入　札　説　明　書

【電子入札システム対応】

マイナンバー等収集管理及び法定調書作成支援業務

令和８年２月

国立研究開発法人国立環境研究所

当研究所の一般競争に係る入札公告（令和８年２月６日付）に基づく入札については、関係法令に定めるもののほか、この入札説明書による。

１．競争入札に付する事項

（１）件　　名　【電子入札システム対応】マイナンバー等収集管理及び法定調書作成支援業務
（２）契約期間　令和８年４月１日から令和１１年３月３１日まで
（３）仕　　様　仕様書による。
（４）履行場所　仕様書による。
（５）入札保証金　免除
（６）契約保証金　免除

２．競争参加に必要な資格

（１）令和７・８・９年度環境省競争参加資格（全省庁統一資格）の「役務の提供等」の「情報処理」又は「その他」において、「Ａ」、「Ｂ」又は「Ｃ」の等級に格付けされている者であること。
（２）国立研究開発法人国立環境研究所契約事務取扱細則第５条の規定に該当しない者であること。なお、未成年者、被保佐人又は被補助人であって、契約締結のために必要な同意を得ている者については、同条中、特別の理由がある場合に該当する。
（３）国立研究開発法人国立環境研究所契約事務取扱細則第６条の規定に該当しない者であること。
（４）契約者等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。
（５）入札説明書において示す暴力団排除等に関する誓約事項に誓約できる者であること。
（６）「ＩＳＯ２７００１（ＩＳＭＳ）」とプライバシーマークの資格を取得していること。
（７）本業務で取り扱う情報の保管、保存場所は「データセンターファシリティスタンダードティア３」相当以上の施設であること。
（８）本業務で取り扱うマイナンバー情報を保管するシステム及びWeb収集に用いるシステムについて、クラウドサービスを利用する場合には、「政府情報システムのためのセキュリティ評価制度（ISMAP）」の登録を受けていることを原則とする。ISMAPに未登録の場合は、別添３の管理基準表を提出し、ISMAP管理基準と同等のセキュリティ対策が可能であることを証明すること。

３．入札心得

（１）入札参加者は、仕様書及び添付書類を熟読のうえ、入札しなければならない。
（２）入札参加者は、前項の書類について疑義があるときは、関係職員の説明を求めることができる。
（３）入札参加者は、入札後、仕様書及び添付書類についての不明等を理由として異議を申し立てることはできない。

４．電子入札システムの利用

本件調達は電子入札システムで行うため、同システムの電子認証（代表者又はその委任を受けた者のＩＣカードに限る。）を取得していること。

・https://www.ebs-cloud.fwd.ne.jp/CALS/Accepter/index.jsp?name1=06A0064006A00600

また、同システム使用にあたっては、業者番号が発行されている必要があり、８．（１）①の提出の際に必要になる。業者番号発行の手続きについては、以下 URL の「電子入札システムの導入について」を参照のこと。

・https://www.nies.go.jp/osirase/chotatsu/kokoku/

なお、同システムによりがたい者は、発注者に申し出た場合に限り紙入札方式によることができる。

５．入札及び開札の日時及び場所

令和８年３月１１日（水）１０時３０分
国立研究開発法人国立環境研究所　研究本館Ⅱ　１階　第１会議室

（茨城県つくば市小野川１６－２）

６．入札説明書等に対する質問

（１） 入札説明書、添付資料等に対する質問がある場合においては、次に従い、質問書を提出すること。

①提出期間：令和８年２月６日（金）から令和８年２月１３日（金）１６時００分まで。

②提出場所：〒３０５－８５０６
茨城県つくば市小野川１６－２
国立研究開発法人国立環境研究所　総務部会計課契約第一係
ＴＥＬ　０２９－８５０－２７７５　（担当：濱田）

③提出方法：電子メールによるデータ（指定様式（※））の送付とする（データ送付先:chotatsu@nies.go.jp）。なお、メールの件名を【質問の提出（マイナンバー等収集管理及び法定調書作成支援業務）（担当：濱田）】とすること。
※当研究所ＷＥＢサイトに掲載（本公告掲載先と同一ページ）

（２）（１）の質問に対する回答書は、次のとおり閲覧に供する。

①期　　間：令和８年２月１９日（木）１０時００分から
令和８年３月１１日（水）１０時３０分まで。

②閲覧場所：当研究所ＷＥＢサイト（本公告掲載先と同一ページ）

（３）（１）の質問がない場合、（２）については行わないものとする。

７．入札参加資格証明書類等の提出

入札に参加しようとする者は、本入札説明書２．（１）、（６）、（７）及び（８）の証明書類を次に従い提出すること。

（１）提出書類

競争参加に必要な資格	提出書類
２．（１）	全省庁統一資格の写し。
２．（６）	ＩＳＯ２７００１マネジメントシステム登録証及びプライバシー登録証の写し。
２．（７）	「データセンターファシリティスタンダード ティア３」相当以上の施設であることが確認できる資料。
２．（８）	利用予定のクラウドサービスについて、「政府情報システムのためのセキュリティ評価制度（ISMAP）」の登録を受けている場合は登録されていることが確認できる資料。受けていない場合は別添３の管理基準表。 ※クラウドサービスを利用しない場合は提出不要。

（２）提出期限：令和８年２月２６日（木）１６時００分
持参する場合の受付時間は、平日の１０時から１６時まで（１２時から１３時を除く）とする。

（３）書面による提出の場合

ア．提出方法　持参又は郵送によって提出すること。ただし、郵送する場合には、書留郵便等の配達の記録が残るものに限る。

イ．提出場所　６．（１）②の場所

ウ．提出部数　２部（提出書類を綴じ込んだ一式）

（４）電子による提出の場合

ア．提出方法　電子ファイル（ＰＤＦ形式）により、電子メールで送信。メールの件名は【入札参加資格証明書類の提出（マイナンバー等収集管理及び法定調書作成支援業務）（担当：濱田）】とすること。

イ．提出場所　chotatsu@nies.go.jp

（５）提出された書類による本競争参加の可否については、次の期間までに連絡をする。

①期　　間：入札日及び開札の２営業日前１７時００分。

８．入札及び開札

（１）電子入札の場合

①電子入札システムにより入札をする予定の者については、同システムにより、入札者又は代理人等の電話連絡先（開札時、開札執行員等からの電話を確実に受けられる番号と

すること。）が記載された書類をＰＤＦ化し添付の上、７．（２）の日時までに提出すること。

②５．の日時までに、同システムに定める手続に従って入札を行うこと。通信状況によっては当該期限内に入札情報が到着しない場合があるので、時間的余裕を持って行うこと。

③入札金額については、１．（１）の業務に関する一切の費用を含めた額とする。

④落札決定に当たっては、入札書に記載された金額に課税対象金額の１０％に相当する額を加算した金額（当該金額に１円未満の端数があるときは、その金額を切り捨てるものとする）をもって落札価格とするので、入札参加者は、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から課税額を除いた金額を入力するものとする。

⑤同システムにより入札した場合には、本入札説明書において示す暴力団排除等に関する誓約事項に誓約したものとして取り扱うこととする。

⑥入札者又は代理人等は、開札時刻に同システムの端末の前で待機しなければならない。

⑦事由のいかんにかかわらず入札の引換え、変更又は取消しを行うことができない。

⑧入札参加者が連合し、又は不穏の行動をなす等の場合において、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、当該入札参加者を入札に参加させず、又は入札の執行を延期し、若しくは取りやめることがある。

（２）紙入札の場合

①紙入札での参加については、紙入札方式参加届（別紙１）を７．（２）の日時までに６．（１）②の場所へ持参、郵送又は電子メール（chotatsu@nies.go.jp）により提出すること。

②入札書（別紙２）には、入札参加者の住所、氏名を記入し、金額の記入はアラビア数字を用いて鮮明に記載すること。なお、郵送による提出の際は入札書に入札回数（第○回）を記載すること。

③入札書及び入札に係る文書に使用する言語は、日本語に限るものとし、また入札金額は、日本国通貨による表示に限るものとする。

④入札金額については、１．（１）の業務に関する一切の費用を含めた額とする。

⑤落札決定に当たっては、入札書に記載された金額に課税対象金額の１０％に相当する額を加算した金額（当該金額に１円未満の端数があるときは、その金額を切り捨てるものとする）をもって落札価格とするので、入札参加者は、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から課税額を除いた金額を入札書に記載するものとする。

⑥入札書は、別紙の書式により作成し、封かんの上で持参又は郵送により提出するものとする。

⑦入札書を持参する場合は、入札書を封かんし、入札参加者の商号又は名称、入札件名及び開札日時を記載し、入札及び開札日に入札箱に投入すること。

⑧当面の間郵送による入札書の提出は３通まで認めることとする。入札書を郵送により提出する場合は、二重封筒とし、表封筒に入札書在中の旨を朱書し、中封筒に入札参加者の入札参加者の商号又は名称、入札件名及び開札日時並びに入札回数（○回目）を記載して書留郵便（配達証明付）により、次に従い郵送すること。

提出期限：入札及び開札の前日（※）１６時００分

※土・日曜日、祝祭日及び年末年始（１２月２９日から１月３日）を除く。

提出場所：本入札説明書６．（１）②と同じ

⑨入札参加者は、入札書を提出する際には、本入札説明書２．（１）の競争参加資格を有することを証明する書類を提出すること。

⑩入札参加者は、代理人又は復代理人（以下「代理人等」という。）をして入札させるときは、その委任状（別紙３、４）を持参させなければならない。なお、⑧により入札書を郵送する場合も同様とし、入札書を郵送する際に委任状を同封するものとする。

⑪入札参加者又はその代理人等は、当該入札に対する他の入札参加者の代理をすることができない。

⑫開札は、入札参加者の面前で行う。ただし、入札参加者又はその代理人等が開札場所に出席しないときは、入札執行事務に関係のない職員を立会させて開札する。この場合、異議の申し立てはできない。

⑬入札参加者又はその代理人等は、開札時刻後においては、開札場に入場することはできない。
⑭提出済の入札書は、その事由のいかんにかかわらず引換え、変更又は取消しを行うことができない。
⑮入札参加者が連合し、又は不穏の行動をなす等の場合において、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、当該入札参加者を入札に参加させず、又は入札の執行を延期し、若しくは取りやめることがある。

９．入札の無効

次の各号に該当する入札書は無効とする。

（１）競争に参加する資格を有しない者の提出した入札書
（２）委任状を提出しない代理人等の提出した入札書
（３）記名を欠いた入札書
（４）入札金額の記載が不明確な入札書
（５）入札金額の記載を訂正した入札書
（６）誤字、脱字等により意志表示が不明瞭である入札書
（７）明らかに連合によると認められる入札書
（８）同一事項の入札について、他の入札参加者の代理人等を兼ねた者の入札書
（９）同一入札執行回について、入札参加者又はその代理人等が二通以上の入札書を提出した場合
（10）その他の入札に関する条件に違反した入札書

１０．落札の決定

本入札説明書２の競争参加資格及び仕様書等の要求要件を全て満たし、当該入札書の入札価格が国立研究開発法人国立環境研究所契約事務取扱細則第１３条の規定に基づいて作成された予定価格の範囲内で、最低の価格をもって有効な入札を行った者を落札者とする。ただし、落札者となるべき者の入札価格によっては、その者により当該契約の内容に適合した履行がなされないおそれがあると認められるとき又は、その者と契約を締結することが公正な取引の秩序を乱すこととなるおそれがあって著しく不適当であると認められるときは、予定価格の制限の範囲内の価格をもって入札した他の者のうち最低の価格をもって入札した者を落札者とする。

１１．再度入札

開札した場合において、入札参加者の入札のうち予定価格の制限に達した価格の入札が無いときは、直ちに再度の入札を行う。なお、以下の事項に留意すること。

・再度入札の時刻は入札執行者（弊所職員）が指定する（電子入札による応札を行う場合は特に留意すること。）。
・再度入札の回数は原則として２回を限度とする。ただし、郵便による入札を行い、開札当日に入札参加者又はその代理人等が開札場所に出席しないときは、入札書の提出数以降の再度入札による入札に参加できないため注意すること。

１２．低入札価格調査制度の実施

（１）本調達は、落札者となるべき者の入札価格が国立環境研究所の規定する基準価格より下回った場合に低入札価格調査を行う。
（２）落札者となるべき者の入札価格が、基準価格を下回った場合、開札執行者は入札者に対して「保留」の旨宣言し、落札者は後日決定する旨を告げて開札を終了する。
（３）その後、国立環境研究所において、入札者からの事情聴取、関係機関への照会等の調査を行う。入札者は、事情聴取及び当所から求められた書類の提出について協力すること。
（４）（３）に基づき調査を行った後の結果の通知は以下による。
①調査の結果、契約の内容に適合した履行がされると認められた場合には、直ちに（２）の落札者となるべき者に落札した旨を通知するとともに、他の入札者全員に対してその旨を通知する。
②調査の結果、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、（２）

の落札者となるべき者以外の者が落札者として決定された場合には、当該落札者には落札者となった旨の必要な通知を行い、最低価格入札者には落札者とならなかった理由等を通知する。併せて他の入札者全員に対して落札決定があった旨を通知する。

１３．同価格の入札が２人以上ある場合の落札者の決定

（１）落札者となるべき同価格の入札をした者が２人以上あるときは、電子入札システムによる電子くじにより落札者を決定する。電子入札システムにより入札を行う場合は、入札時に任意の３桁の数字を入力すること。紙入札による場合は、入札書（別紙２）の記載欄に任意の３桁の数字を記載すること。なお、入力された数字は乱数処理により変換された数字により落札者を決定するため、指定した数字が直接判定に用いられるものではない。

（２）前項の場合において、数字の指定を行わない者があるときは、職員が任意の数字を入力する。

１４．落札内訳書の提出

（１）落札者は、落札者の決定後すみやかに落札額に応じた内訳書を提出すること。なお、内訳書は、可能な限り詳細に記載すること。

（２）内訳書の様式は自由とする。

（３）内訳書は返却しない。

１５．契約書等の提出

（１）契約書を作成する場合においては、落札者は、契約担当者等から交付された契約書の案に記名押印し、速やかにこれを契約担当者等に提出しなければならない。

（２）契約書及び契約に係る文書に使用する言語及び通貨は、日本語及び日本国通貨による。

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

１６．その他

（１）再委託等の制限

落札者は、業務の処理を第三者（再委託等先が乙の子会社（会社法（平成１７年法律第８６号）第２条第３号に規定する子会社をいう。）である場合も含む。以下同じ。）に委託し又は請け負わせてはならない。但し、再委託等承認申請書（別紙）を書面により申請し、承認を得たときは、この限りではない。

※再委託等の取り扱いについては、仕様書及び「契約における再委託等の取扱いについて」（当研究所ＨＰに掲載）を参照すること。

掲載先：https://www.nies.go.jp/osirase/chotatsu/saiitaku.pdf

１７．契約者の氏名

国立研究開発法人国立環境研究所　　理事長　　木本　昌秀

１８．入札結果及び契約情報の公表について

①　入札結果の公表

落札者が決定したときは、その入札結果（落札者を含めた入札者全員の商号又は名称及び入札価格）について、開札場において発表するとともに電子入札システム及び入札情報公開システムにおいて公表する予定である。

②　契約情報の公表

契約を締結したときは、後日当該契約情報を当法人のＷＥＢサイトにおいて公表する。

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、情報を公開する等の取組を進めることとされている。これに基づき、以下のとおり、当法人との関係に係る情報を当法人のＷＥＢサイトで公表することとするので、所要の情報の当法人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お願いする。なお、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すこととする。

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

ア．当法人において役員を経験した者が再就職をしていること又は課長相当職以上の職を経験した者が役員、顧問等として再就職していること

イ．当法人との間の取引高が、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

2) 公表する情報

上記に該当する契約先との契約（予定価格が一定の金額を超えない契約や光熱水料の支出に係る契約等は対象外）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する。

ア．前記②1)アに該当する再就職者の人数、職名及び当法人における最終職名

イ．当法人との間の取引高

ウ．総売上高又は事業収入に占める当法人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

・３分の２以上

エ．一者応札又は一者応募である場合はその旨

3) 提供を求める情報

ア．契約締結時点における前記②1)アに該当する再就職者に係る情報（人数、職名及び当法人における最終職名）

イ．直近の事業年度における総売上高又は事業収入及び当法人との間の取引高

4) 公表の時期

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

１９．電子入札システムの操作及び障害発生時の問合せ先

電子入札システム ポータルサイトアドレス

：https://www.nies.go.jp/osirase/chotatsu/kokoku/e-bidding/index.html

ヘルプデスク 0570-021-777（受付時間：平日 9:00～12:00 及び 13:00～17:30）

Email:sys-e-cydeenasphelp.rx@ml.hitachi-systems.com

◎添付資料

・別紙１　紙入札方式参加届
・別紙２　入札書
・別紙３　委任状（代理人用）
・別紙４　委任状（復代理人用）
・別紙５　暴力団排除等に関する誓約事項
・（各種規程）国立研究開発法人国立環境研究所契約事務取扱細則（抄）
・（参考）　紙入札に当たっての留意事項
・別添１　契約書（案）
・別添２　仕様書
・別添３　ISMAP 管理基準表

（別紙１）

年　　月　　日

紙 入 札 方 式 参 加 届

国立研究開発法人国立環境研究所理事長　殿

住　　所
商号又は名称
代 表 者 名

下記入札案件について、紙入札方式での参加をいたします。

件名：　マイナンバー等収集管理及び法定調書作成支援業務

担当者等連絡先
部署名　：
担当者名：
責任者名：
ＴＥＬ　：
E-mail　：

（別紙２）

入　　札　　書

金 ＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿円＿＿＿

※仕様書（別紙含む）で示す業務内容及び予定件数等により積算した総価を記載（電子入札システムでは入力）すること。なお、記載（入力）に当たっては、仕様書（別紙）の留意事項も参照すること。

電子くじに入力する数字（任意の３桁）：

件名　マイナンバー等収集管理及び法定調書作成支援業務

上記金額をもって貴所入札説明書承諾のうえ入札します。
御採用のうえは確実に履行いたします。
なお、入札説明書別紙５の暴力団排除等に関する誓約事項に誓約します。

年　　月　　日

住　　　所

商号又は名称

代 表 者 名

国立研究開発法人国立環境研究所　理事長　殿

担当者等連絡先
部署名　：
担当者名：
責任者名：
ＴＥＬ　：
E-mail　：

<記入例>

入　　札　　書

金　＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿円＿＿＿

※仕様書で示す業務内容及び業務契約期間に係る一切の費用を記載（電子入札システムでは入力）すること。
※仕様書（別紙含む）で示す業務内容及び予定件数等により積算した総価を記載（電子入札システムでは入力）すること。なお、記載（入力）に当たっては、仕様書（別紙）の留意事項も参照すること。

電子くじに入力する数字（任意の３桁）：

件名　マイナンバー等収集管理及び法定調書作成支援業務

上記金額をもって貴所入札説明書承諾のうえ入札します。
御採用のうえは確実に履行いたします。
なお、入札説明書別紙５の暴力団排除等に関する誓約事項に誓約します。

××年××月××日

住　　　所　　○○県○○市○○１－２－３

商号又は名称　　株 式 会 社 △ △ △ △

代 表 者 名　　代表取締役 □ □ □ □

<（復）代理人 ◎ ◎ ◎ ◎　　>

※代理人又は復代理人が入札する際は、代表者に代わり代理人又は復代理人が記名すること

国立研究開発法人国立環境研究所　理事長　殿

担当者等連絡先
部署名　：
担当者名：
責任者名：
ＴＥＬ　：
E-mail　：

（別紙３）

年　　月　　日

委　任　状

国立研究開発法人国立環境研究所　理事長　殿

住　　所
商号又は名称
代 表 者 名

今般、私は、　　を代理人と定め、令和８年２月６日付け公示された国立研究開発法人国立環境研究所の「マイナンバー等収集管理及び法定調書作成支援業務」に関し、下記の権限を委任いたします。

受任者：住　　所

商号又は名称

役 職 ・ 氏 名

記

1. 本入札に係る一切の権限
2. 1. の事項に係る復代理人を選任すること

担当者等連絡先
部署名　：
担当者名：
責任者名：
ＴＥＬ　：
E-mail　：

（別紙４）

年　　月　　日

委　任　状

国立研究開発法人国立環境研究所　理事長　殿

住　　所
商号又は名称
氏　　名

今般、私は、　　を復代理人と定め、令和８年２月６日付け公示された国立研究開発法人国立環境研究所の「マイナンバー等収集管理及び法定調書作成支援業務」に関し、下記の権限を委任いたします。

受任者：住　　所

商号又は名称

役職・氏名

記

1.本入札に係る一切の権限

担当者等連絡先
部署名　：
担当者名：
責任者名：
ＴＥＬ　：
E-mail　：

（別紙５）

暴力団排除等に関する誓約事項

当社（個人である場合は私、団体である場合は当団体）は、下記事項について、入札書（見積書）の提出をもって誓約いたします。

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

また、国立研究開発法人国立環境研究所（以下「貴所」という。）の求めに応じ、当方の役員名簿（有価証券報告書に記載のもの（生年月日を含む。）。ただし、有価証券報告書を作成していない場合は、役職名、氏名及び生年月日の一覧表）及び登記簿謄本の写しを提出すること並びにこれらの提出書類から確認できる範囲での個人情報を警察に提供することについて同意します。

記

１．次のいずれにも該当しません。また、将来においても該当することはありません。

（１）契約の相手方として不適当な者

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

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

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

エ 役員等が、暴力団又は暴力団員と社会的に非難されるべき関係を有しているとき

（２）契約の相手方として不適当な行為をする者

ア 暴力的な要求行為を行う者

イ 法的な責任を超えた不当な要求行為を行う者

ウ 取引に関して脅迫的な言動をし、又は暴力を用いる行為を行う者

エ 偽計又は威力を用いて国立研究開発法人国立環境研究所の業務を妨害する行為を行う者

オ その他前各号に準ずる行為を行う者

２．暴力団関係業者を再委託又は当該業務に関して締結する全ての契約の相手方としません。

３．再受任者等（再受任者、共同事業実施協力者及び自己、再受任者又は共同事業実施協力者が当該契約に関して締結する全ての契約の相手方をいう。）が暴力団関係業者であることが判明したときは、当該契約を解除するため必要な措置を講じます。

４．暴力団員等による不当介入を受けた場合、又は再受任者等が暴力団員等による不当介入を受けたことを知った場合は、警察への通報及び捜査上必要な協力を行うとともに、発注元の貴所へ報告を行います。

５．貴所の規程類及び法令を遵守して不正、不適切な行為に関与せず、また、貴所の職員等から不正行為の依頼等があった場合には拒絶するとともに、その内容を貴所に通報し、さらに内部監査、その他調査等において、取引帳簿の閲覧・提出等の要請に協力します。

（参考）国立研究開発法人国立環境研究所　規程・規則等
https://www.nies.go.jp/kihon/kitei/

（各種規程）

国立研究開発法人国立環境研究所契約事務取扱細則（抄）

第２章　一般競争契約

（一般競争に参加させることができない者）

第５条　契約責任者は、特別の事由がある場合を除くほか、当該契約を締結する能力を有しない者及び破産者で復権を得ない者を会計規程第３４条第１項の規程による一般競争に参加させることができない。

（一般競争に参加させないことができる者）

第６条　契約責任者は、次の各号の一に該当すると認められる者を、その事実があった後２年間一般競争に参加させないことができる。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、また同様とする。

（１）契約の履行にあたり、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

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

（３）落札者が契約を結ぶこと又は契約者が契約を履行することを妨げた者

（４）監督又は検査の実施に当たり職員の職務の執行を妨げた者

（５）正当な理由がなくて契約を履行しなかった者

（６）前各号の一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、支配人その他使用人として使用した者

２　契約責任者は、前項の規定に該当する者を入札代理人として使用する者を一般競争に参加させないことができる。

（予定価格の作成）

第１３条　契約責任者は、その競争入札に付する事項の価格を当該事項に関する仕様書、設計書等によって予定し、その予定価格を記載した書面を封書にし、開札の際これを開札場所に置かなければならない。

（参　考）

紙入札に当たっての留意事項

１．本調達に関する質問回答について
　本調達に関する質問回答書は当研究所ＷＥＢサイト（本公告掲載先と同一ページ）で閲覧可能である。

２．入札書について
　入札書については、応札者において適当部数コピーの上、記名し用意すること。
　なお、代理人をもって入札する場合の記名は、必ず委任状で委任される者のものと同一とする。

３．委任状について
１）代理人が応札する場合には必ず委任状を提出すること。
２）本社（代表者等）から直接委任を受ける場合には、代理人の委任状（別紙３）を、支社等を経由して委任を受ける場合には、支社長等への代理人の委任状（別紙３）と支社長等から復代理人への委任状（別紙４）の両方を用意すること。

４．**資格審査結果通知書の写しを用意すること。**

５．**郵送による入札を行う場合においても、資格審査結果通知書の写し等必要書類を提出すること。**

（別添１）

契　約　書（案）

国立研究開発法人国立環境研究所　理事長　木本　昌秀（以下「甲」という。）と、（以下「乙」という。）とは、次の条項により契約を締結する。

１．件　　名　　マイナンバー等収集管理及び法定調書作成支援業務

２．契 約 金 額　　総額　金　　円（うち消費税額及び地方消費税額　　円）
年額　金　　円（うち消費税額及び地方消費税額　　円）
に別表（単価表）に定める金額（消費税額及び地方消費税額別途）を加算した金額とする。

３．契 約 期 間　　自　令和８年４月１日　　至　令和１１年３月３１日

４．契約保証金　　免除

５．契約履行の場所及び業務内容　別添仕様書のとおり

（信義誠実の原則）
第１条　甲乙両者は、信義を重んじ誠実に本契約を履行しなければならない。

（権利義務の譲渡等）
第２条　乙は、本契約によって生じる権利又は義務の全部若しくは一部を、甲の承諾を得た場合を除き第三者に譲渡し、又は承継させてはならない。ただし、信用保証協会及び中小企業信用保険法施行令（昭和２５年政令第３５０号）第１条の３に規定する金融機関に対して売掛債権を譲渡する場合にあっては、この限りでない。

（義務の履行）
第３条　乙は、別添仕様書に基づき、頭書の金額をもって頭書の期間中に義務を完全に履行しなければならない。

（再委託等の禁止）
第４条　乙は、業務の処理を第三者（再委託等先が乙の子会社（会社法（平成１７年法律第８６号）第２条第３号に規定する子会社をいう。）である場合も含む。以下同じ。）に委託し又は請け負わせてはならない。但し、再委託等承認申請書（別紙）を甲に提出し、甲の承認を得たときは、この限りではない。

（監督職員）
第５条　甲は、乙の業務実施について、自己に代って監督又は指示する監督職員を選定することができる。
２　監督職員は、本契約書及び仕様書に定められた事項の範囲内において業務の施行に立会い、又は必要な指示を与えることができる。

（業務の報告等）
第６条　甲は、必要と認めたときは、乙に対して業務の実施状況について報告を受け、又は説明を求める等の措置をとることができる。
２　乙は、甲が前項の報告を依頼し、又は書類の提出を求めたときはすみやかにこれに応じるものとする。

（業務内容の変更）
第７条　甲は、必要がある場合には、業務の内容を変更することができる。この場合において、契約金額又は契約期間を変更するときは、甲乙協議して書面によりこれを定めるものとする。
２　日本郵便株式会社が郵便料金の改定を発表した場合には、前項にかかわらず、乙は甲に対して改定後の郵便料金をすみやかに書面で通知し、日本郵便株式会社の適用開始日をもって別表（単価表）２．郵送費を更新する。

（契約の解除）
第８条　甲は、次の各号の一に該当するときは、催告することなくこの契約の全部又は一部を解除することができる。
一　乙の責に帰する事由により、乙がこの契約の全部又は一部を履行する見込みがないと認められるとき。
二　乙が第４条、第１７条又は第１８条の規定に違反したとき。
三　乙又はその使用人が甲の行う監督及び検査に際し不正行為を行い、又は監督者等の職務の執行を妨げたとき。
四　履行期限内に成果品の提出がなかったとき。
２　甲は、乙が次の各号の一に該当すると認められるときは、催告することなくこの契約を解除することができる。
一　法人等（個人、法人又は団体をいう。）の役員等（個人である場合はその者、法人である場合は役員又は支店若しくは営業所（常時契約を締結する事務所をいう。）の代表者、団体である場合は代表者、理事等、その他経営に実質的に関与している者をいう。）が、暴力団（暴力団員による不当な行為の防止等に関する法律（平成３年法律第７７号）第２条第２号に規定する暴力団をいう。以下同じ）又は暴力団員（同法第２条第６号に規定する暴力団員をいう。以下同じ。）であるとき
二　役員等が、自己、自社若しくは第三者の不正の利益を図る目的、又は第三者に損害を加える目的をもって、暴力団又は暴力団員を利用するなどしているとき
三　役員等が、暴力団又は暴力団員に対して、資金等を供給し、又は便宜を供与するなど直接的あるいは積極的に暴力団の維持、運営に協力し、若しくは関与しているとき
四　役員等が、暴力団又は暴力団員であることを知りながらこれを不当に利用するなどしているとき
五　役員等が、暴力団又は暴力団員と社会的に非難されるべき関係を有しているとき
３　甲は、乙が自ら又は第三者を利用して次の各号の一に該当する行為をした場合は、催告することなくこの契約を解除することができる。
一　暴力的な要求行為
二　法的な責任を超えた不当な要求行為
三　取引に関して脅迫的な言動をし、又は暴力を用いる行為
四　偽計又は威力を用いて甲等の業務を妨害する行為
五　その他前各号に準ずる行為
４　甲は、前三項の規定により、この契約の全部又は一部を解除した場合は、既に乙に支払

った契約金額の全部又は一部を乙に返還させることができる。

（再受任者等に関する契約解除）

第９条　乙は、契約後に再受任者等（再受任者、及び乙又は再受任者が当該契約に関して個別に契約する場合の当該契約の相手方をいう。以下同じ。）が第８条第２項及び第３項の一に該当する者（以下「解除対象者」という。）であることが判明したときは、直ちに当該再受任者等との契約を解除し、又は再受任者等に対し契約を解除させるようにしなければならない。

２　甲は、乙が再受任者等が解除対象者であることを知りながら契約し、若しくは再受任者等の契約を承認したとき、又は正当な理由がないのに前項の規定に反して当該再受任者等との契約を解除せず、若しくは再受任者等に対し契約を解除させるための措置を講じないときは、催告することなくこの契約を解除することができる。

（違約金）

第 10 条　次に掲げる場合のいずれかに該当したときは、乙は、甲の請求に基づき、契約金額の１００分の１０に相当する金額を違約金として甲の指定する期間内に支払わなければならない。

一　甲が第８条又は第９条第２項の規定により契約の全部又は一部を解除したとき。

二　乙について破産手続開始の決定があった場合において、破産法（平成１６年法律第７５号）の規定により選任された破産管財人が契約を解除したとき。

三　乙について更生手続開始の決定があった場合において、会社更生法（平成１４年法律第１５４号）の規定により選任された管財人が契約を解除したとき。

四　乙について再生手続開始の決定があった場合において、民事再生法（平成１１年法律第２２５号）の規定により選任された再生債務者等が契約を解除したとき。

五　この契約に関し、乙が私的独占の禁止及び公正取引の確保に関する法律（昭和２２年法律第５４号。以下「独占禁止法」という。）第３条の規定に違反し、又は乙が構成事業者である事業者団体が独占禁止法第８条第１号の規定に違反したことにより、公正取引委員会が乙に対し、独占禁止法第７条の２第１項（独占禁止法第８条の３において準用する場合を含む。）の規定に基づく課徴金の納付命令（以下「納付命令」という。）を行い、当該納付命令が確定したとき（確定した当該納付命令が独占禁止法第６３条第２項の規定により取り消された場合を含む。）。

六　この契約に関し、乙が独占禁止法第３条の規定に違反し、又は乙が構成事業者である事業者団体が独占禁止法第８条第１号の規定に違反したことにより、公正取引委員会が乙又は当該事業者団体（以下「乙等」という。）に対し、独占禁止法第７条若しくは第８条の２の規定に基づく排除措置命令（以下「排除措置命令」という。）を行い、当該排除措置命令が確定したとき。

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

八　この契約に関し、乙（法人にあっては、その役員又は使用人を含む。）の刑法（明治４

０年法律第４５号）第９６条の６又は独占禁止法第８９条第１項若しくは第９５条第１項第１号に規定する刑が確定したとき。

２　前項の規定は、甲に生じた実際の損害の額が違約金の額を超える場合において、甲がその超える分の損害を損害金として請求することを妨げない。

（報告）

第 11 条　乙は、作業終了後すみやかに甲に作業終了の報告をしなければならない。なお、本報告は仕様書に基づき、月毎及び年度毎に報告するものとする。

（検査）

第 12 条　甲は、前条の年度毎の報告があったときは、当該届出を受理した日から１０日以内に検査を行わなければならない。

（契約金の支払）

第 13 条 乙は、前条の検査に合格したときは、甲に当該年度における契約金の支払を請求するものとする。

２　甲は、前項の規定により、乙から適法な契約金の請求を受けたときは、請求書を受理した日から６０日以内に支払うものとする。

（損害賠償）

第 14 条　甲は、第８条又は第９条第２項の規定によりこの契約を解除した場合は、これにより乙に生じた損害について、何ら賠償ないし補償することは要しない。

（担保責任）

第 15 条　甲は、乙が本契約履行後に提出した成果品について１年以内に契約の内容に適合しないものであることを発見したときは、契約不適合である旨を乙に通知し、修補又は既に支払った契約金額の一部を返還させることができるものとする。

（延滞金）

第 16 条　乙は、第８条第４項の規定による契約金額の返還又は第１０条の規定による違約金等の支払いを甲の指定する期間内に行わないときは、当該期間を経過した日から支払いをする日までの日数に応じ、民法（明治２９年法律第８９号）第４０４条で定める法定利率で計算した額の延滞金を甲に支払わなければならない。

（守秘義務）

第 17 条　甲及び乙は、この契約の履行に際し、知り得た相手方の秘密を第三者に漏らし、又は利用してはならない。

（個人情報の取扱い）

第 18 条　乙は、甲から預託を受けた個人情報（生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述又は個人別に付された番号、記号その他の符号により当該個人を識別できるもの（当該情報のみでは識別できないが、他の情報と容易に照会することができ、それにより当該個人を識別できるものを含む。）をいう。以下同じ。）について、善良な管理者の注意をもって取扱う義務を負わなければならない。

２　乙は次の各号に掲げる行為をしてはならない。ただし、事前に甲の承認を受けた場合は、この限りではない。

（１）甲から預託を受けた個人情報を第三者（再委託等する場合における再委託等先を含む。）に預託若しくは提供又はその内容を知らせること。
（２）甲から預託を受けた個人情報を本契約の目的の範囲を超えて使用、複製、又は改変すること。
３　乙は、甲から預託を受けた個人情報の漏洩、滅失、毀損の防止その他の個人情報の適切な管理のために必要な措置を講じなければならない。
４　乙は、甲から預託を受けた個人情報について、作業終了、又は解除をした後に速やかに甲にその媒体を返還するとともに、乙が保存している当該個人情報について、復元不可能な状態に消去し、その旨を甲に通知しなければならない。ただし、甲が別に指示したときは、その指示によるものとする。
５　乙は、預託を受けた個人情報の取扱いに係る業務を第三者に再委託等してはならない。ただし、事前に甲に対して、再委託等業務の内容、再委託等先の詳細等甲が要求する事項を書面により通知し、甲の承認を得た場合は、この限りではない。
６　乙は、前項のただし書に基づく再委託等を行う場合において、再委託等先に対して本条に規定する措置及び義務を遵守させるため、必要な措置をとらなければならない。また、第７項に規定する検査について、預託する個人情報等の秘匿性等その内容やその量等に応じて甲が必要と認めるときは、甲所属の職員又は甲の指定する職員若しくは乙が実施する。
７　甲は、預託する個人情報等の秘匿性等その内容やその量等に応じて必要があると認めるときは、甲所属の職員又は甲の指定する者に乙の事務所又はその他の業務実施場所等において、甲が預託した個人情報の管理体制、実施体制及び管理状況について検査をさせ、乙に対して必要な指示をすることができる。
８　乙は、甲から預託を受けた個人情報について漏洩、滅失、毀損、その他本条にかかる違反等が発生した場合、又はそのおそれが生じた場合には、適切な措置を講じるとともに、甲にその旨を通知して、必要な対応策を甲と協議する。
９　乙は、自らの故意又は過失により生じた前項の事故により、甲に損害が生じた場合には、その賠償の責めに任ずるものとする。
10　第１項及び第２項の規定については、作業終了、又は解除をした後であっても効力を有するものとする。

（本契約に関する疑義の決定）
第 19 条　この契約書に規定がない事項及び疑義のあるときは、甲乙協議のうえ定めるものとする。

この契約の締結を証するため、本契約書２通を作成し、甲乙記名押印のうえ、各１通を保有するものとする。

令和　年　月　日

甲　　茨城県つくば市小野川１６－２
国立研究開発法人国立環境研究所
理事長　木本　昌秀

乙

（別紙）

再委託等承認申請書

年　　月　　日

国立研究開発法人国立環境研究所
　理事長　木本　昌秀　殿

住　　所
会 社 名
代表者氏名

本件業務の実施に当たり、下記により業務の一部を再委託等したく、本件契約書第４条の規定に基づき承認を求めます。

記

１　業務名：

２　契約金額：　　円（税込み）

３　再委託等を行う業務の範囲：

４　再委託等を行う業務に係る経費：　　円（税込み）

５　再委託等を必要とする理由：

６　再委託等を行う相手方の商号又は名称及び住所：

７　再委託等を行う相手方を選定した理由：

以上

担当者等連絡先
部署名　：
担当者名：
責任者名：
ＴＥＬ　：
E-mail　：

別表（単価表）

１．事務経費

	項目	単位	単価（円（税抜））
1	マイナンバー収集業務(本人確認・登録)	1件	
2	不要物返送対応	1件	
3	督促（電話）	1件	
4	督促（郵送）	1件	
5	収集書類再送	1件	
6	本人交付分法定調書作成、送付 (支払調書・源泉徴収票等含む)	1件	
7	税務署提出用法定調書作成	1件	
8	市区町村提出用(総括表含む)法定調書作成	1件	
9	税務署への代理申告	1件	
10	市区町村への代理申告	1件	
11	マイナンバー等移管（前請負業者からの引継）	1式	
12	マイナンバー等移管（次請負業者への引継）	1式	

２．郵送費（令和８年４月１日時点）

	項目	単位	単価（円（税込））
1			
2			
3			
4			
5			

※上記は記載の一例であり、単価表に記載する項目はこれに限るものではない。

（別添２）

仕　様　書

１　件名　マイナンバー等収集管理及び法定調書作成支援業務

２　業務契約期間　　令和８年４月１日～令和 11 年３月 31 日

３　業務実施場所　　請負者及び国立研究開発法人国立環境研究所において行うものとする。

４　業務の目的

国立研究開発法人国立環境研究所（以下「NIES」という。）は外部有識者等への謝金の支払に伴い、所得税法に基づき源泉徴収票等の法定調書を作成しなければならない。法定調書作成にあたり、外部有識者等のマイナンバーの記載が必要となるため、マイナンバーの収集・保管・利用に係る業務、及び法定調書作成に係る支援業務を請負者に委託するものである。

５　業務の概要

（１）業務範囲

ア　マイナンバー収集業務

イ　収集したマイナンバーの保管・廃棄

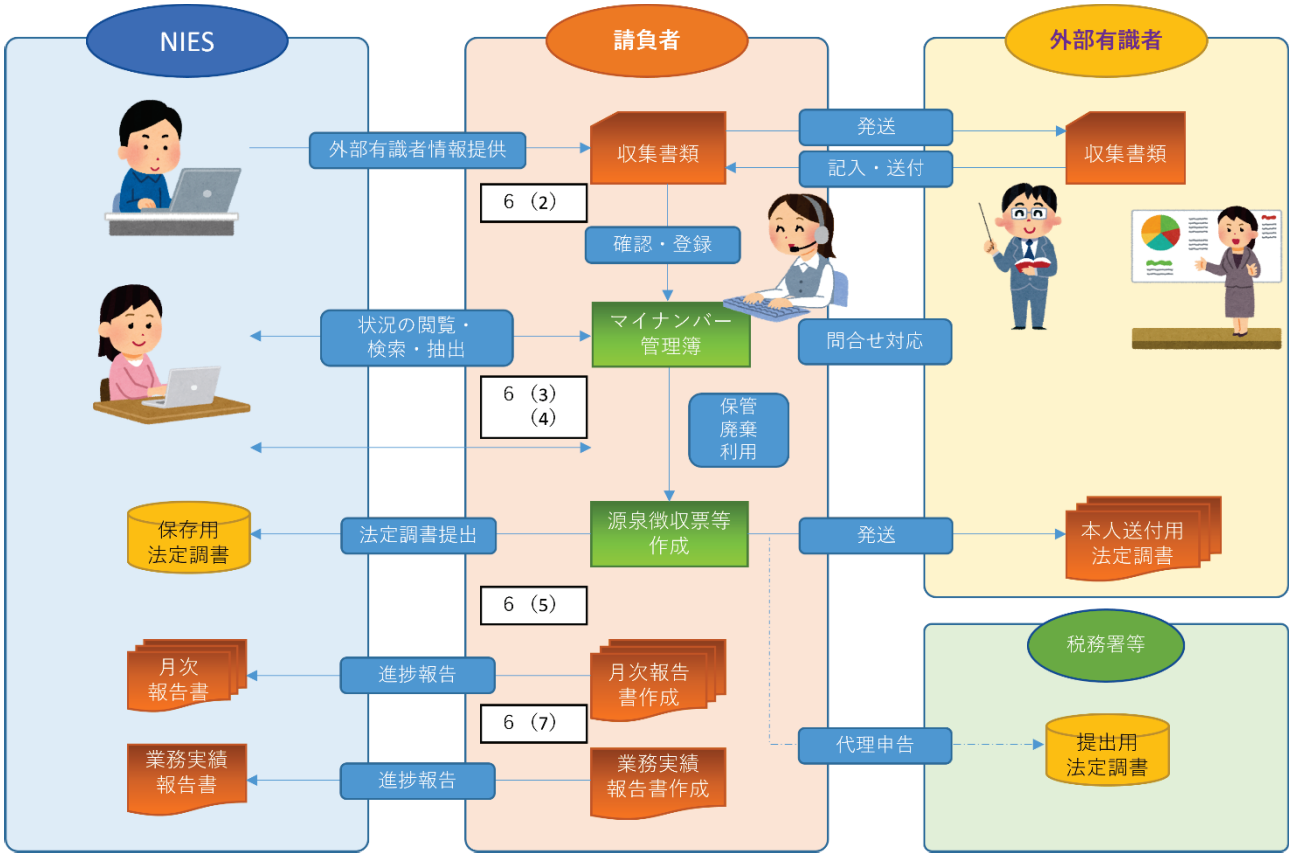
ウ　マイナンバーの利用業務

（２）対象者数

ア　外部有識者　200 名程度／年

（３）業務概観図

業務の全体像及び役割の概要を以下に示す。



６　業務内容

「行政手続における特定の個人を識別するための番号の利用等に関する法律」、「特定個人情報の適正な取扱いに関するガイドライン」、NIES 個人情報等保護規程、NIES における特定個人情報等の安全管理に関する基本方針、NIES が行う個人番号関係事務における特定個人情報等取扱要領、税理士法及び税務に関わる法令その他マイナンバーに関わる法令に準拠して行うこと。

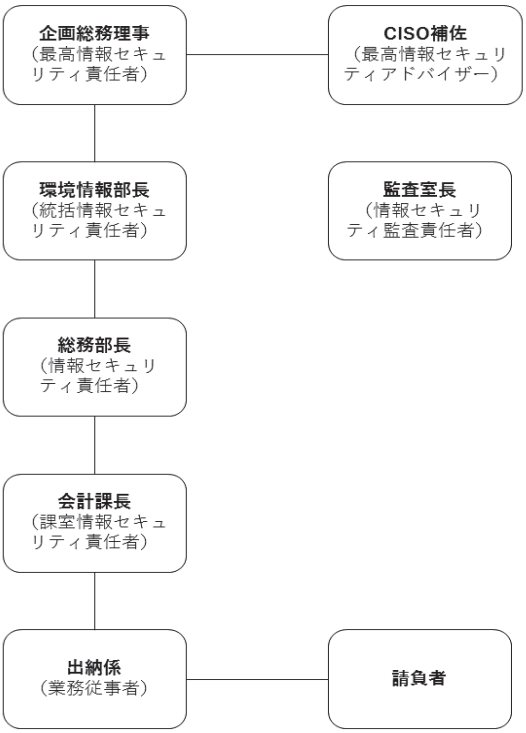
（１）導入準備

以下の準備作業を行うこと。なお、イからエまでの作業を完了した後に作業報告書（イ～エをまとめたもの）を作成し提出すること。

ア　業務実施計画書を作成し、NIES 担当者に提出すること（提出時期は NIES 担当者との打合せによる）。変更があった場合も速やかに NIES 担当者に提出すること。業務実施計画書には、以下の内容を含めること。

・本業務を円滑に実施するための方針や体制・役割
・契約締結後から令和 11 年３月 31 日までの作業とスケジュール
・請負者及び NIES とのコミュニケーションを円滑に行うためのプロセスやルール等
・NIES が既に実施しているマイナンバー関連業務から請負者を介して業務に移行するための計画
・請負者における業務実施体制（ａ～ｅ）。なお、NIES の体制は下図のとおり。
　ａ．統括責任者（１名程度）
　ｂ．統括責任者補佐
　ｃ．取扱区域内担当者（現場責任者１名程度を含む）
　ｄ．コールセンター
　ｅ．税務署への代理申告の担当者（税理士資格を持つ者を充てる）

業務実施体制のうち、取扱区域内担当者の現場責任者には、以下の資格のうちのひとつ、またはその資格に相当する実績を持つ者を充てる。
- 個人情報保護士
- 情報処理安全確保支援士（情報セキュリティスペシャリスト）
- プライバシーマーク審査員
- マイナンバー実務検定１～２級



イ　環境の整備

本業務を行う上で必要な環境を整備すること。

ウ　マニュアルの整備

業務上必要となるマニュアルを整備すること。マニュアル作成にあたっては、NIES の業務を考慮し、（既存のサービス利用マニュアルをベースとする等により）利用実態に合わせたマニュアルとすること。

エ　教育の実施

業務に際して必要な教育を請負業務従事者に実施すること。その際、NIES と協議の上、教育対象者、スケジュール、実施方法を整理し、提示すること。

（２）収集業務

次の点に留意の上、対象者からマイナンバーを収集すること。

ア　マイナンバーの収集及び確認作業

１）請負者は、NIES から指示された外部有識者等に対し、以下によりマイナンバー収集書類を作成し、自宅宛、もしくは NIES から指示された住所へ発送すること。なお、収集書類の様式については、事前に NIES の承諾を得ること。

①収集書類には、提供依頼書（NIES 及び請負者名を明記した主旨説明、利用目的、問合せ先（コールセンター）、提出期限が記載されたもの）、提供要領書（身分証明書類等の提出物・マイナンバー提出方法を解説したもの、FAQ）、氏名・住所等記載用紙、マイナンバーカード写し等の貼り付け台紙、返信用封筒（外部有識者等の郵便料金負担なし、送付先住所記載済）を同封すること。紙書類提出ではなく必要情報・資料の Web アップロードによる収集（以下「Web 収集」という。）を行う場合は、Web 用の提供要領書（アップロード画面へ接続するための QR コード等を含む）、操作説明書類も同封すること。

②Web 収集を取り入れる場合は、対象者が希望により紙収集を選択できるよう、紙収集用の書類、返信用封筒も同封すること。もしくは、請負者の設置する専用窓口に係る案内書類を同封し、連絡のあった希望者にのみ紙収集用の書類を発行しても差し支えない。
③収集書類には、誤記入を防止する施策を行うこと。
④収集書類は FAQ を含め英語対応していること。なお、英語を希望する対象者については NIES から別途指示する。
⑤返信用封筒は、内容物が透けて見えない素材で配達記録が残る方式で発送されるものを用意すること。なお、内容物が透けない素材の書留郵便用封筒（料金後納とし、発生した郵送代は本業務内に含むものとする）を同封しても差し支えない。
⑥Web 収集に用いるシステムの基本的なセキュリティ要件は「７　情報セキュリティの基本的要件」に準じるものとする。

２）請負者は、NIES が収集依頼をしてから２ヶ月以内を目安に収集を完了すること（収集時期によっては１ヶ月以内を目安とする。）。提出期限までに提出されない者に対して、督促（電話、郵送等）を行うこと。督促の方法は NIES との協議により決定すること。また、NIES に対し、請負者が用意するマイナンバーを管理・運用するためのシステム（以下「専用システム」。なお、NIES 担当者はマイナンバーの閲覧は行えないものとする。）を利用して未提出者リスト及び督促状況報告書を提出すること。

３）請負者は、コールセンター（平日（月曜日から金曜日、土日祝祭日を除く）10 時～16 時を含む８時間程度）を設置し、外部有識者等からの問合せに対応すること。

４）請負者は、返送された収集書類に対し、法令に準じた本人確認を行うこととする。なお、開封、確認作業はすべてマイナンバー取扱区域にて行うこと。

５）請負者は、収集書類に不備、不足があった場合は、該当者に対し、再提出依頼を行うこととし、収集書類の紛失者に対しては必要に応じて収集書類の再送付を行うこと。なお、再送付は収集対象者のうち５％程度を想定する。

６）請負者は、返送された収集書類に本業務に無関係の異物が混入していた場合、その情報を NIES に対し報告すること。NIES が対応方法を決定するが、請負者は必要であれば異物返送の対応を行うこと。返送を行う場合、発送は原則として１）⑤の方法に準ずること。

７）請負者は、収集書類を保管する際は、マイナンバー取扱区域内のキャビネット（鍵付き）に保管し、盗難・紛失を避けること。また、物理的な保管場所の区分け、収集書類への専用 ID 印字等の工夫により、NIES 以外の書類・データとの混合を確実に防ぐこと。

８）収集に必要な情報は、専用システム等のアップロード機能を利用して、NIES が請負者に提供することとする。

イ　マイナンバーの登録作業
１）請負者は、専用システム等にマイナンバーを登録する際は、登録内容に誤りがないようにチェックする体制を整備すること。
２）本業務の前請負者より引き継ぎのあったマスタデータについては、NIES 担当者が指定した期日までに専用システムに登録を行うこと。

（３）保管・廃棄業務
ア　専用システム等への登録が完了し不要となった収集書類については、復元不可能な方法で裁断かつ溶解し破棄すること。

イ　収集した外部有識者等の情報は、関連法令が求める保存期間・期限に準じた期間を経過した場合、またはNIESから削除・廃棄の指示を受けた場合、速やかに専用システム内から削除し、削除した証明書を発行しNIES担当者へ提出すること。

（４）利用業務（専用システムの構築）

ア　請負者は、マイナンバーの収集・管理・利用状況の把握のために、各種法定調書（「報酬、料金、契約金及び賞金の支払調書」、「不動産の使用料等の支払調書」、「源泉徴収票」等）ごとに管理簿を供え、権限を与えられたNIES担当者のみが、NIESのネットワークを介して特定のクライアントPCからアクセス可能な、管理簿を出力できる専用システムを構築し提供すること。収集書類（不備のないもの）到着から専用システム閲覧までは３営業日以内とすること。また、NIESが利用するにあたっては、データベースの利用方法や運用マニュアル等を提供し、NIES担当者へ説明・指導等を行うこと。

イ　専用システムの基本的なセキュリティ要件は「７　情報セキュリティの基本的要件」に準じるものとする。主体認証においては、多段階認証またはIPアドレスによる接続制限、もしくはそれらを組み合わせた認証を導入すること。なお、ログイン時に入力する主体認証情報は、NIESの認証基盤で使用されているものとは別とし、パスワード文字列として英数字記号から任意の13桁以上を設定可能とするなど、セキュリティの高い認証方式を採用すること。また、一定回数以上のパスワード誤入力を検知した場合はロックを掛けることができ、本人確認によって仮パスワードを再発行できること。

ウ　利用者の役割に応じた操作権限を付与可能な専用システムであること。

エ　専用システムの利用ログ（ログイン、閲覧、検索、抽出）が記録・閲覧できること。

（５）法定調書の作成・提出等

ア　法定調書の作成

請負者は、年１回、NIES担当者が提供する法定調書作成に必要な個人情報（支払金額、源泉徴収税額、居住地等）に基づき、下記の法定調書を作成すること。なお、件数は各調書の過去の実績件数に基づいた目安であり、当該業務における件数を保証するものではない。

ａ.税務署、市区町村提出用（マイナンバーを付記）

・報酬、料金、契約金及び賞金の支払調書	300件程度（税務署提出）
・不動産の使用料等の支払調書	5件程度（税務署提出）
・不動産等の売買又は貸付けのあっせん手数料の支払調書	0件（税務署提出）
・不動産等の譲受けの対価の支払調書	0件（税務署提出）
・給与所得の源泉徴収票	1件程度（税務署提出）
・給与支払報告書（市区町村毎の総括表を含む）	10件程度（市区町村提出）

ｂ.本人交付用（マイナンバーの記載なし）

・報酬、料金、契約金及び賞金の支払調書	700件程度
・不動産の使用料等の支払調書	5件程度
・不動産等の売買又は貸付けのあっせん手数料の支払調書	0件
・不動産等の譲受けの対価の支払調書	0件
・給与所得の源泉徴収票	10件程度

イ　法定調書の提出

請負者は、別途指定する期日までにマイナンバーを含む法定調書（６（５）アａ）をe-Tax、eLTAXによる代理申告にて提出すること。なお、給与所得の源泉徴収票等の法定調書合計表はNIES担当者がPDFにて作成のうえ事前に共有するため、請負者はその内容に従って申告するものとする。NIESと直接雇用関係にある者に係る法定調書は別途NIES人事課職員に

て申告を行うため、申告期日及び作業順等についてはNIES担当者と協議のうえ調整すること。
本人交付用の法定調書（６（５）アｂ）については、郵送にて対象者宛に送付すること。

ウ　NIESへの提出・納品
全ての法定調書等について、NIES担当者が確認できる形式（PDF、csvファイル等。マイナンバーは記載しない）で提出し、NIES担当者の確認を得てから、各申告先機関及び本人への提出・送付等を行うこと。
本人交付用の法定調書について、発行対象者本人から再発行の求めがあった際には、NIESより随時発行・郵送するため、対象者の検索が容易に可能なPDF形式にて納品すること。
電子データについては、セキュリティが確保された方法で提出すること。具体的には、専用システムもしくはNIESが用意するBoxを利用することを想定している。

（６）予定件数等（別紙のとおり）
※予定件数は件数を保証するものではない。

（７）報告書の提出
定期的な進捗報告（進捗の状況、課題、リスクの報告）を行うこと。
ａ．月次報告書　　１部（毎月末までに）
ｂ．業務実績報告書　　１部（毎年度末までに）
報告書の仕様は、契約締結時においての国等による環境物品等の調達の推進等に関する法律（平成12年法律第100号）第６条第１項の規定に基づき定められた環境物品等の調達の推進に関する基本方針（以下「基本方針」という。）の「印刷」の判断の基準を満たすこと。
ただし、当該「判断の基準」を満たすことが困難な場合には、NIES担当者の了解を得た場合に限り、代替品による納品を認める。
なお、印刷物にリサイクル適性を表示する必要がある場合は、以下の表示例を参考に、裏表紙等に表示すること。

リサイクル適性の表示：印刷用の紙にリサイクルできます。 この印刷物は、グリーン購入法に基づく基本方針における「印刷」に係る判断の基準にしたがい、印刷用の紙へのリサイクルに適した材料［Ａランク］のみを用いて作製しています。

なお、リサイクル適性が上記と異なる場合はNIES担当者と協議の上、基本方針（https://www.env.go.jp/policy/hozen/green/g-law/net/kihonhoushin.html）を参考に適切な表示を行うこと。

７　情報セキュリティの基本的要件
請負者は、収集したマイナンバー等や収集時に受領したマイナンバーに関連するデータや書類が漏えい、滅失または毀損することなく適切な管理を行うために、個人情報保護委員会が定めた「特定個人情報の適正な取扱いに関するガイドライン（事業者編）（令和７年６月最終改正）」、「個人情報の保護に関する法律（令和7年6月1日最終改正）」及び「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」に従い、組織的、人的、物理的、技術的等の安全管理措置を講じること。なお、業務期間中にこれらのガイドライン、法律等が改定された場合には、最新版に従うこと。

（１）組織的安全管理措置
・組織体制の整備
・取扱規程等の整備
・取扱状況を確認する手段の整備
・情報漏えい等事案に対応する体制等の整備
・取扱状況の把握及び安全管理措置の評価及び見直し

・特定個人情報の秘匿性、取扱い等に関し、設備、技術水準、従業者に対する監督・教育の状況等を組織的に整備すること。
・「ISO27001（ISMS)」とプライバシーマークの資格を取得していること。

（２）人的安全管理措置
・事務取扱担当者の監督
・事務取扱担当者等の教育
・法令、内部規程違反等に対する厳正な対処

マイナンバーを取り扱う従業員等を明確化し、従業員等に対し、マイナンバー取扱いに対する情報セキュリティ教育を定期的に実施すること。新規従業員に対しては業務実施前に初回の教育を実施すること。

（３）物理的安全管理措置（マイナンバー取扱区域の整備）
・特定個人情報等を取り扱う区域の管理
・機器及び電子媒体等の盗難等の防止
・電子媒体等の取扱いにおける漏えい等の防止
・マイナンバーの削除、機器及び電子媒体等の廃棄

取扱区域は物理的に仕切られた空間であり、取扱区域内担当者等のみが入退室できるようにすること。入退室記録を定期的に残すこと。私物等の持ち込みを禁止し、特に通信・撮像機器や記録機器（媒体)、筆記具の一切を持ち込めないように適切な安全管理措置を講じていること。取扱区域のパソコンには機器、電子媒体等の持ち込み・持ち出しについて適切な安全管理措置を講じていること。

（４）技術的安全管理措置（専用システム及びデータサーバの整備）
・アクセス制御
・アクセス者の識別と認証
・不正アクセス等による被害の防止等
・情報漏えい等の防止

専用システムを利用すること。専用システム等に係る認証・操作・アクセスログ等は６ヶ月分以上保存し定期的に確認すること。不正アクセスや情報セキュリティインシデント発生時には、速やかにNIESに一次報告の上、当該ログの分析等により、被害状況及び再発防止策等について報告すること。万一の障害発生時にも、早期解決のために24時間体制が可能な対策を講じて、専用システムの利用再開が速やかに可能であること。また、NIESの運用に影響が生じる場合には速やかに障害状況を報告すること。

（５）その他
・本業務で取り扱う情報の保管、保存場所は日本国内とすること。
・本業務で取り扱う情報の保管、保存場所は「データセンターファシリティスタンダード ティア3」相当以上の施設であること。
・本業務で取り扱うマイナンバー情報を保管するシステム及びWeb収集に用いるシステムは、クラウドサービスを利用する場合には、「政府情報システムのためのセキュリティ評価制度（ISMAP)」の登録を受けていることを原則とする。ISMAPに未登録の場合は、国立環境研究所が提供する管理基準表を提出し、ISMAP 管理基準と同等のセキュリティ対策が可能であることを証明すること。

８　共通事項、禁止事項等

「特定個人情報の適正な取扱いに関するガイドライン（事業者編）」第 4-2 特定個人情報の安全管理措置等　第 4-2（1）委託の取扱いにより、請負契約の締結において契約内容に盛り込む事項を以下に記載する。

（１）秘密保持義務

請負者は、本契約による業務に従事する者に対し、本業務に関して知り得た情報をみだりに他人に知らせ、または不当な目的に使用しないよう、必要かつ適切な監督を行わなければならないものとする。

（２）マイナンバーの目的外利用の禁止

本契約により収集したマイナンバーについては、当該事務を処理する目的以外に利用してはならないものとする。

（３）マイナンバーの複製等の禁止

マイナンバーを保管するデータセンター等からのマイナンバー関連書類・データの複製、送信、二次使用及び外部への受渡しまたは持ち出しを禁止するものとする。ただし、NIES から請負者に受渡しするマイナンバー収集に必要な情報については、専用システムのアップロード機能を利用して暗号化した上で受渡しすることとする。

（４）再委託の禁止

本契約に基づく作業にあたり、再委託は禁止とする。ただし、下記事項について事前に NIES の承諾を得たうえで実施する場合は、この限りではない。

・６（５）イの e-Tax、eLTAX による代理申告を、税理士資格を持つ第三者へ再委託する場合

（５）漏えい事案等発生時の責任

以下に定める内容については、本契約の解除及び NIES から請負者への損害賠償の請求ができるものとする。

１）請負者が取り扱うマイナンバーについて、請負者の責めに帰するべき理由による紛失及び二次使用や流出等の漏えいがあったとき。

２）この契約による業務の目的を達成できないと認めるとき。

（６）請負契約終了時後のマイナンバーの返却・廃棄

契約満了に伴い新たな契約相手方が決定した際には、NIES が指定した期日までに管理しているマスタデータ（専用システム内のデータや収集に必要な情報等約 2,400 件）を NIES に対して情報セキュリティ対策が充分に考慮された方法で引き継ぎができるようにすること。また、引き継ぎに係る内容や形式等については、NIES 担当者、新たな契約相手方と協議すること。同時に専用システム内のデータを復元できないよう完全削除を実施し、完全削除したことの証明書を提出すること。

（７）従業員等に対する監督・教育義務

マイナンバー取扱いに対する情報セキュリティ教育を実施すること。また、その実施結果について NIES に報告すること。

（８）業務委託内容の遵守状況の報告

NIES の求めに応じ、マイナンバー管理状況の説明または資料の提出を行うこととする。

（９）マイナンバーを取り扱う従業員等の明確化

マイナンバーを取り扱うための規程、規則、体制及び取扱者について、NIES へ報告することとする。

(10) 請負者の監督・監査

１）NIES は、随時、請負者が必要な安全管理措置が講じられているか実地または書面による監査を行うこととし、請負者は、NIES から要望があった場合は、監査に協力すること。

２）特定個人情報の秘匿性、取扱い等に関し、設備、技術水準、従業者に対する監督・教育の状況、その他請負者の経営環境等について、毎年度、独立した公認会計士や監査法人など外部の監査人が公正な第三者の立場で行う監査を受け、その監査結果を NIES に報告するものとする。

９　著作権等の扱い

（１）請負者は、本業務の目的として作成される成果物に関し著作権法第 27 条及び第 28 条を含む著作権の全てを NIES に譲渡するものとし、当該対価は本契約金額に含むものとする。

（２）請負者は、成果物に関する著作者人格権（著作権法第 18 条から第 20 条までに規定された権利をいう。）を行使しないものとする。ただし、NIES が承認した場合は、この限りではない。

（３）上記（１）及び（２）にかかわらず、成果物に請負者が既に著作権を保有しているもの（以下「既存著作物」という。）が組み込まれている場合は、当該既存著作物の著作権についてのみ、請負者に帰属する。提出される成果物に第三者が権利を有する著作物が含まれる場合には、請負者が当該著作物の使用に必要な費用の負担及び使用許諾契約等に係る一切の手続を行うものとする。

10　情報セキュリティの確保

請負者は、国立研究開発法人国立環境研究所情報セキュリティポリシーを遵守し、情報セキュリティを確保するものとする。特に下記の点に留意すること。なお、国立研究開発法人国立環境研究所情報セキュリティポリシーは以下 URL において公開している。
(https://www.nies.go.jp/security/sec_policy.pdf)

（１）請負者は、請負業務の開始時に、請負業務に係る情報セキュリティ対策の遵守方法及び管理体制、事故時における緊急時の連絡体制について、NIES 担当者に書面で提出すること。また、変更があった場合には、速やかに報告すること。

（２）請負者は、NIES から提供された情報について目的外の利用を禁止する。

（３）請負者は、NIES から要機密情報を提供された場合には、機密保持義務を負うこととし、当該情報の機密性の格付けに応じて適切に取り扱われるための措置を講ずること。

（４）請負者は、業務の実施に困難が予測される場合、情報セキュリティ体制の遵守に懸念が生じた場合には速やかに連絡し協議すること。なお、国立研究開発法人国立環境研究所セキュリティポリシーの履行が不十分と見なされるときまたは請負者において請負業務に係る情報セキュリティ事故の可能性が発生したときは、速やかに対処すると共に必要に応じて NIES の行う情報セキュリティ監査を受け入れること。

（５）請負者は、NIES から提供された要機密情報が業務終了等により不要になった場合には、確実に返却しまたは廃棄し、文書にて報告すること。

（６）業務に用いる電算機（パソコン等）は、使用者の履歴が残るものを用いてこれを保存するとともに、施錠等の適切な盗難防止の措置を講じること。また、不正プログラム対策ソフトが導入されており、利用ソフトウェアやその脆弱性等、適切に管理された電算機を利用すること。

（７）再委託することとなる場合は、事前の承諾を得て再委託先にも以上と同様の制限を課して契約すること。

11　検　　査

毎年度業務終了後、10 日以内に NIES 担当者立会いによる本仕様書に基づく検査を実施し、合格しなければならない。

12　協議事項

本業務に関し疑義等を生じたときは、速やかにNIES担当者と協議の上、その指示に従うものとする。

13　そ　の　他

請負者は、本業務実施に係る活動において、国等による環境物品等の調達の推進等に関する法律（グリーン購入法）を推進するよう努めるとともに、物品の納入等に際しては、基本方針で定められた自動車を利用するよう努めるものとする。

（別紙）

予定件数等

No	項目	単位	令和 8 年度	令和 9 年度	令和 10 年度
1	マイナンバー収集業務(本人確認・登録)	件	200	200	200
2	不要物返送対応	件	3	3	3
3	督促（電話）	件	35	35	35
4	督促（郵送。電話督促に応じなかった者）	件	25	25	25
5	収集書類再送（No.1 のうち 5%）	件	10	10	10
6	本人交付分法定調書作成、送付(支払調書・源泉徴収票等含む)	件	715	715	715
7	税務署提出用法定調書作成（対象者数）	件	306	306	306
8	市区町村提出用(総括表含む)法定調書作成	件	10 ※各市区町村 1 名程度	10 ※各市区町村 1 名程度	10 ※各市区町村 1 名程度
9	税務署への代理申告（申告法定調書の種類数）	件	3	3	3
10	市区町村への代理申告	件	10	10	10
11	マイナンバー等移管（前請負業者からの引継）	件	1800	—	—
12	マイナンバー等移管（次請負業者への引継）	件	—	—	2400

留意事項

1　上表の予定件数等に基づき必要経費（送料含む）を積算し、入札書には経費の総額を記載すること。ただし、本仕様書の件数等は予定値であるため、請求は実績に基づき行うものとし、予定件数等に満たない場合においても異議を申し立てないこと。

2　送料を請求する際には、金額の根拠となる書類（送付件数集計表等）を提出すること。

3　Web 収集を取り入れる場合、紙収集希望者は上記 No.1 のうち 30%を想定すること。

（別添３）

サービス概要

NO.	管理項目	回答
1	対象クラウドサービス名	
2	クラウドサービス提供事業者	
3	サービス内容が分かるURL	
4	利用用途・概要	

ガバナンス基準		適合状況
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
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、マネジメントビュー議事録等に、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。	

	マネジメント基準	適合状況
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	
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	

マネジメント基準		適合状況
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。	

	マネジメント基準	適合状況
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。	
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.]	
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。	

マネジメント基準		適合状況
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、経営時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。	

	マネジメント基準	適合状況
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]	
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]	

	マネジメント基準	適合状況
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。）	

	マネジメント基準	適合状況
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]	
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	

	マネジメント基準	適合状況
	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	

	マネジメント基準	適合状況
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。	
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。	

No	ISMAP 管理策番号	クラウドサービスが遵守すべきISMAP管理策	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	-	-	-
1	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。			
2	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	-	-	-
3	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。			
4	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。			
5	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	6.1.3	関係当局との適切な連絡体制を維持する。			
7	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。			
8	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。			
9	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	-	-	-
10	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。			
11	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	-	-	-
12	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。			
13	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	-	-	-
14	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。			
15	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	-	-	-
16	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。			
17	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。			
18	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。			
19	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	-	-	-
20	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	-	-	-
21	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。			
22	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。			
23	8.1.2	目録の中で維持される資産は、管理する。			
24	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			
25	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。			
26	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。			
27	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**	-	-	-
28	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。			
29	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。			
30	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。			
31	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**	-	-	-
32	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。			
33	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。			
34	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**	-	-	-
35	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。			
36	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。			
-	**9.2**	**利用者アクセスの管理**	-	-	-
37	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。			
38	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。			
39	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。			
40	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。			
41	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。			
42	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。			
43	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。			
44	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。			
45	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。			

46	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**	-	-	-
47	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**	-	-	-
48	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。			
49	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。			
50	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。			
51	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。			
52	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。			
53	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。			
54	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。			
55	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			
56	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。			
57	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。			
58	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**	-	-	-
59	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。			
60	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。			
61	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。			
62	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**	-	-	-
63	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。			
64	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。			
65	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。			
66	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。			
67	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。			
68	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**	-	-	-
69	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。			
70	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。			
71	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。			
72	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。			
73	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。			
74	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。			
75	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。			
76	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。			
77	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。			
78	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**	-	-	-
79	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。			
80	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。			

81	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。			
82	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。			
83	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。			
84	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。			
85	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。			
86	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**	-	-	-
87	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**	-	-	-
88	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**	-	-	-
89	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。			
90	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。			
91	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。			
92	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。			
93	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。			
94	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。			
95	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**	-	-	-
96	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**	-	-	-
97	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。			

98	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。			
99	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**	-	-	-
100	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**	-	-	-
101	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。			
102	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。			
103	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。			
104	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**	-	-	-
105	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。			
106	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。			
107	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。			
108	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**	-	-	-
109	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。			
110	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。			
111	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**	-	-	-
112	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。			
113	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。			

114	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。			
115	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。			
116	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。			
117	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。			
118	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。			
119	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。			
120	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。			
121	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**	-	-	-
122	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**	-	-	-
123	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。			
124	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。			
125	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、必要に応じて委託業務の実施場所及び契約に定める準拠法・裁判管轄を指定する。			
126	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。			
127	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。			
128	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**	-	-	-
129	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。			
130	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**	-	-	-
131	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。			
132	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。			
133	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。			
134	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。			
135	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。			
136	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。			
137	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。			
138	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**	-	-	-
139	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。			
140	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。			
141	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**	-	-	-
142	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**	-	-	-
143	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。			
144	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。			
145	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。			
146	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。			

147	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。			
148	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。			
149	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。			
150	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**	-	-	-
151	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。			
152	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。			
153	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。			