

奥州市ガバメントクラウド接続サービス調達仕様書

令和7年11月28日

奥州市総務部行革デジタル戦略課

目次

第1	総則	1
1	背景・目的	1
(1)	背景	1
(2)	目的	1
2	スコープ概要	1
3	契約形式等	1
(1)	契約期間	1
(2)	契約形式・料金の支払	1
(3)	再委託に当たっての条件	2
(4)	契約不適合責任	2
4	準拠法令等	2
(1)	準拠法令	2
(2)	言語、通貨、計量単位及び期間	2
5	作業上の遵守事項	2
(1)	関係法令等の遵守	2
(2)	作業等に当たっての注意事項	3
(3)	情報セキュリティの確保	3
(4)	作業場所と利用環境	3
6	照会先	3
第2	業務概要	4
1	業務の範囲（スコープ）	4
(1)	全体概要	4
(2)	プロジェクト関係者	4
(3)	業務内容	5
(4)	対象外業務	5
2	接続システム	5
3	スケジュール	6
4	ガバメントクラウド利用方針	6
(1)	利用方式	6
(2)	利用 CSP	6
(3)	利用アカウント	6
(4)	ロケーション	6
第3	設計構築要件	7
1	ガバメントクラウド接続	7
(1)	拠点接続サービス構築	7
(2)	ルーター構築	7
(3)	クラウド接続サービス構築	8
(4)	接続確認	9

2	ガバメントクラウド利用支援.....	9
(1)	利用申請支援.....	9
(2)	CEP ライセンス管理	9
3	運用管理機能設計・構築.....	9
(1)	ユーザー設計.....	9
(2)	テンプレート適用・設計・構築.....	9
(3)	ネットワーク設計・構築.....	9
(4)	テスト.....	10
(5)	継続的な改善に必要な項目の設計・構築.....	10
(6)	一元的な運用管理に関する項目の設計・構築.....	10
(7)	信頼性/可用性設計・構築.....	11
(8)	拡張性設計・構築.....	11
(9)	性能設計・構築.....	11
(10)	運用管理設計.....	11
第4	運用管理補助要件.....	12
1	通信回線・機器保守.....	12
(1)	拠点接続サービス保守.....	12
(2)	クラウド接続サービス保守.....	12
(3)	ルーター保守.....	12
2	運用管理機能運用・保守.....	12
(1)	ユーザー管理.....	12
(2)	保守・メンテナンス.....	12
(3)	監視.....	13
(4)	障害対応.....	13
(5)	情報セキュリティ管理.....	13
(6)	構成管理.....	13
(7)	技術支援.....	13
(8)	ドキュメント管理.....	14
(9)	性能・キャパシティ・コスト管理.....	14
(10)	バックアップ・リストア管理.....	14
(11)	継続的な改善.....	14
3	連絡体制.....	14
第5	業務実施体制.....	15
1	プロジェクト管理.....	15
2	実施体制.....	15
3	会議体.....	15
第6	成果物.....	17
1	納入と承認.....	17
2	ドキュメントの成果物.....	17
(1)	ドキュメントの品質.....	17

(2) ドキュメントの形式.....	17
3 ドキュメントの著作権.....	17
4 納入成果物.....	17
第 7 その他特記事項.....	19
1 引継ぎ対応.....	19
2 仕様書の解釈.....	19
3 ガバメントクラウド関連資料.....	19

第1 総則

1 背景・目的

(1) 背景

令和3年9月1日に「地方公共団体情報システムの標準化に関する法律（令和3年法律第40号）」が施行され、地方公共団体の基幹業務システムについて、全ての地方公共団体が、ガバメントクラウド等に構築された標準化基準に適合した基幹業務システム（以下「標準準拠システム」という。）へ移行することとなった。また、「地方公共団体情報システムのガバメントクラウドの利用について【第3.0版】」（以下「ガバメントクラウドの利用について」という。）において、地方公共団体は事業者と委託契約を締結し、ガバメントクラウド利用権限の一部又は全部を当該事業者（ガバメントクラウド運用管理補助者）に付与し、クラウドサービス等の運用管理の補助を委託することができるとされている。

こうした中、当市においても「地方公共団体情報システム標準化基本方針（令和6年12月24日閣議決定）」、「ガバメントクラウドの利用について」及び「ガバメントクラウド利用権付与兼債務引受契約」に基づいたガバメントクラウド環境及び通信回線の設計構築、運用管理等を実施するため、本件業務を委託する。

(2) 目的

当市がガバメントクラウドを利用するに当たり、「ガバメントクラウドの利用について」に基づいたガバメントクラウド環境及び通信回線の設計構築、運用管理等を行い、各標準準拠システムが移行するための環境を整えるとともに、移行後の安定稼働を確保し、継続的な改善を実施することを目的とする。

2 スcope概要

この調達の名称を「奥州市ガバメントクラウド接続サービス調達」とする。

ガバメントクラウド環境及び通信回線の設計構築、運用管理等を調達範囲とし、以下の内容とする。

- ① ガバメントクラウド接続サービスの導入及び提供
- ② ガバメントクラウド環境の設計構築及び附帯業務としてのプロジェクト管理
- ③ ガバメントクラウド環境の運用管理（回線運用管理を含む。以下同じ。）
- ④ 機器の据付、搬入、工事等を含め、その他一切の附帯業務

3 契約形式等

(1) 契約期間

契約締結日から令和13年8月31日までとする。各工程における作業期間については、以下のとおりとする。

- ① 設計構築： 契約締結日から令和8年8月31日まで
- ② 運用管理： 令和8年9月1日から令和13年8月31日まで（60箇月）

(2) 契約形式・料金の支払

契約の形式については、以下のとおりとする。

- ① 設計構築期間に係る契約は業務委託契約とし、業務完了後に一括で支払を行うものとする。
 - ② 運用管理期間に係る契約は、地方自治法第234条の3に基づく長期継続契約による業務委託契約（60箇月）とし、月額により、各業務完了月の翌月に支払を行うものとする。通信回線の使用料といった業務の単純な請負に係らない内容を含むが、電気通信役務として一体として提供されるものとし、金銭の支払も一元化して請求書を一枚とすること。
- (3) 再委託に当たっての条件
- この調達の全部を第三者に委任し、又は請け負わせること（以下「再委託」という。）は、原則として禁止する。ただし、調達の一部について、以下の事項をあらかじめ書面により示したうえで、当市の承認を得た場合は、この限りではない。なお、再委託業務の内容を変更する場合も同様とする。
- ① 再委託する事業者の商号又は名称、住所
 - ② 再委託する理由
 - ③ 再委託して処理する業務の内容
 - ④ 再委託事業者が取り扱う情報
 - ⑤ 再委託事業者における安全性及び信頼性を確保する対策並びに再委託事業者に対する管理及び監督の方法
 - ⑥ その他当市が適否を判断するために必要な事項
- (4) 契約不適合責任
- システム稼働から1年以内に、契約の内容に適合せず、正常な運用ができないときは、受注者の負担により速やかに修正を行うものとする。
- 品質保証の責任は受注者にあるため、事務手続上の承認がなされた後であっても、品質上の問題が発覚したときには、契約不適合責任の概念が適用されるものである。

4 準拠法令等

(1) 準拠法令

この調達に係る準拠法令は、日本国の法令とする。

(2) 言語、通貨、計量単位及び期間

この調達で用いる言語、通貨、計量単位及び期間については、以下のとおりとする。

- ① 言語は、日本語とする。
- ② 通貨は、日本円とする。
- ③ 計量単位は、原則として、計量法（平成4年法律第51号）に定めるものとする。
- ④ 期間の定めについては、原則として、民法（明治29年法律第89号）及び商法（明治32年法律第48号）の定めるところによる。基準時刻は日本標準時（JST）とするが、サービスの特性により必要な場合は、協定世界時（UTC）とする。

5 作業上の遵守事項

(1) 関係法令等の遵守

以下の点をはじめとして、関係法令を遵守すること。

- ① 労働基準法、労働安全衛生法その他労働関係法令に従い、違反や事故のないよう十分注意すること。違反や事故が発生しその原因が受注者の責に帰す場合は、受注者の責任において処理すること。
- ② 本業務の範囲に使用する機器の特許権、実用新案権等の工業所有権及びプログラム等の著作権その他の知的所有権、また、使用許諾契約等については、全て受注者の責任において処理すること。
- (2) 作業等に当たっての注意事項
当市での作業等に当たっては、以下の点に留意すること。
 - ① 当市及び作業場所管理者の指示に従うこと。
 - ② 当市の平常業務に支障がないよう留意すること。
 - ③ 既存の設備等の保障に十分留意し、万一破損等が生じた場合は受注者の責任において処理すること。
- (3) 情報セキュリティの確保
以下の点をはじめとして、情報セキュリティには十分留意することとし、別紙「情報セキュリティに関する特記事項」を遵守すること。
 - ① この仕様書の閲覧時、契約時及び契約履行中に知り得た秘密は適切に扱い、漏えいのないようにすること。
 - ② サプライチェーンリスクを意識し、当市に対しては納入物件についての最終的かつ全面的な責任を負うこと。
 - ③ 情報セキュリティ体制を証するものとして、契約期間において、安全かつ安定的な運用が将来にわたり確保できることを具体的に提示できること。
- (4) 作業場所と利用環境
インターネット経由で管理インターフェースに接続する場合は、デジタル庁が示す「ガバメントクラウド利用における推奨構成」等に記載されているものと同様の方式で行い、また、同様の情報セキュリティ対策を行うこと。
なお、個人情報を含む業務情報にアクセスする必要がある場合は、当市の庁内ネットワーク経由で行うこと。

6 照会先

本仕様書に関する照会先は、以下のとおりである。

- ① 所在地 : 〒023-8501 岩手県奥州市水沢大手町一丁目1番地
- ② 担当部署 : 奥州市総務部行革デジタル戦略課
- ③ 担当者 : デジタル戦略係長 菊池 知之
- ④ 電話 : 0197-34-2194 (時間外の場合、内線1436)
- ⑤ E-Mail : digital@city.oshu.iwate.jp

第2 業務概要

1 業務の範囲（スコープ）

(1) 全体概要

当市が採用する Cloud Service Provider（以下「CSP」という。）は「Amazon Web Services。以下「AWS」という。」とし、本業務におけるガバメントクラウド運用管理補助者の作業範囲は、下図のとおりとする。一般的なガバメントクラウド運用管理補助者のほか、回線運用管理補助者及び通信回線事業者の責任範囲をその中に含む。

なお、この作業範囲図は、作業の対象範囲を概念的に示したものであり、構築設計図ではない。

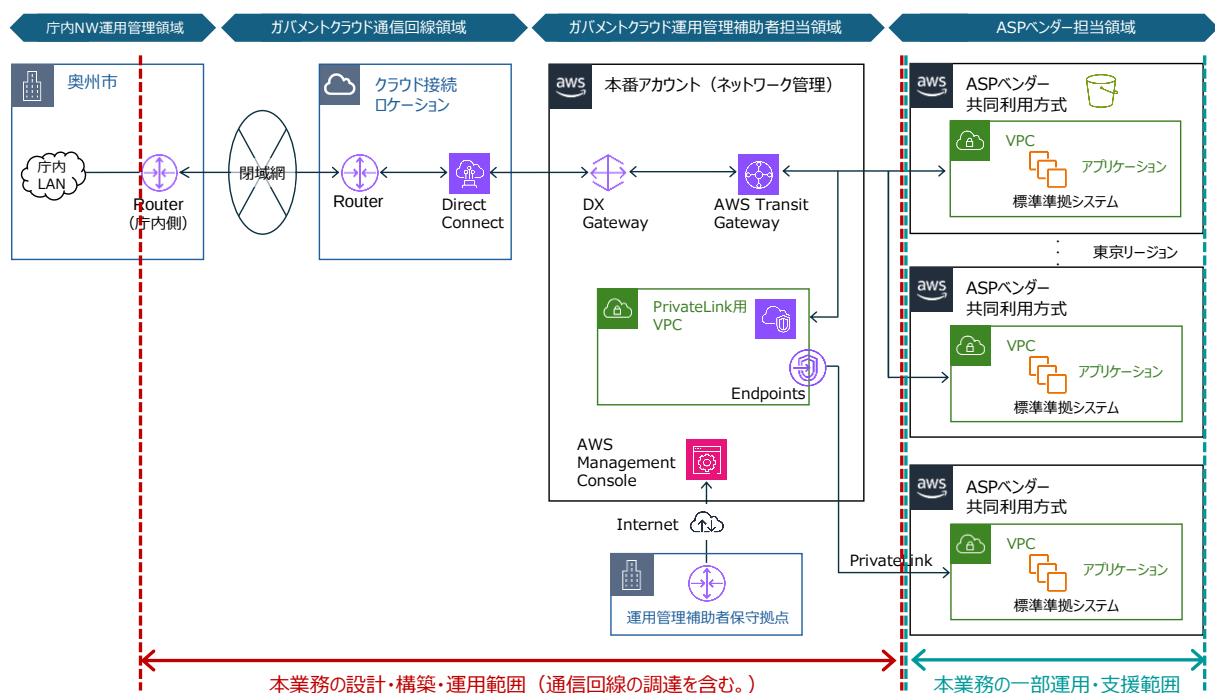


図1. 本業務の作業範囲

(2) プロジェクト関係者

本業務におけるプロジェクト関係者は、下表のとおりとする。

表1. プロジェクト関係者

組織・事業者	主な役割等
市	・受注者と市内ネットワーク及びASPベンダーとの連絡及び調整の実施 ・デジタル庁へのガバメントクラウド利用権限付与等の申請
ガバメントクラウド運用管理補助者（回線運用管理補助者及び通信回線事業者）	（ガバメントクラウド環境への接続に用いる通信回線等の提供） ・市内ネットワークとガバメントクラウド環境とを接続する通信回線（拠点接続サービス・クラウド接続サービス）の提供 ・市内ネットワークと回線領域を接続する機器の提供、設置及び設定（ガバメントクラウド環境の運用管理・ネットワークの運用管理） ・クラウドインフラの設計、権限管理、構築、運用、保守及び継続的な改善

	・ガバメントクラウド環境内ネットワーク構成の設計、設定及び管理のための環境構築、運用及び保守 ・CSPが複数の場合のネットワーク検討支援
ASPベンダー	・標準準拠システムの構築、提供、運用保守等 ・標準準拠システムの修正、改良等 ・標準準拠システム運用開始時の検証
デジタル庁	・CSPとの契約及びガバメントクラウドの利用に関する権限付与
CSP	・ガバメントクラウドとしてクラウドサービス環境を提供

(3) 業務内容

本業務の主な業務内容は、以下のとおりである。

- ① ガバメントクラウド環境に接続するために必要となる通信回線の敷設、機器の設置、設定等を行うこと。
- ② ガバメントクラウド環境に構築したASP領域と接続するためのネットワーク設計・構築を行うこと。また、ASP領域との疎通テスト、システム動作確認等について、本業務で構築する本番アカウント（ネットワーク管理）の個別領域が関与する場合に協力すること。
- ③ 通信回線、及び本番アカウント（ネットワーク管理）の個別領域におけるユーザー管理、保守・メンテナンス、監視、障害対応、一元的な運用管理及び継続的な改善業務等を行うこと。
- ④ ガバメントクラウド環境を利用、運用する際の手続に当たり、技術的助言、補助等の支援を行うこと。
- ⑤ 各ASPベンダー、デジタル庁及びCSPとガバメントクラウド環境構築のために必要な連絡等の支援を行うこと。
- ⑥ その他本業務において構築する環境が継続的に正常かつ良好に稼働するために必要な助言等を行うこと。

(4) 対象外業務

この調達の対象外となる作業については、以下のとおりとする。

- ① 庁内ネットワーク機器の調達及び設定作業
- ② 本番アカウント（ネットワーク管理）外のネットワーク設定作業

2 接続システム

ASP領域において接続する標準準拠システムのASPベンダー、利用方式、VPC数、接続開始時期等は、下表のとおりである。

表2. 接続システム一覧

ASPベンダー	対象業務	利用方式	接続方法	VPC	接続開始時期
富士通Japan	住記、税、就学、年金、後期高齢、介護、印鑑、児扶、児手、子ども・子育て支援、共通機能	共同利用方式/ アカウント分離	Transit Gateway	1	2029年2月
行政システム	選挙人名簿	共同利用方式/	Transit	1	2029年1月

		ネットワーク分離	Gateway		
日立システムズ	障害者福祉	共同利用方式/ ネットワーク分離	Transit Gateway	1	2026年9月
北日本コンピューターサービス	生活保護	共同利用方式/ アカウント分離	Transit Gateway	1	2026年10月
フィデア情報総研	健康管理	共同利用方式/ ネットワーク分離	Transit Gateway	1	2026年9月

3 スケジュール

令和8年9月から、ASPベンダーにおいてガバメントクラウド環境への接続が行えるよう、およそ下表のようなスケジュールとする。ただし、詳細なスケジュールについては、市と受注者との間で協議のうえ、決定すること。

表3. 想定稼働スケジュール

工程	時期
ガバメントクラウド利用申請等	令和8年1月～令和8年2月
通信回線の敷設	令和8年2月～令和8年4月
ルータの設置・庁内ネットワーク機器との接続	令和8年5月
ネットワーク設計	令和8年3月～令和8年5月
ガバメントクラウド環境構築	令和8年5月～8月
テスト	令和8年8月
本稼働（ASPベンダーとの接続開始）	令和8年9月

4 ガバメントクラウド利用方針

(1) 利用方式

ガバメントクラウド利用方式は、単独利用方式とする。

(2) 利用CSP

調達時点におけるガバメントクラウドのCSPは「AWS」を用いる。

ただし、対象業務により、ガバメントクラウドへの接続開始時期が異なることから、時期により他のCSPを採用する可能性があること。

(3) 利用アカウント

運用管理に必要となるガバメントクラウド環境の本番アカウント（ネットワーク管理）の利用権限を付与するものとする。

(4) ロケーション

東京リージョンのみとする。

第3 設計構築要件

1 ガバメントクラウド接続

(1) 拠点接続サービス構築

ア 通信回線要件

提供する通信回線の要件については、以下のとおりとする。

- ① 専用線又は広域イーサネット相当の回線とし、インターネットを経由しない閉域ネットワーク（閉域網）の回線であること。
- ② 回線は冗長化するものとし、主回線は100Mbps以上のギャランティ型（帯域保証又は帯域確保）の回線、従回線は1Gbps以上のベストエフォート型の回線とすること。
- ③ 1Gbpsまでの通信帯域が提供可能なサービスであり、帯域変更ができること。
- ④ 当市が指定する拠点が異なる場所に移転する場合があることを想定し、対応できるネットワーク設計とすること。
- ⑤ 回線終端装置（ONU）のインターフェースは、100BASE-TXから提供すること。
- ⑥ 庁内ネットワークスイッチと回線終端装置（ONU）との接続には、ルーターを設置すること。
- ⑦ ルーティングプロトコルは、BGP及びSTATICが利用できること。
- ⑧ 通信経路は、海外を経由しないこと。

イ 通信回線の敷設

通信回線の敷設については、以下のとおり行うこと。

- ① 当市が指定する拠点へガバメントクラウド環境に接続するための通信回線を敷設すること。
- ② 当市が指定する既設の19インチラックの指定する場所に、回線終端装置（ONU）2式を搭載すること。
- ③ 屋外配線及び屋内配線を行う場合には、事前に許可を得ること。第三者の安全にも十分に配慮し、事故等が発生した場合には速やかに報告するとともに、誠実に対応すること。
- ④ トラブルの未然防止のため、事前に協議のうえ現地調査を行い、通信回線の物理的な引き込み管路を把握すること。
- ⑤ 発生する空箱、梱包材等は全て回収し、正しく廃棄すること。

(2) ルーター構築

ア 機器要件

設置するルーターの機器要件については、以下のとおりとする。

- ① WAN側の接続は、BGP又はSTATICを使用した設計とすること。
- ② LAN側はSTATIC接続とし、VRRP又はHSRPが使用できること。
- ③ 回線終端装置（ONU）とルーターとの接続は、Cat6以上のLANケーブルとし必要数を用意すること。
- ④ 機器はラックマウントに対応すること。
- ⑤ 機器1台につき、100BASE-TXのインターフェースを6ポート以上有すること。
- ⑥ ファームウェアのアップデート等により、必要に応じてセキュリティパッチを適

用できること。

イ ルーター設置

ルーターの設置については、以下のとおり行うこと。

- ① 当市が指定する既設の19インチラックの指定する場所に、ルーター2式をラックマウント金具等で搭載すること。なお、搭載するラックは、回線終端装置（ONU）を搭載するものと同一のものを予定している。
- ② LAN配線を行う場合には、事前に許可を得ること。第三者の安全にも十分に配慮し、事故等が発生した場合には速やかに報告するとともに、誠実に対応すること。
- ③ 庁内ネットワークスイッチからのLANケーブルの配線及び接続については、市側で実施するため、事前に協議調整を行うこと。
- ④ 配線に当たり、結束テープ等で整線し、美観を損ねないこと。ケーブルの使用用途や元先が目視確認できるようラベルを貼付すること。
- ⑤ 設置した機器等は、目視で契約件名や導入事業者等が確認できるよう、シールに印刷して機器等に貼付すること。
- ⑥ 電源は、当市において準備するので接続すること。

ウ ルーター設定

ルーターの設定については、以下のとおり行うこと。

- ① 庁内ネットワークからガバメントクラウド環境に接続できるよう、ルーターを設定すること。
 - ② クラウド側ネットワークへのゲートウェイは、AWS Direct Connect を想定すること。なお、本件の履行期間中に別のCSPを採用する場合には、接続先を追加、変更等すること。
 - ③ 庁内ネットワークとクラウド側ネットワークへのルーティング設定等を行うこと。
 - ④ 庁内ネットワークとの接続は、既設の庁内ネットワークスイッチとVRRP又はHSRPで経路を冗長化するよう設定すること。
 - ⑤ ルーター2式を、敷設した通信回線（主・従回線）にそれぞれ接続したうえで、HA構成などにより冗長構成とすること。
 - ⑥ 冗長構成は、Active-standby構成を基本とし、Active側の機器に障害が発生した場合、又は通信回線、回線終端装置（ONU）及び通信回線のサービス拠点等に障害が発生した場合には、自動的かつ速やかにStandby側のルーターにより従回線を利用し、ガバメントクラウド環境への接続が継続されること。
 - ⑦ 障害が復旧した場合には、再度、Active-standby構成となるようにすること。
 - ⑧ 機器交換等により再設定を行う場合にあっては、設定内容を容易に復元できるようにしておくこと。
 - ⑨ 庁内ネットワーク保守事業者との打合せに参加すること。
- (3) クラウド接続サービス構築

ガバメントクラウド環境の拠点までを接続するクラウド接続サービスの要件については、以下のとおりとする。

- ① ガバメントクラウド環境に閉域接続ができること。
- ② Google Cloud Platform (GCP)、Microsoft Azure、Oracle Cloud Infrastructure

(OCI) 等のAWS以外のCSPにも接続できること。

- ③ マルチクラウドに接続できること。マルチクラウドの場合、CSP間の通信は、クラウド接続サービス網内で折り返し通信できること。
- ④ ガバメントクラウド環境の接続拠点は、東京とすること。
- ⑤ ギャランティ型の回線であること。
- ⑥ 各コネクションの通信帯域は、100Mbpsとすること。
- ⑦ 通信経路は、海外を経由しないこと。
- ⑧ 接続部では、仮想ルーター機能としてBGPにて動的制御の設定ができること。
- ⑨ 1 Gbpsまでの通信帯域が提供可能なサービスであり、帯域変更ができること。

(4) 接続確認

ガバメントクラウド環境への接続確認については、以下のとおり行うこと。

- ① 庁内ネットワークからガバメントクラウド環境までの疎通を確認すること。
- ② ルーターの冗長構成を確認すること。

2 ガバメントクラウド利用支援

(1) 利用申請支援

当市からデジタル庁にガバメントクラウド利用申請を行うに当たり、必要となる情報の提示及び申請資料の作成について支援すること。GCAS (Government Cloud Assistant Service) のアカウント利用申請、CSP環境抽出申請等のほか、GCAS上での実施すべき諸手続に必要な技術支援を行うこと。

(2) CEPライセンス管理

CSP環境の管理インターフェースへのSSOに際して、アクセス元制御を実施するため、Google社が提供するChrome Enterprise Premium (CEP) に関して、必要数分の把握、GCASアカウント紐付け作業及びライセンス管理を実施すること。

3 運用管理機能設計・構築

(1) ユーザー設計

本番アカウント（ネットワーク管理）に関するユーザー及びその権限の設計管理を行うこと。なお、GCASアカウントによる各CSP環境へのSSOが可能になるため、CSP環境内でのユーザー作成は禁止されているものであること。

(2) テンプレート適用・設計・構築

予防的統制や発見的統制、セキュリティ監視情報収集の設定等、ガバナンスに関する設定のため、デジタル庁が公表する必須適用テンプレートを適用すること。

(3) ネットワーク設計・構築

ネットワーク設計及び構築については、設計負荷及び運用負荷の軽減のため、CSPが提供するマネージドサービスを積極的に活用するものとし、以下のとおり行うこと。

- ① 作業対象範囲の要件整理、CIDR、名前解決等、必要に応じて時刻同期のネットワーク設計を実施し、ガバメントクラウド環境全体に係るネットワーク構成等を決定のうえ構築を行うこと。
- ② 運用管理（設計構築におけるテスト期間を含む。）におけるユーザー管理、性能・キ

ャパシティ・コスト管理、情報セキュリティ管理、構成管理、ログ管理等に関する運用設計を行うこと。

- ③ 本設計を実施するに当たり、ASPベンダーを含んだ全体調整等を行うものとし、ヒアリングを実施したうえで要件整理等を行うこと。
 - ④ ガバメントクラウド環境内のCIDR体系を設計する際は、当市の庁内ネットワーク及びASP領域のCIDR体系にも留意すること。特にTransit Gatewayの接続先の共同利用アカウントのVPCのCIDR範囲が重複しないよう留意して設計すること。
 - ⑤ 本番アカウント（ネットワーク管理）のVPC同士、また、本番アカウント（ネットワーク管理）のVPCとASP領域にあるVPCとの接続を行うこと。IPアドレス設計との兼ね合いでCIDR重複する場合を想定し、AWS Private Link、NAT等により回避できるよう設計すること。
 - ⑥ クラウド接続サービスからのホスト接続を承認し、Direct Connect接続に必要なTransit VIFを作成し、接続できるようDX Gatewayを構築、設定すること。
 - ⑦ 各ASP領域へ接続できるよう Transit Gateway等を構築、設定すること。必要に応じて、ASPベンダーとの調整等を行うこと。
 - ⑧ ASPベンダーが実施する疎通テスト、システム動作確認等へ協力すること。
 - ⑨ 受注者の拠点からリモートでの構築及び運用管理ができるよう、GCASガイドを参照し、本番アカウント（ネットワーク管理）への接続環境を整備すること。この場合において、「地方公共団体における情報セキュリティポリシーに関するガイドライン」に記載されているセキュリティ要件を満たすこと。
 - ⑩ CSPの管理コンソールへはGCASを通じてアクセスするものとし、その際必要となるMFAデバイス（ハードウェア）は、受注者が必要数を用意すること。
 - ⑪ CSPが提供するDNSサービス（AWS Route53等）を利用し、名前解決すること。ドメイン名は、当市が指定するものとし、名前解決方式については、市及びASPベンダーと協議のうえ決定すること。
 - ⑫ ガバメントクラウド環境内からの問合せに対し、庁内ネットワークのドメインも含めて名前解決できるよう、当市の現行環境にあるDNSをフォワード先として設定すること。また、当市の現行環境のDNSからのフォワード先としても機能するようにすること。
- (4) テスト
- 本番アカウント（ネットワーク管理）が、問題なく正しく動作することを漏れなく検証すること。
- (5) 継続的な改善に必要な項目の設計・構築
- 移行後に継続的な改善が実施できるよう、GCASガイドを参照し、運用状況の可視化、改善提案等に必要な設計構築を行うこと。
- (6) 一元的な運用管理に関する項目の設計・構築
- 当市のガバメントクラウド環境について一元的に運用管理するものとし、以下のとおり設計構築を行うこと。ただし、CSPが提供する標準的なサービスで実現できない場合にあっては、ASPベンダーにおいて管理するものとする。
- ① 暗号化、不正侵入対策、マルウェア対策、脆弱性対策等の対策について、一元的に管理できること。

- ② ガバメントクラウド環境内の情報システムの状況を一元的に監視できること。
 - ③ CSPが提供するマネージドサービスの利用を原則とし、死活監視に加え、リソースの利用状況を監視できること。また、障害発生を検知した場合には、自動で障害状況等を通知できる仕組みを設け、監視できること。
 - ④ ガバメントクラウド環境内のバックアップを一元的に取得できること。
 - ⑤ 障害やインシデント対応のため、ガバメントクラウド環境内の必要なログを一元的に収集し、保存できること。
 - ⑥ ガバメントクラウド環境内の仮想マシンの起動、停止、バックアップ等のイベント及びジョブのスケジュールを一元的に管理できること。
- (7) 信頼性/可用性設計・構築
- CSP環境における信頼性及び可用性を確保できるよう、必要な設計構築を行うこと。特にCSP上で冗長化を保っていないサービスについては、冗長化設計及び構築を行うこと。
- (8) 拡張性設計・構築
- CSPのオートスケーリング機能の活用により高い拡張性を得ることができることから、システム全体として拡張性設計及び構築を行うこと。
- (9) 性能設計・構築
- 適切な性能を提供できるよう、CSPが提供するサービスにおいて性能設計が可能なリソースについては、性能設計及び構築を行うこと。
- (10) 運用管理設計
- 「第4 運用管理補助要件」にある運用管理を実施できるよう、以下のとおり設計を行うこと。
- ① 設計結果及び連絡体制、対応手順を含めた運用ドキュメント（運用設計書）を作成すること。
 - ② 運用設計の結果に基づき、ガバメントクラウド環境の運用管理に必要な手順書（運用管理手順書）を作成すること。

第4 運用管理補助要件

1 通信回線・機器保守

(1) 拠点接続サービス保守

拠点接続サービス（通信回線（主回線））の保守については、以下のとおり行うこと。

- ① 故障回復時間のサービスレベル水準合意（SLA：Service Level Agreement）を設定し、拠点接続サービス区間の故障により不通が発生した際に、復旧に1時間以上要した場合には、回線料金の返還に応じること。
- ② 回線稼働率のSLAを設定し、それぞれの回線の月間稼働率を99.9%以上とすること。
なお、当該SLAを達成できない場合の補償が定義されていること。
- ③ 網内遅延が生じうる回線を使用する場合は、網内遅延のSLAを設定し、遅延の月間平均値が35ミリ秒を超えた場合の補償が定義されていること。
- ④ 回線終端装置（ONU）に不具合等が発生した場合は、ルーターの保守と同程度の対応を行うこと。

(2) クラウド接続サービス保守

クラウド接続サービスの保守について、回線稼働率のSLAを設定し、それぞれの回線の月間稼働率を99.99%以上とすること。なお、当該SLAを達成できない場合の補償が定義されていること。ただし、CSPが提供する閉域網接続サービス（AWS Direct Connect）のSLAについては、CSP側のSLAに準拠するものとする。

(3) ルーター保守

設置するルーターの保守については、以下のとおり行うこと。

- ① オンサイト保守とし、機器故障時の交換、設定の復元、正常動作の確認、他ルーターとの冗長化の再構成等の現状復帰作業を含むこと。
- ② オンサイト保守の対応時間は、平日：9:00～17:00までとすること。
- ③ 障害発生時のオンサイト保守作業の駆付け目標時間は、障害受付後から4時間以内とすること。

2 運用管理機能運用・保守

(1) ユーザー管理

利用しているユーザー情報に変更（追加、更新、削除等）が生じた場合には、GCASガイドを参照し、変更を行うこと。また、ユーザーに適用している権限設定についても定期的に見直し、適切な権限管理を行うこと。

(2) 保守・メンテナンス

本業務の範囲における必要な設定変更等について、定型業務として実施するものとし、以下のとおり行うこと。

- ① 仮想マシン等に対して、パッチファイルの適用等の脆弱性対応を実施すること。
- ② パッチの取得に当たり、必要なネットワーク経路を確保するとともに、配信サーバ等のパッチファイル配布方針を検討すること。
- ③ ネットワークアクセスコントロールリスト（NACL）、セキュリティグループ（SG）及びNetwork Firewall等のポリシー修正をすること。

- ④ ASPベンダーからの依頼に基づき、各ASP領域へ接続するためのゲートウェイ等のパラメータ及びDNS等の設定変更を行うこと。設定変更に当たっては、対応作業の内容について市と協議のうえ実施すること。
- ⑤ 必要に応じて、仮想マシンの起動、停止、バックアップ等のイベント及びジョブのスケジュールを管理すること。
- ⑥ 必須適用テンプレートに変更があった場合は、再度、テンプレートを適用すること。

(3) 監視

ガバメントクラウド維持の観点から、死活監視のほか、インフラに対する脅威や不正なアクティビティ及び不適切なアクセス設定の検出、リソースの利用状況について監視すること。

(4) 障害対応

ガバメントクラウド環境に構築された情報システムにおける障害時の対応については、GCASガイドを参照し、以下のとおり行うこと。

- ① ガバメントクラウド環境内で障害（情報セキュリティに関するアラートやインシデントへの措置を含む。）が発生している場合は、速やかに復旧に取り組むとともに、当市に障害発生状況や復旧の状況等を通知すること。
- ② ASPベンダーからの問合せ等、復旧に向けた原因調査等に関して積極的に協力すること。
- ③ 障害対応に伴い、必要に応じて、CSPに連絡すること。
- ④ 根本解決が必要なインシデントにあっては、問題管理へエスカレーションを行い、根本原因の調査、恒久的な対策の検討及び対策完了まで管理すること。
- ⑤ その他緊急を要する場合の対応については、市と協議のうえ実施すること。

(5) 情報セキュリティ管理

情報セキュリティ管理については、以下のとおり行うこと。

- ① 情報セキュリティリスクを低減させるための提案、予防対策等を実施すること。
- ② 運用管理用にパソコンを導入する場合にあっては、ウイルス対策ソフトを導入し、個別の対策を実施すること。最新のパターンファイルの適用と定期的なスキャンを実行すること。
- ③ 個人情報の漏えい防止の観点から、ガバメントクラウド環境におけるユーザー（必要に応じてルートユーザー）のアクセスログ及び操作ログを取得すること。
- ④ アクセスログ及び操作ログについて、ユーザー及び第三者による改ざんがなされないよう、書き込み禁止等の防止措置を実施すること。
- ⑤ 少なくとも1年分のログを保存できること。直近2箇月分程度のログはすぐに参照可能であること。

(6) 構成管理

CSPの構成管理サービス等を活用し、システムの維持及び運用に必要な設定パラメータ等の管理を行うこと。

(7) 技術支援

ASPベンダー等のステークホルダーからのガバメントクラウド環境に関する技術的な問合せに対し、技術的助言、補助等を行うこと。

(8) ドキュメント管理

サービスの設定変更等に伴い、必要なドキュメント（設計書、手順書等）の最新化及び版数管理を行うこと。

(9) 性能・キャパシティ・コスト管理

運用管理する領域のリソースの利用料金及び稼働実績（vCPU 利用率、ストレージ使用量、通信量、ログ等）について、ダッシュボード等のツールを活用して収集及び分析を行うこと。性能や閾値超過に起因して発生するインシデントを未然防止すること。

また、「継続的運用経費削減（FinOps）ガイド【1.0版】」及び「ガバメントクラウドを利用した標準準拠システムへの移行後の運用経費に係る見積チェックリスト（令和7年4月版）」の内容を反映し、運用コストの最適化を図ること。

(10) バックアップ・リストア管理

本業務の範囲において障害が発生した場合、迅速に復旧できることを前提にリストアできる状態を確保すること。

(11) 継続的な改善

収集したログや監視、診断結果等进行分析し、運用状況を可視化するとともに、CSPの改善提案機能に基づいて評価を行い、当市に対し、継続的な改善提案を行うこと。

3 連絡体制

本業務の履行に当たって、問合せ等のサポートをする機能として、以下のとおり連絡体制を整備し、運営すること。

- ① 当市の開庁時間（平日：8:30～17:15まで）に電話、メール又は問合せフォームによる連絡を受け付けること。
- ② 開庁時間外にあっても、障害等の緊急時の対応のため、24時間365日、電話、メール又は問合せフォームによる連絡を受け付けること。
- ③ ガバメントクラウド環境全体の停止等、大規模障害時においては、当市が行政という重要インフラであることを鑑み、上記時間帯によらず対応を行うこと。

第5 業務実施体制

1 プロジェクト管理

業務全体における計画、進捗管理、課題管理、変更管理、リスク管理等のプロジェクト管理を適切に行うこと。庁内手続など、当市の職員でなければ行うことのできないこと以外、全てプロジェクト管理の義務を負うこと。

2 実施体制

本業務を確実に履行できる体制について、下表の内容を考慮し、適切なスキルを持った要員を配置して整えること。

なお、本業務はAWSの高度な知識と技術が必要とされるため、AWS Solution Architect - Professional の保有者がプロジェクトに参画又は協力できる体制を整え、支障なく業務を実施できるようにすること。また、契約期間において、受注者はAWSサービスパートナーのセレクトティア以上の認定を受けていること。

表4. 実施体制に係る役割一覧

役割	詳細
統括業務責任者	・ 本業務の統括的なマネジメントを行う。 ・ 市からの要求事項に対して、事業者として迅速に判断ができること。 ・ (独)情報処理推進機構が実施する情報処理技術者試験合格による資格(プロジェクトマネージャー)又は米国プロジェクトマネジメント協会が認定するPMP (Project Management Professional) 試験合格による資格を有すること、若しくはEXIN(Examination Institute for Information Science) が認定するPRINCE2 (PRjects IN Controlled Environments, 2nd version) のPractitioner 試験に合格していること。
業務遂行責任者	・ 本業務を遂行するために必要な全体的な管理を行う。 ・ 各チームのリーダーを支援するとともに、チームをまたぐ横断的な調整を行う。 ・ 本業務に関係するステークホルダーとの調整を行う。 ・ CSP設計、構築及び運用の1年以上の実務経験を有すること。
チームリーダー	・ チーム内のメンバー管理、進捗、課題、問題等に対して、マネジメントを行い、チーム内のタスクを円滑に推進する。 ・ 業務遂行責任者や他チームとの調整を行う。 ・ 市との窓口を担当する。 ・ CSP設計、構築及び運用の1年以上の実務経験を有すること。
チームメンバー	・ チームリーダーの指示のもと、担当領域における業務を遂行する。 ・ チームメンバーの半数以上が、CSP設計、構築及び運用の1年以上の実務経験1年以上を有すること。

3 会議体

ミーティングについては、下表のとおり開催すること。ミーティング後は、その都度、議事録を作成して納入すること。その際、必ず当市のレビューを受け、正当な指摘に対し

ては加除訂正を行うこと。

表5. ミーティング一覧

会議体	開催方式	内容
キックオフ（初回）	対面（ハイブリッドも可）	・プロジェクトの定義及び管理について、ステークホルダー間において合意を得る。
定例会議	オンライン	・円滑なプロジェクト推進のため、全体スケジュールに対する進捗管理及び課題管理に係る報告を行う。 ・プロジェクト計画に変更が必要となる場合の協議を行う。 ・要件及び仕様の調整、作業内容の検討と調整等を行う。
稼働判定会議	対面又はオンライン	・設計、構築、テストの内容を踏まえ、運用開始の判定を行う。

第6 成果物

1 納入と承認

成果物の納入は、当市による検収が行われ、承認された時点で完了する。なお、検収基準を満たさない場合は、承認しない。

当市の検収を受け、正当な契約不適合の指摘がある場合は補正すること。

2 ドキュメントの成果物

(1) ドキュメントの品質

ドキュメントの品質については、以下のとおり担保すること。

- ① ドキュメントの品質は、第一義的には、ドキュメントの利用者がその利用目的を達成できることである。
- ② 社内用語や語義が不安定な言葉については、必ず定義や解釈を示す文章を書き加えること。
- ③ ドキュメント間の整合性を取る。また、様式を揃える、記述内容を定めるなど、ドキュメントの管理基準を策定し、遵守すること。

(2) ドキュメントの形式

いずれもMicrosoft Word/Excel/PowerPoint2016又はAdobe Acrobat Readerで読み込みと複製（印刷を含む。）が可能なデータ形式とする。

3 ドキュメントの著作権

本業務で作成されたドキュメントに関しては、原則として全て当市に著作権が移転するものとする。なお、この際、著作者は、著作者人格権を行使しないものとする。

提案資料等、やむを得ず移転できないものについては、原則として共有とする。この場合、いずれの当事者も相手方への通知や支払の義務を負うことなく、秘密保持義務を侵害しない範囲内で、係る共有著作権を行使することができるものとする。

4 納入成果物

成果物として納入するものは、下表のとおりとする。

これらは一般的な成果物を示すものであり、運用に引き継がれる原始資料として追加が必要なもの等は、作成すること。

表6. 納入成果物一覧

No.	成果物	納入期限
1	実施計画書（プロジェクト管理事項、体制等を含む。）	契約締結後、14日以内
2	業務工程表（スケジュール、WBS）	契約締結後、14日以内
3	環境設計書（構成図・設定パラメータ）	設計構築後
4	テスト結果報告書	設計構築後
5	プロジェクト管理に関する書類（課題管理表、リスク管理表、変更管理表等）	設計構築期間中、随時更新
6	打合せ資料、議事録	会議の後、10営業日以内

7	運用管理設計書	設計構築後
8	運用管理手順書	設計構築後
9	運用管理報告書（月次レポート）	運用保守月の翌20日

第7 その他特記事項

1 引継ぎ対応

本業務の履行期間の満了、全部若しくは一部の解除、又はその他契約の終了事由の如何を問わず、受注者は後継の事業者引継ぎを行うものとし、運用管理業務履歴、最新の環境設定資料等の必要な情報をまとめた運用引継書を作成すること。

2 仕様書の解釈

本仕様書及び添付書類に定めのない事項及び解釈の相違があった場合において、本業務の履行に際し必要な事項が発生した場合は、原則として、当市の解釈が優先して適用されるものとする。ただし、当市の解釈によりがたいと双方が認める場合にあっては、協議のうえ対応するものとする。

3 ガバメントクラウド関連資料

デジタル庁が公表しているガバメントクラウドに関するドキュメントは、以下のとおりである。それぞれ内容を参照し、これらに沿って業務を実施すること。

- ① 地方公共団体情報システム標準化基本方針
- ② 地方公共団体情報システムのガバメントクラウドの利用について
- ③ 地方公共団体情報システム ガバメントクラウド移行に係る手順書
- ④ ガバメントクラウドリスクアセスメント

※契約締結後に閲覧可

- ⑤ ガバメントクラウド利用における推奨構成
- ⑥ GCASガイド

※メンバー専用ページについては、GCAS利用開始後に閲覧可

- ⑦ ガバメントクラウドを利用した標準準拠システムへの移行後の運用経費に係る見積チェックリスト（令和7年4月版）

※契約締結後に閲覧可

仕様書 別紙

情報セキュリティに関する特記事項

(総則)

第1条 受注者は、情報セキュリティの重要性を認識し、奥州市情報セキュリティ規程（平成22年奥州市共同訓令第1号）及び情報セキュリティ実施手順に基づき、本情報セキュリティに関する特記事項（以下「特記事項」という。）を遵守しなければならない。

(責任体制の整備)

第2条 受注者は、委託業務に係る情報セキュリティ責任を有する者（以下「主任担当者」という。）を定め、書面により発注者に報告するものとする。また、主任担当者を変更したときも、同様とする。

(業務従事者の特定)

第3条 受注者は、委託業務に従事する者（以下「業務従事者」という。）の氏名その他必要な事項を記載した名簿を作成し、常備するとともに、書面により発注者に報告するものとする。また、名簿の記載内容を変更したときも、同様とする。

2 業務従事者は、主任担当者の指示に従い、この特記事項に定める事項を遵守しなければならない。

3 委託業務の履行のため、業務従事者が事務室等に立ち入る場合は、受注者は、身分を証する書類を常時携帯させ、及び事業者名の記載された記章又は名札を視認しやすい位置に着用させなければならない。

(教育及び研修の実施)

第4条 受注者は、業務従事者その他関係人に対し、情報セキュリティに対する意識の向上、業務従事者が遵守すべき事項その他委託業務の履行に必要な教育及び研修を実施するものとする。

(秘密保持義務)

第5条 受注者は、発注者から秘密と指定された事項及び委託業務の履行に際し知り得た秘密を第三者に漏らしてはならない。

2 受注者は、業務従事者その他関係人について、前項の義務を遵守させるために誓約書の提出等必要な措置を講じなければならない。

3 前2項の規定は、契約の満了又は解除等契約終了事由の如何にかかわらず、契約の終了後も同様とする。

(業務履行場所)

第6条 受注者は、発注者が指定する場所で業務を行うものとする。

2 受注者は、発注者が指定する場所以外で業務を行う場合は、業務の着手前に、住所等を書面により発注者に報告するものとする。

3 受注者は、前項の規定による場合、その作業場所について、奥州市情報セキュリティ規程及び情報セキュリティ実施手順に規定されている安全対策を確保しなければならない。

(情報資産の適正な管理)

第7条 受注者は、発注者から提供された委託業務に係る資料、貸与品及びその他の情報資産（以下「情報資産等」という。）の漏えい、改ざん、滅失、き損等の防止のため、次の各号の定めるところにより、適正に管理しなければならない。

- (1) 情報資産等の管理責任者を定めるとともに、管理台帳を設け管理状況を記録すること。
- (2) 情報資産等を施錠できる保管庫又は施錠及び入退室管理可能な保管室に格納する等して管理すること。
- (3) 発注者が指定する場合を除き、情報資産等を定められた場所から持ち出さないこと。
発注者の指示を受けて持ち出すときは、データの暗号化など安全確保のために必要な措置を講ずること。
- (4) 事前に書面により発注者に申請し、承認を得た場合を除き、情報資産等を複製又は複写してはならないこと。

2 受注者は、情報資産等について、委託業務を完了した後、遅滞なく返還、廃棄又は消去するものとする。ただし、情報資産等を廃棄又は消去する場合は、発注者の承認又は立会いを得て実施することとし、当該情報資産等が記録された電磁的記録媒体の物理的な破壊、その他記録されている内容が判読できないよう必要な措置を講じなければならない。

3 第1項に規定する情報資産等の管理が適正でないと認められる場合、発注者は受注者に対し、改善のため必要な措置を講じることを求め、又は指示するとともに、改善が図られたと認めるまで業務を中止させることができる。

(目的外使用の禁止)

第8条 受注者は、委託業務において利用する情報資産等を他の用途に使用し、又は発注者の承諾なしに第三者に提供してはならない。

(情報システム等へのアクセス)

第9条 受注者が発注者の情報システム等にアクセスする場合の情報の種類、範囲及びアクセス方法については、発注者の指示に従わなければならない。

(再委託の制限)

第10条 受注者は、委託業務を第三者へ委託（以下「再委託」という。）してはならない。

2 受注者は、委託業務の一部をやむを得ず再委託する必要がある場合は、次の各号に定める事項を明確にしたうえで、業務の着手前に、書面により発注者に申請し、承認を得なければならない。

- (1) 再委託する事業者の商号又は名称、住所
- (2) 再委託する理由
- (3) 再委託して処理する業務の内容
- (4) 再委託事業者が取り扱う情報
- (5) 再委託事業者における安全性及び信頼性を確保する対策並びに再委託事業者に対する管理及び監督の方法
- (6) その他発注者が適否を判断するために必要な事項

3 前項の場合において、受注者は、再委託事業者がこの特記事項に定める一切の義務を遵守させるとともに、発注者に対して、当該事業者の再委託に基づく行為全般について責任を負うものとする。

4 受注者は、再委託事業者との契約において、再委託事業者に対する管理及び監督の方法について、具体的に定めなければならない。

(監査及び検査)

第11条 発注者は、委託業務に係る情報セキュリティ対策について必要があると認めるときは、受注者の委託業務の処理状況等について監査又は検査を行うことができる。

- 2 受注者は、発注者の監査又は検査の実施に協力しなければならない。
- 3 第1項の規定による監査又は検査の結果、受注者の委託業務の処理状況等が適正でないと認められる場合、発注者は受注者に対し、改善のため必要な措置を講じることを求め、又は指示するとともに、改善が図られたと認めるまで業務を中止させることができる。

(業務実施状況の報告)

第12条 受注者は、発注者から委託業務の進捗状況、処理態様、処理の実績、処理に要した時間等について報告を求められた場合には、発注者が指示する方法及び時期により、報告するものとする。

(事故等の報告義務)

第13条 受注者は、委託業務の履行中に事故が生じ、又は生じるおそれがあることを認知したときは、その事故発生の帰責の如何にかかわらず、直ちに発注者に報告し、速やかに応急処置を加えた後、遅滞なく書面により詳細な報告及びその後の具体的な事故防止策を提出しなければならない。

- 2 前項の事故が、委託業務に利用する情報資産等の漏えい、改ざん、滅失、き損等の場合には、受注者は、業務を中止するとともに、速やかに前項に規定する措置を講じなければならない。なお、業務中止の期間は、発注者が指示するまでとする。
- 3 第1項の事故により、以降の業務の円滑な進行を妨げるおそれがあるときは、受注者は、速やかに問題を解決し、業務進行に与える影響を最小限にするよう、努めなければならない。

(事実の公表)

第14条 発注者は、前条の事故が発生した場合は、必要に応じて、受注者の名称を含む当該事故に関する情報を公表することができる。

(契約解除及び損害賠償)

第15条 発注者は、受注者がこの特記事項に定める事項に違反していると認めたときは、原契約の定めるところにより、契約の解除又は損害賠償を請求することができる。