簡易公募型指名競争入札のお知らせ

下記の案件について、簡易公募型指名競争入札を行いますのでお知らせします。参加を希望される方は、宇治市公募型指名競争入札(見積)実施要領、宇治市競争参加業者選定基準及び運用基準、宇治市競争入札心得を熟読、承知のうえ、参加を申し込んで下さい。

令和 7年11月21日

宇治市長　松村　淳子
(担当課：契 約 課)

記

業務名	電子契約サービス導入業務委託		
業務場所	デジタル政策課		
委託期間	令和7年12月24日　～　令和8年3月31日　98日間		
業務概要及び条件	電子契約サービスの構築		
予 定 価 格	¥990,000 (税込)	最低基準価格	¥693,000 (税込)
入札参加者に必要な資格・条件	次の①～③を全て満たすこと ①参加資格者名簿登録 ②ISO27001又はプライバシーマークの取得 ③複数の電子契約サービス導入業務実績（元請、官公庁発注）		
入札参加表明書の受付	提出期限　令和7年11月27日(木)　午後 5時 00分 まで 提出場所　郵便入札 添付資料　別紙参加表明書に記載のとおり		
入札予定	予定日　令和7年12月17日(水) 場　所　宇治市役所　本館８階　大会議室		
前　払　金	無	部　分　払	無
消費税の扱い	消費税及び地方消費税を含んだ金額で行うこと		
そ　の　他	本件はランダム係数を用いた最低制限価格を適用しますのでご注意ください。 本件は郵便による入札を実施します。別紙「説明会に替えて連絡する事項」を熟読してください。		

説明会に替えて連絡する事項

・本案件に係る質疑の受付は、次のとおりとします。
　令和７年１１月２１日（金）午前９時から
　令和７年１２月　４日（木）午後５時まで

・お知らせの入札（見積）予定は、開札予定となります。入札書（見積書）提出については、指名通知時にお知らせする指定期日（持参の場合は提出日）を厳守してください。

・郵便入札について、不参加により指名停止は行いません。

・封筒の雛形は、契約課ホームページ「様式等ダウンロード」よりダウンロードしてご使用ください。

・「郵便入札にあたっての注意事項」及び「宇治市郵便入札の応募案内」を熟読してください。宇治市ホームページ（https://www.city.uji.kyoto.jp/soshiki/27/55607.html）に掲載しています。

・入札、契約等に係る連絡はメールで行っており、競争入札等参加資格審査申請の際に記入いただいたメールアドレス（申請後に変更の届出をしている場合はそのメールアドレス）に送信します。新たにメールアドレスを登録される場合や他のメールアドレスに変更を希望される場合は、競争入札等参加資格審査申請事項変更届を契約課に提出してください。

予定価格を超過して入札した者の取扱いについて

○　本件の入札において予定価格を超過して入札をした者は、本件の落札者が決定せず、再発注を行う際には指名しない場合があります。

○　入札辞退者に不利益を課すことはありません。

電子契約サービス導入業務委託仕様書

1　業務名称

電子契約サービス導入業務委託（以下「本業務」という。）

2　業務概要

本業務の目的は、事業者等の利便性の向上と負担軽減や宇治市（以下「本市」という。）における事務の効率化を図るため、契約手続きを電子化させる電子契約サービス（以下「サービス」という。）の導入及び導入に向けた各種支援を受けるため、サービス提供事業者（以下「受注者」という。）の専門的知見に基づき、導入に向けた各種例規の改正、制度設計及び周知等の準備に対し支援を実施する業務である。

3　委託期間

契約締結日から令和８年３月３１日まで

なお、契約締結後から令和８年３月末までを導入期間とし、令和８年４月以降にサービスの運用開始とすることを想定している。

4　サービス内容及び要件

本市及び契約行為の相手方（以下「契約相手方」という。）　が合意することにより、電子化した契約書（以下「電子契約書」という。）に、受注者がタイムスタンプ及び自身の電子署名を付与することにより、本市及び契約相手方が電子証明書を取得することなく、クラウド上で契約を締結できるサービスの導入支援を行う。

（１）基本要件

① 受注者の電子署名は、産業競争力強化法（平成２５年法律第９８号）第７条の規定に基づく「グレーゾーン解消制度」へ申請し、電子署名及び認証業務に関する法律（平成１２年法律第１０２号）第２条第１項に該当するものであること。

② 受注者が提供するサービスは、建設業法（昭和２４年法律第１００号）上義務付けられている建設工事請負契約に関する書面の交付を代替する措置として、サービスが建設業法施行規則（昭和24年建設省令第１４号）第１３条の４第２項の技術的基準に適合していること。

③ 電子署名は、タイムスタンプにより最低１０年有効性を検証できること。

④ 電子計算機を使用して作成する国税関係帳簿書類の保存方法等の特例に関する法律（平成１０年法律第２５号）への対応ができること。

⑤ 電子署名の検証については、Adobe 社製の無償でダウンロードできる PDF 閲覧ソフトウエアである「Acrobat Reader」によって電子契約書 PDF ファイルを閲覧して、「署名パネル」欄を確認することにより行うことができること。

⑥ 電子署名付与後の文書（PDF ファイル）をダウンロードできること。

⑦ 受注者は本契約が終了し、又は解除されたときは、本市がサービスを利用して締結した契約書の電子データ（以下「契約書データ」という。）について、クラウド上に保存されている全ての契約

書データを受注者と本市との間で合意した方法により引き継ぐこと。

⑧　契約期間中に、認証方式等の変更があった場合も、本市の費用、作業負担なく継続的なサービス提供ができること。

（2）各機能要件

①　基本機能

ア　電子契約の締結に当たり、契約書等データの作成、承認、署名、契約締結、契約書等データの保存、検索、出力等電子契約サービスにおける基本機能を有すること。

イ　本市に係るサービスの利用者数及び利用件数に制限がないこと。

ウ　アカウント情報は無制限に部局ごとに登録できること。

エ　契約相手方は、サービスの利用契約を結ぶことなく無償で利用することが可能であること。

オ　現在、本市の職員が利用している環境で利用できること。また、下記以外のソフトウェアやプラグインのインストール、ＯＳやブラウザ等の設定変更が必要ないこと。

区分	項目	バージョン等
ソフトウェア	ＯＳ	Microsoft Windows10 以降
	ブラウザ	Microsoft Edge
		Google chrome

カ　契約相手方はPC、スマートフォン等のマルチデバイスで操作が可能であること。また、各OS（Windows、macOS、Android、iOS等）での利用が可能であること。

キ　１ファイル当たり２０ＭＢ以上のデータを登録することが可能であること。

ク　契約書データの保存容量に制限がないこと。

②　管理者機能

管理者及び利用者に対し、管理者権限、契約締結権限等を設定できる機能を有すること。

③　利用者機能

ア　本市及び契約相手方について、クラウド上にアップロードされた契約書データを確認し同意する者の設定が可能であること。

イ　本市及び契約相手方に対し、同意依頼の通知メールが届くこと。

ウ　利用者の誤送信を防止するための機能を有すること。

エ　契約締結後、本市及び契約相手方に契約締結した旨の通知メールが届くこと。

オ　保管された契約書データは、本市が入力した契約名、契約相手方名等による検索が可能であること。（管理者でない利用者は権限設定等により他部署のファイルは閲覧等できないこと。）

カ　当該システムへのログイン時にＩＤ及びパスワードによる認証を行うことができること。

（3）動作環境及びネットワーク要件

①　提供するサービスは、総合行政ネットワーク（LGWAN）を介した LGWAN-ASP サービスとして提供されることとし、LGWAN 環境のみで必要な機能を全て利用できるサービスであること。また、契約相手方はインターネット環境で利用できるサービスであることとし、LGWAN 環境は不要とすること。

② 無害化処理及び通信上の制限など地方公共団体情報システム機構が定める LGWAN-ASP 接続約款等の制約により，ダウンロードした際に契約書データに付与された電子署名が破損しないこと。

（4）セキュリティに関する要件

① 提供するサービスのデータセンターは国内に所在地を置き、必要なセキュリティ及び災害対策等の措置が講じられていること。

② ウイルス、情報漏えい及び不法侵入等の対策が施されており、常に最新の状態を保持すること。

③ 情報セキュリティ

ア 政府情報システムのためのセキュリティ評価制度「ISMAP」のサービスリストに登録されていること。

イ ISO/IEC27017 認証を取得していること。

④ 改ざん検知が行われていること。

（5）導入支援に係る要件

① 本市職員及び契約相手方となる事業者等向けの操作説明会をそれぞれ実施するものとし、説明会資料の作成を行うこと。

ア サービス導入時に職員向け説明会および事業者向け説明会をそれぞれ複数回開催すること。

イ 開催方法はオンライン/オフライン同時開催ができること。

ウ 事業者向け説明会に対して、過去に開催した事例を具体的に示し、参加者を増やす施策について事例を用いて提案すること。

② 上記説明会資料とは別に、運用管理を行うための「運用マニュアル」や、サービスの利用に必要な「操作マニュアル（業務フローを含む。）」を作成し提供すること。自治体での電子契約導入における業務フローの検討・作成の支援実績があり、支援経験者を担当者として配置すること。

ア 電子契約導入に関する業務フローの検討・作成の支援を行うこと。

イ 組織情報や利用者の登録支援、利用者権限の設定支援、その他必要な項目の設定支援等、本サービスに必要な環境設定・支援を行うこと。

ウ 操作マニュアルや具体的な運用手順(契約相手方情報の管理方法、契約相手方の本人確認方法)の資料を整備すること。

エ 操作マニュアルや具体的な運用手順（事業者情報の管理方法、事業者の本人確認方法）の資料を整備すること。操作マニュアルや具体的な運用手順の資料を整備すること。

③ 内部運用ルール策定や例規改正における支援を行うこと。なお、例規整備については、本市例規集及び関連する規程等を全て点検し、電子契約の導入に伴い影響のある箇所を特定し、改正検討が必要なポイントについて、例規を専門的に助言できる担当者が１回以上打ち合わせにて説明を行うこと。

（支援内容）

ア　利用自治体の内部運用ルール策定および例規改正の支援を行うこと。
イ　庁内規定（押印規程・印章管理規程・文書管理規程等）の見直しの支援を行うこと。
ウ　電子契約に関する関係規程等の改正、ルールの作成および業務フローの整理・作成について必要な支援を行うこと。
エ　当該自治体の例規集を利用自治体と必要箇所を点検し、電子契約の導入に伴い影響のある箇所を特定すること。
オ　必要に応じ、契約状況の調査の支援、利用部門向けのヒアリングを行うこと。
カ　特定した例規の箇所をまとめ、改正検討が必要なポイントについて、例規を専門的に助言できる担当者が１回以上打ち合わせにて説明を行うこと。

（体制）
ア　例規集に影響のある箇所について専門的に助言できる担当者が調査・検討できる資料を提供し助言すること。
イ　電子契約サービス提供会社が、法規・例規の専門会社と業務提携等を締結しており、必要に応じて例規集の全検索等を依頼できること。
ウ　支援経験者を担当者として配置すること。

（実績）
ア　電子契約サービス提供事業者が、電子契約導入における例規整備制定及び例規改正への支援実績があること。

５　保守・運用

（１）システム障害発生時は、速やかに復旧に向け対応すること。
（２）メンテナンス等によりサービスが停止する場合は、事前に発注者に連絡すること。
（３）日次によるバックアップの取得及び取得したデータの管理を適切に行うこと。
（４）電話、電子メール及びチャット等により、操作等に関する問い合わせ等に対応するヘルプデスクを利用できること。

６　留意事項

（１）本市と連絡調整を十分に行い、円滑に業務を実施することとする。
（２）受注者は、本市がサービスを利用して締結した契約書等（受注者と本市との間の契約を除く。）に含まれる情報を機密として扱い、契約目的以外の利用や第三者への提供を行ってはならない。
（３）本業務の遂行上知り得た秘密を他に漏らしてはならない。契約期間の終了又は解除後も同様とし、本市の許可なく第三者に閲覧、複写、貸与または譲渡してはならない。従事する者が離職した場合も同様に遵守させること。
（４）この仕様書については、基本仕様書とし、追加すべき事項等が生じた場合は本市と受注者と協議し追加できるものとする。
（５）本業務の実施に係る一切の経費は、委託金額に含まれるものとする。

宇治市情報システム統一セキュリティ仕様書

（基本的事項）

第１条　本仕様書は本市における情報システムの統一的な情報セキュリティについて、情報システム開発及び改修等を行う際に考慮すべき事項について定めるものである。

(1)　情報セキュリティ対策は宇治市公共施設情報ネットワークにおいて統一的な対応が必要となるため、情報システム開発及び改修等の受注をした者（以下、「受注者」という）は、以下に示す事項について遵守することを要する。

(2) 受注者は個人情報の保護に関する法律（平成１５年法律第５７号）及びその他業務の実施に係る関係法令の規定を遵守することを要する。

（情報システムの種類）

第２条　情報システムには「業務支援システム」と「住民公開システム」があり、それぞれの情報セキュリティの要求内容は異なる。

（定義）

第３条　この仕様書において、次の各号に掲げる用語の意義は、当該各号に定めるところによる。

(1)　「宇治市公共施設情報ネットワーク」とは、宇治市庁舎内及び庁舎外施設（うじ安心館、水道部庁舎、ゆめりあ宇治、市立小学校・中学校・保育所及び幼稚園、消防署、図書館、公民館等）（以下、「宇治市施設」という）において、標準的な通信プロトコルを用いて構築された情報ネットワーク一式（情報機器（サーバ、クライアント等）やネットワーク機器（スイッチ、ルーター、ファイアウォール等）などのハードウェア資産（以下、「ハードウェア」という）、及びソースコードやデータベース・データ情報などのソフト資産（以下、「ソフトウェア」という）すべてのことをいう。）のことをいう。

(2)　「業務支援システム」とは本市行政事務（市立小中学校での校務事務は除く）において、事務処理を行うためにハードウェア及びソフトウェア等を利用し電子情報を扱う仕組みのことをいう。

(3)　「住民公開システム」とは本市において、インターネットを通じて住民等に情報提供等を行うためにハードウェア及びソフトウェア等を利用し電子情報を扱う仕組みのことをいう。

(4)　「個人情報」とは個人情報の保護に関する法律（平成 15 年法律第 57 号）第 2 条において使用する用語の例による。

（情報資産の取り扱い）

第４条　情報システムで取り扱う情報資産の重要度によって、情報システムを構成する情報機器等の取り扱い（情報機器を設置する区画等）が異なる。受注者は情報システムとその情報資産の取り扱いについて、本市発注担当課（以下、「発注者」という）の指示に従うこと。

（共通仕様）

第５条　受注者は情報システムの開発及び改修等において次の要件を満たすこと。

(1) 本市において、情報ネットワークの系統を業務支援システム用、住民公開システム用（インターネットを含む）及びその他用（総合行政ネットワーク（ＬＧＷＡＮ）を含む）に論理的に分離している。業務支援システム用と情報公開システム用及びその他用の系統間は原則として常時接続をしないこと。

(2)　「外部とのネットワーク接続」については、法令等に基づくとき、又は公益上必要であり、かつ、個人情報の保護に関し必要な措置が講じられていると認める発注者が認めるときを除き、受注者は発注者と協議を行い、承諾を得ること。

(3) サーバ機器（サーバ仮想化の仮想マシンを含む、以下同じ）についてバックアップからのリストアによるシステム復旧を念頭に、バックアップ箇所について発注者の指示に従い設定すること。なお、システム復旧にデータ以外にシステム関連プログラム等のバックアップを必要とする場合は、そのバックアップについても適切に取得できるよう設定すること。バックアップはテープ交換等の物理的な作業以外は、自動スケジュールによる運用を行うこと。

(4)　サーバ機器等の設置・導入をする場合には、発注者が指定する日時、設置場所に行うこと。

(5)　サーバ機器等の電源については、100V を基本とすること。200V 電源が必要な場合は、別途費用、工事等が必要となるため発注者と事前に協議すること。

(6)　宇治市施設に設置するサーバ機器において本市が必要と認める場合には、別表第１のウイルス対策ソフトをインストールできること。ただし、サーバ機器の設置場所が宇治市施設以外の場合、または ASP サービスを利用する場合はこの限りではない。

(7)　発注者と適宜連絡をとりあい、進捗状況について随時報告すること。

(8)　情報システム開発及び改修等にかかる協議内容については、議事録として納品すること。

(9)　情報システム開発及び改修等の成果品に瑕疵が発見された場合の受注者の瑕疵担保責任は、民法の規定どおりとする。ただし、瑕疵担保期間経過後であっても、受注者に故意又は重大な過失があった場合、受注者は発注者に対しその責任を負うものとする。

(10)　受注者は、情報システム開発及び改修等の業務を行う際に当該業務に従事する者について「技術者届」を発注者に提出すること。

(11)　電磁的記録情報による個人情報（以下、「個人データ」という）を取り扱う作業については、個人データの宇治市庁舎外への持ち出しは原則として認めない。また、個人データ以外の個人情報も同様とする。

(12)　受注者は、情報システム開発及び改修等の業務を行う際に個人データを取り扱う場合は、当該業務に従事する者の「秘密保持に関する誓約書」を発注者に提出すること。

(13)　受注者は、情報システム開発及び改修等の業務を行う際に個人データを取り扱う場合は、その取り扱い方法等について発注者の指示に従うこと。また、業務終了後の取り扱いについても同様とすること。

(14)　個人データはインターネット DMZ（住民公開システム等、インターネットに常時接続するサーバ機器を配置する）セグメントにおかないこと。
(15)　ネットワークプロトコルはＴＣＰ／ＩＰとすること。
(16)　情報システム開発及び改修等の業務の全部を一括してまたは大部分を第三者に委託し、または請負わすこと（以下、「再委託」という）をしてはならない。
ア　受注者は、業務の一部をやむを得ず再委託する必要がある場合又は再委託の内容を変更しようとする場合には、あらかじめ次に揚げる項目を記載した書面を発注者に提出して発注者の承諾を得ることを要する。

- 再委託を行う業務の内容
- 再委託で取り扱う情報
- 再委託の期間
- 再委託が必要な理由
- 再委託の相手方（名称、代表者、所在地及び連絡先）
- 再委託の相手方における責任体制並びに責任者及び従事者
- 再委託の相手方に求める個人情報保護措置の内容（契約書等に規定されたものの写し）
- 再委託の相手方の監督方法

イ　前号の場合、、受注者は、再委託の相手方にこの契約に基づく一切の義務を遵守させるとともに、受注者と再委託の相手方との契約内容にかかわらず、発注者に対して再委託の相手方による全ての行為及びその結果について責任を負うものとする。
ウ　受注者は、再委託先に対して本業務の委託をした場合は、その履行状況を管理・監督するとともに、発注者の求めに応じて、管理・監督の状況を発注者に対して適宜報告しなければならない。
(17)　再委託先から本業務を第三者へ委託することについては承諾しないこと。
（業務支援システム個別仕様）
第６条　業務支援システムの開発及び改修等において次の要件を満たすこと。
(1)　発注者が指定する、職員の使用するクライアント機器の標準 OS で正常なシステム稼働を実現すること。
(2)　職員の使用するクライアント機器には、別表第１に示す情報セキュリティ対策を行う。この環境において正常なシステム稼動を実現すること。
(3) IP マルチキャストパケットは本市 IC カード認証システムにおいて通信ができない。本市 IC カード認証システムを使用しない範囲において、使用する場合には事前に発注者からその承諾を得ること。
(4) 本市で構築している Active Directory にドメイン参加すること。
(5) 宇治市公共施設情報ネットワークで稼動すること。
(6) 外字を使用する場合には、本市の状況を十分に考慮に入れること。外字の追加、配布、連携等の管理については、運用の効率化を考慮すること。
(7) 文字コードについては特に定めないが、業務ごとに共通的なものを使用し、職員のクラ

イアントの標準利用環境で特別な操作をすることなく表示が可能であること。ただし、住民記録システム及び住民基本台帳システム（宇治市電子計算機処理の管理及び運営に関する規則（平成6年9月1日規則第34号））データとの連携をする場合には、「unicode」を選択することが望ましい。

(8) 電子公印を使用する場合は、ユニークな公印番号を付与し、「いつ・誰が・何に使用したか」を管理できるようにし、また出力帳票にはユニークな公印番号を出力すること。

(9) 個人データはクライアントには蓄積せず、必ずサーバに蓄積すること。

(10) クライアントのセットアップは本市でも可能とすること。セットアップマニュアル等の作業の詳細がわかる資料を提供すること。

(11) システムのログ取得については、システム障害発生時等の原因追究に必要となる項目を設定すること。

（住民公開システム個別仕様）

第7条　住民公開システムの開発及び改修等において次の要件を満たすこと。

(1) クライアントの一般的なインターネットブラウザを使用しインターネット接続でサービスを実現できること。また、標準的なインターネット使用環境で快適に動作すること。

(2) 個人情報を含む通信はSSLによる暗号化通信を行うこと。

(3) 地方公共団体情報システム機構（J-LIS）が実施する脆弱性診断等により問題点が発見された場合には真摯に対応すること。

(4) 受注者は、システム開発の成果品の納品を行う場合、脆弱性検査を実施し、問題がないことを確認したうえで納品すること。なお、脆弱性検査の実施内容及び実施結果について報告書を添付すること。

（その他）

第8条　本仕様書に定めない事項については、必要に応じて発注者と受注者とが協議を行い、これを定めるものとする。

別表第1

システム等名	システム開発企業名、ソフト名
ＩＣカード認証システム	（株）日立ソリューションズ製　AUthentiGate (株)ディー・ディー・エス　EVE－MA
ウィルス対策ソフト	トレンドマイクロ株式会社　ウィルスバスター　コーポレートエディション

データ保護及び秘密の保持等に関する仕様書

（目的）
第１条　この仕様書は業務委託を実施するにあたり、データの保護及び秘密の保持等に関する受注者の履行すべき責務を定めることを目的とする。
（秘密の保持等）
第２条　受注者は、契約の履行に際して知り得た秘密を他に漏らしてはならない。契約の終了後及び、解除した後も同様とする。
（データの受け渡し）
第３条　業務遂行上必要なデータ及び資料の受け渡しは、発注者と受注者の職員をもって行うものとする。
（運搬）
第４条　委託業務にかかるすべての契約目的物の運搬は、受注者の責任で行うものとし、その経費は受注者の負担とする。
（目的外使用の禁止）
第５条　受注者は、この契約の履行に必要な業務の内容を他の用途に使用してはならない。
（データの複写及び複製の禁止）
第６条　受注者は、委託業務にかかる一切のデータを複写又は、複製してはならない。
２　受注者は、委託業務終了後において、データその他記録媒体等の廃棄をするときは、あらかじめ、発注者の承認を受けるものとし、廃棄に関しては、第三者の利用に供されることのないよう厳重な注意をもって処分しなければならないものとする。
（帰属）
第７条　業務に関連して受注者が開発したプログラム及び作業仕様書は、発注者及び受注者に帰属するものとし、第三者に供与する場合は、あらかじめ発注者と受注者間の協議のうえ決定するものとする。
２　磁気テープのマスターファイル等は、発注者に帰属するものとする。
（安全管理義務）
第８条　受注者は、この委託契約に係わって、発注者から提供された入出力帳票及び媒体の取扱いについて、紛失、損傷、焼失等の事故が生じないように安全かつ適切な管理体制を講じなければならない。
（処理内容の報告等）
第９条　受注者は、委託業務処理方法に応じて処理内容について、発注者に対して報告しなければならない。

２　受注者は、委託業務を処理するうえで、事故等の発生により契約の履行に支障が生じ、または生じると認められるときは、直ちに発注者に対して口頭をもって通知するとともに、遅滞なくその状況を、発注者に書面等をもって報告しなければならない。

３　発注者は、受注者に対して所要の措置をとることを求めることができる。この場合受注者は直ちにこれに応じなければならない。

４　前項の措置に要した経費については、発注者と受注者間の協議のうえ定めるものとする。

（立会検査）

第１０条　発注者は、この契約の履行について必要があるとき、受注者に対して報告を求め、調査を行い、又は立ち会うことができるものとし、受注者はこれに協力しなければならない。

２　発注者は、必要に応じて、受注者の施設設備の管理及び作業管理等の状況について、調査し、勧告することができる。

（附則）

１　受注者は、業務の処理上個人情報を取り扱う場合は、個人情報の保護に関する法律（平成１５年法律第５７号）を遵守しなければならない。

２　受注者は、発注者が承諾した場合を除き、この契約にかかる業務を自ら行うこととし、第三者（受注者の子会社（会社法（平成 17 年法律第 86 号）第 2 条第 1 項第 3 号に規定する子会社をいう。）である場合も含む。）へ業務を委託（以下「再委託」という。）してはならない。

（１）　受注者は、業務の一部をやむを得ず再委託する必要がある場合は、あらかじめ次の各号に揚げる項目を記載した書面を発注者に提出して発注者の承諾を得ることを要する。

イ）再委託を行う業務の内容

ロ）再委託で取り扱う情報

ハ）再委託の期間

ニ）再委託が必要な理由

ホ）再委託の相手方（名称、代表者、所在地及び連絡先）

ヘ）再委託の相手方における責任体制並びに責任者及び従事者

ト）再委託の相手方に求める個人情報保護措置の内容（契約書等に規定されたものの写し）

チ）再委託の相手方の監督方法

（２）　前号の場合、受注者は、再委託の相手方に本契約に基づく一切の義務を遵守させるとともに、受注者と再委託の相手方との契約内容にかかわらず、発注者に対して、再委託先の全ての行為及びその結果について責任を負うものとする。

（３）　受注者は、再委託の相手方に対して本業務の委託をした場合は、その履行を管理・監督するとともに、発注者の求めに応じて、その状況等を発注者に適宜報告しなければならない。

３　受注者は再委託の相手方から本業務を第三者へ委託することについては承諾しないこと。

４　業務に従事するものは、業務の処理上個人情報を取り扱う場合は、所定の誓約書を発注者に提出するものとする。

５　仕様書等の交互符合しないものを発見したときは業務仕様書を優先する。

宇治市個人情報の取扱いに関する特記仕様書（ＡＳＰサービス用）

（基本的事項）

第1条　受注者は、個人情報の保護の重要性を認識し、この契約による業務を実施するに当たっては、宇治市情報セキュリティポリシー及び関係法令等の規定に従い、個人の権利利益を侵害することのないよう、個人情報の取扱いを適切に行わなければならない。また、庁舎外での個人情報の取り扱いが発生する場合には、受注者は、別途定める「個人情報の取扱いに関する特記仕様書の項目遵守の確認表」（ASP サービス用）で確認した項目を遵守しなければならない。

（秘密の保持）

第2条　受注者は、この契約の履行により直接又は間接に知り得た個人情報を第三者に漏らしてはならない。この契約が終了し、又は解除された後においても、同様とする。

（目的以外の使用及び第三者への提供の禁止）

第3条　受注者は、この契約による業務を処理するため取得し、若しくは作成した情報（情報の全部又は一部を複写等した他の媒体を含む。以下同じ。）又は発注者から引き渡された情報を発注者の指示又は承諾を得ることなくこの契約の目的以外に使用し、又は第三者に提供してはならない。

（複写及び複製の禁止）

第4条　受注者は、データバックアップを除き、この契約による業務を処理するため発注者から引き渡しを受け、又は受注者自らが収集し、若しくは作成した情報が記録された資料等を、発注者の承諾なしに複写し、又は複製してはならない。

（適正管理）

第5条　受注者は、この契約による事務を処理するため発注者から引き渡しを受け、又は受注者自らが収集し、若しくは作成した情報の滅失及び毀損の防止に関する措置を講じなければならない。

（個人情報の帰属及び返還、廃棄又は消去）

第6条　発注者から引き渡された個人情報のほか、この契約による業務を処理するために発注者の指定した様式により、及び発注者の名において、受注者が取得し、作成し、加工し、複写し、又は複製等した個人情報は、発注者に帰属するものとする。

2　受注者は、委託業務完了時に、発注者の指示に基づいて、前項の個人情報を返還し、廃棄し、又は消去しなければならない。

3　受注者は、第 1 項の個人情報を返還する場合は、全ての資料（資料名称や情報項目、媒体名、数量等の内容がわかるもの）の明細とともに返還し、複製された資料等がないことを証する書面を発注者に提出しなければならない。

4　受注者は、第 1 項の個人情報を廃棄、又は消去する場合、当該個人情報が記録された電磁的記録媒体の物理的な破壊その他当該個人情報を判読及び復元できないように確実な方法で廃棄し、又は消去しなければならない。

5　受注者は、第 1 項の個人情報を廃棄し、又は消去した時は、完全に廃棄し、又は消去した旨の証明書（情報項目、媒体名、数量、廃棄若しくは消去の方法、責任者、廃棄又は消去の年月日が記載された書面）を発注者に提出しなければならない。

6　受注者は、廃棄又は消去に際し、発注者から立会いを求められたときはこれに応じなければならない。

（事故発生時の対応）

第7条　受注者は、この契約による業務の処理に関して個人情報の漏えい等の事故が発生し、又は発生するおそれがある場合は、その事故等に係る帰責の有無に関わらず、直ちに発注者に対して、当該個人情報の漏えい等の事故に係る個人情報の内容、数量、発生場所、発生状況等を報告し、その指示に従わなければならない。

2　受注者は、前項の個人情報の漏えい等の事故が発生し、又は発生するおそれがある場合に備え、発注者その他の関係者との連絡、証拠保全、被害拡大の防止、復旧、再発防止の措置を迅速かつ適切に実施するために、緊急時対応計画を定めなければならない。

3　発注者は、業務に関し個人情報の漏えい等の事故が発生した場合は、必要に応じて当該事故に関する情報を公表することができる。

4　受注者は、発注者と協議の上、二次被害の防止、類似事案の発生回避等の観点から、可能な限り当該個人情報の漏えい等の事故に係る事実関係、発生原因及び再発防止策の公表に努めなければならない。

（契約解除）

第8条　発注者は、受注者が本特記仕様書に定める義務をはたさない場合は、この契約による業務の全部又は一部を解除することができるものとする。

2　受注者は、前項の規定による契約の解除により損害を被った場合においても、発注者にその損害の賠償を請求することはできない。

（損害賠償）

第9条　受注者の故意又は過失を問わず、本特記仕様書に定める義務に違反し、又は怠った

ことにより発注者が損害を被った場合には、発注者にその損害を賠償しなければならない。

（情報セキュリティへの組織的取組の基本方針）

第10条　受注者は、情報セキュリティに関する組織的取組についての基本的な方針を定めた文書を作成しなければならない。また、当該文書には、経営陣が承認の署名等を行い、情報セキュリティに関する経営陣の責任を明確にしなければならない。

2　受注者は、情報セキュリティに関する基本的な方針を定めた文書について、定期的又はクラウドサービスの提供に係る重大な変更が生じた場合（組織環境、業務環境、法的環境、技術的環境等）に見直しを行わなければならない。この見直しの結果、変更の必要性が生じた場合には、経営陣の承認の下で改定等を実施しなければならない。

（サービス事業者の組織）

第11条　受注者は、外部組織が関わる業務プロセスにおける情報資産に対するリスクを識別し、適切な対策を実施しなければならない。

2　受注者は、情報資産へのアクセスが可能となる外部組織との契約においては、想定される全てのアクセスについて、その範囲を規定しなければならない。

（情報資産の管理）

第12条　受注者は、取り扱う各情報資産について、管理責任者を定めるとともに、その利用の許容範囲（利用可能者、利用目的、利用方法、返却方法等）を明確にし、文書化しなければならない。

2　受注者は、組織における情報資産の価値や、法的要求（個人情報の保護等）等に基づき、取扱いの慎重さの度合いや重要性の観点から情報資産を分類しなければならない。

3　本契約における各情報資産の管理責任者は、自らの責任範囲における全ての情報セキュリティ対策が、情報セキュリティポリシーに則り正しく確実に実施されるよう、定期的にレビュー及び見直しを行わなければならない。

4　受注者は、クラウドサービスの提供に用いる情報システムが、情報セキュリティポリシー上の要求を遵守していることを確認するため、定期的に点検・監査しなければならない。

（従業員に係る情報セキュリティ）

第13条　受注者は、雇用予定の従業員に対して、機密性・完全性・可用性に係る情報セキュリティ上の要求及び責任の分界点を提示・説明するとともに、この要求等に対する明確

な同意をもって雇用契約を締結しなければならない。

2　受注者は、全ての従業員及び派遣労働者等の作業従事者（以下、「従業員等」という。）に対して、情報セキュリティポリシーに関する意識向上のための適切な教育・訓練を実施しなければならない。

3　受注者は、従業員等が、情報セキュリティポリシー又はクラウドサービス提供上の契約に違反した場合の対応手続を備えなければならない。

4　受注者は、従業員等の雇用が終了又は変更となった場合等のアクセス権や情報資産等の扱いについて、実施すべき事項や手続、確認項目等を明確にしなければならない。

（情報セキュリティインシデントの管理）

第14条　受注者は、全ての従業員等に対し、業務において発見あるいは疑いをもった情報システムのぜい弱性や情報セキュリティインシデント（サービス停止、情報の漏えい・改ざん・破壊・紛失、ウイルス感染等）について、どのようなものでも記録し、できるだけ速やかに管理責任者に報告できるよう手続を定め、実施しなければならない。

また、報告を受けた後に、迅速に整然と効果的な対応ができるよう、責任体制及び手順を確立しなければならない。

（コンプライアンス）

第15条　受注者は、個人情報、機密情報、知的財産等、法令又は契約上適切な管理が求められている情報については、該当する法令又は契約を特定した上で、その要求に基づき適切な情報セキュリティ対策を実施しなければならない。

2　受注者は、クラウドサービスの提供及び継続上重要な記録（会計記録、データベース記録、取引ログ、監査ログ、運用手順等）については、法令又は契約及び情報セキュリティポリシー等の要求事項に従って、適切に管理しなければならない。

3　受注者は、利用可否範囲（対象区画・施設、利用が許可される者等）の明示、認可手続の制定、監視、警告等により、認可されていない目的のための情報システム及び情報処理施設の利用を行わせてはならない。

（ユーザサポートの責任）

第16条　受注者は、クラウドサービスの提供に支障が生じた場合には、その原因が連携クラウド事業者に起因するものであったとしても、利用者と直接契約を結ぶクラウド事業者が、その責任において一元的にユーザサポートを実施しなければならない。

（アプリケーション、プラットフォーム、サーバ・ストレージ、ネットワークに共通するセキュリティ対策）

第17条　受注者は、クラウドサービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージ、情報セキュリティ対策機器、通信機器の稼働監視（応答確認等）を行わなければならない。また、稼働停止を検知した場合は、発注者に速報を通知しなければならない。

2　受注者は、クラウドサービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージ、情報セキュリティ対策機器、通信機器の障害監視（サービスが正常に動作していることの確認）を行わなければならない。また、障害を検知した場合は、発注者に速報を通知しなければならない。

3　受注者は、クラウドサービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージ、ネットワークに対し一定間隔でパフォーマンス監視（サービスのレスポンス時間の監視）を行わなければならない。

4　受注者は、クラウドサービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージ等（情報セキュリティ対策機器、通信機器等）の時刻同期の方法を規定し、実施しなければならない。

5　受注者は、クラウドサービスの提供に用いるプラットフォーム、サーバ・ストレージ、情報セキュリティ対策機器、通信機器についての技術的ぜい弱性に関する情報（OS、その他ソフトウェアのパッチ発行情報等）を定期的に収集し、随時パッチによる更新を行わなければならない。

6　受注者は、クラウドサービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージ等（情報セキュリティ対策機器、通信機器等）の監視結果（障害監視、死活監視、パフォーマンス監視）について、定期報告書を作成して発注者等に報告しなければならない。

7　受注者は、クラウドサービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージ等（情報セキュリティ対策機器、通信機器等）に係る稼働停止、障害、パフォーマンス低下等について、速報をフォローアップする追加報告を発注者に対して行わなければならない。

8　受注者は、情報セキュリティ監視（稼働監視、障害監視、パフォーマンス監視等）の実施基準・手順等を定めなければならない。また、クラウドサービスの提供に用いるアプリケーション、プラットフォーム、サーバ、ストレージ、ネットワークの運用・管理に関する手順書を作成しなければならない。

（アプリケーション、プラットフォーム、サーバ・ストレージの運用管理）

第18条　受注者は、クラウドサービスを利用者に提供する時間帯を定め、この時間帯におけるクラウドサービスの稼働率及びアプリケーション、プラットフォーム、サーバ・ストレージの定期保守時間を規定し、発注者に報告しなければならない。

2　受注者は、クラウドサービスの提供に用いるアプリケーション、プラットフォーム、

サーバ・ストレージに対し、利用者の利用状況の予測に基づいて設計した容量・能力等の要求事項を記録した文書を作成し、保存すること。

3　受注者は、利用者の利用状況、例外処理及び情報セキュリティ事象の記録（ログ等）を取得し、記録（ログ等）の保存期間を明示しなければならない。

4　受注者はクラウドサービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージについて定期的にぜい弱性診断を行い、その結果に基づいて対策を行わなければならない。

（アプリケーション、プラットフォーム、サーバ・ストレージの情報セキュリティ対策）

第19条　受注者はクラウドサービスの提供に用いるプラットフォーム、サーバ・ストレージ（データ・プログラム、電子メール、データベース等）についてウイルス等に対する対策を講じなければならない。

2　受注者は、データベースに格納されたデータの暗号化を行わなければならない。

（サービスデータの保護）

第20条　受注者は、利用者のサービスデータ、アプリケーションやサーバ・ストレージ等の管理情報及びシステム構成情報の定期的なバックアップを実施しなければならない。

2　受注者は、バックアップされた情報が正常に記録され、正しく読み出すことができるかどうかについて定期的に確認しなければならない。

（不正アクセスの防止）

第21条　受注者は、ネットワーク構成図を作成しなければならない（ネットワークをアウトソーシングする場合を除く）。また、アクセス制御方針を策定し、これに基づいて、アクセス制御を許可又は無効とするための正式な手順を策定し、受注者に提示しなければならない。

2　受注者は、情報システム管理者及びネットワーク管理者の権限の割当及び使用を制限しなければならない。

3　受注者は、利用者及び管理者（情報システム管理者、ネットワーク管理者等）等のアクセスを管理するための適切な認証方法、特定の場所及び装置からの接続を認証する方法等により、アクセス制御となりすまし対策を行わなければならない。また、運用管理規定を作成すること。ID・パスワードを用いる場合は、その運用管理方法と、パスワードの有効期限を規定に含めなければならない。

4　受注者は、外部及び内部からの不正アクセスを防止する措置（ファイアウォール、リバースプロキシの導入等）を講じなければならない。

5　受注者は、不正な通過パケットを自動的に発見、もしくは遮断する措置（IDS/IPSの導入等）を講じなければならない。

（建物の災害対策）

第22条　受注者は、クラウドサービスの提供に用いるサーバ・ストレージ、情報セキュリティ対策機器等の情報システムが設置されている建物（情報処理施設）については、地震・水害に対する対策が行わなければならない。

（電源・空調の維持と災害対策）

第23条　受注者は、クラウドサービスの提供に用いるサーバ・ストレージ、情報セキュリティ対策機器等の情報システムを設置する場所には、停電や電力障害が生じた場合に電源を確保するための対策を講じなければならない。

2　受注者は、クラウドサービスの提供に用いるサーバ・ストレージ、情報セキュリティ対策機器等の情報システムを設置する場所では、設置されている機器等による発熱を抑えるのに十分な容量の空調を提供しなければならない。

（火災、逃雷、静電気から情報システムを防護するための対策）

第24条　受注者は、サーバルームに設置されているクラウドサービスの提供に用いるサーバ・ストレージ、情報セキュリティ対策機器等の情報システムについて、放水等の消火設備の使用に伴う汚損に対する対策を講じること。

2　受注者は、クラウドサービスの提供に用いるサーバ・ストレージ、情報セキュリティ対策機器等の情報システムを設置するサーバルームには、火災検知・通報システム及び消火設備を備えなければならない。

3　受注者は、情報処理施設に雷が直撃した場合を想定した対策を講じなければならない。

4　受注者は、情報処理施設付近に誘導雷が発生した場合を想定した対策を講じなければならない。

5　受注者は、クラウドサービスの提供に用いるサーバ・ストレージ、情報セキュリティ対策機器等の情報システムについて、作業に伴う静電気対策を講じなければならない。

（建物の情報セキュリティ対策）

第25条　受注者は、重要な物理的セキュリティ境界（カード制御による出入口、有人の受付等）に対し、個人認証システムを用いて、従業員等及び出入りを許可された外部組織等に対する入退室記録を作成し、適切な期間保存しなければならない。

2　受注者は、重要な物理的セキュリティ境界に対して監視カメラを設置し、その稼働時間と監視範囲を定めて監視を行うこと。また、監視カメラの映像をあらかじめ定められた期間保存しなければならない。

3　受注者は、重要な物理的セキュリティ境界からの入退室等を管理するための手順書を作成しなければならない。

4　受注者は、重要な物理的セキュリティ境界の出入口に破壊対策ドアを設置しなければならない。

5　受注者は、重要な物理的セキュリティ境界に警備員を常駐させなければならない。

6　受注者は、サーバルームやラックの鍵管理を行わなければならない。

（機密性・完全性を保持するための対策）

第26条　受注者は、電子データの原本性確保を行わなければならない。

2　受注者は、個人情報は関連する法令に基づいて適切に取り扱わなければならない。

（クラウド事業者の運用管理端末における情報セキュリティ対策）

第27条　受注者は、運用管理端末に、許可されていないプログラム等のインストールを行わせてはならない。また、従業員等が用いる運用管理端末の全てのファイルのウイルスチェックを行わなければならない。また、技術的ぜい弱性に関する情報（OS、その他ソフトウェアのパッチ発行情報等）を定期的に収集し、随時パッチによる更新を行わなければならない。

宇治市個人情報の取扱いに関する特記仕様書の項目遵守の確認表（ASPサービス用）

記入欄の☆印は確認の必須項目とする

項番		点検項目	参照条文	記入欄
1	1			ISMS（情報セキュリティマネジメントシステム）の認証を取得していますか □ はい　□ いいえ プライバシーマークの認証を取得していますか □ はい　□ いいえ
2	1	第1条 基本的事項	1 受注者は、個人情報の保護の重要性を認識し、この契約による業務を実施するに当たっては、宇治市情報セキュリティポリシー及び関係法令等の規定に従い、個人の権利利益を侵害することのないよう、個人情報の取扱いを適切に行わなければならない	☆ 本委託業務の実施に当たっては、個人の権利利益を侵害することがないよう、個人情報の取扱いを適正に行わなければならないことを理解していますか □ はい　□ いいえ
	2			☆ 本委託業務の実施に当たっては、個人の権利利益を侵害することがないよう、個人情報の取扱いを適正に行わなければならないことを作業従事者に周知し、理解させていますか □ はい　□ いいえ （はいを選択した場合） 理解させた本委託業務の実施に当たっては、個人の権利利益を侵害することがないよう、個人情報の取扱いを適正に行わなければならないことを作業従事者に周知し、理解させた結果を記録していますか □ はい　□ いいえ
3	1	第2条 秘密の保持	受注者は、この契約の履行により直接又は間接に知り得た個人情報を第三者に漏らしてはならない。この契約が終了し、又は解除された後においても、同様とする。	☆ 委託された業務の履行にあたり、直接又は間接的に知り得た個人情報を第三者に漏洩してはいけないことを、個人情報取扱いに係る責任者及び従事者に教育又は周知をしていますか □ はい　□ いいえ （はいを選択した場合） 個人情報取扱いに係る責任者及び従業者に対する秘密保持に関する教育又は周知の結果を記録していますか □ はい　□ いいえ
	2			☆ 秘密保持に関する誓約書を個人情報取扱いに係る作業責任者及び作業従事者から取得していますか □ はい　□ いいえ （はいを選択した場合） 作業責任者及び作業従業者から取得した誓約書は、保存され、参照できるようになっていますか □ はい　□ いいえ
	3			秘密保持に関する誓約書には、在職中及び職を退いた後も、職務上知り得た秘密を漏らしてはならないことを明記していますか □ はい　□ いいえ
	4			故意または過失により、秘密保持に関する誓約書に違反し、事故を招いてしまった場合の罰則について、社内ルール等に定めていますか □ はい　□ いいえ （はいを選択した場合） その罰則規定を、正社員だけでなく非正社員にも適用していますか □ はい　□ いいえ （いいえを選択した場合） 誓約書を取得していない理由を記述してください ＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿
4	1	第3条 目的外収集・利用の禁止	1 受注者は、この契約による業務を処理するため取得し、若しくは作成した情報（情報の全部又は一部を複写	☆ 本委託業務において個人情報を収集する場合について、その目的を明確にし必要最小限のものとしなければならないことを理解していますか □ はい　□ いいえ

	2		等した他の媒体を含む。以下同じ。）又は発注者から引き渡された情報を発注者の指示又は承諾を得ることなくこの契約の目的以外に使用し、又は第三者に提供してはならない。	☆ 本委託業務において利用する個人情報について、受託業務外での利用及び第三者への提供が禁止であることを従事者に周知し、理解させていますか □ はい　□ いいえ （はいを選択した場合） 本委託業務において個人情報を収集する場合について、その目的を明確にし必要最小限のものとしなければならないことを従事者に周知し、理解させた結果を記録していますか □ はい　□ いいえ
	3			☆ 本委託業務において個人情報を収集する場合について、その目的を明確にしますか □ はい　□ いいえ （いいえを選択した場合） 個人情報を収集する場合について、その目的を明確にしない理由を記述してください ＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿
	4			☆ 本委託業務において利用する個人情報について、受託業務外での利用が禁止であることを理解していますか □ はい　□ いいえ
	5			☆ 本委託業務において利用する個人情報について、受託業務外での利用が禁止であることを従事者に周知し、理解させていますか □ はい　□ いいえ （はいを選択した場合） 受託業務外での利用が禁止であることを従事者に周知させ、理解させた結果を記録していますか □ はい　□ いいえ
	6			☆ 本委託業務において利用する個人情報について、発注者の承諾なしに第三者へ提供してはならないことを理解していますか □ はい　□ いいえ
	7			☆ 本委託業務において利用する個人情報について、受託業務外での第三者への提供が禁止であることを作業従事者に周知し、理解させていますか □ はい　□ いいえ （はいを選択した場合） 受託業務外での第三者への提供が禁止であることを従事者に周知し、理解させた結果を記録していますか □ はい　□ いいえ
5	1	第4条 複写、複製の禁止	受注者は、データバックアップを除き、この契約による事務を処理するため発注者から引き渡しを受け、又は受注者自らが収集し、若しくは作成した個人情報が記録された資料等を、発注者の承諾なしに複写し、又は複製してはならない。	☆ 本委託業務において利用する個人情報について、データバックアップを除き、発注者の承諾なしに複写し、又は複製してはならないことを理解していますか □ はい　□ いいえ
	2			☆ 本委託業務において利用する個人情報について、データバックアップを除き、発注者の承諾なしに複写し、又は複製してはならないことを作業従事者に周知し、理解させていますか □ はい　□ いいえ （はいを選択した場合） 委託業務外での発注者の承諾なしに複写し、又は複製してはならないことを作業従事者に周知させ、理解させた結果を記録していますか □ はい　□ いいえ
6	1	第5条 適正管理	受注者は、この契約による事務を処理するため発注者から引き渡しを受け、又は受注者自らが収集し、若しくは作成した個人情報の滅失及び毀損の防止に関する措	☆ 本委託業務において利用する個人情報について、滅失及びき損の防止に関する措置を講じなければならないことを理解していますか □ はい　□ いいえ
	2			☆ 本委託業務において利用する個人情報について、滅失及びき損の防止に関する措置を講じなければならないことを従事者に周知し、理解させていますか

			置を講じなければならない。	□ はい　□ いいえ （はいを選択した場合） 本委託業務において利用する個人情報について、滅失及びき損の防止に関する措置を講じなければならないことを従事者に周知させ、理解させた結果を記録していますか □ はい　□ いいえ
7	1	第6条 個人情報の返還又は廃棄	（個人情報の帰属及び返還、廃棄又は消去） 1 発注者から引き渡された個人情報のほか、この契約による業務を処理するために発注者の指定した様式により、及び発注者の名において、受注者が取得し、作成し、加工し、複写し、又は複製等した個人情報は、発注者に帰属するものとする。 2 受注者は、委託業務完了時に、発注者の指示に基づいて、前項の個人情報を返還し、廃棄し、又は消去しなければならない。 3 受注者は、第1項の個人情報を返還する場合は、全ての資料（資料名称や情報項目、媒体名、数量等の内容がわかるもの）の明細とともに返還し、複製された資料等がないことを証する書面を発注者に提出しなければならない。 4 受注者は、第1項の個人情報を廃棄、又は消去する場合、当該個人情報が記録された電磁的記録媒体の物理的な破壊その他当該個人情報を判読及び復元できないように確実な方法で廃棄し、又は消去しなければならない。 5 受注者は、第1項の個人情報を廃棄し、又は消去した時は、完全に廃棄し、又は消去した旨の証明書（情報項目、媒体名、数量、廃棄若しくは消去の方法、責任者、廃棄又は消去の年月日が記載された書面）を発注者に提出しなければならない。 6 受注者は、廃棄又は消去に際し、発注者から立会いを求められたときはこれに応じなければならない。	☆ 発注者の許可無く個人情報の廃棄を行ってはいけないことを理解していますか □ はい　□ いいえ
	2			☆ 個人情報を発注者へ返却するときの手順を定めていますか □ はい　□ いいえ
	3			☆ 個人情報を発注者へ返却するとき、返却の記録を残すことができますか □ はい　□ いいえ （はいを選択した場合） 個人情報返却の記録から何が判断できますか。以下のうち当てはまる項目すべてにチェックしてください □ 返却の日時が判断できる □ 返却の担当者が判断できる □ 返却の処理内容が判断できる □ その他　（具体的に:　　）
	4			☆ 本委託業務において利用する個人情報が不必要となった場合、廃棄又は消去することができますか □ はい　□ いいえ （はいを選択した場合） ☆ 個人情報の廃棄または消去の際には、電磁的記録媒体等に記録されているデータが判読できないよう必要な措置を実施することができますか □ はい　□ いいえ 個人情報の廃棄又は消去の具体的な方法や手段を記述してください ＿＿＿＿＿＿＿＿＿＿ 個人情報の廃棄又は消去の記録を残すことができますか □ はい　□ いいえ （はいを選択した場合） 個人情報の廃棄又は消去の記録から何が判断できますか。以下のうち当てはまる項目すべてにチェックしてください □ 廃棄又は消去を実施した年月日が判断できる □ 廃棄又は消去を実施した担当者が判断できる □ 廃棄又は消去の方法や手段が判断できる □ その他　（具体的に:　　） 個人情報の廃棄又は消去は発注者の立会いのもとで行うことができますか □ はい　□ いいえ （いいえを選択した場合） 個人情報の廃棄又は消去を行うことができない理由を記述してください ＿＿＿＿＿＿＿＿＿＿
	5			☆ （個人情報の複製物がある場合） 業務完了後又は業務に必要なくなった時点で個人情報の複製物を廃棄又は消去することができますか □ はい　□ いいえ （はいを選択した場合） 個人情報の複製物の廃棄または消去の際には、電磁的記録媒体等に記録されているデータが判読できないよう必要な措置を実施することができますか □ はい　□ いいえ

	6		個人情報の複製物の廃棄又は消去の具体的な方法や手段を記述してください _____
	7		個人情報の複製物の廃棄又は消去の記録を残すことができますか ☐ はい　☐ いいえ （はいを選択した場合） 廃棄又は消去の記録から何が判断できますか。以下のうち当てはまる項目すべてにチェックしてくだ ☐ 廃棄又は消去を実施した年月日が判断できる ☐ 廃棄又は消去を実施した担当者が判断できる ☐ 廃棄又は消去の方法や手段が判断できる ☐ その他　（具体的に:　）
	8		提供された個人情報の複製物の廃棄又は消去は発注者の立会いのもとで行うことができますか ☐ はい　☐ いいえ （いいえを選択した場合） 個人情報の複製物の廃棄又は消去を行うことができない理由を記述してください _____
	9		☆ 業務完了後、発注者から提供を受け、又は自らが収集し、若しくは作成した個人情報が記録された全ての資料等は、その契約完了後直ちに発注者に返還することができますか

				□ はい　　□ いいえ （はいを選択した場合） 返還する資料については、資料名称や個人情報の項目、媒体名、数量等内容のわかる明細とともに引き渡すことはできますか □ はい　　□ いいえ （はいを選択した場合） 複製された資料等がないことを証する書面を提出できますか。 □ はい　　□ いいえ （いいえを選択した場合） 複製された資料等がないことを証する書面を提出することができない理由を記述してください ＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿
8	1	第7条 事故時等の対応	1 受注者は、この契約による業務の処理に関して個人情報の漏えい等の事故が発生し、又は発生するおそれがある場合は、その事故等に係る帰責の有無に関わらず、直ちに発注者に対して、当該個人情報の漏えい等の事故に係る個人情報の内容、数量、発生場所、発生状況等を報告し、その指示に従わなければならない。	☆ セキュリティ事故が発生した場合は、その事故発生に係る帰責の有無にかかわらず、直ちに発注者に、個人情報の内容、数量、事件又は事故の発生場所、発生状況等を書面により報告し、発注者の指示に従わなければならないことを理解していますか □ はい　　□ いいえ
	2		2　受注者は、個人情報の漏洩等の事故が発生した場合に備え、発注者その他の関係者との連絡、証拠保全、被害拡大の防止、復旧、再発防止の措置を迅速かつ適切に実施するために、緊急時対応計画を定めなければならない。	☆ 個人情報の紛失、漏洩、改ざん、破損その他の事故が発生した場合に備え、措置を迅速に行うための緊急時対応計画を定めていますか □ はい　　□ いいえ （はいを選択した場合） 緊急時対応計画には、何について記載していますか。以下のうち当てはまる項目すべてにチェックしてください □ 証拠保全に関する活動について記載されている □ 被害拡大の防止に関する活動について記載されている □ 復旧に関する活動について記載されている □ 再発防止に関する活動について記載されている □ 地方公共団体への連絡に関する活動について記載されている （連絡に関する活動が記載されている にチェックした場合） 何について連絡するよう定められていますか。以下のうち当てはまる項目すべてにチェックしてください □ 個人情報の内容 □ 個人情報の数量 □ 事件又は事故の発生場所 □ 発生状況等 □ その他　（具体的に:　　） □ その他　（具体的に:　　） 緊急時対応計画のコピーを提出してください。また、当該資料の名称及び参照箇所を下記に記述してください ＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿
	3		3　発注者は、本委託業務に関し個人情報の漏洩等の事故が発生した場合は、必要に応じて当該事故に関する情報を公表することができる。	☆ セキュリティ事故が発生した場合、発注者により当該事故の内容等の公表を必要に応じ行うことができることを理解していますか □ はい　　□ いいえ

9	1	第10条 情報セキュリティへの組織的取組の基本方針	1　受注者は、情報セキュリティに関する組織的取組についての基本的な方針を定めた文書を作成しなければならない。また、当該文書には、経営陣が承認の署名等を行い、情報セキュリティに関する経営陣の責任を明確にしなければならない。	☆ 情報セキュリティに関する組織的取組についての基本的な方針を定めた文書を作成していますか。 □　はい　　□　いいえ （はいを選択した場合） 以下のうち記述している項目を全てチェックしてください。 □　情報セキュリティの定義、目的及び適用範囲 □　事業戦略や事業目的に照らし合わせた経営陣の情報セキュリティに対する重要性の考え方 □　経営陣が情報セキュリティへの組織的取組の目標と原則を支持していること □　体制の構築と情報資産保護への取組の宣言 □　組織における遵守事項の宣言 □　見直し及び改善への取組の宣言 □　その他（　　）
	2			☆ 当該文書には、経営陣が承認の署名等を行い、情報セキュリティに関する経営陣の責任を明確にしていますか。 □　はい　　□　いいえ
	3			作成した情報セキュリティに関する組織的取組についての基本的な方針（以下「情報セキュリティに関する基本的な方針」という。）を定めた文書について、全ての従業員及び利用者並びに外部組織に対して公表し、通知していますか。 □　はい　　□　いいえ
	4		2　受注者は、情報セキュリティに関する基本的な方針を定めた文書について、定期的又はクラウドサービスの提供に係る重大な変更が生じた場合（組織環境、業務環境、法的環境、技術的環境等）に見直しを行わなければならない。この見直しの結果、変更の必要性が生じた場合には、経営陣の承認の下で改定等を実施しなければならない。	☆ 情報セキュリティに関する基本的な方針を定めた文書について、定期的又はクラウドサービスの提供に係る重大な変更が生じた場合（組織環境、業務環境、法的環境、技術的環境等）に見直しを行っていますか。 □　はい　　□　いいえ
	5			☆ 見直しの結果、変更の必要性が生じた場合には、経営陣の承認の下で改定等を実施していますか。 □　はい　　□　いいえ
10	1	第11条 サービス事業者の組織	1　受注者は、外部組織が関わる業務プロセスにおける情報資産に対するリスクを識別し、適切な対策を実施しなければならない。	☆ 受注者は、外部組織が関わる業務プロセスにおける情報資産に対するリスクを識別し、適切な対策を実施していますか。 □　はい　　□　いいえ
	2			不正アクセス、情報資産の盗難・不正変更、情報処理設備の悪用・破壊等のリスクを軽減するために、外部組織（特に、データセンタ、電気通信事業者、情報セキュリティサービス提供事業者等）による情報資産へのアクセスを管理・制限していますか。 □　はい　　□　いいえ （はいを選択した場合） 以下のうち情報資産にアクセス可能な外部組織すべてにチェックしてください。 □　情報処理施設に定期・不定期に出入りする外部組織（配送業者、設備点検等） □　情報処理施設に常駐する外部組織（SE、警備会社等） □　ネットワークを通じサービスを提供する外部組織（ネットワーク監視サービス等）
	3			情報資産へアクセスする手段を区別し、それぞれに対してアクセスを管理・制限する方針と方法を定めていますか。 □　はい　　□　いいえ

	4		2　受注者は、情報資産へのアクセスが可能となる外部組織との契約においては、想定される全てのアクセスについて、その範囲を規定しなければならない。	☆ 情報資産へのアクセスが可能となる外部組織との想定されるアクセスについて、その範囲を規定していますか。 □　はい　　□　いいえ （はいを選択した場合） 以下のうち外部組織によるアクセス手法すべてにチェックしてください。 □　物理的セキュリティ境界からの入退室 □　情報システムの管理用端末の利用 □　外部ネットワークからの接続 □　データを格納した媒体の交換
11	1	第12条 情報資産の管理	1　受注者は、取り扱う各情報資産について、管理責任者を定めるとともに、その利用の許容範囲（利用可能者、利用目的、利用方法、返却方法等）を明確にし、文書化しなければならない。	☆ 取り扱う各情報資産について、管理責任者を定めるとともに、その利用の許容範囲（利用可能者、利用目的、利用方法、返却方法等）を明確にし、文書化していますか。 □　はい　　□　いいえ （はいを選択した場合） 以下のうち文書化しているものすべてにチェックしてください。 □　情報資産の分類方法と各情報資産の管理責任者 □　情報資産の重要度（業務上の価値に基づいて決定） □　情報資産の保護のレベル（例：機密性・完全性・可用性に対する要求レベル）を各情報資産が直面するリスクの大きさ
	2			情報資産の目録を作成し、情報セキュリティインシデントから復旧するために必要な全ての情報を記載していますか。 □　はい　　□　いいえ （はいを選択した場合） 以下のうち目録を作成しているものすべてにチェックしてください。 □　情報資産の種類 □　情報資産の形式 □　情報資産の所在 □　バックアップ情報 □　ライセンス情報
	3			情報資産の目録における記載内容は、他の目録における記載内容と整合がとれていますか。 □　はい　　□　いいえ
	4			全ての従業員及び外部組織に対して、情報資産の利用の許容範囲に関する規則に従うよう、義務付けていますか。 □　はい　　□　いいえ
	5		2　受注者は、組織における情報資産の価値や、法的要求（個人情報の保護等）等に基づき、取扱いの慎重さの度合いや重要性の観点から情報資産を分類しなければならない。	☆ 組織における情報資産の価値や、法的要求（個人情報の保護等）等に基づき、取扱いの慎重さの度合いや重要性の観点から情報資産を分類していますか。 □　はい　　□　いいえ 情報資産の分類結果は、ラベル付け等により、従業員等に対して明示していますか。 □　はい　　□　いいえ
	6			情報資産の分類及び保護管理策の選定においては、情報資産の共有又は利用制限に係る業務上の必要性とこれにより生じる影響が考慮されていますか。 □　はい　　□　いいえ
	7			情報資産の分類レベルごとに、安全な取扱い手順（処理・保存・伝達・秘密解除・破棄等）を定めていますか。 □　はい　　□　いいえ
	8			取扱いに慎重を要する又は重要と分類される情報を含むシステム出力には、適切な分類ラベルを付与していますか。 □　はい　　□　いいえ （はいを選択した場合）

				以下のうちシステム出力しているものすべてにチェックしてください。 □ 印刷された文書 □ スクリーン表示 □ 記録媒体（例えば、テープ、ディスク、CD） □ 電子的なメッセージ □ 転送ファイル
	9		3 本契約における各情報資産の管理責任者は、自らの責任範囲における全ての情報セキュリティ対策が、情報セキュリティポリシーに則り正しく確実に実施されるよう、定期的にレビュー及び見直しを行わなければならない。	☆ 本契約における各情報資産の管理責任者は、自らの責任範囲における全ての情報セキュリティ対策が、情報セキュリティポリシーに則り正しく確実に実施されるよう、定期的にレビュー及び見直しを実施していますか。 □ はい □ いいえ
	10			管理責任者は、自らの責任範囲における全ての情報セキュリティ対策が、情報セキュリティポリシーに則り正しく確実に実施されるよう、レビュー及び見直しの方法をあらかじめ定めていますか。 □ はい □ いいえ 管理責任者が実施したレビュー及び見直しの結果を記録し、その記録を保管管理していますか。 □ はい □ いいえ
	11		4 受注者は、クラウドサービスの提供に用いる情報システムが、情報セキュリティポリシー上の要求を遵守していることを確認するため、定期的に点検・監査しなければならない。	☆ クラウドサービスの提供に用いる情報システムが、情報セキュリティポリシー上の要求を遵守していることを確認するため、定期的に点検・監査していますか。 □ はい □ いいえ
	12			点検・監査は、十分な技術的能力及び経験を持つ内部の者（例：情報処理安全確保支援士資格を持ち、情報セキュリティに係る技術的対策の実務を一定年数以上経験している者）又は必要に応じて外部の専門家の監督の下で行っていますか。 □ はい □ いいえ
	13			情報システムの点検・監査を実施する際はクラウドサービスの提供中断によるリスクを最小限に抑えるよう考慮されていますか。 □ はい □ いいえ
12	1	第13条 従業員に係る情報セキュリティ	1 受注者は、雇用予定の従業員に対して、機密性・完全性・可用性に係る情報セキュリティ上の要求及び責任の分界点を提示・説明するとともに、この要求等に対する明確な同意をもって雇用契約を締結しなければならない。	☆ 雇用予定の従業員に対して、機密性・完全性・可用性に係る情報セキュリティ上の要求及び責任の分界点を提示・説明するとともに、この要求等に対する明確な同意をもって雇用契約を締結していますか。 □ はい □ いいえ
	2			雇用条件には、情報セキュリティに関する基本的な方針を反映させていますか。 □ はい □ いいえ （はいを選択した場合） 以下のうち雇用条件に記載しているすべてにチェックしてください。 □ 取扱注意情報へのアクセス権を与えられる全ての従業員に対して、アクセスが認められる前に、秘密保持契約書又は守秘義務契約書に署名を求めること □ 従業員の法的な責任について □ 従業員が担うべき情報資産に対する責任 □ 雇用契約を締結する過程で取得した個人情報の扱いに関する組織の責任 □ 雇用終了後も、一定期間は雇用期間における責任が継続すること
	3			雇用終了後も、一定期間は雇用期間における責任が継続するよう、雇用条件を規定していますか。 □ はい □ いいえ
	4		2 受注者は、全ての従業員及び派遣労働者等の作業従事者（以下、「従業員等」という。）に対して、情報セキュリティポリシーに関	☆ 全ての従業員等に対して、情報セキュリティポリシーに関する意識向上のための教育を実施していますか。 □ はい □ いいえ

	5		する意識向上のための適切な教育・訓練を実施しなければならない。	☆ 全ての従業員等に対して、情報セキュリティポリシーに関する意識向上のための訓練を実施していますか。 □ はい　□ いいえ
	6		3　受注者は、従業員等が、情報セキュリティポリシー又はクラウドサービス提供上の契約に違反した場合の対応手続を備えなければならない。	☆ 雇用条件において、従業員等が情報セキュリティポリシー等に従わない場合の対応手続等を明確にしていますか。 □ はい　□ いいえ
	7		4　受注者は、従業員等の雇用が終了又は変更となった場合等のアクセス権や情報資産等の扱いについて、実施すべき事項や手続、確認項目等を明確にしなければならない。	☆ 従業員等の雇用が終了又は変更となった場合等のアクセス権や情報資産等の扱いについて、実施すべき事項や手続、確認項目等を明確にしていますか。 □ はい　□ いいえ （はいを選択した場合） 以下のうち該当するものについてすべてにチェックしてください。 □ 雇用終了時には、支給したソフトウェア、電子ファイル等の電子媒体、会社の書類、手引書等の紙媒体、モバイルコンピューティング装置、アクセスカード等の設備等、全ての返却を求めていること □ 雇用終了後には、情報資産に対する個人のアクセス権を速やかに削除すること □ 雇用の変更を行う場合には、新規の業務に対して承認されていない全てのアクセス権を削除すること □ アクセス権の削除に当たっては、情報システムへの物理的なアクセスキー（情報処理施設の鍵、身分証明書等）の返却だけではなく、電子的なアクセスキー（パスワード等）等を消去すること □ 雇用終了後には、組織の現行の一員であることを認定する書類から削除すること □ 雇用が終了又は変更となる従業員が、稼働中の情報システム等の情報資産にアクセスするために必要なアクセスキーを知っている場合には、雇用の終了又は変更時に当該情報資産へのアクセスキーを変更すること
13	1	第14条 情報セキュリティインシデントの管理	受注者は、全ての従業員等に対し、業務において発見あるいは疑いをもった情報システムのぜい弱性や情報セキュリティインシデント（サービス停止、情報の漏えい・改ざん・破壊・紛失、ウイルス感染等）について、どのようなものでも記録し、できるだけ速やかに管理責任者に報告できるよう手続を定め、実施しなければならない。また、情報システムのぜい弱性や情報セキュリティインシデント報告を受けた後に、迅速に整然と効果的な対応ができるよう、責任体制及び手順を確立しなければならない。	☆ 全ての従業員等に対し、業務において発見あるいは疑いをもった情報システムのぜい弱性や情報セキュリティインシデント（サービス停止、情報の漏えい・改ざん・破壊・紛失、ウイルス感染等）について、どのようなものでも記録し、できるだけ速やかに管理責任者に報告できるよう手続を定めた上で実施していますか。 □ はい　□ いいえ
	2			☆ 情報システムのぜい弱性や情報セキュリティインシデント報告を受けた後に、迅速に整然と効果的な対応ができるよう、責任体制及び手順を確立していますか。 □ はい　□ いいえ 情報セキュリティインシデント及びぜい弱性をハンドリングする組織（CSIRT 等）と連携して情報セキュリティインシデントの正式な報告手順を、報告を受けた後のインシデント対応及び段階的取扱い（例：原因切り分け、部分復旧、完全復旧のフェーズに分けた取扱い）の手順と共に確立していますか。 □ はい　□ いいえ
	3			情報セキュリティインシデントの報告手順は全ての従業員等に周知徹底していますか。 □ はい　□ いいえ
	4			情報セキュリティインシデント報告のための連絡先を取りまとめていますか。 □ はい　□ いいえ
	5			この連絡先を全ての従業員等が認識し、いつでも利用できるようにすることで、適切で時機を逸しない対応を確実に実施していますか。 □ はい　□ いいえ

	6			全ての従業員等に対し、情報システムのぜい弱性や情報セキュリティインシデントの予兆等の情報資産に対する危険を発見した場合には、いかなる場合であってもできる限り速やかに管理責任者に報告する義務があることを認識させていますか。 □ はい　□ いいえ
	7			収集した情報セキュリティインシデント情報を分析し、必要に応じて対策の見直しを実施していますか。 □ はい　□ いいえ
14	1	第15条 コンプライアンス	1　受注者は、個人情報、機密情報、知的財産等、法令又は契約上適切な管理が求められている情報については、該当する法令又は契約を特定した上で、その要求に基づき適切な情報セキュリティ対策を実施しなければならない。	☆ 個人情報、機密情報、知的財産等、法令又は契約上適切な管理が求められている情報については、該当する法令又は契約を特定した上で、その要求に基づき適切な情報セキュリティ対策を実施していますか。 □ はい　□ いいえ （はいを選択した場合） 以下のうちセキュリティ対策について参照しているガイドライン等についてすべてにチェックしてください。 □ 個人情報保護法関係のガイドライン □ 不正競争防止法関係のガイドライン □ 著作権法関係のガイドライン □ e文書法関係のガイドライン □ 電子帳簿保存法関係のガイドライン □ その他（　　）
	2			個人情報や機密情報等を保存する場所は国内法が適用される範囲に位置していますか。 □ はい　□ いいえ
	3		2　受注者は、クラウドサービスの提供及び継続上重要な記録（会計記録、データベース記録、取引ログ、監査ログ、運用手順等）については、法令又は契約及び情報セキュリティポリシー等の要求事項に従って、適切に管理しなければならない。	☆ クラウドサービスの提供及び継続上重要な記録（会計記録、データベース記録、取引ログ、監査ログ、運用手順等）については、法令又は契約及び情報セキュリティポリシー等の要求事項に従って、適切に管理していますか。 □ はい　□ いいえ （はいを選択した場合） 以下のうち当てはまる管理方法についてすべてにチェックしてください。 □ 記録類は、記録の種類（例：会計記録、データベース記録、ログ記録、運用手順等）によって大分類し、さらにそれぞれの種類において保存期間と記録媒体の種別（例：紙、光媒体、磁気媒体等）によって細分類している □ 記録の保存は媒体の製造業者の推奨仕様に従って行っている □ 媒体が劣化する可能性を考慮し、長期保存のためには紙又はマイクロフィルムを利用している □ 国又は地域の法令又は規制によって保存期間が定められている記録を確実に特定している
	4		3　受注者は、利用可否範囲（対象区画・施設、利用が許可される者等）の明示、認可手続の制定、監視、警告等により、認可されていない目的のための情報システム及び情報処理施設の利用を行わせてはならない。	☆ 利用可否範囲（対象区画・施設、利用が許可される者等）の明示、認可手続の制定、監視、警告等により、認可されていない目的のための情報システム及び情報処理施設の利用を制限していますか。 □ はい　□ いいえ
	5			情報システム又は情報処理施設を利用しようとする者に対して、利用しようとしている情報システム又は情報処理施設がクラウド事業者の所有であること、認可されていない目的のためアクセスは許可されないこと等について、警告文を画面表示する等によって警告していますか。 □ はい　□ いいえ
	6			情報システム又は情報処理施設を利用しようとする者に対しての認可されていない目的のためアクセスは許可されないこと等について同意を求めていますか。（利用者については、サービスの利便性を考慮し、クラウドサービスの利用開始時にのみ同意を求めることで対応することも可能） □ はい（常時 ・ 開始時のみ）　□ いいえ
15	1	第16条 ユーザサポートの責任	受注者は、クラウドサービスの提供に支障が生じた場合には、その原因が連携クラウド事業者	☆ クラウドサービスの提供に支障が生じた場合には、その原因が連携クラウド事業者に起因するものであったとしても、利用者と直接契約を結ぶクラウド事業者が、その責任において一元的にユーザサポートを実施できますか。

			に起因するものであったとしても、利用者と直接契約を結ぶクラウド事業者が、その責任において一元的にユーザサポートを実施しなければならない。	□ はい　□ いいえ
	2			連携クラウド事業者が提供しているクラウドサービス部分に係るユーザサポートについては、利用者便益を最優先した方法によって実施できますか。 □ はい　□ いいえ （はいを選択した場合） クラウド事業者は、連携クラウド事業者との間で利用者からの故障対応要求や業務問合せ、作業依頼等に対する取扱手続を定め、合意を得た手段で実施できますか。 □ はい　□ いいえ
16	1	第17条 アプリケーション、プラットフォーム、サーバ・ストレージ、ネットワークに共通するセキュリティ対策	1 受注者は、クラウドサービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージ、情報セキュリティ対策機器、通信機器の稼働監視（応答確認等）を行わなければならない。また、稼働停止を検知した場合は、発注者に速報を通知しなければならない。	☆ クラウドサービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージ、情報セキュリティ対策機器、通信機器の稼働監視（応答確認等）を定期的に実施していますか。 □ はい　□ いいえ
	2			☆ 稼働停止を検知した場合は、発注者に速報を通知することができますか。 □ はい　□ いいえ
	3			監視対象機器の死活監視を行うための方法（pingコマンドなど）、監視インターバル、監視時間帯、監視体制等の実施基準・手順等を明確にしていますか。 □ はい　□ いいえ
	4			実施基準・手順等に従い監視を行い、監視結果について評価・見直しを行っていますか。 □ はい　□ いいえ
	5		2 受注者は、クラウドサービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージ、情報セキュリティ対策機器、通信機器の障害監視（サービスが正常に動作していることの確認）を行わなければならない。また、障害を検知した場合は、発注者に速報を通知しなければならない。	☆ クラウドサービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージ、情報セキュリティ対策機器、通信機器の障害監視（サービスが正常に動作していることの確認）を定期的に実施していますか。 □ はい　□ いいえ
	6			☆ 障害を検知した場合は、発注者に速報を通知することができますか。 □ はい　□ いいえ
	7			サービス稼働状態を監視するための方法、監視インターバル、監視時間帯、監視体制等の実施基準・手順等を明確にしていますか。 □ はい　□ いいえ
	8			実施基準・手順等に従い監視を行い、監視結果について評価・見直しを行っていますか。 □ はい　□ いいえ
	9		3 受注者は、クラウドサービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージ、ネットワークに対し一定間隔でパフォーマンス監視（サービスのレスポンス時間の監視）を行わなければならない。	クラウドサービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージ、ネットワークに対し一定間隔でパフォーマンス監視（サービスのレスポンス時間の監視）を定期的に実施していますか。 □ はい　□ いいえ
	10			監視の実施にあたり、監視方法（コマンドの入力手順、監視ツールの操作手順等）、監視インターバル、監視時間帯、監視体制等の実施基準・手順等を明確にしていますか。
	11			監視の結果、クラウドサービスのレスポンス時間が大きく増加した場合には、SLA 等の利用者との取決めに基づいて、利用者側の管理連絡窓口に速報を通知できますか。 □ はい　□ いいえ
	12			管理責任者は、監視結果をレビューし、必要ならば実施基準・手順等の評価・見直しを行うことができますか。 □ はい　□ いいえ

13	4 受注者は、クラウドサービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージ等（情報セキュリティ対策機器、通信機器等）の時刻同期の方法を規定し、実施しなければならない。	☆	クラウドサービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージ等（情報セキュリティ対策機器、通信機器等）の時刻同期の方法を規定し、実施していますか。 □ はい　□ いいえ （はいを選択した場合） 実施している項目全てにチェックしてください。 □ タイムビジネス信頼・安心認定制度における時刻提供精度要求等を参考にして、日本標準時との同期を取っている □ サーバ・ストレージ間においても時刻同期を取っている。 □ 定期的に時刻同期の状況を確認している
14			全ての機器の時刻同期を行う方法、及び時刻に誤差が生じた場合の修正方法（例：NTPサーバの利用等）について明確にできますか。 □ はい　□ いいえ
15	5 受注者は、クラウドサービスの提供に用いるプラットフォーム、サーバ・ストレージ、情報セキュリティ対策機器、通信機器についての技術的ぜい弱性に関する情報（OS、その他ソフトウェアのパッチ発行情報等）を定期的に収集し、随時パッチによる更新を行わなければならない。	☆	クラウドサービスの提供に用いるプラットフォーム、サーバ・ストレージ、情報セキュリティ対策機器、通信機器についての技術的ぜい弱性に関する情報（OS、その他ソフトウェアのパッチ発行情報等）を定期的に収集し、随時パッチによる更新を実施していますか。 □ はい　□ いいえ
16			情報セキュリティに関する情報を提供している機関（@police、JPCERT/CC、IPA セキュリティセンター等）やセキュリティベンダ、ハードウェアベンダ、ソフトウェアベンダ、オープンソフトウェア・フリーソフトウェア等のセキュリティ情報を提供しているWeb サイト等からぜい弱性に関する情報を入手していますか。 □ はい　□ いいえ
17			ぜい弱性が発見された場合は、提供されたパッチを適用することによる情報システムへの影響を確認した上で、パッチ適用等による対応を実施できますか。 □ はい　□ いいえ
18	6 受注者は、クラウドサービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージ等（情報セキュリティ対策機器、通信機器等）の監視結果（障害監視、死活監視、パフォーマンス監視）について、定期報告書を作成して発注者等に報告しなければならない。		クラウドサービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージ等（情報セキュリティ対策機器、通信機器等）の監視結果（障害監視、死活監視、パフォーマンス監視）について、定期報告書を作成して発注者等に報告できますか。 □ はい　□ いいえ （はいを選択した場合） 稼働率、SLA の実施結果、パフォーマンス監視結果等について報告書により、発注者に定期的に報告できますか。 □ はい　□ いいえ
19			
20			定期報告内容は、月単位で集計できますか。 □ はい　□ いいえ
21	7 受注者は、クラウドサービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージ等（情報セキュリティ対策機器、通信機器等）に係る稼働停止、障害、パフォーマンス低下等について、速報をフォローアップする追加報告を発注者に対して行わなければならない。	☆	クラウドサービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージ等（情報セキュリティ対策機器、通信機器等）に係る稼働停止、障害、パフォーマンス低下等について、速報をフォローアップする追加報告を発注者に対して実施できますか。 □ はい　□ いいえ
22			稼働停止、障害、パフォーマンス低下、その他の情報セキュリティ事象について、第一報（速報）に続いて、より詳しい分析報告を発注者に対して実施できますか。 □ はい　□ いいえ
23			原因の分析結果や復旧の予測を含んだ報告を実施できますか。 □ はい　□ いいえ
24	8 受注者は、情報セキュリティ監視（稼働監視、障害監視、パフォーマンス監視等）の実施基準	☆	情報セキュリティ監視（稼働監視、障害監視、パフォーマンス監視等）の実施基準・手順等を定めていますか。 □ はい　□ いいえ

			監視対象実施基準・手順等を定めなければならない。また、クラウドサービスの提供に用いるアプリケーション、プラットフォーム、サーバ、ストレージ、ネットワークの運用・管理に関する手順書を作成しなければならない。	
	25			☆ クラウドサービスの提供に用いるアプリケーション、プラットフォーム、サーバ、ストレージ、ネットワークの運用・管理に関する手順書を作成していますか。 □ はい　□ いいえ
	26			運用・管理対象、運用・管理方法、運用・管理体制等を明確にしていますか。 □ はい　□ いいえ （はいを選択した場合） 作成している運用・管理方法に当てはまるもの全てにチェックしてください。 □ コンピュータの起動・停止の手順 □ バックアップ手順 □ 媒体の取扱い手順 □ 情報セキュリティインシデントへの対応・報告手順 □ ログの記録と管理手順 □ パフォーマンス監視・評価手順 □ システム監査ツールの不正使用の防止手順 □ その他（　　）
	27			管理責任者は、運用・管理報告についてレビューを実施し、必要であれば実施基準・手順等の評価・見直しを行っていますか。 □ はい　□ いいえ
17	1	第18条 アプリケーション、プラットフォーム、サーバ・ストレージの運用管理	1 受注者は、クラウドサービスを利用者に提供する時間帯を定め、この時間帯におけるクラウドサービスの稼働率及びアプリケーション、プラットフォーム、サーバ・ストレージの定期保守時間を規定し、発注者に報告しなければならない。	☆ クラウドサービスを利用者に提供する時間帯を定め、この時間帯におけるクラウドサービスの稼働率及びアプリケーション、プラットフォーム、サーバ・ストレージの定期保守時間を規定し、発注者に報告することができますか。 □ はい　□ いいえ
	2			クラウドサービスを利用者に提供する時間帯おけるクラウドサービスの稼働率及びアプリケーション、プラットフォーム、サーバ・ストレージの定期保守時間を規定していますか。 □ はい　□ いいえ
	3		2 受注者は、クラウドサービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージに対し、利用者の利用状況の予測に基づいて設計した容量・能力等の要求事項を記録した文書を作成し、保存すること。	☆ クラウドサービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージに対し、利用者の利用状況の予測に基づいて設計した容量・能力等の要求事項を記録した文書を作成し、保存していますか。 □ はい　□ いいえ
	4			要求されたサービス性能を満たすことを確実にするために、アプリケーション、プラットフォーム、サーバ・ストレージの利用を監視・調整していますか。 □ はい　□ いいえ
	5			定期的にアプリケーション、プラットフォーム、サーバ・ストレージの利用状況を監視していますか。 □ はい　□ いいえ
	6		3 受注者は、利用者の利用状況、例外処理及び情報セキュリティ事象の記録（ログ等）を取得し、記録（ログ等）の保存期間を明示しなければならない。	☆ 利用者の利用状況、例外処理及び情報セキュリティ事象の記録（ログ等）を取得し、記録（ログ等）の保存期間を明示していますか。 □ はい　□ いいえ
	7			利用者の利用状況、例外処理及び情報セキュリティ事象の記録として何を取得するか、取得した記録の保管期間、取得した記録の保管方法、取得した記録のチェック（監査等）方法等を明確にしていますか。 □ はい　□ いいえ （はいを選択した場合） 取得している項目全てにチェックしてください。 □ 利用者ID

				□ 端末装置のID 又は所在地 □ 情報システムへのアクセスの成功及び失敗した試みの記録 □ データ及び他の情報資産へのアクセスの成功及び失敗した試みの記録 □ 情報システム構成の変更 □ 特権の利用 □ 情報システムユーティリティ及びアプリケーションの利用 □ アクセスされたファイル及びアクセスの種類 □ ネットワークアドレス及びプロトコル □ アクセス制御システムが発した警報 □ セキュリティ関連システム(例:ウイルス対策システム等)の作動及び停止
	8			システム障害等によるログの欠損をできる限り少なくするために、スタンバイ機等を用いてログサーバの運転を迅速に再開できる状態にしていますか。 □ はい □ いいえ
	9		4 受注者はクラウドサービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージについて定期的にぜい弱性診断を行い、その結果に基づいて対策を行わなければならない。	クラウドサービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージについて定期的にぜい弱性診断を行い、その結果に基づいて対策を行っていますか。 □ はい □ いいえ
	10			ぜい弱性の診断対象(アプリケーション等)、診断方法(ポートスキャンツールやぜい弱性診断ツールの使用等)、診断時期等の計画を明確にしていますか。 □ はい □ いいえ 診断によりぜい弱性に対する対策を実施した場合は、対策の実施についての記録を残していますか。 □ はい □ いいえ
	11			クラウドサービスの提供に用いるアプリケーションについては、開発段階からぜい弱性診断を行うこと等により、導入前にあらかじめぜい弱性対策を実施していますか。 □ はい □ いいえ
18	1	第19条アプリケーション、プラットフォーム、サーバ・ストレージの情報セキュリティ対策	1 受注者はクラウドサービスの提供に用いるプラットフォーム、サーバ・ストレージ(データ・プログラム、電子メール、データベース等)についてウイルス等に対する対策を講じなければならない。	☆ クラウドサービスの提供に用いるプラットフォーム、サーバ・ストレージ(データ・プログラム、電子メール、データベース等)についてウイルス等に対する対策を講じていますか。 □ はい □ いいえ (はいを選択した場合) 対策している項目全てにチェックしてください。 □ 利用者によるサーバ・ストレージ上のデータへのアクセスに対して、ウイルス対策ソフトによるリアルタイムスキャン、情報システムの完全スキャン等による情報セキュリティ対策を行っている □ ウイルス対策ソフトについては、常に最新のパターンファイルを適用している □ ソフトウェアに対する情報セキュリティ対策として、ソフトウェアの構成管理(ソフトウェアのバージョンが正しいこと、意図しないソフトウェアが存在しないことの確認等)を行っている □ 提供するクラウドサービスの一環として、利用者によるダウンロードやHTTP/HTTPS 等を利用したクラウド間転送を許可するファイルについては、ウイルス等の不正なコードが含まれていないことを十分に確認してから提供している
	2		2 受注者は、データベースに格納されたデータの暗号化を行わなければならない。	☆ インターネットからアクセスし得る領域に保存する個人情報、機密情報等のデータについては、暗号化等の対策を行っていますか。 □ はい □ いいえ (はいを選択した場合) 個人情報や機密情報等のデータ保護について対策している項目全てにチェックしてください。 □ 暗号化している □ その他( ) (暗号化している場合) 暗号化を実施する上で対策している項目全てにチェックしてください。 □ 暗号化・復号に使用する鍵については、改変、破壊、紛失から保護するために厳密に管理している

				□ 使用する暗号アルゴリズムは、電子政府推奨暗号リストに掲載されているアルゴリズムのように、その強度について評価、監視している
19	1 2	第20条 サービス データの 保護	1 受注者は、利用者のサービスデータ、アプリケーションやサーバ・ストレージ等の管理情報及びシステム構成情報の定期的なバックアップを実施しなければならない。	☆ 利用者のサービスデータ、アプリケーションやサーバ・ストレージ等の管理情報及びシステム構成情報の定期的なバックアップを実施していますか。 □ はい　□ いいえ 業務要件、セキュリティ要件等を考慮して、バックアップ方法（フルバックアップ、差分バックアップ等）、バックアップ対象（利用者のサービスデータ、アプリケーションやサーバ・ストレージ等の管理情報及びシステム構成情報等）、バックアップの世代管理方法、バックアップの実施インターバル、バックアップのリストア方法等を明確に定めていますか。 □ はい　□ いいえ （はいを選択した場合） バックアップ方法について取得しているものを全てチェックしてください。 □ フルバックアップ □ 差分バックアップ バックアップ対象に含んでいる者を全てチェックしてください。 □ 利用者のサービスデータ □ アプリケーションやサーバ・ストレージ等の管理情報 □ システム構成情報
	3		2 受注者は、バックアップされた情報が正常に記録され、正しく読み出すことができるかどうかについて定期的に確認しなければならない。	バックアップされた情報が正常に記録され、正しく読み出すことができるかどうかについて定期的に確認していますか。 □ はい　□ いいえ
	4			日常の定期確認においては、ファイルをリストアし、ファイルサイズを確認する等の確認を行っていますか。 □ はい　□ いいえ
	5			定期的に復旧訓練を計画・実施し、結果のレビューを行い、必要に応じて方法の見直しを行っていますか。 □ はい　□ いいえ
20	1	第21条 不正アク セスの防 止	1 受注者は、ネットワーク構成図を作成しなければならない（ネットワークをアウトソーシングする場合を除く）。また、アクセス制御方針を策定し、これに基づいて、アクセス制御を許可又は無効とするための正式な手順を策定し、受注者に提示しなければならない。	☆ ネットワーク構成図を作成していますか。（ネットワークをアウトソーシングする場合を除く） □ はい　□ いいえ（□ 作成していない　□ ネットワークをアウトソーシングしている）
	2			☆ アクセス制御方針を策定し、これに基づいて、アクセス制御を許可又は無効とするための正式な手順を策定していますか。 □ はい　□ いいえ （はいを選択した場合） アクセス制御に当たり実施しているものを全てチェックしてください。 □ 利用者、情報システム等の管理者、連携クラウド事業者等アクセスの主体ごとに、アクセス制御に適合する業務上の要求を明確に規定している □ 前項で示した要求に基づいてアクセス制御方針を確立し、文書化し、レビューしている □ アクセス制御には、論理的な方法と物理的な方法があり、この両面を併せて考慮されている
	3		2 受注者は、情報システム管理者及びネットワーク管理者の権限の割当及び使用を制限しなければならない。	☆ 情報システム管理者及びネットワーク管理者の権限の割当及び使用を制限していますか。 □ はい　□ いいえ （はいを選択した場合） 権限の管理に当たり実施しているものを全てチェックしてください。 □ 情報システム管理者及びネットワーク管理者に情報システム又はネットワークへのアクセス権を与える場合は、正式な認可プロセスによってそのアクセス権の割当を管理している □ 情報システム管理者及びネットワーク管理者に情報システム又はネットワークへのアクセス特権を与える必要がある場合は、必要最小限の者に限定し、かつ厳格にその割当を管理している □ 管理者権限の割当一覧を作成して管理している □ 管理者権限の割当又は使用制限を行うための実施マニュアルを整備している

	4 5 6 7 8 9		3 受注者は、利用者及び管理者(情報システム管理者、ネットワーク管理者等)等のアクセスを管理するための適切な認証方法、特定の場所及び装置からの接続を認証する方法等により、アクセス制御となりすまし対策を行わなければならない。また、運用管理規定を作成すること。ID・パスワードを用いる場合は、その運用管理方法と、パスワードの有効期限を規定に含めなければならない。	☆ 利用者及び管理者(情報システム管理者、ネットワーク管理者等)等のアクセスを管理するための適切な認証方法、特定の場所及び装置からの接続を認証する方法等により、アクセス制御となりすまし対策を行っていますか。 □ はい □ いいえ 情報システム管理者、ネットワーク管理者、連携クラウド事業者等が運用・管理・保守等の目的で遠隔から情報システム又はネットワークにアクセスする必要がある場合は、情報セキュリティポリシーに従って、適切な認証方法を利用し、なりすまし対策を行っていますか。 □ はい □ いいえ ☆ アクセス制御となりすまし対策についての運用管理規定を作成していますか。 □ はい □ いいえ ☆ ID・パスワードを用いる場合は、その運用管理方法と、パスワードの有効期限を規定に含めていますか。 □ はい □ いいえ ID・パスワード等の認証情報は、文字列ではなくハッシュ値を保存していますか。 □ はい □ いいえ 高い機密性、完全性が求められるサービスでは、記憶情報・所有情報・生体情報を組み合わせた多要素(二要素)認証を採用していますか。 □ はい □ いいえ
	10 11 12		4 受注者は、外部及び内部からの不正アクセスを防止する措置(ファイアウォール、リバースプロキシの導入等)を講じなければならない。	☆ 外部及び内部からの不正アクセスを防止する措置を講じていますか。 □ はい □ いいえ (はいを選択した場合) 講じている不正アクセス防止用の措置について当てはまるものすべてにチェックしてください。 □ ファイアウォール □ リバースプロキシ □ その他 ( ) ファイアウォールを導入する際には、情報セキュリティポリシーに基づいたソフトウェアやハードウェアを選定し、構築していますか。 □ はい □ いいえ ファイアウォールは、情報セキュリティポリシーに従って運用されていますか。 □ はい □ いいえ
	13		5 受注者は、不正な通過パケットを自動的に発見、もしくは遮断する措置(IDS/IPS の導入等)を講じなければならない。	不正な通過パケットを自動的に発見、もしくは遮断する措置を講じていますか。 □ はい □ いいえ (はいを選択した場合) 講じている不正パケットの検知及び遮断する措置について当てはまるものすべてにチェックしてください。 □ IDS(Intrusion Detection System) □ IPS(Intrusion Prevention System) □ その他 ( ) (IDS/IPS 等を導入している場合) IDS/IPS等を導入している場合に当てはまるものについて当てはまるものすべてにチェックしてください。 □ IDS/IPS 等を導入する際には、業務要件や業務環境に適合したソフトウェアやハードウェアを選定し、構築している □ IDS/IPS 等は、業務要件や業務環境に合わせた設定により運用している
21	1	第22条 建物の災害対策	受注者は、クラウドサービスの提供に用いるサーバ・スト	クラウドサービスの提供に用いるサーバ・ストレージ、情報セキュリティ対策機器等の情報システムが設置されている建物(情報処理施設)については、地震・水害に対する対策を行っていますか。

			レージ、情報セキュリティ対策機器等の情報システムが設置されている建物（情報処理施設）については、地震・水害に対する対策が行わなければならない。		□ はい □ いいえ
	2				情報処理施設は、地震や水害が発生しやすい地域の立地ではありませんか。 □ はい □ いいえ
	3				情報処理施設には、激しい地震の振動にも耐えられるように、免震構造（建物の振動を緩和する仕組み）又は耐震構造（強い振動にも耐えうる頑強な構造）を採用した建物を利用していますか。 □ はい □ いいえ
	4				サーバルームは建物の2階以上に設置することが望ましい。また、屋上からの漏水の危険がある最上階や、水使用設備が隣室又は直上階にある場所ではありませんか。 □ はい □ いいえ
22	1	第23条 電源・空調の維持と災害対策	1 受注者は、クラウドサービスの提供に用いるサーバ・ストレージ、情報セキュリティ対策機器等の情報システムを設置する場所には、停電や電力障害が生じた場合に電源を確保するための対策を講じなければならない。	☆	クラウドサービスの提供に用いるサーバ・ストレージ、情報セキュリティ対策機器等の情報システムを設置する場所には、停電や電力障害が生じた場合に電源を確保するための対策を講じていますか。 □ はい □ いいえ
	2				非常用無停電電源（UPS 等）は、非常用発電機から電力の供給を受けられますか。 □ はい □ いいえ
	3				非常用無停電電源と非常用発電機が非常時に正しく機能するよう、定期的に点検していますか。 □ はい □ いいえ
	4		2 受注者は、クラウドサービスの提供に用いるサーバ・ストレージ、情報セキュリティ対策機器等の情報システムを設置する場所では、設置されている機器等による発熱を抑えるのに十分な容量の空調を提供しなければならない。		クラウドサービスの提供に用いるサーバ・ストレージ、情報セキュリティ対策機器等の情報システムを設置する場所では、設置されている機器等による発熱を抑えるのに十分な容量の空調を提供していますか。 □ はい □ いいえ
	5				サーバルームには、サーバルーム専用の空調設備を設置していますか。 □ はい □ いいえ
	6				空調能力は、情報処理施設の構造、サーバルームの規模と発熱量、設置された機器の使用目的と使用条件等を考慮した設計となっていますか。 □ はい □ いいえ
23	1	第24条 火災、逃雷、静電気から情報システムを防護するための対策	1 受注者は、サーバルームに設置されているクラウドサービスの提供に用いるサーバ・ストレージ、情報セキュリティ対策機器等の情報システムについて、放水等の消火設備の使用に伴う汚損に対する対策を講じること。		サーバルームに設置されているクラウドサービスの提供に用いるサーバ・ストレージ、情報セキュリティ対策機器等の情報システムについて、放水等の消火設備の使用に伴う汚損に対する対策を講じていますか。 □ はい □ いいえ
	2		2 受注者は、クラウドサービスの提供に用いるサーバ・ストレージ、情報セキュリティ対策機器等の情報システムを設置するサーバルームには、火災検知・通報システム及び消火設備を備えなければならない。	☆	クラウドサービスの提供に用いるサーバ・ストレージ、情報セキュリティ対策機器等の情報システムを設置するサーバルームには、火災検知・通報システム及び消火設備を備えていますか。 □ はい □ いいえ
	3				火災感知器は、熱感知器、煙感知器、炎感知器に大別されるが、設備メーカーと協議の上でこれらの最適な組合せを検討して設置していますか。 □ はい □ いいえ
	4				火災感知器の取り付け場所、取り付け個数等は感知器の種類により決めていますか。 □ はい □ いいえ

	5			火災の原因になりやすい通信・電力ケーブル類が多量にあるフリーアクセス床下にも火災検知器を設置していますか。 □ はい　□ いいえ
	6		3 受注者は、情報処理施設に雷が直撃した場合を想定した対策を講じなければならない。	☆ 情報処理施設に雷が直撃した場合を想定した対策を講じていますか。 □ はい　□ いいえ
	7			情報処理施設には避雷針を設置していますか。 □ はい　□ いいえ
	8		4 受注者は、情報処理施設付近に誘導雷が発生した場合を想定した対策を講じなければならない。	情報処理施設付近に誘導雷が発生した場合を想定した対策を講じていますか。 □ はい　□ いいえ
	9			雷サージ（落雷により誘起された大きな誘導電圧）対策として、電源設備の電源引込口にできるだけ近い場所に、避雷器、電源保護用保安器、CVCF等を設置していますか。 □ はい　□ いいえ
	10			情報処理施設は等電位化（全ての接地の一本化）を行っていますか。 □ はい　□ いいえ
	11		5 受注者は、クラウドサービスの提供に用いるサーバ・ストレージ、情報セキュリティ対策機器等の情報システムについて、作業に伴う静電気対策を講じなければならない。	クラウドサービスの提供に用いるサーバ・ストレージ、情報セキュリティ対策機器等の情報システムについて、作業に伴う静電気対策を講じていますか。 □ はい　□ いいえ
	12			静電気の発生を防止するため、サーバルームの床材には静電気を除去する帯電防止フリーアクセスフロア、アースシート等を使用していますか。（導電材を添加した塩化ビニルタイル、高圧ラミネート、帯電防止用カーペット等の使用も可とする） □ はい　□ いいえ
	13			サーバルームの湿度を 40～60%程度に保っていますか。 □ はい　□ いいえ
24	1	第25条 建物の情報セキュリティ対策	1 受注者は、重要な物理的セキュリティ境界（カード制御による出入口、有人の受付等）に対し、個人認証システムを用いて、従業員等及び出入りを許可された外部組織等に対する入退室記録を作成し、適切な期間保存しなければならない。	☆ 重要な物理的セキュリティ境界（カード制御による出入口、有人の受付等）に対し、個人認証システムを用いて、従業員等及び出入りを許可された外部組織等に対する入退室記録を作成し、適切な期間保存していますか。 □ はい　□ いいえ
	2			入退室を確実に記録するため、常時利用する出入口は一ヶ所としていますか。 □ はい　□ いいえ
	3			個人の資格確認による入退室管理を行っていますか。 □ はい　□ いいえ
	4			個人認証システムは、入退室者の氏名及び入退室時刻を記録していますか。 □ はい　□ いいえ
	5		2 受注者は、重要な物理的セキュリティ境界に対して監視カメラを設置し、その稼働時間と監視範囲を定めて監視を行うこと。また、監視カメラの映像をあらかじめ定められた期間保存しなければならない。	重要な物理的セキュリティ境界に対して監視カメラを設置し、その稼働時間と監視範囲を定めて監視を行っていますか。 □ はい　□ いいえ （はいを選択した場合） 監視カメラについて当てはまるものを全てチェックしてください。 □ 監視カメラの映像を定められた期間保存している □ 監視性を高めるため、死角を作らないように監視カメラを設置している □ 監視カメラは、カラー撮影であり、デジタル記録が可能である □ 監視カメラは用途に応じて十分な解像度を持っている

				□ 監視カメラは、撮影日時が画像内に時分秒まで記録可能である □ 非常時に防犯機関等への通報ができる非常通報装置を併設している □ 重要な物理的セキュリティ境界においては、個人認証システムと併設している
	6		3 受注者は、重要な物理的セキュリティ境界からの入退室等を管理するための手順書を作成しなければならない。	☆ 入退室管理のための手順は作成していますか。 □ はい　□ いいえ
	7		4 受注者は、重要な物理的セキュリティ境界の出入口に破壊対策ドアを設置しなければならない。	重要な物理的セキュリティ境界の出入口に破壊対策ドアを設置していますか。 □ はい　□ いいえ
	8			出入口の扉は十分な強度を有する破壊対策・防火扉を使用し、不法侵入、危険物の投込み、延焼を防止できますか。 □ はい　□ いいえ
	9		5 受注者は、重要な物理的セキュリティ境界に警備員を常駐させなければならない。	重要な物理的セキュリティ境界に警備員を常駐していますか。 □ はい　□ いいえ
	10			警備員の常駐時間を定めていますか。 □ はい　□ いいえ （はいを選択した場合） 常駐時間に当てはまる項目にチェックをしてください。 □ 365 日24 時間 □ その他　（具体的に:　　）
	11		6 受注者は、サーバルームやラックの鍵管理を行わなければならない。	☆ サーバルームやラックの鍵管理を行っていますか。 □ はい　□ いいえ
	12			ラックやサーバルームの出入口の鍵は定められた場所に保管し、管理は特定者が行うことができますか。 □ はい　□ いいえ
	13			ラックやサーバルームの出入口の鍵については、受渡し時刻と氏名を記録していますか。 □ はい　□ いいえ
25	1	第26条 機密性・完全性を保持するための対策	1 受注者は、電子データの原本性確保を行わなければならない。	電子データの原本性（真正性）を確保していますか。 □ はい　□ いいえ （はいを選択した場合） 確保するための手段として実施しているものに全てチェックしてください。 □ 時刻認証による方法 □ 署名（ハッシュ値によるもの等）による方法 □ 印刷データ電子化・管理による方法 □ その他（　　）

	2 3 4 5 6		2 受注者は、個人情報は関連する法令に基づいて適切に取り扱わなければならない。	☆ 個人情報は関連する法令に基づいて適切に取り扱っていますか。 □ はい　□ いいえ 個人情報を収集する際には、利用目的を明示し、各個人の同意を得た上で収集していますか。 □ はい　□ いいえ 個人情報の漏洩、滅失、棄損を防止するための措置(例:従業員や協力会社要員に対する必要かつ適切な監督等)を講じていますか。 □ はい　□ いいえ 事前の本人同意無しに個人情報を第三者に提供しませんか。 □ はい　□ いいえ 本人から利用目的の通知、データ開示、データ訂正・追加・削除、データの利用停止等の求めがあった場合は、これに応じることができますか。 □ はい　□ いいえ
26	1 2 3 4 5 6 7 8	第27条 クラウド事業者の運用管理端末における情報セキュリティ対策	受注者は、運用管理端末に、許可されていないプログラム等のインストールを行わせてはならない。また、従業員等が用いる運用管理端末の全てのファイルのウイルスチェックを行わなければならない。また、技術的ぜい弱性に関する情報(OS、その他ソフトウェアのパッチ発行情報等)を定期的に収集し、随時パッチによる更新を行わなければならない。	☆ 運用管理端末に、許可されていないプログラム等のインストールを行っていませんか。 □ はい(行っていない)　□ いいえ(行っている) 運用管理端末の管理者権限の付与を制限していますか。 □ はい　□ いいえ 運用管理端末において、従業員等が行うログイン・ログアウト、特定プログラムの実行、データベース接続などの重要操作等について、操作ログを取得し、保存していますか。 □ はい　□ いいえ 許可されていないプログラム等を運用管理端末にインストールすることを禁止し、従業員等に周知徹底し、違反した場合には罰則を課していますか。 □ はい　□ いいえ ☆ 従業員等が用いる運用管理端末の全てのファイルのウイルスチェックを行っていますか。 □ はい　□ いいえ 運用管理端末のウイルス対策ソフトについては、常に最新のパターンファイルを適用していますか。 □ はい　□ いいえ ☆ 技術的ぜい弱性に関する情報(OS、その他ソフトウェアのパッチ発行情報等)を定期的に収集し、随時パッチによる更新を行っていますか。 □ はい　□ いいえ パッチは、運用管理機能への影響が無いと確認した上で適用していますか。 □ はい　□ いいえ

上記記入のとおり一切相違ありません

住所

商号又は名称

代表者氏名

㊞