入札説明書

件名　独立行政法人統計センター情報システム基盤の構築及びサービス提供業務

（総合評価落札方式（加算方式））

独立行政法人統計センター

令和５年 12 月 27 日

※（注意）　入札説明書等をダウンロードした際は、必ず入札件名、会社名、営業担当者名、電話番号、ＦＡＸ番号を下記宛先までメールにてご連絡をお願いします。
なお、ご連絡先の連絡がない場合、当センターからの連絡事項、仕様書の修正等をお伝えすることができないことになりますので、ご理解、ご協力の程よろしくお願いいたします。
【総務部財務課調達係】　MAIL：koukoku_atmark_nstac.go.jp
※　「_atmark_」を「@」に置き換えて送信してください。

目　次

入札説明書の概要

件名：独立行政法人統計センター情報システム基盤の構築及びサービス提供業務

1　調達日程等

項　目	日　時	場　所
①入札説明会（※１，２）	令和６年１月 15 日 14 時 00 分	総務省第二庁舎１Ｆ105 号室 （東京都新宿区若松町 19-1）
②開札（※３）	令和６年３月 29 日 14 時 00 分	

※１　入札説明会に参加を希望する場合は、令和６年１月 12 日午後５時までに入札説明書 15（２）宛にメールにて連絡すること。なお、参加者が多い場合は日程の調整を行うこととする。

※２　入札説明会に参加する際は、本入札説明書を持参すること。

※３　原則立ち会うこととするが、今般の社会情況に応じて、立ち会えない場合には、開札日の前日までに事前の連絡をすること。

2　提出書類等

項　目	様　式（※１）	提出期限	提出場所
①入札書 （内訳書含む）	別紙様式第１号 （長３封筒に入れ封緘すること）	令和６年 ２月 26 日 14 時 00 分	総務省第二庁舎 ３Ｆ314 号室 独立行政法人 統計センター 総務部財務課 調達係 （東京都新宿区 若松町 19-1）
③委任状	別紙様式第２号		
③総務省競争参加資格	R4～R6 資格審査結果通知書 （全省庁統一資格）写し		
④提案書	別紙様式第３号及び別紙		
⑤再委託承認申請書	別紙様式第４号（※２）		
⑥下見積書	別紙様式第６号	令和６年 ２月 15 日 14 時 00 分	

※１　提出書類は、各様式の注意書きを熟読の上、作成すること。

※２　再委託を予定している場合のみ作成し、提出すること。

3　その他

① 落札者の決定方法　総合評価

② 契約方式　確定契約

③ 留意事項　詳細については、入札説明書等を熟読し、内容を理解、遵守すること。

入札説明書

1　契約担当者の役職及び氏名等

（１）　契約担当者　　契約担当役　独立行政法人統計センター理事長　佐伯　修司

（２）　所 在 地　　〒162-8668 東京都新宿区若松町 19 番１号

2　調達内容

（１）　件　　名　　独立行政法人統計センター情報システム基盤の構築及びサービス提供業務

（２）　業務内容　　仕様書のとおり

（３）　履行期間　　仕様書のとおり

3　競争参加者に必要な資格に関する事項

（１）　独立行政法人統計センター契約事務取扱要領第７条の規定に該当しない者であること。ただし、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、この限りではない。

（２）　独立行政法人統計センター契約事務取扱要領第８条の規定に該当しない者であること。具体的には、以下の各号のいずれかに該当し、且つ、その事実があった後３年を経過していない者（これを代理人、支配人その他の使用人として使用する者についても同じ。）は、競争に参加する資格を有しない。

①　契約の履行に当たり故意に工事製造その他の役務を粗雑に行い、又は物件の品質若しくは数量に関して不正の行為をした者

②　公正な競争の執行を妨げた者又は公正な価格を害し若しくは不正の利益を得るために連合した者

③　落札者が契約を結ぶこと又は契約者が契約を履行することを妨げた者

④　監督又は検査の実施に当たり、職員の職務の執行を妨げた者

⑤　正当な理由がなくて契約を履行しなかった者

⑥　契約により、契約の後に代価の額を確定する場合において、当該代価の請求を故意に虚偽の事実に基づき過大な額で行ったとき。

（３）　令和４・５・６年度総務省競争参加資格（全省庁統一資格）の「役務の提供等」においてＡ、Ｂ又はＣの等級に格付けされた者であること。（「役務の提供等」の営業品目の「情報処理」又は「ソフトウェア開発」に登録してある者であって、かつ「賃貸借」に登録してある者であること。）

（４）　提案書によって当該業務の履行が可能であると証明し、且つ契約担当役が要求要件を満たし当該業務の履行が可能であると判断した者であること。

（５）　総務省及び他省庁等における指名停止等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。ただし、他省庁等における処分期間については、総務省の処分期間を超過した期日は含めない。

（６）　本入札に参加する者は、入札前に必ず統計センターが保持する本業務における資料を閲覧すること。なお、詳細については、「既存資料閲覧要領」を確認すること。

（７）その他必要な書類等の提出を指示された場合は、これに応じなければならない。

4　**入札説明会の日時及び場所**

（１）　日　時　　令和６年１月 15 日　午後２時

（２）　場　所　　総務省第二庁舎　入札室（１階、扉番号 105）

（３）入札説明会に参加を希望する場合は、令和６年１月 12 日午後５時までに入札説明書 15（２）宛にメールにて連絡すること。なお、参加者が多い場合は日程の調整を行うこととする。

5　**入札及び契約手続において使用する言語及び通貨**

日本語及び日本国通貨に限る。

6　**入札保証金及び契約保証金**

免除

7　**提案書の作成等**

（１）　この一般競争入札に参加する者は、提案依頼書に基づき、別紙様式第３号「提案書」等を作成し、提出期限までに提出しなければならない。

（２）　本業務の実施にあたり、適正な履行を確保するために必要な範囲において、本契約の一部について再委託を予定している場合は、別紙様式第４号「再委託承認申請書」を作成し、提出しなければならない。

（３）　提出された提案書等は、独立行政法人統計センターにおいて確認及び審査し、資格があると認められた者に限り、入札の対象者とする。

（４）　契約担当役は、提出された提案書等を本入札の実施以外に使用することはない。

（５）　提案書等の作成に要する費用は、すべて入札者の負担とする。

（６）　提案書等の提出方法

① 入札者は提案書を封筒に入れ、紙媒体で６部（正１部、副５部）及び電子媒体として CD-R 等に納め２部（正・副）提出しなければならない。※詳細は「提案依頼書」参照。

② 提案書を直接提出する場合は、封筒に入れ封緘し、且つその封皮に氏名（法人の場合は、その名称又は商号）及び「令和６年３月 29 日午後２時開札（独立行政法人統計センター情報システム基盤の構築及びサービス提供業務）の提案書在中」と記述しなければならない。

③ 郵便（書留郵便に限る。令和６年２月 26 日午後２時までに必着のこと）により提出する場合は、提案書を封筒に入れ、その封皮には直接提出する場合と同様に氏名等を記述し、提出期限までに下記宛に送付しなければならない（提出部数も同様とする。）。

④ 電子メール（PDF ファイル）により提出する場合は、別添１で定める手続きに従い、提出期限までに提出しなければならない。なお、電報、ファクシミリ、電話その他の方法による入札は認めない。

⑤ 入札者は、提出した提案書の引換え、変更又は取り消しをすることができない。

（７）　**提案書の提出期限**　　**令和６年２月 26 日午後２時迄**

（８）　**提案書の提出場所**　　**〒162-8668 東京都新宿区若松町 19-１**

独立行政法人統計センター総務部財務課調達係

（３階、扉番号 314）

8　**入札方法**

（1）　入札者は入札公告及び入札説明書等を熟読の上、入札しなければならない。この場合において、入札説明書等に疑義があるときは、関係職員に説明を求めることができる。ただし、入札後は、これらの不明を理由として異議を申し立てることはできない。

（2）　入札金額は、総額を記載すること。

（3）　入札金額は、仕様書に基づき、各種手続き等に要する物品及び役務費用の他、保険料及び関税等、指定する納入場所での引き渡しまでに要する一切の経費の合計を見積もり、その金額を入札書に記載すること。また、官給する物品等がある場合には、その受け取りに必要な費用も入札金額に含むものとする。**（入札金額は下見積書の金額を超えないこと。）**

（4）　落札決定に当たっては、入札書に記載された金額に当該金額の 10%に相当する額を加算した金額（当該金額に１円未満の端数があるときは、その端数金額を切り捨てた金額とする。）をもって落札価格とするので、入札者は、消費税及び地方消費税に係る課税事業者であるか免税事業者であるかを問わず、見積もった金額の 110 分の 100 に相当する金額を入札書に記載しなければならない。

（5）　入札書の提出方法

①　入札者は、入札書を封筒に入れ提出しなければならない。

②　入札書は、別紙様式第１号により作成し、提出する場合は、封筒に入れ封緘し、且つその封皮に氏名（法人の場合は、その名称又は商号）及び「令和６年３月 29 日午後２時開札（独立行政法人統計センター情報システム基盤の構築及びサービス提供業務）の入札書在中」と記述しなければならない。

③　**入札書提出の際には、内訳書を作成の上、同封すること。**

内訳書の様式は適宜とし、記載内容は、数量、単価及び金額等を明らかにすること。なお、内訳金額が入札金額と符合しない場合は、入札金額で入札したものとみなす。この場合において、入札者は内訳金額の補正を求められたときは、直ちに入札金額に基づいてこれを補正しなければならない。

④　郵便(書留郵便に限る。令和６年２月 26 日午後２時までに必着のこと)により提出する場合は、入札書提出期限までに、（９）に示す場所あてに送付しなければならない。ただし、やむを得ない理由により入札者又はその代理人が開札に立ち会わず、郵便により提出する場合は、初度入札の入札書在中の封筒には「１回」と、再度入札の入札書在中の封筒には「２回」から順に回数を記載して、それらをまとめ別の封筒に入れ、表面に「入札書在中」と記載して、入札書提出期限までに、（９）に示す場所あてに送付しなければならない。

⑤　電子メール（PDF ファイル）により提出する場合は、別添１で定める手続きに従い、入札書を提出しなければならない。なお、電報、ファクシミリ、電話その他の方法による入札は認めない。

⑥　入札者は、提出した入札書の引換え、変更又は取り消しをすることができない。

（6）代理人による入札

①　代理人が入札する場合には、委任状を別紙様式第２号により作成し、入札書提出時に提出しなければならない。

②　入札者又はその代理人は、本件調達に係る入札について他の入札者の代理人を兼ねるこ

とができない。

（７）資格決定通知書

入札者は前記３（３）による資格決定通知書の写しを入札書提出時に提出しなければならない。

（８）**入札書の提出期限 令和６年２月 26 日午後２時迄**

（９）**入札書の提出場所 〒162-8668 東京都新宿区若松町 19-１**

独立行政法人統計センター総務部財務課調達係

（３階、扉番号 314）

（10）入札に関する注意事項

① 入札者は、「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）等に抵触する行為を行ってはならない。

② 入札者は、入札にあたって、競争を制限する目的で他の入札者と入札価格又は入札意思についていかなる相談も行わず、独自に入札価格を定めなければならない。

③ 入札者は、落札者の決定前に、他の入札者に対して入札価格を意図的に開示してはならない。

④ 公正な価格を害し又は不正の利益を得るための連合をしてはならない。

⑤ 入札者は、正当な理由がないのに商品又は役務をその供給に要する費用を著しく下回る対価で継続して供給し、その他不当に商品又は役務を低い価格で供給し、他の事業者の事業活動を困難にさせる恐れがある入札価格を定めてはならない。

9 入札の無効

次の各号のいずれかに該当する入札書は、無効とする。

（１） 入札公告及び３（１）－（７）に示した競争参加資格のない者が提出した入札書

（２） 委任状を提出しない代理人が提出した入札書

（３） 金額を訂正した入札書、また、それ以外の訂正について訂正印のない入札書

（４） 誤字、脱字等により意思表示が不明確な入札書

（５） 本件責任者及び担当者の役職、氏名及び連絡先の記載がない入札書(但し、代表者印を押印している場合はこの限りではない)

（６） 明らかに連合によると認められる入札書

（７） 明らかに錯誤と認められる入札書

（８） 同一の入札について、２通以上提出された入札書

（９） 入札公告に示した日時までに到着しない入札書

（10） 入札者に係る資格審査が開札日時までに終了しないとき又は資格を有すると認められなかったときの入札書

（11） 入札に関する条件に違反した者の提出した入札書

（12） 提出書類に虚偽又は不正の記載を行った者の提出した入札書

（13） 入札書が郵便で差し出された場合において８（５）④ただし書きに定める記載のない入札書

（14） 入札者に求められる義務を履行しなかった者の提出した入札書

10 入札の延期等

入札者が連合し又は不穏の挙動をする等の場合であって、競争入札を公正に執行するこ

とができない状態にあると認められるときは、当該入札を延期し、又はこれを取り止めることがある。

11　**開札**

（１）　日時及び場所　**令和６年３月 29 日　午後２時**

総務省第二庁舎　入札室（１階、扉番号 105）

（２）　開札

①　開札は、入札者又はその代理人を立ち会わせて行う。ただし、やむを得ない理由により入札者又はその代理人が立ち会わない場合は、入札執行事務に関係のない職員を立ち会わせて行う。

②　入札者又はその代理人は、開札時刻後においては、開札場に入場することはできない。

③　入札者又はその代理人は、契約担当者が特にやむを得ない事情があると認めた場合の外、開札場を退場することができない。

④　開札場では、みだりに私語を発してはならない。

（３）再度入札

①　開札をした場合において、予定価格の制限の範囲内に達した価格の入札がないときは、直ちに再度入札を行うものとする。（入札書は、複数枚用意しておくこと。）

②　再度入札をしても落札者がないときは、入札をやめることがある。この場合、異議の申立てはできない。

③　前号①ただし書きに該当し、事前に２回目以降の入札書の提出がない場合は、入札辞退とする。

12　落札者の決定方法

（１）　本件は、総合評価落札方式（加算方式）により落札者を決定する。よって、本入札説明書における要求要件をすべて満たし、独立行政法人統計センター会計規程第 43 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、且つ、別記「総合評価の方法」によって得られた数値の最も高い数値をもって有効な入札を行った入札者を落札者とする。ただし、落札者となるべき者の入札価格によっては、その者により当該契約の内容に適合した履行がな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は、入札結果を保留とする。この場合、入札参加者は当センターの行う事前聴取等の調査に協力しなければならない。また、調査の結果、上記のただし書きに該当すると認められるときは、予定価格の制限の範囲内で次順位の者を落札者とする。

別記「総合評価の方法」

１　総合評価の得点（以下、「総合評価点」という。）は、入札者の入札価格の得点（以下、「価格点」という。）に、当該入札者の申し込みに係る提案書の各評価項目の得点の合計（以下、「技術点」という。）を加算した数値とする。

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

※価格点が０未満の場合は、技術点の高低に関わらず、落札する資格を有しない。（入札金額が予定価格を上回る場合は、落札者となり得ない。）

３　価格点及び技術点の得点配分は、「提案依頼書」のとおり。

（参考１　価格点の算出方法）

$$\left[1 - \frac{\text{入札価格}}{\text{予定価格}}\right] \times \text{入札価格に対する得点配分}$$

（参考２　総合評価点の算出方法）

$$\text{総合評価点} = \text{価格点} + \text{技術点}$$

（２）　前号の場合において、落札者となるべき総合評価点の最も高い者が２者以上あるときは、技術点が最も高い者を落札者とし、技術点も同じ場合は、直ちに当該入札をした者にくじを引かせて落札者を決定する。

（３）　前号の場合において、当該入札者のうちくじを引かない者又は出席しない者があるときは、これに代わって入札執行事務に関係のない職員にくじを引かせて落札者を決定する。

13　契約書作成の要否及び契約条項

（１）　契約締結に当たっては、本入札説明書に添付する別紙様式第５号契約書（案）に基づく契約書を作成するものとする。

（２） 契約の相手方が遠隔地にあるときは、まず、その者が契約書に記名押印し、更に契約担当者がその当該契約書の送付を受けてこれに記名押印するものとする。

（３） （２）の場合において契約担当者が記名押印したときは、当該契約書の１通を契約の相手方に送付するものとする。

（４） 契約担当者が契約の相手方とともに契約書に記名押印しなければ、本契約は確定しないものとする。

（５） 契約金額は、入札書に記載された書面上の金額の 100 分の 110 に相当する額とする。

（６） 契約金額にかかる支払内訳に関しては、別紙様式第５号契約書（案）に基づき契約書を作成するものとし、設計・構築経費については分割し、運用・保守経費等と合わせて支払うこととする。なお、分割した設計・構築経費については落札後、独立行政法人統計センターと落札者にて協議のうえ、支払い時期を変更する場合がある。

14 **その他**

（１） 契約に要する費用は、すべて落札者の負担とする。

（２） 入札参加者は、入札説明書、仕様書、契約書(案)を熟読し、内容を理解、遵守すること。

（３） 入札参加予定者は、社名及び代表者氏名並びに本件責任者及び担当者の役職、氏名及び連絡先（但し、代表者印を押印している場合は不要とする）を記載した下見積書（概算見積）を令和６年２月 15 日午後２時までに下記 15(２)宛に提出すること。(ｅメール等による送付可)

15 **問い合わせ先**

（１）仕様書及び提案書作成に関する問い合わせ先

独立行政法人統計センター情報システム部
情報システム基盤課基盤企画係　鈴木　惣太郎
〒162-8668 東京都新宿区若松町 19 番１号
電　話　　03-5273-1268
ＦＡＸ　　03-5273-1222
Ｅ-Mail　s-systemkikaku_atmark_nstac.go.jp
※「_atmark_」を「@」に置き換えて送信すること。

（２）契約手続に関する問い合わせ先

独立行政法人統計センター総務部財務課調達係　谷山　仁志
独立行政法人統計センター総務部財務課調達係　緑川　颯人
〒162-8668 東京都新宿区若松町 19 番１号
電　話　03-5273-1219
ＦＡＸ　03-5273-1229
Ｅ-Mail d-choutatsu_atmark_nstac.go.jp
※「_atmark_」を「@」に置き換えて送信すること。
問い合わせは、必ず書面（ファクシミリでも可）又はｅメールで行うこと。
問い合わせ期間　令和６年２月 22 日まで

（別紙様式第１号　入札書）

入　札　書

件名　独立行政法人統計センター情報システム基盤の構築及びサービス提供業務

上記について、入札公告及び入札説明書承諾のうえ入札します。

（金額）

円

（金額は右づめで記載し、左端は￥で締めること）

令和６年　月　日
（日付は、提出日を記載すること）
契約担当役
独立行政法人統計センター
理 事 長　佐伯　修司　殿

住　　所
商号又は名称
代表者（役職及び氏名）
（代理人氏名）
本件責任者（役職及び氏名）
担当者（役職及び氏名）
電話番号
Mail

＜注意＞

１．提出年月日は、必ず記入のこと。
２．金額の訂正は、認めない。
３．開札時における再度入札を考慮して入札書は余分に用意すること。
４．（　）内は、代理人が入札するときに使用すること。
５．用紙の大きさは、Ａ列４（縦）とする。
６．押印は不要であるが、応札事業者の方針として押印を必要とする場合は、この限りではない。

（別紙様式第２号　委任状）

委 任 状

私は、（ *代理人氏名* ）を代理人と定め、契約担当役独立行政法人統計センター理事長の発注する「独立行政法人統計センター情報システム基盤の構築及びサービス提供業務」に関し、下記の権限を委任します。

記

入札及び見積りに関する一切の権限

代理人使用印鑑
（応札事業者が押印を必要とする場合のみ使用すること。）

令和６年　月　日
（日付は、提出日を記載すること）

契約担当役
独立行政法人統計センター
理　事　長　　佐伯　修司　殿

住　　所
商号又は名称
代表者（役職及び氏名）
本件責任者（役職及び氏名）
担当者（役職及び氏名）
電話番号
Mail

＜注意＞

１．　提出年月日は、必ず記入のこと。

２．　用紙の大きさは、Ａ列４（縦）とする。

３．　押印は不要であるが、応札事業者の方針として押印を必要とする場合は、この限りではない。

（別紙様式第３号　提案書）

令和６年　月　日
（日付は、提出日を記載すること）

提　案　書

契約担当役
独立行政法人統計センター
理　事　長　　佐伯　修司 殿

住　　所
商号又は名称
代表者（役職及び氏名）
本件責任者（役職及び氏名）
担当者（役職及び氏名）
電話番号
Mail

入札説明書７について、下記のとおり提案します。

記

「提案依頼書」に基づく書類。

＜注意＞
１．提出年月日は、必ず記入のこと。
２．用紙の大きさは、Ａ列４（縦）とする。
３．押印は不要であるが、応札事業者の方針として押印を必要とする場合は、この限りではない。

（別紙様式第４号　再委託承認申請書）

令和６年　月　日
（日付は、提出日を記載すること）

再委託承認申請書

契約担当役
独立行政法人統計センター
理　事　長　　佐伯　修司 殿

住　　所
商号又は名称
代表者（役職及び氏名）
本件責任者（役職及び氏名）
担当者（役職及び氏名）
電話番号
Mail

契約担当役独立行政法人統計センター理事長の発注する「独立行政法人統計センター情報システム基盤の構築及びサービス提供業務」を落札した場合、他業者へ一部の業務を委託したいので、下記のとおり申請します。

１.契 約 案 件 名	独立行政法人統計センター情報システム基盤の構築及びサービス提供業務
２．委　託　先　名	住所： 名称（会社名）: 代表者（役職名及び氏名）:
３．委託内容(委託範囲)	
４．委　託　金　額	入札書の内訳書に記載
５．委託理由(合理的理由)	
６．業務の実施体制及び管理体制	
７．そ　　の　　他	

＜注意＞
１．提出年月日は、必ず記入のこと。
２．用紙の大きさは、Ａ列４（縦）とする。
３．押印は不要であるが、応札事業者の方針として押印を必要とする場合は、この限りではない。
４．再委託先を複数予定している場合、１～７の内容を記載した一覧表を別添として添付することも可能とする。

（別紙様式第５号　契約書（案））

請　負　契　約　書

契約件名：独立行政法人統計センター情報システム基盤の構築及びサービス提供業務
契約金額：　　円（消費税額及び地方消費税額：　　円）

上記契約を履行するにつき、契約担当役独立行政法人統計センター理事長佐伯修司を甲とし、＜落札者＞を乙として次の条項により契約を締結する。

第１章　総　則

（契約の目的）

第１条　乙は、この契約書のほか、この契約書に附属する仕様書、仕様書に添付された文書等及び入札に際し乙が提出した提案書並びにそのほかの書類で明記したすべての内容（以下「仕様書等」という。）に定める契約物品を仕様書で定める期間に、仕様書で指定する場所に設置して甲の使用に供するものとし、甲は、その代金を乙に支払うものとする。

（代金）

第２条　契約金額をもって、乙に支払われる代金の金額とする。なお、この消費税額及び地方消費税額は、消費税法（昭和 63 年法律第 108 号）第 28 条第１項及び第 29 条並びに地方税法（昭和 25 年法律第 226 号）第 72 条の 82 及び第 72 条の 83 の規定に基づき、算出した額である。

（契約期間）

第３条　契約期間は、契約締結日より令和11年３月31日とする。

（契約保証金）

第４条　甲は、この契約に係る乙が納付すべき契約保証金を免除するものとする。

（債権譲渡の禁止）

第５条　乙は、この契約によって生ずる権利の全部又は一部を甲の承諾を得ずに、第三者に譲渡し、又は承継させてはならない。ただし、信用保証協会、中小企業信用保険法施行令（昭和 25 年政令第 350 号）第１条の３に規定する金融機関、資産の流動化に関する法律（平成 10 年法律第 105 号）第２条第３項に規定する特定目的会社（以下「特定目的会社」という。）又は信託業法（平成 16 年法律第 154 号）第２条第２項に規定する信託会社（以下「信託会社」という。）に対して債権を譲渡する場合にあっては、この限りでない。

２　乙がこの契約により行うこととされた全ての給付を完了する前に、乙が前項ただし書きに基づいて、特定目的会社又は信託会社（以下「丙」という。）に債権の譲渡を行い、乙が甲に対し、民法（明治 29 年法律第 89 号）第 467 条に規定する通知を行

い、若しくは乙若しくは丙が動産及び債権の譲渡の対抗要件に関する民法の特例等に関する法律（平成 10 年法律第 104 号。以下「債権譲渡特例法」という。）第４条第２項に規定する通知を行い又は、乙若しくは丙が民法第 467 条又は債権譲渡特例法第４条第２項に規定する承諾の依頼を行う場合にあっては、甲は次の各号に掲げる事項を主張する権利を留保するものとする。

（１） 甲は、乙に対して有する請求債権については、譲渡対象債権金額と相殺し、又は、譲渡債権金額を軽減する権利を保留する。

（２） 丙は、譲渡対象債権を第一項ただし書きに掲げる者以外の者に譲渡し又はこれに質権を設定しその他債権の帰属及びに行使を害すべきことはできないこと。

（３） 甲は、債権譲渡後も、乙との協議のみにより、納地の変更、契約金額の変更その他契約内容の変更を行うことがあり、この場合、丙は異議を申し立てないものとし、当該契約の変更により、譲渡対象債権の内容に影響が及ぶ場合には、もっぱら乙と丙の間において解決されなければならないこと。

（再委託）

第６条　乙は、本契約の全部を第三者（以下「再委託者」という。）に委託することはできないものとする。ただし、本契約の適正な履行を確保するために必要な範囲において、本契約の一部を再委託する場合は、乙は、あらかじめ再委託者の住所、氏名、再委託する業務の範囲、その必要性及び契約金額について記載した書面を甲又は、甲の指定する者に提出し、甲の承認を受けなければならない。

　なお、乙は、甲から承認を受けた内容を変更しようとするとき、あるいは、再委託者が更に再委託する場合についても同様に甲の承認を受けなければならない。

２　乙は、甲の求める同水準の情報セキュリティ等を確保するための対策を再委託の相手方に行わせなければならない。なお、再委託の相手方に行わせた情報セキュリティ等の対策及び結果を甲に報告しなければならない。

３　乙は、本契約の一部を再委託するときは、再委託した業務に伴う再委託者の行為について、甲に対してすべての責任を負うものとする。

４　乙は、本契約の一部を再委託するときは、乙がこの契約を遵守するために必要な事項について本契約書を準用して、再委託者と約定しなければならない。

（代理人の届出）

第７条　乙は、本契約に基づく業務に関する事務の全部又は一部を行わせるため、代理人を選任する場合は、あらかじめ、書面により甲に届け出るものとする。

（仕様書等の疑義）

第８条　乙は、仕様書等に疑義がある場合は、速やかに甲の説明を求めるものとする。

２　乙は、前項の説明に従ったことを理由として、この契約に定める義務の履行の責めを免れない。ただし、乙がその説明の不適当なことを知って、速やかに異議を申し立てたにもかかわらず、甲が当該説明によることを求めたときは、この限りでない。

第２章　契約の履行

（監督）

第９条　甲は、この契約の適正な履行を確保するため、必要がある場合は、監督職員を定め、乙の作業場所等に派遣して業務内容及び甲が提供した資料等の保護・管理が、適正に行われているか等について、甲の定めるところにより監督をさせ、乙に対し必要な指示をすることができる。

２　甲は、監督職員を定めたとき、その職員の氏名及び権限並びに事務の範囲を乙に通知するものとする。

３　乙は、監督職員の職務の遂行につき、相当の範囲内で協力するものとする。

４　監督職員は、職務の遂行に当たり、乙が行う業務を不当に妨げないものとする。

５　監督を受けるのに必要な費用は、代金に含まれるものとする。

（履行完了の届出）

第１０条　乙は、履行を完了したときは、遅滞なく書面をもって甲に届けるものとする。この場合、成果物として仕様書等において提出が義務づけられているものは、これを添えて届け出るものとする。

（検査）

第１１条　甲又は甲が検査を行う者として定めた職員（以下「検査職員」という。）は、前条の規定により届け出を受理した日から起算して 10 日以内に、乙の立会を求めて、甲の定めるところにより検査を行い、合格又は不合格の判定をするものとする。ただし、乙が立ち会わない場合は、乙の欠席のまま検査をすることができる。

２　甲は、必要があると認めるときは、乙が履行を完了する前に、乙の作業場所又は甲の指定する場所で検査を行うことができる。

３　甲は、前２項の規定により合格又は不合格の判定をした場合は、速やかに乙に対し、その結果を通知するものとする。なお、前条の規定による届け出を受理した日から起算して 14 日以内に通知をしないときは、合格したものとみなす。

４　乙は、検査職員の職務の遂行につき、相当の範囲内で協力するものとする。

５　乙は、検査に先立ち検査職員の指示するところにより、社内検査を実施した場合は、社内検査成績書を甲に提出するものとする。

６　検査を受けるのに必要な費用は、代金に含まれるものとする。

７　甲は、前各項に定める検査に関する事務を第三者に委託することができる。この場合、甲は、適宜の方法により乙にその旨通知するものとする。

（所有権の移転）

第１２条　この契約に基づく成果物の所有権は、前条に規定する甲の検査に合格し、甲が受領したときに乙から甲に移転するものとする。

２　前項の規定により成果物の所有権が甲に移転したときに、甲は乙の責めに帰すべからざる事由による成果物の滅失、毀損等の責任を負担するものとする。

（代金の請求及び支払）

第１３条　乙は、契約の履行を完了した場合において、甲の行う検査に合格したときは、支払請求書により別紙支払金額内訳表のとおり代金を甲に請求するものとする。

２　甲は、前項に定める適法な支払請求書を受理したときは、受理した日から起算して30日（以下「約定期間」という。）以内に代金を支払うものとする。

（支払遅延利息）

第１４条　甲は、約定期間内に代金を乙に支払わない場合は、約定期間満了の日の翌日から支払をする日までの日数に応じ、未支払金額に対し、政府契約の支払遅延に対する遅延利息の率を定める告示（昭和24年大蔵省告示第991号）に基づき、算出した遅延利息を乙に支払うものとする。ただし、約定期間内に支払をしないことが天災地変等やむを得ない理由による場合は、当該理由の継続する期間は、約定期間に算入せず、又は遅延利息を支払う日数に計算しないものとする。

２　前項の規定により計算した遅延利息の額が100円未満である場合は、遅延利息を支払うことを要しないものとする。

３　甲が第11条第１項に定める期間内に合否の判定をしない場合は、その期間を経過した日から合否の判定をした日までの日数は、約定期間の日数から差し引くものとし、また、当該遅延期間が約定期間の日数を超える場合は、約定期間は満了したものとみなし、甲は、その超える日数に応じ、前２項の計算の例に準じ、第１項に定める利率をもって計算した金額を乙に対して支払うものとする。

（納入期限の猶予）

第１５条　乙は、納入期限までに義務を履行できない相当の理由があるときは、あらかじめ、その理由及び納入予定日を甲に申し出て、納入期限の猶予を書面により申請することができる。この場合において、甲は、納入期限を猶予しても、契約の目的の達成に支障がないと認めるときは、これを承認することができる。この場合、甲は原則として甲が承認した納入予定日まではこの契約を解除しないものとする。

２　乙が納入期限までに義務を履行しなかった場合、乙は、前項に定める納入期限の猶予の承認の有無にかかわらず、納入期限の翌日から起算して、契約の履行が完了した日（納入期限遅延後契約を解除したときは、解除の日。）までの日数に応じて、当該契約金額に国の債権の管理等に関する法律施行令（昭和31年政令第337号）第29条第１項本文に規定する財務大臣が決定する率を乗じた金額を甲の指定する期間内に納付しなければならない。ただし、その金額が100円未満であるときは、この限りでない。

３　前項の規定による遅滞金のほかに、第21条第１項の規定による違約金が生じたときは、乙は甲に対し当該違約金を併せて支払うものとする。

４　甲は、乙が納入期限までに義務を履行しなかったことにより生じた直接及び間接の損害（甲の支出した費用のほか、甲の人件費相当額を含む。以下同じ。）について、乙に対してその賠償を請求することができる。ただし、第21条第１項の規定による違約金が生じたときは、同条第３項の規定を適用するものとする。

第３章　契約の効力等

（履行不能等の通知）
第１６条　乙は、理由の如何を問わず、納入期限までに契約の履行を完了する見込みがなくなった場合、又は契約の履行を完了することができなくなった場合は、直ちに甲にこの旨を書面により通知するものとする。

（契約不適合による履行の追完、代金の減額及び契約の解除）
第１７条　成果物が契約の内容に適合しない場合は、甲は、自らの選択により、乙に対し、成果物の修補、代替物の引渡し又は不足分の引渡しによる履行の追完を請求することができる。ただし、甲の責めに帰すべき事由によるものであるときは履行の追完の請求をすることができない。
２　成果物が契約の内容に適合しない場合(甲の責めに帰すべき事由によるものであるときを除く。）、甲は、相当な期間を定め、履行の追完を催告できる。
３　甲が、相当の期間を定めて履行の追完を催告し、その期間内に履行の追完がないときは、甲は、その不適合の程度に応じて代金の減額を請求することができる。
４　前項の規定にかかわらず、次に掲げる場合には、甲は同項の催告をすることなく、直ちに代金の減額を請求することができる。
（１）履行の追完が不能であるとき。
（２）乙が履行の追完を拒絶する意思を明確に表示したとき。
（３）乙が履行の追完をしないで仕様書等に定める時期を経過したとき。
（４）前３号に掲げる場合のほか、甲が第２項の催告をしても履行の追完を受ける見込みがないことが明らかであるとき。
５　甲が、履行の追完を請求した場合で、履行の追完期間中成果物を使用できなかったときは、甲は、当該履行の追完期間に応じて第15条第２項の規定に準じて計算した金額を乙に対し請求することができる。
６　甲が、第２項に規定する催告をし、その期間内に履行の追完がないとき、甲は、この契約を解除することができる。ただし、その期間を経過したときにおける債務の不履行が軽微であるときは、この限りでない。
７　甲が前項に基づき解除した場合、乙は、甲に対し、第21条第１項の規定による違約金を支払うものとする。ただし、甲は返還すべき成果物が既にその用に供せられていたとしても、これにより受けた利益を返還しないものとする。
８　甲は、成果物が契約の内容に適合しないことより生じた直接及び間接の損害について、乙に対してその賠償を請求することができる。ただし、第21条第１項の規定による違約金が生じたときは、同条第３項の規定を適用するものとする。
９　第１項の規定により甲が履行の追完の請求をした場合、乙は、甲に不相当な負担を課するものでないときは、あらかじめ甲の承認を得ることで甲が請求した方法と異なる方法による履行の追完をすることができる。
10　甲が成果物が契約の内容に適合しないことを知ったときは、その不適合を知った日から 1 年以内に乙に対して通知しないときは、甲はその不適合を理由として、履行の追完の請求、代金の減額の請求、損害賠償の請求及び契約の解除をすることができない。
　ただし、乙が引渡しの時にその不適合を知り、又は重大な過失によって知らなかったときは、この限りでない。

11　第１項の規定に基づく履行の追完については、性質の許す限り、この契約の各条項を準用する。
12　第１項の規定に基づき履行の追完がされ、再度引き渡された成果物に、なお本条の規定を準用する。
13　履行の追完に必要な一切の費用は、乙の負担とする。

第４章　契約の変更等

（契約の変更）
第１８条　甲は、契約の履行が完了するまでの間において、必要がある場合は、履行期限、仕様書等の内容その他乙の義務に関し、この契約に定めるところを変更するため、乙と協議することができる。
２　前項の規定により協議が行われる場合は、乙は、見積書等甲が必要とする書類を作成し、速やかに甲に提出するものとする。
３　乙は、この契約により甲のなすべき行為が遅延した場合において、必要があるときは、履行期限等を変更するため、甲と協議することができる。

（事情の変更）
第１９条　甲及び乙は、この契約の締結後、天災地変、法令の制定又は改廃、その他の著しい事情の変更により、この契約に定めるところが不当となったと認められる場合は、この契約に定めるところを変更するため、協議することができる。
２　前条第２項の規定は、前項の規定により契約金額の変更に関して、協議を行う場合に準用する。

（甲の解除権）
第２０条　甲は、乙が次の各号の一に該当するときは、この契約の全部又は一部を解除することができる。
（１）乙が納入期限（第15条第１項により猶予を承認した場合は、その日。）までに、履行を完了しなかったとき又は完了できないことが客観的に明らかなとき。
（２）第11条第１項の規定による検査に合格しなかったとき。
（３）第17条第６項に該当するとき。
（４）前３号に定めるもののほか、乙がこの契約のいずれかの条項に違反したとき。
（５）この契約の履行に関し、乙又はその代理人、使用人に不正又は不誠実な行為があったとき。
（６）乙が、破産の宣告を受け又は乙に破産の申立て、民事再生法の申立て、会社更生手続開始の申立てがあるなど、経営状態が著しく不健全と認められるとき。
（７）乙が、制限行為能力者となり又は居所不明になったとき。
２　甲は、前項に定める場合のほか、甲の都合により必要がある場合は、この契約の全部又は一部を解除することができる。この場合において、甲は、乙と協議の上、乙に対して契約の解除前に発生した乙の損害を賠償するものとする。
（違約金）
第２１条　乙は、前条第１項の規定により、この契約の全部又は一部を甲により解除さ

れた場合は、違約金として解約部分に対する価格の100分の20に相当する金額を甲に対して支払うものとする。ただし、その金額が100円未満であるときは、この限りではない。

２　前項の規定による違約金のほかに、第15条第２項の規定による遅滞金が生じているときは、乙は甲に対し当該遅滞金を併せて支払うものとする。

３　第１項の規定は、甲に生じた直接及び間接の損害の額が、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ものとする。

（乙の解除権）

第２２条　乙は、甲がその責めに帰すべき理由により、契約上の義務に違反した場合においては、相当の期間を定めてその履行を催告し、その期間内に履行がないときは、この契約の全部又は一部を解除することができる。

２　前項の規定は、乙が乙に生じた実際の損害につき、賠償を請求することを妨げない。

３　前項の規定による損害賠償の請求は、解除の日から30日以内に書面により行うものとする。

（著作権の譲渡等）

第２３条　乙は、成果物に関し、著作権法（昭和 45 年法律第 48 号）に規定するすべての権利（同法第 27 条及び第 28 条の権利を含む。）を、甲に無償で譲渡するものとする。

２　甲は、著作権法第 20 条第２項第３号又は第４号に該当しない場合においても、その使用のために、仕様書等で指定する成果物を改変し、また、任意の著作者名で任意に公表することができるものとする。

３　乙は、本業務で生じた成果物について、甲及び甲が指定する第三者に対して著作者人格権を行使することができない。

４　前３項の規定は本業務で生じた中間成果物についても、準用するものとする。

（知的財産権等）

第２４条　乙は、成果物の利用が、第三者の著作権、特許権その他の知的財産権、営業秘密、肖像権、パブリシティー権、プライバシー権、その他の権利又は利益（以下本条において「知的財産権等」という。）を侵害していないことを保証する。

２　甲又は甲から成果物の利用を許諾された者が、成果物の利用に関連して第三者の知的財産権等を侵害した旨の申立てを受けた場合、又は第三者の知的財産権等を侵害するおそれがあると甲が判断した場合、乙は、自己の費用と責任においてこれを解決するものとする。

３　前項の場合において、乙は、甲の指示に従い、乙の費用負担において、知的財産権等の侵害のない他の成果物と交換し、成果物を変更し、又は当該第三者から成果物の継続使用・利用のための権利の取得を行わなければならない。本項の定めは、甲の乙に対する損害賠償を妨げない。

４　第２項の場合において、当該第三者からの申立てによって甲又は甲から成果物の利用を許諾された者が支払うべきとされた損害賠償額、その他当該第三者からの請求、

訴訟等によって甲に生じた一切の損害、及び申立ての対応に要した弁護士等の第三者に支払った費用その他の解決に要した費用は、乙が負担するものとする。

（支払代金の相殺）

第２５条　この契約により乙が甲に支払うべき金額があるときは、甲はこの金額と乙に支払う代金を相殺することができる。

第５章 暴力団排除特約条項

（属性要件に基づく契約解除）

第２６条　甲は、乙が次の各号の一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非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２７条　甲は、乙が自ら又は第三者を利用して次の各号の一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契約担当官等の業務を妨害する行為

（５）その他前各号に準ずる行為

（下請負契約等に関する契約解除）

第２８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、又は正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２９条　甲は、第26条、第27条及び前条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26条、第27条及び前条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３０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。

第６章 談合等特約条項

（談合等の不正行為に係る違約金）

第３１条　乙は、この契約に関し、次の各号の一に該当するときは、甲が契約の全部又は一部を解除するか否かにかかわらず、契約金額の100分の10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）この契約に関し、乙が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３条の規定に違反し、又は乙が構成事業者である事業者団体が独占禁止法第８条第１号の規定に違反したことにより、公正取引委員会が乙に対し、独占禁止法第７条の２第１項（独占禁止法第８条の３におい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。

（２）納付命令又は独占禁止法第７条若しくは第８条の２の規定に基づく排除措置命令（これらの命令が乙又は乙が構成事業者である事業者団体（以下「乙等」という。）に対して行われたときは、乙等に対する命令で確定したものをいい、乙等に対して行われていないときは、各名宛人に対する命令すべてが確定した場合における当該命令をいう。次号において「納付命令又は排除措置命令」という。）において、この契約に関し、独占禁止法第３条又は第８条第１号の規定に違反する行為の実行としての事業活動があったとされたとき。

（３）納付命令又は排除措置命令により、乙等に独占禁止法第３条又は第８条第１号の規定に違反する行為があったとされた期間及び当該違反する行為の対象となった取引分野が示された場合において、この契約が、当該期間（これらの命令に係る事件について、公正取引委員会が乙に対し納付命令を行い、これが確定したときは、当該納付命令における課徴金の計算の基礎である当該違反する行為の実行期間を除く。）に入札（見積書の提出を含む。）が行われたものであり、かつ、当該取引

分野に該当するものであるとき。
（４）　この契約に関し、乙（法人にあっては、その役員又は使用人を含む。）の刑法（明治40年法律第45号）第96条の６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号に規定する刑が確定したとき。
（５）　乙が前項の違約金を甲の指定する期間内に支払わないときは、乙は、当該期間を経過した日から支払いをする日までの日数に応じ、年３パーセントの割合で計算した額の遅延利息を甲に支払わなければならない。
２　乙は、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、前項の契約代金（契約締結後に契約代金に変更があった場合には、変更後の金額）の100分の10に相当する額のほか、契約代金の100分の10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、乙若しくは乙の代理人に対して独占禁止法第７条の２第１項及び第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又は独占禁止法第66条第４項の規定による当該納付命令の全部を取り消す審決が確定したとき。
（２）当該刑の確定において、乙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金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。

第７章 秘密の保全

（秘密の保全）
第３２条　甲及び乙は、この契約の履行に際して、知り得た相手方の秘密を第三者に漏らし、又は利用してはならない。
２　乙は、本業務に従事するすべての者に対し、秘密の保持について厳重に管理・監督しなければならない。

第８章 雑則

（調査）
第３３条　甲は、この契約に基づいて生じた損害賠償、違約金その他金銭債権の保全又はその額の算定等の適正を図るため必要がある場合は、乙に対し、その業務若しくは資産の状況に関して質問し、帳簿書類その他の物件を調査し、参考となるべき報告若しくは資料の提出を求め、又はその職員に乙の営業所、工場その他の関係場所に立ち入り、調査させることができる。
２　乙は、前項に規定する調査に協力するものとする。

（疑義等の対応）
第３４条　この契約について定めのない事項又は疑義等を生じた場合については、甲及

び乙が協議して定めるものとする。

2　この契約に関する紛争は、訴額に応じて甲の所在地の管轄地方裁判所又は簡易裁判所を第一審の専属的合意管轄裁判所とする。

この契約を証するため、この証書２通を作成し、双方記名押印の上各１通を保管する。

令和　年　月　日

甲　　東京都新宿区若松町１９－１
契約担当役
独立行政法人統計センター
理 事 長 佐伯　修司

乙 ＜落札者＞

別 紙

支払金額内訳表（令和６年度）

○設計・構築経費　（単位：円）

年　月	月　別 支払額	消費税及び 地方消費税	合計支払額 （税込）
令和６年12月分			
小　計　①			

○運用・保守経費等　（単位：円）

年　月	月　別 支払額	消費税及び 地方消費税	合計支払額 （税込）
令和７年１月分			
令和７年２月分			
令和７年３月分			
小　計　②			

別 紙

支払金額内訳表（令和７年度）

○設計・構築経費　（単位：円）

年　月	月　別 支払額	消費税及び 地方消費税	合計支払額 （税込）
令和７年４月分			
小　計　③			

○運用・保守経費等　（単位：円）

年　月	月　別 支払額	消費税及び 地方消費税	合計支払額 （税込）
令和７年４月分			
令和７年５月分			
令和７年６月分			
令和７年７月分			
令和７年８月分			
令和７年９月分			
令和７年10月分			
令和７年11月分			
令和７年12月分			
令和８年１月分			
令和８年２月分			
令和８年３月分			
小　計　④			

別 紙

支払金額内訳表（令和８年度）

○設計・構築経費　　（単位：円）

年　月	月　別 支払額	消費税及び 地方消費税	合計支払額 （税込）
令和８年４月分			
小　計　⑤			

○運用・保守経費等　　（単位：円）

年　月	月　別 支払額	消費税及び 地方消費税	合計支払額 （税込）
令和８年４月分			
令和８年５月分			
令和８年６月分			
令和８年７月分			
令和８年８月分			
令和８年９月分			
令和８年10月分			
令和８年11月分			
令和８年12月分			
令和９年１月分			
令和９年２月分			
令和９年３月分			
小　計　⑥			

別 紙

支払金額内訳表（令和９年度）

○設計・構築経費　　（単位：円）

年　月	月　別 支払額	消費税及び 地方消費税	合計支払額 （税込）
令和９年４月分			
小　計　⑦			

○運用・保守経費等　　（単位：円）

年　月	月　別 支払額	消費税及び 地方消費税	合計支払額 （税込）
令和９年４月分			
令和９年５月分			
令和９年６月分			
令和９年７月分			
令和９年８月分			
令和９年９月分			
令和９年10月分			
令和９年11月分			
令和９年12月分			
令和10年１月分			
令和10年２月分			
令和10年３月分			
小　計　⑧			

別 紙

支払金額内訳表（令和 10 年度）

○設計・構築経費　（単位：円）

年　月	月　別 支払額	消費税及び 地方消費税	合計支払額 （税込）
令和10年４月分			
小　計　⑨			

○運用・保守経費等　（単位：円）

年　月	月　別 支払額	消費税及び 地方消費税	合計支払額 （税込）
令和10年４月分			
令和10年５月分			
令和10年６月分			
令和10年７月分			
令和10年８月分			
令和10年９月分			
令和10年10月分			
令和10年11月分			
令和10年12月分			
小　計　⑩			

○調達機器の撤去経費　（単位：円）

年　月	月　別 支払額	消費税及び 地方消費税	合計支払額 （税込）
令和11年３月分			
小　計　⑪			

（単位：円）

年　月	月　別 支払額	消費税及び 地方消費税	合計支払額 （税込）
合　計①～⑪			

（別紙様式第６号　下見積書）

令和　　年　　月　　日

下見積書（内訳）

独立行政法人
統計センター　御中

住所
会社名
代表者（役職及び氏名）
本件責任者（役職及び氏名）
担当者（役職及び氏名）
電話番号
Mail

金　　円（税込）

件　名	独立行政法人統計センター情報システム基盤の構築及びサービス提供業務

（内訳）

1　機器調達費用									
①基本金額						一式			円
②その他経費						一式			円
	単価		工数		月数				
2　設計・構築、システム移行									
(1)基盤環境の設計・構築									
①　PM人件費	円	×	人日	×		ヵ月	＝		円
②　上級SE人件費	円	×	人日	×		ヵ月	＝		円
③　一般SE人件費	円	×	人日	×		ヵ月	＝		円
(2)テスト									
①　PM人件費	円	×	人日	×		ヵ月	＝		円
②　上級SE人件費	円	×	人日	×		ヵ月	＝		円
③　一般SE人件費	円	×	人日	×		ヵ月	＝		円
(3)移行									
①　PM人件費	円	×	人日	×		ヵ月	＝		円
②　上級SE人件費	円	×	人日	×		ヵ月	＝		円
③　一般SE人件費	円	×	人日	×		ヵ月	＝		円
(4)教育									
①　PM人件費	円	×	人日	×		ヵ月	＝		円
②　上級SE人件費	円	×	人日	×		ヵ月	＝		円
③　一般SE人件費	円	×	人日	×		ヵ月	＝		円
	単価		工数		月数				
3　保守・運用									
①　PM人件費	円	×	人日	×	60	ヵ月	＝		円
②　上級SE人件費	円	×	人日	×	60	ヵ月	＝		円
③　一般SE人件費	円	×	人日	×	60	ヵ月	＝		円
4　機器の撤去									
						一式			円
5　小計							＝		**0 円**
6　消費税及び地方消費税			（ 10% ）				＝		**0 円**
7　合計							＝		**0 円**

※工数は人/日で記載してください。
※朱書き箇所は適宜入力及び削除を行ってください。
※人件費単価については、人件費単価が複数存在する場合は経費の名称を記載いただくとともに、
　技術者等の職種（PM、SE、PG等）を明記ください。

別添１

【電子メールによる入札手続について】

１ 電子メールで入札に参加を希望する者の入札書等の提出方法

入札説明書７「提案書の作成等」及び８「入札方法」に記載の書類の提出について、持参、郵送の他、電子メールによる PDF ファイルでの送付も可とします。

つきましては、電子メールによる PDF ファイルで入札関係書類を提出する場合は、以下のとおり提出をお願いします。

なお、電子メールで入札に参加する場合は、提案書提出期限の１日前までにその旨を連絡するとともに、各書類の提出（送付）にあたっては、メール送付後に受信（書類到着）の確認を電話にて必ず行ってください。

(1)提案書等

ア　入札説明書に記載された証明書類について、電子データ化（ＰＤＦ）し、ZIP 形式でパスワード付きで圧縮し（容量は、１メールあたり最大２MB 程度）、添付ファイルとして、３「入札書等の送付先」に指定するあて先に、提案書提出期限までに送付ください。

イ　電子データ（ＰＤＦ）は、「Adobe Acrobat（Reader 及び Standard）」により内容が確認できるものとしてください。

ウ　添付ファイルの解凍パスワード相違等により、解凍できない場合は、連絡させて頂きますので、入札説明書に記載の提出期限までに再送をお願いすることがあります。

同期限までに再送が間に合わない場合は、入札参加を認めないものとします。
上記を踏まえ、メールで提出する場合は早めの送付をお願いします。

(2)入札書

ア　入札書について、電子データ化（ＰＤＦ化、ZIP 形式、パスワード付き圧縮）し、添付ファイルとして、３「入札書等の送付先」に指定するあて先に、入札書提出期限までに送付ください。

入札書のパスワードについては、開札時間の１時間前必着で送付ください。

イ　電子データ（ＰＤＦ）は、「Adobe Acrobat Reader（Reader 及び Standard）」により内容が確認できるものとしてください。

ウ　入札書の電子メール送付にあたっては、送付する電子メールの「件名」に

「【３月 29 日開札】「独立行政法人統計センター情報システム基盤の構築及びサービス提供業務」（１回目）」

と記載し、初度入札で使用する入札書の送付の場合は（１回目）と記載して、期限までに送付してください。

２ 開札方法

開札時刻の経過後、送付されたパスワードを使用し、入札書を確認します。パスワードの送付漏れ、解凍パスワード相違等により提出された入札書の内容確認ができない場合、入札を辞退したものといたします。

開札時刻が経過するまで、パスワードを使用しませんので、パスワード誤り等に十分にご注意ください。

また、統計センターの予定価格内での応札がなかった場合は直ちに再度入札を行います。その際、電話にて現時点での最低価格の連絡を行いますので、速やかに２回目の入札書を準備の上、パスワードを設定のうえ、入札書の送付をお願いいたします。なお、パスワードについては、入札書の送付とは別に送付願います。

※開札時は予定価格の範囲内での応札がなかった場合に備え、待機願います。

３　入札書等の送付先

独立行政法人統計センター総務部財務課調達係

E-Mail　nstac-nyuusatu_atmark_nstac.go.jp

※「_atmark_」を「@」に置き換えて送信してください。

４　その他

添付ファイルの容量超過等により、送付メールが不着や遅延となる場合などが想定されます。いかなる場合においても期限までの送付が間に合わない場合は、入札の参加は認められません。

独立行政法人統計センター
情報システム基盤の構築
及びサービス提供業務
調達仕様書

令和 5 年 12 月 8 日

独立行政法人　統計センター

目次

1. 用語の定義

本仕様書（「13. 附属文書」に示す資料を含む。）において使用する用語の定義を「表 1 用語の定義一覧」に示す。

表 1 用語の定義一覧

No.	用語	定義
1	OCR システム	独立行政法人統計センターに設置されている調査票等の入力に用いる光学式文字読取装置及びその周辺機器。
2	SLA	サービスレベル合意書（Service Level Agreement）の略称。サービス提供者とサービス利用者の間で結ばれるサービスのレベル（定義、範囲、内容、達成目標等）に関する合意書。
3	請負者	独立行政法人統計センター情報システム基盤の構築及びサービス提供業務を請け負った事業者。
4	電磁的記録媒体	電磁的手段で情報を記録する媒体の総称。HDD、SSD、USB メモリ、CD-R 等を含む。
5	外部電磁的記録媒体	端末に USB 等で接続し、切り離し可能な電磁記録媒体の総称。
6	関係システム	次期情報システム基盤上で稼働するシステム及び次期情報システム基盤と外部接続するシステム。
7	関係事業者	関係システムの運用事業者。
8	監視カメラシステム	監視カメラ等による、一部の限られた者以外の者の立ち入りを制限する必要がある区域への入退室の記録及びアクセス管理を行うためのシステム。
9	現行運用事業者	現行の情報システム基盤の運用事業者。
10	現行情報システム基盤	令和元年度に構築した情報システム基盤。
11	現行保守事業者	現行情報システム基盤の保守を行う事業者。
12	次期情報システム基盤	令和 6 年度に構築する情報システム基盤。
13	主管課	独立行政法人統計センター情報システム部情報システム基盤課。

No.	用語	定義
14	情報セキュリティ監査事業者	独立行政法人統計センター情報システム基盤の情報セキュリティ監査業務を請け負った事業者。
15	統一基準群	政府機関等の情報セキュリティ対策のための統一基準群。令和5年7月4日　内閣官房内閣サイバーセキュリティセンター決定。
16	政府共通ネットワーク	総務省が管理する各府省のLANシステム、政府共通プラットフォーム等を相互に接続する政府内専用のネットワーク。
17	政府統計共同利用システム	各府省の統計関係システムを集約し、政府全体で利用するシステムの総称。独立行政法人統計センターにて、運用管理を行っている。オンサイト利用システムを含む。
18	次期設計・構築担当者	請負者のうち、次期情報システム基盤の設計・構築業務を担当する者。
19	次期運用担当者	請負者のうち、次期情報システム基盤の運用業務を担当する者。
20	調達機器	本調達で導入するハードウェア、ソフトウェア及び通信回線並びに統計センターが用意する機器（「要件定義書-表 5　統計センターが用意する機器」に示す。）の総称。
21	統計センター	独立行政法人統計センター。
22	統計データ利活用センター	和歌山県和歌山市東蔵前丁3-17南海和歌山市駅ビルに位置する独立行政法人統計センターの1拠点。
23	統計局システム	センサスマッピングシステム等、総務省統計局が管理・運用するシステムで、統計センターの情報システム基盤から統計局接続用FWを介して接続して利用するシステム。
24	標準ガイドライン	デジタル・ガバメント推進標準ガイドライン。令和5年3月31日 デジタル社会推進会議幹事会決定。
25	複合機事業者	独立行政法人統計センター情報システム基盤複合機及びプリンタ賃貸借を請け負った事業者。
26	要件定義書	独立行政法人統計センター情報システム基盤の構築及びサービス提供業務に係る要件定義

No.	用語	定義
		書。本調達仕様書の別添 1。
27	次期保守担当者	請負者のうち、次期情報システム基盤の保守業務を担当する者。
28	本業務	独立行政法人統計センター情報システム基盤の構築及びサービス提供業務。
29	本調達で導入する PC	「要件定義書-11.2.4①運用管理用 PC」、「要件定義書-11.3.3①ノート型 PC1」、「要件定義書-11.3.3②ノート型 PC2」、「要件定義書-11.3.3③ノート型 PC3」、「要件定義書-11.3.3④ノート型 PC4」、「要件定義書-11.3.3⑤ノート型 PC5」、「要件定義書-11.3.3⑥ノート型 PC6」及び「要件定義書-11.4.4①運用管理用 PC」の総称。
30	主管課が別途契約するセキュリティ監視	主管課が別途契約する、外部機関からのセンサーによるセキュリティ監視。
31	室内 LAN 管理担当者	統計センターの各課室ので、情報システム基盤に関する管理作業の役割を受け待つ担当者。
32	LAN 運用係	主管課において、情報システム基盤における運用作業を受け持つ係。

2. 調達の概要に関する事項

2.1 調達件名

独立行政法人統計センター情報システム基盤の構築及びサービス提供業務

2.2 調達の目的

統計センターでは、国の政策の立案及び遂行を行うための基礎資料となる、国勢調査、労働力調査、消費者物価指数等の各種統計の作成及びこれらに必要な統計技術の研究等の業務を行っている。

本調達においては、上記業務を遂行するために必要となる次期情報システム基盤の構築及びクラウドサービスを含む機能提供を行うとともに、令和5年に改定された「統一基準群」への対応を含むセキュリティ対策の強化を目的としている。当該目的を遂行するために各種機器、各種機器を設置するデータセンターのハウジングサービス、通信回線及びこれらに付帯する運用・保守等業務が含まれる。

2.3 調達の概要

2.3.1 調達範囲

① 本業務の範囲を以下に示す。なお、「要件定義書-表5　統計センターが用意する機器」に示す統計センターが用意する機器についても、主管課の指示に従い設定及び設置作業を行うこと。また、本調達の対象範囲を下記「図 1　本調達範囲」に示す。合わせて、本仕様書に定める設計・構築及び賃貸借保守並びに撤去等に係る一切の費用を含むものとする。

（ア）調達機器（統計センターが用意する機器を除く。）、データセンターのハウジングサービス及びクラウドサービスの提供

（イ）基盤環境の設計・構築（運用設計を含む。）

（ウ）調達機器の搬入、設置及び調整

（エ）テスト

（オ）移行

（カ）教育

（キ）保守（リモート監視を含む。）

（ク）運用（サービスデスク業務、ホームページ基盤の運用を含む。）

（ケ）各申請手続き（ユーザのソフトウェア利用申請、ドメインの引継ぎ　等）

（コ）調達機器の撤去

図 1　本調達範囲

② 調達機器（統計センターが用意する機器を除く。）、利用するクラウドサービス及びデータセンターの賃貸借保守は、本仕様書に明示する機能、性能及びその他の条件等を充足するものであること。

③ 調達機器については、納品にあたり必要な作業等を行った後、次期情報システム基盤について総合的な稼動テストを行い、正常稼働を確認すること。

④ 本仕様書に明示されていない物品及び役務であっても、本調達仕様書に記載の機能を実現するために必要なものがある場合には、請負者の負担で用

意すること。

2.3.2　次期情報システム基盤の概要

①　提供する機能

次期情報システム基盤において提供する機能を下記「表 2　提供機能一覧」に示す。

表 2　提供機能一覧

No.	大項目	小項目
ユーザ提供機能		
1	メール	メール
2		メール無害化及び誤送信防止
3	スケジュール管理	-
4	仮想 PC 及びアプリケーション配信	仮想 PC 管理
5		アプリケーション配信 1
6		アプリケーション配信 2
7	テレワーク	仮想 PC 接続
8	リモートアクセス	-
9	Web 会議	統計センター外部向け Web 会議
10	在席管理及び Web 会議	在席管理
11		統計センター内部向け Web 会議
12	ファイル共有	ファイル保管機能
13		アクセス権管理機能
14		使用容量制限機能
15		ファイル復旧機能
16		検索機能
17	会議室予約	-
18	ファイル転送	インターネットを介したファイル転送
19		政府共通 NW を介したファイル転送
20	申請のオンライン受付及び各種運用手続きのワークフロー管理	-
システム運用機能		
21	仮想化基盤管理	-
22	構成管理	-
23	ログ取得・管理	統合ログ取得
24		ログ保管
25	監視	ネットワーク及び Linux サーバ監視

No.	大項目	小項目
26		Microsoft Windows Server 及び Microsoft365 クラウドサービス監視
27	バックアップ	データセンター内のデータのバックアップ
28		クラウドサービス上のデータのバックアップ
29	特権 ID 管理	特権 ID 管理
30		特権 ID 不正利用検知
31		Active Directory 監査
32	アカウント管理	-
33	シングルサインオン	-
34	DNS	内部 DNS
35		コンテンツ DNS
36		キャッシュ DNS
37	DHCP	-
38	認証局	-
39	システム管理	-
情報セキュリティ機能		
40	主体認証	ディレクトリ
41		IC カード認証
42		ワンタイムパスワードトークン認証
43	仮想ブラウザ	-
44	ファイル転送及びファイル無害化	ファイル無害化
45		ファイル転送
46	エンドポイントマルウェア対策	-
47	ファイアウォール	ファイアウォール
48	不正プロセス検知	端末操作ログ取得
49		不正プロセス検知
50		ブラウザの閲覧履歴取得
51	ソフトウェアアップデート	Microsoft Windows Server に対するソフトウェアアップデート
52		Linux サーバに対するソフトウェアアップデート
53	メールセキュリティ対策	メールセキュリティ対策
54		サンドボックス
55	Web セキュリティ対策	セキュアWebゲートウェイ(SWG)

No.	大項目	小項目
56		クラウドアクセスセキュリティ（CASB）
57		サンドボックス
58		不正侵入防止
59	脆弱性検査ツール	－

② ネットワーク構成案及びシステム構成案

（ア）ネットワーク構成案及びシステム構成案を以下に示す。

(1) 要件定義書-11.1 ネットワーク構成要件

(2) 別添 2 次期情報システム基盤概要構成図

③ 外部との接続

（ア）次期情報システム基盤と外部接続するシステムを以下に示す。

(1) OCR システム

(2) 政府共通ネットワーク

(3) 政府統計共同利用システム

(4) 統計局システム

(5) 監視カメラシステム

2.3.3 契約期間

① 契約期間は契約締結日から調達機器の撤去完了までとする（うち次期情報システム基盤の稼働期間は、令和7年1月1日（水）から令和11年12月31日（月）までとする。）。なお、改元が実施された場合は、新元号に読み替えるものとする。（以下同様とする。）

② 調達機器（統計センターが用意する機器を除く。）の納品期限は、令和6年12月31日（火）までとする。

2.3.4 作業スケジュール

① 本業務で遵守すべき主なスケジュールを下記「図 2 構築スケジュール（案）」及び下記「表 3 マイルストーン（案）」に示す。なお、提案時に本業務を円滑に実施するために最適と考えるより詳細なスケジュール（案）を提案すること。また、受注後主管課に承認を得ること。

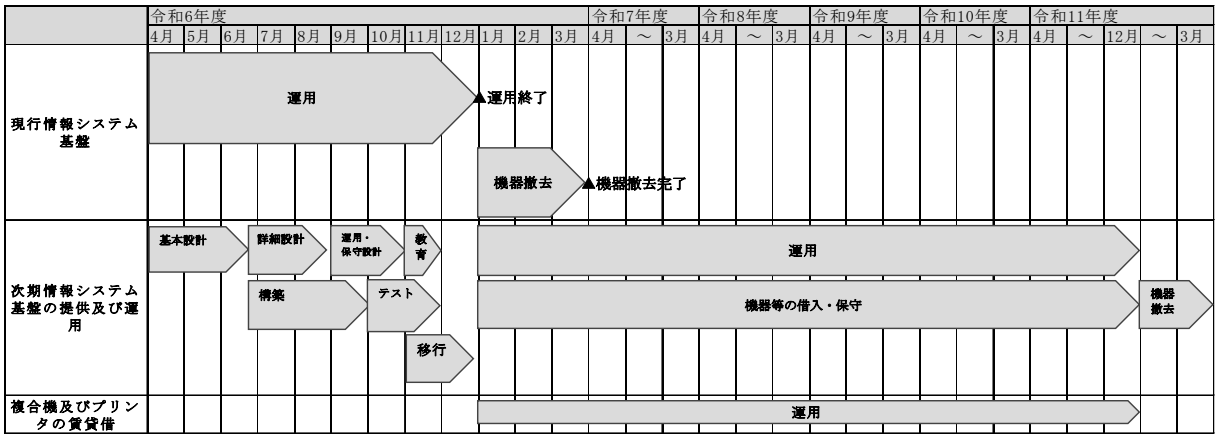


図 2　構築スケジュール（案）

表 3　マイルストーン（案）

No.	マイルストーン	日付
1	基本設計完了	全体作業計画書で定義 （令和 6 年 6 月を想定）
2	詳細設計完了	全体作業計画書で定義 （令和 6 年 8 月を想定）
3	運用・保守設計完了	全体作業計画書で定義 （令和 6 年 10 月を想定）
4	設計・構築完了	令和 6 年 10 月 31 日
5	システム移行完了	令和 6 年 12 月 31 日
6	運用・保守開始	令和 7 年 1 月 1 日
7	運用・保守終了	令和 11 年 12 月 31 日
8	調達機器撤去	令和 12 年 1 月 1 日から令和 12 年 3 月 31 日まで

3.　調達案件及び関連調達案件の調達単位、調達方式等に関する事項

3.1　調達案件、調達方式及び実施時期

① 関連する調達案件名、調達方式及び実施時期を下記「表 4　調達案件、調達方式及び実施時期」に示す。なお、テスト、移行、引継ぎ及び障害対応等、必要に応じて、各調達案件を請け負う事業者と連携すること。

表 4　調達案件、調達方式及び実施時期

調達案件名	調達の方式	実施時期
独立行政法人統計センター情報セキュリティ監査	総合評価落札方式	入札公告・官報公示：令和 6 年 6 月頃 落札者決定　　：令和 6 年 9 月頃

調達案件名	調達の方式	実施時期
独立行政法人統計センター情報システム基盤の複合機の提供業務	最低価格落札方式	入札公告・官報公示：令和 6 年 7 月頃 落札者決定　　：令和 6 年 10 月頃

4.　作業の実施内容に関する事項

4.1　全体作業管理

4.1.1　全体作業計画書の作成

① 契約締結後2週間以内に作業体制、導入スケジュール等を示した「全体作業計画書」を作成し、主管課の承認を得ること。

4.1.2　進捗管理

① 「全体作業計画書」作成時に定義したスケジュールに基づく進捗管理を行うこと。

② 次期情報システム基盤構築にあたりプロジェクト管理の国際標準である PMBOK（Project Management Body of Knowledge）の体系に準じ、WBS（Work Breakdown Structure）を用いること。

③ 進捗及び進捗管理に是正の必要がある場合、その原因及び対応策を明らかにし、速やかに是正計画を策定し、主管課の承認を得ること。

4.1.3　変更管理

① 設計完了後に設計内容に変更が生じた場合、設計変更に伴う影響範囲を特定した上で定例会議において主管課と協議の上、適切な対応策を確定し、行うこと。また、対応策の実施状況を確認し、主管課に報告すること。

4.1.4　課題管理

① 本業務の実施を妨げる要因となる課題を把握・分析し、適切な対策を立案・実施すること。また、対応策の実施状況を確認し、主管課に報告すること。

4.1.5　リスク管理

① リスク発生・消滅時期を適切に管理すること。また、リスクが想定された時点で、事前にリスク発生時の対応策を十分に検討すること。

② リスクが顕在化した場合は速やかに主管課に連絡の上、リスク発生時の対応策を実施し、その結果を主管課に報告すること。

4.1.6　会議

① 次期情報システム基盤の稼働開始までは、原則、週1回の定例会議を開催し、全体の進捗状況、課題解決状況、作業の進行に影響を及ぼす課題、問題、リスク等を報告すること。
② 次期情報システム基盤の稼働開始後は、原則、月1回定例会議を開催し、障害対応状況、課題解決状況、課題、問題、リスク等を報告すること。ただし、作業の進行に影響を及ぼす課題、問題、リスク等は、都度、報告を実施すること。
③ 上記①及び上記②に限らず作業の進捗状況等により必要に応じて会議を開催すること。
④ 開催する会議で協議または報告する事項については、全て資料を作成し論理的かつ効率的に行うこと。
⑤ その他必要な会議については、主管課と協議の上、設置すること。
⑥ 定例会議等を開催した場合は、3営業日以内に議事録を作成及び提出し、主管課の承認を得ること。

4.2 設計・構築に係る作業

4.2.1 設計

① 設計概要

（ア）主管課及び関係事業者と連携し、関係システムを考慮した設計・構築を行うとともに、運用段階の作業等を取りまとめた運用設計を行うこと。
（イ）各種設計書は主管課、次期運用担当者等が次期情報システム基盤を理解するにあたり必要な内容が網羅されており、実態に即した内容とすること。
（ウ）各種設計書には、少なくとも以下の内容を記載すること。なお、各種設計書の内容及び構成は、設計書作成前に主管課と協議の上、決定すること。また、各種設計書の内容及び構成を提案すること。
(1) 利用用途・目的（設計方針）
(2) 利用範囲
(3) 製品情報
(4) システム・機能構成
(5) 次期情報システム基盤で提供する機能
(6) 連携する機器・機能等
(7) 特記事項・制約事項　等
（エ）各調達機器で必要となる電源を明確にすること。
（オ）サーバ、ネットワーク機器、バックアップ機器等は、施錠可能な19インチラックに収容すること。なお、ラックは各データセンターが提供するものでも可とする。また、ラックに収容できない機器についても、19インチラック設置スペースと同等な省スペース設計とし、第三者がアクセスすることができないように措置を行うこと。

（カ）設計・構築の対象は、調達機器及び利用するクラウドサービスとすること。
（キ）ソフトウェアのバージョンの確定は、緊急性の高いバージョンのリリースがあった場合を除き、原則として詳細設計前とする。なお、緊急性の高いバージョンのリリースがあった場合、主管課と協議の上、ソフトウェアのバージョンを確定すること。
（ク）利用するクラウドサービスの確定は、原則として詳細設計前とする。なお、確定のリリースによりシステムの設計・構築に大きな影響がある場合、主管課と協議の上、利用するクラウドサービスや利用方法の見直しを行うこと。

②　基本設計
（ア）「要件定義書」及び「提案書」に基づき、調達機器で実現する機能、設備等を設計し、「基本設計書」として取りまとめ、主管課の承認を得ること。

③　詳細設計
（ア）「基本設計書」に基づき、調達機器に対する詳細設計を行い「詳細設計書」として取りまとめ、主管課の承認を得ること。

④　運用設計
（ア）運用設計にあたり、統計センターで作成した「運用管理規則」を参考に、「標準ガイドライン」に基づき、「運用計画書」を作成し、主管課の承認を得ること。
（イ）請負者は、「全体作業計画書」で定義（令和6年10月を想定）する期日までに運用設計を完了すること。なお、「運用設計書」は、期日に余裕を持って主管課に提出し承認を得ること。また、提出後のシステム移行期間中に改訂が必要となった場合、対応の上、納品期限までに提出すること。
（ウ）「運用設計書」に基づき、移行期間前までに調達機器及び統計センターが用意する機器の設定を行うこと。

⑤　保守設計
（ア）保守設計にあたり、統計センターで作成した「運用管理規則」を参考に、「標準ガイドライン」に基づき、「保守計画書」を作成し、主管課の承認を得ること。
（イ）請負者は、「全体作業計画書」で定義（令和6年10月を想定）する期日までに保守設計を完了すること。なお、「保守設計書」は、期日に余裕を持って主管課に提出し承認を得ること。また、提出後のシステム移行期間

中に改訂が必要となった場合、対応の上、納品期限までに提出すること。

4.2.2　構築

①　現地調査

（ア）構築にあたり現地調査が必要な場合、事前に主管課の承認を得た上で行うこと。

（イ）無線LANアクセスポイントを設置する際は、サイトサーベイを実施した上で、最適な無線LANアクセスポイントの配置を検討すること。

②　機器の設置・設定

（ア）調達機器の設置及び接続を行うこと。また、調達機器を搭載するラックは、転倒しないよう転倒防止措置を施すこと。

（イ）調達機器は、納品場所であるメインデータセンター内、バックアップデータセンター内、統計センター内及び統計データ利活用センター内に設置するものとし、詳細は、主管課が別途指示する。

（ウ）統計センターが用意する機器について、「要件定義書-表5　統計センターが用意する機器」を確認し、必要な設定作業を行うこと。

（エ）調達機器は、新規に敷設するケーブル（電源ケーブル及びネットワークケーブル）に接続すること。

（オ）調達機器の電源ケーブル及びネットワークケーブルには、機器が分かるようタグを付与すること。

（カ）統計センター及び統計データ利活用センターに設置する調達機器は、主管課の指示によりOS及びソフトウェアがインストールされた状態且つ必要な設定がされた状態で搬入し、正常に動作可能な状態に調整した上で納品すること。

（キ）設置・設定においては、現行情報システム基盤のユーザが実施する業務に支障をきたさないよう十分注意すること。

（ク）全てのOS及びソフトウェア、利用するクラウドサービスについて、ユーザ登録を代行すること。

（ケ）調達機器への設定等において、本調達以外の機器への接続及びソフトウェアのインストールを行う必要がある場合、事前に主管課へ報告・説明を行い、承認を受けた上で請負者が接続及びインストールを実施すること。

（コ）統計センター及び統計データ利活用センター執務室内にて作業を行う場合、主管課の許可を得ること。

（サ）機器及び必要資材の搬入等を行う場合、一週間前までに詳細な施工方法、施工範囲、作業員名、スケジュール及び使用車両をあらかじめ定めた書面をもって作業申請を行い、主管課の承認を得ること。また、主管課が行うべき作業がある場合には、これを明示すること。

（シ）令和6年11月1日（金）からのシステム移行の開始に間に合うよう、必要な工事を全て完了すること。
（ス）円滑な工事を実施するために必要な調整を主管課、現行保守事業者、現行運用事業者に対して行うこと。
（セ）関係システムとの接続にあたり、調達機器の設定変更等の調整が必要な場合には対応すること。

4.2.3　テスト

①　テスト実施計画策定

（ア）次期情報システム基盤に求める要件を確実に満たしていることを確認するため、単体テスト、結合テスト及び総合テストを計画し、「テスト実施計画書」を作成すること。
（イ）「テスト実施計画書」について、各種テスト実施前に主管課の承認を得ること。
（ウ）「テスト実施計画書」には、以下を明記すること。
(1)　スケジュール
(2)　テスト項目
(3)　テスト手順
(4)　テストデータ
(5)　合否判定基準　等
（エ）「テスト実施計画書」作成時には、受入テスト期間を可能な限り長期間確保できるようにスケジュールを検討すること。
（オ）「テスト実施計画書」は、令和6年11月1日（金）から開始されるシステム移行等に伴う受入テストに必要な機器を利用できるよう作成すること。
（カ）全てのテストは、原則として令和6年11月30日（土）までに完了すること。

②　テスト実施

（ア）全般
(1)　「テスト実施計画書」に従い、各種テストを行うこと。
(2)　各種テストの進捗状況を主管課へ定期的に報告すること。
(3)　不具合等によりスケジュールの遅延が想定される場合、不具合の内容を主管課に速やかに報告し、対策案を提示の上、行うこと。
（イ）単体テスト
(1)　調達機器及びクラウドサービスが単体で正常に動作することを確認すること。
（ウ）結合テスト1（各拠点内）
(1)　ネットワーク、システム、利用するクラウドサービス等の単位で調

達機器が相互に接続できること並びに冗長化構成が機能すること等、正常に動作することを確認すること。

(2) 統計センターの運用を想定した性能テスト及び負荷テストを行うこと。

(エ) 結合テスト2（各拠点間）

(1) 以下に示す各拠点間の疎通テストを行い、正常に動作することを確認すること。なお、当該テストに係る接続先との調整を行うこと。

- 統計センター
- メインデータセンター
- バックアップデータセンター
- 統計データ利活用センター

(オ) 総合テスト

(1) 主管課の立会いのもと、次期情報システム基盤全体を通して正常に動作することを確認すること。

(カ) バックアップデータセンター切り替えテスト

(1) メインデータセンターが使用不能になった場合を想定し、バックアップデータセンターへの切り替えテストを行うこと。

③ テスト結果報告

(ア) 各種テストの実施後、速やかに「テスト結果報告書」を作成し、主管課の承認を得ること。

(イ) 「テスト結果報告書」には、「テスト実施計画書」のテスト項目ごとに結果を整理した上で、合否を記載すること。

4.2.4 受入テスト支援

① 受入テスト計画支援

(ア) 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、主管課に提示し、承認を得ること。

② 受入テスト実施支援

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

(イ) 主管課等の受入テストに協力し、調達機器（統計センターが用意する機器を除く。）及び各種設定等に起因する障害等が発生した場合には、当該担当者と連携し、原因の特定から対処まで責任を持って対応すること。

③ 受入テスト結果報告書の作成支援

(ア) 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。

4.2.5　情報システムの移行

①　移行計画

（ア）現行情報システム基盤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。なお、次期情報システム基盤への移行にあたり、本仕様書に記載した機能以外の機器等が一時的に必要となる場合には、本調達の範囲内で対応すること。

（イ）移行を実施するにあたり、「移行実施計画書」、「移行設計書」及び「移行手順書」を作成し、主管課の承認を得ること。移行実施計画は、次期情報システム基盤の各構成要素の特性等を十分考慮した上で、確実な移行ができ、業務へ与える影響が極力少ないものとすること。

（ウ）想定する移行対象は「別添3　移行対象一覧」を参照すること。

②　移行実施

（ア）「移行実施計画書」、「移行設計書」及び「移行手順書」に従い、移行を行うこと。

（イ）移行の進捗状況を主管課に定期的に報告すること。

（ウ）移行期間中は仮運用とするが、令和7年1月1日（水）の稼動開始前に現行情報システム基盤から次期情報システム基盤への切り替えを行う機器等については、仮運用であっても、本調達の範囲内で「4.3保守に係る作業」に示す要件のとおり保守業務を行うこと。

（エ）移行期間中は、「運用設計書」に基づき次期情報システム基盤の運用管理を行うこと。

（オ）データ移行にあたり情報漏えい防止に配慮した移行を行うこと。

（カ）現行情報システム基盤と次期情報システム基盤を接続して移行を行うこと。

（キ）現行情報システム基盤の現行情報システム基盤への影響に配慮し、必要に応じて現行保守事業者及び現行運用事業者と連携すること。

（ク）以下に留意し、移行を行うこと。

(1)　現行情報システム基盤のファイルサーバから「要件定義書-11.2.2①メインストレージ」にユーザデータの移行を行うこと。

③　移行結果報告

（ア）移行の結果について、「移行結果報告書」を作成し、主管課の承認を得ること。

4.2.6　引継ぎ

① 以下には主管課向けの引継ぎ内容を記載している。請負者内での引継ぎについては内部にて引継ぎ漏れのないように実施すること。

② 引継ぎ計画

（ア）主管課を対象とした上で「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、スケジュール、引継ぎ項目、引継ぎ内容及びドキュメント一覧を明記すること。

（ウ）次期情報システム基盤を運用する上で必要となる操作方法等について主管課向けに「操作手順書」を作成すること。

③ 引継ぎ実施

（ア）「引継ぎ計画書」に従い、引継ぎを行うこと。

（イ）引継ぎの進捗状況を主管課に定期的に報告すること。

（ウ）引継ぎ時は「操作手順書」を利用すること。

（エ）構築時に主管課と協議した内容等を主管課に共有すること。

④ 引継ぎ完了報告

（ア）引継ぎ後、速やかに「引継ぎ完了報告書」を作成し、主管課の承認を得ること。

（イ）「引継ぎ完了報告書」には、引継ぎ完了日時、引継ぎ項目及び引継ぎ内容を記載すること。

4.2.7 教育

① 教育計画及び実施

（ア）「教育計画書」を作成し、「教育計画書」に従い、教育を行うこと。

② ユーザ向けテキスト作成

（ア）次期情報システム基盤の利用に必要な以下の内容を含むテキストを作成し、主管課の承認を得ること。特に、新たに導入されるWEB会議の機能や、オンラインでのファイル共有の機能、メール誤送信防止等の機能の使い方については、主管課と調整の上、わかりやすい内容となるようにすること。

(1) PC の利用方法

(2) 「要件定義書-1.1 ユーザ提供機能」の利用方法

(3) 「要件定義書-1.3.1 主体認証」の利用方法

(4) 「要件定義書-1.3.2 仮想ブラウザ」の利用方法

(5) 「要件定義書-1.3.3 ファイル無害化及びメール無害化」の利用方法

等

③　主管課向けテキストの作成及び操作説明

（ア）提供する機能全般について、次期情報システム基盤の運用に必要な操作方法等に関するテキストを作成し、主管課の承認を得ること。また、必要に応じて操作説明を行うこと。なお、当該テキストは「4.2.6②(ウ)」に示す「操作手順書」を用いることも可とする。

④　製品マニュアル

（ア）調達機器（統計センターが用意する機器を除く。）の使用に必要な「製品マニュアル」を可能な限り電磁的記録媒体で1セット提供すること。

（イ）電磁的記録媒体で「製品マニュアル」を提供できない場合、紙媒体で以下のとおり提供すること。ただし、(1)について調達数量が10セット以下の製品については、調達数量と同数の「製品マニュアル」を提供すること。

(1)　PC 関連製品に関する製品マニュアル：10 セット

(2)　その他の製品に関する製品マニュアル：2 セット

4.3　保守に係る作業

4.3.1　全般

①　「保守計画書」を作成し、主管課の承認を得ること。

②　保守に係る計画事項として、「標準ガイドライン解説書-第3編第9章　運用及び保守　1.運用開始前の準備　4）保守計画書の作成と確定」に従い、少なくとも以下の項目を記載すること。

（ア）作業概要

（イ）作業体制に関する事項

（ウ）スケジュールに関する事項

（エ）成果物に関する事項

（オ）保守形態、保守環境等

③　「保守計画書」において、保守に係る管理要領として、「標準ガイドライン解説書-第3編第9章　運用及び保守　1.運用開始前の準備　5）保守実施要領の作成と確定」に従い、少なくとも以下の項目を記載すること。

（ア）コミュニケーション管理

（イ）体制管理

（ウ）作業管理

（エ）リスク管理

（オ）課題管理

（カ）システム構成管理
（キ）変更管理
（ク）情報セキュリティ対策

④　「保守計画書」は上記②及び上記③に加え、統計センターが作成する「運用管理規則」を参考に作成すること。

⑤　「保守計画書」に基づき以下の作業を行うこと。
（ア）ハードウェア保守
（イ）ソフトウェア保守
（ウ）通信回線保守
（エ）報告
（オ）SLA管理業務
（カ）リモート監視

⑥　保守対象は、本調達で納品する全ての調達機器（統計センターが用意する機器を除く。）とすること。
⑦　保守を行う保守要員は、十分な知識及び経験を有すること。
⑧　リモートによる保守を行う場合（サポートベンダーを含む。）は、セキュリティに留意し問題がないことを証明し、主管課の承認を得ること。なお、リモート保守に必要な回線等の敷設に係る工事費、回線使用料は請負者の負担とすること。
⑨　保守を行うにあたり電話回線等が必要な場合は、主管課と協議すること。なお、電話回線等の敷設に係る工事費、電話回線等使用料についても本調達の範囲内で対応すること。
⑩　次期情報システム基盤の運用期間中に、調達機器（統計センターが用意する機器を除く。）及びサービス等が、ベンダーの都合による保守サポートの終了等により保守対応ができなくなる場合には、以下の対応を行うこと。なお、対応に係る一切の費用は請負者の負担とすること。
（ア）保守サポートが可能且つ同等以上の機能と性能を持った代替の機器及びサービス等による提供を行うこと。
（イ）代替の機器及びサービス等による提供を行う場合には、主管課の承認を得ること。

⑪　主管課からの要請が、保守時間内に請負者の連絡窓口に到着した場合、直ちに次期情報システム基盤の構成を熟知している者（構築時に中心的な役割を担った者もしくはその情報を引き継いだ者等）を派遣またはリモート保守により、主管課と連携の上、迅速な回復に努めること。また、サービ

スが停止するような重大障害発生時には保守時間にかかわらず、早急に対応すること。

⑫　必要に応じて、運用設計において作成した「操作手順書」の追加及び修正を行うこと。

⑬　障害発生時に請負者またはベンダーに自動通報すること。

⑭　人事異動に伴う作業を可能な限り自動化すること。なお、サーバの機能による実現も可とする。

⑮　調達機器（統計センターが用意する機器を除く。）の連絡窓口を一元化すること。

4.3.2　ハードウェア保守

①　全てのハードウェア（各機器のバッテリー等を含む）について、障害発生時に機器全体の交換または故障パーツの交換を行い、正常動作を確認すること。

②　保守時間は土曜日、日曜日、国民の祝日及び年末年始（12月29日から1月3日）を除く9時から17時30分とし、保守時間内に連絡した場合、保守要員を概ね4時間以内に派遣し正常稼動するよう迅速な対応を図ること。ただし、上記はPCとバックアップデータセンターに係る対応を除く。

③　障害が発生した場合は、原因を特定し、主管課に報告すること。

④　調達機器（統計センターが用意する機器を除く。）に搭載されている電磁的記録媒体を外部へ持ち出す場合は、主管課の承認を得ること。

⑤　交換済み不良部品の処分時等、電磁的記録媒体を永続的に持ち出す場合は、当該媒体について、原則として調達機器（統計センターが用意する機器を除く。）の納品場所内でNIST 800-88 Rev.1 Purge方式相当以上によるデータ消去を行うもしくは物理破壊し、「消去証明書」を発行すること。なお、物理破壊の場合は物理破壊後の写真を撮影し、提出すること。また、電磁的記録媒体は請負者が処分すること。ただし、「消去証明書」を発行することに関しては、直接対応ができない場合は、別途、外部業者に依頼した上で、データ消去などの発行証明書を提出すること。

⑥　メインデータセンター及びバックアップデータセンターに設置する調達機器（統計センターが用意する機器を除く。）の目視確認が必要となる事項がある場合は、1日1回以上、目視による監視を行うこと。

⑦　全てのハードウェアに搭載されるファームウェア（アプライアンスのOSも含む。）について、修正モジュール及びバージョンアップソフトウェアの適用の可否及び要否を検討した上で、適用すること。なお、適用にあたり、必要に応じて検証環境で正常性を確認し、適用することが望ましい。

4.3.3　ソフトウェア保守

① 調達機器に搭載されるソフトウェアを対象に契約期間中のサポート契約を締結すること。
② ソフトウェア不具合時にベンダーから提供される修正モジュール及びバージョンアップソフトウェアを提供すること。なお、提供にあたり次期情報システム基盤への適用の可否及び要否を検討すること。なお、適用にあたり、必要に応じて検証環境で正常性を確認し、適用することが望ましい。
③ ソフトウェアのバージョンアップ及び修正モジュールの適用を行うこと。
④ セキュリティパッチ及びバージョンアップソフトウェア等の脆弱性を解決するために利用されるファイルについては、公式サイトから入手すること。
⑤ 本調達で導入するPC及び仮想PCへのセキュリティパッチ適用（動作確認を含む）を行うこと。
⑥ Microsoft Windows Serverへのセキュリティパッチ適用（動作確認を含む）及びLinuxサーバのセキュリティパッチ適用については可能な限り自動化すること。

4.3.4 通信回線保守

① 問い合わせ等の受付、主管課からの連絡が24時間365日対応可能な体制であること。
② 提供する通信区間の障害等監視を24時間365日行うこと。
③ 障害等を検出した場合は、主管課に電話連絡し障害対応を行うこと。
④ 通信速度のほか、障害対応を含め通信品質の保証値を設けないベストエフォート型の回線は上記の対象外とする。

4.3.5 報告

① 定期報告

（ア）契約期間中は、月次で障害履歴、サポート期間及びセキュリティパッチ更新情報等を取りまとめた「月次報告書」及び「データセンター月次報告書」を作成し、報告を行うこと。なお、報告内容の詳細については、主管課と協議の上、決定すること。

② 障害時報告

（ア）障害等が発生した場合には、速やかに障害等の状況を記載した「障害等報告書」を作成の上、主管課に遅滞なく提出し、承認を得ること。
（イ）障害等に伴い保守作業及び設定変更を行った際は、「障害等報告書」に実施内容を記載の上、主管課に遅滞なく提出し、承認を得ること。
（ウ）障害等による機器等の保守が完了した場合、対応したメーカあるいはベンダーに速やかに実施結果報告を求め、受託者は速やかに「障害等報告書」

に実施結果を記載の上、主管課に提出し、承認を得ること。

4.3.6　SLA管理業務

①　SLAの締結

（ア）下記「表 5　サービスレベル目標」に基づき主管課と協議の上、SLAを締結し、「SLA合意書」を作成すること。

（イ）下記「表 5　サービスレベル目標」に定めた管理指標値を記録、集計し、実績について月次及び年次で「SLA報告書」を作成し、報告すること。

（ウ）クラウドサービスのSLAはクラウドベンダーのものに従う。そのため、設計時に主管課と協議の上、サービスレベルの合意を行うこと。

表 5　サービスレベル目標

SLA項目		内容	サービスレベル値	対象	報告頻度	評価
稼働率	レベル3	稼働率として右記サービスレベル値を保証する。 稼働保証時間24H/365日	99.9%以上	･データセンター ･ネットワーク（ベストエフォートの回線を除く。） ･仮想化基盤	年次及び月次	年次及び月次
	レベル2	稼働率として右記サービスレベル値を保証する。 稼働保証時間24H/365日	99.75%以上	集計業務に利用する以下サーバ ･データベースサーバ ･ファイルサーバ ･バッチ制御サーバ ･バッチ処理サーバ ･家計APIサーバ	年次及び月次	年次及び月次
	レベル1	稼働率として右記サービスレベル値を保証する。	99.5%以上	上記以外のサービス（クラウドサービスは除く）	年次及び月次	年次及び月次

②　SLAの改定

（ア）設定した管理項目、管理指標値、保証値等については、必要に応じて見直しを実施し改訂するものとする。なお、改訂の契機は以下のとおりとする。

(1)　統計センター及び請負者双方の合意事項に明確な変更が生じた場合

(2)　統計センター及び請負者双方が必要と認めた場合

③　SLAに係る免責事項

（ア）以下の場合は、SLAの適用外とする。

(1) 災害により電源供給が停止した場合
(2) 請負者の瑕疵によらず電源供給が停止した場合
(3) 統計センター及び他の調達事業者の過失または故意による障害の場合
(4) 統計センター及び他の調達事業者の過失または故意により障害復旧が行えない場合
(5) 請負者の瑕疵によらず障害監視が行えない場合
(6) 請負者の瑕疵によらず障害通知の受信ができない場合
(7) 統計センター及び請負者双方の協議の上で計測の除外とした場合

④ SLAに係る是正措置

（ア）1ヶ月ごとに達成状況の報告を行い、未達成項目がある場合、請負者は以下に示すような措置により達成度合いの向上に努めること。

(1) 未達成の項目に対する改善策(運用操作説明書の改訂、保守員の配備、仕組み及び手続きの見直し、検証試験の実施、機器等の導入・交換等)を提示し、統計センターの承認を得た上で対策を講じること。また、そのために必要となる作業等は請負者の負担で行うこと。なお、統計センター情報システム基盤の環境に依存する場合、あるいは依存する可能性がある場合も含む。
(2) 改善策の実施効果を実施の月より 3 ヶ月間、1 ヶ月ごとの達成状況報告とともに報告し、統計センターの承認を得ること。

4.3.7 リモート監視

① リモート監視サイトと接続する回線はセキュリティを確保された回線とすること。
② リモート監視の対象は、情報セキュリティ機能として導入するセキュアWebゲートウェイ(SWG)及び不正プロセス検知のために導入する各サービスと機器とし、対象の監視を実現する機能を構築すること。
③ 24時間365日常時対象機器を監視し、重大な事象を検知した場合は、発見時点から60分以内に主管課が指定する担当者に電話で連絡するとともに、当該担当者と協議の上、遮断等の対応を行うこと。
④ インシデント発生の判断は、対象機器が出力するアラートのみで判断するのではなく、セキュリティ監視専門技術者が、誤報確認またはインシデント発生有無、影響度合いを判断すること。
⑤ 主管課がインターネット通信の遮断を依頼した場合は、対象機器の設定変更を行うこと。
⑥ 不正侵入防止機能に対するシグネチャ（パターンファイル）を運用・管理・適用すること。また、必要に応じて請負者独自のシグネチャを提供

し、次期情報システム基盤に適した監視サービスを実現すること。なお、シグネチャは、請負者側で十分な検証を実施した上で適用すること。

⑦　セキュリティ監視結果を取りまとめた「セキュリティ監視月次レポート」を作成すること。「セキュリティ監視月次レポート」には、次期情報システム基盤に対する監視結果に加え、国内の監視状況等、社会における状況を加味すること。

⑧　セキュリティ監視状況を主管課が迅速に入手可能となるよう、過去の監視状況、インシデント発生状況等を検索、閲覧可能なシステムを提供すること。

⑨　監視中に対象機器の障害を検知した場合には、主管課に遅滞なく連絡するとともに、可能な範囲で原因を調査すること。

⑩　リモート監視サイトは国内に設置すること。

4.3.8　調達機器の撤去

①　撤去期限

（ア）令和12年1月1日（火）以降、調達機器の撤去を行うこと。なお、調達機器の撤去は、令和12年3月31日（日）までに完了することとし、詳細については主管課の指示に従うこと。

②　メインデータセンター及びバックアップデータセンター設置機器

（ア）電磁的記録媒体は原則として、調達機器の納品場所内でNIST 800-88 Rev.1 Purge方式相当以上によるデータ消去を行うもしくは物理破壊し、「消去証明書」を発行すること。なお、物理破壊の場合は物理破壊後の写真を撮影し、提出すること。また、電磁的記録媒体は請負者が処分すること。ただし、「消去証明書」を発行することに関しては、直接対応ができない場合は、別途、外部業者に依頼した上で、データ消去などの発行証明書を提出すること。

（イ）各データセンター内の第三者が立ち入ることができない専用区画内でデータ消去、解体等撤去に必要な作業全てを行うこと。

（ウ）「消去証明書」等の発行後、各データセンターから運び出すこと。

③　統計センター及び統計データ利活用センター設置機器

（ア）本調達で導入するPC及び周辺機器等については、統計センター及び統計データ利活用センター内執務室の各事務机から統計センター及び統計データ利活用センター内の主管課が指示する場所まで運搬を行うこと（セキュリティワイヤーの取り外しを含む）。

（イ）電磁的記録媒体は原則として、調達機器の納品場所内でNIST 800-88 Rev.1 Clear方式相当以上によるデータ消去を行うもしくは物理破壊し、

「消去証明書」を発行すること。物理破壊の場合は物理破壊後の写真を撮影し、提出すること。また、電磁的記録媒体は請負者が処分すること。なお、統計センターが用意する機器の物理破壊は不可とする。ただし、「消去証明書」を発行することに関しては、直接対応ができない場合は、別途、外部業者に依頼した上で、データ消去などの発行証明書を提出すること。

（ウ）電磁的記録媒体以外の機器（スイッチ等）については、撤去を行った証跡（写真等）を記載した撤去に係る証明書（撤去報告書）を作成し、提出すること。

（エ）統計センター及び統計データ利活用センター内の主管課が指示する場所でデータ消去、解体等撤去に必要な全ての作業を行うこと。

（オ）「消去証明書」等の発行後、統計センター及び統計データ利活用センターから運び出すこと。

4.4　運用に係る作業

4.4.1　対応時間等

①　業務時間（統計センター常駐）

（ア）9時から18時とする。ただし、土曜日、日曜日及び国民の祝日に関する法律（昭和23年法律第178号）に定める日並びに12月29日から翌年1月3日までの日（以下「閉庁日」という。）を除く。

②　業務時間外の対応

（ア）業務時間外においても携帯メール等によりシステム障害を通知する仕組みとなっているため、障害通知を受信した場合は、必要に応じて主管課へ連絡すること。また、緊急性のあるシステム作業及び障害発生時の作業等、別途主管課からの指示がある場合は、上記「4.4.1①業務時間（統計センター常駐）」の業務時間帯以外においても対応すること。

③　計画停止時の対応

（ア）次期情報システム基盤の停止を伴う作業等、夜間または閉庁日に作業することが適切であると主管課が判断する場合は、上記「4.4.1①業務時間（統計センター常駐）」の業務時間帯以外においても対応すること。

4.4.2　運用業務内容

本業務で実施する運用業務について、下記「表 6　運用業務概要」に概要を記載する。なお、詳細な業務内容は「別添4　運用管理業務一覧」に細分化し、記載しているため、請負者は当該資料を確認し、漏れなく運用管理業務を実施すること。

表 6　運用業務概要

項番		業務概要	
1. 定期報告及び会議	1.1	定期報告	日次報告、週次報告、月次報告及び年次報告を行うこと。
	1.2	会議	定例会議及び適宜実施する会議を行うこと。
2. 運用計画書及び運用設計書の修正	-	-	「運用計画書」及び「運用設計書」の修正を行うこと。
3. 運用管理要領の作成	-	-	「運用管理要領」の作成を行うこと。
4. サービスデザイン	4.1	サービスレベル管理	SLAの締結、SLAの改定、SLAに係る是正措置を行うこと。SLAに係る免責事項は、「別添4 運用管理業務一覧」を確認すること。
	4.2	キャパシティ管理	システム性能管理、ディスク管理を行うこと。
	4.3	可用性管理	システム設定変更、ソフトウェアのアップデート及び修正プログラムの適用、バックアップ及びリストア、計画停止に伴う作業を行うこと。
	4.4	情報セキュリティ管理	証跡管理及び分析、脆弱性対策、不正プログラム対策、不正侵入管理を行うこと。
	4.5	ITサービス継続性管理	切替訓練、切替試験、切戻し試験及び緊急時体制の準備を行うこと。
	4.6	サプライヤ管理	事前調整及び作業時対応を行うこと。
5. サービストランジション	5.1	変更管理	変更要求の受付・記録、変更要求の評価及び変更要求の承認申請を行うこと。
	5.2	リリース管理及び展開管理	受け入れ試験、受け入れ試験結果承認申請、リリースの実施及び構成管理への引渡しを行うこと。
	5.3	サービス資産管理及び構成管理	ハードウェア及びソフトウェアの管理、ソフトウェアインベントリ収集、通信回線装置のソフトウェアの管理並びに各種操作手順書等の管理を行うこと。

項番		業務概要	
	5.4	ナレッジ管理	対応策の共有及び管理並びに問合せの共有及び管理を行うこと。
6. サービスオペレーション	6.1	イベント管理	死活監視、ログ監視、性能監視、データベース性能監視、ポート監視、セキュリティ監視及び目視点検を行うこと。
	6.2	インシデント管理	障害発生報告、障害レベル切り分け、障害管理票作成、障害情報収集・原因調査、復旧方針の策定並びに障害復旧作業の実施及び結果報告を行うこと。
	6.3	問題管理	原因の究明、進捗報告及び障害復旧を行うこと。
	6.4	アクセス管理	ユーザIDの管理を行うこと。
	6.5	サービスデスク	問合せ対応、応対履歴情報の管理及びFAQ提供を行うこと。
			各種申請書に係る対応を行うこと。
7. 継続的サービス改善	-	-	目標及びKPIの設定、業務の改善、目標及びKPIの見直し、改善する業務内容の提案、安定稼働及びユーザに提供するサービスの向上に対しての改善、安定稼働及びユーザに提供するサービスの向上に対して、主管課と協議の上並びに「運用計画書」等の見直しを行うこと。
8. その他作業	8.1	人事異動に伴う作業	クライアント端末の増設・撤去、仮想PCの作成・削除・設定変更、組織グループの作成・削除・設定変更、ユーザIDの追加・削除、メール設定の追加・削除、LANケーブルの作成及び複合機の移設を行うこと。
	8.2	インターネット関係システム管理	サイトアクセス数の解析、不正アクセス及び特徴的な通信の集計、クローラーデータの更新、偽サイト調査、サイト改ざん検知、証明書管理並びにメール経路設定を行うこと。
	8.3	技術的支援等	技術的支援、復旧訓練、主管課の指示に基づく作業を行うこと。
	8.4	業務引継資料の作成及び引継ぎの	現行情報システム基盤の運用事業者からの引継ぎ、次の運用事業者への引継ぎ及び最終バックアップを行うこと。

項番		業務概要	
		実施等	

4.4.3　運用業務実施上の留意点

①　本業務の実施にあたり、運用管理業務は可能な限り自動化すること。

②　運用管理業務を自動化する製品の導入が必要な場合、事前に主管課の許可を得ること。

③　運用管理業務を自動化する製品を導入する場合、必要に応じて「運用計画書」及び「運用設計書」の変更及び追加を行い、主管課の許可を得ること。

④　次期情報システム基盤を構成する全てのソフトウェア及び別途導入する全てのソフトウェアについて、ユーザから不具合に関する照会があった場合は、一次切り分けを実施し、切り分けの結果をユーザへ説明すること。

⑤　データセンター現地での作業

（ア）現地での確認以外に手段がない場合（遠隔での作業が不可能な場合等）は、現地へ赴き作業を行うこと。なお、データセンターへの旅費等については請負者の負担とする。

4.5　ホームページ基盤運用に係る作業

4.5.1　全般

①　監視サイトは国内に設置すること。

4.5.2　対応時間及び運用業務内容

①　24時間365日ホームページ基盤からのメール通知を監視し、重大な事象を検知した場合は、発見時点から15分以内に連絡すること。その後、以下を実施すること。

（ア）一次切り分け(サーバログ等の調査)

（イ）サーバの再起動(必要に応じ)

（ウ）サーバのネットワークからの切り離し(必要に応じ)

（エ）サーバ以外の各種ログ確認(必要に応じ)

②　平日日中帯　(9:00～18:00）は以下を実施すること。

（ア）主管課及びサーバに関する問い合わせ対応(メール・電話受付)

（イ）サーバ(OS及びミドルウェア)に関する軽微な設定変更(メール・電話受付)。

（ウ）導入したOS及びミドルウェアについて以下の対応を行うこと。

（エ）改修履歴を管理し、適用されているバージョンを明確にしておくこと。
（オ）公開されている脆弱性情報を収集し影響を確認すること。
（カ）主管課から提供する脆弱性情報の影響の有無を確認し報告すること。
（キ）情報セキュリティ監査の結果の影響を確認すること。
（ク）脆弱性情報及び情報セキュリティ監査の結果が影響を及ぼすと判断した場合は、統計センターホームページ検証用サーバに修正を適用し、主管課及びホームページコンテンツ事業者へ連絡すること。
（ケ）ホームページコンテンツ事業者から動作検証を完了した旨の連絡を受けた場合は、統計センターホームページサーバに修正を適用すること。

③　月次報告
（ア）当月分のシステム稼働状況、障害状況、問合せ状況、保守作業状況、アクセス件数等をまとめた「月次報告書」を提出すること。

4.5.3　運用業務実施上の留意点
①　「4.5.2対応時間及び運用業務内容」に記載の業務内容以外の作業は、次期保守担当者が実施すること。

5.　成果物の範囲、納品期日等

5.1　成果物
①　本業務に係る最低限の納品成果物は下記「表 7　次期情報システム基盤稼働開始までの納品成果物」、下記「表 8　次期情報システム基盤稼働期間中の納品成果物」のとおり。なお、納品成果物の納品期限は、プロジェクト開始後、「全体作業計画書」で明確にした上で、納品期限前に余裕を持って主管課に提出し、承認を得ること。
②　請負者は下記「表 7　次期情報システム基盤稼働開始までの納品成果物」、下記「表 8　次期情報システム基盤稼働期間中の納品成果物」に示す納品成果物並びにその他作成する資料を取りまとめた完成図書を主管課に提出し、承認を得ること。また、各作業の「作業完了報告書」は、各作業完了後速やかに主管課に提出すること。
③　成果物の作成に当たって、特別なツールを使用する場合は、統計センターの承認を得ること。

表 7　次期情報システム基盤稼働開始までの納品成果物

No.	納品成果物	詳細	納入期限
1	全体作業計画書	-	契約締結後 2 週間以内

No.	納品成果物	詳細	納入期限
2	基本設計書	ネットワーク構成図（物理・論理） 導入機器構成一覧 導入機器仕様一覧 データセンター仕様一覧 通信回線構成一覧 通信回線仕様一覧 ラック構成図 機器等消費電力、発熱量、重量一覧 ネットワーク設計 セキュリティ設計 ストレージ設計 拡張性設計 障害対策 バックアップ／リストア設計 OS、ミドルウェア設計 仮想サーバ及び仮想 PC 設計 業務継続 フロアレイアウト図 SLA 合意書　等	全体作業計画書で定義（令和6年6月を想定）
3	詳細設計書	設定手順書 環境設定書 パラメータシート ポートアサイン図 IP アドレス一覧 導入ライセンス一覧　等	全体作業計画書で定義（令和6年8月を想定）
4	運用計画書	運用計画	全体作業計画書で定義（令和6年8月を想定）
5	運用設計書	システム運用管理障害管理 可用性管理 性能管理 ネットワーク管理 セキュリティ管理 構成管理 変更管理	全体作業計画書で定義（令和 6 年 10 月を想定）

No.	納品成果物	詳細	納入期限
		ストレージ管理 保全管理 報告関連 ヘルプデスク 保守 SLA 管理 業務継続 操作手順書（運用操作説明書、機器等稼動手順書、機器等停止手順書システム復旧手順書、災害対策用機器利用手順書等） サポート登録情報一覧　等	
6	テスト関連ドキュメント	テスト実施計画書 受入テスト計画書（案）	令和 6 年 9 月 30 日
		テスト結果報告書	令和 6 年 11 月 30 日
7	移行関連ドキュメント	移行実施計画書 移行設計書 移行手順書 移行結果報告書	令和 6 年 12 月 31 日
8	引継ぎ関連ドキュメント	引継ぎ計画書 引継ぎ完了報告書	同上
9	教育関連ドキュメント	教育計画書 製品マニュアル 各種テキスト	同上
10	保守関連ドキュメント	保守計画書 保守設計書　等	同上
11	会議議事録	-	会議開催都度 3 営業日以内
12	作業完了報告書	-	作業完了都度 2 営業日以内

表 8　次期情報システム基盤稼働期間中の納品成果物

No.	納品成果物	詳細	納入期限
1	日次報告書	運用の日次報告	報告当日

No.	納品成果物	詳細	納入期限
2	週次報告書	運用の週次報告	報告当日
3	月次報告書	運用・保守の月次報告	翌月 10 日まで
4	年次報告書	運用の年次報告	翌年度 4 月 20 日まで
5	データセンター月次報告書	データセンターの設置機器目視監視報告書及び入退室状況	翌月 10 日まで
6	障害等報告書	障害等報告書	障害発生、対応実施、対応完了時に速やかに提出
7	SLA 報告書	-	月次は翌月 10 日まで、年次は翌年度 4 月 20 日まで
8	KPI 報告書	-	翌年度 4 月 20 日まで
9	セキュリティ監視月次レポート	-	翌月 10 日まで
10	消去証明書	-	消去後速やかに提示
11	撤去報告書	-	撤去後速やかに提示
12	運用計画書（修正版）	運用計画	令和 6 年 12 月 20 日（※最終期日であり、必要に応じて、主管課が定める期日に随時提出。）
13	運用設計書（修正版）	システム運用管理 障害管理 可用性管理 性能管理 ネットワーク管理 セキュリティ管理 構成管理 変更管理 ストレージ管理 保全管理	同上

No.	納品成果物	詳細	納入期限
		報告関連 サービスデスク 保守 SLA 管理 業務継続 操作手順書（運用操作説明書、機器等稼動手順書、機器等停止手順書システム復旧手順書、災害対策用機器利用手順書等） サポート登録情報一覧　等	
14	設計書（修正版）　等	次期情報システム基盤稼働期間中に修正を行った設計書等	同上
15	運用管理要領	運用に係る管理要領	同上
16	IT 資産台帳	-	同上
17	ドキュメント管理台帳	-	同上
18	KPI 報告書	-	同上
19	会議議事録	-	会議開催都度 3 営業日以内
20	作業完了報告書	-	作業完了都度 2 営業日以内

5.2　納品方法

① 納品成果物は紙媒体及び電子媒体（編集可能なMicrosoft Office形式及びPDF形式でDVD等に格納）で各2部を提出すること。

5.3　納品場所

① 原則として、納品成果物は以下の場所において引渡しを行うこと。ただし、主管課が納品場所を別途指示する場合はこの限りではない。

（ア）郵便番号　　：162-8668
（イ）住所　　：東京都新宿区若松町19-1 総務省第2庁舎
（ウ）電話番号　　：03-5273-1268
（エ）主管課　　：統計センター情報システム部情報システム基盤課

6. 満たすべき要件に関する事項

① 本業務の実施においては、「別添1 要件定義書」の各要件を満たすこと。

7. 作業の実施体制・方法に関する事項

7.1 作業実施体制

① 本業務を実施する体制を下記「図 3 設計・構築における体制図」及び下記「図 4 運用・保守における体制図」に示す。

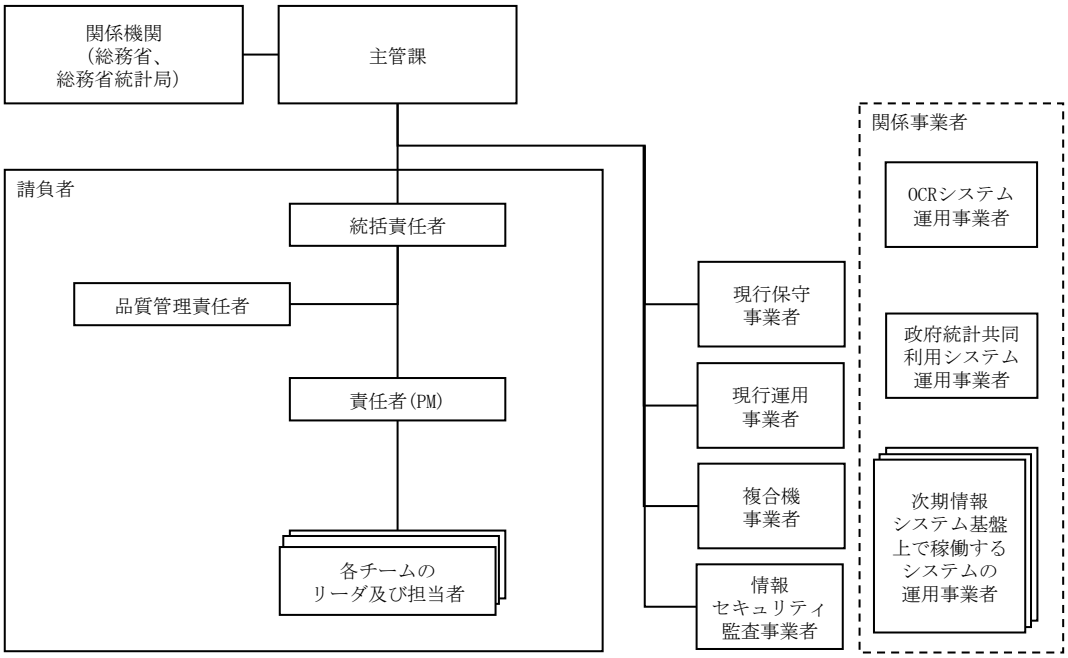


図 3 設計・構築における体制図

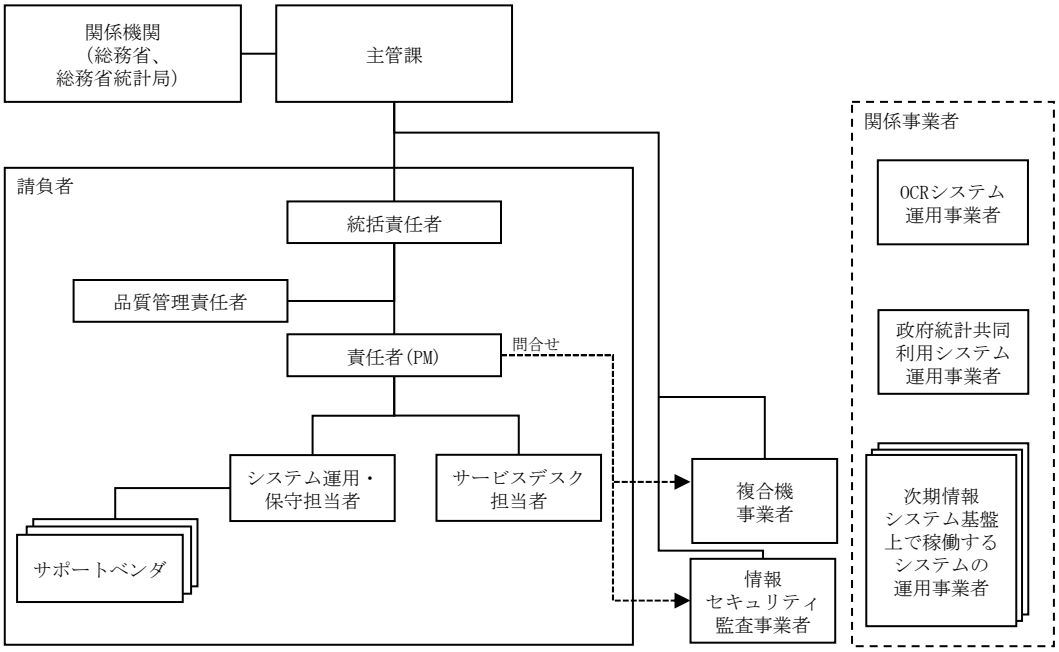


図 4 運用・保守における体制図

② 本業務の実施にあたり、必要なスキル及び経験を有する要員を配した業務実施体制を整え、適切な作業管理の下、作業を行うこと。
③ 本業務の設計・構築における実施体制においては、本業務全体を統括する統括責任者を定めること。
④ 本業務において、納品成果物の品質を管理する品質管理責任者を定めること。また、品質管理の具体的な方法を明示すること。
⑤ 提案する主要な調達機器（統計センターが用意する機器を除く。）や利用するクラウドサービスのベンダーと緊密な連絡・連携体制の構築できること。また、本業務の履行に際しては提案する主要な調達機器（統計センターが用意する機器を除く。）のベンダーからサポートを受けられることとし、本業務実施体制図にて明示すること。
⑥ 納品成果物に対する統計センターが意図しない変更及び機密情報の窃取等が行われないことを保証する管理体制を用意し、当該体制を証明する書類（品質保証体制の責任者及び各担当者がアクセス可能な範囲等を示した管理体制図）を提出すること。
⑦ 運用開始後4ヶ月は、設計・構築担当者を統計センターに常駐させ、主管課等からの問い合わせに対応すること。
⑧ 運用業務における人員の配置は、本仕様書に掲げる「4.4.2 運用業務内容」に応じた体制とすることとし、各業務シフトを考慮した適正人員（想定する人数は4名。なお、1名の責任者を含む。）を配置すること。特に、サービスデスク業務については、次期情報システム基盤のユーザからの問合せの数に応じて、柔軟に対応すること。
⑨ 稼働環境の変更業務（システム設定・変更、データの参照・更新及びデータ復旧）を伴う作業については、常に複数名体制で作業を行い相互牽制が働くようにすること。
⑩ リモートにて運用業務を実施する際には情報漏洩等が発生しないよう、作業実施方法や実施場所について、事前に主管課の承認を得ること。また、リモートで作業を実施する場合であってもメンバ間で相互牽制が働くようにコミュニケーションには留意すること。
⑪ 体制を変更する場合は、主管課の承認を得ること。
⑫ 主管課において、要員の交代の必要があると判断したときは、1週間前までに請負者に通知の上、交代させるものとする。
⑬ 請負者は、主管課と日本語で円滑なコミュニケーションが可能であること。
⑭ 統括責任者、責任者（PM）及び各チームのリーダ間での兼任は不可とする。

7.2　要員に求める資格等の要件

①　本業務の実施にあたり、本業務実施体制内に以下の要員を配置すること。また、契約期間中にやむを得ず要員を交代する必要が生じた場合は、同等以上の資格、経験、能力を持つ要員であることを主管課に示し、承認を得ること。

（ア）統括責任者

(1)　統括責任者は、本業務全体を統括し、現場業務の実施及び遂行に全責任を持つこと。また、業務全体を統括する立場として主管課との調整を図ること。

(2)　統括責任者は、本業務と同等規模以上のシステムの導入経験及び情報処理業務の経験を 10 年以上有すること。

（イ）責任者（PM）

(1)　責任者(PM)は、「4.2 設計・構築に係る作業」、「4.3 保守に係る作業」、「4.4 運用に係る作業」及び構築時における各チームを統括し、当該作業の遂行に全責任を持つこと。また、各チーム内の作業状況を監視及び監督し、各チームリーダに対する指示を行うこと。

(2)　責任者(PM)は、情報処理技術者（プロジェクトマネージャ）または PMI（Project Management Institute）の PMP（Project Management Professional）資格取得者であること。

(3)　責任者は、本業務と同等規模以上のシステムにおいて、プロジェクトマネージャとしての経験を 5 年以上有すること。

（ウ）担当者

(1)　設計・構築作業の担当者

- 設計・構築作業の担当者のうち1名は仮想PC構築の実績を有すること。
- 設計・構築作業の担当者のうち1名はセキュリティの認定資格として情報処理技術者（情報セキュリティスペシャリスト）、情報処理安全確保支援士またはCISSP（Certified Information Systems Security Professional）と同等以上の資格を有すること。
- 設計・構築作業の担当者のうち1名はネットワーク認定資格として情報処理技術者（ネットワークスペシャリスト）またはCCIE(Cisco Certified Internet Expert)、CCNP(Cisco Certified Network Professional)と同等以上の資格を有すること。
- 設計・構築作業の担当者のうち1名は「標準ガイドライン」及び「統一基準群」に基づいた設計・構築経験を有すること。
- 設計・構築作業の担当者のうち1名はITSMSに基づく運用設計及び運

用の実績を有すること。また、ITILに関する資格を有していることが望ましい。

(2) 保守及びシステム運用担当者

- 保守及びシステム運用担当者は、原則、設計・構築作業を担当したメンバが担務することが望ましい。
- 保守及びシステム運用担当者は、設計・構築作業の担当者と同等のスキルを有すること。

(3) サービスデスク担当者

- サービスデスク担当者には、「表 6　運用業務概要　4.サービスデザイン、5. サービストランジション、6. サービスオペレーション」の内容を理解し、運用時のオペレーションを実施可能なスキルを有する要員を配置すること。
- サービスデスク担当者は情報処理技術者（基本情報技術者試験）またはITSSレベル2相当と説明可能な実務経験を有していること。また、ITSSレベル3相当以上の説明可能な資格または実務経験を持っていることが望ましい。

7.3　作業場所

① 作業場所が統計センター内または統計データ利活用センター内となる場合、主管課の指示に従うこと。

8.　作業の実施に当たっての遵守事項

8.1　情報セキュリティ対策

① 請負者は、独立行政法人統計センター情報セキュリティポリシーに規定されている各種セキュリティ対策（本業務の遂行に係る対策に限る。）と同等以上の対策を施し業務を遂行すること。

② 請負者は、本業務の実施のために取り扱う情報について、「別添9　情報保護・管理要領」に基づき、十分な管理を行うこと。

③ 本仕様書において求める情報セキュリティ対策が実施されていることを確認するために、主管課は請負者に対し実施状況の報告または確認（監査等）を求めることがあり、請負者はこれに応じること。

④ 本業務の遂行における情報セキュリティ対策の実施が不十分であると主管課が判断し、改善の指示があった場合には、請負者は、速やかに改善のための対策を実施すること。

8.2　遵守する法令等

8.2.1　法令及び標準等の遵守

①　本業務の実施は、以下の各種規定等に基づくこと。なお、契約期間中に当該文書が改定された場合はそれに従うこととするが、より効率的な作業実施方法について提案がある場合には主管課に提案し協議の上、当該提案に基づき行うことも可とする。

（ア）独立行政法人統計センター情報セキュリティポリシー（統計センター）

（イ）標準ガイドライン

（ウ）統一基準群

9.　成果物の取扱いに関する事項

9.1　知的財産権の帰属

①　請負者は、本業務で生じた成果物（第三者が権利を有する著作物が含まれる場合の当該著作物に係る部分を除く。）について、著作権法（昭和45年法律第48号）（第27条及び第28条の権利を含む。）に規定する一切の権利を、統計センターに無償で譲渡するものとする。

②　統計センターは、著作権法第20条（同一性保持権）第2項、第3号または第4号に該当しない場合においても、その使用のために、成果物を改変し、また、任意の著作者名で任意に公表することができるものとする。

③　請負者は、本業務で生じた成果物について、統計センターによる事前の同意を得なければ、著作権法第18条（公表権）及び第19条（氏名表示権）を行使することができない。

④　請負者は、成果物の利用が、第三者の著作権、特許権その他の知的財産権、営業秘密、肖像権、パブリシティー権、プライバシー権、その他の権利または利益（以下本条において「知的財産権等」という。）を侵害していないことを保証するものとする。

（ア）統計センターまたは統計センターから成果物の利用を許諾された者が、成果物の利用に関連して第三者の知的財産権等を侵害した旨の申し立てを受けた場合または第三者の知的財産権等を侵害するおそれのあると統計センターが判断した場合、請負者は、自己の費用と責任においてこれを解決するものとする。

（イ）上記(ア)の場合において、請負者は、統計センターの指示に従い、請負者の費用負担において、知的財産権等の侵害のない成果物と交換し、成果物を変更しまたは当該第三者から成果物の継続使用・利用のための権利の取得を行わなければならない。本項の定めは、統計センターの請負者に対する損害賠償を妨げない。

（ウ）上記(ア)の場合において、当該第三者からの申し立てによって統計センターから成果物の利用を許諾された者が支払うべきとされた損害賠償額、

その他当該第三者からの請求、訴訟等によって統計センターに生じた一切の損害及び申し立ての対応に要した弁護士等の第三者に支払った費用その他の解決に要した費用は、請負者が負担するものとする。

9.2　契約不適合による履行の追完、代金の減額及び契約の解除

① 成果物が契約の内容に適合しない場合は、統計センターは、自らの選択により、請負者に対し、成果物の修補、代替物の引渡し又は不足分の引渡しによる履行の追完を請求することができる。ただし、統計センターの責めに帰すべき事由によるものであるときは履行の追完の請求をすることができない。

② 成果物が契約の内容に適合しない場合（統計センターの責めに帰すべき事由によるものであるときを除く。）、統計センターは、相当な期間を定め、履行の追完を催告できる。

③ 統計センターが、相当の期間を定めて履行の追完を催告し、その期間内に履行の追完がないときは、統計センターは、その不適合の程度に応じて代金の減額を請求することができる。

④ 前項の規定にかかわらず、次に掲げる場合には、統計センターは同項の催告をすることなく、直ちに代金の減額を請求することができる。

（ア）履行の追完が不能であるとき。

（イ）請負者が履行の追完を拒絶する意思を明確に表示したとき。

（ウ）請負者が履行の追完をしないで仕様書等に定める時期を経過したとき。

（エ）（ア）から（ウ）に掲げる場合のほか、統計センターが②の催告をしても履行の追完を受ける見込みがないことが明らかであるとき。

⑤ 統計センターが、履行の追完を請求した場合で、履行の追完期間中成果物を使用できなかったときは、統計センターは、本契約の契約書の「納入期限の猶予」の規定に準じて計算した金額を請負者に対し請求することができる。

⑥ 統計センターが、②に規定する催告をし、その期間内に履行の追完がないとき、統計センターは、この契約を解除することができる。ただし、その期間を経過したときにおける債務の不履行が軽微であるときは、この限りでない。

⑦ 統計センターが前項に基づき解除した場合、請負者は、統計センターに対し、本契約の契約書の「違約金」の規定による違約金を支払うものとする。ただし、統計センターは返還すべき成果物が既にその用に供せられていたとしても、これにより受けた利益を返還しないものとする。

⑧ 統計センターは、成果物が契約の内容に適合しないことより生じた直接及び間接の損害について、請負者に対してその賠償を請求することができ

る。ただし、本契約の契約書の「違約金」の規定による違約金が生じたときは、統計センターに生じた直接及び間接の損害の額が、違約金の額を超過する場合において、統計センター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ものとする。

⑨　①の規定により統計センターが履行の追完の請求をした場合、請負者は、統計センターに不相当な負担を課するものでないときは、あらかじめ統計センターの承認を得ることで統計センターが請求した方法と異なる方法による履行の追完をすることができる。

⑩　統計センターが、成果物が契約の内容に適合しないことを知ったときは、その不適合を知った日から1年以内に請負者に対して通知しないときは、統計センターはその不適合を理由として、履行の追完の請求、代金の減額の請求、損害賠償の請求及び契約の解除をすることができない。ただし、請負者が引渡しの時にその不適合を知り、又は重大な過失によって知らなかったときは、この限りでない。

⑪　①の規定に基づく履行の追完については、性質の許す限り、本契約の各条項を準用する。

⑫　①の規定に基づき履行の追完がされ、再度引き渡された成果物に、なお本条の規定を準用する。

⑬　①の追完に必要な一切の費用は、請負者の負担とする。

9.3　納品検査

①　検査時期

（ア）納品検査は、全ての調達機器が引き渡し可能となった時点において行う。

②　検査内容

（ア）納品検査は、本仕様書に基づき、主管課の立会いの下で実施する。

③　検査結果

（ア）納品検査の結果、不合格と判断された場合は、請負者の負担と責任において遅滞なく、機器の交換、設定変更等の必要な措置を講じ正常な状態に復した上、納品期限までに再検査を受けなければならない。

（イ）監督及び検査を実施する統計センター職員は以下のとおり。

(1)　監督職員

- 役職：統計センター情報システム部情報システム基盤課LAN運用係長
- 氏名：山口　一也

(2)　検査職員

- 役職：統計センター情報システム部情報システム基盤課課長代理

（基盤担当）
・　氏名：木崎　夏美

10.　入札参加資格に関する事項

10.1 競争参加資格

①　「入札説明書」に示す。

10.2 公的な資格及び認証等の取得

①　請負者は、以下の認証を取得していること。

（ア）本業務を実施予定の組織・部門がISO9001の認証を取得している、または同等以上の対策を実施していること。

（イ）本業務を実施予定の組織・部門がISO27001の認証を取得している、または同等以上の対策を実施していること。

10.3 受注実績

①　過去5年間で、次期情報システム基盤と同等規模（ユーザ規模1,000人）以上の情報システムにおける設計・構築業務のプロジェクト実施を請け負った実績があること。

②　仮想サーバ及び仮想PCを用いた情報システムにおける設計・構築業務のプロジェクト実施及び管理業務を請負った実績があること。

③　クラウドサービスを用いた情報システムにおける設計・構築業務のプロジェクト実施及び管理業務を請負った実績があること。

④　データセンターを含む複数拠点間を結ぶネットワークの構築を請け負った実績があること。

10.4 複数事業者による共同提案

①　複数の事業者が共同提案する場合、全体の意思決定及び運営管理等に責任を持つ共同提案の代表者を定めるとともに、代表者が本調達に係る連絡調整等を行うこと。

②　代表者を中心に各共同提案者が協力して本業務を遂行すること。

③　各共同提案者間の調整は、その当事者となる事業者間において行うとともに、各事業者間でトラブルが発生した場合には、当該事業者間で解決すること。なお、共同提案を構成する事業者間においては、その結成及び運営等について協定を締結すること。

④　共同提案する全ての事業者が、「10.2公的な資格及び認証等の取得」及び「10.3受注実績」を満たすこと。なお、1つの事業者が本調達において、複数の提案及び複数の共同提案を行うことは認めない。

10.5 入札制限

① 各調達の調達仕様書の作成に直接関与した事業者

（ア）各調達における調達仕様書の作成に直接関与した事業者は、透明性及び公正性の確保の観点から、本調達の入札に参加させないものとする。

② CIO補佐官及び支援スタッフ等の属する事業者

（ア）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年法律第224号）に基づき交流採用された職員を除く。）による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（以下「妥当性確認等」という。）について、透明性及び公平性の確保の観点から、CIO補佐官等が現に属するまたは過去2年間に属していた事業者及びその関連する事業者については、CIO補佐官等が妥当性確認等を行う調達案件（当該CIO補佐官等が過去に行ったものを含む。）の入札に参加させないものとする。

（イ）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。）についても、当該CIO補佐官等が妥当性確認等を行った調達案件の入札に参加させないものとする。

11. 再委託に関する事項

① 本業務にかかる業務の全部を再委託してはならない。ただし、必要最小限の範囲で業務の一部を他の事業者に再委託により行わせる場合には、事前に主管課の承認を得ること。

② 再委託を行う場合は、統計センターが請負者に求めるものと同水準の情報セキュリティを確保するための対策を契約に基づき再委託先に行わせること。また、再委託先に行わせた情報セキュリティ対策及びこれを行わせた結果に関する報告を、請負者に求める場合がある。

③ 請負者は、再委託した業務に関し、統計センターに対して全ての責任を負うものとする。

12. その他特記事項

① 本仕様書内の「可能であること」、「できること」等の表記に関しては、追加費用を要することなく各機能及び要件を満たせること。また、「統計センターと協議の上」等の表記に関しては、原則として統計センターの意向を尊重すること。

② 要員は、定められた場所以外に無断で立ち入ってはならない。また、身分証明書を携行するとともに、業務中は名札等を着用すること。

③　総務省第二庁舎の施設、物品等を滅失または毀損させた場合は、請負者の負担と責任において速やかに原状回復させる等の措置を講じること。
④　本契約満了まで統計センター等から調達機器（統計センターが用意する機器を除く。）に関する問い合わせがあった場合、対応すること。
⑤　本業務の実施に伴う疑義が生じた場合及び本仕様書に記載のない事項については、その都度主管課と協議して決定するものとし、質疑及び協議の結果はその都度、文書またはメールにて提出すること。
⑥　請負者は、現地調査等を行う場合、現行情報システム基盤のシステム運用業務に支障をきたさないようにすること。
⑦　必要に応じて、現行保守事業者、現行運用事業者、複合機事業者、関係事業者等と連携して本業務を行うこと。なお、主管課の指示に従い、情報提供を行うこと。

13.　附属文書

①　別添1　要件定義書
②　別添2　次期情報システム基盤概要構成図
③　別添3　移行対象一覧
④　別添4　運用管理業務一覧
⑤　別添5　運用におけるサービスレベル目標
⑥　別添6　従来の実施状況に関する情報の開示
⑦　別添7　業務フロー図
⑧　別添8　統計センター組織図
⑨　別添9　情報保護・管理要領
⑩　別添10　提案依頼書

14.　資料の閲覧

①　入札に参加を希望する者は入札公告期間中に、本調達の仕様を理解するため、必ず以下の資料を閲覧し理解すること。また、現行情報システム基盤の構成等、提案するにあたり必要となる事項について主管課の説明を受け、内容を把握すること。なお、提案時に必要な書類の一部として、その実施記録を提出すること。

（ア）現行情報システム基盤の設計書
（イ）現有ソフトウェア一覧
（ウ）現行情報システム基盤の運用業務に関する報告資料
（エ）運用管理規則
（オ）情報セキュリティポリシー　　等

②　入札を希望する者は、入札公告期間中（土曜日、日曜日、国民の祝日及び

年末年始（12月29日から1月3日）を除く午前9時30分から午後6時00分まで）に事前連絡の上、閲覧すること。

独立行政法人統計センター
情報システム基盤の構築
及びサービス提供業務

別添１
要件定義書

目次

1. 機能要件

Microsoft365 E3を導入し、メールやイントラネットのポータルサイト、外部とのファイル共有等には、Microsoft365のクラウドサービスを利用することを前提とする。下記の要件でMicrosoftクラウドサービスの利用を想定する部分には、特にその旨を記載する。

1.1 ユーザ提供機能

1.1.1 メール

① メール

本機能はMicrosoft365で提供される、Exchange Onlineを用いて実現することを想定している。

（ア）情報系メール機能からの中継または政府共通ネットワーク経由でのメールを送受信できること。

（イ）当該機能を利用するメールクライアントはMicrosoft Outlookとすること。

（ウ）特定の拡張子が添付されたメールの送受信を制限できること。なお、特定の拡張子については主管課と協議の上、決定すること。

（エ）ユーザ1人当たりの容量は1GB以上とすること。

（オ）ユーザごとにメール転送を制限できること。

（カ）長期休暇等によるユーザの不在時に自動応答のメールを送信できること。

（キ）1通当たりの送受信容量を制限できること。

（ク）ユーザごとにメールボックスの容量を制限できること。

（ケ）ユーザのメールボックスがしきい値を超過した場合、ユーザに対して警告メール等により通知できること。

（コ）システム管理用インターフェースとしてGUIを提供すること。

（サ）ユーザの氏名等によりメールアドレスを検索できること。

（シ）メールのログイン時に主体認証を行うこと。その際、Microsoft365が提供する認証機能と連携し、シングルサインオンが実現できること。

② メール無害化及び誤送信防止

本機能は「①メール」機能と連動して動作し、外部からメール受信時のメールの無害化及び送信時の誤送信防止を実現すること。

本機能はオンプレミスで動作するメールセキュリティ製品の組み合わせで実現することを想定している。

（ア）メールはExchange Onlineで受信し、オンプレミスで動作するメールセキュリティ製品に転送した上で、以下に示すフィルタリング及び無害化の処理を行い、「1.1.1①メール」に中継できること。

（イ）受信したメールを無害化専用製品と連携し、以下の方法で無害化できるこ

と。なお、マクロ除去、OLEオブジェクト等の削除のみの提案は不可とする。
(1) 添付ファイルを識別し、ファイルの形式に合わせて、マクロ、OLEオブジェクト等を削除してファイルを再構成すること。

（ウ）以下の添付ファイルについて、無害化できること。
(1) Microsoft Office 文書（Word ファイル、Excel ファイル及び PowerPoint ファイル）
(2) PDF 形式ファイル
(3) 画像ファイル（PNG 及び JPEG を含む。）
(4) ZIP 圧縮ファイル
(5) 一太郎ファイル

（エ）添付ファイルがZIPパスワードロックされている場合でも、ユーザが管理画面上でパスワードを入力することで無害化が可能なこと。
（オ）無害化したメールの原本は、オンプレミスに構築するExchangeサーバに転送し、保存の上、閲覧できる手段を提供すること。
（カ）メールクライアント（Outlookを想定）に既存のアドオン「不審メール報告ボタン」及び「誤送信防止」を移行すること。また、運用期間中は、既存のアドオンと同等の機能を追加費用なしに利用できること。
（キ）メール送信の条件（外部への送信、添付ファイルの有無、送信元メールアドレス等）により、送信の前にメール無害化製品等の機能によって、以下の誤送信防止のための対策が実施できること。
(1) 組織内部への即時送信及び組織外部への遅延送信を実現できること。
(2) 上長等によるクロスチェックができること。

（ク）誤送信防止のために上長等によるクロスチェックを行うための機能を利用する際に主体認証を行うこと。本機能は複数のメールアドレスを持つユーザがログインし、利用する運用を想定している。ユーザ及び運用管理の観点で利便性が向上する提案をすることが望ましい。
（ケ）システム管理用インターフェースとしてGUIを提供すること。

1.1.2 スケジュール管理

本機能はMicrosoft365 で提供される、Exchange Online を用いて実現することを想定している。

① メールクライアントを用いて、ユーザが各自のスケジュールを容易に閲覧、登録、変更、削除及び共有できること。

② 同一グループ内でユーザのスケジュールを一覧で表示できることに加え、ユーザが一覧表示する対象を設定できること。
③ スケジュールの公開及び非公開を設定できること。なお、スケジュールを公開する場合、公開するユーザの設定及び管理できること。
④ スケジュールは、1日、1週間及び1ヶ月単位で表示できること。
⑤ 定期的なスケジュールを登録できること。
⑥ スケジュールの開始前にメール等で事前通知できること。

1.1.3 仮想PC及びアプリケーション配信

本機能はオンプレミスに構築されることを想定している。

① 仮想PC管理

（ア）ユーザが、本調達で導入するPC及び「1.1.4②テレワーク用アプリケーション接続」を利用するPCから、ネットワークを経由し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）有線LANまたは無線LANのどちらを利用する場合も仮想PCを利用できること。
（ウ）画面の転送データは、暗号化及び自動圧縮できること。
（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を調整できること。
（オ）画面転送プロトコルは、Blast、HDXまたはICAとすること。
（カ）仮想デスクトップの提供方式は、１つのWindows OSを単一セッションで画面転送するVDI方式及び１つのWindows OSを複数のユーザでセッション共有して画面転送するSBC(RDSH)方式が選択可能なこと。
（キ）「11.2⑤仮想PC（RDSH）用仮想化基盤」、「11.2⑥仮想PC（VDI）用仮想化基盤」及び「11.2⑦集計業務用PC用仮想化基盤」等の基盤上で稼動する仮想PCを管理できること。
（ク）仮想PCを特定のユーザ専用に割当てできること。
（ケ）同時に複数の仮想PCを作成しユーザを接続順に割当てできること。
（コ）ユーザに仮想PCを割当てる際には、仮想ハードディスクに格納されたユーザプロファイルを切り替えることで高速に割当て可能な方式とすること。
（サ）仮想PC環境におけるマスタPCのOS及びアプリケーションにパッチ等の適用を行った場合、マスタPCから複製した仮想PCに反映できること。
（シ）仮想デスクトップ環境でMicrosoft Teamsの最適化に対応し、エンドポイント端末から直接Teamsクラウド上にオーディオ/ビデオ通信をすることにより仮想デスクトップ側の負荷を軽減できる機能を有すること。
（ス）特定のURL、IPアドレスに該当するコンテンツへのリンクをクリックした際に、仮想PC上のブラウザにて当該コンテンツを開く機能を有すること。

（セ）特定のファイルへのリンクをクリックした際に、一般事務用ネットワークの仮想PC上で、自動的に集計業務用仮想PCが立ち上がり、集計業務用ネットワークのファイルを開く機能を有すること。
（ソ）仮想デスクトップクライアントソフトウェアのエラーメッセージには任意の文字列を表示できることが望ましい。

② アプリケーション配信1
（ア）「1.1.3①仮想PC管理」におけるイメージパターンの削減に努めること。なお、当該機能を利用せずイメージパターンを削減する方法がある場合、提案すること。
（イ）仮想PCに対し、アプリケーションを「11.2⑤(ケ)(2)一般事務用仮想アプリケーション配信用仮想PC」で実行し、画面のみ仮想PCに配信する方式でアプリケーションを配信すること。

③ アプリケーション配信2
（ア）「1.1.3②アプリケーション配信1」における(ア)の機能を有すること。
（イ）仮想PCに対し、アプリケーションを差分ディスクとして配信し、仮想PCのOSで実行する方式でアプリケーションを配信すること。

1.1.4 テレワーク
① インターネットからのリモートアクセス
本機能はZTNAを実現するクラウドサービスを用いて実現することを想定している。
（ア）SaaS型の提供であること。
（イ）インターネット経由で本調達の中で用意するデータセンターへ接続できること。
（ウ）端末とリモートアクセス先が直接IP到達可能でなくてもリモートアクセスを行うことができること。
（エ）本調達の中で用意するデータセンターや統計センターの拠点に攻撃境界面がない構成であること。
（オ）日本国内に接続先があること。また、接続先は複数であることが望ましい。
（カ）クライアント端末から自動で近い接続先を選択して利用する仕組みを有すること。
（キ）障害発生時は、クライアント端末から自動または再接続により次に近い他の接続先を選択して利用する仕組みを有すること。
（ク）ISMAPを取得しているまたは既に申請済みであること。
（ケ）サービス契約終了後はデータ消去が行われること。

(コ) クラウド上のログデータは暗号化されて保存されていること。
(サ) IdPとSAML連携できること。また、複数のIdPを利用できることが望ましい。
(シ) SAMLのユーザ属性からアクセス制御できること。
(ス) アプリケーションはHTTP/HTTPS(80,443)以外のTCP/UDPでも利用可能なこと。
(セ) ユーザからアクセス可能なアプリケーションを制御できること。
(ソ) ユーザ端末の持つ証明書によりアクセス制御できること。
(タ) 社内/社外を判定しアクセス先を制御する仕組みを有すること。
(チ) 「1.2.3②ログ保管」にログ送付可能なこと。
(ツ) Windowsログイン前に特定のサーバへ通信可能な機能を有すること。
(テ) リモートアクセスのために拠点内に配置するソフトウェア（コネクタ）を使用する場合は接続するアプリケーションの数で制限がないこと。
(ト) リモートアクセスのために拠点内に配置するソフトウェア（コネクタ）を使用する場合のアップデートの時間帯を設定できること。
(ナ) リモートアクセスのために拠点内に配置するソフトウェア（コネクタ）を使用する場合のアップデートはアプリへのアクセスを維持しつつ自動で可能なこと。
(ニ) リモートアクセスのため拠点内に配置するソフトウェア（コネクタ）を使用する場合の死活監視が行えること。
(ヌ) リモートアクセスのため拠点内に配置するソフトウェア（コネクタ）を使用する場合、それが停止したとき、同一グループに指定している他のコネクタに自動で切り替わること（リモートアクセスが維持できること)。
(ネ) アクセスに用いるクライアントエージェント及びコネクタを自動でアップデートできること。
(ノ) 管理コンソール上で、リアルタイムにユーザのアクセス状況が確認できること。
(ハ) 管理コンソール上で、利用されているクライアントエージェントのバージョンが確認できること。
(ヒ) 障害発生時の調査のためのリモートアクセス機能を有すること。
(フ) 障害発生時の調査のため、パケットまたはトラフィックログを取得する機能を有すること。
(ヘ) 他サービス契約者のトラフィックによる影響を受けないよう、サービス契約者間で共有されるリソースではなく、契約ごとに専用リソースが提供されることが望ましい。
(ホ) 一人のリモートユーザが複数のデバイスを保有している場合でも追加ライセンスが不要で同時に接続できることが望ましい。

② テレワーク用アプリケーション接続

（ア）「1.1.4①インターネットからのリモートアクセス」を介して、「1.1.3①仮想PC管理」等の次期情報システム基盤が提供するアプリケーションに接続し、リモートアクセスできること。

（イ）「1.1.3①仮想PC管理」以外に接続するアプリケーションは、リモートメンテナンスのためのサービス、ファイル転送サービスを想定している。

（ウ）接続するアプリケーションは、接続する回線により使い分けができること。

③ テレワーク用端末

（ア）本調達で導入するノート型PC、USBシンクライアント及び統計センターが用意する機器のノート型PCをテレワーク用の端末として利用できること。

（イ）本調達で導入するノート型PC、USBシンクライアント及び統計センターが用意する機器のノート型PC には、クライアント証明書を導入すること。また、クライアント証明書は1台ごとに異なること。

（ウ）本調達で導入するノート型PC、USBシンクライアント及び統計センターが用意する機器のノート型PC は、テレワーク時のオンライン会議の通信をインターネットブレイクアウトできることが望ましい。

1.1.5 リモートアクセス

本機能はオンプレミスに構築されることを想定している。

① 政府共通ネットワークを介して、他の中央省庁及び独立行政法人の職員が「11.2②(キ)(15)リモートアクセス用サーバ」を介して接続し、「11.2⑦集計業務用PC用仮想化基盤」及び「仮想PC（VDI）用仮想化基盤」に構築されたリモートアクセスユーザ向けの仮想PCを利用できること。

② 「1.3.1③ワンタイムパスワードトークン認証」を用いた主体認証を行うこと。

③ 端末に専用のアプリケーションを導入せず、Webブラウザ（Microsoft Edge及びGoogle Chrome）を用いて「11.2②(キ)(15)リモートアクセス用サーバ」に接続できること。

④ HTTPS通信のみで「11.2②(キ)(15)リモートアクセス用サーバ」に接続できること。

⑤ Webブラウザを用いたファイルのアップロードができること。その際、1ファイル当たり1.99GBまでサポートすること。なお、1.99GB以上のファイルについてもアップロード可能とする提案を行うことが望ましい。

1.1.6 Web会議

① 統計センター外部向けWeb会議

（ア）以下のサービスについて、指定のライセンスを導入すること。
(1) Zoom business（10 ライセンス）
(2) WebEx エンタープライズ(10 ライセンス)

1.1.7　在席管理及びWeb会議

本機能はMicrosoft365 で提供されるTeams を用いて実現することを想定している。

①　在席管理

（ア）ユーザの在席管理ができること。
（イ）メールクライアントと連携して、ユーザの在席状況を確認できること。
（ウ）在席状況は、アイコン及び文字の情報を使用して視覚的にわかりやすく表示されること。
（エ）在席状況は、手動で変更できること。
（オ）在席、不在のステータスでユーザの在席状況を確認できること。

②　統計センター内部向けWeb会議

（ア）統計センター内部のネットワークを通じて映像及び音声をやり取りできること。
（イ）会議の開催中に参加者間で資料の受け渡しができること。
（ウ）会議参加者全員がファイルを展開、共有及び閲覧する機能を有すること。
（エ）会議参加者全員が閲覧及び書き込みが行えるホワイトボード機能を有すること。
（オ）会議の開催及びメンバーの指定、招集等ができること。
（カ）テキストによりメッセージを共有及び送信できること。
（キ）在席表示されているユーザをクリックすることで、Web会議サービスを起動できること。
（ク）全てのユーザに会議を主催できる個別のIDを付与できること。
（ケ）利用状況のログを月ごとに取得できること。

1.1.8　ファイル共有

本機能はオンプレミスに構築されるファイルサーバにて実現されることを想定している。

①　ファイル保管機能

（ア）ユーザが仮想PCを利用して、ファイルを保管できること。
（イ）ユーザによりフォルダを作成できること。
（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。
（エ）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PCへの

ログイン時に自動で割当てできること。
（オ）仮想PCのユーザ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。
（カ）仮想PCで用いるプロファイルを格納できること。

② アクセス権管理機能
（ア）NTFSによりフォルダ及びファイルへのアクセス権を設定できること。
（イ）ユーザごとにアクセス権を設定し、アクセス制御できること。
（ウ）アクセス制御はフォルダ単位及びファイル単位で作成、参照、更新及び削除を管理できること。
（エ）共有フォルダは、ユーザ単位及びユーザをまとめたグループ単位でアクセス権を設定できること。
（オ）個人用フォルダは、ユーザ単位で作成され、他のユーザによるアクセスを排除できること。
（カ）ユーザ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。
（キ）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。

③ 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しきい値が設定できかつ容量がしきい値に達した際は、システム管理者へ通知できること。

④ ファイル復旧機能
（ア）ユーザが誤ってデータを削除した場合に、ユーザ自身が手順に従い、スナップショットを取得した時点まで当該データを復元できること。

⑤ 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を検索できること。

1.1.9 会議室予約
本機能は、Rwin会議室予約システムを導入し、実現することを想定している。
① 以下の機能を充足すること。
（ア）会議室予約を利用者がスケジュールに取り込めること。
（イ）管理者によるcsv予約できること。
（ウ）管理者による一括予約・キャンセルできること。
（エ）管理者が予約・キャンセルした場合に関係する利用者へ予約・キャンセル

の完了通知メールが送れること。
（オ）会議室利用者へのリマインドができること（例えば15分前にメール通知等）。

1.1.10 ファイル転送

① インターネット回線を経由したファイル転送

本機能はMicrosoft365で提供されるSharePoint Onlineを用いて実現することを想定している。
（ア）Webブラウザを介して、ファイルを授受できること。
（イ）ファイル転送の履歴を記録及び保存できること。
（ウ）ユーザ単位でファイルのアクセス権を設定できること。
（エ）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。
（オ）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。
（カ）外部利用者に対してもセキュリティを確保した形でファイル共有できる機能を提供すること。
（キ）本機能はMicrosoft365で提供されるSharePoint Onlineを用いて実現することを想定している。

② 政府共通ネットワークに向けたファイル転送

本機能はオンプレミスに構築することを想定している。
（ア）Webブラウザを介して、ファイルを授受できること。
（イ）ファイル転送の履歴を記録及び保存できること。
（ウ）ユーザ単位でファイルのアクセス権を設定できること。
（エ）ユーザ単位で授受を行うファイルの容量を制限できること。
（オ）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。
（カ）ユーザ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。
（キ）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。
（ク）「1.3.1③ワンタイムパスワードトークン認証」を用いた主体認証を行うこと。
（ケ）統計センターの職員等は本機能をシングルサインオンで利用できること。

1.1.11 申請のオンライン受付及び各種運用手続きのワークフロー管理

本機能はワークフロー製品を導入しExcel形式の申請書からWebフォームへの申請方法に変更する、ユーザからサービスデスク問い合わせに対応する等、システム運用管理をオンライン化して、運用手続きを効率化することを目的としている。ただし、人事異動、非常勤職員の採用等に伴うアカウントの払出・変更・削除に関する申請は、「1.2.7③アカウント管理に関するワークフロー」を利用する

ものとする。
なお、本機能はISMAPに登録されたクラウドサービスにより実現することを想定している。

① ローコード開発

（ア）Excelによる申請書をWebフォーム化するにあたり、プログラム等の特別なスキルを必要とすることなくGUIで申請書等を作成可能であること。
（イ）Excelからのフォームの取り込みが可能であること。

② 拡張機能（プラグイン等）

（ア）特定の項目へ値を入力すると特定の表からデータを参照し他の項目へ自動で値が入力される機能を有すること。
（イ）入力フォームの表示制御ができること。
（例）特定の質問項目に回答すると次の回答項目を非表示にする等。
（ウ）データを一括更新できること。
（例）承認者が一つ一つ申請を承認することなく一括で承認できる機能
（エ）他社が開発した拡張機能と連携ができること。
（オ）導入にあたっては、以下の拡張機能を導入すること。
(1) アカウントがない人でも WEB フォームからデータ登録できること。ただし利用できる IP アドレス制限ができること。
(2) アカウントを持たないユーザにも情報公開を可能とする機能を有すること。ただし利用できる IP アドレス制限ができること。
(3) 登録しているメールアドレス宛に、 システム内のデータを自動引用したメールを自動・予約・手動で送ることができること。その際、システム内のデータ更新に連動した自動メール送信ができること。

③ Webフォームによる申請

（ア）作成したフォームから利用者が申請できること。なお、申請書が提出された際にメールで通知が可能であること。

④ データの一元管理

（ア）利用者から申請されたデータをデータベース等に登録し一元的に管理できること。

⑤ プロセス管理

（ア）申請書の受付、承認処理等、一連の処理ができること。申請不備があった場合に利用者と連絡するコミュニケーション機能があること

⑥ CSVファイルによるエクスポート及びインポート機能

（ア）提出されたデータをCSVファイルによりエクスポートできること。
（イ）CSVファイルをインポートすることでデータベース等へ一括でデータを登録できること。申請書の受付及び承認処理等、一連の処理ができること。

⑦　想定利用者
（ア）本機能は約80名の利用者を想定している。

1.2　システム運用機能

1.2.1　仮想化基盤管理

本機能のうち、仮想化基盤そのものはオンプレミスに構築し、運用管理に関する機能についてクラウドサービスとして実現することを想定している。ただし、詳細な製品構成やライセンス形態については、実現方法を検討の上、提案すること。

①　仮想化基盤
（ア）サーバをハイパーバイザーにより仮想化すること。なお、仮想サーバを追加した場合に追加ライセンスが不要であること。
（イ）全てのサーバを一括管理できること。ただし、「11.2⑤仮想PC（RDSH）用仮想化基盤」は含まない。
（ウ）仮想サーバの電源管理及びリソースの割当てをできること。
（エ）仮想サーバをテンプレート化し複製できること。
（オ）VLANによる仮想ネットワークを構築できること。
（カ）管理対象の物理サーバに障害が発生した場合に別の物理サーバに切り替えできること。
（キ）物理サーバのメンテナンス時に、仮想サーバを稼動させた状態で別の物理サーバに移動できること。
（ク）物理サーバ間のCPU負荷を自動的に平準化する機能を有すること。また、特定の仮想化サーバに負荷が集中し、そのサーバ上で稼働する仮想マシンのサービスレベルが低下する場合、自動的に異なる仮想化サーバへ一部の仮想マシンを稼働させたまま移行する機能を有すること。なお、移行する際には、仮想マシングループを指定することで、特定の仮想マシンの組み合わせを同一のホスト上に移行させる設定や、同一のホストに移行させない設定が可能なことが望ましい。
（ケ）仮想サーバの配置についてアフィニティルールを設定できること。
（コ）原則として、仮想化ベースのセキュリティ対策（VBS）を有効化すること。
（サ）仮想マシンの作成などで、ストレージ領域を割当てる際に発生するゼロデータ書き込みの処理をストレージシステム側で実行できることが望ましい。

② 仮想化基盤運用管理

（ア）SaaS版で提供可能なことが望ましい。

（イ）仮想サーバのパフォーマンス情報を5分間間隔で収集した値を5日間以上、2時間間隔で収集した値を1ヶ月間、1日間隔で集計した値を5年間保持できること。

（ウ）仮想化基盤の稼働状況（死活監視、イベント監視等）を監視できること。

（エ）障害を検知した場合は、メール等で通知できること。

（オ）仮想化基盤上に仮想サーバとして構築できること。

（カ）仮想化基盤、仮想サーバ、仮想PCサーバ及び仮想PC管理サーバを監視できること。

（キ）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。

（ク）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。

（ケ）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。

（コ）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が制限できること。なお、利用用途に応じた操作権限及び閲覧権限をユーザ単位に設定できること。

（サ）Webブラウザから監視できること。

（シ）使用率、トラフィック情報、アラーム、イベント、インベントリ情報等のデータを出力できること。

（ス）仮想化基盤の動作の条件に「1.3.1①ディレクトリ」を必要としないこと。

（セ）仮想化基盤及びストレージのリソース使用状況から、将来的に必要なリソース量及び必要時期を算出できること。

（ソ）各仮想マシンのリソース使用状況から、リソース割当て過不足の状態及び推奨スペックを自動的に算出、表示できることが望ましい。

（タ）仮想基盤の現状のキャパシティを分析し仮想サーバの増設シナリオを検証、もしくは余剰リソースの検証が可能なことが望ましい。

（チ）監視ツールは、目的や用途に応じて監視項目の異なる画面を作成する事ができる事。なお監視項目には仮想デスクトップに関する項目も含めることができ、本システム運用期間中に必要に応じて変更が可能な事が望ましい。

1.2.2 構成管理

① Windows向け構成管理

本機能は以下の製品を用いて実現することを想定している。

Windows Server: Microsoft Endpoint Configuration Manager (MECM)

Windows PC: 物理 PC の管理に必要なソフトウェアを提供すること。

（ア）サーバ及び端末から構成情報を自動収集し、一元管理できること。
（イ）リモート操作によりアプリケーションをインストールできること。
（ウ）Microsoft Updateと連携し、セキュリティ更新プログラムを展開できること。
（エ）セキュリティ更新プログラムの展開（必須プログラムの検出及び配信）できること。
（オ）ウイルス定義ファイルの配信及び感染状況のレポートをできること。
（カ）次期情報システム基盤のネットワークを介してOSイメージを展開できること。
（キ）仮想PCのマスタPCに対して、ソフトウェア更新プログラムを自動的に適用できること。
（ク）特定のレジストリ値及びファイルの存在を望ましい状態として定義し、管理対象とする機器（サーバ、PC等）の望ましい状態との乖離を確認できること。また、必要に応じて管理対象とする機器（サーバ、PC等）を望ましい状態に自動修復できること。
（ケ）ソフトウェアライセンスの購買情報及び実際のインストール数を比較し、レポートできること。
（コ）シンクライアントPCとして運用した場合（Unified Write Filter）においても、セキュリティパッチを適用できること。
（サ）管理対象とする機器（サーバ、PC等）にソフトウェアを夜間自動配信できること。
（シ）管理対象とする機器（サーバ、PC等）のディスクイメージ配布時におけるWAN回線に対する通信量の削減に配慮した設計をすること。
（ス）管理対象とする機器（サーバ、PC等）の初期セットアップを可能な限り自動化できることが望ましい。その際、Windows仮想サーバの初期セットアップについて、自動化できない部分を明確化し手順化すること。
（セ）統計センターに設置するWindows PCに更新プログラムを適用する場合に、WAN回線及びインターネット回線を占有しないように設計すること。

② Linux向け構成管理

Linux のセキュリティパッチ適用及び構成管理の方法については、下記の要件を満たす方法を提案すること。

（ア）サーバ及び端末から構成情報を自動収集し、一元管理できること。
（イ）脆弱性を含むソフトウェアを検知できること。
（ウ）脆弱性を含むソフトウェアのセキュリティ更新プログラムを展開できること。
（エ）管理対象とする機器（サーバ、PC等）の初期セットアップを可能な限り自動化できることが望ましい。その際、Linux仮想サーバの初期セットアッ

プについて、自動化できない部分を明確化し手順化すること。

1.2.3　ログ取得・管理

①　統合ログ取得

本機能はSIEMソリューションを導入することで実現することを想定している。機能の過不足があれば、提案すること。

（ア）以下のログを取得することを想定している。ただし、他機能で収集するログも存在するため、詳細は設計にて決定すること。

(1)　主体認証ログ
(2)　プロキシに関するログ
(3)　DHCPに関するログ
(4)　Active Directory操作ログ
(5)　ファイアウォールのログ
(6)　「1.3.8メールセキュリティ対策」及び「1.1.1②メール無害化及び誤送信防止」からのログ
(7)　無線IDSのログ
(8)　Microsoft365クラウドサービスからのログ
(9)　ホームページ基盤からのログ

（イ）ログの保管期間は、1年間以上とすること。
（ウ）取得するログの容量は、1日当たり10GB以下とすること。
（エ）収集したログ情報は、リアルタイムで検索し、閲覧できること。
（オ）収集したログ情報を相関分析できること。
（カ）時系列にイベントを配列できること。
（キ）あらゆるイベントの時間を自動的に特定できること。なお、タイムスタンプがない場合でもタイムスタンプを推測できること。
（ク）ログを監視し、異常があればメールにより自動で通知できること。
（ケ）ログ情報をグラフ及びチャートとして、出力できること。
（コ）調達機器に保存されたログが改ざんされた場合においても、ログを取得・管理するサーバへの影響がない構成とすること。
（サ）設計時に、システム変更に応じてルール及びアラートの見直しを行い、編集を行うこと。

②　ログ保管

（ア）統計センターLANを構成するサーバ、ネットワーク機器、アプライアンス機器及びクラウドサービスのログ情報を自動的に収集・保存すること。また、これらの機器のログ収集に必要な台数のサーバを構成すること。

（イ）収集したログ情報は、閲覧や検索ができること。
（ウ）ログデータは、5年以上の長期保管ができること。
（エ）収集したログから、日、週、月ごと等でレポートを出力することが可能であること。
（オ）集計した結果は、PDF、HTML、CSV形式等の主管課がわかりやすい形式で提出されること。
（カ）正規表現を用いたログの検索が可能であること。
（キ）ログの改ざんを検出する仕組みを持つこと。
（ク）ログデータを暗号化して保存できること。
（ケ）ログデータは常に圧縮された状態で保管・管理できること。
（コ）Windowsイベントログを収集する機能を有し、さらにログの内容をわかりやすい内容に解析する機能を有すること。
（サ）採用する仮想化基盤のログをエージェントレスで収集する機能を有すること。
（シ）ログを暗号化/圧縮し送信するログ送信ツールを有すること。
（ス）Windowsイベントログを収集する機能を有し、さらにログの内容をわかりやすい内容に解析する機能を有すること。
（セ）市販のRDB製品を用意する必要なく、独自DBによりログを管理可能であること。
（ソ）製品ライセンスの制限により、上限を超えたログが欠落または収集停止するライセンス体系ではないこと。
（タ）収集したログのうち、任意に選択する機器のログを自動的に他のサービスに転送が可能であること。

1.2.4　監視

①　共通要件

（ア）各収集項目を5分間間隔で収集した値を5日間以上、2時間間隔で収集した値を1ヶ月、1日間隔で集計した値を5年間保持できるように設計すること。
（イ）レポート機能として、日次レポート、週次レポート及び月次レポートを作成できること。
（ウ）収集した項目をCSV形式でエクスポートできること。
（エ）夜間連絡用のメール通知については、障害が1時間継続した場合に限り通知すること。

②　ネットワーク及びLinuxサーバ監視

本機能はオンプレミスに導入し実現することを想定している。

（ア）ネットワーク機器及びLinuxサーバに対し、以下を監視できること。

(1) 死活監視
(2) システム再起動監視
(3) ログインユーザ数監視
(4) 総プロセス数監視
(5) ネットワークトラフィック監視
(6) SNMP 監視
(7) ファイルサーバへのアクセス監視
(8) データベースのテーブルへの稼働監視

(イ) 障害検知時に以下を自動で行うこと。
(1) メールによる障害及び復旧の通知
(2) 監視サーバ上のスクリプト実行
(3) 監視エージェント上のスクリプト実行
(4) 障害継続時の繰り返し通知及びエスカレーション

(ウ) システム全体の障害状況をダッシュボード画面上に表示すること。
(エ) 複数の監視データを重ね合わせグラフを作成できること。

③ Microsoft Windows Server及びMicrosoft 365クラウドサービス監視
本機能は System Center Operations Manager を導入することを想定している。
(ア) Microsoft Windows Server及びMicrosoft製品（SQL Server等）に対し、以下を監視できること。
(1) 死活監視
(2) ログ監視
(3) 性能監視

(イ) 障害検知時にメールにより自動で通知できること。
(ウ) 監視用インターフェースとしてGUIを提供すること。
(エ) 「1.3.1①ディレクトリ」と連動して、認証、権限管理及び権限付与できること。
(オ) スクリプト、管理パック等の追加により以下の監視できること。また、ベンダーより以下の監視スクリプト、管理パック等が提供されていること。
(1) Active Directory
(2) Windows Server
(3) SQL Server
(4) Exchange Online
(5) SharePoint Online

(6) Teams

1.2.5 バックアップ

① データセンター内のデータのバックアップ

本機能はNASのバックアップ機能を用いて実現する場合と、バックアップ製品を利用して実現する場合の2つの実現方法を想定しており、性能面及び費用面を比較の上、適切な方式を提案すること。

(ア)「1.1.8ファイル共有」に保存されている全てのデータ及び「11.2⑤仮想PC（RDSH）用仮想化基盤」の仮想PCに含まれるユーザ領域のデータをバックアップ対象とできること。

(イ)バックアップデータはメインストレージと異なるストレージに格納すること。

(ウ)稼働中のサーバ及びストレージを無停止でバックアップできること。

(エ)仮想サーバ、データベース及びファイル単位でリストアできること。

(オ)システム管理用インターフェースとしてGUIを提供すること。また、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。

(カ)バックアップデータは重複排除できること。

(キ)バックアップの取得は自動化し、バックアップが失敗した際に通知できること。また、手動によるバックアップを取得できること。

(ク)イミュータブルバックアップを実現できること。

(ケ)バックアップは日次で取得できること。

(コ)バックアップ保持期間は180日あること。なお、一日あたりの更新量は1TBとする。これらを考慮し適切な容量を算出し提案すること。

(サ)バックアップ対象のうち2TBについては5年間保持できること。なお、本データの更新量は考慮不要とする。このデータについては、バックアップ製品の障害によるデータ損失に備える対策をすること。

(シ)システム全体をリストアするシナリオにおいて、1時間当たり6TBリストアできること。

(ス)バックアップサーバへのログインは多要素認証とすること。なお、バックアップサーバにWindows serverを使用する場合は、システム基盤のADと独立したAD環境（AD2台、オフラインルートCA1台、EnterpriseCA1台）を物理サーバで構築し、スマートカードログオンとすること。

(セ)バックアップ関連サーバについては、全て物理サーバで構成すること。

(ソ)仮想化基盤上の仮想サーバの数は400台としてライセンス料を算出すること。

(タ)ストレージの性能、容量及び効率化の状況をレポート出力できること。

(チ)整合性を維持した状態で無停止バックアップできること。

(ツ)バックアップ機能を提供する製品は、ランサムウェア復旧保証サービスが

提供することが望ましい。

② クラウドサービス上のデータのバックアップ

本機能はクラウドサービスにより実現することを想定している。

（ア）M365のデータをMicrosoft Azureにバックアップできること。
バックアップ対象は以下のとおりとする。

(1) Exchange Online
(2) SharePoint Online
(3) Teams
(4) Entra ID

（イ）対象データは1ユーザ当たり20GBとする。

（ウ）バックアップに必要となるMicrosoft Azureサービスについても提案に含めること。

1.2.6 特権ID管理

① 特権ID管理

本機能は、管理権限を持ったユーザのログインポリシーについて設定を行うことで実現することを想定している。

（ア）管理者権限を持ったIDユーザのログインについては、多要素認証での認証方法の追加等、ログインポリシーの厳格化を行う等の対策を実施すること。

② 特権ID不正利用検知

本機能については、オンプレミスのActive Directoryを対象とする。

（ア）ネットワーク解析エンジンを利用し、認証、承認及び情報収集を目的として複数のプロトコルにおけるネットワークトラフィックを収集及び解析できること。

（イ）ネットワーク内におけるイベント、ログ等の複数のデータソースから情報を収集し、ユーザ及び組織における他のエンティティの動作を学習し、それらについて動作プロファイルを作成できること。

（ウ）以下を例とする悪意のある攻撃を検出できること。また、当該情報を確認できること。

(1) Pass-the-Ticket (PtT)
(2) Pass-the-Hash (PtH)
(3) Overpass-the-Hash
(4) 偽造 PAC (MS14 068)
(5) ゴールデン チケット

(6) 悪意のあるレプリケーション
(7) 偵察
(8) ブルート フォース
(9) リモート実行

(エ) 以下を例とする異常な動作を検出できること。また、当該情報を確認できること。
(1) 異常なログイン
(2) 未知の脅威
(3) パスワードの共有
(4) 水平方向の活動
(5) 機密性の高いグループの変更

(オ) 以下を例とするセキュリティの問題とリスクを検出できること。また、当該情報を確認できること。
(1) 信頼関係の消失
(2) 脆弱なプロトコル
(3) 既知のプロトコルの脆弱性

③ Active Directory監査

本機能については、Active Directory監査を行うソリューションにて実現することを想定している。

(ア) オンプレミスのActive Directoryに対する監査の機能として、以下の条件を満たすこと。
(1) Active Directory に登録されている ID 数 2200 のライセンスを提供すること。なお、内部ドメインのユーザのみを対象とする。
(2) 既存の設定に脆弱な内容がないかを確認できること。
(3) 挙動を継続的に監視して脆弱な状態が発生した際はすぐに指摘できること。
(4) グループポリシーオブジェクトの問題点を指摘できること。
(5) Active Directory に対する攻撃をリアルタイムに検知できること。
(6) ドメイン間の信頼関係を図示して問題を指摘できること。
(7) ドメイン侵害につながる攻撃経路がリアルタイムで図示できること。
(8) ドメインコントローラーに Active Directory オブジェクト情報取得用エージェントソフトウェアのインストールが不要であること。
(9) 特権アカウントを使用しなくても動作可能なこと。

1.2.7　アカウント管理

本機能については、ID管理ソリューション等を利用して実現することを想定している。

①　基本機能

（ア）システム管理者がアカウント情報を管理できること。

（イ）ユーザの主所属以外に、兼務所属を複数登録・管理できること。

（ウ）グループ及びPC種別で割当てている情報をユーザの主所属または兼務所属の部署ルールまたは職務ルールによって、自動で割当て可能な機能を実装していること。

（エ）利用者画面の表示項目については、主幹課と調整し、決めることができること。

（オ）CSV形式のファイル及びデータベースからユーザ情報を取り込み、一括でメンテナンスできること。

（カ）「1.2.8シングルサインオン」と連携できること。

②　管理対象

（ア）以下の機能のアカウント管理をできること。

(1)　「11.2①(ク)(15)認証サーバ1」

(2)　「11.2①(ク)(16)認証サーバ2」

(3)　「11.2①(ク)(19)IC カード認証サーバ」

(4)　Microsoft 365 で利用する Entra ID

（イ）以下の機能のアカウント管理をできることが望ましい。

(1)　「11.2①(ク)(20)ワンタイムパスワード認証サーバ」

(2)　JP1/Automatic Job Management System3

③　アカウント管理に関するワークフロー処理

（ア）室内LAN管理担当者（補助者も含む）及びLAN運用係によるアカウント管理のワークフロー処理

(1)　システム利用者が、ユーザの登録・変更・削除及びユーザ情報の確認を行う GUI 画面があること。

(2)　システム利用者が、CSV によるユーザ情報の登録・変更・削除を一括で行う機能があること。

(3)　(1)または(2)で更新した情報を申請し、承認者による二段階の承認処理を行うことで、異動情報が確定(システムへの反映)する機能があること。

(4)　(3) の承認を得て、変更情報が確定する機能があること。

(5) 申請時に申請理由を記載するコメント欄があること。
(6) 申請が行われた場合に、承認者に対して、承認要請通知メールを送信する機能があること。
(7) 承認者が承認できないと判断した場合、再申請可能（差し戻し等）な機能があること。
(8) (7)の場合に、承認できない理由と再申請依頼を記載するコメント欄があること。
(9) 申請が承認されなかった場合に、申請者に対して、通知メールを送信する機能があること。
(10) 申請後に誤りがあった場合に、申請者が誤った申請の取り下げを行い、正しく修正した内容で再申請可能な機能があること。
(11) 承認時に承認理由、アカウント開始日及び注意事項を記載するコメント欄があること。
(12) 申請が承認された場合に、申請者に対して、申請承認通知メールを送信する機能があること。
(13) 組織マスタでは組織コード、組織名称及び組織ルールを設定可能であること。
(14) 連携先システムに対して、エージェント等による直接連携またはCSV 連携により、社員マスタ(ユーザーマスタ)の更新情報を同期する機能があること。

（イ）アカウント管理の例外処理
(1) 部署、職務等の所属情報に紐づかない PC 種別情報を個別にユーザに付与する機能があること。
(2) PC 種別情報等の権限ごとに情報資産管理者を配置し、ユーザ情報の確認を行う GUI 画面があること。
(3) 室内 LAN 管理担当者（補助者も含む）または一般ユーザ（本人）が PC 種別の利用を申請し、情報資産管理者、LAN 運用係及び運用事業者の承認を得て、PC 種別情報等の各権限が付与される機能があること。
(4) 部署、職務等の所属情報に紐づかないグループ情報（係コードがないもの）を LAN 運用係または運用事業者が管理画面より変更を行うことが可能であること。
(5) 所属に紐づかない PC 種別情報の申請を第一承認を情報資産管理者が行い、第二承認を LAN 運用係、第三承認を運用事業者が行うことが可能なであること。

1.2.8 シングルサインオン

① 全般

（ア）「1.2.7アカウント管理」と連携し、次期情報システム基盤においてシングルサインオンを提供すること。

② オンプレミスで提供するシングルサインオン

本機能については、オンプレミスに導入できるシングルサインオンの製品を導入して実現することを想定している。

（ア）OSのログイン認証後、「1.1.3①仮想PC管理」、「1.3.2仮想ブラウザ」及び「1.3.2仮想ブラウザ」でのMicrosoft365アプリのログオン、「1.1.10②政府共通ネットワークに向けたファイル転送」及び「1.3.3ファイル転送及びファイル無害化」へのログイン認証にシングルサインオンが利用できること。

③ WEBシステムに提供するシングルサインオン

本機能については、対象システムがオンプレミス・クラウドのどちらで動作しているかに関わらず、以下の要件を実現できること。

（ア）WEBシステムへのログオンを代理認証（最低5システム）できること。なお、システム数に制限がないことが望ましい。

④ クラウドサービスに提供するシングルサインオン

本機能については、Entra IDの機能を利用して、実現できることを想定している。

（ア）SAML/OpenIDConnectに対応すること。

（イ）シングルサインオン時に利用するプロトコルは、HTTPSのみとすること。

1.2.9 DNS

① 内部DNS

本機能は、オンプレミスのActive Directoryの機能により実現することを想定している。

（ア）内部のIPアドレス、ドメイン名及びホスト名間の名前（アドレス）解決をできること。

（イ）名前解決にあたり、正引き及び逆引きに対応すること。

（ウ）冗長構成とし、名前解決を停止させないようにすること。

（エ）キャッシュDNS及びインターネット上のDNSにフォワードしない設定とすること。

② コンテンツDNS

本機能については、外部のクラウドサービスが提供するDNSサービスを利用

して実現することを想定している。

（ア）インターネットからの問い合わせに対し、名前解決を行うこと。

（イ）コンテンツDNSサーバは冗長構成とし、名前解決を停止させないようにすること。

（ウ）ドメイン名に関する正引き及び逆引きができること。

（エ）以下のレコードを登録すること。

(1) SPF、DKIM、DMARC 等メールセキュリティに必要なレコード

(2) ホームページ基盤に必要となるレコード

(3) クラウドサービスを利用する上で必要となるレコード

③ キャッシュDNS

本機能については、LinuxサーバにUnbound等を導入し実現することを想定している。

（ア）キャッシュDNSは次期情報システム基盤外部からの名前解決の要求には応じず、次期情報システム基盤内部からの名前解決の要求のみに回答を行うよう、キャッシュDNSの設定、ファイアウォール等でアクセス制御を行うこと。

（イ）インターネット上のDNSにフォワードすること。

（ウ）冗長構成とし、名前解決を停止させないようにすること。

（エ）DNSキャッシュポイズニング対策として、キャッシュDNSサーバがソースポートランダマイゼーション機能を有すること。

（オ）DNSを採用するにあたり、脆弱性の問題を考慮した製品を選定すること。

1.2.10 DHCP

本機能については、Windows サーバに DHCP 機能を導入することで実現することを想定している。

① DHCPプロトコルによるIPアドレス付与の機能を提供すること。

② IPアドレス付与の対象は、本調達で導入するPC及び仮想PCとすること。

③ 割当てるIPアドレスの範囲を指定できること。

④ 割当て除外IPアドレスを指定できること。

⑤ MACアドレスを指定したIPアドレスを静的付与できること。

⑥ IPアドレスのリース期間を調整できること。

⑦ システム管理用インターフェースとしてGUIを提供すること。

1.2.11 認証局

本機能については、Active Directory Certificate Servicesを導入したサーバを構築することで実現することを想定している。

① SHA-2以上、2,048ビット以上の証明書のみ発行すること。

② サービス提供終了日（2029年12月31日）を超える証明書を発行できること。
③ 目的に応じて、各種暗号化に使用するための証明書を発行できること。
④ アプリケーションに署名するための証明書を発行すること。なお、ルート認証局はスタンドアロン認証局とし、オフラインルート認証局として構築すること。
⑤ 構築完了後にルート認証局をインストールした仮想マシンをパワーオフすること。
⑥ 使用するアルゴリズムは「電子政府における調達のために参照すべき暗号のリスト（CRYPTREC暗号リスト）」に記載があるものを利用すること。

1.2.12 システム管理

本機能については、導入するハードウェアによるため、実現方法は提案による。全てのサーバを一括管理できること。
① 各サーバのファームウェアのバージョン等の情報を収集できること。
② 複数のサーバを対象としたファームウェアの一括バージョンアップができること。
③ 物理サーバの起動直後（BIOS相当）の画面をGUIで操作できること。
④ OSの状態に依存しない各サーバへの電源を投入及び切断ができること。
⑤ 当該サーバのブラウザから、組み込み型管理ソフトウェアに接続することで、要件を満たす構成も可とする。

1.3 情報セキュリティ機能

1.3.1 主体認証

① ディレクトリ

（ア）Active Directoryを導入すること。
（イ）クラウドサービス上で利用するディレクトリとして、Entra IDを導入すること。
（ウ）上記(ア)、(イ）の間で、Entra Connect等を利用して、アカウント情報を同期して管理できること。

② ICカード認証

ICカードを用いた認証ソリューションを用いて実現することを想定している。
（ア）ICカード及びパスワードを用いた2要素認証を実現すること。なお、その際は国家公務員身分証ICカードを用いること。
（イ）「1.3.1①ディレクトリ」と連携できること。
（ウ）「1.3.1①ディレクトリ」に登録したWindowsのパスワードは、ユーザに公

開せずに利用できること。
（エ）規定の回数、認証に失敗した場合、ロックアウトされる等により、認証を拒否する仕組みを講じること。また、一定時間経過後、自動的にロックアウトが解除できること。
（オ）主体認証のパスワードを通信及び保存する場合、その内容を暗号化すること。
（カ）主体認証を行う機能において、認証機能を他者に使用されるまたは使用される危険性を認識した場合、直ちに主体認証を停止できること。

③　ワンタイムパスワードトークン認証
（ア）以下の場合にワンタイムパスワードトークンによるユーザ認証できること。
(1)　「1.1.5 リモートアクセス」による仮想 PC への接続時
(2)　「1.1.10 ファイル転送」の利用時
（イ）ワンタイムパスワードトークンはハードウェアトークンとすること。
（ウ）「1.3.1①ディレクトリ」と連携できること。
（エ）統計センターが許可した者のみが次期情報システム基盤への接続を可能とするため、ユーザを特定する識別子による主体認証を導入し、全ての接続を制御すること。
（オ）規定の回数、認証に失敗した場合、ロックアウトされる等により、認証を拒否する仕組みを講じること。
（カ）ワンタイムパスワードトークンにロックがかかってしまった場合に、１５分後に自動的にロック解除できること。
（キ）ワンタイムパスワードトークンについて、ユーザPINを省略し表示される数字だけで認証できること。
（ク）主体認証を行う機能において、認証機能を他者に使用されるまたは使用される危険性を認識した場合に、直ちに主体認証を停止できること。
（ケ）当該機能の有効期限が2029年12月31日まであること。
（コ）当該機能がWindowsログオンにおいても使用可能なソフトウェアが提供されることが望ましい。

1.3.2　仮想ブラウザ

本機能については、仮想デスクトップ製品のアプリケーション仮想化機能により実現することを想定している。

①　インターネット上のWebサイトを閲覧するために、Webブラウザ（Microsoft Edge、Mozilla Firefox及びGoogle Chrome）を利用できること。
②　当該機能をシングルサインオンで利用できること。
③　仮想PCに対して、画面転送方式により当該機能を提供すること。

④　画面転送プロトコルは、Blast、HDXまたはICAとすること。
⑤　仮想ブラウザ環境のプロファイルを一元管理できること。なお、プロファイルの破損や読み込み速度の問題が発生しにくい方式を提案することが望ましい。
⑥　仮想ブラウザで接続したWebサイト等を印刷できること。
⑦　仮想ブラウザは毎日リフレッシュできること。
⑧　仮想ブラウザにおけるマスタのOS及びアプリケーションにパッチ等の適用を行った場合、マスタから複製した仮想ブラウザに反映できること。
⑨　フォルダリダイレクトを利用してWebサイトのURLをブックマークとして保存できること。

1.3.3　ファイル転送及びファイル無害化

本機能は分離環境でのファイル転送ソリューションと、ファイル無害化ソリューションを組み合わせて実現することを想定している。

①　ファイル無害化

（ア）インターネット接続用ネットワーク、持込・持出用ネットワークからファイルを持ち込む際またはユーザが任意で選択したタイミングで、ファイルを以下の方法で無害化できること。

(1)　ダウンロードファイルを識別し、ファイルの形式に合わせて、マクロ、OLE オブジェクト等を削除してファイルを再構成すること。
(2)　ダウンロードファイルをウイルスチェックできること。

（イ）以下のファイルについて、無害化できること。

(1)　Microsoft Office 文書（Word ファイル、Excel ファイル及び PowerPoint ファイル）
(2)　PDF 形式ファイル
(3)　画像ファイル（PNG 及び JPEG を含む。）
(4)　ZIP 圧縮ファイル
(5)　一太郎ファイル

（ウ）無害化したファイルのみ「11.2.3④内部ネットワーク用ファイアウォール」から内側のネットワークに取り込みできること。
（エ）同一ネットワーク内のファイルについて、任意のタイミングでファイル無害化を実施できること。その際、必要な機器の台数及び機能実現に必要なライセンス数を提案すること。

②　ファイル転送

（ア）ユーザが特定の入力フォルダにダウンロードファイルをアップロードした

場合、ファイルのアップロードを検知して、当該ファイルの無害化が必要な場合には、自動的に無害化した上で、境界を越えて別ネットワークの出力フォルダへ転送されること。なお、境界の両側に入力フォルダ及び出力フォルダを設置し、そこにFile Explorerからアクセスすることでファイルの転送が実現できること。

（イ）当該機能を以下のネットワークの境界で利用できるようにすること。その際、必要な機器の台数及び機能実現に必要なライセンス数を提案すること。

(1) 一般事務用ネットワークとインターネット接続用ネットワークの境界
(2) 一般事務用ネットワークと集計業務用ネットワークの境界
(3) 集計業務用ネットワークと持込・持出用ネットワークの境界
(4) 一般事務用ネットワークと持込・持出用ネットワークの境界

（ウ）ファイルの持込・持出を行う場合には、第三者による承認によって、ファイル転送が実行されること。ただし、一般事務用ネットワークから集計業務用ネットワークへの持ち込みに関しては、承認を不要とする。

1.3.4 エンドポイントマルウェア対策

本機能については、WindowsとLinuxを実行する仮想マシンに対して、エージェントをインストールしたアンチウィルス機能を提供すること。なお、ハイパーバイザーと連携したスキャンサーバによる構成は不可とする。

① 「1.3.6不正プロセス検知」と競合することなく導入できること。
② WindowsとLinuxを単一の管理コンソールで管理できることが望ましい。
③ オフライン環境で動作すること。オフライン環境においても検知率の低下がないことが望ましい。
④ スキャン時のCPUパフォーマンスに与える影響が少ないことが望ましい。
⑤ シグネチャアップデートに依存せずに未知の脅威に対して検知できることが望ましい。
⑥ 仮想化基盤上の仮想サーバの数は400台としてライセンス料を算出すること。

1.3.5 ファイアウォール

本機能はオンプレミスに配置するFWについて共通的な機能を記したものである。

① ファイアウォール

（ア）ステートフルパケットインスペクション機能を有すること。
（イ）アクセス履歴の情報としては通信の送信元及び宛先、要求されたサービ

ス、使用されたプロトコル、日時、ソースポート、実行されたアクション等を含むこと。
（ウ）同一ネットワーク内または異なるネットワーク間で中継されるパケットのアクセス制御をできること。
（エ）IPv4及びIPv6によるアクセス制御が行えること。
（オ）IPアドレス及びポート番号の組み合わせ等、あらかじめ決められたルールに基づき、通信の許可または拒否を制御できること。
（カ）パケットをフィルタリングできること。
（キ）NAT機能（アドレス変換機能）を有すること。
（ク）TCP/UDPポート番号変換機能（NAPT及びIPマスカレード）を有すること。
（ケ）ファイアウォールログを「1.2.3②ログ保管」に転送すること。
（コ）設定変更時に変更内容が即座に反映されない機能を有すること。
（サ）利用ユーザ数は無制限であること。

1.3.6　不正プロセス検知

本機能は、クラウドベースで動作する拡張型ディテクション＆レスポンスソリューションと、それらの運用を自動化するソリューションの組み合わせにより実現することを想定している。

①　全般

（ア）クラウド提供サービスであること。ただしクラウドサービスに送信するデータはログのみとし、不正プロセス検知時にファイルなどのデータをクラウドサービスに送信しないこと。
（イ）日本に設置されたデータセンター上でサービスを提供できること。または、海外のデータセンターを使用する場合は合意管轄裁判所を日本にすること。
（ウ）Webブラウザを利用してクラウド上の管理コンソールにアクセスし、設定やインシデント状況の確認、調査・対応等の集中管理が行えること。また、2要素認証に対応していること。
（エ）当該機能で取得したログの保管期間は一年間とすること。
（オ）当該機能で取得したログは「1.2.3②ログ保管」においても保管すること。

②　端末操作ログ取得

（ア）エージェントを導入することでWindows端末の活動ログとして以下の情報を取得できること。なお、ユーザによる操作も含めること。
(1)　ファイル操作（コピー、削除、リネーム等）
（イ）プロセス起動時に、起動元となった親プロセスの名前を含むフルパス及び起動元のプロセスを一意に特定でき再利用されない情報を記録すること。

（ウ）内部ネットワークをスキャンすることで、ネットワーク上に接続されているプリンタ、持ち込みPC等のエージェント未導入の端末を発見することができること。
（エ）エージェントの変更、終了等の改ざんの試みを防御する機能を有すること。

③　不正プロセス検知
（ア）Windows 10、Windows 11及びWindows Server 2022に対応していること。
（イ）「1.3.1①ディレクトリ」の認証ログを取り込み可能なことが望ましい。
（ウ）Microsoft365等本調達で導入するパブリッククラウドサービスから、監査ログ及びネットワーク接続ログを取り込み可能なことが望ましい。
（エ）カーネルモードで動作すること。
（オ）マルウェア感染のトリガとなる攻撃を検知・防御できること。
（カ）プログラムの脆弱性を利用したコード実行型攻撃を検知・防御できること。
（キ）ポリシー設定及び検知除外の例外リストの設定が指定の内容で稼動すること。
（ク）マルウェア等の感染を検知した場合、感染した全ての機器を特定し、脅威の拡大範囲を確認できること。
（ケ）ファイルのアクセス、プロセスの通信先、レジストリの変更、プロセスの親子関係、ハッシュ値等に加えて、複数の工程で実行されるマルウェアの一連の動作を記録する等、サイバー攻撃及びマルウェアの動作解析に必要な情報を取得すること。
（コ）ユーザがPCの不審な挙動を認識したときに仮想PCの切り離しが行えること。なお、操作方法が容易であることが望ましい。
（サ）機密性3を扱うPCからログ送信する際には、Proxyを経由してログの送付が行われること。
（シ）発生したアラートから関連性のあるものを自動的にグループ化し、インシデントとして管理できること。
（ス）インシデントにグループ化されたアラートとMITRE ATT&CK フレームワークのタクティクス及びテクニックとのマッピングがされており、画面から確認が簡単に行えること。
（セ）インシデントに関連している端末、ユーザ、ファイル、通信先等の情報が一覧で確認できること。
（ソ）インシデントをスコアリングして点数で管理者が重要度を把握することができることが望ましい。機密性の高いサーバが関係するインシデントや特定のメンバーを標的にした攻撃等を、点数づけすることで、高くする等のカスタマイズをすることができることが望ましい。また、トリアージ及び

調査機能を強化するために、スコアに寄与する主な要因を示すことができることが望ましい。

(タ) 侵害されたアカウントや悪意のあるアクティビティを検出するために、ユーザのアクティビティを調査し、ユーザごとのスコアリング機能を有することが望ましい。

(チ) アラートを管理者に通知する方法として、メール及びSyslogが利用できること。

(ツ) 脆弱性攻撃の検知、攻撃性のある振る舞いの検知またはマルウェア検知をした場合に、利用者のクライアント端末画面上にポップアップ通知が行えること。

(テ) 端末の活動ログ検索をスケジュール化し、定期的に検索を行うようにすることができること。

(ト) アラート及びインシデントデータを1年以上保存できること。なお、データの保管は「1.2.3②ログ保管」で保管する構成も可とする。

(ナ) Webブラウザを利用して不正なURLアクセスや、不正なPDFファイルを開く等の未知または既知の脆弱性を悪用する攻撃を検知して、メモリ上の悪意があるコードが実行される前に阻止することができること。本機能はネットワーク未接続状態でも検知精度が低下せず動作することが望ましい。

(ニ) stix/taxiiで配布されるIOC情報（ドメイン、IPアドレス、URL及びハッシュ値）を取り込み、該当した場合に検知できること。

(ヌ) プロセスの親子関係及びコマンド引数の組み合わせにより、子プロセスの呼び出しを阻止する機能があること。本機能はネットワーク未接続状態でも動作すること。

(ネ) 起動された一連のプロセスの流れと実行された行為を監視し、攻撃と思われる振る舞いを検知した場合には、一連のプロセスを強制終了し攻撃を阻止する機能があること。本機能はネットワーク未接続でも動作すること。

(ノ) 収集された端末の活動ログに対し、IOCとの照合を自動的に行い攻撃の可能性がある活動を検知できること。また、新たなIOCが登録された場合には、保存されている過去のログに対しても照合が自動的に行われること。もしくは、保存されている過去のログに対して手動による照合をリモート監視にて実施すること。

(ハ) 収集されたログに対して、管理者によって作成された相関条件を使った検知が行えること。また、既存の統合ログ取得機能で設定している検知ルールを本機能に設定できるか導入時に精査することが望ましい。

(ヒ) インシデント調査では、一画面で、検知アラートより抽出した各種情報（エージェントであれば関連プロセス名、ファイル、接続先IPアドレス、ドメイン名、関連する内部端末名、IPアドレス、ログオンユーザ名等）の情報が一覧で閲覧可能であることが望ましい。

（フ）ランサムウェアの動作を検知した場合にランサムウェアの活動を強制的に停止することで、データの暗号化から保護することができること。本機能はネットワーク未接続状態でも動作することが望ましい。
（ヘ）収集された端末の活動ログに対し、一定期間時間をかけて機械学習を使い学習させることで、エージェント上で実行された不審なコマンド、大量のファイルアップロード、内部ネットワーク上での探索行為等の内部犯行の予兆を検知できることが望ましい。
（ホ）ファイアウォールからのトラフィックログは機械学習を利用して解析し、疑わしいポートスキャン、大量の外部へのデータ送信等を検知できること。また、他の組織内の他端末の活動ベースラインと比較して検知できることが望ましい。
（マ）収集されたクラウドサービスからの監査ログに対し、一定期間時間をかけて機械学習を使い学習させることで、IaaS/PaaS上で不審な設定変更、ログ削除、ユーザ追加等の内部犯行や管理者アカウントの不正利用の可能性を検知できることが望ましい。

④　ブラウザの閲覧履歴取得
（ア）特に、Web閲覧時については、その履歴をURLだけでなく、ウインドウタイトルも合わせて取得できること。本ログの取得については、想定するソリューション以外のソフトウェアを組み合わせて実現することを想定している（例http://www.nirsoft.net/utils/browsing_history_view.html）。

1.3.7　ソフトウェアアップデート
①　Microsoft Windows Serverに対するソフトウェアアップデート
（ア）「1.2.2構成管理」でソフトウェアの状態を管理し、常に最新に保つこと。

②　Linuxサーバに対するソフトウェアアップデート
（ア）「1.2.2構成管理」に記載のとおり、ソフトウェアの状態を管理し、常に最新に保つ方法を提案すること。

1.3.8　メールセキュリティ対策
①　メールセキュリティ対策及びサンドボックス
本機能は、クラウドサービス上で動作することを想定している。
（ア）外部からのメールは、本機能にて不審メールをフィルタリングした上で、「1.1.1②メール」に中継すること。
（イ）クラウドサービスとして提供できること。共有型ではなく占有型であること。データセンターは複数拠点を利用し冗長運用していること。

(ウ) 送信元レピュテーションチェック機能を有していることが望ましい。
(エ) アンチウィルス機能を有していること。なお、複数のアンチウイルスエンジンから任意のエンジンを選択できることが望ましい。
(オ) 定期的に最新のシグネチャ有無を確認し、更新すること。
(カ) アンチスパム機能を有していること。
(キ) メールの件名や本文に含まれる任意のキーワードによるメールブロックが可能であること。
(ク) 迷惑メールへの対応として、スパムカテゴリだけでなく、アダルト、バルク、詐称、フィッシング等のカテゴリごとに管理画面でアクションを指定できること。
(ケ) ビジネスメール詐欺に機械学習エンジン等を用いて対応できることが望ましい。
(コ) 検疫されたフォルダごとに、ユーザへアクセスさせるかどうかを指定可能なこと。
(サ) 単位時間あたりのメール流量の閾値を超えたメール受信を制限できること。
(シ) メールサイズの閾値を超えたメール受信を制限できること。
(ス) 指定した拡張子を持つ添付ファイルを削除し、削除された旨を元メール本文に追記できること。
(セ) 添付ファイルの名前、拡張子、添付ファイル数、添付ファイルサイズ等でフィルタリングできること。
(ソ) SPF、DKIM及びDMARCに対応できること。適用範囲として、ドメインごと、グループごと、ユーザごと等で柔軟に適用できること。
(タ) メールアドレスやIPアドレスを指定してホワイトリストまたはブラックリストに登録できること。管理者側だけでなく、利用者側でも管理できること。
(チ) TLS1.2以上に対応していること。
(ツ) 脅威判定され隔離されたメールを一定期間保留し、その後にリリースできること。
(テ) 不審なメールを検知した際、宛先メールアドレスのユーザに対して検知内容やアクションを示した通知メールを発行できること。テンプレートをカスタマイズできること。
(ト) メールに警告タグを挿入し、ユーザへの注意喚起が容易にできることが望ましい。
(ナ) サンドボックス機能を有しており、URLや添付ファイルの脅威に対応できること。
(ニ) メール本文のURLを書き換えて利用者に配送できることが望ましい。
(ヌ) Microsoft Officeファイル、PDFファイル等（Zipでアーカイブされている

場合を含む）をサンドボックスで分析できること。
（ネ）悪意のある添付ファイルが検知された場合、そのメールを隔離できること。
（ノ）添付ファイルの分析時間のタイムアウト時間を管理者側で変更できること。
（ハ）管理画面の表示言語は英語だけでなく日本語にも切り替えできること。
（ヒ）メール送受信ログ（直近30日間以上）及び監査ログを管理画面で確認できること。
（フ）ディレクトリサービスとのアカウント連携ができること。
（ヘ）NTPによる時刻同期に対応していること。
（ホ）検疫メールの検索機能を有すること。また、検索において以下の条件を指定可能であり、クエリを保存可能であること。
(1) 送信元
(2) 宛先
(3) 件名
(4) 原因
(5) 保存期間

（マ）検疫メールを受信者に通知する手段として、定期的なメール配信の機能を有し、任意の時間に複数回送信可能であること。

1.3.9 Webセキュリティ対策

本機能はクラウドサービスにて実現されることを想定している。

① セキュアWebゲートウェイ(SWG)

（ア）SaaS型の提供であること。
（イ）ISMAPを取得していること。または、既に申請済みであること。
（ウ）サービス契約終了後はデータ消去が行われること。
（エ）クラウド上のログデータは暗号化されて保存されていること。
（オ）拠点からIPsecまたはGREによる接続が可能なこと。
（カ）日本国内に接続先を有すること。なお、複数の接続先があることが望ましい。
（キ）エージェントに社内/社外を判定しアクセスを制御する仕組みを有すること。
（ク）クライアント端末から自動または手動でDCを選択して利用する仕組みを有すること。
（ケ）IdP(Entra ID、Okta等）とSAML連携できること。
（コ）インターネットの利用状況を確認可能なレポートが表示できること。
（サ）アクセスに用いるクライアントエージェントをバージョン指定でアップ

デートできること。
(シ) 管理コンソール上で、利用されているクライアントエージェントのバージョンが確認できること。
(ス) SIEMにリアルタイムのログ送付が可能なこと。
(セ) 通信パケットを取得し、クラウドサービス内に保管し、他のサービスに連携する機能を提供することが望ましい。
(ソ) 障害発生時の調査のためのリモートアクセス機能を有すること。
(タ) 障害発生時の調査のため、パケットまたはトラフィックログを取得する機能を有すること。
(チ) HTTP、HTTPS及びFTPリクエストを対象とすること。
(ツ) Webサイトへのアクセスログを取得できること。
(テ) ユーザ識別及びアプリケーション識別を行うことができること。
(ト) システム管理用インターフェースとしてGUIを提供すること。
(ナ) ユーザが外部に対する全てのWebアクセスは、HTTPSの復号を含めこれを処理可能な構成とすること。
(ニ) ユーザ、部署、日時、場所、プロトコル、コンテンツタイプ等の属性に応じ、アクセス制御等のポリシーを適用できること。
(ヌ) P2Pファイル共有を制御できること。
(ネ) 広告サイトをブロックできること。
(ノ) カテゴリ単位でWebサイトへの閲覧及び投稿を制限できること。
(ハ) ユーザ単位及び組織単位で制限できること。
(ヒ) 管理者が登録したブラックリスト及びホワイトリストを使用できること。
(フ) HTTPSの復号化の例外は一部のサイトのみ許可できること。
(ヘ) CEF(Common Event Format)形式でアラート検知ログ出力、送付できること。また、文字コードはUTF-8(BOMなし)であること。
(ホ) アラート検知ログをrsyslog(syslog(514/TCP)プロトコル)で送付可能であること。なお、「1.2.3②ログ保管」で中継することも可とする。
(マ) syslog送付先を主管課が別途契約するセキュリティ監視のSOCのオンサイト/オフサイトの2カ所設定できること。その際には、「11.7⑨別途契約するセキュリティ監視との接続回線及びVPNゲートウェイ」を経由して送付すること。
(ミ) 主管課が別途契約するセキュリティ監視のSOCからstix/taxiiで配布されるIoC情報（ドメイン、IPアドレス、URL）を取り込み、該当通信を検知及び遮断すること。また、配信されるIoC情報であるSnortルールの取り込みを行えることが望ましい。
(ム) 他サービス契約者のトラフィックによる影響を受けないよう、サービス契約者間で共有されるリソースではなく、契約ごとに専用リソースが提供されることが望ましい。

（メ）一人のユーザが複数のデバイスを保有している場合でも追加ライセンスが不要で同時に接続できることが望ましい。
（モ）「1.3.6③不正プロセス検知」との連携機能を有することが望ましい。

② クラウドアクセスセキュリティ（CASB）

本機能は、クラウドサービスを用いて実現することを想定している。

（ア）エンドポイントにエージェントを入れずにクラウドサービスの可視、制御が可能であるエージェントレス型であること。
（イ）クラウドサービスの登録数が30,000以上あること。なお、日本国内のクラウドサービスについて、網羅（追加、廃止）されていることが望ましい。
（ウ）管理者がウェイトを変更してクラウドサービスのリスクスコアをカスタマイズできること。
（エ）クラウドレジストリの更新にクラウドソーシングの手法を取り入れていること。
（オ）CRMやファイル共有、マーケティング、コラボレーション及びソーシャルメディアのようなカテゴリごとのクラウド使用状況レポートをカテゴリごと表示ができること。
（カ）クラウドレジストリは新しいクラウドサービスのアップデートが少なくとも週1回更新されること。
（キ）管理コンソールからクラウドサービスの新規登録申請を行う仕組みを持っていること。
（ク）クラウドサービスのコンプライアンス認定状況をレジストリ内に持っていること。PCI、ISO、CSA及びHIPAAだけではなく、他の業界の認定も追跡できることが望ましい。
（ケ）Cloudbleed、Heartbleed、Poodle、Freak等の脆弱性があるクラウドサービスの利用があるかどうか監査できることが望ましい。
（コ）サービスの特徴を指定して、クラウドサービスやそのサービス利用状況をフィルタリングして表示できること。
（サ）特定期間での特定ユーザによるサービス利用状況一覧を表示できること。
（シ）Active Directory、Entra ID及びその他のエンタープライズディレクトリと統合して、ユーザ情報を付加して可視化できること。
（ス）企業ファイアウォール、Webプロキシ及びSIEMログデータの継続的（24時間365日）の取り込みと分析をサポートし、組織内でアクセスされているクラウドサービスの継続的で最新の可視性と監視が可能であること。
（セ）ファイアウォール及びWebプロキシのログファイルのフィールドを難読化して送信し、参照する際には難読化されたデータが閲覧できるように難読化解除ができること。（データトークナイゼーション）
（ソ）1GB以上のログファイルの解析をサポートすること。

（タ）複数のファイアウォール及びプロキシベンダーの任意のログフォーマットをサポートすること。
（チ）ログをCASBクラウドにアップロードする前に、ログからCASB分析に関連しない情報を削除してアップロードサイズを最小限にできること。
（ツ）クラウドベースのファイル共有サービス、FTP等のアップロードサイトがデータベースに乗っていない不審なサイトに対するデータアップロードを識別することができること。
（テ）12か月の統計データを保持することができること。
（ト）疑わしい行動をしているユーザを選択して監視するウオッチリストを作成できること。
（ナ）組織で使用しているクラウドサービスのリスクスコアが変化した場合に、警告を上げることができること。
（ニ）脆弱な設定になっているクラウドストレージ（誰でも書き込み、読み込み可能になっているAWSのS3バケット等）に対するアクセス状況を可視化できること。

③　サンドボックス
（ア）クラウド型サンドボックスを用いて既知及び未知のマルウェアを検知・防御できること。
（イ）クラウド型サンドボックスにて検出した未知のマルウェアを検出から1時間以内に検知・防御できること。
（ウ）マルウェアを検知した場合、シグネチャを作成できること。
（エ）提供元から配信されたシグネチャを受信できること。

④　不正侵入防止
（ア）外部からの不正アクセスを防止する機能を有すること。
（イ）不正アクセスを検知した際には、アラートを通知できること。
（ウ）ネットワーク層及びアプリケーション層に対する脆弱性攻撃等（バッファオーバーフロー及びポートスキャンを含む。）を検知・防御できること。
（エ）脆弱性攻撃の検知は、シグネチャ照合及び異常検出に基づくこと。
（オ）シグネチャは脆弱性に基づいて構築されていること。
（カ）異常検出は、RFCに準拠しないプロトコルの使用を検知すること。
（キ）カスタムシグネチャを定義できることが望ましい。

1.3.10 脆弱性検査ツール

本機能は、脆弱性検査ツールの製品を導入することにより実現されることを想定している。

①　エージェントを導入することのできないサーバ機器及びネットワーク機器

も脆弱性管理の対象とすることができること。

② クラウドサービス上の仮想マシンも脆弱性管理の対象とすることができること。

③ 全ての仮想サーバを対象に監査することができること。

④ 脆弱性スキャナとしてエージェントレス型とエージェント型に加え、パッシブ型のスキャナを使用できること。またエージェントレス型においては、OSへのログインを行った上でスキャンすること。

⑤ 管理対象としたサーバ機器及び端末から脆弱性の有無だけでなく、端末の設定情報やインストールされているソフトウェアの情報を取得できること。また取得した情報は画面で確認できるだけでなく、APIで出力できること。

⑥ 追加ライセンスなしにOSやアプリケーションの設定が業界標準の推奨値となっていることを確認できること。

⑦ プラットフォーム脆弱性管理、WebApp脆弱性管理及びパブリッククラウド監査を統合分析する機能を有する製品であること。

⑧ 購入したライセンス数を、本機能や「1.2.6③ Active Directory監査」に対して柔軟に割当てることが可能な製品形態であることが望ましい。また、割り付けた後も変更が可能であることが望ましい。

⑨ コンピュータ機器、NW機器、Active Directory等の異なる情報リソースに対してライセンスを割り付けた際に、どの情報リソースが攻撃される可能性が高いリソースであるのかを追加ライセンスなしにリスクベースで分析し、一覧表示をすることが可能であることが望ましい。

⑩ コンピュータ機器、ネットワーク機器に対して脆弱性管理を行なった場合に、どの機器が攻撃される危険度の高い資産なのかをリスクベースで分析し、一覧で表示することが可能であることが望ましい。

2. ユーザビリティ及びアクセシビリティに関する事項

2.1 情報システムのユーザの種類及び特性

次期情報システム基盤のユーザは約1,450人で、ユーザ区分は「表 1 次期情報システム基盤のユーザ」のとおり。各月ごとの総ユーザ数の見込みは「別紙１ 次期情報システム基盤におけるユーザ数一覧」のとおり。

表 1　次期情報システム基盤のユーザ

No.	ユーザ区分	利用用途	主な利用機能	人数
1	一般ユーザ	統計センターの一般事務を行う。	1.1.1 メール 1.1.2 スケジュール管理 1.1.3 仮想 PC 及びアプリケーション配信 1.1.6Web 会議 1.1.7 在席管理 1.1.8 ファイル共有 1.1.9 会議室予約 1.1.10 ファイル転送	約 830 人
2	メール制限ユーザ（インターネット及び政府共通ネットワークへのメールが制限されているユーザ。）	同上	同上（ただし、インターネット及び政府共通ネットワークへのメール不可）	約 250 人
3	システム管理者（次期運用事業者及び保守担当者含む。）	次期情報システム基盤のシステム管理を行う。	No1 に加えて、 1.2.1 仮想化基盤管理 1.2.2 構成管理 1.2.3 ログ取得・管理 1.2.4 監視 1.2.5 バックアップ 1.2.6 特権 ID 管理 1.2.7 アカウント管理	約 30 人
4	外部ユーザ	他の省庁及び他の独立行政法人の職員等、外部の者にリモートサクセスのための仮想 PC を提供する。	1.1.5 リモートアクセス （インターネット及び政府共通ネットワークへのメール不可）	約 340 人

3. システム方式に関する事項

3.1 情報システムの構成に関する全体の方針

① 統計センターが登録している「nstac.go.jp」、「nstac.jp」、「独立行政法人統計センター.jp」及び「統計センター.jp」の各ドメインについて統計センターが使用し続けられるようにすること。なお、ドメインについては、契約終了後も引き続き統計センターにて使用できること。

② ソフトウェアについては、有償製品・無償製品に関わらず、全ての製品において、サポート（パッチの提供、バージョンアップ等）が受けられる製品を導入すること。また、運用を含む経費削減を考慮したライセンス形態を選択し、導入すること。

③ クラウドサービスを利用する場合には、原則、ISMAPを取得していること。または、既に申請済みであること。ISMAPを取得していない場合は、同等の対策を行うこと。なお、データセンターは国内設置または準拠法・裁判管轄を国内に指定できることを要件とする。

④ 要件を実現するにあたり最適と考えられる構成を提案すること。なお、特別の指定がない限り、アプライアンスによる構成も可とする。

⑤ バックアップデータセンターに導入する調達機器はバージョンアップ、設定変更等の検証環境として利用するため、可能な限りメインデータセンターに導入する調達機器と同一ベンダー同一シリーズの製品とすること。なお、構成の都合により実施できない検証については請負者の環境で実施できること。ただし、上記方針はより効率的なシステム構成の提案や製品選定を妨げるものではない。

⑥ 特に明記がない場合、調達機器は可能な限り統合化を図り、仮想化にてリソース資源の効率化を図ること。なお、仮想化しないものに対しては、その理由を明確にすること。また、ハイパーバイザー型の仮想化ソフトウェアは、Linux OS、Windows OS等の複数のゲストOSでの十分な稼動実績及び信頼性のあるソフトウェアとすること。ただし、上記方針はより効率的なシステム構成の提案や製品選定を妨げるものではない。

⑦ 現行情報システム基盤ではActive DirectoryによるWindowsネットワークを構築している。また、次期情報システム基盤についても、現行情報システム基盤の設定を引き継ぎ、Windowsネットワークを構築すること。

⑧ 同一種類の調達機器に関しては、機種及び型番を全て統一すること。ただし、上記方針はより効率的なシステム構成の提案や製品選定を妨げるものではない。

⑨ 日本マイクロソフト株式会社の製品は、適切な料金プランを選択すること。また、契約期間中は、原因の追究を含めた問い合わせを可能とするサポート契約を締結すること。

⑩　管理用ネットワークと他のネットワークを分離すること。

⑪　以下の項目について、提案するストレージベンダーの技術者による支援を受けられるように必要な契約を締結すること。

（ア）導入支援

(1)　ストレージ設計

(2)　データ移行計画

(3)　ストレージ構築作業

(4)　データ移行作業

（イ）運用支援

(1)　QA サポート

(2)　四半期に一度、専任担当者からのストレージの運用報告を行うこと。

⑫　サーバに搭載するCPUにおいて、指定したCPUより新しいCPUが発表された場合は、後継機種を提案すること。

⑬　メインストレージもしくは、バックアップ機器にて、ランサムウェア対策を実装することが望ましい。

⑭　サポート

（ア）基盤の安定性を維持するため、仮想化ソフトウェア開発元ベンダーより公開される不具合事例やセキュリティ情報を日本語で提供すること。また製品仕様や設定方法の確認に対する技術問い合わせの窓口を提供すること。

（イ）仮想化ソフトウェアにおいて業務停止等の重篤な障害が発生した際には、回避策の提示だけでなく、障害発生の根本原因調査を行うことが望ましい。

（ウ）構築にあたっては、ネットワーク仮想化や仮想デスクトップ、アプリケーション仮想化等の実現にあたり、提供元のベンダーまたはベンダーが認定する技術者による技術サポートを行う体制を構築することが望ましい。

4.　性能に関する事項

次期情報システム基盤において、求める性能の目標値は「表 2　次期情報システム基盤における性能の目標値」のとおり。

下記を実現するために、必要な機能は負荷分散を図る等の対策を講じること。

表 2　次期情報システム基盤における性能の目標値

No.	指標	目標値
1	15 分間に、順次 800 人が仮想 PC にログインした場合、デスクトップ画面が表示されるまでの時間	60 秒以内

No.	指標	目標値
2	仮想PCから仮想ブラウザを起動した場合に完全に表示されるまでの時間	60秒以内
3	15 分間に、順次 800 人がメールクライアントを起動した場合、完全に表示されるまでの時間	15秒以内

5. 信頼性に関する事項

① 耐障害性及び可用性を重視し、信頼性の高い機器を選定すること。
② 調達機器（統計センターが用意する機器を除く。）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（ただし、統計センターが指定する製品を除く。）。
③ 調達機器（統計センターが用意する機器を除く。）は、全て新品（未使用）であること。
④ 各保存データ、設定ファイル等は、情報が正確に記録または保存されること。
⑤ 各種機器は、NTPによる時刻同期を行うこと。
⑥ メインデータセンターに設置する調達機器については、特に明記がない場合、可用性を維持するために、回線、機器等を冗長化する等、単一障害点を排除したシステム構成とすること。単一障害点を排除できない場合は、その理由を明確にすること。
⑦ 冗長化の方法として、特に「２台で構成し冗長構成とする」のように明記していない場合には、仮想化基盤によるHA構成による実現も可とする。

6. 拡張性に関する事項

① 調達機器（統計センターが用意する機器を除く。）のリソースについて、契約期間である5年間を見越した拡張性を保持すること。
② 追加要件が発生した場合でも、柔軟に対応できる設計とすること。
③ 追加要件が発生した場合でも、各機器のCPU、メモリ、ディスク容量、ポート等の拡張に機器の入れ替えなく、スケールアップまたはスケールアウトで対応できること。
④ 上記③の対応と合わせて、ソフトウェアの追加が必要な場合には、ソフトウェアのライセンス追加等で対応できること。

7. 上位互換性に関する事項

① OS、各ソフトウェア等について、修正プログラムの適用または本調達の範囲内でバージョンアップを行う場合は、主管課へ事前に説明し、承認を得ること。なお、説明の際には、検証方法、影響範囲の確認、作業スケジュール等の内容を含めること。

② バージョンアップに技術的な問題等がある場合、主管課と協議の上、対応すること。

8. 中立性に関する事項

① 調達機器（統計センターが用意する機器を除く。）は、可能な限り特定ベンダーの技術に依存しないオープンな技術仕様に基づくものとすること。ただし、本仕様書にて、特定の製品を指定するものは除く。

② 特定ベンダー及び製品に可能な限り依存することなく、他者に引継ぐことが可能なシステム構成であること。

③ 調達機器（統計センターが用意する機器を除く。）の構成要素は、標準化団体（ISO、IETF、IEEE、ITU、JISC等）が規定または推奨する各業界標準に可能な限り準拠すること。

9. 継続性に関する事項

① 災害等によりメインデータセンター設置機器による業務継続が困難になった場合、バックアップデータセンター設置機器を利用し、メインデータセンターで稼動する以下の仮想サーバ等を稼動できるように構成すること。

（ア）「11.2④(ケ)(1)データベースサーバ」

（イ）「11.2.2①メインストレージ」内の主管課が指定するデータ

② 「11.2.2①メインストレージ」に格納するデータのうち、主管課が指定する2TBのデータはバックアップ取得の周期を1時間以内とすること。また、その他のデータはバックアップ取得の周期を24時間以内とすること。

③ データベースのデータは、システムを停止することなく、差分コピー（SQL Server AlwaysOn 可用性グループ（非同期コミットモード））を実現できること。

④ データ更新量等については、資料閲覧の際に主管課に確認し、把握すること。

⑤ バックアップデータセンターの復旧に関する目標値は以下のとおり。

（ア）RPO（目標復旧時点） ：1時間

（イ）RTO（目標復旧時間） ：24時間

（ウ）RLO（目標復旧レベル）：20人が仮想PCを使用して、上記「①」の仮想サーバ等を利用した業務をできること。

⑥ 災害発生時にバックアップデータセンター設置機器を利用するための切り替え手順、メインデータセンター設置機器への切り戻し手順等を示した「災害対策用機器利用手順書」を作成し、主管課の承認を得ること。

10.　情報セキュリティに関する事項

①　以下のドキュメントに準拠すること。

（ア）統一基準群

（イ）独立行政法人統計センター情報セキュリティポリシー（統計センター）

（ウ）別添3　情報保護・管理要領

（エ）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（内閣サイバーセキュリティセンター）

（オ）ログを活用したActive Directoryに対する攻撃の検知と対策（JPCERTコーディネーションセンター）

（カ）Active Directoryのセキュリティ保護に関するベストプラクティス（日本マイクロソフト株式会社）

（キ）CIS Benchmarks（米国　Center for Internet Security）（Microsoft 365及び提案するクラウドサービス（Azure等その他）に係る部分）

②　使用する暗号方式は、提案時点で「電子政府における調達のために参照すべき暗号のリスト（CRYPTREC暗号リスト）」に掲載されている方式を採用すること。また、暗号の鍵長は、128bit以上であること。なお、契約期間中に当該暗号方式が危殆化した場合は、より強度な暗号方式に変更できること。

③　次期情報システム基盤を構成するソフトウェアの脆弱性を悪用した不正を防止するため、設計・構築時に脆弱性の有無を確認すること。また、運用開始にあたり、対処が必要な脆弱性は主管課と協議し、セキュリティパッチを適用の上、導入すること。

④　調達機器について、次期情報システム基盤で利用しない機能及びサービスについては、停止した上で導入すること。

⑤　調達機器について、次期情報システム基盤の提供に必要なポートのみを利用可能とすること。

⑥　IPv6通信について、政府共通ネットワーク向けに送受信するメール及びインターネットに公開するサービスを除き原則利用しない方針とし、不要なIPv6通信を遮断及び無効化すること。

⑦　リリース後のメンテナンスに必要な機器等については提案し、センターと協議の上、導入を行うこと。

11.　情報システム稼働環境に関する事項

11.1 ネットワーク構成要件

ネットワーク構成案を「別添2 次期情報システム基盤概要構成図」及び下記「表3　ネットワーク構成案」に示す。なお、提案時に最適な構成を提案すること。

表 3　ネットワーク構成案

No.	ネットワーク名	概要
1	インターネット接続用ネットワーク	ユーザが安全にインターネットに接続することを可能とする機器を設置するネットワーク。
2	ストレージ用ネットワーク	ストレージを設置するネットワーク。
3	政府共通ネットワーク接続用ネットワーク	政府共通ネットワーク経由で次期情報システム基盤に接続するため、機器を設置するネットワーク。
4	集計業務用ネットワーク	各種統計調査の集計業務等を行うための機器を設置するネットワーク。データベース、バッチ処理等の機能を提供する。
5	一般事務用ネットワーク	一般事務等の業務を行うための機器を設置するネットワーク。認証、イントラネット、在席管理等の機能を提供する。
6	一般事務用仮想 PC 用ネットワーク	一般事務用ネットワークに接続する仮想 PC を設置するネットワーク。
7	集計業務用仮想 PC 用ネットワーク	集計業務用 NW に接続する仮想 PC を設置するネットワーク。
8	管理用ネットワーク	運用管理用 PC を設置するネットワーク。
9	ZTNA 接続用ネットワーク	インターネットから ZTNA 経由で接続するテレワーク用サーバを設置するネットワーク。
10	持込・持出用ネットワーク	外部とファイルを持込・持出するための PC を設置するネットワーク。
11	ドキュメントスキャナ用ネットワーク	調査票を読み取るためのドキュメントスキャナを接続するためのネットワーク。
12	バックアップ用ネットワーク	バックアップ機器を接続するネットワーク。
13	シンクライアント用ネットワーク	シンクライアント化した PC を接続するネットワーク。
14	複合機用ネットワーク	複合機を接続するネットワーク。

11.2 メインデータセンター設置機器要件

メインデータセンターにおける設置機器の構成を「別添2 次期情報システム基盤概要構成図」に示す。なお、設置機器に対する要件は「11.2.1サーバ要件」から「11.2.5その他機器要件」に示す。

「11.2.1サーバ要件」のサーバはそれぞれ「Windows用仮想化基盤」、「他OS用仮想化基盤」、「バッチ処理用仮想化基盤」、「仮想PC（RDSH）用仮想化基盤」及び「仮想PC（VDI）用仮想化基盤」上で実現することを想定している。このうち、「Windows用仮想化基盤」及び「他OS用仮想化基盤」に配置したサーバについては、現行のサーバで利用しているOSに基づいて「Windows用仮想化基盤」及び「他OS用仮想化基盤」に分けたが、実現方法によってはOSの変更もありうるため、その

際にはOSの種別により配置する仮想基盤を見直し、それにあわせて物理サーバのサイジングについて、必要に応じて見直すものとする。

11.2.1サーバ要件

① Windows用仮想化基盤

（ア）「11.2②(キ)(1)仮想化基盤管理サーバ」による管理を実現すること。

（イ）1台当たり、Intel Xeon Gold 6430、または、AMD EPYC 9334相当以上のCPUを1個搭載すること。

（ウ）1台当たり、メモリを384GB以上搭載すること。

（エ）25Gイーサネットを2ポート以上搭載すること。

（オ）10台以上のサーバで構成すること。

（カ）1サーバ当たり2CPU以上搭載可能なことが望ましい。

（キ）全ての物理サーバに、Microsoft Windows Server Datacenter相当以上（コアライセンス）を適用すること。

（ク）以下の仮想サーバを「11.2①Windows用仮想化基盤」上に構築すること。

(1) 一般事務用仮想 PC 管理サーバ

- 「1.1.3①仮想PC管理」の機能により、一般事務用仮想PCを管理する仕組みとすること。一般事務用仮想PCは、原則「11.2⑥仮想PC（VDI）用仮想化基盤」上のものを利用するが、必要により「11.2⑤仮想PC（RDSH）用仮想化基盤」上のものを利用する場合がある。詳細は設計により決定する。
- 2台以上のサーバで構成し、負荷分散による冗長化及び管理情報をデータベースに格納し高可用性を確保できる構成とする。その際、「11.2①(ク)(2)集計業務用仮想PC管理サーバ」とのデータベースの共用は可とする。

(2) 集計業務用仮想 PC 管理サーバ

- (1)と同様に、「1.1.3①仮想PC管理」の機能により、集計業務用仮想PCを管理する仕組みとすること。集計業務用仮想PCは、原則「11.2⑤仮想PC（RDSH）用仮想化基盤」上のものを利用するが、必要により「11.2⑥仮想PC（VDI）用仮想化基盤」上のものを利用する場合がある。詳細は設計により決定する。
- 2台以上のサーバで構成し、負荷分散による冗長化及び管理情報をデータベースに格納し高可用性を確保できる構成とする。その際、「11.2①(ク)(1)一般事務用仮想PC管理サーバ」とのデータベースの共用は可とする。

(3) インターネット接続用仮想 PC 管理サーバ

- (1)と同様に、「1.1.3①仮想PC管理」の機能により、「1.3.2仮想ブラウザ」の機能で用いる、インターネット接続用仮想PCを管理する仕組みを提供すること。インターネット接続用仮想PCには「11.2⑤仮想PC（RDSH）用仮想化基盤」上のものを利用する。
- 2台以上のサーバで構成し、負荷分散による冗長化及び管理情報をデータベースに格納し高可用性を確保できる構成とする。

(4) 会議室予約サーバ
- 「1.1.9会議室予約」を実現すること。
- 1台以上のサーバで構成すること。
- OSはWindows Serverとすること。

(5) Windows 用構成管理サーバ
- 「1.2.2①Windows向け構成管理」を実現すること。
- 当該更改管理サーバ及び構成管理用データベースサーバで構成すること。
- 当該更改管理サーバ及び構成管理用データベースサーバは分離すること。
- 当該更改管理サーバ及び構成管理用データベースサーバはそれぞれ1台以上のサーバで構成すること。
- 仮想サーバを追加した場合に追加ライセンスが不要であること。
- Microsoft Windows Server Update Servicesを構築すること。

(6) KMS サーバ
- Microsoft製品のボリュームライセンス認証機能を提供すること。
- バックアップセンタの災害対策用KMSサーバと連動して、どちらかが障害等で停止したとしても継続して機能を提供できること。
- 1台以上のサーバで構成すること。

(7) 統合ログ取得・管理サーバ
- 「1.2.3①統合ログ取得」を実現すること。
- 1台以上のサーバで構成すること。

(8) Windows 用監視サーバ
- 「1.2.4①共通要件」及び「1.2.4③Microsoft Windows Server及びMicrosoft 365クラウドサービス監視」を実現すること。
- 当該監視サーバ及び監視用データベースサーバで構成すること。
- 当該監視サーバ及び監視用データベースサーバは分離すること。

- 2台以上のサーバで構成すること。
- 仮想サーバを追加した場合に追加ライセンスが不要であること。

(9) アカウント管理サーバ
- 「1.2.7アカウント管理」を実現すること。
- 1台以上のサーバで構成すること。

(10) DHCP サーバ
- 「1.2.10DHCP」を実現すること。
- 2台以上のサーバで構成し、冗長構成とすること。

(11) インターネット接続用 DHCP サーバ
- 「1.2.10DHCP」を実現すること。
- 2台以上のサーバで構成すること。

(12) 認証局サーバ
- 「1.2.11認証局」を実現すること。
- ルート認証局サーバと下位認証局サーバの2台で構成すること。

(13) インターネット接続用認証局サーバ
- 「1.2.11認証局」を実現すること。
- ルート認証局サーバと下位認証局サーバの2台で構成すること。

(14) プリントサーバ
- 独立行政法人統計センター情報システム基盤の複合機の提供業務で調達したプリンタを一元管理できること。
- 可用性を確保するため、冗長構成をとることが望ましい。
- サーバ構成や導入ソフトウェアについては、システム構成に適した複合機の設計を行う中で決定すること。

(15) 認証サーバ 1
- 「1.3.1①ディレクトリ」を実現すること。
- 「1.2.9①内部DNS」を実現すること。
- 2台以上のサーバで構成し、冗長構成とすること。
- 「1.2.10DHCP」、「1.2.11認証局」等、他の機能とサーバを分離すること。
- Active Directoryを構築すること。
- ユーザ管理及びアクセス権管理をできること。

- 現行のドメインを引継ぐことができること。
- マイクロソフト製品以外によるスキーマ拡張を行わないこと。
- Active Directoryの設計は、「1.2.6③Active Directory監査」の機能を実現するセキュリティ製品による解析の結果を踏まえること。
- 各サーバ及びPCのローカル管理者のパスワード変更管理をLocal Administrator Password Solution（LAPS）で管理できるようにすること。
- サービスアカウントを作成する必要がある場合においてグループの管理されたサービスアカウント（gMSA）が利用可能な場合は利用すること。
- Active Directoryのゴミ箱機能を有効にすること。

(16) 認証サーバ2

- 「11.2①(ク)(15)認証サーバ1」と異なるドメインで構築すること。
- 「11.2①(ク)(15)認証サーバ1」のドメインと信頼関係を結ばないこと。
- 「1.3.1①ディレクトリ」を実現すること。
- 2台以上のサーバで構成し、冗長構成とすること。
- 「1.2.10DHCP」、「1.2.11認証局」等、他の機能とサーバを分離すること。
- ユーザ管理及びアクセス権管理をできること。
- Active Directoryの設計は、「1.2.6③Active Directory監査」の機能を実現するセキュリティ製品による解析の結果を踏まえること。
- 各サーバ及びPCのローカル管理者のパスワード変更管理をLocal Administrator Password Solution（LAPS）で管理できるようにすること。
- サービスアカウントを作成する必要がある場合においてグループの管理されたサービスアカウント（gMSA）が利用可能な場合は利用すること。
- Active Directoryのゴミ箱機能を有効にすること。

(17) グループポリシー管理サーバ1

- 「11.2①(ク)(15)認証サーバ1」で管理するドメイン全体のグループポリシーを管理する機能を提供すること。
- グループポリシーの管理にMicrosoft Advanced Group Policy Management（AGPM）による変更承認の仕組みを導入すること。
- 1台以上のサーバで構成すること。

(18) グループポリシー管理サーバ2

- 「11.2①(ク)(16)認証サーバ2」で管理するドメイン全体のグループポリシーを管理する機能を提供すること。
- グループポリシーの管理にMicrosoft Advanced Group Policy Management (AGPM) による変更承認の仕組みを導入すること。
- 1台以上のサーバで構成すること。

(19) IC カード認証サーバ

- 「1.3.1②ICカード認証」を実現すること。
- 認証情報をセキュリティ確保した状態で記録できること。
- 2台以上のサーバで構成し、冗長構成とすること。

(20) ワンタイムパスワード認証サーバ

- 「1.3.1③ワンタイムパスワードトークン認証」を実現すること。
- 2台以上のサーバで構成し、冗長構成とすること。

(21) イントラネットサーバ (Internet Information Services)

- Microsoft Internet Information Servicesを用いたWebサーバを構築すること。
- 1台以上のサーバで構成すること。
- ASP及びASP.NETが動作するよう構成すること。
- 当該サーバについては別途、福利厚生システムを導入する。

(22) 財務会計システムサーバ

- 1台以上で構成すること。
- 当該サーバについては別途、財務会計システムを導入する。

(23) バッチ制御サーバ

- 1台以上のサーバで構成すること。
- 1台当たりに適用するライセンスは、JP1/Automatic Job Management System3 - Manager、JP1/Automatic Job Management System3 - View、JP1/Base及びJP1/Scriptとする。
- バッチ処理サーバ上で実行するジョブを管理できること。
- Microsoft Internet Information Servicesを用いたWebサーバを構築すること。
- ASP及びASP.NETが動作するよう構成すること。

(24) 高速集計サーバ（Adam-Report）
- 2台以上のサーバで構成すること。
- 1台当たりに適用するライセンスは、Adam-Reportメニーコアエディション（4コア）とする。
- Adam-Reportは後継製品(Z-Adam)に無償でバージョンアップ可能なこと。

(25) 集計業務用イントラネットサーバ（Internet Information Services）
- 「11.2①(ク)(21)イントラネットサーバ（Internet Information Services)」と同一構成とすること。
- 1台以上のサーバで構成すること。

(26) 集計業務用イントラネットサーバ（ConceptBase）
- 1台以上のサーバで構成すること。
- ConceptBase Enterprise Search Basic Editionを導入すること。

(27) 開発検証用ファイルサーバ
- ファイルサーバとして構成すること。
- 1台以上のサーバで構成すること。
- Microsoft Windows Serverを導入すること。

(28) Windows サーバ（その他）
- 2台以上のサーバで構成すること。
- Microsoft Windows Serverを導入すること。
- 台数については、契約期間中に追加する可能性がある。追加手順を作成し、運用で対応すること。

(29) RADIUS サーバ
- 2台以上のサーバで構成し、冗長構成とすること。
- IEEE802.1x認証を行えること。
- RADIUSクライアントとして、「11.3.1②フロア用スイッチ」、「11.3.1③執務室用スイッチ」、「11.3.1⑤(ア)無線LANアクセスポイント」、「11.5.1①拠点用コアスイッチ」、「11.5.1②無線LANアクセスポイント」及び「11.5.1③執務室用スイッチ」を利用できること。

(30) システム管理サーバ

- 1台以上のサーバで構成すること。
- 全てのサーバを一括管理できること。
- 各サーバのファームウェアのバージョン等の情報を収集できること。
- 複数のサーバを対象としたファームウェアの一括バージョンアップできること。
- 物理サーバの起動直後（BIOS相当）の画面をGUIで操作できること。
- OSの状態に依存しない各サーバへの電源を投入及び切断できること。
- 当該サーバのブラウザから組み込み型管理ソフトウェアに接続することで、要件を満たす構成も可とする。

(31) 外部電磁的記録装置管理サーバ

- 1台以上のサーバで構成すること。なお、他サーバと統合することも可とする。
- 外部電磁的記録装置の管理機能を有すること。なお、外部電磁的記録装置1台ごとに利用の可否を設定できること（OS標準機能は不可とする。）。
- 管理対象の端末は、90台とする。
- 当該サーバの構築にあたり、事前検証を行うことが望ましい。

(32) 文書管理用サーバ

- 2台以上のサーバで構成すること。
- 当該サーバについては別途、文書管理システムを導入する。

(33) 開発集計用サーバ

- 2台以上のサーバで構成すること。
- Microsoft Windows Serverを導入すること。

(34) プロジェクト管理サーバ

- 1台以上のサーバで構成すること。
- Azure DevOps Serverを導入すること。

(35) 統計局用イントラネットサーバ

- 1台以上のサーバで構成すること。
- 「11.2①(ク)(21)イントラネットサーバ（Internet Information

Services)」と同一構成とすること。
- PHPを導入すること。
- WebDAVを有効化すること。

(36) 脆弱性検査ツール用サーバ
- 「1.3.10脆弱性検査ツール」を実現すること。
- 管理サーバと検知サーバ合わせ、2台以上のサーバで構成すること。
- 検知サーバは、インターネット接続用ネットワークと一般事務用ネットワークに配置すること。

(37) ファイル共有サーバ
- 以下の単位で、ファイルを共有できる仕組みを設けること。
  - ユーザプロファイル用（仮想ディスクの切り替えにより実施する）
  - 一般事務用
  - 集計業務用１
  - 集計業務用２
  - 長期保存用
  - 統計局用

(38) メンテナンス用サーバ
- 仮想PCのメンテナンス用のサーバを導入すること。
- その他機能のメンテナンス用のサーバを導入すること。
- 仮想PCのメンテナンス用サーバは2台以上のサーバで構成すること。
- その他機能のメンテナンス用のサーバは4台以上のサーバで構成すること。なお、統計センター職員が使用するサーバを2台確保すること。

(39) メール無害化及び誤送信防止サーバ
- 「1.1.1②メール無害化及び誤送信防止」を実現すること。
- 1台以上のサーバで構成すること。

(40) メール原本アーカイブサーバ
- Microsoft Exchange Serverを導入すること。
- 「1.1.1②メール無害化及び誤送信防止」で無害化される前の受信したメールの原本を格納すること。

・ 1台以上のサーバで構成すること。

② 他OS用仮想化基盤

（ア）「11.2②(キ)(1)仮想化基盤管理サーバ」による管理を実現すること。
（イ）1台当たり、Intel Xeon Gold 6430、または、AMD EPYC 9334相当以上のCPUを1個以上搭載すること。
（ウ）1台当たり、メモリを256GB以上搭載すること。
（エ）25Gイーサネットを2ポート以上搭載すること。
（オ）5台以上のサーバで構成すること。
（カ）1サーバ当たり2CPU以上搭載可能なことが望ましい。
（キ）以下の仮想サーバを「11.2②他OS用仮想化基盤」上に構築すること。

(1) 仮想化基盤管理サーバ

・ 「1.2.1仮想化基盤管理」を実現すること。
・ 1台以上のサーバで構成すること。

(2) シングルサインオンサーバ

・ 「1.2.8シングルサインオン」を実現すること。なお、当該サーバの構築にあたり事前検証を行い、要件の実現性を示すことが望ましい。
・ 2台以上のサーバで構成し、冗長構成とすること。

(3) 政府共通ネットワーク用メールサーバ

・ 2台以上のサーバで、プライマリ・セカンダリ構成とすること。
・ Sendmail相当の機能を有すること。
・ 統計センター内から特定ドメインへのメールについて、政府共通ネットワークへの経路を設定すること。
・ 統計センター内からインターネットへのメールは、インターネット公開用システム機器のメールサーバへの経路を設定すること。
・ センター内のアプリケーションからSMTP-AUTHによるSMTP認証を行った上でメールの送信ができること。
・ 政府共通ネットワークからの統計センター内へのメールは、クラウド上の「1.1.1②メール」への経路を設定すること。
・ 政府共通ネットワークへのメールの送受信はIPv4及びIPv6について設定すること。
・ 政府共通ネットワークからの特定サブドメインのメールについて、政府統計共同利用システムへの経路を設定すること。なお、IPv4及びIPv6について設定すること。

(4) キャッシュ DNS サーバ
- 「1.2.9③キャッシュDNS」を実現すること。
- 2台以上のサーバで構成し、プライマリ・セカンダリ構成とすること。

(5) ログ保管サーバ
- 「1.2.3②ログ保管」を実現すること。
- 2台以上のサーバで構成すること。

(6) ネットワーク及び Linux 用監視サーバ
- 「1.2.4①共通要件」及び「1.2.4②ネットワーク及びLinuxサーバ監視」を実現すること。
- 1台以上のサーバで構成すること。
- 仮想サーバを追加した場合に追加ライセンスが不要であること。

(7) 仮想アプリケーション配信サーバ 2
- 「1.1.3③アプリケーション配信2」を実現すること。
- 1台以上のサーバで構成すること。

(8) 政府共通 NW 統計局用プロキシサーバ
- 2台以上のサーバで構成し、冗長構成とすること。
- 政府共通ネットワーク及び統計局への接続を中継すること。
- 政府共通ネットワーク及び統計局への接続に対するアクセスログを取得すること。

(9) Linux サーバ（その他）
- 1台以上のサーバで構成すること。
- Linuxをインストールすること。
- Dockerをインストールすること。
- 台数については、契約期間中に追加する可能性がある。追加手順を作成し、運用で対応すること。

(10) 家計 API サーバ
- 2台以上のサーバで構成すること。
- 本サーバには別途、家計APIシステムを導入する。

(11) LAMP サーバ
- 1台以上のサーバで構成すること。

・ Red Hat Enterprise Linuxをインストールすること。

(12) 共用ロードバランサ
・ 一般事務用仮想PC管理用サーバ及び集計業務用仮想PC管理用サーバへの負荷分散を実現すること。
・ 統合windows認証（ntlm）に対応したロードバランシングができること。
・ ２台以上のサーバで構成し、冗長構成とすること。

(13) 情報系ロードバランサ
・ インターネット接続用仮想PC管理用サーバへの負荷分散を実現すること。
・ 統合windows認証（ntlm）に対応したロードバランシングができること。
・ ２台以上のサーバで構成し、冗長構成とすること。

(14) 政府共通 NW 用ロードバランサ
・ 政府共通NW側からのファイル転送、統計局イントラネットサーバ、家計APIサーバへのリクエストを振り分けする機能を有すること。
・ １つのIPアドレスを共有し、複数のホスト名を運用できること。
・ SSL証明書による暗号化を終端すること。
・ ２台以上のサーバで構成し、冗長構成とすること。

(15) リモートアクセス用サーバ
・ 「1.1.5リモートアクセス」を実現すること。
・ 2台以上のサーバで構成し、負荷分散による冗長構成とする。
・ 利用するネットワーク帯域の制限ができること。

(16) テレワーク用サーバ
・ 「1.1.4②テレワーク用アプリケーション接続」を実現すること。
・ 2台以上のサーバで構成し、負荷分散による冗長構成とする。

(17) Linux 用構成管理サーバ
・ 「1.2.2②Linux向け構成管理」を実現すること。
・ 1台以上のサーバで構成すること。

③ バッチ処理用仮想化基盤
（ア）「11.2②(キ)(1)仮想化基盤管理サーバ」による管理を実現すること。

（イ）1台当たり、AMD EPYC 9374F相当以上のCPUを1個以上搭載すること。
（ウ）1台当たり、メモリを512GB以上搭載すること。
（エ）25Gイーサネットを2ポート以上搭載すること。
（オ）1サーバ当たり2CPU以上搭載可能なことが望ましい。
（カ）3台以上のサーバで構成すること。
（キ）全ての物理サーバにバッチ処理ソフトウェアのライセンスを適用すること。なお、1台当たりに適用するライセンスは、JP1/Automatic Job Management System 3 - Agent（搭載する全てのCPU分のプロセッサ数ライセンス）とする。
（ク）全ての物理サーバに、Microsoft Windows Server Datacenter（コアライセンス）を適用すること。
（ケ）以下の仮想サーバを「11.2③バッチ処理用仮想化基盤」上に構築すること。
(1) バッチ処理サーバ
・ 92台以上のサーバで構成すること。
・ 各仮想サーバに、JP1/Automatic Job Management System 3 - Agent、JP1/Base、JP1/Scriptを導入すること。

④ データベースサーバ用仮想化基盤
（ア）「11.2②(キ)(1)仮想化基盤管理サーバ」による管理を実現すること。
（イ）1台当たり、AMD EPYC 9374F相当以上のCPUを1個以上搭載すること。
（ウ）1台当たり、メモリを756GB以上搭載すること。
（エ）25Gイーサネットを2ポート以上搭載すること。
（オ）1サーバ当たり2CPU以上搭載可能なこと。なお、後からCPUの増設が不可の場合、追加で同一スペックのサーバを2台用意すること。なお、コールドスタンバイ構成は不可とする。
（カ）3台以上のサーバで構成すること。
（キ）2台のサーバにデータベースソフトウェアのライセンスを適用すること。なお、適用するライセンスはMicrosoft SQLServer Enterprise Edition（コアライセンス）とする。
（ク）全ての物理サーバに、Microsoft Windows Server Datacenter（コアライセンス）を適用すること。
（ケ）以下の仮想サーバを、「11.2④データベースサーバ用仮想化基盤」上に構築すること。
(1) データベースサーバ
・ 30台以上のサーバで構成すること。
・ 各仮想サーバに、Microsoft SQLServer Enterprise Editionを導入すること。

- 詳細な設定については、データベースの利用状況により主管課と協議の上、決定すること。
- 現行の当該サーバのパフォーマンス等に関する設定を確認し、必要となる設定を導入時に行うこと。
- 次期情報システム基盤における管理者及びデータベースの管理者は別ユーザとすること。
- データベース管理者に付与するデータへのアクセス権は必要最小限とすること。
- データベース管理者への権限付与はシステム台帳と連動させること。

⑤　仮想PC（RDSH）用仮想化基盤

（ア）1台当たり、Intel Xeon Gold 6430、または、AMD EPYC 9334相当以上のCPUを1個以上搭載すること。
（イ）1台当たり、メモリを768GB以上搭載すること。
（ウ）25Gイーサネットを2ポート以上搭載すること。
（エ）7台以上のサーバで構成すること。
（オ）1サーバ当たり2CPU以上搭載可能なことが望ましい。
（カ）1サーバ当たり、メモリについてCPUを追加することなく、256GB以上追加できること。
（キ）メインストレージの接続がサポートされない場合、搭載するディスクは、All Flash（All-NVMe)とすること。実現に必要なディスク容量を確保すること。
（ク）メインストレージの接続がサポートされない場合、ユーザプロファイル領域(仮想PC（RDSH用)）として、一人当たり30GB確保すること。
（ケ）以下の仮想PCを「11.2⑤仮想PC（RDSH）用仮想化基盤」上に構築すること。また、それぞれの上で、「1.3.6不正プロセス検知」を行うこと。

(1)　インターネット接続用仮想 PC（RDSH）
- 「1.3.2仮想ブラウザ」を実現すること 。
- 20台で構成すること。

(2)　一般事務用仮想アプリケーション配信用仮想 PC
- 「1.1.3②アプリケーション配信1」を実現すること。
- 2台で構成すること。

(3)　バッチ作成用仮想 PC（RDSH）
- 4台で構成すること。
- JP1/Scriptを導入すること。

⑥　仮想PC（VDI）用仮想化基盤

（ア）「11.2②(キ)(1)仮想化基盤管理サーバ」による管理を実現すること。

（イ）1台当たり、Intel Xeon Gold 6430、または、AMD EPYC 9334相当以上のCPUを1個以上搭載すること。

（ウ）1台当たり、メモリを1024GB以上搭載すること。

（エ）25Gイーサネットを2ポート以上搭載すること。

（オ）18台以上のサーバで構成すること。

（カ）2台の物理サーバに、NVIDIA A2 Tensor コア GPU相当を搭載すること。

（キ）1サーバ当たり2CPU以上を搭載可能なことが望ましい。

（ク）以下の仮想PCを「11.2⑥仮想PC（VDI）用仮想化基盤」上に構築すること。

(1)　仮想 PC の台数は 1780 台とする。

(2)　仮想 PC の CPU（vCPU）を 2 個以上とすること。

(3)　仮想 PC のメモリは、8GB 以上とすること。

(4)　「1.3.6 不正プロセス検知」を行うこと。

⑦　集計業務用PC用仮想化基盤

集計業務用PC用仮想化基盤を以下の(ア)、(イ)、いずれかの方法で実装すること。

（ア）仮想PC(RDSH)用仮想化基盤により実装

(1)　1 台当たり、 Intel Xeon Gold 6430、または、AMD EPYC 9334 相当以上の CPU を 1 個以上搭載すること。

(2)　1 台当たり、メモリを 768GB 以上搭載すること。

(3)　25G イーサネットを 2 ポート以上搭載すること 。

(4)　8 台以上のサーバで構成すること。

(5)　1 サーバ当たり 2CPU 以上搭載可能なことが望ましい。

(6)　1 サーバ当たり、メモリについて CPU を追加することなく、256GB 以上追加できること。

(7)　メインストレージの接続がサポートされない場合、搭載するディスクは、All Flash（All-NVMe)とすること。実現に必要なディスク容量を確保すること。

(8)　メインストレージの接続がサポートされない場合、ユーザプロファイル領域(集計業務用 PC 用)として、一人当たり 30GB 確保すること。

(9)　以下の仮想 PC を構築すること。その際、契約期間中は Microsoft 365 Apps がサポートされている構成であること。また、それぞれの上で、「1.3.6 不正プロセス検知」を行うこと。

・ 統計局用仮想PC（RDSH）
  ➢ 3台で構成すること。
・ 集計業務用仮想PC（RDSH）
  ➢ 27台で構成すること。

（イ）仮想PC(VDI)用仮想化基盤により実装
(1) 「11.2②(キ)(1)仮想化基盤管理サーバ」による管理を実現すること。
(2) 1台当たり、Intel Xeon Gold 6430、または、AMD EPYC 9334相当以上のCPUを1個以上搭載すること。
(3) 1台当たり、メモリを1024GB以上搭載すること。
(4) 25Gイーサネットを2ポート以上搭載すること。
(5) 14台 以上のサーバで構成すること。
(6) 1サーバ当たり2CPU以上搭載可能なことが望ましい。
(7) 以下の仮想PCを構築すること。
・ 仮想PCの台数は1300台とする。
・ 仮想PCのCPU（vCPU）を2個以上とすること。
・ 仮想PCのメモリは、8GB以上とすること。
・ 「1.3.6不正プロセス検知」を行うこと。

（ウ）(ア)、(イ)のいずれの方法で実装した場合でも、「11.2⑤仮想PC（RDSH）用仮想化基盤」、「11.2⑥仮想PC（VDI）用仮想化基盤」と仮想PCの管理は統一されていることが望ましい。

⑧ 集計業務用仮想サーバ基盤管理
汎用集計ツール等の基盤として、以下の環境を提供すること。
（ア）「11.2②(キ)(1)仮想化基盤管理サーバ」による管理を実現すること。
（イ）1台当たり、AMD EPYC 9374F相当以上のCPUを1個以上搭載すること。
（ウ）1台当たり、メモリを256GB以上搭載すること。
（エ）25Gイーサネットを2ポート以上搭載すること。
（オ）1サーバ当たり2CPU以上搭載可能なことが望ましい。
（カ）3台以上のサーバで構成すること。
（キ）1サーバ当たり、メモリについてCPUを追加することなく、256GB以上追加できること。
（ク）以下の仮想サーバを「11.2⑧集計業務用仮想サーバ基盤」上に構築すること。
(1) 汎用集計ツール用サーバ
・ OSはLinuxを導入すること。

- 4台で構成すること。
- 台数については、契約期間中に追加する可能性がある。追加手順を作成し、対応すること。

(2) 集計業務用仮想サーバ

- OSはLinuxを導入すること。
- 10台で構成すること。
- 台数については、契約期間中に追加する可能性がある。追加手順を作成し、対応すること。

11.2.2 ストレージ要件

① メインストレージ

(ア)「1.1.8ファイル共有」を実現すること。ただし、Windowsの仮想サーバを別途構築して実現する方法でも可とする。

(イ)2筐体以上用意し、冗長構成とすること。うち、半分の筐体が完全に故障してもシステム停止、データ損失が発生しないこと。2筐体以上用意できない場合は、コントローラを冗長構成（2コントローラによるHA構成システム）とし、1セット以上用意すること。コントローラ筐体は給電チャネルを分離・冗長化し、単一障害点を排除したアーキテクチャを必須とする。ディスク領域はディスクの2重障害、シェルフ障害発生時もシステム停止、データ損失が発生しないよう2重化すること。なお、可能な限り冗長化された構成が望ましい。さらに死活監視による、ストレージの自動切り替えができる機能があることが望ましい。

(ウ)50万iops以上の性能を有すること。その際、ブロックサイズは4KBとし、Read, Writeの比率は50%:50%とする。

(エ)ユーザデータ格納領域の実効容量が450TiB以上であること。なお、ストレージ機器の圧縮機能、重複排除機能等による容量効率化の効果を考慮しないこと。

(オ)マイクロソフトSQL Serverバックアップについて、ストレージのスナップショットと連携し実施できること。スナップショットからの復元時も、ストレージOSの機能でリストアできることが望ましい。

(カ)ドライブの障害復旧後に交換したドライブへの切り戻し作業が発生しないこと。

(キ)システムを稼働させたまま、障害が発生したディスクドライブの交換を行えること。障害の自動復旧中に性能劣化が発生しないこと。

(ク)任意の LUN のスナップショットコピーを作成する機能を有すること。また、スナップショットを取得する際に稼動系のパフォーマンスに影響を与えないこと。

(ケ) ストレージシステムの機能だけで筐体間の同期もしくは非同期でのレプリケーションが動作すること。ライセンスを追加することなくレプリケーションが動作すること。
(コ) データを暗号化する機能を有すること。またデータを暗号化しても性能に影響を与えないこと。
(サ) 無停止でストレージ専用OSを更新可能なこと。
(シ) 無停止でコントローラを交換可能なこと。交換作業中においても、50万IOPS以上の性能を維持すること。
(ス) ストレージシステムの稼働中に、ドライブの追加が可能であること。また追加時に、パリティの再配置による性能劣化が起こらないこと。
(セ) ハードウェア故障時（コントローラ、ドライブ、書き込みキャッシュ、電源モジュール、ネットワークポート等）に、管理者へ SNMP Trapを用いた通知が可能であること。
(ソ) ストレージシステムのログファイルをメーカー提供のサポートに転送し、機器本体のステータス監視ができること。
(タ) リモート監視を行い、ストレージ障害時には使用者からの連絡なしに、提供者自ら障害対応を行える体制を整えること。
(チ) ストレージシステムのログファイルをメーカーサポートへ提供する場合に、暗号化もしくは秘匿化が可能であること。
(ツ) ランサムウェア等のマルウェア対策として、ストレージのスナップショット機能で取得した LUN のバックアップについて、ストレージ管理者の管理権限を用いても、設定された期間内であればストレージ内からバックアップを完全に消去することが不可能な機能を有していることが望ましい。
(テ) 保守契約について、導入初年度については年度末までの月数に応じた期間のみの契約を締結し、次年度以降は初年度と変わらない月単価で提供可能であることが望ましい。
(ト) メーカサポートエンジニアが、リモート環境からログインして対応できるサービスを通常の保守メニューの中で提供することが望ましい。
(ナ) 定期的に新しいハードウェアに無停止で交換できるサービスを有することが望ましい。また、新しいハードウェアに交換することで性能が向上することが望ましい。
(ニ) データの増加量及びストレージパフォーマンスの将来予測、それらのレポーティング機能も有することが望ましい。
(ヌ) 仮想PCのブート及びログインストームに対する対策を実装すること。また、仮想PCのブート領域については、SSDを採用すること。
(ネ) 対応プロトコルとして、iSCSI、SMBv3以上、NFSv3以上に対応していること。

11.2.3 ネットワーク機器要件

メインデータセンターに配置するNW機器は、NW仮想化技術やスイッチ類の設定により設定により柔軟に構成を変更できるものとする。

① サーバ接続用スイッチ

（ア）必要台数を用意すること。

（イ）各サーバが搭載する25Gポートを全て集線すること。

（ウ）サーバ及びストレージを集線するスイッチについては、カットスルー方式による低遅延を実現すること。その他機器に集線するスイッチについては、その限りではないが必要な性能を担保すること。

（エ）表 3に示すネットワーク構成を仮想化基盤と連携したレイヤ3機能、FW機能で実現すること。

（オ）物理トポロジーに依存しないネットワークを構成できること。レイヤ3のネットワーク上で、レイヤ2のネットワークを自由に構成できること。

（カ）仮想化基盤管理機能と連動し、仮想ハイパーバイザーと連動したルーティングが行えること。なおSDN機器ベンダー、仮想化ソフトウェアベンダー双方で動作サポートしている機能であること。

（キ）同一ホスト上、かつ異なるネットワーク間の仮想マシン間通信はホスト内部で完結し(ハイパーバイザーで処理され)、物理ルータへの転送が不要な機能を有することが望ましい。

② サーバ管理用スイッチ

（ア）必要台数を用意すること。

（イ）ポートベースVLANが構成できること。

（ウ）1台当たり1000BASE-T対応のポートを48ポート以上有すること。

③ インターネット用ファイアウォール

（ア）「1.3.5ファイアウォール」を実現すること。

（イ）以下の5箇所にファイアウォールを設置すること。

(1) 「11.7①インターネット接続回線 1（Web アクセスのサービス提供用)」にて接続するインターネットとメインデータセンターとの境界。

- 本境界に設置するFWから「1.3.9①セキュアWebゲートウェイ(SWG)」を提供するクラウドサービスとの間をIPsecまたはGREにて接続すること。

(2) 「11.7②インターネット接続回線 2（テレワーク用)」にて接続する

インターネットとメインデータセンターとの境界。
- 本境界に設置するFWでは「1.1.4①インターネットからのリモートアクセス」、「11.2②(キ)(16)テレワーク用サーバ」と連動し、インターネットから本センター内にテレワークで接続する際のセキュリティを担保する機能を提供すること。

(3) 「11.7③インターネット接続回線3（MS365用)」にて接続するインターネットとメインデータセンターとの境界。
(4) 「11.7④インターネット接続回線4（その他運用用)」にて接続するインターネットとメインデータセンターとの境界。
(5) 「11.7⑩機密性3情報持出用回線」にて接続するインターネットとメインデータセンターとの境界。
- 本境界に設置するFWでは「1.1.4①インターネットからのリモートアクセス」、「11.2②(キ)(16)テレワーク用サーバ」と連動し、インターネットから本センター内にテレワークで接続する際のセキュリティを担保する機能を提供すること。

（ウ）接続する回線とその役割に応じて必要な性能や可用性に合わせた構成を提案すること。
（エ）FWをNW仮想化によって実現することが望ましい。

④　内部ネットワーク用ファイアウォール
（ア）2台設置し、冗長構成とすること。なお、ファイアウォールを「11.2.3③(イ)(1)」及び「11.2.3③(イ)(2)」においても利用できる設定を行うこと。
（イ）以下の3箇所にファイアウォールを設置すること。
(1) インターネット接続用ネットワークと情報システム基盤内部ネットワークの境界。
(2) 持ち出し用ネットワークと集計業務用ネットワークの境界。
(3) 政府共通ネットワーク接続用ネットワークと情報システム基盤内部ネットワークの境界。

（ウ）要求性能は以下のとおり。
(1) ファイアウォールスループットは、10Gbps以上であること。

（エ）FWをNW仮想化によって実現することが望ましい。

⑤　管理LAN用ファイアウォール

（ア）管理用ネットワークと情報システム基盤の内部ネットワークとの境界にファイアウォールを設置すること。
（イ）「11.2.3③インターネット用ファイアウォール」とは異なるファイアウォールを設置すること。なお、要求性能は以下のとおり。
(1) ファイアウォールスループットは、9.5Gbps 以上であること。なお、「11.2.3④内部ネットワーク用ファイアウォール」でスループットを確保できる場合は統合することも可とする。
（ウ）FWをNW仮想化によって実現することが望ましい。

⑥　政府共通ネットワーク接続用ファイアウォール
（ア）2台設置し、冗長構成とすること。
（イ）1Gbps以上のファイアウォールスループットを有すること。
（ウ）1台当たり1000BASE-T対応のポートを8ポート有すること。
（エ）1対NNAT、IPマスカレードまたは同等の機能を有すること。
（オ）FWをNW仮想化によって実現することが望ましい。

⑦　政府共通ネットワーク接続用スイッチ
（ア）2台設置し、冗長構成とすること。
（イ）ポートベースVLANをできること。
（ウ）1台当たり1000BASE-T対応のポートを8ポート以上有すること。
（エ）NW仮想化で集約することも可とする。

11.2.4 PC要件
①　運用管理用PC
（ア）2台導入すること。
（イ）ノート型であること。
（ウ）CPUはIntel i3-1315Uプロセッサ相当以上とすること。
（エ）メモリを8GB以上搭載すること。
（オ）SSDを搭載し、ディスク容量は256GB以上であること。
（カ）OSは、日本マイクロソフト株式会社の「日本語版Windows11 Enterprise Edition」とすること。
（キ）ディスプレイは13.3インチ以上14.0インチ以下であること。
（ク）画面画素数がフルHD（1,920×1,080ドット）であること。
（ケ）キーボードは日本語配列であること。
（コ）USB接続可能なスクロール機能付きの有線光学式マウスを添付すること。
（サ）IEEE802.11a/b/g/n/ac/axに対応する無線接続が可能なこと。
（シ）1000BASE-T/100BASE-TXに対応する有線接続が可能なこと。なお、USBによる接続も可とする。

（ス）USB Type Aポートを2ポート以上、USB-Cを1ポート以上有すること。また、USBハブまたは変換ケーブルを提案する場合、本調達全体（「11.2.4① 運用管理用PC」、「11.3.3①ノート型PC1」、11.3.3②ノート型PC2」、「11.3.3③ノート型PC3」及び「11.4.4①運用管理用PC」を含む。）として、60個添付すること。
（セ）外部ディスプレイにHDMI出力が可能なこと。
（ソ）内蔵カメラを有すること。
（タ）PC本体の重量がバッテリー搭載時に1.25kg以下であること。なお、可能な限り軽量であることが望ましい。
（チ）バッテリーでの稼働時間が11時間以上であること。
（ツ）TPM2.0に対応すること。
（テ）初期導入時に主管課の指示により、BIOS設定変更作業を行うこと。
（ト）電源オフ状態から有線接続及び無線接続のネットワーク経由で電源投入が可能であること。また、必要となる管理用ソフトウェアの提供及び設定を行うこと。
（ナ）標準的なセキュリティスロットに対応した機種を選定すること。なお、小型サイズのセキュリティスロットも可とする。ただし、ワイヤーの調達は不要とする。
（ニ）10分間操作がない場合、スクリーンロックする設定を行うこと。
（ヌ）仮想化ベースのセキュリティ(VBS)を有効化すること。
（ネ）請負者が用意する「11.7⑫データ通信機器」を利用可能なこと。
（ノ）メインデータセンター内のラックに収納できること。
（ハ）情報システム基盤停止時においても本機器へのログイン及び設計書等の確認が行えるようにすること。

11.2.5 その他機器要件

① ラック内の拡張要件

（ア）ラック内に21U及び10Uの連続した空きスペースをメインデータセンター内においてそれぞれ1箇所用意すること。また、電力として100V15Aを4本用意すること。

11.2.6 施設・設備要件

① データセンター立地要件

（ア）メインデータセンターは、統計センターから半径50km圏内にあること。
（イ）メインデータセンターは、統計センターを午前9時から午後6時の間に出発した際に、タクシーを除く公共交通機関の利用と徒歩で概ね2時間以内に到着可能な範囲にあること。

② その他

（ア）「11.6施設・設備共通要件」を満たすこと。

11.3 統計センター設置機器要件

統計センターにおける設置機器の構成を「別添2 次期情報システム基盤概要構成図」に示す。なお、ネットワーク機器等の設置機器に対する要件は「11.3.1ネットワーク機器要件」から「11.3.5統計センターが用意する機器」に示す。

11.3.1 ネットワーク機器要件

① バックボーン用スイッチ

（ア）2台設置し、冗長構成とすること。
（イ）筐体内で電源を冗長化すること。
（ウ）レイヤ3スイッチであること。
（エ）パケットフィルタリングをできること。
（オ）スイッチ跨ぎのリンクアグリゲーションをできること。
（カ）1台当たりGbEthernetに対応したポートを36ポート以上用意すること。
（キ）1台当たり1000BASE-SXに対応したポートを3ポート以上用意すること。なお、3ポートは、各フロアとの接続に使用すること。
（ク）メインデータセンターと統計センターを結ぶ通信回線をアクティブ/スタンバイで接続すること。
（ケ）「11.3.1③執務室用スイッチ1」を1台接続すること。
（コ）「11.3.1②フロア用スイッチ」等を接続すること。

② フロア用スイッチ

（ア）3フロアを対象に、各フロア2台を冗長構成として設置すること。
（イ）筐体内で電源を冗長化すること。
（ウ）「11.2①(ク)(29)RADIUSサーバ」と連携したIEEE802.1x認証をできること。
（エ）「11.2①(ク)(29)RADIUSサーバ」と連携した認証VLANにより、シンクライアント用ネットワーク、持込・持出用ネットワーク、複合機用ネットワーク、ドキュメントスキャナ用ネットワーク及び管理用ネットワークについてポートへの自動割当てをできること。なお、リモートから本スイッチに接続された端末への電源投入に関しては端末認証前でも実現できること。
（オ）スイッチを跨いだリンクアグリゲーションをできること。
（カ）MACアドレス認証に対応すること。
（キ）1台当たりGbEthernetに対応したポートを20ポート以上用意すること。
（ク）1台当たり1000BASE-SXに対応したポートを2ポート以上用意すること。
（ケ）「11.3.1①バックボーン用スイッチ」と接続すること。なお、既設のマルチモード光ファイバ（SCコネクタ）ケーブルを使用することも可とする。

利用できるケーブルは以下とする。
　フロア用スイッチを設置する部屋のスプライスボックスと情報システム室のスプライスボックスの間
・　マルチモード光ファイバ(ＳＣコネクタ)2芯×２（空きあり）

（コ）「11.3.1③執務室用スイッチ1」と接続すること。なお、既設のCAT6ケーブルを使用することも可とする。

③　執務室用スイッチ1
（ア）58台設置し、冗長構成とすること。
（イ）「11.3.1②フロア用スイッチ」と本調達で導入するPC及び統計センターが用意するノート型PC等を接続できること。
（ウ）導入する機器以外の接続を拒否できること。また、必要に応じて許可できること。
（エ）「11.2①(ク)(29)RADIUSサーバ」と連携したIEEE802.1x認証ができること。
（オ）MACアドレス認証に対応すること。
（カ）「11.2①(ク)(29)RADIUSサーバ」と連携した認証VLANにより、シンクライアント用ネットワーク、持込・持出用ネットワーク、複合機用ネットワーク、ドキュメントスキャナ用ネットワーク及び管理用ネットワークについてポートへの自動割当てをできること。なお、リモートから本スイッチに接続された端末への電源投入に関しては端末認証前でも実現できること。
（キ）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不能な状態とし、かつ一定時間経過後、自動的に再度利用可能にする機能を有すること。
（ク）1台当たりGbEthernetに対応したポートを48ポート以上用意すること。
（ケ）メインデータセンターに設置する「11.3.1⑤(ア)無線LANアクセスポイント」と同一メーカーの製品であること。
（コ）執務室スイッチ1は全台を集中管理できること。
（サ）無線LANAPにPoE給電できること。

④　執務室用スイッチ2
（ア）3台以上設置すること。
（イ）「11.3.1③執務室用スイッチ1」「(イ)」から「(キ)」、「(ケ)」から「(サ)」の機能を有すること。
（ウ）1台当たりGbEthernetに対応したポートを10ポート以上用意すること。
（エ）ファンレスであること。

⑤　無線LANアクセスポイント

（ア）無線LANアクセスポイント

(1)　無線 LAN コントローラ機能を有すること。

(2)　IEEE802.11a/b/n/ac/ax に対応すること。

(3)　IEEE802.11a/n/ac においては、W52、W53、W56 に対応すること。

(4)　IEEE802.11w 規格に対応した機能を有すること。

(5)　2.4GHz 帯及び 5GHz 帯を同時利用できること。

(6)　2×2:2MIMO に対応すること。

(7)　IEEE802.3af または IEEE802.3at に基づく PoE 電源供給により動作すること。

(8)　通電状態を表示する LED を有すること。

(9)　WPA、WPA2、EAP-TTLS、EAP-PEAP 及び LEAP に対応すること。

(10)　「11.2①(ク)(29)RADIUS サーバ」と連携した IEEE802.1x 認証をできること。

(11)　「11.2①(ク)(29)RADIUS サーバ」と連携した認証 VLAN により、シンクライアント用ネットワーク、持込・持出用ネットワーク、ドキュメントスキャナ用ネットワーク及び管理用ネットワークについてポートへの自動割当てをできること。なお、リモートから本アクセスポイントに接続された端末への電源投入に関しては端末認証前でも実現できること。

(12)　設置したアクセスポイント間で電波自動出力調整できること。

(13)　ビームフォーミング技術等により通信の信頼性と RF のカバレージを改善できること。

(14)　セキュリティワイヤーにより机等に固定できること。

(15)　無線 LAN アクセスポイント全台を集中管理できること。

(16)　無線の不正侵入検知機能を有すること。

(17)　SSID を隠蔽できること。

(18)　サイトサーベイを行い、統計センター及び統計データ利活用センターで最適な台数・配置を行うこと。なお、当該機器は天井裏に設置すること。

(19)　冗長化した執務室スイッチのうち 1 台が停止した場合においても、無線接続が支障なく継続できる提案をすること。なお、ノート型 PC1 及びノート型 PC2 については、無線アクセスポイントに接続する。無線 LAN を利用可能とする範囲は現行同様とする。必要となるアクセスポイント台数を導入すること。

（イ）無線LAN可視化

(1)　導入する全ての無線 LAN アクセスポイントを可視化できること。

(2) 本調達で導入するPC及び統計センターが用意するノート型PCの無線LANネットワークの接続経路を表示し、経路上の問題箇所を一括表示できること。
(3) 無線LAN接続環境の品質を数値化してグラフィカルに表示できること。本機能はクラウドサービスで実現できること。

⑥ 他システム接続用ファイアウォール
（ア）本機器は統計局システム、OCRシステム及び監視カメラシステムへの接続を想定している。
（イ）2台以上設置し、冗長構成とすること。
（ウ）仮想ファイアウォールを10台以上構成できること。
（エ）9.5Gbps以上のファイアウォールスループットを有すること。
（オ）1台当たり1000BASE-SX対応のポートを1ポート以上有すること。なお、OCRシステムとの接続には本ポートを利用すること。
（カ）1台当たり1000BASE-T対応のポートを12ポート有すること。
（キ）パケット及びステートフルインスペクションの各々でフィルタリングできること。
（ク）NAT機能を有すること。
（ケ）1対NNAT、IPマスカレードまたは同等の機能を有すること。
（コ）IPv4及びIPv6によるアクセス制御が行えること。
（サ）アクセス履歴を「1.2.3②ログ保管」に転送できること。
（シ）利用ユーザ数は無制限であること。
（ス）筐体内で電源を冗長化すること。

11.3.2 サーバラック要件
① サーバラック
（ア）42Uラックであること。
（イ）ラックマウント型サーバを搭載できること。
（ウ）搭載する機器は以下のとおり。
(1) 「11.3.1①バックボーン用スイッチ」
(2) 「11.3.1⑥他システム接続用ファイアウォール」
(3) 回線終端装置

（エ）転倒防止措置としてスタビライザを設置すること。なお、床への固定は不要とする。
（オ）施錠できること。

11.3.3 PC要件

① ノート型PC1

(ア) 541台導入すること。

(イ) 「1.1.3①仮想PC管理」を利用できること。

(ウ) 「11.2.4①運用管理用PC」の「(イ)」及び「(キ)」から「(ネ)」の機能を有すること。

(エ) CPUはIntel i3-1315Uプロセッサ相当以上とすること。

(オ) メモリを8GB以上搭載すること。

(カ) SSDを搭載し、ディスク容量は256GB以上であること。

(キ) OSは、日本マイクロソフト株式会社の「日本語版Windows11 Enterprise Edition」とすること。

(ク) USBにはICカードリーダー/ライターと有線光学式マウス及び「11.7⑫データ通信機器」を同時に接続できること。

(ケ) 通信の制御やログイン時に必要なソフトウェアやドライバを導入できるものを選定すること。

(コ) 本機器はシンクライアントとして運用することを想定している。なお、拡張ディスプレイ、WIFI接続、オーディオデバイスの設定変更が可能とすること。

② ノート型PC2

(ア) 60台導入すること。

(イ) 「11.2.4①運用管理用PC」の「(イ)」及び「(キ)」から「(ネ)」の機能を有すること。

(ウ) CPUはIntel Core i3-1315U相当以上またはこれと同等以上の性能を有すること。

(エ) メモリを8GB以上搭載すること。

(オ) SSDを搭載し、ディスク容量は256GB以上であること。

(カ) OSは、日本マイクロソフト株式会社の「日本語版Windows11 Enterprise Edition」とすること。

(キ) 以下の要件を満たすポータブル型ブルーレイディスクドライブを60台添付すること。

(1) 外付け型であること。

(2) 書き込み速度として、BD-R6 倍速以上、BD-R (2 層) 6 倍速以上、DVD-R8 倍速以上、CD-R24 倍速以上の性能を有すること。

(3) OS に対応した書き込みソフトウェアを添付すること。

(4) OS に対応したブルーレイディスク再生ソフトウェアを添付すること。

（ク）「1.3.4エンドポイントマルウェア対策」を導入すること。
（ケ）「1.3.6不正プロセス検知」を導入すること。

③　ノート型PC3
（ア）2台導入すること。
（イ）「11.2.4①運用管理用PC」の「(イ)」及び「(キ)」から「(ネ)」の機能を有すること。
（ウ）CPUはIntel Core i7-1355U相当以上またはこれと同等以上の性能を有すること。
（エ）メモリは32GB以上搭載すること。
（オ）SSDを搭載し、搭載するディスク容量は500GB以上であること。
（カ）OSは、日本マイクロソフト株式会社の「日本語版Windows11 Enterprise Edition」とすること。
（キ）VMware Workstation Proを導入すること。

④　ノート型PC4
（ア）2台導入すること。
（イ）ノート型であること。
（ウ）Apple M2相当以上の性能を有すること。
（エ）メモリ16GB以上搭載すること。
（オ）SSDを搭載すること。
（カ）搭載するディスク容量は500GB以上であること。
（キ）ディスプレイは、Retinaディスプレイ14インチであること。
（ク）スクロール機能付き光学式マウスを添付すること。
（ケ）1000BASE-T/100BASE-TXに対応する有線接続が可能なこと。なお、USBによる接続も可とする。
（コ）IEEE802.11a/b/g/n/acに対応する無線接続が可能なこと。
（サ）外部ディスプレイにHDMI端子で接続できること。なお、必要な場合、変換ケーブルを添付すること。
（シ）OSは、macOSとすること。
（ス）VMware Fusionを導入すること。
（セ）10分間操作がない場合、スクリーンロックする設定を行うこと。

⑤　ノート型PC5
（ア）2台導入すること。
（イ）「11.2.4①運用管理用PC」の「(イ)」及び「(キ)」から「(ネ)」の機能を有すること。
（ウ）CPUはIntel i3-1315Uプロセッサ相当以上とすること。

（エ）メモリを8GB以上搭載すること。
（オ）SSDを搭載し、ディスク容量は256GB以上であること。
（カ）OSは、日本マイクロソフト株式会社の「日本語版Windows11 Enterprise Edition」とすること。
（キ）USBにはICカードリーダー/ライターと有線光学式マウス及び「11.7⑫データ通信機器」を同時に接続できること。
（ク）通信の制御やログイン時に必要なソフトウェアやドライバを導入できるものを選定すること。
（ケ）本PCは、インターネット接続用に利用することを想定している。

⑥　ノート型PC6
（ア）30台導入すること。
（イ）ディスプレイは13.3インチ以上14.0インチ以下であること。
（ウ）キーボードは日本語配列であること。
（エ）IEEE802.11a/b/g/n/acに対応する無線接続が可能なこと。
（オ）1000BASE-T/100BASE-TXに対応する有線接続が可能なこと。なお、USBによる接続も可とする。
（カ）USB Type Aポートを2ポート以上、USB-Cを1ポート以上有すること。また、USBハブまたは変換ケーブルによる提案も可とする。
（キ）CPUはIntel Celeron5205U相当以上またはこれと同等以上の性能を有すること。
（ク）メモリを8GB以上搭載すること。
（ケ）SSDを搭載し、ディスク容量は128GB以上であること。
（コ）OSは、日本マイクロソフト株式会社の「日本語版Windows　10 IoT Enterprise LTSC 」とすること。
（サ）Windows Server クライアントアクセスライセンス(ユーザCAL)を添付すること。
（シ）機密性3情報持出専用端末として設計すること。
（ス）テレワーク用アプリケーション接続 を経由し、ファイル転送が使用可能なこと。
（セ）エンドポイントマルウェア対策として、シグネチャアップデートに依存せずに未知の脅威に対して検知できること。
（ソ）不正プロセス検知を導入すること。
（タ）OSログオン時の認証は、「1.3.1③ワンタイムパスワードトークン認証」または「1.3.1②ICカード認証」による2要素認証とすること。また、そのために必要となる機器は添付すること。

⑦　デスクトップ型PC

（ア）579台導入すること。
（イ）「1.1.3①仮想PC管理」を利用できること。
（ウ）デスクトップ型であること。
（エ）CPUはIntel i3-13100Tプロセッサ相当以上とすること。
（オ）メモリを8GB以上搭載すること。
（カ）SSDを搭載し、ディスク容量は256GB以上であること。
（キ）OSは、日本マイクロソフト株式会社の「日本語版Windows11 Enterprise Edition」とすること。
（ク）キーボードは日本語配列であること。
（ケ）USB接続可能なスクロール機能付きの有線光学式マウスを添付すること。
（コ）IEEE802.11a/b/g/n/acに対応する無線接続が可能なこと。
（サ）1000BASE-T/100BASE-TX/10BASE-Tに対応する有線接続が可能なこと。
（シ）外部ディスプレイにHDMI出力が可能なこと。
（ス）TPM2.0に対応すること。
（セ）初期導入時に主管課の指示により、BIOS設定変更作業を行うこと。
（ソ）電源オフ状態から有線接続ネットワーク経由で電源投入が可能であること。また、必要となる管理用ソフトウェアの提供及び設定を行うこと。
（タ）標準的なセキュリティスロットに対応した機種を選定すること。なお、小型サイズのセキュリティスロットも可とする。ただし、ワイヤーの調達は不要とする。
（チ）10分間操作がない場合、スクリーンロックする設定を行うこと。
（ツ）仮想化ベースのセキュリティ(VBS)を有効化すること。

⑧　PC用ソフトウェア
（ア）「表 4　PCソフトウェア一覧」のソフトウェアを主管課が指定するPCにインストールすること。なお、別紙１のユーザ数を参考に最適なライセンス数の提案などの経費削減に取り組むこと。

表 4　PC ソフトウェア一覧

No.	ソフトウェア名	メーカー名	数量	備考
1	Microsoft 365 E3	日本マイクロソフト（株）	1,450	ユーザライセンス
2	Microsoft Power Apps プレミアムコネクタライセンス	日本マイクロソフト（株）	60	-
3	Microsoft SQLServer Management Studio	日本マイクロソフト（株）	全台	-
4	Acrobat Reader DC	アドビシステムズ（株）	全台	-
5	一太郎（ビューア）	（株）ジャストシステム	全台	-

No.	ソフトウェア名	メーカー名	数量	備考
6	7-Zip	-	全台	-
7	IC カード認証に必要なソフトウェアを導入すること。IC カード認証サーバで一元管理が可能なこと。	-	1,437	デバイスライセンス
8	Adobe Acrobat Standard	アドビシステムズ（株）	35	デバイスライセンス
9	Adobe Acrobat Professional	アドビシステムズ（株）	5	デバイスライセンス
10	JP1/Script アクセスライセンス	（株）日立製作所	136	アクセスライセンス
11	JP1/AutomaticJobManagementSystem3-view	（株）日立製作所	3	デバイスライセンス
12	コリャ英和！一発翻訳マルチリンガル	ロゴヴィスタ（株）	5	デバイスライセンス
13	Microsoft Visual Studio Professional Subscription + GitHub Enterprise	日本マイクロソフト（株）	164	ユーザライセンス
14	Microsoft Visual Studio Enterprise Subscription + GitHub Enterprise	日本マイクロソフト（株）	2	ユーザライセンス
15	Adam-Rex	ゼッタテクノロジー（株）	27	デバイスライセンス
16	Paint Shop Pro	コーレル（株）	4	デバイスライセンス
17	LEADTOOLS Imaging Pro 開発ライセンス	(株)コンポーネントソース	7	ユーザライセンス
18	LEADTOOLS Imaging Pro 内部配布ライセンス（シングル）	(株)コンポーネントソース	無制限	ユーザライセンス
19	ComponentOne Studio for WinForms	メシウス(株)（旧グレープシティ（株)）	65	ユーザライセンス
20	EmEditor Professional	（株）エムソフト	※3	デバイスライセンス
21	Opttech Sort	（株）エージーテック	136	ユーザライセンス
22	ExcelCreator	アドバンスソフトウェア（株）	133	デバイスライセンス ※4
23	SAS/STAT	SASInstituteJapan（株）	2	デバイスライセンス
24	SAS/ETS	SASInstituteJapan（株）	2	デバイスライセンス

No.	ソフトウェア名	メーカー名	数量	備考
25	BaseSAS	SASInstituteJapan（株）	2	デバイスライセンス
26	SAS Analytics Pro	SASInstituteJapan（株）	20	デバイスライセンス
27	R	フリーソフト	全台	-
28	Sandcastle	フリーソフト	105	-
29	WinMerge	フリーソフト	全台	-
30	MANDARA	フリーソフト	380	-
31	「1.3.6 不正プロセス検知」を導入すること。	-	※5	デバイスライセンス
32	NVIDIA Virtual PC	NVIDIA	10	-
33	動画編集ソフト	提案による	10	※6
34	USB シンクライアントを実現するソフトウェア	提案による	必要数	-

※1 フリーソフトは、種類及び数量について変更する可能性がある。

※2ソフトウェアが正常に稼働しない場合は、主管課と請負者で対応について協議すること。

※3 「11.2⑦集計業務用PC用仮想化基盤」を「(ア)仮想PC(RDSH)用仮想化基盤により実装」で実現する場合は、1926ライセンス、「(イ)仮想PC(VDI)用仮想化基盤により実装」で実現する場合は3196ライセンス導入すること。

※4「11.2⑦集計業務用PC用仮想化基盤」を「(ア)仮想PC(RDSH)用仮想化基盤により実装」で実現する場合は、配布ライセンスも導入すること。

※5 「11.2⑦集計業務用PC用仮想化基盤」を「(ア)仮想PC(RDSH)用仮想化基盤により実装」で実現する場合は、1952ライセンス、「(イ)仮想PC(VDI)用仮想化基盤により実装」で実現する場合は3222ライセンス導入すること。

※6 mp4ファイルの部分的な追加、差し替え、削除等の編集及び音量の調整等ができる機能を有する統合型動画編集ソフトウェアとする。

11.3.4 周辺機器

① ケーブルテスター

（ア）ネットワークケーブル（RJ-45コネクタ）に対応すること。

（イ）伝送スピード（10/100/1000BASE）のサポートの可否を判定できること。

（ウ）ケーブル長（90mまで）の測定できること。

（エ）ワイヤーマップを表示できること。

（オ）スプリットペアを検知できること。

（カ）ケーブル終端子を4つ以上添付すること。

（キ）トーン信号によりケーブルの探索が行えること。なお、プローブを添付すること。
（ク）予備バッテリーを添付すること。なお、乾電池の場合は、充電式電池2セット及び充電器を添付すること。
（ケ）キャリングケースを添付すること。
（コ）1台導入すること。

② ハードウェアトークン
（ア）「11.2①(ク)(20)ワンタイムパスワード認証サーバ」と連携し、「1.3.1③ワンタイムパスワードトークン認証」を実現すること。
（イ）480台以上用意すること。

③ ICカードリーダー/ライター
（ア）「1.3.1②ICカード認証」の利用に必要な設定をすること。
（イ）USBケーブルがないこと。また、他のポートに干渉しないように設計すること。
（ウ）1,180台導入すること

11.3.5 統計センターが用意する機器

統計センターが用意する機器を「表 5 統計センターが用意する機器」に示す。主管課の指示に従い設定及び設置作業を行うこと。なお、各機器の仕様は、資料閲覧で確認すること。

表 5 統計センターが用意する機器

No.	機器名	数量	備考
1	PC用ディスプレイ	1,300台	「11.3.3①ノート型PC1」等に接続して利用する。
2	プロジェクタ	9台	-
3	液晶表示装置	3台	-
4	ICカード	600枚	「1.3.1②IC カード認証」の利用に必要な設定をすること。
5	環境監視装置	2台	「11.3.2① サーバラック」に導入すること。 Linux用監視サーバから通知できること。
6	USBシンクライアント用メディア	300台	USBシンクライアント用ソフトウェアを導入すること。 1台ずつ異なるクライアン

No.	機器名	数量	備考
			ト証明書を導入すること。
7	Web 会議用カメラ	4 台	-
8	Web 会議用スピーカー	4 台	-
9	ノート型 PC	300 台	
10	集計業務用キーボード	800 台	-
11	スマートカード	100 台	管理者権限の認証用に利用する。 USB-A ポートに挿入または NFC 経由で認証できること。 FIDO2 対応とすること。
12	ドキュメントスキャナ	10 台	ノート型 PC2 に接続して利用することを想定する。
13	その他ソフトウェア	約 70 本	統計センターでライセンスを所有するもの。
14	その他プリンタ	1 台	統計センターに既設のもの。

11.3.6 施設・設備要件

① 統計センター設置機器にケーブル（電源ケーブル及びネットワークケーブル）を接続すること。

11.4 バックアップデータセンター設置機器要件

バックアップデータセンターにおける設置機器の構成を「別添2 次期情報システム基盤概要構成図」に示す。なお、サーバ等の設置機器に対する要件は「11.4.1 サーバ要件」から「11.4.5その他機器要件」に示す。

11.4.1 サーバ要件

① 災害対策用仮想化基盤

(ア) 「11.4.1①(ク)(3)災害対策用仮想化基盤管理サーバ」による管理を実現すること。

(イ) 1台当たり、Intel Xeon Gold 6430、または、AMD EPYC 9334相当以上のCPUを1個以上搭載すること。

(ウ) 1台当たり、メモリを384GB以上搭載すること。

(エ) 25Gイーサネットを2ポート以上搭載すること。

(オ) 1サーバ当たり2CPU以上搭載可能なことが望ましい。

(カ) 2台以上のサーバで構成すること。

(キ) 全ての物理サーバにMicrosoft Windows Server Datacenter（コアライセ

ンス）を適用すること。

（ク）以下の仮想サーバを「11.4.1①災害対策用仮想化基盤」上に構築すること。

(1) 災害対策用認証サーバ

- 2台以上のサーバで構成すること。
- 「11.2①(ク)(15)認証サーバ1」と連携すること。

(2) 災害対策用データベースサーバ

- 必要数のサーバで構成すること。
- 「11.2④(ケ)(1)データベースサーバ」のデータベースを非同期に複製できること。

(3) 災害対策用仮想化基盤管理サーバ

- 「1.2.1仮想化基盤管理」を実現すること。
- 1台以上のサーバで構成すること。

(4) 災害対策用仮想 PC 管理サーバ

- 「1.1.3①仮想PC管理」の機能により、「11.4.1①(ク)(10)災害対策用仮想PC」を管理する仕組みとすること。
- 2台以上のサーバで構成し、負荷分散による冗長化及び管理情報をデータベースに格納し高可用性を確保できる構成とする。

(5) 災害対策用バッチ実行サーバ

- JP1/Scriptを導入すること。
- 2台以上のサーバで構成すること。

(6) DHCP サーバ

- 「1.2.10DHCP」を実現すること。
- 2台以上のサーバで構成し、冗長構成とすること。

(7) 災害対策用共用ロードバランサ

- 災害対策用仮想PC管理用サーバへの負荷分散を実現すること。
- 統合Windows認証（ntlm）に対応したロードバランシングができること。
- 2台以上のサーバで構成し、冗長構成とすること。

(8) 災害対策用 KMS サーバ

- Microsoft製品のボリュームライセンス認証機能を提供すること。

- バックアップセンタの災害対策用KMSサーバと連動して、どちらかが障害等で停止したとしても継続して機能を提供できること。
- 1台以上のサーバで構成すること。

(9) 災害対策用テレワーク用サーバ
- 「1.1.4②テレワーク用アプリケーション接続」を実現すること。

(10) 災害対策用仮想 PC
- 仮想PCの台数は20台とする。
- 仮想PCのCPU（vCPU）を2個以上とすること。
- 仮想PCのメモリは、8GB以上とすること。
- 「1.3.6不正プロセス検知」を行うこと。
- メインデータセンターで稼動する仮想PCの最新のマスタイメージを利用できるように構成すること。

11.4.2 ストレージ要件

① 災害対策用ストレージ

（ア）「11.2.2①メインストレージ」に格納している全てのデータを非同期レプリケーションできること。

（イ）35万iops以上の性能を有すること。その際、ブロックサイズは4KBとし、Read, Writeの比率は50%:50%とする。もしくはオールフラッシュストレージで構成すること。

（ウ）メインデータセンターとの遠隔地バックアップについては、「9. 継続性に関する事項」のバックアップ要件を満たす構成とすること。

（エ）コントローラは冗長構成（2コントローラによるHA構成システム）とし、1セットを用意すること。

（オ）主要なコンポーネントは冗長構成とし、故障時にはストレージサービスを停止することなく交換できること。

（カ）ディスク障害復旧時にスペアディスクの切り戻し作業が発生しないこと。

11.4.3 ネットワーク機器要件

バックアップデータセンターに配置するNW機器は、NW仮想化技術やスイッチ類の設定により柔軟に構成を変更できるものとする。

① サーバ接続用スイッチ

（ア）必要台数を用意すること。

（イ）各サーバが搭載する25Gポートを全て集線すること。

（ウ）サーバ及びストレージを集線するスイッチについては、カットスルー方式

による低遅延を実現すること。その他機器に集線するスイッチについては、その限りではないが必要な性能を担保すること。
（エ）ネットワークを仮想化基盤と連携したレイヤ3機能、FW機能で構成できること。
（オ）物理トポロジーに依存しないネットワークを構成できること。レイヤ3のネットワーク上で、レイヤ2のネットワークを自由に構成できること。
（カ）仮想化基盤管理機能と連動し、仮想ハイパーバイザーと連動したルーティングが行えること。なおSDN機器ベンダー、仮想化ソフトウェアベンダー双方で動作サポートしている機能であること。
（キ）同一ホスト上、かつ異なるネットワーク間の仮想マシン間通信はホスト内部で完結し(ハイパーバイザーで処理され)、物理ルータへの転送が不要な機能を有することが望ましい。

② サーバ管理用スイッチ
（ア）1台当たり1000BASE-T対応のポートを必要数分有すること。
（イ）ポートベースVLANが構成できること。

③ テレワーク用ファイアウォール
（ア）「1.3.5ファイアウォール」を実現すること。
（イ）「11.7⑥バックアップデータセンター接続用回線」にて接続するインターネットとバックアップデータセンターとの境界に設置すること。
（ウ）本境界に設置するFWでは「1.1.4①インターネットからのリモートアクセス」、「11.4.1①(ク)(9)災害対策用テレワーク用サーバ」と連動し、インターネットから本センター内にテレワークで接続する際のセキュリティを担保する機能を提供すること。
（エ）Microsoft365との接続を行えること。
（オ）接続する回線とその役割に応じて必要な性能や可用性に合わせた構成を提案すること。
（カ）FWをNW仮想化によって実現することが望ましい。

11.4.4 PC要件
① 運用管理用PC
（ア）2台導入すること。
（イ）「11.2.4①運用管理用PC」の「(イ)」から「(ネ)」の機能を有すること。
（ウ）バックアップデータセンター内のラックに収納できること。
（エ）情報システム基盤停止時においても本機器へのログイン及び設計書等の確認が行えるようにすること。

11.4.5 その他機器要件

① ラック内の拡張要件

（ア）ラック内に10U程度の連続した空きスペースをバックアップデータセンター内において1箇所用意すること。また、電力として100V15Aを2本用意すること。

11.4.6 施設・設備要件

① データセンター立地要件

（ア）バックアップデータセンターは、メインデータセンターとの同時被災を回避するため、メインデータセンターから300km以上離れた日本国内の遠隔地とすること。

（イ）バックアップデータセンターは、統計データ利活用センターから100km圏内で、統計データ利活用センターを午前9時から午後6時の間に出発した際に、タクシーを除く公共交通機関の利用と徒歩で3時間以内に到着できること。

② その他

（ア）「11.6施設・設備共通要件」を満たすこと。

11.5 統計データ利活用センター設置機器要件

統計データ利活用センターにおける設置機器の構成を「別添2 次期情報システム基盤概要構成図」に示す。なお、サーバ等の設置機器に対する要件は「11.5.1ネットワーク機器要件」に示す。

11.5.1 ネットワーク機器要件

① 拠点用コアスイッチ

（ア）2台設置し、冗長構成とすること。

（イ）レイヤ3スイッチであること。

（ウ）パケットフィルタリングをできること。

（エ）1台当たりGbEthernetに対応したポートを24ポート以上用意すること。

（オ）メインデータセンターと統計データ利活用センターを結ぶ通信回線をアクティブ/スタンバイで接続すること。

（カ） 「11.5.1③執務室用スイッチ」等を接続すること。

② 無線LANアクセスポイント

（ア）「11.3.1⑤(ア)無線LANアクセスポイント」と同じ要件とすること。

③　執務室用スイッチ

（ア）2台設置し冗長構成とすること。

（イ）「11.3.1③執務室用スイッチ」と同一製品とすること。

11.6 施設・設備共通要件

11.6.1 データセンター要件

①　データセンターの施設要件

（ア）日本データセンター協会が定める「データセンターファシリティスタンダード」の分類における以下の条件を満たすこと。

(1) 建物（B）：ティア 4 相当

(2) セキュリティ（S）：ティア 4 相当

(3) 電気設備（E）：ティア 3 相当以上

(4) 空調設備（H）：ティア 3 相当以上

(5) 通信設備（T）：ティア 3 相当以上

(6) 設備運用（M）：ティア 4 相当

（イ）設備を集中管理及び制御する管理室を設置していること。

（ウ）災害時対応計画が作成されており、災害時にも有人による運用を継続できることを証明すること。

（エ）データセンター内で使用するための電話を貸し出しできること。

（オ）運用管理用PC、製品マニュアル及びその他機器の付属品等について施錠可能な保管場所を提供すること。

（カ）持込・持出管理を実施していること。以下の対策が実施されていることが望ましい。

(1) 手荷物検査

(2) X 線検査

(3) 金属探知ゲート

(4) 3D ボディスキャナ

②　データセンターの立地要件

（ア）データセンターは、公共交通機関の最寄りの駅、バス停等から徒歩15分以内に到着できること。

（イ）データセンターから直線距離で100m以内に消防法（昭和23年法律第186号）による指定数量以上の危険物製造設備、火薬製造設備及び高圧ガス設備がないこと。

③　サービス要件

（ア）調達機器についてネットワーク経由で実施できない作業（LED表示及び点

灯状態の確認、電源のON/OFF等）を主管課の指示に基づき即時にオペレータが代行するサービスを有すること。

（イ）ラック標準の鍵と異なる鍵で施錠できること。なお、データセンターのラックを使用する場合は、データセンター標準の鍵で施錠することも可とする。

11.7 通信回線等要件

① インターネット接続回線1（Webアクセスのサービス提供用）

（ア）2回線でメインデータセンターに接続すること。主・副回線とも、双方向200Mbps以上の帯域保証型インターネット接続サービスを提供すること。アクティブ系に障害が発生した場合、自動でスタンバイ系に切り替わり、アクティブ系が復旧した際も同様に自動で切り替わること。

（イ）「1.3.9①セキュアWebゲートウェイ(SWG)」と接続すること。

（ウ）主回線は、故障時間及び遅延時間またはこれに相当する可用性を表すサービス品質保証を定めた上で、保証内容を提案時に明示すること。なお、障害通知については、主回線はサービス品質目標を定めた上で、品質目標の内容を提案時に明示すること。

② インターネット接続回線2（テレワーク用）

（ア）2回線でメインデータセンターに接続し、主回線、副回線とも、双方向100Mbps以上の帯域保証型のインターネット接続サービスを提供すること。

（イ）アクティブ系に障害が発生した場合、自動でスタンバイ系に切り替わり、アクティブ系が復旧した際も同様に自動で切り替わること。

（ウ）「1.1.4①インターネットからのリモートアクセス」と接続すること。

③ インターネット接続回線3（MS365用）

（ア）Microsoft365サービスとの接続を行うこと。

（イ）Microsoft Azure Peering Serviceまでの経路を冗長化すること。

（ウ）政府共通NW用メールサーバをNATにて公開できること。

（エ）メール無害化及び誤送信防止サーバをNATにて公開できること。

（オ）回線帯域については、利用者数を参考に提案すること。

④ インターネット接続回線4（その他運用用）

（ア）メインデータセンターに接続すること。回線はベストエフォート1Gbpsとすること。

（イ）日本国内のIPv4及びIPv6の固定グローバルアドレスを1個以上提供すること。

⑤　WAN回線

（ア）WAN回線として、以下の間を接続する回線を用意すること。

(1)　メインデータセンター・統計センター間（1Gbps 以上）

(2)　メインデータセンター・統計データ利活用センター間（100Mbps 以上）

(3)　メインデータセンター・バックアップデータセンター間（必要な帯域）

（イ）通信回線は、主回線・副回線とも閉域網（専用線または広域イーサ）とすること。ただし、バックアップデータセンター間は主回線のみでの提案を可とする。

（ウ）アクティブ系に障害が発生した場合、自動でスタンバイ系に切り替わり、アクティブ系が復旧した際も同様に自動で切り替わること。ただし、バックアップデータセンター間は除く。

（エ）統計センターに設置する回線終端装置とメインデータセンターに設置する回線終端装置間の主回線の往復遅延時間は3msec未満であること。なお、往復遅延時間が3msec未満であることの根拠データを示すこと。

（オ）バックアップを行うために必要となる帯域を用意すること。

（カ）VDIの画面転送の通信等を優先して通信するように設計すること。また、ストレージ同期の通信は通常利用を阻害しないように設計すること。

（キ）品質保証内容について提案時に明示すること。

⑥　バックアップデータセンター接続用回線

（ア）双方向100Mbps以上の回線をバックアップデータセンターに接続し、インターネット接続サービスを提供すること。なお、ベストエフォート型も可とする。

（イ）「1.1.4①インターネットからのリモートアクセス」と接続すること。

（ウ）Microsoft365サービスとの接続を行うこと。

⑦　統計センター接続用回線

（ア）双方向1Gbps以上の回線を統計センターに接続し、インターネット接続サービスを提供すること。なお、ベストエフォート型も可とする。

⑧　統計データ利活用センター用回線

（ア）双方向1Gbps以上の回線を統計データ利活用センターに接続し、インターネット接続サービスを提供すること。なお、ベストエフォート型も可とする。

⑨　別途契約するセキュリティ監視との接続回線及びVPNゲートウェイ

（ア）別途契約するセキュリティ監視との接続回線はインターネット回線とし、ベストエフォート100Mbps以上とすること。

（イ）セキュリティ監視のSOCとインターネットVPN（IPsec利用)で接続できること。なおメインデータセンター側はNW仮想化で対応することが望ましいが、IPsecの機器を調達し設置することも可とする。

（ウ）単一のVPNゲートウェイから別途契約するセキュリティ監視のSOCのオンサイト/オフサイトのそれぞれに対して同時にインターネットVPN接続できること。

（エ）インターネットVPN接続は常時接続可能であること。

（オ）アラート検知ログを送付する際の送信元のIPアドレスはIPv4形式であること。

（カ）IPv4の固定グローバルアドレスを1個以上提供すること。

（キ）インターネットVPN接続はIPsec(RFC既定のIPsecプロトコル(500/UDP、4500/UDP))であり、NATトラバーサル対応であること。

⑩　機密性3情報持出用回線

（ア）双方向1Gbps以上の回線をメインデータセンターに接続し、インターネット接続サービスを提供すること。なお、ベストエフォート型も可とする。

（イ）「1.1.4①インターネットからのリモートアクセス」に接続すること。

⑪　クラウドサービス専用接続回線

（ア）メインデータセンターと「11.9 パブリッククラウド要件」との間に専用回線による閉域網を用意すること。

（イ）双方向100Mbps以上の通信帯域を用意すること。

（ウ）アクティブ系に障害が発生した場合、自動でスタンバイ系に切り替わり、アクティブ系が復旧した際も同様に自動で切り替わること。

（エ）メインデータセンターから「11.9 パブリッククラウド要件」への通信が「250GB/月」程度、「11.9 パブリッククラウド要件」からメインデータセンターへの通信が「4.5TB/月」程度と想定している。

⑫　データ通信機器

（ア）LTE方式（4G相当以上）の通信方式であること。

（イ）40台用意すること。

（ウ）無制限に高速データ通信が可能なプラン、もしくは、高速データ通信で利用可能データ量は15GB以上とし、それを超えて通信制限がかかった際でも最大通信速度が1Mbpsで通信が継続となる契約プランを選択すること。も

しくは、総利用可能データ量600GB以上、それを超えて通信制限がかかった際でも最大通信速度が256Kbpsで通信が継続となるプランを選択すること。

（エ）USB及びIEEE802.11gで接続できること。

11.8 ホームページ基盤要件

11.8.1 クラウド要件

① IaaS（パブリック・クラウド）を利用するクラウド型にて構築すること。

② 利用するIaaSについて、ISMAPを取得していること。または既に申請済みであること。

③ 利用するIaaSについて、データセンターが国内に設置されていること。

④ 利用するIaaSについて、準拠法・裁判管轄を国内に指定できること。

⑤ ファイアウォール機能を有すること。対象は、外部との境界及び内部のネットワーク間とする。

⑥ アプリケーションファイアウォール（WAF）機能を有すること。保護対象は、統計センターホームページサーバ及び統計センターホームページ検証用サーバとすること。また、統計センターホームページサーバと統計センターホームページ検証用サーバで異なる設定ができること。

⑦ DDoS保護機能を有すること。

⑧ メール送信サービスを提供すること。スパムメールとして判定されないような対策がされていること。

⑨ 監視機能として、サーバインスタンスの状態、リソース（CPU、メモリー及びディスク）を監視すること。異常があった場合は、メール通知できること。

⑩ 各種ログを取得し不正接続及び侵入、情報資産の漏えい、改ざん、消去、破壊、不正利用等を防止するための対策を講じること。また、異常があった場合は、メール通知できること。なお、当該ログは、「1.2.3①統合ログ取得」、「1.2.3②ログ保管」にて、ログの収集・保管ができること。

⑪ バックアップ機能を有すること。対象は統計センターホームページサーバ、統計センターホームページ検証用サーバ、統計センターホームページ用データベース統計センターホームページ検証用データベースとする。バックアップ頻度は毎日とし、保存期間は７日とする。

⑫ 通信経路上の暗号化（SSL 暗号化通信）を行うこと。なお、サーバ証明書は統計センターが用意するため、費用の発生はないものとし、証明書発行要求（CSR）の作成及びサーバ証明書の登録作業を行うこと。

⑬ 格納データ（データベース含む）の暗号化を行うこと。なお、暗号化の対象等については、設計時に決定する。

⑭ 統計センターホームページサーバ、統計センターホームページ検証用サー

バは、IPv4及びIPv6でインターネットに公開できるようにすること。

⑮　統計センターホームページ検証用サーバにおいては、接続をグローバルIPアドレスで制限すること。

⑯　利用するIaaSの設定については、「1.3.10脆弱性検査ツール」のベンダーが提供するベストプラクティスに従っていることを確認すること。なお、従わない場合は理由を明確にすること。

⑰　「1.3.10脆弱性検査ツール」にて、統計センターホームページサーバ及び統計センターホームページ検証用サーバを検査すること。

⑱　インシデント発生時に統計センターホームページサーバのディスクドライブをフォレンジック調査できるように保全手順を整備すること。また、主管課がテストのためサンプルの提供を依頼した場合は対応すること。

⑲　IPS（侵入防御）を導入すること。また、異常があった場合は、メール通知できること。

11.8.2 サーバ要件

①　統計センターホームページサーバ

（ア）1インスタンス当たり、vCPUを2以上搭載すること。

（イ）1インスタンス当たり、メモリを4GB以上搭載すること。
1インスタンス当たり、データ保存領域を100GB以上搭載すること。

（ウ）2インスタンス以上で構成すること。アクティブ/アクティブの冗長構成であること。それぞれ、異なるアベイラビリティゾーンに配置すること。

（エ）不正プログラム対策を導入すること。また、異常があった場合は、メール通知できること。

（オ）改ざん検知を導入すること。また、異常があった場合は、メール通知できること。

（カ）Wordpressの動作に必要なOS及びミドルウェアをインストールすること。

（キ）ホームページコンテンツ事業者がコンテンツの登録を行えるようにすること。

②　統計センターホームページ検証用サーバ

（ア）1インスタンス当たり、vCPUを2以上搭載すること。

（イ）1インスタンス当たり、メモリを4GB以上搭載すること。

（ウ）1インスタンス当たり、データ保存領域を100GB以上搭載すること。

（エ）1インスタンス以上のサーバで構成すること。

（オ）不正プログラム対策を導入すること。また、異常があった場合は、メール通知できること。

（カ）改ざん検知を導入すること。また、異常があった場合は、メール通知できること。

（キ）Wordpressの動作に必要なOS及びミドルウェアをインストールすること。
（ク）ホームページコンテンツ事業者がコンテンツの登録を行えるようにすること。

③　統計センターホームページ用データベース
（ア）マネージド型サービスとして提供すること。
（イ）1インスタンス当たり、vCPUを4以上搭載すること。
（ウ）1インスタンス当たり、メモリを4GB以上搭載すること。
（エ）1インスタンス当たり、データ保存領域を50GB以上搭載すること。
（オ）2インスタンス以上で構成すること。アクティブ/スタンバイの冗長構成であること。障害発生時は自動フェイルオーバーすること。
（カ）それぞれ、異なるアベイラビリティゾーンに配置すること。
（キ）データベースエンジンとして、MariaDB、MySQL、PostgreSQLを選択できること。

④　統計センターホームページ検証用データベース
（ア）マネージド型サービスとして提供すること。
（イ）1インスタンス当たり、vCPUを2以上搭載すること。
（ウ）1インスタンス当たり、メモリを2GB以上搭載すること。
（エ）1インスタンス当たり、データ保存領域を50GB以上搭載すること。
（オ）1インスタンス以上で構成すること。
（カ）データベースエンジンとして、MariaDB、MySQL、PostgreSQLを選択できること。

11.9 パブリッククラウド要件

11.9.1 環境要件

令和６年８月から令和11年12月末までの間、「11.9.2 サーバ等要件」に掲げるサーバ等の稼働を予定しているため、パブリッククラウド環境を利用できるようにすること。なお、本サービスはMicrosoft Azureとする。

①　ISMAPを取得していること。または既に申請済みであること。
②　データセンターが国内に設置されていること。
③　準拠法・裁判管轄を国内に指定できること。
④　「11.2①(ク)(15)認証サーバ1」のユーザで認証できるようにすること。
⑤　利用するIaaSの設定については、「1.3.10 脆弱性検査ツール」のベンダーが提供するベストプラクティスに従っていることを確認すること。なお、従わない場合は理由を明確にすること。

11.9.2 サーバ等要件

令和６年８月から令和11年12月末までの間、パブリッククラウド環境において、以下に掲げるサーバ等の稼働を予定しているため、そのために必要なリソースを提供すること。

なお、ここに記載している構成は現時点の想定であり、同等の料金での構成変更が、運用中に柔軟に行えること。

仮想サーバの構築等は統計センター職員が行うが、基本的なネットワーク構築、メインデータセンターとの接続等については、請負者が行うこと。

① 仮想マシン

（ア）台数は4とする。

（イ）1台あたり、4vCPU、メモリ16GBとする（Standard_D4_v5)。

（ウ）1台あたり、SSD128GBとする（Standard SSD LRS)。

② 負荷分散機能

（ア）11.9.2①の仮想マシンへのWebアクセスを負荷分散できること。

③ 仮想マシン（GPU)

（ア）NVIDIA GPU A100 １つ

（イ）24vCPU、メモリ220GB、SSD1TBとする。

（ウ）１ヶ月あたり40時間稼働とする。

④ データベース（PaaS、ゾーン冗長)

（ア）データベース数は1とする。

（イ）異なるアベイラビリティゾーンでの冗長構成とする。

（ウ）8vCPU、メモリ40.8GB、ストレージ1TB、バックアップストレージ7.2TBとする。

（エ）Microsoft SQL Serverとする。

⑤ データベース（PaaS)

（ア）データベース数は1とする。

（イ）2vCPU、メモリ10.2GB、ストレージ260GBとする。

（ウ）Microsoft SQL Serverとする。

⑥ プライベートエンドポイント

（ア）プライベートエンドポイント数は2とする。

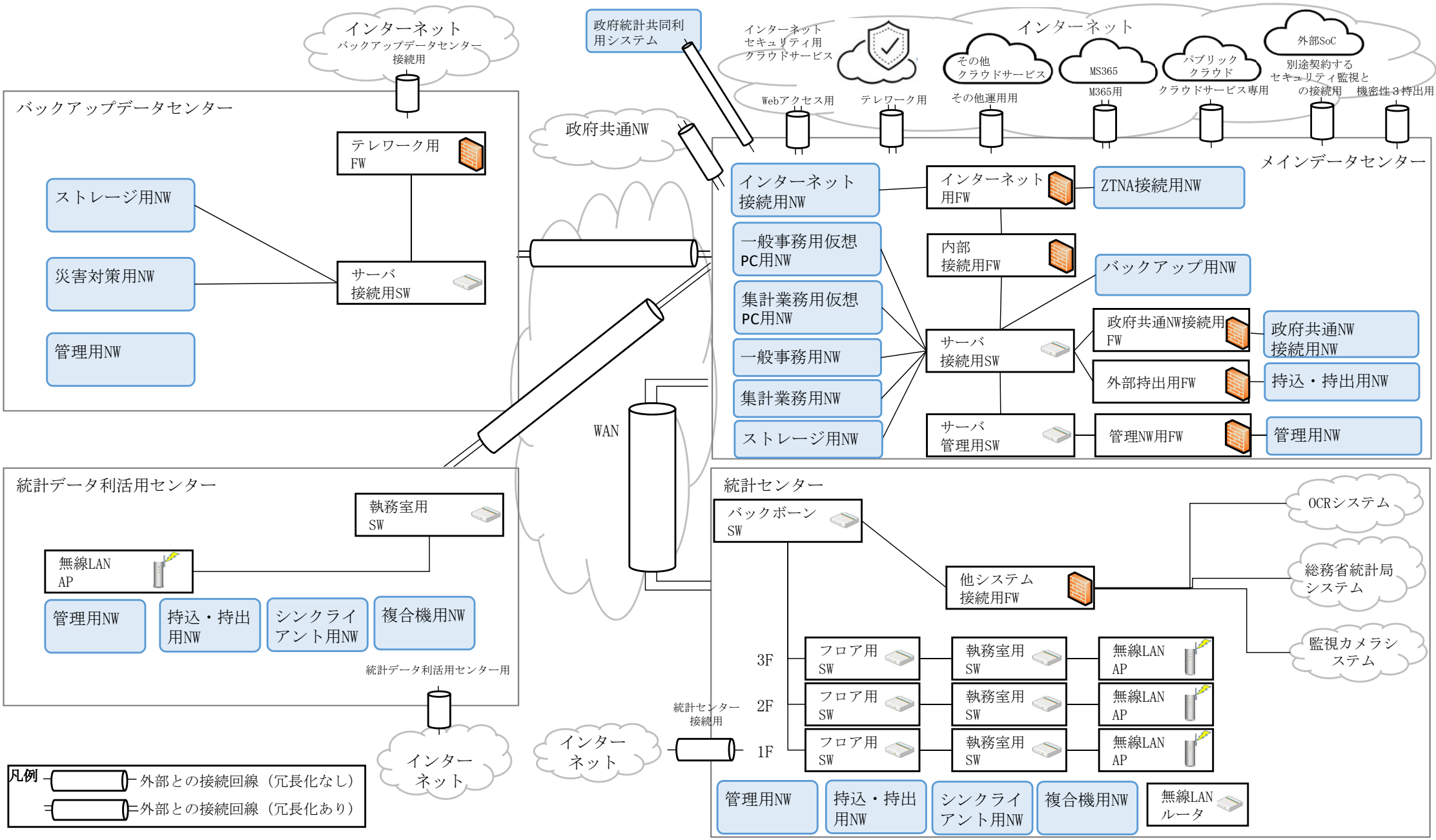
次期情報システム基盤におけるユーザ数一覧（想定）

別紙１

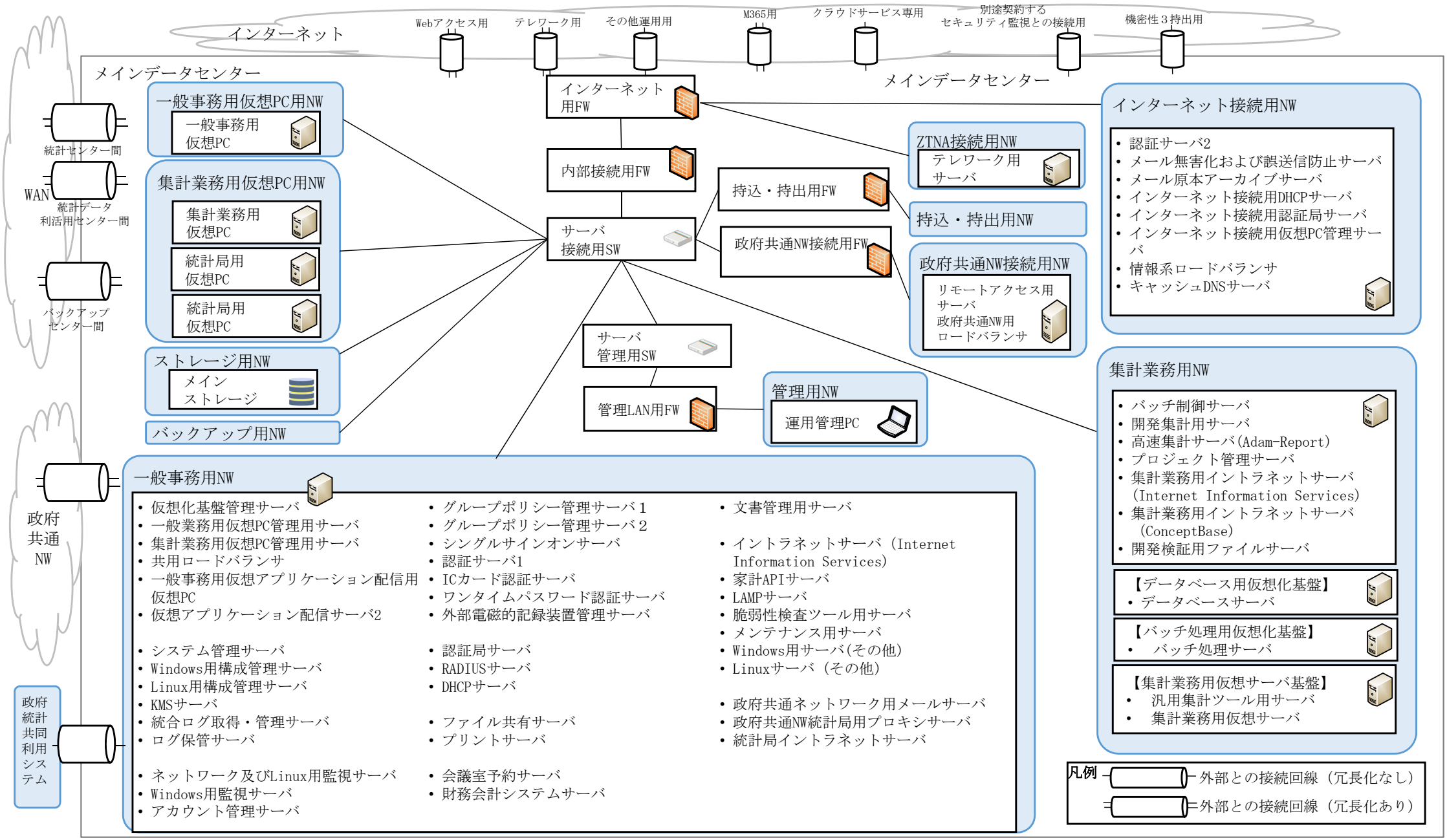
令和6年(2024年)											
1月	2月	3月	4月	5月	6月	7月	8月	9月	10月	11月	12月
-	-	-	1243	1243	1248	1248	1248	1248	1248	1375	1371
令和7年(2025年)											
1月	2月	3月	4月	5月	6月	7月	8月	9月	10月	11月	12月
1371	1371	1371	1354	1354	1358	1358	1358	1308	1308	1308	1360
令和8年(2026年)											
1月	2月	3月	4月	5月	6月	7月	8月	9月	10月	11月	12月
1450	1450	1450	1440	1385	1385	1385	1355	1355	1355	1375	1375
令和9年(2027年)											
1月	2月	3月	4月	5月	6月	7月	8月	9月	10月	11月	12月
1355	1355	1355	1355	1355	1355	1355	1355	1252	1251	1251	1252
令和10年(2028年)											
1月	2月	3月	4月	5月	6月	7月	8月	9月	10月	11月	12月
1249	1245	1245	1245	1245	1248	1248	1248	1248	1248	1259	1259
令和11年(2029年)											
1月	2月	3月	4月	5月	6月	7月	8月	9月	10月	11月	12月
1253	1243	1243	1243	1243	1248	1248	1248	1248	1248	1375	1371

別添2　次期情報システム基盤概要構成図

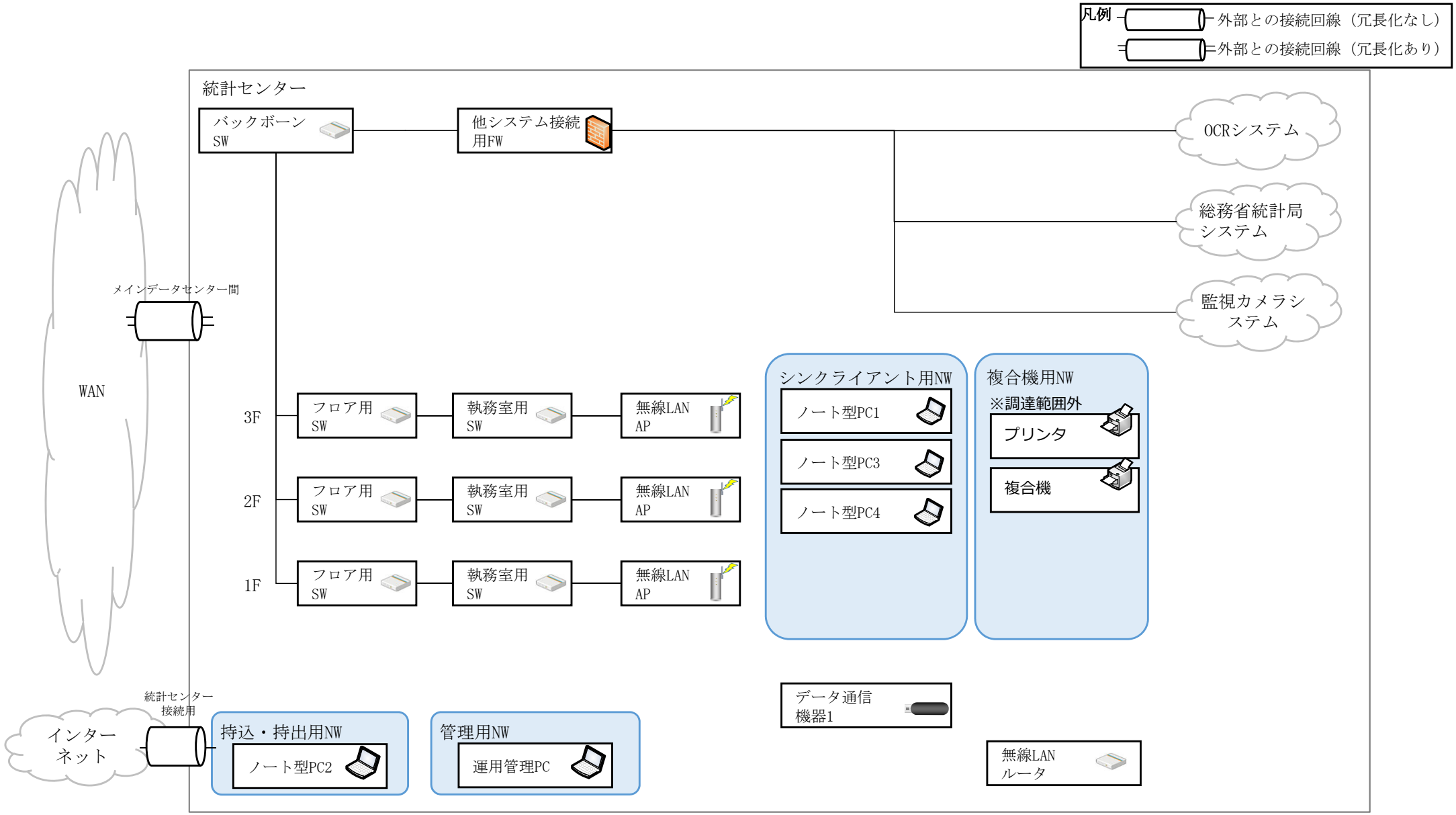
別添2-1　次期情報システム基盤概要構成図(全体)



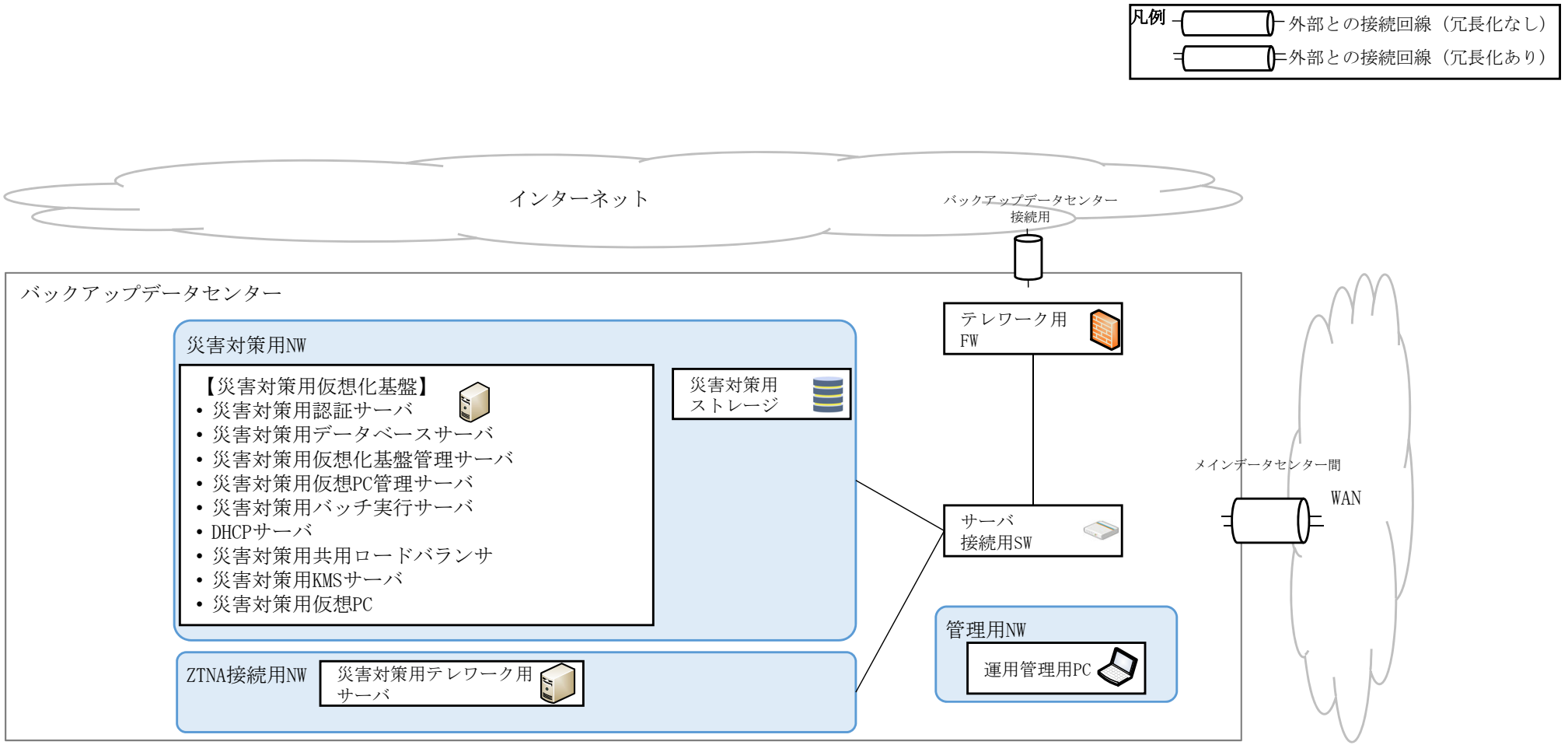
別添2-2　次期情報システム基盤概要構成図（メインデータセンター）



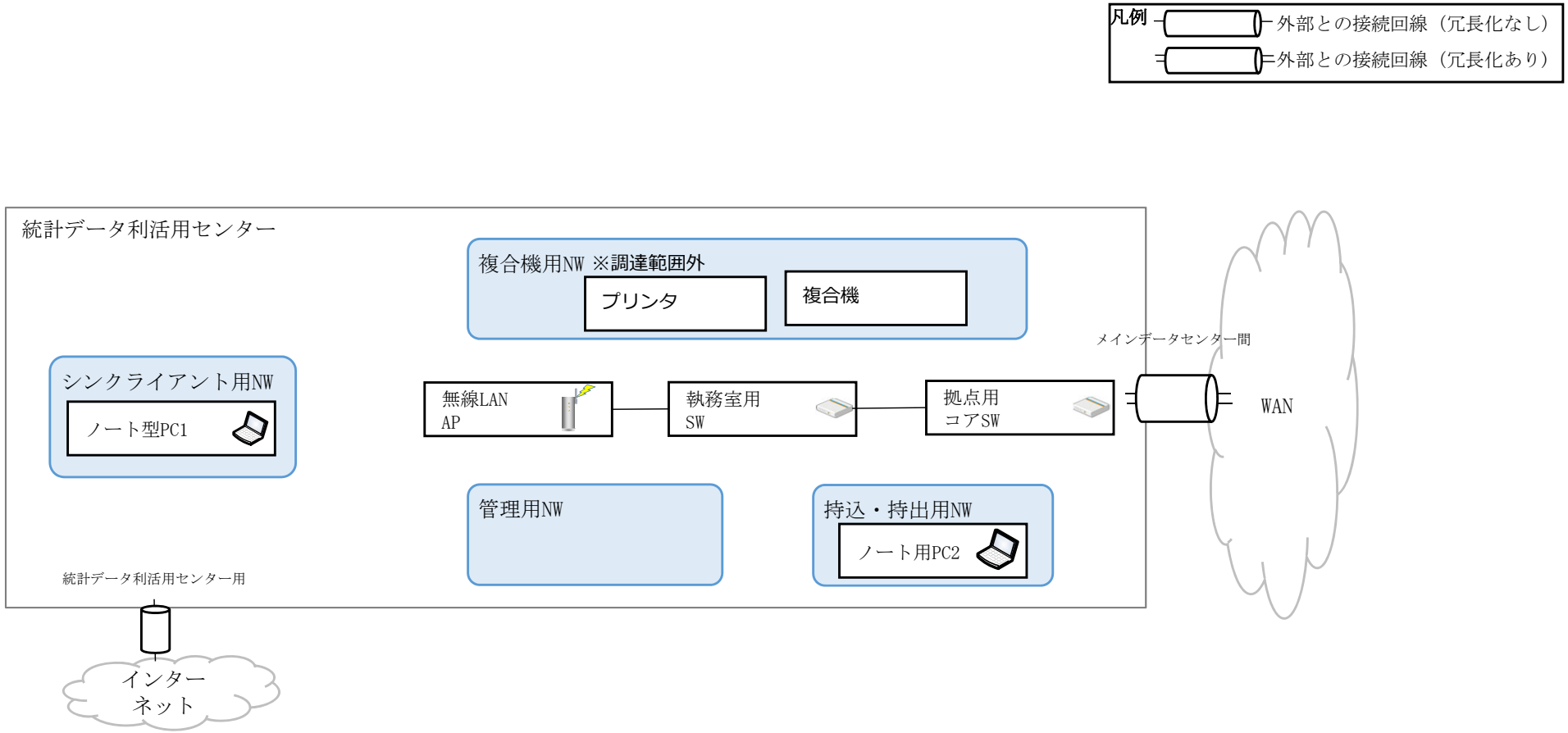
別添2-3　次期情報システム基盤概要構成図（統計センター）



別添2-4　次期情報システム基盤概要構成図（バックアップデータセンター）



別添2-5　次期情報システム基盤概要構成図（統計データ利活用センター）



移行対象一覧

別添３

【凡例】●：請負者が実施、▲：統計センターが実施、－：移行対象外

現行サーバ名	次期サーバ名 または サービス名 ※（）囲いはサービス	データ移行の要否	システム移行の要否	備考
内部メールサーバ	（Exchange Online）	●	●	
政府共通ネットワーク用メールサーバ	政府共通ネットワーク用メールサーバ	－	●	
内部アプリケーション用メールサーバ	－	－	－	政府共通ネットワーク用メールサーバに統合されるため、移行対象外とする。
政府共通ネットワーク用メールゲートウェイサーバ	※実現方法は提案に委ねる	－	●	
仮想PC管理用サーバ	一般事務用仮想PC管理サーバ	－	－	
	集計業務用仮想PC管理サーバ	－	－	
仮想PC接続管理用サーバ	※実現方法は提案に委ねる	－	－	
仮想PC接続管理用負荷分散サーバ	※実現方法は提案に委ねる	－	－	
仮想PC管理用データベースサーバ	※実現方法は提案に委ねる	－	－	
仮想アプリケーション配信サーバ1	一般事務用仮想アプリケーション配信用仮想PC	－	－	
仮想アプリケーション配信サーバ2	仮想アプリケーション配信サーバ2	－	－	
仮想アプリケーション配信サーバ3	－	－	－	廃止のため、移行対象外とする。
在席管理サーバ	（Teams）	－	－	
会議室予約サーバ	会議室予約サーバ	●	●	
構成管理サーバ	Windows用構成管理サーバ	－	－	
	Linux用構成管理サーバ	－	－	
統合ログ取得・管理サーバ	統合ログ取得・管理サーバ	●	●	アプリケーションやセキュリティログを取得・保管
	ログ保管サーバ	●	●	syslog系のログを保管
監視サーバ1	ネットワーク及びLinux用監視サーバ	－	－	
監視サーバ2	Windows用監視サーバ	－	－	
仮想化基盤管理サーバ	仮想化基盤管理サーバ	－	－	
特権ID管理サーバ	－	－	－	特権ID管理は管理方法から変更するので、移行対象外とする。
	（特権ID不正利用検知）	－	－	特権ID不正利用検知の実現方法は、提案による。
特権ID管理データベースサーバ	－	－	－	特権ID管理は管理方法から変更するので、移行対象外とする。
アカウント管理サーバ	アカウント管理サーバ	－	－	
シングルサインオンサーバ1	シングルサインオンサーバ	－	－	
DHCPサーバ	DHCPサーバ	－	－	
認証局サーバ	認証局サーバ	－	－	
設計書管理サーバ	（SharePoint Online）	●	●	
プリントサーバ	プリントサーバ	－	－	
サービスデスク管理サーバ	（申請のオンライン受付及び 各種運用手続きのワークフロー管理）	－	－	
認証サーバ1	認証サーバ1	●	●	オンプレADへの移行を実施する。
	（Entra ID）	●	●	クラウドにもID等は移行を実施する。
ICカード認証サーバ	ICカード認証サーバ	－	－	
ワンタイムパスワード認証サーバ	ワンタイムパスワード認証サーバ	－	－	
イントラネットサーバ（Internet Information Services）#1	イントラネットサーバ（Internet Information Services）	▲	▲	福利厚生システムを導入のため、センター側にて移行実施する。
イントラネットサーバ（SharePoint Server）#2	（SharePoint Online）	●	●	
イントラネットサーバ（バックエンドデータベース）#3	データベースサーバ	▲	▲	福利厚生システムを導入のため、センター側にて移行実施する。
プロキシサーバ	政府共通NW統計局用プロキシサーバ	－	－	
財務会計システムサーバ	財務会計システムサーバ	▲	▲	センター側にて移行実施する。
管理業務Webサーバ	－	－	－	別サービスを利用するため、移行対象外とする。
バッチ制御サーバ	バッチ制御サーバ	－	●	
高速集計サーバ（Adam-Report）	高速集計サーバ（Adam-Report）	●	●	
集計業務用イントラネットサーバ（Internet Information Services）	集計業務用イントラネットサーバ（Internet Information Services）	●	●	
集計業務用イントラネットサーバ（ConceptBase）	集計業務用イントラネットサーバ（ConceptBase）	▲	▲	センター側にて移行実施する。
バッチ作成サーバ	※仮想PCサーバに統合して記載	－	－	
プロジェクト管理サーバ	プロジェクト管理サーバ	●	●	センターが作成する手順書に基づき、請負者が移行実施する。
開発検証用ファイルサーバ	開発検証用ファイルサーバ	▲	▲	センター側にて移行実施する。
検証用サーバ	検証用サーバ	－	－	
不正プロセス検知用サーバ	（不正プロセス検知）	－	－	実現方法は提案による
バックアップサーバ（SharePoint）	（SharePoint Online）	－	－	バックアップは不要になる。
仮想パッチ配信サーバ	－	－	－	Linuxサーバのエンドポイントセキュリティ確保の方法は、提案による。
RADIUSサーバ	RADIUSサーバ	－	－	
システム管理サーバ	システム管理サーバ	－	－	物理サーバのメンテナンスや管理の方法は、提案による。
Excel集計サーバ	－	－	－	ターミナルサーバは廃止するため、移行対象外とする。
外部持ち出し用ネットワーク及びインターネット接続用ファイル無害化サーバ	－	－	－	ファイル転送及び無害化の方法は、提案による。
政府共通ネットワーク用ファイル転送サーバ	－	－	－	ファイル転送の実現方法は提案による。
外部電磁的記録装置管理サーバ	外部電磁的記録装置管理サーバ	－	－	
リモートアクセス用仮想PC接続管理用サーバ	－	－	－	
リモートアクセス用仮想PC接続管理用負荷分散サーバ	－	－	－	
リモートアクセス用ターミナルサーバ	－	－	－	ターミナルサーバは廃止するため、移行対象外とする。
文書管理用サーバ	文書管理用サーバ	▲	▲	
開発集計用サーバ	開発集計用サーバ	－	－	
KMSサーバ	KMSサーバ	－	－	
統計局等イントラネットサーバ	統計局イントラネットサーバ	●	●	

移行対象一覧

別添３

【凡例】●：請負者が実施、▲：統計センターが実施、－：移行対象外

現行サーバ名	次期サーバ名 または サービス名 ※ () 囲いはサービス	データ移行の要否	システム移行の要否	備考
アプリケーション公開サーバ	※仮想PCサーバに統合して記載	－	－	
統計局等データベースサーバ	－			次期システムでは廃止するため、移行対象外とする。
共用系ロードバランサ	共用ロードバランサ	－	－	
	政府共通NW用ロードバランサ	－	－	現行ではリモートアクセス用機器が同等機能を提供。
グループポリシー管理サーバ	グループポリシー管理サーバ１	－	－	
	グループポリシー管理サーバ２	－	－	
メンテナンス用サーバ	メンテナンス用サーバ	－	－	
バッチ処理サーバ	バッチ処理サーバ	－	－	
データベースサーバ	データベースサーバ	●	●	
インターネット接続用サーバ	※仮想PCサーバに統合して記載	－	－	
認証サーバ2	認証サーバ2	－	－	
シングルサインオンサーバ2	－	－	－	廃止のため移行対象外とする。
外部メールサーバ	メール無害化及び誤送信防止サーバ	－	－	
	メール原本アーカイブサーバ	－	－	
メール無害化サーバ	メール無害化及び誤送信防止サーバ	－	－	
インターネット接続用DHCPサーバ	インターネット接続用DHCPサーバ	－	－	
インターネット接続用認証局サーバ	インターネット接続用認証局サーバ	－	－	
インターネット接続用仮想化基盤管理サーバ	仮想化基盤管理サーバ	－	－	
インターネット接続用仮想PC管理用サーバ	インターネット接続用仮想PC管理サーバ	－	－	
インターネット接続用仮想PC接続管理用サーバ	※実現方法は提案に委ねる	－	－	
インターネット接続用仮想PC接続管理用負荷分散サーバ	※実現方法は提案に委ねる	－	－	
インターネット接続用仮想PC管理用データベースサーバ	※実現方法は提案に委ねる	－	－	
情報系ロードバランサ	情報系ロードバランサ	－	－	
バックアップサーバ	－	●	●	バックアップの実現方法は、提案による。
仮想PCサーバ	仮想PC（VDI）用仮想化基盤	－	－	
	インターネット接続用仮想PC（RDSH）	－	－	
	統計局用仮想PC（RDSH）	－	－	
	集計業務用仮想PC（RDSH）	－	－	
	バッチ作成用仮想PC（RDSH）	－	－	
管理業務データベースサーバ	－	－	－	別サービスを利用するため、移行対象外とする。
Webサーバ	－	－	－	
リバースプロキシサーバ	－	－	－	廃止予定のため、移行対象外とする。
コンテンツDNSサーバ	(クラウド事業者又は回線事業者が提供するDNSを利用する)	－	●	
	(クラウド事業者又は回線事業者が提供するDNSを利用する)	－	●	
キャッシュDNSサーバ	キャッシュDNSサーバ	－	－	
インターネット向けファイル転送サーバ	（SharePoint Online）	－	－	
サーバ接続用スイッチ	サーバ接続用スイッチ	－	－	
サーバ管理用スイッチ	サーバ管理用スイッチ	－	－	
インターネット公開用ファイアウォール	インターネット用ファイアウォール	－	－	
インターネット接続用ファイアウォール	内部ネットワーク用ファイアウォール	－	－	
管理LAN用ファイアウォール	管理LAN用ファイアウォール	－	－	
ミラーポートタップ	－	－	－	廃止予定のため、移行対象外とする。
テレワーク用機器	テレワーク用サーバ	－	－	
リモートアクセス用機器	リモートアクセス用サーバ	－	－	政府共通NW用リバースプロキシ機能を兼ねているが、要件としては分離する。
メールセキュリティ対策機器	（メールセキュリティ対策）	－	－	実現方法は提案による
Web閲覧セキュリティ対策機器	（セキュアWebゲートウェイ(SWG)）	－	－	Web閲覧セキュリティ対策の実現方法は、提案による
通信パケット記録装置	－	－	－	廃止予定のため、移行対象外とする。
現行情報システム基盤のファイルサーバ	ファイル共有サーバ	●	●	課室用ファイルサーバ、集計業務用ファイルサーバ及び統計業務基盤システムのファイルサーバの情報を移行する。
脆弱性検査ツール	脆弱性検査ツール用サーバ	－	－	
CASB	（クラウドアクセスセキュリティ（CASB））	－	●	
家計APIサーバ	家計APIサーバ	▲	▲	
その他	LAMPサーバ	▲	▲	
	Windowsサーバ（その他）	▲	▲	
	Linuxサーバ（その他）	▲	▲	
ホームページ基盤	統計センターホームページサーバ	－	－	
	統計センターホームページ用データベース	－	－	
	統計センターホームページ検証用サーバ	－	－	
	統計センターホームページ検証用データベース	－	－	
集計業務用仮想サーバ基盤	汎用集計ツール用サーバ	－	－	
	集計業務用仮想サーバ	－	－	

運用管理業務一覧

別添4

No	目次 Lv1	Lv2	Lv3	Lv4	目的・定義	作業項目	作業内容	実施頻度	提出物
1	業務内容								
2		1. 定期報告及び会議							
3			1.1 定期報告						
4				–					
5					定期的（日次、週次、月次及び年次）に稼動状況の監視結果、サービスデスク対応の件数及び内容及びその他運用管理業務の実施状況を主管課へ報告する。また、週次報告、月次報告及び年次報告は会議を開催し、週次報告では課題解決状況、作業の進行に影響を及ぼす課題、問題及びリスク等を報告に含め、月次報告では週次報告の内容に加えて、SLAの遵守状況、KPI測定結果を報告に含める。なお、詳細な報告内容と様式については、主管課と協議し決定する。	日次報告	以下の項目について内容を取りまとめ、主管係に提出すること。 (1)提出物項目に「日次報告書」と記載されているもの。 ・バックアップ取得 ・定義ファイルの確認 ・更新モジュールの確認 ・ソフトウェアインベントリ収集 ・死活監視 ・性能監視 ・データベース性能監視 ・ポート監視 ・セキュリティ監視 ・目視点検 ・応対履歴情報の管理 (2)保守作業報告書 (3)障害報告書 (4)人事異動報告書 (5)不正プログラム検出報告書	1回/日	日次報告書
6						週次報告	以下の項目について内容を取りまとめ、主管係に提出し報告会を実施すること。 また、その週に発生した障害などトピックとなる事項についても記載し、対策等も含め詳細に説明すること。 (1)提出物項目に「週次報告書」と記載されているもの ・各種申請書対応 ・偽サイト調査 ・ウィルス検知件数 ・ユーザからの不審メール報告件数 ・内閣サイバーセキュリティセンター関連作業（不審メール情報対応件数） (2)日次報告書で取りまとめた項目を集約した内容 (3)変更要求承認申請書 (4)受け入れ試験結果承認申請書 (5)セキュリティ対策計画書	1回/週	週次報告書
7						月次報告	以下の項目について内容を取りまとめ、主管係に提出し報告会を実施すること。 また、月間を通した傾向、前月比などについても記載し報告すること。 (1)提出物項目に「月次報告書」と記載されているもの ・サービスレベルの報告 ・ディスク領域最適化 ・クォータ管理 ・セキュリティ監視月次レポートの確認 ・通信回線装置のソフトウェアの管理 ・目標及びKPIの設定 ・サイトアクセス数の解析 ・不正アクセス及び特徴的な通信の集計 ・クローラーデータの更新 ・不正プログラムチェックの確認 ・ログ監視 (2)週次報告書で取りまとめた項目を集約した内容	1回/月	月次報告書
8						年次報告	以下の項目について内容を取りまとめ、主管係に提出し報告会を実施すること。 また、年間を通した傾向・所感などについても記載し報告すること。 (1)提出物項目に「年次報告書」と記載されているもの ・切替訓練 ・ユーザIDの点検 ・目標及びKPIの見直し ・手順書の確認 (2)月次報告書で取りまとめた項目を集約した内容	1回/年	年次報告書

運用管理業務一覧

別添4

No	目次 Lv1	Lv2	Lv3	Lv4	目的・定義	作業項目	作業内容	実施頻度	提出物
9			1.2 会議						
10				-					
11					主管課への報告及び主管課との協議を会議によって行う。	定例会議	定期報告のうち、週次、月次及び年次の報告に関して会議を行うこと。会議を開催した場合は、3営業日以内に議事録を作成及び提出し、主管課の承認を得ること。	1回/週 1回/月 1回/年	会議議事録
12						適宜実施する会議	(ア)「10.1.1 定期報告」に限らず作業の進捗状況等により必要に応じて会議を開催すること。 (イ) 開催する会議で協議または報告する事項については、全て資料を作成し論理的且つ効率的に行うこと。 (ウ) その他必要な会議については、主管課と協議の上、設置すること。 (エ) 会議を開催した場合は、3営業日以内に議事録を作成及び提出し、主管課の承認を得ること。	適宜	会議議事録
13		2. 運用計画書及び運用設計書の修正							
14			-						
15				-					
16					「運用計画書」及び「運用設計書」を修正し、運用業務を実施可能とする。	「運用計画書」及び「運用設計書」の修正	移行期間中に設計時点から構築時の変更点等にもとづき、必要に応じて「運用計画書」及び「運用設計書」の修正及び追加を行い、主管課の承認を得ること。	-	運用計画書 運用設計書
17		3. 運用実施要領の作成							
18			-						
19				-					
20					次期情報システム基盤の運用実施業務に必要な事項を定める。	「運用実施要領」の作成	運用に係る管理要領として「運用実施要領」を作成し、主管課の承認を得ること。 「運用実施要領」は、「「標準ガイドライン解説書-第3編第9章　運用及び保守　1.運用開始前の準備　3）運用実施要領の作成と確定」に従い、少なくとも以下の項目を記載すること。 (ア) コミュニケーション管理 (イ) 体制管理 (ウ) 作業管理 (エ) リスク管理 (オ) 課題管理 (カ) システム構成管理 (キ) 変更管理 (ク) 情報セキュリティ対策	-	運用実施要領

運用管理業務一覧

別添4

No	目次 Lv1	Lv2	Lv3	Lv4	目的・定義	作業項目	作業内容	実施頻度	提出物
21	4. サービスデザイン								
22		4.1 サービスレベル管理							
23			① SLAの締結						
24					本業務におけるサービスレベルを主管課と合意し、サービスレベルの測定及び報告を実施する。	「SLA合意書」の作成	「別添5　運用におけるサービスレベル目標」に基づき主管課と協議の上、SLAを締結し、「SLA合意書」を作成すること。	-	SLA合意書
25						サービスレベルの測定	サービスレベルは、運用開始後から測定すること。ただし、運用開始後1ヶ月間の評価は、主管課と調整すること。	適宜	-
26						サービスレベルの報告	サービスレベルで定めた項目、目標値に対する実績及び達成状況を月次及び年次で主管課に報告し、分析、評価及び改善を行う。	1回/月 1回/年	月次報告書 年次報告書
27						サービスレベルの目標設定	サービスレベル目標（稼働率及び復旧時間等）については、「別添5　運用におけるサービスレベル目標」を参照すること。	-	-
28						サービスレベルの範囲設定	天変地異等、通常の予測を超えた事態が発生した場合は、サービスレベルの範囲外とする。	-	-
29			② SLAの改定						
30					必要に応じてサービスレベルを改定する。	SLAの改定	設定した管理項目、管理指標値、保証値等については、必要に応じて見直しを実施し改定するものとする。なお、改定の契機は以下のとおりとする。 (1) 統計センター及び請負者双方の合意事項に明確な変更が生じた場合 (2) 統計センター及び請負者双方が必要と認めた場合	適宜	-
31			③ SLAに係る免責事項						
32					サービスレベルの適用外となる事項を定める。	サービスレベルの免責	以下の場合は、SLAの適用外とする。 (1) 災害により電源供給が停止した場合 (2) 請負者の瑕疵によらず電源供給が停止した場合 (3) 統計センター及び他の調達事業者の過失または故意による障害の場合 (4) 統計センター及び他の調達事業者の過失または故意により障害復旧が行えない場合 (5) 請負者の瑕疵によらず障害監視が行えない場合 (6) 請負者の瑕疵によらず障害通知の受信ができない場合 (7) 統計センター及び請負者双方の協議の上で計測の除外とした場合	-	-
33			④ SLAに係る是正措置						
34					未達のサービスレベルについて、達成度合いの向上を図る。	サービスレベル未達成項目の改善	「サービスレベルの報告」において、未達成項目がある場合、請負者は以下に示すような措置により達成度合いの向上に努めること。 (1) 未達成の項目に対する改善策(操作手順書の改訂、要員の配備、仕組み及び手続きの見直し、検証試験の実施、機器等の導入・交換等)を提示し、統計センターの承認を得た上で対策を講じること。また、そのために必要となる作業等は請負者の負担で行うこと。 (2) 改善策の実施効果を実施の月より3ヶ月間、1ヶ月ごとの達成状況報告とともに報告し、統計センターの承認を得ること。	適宜	-

運用管理業務一覧

別添4

No	目次 Lv1	Lv2	Lv3	Lv4	目的・定義	作業項目	作業内容	実施頻度	提出物
35			4.2 キャパシティ管理						
36				① システム性能管理					
37					システム性能の改善を図るため、チューニングや改善提案を行う。仮想サーバへの割当済みリソースの変更が必要となった場合には、速やかに対応を行い、システムの安定的なサービス提供を継続する。	チューニング	システムの性能低下が認められる場合またはシステムの設定変更により性能改善が見込まれる場合は、システム設定の変更、仮想サーバの割当済みリソースの変更等のチューニングを行い、性能の改善を図ること。なお、チューニング作業は、変更管理及びリリース管理として管理すること。	適宜	保守作業計画・報告書
38						改善提案	次期情報システム基盤における既存のリソースで対応が困難であると想定される場合は、改善のための提案を行うこと。	適宜	性能改善提案書
39						仮想サーバの計画的リソース変更	繁忙期等でリソースの変更が必要なことが想定される場合は、あらかじめリソース変更を行うこと。なお、リソース変更は、変更管理及びリリース管理として管理すること。	適宜	保守作業計画・報告書 変更要求承認申請書
40				② ディスク管理					
41					サーバのローカルディスク及び共有ストレージのフォルダ別にディスク使用状況を管理し、不要なテンポラリファイルの増加や利用者の使用量の抑制を図る。	ディスク領域最適化	サーバのローカルディスクの容量が不足するおそれがある場合は、テンポラリファイル等の不要なファイルを削除し、ディスク領域の最適化を行うこと。なお、サーバのローカルディスクの使用状況については、定期的(1回/月)に主管課に報告すること。	適宜 1回/月	月次報告書
42						クォータ管理	共有ストレージの各フォルダについて保存容量の上限を設定すること。なお、各フォルダの使用状況については、定期的(1回/月)に主管課に報告すること。	適宜 1回/月	月次報告書
43			4.3 可用性管理						
44				① システム設定変更					
45					システムを安定して稼動させるため、システム設定の変更を行う。	システム設定変更	設定を変更することにより次期情報システム基盤の安定性について改善が見込まれる場合は、設定の変更を行うこと。なお、システム設定変更は、変更管理及びリリース管理として管理すること。	適宜	保守作業計画・報告書 変更要求承認申請書
46				② ソフトウェアのアップデート及び修正プログラムの適用					
47					システムを安定して稼動させるため、OS等の不具合又は脆弱性の修正に対応したパッチの適用を行う。	ソフトウェアのアップデート及び修正プログラムの適用	OS及びミドルウェア等の不具合等を修正するため、バージョンアップまたは修正プログラムの適用が必要となった場合、当該作業を行うこと。なお、これらの作業は、変更管理及びリリース管理として管理すること。	適宜	保守作業計画・報告書 変更要求承認申請書
48				③ バックアップ及びリストア					
49					データ損失防止及び迅速なシステム復旧のため、サーバや共有ストレージのバックアップ・リストア作業を行う。	バックアップ取得	サーバ及びメインストレージのバックアップを定期的に行うこと。なお、バックアップ結果については、定期的(1回/日)に確認し、主管課に報告すること。また、バックアップが失敗していた場合は、速やかに再バックアップを行う等、確実にバックアップが行われるよう管理すること。	1回/日	日次報告書
50						バックアップ対象の管理	サーバの増減等に合わせて、バックアップ対象を適切に管理すること。	適宜	-
52						リストア	バックアップデータからメインストレージの指定した領域にリストアすること。	適宜	保守作業計画・報告書
53				④ 計画停止に伴う作業					
54					次期情報システム基盤を計画停止するために必要な作業を行う。	計画停止に伴う作業	法定点検等による次期情報システム基盤の計画停止時に、必要な作業を行うこと。	適宜	保守作業計画・報告書

運用管理業務一覧

別添4

No	目次 Lv1	Lv2	Lv3	Lv4	目的・定義	作業項目	作業内容	実施頻度	提出物
55			4.4 情報セキュリティ管理						
56				① 証跡管理及び分析					
57					次期情報システム基盤において、出力される各種ログを保存し、調査が必要となった場合に確実に参照することができるように管理する。 また、出力される各種ログを分析し、インシデントにつながる不正プロセスを監視し、不正プロセス及び情報漏えい等のインシデントを検知した場合に各種対応を実施する。	ログの保存	次期情報システム基盤において統合ログ取得・管理サーバで取得したログについて、最低1年間保存すること。なお、必要に応じてログを一時的に退避する等、ログの取得が継続できるように対処すること。	常時	–
58						ログの分析	取得したログについて、分析を行い、情報漏えい等のインシデントに繋がる不正プロセスを監視すること。また、必要に応じてユーザへのヒアリング、ドメイン、IPアドレスの調査等を行うこと。	常時	保守作業計画・報告書 月次報告書
59						インシデント対応	不正プロセス及び情報漏えい等のインシデントを検知した場合、即時に主管課に報告した上で感染した端末をネットワークから切り離す等の適切な対応を行うこと。	適宜	保守作業計画・報告書
60						インシデント調査	不正プロセス及び情報漏えい等のインシデントを検知した場合、影響範囲の調査を行い、調査結果を主管課に報告すること。	適宜	保守作業計画・報告書
61						インシデント原因追及及び再発防止策検討	不正プロセス及び情報漏えい等のインシデントの原因を追究し、再発防止策の検討を支援すること。	適宜	–
62						過検知への対応	ログの分析の過程で過検知と思われる事象が発生した場合は、検知ルールの変更等の対応を行うこと。	適宜	保守作業計画・報告書 月次報告書
63						要員の配置	証跡管理及び分析作業に必要なスキルを有する要員を配置すること。	–	–
64				② 脆弱性対策					
65					システム基盤を構成している各種機器やサービス等に関するセキュリティ関連情報を収集し、対策が必要な場合は、システム設定の変更や修正プログラムの適用等の対策を行う。	セキュリティ情報の収集・分析	次期情報システム基盤を構成している各種機器やサービス等に関するセキュリティ関連情報を確認すること。なお、該当する事象等がある場合は、以下の内容を取りまとめた「セキュリティ対策計画」を作成し、主管課に報告すること。なお、詳細な実施内容は主管課と協議すること。 (1) 緊急度 (2) 対策の必要性 (3) 対策方法。この際、効率的に脆弱性対策を実施する手法を予め決定すること (4) 対策方法が存在しないゼロデイと呼ばれる状態の場合又は対策が完了するまでの期間に対する一時的な回避方法 (5) 対策方法又は回避方法が次期情報システム基盤に与える影響 (6) 対策の実施予定時期 (7) 対策試験の必要性 (8) 対策試験の方法 (9) 対策試験の実施予定時期 また、確認する情報は以下のものを想定しているが、具体的な内容は、主管課と協議の上、決定すること。 (1) ソフトウェア製造業者のサイトに掲載されている情報 (2) 公的機関が提供する情報	1回/日	セキュリティ対策計画書
66						対策の実施	「セキュリティ対策計画」について主管課の承認が得られた場合は、当該計画に基づき、セキュリティ関連のチューニング等を含むシステム設定の変更、バージョンアップ及び修正プログラムの適用等を行うこと。なお、これらの作業は、変更管理及びリリース管理として管理すること。	適宜	–
67						脆弱性スキャンソフトウェアを利用した脆弱性の確認	脆弱性スキャンソフトウェアの定義ファイルが最新のものに自動更新されているか確認すること。脆弱性スキャンを毎日に実施し、実行結果を確認すること。	1回/日	日次報告書
68				③ 不正プログラム対策					
69					不正プログラム等の情報収集を行うとともに、不正プログラム対策ソフトウェア等を最新の状態に維持するなどの対策を行う。 不正プログラムが発見された場合は、障害・問題管理として対応し、侵入ルートの 特定等、原因を究明するとともに、再発防止を図る。	定義ファイルの確認	各機器の定義ファイルが最新のものに自動更新されているか確認すること。更新されていない機器については再更新を行い、最新の状態を維持すること。	1回/日	日次報告書
70						更新モジュールの確認	各機器の定義モジュールが最新のものに自動更新されているか確認すること。更新されていない機器については再更新を行い、最新の状態を維持すること。	1回/日	日次報告書
71						フィルタ設定変更	不審メール及び不正プログラム等を検知した場合、URLフィルタ、スパムメールフィルタ等の設定変更、ブラックリストへのアドレス登録等を行うこと。	常時	保守作業計画・報告書
72						不正プログラムチェックの確認	不正プログラムチェックを定期的に実施し、実行結果を確認すること。	1回/月	月次報告書
73						不正プログラム発見時の対応	不正プログラムが発見された場合は、駆除の有無、感染状況、感染ルート等の確認を行い、インシデント管理及び問題管理として管理すること。	適宜	保守作業計画・報告書

運用管理業務一覧

別添4

No	目次 Lv1	Lv2	Lv3	Lv4	目的・定義	作業項目	作業内容	実施頻度	提出物
74				④ 不正侵入管理					
75					次期情報システム基盤においては、リモート監視サイト（外部委託業者）等により365日24時間対応でセキュアWebゲートウェイ、不正プロセス監視等を監視し、不正侵入検知・防御及び外部からの不正アクセス防御を行っている。 リモート監視サイトからの報告を受理するとともに、必要に応じて監視センターと協力し、調査・分析を行う。	調査・分析・対策	リモート監視サイトより、不正侵入またはその疑いがある等の報告を受理した場合は、リモート監視サイトと協力して調査及び分析を行うこと。なお、セキュリティインシデントであると認められる場合は、インシデント管理として管理し、防御策を講じること。	適宜	－
76						セキュリティ監視月次レポートの確認	リモート監視サイトから送付される「セキュリティ監視月次レポート」を確認し、内容に応じて詳細に分析を行うこと。また、分析結果については主管課に報告し、改善すべき点がある場合は提案すること。	1回／月	月次報告書
77				⑤不審メールの分析					
78					ユーザからの不審メール報告について、報告を受理するとともに、必要に応じてフィルタ設定変更、検体解析依頼を行う。また、統計センターが受信したメールを監視し、必要に応じてスパムメールフィルタ等の設定変更を行うこと。なお、過検知が発生した場合も対応を行う。	調査・分析・対策	ユーザからの不審メール報告を受理した場合は、ユーザへのヒアリング、URLフィルタ、スパムメールフィルタ等の設定変更、ブラックリストへのアドレス登録、検体解析依頼等を行うこと。また、類似のメールが他のユーザが受信していないことを確認すること。	適宜	不審メールヒアリングシート 週次報告書
79						監視	統計センターが受信したメールのうち、不審メールと思われるメールの件名、送信元アドレス等を元にスパムメールフィルタ等の設定を行うこと。	常時	－
80						ブラックリストの登録	内閣サイバーセキュリティセンター等から提供されるブラックリストをスパムメールフィルタ等に登録を行うこと。また、イントラネットに情報の掲載を行うこと。	適宜	週次報告書
81						過検知への対応	ユーザからのスパムメールフィルタ等の過検知報告を受理した場合は、内容の確認を行い、必要に応じてメール再送等を行うこと。	適宜	メール過検知対応シート
82				⑥ 不正サイト管理					
83					外部から提供される不正サイトの情報を活用し、不正サイトへの接続を遮断、検知等の対応を行う。また、不正サイトへの接続を検知した場合は調査・分析を行う。	調査・分析・対策	不正サイトへの接続を検知した場合は、ユーザへのヒアリング、URLフィルタ等の設定変更、検体解析依頼等を行うこと。	適宜	不正通信検知対応シート
84						ブラックリストの登録	外部から提供されるブラックリストをセキュアWebゲートウェイ及び統合ログ取得・管理サーバに登録を行うこと。	適宜	－
85			4.5 ITサービス継続性管理						
86				－					
87					メインデータセンターからバックアップデータセンターへの切替、バックアップデータセンターからメインデータセンターへの切戻しについて、事前に準備することで、実際に必要になった際に円滑に実施できるようにする。	切替訓練	「災害対策用機器利用手順書」に基づき、切替訓練を年1回以上実施すること。なお、切替訓練のうち、少なくとも1回はバックアップデータセンターに赴き実機を利用した訓練とすること。また、次期情報システム基盤の稼働開始前に、バックアップデータセンターに赴き実機を利用した切替訓練を1回以上実施すること。	1回／年	年次報告書
88						切替試験	バックアップデータセンターへの切替に関する計画の見直し及び修正を行う場合は、切替試験を実施すること。	適宜	－
89						切戻し試験	メインデータセンターへの切戻しに関する計画の見直し及び修正を行う場合は、切戻試験を実施すること。	適宜	－
90						緊急時体制の準備	緊急事態が発生した場合の緊急連絡手段及び備蓄等、体制を準備すること。	適宜	－
91			4.6 サプライヤ管理						
92				－					
93					次期情報システム基盤を構成するハードウェア及びソフトウェアの保守作業について、作業内容の確認等を行う。	事前調整	作業日時、作業時間及び作業内容等について、主管課の承認を得ること。	適宜	－
94						作業時対応	保守作業中は進捗状況を把握し、作業結果を主管課に報告すること。なお、統計センター及び統計データ利活用センター内での作業の場合は、主管課が許可した場合を除き、作業の立会いを行うこと。	適宜	保守作業報告書
95		5. サービストランジション							
96			5.1 変更管理						
97				－					
98					変更管理は、次期情報システム基盤を構成するハードウェア及びソフトウェアに関する全ての変更について、その変更内容と変更による影響について把握することを目的として行う。	変更要求の受付・記録	インシデント管理、問題管理及びキャパシティ管理、主管課からの要求等によって発生する変更要求について、以下の項目を含む変更要求票を作成し、管理すること。 (ア) 変更作業の目的・効果 (イ) 変更作業の対象及び概要 (ウ) 変更作業の実施手順及び切り戻し手順 (エ) 変更内容の動作確認方法 (オ) 変更作業の実施日 (カ) 変更作業の実施者	適宜	－
99						変更要求の評価	変更要求の内容を評価し、主管課に変更要求の承認を申請することが適切か判断すること。	適宜	－
100						変更要求の承認申請	変更要求が適切と判断した場合は、主管課に変更要求の承認を申請すること。	適宜	変更要求承認申請書

運用管理業務一覧

別添4

No	目次 Lv1	Lv2	Lv3	Lv4	目的・定義	作業項目	作業内容	実施頻度	提出物
101			5.2 リリース管理及び展開管理						
102				–					
103					リリース管理は、次期情報システム基盤に対する変更の適用(リリース)を確実に実施するため、リリースにおける正式な手順・方法を確立するとともに、リリース漏れやリリースミスなど、サービスに与える影響を最小限にとどめることを目的として行う。	受け入れ試験	主管課が変更要求を承認した場合は、検証環境等を用いて受入れ試験を行い、手順及びリリース後の動作等に問題がないか確認すること。	適宜	–
104						受け入れ試験結果承認申請	受入れ試験結果の報告と承認申請を主管課へ行うこと。	適宜	受け入れ試験結果承認申請書
105						リリースの実施	承認を得た後、あらかじめ定められた手順に従ってリリースを行うこと。	適宜	–
106						構成管理への引渡し	リリース完了後、リリース対象となったシステム及び関連ドキュメント等について、構成管理に基づき管理すること。	適宜	–
107			5.3 サービス資産管理及び構成管理						
108				–					
109					次期情報システム基盤を構成する要素について、IT資産台帳等を活用し管理する。 構成管理の対象には、ハードウェアやソフトウェアのほか、運用管理を行う上で必要となる操作手順書等のドキュメントを含む。	ハードウェア及びソフトウェアの管理	「IT資産台帳」により次期情報システム基盤を構成するハードウェアの機種名、ソフトウェアの名称、数量及びバージョン等を管理すること。	適宜	–
110						ソフトウェアインベントリ収集	運用管理ツールのソフトウェアインベントリ収集機能を用いて、各ソフトウェアのインストール数、無許可ソフトウェアの有無を調査すること。なお、「IT資産台帳」との乖離が判明した場合は、主管課に報告すること。	適宜	日次報告書
111						通信回線装置のソフトウェアの管理	通信回線装置が動作するために必要なソフトウェアの状態を定期的(1回/月)に調査し、バージョンを調査すること。なお、「IT資産台帳」との乖離が判明した場合は、主管課に報告すること。	1回/月	月次報告書
112						各種操作手順書等の管理	「ドキュメント管理台帳」により次期情報システム基盤の運用管理を行う上で必要となる各種手順書等を管理すること。	適宜	–
113			5.4 ナレッジ管理						
114				–					
115					インシデント、情報セキュリティ管理プロセス、問題管理プロセス等を通じて得られた知識を、組織の知識として管理及び共有する。	対応策の共有及び管理	インシデント管理、情報セキュリティ管理プロセス等から導き出した対応策をナレッジとして、台帳に登録し、運用要員に共有すること。	適宜	–
116						問合せの共有及び管理	サービスデスクにおいて問合せに回答した内容を台帳に登録し、運用要員に共有すること。	適宜	–
117		6. サービスオペレーション							
118			6.1 イベント管理						
119				–					
120					サーバやネットワーク機器、サービス等の稼動状況を監視し、サービス提供が正常に行えているか確認する。 監視運用は、運用管理ツールの自動監視機能等により行う。運用管理ツールは、運用管理端末を用いて操作する。	死活監視	(1)運用管理ツールにより監視対象機器やサービス及びプロセスの停止を即時に検知すること。なお、異常を検知した場合は、一次切り分けを実施すること。 (2)個別アプリケーションの保守事業者に上記一次切り分け結果を連携し、検知した異常への対応を要請すること。なお、検知した異常が、障害であると認められる場合は、インシデント管理及び問題管理として管理すること。 (3)なお、検知した異常における一次切り分け以降の対応(影響範囲及び原因等の調査等)についても、請負者が実施することが望ましい。	常時 適宜	日次報告書
121						ログ監視	(1)運用管理ツールにより監視対象サーバのOS、ミドルウェア、サービス等に関する重要情報(主に障害情報)がログに記録されたことを検知すること。なお、異常を検知した場合は、一次切り分けを実施すること。 (2)個別アプリケーションの保守事業者に上記一次切り分け結果を連携し、検知した異常への対応を要請すること。なお、検知した異常が、障害であると認められる場合は、インシデント管理及び問題管理として管理すること。 (3)なお、検知した異常における一次切り分け以降の対応(影響範囲及び原因等の調査等)についても、請負者が実施することが望ましい。	常時 適宜	日次報告書

運用管理業務一覧

別添4

No	目次				目的・定義	作業項目	作業内容	実施頻度	提出物
	Lv1	Lv2	Lv3	Lv4					
122						性能監視	(1)運用管理ツールにより監視対象サーバのCPU使用率、メモリ使用率及びディスク使用量等を監視し、性能低下を検知すること。なお、異常を検知した場合は、一次切り分けを実施すること。 (2)個別アプリケーションの保守事業者に上記一次切り分け結果を連携し、検知した異常への対応を要請すること。なお、これらの対応は性能管理として管理した上で、調査の結果、障害であると認められる場合は、インシデント管理及び問題管理として管理すること。 (3)なお、検知した異常における一次切り分け以降の対応（影響範囲及び原因等の調査等）についても、請負者が実施することが望ましい。	常時 適宜	日次報告書
123						データベース性能監視	(1)運用管理ツールにより監視対象データベースのバッファキャッシュヒット率、SQL文の実行回数及び接続ユーザ数等を監視し、性能低下を検知すること。なお、異常を検知した場合は、一次切り分けを実施すること。 (2)個別アプリケーションの保守事業者に上記一次切り分け結果を連携し、検知した異常への対応を要請すること。なお、これらの対応は性能管理として管理した上で、調査の結果、障害であると認められる場合は、インシデント管理及び問題管理として管理すること。 (3)なお、検知した異常における一次切り分け以降の対応（影響範囲及び原因等の調査等）についても、請負者が実施することが望ましい。	常時 適宜	日次報告書
124						ポート監視	(1)運用管理ツールにより監視対象ネットワーク機器の各ポート通信量等を監視し、性能低下を検知すること。なお、異常を検知した場合は、一次切り分けを実施すること。 (2)個別アプリケーションの保守事業者に上記一次切り分け結果を連携し、検知した異常への対応を要請すること。なお、これらの対応は性能管理として管理した上で、調査の結果、障害であると認められる場合は、インシデント管理及び問題管理として管理すること。 (3)なお、検知した異常における一次切り分け以降の対応（影響範囲及び原因等の調査等）についても、請負者が実施することが望ましい。	常時 適宜	日次報告書
125						セキュリティ監視	運用管理ツールにより監視対象サーバ、ネットワーク及びサービス等への脅威を即時に検知すること。なお、異常を検知した場合は、当該異常の影響範囲及び原因等を調査し、セキュリティインシデントであると認められる場合は、インシデント管理及び問題管理として管理すること。	常時 適宜	日次報告書
126						目視点検	統計センターの情報システム室内に設置する機器及び温湿度計について、定期的に目視点検すること。 あるいは、WEBなどの機能により遠隔監視によるLED点灯確認を可能とする場合は、WEB機能を用いて、定期的に点検すること。 なお、異常があった場合は、当該異常の影響範囲及び原因等を調査し、障害であると認められる場合は、インシデント管理及び問題管理として管理すること。	1回／日 適宜	日次報告書

運用管理業務一覧

別添4

No	目次 Lv1	Lv2	Lv3	Lv4	目的・定義	作業項目	作業内容	実施頻度	提出物
127			6.2 インシデント管理						
128				–					
129					障害（セキュリティインシデントを含む。）を検知した場合に、速やかにその対応を行い、安定的なサービスの提供を継続することを目的とする。 障害発生からサービスが復旧するまでの間は障害管理票による管理を行い、同様な障害が発生した場合の対応予防に備える。	障害発生報告	障害の発生場所、発生日時及び影響範囲等を把握し、主管課に報告すること。	適宜	–
130						障害レベル切り分け	業務への影響度合いに従い、障害のレベル切り分けを行うこと。	適宜	–
131						障害管理票作成	障害の状況について、定められた「障害管理票」を作成すること。	適宜	–
132						障害情報収集・原因調査	「操作手順書」に基づいて、障害の復旧に必要となる情報を収集し、原因を調査すること。	適宜	–
133						復旧方針の策定	収集した情報等から「操作手順書」に基づいて復旧方針を策定し、主管課の承認を得ること。	適宜	–
134						障害復旧作業の実施及び結果報告	承認された復旧方針及び「操作手順書」に基づき復旧作業を実施し、障害復旧後、主管課に報告すること。	適宜	障害報告書
135						訓練の参加	主管課が実施する、セキュリティ訓練に参加すること。	適宜	–
136			6.3 問題管理						
137				–					
138					障害の業務への影響度合いが高い場合又は障害の根本原因が不明等の理由により障害管理をクローズできない場合については、問題管理とし、対策等を検討する。	原因の究明	「操作手順書」に記載のない障害について、一次切り分けを行い、システム有識者やベンダーへ障害の対応を実施すること。	適宜	–
139						進捗報告	主管課に進捗報告を行うこと。	適宜	障害報告書
140						障害復旧	障害管理に準じ、復旧方針の策定及び修正プログラムの適用等を行うこと。	適宜	–
141			6.4 アクセス管理						
142				① ユーザIDの管理					
143					次期情報システム基盤のユーザIDについて、適切な管理を行う。	ユーザIDの発行	ユーザIDの発行等、次期情報システム基盤で必要となるユーザIDを発行すること。なお、不要になったユーザIDは、速やかに無効化または削除を行うこと。	適宜	–
144						運用管理用ユーザIDの発行	運用管理用ユーザIDは、業務上必要な場合のみ必要最小数発行すること。また、運用管理用ユーザIDは、特権ID管理機能を利用して申請の受付及び管理を行うこと。	適宜	–
145						パスワードの管理	発行したユーザIDのパスワードについて、初期化等を適切に行うこと。	適宜	–
146						ユーザIDの点検	発行したユーザIDについて、不要なユーザIDがないか定期的（1回/半年）に点検すること。なお、不要なユーザIDがあった場合は、速やかに無効化または削除を行うこと。	1回/半年	年次報告書

運用管理業務一覧

別添4

No	目次 Lv1	Lv2	Lv3	Lv4	目的・定義	作業項目	作業内容	実施頻度	提出物
147			6.5 サービスデスク						
148				–					
149					ユーザからの不具合に関する問合せに速やかに対応し、利用者への安定的なサービス提供を継続する。また、利用方法に関する問合せに対応し、円滑なシステムの利用や問題解決のための補佐を行う。	問合せ対応	ユーザからの問合せを受け付け、適切に対応を行うこと。なお、障害が認められた場合は、当該異常の影響範囲及び原因等を調査し、インシデント管理及び問題管理として管理すること。	適宜	–
150						応対履歴情報の管理	サービスデスクに寄せられる問合せに関して応対履歴管理を行うこと。	1回/日	日次報告書
151						FAQ提供	問合せの中で、特に頻繁に問合せのある案件に関してはFAQを作成し、主管課の承諾を得てユーザ用コンテンツとして公開すること。	適宜	FAQコンテンツ
152				–					
153					各種申請書に対し、迅速に対応する。申請書については、契約期間内に追加、変更等を行う場合があり、その場合においても対応する(改正頻度は年1から2件想定)。現在想定している申請書は作業項目のとおり。	人事異動等に関する申請書	「人事異動等に関する申請書」に基づき、次期情報システム基盤で導入したハードウェア及びソフトウェアの増設・移設・撤去、ユーザグループの追加等及びユーザグループに対するメンバー追加等を行うこと。	適宜	週次報告書
154						課室等購入物接続許可申請書	「課室等購入物接続許可申請書」に基づき、課室または個人として持ち込みをしたハードウェア及びソフトウェアについて、増設・移設・撤去に関する作業を行うこと。	適宜	週次報告書
156						情報システム基盤構成変更申請書	「情報システム基盤構成変更申請書」に基づき、次期情報システム基盤を構成するハードウェア及びソフトウェアの変更作業を行うこと。	適宜	週次報告書
157						情報システム接続申請書	「情報システム接続申請書」に基づき、課室等で調達した情報システムを次期情報システム基盤に接続する作業を行うこと。	適宜	週次報告書
158						情報システム基盤例外措置申請書	「情報システム基盤例外措置申請書」に基づき、次期情報システム基盤運営管理規則の例外措置を行うこと。	適宜	週次報告書
159						運用管理等用のユーザID申請書	「運用管理等用のユーザID申請書」に基づき、運用管理用IDの貸し出しに関する作業を行うこと。	適宜	週次報告書
160						非常勤職員ID申請書	「非常勤職員ID申請書」に基づき、非常勤職員ユーザIDの作成、権限変更及び削除を行うこと。	適宜	週次報告書
161						仮ICカード発行申請書	「仮ICカード発行申請書」に基づき、仮ICカードの貸し出しに関する作業を行うこと。	適宜	週次報告書
162						ICカードロック解除申請書	「ICカードロック解除申請書」に基づき、ICカードのロック解除作業を行うこと。	適宜	週次報告書
163						共有フォルダ申請書	「共有フォルダ申請書」に基づき、共有フォルダの作成、容量変更及び削除を行うこと。	適宜	週次報告書
164						共有フォルダアクセス権申請書	「共有フォルダアクセス権申請書」に基づき、以下の作業を行うこと。 ・共有フォルダへのアクセス権設定 ・共有フォルダのアクセス権設定変更 ・共有フォルダのアクセス権削除	適宜	週次報告書
165						データベース申請書	「データベース申請書」に基づき、データベースの作成、容量変更及び削除を行うこと。	適宜	週次報告書
166						データベースユーザ申請書	「データベースユーザ申請書」に基づき、データベースユーザIDの作成、権限変更及び削除を行うこと。	適宜	週次報告書
167						利用職員等用電子メールアドレス変更申請書	「利用職員等用電子メールアドレス変更申請書」に基づき、メールボックスの設定変更を行うこと。	適宜	週次報告書
168						組織、業務等用電子メールアドレス申請書	「組織、業務等用電子メールアドレス申請書」に基づき、メールボックスの作成を行うこと。	適宜	週次報告書
169						リストア作業申請書	「リストア作業申請書」に基づき、対象サーバ又は共有ストレージの対象領域へ、対象データのリストアを行うこと。	適宜	週次報告書
170						室内LAN管理担当者及び同補助者の指名・変更報告書	「室内LAN管理担当者及び同補助者の指名・変更報告書」に基づき、室内LAN管理担当者及び同補助者の変更作業を行うこと。	適宜	週次報告書
171						SharePointサイト申請書	「SharePointサイト申請書」に基づき、サイトの作成を行うこと。	適宜	週次報告書
172						ウェブフィルタリング解除申請書	「ウェブフィルタリング解除申請書」に基づき、ウェブフィルタリングの解除を行うこと。	適宜	週次報告書

運用管理業務一覧

別添4

No	目次 Lv1	Lv2	Lv3	Lv4	目的・定義	作業項目	作業内容	実施頻度	提出物
173	7. 継続的サービス改善								
174		–							
175			–						
176					目標及びKPI（重要業績評価指標）を設定し、継続的な業務の改善を図る。	目標及びKPIの設定	安定稼働及びユーザに提供するサービスの向上に対して、主管課と協議の上、目標及びKPI（重要業績評価指標）を設定し、達成状況を1ヶ月ごとに主管課に報告すること。	適宜 1回/月	月次報告書
177						業務の改善	設定したKPIを達成するために、PDCAサイクルに基づいて継続的に業務の改善を行うこと。	適宜	–
178						目標及びKPIの見直し	運用状況に応じて、設定した目標及びKPIの見直しを年1回行うこと。	1回/年	年次報告書
179						改善する業務内容の提案	改善する業務内容について、随時主管課に提案し、協議の上、実施すること。	適宜	–
180						安定稼働及びユーザに提供するサービスの向上に対しての改善	安定稼働及びユーザに提供するサービスの向上に対して改善提案を実施すること。	適宜	–
181						「運用計画書」等の見直し	改善提案に基づき、「運用計画書」等の見直しを実施すること。	適宜	「運用計画書」等
182	8. その他								
183		8.1 人事異動に伴う作業							
184			–						
185					統計センターにおいて人事異動が発生する場合は、主管課の指示に基づき、内示日から異動発令日までの間（概ね5開庁日）に人事異動に伴う全ての作業が完了するよう、迅速かつ正確に対応する。 想定している作業は作業項目のとおりであるが、機器構成によって変更する場合がある。	クライアント端末の増設・撤去	主管課が取りまとめた人事異動情報に基づき、必要となるPCを用意し、初期インストール作業等を実施した上で、各課室の担当者へ引き渡すこと。PCが不要となる場合は、各課室の担当者から引取り、保管すること。	人事異動時	人事異動作業報告書
186						仮想PCの作成・削除・設定変更	主管課が取りまとめた人事異動情報に基づき、仮想PCの作成・削除・設定変更を行うこと。	人事異動時	人事異動作業報告書
187						組織グループの作成・削除・設定変更	主管課が取りまとめた人事異動情報に基づき、組織グループの作成・削除・設定変更を行うこと。	人事異動時	人事異動作業報告書
188						ユーザIDの追加・削除	主管課が取りまとめた人事異動情報に基づき、ユーザIDの追加・削除を行うこと。各ユーザIDについて、組織グループへの所属情報の更新を行うこと。	人事異動時	人事異動作業報告書
189						メール設定の追加・削除	主管課が取りまとめた人事異動情報に基づき、ユーザIDに対応したメールアドレス及びメールボックスについて、追加・削除を行うこと。	人事異動時	人事異動作業報告書
190						LANケーブルの作成	主管課の指示に基づき、機器の移設等に伴って必要となるLANケーブルを作成し、主管課に引き渡すこと。	人事異動時	人事異動作業報告書
191						複合機の移設	複合機の設置場所の変更が必要となった場合は、主管課の指示に基づき、複合機の設定変更を行うこと。	人事異動時	人事異動作業報告書
192		8.2 インターネット関係システム管理							
193			–						
194					インターネットに関係するシステムについて、Webサーバのアクセス数の解析や改ざん検知、サーバ証明書等の管理、メールの経路設定等を行う。	偽サイト調査	定期的に特定のキーワード（統計センターの名称等）を複数の検索サイトで検索し、統計センターホームページの偽サイトがないか調査すること。	1回/週	週次報告書
199						証明書管理	統計センターホームページ等で使用するサーバ証明書等について、常時有効な状態となるよう管理すること。有効期限の終了が近づいた場合は、証明書発行要求（CSR：Certificate Signing Request）の作成、サーバへの登録等を行うこと。これらの作業は、変更管理及びリリース管理として管理すること。	適宜	変更要求承認申請書
200						メール経路設定	統計センターの外部と送受信するメールのうち、特定のドメインのメールについては、政府共通ネットワークを経由して送受信を行うよう設定すること。経路設定作業は、変更管理及びリリース管理として管理すること。	適宜	変更要求承認申請書

運用管理業務一覧

別添4

No	目次 Lv1	Lv2	Lv3	Lv4	目的・定義	作業項目	作業内容	実施頻度	提出物
201			8.3 技術的支援等						
202				① 技術的支援					
203					主管課が次期情報システム基盤の運用管理業務に関する改善提案等を要求した場合に、可能な範囲で提案等を行う。	運用の改善提案	主管課が次期情報システム基盤の運用管理業務における改善提案を要求した場合、提案を行うこと。	適宜	関連ドキュメント
204						技術情報の提供	主管課が次期情報システム基盤に関連する技術情報の提供を要求した場合、提供を行うこと。	適宜	関連ドキュメント
205						打ち合わせの出席	主管課が要求した場合、次期情報システム基盤に関連する打ち合わせに同席し、技術的提言等を行うこと。	適宜	–
206							主管課が要求した場合、次々期情報システム基盤に関連する打ち合わせに同席し、情報の提供及び技術的提言等を行うこと。	適宜	–
207				② 復旧訓練					
208					次期情報システム基盤が提供するサービスの継続性管理の観点から、システム復旧に関する訓練等を行う。	手順書の確認	復旧に係る手順書等について、所在確認及び内容確認を行うこと。	1回/年	年次報告書
209						復旧訓練の実施	主管課が必要と判断した場合は、障害発生を想定した連絡体制の確認等の訓練を行うこと。	適宜	–
210				③ 主管課の指示に基づく作業					
211					主管課が必要と判断した場合、主管課からの指示に基づき作業を行う。	主管課が必要とする作業	主管課が必要と判断した場合、主管課の指示に基づき作業を行うこと。具体的には次のような作業を想定している。 (1) 各種ログの調査(不審メールの受信履歴及びサーバへのアクセス履歴等) (2) マルウェアチェックの実施(ゼロデイで侵入したマルウェアが後日検出された場合等) (3) ソフトウェアインベントリの収集(無許可ソフトウェアの調査等)	適宜	保守作業計画・報告書
212			8.4 業務引継資料の作成及び引継ぎの実施等						
213				–					
214					現行情報システム基盤の運用事業者から引き継ぎを受け、次期情報システム基盤の運用業務を実施可能にする。 また、本業務終了時には、次の運用業務を実施する事業者へ引継ぎを実施する。	現行情報システム基盤の運用事業者からの引継ぎ	契約締結後、引継ぎ期間(令和6年10月から3か月間を予定)中に、現行情報システム基盤の運用事業者から業務内容を明らかにした書類等により業務内容の引継ぎを受けること。	適宜	–
215						次の運用業務を実施する事業者への引継ぎ	本業務の終了に伴い請負者が変更となる場合には、契約期間満了の1か月前までに本業務に関する業務引継資料(本業務に必要な運用マニュアル等を含む。)を作成し、主管課の指示により次の運用業務を実施する事業者へ引継ぎを行うこと。なお、業務引継ぎに当たっては、次の運用業務を実施する事業者が速やかに業務を開始できるよう、適切な支援を行うこと。	適宜	–
216						最終バックアップ	契約期間の満了月に最終バックアップを実施し、バックアップデータの所在を主管課へ連絡すること。最終バックアップの実施時期については、主管課と協議する。	適宜	–

運用におけるサービスレベル目標

別添5

SLA項目	内容	サービスレベル値	報告頻度	評価
セキュリティ上の重大障害件数	システム運用管理上で発生したセキュリティインシデント件数が右記サービスレベル値を満たす。	0件	年次及び月次	年次及び月次
障害復旧	業務時間内に次期情報システム基盤を構成する機器(PC及び周辺機器を除く。)においてサービスの停止を伴う障害(請負者が「操作手順書」で対応できる範囲に限る。)が発生した場合に、障害が発生した時点からサービス再開までの時間が右記サービスレベル値を満たす。	1時間以内	年次及び月次	年次及び月次
障害対応開始時間	次期情報システム基盤を構成する機器(PC及び周辺機器を除く。)において障害が発生した場合に、障害が発生した時点から10分以内に対応を開始した件数の割合が右記サービスレベル値を満たす。 対応率(%)=(10分以内に対応を開始した件数)÷(障害件数)×100	年99%以上	年次及び月次	年次及び月次
一次回答率	エスカレーションを必要としない問合せに対し、サービスデスク内で回答し完了させた問合せの比率として、右記サービスレベル値を満たす。	90%以上	年次及び月次	年次及び月次
申請対応	申請書に記載された実施希望日に作業を実施し、完了した件数の割合が右記サービスレベル値を満たす。ただし、実施希望日に対応が困難な場合は、申請者に実施可能日時を伝え了承を得ることとし、主管課へその旨を報告し承認を得ることで対応件数に含めることができる。 対応率(%)=(希望日実施件数)÷(申請件数)×100	年99%以上	年次及び月次	年次及び月次
照会(疑義)対応	業務時間内における次期情報システム基盤のユーザからの不具合に関する照会及び利用方法等に関する照会に対して、照会時点から1開庁日以内に対応が完了した件数の割合が右記サービスレベル値を満たす。ただし、時間内に解決することが困難な場合は、照会者へ完了予定を伝え了承を得ることとし、主管課へその旨を報告し承認を得ることで対応件数に含めることができる。 対応率(%)=(対応件数)÷(照会件数)×100	年99%以上	年次及び月次	年次及び月次
経過報告間隔	長時間の調査を要する障害対応及び問合せに対し中間報告を行う時間間隔として、右記サービスレベル値を満たす。	1時間以内	年次及び月次	年次及び月次

従来の実施状況に関する情報の開示

別添6

1.従来の実施に要した経費　（単位：円）

			令和元年～令和6年
独立行政法人統計センター情報システム基盤等運用管理業務の請負			
	人件費	常勤職員	－
		非常勤職員	－
	物件費		－
	請負費	役務（運用員）	217,800,000
		機器・回線リース料	－
		設計・構築費	－
		その他	－
計　(a)			217,800,000
参考値　(b)	減価償却費		－
	退職給付費用		－
	間接部門費		－
(a)+(b)			217,800,000

（注意事項）

- 上記は運用管理業務に係る経費のみである。
- 上記に示した経費は、税抜きの金額を記載している。
- 請負業務のため、費用の詳細な内訳の開示は受けられない。
- 契約期間は令和元年10月～令和6年12月末まで
- 運用管理業務を提供する期間は令和2年1月～令和6年12月末まで。

2.従来の実施に要した要員　（単位：人）

	令和元年度	令和2年度	令和3年度	令和4年度	令和5年度	
（運用業務従事者）						
運用責任者	1	1	1	1	1	
運用担当者	6	6	9	7	6	

※　人数に関しては繁忙期の人数を記載しており、人数の増減は請負事業者の判断による。

（業務の繁閑の状況とその対応）

令和元年、2年、3年、4年、5年度の運用業務の主な対応状況は以下のとおり。

令和元年度　（単位：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
サーバ障害対応										0	0	0
ヘルプデスク業務												
問合せ対応										97	54	48
申請書対応										92	101	80
不正プログラム対応										0	1	0

令和2年度　（単位：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
サーバ障害対応	0	0	0	0	0	0	0	2	0	0	0	3
ヘルプデスク業務												
問合せ対応	46	34	55	61	31	47	57	53	28	70	101	119
申請書対応	219	44	45	96	43	46	89	58	93	38	52	30
不正プログラム対応	0	0	0	0	0	0	0	0	0	0	0	0

令和3年度　（単位：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
サーバ障害対応	0	0	0	0	0	0	0	0	1	5	4	4
ヘルプデスク業務												
問合せ対応	76	77	83	53	73	74	54	59	92	44	38	54
申請書対応	192	57	90	68	51	66	52	74	54	74	51	59
不正プログラム対応	0	0	0	0	0	0	0	0	0	0	0	0

令和4年度　（単位：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
サーバ障害対応	0	0	0	0	0	0	0	0	0	0	0	0
ヘルプデスク業務												
問合せ対応	74	70	69	97	134	97	74	43	74	54	61	49
申請書対応	139	84	64	72	55	77	93	51	69	65	60	73
不正プログラム対応	0	0	0	0	0	0	0	0	0	0	0	0

令和5年度　（単位：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
サーバ障害対応	0	0	0	0	0	1	0					
ヘルプデスク業務												
問合せ対応	80	43	68	43	55	54	52					
申請書対応	174	74	83	80	59	50	78					
不正プログラム対応	0	0	0	0	0	0	0					

※　ヘルプデスク業務の件数は、人事異動が多い月（1、4、7、10月）に増える傾向がある。

3.従来の実施に要した施設及び設備

【施設】
施設名称:総務省第2庁舎
使用場所:情報システム室、2階事務室

【設備及び主な物品】
統計センター貸与:
　内線電話3台(PHS)、作業机4台、移動式本立2台、事務机1台、事務椅子6脚、パイプ椅子1脚、ロッカー1台、ホワイトボード1台、ごみ箱1個、HUBラック1台、HUB1台、プリンタ1台、PC20台(各個人用PC5台、運用管理用PC4台、検証用PC11台)

請負者所有:
PC1台

【利用施設】
施設名称:メインデータセンター
使用場所:
施設名称:バックアップデータセンター
使用場所:
施設名称:統計データ利活用センター
使用場所:和歌山県

【設備及び主な物品】
なし。

(注意事項)
・上記施設、設備等は、運用管理業務を行う範囲において無償貸与(光熱費及び通信費含む)。

データセンター等での現地作業が必要となった回数。

保守作業(テープ交換等)　(単位:回)

	令和元年度	令和2年度	令和3年度	令和4年度	令和5年度	
メインデータセンター	1	1	1	2		
バックアップデータセンター	0	0	0	0		
統計データ利活用センター	0	0	0	0		

4.従来の実施における目標の達成の程度

統計センターの運用管理については、統計センターの業務を確実に実施するため、情報システムの利用者への継続的・安定的なサービスの提供を円滑に行う事を目的としている。

(1) 業務内容

実施要項に記載している運用管理業務を適切に実施している。

(2) セキュリティ上の重大障害件数

セキュリティ上の重大障害は無い。

	令和元年度	令和2年度	令和3年度	令和4年度	令和5年度	
重大障害件数	0	0	0	0		

(3) システム基盤の稼働率(稼働率:システム基盤の稼働率が99%以上であること)

令和2年度にSLAを超えるシステム停止が発生しているが、改善を図り、以後は稼働率を守れている。

	令和元年度	令和2年度	令和3年度	令和4年度	令和5年度	
停止時間	0	24時間	9.75時間	9分		
稼働率	100.00%	99.71%	99.89%	99.99%		

(4) 障害対応(対応率:10分以内に対応を開始した件数の割合が99%以上であること)

令和3年度に一回、システム基盤を構成する機器において障害が発生した場合に、障害が発生した時点から10分以内に対応できなかった障害が発生している。

	令和元年度	令和2年度	令和3年度	令和4年度	令和5年度	
障害件数	0	5	18	5		
10分以内に対応を開始した件数	0	5	17	5		
対応率	100%	100%	92%	100%		

(5) 障害復旧(サービス再開までの時間が1時間を超える件数が年2件以内であること)

令和2年度に1回、令和3年度に1回、業務時間内にシステム基盤を構成する機器においてサービスの停止を伴う障害(運用業者の責務によらないもの及びハードウェア障害を除く。)が発生している。

	令和元年度	令和2年度	令和3年度	令和4年度	令和5年度	
障害件数	0	5	18	4		
未達成件数	0	1	1	0		

(6) 照会対応(対応率:1開庁日以内に対応が完了した件数の割合が99%以上であること)
業務時間内におけるシステム基盤の利用者からの不具合に関する照会や利用方法等に関する照会に対して、照会時点から1開庁日以内に対応が完了した件数の割合は100%であり、サービスの質は確保されている。

	令和元年度	令和2年度	令和3年度	令和4年度	令和5年度	
照会件数	200	709	813	779		
対応件数	200	709	813	779		
対応率	100%	100%	100%	100%		

(7) 申請対応(対応率:実施希望日に作業を完了した件数の割合が99%以上であること)
申請書に記載された実施希望日に作業を実施し、完了した件数の割合は100%であり、サービスの質は確保されている。

	令和元年度	令和2年度	令和3年度	令和4年度	令和5年度	
申請件数	151	836	913	782		
希望日実施件数	151	836	913	782		
対応率	100%	100%	100%	100%		

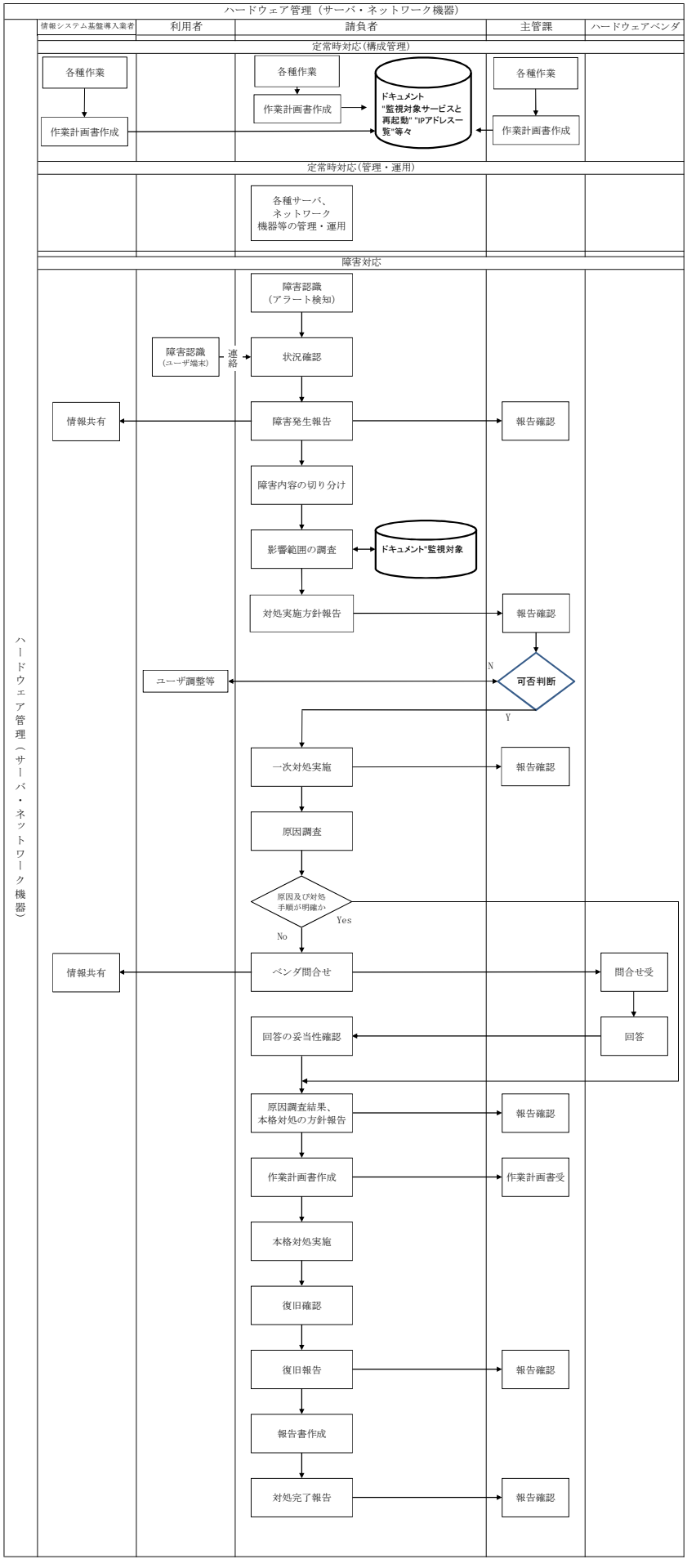
(8) ヘルプデスク利用者アンケート調査結果
ヘルプデスク利用者アンケート調査を実施した結果、各利用者の4つの回答の平均スコアは、令和元年が94.9点、令和2年が86.8点、令和3年が89.2点、令和4年が93.3.9点であり、システム更改後にいったん評価を落としたものの、改善が図られている。

	令和元年度	令和2年度	令和3年度	令和4年度	令和5年度	
問い合わせから回答までに要した時間	94点	82.8点	86.1点	93.4点		
回答又は手順に対する説明の分かりやすさ	93.5点	86.7点	89.2点	91.9点		
回答又は手順に対する結果の正確性	94.5点	86.3点	89.4点	92.7点		
担当者の対応(言葉遣い、親切さ、丁寧さ等)	97.4点	91.5点	92.3点	95.2点		
全体の平均	94.9点	86.8点	89.2点	93.3点		

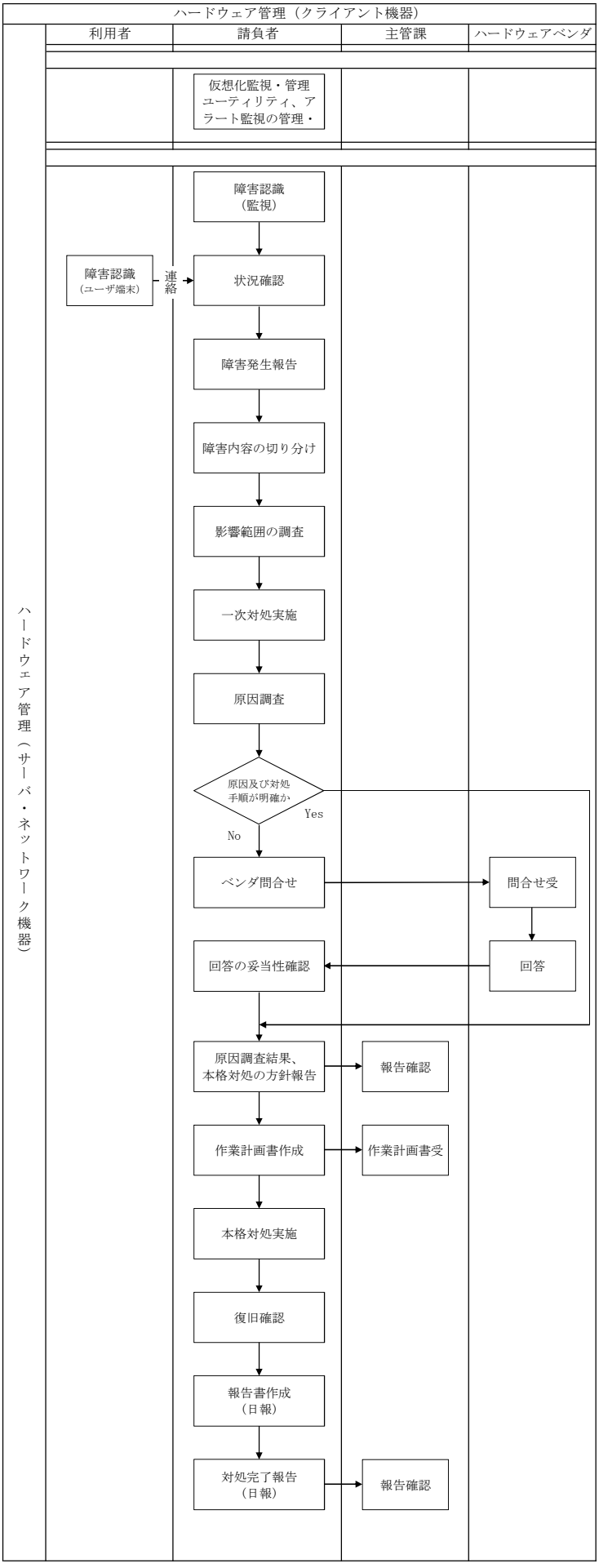
5.従来の実施方法等
従来の実施方法（業務フロー図等） 「別添7　業務フロー図」のとおり 　　なお、本フローは、現行の運用業務を示すものであり、次期の運用業務を示すものではない。 「別添8　　統計センター組織図」

業務フロー図

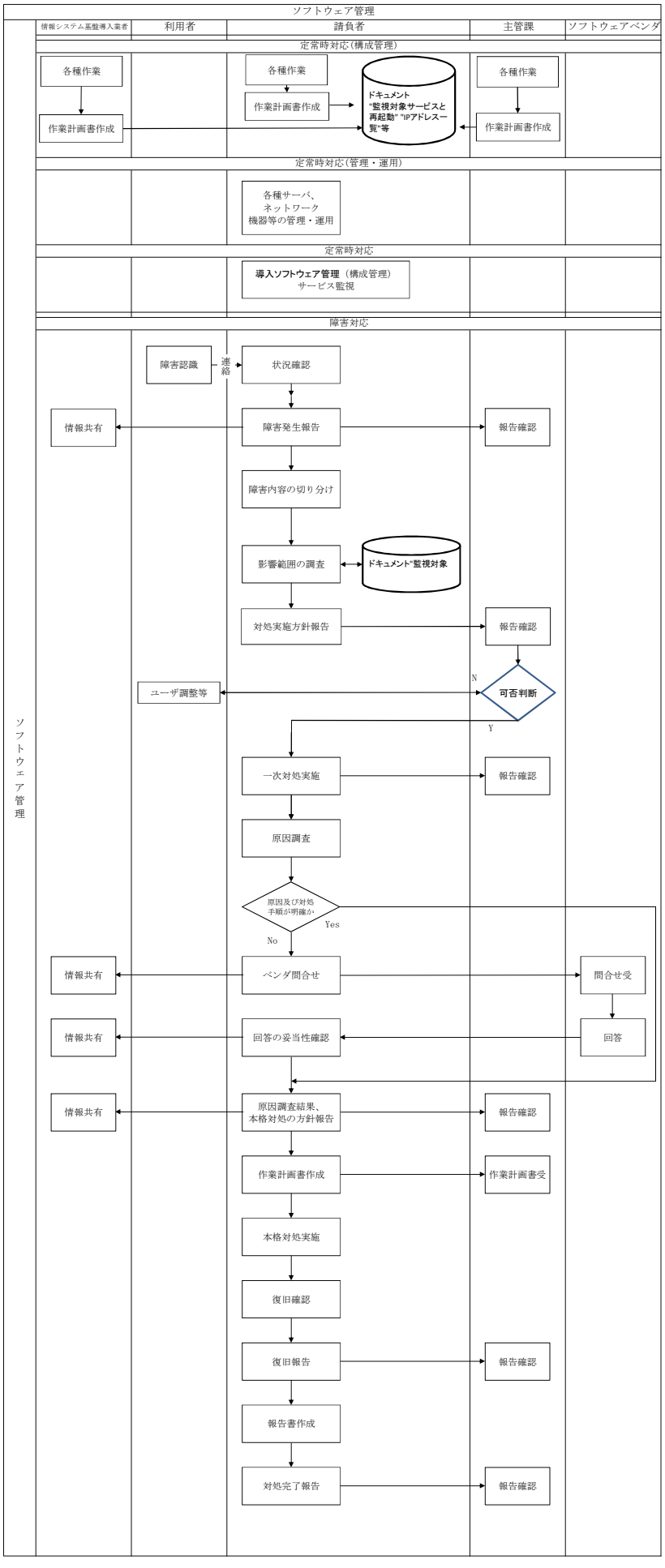
業務フロー図　　別添７



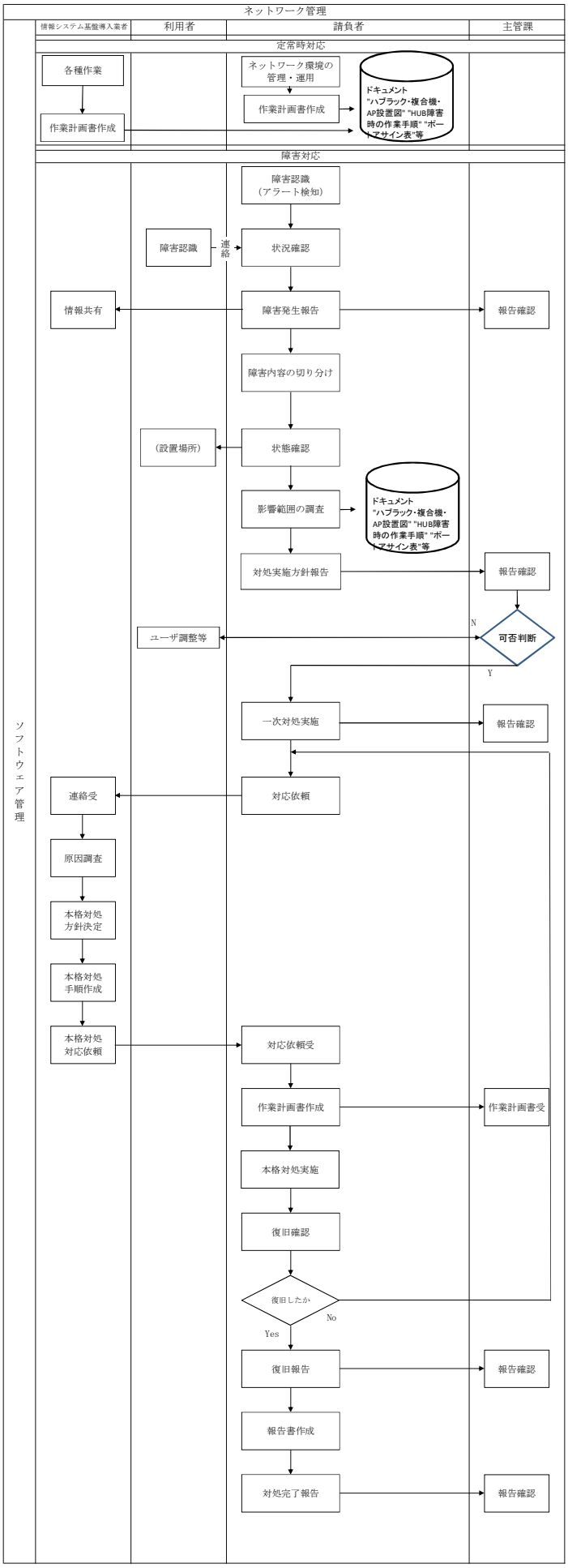
業務フロー図


ハードウェア管理（クライアント機器）
利用者
請負者
主管課
ハードウェアベンダ
仮想化監視・管理
ユーティリティ、ア
ラート監視の管理・
障害認識
（監視）
障害認識
（ユーザ端末）
連絡
状況確認
障害発生報告
障害内容の切り分け
影響範囲の調査
一次対処実施
原因調査
原因及び対処
手順が明確か
Yes
No
ベンダ問合せ
問合せ受
回答
回答の妥当性確認
原因調査結果、
本格対処の方針報告
報告確認
作業計画書作成
作業計画書受
本格対処実施
復旧確認
報告書作成
（日報）
対処完了報告
（日報）
報告確認
ハードウェア管理（サーバ・ネットワーク機器）

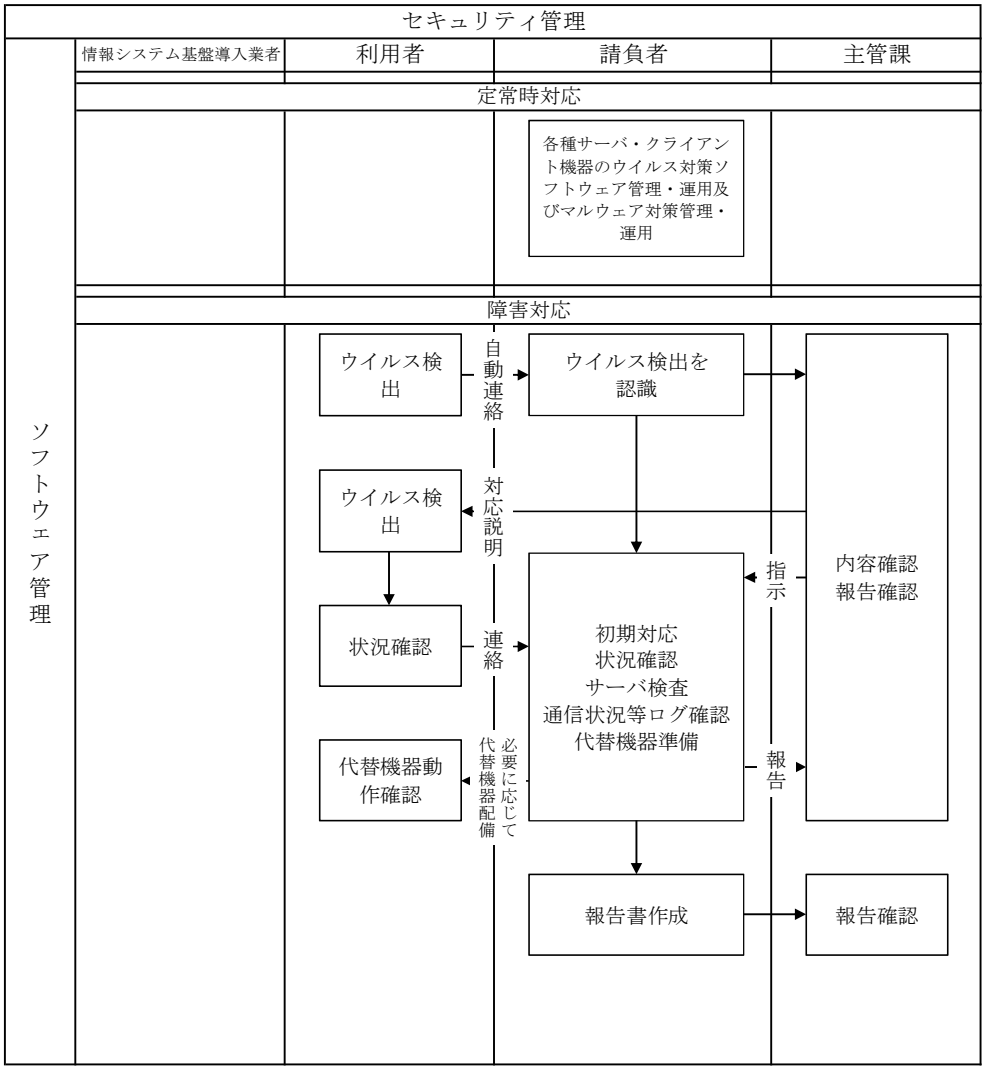
業務フロー図


ソフトウェア管理
情報システム基盤導入業者
利用者
請負者
主管課
ソフトウェアベンダ
定常時対応(構成管理)
各種作業
作業計画書作成
各種作業
作業計画書作成
ドキュメント
"監視対象サービスと再起動" "IPアドレス一覧"等
各種作業
作業計画書作成
定常時対応(管理・運用)
各種サーバ、ネットワーク機器等の管理・運用
定常時対応
導入ソフトウェア管理（構成管理）
サービス監視
障害対応
障害認識
連絡
状況確認
情報共有
障害発生報告
報告確認
障害内容の切り分け
影響範囲の調査
ドキュメント"監視対象
対処実施方針報告
報告確認
N
可否判断
ユーザ調整等
Y
一次対処実施
報告確認
原因調査
原因及び対処手順が明確か
Yes
No
情報共有
ベンダ問合せ
問合せ受
情報共有
回答の妥当性確認
回答
情報共有
原因調査結果、本格対処の方針報告
報告確認
作業計画書作成
作業計画書受
本格対処実施
復旧確認
復旧報告
報告確認
報告書作成
対処完了報告
報告確認
ソフトウェア管理

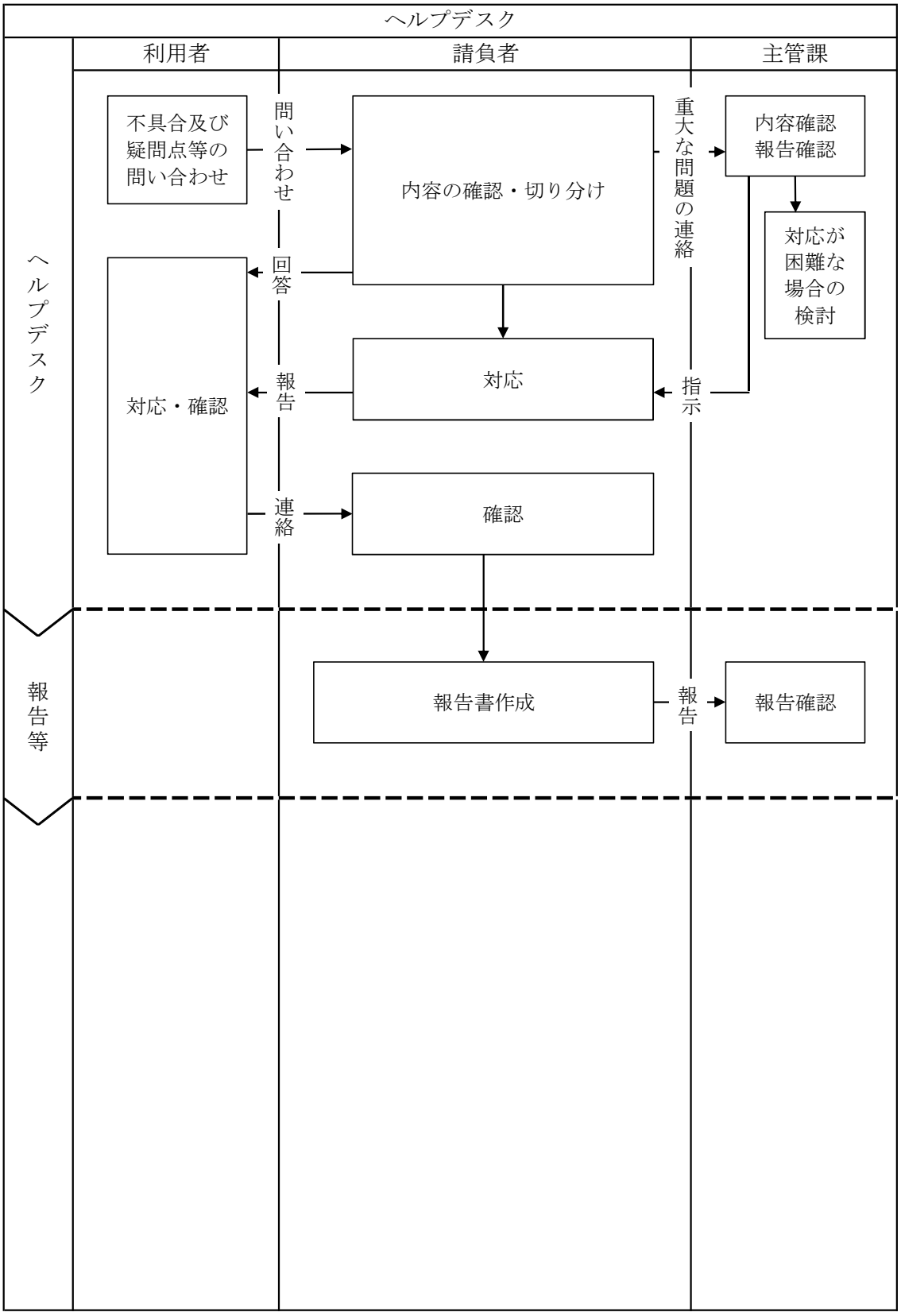
業務フロー図


ネットワーク管理
情報システム基盤導入業者
利用者
請負者
主管課
定常時対応
各種作業
作業計画書作成
ネットワーク環境の管理・運用
作業計画書作成
ドキュメント "ハブラック・複合機・AP設置図" "HUB障害時の作業手順" "ポートアサイン表"等
障害対応
障害認識（アラート検知）
障害認識
連絡
状況確認
情報共有
障害発生報告
報告確認
障害内容の切り分け
（設置場所）
状態確認
影響範囲の調査
ドキュメント "ハブラック・複合機・AP設置図" "HUB障害時の作業手順" "ポートアサイン表"等
対処実施方針報告
報告確認
N
可否判断
ユーザ調整等
Y
一次対処実施
報告確認
連絡受
対応依頼
原因調査
本格対処方針決定
本格対処手順作成
本格対処対応依頼
対応依頼受
作業計画書作成
作業計画書受
本格対処実施
復旧確認
復旧したか
No
Yes
復旧報告
報告確認
報告書作成
対処完了報告
報告確認
ソフトウェア管理

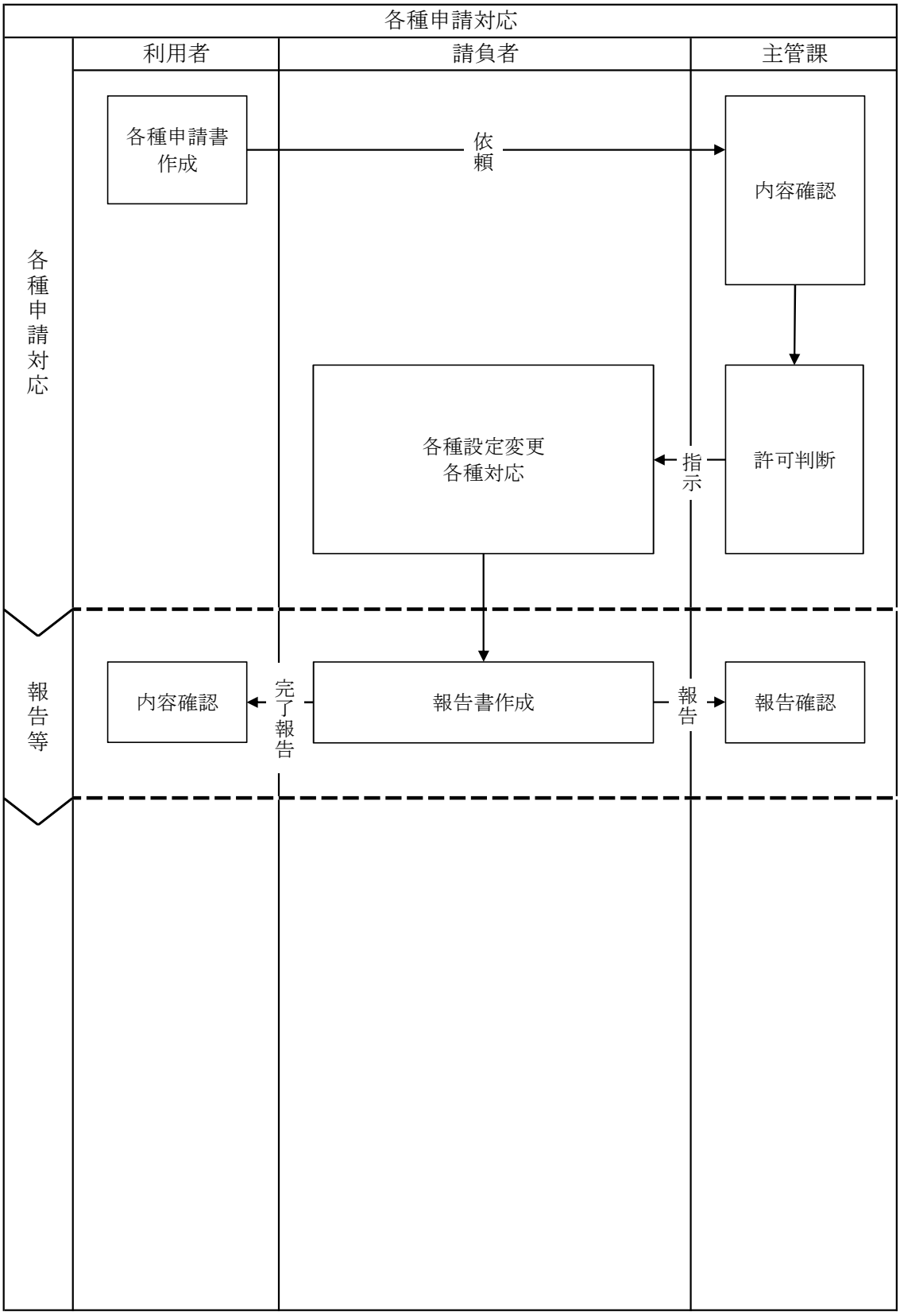
業務フロー図


セキュリティ管理
ソフトウェア管理
情報システム基盤導入業者
利用者
請負者
主管課
定常時対応
各種サーバ・クライアント機器のウイルス対策ソフトウェア管理・運用及びマルウェア対策管理・運用
障害対応
ウイルス検出
自動連絡
ウイルス検出を認識
ウイルス検出
対応説明
状況確認
連絡
初期対応
状況確認
サーバ検査
通信状況等ログ確認
代替機器準備
指示
内容確認
報告確認
代替機器動作確認
必要に応じて代替機器配備
報告
報告書作成
報告確認

業務フロー図

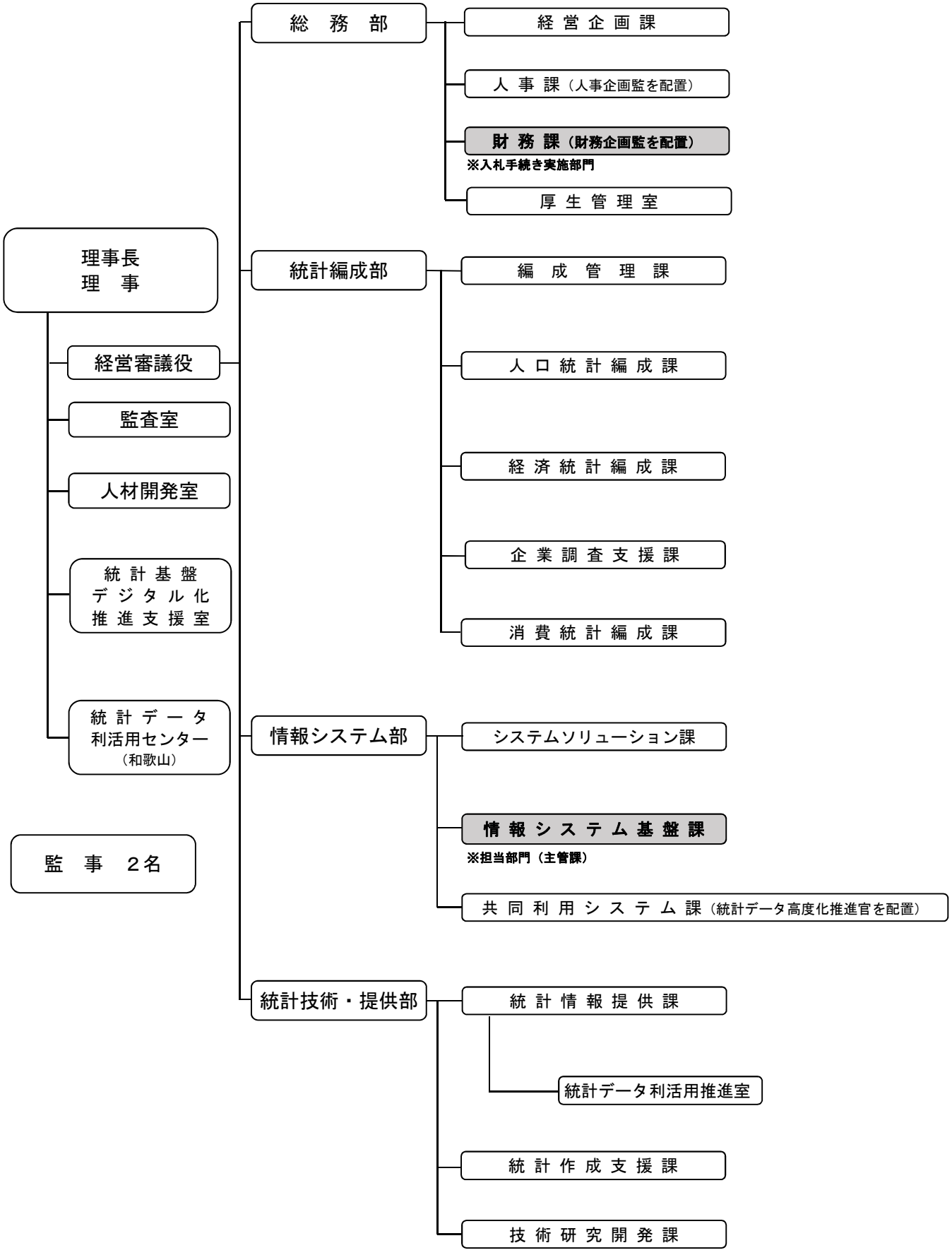

ヘルプデスク
利用者
請負者
主管課
ヘルプデスク
不具合及び疑問点等の問い合わせ
問い合わせ
内容の確認・切り分け
重大な問題の連絡
内容確認
報告確認
対応が困難な場合の検討
回答
対応・確認
報告
対応
指示
連絡
確認
報告等
報告書作成
報告
報告確認

業務フロー図


各種申請対応
利用者
請負者
主管課
各種申請書作成
依頼
内容確認
各種申請対応
各種設定変更
各種対応
指示
許可判断
報告等
内容確認
完了報告
報告書作成
報告
報告確認

統計センター組織図（令和５年４月１日現在）

別添８



別添９

情報保護・管理要領

請負者は、本業務における情報の保護・管理に関して、以下の項目を遵守すること。なお、ここでいう情報とは、本業務実施のために作成した情報（すでに公知である情報を除く。）及び主管課から貸与又は提示された情報をいう。

１．　業務開始前の遵守事項

請負者は下記(1)から(5)までの各項目に定める事項を定めた「情報管理計画書」を作成し、主管課の承認を受けること。

(1)　情報取扱者の指定

情報を取り扱う者（以下「情報取扱者」という。）を指定し、情報取扱者のうち、情報取扱者を統括する立場にある者１名を情報取扱責任者として指定すること。なお、情報取扱者は、守秘義務等の情報の取扱いに関する社内教育又はこれに準ずる講習等（以下「社内情報セキュリティ教育」という。）を受講した者とし、「情報管理計画書」には、上記に従って指定した情報取扱者の所属、役職、氏名、及び社内情報セキュリティ教育の受講状況を明記すること。

(2)　情報の取扱いに関する措置の策定

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

(3)　作業場所における情報セキュリティ確保のための措置の策定

統計センター内又は主管課が指定する場所以外の作業場所において本契約に係る作業を行う場合は、情報セキュリティ確保のために、作業場所の環境、作業に使用する情報システム等に講じる措置を定めること。

(4)　情報漏えい等の事案発生時の対応手順等の策定

情報漏えい等の事案が発生した場合の対応手順等を定めること。

(5)　情報管理計画書の情報取扱者への周知

情報取扱者に対し、情報管理計画書の内容について、周知すること。

２．　業務履行中における遵守事項

(1)　「情報管理計画書」に基づく情報セキュリティ確保

「情報管理計画書」に記載した、情報の取扱い及び作業場所における情報セキュリティ確保のための措置を実施すること。

(2)　「情報管理簿」の作成

情報が記載された各種ドキュメント、情報が記録された電子データ等について、授受方法、保管場所、保管方法、作業場所、使用目的等取扱方法を明確にするため「情報管理簿」を作成すること。

(3)　「情報管理計画書」の変更に関する報告

本業務履行中に、業務開始前に提出した「情報管理計画書」の内容と異なる措置を実施する場合は、以下の手続きを行うこと。

① 情報取扱者の変更を行う場合は、事前にその旨を主管課に報告し、承認を得ること。また、承認された変更の内容を記録し保存すること。

② 「情報管理計画書」に記載した、情報の取扱いに関する措置又は作業場所における情報セキュリティ確保のための措置を変更する場合は、当該箇所を変更した「情報管理計画書」を主管課に提出し、承認を得ること。

③ 一時的に、「情報管理計画書」に記載した、情報の取扱いに関する計画又は作業場所における情報セキュリティ確保のための措置とは異なる措置を実施する場合は、原則として事前にその旨を主管課に報告し、承認を得ること。

(4)　作業場所の確認の受け入れ

統計センターまたは主管課が指定する場所以外の作業場所において本契約に係る作業を行っている場合に、主管課が、その施設及び設備に関し、１(3)で策定した措置の実施状況の確認を要請した際は、これを受け入れること。

３．　業務完了時の遵守事項

本業務完了時に２(2)で作成した「情報管理簿」に記載されているすべての情報について、返却、消去、廃棄の処理を行うこと。なお、その処理について方法、日時、場所、立会人、作業責任者等の事項を網羅した「情報返却等計画書」を事前に主管課に提出し、承認を得ること。処理の終了後、その結果を記載した「情報管理簿」を主管課に提出すること。

独立行政法人統計センター
情報システム基盤の構築及び
サービス提供業務

別添 10
提案依頼書

目次

1. 調達の概要

1.1 目的

本提案依頼書は、「独立行政法人統計センター情報システム基盤の構築及びサービス提供業務に係る調達仕様書（以下「調達仕様書」という。）」で規定された調達を実施するにあたり、本調達に対し、応札する事業者（以下「提案者」という。）に提案書の作成を依頼することを目的としている。

1.2 入札スケジュール

入札スケジュールは以下のとおりとする。

（ア）官報公示　　：令和 5 年 12 月 27 日
（イ）提案書提出期限　：令和 6 年 2 月 26 日
（ウ）開札日　　：令和 6 年 3 月 29 日

2. 調達するシステム等の要件

提案及び調達の実施内容は、「調達仕様書」に記載する要件を全て満たすこと。なお、「調達仕様書」は本調達として求める機能、構成及び業務内容について、最低限の基準を示したものである。従って、「調達仕様書」に記載していない事項であっても、次期情報システム基盤を効率的に稼働させるために必要な機能及び業務を含んだ最適な内容にて、「調達仕様書」の要件を満たす提案書を作成するものとする。また、「調達仕様書」に記載されていない物品及び作業であっても、次期情報システム基盤の稼働に必要なものがある場合は、これを調達の対象として納品するものとする。

3. 提案書作成要領

3.1 提出書類

提案者は、以下の書類を提出すること。

（ア）提案書
（イ）提案者記入欄に所要の記載を行った「別紙　総合評価基準表」
（ウ）一般競争入札参加の資格審査結果通知書の写し
（エ）調達仕様書に要件として記載された資格及び認定の取得証明書の写し
（オ）導入機器一覧
（カ）再委託承認申請書

3.2 記載要領及び様式等

3.2.1 提案書

（ア）正 1 部、副 5 部を提出すること。なお、正 1 部のみに提案者名を記載すること。また、副 5 部には様式や表紙のみならず本文中にも提案者名、

会社ロゴマーク、コーポレートカラー等を表示せず、提案者を特定できないものとすること。

（イ）提案書は、以下の要領に基づき記載すること。

(1) A4 縦長横書き両面とすること。

(2) 頁数制限は設けない。

(3) 提案の記載順序は、「別紙　総合評価基準表」に示す順序とすること。

(4) 「別紙　総合評価基準表」との対応がわかるよう、索引シールを付けること。

(5) 「提案区分」を「必須」とする評価項目全てに対して提案内容を記載すること。

(6) 個々の提案内容における「別紙　総合評価基準表」の対応箇所を明記すること。

(7) 機能証明としてハードウェア及びソフトウェアの諸元は提案書本編に示し、メーカーカタログ等を別添として添付すること。なお、メーカーカタログにおいて要求仕様を満たすことを証明する箇所は、該当箇所を蛍光ペン等でマーキングすること。

3.2.2　提案者記入欄に所要の記載を行った「別紙　総合評価基準表」

（ア）正 1 部、副 5 部を提出すること。正 1 部のみに提案者名を記載すること。副 5 部には提案者名を記載しないこと。

（イ）「別紙　総合評価基準表」は以下の要領に基づき記載すること。

(1) 「提案者記入欄」に、当該評価項目に対応する記載該当箇所を明記すること。なお、「評価項目種別」を「加点」とする評価項目についてのみ、「提案内容の要約」を記載すること。

3.2.3　電子データの提出様式

電子データについては、電子媒体を正副 1 部ずつ（合計 2 部）提出すること。正 1 部のみに提案者名を記載すること。副 1 部には提案者名を記載しないこと。また、電子データは、Microsoft Office 形式及び PDF 形式の 2 種類を提出すること（証明書類については PDF 形式のみでも可とする。）。上記以外のファイル形式の場合は、主管課に連絡し指示を受けること。

3.3　提案依頼事項

（ア）提案者は、「調達仕様書」に記載した項目に対する提案を記述した提案書により提案すること。なお、提案にあたっては、「調達仕様書-2.調達の概要に関する事項」に記載した本調達における業務内容を理解し、具体的な提案を行うこと。

（イ）提案内容は提案者が本調達内で実現し得るものとし、「調達仕様書」に記述のある調達以外の発注を要する提案は記載しないこと。なお、「調達仕様書」に記載した内容と矛盾する提案は行わないこと。ただし、「調達仕様書」が想定する実現方法と比較してより効果的・効率的な案を提案することも可能とするが、その場合は「調達仕様書」が想定する実現方法とは異なる提案である旨を明記すること。

（ウ）万が一、提案内容が実現できない場合は、主管課との協議の上でその他の方法を検討することとし、検討及びその実現に係る費用は提案者の負担とする。

3.4　提出場所

（ア）郵便番号　　：162-8668
（イ）住所　　：東京都新宿区若松町 19-1 総務省第 2 庁舎
（ウ）電話番号　　：03-5273-1219
（エ）契約担当課　　：統計センター総務部財務課

3.5　提出期限

令和 6 年 2 月 26 日 14 時(郵送の場合は必着のこと。)

3.6　提出方法

提案書類の提出方法は、郵送または持参とする。

3.7　留意事項

（ア）提案者は提案書にて提案した事項について、主管課からの指示があった場合は追加の費用請求なく、その事項について実施すること。
（イ）提案に係る経費は提案者の負担とする。
（ウ）提出された提案書類等は、本調達の請負先選定のためのみに使用するものとする。
（エ）提出された提案書等は返却しない。

3.8　問合せ先

「3.4 提出場所」に問い合わせること。

4.　提案書評価

4.1　評価方式

提案者には、次期情報システム基盤の効率的、効果的かつ円滑に安定的なシステム稼働開始及び安定的な運用を行うために、次期情報システム基盤の設計・構築、テスト、移行及び運用・保守を求めるものである。従って、事業者選定にあたって

は、予定価格の制限範囲内の価格をもって有効な入札を行った者のうち、入札価格及び事業者の幅広い能力・ノウハウ等の技術力を総合的に評価して落札者を決定する総合評価落札方式によって行う。

4.2　評価概要

4.2.1　総合評価点数による評価

（ア）提案内容及び入札価格を基に、技術点及び価格点を算出の上、その合計点数を総合評価点数とし、最も総合評価点数が高い者を落札者とする。

（イ）最も総合評価点数が高い者が、2 者以上あるときは、該当者のくじ引きによって落札者を決定する。

総合評価点数　＝　価格点　＋　技術点

4.2.2　技術点及び価格点の配点

技術点及び価格点の比率は、1：1 とし、配点は下記「表 1　技術点及び価格点の配点」のとおりとする。

表 1　技術点及び価格点の配点

評価区分	配点
技術点	21,900 点
価格点	21,900 点

4.3　価格点の評価

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価格点に対する得点配分を乗じて得た値とする。

価格点　＝　価格点の得点配分　×　（1－（入札価格/予定価格））

4.4　技術点

4.4.1　技術点の評価

（ア）技術点は、基礎点及び加点を加算した値とする。

技術点　＝　基礎点　＋　加点

（イ）基礎点及び加点の配点は下記「表 2　基礎点及び加点の配点」のとおりとする。

表 2　基礎点及び加点の配点

評価区分	配点
基礎点	400 点
加点	21,500 点

4.4.2　基礎点の評価

「別紙　総合評価基準表」において「評価項目種別」が「基礎点」に区分されている評価項目が全て合格となった者に基礎点を付与する。なお、基礎点評価項目のうち 1 項目でも不合格となった者は失格とする。

4.4.3　加点の評価

①　加点項目の採点方法

（ア）加点評価の項目は、「別紙　総合評価基準表」において「評価項目種別」が「加点」に区分されている項目である。

（イ）評価項目については提案を必須とする評価項目と任意とする評価項目があり「提案区分」が「必須」の項目について、1 項目でも提案を記載していないまたは「調達仕様書」に記載の要件を満たさない者は失格とする。

（ウ）評価においては、複数の評価者で評価項目ごとに提案内容の審査及び採点を行い、各評価者の評価点の平均を加点とする。

表 3　評価項目の提案区分

提案区分	説明
必須	提案を必須とする評価項目
任意	提案は任意であり、記載がある場合には評価する評価項目

②　評価項目の配点

評価項目は、項目ごとに提案に対する重要度を 3 段階に分け、それぞれ下記「表 4　重要度に基づいた配点」に示す配点とする。

表 4　重要度に基づいた配点

重要度	採点基準	配点
高	評価において重視する項目	400 点
中	有益な提案を期待する項目	200 点
低	上記以外の項目	100 点

③　評価方法

（ア）「評価区分」を「相対」としている評価基準に対する評価方法は、評価項目ごとの配点に対し、採点基準に基づき、5 段階で評価し、下記「表 5　相対評価における採点基準及び得点率」に示す得点率を該当する評価項目の配点に乗算し、算出する。

表 5　相対評価における採点基準及び得点率

評価	採点基準	得点率
A	具体的に記述されており、特に内容が優れている	100%
B	具体的に記述されており、内容が優れている	75%
C	記述の具体性及び内容が平均的な水準である	50%
D	記述の具体性及び内容が平均的な水準に対し劣っている	25%
E	記載が無いまたは評価基準を満たさない	0%

（イ）「評価区分」を「絶対」としている評価基準に対する評価方法は、評価項目ごとの配点に対し、採点基準に基づき、2 段階で評価し、下記「表 6　絶対評価における採点基準及び得点率」に示す得点率を該当する評価項目の配点に乗算し、算出する。

表 6　絶対評価における採点基準及び得点率

評価	採点基準	得点率
A	評価基準を満たしている	100%
F	評価基準を満たしていない	0%

4.5　プレゼンテーション

入札にあたり、責任者（PM）によるプレゼンテーションを実施すること。なお、プレゼンテーションの日程等に関する連絡を主管課から別途行う。

4.6　その他

提案者の提案内容、主管課から提案者に対して、電話等による質問のほか、対面説明または追加資料の提出を求めることがある。

5.　附属文書

別紙　総合評価基準表

以　　上

別紙　総合評価基準表

No.	評価対象	評価項目					評価基準	評価項目種別	提案区分	評価区分		提案重要度	配点	提案書記入欄			評価	得点
		記載文書	項番	大項目	中項目	小項目				相対	絶対			項番	ページ	提案内容の要約		
1	提案書	調達仕様書	2.	調達の概要に関する事項	−	−	調達仕様書に記載の要件全てを実現する旨を明記しているか。	基礎点	必須	−	−	−	−			共通		
2	提案書	調達仕様書	2.2	調達の概要に関する事項	調達の目的	−	本調達の背景、目的及び調達範囲が正確に理解されており、当該事項を踏まえた提案方針が示されているか。	加点	任意	相対	−	中	200			共通		
3	提案書	調達仕様書	2.3.4	調達の概要に関する事項	調達の概要	作業スケジュール	本業務が短期間での構築が必要であることを理解した上で、作業の主体（主管課、関係業者、請負者等）、作業間の依存関係、スケジュール上の留意点、リスク等を考慮したスケジュール（WBS）が示されているか。	加点	任意	相対	−	高	400			共通		
4	提案書	調達仕様書	3.	調達案件及び関連調達案件の調達単位、調達方式等に関する事項	−	−	調達仕様書に記載の要件全てを実現する旨を明記しているか。	基礎点	必須	−	−	−	−			共通		
5	提案書	調達仕様書	4.	作業の実施内容に関する事項	−	−	調達仕様書に記載の要件全てを実現する旨を明記しているか。	基礎点	必須	−	−	−	−			共通		
6	提案書	調達仕様書	4.1	作業の実施内容に関する事項	全体作業管理	−	プロジェクトを管理するための管理項目（進捗、品質等）が具体的に示されており、各管理項目を効果的に管理する手法が示されているか。	加点	任意	相対	−	中	200			共通		
7	提案書	調達仕様書	4.1	作業の実施内容に関する事項	全体作業管理	−	本業務を実施する上で調整が必要となる関係者（関係事業者、現行保守事業者、現行運用事業者、複合機事業者等）が整理されているか。また、関係者間の調整に有用な調整方法が示されているか。	加点	任意	相対	−	低	100			共通		
8	提案書	調達仕様書	4.2.1	作業の実施内容に関する事項	設計・構築に係る作業	設計	設計・構築を効果的に進めるための実施方針及びプロセスが示されており、また設計・構築における課題、リスク及び課題の解決やリスクの低減に効果的な対策が示されているか。	加点	任意	相対	−	高	400			基盤提供		
9	提案書	調達仕様書	4.2.1	作業の実施内容に関する事項	設計・構築に係る作業	設計	各種設計書の文書体系及び各設計書の構成が具体的に示されているか。また、設計の抜け漏れや不整合を生じさせないための効果的な工夫が示されているか。	加点	任意	相対	−	中	200			基盤提供		
10	提案書	調達仕様書	4.2.3	作業の実施内容に関する事項	設計・構築に係る作業	テスト	テスト計画書の記載項目及びテストの関係者が具体的に示されており、テストにおいて故障を効果的に摘出するために有効な対策等が具体的に示されているか。	加点	任意	相対	−	中	200			基盤提供		
11	提案書	調達仕様書	4.2.4	作業の実施内容に関する事項	設計・構築に係る作業	受入テスト支援	受入テストの支援内容が具体的に示されており、受け入れテストでのユーザ負荷の軽減に効果的な対策が具体的に示されているか。	加点	任意	相対	−	中	200			基盤提供		
12	提案書	調達仕様書	4.2.5	作業の実施内容に関する事項	設計・構築に係る作業	情報システムの移行	移行作業の全体像を移行スケジュール等で示した上で、移行方式、作業内容及び留意点が具体的に示されているか。その際は、ユーザの負荷軽減、情報セキュリティ対策、移行漏れ等の移行における課題及びリスクが整理され、課題の解決やリスクの低減に効果的な対策等が示されているか。	加点	任意	相対	−	高	400			基盤提供		
13	提案書	調達仕様書	4.2.6 4.2.7	作業の実施内容に関する事項	設計・構築に係る作業	引継ぎ 教育	円滑な運用開始に向け、引継ぎ及び教育の対象、スケジュール及び実施内容が具体的に示されており、主管課への引継ぎ及び教育をわかりやすく・効率的に実施するための対策等が示されているか。	加点	任意	相対	−	中	200			基盤提供		
14	提案書	調達仕様書	4.3	作業の実施内容に関する事項	保守に係る作業	−	保守の作業内容（特に、障害管理方法及び設定変更等に伴う設計書への反映方法。）が具体的に示されており、環境の維持を誤りなく効率的に行うための効果的な対策等が示されているか。	加点	任意	相対	−	中	200			基盤提供		
15	提案書	調達仕様書	4.3	作業の実施内容に関する事項	保守に係る作業	−	情報の漏洩や不正な侵入等、リモート保守におけるセキュリティ対策についての課題、リスク及び課題の解決やリスクの低減に効果的な対策が示されているか。	加点	任意	相対	−	高	400			基盤提供		
16	提案書	調達仕様書	4.3	作業の実施内容に関する事項	保守に係る作業	−	修正モジュール及びバージョンアップソフトウェアの適用において、適用ミスやデグレードを防ぐ効果的な検証方法が示されているか。	加点	任意	相対	−	中	200			基盤提供		
17	提案書	調達仕様書	4.3.7	作業の実施内容に関する事項	保守に係る作業	リモート監視	監視の対象が整理され、監視内容が具体的に示されているか。また、主に不正プロセス検知において、インシデント発生後に、原因、影響の調査及びその対応を効果的に実施するための工夫が示されているか。	加点	任意	相対	−	中	200			基盤提供		
18	提案書	調達仕様書	4.4	作業の実施内容に関する事項	運用に係る作業	サービスデザイン	運用業務の実施方針及び実施方針を踏まえた運用業務のプロセスが具体的に示されているか。特に、利用者・運用者双方が遠隔地から作業することを想定し、ユーザからの直接受け付け及びテレワーク時のサポートを円滑に実施するための効果的な対策が示されているか。	加点	任意	相対	−	中	200			運用		
19	提案書	調達仕様書	4.4	作業の実施内容に関する事項	運用に係る作業	サービスデザイン/サービストランジション	主管課との円滑なコミュニケーションを行うための取組方針が示されているか。特に、システムへの変更要求における承認ワークフローについて、留意すべき点とそれらを踏まえて効果的な対応策が示されているか。	加点	任意	相対	−	中	200			運用		
20	提案書	調達仕様書	4.4	作業の実施内容に関する事項	運用に係る作業	サービスオペレーション	ログ分析のプロセス、不正プロセスを検知した場合の対応及びログ分析の方法が具体的に示されているか。また、新しい脅威への対応等について有用な提案があるか。	加点	任意	相対	−	中	200			運用		
21	提案書	調達仕様書	4.4	作業の実施内容に関する事項	運用に係る作業	サービスオペレーション	障害対応の作業内容及びプロセスが具体的に示されているか。	加点	任意	相対	−	低	100			運用		

No.	評価対象	評価項目					評価基準	評価項目種別	提案区分	評価区分		提案重要度	配点	提案書記入欄			評価	得点
		記載文書	項番	大項目	中項目	小項目				相対	絶対			項番	ページ	提案内容の要約		
22	提案書	調達仕様書	4.4	作業の実施内容に関する事項	運用に係る作業	その他作業	人事異動に伴う作業について作業内容及びプロセスが具体的に示されているか。	加点	任意	相対	－	低	100			運用		
23	提案書	調達仕様書	4.4	作業の実施内容に関する事項	運用に係る作業	継続的サービス改善	ITILに基づいた継続的な運用改善において、運用上の課題への取組方針及び課題解決のプロセスが示されているか。	加点	任意	相対	－	低	100			運用		
24	提案書	調達仕様書	4.4	作業の実施内容に関する事項	運用に係る作業	運用業務実施上の留意点	運用業務を効率的に実施するために、運用業務を自動化するための検討がなされ、かつ、運用効率や品質の改善に有用な提案が示されているか。	加点	任意	相対	－	中	200			運用		
25	提案書	調達仕様書	4.5	作業の実施内容に関する事項	ホームページ基盤運用に係る作業	－	主管課及びホームページコンテンツ事業者との脆弱性情報の対応状況の共有を迅速に行うことができる仕組みについて、有用な提案が示されているか。	加点	任意	相対	－	中	200			運用		
26	提案書	調達仕様書	5.	成果物の範囲、納品期日等	－	－	調達仕様書に記載の要件全てを実現する旨を明記しているか。	基礎点	必須	－	－	－	－			共通		
27	提案書	調達仕様書	6.	満たすべき要件に関する事項	－	－	調達仕様書に記載の要件全てを実現する旨を明記しているか。	基礎点	必須	－	－	－	－			共通		
28	提案書	調達仕様書	7.	作業の実施体制・方法に関する事項	－	－	調達仕様書に記載の要件全てを実現する旨を明記しているか。	基礎点	必須	－	－	－	－			共通		
29	提案書	調達仕様書	7.	作業の実施体制・方法に関する事項	－	－	設計・構築における体制について本業務の特性を踏まえ、設計・構築時の指示・命令の系統及び主管課、関係事業者等と情報共有を行うための連携図が示されているか。 また、各要員の氏名、所属する組織、保有する資格、業務実績、経験年数、能力、作業、役割分担、本業務への関与度（専任、兼任）及び緊急時の対応が示され、要員選定の根拠が明確に示されているか。	加点	任意	相対	－	高	400			基盤提供		
30	提案書	調達仕様書	7.	作業の実施体制・方法に関する事項	－	－	運用・保守における体制について本業務の特性を踏まえ、保守・運用時の指示・命令の系統及び主管課、関係事業者等と情報共有を行うための連携図が示されているか。 また、各要員の氏名、所属する組織、保有する資格、業務実績、経験年数、能力、作業、役割分担、本業務への関与度（専任、兼任）及び緊急時の対応が示され、要員選定の根拠が明確に示されているか。	加点	任意	相対	－	高	400			運用		
31	提案書	調達仕様書	8.	作業の実施に当たっての遵守事項	－	－	調達仕様書に記載の要件全てを実現する旨を明記しているか。	基礎点	必須	－	－	－	－			共通		
32	提案書	調達仕様書	9.	成果物の取扱いに関する事項	－	－	調達仕様書に記載の要件全てを実現する旨を明記しているか。	基礎点	必須	－	－	－	－			共通		
33	提案書	調達仕様書	10.	入札参加資格に関する事	－	－	調達仕様書に記載の要件全てを実現する旨を明記しているか。	基礎点	必須	－	－	－	－			共通		
34	提案書	調達仕様書	11.	再委託に関する事項	－	－	調達仕様書に記載の要件全てを実現する旨を明記しているか。	基礎点	必須	－	－	－	－			共通		
35	提案書	調達仕様書	12.	その他特記事項	－	－	調達仕様書に記載の要件全てを実現する旨を明記しているか。	基礎点	必須	－	－	－	－			共通		
36	提案書	要件定義書	1.	機能要件	－	－	要件定義書に記載の要件全てを満たしていることを確認できる情報を明記しているか。	基礎点	必須	－	－	－	－			基盤提供		
37	提案書	要件定義書	1.1.1	機能要件	ユーザ提供機能	メール	「要件定義書-1.1.1②メール無害化及び誤送信防止」を実現するにあたり、複数のメールアドレスを持つユーザがログインし利用する運用を想定した上で、ユーザ及び運用管理の観点で利便性が向上する仕組みとなっているか。	加点	任意	相対	－	中	200			基盤提供		
38	提案書	要件定義書	1.1.4	機能要件	ユーザ提供機能	テレワーク	「要件定義書-1.1.4①インターネットからのリモートアクセス」を実現するにあたり、より利便性や可用性が高いサービスを選定しているか。 また、一人のリモートユーザが複数のデバイスを保有している場合でも追加ライセンスが不要で同時に接続できるサービスを選定しているか。	加点	任意	相対	－	中	200			基盤提供		
39	提案書	要件定義書	1.1.4	機能要件	ユーザ提供機能	テレワーク	「要件定義書-1.1.4③テレワーク用端末」は、テレワーク時のオンライン会議の通信をインターネットブレイクアウトできるソフトウェア・ハードウェアの構成となっているか。	加点	任意	－	絶対	中	200			基盤提供		
40	提案書	要件定義書	1.1.5	機能要件	ユーザ提供機能	リモートアクセス	「要件定義書-1.1.5リモートアクセス」を実現するにあたり、大容量のファイルが扱える構成となっているか。また、1.99GBを超える容量のファイルのアップロードが行える手段が示されているか。	加点	任意	相対	－	中	200			基盤提供		
41	提案書	要件定義書	1.1.7	機能要件	ユーザ提供機能	在席管理及びWeb会議	テレワークでの利用を踏まえ、職員が出勤しているのか、テレワークしているのかを、PCの接続元のネットワークに応じて自動的に取得し、画面に表示する機能を有しているか。	加点	任意	－	絶対	高	400			基盤提供		
42	提案書	要件定義書	1.1.11	機能要件	ユーザ提供機能	申請のオンライン受付及び各種運用手続きのワークフロー管理	既存で作成した申請書の移行について、運用方法の改善などの有用な提案があるか。	加点	任意	相対	－	高	400			基盤提供		

No.	評価対象	評価項目					評価基準	評価項目種別	提案区分	評価区分		提案重要度	配点	提案書記入欄			評価	得点
		記載文書	項番	大項目	中項目	小項目				相対	絶対			項番	ページ	提案内容の要約		
43	提案書	要件定義書	1.2.1	機能要件	システム運用機能	仮想化基盤管理	「要件定義書-1.2.1仮想化基盤管理」を実現するにあたり、仮想化マシンのリソース使用状況や仮想化基盤のキャパシティから適切なリソース割り当てを効率的に実現できる構成が示されているか。また、仮想デスクトップ基盤を含めた仮想化基盤の管理を効率的に実現できる構成が示されているか。	加点	任意	相対	-	中	200			基盤提供		
44	提案書	要件定義書	1.2.2	機能要件	システム運用機能	構成管理	「要件定義書-1.2.2構成管理」を実現するにあたり、Windows/Linux双方の管理対象とする機器（サーバ・PC等）の初期セットアップを効率的に実現できる構成が示されているか。	加点	任意	相対	-	中	200			基盤提供		
45	提案書	要件定義書	1.2.3	機能要件	システム運用機能	ログ取得・管理	「要件定義書-1.2.3ログ取得・管理」を実現するにあたり、対象となるログの収集から分析までを効率的に実現できる構成が示されているか。また、運用期間中において、必要に応じて対象ログの追加等を行った際、ルール及びアラートを見直すことが示されているか。 これに加え、仮想化基盤全体が喪失した場合に備えた対策を提案しているか。	加点	任意	相対	-	高	400			基盤提供		
46	提案書	要件定義書	1.2.4	機能要件	システム運用機能	監視	構築時の誤検知及び過検知への対処の方法が効果及び根拠と共に示されているか。また、運用期間中、同様のチューニングを実施することが示されているか。	加点	任意	相対	-	高	400			基盤提供		
47	提案書	要件定義書	1.2.5	機能要件	システム運用機能	バックアップ	「要件定義書-1.2.5バックアップ」を実現するにあたり、性能面、費用面及びランサムウェア等の脅威に対するセキュリティ面において、効果及び根拠と共に適切な構成が示されているか。	加点	任意	相対	-	高	400			基盤提供		
48	提案書	要件定義書	1.2.6	機能要件	システム運用機能	特権ID管理	特権ID管理において、最近の脅威を考慮した検討がなされているか。また、その際に実施するセキュリティ保護を行うために効果的な手法が示されているか。	加点	任意	相対	-	中	200			基盤提供		
49	提案書	要件定義書	1.2.7	機能要件	システム運用機能	アカウント管理	「要件定義書-1.2.7アカウント管理」について、アカウント管理の対象として、以下が含まれていることが示されているか。 ・「11.2.1①(ク)(20)ワンタイムパスワード認証サーバ」 ・JP1/Automatic Job Management System3	加点	任意	-	絶対	高	400			基盤提供		
50	提案書	要件定義書	1.2.8	機能要件	システム運用機能	シングルサインオン	「要件定義書-1.2.8シングルサインオン」を実現するにあたり、複数のオンプレミス及びWebシステムへの対応ができる構成であり、その実現方法や、そのシステム数の上限の制約が示されているか。	加点	任意	-	絶対	高	400			基盤提供		
51	提案書	要件定義書	1.2.9	機能要件	システム運用機能	DNS	コンテンツDNS及びキャッシュDNSにおいてDNSSECを実装する旨が示されているか。	加点	任意	-	絶対	中	200			基盤提供		
52	提案書	要件定義書	1.3.1	機能要件	情報セキュリティ機能	主体認証	「要件定義書-1.3.1主体認証」を実現するにあたり、利用するディレクトリサービス、ICカード認証、ワンタイムパスワード認証等の連携の仕組みを含めた構成が具体的に示されているか。その際、ICカード認証やワンタイムパスワード認証が適用できる範囲が具体的に示されているか。 また、その際、ワンタイムパスワード認証がWindowsログオンにおいても使用可能なソフトウェアが提供されることが示されているか。	加点	任意	相対	-	中	200			基盤提供		
53	提案書	要件定義書	1.3.2	機能要件	情報セキュリティ機能	仮想ブラウザ	「要件定義書-1.3.2仮想ブラウザ」を実現するにあたり、その具体的な構成が示されているか。その際、ユーザ毎のプロファイルの破損やプロファイルの読み込み速度の問題が発生しにくい仕組みが効果及び根拠と共に示されているか。	加点	任意	相対	-	高	400			基盤提供		
54	提案書	要件定義書	1.3.3	機能要件	情報セキュリティ機能	ファイル転送及びファイル無害化	「要件定義書-1.3.3ファイル転送及びファイル無害化」を実現するにあたり、必要な機器の構成、台数、ライセンス数等の具体的な構成が示されているか。また、ユーザがファイル転送及びファイル無害化を実施する際、使いやすくするための対策が示されているか。	加点	任意	相対	-	中	200			基盤提供		
55	提案書	要件定義書	1.3.4	機能要件	情報セキュリティ機能	エンドポイントマルウェア対策	「要件定義書-1.3.4エンドポイントマルウェア対策」を実現するにあたり、必要な構成が示されているか。その際、選定した製品の構成の有効性が効果及び根拠と共に示されているか。	加点	任意	相対	-	中	200			基盤提供		
56	提案書	要件定義書	1.3.6	機能要件	情報セキュリティ機能	不正プロセス検知	「要件定義書-1.3.6不正プロセス検知」を実現するにあたり、必要な構成が示されているか。その際、選定した製品の構成の有効性が示されているか。	加点	任意	相対	-	低	100			基盤提供		
57	提案書	要件定義書	1.3.8	機能要件	情報セキュリティ機能	メールセキュリティ対策	「要件定義書-1.3.8メールセキュリティ対策」を実現するにあたり、必要な構成が示されているか。その際、選定した製品の構成の有効性が示されているか。	加点	任意	相対	-	中	200			基盤提供		
58	提案書	要件定義書	1.3.9	機能要件	情報セキュリティ機能	Webセキュリティ対策	「要件定義書-1.3.9①セキュアWebゲートウェイ(SWG)」、「要件定義書-1.3.9③サンドボックス」及び「要件定義書-1.3.9④不正侵入防止」を実現するにあたり、必要な構成が示されているか。その際、選定した製品の有効性が効果及び根拠と共に示されているか。	加点	任意	相対	-	高	400			基盤提供		
59	提案書	要件定義書	1.3.9	機能要件	情報セキュリティ機能	Webセキュリティ対策	「要件定義書-1.3.9②クラウドアクセスセキュリティ（CASB）」を実現するにあたり、必要な構成が示されているか。その際、選定した製品の有効性が効果及び根拠と共に示されているか。	加点	任意	相対	-	高	400			基盤提供		
60	提案書	要件定義書	1.3.10	機能要件	情報セキュリティ機能	脆弱性検査ツール	「要件定義書-1.3.10脆弱性検査ツール」を実現するにあたり、必要な構成が示されているか。その際、選定した製品の有効性が示されているか。	加点	任意	相対	-	中	200			基盤提供		
61	提案書	要件定義書	2.	ユーザビリティ及びアクセシビリティに関する事項	-	-	要件定義書に記載の要件全てを実現する旨を明記しているか。	基礎点	必須	-	-	-	-			基盤提供		
62	提案書	要件定義書	3.	システム方式に関する事項	-	-	要件定義書に記載の要件全てを満たしていることを確認できる情報を明記しているか。	基礎点	必須	-	-	-	-			基盤提供		

No.	評価対象	評価項目					評価基準	評価項目種別	提案区分	評価区分		提案重要度	配点	提案書記入欄			評価	得点
		記載文書	項番	大項目	中項目	小項目				相対	絶対			項番	ページ	提案内容の要約		
63	提案書	要件定義書	3.1	システム方式に関する事項	情報システムの構成に関する全体の方針	-	バックアップデータセンターに導入する機器及びその他の同一種類の機器について、ベンダ、製品のシリーズ等が統一されていることが示されているか。 または、理由があり統一しない箇所について明確にし、有用であることが示されているか。	加点	任意	相対	-	中	200			基盤提供		
64	提案書	要件定義書	3.1	システム方式に関する事項	情報システムの構成に関する全体の方針	-	サーバに搭載するCPUにおいて、指定したCPUより新しいCPUが発表された場合は、コア数とクロック数が同数以上の後継機種が選定されているか。	加点	任意	-	絶対	低	100			基盤提供		
65	提案書	要件定義書	3.1	システム方式に関する事項	情報システムの構成に関する全体の方針	サポート	システムの基盤となるネットワーク仮想化、仮想デスクトップ及びアプリケーション仮想化について、提供元のベンダまたはベンダが認定する技術者による技術サポートを行う体制が示されており、また、業務停止等の重篤な障害が発生した際には、回避策の提示だけでなく、障害発生の根本原因調査を行うことが示されているか。	加点	任意	相対	-	高	400			基盤提供		
66	提案書	要件定義書	3.1	システム方式に関する事項	情報システムの構成に関する全体の方針	サポート	マイクロソフト製品について、移行、設計及び構築支援を実施する際、コンサルティングサービスによるサポートや構築実施を行う体制が示されているか。	加点	任意	-	絶対	中	200			基盤提供		
67	提案書	要件定義書	4.	性能に関する事項	-	-	要件定義書に記載の要件全てを実現する旨を明記しているか。	基礎点	必須	-	-	-	-			基盤提供		
68	提案書	要件定義書	5.	信頼性に関する事項	-	-	要件定義書に記載の要件全てを満たしていることを確認できる情報を明記しているか。	基礎点	必須	-	-	-	-			基盤提供		
69	提案書	要件定義書	6.	拡張性に関する事項	-	-	要件定義書に記載の要件全てを満たしていることを確認できる情報を明記しているか。	基礎点	必須	-	-	-	-			基盤提供		
70	提案書	要件定義書	7.	上位互換性に関する事項	-	-	要件定義書に記載の要件全てを実現する旨を明記しているか。	基礎点	必須	-	-	-	-			基盤提供		
71	提案書	要件定義書	8.	中立性に関する事項	-	-	要件定義書に記載の要件全てを満たしていることを確認できる情報を明記しているか。	基礎点	必須	-	-	-	-			基盤提供		
72	提案書	要件定義書	9.	継続性に関する事項	-	-	要件定義書に記載の要件全てを満たしていることを確認できる情報を明記しているか。	基礎点	必須	-	-	-	-			基盤提供		
73	提案書	要件定義書	10.	情報セキュリティに関する事項	-	-	要件定義書に記載の要件全てを実現する旨を明記しているか。	基礎点	必須	-	-	-	-			基盤提供		
74	提案書	要件定義書	10.	情報セキュリティに関する事項	-	-	令和5年に改定された統一基準群の改定内容を理解した上で、次期情報システム基盤において想定される脅威及びセキュリティリスクが整理され、効果及び根拠と共にその対応策が示されているか。	加点	任意	相対	-	高	400			基盤提供		
75	提案書	要件定義書	11.	情報システム稼働環境要件	-	-	要件定義書に記載の要件全てを満たしていることを確認できる情報を明記しているか。	基礎点	必須	-	-	-	-			基盤提供		
76	提案書	要件定義書	11.1	情報システム稼働環境要件	ネットワーク構成要件	-	調達機器の選定理由が明確に示された上で、ユーザの利便性、情報セキュリティ及び運用を考慮したシステム構成（ネットワーク構成を含む。）が効果及び根拠と共に示されているか。	加点	任意	相対	-	高	400			基盤提供		
77	提案書	要件定義書	11.2.1	情報システム稼働環境要件	メインデータセンター設置機器要件	サーバ要件	以下について、事前検証の結果が示され、検証結果を踏まえた設計内容が示されているか。 ・「要件定義書-11.2.1②(キ)(2)シングルサインオンサーバ」構築における実現性 ・「要件定義書-11.2.1サーバ要件①(ク)(31)外部電磁的記録装置管理サーバ」構築における実現性	加点	任意	-	絶対	高	400			基盤提供		
78	提案書	要件定義書	11.2.1	情報システム稼働環境要件	メインデータセンター設置機器要件	サーバ要件	「要件定義書-11.2.①(ク)(14)プリントサーバ」において、可用性を確保するため、冗長構成をとる構成が示されているか。	加点	任意	-	絶対	中	200			基盤提供		
79	提案書	要件定義書	11.2.1	情報システム稼働環境要件	メインデータセンター設置機器要件	サーバ要件	「要件定義書-11.2.1⑤仮想PC（RDSH）用仮想化基盤」、「11.2.1⑥仮想PC（VDI）用仮想化基盤」及び「要件定義書-11.2.1⑦集計業務用PC用仮想化基盤」の実現において、仮想PCを実現する有用な提案がなされているか。また、その効果及び根拠が示されているか。	加点	任意	相対	-	高	400			基盤提供		
80	提案書	要件定義書	11.2.1	情報システム稼働環境要件	メインデータセンター設置機器要件	サーバ要件	本調達で導入する仮想化基盤について、CPUの追加による性能の拡張が可能な構成である対象が明確に示されているか。 拡張可能でない場合、初期導入時以上の性能が必要となった際に性能を拡張するため対策が提案されているか。	加点	任意	相対	-	高	400			基盤提供		
81	提案書	要件定義書	11.2.2	情報システム稼働環境要件	メインデータセンター設置機器要件	ストレージ要件	「要件定義書-11.2.2①メインストレージ」の実現において、可能な限り冗長化した構成が効果及び根拠と共に示されているか。また、コントローラ障害時における性能劣化への対策を行っているか。	加点	任意	相対	-	高	400			基盤提供		
82	提案書	要件定義書	11.2.2	情報システム稼働環境要件	メインデータセンター設置機器要件	ストレージ要件	「要件定義書-11.2.2①メインストレージ」を実現するにあたり、ストレージのキャパシティ予測及びランサムウェア等の脅威に対するセキュリティ対策において有効な機能を有していることが効果及び根拠と共に示されているか。	加点	任意	相対	-	高	400			基盤提供		
83	提案書	要件定義書	11.2.2	情報システム稼働環境要件	メインデータセンター設置機器要件	ストレージ要件	「要件定義書-11.2.2①メインストレージ」を実現するにあたり、コスト面や保守性において有効な保守サービスが提供されることが効果及び根拠と共に示されているか。	加点	任意	相対	-	高	400			基盤提供		

No.	評価対象	評価項目					評価基準	評価項目種別	提案区分	評価区分		提案重要度	配点	提案書記入欄			評価	得点
		記載文書	項番	大項目	中項目	小項目				相対	絶対			項番	ページ	提案内容の要約		
84	提案書	要件定義書	11.2.3	情報システム稼働環境要件	メインデータセンター設置機器要件	ネットワーク機器要件	「要件定義書-11.2.3ネットワーク機器要件」及び「要件定義書-11.4.3ネットワーク機器要件」を実現するにあたり、ネットワーク仮想化により、仮想マシン間の通信の効率化及びネットワーク機器の仮想化を実現する構成が示されているか。	加点	任意	-	絶対	高	400			基盤提供		
85	提案書	要件定義書	11.2.4	情報システム稼働環境要件	メインデータセンター設置機器要件	PC要件	本調達で導入するノート型PCが軽量であることが示されているか。	加点	任意	相対	-	中	200			基盤提供		
86	提案書	要件定義書	11.3.1	情報システム稼働環境要件	統計センター設置機器要件	ネットワーク機器要件	既存機器との並行稼働について、その課題とリスク及び課題の解決やリスクの低減に効果的な対策が示されているか。	加点	任意	相対	-	高	400			基盤提供		
87	提案書	要件定義書	11.3.3	情報システム稼働環境要件	統計センター設置機器要件	PC要件	情報システム基盤停止時においても運用管理端末へのログイン及び設計書等の確認が行えるようにする仕組みの実現方法が示されているか。	加点	任意	-	絶対	中	200			基盤提供		
88	提案書	要件定義書	11.3.3	情報システム稼働環境要件	統計センター設置機器要件	PC要件	シンクライアント及び機密性3情報持出専用端末の実現方法が示されているか。	加点	任意	-	絶対	中	200			基盤提供		
89	提案書	要件定義書	11.3.6	情報システム稼働環境要件	統計センター設置機器要件	施設・設備要件	メインデータセンターの設備環境が示され、統計センターにとって有用な提案となっているか。	加点	任意	相対	-	中	200			基盤提供		
90	提案書	要件定義書	11.4	バックアップデータセンター設置機器要件	-	-	遠隔地バックアップについて、具体的な方法が示されているか。	加点	任意	相対	-	低	100			基盤提供		
91	提案書	要件定義書	11.4.6	情報システム稼働環境要件	バックアップデータセンター設置機器要件	施設・設備要件	バックアップデータセンターの設備環境が示され、統計センターにとって有用な提案となっているか。	加点	任意	相対	-	中	200			基盤提供		
92	提案書	要件定義書	11.7	情報システム稼働環境要件	通信回線等要件	-	「要件定義書-11.7通信回線等要件」の実現において、通信回線の諸元が根拠とともに示され、統計センターにとって有用な提案となっているか。 また、インターネット接続回線2（テレワーク用）の帯域が不足した場合に、バックアップデータセンター経由で接続する等の帯域増強の対策が示されているか。	加点	任意	相対	-	中	200			基盤提供		
93	提案書	要件定義書	11.8.1	情報システム稼働環境要件	ホームページ基盤要件	クラウド要件	ホームページ基盤として利用するクラウドサービスを選定するにあたって、比較・評価した項目が具体的に示されているか、また、当該サービスを選定した理由が明確に示されているか。	加点	任意	相対	-	中	200			基盤提供		
94	提案書	-	-	追加提案	-	-	その他、本調達において有用な提案が示されているか。	加点	任意	相対	-	高	400			共通		
95	プレゼンテーション	-	-	プレゼンテーション	-	-	①経験、知識、コミュニケーション能力、責任感及び強いコミットメントが確認でき、適任であると論理的に判断できる。 ②質疑に対し、誠実、かつ、根拠を持った分かりやすい回答ができていると論理的に判断できる。	加点	任意	相対	-	高	400			共通		

No.	評価対象	評価項目					評価基準	評価項目種別	提案区分	評価区分		提案重要度	配点	提案書記入欄			評価	得点
		記載文書	項番	大項目	中項目	小項目				相対	絶対			項番	ページ	提案内容の要約		
96	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、プラチナえるぼし認定企業）】 プラチナえるぼし（＊1）1100点 えるぼし3段階目（＊2）880点 えるぼし2段階目（＊2）660点 えるぼし1段階目（＊2）440点 行動計画（＊3）220点 【次世代法に基づく認定（くるみん認定企業、トライくるみん認定企業、プラチナくるみん認定企業）】 プラチナくるみん（＊4）1100点 くるみん（令和4年4月1日以降の基準（＊5））660点 くるみん（平成29年4月1日～令和4年3月31日までの基準（＊6））660点 トライくるみん（＊7）660点 くるみん（平成29年3月31日までの基準（＊8））440点 【若者雇用促進法に基づく認定（ユースエール認定企業）】 ユースエール認定企業880点 ※（ワーク・ライフ・バランス等の推進に関する指標について） 複数の認定等に該当する場合は、最も配分が高い区分（認定）より加点を行なうものとする。 ＊1 女性の職業生活における活躍の推進に関する法律等の一部を改正する法律（令和元年法第24号）による改正後の女性活躍推進法第12条の規定に基づく認定 ＊2 女性活躍推進法第9条の規定に基づく認定（労働時間等の働き方に係る基準は満たすことが必要） ＊3 常時雇用する労働者の数が100人以下の事業主に限る （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）。 ＊4 次世代法第15条の2の規定に基づく認定 ＊5 次世代法第13条の規定に基づく認定のうち、次世代育成支援対策推進法施行規則の一部を改正する省令（令和3年厚生労働省令第185号。以下「令和3年改正省令」という。）による改正後の次世代育成支援対策推進法施行規則（以下「新施行規則」という。）第4条第1項第1号及び第2号の規定に基づく認定 ＊6 次世代法第13条の規定に基づく認定のうち、令和3年改正省令による改正前の次世代育成支援対策推進法施行規則第4条又は令和3年改正省令附則第2条第2項の規定に基づく認定（ただし、＊8の認定を除く。） ＊7 次世代法第13条の規定に基づく認定のうち、新施行規則第4条第1項第3号及び第4号の規定に基づく認定 ＊8 次世代法第13条の規定に基づく認定のうち、次世代育成支援対策推進法施行規則等の一部を改正する省令（平成29年厚生労働省令第31号。以下「平成29年改正省令」という。）による改正前の次世代育成支援対策推進法施行規則第4条又は平成29年改正省令附則第2条第3項の規定に基づく認定	加点	任意	-	絶対	※	1100			共通		
98	マイナンバーカードの利活用等に関する指標	－	－	－	－	－	【公的個人認証及び電子入札の推進に関する指標】 認定事業者（＊9）700点 ※（マイナンバーカードの利活用等に関する指標について） ＊9 電子署名等に係る地方公共団体情報システム機構の認証業務に関する法律（平成14年法律第153号。以下「公的個人認証法」という。）第17条第1項第4号、第5号若しくは第6号の規定に該当する事業者であって、同条第4項に規定する取り決めを地方公共団体情報システム機構と締結した事業者又は電子署名等に係る地方公共団体情報システム機構の認証業務に関する法律施行規則（平成15年総務省令第120号）第29条第1項の定めにより、総務大臣の認定を受けたものとみなされた事業者	加点	任意	－	絶対	※	700			共通		
								基礎点	400	総計 （基礎点+加点）			21,900					
								加点	21,500									

既存資料閲覧要領

１ 資料の閲覧

入札に参加を希望する者は応札前までに、本調達の仕様を理解するため、必ず「２ 閲覧資料」で示す資料を、主管課が指定した場所にて閲覧し理解すること。また、提案するにあたり必要となる事項について主管課の説明を受け、内容を把握すること。

なお、提案時に必要な書類の一部として、その実施記録を提出すること。

２ 閲覧資料

本件調達に係る閲覧資料は以下のとおり。
なお、閲覧は応札を前提に付録の誓約書を提出した者に限る。

1	現行情報システム基盤の設計書
2	現有ソフトウェア一覧
3	現行情報システム基盤の運用業務に関する報告資料
4	運用管理規則
5	情報セキュリティポリシー

３ 閲覧方法

閲覧を希望する者は、入札公告期間中（土曜日、日曜日、国民の祝日及び年末年始（12月29日から1月3日）を除く午前９時30分から午後６時00分まで）に事前連絡の上、下記の場所において閲覧すること。

なお、閲覧の際には、付録の誓約書を提出すること。

【閲覧場所】

独立行政法人統計センター　情報システム部情報システム基盤課

付録

入札関係資料閲覧に関する誓約書

独立行政法人　統計センター理事長　殿

＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿（以下「弊社」という。）は、このたび、独立行政法人統計センター（以下「貴法人」という。）の行う「独立行政法人統計センター情報システム基盤の構築及びサービス提供業務」の入札（以下「本入札」という。）に関する資料閲覧に関し、下記事項を誓約いたします。

第１条（守秘義務の誓約）
弊社は貴法人の許可なくして、社外はもちろん貴法人職員で本件に直接関与していない者に対しても、本入札に関し弊社が知り得た全ての事項・情報を開示、漏洩し、若しくは自ら使用しないことを約束いたします。

第２条（資料複写の禁止等）
弊社は、守秘義務を厳守するため、貴法人より本入札に関し、開示された資料一切の複写をしないことを約束し、貴法人より返還を要求された場合、これらの資料及びそのコピー並びにそれらに関する資料の一切を直ちに返還することを約束いたします。

第３条（入札後の守秘義務）
弊社は、貴法人において本入札が行われた後といえども、第１条記載の事項・情報を開示、漏洩若しくは使用しないことを約束いたします。

第４条（守秘義務違反後の処置）
弊社は、貴法人とお約束した守秘義務に反した場合、貴法人が行う合法的処置を受けることを約束いたします。

第５条（資料閲覧時の立会い及び監視カメラでの撮影）
弊社は、資料閲覧中の立会い及び監視カメラでの撮影に同意いたします。

令和　　年　月　日

住所＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿
会社名＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿
代表者名＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿
本件責任者(役職及び氏名)＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿
担当者(役職及び氏名)＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿
電話番号＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿
Mail＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿