「次期図書館業務システムの導入及び運用保守業務一式」に係る一般競争入札

（総合評価落札方式）

入札説明書

独立行政法人国立女性教育会館

目　次

Ⅰ．入札説明書

独立行政法人国立女性教育会館の物品納入に係る入札公告（令和7年10月3日付け公告）に基づく入札については、関係法令並びに独立行政法人国立女性教育会館会計規程及び入札心得のほか下記に定めるところによる。

記

１．競争入札に付する事項

（１）作業の名称　　次期図書館業務システムの導入及び運用保守業務一式

（２）作業内容等　　別紙仕様書のとおり。

（３）履 行 期 限　　別紙仕様書のとおり。

（４）作 業 場 所　　別紙仕様書のとおり。

（５）入 札 方 法　　落札者の決定は総合評価落札方式をもって行うので、

① 入札に参加を希望する者（以下「入札者」という。）は「Ⅱ．提出書類」に記載の提出書類を提出すること。

② 上記①の提出書類のうち、入札書については仕様書及び契約書案に定めるところにより、入札金額を見積るものとする。入札金額は、「次期図書館業務システムの導入及び運用保守業務一式」に関する総価とし、総価には本件業務に係る一切の費用を含むものとする。

③ 落札決定に当たっては、入札書に記載された金額に当該金額の10パーセントに相当する額を加算した金額（当該金額に1円未満の端数が生じたときは、その端数金額を切捨てるものとする。）をもって落札価格とするので、入札者は、消費税及び地方消費税に係る課税事業者であるか免税事業者であるかを問わず、見積もった契約金額の110分の100に相当する金額を入札書に記載すること。

④ 入札者は、提出した入札書の引き換え、変更又は取り消しをすることはできないものとする。

２．競争参加資格

（１）独立行政法人国立女性教育会館契約事務取扱要領第13条第1項及び第2項に規定される次の事項に該当する者は、競争に参加する資格を有さない。

①未成年者（婚姻若しくは営業許可を受けている者を除く。）、成年被後見人、被保佐人及び被補助人並びに破産者で復権を得ない者

なお、未成年者、被保佐人又は被補助人であって、契約締結のために必要な同意を得ている場合は、これにあたらない。

②以下の各号のいずれかに該当し、かつ、その事実があった後２年を経過していない者（これを代理人、支配人その他の使用人として使用する者についてもまた同じ。）

（ア）契約の履行に当たり故意に工事若しくは製造を粗雑にし、又は物件の品質若しくは数量に関して不正の行為をした者

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

（ウ）落札者が契約を結ぶこと又は契約者が契約を履行することを妨げた者

（エ）監督又は検査の実施に当たり職員の職務の執行を妨げた者

（オ）正当な理由がなくて契約を履行しなかった者

（カ）前各号のいずれかに該当する事実があった後2年を経過しない者を、契約の履行に当たり、代理人、支配人その他の使用人として使用した者

（２）文部科学省競争参加資格（全省庁統一資格）において、開札時までに令和７・８・９年度の「役務の提供等」のＡ，Ｂ，Ｃ又はＤの等級に格付けされている者であること。なお、競争参加資格を有しない入札者は、速やかに資格審査申請を行う必要がある。

（３）現在、国又は政府関係機関からの補助金交付の停止又は契約に係る指名停止等の行政処分を受けていないこと。

（４）警察当局から暴力団員が実質的に経営を支配する者又はこれに準ずるものとして、官庁等から

の排除要請があり、当該状態が継続している者でないこと。
（５）独立行政法人国立女性教育会館事務局長から取引停止の措置を受けている期間中の者でないこと。

３．入札者の義務
（１）入札者は、当入札説明書を了知のうえ、入札に参加しなければならない。
（２）入札者は、提出書類を提出期限内に提出しなければならない。また、開札日の前日までの間において当会館から当該書類に関して説明を求められた場合は、書面をもって説明しなければならない。

４．入札に関する質問書等の提出方法及び提出期限等
（１）提出期間　令和７年 10 月 3 日（金）から令和７年 10 月 17 日（金）15 時まで
（２）提出先
「Ⅱ．提出書類」の「１．提出先」参照。
（３）提出書類及び提出方法
「Ⅱ．提出書類」の「２．入札に関する質問書等の提出」参照。
（４）回答の共有
問い合わせは、令和7年10月31日（金）までに、入札者全員に回答を共有する。

５．事前提出書類の提出方法及び提出期限等
（１）提出期間　令和７年 10 月 3 日（金）から令和７年 11 月 10 日（月）
（２）提出先
「Ⅱ．提出書類」の「１．提出先」参照。
（３）提出書類及び提出方法
「Ⅱ．提出書類」の「３．事前提出書類の提出」参照。
（４）審査結果
提出された事前提出資料が仕様書等の求める要件を満たしているか審査した結果について、令和７年 12 月 1 日（月）までに回答を行う。要件を満たしていると通知された入札者のみが入札に参加できるものとする。

６．入札書等の提出方法及び提出期限等
（１）提出期間
審査結果通知日から令和７年 12 月 15 日（月）17 時まで（郵送の場合必着）
上記期間を過ぎた入札書等はいかなる理由があっても受け取らない。
（２）提出先
「Ⅱ．提出書類」の「１．提出先」参照。
（３）提出書類及び提出方法
「Ⅱ．提出書類」の「４．入札書等の提出方法及び提出期限等」参照。

７．開札の日時及び場所
（１）開札の日時
令和7年12月16日（火）13時30分
（２）開札の場所
埼玉県比企郡嵐山町菅谷728番地
独立行政法人国立女性教育会館　本館2階会議室（予定）
開札に立会わない場合、開札日時には電話連絡のつく場所で待機すること。開札後、落札者を決定したときは、落札者の氏名（法人の場合はその名称又は商号及び代表者の氏名）及び住所並びに落札金額を連絡する。

８．入札の無効

入札書で次の各号の一に該当するものは、これを無効とする。

（１）公告に示した競争に参加する者に必要な資格のない者が提出した入札書

（２）請負に付される役務の表示及び入札金額のない入札書

（３）入札者本人の氏名（法人の場合は、その名称又は商号及び代表者の氏名）及び押印の無い又は判然としない入札書。

（４）代理人が入札する場合は、入札者本人の氏名（法人の場合は、その名称又は商号及び代表者の氏名）、代理人であることの表示並びに当該代理人の氏名及び押印ない又は判然としない入札書（入札者本人の氏名（法人の場合は、その名称又は商号及び代表者の氏名）又は代理人であることの表示のない又は判然としない場合には、正当な代理であることが代理委任状その他で確認されたものを除く。）

（５）請負に付される役務の表示に重大な誤りがある入札書

（６）入札金額の記載が不明確な入札書

（７）入札金額の記載を訂正したものでその訂正について印の押していない入札書

（８）その他、入札に関する条件を違反した入札書

９．落札者の決定方法

（１）決定方法

落札者の決定は、総合評価落札方式をもって行い、次の要件を共に満たしている者のうち、「（２）総合評価点の計算及び得点配分」によって得られた数値の最も高い者を落札者とする。

①入札価格が予定価格の制限の範囲内であること。

②評価項目一覧の必須項目を全て満たしていること。

（２）総合評価点の計算及び得点配分

総合評価点　＝　技術点（満点500点）　＋　価格点（満点400点）

技術点　＝　必須項目200点 ＋必須項目（段階）100点＋ 加点項目200点

価格点　＝　NWECが定めた最低価格を400点、予定価格を0点とし、最低価格から予定価格の範囲内で点数を算出する。小数点第2位以下は切り捨てとする。

（３）技術審査

「評価項目一覧」の各事項について、次のとおり技術審査を行う。

①必須項目について、「対応可否」欄の全てに「○」が記入されていることを確認する。

※必須項目の仕様を満たさない場合は失格とする。

②「詳細」欄の記載を踏まえ、複数の審査員の合議によって各項目を評価し、評価に応じた得点の合計をもって技術点とする。

（４）価格審査

独立行政法人国立女性教育会館契約事務取扱要領第18条の規定に基づいて作成された予定価格の制限の範囲内で、当会館が入札説明書で指定する要求事項のうち、必須とした項目の最低限の要求をすべて満たしている提案をした入札者の中から、当会館が定める総合評価の方法をもって落札者を定めるものとする。落札者となるべき者の入札価格によっては、その者により当該契約の内容に適合した履行がなされないおそれがあると認められるとき、又はその者と契約することが公正な取引の秩序を乱すこととなるおそれがあって著しく不適当であると認められるときは、予定価格の範囲内の価格をもって入札をした他の者のうち、評価の最も高い者を落札者とすることがある。

（５）再度入札

開札の結果、予定価格の制限に達した価格の入札がないときは、直ちに再度の入札を行う。

入札者の全てが開札に立ち会っていない場合は、下記のとおり取り扱う。

①再度の入札を行うときは電話連絡し、再度入札参加の有無を確認する。

開札日の午後5時00分までに電話連絡が取れなかった場合は、再度入札を辞退したとみな

す。
②再度の入札を行うときは、入札書の受領期限は翌日以降に設定する。
原則、翌日の午後5時00分を入札書の受領期限とする見込み。
③再度の入札の入札書の受領期限までに、立会いの有無及び立会わない場合は開札当日に連絡が取れる連絡先（携帯電話番号等）を、電子メールにより連絡すること。
④開札に立会わない場合、開札日時には電話連絡のつく場所で待機すること。開札後、落札者を決定したときは、落札者の氏名（法人の場合はその名称又は商号及び代表者の氏名）及び住所並びに落札金額を連絡する。

（６）留意事項
落札者が指定の期日までに契約書の取交わしをしないときは、落札の決定を取消すものとする。

10. 入札保証金及び契約保証金　全額免除

11. 契約書作成
（１）競争入札を執行し、契約の相手方が決定したときは、契約の相手方として決定した日から7日以内（契約の相手方が遠隔地にある等特別の事情があるときは、指定の期日まで）に契約書の取り交わしをするものとする。
（２）契約書を作成する場合において、契約書の相手方が隔地にあるときは、まずその者が契約書の案に記名して押印し、さらに理事長が当該契約書の案の送付を受けてこれに記名して押印するものとする。
（３）（２）の場合において、理事長が記名し押印したときは、当該契約書の1通を契約の相手方に送付するものとする。
（４）理事長が契約の相手方とともに契約書に記名し押印しなければ本契約は、確定しないものとする。

12. 支払の条件
契約代金は、業務の完了後、当会館が適法な支払請求書を受理した日の属する月の翌月末日までに契約金額を支払うものとする。

13. 契約者の氏名並びにその所属先の名称及び所在地
〒355-0292　埼玉県比企郡嵐山町大字菅谷728番地
独立行政法人国立女性教育会館　理事長　萩原　なつ子

14. その他
（１）入札結果等、契約に係る情報については、当会館のウェブサイトにて公表（注）するものとする。
（２）落札者は、契約締結時までに入札内訳書を提出するものとする。

（注） 独立行政法人の事務・事業の見直しの基本方針（平成 22 年 12 月 7 日閣議決定）に基づく契約に係る情報の公表について

独立行政法人が行う契約については、「独立行政法人の事務・事業の見直しの基本方針」（平成 22 年 12 月 7 日閣議決定）において、独立行政法人と一定の関係を有する法人と契約をする場合には、当該法人への再就職の状況、当該法人との間の取引等の状況について情報を公開するなどの取組を進めるとされているところです。

これに基づき、以下のとおり、当会館との関係に係る情報を当会館のウェブサイトで公表することとしますので、所要の情報の当方への提供及び情報の公表に同意の上で、応札若しくは応募又は契約の締結を行っていただくよう御理解と御協力をお願いいたします。

なお、案件への応札若しくは応募又は契約の締結をもって同意されたものとみなさせていただきますので、ご了知願います。

（１）公表の対象となる契約先

次のいずれにも該当する契約先

① 当会館において役員を経験した者（役員経験者）が再就職していること又は課長相当職以上の職を経験した者（課長相当職以上経験者）が役員、顧問等として再就職していること

② 当会館との間の取引高が、総売上高又は事業収入の 3 分の 1 以上を占めていること

※ 予定価格が一定の金額を超えない契約や光熱水費の支出に係る契約等は対象外

（２）公表する情報

上記に該当する契約先について、契約ごとに、物品役務等の名称及び数量、契約締結日、契約先の名称、契約金額等と併せ、次に掲げる情報を公表します。

① 当会館の役員経験者及び課長相当職以上経験者（当会館 OB）の人数、職名及び当会館における最終職名

② 当会館との間の取引高

③ 総売上高又は事業収入に占める当会館との間の取引高の割合が、次の区分のいずれかに該当する旨

3 分の 1 以上 2 分の 1 未満、2 分の 1 以上 3 分の 2 未満又は 3 分の 2 以上

④ 一者応札又は一者応募である場合はその旨

（３）当方に提供していただく情報

① 契約締結日時点で在職している当会館 OB に係る情報（人数、現在の職名及び当会館における最終職名等）

② 直近の事業年度における総売上高又は事業収入及び当会館との間の取引高

（４）公表日

契約締結日の翌日から起算して原則として 72 日以内（4 月に締結した契約については原則として 93 日以内）

（５）実施時期

平成 23 年 7 月 1 日以降の一般競争入札・企画競争・公募公告に係る契約及び平成 23 年 7 月 1 日以降に契約を締結した随意契約について適用します。

なお、応札若しくは応募又は契約の締結を行ったにもかかわらず情報提供等の協力をしていただけない相手方については、その名称等を公表させていただくことがあり得ますので、ご了知願います。

入　　札　　心　　得

（１）趣旨

独立行政法人国立女性教育会館（以下「会館」という。）の契約に係る一般競争又は指名競争（以下「競争」という。）を行う場合において、入札者が熟知し、かつ遵守しなければならない事項は、関係法令、会館会計規程及び入札説明書に定めるもののほか、この心得に定めるものとする。

（２）仕様書等

①入札者は、仕様書、契約書案及び添付書類を熟読のうえ入札しなければならない。
②入札者は、前項の書類について疑義があるときは、関係職員に説明を求めることができる。
③入札者は、入札後、第１項の書類についての不明を理由として異議を申し立てることができない。

（３）入札保証金及び契約保証金

入札保証金及び契約保証金は、全額免除する。

（４）入札の方法

入札者は、別紙様式による入札書を直接又は郵便等で提出しなければならない。

（５）入札書の記載

落札決定に当たっては、入札書に記載された金額に当該金額の 10 パーセントに相当する額を加算した金額をもって落札価格とするので、入札者は消費税に係る課税事業者であるか免税事業者であるかを問わず、見積もった契約金額の 110 分の 100 に相当する金額を入札書に記載すること。

（６）入札に立ち会う場合

①開札当日に入札書を持参する場合は、入札書を封筒に入れ、封緘のうえ入札者の氏名を表記し、予め指定された時刻までに契約担当職員等に提出しなければならない。この場合において、入札書とは別に提案書及び証書等の書類を添付する必要のある入札にあっては、入札書と併せてこれら書類を提出しなければならない。
②入札者は、代理人をして入札させるときは、その委任状を持参させなければならない。

（７）郵便等入札

①郵便等入札を行う場合には、二重封筒とし、入札書を中封筒に入れ、封緘のうえ入札者の氏名、宛先、及び入札件名を表記し、予め指定された時刻までに到着するように契約担当職員等あて書留で提出しなければならない。この場合において、入札書とは別に提案書及び証書等の書類を添付する必要のある入札にあっては、入札書と併せてこれら書類を提出しなければならない。
②入札者は、代理人をして入札させるときは、その委任状を同封しなければならない。

（８）代理人の制限

①入札者又はその代理人は、当該入札に対する他の代理をすることができない。
②入札者は、国立女性教育会館契約事務取扱要領第 13 条第 2 項の一に該当すると認められる者を競争に参加することが出来ない期間は入札代理人とすることができない。

（９）条件付きの入札

同第 14 条第 1 項に規定する一般競争に係る資格審査の申請を行ったものは、競争に参加する者に必要な資格を有すると認められること又は指名競争の場合にあっては指名されることを条件に入札書を提出することができる。この場合において、当該資格審査申請書の審査が開札日までに終了しないとき又は資格を有すると認められなかったとき若しくは指名されなかったときは、当該入札書は落札の対象としない。

(10) 入札の取り止め等

入札参加者が連合又は不穏の行動をなす場合において、入札を公正に執行することができないと認められるときは、当該入札者を入札に参加させず又は入札の執行を延期し、若しくは取り止めることがある。

(11) 入札の無効

次の各号の一に該当する入札は、無効とする。

①競争に参加する資格を有しない者による入札
②指名競争入札において、指名通知を受けていない者による入札
③委任状を持参しない代理人による入札
④記名押印を欠く入札
⑤金額を訂正した入札
⑥誤字、脱字等により意思表示が不明瞭である入札
⑦明らかに連合によると認められる入札
⑧同一事項の入札について他人の代理人を兼ね又は2者以上の代理をした者の入札
⑨入札者に求められる義務を満たすことを証明する必要のある入札にあっては、証明書が契約担当職員等の審査の結果採用されなかった入札
⑩入札書受領期限までに到着しない入札
⑪暴力団排除に関する誓約事項（別記）について、虚偽が認められた入札
⑫その他入札に関する条件に違反した入札

(12) 開札

開札には、入札者又は代理人を立ち会わせて行うものとする。ただし、入札者又は代理人が立会わない場合は、入札執行事務に関係のない職員を立会わせて行うものとする。

(13) 落札者の決定

①一般競争入札総合評価落札方式（以下「総合評価落札方式」という。）にあっては、契約担当職員等が採用できると判断した提案書を入札書に添付して提出した入札者であって、その入札金額が予定価格の制限の範囲内で、かつ提出した提案書と入札金額を当該入札説明書に添付の評価手順書に記載された方法で評価、計算し得た評価値（以下「総合評価点」という。）が最も高かった者を落札者とする。
②低入札となった場合は、一旦落札決定を保留し、低入札価格調査を実施の上、落札者を決定する。
③前項の規定による調査の結果その者により当該契約の内容に適合した履行がされないおそれがあると認められるとき、又はその者と契約を締結することが公正な取引の秩序を乱すこととなるおそれがあって著しく不適当であると認められるときは、下記の者を落札者とすることがある。

・総合評価落札方式　予定価格の制限の範囲内の価格をもって入札をした他の者のうち、総合評価点が最も高かった者

(14) 同価格又は同総合評価点の入札者が二者以上ある場合の落札者の決定

①落札となるべき同価格又は同総合評価点の入札をした者が二者以上あるときは、直ちに当該入札をした者又は（12）において立ち会いをした者にくじを引かせて落札者を決定する。
②①の場合において、当該入札をした者のうちくじを引か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職員にくじを引かせるものとする。

(15) 契約書の提出

①落札者は、契約担当職員等から交付された契約書に記名押印し、指定の期日までに契約担当職員等に提出しなければならない。
②理事長が契約の相手方とともに契約書に記名し押印しなければ本契約は、確定しないものとする。

(16) 入札書に使用する言語及び通貨

入札書及びそれに添付する仕様書等に使用する言語は、日本語とし、通貨は日本国通貨に限る。

（17）落札決定の取消し

①落札決定後であっても、この入札に関して連合その他の事由により正当な入札でないことが判明したときは、落札決定を取消すことができる。

②落札者が指定の期日までに契約書の取交わしをしないときは、落札の決定を取消すものとする。

以上

Ⅱ．提出書類

１．提出先

〒355-0292
埼玉県比企郡嵐山町大字菅谷728番地
独立行政法人国立女性教育会館　財務・企画課　担当：宇佐美
TEL：0493-62-6717　E-mail：kaikei@ml.nwec.go.jp

２．入札に関する質問書等の提出

	提出書類		部数
1	入札に関する質問書	様式１	電子ファイル
2	図書館システムの名称等について	様式２	電子ファイル

（１）入札者は、契約書（案）、仕様書等について疑義があるときは入札に関する質問書を提出し説明を求めることができる。

（２）なお、問い合わせの際に「図書館システムの名称等について」の提出をお願いしたい。「Ⅰ．入札説明書」の「５．事前提出書類の提出方法及び提出期限等」に従い「図書館システムの名称等について」を提出しても良いが、会館がサプライチェーン・リスクに係る懸念が払拭されないと判断した場合、機器リスト・参考価格の再提出が時間的に難しいので「入札に関する質問書」等と同時に提出をお願いしたい。

３．事前提出書類の提出

	提出書類		部数
1	図書館システムの名称等について 注意：「２．入札に関する質問書等の提出」により提出した場合は提出不要	様式２	電子ファイル
2	【ISMAP クラウドサービスに登録されている場合】		
	・「ISMAP クラウドサービスリスト」に登録されていることを証明できる書類	－	電子ファイル
3	【ISMAP クラウドサービスに登録されていない場合】		
	・基本言明要件の一覧表	様式３	電子ファイル
	・ISMS（JIS Q 27001）認証登録を証明できる書類	－	１通
	・ISMS クラウドセキュリティ認証（JIS Q 27017）認証登録している場合はそれを証明できる書類	－	１通
4	評価項目一覧 注意：参考資料を添付すること	様式４	２部及び 電子ファイル
5	一般競争（指名競争）参加資格（全省庁統一資格）審査結果通知書	（写し）	１通
6	暴力団等反社会的勢力でないこと等に関する表明・確約書	様式５	電子ファイル
7	受託者の要件のうち以下に関する証明書 ・プライバシーマークまたは ISO/IEC 27001 ・ワーク・ライフ・バランス等の推進に関する取組への政府機関の認証	写し	１通
8	受託者の要件のうち実績に関する証明書	様式６	電子ファイル
9	参考見積書	様式７	電子ファイル

（1）評価項目一覧

①印刷サイズ

A3判

②電子ファイル形式

Excelファイル（行の高さは記入量に応じて変更可能）

③評価項目一覧の構成と概要

下表のとおり。「入札事業者記入欄」について、下表の指示に従い、記入すること。

項目欄名		概要
項目・項番・要件（評価項目）		仕様書に記載の要件を評価項目として示している。
入札事業者記入欄	対応可否	「○」（対応可）もしくは「×」（対応不可）を必須記入。黄色に塗りつぶされた欄は項目の区切りを示しているため、記載不要。
	詳細	具体的な対応内容等を必須記入。 なお、評価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であるように記載すること（必要に応じて、用語解説などを添付してもよい）。
	提案資料該当箇所	別途、詳細を示す提案資料がある場合には、そのページ・項番を記入。
評価区分	必須	本件を実施する上で必須となる事項。「詳細」欄の記載及び提案資料を確認し、評価する。仕様を満たさない場合は失格とする。
	加点	必ずしも提案する必要はない事項。これらの事項については、入札者が「○」（対応可）としている場合にのみ各評価項目に従い評価し、採点する。また、当該項目への提案内容により不合格となることはない。
配点		得られる最高得点を示している。
評価・採点基準		どのような基準で採点するかを示している。

4．入札書等の提出方法及び提出期限等

	提出書類		部数
1	入札書（封緘）	様式８	１通
2	委任状（代理人に委任する場合のみ）	様式９	１通
3	復委任状（復代理人に委任する場合のみ）	様式１０	１通

（1）入札書、委任状、復委任状は持参又は郵送（書留郵便等配達記録が残るものに限る。受付期間内必着。）すること。なお、電子メールによるものは受け付けない。

（2）提出された書類は、本入札における落札者決定の目的にのみ使用し、評価結果に関わらず返却しない。ただし、落札者の提出した「評価項目一覧」は契約書に添付する。

（様式１「入札説明書等資料に関する質問書」）

「次期図書館業務システムの導入及び運用保守業務一式」に係る入札説明書等資料に関する質問書

《次の枠内に記入してください。》

社名	
質問項目	資料名と該当頁・該当箇所（〇行目～〇行目）
質問内容	

備考

・記入に当たっては、可能な範囲で簡潔且つ具体的にご記入願います。
・質問事項は本様式１枚につき１問としてください。
・質問事項が複数ある場合は、本紙を複製（頁を分けて）の上、使用ください。

提 出 先：国立女性教育会館　財務・企画課　宇佐美宛
提出方法：メールにて。提出の際、メール件名に貴社名を入れてください。
メ ー ル：kaikei@ml.nwec.go.jp
期　　限：令和７年 10 月 17 日（金）15 時まで
ワードファイルのままお送りください。
質問及び当館からの回答内容は、入札参加者に共有させていただきます。
共有の際、貴社名は削除いたします。

【国立女性教育会館回答欄】

様式２

図書館システムの名称等について

提出日	
事業者名	
担当者名	
担当者連絡先	メールアドレス 電話番号

図書館システムについてご記入ください

システムが複数ある場合は、このページをコピーしてください。

区分	図書館システム
外部サービス提供業者	
外部サービス提供業者の法人番号 ※１３桁の法人番号を記入 法人番号が不明な場合は本社所在地を記入	
クラウドサービス名・ モバイルアプリケーション名	
アプリケーションのインストールの要否 ※必要または不要と記入	
備考 ※モバイルアプリケーションの場合はバージョンを記入	

ガバナンス基準		適合状況	採用しているセキュリティ対策概要	非採用理由
3	情報セキュリティガバナンス			
	情報セキュリティガバナンスは、組織の情報セキュリティ活動を指導し、管理するシステムである。情報セキュリティの目的及び戦略を、事業の目的及び戦略に合わせて調整する必要があり、法制度、規制及び契約を遵守する必要がある。また、情報セキュリティガバナンスは、内部統制の仕組みによって遂行されるリスクマネジメント手法を通じて、評価、分析及び実施する。			
3.1	情報セキュリティガバナンスのプロセス			
3.1.1 概要				
	経営陣は、情報セキュリティを統治するために、評価、指示、モニタ及びコミュニケーションの各プロセスを実行する。さらに、保証プロセスによって、情報セキュリティガバナンス及び達成したレベルについての独立した客観的な意見が得られる。			
3.1.2　評価				
	評価とは、現在のプロセス及び予定している変更に基づくセキュリティ目的の現在及び予想される達成度を考慮し、将来の戦略的目的の達成を最適化するために必要な調整を決定するガバナンスプロセスである。			
	“評価”プロセスを実施するために、経営陣は、次のことを行う。			
3.1.2.1	経営陣は、事業の取組みにおいて情報セキュリティ問題を考慮することを確実にする。 ・経営陣は、管理者に、情報セキュリティが事業目的を十分にサポートし、支えることを確実にさせる。			
3.1.2.2	経営陣は、情報セキュリティのパフォーマンス結果に対応し、必要な処置の優先順位を決めて開始する。			
3.1.2.3	経営陣は、管理者に、重大な影響のある新規情報セキュリティプロジェクトを経営陣に付託するようにさせる。			
3.1.3 指示				
	指示は、経営陣が、実施する必要がある情報セキュリティの目的及び戦略についての指示を与えるガバナンスプロセスである。指示には、資源供給レベルの変更、資源の配分、活動の優先順位付け並びに、方針、適切なリスク受容及びリスクマネジメント計画の承認が含まれる。			
	“指示”プロセスを実施するために、経営陣は次のことを行う。			
3.1.3.1	経営陣は、その組織のリスク選好を決定する。			
3.1.3.2	経営陣は、情報セキュリティの戦略及び方針を承認する。 (ア)経営陣は、管理者に、情報セキュリティの戦略及び方針を策定・実施させる。 (イ)経営陣は、管理者に、情報セキュリティの目的を事業目的に合わせて調整させる。			
3.1.3.3	経営陣は、適切な投資及び資源を配分する。			
3.1.3.4	経営陣は、管理者に、情報セキュリティに積極的な文化を推進させる。			
3.1.4　モニタ				
	モニタは、経営陣が戦略的目的の達成を評価することを可能にするガバナンスプロセスである。			
	“モニタ”プロセスを実施するために、経営陣は次のことを行う。			
3.1.4.1	経営陣は、情報セキュリティマネジメント活動の有効性を評価する。 (ア)経営陣は、管理者に、事業の観点から適切なパフォーマンス指標を選択させる。 (イ)経営陣は、管理者に、経営陣が以前に特定した措置の実施及びそれらの組織への影響を含む、情報セキュリティのパフォーマンス成果についてのフィードバックを経営陣へ提供させる。			
3.1.4.2	経営陣は、内部及び外部の要求事項への適合性を確実にする。			
3.1.4.3	経営陣は、変化する事業、法制度、規制の環境、及びそれらの情報リスクへの潜在的影響を考慮する。			
3.1.4.4	経営陣は、管理者に、情報リスク及び情報セキュリティに影響する新規開発案件について、経営陣に対し注意を喚起させる。			
3.1.5　コミュニケーション				
	コミュニケーションは、経営陣及び利害関係者が、双方の特定のニーズに沿った情報セキュリティに関する情報を交換する双方向のガバナンスプロセスである。			
	コミュニケーションの方法の一つは、情報セキュリティの活動及び課題を利害関係者に説明する情報セキュリティ報告書である。			
	“コミュニケーション”プロセスを実施するために、経営陣は次のことを行う。			
3.1.5.1	経営陣は、外部の利害関係者に、組織がその事業特性に見合った情報セキュリティのレベルを実践していることを報告する。			
3.1.5.2	経営陣は、管理者に、情報セキュリティ課題を特定した外部レビューの結果を通知し、是正処置を要請する。			
3.1.5.3	経営陣は、情報セキュリティに関する規制上の義務、利害関係者の期待及び事業ニーズを認識する。			
3.1.5.4	経営陣は、管理者に、注意が必要な問題、また、できれば決定が必要な問題について、経営陣へ助言させる。			
3.1.5.5	経営陣は、管理者に、関連する利害関係者に対し、経営陣の方向性及び決定を支援するためにとるべき詳細な行動を、経営陣の方向性及び決定に沿って説明させる。			
3.1.6 保証				
	保証は、経営陣が独立した客観的な監査、レビュー又は認証を委託するガバナンスプロセスである。これは、望ましいレベルの情報セキュリティを達成するためのガバナンス活動の実行及び運営の遂行に関連した目的及び処置を特定し、妥当性を検証する。			
	“保証”プロセスを実施するために、経営陣は次のことを行う。			
3.1.6.1	経営陣は、要求している情報セキュリティ水準に対し、どのように説明責任を果たしているかについて、独立した客観的な意見を監査人等に求める。			
3.1.6.2	経営陣は、管理者に、経営陣が委託する監査、レビュー又は認証をサポートさせる。			

	マネジメント基準	適合状況	採用しているセキュリティ対策概要	非採用理由
4.1	マネジメント基準			
	マネジメント基準は、JIS Q 27001:2014を基に、情報セキュリティについて組織を指揮統制するために調整された活動である情報セキュリティマネジメントを確立、導入、運用、監視、維持及び改善するための基準を定める。マネジメント基準は、原則としてすべて実施しなければならないものである。			
4.2	記載内容について			
	「情報セキュリティ管理基準」の「マネジメント基準」に同じ。 クラウドサービスにおいては、クラウドサービス利用者の環境等を考慮して、クラウドサービス提供者の管理策等を検討し、実施する必要がある。そのため、クラウドサービス利用者及びクラウドサービス事業者間において、クラウドサービスにおける情報セキュリティリスクとその対応について、情報交換することが非常で重要である。 当該情報セキュリティリスクコミュニケーションについては、クラウドサービスにおいて特に考慮するべき事項として、4.9章に規定する。			
4.3	凡例			
	4.4章以降は、以下の構成をとる。 4.4　情報セキュリティマネジメント確立　[27001-4] 4.4.1　組織の役割、責任及び権限　[27001-5.3 / 5.1] 4.4.1.1　トップマネジメントは、情報セキュリティマネジメントに関するリーダーシップ及びコミットメントを発揮する。　[27001-5.1b) / 5.1e) / 5.1f)] その際は、以下を行うこととする。 ・組織のプロセスへ、その組織が必要とする情報セキュリティマネジメント要求事項を統合する ： [27001-X.X.X]は、JIS Q 27001:2014において関連する条項(X.X.X)を示す。			
4.4	情報セキュリティマネジメントの確立 [27001-4.4]			
	情報セキュリティマネジメントを確立するために、その基盤となる適用範囲を決定し、方針を確立する。これらをもとに、情報セキュリティリスクアセスメントを実施し、その対応を計画し実施する。それにより、組織が有効な情報セキュリティマネジメントを実施するための基盤作りを行う。			
4.4.1	組織の役割、責任及び権限 [27001-5.3 / 5.1]			
4.4.1.1	トップマネジメントは、情報セキュリティマネジメントに関するリーダーシップ及びコミットメントを発揮する。　[27001-5.1b) / 5.1e) / 5.1f)] ・組織のプロセスへ、その組織が必要とする情報セキュリティマネジメント要求事項を統合する。 ・情報セキュリティマネジメントがその意図した成果を達成することを確実にする。 ・情報セキュリティマネジメントの有効性に寄与するよう人々を指揮し、支援する。 また、トップマネジメントがリーダーシップ及びコミットメントを発揮していることを以下により確認する。 ・経営会議等の議事録に、トップマネジメントの情報セキュリティマネジメントに関する意思、判断、指示等が記録されていること。 ・情報セキュリティ方針、情報セキュリティ目的及びそれを達成する計画を策定する際に、トップマネジメントの意思、判断、指示等が含まれていること。 ・達成すべきセキュリティの水準として、リスクレベルをトップマネジメントが決定していること。 ・リスクレベルに応じて選択したセキュリティ管理策を実施させる際に、トップマネジメントの意思、判断、指示等が含まれていること。 ・内部監査において確認すべき事項に、トップマネジメントが要求する情報セキュリティ要求事項等が含まれていること。 ・内部監査報告書やそれらに基づく是正処置、マネジメントピュー議事録等に、トップマネジメントの意思、判断、指示等が含まれていること。			
4.4.1.2	トップマネジメントは、組織の役割について、以下の責任及び権限を割り当て、伝達する。 [27001-5.3] ・情報セキュリティマネジメントを、本管理基準の要求事項として適合させる。 ・情報セキュリティマネジメントのパフォーマンス評価をトップマネジメントに報告する。 また、情報セキュリティマネジメントを本管理基準の要求事項に適合させるために、以下のような責任・権限を割り当てていることを確認する。 ・セキュリティ要求事項を盛り込んだ情報セキュリティ方針等の文書を策定する責任・権限 ・リスクアセスメントにおいて、リスクを運用管理する責任・権限を持つリスク所有者 ・セキュリティ要求事項を満たす管理策を教育、普及させる責任・権限 ・セキュリティ要求事項を満たしているか監査する責任・権限 ・各プロセスの結果及び効果をトップマネジメントに報告する責任・権限 ・各プロセスの結果及び効果を組織内に周知する責任・権限			
4.4.1.3	トップマネジメントは、管理層がその責任の領域においてリーダーシップを発揮できるよう、管理層の役割を支援する。 [27001-5.1h)] 管理層が、その職掌範囲、組織等において、リーダーシップを発揮できるよう、トップマネジメントは、管理層に、必要な権限を委譲していることを確認する。			
4.4.2	組織及びその状況の理解 [27001-4.1]			
4.4.2.1	組織は、組織の目的に関連し、かつ、情報セキュリティマネジメントの意図した成果を達成する組織の能力に影響を与える、以下の課題を決定する。 [27001-4.1] ・外部の課題 ・内部の課題 これらの課題の決定とは、組織の外部状況及び内部状況の確定のことをいう。外部状況及び内部状況には、以下のようなものが含まれる。 a)　外部状況 ・国際、国内、地方又は近隣地域を問わず、文化、社会、政治、法律、規制、金融、技術、経済、自然及び競争の環境 ・組織の目的に影響を与える主要な原動力及び傾向 ・外部ステークホルダとの関係並びに外部ステークホルダの認知及び価値観			
	b)　内部状況 ・統治、組織体制、役割及びアカウンタビリティ ・方針、目的及びこれらを達成するために策定された戦略 ・資源及び知識として見た場合の能力（例えば、資本、時間、人員、プロセス、システム及び技術） ・情報システム、情報の流れ及び意思決定プロセス（公式及び非公式の双方を含む。） ・内部ステークホルダとの関係並びに内部ステークホルダの認知及び価値観 ・組織文化 ・組織が採択した規格、指針及びモデル ・契約関係の形態及び範囲			
4.4.3	利害関係者のニーズ及び期待の理解 [27001-4.2]			
4.4.3.1	組織は、利害関係者のニーズ及び期待を理解するために、以下を決定する。 [27001-4.2] ・情報セキュリティマネジメントに関連する利害関係者 ・利害関係者の、情報セキュリティに関連する要求事項 利害関係者の要求事項には、法的及び規制の要求事項並びに契約上の義務を含めてもよいが、利害関係者には、以下のようなものが含まれる。 ・組織内で情報セキュリティマネジメントプロセスを推進する役割・権限を持つ人又は組織。例えば、以下のようなものをいう。 -情報セキュリティに関する方針等を策定する人又は組織(トップマネジメント等) -セキュリティ管理策を全組織に徹底させる人又は組織(総務部、情報システム部等) -情報セキュリティ監査を行う人又は組織(監査室等) -組織内の情報セキュリティ専門家 ・取引先、パートナー、サプライチェーン上の関係者 ・親会社、グループ会社 ・当該組織のセキュリティを監督する省庁、政府機関 ・所属するセキュリティ団体、協会			

	マネジメント基準	適合状況	採用しているセキュリティ対策概要	非採用理由
4.4.4	適用範囲の決定 [27001-4.3]			
	情報セキュリティマネジメントを確立、導入、運用、監視、レビュー、維持及び改善するために、まず適用範囲を明確にし、組織に合った情報セキュリティマネジメントを構築する基盤を整える。			
4.4.4.1	組織は、情報セキュリティマネジメントの境界及び適用可能性を明確にし、適用範囲を決定する。 [27001-4.3] a) 組織は以下の点を考慮して適用範囲及び境界を定義する。 ・自らの事業 ・体制 ・所在地 ・資産 ・技術の特徴 ・外部及び内部の課題 ・利害関係者の情報セキュリティに関連する要求事項 ・組織が実施する活動と他の組織が実施する活動との間のインタフェース及び依存関係 b) 情報セキュリティマネジメントの目的や目標は、組織の特徴によって異なる。			
	c) 情報セキュリティマネジメントに対する要求事項はそれぞれの組織の事業によって、外部状況、内部状況の双方があり、これらを考慮して適用範囲を定義する。 ・外部状況には、以下のようなものが含まれる。 －国際、国内、地方又は近隣地域を問わず、文化、社会、政治、法律、規制、金融、技術、経済、自然及び競争の環境 －組織の目的に影響を与える主要な原動力及び傾向 －外部ステークホルダとの関係並びに外部ステークホルダの認知及び価値観 ・内部状況には、以下のようなものが含まれる。 －統治、組織体制、役割及びアカウンタビリティ －方針、目的及びこれらを達成するために策定された戦略 －資源及び知識として見た場合の能力（例えば、資本、時間、人員、プロセス、システム及び技術） －情報システム、情報の流れ及び意思決定プロセス（公式及び非公式の双方を含む。） －内部ステークホルダとの関係並びに内部ステークホルダの認知及び価値観 －組織文化 －組織が採択した規格、指針及びモデル －契約関係の形態及び範囲			
4.4.5	方針の確立 [27001-5.2 / 6.2 / 5.1]			
4.4.5.1	トップマネジメントは、以下を満たす組織の情報セキュリティ方針を確立する。 [27001-5.2] ・組織の目的に対して適切であること。 ・情報セキュリティ目的、又は情報セキュリティ目的を設定するための枠組 ・情報セキュリティに関連して適用する要求事項を満たすことへのコミットメントを含むこと。 ・情報セキュリティマネジメントの継続的改善へのコミットメントを含むこと。 また、情報セキュリティ方針は情報セキュリティマネジメントにおける判断の基盤となる考え方を記載したものであり、組織の戦略に従って慎重に作成する。			
4.4.5.2	組織は、情報セキュリティ目的及びそれを達成するための計画を策定する。 [27001-6.2] a) 情報セキュリティ目的は、以下を満たすこととする。 ・情報セキュリティ方針と整合していること。 ・（実行可能な場合）測定可能であること。 ・適用される情報セキュリティ要求事項、並びにリスクアセスメント及びリスク対応の結果を考慮に入れること。 b) 情報セキュリティ目的は、関係者に伝達し、必要に応じて更新するとともに、情報セキュリティ目的を達成するための計画においては、以下を決定する。 ・実施事項 ・必要な資源 ・責任者 ・達成期限 ・結果の評価方法			
4.4.5.3	トップマネジメントは、以下によって、情報セキュリティマネジメントに関するリーダーシップ及びコミットメントを発揮する。 [27001-5.1a)] ・情報セキュリティ方針及び情報セキュリティ目的を確立すること。 ・情報セキュリティ方針及び情報セキュリティ目的は組織の戦略的な方向性と相矛盾しないこと。 また、情報セキュリティ方針は組織に伝えられるように文書化され、しかるべき方法で利害関係者が入手できるようにするとともに、トップマネジメントが情報セキュリティ方針にコミットした証拠を、以下のような記録をもって示す。 ・文書化された情報セキュリティ方針への署名 ・情報セキュリティ方針が議論された会議の議事録 これらはトップマネジメントの責任を明確にするために実施する。			
4.4.6	リスク及び機会に対処する活動 [27001-6.1]			
4.4.6.1	リスク及び機会を決定する。 [27001-6.1.1] a) 組織は、外部及び内部の課題、利害関係者の情報セキュリティに関連する要求事項を考慮し、以下のために対処する必要があるリスク及び機会を決定する。 ・情報セキュリティマネジメントが、組織が意図した成果を達成する。 ・望ましくない影響を防止又は低減する。 ・継続的改善を達成する。 当該決定の際、組織は、以下を計画する。 ・決定したリスク及び機会に対処する活動 ・リスク及び機会に対処する活動の情報セキュリティマネジメントプロセスへの統合及び実施方法 ・リスク及び機会に対処する活動の有効性の評価方法 b) リスク及び機会に対処する活動の記録として、具体的な対処計画（実施時期、実施内容、実施者、実施場所、実施に必要な資源などを規定した計画）を作成していることを確認するとともに、当該計画を作成する際、各対処計画が、情報セキュリティマネジメントプロセスの一部として実施されるよう、考慮するとともに、当該対処の有効性を評価する方法（実施状況や実施したことによる効果を評価する方法）を作成していることも確認する。			
4.4.7	情報セキュリティリスクアセスメント [27001-6.1.2]			
4.4.7.1	組織は、以下によって、情報セキュリティリスクアセスメントのプロセスを定め、適用する。 [27001-6.1.2a) / 6.1.2b)] a) 以下を含む情報セキュリティのリスク基準を確立し、維持する。 ・リスク受容基準 ・情報セキュリティリスクアセスメントを実施するための基準 b) リスク受容基準に、以下を反映するよう、考慮する。 ・組織の価値観 ・目的 ・資源			
	c) リスク受容基準を策定する際には、以下の点を考慮する。 ・原因及び発生し得る結果の特質及び種類、並びにこれらの測定方法 ・発生頻度 ・発生頻度、結果を考える時間枠 ・リスクレベルの決定方法 ・利害関係者の見解 ・リスク基準は、法令及び規制の要求事項、並びに組織が合意するその他の要求事項によって、組織に課せられるもの又は策定されるものもあること。 d) 情報セキュリティアセスメントを繰り返し実施した際に、以下の結果を生み出すこと。 ・情報セキュリティリスクアセスメントの結果に、一貫性及び妥当性があること。 ・情報セキュリティリスクアセスメントの結果が比較可能であること。 なお、情報セキュリティマネジメントにおけるリスクアセスメント手法には、定番といえるものがなく、それぞれの組織に適合したものを選択している場合が多いことから、必要に応じてツールを利用するなどが必要になる。			
4.4.7.2	組織は、以下によって、情報セキュリティリスクを特定する。 [27001-6.1.2c)] a) 情報セキュリティリスクアセスメントのプロセスを適用し、情報の機密性、完全性及び可用性の喪失に伴うリスクを特定する。 b) リスクを特定する過程において、リスク所有者を特定する。 c) リスクを特定する際には、以下について考慮する。 ・リスク源 が組織の管理下にあるか否かに関わらず、リスク源又はリスクの原因が明らかでないリスクも特定の対象にすること。 ・波及効果及び累積効果を含めた、特定の結果の連鎖を注意深く検討すること。 ・何が起こり得るのかの特定に加えて、考えられる原因及びどのような結果が引き起こされることがあるのかを示すシナリオ ・全ての重大な原因及び結果 ・以下を特定すること。 －リスク源 －影響を受ける領域、事象 －原因及び起こり得る結果 この段階で特定されなかったリスクは、今後の分析の対象から外されてしまうため、ある機会を追及しなかったことに伴うリスクも含め、リスクの包括的な一覧を作成する。			
4.4.7.3	組織は、以下によって、情報セキュリティリスクを分析する。 [27001-6.1.2d)] a) 以下の手順によりリスク分析を行う。 ・特定されたリスクが実際に生じた場合に起こり得る結果の分析を行う。 ・特定されたリスクの発生頻度の分析を行う。 ・リスクレベルを決定する。 ・特定した脅威やぜい弱性を基に、以下の点を考慮する。 －セキュリティインシデントが発生した場合の事業影響度 －セキュリティインシデントの発生頻度 －管理策が適用されている場合はその効果 b) リスク分析の際には、以下の点についても考慮する。 ・リスクの原因及びリスク源 ・リスクの好ましい結果及び好ましくない結果 ・リスクの発生頻度 ・リスクの結果及び発生頻度に影響を与える要素 なお、リスク分析は、状況に応じて、定性的、半定量的、定量的、又はそれらを組み合わせた手法で行うことが可能である。			

マネジメント基準		適合状況	採用しているセキュリティ対策概要	非採用理由
4.4.7.4	組織は、以下によって、情報セキュリティリスクを評価する。 [27001-6.1.2e)] ・リスク分析の結果、決定されたリスクレベルとリスク基準との比較をする。 ・リスク対応のための優先順位付けを行う。 ・リスク評価の結果は今後の改善に利用するため保管する。 なお、リスク対応の優先順位を決定する際には、より広い範囲の状況を考慮し、他者が負うリスクの受容レベルについて考慮するとともに、法令、規制、その他の要求事項についても考慮する。			
4.4.8	情報セキュリティリスク対応 [27001-6.1.3]			
4.4.8.1	組織は、情報セキュリティアセスメントの結果を考慮して、適切な情報セキュリティリスク対応の選択肢を選定する。 [27001-6.1.3a)] 情報セキュリティリスク対応の選択肢には、以下が含まれる。 ・リスクを生じさせる活動を開始又は継続しないと決定することによるリスクの回避 ・ある機会を目的としたリスクの引受け又はリスクの負担 ・リスク源の除去 ・発生頻度の変更 ・結果の変更 ・（契約及びリスクファイナンス を含む）他者とのリスクの共有 ・情報に基づいた意思決定によるリスクの保有 さらに、リスク対応の評価や改善に役立てるため、どの選択肢を選んだ場合も、その理由を明確にし、記載する。			
4.4.8.2	組織は、選定した情報セキュリティリスク対応の実施に必要な全ての管理策を決定する。 [27001-6.1.3b)] リスク対応のための方針を決めた上で、管理策の目的（管理目的）及び管理策について検討する。以下を考慮しつつ、対応による効果と対応に必要な費用及び労力のバランスを取り、適切な情報セキュリティ対応の選択肢を選定する。 ・リスクの受容可能レベル ・関連する法令 ・規制や契約上の要求事項 ・その他の社会的責任 なお、具体的な管理策の選定においては、管理目的に対応した「管理策基準」から適切なものを選択するが、「管理策基準」はすべてを網羅しているわけではないので、組織の事業や業務などによってその他の管理策を追加してもよい 。			
4.4.8.3	組織は、管理策が見落とされていないことを検証する。 [27001-6.1.3c)] 必要な管理策の見落としがないか、管理策基準を参照するが、管理策基準に示す管理目的及び管理策以外の管理目的及び管理策が必要になった場合、他の管理目的及び管理策を追加することができる。			
4.4.8.4	組織は、情報セキュリティリスク対応計画を策定する。 [27001-6.1.3e)] a)情報セキュリティリスク対応計画には、以下を含む。 ・期待される効果を含む、対応選択肢選定の理由 ・情報セキュリティリスク対応計画の承認者及び対応計画の実施責任者 ・対応内容 ・必要な資源 ・費用・労力、制約 ・後日の報告、監視に必要な要求事項 ・対応工程における節目ごとの目標 ・対応時期及び日程 b) 責任及び権限について 情報セキュリティマネジメントにおいては最終的な承認をトップマネジメントが行っていることがほとんどであり、責任がトップマネジメントに集中している。 一方で、情報セキュリティリスクアセスメント及びリスク対応については、責任及び権限を持つリスク所有者が、責任及び権限を持つ。 リスク所有者は、トップマネジメント、又はトップマネジメントから任命され、責任及び権限が委譲された者であることが多いことから、情報セキュリティマネジメントにおいて、トップマネジメント及びリスク所有者が、どのような責任を持つかについて明確にする。			
4.4.8.5	組織は、リスク所有者から、情報セキュリティリスク対応計画について承認を得、かつ、リスク所有者に、残留している情報セキュリティリスクを受け入れてもらう。 [27001-6.1.3f)] すべてのリスクについて管理目的や管理策を選択した時点で、残留リスクについて明確にし、今後の対応計画を作成する。計画の作成においては以下の点について考慮する。 ・技術的に対応可能になる時期 ・コスト的に対応可能になる時期 残留リスクについては、定期的に見直しを行い、必要に応じて、対応の対象とするとともに、リスク対応後の残留リスクについては、リスク所有者のほか、経営陣やその他の利害関係者に認識させることを考慮する。 また、リスク所有者の責任を明確にするために、承認された会議の議事録を正しく保管する。			
4.5	情報セキュリティマネジメントの運用 [27001-8]			
4.5.1	資源管理 [27001-7.1 / 5.1]			
4.5.1.1	組織は、情報セキュリティマネジメントの確立、実施、維持及び継続的改善に必要な資源を決定し、提供する。 [27001-7.1] 管理目的を満たすためには、継続的に管理策を実施するとともに、人員の増加、システムの増加などの環境の変化に対応するために、適切な時期に適切に提供できるよう、経営資源を確保する。			
4.5.1.2	トップマネジメントは、情報セキュリティマネジメントに必要な資源が利用可能であることを確実にするため、以下のような資源を割り当てる。 [27001-5.1c)] ・情報セキュリティマネジメントの各プロセスに必要な人又は組織 ・情報セキュリティマネジメントの各プロセスに必要な設備、装置、システム ・上記に必要な費用			
4.5.2	力量、認識 [27001-7.2 / 7.3 / 5.1]			
4.5.2.1	トップマネジメントは、有効な情報セキュリティマネジメント及びその要求事項への適合の重要性を伝達する。 [27001-5.1d)] トップマネジメントは情報セキュリティマネジメントについて責任を負うが、実施においては組織全体の協力が必要であることを、情報セキュリティ方針と共に関係者に伝える。 また、組織が同じ規定に従って同じ判断ができるように、情報分類等の基準を策定するが、個人情報のように組織によって解釈が一部異なる情報の場合は、一般的な考え方に加え、自社の考え方を明確にした上で、関係者に伝える。			
4.5.2.2	組織は、組織の情報セキュリティパフォーマンスに影響を与える業務をその管理下で行う人（又は人々）に必要な力量を決定する。 [27001-7.2a)] 情報セキュリティマネジメントに関係する業務及び影響のある業務を特定し、役割を明確にした業務分掌を作成する。これらの業務分掌においては以下の点を明確にする。 ・役職名 ・業務内容 ・担当者の責任範囲 ・業務に必要な知識 ・業務に必要な資格 ・業務に必要な経験 知識や資格、経験などは環境や目的の変化によって変更される可能性があるため、最新の情報となるように随時見直しを行う。			
4.5.2.3	組織は、適切な教育、訓練又は経験に基づいて、組織の情報セキュリティパフォーマンスに影響を与える業務をその管理下で行う人（又は人々）が力量を備えられるようにする。 [27001-7.2b)] 適用される処置には、例えば、現在雇用している人々に対する教育訓練の提供、指導の実施、配置転換の実施などがある（教育や訓練などが間に合わないと判断される場合には相応の力量を有した要員の雇用が、また、社内業務との関連が少ない業務においては外部委託などがある。）。			
4.5.2.4	組織は、必要な力量を身に着けるための処置をとり、とった処置の有効性を評価する。 [27001-7.2c)] 必要な力量を身に着けるための処置としては、教育訓練が重要である。教育は「必要な知識を得させる」、訓練は「必要なスキル及び経験を得させる」ために実施する。教育の内容は一般的な脅威やぜい弱性などの知識だけではなく、業務上のリスクについてなど、組織の特徴を反映した内容を盛り込むなど、実効性のある内容となるようにする。 教育及び訓練を実施した結果、必要な力量が持てたかどうかを確認するために、以下を実施する。 ・知識の確認テスト ・スキルの実習テスト ・チェックリストなどによるベンチマーク 実施結果については記録し、要員選択の客観性を確保する。			
4.5.2.5	組織は、力量を常に把握し、その証拠として、適切な文書化した情報を組織が定めた期間保持する。 [27001-7.2d)] 教育、訓練については以下を検討し、定期的に実施する。 ・教育・訓練基本計画 ・教育・訓練実施計画 ・確認テスト又は評価報告 教育や訓練の一部を免除する場合は、それがどの技能や経験、資格に当てはまるかを明確にし、それぞれの担当者について調査し、一覧にする。資格については有効期限などを明確にし、更新する。			
4.5.2.6	組織の管理下で働く人々は、情報セキュリティ方針を認識する。 [27001-7.3a)] 情報セキュリティの活動について、組織が定めた目的と重要性について、情報セキュリティ方針の通達や教育の一環として周知徹底することによって、管理策がなぜ実施されているのかについての関係者の理解を深める。			
4.5.2.7	組織の管理下で働く人々は、情報セキュリティパフォーマンスの向上によって得られる便益を含む、情報セキュリティマネジメントの有効性に対する自らの貢献を認識する。 [27001-7.3b)] 以下の点について組織の管理下で働く人々に伝えることによって、各人の役割及び情報セキュリティマネジメントの有効性に対する自らの貢献を明確にする。 ・情報セキュリティマネジメントにおけるそれぞれの役割 ・役割を実行するための業務と手順（異常を検知した場合の報告手順も含む。） ・これらが記載された文書の所在			
4.5.2.8	組織の管理下で働く人々は、情報セキュリティマネジメントの要求事項に適合しないことの意味を認識する。 [27001-7.3c)]			
4.5.3	コミュニケーション [27001-7.4]			

マネジメント基準		適合状況	採用しているセキュリティ対策概要	非採用理由
4.5.3.1	組織は、情報セキュリティマネジメントに関連する内部及び外部のコミュニケーションを実施する必要性を決定する。 [27001-7.4] a)　内部及び外部のコミュニケーションを実施する際は、以下を考慮することとする。 ・コミュニケーションの内容（何を伝達するか。） ・コミュニケーションの実施時期 ・コミュニケーションの対象者 ・コミュニケーションの実施者 ・コミュニケーションの実施プロセス b)　内部コミュニケーションでは、以下に示すような者と、適宜及び定期的なコミュニケーションを実施する。 ・トップマネジメント ・情報セキュリティマネジメントを本管理基準の要求事項に適合させる権限者 ・情報セキュリティマネジメントのパフォーマンスをトップマネジメント又は組織内に報告する権限者 ・組織内の従業員			
	c)　外部コミュニケーションでは、以下に示すような者と、必要に応じて、コミュニケーションを実施する。 ・取引先、パートナー、サプライチェーン上の関係者 ・親会社、グループ会社 ・当該組織のセキュリティを監督する省庁、政府機関 ・所属するセキュリティ団体、協会			
4.5.4	情報セキュリティマネジメントの運用の計画及び管理 [27001-8.1]			
4.5.4.1	組織は、情報セキュリティ要求事項を満たすため、リスク及び機会に対処する活動を実施するために必要なプロセスを計画し、実施し、かつ管理する。 [27001-8.1]			
4.5.4.2	組織は、情報セキュリティ目的を達成するための計画を実施する。 [27001-8.1]			
4.5.4.3	組織は、計画通りに実施されたことを確信するために、文書化した情報を保持する。 [27001-8.1] 文書化した情報に、以下の情報が集められているかどうかを確認する。 ・管理策の実施状況 ・管理策の有効性 ・管理策を取り巻く環境の変化 また、これらの情報を把握し判断する体制を構築する。			
4.5.4.4	組織は、計画した変更を管理し、意図しない変更によって生じた結果をレビューし、必要に応じて、有害な影響を軽減する処置をとる。 [27001-8.1]			
4.5.4.5	組織は、外部委託するプロセスを決定し、かつ、管理する。 [27001-8.1]			
4.5.5	情報セキュリティリスクアセスメントの実施 [27001-8.2 / 8.3]			
4.5.5.1	組織は、以下のいずれかの場合において、情報セキュリティリスクアセスメントを実施する。 [27001-8.2] ・あらかじめ定めた間隔 ・重大な変更が提案された場合 ・重大な変化が生じた場合			
4.5.5.2	組織は、情報セキュリティリスク対応計画を実施する。 [27001-8.3] 情報セキュリティリスク対応計画の実施においては、明確にされた個々の責任について全うしていることを確認するための方策を講じる。			
4.5.5.3	トップマネジメントは、情報セキュリティリスク対応計画のために十分な経営資源を提供する。 情報セキュリティリスク対応計画には相応の経営資源が必要になるところ、以下の点について考慮する。 ・管理策の導入及び運用にかかる費用、人員、作業工数、技術 ・セキュリティインシデント発生時の一時対応にかかる費用 ・その他のリスク対応にかかる費用 運用においては管理策の効果測定などを実施するために必要な経営資源について考察し、予算化する。			
4.6	情報セキュリティマネジメントの監視及びレビュー [27001-5.1 / 8.2 / 9 / 10.2]			
4.6.1	有効性の継続的改善 [27001-10.2 / 8.2 / 9.2 / 9.3 / 5.1]			
4.6.1.1	組織は、以下を実施し、情報セキュリティマネジメントの適切性、妥当性及び有効性を継続的に改善する。 [27001-10.2 / 8.2 / 9.2 / 9.3] ・定期的な情報セキュリティリスクアセスメント ・定期的な情報セキュリティ内部監査 ・トップマネジメントによる定期的なマネジメントレビュー 継続的改善においては、これまで実施してきた管理策だけはなく、環境の変化に伴う新たな脅威やぜい弱性についても不適合を検出し処置する。			
4.6.1.2	トップマネジメントは、継続的改善を促進する。 [27001-5.1g)] 4.6.1.1.を実施するための、役割、責任及び権限を割り当て、実施するよう関係者に伝達する。			
4.6.2	パフォーマンス評価 [27001-9]			
4.6.2.1	組織は、情報セキュリティパフォーマンス及び情報セキュリティマネジメントの有効性を継続的に評価し、以下を決定する。 [27001-9.1] ・必要とされる監視及び測定の対象（情報セキュリティプロセス及び管理策を含む。） ・妥当な結果を確実にするための、監視、測定、分析及び評価の方法（比較可能で再現可能な結果を生み出す方法とする。） ・監視及び測定の実施時期及び頻度 ・監視及び測定の実施者 ・監視及び測定の結果の、分析（因果関係、相関関係を含む）及び評価の時期及び頻度 ・監視及び測定の結果の、分析及び評価の実施者 ・分析及び評価の結果に応じた対応措置 ・分析及び評価の結果の報告頻度			
4.6.2.2	組織は、あらかじめ定めた間隔で内部監査を実施する。 [27001-9.2a) / 9.2b)] a) 内部監査を実施する際は、以下を確認する。 ・以下に適合していること。 －情報セキュリティマネジメントに関して、組織自体が規定した要求事項 －本マネジメント基準の要求事項 ・情報セキュリティマネジメントが有効に実施され、維持されていること。 b) 内部監査は、管理策の有効性を総合的に確認するために定期的に実施し、計画及び結果について以下の文書で管理する。 ・内部監査基本計画 ・内部監査実施計画 ・内部監査報告書 基本計画書では対象範囲、目的、管理体制及び期間又は期日について、実施計画では実施時期や実施場所、実施担当者及びその割当て及び詳細な監査の手法についてあらかじめ決める。 予定通り実施されたことを証明するためにも、実施報告書を作成する。			
	c) 適合性の監査においては、以下の項目を対象に含む。 ・関連する法令又は規制の要求事項 ・情報セキュリティリスクアセスメントなどによって特定された情報セキュリティ要　求事項 d) 情報セキュリティマネジメントが有効に実施され、維持されていることの監査においては、以下の項目を対象に含む。 ・管理策の有効性及び維持 ・管理策が期待通りに実施されていること。			
4.6.2.3	組織は、頻度、方法、責任及び計画に関する要求事項及び報告を含む、監査プログラムの計画、確立、実施及び維持する。 [27001-9.2c)] 監査プログラムでは、関連するプロセスの重要性及び前回までの監査の結果を考慮する。 監査は一度にすべての適用範囲について実施するだけではなく、範囲の一部のみを対象とする場合もあり、毎回の監査の目的を明確にし、適切な監査計画を実施することが重要であることから、監査プログラムの作成においては、以下の点を考慮する。 ・監査の目的と重点目標 ・対象となる監査プロセスの状況と重要性 ・対象となる領域の状況と重要性 ・前回までの監査結果			
4.6.2.4	組織は、監査基準及び監査範囲を明確にする。[27001-9.2d)] 監査プログラムでは全体的な監査の日程だけではなく、以下の内容について含める。 ・監査の基準（以下の内容も含む。） －目的、権限と責任 －独立性、客観性と職業倫理 －専門能力 －業務上の義務 －品質管理 －監査の実施方法 －監査報告書の形式 ・監査の範囲 ・監査の頻度又は時期 ・監査の方法（個別の情報セキュリティ監査基準を作成し、内部監査、外部組織による監査のいずれにおいても、品質の高い監査を実施できるように準備を整える。）			
4.6.2.5	組織は、監査プロセスの客観性及び公平性を確実にする監査員の選定及び監査の実施を行う。 [27001-9.2e)] 監査人の選定においては監査基準に従い、以下の点を考慮する。 ・外観上の独立性 ・精神上の独立性 ・職業倫理と誠実性 なお、内部の監査員の場合は、自らが従事している業務については自身で監査しないように、他の担当者を割り当てる。			
4.6.2.6	組織は、監査の結果を関連する管理層に報告することを確実にする。 [27001-9.2f)]			
4.6.2.7	組織は、監査プログラム及び監査結果の証拠として、文書化した情報を保持する。 [27001-9.2g)] 監査手順に以下の内容を反映させるとともに、文書化し、お互いのコミュニケーションのために活用する。 ・監査の計画・実施に関する責任及び要求事項 ・結果報告・記録維持に関する責任と要求事項 要求事項については監査品質を確保するための必須条件であり、責任者と監査人が同じ目的をもって監査を実施する。			
4.6.3	マネジメントレビュー [27001-9.3]			

	マネジメント基準	適合状況	採用しているセキュリティ対策概要	非採用理由
4.6.3.1	トップマネジメントは、あらかじめ定めた間隔で、マネジメントレビューする。 [27001-9.3] あらかじめ定められた間隔でマネジメントレビューを実施するために、以下の点について考慮するとともに、文書化する。 ・マネジメントレビュー基本計画 ・マネジメントレビュー実施計画 ・マネジメントレビューのための実施報告 基本計画書では目的及び実施時期について、実施計画では詳細な監査の手法についてあらかじめ決める。			
4.6.3.2	トップマネジメントは、マネジメントレビューにおいて、以下を考慮する。 [27001-9.3] ・前回までのマネジメントレビューの結果とった処置の状況 ・情報セキュリティマネジメントに関連する外部及び内部の課題の変化 ・以下に示す内容を含めた、情報セキュリティパフォーマンスに関するフィードバック -不適合及び是正処置 -監視及び測定の結果 -監査結果 -情報セキュリティ目的の達成 ・利害関係者からのフィードバック ・情報セキュリティリスクアセスメントの結果及び情報セキュリティリスク対応計画の状況 ・継続的改善の機会 また、これらの情報を構成することが予想される活動及び事象を記録し、必要に応じて報告するとともに、緊急性が高いものについてはあらかじめ定義しておき、誰もが同じ判断をできるように基準を定める。			
4.6.3.3	マネジメントレビューからのアウトプットには、継続的改善の機会及び情報セキュリティマネジメントのあらゆる変更の必要性に関する決定を含める。 [27001-9.3] マネジメントレビューの結果を改善策に反映するために、以下の活動を実施し、改善策を検討する。 ・情報セキュリティマネジメントの有効性の改善 ・情報セキュリティリスクアセスメント及び情報セキュリティリスク対応計画の更新 ・情報セキュリティマネジメントに影響を与える可能性のある内外の事象を考慮の上での手順及び管理策の修正 ・必要となる経営資源の特定 ・パフォーマンス測定方法の改善 なお、改善策の立案においては、情報セキュリティリスク対応の選択肢を選択した際の記録を参考にする。			
4.6.3.4	組織は、マネジメントレビューの結果の証拠として文書化した情報を保持する。 [27001-9.3] マネジメントレビューの結果は次回のマネジメントレビューに活用されるため、実施内容と結果が分かるように具体的に記録する。			
4.7	情報セキュリティマネジメントの維持及び改善 [27001-10]			
4.7.1	是正処置 [27001-10.1]			
4.7.1.1	組織は、不適合が発生した場合、不適合の是正のための処置を取る。 [27001-10.1a)] a) 是正措置 を取る際は、以下を実施する。 ・その不適合を管理し、是正するための処置 ・その不適合によって起こった結果への対処 ・是正処置を手順どおりに実施するために、以下について文書化する。 －不適合の再発防止を確実にするために選択した処置の必要性の評価 －必要な是正処置の決定 －必要な是正処置の実施 －実施した処置の記録 －実施した是正処置のレビュー			
	b) 不適合は以下の活動によって検出される。 ・定期的な情報セキュリティリスクアセスメント ・定期的な情報セキュリティ内部監査 ・定期的なマネジメントレビュー ・不適合を手順どおりに検出するために、以下について文書化する。 －情報セキュリティマネジメントに対する不適合の特定 －情報セキュリティマネジメントに対する不適合の原因の決定 なお、単一の活動だけでは判断できない場合もあるので、複合的な結果の考察から不適合を検出する。			
4.7.1.2	組織は、不適合が再発又は他のところで発生しないようにするため、その不適合の原因を除去するための処置をとる必要性を評価する。 [27001-10.1b)] 必要性を評価する際は、以下を実施する。 ・その不適合のレビュー ・その不適合の原因の明確化 ・類似の不適合の有無、又はそれが発生する可能性の明確化			
4.7.1.3	組織は、必要な処置を実施する。 [27001-10.1c)]			
4.7.1.4	組織は、とった全ての是正処置の有効性をレビューする。 [27001-10.1d)]			
4.7.1.5	組織は、必要な場合には、情報セキュリティマネジメントの変更を行う。 [27001-10.1e)]			
4.7.1.6	組織は、是正処置は、検出された不適合のもつ影響に応じたものとする。 [27001-10.1]			
4.7.1.7	組織は、是正処置の証跡として、以下の文書化した情報を保持する。 [27001-10.1f) / 10.1g)] ・不適合の性質及びとった処置 ・是正処置の結果			
4.8	文書化した情報の管理 [27001-7.5]			
4.8.1	文書化の指針 [27001-7.5.1]			
4.8.1.1	組織は、情報セキュリティマネジメントが必要とする以下の情報を文書化する。 [27001-7.5.1] ・情報セキュリティ方針 ・情報セキュリティ目的 ・情報セキュリティリスクアセスメントのプロセス ・情報セキュリティリスク対応のプロセス ・情報セキュリティリスクアセスメントの結果 ・情報セキュリティリスク対応計画 ・パフォーマンス測定の結果 これらの内容についてはどの文書に記載されていてもかまわないが、その内容を知る必要がある担当者には必ず伝わるように構成するとともに、知る必要性のない者が閲覧できないことを確実にする。			
4.8.2	文書の作成・変更及び管理 [27001-7.5.2 / 7.5.3]			
4.8.2.1	組織は、以下を行うことによって、文書化した情報を作成及び更新する。 [27001-7.5.2] ・適切な識別情報の記述（例えば、表題、日付、作成者、参照番号） ・適切な形式（例えば、言語、ソフトウェアの版、図表）及び媒体（例えば、紙、電子媒体）の選択 ・適切性及び妥当性に関する、適切なレビュー及び承認 ・文書化した情報のライフサイクルの定義や、それに応じた処理ができるような手順の策定 ・文書を発行する前における、適正性のレビュー及び承認 ・必要に応じた、文書の更新及び再承認 ・廃止文書の誤使用の防止 ・廃止文書を何らかの目的で保持する場合における、廃止文書であることが分かる適切な識別情報の記述 ・法的及び規制の要求事項及び環境の変化に従い、定めた頻度での更新 また、これらのすべての活動が文書管理に反映されているか、またその活動が業務に大きな障害を与えていないかなどを考慮し、適切な文書管理手順を策定する。			
4.8.2.2	組織は、以下のことを確実にするために、情報セキュリティマネジメントで要求された文書化した情報を、管理する。 [27001-7.5.3] ・文書化した情報が、必要なときに、必要なところで、入手可能かつ利用に適した状態であること。 ・文書化した情報が十分に保護されていること（例えば、機密性の喪失、不適切な使用及び完全性の喪失からの保護）。 ・文書化した情報の配付、アクセス 、検索及び利用 ・文書化した情報の読みやすさが保たれることを含む、保管及び保存 ・文書化した情報の変更の管理（例えば、版の管理） ・文書化した情報の保持及び廃棄 また、情報セキュリティマネジメントの計画及び運用のために組織が必要と決定した文書は、外部から入手したものであっても、必要に応じて、特定し、管理する。			
4.9	情報セキュリティリスクコミュニケーション			
	利害関係者間の有効なコミュニケーションは、意思決定に大きな影響を与えることがある。情報セキュリティリスクコミュニケーションは、意思決定者とその他の利害関係者（クラウドサービス利用者及びクラウドサービスの提供にかかわる委託先を含む。）との間で情報セキュリティリスクに関する情報を交換、共有し、リスクを管理する方法に関する合意を得る。			
4.9.1	リスクコミュニケーションの計画			
4.9.1.1	リスクコミュニケーション計画を策定する。 リスクコミュニケーション計画は、以下の２つに分けて策定し、文書化する。 ・通常運用のためのリスクコミュニケーション計画 ・緊急事態のためのリスクコミュニケーション計画 リスクコミュニケーション計画は、意思決定者とその他の利害関係者（クラウドサービス利用者及びクラウドサービスの提供にかかわる委託先を含む。）との間でどのようにコミュニケーションを図るかに留意し、以下の内容について含める。 ・適切な利害関係者の参画による、効果的な情報交換／共有 ・法令、規制及び ガバナンスの要求事項の順守 ・コミュニケーション及び協議に関するフィードバック及び報告の提供 ・組織に対する信頼を醸成するためのコミュニケーションの活用 ・危機又は不測の事態発生時の利害関係者とのコミュニケーションの実施			
4.9.2	リスクコミュニケーションの実施			
4.9.2.1	リスクコミュニケーションを実施する仕組みを確定する。 リスクに関する論議、その優先順位の決定及び適切なリスク対応、並びにリスク受容を行い、主要な意思決定者と利害関係者（クラウドサービス利用者及びクラウドサービスの提供にかかわる委託先を含む。）の協調を得る仕組みを確定する。この仕組みでは次の事項を確実にする。 ・リスクマネジメントの枠組みの主要な構成要素、及びその後に行うあらゆる修正の適切な伝達 ・枠組み、その有効性及び成果に関する適切な内部報告 ・適切な階層及び時期に利用可能な、リスクマネジメントの適応から導出される関連情報の提供 ・内部の利害関係者との協議のためのプロセス 仕組みには、適切な場合には、多様な情報源からのリスク情報について、まとめ上げるプロセスが含まれ、また、リスク情報の影響の受けやすさを考慮する必要がある場合もある。なお、この仕組みを設ける場として、委員会がある。			

マネジメント基準		適合状況	採用しているセキュリティ対策概要	非採用理由
4.9.2.2	リスクコミュニケーションを実施する。 リスクコミュニケーションは、次の点を達成するために、リスクマネジメントプロセスのすべての段階で継続的に実施する。 ・組織のリスクマネジメント結果の保証を提供する ・リスク情報を収集する ・リスクアセスメントの結果を共有しリスク対応計画を提示する ・意思決定者と利害関係者（クラウドサービス利用者及びクラウドサービスの提供にかかわる委託先を含む。）の相互理解の欠如による情報セキュリティ違反の発生及び結果を回避又は低減する ・意思決定を支援する ・新しい情報セキュリティ知識を入手する ・他の組織と協調しすべてのインシデントの結果を低減するための対応計画を立案する ・意思決定者及び利害関係者（クラウドサービス利用者及びクラウドサービスの提供にかかわる委託先を含む。）にリスクについての責任を意識させる ・セキュリティ意識を改善する リスクコミュニケーションの実施においては、組織内の適切な広報又はコミュニケーション部門と協力し、リスクコミュニケーション関連の全タスクを調整して行う。			

管理策基準		適合状況	採用しているセキュリティ対策概要	非採用理由
5	情報セキュリティのための方針群			
5.1	情報セキュリティのための経営陣の方向性 管理目的：情報セキュリティのための経営陣の方向性及び支持を、事業上の要求事項並びに関連する法令及び規制に従って提示するため。			
5.1.1	情報セキュリティのための方針群は、これを定義し、管理層が承認し、発行し、従業員及び関連する外部関係者に通知する。 (脚注）管理層には、経営陣及び管理者が含まれる。ただし、実務管理者（administrator）は除かれる。			
5.1.2	情報セキュリティのための方針群は、あらかじめ定めた間隔で、又は重大な変化が発生した場合に、それが引き続き適切、妥当かつ有効であることを確実にするためにレビューする。			
6	情報セキュリティのための組織			
6.1	内部組織 管理目的：組織内で情報セキュリティの実施及び運用に着手し、これを統制するための管理上の枠組みを確立するため。			
6.1.1	全ての情報セキュリティの責任を定め、割り当てる。			
6.1.1.13.PB	クラウドサービス事業者は、クラウドサービス利用者、クラウドサービス事業者及び供給者と、情報セキュリティの役割及び責任の適切な割当てについて合意し、文書化する。			
6.1.2	相反する職務及び責任範囲は、組織の資産に対する、認可されていない若しくは意図しない変更又は不正使用の危険性を低減するために、分離する。			
6.1.3	関係当局との適切な連絡体制を維持する。			
6.1.3.3.PB	クラウドサービス事業者は、クラウドサービス利用者に、クラウドサービス事業者の組織の地理的所在地、及びクラウドサービス事業者がクラウドサービス利用者のデータを保管する可能性のある国々及びその法管轄を通知する。			
6.1.4	情報セキュリティに関する研究会又は会議、及び情報セキュリティの専門家による協会・団体との適切な連絡体制を維持する。			
6.1.5	プロジェクトの種類にかかわらず、プロジェクトマネジメントにおいては、情報セキュリティに取り組む。			
6.2	モバイル機器及びテレワーキング 管理目的：モバイル機器の利用及びテレワーキングに関するセキュリティを確実にするため。			
6.2.1	モバイル機器を用いることによって生じるリスクを管理するために、方針及びその方針を支援するセキュリティ対策を採用する。			
6.2.2	テレワーキングの場所でアクセス、処理及び保存される情報を保護するために、方針及びその方針を支援するセキュリティ対策を実施する。			
6.3.P	クラウドサービス利用者及びクラウドサービス事業者の関係 管理目的：情報セキュリティマネジメントのための、クラウドサービス利用者及びクラウドサービス提供者間の共同責任の関係を説明するため。			
6.3.1.P	クラウドサービス利用者及びクラウドサービス事業者の両者は、クラウドサービスの利用における情報セキュリティの共同責任について、文書化し、公表し、伝達し、実装する。			
6.3.1.1.PB	クラウドサービス事業者は、クラウドサービス利用の一環としてクラウドサービス利用者が実施及び管理を必要とする情報セキュリティの役割と責任に加え、クラウドサービスの利用に対する、クラウドサービス事業者の情報セキュリティ管理策及び責任を文書化し、通知する。			
7	人的資源のセキュリティ			
7.1	雇用前 管理目的：従業員及び契約相手がその責任を理解し、求められている役割にふさわしいことを確実にするため。			
7.1.1	全ての従業員候補者についての経歴などの確認は、関連する法令、規制及び倫理に従って行う。また、この確認は、事業上の要求事項、アクセスされる情報の分類及び認識されたリスクに応じて行う。			
7.1.2	従業員及び契約相手との雇用契約書には、情報セキュリティに関する各自の責任及び組織の責任を記載する。			
7.2	雇用期間中 管理目的：従業員及び契約相手が、情報セキュリティの責任を認識し、かつ、その責任を遂行することを確実にするため。			
7.2.1	経営陣は、組織の確立された方針及び手順に従った情報セキュリティの適用を、全ての従業員及び契約相手に要求する。			
7.2.2	組織の全ての従業員、及び関係する場合には契約相手は、職務に関連する組織の方針及び手順についての、適切な、意識向上のための教育及び訓練を受け、また、定めに従ってその更新を受ける。			
7.2.2.19.PB	クラウドサービス事業者は、クラウドサービス利用者のデータ及びクラウドサービスの派生データの適切な取扱いに関して、従業員に意識向上のための教育及び訓練を提供し、かつ同じことをするよう契約相手に要請する。			
7.2.3	情報セキュリティ違反を犯した従業員に対して処置をとるための、正式かつ周知された懲戒手続を備える。			
7.3	雇用の終了及び変更 管理目的：雇用の終了又は変更のプロセスの一部として、組織の利益を保護するため。			
7.3.1	雇用の終了又は変更の後もなお有効な情報セキュリティに関する責任及び義務を定め、その従業員又は契約相手に伝達し、かつ、遂行させる。			
8	資産の管理			
8.1	資産に対する責任 管理目的：組織の資産を特定し、適切な保護の責任を定めるため。			
8.1.1	情報、情報に関連するその他の資産及び情報処理施設を特定する。また、これらの資産の目録を、作成し、維持する。			
8.1.1.6.PB	クラウドサービス事業者の資産目録は、クラウドサービス利用者のデータ及びクラウドサービスの派生データを明確に特定する。			
8.1.2	目録の中で維持される資産は、管理する。			
8.1.2.7.PB	クラウドサービス事業者は、クラウドサービス利用者に対し、当該利用者の資産（バックアップを含む）を管理するため、次のいずれかを提供する。 (a)当該利用者の管理する資産を、記録媒体に記録する（バックアップを含む）前に暗号化し、当該利用者が暗号鍵を管理し消去する機能 (b) 当該利用者が、当該利用者の管理する資産を記録媒体に記録する（バックアップを含む）前に暗号化し、暗号鍵を管理し消去する機能を実装するために必要となる情報			
8.1.3	情報の利用の許容範囲、並びに情報及び情報処理施設と関連する資産の利用の許容範囲に関する規則は、明確にし、文書化し、実施する。			
8.1.4	全ての従業員及び外部の利用者は、雇用、契約又は合意の終了時に、自らが所持する組織の資産の全てを返却する。			
8.1.5.P	クラウドサービス事業者の領域上にあるクラウドサービス利用者の資産は、クラウドサービス利用の合意の終了時に、時機を失せずに返却または除去する。			
8.2	情報分類 管理目的：組織に対する情報の重要性に応じて、情報の適切なレベルでの保護を確実にするため。			
8.2.1	情報は、法的要求事項、価値、重要性、及び認可されていない開示又は変更に対して取扱いに慎重を要する度合いの観点から、分類する。			
8.2.2	情報のラベル付けに関する適切な一連の手順は、組織が採用した情報分類体系に従って策定し、実施する。			
8.2.2.7.PB	クラウドサービス事業者は、クラウドサービス利用者が扱う情報及び関連資産を当該利用者が分類し、ラベル付けするためのサービス機能について文書化し、開示する。			
8.2.3	資産の取扱いに関する手順は、組織が採用した情報分類体系に従って策定し、実施する。			
8.3	媒体の取扱い 管理目的：媒体に保存された情報の認可されていない開示、変更、除去又は破壊を防止するため。			
8.3.1	組織が採用した分類体系に従って、取外し可能な媒体の管理のための手順を実施する。			
8.3.2	媒体が不要になった場合は、正式な手順を用いて、セキュリティを保って処分する。			
8.3.3	情報を格納した媒体は、輸送の途中における、認可されていないアクセス、不正使用又は破損から保護する。			
9	アクセス制御			
9.1	アクセス制御に対する業務上の要求事項 管理目的：情報及び情報処理施設へのアクセスを制限するため。			
9.1.1	アクセス制御方針は、業務及び情報セキュリティの要求事項に基づいて確立し、文書化し、レビューする。			
9.1.2	利用することを特別に認可したネットワーク及びネットワークサービスへのアクセスだけを、利用者に提供する。			

管理策基準		適合状況	採用しているセキュリティ対策概要	非採用理由
9.2	利用者アクセスの管理 管理目的：システム及びサービスへの、認可された利用者のアクセスを確実にし、認可されていないアクセスを防止するため。			
9.2.1	アクセス権の割当てを可能にするために、利用者の登録及び登録削除についての正式なプロセスを実施する。			
9.2.1.6.PB	クラウドサービスのユーザによるクラウドサービスへのアクセスをクラウドサービス利用者が管理するため、クラウドサービス事業者は、クラウドサービス利用者に、ユーザの登録及び登録削除の機能及び仕様を提供する。			
9.2.2	全ての種類の利用者について、全てのシステム及びサービスへのアクセス権を割り当てる又は無効化するために、利用者アクセスの提供についての正式なプロセスを実施する。			
9.2.2.8.PB	クラウドサービス事業者は、クラウドサービスのユーザのアクセス権を管理する機能及び仕様を提供する。			
9.2.3	特権的アクセス権の割当て及び利用は、制限し、管理する。			
9.2.3.11.PB	クラウドサービス事業者は、特定したリスクに応じて、クラウドサービスの管理能力にあわせたクラウドサービス利用者の管理者認証に、十分に強固な認証技術を提供する。			
9.2.4	秘密認証情報の割当ては、正式な管理プロセスによって管理する。			
9.2.4.9.PB	クラウドサービス事業者は、秘密認証情報を割り当てる手順、及びユーザ認証手順を含む、クラウドサービス利用者の秘密認証情報の管理手順について、情報を提供する。			
9.2.5	資産の管理責任者は、利用者のアクセス権を定められた間隔でレビューする。			
9.2.6	全ての従業員及び外部の利用者の情報及び情報処理施設に対するアクセス権は、雇用、契約又は合意の終了時に削除し、また、変更に合わせて修正する。			
9.3	利用者の責任 管理目的：利用者に対して、自らの秘密認証情報を保護する責任をもたせるため。			
9.3.1	秘密認証情報の利用時に、組織の慣行に従うことを、利用者に要求する。			
9.4	システム及びアプリケーションのアクセス制御 管理目的：システム及びアプリケーションへの、認可されていないアクセスを防止するため。			
9.4.1	情報及びアプリケーションシステム機能へのアクセスは、アクセス制御方針に従って、制限する。			
9.4.1.8.PB	クラウドサービス事業者は、クラウドサービスへのアクセス、クラウドサービス機能へのアクセス、及びサービスにて保持されるクラウドサービス利用者のデータへのアクセスを、クラウドサービス利用者が制限できるよう、アクセス制御を提供する。			
9.4.2	アクセス制御方針で求められている場合には、システム及びアプリケーションへのアクセスは、セキュリティに配慮したログオン手順によって制御する。			
9.4.2.2.B	強い認証及び識別情報の検証が必要な場合には、パスワードに代えて、暗号による手段、スマートカード、トークン、生体認証などの認証方法を用いる。			
9.4.3	パスワード管理システムは、対話式とすること、また、良質なパスワードを確実にするものとする。			
9.4.4	システム及びアプリケーションによる制御を無効にすることのできるユーティリティプログラムの使用は、制限し、厳しく管理する。			
9.4.5	プログラムソースコードへのアクセスは、制限する。			
9.5.P	共有化された仮想環境におけるクラウドサービス利用者のデータのアクセス制御 管理目的：共有化されたクラウドコンピューティング上の仮想環境における情報セキュリティを確実にするため。			
9.5.1.P	クラウドサービス利用者のクラウドサービス上の仮想環境は、他のクラウドサービス利用者及び認可されていない者から保護する。			
9.5.2.P	クラウドコンピューティング環境における仮想マシンは、事業上のニーズを満たすため、要塞化する。			
9.5.2.1.PB	クラウドサービス事業者は、仮想マシンを設定する際には、適切に要塞化し(例えば、クラウドサービスを実行するのに必要なポート、プロトコル及びサービスのみを有効とする）、利用する各仮想マシンに適切な技術的管理策(例えば、マルウェア対策、ログ取得）を実施する。			
10	暗号			
10.1	暗号による管理策 管理目的：情報の機密性、真正性及び／又は完全性を保護するために、暗号の適切かつ有効な利用を確実にするため。			
10.1.1	情報を保護するための暗号による管理策の利用に関する方針は、策定し、実施する。			
10.1.1.9.PB	クラウドサービス事業者は、クラウドサービス利用者に、当該利用者が処理する情報を保護するために暗号技術を利用する機能を提供し、または、暗号技術を利用する環境についての情報を提供する。			
10.1.2	暗号鍵の利用、保護及び有効期間（lifetime）に関する方針を策定し、そのライフサイクル全体にわたって実施する。			
10.1.2.20.PB	クラウドサービス事業者は、クラウドサービス利用者に、当該利用者の管理する情報の暗号化に用いる暗号鍵を当該利用者が管理する機能を提供し、または、当該利用者が暗号鍵を管理する方法についての情報を提供する。			
11	物理的及び環境的セキュリティ			
11.1	セキュリティを保つべき領域 管理目的：組織の情報及び情報処理施設に対する認可されていない物理的アクセス、損傷及び妨害を防止するため。			
11.1.1	取扱いに慎重を要する又は重要な情報及び情報処理施設のある領域を保護するために、物理的セキュリティ境界を定め、かつ、用いる。			
11.1.2	セキュリティを保つべき領域は、認可された者だけにアクセスを許すことを確実にするために、適切な入退管理策によって保護する。			
11.1.3	オフィス、部屋及び施設に対する物理的セキュリティを設計し、適用する。			
11.1.4	自然災害、悪意のある攻撃又は事故に対する物理的な保護を設計し、適用する。			
11.1.5	セキュリティを保つべき領域での作業に関する手順を設計し、適用する。			
11.1.6	荷物の受渡場所などの立寄り場所、及び認可されていない者が施設に立ち入ることもあるその他の場所は、管理する。また、認可されていないアクセスを避けるために、それらの場所を情報処理施設から離す。			
11.2	装置 管理目的：資産の損失、損傷、盗難又は劣化、及び組織の業務に対する妨害を防止するため。			
11.2.1	装置は、環境上の脅威及び災害からのリスク並びに認可されていないアクセスの機会を低減するように設置し、保護する。			
11.2.2	装置は、サポートユーティリティの不具合による、停電、その他の故障から保護する。			
11.2.3	データを伝送する又は情報サービスをサポートする通信ケーブル及び電源ケーブルの配線は、傍受、妨害又は損傷から保護する。			
11.2.4	装置は、可用性及び完全性を継続的に維持することを確実にするために、正しく保守する。			
11.2.5	装置、情報又はソフトウェアは、事前の認可なしでは、構外に持ち出さない。			
11.2.6	構外にある資産に対しては、構外での作業に伴った、構内での作業とは異なるリスクを考慮に入れて、セキュリティを適用する。			
11.2.7	記憶媒体を内蔵した全ての装置は、処分又は再利用する前に、全ての取扱いに慎重を要するデータ及びライセンス供与されたソフトウェアを消去していること、又はセキュリティを保って上書きしていることを確実にするために、検証する。			
11.2.7.4.PB	クラウドサービス事業者は、資源（例えば、装置、データストレージ、ファイル、メモリ）のセキュリティを保った処分又は再利用の取り決めを、時期を失せずに行うことを確実にする仕組みを整備する。			
11.2.8	利用者は、無人状態にある装置が適切な保護対策を備えていることを確実にする仕組みを整備する。			
11.2.9	書類及び取外し可能な記憶媒体に対するクリアデスク方針、並びに情報処理設備に対するクリアスクリーン方針を適用する。 （脚注）クリアデスクとは、机上に書類を放置しないことをいう。また、クリアスクリーンとは、情報をスクリーンに残したまま離席しないことをいう。			
12	運用のセキュリティ			
12.1	運用の手順及び責任 管理目的：情報処理設備の正確かつセキュリティを保った運用を確実にするため。			
12.1.1	操作手順は、文書化し、必要とする全ての利用者に対して利用可能とする。			
12.1.2	情報セキュリティに影響を与える、組織、業務プロセス、情報処理設備及びシステムの変更は、管理する。			
12.1.2.11.PB	クラウドサービス事業者は、クラウドサービス利用者の情報セキュリティに悪影響を及ぼす可能性のあるクラウドサービスの変更に関する情報を、クラウドサービス利用者に提供する。			
12.1.3	要求された主要なシステム資源の使用を満たすことを確実にするために、資源の利用を監視・調整し、また、将来必要とする容量・能力を予測する。			
12.1.3.9.PB	クラウドサービス事業者は、資源不足による情報セキュリティインシデントを防ぐため、全資源の容量を監視する。			
12.1.4	開発環境、試験環境及び運用環境は、運用環境への認可されていないアクセス又は変更によるリスクを低減するために、分離する。			
12.1.5.P	クラウドコンピューティング環境の、管理のための操作手順を定義し、文書化し、監視する。			

管理策基準		適合状況	採用しているセキュリティ対策概要	非採用理由
12.1.5.1.PB	クラウドサービス事業者は、重要な操作及び手順に関する文書を、それを求めるクラウドサービス利用者に提供する。			
12.2	マルウェアからの保護 管理目的：情報及び情報処理施設がマルウェアから保護されることを確実にするため。			
12.2.1	マルウェアから保護するために、利用者に適切に認識させることと併せて、検出、予防及び回復のための管理策を実施する。			
12.3	バックアップ 管理目的：データの消失から保護するため。			
12.3.1	情報、ソフトウェア及びシステムイメージのバックアップは、合意されたバックアップ方針に従って定期的に取得し、検査する。			
12.4	ログ取得及び監視 管理目的：イベントを記録し、証拠を作成するため。			
12.4.1	利用者の活動、例外処理、過失及び情報セキュリティ事象を記録したイベントログを取得し、保持し、定期的にレビューする。			
12.4.1.15.PB	クラウドサービス事業者は、クラウドサービス利用者に、ログ取得機能を提供する。			
12.4.2	ログ機能及びログ情報は、改ざん及び認可されていないアクセスから保護する。			
12.4.3	システムの実務管理者及び運用担当者の作業は、記録し、そのログを保護し、定期的にレビューする。			
12.4.4	組織又はセキュリティ領域内の関連する全ての情報処理システムのクロックは、単一の参照時刻源と同期させる。			
12.4.4.4.PB	クラウドサービス事業者は、クラウドサービス利用者に、クラウドサービス事業者のシステムで利用するクロックに関する情報及びクラウドサービス利用者がクラウドサービスのクロックにローカルクロックを同期させる方法についての情報を提供する。			
12.4.5.P	クラウドサービス利用者は、利用するクラウドサービスの操作を監視する機能を有する。			
12.5	運用ソフトウェアの管理 管理目的：運用システムの完全性を確実にするため。			
12.5.1	運用システムに関わるソフトウェアの導入を管理するための手順を実施する。			
12.6	技術的ぜい弱性管理 管理目的：技術的ぜい弱性の悪用を防止するため。			
12.6.1	利用中の情報システムの技術的ぜい弱性に関する情報は、時機を失せずに獲得する。また、そのようなぜい弱性に組織がさらされている状況を評価する。さらに、それらと関連するリスクに対処するために、適切な手段をとる。			
12.6.1.18.PB	クラウドサービス事業者は、提供するクラウドサービスに影響を及ぼす可能性のある技術的ぜい弱性の管理についての情報を、クラウドサービス利用者が利用可能となるようにする。			
12.6.2	利用者によるソフトウェアのインストールを管理する規則を確立し、実施する。			
12.7	情報システムの監査に対する考慮事項 管理目的：運用システムに対する監査活動の影響を最小限にするため。			
12.7.1	運用システムの検証を伴う監査要求事項及び監査活動は、業務プロセスの中断を最小限に抑えるために、慎重に計画し、合意する。			
13	通信のセキュリティ			
13.1	ネットワークセキュリティ管理 管理目的：ネットワークにおける情報の保護、及びネットワークを支える情報処理施設の保護を確実にするため。			
13.1.1	システム及びアプリケーション内の情報を保護するために、ネットワークを管理し、制御する。			
13.1.2	組織が自ら提供するか外部委託しているかを問わず、全てのネットワークサービスについて、セキュリティ機能、サービスレベル及び管理上の要求事項を特定し、また、ネットワークサービス合意書にもこれらを盛り込む。			
13.1.3	情報サービス、利用者及び情報システムは、ネットワーク上で、グループごとに分離する。			
13.1.4.P	仮想ネットワークを設定する際には、クラウドサービス事業者のネットワークセキュリティ方針に基づき、仮想ネットワークと物理ネットワークの設定の整合性を検証する。			
13.2	情報の転送 管理目的：組織の内部及び外部に転送した情報のセキュリティを維持するため。			
13.2.1	あらゆる形式の通信設備を利用した情報転送を保護するために、正式な転送方針、手順及び管理策を備える。			
13.2.2	合意では、組織と外部関係者との間の業務情報のセキュリティを保った転送について、取り扱う。			
13.2.3	電子的メッセージ通信に含まれた情報は、適切に保護する。			
13.2.4	情報保護に対する組織の要件を反映する秘密保持契約又は守秘義務契約のための要求事項は、特定し、定めに従ってレビューし、文書化する。			
14	システムの取得、開発及び保守			
14.1	情報システムのセキュリティ要求事項 管理目的：ライフサイクル全体にわたって、情報セキュリティが情報システムに欠くことのできない部分であることを確実にするため。これには、公衆ネットワークを介してサービスを提供する情報システムのための要求事項も含む。			
14.1.1	情報セキュリティに関連する要求事項は、新しい情報システム又は既存の情報システムの改善に関する要求事項に含める。			
14.1.2	公衆ネットワークを経由するアプリケーションサービスに含まれる情報は、不正行為、契約紛争、並びに認可されていない開示及び変更から保護する。			
14.1.3	アプリケーションサービスのトランザクションに含まれる情報は、次の事項を未然に防止するために、保護する。 ・不完全な通信 ・誤った通信経路設定 ・認可されていないメッセージの変更 ・認可されていない開示 ・認可されていないメッセージの複製又は再生			
14.2	開発及びサポートプロセスにおけるセキュリティ 管理目的：情報システムの開発サイクルの中で情報セキュリティを設計し、実施することを確実にするため。			
14.2.1	ソフトウェア及びシステムの開発のための規則は、組織内において確立し、開発に対して適用する。			
14.2.1.13.PB	クラウドサービス事業者は、開示方針に反しない範囲で、セキュリティを保つための開発手順及び慣行についての情報を提供する。			
14.2.2	開発のライフサイクルにおけるシステムの変更は、正式な変更管理手順を用いて管理する。			
14.2.3	オペレーティングプラットフォームを変更するときは、組織の運用又はセキュリティに悪影響がないことを確実にするために、重要なアプリケーションをレビューし、試験する。			
14.2.4	パッケージソフトウェアの変更は、抑止し、必要な変更だけに限る。また、全ての変更は、厳重に管理する。			
14.2.5	セキュリティに配慮したシステムを構築するための原則を確立し、文書化し、維持し、全ての情報システムの実装に対して適用する。			
14.2.6	組織は、全てのシステム開発ライフサイクルを含む、システムの開発及び統合の取組みのためのセキュリティに配慮した開発環境を確立し、適切に保護する。			
14.2.7	組織は、外部委託したシステム開発活動を監督し、監視する。			
14.2.8	セキュリティ機能（functionality）の試験は、開発期間中に実施する。			
14.2.9	新しい情報システム、及びその改訂版・更新版のために、受入れ試験のプログラム及び関連する基準を確立する。			
14.3	試験データ 管理目的：試験に用いるデータの保護を確実にするため。			
14.3.1	試験データは、注意深く選定し、保護し、管理する。			
15	供給者関係			
15.1	供給者関係における情報セキュリティ 管理目的：供給者がアクセスできる組織の資産の保護を確実にするため。			
15.1.1	組織の資産に対する供給者のアクセスに関連するリスクを軽減するための情報セキュリティ要求事項について、供給者と合意し、文書化する。			
15.1.1.14.B	組織が実施する、並びに組織が供給者に対して実施を要求するプロセス及び手順には、情報、情報処理施設及び移動が必要なその他のものの移行の管理、並びにその移行期間全体にわたって情報セキュリティが維持されることの確実化を含める。			

管理策基準		適合状況	採用しているセキュリティ対策概要	非採用理由
15.1.1.16.B	当該事業者が提供するサービス上で取り扱われる情報に対して国内法以外の法令及び規制が適用された結果、クラウドサービス利用者の意図しないまま当該利用者の管理する情報にアクセスされ、又は処理されるリスクを評価して外部委託先を選定し、必要に応じてクラウドサービス利用者が扱う情報が取り扱われる場所及び契約に定める準拠法・裁判管轄を指定する。			
15.1.2	関連する全ての情報セキュリティ要求事項を確立し、組織の情報に対して、アクセス、処理、保存若しくは通信を行う、又は組織の情報のためのIT 基盤を提供する可能性のあるそれぞれの供給者と、この要求事項について合意する。			
15.1.2.18.PB	クラウドサービス事業者は、クラウドサービス事業者とクラウドサービス利用者の間に誤解が生じないように、クラウドサービス事業者が実行する適切な情報セキュリティ対策を、合意の一環として定める。			
15.1.3	供給者との合意には、情報通信技術（以下「ICT」という。）サービス及び製品のサプライチェーンに関連する情報セキュリティリスクに対処するための要求事項を含める。			
15.2	供給者のサービス提供の管理 管理目的：供給者との合意に沿って、情報セキュリティ及びサービス提供について合意したレベルを維持するため。			
15.2.1	組織は、供給者のサービス提供を定常的に監視し、レビューし、監査する。			
15.2.2	関連する業務情報、業務システム及び業務プロセスの重要性、並びにリスクの再評価を考慮して、供給者によるサービス提供の変更（現行の情報セキュリティの方針群、手順及び管理策の保守及び改善を含む）を管理する。			
16	情報セキュリティインシデント管理			
16.1	情報セキュリティインシデントの管理及びその改善 管理目的：セキュリティ事象及びセキュリティ弱点に関する伝達を含む、情報セキュリティインシデントの管理のための、一貫性のある効果的な取組みを確実にするため。			
16.1.1	情報セキュリティインシデントに対する迅速、効果的かつ順序だった対応を確実にするために、管理層の責任及び手順を確立する。			
16.1.2	情報セキュリティ事象は、適切な管理者への連絡経路を通して、できるだけ速やかに報告する。			
16.1.3	組織の情報システム及びサービスを利用する従業員及び契約相手に、システム又はサービスの中で発見した又は疑いをもった情報セキュリティ弱点は、どのようなものでも記録し、報告するように要求する。			
16.1.4	情報セキュリティ事象は、これを評価し、情報セキュリティインシデントに分類するか否かを決定する。			
16.1.5	情報セキュリティインシデントは、文書化した手順に従って対応する。			
16.1.6	情報セキュリティインシデントの分析及び解決から得られた知識は、インシデントが将来起こる可能性又はその影響を低減するために用いる。			
16.1.7	組織は、証拠となり得る情報の特定、収集、取得及び保存のための手順を定め、適用する。			
16.1.7.13.PB	クラウドサービス事業者は、クラウドサービス利用者と、クラウドコンピューティング環境内の潜在的なディジタル形式の証拠、又はその他の情報の要求に対応する手順を合意する。			
17	事業継続マネジメントにおける情報セキュリティの側面			
17.1	情報セキュリティ継続 管理目的：情報セキュリティ継続を組織の事業継続マネジメントシステムに組み込むため。			
17.1.1	組織は、困難な状況（adverse situation）（例えば、危機又は災害）における、情報セキュリティ及び情報セキュリティマネジメントの継続のための要求事項を決定する。			
17.1.2	組織は、困難な状況の下で情報セキュリティ継続に対する要求レベルを確実にするための、プロセス、手順及び管理策を確立し、文書化し、実施し、維持する。			
17.1.3	確立及び実施した情報セキュリティ継続のための管理策が、困難な状況の下で妥当かつ有効であることを確実にするために、組織は、定められた間隔でこれらの管理策を検証する。			
17.2	冗長性 管理目的：情報処理施設の可用性を確実にするため。			
17.2.1	情報処理施設は、可用性の要求事項を満たすのに十分な冗長性をもって、導入する。			
18	順守			
18.1	法的及び契約上の要求事項の順守 管理目的：情報セキュリティに関連する法的、規制又は契約上の義務に対する違反、及びセキュリティ上のあらゆる要求事項に対する違反を避けるため。			
18.1.1	各情報システム及び組織について、全ての関連する法令、規制及び契約上の要求事項、並びにこれらの要求事項を満たすための組織の取組みを、明確に特定し、文書化し、また、最新に保つ。			
18.1.2	知的財産権及び権利関係のあるソフトウェア製品の利用に関連する、法令、規制及び契約上の要求事項の順守を確実にするための適切な手順を実施する。			
18.1.2.13.PB	クラウドサービス事業者は、知的財産権の順守に対応するためのプロセスを確立する。			
18.1.3	記録は、法令、規制、契約及び事業上の要求事項に従って、消失、破壊、改ざん、認可されていないアクセス及び不正な流出から保護する。			
18.1.3.13.PB	クラウドサービス事業者は、クラウドサービス利用者に、クラウドサービスの利用に関して、クラウドサービス事業者が収集し、蓄積する記録の保護について、情報を提供する。			
18.1.4	プライバシー及び個人識別情報（PII） の保護は、関連する法令及び規制が適用される場合には、その要求に従って確実に行う。			
18.1.5	暗号化機能は、関連する全ての協定、法令及び規制を順守して用いる。			
18.1.5.7.PB	クラウドサービス事業者は、クラウドサービス利用者に、適用する協定、法令及び規則を順守していることをレビューするため、クラウドサービス事業者が実装した暗号による管理策の記載を、提供する。			
18.2	情報セキュリティのレビュー 管理目的：組織の方針及び手順に従って情報セキュリティが実施され、運用されることを確実にするため。			
18.2.1	情報セキュリティ及びその実施の管理（例えば、情報セキュリティのための管理目的、管理策、方針、プロセス、手順）に対する組織の取組みについて、あらかじめ定めた間隔で、又は重大な変化が生じた場合に、独立したレビューを実施する。			
18.2.2	管理者は、自分の責任の範囲内における情報処理及び手順が、適切な情報セキュリティのための方針群、標準類、及び他の全てのセキュリティ要求事項を順守していることを定期的にレビューする。			
18.2.3	情報システムを、組織の情報セキュリティのための方針群及び標準の順守に関して、定めに従ってレビューする。			

評価項目一覧

事業者名	

様式4

【入札事業者記入欄の記載方法・留意事項】
- 事業者は「対応可否」欄に「○」（対応可）もしくは「×」（対応不可）を入力し、具体的な対応内容等を「詳細」欄に記載してください。
- 別途、詳細を示す提案資料（カタログ含む）がある場合には、そのページ・項番を記載してください。
- 灰色のセルの記載は特段は不要ですが、任意で記載いただいても構いません。ただし、記載は段階評価の対象にはならず、対応可否に応じた満点か不合格かのみの評価となります。
- 黄色のセルは項目の区切りを示しているため、対応可否等の記載は不要です。
- 必須項目をすべて満たした場合は200点を与える。

項目	項番	要件（評価項目）	入札事業者記入欄				評価区分	配点	会館記入欄	
			対応可否（○×入力）	詳細（具体的な対応内容等）	提案資料該当箇所 ページ	提案資料該当箇所 項番			評価	採点
1.図書館業務システム機能要件	1.1.	包括的要件								
	（1）	現有のデータ量を全て収容し、契約期間中のデータ増加に対してはフレキシブルに記憶容量を追加する等、適切な運用ができること。					必須			
	（2）	継続的な運用保守体制及びセキュリティ対策が十分に施されているシステムであること。					必須			
	（3）	クラウドサービスが問題なく動作し、なおかつセキュアな運用を実現するよう、サーバとクライアントの通信については、暗号化通信（httpsプロトコル）にて運用すること。					必須			
	（4）	現行システムのデータ継承ができること。					必須			
	（5）	契約期間中に機能拡張があった場合は、会館の要求に合わせて追加を可能とすること。					必須			
	（6）	災害や事故の際に事業を継続もしくは早期再開できるバックアップ体制と、修復する体制を備えること。					必須			
	（7）	障害の検知、調査、対応及び監査証跡の確保のために、十分なログ情報を取得できること。					必須			
	（8）	個人情報に該当するデータに関しては、十分な機密保持のための対策が施されていること。					必須			
	1.2	共通要件								
	（1）	全ての機能は、キーボード、マウスによる操作を基本とし、容易に操作できること。					必須［段階］	50		
	（2）	一画面に複数のウィンドウを開き、併行して複数の図書館業務及び表作成などの事務作業が実行できる機能を有すること。					必須			
	（3）	サーバデータへの不正なアクセスを防ぐためのセキュリティ機能を有すること。					必須			
	（4）	国立情報学研究所（以下、「NII」という）が提供するサービスを受けられるシステムであり、NACSIS-CAT、NACSIS-ILLに対応し、多言語対応機能を実装していること。最新のCATP/スキーマバージョンに対応していること。					必須			
	（5）	使用する文字コードはすべて、NIIが多言語対応目録システムで使用するUCS文字コードの仕様と同一であること。					必須			
	（6）	NACSIS-CAT/ILLへの接続時にはあらかじめ登録したID、パスワードで自動的にログインする機能を有すること。					必須			
	（7）	業務の必要な処理画面上でNIIデータベース及び業務用データベースをシームレスに検索する機能を要すること。					必須			
	（8）	帳票はPDFのほかに、Microsoft Excel等で加工可能なテキスト形式で出力されること。					必須			
		帳票の作成・編集機能を有する場合には加点する。					加点	10		
	（9）	納入時までにハードウェアのスペックに変更があった場合、もしくは、アプリケーションソフトにバージョンアップがあったときは、別途協議すること。					必須			

(10)	業務用システム・利用者システム共にWebクライアント方式であること。					必須				
(11)	業務用クライアントはセキュリティ対策のため、利用できるIPアドレスを指定でき、指定されたIPアドレスを持つクライアントのみアクセスを許可できること。					必須				
(12)	各業務画面の日付入力項目においては、カレンダーからの選択入力ができること。					必須				
(13)	各業務機能において検索したデータの一覧表示について、各項目値の表示列を、業務担当者毎に任意で表示・非表示が切り替えられる機能を有すること。また複数の項目をソートキーとして、データ一覧の表示順を切り替えられる機能を有すること。					必須				
(14)	各業務機能において検索したデータの一覧をMicrosoft Excel等で編集できること。					必須				
	各業務機能において検索したデータの一覧をテキスト形式で出力可能な場合は加点する。					加点	10			
(15)	各業務で行われた処理の結果がOPAC上に即時反映される場合、加点する。					加点	10			
(16)	ISBNの13桁化には全業務機能及び帳票が対応済みであること。					必須				
(17)	OPAC及びInternet上に公開するWeb機能はクロスサイトスクリプティング脆弱性に対応したサニタイジング処理が組み込まれていること。					必須				
(18)	利用者・業務担当者に対してメール通知機能を有すること。メール内容はテンプレート設定及び自由記述が可能であること。					必須				
(19)	メール送信に失敗した場合は、送信に失敗した旨のメールが管理者宛てに送信されること。					必須				
(20)	操作者の処理対象となるデータの参照・更新が制限できること。					必須				
(21)	各種帳票の抽出条件は、範囲指定や個別指定のほか、「範囲外」、「等しくない」、「未入力」等の指定もできること。					必須				
(22)	業務画面で納入者・予算・所在の各項目を入力時に、直接コード値を入力することができること。コード値が不明な場合は、簡易な操作で入力できるよう支援機能を有すること。入力方法はプルダウン選択方式に変更することも可能なこと。					必須				
(23)	書誌・所蔵・図書発注・雑誌契約・ILL依頼・ILL受付・利用者・予算・納入者の各データベースで保有している項目の他に、会館独自の項目をコード型・フィールド型で10個以上追加できること。また、項目名の文言やコード値は自由に設定できること					必須				
(24)	アクセスログ等の証跡を保存及び提供が可能であること。					必須				
(25)	文部科学省および日本図書館協会の統計データを集計できること。					必須				
1.3.	各業務要件									
1.3.1	共通管理業務									
(1)	予算情報									
①	予算情報を予算コードにより管理する予算テーブルを持ち、各業務での処理に自動で連動し、執行状況をリアルタイムで確認できること。					必須				
(2)	利用者情報									
①	利用者情報の登録・更新・削除ができること。					必須				
②	ファイル読込みによる利用者情報一括登録・更新機能を有すること。					必須				
③	利用者情報について、システムに登録されているすべての利用者データをバックアップとしてファイル出力することができること。					必須				
④	利用者IDの付け替え機能を有すること。その際、旧利用者IDの貸出データや予約データなども新利用者IDへ引き継ぐこと。旧利用者IDもそのままデータとして保持すること。					必須				
(3)	業務操作者情報									
①	業務操作者ID毎に業務の利用可否をコントロールできること。なお利用できない機能はメニューも非表示にできること。					必須				
②	業務利用可否権限は業務操作者をグループ化して管理できること。					必須				
(4)	通貨情報									
①	国別の通貨情報を通貨コードにより管理する通貨テーブルを持ち、図書受入・雑誌受入の業務処理において管理できること。					必須				
(5)	納入者情報									
①	納入者情報の新規作成・流用作成・修正処理が行える機能を有すること。					必須				
(6)	番号管理									
①	会館では物品管理上、図書所蔵データ(和雑誌記事データ、新聞記事データを含む)及び製本雑誌データを「資料番号」で管理している。資料番号は、図書所蔵データ及び製本雑誌データに対して一意であること。					必須				
(7)	データ管理									
①	各処理画面へのデータ入力時には、コードの完全一致、コードの前方一致、コードに対する表示形からの検索によって呼び出す機能を有すること。					必須				
②	書誌データの呼び出しにおいては、書名・著者名・キーワード・ISBN・ISSNを含む目録システムでの検索機能を各業務にて備えていること。					必須				
③	検索キーは、日本語については分かち機能を実装し、システムが自動生成すること。個別に検索キーを追加することができること。					必須				
	追加した検索キーの修正及び削除ができる場合は加点する。					加点	10			
④	図書館システムで使用する各種動作パラメータの設定ができる管理機能を有すること。					必須				
1.3.2	図書受入									
(1)	包括的要件									
①	複数担当者で受入業務を処理する機能を有すること。					必須				
②	NACSIS-CATと会館書誌データベースの検索がシームレスに行え、該当データを各処理段階における書誌データとして引用できること。またオリジナル作成もできること。					必須				
③	継続図書の管理ができること。					必須				
(2)	選定・発注									
①	選定・発注リストの作成ができること。					必須				
②	継続本の発注データが作成できること。					必須				
③	選定中のデータを検索して発注データの作成ができること。					必須				
④	選定段階のデータを一括発注できること。					必須				
⑤	CSV、TSV等の汎用的なファイル形式のデータから一括発注データ作成ができること。					必須				
	取り込み時に自動で重複チェックを行うことが可能な場合加点とする。					加点	10			
⑥	購入依頼のデータから一括発注データ作成ができること。					必須				
(3)	受入									
①	発注データを検索して受入処理ができること。					必須				
②	発注処理を介さずに受入処理ができること。					必須				
③	ファイル読込みによる受入データー括登録機能を有すること。					必須				
④	継続本の受入・納品状況が管理できること。					必須				
⑤	値引率、通貨別円換算率、消費税率を設定できること。定価から納入価格を自動算出できること。					必須				
⑥	資料番号は備消区分により番号体系を選択でき、自動採番が可能であること。					必須				
⑦	資料番号の付与は上記の他に任意の検索集合体を作成し、そこから任意の開始番号を指定して付与ができる機能を有すること。本機能によって既にある資料番号があった場合はスキップすることもできること。					必須				

（4）	支払								
①	支払予定内訳書が出力できること。					必須			
②	受入レコードに対して、支払・支払の保留を一覧表示、選択し処理できること。					必須			
③	支払画面の検索結果のソート指定ができること。（受入日、資料番号、タイトル）					必須			
④	支払処理毎に支払番号を付与できること。					必須			
⑤	支払番号を複数指定しての図書明細書の作成ができること。					必須			
（5）	所蔵登録								
①	支払処理、目録処理が完了したデータを抽出して所蔵登録ができること。所蔵登録が完了したデータはOPAC、ILL、閲覧、所蔵管理にて利用できる状態になること。					必須			
②	所蔵登録したデータから整理済図書リストが作成できること。					必須			
（6）	帳票・統計表								
①	未払リストについては納入業者ごとに受入日、受入番号、書名、納入価格、予算名称、摘要が印刷できること。					必須			
②	支払予定内訳書については納入業者ごとに書名、冊数、金額、摘要が印刷できること。								
③	以下の統計表が作成できること。 (ア)分類別受入冊数統計表 (イ)受入区分別受入統計 (ウ)納入者別支払額統計 (エ)資料区分別受入統計								
1.3.3	図書目録								
（1）	包括的要件								
①	NACSIS-CATの図書書誌レコードに準拠した書誌レコードを持つこと。					必須			
②	NACSIS-CATの書誌階層に準拠した管理ができること。					必須			
③	NACSIS-CATの図書書誌レコードの項目に加え、言語区分に基づく和洋区分、作成者・作成日の各項目に加えて受入情報も持つこと。多言語に完全対応し、会館データベースも多言語で登録・表示できること。					必須			
④	NACSIS-CATと会館目録システムの切り替えはワンタッチで行えること。					必須			
⑤	目録データベースにレコードの登録・修正・削除ができ、即時更新が行えること。					必須			
⑥	書誌データベース中にURLフィールドを格納できOPACにてハイパーリンクができること。					必須			
（2）	書誌作成								
①	標準分類コードを検索、引用する機能を有すること。					必須			
②	会館目録データベースに対し、所蔵レコードの付け替えができること。					必須			
③	CSV、TSV等の汎用的なファイル形式で作成した外部作成データを書誌・所蔵ファイルに取り込む機能を有すること。					必須			
④	1つのファイルにおいて、集合書誌レコード、単行書誌レコードの階層関係を書誌リンクにより表示できる機能を有すること。					必須			
⑤	所蔵の巻数、子書誌の巻数はOPACにおいて文字列の順でなく、巻数の順でソートができるように表示順の項目をもち、かつ表示順の設定は自動でできること。					必須			
⑥	図書1冊ごとに対応した所蔵ファイルによって所在管理する機能を有すること。					必須			
⑦	図書受入処理を経なくても目録登録処理を行う機能を有すること。					必須			
⑧	会館書誌データ登録の際にISBN、NCID番号等により重複チェックを行う機能を有すること。					必須			
⑨	書誌項目中にLOCALタグ(自館オリジナルのデータが入力でき、NACSIS-CATアップロード時にも上書きされない項目)を持てること。LOCALタグ中のデータをOPACに表示するかどうかパラメータで設定できること。					必須			
⑩	テキストファイルより雑誌記事を一括登録できる機能を有すること。その際、資料番号及び配架場所を設定できること。					必須			
⑪	テキストファイルより新聞記事を一括登録できる機能を有すること。その際、資料番号及び配架場所を設定できること。					必須			
（3）	典拠管理								
①	NACSIS-CATの著者名典拠、統一書名典拠レコードに準拠した典拠レコードを持つこと。					必須			
②	NACSIS-CATの著者名典拠、統一書名典拠レコードの項目に加え、作成者・作成日の情報も持つこと。					必須			
③	条件を指定することにより、NACSIS-CATデータからオンラインにて著者名典拠、統一書名典拠データのダウンロードができ、そのダウンロードデータにて直接会館データベースを更新できる機能を有すること。					必須			
（4）	その他								
①	電子ブックを一括登録してOPACで検索できる機能を有すること。ファイルフォーマットはCATP形式に対応可能なこと。					必須			
②	電子ジャーナルを一括登録してOPACで検索できる機能を有すること。					必須			
（5）	帳票								
①	以下の帳票が作成できること。 ①バーコードラベル ②請求記号ラベル ③整理済資料リスト ④寄贈リスト ⑤図書原簿 ⑥除籍原簿 ⑦図書目録プルーフリスト ⑧雑誌目録プルーフリスト ⑨雑誌所蔵リスト					必須			
1.3.4	雑誌業務								
（1）	包括的要件								
①	複数担当者で受入業務を処理する機能を有すること。					必須			
②	NIIと会館書誌データベースの検索がシームレスに行え、該当データを各処理段階における書誌データとして引用できること。またオリジナル作成もできること。					必須			
③	契約、受入、製本、目録の各機能を有すること。					必須			
④	受入データは製本が完了するまで保持し、メンテナンスができ、条件を指定して一括削除ができること。					必須			
（2）	発注・契約								
①	契約レコードの新規登録・修正・削除が行えること。また、契約レコードは年度単位に管理できること。					必須			
②	当該年度の雑誌契約データを一括複写して翌年度の雑誌契約データを作成できること。					必須			
③	契約レコードの登録、修正、コピー入力、削除を行えること。					必須			
④	契約データを年度毎、納入者毎に指定して一括して出力ができること。					必須			
⑤	契約データを一括して更新できる機能を有すること。					必須			
⑥	割引率、税率、レートによって価格を自動算出すること。ただし、自動算出しない設定もできること。					必須			
⑦	通貨及び原価を入力していない場合は、価格として任意の値を入力できること。					必須			
⑧	新規の発注・契約データの場合、書誌データの新規作成の後、リンクポイントを自動生成して発注・契約データの入力ができること。					必須			
⑨	以下の帳票が作成できること。 (ア)新規雑誌一覧表 (イ)受入雑誌一覧表 (ウ)雑誌契約一覧表					必須			
（3）	受入								
①	雑誌の新着巻号レコードについて、単一の画面上で次受入巻号の予測値を入力域に表示すること。					必須			

②	前払金額は、当該年度の契約額を契約冊数で割った値とすること。ただし、年度の最終受入巻号は端数を加算した値を表示すること。					必須			
③	支払対象外の巻号の受付ができ、増刊号（特集記事情報等）の登録ができること。					必須			
④	年鑑類の資料を対象に単冊登録処理ができること。また、単冊登録処理時には原簿番号も入力できること。単冊登録されたデータはOPAC、ILL、閲覧、所蔵管理にて利用できること。					必須			
⑤	チェックイン画面に最初に表示する件数の上限を指定できること。また全件表示することもできること。					必須			
⑥	受入単位に特集記事の入力ができ、OPACでの検索対象となること。このときの特集記事データの検索用アクセスポイントは自動で生成されること。					必須			
⑦	受入単位にURLが登録できること。このURLはOPAC画面上でリンクができること。					必須			
⑧	受入されたレコードをもとに会館雑誌の包括所蔵レコードが自動更新されること。					必須			
⑨	受入巻号データの一括削除が行えること。本機能は所定の抽出条件やファイル読み込みにより削除集合を作成・一覧表示しそのなかからさらに削除対象を選択・除外できること。					必須			
⑩	以下の帳票が作成できること。 (ア)受入チェックリスト (イ)未着・欠号リスト					必須			
（4）	支払（前金・後金）								
①	前金・後金支払処理ができること。					必須			
②	雑誌支払明細書の作成ができること。								
③	支払対象データは一覧表示でき支払／支払保留の指定ができること。					必須			
（5）	精算								
①	前金支払処理ができる機能を有すること。					必須			
②	精算対象となった巻号は、精算処理されたことが識別できる形で、後金払の欠号情報として管理すること。					必須			
（6）	帳票								
①	未払リストについては納入業者ごとに受入日、誌名、納入価格、摘要が印刷できること。					必須			
②	支払予定内訳書については納入業者ごとに誌名、巻号、冊数、金額、摘要が印刷できること。					必須			
（7）	雑誌目録								
①	書誌レコードは、NACSIS-CATの雑誌書誌レコードに準拠すること。					必須			
②	所蔵レコードは、NACSIS-CATの雑誌所蔵レコードに準拠すること。					必須			
③	書誌データベース中にURLフィールドをもち、OPACにてハイパーリンクができる機能を有すること。					必須			
④	NACSIS-CAT雑誌書誌レコードによる雑誌書誌レコードの生成・上書きができること。					必須			
⑤	雑誌所蔵レコードの所蔵年次・所蔵巻号を表示し、それをもとに手入力で編集を行い、対応するNACSIS-CAT雑誌所蔵レコードを更新する機能を有すること。					必須			
⑥	会館雑誌所蔵データベースの更新及びNACSIS-CATの雑誌目録データベースのオンラインでの更新ができること。					必須			
⑦	NACSIS-CATへの雑誌所蔵データの一括アップロードがオンラインでできること。					必須			
⑧	校正用のプルーフリストの作成ができること。					必須			
（8）	雑誌製本								
①	雑誌製本の各処理については、所蔵する全レコードを処理対象として扱えること。					必須			
②	製本レコードには製本予算及び金額を設定できること。					必須			
③	製本レコード作成時に、版型と製本費を連動して設定できること。					必須			
④	登録した製本雑誌の図書原簿を作成できる帳票機能を有すること。					必須			
⑤	製本雑誌1冊ごとに所蔵ファイルを持ち、所在管理ができること。					必須			
1.3.5	閲覧業務								
（1）	包括的要件								
①	システム及びネットワークトラブル等時に利用するローカル閲覧機能を有すること。					必須			
②	貸出・返却の履歴を参照できる機能があり、業務担当者のみ操作ができるよう制御できること。					必須			
③	図書館カレンダー機能を用意し、返却期限日、延長期限日が自動設定できること。					必須			
④	利用者区分別にカレンダー上の特別貸出期間を設定できること。					必須			
⑤	利用できない利用者、貸出できない本を処理した場合は効果音が鳴ること。					必須			
（2）	貸出返却条件設定								
①	資料種別、利用者区分グループ単位による貸出返却条件（貸出冊数・日数・更新回数・罰則等）が設定できること。					必須			
②	資料種別に対して異なる貸出条件を設定できること。					必須			
③	返却期限日が過ぎている資料貸出者に対して、罰則付与を自動で設定できること。					必須			
④	貸出返却条件の設定機能は利用者区分グループと貸出種別毎に1件ずつ設定できる機能を有すること。					必須			
⑤	貸出期間の設定は日数の他に、月指定や年指定ができること。					必須			
（3）	貸出								
①	利用者ID読み取りの際、現在貸出中履歴を一覧表示できる機能を有すること。					必須			
②	貸出条件に反する貸出要求時にはエラーとすること。エラーの場合はそのことが明確に判るように、エラーメッセージが表示されること。エラーの場合でも、強制貸出できること。					必須			
③	同一利用者・同一資料での貸出要求時には、継続貸出として処理できること。					必須			
④	利用者IDの直接入力でも貸出処理ができること。また番号、利用者の名前、名前のヨミの検索結果からも貸出できること。					必須			
⑤	未登録資料貸出の時、資料名等を登録できること。					必須			
⑥	返却期限日の修正ができること。					必須			
⑦	利用者IDを読み込んだ状態のまま、「利用者情報」画面へ利用者IDを引き継いで遷移できること。					必須			
（4）	返却								
①	貸出履歴テーブルの貸出履歴レコードは、返却情報を付加した上で蓄積すること。					必須			
②	予約されている資料である場合は、予約者等の予約情報を表示すること。また予約者に対してメール通知ができること。					必須			
③	返却期限の過ぎた図書の利用者に対して、メールで警告を送る機能を有すること。					必須			
④	返却期限日を指定して返却期限日の変更ができること。返却期限日の一括修正機能を有すること。					必須			
（5）	利用者情報								
①	利用者の貸出状況、予約状況、個人情報、コメント、罰則情報が確認できること。個人情報については表示させない設定もできること。					必須			
（6）	帳票及び督促								

①	以下の帳票が作成できること。 (ア)分類別統計表 (イ)利用者区分別 / 分類別統計表 (ウ)ベストリーダーリスト (エ)利用者リスト (オ)貸出リスト(所在別請求記号順、利用者順) (カ)予約リスト、予約票					必須				
②	督促機能は以下の要件をみたすこと。 (ア)督促対象データを抽出し、画面に一覧表示できること。 (イ)画面に一覧表示されたデータを対象として督促チェックリストが出力できること。 (ウ)抽出条件は、貸出日や利用者区分による絞込みが可能で、予約者がいる貸出データや延滞している利用者の確認が容易にできる項目を有すること。 (エ)確定された督促データの集合から、各種督促方法が選択できること(掲示用、事務用、はがき、利用者別、メール、封書、宛名、はがき)。 (オ)督促メールを自動で送信できること。自動送信の実行周期、抽出条件、定型文言は複数パターン設定でき、利用者区分ごとに定型文言を指定できること。 (カ)はがき、封書に関しては、出力時に名前・住所共に本人、保護者の選択ができること。					必須				
③	返却期限通知機能を有すること。本機能は督促と同等の抽出機能を有し、メール通知ができること。					必須				
1.3.6	所蔵管理									
(1)	包括的要件									
①	図書については物理的な1冊ごとに所在を管理すること。					必須				
②	雑誌については所在コード(場所)、所蔵レコード(巻号)単位に所在を管理すること。					必須				
③	所在は棚番号等詳細な情報を設定することもできること。また、棚番号を設定する場合は、資料単位で一冊ずつ設定する他に、資料番号の範囲指定やファイル読み込み等により一括で設定することもできること。					必須				
④	資料単位の所在の変更処理ができること。					必須				
⑤	資料番号の付け替え機能を有すること。蔵書点検機材にて作成されたデータにより一括しての変更処理ができること。					必須				
⑥	雑誌は所在コードの入力により一括して所在の変更処理ができること。					必須				
⑦	蔵書点検機材に作成されたデータを元に点検処理ができること。					必須				
⑧	不在一覧からの除籍処理ができること。また除籍済リストの作成ができること。					必須				
⑨	除籍準備処理機能を有すること。また除籍準備リストの作成ができること。					必須				
⑩	配架処理機能を有すること。					必須				
⑪	除籍資料の復籍処理機能を有すること。					必須				
1.3.7	相互貸借									
(1)	包括的要件									
①	NACSIS-ILLを利用した依頼・受付業務が行えること。					必須				
②	NACSIS-ILLを経由しない受付処理ができること。					必須				
③	NACSIS-ILL経由の依頼・受付レコードに対するすべての処理は、透過的にNACSIS-ILLに反映されること。					必須				
④	多言語対応機能を実装し、最新のCATP/スキーマバージョンに対応していること。					必須				
⑤	OPACの検索結果から相互貸借申し込み画面に書誌情報を引用できること。					必須				
⑥	マイライブラリで利用者が入力したデータを自動的にシステムに取り込み、依頼データとして自動的に登録できること。また、登録したデータをそのまま利用して、NACSIS-ILLへ依頼登録できること。					必須				
(2)	依頼・受付									
①	NACSIS-ILL依頼レコード・受付レコードの新規作成・修正・処理段階変更ができること。					必須				
②	NACSIS-ILLレコードの状態遷移を反映しデータベースを更新できること。 NACSIS-ILLで他館からの依頼レコードが到着していた場合は対応する受付レコードを生成すること。画面表示に際してはこれらを視覚的に識別できること。					必須				
③	依頼時の所蔵館一覧画面では、各項目の昇順・降順の並び替えができること。また自館の所蔵データを自動検索し、所蔵データがあった場合はその旨を表示できること。					必須				
(3)	帳票									
①	受付作業票、送付票の作成ができること。					必須				
②	依頼・受付のプルーフリスト(相手館別)が作成できること。					必須				
(4)	その他									
①	参加組織一覧、参加組織メンテナンス機能を有すること。					必須				
②	料金相殺の対応として、各種詳細画面、受付・依頼票に相殺表示ができること。					必須				
③	各種帳票の出力条件には相殺館の指定ができること。					必須				
④	依頼検索時の所蔵館一覧中に相殺表示がされること。					必須				
⑤	依頼検索時の所蔵館一覧で表示中の各項目にてソート表示ができること。					必須				
⑥	一括発送、一括受付、一括保存(Web依頼データ)の機能があること。					必須				
⑦	依頼・受付番号は依頼毎、受付毎、複写毎、貸借毎、さらにそれぞれの掛け合わせ毎の自動付与ができること。本機能により付与された結果の値に対して修正ができること。					必須				
⑧	文献複写受付時にモノクロ・カラーコピー等の料金項目を複数設定できること。また、複数料金項目を設定した場合、帳票にも複数印字されること。					必須				
1.3.8	蔵書点検									
(1)	包括的要件									
①	所在、請求記号の範囲により蔵書点検範囲を指定できること。					必須				
②	資料ごとに蔵書点検で不明になった回数を管理できること。					必須				
③	蔵書点検用ハンディーターミナルから読み取ったデータを取得し、そのデータを元に蔵書点検処理ができること。					必須				
④	読み取った資料IDリストについてはファイルが複数に分かれていても、点検処理ができること。					必須				
⑤	点検処理の結果、所在不明になった資料のデータを個別または一括で不明状態にできること。					必須				
⑥	点検処理の結果、エラーとなったデータの履歴を業務画面から参照できること。					必須				
(2)	帳票									
①	以下の帳票出力ができること。 (ア)不明資料リスト (イ)発見資料リスト					必須				
1.3.9	蔵書検索									
(1)	包括的要件									
①	インターネットを経由して会館内及び会館外から利用が可能であること。					必須				
②	操作性の優れたGUIによる検索ができること。					必須 [段階]	50			
	レスポンシブデザインに対応している場合は加点する。					加点	5			
③	スマートフォンに対応していること。スマートフォンで目録検索から提供するすべての機能を利用できること。					必須				
④	図書・雑誌・地方行政資料・和雑誌記事・新聞記事・AV資料等の検索ができること。					必須				
⑤	会館が作成している「女性情報シソーラス」を用いた同義語検索ができること。					必須				

	シソーラス展開して検索ができる場合は加点する。					加点	50			
⑥	検索時の文字コードはUCSコードであり、UCSコードに対応する文字フォントで表示されること。					必須				
⑦	NIIが提供する検索専用サーバ又はCiNii Booksを利用して、全国総合目録の検索ができること。一度入力した検索語を再入力することなく検索が可能な、会館データベースとNDLサーチ、CiNii Books、CiNii Research、学術機関リポジトリポータル IRDB、Googleブック検索、Google Scholarとの横断検索機能があること。					必須				
⑧	英語版のOPACを有すること。このとき一般的なガイドの英語表示の他に最低でも所在場所(配架場所名)と状態(貸出中等)の表示は英語表記ができること					必須				
（2）	蔵書検索インターフェース									
①	資料区分（図書・雑誌・地方行政資料・和雑誌記事・新聞記事・AV資料等）を指定して検索できること。					必須				
②	出版年（年月日を指定できること）、出版国、言語、媒体種別、配架場所（所在）を指定して検索できること。					必須				
	検索語未入力の状態で出版年、出版国、言語、媒体種別、配架場所を指定しても検索できる場合は加点する。					加点	20			
③	検索結果の並び順(書名・著者名・出版年)及び昇順・降順を指定できること。					必須				
④	一画面に表示する件数が設定できること。					必須				
⑤	データベース中の下記項目に対する任意の文字列（以下、検索語）を入力して検索できること。 (ア)タイトル類：書誌中の「本標題」・「並列標題」・「その他の標題」・「標題関連情報」・「統一書名」・「内容注記」・「件名」・「書誌構造リンク」に含まれる標題及びそのヨミ。 (イ)著者名類：書誌中の「書誌構造リンク」に含まれる著編者名及びそのヨミ、著者名典拠 (ウ)コード類：書誌中の「ISBN」・「ISSN」・「NC書誌ID」。					必須				
⑥	検索語に対して近似値による別のキーワード候補を表示し、クリックすることで再検索を行う機能(もしかして検索機能)を有すること。					必須				
⑦	ファセットブラウジング機能を有すること。					必須				
⑧	検索結果一覧に所蔵情報を表示できること。表示しない設定もでき、表示する上限件数を設定できること。					必須				
⑨	検索結果一覧から任意のデータを選択して、メールで任意のアドレスへ送信したり、ファイルに出力したりできること。					必須				
⑩	所蔵情報に棚の名称等の詳細な所在場所（配架場所）が登録されている場合は、OPACにも表示されること。					必須				
⑪	親書誌、著者名、件名、標準分類等からの関連展開ができる機能を有すること。					必須				
⑫	件名細目がある場合は、細目も含めた形で関連展開ができること。					必須				
⑬	書誌詳細画面において和雑誌記事の場合には「掲載ページ」、新聞記事の場合には「人名」を表示できること。					必須				
⑭	図書・雑誌の書誌情報中にURL情報を持ち、OPAC上で該当情報にリンクできること。					必須				
⑮	書誌事項の内容をもとに検索機能を有すること。入力されたキーワードを分かちした結果で検索する機能を有すること。					必須				
⑯	ローカル検索時に検索結果が0件の場合は、予め指定したWebサイトに対して検索語を引き継いで検索できること。					必須				
⑰	検索語入力域にてAND、OR、NOTを利用した検索ができること。					必須				
⑱	書影画像をOPAC画面上へ自動で表示できること。					必須				
⑲	所蔵詳細画面から、CiNii Research、Google Books、Google Scholar等へ連携して検索できること。連携するWebサイトは追加・変更・削除ができること。					必須				
⑳	文献管理ツールとの連携が可能であること。OPACにて指定されたデータが各パーソナルデータベースに自動的に格納できること。					必須				
㉑	OPACのアクセス状況がわかる統計リストを作成できること。					必須				
（3）	女性情報シソーラス									
①	シソーラス辞書の管理・メンテナンスが容易に行えること。					必須				
②	シソーラス辞書をファイル出力できること。また、Winetとファイル連携できる機能を有すること。					必須				
（4）	利用者支援									
①	新着資料（図書、雑誌・新聞、地方行政資料、和雑誌記事、新聞記事）を月別に通覧できること。また、新着資料として表示される期間を月単位、日付単位で設定できること。					必須				
②	雑誌タイトルリストの照会ができること。このとき資料が電子ジャーナル資料の場合、自動的に電子ジャーナルとして区分けして表示できること。					必須				
③	分類を指定して検索する、分類検索機能を有すること。					必須				
④	OPACのタイトルバーに表示される文言("OPAC"等)は会館の運用に合わせてパラメータにより変更できること。また、OPACが英語版の時は、タイトルバーの文言も自動的に英語に切り替わること。					必須				
⑤	利用希望者が自分で新規利用者登録を行える機能及びその承認機能があれば加点する。					加点	10			
⑥	利用者認証は図書館システム独自の認証の他に、Shibboleth、LDAP、NIS等の認証サーバとの連携ができるよう考慮されていること。					必須				
⑦	OPACヘルプは日本語・英語別に標準的なものを提供すること。					必須				
1.3.10	マイライブラリ									
（1）	包括的要件									
①	インターネットを経由して会館内及び会館外から利用が可能であること。					必須				
②	利用者の個人用ページが提供されること。					必須				
③	個人用ページはパスワードにより保護されていること。					必須				
④	日本語版と英語版の表示切り替えが可能で、それぞれの言語によるオンラインヘルプを提供すること。					必須				
（2）	機能									
①	利用者個人向けのお知らせを掲載できること。					必須				
②	利用者個人の貸出状況、貸出履歴、予約状況、文献複写依頼状況、現物貸借依頼状況を表示できること。					必須				
③	利用者個人が登録したキーワードに基づいて、新着資料を表示できること（新着アラート機能）。また、電子メール通知の設定が可能であること。					必須				
④	図書の予約、貸出期間の延長、文献複写、現物貸借の申し込みができること。					必須				
⑤	ブックマークした資料の情報をマイフォルダに登録できること。必要なくなった資料はマイフォルダから削除できること。					必須				
1.3.11	運用管理／業務支援／その他									
（1）	運用管理									
①	図書館業務の運用履歴が管理できること。また個人情報に関する参照、リスト出力、登録、更新、削除の実行履歴が管理されること。					必須				
（2）	業務支援									
①	図書館業務で構築されるデータベースから、多種・多様な抽出条件と出力項目を指定してデータをファイル出力できること。					必須				
②	設定した出力項目を保存することができ、次回利用時に簡易な操作で再設定できること。					必須				
③	ファイル出力時に、CSV／TSV等のファイル形式が選択でき、Microsoft Excel等で加工できること。出力項目は、制御項目を除く項目を出力可能とし、各種コードに対応する名称データも引用できること。					必須				

	④	本機能はSQL等のユーティリティでなく、エンドユーザが操作できるGUIの画面から操作できること。					必須				
	（3）	その他									
	①	現行システムからのデータ移行ができること。現行のコード体系のうち必要なコードはそのまま使用できること。					必須				
	②	現行のデータは正規化を行った後移行すること。なお、正規化の条件は会館職員と協議を行い、必要に応じてプログラムチェック、リスト出力の処理を行った後、移行すること。					必須				
2. クラウドサービスのセキュリティ要件	（1）	管理基準									
	①	「政府情報システムのためのセキュリティ評価制度（ISMAP）管理基準」に基づく「ISMAPクラウドサービスリスト」に登録済みか、または申請済みであり、登録予定時期が明確に提示できること。ただし、「ISMAPクラウドサービスリスト」に登録されていない場合は、ISMAP管理基準の管理策基準が求める対策と同等以上の水準を満たしていることが確認できる情報として基本言明要件の一覧表（様式3）を提示できること。					必須				
	②	ISMS（JIS Q 27001）に準拠した情報セキュリティ管理体系を備えていること。									
	③	ISMSクラウドセキュリティ認証（JIS Q 27017）を取得している場合は加点する。					加点	10			
	（2）	データセンター									
	①	クラウドサービスを提供するデータセンターは、日本国内に設置されたデータセンターであり、データセンター専用施設であること。					必須				
	②	ISMAPクラウドサービスリストに掲載されたデータセンターであること。									
	③	Tier3以上の基準を満たしており、建築基準法の新耐震基準に適合していること。物理的な侵入対策、災害対策（耐震、防火、電源供給安定性など）を講じていること。									
	④	ネットワークセキュリティとしてファイアウォール、IDS/IPS、DDoS攻撃対策など、多層的なセキュリティ対策が講じられていること。									
	（3）	障害復旧対応									
	①	システムの冗長化など、災害時の機能・サービス停止等のリスクを最小限に抑える措置として次の対策が取られていること。 ・サーバのバックアップはシステム稼働に支障なく自動で行われること。 ・バックアップを5世代以上保存し復元ポイントを指定できること。 ・サーバ監視を24時間365日とし、サーバに障害が発生し復旧を必要と判断した時は、バックアップから復旧すること。					必須				
	（4）	ソフトウェアの脆弱性対策									
	①	OS、ミドルウェア及びソフトウェア等については、システム稼働中にメーカーサポートを受けられる安全なプロダクトを選定すること。					必須				
	②	不正侵入の経路となるバックドアや脆弱性の有無を確認し、脆弱性が存在する場合は、バージョンアップやセキュリティパッチの適用等の対策を講ずること。									
	（5）	ソフトウェアのバージョンアップ									
	①	ソフトウェアのバージョンアップ等が行われた場合に対応すること。					必須				
	（6）	OSバージョンアップ及びセキュリティパッチ適用に伴うサーバリソースの拡張									
	①	拡張作業に伴う影響を最小にするよう、適切なタイミングと方法で実施されること。					必須				
	②	計画的なメンテナンスやバージョンアップについては、事前に会館へ通知すること。									
	③	サーバリソースの利用状況が常に監視され、パフォーマンスの低下やリソース不足が発生しないよう、予防的な対策が講じられていること。									
	④	サーバの安定稼働に必要なリソースが常に確保され、アクセス負荷の変動に柔軟に対応できる構成であること。									
	⑤	OSのバージョンアップ及びセキュリティパッチの適用に必要なサーバリソース（CPU、メモリ、ストレージ、ネットワーク帯域など）は、受託者の責任において拡張・最適化されること。									
	（7）	ドメイン									
	①	Webサーバは会館が新規に取得する独自ドメインを設定すること。					必須				
	②	DNSサーバでレコードを設定するためのエントリーを提示すること。									
	③	使用するドメインの維持管理及びDNS設定はこの調達の対象外とする。									
	（8）	通信の暗号化TLS（SSL）									
	①	Webサーバ及びCMSサーバはインターネットを介して転送される情報に対しTLS（SSL）機能を適切に設定すること。					必須				
	②	TLS（SSL）機能のために証明局により発行された電子証明書を用いる。電子証明書の維持管理はこの調達に含む。 TLS（SSL）通信を行う情報システムの構築/運用/保守に際しては、SSL/TLS暗号設定ガイドラインに基づく設定・管理を実施すること									
	③	OV（組織認証）を用いる場合は加点する。					加点	10			
	（9）	メール配信時のなりすましメール対策									
	①	会館の所有する独自ドメインを使用できること。					必須				
	②	ヘッダFrom に、会館の所有する独自ドメインのメールアドレスが設定できること。									
	③	なりすましメール対策を講じるためにDNS サーバでSPF、DKIMレコードを設定するためのエントリーを提示すること。									
	④	メール送信時に、TLS 設定等通信時の暗号化ができること。									
	（10）	業務画面のログイン管理									
	①	IPアドレスによるアクセス元制限に対応する。					必須				
	②	ログイン時のパスワードは、12文字以上であること。									
	③	管理者は、アカウントごとに権限設定ができること（業務操作者、管理者など）。									
	（11）	業務画面の操作ログ管理									
	①	管理者は、サイバーセキュリティインシデントの検知、調査、対応、および監査証跡の確保のために、十分なログ情報を取得し、保護すること。取得したログは1年間以上保存すること。					必須				
	（12）	その他									
	①	情報システムのライフサイクルを念頭に置いた脆弱性対策が講じられていること。					必須				
3. データ移行要件											
	（1）	受託者は、現行システム業者が抽出したデータを本システムで動作するように変換を行い、データをチェックするとともに、本システムにセットアップし、動作の確認を行うこと。					必須				
	（2）	移行作業においてはデータの取り扱いを厳重に行い、個人方法等が流出・流用・改編されることがないこと。									
	（3）	移行作業計画を作成し、会館と協議のうえ決定すること。									
	（4）	データ移行後、移行対象データとシステムにセットアップされたデータを照合し、全ての移行対象データが問題なくセットアップされていることを確認すること。									
	（5）	移行作業計画及び結果について、書面で報告すること。									
4. ネットワー											

ク要件	（1）	会館基幹LANに接続された業務用端末と図書館システムに接続するインターネット回線は次のどちらかの方式とする。ただし、現在利用中の情報システムの利用に影響を与えないこと。 ①会館基幹LANの事務用インターネット回線を利用する方式。 ②本図書館システム用のインターネット専用回線と専用ネットワーク機器を設置する方式。					必須			
5. 研修要件											
	（1）	職員向けに、対面でシステム操作の研修を運用開始までに1回実施すること。					必須			
	（2）	システム全体の機能・構成等について、日本語による基本マニュアルを冊子またはPDFファイルで提供すること。								
	（3）	業務端末等の日本語操作マニュアルを冊子またはPDFファイルで提供すること。								
	（4）	利用者向けマニュアルをPowerPointまたはWord形式で提供すること。								
6.運用保守要件	（1）	運用保守の連絡体制								
		運用保守連絡体制図（運用保守担当者連絡先、ヘルプデスク連絡先、インシデント対応連絡先を含むこと）を作成し提出すること。連絡体制及び連絡先を変更する場合は速やかに新しいものを提出すること。					必須			
	（2）	障害対策								
	①	障害の発生が確認された場合は、会館に速やかに通知するとともに、対応策について協議し、復旧等の対応を取ること。					必須			
	②	障害対応状況について、随時通知すること。								
	③	障害に伴い発生する業務への影響を最小限とするための対策を講ずること。								
	④	復旧後に対応履歴を含む障害対応報告を行うこと。								
	⑤	想定できる障害に対して、対策を施すことにより、業務再開までに要する時間を短縮する措置を講ずること。								
	（3）	ヘルプデスク業務								
	①	平日9:00～17:00（会館の休館日、年末年始を除く）において、業務担当者からの本システムに関する質問事項等に対応すること。					必須			
	②	サポートを行う窓口を一元化し、利便性を図ること。								
	③	標準化された実施手順やルールに基づいたサポートを提供すること。								
	④	電子メール・受付システム等による問合せは、365日24時間受け付けるものとする。								
	（4）	セキュリティ管理								
	①	脆弱性対策: 定期的な脆弱性診断を実施し、発見された脆弱性にはパッチ適用や設定変更などの対策を行う体制であること。					必須			
	②	アクセス管理: システムへのアクセス権限を厳格に管理し、不正なアクセスを防止する。不正アクセスと疑われる行為が発覚した場合、アクセスログをレビューし不審な活動がないか確認する体制であること。					必須			
	③	ウイルス対策: 最新のウイルス対策ソフトウェアを導入し、定期的にシステムのスキャンを実施、マルウェア感染が疑われる場合は、迅速に隔離・駆除を行う体制があれば加点する。					加点	10		
	（5）	情報セキュリティ対策履行状況の報告								
		良好な運用を継続するために、この項で示す運用保守要件の履行状況を年１回以上報告すること。					必須			
	（6）	契約終了時の対応								
	①	契約終了時、本システムから他システムにデータ移行が必要となったときには、本システムから必要なデータを抽出すること。					必須			
	②	情報流出がないよう全てのデータを抹消し、その完了を報告すること。								
	（7）	長期利用への対応								
		会館が令和13年9月1日以降においても本業務で導入する図書館業務システムの運用・保守の継続を希望する場合、本仕様書に示された要件に基づき、サービス利用や、運用・保守等支援の継続を可能とすること。					必須			
	（8）	サービス提供終了時の事前通知								
	①	サービス提供事業者の都合によりサービスの提供を終了する場合、受託者は、サービス終了予定日の12ヶ月前までに、書面（電子メールによるPDFの送付可）により会館に対しその旨を通知するものとする。					必須			
	②	受託者は、サービス終了の通知にあたり、会館が代替サービスへ円滑に移行できるよう、データのエクスポート方法、移行期間中のサポート体制及びその他必要な支援策について具体的に提示するものとする。会館は、提示された支援策に基づき、受託者と協議の上、移行計画を策定できるものとする。								
	③	受託者からサービス終了の通知があった場合、会館は、サービス終了予定日に関わらず、本契約を解除する権利を有するものとする。この場合、会館は、受託者に対し、未利用期間にかかる利用料の返還を求めることができるものとする。								
7. プロジェクト管理に関する要件	（1）	スケジュール管理								
	①	受託者は、契約後速やかに会館職員と協議を行い、業務計画書（スケジュールと作業内容等が明記されているもの）及び実施体制表を作成し提出すること。					必須			
	②	定期的に進捗報告を行い、必要に応じて打ち合わせ（オンライン可）を行うこと。								
	③	業務計画書に示したスケジュールが遅延し、運用開始に間に合わない場合、遅延しているタスクの支援を行う遅延回復要員を追加して対応すること。ただし、会館の責に帰すべき事由によりスケジュールの回復が困難となった場合は、この限りでない。								
	（2）	体制管理								
	①	本業務を円滑に実施するために、導入システム及び図書館業務を熟知したシステムエンジニアを含む最適な体制を構築すること。					必須			
	②	通常時の連絡体制の他、非常時の連絡体制についても提示すること。								
	③	①または②について変更が生じた場合、受託者は速やかに変更内容を提出すること。								
8.情報セキュリティに関する要件										
	（1）	本業務のために会館から提供される情報については、本業務の目的以外に利用しないこと。なお、本項の規程は本業務が完了し、又は本契約が解除その他の理由により終了した後であっても、その効力を有するものとする。								
	（2）	本業務における作業の一切（会館より開示された資料や情報を含む）について、秘密の保持に留意し、漏えい防止の責任を負うこと。								
	（3）	情報セキュリティを確保する為の体制及び機密情報の責任者を定め、その内容を書面にて会館に提出すること。								
	（4）	本業務の遂行において情報セキュリティが侵害され、又はそのおそれがある場合には、速やかに必要な措置を講ずるとともに、会館に報告すること。また、会館の指示があったときには、その指示に従うものとする。								
	（5）	会館から情報セキュリティ対策の履行状況の確認を求められた場合には、速やかに状況等を報告すること。また、会館は、必要があると認められるときは、情報セキュリティ対策の実施状況を確認する為の調査をする場合がある。								

	（6）	会館との秘密情報の受け渡しは、安全管理措置が講じられた方法を採用すること。また、本業務完了又は契約解除等により、会館が提供した紙媒体及び電子媒体（これらの複製を含む）が不要になった場合には、速やかに会館に返却又は破砕、溶解及び焼却等の方法により情報を復元困難かつ判読不能な方法で破棄若しくは消去し会館に書面にて報告すること。ただし、会館が別段の指示をしたときは、その指示に従うものとする。					必須			
	（7）	会館が貸出した資料等については、十分な注意を払い、紛失又は滅失しないよう万全の措置を取ること。								
	（8）	本プロジェクトに従事するものを限定し、情報取扱者名簿を作成し、会館に提出すること。また、受託者の資本関係・役員の情報、本業務の実施場所、本業務の全ての従事者の所属、専門性（情報セキュリティに係る資格・研修実績等）に関する情報を会館に提供すること。なお、本業務の実施期間中に従事者を変更等する場合は、事前にこれらの情報を会館に再提供すること。								
	（9）	本業務に関わるインシデントが発生した場合の対処方法について、事前に会館と協議し決定すること。また、インシデント発生時は、決定した対処方法に基づく対応を行うこと。								
	（10）	再委託・下請負を行う場合、事前に会館の承認を得ることとし、再委託・下請負することにより生じる脅威に対して情報セキュリティが十分に確保されるように再委託・下請負先に担保させ、受託者の責任において、再委託・下請負先の情報セキュリティ対策の実施状況を確認すること。								
	（11）	作業環境及び作業工程において、セキュリティを維持するための手順及び環境を定めること。								
	（12）	上記（1）～（11）の要件を達成できなくなった場合、又はその恐れが予見された場合は、必要となる改善策を提案し、会館と協議の上実施すること。								
9.受託者の要件										
	（1）	受託者は、以下の要件を満たすことを証明する書類の写しを提出すること。								
	①	一般社団法人日本情報経済社会推進協会の認定するプライバシーマークまたは情報セキュリティマネジメントシステム適合性評価制度の認証ISO/IEC 27001を取得していること。					必須			
	②	大学図書館または専門図書館へのクラウドシステムの導入実績が１０館以上あること。								
	（2）	以下のワーク・ライフ・バランス等の推進に関する取組への政府機関の認定を受けている事業者は加点する。								
	①	女性の職業生活における活躍の推進に関する法律（平成27年法律第64号）に基づく認定等（えるぼし、プラチナえるぼし認定企業等）					加点	35		
	②	次世代育成支援対策推進法（平成15年法律第120号）に基づく認定（トライくるみん、くるみん、プラチナくるみん認定企業等）								
	③	青少年の雇用の促進等に関する法律（昭和45年法律第98号）に基づく認定（ユースエール認定企業）								

【評価・採点基準】

評価	詳細	採点	点数
非常に優れている	大変優れた提案がなされ、すべて具体的に説明されており、また、その内容に矛盾がない。	満点	配点の100%
やや優れている	優れた提案がなされ、必要な説明がされている。	部分点	配点の80%
普通	仕様を満たす最低限の提案がなされ、必要な説明がされている。	部分点	配点の50%（小数点以下は切り捨て）
不可	仕様を満たさない。説明がない。又は、説明が不適切（誤り、矛盾、不十分等）である。	なし	0

認定	認定等の区分	項目別得点
女性活躍推進法に基づく認定（えるぼし認定企業・プラチナえるぼし認定企業）	プラチナえるぼし	35
	認定基準〇（5）	30
	認定基準〇（3～4）	20
	認定基準〇（1～2）	10
	行動計画	5
次世代法に基づく認定（くるみん認定企業・プラチナくるみん認定企業）	プラチナくるみん認定企業（令和7年4月以降基準）	35
	プラチナくるみん認定企業（令和7年3月以前基準）	30
	くるみん認定企業（令和7年4月以降基準）	25
	くるみん認定企業（令和4年4月～令和7年3月基準）	20
	くるみん認定企業（平成29年～令和4年3月基準）	15
	トライくるみん	10
	くるみん認定企業（平成29年以前基準）	5
若者雇用促進法に基づく認定（ユースエール認定企業）		15

複数の認定を取得している場合、得点が最も高い項目の得点を加点する。

（様式５）

暴力団等反社会的勢力でないこと等に関する表明・確約書

独立行政法人国立女性教育会館
事務局長　磯山武司　　殿

法人名：
住　所：
代表者氏名：
昭和・平成　　年　　月　　日生（　　歳）

１．私及び当社（以下「私」という。）は、現在又は将来にわたって、次の各号の反社会的勢力のいずれにも該当しないことを表明、確約〈**いたします・いたしません**〉。
①暴力団　　②暴力団員　　③暴力団準構成員　　④暴力団関係企業
⑤総会屋等　　⑥社会運動等標ぼうゴロ　　⑦特殊知能暴力集団等
⑧暴力団員でなくなってから５年を経過していない者
⑨その他暴力、威力又は詐欺的手法を駆使し経済的利益を追求する者

２．私は、現在又は将来にわたって、前項の反社会的勢力又は反社会的勢力と密接な交友関係にある者（以下「反社会的勢力等」という。）と次の各号のいずれかに該当する関係がないことを表明、確約〈**いたします・いたしません**〉。
①反社会的勢力等によって、その経営を支配されている関係
②反社会的勢力等が、その経営に実質的に関与している関係
③自己、自社若しくは第三者の不正の利益を図り、又は第三者に損害を加えるなど、反社会的勢力を利用している関係
④反社会的勢力等に対して資金等を提供し、又は便宜を供与するなどの関係
⑤その他役員等又は経営に実質的に関与している者が、反社会的勢力等との社会的に非難されるべき関係

３．私は、自ら又は第三者を利用して次の各号のいずれの行為も行わないことを表明、確約〈**いたします・いたしません**〉。
①暴力的な要求行為
②法的な責任を超えた不当な要求行為
③取引に関して脅迫的な言動をし、または暴力を用いる行為
④風説を流布し、偽計又は威力を用いて貴法人の信用を毀損し、又は貴法人の業務を妨害する行為
⑤その他前各号に準ずる行為

（２頁に続く）

（様式５）

４．私は、下請け又は再委託先業者（下請け又は再委託契約が数次にわたるときは、その全てを含む。以下同じ。）との関係において、次の各号のとおりであることを表明、確約〈**いたします・いたしません**〉。

①下請け又は再委託先業者が前１及び２に該当せず、将来においても前１、２及び３に該当しないこと

②下請け又は再委託先業者が前号に該当することが判明した場合には、直ちに契約を解除し、又は契約解除のための措置をとること

５．私は、下請け又は再委託先業者が、反社会的勢力から不当要求又は業務妨害等の不当介入を受けた場合は、これを拒否し、又は下請け又は再委託先業者をしてこれを拒否させるとともに、速やかにその事実を貴法人に報告し、貴法人の捜査機関への通報に協力することを表明、確約〈**いたします・いたしません**〉。

６．私は、これら各項のいずれかに反したと認められることが判明した場合及び、この表明、確約が虚偽の申告であることが判明した場合は、催告なしでこの取引が停止され又は解約されても一切異議を申し立てず、また賠償ないし補償を求めないとともに、これにより損害が生じた場合は、一切私の責任とすることを表明、確約〈**いたします・いたしません**〉。

令和　　年　　月　　日

（ふりがな）
署　　名 ＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿ ㊞

提出前に再確認ください。
☐全ての〈いたします・いたしません〉、どちらかにマルが記されていること。
不明な点がある場合は会館までお問い合わせください。
0493-62-6717（独）国立女性教育会館財務・企画課　会計・施設係：宇佐美

様式６

事業者要件のうち実績に関する証明書

提出日	令和７年　月　日
事業者名	

「９．受託者の要件（１）②」に関して、過去に大学図書館または専門図書館へのクラウドシステムについて、以下の取引実績（10 館以上）があることを証明します。

・大学図書館または専門図書館

取引先名	クラウドシステムの取引の期間

以上

様式7①

参 考 見 積 書

件名：次期図書館業務システムの導入及び運用保守業務一式

入札金額　金　　円也

（消費税に係る課税業者であるか免税業者であるかを問わず、見積もった金額の110分の100に相当する金額）

令和　　年　　月　　日

入札者住所

法人名

代表者氏名

印

様式7②

参考見積書・内訳書

金額及び金額の合計は自動的に入力されますが、誤りがないか確認してください

件名：次期図書館業務システムの導入及び運用保守業務一式

入札者氏名：

法人の場合は、その名称又は商号及び代表者の氏名を記載してください

黄色のセルに税込相当の単価を入力してください

件名		数量	単価		金額
構築業務一式		1		円	0 円
運用保守		60		円/月	0 円
合計					0 円
合計（上記金額の110分の100）					0 円

様式8①

入 札 書

内訳書からリンクしていますが、金額に誤りがないか確認してください

件名：次期図書館業務システムの導入及び運用保守業務一式

入札金額　金　　0 円也

（消費税に係る課税業者であるか免税業者であるかを問わず、見積もった金額の110分の100に相当する金額）

仕様書に従って上記の役務を請負うものとして、入札に関する条件を承諾のうえ、上記の金額によって入札します。

入札書受領期限以前の入札書作成日を記載してください

令和　　年　　月　　日

独立行政法人国立女性教育会館　事務局長殿

法人の場合は、その名称又は商号及び代表者の氏名を記載してください

入札者住所

法人名

代表者氏名　　印

代理人が入札する場合に氏名を記載してください（代理人を定めない場合は削除してください）

代理人

氏名　　印

復代理人が入札する場合に氏名を記載してください（復代理人を定めない場合は削除してください）

復代理人

氏名　　印

様式８②

内 訳 書

金額及び金額の合計は自動的に入力されますが、誤りがないか確認してください

件名：次期図書館業務システムの導入及び運用保守業務一式

入札者氏名：

法人の場合は、その名称又は商号及び代表者の氏名を記載してください

黄色のセルに税込相当の単価を入力してください

件名		数量	単価		金額
構築業務一式		1		円	0 円
運用保守		60		円/月	0 円
合計					0 円
合計（上記金額の110分の100）					0 円

（別紙様式９）

委　　任　　状

令和　　年　　月　　日

独立行政法人国立女性教育会館　　御中

委任者（競争加入者）　住　　所

法 人 名 称

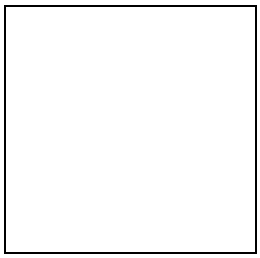
代表者氏名　　印

私は、＿＿＿＿＿＿＿＿＿＿＿＿を代理人と定め、下記の一切の権限を委任します。

記

１．　**令和７年10月３日公告**の独立行政法人国立女性教育会館において行われる
「次期図書館業務システムの導入及び運用保守業務一式」の
一般競争入札に関する件

受任者（代理人）使用印鑑



（別紙様式１０）

委　　任　　状（復）

令和　　年　　月　　日

独立行政法人国立女性教育会館　　御中

委任者（競争加入者）　住　所

名　称

氏　名　　印

私は、＿＿＿＿＿＿＿＿＿＿を＿＿＿＿＿＿＿＿＿＿の復代理人と定め、

下記の一切の権限を委任します。

記

令和７年 10 月３日公告の独立行政法人国立女性教育会館において行われる
「次期図書館業務システムの導入及び運用保守業務一式」の
一般競争入札に関する件

受任者（復代理人）使用印鑑