築時の設定情報を複製し，あらかじめ用意した予備機にその設定情報を反映し，本番機と同様の動作が可能な状態にすること。

なお，本番機の設定情報が変更された場合には，変更後の設定情報を機械可読なテキスト形式のファイルとして取得し，そのファイルを運用管理セグメント用端末の中で保管できること。また，そのファイルを予備機で読み込み，設定情報を予備機に反映し，設定情報に基づいて機能できること。

3.5.宮内庁 NWS 運用管理クライアント端末

運用管理業務で日常的に利用する端末を２式用意すること。

3.5.1.ハードウェアの特質，要件

(1) Ａ４ノート型パソコンであること。

(2)　業務継続性を高めるため，単相 100Ｖ商用電源だけでなく，パソコンに搭載されたバッテリでの駆動が可能なこと。また，バッテリのみでの駆動時間は連続で 5 時間以上であること。ただし，一般社団法人電子情報技術産業協会（JEITA）が定めるバッテリ搭載端末 の駆動時間測定方法（Ver. 2.0）に基づく駆動時間であること。

(3) CPU は，次の仕様を満たすこと。

①　コア数 2 以上で，3.0GHz 以上の最大クロック周波数を有すること。

②　キャッシュメモリは 3MB 以上を有すること。

③　バス・スピードは 4 GT/s 以上を有すること。

④　最大メモリ帯域幅は 34GB/s 以上を有すること。

(4) 主記憶装置は，次の仕様を満たすこと。

①　システムメモリについては，16GB 相当以上のメモリを有すること。

②　最大データ転送速度が 17.0GB/s 以上であること。

③　メモリクロックが 133MHz 以上であること。

(5) 補助記憶装置は，次の仕様を満たすこと。

①　光学式ドライブを有していないこと。

②　記憶容量が 480GB 以上の SSD を有すること。

③　政府推奨暗号と同等以上の暗号化機能を有すること。

なお，本機能の実現に当たり暗号化ソフトウェアを用いても差し支えない。

暗号化時に生成した鍵等については，端末の個体毎に整理し，甲で効率的に管理しやすくすること。また，暗号化と鍵の管理方法等については，暗号化の前に甲担当者と協議して甲の承諾を得た上で暗号化を実施すること。

(6) インタフェースは，次の仕様を満たすこと。

① IEEE 802.3 規格に準拠した 10BASE-T/100BASE-TX/1000BASE-T に対応したネットワーク・インタフェースを一つ以上有していること。

② USB2.0 インタフェースを 2 ポート以上，USB3.0 インタフェースを 1 ポート以上有し，合計 3 ポート以上の USB インタフェースを有すること。

なお, USB2.0 インタフェースを 1 ポート以上, USB3.0 インタフェースを 2 ポート以上，又は，USB3.0 インタフェースを 3 ポート以上であっても構わない。

(7) キーボード，ディスプレイ及びマウスは，次の仕様を満たすこと。

① JIS 配列若しくは OADG に準拠した日本語キーボード（テンキーボードを内蔵）であること。

② 15.6 型ワイドカラー液晶で，画面解像度 1，920×1080 ドット以上の表示機能を有すること。

③ 外付けディスプレイ接続用として, HDMI のディスプレイインタフェースを一つ以上有していること。

④ マウスは，USB 接続可能で，総ボタン数（ホイールボタン機能を含む。）を３つ，スクロールホイール機能を有した光学式であること。

(8) ソフトウェア

次のソフトウェアをインストールし，適切にライセンス処理を行い，各機能が確実に動作可能な状態で提供すること。

① 業務継続性，システムの運用効率性及び安定性の観点から現行のクライアント端末の OS と同じマイクロソフト社製 Windows 10（64bit）とし，Pro 以上であること。ただし，OS のサービス提供モデル（WaaS）は，SAC に対応し，運用管理可能なこと。また，搭載する OS は，WSUS によるアップデート等の制御が可能なこと。

② 業務継続性の観点から，クライアント端末で利用しているマイクロソフト社製 Office Professional Plus 2016 で作成した文書を継続的に使用でき，同等以上の性能・機能を有する製品の最新バージョンを搭載すること。

③ その他，運用管理に必要なもの

(9) その他，次の仕様を満たすこと。

① 製造事業者等において，法人向け製品として製造・販売されていること。

② ワイヤロック等で端末本体の盗難防止が可能なこと。

④ はめ込み式や，ねじ式など HDD（若しくは SSD）の着脱が簡便であること。

(10) 環境配慮に関して，省エネ法に基づくエネルギー消費効率について，省エネ基準達成率が AA 以上であること。

3.6.ディレクトリサーバ機能

3.6.1.機能要件

(1) 甲で利用する全ての Windows サーバ機器（Windows Server 2012 又は 2016 を搭載）及び Windows クライアント端末（Windows 10 を搭載。若干数 Windows 7 あり。）をディレクトリ・サービスにより一元管理する機能を有すること。

(2) 本調達仕様書（案）「2.3.オペレーティングシステムの集約化」に従い，必要となる数量の

CAL も調達すること。

(3) 管理下の Windows サーバ，クライアント端末上のフォルダやファイルに対して，アクセス権が設定できること。

(4) 管理下の Windows サーバ，クライアント端末に対し，ディレクトリ・サービスにより共通のポリシーを適用できること。

(5) 本調達仕様書（案）「3.8.ユーザ管理用サーバ機能」と連携すること。
なお，連携機能に関しては本調達仕様書（案）「3.8.1.機能要件」を参照すること。

(6) ユーザの認証失敗のログを取得可能なこと。

(7) 以下に DHCP 要件を示す。

(ア) DHCP による IP アドレス付与の機能を有すること。

(イ) 割り当てる IP アドレスの範囲が指定できること。

(ウ) サービス提供範囲に位置するクライアントからの要求に対して応答できる性能を有すること。

(エ) MAC アドレスフィルタ機能を有すること。

(オ) DHCP サーバ機能を提供すること。

(8) 内部 NTP サーバ機能を有し，宮内庁統合 NW の DMZ 用 NTP サーバと時刻同期できること。

(9) ドメインユーザを Protected Users グループに所属させることにより，NTLM ハッシュがメモリに保存されないようにし，Pass-the-Hash による攻撃を防ぐこと。

(10) Credential Guard の機能により，攻撃ツールが不正にメモリにアクセスし，ドメインユーザの認証情報が不正に窃取されることを抑止すること。

3.6.2.機器構成要件

以下の要件を満たし，適切に動作する構成のサーバ機器等を宮内庁本庁及び京都事務所に設置し，適切に稼働させ，継続的な運用が可能な状態にすること。ただし，現行宮内庁 NWS と異なり，本調達では全ユーザを宮内庁本庁サーバで一括処理することとし，京都事務所サーバは災害復旧を目的としたディザスタリカバリサイト（以下「DR サイト」という。）とすることでサイトでの機能分離を図り，バックアップ等に関する運用管理業務の軽減を図る。また，ファイルサーバ，ウイルス対策サーバ（クライアント端末用）も同様とする。

なお，宮内庁本庁サーバへのアクセスが途絶するような障害等が発生し，宮内庁本庁サーバが機能しなくなった場合には，その状態を京都事務所サーバが検知して宮内庁本庁サーバの役割を自動的に代行するようにし，業務継続性を向上させる。

(1) 宮内庁本庁

(ア) 宮内庁の全ユーザが，サーバ機器等に同時アクセスした場合であっても業務を遅滞なく遂行可能とする処理性能を有する機器構成とする設計を行い，適切な設定を反映することによって確実に動作させること。

(イ) 本調達仕様書（案）「3.6.1.機能要件」に挙げる各機能を有し，本調達仕様書（案）「3.1.サーバ機能共通要件」を満たしたサーバ機器等を過不足なく用意すること。

(ウ) 宮内庁本庁に導入するサーバ機器等は，本庁サーバ室内での冗長化を行うこと。

なお，冗長化を行うサーバ機器等も本調達仕様書（案）「3.1.サーバ機能共通要件」を満たすこと。

(エ) 宮内庁本庁に導入するサーバ機器等のシステム領域及びデータ領域のリモート・バックアップを京都事務所で行うことが可能なこと。

(2) **京都事務所**

(ア) 宮内庁本庁に導入するサーバ機器等のシステム領域及びデータ領域のリモート・バックアップを行うことが可能なこと。

(イ) 前項でリモート・バックアップした内容は，バックアップ直後の 1 世代分に加えて過去 2 世代分，合計 3 世代のバックアップの保管を行うことが可能なこと。

(ウ) 宮内庁本庁に設置したディレクトリサーバ機能を搭載したサーバ機器等が，自然災害などにより利用できなくなった場合，京都事務所に設置したディレクトリサーバ機能を搭載したサーバ機器等が DR サイトとして機能し，宮内庁本庁に設置したディレクトリサーバ機能の代行を自動的に行い，ユーザの業務継続性を確保し，業務が遂行可能となる性能を有する機器構成とすること。

(エ) 本調達仕様書（案）「3.6.1.機能要件」に挙げる各機能を有し，本調達仕様書（案）「3.1.サーバ機能共通要件」を満たしたサーバ機器等を過不足なく用意すること。

3.7.特権 ID 管理機能

特権 ID は，非常に高い権限を持つことから，使用上，管理を厳格にする必要がある。特権 ID で操作されるサーバ等，又は特権 ID で操作する作業者，作業用クライアント端末等において，特権 ID 管理機能を導入し，特権 ID のアクセス管理やトレーサビリティを確保することが重要である。具体的には，次の機能を有すること。

(1) 「誰が」「いつ」「どの特権 ID」を「何のために利用」するのか，特権 ID の利用申請により，承認後，特権 ID が利用可能になること。

(2) 個人用 ID を作業者に付与し，当該 ID と特権 ID との紐付けを行うことで，特権 ID を複数人で共用する場合でも個人用 ID の操作ログから追跡可能であること。

(3) 作業者の全ての操作内容を記録すること。

(4) サーバ OS に依存せず，UNIX 系サーバ（Linux 等）や Windows サーバも操作ログを記録すること。

(5) 特権 ID 管理機能を導入するに当たり，運用管理セグメント用端末に同機能を利用するためのソフトウェアのインストール・アンインストール，設定が必要になった場合は，甲を介して宮内庁統合 NW 受託者へ協力を依頼すること。ただし，宮内庁統合 NW 受託者へ協力を依頼するのは，2020 年 1 月末日までとし，2020 年 2 月 1 日以降は，乙が運用管理セグメント用端末を用いて運用管理業務を行う。

(6) 特権 ID 管理機能から出力されるログ等があり，宮内庁統合 NW 受託者が導入する SOC サービスにおいて，それらを利用したい場合かつ乙による詳細設計書の最終確定以前の場合には，必要となるログ等の仕様を宮内庁統合 NW 受託者の責任で明らかにした上で甲と協議をして承諾を得た後，甲を介して乙に利用の依頼がなされるので，乙はそれに協力すること。

(7) 管理対象となる機器は以下を想定すること。また下記の（ア）から（ケ）に示すサーバ群で管理

対象とするアカウントは原則としてOSの特権IDを対象とすること。その他，各種アプリケーションやミドルウェアの特権IDや，下記の（コ）に示すサーバでも特権ID管理の対象とする方が望ましいアカウントがある場合は，甲と協議の上，対応可能であると合意したものは対象とすること。

(ア)　ディレクトリサーバ
(イ)　ファイルサーバ
(ウ)　ユーザ管理用サーバ
(エ)　電子メール中継サーバ
(オ)　ウイルス対策サーバ
(カ)　バックアップサーバ
(キ)　プロキシサーバ
(ク)　内部 DNS サーバ
(ケ)　WSUS サーバ
(コ)　その他，本調達及び宮内庁統合NWに導入するUNIX系サーバ（Linux等）やWindowsサーバ

(8)　特権IDの利用状況についてレポートを出力することが可能なこと。
(9)　万一，特権ID管理の仕組みに障害等が発生しても，速やかに復旧し特権IDでログインできる仕組みを有すること。
(10)甲担当者が簡便に操作可能なユーザインタフェースを有すること。また，甲担当者が利用するための手引き書を整備すること。

3.8.ユーザ管理用サーバ機能

3.8.1.機能要件

(1)　本機能は，本調達仕様書（案）「3.6.ディレクトリサーバ機能」，「3.14.ファイルサーバ機能」及び「グループウェアサーバ機能（本調達システムには含まれていない現行システム）」と連携し，アカウント情報（ユーザID）を一元的に管理し，以下の機能を実現すること。

なお，現行でのユーザ管理用サーバ機能と連携するサーバ機能のシステム構成概要図に関連した文書（設計，設定，承認フロー等）について閲覧を希望する者は，甲に閲覧申請を行い，甲の許可を得た上で閲覧可能とする。

①　ユーザ管理機能

(ア) 職員管理機能

・　文書取扱主任（「宮内庁行政管理文書管理細則（平成23年4月1日総括文書管理者決定）」で定義されている。）による申請（新規，修正，削除）機能（担当文書取扱主任のみに制限），甲担当者の申請承諾機能，情報管理室の処置機能（バッチ指示，ファイル出力），バッチ処理，申請，承認時の次処理者への処理依頼メール通知機能を有すること。

・　甲にIDを持つユーザに関する情報（個人ID，ユーザ名，組織名，職位等）を管理すること。

・　文書取扱主任にて，ユーザの新規登録・修正・削除の依頼（以下「登録依頼」という。）が行えること。

－　文書取扱主任による登録依頼は電子メールにて甲担当者に通知されること。

・　文書取扱主任による依頼を甲担当者にて確認後，承認又は取消ができること。
  - 情報係にて承認された登録依頼は電子メールにて情報管理室に通知されること。
  - 甲担当者にて取り消された登録依頼は電子メールにて文書取扱主任に通知されること。
・　甲担当者にて承諾された依頼について，情報管理室にて本調達仕様書（案）「3.6.ディレクトリサーバ機能」「3.14.ファイルサーバ機能」及び「グループウェアサーバ機能（本調達システムには含まれない。）」への登録処理を行えること。
  - バッチ処理対象の依頼を指定日にデータベースに反映できること。

(イ) 職位管理機能

・ 職位に関する情報（職位 ID，職名等）を管理すること。

② ID 管理機能

(ア) CSV ファイルによるユーザアカウントの一括管理機能を有すること。また，任意のフォルダに保存された CSV ファイルの取り込みが可能であり，更に任意のフォルダに CSV ファイルを出力が可能なこと。

なお，ユーザアカウントの初期登録における CSV ファイルは甲が乙に提示するものとする。

(イ) ユーザアカウントの作成時にパスワードを自動生成（初期パスワード作成）可能なこと。また，パスワードの強度（長さ・文字の種類等）を設定可能なこと。

(ウ) 本調達仕様書（案）「3.6.ディレクトリサーバ機能」と連携し，ディレクトリサーバ機能に対してユーザアカウント作成・変更・削除，アクセス権の設定・変更等が可能なこと。

(エ) グループウェアサーバ機能（本調達には含まれていない現行システム）と連携できること。

(オ) 本調達仕様書（案）「3.6.ディレクトリサーバ機能」に対して，セキュリティグループを作成できること。また，ユーザの属性情報を自動的に認識し，該当するセキュリティグループに所属させることが可能なこと。

(カ) 本調達仕様書（案）「3.6.ディレクトリサーバ機能」のユーザアカウント作成時に，本調達仕様書（案）「3.14.ファイルサーバ機能」へユーザのフォルダ（ホームフォルダ）を作成できること。また，ユーザアカウントの削除時に，このフォルダを削除可能なこと。

(キ) 本調達仕様書（案）「3.14.ファイルサーバ機能」にフォルダ（共有フォルダ）を作成できること。また，フォルダに（オ）で作成したセキュリティグループを割り当てるとともにアクセス権を設定可能なこと。または，AD 側の アクセス権設定で実施でも構わないものとする。

(ク) ユーザの属性情報を自動的に識別し，現行グループウェアサーバ機能のアクセス権を設定可能なこと。

(ケ) 指定した日時にユーザアカウントが自動的に作成可能なこと。

(コ) ユーザアカウントに有効期限を設け，期限を超過したユーザアカウントを自動的に

無効化又は削除可能なこと。また，管理者にその旨を通知すること。

(サ)　ワークフロー（申請～承認）により，ユーザアカウントを新規作成・変更・削除できること。また，申請者や承認者に電子メールで通知すること。

(シ)　ユーザアカウントの情報を CSV 等の可読可能なフォーマットで外部出力する機能を有すること。

(ス)　本調達仕様書（案）「3.6.ディレクトリサーバ機能」及び現行グループウェアサーバ機能ごとにユーザアカウントの登録状況を一覧表形式で確認できること。

(セ)　管理者が強制的にユーザアカウントのパスワードをリセットする機能を有すること。

(ソ)　ユーザアカウントのパスワードは暗号化を施し，管理・保存することが可能なこと。

(2)　ユーザ管理用サーバ機能利用のためのアクセスについては，以下のとおりとする。

①　操作画面は GUI (Graphical User Interface)により，簡便で効率的なアクセス，設定及び管理操作が可能なこと。

②　管理者のみがユーザ管理用サーバ機能へのアクセスが可能となるアクセス管理機能を有すること。

③　管理者の操作履歴を保存し，これを参照可能なこと。

(3)　本機能は本調達仕様書（案）「3.14.ファイルサーバ機能」と連携し，宮内庁行政文書管理規則（平成 23 年宮内庁訓令第 5 号）及び宮内庁行政文書管理細則に準じたフォルダ階層，アクセス管理ができること。

3.8.2.機器構成要件

次の要件を満たし，適切に動作する構成のサーバ機器等を本庁サーバ室のみに設置すること。

(1)　本調達仕様書（案）「3.8.1.機能要件」に挙げる各機能を有し，本調達仕様書（案）「3.1.サーバ機能共通要件」を満たしたサーバ機器等を過不足なく用意すること。

3.9.内部 DNS サーバ機能

3.9.1.機能要件

(1)　DNS サーバ機能を有し，名前解決ができること。

3.9.2.機器構成要件

次の要件を満たし，適切に動作する構成のサーバ機器等を本庁サーバ室のみに設置すること。

(1)　本調達仕様書（案）「3.9.1.機能要件」に挙げる各機能を有し，本調達仕様書（案）「3.1.サーバ機能共通要件」を満たしたサーバ機器等を過不足なく用意すること。

3.10.WSUS サーバ機能

3.10.1.機能要件

(1)　管理対象機器は，甲が運用する全ての Windows サーバ機器，端末とすること。

(2)　管理対象機器に対し，修正プログラムや累積的セキュリティ更新プログラムを自動的に配信できる機能を実現すること。

(3)　管理対象機器にウイルス対策ソフトのパターンファイルを WSUS サーバで配信する場合

は，次の機能を実現する仕組みも提供すること。

① 端末個別にパターンファイルの配信状況（配信日時，配信有無，パターンファイルのバージョン等）を管理できること。

② 管理対象機器に対し，ウイルス対策ソフトによる保護状態（有効／無効）を管理できること。

③ マルウェア検知時，管理画面から検知された機器を特定できるとともに，検知されたマルウェアの情報（名称，検知されたファイル名等）を確認できること。

④ マルウェア検知時，検知された端末に警告画面を表示するとともに，甲担当者へ警告メールを発信すること。

3.10.2.機器構成要件

次の要件を満たし，適切に動作する構成のサーバ機器等を本庁サーバ室のみに設置すること。

(1) 本調達仕様書（案）「3.10.1.機能要件」に挙げる各機能を有し，本調達仕様書（案）「3.1.サーバ機能共通要件」を満たしたサーバ機器等を過不足なく用意すること。

3.11.バックアップサーバ機能

3.11.1.機能要件

(1) バックアップ対象は，各サーバ機能のシステム領域及びデータ領域とし，ネットワークを介して原則オンラインにてバックアップを取得できること。ただし，システムから切り離して行う作業を行わない場合は必ず行うこと。

(2) 宮内庁 NWS に負荷をかけるおそれがある場合は，バックアップ用のネットワークセグメントを配置すること。

なお，宮内庁 WAN を介してのバックアップを行うことを提案する場合は，宮内庁 WAN の構成及び各回線の帯域幅を考慮し，宮内庁 WAN を利用したユーザの業務に支障ないような設計とすること。

(3) バックアップ取得中，バックアップ対象サーバ機能を原則停止しないこと。ただし，システムから切り離して行う作業を行わない場合は必ず行うこと。

(4) スケジュールに基づいたバックアップが自動でできること。また，年末年始等の長期休暇を想定し，甲の業務状況にあわせ，手動又は任意のスケジュールによるバックアップもできること。

なお，本調達システムの運用におけるバックアップのスケジュール等については，甲と管理者との協議の上で決定するものとするが，管理者において有益と考察される提案を行うこと。

(5) フルバックアップ及び差分バックアップができること。

なお，現行システムにおいては，フルバックアップを毎週金曜日の夜，差分バックアップは毎日行っている。

(6) バックアップが失敗した場合，バックアップ処理をリトライできること。

(7) ファイル及びフォルダ単位並びにサーバ単位のいずれかの場合においてもリストアできること。

(8) バックアップを取得したサーバ以外のサーバからもリストアの操作ができること。

(9)　バックアップのメディアの世代管理ができること。

①　イメージバックアップは 3 世代以上保管できること。

②　データバックアップは 3 週間以上保管できること。

(10)　システム領域を復旧するためのバックアップメディア（以下「システム領域復旧メディア」という。）を作成できること。

なお，システム領域復旧メディアの種類は DVD や USB メモリ等の汎用性が高いメディアとすること。また，納品時点でのシステム領域復旧メディアの作成は乙が行うこととし，この時必要となるメディアは乙の負担において過不足なく用意すること。

(11)　システム領域のリストアは，OS をはじめからインストールすることなく，システム領域復旧メディアから起動しリストアできるよう，作業の効率化を図り，短時間での障害復旧ができること。

3.11.2.機器構成要件

次の要件を満たし，適切に動作する構成のサーバ機器等を各拠点に設置すること。

なお，「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）を踏まえ，平常時の情報システム設置拠点と同時被災しないことが想定される場所にバックアップシステムを確保する等の措置を講ずることとし，本庁サーバ室のリモート・バックアップ拠点を京都事務所とする。

(1)　宮内庁本庁

①　本調達仕様書（案）「3.11.1.機能要件」に挙げる各機能を有し，本調達仕様書（案）「3.1.サーバ機能共通要件」を満たしたサーバ機器等を過不足なく用意すること。

②　本庁サーバ室に設置された機器についてのバックアップ対象となるサーバ機能は，以下のとおり。

(ア)　ディレクトリサーバ機能

(イ)　ファイルサーバ機能

(ウ)　ユーザ管理用サーバ機能

(エ)　電子メール中継サーバ機能（宮内庁統合 NW に含まれる。）

(オ)　ウイルス対策サーバ機能

(カ)　ネットワーク運用管理機能

(キ)　サーバ運用管理機能

(ク)　CAD サーバ機能（本調達システムには含まれていない現行システム）

(ケ)　特権 ID 管理機能

(コ)　内部 DNS サーバ機能

(サ)　WSUS サーバ機能

(シ)　ログ収集サーバ機能

(ス)　振る舞いログ分析（UEBA）サーバ機能

③　前項②においてバックアップされた機能の全てをリモート・バックアップ拠点である京都事務所でもバックアップを保存できること。

(2)　京都事務所

①　本調達仕様書（案）「3.11.1.機能要件」に挙げる各機能を有し，本調達仕様書（案）「3.1.サ

ーバ機能共通要件」を満たしたサーバ機器等を過不足なく用意すること。

② 3.11.2.(1)③記載のとおり，宮内庁本庁のバックアップされた機能の全てをリモート・バックアップ拠点である京都事務所でも保存できること。

3.12.ウイルス対策サーバ機能

3.12.1.機能要件

(1) サーバ及びクライアント端末に，オンライン及びオフラインスキャン可能なウイルス対策ソフトを導入すること。また，定期的に自動でパターンファイルや検索エンジン等の更新，フルスキャンを行うこと。

(2) クライアント端末のウイルス対策ソフトは，当庁で平成 28 年度に更新した資産管理ソフトウェアと連携可能なウイルス対策ソフトから選定すること。例えば，資産管理ソフトウェア標的型攻撃対策ログ収集機能により，ウイルス対策ソフトと連携しウイルスを検知したクライアント端末をネットワークから自動的に遮断する対策を講じている。

(3) 多層型防御の観点から，サーバ及びクライアント端末のウイルス対策ソフトは，ウイルス対策ルール又はパターンファイルの公開時期のずれなどによる対策の遅れを吸収するため，異なる製造業者の製品を導入すること。

(4) 管理対象機器に対し，次の機能を有すること。

① 端末個別にパターンファイルの配信状況（配信日時，配信有無，パターンファイルのバージョン等）を管理できること。

② 管理対象機器に対し，ウイルス対策ソフトによる保護状態（有効／無効）を管理できること。

③ マルウェア検知時，管理画面から検知された機器を特定できるとともに，検知されたマルウェアの情報（名称，検知されたファイル名等）を確認できること。

④ マルウェア検知時，検知された端末に警告画面を表示するとともに，甲担当者へ警告メールを発信すること。

3.13.ログ収集サーバ機能

3.13.1.機能要件

(1) ログ受信方式として，Syslog，SNMP，Windows のファイル共有又は SPC 転送のいずれかに対応し収集対象となる機器群から必要なログを収集することが可能なこと。

(2) ログ収集の対象として，各サーバの OS 等のイベントログ及び監査ログに対応していること。

(3) 各機器が出力するイベントログは，そのままの形式では内容の理解が困難であるが，インシデント等の発生時に対応を行うに当たってログ解析等を迅速に行うために，収集したログの視認性，可読性及び判読性の全てを向上させる機能を有すること。

(4) インシデント等の発生時に対応を行うに当たってログ解析等を迅速に行うために，次に示す検索条件を指定しての検索が可能なこと。また，検索条件の保存が可能なこと。

(ア) 自由なキーワードを指定しての検索

(イ) ログ発生元のサーバ，機器を指定しての検索

(ウ) アプリケーションを指定しての検索

(エ) IP アドレスやユーザ名などを指定しての検索

(オ) syslog の facility(auth, cron, mail など)を指定しての検索
(カ) syslog の priority(info, warn, err など)を指定しての検索
(キ) プロセス ID を指定しての検索

(5) 前項(4)に示した検索条件を AND 及び OR を組合せての検索が可能なこと。

(6) 異なるシステム・フォーマットのログを統合した横断検索が可能なこと。

(7) 前項(4)～(6)の検索結果を，CSV 形式でのファイル出力が可能なこと。

(8) 検索結果で表示されたログに対し，マウスのクリック操作等による絞込検索によって，ログの追跡（トラッキング）が可能なこと。

(9) 収集したログに対し，グラフ形式や表形式での出力などが可能な集計機能を有すること。

(10) 検索機能及び集計機能で保存した各条件を基にし，定期的かつ自動的にレポートを出力することが可能なこと。また，レポートの定期自動出力は，日次，週次，月次で可能なこと。

(11) 収集したログの項目に対し，独自の意味付け及びタグ付けを行うことが可能なこと。

(12) 収集したログが改ざんされないような仕組みを具備すること。

(13) 収集したログに対し，圧縮を施して保管することが可能なこと。

(14) 収集したログのバックアップが可能なこと。

(15) 既存資産を有効活用して費用対効果を高めつつ情報セキュリティ対策を強化するため，現行資産管理サーバとの連携が可能であること。

3.13.2.機器構成要件

(1) 本調達仕様書（案）「3.13.1.機能要件」に挙げる各機能を有し，本調達仕様書（案）「3.1.サーバ機能共通要件」を満たしたサーバ機器等を過不足なく用意すること。

(2) ログ収集サーバに搭載された補助記憶装置は，運用中でも増設可能とし，容量の拡張が可能なこと。

(3) ログ収集の対象となる機器は，次のとおり。ただし，次の（ア）～（エ）については，宮内庁本庁及び京都事務所の両方に設置したサーバが対象となる。
(ア) ディレクトリサーバ
(イ) ファイルサーバ
(ウ) バックアップサーバ
(エ) プロキシサーバ
(オ) ユーザ管理用サーバ
(カ) 電子メール中継サーバ
(キ) ウイルス対策サーバ
(ク) WSUS サーバ
(ケ) フェデレーション(ADFS)サーバ ※グループウェアシステムに含まれる。
(コ) 特権 ID 管理サーバ
(サ) 内部 DNS サーバ

(4) 収集したログについて，ログ収集サーバ上での保存期間は，「適切なログの管理による標的型攻撃対策について（情報提供）（閣副安危第 375 号，平成 24 年 7 月 5 日）」「政府機関における情報システムのログ取得・管理の在り方の検討に係る調査報告書（内閣官房情報セキュリティセンター，平成 24 年 3 月）」に基づき，原則 1 年間とし，ログ収集サーバ

に搭載された補助記憶装置の容量を十分に用意すること。

(5)　次に示す要件を満たすログ用外部バックアップ装置を用意すること。また，収集したログについて，ログ収集サーバ上での保存が 1 年間分蓄積された時点で，ログ用外部バックアップ装置への退避を行うこと。

(ア)　ログ収集サーバに搭載された補助記憶装置に保存された 1 年間分のログデータについて，3 世代分以上の保存が可能な容量を有すること。

(イ)　USB3.0 以上のシリアルバス規格又は 1Gbps 以上の帯域を有するイーサネット規格等のインタフェースでログ収集サーバとの接続が可能なこと。

(ウ)　可搬可能なコンパクト設計であること。

(エ)　自動暗号化機能を有すること。

なお，暗号化については，AES256bit 又はそれ相当以上の暗号強度であること。

3.14.ファイルサーバ機能

3.14.1.機能要件

(1)　本調達仕様書（案）「3.6.ディレクトリサーバ機能」により，フォルダやファイルに対してアクセス権が設定できること。

(2)　ファイルサーバ上に保存されている共有フォルダやファイルは本調達仕様書（案）「3.11.バックアップサーバ機能」により，定期的にバックアップが取得できること。

(3)　本調達仕様書（案）「3.8.ユーザ管理用サーバ機能」と連携し，宮内庁行政文書管理規則及び宮内庁行政文書管理細則に準じたフォルダ階層とアクセス管理ができること。

なお，連携機能に関しては本調達仕様書（案）「3.8.1.機能要件」を参照すること。また，宮内庁行政文書管理規則について閲覧を希望する者は，甲に閲覧申請を行い，甲の許可を得た上で閲覧可能とする。

(4)　庁内ポータルサイト機能

ユーザが行政事務の参考となる情報や資料を提供するため，次に挙げる各機能を有すること。ページ構成，編集もシンプルな UI とし，ユーザが利用しやすい画面にすること。

①　ユーザが Web ブラウザを介して，情報や資料の参照，検索ができること。

②　甲の各部局からのお知らせに利用可能な CMS ページを整備すること。

③　運用開始時は 21 部局分のページを用意すること（詳細は契約締結後に甲より提示する）。

④　各部局における掲示板については，各部局に所属するユーザのみが利用可能となるよう，ユーザの属性情報に基づく利用制限を行うことが可能なこと。また，ユーザの異動に伴って利用可能又は利用制限する掲示板を適切に変更することが可能なこと。

⑤　ページ構成は，次のとおりとする。

- 各部局からのお知らせ
- 各部局掲示板
- 職員録・電話帳へのリンク
- 各種マニュアル・申請書へのリンク
- 外部システム，サイト等へのリンク

3.14.2.機器構成要件

以下の要件を満たし，適切に動作する構成のサーバ機器等を各拠点に設置すること。

(1) 宮内庁本庁

① 本調達仕様書（案）「3.14.1.機能要件」に挙げる各機能を有し，本調達仕様書（案）「3.1 サーバ機能共通要件」を満たしたサーバ機器等を過不足なく用意すること。

② 前項①とは異なるサーバ機器等にて，本機能の冗長化を行うこと。

なお，冗長化を行うサーバ機器等も本調達仕様書（案）「3.1.サーバ機能共通要件」を満たすこと。

3.15.振る舞いログ分析（UEBA）サーバ

各機器から Syslog 等で送信されるログを集中的に管理し利用者に紐づいた異常な振る舞いを分析することができるサーバ。ログの集中管理対象としては，本調達で導入する機器だけでなく，その他の宮内庁 NWS のサーバ群（AD サーバなど）も解析対象とする。必要な要件については次のとおり。

3.15.1.攻撃検知等要件

以下に記載の攻撃を検知することができること。

(1) リモートアクセスユーザが複数の拠点から同時にアクセスをしている。

(2) リモートアクセスユーザが普段とは異なる場所からアクセスをする。

(3) 庁内の端末から庁外のサイトに対して，頻度の高いアクセスが発生する。

(4) 庁内の端末から他の庁内の端末やサーバに対して，頻度の高いアクセスが発生する。

(5) 特権アカウントへの切り替えが頻繁に繰り返される。

(6) サーバに対して普段アクセスをしないユーザからのアクセスがある。

(7) 普段利用していない端末からログインがされる。

(8) 通常のログイン時間やログイン場所とは明らかに異なる時間や場所から繰り返しログインがされる。

(9) ログイン失敗のアカウントが非常に多い。

(10) ユーザが通常アクセスを行わないファイルサーバに保管されているファイルに対してアクセスを行い，正式に利用が認められていない外部の Dropbox や Google drive 等のクラウドストレージへアップロードし，外部サーバへデータを持ち出す。

3.15.2.分析要件

収集したログをもとに以下の観点から分析できること。

(1) 単純分析：単一のログをもとにインシデントの検知。

(2) 相関分析：複数のログをもとにインシデントの検知。

最低限，次のログを対象に相関分析が可能なこと。

・AD のログ，ウイルス対策ソフトのログ，プロキシサーバのログ，メール送受信のログ，VPN のログ

上記以外にも設計時に甲と協議の結果，取り込むことが有意義と考えられるログについては，サーバの容量を勘案した上で，取り込みを行うこと。

(3) 閾値分析：定められた閾値をもとにインシデントの検知。

(4) 振舞分析 : 通信や利用者の振る舞いをもとにインシデントの検知。各端末及び各利用者の通常の振舞を 1 日単位で定義・分析し，通常の行動とは異なる行動が発生した場合に検知できること。

3.15.3.設定要件

乙は，振る舞いログ分析（UEBA）サーバの解析機能が充分に発揮できるよう，宮内庁における情報システムとその利用実態について，充分な理解に努めた上で，3.15.1.攻撃検知要件及び 3.15.2.分析要件を定めるに当たり，適切に設定して，甲の承諾を得ること。また，運用開始後 6 か月程度を目途に改めて設定の見直しを行い，その後も，設定変更の必要又は甲の求めに応じて，適宜設定の見直しを行うこと。

3.15.4.負荷軽減

セキュリティ分析の負荷を低減するため以下の機能を提供すること。

(1) セキュリティインシデントの予兆検知は可能な限り自動化されること。

(2) 機械学習（教師なし）により，平常時の行動パターンをもとに，ユーザごとに振舞のベースラインが自動的に作成され，更新もされること。

(3) 特定のユーザに対し，異常時のタイムラインだけではなく，正常時のタイムラインと比較を行いユーザの振舞を分析・報告可能なこと。また，タイムラインはユーザ単位で表示，分析ができること。

(4) 担当者が製品特有のクエリ言語/Search 文による分析といった専門知識を用いず，標準で提供される選択項目を選択することにより容易にログの検索ができること。

(5) ログの検索や分析の結果が図や表といった視覚的なインタフェースで出力されること。

(6) インシデント検知時は，自動的に管理画面及びメールで警告を通知すること。

(7) インシデント検知時は，管理画面に検知した脅威に対してスコア（点数）表示することにより，対処の優先順位が判断しやすいこと。

3.15.5.機器構成要件

(1) 本調達仕様書（案）3.15.1.～3.15.4 に挙げる各要件を有し，本調達仕様書（案）「3.1.サーバ機能共通要件」を満たしたサーバ機器等を過不足なく用意すること。

(2) 振る舞いログ分析（UEBA）サーバに搭載された補助記憶装置は，運用中でも増設可能とし，容量の拡張が可能なこと。

(3) 収集したログについて，振る舞いログ分析（UEBA）サーバ上での保存期間は，「適切なログの管理による標的型攻撃対策について（情報提供）（閣副安危第 375 号，平成 24 年 7 月 5 日）」「政府機関における情報システムのログ取得・管理の在り方の検討に係る調査報告書（内閣官房情報セキュリティセンター，平成 24 年 3 月）」に基づき，原則 1 年間とし，ログ収集サーバに搭載された補助記憶装置の容量を十分に用意すること。

(4) 次に示す要件を満たすログ用外部バックアップ装置を用意すること。また，収集したログについて，振る舞いログ分析（UEBA）サーバ上での保存が 1 年間分蓄積された時点で，ログ用外部バックアップ装置への退避を行うこと。

（ア） 振る舞いログ分析（UEBA）サーバに搭載された補助記憶装置に保存された 1 年間分のログデータについて，3 世代分以上の保存が可能な容量を有すること。

（イ） USB3.0 で振る舞いログ分析（UEBA）サーバと接続が可能なこと。

(ウ) 可搬可能なコンパクト設計であること。

(エ) 自動暗号化機能を有すること。

なお，暗号化については，AES256bit 又はそれ相当以上の暗号強度であること。

3.15.6.その他要件

(1) UEBA 機能を導入するに当たり，運用管理セグメント用端末に同機能を利用するためのソフトウェアのインストール・アンインストール，設定が必要になった場合は，甲を介して宮内庁統合 NW 受託者へ協力を依頼すること。ただし，宮内庁統合 NW 受託者へ協力を依頼するのは，2020 年 1 月末日までとし，2020 年 2 月 1 日以降は，乙が運用管理セグメント用端末を用いて運用管理業務を行う。

(2) UEBA 機能から出力されるログ等があり，宮内庁統合 NW 受託者が導入する SOC サービスにおいて，それらを利用したい場合かつ乙による詳細設計書の最終確定以前の場合には，必要となるログ等の仕様を宮内庁統合 NW 受託者の責任で明らかにした上で甲と協議をして承諾を得た後，甲を介して乙に利用の依頼がなされるので，乙はそれに協力すること。

4. 資産管理サーバの資産管理ソフトウェアのバージョンアップグレード作業

当庁で使用している資産管理ソフトウェアは，平成 28 年度に「パーソナルコンピュータ及びサーバ等の賃貸借及びサーバ等保守」として，政府調達（WTO）対象の一般競争入札を行い，2017 年 3 月 1 日から 2021 年 2 月 28 日までの 48 か月間（国庫債務負担行為）の賃貸借及び保守契約を締結し運用している。また，パーソナルコンピュータ及びサーバの更新作業を 2020 年度中（2021 年 3 月より運用開始予定）に実施する予定である。

上記の間，資産管理ソフトウェアを最新のバージョンへとアップグレードすることにより，資産管理サーバ及びクライアント端末約 1,200 個を，宮内庁ＮＷ上で遜色なく動作させること。作業は契約期間中に最大で 4 回実施するものとするが，宮内庁 NWS への影響を鑑み，実施要否及び実施時期については甲乙協議の上で決定する。役務内容については次のとおり。

(1) 乙は，納入までに事前準備として必要なハードウェア及びソフトウェアは乙の負担で準備すること。

(2) 乙は，本業務の事前稼働検証，ソフトウェアのインストール及び環境設定，動作確認等の作成等を行うに当たり，当該各作業の実施前には，十分な時間的余裕をもって甲と調整し，各作業工程表を提出し，甲の承諾を得ること。

(3) 本業務の実施に当たり，資産管理サーバを除く各既存システムの業務に影響を与えないこと。

(4) 本業務の実施に当たり，関係事業者の協力を得る場合は，甲担当者及び関係事業者と協議し，乙の負担において実施すること。ただし，作業実施予定日の 5 日前までに乙が作業内容（設定，手順等）を甲に具体的に説明した上で，通常の保守業務又は運用管理業務の範囲内の作業と認められる場合には，甲担当者を介し，甲担当者の指示として当該作業を現行事業者に通常業務として依頼することができる。

(5) 本業務に必要な機器及び消耗品等は，全て乙の責任と負担において用意し，実施すること。

(6) 本業務の実施に当たり，乙は，業務全般を掌握し，本業務の実施に当たる者を指揮監督する業務管理責任者及びこれを補佐する者(以下「業務管理責任者等」という。）を選任し，該当者の資格，経験及び国籍を証明する書面を提出の上，契約後 10 日以内に甲の承諾を得ること(変更する場合においても同じ。)。

(7) 業務管理責任者等は業務の進捗状況全体を把握し，甲に対して内容及び結果を定期的に報告すること。また，甲からの業務等に対する問合せに対し，業務管理責任者等は速やかに対応するとともに，各工程の終了時には，その作業結果について甲の承諾を得ること。

(8) 甲から乙に対する指示，協議申し出は，全て，(6)で選任された業務管理責任者等を通じて行うものとする。

(9) 本業務の実施に当たり，稼働中の各既存システムに対して不具合や問題を生じさせた場合は，乙の責任と負担において適切に対応し，是正すること。

(10) ユーザの作業が発生する場合は，あらかじめ甲に協議の上，その承諾を得ること。

(11) 本業務は，原則として，平日の業務時間（8:30～17:45）に実施すること。ただし，サーバ等各既存システムに影響を与える作業の場合は，ユーザの業務が停止しないよう，原則として，休日又は平日の業務時間（8:30～17:45）以外を利用し，実施すること。いずれの場合も事前にその工程及び作業方法について，甲の承諾を得ること。

なお，国会開会時には，システム停止が許容されない場合がある。

(12) 本業務に当たり，既存環境に設定，ツール等のインストールが必要となる際には，甲及び関係事業者に設計等の情報を開示するとともに甲からの指示に従うこと。

なお，別途機器が必要な場合は，乙の責任と負担において適切な情報セキュリティ対策と設定を施した上で安全に導入すること。

(13) 作業に際しては，甲担当者及び端末賃貸借保守事業者と必要な調整を行い，乙の責任と負担において，作業を実施すること。また，実施に当たり甲及び端末賃貸借保守事業者との調整に伴い発生する費用は，乙が負担すること。

(14) 作業実施前に資産管理サーバのシステムバックアップを取得すること。

(15) 資産管理サーバに甲が指定する資産管理ソフトウェアのバージョンアップグレード作業を実施すること。

(16) 甲が指定するクライアント端末に対し，甲が指定する資産管理ソフトウェアのバージョンアップグレード作業を実施すること。

(17) (15)及び(16)のバージョンアップグレード完了後に，正常に動作することを数台程度確認すること。

(18) (17)にて正常に動作することを確認できなかった場合には，切り戻しを実施し，原因を確認した後，甲に報告すること。

(19) (17)にて正常に動作することを確認できた場合には，甲が指定するクライアント端末にバージョンアップグレードを実施すること。

5. 宮内庁ＮＷＳの運用管理業務に係る請負業務内容

5.1.請負範囲

運用管理業務における請負者として，関係事業者並びに宮内庁統合 NW 受託者と密に連携しつつ，公共サービス改革法の第１条,趣旨と目的に基づいて民間事業者の創意と工夫による次期宮内庁NWSの運用管理業務を柔軟かつ確実に実施し，甲における IT ガバナンス及び情報セキュリティガバナンスの強化に努めること。具体的には，以下のとおりとし，それぞれに対して具体的な方針や実現方法などを示すこと。

(1) 運用管理業務を行う場合において，運用管理セグメントでの作業を行う際には，運用管理セグ

メント用端末を用いること。

(2)　次期宮内庁 NWS の運用管理業務については，次に挙げる宮内庁統合 NW に含まれるサービスは対象外とする。

- 統合 SOC サービス
- 宮内庁 WAN
- インターネット接続回線サービス（インターネット接続機器を除く）

なお，詳細については別紙 4 を参照すること。ただし，日常の運用管理業務の円滑な遂行及び障害やインシデントへの迅速な対応のため，甲担当者や運用管理業務の対象となるハードウェア及びソフトウェア等の製造事業者等との連携だけでなく，安定的で良質な運用管理業務を行うのに必要なログ等の情報共有を，甲の承諾を得た上で，必要に応じて宮内庁統合 NW 受託者と互いに行うこと。

(3)　宮内庁 NWS において，障害やインシデントが発生した場合，乙は，甲担当者，運用管理業務の対象となるハードウェア及びソフトウェア等の製造事業者等，甲の承諾を得た上で，必要に応じて宮内庁統合 NW 受託者と密な連携をすることにより，迅速な解決を図り，甲の事務が極力遅滞なく遂行可能な状態に復帰させることに努めること。

(4)　本調達に先行する宮内庁統合 NW の調達の構築期間中に，甲の承諾を得た上で宮内庁統合 NW の基本設計書及び詳細設計書を必ず精読して理解し，甲を介して宮内庁統合 NW 受託者と協議を行い，それぞれが互いに効率的に連携して安定的で良質な運用管理業務を実施可能な運用管理設計を行うこと。

(5)　IT サービスマネジメントシステム（ITSMS）として ISO/IEC 20000 シリーズ又は ITIL の最新版に則して運用管理業務を実施することにより，PDSA サイクルによる継続的な改善を行い，次に掲げる効果を可能な限り導き出すための方策を具体的に示すこと。

- 宮内庁 NWS を取り巻く環境の変化への対応力向上
- 宮内庁 NWS のユーザの満足度向上
- 宮内庁 NWS を利用した業務継続性の強化

(6)　絶え間なく変化する情報通信技術や情報セキュリティなどに追従するため，運用管理従事者に対し，それらを学習する機会を適切に設け，運用管理従事者の能力向上を図り，運用管理業務の継続的な改善を行うこと。

(7)　作業範囲は，「6.運用管理に関する要件」に従うこととし，各現行システムについては，「13.資料閲覧」時に供する各運用管理手順書等，さらには運用管理業務の対象となるハードウェア及びソフトウェア等の製造事業者等が提供する手順書，マニュアルや FAQ などに従うこと。

(8)　各運用管理手順書について，記載内容以外に運用管理業務を効率的に効果的に行う方法などがある場合や不明瞭な内容又は不足があると認識した場合には，運用管理業務の対象となるハードウェア及びソフトウェア等の製造事業者等の手順書，マニュアル，FAQ や技術サポートサイトなどを参照し，当該手順書の修正等を適宜行い，継続的な改善を行うこと。

なお，製造事業者等の技術サポートサイトの一例としては，次のようなサイトがあるが，宮内庁 NWS を構成するハードウェア及びソフトウェア等の製造事業者等の技術サポートサイトをあらかじめ調査し，各運用管理手順書の中で一覧としてまとめ，変更があった場合には，この一覧を適宜修正すること。

＜技術サポートサイトの一例＞

・ 日本マイクロソフト社 TechNet
https://technet.microsoft.com/ja-jp/

(9) 運用管理業務を円滑かつ効果的に行うため，PMI の PMBOK の最新版に則してステークホルダーマネジメントを行うこと。

(10) 運用管理業務の実施に当たり，現行システムへの追加・設定変更が必要となる場合には，甲及び現行システムの構築・保守事業者とその妥当性や有効性について十分に協議・検討し，甲の承諾を得た上で，ユーザサービスに影響がないよう，変更管理などの必要な管理を確実に実施すること。

(11) 宮内庁 NWS の投資対効果を最大化するため，宮内庁 NWS を構成する各ソフトウェア及びハードウェアに「標準装備」されている個々の機能を最大限に活用するだけでなく，それぞれが連携した場合の機能を最大限活用することに努め，情報システムの利便性の向上や情報セキュリティ対策の向上を図ること。

なお，別途，ソフトウェア又はハードウェアの機能やモジュール等の追加購入及びセットアップ作業が必要となる場合は，必要となる費用の概算や作業内容等を可能な限り甲担当者へ提供し，甲担当者の検討に協力すること。

(12) 情報セキュリティについて，その対策のための措置として現行システムへの設定変更，必要なログの取得などの作業を甲の判断で甲担当者から依頼された場合には，その依頼内容についての実現方法について可能な限り迅速に検討し，確実に実施することにより，情報セキュリティ対策の強化を継続的に行うこと。

5.2.対象機器

運用管理業務の対象機器は，甲におけるネットワーク機器，サーバ機器，クライアント端末，プリンタ，ケーブル（これらの周辺機器や附属品を含む。）とする。

なお，詳細については，「13.資料閲覧」時に供する「機器一覧」，「ラック構成図」，「全体概要図」ほかを参照すること。

5.3.サービスレベル

(1) 運用管理業務の効率化と品質向上並びに円滑化を図るため，以下に示す指標に対してサービスレベルアグリーメント（SLA）を締結すること。

① 運用管理業務の一次回答時間

（ア） ユーザからの質問等に対する一次回答時間は 1 時間以内とすること。回答時間は以下の計算式による。

（乙がユーザに回答した時刻）－（ユーザが乙に対して質問等した時刻）

（ただし，17 時 45 分以降の質問については翌営業日の 9 時 30 分までに回答すること。）

② 運用管理業務の解決時間

（ア） ユーザからの質問等に対する解決時間は 2 営業日以内とすること。解決時間は以下の計算式による。

（ユーザの質問等が解決した日時）－（ユーザが乙に対して質問等した日時）

（イ） 乙の作業範囲外のものについてはサービスレベルの対象外とする。ただし，この場合においても質問等の解決に向けて協力すること。

③　障害報告時間

（ア）　各システム又は外部監視等により検出された機器等の障害について，30 分以内に甲担当者に対し報告すること。障害報告時間は以下の計算式による。

（乙が甲担当者に報告した時刻）－（障害確認時刻）

（ただし，17 時 45 分以降の障害発生については，翌営業日の 9 時までに報告すること。）

④　障害解決時間

（ア）　各システム又は外部監視等により検出された機器等の障害について，1 営業日以内に解決させること。障害解決時間は以下の計算式による。

（障害が解決した日時）－（障害確認日時）

（イ）　乙の作業範囲外のものについてはサービスレベルの対象外とする。ただし，この場合においても障害の解決に向けて協力すること。

⑤　運用要領及び運用計画の遵守

（ア）　運用要領及び運用計画の遵守状況に関して，甲から指摘された改善要求件数は，0 件であること。

(2)　サービスレベルの遵守状況については，月 1 回開催の SLA 報告会議において報告し，甲の承諾を得ること。

(3)　甲の要求水準は，「上記(1)①から⑤に掲げる指標全ての遵守率について 99%以上であること」とする。ただし，乙の作業範囲外のもの，又はやむを得ない事情によるものであることを甲が承諾したものについてはサービスレベル測定の対象外とする（例えば甲担当者と連絡がつかない，地方部局とのやり取りなど。）。

(4)　(3)で要求した水準を満たせなかった場合，具体的な解決策を検討し，(2)の報告時に合わせて報告すること。

(5)　3 か月連続して(3)の要求水準を満たせなかった場合，運用管理体制の強化，若しくは「5.4.作業実施体制」の変更を指示することがあるが，(3)の要求水準を満たせるまでの期間において，乙は運用管理業務の範囲内でこれに対応すること。

5.4.作業実施体制

宮内庁 NWS の体制を以下に示す。本調達の運用期間中にクライアント端末，プリンタ及び複合機の増設が生じた場合でも，本調達の範囲内として運用対象とすること。

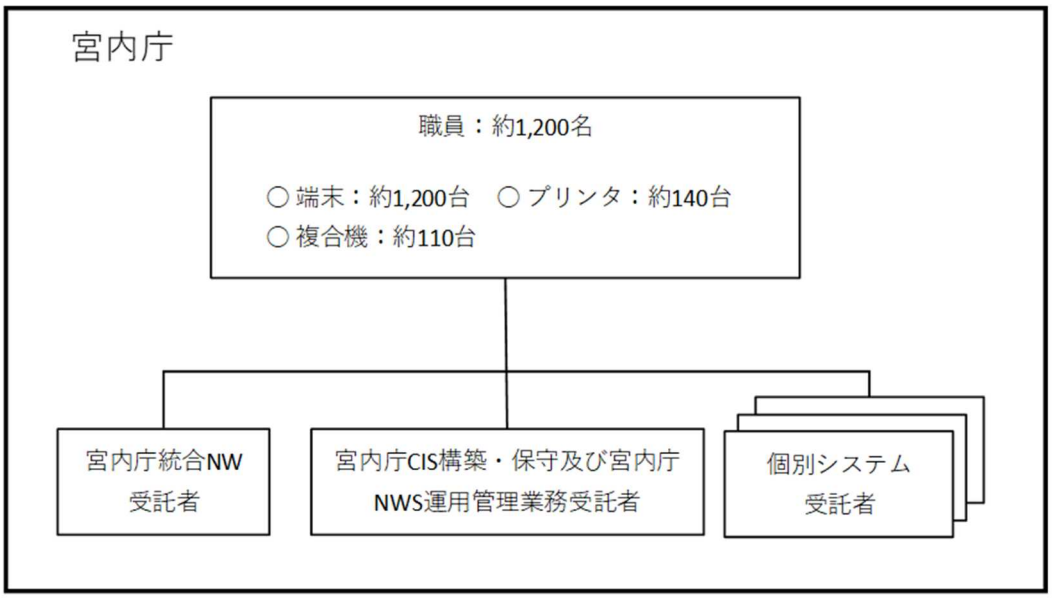


図1.宮内庁NWS体制

(1)　宮内庁 NWS の運用管理業務について，情報管理室に休日を除いた平日に常駐する運用作業員（以下「運用作業員」という。）の管理者（以下「運用管理責任者」という。）を 1 名以上配置すること。

(2)　運用管理責任者は，1 週間のうち休日を除く平日の 60%以上，情報管理室に勤務すること。平日 1 日の勤務時間を 8：30～17：45（休憩時間 60 分を含む。）とした場合，運用管理責任者の勤務は次のとおりとなる。

1 週間のうち平日が 5 日の場合：　休憩時間を除く 24 時間 45 分以上
1 週間のうち平日が 4 日の場合：　休憩時間を除く 19 時間 48 分以上
1 週間のうち平日が 3 日の場合：　休憩時間を除く 14 時間 51 分以上
1 週間のうち平日が 2 日の場合：　休憩時間を除く 9 時間 54 分以上
1 週間のうち平日が 1 日の場合：　休憩時間を除く 4 時間 57 分以上

(3)　乙は，情報管理室に休日を除いた平日に常駐する運用作業員を 1 名以上配置すること。ただし，運用作業員が 1 名のみの場合，運用管理責任者が運用作業員を兼ねることを不可とする。

なお，「5.1.請負範囲」を遂行困難，又は「5.3.サービスレベル」を満たしていないと甲が判断し，これらに基づき乙に対して改善要求をした場合には，乙は，必ず人数の増加や運用作業員の交替の措置を乙の責任と負担で施すこと。

(4)　運用管理責任者又は運用作業員は，運用管理報告書を作成の上，毎週 1 回開催の運用管理会議において，運用管理会議開催日の前週の一週間分の作業状況を報告し，甲の承諾を得ること。また，運用管理会議開催日の翌週の一週間分の運用管理責任者及び運用作業員の勤務予定表を提出すること。その勤務予定表に基づき，情報管理室に 1 名のみの配置となる日時を確認し，この日時について甲担当者 1 名が情報管理室に勤務することを調整することで，情報管理室の配置要員を 2 名とする。

なお，当該会議には，運用管理責任者も同席すること。

(5)　運用管理責任者及び運用作業員の勤務時間は，原則，休日を除く平日の 8：30～17：45（休憩時間 60 分を含む。）とする。ただし，ユーザの業務への影響等を考慮し，当該勤務時間外でないと実

施できない作業については，甲と事前に協議の上で作業実施を決定した場合，この限りではない。

なお，運用管理責任者と運用作業員が同時に情報管理室に勤務する場合には，休憩等は時間差で行い，情報管理室で運用管理業務を行う者が不在とならないようにすること。

(6) 運用作業員が不慮の事故，疾病又は休暇により勤務できない場合は，甲担当者と協議の上，乙の責任において，代替要員の運用作業員を情報管理室に派遣し，運用作業員が 1 名もいない状況を回避して業務に支障を来さぬようにすること。

なお，運用作業員が 1 名のみの場合，運用管理責任者が代替要員を兼ねることを原則不可とする。ただし，運用作業員が勤務できない日数が平日の連続した 2 日間以下であることが事前に確認可能であり，運用作業員が勤務できない最初の日から数えて休日を除いた平日 5 日前までにあらかじめその旨を甲担当者へ報告して承諾を得た場合には，確認ができた運用作業員が勤務できない日に限り，運用管理責任者が代替要員を兼ねることを許可する。

(7) 運用管理責任者及び運用作業員の勤務予定表を除いた実施体制そのものを変更する場合，甲担当者との協議を行うための十分な期間（平日で 10 日間以上）を設け，変更する理由を明確に甲担当者へ報告し，協議の上で承諾を得ること。

5.5.リモートで運用作業員のサポートを行う場合の要件

リモートにより，運用作業員のサポートを実施する（以下，「サポート業務」という。）には，セキュリティが確保された体制となっているか，サポート人員の実績・資格等が運用作業員と同等以上であるかなどの条件を満たす必要があり，情報管理室での勤務するのと遜色ないサービスレベルが維持されることを前提に認めることは，あり得る。

サポート業務の遂行に当たっては，乙が保有する運用拠点からリモートで運用作業を行うことを可とするが，宮内庁内の機器に対しオペレーションを伴う作業を行う場合においては，以下の要件を遵守すること。

なお，運用拠点及び運用管理業務を行う居室（以下，「運用居室」という。）について，要件遵守の確認のため，甲が立ち入りを求めた場合は，入室を許可すること。

5.5.1.基本要件

(1) 甲より受領した情報については厳重に管理を行い，サポート業務遂行以外の目的に利用してはならない。

(2) 記録された映像やログ等は，甲からの求めがあった場合は，速やかに提供すること。

5.5.2.ネットワーク接続形態要件

(1) 運用管理業務をリモートで行うに当たって宮内庁NWSに接続を行う場合は，以下(2)の条件を満たす閉域等されたネットワーク（以下，「閉域等NW」という。）にて接続を行うこと。

(2) 接続される閉域等NWについて，インターネットを介した VPN を用いる場合には，OSI階層モデルのネットワーク層以下での経路の暗号化手続きを行う通信経路上のセキュリティを配慮した方式であるか，又は，インターネットを介さない閉域網（専用線，閉域IP通信（IP-VPN）等）の利用とする。

(3) 該当の閉域等NWには，あらかじめ甲に申請し許可を得た端末以外の端末は接続できない措置を講じること。

(4) 閉域等NWを利用して接続を行う場合は，宮内庁内に設置する機器等も含めその設営等に係る費用は，すべて乙が負担すること。

5.5.3.運用拠点要件

(1) 運用拠点は，公共交通機関を利用して，当庁へ 2 時間を目途に到着できる場所に存在すること。

(2) 運用拠点には，運用管理責任者を配置すること。

(3) 運用拠点は，防火構造，空調設備を備えた建物であること。

(4) 運用拠点は，免震ないしは耐震構造建物となっており，震度６相当の地震にも耐えうること。

(5) 運用拠点には，常時安定した電力供給ができるほか，電力の瞬間停電等の際も，連続的な運転を可能にする措置が講じられていること。

(6) 運用拠点には，機械的に判別できる本人認証技術を用いた入場制限がなされており，乙関係者以外の人員が出入りできない措置が講じられていること。

(7) 運用拠点への出入りは，監視カメラにより撮影され，その映像は記録されていること。記録した映像の保管・管理は，甲乙協議の上で決定すること。

5.5.4.運用居室要件

(1) 運用居室は，他の居室と壁で完全に仕切られているなど独立した居室であること。

(2) 運用居室は原則としてサポート業務専用の居室とすること。やむを得ず他業務と共有をする場合は，共有期間を明示した上で他業務内容及びその必要性についてあらかじめ甲にその理由を記した書面を提出し承諾を得ること。

(3) 運用居室内には，あらかじめ甲が承諾し登録された人員以外が出入りできない措置が講じられていること。

(4) 運用居室には，機械的に判別できる本人認証技術を２種類以上用いた入場制限がなされていること。

(5) 運用居室内に入室可能な人員は，あらかじめ甲に書面にて名簿を提出し承諾を得ること。この人員を変更する場合は，その都度変更した名簿を甲に提出して承諾を得ること。

(6) 運用居室への入退室は，人員ごとに入室時刻及び退室時刻を自動的に記録（ログ等）ができるものとし，甲がこの記録を求めた場合は，即座に提出すること。また，この記録は，意図的な改ざんされないような仕組みを具備すること。

(7) 運用居室内では，原則として宮内庁ＮＷＳに接続する閉域等NW以外の他回線の引き込みを行わないこと。やむを得ず他回線の引き込みを行う場合は，あらかじめ甲にその理由を記した書面を提出し承諾を得ること。

(8) 運用居室内に人員が滞在している間は，常時監視カメラにより撮影され，その映像は記録されていること。

(9) 監視カメラで撮影される範囲は，死角がないように居室全体とすること。

(10) 監視カメラには，同カメラ自体に撮影を妨げる行為があった場合，それを検知し，その記録（ログ等）を保存できること。

(11) 監視カメラで記録した映像及びログ等は，少なくとも１年保存・管理すること。詳細について

は，甲乙協議の上で決定すること。

5.5.5.運用端末要件

(1)　運用端末は本業務を行うための専用端末とし，他の用途には使用しないこと。

(2)　運用端末の操作は，あらかじめ登録されている人員のみとし，登録されているどの人員が，いつ，どんな操作をしたのか記録等（ログ等）をすること。また，運用端末を操作する際にコンピュータ・ネットワークを利用する人を識別するための番号であるユーザIDを使用する場合は，総務省「国民のための情報セキュリティサイト」を踏まえ，次のルールを遵守すること。

【ユーザID及びパスワードのルール】

① パスワードの長さ

管理者権限ユーザの場合は13桁以上，一般権限ユーザの場合は8桁以上とすること。

② パスワードは，数字，アルファベット大文字と小文字及び記号の4つの文字種を組み合わせること。

③ 数字の単なる羅列など，他人に推測されやすいパスワードやデフォルト（製品の初期値等）のパスワードは速やかに本ルールに沿って変更すること。

④ 本業務の運用端末操作ためのユーザID及びパスワードは，他の業務の端末操作等では使用しないこと。

⑤ 運用作業員ごとの個別ユーザIDで，作業すること。

※［参考］総務省 国民のための情報セキュリティサイト

http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/basic/privacy/01.html

(3)　運用端末は，宮内庁NWS以外に接続を行わないこと。また，運用端末を誤って他のネットワークに接続した場合は，外部との通信ができないような仕組みを講じること。

(4)　運用端末は，セキュリティワイヤー等で什器等固定物に繋げ，施錠等し，持ち出しができない措置を講じること。

(5)　運用端末に，USBメモリ等の外部電磁的記録媒体を接続し，データの取り込み，書き込み及び持ち出しができない措置を講じること。やむを得ず運用端末に外部電磁的記録媒体を接続する必要が生じる場合は，あらかじめ甲にその理由を記した書面を提出し承諾を得ること。また，承諾を得た後，外部電磁的記録媒体を運用端末へ接続する直前には，必ずウイルス検査を行い，ウイルスが存在していないことを確認した上で接続すること。

(6)　運用端末のハードディスクは，暗号化される措置を講じること。

(7)　運用端末に保管するファイルは，自動的に暗号化される措置を講じること。

(8)　運用端末は，ウイルス対策ソフトがインストールされており，常に最新の状態でウイルス対策ができる措置を講じること。

(9)　運用端末のOS及び各種ソフトウェア等の脆弱性情報を常に確認し脆弱性対策を講じること。

(10)　万一，運用端末がマルウェアに感染した場合又は感染のおそれがあると判断した場合は，当該端末を即座に宮内庁NWSから切り離し，速やかに甲に書面による報告を行うこと。感染原因の追及に当たっては，セキュリティオペレーションセンター等の支援を得て，乙の負担においてフォレンジック調査等を行い，侵入経路，感染ルート等の原因調査を行い，その結果及び今後の防止対策を講じた上で，甲に説明を行うこと。

(11)　運用管理業務の契約期間満了後には，速やかに運用端末内で保管・管理されている甲に関する一切の情報が残らない（復元を不可能とする）措置をとり，データ消去証明書を甲に提出すること。

なお，データ消去に当たっては，甲が定めた「情報処理及び情報システムについての対策規程（平成27年３月10日 統括情報セキュリティ責任者決定)」を遵守すること。

※ 参考：「情報処理及び情報システムについての対策規程」より抜粋

○ 付録「データ抹消ツール」の設定要件

以下のいずれかのデータ上書き方式を設定すること。これらの設定をすることができないものを用いないこと。

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）

6.　運用管理に関する要件

6.1.運用管理計画の策定

6.1.1.サービスレベルの合意

甲とサービスレベルについて合意し，サービスレベル合意書【5.3.サービスレベル】を契約締結後，運用管理業務開始 10 日（休日を除く）前までに遅滞なく提出すること。

6.1.2.運用管理計画書の策定

(1)　乙は，次に挙げる各文書を十分に理解した上で，本調達仕様書（案）「4.宮内庁 NWS の運用管理業務に係る請負業務内容」に基づいた宮内庁 NWS の運用設計を行い，宮内庁 NWS の日々の安定稼働を確保することを目的とした，宮内庁 NWS の運用管理計画書の案を作成し，本調達の提案書と共に提出すること。

(ア) 宮内庁 CIS の運用管理計画書（案）

(イ) 宮内庁業務継続計画　http://www.kunaicho.go.jp/kunaicho/shiryo/gyomukeizoku.html

(ウ) 宮内庁 NWS に関する各計画書など

(2)　乙は，(1)に掲げる運用管理計画書の案を基に作成した正式版を，運用管理業務開始 10 日（休日を除く）前までに甲担当者の確認を受け，承諾を得た上で確定版とすること。

(3)　乙は，(2)に掲げる運用管理計画書の確定版について，運用管理業務を実施してく中で，必要に応じて修正箇所を提案し，更新すること。

なお，更新する場合は甲担当者と合意の上，更新すること。

6.1.3.各手順書の作成

(1)　乙は，宮内庁 CIS の運用管理手順書（案），甲担当者向け停電時復旧手順書（案），情報セキュリティインシデント対応手順書（案），ユーザ手順書（案）などの運用管理に関する各手順書及び本調達仕様書（案）「5.宮内庁 NWS の運用管理業務に係る請負業務内容」を基に，本調達に対する提案書，宮内庁 NWS の運用管理計画書（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，実施手順等を取りまとめた各手順書の案を作成し，本調達の提案書と共に提出すること。

(2)　乙は，(1)に掲げる各手順書の案を基に作成した正式版を，運用管理業務開始 10 日（休日を除く）前までに甲担当者の確認を受け，承諾を得た上で確定版とすること。

(3)　乙は，(2)に掲げる各手順書の確定版について，運用管理業務を実施していく中で，必要に応じて修正箇所を提案し，更新すること。

なお，更新する場合は甲担当者と合意の上，更新すること。

6.1.4.運用管理実施要領の作成

(1)　乙は，管理標準ガイドラインの「第 9 章　運用及び保守」にて示されている運用管理要領の作成・記載内容などを参考にし，宮内庁 NWS の運用管理を効率的に実施できるよう，宮内庁 NWS の運用管理計画書及び保守作業計画書と整合をとりつつ，運用・保守工程におけ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に係る実施ルールを定義する運用管理実施要領の案を作成し，本調達の提案書と共に提出すること。

(2)　乙は，(1)に掲げる運用管理実施要領の案を基に作成した正式版を，運用管理業務開始 10 日（休日を除く）前までに甲担当者の確認を受け，承諾を得た上で確定版とすること。

(3)　乙は，(2)に掲げる運用管理実施要領の確定版について，運用管理業務を実施してく中で，必要に応じて修正箇所を提案し，更新すること。

なお，更新する場合は甲担当者と合意の上，更新すること。

6.2.作業実績の報告

乙は，本調達仕様書（案）5.1 に示す作業等を実施すること。

なお，作業実績の報告については以下の事項に留意すること。

- サイバー攻撃に関する最新動向の調査に当たっては，宮内庁 CIS に限らず，甲に対し有用な提案がある場合は積極的に提案すること。

6.2.1.週次運用管理報告書の作成

「運用管理計画書」，「保守作業計画書」，「運用・保守実施要領」に基づき，以下の内容について週次で「週次運用管理報告書」を取りまとめること。

- 情報システムの構成と運転状況（情報セキュリティ監視状況を含む）
- 情報システムの定期点検状況
- 情報システムの利用者サポート，教育・訓練状況
- 情報セキュリティ管理の実施状況
- リスク・課題の把握・対応状況

6.2.2.月次運用管理報告書の作成

「運用管理計画書」,「保守作業計画書」,「運用・保守実施要領」に基づき，以下の内容について月次で「月次運用管理報告書」を取りまとめること。

なお，情報セキュリティ管理については，サイバー攻撃に関する最新動向等を入手し，宮内庁 NWS において可能な防御策を確認の上，報告を実施すること。また，報告には，少なくとも作業実施者名，作業実施者スキルレベル，作業開始日時，作業終了日時を含めること。

- 運用・保守業務の内容や工数，作業時間等の作業実績状況
- サービスレベルの達成状況
- 情報システムの構成と運転状況（情報セキュリティ監視状況を含む）
- 情報システムの定期点検状況
- 情報システムの利用者サポート，教育・訓練状況
- 情報セキュリティ管理の実施状況
- リスク・課題の把握・対応状況
- サイバー攻撃に関する最新動向等及び庁内 LAN で可能な防御策等

6.2.3.作業実績の評価

月間の運用・保守実績を評価し，達成状況が SLA に満たない場合はその要因の分析を行うとともに，達成状況の改善に向けた対応策を提案すること。

6.2.4.作業実績の報告の実施

運用・保守作業報告書の内容について，定例の運用管理会議に出席し当庁に報告すること。

6.3.定常運用管理業務

6.3.1.業務管理

6.3.1.1　定例会議

甲に対し定期的に運用報告を実施すること。

(1)　運用管理会議

運用作業員は，運用計画書に基づき実施した運用管理業務の内容及び障害・インシデント等の対応状況について，運用管理業務週報に記録し，甲に毎週 1 回開催の運用管理会議において報告すること。ただし，重大な報告は都度行うこと。

①　運用管理会議の出席者については，以下の要員とする。

- 甲担当者，宮内庁 CIO 補佐官（内閣官房政府 CIO 補佐官）
- 乙は運用管理責任者及び運用作業員
- その他，甲が承諾をした者

②　報告事項については，以下の項目を含むものとする。

- 前回議事録
- ネットワーク運用支援作業報告
- ユーザサービス作業報告
- 障害対応ヘルプデスク作業報告

・　ヘルプデスク対応管理表
・　課題事項一覧表
・　ウイルス検知報告（種別・個人別のウイルス検知表）
・　日毎の入退室管理実績表
・　日毎の次週作業予定表
・　障害対応報告書（障害が発生した場合）
・　その他，甲が希望する資料

(2)　SLA 報告会議（月 1 回開催）会議

乙は，1 か月ごとにサービスレベルアグリーメントの達成状況の確認を行い，達成状況について，サービスレベル報告書に記録し，甲に毎月 1 回開催の SLA 報告会議において報告すること。

①　SLA 会議の出席者については，以下の要員とする。
・　甲担当者，宮内庁 CIO 補佐官（内閣官房政府 CIO 補佐官）
・　乙は運用管理責任者及び運用作業員
・　その他，甲が承諾をした者

②　報告事項については，以下の項目を含むものとする。
・　「5.3.サービスレベル」の 5 項目を始めとするサービスレベル合意書において設定した項目の達成状況についてまとめたサービスレベル報告書
・　サービスレベルを満たせなかった場合の原因及び対策に関する報告資料
・　報告期間（報告実施前月の 1 か月間）に対応した 1 件ごとの作業内容に関する詳細情報（部署名・氏名・状況・処置・発生日時・一次回答日時・所要時間・解決時間等々）
・　本要求仕様の各項目に要した 1 か月分の工数（時間単位）をまとめ，SLA 報告会議時に報告すること。

6.3.1.2　手順書等の整備

(1)　運用管理業務に必要となる手順書，運用管理フロー図等を適切に整備すること。

(2)　手順書等に変更が生じた場合は，速やかに更新し甲担当者の承諾を得ること。

6.3.1.3　提案

(1)　運用管理実績報告の他に，本調達仕様書（案）「1. 4. 背景と目的」における各目的の実現を達成するための継続的改善活動（PDＳA サイクル）として，定期的ないし随時に，運用にかかる評価，問題提起，改善提案，最新技術情報の提供を甲へ行い，甲と積極的に協議する機会を設けること。

なお，甲が自らの調査等に基づいて乙へ提案を行う場合においても，運用管理実績報告の他に，本調達仕様書（案）「1.4.背景と目的」における各目的の実現を達成するための継続的改善活動（PDＳA サイクル）である場合には，乙は，甲からの提案内容について甲と積極的に協議する機会を設けること。

(2)　協議の結果，提案内容を甲が承諾した場合には，実現に向けた具体的な提案（運用手順の変更内容や各機器の設定の変更内容等）を行った上で，実現を図ること。ただし，新たなハードウェア及びソフトウェアの購入が必要である場合，それらの購入費用及び保守費

用は，本調達には含めないこととし，別途予算確保できた場合にのみ，実施することとする。

6.3.2.情報の管理

(1)　調査，保守作業，システム構築等による文書又は電子データの持ち出し，持ち込みが発生する場合は，甲担当者の承諾のもと，文書にて内容を説明した上で持ち出し又は持ち込みを実施すること。

(2)　電子メールや甲の指示する電子媒体で情報を授受する際は，パスワード等による漏洩防止対策を行うこと。

6.3.3.資産管理に使用する資料等

宮内庁 NWS に接続されるハードウェア（クライアント端末含む），配線及びソフトウェア（ライセンス）の情報，接続情報等を可能な限り自動で，自動化できないものは手動にて適時に収集し，資産管理，インベントリ管理を行うこと。また使用権を得ているライセンスについて契約更新等の支援を行うこと。（既存インベントリ収集用のシステムとして資産管理ソフトウェアを使用）以下の資料を作成し，常時メンテナンスすること。

(1)　資産管理台帳

①　宮内庁 NW に接続されるハードウェア及びソフトウェアについて，必要な情報を管理すること。

②　必要に応じハードウェア，ソフトウェアを分冊にする等メンテナンスしやすい様式とすること。

(2)　論理構成図

①　資産管理台帳に基づき，ネットワーク及びサーバについて論理構成図を必要に応じて修正すること。

②　宮内庁 NW にネットワークセグメント，ルーティング情報が追加された場合は，論理構成図に追加すること。

(3)　物理構成図

①　資産管理台帳に基づき，ネットワーク及びサーバについて物理構成図を必要に応じて修正すること。

(4)　機器配置図

①　ネットワーク，サーバ，クライアント端末，プリンタ等のデジタル周辺機器に係る機器配置図の内容が最新となるように努めること。

②　新しく宮内庁 NW にネットワークセグメント，ルーティング情報が追加された場合は，機器配置図に追加すること。

(5)　ライセンス契約管理

①　ライセンス管理については，契約更新手続き支援（期限到来アナウンス，更新書類の記入，手続き支援等）を行うこと。

(6)　配線図

①　サーバ室内の電源配線図，ネットワーク機器のポートアサイン図が最新になるよう必要に応じて更新すること。

(7)　その他必要な文書

① 上記文書以外に運用管理業務内で管理すべき情報（サーバ設定情報等）がある場合は文書を作成し記録すること。

② 上記(1)の資産管理台帳等に記載された資産に変更がなされた場合，変更の実施者，変更の承諾者，変更事由，変更箇所，変更に伴う他への影響範囲，テスト結果，変更の実施日時，リリース日時等を記録し管理を行うこと。

6.3.4.ポリシー管理

グループポリシー設定等を適切に管理すること。

6.3.5.データ管理

定期バックアップ及びリストア

(1) バックアップ対象

3.11.2(1)②を参照すること。

ただし，個別システムのバックアップ運用については，「6.4.宮内庁 CIS 以外の宮内庁 NWS の運用管理」の項目を参照すること。

(2) バックアップの方式・機能

① 本調達で導入されるバックアップソフトウェアを使用し，データバックアップを取得すること。

② 本調達で導入されるイメージバックアップソフトウェアを使用し，サーバのイメージバックアップを取得すること。

③ データ消失時のリストアを行うこと。

(3) 定常業務

① バックアップログを毎日チェックすること。

② 各テープ装置のテープメディアを交換すること。

③ 定期的に各テープ装置のクリーニングを実施すること。

④ 地方サーバで使用するデータカートリッジのローテーション管理。

(4) バックアップ媒体の保存

① 一時保管

- KMS サーバは，テープメディアをサーバ室に保管
- ファイルサーバは，バックアップサーバをサーバ室に設置

② 外部保管

- 月次フルバックアップを録取したテープメディアを指定の外部保管先に保管。（保管先は，契約締結後，乙に対し甲担当者より指示する。）

6.3.6.ネットワーク管理

(1) ネットワーク・サーバ等監視

① 監視概要

- ネットワークセグメント及び各機器の死活，サーバの重要プロセス及びサービス稼働状況，サーバのシステムログに出力された障害情報，ネットワーク機器及びサーバのリソース，パフォーマンス状況，メールログ，プロキシログ，さらにはクライアント端末の操作ログ等を

監視すること。

・ 閣副安危第 375 号（平成 24 年 7 月 5 日）「適切なログの管理による標的型攻撃対策について（情報提供）」（http://www.nisc.go.jp/active/general/pdf/logkanri_kanki_120705.pdf）に基づき，これらのログを 1 年間以上保存し，不正の検知，原因特定，問題の解決に役立てること。

なお，セキュリティ向上のため，「6.3.8.情報セキュリティ管理」と「6.3.9.性能管理」を甲は乙との協議の上，蓄積するログの種類，期間について設定・変更が可能とする。また，証跡の不当な消去や改ざんを防止するため，証跡に関するアクセス制御を考慮し，保護に努めること。

② 監視対象

・ 別紙 2，3 及び 4 に記載の各拠点に設置してある各種ネットワーク機器及び全サーバ機器等を監視対象とする。

③ 監視体制

・ 平日 8:30～17:45 においては，甲庁舎内の情報管理室にて常時監視すること。

④ 監視基盤

・ ネットワークセグメント及び機器の死活，サーバの重要プロセス及びサービス稼働状況については，次期宮内庁 NW で導入される監視ツールを使用し監視すること。

・ 新しく宮内庁 NW に接続された機器がある場合，甲担当者と協議の上，監視ツール上に追加すること。

・ 監視ツールの最新データベースのバックアップも取得すること。

(2) ネットワーク上のコンピュータの IP アドレス，ホスト名の台帳管理

① 管理台帳

・ 現行の管理台帳を使用し政府共通 NW グローバルアドレスを含む各セグメントの IP アドレス，機器の設置場所，接続状況及びホスト名を管理すること。

(3) 資産管理ソフトウェアによるインベントリ管理

・ 資産管理ソフトウェア及び WSUS 上に登録されたサーバやクライアント端末について，機器の設置場所や構成に変更があった場合は登録情報を更新し，データベースのメンテナンスを実施すること。

(4) ネットワーク機器の設定変更

・ ネットワーク機器が追加された場合，甲担当者の指示のもと，ルータやモデム，スイッチ等のネットワーク機器の設定を変更し，疎通確認すること。

・ ネットワーク機器の設定情報を修正した際には最新のコンフィグ情報を取得し，ファイルサーバ等に保存すること。

6.3.7.ユーザ管理

6.3.7.1 アカウント管理

(1) 現行の宮内庁 NW では，ユーザ管理システムによりアカウントの管理を実施している。AD サーバ及びグループウェアサーバと連動して管理すること。

(2) 甲アカウントは，ユーザの属性情報を含めて管理しており，ユーザの異動などによる属性情報の変更があった場合には，遅滞なく適切に変更を行うこと。

6.3.7.2　パスワードの管理

(1)　各サーバ，ネットワーク機器のパスワードを管理すること。

(2)　甲担当者からの指示により，ドメイン管理者用のパスワードやネットワーク機器のパスワード変更を行うこと。

(3)　管理者用のパスワード変更等，影響範囲の大きいものは事前に計画書を作成し，甲担当者の承諾を得ること。

6.3.7.3　アクセス権の管理

(1)　ファイルサーバアクセス権限の管理をすること。

(2)　各部局の庶務係からの問合せに対し支援を行うこと。

(3)　IDM の仕組みを理解した上で，個人認証方式によるアカウント管理及びアクセス権管理を行うこと。

6.3.8.情報セキュリティ管理

6.3.8.1　コンピュータウイルス対策

(1)　基本方針

「13.資料閲覧」時に供する甲の情報セキュリティポリシーに則り，サーバ（Linux サーバを含む），クライアント端末，貸出し用クライアント端末，地方サーバ及び各業務システムに対しウイルス対策ソフトウェアを最新に維持すること。日常的に情報セキュリティに関する情報収集を行うとともに遅滞なく適切な対策立案を行い，対策立案を行った場合には，甲担当者にその内容を報告し，その実行について協議を行い，甲の承諾を得た上で実施すること。

なお，情報セキュリティに関する情報収集を行う場合は，本調達仕様書（案）「1.15.1.情報セキュリティの確保」の(11)を参考にしつつ，宮内庁 NWS で採用したソフトウェア及びハードウェア等の製造事業者等が提供する情報等も参考にすること。

(2)　ウイルス等に感染の可能性がある場合の対応

(ア)　速やかに甲担当者にウイルス感染の可能性について報告を行うとともに，対象となる全ユーザに通知及び所要の対応をとること。

(イ)　感染経路として WEB 閲覧が疑われる場合は，ウイルスの感染元となるインターネットサイトの URL を分析する無料のサービス等を利用し，確認を行うこと。次に示すのは，そのサービスの一例である。

- Virustotal　https://www.virustotal.com/ja/
- TrendMicro　https://global.sitesafety.trendmicro.com/?cc=jp
- Norton　https://safeweb.norton.com/

(ウ)　ウイルス等の検体の抽出が可能な場合は，検体を抽出し，宮内庁 NWS で採用したウイルス対策ソフトウェアの製造業者へそれを提供し，解析を依頼すること。

(エ)　ウイルス等又は事象が既知であり，製造事業者等から対策が提供可能な場合には，再発防止策を講じ，甲担当者の承諾を得た上で必要な対応をとること。

(オ)　ウイルス等の内容，ふるまいなどから，その影響範囲が広い又は影響度が強いと考えられる場合には，本調達仕様書（案）の「6.3.14.情報セキュリティインシデント対応」に従って適切

な対応を行うこと。

(3) 対応拠点

別紙 2，3 及び 4 に記載の各拠点に設置してある各種ネットワーク機器及び全サーバ機器等を対象とする。

(4) 適用促進

ウイルスソフト適用状況を可能な限り自動的に常時把握し，適用不備のあるノードの管理者に対し適用促進を行うこと。

6.3.8.2 Windows 等のセキュリティパッチ対策及びバージョンアップ作業

(1) ソフトウェア配布方式

① ソフトウェアのアップデートやパッチに関しては，資産管理ソフトウェアや WSUS などを使用し，ネットワークを通じクライアント端末に直接インストールする方式 （自動配信方式。ユーザがダウンロードしてインストールする場合も含む。），又は甲の指示する電子媒体によりデリバリする方式（媒体方式）によるものとすること。

② ネットワーク接続していないクライアント端末に関しては，別途指示を行うこととする。

③ サーバへの Windows セキュリティパッチ適用に関しては，甲担当者からの指示により実施すること。実施時には，行事などの実施時間に重複しないよう，適用スケジュールを策定し，甲担当者と事前調整を行うこととする。

④ サーバにインストールされたソフトウェアのアップデートやパッチに関しては，別途指示を行うこととする。

⑤ 現行の運用管理業務では， クライアント端末への Windows セキュリティパッチ適用において，WSUS を利用して拠点別に Windows パッチを配布している。

※ 特に NISC（内閣サイバーセキュリティセンター）より注意喚起されたセキュリティ事象に関しては，調査・報告を行い，甲の現状に適した対策を提案すること。

⑥ クライアント端末がソフトウェアの配布を受ける際，既に同一のセグメント内のクライアント端末に配布されたソフトウェアがキャッシュとして残っていた場合，当該クライアント端末からソフトウェアを配布すること。

(2) 配布の必要性検討

運用作業員は，ソフトウェアの配布，更新について，必要性，問題点，適用是非について検討後，甲担当者の承諾を得て実施を行うこと。

【現行の運用管理業務（参考)】

① Microsoft がセキュリティパッチを公表後，遅滞なく動作テストを開始すること（甲担当者が指定したクライアント端末 3～5 台を利用すること)。

② 甲担当者が指定したクライアント端末で作動不良が発生しなかった場合は，甲担当者の承諾を受けクライアント端末に適用開始すること。

③ トラフィック状況や配布対象拠点のスケジュール，配布にかかる時間等を考慮し，甲担当者の承諾の得た配布スケジュールを組むこと。

④ パッチ適用についてのユーザへの周知は余裕を持って最低 4 日前には行うこと。

⑤ 配布後速やかにクライアント端末に適用すること。

⑥ 適用が遅いクライアント端末は個別対応とすること（ユーザの希望に添う形で次の配布前ま

でに対応が終了することが望ましい。)。

(3) 配布対象拠点

別紙 2，3 及び 4 に記載の各拠点に設置してあるクライアント端末を対象とする。

(4) 配布対象ソフトウェアの事前動作テスト

① 配布するソフトウェアが甲の環境で問題なく動作するかどうかの確認を実機で検証すること。

② 検証結果を甲担当者へ報告すること。

③ 資産管理ソフトウェアで配布が可能なパッケージになるよう，必要に応じてバッチファイルやスクリプトを作成すること。

④ 配布に際してユーザの対話的操作が必要なパッチは，対話的操作なしで配布・適用が可能になるようバッチファイルやスクリプトを作成すること。

(5) 配布対象ソフトウェア

① Windows セキュリティパッチ。

② Office セキュリティパッチ（甲担当者と協議の上，適用作業を実施)。

③ 一太郎，ATOK セキュリティパッチ。

④ プリンタドライバ。

⑤ その他，甲担当者が指定するセキュリティパッチやバージョンアップ版。

(6) 適用状況確認

セキュリティパッチの配布状況の確認を行うこと。未適用端末については，その適用が終了するまで個別対応にて適用作業を実施し，パッチ適用状況がまばらにならないよう適切に適用管理を行うこととすること（各端末のバージョンを揃えること。)。

(7) マスタ作成

Windows パッチ，各ソフトウェアのパッチ適用後のクライアント端末マスタを甲の指示する電子媒体により作成すること。

6.3.8.3 インターネット対策

(1) 甲担当者が情報セキュリティポリシーに基づき実施するアクセス制御，プロバイダ提供のコンテンツフィルタの設定（甲担当者が禁止した URL 閲覧のアクセス禁止設定）について対応すること。例外対応として，甲担当者からの指示により，一時的に閲覧が必要な URL をコンテンツフィルタのホワイトリストに登録し，閲覧可能な状態とすること。

(2) 迷惑メールについての資料を適宜甲担当者へ提出し，甲担当者から指示のある削除用キーワードをシステムへ登録するか，あるいはアドレスの一時的な停止について対応すること。

6.3.8.4 政府共通ネットワーク

(1) 新規メールドメイン登録依頼が来た場合，甲担当者の承諾を得た上で速やかに登録作業を実施すること。

(2) 甲担当者からの指示により，指定のポートを一時的に開放する等，政府共通 NW ファイアウォールの設定変更作業を実施すること。

(3) 新規の経路情報の登録依頼があった場合，ネットワーク機器やサーバへ速やかに経路情報を登録すること。

6.3.9.性能管理

6.3.9.1　システム運用と性能管理

(1)　日次運用

ハードウェア，ソフトウェアの安定的かつ正常な稼動を確保する観点で，以下のサーバに対してハードウェアの外観点検（例：インジケータランプの状態確認，ケースの変形有無確認），各リソース（CPU，メモリ等の主記憶装置，HDD 等の補助記憶装置）の使用状況（平均，ピーク，時間変化）等の実測値の把握及び適切なリソース割当て作業の実施，正常設定の確認等（各サーバの設定の変更前後の管理や世代管理，ログ（イベントログ，Syslog 等）の確認とログが一杯になった時の保存・退避・消去）を実施すること。

なお，今後の各システムの更新に伴い，対象となるサーバは増減することがある。

① ActiveDirectory サーバ
② ファイルサーバ
③ バックアップ管理サーバ，バックアップメディアサーバ
④ 外部ファイル共有サーバ
⑤ ユーザ管理サーバ
⑥ メール中継サーバ
⑦ ウイルス対策サーバ
⑧ WSUS サーバ
⑨ クライアント運用管理サーバ
⑩ プロキシサーバ
⑪ 京都サーバ
⑫ ネットワーク管理システム
⑬ グループウェアシステム
⑭ 正倉院宝物公開管理システム
⑮ CAD システム
⑯ KMS サーバ
⑰ 資産管理サーバ
⑱ 標的型攻撃対策システム
⑲ ADFS サーバ
⑳ 暗号化管理サーバ
㉑ 暗号化ファイルサーバ
㉒ その他

マシン室設置の各ネットワーク機器，ファイアウォール，アプライアンス機器及び無停電電源装置（UPS）についても，インジケータランプの確認等を実施すること。

6.3.9.2　システム稼働状態の把握

システムに負荷がかかっているかどうかの判断をするために，【6.3.9.1.システム運用と性能管理】にて取得した情報からハードウェア資源の使用量が基準を超えていないか把握すること。

6.3.9.3　トラフィック状態の把握

別紙 2，3 及び 4 に記載の各拠点のトラフィックを監視すること。ネットワークの負荷を判断するために，常時監視によりトラフィック量が基準を超えていないか，把握すること。

6.3.10.サーバ室温度管理

サーバ室の室温が 28℃以上になった時，甲担当者及び運用担当者のメールアカウント及び運用担当者又はその管理者の携帯メールに異常を知らせるためのアラートメールを送信する設定をすること。運用担当者又はその管理者は，アラートメール受信（24 時間 365 日受信対応が可能であること。）後は速やかに，甲担当者に報告を行い，空調機確認のアクションを取ること。

6.3.11.予備機器，消耗品等の管理

⑴管理対象

クライアント端末，HUB，UTP ケーブル，デジタル周辺機器等の予備機，保証書及びライセンス証書並びに保証書（写し）も含む。

⑵保管場所

保管場所については，甲からの指示に従うこと。

⑶管理内容

予備機器，消耗品の在庫状況及び修理状況を把握すること。

⑷緊急支援

予備機器が修理未了及び消耗品に欠品がある状況で障害が発生した場合は，甲担当者と相談の上，障害復旧支援を行うこと。

6.3.12.ユーザサービス（ヘルプデスク）

6.3.12.1 サービス範囲

サービスデスク業務は，宮内庁 NW を利用するユーザ及び当該ユーザが利用する機器等に対し提供される。運用管理業務は，通常運用管理，障害対応と適切に連携して行うことが求められる。

6.3.12.2 ユーザサービス

宮内庁 NW の利用に際しては，ユーザの申請に基づきサービスを提供することが原則となっている。ユーザサービスはユーザからの申請を受付けて対応するものであり，以下に列挙する作業内容を含む（具体的内容は例示であり，これに限定されるものではない。）。

(1)　アカウント関連の申請対応

ユーザアカウントの新規作成，変更，メールアドレスの新規作成，パスワード新規作成，再発行，人事異動に付随した各種設定変更（人事異動情報は，ユーザ管理システムを使用）及びユーザアカウント・機器等の関連付け情報の管理等，ユーザへのサービスに影響がないよう必要な作業を確実に実施すること。

(2)　ソフトウェア，アプリケーション等の配布（インストール）管理

ソフトウェア，アプリケーション及びドライバ等の配布（インストール），削除（アンインストール）及び同ライセンス管理を行うこと。

(3) アクセス権の付与

① 人事異動等に伴うファイルサーバへの共有フォルダアクセス権の付与。

② ファイルサーバへの一時的なアクセス権の付与。

③ 個別又は組織横断的な利用権限を設定する必要のある特定のフォルダの利用設定。

(4) インターネット（外部）からの情報のダウンロード

原則として禁止しているインターネット（外部）からの情報のダウンロードのための，一時的なコンテンツフィルタリングの設定変更を行うこと。

(5) 貸出し用クライアント端末，デジタル周辺機器等の貸与，設定及び管理

① 情報管理室に保管されている貸出し用クライアント端末等について，甲担当者からの指示に基づき，貸出し，設定及びその管理を行うこと。また，貸出し時には，スタンドアロン用，宮内庁NW 接続用に応じ，ソフトウェア，アプリケーション及びドライバ等のインストールを行うこと。

② 個別ユーザの申請に基づきソフトウェアの追加，設定を行うこと。

③ 貸出し用クライアント端末全台に対し新規ソフトウェアをインストールする作業等，個別ユーザ申請とは言えないものは，随時運用管理とし，本調達の対象外とする。

④ 必要に応じて，ユーザ等への貸出し機器の説明や操作方法についての説明を実施すること。

(6) IP アドレスの管理

① 機器等，クライアント端末，プリンタ等，個別システムの IP アドレス及び関連情報を管理すること。

② ネットワークに接続する必要がある機器等に対して，IP アドレスの付与，変更，削除を行うこと。

(7) 簡易配線

クライアント端末及びプリンタ等の新設，増設，移設に伴う UTP ケーブル等の簡易配線及び UTP ケーブル作成を行うこと。

(8) 申請全般に係る対応

ユーザ管理システムに関するユーザからの使用方法などの問合せについて対応すること。

(9) イントラネット上の FAQ（宮内庁職員情報ボード）の更新作業

宮内庁職員情報ボードに関するユーザからのアクセス権限，更新作業依頼などの問合せについて対応すること。

(10) その他，個別事項に係る対応について

ユーザからの各種問合せ，申請等に関して，随時対応すること。

6.3.13.問合せヘルプ

問合せヘルプ対応は，ユーザサービス業務，障害対応の窓口となるものである。以下の対応内容を含むものとする。

なお，対応は分かりやすい日本語とする。

(1) 問合せ対応

① ユーザが利用するハードウェア及びソフトウェアの操作，障害等に関する問合せ対応

② サーバ，ネットワーク機器等の設定，障害等に関する問合せ対応

③ 各地方拠点との接続環境に関する問合せ対応

(2) 一次切り分け

① 問題の所在の切り分け

② 障害対応（ユーザの利用する機器等のリプレイス等）

(3) リモートツールによる対応

① 現行宮内庁 NW では，資産管理ソフトウェアを全拠点のクライアント端末に配布済みであり，問合せヘルプ業務において本製品を利用することが可能である。

② ユーザに負担なく円滑に支援業務を遂行すること。

(4) オンサイトによる対応

6.3.14.情報セキュリティインシデント対応

甲担当者，宮内庁 NWS に含まれる各システムの保守事業者

6.3.14.1 現状把握

(1) 影響範囲の推定

① 各種ログ(操作，実行，通信等の履歴)を確認，整理，解析することで，情報セキュリティインシデントの影響範囲を推定すること。

-【参考】ログの取得については次を参照。「適切なログの管理による標的型攻撃対策について（情報提供）（閣副安危第 375 号 平成 24 年 7 月 5 日）」

http://www.nisc.go.jp/active/general/pdf/logkanri_kanki_120705.pdf

② 必要に応じて宮内庁統合 NW の統合 SOC サービスからの情報の提供を受け，プロキシサーバやファイアウォール等にある外部（インターネット等）との通信ログを確認，時系列による整理と解析を行って攻撃対象範囲の絞り込みを行いつつ，実際に攻撃対象となった端末又はサーバの特定を行うこと。

③ ネットワーク機器等の設定情報やログの改ざんが無いかの確認を行うこと。また，次の注意喚起などを参考にし，AD などのディレクトリ・サービスに対し，サーバ上の各種ログも解析すること。

<<< JPCERT/CC Alert 2014-12-19 >>> Active Directory のドメイン管理者アカウントの不正使用に関する注意喚起 https://www.jpcert.or.jp/at/2014/at140054.html

④ 攻撃対象となった端末又はサーバ及び外部への不審な通信履歴などが特定された場合，適宜，プロキシサーバやファイアウォールなどの設定の見直しを図りつつ，各組織の判断により外部との通信を遮断（遮断した場合の影響を十分に考慮，対処した上で）するなどの処置を検討する。

(2) 被害の特定

まず証拠保全を行う。次に攻撃対象となった端末又はサーバ上のファイルに不正なアクセス又は操作の履歴がないか確認することで，被害の特定をする。

- 攻撃対象となった端末又はサーバ上での証拠保全を行う
  - 「証拠保全ガイドライン 第 6 版」（2017 年 5 月 9 日 特定非営利活動法人デジタル・フォレンジック研究会 「技術」分科会ワーキング・グループ）
    https://digitalforensic.jp/home/act/products/df-guideline-6th/
  - デジタル・フォレンジックを実施し，電磁的記録の証拠保全及び調査・分析を行い，電磁的記録の改ざん・毀損等について分析・情報収集等を行う。
  - 不正なアクセス又は操作履歴がないかの具体的な確認方法は，以下も参考になる。
  - 【注意喚起】潜伏しているかもしれないウイルスの感染検査を今すぐ！(IPA)
  - https://www.ipa.go.jp/security/ciadr/vul/20150629-checkpc.html

- 「高度サイバー攻撃への対処におけるログの活用と分析方法」
- https://www.jpcert.or.jp/research/apt-loganalysis.html
- JPCERT/CC「ログを活用した Active Directory に対する攻撃の検知と対策」
- https://www.jpcert.or.jp/research/AD.html

・ 攻撃対象となった端末又はサーバにて適切に証拠保全がなされたならば，2 社以上の異なる製造業者製のウイルス対策ソフトウェア（必ず最新にアップデートしたもの）を用いてフルスキャンを実行
  - 既にインストールされているウイルス対策ソフトウェアの製造業者とは異なる製造業者製ウイルス対策ソフトウェアを用いることにより，製造業者の得意，不得意，そして新しいウイルスへの対応の早さなどの違いを補完し合う。
    なお，ウイルス対策ソフトウェアは，同一 OS(Operating System)上ではシステム競合を起こすため，必ず一つの OS 上では一つのウイルス対策ソフトウェアとなるよう，適切にアンインストール又はインストールを行うこと。

・ 攻撃対象となった端末又はサーバ上での操作ログの確認，時系列による整理と解析
・ 攻撃対象となった端末又はサーバを起点とした通信ログの確認，時系列による整理と解析
・ ここまでに得られた各ログを時系列に並べて整理し，ログ同士の関係性がないか解析（相関分析等）し，感染経路を特定
・ 攻撃対象となった端末又はサーバについては，ウイルス対策ソフトウェアと連携して遮断の上，端末の資産管理ソフトウェアにてネットワークの隔離を行いながら調査に必要な通信の解析及びリモートによる解析を行うこと。

(3) 情報の取り扱い状況の確認

攻撃対象となった端末又はサーバ上での情報の取り扱いについて，組織における情報セキュリティポリシーやその他規程に則り，適切な情報の取り扱いをしているかを確認する。

・ 取り扱われていた情報はどういう性質（機密性，完全性，可用性）のものだったか
・ ファイル又はフォルダへのアクセス制御を施していたか
・ ファイル又はフォルダに暗号化を施していたか（暗号危殆化に配慮しつつ）
・ パスワードの管理は適切であったか
  - 同じパスワードの使い回しはしていないか
  - 比較的わかりやすいパスワードでないか
  - 付箋紙などに書いて人の目につきやすいところに置いていないか　など

(4) 脆弱性の確認

セキュリティ侵害のリスクを減らす目的で，既知の脆弱性を点検する。脆弱性の対策が施されていなければ，対策を施す。

・ インストールされているソフトウェアのセキュリティパッチの適用状況の確認
・ OS 及び各アプリケーションソフトウェアが最新のものにバージョンアップされていることの確認（MyJVN バージョンチェッカの利用）
  http://jvndb.jvn.jp/apis/myjvn/vccheck.html
・ プロキシサーバ，ファイアウォール，ネットワーク機器等が適切に設定されていることの確認
・ 既知の脆弱性の対策の適用状況の確認　など

(5) 残存リスク等の把握

・ リスクアセスメント（①標的とされる蓋然性の高い業務領域の選定，②リスク評価の実施）を実施しつ

つ，改めて取り扱う情報は何であり，どのような社会的意味を持ち，どのような影響を与えるものかなどを分析し直す。

- 「国家安全保障戦略（平成 25 年 12 月 17 日　国家安全保障会議決定　閣議決定）」(5)サイバーセキュリティの強化「平素から，リスクアセスメントに基づくシステムの設計・構築・運用」 http://www.cas.go.jp/jp/siryou/131217anzenhoshou.html
- 「高度サイバー攻撃対処のためのリスク評価等のガイドライン（平成 26 年 7 月 10 日　NISC）」 http://www.nisc.go.jp/active/general/risk.html
- 「情報セキュリティマネジメントと PDCA サイクル（IPA）」 http://www.ipa.go.jp/security/manager/protect/pdca/risk_ass.html

6.3.15.情報システムインシデント対応

宮内庁本庁舎及び各拠点に設置されている宮内庁 NWS を構成するサーバ機器，ネットワーク機器，クライアント端末が対象。ただし，宮内庁統合 NW のインターネット側に設置されている機器等は除くこととする。

なお，宮内庁統合 NW との境界点で発生した情報システムインシデントについては，宮内庁統合 NW 受託者と互いに情報共有を行い，密に協力して対応することにより，迅速な解決を行うことにより，ユーザの業務遂行への影響を最小化すること。

(1)　障害検知

①　リモート検知

宮内庁 NW 各拠点のネットワーク（ただしアクセススイッチ，ルータまで）及びサーバ等について，監視装置により異常検知すること。

②　ユーザによる通報

ユーザからの通報に対し，速やかに状況を確認すること（ユーザからの通報には，電話による通知とメールによる通知の 2 種類がある。）。

(2)　発生時対応

①　一次切り分け

- 障害を検知した場合は速やかに障害発生機器等を特定し，ハードウェア障害，ソフトウェア障害等の一次切り分けを実施すること。
- 全ての情報機器のうち，データの保存されている障害機器を持ち出すことになった場合は，情報漏えいがないようデータ消去すること。
- 物理的にデータ消去が不可能な場合には，甲担当者に報告した上で指示を仰ぐこと。

②　システム保守事業者，製造事業者等保守契約の関係者に連絡をとること。また，修理に必要な障害内容報告書を作成すること。

③　必要に応じて障害機器における障害発生日時前のコンフィグやログを取得し，障害切り分けを行うこと。

④　回線異常と判断した場合は，甲担当者を通じて回線事業者へテスト及び修理対応を依頼すること。

⑤　ディスクリソースやメモリリソースでの異常と判断した場合は，甲担当者の承諾を得た上で復旧作業を行うこと。

⑥ サービスデスクによるクライアント端末障害対応

・ クライアント端末については，リモートツールによるユーザとの対話形式での対応を行うものとする。

・ 甲担当者の指示により，障害機器については，システム保守事業者，製造事業者等の保守契約関係事業者に連絡をとり，修理完了まで管理すること。ただし，クライアント端末のシステム不調に対しては，その不調の状態に応じて HDD の初期化，OS の再設定，個別ソフトウェアの再インストールなどを適宜実施し，当該クライアント端末を利用するユーザの環境に合わせて正常に動作するよう適切に設定を行うこと。

なお，マスタ・イメージが存在するクライアント端末（一般事務用端末，追加一般事務用端末，CAD 用端末）については，そのマスタ・イメージを利用して復元を行い，当該クライアント端末を利用するユーザの環境に合わせて正常に動作するよう適切に設定を行うこと。

・ プリンタ（リース物品）の障害について保守が必要な場合は，甲担当者に対して，製造事業者等窓口に保守を依頼するよう伝えること。

(3) 復旧

① 各システムの保守事業者，製造事業者等保守契約の関係者による復旧作業に対し，適切に情報提供等の支援を行うこと。復旧後の動作確認を実施すること。

② 復旧作業に際し，作業員がサーバ室への入室が必要となる場合は，事前に保守担当者の氏名や機器の搬入経路等を把握し，甲担当者の承諾を得た上で入庁及び搬入の手続きを支援すること。また，来室した時点で本人確認を行い，入退室の時刻や作業内容を指定の書類へ記載し管理すること。

③ 冗長化された機器の障害復旧作業は，保守事業者と協力し，切り戻しまで行うこと。

④ クライアント端末及びプリンタで発生した障害については，指定の書式で記録し，発生時の現象や復旧までの対応を管理すること。

(4) ステータス管理

① 障害検知から復旧完了までのステータスを逐次記録し，遅滞することなく報告すること。

② 継続的又は断続的に発生している障害がある場合は，構築事業者や保守事業者と協力し，対策を講じること。

(5) 事後管理

① 障害検知から復旧完了までの記録を含む障害情報，障害対応支援内容につき履歴管理情報を更新すること。

② 発生した障害について，再発を防止できる対策を講じ，甲担当者へ報告すること

6.4.宮内庁 CIS 以外の宮内庁 NWS の運用管理

個別システムの運用管理については，【6.3.8.情報セキュリティ管理】及び【6.3.9.性能管理】に記載されている各項目のほか，次のとおり個別システムの運用管理を実施すること。

6.4.1.正倉院宝物公開管理システム

必要に応じてバックアップテープを本庁から送付すること。また，返却されたテープを管理すること。また，正倉院宝物公開管理システムの宝物管理用端末 2 式（正倉院事務所）は，本調達の運

用管理の対象となるので，次の作業内容を実施すること。

(1) OS のアップデート又はパッチ適用

(2) ウイルス対策ソフトのアップデート又はパッチ適用
必要に応じたソフトウェアのインストール又はアンインストール

6.4.2.ＣＡＤシステム

① データベースのバックアップ取得状況を確認すること。

② UPS を含むシステム全体の LED 表示状態確認をすること。

6.4.3.電子メール中継サーバ

① サーバのデータ領域のバックアップ取得状況を確認すること。

② UPS を含むシステム全体の LED 表示状態確認をすること。

6.4.4.グループウェアシステム

グループウェアシステムに関して，次のとおり実施すること。

(1) グループウェア機能が適切に提供されているか，サーバ等の稼働確認を行うこと。適切に機能が提供されていない場合は，遅滞なくインシデント管理を行うこと。

(2) ユーザがグループウェアシステムを利用するために用いるクライアントソフトウェアとグループウェア機能を提供するサーバ等との連携が正常に機能しているか確認を行うこと。

(3) メール中継サーバとグループウェア機能を提供するサーバ等との連携が正常に機能しているか確認を行うこと。

(4) ユーザのメールアドレス，グループメールアドレスの管理（作成，変更，削除）を行うこと。

(5) ユーザのグループウェアのアカウントについて，ディレクトリサーバとの連携が正常に機能しているか確認を行うこと。

(6) メール誤送信防止機能が適切に提供されているか，サーバ等の稼働確認を行うこと。

(7) グループウェアシステムのオンプレミス型のサーバ等に対し，ソフトウェアのアップデート又はパッチ適用を適切に行うこと。

(8) グループウェアシステムのオンプレミス型のサーバ等のハードウェアにおいて，LED 表示状態を確認すること。

(9) グループウェアシステムのオンプレミス型のサーバ等において，冗長化された構成であるものについては，冗長化機能が正常に機能しているか確認を行うこと。

(10) 現行のグループウェアシステムの賃貸借期間は，2021 年 8 月 31 日までである。この間にグループウェアシステムの更改がある場合には，ユーザが更改後のグループウェアシステムの（以下，「次期グループウェアシステム」という。）を利用して行う業務が遅滞なく遂行できるよう，次期グループウェアシステムの稼働後の効率的かつ安定的な運用を見据え，設計・構築段階から IT サービスマネジメントの観点で可能な限り協力し，適宜助言を行うこと。

6.4.5.標的型攻撃対策システム

標的型攻撃対策システムに関して，以下のとおり実施すること。ただし，現行の標的型攻撃対策システム構成要素のうち，メール標的型攻撃対策サーバ及び簡易 SOC サービスについては含まない。

(1) Web 標的型攻撃対策サーバ及びファイアウォールの稼働確認を行うこと。
(2) 簡易 SOC サービスからの情報セキュリティインシデント発生の報告を確認し，その内容に対して次の事実確認を行うこと。

運用管理業務の対象となる甲の各拠点（ただし，データセンタを除く。）に設置されたサーバ，ネットワーク機器，クライアント端末に関する不正な通信の可能性がある場合には，情報セキュリティインシデント対応を行うこと。

(3) ファイアウォールの稼働確認を行うこと。
(4) ファイアウォールポリシーの更新を行うこと。
(5) UPS を含むシステム全体の LED 表示状態を確認すること。

6.4.6.電子ファイルの暗号化及びアクセス制御機能

電子ファイルの暗号化及びアクセス制御機能について，以下のとおり実施すること。

(1) OS のアップデート又はパッチ適用
(2) ウイルス対策ソフトのアップデート又はパッチ適用
必要に応じたソフトウェアのインストール又はアンインストール
(3) ソフトウェアに対する修正パッチ及び修正モジュールがメーカから提供された場合に，適用要否を検討し，甲担当者と協議し，必要なパッチについて適用を行うこと。
(4) 運用上バックアップが必要なファイル群のバックアップ
(5) 暗号鍵及びシステム復旧する上で必要なログファイルのバックアップ
(6) UPS を含むシステム全体の LED 表示状態を確認すること。
(7) 電子ファイルの暗号化及びアクセス制御機能のサーバ等において，冗長化された構成であるものについては，冗長化機能が正常に機能しているか確認を行うこと。
(8) 甲担当者の求めに応じて，必要な設定変更を行うこと。
(9) 障害が発生した場合は，バックアップイメージ等からシステム復旧を行うなどの措置を行うこと。また，復旧後に暗号化機能が正常に動作しているか確認すること。

6.4.7.Web 無害化機能

Web 無害化機能について，甲担当者の求めに応じて，プロキシ設定変更を行うこと。

6.5. 機器等の変動に関する支援

乙は，将来更新が予定されている本調達仕様書（案）「6.6.機器等の変動」に示す 11 の各次期システム等について，更新作業を適正かつ円滑に行うため，11 の各次期システム等機器賃貸等事業者（以下「次期システム事業者」という。）が開催する会議への参加，各次期システム運用に必要な環境設定支援，検証等を専門的知識からの支援，助言を行うこと（表 1.各次期システム等機器変動（更新・移行）に伴い想定される乙の作業等）。

なお，各次期システム更新に係る設計，開発は次期システム業者が実施する。

表 1.各次期システム等機器等変動に伴い想定される乙の作業等

項　目	詳　細	役　　割			想定される受注者の作業等
		受注者	次期システム機器 賃貸借等事業者	宮内庁	
会議	運用業務設計に係る調整会議	参加	開催	参加・議事承認	毎週1回（60分×1回）の会議（運用管理責任者，運用作業員1名参加）
	システム更新に係る調整会議	参加	開催	参加・議事承認	
	テスト支援に係る調整会議	参加	開催	参加・議事承認	
	運用管理支援業務移行に係る調整会議	参加	開催	参加・議事承認	
システム運用業務設計（支援）	システム運用業務設計	支援	実施	設計承認	NW，システム構成，体制等の情報提供，助言
システム移行（支援）	システム移行作業支援	支援	実施	更新・移行結果承認	移行に伴うスケジュール調整，作業支援，トラブル発生時の支援
試験（支援）	単体試験 結合試験 総合試験	支援	実施	試験結果承認	システム全体の機能・性能の確認及び運用手順の検証支援
	受入試験			試験実施	
教育	システムの概要，運用，データ管理に係る教育	受講	開催	教育結果承認	2時間×4回程度想定
	テスト支援に係る教育	受講	開催	教育結果承認	
	運用マニュアル，仕様書の説明	受講	開催	教育結果承認	

6.5.1. 会議

次期システム事業者が開催するシステム更新・移行に係る会議に参加すること。

6.5.2. システム運用業務設計（支援）

次期システムの運用業務設計は次期システム事業者が実施する。乙は，宮内庁 NW 及び各システムの構成や運用体制等の情報について速やかに提示する等，次期システム事業者の支援を行うこと。

6.5.3. システム移行作業（支援）

次期システム事業者より提示されるシステム移行計画書に基づき移行スケジュールの調整支援，システム運用管理業務を移行すること。移行時においてトラブルが発生した場合には，次期システム事業者と連携し速やかにトラブルを解消すること。

6.5.4. テスト（支援）

次期システム事業者が作成，提示するテスト計画書，テスト実施要項に基づきテスト項目を支援すること。想定される次期システム事業者が行う各テストは次のとおり。各テスト実施に当たり，次期システム支援事業者及び甲より支援を求められた場合には支援を行うこと。

(1) 単体テスト
(2) 結合テスト
(3) 総合テスト
(4) 受入テスト

6.5.5. 教育

乙は，次期システム事業者が作成する教育計画書に基づき各システム運用管理業務支援に係る教育を受講すること。

6.5.6. その他

(1) 機器等の変動に関し，新規資産納入者への甲についての情報提供，導入検討，移行等必要となる支援を行うこと。
(2) 毎年 4 月 1 日付の人事異動はユーザ登録件数が多いことを理解した上で円滑に登録作業を遂行すること。

6.6. 機器等の変動

6.6.1. 宮内庁統合 NW 更新に伴う支援

「宮内庁デジタル・ガバメント中長期計画」（平成 30 年 6 月 22 日宮内庁行政情報化推進委員会決定）に基づくネットワークの更新作業を平成 31 年度に実施する予定である。更新スケジュールの概要は「図 2-1.宮内庁 NW 更新スケジュール」のとおり。詳細は，受注後に甲に確認すること。これに伴い，以下の支援を行うこと。

(1) 業務支援
① 宮内庁統合 NW の次期更新に係る会議に参加し，次に示す観点に基づいて次期宮内庁統合 NW の設計や運用等について助言すること。
ア 次期宮内庁統合 NW と宮内庁 CIS を始めとした宮内庁 NWS の各システムとの連携が円滑になり，ユーザの業務の効率化を実現
イ 宮内庁 NWS 全体として，各システムが連携し，効果的な情報セキュリティ対策の強化を実現
② 移行期間中においては，次期宮内庁 NWS 請負者と連携し，機器等の設定等について十分な調整を行い，甲からの問合せに対応すること。
③ 次期宮内庁統合 NW の受入テストの実施に立ち合うこと。
なお，受入テストの実施の主体は甲となる。また，次期宮内庁 NWS 請負者が受入テストの支援を行う。

(2) 更新機器等の管理
① 更新されるネットワーク機器等の運用管理等を行うこと。
② サーバ室への導入機器が発生する場合には，技術的な問題解決を行うとともに，協業して目

的を達成すること。

(3)　不測の事態への対応支援

導入に際して，宮内庁 NW に障害が発生した場合には，甲担当者及び障害に関連する現行他システム保守事業者と綿密な調整・連携を行い復旧に努めること。

(4)　設置・作業時の立会い

適宜，必要に応じて現地立会いを行うこと。

(5)　その他

本調達仕様書（案）に記載なき事項でも，本システムの構築・稼働・運用に必要と認められる事項は，甲と協議の上実施すること。

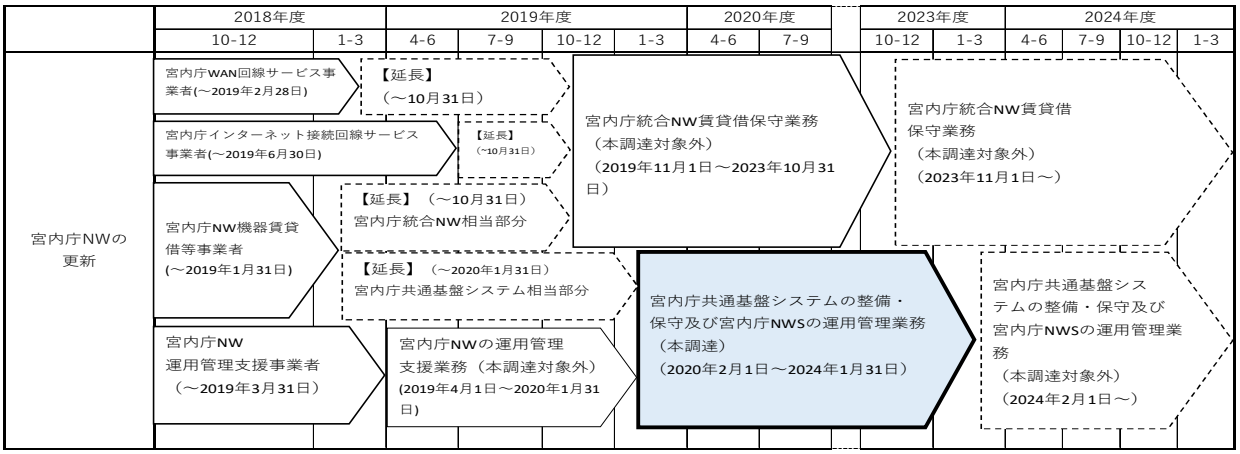


図 2-1.宮内庁 NW 更新スケジュール

6.6.2.　正倉院宝物公開管理システムの更新に伴う支援

正倉院宝物公開管理システムの更新作業を 2019 年度(2020 年 1 月より運用開始予定及び 2023 年度（2024 年 1 月より運用開始予定）に実施する予定である。更新スケジュールの概要は「図 2-2.正倉院宝物管理システム更新スケジュール」のとおり。詳細は，受注後に甲に確認すること。これに伴い，以下の支援を行うこと。

(1)　業務支援

正倉院宝物公開管理システムの次期更新に係る会議に参加し，運用管理等について助言すること。また，移行期間中においては，次期本システム請負者と連携し，環境設定等について十分な調整を行い，甲からの問合せに対応すること。

(2)　本調達仕様書（案）　6.6.1(2)～(5)と同じ。

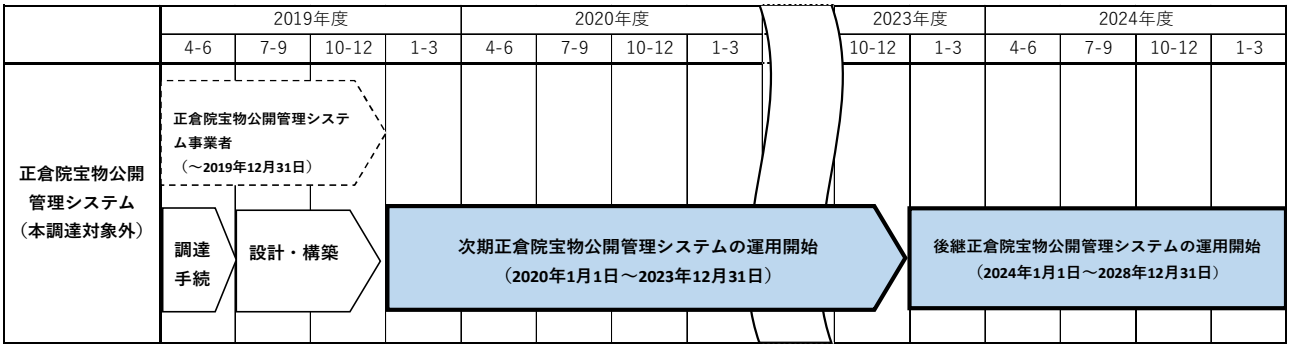


図 2-2.正倉院宝物公開管理システム更新スケジュール

6.6.3. 宮内庁公開システムの更新に伴う支援

宮内庁公開システムの更新作業を 2019 年度（2020 年 2 月から運用開始予定）及び 2023 年度（2024 年 2 月から運用開始予定）に実施する予定であるが，当該システムは政府共通 PF に移行したため，次期更新に係る会議への出席等は要さない。ただし，更新時に DNS 変換等が必要な場合，甲担当者の指示に従い対応すること。

6.6.4. パーソナルコンピュータ及びプリンタの更新に伴う支援

パーソナルコンピュータ及びプリンタの更新作業を 2020 年度中（2021 年 3 月より運用開始予定）に実施する予定である。更新スケジュールの概要は「図 2-4.パーソナルコンピュータ及びプリンタ更新スケジュール」のとおり。詳細は，受注後に甲に確認すること。これに伴い，以下の支援を行うこと。

(1) 業務支援

パーソナルコンピュータ及びプリンタの次期更新に係る会議に参加し，運用管理等について助言すること。また，入れ替え期間中においては，次期本調達請負者と連携し，甲からの問合せに対応すること。

(2) 本調達仕様書（案） 6.6.1(2)～(5)と同じ。

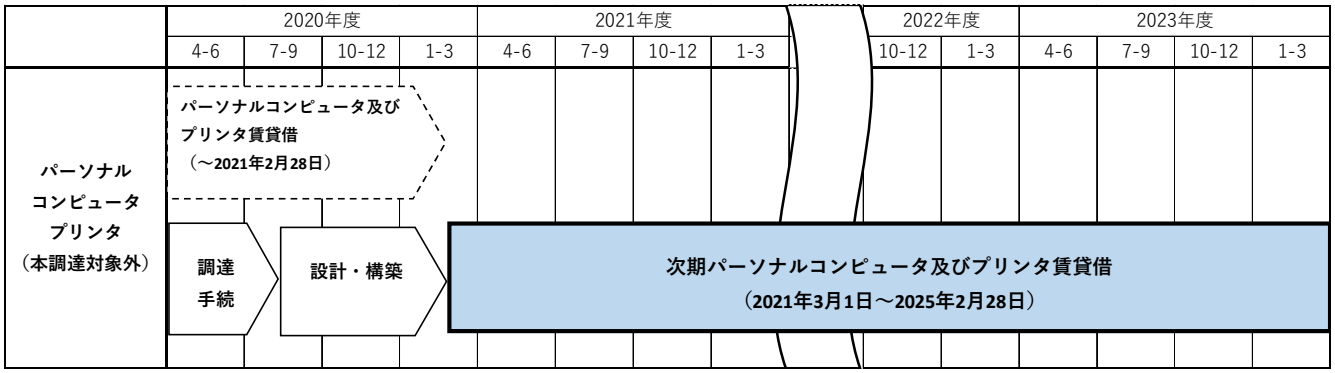


図 2-4.パーソナルコンピュータ及びプリンタ更新スケジュール

6.6.5. CAD システムの更新に伴う支援

CAD システムの更新作業を 2020 年度中（2021 年 3 月より運用開始予定）に実施する予定である。更新スケジュールの概要は「図 2-5.CAD システム更新スケジュール」のとおり。詳細は，受注後に甲に確認すること。これに伴い，以下の支援を行うこと。

(1) 業務支援

CAD システムの次期更新に係る会議に参加し，運用管理等について助言すること。また，移行期間中においては，次期本システム請負者と連携し，環境設定等について十分な調整を行い，甲からの問合せに対応すること。

(2) 本調達仕様書（案） 6.6.1(2)～(5)と同じ。

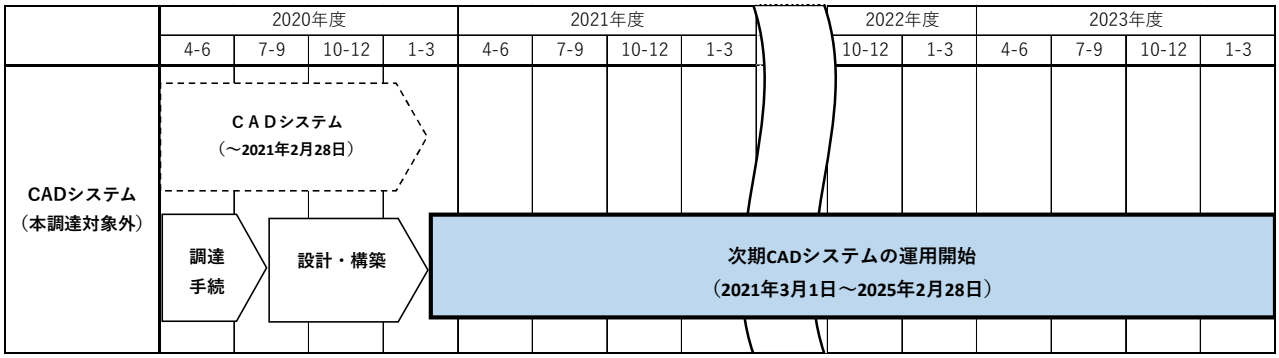


図 2-5.CAD システム更新スケジュール

6.6.6. グループウェアシステムの更新に伴う支援

グループウェアシステムの更新作業を 2021 年度中（2021 年 9 月より運用開始予定）に実施する予定である。更新スケジュールの概要は「図 2-6.グループウェアシステム更新スケジュール」のとおり。詳細は，受注後に甲に確認すること。これに伴い，以下の支援を行うこと。

(1) 業務支援

グループウェアシステムの次期更新に係る会議に参加し，運用管理等について助言すること。また，移行期間中においては，次期本システム請負者と連携し，環境設定等について十分な調整を行い，甲からの問合せに対応すること。

(2) 本調達仕様書（案） 6.6.1(2)～(5)と同じ。

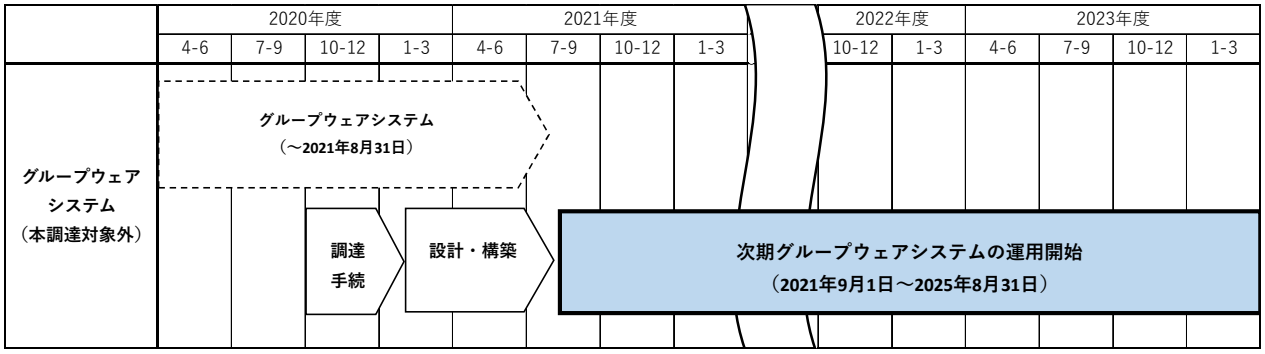


図 2-6.グループウェアシステム更新スケジュール

6.6.7. 標的型攻撃対策システムの更新に伴う支援

標的型攻撃対策システムの更新作業を 2021 年度中（2021 年 11 月より運用開始予定）に実施する予定である。更新スケジュールの概要は「図 2-7.標的型攻撃対策システム更新スケジュール」のとおり。詳細は，受注後に甲に確認すること。これに伴い，以下の支援を行うこと。

(1) 業務支援

標的型攻撃対策システムの次期更新に係る会議に参加し，運用管理等について助言すること。また，移行期間中においては，次期本システム請負者と連携し，環境設定等について十分な調整を行い，甲からの問合せに対応すること。

(2) 本調達仕様書（案） 6.6.1(2)～(5)と同じ。

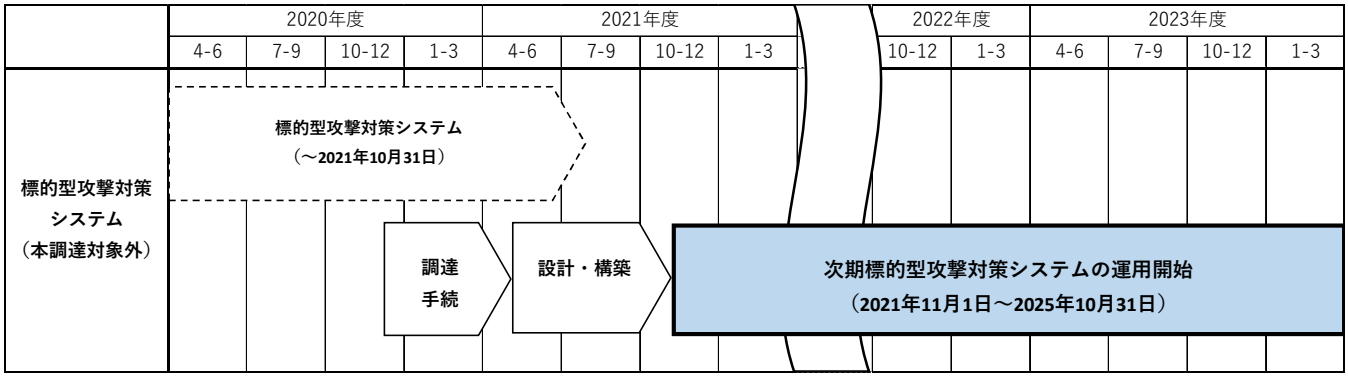


図 2-7.標的型攻撃対策システム更新スケジュール

6.6.8. ファイル自動暗号化システムの更新に伴う支援

ファイル自動暗号化システムの更新作業を 2021 年度中（2022 年 3 月より運用開始予定）に実施する予定である。更新スケジュールの概要は「図 2-8.ファイル自動暗号化システム更新スケジュール」のとおり。詳細は，受注後に甲に確認すること。これに伴い，以下の支援を行うこと。

(1) 業務支援

ファイル自動暗号化システムの次期更新に係る会議に参加し，運用管理等について助言すること。また，移行期間中においては，次期本システム請負者と連携し，環境設定等について十分な調整を行い，甲からの問合せに対応すること。

(2) 本調達仕様書（案） 6.6.1(2)～(5)と同じ。

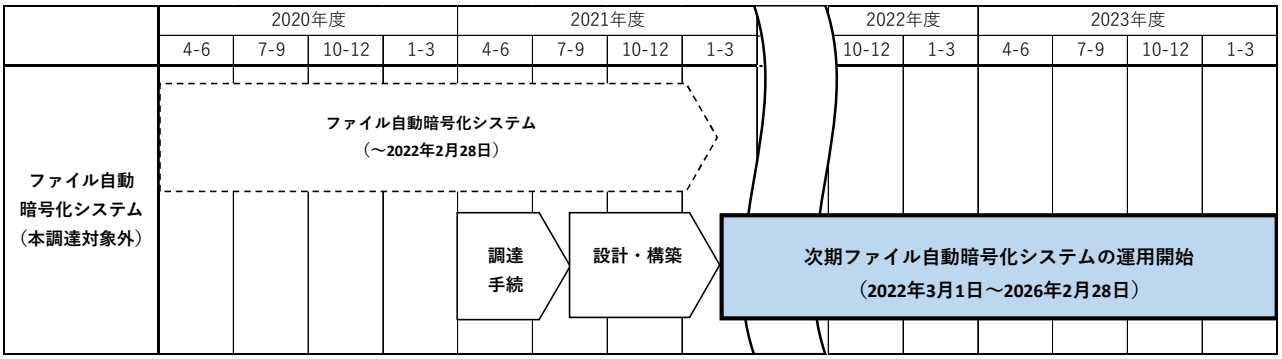


図 2-8.ファイル自動暗号化システム更新スケジュール

6.6.9. WEB 無害化システムの更新に伴う支援

WEB 無害化システムの更新作業を 2021 年度中（2022 年 3 月より運用開始予定）に実施する予定である。更新スケジュールの概要は「図 2-9.WEB 無害化システム自動暗号化システム更新スケジュール」のとおり。詳細は，受注後に甲に確認すること。これに伴い，以下の支援を行うこと。

(1) 業務支援

WEB 無害化システムの次期更新に係る会議に参加し，運用管理等について助言すること。また，移行期間中においては，次期本システム請負者と連携し，環境設定等について十分な調整を行い，甲からの問合せに対応すること。

(2) 本調達仕様書（案） 6.6.1(2)～(5)と同じ。

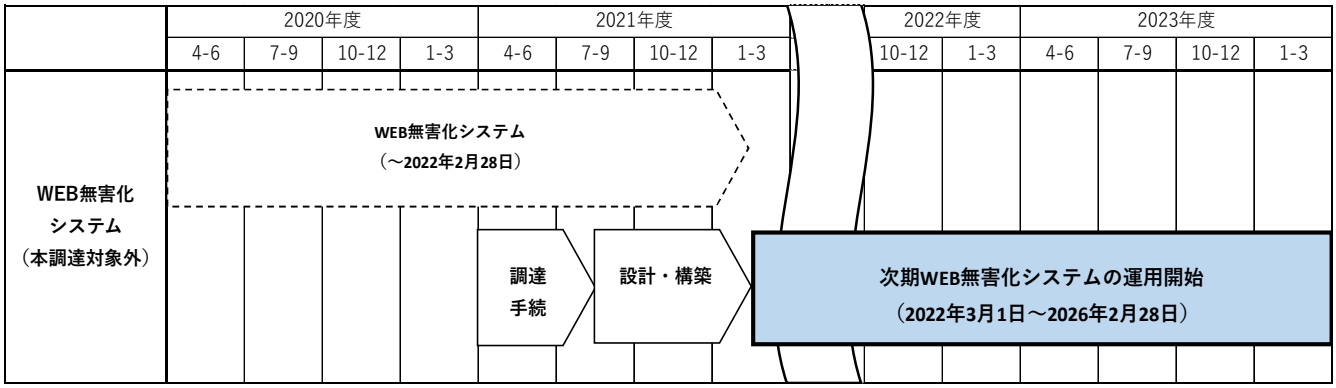


図 2-9.WEB 無害化システム更新スケジュール

6.6.10. 図書寮文庫所蔵資料目録・画像公開システムの更新に伴う支援

図書寮文庫所蔵資料目録・画像公開システムの更新作業を 2021 年度（2021 年 11 月から運用開始予定）に実施する予定であるが，当該システムは宮内庁 NW 外のクラウド環境にシステムを構築しているため，次期更新に係る会議への出席等は要さない。ただし，更新時にクライアント端末へのソフトウェアインストール等が必要な場合，甲担当者の指示に従い対応すること。

6.6.11. テレワーク導入に伴う支援

「宮内庁におけるテレワーク試行実施要領」に基づき実施（予定）するもので，実施の際には，円滑に導入できるよう支援を行うこと。

(1) 通信確認

テレワーク実施に伴い，次の確認を行うこと。

① ログイン動作確認
② メール動作確認
③ インターネット接続確認
④ 各アプリケーションの動作確認

(2) 実施状況（実績）

- 平成 27 年度～平成 29 年度
- 対象者：平成 27 年度 3 名，平成 28 年度 5 名，平成 29 年度 7 名
- 対象期間： 通年
- 利用サービス： 「13.資料閲覧」時に確認すること。

6.7. 計画停電対応

(1) 年 1 回実施される法定点検に伴う計画停電対応については，本調達の範囲内とし，次の対応を行うこと。

なお，法定停電日の具体的な日程については，甲担当者がその都度指示をする。

① 通常，法定点検に伴う計画停電は，休日に行われるので，休日対応とする。
② 停電の時間帯を基準に，サーバ及びネットワーク機器等の停止時間及び起動完了時間について，計画書を作成し機器等の停止及び起動を実施すること。

③　サーバ及びネットワーク機器等の停止，起動及び起動後のサーバ及びネットワーク機器等の動作確認を行うこと。

(2)　法定の停電以外の単発的な停電については，本調達の範囲外であるが，甲担当者の求めに応じて必要経費を見積り，法定停電と同様の対応を行うこと。

7.　会議体の設置

7.1.目的

本業務における基本設計書（宮内庁統合 NW の基本設計書は，6 月上旬に提出される予定。）及び詳細設計書（宮内庁 CIS の整備保守及び宮内庁 NWS の運用管理業務の契約締結前には内容が確認できる予定。）の確認・検討，作業の進捗状況，課題管理の対応状況等を確認し，実施するため，「宮内庁 NWS 統括会議」（以下，「統括会議」という。）を開催する。

7.2.会議体スケジュール

凡例

★ 契約締結
◆ 入札公告
● 基本設計書
▲ 詳細設計書

7.3.開催開始時期

宮内庁 CIS の契約締結日から運用開始前日までの毎週木曜日 13:30 から 15:00 を基本とする。

7.4.会議開催場所

甲が指定する場所。

7.5.会議必須参加者

(1)　甲

(2)　宮内庁統合 NW 受託者

(3)　宮内庁 CIS 受託者（次期運用管理事業者）

(4)　運用管理支援事業者

7.6.会議内容等

(1)　会議参加者は，本調達の目的を達成し，宮内庁 NWS 全体として機能するようために必要な情報共有及び議論を積極的に行い，協力し合うこと。

(2)　乙は，次期運用管理事業者として，運用管理業務の実施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積極的に行うこと。

(3)　会議で取り上げる題材は主に次のとおりとするが，その時々の状況に応じて変更を可とする。会議で取り上げる題材の資料は，会議開始日の前日までに甲へ提出すること。

・進捗状況（進捗管理）

・課題対応状況（課題管理）

・リスク対応状況（リスク管理）

・その他（必要に応じて）

特に宮内庁統合 NW と宮内庁 CIS との間で連携する内容を始めとして，契約が異なる情報システム間の連携が必要となる内容については，優先順位を上げて議論することとする。

なお，個別具体的な議論が必要な場合は，統括会議で協議の上で適宜，統括会議を親会議としたワーキング・グループを設置して議論し，円滑に設計・構築・運用を行い，議論の結果を統括会議へ報告すること。

8.　応札者条件

8.1.応札者としての条件

(1)　公共サービス改革法第 15 条において準用する同法第 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。以下「予決令」という。）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)　予決令第 71 条の規定に該当しない者であること。

(4)　平成 31・32・33 年度内閣府競争参加資格（全省庁統一資格）「役務の提供等」の「A」又は「B」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。

(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)　当庁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)　本調達仕様書の作成に直接関与した事業者及びその関連事業者（「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子会社並びに緊密な利害関係を有する事業者をいう。）ではないこと。

(9)　調達計画書及び調達仕様書の妥当性確認並びに入札事業者の審査に関する業務を行う宮内庁 CIO 補佐官及びその支援スタッフ等（常時勤務を要しない官職を占める職員，「一般職の任期付職員の採用及び給与の特例に関する法律」（平成 12 年 11 月 27 日法律第 125 号）に規定する任期付職員及び「国と民間企業との間の人事交流に関する法律」（平成 11 年 12 月 22 日法律第 224 号）に基づき交流採用された職員を除く。）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。又は，宮内庁 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。

（注）入札参加グループとは本業務の実施を目的に複数の事業者が組織体を構成し，本業務の入札に参加する者のことを指す。

(11) 本業務の実施予定組織・部門は，品質管理体制として ISO9001:2015 又は，組織能力成熟度の CMMI レベル３以上のどちらかの認証を取得しているか，同等の品質管理体制を構築できていることを必要十分に証明することが可能な資料を提出すること。

(12) 本業務の実施予定組織・部門は，プライバシーマーク付与認定，又は ISO/IEC27001 認証（国際標準）若しくは JIS Q 27001 認証（日本工業標準）のいずれかを取得していること。

(13) 本業務の実施予定部門が ISO14001 の認証を取得しており，環境マネジメントを適確に行う体制が整備されていることを証明すること。

(14) 過去５年以内に，本件と同等規模以上の情報システム構築（設計，開発及び導入）及び保守運用を請け負った実績を有すること。ただし，ヘルプデスクのみの実績は認めない。

(15) 資本関係・役員等の情報，受託作業の実施場所に関する情報，受託業務の従事者の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績及び国籍に関する情報を提案書とともに提出すること。

(16) 保守性を高めるためにベンダーロックインとならないよう，システムの設計において属人性を排除しつつ標準化を図り，オープンな技術やフレームワークによるシステム構築が可能であること。

8.2.本整備業務及び本保守業務の実施体制としての条件

(1) 本整備業務及び本保守業務の確実な実施を担保するための作業体制をそれぞれ整えること。

(2) 各業務の作業体制表の作成に当たっては，作業責任者，役割，連絡先を明確にすること。

(3) 本整備業務におけるプロジェクトマネージャを１名以上配置し，プロジェクトマネージャの円滑なコミュニケーションによるプロジェクトマネジメントを実施することにより，本整備業務が遅滞なく完了させ，本保守業務及び本運用管理業務への移行をシームレスに橋渡しすること。プロジェクトマネージャは，以下の各条件を満たすこと。

① 過去 5 年以内に構築がなされた宮内庁 NWS の規模と 同等以上の情報システムにおいて，情報システム設計，構築，運用等のプロジェクトマネージャ又はプロジェクトリーダを務め，プロジェクトを成功に導いた経験を有すること。また，その経験を証明する情報システムの受注実績，規模（管理する要員数，受注金額など）などを示す証跡を提出すること。

② 情報システム設計・構築・運用等いずれかの業務経験を 5 年以上有すること。

③ 米国 PMI 認定の PMP の資格を有するか，又は「IT スキル標準 V3 2011」（平成 24 年 3 月 26 日 IPA）のプロジェクトマネジメントのいずれかの専門分野で達成度指標及びスキル熟達度ともにレベル 4 に相当する実務上の知識・経験を有すること。

④ 米国 PMI の PMBOK 最新版を PDU 対象の研修受講により理解していること。また，その受講証明書を提出すること。

⑤ PMBOK 最新版に基づくステークホルダーマネジメントを熟知しており，コミュニケーシ

ョン能力及び説明能力が高いこと。

(4)　原則としてプロジェクト体制の変更は認めないこととする。ただし，進捗に著しい遅れが発生した等で要員の追加及び作業担当者の変更がやむを得ない場合は，速やかに改善策を提示し甲の承諾を得ること。

8.3.運用管理従事者の要件

8.3.1.共通要件

(1)　業務遂行においてユーザや現行各システムの構築・保守事業者と日本語による円滑で適切な意思疎通が図ることが可能なこと。

(2)　職業安定法第 44 条（労働者供給事業の禁止）及び労働基準法第 6 条（中間搾取の排除）に抵触した状態での運用仮従事者でないこと。

(3)　製造事業者等が提供する製品マニュアル及び技術文献，一般的に書店などで入手可能な情報通信技術関連書籍などを参照しつつ，本調達で求める運用管理従事者（運用管理責任者，運用作業員，代替要員）の要件を満たした技術者としての専門的知識をあわせて最大限に活用し，甲からの情報システムに関する問合せなどの対応を適切に努め，宮内庁 NWS が可能な限り効果的に利用可能となるよう維持運用に努めること。

(4)　社会情勢と環境の変化に合わせて変化する情報通信分野に関する技術や製品などについて継続的な情報収集や学習を行い，その知識を活用することにより，能動的に適切な宮内庁 NWS の維持運用に努めること。

8.3.2.運用管理責任者（個人）の実績・資格

(1)　乙は，運用管理業務の円滑な実行や，運用作業員のみでは対処出来ない技術的な問題の解決やステークホルダーとの調整を円滑に行うため，運用管理責任者を設け，運用作業員のサポートを行うこと。

なお，運用管理責任者は，1 週間のうち休日を除く平日の 60%以上，1 名が情報管理室に勤務することとし，以下の実績・資格を有することとする。ただし，運用管理責任者を複数配置する場合において，以下の③，④については，同一の者が両方を満たす必要はなく，運用管理責任者全体で③及び④を満たせばよいこととする。その場合には，運用管理責任者同士が密に連携をとって業務に臨むこと。

①　過去 5 年以内に構築がなされた宮内庁 NWS の規模と 同等以上の情報システムにおいて，情報システム設計，構築，運用等の責任者を務め，プロジェクトを成功に導いた経験を有すること。また，その経験を証明する情報システムの受注実績を示す文書を提出すること。

②　情報システム設計・構築・運用等いずれかの業務経験を 5 年以上有すること。

③　「IT スキル標準 V3 2011」の IT サービスマネジメントの専門分野のうち，オペレーション，運用管理，システム管理又はサービスデスクのいずれか一つで達成度指標及びスキル熟達度ともにレベル 4 以上に相当する実務上の知識・経験を有すること。

④　「情報処理促進法」に基づいて行われる情報処理技術者試験のうち，ネットワークスペシャリスト試験の合格者及び又は「情報処理促進法」第 15 条の規定に基づく情報処理安全確保支援士の登録を受けている者（又は同等の資格を有する者）であるか，又は「IT ス

キル標準 V3 2011」の IT スペシャリストのいずれかの専門分野で達成度指標及びスキル熟達度ともにレベル 4 に相当する実務上の知識・経験を有すること。

8.3.3.運用作業員（個人）の実績・資格

(1) 運用作業員（常駐者及び応援者）は，以下の実績・資格を有すること。

① 過去 5 年以内に構築がなされた宮内庁 NW の規模と 同等以上の情報システムにおいて，企画，設計・開発，運用に関する業務 3 年以上従事した経験を有すること。ヘルプデスク業務のみの実績は認めない。

② 「IT スキル標準 V3 2011」 の IT スペシャリストの専門分野のうち，ネットワーク，プラットフォーム，セキュリティ，システム管理のいずれか一つで達成度指標及びスキル熟達度ともにレベル 3 に相当する実務上の知識・経験を有すること。

③ 「IT スキル標準 V3 2011」の IT サービスマネジメントの専門分野「オペレーション」で達成度指標及びスキル熟達度ともにレベル 3 以上に相当する実務上の知識・経験を有すること。

④ ITIL Foundation 以上の資格を有し，証明できること。

⑤ Windows サーバ及びクライアント，Linux サーバ，それらを接続するネットワーク機器についての運用経験を有しており，業務上必要なシェル・コマンドの操作，スクリプト及びバッチファイルの作成と正常動作確認ができる能力を有していること。

⑥ 甲で現在利用している汎用ソフトウェアや汎用ミドルウェア全般についての専門知識と操作経験を有しており，迅速なヘルプデスク業務が実施可能な能力を有していること。

8.3.4.代替要員の実績・資格

(1) 代替要員の実績・資格は，運用作業員の実績・資格の(1)に準ずる。

(2) 代替要員は，運用作業員の不慮の事故，疾病又は休暇により勤務できない場合を想定し，運用作業員との日頃からのコミュニケーションを積極的に行うなどし，宮内庁 NWS の運用の状態の把握に努め，運用作業員からの業務の引継が円滑かつ確実に行うことが可能な状態を維持すること。

9. 移行・切替要件

移行・切替要件を次に示す。

9.1.移行・切替計画の策定

(1) 宮内庁 NWS の安定した稼働及び業務の継続に影響を与えることがないよう，安全で確実な移行・切替計画を策定すること。

(2) 移行計画は無理な移行とならないよう，安全かつ余裕を持ったスケジュールで切替計画を策定すること。

(3) 回線の切替日程は特定日に拠点の切替作業が集中しないよう，1 日に行う切替の日程上限は 2 拠点以内を目途とし，順次切替行っていくこと。

(4) 本番移行の 2 週間以上前には移行リハーサルを実施し，本番時の切替が確実に行えるようにすること。本番移行時にはリハーサル時と本番時の環境の差分について明確にし，差異がある場合はリスク対処策を提示し甲の承諾を得ること。

(5)　移行切替後に不具合や問題が発生した際に，切り戻しが行えるよう，平行運用期間を 1.5 か月程度持たせること。

(6)　甲担当者と協議の上，移行・切替計画書を作成し，承諾を得ること。

9.2.移行・切替の方針

(1)　担当者が承諾した日時を除き，宮内庁統合 NW を始め各現行システムのサービスを停止することなく，移行・切替を実施すること。

(2)　現行システムにおけるデータ利用に係る実態調査を行い，甲と協議の上，必要な全ての機能の移行・設定作業を行うこと。

(3)　宮内庁統合 NW を始め各現行システムの停止を伴う作業が避けられない場合には，ユーザへの影響を最小限に抑えるため，原則として平日の勤務時間外又は休日を作業実施日として検討し，甲担当者の承諾を得ること。また，事前にその工程及び作業方法について，甲の承諾を得ること。
なお，国会開催時には，システム停止が許容されない場合がある。

(4)　宮内庁 CIS 導入に当たって，現行環境に設定，ツール等のインストール・アンインストールが必要となる際には，甲及び現行システムの構築・保守事業者及び管理者に設計等の情報を開示するとともに，甲からの指示に従うこと。

(5)　各現行システムの構築・保守事業者及び管理者間の各種調整などについては，甲の承諾を得た上で乙の責任のもとに実施することとし，宮内庁 CIS 導入に当たり，その調整等による不都合，負荷などが発生しないようにすること。

(6)　現行の環境は，各課に VLAN を割り当て，ネットワークセグメントを分割して運用している。宮内庁 CIS の導入作業においても現行と同様の構成を踏襲するため，宮内庁 CIS はこの設定が可能であることを原則とする。
なお，移行の際に問題が発生した場合の切り戻し，又は順次移行などの移行設計を考慮した上で機器の選定を行うこと。

(7)　本業務により，宮内庁 NWS を始め各現行システムに不具合や問題を与えた場合は乙の責任と負担において対処すること。本作業に起因して発生した作業を関係事業者へ依頼する場合は，甲と事前に協議を行い甲の承諾を得た上で，乙が作業費用を負担すること。ただし，作業実施予定日の 10 日（休日を除く。）前までに乙が作業内容（設定，手順等）について文書にて甲担当者へ具体的に説明した上で，通常の保守業務又は運用管理業務の範囲内の作業と認められる場合には，甲担当者を介し，甲担当者の指示として当該作業を関係事業者に通常業務として依頼することができる。

(8)　移行・切替の際に，宮内庁 NWS に連携する各現行システム等に影響があると懸念される場合には，事前に甲担当者へ可能な限り速やかに報告し，対応策を協議すること。

(9)　データ移行が必要な場合には，甲に極力作業を発生させない方法でデータ移行を実現すること。やむを得ず甲の作業が発生する場合は，甲担当者とあらかじめ協議し，その承諾を得ること。

(10)　移行対象データについては，宮内庁 NWS が正常に動作し，監査やセキュリティインシデント対応を適切に行う上で必要となる全てのデータを移行対象とすること。移行対象データについては，対象データを甲に提示し，甲の承諾を得ること。ただし，甲が宮内庁 CIS へ移行しないよう指示するデータは除くこととする。
なお，共有ファイルサーバにおいては，現行の実態を調査した上で，重複していること，長期間利用されていないこと等が確認されたファイルが明らかになった場合，甲と協議し，移行の対応内容を決定すること。移行対象のデータは最低限以下を想定している。
(ア) ディレクトリサーバ等に格納されているユーザ情報
※　ユーザ管理システム内で保存している関連情報についても必要に応じて実施すること。

(イ) 庁内ポータル内に格納されている各種コンテンツ
(ウ) ファイルサーバ内に格納されている各種ファイル
(エ) その他宮内庁 NWS が正常に動作する上で必要となるデータ

(11) 移行・切替のために機器の追加が必要な場合は，乙の責任と負担において準備を行い，作業終了後に撤去すること。

9.3.移行準備作業

(1) 移行・切替準備，移行・切替作業及び検証の手順等を示した移行・切替手順書を作成すること。同作業の手順には，各作業が正しく行われていることの確認（作業毎のチェック項目と作業の成否の判定基準等）を含めること。

(2) 切替時に現行システム事業者，運用管理支援事業者，各関係事業者に対応を求める場合は，各事業者に実施を求める内容，対応予定日を記載した切替手順書を作成すること。各関係事業者作業依頼は原則として，1 か月以上前に提示を行い，1 週間以上前までに甲の合意を得ること。

(3) 移行・切替作業及び移行・切替後動作検証等の同作業に係る時間単位での詳細スケジュールを作成すること。

(4) 移行・切替作業において想定されるリスクを検討し，リスクが顕在化した場合に備え，具体的な切戻し方法等を含めた緊急時の対応計画表を作成することとし，甲担当者の承諾を得，移行・切替手順書に加えること。

(5) 切り戻し作業が迅速に行えるような移行手順を検討し，原則として切り戻しが不可能な移行手順や，切り戻し時に連携するシステムの各関係事業者に負荷を与えるような移行は実施しないこと。

9.4.移行作業

(1) 移行・切替作業において，何らかのトラブルが発生した場合は，速やかに甲担当者へ連絡すること。

(2) トラブルの内容により移行が困難と判断された場合は，甲及び関係事業者に承認を得て，速やかに切り戻し作業を行うこと。切り戻し完了後は正常にシステムが稼働していることを確実に確認すること。切り戻しによる各関係事業者への依頼作業については，甲と協議の上で，原則として乙が負担すること。

(3) 移行・切替作業の結果について，移行・切替作業結果報告書を作成し，甲担当者に提出すること。

(4) 移行時には甲の責任者は連絡が取れる体制にしておくこと。また，作業場所には委託事業者だけでなく，甲担当者を配置すること。

(5) 移行・切替作業実施後は，問合せ等の対処が円滑に行えるよう体制を確保すること。

9.5.運用管理業務の引継ぎ

9.5.1.本調達の落札決定後

(1) 乙は，本調達の落札決定後，運用管理業務開始日から速やかに運用管理業務に着手できるよう，本調達仕様書「7.会議体の設置」で示した統括会議等を活用するなどし，乙の責任と負担において，落札決定後から契約履行開始日までに現行運用管理支援事業者，宮内庁統合 NW の構築事業者，宮内庁 CIS の構築担当者などから確実に運用管理業務を引き継ぐこと。

なお，乙が引継ぎ作業を進める上で，現行運用管理支援事業者，宮内庁統合 NW の構築事業者，宮内庁 CIS の構築担当者などへ運用管理業務の引継ぎに関する依頼を求める場合は，甲に対して具体的に依頼内容を事前説明すること。乙の依頼内容が通常の保守業務又は運用管理業務の範囲内の作業であると甲が認める場合には，甲担当者を介し，甲担当者の指示として各事業

者に対して依頼することができる。

9.5.2.本調達の契約期間終了の 1 か月前

(1) 乙は，運用管理業務の契約期間終了の 1 か月前から，次々期運用管理事業者（2024 年 2 月 1 日から業務開始を予定）に対する引継ぎを運用管理業務の作業範囲として行うこと。ただし，甲又は次々期運用管理事業者の事由により，引継ぎ業務が本調達の契約期間外に及ぶ場合には，本調達の範囲外とする。

(2) 乙は，次々期運用管理事業者への引継ぎ作業の開始予定日の営業日 5 日前までに，次のような資料の作成又は更新を行った上で甲担当者に提出して甲担当者の承諾を得ること。

① 運用管理業務を行う中で把握した課題事項等，運用管理業務を遂行してきた中で得た知見をとりまとめた資料等

② 運用管理業務の実態に即した最新の各手順書等

(3) 乙は，(2)で作成した資料等を用いて甲担当者及び次々期運用管理事業者に対し適切な説明を実施すること。また，甲担当者及び次々期運用管理事業者引き継ぎの内容に関する質問にも適宜対応すること

(4) 当該引継ぎに必要な資料等の作成の経費は，乙の負担とする。

10. 運用・保守管理要件

乙は，本調達にて提供するサービス及び機器等について，次の運用・保守を行うこと。

なお，運用及び保守を提供する対象のサービス及び機器の一覧は別紙 4 を参照すること。

10.1.基本方針

(1) 運用管理・保守業務の統括者を配置し，全体の管理を行うこと。

(2) 構成・変更管理，運用・監視，保守を行う体系化された体制を確立すること。

(3) 連絡体制を明確化し，甲担当者，関係者への連絡を円滑かつ迅速に行える仕組みとすること。

(4) ITIL，ISO20000 等の業界標準の運用・保守管理基準を参考に運用・保守業務項目を定義すること。

(5) 上記(1)～(4)について運用管理・保守説明書としてまとめ，甲担当者の指定する期限までに提出すること。

(6) 運用・保守業務の支援ツールを導入して作業を効率化すること。

(7) 甲担当者の負荷軽減に配慮すること。

(8) 運用・保守対応時間帯は，平日の 9 時 00 分から 17 時 00 分とし，休日を除く月曜日から金曜日（原則として当日対応）までとすること。

(9) 24 時間×7 日間／週の稼働を基本とすることとし，必要な保守による停止の際には，ユーザに不便を与えないよう配慮し，効率的に作業を行うこと。

10.2.問合せ受付窓口対応

(1) 甲担当者及び宮内庁統合 NW 受託者が，運用・保守及び障害等について問合せ可能で一元的な受付窓口（以下「運用・保守受付窓口」という。）を設置すること。

(2) 運用・保守受付窓口は，E-mail や FAX 等による 24 時間×7 日間／週での受付が可能であること。

(3) 運用・保守対応時間帯は，平日の 9 時 00 分から 17 時 00 分とし，休日を除く月曜日から金曜日（原則として当日対応）までとする。ただし，甲担当者が対象製品の故障の重要度，緊急度が大き

いと判断した場合はこの限りではない。また，ハードウェア障害に関する復旧対応，個別のサービス・製品に対する問合せ窓口については ，個別の窓口を用意し，24 時間×7 日間／週で対応を行うこと。

(4) 運用・保守対応時間内は，電話によるサポートを随時行うこと。

(5) 受け付けた問合せをインシデントとして管理し，インシデントのクローズまで， 対応を継続すること。

(6) 障害について対応したときは，障害報告書を作成し，甲に報告すること。

10.3.運用・保守要件

(1) 各種の障害発生を想定し，甲担当者及びユーザへの報告・通知の手順，障害復旧の手順，体制，役割分担，連絡方法などの計画を策定すること。策定した計画は甲担当者の承諾を得ること。また，運用において PDCA サイクルを実施し，障害対応業務の実施内容を継続的に評価，改善することで長期にわたっての安定的，効率的かつ高品質なサービス提供を行うための計画の随時見直しを行うこと。

(2) 障害発生時には，甲担当者，次期運用管理事業者（宮内庁 CIS 受託者），運用管理支援業者及び障害に関連する各現行システムの構築・業者と綿密な調整・連携を行い，保守作業を行うこと。また，各拠点に対応要員を派遣する必要がある場合はその手配と各拠点との調整を行うこと。

(3) 発生した障害を事案ごとに記録・管理し，状況が常に把握できる仕組みとすること。

(4) 甲担当者又は管理者からの問合せによる宮内庁 CIS の障害の有無を確認し，原因の切り分け，調査の支援を行うこと。

(5) 障害復旧のための対応策を検討すること。
なお，甲担当者への対応策の内容の説明及び実施に必要な調整を行うこと。

(6) 原則として障害発生の当日中に対応を開始し，早急に復旧させること。ただし，根本的な対策が取れない場合は暫定的な復旧策を検討・提案し，対策の実施においては甲担当者の承諾を事前に得ること。

(7) 障害が発生した場合は，障害個所の修理又は交換を行うこと。機器交換時には，機器が物理的に適正に機能することを動作確認し，この確認結果を甲担当者へ遅滞なく報告し，報告内容について甲担当者の承諾を得ること。

(8) 機器等の修理又は交換を行う場合，据え付け・調整作業を行うこと。これらの作業により設定内容が失われた場合は，甲担当者の指示により再設定を行うこと。

(9) 甲担当者が，障害復旧したことを確認できるまで対応を行うこと。

(10) 障害対応した際，対応後速やかに障害報告書を作成し，遅滞なく甲担当者に報告すること。

(11) 発生した障害に対して関連情報収集及び解析を行い，原因を究明し，再発防止策を検討すること。
再発防止策の検討結果を甲担当者へ遅滞なく報告し，報告内容について甲担当者の承諾を得ること。

(12) 報告書については次の報告内容とし，その他必要と考えられる項目についても報告する仕組みとすること。
① 発生状況（発生日時，回復時間，故障時間，影響拠点，障害概要）
② 障害対応状況（故障原因，故障機器，対処内容，現在の状況）
③ 障害の原因とその対応策
④ 再発防止策

(13) 地震，水害，停電等の災害発生による被害を想定し，甲担当者及びユーザへの報告・通知の手順，障害復旧の手順，体制，役割分担，連絡方法などの計画を策定すること。策定した計画は甲担当者

の承諾を得ること。また，運用において随時見直しを行うこと。

(14) 災害発生時には，上記（13）の計画に沿って迅速な復旧を行うこと。

10.4.保守要件

以下，保守業務として実施すべき保守の要件について記載を行う。

なお，宮内庁 LAN の一部の機器（詳細は，別紙４を参照）については，宮内庁統合 NW 受託者により暫定的に運用管理された後，乙に引き継がれることを想定している。運用を引き継いだ機器についても，ハードウェア交換等の一部の保守業務については，引き続き宮内庁統合 NW 受託者にて対応をする。

10.4.1.基本要件

(1) 乙は，次の要件を満たす保守体制を整備し，保守運用計画書を提出し，保守運用手順書に基づき，保守対応をすること。

なお，保守対応とは，問合せ受付窓口対応，システム保守対応，ハードウェア保守対応，ソフトウェア保守対応の総称を示すものとする。本調達機器及び各事業者の役割範囲については，別紙４を参照すること。

(2) 保守期間は，契約期間が終了するまでとする。

(3) 乙は，甲及び宮内庁統合 NW 受託者の求めに応じて必要な障害対応，原因究明，設定変更等の対応を行うこと。

(4) 乙は，保守対応における責任体制を明確にするため，担当者名を明記した保守体制図を提出すること。

なお，体制を変更する必要が生じた場合には，変更内容を記載した文書をもって報告し，甲の承諾を得ること。

(5) 設計･構築の従事者を保守体制に原則含めること。ただし，保守体制に含めることが困難な場合は，設計・構築の従事者から十分に引継ぎを受け，内容を十分に理解した者を保守体制に含めること。

(6) 障害発生時には，甲担当者及び宮内庁統合 NW 受託者，障害に関連する現行他システム保守業者と綿密な調整・連携を行い，乙の責任と負担で保守作業を行うこと。

(7) 調達機器について，技術的サポートを行うこと。また，今後の運用中に調達機器と他の機器との接続及び別途調達したソフトウェアを甲担当者又は宮内庁統合 NW 受託者がインストール・アンインストールするような場合，甲担当者と密接に連絡が取れる体制を作り，連絡があった場合は支援すること。

(8) 保守対応は日本語で実施すること。

(9) 宮内庁 CIS に蓄積しているデータは，設定されたスケジュールに従いバックアップを行うことが可能なこと。

10.4.2.システム保守要件

(1) 重大障害発生時や切り分け困難時等，各ハードウェア及びソフトウェア製造事業者等では解決できない事象発生を想定し，乙において，ハードウェア・ソフトウェアで構成されるシステム全体の保守を実施すること。

(2) 乙は，対応依頼を受け付けた障害を解消するため，適切かつ迅速な対応を行うこと。必要に応じて，各ハードウェア製造事業者等及び各ソフトウェア製造事業者等と協力し，ハードウェア保守対応，ソ

フトウェア保守対応を行うこと。

(3) システム保守対応の対応時間は，問合せ受付窓口対応の受付時間に準ずる。ただし，対象製品の故障の重要度，緊急度が大きいと判断した場合，甲から要請した場合はこの限りでない。

なお，対応時間外のシステム保守対応については，本調達に含まないものとする。

(4) 発生した障害に対して解析を行い，原因を究明し，再発防止策を検討すること。

(5) 甲及び宮内庁統合 NW 受託者並びに他システムの保守業者からの問合せや相談に応じること。

10.4.3.ハードウェア保守要件

10.4.3.1 基本要件

オンプレミス型での提供とする場合は，次の要件を満たすこと。

(1) 各ハードウェア障害時には，当該機器又はそれを構成する部品等の調達・交換・修理等を迅速に行う等，乙の負担により常時正常な稼動を保証すること。

なお，補助記憶装置の交換等によりソフトウェアの再インストールやシステムの環境設定，動作確認等が必要な場合，正常稼動するまでの作業も迅速に行うこと。

(2) 安定したサポートの実現及び保守サービスの品質維持のため，特に指定がない限り，本調達機器に関しては， 製造事業者等が提供するハードウェア保守サービスを購入すること。

なお，各ハードウェアの保守サービスレベルについては，原則 24 時間×7 日間／週 のオンサイト保守対応とすること。

(3) 調達機器に障害が発生した場合，(2)の保守サービスレベルの範囲で，ハードウェア障害と判断された時点から，原則 4 時間以内に技術者を派遣し，障害装置の修復，故障部品の修理にあたるものとする。

なお，賃貸借及び保守期間中は，必要な交換部品を必ず保持すること。

(4) 乙は，問合せ受付窓口対応及びシステム保守対応の受付時間外における障害に備えるため，各ハードウェア及びソフトウェア製造事業者等へ，甲担当者及び宮内庁統合 NW 受託者から直接問合せが可能な窓口を用意すること。

(5) ハードウェアの修理又は交換を行う際に，ラックからの取り外しや，据え付け・調整作業が必要な場合は，実施すること。また，必要に応じて，コンフィグの再投入等， 設定作業を行うこと。

(6) 障害個所の修理又は交換後，機器が適正に機能するのかを宮内庁統合 NW 受託者と協力して動作確認すること。

(7) 保守期間中，ハードウェアに対する修正ファームウェアの適用要否に関する情報を提供すること。

(8) 調達機器のファームウェアのバージョンアップがあった場合は，乙は，ファームウェアのバージョンアップについて確認を行い，実機に反映し，検証を実施すること。

(9) 1 年に 1 回以上，本調達に係る全ての機器の定期点検を行うこと。

(10) 本調達ハードウェアに搭載された補助記憶装置に障害が発生した際に，当該補助記憶装置を取り外し交換供給することとし，取り外した補助記憶装置については甲担当者が廃棄を行うのでこれを了承すること。

10.4.3.2 特記要件

保守の基本的な種類については，「1.3 用語の定義」を参照すること。

(1) サーバ（クラウドサービスプロバイダが提供するサービスとしてのサーバを除く。）及びスイッチ

① 共通事項

納入から 1 年間は，無償保証交換とすること。

② 特記事項

ア サーバ

オンプレミス型での提案をし，本調達仕様書（案）内でサーバ構成を明記しているものは，次のとおり保守対応すること。

(ア)シングル構成又は二重化構成で，本庁と京都間での相互バックアップを取得していない場合

休日を除く月曜日から金曜日までの 9:00 から 17:00 までのオンサイト保守対応とし，ハードウェア障害と判断された時点から，原則 4 時間以内に技術者を派遣し，障害装置の修復，故障部品の修理にあたるものとする。

なお，契約期間中は，必要な交換部品を必ず保持すること。

(イ)二重化構成で，本庁と京都間での相互バックアップを取得している場合

原則としてスポット対応とする。ただし，応札者の提案においてオンサイト保守対応を阻害するものではない。

なお，スポット保守対応とする場合には，運用管理業務での情報システムインシデント対応を確実に行った上で，ステム保守事業者，製造事業者等保守契約の関係者に連絡を行う際に，スポット保守の見積依頼を同時に行い，甲へ見積書を提出すること。

イ スイッチ

(ア)二重化構成（サーバセグメント用サーバ・ネットワークスイッチ，運用管理セグメント用サーバスイッチ）

後出しセンドバック保守とする。

10.4.4.ソフトウェア保守

(1) 乙は，ソフトウェア（OS 含む）及び関連ソフトウェアに関する問合せ，セキュリティ情報等の提供，障害発生時における解決支援に対応すること。

なお，導入したソフトウェア（OS 含む）について，導入後，甲が必要と認めた場合には，最新パッチ等の提供及び動作検証等の支援を行うこと。

(2) 納入したソフトウェアに対する修正パッチ・修正モジュール又はマイナーアップデートが製造事業者等から提供された場合，それらが提供された日から起算して原則 2 日（休日を除く。）以内に甲担当者へ報告し，適用要否の協議を実施すること。ただし，重大かつ緊急性を有する修正パッチ・修正モジュール又はマイナーアップデートについては，可能な限り遅滞なく甲担当者へ報告し，適用要否の協議を実施した上で適用作業を実施すること。

(3) 宮内庁ＬＡＮの一部の機器については，宮内庁統合 NW 受託者による暫定運用管理期間が設けられている。当該期間中は，宮内庁統合 NW 受託者が修正パッチ・修正モジュール又はマイナーアップデートの適用作業を行うが，当該期間終了後は，乙にて作業を実施するものとする。

10.4.5.サービス保守要件

本調達で乙がクラウドサービス等を提供する場合，乙の責任と負担においてファームウェア及びソフトウェアを可能な限り最新版にすることにより，ユーザの利便性，業務効率性及び情報セキュリティ対策を継続的に保つこと。

なお，各サービスそのものの SLA を順守するために必要となる保守を乙の責任と負担で適宜実施すること。

10.4.6.運用・保守業務フロー

甲，乙及び宮内庁統合 NW を含むその他保守事業者の運用・保守業務フローは，別紙５のとおり。

11. 仕様要件についての証明における記載要項

11.1.概要

応札者は，本記載要項に基づき，運用管理業務を履行する能力があることを，代表者の証明する適合証明書における仕様要件についての証明は，要件を満たしていることを具体的な記載資料（以下「提出資料」という。）を提出して証明すること。記載内容が要求要件を満たしているか否かの判定は，甲において，提出資料の書面により行う。

11.2.記載に際しての基本要件

(1) 提出資料は，単なる意思表示ではなく，運用管理業務の目的，内容を踏まえ，実施に当たっての詳細かつ具体的な実現方法を示していること。

(2) 本調達仕様書（案）は，運用管理業務として求める最低限必要とされる要件を示したものである。従って，本調達仕様書（案）の要件を全て満たした上で，本調達仕様書（案）に記載されていない事項であっても，運用管理業務を実施するに当たり，必要と思われる事項については提出資料に記載すること。

(3) 提出資料において記載された内容は，運用管理業務範囲の対象として実施するものとする。

11.3.業務要件等に関する提案

(1) 全体要件に関する資料

運用管理業務の目的・内容を踏まえ，実施に当たっての基本方針を具体的に記載すること。

(2) 請負業務内容に関する資料

本調達仕様書（案）に記載の各項目について，運用管理業務の円滑化・効率化を目的として創意工夫し，具体的な業務の実施方法等を記載すること。

11.4.応札者条件に関する証明

(1) 応札者に関する証明

「8.1. 応札者としての条件」に示す要件について具体的に記載し，証明書の写し等を添付すること。

(2) 作業実施体制に関する証明

「5.4. 作業実施体制」に示す必要な要員を記載した体制図を提出すること。また，各要員に関して，本調達における各要員の役割，「8.3.2. 運用管理責任者（個人）の実績・資格」及び「8.3.3. 運用作業員（個人）の実績・資格」に示す要件について具体的（運用管理従事者の氏名，実務経験・実績，IT スキル標準（Ver3.0）の達成度指標，要素技術スキル等）に記載し，証明書の写し等を添付すること。

11.5.提出資料作成要領

(1)　提出資料の印刷用紙は，原則としてＡ４判縦長横書きとする。ただし，図表等についてはＡ３判も可とする。添付する説明資料やパンフレット等がある場合にはこの限りではない。

(2)　提出資料本文は日本語で記載し，分かりやすい構成を心掛け，目次及び通しのページ番号を付与すること。

なお，必要に応じて用語解説等を添付すること。

(3)　応札者の名称，所在地，代表者氏名等を記載すること。また，提出資料に対する照会先（連絡担当者名，所属，電話番号，FAX 番号，E-mail アドレス）を記載すること。

(4)　提出資料は紙媒体で 2 部，甲の指示する電子媒体で 2 部ずつ提出すること。また，機能証明書，提案資料の電子ファイルを格納した甲の指示する電子媒体を 1 式提出すること。

(5)　提案に際して質問事項がある場合は，入札説明書（別添 3）に記載の FAX 番号又は E-mail アドレス宛てに提出すること。質問に対する回答は，入札説明書を受領した全ての事業者に対し速やかに回答を行う。

11.6.留意事項

(1)　提出に係る経費は，応札者の負担とする。

(2)　提出資料は，合否の判定のみに用い，採点等の対象とするものではない。

(3)　提出資料について，照会や資料要求を行うことがある。

(4)　仕様要件を満たしていないと甲が判断した場合には，応札できないものとする。また，一旦提出された提出資料の差し替えや再提出は，一切認めない。

12. その他特記事項

12.1.検査・指示

甲は，乙に対して質問，検査，資料等の提出に関する指示及び改善要求を行うことがある。これらを甲から求められた際には，乙はこれに速やかに応じること。

12.2.新規資産にかかる運用要件

運用管理業務時点では存在しない新規資産が導入された場合には，当該資産について運用管理業務の対象とするかどうか甲と協議すること。

12.3.政府機関からの調査依頼支援

政府機関からの宮内庁 NWS に関する調査依頼又は対応指示事項が年々増加している。乙は運用管理業務対象の資料作成，提出等の支援を行うこと。

13. 資料閲覧

13.1.参考資料

希望する者は，次を所定の手続きにより閲覧することができる。

・宮内庁情報セキュリティポリシー
・ラック構成図
・宮内庁文書管理細則
・宮内庁情報ネットワークシステム機器の賃貸借及び保守完成図書

※ 「基本設計書 電子メール中継サーバ」の十分な理解を必須とする。

・宮内庁統合ネットワークの各設計書

※ 宮内庁統合 NW は，本調達の公示時点では構築中であるため，各設計書を確認しつつ，適宜，甲に確認を行うこと。

※ 宮内庁統合 NW に係る基本設計書は，６月上旬に同業務受託事業者から提出される予定。

・グループウェアシステムの賃貸借及び保守 完成図書
・パーソナルコンピュータ及びサーバ等の賃貸借及びサーバ等保守 完成図書
・宮内庁 WAN の通信回線サービス 完成図書
・インターネット接続回線サービス 完成図書
・電子ファイルの暗号化及びアクセス制御機能の賃貸借及び保守 完成図書
・Web 無害化機能の賃貸借及び保守 完成図書
・標的型攻撃対策システムの賃貸借及び保守 完成図書
・インターネットアクセス用セキュリティ機器の購入及び導入作業 完成図書
・サーバリソース利用状況
・宮内庁ネットワークシステムの運用管理支援業務　成果物
・運用管理支援業務　月報

13.2.閲覧要領

(1)　閲覧手続

参考資料の閲覧を希望する場合は，必ず資料閲覧可能期間に，(2)の連絡先にあらかじめ連絡の上，別紙 1「資料閲覧願い」に必要事項を記載し，閲覧日及び閲覧希望資料を調整すること。閲覧期限は 2019 年 7 月上旬頃までの予定である。

(2)　閲覧時の注意

閲覧時にて知り得た内容は，適合証明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。

○ 資料閲覧可能期間：2019 年 6 月中旬から 7 月上旬頃までの予定（土日祝日を除く）

○ 連絡先

〒100-8111　東京都千代田区千代田 1-1（皇居内）
電話番号：03-3213-1111（内線 3231）
担 当 係：宮内庁長官官房秘書課調査企画室情報係

14. 契約条件等

14.1.特定個人情報

個人情報保護委員会の「「特定個人情報の適正な取扱いに関するガイドライン（事業者編）」及び「（別冊）金融業務における特定個人情報の適正な取扱いに関するガイドライン」に関するＱ＆Ａの更新（平成 28 年 6 月 21 日）」を参照すること。

乙は，例えば「個人番号を用いて情報システムの不具合を再現させ検証する」や「個人番号をキーワードとして情報を抽出する」ような作業は一切無く，ユーザのみが個人番号をその内容に含む電子データを取り扱い，個人番号を用いた業務を行う。

14.2.秘密保持

(1)　乙は，履行期間中はもとより履行期間終了後にあっても，本業務を履行する上で知り得た甲に係る情報を第三者に開示又は漏えいしないこととし，そのために必要な措置を講ずること。
(2)　甲が提供する資料は原則貸し出しとし，甲の指定する日までに返却すること。当該資料は複製してはならず，原則として第三者に提供し，又は閲覧させてはならない。
(3)　上記(1)の情報及び(2)の資料を第三者に開示することが必要となる場合は，事前に甲と協議の上，甲の承諾を得ること。
(4)　本調達で整備する宮内庁 CIS 以外で宮内庁 NWS の運用にかかる ID・パスワードは，現行運用管理支援事業者から引継ぎ，パスワードを変更すること。
(5)　乙は，本調達における全て業務の実施においては，情報セキュリティを確保するための体制を整備すること。
(6)　乙は，本調達における全ての業務の遂行においては，情報セキュリティの侵害が発生した，又は発生するおそれがある場合には，速やかに甲に報告すること。

14.3.瑕疵（かし）担保責任

本調達機器等の不良，製造過程における設計・設定及びこれらに搭載されるソフトウェアに瑕疵のあることが発見された場合には，乙は甲の請求により新規取替え又は補修を行い，その瑕疵によって生じた損害を賠償すること。

14.4.賠償・復旧

甲の現行の正常可能機器及びシステムが，本業務により不具合や問題が生じた場合は，迅速に復旧のための措置を乙の責任と負担において実施すること。

14.5.第三者への請負，著作権等

(1)　乙は，本業務の全部を一括して又は主たる部分を請負等により第三者に実施させてはならない。ただし，次の場合においてはこの限りではない。
(ア)　乙が，書面により請負等を受ける事業者の名称・住所・請負等の業務の範囲・請負等の必要性・請負等の金額等を事前に甲に申請し，その承諾を受けた場合。
なお，請負等の内容を変更しようとする場合も同様とする。
(イ)　乙が，コピー・ワープロ・印刷・製本・トレース・資料整理・計算処理・翻訳・参考書籍等の購入・消耗品購入・会場借上等の軽微な業務を請負等しようとする場合。
(2)　上記に基づき，第三者に業務を請負等する場合は，「14.2.秘密保持」に従いその者に対し，秘密の保持及び情報セキュリティの確保を同様に請負契約等において課すこと。
(3)　乙及び請負等を受けた第三者は，甲が定める情報セキュリティポリシー等を遵守し，「14.2.秘密保持」に基づき，その内容を秘密にする措置をとらなければならない。
(4)　乙が上記(1)に基づき第三者に請負等する場合において，請負等を受けた第三者が更にその業務の一部を請負等する等複数の段階で請負等が行われるときは，あらかじめ当該複数段階の請負等を受ける事業者の名称・住所・請負等の業務の範囲を記載した書面（履行体制に関する書面）を甲に提出しなければならない。当該書面の内容を変更しようとする場合も同様とする。
(5)　乙が上記(1)に基づき第三者に業務を請負等する場合において，これに伴う第三者の行為については，その責任を乙が負うものとする。
なお，再々請負等の場合も同様とする。

(6)　請負等事業の実施に当たり，甲の意図しない変更が行われないことを保証する管理が，一貫した品質保証体制の下でなされていること。また，当該品質保証体制が書類等で確認できること。

(7)　本調達機器に甲の意図しない変更が行われるなどの不正が見つかった時（不正が行われていると疑わしい場合も含む）に，追跡調査や立入検査等，甲と乙が連携して原因を調査，排除できる体制を整備していること。また，当該体制が書類等で確認できること。

(8)　当該管理体制を確認する際の参照情報として，資本関係・役員等の情報，請負等事業の実施場所，請負等事業従事者の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績及び国籍に関する情報提供を行うこと。

(9)　本業務の実施に当たっては，必要に応じて納入場所の環境について事前に確認を行うこととし，甲の業務に極力支障が生じないよう計画し実施すること。また，現行運用管理支援事業者，甲の他の現行宮内庁 NWS 賃貸借保守事業者等関係者との連携・協力を図りつつ宮内庁 NWS 及び関連する各現行システムの円滑かつ安定的な稼働に支障を来すことのないよう業務を実施すること。

(10)　テスト計画書に基づき，単体，結合，総合テストを実施する際に使用するテスト用データは，乙において準備すること。

なお，関係事業者の協力が必要な場合は，甲及び関係事業者と協議し原則として乙の責任と負担において行うこと。

(11)　本業務の実施に必要となる工業所有権及び著作権等については，全て乙の責任において当該工業所有権及び著作権等の使用に必要な費用を負担し，使用承諾等に係る一切の手続きを行うこと。また，本業務の実施に伴い，甲のシステムのアプリケーションの著作権は，全て甲に帰属するものとし，著作者人格権について，乙はこれを行使しないものとする。

(12)　本調達仕様書に基づく作業に関し，第三者との間に著作権に係る権利侵害の紛争等が生じた場合は，当該紛争の原因が専ら甲の責めに帰す場合を除き，乙の責任と負担において一切の処理をすること。

(13)　本業務の実施に伴い，本調達機器等の搬入・設置・修理・交換等物理的作業の実施に当たって甲の敷地内の作業場所を使用する場合は，事前に甲に申請しその承諾を得なければならない（ただし緊急に措置しなければならない場合を除く）。その場合，乙は作業場所を整理・整頓し，安全に留意して事故の防止に努めるとともに，労働基準法・労働安全衛生法を遵守して安全の徹底を図り作業すること。当該作業に伴い必要となった養生品・梱包箱等で当該作業の後不要となるものは，乙の負担で速やかに撤去すること。

(14)　上記作業による甲の諸設備の破損等は，甲の指示に従い，乙の責任と負担において修復等を実施すること。また，本業務の実施に伴う措置に起因して，正常な使用状態で甲の他の機器及びシステムに不具合や問題が発見された場合は，迅速に復旧のための措置を乙の責任と負担において実施すること。

(15)　本業務の実施に必要となる消耗品等は，乙の負担で用意するものとする。

(16)　乙は，本調達仕様書に疑義が生じた場合，本調達仕様書により難い事由が生じた場合及び本調達仕様書に記載のない事項については，甲と速やかに協議し，その指示に従うこと。

(17)　本調達仕様書に記載なき事項でも，本調達の構築・稼働・運用に必要と認められる事項は，甲と協議の上，実施すること。

(18)　乙は，甲との協議結果をその都度作成し，文書あるいはメールにて提出すること。

(19)　本運用管理業務の実施に必要となる用紙，記録媒体，バックアップテープ等については甲

担当者が用意するが，その他の消耗品（筆記用具等）については，乙の負担で用意するものとする。

(20)　情報管理室には原則として乙の所有物（常駐者及び応援者個人の所有物を含む。）を持ち込まないこと。やむを得ず持ち込んだ場合には，事前に甲担当者と協議し，甲担当者の承諾を得た上で持ち込むこと。また，持ち込んだ物品については，ラベリング及びリスト化を行い，甲の所有物との判別がつくように管理すること。

別紙１

平成　　年　　月　　日

宮内庁長官官房秘書課調査企画室長　　殿

住　　所
会　社　名
代表者氏名　　印

資料閲覧願い

標記について，「宮内庁共通基盤システムの整備・保守及び宮内庁 NWS の運用管理業務」の閲覧資料を閲覧したいので申請します。

申請に当たっては貴庁の指定する日時，場所で行い，機密に関する誓約書（別紙）を遵守した上で，亡失，汚損等ないように取り扱うものとし，閲覧終了後，直ちに返却します。

連　絡　先
（会社名）
（部署名）
（担当者氏名）　　印
（電話番号）
（メールアドレス）

宮内庁長官官房秘書課調査企画室長　　殿

機密保持に関する誓約書

標記について，「宮内庁共通基盤システムの整備・保守及び宮内庁 NWS の運用管理業務」における機密情報の取り扱いについて，下記の事項の遵守を誓約いたします。

なお，本誓約書に規定の事項は，私が作業に従事しなくなった場合にも，適用されるものとし，本誓約書に違反し，第三者に開示・漏えい，若しくは無許可に使用した場合には，貴庁は，私の所属する会社に対し，当該行為の差し止め，及び損害賠償を請求することに異存はありません。

記

１　機密情報とは

（１）本作業に関する電子データ，その他有形な媒体により提供された情報で，かつ宮内庁が機密であると指定したもの。

（２）宮内庁から口頭で開示された情報で，かつ宮内庁が機密であると指定したもの。

２　本作業によって知り得た機密情報について，宮内庁の承認がない場合は，第三者に開示，漏えいしないこと。

３　情報媒体による持ち出し，インターネットによる持ち出しを行わないこと。

４　本作業によって知り得た機密情報は，見積り作成のために使用する以外の目的では使用しないこと。

５　宮内庁からの文書による要求があった場合には，機密情報を返還，又は宮内庁立会いの下で破棄すること。

以　上

平成　　年　　月　　日

（会社名）
（部署名）
（担当者氏名）　　印
（電話番号）
（メールアドレス）

別紙２　宮内庁ＮＷ設置拠点・設置場所等

・御移居に伴い当該施設の名称が変更となる可能性があるので，留意すること。

拠点情報					事務，CAD端末概数（※１）	タブレット端末（※２）	システム関連端末（※３）	回線情報			備考
番号	拠点名１	拠点名２	郵便番号	住所				種別	帯域確保	帯域	
1	宮内庁本庁		100-8111	東京都千代田区千代田1番1号	E	◆	●	光	有	100Mbps	
2	宮内庁本庁（バックアップ回線）							光	有	10Mbps	
3	東宮御所		107-0051	東京都港区元赤坂2丁目1-8	D			光	有	100Mbps	
4	東宮御所（バックアップ回線）							光	有	10Mbps	
5	秋篠宮邸		詳細は契約締結後に開示します。		D			光		100Mbps	
6	常陸宮邸				A			光		100Mbps	
7	三笠宮邸				B			光		100Mbps	
8	三笠宮東邸				A			光		100Mbps	
9	高円宮邸				A			光		100Mbps	
10	高輪皇族邸　御殿棟				B			光		100Mbps	
11	高輪皇族邸　仮設事務棟				C			光		100Mbps	
12	三番町分庁舎		102-0075	東京都千代田区三番町2-18 宮内庁分庁舎	A			モバイルLTE		-	通信容量は7G以上とすること
13	埼玉鴨場		343-0021	埼玉県越谷市大字大林39	A			光		100Mbps	
14	新浜鴨場		272-0136	千葉県市川市新浜2-5-1	A			光		100Mbps	
15	多摩陵墓監区事務所	多摩部	193-0824	東京都八王子市長房町1833	A			光		100Mbps	
16	多摩陵墓監区事務所	豊島岡部	112-0012	東京都文京区大塚5-39-1	A			光		100Mbps	
17	多摩陵墓監区事務所	真野部	952-0313	新潟県佐渡市真野457	A			光		100Mbps	
18	桃山陵墓監区事務所	桃山部	612-0831	京都府京都市伏見区桃山町古城山	B			光		100Mbps	
19	桃山陵墓監区事務所	深草部	612-0871	京都府京都市伏見区深草坊町63-4	A			光		100Mbps	
20	桃山陵墓監区事務所	宇治部	611-0002	京都府宇治市木幡中村65	A			光		100Mbps	
21	桃山陵墓監区事務所	田邑部	616-8202	京都府京都市右京区宇多野馬場町1-1	A			光		100Mbps	
22	桃山陵墓監区事務所	嵯峨部	616-8382	京都府京都市右京区嵯峨天竜寺角倉町3077	A			光		100Mbps	
23	桃山陵墓監区事務所	金原部	617-0002	京都府向日市寺戸町大牧35	A			光		10Mbps	
24	桃山陵墓監区事務所	三島部	567-0018	大阪府茨木市太田3-10-3	A			光		100Mbps	
25	桃山陵墓監区事務所	可愛部	895-0065	鹿児島県薩摩川内市宮内町字脇園1935-1	A			光		10Mbps	
26	桃山陵墓監区事務所	高屋部	899-6404	鹿児島県霧島市溝辺町麓3392	A			光		100Mbps	
27	桃山陵墓監区事務所	吾平部	893-1101	鹿児島県鹿屋市吾平町上名字吾平山	A			モバイルLTE		-	通信容量は7G以上とすること
28	月輪陵墓監区事務所	月輪部	605-0977	京都府京都市東山区泉涌寺山内町34-2	B			光		100Mbps	
29	月輪陵墓監区事務所	山科部	607-8425	京都府京都市山科区御陵上御廟野町52	A			光		100Mbps	
30	月輪陵墓監区事務所	神楽岡部	606-8224	京都府京都市左京区北白川追分町57-1	A			光		100Mbps	
31	月輪陵墓監区事務所	北山部	603-8373	京都府京都市北区衣笠北高橋町1-1	A			光		100Mbps	
32	月輪陵墓監区事務所	大原部	601-1241	京都府京都市左京区大原勝林院町34-2	A			光		100Mbps	
33	月輪陵墓監区事務所	長等部	520-0037	滋賀県大津市御陵町3-2	A			ADSL		100Mbps	
34	畝傍陵墓監区事務所	畝傍部	634-0061	奈良県奈良市橿原市大久保町509	B			光		100Mbps	
35	畝傍陵墓監区事務所	奈良部	630-8236	奈良県奈良市下三条町47	A			光		100Mbps	
36	畝傍陵墓監区事務所	佐紀部	631-0803	奈良県奈良市山陵町325	A			光		100Mbps	
37	畝傍陵墓監区事務所	山辺部	632-0052	奈良県天理市柳本町1876	A			光		100Mbps	
38	畝傍陵墓監区事務所	忍坂部	633-0005	奈良県桜井市大字忍阪556	A			光		100Mbps	
39	畝傍陵墓監区事務所	傍丘部	639-0264	奈良県香芝市今泉1	A			光		10Mbps	
40	畝傍陵墓監区事務所	掖上部	634-0144	奈良県高市郡明日香村大字平田1658-1	A			ADSL		47Mbps	
41	畝傍陵墓監区事務所	吉野部	639-3115	奈良県吉野郡吉野町大字吉野山1023	A			ADSL		8Mbps	
42	古市陵墓監区事務所	古市部	583-0857	大阪府羽曳野市誉田6-11-3	B			光		100Mbps	
43	古市陵墓監区事務所	藤井寺部	583-0024	大阪府藤井寺市藤井寺4-764	A			光		100Mbps	
44	古市陵墓監区事務所	磯長部	583-0991	大阪府南河内郡太子町大字春日1532	A			光		100Mbps	
45	古市陵墓監区事務所	百舌鳥部	590-0035	大阪府堺市堺区大仙町7-1	A			光		100Mbps	
46	古市陵墓監区事務所	高野山部	648-0211	和歌山県伊都郡高野町大字高野山	A			ADSL		47Mbps	
47	那須御用邸管理事務所		329-3200	栃木県那須郡那須町大字湯本207	A			光		100Mbps	
48	須崎御用邸管理事務所		415-0014	静岡県下田市須崎字嵐の尾1206-1	A			光		100Mbps	
49	葉山御用邸管理事務所		240-0111	神奈川県三浦郡葉山町一色2038-1	A			光		100Mbps	
50	正倉院事務所		630-8211	奈良県奈良市雑司町129	B		★	光		100Mbps	
51	御料牧場		329-1224	栃木県塩谷郡高根沢町上高根沢6020	C			光		100Mbps	
52	京都事務所		602-8611	京都市上京区京都御苑3番	D		▲	光	有	100Mbps	
53	京都事務所（バックアップ回線）							光	有	10Mbps	
54	桂離宮		615-8014	京都府京都市西京区桂御園1-1	A			光		10Mbps	
55	修学院離宮		606-8052	京都府京都市左京区修学院藪添1-2	A			光		100Mbps	

※１　A：１個以上～10個未満，B：10個以上～30個未満，C：30個以上～50個未満，D：50個以上～100個未満，E：100個以上

※２　◆：タブレット端末

※３　●：統合運用管理端末(運用管理セグメント用端末)，★：宝物管理システム用端末，▲参観受付システム用端末

別紙3. 各フロア配線、必要ポート数状況

閲覧資料により既存の資料を確認し，既存で各フロア間のリンクが冗長化されている箇所については，同様にリンク冗長を行うこと。
また，最新の構成については、閲覧資料と本資料を照らし合わせの上、必要な機器群を見積もること。
なお，御移居に伴い該当施設の名称が変更となる可能性があるので，留意すること。

No.	場所		FROM	配線状況	（距離）	TO	19インチラックの有無(TO側)	必要なCAT5のポート数(TO側)	配線間の必要帯域
1	本庁	本庁舎	情報管理室	光ケーブル	550m以下	秘書課	有	48ポート以上	1Gbps
2	本庁	本庁舎	情報管理室	光ケーブル	550m以下	調査企画室	有	24ポート以上	1Gbps
3	本庁	本庁舎	調査企画室	CAT5		調査企画室分室	無	24ポート以上	1Gbps
4	本庁	本庁舎	情報管理室	光ケーブル	550m以下	総務課	有	48ポート以上	1Gbps
5	本庁	本庁舎	情報管理室	光ケーブル	550m以下	宮務課	有	24ポート以上	1Gbps
6	本庁	本庁舎	情報管理室	光ケーブル	550m以下	侍従長秘書室	有	24ポート以上	1Gbps
7	本庁	本庁舎	情報管理室	光ケーブル	550m以下	侍従職	有	48ポート以上	1Gbps
8	本庁	本庁舎	情報管理室	光ケーブル	550m以下	掌典職	有	24ポート以上	1Gbps
9	本庁	本庁舎	情報管理室	光ケーブル	550m以下	式部職	有	48ポート以上	1Gbps
10	本庁	本庁舎	情報管理室	光ケーブル	550m以下	管理課	有	24ポート以上	1Gbps
11	本庁	本庁舎	管理課	CAT5		宮殿管理官付	有	8ポート以上	1Gbps
12	本庁	本庁舎	情報管理室	光ケーブル	550m以下	庭園課	有	8ポート以上	1Gbps
13	本庁	本庁舎	庭園課	CAT5		管理課参観係	有	8ポート以上	1Gbps
14	本庁	本庁舎	情報管理室	光ケーブル	550m以下	主計課	有	48ポート以上	1Gbps
15	本庁	本庁舎	情報管理室	光ケーブル	550m以下	用度課	有	48ポート以上	1Gbps
16	本庁	本庁舎	情報管理室	光ケーブル	550m以下	第3会議室	有	48ポート以上	1Gbps
17	本庁	本庁舎	第3会議室	CAT5		情報管理室(保守員室)	有	24ポート以上	1Gbps
18	本庁	本庁舎	第3会議室	CAT5		設備管理係詰所1	無	8ポート以上	1Gbps
19	本庁	本庁舎	設備管理係詰所1	CAT5		設備管理係詰所2	無	8ポート以上	1Gbps
20	本庁	本庁舎	情報管理室	光ケーブル	550m以下	車馬課	有	24ポート以上	1Gbps
21	本庁	車馬課	車馬課	CAT5		車馬課事務室1	無	8ポート以上	1Gbps
22	本庁	車馬課	車馬課	CAT5		車馬課事務室2	無	8ポート以上	1Gbps
23	本庁	車馬課	車馬課	CAT5		運転手控え室	無	8ポート以上	1Gbps
24	本庁	車馬課	車馬課	CAT5		整備工場	無	8ポート以上	1Gbps
25	本庁	宮殿	情報管理室	光ケーブル	550m以下	宮殿殿部仕人室	有	8ポート以上	1Gbps
26	本庁	宮殿	宮殿殿部仕人室	CAT5		侍従候所	無	8ポート以上	1Gbps
27	本庁	宮殿	情報管理室	光ケーブル	550m以下	宮殿大膳課	有	48ポート以上	1Gbps
28	本庁	宮殿	宮殿大膳課	CAT5		管理係	有	24ポート以上	1Gbps
29	本庁	御所	情報管理室	光ケーブル	550m以上	御所	有	48ポート以上	1Gbps
30	本庁	御所	御所	CAT5		主膳	有	8ポート以上	1Gbps
31	本庁	御所	御所	CAT5		女官候所	無	8ポート以上	1Gbps
32	本庁	御所	御所	CAT5		出仕室	無	8ポート以上	1Gbps
33	本庁	御所	御所	CAT5		女子職員室	無	8ポート以上	1Gbps
34	本庁	書陵部	書陵部BF	光ケーブル	550m以下	書陵部1F	有	24ポート以上	100Mbps
35	本庁	書陵部	書陵部BF	光ケーブル	550m以下	書陵部2F	有	48ポート以上	100Mbps
36	本庁	書陵部	書陵部BF	光ケーブル	550m以下	書陵部3F	有	24ポート以上	100Mbps
37	本庁	書陵部	書陵部BF	光ケーブル	550m以下	書陵部4F	有	48ポート以上	100Mbps
38	本庁	書陵部	書陵部BF	光ケーブル	550m以下	楽部	有	24ポート以上	100Mbps
39	本庁	三の丸尚蔵館	三の丸尚蔵館	CAT5		三の丸尚蔵館	有	24ポート以上	1Gbps
40	本庁	東御苑	三の丸尚蔵館	光ケーブル	550m以下	東御苑	有	8ポート以上	100Mbps
41	本庁	東御苑	東御苑	CAT5		東御苑事務室1	無	8ポート以上	1Gbps
42	本庁	病院1、病院2	三の丸尚蔵館	光ケーブル	550m以下	病院1、病院2	有	48ポート以上	100Mbps
43	本庁	主馬班	三の丸尚蔵館	光ケーブル	550m以下	主馬班	有	24ポート以上	100Mbps
44	本庁	主馬班	主馬班	CAT5		主馬班事務室1	無	8ポート以上	1Gbps
45	本庁	本庁舎	情報管理室	光ケーブル	550m以下	庁舎3階	有	8ポート以上	1Gbps
46	本庁	生物学御研究所	情報管理室	構内内線	2km以下	生物学御研究所	無	1ポート以上	4.6Mbps程度
47	本庁	賢所	情報管理室	構内内線	2km以下	賢所	無	8ポート以上	4.6Mbps程度
48	本庁	車馬課北口玄関	情報管理室	構内内線	2km以下	車馬課北口玄関	無	8ポート以上	4.6Mbps程度
49	本庁	設備管制室	情報管理室	構内内線	2km以下	設備管制室	無	8ポート以上	4.6Mbps程度
50	本庁	水道詰所	情報管理室	構内内線	2km以下	水道詰所	無	8ポート以上	4.6Mbps程度
51	本庁	大道庭園事務所	情報管理室	構内内線	2km以下	大道庭園事務所	無	8ポート以上	4.6Mbps程度
52	本庁	主馬班診療所	情報管理室	構内内線	2km以下	主馬班診療所	無	1ポート以上	4.6Mbps程度
53	本庁	平川門守衛所	情報管理室	構内内線	2km以下	平川門守衛所	無	1ポート以上	4.6Mbps程度
54	東宮御所	東宮御所	IP-VPNルータ	CAT5		東宮御所マシン室	有	24ポート以上	100Mbps
55	東宮御所	東宮御所	東宮御所マシン室	CAT5		東宮御所マシン室	有	48ポート以上	1Gbps
56	東宮御所	東宮御所	東宮御所マシン室	CAT5		侍従室	有	24ポート以上	1Gbps
57	東宮御所	東宮御所	東宮御所マシン室	CAT5		主膳	有	24ポート以上	1Gbps
58	東宮御所	東宮御所	東宮御所マシン室	CAT5		内舎人	有	24ポート以上	1Gbps
59	東宮御所	東宮御所	東宮御所マシン室	CAT5		女官室	有	24ポート以上	1Gbps
60	東宮御所	赤坂設備係	東宮御所マシン室	構内内線	2km以下	赤坂設備係	無	8ポート以上	4.6Mbps程度
61	東宮御所	配車第二係	東宮御所マシン室	構内内線	2km以下	配車第二係	無	8ポート以上	4.6Mbps程度
62	東宮御所	赤坂庭園設備係	東宮御所マシン室	構内内線	2km以下	赤坂庭園設備係	無	8ポート以上	4.6Mbps程度
63	宮邸	秋篠宮邸	IP-VPNルータ	CAT5		秋篠宮邸	無	24ポート以上	100Mbps
64	宮邸	秋篠宮邸	秋篠宮邸	CAT5		仮事務所	無	24ポート以上	100Mbps
65	宮邸	秋篠宮邸	秋篠宮邸	構内内線	2km以下	侍女長補	無	1ポート以上	4.6Mbps程度
66	宮邸	常陸宮邸	IP-VPNルータ	CAT5		常陸宮邸	無	24ポート以上	100Mbps
67	宮邸	三笠宮邸	IP-VPNルータ	CAT5		三笠宮邸	無	24ポート以上	100Mbps
68	宮邸	三笠宮邸	三笠宮邸	構内内線	2km以下	運転技官	無	1ポート以上	4.6Mbps程度
69	宮邸	三笠宮東邸	IP-VPNルータ	CAT5		三笠宮東邸	無	24ポート以上	100Mbps
70	宮邸	高円宮邸	IP-VPNルータ	CAT5		高円宮邸	無	24ポート以上	100Mbps
71	陵墓監区事務所	多摩陵墓監区事務所	IP-VPNルータ	CAT5		多摩陵墓監区事務所	無	24ポート以上	100Mbps
72	陵墓監区事務所	桃山陵墓監区事務所	IP-VPNルータ	CAT5		桃山陵墓監区事務所	無	24ポート以上	100Mbps
73	陵墓監区事務所	月輪陵墓監区事務所	IP-VPNルータ	CAT5		月輪陵墓監区事務所	無	24ポート以上	100Mbps

No.	場所		FROM	配線状況	（距離）	TO	19インチラックの有無(TO側)	必要なCAT5のポート数(TO側)	配線間の必要帯域
74	陵墓監区事務所	畝傍陵墓監区事務所	IP-VPNルータ	CAT5		畝傍陵墓監区事務所	無	24ポート以上	100Mbps
75	陵墓監区事務所	古市陵墓監区事務所	IP-VPNルータ	CAT5		古市陵墓監区事務所	無	24ポート以上	100Mbps
76	御用邸	須崎御用邸	IP-VPNルータ	CAT5		須崎御用邸	無	24ポート以上	100Mbps
77	御用邸	葉山御用邸	IP-VPNルータ	CAT5		葉山御用邸	無	24ポート以上	100Mbps
78	御用邸	葉山御用邸	葉山御用邸	構内内線	2km以下	御殿棟	無	1ポート以上	4.6Mbps程度
79	御用邸	那須御用邸	IP-VPNルータ	CAT5		那須御用邸	無	24ポート以上	100Mbps
80	御用邸	那須御用邸	那須御用邸事務所	構内内線	2km以下	工務課詰め所	無	1ポート以上	4.6Mbps程度
81	御用邸	那須御用邸	那須御用邸事務所	構内内線	2km以下	自動車班詰め所	無	1ポート以上	4.6Mbps程度
82	御用邸	那須御用邸	那須御用邸事務所	構内内線	2km以下	付属邸	無	24ポート以上	4.6Mbps程度
83	正倉院事務所	正倉院事務所	IP-VPNルータ	CAT5		正倉院事務所マシン室	有	1ポート以上	100Mbps
84	正倉院事務所	正倉院事務所	正倉院事務所マシン室	光ケーブル	550m以上	別館管制室	有	8ポート以上	100Mbps
85	正倉院事務所	正倉院事務所	正倉院事務所マシン室	光ケーブル	550m以上	本館	有	24ポート以上	100Mbps
86	正倉院事務所	正倉院事務所	正倉院事務所マシン室	光ケーブル	550m以上	保存修理棟	有	24ポート以上	100Mbps
87	正倉院事務所	正倉院事務所	正倉院事務所マシン室	光ケーブル	550m以上	保存科学実験棟	有	24ポート以上	100Mbps
88	御料牧場	御料牧場事務所	IP-VPNルータ	CAT5		御料牧場マシン室	有	24ポート以上	100Mbps
89	御料牧場	御料牧場事務所	御料牧場マシン室	CAT5		御料牧場マシン室	有	48ポート以上	1Gbps
90	御料牧場	養豚・加工係（肉加工所）	御料牧場マシン室	構内内線	2km以下	養豚・加工係（肉加工所）	無	1ポート以上	4.6Mbps程度
91	御料牧場	管理係	御料牧場マシン室	構内内線	2km以下	管理係	無	1ポート以上	4.6Mbps程度
92	御料牧場	育馬係	御料牧場マシン室	構内内線	2km以下	育馬係	無	1ポート以上	4.6Mbps程度
93	御料牧場	衛生係	御料牧場マシン室	構内内線	2km以下	衛生係	無	1ポート以上	4.6Mbps程度
94	御料牧場	育牛係	御料牧場マシン室	構内内線	2km以下	育牛係	無	1ポート以上	4.6Mbps程度
95	御料牧場	乳製品係	御料牧場マシン室	構内内線	2km以下	乳製品係	無	1ポート以上	4.6Mbps程度
96	御料牧場	養豚・加工係	御料牧場マシン室	構内内線	2km以下	養豚・加工係	無	1ポート以上	4.6Mbps程度
97	御料牧場	育羊係	御料牧場マシン室	構内内線	2km以下	育羊係	無	1ポート以上	4.6Mbps程度
98	御料牧場	養鶏係	御料牧場マシン室	構内内線	2km以下	養鶏係	無	1ポート以上	4.6Mbps程度
99	御料牧場	耕作係	御料牧場マシン室	構内内線	2km以下	耕作係	無	1ポート以上	4.6Mbps程度
101	御料牧場	農機具係	御料牧場マシン室	構内内線	2km以下	農機具係	無	1ポート以上	4.6Mbps程度
102	御料牧場	そ采係	御料牧場マシン室	構内内線	2km以下	そ采係	無	1ポート以上	4.6Mbps程度
103	御料牧場	外交団休所	御料牧場マシン室	構内内線	2km以下	外交団休所	無	1ポート以上	4.6Mbps程度
104	京都事務所	京都事務所	IP-VPNルータ	CAT5		京都事務所マシン室	有	1ポート以上	100Mbps
105	京都事務所	京都事務所	京都事務所マシン室	CAT5		庶務課	有	24ポート以上	1Gbps
106	京都事務所	京都事務所	京都事務所マシン室	CAT5		管理課	有	24ポート以上	1Gbps
107	京都事務所	京都事務所	管理課	CAT5		林園課	有	24ポート以上	1Gbps
108	京都事務所	京都事務所	京都事務所マシン室	CAT5		管理課（管理棟）	有	24ポート以上	1Gbps
109	京都事務所	京都御所	京都事務所マシン室	構内内線	2km以下	京都御所	無	8ポート以上	4.6Mbps程度
110	京都事務所	大宮御所	京都事務所マシン室	構内内線	2km以下	大宮御所	無	1ポート以上	4.6Mbps程度
111	京都事務所	大宮御殿	京都事務所マシン室	構内内線	2km以下	大宮御殿	無	1ポート以上	4.6Mbps程度
112	京都事務所	京都庭園	京都事務所マシン室	構内内線	2km以下	京都庭園	無	1ポート以上	4.6Mbps程度
113	離宮	修学院離宮	修学院離宮	構内内線	2km以下	別館	無	1ポート以上	4.6Mbps程度
114	本庁	三の丸尚蔵館	情報管理室	光ケーブル	550m以下	三の丸尚蔵館	有	24ポート以上	100Mbps
115	本庁	書陵部	情報管理室	光ケーブル	550m以下	書陵部BF	有	24ポート以上	100Mbps
116	本庁	御所	情報管理室	光ケーブル	550m以下	御所	有	48ポート以上	100Mbps
117	高輪皇族邸	御殿棟	IP-VPNルータ	光ケーブル	550m以下	御殿棟	無	48ポート以上	100Mbps
118	高輪皇族邸	仮設事務棟	IP-VPNルータ	光ケーブル	550m以下	仮設事務棟	無	48ポート以上	100Mbps
119	宮邸	秋篠宮邸	秋篠宮邸	CAT6		秋篠宮邸　仮設事務所	無	48ポート以上	100Mbps
120	宮邸	秋篠宮邸	秋篠宮邸	CAT6		赤坂御用地事務所・収蔵庫棟	無	48ポート以上	100Mbps

別紙4　本調達機器及び各事業者の役割範囲

本調達機器及びその他作業対象機器について，各事業者の役割分担を示す。各役割の詳細については，調達仕様書及び本紙を参照すること。
なお，乙（宮内庁CIS事業者）の役割範囲は「〇」印で示す。

No.	現行/新規	区分	調達機器要件 調達仕様書記載箇所	対象機器	種別	設計/構築	物品調達	物品保守契約 （詳細は調達仕様書(案)を確認すること。）	運用/監視 （移行期間中）	運用/監視 （システム更新後）	システム 保守業務	備考
1	現行	宮内庁LAN	3. 1. 3.	コンソール（キーボード・ディスプレイ，マウス）機器	サーバ機器以外 （シングル）	〇	〇	〇	〇	〇	〇	
2	現行		3. 2.	無停電電源装置(UPS)	サーバ機器以外 （シングル・二重化）	〇	〇	〇	〇	〇	〇	調達仕様書3.2.(1)を参照のこと。
3	現行		3. 3.	サーバセグメント用サーバ・ネットワークスイッチ	スイッチ （二重化）	〇	〇	後出しセンドバック （導入年の次年度以降）	〇	〇	〇	
4	現行		3. 4.	運用管理セグメント用サーバスイッチ	スイッチ （二重化）	〇	〇	後出しセンドバック （導入年の次年度以降）	〇	〇	〇	
5	現行		3. 5.	宮内庁NWS運用管理クライアント端末	端末 （シングル）	〇	〇	〇	〇	〇	〇	
6	現行		3. 6.	ディレクトリサーバ	サーバ （二重化）	〇	〇	〇	〇	〇	〇	調達仕様書3.6.2.を参照のこと。
7	新規		3. 7.	特権ID管理	サーバ （二重化）	〇	〇	〇	〇	〇	〇	
8	現行		3. 8.	ユーザ管理用サーバ	サーバ （二重化）	〇	〇	〇	〇	〇	〇	
9	現行		3. 9.	内部DNSサーバ	サーバ （二重化）	〇	〇	〇	〇	〇	〇	
10	現行		3. 10.	WSUSサーバ	サーバ （二重化）	〇	〇	〇	〇	〇	〇	
11	現行		3. 11.	バックアップサーバ	サーバ （二重化）	〇	〇	〇	〇	〇	〇	
12	現行		3. 12.	ウイルス対策サーバ（クライアント端末用）	サーバ （二重化）	〇	〇	〇	〇	〇	〇	調達仕様書3.6.2.を参照のこと。
13	現行		3. 12.	ウイルス対策サーバ（サーバ用）	サーバ （二重化）	〇	〇	〇	〇	〇	〇	
14	新規		3. 13.	ログ収集サーバ	サーバ （シングル）	〇	〇	〇	〇	〇	〇	
15	現行		3. 14.	ファイルサーバ	サーバ （二重化）	〇	〇	〇	〇	〇	〇	調達仕様書3.6.2.を参照のこと。
16	新規		3. 15.	振る舞いログ分析（UEBA）サーバ	サーバ （シングル）	〇	〇	〇	〇	〇	〇	
17	現行	宮内庁WAN及びインターネット接続回線サービス接続	—	宮内庁WAN（閉域網）	回線	宮内庁統合NW事業者	宮内庁統合NW事業者	宮内庁統合NW事業者	宮内庁統合NW事業者	宮内庁統合NW事業者	宮内庁統合NW事業者	WAN回線サービス ※回線サービスに付帯する機器は，SLAに基づいて保守をすること。
18	現行		—	宮内庁WANルータ	回線機器	宮内庁統合NW事業者	宮内庁統合NW事業者	宮内庁統合NW事業者	宮内庁統合NW事業者	宮内庁統合NW事業者	宮内庁統合NW事業者	WAN回線サービス ※回線サービスに付帯する機器は，SLAに基づいて保守をすること。
19	現行		—	インターネット接続回線サービス	回線	宮内庁統合NW事業者	宮内庁統合NW事業者	宮内庁統合NW事業者	宮内庁統合NW事業者	宮内庁統合NW事業者	宮内庁統合NW事業者	インターネット回線サービス ※回線サービスに付帯する機器は，SLAに基づいて保守をすること。
20	現行		—	インターネット接続機器	回線機器 （二重化）	宮内庁統合NW事業者	宮内庁統合NW事業者	宮内庁統合NW事業者	宮内庁統合NW事業者※1（2020年1月末日まで） ただしWAN側からの監視は実施	〇 ※1（2020年2月1日から）	宮内庁統合NW事業者	

No.	現行/新規	区分	調達機器要件 調達仕様書記載箇所	対象機器	種別	設計/構築	物品調達	物品保守契約 （詳細は調達仕様書(案)を確認すること。）	運用/監視 （移行期間中）	運用/監視 （システム更新後）	システム 保守業務	備考
21	現行		—	DNSサービス(コンテンツサーバ)	サービス	宮内庁統合NW 事業者	宮内庁統合NW 事業者	宮内庁統合NW 事業者	宮内庁統合NW 事業者	宮内庁統合NW 事業者	宮内庁統合NW 事業者	
22	現行		—	メールゲートウェイサービス	サービス	宮内庁統合NW 事業者	宮内庁統合NW 事業者	宮内庁統合NW 事業者	宮内庁統合NW 事業者	宮内庁統合NW 事業者	宮内庁統合NW 事業者	
23	現行		—	外部ファイル共有サービス	サービス	宮内庁統合NW 事業者	宮内庁統合NW 事業者	宮内庁統合NW 事業者	宮内庁統合NW 事業者	宮内庁統合NW 事業者	宮内庁統合NW 事業者	
24	現行	宮内庁LAN	—	コアスイッチ	スイッチ （二重化）	宮内庁統合NW 事業者	宮内庁統合NW 事業者	後出しセンドバック （導入年の次年度以降）	宮内庁統合NW事業者※1（2020年1月末日まで）	○ ※1（2020年2月1日から）	宮内庁統合NW 事業者	二重化構成なので，後出しセンドバック保守（導入年の次年度以降）
25	現行		—	フロア集約スイッチ	スイッチ （二重化）	宮内庁統合NW 事業者	宮内庁統合NW 事業者	後出しセンドバック （導入年の次年度以降）	宮内庁統合NW事業者※1（2020年1月末日まで）	○ ※1（2020年2月1日から）	宮内庁統合NW 事業者 ※3	二重化構成なので，後出しセンドバック保守（導入年の次年度以降）
26	現行		—	エッジスイッチ	スイッチ （シングル）	宮内庁統合NW 事業者	宮内庁統合NW 事業者	先出しセンドバック保守（導入年の次年度以降）	宮内庁統合NW事業者※1（2020年1月末日まで）	○ ※1（2020年2月1日から）	宮内庁統合NW 事業者 ※3	シングル構成なので，先出しセンドバック保守（導入年の次年度以降）
27	現行		—	構内内線モデム接続用スイッチ	スイッチ （シングル）	宮内庁統合NW 事業者	宮内庁統合NW 事業者	先出しセンドバック保守（導入年の次年度以降）	宮内庁統合NW事業者※1（2020年1月末日まで）	○ ※1（2020年2月1日から）	宮内庁統合NW 事業者 ※3	シングル構成なので，先出しセンドバック保守（導入年の次年度以降）
28	現行		—	構内内線モデム	電信電話変換機器	宮内庁統合NW 事業者※4	宮内庁統合NW 事業者※4	保守不要 ※スポット保守（2019年11月1日～予備機として統合NWで調達したものに限る）	運用管理 支援事業者※2	○	宮内庁統合NW 事業者 ※3 ただし，予備機として統合NWで調達したものに限る	
29	現行		—	各地方拠点スイッチ	スイッチ （シングル）	宮内庁統合NW 事業者	宮内庁統合NW 事業者	先出しセンドバック保守（導入年の次年度以降）	宮内庁統合NW事業者※1（2020年1月末日まで）	○ ※1（2020年2月1日から）	宮内庁統合NW 事業者 ※3	シングル構成なので，先出しセンドバック保守（導入年の次年度以降）
30	現行		—	政府共通NW用境界スイッチ	スイッチ （二重化）	宮内庁統合NW 事業者	宮内庁統合NW 事業者	後出しセンドバック （導入年の次年度以降）	宮内庁統合NW事業者※1（2020年1月末日まで）	○ ※1（2020年2月1日から）	宮内庁統合NW 事業者	二重化構成なので，後出しセンドバック保守（導入年の次年度以降）
31	現行		—	DMZサーバ接続スイッチ	スイッチ （二重化）	宮内庁統合NW 事業者	宮内庁統合NW 事業者	後出しセンドバック （導入年の次年度以降）	宮内庁統合NW事業者※1（2020年1月末日まで）	○ ※1（2020年2月1日から）	宮内庁統合NW 事業者	二重化構成なので，後出しセンドバック保守（導入年の次年度以降）
32	現行		—	運用管理LANスイッチ	スイッチ （シングル）	宮内庁統合NW 事業者	宮内庁統合NW 事業者	先出しセンドバック保守（導入年の次年度以降）	宮内庁統合NW事業者※1（2020年1月末日まで）	○ ※1（2020年2月1日から）	宮内庁統合NW 事業者	シングル構成なので，先出しセンドバック保守（導入年の次年度以降）
33	現行		—	インターネット境界接続スイッチ	回線	宮内庁統合NW 事業者	宮内庁統合NW 事業者	宮内庁統合NW事業者	宮内庁統合NW事業者	宮内庁統合NW事業者	宮内庁統合NW 事業者	インターネット回線サービス ※回線サービスに付帯する機器は，SLAに基づいて保守をすること。
34	現行	宮内庁LAN	—	政府共通NWファイアウォール	回線機器 以外	宮内庁統合NW 事業者	宮内庁統合NW 事業者	先出しセンドバック保守（導入年の次年度以降）	宮内庁統合NW事業者※1（2020年1月末日まで）	○ ※1（2020年2月1日から）	宮内庁統合NW 事業者	
35	新規		—	DMZファイアウォール	回線機器 以外 （二重化）	宮内庁統合NW 事業者	宮内庁統合NW 事業者	宮内庁統合NW 事業者	宮内庁統合NW事業者※1（2020年1月末日まで）	○ ※1（2020年2月1日から）	宮内庁統合NW 事業者	
36	現行		—	セグメント間ファイアウォール	回線機器 以外	宮内庁統合NW 事業者	宮内庁統合NW 事業者	先出しセンドバック保守（導入年の次年度以降）	宮内庁統合NW事業者※1（2020年1月末日まで）	○ ※1（2020年2月1日から）	宮内庁統合NW 事業者	
37	既存納入機器		—	インターネット接続ファイアウォール （web標的型攻撃対策装置）	別調達	※5	各事業者	各事業者	運用管理 支援事業者※2	○	各事業者	
38	現行		—	電子メール中継サーバ	サーバ （二重化）	宮内庁統合NW 事業者	宮内庁統合NW 事業者	（HW） 不要 ※障害発生時にスポット保守 （SW） 平日日勤帯	宮内庁統合NW事業者※1（2020年1月末日まで）	○ ※1（2020年2月1日から）	宮内庁統合NW 事業者	システム領域のバックアップは，宮内庁CISで京都に設置するバックアップサーバにて行う。そのため，宮内庁CISの調達で用意するバックアップシステムのエージェントの導入及びバックアップが正常に動作するまで協力すること。
39	現行		—	Webプロキシサーバ	サーバ （二重化）	宮内庁統合NW 事業者	宮内庁統合NW 事業者	宮内庁統合NW事業者	宮内庁統合NW事業者※1（2020年1月末日まで）	○ ※1（2020年2月1日から）	宮内庁統合NW 事業者	

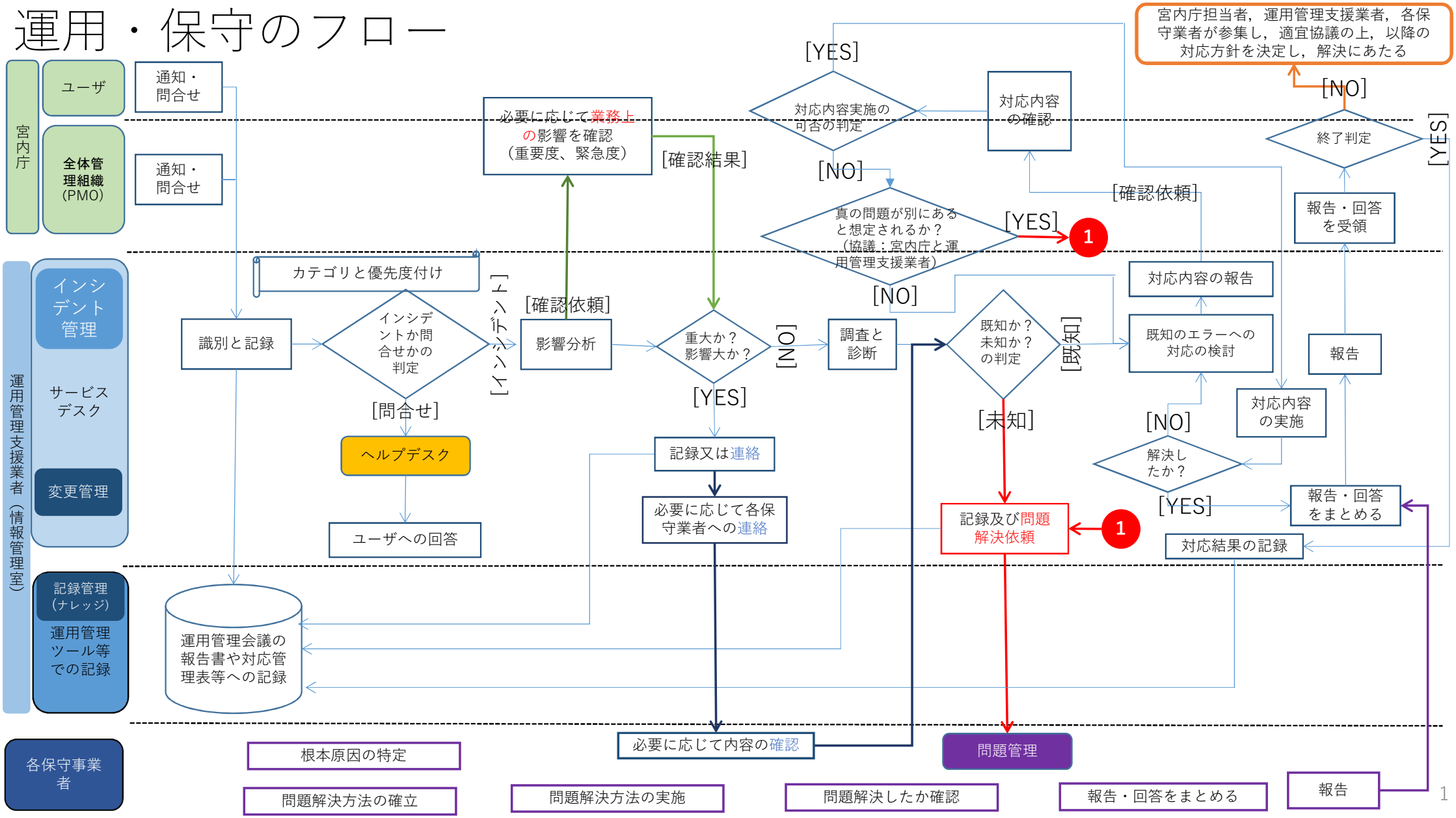
No.	現行/新規	区分	調達機器要件 調達仕様書記載箇所	対象機器	種別	設計/構築	物品調達	物品保守契約 （詳細は調達仕様書(案)を確認すること。）	運用/監視 （移行期間中）	運用/監視 （システム更新後）	システム 保守業務	備考
40	現行	宮内庁LAN	—	ゲートウェイ型ウイルス対策サーバ	サーバ （二重化）	宮内庁統合NW 事業者	宮内庁統合NW 事業者	宮内庁統合NW 事業者	宮内庁統合NW事業者※1（2020年1月末日まで）	○ ※1（2020年2月1日から）	宮内庁統合NW 事業者	
41	現行		—	DMZ用DNSサーバ	サーバ （二重化）	宮内庁統合NW 事業者	宮内庁統合NW 事業者	宮内庁統合NW 事業者	宮内庁統合NW事業者※1（2020年1月末日まで）	○ ※1（2020年2月1日から）	宮内庁統合NW 事業者	
42	現行		—	DMZ用NTPサーバ	サーバ （二重化）	宮内庁統合NW 事業者	宮内庁統合NW 事業者	宮内庁統合NW 事業者	宮内庁統合NW事業者※1（2020年1月末日まで）	○ ※1（2020年2月1日から）	宮内庁統合NW 事業者	
43	新規		—	TLS復号スイッチ	回線機器 以外	宮内庁統合NW 事業者	宮内庁統合NW 事業者	宮内庁統合NW 事業者	宮内庁統合NW事業者※1（2020年1月末日まで）	○ ※1（2020年2月1日から）	宮内庁統合NW 事業者	
44	新規		—	シリアルコンソールターミナルサーバ	回線機器 以外	宮内庁統合NW 事業者	宮内庁統合NW 事業者	先出しセンドバック保守（導入年の次年度以降）	宮内庁統合NW事業者※1（2020年1月末日まで）	○ ※1（2020年2月1日から）	宮内庁統合NW 事業者	
45	新規		—	運用管理セグメント拠点間接続用VPN装置	回線機器 以外	宮内庁統合NW 事業者	宮内庁統合NW 事業者	先出しセンドバック保守（導入年の次年度以降）	宮内庁統合NW事業者※1（2020年1月末日まで）	○ ※1（2020年2月1日から）	宮内庁統合NW 事業者	
46	新規		—	エンドポイントセキュリティ対策の強化	サーバ （シングル）	宮内庁統合NW 事業者	宮内庁統合NW 事業者	宮内庁統合NW 事業者	宮内庁統合NW 事業者	○	宮内庁統合NW 事業者	
47	新規		—	無停電電源装置(UPS)	回線機器以外 （シングル）	宮内庁統合NW 事業者	宮内庁統合NW 事業者	先出しセンドバック保守（導入年の次年度以降）	宮内庁統合NW事業者※1（2020年1月末日まで）	○ ※1（2020年2月1日から）	宮内庁統合NW 事業者	
48	現行		—	監視サービス	サービス	宮内庁統合NW 事業者	宮内庁統合NW 事業者	宮内庁統合NW 事業者	宮内庁統合NW 事業者	宮内庁統合NW 事業者	宮内庁統合NW 事業者	
49	現行		—	運用管理セグメント用端末	端末	宮内庁統合NW 事業者	宮内庁統合NW 事業者	宮内庁統合NW 事業者	宮内庁統合NW事業者※1（2020年1月末日まで）	○ ※1（2020年2月1日から）	宮内庁統合NW 事業者	日常の運用管理業務で庁内職員，保守事業者等とコミュニケーション（メール，Web）を行うために利用するための端末は，宮内庁CISで調達する「宮内庁NWS運用管理クライアント端末」となる。 運用管理セグメント用端末は，通常の生活系ネットワークにつながっていないため，定期的にパッチを当てるための運用ルールと手順書の作成は，統合NW受託者で行う。
50	新規	統合SOCサービス	—	統合SOCサービス	サービス	宮内庁統合NW 事業者	宮内庁統合NW 事業者	宮内庁統合NW 事業者	宮内庁統合NW 事業者	宮内庁統合NW 事業者	宮内庁統合NW 事業者	
51	既存納入機器	既存納入機器	—	Web標的型攻撃対策装置	別調達	※5	各事業者	各事業者	運用管理 支援事業者※2	○	各事業者※6	
52	既存納入機器	既存納入機器	—	メール標的型攻撃対策装置	別調達	※5	各事業者	各事業者	運用管理 支援事業者※2	○	各事業者※6	
53	既存納入機器	既存納入機器	—	グループウェアシステム	別調達	※5	各事業者	各事業者	運用管理 支援事業者※2	○	各事業者	
54	既存納入機器	既存納入機器	—	Web無害化システム	別調達	※5	各事業者	各事業者	運用管理 支援事業者※2	○	各事業者	
55	既存納入機器	既存納入機器	—	GWプロキシサーバ	別調達	※5	各事業者	宮内庁統合NW 事業者	宮内庁統合NW 事業者	○	宮内庁統合NW 事業者	当該機器は買取機器であり，再設計及び機器の保守（保守移管の上で）を統合NW受託者が行う。
56	既存納入機器	既存納入機器	—	その他宮内庁ネットワークシステム内既存機器	別調達	※5	各事業者	各事業者	運用管理 支援事業者※2	○	各事業者	
57	新規	その他統合NW機器	—	その他宮内庁統合NW調達にてオンプレミスにて納入する機器群	宮内庁統合NW 調達	宮内庁統合NW 事業者	宮内庁統合NW 事業者	宮内庁統合NW 事業者	－	○ ※1（2020年2月1日から）	宮内庁統合NW 事業者	
58	新規		—	その他宮内庁統合NW調達にてクラウドサービスを採用する機器群	サービス	宮内庁統合NW 事業者	宮内庁統合NW 事業者	宮内庁統合NW 事業者	宮内庁統合NW 事業者	宮内庁統合NW 事業者	宮内庁統合NW 事業者	

No.	現行/新規	区分	調達機器要件 調達仕様書記載箇所	対象機器	種別	設計/構築	物品調達	物品保守契約 （詳細は調達仕様書(案)を確認すること。）	運用/監視 （移行期間中）	運用/監視 （システム更新後）	システム 保守業務	備考

※の説明

※1	宮内庁LANの一部の機器については，次期運用管理事業者（宮内庁CIS受託者）にて運用を行うこととするが，WAN回線及びWANルータ，メールゲートウェイなどサービスの一部として提供される機器などについては，宮内庁統合NW事業者にて運用，保守を行うこととする。また，併せて最終的に次期運用管理事業者（宮内庁CIS受託者）にて運用を行う機器であっても次期運用管理事業者（宮内庁CIS受託者）に運用を引継ぎするまでの暫定運用管理期間中については宮内庁統合NW事業者にて運用を行う。
※2	平成31年度「宮内庁ネットワークシステムの運用管理支援業務」の受託事業者で，宮内庁に常駐している（夜間，休日を除く。）。契約期間は2020年1月31日まで。
※3	以下，全て保守対応時の内容となる。 ユーザによるネットワーク機器（本庁を除く）の物理的な入れ替え作業を行うことを可能とするが，その作業範囲は既設ネットワーク機器に接続されているケーブルを，交換用ネットワーク機器の同じ位置に接続し，電源のON/OFFまでとする。そのため，ユーザの実施を支援するよう分かりやすい内容で手順書を作成すること。また，職員によるネットワーク機器の物理的な入れ替え作業の前に，センドバック保守による交換用ネットワーク機器の送付先は，交換対象となる現地ではなく，情報管理室とする。情報管理室にて受領した交換用ネットワーク機器は，次期運用管理事業者（宮内庁CIS受託者）にて，あらかじめバックアップされていた設定情報（コンフィグ情報）を交換用ネットワーク機器に入れ，動作を確認した後，宮内庁の負担で現地へ送付する。同時に現地職員へ交換に関する手順書を送付し，交換の依頼を行う。 なお，本庁に設置されたネットワーク機器の物理的な入れ替え作業は，次期運用管理事業者（宮内庁CIS受託者）にて実施する。
※4	甲は現行機器74個の買取を平成30年中に行っている。そのため，本調達では現行機器の予備機としての位置づけで調達すること。ただし納入時に，予備機との交換時に必要となる設定の洗い出し及び手順書を配備し，正常に動作するかのテストは行うこと。
※5	各現行システムの設計に関する変更が必要となる場合は，甲を介して設計変更が必要となる各現行システムの受託事業者と必要な調整を行った上で，次期宮内庁NWS全体が正常に稼働し，かつユーザの業務に支障がないような設計に基づく設定変更の内容（変更前と変更後の差分等）を明らかにし，甲の承諾を得た後，宮内庁統合NW事業者の責任と負担において具体的な設定変更の作業を行うこと。ただし，設定変更が必要となる日の10日（休日を除く。）前までに宮内庁統合NW事業者が作業内容（設定，手順等）について文書にて甲へ具体的に説明した上で，通常の保守業務又は運用管理業務の範囲内の作業と認められる場合には，甲を介し，甲の指示として当該作業を関係事業者に通常業務として依頼することができる。
※6	本調達と並行し，甲の負担と責任において，次に示す標的型攻撃対策システムの設計変更の調達を行う。甲は，宮内庁統合NW事業者と協議を行いつつ，標的型攻撃対策システムと本調達とのインタフェース及び接続方法を整理して明らかにし，甲の求めに応じて標的型攻撃対策システムの構築・保守事業者へ標的型攻撃対策システムの設計変更を実施させるものとする。標的型攻撃対策システムの設計変更に伴う作業等の標的型攻撃対策システムの構築・保守事業者への費用は甲が負担する。本調達の提案者は，次に示す標的型攻撃対策システムの設計変更の内容を十分に理解した上で，統合SOCサービスが適切に機能し，ユーザが適切にインターネット接続及びメール送受信が可能となるような提案を行うこと。

運用・保守のフロー


宮内庁
ユーザ
全体管理組織(PMO)
運用管理支援業者（情報管理室）
インシデント管理
サービスデスク
変更管理
記録管理(ナレッジ)
運用管理ツール等での記録
各保守事業者
通知・問合せ
通知・問合せ
必要に応じて業務上の影響を確認（重要度、緊急度）
[確認結果]
宮内庁担当者，運用管理支援業者，各保守業者が参集し，適宜協議の上，以降の対応方針を決定し，解決にあたる
[YES]
対応内容実施の可否の判定
対応内容の確認
[NO]
[確認依頼]
終了判定
[NO]
[YES]
報告・回答を受領
真の問題が別にあると想定されるか？（協議：宮内庁と運用管理支援業者）
[YES]
1
[NO]
カテゴリと優先度付け
識別と記録
インシデントか問合せかの判定
[インシデント]
[確認依頼]
影響分析
重大か？影響大か？
[NO]
[YES]
調査と診断
既知か？未知か？の判定
[既知]
[未知]
対応内容の報告
既知のエラーへの対応の検討
報告
対応内容の実施
[NO]
解決したか？
[YES]
報告・回答をまとめる
[問合せ]
ヘルプデスク
ユーザへの回答
記録又は連絡
必要に応じて各保守業者への連絡
記録及び問題解決依頼
1
対応結果の記録
運用管理会議の報告書や対応管理表等への記録
必要に応じて内容の確認
問題管理
根本原因の特定
問題解決方法の確立
問題解決方法の実施
問題解決したか確認
報告・回答をまとめる
報告

問題管理とインシデント管理の違い

問題管理の目的

インシデントの根本原因の除去とワークアラウンドの提供によって、インシデント発生による業務への悪影響を最小化する。

より本質的な解決であるため、保守事業者

運用管理支援事業者、職員（情報係）

問題	問題管理	インシデント	インシデント管理
虫歯	歯医者での虫歯の治療	虫歯が痛くて食べ物が食べられない	鎮痛剤で一時しのぎする
ディスクのオバーフロー	オーバーフローしないような処置（ファームウェアの改良等）を施す	ディスクを利用しているサービスが停止する	ディスクが搭載された装置をリブート/リセットする
アプリケーションのバグ	バグを発生させているソースコードの当該箇所を改修する	文字化けをおこし、業務上の支障が生じる	文字コード変換ツールなどを用いて可読文字に変換する

根本原因を特定し、それを低減又は除去するための活動やワークアラウンドの調査・検証の結果、根本的な解決を図るための本質的な解決方法が見つかっているものは、「既知のエラー/誤り」となる。

インシデント管理と問題管理は、同じ問題を端緒とする解決プロセスであっても、暫定的な処置でも構わないインシデント管理での解決と、本質的な解決を目指す問題管理での解決では、異なる。
インシデント管理では、暫定的な処置であっても、サービスが復旧すれば解決とみなされる。
問題管理の場合、根本原因が除去され再発の可能性がなくなったとき、初めて解決したことになる。

【別添2】

宮内庁共通基盤システムの整備・保守及び宮内庁 NWS の運用管理業務に係る民間競争入札

総合評価基準書

宮 内 庁

本書は，宮内庁が調達する「宮内庁共通基盤システムの整備・保守及び宮内庁NWS の運用管理業務」に係る評価基準を取りまとめた総合評価基準書である。評価の方法及び提案内容の評価基準について以下に記す。

◎前提事項

評価基準書の必須項目を満たさない提案は【不合格】とし，審査は行わない。

1．総合評価（加点方式）

総合評価（加点方式）は，提案内容を評価した技術点と入札価格の得点（価格点。入札価格を予定価格で除した値を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）の合計で得た数値の最も高い者を，落札者とする。

なお，技術点と価格点の比率は1：1とする。

技術点（満点 4,000 点） ＋ 価格点（満点 4,000 点） ＝ 総合評価点（満点 8,000 点）

上記総合点が高いものが2社以上となった場合は，技術点の高いものを落札者とする。

2．技術点の評価方法

技術点は「基礎点（仕様準拠に対する得点）」と「加点（付加価値提案に対する得点）」を算出した後，以下の算式により決定する。

基礎点（500 点） ＋ 加点（満点 3,500 点） ＝ 技術点（満点 4,000 点）

(1) 基礎点項目に対する評価

別紙「評価基準表」で必須とした要求要件を設定したものであり，すべて満たしているか否かを確認し，満たしている場合は「合格」とし「基礎点」を与える。

なお，本調達では，提案書に具体的かつ明確に記述されていることが必要であり，文章による意思表現だけにとどまる場合には，「不合格」とすることがある。

(2) 加点項目に対する評価

2の(1)によって「合格」となった提案書に対し，以下により評価を行う。

ア 別紙「評価基準表」の「評価点」欄に加点点数を示している項目について

評価する。

イ 別紙「評価基準表」における各評価項目の評価基準の内容に基づき，表１のとおり評価を行う。

表１：評価基準

評価	基準
特に優秀	提案内容が特に優れている。
優　秀	提案内容が優れている。
標　準	提案内容が標準的である。
加点なし	要件は満たしているが，加点すべき要素がない。

３．配点方針

(1)　技術点の配点方針

技術点は，表２のとおり配点を設定するものとする。各評価項目における配点・評価基準については，別紙「評価基準表」を参照。

表２：配点方針

評価	最大加点		
	４０	１００	２００
特に優秀	４０	１００	２００
優　秀	２０	５０	１００
標　準	１０	２５	５０
加点なし	０	０	０

(2)　女性の活躍推進に向けた公共調達に関する取組指針に基づく配点方針

「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 9 月 4 日法律第 64 号（以下「女性活躍推進法」という。））及び「女性の活躍推進に向けた公共調達及び補助金の活用に関する取組指針について」（平成 28 年 3 月 22 日すべての女性が輝く社会づくり本部決定（以下，「取組指針」という。））に基づき，ワーク・ライフ・バランスを推進する企業として法令に基づく認定を受けた企業その他これに準ずる企業（以下「ワーク・ライフ・バ

ランス等推進企業」という。）を評価する項目を以下のとおり設定する。

表３：配点方針

評価項目	認定等の区分※1		配点
ワーク・ライフ・バランス等の推進に関する指標	女性活躍推進法に基づく認定（えるぼし認定企業）	1段階目 ※2	40
		2段階目 ※2	80
		3段階目	120
		行動計画 ※3	20
	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）	くるみん	40
		プラチナくるみん	80
	若者雇用促進法に基づく設定（ユースエール認定企業）		80

※１　複数の認定等が該当する場合，最も配点が高い区分により加点。

※２　「労働時間等の働き方」に係る基準は満たすことが必要。

※３　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。）。

評 価 基 準 表

【別紙】

評価対象	必須	加点	加点評価 特に優秀	加点評価 優秀	加点評価 標準	加点評価 加点なし	評価基準
1. 一般的事項							
1.1 件名							
1.4 背景と目的							
甲は，行政事務を行う上で必要となる文書作成，情報伝達等の基盤として宮内庁NWSをこれまで整備し，運用を行ってきた。宮内庁NWSは，宮内庁LANと宮内庁WANとで構成されており，一府省庁一ネットワークの体制になっている。また，インターネット接続回線サービスを本庁だけに集約し，各拠点は，WANを介してインターネット接続を行っている。 甲は，「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（平成30年6月15日　閣議決定）（以下「創造宣言」という。）」において「平成30 年度までにシステム数の半減（平成24 年度（1450 システム）比），平成33 年度を目途に運用コストの3割削減（平成25 年度（約4000億円）比）を目指すため，引き続き達成に向けた取組を着実に実施」すること等が目標として掲げられていることを踏まえ，これまで，宮内庁本庁サーバ及び地方サーバ（正倉院事務所，御料牧場，京都事務所に設置されている）（以下「地方サーバ」という。）の集約化を始め，情報システム構成及び運用の効率化・合理化を図るとともに，安全性，信頼性及び可用性並びに柔軟性が確保されたネットワーク環境を構築するにあたり，機器・ソフトウェア等を刷新し，ネットワークの再構築と高速化を推進してきた。また，「デジタル・ガバメント実行計画（平成30年7月20日改定　デジタル・ガバメント閣僚会議決定）」においてマネジメント及びプロセスの強化として，政府情報システム改革の着実な推進，情報利活用と情報セキュリティの一体的推進，標準ガイドライン群の充実・拡充・定着が求められている。宮内庁においては，デジタル・ガバメント実行計画に基づき，「宮内庁デジタル・ガバメント中長期計画（平成30年6月22日　行政情報化推進委員会決定）」を策定した。 本調達では，これまでのそれらの取り組みを踏まえ，次の事項を更に推進し，宮内庁デジタル・ガバメント中長期計画の着実な実施を目的とする。 (1) 情報セキュリティ対策の更なる向上 (2) 情報システムの運用コストの削減 (3) 情報システムにおけるユーザの利便性の向上 (4) 情報システム構成及び運用の効率化・合理化 (5) 業務継続性の向上 さらに本調達では，現行までの宮内庁NWSの構築・保守業務と運用管理業務を分離してきたことをやめ，日常的に利用する基盤サーバ群の運用管理業務と次期宮内庁NWSの中核となる宮内庁共通基盤システム（以下「宮内庁CIS」（Common Infrastructure System）という。）の構築・保守業務の一体的な作業による効率化だけでなく，情報セキュリティインシデント及び情報システム障害対応の迅速化によって，利用者であるユーザの業務への影響，とりわけ情報システムを正常に利用できないことによる業務遅延などを最小化し，構築・保守業務と運用管理業務を一体的に行い，より効果的なITマネジメントを図ることを目指す。そのため，本調達では，宮内庁CISの構築・保守だけでなく，競争の導入による公共サービスの改革に関する法律（以下「公共サービス改革法」という。）及び公共サービス改革基本方針の趣旨・目的に基づいた次期宮内庁NWSの運用管理業務の調達を含めるため，官民競争入札・民間競争入札（いわゆる市場化テスト）を活用し，次期宮内庁NWSの運用管理業務の実施については，「宮内庁共通基盤システムの整備・保守及び次期宮内庁NWSの運用管理業務に係る民間競争入札実施要項（以下「実施要項」という。）」を基本とする。また，公共サービス改革法の第1条に基づき，民間事業者の創意と工夫を活用することにより，より良質かつ低廉な次期宮内庁NWSの運用管理業務を実現し，ITガバナンス及び情報セキュリティガバナンスの強化を図るとともに，継続的改善活動（PDSAサイクル）の徹底により，内的要因（ユーザニーズ）や外的要因（サイバー攻撃）が変化した場合でも，それらに柔軟に対応し，適切なサービスを継続的に提供することが本調達の第二の目的となる。本調達仕様書は，甲が受注者となる民間事業者に請け負わせる，次期宮内庁NWSの運用管理業務について適用する。	必須						左記の内容を理解しているか。
1.5 宮内庁における情報システムの概要							
1.5.1.宮内庁における情報システム等							
甲が利用する情報システム等について，以下のとおり示す。応札者は，以下について十分に把握し，必要ならば，甲担当者への確認を行うか，「13.資料閲覧」時に確認するなどし，宮内庁における情報システムとその利用実態について十分な理解に努めた上で，本調達の二つの目的を達成する提案を行うこと。 【情報システム一覧表の記載は省略】	必須						本調達の目的を十分に理解しているか。
		加点	200	100	50	0	本調達の目的を十分理解した上で，具体的で有効かつ妥当性のある提案があれば，加点として評価する。
1.5.2.宮内庁NWSの概要							
現在，宮内庁NWSは，甲が業務を遂行するために使用する，甲の各拠点等に設置された情報通信機器等とそれらを繋ぐネットワークにより構成され，宮内庁LAN，宮内庁WANとインターネット接続回線サービス，グループウェア，クライアント端末及びプリンタ等に大きく分類され，本調達仕様書（案）「1.5.1.宮内庁における情報システム等」の(1)に示した表中のとおりである。また，ネットワーク機器を設置している主な拠点は次のとおりである。 なお，御移居に伴い該当施設の名称が変更となる可能性があるので留意すること。 (1)　宮内庁本庁 ①　本庁サーバ室（本庁舎内） ②　各課室19インチラック内 ③　各課室（本庁舎内と本庁舎以外の御所，書陵部，三の丸尚蔵館を含む） (2)　東宮御所 ①　東宮御所内サーバ室 ②　各課室 (3)　宮邸 ①　秋篠宮邸 ②　常陸宮邸 ③　三笠宮邸 ④　三笠宮東邸 ⑤　高円宮邸 (4)　その他 　高輪皇族邸 (5)　御用邸 ①　那須御用邸管理事務所 ②　須崎御用邸管理事務所 ③　葉山御用邸管理事務所 (6)　陵墓監区事務所 ①　多摩陵墓監区事務所 ②　桃山陵墓監区事務所 ③　月輪陵墓監区事務所 ④　畝傍陵墓監区事務所 ⑤　古市陵墓監区事務所 (7)　京都事務所 ①　京都事務所内サーバ室 ②　各課室 (8)　正倉院事務所 ①　正倉院事務所内サーバ室 ②　各課室 (9)　御料牧場 ①　御料牧場内サーバ室 ②　各課室 宮内庁NWSにおいては，ユーザ管理機能，グループウェア（電子メール機能，スケジュール機能等），標的型攻撃対策を中心としたネットワーク情報セキュリティ対策機能などのネットワーク情報サービスが提供されている。 次期宮内庁NWSの中核である本調達は，ユーザが業務を遂行する上で重要な基盤となるが，操作性の向上など業務の更なる効率化と利用状況の向上，並びに近年，「標的型メール」攻撃を始めとする不正アクセスやウイルス感染による情報漏えいのリスク・脅威は増大していることから，情報セキュリティ対策の更なる向上を目的の一つとしてシステムの更改並びに見直しを実施するものである。 なお，別途調達される宮内庁統合NWでは，ネットワークに関する部分，現行宮内庁LANのネットワーク部分，現行宮内庁WAN及び現行インターネット接続回線サービスを同一調達内で行い，さらにその調達内で新たに統合SOCサービスを加えてネットワーク全体でのシームレスな情報セキュリティ対策の強化を図ることとなる。 また，宮内庁WANの回線は，平成26年度の「宮内庁WANの通信回線サービスの調達仕様書」に基づく調達において，それ以前までメタル回線であった地方拠点（ただし，高野山部，吉野部，掖上部を除く），正倉院事務所や御料牧場などでの光回線化を行い，ネットワークの帯域幅増加による高速化と電磁ノイズ対策強化による安定化を図ったことから，クライアント端末上のソフトウェアのパッチの配信やリモートでの運用管理などが効率的に行うことができるようになった。現行の宮内庁WANの回線種別を別紙2に示す。ただし，宮内庁WANは，本調達の公示時点では宮内庁統合NWの一部として構築中であるため，本調達の応札者は，提案に際して甲に確認すること。	必須						左記の構成を理解しているか。
1.5.3.運用管理業務の軽減に関するこれまでの主な取組							
甲が取り組み，実現してきた宮内庁NWSの運用管理業務の効率化について，次のとおり示す。応札者は，次について十分に把握し，必要ならば，甲担当者への確認を行うか，「13.資料閲覧」時に確認するなどし，宮内庁における情報システムについて十分な理解に努めた上で，より一層の宮内庁NWSの運用管理業務の効率化に資する提案を行うこと。	必須						これまでの運用管理業務の効率化について理解しているか。
		加点	200	100	50	0	宮内庁における情報システムについて十分に理解し，より一層の宮内庁NWSの運用管理業務の効率化に資する具体的な提案があれば加点とする。
1.6.作業内容							
1.6.1.調達範囲							
本調達における主な調達区分は次のとおりとなる。各調達の詳細な範囲は次項以降を参照すること。 (1) 統括管理 本業務全体に係る作業実施計画作成，体制整備，進捗管理及び課題管理等を行う。	必須						本調達における区分を理解しているか。
(2)設計 調達仕様書，提案書及び各種ドキュメントに基づき，宮内庁LAN基盤サーバ群等の機器に関する設計，移行業務及び運用管理業務の計画作成等を行う。 宮内庁統合NWでなされた全体ネットワーク設計方針を前提とし，調達仕様書，提案書及び各種ドキュメントに基づき，宮内庁LAN 基盤サーバ群等の機器に関する設計，移行業務及び運用管理業務の計画作成等を行う。設計に当たっては，宮内庁統合NW側の方針を精読し，設計方針に則って必要な作業を実施する。	必須						
(3)構築 各種設計書及びドキュメントに基づき，機器等について，稼働に必要なソフトウェアのインストールや設定等を実施して指定の場所に搬入し，設置調整等の構築作業を行い，必要十分な機能を確実に動作させる。	必須						
(4)テスト 各種テストの計画書を作成し，テストを実施する。 なお，甲担当者が主体となって実施する受入テストの支援を行う。	必須						
(5)移行 各種設計書及び移行実施計画書に基づき，現行システムから次期システムへの移行を行い，宮内庁NWSを用いたユーザの業務の継続性を保つ。	必須						
(6)保守 宮内庁LAN等の機器障害発生時における連絡調整，障害機器等への対応及び保守業務結果に関する報告等を行う。	必須						
(7)運用管理業務 運用管理に係る手順書の整備，各種管理，定例会議での報告，機器等変動に関する支援，計画停電対応及びヘルプデスク業務等を行う。運用管理業務は，日々の運用の中で，ユーザの異動，情報セキュリティ対策の導入などの要因に基づく宮内庁NWSの変更管理が軸となる。	必須						
1.6.2.現行宮内庁NWS構成							
以下に現状の宮内庁NWSの構成及び，機器の更改範囲について示す。 詳細な現状構成については，閲覧資料を参照の上，詳細なシステム構成を把握すること。 【図は省略】 上に示す機器更改範囲を対象として，必要な機器群の更改を行うとともに，機器更改対象範囲ではない部分においても，移行期間中及び次期宮内庁NWS全体が正常に動作するように本受託者は適切な設計を行うこと。また，更改に当たって連携する周辺システムへの設計に関する変更が必要となる場合は，受託者の負担の下，次期宮内庁NWS全体が正常に稼働するよう作業を行うこと。 IPアドレス設計，セグメント設計，通信フロー設計，バックアップ設計など宮内庁ネットワークシステムとして統一的な設計及び運用が求められる事項については，本調達仕様書（案）で定める会議体又は甲を通じて宮内庁統合NW受託者と協議を行った上で進めていくこと。	必須						現状の宮内庁NWSの構成及び機器の更改範囲を理解しているか。
1.6.3.次期宮内庁NWS概要							

評価対象	必須	加点	加点評価 特に優秀	加点評価 優秀	加点評価 標準	加点評価 加点なし	評価基準
次期宮内庁NWSについてのシステム構成の全体概要は次のとおり。 【概要図の記載は省略】 次期宮内庁NWSにおける現行システムとの主要な変更点は次のとおりとなる。 (1) 特権ID管理機能の導入 (2) ログ収集機能サーバの導入 (3) 振る舞いログ分析(UEBA)サーバの導入	必須						次期宮内庁NWSについてのシステム構成の全体概要を理解しているか。
1.6.4.スケジュール(案)							
乙は次のスケジュール(案)を参考にし，各作業におけるWBSのクリティカルパスを明確にした上で，遅延なきよう各作業の進め方を工夫すること。また，宮内庁CISの構築は，宮内庁統合NWの構築期間と並行して行われるが，本調達の目的を達成するため，宮内庁NWS全体として機能するよう双方で協力しながら設計・構築を行うこと。本調達の各作業内容については，次項を参照すること。 ※表の記載は省略。	必須						スケジュールを理解しているか。
1.6.5.作業内容及び各事業者との役割範囲							
本受託にて実施する作業内容について記載する。 現行各システム事業者，次期運用管理事業者(宮内庁CIS受託者)，運用管理支援事業者及び各事業者等との役割分担については，別紙4を参照すること。作業及びシステム実装に求められる各要件については「3.システム要件」に記載されている詳細な要件を参照のこと。	必須						作業内容及び役割範囲を理解しているか。
1.7.契約期間							
(1) 設計・構築業務 契約締結日から2020年1月31日まで (2) 運用管理・保守業務 2020年2月1日から2024年1月31日までの48か月 なお，契約期間終了後に，再賃貸借又は買取をする場合がある。	必須						契約期間を理解しているか。
1.8.納入							
(1) 納入は，甲担当者の指示を受けてから行うこととし，乙側責任者は，作業開始の連絡及び作業終了の報告の上，確認を受けること。 (2) 納入時は，既設建物，特に室内の床板，敷物及びカーテン等の室内装飾を汚損又は破損しないように細心の注意を払うこと。 (3) 納入時に生じた梱包箱等不要物は適切に処分すること。 (4) 別途配線等工事が必要な場合は，事前に甲担当者の了承を受け，乙の負担で実施すること。 (5) 甲及び関係事業者との調整で発生する費用は，乙の負担で実施すること。	必須						納入に係る条件を理解した上で実施できるか。
1.8.1.納入条件							
(1) 本調達仕様書(案)に明示された機能，性能及びその他の条件を全て満たしていること。 (2) 提供予定の内容を示したネットワーク図(様式適宜)，機器類明細書を提出すること。 (3) 本調達仕様書(案)に記載している事項及びそれらに付随して発生する費用を全て負担すること。乙は本調達で導入する機器の設計・構築，インストール・アンインストール及び環境設定，現行データの移行，動作確認・テストを納入期限までに完了の上設置し，契約開始日から完全に利用可能な状態にし，サービスを開始できる体制とすること。 なお，サービス利用開始日において全部又は一部が利用できない場合は，代替措置を乙の責任と負担で提供すること。 (4) 搬入，据付，配線，調整，既設設備との接続に要する全ての費用及び契約期間中の保守費用は，本調達に含まれる。 (5) 機器等については，原則，「国等による環境物品等の調達の推進等に関する法律(グリーン購入法)に基づく「環境物品等の調達の推進に関する基本方針(平成30年2月9日変更閣議決定)」に規定された製品については判断基準を満たすものとすること。 (6) 本調達が正常に稼働するために必要となる機器及び役務等については，甲担当者に報告の上，乙の責任において供給，実施すること。 (7) その他，納入に関する不明な点は甲乙協議の上，実施すること。	必須						納入に係る条件を理解した上で実施できるか。
1.8.2.納入期限							
2020年1月31日	必須						納入期限を守れるか。
		加点	200	100	50	0	本件を期限内に円滑に完了させるための施策が具体的に記載され，かつ妥当性のある内容である場合には，加点として評価する。
1.8.3.納入場所							
支出負担行為担当官の指定する場所(「別紙2宮内庁NW設置拠点・設置場所等」参照)	必須						「別紙2宮内庁NW設置拠点・設置場所等」を理解し納入場所を把握できているか。
1.8.4.納入検査							
納入検査は，乙側責任者及び甲担当者立会いの上行い，不合格品の生じた場合には，新規取替え等甲担当者の指示に基づき必要な処置をとること。	必須						不合格品の生じた際の対応を理解しているか。
1.9.納入後に求める環境配慮(温室効果ガスの排出抑制のための取組要件)							
本調達に際して，「宮内庁環境配慮の方針」(平成19年3月14日宮内庁環境配慮の方針推進委員会決定)の内，「2. (2)③温室効果ガスの排出抑制のための取組」について，助言等を行うこと。 (参考)宮内庁の環境配慮について http://www.kunaicho.go.jp/kunaicho/shiryo/kankyo/kankyou-hairyo.html	必須						「宮内庁環境配慮の方針」を理解の上，助言等を行っているか。
		加点	100	50	25	0	機器の性能以外の部分での，温室効果ガスの排出抑制のための取組について，具体的に記載され，かつ妥当性のある内容である場合には，加点として評価する。
1.10.保証							
現場に搬入・設置等，搬入過程における傷・損傷等及び納入検査後に発覚した初期不良やユーザによる故意ではない見え隠れする部分の不具合等については，乙は直ちに新規取替え又は補修を行い，納入後1年間の保証義務を負うこと。 なお，それ以上の保証期間の明記があるものは，その期間の保証義務を負うこと。	必須						保証義務について，理解しているか。
1.11.成果物							
本調達の成果物は，次の表のとおり実施前又は実施後に甲担当者に提出すること。 次の表に明記のない，各成果物の詳細な内容や提出期限は，甲担当者と協議の上決定すること。 成果物の形態は，次のとおりとする。 (1) 成果物は，主として日本語表記とすること。 (2) 情報処理に関する用語の表記は，JISの規定に従うこと。 (3) 成果物は，紙媒体及び電磁的記録媒体(以下「電子媒体」という。)により作成し，2部提出すること。紙媒体はファイル等にまとめ，各項目にはインデックスを貼付すること。 (4) 電子媒体は，甲担当者の端末にて読み取り可能な形式(マイクロソフト社のWord2016，Excel2016，PowerPoint2016並びにAdobe社のAcrobatReaderDCを標準)で電子媒体(CD-R又はDVD-R等)に納め，2部提出すること。 (5) 成果物に修正等があった場合，紙媒体は，更新履歴と修正ページ，電子媒体は，更新履歴と修正後の全編を速やかに提出すること。 (6) 納品後，甲担当者において改変が可能となるよう，図表等の元データも併せて編集可能な形式で提出すること。 【表の記載は省略】	必須						成果物の提出について，理解しているか。
		加点	40	20	10	0	成果物を継続的に利用・管理していくに当たって次のような具体的で有用な提案があれば，加点として評価する。 ・成果物の修正等があった際，改めた当該部分を単に提出するのではなく，紙媒体としてファイルに綴ってある成果物から当該部分を抜き出し，乙が直接差し替える。ただし，この差し替え前後に甲担当者の承諾を得ること。 ・成果物の文書について，見やすさ・使いやすさを考慮した具体的な工夫を施す。
1.12.契約期間終了後の引取り							
(1) 契約期間終了後の機器等の引取りは，全て乙の責任と負担において実施するものとする。また，実施に当たり甲及び関係事業者との調整に伴い発生する費用は，乙が負担すること。 (2) 機器等の引取りは，甲担当者の指示により行い，乙側責任者は，作業の開始及び終了時に甲担当者に報告の上，確認を受けてから行うこと。その際，既設建物，特に室内の床板，敷物及びカーテン等の室内装飾を汚損又は破損しないように細心の注意を持って行うこと。引取り時に生じた梱包箱等不要物は適切に処分すること。 (3) 機器等の引取りの際は，搭載されているHDD等の補助記録装置内の情報が残らない(復元を不可能とする)措置を宮内庁庁舎内で講ずること。対応できないことがある場合は，事前にこの根拠を明確にした文書を作成し，甲と協議の上で承諾を受けた後，適切な対応を行うこと。 なお，データ消去作業後は，データ消去証明書を作成し，甲担当者の承諾を得ること。	必須						契約期間終了後の引取りについて，理解しているか。
1.13.指示等の書面主義							
本調達の具体的な指示，報告，申出，質問，回答及び協議等は，原則文書で行う。ただし，緊急又はやむを得ない場合は口頭で行うことができるが，事後必ずその内容を記した文書を取り交わすこと。	必須						左記ついて，理解した上で対応できるか。
1.14.役務作業要件							
(1) 乙は，契約開始日までに事前準備として必要なハードウェア及びソフトウェアは乙の負担で準備すること。	必須						左記ついて，理解した上で対応できるか。
(2) 乙は，本業務の事前稼働検証，機器等の導入・設置，設計・構築・各種ソフトウェアのインストール及び環境設定，動作確認，現行のデータ移行手順書等の作成及び教育等を行うに当たり，当該各作業の実施前には，十分な時間的余裕をもって甲と調整し，各作業工程表を提出し，甲の承諾を得ること。	必須						
(3) 本業務の実施に当たり，各現行システムの業務に影響を与えないこと。また，ユーザ端末のデータ移行・切替えに当たり，ユーザの負担を軽減する方策を検討すること。	必須						
(4) 本業務の実施に当たり，関係事業者の協力を得る必要がある場合は，協力が必要となる日の原則10日(休日を除く。)前までに乙が文書にて甲へ具体的に説明して甲の承諾を得た上で，甲及び関係事業者と協議して合意を得ること。合意を得た場合には，原則として，乙の負担において関係事業者から協力を得ること。	必須						
(5) 本業務の実施に当たり，関係事業者の協力を得る必要がある場合は，協力が必要となる日の原則10日(休日を除く。)前までに乙が文書にて甲へ具体的に説明して甲の承諾を得た上で，甲及び関係事業者と協議して合意を得ること。合意を得た場合には，原則として，乙の負担において関係事業者から協力を得ること。	必須						
(6) 本業務の実施に当たり，乙は，業務全般を掌握し，かつ，本業務を指揮監督する業務管理責任者及びこれを補佐する者(以下「業務管理責任者等」という。)を選任し，業務管理責任者等の資格，経験及び国籍を証明する文書を提出の上，契約日から起算して5日(休日を除く。)以内に甲の承諾を得ること。 なお，業務管理責任者等を変更する場合は，原則として変更予定日の10日(休日を除く。)前までに前述の資格等証明文書を提出の上，甲の承諾を得ること。	必須						
(7) 業務管理責任者等は，業務の進捗状況全体を把握し，甲に対して内容及び結果を定期的に報告すると共に各工程の終了時には，その結果報告を提出し甲の承諾を得ること。また，甲からの本業務等に関する問合せに対しては，問合せを行った日から起算して原則2日(休日を除く。)以内に回答すること。ただし，甲が問合せ時に回答期限を設定した場合には，これに従うこと。	必須						
(8) 甲から乙に対する指示，協議申し出は，業務管理責任者等を通じて行うものとする。	必須						
(9) 本業務の実施に当たり，乙の故意又は過失により稼働中の各現行システムに対して不具合や問題を生じさせた場合は，乙の責任と負担において適切に対処し，正常化すること。	必須						
(10) ユーザの作業が発生する場合は，作業が必要となる日の10日(休日を除く。)前までに乙が作業内容について文書にて甲へ具体的に説明して協議の上，承諾を得ること。	必須						

評価対象	必須	加点	加点評価 特に優秀	加点評価 優秀	加点評価 標準	加点評価 加点なし	評価基準
(11) 本システムの導入日は，原則として，平日の業務時間（8:30～17:45）に実施すること。ただし，サーバ等各現行システムに影響を与える作業の場合は，ユーザの業務が停止しないよう，原則として，休日又は平日の業務時間（8:30～17:45）以外を利用し，実施すること。	必須						左記ついて，理解した上で対応できるか。
(12) 本業務に当たり，現行環境の設定変更，ソフトウェアのインストール・アンインストールが必要となる場合には，関係事業者への設計・設定変更依頼書にて甲及び関係事業者に依頼すること。	必須						
(13) (12)の作業に伴い，本調達以外の機器が必要な場合は，乙の責任と負担において適切な情報セキュリティ対策を機器に対して施した上で安全に導入すること。	必須						
(14) 本業務の実施に当たり，納入する機器等は，本調達仕様書（案）を満たす増設機器（メモリ（以下「主記憶装置」という。）及びハードディスク等（以下「補助記憶装置等」））を全て取り付けた形で，正常動作の確認を行った上で納入すること。	必須						
(15) 本業務の実施に当たり，導入する宮内庁CISの動作が正常であることを確認すること。	必須						
(16) 本業務を遂行するに当たり，宮内庁CISで新規に導入した機器等に必要な情報（政府共通NWやインターネット等を介して利用するユーザの宮内庁NWのシステム環境等）は，本業務の契約締結後に甲担当者より提示する。	必須						
(17) 乙は，マルチベンダ構成により調達を行う場合，納入及び運用を確実に実現するため，事前に関係事業者との間で必要な書類等を取り交わす等，十分な合意を得るとともに，その実施のための体制を整備した計画を作成し，甲に提出し，承諾を得ること。	必須						
(18) 関係事業者の各種調整などで生じた作業は，あらかじめ甲の承諾を得た上で乙の責任と負担において実施することとし，本業務に当たり，その調整等による不都合，負荷などができる限り発生しないようにすること。	必須						
(19) 機器の設定ファイル等は，一般的なテキスト・エディタ等での可読なファイルフォーマットで保存の上，時系列での保守ができるように構成管理し，変更があるときはその都度提出すること。	必須						
(20) 本調達機器等を甲が管理するための情報資産台帳に必要事項（ホスト名，IPアドレスなどのネットワーク設定の情報）を記入し，提出すること。 なお，IPアドレスの払い出しやネットワーク設定等は，甲を介して現行運用管理支援事業者及び宮内庁統合NWの保守・運用事業者と必要な調整を行い，甲の承諾を得た上で，乙の責任と負担において実施すること。	必須						
(21) 本調達機器に関しては，現行機器の設定情報等を提供するので，その設定情報を活用し，効率的な設計・設定を行うこと。	必須						
(22) 本業務は，次の標準ガイドライン群の各文書を十分に理解した上で，記載内容に準じて実施すること。 （参考）「デジタル・ガバメント推進標準ガイドライン」（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）に関連する指針類等に係る文書体系を以下「標準ガイドライン群」という。 https://cio.go.jp/guides	必須						

1.14.役務作業要件 【再掲】

(1) 乙は，契約開始日までに事前準備として必要なハードウェア及びソフトウェアは乙の負担で準備すること。							
(2) 乙は，本業務の事前稼働検証，機器等の導入・設置，設計・構築・各種ソフトウェアのインストール及び環境設定，動作確認，現行のデータ移行手順書等の作成及び教育等を行うに当たり，当該各作業の実施前には，十分な時間的余裕をもって甲と調整し，各作業工程表を提出し，甲の承諾を得ること。							
(3) 本業務の実施に当たり，各現行システムの業務に影響を与えないこと。また，ユーザ端末のデータ移行・切替えに当たり，ユーザの負担を軽減する方策を検討すること。							
(4) 本業務の実施に当たり，関係事業者の協力を得る必要がある場合は，協力が必要となる日の原則10日（休日を除く。）前までに乙が文書にて甲へ具体的に説明して甲の承諾を得た上で，甲及び関係事業者と協議して合意を得ること。合意を得た場合には，原則として，乙の負担において関係事業者から協力を得ること。							
(5) 本業務の実施に当たり，関係事業者の協力を得る必要がある場合は，協力が必要となる日の原則10日（休日を除く。）前までに乙が文書にて甲へ具体的に説明して甲の承諾を得た上で，甲及び関係事業者と協議して合意を得ること。合意を得た場合には，原則として，乙の負担において関係事業者から協力を得ること。							
(6) 本業務の実施に当たり，乙は，業務全般を掌握し，かつ，本業務を指揮監督する業務管理責任者及びこれを補佐する者(以下「業務管理責任者等」という。）を選任し，業務管理責任者等の資格，経験及び国籍を証明する文書を提出の上，契約日から起算して5日（休日を除く。）以内に甲の承諾を得ること。 なお，業務管理責任者等を変更する場合は，原則として変更予定日の10日（休日を除く。）前までに前述の資格等証明文書を提出の上，甲の承諾を得ること。							
(7) 業務管理責任者等は，業務の進捗状況全体を把握し，甲に対して内容及び結果を定期的に報告すると共に各工程の終了時には，その結果報告を提出し甲の承諾を得ること。また，甲からの本業務等に関する問合せに対しては，問合せを行った日から起算して原則2日（休日を除く。）以内に回答すること。ただし，甲が問合せ時に回答期限を設定した場合には，これに従うこと。							
(8) 甲から乙に対する指示，協議申し出は，業務管理責任者等を通じて行うものとする。							
(9) 本業務の実施に当たり，乙の故意又は過失により稼働中の各現行システムに対して不具合や問題を生じさせた場合は，乙の責任と負担において適切に対処し，正常化すること。							
(10) ユーザの作業が発生する場合は，作業が必要となる日の10日（休日を除く。）前までに乙が作業内容について文書にて甲へ具体的に説明して協議の上，承諾を得ること。							
(11) 本システムの導入日は，原則として，平日の業務時間（8:30～17:45）に実施すること。ただし，サーバ等各現行システムに影響を与える作業の場合は，ユーザの業務が停止しないよう，原則として，休日又は平日の業務時間（8:30～17:45）以外を利用し，実施すること。		加点	200	100	50	0	役務作業全般に関して，仕様書を踏まえて具体的に記載され，有効かつ妥当性のある内容である場合には，加点として評価する。
(12) 本業務に当たり，現行環境の設定変更，ソフトウェアのインストール・アンインストールが必要となる場合には，関係事業者への設計・設定変更依頼書にて甲及び関係事業者に依頼すること。							
(13) (12)の作業に伴い，本調達以外の機器が必要な場合は，乙の責任と負担において適切な情報セキュリティ対策を機器に対して施した上で安全に導入すること。							
(14) 本業務の実施に当たり，納入する機器等は，本調達仕様書（案）を満たす増設機器（メモリ（以下「主記憶装置」という。）及びハードディスク等（以下「補助記憶装置等」））を全て取り付けた形で，正常動作の確認を行った上で納入すること。							
(15) 本業務の実施に当たり，導入する宮内庁CISの動作が正常であることを確認すること。							
(16) 本業務を遂行するに当たり，宮内庁CISで新規に導入した機器等に必要な情報（政府共通NWやインターネット等を介して利用するユーザの宮内庁NWのシステム環境等）は，本業務の契約締結後に甲担当者より提示する。							
(17) 乙は，マルチベンダ構成により調達を行う場合，納入及び運用を確実に実現するため，事前に関係事業者との間で必要な書類等を取り交わす等，十分な合意を得るとともに，その実施のための体制を整備した計画を作成し，甲に提出し，承諾を得ること。							
(18) 関係事業者の各種調整などで生じた作業は，あらかじめ甲の承諾を得た上で乙の責任と負担において実施することとし，本業務に当たり，その調整等による不都合，負荷などができる限り発生しないようにすること。							
(19) 機器の設定ファイル等は，一般的なテキスト・エディタ等での可読なファイルフォーマットで保存の上，時系列での保守ができるように構成管理し，変更があるときはその都度提出すること。							
(20) 本調達機器等を甲が管理するための情報資産台帳に必要事項（ホスト名，IPアドレスなどのネットワーク設定の情報）を記入し，提出すること。 なお，IPアドレスの払い出しやネットワーク設定等は，甲を介して現行運用管理支援事業者及び宮内庁統合NWの保守・運用事業者と必要な調整を行い，甲の承諾を得た上で，乙の責任と負担において実施すること。							
(21) 本調達機器に関しては，現行機器の設定情報等を提供するので，その設定情報を活用し，効率的な設計・設定を行うこと。							
(22) 本業務は，次の標準ガイドライン群の各文書を十分に理解した上で，記載内容に準じて実施すること。 （参考）「デジタル・ガバメント推進標準ガイドライン」（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）に関連する指針類等に係る文書体系を以下「標準ガイドライン群」という。 https://cio.go.jp/guides							

1.15.情報セキュリティ対策

1.15.1.情報セキュリティの確保

情報セキュリティを確保するために応札者は以下の作業を実施することとし，発生する費用は本調達に含まれるものとする。また，その実施内容及び管理体制についてまとめた情報セキュリティ管理計画書を提出すること。	必須						
(1) 本業務の実施において，情報セキュリティを確保するための体制を整備すること。	必須						
(2) 秘密保持等のため次の項目を遵守すること。 ① 取り扱う情報は甲の情報処理業務にのみ使用し，他の目的には使用しないこと。 ② 取り扱う情報は甲の情報処理業務を行う者以外には秘密とすること。 ③ 取り扱う情報を甲の指定した場所から持ち出さないこと。 ④ 当該情報を甲の許可なく複製しないこと。 ⑤ 当該情報は，業務終了時に，返却，消去又は廃棄を確実に行うこと。	必須						
(3) 甲が定める「宮内庁情報セキュリティポリシー」を遵守すること。また，「政府機関の情報セキュリティ対策のための統一基準群（内閣サイバーセキュリティセンター）」の最新版を遵守すること。ただし，遵守のために別途，ソフトウェア又はハードウェアの機能やモジュール等の追加購入及びセットアップ作業が必要となる場合，又は現行システムに対する大幅な設計変更が必要となる場合には，必要となる費用の概算や作業内容等を可能な限り甲担当者へ提供し，甲担当者の検討に協力すること。	必須						
(4) 本調達においては，外部からの攻撃に対する情報セキュリティ対策のみでなく，内部での情報セキュリティ対策，外部の情報システムに対して悪影響を与えないための情報セキュリティ対策等，総合的な情報セキュリティ対策を講じること。	必須						左記ついて，理解した上で対応できるか。
(5) 総合的な情報セキュリティ対策を講じる上で，宮内庁統合NW，標的型攻撃対策システム，クライアント端末，資産管理サーバ，KMSサーバなどと連携して機能する対策については，連携する各システムの設計書や機器上の設定内容等を十分に確認し，理解すること。 なお，連携する各システムの機器上の設定の変更が必要となる場合には，甲を介して各システムの保守事業者，現行運用管理支援事業者と必要な調整を行い，設定変更の内容（変更前と変更後の差分等）を明らかにし，甲の承諾を得た上で，乙の責任と負担において具体的な設定変更の作業依頼書を作成すること。ただし，作業実施予定日の10日（休日を除く。）前までに乙が作業内容（設定，手順等）について文書にて甲へ具体的に説明した上で，通常の保守業務又は運用管理業務の範囲内の作業と認められる場合には，甲を介し，甲の指示として当該作業を関係事業者に通常業務として依頼することができる。	必須						
(6) 本調達システム内部への侵害拡大を防止するため，独立行政法人情報処理推進機構（以下「IPA」という。）の「『高度標的型攻撃』対策に向けたシステム設計ガイド」の最新版（以下「高度標的型攻撃対策ガイド」という。）のシステム設計対策セットを十分に理解した上で，各対策セットの適用を検討し，攻撃者が侵入しづらく，内部侵害拡大がしづらいシステム設計を行うこと。また，その設計内容を各機器等の設定に対して確実に反映し，機能させること。	必須						

評価対象	必須	加点	加点評価 特に優秀	加点評価 優秀	加点評価 標準	加点評価 加点なし	評価基準
(7) 高度標的型攻撃対策ガイドを十分に理解した上で，ネットワークの設計については，次の表で例示するネットワークセグメントの分離単位を基本とし，適切な設計を行うこと。ただし，現行宮内庁NWSにおいては，ハートビート・CSV（Cluster Shared Volume）用セグメント，ライブ・マイグレーション用セグメントもある。各セグメント間を行き来する通信は，原則不可とし，ユーザが利用する機能又は受けるサービスを滞りなく提供するために必要な通信などについては，必要最小限にするアクセス制御を施すこと。 なお，ネットワークセグメントの分離単位及びアクセス制御の設定内容については，あらかじめ甲と協議の上，決定すること。 【表の記載は省略】	必須						
(8) ユーザが利用する業務やアプリケーション，宮内庁CISのネットワークの制御及び運用などで不要な通信プロトコル，通信ポート，ソフトウェア上の機能又はサービスを明らかにしてから甲と協議し，甲の承諾を得た上で，停止やブロックするなどの不要な機能を利用不可とする設計を適切に行うこと。	必須						
(9) ネットワークスイッチ等のネットワーク機器は，前項(8)で示した不要機能を予め排除したOS又はファームウェアを採用し，ユーザの業務が滞りなく遂行でき，宮内庁CISのネットワークの制御及び運用などが適切に行うことが可能な必要最低限の機能が実装されたものとすること。	必須						
(10) 本調達で導入するHDD等の補助記憶装置を搭載する機器が，故障・障害等により乙が新規交換した場合，情報漏出防止のため，交換されたHDD等は甲が処分できること（本号を前提とした契約が可能であること）。 ただし，やむを得ない事情により交換されたHDD等の返却が必要な場合は，事前に甲の承諾を得た上で，甲の立ち会いの下，記録されているデータを完全に消去し，データ消去証明書を提出すること。	必須						
(11) 本調達における全ての機器に搭載されるオペレーティングシステム（以下「OS」という。）及びソフトウェアは，次の情報セキュリティに関する情報提供サイト等を参考にし，納入期限までに指摘されている脆弱性やセキュリティホール等に対して修正モジュールの導入など適切な処理を施し，安全なシステムの構築を行うこと。 ① NISCから発出される情報 https://twitter.com/nisc_forecast ② 警察庁から発出される情報 https://www.npa.go.jp/cyberpolice/ ③ IPAから発出される情報 http://www.ipa.go.jp/security/index.html http://jvndb.jvn.jp/index.html ④ JPCERT/CC から発出される情報 https://www.jpcert.or.jp/ ⑤ JC3 から発出される情報 https://www.jc3.or.jp/info/index.html	必須						
(12) 本調達で導入する機器のうち「ウイルス対策機能」を有することが機能要件に含まれる場合には，以下を満たすこと。 (ア) ウイルス対策ルール（又はパターンファイル）は，自動的に更新されること。 (イ) ウイルススキャンのエンジンは，サーバ機器とクライアントPCとでは異なる製造業者の製品を採用し，ウイルス対策ルール又はパターンファイルの公開時期のずれなどによる対策の遅れを吸収するため，多層型防御による情報セキュリティ対策の強化が可能なこと。 本調達で導入する機器のうち「ウイルス対策機能」を有することが機能要件に含まれる場合には，以下を満たすこと。 (ア) ウイルス対策ルール（又はパターンファイル）は，自動的に更新されること。 (イ) ウイルススキャンのエンジンは，サーバ機器とクライアントPCとでは異なる製造業者の製品を採用し，ウイルス対策ルール又はパターンファイルの公開時期のずれなどによる対策の遅れを吸収するため，多層型防御による情報セキュリティ対策の強化が可能なこと。	必須						左記ついて，理解した上で対応できるか。
(13) 本業務の実施に当たり，乙又はその従業員，本調達の役務内容の一部を請負等する先，もしくはその他の者により意図せざる変更が加えられないための管理体制が整備されていること。	必須						
(14) 乙の資本関係・役員等の情報，受注作業の実施場所に関する情報，受注業務の従事者の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績及び国籍に関する情報を提供すること。	必須						
(15) 乙は，受注業務の一部を請負等する場合は，あらかじめ情報セキュリティ管理計画書に相手方を含めた管理体制を記載の上，提出し，甲の承諾を受けること。また，再請負の相手方から更に第三者に請負が行われる場合においても同様とする。 なお，再委託先の変更等を行う必要が生じた場合は，情報セキュリティ管理計画書の該当部分を変更の上，甲に提出し，承諾を受けること。	必須						
(16) 情報セキュリティインシデントへの対処方法が確立されていること。	必須						
(17) 情報セキュリティ対策その他の契約の履行状況を定期的に確認し，甲へ報告すること。	必須						
(18) 乙の講ずる情報セキュリティ対策が甲の所有するポリシー等の基準を満たしていない場合には，乙は，甲と協議の上で追加的なセキュリティ対策を講ずること。	必須						
(19) 本調達に係る業務の遂行における情報セキュリティ対策の履行状況を確認するために，甲が情報セキュリティ監査の実施を必要と判断した場合は，甲がその実施内容（監査内容，対象範囲，実施等）を定めて，情報セキュリティ監査を行う（甲が選定した事業者による監査を含む。）。また，乙は自ら実施した外部監査についても甲へ報告すること。 情報セキュリティ監査の実施については，これらに記載した内容を上回る措置を講ずることを妨げるものではない。	必須						
(20) JPCERT/CC「攻撃者が悪用するWindowsコマンド(2015-12-02)」を参考にして，甲職員のクライアント端末に必要のないWindowsコマンドを，AppLockerやソフトウェア制限ポリシー等を使用して制限することで，攻撃者による悪用を低減すること。 https://www.jpcert.or.jp/magazine/acreport-wincommand.html 制限するコマンドの選定は，契約後，甲担当者と協議の上，決定する。	必須						

1.15.1.情報セキュリティの確保 【再掲】

情報セキュリティを確保するために応札者は以下の作業を実施することとし，発生する費用は本調達に含まれるものとする。また，その実施内容及び管理体制についてまとめた情報セキュリティ管理計画書を提出すること。							
(1) 本業務の実施において，情報セキュリティを確保するための体制を整備すること。							
(2) 秘密保持等のため次の項目を遵守すること。 ① 取り扱う情報は甲の情報処理業務にのみ使用し，他の目的には使用しないこと。 ② 取り扱う情報は甲の情報処理業務を行う者以外には秘密とすること。 ③ 取り扱う情報を甲の指定した場所から持ち出さないこと。 ④ 当該情報を甲の許可なく複製しないこと。 ⑤ 当該情報は，業務終了時に，返却，消去又は廃棄を確実に行うこと。							
(3) 甲が定める「宮内庁情報セキュリティポリシー」を遵守すること。また，「政府機関の情報セキュリティ対策のための統一基準群（内閣サイバーセキュリティセンター）」の最新版を遵守すること。ただし，遵守のために別途，ソフトウェア又はハードウェアの機能やモジュール等の追加購入及びセットアップ作業が必要となる場合，又は現行システムに対する大幅な設計変更が必要となる場合には，必要となる費用の概算や作業内容等を可能な限り甲担当者へ提供し，甲担当者の検討に協力すること。							
(4) 本調達においては，外部からの攻撃に対する情報セキュリティ対策のみでなく，内部での情報セキュリティ対策，外部の情報システムに対して悪影響を与えないための情報セキュリティ対策等，総合的な情報セキュリティ対策を講じること。							
(5) 総合的な情報セキュリティ対策を講じる上で，宮内庁統合NW，標的型攻撃対策システム，クライアント端末，資産管理サーバ，KMSサーバなどと連携して機能する対策については，連携する各システムの設計書や機器上の設定内容等を十分に確認し，理解すること。 なお，連携する各システムの機器上の設定の変更が必要となる場合には，甲を介して各システムの保守事業者，現行運用管理支援事業者と必要な調整を行い，設定変更の内容（変更前と変更後の差分等）を明らかにし，甲の承諾を得た上で，乙の責任と負担において具体的な設定変更の作業依頼書を作成すること。ただし，作業実施予定日の10日（休日を除く。）前までに乙が作業内容（設定，手順等）について文書にて甲へ具体的に説明した上で，通常の保守業務又は運用管理業務の範囲内の作業と認められる場合には，甲を介し，甲の指示として当該作業を関係事業者に通常業務として依頼することができる。							
(6) 本調達システム内部への侵害拡大を防止するため，独立行政法人情報処理推進機構（以下「IPA」という。）の「『高度標的型攻撃』対策に向けたシステム設計ガイド」の最新版（以下「高度標的型攻撃対策ガイド」という。）のシステム設計対策セットを十分に理解した上で，各対策セットの適用を検討し，攻撃者が侵入しづらく，内部侵害拡大がしづらいシステム設計を行うこと。また，その設計内容を各機器等の設定に対して確実に反映し，機能させること。							
(7) 高度標的型攻撃対策ガイドを十分に理解した上で，ネットワークの設計については，次の表で例示するネットワークセグメントの分離単位を基本とし，適切な設計を行うこと。ただし，現行宮内庁NWSにおいては，ハートビート・CSV（Cluster Shared Volume）用セグメント，ライブ・マイグレーション用セグメントもある。各セグメント間を行き来する通信は，原則不可とし，ユーザが利用する機能又は受けるサービスを滞りなく提供するために必要な通信などについては，必要最小限にするアクセス制御を施すこと。 なお，ネットワークセグメントの分離単位及びアクセス制御の設定内容については，あらかじめ甲と協議の上，決定すること。 【表の記載は省略】							
(8) ユーザが利用する業務やアプリケーション，宮内庁CISのネットワークの制御及び運用などで不要な通信プロトコル，通信ポート，ソフトウェア上の機能又はサービスを明らかにしてから甲と協議し，甲の承諾を得た上で，停止やブロックするなどの不要な機能を利用不可とする設計を適切に行うこと。							
(9) ネットワークスイッチ等のネットワーク機器は，前項(8)で示した不要機能を予め排除したOS又はファームウェアを採用し，ユーザの業務が滞りなく遂行でき，宮内庁CISのネットワークの制御及び運用などが適切に行うことが可能な必要最低限の機能が実装されたものとすること。							
(10) 本調達で導入するHDD等の補助記憶装置を搭載する機器が，故障・障害等により乙が新規交換した場合，情報漏出防止のため，交換されたHDD等は甲が処分できること（本号を前提とした契約が可能であること）。 ただし，やむを得ない事情により交換されたHDD等の返却が必要な場合は，事前に甲の承諾を得た上で，甲の立ち会いの下，記録されているデータを完全に消去し，データ消去証明書を提出すること。							
(11) 本調達における全ての機器に搭載されるオペレーティングシステム（以下「OS」という。）及びソフトウェアは，次の情報セキュリティに関する情報提供サイト等を参考にし，納入期限までに指摘されている脆弱性やセキュリティホール等に対して修正モジュールの導入など適切な処理を施し，安全なシステムの構築を行うこと。 ① NISCから発出される情報 https://twitter.com/nisc_forecast ② 警察庁から発出される情報 https://www.npa.go.jp/cyberpolice/ ③ IPAから発出される情報 http://www.ipa.go.jp/security/index.html http://jvndb.jvn.jp/index.html ④ JPCERT/CC から発出される情報 https://www.jpcert.or.jp/ ⑤ JC3 から発出される情報 https://www.jc3.or.jp/info/index.html	加点	100	50	25	0	情報セキュリティを確保するための基本的な考え方，作業プロセスや管理方法等が論理的に示されており，その対応の効果により，セキュリティ要件の確実な達成に繋がることを具体的に示した場合には加点として評価する。
(12) 本調達で導入する機器のうち「ウイルス対策機能」を有することが機能要件に含まれる場合には，以下を満たすこと。 (ア) ウイルス対策ルール（又はパターンファイル）は，自動的に更新されること。 (イ) ウイルススキャンのエンジンは，サーバ機器とクライアントPCとでは異なる製造業者の製品を採用し，ウイルス対策ルール又はパターンファイルの公開時期のずれなどによる対策の遅れを吸収するため，多層型防御による情報セキュリティ対策の強化が可能なこと。 本調達で導入する機器のうち「ウイルス対策機能」を有することが機能要件に含まれる場合には，以下を満たすこと。 (ア) ウイルス対策ルール（又はパターンファイル）は，自動的に更新されること。 (イ) ウイルススキャンのエンジンは，サーバ機器とクライアントPCとでは異なる製造業者の製品を採用し，ウイルス対策ルール又はパターンファイルの公開時期のずれなどによる対策の遅れを吸収するため，多層型防御による情報セキュリティ対策の強化が可能なこと。							
(13) 本業務の実施に当たり，乙又はその従業員，本調達の役務内容の一部を請負等する先，もしくはその他の者により意図せざる変更が加えられないための管理体制が整備されていること。							
(14) 乙の資本関係・役員等の情報，受注作業の実施場所に関する情報，受注業務の従事者の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績及び国籍に関する情報を提供すること。							
(15) 乙は，受注業務の一部を請負等する場合は，あらかじめ情報セキュリティ管理計画書に相手方を含めた管理体制を記載の上，提出し，甲の承諾を受けること。また，再請負の相手方から更に第三者に請負が行われる場合においても同様とする。 なお，再委託先の変更等を行う必要が生じた場合は，情報セキュリティ管理計画書の該当部分を変更の上，甲に提出し，承諾を受けること。							
(16) 情報セキュリティインシデントへの対処方法が確立されていること。							
(17) 情報セキュリティ対策その他の契約の履行状況を定期的に確認し，甲へ報告すること。							
(18) 乙の講ずる情報セキュリティ対策が甲の所有するポリシー等の基準を満たしていない場合には，乙は，甲と協議の上で追加的なセキュリティ対策を講ずること。							

評価対象	必須	加点	加点評価				評価基準
			特に優秀	優秀	標準	加点なし	
(19) 本調達に係る業務の遂行における情報セキュリティ対策の履行状況を確認するために，甲が情報セキュリティ監査の実施を必要と判断した場合は，甲がその実施内容（監査内容，対象範囲，実施等）を定めて，情報セキュリティ監査を行う（甲が選定した事業者による監査を含む。）。また，乙は自ら実施した外部監査についても甲へ報告すること。 情報セキュリティ監査の実施については，これらに記載した内容を上回る措置を講ずることを妨げるものではない。							
(20) JPCERT/CC「攻撃者が悪用するWindowsコマンド(2015-12-02)」を参考にして，甲職員のクライアント端末に必要のないWindowsコマンドを，AppLockerやソフトウェア制限ポリシー等を使用して制限することで，攻撃者による悪用を低減すること。 https://www.jpcert.or.jp/magazine/acreport-wincommand.html 制限するコマンドの選定は，契約後，甲担当者と協議の上，決定する。							
1.15.2.情報セキュリティが侵害された場合の対応							
(1) 情報セキュリティインシデントが発生した場合に備え，連絡・報告フロー，体制，対応手順等を明示した提出成果物を提出の上，甲担当者の承諾を得ること。また，提出成果物には，次の項目を記載することとし，その他必要と考えられる項目も記載すること。 (ア) 標的型攻撃 (イ) 不正アクセス (ウ) 情報漏えい (エ) 未知のマルウェア感染 (オ) 既知のマルウェア感染	必須						左記ついて，理解した上で対応できるか。
(2) 本調達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又はそのおそれがある場合には，速やかに甲担当者へ報告し，甲担当者と協議を行いつつ対応を行うこと。これに該当する場合には，次の事象を含む。また，甲担当者が必要とする情報を開示すること。 (ア) 乙に提供し，又は乙によるアクセスを認める甲の情報の外部への漏えい及び目的外利用 (イ) 乙による甲のその他の情報へのアクセス	必須						
1.15.2.情報セキュリティが侵害された場合の対応 【再掲】							
(1) 情報セキュリティインシデントが発生した場合に備え，連絡・報告フロー，体制，対応手順等を明示した提出成果物を提出の上，甲担当者の承諾を得ること。また，提出成果物には，次の項目を記載することとし，その他必要と考えられる項目も記載すること。 (ア) 標的型攻撃 (イ) 不正アクセス (ウ) 情報漏えい (エ) 未知のマルウェア感染 (オ) 既知のマルウェア感染		加点	100	50	25	0	情報セキュリティインシデント発生時の連絡・報告フロー，体制対応手順等に関して，具体的に記載されており，かつ妥当性のある内容である場合には，加点として評価する。
(2) 本調達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又はそのおそれがある場合には，速やかに甲担当者へ報告し，甲担当者と協議を行いつつ対応を行うこと。これに該当する場合には，次の事象を含む。また，甲担当者が必要とする情報を開示すること。 (ア) 乙に提供し，又は乙によるアクセスを認める甲の情報の外部への漏えい及び目的外利用 (イ) 乙による甲のその他の情報へのアクセス							
1.15.3.その他							
その他，情報セキュリティ対策について，本調達仕様書（案）「1.2.背景と目的」の実現のために有効かつ必要な提案を具体的に行うこと。	必須						「1.2.背景と目的」を理解し，具体的な提案ができるか。
		加点	100	50	25	0	「1.2.背景と目的」を十分理解した上で，妥当性がありかつ有効な提案があれば加点として評価する。
1.16.宮内庁NWSの運用管理業務							
1.16.1.運用管理業務開始時期							
乙は，宮内庁NWSの運用管理業務は，2020年2月1日から開始すること。 なお，乙は，2020年2月1日から円滑に滞りなく宮内庁NWSの運用管理業務が開始できるよう，宮内庁CISの構築期間中から宮内庁NWSの運用管理業務に必要となる事項の洗い出しを行い，それらに対して必要な対策を事前に講じ，十分に準備を行うこと。	必須						開始時期及び十分な準備の必要性を理解しているか。
		加点	100	50	25	0	具体的な対応策方針が示されている場合には加点とする。
1.16.2.実施							
1.16.2.1 実施							
(1) 乙は，公共サービス改革法の第24条に基づき，宮内庁NWSの運用管理業務を実施しなければならない。 (2) 乙は，公共サービス改革法の第25条に基づき，秘密保持義務等を負う。	必須						左記ついて，理解した上で対応できるか。
1.16.3.成果物							
(1) 乙は，以下の成果物を納品すること。ただし，それぞれの納品時期については，契約締結後速やかに甲と乙が協議し，甲が承諾した上で定めるものとする。ただし，①，②については，契約締結後，運用管理業務開始10日（休日を除く）前までに遅滞なく提出すること。 ① 運用管理計画書 ② サービスレベル合意書(SLA) ③ サービスレベル報告書 ④ 運用管理報告書（週次，月次） ⑤ 改善提案書 ⑥ その他，運用管理作業において作成・更新した各種資料 (2) 成果物は全て日本語表記とし，紙媒体及び甲の指示する電子媒体をそれぞれ2部ずつ作成すること。	必須						左記ついて，理解した上で対応できるか。
		加点	40	20	10	0	成果物を継続的に利用・管理していくに当たって次のような具体的で有用な提案があれば，加点として評価する。 ・成果物の修正等があった際，改めた当該部分を単に提出するのではなく，紙媒体としてファイルに綴ってある成果物から当該部分を抜き出し，乙が直接差し替える。ただし，この差し替え前後に甲担当者の承諾を得ること。 ・成果物の文書について，見やすさ・使いやすさを考慮した具体的な工夫を施す。 ・運用管理作業に伴い作成した資料は，都度個別に提出するのではなく，体系立てて整理した「運用管理作業資料」などのような簿冊にまとめて提出し，新規資料は乙が簿冊に追加，更新があれば乙が簿冊から当該部分を抜き出して差し替える。ただし，この差し替え前後に甲担当者の承諾を得ること。
1.17.創意工夫の発揮							
本業務を実施するに当たっては，以下の観点から提案を行い，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。 (1) 宮内庁NWSの運用管理業務に対する提案 乙は，運用管理業務の実施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。 (2) 運用管理業務以外に対する改善提案 乙は，運用管理業務以外に関して，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，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。	必須						落札後に提案すべきことについて，理解しているか。
2. 特記事項							
2.1.基本事項							
(1) 本調達仕様書（案）「1.4.背景と目的」に沿い，本調達の設計・構築・稼働・運用に必要と認められる事項については，本調達仕様書（案）に記載なき事項であっても，具体的に提案を行うこと。	必須						それぞれを理解した上で，具体的な提案ができるか。
(2) 創造宣言に基づき，宮内庁NWSの運用コストについて，平成25年度に比して3割削減達成を目指し，宮内庁CISの保守及び運用効率の最大化を図ることを設計段階から考慮しつつ，本調達仕様書「1.11.成果物」の各文書に適切に反映することにより，本調達仕様書「1.4.背景と目的」における各目的の実現を達成すること。	必須						
(3) 本調達システムでは，次の事項に基づきつつ，宮内庁NWSの全体最適に資する設計を行うこと。 ① 現行宮内庁NWSに導入されているサーバについて，「13.資料閲覧」時に，これまでの各リソースの使用状況（平均，ピーク，時間変化）等を把握し，CPU，メモリ等の主記憶装置，HDD等の補助記憶装置，外部インタフェースの種類やポート数等の拡張余地（上限値）に係るハードウェア仕様が，アプリケーションプログラムの機能要件やユーザの業務量に照らして，過大となっていないか，サーバのハードウェアのグレードが適正な範囲に収まっているかを確認した上で，定量的かつ具体的に根拠を示しつつ本調達におけるサーバリソースのサイジングの実施及び全体最適な情報システムの設計を行うこと。 なお，ハイパースレッディングや仮想化技術を用いる場合には，用いない場合と比較してCPU使用率の表示の特異性を考慮した上でサイジング及び設計を行うこと。 ② 次に例示する情報に留まらず，最新の技術及び製品の動向を十分に調査した上で，前項①と相まってハードウェアのコスト削減を図ること。「平成27年版 情報通信白書（総務省）」によれば，次のとおり。 ア．データ伝送速度が指数関数的に向上し，固定ネットワーク，モバイルネットワークともにあらゆるデータが瞬時に共有可能な状況になってきている。 イ．コンピューティング分野は，いわゆる「ムーアの法則」に従いCPU等の計算能力が指数関数的に向上するとともに，データを蓄積するストレージの大容量化も進んできた。 ウ．ムーアの法則：世界最大の半導体製造業者Intel社の創設者の一人であるゴードン・ムーア博士が1965年に経験則として提唱した「半導体の集積密度は18～24か月で倍増する」という法則。 エ．HDDやフラッシュメモリ，光ディスクなどに代表されるデータの記憶・保存に係る記憶装置等の製品においても同様の変化がみられる。2000年以降は，面積あたりの記憶機密度は年率30%～50%の増加率で向上しており，これに伴い記憶装置の単価の減少が続いている。市販のHDDのGBあたり単価に換算すると，1985年から30年間で約100万分の1まで下がっている。 オ．Less’s Law：ムーアの法則と対比させLess’s Lawとして，ストレージは12か月でコストが半減し，同時に容量が2倍になるという法則として言及されることがある。	必須						左記について，理解した上で対応できるか。
(4) 本調達で要求する機能要件及び性能要件を満たし，宮内庁統合NWの技術的仕様及び設計・設定内容を十分に理解した上で，1，200名規模で利用するのに十分な処理性能を提供するため，本調達仕様書（案）に記載する機器等以外の新たなハードウェア又はソフトウェアの追加あるいは構成を変更しても構わない。その場合，新たに追加したハードウェア又はソフトウェアの製品資料及び機能証明書を提出し，その機能を採用する理由及び効果を提案書に具体的に記載すること。	必須						
2.1.基本事項 【再掲】							
(1) 本調達仕様書（案）「1.4.背景と目的」に沿い，本調達の設計・構築・稼働・運用に必要と認められる事項については，本調達仕様書（案）に記載なき事項であっても，具体的に提案を行うこと。							
(2) 創造宣言に基づき，宮内庁NWSの運用コストについて，平成25年度に比して3割削減達成を目指し，宮内庁CISの保守及び運用効率の最大化を図ることを設計段階から考慮しつつ，本調達仕様書「1.11.成果物」の各文書に適切に反映することにより，本調達仕様書「1.4.背景と目的」における各目的の実現を達成すること。							

評価対象	必須	加点	加点評価 特に優秀	優秀	標準	加点なし	評価基準
(3) 本調達システムでは，次の事項に基づきつつ，宮内庁NWSの全体最適に資する設計を行うこと。 ① 現行宮内庁NWSに導入されているサーバについて，「13.資料閲覧」時に，これまでの各リソースの使用状況（平均，ピーク，時間変化）等を把握し，CPU，メモリ等の主記憶装置，HDD等の補助記憶装置，外部インタフェースの種類やポート数等の拡張余地（上限値）に係るハードウェア仕様が，アプリケーションプログラムの機能要件やユーザの業務量に照らして，過大となっていないか，サーバのハードウェアのグレードが適正な範囲に収まっているかを確認した上で，定量的かつ具体的に根拠を示しつつ本調達におけるサーバリソースのサイジングの実施及び全体最適な情報システムの設計を行うこと。 なお，ハイパースレッディングや仮想化技術を用いる場合には，用いない場合と比較してCPU使用率の表示の特異性を考慮した上でサイジング及び設計を行うこと。 ② 次に例示する情報に留まらず，最新の技術及び製品の動向を十分に調査した上で，前項①と相まってハードウェアのコスト削減を図ること。「平成27年版 情報通信白書（総務省）」によれば，次のとおり。 ア．データ伝送速度が指数関数的に向上し，固定ネットワーク，モバイルネットワークともにあらゆるデータが瞬時に共有可能な状況になってきている。 イ．コンピューティング分野は，いわゆる「ムーアの法則」に従いCPU等の計算能力が指数関数的に向上するとともに，データを蓄積するストレージの大容量化も進んできた。 ウ．ムーアの法則：世界最大の半導体製造業者Intel社の創設者の一人であるゴードン・ムーア博士が1965年に経験則として提唱した「半導体の集積密度は18～24か月で倍増する」という法則。 エ．HDDやフラッシュメモリ，光ディスクなどに代表されるデータの記憶・保存に係る記憶装置等の製品においても同様の変化がみられる。2000年以降は，面積あたりの記憶機密度は年率30%～50%の増加率で向上しており，これに伴い記憶装置の単価の減少が続いている。市販のHDDのGBあたり単価に換算すると，1985年から30年間で約100万分の1まで下がっている。 オ．Less’s Law：ムーアの法則と対比させLess’s Lawとして，ストレージは12か月でコストが半減し，同時に容量が2倍になるという法則として言及されることがある。		加点	200	100	50	0	本調達の目的を十分理解した上で，妥当性がありかつ有効な提案があれば加点として評価する。
(4) 本調達で要求する機能要件及び性能要件を満たし，宮内庁統合NWの技術的仕様及び設計・設定内容を十分に理解した上で，1，200名規模で利用するのに十分な処理性能を提供するため，本調達仕様書（案）に記載する機器等以外の新たなハードウェア又はソフトウェアの追加あるいは構成を変更しても構わない。その場合，新たに追加したハードウェア又はソフトウェアの製品資料及び機能証明書を提出し，その機能を採用する理由及び効果を提案書に具体的に記載すること。							
2.2.機器等の設定							
2.2.1.オンプレミス							
宮内庁CISで導入されるオンプレミスの機器について記載する。 (1) 本調達機器等は中古品でないものとする。	必須						左記について，理解した上で対応できるか。
(2) ネットワークの管理やアプリケーション等での通信に利用される，OSI参照モデルのデータリンク層より上位（レイヤ3以上）の通信プロトコルは，IPv4(RFC 791)及び TCP(RFC 793)又はUDP(RFC 768)（以下「TCP/IP」という。）を基本とする。 なお，レイヤ3以上で，コスト削減及び運用管理業務の効率化の実現が可能な通信プロトコルを採用するのであれば，TCP/IP以外の通信プロトコルを基盤として採用を阻害するものではない。ただし，TCP/IP以外の通信プロトコルを基盤として採用した場合であったとしても，インターネット接続を可能とし，サーバ機器及びクライアント端末などが TCP/IP での通信が可能なこと。	必須						
(3) 本調達機器等の構成について，構成品一覧を提示し甲の承諾を得ること。（製造事業者等の製品型番が分かる品目表を提出すること）。	必須						
(4) 同一の種類の機器に関しては，オーバースペックにならないよう適材適所での設計に配慮し，保守性を高める観点から，可能な限り機種又はシリーズを揃えること。	必須						左記について，理解しているか。
		加点	40	20	10	0	具体的な提案があり，妥当な内容であれば加点として評価する。
(5) 同一種類のソフトウェアについては，可能な限りバージョンを統一すること。	必須						左記について，理解しているか。
(6) 本調達機器等は省スペース設計であること。	必須						左記について，理解しているか。
		加点	40	20	10	0	本調達機器が省スペース設計，省電力設計であることを具体的に示し，妥当な内容であれば加点とする。
(7) 本調達機器等は省電力設計であること。 なお，提案を行う各ハードウェアの消費電力を示す資料を添付し，最大消費電力を具体的に示すこと。	必須						左記について，理解した上で対応できるか。
(8) 本調達及びその構成，配置については，運用管理環境を考慮して，最適化を図るとともに，最新の技術を採用すること。	必須						
(9) ハードウェア及びソフトウェアは，製造事業者等による製品の動作が保証又は確認されたものであること。ただし，製造事業者等による製品の動作の保証又は確認ができない場合には，提案書の提出時までに応札者の検証環境での結果又は過去の実績から動作の証明が可能であるならば，その証跡を提出すること。	必須						
(10) 本調達で採用するソフトウェアのバージョン確定に当たっては，甲と協議すること。また，バージョン確定後から納入期限までにバージョンアップ又はパッチ適用の必要性があることが確認された場合には，動作確認が済んでいるものに限り，甲の承諾を得た後，最新バージョンとすること。	必須						
(11) 納入期限までに発見された本調達機器等の不具合や問題については，乙の責任と負担において迅速に対応すること。	必須						
(12) 本調達機器等に欠陥があった場合は，迅速に物品交換等の対応をとること。	必須						
(13) 本調達機器等に搭載されるハードウェア及びソフトウェアについて，納入期限までに指摘されているセキュリティホール等に関して，修正モジュールの導入など，適切な処理を施すこと。	必須						
(14) サポートライフサイクルポリシーが公表されているハードウェア及びソフトウェアについては，本調達の賃貸借期間終了まで対策用ファイルの提供が継続されると見込まれるハードウェア及びソフトウェアを選定すること。また，適宜入手したサポートライフサイクルポリシーの情報から必要と判断した場合は，後継となるハードウェア及びソフトウェアへの更新等の計画を策定すること。	必須						左記について，理解した上で対応できるか。
		加点	40	20	10	0	サポートライフサイクルポリシーが公表されているハードウェア及びソフトウェアについて，本調達の賃貸借期間満了まで対策用ファイルの提供が継続されると見込まれるハードウェア及びソフトウェアを選定していることを具体的に示した場合及び適宜入手したサポートライフサイクルポリシーの情報から必要と判断した場合は，後継となるハードウェア及びソフトウェアへの更新等の計画策定の具体的な手順を示した場合には加点として評価する。
(15) サポートライフサイクルポリシーが公表されていないハードウェア及びソフトウェアについては，後継となるハードウェア及びソフトウェアの有無や販売等開始からの経過年数等を考慮するなどして，本調達の賃貸借期間終了まで対策用ファイルの提供が継続されると見込まれるハードウェア及びソフトウェアを選定すること。また，後継となるハードウェア及びソフトウェアの販売等に関する情報を適宜入手し，当該情報を考慮して，後継となるハードウェア及びソフトウェアへの更新等の計画を策定すること。	必須						左記について，理解した上で対応できるか。
		加点	40	20	10	0	サポートライフサイクルポリシーが公表されていないハードウェア及びソフトウェアについて，後継となるハードウェア及びソフトウェアの有無や販売等開始からの経過年数等を考慮するなどして，本調達の賃貸借期間満了まで対策用ファイルの提供が継続されると見込まれるハードウェア及びソフトウェアを選定していることを具体的に示した場合及び後継となるハードウェア及びソフトウェアの販売等に関する情報を適宜入手し，当該情報を考慮して，後継となるハードウェア及びソフトウェアへの更新等の計画策定の具体的な手順を示した場合には加点として評価する。
(16) 本調達機器等の設置及び導入後の基本動作確認は，乙の責任と負担において対応すること。	必須						左記について，理解した上で対応できるか。
(17) 納入するハードウェアの設置・接続に必要な接続器具やケーブル等は，乙の負担において必要数供給すること。	必須						
(18) 本仕様を満たす機器等は，仕様を満たす増設機器として，メモリ等主記憶装置及びハードディスク等補助記憶装置等を全て取り付けた形で，正常動作の確認を行った上で納入すること。 なお，LANケーブル等の既設の接続方法を継続使用可能なものについては，原則として既設の接続方法を使用するものとする。	必須						
(19) 本調達機器等は，人体に危険がないものであること。	必須						
(20) 本調達機器等は，原則として単相100V商用電源を使用するものであること。	必須						
(21) 本調達機器等は，原則として特別な空調設備を必要とせず，支出負担行為担当官の指定する場所に設置可能であること。	必須						
(22) 本調達機器等は，ハードウェア，ソフトウェアともに，原則として日本語対応のものであること。	必須						
(23) 導入する機器はISO9001を取得した組織にて製造された製品であること。	必須						
(24) 導入する機器を構成するハードウェア及び実装されるソフトウェアのうち，JIS等の国内規格，ISO等の国際規格に定めのある製品については，当該規格に準拠していること。	必須						
(25) 各種災害(地震等)対策等を十分に考慮し，安全かつ信頼性のあるシステムを構築し，可用性と保守性の高い運用管理を可能にすること。	必須						
(26) 将来におけるハードウェア，ソフトウェアの増強，ネットワークの拡大，接続機器の増設及び拡張のため，互換性，移植性，接続性を確保でき，柔軟に対応できるよう標準化が考慮されていること。	必須						
(27) 甲においては，「電子政府システムのIPv6対応に向けたガイドラインhttp://www.kantei.go.jp/jp/singi/it2/cio/dai24/24siryou4-2.pdf（平成19年3月30日総務省）」により，宮内庁NWSに含まれる他のシステムとの運用管理面での整合性を保ちつつ，IPv6対応を進めることとし，当面はIPv4を念頭にシステムの稼働を行う。 なお， ネットワーク機器については，RFC 8200を基本仕様としたIPv6に対応済み，若しくは，将来的にソフトウェアのバージョンアップ等によりIPv6に対応できる機器を選定すること。また，その他の機器についても，可能な限りIPv6に対応できる機器を選定することとする。	必須						
(28) ネットワークは，OSI参照モデルの物理層（レイヤ1）及びデータリンク層（レイヤ2）は，IEEE 802.3 ETHERNET WORKING GROUP（ http://grouper.ieee.org/groups/802/3/ ）にて標準化された技術を基本とする。	必須						
(29) 調達するソフトウェアは，原則として日本語に対応していること。ただし，日本語に対応していない場合には，利用，運用，管理，保守を行うのに必要十分な手順書等を乙が日本語で提供すること。また，乙が提供する日本語手順書等については，利用実態及び製造業者等の提供する手順書等の変更にあわせ，必要に応じて修正を行うこと。	必須						
(30) 応札者が提案するソフトウェアについては，製造業者等が提供する政府・公共機関を対象としたプログラムを適用し，ソフトウェアライセンス管理の集約化による負荷の軽減及び投資対効果の向上を図ること。導入予定のソフトウェアについて，甲のライセンスの保有状況を確認し，ライセンスを保有している場合には，既存ライセンスを最大限有効活用し，コスト削減を図ること。	必須						
2.2.2.クラウドサービス							
本調達において，クラウドサービスを採用する場合は，次に示す要件を満たすこと。また，本調達における契約期間終了後も，本調達において利用するクラウド環境を契約期間終了前に契約の延長手続き等を実施することにより，そのまま継続利用することが可能なこと。	必須						クラウドサービスを採用する場合，左記について理解した上で対応できるか。
(1) 日本国内に物理的に設置され，運用されていること。	必須						
(2) 準拠法を日本の法律とすること。	必須						
(3) 管轄裁判所を日本国内の裁判所とすること。	必須						
(4) ISO/IEC 27001 に準拠し，ISMS 審査機関による認証を証明できること。	必須						

評価対象	必須	加点	加点評価 特に優秀	加点評価 優秀	加点評価 標準	加点評価 加点なし	評価基準
(5) IaaSサービスを提供する場合はISO27017に準拠していること。	必須						クラウドサービスを採用する場合，左記について理解した上で対応できるか。
(6)「クラウドサービス利用のための情報セキュリティマネジメントガイドラインhttp://www.meti.go.jp/press/2013/03/20140314004/20140314004-2.pdf（2013年度版経済産業省）」に対し，乙は主に「クラウド事業者の実施が望まれる事項」について可能な限り遵守すること。 なお，遵守することができない内容については，甲に対してあらかじめ該当箇所を示した上で理由の詳細と可能な限り代替策等を報告すること。	必須						
(7) 情報資産の所有権がクラウドサービス事業者に移管されるものではないこと。したがって，甲担当者が要求する任意の時点で情報資産を他の環境に移管させることができること。	必須						
(8) 採用するクラウドサービスを選定する際には，事前にクラウドサービスプロバイダに第三者へのクラウド環境の引継ぎ等の手続きについて確認した上で，乙，運用管理事業者及び甲へのクラウド環境の引継ぎに遺漏が無いよう，クラウドサービスプロバイダとの契約内容や引継ぎ手順等を整備しておくこと。	必須						
(9) 法令や規制に従って，クラウドサービス上の記録を保護すること。	必須						
(10) 情報資産が残留して漏えいすることがないよう，必要な措置を講じること。	必須						
(11) 自らの知的財産権についてクラウド利用者に利用を許諾する範囲及び制約を，契約の締結前に甲担当者に対して正確に説明し，確認を行うこと。	必須						
(12) インターネット回線接続サービス及び宮内庁WANの通信回線接続サービスの技術的仕様及び設計・設定内容を十分に考慮した上で，クラウドサービスを1，200名規模で利用するのに十分な処理性能を提供し，ユーザの業務遂行が効率的かつ確実に可能なこと。	必須						
(13) クラウドサービスへのアクセス制限を指定したIPアドレス等に基づいて可能なこと。また，アクセス制御の設定を適切に行い，情報セキュリティ対策を確実に行うこと。	必須						
(14) 業務継続性を確保するため，本調達においてバックアップサイトをクラウドサービス型で提供する場合は，バックアップサイトについても上記(1)～(13)を満たすこと。 なお，バックアップサイトをクラウドサービス型で提供する場合は，本調達のメインシステムが物理的に設置された場所と異なる同時被災しない場所に設置され，運用されていること。	必須						
2.2.3.データセンタ仕様							
本調達にオンプレミスの機器を宮内庁の外部のデータセンタに設置して提供する場合は，次の仕様を満たすこと。また，本調達における契約期間終了後も，本調達において利用するデータセンタ環境を契約期間終了前に契約の延長手続き等を実施することにより，そのまま継続利用することが可能なこと。	必須						外部のデータセンタに設置して提供する場合，左記について理解した上で対応できるか。
(1) 日本国内に物理的に設置され，運用されていること。	必須						
(2) 当庁から50Km以内の距離に存在し，必要に応じて駆けつけが可能なこと。	必須						
(3) データセンタ専用の建物であり制震又は免震構造であること。	必須						
(4) データセンタ設置エリアは活断層及び航空機発着航路に設定されていないこと。	必須						
(5) データセンタ専用の自家発電設備を有し，48時間以上の無給油発電が可能なこと。	必須						
(6) データセンタのルーム内への入室には2種類以上の認証装置を経由し，生体認証等による入室制限を行うことが可能なこと。	必須						
(7) データセンタの入口，サーバルームへの入室扉前には，監視カメラが設置されており，常時監視されていること。	必須						
(8) データセンタのラックは，当庁専用のラックとし他と共用しないこと。	必須						
(9) 可能な限り，甲からの書面等の申請に応じて，甲担当者が入室することが可能なこと。	必須						
(10) データセンタは，データセンタ運営・維持管理業務において，事業継続の国際規格ISO22301を取得した事業者が提供していること。	必須						
(11) データセンタへ設置した機器に対する運用管理業務が，情報管理室から十分に情報セキュリティ対策を施した上でリモートで実施できること。							
2.3.オペレーティングシステムの集約化							
2.3.1.クライアント端末							
(1) 本調達で調達するクライアント端末のOS（以下「クライアントOS」という。）は，業務継続性，宮内庁NWSの運用効率性及び安定性の観点から現行OSに準拠したマイクロソフト社製Windows 10 Enterprise 64bitまたはこれと同等以上の性能・機能を有する製品を搭載すること。	必須						左記について，理解した上で対応できるか。
(2) クライアントOSは，全て同一のエディション及びバージョンで揃えること。	必須						
(3) クライアントOSの品質や機能等が起因となった障害が発覚した場合に，その製造事業者等が責任をもって迅速に対処できること。	必須						
(4) クライアントOSにおいて脆弱性が発覚した場合に，その製造事業者等が責任をもって迅速に対策パッチの提供を行い，この周知を遅滞なく実施可能なこと。	必須						
(5) JPCERT/CC「ログを活用したActive Directory に対する攻撃の検知と対策」36頁「Active Directoryに対する攻撃の対策」の表の予防策を実施すること。	必須						
2.3.2.サーバ							
(1) 原則として，本調達システムで採用するサーバは，Windows 系OSのうちサーバ用として1種類，UNIX及びUNIXの派生OS，又はLinuxを含むUNIXに類似したシステム体系を持ったOS(以下「UNIX系OS」という)のうち1種類とを合わせて，計2種類(以下「標準サーバOS」という)に集約し，保守及び運用の効率化を図ること。ただし，提供される機能に特化したアプライアンス型のサーバについては，この限りではない。また，既存アプリケーションを動作させる上でやむを得ない理由がある場合に限り，甲の承諾を得た後，別バージョンを導入することを可とする。	必須						左記について，理解した上で対応できるか。
(2) ライセンス料金体系及びその制約条件やライフサイクルなどを十分に理解し，サーバ・ハードウェアのサイジングと合わせ，全体最適かつ本調達システムが安定稼働するのに必要な設計となるライセンス数を過不足なく用意すること。	必須						
(3) 標準サーバOSのうち，Windows系OSの場合は，次の条件を満たすこと。 現行宮内庁NWSの構成を参考にしつつ，本調達仕様書（案）における課題の解決，要件を満たす上で必要となる数量の CAL も調達すること。	必須						
(4) 標準サーバOSのうち，UNIX系OSの場合は，次の条件を満たすこと。 (ア) ユーザ数と同規模以上の組織・団体における情報システムにおいて，十分な利用実績があること。 (イ) ISO/IEC15408の評価保証レベル（EAL，Evaluation Assurance Level）において，EAL4以上の認証を取得している（IPAまたはCCRA（Common Criteria Recognition Arrangement）のポータルサイト等で確認が可能である），あるいは今までにEAL4以上の認証を取得した実績のあるOSの後継OSであること。	必須						
(5) 標準サーバOSの品質や機能等が起因となった障害が発覚した場合に，その製造業者が責任をもって迅速に対処できること。	必須						
(6) 標準サーバOSにおいて脆弱性が発覚した場合に，その製造業者が責任をもって迅速に対策パッチの提供を行い，この周知を遅滞なく実施可能なこと。	必須						
(7) 仮想化技術を採用する場合には，次のことを満たすこと。 (ア) 保守・運用性の向上を図るため，仮想化技術として採用するハイパー・バイザの種類は，一つだけとすること。 (イ) ハイパー・バイザ上で，標準サーバOS及びクライアントOSがゲストOSとして正常に動作することの確認がとれていること。 (ウ) 異なるサーバ・ハードウェア間で，同一製造業者のハイパー・バイザであれば，仮想マシンのインポート又はエクスポートによる容易なサーバ・ハードウェアの移行が可能なこと。 (エ) 異なるサーバ・ハードウェア間で，同一製造業者のハイパー・バイザであれば，仮想マシンを停止させることなく，別のサーバ・ハードウェアへ移動することが可能なこと。 (オ) 業務継続性の向上の観点から，本調達システムの運用開始後，拠点間でのクラスタ構成が可能なこと。 (カ) 投資対効果を最大化するため，本調達システムの運用開始後，ハイパー・バイザを搭載するサーバ・ハードウェアのCPU，メモリ等の主記憶装置、HDD等の補助記憶装置及び外部インタフェース等のリソースの使用状況の実測値を監視し，必要に応じて設定変更を行い，最適なリソースの割当てが可能なこと。 (キ) 投資対効果を最大化するため，本調達システムの運用開始後，ハイパー・バイザを搭載するサーバ・ハードウェアのCPU，メモリ等の主記憶装置，HDD等の補助記憶装置及び外部インタフェース等のリソースの使用状況に余裕（以下「余裕リソース」という。）がある場合，この余裕リソースに対して新たな仮想マシンの割当てが可能なこと。	必須						
(8)標準サーバOS及びハイパー・バイザは，本調達時点で販売されており，かつ本調達システムの賃貸借期間内において，ソフトウェアのアップデート（サービスパック及びセキュリティパッチ）の提供等販売元からのサポートが保証されていること。	必須						
2.3.3.ネットワークスイッチ							
(1) 本調達で調達するネットワークスイッチのファームウェアは，業務継続性，システムの運用効率性の観点から，管理手段として，可能な限り同様なコマンド操作が可能なインタフェース（CLI）又はWebインタフェースを実装した製品で揃えること。	必須						左記について，理解した上で対応できるか。
(2) 本調達で調達するネットワークスイッチのファームウェアの品質や機能等が起因となった障害が発覚した場合に，その製造事業者等が責任をもって迅速に対処できること。	必須						
(3) 本調達で調達するネットワークスイッチのファームウェアにおいて脆弱性が発覚した場合に，その製造事業者等が責任をもって迅速に対策パッチ又は対処済みファームウェアの提供を行い，この周知を遅滞なく実施可能なこと。	必須						
2.4.サーバ機器の集約化							
宮内庁CISにおいては，現行宮内庁NWSよりサーバの物理的台数を集約化し，ハードウェアリソースをより効率的に利用することにより，コスト削減を実現すること。 なお，宮内庁CISを構成するサーバ，アプライアンス機器等の集約化に当たっては，現行宮内庁NWSの構成の見直しを行っても構わないとする。ただし，サーバ機器の集約化にあたっては，集約化後の構成でも現行宮内庁NWSと同等以上の実効性能とし，宮内庁CISの契約期間中を考慮した実効性能を有すること。	必須						左記について，理解した上で対応できるか。
		加点	100	50	25	0	具体的で妥当性があり，かつ有効な提案があれば加点として評価する。
3. システム要件							
3.1.サーバ機能共通要件							
3.1.1.共通仕様							

評価対象	必須	加点	加点評価 特に優秀	加点評価 優秀	加点評価 標準	加点評価 加点なし	評価基準
各サーバ機能の共通仕様を以下に示す。 (1) サーバ用OSの選択は，本調達仕様書（案）「2.3.オペレーティングシステムの集約化」に従い，また，以下を満たすこと。 ① Windows系のサーバ用OSを採用する場合には，Windows Server 2016以降であること。また，この場合のサーバを，以下「Windows系サーバ」という。 ② UNIX系のサーバ用OSを採用する場合には，Linux kernel のバージョンは3.10以降であること。 ③ 仮想化技術を採用する場合には，前項①と②のサーバ用OSがゲストOSとして正常に動作することの確認がとれていること。 なお，本調達仕様書（案）「1.5.3.2 サーバの集約化による運用管理業務の軽減」に示したとおり，現行宮内庁NWSでは仮想化技術を採用している。	必須						
(2) 本調達仕様書（案）「3.12.1.機能要件」を満たすウイルス策機能を有すること。	必須						左記について，理解した上で対応できるか。
(3) バックアップサーバ機能と連携する場合には，システムを停止することなく，OSを含むシステムエリア，ユーザデータエリアのデータバックアップが可能なこと。障害時にはバックアップしたデータからリカバリが可能なこと。	必須						
(4) NTP又はSNTPによる時刻同期が可能なこと。	必須						
(5) ログレポート機能として，HTTP，Syslog， SNMP，SMTPメールのいずれかに対応していること。	必須						
(6) Windows系のサーバ用OSを採用する場合には，タスクスケジューラのログをレポート可能なこと。	必須						左記について，理解した上で対応できるか。
(7) UPSの管理機能を有し，停電を検出した場合にはシステムを自動的にシャットダウンできること。	必須						
(8) 設定管理（コンソール）機能は，本調達仕様書（案）「3.1.3. コンソール（キーボード・ディスプレイ・マウス）機器要件」への接続，またはネットワークを介して使用できること。	必須						
3.1.2.サーバ機器構成要件							
(1) 本調達システムの各サーバ機能を実現するためのサーバ機器は，それぞれ，「別紙4 本調達機器及び各事業者の役割範囲」に示された現行宮内庁NWSにおける各サーバの構成要素（CPU，メモリ，HDD等の補助記憶装置，データ通信用ネットワーク・インタフェース等）以上の性能及び容量又は数量を有し，本調達システムの契約期間中の利用率変化（利用推移）をあらかじめ考慮した構成とすること。	必須						
(2) 本調達仕様書（案）「2.4.サーバ機器の集約化」に従い，各サーバ機器の集約化を行う場合には，以下の要件を満たすこと。 ① 集約化後のサーバ機器上の全てのサーバ機能が，同時に，現行宮内庁NWSにおける各サーバ機能を実装したサーバ機器のCPU，メモリの最大リソース量と同等程度のリソース消費をそれぞれ発生させたとしても，ユーザの業務に支障なく，集約化後のサーバ機器が安定稼働可能となる性能のCPU，メモリを有すること。 ② 集約化後のサーバ機器上の全てのサーバ機能が，同時に，現行宮内庁NWSにおける各サーバ機能を実装したサーバ機器上のディスクI/O（Input/Output），データ通信用ネットワークの最高データ転送速度（最大帯域幅）と同等程度のデータ転送量をそれぞれ発生させたとしても，ユーザの業務に支障なく，集約化後のサーバ機器が安定稼働可能となる性能のHDD等の補助記憶装置，データ通信用ネットワーク・インタフェースを有すること。 ③ 集約化後のサーバ機器に搭載されるHDD等の補助記憶装置の容量は，サーバ機器を集約したことによるディスク利用率が向上するような設計を行い，本調達システムの契約期間を考慮した構成とすること。 ④ 仮想化技術を採用した場合の要件を以下に示す。 ・ 各サーバ機能の冗長化や連携が有効に働くよう考慮した設計とすること。 ・ 仮想化技術で集約化されたサーバ機器が停止した際，他の物理的に異なるサーバ機器で，その停止した仮想化されたサーバ機能を収容し，自動的に再起動することにより，業務継続性を向上させる機能を有すること。同様に，一つの仮想化されたサーバ機能が停止した場合においても同様な機能を提供可能なこと。	必須						
(3) 補助記憶装置は耐障害性や性能を考慮し，RAID1/1+0/5/6 等から適切な構成とすること。	必須						
(4) 補助記憶装置はホットプラグ対応であること。	必須						
(5) DVDスーパーマルチ2層対応ドライブ（8倍速以上のDVD-R，4倍速以上のDVD-RW，24倍速以上のCD-R，10倍速以上のCD-RW）を有すること。 なお，同等の機能を有する外付けDVDスーパーマルチ2層対応ドライブを用いることも可とする。	必須						
(6) 管理用ネットワーク・インタフェースとして，IEEE802.3規格に準拠した10BASE-T/100BASE-TXのポートを2つ以上有すること。	必須						
(7) データ通信用ネットワーク・インタフェースとして，IEEE802.3規格に準拠した1000BASE-Tのポートを2つ以上有すること。 なお，各サーバ機能のサーバ機器の集約化を行う場合には，本調達仕様書（案）3.1.2.(2)を満たすためのポート数を有すること。	必須						
(8) USB2.0又はUSB3.0のポートを2つ以上有すること。	必須						
(9) EIA規格準拠19インチラックに搭載可能なこと。また，サーバ機器の盗難及び不正な持ち出しを防止するため，盗難を防止可能な措置を実施すること。防止策は、筐体本体及びディスク等データの格納されている領域に対する措置を実施すること。	必須						
(10) 電源装置が冗長化されていること。	必須						
(11) 電源装置はホットプラグ対応であること。	必須						
(12) 冷却ファンが冗長化されていること。	必須						
(13) 本調達仕様書（案）「3.2.無停電電源装置（UPS）」の要件を満たし，応札者が提案するサーバ機器の電源容量及び台数に適したUPSを過不足なく用意すること。	必須						
(14) 本調達仕様書（案）「3.1.3. コンソール（キーボード・ディスプレイ・マウス）機器要件」を満たした機器と接続可能かつ操作可能なこと。	必須						
(15) HDD等の補助記憶装置が故障等により交換が必要になった場合には，本調達仕様書（案）「1.15.情報セキュリティの確保(10)」を満たす対応が可能なこと。	必須						
3.1.3.コンソール（キーボード・ディスプレイ・マウス）機器要件							
(1) 一つの拠点にて複数台のサーバ機器を設置する場合には，サーバ機器の設定管理の作業を効率的に行うため，KVMスイッチ（Keyboard Video Mouse switch）を用意することにより，キーボード，ディスプレイ（ビデオ），マウスを共有して使用できること。	必須						
(2) KVMスイッチを用いる場合には，サーバ機器台数以上のKVMスイッチのポートの数を用意し，各サーバ機器とKVMスイッチの接続に必要となるケーブルを過不足なく用意すること。	必須						
(3) ディスプレイは液晶15インチ以上，解像度1024×768以上であること。	必須						
(4) キーボードは，OADG標準又はJIS標準配列に準拠もしくは同等品であること。	必須						
(5) キーボード，ディスプレイ，マウスのそれぞれの数は，サーバ機器の台数及びKVMスイッチの有無を考慮し，過不足なく用意すること。	必須						
(6) EIA規格準拠19インチラックに搭載可能なこと。	必須						
3.2.無停電電源装置（UPS）							
本調達仕様書（案）の各サーバ機能を搭載したサーバ機器に接続するUPSの標準仕様を，以下に示す。 (1) サーバ機器等で電源を二重化した機器については，UPSを複数台準備し，異なるUPSに接続すること。	必須						
(2) UPSに接続するサーバ機器の定格電流・電圧及び電源プラグ（入力端子）の形状に適合すること。	必須						
(3) 停電時，自動的にバックアップ電源に切り替わり，接続している全てのサーバを自動的かつ安全にシャットダウンさせる機能を有すること。	必須						
(4) 瞬間的な停電，及び短時間（1～2分程度）の停電時においても，バックアップ電源に切り替り給電できること。	必須						左記について，理解した上で対応できるか。
(5) 指定時刻に自動的に電源投入・切断可能なカレンダー機能を有すること。	必須						
(6) 復電時，UPSに接続されている機器を自動復旧させる機能を有すること。	必須						
(7) IEEE802.3規格に準拠した10BASE-T/100BASE-TXの管理用ポートを1つ以上持つこと。	必須						
(8) EIA規格準拠19インチラックに搭載可能なこと。	必須						
3.3.サーバセグメント用サーバ・ネットワークスイッチ							
サーバセグメント用のサーバ・ネットワークスイッチとして，次の機能及び仕様を満たし，かつ，宮内庁統合NWにて調達を行ったコア・ネットワークスイッチと接続して機能するものを冗長構成にて提供すること。	必須						左記について，理解した上で対応できるか。
3.3.1.一般機能要件							
(1) 96Gbps以上のスイッチファブリックを実装する固定ボックス型のレイヤ2以上に対応したスイッチ製品であること。	必須						
(2) レイヤ3パケット転送能力として70Mpps以上を有すること。	必須						
(3) IEEE802.1q VLAN Taggingに準拠していること。	必須						
(4) STPとして，IEEE802.1d，IEEE802.1w，IEEE802.1s にそれぞれ準拠したスパニングツリー機能を有すること。	必須						
(5) IEEE802.1x に準拠した認証機能を有すること。	必須						
(6) IEEE 802.3x に準拠した全二重イーサネットにおけるフロー制御機能を有すること。	必須						
(7) IEEE 802.3ad Link Aggregation機能を有すること。	必須						

評価対象	必須	加点	加点評価				評価基準
			特に優秀	優秀	標準	加点なし	
(8) IEEE802.1pの優先制御機能を有すること。	必須						左記について，理解した上で対応できるか。
(9) Round Robin 又はStrict Priority Queuing等の QoS に対応していること。	必須						
(10) トラフィックの流量を制限（Rate Limit）する機能を有すること。	必須						
(11) DHCPリレー機能を有すること。	必須						
(12) 送信元及び受信元のMACアドレス及びIPアドレス，TCP/UDPポート番号，又はこれらのフィールドの任意の組み合わせに基づくパケットフィルタ機能を有すること。	必須						
(13) ポリシーベースルーティング機能を有すること。	必須						
(14) VLAN IDは，4,000以上利用可能であること。	必須						
(15) 9,000Byte以上のジャンボフレームに対応していること。	必須						
(16) 10,000以上のMACアドレスに対応していること。	必須						
(17) IPv4ルーティングテーブル数が11,000以上に対応していること。	必須						左記について，理解した上で対応できるか。
(18) ハードウェアで1ポート当たり4 つ以上のキューに対応していること。	必須						
3.3.2.インタフェース仕様							
(1) IEEE802.3規格に準拠した10BASE-T/100BASE-TX/1000BASE-T インタフェースを有し，SFPインタフェースを有すること。	必須						左記について，理解した上で対応できるか。
(2) SFPインタフェースは，IEEE802.3規格に準拠した 1000BASE-SX/LXに対応可能であること。	必須						
(3) EIA規格準拠19インチラックに搭載可能であること。	必須						
3.3.3.セキュリティ機能要件							
(1) 予期していないポートでBPDUを受信した際，ループを防ぐためにそのポートを自動的にダウンする機能を有すること。	必須						左記について，理解した上で対応できるか。
(2) スイッチの追加等により期待されていないBPDUを受けルートブリッジが変更されてしまう事態を防止する機能を有すること。	必須						
(3) 光ファイバやツイストペアケーブルの単一方向リンク（片対障害）検出機能を有すること。	必須						
(4) ポートごとに通信可能なMACアドレス，又はMACアドレス数を制限する機能を有すること。	必須						
(5) MACアドレスとIPアドレスのマップをスイッチ上で管理することによって偽造ARPによる不正な通信盗聴（ARPスプーフィング）を防止する機能を有すること。	必須						
(6) 特定のポートのDHCPスヌーピングを介して取得したIPアドレスのみを許可することで，不正な接続（IPスプーフィング）を防止する機能を有すること。	必須						
(7) 不正なDHCPサーバの接続やDHCPメッセージを使ったDoS攻撃を防止する機能を有すること。	必須						
3.3.4.ネットワーク管理機能要件							
(1) シリアル接続によるコンソールポートを有すること。	必須						左記について，理解した上で対応できるか。
(2) Telnet / SSHによるリモート・コンソール機能を有すること。	必須						
(3) トラフィック解析のためポートのミラーリング機能を有し，同一筐体内のみならず，他の筐体のポートもリモート・ミラーリングできる機能を有すること。	必須						
(4) ソフトウェア及び設定情報をTFTPにてアップロード及びダウンロードする機能を有すること。	必須						
(5) NTP又はSNTPによる時刻同期が可能なこと。	必須						
(6) DNSを参照しIPアドレスの代わりにホスト名を使用できる機能を有すること。	必須						
(7) Syslogサーバにメッセージを送信する機能を有すること。	必須						
(8) SNMPによる管理機能を有すること。	必須						
(9) SSHv1/v2機能を有すること。	必須						
(10) RMONを使った管理機能を有すること。	必須						
(11) 隣接するデバイスとの間で，トポロジの管理を行う機能を有すること。	必須						
(12) 近隣ノードの自動検知が可能なIEEE 802.1ab LLDPに対応し，ネットワーク管理の効率化が可能なこと。	必須						
3.3.5.信頼性要件							
(1) 電源部を冗長化し，一方に障害が発生した場合にも機体が通常どおり稼動できること。 なお，電源部の冗長化の方法は，スイッチ筐体の内部と外部のどちらでも構わない。	必須						左記について，理解した上で対応できるか。
(2) 動作温度が0℃～40℃に対応していること。	必須						
(3) 動作湿度が10%～90%に対応していること。	必須						
(4) VCCI クラスAに準拠していること。	必須						
(5) 起動時にPOST等の自己診断プログラムによる自己診断機能を有すること。	必須						
3.3.6.構成要件							
(1) 応札者が提案する宮内庁本庁及び京都事務所での各サーバの構成及びサーバセグメントの設計にあわせつつ，宮内庁NWSが適切に機能するために十分なポート数を用意し，必要に応じて適切なSFPトランシーバのメディアタイプを過不足なく用意すること。 なお，未使用となるポート数は，スイッチに搭載されている全てのポート数に対して40%以下とすること。	必須						左記について，理解した上で対応できるか。
(2) サーバスイッチとコアスイッチとの間は，リンクアグリゲーションプロトコル（IEEE 802.3ad）を使用し，実効スループットで4Gbps以上の帯域まで利用できること。	必須						
(3) ホットスタンバイによる冗長構成とし，冗長経路において物理的なネットワークのループが構成される場合には，論理的にイーサネットフレームのループでのやり取りが発生しないような対策を講じ，高い耐障害性を確保すること。	必須						
3.4.運用管理セグメント用サーバスイッチ							
運用管理セグメント用のサーバスイッチとして，次の機能及び仕様を満たすものを提供すること。	必須						左記について，理解した上で対応できるか。
3.4.1.一般機能要件							
(1) 固定ボックス型のレイヤ2以上に対応したスイッチ製品であること。	必須						左記について，理解した上で対応できるか。
(2) IEEE802.1q VLAN Tagging機能を有すること。	必須						
3.4.2.インタフェース仕様							
(1) IEEE802.3規格に準拠した1000BASE-SX/LX，100BASE-FX，10BASE-T/100BASE-TX/1000BASE-Tの各インタフェースに対応可能であること。 なお，物理ポートの故障に備え，運用に支障の無い程度の予備ポートを有すること。	必須						左記について，理解した上で対応できるか。
(2) EIA規格準拠19インチラックに搭載可能なこと。	必須						
3.4.3.セキュリティ機能要件							
(1) 送信元/受信元MACアドレスに基づいたフィルタ機能を有すること。	必須						左記について，理解した上で対応できるか。
3.4.4.ネットワーク管理機能要件							
(1) シリアル接続によるコンソールポートを有すること。	必須						
(2) Telnet / SSHによるリモート・コンソール機能を有すること。	必須						
(3) 設定情報をクライアント端末上の標準的なテキスト編集ソフトウェア等で読み込み及び編集可能な形式で保存可能なこと。	必須						

評価対象	必須	加点	加点評価				評価基準
			特に優秀	優秀	標準	加点なし	
(4) ソフトウェア及び設定情報をTFTPにてアップロード及びダウンロードする機能を有すること。	必須						左記について，理解した上で対応できるか。
(5) NTP又はSNTPによる時刻同期が可能なこと。	必須						
(6) Syslogサーバにメッセージを送信する機能を有すること。	必須						
(7) SNMPによる管理機能を有すること。	必須						
(8) SSHv1/v2機能を有すること。	必須						
(9) 管理用のRADIUSユーザ認証機能を有し，管理者以外が設定情報を参照，変更できないような機能を有すること。	必須						
3.4.5.信頼性要件							
(1) 動作温度は0℃～40℃に対応していること。	必須						左記について，理解した上で対応できるか。
(2) 筐体の動作湿度が20%～70%に対応していること。	必須						
3.4.6.機器構成要件							
詳細な接続形態及び接続帯域，必要ポート数及び速度については，「別紙3 各フロア配線，必要ポート数状況」を参照した上で次のとおりとすること。	必須						左記について，理解した上で対応できるか。
(1) 宮内庁NWSの運用管理セグメントの設計を十分に理解した上で，応札者が提案する各サーバの構成に合わせ，宮内庁NWSを適切に機能させるための運用管理を実現するために十分なポート数を用意し，必要に応じて適切なSFPトランシーバのメディアタイプを過不足なく用意すること。 なお，未使用となるポート数は，スイッチに搭載されている全てのポート数に対して40%以下とすること。	必須						
(2) 乙が宮内庁本庁用及び京都事務所用にあらかじめ用意した予備機各1台によるコールドスタンバイでの冗長構成とする。本番機の構築時の設定情報を複製し，あらかじめ用意した予備機にその設定情報を反映し，本番機と同様の動作が可能な状態にすること。 なお，本番機の設定情報が変更された場合には，変更後の設定情報を機械可読なテキスト形式のファイルとして取得し，そのファイルを運用管理セグメント用端末の中で保管できること。また，そのファイルを予備機で読み込み，設定情報を予備機に反映し，設定情報に基づいて機能できること。	必須						
3.5.製造業者宮内庁NWS運用管理クライアント端末							
運用管理業務で日常的に利用する端末を2式用意すること。	必須						左記について，理解した上で対応できるか。
3.5.1.ハードウェアの特質，要件							
(1) A4ノート型パソコンであること。	必須						左記について，理解した上で対応できるか。
(2) 業務継続性を高めるため，単相100V商用電源だけでなく，パソコンに搭載されたバッテリでの駆動が可能なこと。また，バッテリのみでの駆動時間は連続で5時間以上であること。ただし，一般社団法人電子情報技術産業協会（JEITA）が定めるバッテリ搭載PC の駆動時間測定方法（Ver. 2.0）に基づく駆動時間であること。	必須						
(3) CPUは，次の仕様を満たすこと。 ① コア数2以上で，3.0GHz 以上の最大クロック周波数を有すること。 ② キャッシュメモリは3MB 以上を有すること。 ③ バス・スピードは4 GT/s以上を有すること。 ④ 最大メモリ帯域幅は34GB/s以上を有すること。	必須						
(4) 主記憶装置は，次の仕様を満たすこと。 ① システムメモリについては，16GB 相当以上のメモリを有すること。 ② 最大データ転送速度が17.0GB/s以上であること。 ③ メモリクロックが133MHz以上であること。	必須						
(5) 補助記憶装置は，次の仕様を満たすこと。 ① 光学式ドライブを有していないこと。 ② 記憶容量が480GB以上のSSDを有すること。 ③ 政府推奨暗号と同等以上の暗号化機能を有すること。 なお，本機能の実現に当たり暗号化ソフトウェアを用いても差し支えない。 暗号化時に生成した鍵等については，端末の個体毎に整理し，甲で効率的に管理しやすくすること。また，暗号化と鍵の管理方法等については，暗号化の前に甲担当者と協議して甲の承諾を得た上で暗号化を実施すること。	必須						
(6) インタフェースは，次の仕様を満たすこと。 ① IEEE 802.3 規格に準拠した 10BASE-T/100BASE-TX/1000BASE-T に対応したネットワークインタフェースを1つ以上有していること。 ② USB2.0 インタフェースを2ポート以上，USB3.0インタフェースを1ポート以上有し，合計3ポート以上のUSBインタフェースを有すること。 なお，USB2.0 インタフェースを1ポート以上，USB3.0インタフェースを2ポート以上，又は，USB3.0インタフェースを3ポート以上であっても構わない。	必須						
(7) キーボード，ディスプレイ，マウスは，次の仕様を満たすこと。 ① JIS 配列もしくはOADG に準拠した日本語キーボード（テンキーボードを内蔵）であること。 ② 15.6型ワイドカラー液晶で，画面解像度1,920×1080ドット以上の表示機能を有すること。 ③ 外付けディスプレイ接続用として，HDMIのディスプレイインタフェースを一つ以上有していること。 ④ マウスは，USB接続可能で，総ボタン数（ホイールボタン機能を含む。）を3つ，スクロールホイール機能を有した光学式であること。	必須						
(8) ソフトウェア 次のソフトウェアをインストールし，適切にライセンス処理を行い，各機能が確実に動作可能な状態で提供すること。 ① 業務継続性，システムの運用効率性及び安定性の観点から現行のクライアント端末のOSと同じマイクロソフト社製Windows 10（64bit）とし，Pro以上であること。ただし，OSのサービス提供モデル（WaaS）は，SACに対応し，運用管理可能なこと。また，搭載するOSは，WSUSによるアップデート等の制御が可能なこと。 ② 業務継続性の観点から，クライアント端末で利用しているマイクロソフト社製Office Professional Plus 2016で作成した文書を継続的に使用でき，同等以上の性能・機能を有する製品の最新バージョンを搭載すること。 ③ その他，運用管理に必要なもの	必須						
(9) その他，次の仕様を満たすこと。 ① 製造事業者等において，法人向け製品として製造・販売されていること。 ② ワイヤロック等で端末本体の盗難防止が可能なこと。 ③ はめ込み式や，ねじ式などHDD（もしくはSSD）の着脱が簡便であること。	必須						
(10) 環境配慮に関して，省エネ法に基づくエネルギー消費効率について，省エネ基準達成率がAA 以上であること。	必須						
3.6.ディレクトリサーバ機能							
3.6.1.機能要件							
(1) 甲で利用する全てのWindows サーバ機器（Windows Server 2012 又は2016を搭載）及びWindowsクライアント端末（Windows 10を搭載。若干数WINDOWS7あり。）をディレクトリ・サービスにより一元管理する機能を有すること。	必須						左記について，理解した上で対応できるか。
(2) 本調達仕様書（案）「2.3.オペレーティングシステムの集約化」に従い，必要となる数量の CAL も調達すること。	必須						
(3) 管理下のWindowsサーバ，クライアント端末上のフォルダやファイルに対して，アクセス権が設定できること。	必須						
(4) 管理下のWindowsサーバ，クライアント端末に対し，ディレクトリ・サービスにより共通のポリシーを適用できること。	必須						
(5) 本調達仕様書（案）「3.8.ユーザ管理用サーバ機能」と連携すること。 なお，連携機能に関しては本調達仕様書（案）「3.8.1.機能要件」を参照すること。	必須						
(6) ユーザの認証失敗のログを取得可能なこと。	必須						
(7) 以下にDHCP要件を示す。 (ア) DHCP によるIP アドレス付与の機能を有すること。 (イ) 割り当てるIP アドレスの範囲が指定出来ること。 (ウ) サービス提供範囲に位置するクライアントからの要求に対して応答できる性能を有すること。 (エ) MACアドレスフィルタ機能を有すること。 (オ) DHCPサーバ機能を提供すること。	必須						
(8) 内部NTPサーバ機能を有し，宮内庁統合NWのDMZ用NTPサーバと時刻同期できること。	必須						
(9) ドメインユーザをProtected Usersグループに所属させることにより，NTLMハッシュがメモリに保存されないようにし，Pass-the-Hashによる攻撃を防ぐこと。	必須						
(10) Credential Guardの機能により，攻撃ツールが不正にメモリにアクセスし，ドメインユーザの認証情報が不正に窃取されることを抑止すること。	必須						
3.6.2.機器構成要件							
以下の要件を満たし，適切に動作する構成のサーバ機器等を宮内庁本庁及び京都事務所に設置し，適切に稼働させ，継続的な運用が可能な状態にすること。ただし，現行宮内庁NWSと異なり，本調達では全ユーザを宮内庁本庁サーバで一括処理することとし，京都事務所サーバは災害復旧を目的としたディザスタリカバリサイト（以下「DRサイト」という。）とすることでサイトでの機能分離を図り，バックアップ等に関する運用管理業務の軽減を図る。また，ファイルサーバ，ウイルス対策サーバ（クライアント端末用）も同様とする。 なお，宮内庁本庁サーバへのアクセスが途絶するような障害等が発生し，宮内庁本庁サーバが機能しなくなった場合には，その状態を京都事務所サーバが検知して宮内庁本庁サーバの役割を自動的に代行するようにし，業務継続性を向上させる。	必須						

評価対象	必須	加点	加点評価				評価基準
			特に優秀	優秀	標準	加点なし	
(1) 宮内庁本庁 (ア) 宮内庁の全ユーザが，サーバ機器等に同時アクセスした場合であっても業務を遅滞なく遂行可能とする処理性能を有する機器構成とする設計を行い，適切な設定を反映することによって確実に動作させること。 (イ) 本調達仕様書（案）「3.6.1.機能要件」に挙げる各機能を有し，本調達仕様書（案）「3.1.サーバ機能共通要件」を満たしたサーバ機器等を過不足なく用意すること。 (ウ) 宮内庁本庁に導入するサーバ機器等は，本庁サーバ室内での冗長化を行うこと。 なお，冗長化を行うサーバ機器等も本調達仕様書（案）「3.1.サーバ機能共通要件」を満たすこと。 (エ) 宮内庁本庁に導入するサーバ機器等のシステム領域及びデータ領域のリモート・バックアップを京都事務所で行うことが可能なこと。	必須						左記について，理解した上で対応できるか。
(2) 京都事務所 (ア) 宮内庁本庁に導入するサーバ機器等のシステム領域及びデータ領域のリモート・バックアップを行うことが可能なこと。 (イ) 前項でリモート・バックアップした内容は，バックアップ直後の1世代分に加えて過去2世代分，合計3世代のバックアップの保管を行うことが可能なこと。 (ウ) 宮内庁本庁に設置したディレクトリサーバ機能を搭載したサーバ機器等が，自然災害などにより利用できなくなった場合，京都事務所に設置したディレクトリサーバ機能を搭載したサーバ機器等がDRサイトとして機能し，宮内庁本庁に設置したディレクトリサーバ機能の代行を自動的に行い，ユーザの業務継続性を確保し，業務が遂行可能となる性能を有する機器構成とすること。 (エ) 本調達仕様書（案）「3.6.1.機能要件」に挙げる各機能を有し，本調達仕様書（案）「3.1.サーバ機能共通要件」を満たしたサーバ機器等を過不足なく用意すること。	必須						
3.7.特権ID管理機能							
特権IDは，非常に高い権限を持つことから，使用上，管理を厳格にする必要がある。特権IDで操作されるサーバ等，又は特権IDで操作する作業者，作業用クライアントPC等において，特権ID管理機能を導入し，特権IDのアクセス管理やトレーサビリティを確保することが重要である。具体的には，次の機能を有すること。	必須						
(1) 「誰が」「いつ」「どの特権ID」を「何のために利用」するのか，特権IDの利用申請により，承認後，特権IDが利用可能になること。	必須						
(2) 個人用IDを作業者に付与し，当該IDと特権IDとの紐付けを行うことで，特権IDを複数人で共用する場合でも個人用IDの操作ログから追跡可能であること。	必須						
(3) 作業者の全ての操作内容を記録すること。	必須						
(4) サーバOSに依存せず，UNIX系サーバ（Linux等）やWindowsサーバも操作ログを記録すること。	必須						
(5)特権ID管理機能を導入するに当たり，運用管理セグメント用端末に同機能を利用するためのソフトウェアのインストール・アンインストール，設定が必要になった場合は，甲を介して宮内庁統合NW受託者へ協力を依頼すること。ただし，宮内庁統合NW受託者へ協力を依頼するのは，2020年1月末日までとし，2020年2月1日以降は，乙が運用管理セグメント用端末を用いて運用管理業務を行う。	必須						
(6) 特権ID管理機能から出力されるログ等があり，宮内庁統合NW受託者が導入するSOCサービスにおいて，それらを利用したい場合かつ乙による詳細設計書の最終確定以前の場合には，必要となるログ等の仕様を宮内庁統合NW受託者の責任で明らかにした上で甲と協議をして承諾を得た後，甲を介して乙に利用の依頼がなされるので，乙はそれに協力すること。	必須						
(7) 管理対象となる機器は以下を想定すること。また下記の（ア）から（ケ）に示すサーバ群で管理対象とするアカウントは原則としてOSの特権IDを対象とすること。その他，各種アプリケーションやミドルウェアの特権IDや，下記の（コ）に示すサーバでも特権ID管理の対象とする方が望ましいアカウントがある場合は，甲と協議の上，対応可能であると合意したものは対象とすること。 (ア) ディレクトリサーバ (イ) ファイルサーバ (ウ) ユーザ管理用サーバ (エ) 電子メール中継サーバ (オ) ウイルス対策サーバ (カ) バックアップサーバ (キ) プロキシサーバ (ク) 内部 DNS サーバ (ケ) WSUS サーバ (コ) その他，本調達及び宮内庁統合NWに導入するUNIX系サーバ（Linux等）やWindowsサーバ (7) 管理対象となる機器は以下を想定すること。また下記の（ア）から（ケ）に示すサーバ群で管理対象とするアカウントは原則としてOSの特権IDを対象とすること。その他，各種アプリケーションやミドルウェアの特権IDや，下記の（コ）に示すサーバでも特権ID管理の対象とする方が望ましいアカウントがある場合は，甲と協議の上，対応可能であると合意したものは対象とすること。 (ア) ディレクトリサーバ (イ) ファイルサーバ (ウ) ユーザ管理用サーバ (エ) 電子メール中継サーバ (オ) ウイルス対策サーバ (カ) バックアップサーバ (キ) プロキシサーバ (ク) 内部 DNS サーバ (ケ) WSUS サーバ (コ) その他，本調達及び宮内庁統合NWに導入するUNIX系サーバ（Linux等）やWindowsサーバ	必須						
(8) 特権IDの利用状況についてレポートを出力することが可能なこと。	必須						
(9) 万一，特権ID管理の仕組みに障害等が発生しても，速やかに復旧し特権IDでログインできる仕組みを有すること。	必須						
(10)甲担当者が簡便に操作可能なユーザインタフェースを有すること。また，甲担当者が利用するための手引き書を整備すること。	必須						
3.8.ユーザ管理用サーバ機能 **3.8.1 機能要件**							
(1) 本機能は，本調達仕様書（案）「3.6.ディレクトリサーバ機能」，「3.14.ファイルサーバ機能」及び「グループウェアサーバ機能（本調達システムには含まれていない既存システム）」と連携し，アカウント情報（ユーザID）を一元的に管理し，以下の機能を実現すること。 なお，現行でのユーザ管理用サーバ機能と連携するサーバ機能のシステム構成概要図に関連した文書（設計，設定，承認フロー等）について閲覧を希望する者は，甲に閲覧申請を行い，甲の許可を得た上で閲覧可能とする。	必須						
① ユーザ管理機能 (ア) 職員管理機能 ○ 文書取扱主任（「宮内庁行政管理文書管理細則（平成23年4月1日総括文書管理者決定）」で定義されている。）による申請（新規，修正，削除）機能（担当文書取扱主任のみに制限），情報係の申請承諾機能，情報管理室の処置機能（バッチ指示，ファイル出力），バッチ処理，申請，承認時の次処理者への処理依頼メール通知機能を有すること。 ○ 甲にIDを持つユーザに関する情報（個人ID，ユーザ名，組織名，職位等）を管理すること。 ○ 文書取扱主任にて，ユーザの新規登録・修正・削除の依頼（以下「登録依頼」という。）が行えること。 ・文書取扱主任による登録依頼は電子メールにて甲担当者に通知されること。 ○ 文書取扱主任による依頼を情報係にて確認後，承認又は取消ができること。 ・甲担当者にて承認された登録依頼は電子メールにて情報管理室に通知されること。 ・甲担当者にて取り消された登録依頼は電子メールにて文書取扱主任に通知されること。 ○ 甲担当者にて承諾された依頼について，情報管理室にて本調達仕様書（案）「3.7.ディレクトリサーバ機能」「3.14.ファイルサーバ機能」及び「グループウェアサーバ機能（本調達システムには含まれない。）」への登録処理を行えること。 ・バッチ処理対象の依頼を指定日にデータベースに反映できること。	必須						
(イ) 職位管理機能 ・職位に関する情報（職位ID，職名等）を管理すること。	必須						
② ID管理機能 (ア) CSVファイルによるユーザアカウントの一括管理機能を有すること。また，任意のフォルダに保存されたCSVファイルの取り込みが可能であり，更に任意のフォルダに CSV ファイルを出力が可能なこと。 なお，ユーザアカウントの初期登録におけるCSVファイルは甲が乙に提示するものとする。	必須						
(イ) ユーザアカウントの作成時にパスワードを自動生成（初期パスワード作成）可能なこと。また，パスワードの強度（長さ・文字の種類等）を設定可能なこと。	必須						
(ウ) 本調達仕様書（案）「3.7.ディレクトリサーバ機能」と連携し，ディレクトリサーバ機能に対してユーザアカウント作成・変更・削除，アクセス権の設定・変更等が可能なこと。	必須						
(エ) グループウェアサーバ機能（本調達には含まれていない既存システム）と連携できること。	必須						
(オ) 本調達仕様書（案）「3.6.ディレクトリサーバ機能」に対して，セキュリティグループを作成できること。また，ユーザの属性情報を自動的に認識し，該当するセキュリティグループに所属させることが可能なこと。	必須						
(カ) 本調達仕様書（案）「3.6.ディレクトリサーバ機能」のユーザアカウント作成時に，本調達仕様書「3.14.ファイルサーバ機能」へユーザのフォルダ（ホームフォルダ）を作成できること。また，ユーザアカウントの削除時に，このフォルダを削除可能なこと。	必須						
(キ) 本調達仕様書（案）「3.14.ファイルサーバ機能」にフォルダ（共有フォルダ）を作成できること。また，フォルダに（エ）で作成したセキュリティグループを割り当てるとともにアクセス権を設定可能なこと。または，AD側の アクセス権設定で実施でも構わないものとする。	必須						
(ク) ユーザの属性情報を自動的に識別し，既存グループウェアサーバ機能のアクセス権を設定可能なこと。	必須						
(ケ) 指定した日時にユーザアカウントが自動的に作成可能なこと。	必須						
(コ) ユーザアカウントに有効期限を設け，期限を超過したユーザアカウントを自動的に無効化又は削除可能なこと。また，管理者にその旨を通知すること。	必須						
(サ) ワークフロー（申請～承認）により，ユーザアカウントを新規作成・変更・削除できること。また，申請者や承認者に電子メールで通知すること。	必須						
(シ) ユーザアカウントの情報をCSV等の可読可能なフォーマットで外部出力する機能を有すること。	必須						
(ス) 本調達仕様書（案）「3.6.ディレクトリサーバ機能」及び既存グループウェアサーバ機能ごとにユーザアカウントの登録状況を一覧表形式で確認できること。	必須						

評価対象	必須	加点	加点評価				評価基準
			特に優秀	優秀	標準	加点なし	
(セ)　管理者が強制的にユーザアカウントのパスワードをリセットする機能を有すること。	必須						
(ソ) ユーザアカウントのパスワードは暗号化を施し，管理・保存することが可能なこと。	必須						
(2) ユーザ管理用サーバ機能利用のためのアクセスについては，以下のとおりとする。 ① 操作画面は GUI (Graphical User Interface)により，簡便で効率的なアクセス，設定及び管理操作が可能なこと。 ② 管理者のみがユーザ管理用サーバ機能へのアクセスが可能となるアクセス管理機能を有すること。 ③ 管理者の操作履歴を保存し，これを参照可能なこと。	必須						
(3) 本機能は本調達仕様書（案）「3.14.ファイルサーバ機能」と連携し，宮内庁行政文書管理規則（平成23年宮内庁訓令第5号）及び宮内庁行政文書管理細則に準じたフォルダ階層，アクセス管理ができること。	必須						
3.8.2.機器構成要件							
次の要件を満たし，適切に動作する構成のサーバ機器等を本庁サーバ室のみに設置すること。 (1) 本調達仕様書（案）「3.8.1.機能要件」に挙げる各機能を有し，本調達仕様書「3.1.サーバ機能共通要件」を満たしたサーバ機器等を過不足なく用意すること。	必須						左記について，理解した上で対応できるか。
3.9.内部DNSサーバ機能							
3.9.1.機能要件							
(1) DNSサーバ機能を有し，名前解決ができること。	必須						左記について，理解した上で対応できるか。
3.9.2.機器構成要件							
次の要件を満たし，適切に動作する構成のサーバ機器等を本庁サーバ室のみに設置すること。 (1)　本調達仕様書（案）「3.9.1.機能要件」に挙げる各機能を有し，本調達仕様書（案）「3.1.サーバ機能共通要件」を満たしたサーバ機器等を過不足なく用意すること。	必須						左記について，理解した上で対応できるか。
3.10.WSUSサーバ機能							
3.10.1.機能要件							
(1)　管理対象機器は，甲が運用する全てのWindowsサーバ機器，端末とすること。	必須						
(2)　管理対象機器に対し，修正プログラムや累積的セキュリティ更新プログラムを自動的に配信できる機能を実現すること。	必須						
(3)　管理対象機器に対し，ウイルス対策ソフトのパターン定義ファイルを配信し，端末個別に配信状況（配信日時，配信有無，パターン定義ファイルのバージョン等）を管理できること。	必須						左記について，理解した上で対応できるか。
(4) 管理対象機器に対し，ウイルス対策ソフトによる保護状態（有効／無効）を管理できること。	必須						
(5)　マルウェア検知時，管理画面から検知された機器を特定できるとともに，検知されたマルウェアの情報を確認できること。	必須						
(6) マルウェア検知時，検知された端末に警告画面を表示するとともに，甲担当者へ警告メールを発信すること。	必須						左記について，理解した上で対応できるか。
3.10.2.機器構成要件							
次の要件を満たし，適切に動作する構成のサーバ機器等を本庁サーバ室のみに設置すること。 (1)　本調達仕様書（案）「3.10.1.機能要件」に挙げる各機能を有し，本調達仕様書（案）「3.1.サーバ機能共通要件」を満たしたサーバ機器等を過不足なく用意すること。	必須						左記について，理解した上で対応できるか。
3.11.バックアップサーバ機能							
3.11.1.機能要件							
(1) バックアップ対象は，各サーバ機能のシステム領域及びデータ領域とし，ネットワークを介して原則オンラインにてバックアップを取得できること。ただし，システムから切り離して行う作業を行わない場合は必ず行うこと。	必須						
(2) 宮内庁NWSに負荷をかけるおそれがある場合は，バックアップ用のネットワークセグメントを配置すること。なお，宮内庁WANを介してのバックアップを行うことを提案する場合は，宮内庁WANの構成及び各回線の帯域幅を考慮し，宮内庁WANを利用したユーザの業務に支障ないような設計とすること。	必須						
(3) バックアップ取得中，バックアップ対象サーバ機能を原則停止しないこと。ただし，システムから切り離して行う作業を行わない場合は必ず行うこと。	必須						
(4) スケジュールに基づいたバックアップが自動でできること。また，年末年始等の長期休暇を想定し，甲の業務状況にあわせ，手動又は任意のスケジュールによるバックアップもできること。 なお，本調達システムの運用におけるバックアップのスケジュール等については，甲と管理者との協議の上で決定するものとするが，管理者において有益と考察される提案を行うこと。	必須						
(5) フルバックアップ及び差分バックアップができること。 なお，現行システムにおいては，フルバックアップを毎週金曜日の夜，差分バックアップは毎日行っている。	必須						
(6) バックアップが失敗した場合，バックアップ処理をリトライできること。	必須						
(7) ファイル及びフォルダ単位並びにサーバ単位のいずれかの場合においてもリストアできること。	必須						
(8) バックアップを取得したサーバ以外のサーバからもリストアの操作ができること。	必須						
(9) バックアップのメディアの世代管理ができること。 ① イメージバックアップは3世代以上保管できること。 ② データバックアップは3週間以上保管できること。	必須						
(10) システム領域を復旧するためのバックアップメディア（以下「システム領域復旧メディア」という。）を作成できること。 なお，システム領域復旧メディアの種類は DVD や USBメモリ等の汎用性が高いメディアとすること。また，納品時点でのシステム領域復旧メディアの作成は乙が行うこととし，この時必要となるメディアは乙の負担において過不足なく用意すること。	必須						
(11) システム領域のリストアは，OSをはじめからインストールすることなく，システム領域復旧メディアから起動しリストアできるよう，作業の効率化を図り，短時間での障害復旧ができること。	必須						
3.11.2.機器構成要件							
次の要件を満たし，適切に動作する構成のサーバ機器等を各拠点に設置すること。 なお，「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）を踏まえ，平常時の情報システム設置拠点と同時被災しないことが想定される場所にバックアップシステムを確保する等の措置を講ずることとし，本庁サーバ室のリモート・バックアップ拠点を京都事務所とする。	必須						左記について，理解した上で対応できるか。
(1) 宮内庁本庁 ① 本調達仕様書（案）「3.11.1.機能要件」に挙げる各機能を有し，本調達仕様書（案）「3.1.サーバ機能共通要件」を満たしたサーバ機器等を過不足なく用意すること。	必須						
②本庁サーバ室に設置された機器についてのバックアップ対象となるサーバ機能は，以下のとおり。 (ア)　ディレクトリサーバ機能 (イ)　ファイルサーバ機能 (ウ)　ユーザ管理用サーバ機能 (エ)　電子メール中継サーバ機能（宮内庁統合NWに含まれる。） (オ)　ウイルス対策サーバ機能 (カ)　ネットワーク運用管理機能 (キ)　サーバ運用管理機能 (ク)　CADサーバ機能（本調達システムには含まれていない既存システム）	必須						
③ 前項②においてバックアップされた機能の全てをリモート・バックアップ拠点である京都事務所でもバックアップを保存できること。	必須						
(2) 京都事務所 ① 本調達仕様書（案）「3.11.1.機能要件」に挙げる各機能を有し，本調達仕様書（案）「3.1.サーバ機能共通要件」を満たしたサーバ機器等を過不足なく用意すること。	必須						
② 3.11.2.(1)③記載のとおり，宮内庁本庁のバックアップされた機能の全てをリモート・バックアップ拠点である京都事務所でも保存できること。	必須						
3.12.ウイルス対策サーバ機能							
3.12.1.機能要件							
(1) サーバ及びクライアント端末に，オンライン及びオフラインスキャン可能なウイルス対策ソフトを導入すること。また，定期的に自動でパターンファイルや検索エンジン等の更新，フルスキャンを行うこと。	必須						
(2) クライアント端末のウイルス対策ソフトは，当庁で平成28年度に更新したSKYSEA Client View(GL)と連携可能なウイルス対策ソフトから選定すること。例えば，SKYSEA Client View(GL)標的型攻撃対策ログ収集機能により，ウイルス対策ソフトと連携しウイルスを検知したクライアント端末をネットワークから自動的に遮断する対策を講じている。	必須						
(3) 多層型防御の観点から，サーバ及びクライアント端末のウイルス対策ソフトは，ウイルス対策ルール又はパターンファイルの公開時期のずれなどによる対策の遅れを吸収するため，異なる製造業者の製品を導入すること。	必須						
(4) クライアント端末では，シグネチャ型ウイルス対策ソフトとふるまい検知等の技術を用いるウイルス対策ソフトを組み合わせることにより，ウイルス感染リスクの低減を図ること。 なお，ふるまい検知型ウイルス対策ソフトは，クライアント端末への負荷による業務への影響を抑えた製品を提供すること。	必須						
3.13.ログ収集サーバ機能							
3.13.1.機能要件							
(1)　ログ受信方式として，Syslog，SNMP，Windowsのファイル共有又はSPC転送のいずれかに対応し収集対象となる機器群から必要なログを収集することが可能なこと。	必須						
(2)　ログ収集の対象として，各サーバのOS等のイベントログ及び監査ログに対応していること。	必須						

評価対象	必須	加点	加点評価 特に優秀	加点評価 優秀	加点評価 標準	加点評価 加点なし	評価基準
(3) 各機器が出力するイベントログは，そのままの形式では内容の理解が困難であるが，インシデント等の発生時に対応を行うに当たってログ解析等を迅速に行うために，収集したログの視認性，可読性及び判読性の全てを向上させる機能を有すること。	必須						左記について，理解した上で対応できるか。
(4) インシデント等の発生時に対応を行うに当たってログ解析等を迅速に行うために，次に示す検索条件を指定しての検索が可能なこと。また，検索条件の保存が可能なこと。 (ア) 自由なキーワードを指定しての検索 (イ) ログ発生元のサーバ，機器を指定しての検索 (ウ) アプリケーションを指定しての検索 (エ) IPアドレスやユーザ名などを指定しての検索 (オ) syslog の facility(auth, cron, mailなど)を指定しての検索 (カ) syslog の priority(info, warn, errなど)を指定しての検索 (キ) プロセスIDを指定しての検索	必須						
(5) 前項(4)に示した検索条件を AND 及び OR を組合せての検索が可能なこと。	必須						
(6) 異なるシステム・フォーマットのログを統合した横断検索が可能なこと。	必須						
(7) 前項(4)～(6)の検索結果を，CSV形式でのファイル出力が可能なこと。	必須						
(8) 検索結果で表示されたログに対し，マウスのクリック操作等による絞込検索によって，ログの追跡（トラッキング）が可能なこと。	必須						
(9) 収集したログに対し，グラフ形式や表形式での出力などが可能な集計機能を有すること。	必須						
(10) 検索機能及び集計機能で保存した各条件を基にし，定期的かつ自動的にレポートを出力することが可能なこと。また，レポートの定期自動出力は，日次，週次，月次で可能なこと。	必須						
(11) 収集したログの項目に対し，独自の意味付け及びタグ付けを行うことが可能なこと。	必須						
(12) 収集したログが改ざんされないような仕組みを具備すること。	必須						
(13) 収集したログに対し，暗号化して保管することが可能なこと。	必須						
(14) 収集したログに対し，圧縮を施して保管することが可能なこと。	必須						
(15) 収集したログのバックアップが可能なこと。	必須						
(16) 既存資産を有効活用して費用対効果を高めつつ情報セキュリティ対策を強化するため，SkySea との連携が可能であること。	必須						
3.13.2.機器構成要件							
(1) 本調達仕様書（案）「3.14.1.機能要件」に挙げる各機能を有し，本調達仕様書（案）「3.1.サーバ機能共通要件」を満たしたサーバ機器等を過不足なく用意すること。	必須						左記について，理解した上で対応できるか。
(2) ログ収集サーバに搭載された補助記憶装置は，運用中でも増設可能とし，容量の拡張が可能なこと。	必須						
(3) ログ収集の対象となる機器は，次のとおり。ただし，次の（ア）～（エ）については，宮内庁本庁及び京都事務所の両方に設置したサーバが対象となる。 (ア) ディレクトリサーバ (イ) ファイルサーバ (ウ) バックアップサーバ (エ) プロキシサーバ (オ) ユーザ管理用サーバ (カ) 電子メール中継サーバ (キ) ウイルス対策サーバ (ク) WSUSサーバ (ケ) フェデレーション(ADFS)サーバ ※グループウェアシステムに含まれる。 (コ) 特権ID管理サーバ (サ) 内部DNSサーバ	必須						左記について，理解した上で対応できるか。
(4) 収集したログについて，ログ収集サーバ上での保存期間は，「適切なログの管理による標的型攻撃対策について（情報提供）（閣副安危第 375 号，平成24年7月5日）」「政府機関における情報システムのログ取得・管理の在り方の検討に係る調査報告書（内閣官房情報セキュリティセンター，平成24年3月）」に基づき，原則1年間とし，ログ収集サーバに搭載された補助記憶装置の容量を十分に用意すること。	必須						
(5) 次に示す要件を満たすログ用外部バックアップ装置を用意すること。また，収集したログについて，ログ収集サーバ上での保存が1年間分蓄積された時点で，ログ用外部バックアップ装置への退避を行うこと。 (ア) ログ収集サーバに搭載された補助記憶装置に保存された1年間分のログデータについて，3世代分以上の保存が可能な容量を有すること。 (イ) USB3.0以上のシリアルバス規格又は1Gbps以上の帯域を有するイーサネット規格等のインタフェースでログ収集サーバとの接続が可能なこと。 (ウ) 可搬可能なコンパクト設計であること。 (エ) 自動暗号化機能を有すること。なお，暗号化については，AES256bit又はそれ相当以上の暗号強度であること。	必須						
3.14.ファイルサーバ機能							
3.14.1.機能要件							
(1) 本調達仕様書（案）「3.6.ディレクトリサーバ機能」により，フォルダやファイルに対してアクセス権が設定できること。	必須						左記について，理解した上で対応できるか。
(2) ファイルサーバ上に保存されている共有フォルダやファイルは本調達仕様書（案）「3.11.バックアップサーバ機能」により，定期的にバックアップが取得できること。	必須						
(3) 本調達仕様書（案）「3.8.ユーザ管理用サーバ機能」と連携し，宮内庁行政文書管理規則及び宮内庁行政文書管理細則に準じたフォルダ階層とアクセス管理ができること。なお，連携機能に関しては本調達仕様書「3.8.1.機能要件」を参照すること。また，宮内庁行政文書管理規則について閲覧を希望する者は，甲に閲覧申請を行い，甲の許可を得た上で閲覧可能とする。	必須						
(4) 庁内ポータルサイト機能 ユーザが行政事務の参考となる情報や資料を提供するため，次に挙げる各機能を有すること。 ページ構成，編集もシンプルなUIとし，ユーザが利用しやすい画面にすること。 ① ユーザがWebブラウザを介して，情報や資料の参照，検索ができること。 ② 甲の部局からのお知らせに利用可能なCMSページを整備すること。 ③ 運用開始時は21部局分のページを用意すること（詳細は契約締結後に甲より提示する）。 ④ 各部局における掲示板については，各部局に所属するユーザのみが利用可能となるよう，ユーザの属性情報に基づく利用制限を行うことが可能なこと。また，ユーザの異動に伴って利用可能又は利用制限する掲示板を適切に変更することが可能なこと。 ⑤ ページ構成は，次のとおりとする。 ・ 各部局からのお知らせ ・ 各部局掲示板 ・ 職員録・電話帳へのリンク ・ 各種マニュアル・申請書へのリンク ・ 外部システム，サイト等へのリンク	必須						左記について，理解した上で対応できるか。
		加点	100	50	25	0	本要件を実現するための技術要素，実現方針，作業プロセスや管理方法等を，その根拠と効果も含めて具体的に示されていれば，加点とする。
3.14.2.機器構成要件							
以下の要件を満たし，適切に動作する構成のサーバ機器等を各拠点に設置すること。 (1) 宮内庁本庁 ① 本調達仕様書（案）「3.14.1.機能要件」に挙げる各機能を有し，本調達仕様書（案）「3.1サーバ機能共通要件」を満たしたサーバ機器等を過不足なく用意すること。 ② 前項①とは異なるサーバ機器等にて，本機能の冗長化を行うこと。なお，冗長化を行うサーバ機器等も本調達仕様書（案）「3.1.サーバ機能共通要件」を満たすこと。	必須						左記について，理解した上で対応できるか。
3.15.振る舞いログ分析（UEBA）サーバ							
各機器からSyslog等で送信されるログを集中的に管理し利用者に紐づいた異常な振る舞いを分析することができるサーバ。ログの集中管理対象としては，本調達で導入する機器だけでなく，その他の宮内庁NWSのサーバ群（ADサーバなど）も解析対象とする。必要な要件については次のとおり。	必須						左記について，理解した上で対応できるか。
3.15.1.攻撃検知等要件							
以下に記載の攻撃を検知することができること。	必須						左記について，理解した上で対応できるか。
(1) リモートアクセスユーザが複数の拠点から同時にアクセスをしている。	必須						
(2) リモートアクセスユーザが普段とは異なる場所からアクセスをする。	必須						
(3) 社内の端末から社外のサイトに対して，頻度の高いアクセスが発生する。	必須						
(4) 社内の端末から他の社内の端末やサーバに対して，頻度の高いアクセスが発生する。	必須						
(5) 特権アカウントへの切り替えが頻繁に繰り返される。	必須						
(6) サーバに対して普段アクセスをしないユーザからのアクセスがある。	必須						
(7) 普段利用していない端末からログインがされる。	必須						
(8) 通常のログイン時間やログイン場所とは明らかに異なる時間や場所から繰り返しログインがされる。	必須						

評価対象	必須	加点	加点評価 特に優秀	加点評価 優秀	加点評価 標準	加点評価 加点なし	評価基準
(9) ログイン失敗のアカウントが非常に多い。	必須						
(10) ユーザが通常アクセスを行わないファイルサーバに保管されているファイルに対してアクセスを行い，正式に利用が認められていない外部のDropboxやGoogle drive等のクラウドストレージへアップロードし，外部サーバへデータを持ち出す。	必須						
3.15.2.分析要件							
収集したログをもとに以下の観点から分析できること。	必須						左記について，理解した上で対応できるか。
(1) 単純分析：単一のログをもとにインシデントの検知。	必須						
(2) 相関分析：複数のログをもとにインシデントの検知。 最低限次のログを対象に相関分析が可能なこと。 ・ADのログ，ウイルス対策ソフトのログ，プロキシサーバのログ，メール送受信のログ，VPNのログ 上記以外にも設計時に甲と協議の結果，取り込むことが有意義と考えられるログについては，サーバの容量を勘案した上で，取り込みを行うこと。	必須						
(3) 閾値分析：定められた閾値をもとにインシデントの検知。	必須						
(4) 振舞分析：通信や利用者の振る舞いをもとにインシデントの検知。各端末および各利用者の通常の振舞を1日単位で定義・分析し，通常の行動とは異なる行動が発生した場合に検知できること。	必須						
3.15.3.設定要件							
乙は，振る舞いログ分析（UEBA）サーバの解析機能が充分に発揮できるよう，宮内庁における情報システムとその利用実態について，充分な理解に努めた上で，3.15.1.攻撃検知要件及び3.15.2.分析要件を定めるに当たり，適切に設定して，甲の承諾を得ること。また，運用開始後6か月程度を目途に改めて設定の見直しを行い，その後も，設定変更の必要又は甲の求めに応じて，適宜設定の見直しを行うこと。	必須						左記について，理解した上で対応できるか。
3.15.4.負荷軽減							
セキュリティ分析の負荷を低減するため以下の機能を提供すること。	必須						左記について，理解した上で対応できるか。
(1) セキュリティインシデントの予兆検知は可能な限り自動化されること。	必須						
(2) 機械学習（教師なし）により，平常時の行動パターンをもとに，ユーザごとに振舞のベースラインが自動的に作成され，更新もされること。	必須						
(3) 特定のユーザに対し異常時のタイムラインだけではなく，正常時のタイムラインと比較を行いユーザの振舞を分析・報告可能なこと。また，タイムラインはユーザ単位で表示，分析ができること。	必須						
(4) 担当者が製品特有のクエリ言語/Search文による分析といった専門知識を用いず，標準で提供される選択項目を選択することにより容易にログの検索ができること。	必須						
(5) ログの検索や分析の結果が図や表といった視覚的なインタフェースで出力されること。	必須						
(6) インシデント検知時は，自動的に管理画面及びメールで警告を通知すること。	必須						
(7) インシデント検知時は，管理画面に検知した脅威に対してスコア（点数）表示することにより，対処の優先順位が判断しやすいこと。	必須						
3.15.5.機器構成要件							
(1) 本調達仕様書（案）3.15.1.～3.15.4に挙げる各要件を有し，本調達仕様書（案）「3.1.サーバ機能共通要件」を満たしたサーバ機器等を過不足なく用意すること。	必須						左記について，理解した上で対応できるか。
(2) 振る舞いログ分析（UEBA）サーバに搭載された補助記憶装置は，運用中でも増設可能とし，容量の拡張が可能なこと。	必須						
(3) 収集したログについて，振る舞いログ分析（UEBA）サーバ上での保存期間は，「適切なログの管理による標的型攻撃対策について（情報提供）（閣副安危第 375 号，平成24年7月5日）」「政府機関における情報システムのログ取得・管理の在り方の検討に係る調査報告書（内閣官房情報セキュリティセンター，平成24年3月）」に基づき，原則1年間とし，ログ収集サーバに搭載された補助記憶装置の容量を十分に用意すること。	必須						
(4) 次に示す要件を満たすログ用外部バックアップ装置を用意すること。また，収集したログについて，振る舞いログ分析（UEBA）サーバ上での保存が1年間分蓄積された時点で，ログ用外部バックアップ装置への退避を行うこと。 (ア) 振る舞いログ分析（UEBA）サーバに搭載された補助記憶装置に保存された1年間分のログデータについて，3世代分以上の保存が可能な容量を有すること。 (イ) USB3.0で振る舞いログ分析（UEBA）サーバと接続が可能なこと。 (ウ) 可搬可能なコンパクト設計であること。 (エ) 自動暗号化機能を有すること。 なお，暗号化については，AES256bit又はそれ相当以上の暗号強度であること。	必須						
3.15.6.その他要件							
(1) UEBA機能を導入するに当たり，運用管理セグメント用端末に同機能を利用するためのソフトウェアのインストール・アンインストール，設定が必要になった場合は，甲を介して宮内庁統合NW受託者へ協力を依頼すること。ただし，宮内庁統合NW受託者へ協力を依頼するのは，2020年1月末日までとし，2020年2月1日以降は，乙が運用管理セグメント用端末を用いて運用管理業務を行う。	必須						左記について，理解した上で対応できるか。
(2) UEBA機能から出力されるログ等があり，宮内庁統合NW受託者が導入するSOCサービスにおいて，それらを利用したい場合かつ乙による詳細設計書の最終確定以前の場合には，必要となるログ等の仕様を宮内庁統合NW受託者の責任で明らかにした上で甲と協議をして承諾を得た後，甲を介して乙に利用の依頼がなされるので，乙はそれに協力すること。	必須						
4. 資産管理サーバの資産管理ソフトウェアのバージョンアップグレード作業							
当庁で使用している資産管理ソフトウェアは，平成28年度に「パーソナルコンピュータ及びサーバ等の賃貸借及びサーバ等保守」として，政府調達（WTO）対象の一般競争入札を行い，2017年3月1日から2021年2月28日までの48か月間（国庫債務負担行為）の賃貸借及び保守契約を締結し運用している。また，パーソナルコンピュータ及びサーバの更新作業を2020年度中（2021年3月より運用開始予定）に実施する予定である。 上記の間，資産管理ソフトウェアを最新のバージョンへとアップグレードすることにより，資産管理サーバ及びクライアント端末約1,200個を，宮内庁NW上で遜色なく動作させること。作業は契約期間中に最大で4回実施するものとするが，宮内庁NWSへの影響を鑑み，実施要否及び実施時期については甲乙協議の上で決定する。役務内容については次のとおり。	必須						左記について，理解した上で対応できるか。
(1) 乙は，納入までに事前準備として必要なハードウェア及びソフトウェアは乙の負担で準備すること。	必須						
(2) 乙は，本業務の事前稼働検証，ソフトウェアのインストール及び環境設定，動作確認等の作成等を行うに当たり，当該各作業の実施前には，十分な時間的余裕をもって甲と調整し，各作業工程表を提出し，甲の承諾を得ること。	必須						
(3) 本業務の実施に当たり，資産管理サーバを除く各既存システムの業務に影響を与えないこと。	必須						
(4) 本業務の実施に当たり，関係事業者の協力を得る場合は，甲担当者及び関係事業者と協議し，乙の負担において実施すること。ただし，作業実施予定日の5日前までに乙が作業内容（設定，手順等）を甲に具体的に説明した上で，通常の保守業務又は運用管理業務の範囲内の作業と認められる場合には，甲担当者を介し，甲担当者の指示として当該作業を現行事業者に通常業務として依頼することができる。	必須						
(5) 本業務に必要な機器及び消耗品等は，全て乙の責任と負担において用意し，実施すること。	必須						
(6) 本業務の実施に当たり，乙は，業務全般を掌握し，本業務の実施に当たる者を指揮監督する業務管理責任者及びこれを補佐する者(以下「業務管理責任者等」という。）を選任し，該当者の資格，経験及び国籍を証明する書面を提出の上，契約後10日以内に甲の承諾を得ること(変更する場合においても同じ。)。	必須						
(7) 業務管理責任者等は業務の進捗状況全体を把握し，甲に対して内容及び結果を定期的に報告すること。また，甲からの業務等に対する問合せに対し，業務管理責任者等は速やかに対応するとともに，各工程の終了時には，その作業結果について甲の承諾を得ること。	必須						
(8) 甲から乙に対する指示，協議申し出は，全て，(6)で選任された業務管理責任者等を通じて行うものとする。	必須						
(9) 本業務の実施に当たり，稼働中の各既存システムに対して不具合や問題を生じさせた場合は，乙の責任と負担において適切に対応し，是正すること。	必須						
(10) ユーザの作業が発生する場合は，あらかじめ甲に協議の上，その承諾を得ること。	必須						
(11) 本業務は，原則として，平日の業務時間（8:30～17:45）に実施すること。ただし，サーバ等各既存システムに影響を与える作業の場合は，ユーザの業務が停止しないよう，原則として，休日又は平日の業務時間（8:30～17:45）以外を利用し，実施すること。いずれの場合も事前にその工程及び作業方法について，甲の承諾を得ること。 なお，国会開会時には，システム停止が許容されない場合がある。	必須						
(12) 本業務に当たり，既存環境に設定，ツール等のインストールが必要となる際には，甲及び関係事業者に設計等の情報を開示するとともに甲からの指示に従うこと。 なお，別途機器が必要な場合は，乙の責任と負担において適切な情報セキュリティ対策と設定を施した上で安全に導入すること。	必須						
(13) 作業に際しては，甲担当者及び端末賃貸借保守事業者と必要な調整を行い，乙の責任と負担において，作業を実施すること。また，実施に当たり甲及び端末賃貸借保守事業者との調整に伴い発生する費用は，乙が負担すること。	必須						
(14) 作業実施前に資産管理サーバのシステムバックアップを取得すること。	必須						
(15) 資産管理サーバに甲が指定する資産管理ソフトウェアのバージョンアップグレード作業を実施すること。	必須						
(16) 甲が指定するクライアント端末に対し，甲が指定する資産管理ソフトウェアのバージョンアップグレード作業を実施すること。	必須						
(17) (15)及び(16)のバージョンアップグレード完了後に，正常に動作することを数台程度確認すること。	必須						
(18) (17)にて正常に動作することを確認できなかった場合には，切り戻しを実施し，原因を確認した後，甲に報告すること。	必須						
(19) (17)にて正常に動作することを確認できた場合には，甲が指定するクライアント端末にバージョンアップグレードを実施すること。	必須						
5. 宮内庁NWSの運用管理業務に係る請負業務内容							
5.1.請負範囲							
運用管理業務における請負者として，関係事業者並びに宮内庁統合NW受託者と密に連携しつつ，公共サービス改革法の第1条，趣旨と目的に基づいて民間事業者の創意と工夫による次期宮内庁NWSの運用管理業務を柔軟かつ確実に実施し，甲におけるITガバナンス及び情報セキュリティガバナンスの強化に努めること。具体的には，以下のとおりとし，それぞれに対して具体的な方針や実現方法などを示すこと。	必須						
(1) 運用管理業務を行う場合において，運用管理セグメントでの作業を行う際には，運用管理セグメント用端末を用いること。	必須						

評価対象	必須	加点	加点評価 特に優秀	加点評価 優秀	加点評価 標準	加点評価 加点なし	評価基準
(2) 次期宮内庁NWSの運用管理業務には，次に挙げる宮内庁統合NWに含まれるサービスは対象外とする。 ・ SOC ・ 宮内庁WAN ・ インターネット接続回線サービス（インターネット接続機器を除く） なお，詳細については別紙4を参照すること。 ただし，日常の運用管理業務の円滑な遂行及び障害やインシデントへの迅速な対応のため，甲担当者や運用管理業務の対象となるハードウェア及びソフトウェア等の製造事業者等との連携だけでなく，安定的で良質な運用管理業務を行うのに必要なログ等の情報共有を，甲の承諾を得た上で，必要に応じて宮内庁統合NW受託者と互いに行うこと。	必須						それぞれの項目を理解した上で，具体的な提案を示せるか。
(3) 宮内庁NWSにおいて，障害やインシデントが発生した場合，乙は，甲担当者，運用管理業務の対象となるハードウェア及びソフトウェア等の製造事業者等，甲の承諾を得た上で，必要に応じて宮内庁統合NW受託者と密な連携をすることにより，迅速な解決を図り，甲の事務が極力遅滞なく遂行可能な状態に復帰させることに努めること。	必須						
(4) 本調達に先行する宮内庁統合NWの調達の構築期間中に，甲の承諾を得た上で宮内庁統合NWの基本設計書及び詳細設計書を必ず精読して理解し，甲を介して宮内庁統合NW受託者と協議を行い，それぞれが互いに効率的に連携して安定的で良質な運用管理業務を実施可能な運用管理設計を行うこと。	必須						
(5) ITサービスマネジメントシステム（ITSMS）としてISO/IEC 20000シリーズ又はITILの最新版に則して運用管理業務を実施することにより，PDSAサイクルによる継続的な改善を行い，次に掲げる効果を可能な限り導き出すための方策を具体的に示すこと。 ・ 宮内庁NWSを取り巻く環境の変化への対応力向上 ・ 宮内庁NWSのユーザの満足度向上 ・ 宮内庁NWSを利用した業務継続性の強化	必須						
(6) 絶え間なく変化する情報通信技術や情報セキュリティなどに追従するため，運用管理従事者に対し，それらを学習する機会を適切に設け，運用管理従事者の能力向上を図り，運用管理業務の継続的な改善を行うこと。	必須						
(7) 作業範囲は，「6.運用管理に関する要件」に従うこととし，各現行システムについては，「13.資料閲覧」時に供する各運用管理手順書等，さらには運用管理業務の対象となるハードウェア及びソフトウェア等の製造事業者等が提供する手順書，マニュアルやFAQなどに従うこと。	必須						
(8) 各運用管理手順書について，記載内容以外に運用管理業務を効率的に効果的に行う方法などがある場合や不明瞭な内容又は不足があると認識した場合には，運用管理業務の対象となるハードウェア及びソフトウェア等の製造事業者等の手順書，マニュアル，FAQや技術サポートサイトなどを参照し，当該手順書の修正等を適宜行い，継続的な改善を行うこと。 なお，製造事業者等の技術サポートサイトの一例としては，次のようなサイトがあるが，宮内庁NWSを構成するハードウェア及びソフトウェア等の製造事業者等の技術サポートサイトをあらかじめ調査し，各運用管理手順書の中で一覧としてまとめ，変更があった場合には，この一覧を適宜修正すること。 ＜技術サポートサイトの一例＞ ・ 日本マイクロソフト社 TechNet https://technet.microsoft.com/ja-jp/	必須						
(9) 運用管理業務を円滑かつ効果的に行うため，PMIのPMBOKの最新版に則してステークホルダーマネジメントを行うこと。	必須						
(10) 運用管理業務の実施に当たり，既存システムへの追加・設定変更が必要となる場合には，甲及び既存システムの構築・保守事業者とその妥当性や有効性について十分に協議・検討し，甲の承諾を得た上で，ユーザサービスに影響がないよう，変更管理などの必要な管理を確実に実施すること。	必須						
(11) 宮内庁NWSの投資対効果を最大化するため，宮内庁NWSを構成する各ソフトウェア及びハードウェアに「標準装備」されている個々の機能を最大限に活用するだけでなく，それぞれが連携した場合の機能を最大限活用することに努め，情報システムの利便性の向上や情報セキュリティ対策の向上を図ること。 なお，別途，ソフトウェア又はハードウェアの機能やモジュール等の追加購入及びセットアップ作業が必要となる場合は，必要となる費用の概算や作業内容等を可能な限り甲担当者へ提供し，甲担当者の検討に協力すること。	必須						
(12) 情報セキュリティについて，その対策のための措置として既存システムへの設定変更，必要なログの取得などの作業を甲の判断で甲担当者から依頼された場合には，その依頼内容についての実現方法について可能な限り迅速に検討し，確実に実施することにより，情報セキュリティ対策の強化を継続的に行うこと。	必須						

5.1.請負範囲 【再掲】

運用管理業務における請負者として，関係事業者並びに宮内庁統合NW受託者と密に連携しつつ，公共サービス改革法の第1条，趣旨と目的に基づいて民間事業者の創意と工夫による次期宮内庁NWSの運用管理業務を柔軟かつ確実に実施し，甲におけるITガバナンス及び情報セキュリティガバナンスの強化に努めること。具体的には，以下のとおりとし，それぞれに対して具体的な方針や実現方法などを示すこと。							
(1) 運用管理業務を行う場合において，運用管理セグメントでの作業を行う際には，運用管理セグメント用端末を用いること。	必須						
(2) 次期宮内庁NWSの運用管理業務には，次に挙げる宮内庁統合NWに含まれるサービスは対象外とする。 ・ SOC ・ 宮内庁WAN ・ インターネット接続回線サービス（インターネット接続機器を除く） なお，詳細については別紙4を参照すること。 ただし，日常の運用管理業務の円滑な遂行及び障害やインシデントへの迅速な対応のため，甲担当者や運用管理業務の対象となるハードウェア及びソフトウェア等の製造事業者等との連携だけでなく，安定的で良質な運用管理業務を行うのに必要なログ等の情報共有を，甲の承諾を得た上で，必要に応じて宮内庁統合NW受託者と互いに行うこと。		加点	200	100	50	0	左記(1)～(11)について，具体的な方針・実現方法を示し，有効かつ妥当性のある内容であれば加点として評価する。
(3) 宮内庁NWSにおいて，障害やインシデントが発生した場合，乙は，甲担当者，運用管理業務の対象となるハードウェア及びソフトウェア等の製造事業者等，甲の承諾を得た上で，必要に応じて宮内庁統合NW受託者と密な連携をすることにより，迅速な解決を図り，甲の事務が極力遅滞なく遂行可能な状態に復帰させることに努めること。							
(4) 本調達に先行する宮内庁統合NWの調達の構築期間中に，甲の承諾を得た上で宮内庁統合NWの基本設計書及び詳細設計書を必ず精読して理解し，甲を介して宮内庁統合NW受託者と協議を行い，それぞれが互いに効率的に連携して安定的で良質な運用管理業務を実施可能な運用管理設計を行うこと。							
(5) ITサービスマネジメントシステム（ITSMS）としてISO/IEC 20000シリーズ又はITILの最新版に則して運用管理業務を実施することにより，PDSAサイクルによる継続的な改善を行い，次に掲げる効果を可能な限り導き出すための方策を具体的に示すこと。 ・ 宮内庁NWSを取り巻く環境の変化への対応力向上 ・ 宮内庁NWSのユーザの満足度向上 ・ 宮内庁NWSを利用した業務継続性の強化							
(6) 絶え間なく変化する情報通信技術や情報セキュリティなどに追従するため，運用管理従事者に対し，それらを学習する機会を適切に設け，運用管理従事者の能力向上を図り，運用管理業務の継続的な改善を行うこと。							
(7) 作業範囲は，「6.運用管理に関する要件」に従うこととし，各現行システムについては，「13.資料閲覧」時に供する各運用管理手順書等，さらには運用管理業務の対象となるハードウェア及びソフトウェア等の製造事業者等が提供する手順書，マニュアルやFAQなどに従うこと。							
(8) 各運用管理手順書について，記載内容以外に運用管理業務を効率的に効果的に行う方法などがある場合や不明瞭な内容又は不足があると認識した場合には，運用管理業務の対象となるハードウェア及びソフトウェア等の製造事業者等の手順書，マニュアル，FAQや技術サポートサイトなどを参照し，当該手順書の修正等を適宜行い，継続的な改善を行うこと。 なお，製造事業者等の技術サポートサイトの一例としては，次のようなサイトがあるが，宮内庁NWSを構成するハードウェア及びソフトウェア等の製造事業者等の技術サポートサイトをあらかじめ調査し，各運用管理手順書の中で一覧としてまとめ，変更があった場合には，この一覧を適宜修正すること。 ＜技術サポートサイトの一例＞ ・ 日本マイクロソフト社 TechNet https://technet.microsoft.com/ja-jp/							
(9) 運用管理業務を円滑かつ効果的に行うため，PMIのPMBOKの最新版に則してステークホルダーマネジメントを行うこと。							
(10) 運用管理業務の実施に当たり，既存システムへの追加・設定変更が必要となる場合には，甲及び既存システムの構築・保守事業者とその妥当性や有効性について十分に協議・検討し，甲の承諾を得た上で，ユーザサービスに影響がないよう，変更管理などの必要な管理を確実に実施すること。							
(11) 宮内庁NWSの投資対効果を最大化するため，宮内庁NWSを構成する各ソフトウェア及びハードウェアに「標準装備」されている個々の機能を最大限に活用するだけでなく，それぞれが連携した場合の機能を最大限活用することに努め，情報システムの利便性の向上や情報セキュリティ対策の向上を図ること。 なお，別途，ソフトウェア又はハードウェアの機能やモジュール等の追加購入及びセットアップ作業が必要となる場合は，必要となる費用の概算や作業内容等を可能な限り甲担当者へ提供し，甲担当者の検討に協力すること。							左記(1)～(11)について，具体的な方針・実現方法を示し，有効かつ妥当性のある内容であれば加点として評価する。
(12) 情報セキュリティについて，その対策のための措置として既存システムへの設定変更，必要なログの取得などの作業を甲の判断で甲担当者から依頼された場合には，その依頼内容についての実現方法について可能な限り迅速に検討し，確実に実施することにより，情報セキュリティ対策の強化を継続的に行うこと。							

5.2.対象機器

運用管理業務の対象機器は，甲におけるネットワーク機器，サーバ機器，クライアント端末，プリンタ，ケーブル（これらの周辺機器や附属品を含む。）とする。 なお，詳細については，「13.資料閲覧」時に供する「機器一覧」，「ラック構成図」，「全体概要図」ほかを参照すること。	必須						左記について，理解した上で対応できるか。

5.3.サービスレベル

(1) 運用管理業務の効率化と品質向上並びに円滑化を図るため，以下に示す指標に対してサービスレベルアグリーメント（SLA）を締結すること。	必須						左記について，理解した上で対応できるか。
① 運用管理業務の一次回答時間 （ア） ユーザからの質問等に対する一次回答時間は1時間以内とすること。回答時間は以下の計算式による。 （乙がユーザに回答した時刻）－（ユーザが乙に対して質問等した時刻） （ただし，17時45分以降の質問については翌営業日の9時30分までに回答すること。）	必須						
② 運用管理業務の解決時間 （ア） ユーザからの質問等に対する解決時間は2営業日以内とすること。解決時間は以下の計算式による。 （ユーザの質問等が解決した日時）－（ユーザが乙に対して質問等した日時） （イ） 乙の作業範囲外のものについてはサービスレベルの対象外とする。ただし，この場合においても質問等の解決に向けて協力すること。	必須						
③ 障害報告時間 （ア） 各システム又は外部監視等により検出された機器等の障害について，30分以内に甲担当者に対し報告すること。障害報告時間は以下の計算式による。 （乙が甲担当者に報告した時刻）－（障害確認時刻） （ただし，17時45分以降の障害発生については，翌営業日の9時までに報告すること。）	必須						
④ 障害解決時間 （ア） 各システム又は外部監視等により検出された機器等の障害について，1営業日以内に解決させること。障害解決時間は以下の計算式による。 （障害が解決した日時）－（障害確認日時） （イ） 乙の作業範囲外のものについてはサービスレベルの対象外とする。ただし，この場合においても障害の解決に向けて協力すること。	必須						
⑤ 運用要領及び運用計画の遵守 （ア） 運用要領及び運用計画の遵守状況に関して，甲から指摘された改善要求件数は，0件であること。	必須						
(2) サービスレベルの遵守状況については，月１回開催のSLA報告会議において報告し，甲の承諾を得ること。	必須						
(3) 甲の要求水準は，「上記(1)①から⑤に掲げる指標全ての遵守率について99%以上であること」とする。ただし，乙の作業範囲外のもの，又はやむを得ない事情によるものであることを甲が承諾したものについてはサービスレベル測定の対象外とする（例えば甲担当者と連絡がつかない，地方部局とのやり取りなど。）。	必須						
(4) (3)で要求した水準を満たせなかった場合，具体的な解決策を検討し，(2)の報告時に合わせて報告すること。	必須						
(5) 3か月連続して(3)の要求水準を満たせなかった場合，運用管理体制の強化，若しくは「5.4.作業実施体制」の変更を指示することがあるが，(3)の要求水準を満たせるまでの期間において，乙は運用管理業務の範囲内でこれに対応すること。	必須						

5.4.作業実施体制

宮内庁NWSの体制を以下に示す。本調達の運用期間中にクライアント端末，プリンタ及び複合機の増設が生じた場合でも，本調達の範囲内として運用対象とすること。 【図は省略】	必須						
(1) 宮内庁NWSの運用管理業務について，情報管理室に休日を除いた平日に常駐する運用作業員（以下「運用作業員」という。）の管理者（以下「運用管理責任者」という。）を1名以上配置すること。	必須						

評価対象	必須	加点	加点評価				評価基準
			特に優秀	優秀	標準	加点なし	
(2) 運用管理責任者は，1週間のうち休日を除く平日の60%以上，情報管理室に勤務すること。平日1日の勤務時間を8:30～17:45（休憩時間60分を含む。）とした場合，運用管理責任者の勤務は次のとおりとなる。 1週間のうち平日が5日の場合： 休憩時間を除く24時間45分以上 1週間のうち平日が4日の場合： 休憩時間を除く19時間48分以上 1週間のうち平日が3日の場合： 休憩時間を除く14時間51分以上 1週間のうち平日が2日の場合： 休憩時間を除く9時間54分以上 1週間のうち平日が1日の場合： 休憩時間を除く4時間57分以上	必須						左記について，理解した上で対応できるか。
(3) 乙は，情報管理室に休日を除いた平日に常駐する運用作業員を1名以上配置すること。ただし，運用作業員が1名のみの場合，運用管理責任者が運用作業員を兼ねることを不可とする。 なお，「5.1.請負範囲」を遂行困難，又は「5.3.サービスレベル」を満たしていないと甲が判断し，これらに基づき乙に対して改善要求をした場合には，乙は，必ず人数の増加や運用作業員の交替の措置を乙の責任と負担で施すこと。	必須						
(4) 運用管理責任者又は運用作業員は，運用管理報告書を作成の上，毎週1回開催の運用管理会議において，運用管理会議開催日の前週の一週間分の作業状況を報告し，甲の承諾を得ること。また，運用管理会議開催日の翌週の一週間分の運用管理責任者及び運用作業員の勤務予定表を提出すること。その勤務予定表に基づき，情報管理室に1名のみの配置となる日時を確認し，この日時について甲担当者1名が情報管理室に勤務することを調整することで，情報管理室の配置要員を2名とする。 なお，当該会議には，運用管理責任者も同席すること。	必須						
(5) 運用管理責任者及び運用作業員の勤務時間は，原則，休日を除く平日の8:30～17:45（休憩時間60分を含む。）とする。ただし，ユーザの業務への影響等を考慮し，当該勤務時間外でないと実施できない作業については，甲と事前に協議の上で作業実施を決定した場合，この限りではない。 なお，運用管理責任者と運用作業員が同時に情報管理室に勤務する場合には，休憩等は時間差で行い，情報管理室で運用管理業務を行う者が不在とならないようにすること。	必須						
(6) 運用作業員が不慮の事故，疾病又は休暇により勤務できない場合は，甲担当者と協議の上，乙の責任において，代替要員の運用作業員を情報管理室に派遣し，運用作業員が1名もいない状況を回避して業務に支障を来さぬようにすること。 なお，運用作業員が1名のみの場合，運用管理責任者が代替要員を兼ねることを原則不可とする。 ただし，運用作業員が勤務できない日数が平日の連続した2日間以下であることが事前に確認可能であり，運用作業員が勤務できない最初の日から数えて休日を除いた平日5日前までにあらかじめその旨を甲担当者へ報告して承諾を得た場合には，確認ができた運用作業員が勤務できない日に限り，運用管理責任者が代替要員を兼ねることを許可する。	必須						
(7) 運用管理責任者及び運用作業員の勤務予定表を除いた実施体制そのものを変更する場合，甲担当者との協議を行うための十分な期間（平日で10日間以上）を設け，変更する理由を明確に甲担当者へ報告し，協議の上で承諾を得ること。	必須						
5.5.リモートで運用作業員のサポートを行う場合の要件							
リモートにより，運用作業員のサポートを実施する（以下，「サポート業務」という。）には，セキュリティが確保された体制となっているか，サポート人員の実績・資格等が運用作業員と同等以上であるかなどの条件を満たす必要があり，情報管理室での勤務するのと遜色ないサービスレベルが維持されることを前提に認めることは，あり得る。 サポート業務の遂行に当たっては，乙が保有する運用拠点からリモートで運用作業を行うことを可とするが，宮内庁内の機器に対しオペレーションを伴う作業を行う場合においては，以下の要件を遵守すること。 なお，運用拠点及び運用管理業務を行う居室（以下，「運用居室」という。）について，要件遵守の確認のため，甲が立ち入りを求めた場合は，入室を許可すること。	必須						リモートによるサポートを実施する場合，左記を理解した上で対応できるか。
5.5.1.基本要件							
(1) 甲より受領した情報については厳重に管理を行い，サポート業務遂行以外の目的に利用してはならない。	必須						リモートによるサポートを実施する場合，左記を理解した上で対応できるか。
(2) 記録された映像やログ等は，甲からの求めがあった場合は，速やかに提供すること。	必須						
5.5.2.ネットワーク接続形態要件							
(1) 運用管理業務をリモートで行うに当たって宮内庁NWSに接続を行う場合は，以下(2)の条件を満たす閉域等されたネットワーク（以下，「閉域等NW」という。）にて接続を行うこと。	必須						リモートによるサポートを実施する場合，左記を理解した上で対応できるか。
(2) 接続される閉域等NWについて，インターネットを介した VPN を用いる場合には，OSI階層モデルのネットワーク層以下での経路の暗号化手続きを行う通信経路上のセキュリティを配慮した方式であるか，又は，インターネットを介さない閉域網（専用線，閉域IP通信（IP-VPN）等）の利用とする。	必須						
(3) 該当の閉域等NWには，あらかじめ甲に申請し許可を得た端末以外の端末は接続できない措置を講じること。	必須						
(4) 閉域等NWを利用して接続を行う場合は，宮内庁内に設置する機器等も含めその設営等に係る費用は，すべて乙が負担すること。	必須						
5.5.3.運用拠点要件							
(1) 運用拠点は，公共交通機関を利用して，当庁へ2 時間を目途に到着できる場所に存在すること。	必須						リモートによるサポートを実施する場合，左記を理解した上で対応できるか。
(2) 運用拠点には，運用管理責任者を配置すること。	必須						
(3) 運用拠点は，防火構造，空調設備を備えた建物であること。	必須						
(4) 運用拠点は，免震ないしは耐震構造建物となっており，震度6相当の地震にも耐えうること。	必須						
(5) 運用拠点には，常時安定した電力供給ができるほか，電力の瞬間停電等の際も，連続的な運転を可能にする措置が講じられていること。	必須						
(6) 運用拠点には，機械的に判別できる本人認証技術を用いた入場制限がなされており，乙関係者以外の人員が出入りできない措置が講じられていること。	必須						
(7) 運用拠点への出入りは，監視カメラにより撮影され，その映像は記録されていること。記録した映像の保管・管理は，甲乙協議の上で決定すること。	必須						リモートによるサポートを実施する場合，左記を理解した上で対応できるか。
5.5.4.運用居室要件							
(1) 運用居室は，他の居室と壁で完全に仕切られているなど独立した居室であること。	必須						リモートによるサポートを実施する場合，左記を理解した上で対応できるか。
(2) 運用居室は原則としてサポート業務専用の居室とすること。やむを得ず他業務と共有をする場合は，共有期間を明示した上で他業務内容及びその必要性についてあらかじめ甲にその理由を記した書面を提出し承諾を得ること。	必須						
(3) 運用居室内には，あらかじめ甲が承諾し登録された人員以外が出入りできない措置が講じられていること。	必須						
(4) 運用居室には，機械的に判別できる本人認証技術を2種類以上用いた入場制限がなされていること。	必須						
(5) 運用居室内に入室可能な人員は，あらかじめ甲に書面にて名簿を提出し承諾を得ること。この人員を変更する場合は，その都度変更した名簿を甲に提出して承諾を得ること。	必須						
(6) 運用居室への入退室は，人員ごとに入室時刻及び退室時刻を自動的に記録（ログ等）ができるものとし，甲がこの記録を求めた場合は，即座に提出すること。また，この記録は，意図的な改ざんされないような仕組みを具備すること。	必須						
(7) 運用居室内では，原則として宮内庁NWSに接続する閉域等NW以外の他回線の引き込みを行わないこと。やむを得ず他回線の引き込みを行う場合は，あらかじめ甲にその理由を記した書面を提出し承諾を得ること。	必須						
(8) 運用居室内に人員が滞在している間は，常時監視カメラにより撮影され，その映像は記録されていること。	必須						
(9) 監視カメラで撮影される範囲は，死角がないように居室全体とすること。	必須						
(10) 監視カメラには，同カメラ自体に撮影を妨げる行為があった場合，それを検知し，その記録（ログ等）を保存できること。	必須						
(11) 監視カメラで記録した映像及びログ等は，少なくとも1年保存・管理すること。詳細については，甲乙協議の上で決定すること。	必須						
5.5.5.運用端末要件							
(1) 運用端末は本業務を行うための専用端末とし，他の用途には使用しないこと。	必須						

評価対象	必須	加点	加点評価 特に優秀	加点評価 優秀	加点評価 標準	加点評価 加点なし	評価基準
(2) 運用端末の操作は，あらかじめ登録されている人員のみとし，登録されているどの人員が，いつ，どんな操作をしたのか記録等（ログ等）をすること。また，運用端末を操作する際にコンピュータ・ネットワークを利用する人を識別するための番号であるユーザIDを使用する場合は，総務省「国民のための情報セキュリティサイト」を踏まえ，次のルールを遵守すること。 【ユーザID及びパスワードのルール】 ① パスワードの長さ 管理者権限ユーザの場合は13桁以上，一般権限ユーザの場合は8桁以上とすること。 ② パスワードは，数字，アルファベット大文字と小文字及び記号の4つの文字種を組み合わせること。 ③ 数字の単なる羅列など，他人に推測されやすいパスワードやデフォルト（製品の初期値等）のパスワードは速やかに本ルールに沿って変更すること。 ④ 本業務の運用端末操作ためのユーザID及びパスワードは，他の業務の端末操作等では使用しないこと。 ⑤ 運用作業員ごとの個別ユーザIDで，作業すること。 ※ [参考] 総務省 国民のための情報セキュリティサイト http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/basic/privacy/01.html	必須						リモートによるサポートを実施する場合，左記を理解した上で対応できるか。
(3) 運用端末は，宮内庁NWS以外に接続を行わないこと。また，運用端末を誤って他のネットワークに接続した場合は，外部との通信ができないような仕組みを講じること。	必須						
(4) 運用端末は，セキュリティワイヤー等で什器等固定物に繋げ，施錠等し，持ち出しができない措置を講じること。	必須						
(5) 運用端末に，USBメモリ等の外部電磁的記録媒体を接続し，データの取り込み，書き込み及び持ち出しができない措置を講じること。やむを得ず運用端末に外部電磁的記録媒体を接続する必要が生じる場合は，あらかじめ甲にその理由を記した書面を提出し承諾を得ること。また，承諾を得た後，外部電磁的記録媒体を運用端末へ接続する直前には，必ずウイルス検査を行い，ウイルスが存在していないことを確認した上で接続すること。	必須						
(6) 運用端末のハードディスクは，暗号化される措置を講じること。	必須						
(7) 運用端末に保管するファイルは，自動的に暗号化される措置を講じること。	必須						
(8) 運用端末は，ウイルス対策ソフトがインストールされており，常に最新の状態でウイルス対策ができる措置を講じること。	必須						
(9) 運用端末のOS及び各種ソフトウェア等の脆弱性情報を常に確認し脆弱性対策を講じること。	必須						
(10) 万一，運用端末がマルウェアに感染した場合又は感染のおそれがあると判断した場合は，当該端末を即座に宮内庁NWSから切り離し，速やかに甲に書面による報告を行うこと。感染原因の追及に当たっては，セキュリティオペレーションセンター等の支援を得て，乙の負担においてフォレンジック調査等を行い，侵入経路，感染ルート等の原因調査を行い，その結果及び今後の防止対策を講じた上で，甲に説明を行うこと。	必須						
(11) 運用管理業務の契約期間満了後には，速やかに運用端末内で保管・管理されている甲に関する一切の情報が残らない（復元を不可能とする）措置をとり，データ消去証明書を甲に提出すること。 なお，データ消去に当たっては，甲が定めた「情報処理及び情報システムについての対策規程（平成27年3月10日 統括情報セキュリティ責任者決定）」を遵守すること。 ※ 参考：「情報処理及び情報システムについての対策規程」より抜粋 ○ 付録「データ抹消ツール」の設定要件 以下のいずれかのデータ上書き方式を設定すること。これらの設定をすることができないものを用いないこと。 【以下，記載省略】	必須						
6.1.運用管理計画の策定							
6.1.1.サービスレベルの合意							
甲とサービスレベルについて合意し，サービスレベル合意書【2.2.サービスレベル】を契約締結後，運用管理業務開始10日（休日を除く）前までに遅滞なく提出すること。	必須						左記について，理解した上で対応できるか。
6.1.2.運用管理計画書の策定							
(1) 乙は，次にあげる各文書を十分に理解した上で，本調達仕様書（案）「4.宮内庁NWSの運用管理業務に係る請負業務内容」に基づいた宮内庁NWSの運用設計を行い，宮内庁NWSの日々の安定稼働を確保することを目的とした，宮内庁NWSの運用管理計画書の案を作成し，本調達の提案書と共に提出すること。 (ア) 宮内庁CISの運用管理計画書（案） (イ) 宮内庁業務継続計画 http://www.kunaicho.go.jp/kunaicho/shiryo/gyomukeizoku.html (ウ) 宮内庁NWSに関する各計画書など	必須						左記について，理解した上で提出できるか。
		加点	100	50	25	0	具体的な方針・実現方法を示し，有効かつ妥当性のある内容であれば加点として評価する。
(2) 乙は，(1)に掲げる運用管理計画書の案を基に作成した正式版を，運用管理業務開始10日（休日を除く）前までに甲担当者の確認を受け，承諾を得た上で確定版とすること。	必須						左記について，理解した上で対応できるか。
(3) 乙は，(2)に掲げる運用管理計画書の確定版について，運用管理業務を実施してく中で，必要に応じて修正箇所を提案し，更新すること。 なお，更新する場合は甲担当者と合意の上，更新すること。	必須						
6.1.3.各手順書の作成							
(1) 乙は，宮内庁CISの運用管理手順書（案），甲担当者向け停電時復旧手順書（案），情報セキュリティインシデント対応手順書（案），ユーザ手順書（案）などの運用管理に関する各手順書及び本調達仕様書（案）「5.宮内庁NWSの運用管理業務に係る請負業務内容」を基に，本調達に対する提案書，宮内庁NWSの運用管理計画書（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，実施手順等を取りまとめた各手順書の案を作成し，本調達の提案書と共に提出すること。	必須						左記について，理解した上で提出できるか。
		加点	100	50	25	0	具体的な方針・実現方法を示し，有効かつ妥当性のある内容であれば加点として評価する。
(2) 乙は，(1)に掲げる各手順書の案を基に作成した正式版を，運用管理業務開始10日（休日を除く）前までに甲担当者の確認を受け，承諾を得た上で確定版とすること。	必須						左記について，理解した上で対応できるか。
(3) 乙は，(2)に掲げる各手順書の確定版について，運用管理業務を実施していく中で，必要に応じて修正箇所を提案し，更新すること。 なお，更新する場合は甲担当者と合意の上，更新すること。	必須						
6.1.4.運用管理実施要領の作成							
(1) 乙は，管理標準ガイドラインの「第9章 運用及び保守」にて示されている運用管理要領の作成・記載内容などを参考にし，宮内庁NWSの運用管理を効率的に実施できるよう，宮内庁NWSの運用管理計画書及び保守作業計画書と整合をとりつつ，運用・保守工程におけ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に係る実施ルールを定義する運用管理実施要領の案を作成し，本調達の提案書と共に提出すること。	必須						左記について，理解した上で提出できるか。
		加点	100	50	25	0	具体的な方針・実現方法を示し，有効かつ妥当性のある内容であれば加点として評価する。
(2) 乙は，(1)に掲げる運用管理実施要領の案を基に作成した正式版を，運用管理業務開始10日（休日を除く）前までに甲担当者の確認を受け，承諾を得た上で確定版とすること。	必須						左記について，理解した上で対応できるか。
(3) 乙は，(2)に掲げる運用管理実施要領の確定版について，運用管理業務を実施してく中で，必要に応じて修正箇所を提案し，更新すること。 なお，更新する場合は甲担当者と合意の上，更新すること。	必須						
6.2.作業実績の報告							
乙は，本調達仕様書（案）5.1.に示す作業等を実施すること。 なお，作業実績の報告については以下の事項に留意すること。 ・ サイバー攻撃に関する最新動向の調査に当たっては，宮内庁CISに限らず，甲に対し有用な提案がある場合は積極的に提案すること。	必須						左記について，理解した上で対応できるか。
6.2.1.週次運用管理報告書の作成							
「運用管理計画書」，「保守作業計画書」，「運用・保守実施要領」に基づき，以下の内容について週次で「週次運用管理報告書」を取りまとめること。 ・ 情報システムの構成と運転状況（情報セキュリティ監視状況を含む） ・ 情報システムの定期点検状況 ・ 情報システムの利用者サポート，教育・訓練状況 ・ 情報セキュリティ管理の実施状況 ・ リスク・課題の把握・対応状況	必須						左記について，理解した上で対応できるか。
		加点	40	20	10	0	報告書の見やすさ，理解しやすさを考慮した具体的な工夫が施された提案がある場合には，加点をして評価する。
6.2.2.月次運用管理報告書の作成							
「運用管理計画書」，「保守作業計画書」，「運用・保守実施要領」に基づき，以下の内容について月次で「月次運用管理報告書」を取りまとめること。 なお，情報セキュリティ管理については，サイバー攻撃に関する最新動向等を入手し，宮内庁NWSにおいて可能な防御策を確認の上，報告を実施すること。また，報告には，少なくとも作業実施者名，作業実施者スキルレベル，作業開始日時，作業終了日時を含めること。 ・ 運用・保守業務の内容や工数，作業時間等の作業実績状況 ・ サービスレベルの達成状況 ・ 情報システムの構成と運転状況（情報セキュリティ監視状況を含む） ・ 情報システムの定期点検状況 ・ 情報システムの利用者サポート，教育・訓練状況 ・ 情報セキュリティ管理の実施状況 ・ リスク・課題の把握・対応状況 ・ サイバー攻撃に関する最新動向等及び庁内LANで可能な防御策等	必須						左記について，理解した上で対応できるか。
		加点	40	20	10	0	報告書の見やすさ，理解しやすさを考慮した具体的な工夫が施された提案がある場合には，加点をして評価する。
6.2.3.作業実績の評価							
月間の運用・保守実績を評価し，達成状況がSLAに満たない場合はその要因の分析を行うとともに，達成状況の改善に向けた対応策を提案すること。	必須						左記について，理解した上で対応できるか。
6.2.4.作業実績の報告の実施							
運用・保守作業報告書の内容について，定例の運用管理会議に出席し当庁に報告すること。	必須						左記について，理解した上で対応できるか。
6.3.定常運用管理業務							
6.3.1.業務管理							
6.3.1.1 定例会議							
甲に対し定期的に運用報告を実施すること。	必須						

評価対象	必須	加点	加点評価				評価基準
			特に優秀	優秀	標準	加点なし	
(1) 運用管理会議 運用作業員は，運用計画書に基づき実施した運用管理業務の内容及び障害・インシデント等の対応状況について，運用管理業務週報に記録し，甲に毎週1回開催の運用管理会議において報告すること。ただし，重大な報告は都度行うこと。	必須						左記について，理解した上で対応できるか。
① 運用管理会議の出席者については，以下の要員とする。 ・ 甲担当者，宮内庁CIO補佐官（内閣官房政府CIO補佐官） ・ 乙は運用管理責任者及び運用作業員 ・ その他，甲が承諾をした者	必須						
② 報告事項については，以下の項目を含むものとする。 ・ 前回議事録 ・ ネットワーク運用支援作業報告 ・ ユーザサービス作業報告 ・ 障害対応ヘルプデスク作業報告 ・ ヘルプデスク対応管理表 ・ 課題事項一覧表 ・ ウイルス検知報告（種別・個人別のウイルス検知表） ・ 日毎の入退室管理実績表 ・ 日毎の次週作業予定表 ・ 障害対応報告書（障害が発生した場合） ・ その他，甲が希望する資料	必須						
(2) SLA報告会議（月1回開催）会議 乙は，1か月ごとにサービスレベルアグリーメントの達成状況の確認を行い，達成状況について，サービスレベル報告書に記録し，甲に毎月1回開催のSLA報告会議において報告すること。	必須						
① SLA会議の出席者については，以下の要員とする。 ・ 甲担当者，宮内庁CIO補佐官（内閣官房政府CIO補佐官） ・ 乙は運用管理責任者及び運用作業員 ・ その他，甲が承諾をした者	必須						
② 報告事項については，以下の項目を含むものとする。 ・ 【5.3.サービスレベル】の5項目を始めとするサービスレベル合意書において設定した項目の達成状況についてまとめたサービスレベル報告書 ・ サービスレベルを満たせなかった場合の原因及び対策に関する報告資料 ・ 報告期間（報告実施前月の1か月間）に対応した1件ごとの作業内容に関する詳細情報（部署名・氏名・状況・処置・発生日時・一次回答日時・所要時間・解決時間等々） ・ 本要求仕様の各項目に要した1か月分の工数（時間単位）をまとめ，SLA報告会議時に報告すること。	必須						
6.3.1.2. 手順書等の整備							
(1) 運用管理業務に必要となる手順書，運用管理フロー図等を適切に整備すること。	必須						左記について，理解した上で対応できるか。
		加点	40	20	10	0	具体的な方針・整備方法を示し，有効かつ妥当性のある内容であれば加点として評価する。
(2) 手順書等に変更が生じた場合は，速やかに更新し甲担当者の承諾を得ること。	必須						左記について，理解した上で対応できるか。
6.3.1.3. 提案							
(1) 運用管理実績報告の他に，本調達仕様書（案）「1.4.背景と目的」における各目的の実現を達成するための継続的改善活動（PDSAサイクル）として，定期的ないし随時に，運用にかかる評価，問題提起，改善提案，最新技術情報の提供を甲へ行い，甲と積極的に協議する機会を設けること。 なお，甲が自らの調査等に基づいて乙へ提案を行う場合においても，運用管理実績報告の他に，本調達仕様書（案）「1.4.背景と目的」における各目的の実現を達成するための継続的改善活動（PDSAサイクル）である場合には，乙は，甲からの提案内容について甲と積極的に協議する機会を設けること。	必須						左記について，理解した上で対応できるか。
(2) 協議の結果，提案内容を甲が承諾した場合には，実現に向けた具体的な提案（運用手順の変更内容や各機器の設定の変更内容等）を行った上で，実現を図ること。ただし，新たなハードウェア及びソフトウェアの購入が必要である場合，それらの購入費用及び保守費用は，本調達には含めないこととし，別途予算確保できた場合にのみ，実施することとする。	必須						
6.3.2.情報の管理							
(1) 調査，保守作業，システム構築等による文書又は電子データの持ち出し，持ち込みが発生する場合は，甲担当者の承諾のもと，文書にて内容を説明した上で持ち出し又は持ち込みを実施すること。	必須						左記について，理解した上で対応できるか。
(2) 電子メールや甲の指示する電子媒体で情報を授受する際は，パスワード等による漏洩防止対策を行うこと。	必須						
6.3.3.資産管理に使用する資料等							
宮内庁NWSに接続されるハードウェア（クライアント端末含む），配線及びソフトウェア（ライセンス）の情報，接続情報等を可能な限り自動で，自動化できないものは手動にて適時に収集し，資産管理，インベントリ管理を行うこと。また使用権を得ているライセンスについて契約更新等の支援を行うこと。（既存インベントリ収集用のシステムとして資産管理ソフトウェアを使用）以下の資料を作成し，常時メンテナンスすること。	必須						左記について，理解した上で対応できるか。
(1) 資産管理台帳 ① 宮内庁NWに接続されるハードウェア及びソフトウェアについて，必要な情報を管理すること。 ② 必要に応じハードウェア，ソフトウェアを分冊にする等メンテナンスしやすい様式とすること。	必須						
(2) 論理構成図 ① 資産管理台帳に基づき，ネットワーク及びサーバについて論理構成図を必要に応じて修正すること。 ② 新しく宮内庁NWにネットワークセグメント，ルーティング情報が追加された場合は，論理構成図に追加すること。	必須						
(3) 物理構成図 ① 資産管理台帳に基づき，ネットワーク及びサーバについて物理構成図を必要に応じて修正すること。	必須						
(4) 機器配置図 ① ネットワーク，サーバ，クライアント端末，プリンタ等のデジタル周辺機器に係る機器配置図の内容が最新となるように努めること。 ② 宮内庁NWにネットワークセグメント，ルーティング情報が追加された場合は，機器配置図に追加すること。	必須						
(5) ライセンス契約管理 ① ライセンス管理については，契約更新手続き支援（期限到来アナウンス，更新書類の記入，手続き支援等）を行うこと。	必須						
(6) 配線図 ① サーバ室内の電源配線図，ネットワーク機器のポートアサイン図が最新になるよう必要に応じて更新すること。	必須						
(7) その他必要な文書 ① 上記文書以外に運用管理業務内で管理すべき情報（サーバ設定情報等）がある場合は文書を作成し記録すること。 ② 上記(1)の資産管理台帳等に記載された資産に変更がなされた場合，変更の実施者，変更の承諾者，変更事由，変更箇所，変更に伴う他への影響範囲，テスト結果，変更の実施日時，リリース日時等を記録し管理を行うこと。	必須						
6.3.4.ポリシー管理							
グループポリシー設定等を適切に管理すること。	必須						左記について，理解した上で対応できるか。
6.3.5.データ管理							
(1) 定期バックアップ及びリストア バックアップ対象 3.11.2(1)②を参照すること。 ただし，個別システムのバックアップ運用については，「6.4.宮内庁CIS以外の宮内庁NWSの運用管理」の項目を参照すること。	必須						左記について，理解した上で対応できるか。
(2) バックアップの方式・機能 ① 本調達で導入されるバックアップソフトウェアを使用し，データバックアップを取得すること。 ② 本調達で導入されるイメージバックアップソフトウェアを使用し，サーバのイメージバックアップを取得すること。 ③ データ消失時のリストアを行うこと。	必須						
(3) 定常業務 ① バックアップログを毎日チェックすること。 ② 各テープ装置のテープメディアを交換すること。 ③ 定期的に各テープ装置のクリーニングを実施すること。 ④ 地方サーバで使用するデータカートリッジのローテーション管理。	必須						
(4) バックアップ媒体の保存 ① 一時保管 ・ KMSサーバは，テープメディアをサーバ室に保管 ・ ファイルサーバは，バックアップサーバをサーバ室に設置 ② 外部保管 ・ 月次フルバックアップを録取したテープメディアを指定の外部保管先に保管。 （保管先は，契約締結後，乙に対し甲担当者より指示する。）	必須						
6.3.6.ネットワーク管理							
(1) ネットワーク・サーバ等監視 ① 監視概要 ・ ネットワークセグメント及び各機器の死活，サーバの重要プロセス及びサービス稼働状況，サーバのシステムログに出力された障害情報，ネットワーク機器及びサーバのリソース，パフォーマンス状況，メールログ，プロキシログ，さらにはクライアント端末の操作ログ等を監視すること。 ・ 閣副安危第375 号（平成24年7月5日）「適切なログの管理による標的型攻撃対策について（情報提供）」（http://www.nisc.go.jp/active/general/pdf/logkanri_kanki_120705.pdf）に基づき，これらのログを1年間以上保存し，不正の検知，原因特定，問題の解決に役立てること。 なお，セキュリティ向上のため，「6.3.8.情報セキュリティ管理」と「6.3.9.性能管理」を甲は乙との協議の上，蓄積するログの種類，期間について設定・変更が可能とする。また，証跡の不当な消去や改ざんを防止するため，証跡に関するアクセス制御を考慮し，保護に努めること。 ② 監視対象 ・ 別紙2，3及び4に記載の各拠点に設置してある各種ネットワーク機器及び全サーバ機器等を監視対象とする。 ③ 監視体制 ・ 平日8:30～17:45においては，甲庁舎内の情報管理室にて常時監視すること。 ④ 監視基盤 ・ ネットワークセグメント及び機器の死活，サーバの重要プロセス及びサービス稼働状況については，次期宮内庁NWで導入される監視ツールを使用し監視すること。 ・ 新しく宮内庁NWに接続された機器がある場合，甲担当者と協議の上，監視ツール上に追加すること。 ・ 監視ツールの最新データベースのバックアップも取得すること。	必須						左記について，理解した上で対応できるか。
(2) ネットワーク上のコンピュータのIPアドレス，ホスト名の台帳管理 ① 管理台帳 ・ 既存の管理台帳を使用し政府共通ネットワークグローバルアドレスを含む各セグメントのIPアドレス，機器の設置場所，接続状況及びホスト名を管理すること。	必須						
(3) 資産管理ソフトウェアによるインベントリ管理 ・ 資産管理ソフトウェア及びWSUS上に登録されたサーバやクライアント端末について，機器の設置場所や構成に変更があった場合は登録情報を更新し，データベースのメンテナンスを実施すること。	必須						
(4) ネットワーク機器の設定変更 ・ ネットワーク機器が追加された場合，甲担当者の指示のもと，ルータやモデム，スイッチ等のネットワーク機器の設定を変更し，疎通確認すること。 ・ ネットワーク機器の設定情報を修正した際には最新のコンフィグ情報を取得し，ファイルサーバ等に保存すること。	必須						

評価対象	必須	加点	加点評価				評価基準
			特に優秀	優秀	標準	加点なし	
6.3.7.ユーザ管理							
6.3.7.1 アカウント管理							
(1) 現行の宮内庁NWでは，ユーザ管理システムによりアカウントの管理を実施している。ADサーバ及びグループウェアサーバと連動して管理すること。	必須						左記について，理解した上で対応できるか。
(2) 甲アカウントは，ユーザの属性情報を含めて管理しており，ユーザの異動などによる属性情報の変更があった場合には，遅滞なく適切に変更を行うこと。	必須						
6.3.7.2 パスワードの管理							
(1) 各サーバ，ネットワーク機器のパスワードを管理すること。	必須						左記について，理解した上で対応できるか。
(2) 甲担当者からの指示により，ドメイン管理者用のパスワードやネットワーク機器のパスワード変更を行うこと。	必須						
(3) 管理者用のパスワード変更等，影響範囲の大きいものは事前に計画書を作成し，甲担当者の承諾を得ること。	必須						
6.3.7.3 アクセス権の管理							
(1) ファイルサーバアクセス権限の管理をすること。	必須						左記について，理解した上で対応できるか。
(2) 各部局の庶務係からの問合せに対し支援を行うこと。	必須						
(3) IDMの仕組みを理解した上で，個人認証方式によるアカウント管理及びアクセス権管理を行うこと。	必須						
6.3.8.情報セキュリティ管理							
6.3.8.1 コンピュータウイルス対策							
(1) 基本方針 「13.資料閲覧」時に供する甲の情報セキュリティポリシーに則り，サーバ（Linuxサーバを含む），クライアント端末，貸出し用クライアント端末，地方サーバ及び各業務システムに対しウイルス対策ソフトウェアを最新に維持すること。日常的に情報セキュリティに関する情報収集を行うとともに遅滞なく適切な対策立案を行い，対策立案を行った場合には，甲担当者にその内容を報告し，その実行について協議を行い，甲の承諾を得た上で実施すること。 なお，情報セキュリティに関する情報収集を行う場合は，本調達仕様書（案）「1.15.1.情報セキュリティの確保」の(11)を参考にしつつ，宮内庁NWSで採用したソフトウェア及びハードウェア等の製造事業者等が提供する情報等も参考にすること。	必須						左記について，理解した上で対応できるか。
(2) ウイルス等に感染の可能性がある場合の対応 (ア) 速やかに甲担当者にウイルス感染の可能性について報告を行うとともに，対象となる全ユーザに通知及び所要の対応をとること。	必須						
(イ) 感染経路としてWEB閲覧が疑われる場合は，ウイルスの感染元となるインターネットサイトの URL を分析する無料のサービス等を利用し，確認を行うこと。次に示すのは，そのサービスの一例である。 ・ Virustotal https://www.virustotal.com/ja/ ・ TrendMicro https://global.sitesafety.trendmicro.com/?cc=jp ・ Norton https://safeweb.norton.com/	必須						
(ウ) ウイルス等の検体の抽出が可能な場合は，検体を抽出し，宮内庁NWSで採用したウイルス対策ソフトウェアの製造業者へそれを提供し，解析を依頼すること。	必須						
(エ) ウイルス等又は事象が既知であり，製造事業者等から対策が提供可能な場合には，再発防止策を講じ，甲担当者の承諾を得た上で必要な対応をとること。	必須						
(オ) ウイルス等の内容，ふるまいなどから，その影響範囲が広い又は影響度が強いと考えられる場合には，本調達仕様書（案）の「6.3.14.情報セキュリティインシデント対応」に従って適切な対応を行うこと。	必須						
(3) 対応拠点 別紙1，3及び5に記載の各拠点に設置してある各種ネットワーク機器及び全サーバ機器等を対象とする。	必須						
(4) 適用促進 ウイルスソフト適用状況を可能な限り自動的に常時把握し，適用不備のあるノードの管理者に対し適用促進を行うこと	必須						
6.3.8.2 Windows等のセキュリティパッチ対策及びバージョンアップ作業							
(1) ソフトウェア配布方式 ① ソフトウェアのアップデートやパッチに関しては，資産管理ソフトウェアやWSUSなどを使用し，ネットワークを通じクライアント端末に直接インストールする方式 （自動配信方式。ユーザがダウンロードしてインストールする場合も含む。），又は甲の指示する電子媒体によりデリバリする方式（媒体方式）によるものとすること。 ② ネットワーク接続していないクライアント端末に関しては，別途指示を行うこととする。 ③ サーバへのWindowsセキュリティパッチ適用に関しては，甲担当者からの指示により実施すること。実施時には，行事などの実施時間に重複しないよう，適用スケジュールを策定し，甲担当者と事前調整を行うこととする。 ④ サーバにインストールされたソフトウェアのアップデートやパッチに関しては，別途指示を行うこととする。 ⑤ 現行の運用管理業務では，クライアント端末へのWindowsセキュリティパッチ適用において，WSUSを利用して拠点別にWindowsパッチを配布している。 ※ 特にNISC（内閣サイバーセキュリティセンター）より注意喚起されたセキュリティ事象に関しては，調査・報告を行い，甲の現状に適した対策を提案すること。	必須						左記について，理解した上で対応できるか。
⑥ クライアント端末がソフトウェアの配布を受ける際，既に同一のセグメント内のクライアント端末に配布されたソフトウェアがキャッシュとして残っていた場合，当該クライアント端末からソフトウェアを配布すること。							
(2) 配布の必要性検討 運用作業員は，ソフトウェアの配布，更新について，必要性，問題点，適用是非について検討後，甲担当者の承諾を得て実施を行うこと。 【現行の運用管理業務（参考）】 ① Microsoftがセキュリティパッチを公表後，遅滞なく動作テストを開始すること（甲担当者が指定したクライアント端末3～5台を利用すること）。 ② 甲担当者が指定したクライアント端末で作動不良が発生しなかった場合は，甲担当者の承諾を受けクライアント端末に適用開始すること。 ③ トラフィック状況や配布対象拠点のスケジュール，配布にかかる時間等を考慮し，甲担当者の承諾の得た配布スケジュールを組むこと。 ④ パッチ適用についてのユーザへの周知は余裕を持って最低4日前には行うこと。 ⑤ 配布後速やかにクライアント端末に適用すること。 ⑥ 適用が遅いクライアント端末は個別対応とすること（ユーザの希望に添う形で次の配布前までに対応が終了することが望ましい。）。	必須						
(3) 配布対象拠点 別紙2，3及び5に記載の各拠点に設置してあるクライアント端末を対象とする。	必須						
(4) 配布対象ソフトウェアの事前動作テスト ① 配布するソフトウェアが甲の環境で問題なく動作するかどうかの確認を実機で検証すること。 ② 検証結果を甲担当者へ報告すること。 ③ 資産管理ソフトウェアで配布が可能なパッケージになるよう，必要に応じてバッチファイルやスクリプトを作成すること。 ④ 配布に際してユーザの対話的操作が必要なパッチは，対話的操作なしで配布・適用が可能になるようバッチファイルやスクリプトを作成すること。	必須						
(5) 配布対象ソフトウェア ① Windowsセキュリティパッチ。 ② Officeセキュリティパッチ（甲担当者と協議の上，適用作業を実施）。 ③ 一太郎，ATOKセキュリティパッチ。 ④ プリンタドライバ。 ⑤ その他，甲担当者が指定するセキュリティパッチやバージョンアップ版。	必須						
(6) 適用状況確認 セキュリティパッチの配布状況の確認を行うこと。未適用端末については，その適用が終了するまで個別対応にて適用作業を実施し，パッチ適用状況がまばらにならないよう適切に適用管理を行うこととすること（各端末のバージョンを揃えること。）。	必須						
(7) マスタ作成 Windowsパッチ，各ソフトウェアのパッチ適用後のクライアント端末マスタを甲の指示する電子媒体により作成すること。	必須						
6.3.8.3 インターネット対策							
(1) 甲担当者が情報セキュリティポリシーに基づき実施するアクセス制御，プロバイダ提供のコンテンツフィルタの設定（甲担当者が禁止したURL閲覧のアクセス禁止設定）について対応すること。例外対応として，甲担当者からの指示により，一時的に閲覧が必要なURLをコンテンツフィルタのホワイトリストに登録し，閲覧可能な状態とすること。	必須						左記について，理解した上で対応できるか。
(2) 迷惑メールについての資料を適宜甲担当者へ提出し，甲担当者から指示のある削除用キーワードをシステムへ登録するか，あるいはアドレスの一時的な停止について対応すること。	必須						
6.3.8.4 政府共通ネットワーク							
(1) 新規メールドメイン登録依頼が来た場合，甲担当者の承諾を得た上で速やかに登録作業を実施すること。	必須						左記について，理解した上で対応できるか。
(2) 甲担当者からの指示により，指定のポートを一時的に開放する等，政府共通ネットワークファイアウォールの設定変更作業を実施すること。	必須						
(3) 新規の経路情報の登録依頼があった場合，ネットワーク機器やサーバへ速やかに経路情報を登録すること。	必須						
6.3.9.性能管理							
6.3.9.1 システム運用と性能管理							

評価対象	必須	加点	加点評価 特に優秀	加点評価 優秀	加点評価 標準	加点評価 加点なし	評価基準
(1) 日次運用 ハードウェア，ソフトウェアの安定的かつ正常な稼動を確保する観点で，以下のサーバに対してハードウェアの外観点検（例：インジケータランプの状態確認，ケースの変形有無確認），各リソース（CPU，メモリ等の主記憶装置、HDD等の補助記憶装置）の使用状況（平均，ピーク，時間変化）等の実測値の把握及び適切なリソース割当て作業の実施，正常設定の確認等（各サーバの設定の変更前後の管理や世代管理，ログ（イベントログ，Syslog等）の確認とログが一杯になった時の保存・退避・消去）を実施すること。 なお，今後の各システムの更新に伴い，対象となるサーバは増減することがある。 ① ActiveDirectoryサーバ ② ファイルサーバ ③ バックアップ管理サーバ，バックアップメディアサーバ ④ 外部ファイル共有サーバ ⑤ ユーザ管理サーバ ⑥ メール中継サーバ ⑦ ウイルス対策サーバ ⑧ WSUSサーバ ⑨ クライアント運用管理サーバ ⑩ プロキシサーバ ⑪ 京都サーバ ⑫ ネットワーク管理システム ⑬ グループウェアシステム ⑭ 正倉院宝物公開管理システム ⑮ CADシステム ⑯ KMSサーバ ⑰ 資産管理サーバ ⑱ 標的型攻撃対策システム ⑲ ADFSサーバ ⑳ 暗号化管理サーバ ㉑ 暗号化ファイルサーバ ㉒ その他 マシン室設置の各ネットワーク機器，ファイアウォール，アプライアンス機器及び無停電電源装置（UPS）についても，インジケータランプの確認等を実施すること。	必須						左記について，理解した上で対応できるか。
6.3.9.2 システム稼働状態の把握							
システムに負荷がかかっているかどうかの判断をするために，【6.3.9.1.システム運用と性能管理】にて取得した情報からハードウェア資源の使用量が基準を超えていないか把握すること。	必須						左記について，理解した上で対応できるか。
6.3.9.3 トラフィック状態の把握							
別紙2，3及び5にに記載の各拠点のトラフィックを監視すること。ネットワークの負荷を判断するために，常時監視によりトラフィック量が基準を超えていないか，把握すること。	必須						左記について，理解した上で対応できるか。
6.3.10.サーバ室温度管理							
サーバ室の室温が28℃以上になった時，甲担当者及び運用担当者のメールアカウント及び運用担当者又はその管理者の携帯メールに異常を知らせるためのアラートメールを送信する設定をすること。運用担当者又はその管理者は，アラートメール受信（24時間365日受信対応が可能であること。）後は速やかに，甲担当者に報告を行い，空調機確認のアクションを取ること。	必須						左記について，理解した上で対応できるか。
6.3.11.予備機器，消耗品等の管理							
(1) 管理対象 クライアント端末，HUB，UTPケーブル，デジタル周辺機器等の予備機，保証書及びライセンス証書ならびに保証書（写し）も含む。	必須						左記について，理解した上で対応できるか。
(2) 保管場所 保管場所については，甲からの指示に従うこと。	必須						
(3) 管理内容 予備機器，消耗品の在庫状況及び修理状況を把握すること。	必須						
(4) 緊急支援 予備機器が修理未了及び消耗品に欠品がある状況で障害が発生した場合は，甲担当者と相談の上，障害復旧支援を行うこと。	必須						
6.3.12.ユーザサービス（ヘルプデスク）							
6.3.12.1 サービス範囲							
サービスデスク業務は，宮内庁NWを利用するユーザ及び当該ユーザが利用する機器等に対し提供される。運用管理業務は，通常運用管理，障害対応と適切に連携して行うことが求められる。	必須						左記について，理解した上で対応できるか。
6.3.12.2 ユーザサービス							
宮内庁NWの利用に際しては，ユーザの申請に基づきサービスを提供することが原則となっている。ユーザサービスはユーザからの申請を受付けて対応するものであり，以下に列挙する作業内容を含む（具体的内容は例示であり，これに限定されるものではない。）。	必須						
(1) アカウント関連の申請対応 ユーザアカウントの新規作成，変更，メールアドレスの新規作成，パスワード新規作成，再発行，人事異動に付随した各種設定変更（人事異動情報は，ユーザ管理システムを使用）及びユーザアカウント・機器等の関連付け情報の管理等，ユーザへのサービスに影響がないよう必要な作業を確実に実施すること。	必須						
(2) ソフトウェア，アプリケーション等の配布（インストール）管理 ソフトウェア，アプリケーション及びドライバ等の配布（インストール），削除（アンインストール）及び同ライセンス管理を行うこと。	必須						
(3) アクセス権の付与 ① 人事異動等に伴うファイルサーバへの共有フォルダアクセス権の付与。 ② ファイルサーバへの一時的なアクセス権の付与。 ③ 個別又は組織横断的な利用権限を設定する必要のある特定のフォルダの利用設定。	必須						
(4) インターネット（外部）からの情報のダウンロード 原則として禁止しているインターネット（外部）からの情報のダウンロードのための，一時的なコンテンツフィルタリングの設定変更を行うこと。	必須						
(5) 貸出し用クライアント端末，デジタル周辺機器等の貸与，設定及び管理 ① 情報管理室に保管されている貸出し用クライアント端末等について，甲担当者からの指示に基づき，貸出し，設定及びその管理を行うこと。また，貸出し時には，スタンドアロン用，宮内庁NW接続用に応じ，ソフトウェア，アプリケーション及びドライバ等のインストールを行うこと。 ② 個別ユーザの申請に基づきソフトウェアの追加，設定を行うこと。 ③ 貸出し用クライアント端末全台に対し新規ソフトウェアをインストールする作業等，個別ユーザ申請とは言えないものは，随時運用管理とし，本調達の対象外とする。 ④ 必要に応じて，ユーザ等への貸出し機器の説明や操作方法についての説明を実施すること。	必須						左記について，理解した上で対応できるか。
(6) IPアドレスの管理 ① 機器等，クライアント端末，プリンタ等，個別システムのIPアドレス及び関連情報を管理すること。 ② ネットワークに接続する必要がある機器等に対して，IPアドレスの付与，変更，削除を行うこと。	必須						
(7) 簡易配線 クライアント端末及びプリンタ等の新設，増設，移設に伴うUTPケーブル等の簡易配線及びUTPケーブル作成を行うこと。	必須						
(8) 申請全般に係る対応 ユーザ管理システムに関するユーザからの使用方法などの問合せについて対応すること。	必須						
(9) イントラネット上のFAQ（宮内庁職員情報ボード）の更新作業 宮内庁職員情報ボードに関するユーザからのアクセス権限，更新作業依頼などの問合せについて対応すること。	必須						左記について，理解した上で対応できるか。
(10) その他，個別事項に係る対応について ユーザからの各種問合せ，申請等に関して，随時対応すること。	必須						
6.3.12.2 ユーザサービス 【再掲】							
宮内庁NWの利用に際しては，ユーザの申請に基づきサービスを提供することが原則となっている。ユーザサービスはユーザからの申請を受付けて対応するものであり，以下に列挙する作業内容を含む（具体的内容は例示であり，これに限定されるものではない。）。		加点	100	50	25	0	効果的なユーザサービスを実現するに当たり，具体的な提案を示し，それが有効かつ妥当性があると認められる場合は加点として評価する。
(1) アカウント関連の申請対応 ユーザアカウントの新規作成，変更，メールアドレスの新規作成，パスワード新規作成，再発行，人事異動に付随した各種設定変更（人事異動情報は，ユーザ管理システムを使用）及びユーザアカウント・機器等の関連付け情報の管理等，ユーザへのサービスに影響がないよう必要な作業を確実に実施すること。							
(2) ソフトウェア，アプリケーション等の配布（インストール）管理 ソフトウェア，アプリケーション及びドライバ等の配布（インストール），削除（アンインストール）及び同ライセンス管理を行うこと。							
(3) アクセス権の付与 ① 人事異動等に伴うファイルサーバへの共有フォルダアクセス権の付与。 ② ファイルサーバへの一時的なアクセス権の付与。 ③ 個別又は組織横断的な利用権限を設定する必要のある特定のフォルダの利用設定。							
(4) インターネット（外部）からの情報のダウンロード 原則として禁止しているインターネット（外部）からの情報のダウンロードのための，一時的なコンテンツフィルタリングの設定変更を行うこと。							
(5) 貸出し用クライアント端末，デジタル周辺機器等の貸与，設定及び管理 ① 情報管理室に保管されている貸出し用クライアント端末等について，甲担当者からの指示に基づき，貸出し，設定及びその管理を行うこと。また，貸出し時には，スタンドアロン用，宮内庁NW接続用に応じ，ソフトウェア，アプリケーション及びドライバ等のインストールを行うこと。 ② 個別ユーザの申請に基づきソフトウェアの追加，設定を行うこと。 ③ 貸出し用クライアント端末全台に対し新規ソフトウェアをインストールする作業等，個別ユーザ申請とは言えないものは，随時運用管理とし，本調達の対象外とする。 ④ 必要に応じて，ユーザ等への貸出し機器の説明や操作方法についての説明を実施すること。							
(6) IPアドレスの管理 ① 機器等，クライアント端末，プリンタ等，個別システムのIPアドレス及び関連情報を管理すること。 ② ネットワークに接続する必要がある機器等に対して，IPアドレスの付与，変更，削除を行うこと。							
(7) 簡易配線 クライアント端末及びプリンタ等の新設，増設，移設に伴うUTPケーブル等の簡易配線及びUTPケーブル作成を行うこと。							
(8) 申請全般に係る対応 ユーザ管理システムに関するユーザからの使用方法などの問合せについて対応すること。							
(9) イントラネット上のFAQ（宮内庁職員情報ボード）の更新作業 宮内庁職員情報ボードに関するユーザからのアクセス権限，更新作業依頼などの問合せについて対応すること。							
(10) その他，個別事項に係る対応について ユーザからの各種問合せ，申請等に関して，随時対応すること。							
6.3.13.問合せヘルプ							

評価対象	必須	加点	加点評価 特に優秀	加点評価 優秀	加点評価 標準	加点評価 加点なし	評価基準
問合せヘルプ対応は，ユーザサービス業務，障害対応の窓口となるものである。以下の対応内容を含むものとする。 なお，対応は分かりやすい日本語とする。	必須						左記について，理解した上で対応できるか。
(1) 問合せ対応 ① ユーザが利用するハードウェア及びソフトウェアの操作，障害等に関する問合せ対応 ② サーバ，ネットワーク機器等の設定，障害等に関する問合せ対応 ③ 各地方拠点との接続環境に関する問合せ対応	必須						
(2) 一次切り分け ① 問題の所在の切り分け ② 障害対応（ユーザの利用する機器等のリプレイス等）	必須						
(3) リモートツールによる対応 ① 現行宮内庁NWでは，資産管理ソフトウェアを全拠点のクライアント端末に配布済みであり，問合せヘルプ業務において本製品を利用することが可能である。 ② ユーザに負担なく円滑に支援業務を遂行すること。	必須						
(4) オンサイトによる対応	必須						

6.3.13.問合せヘルプ 【再掲】

問合せヘルプ対応は，ユーザサービス業務，障害対応の窓口となるものである。以下の対応内容を含むものとする。 なお，対応は分かりやすい日本語とする。		加点	100	50	25	0	左記(1)から(4)について，効果的なユーザサービスを実現するに当たり，具体的な提案を示し，それが有効かつ妥当性があると認められる場合は加点として評価する。
(1) 問合せ対応 ① ユーザが利用するハードウェア及びソフトウェアの操作，障害等に関する問合せ対応 ② サーバ，ネットワーク機器等の設定，障害等に関する問合せ対応 ③ 各地方拠点との接続環境に関する問合せ対応							
(2) 一次切り分け ① 問題の所在の切り分け ② 障害対応（ユーザの利用する機器等のリプレイス等）							
(3) リモートツールによる対応 ① 現行宮内庁NWでは，資産管理ソフトウェアを全拠点のクライアント端末に配布済みであり，問合せヘルプ業務において本製品を利用することが可能である。 ② ユーザに負担なく円滑に支援業務を遂行すること。							
(4) オンサイトによる対応							

6.3.14.情報セキュリティインシデント対応

6.3.14.1 現状把握

(1) 影響範囲の推定 (ア) 各種ログ(操作，実行，通信等の履歴)を確認，整理，解析することで，情報セキュリティインシデントの影響範囲を推定すること。 -【参考】ログの取得については次を参照。「適切なログの管理による標的型攻撃対策について（情報提供）（閣副安危第 375 号 平成24年7月5日）」 http://www.nisc.go.jp/active/general/pdf/logkanri_kanki_120705.pdf (イ) 必要に応じて宮内庁統合NWのSOCサービスからの情報の提供を受け，プロキシサーバやファイアウォール等にある外部（インターネット等）との通信ログを確認，時系列による整理と解析を行って攻撃対象範囲の絞り込みを行いつつ，実際に攻撃対象となったPC又はサーバの特定を行うこと。 (ウ) ネットワーク機器等の設定情報やログの改ざんが無いかの確認を行うこと。また，次の注意喚起などを参考にし，ADなどのディレクトリ・サービスに対し，サーバ上の各種ログも解析すること。 <<< JPCERT/CC Alert 2014-12-19 >>> Active Directory のドメイン管理者アカウントの不正使用に関する注意喚起 https://www.jpcert.or.jp/at/2014/at140054.html (エ) 攻撃対象となった端末又はサーバ及び外部への不審な通信履歴などが特定された場合，適宜，プロキシサーバやファイアウォールなどの設定の見直しを図りつつ，各組織の判断により外部との通信を遮断（遮断した場合の影響を十分に考慮，対処した上で）するなどの処置を検討する。	必須						左記について，理解した上で対応できるか。
(2) 被害の特定 まず証拠保全を行う。次に攻撃対象となったPC又はサーバ上のファイルに不正なアクセス又は操作の履歴がないか確認することで，被害の特定をする。 ・ 攻撃対象となったPC又はサーバ上での証拠保全を行う -「証拠保全ガイドライン 第6版」（2017年5月9日 特定非営利活動法人デジタル・フォレンジック研究会 「技術」分科会ワーキング・グループ） https://digitalforensic.jp/home/act/products/df-guideline-6th/ - デジタル・フォレンジックを実施し，電磁的記録の証拠保全及び調査・分析を行い，電磁的記録の改ざん・毀損等について分析・情報収集等を行う。 - 不正なアクセス又は操作履歴がないかの具体的な確認方法は，以下も参考になる。 -【注意喚起】潜伏しているかもしれないウイルスの感染検査を今すぐ！（IPA） - https://www.ipa.go.jp/security/ciadr/vul/20150629-checkpc.html -「高度サイバー攻撃への対処におけるログの活用と分析方法」 - https://www.jpcert.or.jp/research/apt-loganalysis.html - JPCERT/CC「ログを活用したActive Directoryに対する攻撃の検知と対策」 - https://www.jpcert.or.jp/research/AD.html ・ 攻撃対象となったPC又はサーバにて適切に証拠保全がなされたならば，2社以上の異なる製造業者製のウイルス対策ソフトウェア（必ず最新にアップデートしたもの）を用いてフルスキャンを実行 - 既にインストールされているウイルス対策ソフトウェアの製造業者とは異なる製造業者製ウイルス対策ソフトウェアを用いることにより，製造業者の得意，不得意，そして新しいウイルスへの対応の早さなどの違いを補完し合う。なお，ウイルス対策ソフトウェアは，同一OS(Operating System)上ではシステム競合を起こすため，必ず1つのOS上では1つのウイルス対策ソフトウェアとなるよう，適切にアンインストール又はインストールを行うこと。 ・ 攻撃対象となったPC又はサーバ上での操作ログの確認，時系列による整理と解析 ・ 攻撃対象となったPC又はサーバを起点とした通信ログの確認，時系列による整理と解析 ・ ここまでに得られた各ログを時系列に並べて整理し，ログ同士の関係性がないか解析（相関分析等）し，感染経路を特定 ・ 攻撃対象となった端末又はサーバについては，ウイルス対策ソフトウェアと連携して遮断の上，端末の資産管理ソフトウェアにてネットワークの隔離を行いながら調査に必要な通信の解析及びリモートによる解析を行うこと。	必須						左記について，理解した上で対応できるか。
(3) 情報の取り扱い状況の確認 攻撃対象となったPC又はサーバ上での情報の取り扱いについて，組織における情報セキュリティポリシーやその他規程に則り，適切な情報の取り扱いをしているかを確認する。 ・ 取り扱われていた情報はどういう性質（機密性，完全性，可用性）のものだったか ・ ファイル又はフォルダへのアクセス制御を施していたか ・ ファイル又はフォルダに暗号化を施していたか（暗号危殆化に配慮しつつ） ・ パスワードの管理は適切であったか - 同じパスワードの使い回しはしていないか - 比較的わかりやすいパスワードでないか - 付箋紙などに書いて人の目につきやすいところに置いていないか など	必須						
(4) 脆弱性の確認 セキュリティ侵害のリスクを減らす目的で，既知の脆弱性を点検する。脆弱性の対策が施されていなければ，対策を施す。 ・ インストールされているソフトウェアのセキュリティパッチの適用状況の確認	必須						
・ OS及び各アプリケーションソフトウェアが最新のものにバージョンアップされていることの確認（MyJVN バージョンチェッカの利用） http://jvndb.jvn.jp/apis/myjvn/vccheck.html ・ プロキシサーバ，ファイアウォール，ネットワーク機器等が適切に設定されていることの確認 ・ 既知の脆弱性の対策の適用状況の確認 など	必須						
(5) 残存リスク等の把握 ・ リスクアセスメント（①標的とされる蓋然性の高い業務領域の選定，②リスク評価の実施）を実施しつつ，改めて取り扱う情報は何であり，どのような社会的意味を持ち，どのような影響を与えるものかなどを分析し直す。 「国家安全保障戦略（平成25年12月17日 国家安全保障会議決定 閣議決定）」（5）サイバーセキュリティの強化「平素から，リスクアセスメントに基づくシステムの設計・構築・運用」 http://www.cas.go.jp/jp/siryou/131217anzenhoshou.html 「高度サイバー攻撃対処のためのリスク評価等のガイドライン（平成26年7月10日 内閣サイバーセキュリティセンター(NISC)）」 http://www.nisc.go.jp/active/general/risk.html 「情報セキュリティマネジメントとPDCAサイクル（IPA）」 http://www.ipa.go.jp/security/manager/protect/pdca/risk_ass.html	必須						左記について，理解した上で対応できるか。

6.3.15.情報システムインシデント対応

宮内庁本庁舎及び各拠点に設置されている宮内庁NWSを構成するサーバ機器，ネットワーク機器，クライアント端末が対象。ただし，宮内庁統合NWのインターネット側に設置されている機器等は除くこととする。 なお，宮内庁統合NWとの境界点で発生した情報システムインシデントについては，宮内庁統合NW受託者と互いに情報共有を行い，密に協力して対応することにより，迅速な解決を行うことにより，ユーザの業務遂行への影響を最小化すること。	必須						
(1) 障害検知 ① リモート検知 宮内庁NW各拠点のネットワーク（ただしアクセススイッチ，ルータまで）及びサーバ等について，監視装置により異常検知すること。 ② ユーザによる通報 ユーザからの通報に対し，速やかに状況を確認すること（ユーザからの通報には，電話による通知とメールによる通知の2種類がある。）。	必須						
(2) 発生時対応 ① 一次切り分け ・ 障害を検知した場合は速やかに障害発生機器等を特定し，ハードウェア障害，ソフトウェア障害等の一次切り分けを実施すること。 ・ 全ての情報機器のうち，データの保存されている障害機器を持ち出すことになった場合は，情報漏えいがないようデータ消去すること。 ・ 物理的にデータ消去が不可能な場合には，甲担当者に報告した上で指示を仰ぐこと。 ② システム保守事業者，製造事業者等保守契約の関係者に連絡をとること。また，修理に必要な障害内容報告書を作成すること。 ③ 必要に応じて障害機器における障害発生日時前のコンフィグやログを取得し，障害切り分けを行うこと。 ④ 回線異常と判断した場合は，甲担当者を通じて回線事業者へ試験及び修理対応を依頼すること。 ⑤ ディスクリソースやメモリリソースでの異常と判断した場合は，甲担当者の承諾を得た上で復旧作業を行うこと。	必須						左記について，理解した上で対応できるか。

評価対象	必須	加点	加点評価 特に優秀	加点評価 優秀	加点評価 標準	加点評価 加点なし	評価基準
⑥ サービスデスクによるクライアント端末障害対応 ・ クライアント端末については，リモートツールによるユーザとの対話形式での対応を行うものとする。 ・ 甲担当者の指示により，障害機器については，システム保守事業者，製造事業者等の保守契約関係事業者に連絡をとり，修理完了まで管理すること。ただし，クライアント端末のシステム不調に対しては，その不調の状態に応じてHDDの初期化，OSの再設定，個別ソフトウェアの再インストールなどを適宜実施し，当該クライアント端末を利用するユーザの環境に合わせて正常に動作するよう適切に設定を行うこと。 なお，マスタ・イメージが存在するクライアント端末（一般事務用端末，追加一般事務用端末，CAD用端末）については，そのマスタ・イメージを利用して復元を行い，当該クライアント端末を利用するユーザの環境に合わせて正常に動作するよう適切に設定を行うこと。 ・ プリンタ（リース物品）の障害について保守が必要な場合は，甲担当者に対して，製造事業者等窓口に保守を依頼するよう伝えること。							
(3) 復旧 ① 各システムの保守事業者，製造事業者等保守契約の関係者による復旧作業に対し，適切に情報提供等の支援を行うこと。復旧後の動作確認を実施すること。 ② 復旧作業に際し，作業員がサーバ室への入室が必要となる場合は，事前に保守担当者の氏名や機器の搬入経路等を把握し，甲担当者の承諾を得た上で入庁及び搬入の手続きを支援すること。また，来室した時点で本人確認を行い，入退室の時刻や作業内容を指定の書類へ記載し管理すること。 ③ 冗長化された機器の障害復旧作業は，保守事業者と協力し，切り戻しまで行うこと。 ④ クライアント端末及びプリンタで発生した障害については，指定の書式で記録し，発生時の現象や復旧までの対応を管理すること。	必須						
(4) ステータス管理 ① 障害検知から復旧完了までのステータスを逐次記録し，遅滞することなく報告すること。 ② 継続的又は断続的に発生している障害がある場合は，構築事業者や保守事業者と協力し，対策を講じること。	必須						
(5) 事後管理 ① 障害検知から復旧完了までの記録を含む障害情報，障害対応支援内容につき履歴管理情報を更新すること。 ② 発生した障害について，再発を防止できる対策を講じ，甲担当者へ報告すること	必須						
6.4.宮内庁CIS以外の宮内庁NWSの運用管理							
個別システムの運用管理については，【6.3.8.情報セキュリティ管理】及び【6.3.9.性能管理】に記載されている各項目のほか，次のとおり個別システムの運用管理を実施すること。	必須						左記について，理解した上で対応できるか。
6.4.1.正倉院宝物公開管理システム							
必要に応じてバックアップテープを甲本庁から送付すること。また，返却されたテープを管理すること。また，正倉院宝物公開管理システムの宝物管理用端末2式（正倉院事務所）は，本調達の運用管理の対象となるので，次の作業内容を実施すること。	必須						左記について，理解した上で対応できるか。
(1) OSのアップデート又はパッチ適用	必須						
(2) ウイルス対策ソフトのアップデート又はパッチ適用 必要に応じたソフトウェアのインストール又はアンインストール	必須						
6.4.2.CADシステム							
① データベースのバックアップ取得状況を確認すること。	必須						左記について，理解した上で対応できるか。
② UPSを含むシステム全体のLED表示状態確認をすること。	必須						
6.4.3.電子メール中継サーバ							
① サーバのデータ領域のバックアップ取得状況を確認すること。	必須						左記について，理解した上で対応できるか。
② UPSを含むシステム全体のLED表示状態確認をすること。	必須						
6.4.4.グループウェアシステム							
グループウェアシステムに関して，次のとおり実施すること。	必須						左記について，理解した上で対応できるか。
(1) グループウェア機能が適切に提供されているか，サーバ等の稼働確認を行うこと。適切に機能が提供されていない場合は，遅滞なくインシデント管理を行うこと。	必須						
(2) ユーザがグループウェアシステムを利用するために用いるクライアントソフトウェアとグループウェア機能を提供するサーバ等との連携が正常に機能しているか確認を行うこと。	必須						
(3) メール中継サーバとグループウェア機能を提供するサーバ等との連携が正常に機能しているか確認を行うこと。	必須						
(4) ユーザのメールアドレス，グループメールアドレスの管理（作成，変更，削除）を行うこと。	必須						
(5) ユーザのグループウェアのアカウントについて，ディレクトリサーバとの連携が正常に機能しているか確認を行うこと。	必須						
(6) メール誤送信防止機能が適切に提供されているか，サーバ等の稼働確認を行うこと。	必須						
(7) グループウェアシステムのオンプレミス型のサーバ等に対し，ソフトウェアのアップデート又はパッチ適用を適切に行うこと。	必須						
(8) グループウェアシステムのオンプレミス型のサーバ等のハードウェアにおいて，LED表示状態を確認すること。	必須						
(9) グループウェアシステムのオンプレミス型のサーバ等において，冗長化された構成であるものについては，冗長化機能が正常に機能しているか確認を行うこと。	必須						
(10) 現行のグループウェアシステムの賃貸借期間は，平成33年8月31日（火）までである。この間にグループウェアシステムの更改がある場合には，ユーザが更改後のグループウェアシステムの（以下，「次期グループウェアシステム」という。）を利用して行う業務が遅滞なく遂行できるよう，次期グループウェアシステムの稼働後の効率的かつ安定的な運用を見据え，設計・構築段階からITサービスマネジメントの観点で可能な限り協力し，適宜助言を行うこと。	必須						
6.4.5.標的型攻撃対策システム							
標的型攻撃対策システムに関して，以下のとおり実施すること。ただし，現行の標的型攻撃対策システムを構成要素のうち，メール標的型攻撃対策サーバ及びSOCサービスについては含まない。	必須						左記について，理解した上で対応できるか。
(1) Web標的型攻撃対策サーバ及びファイアウォールの稼働確認を行うこと。	必須						
(2) SOCサービスからの情報セキュリティインシデント発生の報告を確認し，その内容に対して次の事実確認を行うこと。 運用管理業務の対象となる甲の各拠点（ただし，データセンタを除く。）に設置されたサーバ，ネットワーク機器，クライアント端末に関する不正な通信の可能性がある場合には，情報セキュリティインシデント対応を行うこと。	必須						
(3) ファイアウォールの稼働確認を行うこと。	必須						
(4) ファイアウォールポリシーの更新を行うこと。	必須						
(5) UPSを含むシステム全体のLED表示状態を確認すること。	必須						
6.4.6.電子ファイルの暗号化及びアクセス制御機能							
電子ファイルの暗号化及びアクセス制御機能について，以下のとおり実施すること。	必須						左記について，理解した上で対応できるか。
(1) OSのアップデート又はパッチ適用	必須						
(2) ウイルス対策ソフトのアップデート又はパッチ適用 必要に応じたソフトウェアのインストール又はアンインストール	必須						
(3) ソフトウェアに対する修正パッチ及び修正モジュールがメーカから提供された場合に，適用要否を検討し，甲担当者と協議し，必要なパッチについて適用を行うこと。	必須						
(4) 運用上バックアップが必要なファイル群のバックアップ	必須						
(5) 暗号鍵及びシステム復旧する上で必要なログファイルのバックアップ	必須						
(6) UPSを含むシステム全体のLED表示状態を確認すること。	必須						
(7) 電子ファイルの暗号化及びアクセス制御機能のサーバ等において，冗長化された構成であるものについては，冗長化機能が正常に機能しているか確認を行うこと。	必須						
(8) 甲担当者の求めに応じて，必要な設定変更を行うこと。	必須						
(9) 障害が発生した場合は，バックアップイメージ等からシステム復旧を行うなどの措置を行うこと。また，復旧後に暗号化機能が正常に動作しているか確認すること。	必須						
6.4.7.Web無害化機能							
Web無害化機能について，甲担当者の求めに応じて，プロキシ設定変更を行うこと。	必須						左記について，理解した上で対応できるか。

評価対象	必須	加点	加点評価 特に優秀	優秀	標準	加点なし	評価基準
6.5. 機器等の変動に関する支援							
乙は，将来更新が予定されている本調達仕様書（案）「6.6.機器等の変動」に示す11の各次期システム等について，更新作業を適正かつ円滑に行うため，11の各次期システム等機器賃貸等事業者（以下「次期システム事業者」という。）が開催する会議への参加，各次期システム運用に必要な環境設定支援，検証等を専門的知識からの支援，助言を行うこと（表1.各次期システム等機器変動（更新・移行）に伴い想定される乙の作業等）。なお，各次期システム更新に係る設計，開発は次期システム業者が実施する。 【表1の記載は省略】	必須						左記について，理解した上で対応できるか。
6.5.1.会議							
次期システム事業者が開催するシステム更新・移行に係る会議に参加すること。	必須						左記について，理解した上で対応できるか。
6.5.2.システム運用業務設計（支援）							
次期システムの運用業務設計は次期システム事業者が実施する。乙は，宮内庁NW及び各システムの構成や運用体制等の情報について速やかに提示する等，次期システム事業者の支援を行うこと。	必須						左記について，理解した上で対応できるか。
		加点	40	20	10	0	効果的な支援を行うための具体的で有効かつ妥当性のある方針・提案を示した場合は，加点として評価する。
6.5.3.システム移行作業（支援）							
次期システム事業者より提示されるシステム移行計画書に基づき移行スケジュールの調整支援，システム運用管理業務を移行すること。移行時においてトラブルが発生した場合には，次期システム事業者と連携し速やかにトラブルを解消すること。	必須						左記について，理解した上で対応できるか。
		加点	40	20	10	0	効果的な支援を行うための具体的で有効かつ妥当性のある方針・提案を示した場合は，加点として評価する。
6.5.4.試験（支援）							
次期システム事業者が作成，提示する試験計画書，試験実施要項に基づき試験項目を支援すること。 想定される次期システム事業者が行う各試験は次のとおり。各試験実施に当たり，次期システム支援事業者及び甲より支援を求められた場合には支援を行うこと。 (1) 単体試験 (2) 結合試験 (3) 総合試験 (4) 受入試験	必須						左記について，理解した上で対応できるか。
		加点	40	20	10	0	効果的な支援を行うための具体的で有効かつ妥当性のある方針・提案を示した場合は，加点として評価する。
6.5.5.教育							
乙は，次期システム事業者が作成する教育計画書に基づき各システム運用管理業務支援に係る教育を受講すること。	必須						左記について，理解した上で対応できるか。
6.5.6.その他							
(1) 機器等の変動に関し，新規資産納入者への甲についての情報提供，導入検討，移行等必要となる支援を行うこと。	必須						左記について，理解した上で対応できるか。
		加点	100	50	25	0	効果的な支援を行うための具体的で有効かつ妥当性のある方針・提案を示した場合は，加点として評価する。
(2) 毎年4月1日付の人事異動はユーザ登録件数が多いことを理解した上で円滑に登録作業を遂行すること。	必須						左記について，理解した上で対応できるか。
		加点	40	20	10	0	人事異動が多い時期の業務に具体的にどのような工夫を施すかを示し，それが有効かつ妥当性がある場合は，加点として評価する。
6.6.機器等の変動							
6.6.1.宮内庁統合NW更新に伴う支援							
「宮内庁デジタル・ガバメント中長期計画」（平成30年6月22日　宮内庁行政情報化推進委員会決定）に基づくネットワークの更新作業を平成31年度に実施する予定である。更新スケジュールの概要は「図2-1.宮内庁NW更新スケジュール」のとおり。詳細は，受注後に甲に確認すること。これに伴い，以下の支援を行うこと。 【図2-1.の記載は省略】	必須						左記について，理解した上で対応できるか。
(1) 業務支援 ① 宮内庁統合NWの次期更新に係る会議に参加し，次に示す観点に基づいて次期宮内庁統合NWの設計や運用等について助言すること。 (ア) 次期宮内庁統合NWと宮内庁CISを始めとした宮内庁NWSの各システムとの連携が円滑になり，ユーザの業務の効率化を実現 (イ) 宮内庁NWS全体として，各システムが連携し，効果的な情報セキュリティ対策の強化を実現 ② 移行期間中においては，次期宮内庁NWS請負者と連携し，機器等の設定等について十分な調整を行い，甲からの問合せに対応すること。 ③ 次期宮内庁統合NWの受入テストの実施に立ち合うこと。 なお，受入テストの実施の主体は甲となる。また，次期宮内庁NWS請負者が受入テストの支援を行う。	必須						
(2) 更新機器等の管理 ① 更新されるネットワーク機器等の運用管理等を行うこと。 ② サーバ室への導入機器が発生する場合には，技術的な問題解決を行うとともに，協業して目的を達成すること。	必須						
(3) 不測の事態への対応支援 導入に際して，宮内庁NWに障害が発生した場合には，甲担当者及び障害に関連する現行他システム保守事業者と綿密な調整・連携を行い復旧に努めること。	必須						
(4) 設置・作業時の立会い 適宜，必要に応じて現地立会いを行うこと。	必須						
(5) その他 本調達仕様書（案）に記載なき事項でも，本システムの構築・稼働・運用に必要と認められる事項は，甲と協議の上実施すること。	必須						
6.6.2.正倉院宝物公開管理システムの更新に伴う支援							
正倉院宝物公開管理システムの更新作業を2019年度（2020年1月より運用開始予定及び2023年度（2024年1月より運用開始予定）に実施する予定である。更新スケジュールの概要は「図2-2.正倉院宝物管理システム更新スケジュール」のとおり。詳細は，受注後に甲に確認すること。これに伴い，以下の支援を行うこと。 【図2-2.の記載は省略】	必須						左記について，理解した上で対応できるか。
(1) 業務支援 正倉院宝物公開管理システムの次期更新に係る会議に参加し，運用管理等について助言すること。また，移行期間中においては，次期本システム請負者と連携し，環境設定等について十分な調整を行い，甲からの問合せに対応すること。	必須						
(2) 本調達仕様書（案）6.6.1(2)～(5)と同じ。	必須						
6.6.3.宮内庁公開システムの更新に伴う支援							
宮内庁公開システムの更新作業を2019年度（2020年2月から運用開始予定）及び2023年度（2024年2月から運用開始予定）に実施する予定であるが，当該システムは政府共通PFに移行したため，次期更新に係る会議への出席等は要さない。ただし，更新時にDNS変換等が必要な場合，甲担当者の指示に従い対応すること。	必須						左記について，理解した上で対応できるか。
6.6.4.パーソナルコンピュータ及びプリンタの更新に伴う支援							
パーソナルコンピュータ及びプリンタの更新作業を2020年度中（2021年3月より運用開始予定）に実施する予定である。更新スケジュールの概要は「図2-4.パーソナルコンピュータ及びプリンタ更新スケジュール」のとおり。詳細は，受注後に甲に確認すること。これに伴い，以下の支援を行うこと。 【図2-4.の記載は省略】	必須						左記について，理解した上で対応できるか。
(1) 業務支援 パーソナルコンピュータ及びプリンタの次期更新に係る会議に参加し，運用管理等について助言すること。また，入れ替え期間中においては，次期本調達請負者と連携し，甲からの問合せに対応すること。	必須						
(2) 本調達仕様書（案）6.6.1(2)～(5)と同じ。	必須						
6.6.5.CADシステムの更新に伴う支援							
CADシステムの更新作業を2020年度中（2021年3月より運用開始予定）に実施する予定である。更新スケジュールの概要は「図2-5.CADシステム更新スケジュール」のとおり。詳細は，受注後に甲に確認すること。これに伴い，以下の支援を行うこと。 【図2-5.の記載は省略】	必須						左記について，理解した上で対応できるか。
(1) 業務支援 CADシステムの次期更新に係る会議に参加し，運用管理等について助言すること。また，移行期間中においては，次期本システム請負者と連携し，環境設定等について十分な調整を行い，甲からの問合せに対応すること。	必須						
(2) 本調達仕様書（案）6.6.1(2)～(5)と同じ。	必須						
6.6.6.グループウェアシステムの更新に伴う支援							
グループウェアシステムの更新作業を2021年度中（2021年9月より運用開始予定）に実施する予定である。更新スケジュールの概要は「図2-6.グループウェアシステム更新スケジュール」のとおり。詳細は，受注後に甲に確認すること。これに伴い，以下の支援を行うこと。 【2-6.図の記載は省略】	必須						

評価対象	必須	加点	加点評価				評価基準
			特に優秀	優秀	標準	加点なし	
(1) 業務支援 グループウェアシステムの次期更新に係る会議に参加し，運用管理等について助言すること。また，移行期間中においては，次期本システム請負者と連携し，環境設定等について十分な調整を行い，甲からの問合せに対応すること。	必須						左記について，理解した上で対応できるか。
(2) 本調達仕様書（案）6.6.1(2)～(5)と同じ。	必須						

6.6.7.標的型攻撃対策システムの更新に伴う支援

標的型攻撃対策システムの更新作業を2021年度中（2021年11月より運用開始予定）に実施する予定である。更新スケジュールの概要は「図2-7.標的型攻撃対策システム更新スケジュール」のとおり。詳細は，受注後に甲に確認すること。これに伴い，以下の支援を行うこと。 【図2-7.の記載は省略】	必須						左記について，理解した上で対応できるか。
(1) 業務支援 標的型攻撃対策システムの次期更新に係る会議に参加し，運用管理等について助言すること。また，移行期間中においては，次期本システム請負者と連携し，環境設定等について十分な調整を行い，甲からの問合せに対応すること。	必須						
(2) 本調達仕様書（案）6.6.1(2)～(5)と同じ。	必須						

6.6.8.ファイル自動暗号化システムの更新に伴う支援

ファイル自動暗号化システムの更新作業を2021年度中（2022年3月より運用開始予定）に実施する予定である。更新スケジュールの概要は「図2-8.ファイル自動暗号化システム更新スケジュール」のとおり。詳細は，受注後に甲に確認すること。これに伴い，以下の支援を行うこと。 【図2-8.の記載は省略】	必須						左記について，理解した上で対応できるか。
(1) 業務支援 ファイル自動暗号化システムの次期更新に係る会議に参加し，運用管理等について助言すること。また，移行期間中においては，次期本システム請負者と連携し，環境設定等について十分な調整を行い，甲からの問合せに対応すること。	必須						
(2) 本調達仕様書（案）6.6.1(2)～(5)と同じ。	必須						

6.6.9.WEB無害化システムの更新に伴う支援

WEB無害化システムの更新作業を2021年度中（2022年3月より運用開始予定）に実施する予定である。更新スケジュールの概要は「図2-9.WEB無害化システム自動暗号化システム更新スケジュール」のとおり。詳細は，受注後に甲に確認すること。これに伴い，以下の支援を行うこと。 【図2-9.の記載は省略】	必須						左記について，理解した上で対応できるか。
(1) 業務支援 WEB無害化システムの次期更新に係る会議に参加し，運用管理等について助言すること。また，移行期間中においては，次期本システム請負者と連携し，環境設定等について十分な調整を行い，甲からの問合せに対応すること。	必須						
(2) 本調達仕様書（案）6.6.1(2)～(5)と同じ。	必須						

6.6.10.図書寮文庫所蔵資料目録・画像公開システムの更新に伴う支援

図書寮文庫所蔵資料目録・画像公開システムの更新作業を2021年度（2021年11月から運用開始予定）に実施する予定であるが，当該システムは宮内庁NW外のクラウド環境にシステムを構築しているため，次期更新に係る会議への出席等は要さない。ただし，更新時にクライアント端末へのソフトウェアインストール等が必要な場合，甲担当者の指示に従い対応すること。	必須						左記について，理解した上で対応できるか。

6.6.11.テレワーク導入に伴う支援

「宮内庁におけるテレワーク試行実施要領」に基づき実施（予定）するもので，実施の際には，円滑に導入できるよう支援を行うこと。	必須						左記について，理解した上で対応できるか。
(1) 通信確認 テレワーク実施に伴い，次の確認を行うこと。 ① ログイン動作確認 ② メール動作確認 ③ インターネット接続確認 ④ 各アプリケーションの動作確認	必須						
実施状況（実績） ・ 平成27年度～平成29年度 ・ 対象者：平成27年度3名，平成28年度 5名，平成29年度 7名 ・ 対象期間：通年 ・ 利用サービス：「13. 資料閲覧」にて確認すること。	必須						

6.7.計画停電対応

(1) 年1 回実施される法定点検に伴う計画停電対応については，本調達の範囲内とし，次の対応を行うこと。 なお，法定停電日の具体的な日程については，甲担当者がその都度指示をする。 ① 通常，法定点検に伴う計画停電は，休日に行われるので，休日対応とする。 ② 停電の時間帯を基準に，サーバ及びネットワーク機器等の停止時間及び起動完了時間について，計画書を作成し機器等の停止及び起動を実施すること。 ③ サーバ及びネットワーク機器等の停止，起動及び起動後のサーバ及びネットワーク機器等の動作確認を行うこと。	必須						左記について，理解した上で対応できるか。
(2) 法定の停電以外の単発的な停電については，本調達の範囲外であるが，甲担当者の求めに応じて必要経費を見積り，法定停電と同様の対応を行うこと。	必須						

7. 会議体の設置

7.1.目的

本業務における基本設計書及び詳細設計書の検討，作業の進捗状況，課題管理の対応状況等を確認し，宮内庁統合NW受託者との認識合わせを実施することにより，宮内庁CISの構築及び運用を確実に実施するため，「宮内庁NWS統括会議」（以下，「統括会議」という。）を開催する。	必須						左記について，理解した上で対応できるか。

7.2.会議体スケジュール

【スケジュール図の記載は省略】	必須						左記について，理解した上で対応できるか。

7.3.開催開始時期

宮内庁CISの契約締結日から運用開始前日までの毎週木曜日13：30から15：00を基本とする。	必須						左記について，理解した上で対応できるか。

7.4.会議開催場所

甲が指定する場所。	必須						左記について，理解した上で対応できるか。

7.5.会議必須参加者

(1) 甲 (2) 宮内庁統合NW受託者 (3) 次期運用管理事業者（宮内庁CIS受託者） (4) 運用管理支援事業者	必須						左記について，理解した上で対応できるか。

7.6.会議内容等

(1) 会議参加者は，本調達の目的を達成し，宮内庁NWS全体として機能するようために必要な情報共有及び議論を積極的に行い，協力し合うこと。 (2) 乙は，次期運用管理事業者として，運用管理業務の実施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積極的に行うこと。 (3) 会議で取り上げる題材は主に次のとおりとするが，その時々の状況に応じて変更を可とする。会議で取り上げる題材の資料は，会議開始日の前日までに甲へ提出すること。 ・進捗状況（進捗管理） ・課題対応状況（課題管理） ・リスク対応状況（リスク管理） ・その他（必要に応じて） 特に宮内庁統合NWと宮内庁CISとの間で連携する内容を始めとして，契約が異なる情報システム間の連携が必要となる内容については，優先順位を上げて議論することとする。 なお，個別具体的な議論が必要な場合は，統括会議で協議の上で適宜，統括会議を親会議としたワーキング・グループを設置して議論し，円滑に設計・構築・運用を行い，議論の結果を統括会議へ報告すること。	必須						左記について，理解した上で対応できるか。

評価対象	必須	加点	加点評価 特に優秀	加点評価 優秀	加点評価 標準	加点評価 加点なし	評価基準
8. 応札者条件							
8.1.応札者としての条件							
(1) 公共サービス改革法第15条において準用する同法第10条各号（第11号を除く。）に該当する者でないこと。	必須						
(2) 予算決算及び会計令（昭和22年勅令第165号。以下「予決令」という。）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。	必須						
(3) 予決令第71条の規定に該当しない者であること。	必須						
(4) 平成31・32・33年度内閣府競争参加資格（全省庁統一資格）「役務の提供等」の「A」又は「B」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。	必須						
(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。	必須						
(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。	必須						
(7) 当庁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。	必須						
(8) 本調達仕様書の作成に直接関与した事業者及びその関連事業者（「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子会社並びに緊密な利害関係を有する事業者をいう。）ではないこと。	必須						
(9) 調達計画書及び調達仕様書の妥当性確認並びに入札事業者の審査に関する業務を行う宮内庁CIO補佐官及びその支援スタッフ等（常時勤務を要しない官職を占める職員，「一般職の任期付職員の採用及び給与の特例に関する法律」（平成12年11月27日法律第125号）に規定する任期付職員及び「国と民間企業との間の人事交流に関する法律」（平成11年12月22日法律第224号）に基づき交流採用された職員を除く。）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。又は，宮内庁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。	必須						左記の条件を満たしているか。
(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。 （注）入札参加グループとは本業務の実施を目的に複数の事業者が組織体を構成し，本業務の入札に参加する者のことを指す。	必須						
(11) 本業務の実施予定組織・部門は，品質管理体制としてISO9001:2015又は，組織能力成熟度のCMMIレベル3以上のどちらかの認証を取得しているか，同等の品質管理体制を構築できていることを必要十分に証明することが可能な資料を提出すること。	必須						
(12) 本業務の実施予定組織・部門は，プライバシーマーク付与認定，又はISO/IEC27001認証（国際標準）若しくはJIS Q 27001認証（日本工業標準）のいずれかを取得していること。	必須						
(13) 本業務の実施予定部門がISO14001 の認証を取得しており，環境マネジメントを適確に行う体制が整備されていることを証明すること。	必須						
(14) 過去5年以内に，本件と同等規模以上の情報システム構築（設計，開発及び導入）及び保守運用を請け負った実績を有すること。ただし，ヘルプデスクのみの実績は認めない。	必須						
(15) 資本関係・役員等の情報，受託作業の実施場所に関する情報，受託業務の従事者の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績及び国籍に関する情報を提案書とともに提出すること。	必須						
(16) 保守性を高めるためにベンダーロックインとならないよう，システムの設計において属人性を排除しつつ標準化を図り，オープンな技術やフレームワークによるシステム構築が可能であること。	必須						
8.2.本整備業務及び本保守業務の実施体制としての条件							
(1) 本整備業務及び本保守業務の確実な実施を担保するための作業体制をそれぞれ整えること。	必須						
(2) 各業務の作業体制表の作成に当たっては，作業責任者，役割，連絡先を明確にすること。	必須						左記の条件を満たしているか。
(3) 本整備業務におけるプロジェクトマネージャを1名以上配置し，プロジェクトマネージャの円滑なコミュニケーションによるプロジェクトマネジメントを実施することにより，本整備業務が遅滞なく完了させ，本保守業務及び本運用管理業務への移行をシームレスに橋渡しすること。プロジェクトマネージャは，以下の各条件を満たすこと。	必須						左記の条件を満たしているか。
① 過去5 年以内に構築がなされた宮内庁NWSの規模と 同等以上の情報システムにおいて，情報システム設計，構築，運用等のプロジェクトマネージャ又はプロジェクトリーダを務め，プロジェクトを成功に導いた経験を有すること。また，その経験を証明する情報システムの受注実績，規模（管理する要員数，受注金額など）などを示す証跡を提出すること。 ② 情報システム設計・構築・運用等いずれかの業務経験を5 年以上有すること。 ③ 米国PMI(Project Management Institute)認定のPMP(Project Management Professional)の資格を有するか，又は「IT スキル標準V3 2011」（平成24年3月26 日 IPA）のプロジェクトマネジメントのいずれかの専門分野で達成度指標及びスキル熟達度ともにレベル4に相当する実務上の知識・経験を有すること。 ④ 米国PMIのPMBOK(Project Management Body of Knowledge)最新版をPDU(Professional Development Unit)対象の研修受講により理解していること。また，その受講証明書を提出すること。 ⑤ PMBOK最新版に基づくステークホルダーマネジメントを熟知しており，コミュニケーション能力及び説明能力が高いこと。		加点	40	20	10	0	単に所持している資格条件だけでなく，具体的事例（これまで担ってきた役割，顧客と人間関係構築，出せた結果など）を用いてコミュニケーション能力及び説明能力が高いことを示した場合は加点とする。
(4) 原則としてプロジェクト体制の変更は認めないこととする。ただし，進捗に著しい遅れが発生した等で要員の追加及び作業担当者の変更がやむを得ない場合は，速やかに改善策を提示し甲の承諾を得ること。	必須						左記について，理解した上で対応できるか。
8.3.運用管理従事者の要件							
8.3.1.共通要件							
(1) 業務遂行においてユーザや既存各システムの構築・保守事業者と日本語による円滑で適切な意思疎通が図ることが可能なこと。	必須						
(2) 職業安定法第44条（労働者供給事業の禁止）及び労働基準法第6条（中間搾取の排除）に抵触した状態での運用仮従事者でないこと。	必須						
(3) 製造業者等が提供する製品マニュアル及び技術文献，一般的に書店などで入手可能な情報通信技術関連書籍などを参照しつつ，本調達で求める運用管理従事者（運用管理責任者，運用作業員，代替要員）の要件を満たした技術者としての専門的知識をあわせて最大限に活用し，甲からの情報システムに関する問合せなどの対応を適切に努め，宮内庁NWSが可能な限り効果的に利用可能となるよう維持運用に努めること。	必須						左記の条件を満たしているか。
(4) 社会情勢と環境の変化に合わせて変化する情報通信分野に関する技術や製品などについて継続的な情報収集や学習を行い，その知識を活用することにより，能動的に適切な宮内庁NWSの維持運用に努めること。	必須						
8.3.2.運用管理責任者（個人）の実績・資格							
(1)乙は，運用管理業務の円滑な実行や，運用作業員のみでは対処出来ない技術的な問題の解決やステークホルダーとの調整を円滑に行うため，運用管理責任者を設け，運用作業員のサポートを行うこと。 なお，運用管理責任者は，１週間のうち休日を除く平日の60%以上，1名が情報管理室に勤務することとし，以下の実績・資格を有することとする。ただし，運用管理責任者を複数配置する場合において，以下の③，④については，同一の者が両方を満たす必要はなく，運用管理責任者全体で③及び④を満たせばよいこととする。その場合には，運用管理責任者同士が密に連携をとって業務に臨むこと。	必須						左記の条件を満たしているか。
① 過去5 年以内に構築がなされた宮内庁NWSの規模と 同等以上の情報システムにおいて，情報システム設計，構築，運用等の責任者を務め，プロジェクトを成功に導いた経験を有すること。また，その経験を証明する情報システムの受注実績を示す文書を提出すること。	必須						
②情報システム設計・構築・運用等いずれかの業務経験を5 年以上有すること。	必須						
③ 「IT スキル標準V3 2011」のIT サービスマネジメントの専門分野のうち，オペレーション，運用管理，システム管理又はサービスデスクのいずれか一つで達成度指標及びスキル熟達度ともにレベル4以上に相当する実務上の知識・経験を有すること。	必須						
④ 「情報処理促進法」に基づいて行われる情報処理技術者試験のうち，ネットワークスペシャリスト試験の合格者及び又は「情報処理促進法」第15条の規定に基づく情報処理安全確保支援士の登録を受けている者（又は同等の資格を有する者）であるか，又は「IT スキル標準V3 2011」のITスペシャリストのいずれかの専門分野で達成度指標及びスキル熟達度ともにレベル4に相当する実務上の知識・経験を有すること。	必須						
8.3.2.運用管理責任者（個人）の実績・資格 【再掲】							
(1)乙は，運用管理業務の円滑な実行や，運用作業員のみでは対処出来ない技術的な問題の解決やステークホルダーとの調整を円滑に行うため，運用管理責任者を設け，運用作業員のサポートを行うこと。 なお，運用管理責任者は，１週間のうち休日を除く平日の60%以上，1名が情報管理室に勤務することとし，以下の実績・資格を有することとする。ただし，運用管理責任者を複数配置する場合において，以下の③，④については，同一の者が両方を満たす必要はなく，運用管理責任者全体で③及び④を満たせばよいこととする。その場合には，運用管理責任者同士が密に連携をとって業務に臨むこと。		加点	40	20	10	0	単に所持している資格条件だけでなく，具体的事例（これまで担ってきた役割，顧客と人間関係構築，出せた結果など）を用いてコミュニケーション能力及び説明能力が高いことを示した場合は加点とする。
① 過去5 年以内に構築がなされた宮内庁NWSの規模と 同等以上の情報システムにおいて，情報システム設計，構築，運用等の責任者を務め，プロジェクトを成功に導いた経験を有すること。また，その経験を証明する情報システムの受注実績を示す文書を提出すること。							
②情報システム設計・構築・運用等いずれかの業務経験を5 年以上有すること。							
③ 「IT スキル標準V3 2011」のIT サービスマネジメントの専門分野のうち，オペレーション，運用管理，システム管理又はサービスデスクのいずれか一つで達成度指標及びスキル熟達度ともにレベル4以上に相当する実務上の知識・経験を有すること。							

評価対象	必須	加点	加点評価 特に優秀	優秀	標準	加点なし	評価基準
④ 「情報処理促進法」に基づいて行われる情報処理技術者試験のうち，ネットワークスペシャリスト試験の合格者及び又は「情報処理促進法」第15条の規定に基づく情報処理安全確保支援士の登録を受けている者（又は同等の資格を有する者）であるか，又は「IT スキル標準V3 2011」のITスペシャリストのいずれかの専門分野で達成度指標及びスキル熟達度ともにレベル4に相当する実務上の知識・経験を有すること。							
8.3.3.運用作業員（個人）の実績・資格							
(1) 運用作業員（常駐者及び応援者）は，以下の実績・資格を有すること。	必須						左記の条件を満たしているか。
① 過去5 年以内に構築がなされた宮内庁NWの規模と 同等以上の情報システムにおいて，企画，設計・開発，運用に関する業務3 年以上従事した経験を有すること。ヘルプデスク業務のみの実績は認めない。	必須						
② 「IT スキル標準V3 2011」のITスペシャリストの専門分野のうち，ネットワーク，プラットフォーム，セキュリティ，システム管理のいずれか1つで達成度指標及びスキル熟達度ともにレベル3に相当する実務上の知識・経験を有すること。	必須						
③ 「IT スキル標準V3 2011」のIT サービスマネジメントの専門分野「オペレーション」で達成度指標及びスキル熟達度ともにレベル3以上に相当する実務上の知識・経験を有すること。	必須						
④ ITIL Foundation 以上の資格を有し，証明できること。	必須						
⑤ Windows サーバ及びクライアント，Linux サーバ，それらを接続するネットワーク機器についての運用経験を有しており，業務上必要なシェル・コマンドの操作，スクリプト及びバッチファイルの作成と正常動作確認ができる能力を有していること。	必須						
⑥ 甲で現在利用している汎用ソフトウェアや汎用ミドルウェア全般についての専門知識と操作経験を有しており，迅速なヘルプデスク業務が実施可能な能力を有していること。	必須						
8.3.3.運用作業員（個人）の実績・資格 【再掲】							
(1) 運用作業員（常駐者及び応援者）は，以下の実績・資格を有すること。		加点	40	20	10	0	単に所持している資格条件だけでなく，具体的事例（これまで担ってきた役割，顧客と人間関係構築，出せた結果など）を用いてユーザからの照会に対し，迅速な対応ができることを示した場合は加点とする。
① 過去5 年以内に構築がなされた宮内庁NWの規模と 同等以上の情報システムにおいて，企画，設計・開発，運用に関する業務3 年以上従事した経験を有すること。ヘルプデスク業務のみの実績は認めない。							
② 「IT スキル標準V3 2011」のITスペシャリストの専門分野のうち，ネットワーク，プラットフォーム，セキュリティ，システム管理のいずれか1つで達成度指標及びスキル熟達度ともにレベル3に相当する実務上の知識・経験を有すること。							
③ 「IT スキル標準V3 2011」のIT サービスマネジメントの専門分野「オペレーション」で達成度指標及びスキル熟達度ともにレベル3以上に相当する実務上の知識・経験を有すること。							
④ ITIL Foundation 以上の資格を有し，証明できること。							
⑤ Windows サーバ及びクライアント，Linux サーバ，それらを接続するネットワーク機器についての運用経験を有しており，業務上必要なシェル・コマンドの操作，スクリプト及びバッチファイルの作成と正常動作確認ができる能力を有していること。							
⑥ 甲で現在利用している汎用ソフトウェアや汎用ミドルウェア全般についての専門知識と操作経験を有しており，迅速なヘルプデスク業務が実施可能な能力を有していること。							
8.3.4.代替要員の実績・資格							
(1) 代替要員の実績・資格は，運用作業員の実績・資格の(1)に準ずる。	必須						左記の条件を満たしているか。
(2) 代替要員は，運用作業員の不慮の事故，疾病又は休暇により勤務できない場合を想定し，運用作業員との日頃からのコミュニケーションを積極的に行うなどし，宮内庁NWSの運用の状態の把握に努め，運用作業員からの業務の引継が円滑かつ確実に行うことが可能な状態を維持すること。	必須						

9. 移行・切替要件

9.1.移行・切替計画の策定

(1) 宮内庁NWSの安定した稼働及び業務の継続に影響を与えることがないよう，安全で確実な移行・切替計画を策定すること。	必須						左記について，理解した上で対応できるか。
(2) 移行計画は無理な移行とならないよう，安全かつ余裕を持ったスケジュールで切替計画を策定すること。	必須						
(3) 回線の切替日程は特定日に拠点の切替作業が集中しないよう，1日に行う切替の日程上限は2拠点以内を目途とし，順次切替行っていくこと。	必須						
(4) 本番移行の2週間以上前には移行リハーサルを実施し，本番時の切替が確実に行えるようにすること。本番移行時にはリハーサル時と本番時の環境の差分について明確にし，差異がある場合はリスク対処策を提示し甲の承諾を得ること。	必須						
(5) 移行切替後に不具合や問題が発生した際に，切り戻しが行えるよう，平行運用期間を1.5か月程度持たせること。	必須						
(6) 甲担当者と協議の上，移行・切替計画書を作成し，承諾を得ること。	必須						
9.2.移行・切替の方針							
(1) 担当者が承諾した日時を除き，宮内庁統合NWを始め各現行システムのサービスを停止することなく，移行・切替を実施すること。	必須						左記について，理解した上で対応できるか。
(2) 現行システムにおけるデータ利用に係る実態調査を行い，甲と協議の上，必要な全ての機能の移行・設定作業を行うこと。	必須						
(3) 宮内庁統合NWを始め各現行システムの停止を伴う作業が避けられない場合には，ユーザへの影響を最小限に抑えるため，原則として平日の勤務時間外又は休日を作業実施日として検討し，甲担当者の承諾を得ること。また，事前にその工程及び作業方法について，甲の承諾を得ること。 なお，国会開催時には，システム停止が許容されない場合がある。	必須						
(4) 宮内庁CIS導入に当たって，現行環境に設定，ツール等のインストール・アンインストールが必要となる際には，甲及び現行システムの構築・保守事業者及び管理者に設計等の情報を開示するとともに，甲からの指示に従うこと。	必須						
(5) 各現行システムの構築・保守事業者及び管理者間の各種調整などについては，甲の承諾を得た上で乙の責任のもとに実施することとし，宮内庁CIS導入に当たり，その調整等による不都合，負荷などが発生しないようにすること。	必須						
(6) 現行の環境は，各課にVLANを割り当て，ネットワークセグメントを分割して運用している。宮内庁CISの導入作業においても現行と同様の構成を踏襲するため，宮内庁CISはこの設定が可能であることを原則とする。 なお，移行の際に問題が発生した場合の切り戻し，又は順次移行などの移行設計を考慮した上で機器の選定を行うこと。	必須						
(7) 本業務により，宮内庁NWSを始め各現行システムに不具合や問題を与えた場合は乙の責任と負担において対処すること。本作業に起因して発生した作業を関係事業者へ依頼する場合は，甲と事前に協議を行い甲の承諾を得た上で，乙が作業費用を負担すること。ただし，作業実施予定日の10日（休日を除く。）前までに乙が作業内容（設定，手順等）について文書にて甲担当者へ具体的に説明した上で，通常の保守業務又は運用管理業務の範囲内の作業と認められる場合には，甲担当者を介し，甲担当者の指示として当該作業を関係事業者に通常業務として依頼することができる。	必須						
(8) 移行・切替の際に，宮内庁NWSに連携する各現行システム等に影響があると懸念される場合には，事前に甲担当者へ可能な限り速やかに報告し，対応策を協議すること。	必須						
(9) データ移行が必要な場合には，甲に極力作業を発生させない方法でデータ移行を実現すること。やむを得ず甲の作業が発生する場合は，甲担当者とあらかじめ協議し，その承諾を得ること。	必須						
(10) 移行対象データについては，宮内庁NWSが正常に動作し，監査やセキュリティインシデント対応を適切に行う上で必要となる全てのデータを移行対象とすること。移行対象データについては，対象データを甲に提示し，甲の承諾を得ること。ただし，甲が宮内庁CISへ移行しないよう指示するデータは除くこととする。 なお，共有ファイルサーバにおいては，現行の実態を調査した上で，重複していること，長期間利用されていないこと等が確認されたファイルが明らかになった場合，甲と協議し，移行の対応内容を決定すること。移行対象のデータは最低限以下を想定している。 (ア) ディレクトリサーバ等に格納されているユーザ情報 ※ ユーザ管理システム内で保存している関連情報についても必要に応じて実施すること。 (イ) 庁内ポータル内に格納されている各種コンテンツ (ウ) ファイルサーバ内に格納されている各種ファイル (エ) その他宮内庁NWSが正常に動作する上で必要となるデータ	必須						
(11) 移行・切替のために機器の追加が必要な場合は，乙の責任と負担において準備を行い，作業終了後に撤去すること。	必須						
9.3.移行準備作業							
(1) 移行・切替準備，移行・切替作業及び検証の手順等を示した移行・切替手順書を作成すること。同作業の手順には，各作業が正しく行われていることの確認（作業毎のチェック項目と作業の成否の判定基準等）を含めること。	必須						左記について，理解した上で対応できるか。
(2) 切替時に現行システム事業者，運用管理支援事業者，各関係事業者に対応を求める場合は，各事業者に実施を求める内容，対応予定日を記載した切替手順書を作成すること。各関係事業者作業依頼は原則として，1か月以上前に提示を行い，1週間以上前までに甲の合意を得ること。	必須						
(3) 移行・切替作業及び移行・切替後動作検証等の同作業に係る時間単位での詳細スケジュールを作成すること。	必須						
(4) 移行・切替作業において想定されるリスクを検討し，リスクが顕在化した場合に備え，具体的な切戻し方法等を含めた緊急時の対応計画表を作成することとし，甲担当者の承諾を得，移行・切替手順書に加えること。	必須						
(5) 切り戻し作業が迅速に行えるような移行手順を検討し，原則として切り戻しが不可能な移行手順や，切り戻し時に連携するシステムの各関係事業者に負荷を与えるような移行は実施しないこと。	必須						
9.4.移行作業							
(1) 移行・切替作業において，何らかのトラブルが発生した場合は，速やかに甲担当者へ連絡すること。	必須						

評価対象	必須	加点	加点評価				評価基準
			特に優秀	優秀	標準	加点なし	
(2) トラブルの内容により移行が困難と判断された場合は，甲及び関係事業者に承認を得て，速やかに切り戻し作業を行うこと。切り戻し完了後は正常にシステムが稼働していることを確実に確認すること。切り戻しによる各関係事業者への依頼作業については，甲と協議の上で，原則として乙が負担すること。	必須						左記について，理解した上で対応できるか。
(3) 移行・切替作業の結果について，移行・切替作業結果報告書を作成し，甲担当者に提出すること。	必須						
(4) 移行時には甲の責任者は連絡が取れる体制にしておくこと。また，作業場所には委託事業者だけでなく，甲担当者を配置すること。	必須						
(5) 移行・切替作業実施後は，問合せ等の対処が円滑に行えるよう体制を確保すること。	必須						
9.5.運用管理業務の引継ぎ							
9.5.1.本調達の落札決定後							
(1) 乙は，本調達の落札決定後，運用管理業務開始日から速やかに運用管理業務に着手できるよう，本調達仕様書「7.会議体の設置」で示した統括会議等を活用するなどし，乙の責任と負担において，落札決定後から契約履行開始日までに現行運用管理支援事業者，宮内庁統合NWの構築事業者，宮内庁CISの構築担当者などから確実に運用管理業務を引き継ぐこと。 なお，乙が引継ぎ作業を進める上で，現行運用管理支援事業者，宮内庁統合NWの構築事業者，宮内庁CISの構築担当者などへ運用管理業務の引継ぎに関する依頼を求める場合は，甲に対して具体的に依頼内容を事前説明すること。乙の依頼内容が通常の保守業務又は運用管理業務の範囲内の作業であると甲が認める場合には，甲担当者を介し，甲担当者の指示として各事業者に対して依頼することができる。	必須						左記について，理解した上で対応できるか。
9.5.2.本調達の契約期間終了の1か月前							
(1) 乙は，運用管理業務の契約期間終了の1か月前から，次々期運用管理事業者（2024年2月1日から業務開始を予定）に対する引継ぎを運用管理業務の作業範囲として行うこと。ただし，甲又は次々期運用管理事業者の事由により，引継ぎ業務が本調達の契約期間外に及ぶ場合には，本調達の範囲外とする。 (2) 乙は，次々期運用管理事業者への引継ぎ作業の開始予定日の営業日5日前までに，次のような資料の作成又は更新を行った上で甲担当者に提出して甲担当者の承諾を得ること。 ① 運用管理業務を行う中で把握した課題事項等，運用管理業務を遂行してきた中で得た知見をとりまとめた資料等 ② 運用管理業務の実態に即した最新の各手順書等 (3) 乙は，(2)で作成した資料等を用いて甲担当者及び次々期運用管理事業者に対し適切な説明を実施すること。また，甲担当者及び次々期運用管理事業者引き継ぎの内容に関する質問にも適宜対応すること (4) 当該引継ぎに必要な資料等の作成の経費は，乙の負担とする。	必須						左記について，理解した上で対応できるか。
10. 運用・保守管理要件							
乙は，本調達にて提供するサービス及び機器等について，次の運用・保守を行うこと。 なお，運用及び保守を提供する対象のサービス及び機器の一覧は別紙4を参照すること。	必須						左記について，理解した上で対応できるか。
10.1.基本方針							
(1) 運用管理・保守業務の統括者を配置し，全体の管理を行うこと。	必須						左記について，理解した上で対応できるか。
(2) 構成・変更管理，運用・監視，保守を行う体系化された体制を確立すること。	必須						
(3) 連絡体制を明確化し，甲担当者，関係者への連絡を円滑かつ迅速に行える仕組みとすること。	必須						
(4) ITIL，ISO20000 等の業界標準の運用・保守管理基準を参考に運用・保守業務項目を定義すること。	必須						
(5) 上記(1)～(4)について運用管理・保守説明書としてまとめ，甲担当者の指定する期限までに提出すること。	必須						
(6) 運用・保守業務の支援ツールを導入して作業を効率化すること。	必須						
(7) 甲担当者の負荷軽減に配慮すること。	必須						
(8) 運用・保守対応時間帯は，平日の9時00分から17時00分とし，休日を除く月曜日から金曜日（原則として当日対応）までとすること。	必須						
(9) 24時間×7日間／週の稼働を基本とすることとし，必要な保守による停止の際には，ユーザに不便を与えないよう配慮し，効率的に作業を行うこと。	必須						
10.2.基本方針							
(1) 甲担当者及び宮内庁統合NW受託者が，運用・保守及び障害等について問合せ可能で一元的な受付窓口（以下「運用・保守受付窓口」という。）を設置すること。	必須						左記について，理解した上で対応できるか。
(2) 運用・保守受付窓口は，E-mailやFAX等による24時間×7日間／週での受付が可能であること。	必須						
(3) 運用・保守対応時間帯は，平日の9時00分から17時00分とし，休日を除く月曜日から金曜日（原則として当日対応）までとする。ただし，甲担当者が対象製品の故障の重要度，緊急度が大きいと判断した場合はこの限りではない。また，ハードウェア障害に関する復旧対応，個別のサービス・製品に対する問合せ窓口については ，個別の窓口を用意し，24時間×7日間／週で対応を行うこと。	必須						
(4) 運用・保守対応時間内は，電話によるサポートを随時行うこと。	必須						
(5) 受け付けた問合せをインシデントとして管理し，インシデントのクローズまで， 対応を継続すること。	必須						
(6) 障害について対応したときは，障害報告書を作成し，甲に報告すること。	必須						
10.3.運用・保守要件							
(1) 各種の障害発生を想定し，甲担当者及びユーザへの報告・通知の手順，障害復旧の手順，体制，役割分担，連絡方法などの計画を策定すること。策定した計画は甲担当者の承諾を得ること。また， 運用においてPDCA サイクルを実施し，障害対応業務の実施内容を継続的に評価，改善することで長期にわたっての安定的，効率的かつ高品質なサービス提供を行うための計画の随時見直しを行うこと。	必須						左記について，理解した上で対応できるか。
(2) 障害発生時には，甲担当者，次期運用管理事業者（宮内庁CIS受託者），運用管理支援業者及び障害に関連する各現行システムの構築・業者と綿密な調整・連携を行い，保守作業を行うこと。また，各拠点に対応要員を派遣する必要がある場合はその手配と各拠点との調整を行うこと。	必須						
(3) 発生した障害を事案ごとに記録・管理し，状況が常に把握できる仕組みとすること。	必須						
(4) 甲担当者又は管理者からの問合せによる宮内庁CISの障害の有無を確認し，原因の切り分け，調査の支援を行うこと。	必須						
(5) 障害復旧のための対応策を検討すること。 なお，甲担当者への対応策の内容の説明及び実施に必要な調整を行うこと。	必須						
(6) 原則として障害発生の当日中に対応を開始し，早急に復旧させること。ただし，根本的な対策が取れない場合は暫定的な復旧策を検討・提案し，対策の実施においては甲担当者の承諾を事前に得ること。	必須						
(7) 障害が発生した場合は，障害個所の修理又は交換を行うこと。機器交換時には，機器が物理的に適正に機能することを動作確認し，この確認結果を甲担当者へ遅滞なく報告し，報告内容について甲担当者の承諾を得ること。	必須						
(8) 機器等の修理又は交換を行う場合，据え付け・調整作業を行うこと。これらの作業により設定内容が失われた場合は，甲担当者の指示により再設定を行うこと。	必須						
(9) 甲担当者が，障害復旧したことを確認できるまで対応を行うこと。	必須						
(10) 障害対応した際，対応後速やかに障害報告書を作成し，遅滞なく甲担当者に報告すること。	必須						
(11) 発生した障害に対して関連情報収集及び解析を行い，原因を究明し，再発防止策を検討すること。 再発防止策の検討結果を甲担当者へ遅滞なく報告し，報告内容について甲担当者の承諾を得ること。	必須						
(12) 報告書については次の報告内容とし，その他必要と考えられる項目についても報告する仕組みとすること。 ① 発生状況（発生日時，回復時間，故障時間，影響拠点，障害概要） ② 障害対応状況（故障原因，故障機器，対処内容，現在の状況） ③ 障害の原因とその対応策 ④ 再発防止策	必須						
(13) 地震，水害，停電等の災害発生による被害を想定し，甲担当者及びユーザへの報告・通知の手順， 障害復旧の手順，体制，役割分担，連絡方法などの計画を策定すること。策定した計画は甲担当者の承諾を得ること。また，運用において随時見直しを行うこと。	必須						
(14) 災害発生時には，上記（13）の計画に沿って迅速な復旧を行うこと。	必須						
10.4.運用・保守要件							
以下，保守業務として実施すべき保守の要件について記載を行う。 なお，宮内庁LANの一部の機器（詳細は，別紙4を参照）については，宮内庁統合NW受託者により暫定的に運用管理された後，乙に引き継がれることを想定している。運用を引き継いだ機器についても，ハードウェア交換等の一部の保守業務については，引き続き宮内庁統合NW受託者にて対応をする。	必須						左記について，理解した上で対応できるか。
10.4.1.基本要件							
(1) 乙は，次の要件を満たす保守体制を整備し，保守運用計画書を提出し，保守運用手順書に基づき，保守対応をすること。 なお，保守対応とは，問合せ受付窓口対応，システム保守対応，ハードウェア保守対応，ソフトウェア保守対応の総称を示すものとする。本調達機器及び各事業者の役割範囲については，別紙4を参照すること。	必須						左記について，理解した上で対応できるか。
(2) 保守期間は，契約期間が終了するまでとする。	必須						
(3) 乙は，甲及び宮内庁統合NW受託者の求めに応じて必要な障害対応，原因究明，設定変更等の対応を行うこと。	必須						
(4) 乙は，保守対応における責任体制を明確にするため，担当者名を明記した保守体制図を提出すること。 なお，体制を変更する必要が生じた場合には，変更内容を記載した文書をもって報告し，甲の承諾を得ること。	必須						
(5) 設計・構築の従事者を保守体制に原則含めること。ただし，保守体制に含めることが困難な場合は，設計・構築の従事者から十分に引継ぎを受け，内容を十分に理解した者を保守体制に含めること。	必須						

評価対象	必須	加点	加点評価 特に優秀	加点評価 優秀	加点評価 標準	加点評価 加点なし	評価基準
(6) 障害発生時には，甲担当者及び宮内庁統合NW受託者，障害に関連する現行他システム保守業者と綿密な調整・連携を行い，乙の責任と負担で保守作業を行うこと。	必須						
(7) 調達機器について，技術的サポートを行うこと。また，今後の運用中に調達機器と他の機器との接続及び別途調達したソフトウェアを甲担当職員又は宮内庁統合NW受託者がインストール・アンインストールするような場合，甲担当職員と密接に連絡が取れる体制を作り，連絡があった場合は支援すること。	必須						
(8) 保守対応は日本語で実施すること。	必須						
(9) 宮内庁CISに蓄積しているデータは，設定されたスケジュールに従いバックアップを行うことが可能なこと。	必須						
10.4.2.システム保守要件							
(1) 重大障害発生時や切り分け困難時等，各ハードウェア及びソフトウェア製造業者等では解決できない事象発生を想定し，乙において，ハードウェア・ソフトウェアで構成されるシステム全体の保守を実施すること。	必須						左記について，理解した上で対応できるか。
(2) 乙は，対応依頼を受け付けた障害を解消するため，適切かつ迅速な対応を行うこと。必要に応じて，各ハードウェア製造事業者等及び各ソフトウェア製造事業者等と協力し，ハードウェア保守対応，ソフトウェア保守対応を行うこと。	必須						
(3) システム保守対応の対応時間は，問合せ受付窓口対応の受付時間に準ずる。ただし，対象製品の故障の重要度，緊急度が大きいと判断した場合，甲から要請した場合はこの限りでない。 なお，対応時間外のシステム保守対応については，本調達に含まないものとする。	必須						
(4) 発生した障害に対して解析を行い，原因を究明し，再発防止策を検討すること。	必須						
(5) 甲及び宮内庁統合NW受託者並びに他システムの保守業者からの問合せや相談に応じること。	必須						
10.4.3.ハードウェア保守要件							
10.4.3.1 基本要件							
オンプレミス型での提供とする場合は，次の要件を満たすこと。	必須						
(1) 各ハードウェア障害時には，当該機器又はそれを構成する部品等の調達・交換・修理等を迅速に行う等，乙の負担により常時正常な稼動を保証すること。 なお，補助記憶装置の交換等によりソフトウェアの再インストールやシステムの環境設定，動作確認等が必要な場合，正常稼動するまでの作業も迅速に行うこと。	必須						
(2) 安定したサポートの実現及び保守サービスの品質維持のため，特に指定がない限り，本調達機器に関しては，製造事業者等が提供するハードウェア保守サービスを購入すること。 なお，各ハードウェアの保守サービスレベルについては，原則24時間×7日間／週 のオンサイト保守対応とすること。	必須						
(3) 調達機器に障害が発生した場合，(2)の保守サービスレベルの範囲で，ハードウェア障害と判断された時点から，原則4時間以内に技術者を派遣し，障害装置の修復，故障部品の修理にあたるものとする。 なお，賃貸借及び保守期間中は，必要な交換部品を必ず保持すること。	必須						
(4) 乙は，問合せ受付窓口対応及びシステム保守対応の受付時間外における障害に備えるため，各ハードウェア及びソフトウェア製造事業者等へ，甲担当者及び宮内庁統合NW受託者から直接問合せが可能な窓口を用意すること。	必須						
(5) ハードウェアの修理又は交換を行う際に，ラックからの取り外しや，据え付け・調整作業が必要な場合は，実施すること。また，必要に応じて，コンフィグの再投入等，設定作業を行うこと。	必須						
(6) 障害個所の修理又は交換後，機器が適正に機能するのかを宮内庁統合NW受託者と協力して動作確認すること。	必須						
(7) 保守期間中，ハードウェアに対する修正ファームウェアの適用要否に関する情報を提供すること。	必須						
(8) 調達機器のファームウェアのバージョンアップがあった場合は，乙は，ファームウェアのバージョンアップについて確認を行い，実機に反映し，検証を実施すること。	必須						
(9) 1年に1回以上，本調達に係る全ての機器の定期点検を行うこと。	必須						
(10) 本調達ハードウェアに搭載された補助記憶装置に障害が発生した際に，当該補助記憶装置を取り外し交換供給することとし，取り外した補助記憶装置については甲担当者が廃棄を行うのでこれを了承すること。	必須						
10.4.3.2 特記要件							
保守の基本的な種類については，1.3用語の定義を参照すること。 (1) サーバ（クラウドサービスプロバイダが提供するサービスとしてのサーバを除く。） ① 共通事項 納入から1年間は，無償保証交換とすること。 ② 特記事項 ア サーバ オンプレミス型での提案をし，本調達仕様書（案）内でサーバ構成を明記しているものは，次のとおり保守対応すること。 (ア)シングル構成又は二重化構成で，本庁と京都間での相互バックアップを取得していない場合 休日を除く月曜日から金曜日までの9:00から17:00までのオンサイト保守対応とし，ハードウェア障害と判断された時点から，原則4時間以内に技術者を派遣し，障害装置の修復，故障部品の修理にあたるものとする。 なお，契約期間中は，必要な交換部品を必ず保持すること。 (イ)二重化構成で，本庁と京都間での相互バックアップを取得している場合 原則としてスポット対応とする。ただし，応札者の提案においてオンサイト保守対応を阻害するものではない。 なお，スポット保守対応とする場合には，運用管理業務での情報システムインシデント対応を確実に行った上で，ステム保守事業者，製造事業者等保守契約の関係者に連絡を行う際に，スポット保守の見積依頼を同時に行い，甲へ見積書を提出すること。 イ スイッチ (ア)二重化構成（サーバセグメント用サーバ・ネットワークスイッチ，運用管理セグメント用サーバスイッチ） 後出しセンドバック保守とする。	必須						左記について，理解した上で対応できるか。
10.4.4.ソフトウェア保守							
(1) 乙は，ソフトウェア（OS 含む）及び関連ソフトウェアに関する問合せ，セキュリティ情報等の提供，障害発生時における解決支援に対応すること。 なお，導入したソフトウェア（OS 含む）について，導入後，甲が必要と認めた場合には，最新パッチ等の提供及び動作検証等の支援を行うこと。	必須						
(2) 納入したソフトウェアに対する修正パッチ・修正モジュール又はマイナーアップデートが製造事業者等から提供された場合，それらが提供された日から起算して原則2日（休日を除く。）以内に甲担当者へ報告し，適用要否の協議を実施すること。ただし，重大かつ緊急性を有する修正パッチ・修正モジュール又はマイナーアップデートについては，可能な限り遅滞なく甲担当職員へ報告し，適用要否の協議を実施した上で適用作業を実施すること。	必須						左記について，理解した上で対応できるか。
(3) 宮内庁LANの一部の機器については，宮内庁統合NW受託者による暫定運用管理期間が設けられている。当該期間中は，宮内庁統合NW受託者が修正パッチ・修正モジュール又はマイナーアップデートの適用作業を行うが，当該期間終了後は，乙にて作業を実施するものとする。	必須						
10.4.5.サービス保守要件							
本調達で乙がクラウドサービス等を提供する場合，乙の責任と負担においてファームウェア及びソフトウェアを可能な限り最新版にすることにより，ユーザの利便性，業務効率性及び情報セキュリティ対策を継続的に保つこと。 なお，各サービスそのもののSLAを順守するために必要となる保守を乙の責任と負担で適宜実施すること。	必須						左記について，理解した上で対応できるか。
10.4.6.運用・保守業務フロー							
甲，乙及び宮内庁統合NWを含むその他保守事業者の運用・保守業務フローは，別紙5のとおり。	必須						左記について，理解した上で対応できるか。
11. 仕様要件についての証明における記載要項							
11.1.概要							
応札者は，本記載要項に基づき，運用管理業務を履行する能力があることを，代表者の証明する適合証明書における仕様要件についての証明は，要件を満たしていることを具体的な記載資料（以下「提出資料」という。）を提出して証明すること。記載内容が要求要件を満たしているか否かの判定は，甲において，提出資料の書面により行う。	必須						左記について，理解した上で対応できるか。
11.2.記載に際しての基本要件							
(1) 提出資料は，単なる意思表示ではなく，運用管理業務の目的，内容を踏まえ，実施に当たっての詳細かつ具体的な実現方法を示していること。	必須						左記について，理解した上で対応できるか。
(2) 本調達仕様書（案）は，運用管理業務として求める最低限必要とされる要件を示したものである。従って，本調達仕様書の要件を全て満たした上で，本調達仕様書に記載されていない事項であっても，運用管理業務を実施するに当たり，必要と思われる事項については提出資料に記載すること。	必須						
(3) 提出資料において記載された内容は，運用管理業務範囲の対象として実施するものとする。	必須						
11.3.業務要件等に関する提案							
(1) 全体要件に関する資料 運用管理業務の目的・内容を踏まえ，実施に当たっての基本方針を具体的に記載すること。		必須					左記について，具体的な方針を記載しているか。
		加点	100	50	25	0	有効かつ妥当性のある基本方針を示した場合は加点とする。
(2) 請負業務内容に関する資料 本調達仕様書（案）に記載の各項目について，運用管理業務の円滑化・効率化を目的として創意工夫し，具体的な業務の実施方法等を記載すること。		必須					左記について，具体的な方法等を記載しているか。
		加点	100	50	25	0	運用管理業務の円滑化・効率化を実現するための具体的な実施方法等を示した場合は加点とする。

評価対象	必須	加点	加点評価 特に優秀	加点評価 優秀	加点評価 標準	加点評価 加点なし	評価基準
11.4.応札者条件に関する証明							
(1) 応札者に関する証明 「8.1. 応札者としての条件」に示す要件について具体的に記載し，証明書の写し等を添付すること。	必須						左記について，理解した上で対応できるか。
(2) 作業実施体制に関する証明 「5.4. 作業実施体制」に示す必要な要員を記載した体制図を提出すること。また，各要員に関して，本調達における各要員の役割，「8.3.2. 運用管理責任者（個人）の実績・資格」及び「8.3.3. 運用作業員（個人）の実績・資格」に示す要件について具体的（運用管理従事者の氏名，実務経験・実績，ITスキル標準（Ver3.0）の達成度指標，要素技術スキル等）に記載し，証明書の写し等を添付すること。	必須						
11.5.提出資料作成要領							
(1) 提出資料の印刷用紙は，原則としてA4判縦長横書きとする。ただし，図表等についてはA3判も可とする。添付する説明資料やパンフレット等がある場合にはこの限りではない。	必須						左記について，理解した上で対応できるか。
(2) 提出資料本文は日本語で記載し，分かりやすい構成を心掛け，目次及び通しのページ番号を付与すること。 なお，必要に応じて用語解説等を添付すること。	必須						
(3) 応札者の名称，所在地，代表者氏名等を記載すること。また，提出資料に対する照会先（連絡担当者名，所属，電話番号，FAX番号，E-mailアドレス）を記載すること。	必須						
(4) 提出資料は紙媒体で2部，甲の指示する電子媒体で2部ずつ提出すること。また，機能証明書，提案資料の電子ファイルを格納した甲の指示する電子媒体を1式提出すること。	必須						
(5) 提案に際して質問事項がある場合は，入札説明書（別添3）に記載のFAX番号又はE-mailアドレス宛てに提出すること。	必須						
11.6.留意事項							
(1) 提出に係る経費は，応札者の負担とする。	必須						左記について，理解した上で対応できるか。
(2) 提出資料について，照会や資料要求を行うことがあるので，その際は応じること。	必須						
(3) 仕様要件を満たしていないと甲が判断した場合には，応札できないものとする。また，一旦提出された提出資料の差し替えや再提出は，一切認めない。	必須						
12. その他特記事項							
12.1.検査・指示							
甲は，乙に対して質問，検査，資料等の提出に関する指示及び改善要求を行うことがある。これらを甲から求められた際には，乙はこれに速やかに応じること。	必須						左記について，理解した上で対応できるか。
12.2.新規資産にかかる運用要件							
運用管理業務時点では存在しない新規資産が導入された場合には，当該資産について運用管理業務の対象とするかどうか甲と協議すること。	必須						左記について，理解した上で対応できるか。
12.3.政府機関からの調査依頼支援							
政府機関からの宮内庁NWSに関する調査依頼又は対応指示事項が年々増加している。乙は運用管理業務対象の資料作成，提出等の支援を行うこと。	必須						左記について，理解した上で対応できるか。
		加点	40	20	10	0	具体的で有効かつ妥当性のある支援策を示されている場合は加点となる。
14. 契約条件等							
14.1.特定個人情報							
個人情報保護委員会の「「特定個人情報の適正な取扱いに関するガイドライン（事業者編）」及び「（別冊）金融業務における特定個人情報の適正な取扱いに関するガイドライン」に関するQ＆Aの更新（平成28年6月21日）」を参照すること。 乙は，例えば「個人番号を用いて情報システムの不具合を再現させ検証する」や「個人番号をキーワードとして情報を抽出する」ような作業は一切無く，ユーザのみが個人番号をその内容に含む電子データを取り扱い，個人番号を用いた業務を行う。	必須						左記について，理解した上で対応できるか。
14.2.秘密保持							
(1) 乙は，履行期間中はもとより履行期間終了後にあっても，本業務を履行するうえで知り得た甲に係る情報を第三者に開示又は漏えいしないこととし，そのために必要な措置を講ずること。	必須						左記について，理解した上で対応できるか。
(2) 甲が提供する資料は原則貸し出しとし，甲の指定する日までに返却すること。当該資料は複製してはならず，原則として第三者に提供し，又は閲覧させてはならない。	必須						
(3) 上記(1)の情報及び(2)の資料を第三者に開示することが必要となる場合は，事前に甲と協議のうえ，甲の承諾を得ること。	必須						
(4) 本調達で整備する宮内庁CIS以外で宮内庁NWSの運用にかかるID・パスワードは，現行運用管理支援事業者から引継ぎ，パスワードを変更すること。	必須						
(5) 乙は，本調達における全て業務の実施においては，情報セキュリティを確保するための体制を整備すること。	必須						
(6) 乙は，本調達における全ての業務の遂行においては，情報セキュリティの侵害が発生した，又は発生するおそれがある場合には，速やかに甲に報告すること。	必須						
14.3.瑕疵（かし）担保責任							
本調達機器等の不良，製造過程における設計・設定及びこれらに搭載されるソフトウェアに瑕疵のあることが発見された場合には，乙は甲の請求により新規取替えまたは補修を行い，その瑕疵によって生じた損害を賠償すること。	必須						左記について，理解した上で対応できるか。
14.4.賠償・復旧							
甲の既存の正常可能機器及びシステムが，本業務により不具合や問題が生じた場合は，迅速に復旧のための措置を乙の責任と負担において実施すること。	必須						左記について，理解した上で対応できるか。
14.5.第三者への請負，著作権等							
(1) 乙は，本業務の全部を一括して又は主たる部分を請負等により第三者に実施させてはならない。ただし，次の場合においてはこの限りではない。 (ア) 乙が，書面により請負等を受ける事業者の名称・住所・請負等の業務の範囲・請負等の必要性・請負等の金額等を事前に甲に申請し，その承諾を受けた場合。 なお，請負等の内容を変更しようとする場合も同様とする。 (イ) 乙が，コピー・ワープロ・印刷・製本・トレース・資料整理・計算処理・翻訳・参考書籍等の購入・消耗品購入・会場借上等の軽微な業務を請負等しようとする場合。	必須						
(2) 上記に基づき，第三者に業務を請負等する場合は，「14.2.秘密保持」に従いその者に対し，秘密の保持及び情報セキュリティの確保を同様に請負契約等において課すこと。	必須						
(3) 乙及び請負等を受けた第三者は，甲が定める情報セキュリティポリシー等を遵守し，「14.2.秘密保持」に基づき，その内容を秘密にする措置をとらなければならない。	必須						
(4) 乙が上記(1)に基づき第三者に請負等する場合において，請負等を受けた第三者が更にその業務の一部を請負等する等複数の段階で請負等が行われるときは，あらかじめ当該複数段階の請負等を受ける事業者の名称・住所・請負等の業務の範囲を記載した書面（履行体制に関する書面）を甲に提出しなければならない。当該書面の内容を変更しようとする場合も同様とする。	必須						
(5) 乙が上記(1)に基づき第三者に業務を請負等する場合において，これに伴う第三者の行為については，その責任を乙が負うものとする。 なお，再々請負等の場合も同様とする。	必須						
(6) 請負等事業の実施に当たり，甲の意図しない変更が行われないことを保証する管理が，一貫した品質保証体制の下でなされていること。また，当該品質保証体制が書類等で確認できること。	必須						
(7) 本調達機器に甲の意図しない変更が行われるなどの不正が見つかった時（不正が行われていると疑わしい場合も含む）に，追跡調査や立入検査等，甲と乙が連携して原因を調査，排除できる体制を整備していること。また，当該体制が書類等で確認できること。	必須						
(8) 当該管理体制を確認する際の参照情報として，資本関係・役員等の情報，請負等事業の実施場所，請負等事業従事者の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績及び国籍に関する情報提供を行うこと。	必須						

評価対象	必須	加点	加点評価 特に優秀	加点評価 優秀	加点評価 標準	加点評価 加点なし	評価基準
(9) 本業務の実施に当たっては，必要に応じて納入場所の環境について事前に確認を行うこととし，甲の業務に極力支障が生じないよう計画し実施すること。また，現行運用管理支援事業者，甲の他の現行宮内庁NWS賃貸借保守事業者等関係者との連携・協力を図りつつ宮内庁NWS及び関連する各既存システムの円滑かつ安定的な稼働に支障を来すことのないよう業務を実施すること。	必須						左記について，理解した上で対応できるか。
(10) 試験計画書に基づき，単体，結合，総合試験を実施する際に使用する試験用データは，乙において準備すること。 なお，関係事業者の協力が必要な場合は，甲及び関係事業者と協議し原則として乙の責任と負担において行うこと。	必須						
(11) 本業務の実施に必要となる工業所有権及び著作権等については，全て乙の責任において当該工業所有権及び著作権等の使用に必要な費用を負担し，使用承諾等に係る一切の手続きを行うこと。また，本業務の実施に伴い，甲のシステムのアプリケーションの著作権は，全て甲に帰属するものとし，著作者人格権について，乙はこれを行使しないものとする。	必須						
(12) 本調達仕様書（案）に基づく作業に関し，第三者との間に著作権に係る権利侵害の紛争等が生じた場合は，当該紛争の原因が専ら甲の責めに帰す場合を除き，乙の責任と負担において一切の処理をすること。	必須						
(13) 本業務の実施に伴い，本調達機器等の搬入・設置・修理・交換等物理的作業の実施に当たって甲の敷地内の作業場所を使用する場合は，事前に甲に申請しその承諾を得なければならない（ただし緊急に措置しなければならない場合を除く）。その場合，乙は作業場所を整理・整頓し，安全に留意して事故の防止に努めるとともに，労働基準法・労働安全衛生法を遵守して安全の徹底を図り作業すること。当該作業に伴い必要となった養生品・梱包箱等で当該作業の後不要となるものは，乙の負担で速やかに撤去すること。	必須						
(14) 上記作業による甲の諸設備の破損等は，甲の指示に従い，乙の責任と負担において修復等を実施すること。また，本業務の実施に伴う措置に起因して，正常な使用状態で甲の他の機器及びシステムに不具合や問題が発見された場合は，迅速に復旧のための措置を乙の責任と負担において実施すること。	必須						
(15) 本業務の実施に必要となる消耗品等は，乙の負担で用意するものとする。	必須						
(16) 乙は，本調達仕様書（案）に疑義が生じた場合，本調達仕様書（案）により難い事由が生じた場合及び本調達仕様書（案）に記載のない事項については，甲と速やかに協議し，その指示に従うこと。	必須						
(17) 本調達仕様書（案）に記載なき事項でも，本調達の構築・稼働・運用に必要と認められる事項は，甲と協議の上，実施すること。	必須						
(18) 乙は，甲との協議結果をその都度作成し，文書あるいはメールにて提出すること。	必須						
(19) 本運用管理業務の実施に必要となる用紙，記録媒体，バックアップテープ等については甲担当者が用意するが，その他の消耗品（筆記用具等）については，乙の負担で用意するものとする。	必須						
(20) 情報管理室には原則として乙の所有物（常駐者及び応援者個人の所有物を含む。）を持ち込まないこと。やむを得ず持ち込んだ場合には，事前に甲担当者と協議し，甲担当者の承諾を得た上で持ち込むこと。また，持ち込んだ物品については，ラベリング及びリスト化を行い，甲の所有物との判別がつくように管理すること。	必須						
小計			3380	1690	845	0	

女性の活躍推進に向けた公共調達に関する取組指針に基づく配点

「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9月4日法律第64号（以下「女性活躍推進法」という。））及び「女性の活躍推進に向けた公共調達及び補助金の活用に関する取組指針について」（平成28年3月22日全ての女性が輝く社会づくり本部決定（以下，「取組指針」という。））に基づき，ワーク・ライフ・バランスを推進する企業として法令に基づく認定を受けた企業その他これに準ずる企業（以下「ワーク・ライフ・バランス等推進企業」という。）の評価。 ※ それぞれの認定に該当する場合は，認定等を証する書類（当該認定等の根拠法令に基づき厚生労働省が定める各都道府県労働局長が発出した認定通知等）の写しを提出すること。			総合評価基準書3.(2)「表３：配点方針」記載のとおり ※ 最も高い配点は120点			各認定通知書等に基づく評価
総計							