総合教育センターインターネット接続システム業務委託仕様書

1. 業務の目的

秋田県総合教育センター（以下、「当センター」という）における安定したインターネット接続環境を確保し、増加するリモート講座（双方向 Web 会議）等のトラフィックにも対応可能な、高速かつ信頼性の高いネットワークシステムを構築・運用することを目的とする。

2. 契約期間

令和 8 年 4 月 1 日から令和 13 年 3 月 31 日までとする。

ただし、本業務は以下の 2 期に区分して実施するものとする。

(1) 第 1 期（現行保守、新システム構築・移行期間）

令和 8 年 4 月 1 日から令和 8 年 9 月 30 日まで

※新システム運用開始に向けた環境構築および移行作業を実施する期間を含む。

(2) 第 2 期（新システム運用・保守期間）

令和 8 年 10 月 1 日から令和 13 年 3 月 31 日まで

※本仕様書に基づく新システムの運用および保守業務を実施する期間とする。

3. 業務内容

以下のとおり、システムの構築、設定、及び契約期間中の運用保守業務を行うこと。

(1) ハードウェア、ソフトウェア、ライセンス、保守サポートを一体の月額費用として提供すること。なお、第 1 期におけるシステムの構築およびデータ・設定移行に伴う初期作業費用等については、月額委託料に含めて平準化して請求すること。

(2) 本業務の保守範囲は、事業者が当センター内に設置する内部 L3 スイッチまでとする。当該スイッチの LAN ポートから先の、当センター内 LAN（各種サーバ、端末 PC、プリンタ、ネットワーク配線等）の構築・運用保守は本業務の対象外とする。

4. システム構成要件

(1) 第 1 期（現行保守、新システム構築・移行期間）

現行システムの継続性を担保するため、以下の要件を満たす環境を維持・運用すること。

■通信機器

① ファイアウォール

② 外部 L3 スイッチ

③ 内部 L3 スイッチ

④　内部 DNS/Proxy サーバ
⑤　Backup サーバ
⑥　外部 DNS サーバ
⑦　L2VPN ルーター
※⑥はインターネット事業者が提供するサービスでも可とする。

■設置場所

・　ファイアウォール、内部 DNS／Proxy サーバ、Backup サーバ、外部 L3 スイッチはデータセンターに設置すること。
・　内部 L3 スイッチは、当センター3 階のコンピュータ室内に設置すること。

■構成要件

・　業務系セグメント、内部セグメント 1、内部セグメント 2 には、既存のサーバや、端末 PC，プリンタ等が接続されているが、これらサーバ及び端末 PC から本システムを利用できること。
・　業務系セグメント、内部セグメント 1、内部セグメント 2 は Proxy サーバにより、L2VPN を介してインターネットへ接続できること。
・　外部 DNS サーバに対して、当センターの担当者が指定するサイトの名前解決を設定すること。また，その設定を解除できること。
・　L3-SW により、指定する VLAN を構成すること。
・　事業者は、本システムを適切に設定し、正常に稼働させ、更に、運用保守するために必要なハード、ソフト及び各種ライセンス、故障や不具合発生時の調査・修理・部品交換・本体交換に関わる費用全てを負担すること。なお、第 1 期において使用する通信機器等については、本仕様書の要件を満たす限りにおいて、レンタル機器等の使用を認める。
・　本システムの運用にあたっては、情報漏洩対策等のセキュリティ保持に十分配慮すること。
・　内部のネットワーク上の情報が外部に漏れないこと。
・　当センターとデータセンターを接続する回線は、フレッツ・VPN ワイドを利用し接続し、データセンターからインターネット接続できること。
・　データセンターにおいて無停電電源装置を用意すること。

■新システム構築・移行期間

第 2 期に使用する新システムの構築および第 1 期システムから第 2 期システムへの移行期間とする。

(2) 第 2 期（運用・保守期間）

■通信機器

①　ファイアウォール

② Proxy/DNS

③ 内部 L3 スイッチ

④ 拠点間接続機器

■ネットワーク回線

・ リモート講座等での安定した通信を確保するため、当センターと事業者のデータセンター間を、1Gbps 帯域保証型のダークファイバーを利用した専用線で接続すること。

・ 事業者のデータセンターが利用するインターネットバックボーンは、1Gbps 以上の帯域確保型（ギャランティ型）IP トランジットサービスであること。

■設置場所

・ ファイアウォール、DNS キャッシュ（機能を含む）は事業者のデータセンター内に設置すること。

・ 内部 L3 スイッチは、当センター3 階のコンピュータ室内に設置すること。

・ データセンターにおいて無停電電源装置を用意すること。

5. 主要機器及びサービスの指定仕様

調達する機器及びサービスは、以下の指定を満たすか、それを上回る性能・機能を有するものであること。

(1) 第 1 期（システム構築・移行期間）

機器・サービス	指定仕様
①ファイアウォール	・ 1U、19 インチラック搭載可能。 ・ NIC：10/100/1000BASE-T x8 ポート以上、AUTO MDI/MDIX。 ・ ファイアウォールスループット 1Gbps 以上。 ・ 最大サポートユーザー数 無制限。 ・ ソフトウェアは指定しないが、ファームウェアのライセンスを含むこと。 ・ Web ページから各種設定ができること。 ・ 情報の通過量を[Mbps]で表示できること。
②外部 L3 スイッチ ③内部 L3 スイッチ	・ 1U、19 インチラック搭載可能。 ・ NIC：10/100/1000BASE-T x24 ポート以上、AUTO MDI/MDIX。 ・ スイッチング容量 128Gbps 以上。 ・ パケットフォワーディングレート 95Mpps 以上。 ・ RSTP、LACP 対応、IEEE802.1Q-2003 VLAN 対応。 ・ RIPv1/v2。 ・ ソフトウェアは指定しないが、ファームウェアのライセンスを含むこと。

④内部 DNS/Proxy サーバ ⑤Backup サーバ ⑥外部 DNS サーバ	・ 1U、19 インチラック搭載可能。 ・ CPU：Xeon E-2234 3.6GHz 相当以上。 ・ RAM：8GB 以上(ECC 付き)。 ・ 実質利用可能容量 400GB 以上のストレージを有し、RAID1 等の冗長構成が組まれていること。 ※仮想環境で構築する場合も、基盤となるハードウェアにおいて同等の耐障害性を確保すること。 ・ NIC：10/100/1000BASE-T×2 ポート以上。 ・ シリアル：RS-232C x1 以上。 ・ 冗長電源であること。 ・ 運用保守上必要であれば，ディスプレイ、キーボード等の周辺機器を準備すること。 ・ 上記条件相当の環境であれば仮想環境での構築も可とする。 ・ バックアップサーバへ指定するログやコンテンツを定期的にバックアップするためのスクリプトを実行すること。 ・ OS も含めてバックアップ・リストアできること。 ・ 不要なサービスは全て停止するなどの十分なセキュリティ対策を施し，安全なサービスを提供できること。 ・ 不正アクセス防御やウィルス・ワーム・スパイウェア侵入防御などについて IP アドレスベースのフィルタ機能を有すること。 ・ アクセスログ、システムログ等の自動ローテーション機能を有すること。 ・ 指定された内部の端末からパスワードを漏えいすることなく安全にファイル転送できること。
④内部 DNS/Proxy サーバ	・ 所内 LAN に接続された端末 PC のために、NTP サーバとしても運用すること。
⑥外部 DNS サーバ	・ 当センターが指定する 10 個程度のアドレスについて，その名前解決を設定できること。 （例）xxx.akita-c.ed.jp ⇒ XX.XX.XX.XX ・ インターネット接続業者が提供するサービスの場合，ソフトウェアを問わない。
⑦VPN ルーター	・ 1U、19 インチラック収納可能。 ・ NIC：10/100/1000BASE-T x3 ポート以上，AUTO MDI/MDIX。 ・ スループット（Mbps）：通常時　900Mbps 以上。 L2TPv3 接続時　900Mbps 以上 ・ 各種ブロードバンド回線対応。

	・ ソフトウェアは指定しないが，必要に応じファームウェアのライセンスを含むこと。

(2) 第 2 期（運用・保守期間）

機器・サービス	指定仕様
①ファイアウォール	・ ファイアウォールスループット 25Gbps 以上、各種処理性能は、以下のとおりとすること。 ・ 同時セッション数：3,000,000 以上であること。 ・ 新規セッション処理性能：毎秒 120,000 以上であること。 ・ 冗長化された電源を内蔵できること。 ・ アプリケーションコントロール、Web フィルタリング、アンチウイルス、アンチスパム、侵入防御（IPS）等の統合脅威管理（UTM）機能を有すること。 ・ 検知したログを 1 年以上保存・閲覧できる機能を有すること。なお、ログの保存については機器本体の内蔵ストレージに限定せず、メーカーが提供するクラウドログサービス（1 年間の長期保存対応）等を利用した構成も可とする。 ・ 専用の ASIC を搭載し、CPU の負荷を軽減して高速処理を実現できるアーキテクチャであること。 ・ システム設定のバックアップは、暗号化とパスワードを設定してエクスポート可能であること。
②プロキシ	・ 特定のカテゴリ（アダルト、ギャンブル等）や個別の URL を指定して Web アクセスをブロックする URL フィルタリング機能を有すること。 ・ 固定プライベート IP アドレスを持つ端末は、いつ、どのサイトにアクセスしたかを記録するアクセスログを取得すること。なお、変動プライベート IP アドレスを持つ端末のアクセスログは含まない。
③内部 L3 スイッチ	・ 1U サイズで 19 インチラックへ搭載可能であること。 ・ 冗長化された電源を内蔵できること。 ・ 24 ポート以上の 10/100/1000BASE-T ポートを有すること。 ・ スイッチング容量 128Gbps 以上、パケットフォワーディングレート 95Mpps 以上の性能を有すること。 ・ 最大動作温度は 55℃であること。 ・ IPv4 ACL および IPv6 ACL をサポートしていること。

④拠点間接続機器	・ 1Gbps 回線に対応したスループット 1Gbps 以上の通信機器であること。※回線事業者の提供機器を利用

6. 移行業務要件

令和 8 年 10 月 1 日の新システム運用開始に先立ち、以下の移行業務を実施すること。

(1) データ及び設定の完全移行

- 当センターから開示する現行機器の設定情報に基づき、現行ファイアウォール、L3 スイッチ等に設定されている全てのネットワーク設定（VLAN 設定、ルーティング、ACL 等）を新環境へ反映させること。

(2) サービス停止時間の極小化

- 移行作業は、原則として当センターの業務に影響を与えない夜間または休日に実施すること。または当センターが指定した日時に行うこと。

(3) 移行後の動作確認

- 移行完了後、全ての機能が正常に動作することを事業者が確認し、当センター担当者による最終確認を受けること。

7. 運用保守要件

(1) 24 時間 365 日の死活監視を行うこと。

(2) 保守対応時間は、土日祝日及び年末年始を除く平日 8:30～17:15 とする。ただし、ネットワークの全断等の重大な障害発生時においては、上記保守対応時間外であってもリモート対応を含め速やかに復旧作業に着手し、サービス再開を目指すこと。

(3) 契約期間中における対象ハードウェア故障、ソフトウェアのアップデート、設定変更、技術的な問い合わせ対応、及びそれに伴う人件費・交通費等の一切の費用は月額委託料に含むものとする。

(4) 本仕様書に記載される全てのネットワーク機器およびサーバ設備に対し、ハードウェア障害時のオンサイト保守を適用すること。当センター内に設置される機器（内部 L3 スイッチ等）については、現地での交換作業を含むオンサイト保守とすること。事業者のデータセンター内に設置される機器については、事業者の責任において迅速に復旧を実施すること。

8. 業務報告

事業者は、毎月 10 日までに、前月分の業務内容について以下の項目を含む業務報告書を作成し、当センターへ提出すること。

(1) 全体報告

- 作業実施期間、作業内容の総括
- 特記事項の有無

・　報告書の発行責任者及び担当者の連絡先

(2) 機器別稼働状況

・　ファイアウォール、各 L3 スイッチについて、以下の内容を個別に記載すること。

・　当月中の設定変更、追加作業等の有無及びその内容

・　機器の動作状況（正常、または異常の内容）

(3) セキュリティレポート

・ ファイアウォールの UTM 機能のログに基づき、以下の項目を含む月次セキュリティレポートを提出すること。

・ DoS 攻撃

・ 不正侵入（IPS）

・ マルウェア

・ 不正サイトへのアクセス

9. 情報セキュリティ要件（第 2 期）

秋田県情報セキュリティポリシーを遵守し、セキュリティ対策を万全に期すため、以下の対策を講じること。

(1)技術的対策

・ 各種ログやセキュリティ上必要な記録を取得し保存すること。また、必要に応じて定期又は随時に障害、不正アクセス等の異常が無いか各種ログの確認を行い、異常が認められた場合は適切な対応を行った上で担当者に報告すること。

・ 定期的にバックアップを実施し、バックアップを適切に保管すること。

・ 不正プログラム対策機能（UTM 機能等）の有効化により、ランサムウェアの感染、不正アクセス等に対して必要な対策を行うこと。

・ ソフトウェアの欠陥について、緊急度に応じてソフトウェアの更新を行うこと。

・ 使用されていないポートを閉鎖すること。

・ 不要なサービスの削除又は停止を行うこと。

・ 提供する通信機器等の設置時、施錠管理や容易に取り外せないように固定するなど盗難防止の対策を講じること。

(2)管理的対策

・ セキュリティインシデント発生時またはその恐れがある場合は、速やかに当センターへ報告するとともに、秋田県庁の CSIRT（デジタル政策推進課 情報基盤・システム管理チームの PoC）への報告および調査に協力すること。

(3)監査及び公表

・ 県が必要と認めた場合、事業者の業務実施状況について監査、検査を行うことができるものとする。

・ 重大な情報セキュリティインシデントが発生した場合、県はその事実を公表することができるものとする。

10. 個人情報の取り扱い

現行契約書（【捺印版】契約書）の別記「個人情報取扱特記事項」を遵守すること。

11. 秘密の保持

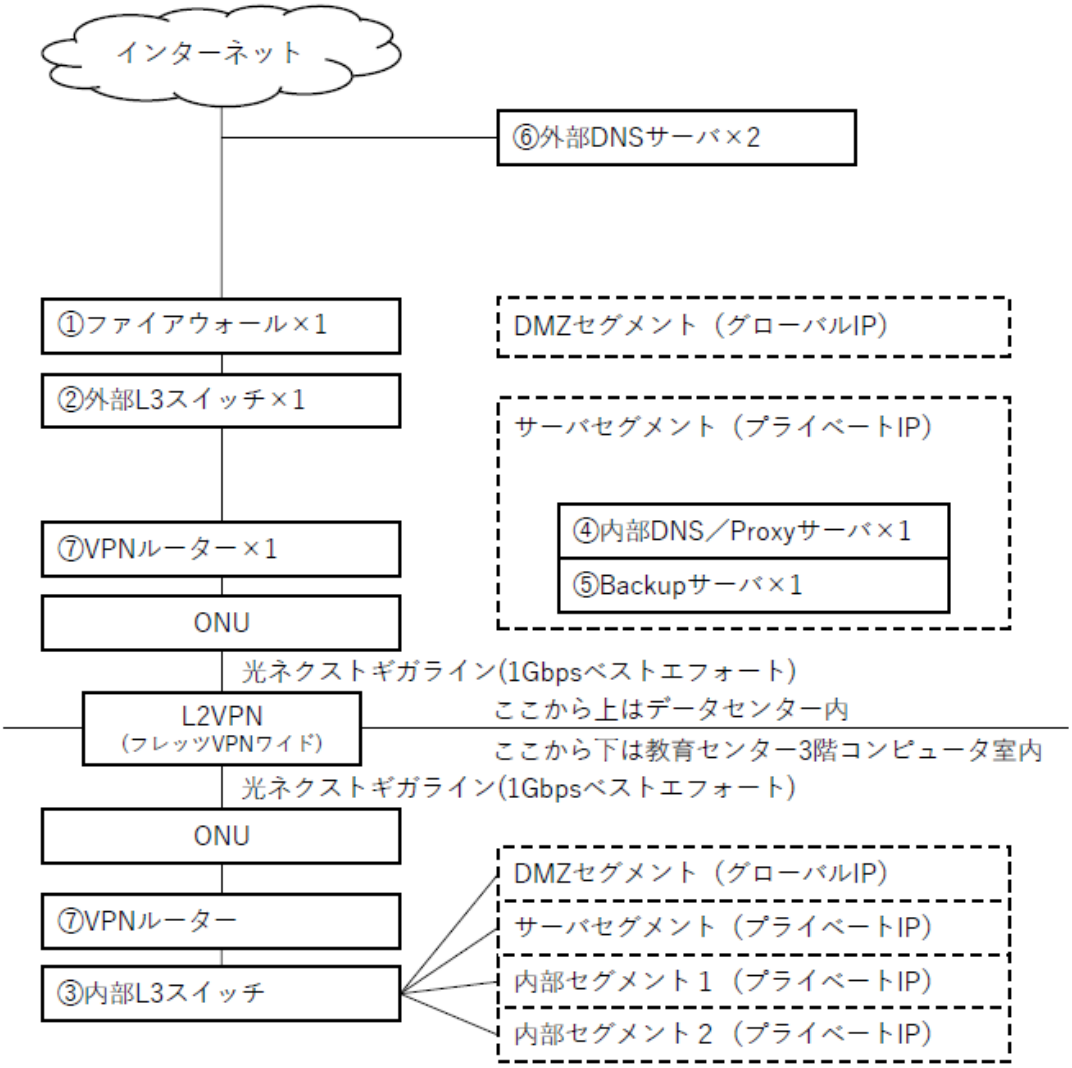
本業務に関して知り得た一切の情報を、当センターの許可なく第三者に漏洩してはならない。

12. 契約終了時の措置

本契約が終了する場合、事業者は当センターが指定する次の事業者に対し、業務の引き継ぎを誠実に実施すること。また、各機器の設定情報の一切を、当センターが指定する形式で遅滞なく引き渡すこと。事業者のデータセンターに設置された機器群（ファイアウォール等のログ・設定情報を含む）の撤去にあたっては、復元不可能な方法でデータ消去を行い、当センターに対して「データ消去証明書」（またはそれに準ずる作業記録）を提出すること。

以上

別紙　現行構成図


インターネット
⑥外部DNSサーバ×2
①ファイアウォール×1
②外部L3スイッチ×1
DMZセグメント（グローバルIP）
サーバセグメント（プライベートIP）
④内部DNS／Proxyサーバ×1
⑤Backupサーバ×1
⑦VPNルーター×1
ONU
光ネクストギガライン(1Gbpsベストエフォート)
L2VPN
（フレッツVPNワイド）
ここから上はデータセンター内
ここから下は教育センター3階コンピュータ室内
光ネクストギガライン(1Gbpsベストエフォート)
ONU
⑦VPNルーター
③内部L3スイッチ
DMZセグメント（グローバルIP）
サーバセグメント（プライベートIP）
内部セグメント１（プライベートIP）
内部セグメント２（プライベートIP）