佐賀県公共ネットワーク監視サーバ
共通基盤移行・構築業務委託仕様書（案）

令和８年９月

佐賀県総務部行政デジタル推進課

目　次

第 1 章　総論

1.1　本業務の背景

佐賀県公共ネットワークにおいては、県庁に設置した現行仮想化基盤サーバ上に、ネットワーク監視サーバ、トラフィック収集サーバ及び Syslog/NTP サーバを仮想マシンとして稼働させ、ネットワーク機器等の死活監視、SNMP による監視、SNMP トラップの受信及びメール通知、トラフィック情報の収集・蓄積、Syslog の収集・保存並びに時刻同期を行っている。

これらの監視サーバについては、導入から 7 年が経過し、ハードウェア保守期限を迎えていることから、機器老朽化に伴う障害リスクの低減および安定した監視サービスの継続を図るため、監視サーバの更新を実施する必要がある。

更新に際しては、庁内情報システムの全体最適化の方針を踏まえ、新たな監視サーバを共通基盤上に構築するとともに、現行ネットワーク監視サーバと現行トラフィック収集サーバの機能を統合することとし、今回の構築業務委託を行う。

1.2　本調達の目的

本調達では、監視サーバの更新により信頼性及び可用性の向上を図り、佐賀県公共ネットワークの安定運用に資することを目的とする。

1.3　用語の定義

本書中に記載のある各種用語の定義は下表のとおり。

表 1.3　用語の定義

用語	説明等
公共ネットワーク	県庁、県現地機関、県立学校、市町等の施設を結ぶ佐賀県公共ネットワーク情報通信基盤をいう。
情報系ネットワーク	佐賀県が運用・管理する公共ネットワークのうち、県庁イントラネットを構成し、総務部行政デジタル推進課が運用・管理する LAN 及び WAN で、職員用のネットワーク PC が接続されているネットワークのこと。個人番号利用事務系（レベル 1）、個人番号関係事務系（レベル 2）及びインターネット接続業務系（レベル 3）の 3 つに論理分割されている。
幹線系施設	公共ネットワークにおいて本庁舎に接続し、支線系施設を配下に持つ以下の施設をいう。 佐賀土木事務所／唐津総合庁舎／伊万里総合庁舎／鳥栖総合庁舎／武雄総合庁舎
支線系施設	公共ネットワークにおいて本庁舎または幹線系施設に接続する施設をいう。主な施設種別は以下のとおり。 防災（支部）／防災（副支部）／県現地機関（防災）／消防本部／県現地機関（一般）／県立学校／市町／警察庁舎
重要拠点	障害発生を認識した場合には、24 時間 365 日で速やかな復旧を図る必要がある拠点をいう。

通常拠点	障害発生を認識した場合には、県庁開庁日の 8 時 30 分から 17 時 30 分で速やかな復旧を図る必要がある拠点をいう。
ネットワーク運用保守業者	公共ネットワーク（情報系ネットワークを含む）の運用・保守業務委託業者をいう。
共通基盤	個別に導入されたシステムを統合・集約することで、全体最適化された情報システム構成をとることを目的として整備したネットワーク基盤、仮想サーバ基盤及びストレージ基盤から構成される庁内情報システムの共通基盤をいう。
基盤運用保守業者	共通基盤の運用・保守業務委託業者をいう。

第 2 章　現行業務及びシステムの状況

2.1　現行業務の状況

現行の監視系サーバにより、公共ネットワークを構成するネットワーク機器等について、次の業務を行っている。

（1）　監視業務

ネットワーク機器等の死活監視（Ping 監視）、SNMP による状態監視及び性能監視、SNMP トラップの受信並びにイベント発生時のメール通知を行っている。

（2）　トラフィック情報の収集・蓄積業務

ネットワーク機器等のトラフィック情報の収集及び蓄積を行っている。

（3）　ログ収集・時刻同期業務

ネットワーク機器等から送信される Syslog の収集・保存を行うとともに、NTP サーバとして各機器への時刻同期を提供している。

2.2　現行システムの状況

現行システムの構成は次のとおり。

（1）　現行仮想化基盤サーバ

県庁に設置した物理サーバ（#1、#2）にハイパーバイザーを導入し、その上で各種監視系サーバを仮想マシンとして稼働させている。監視用 L2 スイッチ及び監視用 FW を経由して幹線 L3 スイッチに接続している。

（2）　現行ネットワーク監視サーバ

ネットワーク機器等の死活監視、SNMP による監視、SNMP トラップの受信及びメール通知を行っており、仮想マシンで動作している。監視ソフトウェアは SNMPc（株式会社ロジックベイン製）を使用している。

（3）　現行トラフィック収集サーバ

ネットワーク機器等のトラフィック情報の収集及び蓄積を行っており、仮想マシンで動作している。

（4）　現行 Syslog/NTP サーバ

ネットワーク機器等から送信される Syslog の収集・保存を行うとともに、時刻同期を提供する NTP サーバとしての機能を有し、仮想マシンで動作している。特定のログを検知した際に通知を行うためのスクリプトを実行している。

いずれのサーバも導入から 7 年が経過し、ハードウェア保守期限を迎えている。

第 3 章　本委託業務の概要

3.1　本業務の範囲

本調達の範囲は、下図「監視サーバ構築イメージ図」の赤線部分とし、監視サーバの構築に必要なソフトウェアの調達、サーバおよびネットワーク設計、構築、試験、切替を行うものとする。

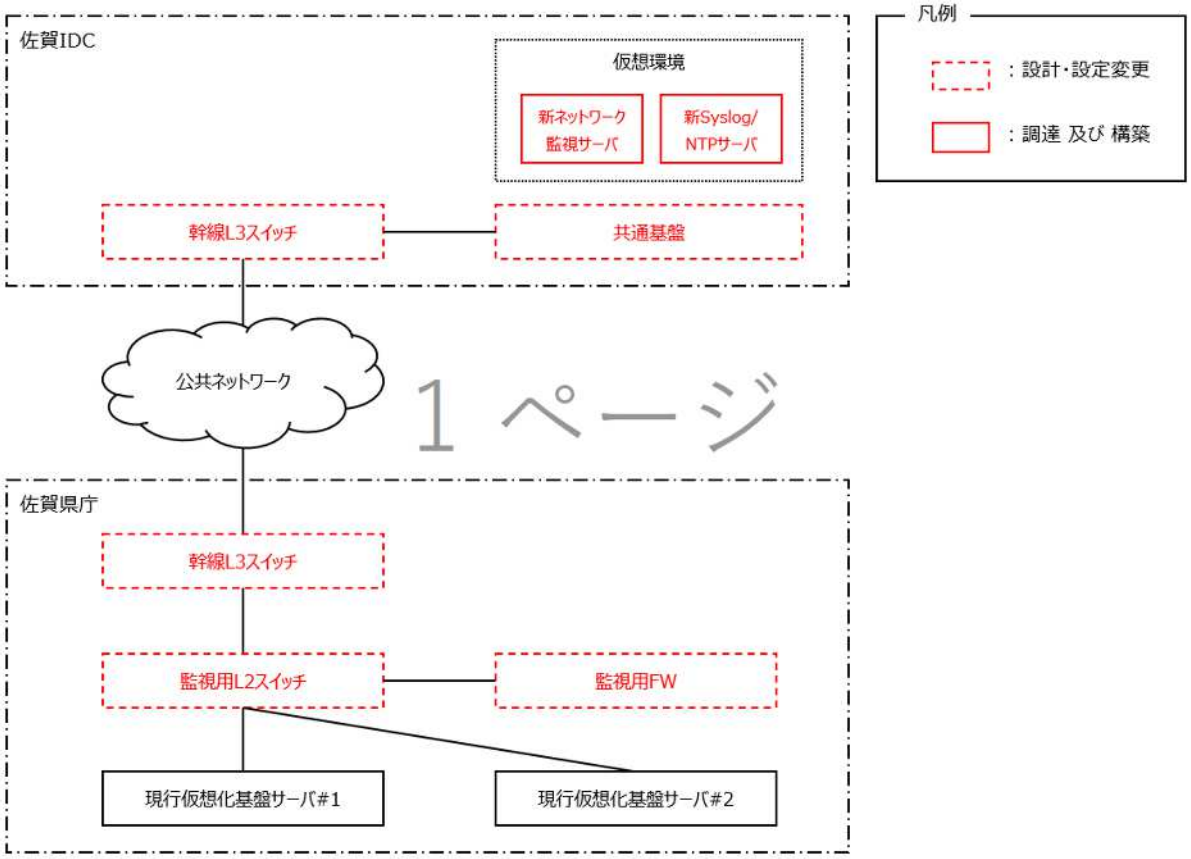

図 3-1　監視サーバ構築イメージ図（本委託業務の責任範囲）

本業務により新たに構築する対象は、次の 2 サーバとする。

- 新ネットワーク監視サーバ（現行ネットワーク監視サーバと現行トラフィック収集サーバの機能を統合）
- 新 Syslog/NTP サーバ

3.2　委託対象システム構成

3.2.1　ハードウェア

新ネットワーク監視サーバ及び新 Syslog/NTP サーバのハードウェアは、共通基盤から仮想マシンとして提供される。仮想マシンに割り当てる各リソース（vCPU、メモリ等）は、受託者が設計し、佐賀県を通じて基盤運用保守業者に仮想マシンの作成を依頼すること。

3.2.2 ソフトウェア

OS 及び各リソースは共通基盤から仮想マシンで提供され、バックアップ及びウイルス対策機能（仮想アプライアンスは除く）も共通基盤にて提供される。これら以外に必要となるソフトウェア等は、受託者にて用意すること。

ネットワーク監視ソフトウェアは、現行ネットワーク監視ソフトウェア（SNMPc：株式会社ロジックベイン製）の後継である「ThirdEye：株式会社ロジックベイン製」又はこれと同等以上の機能を有する製品を用意すること。詳細な要件は「4.1.2　ネットワーク監視ソフトウェア要件」に示す。

新 Syslog/NTP サーバの OS は、共通基盤で提供される Red Hat Enterprise Linux 9 を利用すること。

3.2.3 ネットワーク

新サーバを共通基盤で構築する際に公共ネットワークで必要となるネットワーク設計及び設定は、本業務の範囲で行うこと。共通基盤側で必要となるネットワーク設計・設定については、佐賀県を通じて基盤運用保守業者に依頼すること。

現行サーバと新サーバを平行稼働させる場合は、必要なネットワーク設計及び設定（IP アドレス、SNMP トラップ、コミュニティ名等）を行うこと。また、ネットワーク運用業者又は基盤運用保守業者にネットワーク等の設計・設定変更を依頼する場合の費用は、受託者にて負担すること。

3.3 委託作業

本業務における委託作業は次のとおり。その詳細は第 5 章で示す。

3.3.1 システム要件定義フェーズ

共通基盤上への監視サーバ構築に向け、現行システムの構成及び設定を分析のうえ、新サーバに必要となるリソース要件、ネットワーク要件及び機能要件を整理する。

3.3.2 設計フェーズ

システム要件定義フェーズの成果物をもとに、サーバ及びネットワークの設計を行い、パラメータシート、物理構成図及び論理構成図を作成する。

3.3.3 構築フェーズ

設計フェーズの成果物をもとに、監視ソフトウェアの調達、共通基盤上でのサーバ構築及び各種設定を行う。

3.3.4 試験フェーズ

本番ネットワーク接続までに十分な試験を行い、設計フェーズの成果物のとおりの動きをすることを確認する。

3.3.5　移行フェーズ

現行サーバから新サーバへの切替を行い、業務支障や監視への影響を最小限にしたうえで、県の了承を受ける。

3.4　スケジュール

委託期間は、契約締結の日から令和９年３月 31 日までとする。当該期間内に全工程を終了し、全成果物を納品して、県の承認を受けること。

フェーズ	2025（令和８）年				2026（令和９）年		
	９月	１０月	１１月	１２月	１月	２月	３月
現行システム運用							
要件定義フェーズ							
設計フェーズ							
構築・試験フェーズ							
移行フェーズ							
新システム運用							

図 3-2　スケジュール（想定）

第４章　委託対象システムの詳細要件

4.1　機能要件

4.1.1　共通要件

ア　新ネットワーク監視サーバおよび新 Syslog/NTP サーバは、共通基盤上に構築を行うこと。

イ　共通基盤では、OS および各リソース（vCPU、メモリ）を仮想マシンで提供するため、それ以外に必要なソフトウェア等は、受託者にて用意すること。

ウ　バックアップおよびウイルス対策機能（仮想アプライアンスは除く）は、共通基盤にて提供される。

エ　受託者は新ネットワーク監視サーバおよび新 Syslog/NTP サーバで必要となる各リソースを設計し、佐賀県を通じて基盤運用保守業者に仮想マシンの作成および共通基盤で必要なネットワーク設計・設定を依頼すること。

オ　新サーバを共通基盤で構築する際に公共ネットワークで必要なネットワーク設計、設定を行うこと。

カ　現行サーバと新サーバを平行稼働させる場合は、必要なネットワーク設計および設定（IP アドレス、SNMP トラップ、コミュニティ名等）を行うこと。

キ　ネットワーク運用業者または、基盤運用保守業者にネットワーク等の設計・設定変更を依頼する場合の費用は受託者にて負担すること。

ク　現行ネットワーク監視サーバと現行トラフィック収集サーバの機能を統合して、新ネットワーク監視サーバとして構築すること。

ケ　新ネットワーク監視サーバ自身の監視は、共通基盤の監視を利用すること。

4.1.2　ネットワーク監視ソフトウェア要件

ネットワーク監視ソフトウェアは、「ThirdEye：株式会社ロジックベイン製」又はこれと同等以上の機能を有する製品を用意することとし、次の要件を満たすこと。

ア　VMWare ESXi 8.0 以上に対応していること。

イ　ネットワーク機器等の死活監視（Ping 監視）が可能であること。

ウ　SNMPv2c 及び SNMPv3 に対応し、ネットワーク機器の状態監視及び性能監視が可能であること。

エ　SNMP トラップを受信し、イベントの記録及び通知が可能であること。

オ　標準 MIB に加え、ベンダー独自の拡張 MIB を利用した SNMP 監視が可能であること。

カ　SNMP を用いて、監視対象機器に装着された光トランシーバ（SFP／SFP＋等）のデジタル光監視（DOM／DDM）情報（光送信レベル（Tx）、光受信レベル（Rx）、モジュール温度、電源電圧及びバイアス電流）を収集できること。

キ　光レベル監視においては、CISCO-ENTITY-SENSOR-MIB（entSensorValue 等）をはじめとする各ベンダーの拡張 MIB に対応し、取得値のスケール変換及びポート（インタフェース）との対応付けを行ったうえで、値をグラフ表示及び履歴管理できること。

ク　光送信レベル（Tx）及び光受信レベル（Rx）について、任意のしきい値を%などの数値で設定でき、しきい値を超過した場合に、指定するメールアドレス宛への通知及びイベント記録が可能であること。

ケ　光レベルの監視対象は、少なくとも次に掲げる機器及び光トランシーバとし、対象拠点（幹線系施設及び支線系施設）に応じて監視項目を設定できること。

（対象機器の例）Cisco Catalyst 9500／9300／9200L シリーズ 等

（対象光トランシーバの例）SFP-10G-SR／LR／ER／ZR、GLC-SX-MMD 等（DOM 対応品）。ただし GLC-TE 等の銅 SFP 及び AOC は対象外とする。

コ　監視ソフトウェア標準の機能で DOM 監視が実装できない場合は、テンプレート化した SNMP 監視項目の作成等により同等の監視を実現できること。この場合においても、ライセンス数は監視項目数ではなく監視対象機器数に基づき算定されること。

サ　CPU 使用率、メモリ使用率、インタフェース帯域使用率等の性能情報を収集し、グラフ表示及び履歴管理が可能であること。

シ　異常を検知した場合、指定したメールアドレス宛に自動でメール通知ができること。また、通知条件及び通知内容を設定可能であること。

ス　2,000 ノード以上のデバイスを監視対象として設定できること。また、1 ノードに対して複数の監視項目(Ping、CPU、メモリ、トラフィック等)を設定する場合においても、ライセンス数は監視項目数ではなく監視対象機器数に基づき算定されること。

セ　監視対象機器の状態及び接続関係を視覚的に把握できるマップ機能及びダッシュボード機能を有すること。

ソ　監視対象機器の追加、削除及び監視設定の変更をGUIにより容易に実施できること。

タ　監視対象機器を選択し、監視画面上からターミナル(TeraTerm等)を起動できること。

チ　マップ機能において、任意の画像を背景に設定可能なこと。また、背景画像の任意の位置にアイコンを配置可能なこと。

ツ　監視対象機器の自動検出機能を有し、監視対象の登録作業を効率化できること。

テ　対象拠点をツリー表示で任意のグループに分けることが可能なこと。

ト　正常な機器のアイコン色(例：緑色)と異常が発生している機器のアイコン色(例：赤色)のように、機器の状態が色で判別できる機能をもつこと。

ナ　特定のベンダーに依存せず、マルチベンダーのネットワーク機器等を監視対象として管理できること。

ニ　Cisco、Alaxala、Aruba、Fortinet等の機器コンフィグレーション情報を自動的に取得及びバックアップできること。また、取得したコンフィグレーション情報について、世代管理及び変更履歴管理を行い、差分比較が可能であること。

ヌ　監視データ及びイベントログを保存し、障害発生時の調査及び分析に利用できること。

ネ　監視ソフトウェアの設定情報、監視対象情報及び監視履歴について、バックアップ及び復元が可能であること。

ノ　バックアップにおいては、テンプレート化したコマンド(showコマンド等)を監視画面上から投入可能なこと。また、スケジュール設定等により、任意のタイミングで実行可能なこと。

ハ　5年間のメーカサポートが受けられること。また、メーカサポート期間中は、ヒ～への対応が可能であること。なお、サポート受付時間は平日9-17時以上とする。

ヒ　無制限の問い合わせ対応が行えること。

フ　バグや脆弱性の修正に関するサポートを受けられること。

ヘ　アップグレードのためのアップデートファイルを無償で提供できること。

4.1.3　ネットワーク監視サーバ構築要件

新ネットワーク監視サーバについては、現行監視機能の移行に加え、DOM／DDMに対応したSFP等の光トランシーバに係る光レベル監視を実装するものとし、次の要件を満たすこと。

ア　現行ネットワーク監視サーバに登録されているすべての機器及び監視項目（Ping、SNMP等）を登録すること。

イ　現行のトラフィック収集サーバに登録されているすべての機器のトラフィック情報を収集する設定を行うこと。

ウ　障害発生時の影響が特に大きい機器については、CPU使用率、メモリ使用率、インタフェース状態、インタフェース帯域使用率等の情報を収集する設定を行うこと。

エ　県庁を含む幹線系施設及びその配下の支線系施設ごとにグループ化を行うこと。

オ　異常を検知した場合に、県が指定するメールアドレス宛に通知する設定を行うこと。

カ　コンフィグレーション情報のバックアップが取得可能な機器について、バックアップ設定を行うこと。バックアップは毎月1回以上、3世代以上分を管理できるようにすること。

キ　対象拠点の保守区分（重要拠点、通常拠点）がメール通知で分かるように設定を行うこと。

ク　新Syslog/NTPサーバと時刻同期をさせること。

ケ　監視サーバには、Webブラウザを用いてアクセスできるようにすること。

コ　監視対象機器のうち、DOM／DDMに対応したSFP等の光トランシーバを搭載し、SNMPによりDOM情報を取得可能な機器を調査し、DOM監視対象として整理すること。

サ　DOM監視対象について、機器名、設置拠点、インタフェース名、接続先、光トランシーバ型番、取得対象項目、MIB・OID、ポーリング間隔、しきい値、通知条件、グラフ表示項目及び履歴保存条件をパラメータシートに整理すること。

シ　障害発生時の影響が特に大きい幹線系又は重要拠点の光リンクについては、受信光レベル（Rx）及び送信光レベル（Tx）の監視を優先して設定すること。

ス　DOM情報を取得できない機器、非対応の光トランシーバ、銅線系SFP、メディアコンバータ等については、その理由を整理し、Ping監視、インタフェース状態監視、トラフィック監視又はログ監視等の代替監視方法を県と協議のうえ設定すること。

セ　DOM監視に係るしきい値は、光トランシーバの仕様、機器から取得される警告値・障害値、現行運用で把握している正常時の実測値等を踏まえ、県と協議のうえ設定すること。

ソ　DOM監視に係る異常通知については、対象拠点、機器名、インタフェース名、取得項目、取得値、しきい値、発生時刻及び保守区分を把握できる通知内容とすること。

4.1.4　Syslog/NTPサーバ構築要件

ア　OSは共通基盤で提供されるRed Hat Enterprise Linux 9を利用すること。

イ　シスログ機能にはrsyslogを使用すること。

ウ　NTP機能にはchronyを使用すること。

エ　rsyslogの設定は現行Syslogサーバの設定を踏襲し、各機器から送信されるログ情報を適切に受信できるようにすること。

オ　現行Syslogサーバでは、特定のログを検知した際に通知を行うためのスクリプトを実行している。新Syslogサーバにおいても、当該機能を引き継ぐこと。なお、新ネットワーク監視サーバで同等の機能を提供できる場合は、当該サーバで実装しても問題ない。

カ　ログ情報は、1年間分を保存できるようにすること。

キ　chronyの設定は、現行NTPサーバの設定を踏襲し、各機器が正常に時刻同期できるようにすること。

ク　DOM監視に係るイベント又は通知をSyslog等で連携する場合は、ログ受信、保存、検索及び通知の運用に支障がないよう設定すること。

4.2　その他

（1）　作業にあたっては、現行のネットワーク監視業務に支障が出ないようにすること。

（2） 現行サーバと新サーバを平行稼働させる場合は、既存ネットワークやその他のシステムに影響を及ぼさないようにすること。

（3） 新ネットワーク監視サーバ自身の監視は、共通基盤の監視を利用すること。

（4） DOM 監視の設定又は試験にあたり、本番機器に対する設定変更、SNMP 設定変更、MIB 取得又はポーリング増加を伴う場合は、事前に影響範囲を整理し、県の承諾を得たうえで実施すること。

第 5 章　委託作業における詳細要件

5.1　システム要件定義フェーズ

「3.3.1　システム要件定義フェーズ」及び「4.1　機能要件」に基づき各種要件を整理すること。

本業務は共通基盤を利用することから、共通基盤の概要や提供機能・サービス内容を把握のうえ、新ネットワーク監視サーバ及び新 Syslog/NTP サーバで必要となる各リソース（vCPU、メモリ等）並びに共通基盤で必要となるネットワーク要件を整理し、佐賀県を通じて基盤運用保守業者に仮想マシンの作成及び設定を依頼すること。

また、DOM 監視については、監視対象候補となる機器、光トランシーバ、インタフェース、取得可能な DOM 項目、利用する MIB・OID、想定ポーリング間隔、通知要否及び取得不可時の代替監視方法を整理すること。

5.2　設計フェーズ

システム要件定義フェーズの成果をもとに、サーバ設計及びネットワーク設計を行い、パラメータシート、物理構成図及び論理構成図を作成すること。

新サーバを共通基盤で構築する際に公共ネットワークで必要なネットワーク設計を行うとともに、現行サーバと新サーバを平行稼働させる場合は、IP アドレス、SNMP トラップ、コミュニティ名等の設計を併せて行うこと。

DOM 監視を行う機器については、監視対象インタフェース、取得対象 DOM 情報、利用 MIB・OID、ポーリング間隔、しきい値、通知条件、グラフ表示、履歴保存及び取得不可時の代替監視に関する設計を行うこと。

5.3　構築フェーズ

設計フェーズの成果物をもとに、ネットワーク監視ソフトウェアの調達及び導入、共通基盤上でのサーバ構築並びに「4.1.3　ネットワーク監視サーバ構築要件」及び「4.1.4　Syslog/NTP サーバ構築要件」に示す各種設定を行うこと。

ア　DOM 監視対象機器について、SNMP により DOM 情報を取得できるよう、必要な MIB 定義、OID 監視項目、テンプレート、ポーリング設定、グラフ表示設定及び履歴保存設定を行うこと。

イ　DOM 監視に係るしきい値及び通知条件は、設計フェーズで県と合意した内容に基づき設定すること。

ウ　ネットワーク運用保守業者又は基盤運用保守業者への設計・設定変更の依頼が必要となる場合は、事前に県担当者へ報告を行い、必要な作業調整を行うこと。なお、当該依頼に係る費用は受託者にて負担すること。

5.4　試験フェーズ

5.4.1　試験計画書の作成

実施する試験について、試験内容を記載した「試験計画書」及び「試験手順書兼成績書」を作成し、県の承諾を得ること。DOM 監視に係る試験については、取得試験、表示試験、履歴保存試験、しきい値通知試験及び取得不可時の代替監視確認を含めること。

5.4.2　試験実施要件

ア　各サーバは、本番ネットワーク接続までに十分な試験を行うこと。なお、試験内容については、「試験計画書」及び「試験手順書兼成績書」を作成して、県の承諾を得ること。

イ　現行サーバと新サーバを平行稼働させる場合は、既存ネットワークやその他のシステムに影響を及ぼさないようにすること。

ウ　DOM 監視対象として設定した機器について、SNMP により DOM 情報が取得できること、取得値が監視画面及びグラフに表示されること、履歴として保存されることを確認すること。

エ　DOM 情報のしきい値超過又は異常イベントについて、イベント記録及びメール通知が設計どおりに行われることを確認すること。

オ　DOM 情報を取得できない機器又は対象外とした光トランシーバについては、取得不可理由及び代替監視方法がパラメータシート又は DOM 監視設計一覧に整理されていることを確認すること。

5.5　移行フェーズ

5.5.1　切替

ア　現行サーバから新サーバに切替を行う場合は、業務支障や監視への影響を最小限にすること。なお、万が一、切替時に業務支障を伴う場合は、事前に影響範囲、停止時間等を県に説明のうえ、了承を得たうえで実施すること。

イ　現行サーバから新サーバへの切替において、「移行計画書」を作成のうえ、県の了承を得ること。

ウ　DOM 監視については、切替後に監視対象機器の DOM 情報取得、グラフ表示、履歴保存及び通知設定が継続して有効であることを確認すること。

5.5.2　マニュアルの作成およびネットワーク運用保守業者への教育

ア　各サーバの機器操作マニュアル及び運用保守マニュアルを作成すること。

イ　各サーバのマニュアルをもとに、ネットワーク運用保守業者に実機を用いた説明会を行うこと。また、ネットワーク運用保守業者からマニュアルの追記や修正を求められた場合は、可能な限り応じること。

ウ　DOM 監視に係る画面確認方法、グラフ確認方法、しきい値変更方法、通知確認方法及び取得不可時の一次切り分け方法を運用保守マニュアルに記載し、ネットワーク運用保守業者への説明に含めること。

5.5.3　その他

本サーバの運用・保守業務は、ネットワーク運用保守業者が実施する。運用において必要な事項については、事前に県及びネットワーク運用保守業者にもれなく引き継ぐこと。

第 6 章　委託業務遂行に関する要件

6.1　プロジェクト管理

6.1.1　プロジェクト管理方法

ＰＭＢＯＫ（Project Management Body of Knowledge）など、世界的にも標準手法として認知されているプロジェクト管理方法を用いること。

6.1.2　プロジェクト基礎データの収集報告方法

プロジェクトの進捗・品質を担保するために必要な基礎データを明確にし、その取得方法、報告方法について県と合意した上収集すること。県に対する報告は収集した基礎データをもとに行うこと。

6.2　体制及び要員に関する要件

6.2.1　プロジェクト体制

ア　本業務に遂行に関するプロジェクト実施体制を敷くこと。

イ　外部組織、協力会社などが存在する場合、その関係、役割、作業分担、責任範囲及び指揮系統を明確にすること。

ウ　DOM 監視の設計及び設定に必要な SNMP、MIB、Cisco 等ネットワーク機器及び光トランシーバに関する知識を有する要員を配置すること。

6.2.2　要員計画

本業務を遂行するために、プロジェクトマネージャーを 1 人割り当てること。

プロジェクト要員を計画し、要員の情報(プロフィール情報、スキル情報、参画期間、経験情報)を明確にすること。

6.3　打合せ・報告に関する要件

受託者は、本業務のスケジュール等に十分配慮し、県との打合せ・報告等を主体的に行うこと。

新サーバの構築にあたっては、県、ネットワーク運用保守業者及び基盤運用保守業者と十分協議のうえ業務を進めること。また、切替時に業務支障を伴う場合は、事前に影響範囲、停止時間等を県に説明のうえ、了承を得たうえで実施すること。

DOM監視対象、しきい値、通知条件、取得不可時の代替監視方法及び運用引継ぎ内容については、設計フェーズ及び試験フェーズにおいて県と協議し、合意内容を議事録又は設計資料に記録すること。

6.4 セキュリティに関する要件

6.4.1 資料及びデータの取り扱い

ア 本業務を実施するにあたり必要と思われる資料及びデータの提供は、県が妥当と判断する範囲で行う。

イ 受託者は県から提供された資料及びデータを、本業務を実施する目的のみに用いるものとし、県の許可なくして複写又は複製してはならない。

ウ 受託者は業務終了後、県から提供された全ての資料及びデータを県に返却すること。

エ 契約の終了時のほか、保存されたデータを別のシステムに移行する必要が発生する場合は、サーバ上に保存されたデータについて、汎用性のあるデータ形式に変換し、当該データ構造と項目の説明資料を付して提供すること。その際、県から説明を求められる場合は誠意をもって対応すること。

オ 上記に限らず保存データをシステムから取り出す場合は、一時的なものも含めて、不要になった記憶媒体上のデータは復元できないよう除去し、（求めに応じて）、その結果を県に書面で報告すること。なお、実施方法等の詳細については、県と協議するものとする。

6.4.2 資料及びデータの取り扱い

ア 作業員の管理

- 本プロジェクトのプロジェクトマネージャは本プロジェクトに関する資料及びデータを取り扱う作業員を限定し、適切に管理すること。
- 本プロジェクトに関する資料及びデータを取り扱う作業環境（庁内の指定された作業場所や受託者のプロジェクトルーム等）に入退場する作業員を適切に管理し、第三者への情報漏洩を防ぐこと。

イ 作業端末のセキュリティ

- 本プロジェクトに関するデータを取り扱う作業端末がウイルス対策ソフトの導入やセキュリティパッチの適用など、適切なセキュリティ対策が施されていること。
- 本プロジェクトに関するデータを取り扱う作業端末が情報漏洩リスクのあるソフトウェア（ウィニーなどのP2Pファイル共有ソフトウェアなど）をインストールしていないこと。
- 本プロジェクトに関するデータを取り扱う作業端末上で、データへのアクセス権限の設定や作業員のアクセスログを取るなどの工夫を行い、適切な作業員のみが同データにアクセスしていることを確認できるよう管理すること。
- 本プロジェクトに関するデータを取り扱う作業端末は、ほかの用務での使用は行わないこととし、原則設置場所を固定すること。

6.5　本委託業務の納品物

6.5.1　納品物の内容

表 6-1 に記すものを県が示す期限までに納品すること。内容は県担当者と協議し、承認を得たものを提出すること。

表 6-1　成果物一覧

フェーズ	成果物	内容
設計	パラメータシート	新ネットワーク監視サーバ、新 Syslog/NTP サーバの設定情報を整理したもの。DOM 監視対象がある場合は、DOM 監視設定情報を含めること。
設計	物理構成図	本業務で構築するサーバ及び関連機器の物理構成を示したもの。
設計	論理構成図	本業務で構築するサーバ及び関連機器の論理構成を示したもの。
試験	試験計画書	試験方針、実施内容及び実施理由を定義した計画書。DOM 監視に係る取得、表示、履歴保存、しきい値通知及び代替監視確認を含めること。
試験	試験手順書兼成績書	試験の手順及び実施結果をまとめたもの。DOM 監視の取得結果、画面表示結果、通知試験結果及び取得不可時の確認結果を含めること。
移行	移行計画書	現行サーバから新サーバへの切替に係る計画。DOM 監視設定の移行又は新規設定確認を含めること。
移行	機器操作マニュアル	各サーバの機器操作手順をまとめたもの。
移行	運用保守マニュアル	各サーバの運用保守手順をまとめたもの。DOM 監視の確認方法、しきい値変更方法、通知確認方法及び一次切り分け方法を含めること。

6.5.2　形式等

納品図書については、電子媒体に記録したもの（PDF 形式及び PDF 変換前の編集可能な Microsoft Office 等のデータ形式の 2 種類）を納品すること。

6.5.3　納品場所

佐賀県庁新館 6 階　行政デジタル推進課（佐賀県佐賀市城内 1 丁目 1 番 59 号）

第 7 章　その他

7.1　知的財産権の帰属等

知的財産権等については、委託契約書による。

7.2　機密保持

（1）　受注者は、個人情報等の管理を適正かつ厳格に行うこと。

（2）　受託者は、本業務において知り得た業務上の情報を履行期間中、委託の終了又は解除後を問わず、佐賀県の承認なしに第三者に開示または洩してはならない。

（3） 佐賀県が施設外への持ち出しを認めない資料については、施設内にて閲覧を行うこと。

7.3 情報セキュリティに関する受託者の責任

受託者は、佐賀県のホームページに公開している「佐賀県情報セキュリティ基本方針」を遵守すること。なお、個人情報の扱いについては、別記「個人情報取扱特記事項」を遵守すること。

また、脆弱性の監視を行い、新たな脆弱性が確認された際には、県と相談のうえ、速やかに対応を行うこと。本委託業務の報告書等の納品の前に既知の脆弱性診断を行い、問題を解消したうえで納品すること。

DOM 監視に必要な SNMP 設定、コミュニティ名、認証情報、MIB 情報及び監視設定情報については、情報セキュリティ上適切に管理し、不要な範囲への開示を行わないこと。

7.4 契約不適合責任

納入成果物が本仕様書に適合しない旨の県からの通知があった場合には、受託者の責任及び負担において、県が相当と認める期日までに補修を完了するものとする。

7.5 法令等の遵守

（1） 受託者は、民法（明治 29 年法律第 89 号）、刑法（明治 40 年法律第 45 号）、著作権法、不正アクセス行為の禁止等に関する法律（平成 11 年法律第 128 号）等の関係法規を遵守すること。

（2） 受託者は、個人情報の保護に関する法律（平成 15 年法律第 57 号）及び受託者が定めた個人情報保護に関するガイドライン等を遵守し、個人情報を適正に取り扱うこと。

7.6 その他

（1） 本仕様書に記載のない事項については、佐賀県と受託者とが十分に協議を行い決定するものとする。

（2） 本業務を佐賀県の許可なく再委託することは禁止する。

以上