市町村立学校向け県業務システム接続用
ネットワーク構築及び運用保守管理業務委託
仕様書

令 和 ７ 年 ３ 月

山形県教育委員会

１　委託業務の名称

市町村立学校向け県業務システム接続用ネットワーク構築及び運用保守管理業務委託

２　委託期間

（構築期間）契約締結日から令和７年 12 月 31 日まで

（運用保守期間）令和８年１月１日から令和 12 年３月 31 日まで

３　委託業務の概要

市町村立小中学校（以下、「学校」という。）に勤務する県費負担教職員の給与及び旅費事務については県の給与等システム及び財務会計システム（以下、「県業務システム」という。）により管理・執行している。平成 25 年度まで、県業務システムを利用する場合は、学校事務職員が４校に１校の割合で設置されている県専用端末設置校へ出張し自校分のデータ入力作業を行っており、県専用端末不足に起因する学校事務職員の入力作業負荷が大きな課題となっていた。

また、給与明細等の県庁で一括出力される帳票については、県教育事務所経由で各市町村教育委員会等へ郵送したうえで、市町村教育委員会等が更に学校へ配送するか、学校職員が受け取りに出向いている状況であり、紙ベースでの帳票事務は県職員及び学校職員の大きな負担となっていた。

そこで、平成 26 年度より行われた給与等システムの再構築により、従来は県庁で一括出力し配送していた帳票をネットワーク経由で各学校へ配信する機能が追加されたのに併せ、SSL-VPN 装置等を導入し各学校が県業務システムへ直接アクセス可能なネットワークを構築することで、データ入力作業や帳票出力作業を各学校から行える環境を整備し、前述の課題解決を図ったところである。

この構築されたネットワークについて、令和８年１月から導入機器のメーカー保守等が行われなくなる。このため、SSL-VPN 装置等の機器更新等を行い、システムの再構築を行うのに加え、安定した稼働を図るため、運用保守管理業務を行うものである。

４　委託業務の内容

本委託業務は、各学校に市町村が設置している端末とインターネット接続環境を利用し、山形県基幹高速通信ネットワーク（以下、「基幹ネットワーク」という。）経由で県業務システムにセキュアにアクセス可能なネットワークを構築するとともに、各学校への展開を行うものである。

構築にあたっては、各学校の端末やインターネット接続環境について事前に十分な調査を実施した上で、全ての学校が接続可能なように適切なネットワーク設計を行うこと。

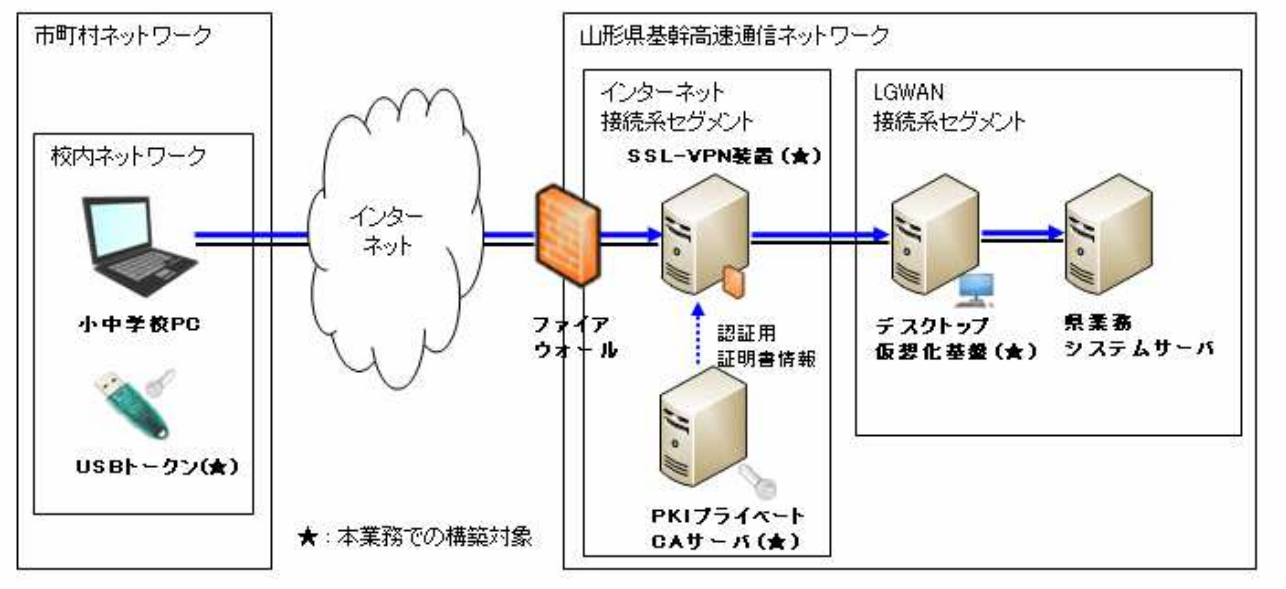
また、多種多様な環境にある各学校において遅滞なく接続するための様々な接続パターンやＱ＆Ａを網羅した接続手順書及び操作マニュアル（以下、「マニュアル」という。）を作成すること。

更に、各学校へのネットワーク展開前に説明会を開催し学校事務職員への十分な情報提供、接続試験期間中の問合せ対応や接続不良校への対策作業等の導入支援作業も業務委託内容となる。

また、保守運用管理にあたっては、ネットワークを適切に維持するために、ネットワーク機器の維持保守管理を行うとともに、県からの問い合わせ対応等ネットワークの運用保守管理業務を行うこと。

(1)　ネットワークシステムの構築及び接続支援

構築するネットワークシステムの概要は以下のとおり



（全体構成図）

学校に市町村が設置している端末とインターネット接続環境を利用し、基幹ネットワーク経由で県業務システムサーバへのアクセス環境を構築する。

インターネットを介した学校端末から基幹ネットワークへの通信には SSL-VPN 装置を導入し SSL-VPN 通信を採用することで、セキュアで安全な通信経路を確立する。

SSL-VPN 通信を確立する際の認証は電子証明書を利用した認証方式とし、電子証明書は物理デバイス（USB トークン）にセキュアに格納することで PIN 番号（暗証番号）と物理デバイス（USB トークン）による二因子認証の仕組みを採用する。

電子証明書の発行や失効管理は PKI プライベート CA サーバを構築し証明書を管理し、SSL-VPN 装置と連携し証明書の登録・失効管理を実施すること。

SSL-VPN 装置を配備するインターネット系セグメントからは、LGWAN 接続系セグメントに配備された県業務システムサーバへ直接アクセスできない。このため、LGWAN 接続系セグメントにデスクトップ仮想化基盤を導入し、学校端末が SSL-VPN 通信の確立後、デスクトップ仮想化基盤で稼働する Windows Server のリモートデスクトップ機能経由で県業務システムを利用できる構成とする。なお、県業務システムはクライアント OS を Windows とする仕様であるため、デスクトップ仮想化基盤上のリモートデスクトップ機能は、Windows Server のリモートデスクトップサービスによって実現することを想定している。必要となる仮想サーバ等をデスクトップ仮想化基盤に構築すること。

利用にあたっては極力、クライアントにソフトをインストールすることなく、既存の Web ブラウザ（主に Microsoft Edge）のみでの利用が可能なこと。

なお、② 構築作業要件 の「(参考) 各学校の端末・インターネット接続環境の概要」の内容に基づき、利用ユーザ数は 350、同時利用可能ユーザ数は 150 を想定している。

① 導入機器

ネットワークシステム構築のために受託者が導入する機器及び数量等は次のとおりとする。

＜県が買取とし保守が必要な物品＞ ※ 保守サービスレベルは平日の日中時間帯(9:00～17:00)とする

ア SSL-VPN 装置（１式）

- SSL-VPN 接続機能を提供できること。
- SSL-VPN 接続時に、端末の OS の種類やバージョン、セキュリティ対策ソフトの種類やウィルス定義ファイルの更新日付等で接続可否を管理できること。
- SSL-VPN 接続時に発生したキャッシュやダウンロードファイルを接続終了時に一括して削除させることで情報漏えいを防止する機能を有すること。
- 電源ユニット等の搭載部品について冗長化構成が可能であること。
- 委託期間中有効な SSL 用サーバ証明書を購入すること。
- その他の仕様は「別紙１ SSL-VPN 装置仕様」のとおり。

イ PKI プライベート CA サーバ（１式）

- 自組織内で認証局の運営・管理機能を提供できること。
- 証明書の要求・作成・失効・有効期限切れまでの証明書ライフサイクル全体を管理できること。
- 認証局は厳重に管理できる機能を有すること。例えば、管理者の利用は専用の USB トークンを利用し二因子認証以上の認証を経て許可されること。
- 管理者の操作履歴は全て記録され削除できないこと。
- 現環境で発行された証明書を継続利用できるようにするため、導入に際しては現在稼働中の PKI プライベート CA サーバ(JCCH・セキュリティ・ソリューション・システムズ社製「Gleas」)からの証明書データ移行をおこなうこと。
- その他の仕様は「別紙２ PKI プライベート CA サーバ仕様」のとおり。

ウ デスクトップ仮想化基盤（１式）

- Windows Server のリモートデスクトップサービスによるリモートデスクトップ機能を提供できること。なお、Windows Server については、適宜ウィルス対策を施すこと。
- 電源ユニット等の搭載部品について冗長化構成が可能であること。
- その他の仕様は「別紙３ デスクトップ仮想化基盤仕様」のとおり。

エ ネットワークセキュリティパッケージ（１式）

- ログ監視サービスを提供できること。
- ログ監視サービスに対応するために必要な UTM およびライセンスを提供すること。
- UTM 故障時、現地対応による保守を行えること。
- その他の仕様は「別紙４ ネットワークセキュリティパッケージ仕様」のとおり。

＜県が買取とし保守が不要な物品＞

オ USB トークン（50 本）

- USB 端子を有し、電子証明書を格納でき高度な暗号アルゴリズムによる認証機能を有し

ていること。

- 耐タンパー性を有し、米国 FIPS 140-2Level3 認証を取得している製品であること
- RSA 公開鍵暗号方式について 2048 ビット鍵長に対応していること。また楕円曲線暗号方式にも対応が可能なものであること。
- 端末の OS が Windows 11 の場合、ミドルウエアやドライバ等のソフトウェアは自動でインストールされること。
- 本件で導入する認証局との連携が可能なこと。
- 現在県が保有する Safenet eToken5110 と互換可能であること

② 構築作業要件

主な作業要件は下記のとおり。

ア 事前調査

学校の端末・インターネット接続環境、県業務システムのネットワーク設計情報等について事前調査を行うこと。

- 調査の実施は県が行うが、調査票の作成や調査結果の集計・分析作業を行う
- 調査の結果、端末やインターネット接続環境に問題がある場合には解決策を提示すること（問題を解決するための設定変更費用は県の負担を予定している）
- 調査や問題解決のために学校（現地）での作業を行うこともある

（参考）各学校の端末・インターネット接続環境の概要

なお、当該情報は全学校の一部についての情報であり、これら以外の環境もあることが考えられるので留意すること。

項目	摘要	備考
接続予定学校数	約 310 校(山形県内の全市町村立小中学校)	Ｒ６．４．１ 時点。
対象 OS	Windows 11	
対象ブラウザ	Microsoft Edge	
セキュリティ対策ソフト	TrendMicro ウィルスバスター Mcafee アンチウィルス Fsecure Client Security Symantec Endpoint Protection NOD32 AntiVirus Doctor Web AntiVirus Microsoft Security Essentials Windows Defender	
インターネット接続環境	・学校独自に民間プロバイダと契約 ・公共 LAN (役場等の拠点まではフレッツ VPN 等の事業者通信網、自治体整備の光回線等により接続)	

イ　認証方式の詳細検討

認証方式は二因子認証以上を予定しているが、詳細は県と協議して決めること。

ウ　SSL－VPN ネットワーク及びデスクトップ仮想化基盤の設計、機器の導入及び設定、基幹ネットワークとの接続

上記ア、イを踏まえ、全ての学校が接続可能なネットワーク及びデスクトップ仮想化基盤の設計を行い、必要となる機器を調達し、所要の設定を施したうえで基幹ネットワークへ接続する。

設計及び接続にあたっては県情報主管課及び基幹ネットワーク運用管理業者と事前に十分な協議を行い、基幹ネットワークに大きな変更をあたえないようにすること。基幹ネットワークの変更が必要となる場合、基幹ネットワーク運用管理業者による変更作業費用は受託者が負担する事。

なお、機器は県が指定する場所へ設置し、県が提供する基幹ネットワーク機器のポートへ接続(結線)を行うこと。設置・接続に際して必要な LAN ケーブルは受託者が用意するものとする。

エ　SSL－VPN ネットワーク及びデスクトップ仮想化基盤のテスト

上記ウの設計に基づき、構築したネットワーク及びデスクトップ仮想化基盤について接続テスト、セキュリティ要件テスト等を行うこと。

オ　関係者との連携

必要に応じて県業務システム主管課や関係事業者と調整し本業務を遂行すること。

カ 簡便な運用管理環境の構築

ネットワークシステムの監視作業は県職員が行う可能性がある。専門知識を有しない職員でも監視や障害の発見・対応が可能な環境及び業務フローを構築すること。

キ 進捗管理

下記の方針に基づいた進捗管理を行うこと。

- 進捗報告会を定期的に開催すること。開催後は速やかに議事録を作成、提出し、活動内容や進捗状況、課題・解決方法などを共有すること。頻度については関係者の合意に基づき、開発の各フェーズで適宜見直すものとする。
- 進捗状況を的確に把握するため進捗管理表及び課題管理表を作成し、進捗報告会等において定期的に報告すること。
- 喫緊の問題が発生した場合などは、状況を把握したうえで適宜報告すること。
- 障害発生時及び緊急事態に備えた連絡体制を整備し、システム開発・保証期間中に委託業務の遂行上問題・事故等が発生した場合、受託者は速やかに県に報告すること。なお、重要な事項又は急を要する事故の場合は、電話等により直ちに報告するとともに後日書面または電子文書にて報告すること。

ク 留意事項

本業務を遂行にあたっては、下記の点に留意すること。

- システムの品質向上、作業漏れ防止を目的とし、開発標準とともに各種作業や手続き、ドキュメント・テンプレート等の標準化をすること。
- ドキュメントのバージョン管理を適切に行い、仕様変更などの際には更新内容について県の承認を得ること。
- 将来システムのブラックボックス化を招かないように、明確な機能分割を行い、設計ドキュメントのメンテナンス等が正確かつ効率的にできるように配慮すること。
- システムに関わる当事者間のオープンなコミュニケーションを重視し、意識のずれが生じないようにプロジェクトを推進すること。
- 開発時に使用するデータ、特に個人情報に係るものは基本的にダミーデータを用意するものとし、テスト等で稼働環境に近いデータが必要な場合は、個人が特定できないように加工するなど、個人情報漏洩が起こらないようにすること。
- 開発時に使用する稼働環境等の管理者パスワードについては、必要な開発者以外に周知しないこと。また、開発者が使用するアカウントについても十分注意して管理し、不要なアカウントを発行しないようにすること。これらのアカウント・パスワードは、本稼働前に必ず削除もしくは変更すること。
- 県がプロジェクトを進める上で不適格と判断したプロジェクトマネージャーは、プロジェクト期間中であっても変更を求める場合がある。
- プロジェクトの進捗状況や課題の適確な把握のため、受託者の内部会議に県が参加する場合がある。

③　学校への導入支援

ア　導入前作業

- 事前調査結果を踏まえ、全ての接続パターンや想定されるＱ＆Ａを網羅したマニュアルを作成すること。マニュアルはネットワークやパソコンについての高度な技術スキルを有しない学校事務職員が理解し操作可能な内容とすること。

イ　説明会の開催

- ネットワーク使用者向けの説明会を開催すること。なお、説明会の開催については WEB 会議等によることも可能とする。
- 受託者は説明シナリオの検討、説明会用資料の作成、当日の講師等を行うこと（説明会用資料の印刷は必要に応じて県が行う）。
- 説明会の詳細は県と協議して決めること。

ウ　接続試験支援

- 接続試験期間中に全校が県業務システムへアクセスできるように支援すること。
- ①のマニュアル等に基づき行う各校での接続試験において、各校からの問合せに対応をすること。対応場所は県と協議して決めること。
- 接続できないまたは県業務システムが通常動作しないなど何らかの障害がある学校への対策を検討し、必要に応じて現地での作業とする。
- 現段階で県が想定する作業は、運用開始前２～３ヶ月間程度問合せに対応すること、

また、並行して１ヶ月間程度、各学校を回って現場で対応することを見込んでいる。
なお、実際には接続試験の状況等により変わる場合がある。

(2)　ネットワーク機器の維持保守管理及びネットワークの運用保守管理

①　ネットワーク機器の維持保守管理等

ア　ネットワーク機器の維持保守管理

(1)の②により導入した機器について、維持及び保守管理を行うこと。

なお、保守管理する機器について、ハードウェアの保守サービスレベルは平日の日中時間帯(9:00～17:00)とする。

また、機器一覧内の SSL-VPN 装置について委託期間中、有効な SSL サーバ証明書を適宜購入し配備すること。

イ　ネットワーク機器の設定

基幹ネットワークの構成変更が発生した場合等、県からの依頼に基づいてネットワーク機器の設定変更に必要な設計・設定を適宜実施すること。ただし、大規模な変更となる場合、対応について県と受託者が別途協議すること。

②　運用保守管理

以下の要件に基づき、運用保守管理業務を実施すること。

なお、ネットワークシステムは下記ウ、エで対応している間を除き、原則 24 時間 365 日稼働させるものとする。

ア　問合せ対応

県からの問合せに対応すること。

対応する時間は原則、県庁舎開庁日の開庁・時間（08:30～17:15）とする。

（小中学校からの直接の問合せ対応は予定していない）

イ　小中学校現地対応

問合せ対応の内、小中学校での動作不具合について必要に応じ、小中学校を訪問しての対応を行うこと。対応に際しては、県が事前に対象の小中学校と協議して決定した日程等に基づいて行うこと。

ウ　障害復旧作業

維持保守管理対象機器に障害が発生した場合、原則として障害の発見又は連絡受付（障害把握）から概ね 4 時間以内に技術者が対応を開始し、障害把握後概ね 8 時間以内に障害を復旧すること。ただし、ハードウェア障害等の事由のため復旧に時間を要する場合は、対応を県と協議すること。

対応する時間は原則、県庁舎開庁日の開庁時間（08:30～17:15）とする。ただし、ネットワークが機能しなくなる等の重大な障害が発生した場合または発生が見込まれる場合は速やかに対応すること。

エ　計画停止対応作業

年１回程度予定している県庁舎電源設備点検時に機器の停止、起動作業を行うこと。

オ　ネットワーク変更支援

学校側のネットワーク環境に変更が発生した場合の相談対応、接続支援を行うこと。

カ　セキュリティ対策

定期的に維持保守管理対象機器のセキュリティ情報等を入手し、ネットワークへの影響度を調査し、県とセキュリティパッチの適用についての検討を行うこと。県が必要と判断した場合にはパッチの適用を行うこと。

キ　ログ監視サービス

ログ監視サービスにより常時システムの稼働状況等について監視すると共に、インシデント発生時には速やかに対応を行うこと。

また、UTM 故障時には必要に応じて現地より保守を行うこと。

５　導入スケジュール

県で予定している導入スケジュールは次のとおり。詳細は県と協議して決めること。

No.	作業概要	実施時期
1	SSL-VPN ネットワークの構築	契約締結から 令和７年 10 月中旬 まで
2	説明会の開催	令和７年 10 月下旬 から 令和７年 11 月末 まで
3	小中学校接続試験	令和７年 11 月 から 令和７年 12 月末 まで
4	ネットワークシステム経由での県業務システムの利用及び運用保守	令和８年１月 から令和 12 年３月末まで

６　受託者の要件

- 本委託業務を行う受託者は、次の要件を満たしていること。情報セキュリティマネジメントシステム適合性評価制度に関して JIS Q 27001（ISO/IEC27001）の基準に適合することによる認証を受けていること。
- 国、都道府県又は地方自治法第 252 条の 19 第 1 項に規定する指定都市において、USB トークンを利用した本委託業務と同等のネットワークシステム（システムを利用するユーザ数が 350 以上の規模を指す。）の設計及び構築を履行した実績があること。
- 国、都道府県又は地方自治法第 252 条の 19 第 1 項に規定する指定都市において、デスクトップ仮想化基盤を利用した仮想デスクトップ機能を提供するシステム（システムを利用するユーザ数が 350 以上のものに限る。）の設計及び構築を履行した実績があること。
- 過去５年以内に国、都道府県又は地方自治法第 252 条の 19 第 1 項に規定する指定都市において、USB トークンを利用した本委託業務と同等のネットワークシステム（システムを利用するユーザ数が 350 以上の規模を指す。）の運用保守管理業務を受託した実績があること。
- 過去５年以内に国、都道府県又は地方自治法第 252 条の 19 第 1 項に規定する指定都市において、デスクトップ仮想化基盤を利用したリモートデスクトップ機能を提供するシステム（システムを利用するユーザ数が 350 以上のものに限る。）の運用保守管理業務を受託した実績があること。

７　成果品

(1) 成果品の内容

受託者は、本委託業務に関する成果品の内容、体裁及び数量について、県と協議し、その承認を受けたのち、指定された様式等で作成すること。

なお、成果品の内容、体裁及び数量について、現在想定している内容は下記のとおり。

また、下記成果品を更新する場合、更新箇所を明示して、更新後のドキュメントを作成すること。

① 構築資料（紙媒体で一式、電子ファイルで一式）

ア 操作マニュアル

- USB トークンの取扱い、SSL-VPN 接続方法、障害発生時の対応方法等が記載されていること。

イ 運用管理マニュアル

- システム監視方法、障害発生時の運用、セキュリティ運用等が記載されていること。

ウ 各種設定資料

- ネットワーク構成図
- 導入機器構成・諸元
- ラック設置図
- 各種設定情報
- 各種テスト仕様書
- 各種テスト結果報告書

エ 説明会用資料

- 説明会で利用する講師用スライドやテキスト等

オ 接続試験支援時の資料

- 問合せ対応票等
- 接続支援時に作成した資料等

カ 仕様確認・進捗報告資料

- 打合せ議事録
- プロジェクト進捗管理表

② プロジェクト計画書（紙媒体で一式、電子ファイルで一式）

作業に先立ち以下の事項等を記載したプロジェクト計画書を提出し、県の了解を得ること。

- 基本方針（ネットワーク機器の更新業務の目的、受託者の責任範囲、遵守すべきルール等）
- 作業工程とスケジュール（ネットワーク機器の更新作業手順等を含む）
- 業務実施体制（統括責任者、チームリーダー、情報取扱責任者等）
- 進捗情報の確認方法（定例会議の開催間隔、報告内容等）
- 記録管理の方法（議事録、課題管理票等の承認者と様式等）
- 成果品

③ 運用保守管理事業計画書

運用スケジュールや体制、作業内容等を記載した事業計画書を提出すること。

④ 運用保守管理報告書（紙媒体で一式、電子ファイルで一式）

ア 運用状況報告

運用状況の報告を行うこと。

イ 改善策提案

必要に応じて、運用上の課題事項の抽出及び改善策の提言等を行うこと。

ウ 操作マニュアルの改訂

システムの操作マニュアル（別添「市町村立学校向け県業務システム接続用ネットワーク接続操作マニュアル」）について、運用による変更が生じた場合は改訂版を作成すること。

(2) 納入期日

① 構築資料

県と協議のうえ、県が指定する期日までに納入すること。また、当該資料を更新した場合は、随時納入すること。

② プロジェクト計画書

契約後速やかに提出すること。

③ 運用保守管理事業計画書

令和７年 12 月末（令和８年１月１日より運用開始を想定）

④ 業務完了報告書

ア 運用状況報告

当月の業務完了報告書を翌月の 10 日までに納入すること。

ただし、令和 12 年 3 月分は令和 12 年 3 月 31 日までに提出すること。

イ 改善提案

随時

(3) その他

上記のほか、必要な書類等については、県と協議して定めるものとする。

８ その他特記事項

- 委託業務の作業場所及び業務の実施に必要な一切の設備・機器等については、県から別途指示がない限り、受託者の責任において確保すること。
- 本契約期間終了後に本業務で構築した SSL-VPN ネットワーク等の運用保守管理を受託する事業者がいる場合は、次期受託事業者へ運用保守管理等に係る引継ぎ等を行うこと。
- 受託者は、本仕様書の解釈、本仕様書に定めのない事項又は本委託業務の実施に必要な詳細事項に関する疑義が生じたときは、遅滞なく県と協議して定めるものとする。
- 本業務の遂行にあたっては「山形県情報セキュリティポリシー」を遵守すること。
- 県庁舎及び学校において作業を行う場合は、「山形県庁内管理規則」等の県庁舎等管理に係る規定を遵守し、場所の使用に係る一切の事項について県の指示に従うとともに、業務従事者の品位の保持に努めること。

別紙１ SSL-VPN 装置仕様（物理）

- 19 インチサーバラック(EIA 規格)に搭載可能な 1U サイズ以下のラックマウント型であること。
- サービス用ネットワークインターフェースとして、1000BASE-T に対応するポート(コネクタ形状は RJ-45)を 1 ポート以上有していること。
- スループットが 1Gbps 以上であること。
- ハードウェアの動作状態を LCD/操作パネル、または SSH、GUI によってモニタリングする機能を有すること。またこれを利用してハードウェア電源管理、管理用 IP アドレスの設定が可能なこと。
- 管理用インターフェースとして 1000BASE-T ポート(コネクタ形状は RJ-45)、シリアルコンソールおよび Web インターフェースを有すること。
- 電源ユニットが冗長化されていること。
- サービス用とは別に管理用インターフェースに対し、デフォルトゲートウェイが設定できること。
- SSL サーバ証明書をバックアップファイルに含められること。
- バックアップファイルからリストアすることにより、SSL サーバ証明書も復元できること。
- 設定アーカイブを暗号化可能であること。
- 設定ファイルの入出力として、下記のいずれか１つ以上の方法に対応していること。
  - アーカイブファイルとしてのインポート/エクスポート
  - テキストファイルとしてのインポート/エクスポート
  - 機器自体のディスクに保存されたファイルからのインポート/エクスポート
  - Web GUI からのインポート/エクスポート
  - CLI を利用したインポート/エクスポート
- 機器に対応が必要な異常が発生した場合、SNMP 及びメールで警告を送信できること。
- マルチテナント等の環境で、接続対象サーバの IP アドレスが重複する環境でも、サーバの IP アドレスを変更することなく、対応が可能なこと。
- 複数のルーティングテーブルを保持できること。
- 3 台以上の機器間で設定の同期が可能なこと。
- 同時に 150 ユーザの接続に対応できること。
- クライアント環境として Windows、macOS、Linux、Android、iOS の OS に対応すること。
- SSL-VPN 接続の際に、ユーザ ID / パスワードだけでなく、クライアントデバイスの OS の種類やバージョン、セキュリティソフトの種類やウィルス定義ファイル更新日付、クライアントデバイスの持つ固有の ID や、予め管理者が配布したファイルが指定のディレクトリに配置されていることなどを確認して、接続可否を管理できること。
- アクセス方式として、トンネルモード、リバースプロキシ方式による内部 Web アプリケーションへの接続、ブラウザベースの RDP 接続をサポートすること。これらのリソースに対してユーザ/グループ毎に接続可否の設定が可能であること。
- SSL-VPN 通信時にはインターネットやローカルネットワークとの接続を遮断できること
  但し、ローカルネットワーク内でもプリンター等のリソースへのアクセス許可は可能とするなどの柔軟な設定が可能なこと

- Windows クライアントの場合には、クライアントと SSL-VPN のトンネル内でデータ圧縮などを用いた高速通信が可能であること。
- 認証、クライアントチェック、利用環境定義などの接続ポリシーを管理者が GUI で設定可能であること。
- LDAP 等の認証サーバと連携して、内部サーバに対してシングルサインオンが可能なこと。
- IPv6 でのサービスにも対応すること
- ネットワーク遅延の影響を低減するため、同一筐体にて WAN 最適化機能を提供する仕組みを提供可能であること。
- 導入後の追加的な要件に柔軟に対応できるよう、スクリプトベース(TCL 等)で動作のカスタマイズが可能であること。

別紙２ PKI プライベート CA サーバ仕様

(認証局について)

- 自組織内部でのプライベート認証局の運営を前提とする。共用サービス（マネージド）型の認証局は不可。
- 認証用クライアント証明書といったエンドエンティティ向け電子証明書のライフサイクル管理（ユーザ登録、証明書発行、失効／有効期限管理）ができる製品であること。
- 発行済み証明書の失効や有効期限到達における再発行の際に、ライセンスなどの再購入コストが発生しないこと。
- 証明書の失効確認は、失効リスト（CRL)、及びオンライン証明書状態プロトコル（OCSP）に対応するものであること。
- 暗号の 2010 年問題に対応可能なものであること（RSA 鍵長 2048bit 以上、ダイジェストアルゴリズム SHA-2 に対応可能なもの)。また、楕円曲線暗号にも対応すること。
- システム内で、認証局の追加が可能なこと。これは認証局の筐体を増やすことを意味するのではなく、筐体内部で論理的に複数の認証局を持てるということを指す。
- 万単位の証明書管理に対応できること。規模に応じてハードウェアの拡張・変更はあってもよいが、その場合には既存のデータを継続利用できること。
- 認証局の秘密鍵の生成・保護に専用装置（Hardware Security Module）を使うとなった場合にも対応が可能なこと。
- 発行されたクライアント証明書は以下デバイスでの利用が可能なこと。
  - パソコン：Windows、macOS
  - スマートデバイス：iPhone / iPad、Android、Windows 10 タブレット
  - 認証デバイス：USB トークン、IC カード
- Windows ドメイン用のユーザ証明書、コンピュータ証明書の発行が可能なこと。

(管理機能について)

- 認証局の管理操作は WEB GUI でおこなえること。また、日本語に対応していること。
- 管理画面へのログインは、多要素認証による高セキュリティな方法を採用していること。
- 管理者によるユーザアカウント登録と証明書発行は、以下の対応が可能なものとする。
  - WEB GUI による逐次登録・発行
  - CSV ファイルアップロードによる一括登録・発行
  - ディレクトリサービス（LDAP/Active Directory）からの一括登録・発行
  - 外部システムとの API 連携による登録・発行
- 証明書の発行プロファイルは、テンプレートなどのしくみにより管理者が容易に操作できること。
- 発行した証明書について、PKCS#12 フォーマットでのダウンロードが可能なこと。
- 証明書失効に関し、失効リスト（CRL）の更新は失効時自動更新でも手動更新でも可能なこと。
- 多様な条件でのユーザアカウントや証明書の検索が可能なこと。また検索結果はファイル出力が可能なこと。

- 証明書の発行や有効期限の到達を、利用者や管理者に通知する機能を有すること。
- 単独管理者による運用も、複数管理者による合議制操作（デュアルコントロール）も可能なこと。
- USB トークン・IC カードといった認証デバイスへの証明書インポート機能があること。また、それら認証デバイス情報の管理機能を有すること。
- 管理者操作ログなどの監査機能を有すること。

(その他)

- 認証局はアプライアンス提供で、かつ Windows ベースのものではないこと。
- アプライアンスのハードディスクや電源ユニットは冗長化されていること。
- 機器障害に備え、ユーザデータ、証明書データ、設定情報等のデータバックアップ機能を有していること。
- 障害により本サーバが停止しても、SSL-VPN 装置を経由した業務システムの利用には直ちに影響がないような構成とすること。

別紙３ デスクトップ仮想化基盤仕様（物理）

(機器等数量について)

- ハードウェア
  - デスクトップ仮想化基盤用サーバ ： 2 台
  - デスクトップ仮想化基盤用ストレージ装置 ： 1 台
  - L2 スイッチ ： 1 台
  - 無停電電源装置 ： 1 台
  - コンソールユニット ： 1 台
  - コンソールスイッチ ： 1 台
- ソフトウェア
  - オペレーティングシステム ： 1 式
  - Office ソフト ： 1 式

(ハードウェアの仕様について)

1. デスクトップ仮想化基盤用サーバ
   - 19 インチサーバラック(EIA 規格)に搭載可能な 1U サイズ以下のラックマウント型であること。
   - ハードウェアの動作状態を LCD/操作パネル、または SSH、GUI によってモニタリングする機能を有すること。またこれを利用してハードウェア電源管理、管理用 IP アドレスの設定が可能なこと。
   - 下記のプロセッサに関する仕様をすべて満たしていること。
     - Intel Xeon Gold プロセッサ 5416 2.0GHz(コア数 16) CPU を 2 基搭載していること。
     - 1 プロセッサあたり、L3 キャッシュメモリとして、24MB 以上を搭載していること。
   - 下記のメモリに関する仕様をすべて満たしていること。
     - デュアルランクレジスタ付き DIMM (RDIMM) DDR4 2666MHz 以上のメモリ を計 128GB 以上搭載していること。
     - RDIMM メモリを最大 768GB 以上搭載可能であること。
     - 空きメモリスロットを 16 スロット以上有していること。
   - CD/DVD-ROM の読み取りが可能な本体内蔵型 CD/DVD ドライブを有すること。
   - 下記のディスクドライブに関する仕様を全て満たしていること。
     - 本体内蔵型ハードディスクドライブ(12Gb SAS 以上に対応した 2.5 型 10krpm 以上のドライブ)であること。
     - RAID1 構成時(スペア 1 台)において 300GB 以上の記憶容量を確保していること。
     - 2GB 以上のフラッシュバックアップ式書き込み/読み込みキャッシュを有するハードウェア RAID コントローラを有していること。
     - ディスクドライブ障害発生時にサーバ本体の電源を切断することなく、電源を入れたままの状態で交換が可能であること。
     - ディスクドライブスロットを標準 8 スロット以上有していること。

- ネットワークインターフェースとして、10BASE-T/100BASE-TX/1000BASE-T に対応するポート(コネクタ形状は RJ-45)を 4 ポート以上有していること。
- デスクトップ仮想化基盤用ストレージ装置との接続用に、下記の仕様を満たすファイバチャネルホストバスアダプターを有していること。
  - 32Gb/s の ポートを搭載した ファイバチャネルホストバスアダプター を 2 枚搭載していること(マルチパス構成、コネクタ形状は Dual-LC コネクタであること)。
- 下記のインターフェースを有すること。
  - PS/2 又は USB キーボードインターフェース
  - PS/2 又は USB マウスインターフェース
  - モニターインターフェース
  - USB 2.0/3.0 インターフェース
  - リモート管理用として、前述のネットワークインターフェースとは独立したインターフェース(コネクタ形状は RJ-45)
- 下記の電源ユニットに関する仕様を全て満たしていること。
  - 電源ユニットが冗長化されており、ユニットの障害時にサーバの電源を停止することなくユニットの交換が可能なこと。
  - 電源ユニットは、100V 電源及び 200V 電源で動作すること。
  - 消費電力は、筐体 1 台当たり最大 505W 以下であること。
- 下記のオペレーティングシステムでの動作をサポートしていること。
  - Windows Server 2025
- 付属品または添付品として下記を有すること。
  - ケーブル長 2m 以上の C13 電源コード(コンセント側プラグ形状は 100V 用 NEMA5-15P、プラグ形状を変換するためのアダプタが必要な場合は変換アダプタを添付すること)
  - 県が別に指定する 19 インチサーバラック(EIA 規格)へサーバを搭載するために必要なスライド式ラックレール及び部品
  - ケーブル長 2m 以上のファイバチャネルケーブル(デスクトップ仮想化基盤用ストレージ装置と前述のファイバチャネルホストバスアダプターとの接続用、両端に LC コネクタが付いていること)

2. デスクトップ仮想化基盤用ストレージ装置
- 19 インチサーバラック(EIA 規格)に搭載可能な 2U サイズ以下のラックマウント型であること。
- 下記のコントローラ及びキャッシュに関する仕様を全て満たしていること。
  - デュアルコントローラ構成であること。
  - コントローラあたり、読み込み/書き込みデータキャッシュとして利用可能な 8GB 以上のキャッシュメモリを備えていること。
  - 時間制限のないキャッシュのバックアップが可能なこと。
- 下記のディスクドライブに関する仕様を全て満たしていること。
  - SAS 2.5 型 SSD 複数台構成の RAID6（スペア 2 台）による 実効 5.76TB の領域を確保できること。
  - ディスクドライブ障害発生時にサーバ本体の電源を切断することなく、電源を入れたままの状態で交換が可能であること。

- ディスクドライブスロットを標準 24 スロット以上有していること。

・ 下記の性能及び機能に関する仕様をすべて満たしていること。
- 最大 325,000IOPS 以上の性能を有すること。
- 64 以上のスナップショットを取得可能であること。
- SSD ボリューム、HDD ボリュームの混在が可能なこと。
- 筐体障害対策として筐体間コピーの機能を有すること。

・ 下記のホストインターフェースに関する仕様をすべて満たしていること。
- コントローラあたり 4 ポート以上の 16Gb FC ポートを備えていること。また、別途 SFP+トランシーバーが必要な場合は全てのポートに用意すること。
- 最大 4 台のサーバと直接接続によりデュアルコントローラーマルチパス構成が可能であること。

・ ストレージのマルチパスについて、OS が提供する標準冗長パス機能での構成が可能であること。

・ 下記の電源ユニットに関する仕様を全て満たしていること。
- 電源ユニットが冗長化されており、ユニットの障害時にサーバの電源を停止することなくユニットの交換が可能なこと。
- 電源ユニットは、100V 電源及び 200V 電源で動作すること。
- 消費電力は、最大 450W 以下であること。

・ 付属品または添付品として下記を有すること。
- ケーブル長 2m 以上の C13 電源コード(コンセント側プラグ形状は 100V 用 NEMA5-15P、プラグ形状を変換するためのアダプタが必要な場合は変換アダプタを添付すること)
- 県が別に指定する 19 インチサーバラック(EIA 規格)へサーバを搭載するために必要なスライド式ラックレール及び部品

3. L2 スイッチ

・ 19 インチサーバラック(EIA 規格)に搭載可能な 1U サイズ以下のラックマウント型であること。

・ 下記の性能及び機能に関する仕様をすべて満たしていること。
- 48Gbps 以上のスイッチ容量を有していること。
- 最大で 35Mpps 以上のパケット処理能力を有すること。
- 8000 以上の MAC アドレスに対応可能であること。
- IEEE802.3ad Link Aggregation Protocol (LACP)に対応していること。
- IEEE802.1q VLAN タギング機能に準拠していること。
- SNMP による管理機能を有すること。また、トラフィック管理のための RMON 機能を有していること。

・ 下記のネットワークインターフェースに関する仕様を全て満たしていること。
- 10BASE-T/100BASE-TX/1000BASE-T に対応するポート(コネクタ形状は RJ-45)を 24 ポート以上有していること。
- Gigabit Ethernet SFP ポートを 2 ポート以上有すること。

・ 下記の電源ユニットに関する仕様を全て満たしていること。
- 電源ユニットは、100V 電源で動作すること。
- 消費電力は、最大 20W 以下であること。

- 付属品または添付品として下記を有すること。
  - 100V 用電源コード(コンセント側プラグ形状は 100V 用 NEMA5-15P、プラグ形状を変換するためのアダプタが必要な場合は変換アダプタを添付すること)
  - 県が別に指定する 19 インチサーバラック(EIA 規格)へサーバを搭載するために必要な部品

4. 無停電電源装置
   - 19 インチサーバラック(EIA 規格)に搭載可能な 2U サイズ以下のラックマウント型であること。
   - 入力側の電圧は単相 100V で、プラグ形状は NEMA L5-30P であること。
   - 出力側として NEMA 5-15R のコンセントを 6 つ以上有すること。また、入力側プラグ形状が NEMA L5-30P のパワーディストリビューションユニットを付属品として使う場合は、NEMA L5-30R のコンセントを 1 つ以上有すること。
   - 2250W 以上の最大出力容量を有すること。
   - 下記の性能及び機能に関する仕様をすべて満たしていること。
     - 停電時、最大出力で 3 分以上の電力供給が可能であること。
     - 低電圧及び過電圧状態を調整できる機能を備えていること。
     - セルフテストにより、無停電電源装置の動作異常やバッテリ電圧の低下等を確認することが可能であること。
     - 動作状態を LCD/操作パネルによってモニタリングする機能を有すること。
     - ネットワーク経由で無停電電源装置の電源切断及び電源投入を行えること。
     - ネットワーク経由で無停電電源装置のセルフテストの実行、スケジュール管理を行えること。
   - 下記のバッテリに関する仕様をすべて満たしていること。
     - 本体内蔵型であること。
     - 装置の電源を切断することなく、電源を入れたままの状態でバッテリの交換が可能であること。
   - ネットワークインターフェースとして、10BASE-T/100BASE-TX に対応するポート(コネクタ形状は RJ-45)を 1 ポート以上有していること。
   - 停電発生時にサーバをネットワーク経由で自動シャットダウンするために必要なオプションおよびソフトウェアを有すること。
   - 付属品または添付品として下記を有すること。
     - 合計 16 口のコンセントを提供可能なパワーディストリビューションユニット(入力側プラグ形状は NEMA L5-30P、出力側コンセント形状は NEMA 5-15R)、もしくは外付コンセントユニット(出力側コンセント形状は NEMA 5-15R)
     - 県が別に指定する 19 インチサーバラック(EIA 規格)へサーバを搭載するために必要なスライド式ラックレール及び部品

5. コンソールユニット
   - 19 インチサーバラック(EIA 規格)に搭載可能な 1U サイズ以下のラックマウント型であること。
   - ディスプレイ部分に関する下記の仕様を全て満たしていること。
     - 18.0 インチ以上の TFT フラットパネルであること。

- 解像度 1600×1200 以上の入力解像度に対応していること。
- ディスプレイバックライトが、ディスプレイ部を閉じたときに自動消灯し、開いたときに自動復帰するものであること。

・ キーボード部分に関する下記の仕様を全て満たしていること。
- 日本語版 106 キー配列（OADG109 準拠含む）であること。
- タッチパッド又はトラックボールのいずれか(本体内蔵型)を備えていること。

・ 下記のインターフェースを有すること。
- VGA インターフェース
- PS/2 又は USB キーボードインターフェース
- PS/2 又は USB マウスインターフェース

・ 下記の電源ユニットに関する仕様を全て満たしていること。
- 電源ユニットは、100V 電源及び 200V 電源で動作すること。
- 消費電力は、最大 50W 以下であること。

・ 付属品または添付品として下記を有すること。
- C13 電源コード(コンセント側プラグ形状は 100V 用 NEMA5-15P、プラグ形状を変換するためのアダプタが必要な場合は変換アダプタを添付すること)
- PS/2 又は USB ケーブルもしくはその両方(キーボード/マウス接続用)
- VGA ケーブル(ディスプレイ接続用)
- 県が別に指定する 19 インチサーバラック(EIA 規格)へサーバを搭載するために必要なスライド式ラックレール及び部品

6. コンソールスイッチ

・ 19 インチサーバラック(EIA 規格)に搭載可能な 1U サイズ以下のラックマウント型であること。

・ 下記のインターフェースを有すること。
- モニターインターフェース
- PS/2 又は USB キーボードインターフェース
- PS/2 又は USB マウスインターフェース

・ サーバ側インターフェースとしてのポート(コネクタ形状は RJ-45)を 8 ポート以上有していること。

・ 下記の電源ユニットに関する仕様を全て満たしていること。
- 電源ユニットは、100V 電源及び 200V 電源で動作すること。
- 消費電力は、最大 50W 以下であること。

・ デスクトップ仮想化基盤用サーバ及びコンソールユニットとの接続ができるよう、接続用ケーブル及び接続用インターフェースアダプタを用意すること。

・ 付属品または添付品として下記を有すること。
- C13 電源コード(コンセント側プラグ形状は 100V 用 NEMA5-15P、プラグ形状を変換するためのアダプタが必要な場合は変換アダプタを添付すること)
- 県が別に指定する 19 インチサーバラック(EIA 規格)へサーバを搭載するために必要なスライド式ラックレール及び部品

（ソフトウェアの仕様について）

1. オペレーティングシステム
   - オペレーティングシステムはWindows Server（バージョンは2025以降)であること。
   - デスクトップ仮想化基盤用サーバ1台につき、Windows Server の仮想マシンを4台分利用可能な権利を有するCPUコア数ベース分のアカデミック版サーバライセンスを用意すること。
   - 小中学校PC接続用として、Windows Serverアカデミック版ユーザークライアントアクセスライセンスを350ユーザ分、Windows RDSアカデミック版ユーザークライアントアクセスライセンスを350ユーザ分用意すること。
2. Officeソフト
   - Microsoft Excel（バージョンは2024以降）を導入すること。
   - 350端末分が利用可能なアカデミックオープンライセンスを用意すること。

別紙４ ネットワークセキュリティパッケージ仕様

(機器等数量について)

- ハードウェア
  - UTM ： 1台
- ソフトウェア
  - UTMライセンス ： 1式

(ハードウェアの仕様について)

1. UTM
   - Gigabit Ethernet対応のWANポート(コネクタ形状はRJ-45)を1ポート有すること。
   - Gigabit Ethernet対応のLANポート(コネクタ形状はRJ-45)を3ポート以上有すること。
   - IPアドレス/ポート番号ベースのパケットフィルタリングによるファイアウォール機能を有すること。
   - アンチウィルス、Webフィルタ、アプリケーション制御、IDS/IPS等のUTM機能を有すること。
   - タグVLAN（IEEE802.1Q）の機能を有すること。
   - SNMPエージェントの機能を有すること。
   - GUIにより各種機能の設定等の運用管理が可能であること。
   - 後述のログ監視サービスとの連携が可能な機種であること。

(ソフトウェアの仕様について)

1. UTMライセンス
   - UTM の機能（AV/IPS/Web フィルタ/アンチスパム）を利用するためのライセンスであること。

(ログ監視サービスの仕様について)

- 本調達で導入するUTMのログを収集し、セキュリティインシデントの有無や関係するイベントを監視および分析を行うこと。
- UTM のログをネットワーク経由で収集すること。ただし、ログ内容を第三者に読み取られるリスクを低減させるため、ログまたは通信を暗号化して収集すること。
- UTM のログは、データセンター内のサーバルームにあるネットワークセキュリティパッケージサービス専用の設備で収集すること。また、サービス設備があるサーバルーム並びにサーバラックは入退室と施錠の管理がされており、本業務と無関係の第三者が、無断でアクセスできないようなセキュリティ対策が施されていること。
- サービス設備があるデータセンターは、ISO/IEC27001の認証を取得しており、現在も認証が有

効であること。

- サービス設備があるデータセンターは、災害や障害発生時などの緊急時に発注者が現場の状況を迅速に確認できるよう、山形県庁から車で1時間以内に移動可能な場所に立地していること。
- 過去5年以内に地方自治体における業務実績がある、または本調達時点で業務履行中であること。
- セキュリティインシデントまたはその可能性があるイベントを検知した際は、発注者または発注者が委託する事業者が指定したメールアドレスに、24時間365日メールで通知できること。
- セキュリティインシデントまたはその可能性があるイベント等についての分析結果をまとめた分析レポートを、サービスが提供するポータルサイト等において、発注者または発注者が委託する事業者が過去分含め任意月の分をダウンロードできるようにすること。
- 上述の分析レポートをダウンロードするポータルサイト等は、IDとパスワードによる認証制限が設けられており、認証情報を知る者以外は分析レポートを閲覧およびダウンロードできないこと。