別紙４　「クラウド型統合セキュリティ基盤」に関する特記仕様

ネットワーク要件

項目	仕様
アクセス制御	ユーザー単位でのターゲットサーバーへのアクセス制限が可能であること。
Web フィルタリング	Web サイトのカテゴリ分類による制御が可能であり、カテゴリ内の特定サイトをホワイトリスト化できること。
IP アドレス管理	外部 SaaS の IP 制限に対応するため、占有の固定グローバル IP アドレスを無償で 3 つまで払い出し、送信ソース IP として固定できること。
接続性・拠点連携	コネクタ等の設置により、社外端末から拠点内へセキュアな TCP/IP 通信が可能であること（ZTNA）。また、拠点間通信（SD-WAN）が可能であること。
ロケーション検知	拠点内接続を自動認識し、クラウドを経由しない直接アクセスが可能であること。社外接続時は SWG/ZTNA 経由を強制し、ラテラルムーブメントを遮断すること。
パフォーマンス	通信量に応じたオートスケール機能を備え、突発的な負荷増大時も遅延なく稼働すること。回線や通信速度の指定なく利用可能であること。
通信制御・透過性	契約帯域内において、TLS インスペクションの同時接続数やユーザー数による制限なく、全通信の確認・制御が可能であること。

セキュリティ

項目	詳細仕様
認証連携	Entra ID（旧 Azure AD）と連携し、ユーザー・グループ単位で SSO（シングルサインオン）およびアクセス管理ができること。
多要素・端末認証	管理コンソールの二要素認証に対応すること。また、接続時に端末のセキュリティ状態をチェック（検疫）し、認可を制御できること。
CASB	Header Injection によるテナント制御、シャドーIT の可視化、組織特有サイトの定義が可能であること。ストレージへの操作（UP/DL/Login 等）を詳細に制御できること。
DLP	個人情報や機密情報の検知・流出防止機能（DLP）を有し、特定データ検知時にアラートや遮断が可能であること。
脅威対策（Malware/IPS）	Anti-Malware 機能により通信を継続スキャンし、検知・防御すること。DDoS 対策やインジェクション攻撃等の IPS 機能を備えていること。
暗号化通信検査	HTTPS 通信を復号・検査し、ポリシー違反や拒否エントリを検索・ロギングできること。
エンドポイント連携	EDR/XDR 製品との連携、または同等の機能を有し、EPP（エンドポイント保護）機能も備えていること。

サービス要件

項目	詳細仕様
サポート・言語	平日 9:00-17:00 の日本語による技術サポートを提供すること。管理コンソールは Web ベースで、日本語表示に対応していることが望ましい。
認証・コンプライアンス	ISO 27001/27017/27018/27701/14001、Cyber Essentials、GDPR、CSA STAR、SOC1,2,3 の全ての認証を取得していること。
システム構成	ログや管理サーバーは他ユーザーと共有しない専用環境（シングルテナント）であること。占有のバックボーンネットワークを有していること。
可用性（SLA）	稼働率 99.999%以上を保証すること。東西全域被災時でも事業継続が可能な冗長性を有していること。
ログ保管	トラフィックデータやイベントログを 90 日間（3 ヶ月）すること。

管理機能	SWG/ZTNA を含む全機能を単一の Web コンソールで統合管理（通信確認/管理）ができること。詳細なログ検索・テンプレート作成・ロール設定が可能であること。
最小構成・保守	VPN ユーザー10 名から利用可能であること。