仕　様　書

１　業務名

内部通信監視サービスの構築及び運用・保守業務

２　履行期間

契約締結日から令和１３年（２０３１年）１１月３０日まで

⑴　準備期間

契約締結日から令和７年（２０２５年）１１月３０日

⑵　サービス提供期間

令和７年（２０２５年）１２月１日から令和１３年（２０３１年）１１月３０日

３　履行場所

広島市企画総務局行政経営部システム基盤課（広島市中区国泰寺町一丁目４番２１号)、その他本市が指定する場所

４　業務の目的

本業務は、令和元年（２０１９年）６月に策定した「広島市基幹系システム等の更新指針」に基づいて、基幹系システム等の情報セキュリティ対策を強化するため、基幹系システム等のサーバ・端末等の通信を監視するサービス（以下「内部通信監視サービス」という。）を構築し、運用・保守を実施するものである。

５　業務の概要

本市は、原則、本業務で必要となるハードウェア、ソフトウェア等を所有せず、受注者が提供するサービスを利用するものとする。

受注者は、独立行政法人情報推進機構が策定した「「高度標的型攻撃」対策に向けたシステム設計ガイド」を踏まえ、本仕様書の要件を満たす内部通信監視装置等を導入し、必要なサービス提供を行うこと。

⑴　監視対象

基幹系システム等を構成するネットワーク上に監視ポイントを８か所以上設置し、各監視ポイントにおけるすべての通信（許可された通信を含む。）を監視対象とすること。監視ポイントは、契約締結後に本市と協議の上決定することとし、受注者は、通常の通信に影響を与えないよう監視を行うこと。

⑵　監視時間

２４時間３６５日（SOC サービスによる有人監視を原則とする。）

⑶　監視内容

各段階で想定される監視内容を次に示す。

ア　初期侵入段階の検知

・　未知のウイルス等のダウンロード

・　不正な通信先（URL や IP アドレスを含む。）へのアクセスの検知
・　不審な証明書の検知

イ　基盤構築段階の検知

・　バックドアの開設（C&C サーバ（不正な接続先としてデータベース登録されているもの以外を含む。）へのコネクトバック通信）
・　攻撃に悪用される可能性のあるツールのダウンロード
・　ネットワーク環境の調査、探索（IP アドレスの探索、サービス状態や OS 情報等の端末情報の探索、ファイル共有の探索）

ウ　内部侵入・調査段階の検知

・　管理者及び一般ユーザのログインの試行（多数の失敗）
・　内部システムへの不正なアクセスや脆弱性（セキュリティホール）へのアクセス
・　内部ネットワーク内で FTP や Windows ファイル共有を通じて攻撃に利用される攻撃用ツールのコピー
・　許可された端末以外からの各サーバへのリモート操作

エ　目的遂行段階の検知

・　圧縮ファイル送信
・　不審な外部への通信（IP ヘッダ情報や通信先（危険な通信先としてデータベース登録されているもの以外を含む。）、GET メソッドなどの確認等）
・　危険な通信（脅威を含む URL や IP アドレスへのアクセス）
・　長時間維持されたセッション、大量のデータを送受信していたセッション及び短時間で連続的に繰り返し発生するセッション

6　業務の内容

⑴　準備期間に実施する業務

ア　機器等の調達

次の要件を満たす機器等を調達すること。その他サービスの構築に当たって必要となる機器等があれば、本業務において合わせて調達すること。

(ｱ) 内部通信監視装置：　２台以上（冗長構成※とする。）

構成	1台当たりの要件等
内部通信監視装置	・パロアルトネットワークス社製 PA-3430 又はこれと同等のもの ・次の機能を有すること。 ➢ 侵入防止機能（IPS・IDS） ➢ アンチウイルス機能 ➢ アンチスパイウェア機能（C&C 通信対策） ➢ URL フィルタリング機能 ➢ サンドボックス機能（未知のマルウェア対策） ・　将来的な機能拡張を見据えて、次の機能等を有すること。 ➢ 悪性ファイルが検出された場合に、サンドボックス機能により、即時にシグネチャを自動生成し、該当ファイルを数分でブロックするとともに、管理者にメール通知を行う機能 ➢ 筐体内で SSH 通信を復号化し、ポートフォワード通信を検知可能であること。また、筐体内で SSL TLS1.2 に準拠した通信を復号化し、アプリケーションの識別及び contents 検査のポリシーが適用可能であること。 ・監視ポイントを通過するすべての通信を相関的に分析し、不審な通信やプログラムの動作等を検知するとともに、問題のあるサーバ及び端末を特定できること。 ・ミラーポート接続に対応していること。 ・syslog へのログ出力に対応していること。 ・最大 12 以上の監視ポイントを設定できること。原則として、1 筐体にすべての監視ポイントを設定する。 ・監視ポイントとの接続用に次のインターフェースを有すること。 ➢ 10G BASE-T × 12 ポート以上 ・19 インチ幅のラック搭載型とし、2U 以内に収納可能であるとともに、電源が冗長化されていること。
その他	・サービス提供期間を通じて製造元によるサポートを受けられること。 ・その他運用に必要なライセンスを準備すること。

※ 既設ネットワーク機器の制約によりポートミラーリングの冗長化を行えない。アクティブ/スタンバイ構成となり、本番系から待機系への切替えを自動で行えないため、障害等が発生した場合は、受注者において現地でケーブルの差替えなどを実施すること。

(ｲ) ログ管理装置：　２台以上（冗長構成※とする。）

構成	1台当たりの要件等
OS	・Red Hat Enterprise Linux 9 又はこれと同等のもの ・サービス提供期間中に OS 開発元のサポート期限を迎える場合は、当該期限までに後継の OS へバージョンアップするなど、常にサポートが受けられる状態を維持すること。
ソフトウェア	・rsyslog 又はこれと同等のもの
その他	・必要なハードウェア一式を準備すること。 ・CPU、メモリ、ハードディスク等については、サービス提供を行う上で必要な性能を有すること。 ・19 インチ幅のラック搭載型とし、2U 以内に収納可能であるとともに、電源が冗長化されていること。

※ ログの欠損が発生しないよう本番系・待機系ともにログの収集を行える構成とすること。

(ｳ) ＶＰＮ装置：　２台以上（冗長構成※とする。）

構成	1台当たりの要件等
VPN 装置	・SOC サービスとの接続は、閉域網（IP-VPN 接続（IKEv2））によることとし、これに対応したハードウェアを準備すること。 ・19 インチ幅のラック搭載型（ラックマウントキットを使用しての設置も可とする。）とし、1U 以内に収納可能であること。 ・所要の回線費用は、本業務に含めること。

※ 既設ネットワーク機器の制約によりポートミラーリングの冗長化を行えない。アクティブ/スタンバイ構成となり、本番系から待機系への切替えを自動で行えないため、障害等が発生した場合は、受注者において現地でケーブルの差替えなどを実施すること。

(ｴ) 内部通信監視装置接続用スイッチ：　２台以上（冗長構成とする。）

構成	1台当たりの要件等
内部通信監視装置接続用スイッチ（以下「接続用スイッチ」という。）	・内部通信監視装置、ログ管理装置、VPN 装置との接続に当たって必要なインターフェースを備えていること。 ・19 インチ幅のラック搭載型（ラックマウントキットを使用しての設置も可とする。）とし、1U 以内に収納可能であるとともに、電源が冗長化されていること。

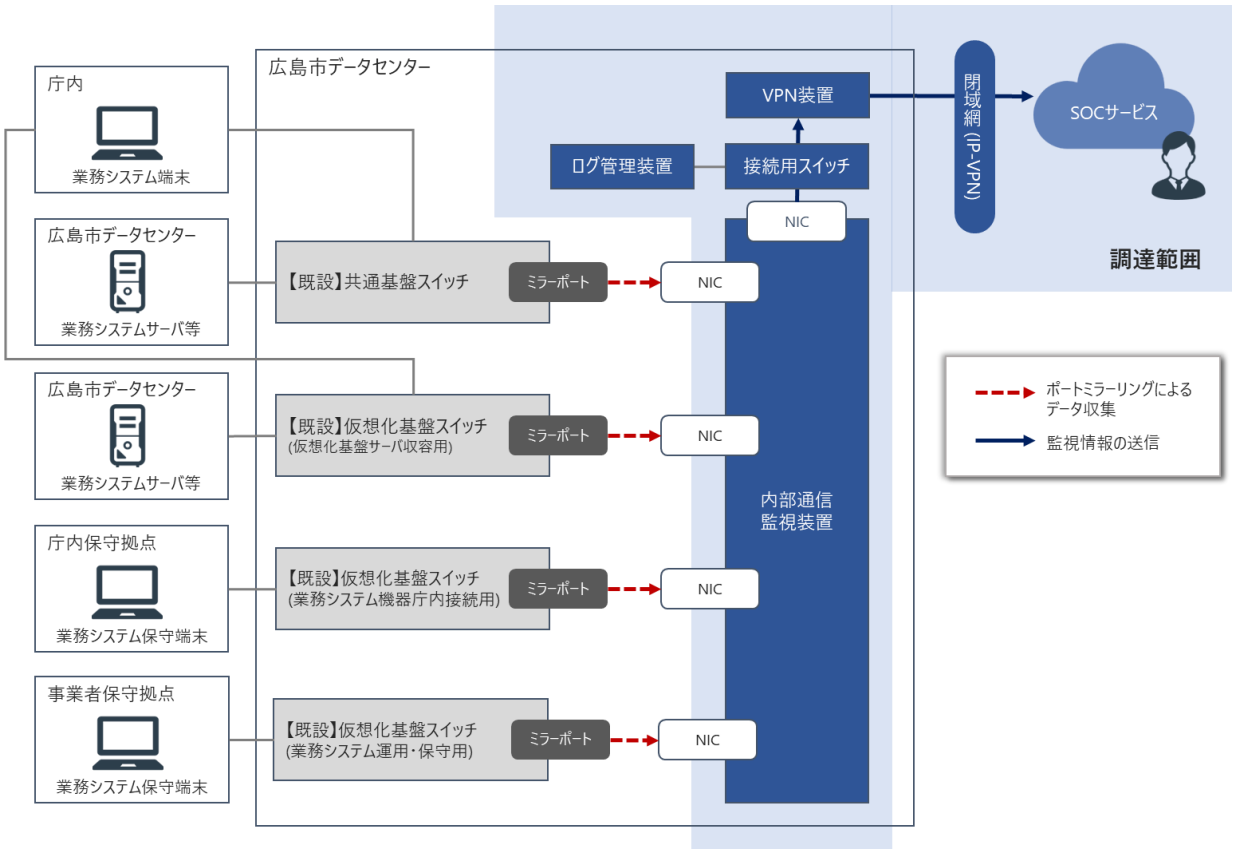
(オ) ＳＯＣサービス：　１式

構成	要件等
SOC サービス	・経済産業省が策定した「情報セキュリティサービス基準（セキュリティ監視・運用サービス）」への適合性を第三者機関により認定されたサービスで、本業務の要件を満たすことができるもの ・セキュリティインシデントの対応状況や問合せ状況、レポート等を閲覧できる本市専用のポータルサイトを提供すること。ポータルサイト接続時には、多要素によるユーザ認証を行うとともに、閲覧に関する通信の暗号化を行うこと。 ・サービス提供主体（組織・部門）が、ISO/IEC 27001 の認証及びプライバシーマークを取得していること。 ・サービス提供環境（マシンルーム・監視ルーム）において、監視運用基盤へのアクセス及び利用が、物理的又は論理的に制限されていること。また、サービス提供環境の管理が、サービス提供主体の情報セキュリティマネジメントシステム（ISMS）の基で実施されていること。 ・サービス提供環境内に設置されたすべての端末の操作ログを録画にて取得すること。また、取得するすべての操作ログはサーバで集中管理され、セキュリティ監査等の用途に応じプレイバック／レポーティングが可能なこと。 ・次のいずれかの資格を有する従事者を１名以上配置すること。 ➢ 情報処理安全確保支援士 ➢ CISA（Certified Information System Auditor） ➢ CISM（Certified Information Security Manager） ➢ CISSP （Certified Information Systems Security Professional） ➢ GIAC（Global Information Assurance Certification） ➢ CND（Certified Network Defender） ・日本語での対応が可能であり、サービスに関わるすべての業務が日本国内で行われること。

イ　設計・構築等

必要な調査・分析及びヒアリングを行った上で、設計・構築、必要なテスト等を実施すること。本市の想定する機器等の構成イメージは次図のとおり。

監視ポイントを含む最終的な構成については、契約締結後に本市と協議の上決定する。



(ｱ) 概要設計

概要設計書を作成し、本市の承認を得ること。想定される主な設計内容を次に示す。

a　機能設計

機能の実現方法を定義する機能設計を行い、概要設計書に記述すること。

b　ハードウェア設計

機器構成及び機器の設定内容を定義するハードウェア設計を行い、概要設計書に記述すること。

c　ソフトウェア設計

ソフトウェア構成及びソフトウェアの環境設定を定義するソフトウェア設計を行い、概要設計書に記述すること。

d　ネットワーク設計

ネットワーク構成及びネットワーク方式を定義するネットワーク設計を行い、概要設計書に記述すること。

(ｲ) 詳細設計

概要設計書に基づき、具体的な仕様、運用等を記述した詳細設計書、ハードウェア・ソフトウェアの環境設定書、監視ネットワーク構成図を作成し、本市の承認を得ること。

(ｳ) 構築

- 本市データセンター等に機器等を搬入・設置し、概要設計書、詳細設計書、監視ネットワーク構成図等に基づき、内部通信監視サービスを構築すること。本市データセンターの利用に当たっては、契約締結後、本市が貸与する手引きの内容に従うこと。
- SOC サービスの導入に当たって、内部通信監視装置等から SOC サービスに通信ログ等の監視情報を送信する必要がある場合は、閉域網（IP-VPN 接続（IKEv2））を利用すること。
- ログ管理装置には、原則として、本市が提供するウイルス対策ソフト（Trend Micro Apex One 又は Deep Security）を導入すること。これらのウイルス対策ソフトに対応していない場合は、受注者において必要なセキュリティ対策を講じること。
- 内部通信監視装置を既設ネットワーク機器のミラーポートに接続する場合、その他の既設環境で設定変更が必要となる場合は、本市がこれらの機器等を管理する事業者（以下「既設機器等事業者」という。）に委託して、設定変更作業を実施する。受注者は、設定変更に必要な情報（ミラーポートの設計内容、設定変更手順書、タイムスケジュール等）を提示し、本市の承認を得ること。
- 既設機器等事業者が設定変更作業を実施する場合、受注者は、都度、作業時及び翌開庁日の立会いを行うこと。
- 本業務で調達する機器間の配線は、部材の調達を含めて受注者において実施すること。なお、本市データセンター内で既設ネットワーク機器等への配線が必要となる場合は、本市がデータセンター事業者に委託して実施する。
- 構築作業は、既設機器等事業者その他の関連する事業者と緊密に連携・協力して行うこと。

(ｴ) テスト

a　システムテスト

構築した内部通信監視サービスが正しく動作するかを確認するために、脆弱性、ウイルス、危険ファイルのダウンロード制御、スパイウェア、URL フィルタリングなどのシステムテストを実施すること。ただし、本市が不要と認めたものについては省略することができる。

- システムテスト計画書及びシステムテスト仕様書を作成し、本市の承認を得た上で、システムテストを実施すること。
- システムテストは、ネットワークの負荷に影響を与えないよう実施すること。
- システムテストの結果については、合否を判断できる形式でシステムテスト結果報告書を作成し、本市の承認を得ること。
- システムテストを通じて発生した課題・問題点については、原則、すべての原因を究明し、適切に対処した上で、課題・問題点の内容、原因、対処内容をシステムテスト結果報告書に記述すること。システムテスト終了までに完了しない課題・問題点については、影響範囲及び対応期限を明確に示し、本市の承認を得ること。
- システムテストの作業場所及びシステムテストを行う環境は受注者が準備すること。本市データセンターへ設置した機器等に対するシステムテストについては、原則、本市

データセンターにおいて実施し、受注者は、必要な機器及びネットワーク環境を準備すること。

b　ユーザテスト

本市が、必要な機能等が適切に実現されているか、業務遂行上の問題がないかなど、本市の求める要件が実現されているかを確認するため、ユーザテストを実施する。ただし、本市が不要と認めたものについては省略することができる。

- ユーザテスト計画書及びユーザテスト仕様書を作成し、本市の承認を得ること。
- ユーザテストの結果については、合否を判断できる形式でユーザテスト結果報告書を作成し、本市の承認を得ること。
- ユーザテストを通じて発生した課題・問題点については、原則、すべての原因を究明し、適切に対処した上で、課題・問題点の内容、原因、対処内容をユーザテスト結果報告書に記述すること。

（オ）その他

- 受注者は、セキュリティインシデント、機器等の障害を検知した場合の対応手順等を整理し、これをまとめた障害対応マニュアルを作成すること。
- セキュリティインシデントが発生した際の対応は、本業務とは別に委託する統合運用事業者又は本市職員（以下これらをまとめて「本市運用担当者」という。）が実施する。受注者は、障害対応マニュアルなどを基に、対応方法を説明し、引継ぎを行うこと。
- サービス提供開始までに、本市と受注者で協議の上、SLA（Service Level Agreement）を締結すること。
- 本市が想定する SLA の主な項目を次表に示す。

サービスレベル項目		項目内容	基準	サービスレベル目標
可用性	サービス提供保証時間	サービス提供保証時間を定義する。	実サービス提供時間	24 時間（計画停止は除く）
	サービス稼動率	サービス提供保証時間に渡りサービス提供が行えているか管理する。	（実サービス提供時間－停止時間）÷サービス提供保証時間〔%〕	99.95%以上
障害対応	復旧時間	機器等の障害によるサービス停止が発生した際の復旧に要する時間を管理する。	障害連絡後、復旧に要した時間	12 時間以内
	障害報告書提出時間	障害報告を行う。	障害復旧後に障害報告書を提出するまでの時間	障害復旧後 3 日以内
	障害発生通知遵守率	適切な障害報告がなされているか管理する。	（障害検知後 30 分以内（※）に本市に報告した障害件数）÷障害発生件数〔%〕	100%
セキュリティ	事故件数	ハードウェア、ソフトウェア、施設等において、万全のセキュリティ対策を行う。	受注者の責めに帰すべき事由で発生した情報漏洩等のセキュリティに係る事故件数	0 件

（※）危険度の高いセキュリティインシデント、機器等の障害によるサービス停止が発生した場合を想定する。その他のセキュリティインシデント等が発生した場合については、設計段階で検討する。

⑵ サービス提供期間に実施する業務

ア　運用・保守

運用・保守計画書を作成した上で、内部通信監視サービスを構成する機器等の運用・保守を行うこと。作業場所は、必要に応じて受注者が準備するものとし、内部通信監視サービスを構成する機器等との接続は、閉域網によること。受注者は、作業場所を準備しようとする場合、あらかじめ本市の承認を得ること。

㈠ 監視作業

- 監視ポイントを通過するすべての通信を対象に、２４時間３６５日リアルタイムに監視を実施すること。監視はSOCサービスによる有人監視を原則とする。
- 検知したセキュリティインシデントの危険度の分析・判定を行い、ポータルサイト、メール等を通じて本市運用担当者等へその内容を通知すること。
- 監視ポイントごとに対応の優先度が異なるため、複数の監視ポイントで同時に危険度が高いセキュリティインシデントが発生した場合であっても、特に優先して対応しなければならないものを一目で判別できるよう、通知内容には監視ポイント固有の識別子を付加すること。また、検知日時、送信元・宛先情報、セキュリティインシデントの分析内容を容易に確認できるようにすること。
- セキュリティインシデントの危険度は、次の例を参考に４段階以上に分類すること。
  - 危険度３：　攻撃が成功しており、緊急事態であると判断したもの
  - 危険度２：　攻撃が成功した可能性が高いと判断したもの
  - 危険度１：　影響を受ける可能性は低いが、経過観察が必要と判断したもの
  - 危険度０：　問題がない通信ではないが、攻撃ではないと判断したもの
- 危険度が高いセキュリティインシデントが発生した場合においては、これを判断してから３０分以内に、本市運用担当者等へ電話により緊急連絡を行うこと。
- 新たな攻撃手法等に対して、個別のシグネチャ又はルールを作成すること。
- 検知精度を向上させるため、随時、検知ポリシーの見直しを検討し、本市と協議の上で、変更作業を実施すること。

㈡ 保守作業

- 本市からの保守に関する連絡及びこれに伴う対応は、２４時間３６５日受け付けること。
- 定期的な保守作業は、実施日、実施内容等をあらかじめ定めて実施すること。
- 緊急に必要な保守作業は、別途必要な調整を行った上で実施すること。
- 内部通信監視装置と接続する既設ネットワーク機器において障害等が発生した場合は、既設機器等事業者が実施する障害対応を受けて、内部通信監視サービスへの影響を確認し、必要に応じて復旧作業を行うこと。
- 導入した機器等の障害への対応とバージョンアップ等の変更への対応を実施すること。
- 保守作業に必要な機器やソフトウェア等を本市データセンターに持ち込む場合は、事前に本市と協議すること。

ａ　ハードウェア保守

- 本業務で導入するハードウェアの予防点検、部品交換等の保守作業を実施すること。

ｂ　ソフトウェア保守

・　シグネチャやパターンファイルは、開庁日に日に１回以上更新し、最新の脅威を検知できる環境を維持すること。
・　改良、機能強化等によるバージョンアップの情報を本市に提供し、本市と協議の上、実施の可否を決定し対応すること。
・　バージョンアップ等の情報提供、問合せ対応を実施すること。
・　本業務で導入するソフトウェアについては、パッチを含み、必要性を検証し、事前に本市の承認を得た上で、バージョンアップ及びパッチの適用を容易に行うことができること。

(ｳ) 技術的支援・問合せ対応

・　本市運用担当者等に対して、検知したセキュリティインシデントの解決に向けた技術的支援を行うこと。
・　本市からのメール等による問合せに対応すること。また、問合せ一覧表を作成し、問合せ内容、対応状況等を管理すること。

(ｴ) 障害対応

・　障害対応マニュアルに基づき対応すること。
・　緊急対応が必要な機器等の障害を検知した場合、直ちに、本市運用担当者等に対して障害発生連絡を行い、障害原因の調査・特定を行った上で、最善の方法等により復旧作業を行うこと。障害発生連絡後は、速やかに対応を開始する体制を整えること。
・　障害対応中は、随時、その作業状況を本市、関連する業務システム構築事業者等に報告すること。
・　障害復旧後、３日以内に、障害の発生内容（発生日時、場所、障害事象等）、対応内容（対応日時、原因等）を記述した障害報告書を作成し、本市、関連する業務システム構築事業者等に対して報告すること。

(ｵ) サービスレベルの維持

・　SLA に従って、サービス品質の維持に努めること。

(ｶ) 履行状況報告

・　月次で、SLA の達成状況、監視ポイントにおけるすべての通信を相関的に分析したレポート、実施した運用・保守作業等をまとめた履行状況報告書を作成し、本市に対して報告すること。報告は、原則として対面によること。

イ　その他

・　サービス提供期間中に、内部通信監視装置と接続する一部の既設ネットワーク機器において機器更改が予定されている。更改後の機器においても引き続き監視作業が行えるよう必要な対応を実施すること。
　➢　共通基盤スイッチ：　令和９年１月から更改後の機器で運用開始予定

⑶　履行期間を通じて実施する業務

すべての工程におけるプロジェクト管理（各作業の進捗状況の把握、課題・問題点の早期発見と解決策の検討、本市への迅速な状況報告等）を徹底すること。

報告等に係る各様式は、原則、契約締結後に本市が提供する雛形を使用するものとするが、必

要に応じて、本市と受注者で協議の上、内容の見直しを行う。

ア　実施計画書の作成

- 業務履行開始に当たり、契約締結日から１０日以内に広島市委託契約約款第６条に規定する実施計画書を作成し、本市の承認を得ること。
- 実施計画書には、作業方法、現場責任者の氏名・連絡先、作業実施体制（業務従事者の氏名・連絡先、役割分担、過去の業務従事実績を明記）及びスケジュールを明記すること。
- 実施計画書を変更する必要があるときは、本市の承認を得た上で計画を変更し、変更後の実施計画書を提出すること。
- 実施計画書は、原則として「実施計画書雛形」を使用すること。

イ　ＷＢＳ（ダブリュー・ビー・エス： Work Breakdown Structure）の作成

- 受注者は、実施計画書を本市が承認した後、速やかにＷＢＳを作成し提出すること。
- ＷＢＳは、原則として「ＷＢＳ雛形」を使用すること。

ウ　実施報告書等の作成

- 契約書に定める支払期終了時に、完了した業務の業務履行完了日、提出した成果物の一覧を記述した実施報告書を提出すること。
- 受注者は、準備期間中は、定期的（月１回以上）に本業務の進捗状況に関する報告書（以下「進捗報告書」という。）を作成した上で、進捗報告会で報告すること。
- 進捗報告書は、原則として「進捗報告書雛形」を使用すること。

エ　コミュニケーション管理

- 本業務を履行するに当たり、必要な会議体を提案し実施すること。
- 会議の実施に際しては、議事内容を事前に提示すること。
- 会議体以外に本市と受注者間でコミュニケーションを円滑にする方法があれば、提案し実施すること。

オ　議事録の作成

- 会議終了後は、受注者が議事録を作成し、速やかに提出すること。また、内容に疑義がある場合は、速やかに補正すること。
- 議事録は、原則として「議事録雛形」を使用すること。

カ　課題管理

- 会議体等で取り上げた課題については、議事録とは別に一覧（以下「課題管理表」という。）にまとめること。また、課題管理表は受注者が対応・回答すべきもの、本市が対応・回答すべきものに分け、それぞれ対応・回答期限を明記すること。

7　成果物

成果物の作成は、作成途中の原稿を随時提出するなど、本市と協議しながら行うこと。作成に当たり、本市の関係部署等と調整を行う必要が生じた場合には、本市と協議した上で、必要な資料を作成すること。

⑴　成果物の定義

本業務の成果物を次に示す。本仕様書で成果物として定義されていないドキュメント等については、契約締結後、本市と受注者で協議の上、成果物に含めるか否かを決定する。受注者は、必要に応じて、成果物の構成管理を行うこと。

なお、成果物は、本市と協議の上、統合又は分割してもよい。

ア　準備期間中の成果物

工程	成果物	内容	提出時期
概要設計	概要設計書	どのような機能が実装されるか等を記述した設計文書	工程終了後速やかに
詳細設計	詳細設計書	概要設計書に基づき、内部通信監視サービスの構築に必要となる具体的な仕様、運用等を記述した設計文書	工程終了後速やかに
	監視ネットワーク構成図	概要設計書に基づき、監視対象、監視ネットワーク等の構成を記述した文書	
	ハードウェア環境設定書	ハードウェアを稼動させるために必要な環境情報等を記述した文書	
	ソフトウェア環境設定書	ソフトウェアを稼動させるために必要な環境情報等を記述した文書	
テスト	システムテスト計画書	テストの位置付け、目的、テストケース（何をテストするかを定めたもの）の定義方法、テストツール、使用データ、スケジュール、体制等を記述した文書	工程終了後速やかに
	システムテスト仕様書	テストシナリオ、合格基準等を記述した文書	
	システムテスト結果報告書	テストの結果等を記述した文書	
	ユーザテスト計画書	テストの位置付け、目的、テストケース（何をテストするかを定めたもの）の定義方法、テストツール、使用データ、スケジュール、体制等を記述した文書	
	ユーザテスト仕様書	テストシナリオ、合格基準等を記述した文書	
	ユーザテスト結果報告書	テストの結果等を記述した文書	
その他	障害対応マニュアル	セキュリティインシデント、機器等の障害を検知した場合の対応手順等を記述した文書	サービス提供開始まで

イ　サービス提供期間中の成果物

工程	成果物	内容	提出時期
運用・保守	運用・保守計画書	運用・保守作業の実施計画（年間計画）、方法等を記述した文書	年次、月次、随時
	問合せ一覧表	本市からのメール等による問合せ内容、対応状況等を記述した文書	随時
	履行状況報告書	SLA の達成状況、監視ポイントにおけるすべての通信を相関的に分析したレポート、実施した運用・保守作業等を記述した文書	月次
	障害報告書	障害の発生内容（発生日時、場所、障害事象等）、対応内容（対応日時、原因等）等を記述した文書	随時（障害復旧後、３日以内）
	改版した設計書等	準備期間中に作成した設計書等を改版した文書	随時

ウ　その他履行期間中の成果物

工程	成果物	内容	提出時期
プロジェクト管理	実施計画書	プロジェクトの作業対象範囲、作業内容、成果物、作業スケジュール、推進体制等の具体的な事項等を記述した文書	契約締結後１０日以内
	ＷＢＳ	プロジェクト全体を細かい作業に分割した作業項目の工程表	実施計画書提出後速やかに
	進捗報告書	作業の予定・実績等の進捗状況等を記述した文書	随時
	議事録	各種会議の議事内容等を記述した文書	会議終了後速やかに
	課題管理表	課題の発生日・内容・対応状況等の課題の状況等を記述した文書	随時
	実施報告書	業務履行完了に当たり、実施結果等を記述した文書	契約書に定める支払期終了時

⑵　納品形態等

各成果物は、簡易製本の上、紙により提出するとともに、その電子データをＣＤ－Ｒ等、本市が別途指定する記録媒体により提出すること。ただし、紙による提出が難しいものについては、本市と受注者が協議の上、納品形態を決定する。

ア　用紙サイズ

用紙サイズは原則としてＡ４版とするが、必要に応じてＡ３版の使用も可とする。ただし、Ａ３版を使用した際は、見開きしやすいよう必ずＡ４版と同じ大きさに折りたたむこと。

イ　電子データの形態

各成果物は、Microsoft 社の Word、Excel、PowerPoint のいずれかの形式及びＰＤＦ形式（ＰＤＦファイル内の文字検索が可能なこと。）の２種類を提出すること。

８　留意事項

⑴　受注者に求める資格等

- ISO/IEC 9001（品質マネジメントシステム）若しくはこれに準ずる認証を取得していること、又はこれらと同等以上の品質管理が行える体制を整備していること。
- ISO/IEC 27001（情報セキュリティマネジメントシステム）若しくはこれに準ずる認証をしていること、又はこれらと同等以上のセキュリティ管理が行える体制を整備していること。

⑵　契約期間終了に伴う対応

- 本業務の契約が事由の如何を問わず終了する場合、受注者は本市の指示のもと、契約終了日までに被引継者への引継ぎを行うこと。
- 本市が後継サービスを構築する際は、本市が作成する移行計画のとおりに後継サービスへのデータ移行が行えるよう、受注者は、本市及び後継サービスの構築事業者に協力すること。
- ログ等のデータについては、本市と協議の上、可搬記録媒体等に保存し、本市に提出すること。
- 契約期間終了後は、特に取扱いを指定していないものを除き、本業務で導入したすべての機器を撤去すること。
- 機器の更新、機器の故障などでサーバやストレージ等の機器の情報を記録する媒体が不要となり、廃棄を行う場合は、重要な情報が外部に漏れることを防ぐため、媒体に保存されているデータを確実に消去し、完全に判読不能な状態にすること。
- 機器の更新、機器の故障、契約期間終了等により、媒体を物理的に破壊する場合は、媒体を本市データセンターから持ち出す前に、本市職員の立会いの上で物理的に破壊し、情報の復元が完全に不可能な状態にしてから廃棄すること。
- 機器の更新、機器の故障、契約期間終了等により、媒体を論理的に破壊する場合は、本市の様式である「電磁的記録媒体に関するリスクアセスメント票」に設置場所やディスクの暗号化の有無などの必要事項を記載して本市に提出するとともに、媒体内のデータに意味のないデータを上書きするなどにより完全に消去し、データ消去証明等を本市に提出すること。
- 廃棄に際しては、あらかじめ本市の承認を得ること。

⑶　その他

- 受注者は、業務の履行に際して、広島市情報セキュリティポリシーを遵守すること。
- 本仕様書に疑義があるとき、又は定めのない事項については、本市と受注者で協議の上、定めるものとする。