国際教養大学学内用ファイアウォール等更新業務委託仕様書

1. 調達物品名及び構成内訳

(1) ファイアウォール本体装置　　正副各１台
(2) ファイアウォール管理クラウドシステム　　１式
(3) その他必要なライセンス　　１式
(4) その他必要なソフトウェア　　１式

2. 更新の技術的要件

(1) 本更新に係る機能及び技術等の要求要件を以下に示す。
(2) 以下の要件は全て必須の要求要件である。
(3) 必須の要求要件は本学が必要とする最低限の要求要件を示しており、すべての調達およびシステム構築を実施できない場合は、決定の対象から除外する。
(4) 次年度以降のライセンス費用については別途協議するが、本学が予定する費用を大幅に上回り本システムの維持が困難と判断される場合は、決定の対象から除外する。

2.1 ファイアウォール本体装置　正副各1台(設置場所:中嶋記念図書館サーバ室)

2.1.1 ファイアウォール本体装置の技術的要件

(1) 19 インチラックにマウントが可能なこと。
(2) 27Gbps 以上のファイアウォールスループットを有すること。
(3) 4Gbps 以上のスループット（ファイアウォールと IPS の同時動作時）を有すること。
(4) 毎秒 280,000 以上の新規セッション数を処理する機能を有すること。
(5) 最大同時セッション数として 3,000,000 以上のセッションを処理する機能を有すること。
(6) 10/100/1000base-T を合計 16 ポート以上、SFP ポートを 8 ポート以上、SFP＋ポートを 4 ポート以上備えること。
(7) 仮想ルータもしくは仮想ＦＷを 10 以上構成可能であること。
(8) RJ45 の Gigabit Ethernet ポートを 16 個以上、SFP ポートを 8 個以上、SFP+ポートを 4 個以上備えていること。
(9) NAT 機能を有すること。
(10) DoS 攻撃防御機能を有すること。
(11) IEEE802.1Q VLAN トランク機能を有すること。
(12) IEEE802.3ad リンクアグリゲーション機能を有すること。（Static, LACP）
(13) ジャンボフレーム（9,216Bytes）をサポートすること。
(14) RIPv2, OSPF, BGP のダイナミックルーティングに対応していること。
(15) IPv4 および IPv6 の OSPF Graceful Restart に対応していること。
(16) IPsecVPN によるサイト間 VPN に対応していること。
(17) IPsec サイト間 VPN における IKE/証明書認証に対応していること。
(18) Active/Standby(Passive)、Active/Active 両方の冗長構成に対応していること。（尚、いづれの冗長構成でもアプリケーション識別や IPS 機能、アンチウィルス機能も制限なく利用可能なこと）
(19) 冗長構成の OS アップグレード作業時、セッションを維持しつつアップグレード作業が可能であること。

(20) シグネチャやプロトコル検証、アノマリー検出、振る舞い分析など、複数の手法を統合した多層脅威検出エンジンで防御していること
(21) 1 つのセキュリティポリシーで IPv4 および IPv6 通信に対するアクセス制御やアプリケーション識別による制御が可能であること。
(22) 管理専用の GUI が用意されていること。
(23) IPv4/IPv6 通信に対して、脆弱性防御、アンチウィルス、アンチスパイウェア、ファイルフィルタ、データフィルタといったコンテンツスキャニング機能を、フローベース又はプロキシベースで処理できること。
(24) 専用のアプリケーション識別エンジンを搭載しており、全てのトラフィックを対象にしたアプリケーションの識別のシグネチャが提供されていること。
(25) 同一の TCP/UDP ポートを使用するアプリケーションに対し、異なるセキュリティポリシーを設定可能であること。
(26) GRE 等のトンネル通信に対してもコンテンツスキャンが可能であること。
(27) PDF、Excel、WORD、PPT、ZIP など 50 種類以上のファイルタイプによる通信の可視化やフィルタリングが可能なこと。
(28) ファイアウォールのポリシーは送信元/送信先とアプリケーション名を元に処理可能であること。
(29) ファイアウォールのポリシー毎にウィルススパイウェア、URL フィルタリング等のコンテンツ検査機能を有効/無効に設定が可能であること。
(30) Web アプリケーションの制御が可能なこと。
(31) アプリケーション制御ルール毎に曜日や時間を指定して有効化できること。
(32) アプリケーションの使用帯域の制限が可能なこと。
(33) ファイアウォールのセキュリティポリシー上で URL カテゴリを直接指定し、URL カテゴリ毎のアクセス制御が可能であること。
(34) クレジットカード番号、またはカスタマイズした文字列パターンでのデータフィルタが可能であること。
(35) 感染したコンピュータと C&C サーバ間の通信を検知および遮断できること。
(36) 内部クライアントから外部の危険なサイトや C&C サーバに対する通信開始時に行われる悪意のあるサイトに対する DNS 正引き（名前解決）が行われた場合に、ファイアウォール上で予め定義した偽りの IP アドレスを返答させることにより、不正通信を行った内部クライアントの IP アドレスの特定が可能な機能を有すること。
(37) 筐体内で SSH 通信を複合化し、ポートフォワード通信を検知可能であること。
(38) 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およびコンテンツ検査のポリシーが適用可能であること。
(39) SAML に対応した認証機能を有すること。
(40) Active Directory 等と連携し、IPv4 及び IPv6 環境に関わらず IP アドレスとユーザ情報を紐付け、可視化と制御が可能であること。
(41) Syslog メッセージより取得したユーザ情報を基にトラフィックの可視化が可能であること。
(42) ポリシーベースの QoS に対応しており、アドレス、ポート番号、利用ユーザ、アプリケーションといった情報を基に帯域制御が可能であること。
(43) 追加機器等なく、未知のファイルをサンドボックスに送付することが可能であり、サンドボックスでの分析の結果悪意のあるファイルであると判定された場合には、自動的に防御シグネチャが適応されること。
(44) 未知のマルウェア感染が疑われるファイルを自動的に仮想実行環境上で検査し、未知のマルウェアの早期発見と対策が可能なクラウドシステムと連携する機能を有すること。
(45) メール本文に含まれる URL リンク情報を検査し、危険と判定された場合、タグをつけ処理出来る様にすること。
(46) サンドボックスで危険と判定された場合、その解析結果を管理 GUI にて参照可能なこと。
(47) 宛先/送信元の国別アドレスでポリシー制御が可能であること。
(48) ミラーポート接続、L1 モード(MAC アドレスを保持しない)、L2(ブリッジ)モード、L3(ルータ)モードに対応し、一筐体内で複数のモードを同時に利用可能であること。
(49) Ping によるスタティックルートの死活監視を行い、監視先がダウンした際には当該ルートを動的に削除する機能を有すること。
(50) 設定操作は、候補コンフィグを作成し、コミット操作にて設定を有効にするアーキテクチャであること。また、候補コンフィグで実行中の状態に戻すことが可能であること。

(51) 設定情報を名前付きのスナップショットとして保存可能であり、またスナップショットから設定を復元できること。
(52) 設定情報をテキスト形式でインポート/エクスポート可能であること。
(53) コミット操作に関しては、管理者毎に、その管理者が設定変更した分だけをコミットできること。
(54) 設定を戻したい場合は、管理者毎に、その管理者が設定変更した分だけを戻すことができること。
(55) インターネット経由でファームウェアならびにシグネチャファイルを製品に直接ダウンロードおよびインストール可能であること。また Proxy 経由でもこれが可能であること。
(56) 脅威を検知した IP アドレスからの通信に対して、通信を遮断する機能を有すること。
(57) Syslog データ転送方式として UDP に加えて TCP または SSL に対応していること。
(58) telnet/ssh によるコマンドラインインタフェースを有すること。
(59) SNMP プロトコルによる管理処理部のモニタリングが可能なこと。
(60) WebUI は日本語を含む複数の言語に対応していること。
(61) IPv6 による WebUI/CLI の管理通信に対応していること。
(62) ファイアウォールポリシーは、10,000 以上サポートできること。
(63) インターネットサービスの IP アドレスデータベースを有し、Amazon、Salesforce、Microsoft Azure、Microsoft Office 365、Box、Google Cloud を宛先に選択し、ルーティングできること。また、インターネットサービスの IP アドレスデータベースを管理者が更新することなく動的に更新される運用が可能なこと。
(64) SD-WAN 機能により、複数インターフェースのバンド幅、通信量、セッションに基づく WAN 最適化を行えること。
(65) Web プロキシサーバ(フォワードプロキシ) 機能を有し、プロキシの自動設定ファイル(PAC)、Web プロキシ自動検出プロトコル(WPAD)で Web ブラウザを設定する方法を展開できること。
(66) Web フィルタリング機能は、87 以上のカテゴリーに分類されて、クラウドクエリを行って最新の URL 情報に基づくフィルタリング機能を提供できること。
(67) ASIC によるセキュリティスキャンが可能な製品であること。

2.1.2 ファイアウォール本体装置の設定作業

(1) 既存ファイアウォールの設定を引き継いだ上で必要な場合は追加設定を行うこと。
(2) 不要な機能は全て停止するなどの十分なセキュリティ対策を施し，安全なネットワークを構築すること。
(3) 導入時点での最新ファームウェアが適用されていること
(4) 以下の機能について本学と協議の上適宜設定を行うこと。
(5) 脆弱性が発見された場合は，その対策を迅速に継続して行うこと。
(6) 本装置の設置・運用により、本学の電源、ネットワーク等を含む既設機器やサービスに対して、過度の負荷や障害を与えないこと。
(7) ログおよびレポートが外部の記憶装置に転送できるようにすること。

2.2 ネットワーク管理クラウドシステム 1式

2.2.1 ネットワーク管理クラウドシステムの技術的要件

(1) 通信量の統計情報を元に、宛先/送信元の国別で通信量をする機能を有すること。
(2) レポートデータを PDF 形式でエクスポートし、スケジュール機能により定期的に電子メールに添付し送付することが可能であること。
(3) WebUI 上で動的に表示を切り替えることができるリアルタイムレポート機能を搭載し、利用頻度の多いアプリケーション、URL カテゴリ、脅威をランキング形式で表示できること。
(4) 管理とレポートをクラウドベースで提供出来ること
(5) 1 日あたり 20GB のログ保存が出来、又 365 日保存出来ること

3. 構築する上での一般的な留意事項

(1) すべてのソフトウェアについてインストールと設定後に、必ず動作確認を行うこと。
(2) 全てのソフトウェアとハードウェアが既存のシステムと協調し、適切な速度で正常に動作すること。
(3) この仕様書で不明な点は、導入時に本学と協議の上決定する。
(4) グローバル IP アドレスは、本学が所有しているアドレス、本学が契約中のインターネット接続業者から借用しているアドレスを付与すること。
(5) ドメインは、必要に応じて本学が利用しているドメイン名を利用すること。
(6) 本システムの設置・運用により、本学の電源、ネットワーク等を含む既設機器やサービスに対して、過度の負荷や障害を与えないこと。

4. 調達物品の搬入、設置、配線に関する事項

(1) 電源は同一ラック内に本学が指定する UPS までを本学の負担とする。
(2) 信号線工事に関しては館内 LAN 幹線の指定の HUB までを本学の負担とする。
(3) システム構成機器類の設置、配線、調整を行うこと。また、ネットワークの調整、動作確認を行うこと。
(4) 新規の電源工事、通信配線工事が必要な場合は、計画書を提出し、本学と協議のうえ、本学の指示に従うこと。またこれに要する費用は今回の調達に含むこと。
(5) 学内 LAN との接続に際して、ルータ、ハブ等に設定、調整が必要な場合は本学と十分協議し、本学の指示に従うこと。
(6) 既設の施設内の空間、空調等の物理的環境で対応できること。
(7) ハードウェアの動作確認に必要なソフトウェアの調達、インストール及び調整は、受注者が行うこと。

以上