契約番号：	135-021
	135-022
	135-023
	135-024
	151-076

入　札　公　告

次のとおり一般競争入札に付します。

記

１．競争入札に付する事項
（１）入 札 件 名：「第2期基盤情報システムの構築及び移行業務」
（２）仕　　様：入札説明書による。
（３）数　　量：一式
（４）作 業 期 間：契約締結日から２０２６年　３月３１日
（５）作 業 場 所：別途仕様書指定場所

２．必要書類等の提出場所等
（１）契約事項を示す場所及び入札説明書を交付する場所
郵 便 番 号：１１０－００１５
所　在　地：東京都台東区東上野一丁目２８番９号　キクヤビル３階
機　関　名：公益財団法人核物質管理センター
担 当 部 署：総務部　契約課
フ リ ガ ナ：イイズミ　ジュンコ
担 当 者 名：飯泉　順子
電 話 番 号：０３－５８１６－７７６５
Ｆ　Ａ　Ｘ：０３－３８３４－５２６５
Ｍ ａ ｉ ｌ：keiyaku－info@jnmcc. or. jp
交 付 方 法：センターホームページ内「調達情報」よりダウンロードすること。
（２）入札説明書のダウンロード可能期間
２０２５年　２月２８日（金）～ ２０２５年　３月１９日（水）　午後５時まで
（３）質問書提出期限（本入札に参加するには、期限までに質問書を提出すること）
２０２５年　３月２４日（月）　午後４時まで
公益財団法人核物質管理センター　東京本部
総務部　契約課　必着（ＦＡＸ・電子メール可）
なお、質疑がない場合でも、その旨を記載し提出すること。
（４）提案書等の提出期限
２０２５年　３月３１日（月）　午後４時まで
公益財団法人核物質管理センター　東京本部　総務部　契約課　必着（郵送可）
なお、提案書を郵送する場合、書留郵便若しくは配達記録が残るようにすること。
（５）プレゼンテーションの日時及び場所
①日　時
別途指定する。
②場　所
東京都台東区東上野１丁目２８番９号　キクヤビル６階
公益財団法人核物質管理センター　東京本部　６階大会議室

（６） 入札及び開札の日時及び場所
２０２５年　５月２１日（水）　午後１時３０分
公益財団法人核物質管理センター　東京本部　６Ｆ大会議室
なお、入札書を郵送する場合、書留郵便若しくは配達記録が残るように、東京本部総務部　契約課まで　２０２５年　５月２０日（火）　午後５時必着とする。

３．入札方法
（１） 本件は総合評価落札方式による入札のため、提案書を提出し審査を受けなければならない。
（２） ２０２５年度に実施する構築移行業務に係る請負金額一式とする。
（３） 落札決定にあたっては、入札書に記載された金額（非課税分を除く）に当該金額の10パーセント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、その端数を切り捨てる。）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業者か免税業者であるかを問わず、見積もった契約金額の110分の100に相当する金額を入札書に記載すること。

４．競争入札に参加する者に必要な資格
（１）次の①～⑤に該当する者は入札に参加することができない。
①成年被後見人
②未成年者、被保佐人及び被補助人（契約締結のための必要な同意を得ている場合は除く。）
③破産者で復権を得ない者
④競争に参加することを妨げ、又は契約の締結もしくは履行を妨げ、公序良俗に違反した者であって、その事実があった後２年を経過しない者（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、同様とする。）
⑤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又は同法第２条第６号に規定する暴力団員もしくはこれらと関係する者
（２）２０２５年度　国・地方公共団体等における競争参加資格（東北、関東・甲信越）の「役務の提供等」の資格を有すると認められた者

５．入札保証金
免除する。

６．入札の無効
入札参加資格のない者のした入札及び入札に関する条件に違反した入札は無効とする。

７．契約書作成の要否
契約締結にあっては、契約書を作成するものとする。

８．落札者の決定方法
予定価格の制限の範囲内で、契約担当者が入札説明書で必須とした項目の最低限の要求要件をすべて満たしている提案をした入札者の中から、センターが定める総合評価の方法をもって落札者を決定する。

９．その他
詳細については、入札説明書による。

２０２５年　２月２８日

公益財団法人核物質管理センター
総務部長　猪　狩　　和

契約番号:	135-021
	135-022
	135-023
	135-024
	151-076

入 札 説 明 書

一般競争入札の詳細は下記のとおりとする。

記

1．競争入札に付する事項
（1）入 札 件 名: 「第2期基盤情報システムの構築及び移行業務」
（2）仕　　様: 仕様書による。
（3）数　　量: 一式
（4）作 業 期 間: 契約締結日から２０２６年　3月３１日
（5）作 業 場 所: 別途仕様書指定場所

2．必要書類等の提出場所等
（1）契約事項を示す場所及び提出場所等
郵 便 番 号：１１０－００１５
所　在　地：東京都台東区東上野一丁目２８番９号　キクヤビル３階
機　関　名：公益財団法人核物質管理センター
担 当 部 署：総務部　契約課
フ リ ガ ナ：イイズミ　ジュンコ
担 当 者 名：飯泉　順子
電 話 番 号：０３－５８１６－７７６５
Ｆ　Ａ　Ｘ：０３－３８３４－５２６５
Ｍ ａ ｉ ｌ：keiyaku－info@jnmcc. or. jp
（2）質問書提出期限（本入札に参加するには、期限までに質問書を提出すること）
２０２５年　3月２４日（月）　午後４時まで
公益財団法人核物質管理センター　東京本部
総務部　契約課　必着（ＦＡＸ・電子メール可）
なお、質疑がない場合でも、その旨を記載し提出すること。
（3）提案書等の提出期限（11. その他（１）②に示す書類）
２０２５年　3月３１日（月）　午後４時まで
公益財団法人核物質管理センター　東京本部　総務部　契約課　必着（郵送可）
なお、提案書を郵送する場合、書留郵便若しくは配達記録が残るようにすること。
（4）プレゼンテーションの日時及び場所
① 日　時
別途指定する。
② 場　所
東京都台東区東上野１丁目２８番９号　キクヤビル６階
公益財団法人核物質管理センター　東京本部　６階大会議室
（5）入札及び開札の日時及び場所
２０２５年　5月２１日（水）　午後１時３０分
公益財団法人核物質管理センター　東京本部　６Ｆ大会議室
なお、入札書を郵送する場合、書留郵便若しくは配達記録が残るように、東京本部総務部　契約課まで　２０２５年　5月２０日（火）　午後５時必着とする。

３．入札方法

（１） 本件は総合評価落札方式による入札のため、提案書を提出し審査を受けなければならない。

（２） ２０２５年度に実施する構築移行業務に係る請負金額一式とする。

（３） 落札決定にあたっては、入札書に記載された金額（非課税分を除く）に当該金額の10パーセント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、その端数を切り捨てる。）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業者か免税業者であるかを問わず、見積もった契約金額の110分の100に相当する金額を入札書に記載すること。

４．競争入札に参加する者に必要な資格

（１）次の①～⑤に該当する者は入札に参加することができない。

①成年被後見人

②未成年者、被保佐人及び被補助人（契約締結のための必要な同意を得ている場合は除く。）

③破産者で復権を得ない者

④競争に参加することを妨げ、又は契約の締結もしくは履行を妨げ、公序良俗に違反した者であって、その事実があった後２年を経過しない者（代理人、支配人、その他のとして使用する者についても、同様とする。）

⑤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又は同法第２条第６号に規定する暴力団員もしくはこれらと関係する者

（２） ２０２５年度　国・地方公共団体等における競争参加資格（東北、関東・甲信越）の「役務の提供等」の資格を有すると認められた者

５．入札保証金

免除する。

６．提案書の審査

提出された提案書は契約担当者において審査し、採用し得ると判断した提案書を提出した者のみ落札決定の対象とする。

７．入札及び開札

（１）入札は契約の申込みとして取り扱う。

（２）代理人又は復代理人（以下「代理人」という。）が入札する場合は、入札書（参考資料２）に、代表者の氏名（年間委任状が提出されている場合は当該代理人の氏名）及び法人名称もしくは商号、代理人であることの表示並びに当該代理人の氏名を記入して押印をしておくとともに、その者に対する委任状（参考資料１）その他これに準ずる書類をもって代理権のあることを証明するものとし、入札書と同時に提出することとする。

（３）入札書の記載方法

入札は、すべて入札書で行う。入札書は横書、楷書で明確に記載し、数字はアラビア数字を用いて作成したうえ、封かんし、封皮には、自己の氏名（法人の場合はその名称又は商号）及び「何月何日開札、＿＿＿＿の入札書在中」と記入しなければならない。

郵便により提出するときは、二重封筒とし、入札書を中封筒に入れて密封のうえ当該中封筒の封皮には直接提出する場合と同様に氏名等を記入し、外封筒の封皮には、「何月何日開札、＿＿＿＿の入札書在中」と記入しなければならい。

（４）代表者（年間委任状による受任者を含む）又は、その代理人（以下「競争入札参加者等」という。）は、入札書の記載事項を訂正する場合は、当該訂正部分について押印をしておかなければばらない。

（５）競争入札参加者等は、その提出した入札書の差換え、変更、又は、取消をすることができない。

（６）開札は、第２項第５号に掲げる日時及び場所で競争入札参加者等の立会いのもとに行うものとする。

（７）競争入札参加者等が開札に立会わないときは、入札事務に関係のないセンター職員を立会わせて行うものとする。

（８）競争入札参加者等が開札現場において、次の①～③に該当する行為があると認められたときは、入札から排除する。
①入札に際し、不当に価格を競り上げ、又は競り下げる目的をもって連合した者
②入札に参加することを妨げた者
③入札事務担当者の職務の執行を妨げた者
（９）競争入札参加者等は、開札時刻後において、入札現場に入場することができない。
（10）競争入札参加者等は、契約担当者が特に止むを得ない事情があると認めた場合のほか、入札現場を退場することができない。

８．入札の無効
競争入札参加者等が次の各号の一に該当する場合における入札は、無効とする。
（１）第５項に掲げる資格を有していない者及び前項第８号に該当する者の行った入札。
（２）郵送により提出された入札書が所定の日時までに到着しなかったとき。
（３）提出された入札書が、その封筒の表記から当該入札の入札書であることが確認し難いとき。
（４）入札書の記載事項が不明なとき。
（５）入札書に記名、押印並びに代理人の場合は、代理人の表示がないとき。
（６）同一人が２以上の入札書を提出したとき。
（７）競争入札参加者等が他の競争入札参加者の代理人として入札書を提出したとき。
（８）前各号のほか、入札に必要な条件を備えないとき。

９．落札者の決定方法
（１）予定価格の制限の範囲内で、契約担当者が入札説明書で必須とした項目の最低限の要求要件をすべて満たしている提案をした入札者の中から、センターが定める総合評価の方法をもって落札者を決定する。
開札をした場合において、各人の入札のうち予定価格の制限に達した価格の入札がないときは、再度の入札を行うものとする。
なお、入札回数は再度入札を含め３回までとする。
（２）総合評価点の数値の最も高い者が２人以上あるときは、くじにより落札者を決定する。当該競争参加者のうち出席しない者があるときは、これに代わって入札事務に関係のないセンターの職員がくじを引くものとする。
（３）再度の入札を行ってもセンターの予定価格に達しない場合は、３回目の最低入札価格提示者と減額交渉を行うものとする。
（４）落札者が契約担当者の定める期日までに、センターが妥当と判断する理由により契約書の取り交わしをしないときには、落札者の決定を取り消すことができるものとする。

10．契約書の作成
本契約には、センターの定める契約条件による契約書を作成する。

11．その他
（１）提出書類
① ２０２５年　３月２４日（月）　午後４時まで（ＦＡＸ・電子メール可）
・質問書（参考資料４）
② ２０２５年　３月３１日（月）　午後４時まで（郵送可）
・『応札資料作成要領』に示す書類　必要部数
・契約者情報連絡書　１部
・資格要件確認書に記載されている資料　１部
③入札・開札当日
・代理人が入札する場合は、その者に対する委任状　（参考資料１）または、これに準ずる書類。
（２）入札に必要な費用は、全て入札者の負担とする。
（３）開示した資料・図面等は必ず返却する。

提出書類確認表

案件名：「第2期基盤情報システムの構築及び移行業務」

開札日：2025年 5月21日(水) 午後1時30分

確認	提出書類名	提出期限	参考資料No.	備考
	質問書	2025年 3月24日(月) 午後4時まで(電子メール可)	4	入札参加者は必ず提出すること
	『応札資料作成要領』に示す書類	2025年 3月31日(月) 午後4時まで(郵送可)	―	
	資格要件確認書 (記載されている資料含む)	2025年 3月31日(月) 午後4時まで(郵送可)	6	記入例を参考にすること
			7	「品質保証計画書」を提出済みの場合参考にすること
	契約者情報連絡書	2025年 3月31日(月) 午後4時まで(郵送可)	10	「紙の契約書」か「電子契約」かを必ず選択すること
	入札辞退届	決定後速やかに(電子メール可)	3	
	入札書	【郵送の場合】2025年 5月20日(火) 午後5時必着	2	「入札書」と「委任状」についてを参考にすること
	委任状	【郵送の場合】2025年 5月20日(火) 午後5時必着	1	「入札書」と「委任状」についてを参考にすること

◆ 必ずお読みください ◆

「入札書」と「委任状」について

入札者により提出いただく「入札書」と「委任状」が異なります。
下記を参考の上書類を作成、提出してください。

入札者	提出書類		参考資料No.	書類記載名	押印省略	提出方法
代表者	入札書		2（A）	「代表者」	不可	郵送又は持参
	委任状	1通目	—	—	—	—
		2通目	—	—	—	—
代理人	入札書		2（B）	「代表者」と「代理人」	不可	郵送又は持参
	委任状	＊1通目	＊1（A）又は1（B）	「代表者」から「代理人」へ	不可	郵送又は持参
		2通目	—	—	—	—
復代理人	入札書		2（C）	「代理人」と「復代理人」	不可	郵送又は持参
	委任状	＊1通目	＊1（A）又は1（B）	「代表者」から「代理人」へ	不可	郵送又は持参
		2通目	1（C）	「代理人」から「復代理人」へ		

※ 代　表　者：「資格審査結果通知書（全省庁統一資格）」記載の法人代表者
　代　理　人：代表者以外（支店長、部長、課長等の社員等）
　復代理人：代理人が更に選任した代理人（支店等の社員等）

＊ 事前に「参考資料№1（A）（委任期間あり）」を提出済の場合は「委任状1通目」の提出は不要

提出方法（いずれか）	⇒	郵送、持参
押印の省略	⇒	不可

参考資料１(A)

(支店長等が一定期間代理人となる場合)

年　月　日

※提出日を記入
(郵送の場合は発送日)

委　任　状

公益財団法人核物質管理センター
総務部長　猪狩　和　殿

住　所

会 社 名

代表者名　　印

※代表者の肩書と氏名を記入

私は、下記の者を代理人と定め、下記の一切の権限を委任します。

記

代 理 人　住　所

※支店・営業所等の所在地を記入

会 社 名

※会社名及び支店・営業所等の名称を記入

代理人名　　印

※代理人の肩書及び氏名を記入

委任事項
1. 入札及び見積に関する件
2. 契約締結に関する件
3. 契約代金の請求及び受領に関する件
4. 復代理の選任に関する件
5.【その他、必要に応じて記載】

委任期間　〇〇年〇月〇日から〇〇年〇月〇日まで

代理人使用印鑑	印

※これは参考例であり、必要に応じ適宜追加・修正して差し支えない。

提出方法（いずれか）	⇒	郵送、持参
押印の省略	⇒	不可

参考資料１(B)

(社員等が入札のつど代理人となる場合)

年　月　日

※提出日を記入
(郵送の場合は発送日)

委　任　状

公益財団法人核物質管理センター
総務部長　猪狩　和　殿

住　所

会 社 名

代表者名　　印

※代表者の肩書と氏名を記入

私は、＿＿＿＿＿＿＿＿を代理人と定め、下記の一切の権限を委任します。

※代理人の氏名を記入

記

委任事項

２０２５年５月２１日に行われる「第２期基盤情報システムの構築及び移行業務」の入札に関する件について

代理人使用印鑑	印

※これは参考例であり、必要に応じ適宜追加・修正して差し支えない。

提出方法（いずれか）	⇒	郵送、持参
押印の省略	⇒	不可

参考資料１(C)

(支店等の社員等が入札のつど復代理人となる場合)

年　月　日

※提出日を記入
(郵送の場合は発送日)

委　任　状

公益財団法人核物質管理センター
総務部長　猪狩　和　殿

住　所
※支店・営業所等の所在地を記入

会 社 名
※会社名及び支店・営業所等の名称を記入

代理人名　印
※代理人の肩書及び氏名を記入

私は、＿＿＿＿＿＿＿＿＿＿を復代理人と定め、下記の一切の権限を委任します。
※復代理人の氏名を記入

記

委任事項

２０２５年５月２１日に行われる「第２期基盤情報システムの構築及び移行業務」の入札に関する件について

復代理人使用印鑑	印

【注意】この場合、代表者からの代理委任状(復代理の選任に関する委任を含む)が必要
※これは参考例であり、必要に応じ適宜追加・修正して差し支えない。

提出方法（いずれか）	⇒	郵送、持参
押印の省略	⇒	不可

参考資料２(A)
(代表者が入札する場合)

入　　札　　書

件　　名：「第2期基盤情報システムの構築及び移行業務」

上記件名を入札説明書に定められた事項を承諾のうえ、下記のとおり入札いたします。

入札金額

拾	億	千	百	拾	万	千	百	拾	円

（消費税及び地方消費税を除いた金額）

年　　月　　日

※提出日を記入
(郵送の場合は発送日)

公益財団法人核物質管理センター
総務部長　猪狩　和　　殿

住　　所

会 社 名

代表者名　　印

※代表者の肩書と氏名を記入

提出方法（いずれか）	⇒	郵送、持参
押印の省略	⇒	不可

参考資料２(B)

(社員等の代理人が入札する場合)

入　　札　　書

件　　名：「第2期基盤情報システムの構築及び移行業務」

上記件名を入札説明書に定められた事項を承諾のうえ、下記のとおり入札いたします。

入札金額

拾	億	千	百	拾	万	千	百	拾	円

（消費税及び地方消費税を除いた金額）

年　　月　　日

※提出日を記入
(郵送の場合は発送日)

公益財団法人核物質管理センター
総務部長　猪狩　和　　殿

住　　所

会 社 名

代表者名　　印

※代表者の肩書と氏名を記入

代理人名　　印

※委任状に記載の代理人氏名を記入

提出方法（いずれか）	⇒	郵送、持参
押印の省略	⇒	不可

参考資料２(C)

(支店等の社員等が復代理人として入札する場合)

入　　札　　書

件　　名：「第2期基盤情報システムの構築及び移行業務」

上記件名を入札説明書に定められた事項を承諾のうえ、下記のとおり入札いたします。

入札金額

拾	億	千	百	拾	万	千	百	拾	円

（消費税及び地方消費税を除いた金額）

年　　月　　日

※提出日を記入
(郵送の場合は発送日)

公益財団法人核物質管理センター
総務部長　猪狩　和　　殿

住　　所

会 社 名

代理人名　　印

※委任状に記載の代理人氏名を記入

復代理人名　　印

※委任状に記載の復代理人氏名を記入

提出方法（いずれか）	⇒	FAX、電子メール、郵送、持参
押印の省略	⇒	可

参考資料 10

※本書類は参考見積書に添付してご提出ください。

公益財団法人　核物質管理センター　御中

年　　月　　日

契約者情報連絡書

案　件　名	「第2期基盤情報システムの構築及び移行業務」

契約書記載情報	※契約書に記載する「契約名義人」情報を記載してください。
所在地	（〒　　－　　）
名称	
役職	
氏名	
契約名義人 （□内に✓を記入する）	「資格審査結果通知書（全省庁統一資格）」記載の法人代表者と □ 同じ □ 異なる（代理人）⇒ 代表者から代理人への「委任状」を提出してください
※注意事項	※契約名義人はセンターと契約締結をする代表者または代理人です。 （契約日が4月1日の場合は4月1日時点の契約名義人を記載） ※ 契約名義人に変更があった場合は速やかに本書類の再提出をお願いします。

契約書送付先情報	※「契約書を送付する」情報を記載してください。
住所	（〒　　－　　）
名称	
所属	
役職	
フリガナ	
氏名	
電話番号	－　　－
契約書 （□内に✓を記入する）	□ 紙の契約書　　□ 電子契約　　で取り交わし希望
電子契約書 送付先アドレス	＠

適格請求書発行事業者登録番号	（Tで始まる13桁の数字） T

※「登録番号」について、ご不明な点がございましたら下記までお問合せください。
（公財）核物質管理センター　総務部　経理課　TEL:03-5816-7764

センター使用欄	

提出方法（いずれか）	⇒	FAX、電子メール、郵送、持参
押印の省略	⇒	可

参考資料３

入　札　辞　退　届

件　　名：「第2期基盤情報システムの構築及び移行業務」

上記の入札を都合により辞退します。

年　月　日

公益財団法人核物質管理センター
総務部長　猪狩　和　殿

住　所

会 社 名

責任者名

担当者名

連 絡 先

※これは参考例であり、必要に応じ適宜追加・修正して差し支えない。

提出方法（いずれか）	⇒ FAX、電子メール、郵送、持参
押印の省略	⇒ 可

参考資料 4

参加者は必ず提出すること

※質疑がない場合でも、その旨を記載し提出すること

年　月　日

「第2期基盤情報システムの構築及び移行業務」に係る質問書

会　社　名	
連　絡　先	担当者名 TEL FAX
質問	
回答	

センター使用欄	

資格要件確認書

契約番号	135-021, 135-022, 135-023, 135-024, 151-0xx	請求元課室：	情報セキュリティ室
契約件名	第2期基盤情報システムの構築及び移行業務	購買区分：	C
参加者名		評価の有無：	有（下記のとおり）

評価項目		仕様書ページ	確認項目	証明資料	センター記入欄		
					判定	判定理由	判定者
1 業務の実施・管理体制等	1.1 業務の実施体制		① 業務の実施に十分な人員数及びスキル（業務遂行に必要な有資格等）が確保されていること。				請求元課室長
			② 必要な業務分担（設計開発、製造、調達、試験、検査、保守、設置工事、品質保証等）及び管理体制（品質管理責任者、作業管理者等を含む）がとられていること。				請求元課室長
	1.2 品質管理及び情報セキュリティ体制		① 受注する製品及びサービスを要求項目に沿って提供できる品質管理システム（設計・開発を含む）が確立していること。	JIS Q 9001認証証明書			請求元課室長
			② 情報セキュリティに対する管理体制が確立していること。	ISO/JIS Q 27001認証証明書 情報セキュリティ体制表			請求元課室長
	1.3 コンプライアンス		①コンプライアンス違反の有無（有の場合はどのように改善したか。）				請求元課室長
			②不適合事象の有無（有の場合はどのように改善したか。）				請求元課室長
2 技術確認事項	2.1 技術能力の確認	P20 4.2.1 No.2	作業従事者には、以下の資格を保持する者を1名以上含めること。 ・システムアーキテクト（IPA） ・ネットワークスペシャリスト（IPA） ・情報処理安全確保支援士又は情報セキュリティスペシャリスト（IPA）	資格証明書			請求元課室長
		P26 7.1.2	作業従事者には、以下の経験を有する者を1名以上含めること。 ・本システムと同等規模以上のゼロトラストを前提としたネットワークサービスの構築実績を有すること。 ・本システムと同等規模以上の統合認証サービス（Microsoft Entra ID）の構築実績を有すること。（※Azure Active Directory の構築実績も同等の実績として認める。） ・本システムと同等規模以上のオンプレミス環境をクラウドに移行した実績を有すること。	実績表			
	2.2 技術設備の確認	（例）P.2 3(1)	（例） ①●●の製造する設備を持っていること。				請求元課室長
		P.2 3(3)	②●●の試験する設備を持っていること。				

資格要件確認書

契約番号	135-021, 135-022, 135-023, 135-024, 151-0xx	請求元課室：	情報セキュリティ室
契約件名	第2期基盤情報システムの構築及び移行業務	購買区分：	C
参加者名		評価の有無：	有（下記のとおり）

評価項目		仕様書ページ	確認項目	証明資料	センター記入欄		
					判定	判定理由	判定者
	2.3						請求元課室長
	物品性能の確認	（例）P.3 4(1)	（例）①納品される製品は、●●の性能要件を満たしていること。				
		P.3 4(2)	②納品される製品は、●●の環境でも稼働していること。				
		P.3 4(3)	③空調用冷水設備の性能は次の値を保証すること。				
		P.3 4(4)	④●●時間以上の連続運転を保証すること。				
		P.3 4(5)	⑤納品される物品の●クラス相当の耐震設計基準を満たしていること。				
		P.3 4(6)	⑥納品される製品の●●年の設計耐用年数を満たしていること。				
	2.4 物品の実績の確認	（例）P.4 5(1)）	（例）①過去5年間で、当該製品は、（耐震設計基準●クラスで）納入実績を示すこと。				請求元課室長
			②過去●年以内に同等製品（同等なサービス）の受注を受けた実績があること。（上記の実績は、当該製品（サービス）に対して重大な不適合を発生させ、発注元に損益を与えた事例がないものとする。）				
	2.5 ●●	（例）P5 6(1)	（例）①工場立会検査に対応できること。				請求元課室長
		P5 6(2)	②受注者の品質管理システムについて品質監査を実施できること。				

注）各確認事項を証する資料名を「証明資料」欄に記載し、当該資料を入札仕様書又は見積書に添付のうえ契約担当者に提出すること。

参考資料 6

提出方法（いずれか）	⇒	電子メール、郵送、持参
押印の省略	⇒	可

資格要件確認書

契約番号：XXX-XXX
契約件名：XXXXXXXXXXXXX
社　　名：●●●●株式会社

社名を記入してください。
※社印は不要です。

提出する資料名を記入してください。

※タイトル行（太線内）は変更しないでください。

本書は、案件ごとに記入してください。
記入後の本書と証明資料は、入札仕様書等の書類と合わせて、入札仕様書等の提出期限までにメールまたはFAXにて提出してください。

評価項目		仕様書ページ	確認項目	証明資料	センター記入欄		
					判定	判定理由	判定者
1 業務の実 管理体制等	体制		数及び必要な有資格等）が確保されて	●●資格証（写）			
			開発を含む）が確立している こと。	QMS体制図			
			② 情報セキュリティに対する 管理体制 と。	情報セキュリティ体制			
2 技術確認事項	2.1 技術能力の確認	P.1 2(3)	① ○○の資格を有する作業員を配置できること。	~~●●資格証（写）~~ □□証明書			
	2.2 技術設備の確認			一覧			
	2.3 物品性能の確認	P.3 4(1)	の性能要件を満たしていること。	製品のスペックがわかる資料（カタログ等）			
	2.4 物品の実績の確認	P.4 5(1)	① 過去5年間で、当該製品は、（耐震設計基準●クラスで）納入実績を示すこと。	納品実績表			

「センター記入欄」には何も記入しないでください。

複数例示された資料から選択する場合は提出する資料名を○で囲んでください。

例示された資料と提出資料が異なる場合は実際の資料名に訂正してください。

注）参加者は、各確認事項を証する資料名を「証明資料」欄に記載し当該資料を添付のうえ契約担当者へ提出すること。

第 2 期基盤情報システムの構築及び移行業務

仕様書

2025 年度

公益財団法人　核物質管理センター

― 目次 ―

1. 案件の概要

1.1. 調達件名

第 2 期基盤情報システムの構築及び移行業務

1.2. 調達の背景

公益財団法人核物質管理センター（以下、「センター」という。）では、核物質管理に係る中核機関として品質保証を徹底し、業務の高い信頼性を確保し、継続的かつ安定的に業務を遂行することが求められる。

本調達において、現行のオンプレミス構成から、クラウド化や仮想分離の廃止等の方針を踏まえ、確実に第 2 期基盤情報システム（以下、「本システム」という。）の構築及び移行を行い、基盤情報システム全体の安定運用を継続し厳格な情報セキュリティ対策を引き続き実践するとともに、コストの適正化を図る。

1.3. 調達目的及び調達の期待する効果

センター全体の業務を支える情報インフラとなる本システムを構築することにより、以下を実現し、情報セキュリティを維持することを目的とする。

- センターの有する機微情報の漏えい対策の維持
- センターの事業継続性の向上
- センターの情報インフラの一元管理の実現
- 運用・保守業務の効率性の改善
- クラウドサービスの活用
- ゼロトラストを前提としたセキュリティの強化　等

1.4. 業務・情報システムの概要

本システムは、センター全体の業務を支える情報インフラとなる「ネットワークサービス（LAN/WAN/テレワーク/インターネット）」、「基盤サービス（統合認証、ファイル共有、システム運用管理・監視、バックアップ管理等）」及び「端末サービス」を提供するためのシステムである。

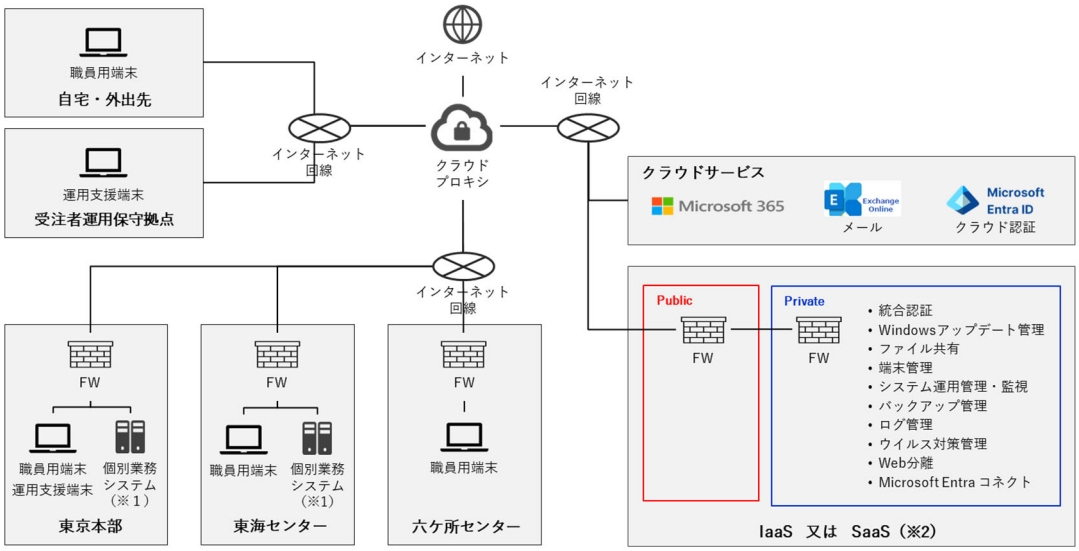
ネットワークサービスは従来のオープン系・クローズド系で構成していた仮想分離を廃止し、ゼロトラストを前提としたネットワークを提供する。

基盤サービスは現行のオンプレミス構成から、クラウドサービスを利用した構成に変更する。また、仮想分離の廃止に伴い、仮想デスクトップを廃止する。

端末サービスは職員用端末（デスクトップ PC）とテレワーク端末（ノート PC）で利用形態を分けていたが、全ての端末をノート PC に刷新することで、職員用端末に統一する。

各課室が個別に管理・運用している個別業務システムは、本業務で構築する LAN と接続する。

なお、基本的にはクラウド化を前提としているが、同等レベルの機能やセキュリティを担保できるのであれば、一部機能をオンプレミス上で構成する提案を妨げるものではない。



※1　個別業務システムは本調達の範囲外となるが、個別業務システムとの接続までは実施する。
※2　クラウド化した際と同等レベルの機能やセキュリティを維持できるのであれば、一部機能をオンプレミス上に構成する提案を妨げるものではない。

図 1-1 本システムの全体構成図

1.5. 契約期間

本調達案件は、以下の 2 件の契約からなる。それぞれの契約期間を以下に示す。

(ア) 第 2 期基盤情報システムの構築及び移行業務に関する契約

契約期間は、契約締結日（2025 年 7 月頃を想定。）から 2026 年 3 月 31 日とする。

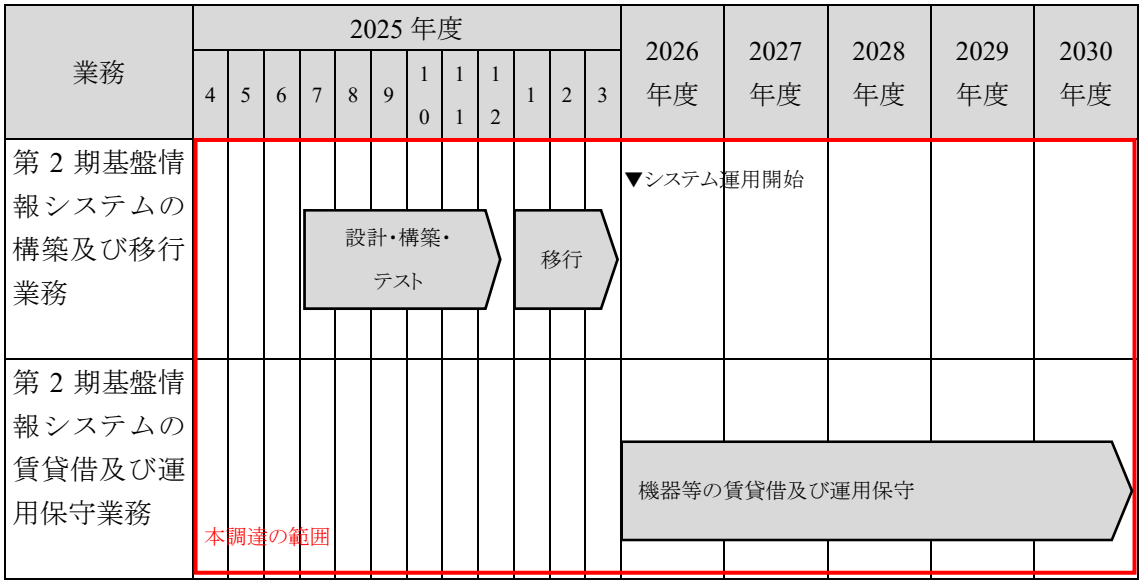
(イ) 第 2 期基盤情報システムの賃貸借及び運用保守業務に関する契約

契約期間は、契約締結日（2026 年 4 月頃を想定。）から 2031 年 3 月 31 日とする。ただし、第 2 期基盤情報システムの構築及び移行業務から賃貸借及び運用保守業務の開始までの期間において発生する不具合等（初期不良、機器の故障等）への修理・交換作業についても、賃貸借及び運用保守業務の開始後と同様に行い、その費用は本業務の受注者の負担とする。

1.6. 作業スケジュール

本業務の作業スケジュール（想定）を以下に示す。

表 1-1 作業スケジュール（想定）



2.　情報システムに求める要件

本業務の実施に当たっては、「別紙 1_要件定義書」の各要件を満たすこと。

3.　作業の実施内容

3.1.　「第 2 期基盤情報システムの構築及び移行業務」の実施内容

3.1.1.　設計・構築実施計画書等の作成

設計・構築実施計画書等の作成に係る要件を以下に示す。

(ア) 受注者は、センターの指示に基づき、「設計・構築実施計画書」及び「設計・構築実施要領」を作成し、センターの承認を得ること。

(イ) 「設計・構築実施計画書」には、以下の項目について記載すること。また、附属文書として作業項目、作業内容、スケジュールをより詳細に階層化し、担当者等を記載した Work Breakdown Structure（WBS）を作成すること。なお、WBS については作業項目ごとの計画工数を記載すること。

① 作業概要

設計・構築の対象範囲、作業項目、作業概要等について記載する。

② 作業体制に関する事項

受注者のみならず、設計・構築に関連する全ての関係者について、その体制、関係者間の関係性、役割分担・責務等について記載する。

③ スケジュールに関する事項

本調達仕様書及び受注者の提案書に基づく作業内容、スケジュール概要、マイルストーン等について記載する。

④ 納入物に関する事項

設計・構築によって作成される納入物名、納入物の内容、品質基準、担当者、提出期限、提出方法、提出部数等について記載する。

⑤ 設計・構築形態等

設計・構築方式、構築手法、設計・構築時に利用するツール等について記載する。

⑥ WBS（別添等）

作業項目、作業内容、スケジュールを階層化し、担当者、作業項目間の依存関係、EVM などに基づく管理指標等を設定した WBS

(ウ) 「設計・構築実施要領」には、以下の項目について記載すること。

① コミュニケーション管理

関係者との合意形成に関する手続き、連絡調整に関する方法、受注者が作業を進める上で必要となる会議・開催頻度・参加者、議事録等の管理等について記載する。

② 体制管理

受注者における作業体制の管理手法等について記載する。

③ 工程管理

設計・構築における作業、その工程の管理手法等について記載する。

④ 品質管理

納入物の品質を確保するために、品質基準、品質管理方法等について記載

する。

⑤ リスク管理

設計・構築における作業を阻害する可能性のあるリスクを適切に管理するため、リスク認識の手法、リスクの管理手法、顕在時の対応手順、リスクの見直し方法等について記載する。

⑥ 課題管理

設計・構築において解決すべき問題について、発生時の対応手順、管理手法等について記載する。

⑦ システム構成管理

設計・構築における本システムの構成（ハードウェア、ソフトウェア、ネットワーク、クラウドサービス等）の管理手法等について記載する。

⑧ 変更管理

設計・構築の進捗により変更が生じた場合は、変更内容について、管理対象、変更手順、管理手法等について記載する。

⑨ 情報セキュリティ対策

設計・構築における情報漏えい対策・ルール等について記載する。また、受注者若しくはその従業員又はその他の者による意図せざる変更が加えられないための管理体制について記載する。

⑩ 文書管理

納入物に関して誤字脱字の修正、用語の統一等内容の管理手法などについて記載する。

(エ) 受注者は、会議体の議事録を、原則として、会議実施後 3 営業日以内に作成し、センターに提示すること。これは、「第 2 期基盤情報システムの構築及び移行業務」だけでなく、「第 2 期基盤情報システムの賃貸借及び運用保守業務」においても同様とすること。

3.1.2. 設計

本システムの設計に係る要件を以下に示す。

(ア) 受注者は、要件定義の内容に関する認識に可能な限り相違が生じないよう、センターと要件定義の内容について確認及び調整の上、「別紙 1 要件定義書」の要件定義を確定すること。なお、要件定義の確定に当たっては、受注者が応札時に提出した提案書等の内容を盛り込むこと。

(イ) 受注者は、「別紙 1 要件定義書」に基づき、本システムの業務、機能及び非機能要件を満たすための実現方式、システム構成、採用製品等を定義した基本設計書及び詳細設計書を作成し、納入物についてセンターの承認を得ること。

(ウ) 受注者は、「別紙 1 要件定義書」に基づき、以下に示す設計作業を実施し、「基本設計書」及び「詳細設計書」として取りまとめセンターに提出すること。なお、各設計書の記載内容、記載粒度については、センターと協議の上決定すること。

① ネットワークサービス設計
② 基盤サービス設計
③ 端末サービス設計

(エ)「基本設計書」の作成に当たっては、最低限以下の設計を行うこと。
① 設備設計
② 機能設計
③ IP アドレス(ドメイン)の設計
④ ルーティング設計
⑤ 物理構成設計
⑥ 論理構成設計(ネットワークトポロジー等)
⑦ セキュリティ対策(暗号化、ファイアウォール、電子署名等)の設計
⑧ 性能・拡張性・信頼性設計
⑨ 端末等設計

(オ)「詳細設計書」の作成に当たっては、最低限以下の設計を行うこと。
① ネットワーク監視のパラメータ設計(ネットワーク監視パラメータ、サーバ監視パラメータ等)
② ネットワーク機器のパラメータ設計(ファイアウォール、ルータ、スイッチ等の設定値等)
③ サーバの詳細設計(サーバの構成(冗長構成等)、ストレージ構成、ソフトウェア機能(OS、ミドルウェア等)、パラメータ設定等)
④ セキュリティ対策のパラメータ設計
⑤ クラウドサービスの詳細設計(クラウドサービス機能、パラメータ設定等)

(カ) 設計に当たり、既存の機器・システムの設定情報等の確認作業が必要となる場合は、業務への影響が生じない範囲で確認作業を行うこと。なお、一部の機器については東京本部からのリモートアクセスによる確認が可能な場合もあるため、事前にセンターへの確認を行うこと。

3.1.3. 構築・導入設置

本システムの構築・導入設置に係る要件を以下に示す。

(ア) 受注者は、構築に当たり、情報セキュリティ確保のためのルール遵守や納入物の確認方法(例えば、インストール・設定内容の検査、現場での抜き打ち調査等についての実施主体、手順、方法等)を定め、センターの承認を得ること。
(イ) 受注者は、「基本設計書」及び「詳細設計書」に基づき、本システムの構築を行うこと。
(ウ) 受注者は、機器等の導入設置に当たり、センターの各拠点(東京本部、東海センター及び六ヶ所センター)の設置環境(電源環境、ラックスペース、配線環境等)について、事前に現地調査を行うこと。
(エ) 受注者は、現地調査の結果を踏まえ、センターと協議を行い、「導入設置計画書」

を作成して、センターの承認を得ること。
(オ) 受注者は、「基本設計書」、「詳細設計書」及び「導入設置計画書」に基づき、「導入設置手順書」を作成し、センターの承認を得ること。
(カ) 受注者は、「導入設置手順書」に基づき、機器等の導入設置、各種設定作業を実施すること。
(キ) 受注者は、機器等の導入設置、各種設定作業の結果を「導入設置報告書」に取りまとめ、センターに報告すること。

3.1.4. テスト

本システムにおいて、受注者が行うテストに係る要件を以下に示す。

(ア) 受注者は、「別紙 1 要件定義書」の「3.12. テストに関する事項」に沿って、単体テスト、結合テスト及び総合テストを実施すること。

3.1.5. 受入テスト支援

本システムの受入テスト支援に係る要件を以下に示す。

(ア) 受注者は、「受入テスト計画書」及び「受入テスト仕様書」の案を作成し、センターに提示すること。
(イ) 受注者は、センターが受入テストを実施するに当たり、環境整備及び運用等の支援を行うこと。また、役職員に対して、問合せ対応等の支援を行うこと。
(ウ) 受注者は、受入テストの実施状況を「受入テスト報告書」の案として、センターに提示すること。

3.1.6. 運用計画及び運用実施要領の作成

本システムの「運用計画」及び「運用実施要領」の作成に係る要件を以下に示す。

(ア) 受注者は、「基本設計書」及び「詳細設計書」に基づき、運用設計を行うこと。
(イ) 受注者は、運用設計に基づき、定常時における作業内容、その想定スケジュール、障害発生時における作業内容等を取りまとめた「運用計画」を作成し、センターの承認を得ること。
(ウ) 受注者は、運用設計に基づき、運用業務の管理方法や手順、順守事項等について定めた「運用実施要領」を作成し、センターの承認を得ること。
(エ) 受注者は、計画的に発生する作業内容、想定される時期などを取りまとめた「中長期運用作業計画書」を作成し、センターの承認を得ること。
(オ) 「運用実施要領」は、「運用計画」における作業内容、スケジュール等との整合性を図った上で作成すること。また、運用業務を管理する上での具体的な方法等を示した「運用手順書」等も併せて作成すること。
(カ) 「運用計画」には、以下の項目について記述すること。

① 作業概要

監視、運用の対象範囲、作業概要等について記載する。

② 作業体制に関する事項

受注者のみならず、運用に関連する全ての関係者について、その体制、関係者間の関係性、役割分担・責務等について記載する。

③ スケジュールに関する事項

作業内容、そのスケジュール、関係する他の作業工程、そのスケジュール等について記載する。

④ 提出物に関する事項

運用によって作成される提出物の内容、提出期限、提出方法、提出部数等について記載する。

⑤ 運用形態等

運用形態、運用手法、運用環境、運用ツール等を必要に応じて記載する。

(キ)「運用実施要領」には、以下の項目について記述すること。また、様式を定めたうえで、必要に応じて「各種管理台帳」を作成すること。

① コミュニケーション管理

関係者との合意形成に関する手続き、連絡調整に関する方法、受注者が参加すべき会議・開催頻度・議事録等の管理等について記載する。

② 体制管理

受注者における作業体制の管理手法等について記載する。

③ 作業管理

運用の作業、その品質の管理手法等について記載する。

④ リスク管理

運用における作業を阻害する可能性のあるリスクを適切に管理するため、リスク認識の手法、リスクの管理手法、顕在時の対応手順等について記載する。

⑤ 課題管理

運用において発生したインシデント及び解決すべき問題について、発生時の対応手順、管理手法等について記載する。

⑥ システム構成管理

運用における本システムの構成（ハードウェア、ソフトウェア、ネットワーク、クラウドサービス等）の管理手法等について記載する。

⑦ 変更管理

運用により発生する変更内容について、管理対象、変更手順、管理手法等について記載する。

⑧ 情報セキュリティ対策

運用における情報漏えい対策等について記載する。また、受注者若しくはその従業員又はその他の者による意図せざる変更が加えられないための管理体制について記載する。

3.1.7. 保守計画及び保守実施要領の作成

本システムの「保守計画」及び「保守実施要領」の作成に係る要件を以下に示す。

(ア) 受注者は、「基本設計書」及び「詳細設計書」に基づき、保守設計を行うこと。
(イ) 受注者は、保守設計に基づき、定常時における作業内容、その想定スケジュール、障害発生時における作業内容等を取りまとめた「保守計画」を作成し、センターの承認を得ること。
(ウ) 受注者は、保守設計に基づき、保守業務の管理方法や手順、順守事項等について定めた「保守実施要領」を作成し、センターの承認を得ること。
(エ) 受注者は、計画的に発生する作業内容、想定される時期などを取りまとめた「中長期保守作業計画書」を作成しセンターの承認を得ること。
(オ) 「保守実施要領」は、「保守計画」における作業内容、スケジュール等との整合性を図った上で作成すること。また、保守業務を管理する上での具体的な方法等を示した「保守手順書」等も併せて作成すること。
(カ) 「保守計画」には、以下の項目について記述すること。

① 作業概要
保守の対象範囲、作業概要等について記載する。

② 作業体制に関する事項
受注者のみならず、保守に関連する全ての関係者について、その体制、関係者間の関係性、役割分担・責務等について記載する。

③ スケジュールに関する事項
作業内容、そのスケジュール、関係する他の作業工程、そのスケジュール等について記載する。

④ 提出物に関する事項
保守によって作成される提出物、提出期限、提出方法、提出部数等について記載する。

⑤ 保守形態等
保守形態、保守手法、保守環境、保守ツール等を必要に応じて記載する。

(キ) 「保守実施要領」には、以下の項目について記述すること。また、様式を定めたうえで、必要に応じて「各種管理台帳」を作成すること。

① コミュニケーション管理
関係者との合意形成に関する手続き、連絡調整に関する方法、受注者が参加すべき会議・開催頻度・議事録等の管理等について記載する。

② 体制管理
受注者における作業体制の管理手法等について記載する。

③ 作業管理
保守の作業、その品質の管理手法等について記載する。

④ リスク管理
保守における作業を阻害する可能性のあるリスクを適切に管理するため、リスク認識の手法、リスクの管理手法、顕在時の対応手順等について記載する。

⑤ 課題管理

保守において発生したインシデント及び解決すべき問題について、発生時の対応手順、管理手法等について記載する。

⑥ システム構成管理

保守における本システムの構成（ハードウェア、ソフトウェア、ネットワーク、クラウドサービス等）の管理手法等について記載する。

⑦ 変更管理

保守により発生する変更内容について、管理対象、変更手順、管理手法等について記載する。

⑧ 情報セキュリティ対策

保守における情報漏えい対策等について記載する。また、受注者若しくはその従業員又はその他の者による意図せざる変更が加えられないための管理体制について記載する。

3.1.8. 移行計画

本システムの移行計画に係る要件を以下に示す。

(ア) 受注者は、「別紙 1 要件定義書」の「3.12. 移行に関する事項」の定めに沿って、「3.12.2.1.移行計画」に示す要件を実施すること。

3.1.9. 教育

本システムの構築に係る教育の要件を以下に示す。

(ア) 受注者は、「別紙 1 要件定義書」の「3.15. 教育に関する事項」の定めに沿って、センターに対し、教育を実施すること。

3.1.10. 移行

本システムの移行に係る要件を以下に示す。

(ア) 受注者は、「別紙 1 要件定義書」の「3.12. 移行に関する事項」の定めに沿って、移行期間の作業を実施すること。

3.1.11. 工事

本システムのケーブル敷設工事に係る要件を以下に示す。

(ア) 受注者は、「別紙 1 要件定義書」の「3.13. ケーブル敷設工事」並びに公共建設工事標準仕様書（電気設備工事編）令和 4 年度版、公共建築改修工事標準仕様書（電気設備工事編）令和 4 年度版の定めに沿って、工事を実施すること。

(イ) 受注者は、現場代理人等通知書及び施工体制台帳の写しを提出すること。

(ウ) 受注者は、機器等の導入設置、敷設工事の結果を「工事完了報告書」に取りまとめ、センターに報告すること。

3.1.12. 定例会等の実施

(ア) 受注者は、定例会を定期的に開催するとともに、業務の進捗状況を作業実施要領に基づき報告すること。

(イ) センターから要請があった場合、又は、受注者が必要と判断した場合、必要資料を作成の上、定例会とは別に会議を開催すること。

(ウ) 受注者は、会議終了後、3 日以内（行政機関の休日（行政機関の休日に関する法律（昭和 63 年法律第 91 号）第 1 条第 1 項各号に掲げる日をいう。）を除く。）に議事録を作成し、センターの承認を得ること。

3.2. 「第 2 期基盤情報システムの賃貸借及び運用保守業務」の実施内容

3.2.1. 機器等の賃貸借

本システムの機器等の賃貸借に係る要件を以下に示す。

(ア) 受注者は、「別紙 1 要件定義書」の「3.10. 情報システム稼働環境に関する事項」に示した、本業務で調達する機器等の賃貸借を行うこと。

3.2.2. 運用業務

本システムの運用に係る要件を以下に示す。

(ア) 受注者は、「別紙 1 要件定義書」の「3.16. 運用に関する事項」に定められた要件を実施すること。

3.2.3. 保守対応

本システムの保守対応に係る要件を以下に示す。

(イ) 受注者は、「別紙 1 要件定義書」の「3.17. 保守に関する事項」に定められた要件を実施すること。

3.2.4. 引継ぎ

(ア) 受注者は、「別紙 1 要件定義書」の「3.14. 引継ぎに関する事項」の定めに沿って、第 3 期基盤情報システム関係事業者への引継ぎのための資料・情報を提出すること。

3.3. 納入物等の範囲、納入期日等

3.3.1. 納入物一覧

本調達案件の各契約に係る納入物を以下に示す。なお、「提出時期」については各業務の契約締結時期や作業計画等を踏まえ、必要に応じてセンターと協議の上で見直しを行うこと。

3.3.1.1. 第 2 期基盤情報システムの構築及び移行業務

本システムの構築及び移行業務に係る納入物を以下に示す。

表 3-1 納入物一覧（第 2 期基盤情報システムの構築及び移行業務）

No.	書類名	提出時期	納入期限	納入部数
1	情報セキュリティ管理計画書	契約後速やかに	契約後速やかに	電磁記録媒体 1 部
2	現場代理人等通知書及び施工体制台帳の写し	契約後速やかに	契約後速やかに	電磁記録媒体 1 部
3	設計・構築実施計画書	2025 年 7 月末頃	2026 年 3 月 20 日	電磁記録媒体 1 部
4	設計・構築実施要領	2025 年 7 月末頃	2026 年 3 月 20 日	電磁記録媒体 1 部
5	要件定義書（確定版）	2025 年 7 月末頃	2026 年 3 月 20 日	電磁記録媒体 1 部
6	基本設計書	2025 年 8 月末頃	2026 年 3 月 20 日	電磁記録媒体 1 部
7	詳細設計書	2025 年 9 月末頃	2026 年 3 月 20 日	電磁記録媒体 1 部
8	導入設置計画書	2025 年 10 月末頃	2026 年 3 月 20 日	電磁記録媒体 1 部
9	導入設置手順書	2025 年 10 月末頃	2026 年 3 月 20 日	電磁記録媒体 1 部
10	導入設置報告書	2025 年 10 月末頃	2026 年 3 月 20 日	電磁記録媒体 1 部
11	単体テスト計画書・単体テスト仕様書	2025 年 11 月末頃	2026 年 3 月 20 日	電磁記録媒体 1 部
12	単体テスト結果報告書	2025 年 12 月末頃	2026 年 3 月 20 日	電磁記録媒体 1 部
13	結合テスト計画書・結合テスト仕様書	2025 年 11 月末頃	2026 年 3 月 20 日	電磁記録媒体 1 部
14	結合テスト結果報告書	2025 年 12 月末頃	2026 年 3 月 20 日	電磁記録媒体 1 部
15	テストデータ・テストツール等（結合テスト）	2025 年 12 月末頃	2026 年 3 月 20 日	電磁記録媒体 1 部
16	総合テスト計画書・総合テスト仕様書	2025 年 12 月末頃	2026 年 3 月 20 日	電磁記録媒体 1 部
17	総合テスト結果報告書	2025 年 12 月末頃	2026 年 3 月 20 日	電磁記録媒体 1 部
18	テストデータ等（総合テスト）	2025 年 12 月末頃	2026 年 3 月 20 日	電磁記録媒体 1 部
19	受入テスト計画書(案)	2025 年 12 月末頃	2026 年 3 月 20 日	電磁記録媒体 1 部
20	受入テスト仕様書(案)	2025 年 12 月末頃	2026 年 3 月 20 日	電磁記録媒体 1 部

No.	書類名	提出時期	納入期限	納入部数
21	受入テスト報告書(案)	2026 年 1 月末頃	2026 年 3 月 20 日	電磁記録媒体 1 部
22	運用計画	2025 年 9 月末頃	2026 年 3 月 20 日	電磁記録媒体 1 部
23	運用実施要領 (各種管理台帳を含む。)	2025 年 9 月末頃	2026 年 3 月 20 日	電磁記録媒体 1 部
24	運用手順書	2025 年 11 月末頃	2026 年 3 月 20 日	電磁記録媒体 1 部
25	保守計画	2025 年 11 月末頃	2026 年 3 月 20 日	電磁記録媒体 1 部
26	保守実施要領(各種管理台帳を含む。)	2025 年 11 月末頃	2026 年 3 月 20 日	電磁記録媒体 1 部
27	保守手順書	2025 年 11 月末頃	2026 年 3 月 20 日	電磁記録媒体 1 部
28	教育実施計画書	2025 年 12 月末頃	2026 年 3 月 20 日	電磁記録媒体 1 部
29	教育結果報告書	2026 年 2 月末頃	2026 年 3 月 20 日	電磁記録媒体 1 部
30	説明資料(受入テスト用)	2025 年 11 月末頃	2026 年 3 月 20 日	電磁記録媒体 1 部
31	説明資料(全役職員用)	2025 年 12 月末頃	2026 年 3 月 20 日	電磁記録媒体 1 部
32	基盤情報システム利用者マニュアル	2025 年 12 月末頃	2026 年 3 月 20 日	電磁記録媒体 1 部
33	端末移行マニュアル	2025 年 12 月末頃	2026 年 3 月 20 日	電磁記録媒体 1 部
34	移行計画書	2025 年 12 月末頃	2026 年 3 月 20 日	電磁記録媒体 1 部
35	移行手順書	2025 年 12 月末頃	2026 年 3 月 20 日	電磁記録媒体 1 部
36	移行結果報告書	2026 年 3 月頃	2026 年 3 月 20 日	電磁記録媒体 1 部
37	工事完了報告書	2026 年 3 月頃	2026 年 3 月 20 日	電磁記録媒体 1 部
38	中長期運用作業計画書	2025 年 12 月末頃	2026 年 3 月 20 日	電磁記録媒体 1 部
39	中長期保守作業計画書	2025 年 12 月末頃	2026 年 3 月 20 日	電磁記録媒体 1 部
40	脆弱性検査結果報告書	2026 年 3 月頃	2026 年 3 月 20 日	電磁記録媒体 1 部
41	議事録	会議開催後 3 営業日以内	2026 年 3 月 20 日	電磁記録媒体 1 部
42	情報セキュリティ管理報告書	2026 年 3 月頃	2026 年 3 月 20 日	電磁記録媒体 1 部

3.3.1.2. 第 2 期基盤情報システムの賃貸借及び運用保守業務

本システムの賃貸借及び運用保守業務に係る納入物を以下に示す。

※2026 年 4 月 1 日～2031 年 3 月 31 日まで別途契約

表 3-2 納入物一覧(第 2 期基盤情報システムの賃貸借及び運用保守業務)

No.	書類名	提出時期	納入期限	部数
1	情報セキュリティ管理計画書	契約後速やかに	契約後速やかに	電磁記録媒体 1 部

No.	書類名	提出時期	納入期限	部数
2	ライセンス関連資料(ライセンス証書等)	2026 年 4 月 20 日	2026 年 4 月 30 日	電磁記録媒体 1 部
3	議事録	会議開催後 3 営業日以内	2026 年度から 2030 年度まで、毎年度 3 月 31 日(※)	電磁記録媒体 1 部
4	運用保守報告書	月次報告時	2026 年度から 2031 年度まで、毎年度 3 月 31 日(※)	電磁記録媒体 1 部
5	引継ぎ結果報告書	第 3 期基盤情報システム関係事業者への引継ぎ完了後速やかに	2031 年 3 月 31 日	電磁記録媒体 1 部
6	情報セキュリティ管理報告書	2031 年 3 月頃	2031 年 3 月 31 日	電磁記録媒体 1 部

※ 納入期日が営業日でない場合は、原則として前営業日とする。納入期日以降に特に報告が必要な事象が発生した場合は、別途センターと協議すること。

3.3.2. 納入方法

(ア) 納入物は全て日本語で作成すること。

(イ) 用字・用語・記述符号の表記については、「公用文作成の要領(昭和 27 年 4 月 4 日内閣閣甲第 16 号内閣官房長官依命通知)」を参考にすること。

(ウ) 情報処理に関する用語の表記については、日本工業規格(JIS)の規定を参考にすること。

(エ) 納入物は電磁的記録媒体により作成し、センターから特別に示す場合を除き、原則電磁的記録媒体 1 部を納入すること。

(オ) 紙媒体による納入について、用紙のサイズは、原則として日本工業規格 A 列 4 番とするが、必要に応じて日本工業規格 A 列 3 番を使用すること。

(カ) 電磁的記録媒体による納入について、CD-R 又 DVD-R の媒体に格納して納入すること。

(キ) 納入後センターにおいて改変が可能となるよう、図表等の元データも併せて納入すること。

(ク) 納入物の作成に当たって、特別なツールを使用する場合は、センターの承認を得ること。

(ケ) 納入物の作成に当たり、受注者の標準様式等を用いることを可とするが、個々の納入物の具体的な内容については、作成開始時点でセンターの確認を受けること。

(コ) 納入物が外部に不正に使用されたり、納入過程において改ざんされたりすることのないよう、安全な納入方法を提案し、納入物の情報セキュリティの確保に留意すること。
(サ) 電磁的記録媒体により納入する場合は、不正プログラム対策ソフトウェアによる確認を行うなどして、納入物に不正プログラムが混入することのないよう、適切に対処すること。

3.3.3. 納入場所

原則として、納入は次の場所において引渡しを行うこと。ただし、センターが納入場所を別途指示する場合はこの限りではない。

〒110-0015
東京都台東区東上野 1 丁目 28 番 9 号 キクヤビル 3 階
センター 総務部情報セキュリティ室

4.　作業の実施体制・方法

4.1.　作業実施体制

プロジェクトの推進体制及び受注者に求める作業実施体制は次の図及び表のとおりである。なお、受注者内のチーム編成については想定であり、受注者決定後に協議の上、見直しを行う。

また、受注者は本業務開始時に、本業務に関与するすべての要員の一覧を作成し、センターに提示すること。また、要員を変更する場合、センターの承認を得た上で、速やかに一覧を更新し、提示すること。

要員の兼任については、作業フェーズが異なる要員（例：構築チームリーダと移行・引継ぎチームリーダ）の兼任は可能とする。一方で、作業フェーズが重複する要員（例：実施責任者と各チームリーダ）の兼任は不可とする。

4.1.1. 第 2 期基盤情報システムの構築及び移行業務

本システムの構築及び移行業務の作業実施体制を以下に示す。

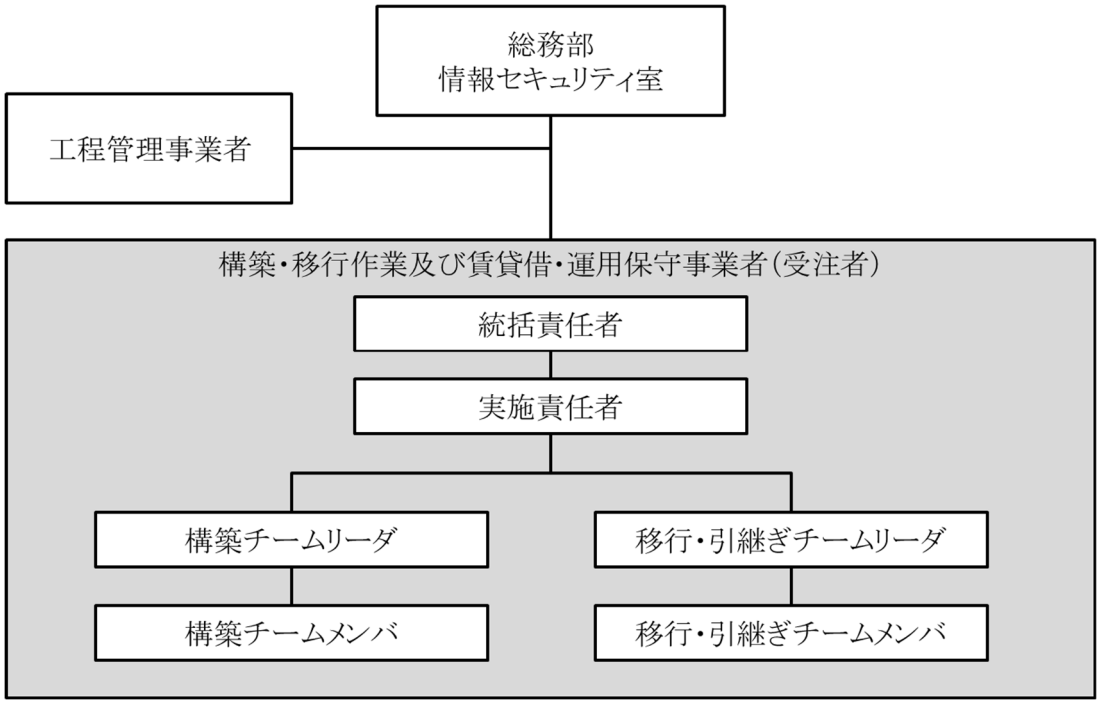


図 4-1 作業実施体制図（構築及び移行業務）（想定）

表 4-1 作業実施体制（構築及び移行業務）（想定）

No.	要員	役割
1	統括責任者	本業務全体を統括し、必要な意思決定を行う。
2	実施責任者	本業務全体の管理を行い、業務の遂行に必要な意思決定を行う。原則として、全ての進捗会議に出席する。
3	構築チームリーダ	本システムに関する設計・構築・テスト、受入テスト支援、運用設計、保守設計等の作業管理、課題管理等を行う。 また、構築工程における関連する組織・部門とのコミュニケーション窓口を担う。
4	構築チームメンバ	本システムに関する設計・構築・テスト、受入テスト支援、運用設計、保守設計等を行う。
5	移行・引継ぎチームリーダ	本システムに関する移行、引継ぎ等の作業管理や課題管理等を行う。 また、移行工程における関連する組織・部門とのコミュニケーション窓口を担う。
6	移行・引継ぎチームメンバ	本システムに関する移行、引継ぎ等を行う。

4.1.2. 第 2 期基盤情報システムの賃貸借及び運用保守業務

本システムの賃貸借及び運用保守業務の作業実施体制を以下に示す。

※2026 年 4 月 1 日～2031 年 3 月 31 日まで別途契約

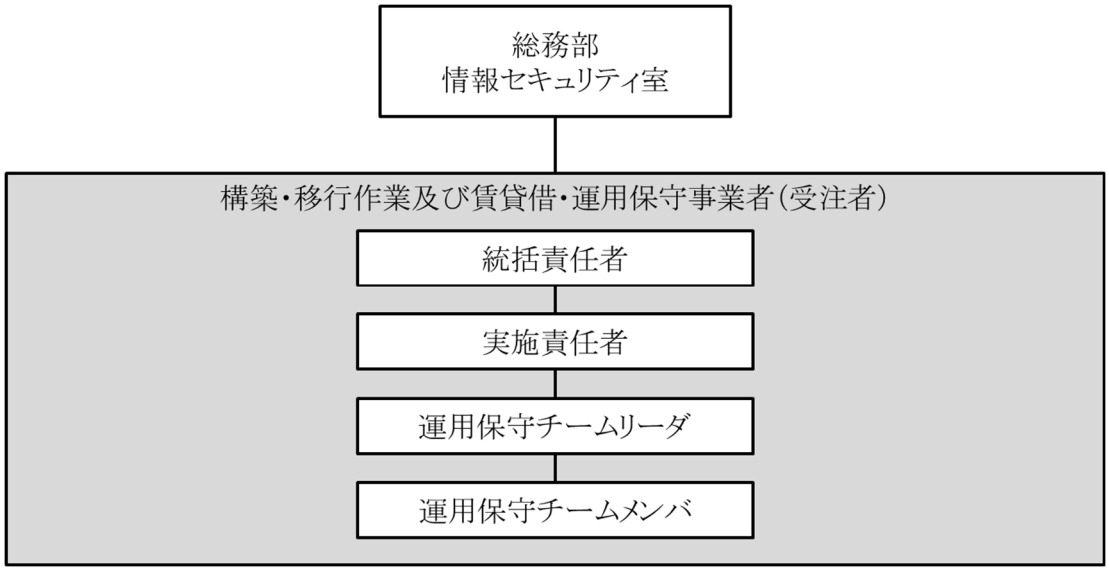


図 4-2 作業実施体制図（賃貸借及び運用保守業務）（想定）

表 4-2 作業実施体制（賃貸借及び運用保守業務）（想定）

No.	要員	役割
1	統括責任者	本業務全体を統括し、必要な意思決定を行う。
2	実施責任者	本業務全体の管理を行い、業務の遂行に必要な意思決定を行う。原則として、全ての進捗会議に出席する。
3	運用保守チームリーダ	本システムの運用管理、導入した機器等に関するハードウェア保守、ソフトウェア保守、クラウドサービス保守の作業管理や課題管理等を行う。 また、関連する組織・部門とのコミュニケーション窓口を担う。
4	運用保守チームメンバ	本システムの運用管理、導入した機器等に関するハードウェア保守、ソフトウェア保守、クラウドサービス保守を行う。

4.2. 作業要員に求める資格等の要件

本業務の各契約における作業要員に求める資格及び経験等の要件を以下に示す。

4.2.1. 第 2 期基盤情報システムの構築及び移行業務

本システムの構築及び移行業務に係る要件を以下に示す。

表 4-3 作業要員に求める資格・経験等の要件（構築及び移行業務）

No	要員	資格	経験等
1	実施責任者	以下の資格のいずれか一つ以上を有すること。 ① プロジェクトマネージャ（IPA※1） ② Project Management Professional（PMI※2） ただし、IT スキル標準 V3 2011 に基づき、当該資格保有者等と同等の能力を有することを示した場合は、これを認める場合がある（その根拠を明確に示し、センターの承認を得ること。）。	本システムと同規模（端末 200 台程度かつ複数拠点）以上の情報システムの構築プロジェクトにおいて、実施責任者としての経験を有すること。
2	構築チームリーダ	以下の資格のいずれか一つ以上を有すること。 ① システムアーキテクト（IPA） ② ネットワークスペシャリスト（又は旧テクニカルエンジニア（ネットワーク））（IPA） ③ 情報処理安全確保支援士（又は情報セキュリティスペシャリスト、旧テクニカルエンジニア（情報セキュリティ））（IPA） ただし、IT スキル標準 V3 2011 に基づき、当該資格保有者等と同等の能力を有することを示した場合は、これを認める場合がある（その根拠を明確に示し、センターの承認を得ること。）。	本システムと同規模（端末 200 台程度かつ複数拠点）以上の情報システムの構築プロジェクトにおいて、チームリーダとしての経験を有すること。

3	構築チームリーダまたは構築チームメンバ	Microsoft Azure、AWS 等の IaaS アーキテクチャに関する上位資格（Microsoft Certified: Azure Solutions Architect Expert （AZ-305）等）のいずれか一つ以上を有すること。	本システムと同規模（端末 200 台程度かつ複数拠点）以上の情報システムのクラウド上での構築プロジェクトにおいて、チームメンバとしての経験を有すること。
4	移行・引継ぎチームリーダ	以下の資格のいずれか一つ以上を有すること。 ① システムアーキテクト（IPA） ② ネットワークスペシャリスト（又は旧テクニカルエンジニア（ネットワーク））（IPA） ③ 情報処理安全確保支援士（又は情報セキュリティスペシャリスト、旧テクニカルエンジニア（情報セキュリティ））（IPA） ただし、IT スキル標準 V3 2011 に基づき、当該資格保有者等と同等の能力を有することを示した場合は、これを認める場合がある（その根拠を明確に示し、センターの承認を得ること。）。	・本システムと同規模（端末 200 台程度かつ複数拠点）以上の情報システムの構築プロジェクトにおいて、チームリーダとしての経験を有すること。 ・本システムと同規模（端末 200 台程度かつ複数拠点）以上の情報システムのオンプレミスからクラウドサービスへの移行プロジェクトにおいて、チームリーダとしての経験を有すること。

※1 IPA：独立行政法人情報処理推進機構

※2 PMI：Project Management Institute

4.2.2. 第 2 期基盤情報システムの賃貸借及び運用保守業務

本システムの賃貸借及び運用保守業務に係る要件を以下に示す。

※2026 年 4 月 1 日～2031 年 3 月 31 日まで別途契約

表 4-4 作業要員に求める資格・経験等の要件（賃貸借及び運用保守業務）

No	要員	資格	経験等
1	実施責任者	以下の資格のいずれか一つ以上を有すること。 ① プロジェクトマネージャ（IPA※1） ② Project Management Professional（PMI※2） ただし、IT スキル標準 V3 2011 に基づき、当該資格保有者等と同等の能力を有することを示した場合は、これを認める場合がある（その根拠を明確に示し、センターの承認を得ること。）。	本システムと同規模（端末 200 台程度）以上の情報システムの運用保守プロジェクトにおいて、実施責任者としての経験を有すること。
2	運用保守チームリーダ	以下の資格のいずれか一つ以上を有すること。 ① システムアーキテクト（IPA） ② ネットワークスペシャリスト（又は旧テクニカルエンジニア（ネットワーク））（IPA） ③ 情報処理安全確保支援士（又は情報セキュリティスペシャリスト、旧テクニカルエンジニア（情報セキュリティ））（IPA） ④ IT サービスマネージャ（又は旧テクニカルエンジニア（システム管理））（IPA） ただし、IT スキル標準 V3 2011 に基づき、当該資格保有者等と同等の能力を有することを示した場合は、これを認める場合がある（その根拠を明確に示し、センターの承認を得ること。）。	本システムと同規模（端末 200 台程度）以上の情報システムの運用保守プロジェクトにおいて、チームリーダとしての経験を有すること。

※1 IPA：独立行政法人情報処理推進機構

※2 PMI：Project Management Institute

4.3. 作業場所

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

(イ) 本業務において実施する会議については、Web 会議又は東京本部で行うものとする。

4.4. 作業時間

(ア) センターの各拠点で定時時間外や休日の作業が必要となる場合は、センターと

協議し作業時間について合意を得た上で作業を行うこと。

4.5.　作業の管理に関する要領

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

(イ) 受注者は、「運用実施要領」及び「保守実施要領」に基づき、運用保守業務に係るコミュニケーション管理、体制管理、作業管理、リスク管理、課題管理、システム構成管理、変更管理、情報セキュリティ対策を行うこと。

(ウ) 受注者は、当該業務で納入又は更新する全てのソフトウェアの種類、バージョン及びサポート期間の終了日に係る情報並びにこれらの変更情報について、現在の状況を正確に反映した文書を整備すること。また、これらの内容に変更がある場合には文書を更新することで情報を提供すること。

5.　作業の実施に当たっての遵守事項

5.1.　機密保持、資料の取扱い

受注者は、機密保持や資料の取扱い等について、以下の措置を講ずること。

(ア) 業務上知り得た情報は、本業務以外の目的で利用しないこと。
(イ) 業務上知り得た情報について第三者への開示や漏えいをしないこと。
(ウ) 業務上知り得た情報は、センターの許可なく「5.3　作業場所」以外の場所に持出さないこと。
(エ) 受注者の責に起因する情報セキュリティインシデントが発生するなどの万一の事故があった場合、直ちにセンターに報告すること。また、受注者の責によりセンターに損害が生じた場合に賠償等の責任を負うこと。
(オ) 業務の履行中に受け取った情報の管理を行い、業務終了後は返却又は抹消等を行い、復元不可能な状態にすること。
(カ) 適切な措置が講じられていることを確認するため、遵守状況の報告を行うこと。また、必要に応じて行うセンターによる実地調査を受け入れること。

6. 納入物等の取扱いに関する事項

6.1. 知的財産権の帰属

本業務における知的財産権の帰属に係る要件を以下に示す。

(ア) 納入物に関する著作権、著作隣接権、商標権、商品化権、意匠権及び所有権（以下、「著作権等」という。）は、センターが保有するものとする。
(イ) 納入物に含まれる受注者又は第三者が権利を有する著作物等（以下、「既存著作物」という。）の著作権等は、個々の著作権者等に帰属するものとする。
(ウ) 納入物に既存著作物等が含まれる場合には、受注者が当該既存著作物の使用に必要な費用の負担及び使用許諾契約等に係る一切の手続を行うものとする。
(エ) 本業務の遂行に当たって、第三者が権利を有する著作権、知的財産権等を有するものを使用する場合は、受注者の責任において、その権利の使用に必要な費用の負担及び使用許諾契約等に係る一切の手続を行うこと。

6.2. 契約不適合責任

本業務における契約不適合責任に係る要件を以下に示す。

(ア) 受注者は、当該業務について仕様書及び契約内容等との不一致（以下「契約不適合」という。）が発見されたときは、センターの当該契約不適合にかかる請求に基づき、受注者の負担においてセンターが定めた期限までに、業務の再履行その他必要な措置を執らなければならない。
(イ) 前項の請求は、センターが当該契約不適合を知ったときから1年以内に不適合の内容を受注者に通知する。ただし、当該契約不適合を知った時から1年以内に不適合の内容を受注者に通知する。ただし、当該不適合を知った時から5年を経過した場合もしくは検収後10年を超えて発見された契約不適合は除く。

6.3. 検収

本業務における検収について以下に示す。

(ア) 本業務の受注者は、「4.3 納入物等の範囲、納入期日等」に示す納入物等の完納及び内容の確認をもって検収とする。
(イ) 検収の結果、納入物等に不備又は誤り等が見つかった場合には、直ちに必要な修正、改修、交換等を行い、変更点についてセンターに説明を行った上で、指定された日時までに再度納入すること。

7. 入札参加資格に関する事項

7.1. 入札参加要件

本調達における入札への参加要件について以下に示す。

7.1.1. 業務に必要な資格等

(ア) 品質管理体制について、ISO9001 又は CMMI のレベル 3 以上の認定を受けていること（当該認定を受けていることが確認できる認証の写し等を提出すること。）。なお、事業部単位で認定を受けている場合は、当該事業部が本業務の実施体制に参画することができることを確認できる書類を含むこと。

(イ) 情報セキュリティの徹底を図る観点からISO/IEC27001の認定を受けていること（当該認定を受けていることが確認できる認証の写し等を提出すること。）。なお、事業部単位で認定を受けている場合は、当該事業部が本業務の実施体制に参画することができることを確認できる書類を含むこと。

(ウ) プライバシーマークの使用許諾又は個人情報保護マネジメントシステム（JIS Q 15001）の認定を受けていること（当該認定を受けていることが確認できる認証の写し等を提出すること。）。

7.1.2. 受注実績

(ア) 本システムと同等規模以上のゼロトラストを前提としたネットワークサービスの構築実績を有すること。

(イ) 本システムと同等規模以上の統合認証サービス（Microsoft Entra ID）の構築実績を有すること。（※Azure Active Directory の構築実績も同等の実績として認める。）

(ウ) 本システムと同等規模以上のオンプレミス環境をクラウドに移行した実績を有すること。

(エ) 上記の実績は同一調達における実績であっても、複数調達の実績であってもよい。

8. 再委託に関する事項

8.1. 再委託の制限及び再委託を認める場合の条件

(ア) 本業務の受注者は、業務の全部又は以下に示す各部分を一括して再委託してはならない。

- ✓ 設計・構築実施計画書等の作成
- ✓ 設計
- ✓ 導入設置計画書の作成
- ✓ 移行計画書の作成
- ✓ 運用計画及び運用実施要領の作成
- ✓ 保守計画及び保守実施要領の作成

(イ) 受注者における統括責任者及び実施責任者を再委託先事業者の社員や契約社員とすることはできない。

(ウ) 受注者は再委託先の行為について一切の責任を負うものとする。

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

8.2. 承認手続

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

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

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

8.3. 再委託先の契約違反等

(ア) 再委託先において、本調達仕様書の「9.1.再委託の制限及び再委託を認める場合の条件」から「9.2.承認手続」に定める事項に関する義務違反又は義務を怠った場合には、受注者が一切の責任を負うとともに、センターは、当該再委託先への再委託の中止を請求することができる。再々委託先についても同様とする。

9. その他特記事項

(ア) 本調達案件で調達する、端末、ネットワーク機器等について、賃貸借期間終了後にセンターが希望する場合、買取りを可能とすること。

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

10. 附属資料

① 別紙 1 要件定義書

② 閲覧要領

閲覧対象とする資料は以下のとおり。

- センターの情報セキュリティポリシー、情報管理規程、情報管理要領
- 保守業務の実績とりまとめ
- サーバ利用状況確認結果
- 以下の契約に関する成果物等一式
  - 2017 年度システム再構築に向けた構想策定及び要件定義等支援業務
  - 2018 年度次期基盤情報システムの構築に係る工程管理等支援業務
  - 2018 年度次期基盤情報システムの構築及び機器等の賃貸借・保守業務(保守業務月次報告書一式含む)
  - 2021 年度基盤情報システム(オープン環境)のデータセンターへの移設作業
  - 2022 年度基盤情報システムの更新に向けた検討業務
  - 2023 年度基盤情報システムの更新に向けた要件定義等支援業務

別紙 1

第 2 期基盤情報システムの構築及び移行業務

要件定義書

2025 年度

公益財団法人　核物質管理センター

― 目次 ―

1. 業務要件の定義

本章では、第 2 期基盤情報システム（以下「本システム」という。）を用いて実施する、公益財団法人核物質管理センター（以下「センター」という。）の業務等に関する要件を定義する。

なお、本システムはセンターの業務全般を支える情報インフラ基盤を提供するためのシステムであるため、特定の個別業務システムについては定義の対象外とする。

1.1. 業務概要

本システムを利用して実施する主な業務の概要は以下のとおりである。なお、個別業務の概要については定義しない。

表 1-1 業務概要一覧

No.	業務分類	主な業務の概要
1	文書作成及び管理	・ ワードプロセッサ、表計算ソフトウェア、プレゼンテーションソフトウェア等による文書作成、編集、閲覧等を行う。 ・ 文書等の電子ファイルの保管、共有、権限設定、その他必要な管理等を行う。
2	情報共有及びコミュニケーション	・ 電子メール、グループウェア、ファイル共有等のツールを用いて、役職員間又は外部関係者との連絡、情報共有等を行う。
3	ウェブサイト等の利用	・ インターネット・イントラネット上のウェブサイト等を閲覧、利用する。
4	個別業務システムの利用	・ 本システムと接続した既存システム（以下、「個別業務システム」という。）を利用して業務を行う。

1.2. 時期・時間

本システムの稼働時間及びセンターの役職員が業務で利用する時間や繁忙期等の特徴を以下に示す。

表 1-2 時間・時期

No.	項目	説明
1	本システムの稼働時間	・ 24 時間 365 日とする。ただし、運用保守作業、法定点検による停電及び大規模災害時による停止時間を除く。
2	本システムの利用時間やセンターの繁忙期等	・ 主に平日 9 時 00 分～17 時 30 分において利用されるが、時間外の利用も存在する。 ・ 本システムは年間を通じて利用される。 ・ 主に 4 月に大規模な人事異動がある。

1.3. 規模

センターの業務に関する規模等を、業務の拠点別に以下に示す。

表 1-3 東京本部の規模等

No.	項目	規模
1	利用者数	約 35 名
2	端末数	約 40 台
3	室数	6 室

表 1-4 東海保障措置センターの規模等

No.	項目	規模
1	利用者数	約 100 名
2	端末数	約 100 台
3	室数	15 室

表 1-5 六ケ所保障措置センターの規模等

No.	項目	規模
1	利用者数	約 60 名
2	端末数	約 70 台
3	室数	8 室

1.4. 場所等

1.4.1. 業務の実施場所

センターの業務において本システムを利用する場所及びネットワーク接続環境を以下に示す。

表 1-6 場所等

No.	場所名	住所等
1	東京本部	東京都台東区東上野 1-28-9
2	東海保障措置センター	茨城県那珂郡東海村白方白根 2-53
3	六ケ所保障措置センター	青森県上北郡六ヶ所村大字尾駮字野附 504-36
4	自宅(テレワーク)	-
5	受注者の運用保守拠点	-

1.4.2. 諸設備・物品等

本システムに関連する諸設備については、「表 1-9 調達範囲外の機能・設備等」を参照すること。

1.5. 管理すべき指標

本システムを整備し運用管理・監視する上で、管理すべき指標を以下に示す。

表 1-7 管理すべき指標

No.	指標の種類	指標名	計算式	目標値	計測方法
1	情報セキュリティ対策	重大な情報セキュリティインシデントの件数	サイバー攻撃によるシステム停止を伴う障害、端末感染による情報漏えい等の発生件数(年間)	0 件	運用保守作業報告
2	情報システム性能指標	稼働率	「月間実稼働時間」／「月間予定稼働時間」×100	99.9%(※)	運用保守作業報告

※SaaS の稼働率はクラウドサービス事業者の目標値に準ずるため、当該目標値の対象外とする。

1.6. 情報システム化の範囲

本システムにより情報システム化を行う機能の範囲及び調達対象外とする機能・設備等を以下に示す。

表 1-8 情報システム化の範囲（機能一覧）

No.	分類	機能
1	ネットワークサービス	LAN サービス
2		テレワークサービス
3		WAN サービス
4		インターネットサービス
5	基盤サービス	統合認証サービス（DNS、NTP サービス含む）
6		Windows アップデート管理サービス
7		ファイル共有サービス
8		メールサービス
9		端末管理サービス
10		システム運用管理・監視サービス
11		バックアップ管理サービス
12		ログ管理サービス
13		ウイルス対策管理サービス
14		クラウドプロキシサービス
15		クラウド認証サービス
16		Web 分離サービス
17	端末サービス	職員用端末
18		ウイルススキャン端末 ※
19		運用支援端末(受注者で準備も可)
20	その他	グループウェアサービス※

※既存環境を使用し必要に応じて別途調達予定のため本調達対象外とする。

表 1-9 調達範囲外の機能・設備等

No.	分類	機能等
1	会議室設備	Web 会議用スピーカーフォン
2		Web 会議用カメラ
3	執務室設備	ネットワークプリンタ
4		FAX

1.7. 業務の継続の方針等

業務継続の方針等については、以下の資料を参照すること。

- 「事業継続ガイドライン」（令和 5 年 3 月内閣府策定）
- 「公益財団法人核物質管理センター事業継続計画書」

これら業務継続の方針等を踏まえて、本システムの運用開始までに、定常時のサイバー攻撃等及び非常時の大規模災害等に備えたネットワーク復旧のための具体的な計画と手段を本システムの運用継続計画として整備すること。随時、本システムの継続を脅かすリスクを評価し、適切な対策を実施すること。また、今後、業務継続ガイドライン等が改訂された際には、センターと協議の上、改訂後の業務継続計画等に準拠した対応を行うこと。

1.8. 情報セキュリティの方針

1.8.1. 準拠すべき方針等

情報セキュリティの方針は以下の文書に準拠すること。具体的な情報セキュリティに関する要件は、「3.9. 情報セキュリティに関する事項」を参照すること。なお、本要件定義書の策定後に各文書の改訂が行われた場合には、原則として最新版への準拠を求めるが、やむを得ず対応が難しい場合にはセンターと協議の上で対応方針を定めること。

1.8.1.1. 準拠文書

- 「情報セキュリティ関係規程」（以下の 3 点の文書を指す）
  - 「センター情報セキュリティポリシー」
  - 「情報管理規程」
  - 「情報管理要領」

1.8.1.2. 参考文書

- 「政府機関等のサイバーセキュリティ対策のための統一基準群（令和 5 年度版）」（以下「統一基準群」という。）
- 「政府情報システムにおけるクラウドサービスの適切な利用に係る基本方針（2023 年（令和 5 年）9 月 29 日デジタル社会推進会議幹事会決定）」（以下「クラウド方針」という。）
- 「ゼロトラストアーキテクチャ適用方針（令和 4 年 6 月 30 日）」（以下「ゼロトラスト適用方針」という。）

2. 機能要件の定義

2.1. 機能に関する事項

2.1.1. サービス一覧

本システムにおいて、提供を求めるサービスの一覧を以下に示す。

表 2-2-1 第 2 期基盤情報システムのサービス一覧

No.	分類	サービス名	サービスの概要
1	ネットワークサービス	LAN サービス	各拠点内の PC 端末、システム等が接続するための LAN 回線及び無線 LAN 環境を提供する。 ※無線 LAN アクセスポイントまでの配線は閲覧資料「既存のネットワークに係る資料一式」を参照の上、現行システムを流用することも可能
2		WAN サービス	各拠点の LAN を相互接続するために WAN 環境を提供する。
3		テレワークサービス	外部から本システムに接続するための環境を提供する。
4		インターネットサービス	各拠点内の PC 端末がインターネット及びクラウドサービスに接続するためのインターネットサービスを提供する。
5	基盤サービス	統合認証サービス	Active Directory による統合認証サービスを提供する。また、時刻サービスを提供する。
6		Windows アップデート管理サービス	Windows 及びオフィススイートソフトウェアの更新サービスを提供する。
7		ファイル共有サービス	役職員向けのファイル共有機能を提供する。
8		端末管理サービス	本システムの各端末の一元管理機能（情報資産管理、構成管理、デバイス管理等）及びウイルス対策ソフトウェアの管理機能を提供する。
9		システム運用管理・監視サービス	本システムのハードウェア、ソフトウェア及びネットワークの統合運用管理・監視機能を提供する。
10		バックアップ管理サービス	本システムの各サービスのバックアップを一元管理するための機能を提供する。
11		ログ管理サービス	本システムの各機器が出力するログの管理機能を提供する。
12		ウイルス対策管理サービス	本システムの各サーバおよび端末のウイルス対策ソフトウェアの管理機能を提供する。
13		クラウドプロキシサービス	本システムのクラウドプロキシ機能を提供する。
14		メールサービス	Microsoft365 の Exchange Online を提供する。

No.	分類	サービス名	サービスの概要
15		クラウド認証サービス	Microsoft Entra ID によるクラウド認証サービスを提供する。
16		Web 分離サービス	インターネットを閲覧する際にリモートブラウザ（RBI）機能を提供する。
17	端末サービス	職員用端末	センターの全役職員に配付する端末を提供する。
18		ウイルススキャン端末	USB メモリや光学メディア等からデータの読込みを行う際のウイルススキャンを行うための端末を提供する。 ※既存環境を使用し別途調達予定のため本調達対象外とする
19		運用支援端末	受注者が本システムを運用管理・監視するための端末を提供する。
20	その他	ネットワークプリンタサービス	ネットワークに接続された端末から文書を印刷する機能を提供する。 ※ネットワークプリンタのハードウェアの調達は対象外だが、対象機器の設定等は実施すること

2.1.2. サービスの機能要件

2.1.2.1. ネットワークサービス

本システムのネットワークサービスは、以下の要件を満たすこと。

(1) LAN サービス

(ア) 本システムの職員用端末、運用支援端末並びにセンターの各課室が所管する個別業務システムが相互に接続するための LAN 機能及び無線 LAN 機能を提供すること。

(イ) LAN サービスとして備える機能の詳細については、「3.10.4.2 ネットワーク要件」を参照すること。

(2) WAN サービス

(ア) 東京本部、東海保障措置センター、六ケ所保障措置センターの各拠点を、インターネット回線を経由した SSL-VPN 等により接続すること。センターが指定する IPv4 プライベート IP アドレスが各拠点内で制限なく使用できること。

(イ) 通信先に応じて通信を分割するスプリットトンネリング機能を有すること。これにより、WAN サービスを経由する必要のない通信（一般 Web サイト向け通信、各種クラウドサービス向け通信等）についてはローカルブレイクアウトを実現すること。

(ウ) ネットワークの以下の項目を変更できること。

・ プライベート IP アドレス
・ ダイナミックルーティングプロトコル
・ VLAN
・ アクセス制御リスト
・ 帯域制御

(3) テレワークサービス

(ア) 出張時やテレワーク時において、各拠点内の個別業務システムを利用する際に、インターネット回線を経由した SSL-VPN 等により、職員用端末を本システムに接続できること。

(イ) 通信先に応じて通信を分割するスプリットトンネリング機能を有すること。これにより、テレワークサービス利用中であっても、LAN サービスを経由する必要のない通信（一般 Web サイト向け通信、各種クラウドサービス向け通信等）についてはローカルブレイクアウトを実現すること。

(ウ) 頻繁な切断やタイムアウト、レスポンスの悪化等が生じにくい技術方式等を選択すること。

(エ) 出張時やテレワーク時に最大 30 人の利用者が、同時接続可能であること。また、SSL-VPN 等においては通信品質を劣化させないだけのリソースを割り当てること。

(4) インターネットサービス

(ア) 回線帯域については、本要件定義書の各要件を満たすことを前提に、受注者が提案するシステム構成及び採用する製品に応じて、必要十分な回線帯域を提案すること。また、帯域確保型とベストエフォート型を組み合わせたバーストタイプのサービスを提案してもよい。なお、現行のインターネット接続回線の帯域は、2Gbps（ベストエフォート型）である。

(イ) 回線帯域等の提案に当たっては、製品仕様、他組織での事例等を踏まえ、実現性が高く、かつ過剰な構成を避けた提案を行うこと。また、設計段階において必要に応じて実測や検証等を行った上で、サイジングの精緻化を行うこと。

(ウ) トラフィックグラフを Web 上で参照できること。また、当該 Web へのアクセスには、アクセス制限機能を有すること。

(エ) トラフィックの情報は、過去 1 か月以上保存し、任意の期間のトラフィックを抽出できること。

(オ) トラフィックの情報は、ダウンロードし、センターが保存できること。

(カ) 任意の期間のトラフィックデータを数値データ化した CSV ファイルが出力可能であること。

2.1.2.2. 基盤サービス

本システムの基盤サービスは、以下の要件を満たすこと。

(1) 統合認証サービス

(ア) 以下の要件を満たす「統合認証サービス」を提供すること。

- Active Directory による利用者アカウント管理ができること。
- 端末ログイン時の認証管理ができること。
- ログインパスワードポリシー（長さや文字種、有効期限等）の設定ができること。
- 端末におけるユーザ権限の制御・管理ができること。
- 定義されたポリシーに基づき、利用者の登録や属性変更を、自動的に宛先のシステムに反映するためのプロビジョニング機能を有すること。
- アカウント情報やポリシーの追加・変更・削除等、重要な操作を監視ログに記録ができること。
- アカウント情報やポリシーの設定は、既存の認証サーバの設定情報をもとに受注者が設計し、センターと協議の上で決定すること。なお、既存の認証サーバの機器構成等は、閲覧資料「情報システムの資産管理情報等の調査および資料作成助成等業務　成果物一式」を参照すること。
- アカウント情報やポリシーの追加・変更・削除等を一元的に行うことが可能なこと。
- 可能な限り認証を意識せず各機能を利用可能なこと。
- 「ファイル共有サービス」の認証及びアクセス権限の設定・管理ができること。
- 「端末管理サービス」との連携が可能であること。
- 内部 DNS サービスを提供すること。
- 時刻同期サービスを提供すること。
- 役職員がテレワーク環境から直接本システムのクラウドサービスを利用できるように、認証情報や利用者アカウント情報を、後述の「クラウド認証サービス」と過不足なく連携する機能を有すること。
- 認証情報の同期に当たっては、直接パスワードを同期させずに、パスワードのハッシュ値を同期するなどの方式とすること。
- 職員用端末へのログイン時に、クラウド認証サービスに対しても自動的にシングルサインオンを行う「シームレスシングルサインオン（sSSO）」ができること。

(2) Windows アップデート管理サービス

(ア) Windows 及びオフィススイートソフトウェアの更新プログラムの適用（適用対象更新プログラムの指定、適用日時の指定等）を一元管理できること。

(イ) テレワーク時など端末が外部にある状態であっても、インターネットを経由して職員用端末のアップデート管理を可能とすること。

(ウ) ウイルススキャン端末はスタンドアロンのため、USB メモリを用いてアップデートするが、詳細については運用設計によるものとする。

(3) ファイル共有サービス

(ア) 利用者間で、電子ファイルを共有するためのファイル共有サービスを提供すること。
(イ) 職員用端末の OS 標準のファイル管理ソフトウェアからアクセスできること。
(ウ) ファイルサーバ全体として15TB 以上のデータ（電子ファイル）を格納可能な容量を提供すること。
(エ) アクセスログを記録し、不正アクセス等の分析を行うためのログ情報を出力できること。
(オ) 格納するデータは暗号化できること。
(カ) 「統合認証サービス」と連携し、フォルダ単位、ユーザ単位、ユーザグループ単位等によるアクセス制御ができること。
(キ) ストレージの利用容量管理のために、利用者又は共有フォルダ単位で、使用できるストレージ容量に制限をかけることができること。

(4) メールサービス

(ア) 役職員同士及び外部との連絡のために利用するためのメールサービスを提供すること。
(イ) メールアカウントは最大 210 アカウントを提供可能とすること。
(ウ) 1 メールアカウントあたりのメールボックス容量の上限は、100GB 以上とすること。
(エ) メールボックスの容量がしきい値に近づいた場合には、利用者への通知を可能とし、しきい値に達した場合はメールの送受信に制限を行う等の段階的な制限設定が可能であること。
(オ) 電子メールクライアントからメールの送信及び送受信ができること。
(カ) 電子メールクライアントの送受信要求は MAPI に対応すること。
(キ) メール形式は、テキスト形式のメールのほか、HTML 形式のメールにも対応すること。
(ク) メールの宛先や内容により分類して整理できること。また、メールを配信するフォルダは階層的に作成でき、条件を指定して参照したいメールを検索できること。
(ケ) フォルダに対して送信者、主題中のキーワードをもとにメールの自動振り分けを行う機能を有すること。メールを振り分けるアドレスやキーワードは、利用者が複数指定できること。
(コ) アドレス帳には、ユーザ名（日本語、ローマ字）、電子メールアドレス、組織名等の情報が設計可能であること。また、「統合認証サービス」で管理する情報と連携可能であること。

(5) 端末管理サービス

(ア) 職員用端末、ウイルススキャン端末及び運用支援端末（以下、総称して「PC 端末」という。）に対し、以下の管理機能を提供すること。

- PC 端末のハードウェア情報（コンピュータ名、ホスト名、ログオンユーザ名など）及びソフトウェア情報（各ソフトウェアのインストール状況等）の一元管理を行うための、資産管理機能を有すること。
- PC 端末のソフトウェア資産（アップデートパッチ等も含む。）の管理・配付・棚卸し等を行うためのソフトウェア資産管理機能を有すること。
- USB メモリ等の外部電磁的記録媒体の接続制限・管理や、ファイル書き出し時の自動暗号化を制御するためのデバイス管理機能を有すること。
- PC 端末のログを収集・管理するための端末ログ管理機能を有すること。

(イ) PC 端末に搭載されるウイルス対策ソフトウェアに対し、以下の管理機能を提供できること。

- PC 端末のウイルス対策ソフトウェアの状態管理が可能であること。
- PC 端末のウイルス対策ソフトウェアへのウイルス定義ファイルの配信・更新が可能であること。

(6) システム運用管理・監視サービス

(ア)「3.16. 運用に関する事項」に示す本システムの運用作業を可能とするため、以下の機能を提供すること。なお、システム運用管理・監視サービスの管理対象は、本業務において調達する機器のみとする。また、各監視機能の設定値（アラートを通知するしきい値等）は受注者が設計し、センターと協議の上で定めるものとする。

- ポーリング、SNMP、ログ監視、プロセス管理等によるクラウドサービス、ハードウェア及びソフトウェアプロセスに対する死活監視機能
- CPU 使用率、メモリ使用率、ストレージ空き容量等のリソース監視機能
- 本システムの各サーバのイベントログの監視及びネットワーク機器の syslog 監視を行うことにより、ファイアウォールのブロック発生状況、「統合認証サービス」の認証失敗状況、不正プログラム検知状況のセキュリティ監視を行う。
- 東京本部及び受注者の運用保守拠点より全拠点の PC 端末のデスクトップ画面を確認可能とする。
- マルチベンダネットワーク機器のコンフィグファイルの管理及び世代管理を可能とする。
- ネットワーク機器のポート状態が監視可能とする。
- クラウドサービスの監視については、クラウドサービスが提供する API やダッシュボード等を活用した稼働状況監視ができることが望ましい。

(7) **バックアップ管理サービス**

(ア)「3.8 継続性に関する事項」に示す、本システムのバックアップ（業務データのバックアップ及びシステムバックアップ）をスケジューリング等により自動化・管理するための機能を提供すること。

(イ) 具体的なバックアップ方法、タイミングについては運用設計にて決定する。

(ウ) リストア手順については、運用設計にて決定する。

(8) **ログ管理サービス**

(ア) 本システムのクラウドサービス、サーバ、ネットワーク機器及び端末における、システムログ、メール送信ログ、Web アクセスログ、ファイル操作等のログを収集、保管する機能を有すること。

(イ) 管理対象のサーバから自動出力されたログを一元管理できること。

(ウ) 収集したログに対して統計的な集計・分析を行い、グラフ等により結果を出力できる機能を有すること。

(エ) ログを収集・長期保存・アーカイブができ、必要に応じて閲覧できる機能を有すること。なお、各ログは最低 1 年間の保存が可能であること。

(オ) ログの検索・集計結果は、CSV 形式又は PDF 形式で出力する機能を有すること。

(9) **ウイルス対策管理サービス**

(ア) 基本機能

- 本システムの各サーバ及び PC 端末に搭載されるウイルス対策ソフトウェアに対し、以下の管理機能を提供する。
- ウイルス対策ソフトウェアの状態（適用状況、ウイルス定義ファイル更新状況等）を確認する。
- ウイルス対策ソフトウェアへのウイルス定義ファイルの配信・更新をする。
- クラウドサービスや管理サーバから PC 端末に対してウイルススキャンの実行や、ウイルス定義ファイルの更新を可能とする。
- ウイルス定義ファイルの配信方法については運用設計によるものとする。
- ウイルススキャン端末はスタンドアロンのため、USB メモリを用いてウイルス定義ファイルを更新するが、詳細については運用設計によるものとする。

(イ) 不正プログラム対策機能

- 職員用端末、サーバ等のエンドポイントにおいて、既知及び未知の不正プログラムの検知及びその実行の防止のための機能を提供すること。
- 未知の不正プログラムに対しては、シグネチャに依存しない検知技術（OS のプロセスやメモリ、レジストリへの不正なアクセスや書き込み等を監視・検知する方式等）を採用すること。また、エンドポイントでの不正プログラム対策に加えて、クラウドプロキシやファイアウォール等によるゲートウェイ型の対策を組み合わせることが望ましい。

・ エンドポイントにおいて検知した不正プログラムを除去する機能を有すること。また、クラウドサービス内での不正プログラム検知については、検知した不正プログラムを早期に隔離し、ダウンロードを制限するなど、職員用端末の感染を防止するための機能を備えること。
・ 不正プログラムの検知時に、各端末のログから侵入経路や影響範囲の特定を行うための調査・分析機能を有すること。
・ 定期フルスキャン設定を有効とすること。
・ 自動検査機能を有効とし、利用者が停止できない設定とすること。

(ウ) 脅威ハンティング機能
・ ハッシュ値により職員用端末内のファイルを検出する機能を有すること。また、ハッシュ値以外にも、職員用端末の様々な情報（プロセス、通信状態、レジストリ値等）を検索できることが望ましい。
・ 脅威ハンティング機能は、SHA256 のハッシュ値に対応すること。
・ 脅威ハンティング機能により検出した端末に対して、隔離やプロセス停止・削除等の対応を容易に実行できることが望ましい。
・ 脅威ハンティングによる検知結果（検知端末数等）を出力できること。
・ レポート機能（検出した検体及びその検体の挙動の調査結果等の出力）を有すること。
・ 運用負荷軽減の観点から、STIX/TAXII 方式により、指定したクラウドサービス、サーバ、機器等から自動的にハッシュ値を取り込めることが望ましい。

(10) **クラウドプロキシサービス**
(ア) 職員用端末や各拠点内の機器がインターネットに接続する際のプロキシ機能を提供すること。または、SASE、クラウドファイアーウォール等のインターネットに接続する際に、代理で外部（インターネット）にアクセスする機能を有すること。
(イ) テレワーク等を想定し、職員用端末が LAN サービスに接続されていない状態においても適用される方式とすること。
(ウ) 外部 Web サイト閲覧等の際の HTTP パケットに対してウイルススキャンを行う機能を有すること。
(エ) URL カテゴリフィルタリング機能を有すること。
(オ) SSL 復号化及び再暗号化機能を有すること。
(カ) URL や IP アドレス等のレピュテーション情報をもとに既知の脅威からの保護機能を有すること。
(キ) ファイルタイプに基づくアップロード・ダウンロード等の制御機能を有すること。
(ク) クラウドサービスのドメイン及び IP アドレスが不定期に変更される可能性があることを考慮し、URL リストの自動更新機能を有すること。

(11) **クラウド認証サービス**

(ア) クラウドサービスを利用する際の認証基盤として利用できること。

(イ) Microsoft 365、その他 SaaS 等のインターネット経由で利用する機能・サービスに対する IdP（Identity Provider）として、フェデレーション認証を提供できること。

(ウ) 利用者のアカウント情報（利用者アカウント ID 等の認証情報、グループ/所属部署等の属性情報等）を一元的に管理できること。

(エ) アカウント情報は、「統合認証サービス」との連携により同期できること。認証情報の同期に当たっては、パスワードのハッシュ値を同期する方式とすること。

(オ) テレワーク時など外部からのアクセスに対しては、知識認証及び所有認証を組み合わせた認証（以下「多要素主体認証」という。）を求めること。

(カ) アクセス元のユーザ利用者アカウント、デバイス、ネットワーク等の状態に応じて、Microsoft 365、その他 SaaS 等のインターネット経由で利用する機能・サービスに対するアクセス可否を制御できること。

(キ) 管理者が利用者の認証アクセス状況をレポートとして確認することができること。

(ク) 主要な機能をブラウザで管理できること。また、特殊な機能の設定及び一括処理をする際には、PowerShell や API を使用したプログラム等からの管理ができること。

(12) Web **分離サービス**

(ア) インターネット等を閲覧する際に、PC 端末上に情報を保存することなく、画面転送等を介して、PC 端末内のブラウザ等から閲覧できること。また、閲覧終了時に当該データを端末に残さないこと。

(イ) ブラウザ終了時に閲覧に関連する情報（ウェブキャッシュ、URL、cookie 等）を消去できること。

2.1.2.3. 端末サービス

本システムの端末サービスは、以下の要件を満たすこと。

(1) **職員用端末**

(ア) 職員用端末において備える機能については、「3.10.2 ハードウェア構成」及び「3.10.3 ソフトウェア構成」を参照すること。

(イ) PC 端末のハードウェア情報（コンピュータ名、ホスト名、ログオンユーザ名など）及びソフトウェア情報（各ソフトウェアのインストール状況）を一元管理する。

(ウ) PC 端末のソフトウェア資産（アップデートパッチも含む。）の管理・配付・棚卸しを管理する。

(エ) USB メモリ等の外部電磁的記録媒体の接続制限・管理や、ファイル書き出し時の自動暗号化を制御する。
(オ) PC 端末のログを収集・管理する。

(2) **ウイルススキャン端末**

(ア) ウイルススキャン端末は、既存の端末を利用すること。
(イ) PC 端末のハードウェア情報（コンピュータ名、ホスト名、ログオンユーザ名など）及びソフトウェア情報（各ソフトウェアのインストール状況）を一元管理する。
(ウ) PC 端末のソフトウェア資産（アップデートパッチも含む。）の管理・配付・棚卸しを管理する。
(エ) USB メモリ等の外部電磁的記録媒体の接続制限・管理や、ファイル書き出し時の自動暗号化を制御する。
(オ) PC 端末のログを収集・管理する。

(3) **運用支援端末**

(ア) 本システムの職員用端末を統合管理するための「端末管理サービス」のクライアント機能を提供すること。
(イ) 本システムのサーバ、ネットワーク機器の運用を統合管理するための「システム運用管理・監視サービス」のクライアント機能を提供すること。
(ウ) 本システムのバックアップを統合管理するための「バックアップ管理サービス」のクライアント機能を提供すること。
(エ) 本システムのログを統合管理するための「ログ管理サービス」のクライアント機能を提供すること。
(オ) PC 端末のハードウェア情報（コンピュータ名、ホスト名、ログオンユーザ名など）及びソフトウェア情報（各ソフトウェアのインストール状況）を一元管理する。
(カ) PC 端末のソフトウェア資産（アップデートパッチも含む。）の管理・配付・棚卸しを管理する。
(キ) USB メモリ等の外部電磁的記録媒体の接続制限・管理や、ファイル書き出し時の自動暗号化を制御する。
(ク) PC 端末のログを収集・管理する。

なお、運用支援端末については、上記要件に加えて、以下の要件を満たすことで、受注者が用意する端末を運用支援端末として利用することを提案してもよい。

(ケ) 「3.9. 情報セキュリティに関する事項」の各要件と同等以上の情報セキュリティ対策が実施されていること。

(コ) 原則として、「3.10.3. ソフトウェア構成」の各要件を満たすこととし、本システムの運用保守業務を実施する上で必要となるアプリケーション等がある場合、センターの承認を得ること。
(サ) 本システムの運用保守業務以外の目的で利用しないこと。
(シ) 受注者の運用保守拠点からのみ利用可能とすること。
(ス) アクセスログ及び操作ログ（画面録画）を取得すること。
(セ) シンクライアント等の端末に情報を保存させないリモート接続環境を構築すること。
(ソ) 本システムの運用保守目的で構築したリモート接続環境が、本システム全体のセキュリティホールとならないように、不正プログラム対策、サービス不能攻撃対策、標的型攻撃対策等の情報セキュリティ対策を講じること。

2.2. 情報・データに関する事項

本システムにおいて取り扱う情報・データの一覧を以下に示す。

表 2-2-2 データ一覧

No.	データ名	データ概要	該当サービス
1	電子メールデータ	・ センターの業務において送受信される電子メールデータ。	メールサービス
2	共有ファイルデータ	・ センターの業務において管理・保有される業務データ（Word ファイル、Excel ファイル、PDF ファイル等）。	ファイル共有サービス
3	ログデータ	・ 本システムを構成するクラウドサービス、サーバ、ネットワーク機器及びソフトウェア製品から出力されるログデータ（ソフトウェアログ、証跡管理用ログ、性能情報等）。 ・ 上記ログデータのアーカイブデータ	ログ管理サービス
4	バックアップデータ	・ 本システムで管理・保有される業務データのバックアップ（電子メールデータ、共有ファイルデータ、統合認証サービスのディレクトリ情報等）。 ・ IaaS環境の切り戻し、ハードウェアの交換時等における迅速な復旧を可能とするためのシステムバックアップ（各サーバのシステムバックアップ、各ネットワーク機器の設定情報等）。 ・ 職員用端末のキッティング用のマスタイメージ	バックアップ管理サービス
5	その他データ	・ No.1～4 以外のその他データ（各種基盤サービスの設定情報等）。 ※ 受注者の設計による	全般

3. 非機能要件の定義

3.1. システム方式に関する事項

本システムにおけるシステム方式（全体の方針、全体構成）を以下に示す。

3.1.1. 情報システムの構成に関する全体の方針

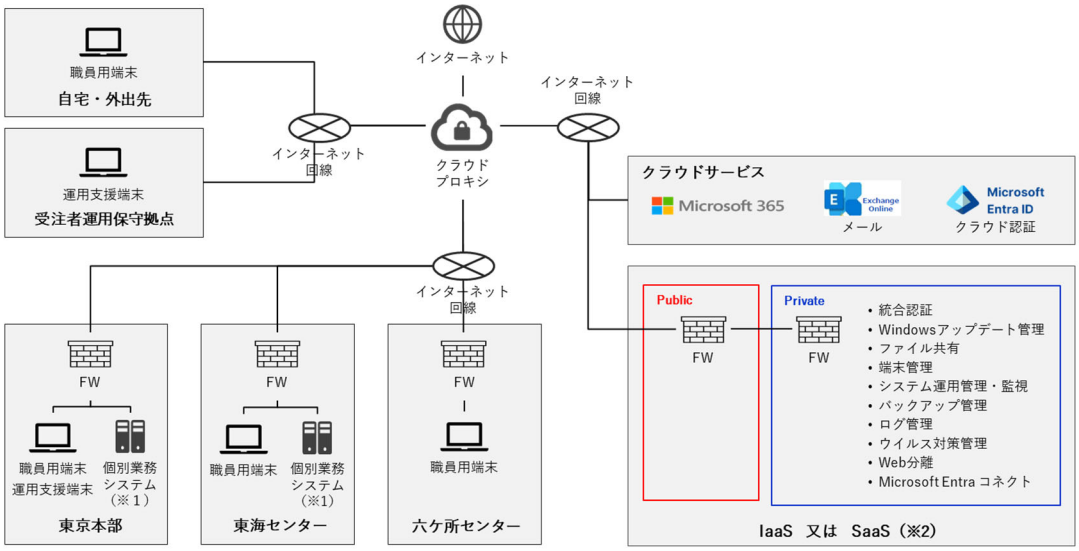
本システムのシステム構成に関する全体方針を以下に示す。

表 3-1 情報システムの構成に関する全体方針

No.	分類	全体方針
1	システム基盤の方針	本業務において、センターにおける新たな情報システム基盤を再構築する。
2		以下の基盤サービスは、既存のシステム・機器を継続利用し、本システムが提供するネットワークに配置する。 ・ グループウェアサービス ・ ネットワークプリンタ
3	ソフトウェア製品の活用方針	広く市場に流通し、利用実績を十分に有するソフトウェア製品を活用する。
4		導入するソフトウェア製品は、バージョン等を指定したもの以外、原則として最新のバージョンとする。
5	クラウドサービスの活用方針	本システムはクラウドネイティブの構成として、「クラウド方針」に準拠し、クラウドサービスの提供機能を最大限活用するようデザインされたアーキテクチャとすること。特に、信頼性、拡張性、継続性等の向上に寄与するクラウドサービスと構成を選定すること。なお、各サービスにおいて要件を満たす最適な提案が可能な場合は、オンプレミスを含めたハイブリッド構成とする提案を妨げるものではない。
6	情報セキュリティの方針	従来のオープン系・クローズド系で構成していた仮想分離を廃止し、「ゼロトラスト適用方針」に準拠したネットワークを構築する。
7	個別業務システムの移行方針	各課室が個別に管理・運用している情報システムは、本システムが提供するネットワークに配置する。

3.1.2. 情報システムの全体構成

本システムの全体構成図（概要図）を以下に示す。



※1　個別業務システムは本調達の範囲外となるが、個別業務システムとの接続までは実施する。
※2　クラウド化した際と同等レベルの機能やセキュリティを維持できるのであれば、一部機能をオンプレミス上に構成する提案を妨げるものではない。

図 3-1　本システムの全体構成図（概要図）

3.1.3. クラウドサービスの選定、利用に関する要件

本システムにおいて、クラウドサービスを選定、利用する場合の要件を以下に示す。

(ア) セキュリティ確保のため、本システムで用いるクラウドサービスは、原則として ISMAP クラウドサービスリストまたは ISMAP-LIU クラウドサービスリストに登録されているクラウドサービスを選定すること。なお、例外的に ISMAP クラウドサービスリスト、または ISMAP-LIU クラウドサービスリストに登録されていないクラウドサービスを選定する場合は、受注者の責任において、当該クラウドサービスが「ISMAP 管理基準」の管理策基準における統制目標（3 桁の番号で表現される項目）及び末尾に B が付された詳細管理策（4 桁の番号で表現される項目）と同等以上のセキュリティ水準を確保していることものを選定すること。

(イ) 情報資産を管理するデータセンターの設置場所に関しては、国内であることを基本とする。設置場所の考え方についてはクラウド方針を参照すること。

(ウ) 契約の解釈が日本法に基づくものであること。

(エ) クラウドサービスの利用契約に関連して生じる一切の紛争は、日本の地方裁判所を専属的合意管轄裁判所とするものであること。

(オ) センターの指示によらない限り、一切の情報資産について日本国外への持ち出しを行わないこと。情報資産を国外に設置されるクラウドサービスに保管する際の考え方については「クラウド方針」を参照すること。
(カ) 障害発生時に縮退運転を行う際にも、情報資産が日本国外のデータセンターに移管されないこと。
(キ) 情報資産の所有権がクラウドサービス事業者に移管されるものではないこと。従って、センターが要求する任意の時点で情報資産を他の環境に移管させることができること。
(ク) クラウドサービスの可用性を保証するための十分な冗長性、障害時の円滑な切替え等の対策が講じられていること。
(ケ) クラウドサービス上で取り扱う情報について、機密性及び完全性を確保するためのアクセス制御、暗号化及び暗号鍵の保護並びに管理を確実に行うこと。
(コ) クラウドサービスに係るアクセスログ等の証跡を保存し、センターからの要求があった場合は提供すること。
(サ) インターネット回線を通じたセキュリティ侵害を防ぐため、インターネット回線とクラウドサービスとの接続点の通信を監視すること。

3.1.4. 開発方式及び開発手法

以下の開発方式及び開発手法に従い、本システムを開発すること。

(ア) 基盤サービスの開発方式は、既製ソフトウェア製品を用いて構築する方式とし、アプリケーションの開発は行わない前提とする。
(イ) 本システムの開発手法は、ウォータフォール型とする。
(ウ) 受注者は必要に応じて、更新プログラムの適用、脆弱性対応等でシステムに変更を加える前に動作検証等が行える環境を用意すること。

3.2. 規模に関する事項

3.2.1. 機器数及び設置場所

本システムを構成する機器について、機器数及び設置場所を以下に示す。

表 3-2 機器数及び設置場所

No.	分類	ハードウェア名	想定数量	設置場所	補足
1	ネットワーク機器（東海センター）	ファイアウォール	1 台	東海センター	
2		ディストリビューションスイッチ	2 台		
3		アクセススイッチ	11 台		
4		無線 LAN アクセスポイント	9 台		
5	ネットワーク機器（東京本部）	ファイアウォール	1 台	東京本部	
6		ディストリビューションスイッチ	2 台		
7		アクセススイッチ	6 台		
8		無線 LAN アクセスポイント	7 台		
9		無線 LAN コントローラ	1 台		
10	ネットワーク機器（六ヶ所センター）	ファイアウォール	1 台	六ヶ所センター	
11		ディストリビューションスイッチ	2 台		
12		アクセススイッチ	6 台		
13		無線 LAN アクセスポイント	6 台		
14	PC 端末	職員用端末	240 台	東京本部、東海センター、六ヶ所センター	台数は予備用端末を含む。
15		ウイルススキャン端末	—		調達対象外
16		運用支援端末	6 台	東京本部又は受注者の運用保守拠点	
17	その他	ネットワークプリンタ	—	東京本部 東海センター 六ケ所センター	調達対象外

3.2.2. データ量

本システムで取扱うデータのデータ量について以下に示す。

表 3-3 データ量

No.	サービス名	データ名	データ量	補足
1	メールサービス	電子メールデータ	100GB /1 アカウント	最大アカウント数:220
2	ファイル共有サービス	共有ファイルデータ	15TB	
3	ログ管理サービス	ログデータ	受注者の設計による	
4	バックアップ管理サービス	バックアップデータ	受注者の設計による	
5	全般	その他データ	受注者の設計による	

3.2.3. 処理件数

本システムの処理件数について以下に示す。

表 3-4 データ処理件数

No.	サービス名	処理名	処理件数	補足
1	メールサービス	メール送信件数 （1 日あたり）	約 60 件/ 1 アカウント	

3.2.4. 利用者数

本システムの利用者数について以下に示す。

表 3-5 利用者数

No.	利用者区分		利用者数	補足
1	役職員	東京本部	約 35 人	
2		東海センター	約 100 人	
3		六ケ所センター	約 70 人	
4	受注者	東京本部又は受注者の運用保守拠点	約 6 人	現時点での想定

3.3. 性能に関する事項

3.3.1. 応答時間

本システムの応答時間に係る指標と目標値を以下に示す。受注者は、以下の目標値を満たすことのできるよう本システムを構築すること。

なお、各設定対象の詳細な測定条件については、本システムの設計段階においてセンターと協議の上で決定すること。

表 3-6 応答時間に係る目標値

No.	設定対象	指標名	処理内容	目標値	目標値達成率
1	統合認証サービス	サーバ処理時間(※)	PC 端末のログイン処理	2 秒以内	80%
2	ファイル共有サービス		1MB の電子ファイルを共有フォルダ上でコピー	3 秒以内	80%
3			10MB の電子ファイルを共有フォルダ上でコピー	5 秒以内	80%

※サーバ処理時間とは、サーバがクライアント(PC 端末等)からの処理要求を受信した時点から、処理応答の送信を開始するまでの時間を指す。

3.4. 信頼性に関する事項

3.4.1. 可用性に関する事項

3.4.1.1. 可用性に係る目標値

本システムの可用性に係る指標と目標値を以下に示す。受注者は、以下の目標値を満たすことのできるよう本システムを構築すること。

表 3-7 可用性に係る目標値

No.	設定対象	指標名	目標値	補足
1	LAN サービス	稼働率(※)	99.9%以上	アクセススイッチの停止時間は含まないこと。
2	統合認証サービス		99.9%以上	
3	ファイル共有サービス		99.9%以上	
4	メールサービス		99.9%以上	
5	クラウド認証サービス		99.9%以上	

※ 本システムのサービス提供時間(24 時間 365 日)のうち、稼働率の測定対象は平日の 9:00～17:30 とし、センターと事前に合意した計画停止時間は除くものする。

3.4.1.2. 可用性に係る対策

受注者は、表 3-7 に示す可用性に係る目標値を満たすために必要な可用性対策(冗長化等)を行うこと。

(ア) 運用保守上の人的ミスに起因する障害が本システムの可用性に影響を与える事態を未然に防止するため、「3.16 運用に関する事項」及び「3.17 保守に関する事項」を踏まえ、適切な手順書を整備すること。また、定型的なオペレーションは自動化すること。

3.4.2. 完全性に関する事項

本システムに係る完全性要件を以下に示す。

(ア) 「3.8 継続性に関する事項」に示す目標復旧地点を満たすよう、バックアップ取得を行うこと。

(イ) システム運用中に障害・トラブル等が発生した際に原因追求が可能となるよう、操作ログやアクセスログ等のシステムログ、例外事象の発生に関するログ等を取得・保管し、必要な時に出力可能とすること。

3.5. 拡張性に関する事項

本システムの拡張性に係る要件を以下に示す。なお、ここで求める性能拡張を実施する際の費用については、別途センターとの協議を行うものとする。

(ア) 利用者数や業務量、業務内容等の変化により、本システムで必要となる処理能力や取り扱うデータ容量が大幅に増加した場合でも、本システムの基本的な構成を見直すことなくスケールアウト、スケールアップ等により柔軟な性能拡張ができること。

(イ) 特に以下の事項については、将来的な拡張を見据えた高い拡張性を有する構成とし、スケールアップ又はスケールアウトのみで拡張可能とすること。

・ 「ファイル共有サービス」のデータ格納容量
・ 「メールサービス」のメールボックス容量

3.6. 上位互換性に関する事項

本システムの上位互換性に係る要件を以下に示す。

(ア) 本システムのサーバ等に導入するソフトウェア製品は、OS 又は実行環境（.NET Framework、JRE（Java Runtime Environment）等）の将来的なバージョンアップに備え、特定バージョンに依存する機能やソフトウェアベンダが非推奨としている機能の利用を最低限とすること。

(イ) 本システムの端末に導入するソフトウェア製品は、OS、実行環境（.NET Framework、JRE（Java Runtime Environment）等）又はブラウザの将来的なバージョンアップに備え、特定バージョンに依存する機能やソフトウェアベンダが非推奨としている機能の利用を最低限とすること。

(ウ) クラウドサービスの利用においてマネージドサービスを採用する場合、軽微なバージョンアップについては自動適用を前提とすること。

(エ) ソフトウェアの大規模なバージョンアップについては、各種サービスへの影響を事前に精査し、適用を検討すること。

3.7. 中立性に関する事項

本システムの中立性に係る要件を以下に示す。

(ア) 本システム及び本システムに係る設計資料等は、特定の事業者に依存することなく、他者に引き継ぐことが可能な構成とすること。

(イ) 本システムのクラウドサービス、ハードウェア及びソフトウェア製品は、可能な限り以下の中立性を有する製品を選定すること。ただし、デファクトスタンダードとして広く利用されている製品については、この限りではない。

- 特定ベンダの技術に依存しない、オープンな技術仕様に基づく製品であること。
- オープンなインタフェースを利用して接続又はデータの入出力が可能であること。
- 標準化団体（ISO、IETF、IEEE、ITU、JISC 等）が規定又は推奨する各種業界標準に準拠するなど、具体的仕様が開かれた参画プロセスの下で合意され、実装可能なレベルで公開されている技術に基づくこと。
- 誰もが採用可能であること。

(ウ) 本システムの将来的な更改の際に、移行の妨げとなることや特定の装置や情報システムに依存することを防止するため、原則として本システム内のデータ形式はテキスト形式等の特定の製品に依存しないデータ形式で取り出すことができること。

(エ) 第 3 期基盤情報システム関係事業者への引継ぎ時における移行データ等の抽出に必要な設定変更作業が発生する場合においても、追加契約や費用等が発生しないこと。

3.8. 継続性に関する事項

本システムにおいて、ハードウェア障害又はデータ破壊等が発生した際の復旧に係る継続性の要件を以下に示す。

3.8.1. 継続性に係る目標値

本システムの継続性に係る目標値を以下に示す。

なお、ここで示す目標値はハードウェア障害又はデータ破壊が生じた際の復旧に係る目標値であり、大規模災害等による障害発生時の復旧については対象外とする。

表 3-8 継続性に係る目標値

No.	設定対象	指標及び目標値		
		目標復旧時間（RTO）※	目標復旧地点（RPO）	目標復旧レベル（RLO）
1	LAN サービス	24 時間以内	-	全ての機能
2	WAN サービス		-	
3	テレワークサービス		-	
4	インターネットサービス		-	
5	総合認証サービス		5 営業日前	
6	Windows アップデート管理サービス		-	
7	ファイル共有サービス		1 営業日前	
8	メールサービス		1 営業日前	
9	端末管理サービス		-	
10	システム運用管理・監視サービス		-	
11	バックアップ管理サービス		-	
12	ログ管理サービス		-	
13	ウイルス対策管理サービス		-	
14	クラウドプロキシサービス		-	
15	クラウド認証サービス		-（統合認証サービスのデータと連携されるため）	
16	Web 分離サービス		-	

※「目標復旧時間（RTO）」の計測開始時は、障害検知時とする。

3.8.2. 継続性に係る対策

本システムは、以下の継続性に係る対策要件を満たすこと。

(1) 業務データのバックアップ

(ア) 各サービスの業務データについて、バックアップの取得方法、保存先、取得周期、世代数等を検討し、「3.8.1. 継続性に係る目標値」に定める各目標値を満たすことのできるバックアップ・リカバリ環境を構築すること。なお、業務データのバックアップ対象は以下を想定しているが、詳細は本システムの設計時にセンターと協議の上で決定すること。

表 3-9 バックアップ対象業務データ一覧

No.	サービス名	データ名	データ概要
1	統合認証サービス	ディレクトリデータ	・ センターの業務において管理されるアカウント、グループポリシー等のデータ。
2	メールサービス	電子メールデータ	・ センターの業務において送受信される電子メールデータ。
3	ファイル共有サービス	共有ファイルデータ	・ センターの業務において管理・保有される業務データ（Word、Excel、PDF 等）。
4	全般	その他データ	・ その他、システムの復旧に必要となる各種データ（受注者の設計による。）

(イ) 業務データのバックアップ処理は、「バックアップ管理サービス」のスケジュール設定等により自動化し、成否が確認できること。

(ウ) バックアップ処理の実行日時、実行周期等は、業務への影響が最小となるよう設計すること。

(エ) バックアップ処理は、必要に応じて手動実行できること。

(2) システムバックアップ

(ア) 各サービスのシステムバックアップデータについて、バックアップの取得方法、保存先、取得周期、世代数等を検討し、「3.8.1. 継続性に係る目標値」に定める各目標値を満たすことのできるシステムバックアップ・リカバリ環境を構築すること。なお、システムバックアップ対象は、本システムの各サービスを復旧するために必要となる全ての機器とすること。

(イ) システムバックアップは、可能な限り「バックアップ管理サービス」のスケジュール設定等により自動化し、成否が確認できること。

(ウ) バックアップ処理の実行日時、実行周期等は、業務への影響が最小となるよう設計すること。

(エ) バックアップ処理は、必要に応じて手動実行できること。

(3) **バックアップデータの保管**

(ア) データ消失時の影響が大きいことを考慮の上、バックアップデータの保管方法については、受注者にて提案を行い、センターと協議の上、決定すること。

(4) **その他の継続性対策**

(ア) アベイラビリティゾーン（以下「AZ」という）については、マルチ AZ によって複数の AZ をまたいだシステム冗長化を実現し、可用性を高める方針とすること。

(イ) ネットワーク機器については、予備機を必要に応じて提案すること。また、職員用端末については予備用端末を含めた台数を指定しているため、受注者側での予備機の準備は不要とする。

3.9. 情報セキュリティに関する事項

3.9.1. 情報セキュリティ対策要件

本システムにおける、情報セキュリティ対策要件を以下に示す。

(1) 情報システムのライフサイクル

情報システムのライフサイクルにおける情報セキュリティ対策要件を以下に示す。

(ア) 受注者は、本システムの情報セキュリティ対策が行えるよう、以下の要件を満たすこと。

- 本システムの構築時の構成（クラウドサービス、ハードウェア、ソフトウェア製品に関する詳細情報）が記載された文書を設計書に含めるとともに、文書どおりの構成とすることに加え、本システムに関する運用開始後の最新の構成情報及び稼働状況の管理を行う方法又は機能を備えること。
- 本システムの構築時の構成（ネットワーク接続、ネットワーク機器に関する詳細情報）が記載された文書を設計書に含めるとともに、文書どおりの構成とすること加え、本システムに関する運用開始後の最新の構成情報及び稼働状況の管理を行う方法又は機能を備えること。
- 本システムの情報セキュリティ水準を維持するための手順が記載された文書を作成し、運用作業を可能とすること。
- 情報セキュリティインシデントを認知した際の対処手順が記載された文書を作成し、運用作業を可能とすること。

(イ) 受注者は、機器等の調達に当たっては、以下の要件を満たすこと。

- 調達した機器にセンターの意図しない不正な変更が行われるなどの不正が見つかったときに、追跡調査や立入検査等、センターと受注者が連携して原因を調査・排除できる体制を整備していること。また、当該体制が書類等で確認できること。
- 経済産業省が定める「IT 製品の調達におけるセキュリティ要件リスト」の適合製品又は ISO/IEC15408(Common Criteria)認証取得製品の選定に努めること。

(ウ) 受注者は、機器等の納入時の確認・検査手続きとして、以下を確認可能な資料をセンターに書面にて提出し、承認を得ること。

- 情報セキュリティに関する事項に示す要件が漏れなく実装されていること。
- 機器等に不正プログラムが混入していないこと。

(エ) 受注者は、本システムを構築するに当たって、以下の要件を満たすこと。また、センターの求めに応じて、以下の要件を満たしていることを記載した文書をセンターに提出すること。

- 情報セキュリティ対策要件の適切な実装
- 情報セキュリティの観点に基づく試験の実施

・　本システムの設計、構築及びテスト工程における情報セキュリティ対策

(オ) 受注者は、本システムを構成するクラウドサービス、ソフトウェア及びハードウェアの脆弱性を悪用した不正を防止するため、構築時に脆弱性の有無を確認の上、運用上対処が必要な脆弱性は修正の上で納入すること。

(カ) 受注者は、本システムの移行段階において外部電磁的記憶媒体又は移行用のサーバ装置等を利用する場合、データの暗号化や移行後の不要なデータの削除等、情報セキュリティの観点から必要な措置を講ずること。

(キ) 受注者は、不正な行為及び意図しない情報システムへのアクセス等の事象が発生した際に追跡できるように、保守作業時の本システムへの操作を記録すること。

(2) 情報システムのセキュリティ要件

受注者は、以下のセキュリティ対策を実施すること。

表 3-10 セキュリティ対策要件

No.	分類	セキュリティ要件
1	主体認証	・ 本システムによる各サービスを許可された者のみに提供するため、本システムにアクセスする主体のうち本人確認の認証を行う機能として識別コード（ID）とパスワードによる主体認証を行うこと。 ・ 端末へのログインについては、識別コード・パスワードによる認証と所有認証を組み合わせた多要素主体認証を行うこと。 ・ 本システムの認証履歴の記録と通知を行う機能を備えること。 ・ 指定回数以上の認証失敗時にアクセス拒否を行う機能を備えること。 ・ 大規模な辞書を用いたパスワード解析への耐性を備えること。 ・ 本システムへのリモート接続を行う際には、多要素主体認証を要求すること。
2	アクセス制御・権限管理	・ 主体のアクセス権を適切に管理するため、主体が用いるアカウント（識別コード、主体認証情報、権限等）を管理（登録、更新、停止、削除等）するための機能を備えること。 ・ 本システムに蓄積された情報の窃取や漏えいを防止するため、情報へのアクセスを制限できる機能を備えること。 ・ 本システムの利用範囲を利用者の職務に応じて制限するため、本システムのアクセス権を職務に応じて制御する機能を備えるとともに、アクセス権の割り当てを適切に設計すること。 ・ 特権を有する管理者による不正を防止するため、管理者権限を制御する機能を備えること。 ・ 電子証明書等により、本システムの運用機能にアクセス可能な端末を、特定の端末に制限すること。

No.	分類	セキュリティ要件
		・ 本システムへアクセス可能な端末を、最新の脆弱性対策や不正プログラム対策が施されている端末に限定すること。 ・ IP アドレス等による接続元制限を実施できること。 ・ 本システムへの通信は必要最低限の宛先・Port のみを許可する等の通信制御を実施すること。
3	ログ取得・管理	・ 本システムの利用記録、問題・インシデントに関するログを取得し、蓄積すること。悪意ある第三者等からの不正侵入、不正操作等の有無について点検又は分析を行うことのできるログ分析機能を有すること。 ・ ログの不正な改ざんや削除を防止するため、ログに対するアクセス制御機能を備えるとともに、ログのアーカイブデータの保護（消失及び破壊や改ざん等の脅威の軽減）のための措置を含む設計とすること。 ・ 情報セキュリティインシデント発生時の原因追及や不正行為の追跡において、ログの分析等を容易にするため、システム内の機器を正確な時刻に同期する機能を備えること。
4	暗号化・電子署名	・ 本システムに蓄積された情報の窃取や漏えいを防止するため、保護すべき情報を利用者が直接アクセス可能な機器に保存しないことに加えて、保存された情報を暗号化する機能を備えること。 ・ 電子署名の付与及び検証を行う機能を設ける必要性の有無を検討し、必要があると認めたときは、当該機能を設けること。 ・ 暗号化又は電子署名を使用する場合には、原則、「電子政府推奨暗号リスト」に記載されたアルゴリズム及びそれを利用した安全なプロトコルを採用すること。 ・ 電子署名に使用するアルゴリズムが危殆化した場合又はそれを利用した安全なプロトコルに脆弱性が確認された場合を想定した緊急対応手順を定めること。 ・ 電子署名の付与に用いる鍵について、管理手順を定めること。 ・ 電子署名の正当性を検証するための情報又は手段を、署名検証者へ安全な方法で提供すること。 ・ 電子署名のために選択されたアルゴリズムの危殆化に関する情報を定期的に入手し、センターに報告すること。
5	ソフトウェアの脆弱性対策	・ 運用開始後、新たに発見される脆弱性を悪用した不正を防止するため、本システムを構成するソフトウェア及びハードウェアの更新を行う方法を備えること。また、セキュリティパッチ、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するファイルは信頼できる方法で入手すること。

No.	分類	セキュリティ要件
		・ 本システムの構築範囲において、構築時に第三者による脆弱性検査(クラウドサービスの管理設定不備の検査等を含む)を実施し、その結果をセンターに書面にて報告すること。また、検査の実施に当たっては、客観性及び網羅性の確保に留意すること。 ・ 把握した脆弱性情報について、対処の要否、可否を判断すること。対処するものに関して対処方法、対処しないものに関してその理由、代替措置及び影響をセンターに書面にて報告の上、承認を得ること。
6	不正プログラム対策	・ 不正プログラム(ウイルス、ワーム、ボット等)による脅威に備えるため、想定される不正プログラムの感染経路の全てにおいて感染を防止する機能を備えるとともに、新たに発見される不正プログラムに対応するために機能の更新が可能であること。 ・ 本システム全体として不正プログラムの感染防止機能を確実に動作させるため、当該機能の動作状況及び更新状況を一元管理する機能を備えること。 ・ 未知のランサムウェア等を検知した際、検知までの間にファイルの暗号化処理等が行われるケースを想定し、当該ファイルを容易に復元可能とする機能を有すること。
7	サービス不能攻撃対策	・ 本システムで採用するクラウドサービスについては、サービス不能攻撃対策が施されたものを選定すること。
8	情報窃取・侵入対策	・ 物理的な手段によるセキュリティ侵害に対抗するため、運用支援端末(受注者が準備する運用支援端末も含む)については、外部からの侵入対策が講じられた場所に設置すること。 ・ 受注者の運用保守拠点においては、セキュリティカード等による入退室管理を実施すること。なお、入退室に関しては、共連れ及び不正な入退出を防止するための対策を講じること。 ・ 情報の漏えいを防止するため、運用支援端末や受注者の運用保守拠点において以下に示すような物理的な手段による情報窃取行為を防止・検知するための対策を行うこと。 ➢ 端末の離席対策(自動スクリーンロック等) ➢ 端末のワイヤーロック ➢ ディスプレイの盗み見防止フィルタ ➢ メモリデバイス等の持込みの監視及び制限

(3) 情報システムの構成要素

情報システムの構成要素における、情報セキュリティ対策要件を以下に示す。

(ア) 受注者は、本システムの各ハードウェアは、盗難、不正な持ち出し、第三者による不正操作、表示用デバイスの盗み見等の物理的な脅威から保護するため、原則としてすべての機器を施錠可能なサーバラック内に格納する設計とすること。受注者は、端末又はサーバの運用を終了する際に、端末の電磁的記録媒体の全ての情報を抹消すること。

(イ) 受注者は、本システムの各サーバへのリモート接続を行う際は、送受信される情報の漏えいを防止するため、リモートログインの認証及び通信の暗号化を施すこと。

(ウ) 受注者は、メールサービスにおいて、以下の要件を満たすこと。

・ 外部からの受信メールに対して迷惑メールフィルタ機能を有すること。
・ メール送受信におけるマルウェア対策機能を有すること。
・ 電子メールサーバが電子メールの不正な中継を行わないように設定すること。
・ 電子メールクライアントから電子メールサーバへの電子メールの受信時及び送信時に主体認証を行う機能を備えること。
・ 送信時に SPF を設定すること。また、受信時に SPF チェックを行うこと。ただし、SPF チェックを行う際に、対象ドメインを指定／除外できること。
・ 送信時に DKIM による電子署名を付加すること。また、受信時に DKIM の検証を行うこと。ただし、検証を行う際に、対象ドメインを指定／除外できること。
・ 送信時に DMARC を設定すること。また、受信時に DMARC の検証を行うこと。ただし、検証を行う際に、対象ドメインを指定／除外できること。

(エ) 受注者は、本システムの構成要素としてウェブサーバを使用する場合は、以下の要件を満たすこと。

・ 不要な機能を停止又は制限すること。
・ ウェブサーバに保存する情報を特定し、サービスの提供に必要のない情報がウェブサーバに保存されないことを確認すること。

(オ) 受注者は、内部 DNS サービスにおいて、名前解決の要求への適切な応答をするための措置を講ずること。

(カ) 受注者は、データベースを利用する場合は以下の要件を満たすよう、本システムを構築すること。

・ データベースに対する内部不正を防止するため、管理者アカウントの適正な権限管理を行うこと。
・ データベースに格納されているデータにアクセスした利用者を特定できるよう、措置を講ずること。
・ データベースに格納されているデータに対するアクセス権を有する利用者によるデータの不正な操作を検知できるよう、対策を講ずること。
・ データベース及びデータベースへアクセスする機器等の脆弱性を悪用した、データの不正な操作を防止するための対策を講ずること。

(キ) 受注者は、データの窃取、電磁的記録媒体の盗難等による情報の漏えいを防止する必要がある場合は、適切に暗号化をすること。
(ク) 受注者は、通信回線装置が動作するために必要なソフトウェアを利用し、当該ソフトウェアを変更する場合は、センターの承認を得ること。
(ケ) 受注者は、本システムの通信回線装置へのリモート接続を行う際は、送受信される情報の漏えいを防止するため、リモートログインの認証及び通信の暗号化を施すこと。
(コ) 受注者は、通信回線装置が動作するために必要なソフトウェアを利用する場合、センターの求めに応じ、許可されていないソフトウェアがインストールされていない旨を定期的に報告すること。
(サ) 受注者は、通信回線装置の運用を終了する場合には、当該通信回線を構成する通信回線装置が運用終了後に再利用された時又は廃棄された後に、運用中に保存していた情報が漏えいすることを防止するため、当該通信回線装置の電磁的記録媒体に記録されている全ての情報を抹消すること。

(4) その他の情報セキュリティ対策要件

その他の情報セキュリティ対策要件を以下に示す。

(ア) 受注者は、センターの情報セキュリティポリシー及び情報管理規程（以下、「情報セキュリティ関係規程」という。）を十分に理解し、遵守すること。
(イ) 受注者は、センターから管理情報等を提供された場合には、本業務以外の目的外利用をしないこと。
(ウ) 受注者は、本業務の開始時に、本業務に係る情報セキュリティ対策の実施内容及び管理体制について、センターに書面にて提出し、承認を得ること。
(エ) 受注者は、本システムの開発において、意図せざる変更が加えられないよう、以下の要件を満たすこと。

・ 本システムの開発工程において、センターの意図しない変更が行われないことを保証する管理が、一貫した品質保証体制の下でなされていること。また、当該品質保証体制について、センターに書面にて提出し、承認を得ること。
・ 本システムにセンターの意図しない変更が行われるなどの不正が見付かったときに、追跡調査や立入検査等、センターと受注者が連携して原因を調査・排除できる体制を整備していること。また、当該体制について、センターに書面にて提出し、承認を得ること。

(オ) 受注者は、本業務の開始時に受注者の資本関係・役員等の情報、委託事業の実施場所、委託事業従事者の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績及び国籍に関する情報について、センターに書面にて提出し、承認を得ること。

(カ) 受注者は、本業務において情報セキュリティインシデントが発生した場合の対処方法を整備すること。

(キ) 受注者は、センターの求めに応じ、情報セキュリティ対策その他の契約の履行状況についてセンターに定期的に報告を行うこと。また、情報セキュリティ対策の履行が不十分と見なされるときは、必要に応じてセンターの行う情報セキュリティ対策に関する監査を受け入れること。

(ク) 受注者は、情報セキュリティ対策の履行が不十分な場合、センターと改善について協議を行い、合意した改善策を実施すること。

(ケ) 受注者は、本業務の一部を再委託する場合、再委託先に(ア)～(ク)の措置の実施を担保させることで、受注者の責任で情報セキュリティの確保を行うこと。また、再委託先の情報セキュリティ対策状況について、センターに書面にて提出し、承認を得ること。

(コ) 受注者は、本業務においてセンターより受領した情報又は作成した情報について、業務終了等により不要になった場合には、確実に返却又は廃棄すること。

3.10. 情報システム稼働環境に関する事項

3.10.1. クラウドサービス構成

本システムのクラウドサービス構成に係る要件を以下に示す。

なお、ここで示す構成は要件定義時点の想定である。セキュリティ対策、運用保守の最適化、ライフサイクルコスト等を考慮し、想定構成とは異なるプラットフォームを提案することを妨げるものではない。

表 3-11 クラウドサービス構成

No.	サービス名	想定構成
1	統合認証サービス	IaaS
2	クラウド認証サービス	SaaS
3	Windows アップデート管理サービス	SaaS
4	ファイル共有サービス	SaaS
5	メールサービス	SaaS
6	端末管理サービス	SaaS
7	システム運用管理・監視サービス	SaaS
8	バックアップ管理サービス	SaaS
9	ログ管理サービス	SaaS
10	ウイルス対策管理サービス	SaaS
11	クラウドプロキシサービス	SaaS
12	Web 分離サービス	SaaS

3.10.2. ハードウェア構成

本システムのハードウェア構成に係る要件を以下に示す。

なお、各ハードウェアの機種選定に当たっては、機能や性能が過剰とならない範囲で、同一の操作性・保守性を有する機器（同一シリーズの機種等）の選定に努め、運用性及び保守性の向上を図ること。また、現行システムにおけるリソースの利用状況等についても閲覧可能であるため参考の上、性能を検討すること。

3.10.2.1. ハードウェア要件（共通要件）

受注者は、本システムの全てのファームウェアについて以下の共通要件を満たすこと。

(1) 製品サポートに係る要件

(ア) 本システムの運用期間中に、製造元による製品サポート（技術サポート、バグ修正パッチの提供、セキュリティパッチの提供等）が継続して提供されるファームウェアであること。

(イ) やむを得ず運用期間中にサポート期限を迎えるファームウェアを導入する必要がある場合は、当該サポート期限を迎える前に、サポートが継続されるバージョンへのバージョンアップ対応及び必要なテスト等を無償で行うこと。

(2) ファームウェアに係る要件

(ア) 導入するファームウェアのバージョンは、原則として本業務の契約時点での最新バージョンとすること。
(イ) 互換性等の理由により最新バージョン以外のファームウェアを導入する場合は、事前にセンターの承認を得ること。

3.10.2.2. ハードウェア要件（ネットワークサービス）

本システムのネットワークサービスを実現するための想定ハードウェア構成図を図 3-2 に示す。また、最低限必要と考えるハードウェアの一覧を表 3-12 ハードウェア一覧（ネットワークサービス）に、それぞれに示す。なお、各ハードウェアの詳細な構成は受注者の設計によるものとする。

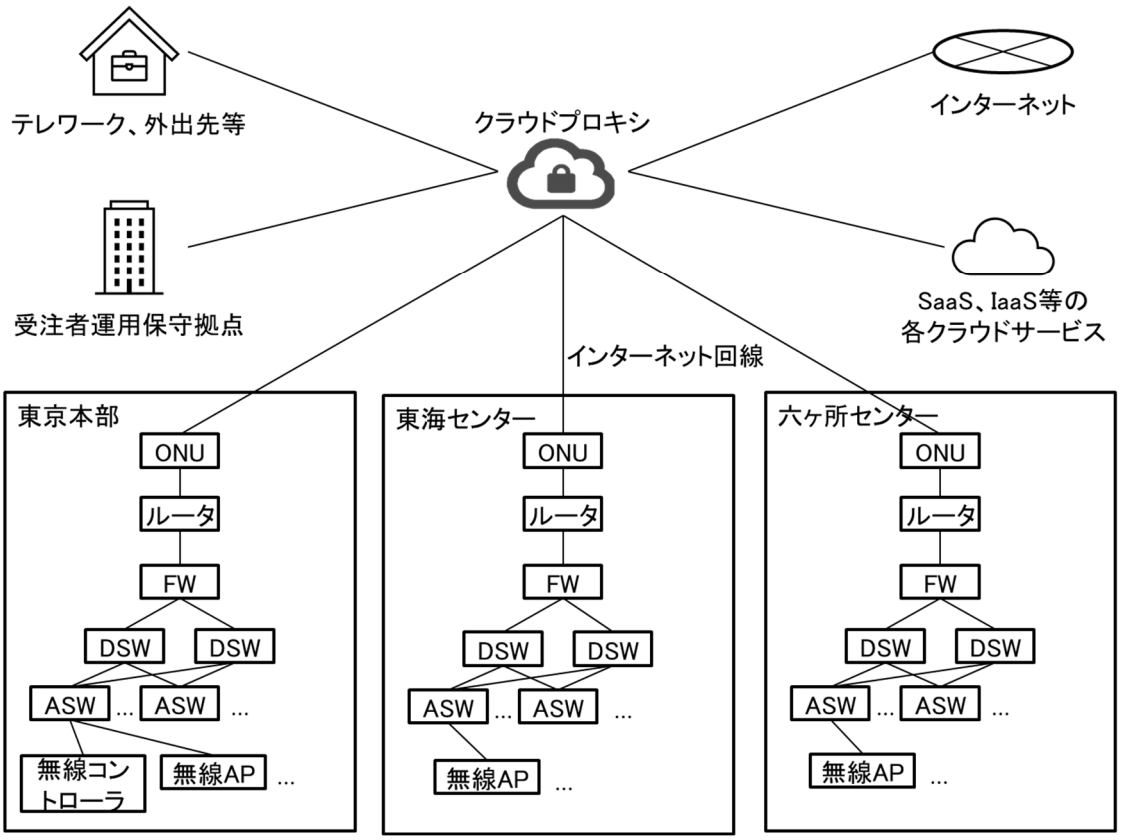


図 3-2 想定ハードウェア構成図（ネットワークサービス）

表 3-12 ハードウェア一覧（ネットワークサービス）

No.	分類	ハードウェア名	概要	想定数量
1	ネットワーク機器（東海センター）	ファイアウォール	東海センター内の LAN と他のセグメント間の通信制御を行うファイアウォール。 東海センター内のコアスイッチを兼ねる	1 台
2		ディストリビューションスイッチ	東海センター内に設置する L2 スイッチ	2 台
3		アクセススイッチ		11 台
4		無線 LAN アクセスポイント	東海センター内に設置するアクセスポイント	9 台
5	ネットワーク機器（東京本部）	ファイアウォール	東京本部の LAN と他のセグメント間の通信制御を行うファイアウォール。東京本部内のコアスイッチを兼ねる。	1 台
6		ディストリビューションスイッチ	東京本部内に設置する L2 スイッチ	2 台
7		アクセススイッチ		6 台
8		無線 LAN アクセスポイント	東京本部内に設置するアクセスポイント	7 台
9		無線 LAN コントローラ	東京本部内に設置するコントローラ	1 台
10	ネットワーク機器（六ヶ所センター）	ファイアウォール	六ヶ所センターの LAN と他のセグメント間の通信制御を行うファイアウォール。六ヶ所センター内のコアスイッチを兼ねる。	1 台
11		ディストリビューションスイッチ	六ヶ所センター内に設置する L2 スイッチ	2 台
12		アクセススイッチ		6 台
13		無線 LAN アクセスポイント	六ヶ所センター内に設置するアクセスポイント	6 台

(1) ファイアウォール

ファイアウォールのハードウェア要件を以下に示す。

表 3-13 ファイアウォールのハードウェア要件

No.	項目	ハードウェア要件	補足
1	機能	DIX Ethernet Ver2 フレームによる通信ができること。また、IEEE802.3 フレームを利用している場合は、IEEE802.3 フレームによる通信ができること。	
2		IP アドレスによるルーティング機能を有すること。	
3		IP アドレス及びポート番号に基づき、通信の許可及び拒否を制御できること。	
4		ステートフルインスペクション機能を有すること。	
5		QoS 等の通信制御機能を有すること。	
6		IEEE802.1Q に準拠した VLAN 機能を有すること。	
7		通信ログ、操作ログ等の記録・出力・転送ができること。	
8	性能	収容する機器に応じて必要なポート数を有すること。	
9		収容する機器及び使用ポート数に応じた必要最低限の処理能力を有すること。	

(2) ディストリビューションスイッチ及びアクセススイッチ

ディストリビューションスイッチ及びアクセススイッチのハードウェア要件を以下に示す。

表 3-14 ディストリビューションスイッチ及びアクセススイッチのハードウェア要件

No.	項目	ハードウェア要件	補足
1	機能	IEEE802.3 フレーム及び DIX Ethernet Ver2 フレームによる通信ができること。	
2		QoS 等の通信制御機能を有すること。	
3		IEEE802.1Q に準拠した VLAN 機能を有すること。	
4		IEEE802.1D,IEEE802.1w, IEEE802.1s に準拠したスパニングツリープロトコル機能を有すること。	
5		MAC アドレス等による認証を行うためのポートセキュリティ機能を有すること。	
6		通信ログ、操作ログ等の記録・出力・転送ができること。	
7		無線 LAN アクセスポイントに接続するスイッチは PoE 給電機能を有すること。	
8	性能	収容する機器に応じて必要なポート数を有すること。	

No.	項目	ハードウェア要件	補足
9		収容する機器及び使用ポート数に応じた必要最低限の処理能力を有すること。	

(3) 無線 LAN アクセスポイント

無線 LAN アクセスポイント要件を以下に示す。

表 3-15 無線 LAN アクセスポイント要件

No.	項目	ハードウェア要件	補足
1	機能	2.4GHz/5GHz/6GHz 帯の同時使用が可能であり、無線 LAN 接続時に 6GHz 帯に優先して接続させるように制御できること。	
2		IEEE802.11 a/b/g/ n/ac/ax（6E）に対応していること。	
3		暗号化規格は WPA2 方式または WPA3 方式を採用すること。	
4		ESS-ID ステルス機能を有すること。	
5		IEEE802.1X 等に基づいた認証機能を有すること。	
6		送信ビームフォーミング機能を有すること。なお、この機能を実現させるために、無線 LAN クライアント側に特別なソフトウェアが不要であること。	
7		複数の VLAN を設定できること。	
8		PoE 給電機能を有すること。給電規格は、提案するアクセススイッチと整合したものとすること。	
9		無線 LAN クライアント間の通信を遮断する機能を有すること。	
10		マルチ SSID の機能を有すること。	
11	性能	収容する機器に応じて必要なポート数を有すること。	
12		収容する機器及び使用ポート数に応じた必要最低限の処理能力を有すること。	

(4) 無線 LAN コントローラ

無線 LAN コントローラ要件を以下に示す。なお、機能を満たせる場合、無線 LAN アクセスポイントとの一体型の製品、仮想アプライアンス、SaaS サービス等の利用を提案してもよい。

表 3-16 無線 LAN コントローラ要件

No.	項目	ハードウェア要件	補足
1	機能	導入する全ての無線 LAN アクセスポイントに対し、各種設定（アクセス制御、チャネル、電波強度、セキ	

No.	項目	ハードウェア要件	補足
		ュリティ設定等)、モニタリング等の一括管理機能を有すること。	
2		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。	
3		無線 LAN アクセスポイントから収集した電波関連情報をもとに、チャネルや送信電力を自動で変更・調整する機能を有すること。	
4		1 つの SSID に対して複数の VLAN を適応することができること(本機能は無線 LAN アクセスポイント側の機能として有していれば許容する)。	
5		無線 LAN アクセスポイントごと又は SSID ごとに、接続可能なクライアント数の制限ができること。	
6	性能	収容する機器に応じて必要なポート数を有すること。	
7		収容する機器及び使用ポート数に応じた必要最低限の処理能力を有すること。	

3.10.2.3. ハードウェア要件（端末サービス）

本システムの端末サービスを構成する各ハードウェアの一覧及びハードウェア要件を以下に示す。

表 3-17 ハードウェア一覧（端末サービス）

No.	分類	ハードウェア名	数量
1	PC 端末	職員用端末	240 台
2		運用支援端末	6 台

(1) 職員用端末

職員用端末のハードウェア要件を以下に示す。

表 3-18 職員用端末のハードウェア要件

No.	項目	ハードウェア要件	補足
1	筐体	ノート型 PC 端末であること。また、本体質量は 1,000g 以下であること。	
2	CPU	Intel 社製 Core i7、Core Ultra 5 シリーズ（ノート型 PC 向け製品）以上の性能を有すること。	
3	メモリ	16GB 以上の容量を有すること。	
4	内蔵ディスク	SSD で 512GB 以上の容量を有すること。	
5	ネットワークインタフェース	無線ネットワークへの接続が可能であること。また、IEEE802.11 a/b/g/ n/ac/ax(6E)に対応していること。1000BASE-T に対応したネットワークインタフェースを 1 ポート以上備えること。	
6	USB ポート	USB3.0 以上に対応した USB ポートを 1 ポート以上備えること。	
7	ディスプレイ	ディスプレイは 13-14 インチであること	
8	バッテリー	バッテリーは最低 3 時間以上稼働できること。	
9	外付けディスプレイ	ディスプレイは FullHD 以上の解像度を有する 23 インチ以上であること。入力端子に HDMI を有すること。	
10	外付けキーボード	テンキーを含む JIS キーボードであること。	
11	マウス	USB 接続が可能な有線マウスであること。	
12	USB ハブ	USB3.0 以上に対応した USB ポートを 3 ポート以上備えること。	

(2) 運用支援端末

職員用端末と同一にする。

※受注者が準備する場合を除く。

3.10.3. ソフトウェア構成

本システムのソフトウェア構成に係る要件を以下に示す。

3.10.3.1. ソフトウェア要件（共通要件）

受注者は、本システムの全てのソフトウェアについて以下の共通要件を満たすこと。

(1) 製品サポートに係る要件

(ア) 本システムの運用期間中に、製造元による製品サポート（技術サポート、バグ修正パッチの提供、セキュリティパッチの提供等）が継続して提供されるソフトウェアであること。

(イ) やむを得ず運用期間中にサポート期限を迎えるソフトウェアを導入する必要がある場合は、当該サポート期限を迎える前に、サポートが継続されるバージョンへのバージョンアップ対応及び必要なテスト等を無償で行うこと。

(2) ソフトウェアバージョンに係る要件

(ア) 導入するソフトウェアのバージョンは、原則として本業務の契約時点での最新バージョンとすること。

(イ) 互換性等の理由により最新バージョン以外のソフトウェアを導入する場合は、事前にセンターの承認を得ること。

(3) ライセンスに係る要件

(ア) ソフトウェアの利用者数や導入先のサーバ装置の台数、性能等に応じて、ライセンス費用の観点で適したライセンス形態を選択すること。

(イ) サーバ OS の導入に当たってクライアントアクセスライセンス（CAL）等が必要となる場合は、必要数を用意すること。なお、センターで保有する CAL ライセンスの提供は行わない前提とする。

3.10.3.2. ソフトウェア要件（基盤サービス）

本システムの基盤サービスのソフトウェア構成は、受注者の設計によるものとする。受注者は、本要件定義書の各要件を満たすために必要なソフトウェアを選定し、本システムの基盤サービスを構築すること。

本システムの基盤サービスに最低限必要と考えるソフトウェアの要件を以下に示す。

(1) 統合認証サーバ

(ア) サーバの OS は、「統合認証サービス」の提供に必要なソフトウェアがサポートする最新の Windows Server OS を搭載すること。

(イ) 「統合認証サービス」の提供に必要なソフトウェアを搭載すること。
(ウ) 「システム運用管理・監視サービス」、「バックアップ管理サービス」及び「ログ管理サービス」による管理のために必要なエージェントソフトウェアがある場合は、これを搭載すること。
(エ) 「ウイルス対策管理サービス」で管理可能なウイルス対策ソフトウェアを搭載すること。

(2) Syslog サーバ
(ア) ネットワーク機器等が出力する Syslog ファイルの取得に必要なソフトウェアを搭載すること。
(イ) 「システム運用管理・監視サービス」、「バックアップ管理サービス」及び「ログ管理サービス」による管理のために必要なエージェントソフトウェアがある場合は、これを搭載すること。
(ウ) 「ウイルス対策管理サービス」で管理可能なウイルス対策ソフトウェアを搭載すること。

3.10.3.3. ソフトウェア構成要件（端末サービス）

本システムの各端末に導入するソフトウェアは、以下の要件を満たすこと。

(1) 職員用端末

職員用端末のソフトウェア要件を以下に示す。

表 3-19 職員用端末のソフトウェア要件

No.	ソフトウェア名	ソフトウェア要件	補足
1	クライアント OS	Microsoft Windows 11Enterprise（64bit）であること。	
2	ブラウザ	Microsoft Edge であること。	
3	オフィススイート	Microsoft 365 Apps for enterprise であること。 Word、Excel、PowerPoint、Outlook、Exchange、OneNote、PowerApps	
4	設計図・図面作成ソフトウェア	Microsoft Visio Standard 2024 であること。なお、運用期間中にアップデートが可能となるようにソフトウェアアシュアランス権も有すること。	100 ライセンス用意すること。
5	PDF 編集ソフトウェア	Adobe Acrobat VIPFRL ライセンスの FRL-Offline と同等以上の機能を有する製品であること。	
6	ファイル圧縮・解凍ソフトウェア	Zip 形式の圧縮及び解凍が可能で Windows11 標準機能あること。	
7	端末管理エージェント	「端末管理サービス」による端末管理が可能であること。	
8	ウイルス対策ソフトウェア	「ウイルス対策管理サービス」から一元管理可能なウイルス対策ソフトウェアであること。	

(2) 運用支援端末

運用支援端末のソフトウェア要件を以下に示す。

表 3-20 運用支援端末のソフトウェア要件

No.	ソフトウェア名	ソフトウェア要件	補足
1	クライアント OS	Microsoft Windows 11Enterprise（64bit）であること。	
2	ブラウザ	Microsoft Edge であること。	
3	オフィススイート	Microsoft 365 Apps for enterprise であること。	
4	PDF 編集ソフトウェア	Adobe Acrobat VIPFRL ライセンスの FRL-Offline と同等以上の機能を有する製品であること。	
5	ファイル圧縮・解凍ソフトウェア	Zip 形式の圧縮及び解凍が可能で Windows10 標準機能あること。	
6	運用支援用クライアントソフトウェア	「端末管理サービス」、「システム運用管理・監視サービス」、「バックアップ管理サービス」、「ログ管理サービス」及び「ウイルス対策管理サービス」を用いて本システムの各種運用管理・監視を行うために必要なクライアントソフトウェアを導入すること。	
7	端末管理エージェント	「端末管理サービス」による端末管理が可能であること。	
8	ウイルス対策ソフトウェア	「ウイルス対策管理サービス」から一元管理可能なウイルス対策ソフトウェアであること。	

3.10.4. ネットワーク構成

3.10.4.1. ネットワーク構成図

本システムのネットワーク構成図（論理構成図及び物理構成図）は、受注者の設計によるものとする。なお、ネットワーク構成図の概要は、「図 3-2 想定ハードウェア構成図」を参照すること。

3.10.4.2. ネットワーク要件

本システムのネットワークに係る要件を以下に示す。

(1) 物理構成

（ア）各拠点の WAN と LAN の接続点には、拠点間及びセグメント間の不正な経路による通信を遮断するためのファイアウォールを設けること。

（イ）各拠点のファイアウォールの配下には、フロア又は建屋等の単位でディストリビューションスイッチを設けること。なお、ディストリビューションスイッチの設置単位は以下のフロア・建屋単位を想定しているが、本システムの設計段階において、利用者数、接続機器数、利用帯域、設置場所等を調査の上で、最終的な設置単位及び数量を決定すること。

- 東京本部 3 階
- 東京本部 6 階
- 東海センター 事務棟
- 東海センター 開発試験棟
- 東海センター 保障措置分析棟
- 東海センター 新分析棟
- 六ヶ所センター 1 階
- 六ヶ所センター 2 階

（ウ）各拠点のディストリビューションスイッチの配下には、無線 LAN アクセスポイントへ接続するためのアクセススイッチを設けること。

（エ）無線 LAN アクセスポイントの設置単位は以下のフロアを想定しているが、本システムの設計段階において、利用者数、接続機器数、利用帯域、設置場所等を調査の上で、最終的な設置単位及び数量を決定すること。

- 東京本部 3 階（3 台）
- 東京本部 6 階（4 台）
- 東海センター 事務棟 1 階（3 台）
- 東海センター 事務棟 2 階（4 台）
- 東海センター 開発試験棟 （3 台）
- 東海センター 新分析棟 1 階（1 台）
- 六ヶ所センター 1 階（3 台）
- 六ヶ所センター 2 階（3 台）

(オ) 無線 LAN の設計、構築時にサイトサーベイを実施し、その結果を用いて適切な電波設計を行うこと。
(カ) 職員用端末及び個別業務システムの LAN サービスの配線は、現行システムの配線を流用すること。移行時は必要に応じて配線を実施すること。
(キ) 各拠点のネットワーク機器（ディストリビューションスイッチを除く）は、原則として冗長化を不要とする。ただし、「3.17 保守に関する事項」に示す保守作業の効率化に寄与し、かつ本システムのライフサイクルコストの低減に有効である場合には、機器の冗長化についてセンターに提案してもよい。

(2) 論理構成（セグメント構成）

(ア) 拠点間や外部との接続に関するセキュリティ対策、機器の役割、機器間のトラフィック量等を踏まえ、VLAN 機能等による適切なセグメント分割を行うこと。
(イ) 機密性の高い情報を保存するサーバを収容するための、重要サーバセグメントを設けること。
(ウ) 基盤サービスや各種ネットワーク機器を管理するための運用管理・監視用セグメントを設けること。
(エ) セグメント間の通信は、必要最低限の通信のみ許可する設計とし、設定に先立ち、設計内容をセンターへ説明し承認を得ること。
(オ) 許可されないセグメント間通信が発生した時は、直ちにログに記録すると同時に通知する機能を有すること。なお、「システム運用管理・監視サービス」や「ログ管理サービス」等との連携により実現してもよい。

(3) ネットワークセキュリティ

(ア) 各セグメント間の通信は、ファイアウォールにより業務上又はシステム上必要な通信のみを許可し、その他の通信を遮断すること。
(イ) MAC アドレス認証等によるポートセキュリティ機能により、許可されていない機器の接続を防ぐための対策を講ずること。
(ウ) ネットワーク機器の運用や設定変更等を行うための管理機能については、SSH 等による認証及び暗号化並びにアクセス制御を行うとともに、操作ログを取得できること。
(エ) 無線 LAN 環境を提供するにあたり、複数の IP アドレスを払い出せる DHCP の機能及びデジタル証明書での認証が可能な RADIUS の機能として、最適と考えるものを提案すること。

(4) 回線帯域・プロトコル等

(ア) 導入する機器類及びケーブル類は、原則として 1Gbps 以上の通信速度に対応した規格（1000BASE-T 等）を採用すること。
(イ) 建屋間の配線等、長距離配線が必要な場合には、配線距離に応じて適切な規格（光ファイバ等による規格）を採用すること。

(ウ) 使用するプロトコルについては標準プロトコル又は業界標準のプロトコルの利用を基本とし、物理層・データリンク層については IEEE802.3 及びその拡張版を採用し、ネットワーク層、トランスポート層については TCP/IP に対応すること。
(エ) 機器の冗長化を行う場合は、VRRP や STP 等の実績のある規格及び方式を採用すること。

(5) 運用管理・監視機能

(ア) LAN を構成する全てのネットワーク機器について、ICMP、SNMP 等に対応する機器を選定し、「システム運用管理・監視サービス」よる統合管理を可能とすること。
(イ) LAN を構成する全てのネットワーク機器について、ログの転送による「ログ管理サービス」でのログの一元管理を可能とすること。

3.10.5. 施設・設備要件

3.10.5.1. 設置要件

(ア) センターの各拠点（東京本部、東海センター及び六ヶ所センター）の設置環境（電源環境、ラックスペース、配線環境等）について、事前に現地調査を行い、センターと協議の上で各機器の設置方法を定めること。
(イ) 設置に必要となる一切の機器・機材（ラック、電源ケーブル、通信ケーブル、その他部材等）については、受注者により準備すること。なお、センターの各拠点の既存のラックや電源等を利用できる場合があるため、利用可能な既存設備については、現地調査とあわせてセンターへの確認を行うこと。
(ウ) 東海センターにおいては、複数建屋をまたがる接続を行う必要があるため、建屋間の配線が必要となることに留意すること。ただし、現在敷設済みの未使用光ファイバケーブル（1Gbps 対応規格、SC コネクタ）のメディアコンバータを交換することにより、既存ケーブルを活用してもよい。敷設済みの設備については閲覧資料「既存のネットワークに係る資料一式」を参照の上で、現地調査時に確認を行うこと。

3.11. テストに関する事項

3.11.1. テストの種類及び概要

受注者は、表 3-21 に示すテストを実施すること。各テスト開始前にテスト計画書及びテスト仕様書を作成し、センターの承認を得ること。

また、各テスト終了時に、実施内容、結果及び次工程への申し送り事項等について、テスト結果報告書に記載し、センターに報告すること。

表 3-21 テストの種類及び概要

No.	テストの種類	テストの概要
1	単体テスト	(ア) クラウドサービス、サーバ、ネットワーク機器等の機器単位において、ハードウェア・ソフトウェアの起動、停止、設定確認等を行う。
2	結合テスト	(ア) 本システムのサービス単位でクラウドサービス、ハードウェア、ソフトウェア及び必要に応じてネットワークを組み合わせ、各サービス単位での動作の確認を行う。 (イ) 本システムが「詳細設計書」どおりに構築されていることを確認する。
3	総合テスト	(ア) 本システムの拠点間のネットワークを接続し、各サービスを組み合わせ、システム全体で機能要件及び非機能要件を満たすことを確認する。 (イ) 本システムが「基本設計書」どおりに構築されていることを確認する。
4	受入テスト	(ア) 本システムが要件定義書（確定版）において要求した事項を備えているかどうかを、センターの役職員が確認する。受注者は受入テストの支援を実施する。

3.11.2. テスト環境及びテストデータ等

テストの実施に当たってのテスト環境、テストデータ等について以下を満たすこと。

(1) テスト環境の要件

(ア) 各テストの実施に当たっては、現行システムの安定稼働に影響が出ないようにすること。

(イ) 総合テスト及び受入テストは、各拠点間が接続されている状態で実施すること。

(2)　**テストデータ・テストツールの要件**

(ア) 各テストの実施に当たり必要となるテストデータは、受注者が擬似データを作成すること。

(イ) 単体テスト、結合テスト、総合テストにおいてテスト実施時の証跡を取得、保存すること。

(ウ) テストで使用したテストデータ、テストツール等は、本システム稼動後の運用保守工程で再利用できるようにしておくこと。

3.12. 移行に関する事項

本システムの移行要件を以下に示す。

3.12.1. 移行方針

(ア) 移行は、図 3-3 に示す移行期間に、以下の作業を行うことにより実施するものとする。

① 受注者は、本システムの提供する各サービスのサービス提供を開始する。提供するサービスは、ネットワークサービス及び基盤サービスだけではなく、端末サービスも含み、職員用端末、ウイルススキャン端末及び運用支援端末の設定を行う。

② 受注者は、職員用端末を各役職員に配付する。

③ 受注者は、現行の統合認証サービスの Active Directory 関連データ（アカウント情報、グループポリシー等）移行を行う。

④ 役職員は、現行の職員用端末から、本システムの職員用端末へのデータ（電子メールデータ、電子ファイル等）移行を行う。

⑤ 受注者は、現行のファイル共有サービスから本システムのファイル共有サービスへのデータ移行を行う。

⑥ 担当原課は、移行対象の個別業務システムについて、現行のネットワークから本システムのネットワークへの移行を順次行う。

⑦ 担当原課は、ファイル共有機能を有する個別業務システムから、本システムのファイル共有サービスへのデータ移行を実施する。

⑧ 本システムは、移行作業完了まで既存システムと並行運用出来るよう考慮する。

・ 受注者は、構築フェーズ終了までに「3.12.2.1 移行計画」に示す作業を行う。

・ 上記(ア)④～⑦の作業に十分な時間を確保するため、受注者は、移行期間の極力早い時期に、（ア）①～③の作業を行い、表 2-2-1 に示す全てのサービスを提供する。

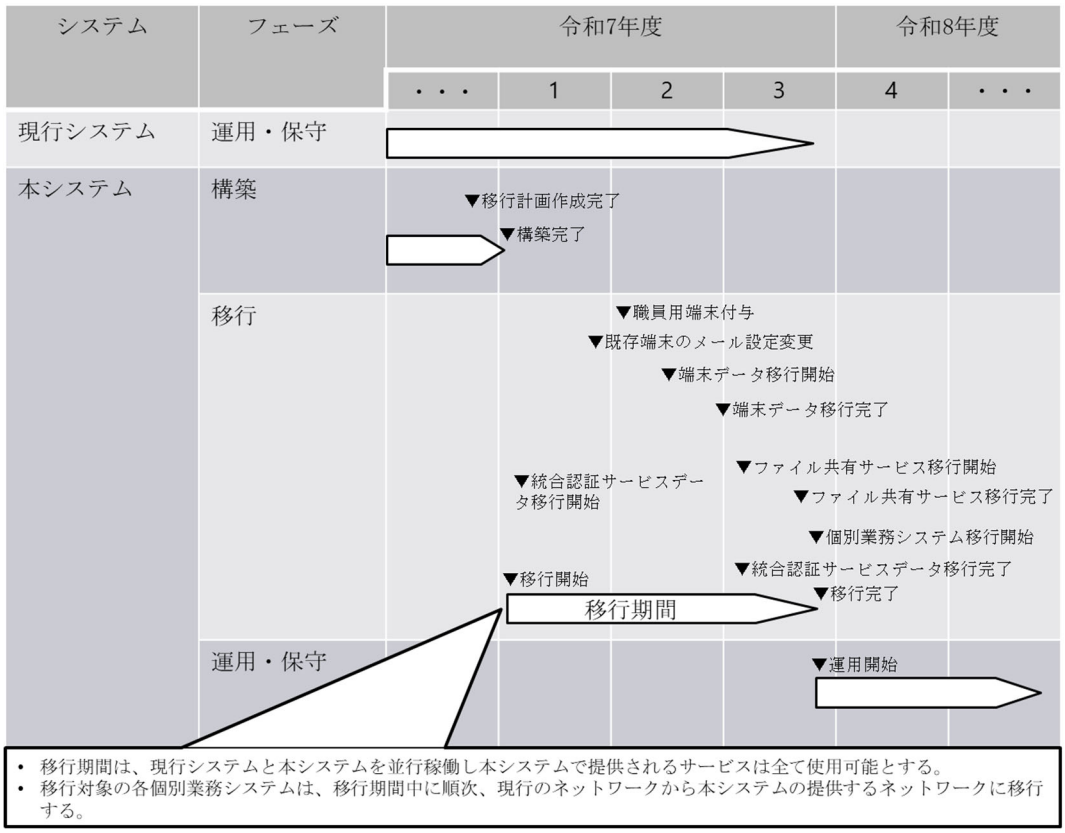


図 3-3 本システムの構築・移行作業スケジュール

3.12.2. 移行に係る作業要件

受注者は、本システムの移行に当たり、以下の作業を実施すること。

3.12.2.1. 移行計画

(ア) 構築フェーズの終了までに、「3.12.1 移行方針」の方針に沿って、移行スケジュール、移行方式等、移行に必要な作業を整理し、移行計画を取りまとめ、「移行計画書」を作成すること。また、具体的な作業手順については、別途「移行手順書」を作成すること。「移行計画書」及び「移行手順書」は、センターの承認を得ること。

(イ) 移行計画には、サーバ、ネットワーク機器の起動、各種サービスの設定変更のほか、各個別業務システムの移行、職員用端末の配付計画も含めること。本要件定義書作成時点で移行対象と想定している個別業務システムを「付録 1 移行対象システム一覧」に示す。

(ウ) 移行のために必要な環境及び移行方法は、移行失敗リスク、コスト、役職員への影響等を考慮し、最適と考えるものを提案すること。

(エ) 各個別業務システムの移行スケジュール、移行に必要な作業等は、センターの担当者と調整の上、それぞれ決定すること。

(オ) 現行システムの認証情報、権限情報の提供等、移行に当たり各個別業務システムの担当原課に求める作業は、移行計画に含めること。

(カ) ファイル共有サービスのデータ移行に関し、データ移行時間の確認やデータ移行リハーサルが必要となる場合には、その実施可否、実施方法、役割分担等についてセンターの合意を得た上で、必要な作業を行うこと。
(キ) 端末配付時に役職員が実施する作業は、「端末移行マニュアル」に記載すること。ただし、職員用端末の使用に当たって役職員が行う設定等の作業は最小限とすること。
(ク) 移行に当たりセンターの担当者が実施する組織内の調整について、これを支援すること。
(ケ) センターの役職員に対して、移行方針及び移行に係る作業の進め方について、移行説明会を実施すること。
(コ) 移行データの本システムへのインポートにおいて移行用のツール等を要する場合には、必要なツールを受注者にて準備し、事前にテストを実施すること。

3.12.2.2. 移行期間に実施する作業

(ア) 「移行計画書」及び「移行手順書」に従い、センターの WAN への接続設定、本システムの提供する各サービスの起動、ネットワーク機器等の設定、ウイルススキャン端末及び運用支援端末の設定、設置等を実施し、本システムの提供する各サービスを利用可能とすること。
(イ) 受注者は端末移行マニュアルを作成し、リハーサルを行う。
(ウ) 職員用端末は、必要な設定を行った上で、センターの各拠点に配付すること。
(エ) 現行の職員用端末から本システムの職員用端末へのデータ移行は、センターの各役職員が実施する。受注者は、役職員からの問合せへの対応を行う等、漏れなくデータが移行できるように支援すること。
(オ) 職員用端末には、一部の担当原課又は役職員にのみ導入が必要なソフトウェアが存在する。受注者は、導入に当たっての担当原課又は役職員からのソフトウェア導入に関する問合せへの対応を行う等の支援を行うこと。
(カ) 移行に当たり既存の機器やサービスを停止する必要がある場合は、停止日時、停止時間等について事前にセンターと協議の上で、業務への影響が極力生じないよう休日夜間に実施すること。
(キ) センター及び担当原課は、現行のファイル共有サービスから本システムのファイル共有サービスにデータ移行を行う。移行完了後、センター及び担当原課は移行したデータが適切か確認を行う。
(ク) 個別業務システムの移行については、個別業務システムの機器に対してセンターにて各種設定変更を行い本システムにて利用出来るように移行する。個別業務システムのシステムごとの設定項目を整理し必要な設定値を展開するとともに切り替え日の取りまとめを行い移行作業の支援を行う。各個別業務システムの担当原課との認識の相違が発覚した場合等、移行に係る作業を行う上での支障が発覚した場合は、速やかにセンターに報告し、解決に向けた調整・協議において、センターを支援すること。

(ケ) 移行期間の終了時には、作業の実施内容や結果について、「移行結果報告書」に記載の上、センターに報告すること。

3.13. ケーブル敷設工事に関する事項

本システムのケーブル敷設工事に係る作業内容を以下に示す。

3.13.1. 事前確認

工事に当たり、工事資材の搬入経路や配線場所等の事前確認をセンターと調整した上で行うこと。

3.13.2. 工事現場管理

工事を完成させるために、施工管理体制を確立し、品質、工程、安全等の施工管理を行うこと。

3.13.3. ケーブル敷設作業

各拠点のケーブル敷設に当たっては、以下の条件に留意すること。

- ケーブルは公共建設工事標準仕様書（電気設備工事編）令和4年度版に記載の内容に従い、敷設すること。
- 現地確認を行い、ケーブルの引き込みが困難と判断する施工箇所がある場合は、センターと協議の上、ケーブル敷設のため貫通工事を行うこと。
- ケーブルの両端に表示札を取り付け、名称、品名、接続先、施工年等の情報を記載すること。
- 適切な養生を行い、施設や什器類、他システムの機器等に損害を与えないこと。受注者の責めに帰する事由により損傷等を与えた場合、受注者の負担と責任により原状に復すること。
- 配線完了後にケーブルの伝送品質測定を行うこと(メーカー出荷時に伝送品質検査済みのものを除く)。
- 配線完了後に伝送損失の測定を行うこと。なお、市場の一般的な SFP モジュールの仕様を確認し、その許容伝送損失以下であることを確認すること。
- 工事の記録として施工写真を撮影すること。

3.13.4. 搬入及び後片付け

当該工事に関する部分の後片付け及び清掃を行うこと。

3.13.5. 作業日程等の条件

作業はシステムに影響を与えない事を前提に休日（土日・祝日）に実施すること。実施ただし、センターと協議し、作業時間等について合意を得た上で平日での作業も可能とする。

3.14. 引継ぎに関する事項

本システムの引継ぎに係る要件を以下に示す。

3.14.1. 現行システム関係事業者からの引継ぎ

受注者は、本業務を実施するために必要な情報（引継ぎが必要な残存課題、検討事項等）について、引継ぎ元である現行システム関係事業者（運用支援事業者、保守事業者等）からの引継ぎを受けること。

3.14.2. 第 3 期基盤情報システム関係事業者への引継ぎ

受注者は、第 3 期基盤情報システム関係事業者に対し、以下の引継ぎを行うこと。引継ぎは、本システムの運用終了までに実施すること。

(ア) 本システムの全体構成、設計・開発に係る各種資料・情報

第 3 期基盤情報システム関係事業者の本システムの理解のため、適宜、設計書、テスト結果等を用いて、システムの概要や本システムで提供するサービス・機能の説明を行うこと。

(イ) 本システムの残課題

本システムの残課題について、第 3 期基盤情報システム関係事業者への引継ぎを行うこと。引継ぎに当たっては、各課題の対応主体や、対応期限等を明確にすること。

(ウ) 運用保守に係る各種資料・情報

第 3 期基盤情報システム関係事業者が業務を理解し、円滑に運用保守業務を実施できるよう、運用保守計画、運用保守実施要領、運用保守手順書等、運用保守業務、中長期運用保守作業計画書に係る各種資料を基に説明し、運用保守業務を引き継ぐこと。また、第 3 期基盤情報システム関係事業者に対し、情報提供や問合せ対応等のほか、必要に応じて運用上や現行システムからの変更点について研修を行う等の支援を行うこと。

(エ) その他、引継ぎが必要と考えられる資料・情報

上記のほか、引継ぎが必要と考えられる資料・情報があれば、文書等にまとめ、第 3 期基盤情報システム関係事業者に説明を行うこと。

3.14.2.1. 引継ぎ手順

(ア) 引継ぎ作業の結果は「引継ぎ結果報告書」に取りまとめ、センターに提出すること。

3.15. 教育に関する事項

3.15.1. 教育対象者、教育内容、教育方法等

本業務において実施を求める教育の対象者、教育内容、教育方法等を以下に示す。

表 3-22 教育対象者、教育内容、教育方法等

No.	教育対象者	教育内容	教育の実施時期	教育方法	教材	教育対象者数
1	受入テスト実施担当	受入テストの実施手順	受入テスト開始時	センターの各拠点における集合研修(3 拠点)	説明資料(受入テスト用)、受入テスト関連資料	数人程度
2	全ての役職員	本システムの利用方法	移行前	センターの各拠点における集合研修(3 拠点)	説明資料(全役職員用)、基盤情報システム利用者マニュアル	約 190 名(合計)
3	全ての役職員	職員用端末の移行作業手順	移行前	教材の配付	端末移行マニュアル	約 190 名(合計)

3.15.2. 教育に係る作業要件

(1) 教育実施計画書の作成

受注者は、教育開始前までにセンターと協議の上、受注者の体制や役割を定め、以下の事項について記載した「教育実施計画書」を作成し、センターの承認を得ること。

- 体制及び役割(センター担当者/受注者)
- 教育内容
- 教育スケジュール
- 対象者
- 教育環境
- 教育方法
- その他研修実施に当たって必要と考えられる事項

(2) 研修の実施

受注者は、教育実施計画書に従い、教育を実施すること。

教育に当たって必要な端末及び物品については受注者で用意すること。また、集合研修後、教育対象者に対し、研修の理解度等についてアンケートを実施すること。

3.15.3. 研修の実施報告と評価

教育の完了後、集合研修で取得したアンケート結果等に基づき報告書を取りまとめ、センターに報告すること。また、センターから改善要求があった場合は、教材等の修正を行うこと。

3.15.4. 教材の作成方針

(ア) 教材は、研修開始の 2 週間前までに用意すること。なお、集合研修で使用する教材は、そのまま利用者個人による自己学習用の教材としても利用できるように作成すること。

(イ) 基盤情報システム利用者マニュアル及び端末移行マニュアルは、画面キャプチャ等を用いて、作業手順や操作方法のイメージが理解し易い構成とすること。

3.15.5. 教材の種類と概要

本システムにおける教材の種類、概要及び実施時期を表 3-23 に示す。

表 3-23 教材の種類及び概要

No.	教材	教材の概要	補足
1	説明資料（受入テスト用）	受入テストで実施する作業、手順の概要等を説明したもの。	PowerPoint 形式の資料を想定
2	受入テスト関連資料	受入テスト実施担当が行う受入テストにおいて、テスト体制、テスト環境、テストスケジュール、作業内容、テストシナリオ、合否判定基準等を説明したもの。	
3	説明資料（全役職員用）	本システムにおける各サービスの概要、利用方法等を説明したもの。	PowerPoint 形式の資料を想定
4	基盤情報システム利用者マニュアル	役職員が端末から利用するサービスの操作方法等について説明したもの。	Word 形式及び PDF 形式の資料を想定
5	端末移行マニュアル	職員用端末の移行において、役職員が実施するデータ移行、設定変更等の作業や手順を説明したもの。	Word 形式及び PDF 形式の資料を想定

3.16. 運用に関する事項

本システムの運用要件を以下に示す。受注者は、本項に示す運用要件を実施可能となるよう本システムを構築するとともに、必要な運用作業を行うこと。

3.16.1. 作業条件

運用業務の作業条件を以下に示す。

3.16.1.1. 対応時間、実施頻度

各作業の対応時間及び実施頻度を以下に示す。

表 3-24 各運用作業の対応時間及び実施頻度

No.	作業分類	作業項目	対応時間	実施頻度	補足
1	運用管理・監視等業務	死活監視	平日 9:00～17:30（※1）	常時	本システムのシステム運用管理・監視サービス、バックアップ管理サービス及びログ管理サービスを利用して実施することを想定
2		リソース監視			
3		セキュリティ監視			
4		バックアップ管理			
5		ログ管理			
6		問題・インシデント対応		随時	監視等により異常を検知した場合に実施
7		ファームウェア等の脆弱性管理支援		日時	―
8		ソフトウェアの脆弱性管理		日時	―
9		計画停止	休日又は平日 9:00～17:30 以外の時間帯	随時	インシデント対応、セキュリティパッチの適用作業等に対応
10		構成管理	平日 9:00～17:30	随時	システム構成の変更時に実施

※1：対応時間外の作業が必要な場合はセンターと協議し、作業時間等について合意を得た上で作業を行うこと。

3.16.1.2. 作業場所・作業環境

(ア) 原則としてセンターの東京本部に常駐又は受注者の運用保守拠点より作業を実施すること。なお、センターからの指示があった場合は、東京本部、東海センター及び六ヶ所センターでの現地作業を実施すること。

(イ) 運用作業の実施に当たっては、原則としてセンターが用意する本システムの「運用支援端末」(6 台程度)を利用すること。なお、「2.1.2.3.(3) 運用支援端末」の要件を満たすことで、受注者が用意する端末を運用支援端末として利用することを提案してもよい。

3.16.2. 運用管理・監視等要件

本システムの運用管理・監視等に係る作業要件を以下に示す。

3.16.2.1. 死活監視

本システムを構成するサーバ、ネットワーク機器等の稼動状況を監視し、障害の発生を早期検知するため、以下の監視を実施すること。

なお、監視の実施に当たっては、本システムの「システム運用管理・監視サービス」を利用すること。

(1) 監視対象

死活監視の対象は、本システムを構成するサーバ、ネットワーク機器等とすること。

(2) 監視内容

以下の監視を行い、「システム運用管理・監視サービス」のアラート等により異常を検知した際はセンターの担当者へ報告すること。

(ア) 定期的なポーリング等により、本システムの稼働状況、ハードウェアの異常・障害を検知すること。

(イ) ハードウェアの異常時等に発行される SNMP トラップを検知すること。

(ウ) ハードウェア及びソフトウェア製品から出力されるログを監視し、エラー等を検知すること。

(エ) サーバに搭載するソフトウェア製品のプロセス(サービス)を監視し、プロセスダウンを検知すること。

3.16.2.2. リソース監視

本システムを構成するサーバ、ネットワーク機器等の稼動状況を監視し、リソースの不足・逼迫等を検知するため、以下の作業を実施すること。

なお、監視の実施に当たっては、本システムの「システム運用管理・監視サービス」を利用すること。

(1) **監視対象**

リソース監視の対象は、本システムを構成するサーバ、ネットワーク機器等とすること。

(2) **監視内容**

以下の監視を行い、「システム運用管理・監視サービス」のアラート等により異常やリソース不足を検知した際はセンターの担当者へ報告すること。

(ア) CPU 使用率、メモリ使用率、ストレージ空き容量、ネットワーク帯域等のリソースを監視し、しきい値を超えた場合に検知すること。

3.16.2.3. セキュリティ監視

本システムの情報セキュリティに関する事象の発生を監視し、情報セキュリティ上の脅威を早期検知するため、以下の作業を実施すること。

なお、監視の実施に当たっては、本システムの「システム運用管理・監視サービス」、「端末管理サービス」、「ウイルス対策管理サービス」、「クラウドプロキシサービス」等を利用すること。

(1) **監視対象**

セキュリティ監視の対象は、本システムを構成するサーバ及びネットワーク機器等とすること。

(2) **監視内容**

以下の監視を行い、「システム運用管理・監視サービス」等のアラート等により異常を検知した際はセンターの担当者へ報告すること。

(ア) ファイアウォールにおけるブロックの発生状況を監視し、異常を検知すること。
(イ) 統合認証サービス、クラウド認証サービス等における認証の失敗状況を監視し、異常を検知すること。
(ウ) サーバ及び端末の不正プログラム検知状況を監視し、異常を検知すること

3.16.2.4. バックアップ管理

本システムのバックアップを取得・管理し、障害・災害時に本システムを復旧可能とするため、以下の作業を実施すること。

なお、バックアップ管理の実施に当たっては、本システムの「バックアップ管理サービス」の機能を利用すること。

(1) **管理対象**

バックアップ管理の対象は、「3.8.2 継続性に係る対策」に示すデータを対象とすること。

(2) **作業内容**

作業内容の要件を以下に示す。

(ア) 「バックアップ管理サービス」のスケジュール設定等を利用し、バックアップ対象データに対し、定期的にバックアップデータを取得すること。
(イ) バックアップデータについて、必要な世代管理を行うこと。
(ウ) ハードウェアの故障やデータ破壊が発生した場合、必要に応じて、バックアップデータからの復旧作業を行うこと。なお、復旧作業は「3.16.2.6 問題・インシデント対応」に基づいて対応すること。

3.16.2.5. ログ管理

本システムのログ監視や証跡管理等を行うため、ログ管理に係る以下の作業を行うこと。

なお、ログ管理の実施に当たっては、本システムの「ログ管理サービス」の機能を利用すること。

(1) **管理対象**

ログ取得の対象は、本システムを構成するサーバ及びネットワーク機器とすること。管理対象ログファイルを以下に示す。

表 3-25 管理対象ログファイル

No.	対象ログファイル	概要及び用途	保管期間
1	ソフトウェアログ	クラウドサービス、サーバ、ネットワーク機器及びソフトウェア等の動作に伴い出力されるログファイル。障害発生時の原因特定や追跡調査の際に利用する。	1 年間
2	証跡管理用ログ	情報セキュリティインシデント発生時に原因の特定、追跡調査及び点検等に用いる。	1 年間
3	性能情報	サーバの稼動統計情報が記録されたログファイル。リソース使用状況の確認に利用する。	1 年間

(2) **作業内容**

作業内容の要件を以下に示す。

(ア) 本システムの「ログ管理サービス」により、管理対象ログの収集及び蓄積を行うとともに、正常にログを収集・蓄積できていることを定期的に確認すること。
(イ) サーバ、ネットワーク機器等のログ（syslog）の出力内容、レベル（情報/警告/重大/エラー等）別の出力件数等を確認・記録し、異常を検知した場合はセンターの担当者に報告すること。なお、ログの出力内容、レベル等については設計時に検討し、センターと協議の上、決定すること。
(ウ) センターからの求めに応じて、蓄積されたログに対して「ログ管理サービス」の機能を用いて集計・解析等を行い、結果をセンターに報告すること。

3.16.2.6. 問題・インシデント対応

本システムの異常や問題等を検知した際は、以下の要件に基づき必要な対応を行うこと。

(ア) 以下の例に示す異常、障害、問題等（以下「インシデント」という。）を検知した場合は、センターに報告すること。
- 死活監視により、本システムの異常、障害等を検知した場合
- リソース管理により、本システムのリソース不足を検知した場合
- バックアップ管理により、バックアップの異常、失敗等を検知した場合
- ソフトウェア脆弱性管理により、本システムに関係のある脆弱性情報やバージョンアップ情報を入手した場合
- データ破損等により、バックアップデータからのリカバリが必要となった場合
- その他、本システムに関連する問題が発生した場合

(イ) 発生したインシデントに対し、センターと協議の上で当該事象の調査、発生原因の調査、対応方法の検討及び復旧対応を行うこと。

(ウ) インシデントへの対応完了後には、当該インシデントの発生経緯、原因、復旧作業、再発防止策等について取りまとめた報告書を作成し、センターの確認を受けること。

3.16.2.7. ファームウェア等の脆弱性管理支援

本システムのハードウェアに搭載されたファームウェアの脆弱性情報を管理するため、以下の作業を実施すること。

(ア) 本システムのハードウェアに搭載されたファームウェアにおける脆弱性対策の状況（脆弱性の公開情報及び製造元によるセキュリティパッチ又はバージョンアップの公開状況等）を定期的に確認すること。

(イ) 脆弱性対策状況の確認によって脆弱性情報を入手した場合、適用可否の方針案の作成を支援し、センターへ報告すること。

(ウ) 運用保守チームメンバの保守担当者が行うセキュリティパッチ又はバージョンアップ対応を支援すること。この際、必要に応じて本システムの運用保守チームメンバの保守担当者への連絡・確認を行うこと。

3.16.2.8. ソフトウェアの脆弱性管理

本システムのソフトウェア製品の脆弱性情報を管理するため、以下の作業を実施すること。

(ア) サーバ、端末及びネットワーク機器で利用するソフトウェアにおける脆弱性対策の状況（脆弱性の公開情報及び製造元によるセキュリティパッチの公開状況等）を定期的に確認すること。

(イ) 脆弱性対策状況の確認によって脆弱性情報を入手した場合、適用可否の方針案を検討し、センターへ報告すること。
(ウ) 運用保守チームメンバの保守担当者から受領する手順及び必要な電子ファイルを基にセキュリティパッチ又はバージョンアップ対応をすること。この際、必要に応じて本システムの運用保守チームメンバの保守担当者への連絡・確認を行うこと。
(エ) 上記の対応の結果、本システムが正常に動作していることを確認すること。
(オ) 対応日時、対応内容等について報告書を作成し、センターに報告すること。

3.16.2.9. 計画停止

障害対応やセキュリティパッチの適用のために計画停止を行う必要がある場合は、センターと協議の上で以下の要件に基づき計画停止を行うこと。

(ア) 問題・インシデント対応やセキュリティパッチの適用等を目的として、計画停止の必要がある場合、作業計画を策定し、センターの承認を得ること。
(イ) 作業計画には、計画停止中に行う作業の切り戻しのための判断基準、期限、手順等を記載すること。
(ウ) 作業計画に基づき、機器類又はソフトウェアの停止による計画停止を行い、必要な作業を実施すること。
(エ) 作業実績等を取りまとめた報告書を作成し、センターへ提出すること。

3.16.2.10. 構成管理

本システムを構成するクラウドサービス、ハードウェア、ソフトウェア及びネットワークについて、以下の要件に基づく構成情報の管理を行うこと。

(1) 管理対象

構成管理の対象は、本システムを構成するクラウドサービス、サーバ及びネットワーク機器とすること。

構成管理における管理対象は以下に示す例に基づき、センターの承認を得た上で定めること。

表 3-26 管理対象

No.	資産	管理項目（例）	整備する文書（例）
1	クラウドサービス	利用サービス等の名称、クラウドサービス等の提供者の名称、利用期間、クラウドサービス等の概要、ドメイン名、クラウドサービス等で取り扱う情報の格付及び取扱い制限に関する事項、情報の暗号化に用いる鍵の管理主体、クラウドサービス等で取り扱う情報が保存される国・地域、サービスレベル等	・ クラウドサービス一覧
2	ハードウェア	メーカー名、品番、シリアル番号、数量、設置場所、OS、バージョン、実装メモリ、ハードディスク容量、MAC アドレス（※）、IP アドレス 等	・ ハードウェア一覧 ・ ハードウェア構成図
3	ソフトウェア	名称、バージョン、数量、契約ライセンス数、サポート期限、使用済ライセンス数、媒体保管場所 等	・ ソフトウェア一覧 ・ ハードウェアとソフトウェアの関連図
4	ネットワーク	ネットワーク種類、帯域、設定情報 等	・ ネットワーク接続構成図 ・ ネットワーク機器構成図
5	その他（ケーブル、消耗品等）	名称、数量、購入日、設置場所、保管場所 等	・ 消耗品一覧

※MAC アドレスの登録が必要となる機器等のみ

(2) **対応内容**

構成管理における対応内容の要件を以下に示す。

(ア) 本システムを構成するクラウドサービス、ハードウェア、ソフトウェア、ネットワーク等の各資産を台帳等により記録し、適切に管理すること。

(イ) 本システムの構成を変更した際には、変更内容等の情報をセンターに報告し、それらの情報を更新すること。

3.16.3. 業務運用支援作業

情報セキュリティ室の業務を支援するための、業務運用支援の要件を以下に示す。

受注者は、本項に定める事項の他、機器の設定情報、マニュアル、機器取扱説明書等を充分理解のうえ実施するものとし、あらかじめ業務の分担、人員配置、スケジュール、実施方法等について実施要領を定めセンターの確認を受けること。

3.16.3.1. 定常業務

(ア) ウイルス対策ソフトウェアの更新確認

- パターンファイルの更新があった場合には、ウイルス対策ソフトウェアが導入されているセンターの各種端末・サーバへの適用を実施するとともに、適用状況を確認・記録すること。
- 東京本部、東海センター及び六ケ所センターに設置されているウイルススキャン端末（スタンドアロン環境、数台程度）に対しては、現地の職員がパターンファイルの適用を実施するため、パターンファイルの提供、作業手順の連絡等の支援の実施方法を提案すること。

(イ) 情報セキュリティ関連情報の確認

- JPCERT/CC 等により公開された脆弱性情報を確認し、センターの情報システムで利用しているハードウェア・ソフトウェア等への影響がある情報について、センターの担当者へ報告すること。

(ウ) セキュリティパッチの適用

- センターの情報システムで利用しているハードウェア・ソフトウェア等のセキュリティパッチ（セキュリティアップデートを含む。）の情報が公開された際に、当該パッチファイルを入手し、関係する情報システムへのパッチ適用を実施すること。
- セキュリティパッチの適用に当たっては、事前に情報システムへの影響度を調査した上で、適用可否を判断すること。

(エ) 情報システムの設定変更

- センターからの求めに応じて、センターが管理する情報システムの設定変更作業を実施すること。なお、設定変更を行う主な対象及び実施頻度を以下に示す。

表 3-27 主な設定変更対象及び実施頻度

No.	対象	設定変更例	実施頻度
1	統合認証サービス	アカウントの登録・変更・削除、権限の変更、グループポリシーの変更	随時 （月 1 回程度を想定）
2	内部 DNS サービス	レコードの設定変更	随時 （年 1 回程度を想定）
3	ファイル共有サービス	アクセス権限の変更、記憶領域の追加割当	随時 （月 1 回程度を想定）
4	メールサービス	メールアカウントの設定の変更	随時 （月 1 回程度を想定）
5	端末管理サービス	管理対象の追加・変更・削除、デバイス管理の設定の変更	随時 （月 1 回程度を想定）
6	ログ管理サービス	保存対象の変更、保存期間の変更	随時 （年 1 回程度を想定）
7	ネットワーク機器等	不正通信元 IP アドレスからの通信遮断 等	随時 （月 1 回程度を想定）
8	クラウドプロキシサービス	ブラックリスト対象 URL の追加・変更・削除等の設定変更	随時 （月 1 回程度を想定）
9	各種ソフトウェア製品	ウイルス対策ソフトウェアの検索エンジンのアップデート、Web 接続先のフィルタ設定	随時 （年 1 回程度を想定）

(オ) PC 端末交換時の初期設定作業

- PC 端末（職員用端末及び運用支援端末）の故障等により交換が必要となった場合に、予備機に対して必要な初期設定（アカウント設定、ネットワーク設定、ライセンス設定等）を行い、端末の交換対応を行うこと。
- 予備端末の OS 及び標準ソフトウェアのインストール等のキッティング作業を実施すること。
- PC 端末の交換時の初期設定作業を効率的に行うために、必要に応じて端末のシステムバックアップ等の取得・管理を行うこと。

(カ) ヘルプデスク支援業務

- 情報セキュリティ室の職員がセンターの役職員から質問を受け付けた際に、回答・助言等の支援を行うこと。
- ヘルプデスク支援における情報セキュリティ室からの問合せ内容、回答・助言内容、対応内容等を記録し、管理すること。

- 情報システムのハードウェア製品のファームウェアのバージョンアップまたはパッチ適用を実施するに当たり、必要なアップデートファイル、技術情報など必要に応じて適切な窓口に問合せを行う。
- 情報システムのソフトウェア製品のバージョンアップまたはパッチ適用を実施するに当たり、必要なアップデートファイル、技術情報など必要に応じて適切な窓口に問合せを行う。
- 情報システムのハードウェアに関する技術的な問合せを行う。

3.16.3.2. 定常外業務

(1) 情報セキュリティインシデント対応

(ア) インシデント検知時の対応を運用計画及び運用実施要領に基づき実施すること。
(イ) ウイルス対策管理サービスによるマルウェアを検知した場合、当該サービスの提供ベンダへの連絡・確認を行うとともに、当該検知内容への対応を実施すること。
(ウ) システム運用管理・監視サービス、ウイルス対策管理サービス等により不審な通信を検知した場合、当該通信元の調査及び通信の遮断設定等の対応を実施すること。
(エ) その他、情報セキュリティインシデント発生時に、ログ情報の調査等の証跡確認を実施すること。

(2) 原因調査及び再発防止策の検討支援

(ア) センターが情報セキュリティインシデントの原因調査及び再発防止策の検討を実施するに当たり、情報システムの調査、公開情報の調査、情報提供等の技術的支援を実施すること。

3.16.4. その他支援作業

(1) 外部発注業者との打合せ支援

(ア) センターが他の外部発注業者との打合せを行う際、センターからの求めに応じて、同席、助言、情報提供等の技術的支援を行うこと。

(2) 情報セキュリティ対策の検討・導入支援

(ア) センターが情報セキュリティ対策の導入等について検討する際、センターからの求めに応じて、助言、情報提供等の技術的支援を行うこと。

(3) **ログ情報等の現地収集**

(ア) 東京本部、東海センター及び六ヶ所センターのスタンドアロン環境等のログ情報や設定情報等を収集する必要が生じた際は、現地での情報収集作業を実施すること。

(4) **サポート期限を迎えるファームウェア及びソフトウェアに対する対応**

(ア) サポート期限を迎えるファームウェア及びソフトウェアのバージョンアップを実施した際、「基本設計書」や「詳細設計書」、「運用計画」、「運用実施要領」及び「運用作業手順書」等の図書へ更新すること。

(5) **その他**

(ア) その他、上記に付随する作業でセンターとの協議により定められた作業を実施すること。

3.16.5. 運用実績の報告

「3.16 運用に関する事項」において実施した作業について、報告資料を作成し、月次の頻度で報告を行うこと。ただし、インシデント発生時等の有事の際は都度報告を行うこと。なお、報告内容の詳細は、受注後にセンターと協議の上で定めること。

各作業の報告内容の例及び報告頻度を以下に示す。

表 3-28 本システムの運用に係る報告内容

No.	作業項目	報告内容（例）
1	死活監視	・ システムの稼働率 ・ 異常検知数 ・ 異常検知を報告するまでの時間 ・ システム停止回数 ・ システム停止時間
2	リソース監視	・ ストレージ空き容量 ・ メモリ使用率 ・ CPU 稼働率 ・ 通信速度の推移
3	セキュリティ監視	・ ファイアウォールのブロック件数 ・ 統合認証サービス、クラウド認証サービスへのログイン失敗件数 ・ 不正プログラムの検知回数 ・ セキュリティ事故件数
4	問題・インシデント対応	・ 対応実績及び直近の対応予定
5	ファームウェアの脆弱管理	・ 脆弱性対策の状況
6	ソフトウェアの脆弱管理	・ 脆弱性対策の状況
7	構成管理	・ 本システムの構成の変更内容

表 3-29 業務運用支援作業に係る報告内容

No.	作業項目	報告内容（例）
1	定常業務	・ 定常業務における実績等
2	その他定常業務	・ セキュリティパッチの適用実績 ・ ・ 情報システムの設定変更実績 ・ ヘルプデスクの問合せ件数、対応実績等
3	情報セキュリティインシデント対応支援	・ 情報セキュリティインシデントへの対応実績等
4	その他支援作業	・ 情報セキュリティ対策の検討・導入支援に係る報告等

3.17. 保守に関する事項

本システムの保守要件を以下に示す。受注者は、本項に示す保守要件を実施可能となるよう本システムを構築するとともに、必要な保守作業を行うこと。

3.17.1. 作業条件

保守業務の作業条件を以下に示す。

3.17.1.1. 対応時間、実施頻度

各作業の対応時間及び実施頻度を以下に示す。

表 3-30 各作業の対応時間及び実施頻度

No.		作業分類	作業項目	対応時間	実施頻度	備考
1	定常時対応	クラウドサービス保守	脆弱性及び不具合の対応	平日 9:00～17:30	随時	
2		ハードウェア保守	ファームウェア等の脆弱性対応	平日 9:00～17:30（※）	随時	
3			問合せ対応	平日 9:00～17:30	随時	
4		ソフトウェア保守業務	ソフトウェアの脆弱性対応	平日 9:00～17:30（※）	随時	
5			問合せ対応	平日 9:00～17:30	随時	
6		その他	サポート期限を迎えるファームウェア及びソフトウェアに対する対応	平日 9:00～17:30（※）	随時	
7		保守実績の報告	保守実績の報告	平日 9:00～17:30	月次	
8	障害発生時対応	ハードウェア保守	障害対応	平日 9:00～17:30（※）	随時	

※ 対応時間外の作業が必要な場合はセンターと協議し、作業時間等について合意を得た上で作業を行うこと。なお、システムを停止する必要があるメンテナンスはシステムに影響を与えない事を前提に休日（土日・祝日）に実施すること。但し、重大な障害が発生している場合は即時対応すること。

3.17.1.2. 作業場所

センターの東京本部又は受注者が用意する運用保守拠点より本システムへ接続し、保守作業を実施すること。

センターから障害対応を依頼された際に、センターの各拠点への駆けつけ対応により必要な作業を実施すること。

3.17.2. クラウドサービス保守要件

本システムのクラウドサービス保守に係る作業要件を以下に示す。

(ア) 利用しているクラウドサービスにおいて脆弱性及び不具合が確認された場合は、その対応についてセンターと協議し、パッチ適用要否を判断すること。

(イ) クラウドサービスにおいてバージョンアップ等の情報が公開された場合には、バージョンアップに伴う影響調査を実施した上で、センターと協議し、適用等の可否を決定すること。

3.17.3. ハードウェア保守要件

本システムのハードウェア保守に係る作業要件を以下に示す。

(ア) 要件定義フェーズで稼働率目標値及び継続性目標値を設定し、それらを満たすべく、ハードウェアの修理、交換の必要な復旧作業を行う。

(イ) 本システムのネットワーク機器等のハードウェア保守は原則オンサイト保守とする。なお、機器の特性に応じてその他の保守形式を提案してもよい。

(ウ) 各拠点に設置された端末のハードウェア保守はオンサイト対応とし、キッティング作業の一部（マスタのインストール）が完了している状態の端末と交換する。東海保障措置センター及び六ヶ所保障措置センターの端末はセンターにて確認のうえ東京本部に送付されるため、東京本部で対応すること。

(エ) 本システムのハードウェアのファームウェアに脆弱性が発見された際には、センターへの報告を行うこと。

(オ) 本システムのハードウェアのファームウェアのバージョンアップ情報又はパッチ情報について、センターへの連絡を行うとともに、本システムへの影響度を考慮した適用可否の方針案をセンターへ報告すること。

(カ) 本システムのハードウェアのファームウェアのバージョンアップ又はパッチ適用を実施するに当たり、必要なアップデートファイル、技術情報、作業手順書の提供並びに問合せ対応を行う。また必要に応じて、現地での作業を行うこと。

(キ) センターから、本システムのハードウェアに関する技術的な問合せがあった場合、情報提供や助言の対応を行う。必要に応じてハードウェアの製造元に確認を行う。

3.17.3.1. 障害発生時対応

センターからの障害対応依頼に応じて、以下の障害発生時対応作業を実施すること。

(ア)「3.4. 信頼性に関する事項」に示す稼働率目標値及び「3.8. 継続性に関する事項」に示す継続性目標値を満たすべく、ハードウェアの修理、交換等の必要な復旧作業を行うこと。
(イ) 本システムのネットワーク機器等のハードウェア保守は原則オンサイト保守とすること。なお、機器の特性に応じてその他の保守形式を提案してもよい。
(ウ) 各ハードウェアの保守においてハードディスク等の電磁的記録媒体の交換を行う場合でも、故障したハードディスクの返却は不要とすること。

3.17.3.2. ファームウェア等の脆弱性対応

ハードウェアに搭載されたファームウェアの脆弱性対応等について、以下の作業を実施すること。

(ア) 本システムのハードウェアのファームウェアに脆弱性が発見された際には、センターへの報告を行うこと。
(イ) 本システムへの影響度を考慮した適用可否の方針案をセンターへ報告すること。
(ウ) 本システムのハードウェアのファームウェアのバージョンアップ又はパッチ適用を実施するに当たり、必要なアップデートファイル、技術情報、並びに問合せ対応を行うこと。また、現地での作業を行うこと。
(エ) 作業手順書等の作成にあたり、製造元から提供される手順書を本システムに即した手順に改版の上、作成すること。
(オ) 上記の対応の結果、本システムが正常に動作していることを確認すること。
(カ) 対応日時、対応内容等について報告書を作成し、センターへ報告すること。

3.17.3.3. 問合せ対応

センターからハードウェアについて技術的な問合せがあった場合には、以下の作業を実施すること。

(ア) センターから、本システムのハードウェアに関する技術的な問合せがあった場合、情報提供や助言等の対応を行うこと。
(イ) 必要に応じてハードウェアの製造元に確認を行うこと。

3.17.4. ソフトウェア保守要件

本システムのソフトウェア保守に係る作業要件を以下に示す。

3.17.4.1. ソフトウェアの脆弱性対応

本システムのソフトウェア製品の脆弱性対応等について、以下の作業を実施すること。

(ア) 本システムのソフトウェア製品に脆弱性が発見された際には、センターへの報告を行うこと。
(イ) 本システムへの影響度を考慮した適用可否の方針案の検討を支援し、センターへ報告すること。
(ウ) 本システムのソフトウェア製品のバージョンアップ又はパッチ適用を実施するに当たり、必要なアップデートファイル、技術情報、並びに問合せ対応等の支援を行うこと。また必要に応じて、現地での作業を支援すること。
(エ) 作業手順書等を作成し、運用保守チームメンバの運用担当者に提供すること。作業手順書等の提供にあたり、製造元から提供される手順書を本システムに即した手順に改版すること。

3.17.4.2. 問合せ対応

センターからソフトウェアについて技術的な問合せがあった場合には、以下の作業を実施すること。

(ア) センターから、本システムのソフトウェアに関する技術的な問合せがあった場合、情報提供や助言等の対応を行うこと。
(イ) 必要に応じてソフトウェアの製造元に確認を行うこと。

3.17.5. その他の保守要件

3.17.5.1. サポート期限を迎えるファームウェア及びソフトウェアに対する対応

受注者は稼働している機器のファームウェア及びソフトウェアがサポート期限を迎える際に以下の作業を実施すること。

(ア) 受注者は中長期保守作業計画書を作成し、保守期間中に更新が想定されるソフトウェアを予め整理し、センターに報告すること。
(イ) 必要に応じてファームウェア及びソフトウェアの製造元に確認を行うこと。
(ウ) 事前にテストを行い本システムへの影響がないことを確認すること。
(エ) 対象のファームウェア及びソフトウェアのバージョンアップ等の対応を行うこと。
(オ) 対象のファームウェア及びソフトウェアのバージョンアップ等の対応内容を取りまとめ、センターに報告すること。

3.17.5.2. 脆弱性診断の対応

受注者は本システムのクラウドサービス、ハードウェア及びソフトウェアについて、以下の作業を実施すること。

（ア）受注者は年次に 1 回、本システムのクラウドサービス、ハードウェア及びソフトウェアを対象に、脆弱性の特定を目的とした脆弱性診断を実施すること。なお、脆弱性診断の対象は IaaS を想定し、SaaS は対象外とする。

（イ）脆弱性診断を実施後、報告書を取りまとめ、センターに報告すること。また、脆弱性対応が必要となった際には対応内容を含めセンターへ提案し、対応すること。

3.17.6. 保守実績の報告

保守業務において行う作業について、報告資料を作成し、メール等により月次報告を行うこと。ただし、センターからの求めがあった場合は、打合せによる報告を行うこと。

各作業の報告内容を以下に示す。

表 3-31 報告内容

No.	作業分類	作業項目	報告内容
1	クラウドサービス保守	脆弱性及び不具合の対応	・ 本システムのハードウェアの稼動状況（故障・障害件数等） ・ 各作業項目の作業実績 ・ 直近の作業予定 ・ その他、必要な技術情報、助言 ・ サポート期限を迎えるソフトウェアのアップデート作業
2	ハードウェア保守	障害発生時対応	
3		ファームウェア等の脆弱性対応	
4		問合せ対応	
5	ソフトウェア保守	ソフトウェアの脆弱性対応	
6		問合せ対応	
7		ソフトウェアのアップデート作業	
8	その他	サポート期限を迎えるファームウェア及びソフトウェアに対する対応	

応札資料作成要領

本書は、「第 2 期基盤情報システムの構築及び移行業務」の調達に係る応札資料の作成要領を取りまとめたものである。

1. 提出物

（1） 提出物

応札者がセンターへ提出する資料は以下のとおりとする。

No.	資料名称	資料内容	紙媒体 部数	電子媒体 部数
1	資格審査結果通知書(全省庁統一資格)等の写し	入札説明書「４．競争入札に参加する者に必要な資格」に定める、国・地方公共団体等における競争参加資格(東北、関東・甲信越)の「役務の提供等」の資格審査結果通知書(全省庁統一資格) 等の写し	1部	―
2	提案書	調達仕様書及び要件定義書に記載された要求仕様をどのように実現するかを提案書にて説明したもの。本資料は提案書本文及び添付資料にて構成する。	8部	1部 (CD-R又は DVD-R)
3	参考見積書	「第2期基盤情報システムの構築及び移行業務」を実施するために必要な経費の全ての額(消費税及び地方消費税額を含む。)の内訳を記載したもの。		

2. 提案書作成要領及び説明（プレゼンテーション）要領

（1） 提案書様式

① 「別紙 1 評価項目及び得点配分」に示す事項に沿って提案内容を記載すること。

② 提案書は原則として A4 版・両面・横書きとするが、特別に大きな図面等が必要な場合には、A3 版にて提案書の中に折り込むこと。

③ 提案書本文は 90 頁を上限とする。ただし、表紙、目次、添付資料に関してはこの頁数に含まない。

④ 「別紙 1 評価項目及び得点配分」に示す各評価項目と、提案書の頁番号及び添付

資料の対応関係を示した一覧表を添付すること。

⑤ 提案書に補足の説明（製品カタログ、資格証明書等）がある場合は、必要に応じて資料を添付すること。添付する場合には、提案書の該当箇所を明記すること。

⑥ 提案書を評価する者が特段の専門的な知識や商品に関する一切の知識を有しなくても評価が可能な提案書を作成すること。なお、必要に応じて用語解説などを添付すること。

⑦ センターから連絡が取れるよう、提案書には連絡先（電話番号、FAX 番号、及びメールアドレス）を明記すること。

⑧ 日本語で記載すること。

⑨ 提案書本文のフォントサイズは 11 ポイント以上とすること。

⑩ 電子媒体（CD-R 又は DVD-R）に格納するファイル形式は、原則として、Microsoft Word 2019、Microsoft PowerPoint 2019、Microsoft Excel 2019 のいずれかで正しく表示が可能な形式又は PDF 形式とする。（これに拠りがたい場合は、センターまで申し出ること。）

（２） 応札者による提案書の説明（プレゼンテーション）

① 提出された提案書に基づき、センターの指定する日時にプレゼンテーションを実施すること。

② プレゼンテーションの日時等については、提案書受領期限後にセンターと応札者とで別途調整する。また、プレゼンテーションの時間は、1 社あたり概ね 60 分程度（プレゼンテーション 20 分、質疑応答 40 分）を想定している。なお、プレゼンテーションに係る準備時間は、持ち時間に含まないものとする。

③ プレゼンテーションは、提案書の説明及び提案書の内容に関するヒアリングを行うもので、技術点の評価対象外とする。なお、提案書にない新たな提案は認めない。

④ プレゼンテーションにあたっては、与えられた時間を踏まえ、必要に応じて提案書とは別に要約版資料を用意するなど、効率的に実施すること。

⑤ 説明者は、本業務を請け負った場合における、中心的役割を担う者とすること。

⑥ 説明にあたっては、内の会議室にてプレゼンテーションを行うこととし、応札者により端末その他必要な機器を準備すること。ただし、プロジェクタ（映像入出力端子：HDMI）及び映写用のスクリーンはセンターにて準備する。

⑦ プレゼンテーション参加人数は、5 名程度とし、出席者を事前にセンターに連絡すること。

⑧ プレゼンテーションを行わない場合は、不合格とする。なお、不測の事態によりプレゼンテーションを行うことが困難となった場合は、入札説明書に示す連絡先へ連絡すること。

⑨ プレゼンテーションにより知り得た情報を第三者に漏らしてはならない。

3. 参考見積書に係る様式

（1） 見積書（サマリ）

以下の表に基づき、作業実施内容ごとの費用を記載すること。なお、「作業実施内容」の追加・変更は行わないこと。

No.	調達案件名	作業実施内容（※）	費用（税抜き）
1	第2期基盤情報システムの構築及び移行業務	設計・構築実施計画書等の作成	
		設計	
		構築・導入設置	
		テスト	
		受入テスト支援	
		運用計画及び運用実施要領の作成	
		保守計画及び保守実施要領の作成	
		移行計画	
		教育	
		移行	
		工事	
		引継ぎ	
		定例会等の実施	
2	第2期基盤情報システムの賃貸借・運用保守業務	機器等の賃貸借	
		運用業務	
		保守対応	
計（税抜き）			
消費税			
計（税込み）			

※作業実施内容の詳細については、調達仕様書の「4. 作業の実施内容」を参照

（2） 見積書（明細）

見積書（サマリ）の「作業実施内容」ごとに、費用の明細を作成すること。明細の様式は任意とするが、以下の事項を満たすこと。

① 要員ランク別の単価及び工数（人月）を記載すること。
② 機器・ソフトウェア等の物品については、単価及び数量を記載すること。
③ 「出精値引き」、「調整額」等の名目による経費の根拠のない減額や端数処理は行わ

ないこと。

（３）　見積書（年度別費用）

以下の表に基づき、調達案件ごとの年度別費用を記載すること。

No.	調達案件名	年度別費用（税抜き）					
		令和7年度	令和8年度	令和9年度	令和10年度	令和11年度	令和12年度
1	第2期基盤情報システムの構築及び移行業務						
2	第2期基盤情報システムの賃貸借・運用保守業務						
計（税抜き）							
消費税							
計（税込み）							

4. 評価基準

（1）落札方式及び得点配分

① 次の要件を全て満たしている者のうち、「（2） 総合評価点の算出」によって得られた数値の最も高い者を落札者とする。

(ア)入札価格が予定価格の範囲内であること。

(イ)「別紙１ 評価項目及び得点配分」に示す「基礎点」の評価基準を全て満たしていること。

② 技術点と価格点の得点配分は、以下のとおりする。

価格点	技術点				総合評価点（合計）
	基礎点		加点		
	技術力に対する基礎点	後年度費用に対する基礎点	技術力に対する加点（※1）	後年度費用に対する加点（※2）	
255 点	100 点	2 点	920 点	763 点	2,040 点

※1 「技術力に対する加点」とは、「別紙１ 評価項目及び得点配分」の加点項目のうち、「6-1.後年度予定コストの提案」以外の加点の総称をいう。

※2 「後年度費用に対する加点」とは、「別紙１ 評価項目及び得点配分」の加点項目のうち、「6-1.後年度予定コストの提案」の加点のことをいう。

（2）総合評価点の算出

① 総合評価点は、価格点と技術点を足し合わせた値とする。

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

価格点 ＝ （1 － （入札価格 ÷ 予定価格） ）× 255 点

③ 技術点は、「（3） 技術点の算出」によって得られた値とする。

（3） 技術点の算出

① 技術点は、基礎点と加点を足し合わせた値とする。

② 基礎点は、「別紙１ 評価項目及び得点配分」に示す「基礎点」の評価基準を満た

す者に、該当する項目の基礎点を付与する。１項目でも基礎点の基準を満たすことができない場合は失格とする。なお、「6-1.後年度予定コストの提案」においては、後年度予定コストが税込で XXX,XXX,XXX 円を上限として提案すること。これを超過した額での提案は失格とする。

③　加点は、「別紙２　技術評価加点付与基準」に従い、各評価項目に対する「評価区分」を評価し、対応する点数を加点として付与する。

5.　その他留意事項

（１）　質問の受付

本要領に関する質問がある場合は、入札説明書に従い質問書を提出すること。

（２）　提案書等の提出

①　提案書等の提出先は、入札説明書に従うこと。

②　持参する場合の受付時間は、平日の１０時００分から１７時００分まで（１２時から１３時までは除く。）とする。

③　郵送する場合は、封書の表に「第２期基盤情報システムの構築及び移行業務に係る提案書等在中」と明記すること。提出期限までに提出先に現に届かなかった提案書等は、無効とする。

④　提出された提案書等は、その事由の如何にかかわらず、変更又は取消しを行うことはできない。また、返還も行わない。

⑤　１者当たり１件の提案を限度とし、１件を超えて申し込みを行った場合は全てを無効とする。

⑥　作業要員に求める資格等の証跡として、体制図の写しを提出すること。なお、写しは必要に応じて墨塗を行うこと。

⑦　受注実績の証跡として、契約書の写しを提出すること。なお、写しは必要に応じて墨塗を行うこと。

⑧　参加資格を満たさない者が提出した提案書等は、無効とする。

⑨　虚偽の記載をした提案書等は、無効とする。

⑩　落札した場合は、提案書において「後年度予定コスト」として提案した費用を後年度の各調達案件を契約する上での上限額とし、極端な物価変動等を除き、これを超えた額での契約は認めないものとする。

⑪　電子媒体の提出に当たっては、事前にウイルスの感染等について問題ないことを確認した上で提出を行うこと。

⑫　提出された提案書等は、センターにおいて、提案書等の審査以外の目的に提出者に無断で使用しない。

6．別紙

別紙１　評価項目及び得点配分

別紙２　技術評価加点付与基準

別紙1 評価項目及び得点配分

評価項目			評価基準		相対評価/絶対評価	得点配分（満点）		
			基礎点	加点		基礎点	加点	合計
1.	業務の目的、目標及び内容					**20**	**90**	**110**
	1-1. 業務の目的					5	0	5
		1-1-1.	「第2期基盤情報システムの構築及び移行業務」（以下「本業務」という。）の目的の理解が示されており、調達仕様書に明示したセンターの目的と整合していること		－	5		5
	1-2. 目標設定の妥当性					5	0	5
		1-2-1.	本業務の目標が設定されており、目標設定の妥当性と目標達成に向けた計画性があること		－	5		5
	1-3. 業務の内容					10	90	100
		1-3-1.	本業務の実施内容が、具体的かつ詳細で明確になっていること	成果物の品質向上に有益な工夫が提案がなされている場合は加点する	相対評価	5	30	35
		1-3-2.	本業務の実施に当たり、センターの基盤情報システムの経緯・背景を踏まえ、本業務の実施内容において想定されるリスクが記載されていること	想定されるリスクに事前対応するための有益な提案がなされている場合は加点する	相対評価	5	30	35
		1-3-3.		関係するセンター役職員または情報セキュリティ室の作業負荷低減が見込める提案がなされている場合は加点する	相対評価		30	30
2.	情報システムの機能及び非機能					**25**	**660**	**685**
	2-1. 情報システムの機能					5	390	395
		2-1-1.	第2期基盤情報システム（以下「本システム」という。）における要件定義書「2.1.2.サービスの機能要件」に記載の各要件を実現するための技術や仕組み、製品名等の概要及び選定理由が示されていること ※複数の製品・サービスを組み合わせて機能を実現する場合はその旨を明記すること		－	5		5
		2-1-2.		要件定義書「2.1.2.1.ネットワークサービス（4）インターネットサービス」について、必要となる回線帯域の案及び設計段階における検証・見直しの方針が提示されており、必要十分な回線帯域の確保に向けた実現性の高い提案がなされている場合は加点する	相対評価		90	90
		2-1-3.		要件定義書「2.1.2.2.基盤サービス（2）Windowsアップデート管理サービス」について、Windows Server Update Service（WSUS）がサポート終了を予定していることを受け、代替となるサービスが提案されており、本システムにおける具体的な運用方法、当該サービスを利用した運用実績等が提案されている場合は加点する	相対評価		30	30
		2-1-4.		要件定義書「2.1.2.2.基盤サービス（3）ファイル共有サービス」について、利用者の視点に基づき、従来型のファイルサーバとの差異を緩和するための導入・運用時の工夫等が示されており、センター職員の円滑な利用に有益な提案がなされている場合は加点する	相対評価		30	30
		2-1-5.		要件定義書「2.1.2.2.基盤サービス（6）システム運用管理・監視サービス」について、マルチベンダとなる想定の各サービスの管理・監視が可能であること、具体的な運用方法、当該サービスを利用した運用実績等が提案されている場合は加点する	相対評価		30	30
		2-1-6.		要件定義書「2.1.2.2.基盤サービス（9）ウイルス対策管理サービス」について、本システムで発生しうる不正プログラムに係る脅威が具体的に示され、当該脅威への対応が可能であること、不正プログラムを効果的に検知するためのチューニングなどの手法が具体的に示されている場合は加点する	相対評価		90	90
		2-1-7.		要件定義書「2.1.2.2.基盤サービス（11）クラウドプロキシサービス」について、インターネット回線を用いた通信が基本となる本システムで、発生しうる脅威が具体的に示され、当該脅威への対応策、本システムのセキュリティを確保するための技術的手段や実現方式が具体的に示されている場合は加点する	相対評価		90	90
		2-1-8.		要件定義書「3.8.2.継続性に係る対策（3）バックアップデータの保管」について、具体的な保管方法が示されており、データ消失時の復旧にあたり有効と判断できる提案がなされている場合は加点する	相対評価		30	30
	2-2. 情報システムの非機能					20	270	290
		2-2-1.	本システム全体のシステム構成図が提案されていること		－	5		5
		2-2-2.		提案するシステム構成において、要件定義書「表 3-6 応答時間に係る目標値」に記載の要件を満たすためのポイントや工夫が根拠とともに具体的に提案されている場合は加点する	相対評価		30	30
		2-2-3.	要件定義書「表 3-7 可用性に係る目標値」の稼働率を維持するための具体的な手段が示されており、要件と整合していること		－	5		5

評価項目			評価基準		相対評価/絶対評価	得点配分（満点）		
			基礎点	加点		基礎点	加点	合計
		2-2-4.	要件定義書「3.9.1情報セキュリティ対策要件 (2)情報システムのセキュリティ要件」に記載の各要件を実現するための技術や製品名、対策方法が提案されていること		－	5		5
		2-2-5.		提案するシステム構成から想定されるセキュリティリスクについて、「近年のセキュリティリスクの傾向」及び「センターの業務特性」を踏まえたリスク分析が行われ、具体的な対応策の提案がなされており、情報セキュリティ確保の観点から有効性が高いと判断できる場合は加点する	相対評価		90	90
		2-2-6.		本システムはクラウドサービスの活用を想定した業務基盤システムであり、セキュリティインシデント等による影響を最小限とする必要があることを理解した上で、各テスト工程における不具合の検知、品質確保のための工夫が示されており、品質確保の観点で有効性が高いと判断できる場合は加点する	相対評価		30	30
		2-2-7.		センター職員による受入テストの実施にあたり、品質を損なうことなく実施に係る作業負荷を軽減するための工夫が示されており、受入テスト作業の効率化の観点から有効性の高い提案がなされている場合には加点する	相対評価		30	30
		2-2-8.		本システムの移行において、移行対象データ、移行先（SaaS、IaaS）の特性に応じた具体的な移行方法が提案されており、移行の成功に向けた実現性の高い提案がなされている場合には加点する	相対評価		30	30
		2-2-9.		本システムはオンプレミス環境からクラウド環境への移行であることを踏まえ、想定されるリスク分析が行われ、具体的な対応策が示されており、移行の成功に向けた実現性の高い提案がなされている場合には加点する	相対評価		30	30
		2-2-10.	要件定義書「3.16.2.運用管理・監視等要件」に記載の各要件を実現するための具体的な手段が示されており、要件と整合していること			5		5
		2-2-11.		本システムの運用保守期間中に実施する脆弱性対応、インシデント対応等が確実に実施されるための工夫が示されており、本システムのセキュリティ維持に有効性が高いと判断できる場合には加点する	相対評価		30	30
3.	業務の実施・管理体制					**35**	**50**	**85**
	3-1. 業務の実施体制					5	0	5
		3-1-1.	本業務の実施体制が、構築業務、移行業務、賃貸借・運用保守業務についてそれぞれ示されており、調達仕様書「5.1. 作業実施体制」で求める要件と整合していること		－	5		5
	3-2. 業務実施のための経営基盤					5	0	5
		3-2-1.	提案者の概要（会社概要等）が示されており、業務を円滑に実施するために必要な経営基盤、設備等を有していること		－	5		5
	3-3. 業務担当者の実績及び能力					25	50	75
		3-3-1.	本業務の実施における「実施責任者」の資格・経験等が、調達仕様書「5.1. 作業実施体制」のうち「5.2.1.」で求める要件と整合していること ※経験は、調達機関名称、調達案件名称、案件概要、案件規模を記載する	本業務の実施における「実施責任者」について、調達仕様書で求める要件以上の経験を有しており、本業務を成功させるために有用であると判断できる場合は加点する（最大5件まで） ※経験は、調達機関名称、調達案件名称、案件概要、案件規模を記載する	絶対評価	5	10	15
		3-3-2.	本業務の実施における「構築チームリーダ」の資格・経験等が、調達仕様書「5.1. 作業実施体制」のうち「5.2.1.」で求める要件と整合していること ※経験は、調達機関名称、調達案件名称、案件概要、案件規模を記載する	本業務の実施における「構築チームリーダ」について、調達仕様書で求める要件以上の経験を有しており、本業務を成功させるために有用であると判断できる場合は加点する（最大5件まで） ※経験は、調達機関名称、調達案件名称、案件概要、案件規模を記載する	絶対評価	5	10	15
		3-3-3.	本業務の実施における「移行・引継ぎチームリーダ」の資格・経験等が、調達仕様書「5.1. 作業実施体制」のうち「5.2.1.」で求める要件と整合していること ※経験は、調達機関名称、調達案件名称、案件概要、案件規模を記載する	本業務の実施における「移行・引継ぎチームリーダ」について、調達仕様書で求める要件以上の経験を有しており、本業務を成功させるために有用であると判断できる場合は加点する（最大5件まで） ※経験は、調達機関名称、調達案件名称、案件概要、案件規模を記載する	絶対評価	5	10	15
		3-3-4.	本業務の主目的であるクラウド化を実現するために必要となるクラウドサービスの設計・構築に係る資格・経験等が示されていること ※経験は、調達機関名称、調達案件名称、案件概要、案件規模を記載する	本業務の実施における「構築チームリーダまたは構築チームメンバ」について、調達仕様書で求める要件以上の経験を有しており、本業務を成功させるために有用であると判断できる場合は加点する（最大5件まで） ※経験は、調達機関名称、調達案件名称、案件概要、案件規模を記載する	絶対評価	5	10	15
		3-3-5.	本業務の実施における「運用・保守チームリーダ」の資格・経験等が、調達仕様書「5.1. 作業実施体制」のうち「5.2.2.」で求める要件と整合していること ※経験は、調達機関名称、調達案件名称、案件概要、案件規模を記載する	本業務の実施における「運用・保守チームリーダ」について、調達仕様書で求める要件以上の経験を有しており、本業務を成功させるために有用であると判断できる場合は加点する（最大5件まで） ※経験は、調達機関名称、調達案件名称、案件概要、案件規模を記載する	絶対評価	5	10	15

評価項目			評価基準		相対評価/絶対評価	得点配分（満点）		
			基礎点	加点		基礎点	加点	合計
4.	組織の業務実績					**5**	**30**	**35**
	4-1. 過去の業務実績					5	30	35
		4-1-1.	応札者の業務実績が、調達仕様書「8.1.2.受注実績」で求める要件と整合していること ※実績は、調達機関名称、調達案件名称、案件概要、案件規模を記載する	調達仕様書「8.1.2.受注実績」で求める要件に整合する実績が2件以上ある場合は加点する（最大6件まで） ※実績は、調達機関名称、調達案件名称、案件概要、案件規模を記載する	絶対評価	5	30	35
5.	業務の実施計画					**15**	**90**	**105**
	5-1. 業務の実施計画					15	90	105
		5-1-1.	調達仕様書「4.1.第2期基盤情報システムの構築及び移行業務」及び「4.2.第2期基盤情報システムの賃貸借及び運用保守業務」の作業スケジュールが、WBS（Work Breakdown Structure）のレベル3以上に詳細化されており、「1-3. 業務の内容」において提案する作業内容と整合していること	スケジュールやマイルストーンが詳細に計画されており、マイルストーンを遵守するための有益な工夫が示されている場合は加点する	相対評価	5	30	35
		5-1-2.	本業務を計画どおりに実施するための進捗管理方法が示されていること	進捗状況の定量的な管理手法、報告基準等が提案されており、本業務の遅延防止や遅延発生時の早期対応等に寄与できると判断できる場合は加点する	相対評価	5	30	35
		5-1-3.	本業務を計画どおりに実施するための課題及びリスクの進捗管理方法が示されていること	本業務のステークホルダを含めた課題・リスクを漏れなく洗い出すための工夫（コミュニケーション方法等）が提案されており、確実な課題解決の推進に寄与できると判断できる場合は加点する	相対評価	5	30	35
（1～5の合計）						**100**	**920**	**1,020**
6.	後年度に必要となる費用					**2**	**763**	**765**
	6-1. 後年度予定コストの提案					2	763	765
		6-1-1.	令和8年度～令和12年度までに必要となる後年度予定コストについて、その合計額（税込み）と内訳が見積書により示されていること ※「後年度予定コスト」とは、調達仕様書に示す「4.2.第2期基盤情報システムの賃貸借及び運用保守に関する業務」の実施に必要となる費用のことをいう。		－	1		1
		6-1-2.	後年度予定コストの合計額（税込み）が、センターが設定する上限コスト「¥1,150,000,000」以下であること	後年度予定コストの合計額（税込み）が、センターの設定する「加点基準コスト」を下回っている場合は加点する ※「加点基準コスト」は、左記の「上限コスト」とは異なる値であり、非開示とする	絶対評価	1	763	764
合　計						**102**	**1,683**	**1,785**

別紙2 技術評価加点付与基準

評価項目			加点評価項目	評価区分			
				大変優れている	優れている	やや優れている	加点に値しない
1.	業務の目的、目標及び内容			**90**	**60**	**30**	**0**
	1-3.	業務の内容		90	60	30	0
		1-3-1.	成果物の品質向上に有益な工夫が提案がなされている場合は加点する	30	20	10	0
		1-3-2.	想定されるリスクに事前対応するための有益な提案がなされている場合は加点する	30	20	10	0
		1-3-3.	関係するセンター役職員または情報セキュリティ室の作業負荷低減が見込める提案がなされている場合は加点する	30	20	10	0
2.	情報システムの機能及び非機能			**660**	**440**	**220**	**0**
	2-1.	情報システムの機能		390	260	130	0
		2-1-2.	要件定義書「2.1.2.1.ネットワークサービス（4）インターネットサービス」について、必要となる回線帯域の案及び設計段階における検証・見直しの方針が提示されており、必要十分な回線帯域の確保に向けた実現性の高い提案がなされている場合は加点する	90	60	30	0
		2-1-3.	要件定義書「2.1.2.2.基盤サービス（2）Windowsアップデート管理サービス」について、Windows Server Update Service（WSUS）がサポート終了を予定していることを受け、代替となるサービスが提案されており、本システムにおける具体的な運用方法、当該サービスを利用した運用実績等が提案されている場合は加点する	30	20	10	0
		2-1-4.	要件定義書「2.1.2.2.基盤サービス（3）ファイル共有サービス」について、利用者の視点に基づき、従来型のファイルサーバとの差異を緩和するための導入・運用時の工夫等が示されており、センター職員の円滑な利用に有益な提案がなされている場合は加点する	30	20	10	0
		2-1-5.	要件定義書「2.1.2.2.基盤サービス（6）システム運用管理・監視サービス」について、マルチベンダとなる想定の各サービスの管理・監視が可能であること、具体的な運用方法、当該サービスを利用した運用実績等が提案されている場合は加点する	30	20	10	0
		2-1-6.	要件定義書「2.1.2.2.基盤サービス（9）ウイルス対策管理サービス」について、本システムで発生しうる不正プログラムに係る脅威が具体的に示され、当該脅威への対応が可能であること、不正プログラムを効果的に検知するためのチューニングなどの手法が具体的に示されている場合は加点する	90	60	30	0
		2-1-7.	要件定義書「2.1.2.2.基盤サービス（11）クラウドプロキシサービス」について、インターネット回線を用いた通信が基本となる本システムで、発生しうる脅威が具体的に示され、当該脅威への対応策、本システムのセキュリティを確保するための技術的手段や実現方式が具体的に示されている場合は加点する	90	60	30	0
		2-1-8.	要件定義書「3.8.2.継続性に係る対策（3）バックアップデータの保管」について、具体的な保管方法が示されており、データ消失時の復旧にあたり有効と判断できる提案がなされている場合は加点する	30	20	10	0
	2-2.	情報システムの非機能		270	180	90	0
		2-2-2.	提案するシステム構成において、要件定義書「表 3-6 応答時間に係る目標値」に記載の要件を満たすためのポイントや工夫が根拠とともに具体的に提案されている場合は加点する	30	20	10	0
		2-2-5.	提案するシステム構成から想定されるセキュリティリスクについて、「近年のセキュリティリスクの傾向」及び「センターの業務特性」を踏まえたリスク分析が行われ、具体的な対応策の提案がなされており、情報セキュリティ確保の観点から有効性が高いと判断できる場合は加点する	90	60	30	0
		2-2-6.	本システムはクラウドサービスの活用を想定した業務基盤システムであり、セキュリティインシデント等による影響を最小限とする必要があることを理解した上で、各テスト工程における不具合の検知、品質確保のための工夫が示されており、品質確保の観点で有効性が高いと判断できる場合は加点する	30	20	10	0
		2-2-7.	センター職員による受入テストの実施にあたり、品質を損なうことなく実施に係る作業負荷を軽減するための工夫が示されており、受入テスト作業の効率化の観点から有効性の高い提案がなされている場合には加点する	30	20	10	0
		2-2-8.	本システムの移行において、移行対象データ、移行先（SaaS、IaaS）の特性に応じた具体的な移行方法が提案されており、移行の成功に向けた実現性の高い提案がなされている場合には加点する	30	20	10	0
		2-2-9.	本システムはオンプレミス環境からクラウド環境への移行であることを踏まえ、想定されるリスク分析が行われ、具体的な対応策が示されており、移行の成功に向けた実現性の高い提案がなされている場合には加点する	30	20	10	0
		2-2-11.	本システムの運用保守期間中に実施する脆弱性対応、インシデント対応等が確実に実施されるための工夫が示されており、本システムのセキュリティ維持に有効性が高いと判断できる場合には加点する	30	20	10	0

3.	業務の実施・管理体制			**50**	**35**	**20**	**0**
	3-3.	業務担当者の実績及び能力		50	35	20	0
		3-3-1.	本業務の実施における「実施責任者」について、調達仕様書で求める要件以上の経験を有しており、本業務を成功させるために有用であると判断できる場合は加点する（最大5件まで）	10	7	4	0
		3-3-2.	本業務の実施における「構築チームリーダ」について、調達仕様書で求める要件以上の経験を有しており、本業務を成功させるために有用であると判断できる場合は加点する（最大5件まで）	10	7	4	0
		3-3-3.	本業務の実施における「移行・引継ぎチームリーダ」について、調達仕様書で求める要件以上の経験を有しており、本業務を成功させるために有用であると判断できる場合は加点する（最大5件まで）	10	7	4	0
		3-3-4.	本業務の実施における「構築チームリーダまたは構築チームメンバ」について、調達仕様書で求める要件以上の経験を有しており、本業務を成功させるために有用であると判断できる場合は加点する（最大5件まで）	10	7	4	0
		3-3-5.	本業務の実施における「運用・保守チームリーダ」について、調達仕様書で求める要件以上の経験を有しており、本業務を成功させるために有用であると判断できる場合は加点する（最大5件まで）	10	7	4	0
4.	組織の業務実績			**30**	**20**	**10**	**0**
	4-1.	過去の業務実績		30	20	10	0
		4-1-1.	調達仕様書「8.1.2.受注実績」で求める要件に整合する実績が2件以上ある場合は加点する（最大6件まで）	30	20	10	0
5.	業務の実施計画			**90**	**60**	**30**	**0**
	5-1.	業務の実施計画		90	60	30	0
		5-1-1.	スケジュールやマイルストーンが詳細に計画されており、マイルストーンを遵守するための有益な工夫が示されている場合は加点する	30	20	10	0
		5-1-2.	進捗状況の定量的な管理手法、報告基準等が提案されており、本業務の遅延防止や遅延発生時の早期対応等に寄与できると判断できる場合は加点する	30	20	10	0
		5-1-3.	本業務のステークホルダを含めた課題・リスクを漏れなく洗い出すための工夫（コミュニケーション方法等）が提案されており、確実な課題解決の推進に寄与できると判断できる場合は加点する	30	20	10	0
6.	後年度予定コスト			**763**			
	6-1.	後年度に発生する予定コスト		763			
		6-1-2.	後年度予定コストの合計額（税込み）が、センターの設定する「加点基準コスト」を下回っている場合は加点する ※「加点基準コスト」は、「上限コスト」とは異なる値であり、非開示とする	以下の式により算出する。 小数点以下は切り捨てる。また、負の値は0点として扱う。 $763 \times \left(1 - \frac{\text{提案された後年度予定コスト}}{\text{加点基準コスト}}\right)$			