人事院ネットワークシステムの
更改整備及び運用・保守業務一式
調達仕様書

別紙１　要件定義書

人事院事務総局総務課情報管理室

1. 目次

1. 業務要件の定義

次期システムについては、現行システムの利用者に対するサービスを継承することを前提としつつ、情報セキュリティの強化、行政事務の高度化及び効率化並びにワークライフバランス等の推進を目的として、新規サービスの導入等を行うこととしている。

1.1 利用者

利用者は、業務に応じて職員用シンクライアントまたは職員用ファットクライアントが割り当てられ、当該クライアントにより次期システムを利用する。

また、次期システムの仮想デスクトップにおいては、利用者の業務に応じて、２種類（簡易データベースを含むものと含まないもの）以上のマスタイメージを作成する想定である。

利用者のクライアントの区分と仮想デスクトップのマスタイメージの関係を「表 1 利用者の区分」に示す。

なお、次期システムでは、情報セキュリティの強化の観点から、外部記録媒体によるファイルの授受について本院及び地方支分部局等に設置する共用のファットクライアント（20台程度）でのみ行うことを想定している。

表 1　利用者の区分

クライアントの区分	仮想デスクトップのマスタイメージ		合計
	簡易データベースなし	簡易データベースあり	
職員用シンクライアント	537	160	697
職員用ファットクライアント	3	－	3
合計	540	160	700

（注１）本表は、簡易データベースの有無に着目して整理したもの。仮想デスクトップのマスタイメージ数を２に限定するものではない。

1.2 拠点単位のクライアント利用者数

現時点で想定する、拠点ごとのクライアント台数を「表 2　拠点ごとのクライアント台数」に示す。

表 2　拠点ごとのクライアント台数

拠点	職員用シンクライアント台数	職員用ファットクライアント台数	共用ファットクライアント台数
本院	477	3	8
北海道事務局	17	0	1
東北事務局	15	0	1
関東事務局	28	0	1
中部事務局	16	0	1
近畿事務局	24	0	1
中国事務局	17	0	1
四国事務局	15	0	1
九州事務局	20	0	1
沖縄事務所	9	0	1
公務員研修所	40	0	1
西ケ原研修合同庁舎	－	－	1
政府控室	4	－	1
計	682	3	20

（注１）運用業務用シンクライアント、運用業務用ファットクライアント及び予備は含まない。

（注２）次期システムでは、職員用シンクライアント、職員用ファットクライアント及び運用業務用シンクライアントにおいて仮想デスクトップを利用する。なお、西ケ原研修合同庁舎については、公務員研修所等の職員が、業務上の必要が生じた際に自身のクライアントを携帯の上、同庁舎に赴いて次期システムを利用する。

1.3 拠点所在地

次期システムの拠点所在地を、「表 3　拠点一覧」に示す。

表 3　拠点一覧

拠点名	所在地
本院	東京都千代田区霞が関１－２－３中央合同庁舎第５号館別館
北海道事務局	北海道札幌市中央区大通西12丁目札幌第３合同庁舎
東北事務局	宮城県仙台市青葉区本町３－２-23仙台第２合同庁舎
関東事務局	埼玉県さいたま市中央区新都心１－１さいたま新都心合同庁舎１号館

拠点名	所在地
中部事務局	愛知県名古屋市中区三の丸２−５−１名古屋合同庁舎第２号館
近畿事務局	大阪府大阪市福島区福島１−１−60大阪中之島合同庁舎
中国事務局	広島県広島市中区上八丁堀６−30広島合同庁舎２号館
四国事務局	香川県高松市サンポート３−33サンポート合同庁舎（南館）
九州事務局	福岡県福岡市博多区博多駅東２−11−１福岡合同庁舎
沖縄事務所	沖縄県那覇市樋川１−15−15那覇第1地方合同庁舎
公務員研修所	埼玉県入間市宮寺3131
西ケ原研修合同庁舎	東京都北区西ケ原２−２−１
政府控室	東京都千代田区永田町１−７−１参議院別館

1.4 サービス提供時間

計画停止を除く24時間365日とする。

なお、運用担当者の常駐時間は、開庁日の9:30～17:30とする。

1.5 情報システム化の範囲

現行システムにおける情報システム化の範囲を原則として踏襲するが、業務の高度化及び効率化の観点、セキュリティ強化を果たすための観点等から提案による見直しを行う。

なお、次期システムにおいて、新規に追加する機能は、「表 4　次期システムとして提供する機能」にて新規追加として示す機能である。

2. 機能要件の定義

2.1 機能概要

次期システムとして提供する機能を「表 4　次期システムとして提供する機能」に示す。各機能の要件を、「2.2　利用者提供機能」及び「2.3　システム運用機能」に示す。

表 4　次期システムとして提供する機能

No.	機能分類	機能	機能詳細記載箇所	新規追加（注１）
1	利用者提供機能	仮想デスクトップ	2.2.1	○
2		文書作成	2.2.2	−
3		表計算	2.2.3	−

No.	機能分類	機能	機能詳細 記載箇所	新規追加（注1）
4		プレゼンテーション	2.2.4	－
5		簡易データベース	2.2.5	－
6		PDF 形式ファイル作成・閲覧等	2.2.6	－
7		メールクライアント	2.2.7	－
8		リアルタイムコミュニケーション	2.2.8	○
9		電子メール送受信	2.2.9	－
10		ファイル共有	2.2.10	－
11		会議室等予約及びスケジュール管理	2.2.11	－
12		プリント	2.2.12	－
13		Web ブラウジング	2.2.13	－
14		統合ディレクトリ	2.2.14	－
15		内部 DNS	2.2.15	－
16		NTP	2.2.16	－
17		ファイル転送	2.2.17	○
18		外部接続	2.2.18	○
19	システム運用機能	仮想化基盤管理	2.3.1	－
20		監視	2.3.2	－
21		統合資産管理	2.3.3	－
22		アカウント等の管理	2.3.4	－
23		バックアップ管理	2.3.5	－
24		ライセンス管理	2.3.6	－
25		パッチ配信（WSUS）	2.3.7	－
26		ログ取得及び管理	2.3.8	○
27		DHCP	2.3.9	－

（注１）次期システムで新しく追加する機能については、「○」を付している。

2.2 利用者提供機能

2.2.1 仮想デスクトップ

（ア） 利用者がクライアントからネットワークを通じてサーバ上のデスクトップ環境を呼び出して操作できること。

（イ） サーバ上のデスクトップ環境では、「2.2.2　文書作成」から「2.2.17　ファイル転送」の機能が利用できること。
（ウ） 画面の転送データは、暗号化及び圧縮を自動的に行えること。
（エ） 画面転送の仕組みにおいて、回線の帯域、印刷データの大小等に応じて、画質、帯域制御、リフレッシュレート等で導入後も画面の調整ができること。
（オ） 院外からでも人事院が準備する外部接続用クライアントを使用して業務を遂行できるよう、仮想デスクトップへのアクセスを提供すること。なお、詳細は「2.2.18　外部接続」に記載する。
（カ） クライアントが有線または無線のどちらで次期システムにアクセスする場合も仮想デスクトップが利用できること。
（キ） 外部接続機能を用いて院外から仮想デスクトップにアクセスする場合には、院内からのアクセスよりもセキュリティを強化するため、多要素認証機能を導入すること。
（ク） 仮想デスクトップの基本ソフトウェアを即時に初期状態へ戻せること。
（ケ） 仮想デスクトップは、システム管理者が利用者及び仮想デスクトップ単位で強制的に再起動ができること。その際には他の利用者に影響を与えないこと。
（コ） 仮想デスクトップのマスタイメージを作成及び更新することで、各仮想デスクトップに反映できること。
（サ） 複数のマスタイメージを作成できること。
（シ） 利用者が新規に仮想デスクトップへの接続要求を行った段階で、空いている仮想デスクトップの自動的な割当てができること。
（ス） 仮想デスクトップを割り当てた利用者については、 マスタイメージが変更されても、同一の仮想デスクトップの割り当てができること。
（セ） カット、コピー及びペーストの操作について、システム管理者がローカル側及び仮想デスクトップ側の双方向で許可及び不許可の設定ができること。
（ソ） 利用者及び仮想デスクトップ単位でログイン状況の把握ができること。また、システム管理者がログイン中の利用者を強制的に切断できること。
（タ） シンクライアント、職員用ファットクライアント及び運用業務用ファットクライアントから接続できること。
（チ） 接続用のクライアントソフトウェアはデバイス数に関わらず使用できること。有償である場合は本環境で必要と考えられる数量のライセンスを提供すること。
（ツ） 仮想デスクトップを提供するサーバとクライアント間の通信が切断され

た際の挙動(シャットダウン、ログオフ、そのままログオン状態を維持等)を任意に設定できること。

(テ) サーバ仮想化及び仮想デスクトップに用いる仮想化ソフトウェアは、同一製品を用いて運用管理の負担を減らすこと。

(ト) 仮想デスクトップを利用するシンクライアント上には、保存したデータが残らないよう構成できること。ただし、ファットクライアントについては、別途協議とする。

(ナ) セキュリティパッチの適用及びアプリケーションのバージョンアップをサーバ上で一括して行うことができること。

(ニ) 仮想デスクトップに搭載する Windows OS は、Microsoft 社 Windows 10 Enterprise 正規版とすること。

2.2.2 文書作成

(ア) Microsoft 社 Word 2016 またはその後継バージョンのソフトウェアが 740 名で利用できること。

(イ) ジャストシステム社 一太郎 Pro 3 またはその後継バージョンのソフトウェアが 740 名で利用できること。ただし、当該ソフトウェアのライセンスは、バージョンアップ版を導入すること。

2.2.3 表計算

(ア) Microsoft 社 Excel 2016 またはその後継バージョンによる表計算ソフトウェアが 740 名で利用できること。

2.2.4 プレゼンテーション

(ア) Microsoft 社 PowerPoint 2016 またはその後継バージョンのプレゼンテーションソフトウェアが 740 名で利用できること。

2.2.5 簡易データベース

(ア) Microsoft 社 Access 2016 またはその後継バージョンの導入による簡易データベースソフトウェアが 160 名で利用できること。

2.2.6 PDF形式ファイル作成・閲覧等

(ア) PDF 形式ファイルを作成・閲覧等が可能なソフトウェアが利用できること。なお、本調達においては、人事院が別途調達する PDF 形式ファイル作成・閲覧等ソフトウェアのインストール及び設定作業を行うこと。

2.2.7 メールクライアント

（ア） Microsoft 社 Outlook 2016 またはその後継バージョンの導入によるメールクライアントソフトを利用できること。

2.2.8 リアルタイムコミュニケーション

（ア） テキストメッセージのリアルタイムな送受信ができること。

（イ） １対１及び複数人の利用者間でのテキストメッセージの交換ができること。

（ウ） 他の利用者のログイン状況が確認できること。

（エ） 他の利用者のログイン状況を確認した上で、クライアントからコミュニケーションを開始できること。

（オ） クライアントから１対１でのリアルタイムなファイル交換ができること。

（カ） メッセージは履歴として保存できること。利用者は、メッセージを送信した後でも、修正または取消しができること。

（キ） 利用者の利用停止ができること。

（ク） 最低文字数、有効期限、文字種、ログイン拒否までの試行回数等のパスワードポリシーが設定できること。

（ケ） 人事院ネットワークシステム内部でのみ利用できること。

（コ） 利用者が個別に、任意のグループ作成並びに利用者の追加、変更及び削除が管理できること。

（サ） システム管理者によるログの確認ができること。

（シ） 次期システム外とのコミュニケーション及び情報共有の機能を有する場合は、使用できないように設定できること。

2.2.9 電子メール送受信

（ア） 利用者に対し、メール送受信サービスの提供を行うこと。

（イ） Microsoft 社 Outlook 2016 またはその後継バージョンによるメール機能が利用できること。

（ウ） メールは少なくとも以下のファイル形式のファイルが添付できること。

- テキストファイル
- Microsoft 社 Office 文書（Word ファイル、Excel ファイル及び PowerPoint ファイル）
- ジャストシステム社 一太郎文書
- PDF 形式ファイル
- ZIP 圧縮ファイル

（エ） システム管理者による利用者個人のメール転送の制限または設定ができ

ること。

（オ） メール通信ログの取得ができること。

（カ） メールクライアントからの送信要求は SMTP（s)、受信要求は IMAP（s）に対応すること。

（キ） クライアントの不在時に自動応答の送信ができること。

（ク） メーリングリスト機能を有していること。

（ケ） １通当たりの受信容量制限について、設定ができること。

（コ） 利用者ごとにメールボックスの容量制限ができること。

（サ） 一人当たりのメールボックス容量は 4GB 以上とすること。

（シ） 利用者のメールボックスが閾値を超過した場合、利用者に対して警告メール等の通知ができること。

（ス） メールクライアントでのメール受信時に、ID 及びパスワードによる利用者認証を行うこと。

（セ） 統合ディレクトリとアカウント連携ができること。

（ソ） メールデータが移行できること。

（タ） 電子メール送受信機能は、メールボックスデータベースファイルの破損に備え、冗長化すること。

2.2.10 ファイル共有

(1) 基本要件

（ア） ファイル共有について、要求する容量を「表 5　ファイル共有に係る容量の内訳」に整理する。

表 5　ファイル共有に係る容量の内訳

		共有フォルダ	個人用フォルダ
概要		各部署で共有するフォルダ	利用者個人が占有するフォルダ
容量	個別	20TB 以上	8TB 以上 （利用者一人当たり約 10GB 以上）
	合計	28TB 以上	

（イ） 利用者によるフォルダの作成ができること。

（ウ） 利用する共有フォルダ及び個人用フォルダは、ネットワークドライブとしてアクセスできること。ネットワークドライブは、共有フォルダ及び個人用フォルダを仮想デスクトップへのログイン時に自動で割当てできること。

（エ） ファイルサーバ上に保管されたファイルについては、定期的にフルスキャンによるウイルスチェックができること。なお、フルスキャンによる業務への影響を可能な限り小さくする仕組みとすること。

(2) ファイル共有機能

（ア） 利用者がファイル共有を利用できること。

（イ） 仮想デスクトップの利用者がフォルダリダイレクト及び共有フォルダとして利用できること。

(3) アクセス権管理機能

（ア） フォルダ及びファイルへのアクセス権の設定ができること。

（イ） 利用者ごとにアクセス権を設定し、アクセス制御ができること。アクセス制御は、フォルダ及びファイル単位に作成、参照、更新及び削除を管理できること。

（ウ） 共有フォルダは、利用者及び利用者をまとめたグループ単位でアクセス権が設定できること。

（エ） 個人用フォルダは、利用者単位で作成され、少なくとも他の利用者によるアクセスを排除できること。

（オ） 利用者がフォルダ及びファイルへの閲覧及び編集権限を設定できること。

（カ） 階層化されたフォルダにおいて、上位フォルダに設定したアクセス権が下位フォルダに継承できること。

(4) 使用容量制限機能

（ア） 共有フォルダ及び個人用フォルダの容量制限値を設定できること。また、フォルダの容量に任意の閾値が設定でき、容量が閾値に達した際は、システム管理者へ通知できること。

(5) ファイル復旧機能

（ア） 利用者が誤ってデータを削除した場合に、利用者自身により、手順に沿って復元できること。

(6) 検索機能

（ア） 共有フォルダ及び個人用フォルダに保存されているファイルの検索ができること。

2.2.11 会議室等予約及びスケジュール管理

(1) 会議室等予約機能

（ア） 会議室及び備品の予約管理ができること。

（イ） 他の利用者に対し、会議の招集依頼が可能であり、依頼を受けた利用者のスケジュールに自動的に登録できること。

（ウ） 会議の招集依頼を受けた利用者は、参加、仮承諾、不参加等の応答を依頼

者に行えること。また、会議への出欠予定応答の状態が一覧で容易に確認できること。

（エ） 一度の予約で定期的に開催される会議の予約ができること。

（オ） 複数の利用者が同時に閲覧、予約、変更及び削除の操作ができること。ただし、同一の設備に対して重複予約ができないように設定できること。

（カ） 利用者が予約を行う際に、指定した設備の空き時間を検索できること。また、指定した時間帯に利用可能な設備を検索できること。

（キ） 各設備の予約状況が１日、１週間及び１ヶ月単位で表示できること。

（ク） 予約の画面から設備概要（例:「XX 会議室 定員 XX 人」等）が確認できること。

（ケ） 「2.2.9　電子メール送受信」等と連動し、設備を予約した際に関係者へ通知できること。

(2)　スケジュール管理機能

（ア） 利用者が各自のスケジュールの閲覧、登録、変更、削除及び共有が容易にできること。

（イ） スケジュールの登録時に「2.2.11(1)　会議室等予約機能」と連携し、会議室等の予約ができること。

（ウ） 「2.2.14　統合ディレクトリ」に基づいて設定した権限により、同一グループ内の利用者のスケジュールを一覧で表示できることに加え、一覧表示の対象アカウントを利用者で設定できること。

（エ） スケジュールの公開及び非公開の設定ができ、スケジュールを公開する利用者の範囲も設定及び管理できること。

（オ） スケジュールは、１日、１週間及び１ヶ月単位の表示ができること。

（カ） 毎週、毎月等の定期的なスケジュールの登録ができること。

（キ） 同じ組織またはグループに所属する複数の利用者のスケジュール及び空き時間を検索し、一覧で表示できること。

（ク） スケジュールの開始前にメール等で事前通知できるリマインダ機能を有していることが望ましい。

（ケ） メールクライアントツールから参照できること。

2.2.12 プリント

（ア） 院内の複合機及びプリンタから印刷できること。なお、本調達においては、人事院が別途調達する複合機及びプリンタが利用できるようにソフトウェアのインストール及び設定作業を行うこと。なお、複合機及びプリンタの仕様は、資料閲覧とする。

2.2.13 Webブラウジング

（ア） インターネットに接続して、Web サイトが閲覧できること。

（イ） Web サイトからファイルをダウンロードできること。

（ウ） URL フィルタリングにより、閲覧可能な Web サイトの制限ができること。なお、URL フィルタリングに係る要件は「3.6.4　Web セキュリティ」を参照すること。

2.2.14 統合ディレクトリ

(1)　利用者管理機能

（ア） 機器、組織、アカウント情報、アクセス権等の情報が一元管理できること。

（イ） 機器、組織、アカウント情報、アクセス権等の登録、変更及び削除を一元的にできること。

（ウ） パスワードについて、長さ、文字種、有効期限等を設定できること。

（エ） 利用者がパスワードを変更できること。

（オ） サーバの稼働状況及びアクセス状況のログが取得できること。

（カ） アカウントについて、有効期限等の制約事項に基づき制限を設定できること。

（キ） 利用者が過去に使用した所定回数分のパスワードを記憶し、それらの再使用を禁止できること。

（ク） パスワードの入力を所定の回数続けて失敗した場合、一時的にログイン不可状態にできること。

（ケ） アカウントに対して利用停止及び再開の設定ができること。

（コ） 利用者が仮想デスクトップを利用してログイン操作を行うことにより、ネットワーク上の機器にアクセスできること。

（サ） サーバに保存されているアカウントのパスワードを暗号化技術により暗号化し、システム管理者を含めて識別できない状態で保存できること。

（シ） 統合ディレクトリサーバでポリシー管理ができ、グループポリシー等によりログイン時に設定情報を配布できること。

（ス） ドメインコントローラの機能が提供できること。

2.2.15 内部DNS

（ア） IPv4 アドレス及び IPv6 アドレスのレコードを登録できること。

（イ） 外部からのゾーン転送の制限ができること。

（ウ） インターネットまたは政府共通ネットワーク宛ての名前解決を、それぞれ指定した DNS サーバに転送すること。

（エ） 内部のサーバに対する名前解決機能を有すること。なお、次期システムの

ドメイン名については現行システムから変更すること。

（オ） 次期システム内に設置している機器からの名前解決要求に対応すること。導入する内部 DNS については､実績及び信頼性のある機能を導入すること。

2.2.16 NTP

（ア） 本調達で導入する機器に対し、時刻の同期機能を提供できること。

（イ） NTP 機能は、指定した外部の NTP サーバと時刻同期ができること。

2.2.17 ファイル転送

（ア） Web ブラウザを介して、ファイルの送受信ができること。

（イ） 次期システム内及びインターネットからファイル転送が利用できること。

（ウ） 次期システム外の関係者がファイル転送を利用する際には、利用者が起点となること。

（エ） オンプレミスで構築する場合は、インターネット DMZ に構築すること。なお、外部サービスを利用する場合は、データの保存先は国内に限定すること。

（オ） 利用者の操作履歴及び接続元 IP アドレスを含むログ情報をシステムログサーバに対して、セキュリティ面を考慮した転送ができること。

（カ） 利用者 800 名を登録できること。

（キ） Internet Explorer 及び Firefox から利用できること。

（ク） 1GB 程度のファイルを転送できること。

（ケ） ファイル転送の履歴を記録及び保存できること。

（コ） 「2.2.14　統合ディレクトリ」と連携できること。

（サ） 利用者単位でアクセス権限の設定ができること。

（シ） 利用者単位にアップロードするファイルの容量を制限できること。

（ス） システム管理者がファイルの保存期間を一括設定できること。

（セ） ファイルのダウンロード及びアップロードの通信を暗号化できること。

（ソ） 利用者がダウンロード及びアップロード回数の制限並びに公開期間を設定できること。

（タ） ファイルのアップロード時に、ウイルスチェックが実行できること。

（チ） ファイルのアップロード時に、ダウンロード可能な期間及び回数を設定できること。また、システム管理者がそれぞれの初期値及び上限値を設定できること。

（ツ） 送信者がファイルをアップロードしたことを受信者に自動で通知されること。

（テ） 受信者がファイルをダウンロードしたことを送信者に自動で通知できる

こと。

（ト） Web ブラウザを介してファイルを送受信できること。

（ナ） ファイルの送信先には､受信に使用する URL をメールで通知ができること。この URL は、受信者以外に閲覧できない URL であること。また、ファイルのダウンロードの際は、パスワード認証できること。

（ニ） 複数のファイルをアップロードできること。また、複数の宛先に対して送信できること。

（ヌ） 外部ストレージ接続をサポートし、CIFS、iSCSI または NFS プロトコルをサポートできること。

（ネ） 連続してログオンに失敗した場合に、アカウントをロックできること。また、アカウントのロックを自動解除できること。

（ノ） アカウント管理画面を有し、手動操作によりアカウントの登録、変更及び削除ができること。

（ハ） アカウントの登録情報を CSV 形式でエクスポートできること。

（ヒ） CSV 形式によりアカウントのインポート（一括登録、変更及び削除）ができること。

（フ） 利用者単位で利用可能容量制限（クォータ）を設定できること。

（ヘ） アップロード可能なファイルの拡張子を設定できること。

（ホ） システムが発信するメール通知文書をシステム管理者が任意に設定できること。

（マ） ログオン画面及び操作画面の説明及び画像を変更できること。

（ミ） システムの利用状況及び統計情報を参照できること。

（ム） ファイル転送履歴を参照できること。また、履歴は画面表示及び CSV ファイルでの出力ができること。

（メ） ファイルの保存先は、国内に限定すること。

（モ） ファイルの保存に使用するストレージは、利用者全体で 100GB 以上とすること。

（ヤ） オンプレミスによる構築または外部サービスの利用どちらの提案も可能とするが、上記(ア)から(モ)の要件を満たすこと。

2.2.18 外部接続

（ア） 職員用シンクライアントを用いて院外から次期システムに接続の上、仮想デスクトップを利用することを予定しているため、本調達において、外部接続用機器の設計及び構築を行うこと。

（イ） 外部接続用クライアントは、職員用シンクライアントに限定する。なお、外部接続における同時接続数は、16 を想定している。

（ウ） 外部接続で利用するインターネット回線は別途調達する予定であり、本調達の対象外とする。
（エ） 院外から次期システムに接続するに当たり、多要素認証機能を導入すること。
（オ） 外部接続用クライアントと本院に設置した機器間の通信を暗号化する設備を導入すること。

2.3 システム運用機能

2.3.1 仮想化基盤管理

（ア） 仮想化基盤環境のシステム稼働状況（死活監視、イベント監視等）を監視する機能を実装できること。
（イ） 障害を検知した場合は、メール等で通知する設定ができること。
（ウ） 仮想化基盤サーバ上の仮想サーバとして構築できること。
（エ） 仮想化基盤サーバ、仮想サーバ、仮想デスクトップ及び仮想デスクトップ管理サーバを監視できること。
（オ） 仮想サーバの CPU、メモリ、ディスク等について、性能監視できること。
（カ） リソース情報（CPU、メモリ、ディスク使用率等）を取得できること。
（キ） パフォーマンス及びトラフィック情報を一定の間隔で表示できること。
（ク） アカウントに操作権限を付与する機能を有し、権限により表示内容及び操作の制限ができること。利用用途に応じた操作権限及び閲覧権限を利用者単位に設定できること。
（ケ） Web ブラウザから監視ができること。
（コ） 使用率、トラフィック情報、アラームまたはイベント及びインベントリ情報等のデータを出力できること。
（サ） 仮想デスクトップを運用するに当たり、以下の性能監視ができること。
- 仮想化基盤ホスト（CPU、メモリ、ディスク及びネットワーク）
- 仮想デスクトップ（CPU、メモリ、ディスク及びネットワーク）
- ストレージの使用量

2.3.2 監視

（ア） サーバ及びネットワーク機器並びにアプライアンス機器を含めたシステム稼働状況（死活監視、イベント監視等）を監視できること。
（イ） 障害を検知した場合は、メール等で通知する設定ができること。
（ウ） 仮想化基盤サーバ上の仮想サーバとして構築できること。
（エ） 監視ログを 90 日以上保管できること。
（オ） 監視対象機器に対し、ping による ICMP パケットでの死活監視を定期的に

実施できること。

（カ） SNMP による監視機能を有し、非 SNMP 装置については、WMI、Telnet 及び SSH による監視ができること。リソース情報（CPU、メモリ、ディスク使用率等をいう。以下同じ。）を取得でき、ディスク使用率ではパーティションごとの監視もできること。

（キ） Windows サービス及び TCP サービスポート並びにプロセスの CPU、メモリ等の可用性を監視できること。

（ク） メールサーバ、データベースサーバ、利用者管理サーバ等の SNMP 対応アプリケーションを監視できること。

（ケ） 仮想サーバのリソース情報の性能監視ができること。

（コ） パフォーマンス及びトラフィック情報をリアルタイムに表示できること。

（サ） サブネットごとに指定した IP アドレスの範囲及び CSV ファイル内の装置を一括して自動検出できること。また、装置を個別に登録できること。

（シ） 監視対象機器の監視項目をテンプレート化でき、同じタイプの装置を同じ監視設定で容易に登録できること。

（ス） アラームの承認、抑制及びエスカレーションを行うこと。また、アラームの内容を検索できること。

（セ） 障害検知時にメール、プログラム実行、音声等により障害を通知できること。

（ソ） 監視項目に閾値を設定でき、閾値を超えた場合にメール等で通知できること。また、障害通知メールのテンプレートが作成できること。

（タ） 監視対象から解除できること。

（チ） アカウントに操作権限を付与する機能を有し、権限により表示内容及び操作の制限ができること。

（ツ） Web ブラウザから監視ができること。

（テ） 可用性、応答時間、リソース情報、アラーム、イベント、インベントリ情報等のレポートを作成できること。

（ト） 作成したレポートを HTML 形式、CSV 形式または PDF 形式のいずれかのファイルへ出力できること。

（ナ） 本機能のサーバは冗長構成にはせず、仮想化基盤の HA 機能にて速やかに復旧できること。

（ニ） 監視対象機器のトラフィック及びインターフェース（エラー値、パケット数等）の情報を SNMP により監視できること。

（ヌ） 監視対象機器の MIB 情報が対応している場合は、リソース情報が取得できること。

（ネ） Windows 及び Linux サーバはプロセスごとにプロセス数、CPU 使用時間割

合及びメモリ使用量の監視ができること。

（ノ） メニュー操作によって標準MIB及び製造元の独自のプライベートMIB情報を容易に収集できること。

（ハ） 監視対象機器への ICMP 及び TCP サービスの応答状況並びにレスポンスタイムが監視できること。

（ヒ） 取得した性能情報をグラフとして表示できること。

（フ） SNMP及びレスポンスの監視間隔は、１分間隔の設定ができること。

（ヘ） 取得したリソース情報を、90日以上保管できること。

（ホ） 閾値を設定し、アラートとして検知できること。監視項目ごとに閾値の上限及び下限の設定ができること。

（マ） 監視対象機器におけるインターフェースのUp及びDownの状態を把握できること。また、状態が遷移した場合（UpからDown状態またはDownからUp状態）にアラートとして検知できること。

（ミ） WebGUIによる設定及びグラフ情報の確認ができること。また、操作画面は日本語で表示できること。

（ム） 装置テンプレートのインポート及びエクスポートができること。

（メ） 仮想デスクトップを運用するに当たり、以下の性能監視ができること。

- 仮想ホスト（CPU、メモリ及びディスク及びネットワーク）
- 仮想ゲスト（CPU、メモリ及びディスク及びネットワーク）
- ストレージの使用量及びIOPS

2.3.3 統合資産管理

(1) 資産管理

（ア） 統合資産管理の対象は、職員用ファットクライアント及び利用者に提供する仮想デスクトップとするが、その他対象とする機器等がある場合は、提案すること。

（イ） ハードウェア、ソフトウェア及びライセンス情報の収集を行い、資産管理できること。

（ウ） 対象をグループ化し、階層化（グループツリー）して登録できること。

（エ） クライアントは所属グループに登録できること。

（オ） 仮想化基盤サーバ上の仮想サーバとして構築できること。

（カ） 仮想化基盤サーバの障害発生時は、HA機能にて速やかに復旧できること。

（キ） 保守契約期間中において、電話、E-Mail及びFAXによる製造元へ直接の問合せ対応ができ、セキュリティ、不具合等の修正プログラムを提供できること。

（ク） 管理対象に関するコンピュータ名、CPU情報、メモリ容量、ストレージ容

量、ストレージ空き容量、IP アドレス、MAC アドレス等の各種ハードウェア情報を資産情報として自動的に収集できること。

（ケ） 管理対象のソフトウェアに関する OS、インストール状況（アプリケーションのバージョン、Microsoft 社 Office のインストール状況、Windows 更新プログラムの適用状況及びストレージ上に存在する実行ファイル一覧を含む）等についても、自動的に収集できること。

（コ） 収集したハードウェア及びソフトウェア情報を一覧で表示できること。

（サ） 資産情報の検索の際は、インベントリ情報、Windows OS のバージョン、サービスパック等から、同時に複数の項目またはキーワードを指定して検索できること。

（シ） 検索の際には、次期システムから削除された仮想デスクトップを含む管理対象のクライアントも、検索対象として指定できること。

（ス） 印刷を禁止できること。また、プリンタ単位及び利用者単位に制御設定できること。

(2) ソフトウェア配布

（ア） 管理対象に対して OS 更新プログラムを配布し、セキュリティパッチを適用する際は、パッチ適用サーバと連携し、更新日及び更新時間を設定して適用できること。

（イ） 管理対象に対して、ツール、スクリプト（汎用的な VBScript）等を用いたソフトウェア配布ができること。なお、配布対象は、製造元の Web サイトから保守費用の範囲内で個数に制限なくダウンロードできること。

（ウ） Adobe Reader、Flash、Java 等も容易に配布できること。

(3) 通信帯域制限

（ア） 管理対象と管理サーバ間の通信帯域の上限値をグループごとに設定できること。

(4) レポート機能

（ア） 収集されたログを集計及びグラフ化し、レポートデータを閲覧できること。

（イ） 管理対象の稼働時間をもとに作業時間を算出し、利用者単位及び部署単位に集計したレポートデータをグラフ化または一覧表で閲覧できること。

（ウ） グラフ及びレポートデータは、以下の内容を表示できること。

- 管理対象の稼働状況のレポートとして、クライアント稼働時間、時間帯別使用状況、未稼働のクライアント一覧及びクライアントごとのデバイス書込み状況
- アプリケーション、Web アクセス及びセキュリティのレポートとして、時間帯別 Web アクセス使用状況、注意表示（アラート）件数、アプリケーション使用状況及び Web アクセス状況

・ ファイルサーバアクセス及び印刷状況のレポートとして、時間帯別ファイルサーバアクセス数状況、クライアント別ファイルサーバアクセス状況、ファイル別アクセス数の比較及びクライアントごとの印刷枚数

（エ） ファイルサーバのファイル数、総ファイルサイズ、各フォルダの最終使用日時等の使用状況を収集できること。

（オ） すべて及び一部のファイルサーバの利用状況を表示できること。

（カ） 製造元の Web サイトからレポートを作成するためのプログラムをダウンロードし、作成したいレポートのスケジュール、集計期間、部署等を設定することで、必要なレポートを出力できること。

（キ） 集計結果は、Excel ファイル、CSV ファイル等としてダウンロードできること。

(5) 制限・制御及びアラート管理

（ア） 事前定義したルールに反した際に、通知する機能及び操作を禁止できること。

（イ） アラート発生時におけるクライアント操作画面を、マウスカーソルの位置が強調された形式で表示する等により、不正操作及び誤操作発生時に早期の問題把握ができること。

（ウ） 脆弱性の高いアプリケーションは指定したバージョンのみ起動許可する設定ができること。

（エ） 任意のアプリケーションの実行について、ハッシュ値及びバージョンリソースから実行ファイルを特定し、実行の検知及び禁止ができること。

（オ） 収集したログに基づいて、事前定義されたルールに反した際に、その操作ログはアラートログとして、ログ閲覧画面及び検索画面にて、アラート項目の優先順位に応じて色分けして表示できること。

（カ） アプリケーションの指定は、ファイル名を偽装したアプリケーションと正確に区別できるよう、ハッシュ値で指定できること。

（キ） 使用を禁止するアプリケーションは、ブラックリスト方式またはホワイトリスト方式のいずれかを選択して指定できること。

(6) 証跡管理

（ア） 証跡管理として、少なくとも以下の情報が記録できること。

・ 電源オン及び電源オフの日時
・ ログオン及びログオフの日時
・ 実行されたソフトウェアの起動及び起動期間
・ プリンタ出力ログ
・ ファイル操作（コピー、削除、リネーム等）
・ クリップボードにコピーされた内容

（イ） 印刷が実行された際に、その印刷されたドキュメント名、１回の印刷枚数及びファイルパスが記録できること。

（ウ） 起動元アプリケーションのファイルパス、ハッシュ値及びプロセス ID を記録できること。

（エ） ウイルス対策ソフトウェア等に対応するため、検知対象のイベントは任意に設定できること。

（オ） コマンドプロンプト(cmd.exe)及び Windows PowerShell(powershell.exe)で実行したコマンドを記録できること。

（カ） 収集されたファイル操作ログから、どのような操作（コピー、ファイル名変更、新規作成、削除等）が行われたかを抽出して表示できること。

（キ） 特定の操作ログから前後５分間の操作ログを検索して、抽出できること。

（ク） ストレージ上にバックアップとして保存されたログについては、閲覧する際にリストアすることなく、通常のログ検索と同様に管理コンソールから直接検索して閲覧できること。

（ケ） クライアントから収集したログデータをバックアップする際、ログデータを圧縮してバックアップする設定ができること。

（コ） 証跡管理機能送信メールログを取得できること。

（サ） クライアントログは、90 日以上保管できること。

(7) デバイス管理

（ア） 仮想デスクトップ、職員用ファットクライアント及び運用業務用ファットクライアントへの USB デバイスの接続について、不可とする設定をすること。

2.3.4 アカウント等の管理

（ア） 利用者のアクセス権を適切に管理するため、利用者が用いるアカウント（識別コード、主体認証情報）を管理（登録、停止、削除等）できること。

（イ） 情報システムの利用範囲を利用者の区分に応じて制限するため、情報へのアクセス権を制御できること。

（ウ） 特権を有するシステム管理者による不正を防止するため、管理者権限を制御できること。

2.3.5 バックアップ管理

(1) バックアップ対象

（ア） バックアップの対象は以下とすること。

- 仮想基盤ストレージ
- メールデータ

・ ファイル共有
・ ログデータ

（イ） ファイルサーバに含まれるデータファイル、仮想基盤ストレージに保存される仮想化サーバ及び仮想化デスクトップの復元に必要なデータをバックアップできること。

(2) バックアップ及びリストア方式

（ア） フルバックアップ、増分バックアップ及び差分バックアップができること。

（イ） バックアップ専用のソフトウェアを使用し、バックアップストレージ機器の重複排除機能と連携動作できること。

（ウ） 増分及び差分データを合成し、新たなフルバックアップを生成できること。

（エ） 稼働中のサーバ及びストレージ機器を無停止でバックアップできること。

（オ） 仮想化基盤ソフトウェアと連携して、仮想マシンのイメージバックアップの取得並びにイメージ増分及び差分バックアップができること。

（カ） 管理コンソール GUI が日本語表示に対応しており、GUI で作成したバックアップジョブをコマンドで実行できること。

（キ） 同一のバックアップソフトウェアで物理サーバ及び仮想サーバをバックアップできること。

（ク） バックアップデータとともにバックアップ情報を含むメタデータを別のバックアップサーバに複製し、緊急の際は複製先から即時にデータの復旧ができること。

（ケ） 仮想マシン個別単位でのバックアップ及びリストアができること。

（コ） メールサーバの専用エージェントを用意し、論理的に不整合のないバックアップができること。

（サ） 仮想マシンのイメージバックアップから、ファイル単位でのリストアができること。

（シ） スケールアップに備えて、バックアップ管理サーバ及びバックアップ実行サーバを分けて動作できること。

（ス） バックアップ管理サーバの OS が Windows 及び Linux に対応できること。

（セ） バックアップサーバ側での重複排除ができること。

（ソ） ストレージ機器のスナップショットの管理ができること。

（タ） 24 時間 365 日のサポートができること。

（チ） バックアップの実効状況及び結果の監視ができること。

（ツ） 仮想デスクトップの共有フォルダ内の利用者データ、仮想デスクトップテンプレート等をバックアップできること。

（テ） バックアップは、ハードディスクまたはSSDからハードディスクまたはSSD（「ディスク to ディスク」）の構成で実施できること。ただし、追加的な対

策（テープバックアップ等）を行うことが望ましい。

（ト） 業務に用いるデータのバックアップ処理は、業務への影響をできるだけ排除したタイミングで取得できること。

（ナ） バックアップの取得は自動化し、成否についてシステム管理者へ通知できること。なお、システム管理者により手動でバックアップが取得できること。

（ニ） 稼働中のサーバ及びストレージ機器を無停止でバックアップできること。

（ヌ） 「3.7.2(3)　バックアップ用ストレージ」にバックアップデータを格納すること。

（ネ） 対象サーバに含まれるアプリケーションのバックアップにおいて無停止でバックアップできること。

(3)　世代管理

（ア） バックアップ取得周期は毎日とし、３世代以上取得すること。

（イ） バックアップ取得中に障害が発生しても１世代前のバックアップ取得時の状態まで復旧できること。

（ウ） ファイルサーバについては、毎日スナップショットを取得し 7 日分を保持すること。

2.3.6 ライセンス管理

（ア） Microsoft 社製品のライセンス認証ができること。

（イ） 仮想化基盤サーバ上の仮想サーバとして構築できること。

（ウ） 一括でクライアントのライセンス認証ができること。

2.3.7 パッチ配信（WSUS）

（ア） 管理対象の OS 及び Office アプリケーションのパッチファイルの配信及び配信状況が管理できること。

（イ） 仮想化基盤サーバ上の仮想サーバとして構築できること。

（ウ） サーバ、仮想デスクトップ、職員用ファットクライアント及び運用業務用ファットクライアントにパッチファイルを配信できること。

（エ） 対象別にパッチファイルの配信状況及び適用状況を確認できること。

（オ） パッチファイルの適用は、スケジュール化できること。

（カ） 本機能のサーバは冗長構成にはせず、仮想化基盤サーバの HA 機能にて速やかに復旧できること。

（キ） Windows セキュリティパッチをシンクライアント及び職員用ファットクライアントへ配布できること。

2.3.8 ログ取得及び管理

（ア） 以下の項目のログ情報が取得できること。

- 事象を発生させた利用者または機器の識別情報
- 事象を発生した日付及び時刻情報
- 事象の結果（成功、失敗、エラー等）の情報

（イ） ファイルサーバの負荷低減のため、ファイルアクセスログは、エージェントレスで収集できること。

（ウ） サーバ負荷を軽減するため、原則として OS にはログ収集を行うソフトウェアであるクライアントツールを使用せずログの収集ができること。なお、クライアントツールを使用する場合は、非常駐型とすること。

（エ） 収集したログをリアルタイムに GUI で閲覧できること。また、システムへのアクセスを監査できること。

（オ） 収集したログは、キーワード等による検索条件の指定ができ、結果を一覧表示できること。

（カ） 検索条件を設定及び保存することができ、保存した検索条件を読み出し、検索できること。

（キ） 検索結果を CSV 形式で出力できること。

（ク） 収集したログを暗号化し保存できること。

（ケ） 収集したログは圧縮して保存できること。

（コ） 収集したログの改ざんを検知できること。

（サ） 製品の脆弱性に対する影響を公開していること。

（シ） ログからレポートを作成できること。

（ス） アクセスできるログをグループまたは利用者単位で制限できること。

（セ） ファイルサーバのアクセスログの取得を行い、90 日以上保管できること。

（ソ） メール通信ログの取得を行い、90 日以上保管できること。

（タ） ウイルス検知ログの取得を行い、90 日以上保管できること。

（チ） Web プロキシログの取得を行い、90 日以上保管できること。

（ツ） システムログの取得を行い、90 日以上保管できること。

2.3.9 DHCP

（ア） クライアント及び仮想デスクトップに対し、IP アドレスを自動で付与できること。

（イ） 主管課が許可していないクライアントに対し、IP アドレスを自動的に付与しないこと。

3. 非機能要件の定義

3.1 ユーザビリティ及びアクセシビリティに関する事項

3.1.1 次期システムの利用者数

（ア） 次期システムの利用者数は、「表 1　利用者の区分」を参照すること。

3.1.2 アクセシビリティ要件

（ア） 利用者提供機能は、日本語に対応すること。

（イ） システム管理機能は、原則として日本語に対応すること。日本語に対応しない場合は、利便性について日本語の場合と相違がないよう対応すること。

3.2 システム方式に関する事項

3.2.1 全体方針

（ア） 本調達で導入する機器は人事院が指定する場所に設置し、オンプレミス環境で提供すること。なお、ファイル転送については、外部サービスによる実現も可能とする。

（イ） 次期システムは、情報セキュリティ機能の高度化、ログ管理の厳格化及び実行形式の添付ファイルの無効化に加えて、新たにクライアントにデータを保持させない仕組みの導入等を行い、情報セキュリティインシデントの発生リスク及び情報漏えいリスクの軽減を図ること。

3.2.2 次期システムの全体構成

（ア） 次期システムの全体構成イメージは、調達仕様書「図 1　本調達における賃貸借保守の範囲」及び「図 2　本調達における設計・構築・運用の範囲」を参照すること。本調達仕様書の各要件を満たす最適な構成を提案すること。

3.3 規模に関する事項

3.3.1 設置場所

（ア） 次期システムの設置場所は、「表 3　拠点一覧」を参照すること。

3.4 性能に関する事項

（ア） 設計において、主管課と協議の上、性能に係る指標を決定すること。

（イ） 運用において、主管課と協議の上、実績値をもとに性能に係る指標の目標値を設定すること。

3.5 信頼性に関する事項

3.5.1 信頼性要件

（ア） 本調達で導入する機器は官公庁案件等で導入実績のある機器またはその後継機を選定すること。

（イ） フリーソフトウェア、シェアウェアソフト等の製造元によるサポートがされないソフトウェアでの実現は不可とする。

（ウ） クラスタリングまたは冗長化する機器を以下に示す。

- 仮想化基盤サーバ
- コアスイッチ及びサーバスイッチ
- インターネット回線用 FW
- 政府共通 NW 用 FW
- 振る舞い検知
- 負荷分散装置
- 管理セグメント用スイッチ

（エ） 仮想化基盤サーバは、物理サーバ１台に障害が発生した場合でも通常業務に影響なく、利用者に機能を提供できること。

（オ） 停電発生時において、自動的かつ安全にシャットダウンできること。

（カ） 各種保存データ、設定ファイル等は情報が正確に記録または保存できること。

（キ） 本調達で導入するハードウェア、ソフトウェア、ネットワーク等は、運用開始後４年間以上の保守及びサポートが提供されること。

（ク） 本調達で導入するハードウェア、ソフトウェア及びネットワークにおける機器等は、すべて新品（未使用機器）であること。

3.6 情報セキュリティに関する事項

3.6.1 不正プログラム対策機能（クライアント）

(1) 不正プログラム検知

(ア) ローカルディスク上に格納されているファイルに対し、リアルタイムで不正プログラムの検知及び処置ができること。

(イ) システム管理者が指定した時刻に自動及び任意で不正プログラムが検知できること。

(ウ)

(エ) 不正プログラムに感染したクライアントに対して、起動している不正プログラムのプロセスを停止または、不正プログラムのファイルを削除できること。検知された不正プログラム名、ファイルハッシュまたはファイルパスなど不正プログラムを特定するための情報を使用することで、プロセスの停止、レ

ジストリキーの削除及びファイルの削除ができること。

(オ)圧縮ファイル内で自動実行される可能性のある、不正プログラムに係るコードと疑われるコードを検知できること。

(カ)特定のファイル及びフォルダを不正プログラム検知の対象から除外する設定ができること。

(キ)ファイルタイプを正しく識別し、感染の危険があるとされるファイルだけを検索できること。

(ク)最新のセキュリティ情報を参照して、不正プログラムの検索ができること。

(ケ)シグネチャ方式に加えて、アノマリ方式により、不正プログラム実行前のファイル検知及び実行後の挙動の検知ができること。

(コ)メール及びSNMPトラップによる通知ができること。

(2) パターンファイルの更新

(ア)不正プログラムを検知するためのパターンファイル及び検索エンジンの更新ができること。

(イ)緊急の対応が必要となるパターンファイルの配信時は、不正プログラム対策の管理サーバから強制的に更新ができること。

(ウ)パターンファイル及び検索エンジンのロールバックができること。

(エ)パターンファイル、検索エンジン及びプログラム(修正モジュール等を含む)について、自動更新により最新のバージョンを保持できること。

3.6.2 不正プログラム対策機能（仮想化基盤）

(1) 不正プログラム検知

(ア)ローカルディスク上に格納されているファイルに対し、リアルタイムで不正プログラムの検知及び処置ができること。

(イ)システム管理者が指定した時刻に自動及び任意で不正プログラムが検知できること。

(ウ)圧縮ファイル内で自動実行される可能性のある、不正プログラムコードと疑われるコードを検知できること。

(エ)特定のファイル及びフォルダを不正検索の対象から除外する設定ができること。

(オ)ファイルタイプを正しく識別し、感染の危険があるとされるファイルだけを検索できること。

(2) パターンファイルの更新

(ア)不正プログラムを検知するためのパターンファイル及び検索エンジンの更

新ができること。

(イ)緊急の対応が必要となるパターンファイルの配信時は、不正プログラム対策の管理サーバから強制的に更新ができること。

(ウ)パターンファイル及び検索エンジンのロールバックができること。

(エ)パターンファイル、検索エンジン及びプログラム(修正モジュール等を含む)について、自動更新により最新のバージョンを保持できること。

3.6.3 メールセキュリティ対策

(1) 不正プログラム検知

(ア) 電子メールに対してリアルタイムの不正プログラム検索を実行し、不正プログラム検知時に駆除、削除等の処理を自動で実行できること。

(イ) パターンファイル及び検索エンジンを自動更新できること。

(ウ) 不正プログラム検知時に稼働監視機能に通知できること。

(エ) すべての不正プログラムに関するイベントを記録可能であり、ログの検索ができること。

(オ) 一定時間内の不正プログラム検知数がシステム管理者の設定した閾値を越えた場合に、特別な警告をシステム管理者に対して送信できること。

(カ) 拡張子を指定して、メールの添付ファイルをブロックできること。

(キ) 多重圧縮されたファイルの不正プログラム検索ができること。また、多重圧縮は 20 階層以上に対応できること。

(ク) 圧縮ファイルの形式は 20 種類以上、また、エンコード形式は５種類以上に対応できること。

(ケ) 利用者単位でスパムメールのポリシー（メールアドレスのブラックリスト及びホワイトリスト）を個別に作成及び登録できること。

(コ) 不正プログラム検知ソフトは、ネイティブ 64 ビットをサポートしていること。

(サ) システム管理用インターフェースとして GUI を利用できること。

(シ) 電子メールに対して不正プログラム検索を実行し、さらに添付ファイルについてはファイル種別を判断して検知できること。

(2) 添付ファイルチェック機能

(ア) 特定の文字列を含むファイル名及び特定の拡張子を持つファイルが添付された場合、当該メール及びファイルを削除できること。なお、処置については受信者に通知できること。

(イ) 添付ファイルチェックの対象となる特定の拡張子について、システム管理者が設定できること。

(ウ) 圧縮されたファイル内に禁止された特定拡張子を持つファイルがあった

場合も添付ファイルを削除して送信できること。

3.6.4 Webセキュリティ

(1) 基本要件

（ア） インターネットへのWebアクセスが中継できること。

（イ） HTTP1.1に対応したHTTP、HTTPS及びFTPリクエストが中継できること。

（ウ） Webベースの GUI または CLI で設定ができること。CLI では SSH をサポートできること。

（エ） HTML コンテンツ、画像データ等の Web コンテンツのキャッシュができること。

（オ） 統合ディレクトリと連携して認証できること。

（カ） アクセス元のクライアント等の IP アドレス、アクセス先の URL、アクセス結果（許可または拒否）、アクセスした日時等を記録できること。

（キ） 次期システム内部の Web アクセスは、除外設定できること。

（ク） IPv4 及び IPv6 のデュアルスタックに対応できること。

（ケ） イベントログをシステムログで転送できること。

（コ） キャッシュ機能を有し、Web アクセスに対し高速化できること。

（サ） Web 閲覧をする際に、クライアント及び Web アクセス先との通信間でプロキシ機能を提供し、URL によりアクセスを制限できること。

（シ） プロキシに接続する際は、統合ディレクトリと連携できること。

（ス） 次期システム内のクライアントより、Web ブラウザ等を使用してインターネット上の任意の公開サーバに透過的に接続し、その情報にアクセスできること。

(2) URLフィルタ機能

（ア） Web 閲覧をする際に URL によりブラックリスト及びホワイトリスト並びにキーワード及びフレーズ検出の両方でアクセスを制限できること。

（イ） スクリプトフィルタリング機能により、ActiveX、Java アプレット、Cookie 等、Web ページのプラグインをブロックできること。

（ウ） レピュテーション情報を用いて、不審サイトへのアクセスをブロックできること。

(3) 通信プロトコル対応

（ア） HTTP、HTTPS 及び FTP over HTTP プロトコルに対応し、任意のポート番号による通信に対応できること。

(4) カテゴリ制御機能

（ア） Web サイトのカテゴリごとに、許可、警告、ブロック等、アクセス時の挙動を設定できること。

（イ） ファイルのダウンロード及びアップロード並びに掲示板への書込みを禁止できること。
（ウ） フリーメール、ネットワークストレージサイト等の Web サイトの利用を禁止できること。代表的な Web サイトの情報については、製造元から最新版のデータが提供されること。

(5) 状況レポート作成機能

（ア） すべてのログは、キーワード、送信元アドレス、宛先アドレス及びアクセス日時で検索できること。
（イ） 使用状況等のレポートを作成できること。

(6) 統合管理コンソール機能

（ア） システム管理用インターフェースとして、Web ベースの GUI を提供できること。
（イ） Web 画面上で統計情報を閲覧できること。
（ウ） 管理用サーバ機能により、クライアントから管理コンソールにて設定変更、状況確認等ができること。

3.6.5 侵入検知及び防御機能

(1) 基本要件

（ア） インターネットからの不正アクセスと判断される通信を検知及び防御できること。
（イ） 検知結果及び詳細情報を確認できること。

(2) 侵入検知及び防御機能

（ア） IPv4 及び IPv6 によるアクセス制御、不正アクセスの検知及び防御ができること。
（イ） パケットの IP アドレス、プロトコル、ポート番号及びそれらの組合せ等で設定するルールに基づき、通信の許可及び拒否の制御ができること。
（ウ） Dos 攻撃を防御できること。
（エ） 不正侵入検知シグネチャをインターネット経由で自動及び手動で更新できること。
（オ） シグネチャ方式及びアノマリ方式で検知できること。
（カ） 不正アクセスの検知を SNMPTrap、電子メール等で通知できること。
（キ） システム管理用インターフェースとして、Web ベースの GUI を提供できること。
（ク） 予め設定されたイベントを検出した場合、通知できること。
（ケ） インバウンド及びアウトバウンドの通信について、リアルタイムに不正アクセスの検知及び防御ができること。

（コ） トラフィックのパターンを分析し、不正プログラムによる攻撃、DoS 及び DDoS 攻撃、アプリケーション及びサーバの脆弱性を狙う通信等を検知及び防御できること。

（サ） シグネチャ情報は、常に最新の状態に保つことができること。

（シ） FW との連携により、各セグメントにポリシーの設定及び管理ができること。

3.6.6 振る舞い検知機能

(1) 基本要件

（ア） インターネット経由の Web アクセスに係るファイルについて、複数の判定基準による閾値チェックを行い、不正プログラムへの感染の疑いがある通信かどうかを判定できること。

（イ） 不正プログラムの疑いがあるファイルかどうかを判定し、必要に応じて運用担当者に通知できること。

（ウ） Web アクセス時に利用者管理機能と連携して、利用者認証できること。

（エ） SSL 通信については、復号化した上で不正プログラム検査を実施できること。

（オ） 不正プログラム検知されたアクセス先への次回以降のアクセスを、一定期間ブロックできること。

(2) 検知及び防御機能

（ア） 振る舞い検知型技術をベースとした検知アルゴリズムを用いることにより、以下のように未知の不正プログラムを検知及び防御できること。

- 未知の不正プログラム感染を予防し、クライアントを防御できること。
- サンドボックス機能以外にフィルタリングができること。
- 不審なファイルに対する分析及びシグネチャの作成ができること。
- 分析及びシグネチャ作成時は外部にデータを送付せず、内部で処理することを選択できること。

（イ） クライアントへの不正プログラムの感染なく、不正なプログラムを検知できること。

(3) 隔離機能

（ア） 不正プログラム検知後、不正プログラムを隔離できること。

(4) 管理機能

（ア） 誤検知をレポートし修正できること。

（イ） リモートを含め、本ソフトウェアの管理操作は、日時、利用者アカウント、操作内容等の証跡が記録できること。

（ウ） 他のセキュリティアプライアンスからの解析依頼に対し、解析できること。

3.6.7 統合資産管理

（ア） ISO27001 及びプライバシーマークを取得している製造元の製品を選択できること。

（イ） BitLocker またはその他のサードパーティ製品により、ストレージを暗号化した際に生成される回復キーを収集し、管理できること。

（ウ） アプリケーションの実行、禁止アプリケーションの名前変更、インストールの実行、Windows システム構成変更、レジストリ変更、Windows ストアアプリの自動更新等を禁止できること。ネットワーク内のどのセグメントに接続されているか把握できること。

3.6.8 ログ取得、管理機能

（ア） 各システムから収集したログの暗号化ができること。

（イ） ログの不正な改ざん及び削除を防止するため、ログに対するアクセスを制御できること。

（ウ） 収集したログの改ざんを検知できること。

（エ） 他アプリケーションでも利用可能な形式で出力すること。

3.6.9 通信回線対策

（ア） 不正の防止及び発生時の影響範囲を限定するため、外部との通信を行うサーバ及びネットワーク機器のネットワークと、内部のサーバ、クライアント等のネットワークを通信回線上で分離できること。

（イ） 利用者のセグメントごとに内部のネットワークを通信回線上で分離できること。

（ウ） 通信回線を介した不正を防止するため、不正アクセス及び許可されていない通信プロトコルを遮断できること。

（エ） 接続先のサーバのなりすましを防止するため、サーバの正当性を確認できること。

（オ） クライアントのなりすましを防止するため、クライアントの MAC アドレス認証により DHCP の IP アドレスの払出しを制御できること。

（カ） ネットワーク内部の通信を暗号化できること。暗号化の際に使用する暗号アルゴリズムについては、「電子政府における調達のために参照すべき暗号のリスト（CRYPTREC 暗号リスト）（平成 25 年３月１日　総務省及び経済産業省策定）」を参照し決定すること。

3.6.10 脆弱性対策

（ア） 情報システムを構成するハードウェア及びソフトウェアの脆弱性を悪用

した不正を防止するため、構築時に判明している脆弱性については、修正の上、納入すること。

（イ） 運用開始後、新たに発見される脆弱性を悪用した不正を防止するため、情報システムを構成するハードウェア及びソフトウェアの更新を効率的に実施する機能及び方法を備えること。

3.6.11 機密性・完全性の確保

（ア） 情報システムに蓄積された情報の窃取及び漏えいを防止するため、情報へのアクセスを制限できること。

3.6.12 機器等の調達における対策

（ア） 機器等については、製造元保証品を採用すること。

3.6.13 その他

（ア） 次期システムに関する管理者権限は、必要に応じて主管課より貸与するものとする。また、管理者権限は、必要最小限の範囲での利用とし、作業終了後は、速やかに返却すること。

（イ） 次期システムにおける不正行為の検知、情報セキュリティインシデントの原因の特定等のため、次期システムの利用記録に関する証跡を蓄積し、一定期間保管すること。

（ウ） 障害、事故等の発生要因を減らすとともに、障害、事故等の発生時には迅速に対処するため、構築時の次期システムの構成（ハードウェア、ソフトウェア及びサービス構成に関する詳細情報）が記載された文書を提出するとともに文書どおりの構成とし、加えて次期システムに関する運用開始後の最新の構成情報及び稼働状況の管理ができること。

（エ） 主管課が用意するラックに機器を搭載し、ラックを施錠すること。

（オ） 内閣サイバーセキュリティセンター（NISC）からセキュリティ対応の指示、要請等があった場合、主管課と協議の上、必要な支援を行うこと。

3.7 情報システム稼働環境に関する事項

3.7.1 サーバ要件

(1) 仮想化基盤要件

（ア） サーバに実装されたファームウェアの監視及び正常性の確認ができること。

（イ） ファームウェアの正常性確認ロジックそのものを改ざんされないよう、そのロジックは独立したサーバ管理プロセッサーにROMとして組み込まれて

おり、不変であること。

（ウ） サーバ起動時にファームウェアの改ざんがないことを確認してから起動できること。

（エ） 特定のワークロードに対して調整された、BIOS 内にあらかじめ設定済みのサーバプロファイルを使用して、CPU、メモリ及び I/O 帯域を自動的に適切な設定に変更できること。

（オ） 16Gbps 以上の FC ポートを２個以上実装すること。

（カ） 電源及びファンを冗長化すること。

（キ） CPU は、Intel Xeon スケーラブルプロセッサーを搭載し、本サーバに実装する仮想マシンをすべて起動した状態で、安定稼働する処理性能を維持すること。

（ク） メモリは、本サーバ上で稼働させる仮想マシンをすべて起動した状態で安定稼働させる容量であること。なお、仮想マシンのメモリはオーバーコミットさせないこと。

（ケ） 内蔵するハードディスクドライブを使用する場合には、10krpm 以上の SAS ディスクまたは SSD とすること。

（コ） ディスクは単一以上のディスク障害を考慮し RAID1 または RAID5 以上により冗長化すること。

（サ） 仮想マシンのデータは共有ストレージに実装すること。

（シ） 仮想化基盤サーバのうち１台が故障しても、システム全体が縮退運転することなくサービスの提供を継続できること。

（ス） 本体とは独立した管理モジュールを持ち、リモート操作による電源のオン及びオフ並びにハードウェアヘルスステータスが取得できること。

（セ） 管理モジュールにより、遠隔地にある DVD 等のインストールディスクをローカルディスクとして認識させ、インストール作業が実施できること。

（ソ） ネットワークインターフェースは、仮想マシンの機能を実現するために使用する 10GBase 対応のポートを２個以上有し、冗長化すること。

（タ） 搭載する仮想サーバのリソースを提供できること。

（チ） 仮想サーバを搭載する複数の物理サーバを一元的に管理できること。

（ツ） 物理サーバに障害が発生しても、他の物理サーバに仮想サーバを割り振って自動復旧できること。

（テ） メモリ共有及びメモリ圧縮機能により、効率的にメモリが使用できること。

（ト） CPU の負荷をロードバランスし、効率的な CPU リソースを利用できること。

（ナ） FC-SAN、iSCSI 及び NFS によるストレージへのアクセスができること。

（ニ） 仮想サーバのコピーを GUI から作成できること。

（ヌ） 仮想サーバの差分データをバックアップサーバへ提供できること。

（ネ） 仮想サーバのバックアップ機能を外部ストレージにオフロードできること。
（ノ） 仮想サーバを統合管理できること。
（ハ） 以下の機能を実現すること。
- 「2.2.1　仮想デスクトップ」
- 「2.2.8　リアルタイムコミュニケーション」
- 「2.2.9　電子メール送受信」
- 「2.2.11　会議室等予約及びスケジュール管理」
- 「2.2.14　統合ディレクトリ」
- 「2.2.15　内部 DNS」
- 「2.2.16　NTP」
- 「2.3.1　仮想化基盤管理」
- 「2.3.2　監視」
- 「2.3.3　統合資産管理」
- 「2.3.4　アカウント等の管理」
- 「2.3.6　ライセンス管理」
- 「2.3.7　パッチ配信（WSUS）」
- 「2.3.8　ログ取得及び管理」
- 「2.3.9　DHCP」

3.7.2 ストレージ要件

(1)　仮想化基盤用ストレージ要件

（ア） サーバ及び仮想デスクトップの速度を確保するため、FC16Gbps で接続するフラッシュ（SSD またはフラッシュモジュール）のみを搭載したオールフラッシュストレージを導入すること。
（イ） コントローラは冗長構成で、片側のコントローラで障害が発生しても性能影響のないアクティブ-スタンバイ構成で導入できること。
（ウ） コントローラ障害時にも書込み性能に影響がないように、書込みキャッシュは、コントローラ外に独立し、二重化以上の可用性で導入すること。
（エ） 仮想化基盤用ストレージが停止した場合、利用者に多大な影響を及ぼすことから、コントローラ、キャッシュモジュール、フラッシュディスク及び電源がそれぞれ個別にコンポーネントモジュール化し、無停止及び個々の性能影響なく交換できること。
（オ） サービス継続を重視するため、同一シェルフ内で SSD の４本同時障害に対してもサービス停止が発生しないこと。
（カ） 長期保守の観点から、同一シェルフ内で、異なる容量及び異なるタイプ

（MLC 及び 3D TLC）の SSD 並びに NVMe 対応のフラッシュモジュールが混在できること。

（キ） ストレージ管理に当たり、GUI ベースの管理ツールを提供すること。また、各種情報（容量、IOPS、遅延及びスループット）がリアルタイムで可視化できること。

（ク） ストレージシステムの停止は、シャットダウンコマンドを不要とし、システムの停止方法は電源ケーブルを抜くことで対応できること。

（ケ） 将来的に DR サイトを構築する場合、追加で費用負担することなく非同期及び同期の機器外レプリケーション機能を提供できること（レプリケーション相手のストレージ及びレプリケーションライセンスは含まないものとする）。

（コ） 機器のスペース節約のため、インラインでの重複排除ができること。効果的なデータ削減を実現するため、512byte から 32KB までの可変長で実装できること。

（サ） 重複排除、圧縮及び暗号化機能は常時有効にできること。

（シ） 1Lun のサイズは、最大 4PB まで作成できること。

（ス） ストレージ機器は、汎用 OS ではなく、専用の OS を搭載できること。

(2) ファイル共有ストレージ

（ア） SMB プロトコル及び NFS プロトコルでアクセス可能なストレージとし、Windows OS からネットワークドライブとして利用可能及び Linux OS からもデータドライブとしてマウントできること。

（イ） Linux、Windows 等の各クライアントから同時にファイルを共有できること。

（ウ） 統合ディレクトサーバと連携し、利用者認証機能をサポートできること。

（エ） ディスク割当て設定により、ディスク使用量の制限ができること。

（オ） スナップショット機能により、利用者が自ら前日の内容にファイルを戻すことができること。なお、スナップショット領域は全体実効容量の 10%程度を最低限確保できること。

（カ） ストレージのシステム領域及びスナップショット領域を除いた、ファイル共有分の実効保存容量として 28TB 以上を用意すること。

（キ） アクティブ・アクティブ及びデュアルコントローラの HA 構成とし、片方のコントローラが障害で停止したとしても、ファイルサーバとしてのサービス提供が継続できること。

（ク） コントローラごとに 10Gbps の Ethernet ポートを２つ以上使用でき、ポート障害に対する可用性を確保すること。

（ケ） ストレージ専用 OS を搭載すること。

（コ） SMB1/2.x/3.x、NFS V3/V4、FC 及び iSCSI を実装可能なユニファイドスト

レージであること。

（サ） 不正プログラム等の対策のため、SMB プロトコルは、ドメインコントローラとの通信及びクライアントとの通信それぞれ個別に利用可能なプロトコルを指定できること。

（シ） データの削除等により、ボリューム内のデータ使用率が減少または増大した際に、業務を中断することなく必要に応じてボリュームを拡大または縮小でき、空いた領域を別用途に利用できること。

（ス） 運用管理及びアプリケーションとの整合性を考慮し、ファイルアクセスプロトコル及びブロックアクセスプロトコルの差異に関わらず単一のファイルシステムを用いて管理できること。

（セ） スナップショット領域を容量単価が低いオブジェクトストレージ等にオフロードできること。

（ソ） 必要に応じてボリューム容量を動的に増減できること。

（タ） データ領域の効率的利用を目的とし、ファイル共有領域に対し、ブロックレベルの重複排除機能及び圧縮を実装できること。

（チ） ファイルへのアクセスを高速化する手段として、SSD を搭載すること。ストレージへの読み書き要求をキャッシュできること。

（ツ） パフォーマンスへの影響を最小限に抑えつつ、同一 RAID グループ内で二重ディスクの障害からデータを保護できること。

（テ） 10GbE SR ポートを 12 ポート以上有すること。なお、うち８つは FC ポートとしても利用できること。

（ト） メモリを 256GB 以上搭載すること。

（ナ） NVRAM（不揮発性 RAM）を 16GB 以上有すること。また、電源その他障害時に書込みデータを保護できること。

（ニ） キャッシュとして利用できる NVMe フラッシュを 2TB 以上搭載すること。

（ヌ） 日本語での Web ブラウザベースの GUI 管理画面を提供すること。

(3) バックアップ用ストレージ

（ア） 「2.3.5 バックアップ管理」の機能を実現すること。

（イ） ファイルサーバに含まれるデータファイル、仮想基盤ストレージに保存される仮想サーバ及び仮想デスクトップのマスタイメージをバックアップするための保存領域を搭載すること。

（ウ） ディスク障害を考慮し、システム領域は RAID1、データ保存領域は RAID5 以上でデータ保護されていること。

（エ） 機器のスペース節約のため、重複排除機能を有し、ディスクの本数を削減すること。

（オ） FC 接続できること。

（カ） 10GbE ポートが標準搭載されていること。
（キ） I/O モジュールは用途に合わせて導入時にカスタマイズできること。
（ク） Web ベースの管理画面により、ハードウェアの監視及びログの収集ができること。
（ケ） 将来的にテープバックアップが必要になった場合に備えて、Ethernet を介さずにテープ装置を接続し、バックアップデータをテープアウトできること。また、そのバックアップデータから直接リストアできること。
（コ） バックアップデータの独立性確保のため、バックアップ用ストレージは、ファイルサーバ及び仮想基盤ストレージとは別の機器で用意できること。
（サ） Web コンソールより、ハードウェアの監視及びログ収集ができること。
（シ） ホットスペアが含まれていること。さらにディスク交換時には自動的にデータコピーが実行され、ディスクへの再配置ができること。

(4) FCスイッチ

（ア） FC スイッチを用いて、仮想基盤ストレージ及びバックアップストレージを、仮想基盤サーバ等と接続すること。
（イ） FC スイッチは機器を冗長化し、FC スイッチに障害が発生した場合は、動的にトラフィックを再ルーティングできること。
（ウ） 16GbpsFC ポートを 48 ポートまで拡張でき、必要に応じてポート数のアクティベーションを分割できること。
（エ） ポートごとに 16Gbps の帯域性能を持ち、2/4/8/16Gbps の帯域を自動検知して接続できること。
（オ） 仮想化基盤全体の動作に係る重要な機能のため、FC でトラフィックを転送中でも、転送を止めることなくソフトウェアのアップグレード（入替え）ができること。
（カ） 可用性確保の観点から Ethernet スイッチとは別の機器で実装すること。
（キ） SNMP v3 による管理ができること。
（ク） バックアップトラフィックによって VDI トラフィックが影響を受けないよう、QoS によりアプリケーションデータトラフィックの優先順位付けができること。
（ケ） マルチパス機能によって、等価コストパス間でのロードバランシングができること。

3.7.3 ネットワーク機器要件

(1) コアスイッチ・サーバスイッチ

（ア） 機器を冗長化の上、インターネット用 FW、政府共通用 FW、拠点向けルータ、フロアスイッチ及び仮想化基盤サーバを接続すること。

（イ） 電源を冗長化すること。
（ウ） 1GBASE-T 及び 10GBASE-T 対応のポートを 48 ポート以上実装できること。
（エ） 40G 対応の QSFP+ポートを６ポート以上実装できること。
（オ） 1.4Tbps のスイッチング容量をサポートできること。
（カ） 転送レート１Bpps のスイッチング能力をサポートできること。
（キ） レイヤ２及びレイヤ３の全ポートにおいて、ラインレートのトラフィックスループットのパフォーマンスを維持できること。
（ク） AC 及び DC 電源をサポートすること。
（ケ） Gateway 冗長プロトコルとして、HSRP 及び VRRP 機能をサポートできること。
（コ） IEEE802.1Q VLAN Tagging 機能を導入できること。
（サ） IEEE802.1D、802.1w 及び 802.1s 標準スパニングツリー機能をサポートできること。
（シ） IPv4 Dynamic Routing Protocol は、RIPv2、OSPF 及び BGP をサポートできること。
（ス） 複数のスイッチにまたがるリンクアグリゲーションに対応できること。
（セ） スパニングツリープロトコルを必要とすることなく、レイヤ２マルチパス化を実現できること。

(2) フロアスイッチ

（ア） 本院の各フロア（１階から８階まで）にフロアスイッチを配置すること。
（イ） コアスイッチ及びサーバスイッチからエッジスイッチに至るまでの経路を冗長化すること。
（ウ） 10BASE-T、100BASE-TX 及び 1000BASE-T 準拠の Ethernet ポートを 48 ポート以上実装できること。
（エ） IEEE802.1x、Web 及び MAC 認証利用者に対し、利用者単位で異なるアクセスリストを動的に割り当てることができること。
（オ） 日時及び時間帯を指定できるアクセスリスト機能を搭載できること。
（カ） 同一 VLAN 内でブロードキャストドメインを分割し、共通のセグメント内のホスト間トラフィックを制限できること。
（キ） SSH によってスイッチにログインし、各種ポート設定及びステータスを確認できること。
（ク） レイヤ２のアクティブリンク及びバックアップリンクのペアを作成し、100msec 未満のコンバージェンス時間で冗長化経路をサポートできること。
（ケ） ポートにてリンクフラップ等の障害を検知した際、ポートを一時的に使用できない状態にし、さらに一定時間経過後、自動的に再度利用できる状態にすること。

(3) エッジスイッチ

（ア） フロアスイッチに接続し、本院の利用者が利用するクライアント等を収容するスイッチとして、本院の各フロアにエッジスイッチ 88 台を配置すること。

（イ） 機器故障を考慮し、予備機を１台用意すること。

（ウ） 1U サイズであること。

（エ） 10BASE-T、100BASE-TX 及び 1000BASE-T 準拠の Ethernet ポートを 24 ポート以上実装できること。

（オ） クライアント接続用ポートで BPDU パケットを受信した場合、自動的にポートをシャットダウンできること。

（カ） エラーにより無効化されたポートを自動的に再試行できること。

（キ） QoS 機能によりパケットの重み付けと、優先転送制御ができること。

（ク） 802.1p サービスクラスでのパケット単位マーキング及び再分類ができること。

（ケ） SSH によってリモート接続し、ポートの設定変更及びステータスの取得ができること。

（コ） SNMPv3 に対応したステータスの取得ができること。

（サ） IEEE 802.3ad に対応し、複数のリンクを束ねて使用できること。

(4) インターネット回線用スイッチ

（ア） インターネット回線の ONU と、インターネット用 FW 間に設置し、インターネット用 FW を冗長化すること。

（イ） 10BASE-T、100BASE-TX 及び 1000BASE-T 準拠の Ethernet ポートを８ポート以上実装できること。

（ウ） IEEE 802.3ad に対応しており、複数のリンクを束ねて利用できること。

（エ） クライアント接続用ポートで BPDU パケットを受信した場合、自動的にポートをシャットダウンできること。

（オ） 機器故障を考慮し、予備機を１台用意すること。

(5) インターネット回線用FW

（ア） 本院とインターネットの境界に FW を設置すること。

（イ） 機器は冗長化し、１台に障害が発生しても通信できること。

（ウ） Ethernet インターフェースとして 1Gbps のツイストペアケーブルのポートを８つ以上有し、かつ 1Gbps の光ケーブルのポートを８つ以上接続できること。

（エ） サーバセグメントの通信制御にも使えるように、10Gbps の Ethernet ポートを２つ以上接続できること。

（オ） すべての Ethernet ポートを使用した場合でも、ワイヤーレートでの通信

を実現するため、IPv4 における FW スループットが 24Gbps 以上であること。

（カ） FW レイテンシが３μ秒以内（UDP 64 バイトパケット時）であること。

（キ） １台の機器上に仮想的な FW 装置を複数台動作させることができること。

（ク） 侵入防止（IPS 機能）、Web の URL フィルタリング、アンチウイルス、サンドボックスによる脅威からの保護、アプリケーション等、柔軟性のあるセキュリティ対策ができること。

（ケ） ポート及びプロトコルのみならず、アプリケーションの種別を認識してフィルタリングの設定ができること。

(6) 政府共通NW用FW

（ア） サーバスイッチと政府共通 NW 用 L2 スイッチ（本調達対象外）の間に FW を設置すること。

（イ） 「3.7.3(5)インターネット回線用」と同等の機能であること。

(7) 振る舞い検知

（ア） 機器は冗長化し、１台に障害が発生しても通信できること。

（イ） Ethernet インターフェースとして 1Gbps のツイストペアケーブルのポートを６つ以上有し、かつ 1Gbps の光ケーブルのポートを２つ以上接続できること。

（ウ） VM サンドボックスによる１時間当たりの処理ファイル数が 160 以上であること。

（エ） AV スキャンによる１時間当たりの処理ファイル数が 6,000 以上であること。

（オ） エミュレーション環境は８以上実装できること（VM 数）。

（カ） 電源は冗長化できること。

（キ） 「3.7.3(5)　インターネット回線用」及び「3.7.3(6)　政府共通 NW 用」と同一の製造元による製品であること。

(8) 負荷分散装置

（ア） 負荷分散装置は、主に仮想サーバ群の冗長化のために使用できること。

（イ） レイヤ４及びレイヤ７の負荷分散ができること。

（ウ） 負荷分散機能として、以下のロードバランシング方式を備えることができること。

- Round Robin（均等）
- Ratio （比率）
- Least Connections（最小接続）
- Fastest （最速）
- Least Sessions（最小セッション）

- Weighted Least Connection（重み付け最小接続）
- Observed（監視）
- Predictive（予測）
- Dynamic Ratio（動的比率）

（エ） ヘルスチェック機能として、以下のモニタリング方法をサポートできること。

- ICMP
- TCP
- UDP
- Diameter
- RADIUS
- HTTP
- HTTPS
- FTP
- IMAP
- LDAP
- MSSQL
- MySQL
- NNTP
- Oracle
- POP3
- PostgreSQL
- Real Server
- SASP
- RPC
- SIP
- SMB
- SOAP
- WAP
- WMI
- Firepass
- DNS

（オ） HTTP ヘッダの変更、挿入及び削除ができること。

（カ） レイヤ７のデータペイロードの情報をもとにして、トラフィック制御ができること。

（キ） VLAN ごとにルーティングテーブル及び管理ドメインを分割できること。

（ク） 分散対象サーバの IP アドレスに重複があった場合でも、サーバの IP アドレスを変更することなく、負荷分散処理ができること。
（ケ） バックアップファイルからリストア時に、SSL サーバ証明書も復元できること。
（コ） スクリプトベースの柔軟なルール分散を定義できること。
（サ） Web ブラウザより HTTPS で GUI 管理及び設定ができること。
（シ） 負荷分散機能のほかに SSL-VPN 機能を統合でき、１台の機器内で両機能を利用できること。
（ス） サービス用とは別に管理用インターフェースに対し、デフォルトゲートウェイが設定できること。
（セ） 機器は冗長化すること。
（ソ） 同時接続セッション数が 14,000,000 セッション保持できること。
（タ） L4 新規 HTTP コネクションを１秒当たり 600,000 コネクション受信できること。
（チ） SSL ハードウェアオフロードに対応できること。
（ツ） 2048 ビットの RSA 暗号化キー使用時に毎秒 2,500 以上のトランザクションが処理できること。

(9) 管理セグメント用スイッチ

（ア） 導入する機器に従い、管理ポートを接続するためのスイッチを２台設置すること。
（イ） 機器故障を考慮し、予備機を１台用意すること。
（ウ） 10BASE-T、100BASE-TX 及び 1000BASE-T 準拠の Ethernet ポートを 24 ポート以上実装できること。
（エ） クライアント接続用ポートで BPDU パケットを受信した場合、自動的にポートをシャットダウンできること。
（オ） エラーにより無効化されたポートを自動的に再試行できること。
（カ） QoS 機能によりパケットの重み付けと、優先転送制御ができること。
（キ） 802.1p サービスクラスでのパケット単位マーキング及び再分類ができること。
（ク） SSH によってリモート接続し、ポートの設定変更及びステータスが取得できること。
（ケ） SNMPv3 に対応したステータスが取得できること。
（コ） IEEE 802.3ad に対応し、複数のリンクを束ねて使用できること。

3.7.4 クライアント要件

(1) シンクライアント

① 職員用シンクライアント

（ア） 台数は、700 台用意すること。

（イ） 「2.2.1 仮想デスクトップ」が利用できること。

（ウ） 14.0 インチ以上の A4 ノート型であること。

（エ） 形状は、液晶ディスプレイ、キーボード等を内蔵したノート型パーソナルコンピュータであり、バッテリーを同時に装着及び使用できること。

（オ） CPU は、インテル Celeron プロセッサー 3855U（1.60GHz）またはその後継バージョンであること。

（カ） グラフィックスアクセラレーターは、Intel HD Graphics 510（CPU 内蔵）またはその後継バージョンであること。

（キ） メモリは、４GB 以上搭載すること。

（ク） メモリは、DDR4 SDRAM/PC4 17000 またはその後継バージョンを内蔵していること。

（ケ） 内蔵ディスプレイは、14.0 インチ以上の LED バックライト付き TFT カラー LCD で HD（1,366×768 ドット）及び 1,677 万色（アンチグレア処理）以上であること。

（コ） 外部ディスプレイ表示は、内部ディスプレイと同等以上の解像度及び表示色であり、デジタル出力できること。

（サ） スマートカードリーダ及び SD メモリーカードスロットを搭載できること。

（シ） キーボードは、日本語キーボード及び JIS 配列に準拠していること。

（ス） マウスは、２ボタン以上かつ縦スクロールが可能な USB 接続の光学式またはレーザー式であること。

（セ） ネットワークは、10BASE-T、100BASE-TX 及び 1000BASE-T に準拠したポートを１つ以上搭載すること。Wakeup On LAN に対応できること。

（ソ） 無線 LAN は、IEEE 802.11a/b/g/n/ac 準拠(5GHz 帯チャンネル:W52/W53/W56)及び Wi-Fi に準拠していること。

（タ） USB ポートは、USB3.0 インターフェースが２つ以上搭載されていること。

（チ） バッテリー駆動時間は、JEITA2.0 に基づき、2.5 時間以上であること。

（ツ） 消費電力は、最大消費電力が 70W 以下で対応できること。また、通常運転時は 5W 以下であり、電圧は 100V で対応できること。

（テ） 質量は、約 2.0kg 以下であること。

（ト） 日本語の取扱説明書を添付すること。

（ナ） 本体動作時において、温度 10℃から 35℃まで及び湿度 20%から 80%までの環境（ただし、結露しないこと）での動作が保証されていること。

② 運用業務用シンクライアント

（ア） 本クライアントは、運用担当者が運用業務で使用する。

（イ） 台数は、運用業務で必要となる台数を用意すること。
（ウ） 「2.2.1　仮想デスクトップ」が利用できること。
（エ） ハードウェアは、職員用シンクライアントと同一製品であること。
（オ） ソフトウェアは、職員用シンクライアントと同一製品であること。

(2)　ファットクライアント

①　職員用ファットクライアント・共用ファットクライアント

（ア） 台数は、40 台用意すること。
（イ） 職員用ファットクライアントについては、「2.2.1 仮想デスクトップ」が利用できること。
（ウ） 14.0 インチ以上の A4 ノート型であること。
（エ） 形状は、液晶ディスプレイ、キーボード等を内蔵したノート型パーソナルコンピュータであり、バッテリーを同時に装着及び使用できること。
（オ） CPU は、インテル Core i5-7200U プロセッサー（2.50GHz）またはその後継バージョンであること。
（カ） メモリは、8GB 以上搭載すること。
（キ） 内蔵ディスプレイは、14.0 インチ以上の LED バックライト付き TFT カラー LCD で HD（1,366×768 ドット）及び 1,677 万色（アンチグレア処理）以上であること。
（ク） 外部ディスプレイ表示は、内部ディスプレイと同等以上の解像度及び表示色であり、デジタル出力できること。
（ケ） ストレージは、標準 100GB 以上であること。
（コ） キーボードは、日本語キーボード及び JIS 配列に準拠していること。
（サ） マウスは、２ボタン以上かつ縦スクロールが可能な USB 接続の光学式またはレーザー式であること。
（シ） ネットワークは、10BASE-T、100BASE-TX 及び 1000BASE-T に準拠したポートを１つ以上搭載すること。Wakeup On LAN に対応できること。
（ス） 無線 LAN は、IEEE 802.11a/b/g/n/ac（5GHz 帯チャンネル：W52/W53/W56）及び Wi-Fi に準拠（MU-MIMO 対応）していること。
（セ） USB ポートは、USB3.0 インターフェースが４つ以上搭載されていること。
（ソ） バッテリー駆動時間は、JEITA2.0 に基づき、2.5 時間以上であること。
（タ） 消費電力は、最大消費電力が 70W 以下であること。また、通常運転時は 5W 以下であること。電圧は 100V 対応であること。
（チ） 質量は、約 2.2kg 以下であること。
（ツ） 日本語の取扱説明書を添付すること。
（テ） 盗難防止用ワイヤーロックの取付けができること。
（ト） 本体動作時において、温度 10℃から 35℃まで及び湿度 20%から 80%までの

環境（ただし、結露しないこと）での動作が保証されていること。

（ナ） ハードディスクのデータは暗号化できること。

（ニ） 端末紛失時における情報漏えい防止等のため、端末にデータを保持させない仕組みであること。なお、具体的な方法は、受注後に主管課と協議の上、決定すること。

（ヌ） ファットクライアントに搭載する Windows OS は、Microsoft 社 Windows 10 Enterprise 正規版とすること。

（ネ） 職員用ファットクライアントは、職員が、仮想デスクトップで動作しないソフトウェアであって常態的に利用するものをローカルで利用するために使用する。また、共用ファットクライアントは、USB デバイスを用いた院外とのファイルのやりとり及びファイル転送を用いた院内とのファイルのやりとりを行うために使用し、院内に物理的に接続しない形態とする。

② 運用業務用ファットクライアント

（ア） 本クライアントは、運用担当者が運用業務で使用する。

（イ） 端末の台数は、運用業務で必要となる台数を用意すること。

（ウ） ハードウェア及びソフトウェアは、「①職員用ファットクライアント・共用ファットクライアント」に記載の製品と同一であること。

（エ） Microsoft 社 Word 2016 またはその後継バージョンによる文書作成ソフトウェアが利用できること。

（オ） Microsoft 社 Excel 2016 またはその後継バージョンによる表計算ソフトウェアが利用できること。

（カ） 印刷できること。

（キ） 所定の場所からの移動ができないようワイヤーにより固定すること。

3.7.5 その他ハードウェア要件

(1) KVM装置

（ア） 本調達で導入しラックマウントするサーバについては、切替器を使ってラックマウントしたコンソールに接続できること。

（イ） コンソールは 1U サイズの引き出し型とすること。

（ウ） コンソールに備えるモニターは 10 インチ以上かつ 1,024×768 以上の解像度とすること。

（エ） コンソールにはマウス、トラックボール等のポインティングデバイスとすること。

(2) 無停電電源装置（UPS）

（ア） サーバ及びネットワーク機器（フロアスイッチ及びエッジスイッチを除く）については、無停電電源装置により不意の停電に備えること。

（イ） 商用電源の供給が停止した場合には、安全にシステムを停止させることが自動的にできること。
（ウ） 電源ユニットを複数持つ機器については、無停電電源装置１台に故障が発生しても継続稼働できるよう、２系統以上の電源供給ラインを確保できること。

3.7.6 施設・設備に関する事項

(1) 施設・設備の条件

① 設置場所

（ア） サーバ及びネットワーク機器（フロアスイッチ及びエッジスイッチを除く）は、主管課が指定するサーバ室内のラック（３台程度。本調達の対象外）に収容すること。
（イ） フロアスイッチは、本院の１階から８階までの EPS 内に設置すること。
（ウ） エッジスイッチは、執務室内に設置すること。

② ラック

（ア） サーバ室内のラックのサイズは、高さ 2,000㎜ 以下、奥行 1,100㎜ 以下及び 42U 以下の 19 インチラックとする。

③ 耐荷重

（ア） サーバ室の床耐荷重は 500kg/㎡である。

④ 電源

（ア） サーバ室が提供する電源（本調達の対象外）は、200V×20A 及び 100A×20A とする。なお、詳細は資料閲覧とする。

⑤ フロア配線

（ア） 本院及び地方支分部局等のフロアの配線は、既存のものを流用すること。

3.8 テストに関する事項

3.8.1 基本方針

（ア） 次期システムの正常稼動を保証するために、単体テスト、結合テスト及び総合テストを行うこと。
（イ） 単体テストは、ハードウェア及びソフトウェアが個別単体において、正しく機能することの確認を行うこと。
（ウ） 結合テストは、関連するハードウェア及びソフトウェアが、相互に正しく機能することを確認するため、段階的に結合した状態でテストを行い、各機能が要件どおり動作することを確認すること。

（エ） 総合テストは、次期システム全体として要件どおりにシステムが構築されていることを確認するため、システムが納品可能な状態であることを確認すること。さらに運用業務の遂行を想定した総合的な機能試験及び非機能試験（性能の確認、障害対応、バックアップ、リストア等）を行うこと。
（オ） 総合テストは、本院に設置された環境上で行うこと。
（カ） テスト方法及びスケジュールは、通信回線事業者、プリンタ事業者及び主管課と調整及び協議の上、利用者の業務影響がないよう検討を行うこと。

3.8.2 テスト計画
（ア） テストを実施するに当たり、「テスト実施計画書」を作成し、主管課の承認を得て作業を行うこと。
（イ） 「テスト実施計画書」には、テスト実施体制、テスト実施環境、作業内容、作業スケジュール、テストシナリオ、合否判定基準等を明記すること。

3.8.3 テスト実施
（ア） 「テスト実施計画書」に従い、各テストを実施すること。
（イ） テスト項目ごとに証跡を取得すること。
（ウ） テスト項目ごとにテスト結果を記入した上で、テスト結果の合否を記載すること。
（エ） テスト実施者以外においてもテストが適切に実施されていることを確認すること。
（オ） テストで発生した問題に対する原因及び影響範囲を分析し、対策すること。

3.8.4 テスト結果報告
（ア） 各テストに対する「テスト結果報告書」を作成すること。
（イ） テスト結果に対して定量的及び定性的な評価を行い、テストにおいて品質が担保されていることを示すこと。
（ウ） テスト完了基準を満たしていることを示すこと。
（エ） 「テスト結果報告書」には、テスト結果を記入したテスト項目及び証跡を含むこと。

3.9 受入テスト支援
3.9.1 受入テスト計画
（ア） 各種設計書等の内容に基づき、主管課及び各局課等が実施する受入テストの計画を行うこと。
（イ） 受入テストの計画においては、「受入テスト計画書（案）」を作成し、主管

課に提示すること。

（ウ） 「受入テスト計画書（案）」で記載する内容については、主管課と協議の上、決定すること。

3.9.2 受入テスト実施支援

（ア） 各種設計書等の内容に基づき、主管課及び各局課等が実施する受入テストの支援を行うこと。

（イ） 主管課が実施する受入テストの期間中、受入テストに必要となるデータ等を適宜提供するとともに、主管課からの問合せ対応等を行うこと。

（ウ） 受入テストにおいて発覚した不具合等については、原因の切分けを行うとともに、速やかに対処すること。

3.9.3 受入テスト結果報告書の作成支援

（ア） 受注者は、主管課が作成する「受入テスト結果報告書」の作成に必要となる情報提供等を行うこと。

3.10 移行に関する事項

3.10.1 基本方針

（ア） 次期システム各構成要素の特性等を十分考慮した上で、確実な移行が実施でき、現行システム及び業務に与える影響が極力少ないものとすること。

（イ） 現行システムの機器等との並行運用の必要性を含め、具体的な移行方法等を検討すること。

（ウ） 現行システムの構成及び運用、関連する他の情報システム等を把握し、関係者と必要な調整を行った上で、受託者の責任において移行すること。

（エ） 現行システムの運用事業者への移行作業に係る協力依頼等が必要な際は、主管課の承認を得ること。

（オ） 関連する他の情報システムの情報は、資料を閲覧して把握すること。

（カ） 移行作業に必要な機器は、受託者が提供し、作業終了後に撤去すること。

（キ） 移行に伴い必要となるケーブル類、電源タップ等及びこれに係わる工事については、受託者の費用負担において用意すること。

（ク） 機器を接続する各ケーブルは、タグ、テープ等により接続先機器等を識別できること。

（ケ） 導入機器等の搬入及び搬出は、受託者が行うこと。なお、養生が必要な場合は、対応すること。

（コ） 機器等の梱包材については、受託者にて破棄すること。

（サ） 現行システムの停止を伴う作業が避けられない場合は、利用者への影響を

最小限に抑えるため、基本的に閉庁日の作業とし、事前に主管課の承認を得ること。また、各執務室内への機器の搬入、設置及び調整も、利用者の業務に支障を与えないよう同様の対応を行うこと。

（シ）次期システムへの移行は各拠点の機器、回線、本院の各フロア、回線及び各種サーバシステムの切替えが必要である。切替え方法及び切替えスケジュールは、通信回線事業者、プリンタ事業者及び主管課と調整及び協議の上、利用者の業務影響がなく、期間内に終了するよう検討すること。

（ス）現行システムと次期システムが並行稼動する期間は、現行システムの運用事業者と連携し、トラブル及び問合せに対応する体制を保持すること。

（セ）大規模なトラブル等により本番稼働への影響が大きい場合には、現行システムへの切戻しを行うこと。

（ソ）切戻し作業は、受託者の責任により実施し、切戻しにより発生する費用はすべて受託者で負担すること。

（タ）移行対象データは、アカウント情報、ファイル共有データ、メール関連データ、スケジュール、会議室予約、デバイス管理等を想定しているが、その他の必要となるデータについては、主管課と協議の上、決定すること。

3.10.2 移行計画

（ア）「移行実施計画書」を作成すること。

（イ）「移行実施計画書」には、移行方針、移行実施体制、移行環境、移行全体スケジュール、コミュニケーションルール、移行判定の考え方、リスク及びコンティンジェンシープラン等を記載すること。

（ウ）システム移行及びデータ移行に係る方針、方法等について「移行設計書」を作成すること。

（エ）システム移行設計には、ハードウェア、ソフトウェア、ネットワーク設定等を含むこと。

（オ）データ移行設計には、データ移行対象、移行期間、利用者への影響等を含むこと。

（カ）「移行設計書」において、移行判断基準を定めること。

（キ）移行判断基準は、可能な限り定量的なものとすること。

（ク）「移行設計書」に基づき、移行を実施する手順として、「移行手順書」を作成すること。

（ケ）「移行手順書」には、移行に係る作業項目、担当者、操作対象、操作方法、想定時間、作業結果の確認方法、作業間の依存関係等を記載すること。

（コ）円滑なシステム移行、移行データ漏れの防止等を考慮した上で、移行リハーサルを提案し、当該結果を踏まえ移行計画を更新すること。

3.10.3 移行作業

（ア） 「移行実施計画書」、「移行設計書」及び「移行手順書」に従い、移行を実施すること。

（イ） 移行作業に対する証跡を取得すること。

（ウ） 移行作業中は、作業項目ごとに作業状況（作業中、作業完了等）を把握すること。

（エ） 移行実施者以外においても移行が適切に実施されていることを確認すること。

（オ） 移行で発生した問題に対する原因及び影響範囲を分析し、対策を講じること。

3.10.4 移行結果報告

（ア） 移行判定基準に基づき移行結果を判定し、「移行結果報告書」に取りまとめ、主管課の承認を得ること。

（イ） 移行判断基準を満たしていることを示すこと。

（ウ） 「移行結果報告書」には、移行作業に対する証跡を含むこと。

3.11 引継ぎに関する事項

3.11.1 基本方針

（ア） 受託者のうち、設計・構築を実施したチームから運用担当者及び保守担当者への引継ぎを行うこと。

（イ） 主管課の依頼に基づき、必要に応じて現行システムの運用事業者との引継ぎを行うこと。

3.11.2 引継ぎ計画

（ア） 「引継ぎ計画書」を作成し、主管課の承認を得ること。

（イ） 「引継ぎ計画書」には、引継ぎ実施方針、引継ぎ項目、引継ぎ方法、引継ぎスケジュール、コミュニケーションルール、引継ぎ完了基準等を記載すること。

（ウ） 引継ぎ完了基準に、引継ぎ元及び引継ぎ先の双方における引継ぎ完了の合意形成を含めること。

3.11.3 引継ぎの実施

（ア） 「引継ぎ計画書」に従い、引継ぎを実施すること。

（イ） 引継ぎ作業中は、引継ぎ項目ごとに作業状況（作業中、作業完了等）を把

握すること。

（ウ） 引継ぎで発生した問題に対する原因及び影響範囲を分析し、対策を講じること。

3.11.4 引継ぎの完了報告

（ア） 「引継ぎ完了報告書」を作成し、主管課の承認を得ること。

（イ） 引継ぎ完了基準を満たしていることを示すこと。

3.12 教育に関する事項

3.12.1 基本方針

（ア） 主管課に「利用者マニュアル」及び「運用・保守マニュアル」を事前配布し、次期システムの理解を促進すること。

（イ） 利用者に「利用者マニュアル」を事前配布し、机上での次期システムの理解を促進すること。

（ウ） 主管課に対して、「利用者マニュアル」及び「運用・保守マニュアル」を用いた研修を実施することが望ましい。

3.12.2 教育計画

（ア） 「教育計画書」を作成し、主管課の承認を得ること。

（イ） 「教育計画書」には、教育実施方針、教育方法、教育スケジュール、コミュニケーションルール等を記載すること。

3.12.3 教育の実施

（ア） 「教育計画書」に従い、教育を実施すること。

（イ） 次期システムの操作方法等を示した「利用者マニュアル」を作成すること。

（ウ） 主管課等の人事院職員が実施する運用業務については、主管課と協議の上、「運用・保守マニュアル」を作成すること。

（エ） 主管課による次期システムに関する規程の作成を支援すること。

3.13 運用に関する事項

3.13.1 運用概要

（ア） 常駐時間帯は、原則、開庁日の９時 30 分から 17 時 30 分まで（休憩時間１時間を含む）とする。なお、サービスの停止等、重大な障害が発生した場合は、主管課と連携の上、継続して対応を行うこと。

（イ） 常駐場所は主管課の指定する場所とする。常駐場所は、日々整理整頓し、清潔保持に努めるとともに、勤務場所の環境美化に関する必要な措置を行

うこと。

（ウ） 運用担当者は、常駐要員として２名配置すること。

（エ） 運用を開始するに当たり、システム稼働計画、要員稼働計画等を記載した「運用・保守実施計画書」を作成し、主管課の承認を得ること。

（オ） 別途閲覧に供する「人事院業務継続計画」で定める対応が可能となるよう連絡網を整備すること。また、大規模災害の発生等において受託者と連携し、状況の確認及び対策協議を行うこと。

（カ） 運用業務の項目は、「3.13.2　定常運用業務」以降の項目に示す。

3.13.2 定常運用業務

(1)　定期報告

（ア） 問合せ及びインシデントへの対応状況、課題管理状況、リソース状況等について、 月次で報告を行うこと。実施に関する詳細については、主管課と受託者が別途協議の上、決定すること。

（イ） 報告会を実施した際は、議事録を作成し、主管課の承認を受け、提出すること。

(2)　監視

（ア） 機器の死活監視を行うこと。

（イ） 監視ツール等を用いて、機器の死活状況、イベントログ、サービス、プロセス及びリソース等を常時監視すること。

（ウ） 構成機器の LED ランプを目視し、ハードウェア障害、エラー等の症状を示す表示がないか確認すること。

（エ） サーバ、仮想デスクトップ及びファットクライアントのウイルスパターンファイルの配布状況を確認すること。

（オ） スケジュールバックアップが正常に完了していることを確認すること。

（カ） 次期システムにおけるトラフィック情報の取得を行い、トラフィック情報の取得状況を確認すること。なお、トラフィック情報の取得周期については、主管課と協議の上、決定すること。

（キ） クライアント及び各サーバを監視し、ウイルスを検出した場合、直ちに利用者及び対象のクライアントに関する情報を主管課に報告すること。また、ウイルスパターンファイルの更新等に障害が発生しているクライアントの有無を確認し、障害が発生している場合は、主管課に報告すること。

(3)　パターンファイルの取得

（ア） オフライン環境下のデバイスに適用するため、パターンファイルをセキュリティベンダのホームページからダウンロードし、所定の共有フォルダに格納を行うこと。

(4) パッチ適用

（ア） 十分な検証を実施し、主管課と協議の上、サーバ、仮想デスクトップ及びファットクライアントに対して、セキュリティパッチの適用を行うこと。

（イ） 仮想デスクトップ及び職員用ファットクライアントへのパッチ適用は、毎月１回程度対応すること。なお、緊急性の高いものについては、随時対応を行うこと。

（ウ） パッチ適用を実施する際は、事前に適用の必要性を検討し、動作検証を行うこと。

（エ） 上記（ウ）で検討及び検証した結果を踏まえ、パッチの適用方法を検討し、適用の必要性、動作検証結果及び適用方法を主管課に報告し、承認を得た上で、パッチの適用を行うこと。

(5) バックアップ

（ア） バックアップ設計及び実行計画を策定すること。

（イ） パッチ適用後、端末のマスタイメージ及びサーバのシステムバックアップの取得を行うこと。

（ウ） バックアップデータの整理及び管理を行うこと。

(6) 管理用アカウント管理

（ア） 本調達で導入するサーバ等の管理用アカウント及びパスワード管理を行うこと。

(7) SLA管理

（ア） 運用・保守業務の効率化及び品質向上並びに円滑化を図るため、主管課と協議の上、決定する管理指標に対して SLA を決定すること。

（イ） 管理指標に対する実績値を取りまとめ、四半期に１度、SLA の遵守状況に関する報告を行うこと。

（ウ） SLA は努力目標型とし、達成状況等を踏まえて、主管課と協議の上、運用・保守業務の改善、管理指標の見直し等を行うこと。

（エ） 主管課及び受託者で協議の上、計測の除外とした場合は、SLA の適用外とする。

(8) 定期停電対応

（ア） 定期停電対応について、計画に基づき機器の停止及び起動を行うこと。なお、定期停電対応は、開庁日の業務時間後及び閉庁日に実施する。

(9) 運用・保守業務の改善提案

（ア） 運用・保守業務の実施状況を分析し、改善提案を行うこと。また、同提案については、主管課と協議の上、実施すること。

(10) 外部監査対応支援

（ア） 外部監査が行われる場合、必要な資料及び証跡の提供等の対応を行うこと。

3.13.3 非定常業務

(1) アカウント及び関連する情報の管理

（ア） 利用者の追加、変更及び削除に伴い、アカウント、メールアドレス、メールボックス及び個人フォルダの登録、変更及び削除を行うこと（年間 300 件程度）。

（イ） 不正なアカウントによる不正操作等を防止するため、定期的に使用されていないアカウントの無効化を行うこと。

（ウ） 利用者によるパスワード再発行の仕組みがない場合は、依頼によりパスワードの再発行等の作業を行うこと。

(2) 仮想デスクトップの割当て

（ア） 主管課の依頼に基づき、利用者へ仮想デスクトップの割当て、変更及び削除を行うこと。

(3) ファイルサーバ管理

（ア） 主管課の指示に基づき、ファイルサーバの共有フォルダの新規作成、変更、削除及びクォータの設定を行うこと。

(4) デバイス管理

（ア） 主管課の指示に基づき、資産管理に関する設定を行うこと。

(5) ライセンス管理

（ア） OS、ミドルウェア等のソフトウェアのライセンス管理を実施すること。なお、対象とする製品等は主管課と協議の上、決定すること。

(6) 証跡管理

（ア） 主管課の指示に基づき、証跡ログの提出を行うこと。

（イ） ログの取得対象は以下を想定しているが、主管課と協議の上、決定すること。

- 仮想デスクトップ及び職員用ファットクライアントに関するログ
- サーバ、ネットワーク機器等に関するログ　等

(7) ログ調査

（ア） 主管課からの指示に基づき、各サーバのログから、URL へのアクセス履歴、特定のメールアドレスからの受信履歴及びサーバへのログイン履歴の有無の調査を行うこと。

(8) 人事院ホームページに対するパッチ適用

（ア） 平成 31 年 1 月以降に政府共通 PF 内に新たに構築される人事院ホームページへの OS 等のパッチ適用を行うこと。なお、パッチ適用方法等の詳細は、主管課と協議の上、決定すること。

(9) 構成変更

① 仮想デスクトップマスタイメージの更新

（ア） OS 及びソフトウェアを変更並びにマスタイメージの再配布を行うこと。

② メールの受信許可及び拒否リストの設定

（ア） 送信者のメールアドレス、ドメイン等の受信許可及び拒否リストの設定を行うこと。

③ Web フィルタリングのルールの変更

（ア） Web サイトにおける接続制限の追加及び削除を行うこと。

④ グループポリシーの設定

（ア） グループポリシーの設定を行うこと。

⑤ 新規メールドメインの追加設定

（ア） 政府共通 NW における新規メールドメインの追加依頼に応じて、メールサーバへの追加設定を行うこと。

⑥ DNS サーバの設定変更

（ア） IP アドレス及びホスト名の変更に伴い、必要に応じて DNS サーバへの登録及び変更を行うこと。

⑦ スイッチのポート開閉設定

（ア） スイッチのポート開閉を行うこと。

⑧ 変更管理

（ア） 構成変更に伴う導入機器のパラメータシートの更新を行うこと。

(10) 台帳管理

① 運用インシデント管理表

（ア） 次期システムを構成するハードウェア及びソフトウェアの障害等の記録を行うこと。

② 管理者アカウント管理台帳

（ア） 管理者アカウント及びパスワードを記録し、変更時に更新を行うこと。

③ 資産管理台帳

（ア） 次期システムを構成するハードウェア及びソフトウェアを記録し、変更時に更新を行うこと。

④ 仮想デスクトップのマスタイメージ管理台帳

（ア） 仮想デスクトップのマスタイメージの構成を記録し、変更時に更新を行うこと。

⑤ ライセンス契約台帳、保守契約台帳の管理

（ア） ソフトウェアのライセンス契約台帳及びハードウェアの保守契約台帳の更新を行うこと。

(11) ドキュメント管理

（ア） 以下のドキュメントを作成し、変更が発生した場合、追記及び修正を行う

こと。

- 運用・保守体制表
- 運用・保守手順書
- 障害対応手順書
- ネットワーク構成図
- ラック搭載図
- 電源配線図
- ネットワーク機器のポートアサイン表
- その他運用・保守業務に係る資料

（イ） 設計・構築に関するドキュメントも含め、次期システムに係るすべてのドキュメントの変更及び改訂の管理を行うこと。

（ウ） 運用業務開始前にドキュメントの保管方法及び管理基準を策定し、主管課の承認を得ること。

（エ） ドキュメントは適切に保管及び管理を行うこと。

(12) 人事異動・組織改編に伴う対応

（ア） 人事異動等に伴うクライアントの追加及び入替え等にあわせ、システムに必要な設定等を行うこと。

(13) 次々期システム事業者等への引継ぎ

（ア） 主管課の依頼に基づき、必要に応じて次々期システム事業者等との引継ぎを行うこと。

3.13.4 障害・セキュリティインシデント対応

(1) 障害対応

① 障害対応受付及び一次切分け

（ア） ハードウェア及びソフトウェアの障害発生時に、原因の一次切分けを行うこと。

（イ） 一次切分けの結果、ハードウェア障害の場合は、障害対象機器を特定の上、保守担当者に対応を依頼すること。ソフトウェア障害の場合は、問題の箇所の特定を行いつつ、保守担当者に対応を依頼すること。

② 仮想デスクトップの復旧

（ア） 仮想デスクトップの復旧は、仮想デスクトップの再起動及び再割当てにより対応すること。

③ ファットクライアントの復旧

（ア） ファットクライアントの復旧は、マスタイメージを利用したリカバリを実施し、必要な初期設定を行うこと。

④ システム復旧後の確認

（ア） 障害への対処完了後、動作確認を行うこと。
（イ） バックアップイメージからシステム復旧を行う必要がある場合は、主管課と協議の上、実施し復元後に動作確認を行うこと。

⑤ サーバ回復時のデータ復旧

（ア） サーバについては、修理完了後、バックアップデータからデータの復旧を行うこと。

⑥ 障害情報管理

（ア） 障害発生から復旧完了までの障害の内容及び対応状況について、「障害管理表」に記載し管理を行うこと。

(2) セキュリティインシデント対応

① 初期対応

（ア） 運用マニュアルに沿った初動対応を行うこと。

② サーバログイン履歴確認

（ア） ログからサーバログイン履歴を確認すること。

③ 不正プログラム検知時の対応

（ア） 不正プログラムを検知した場合、速やかに主管課に報告し、必要に応じてログ取得及び検体採取を行うこと。

④ 不審 URL ブロック

（ア） 主管課より不審 URL の報告を受けた際に、URL フィルタの設定変更を行うこと。

⑤ FW のトラフィック確認

（ア） 主管課の指示に基づき、FW のトラフィックログの抽出及び調査を行うこと。
（イ） 主管課と協議の上、不正アクセスと判断した場合に、FW ポリシーの設定変更を行うこと。

⑥ 未承認アプリケーションの使用禁止

（ア） 主管課の未承認アプリケーションの動作の制限を行うこと。

3.14 保守に関する事項

3.14.1 保守概要

（ア） 「仮想デスクトップにログインの上、ファイルサーバのファイルにアクセスして業務を行う」のに必要な機器等（ただし、端末及びエッジスイッチを除く。）については、24 時間 365 日の保守対応を可能とすること。端末を除くその他の機器等については、原則として、開庁日の午前９時から午後５時までのオンサイト対応とする。端末については、原則として、翌開庁日の午前９時から午後５時までのオンサイトで、修理、交換又は調整を行うこと。

（イ） サーバのストレージの障害による交換対応を行う場合、ツール等を使用したデータの抹消、物理的な破壊を行う等、データの読取りが不可な状態にしたことを証明する書面を主管課に提出すること。
（ウ） 保守の対象は、本調達で導入した機器及びソフトウェアとすること。
（エ） 保守に係る一切の費用は調達に含めること。
（オ） 次期システムの運用期間中に、本調達で導入した機器、ソフトウェア、サービス等が、製造元の都合による保守サポートの終了等により保守対応が終了する場合には、主管課の承認の上、受託者の負担において、保守サポートが可能かつ同等以上の機能と性能を持った代替の機器、ソフトウェアまたはサービスを提供すること。

3.14.2 定常業務

(1) 情報提供、予防保守

（ア） 製造元等からのサポートに基づき、機器等の不具合及び脆弱性、点検、パーツ交換、ファームウェアのバージョンアップ等に関する情報を入手し、主管課に提供すること。また、必要に応じて、当該情報に基づく対応を行うこと。
（イ） 本調達で導入するハードウェア等について、製造元等が予防保守事項を定めている場合には、定期的な点検、パーツ交換等を適切に実施すること。

3.14.3 非定常業務

(1) ハードウェア保守

① サーバ及びネットワーク機器

（ア） サーバ及びネットワーク機器の製造元と、平成 34 年 9 月 30 日までの保守契約の締結を行うこと。
（イ） サーバ及びネットワーク機器に故障が発生した場合、主管課の承認を得た上で、機器全体または一部の交換を行い、正常動作を確認すること。
（ウ） 故障の原因を特定し主管課に報告を行うこと。
（エ） データを記録する部品については、データ消去を行い、「消去証明書」を主管課に提出し承認を得た上で、院外に持ち出すこと。なお、サーバ及びストレージ搭載のハードディスク（SSD 含む）は、保守交換したハードディスクは返却しない保守サービスの提供を行うこと。
（オ） 院内でのデータ消去が困難な機器及び部品については、院外に持ち出すに当たり、セキュアな持出し方法を確立することを条件とし、院外でのデータ消去後、「消去証明書」を主管課に提出し承認を得ること。
（カ） 機器の持出しが必要な場合は、主管課の許可を得ること。

② クライアント

（ア） クライアントの製造元と平成 34 年９月 30 日までの保守契約の締結を行うこと。

（イ） 故障の原因を特定し、主管課に報告を行うこと。

（ウ） データを記録する部品については、データ消去を行い、「消去証明書」を主管課に提出し承認を得た上で、院外に持ち出すこと。ただし、院内でのデータ消去が困難な機器及び部品については、院外に持ち出すに当たり、セキュアな持ち出し方法を確立することを条件とし、院外でのデータ消去後、「消去証明書」を主管課に提出し承認を得ること。

（エ） ファットクライアント搭載のストレージにおいては、保守交換したストレージを院外へ持ち出さない保守サービスの提供を行うこと。

③ その他機器

（ア） その他本調達で納入するすべての機器について、製造元と平成 34 年９月 30 日までの保守契約の締結を行うこと。

（イ） その他機器に故障が発生した場合、機器全体または故障パーツの交換を行い、正常動作確認を行うこと。なお、機器、故障パーツ等の交換においては、即時対応できるよう、交換部品及び運送手段が確保されていること。

（ウ） 無停電電源装置で、バッテリー劣化障害と判断された場合、バッテリー交換を賃貸借期間内に１回まで行うこと。

(2) ソフトウェア保守

① サーバ及びネットワーク機器のソフトウェア保守要件

（ア） ソフトウェアのセキュリティパッチ、不具合修正パッチ及び機能改善パッチは、本調達の範囲内で提供を行うこと。

② 端末のソフトウェア保守要件

（ア） 業務端末に搭載されるソフトウェア（ファームフェアを含む）は、製造元と平成 34 年９月 30 日までの保守契約の締結を行うこと。

（イ） ソフトウェアのセキュリティパッチ、不具合修正パッチ及び機能改善パッチは、平成 34 年９月 30 日まで本調達の範囲内で提供を行うこと。

3.14.4 障害発生時対応

（ア） 保守担当者は運用担当者が実施する切分けの結果、機器等に起因する異常と判明した場合、原因調査及び復旧対応を行うこと。なお、通信回線、プリンタ等の障害において、原因の特定や基盤側の設定変更等、必要に応じて運用担当者は協力の上、確実かつ早期復旧に向け対応すること。