

## 【別紙 10】ファイアウォール

- (1) アプライアンス製品であること。
- (2) 10/100/1000Base-T ポートを 10 ポート 以上有すること。
- (3) USB ポートを 2 ポート以上有すること。
- (4) コンソールポートを 1 ポート以上有すること。
- (5) 同時セッション数は 4,000,000 以上有すること。
- (6) 新規セッション数/秒は 300,000 以上有すること。
- (7) ファイアウォールスループットは 30Mpps 以上有すること。
- (8) IPSecVPN スループットは 20Gbps 以上有すること。
- (9) IEEE802.1Q VLAN タギング機能を有すること。
- (10) IEEE802.3ad リンクアグリゲーション機能を有すること。
- (11) 同一機種を2台で冗長構成とすること。
- (12) RADIUS、LDAP によるユーザ認証機能を有すること。
- (13) ポリシー数は10,000 以上設定する機能を有すること。
- (14) ファイアウォール機能としてNAT およびPAT 機能を有すること。
- (15) セキュリティ機能としてファイアウォール機能・VPN 機能の他にライセンスを購入することによりアンチウイルス機能、不正侵入検知機能、コンテンツフィルタリング機能、アンチスパム機能を有すること。
- (16) 不正侵入機能のスループットは1.4Gbps 以上有すること。
- (17) アノマリ方式の不正侵入検知機能によりDoS 攻撃から防御が可能であること。
- (18) 不正侵入検知機能としてセキュリティポリシー毎にシグネチャの適用が可能であること。
- (19) プロキシベースでのアンチウイルス検知が可能であること。
- (20) アンチウイルス (HTTP) のスループットは200Mbps 以上を有すること。
- (21) ウィルスを検知した時、ウィルスの詳細情報へのリンクをログに出力する機能を有すること。
- (22) ウィルスパターンファイルの更新は、自動アップデート設定が可能であること。

- (2 3) コンテンツフィルタリング機能は76以上のカテゴリ(危険なサイトや不適切なサイト等の制限すべき事項)が用意されているとともに、各カテゴリについて、あるグループは許可・監視、あるグループはブロックといったグループ毎の設定が可能であること。
- (2 4) 特定の単語を登録し、サイトのブロックが可能であること。
- (2 5) ブロックした時の表示は日本語でかつ編集が可能であること。
- (2 6) 論理的な仮想セキュリティ・ドメインを10 以上の設定であること。。
- (2 7) クライアントライセンスが無制限であること。
- (2 8) SNMPv1、v2c、v3 機能を有すること。
- (2 9) 設定はWEB GUI、CLI いずれにも対応していること。WEB GUI は日本語対応していること。
- (3 0) Syslog サーバへのログ 送信機能を有すること。
- (3 1) 電源はAC100V とすること。
- (3 2) UPS に接続すること。(今回導入するバックボーンスイッチとの共有は可能とする。)
- (3 3) 講義棟2F の既存ラックに搭載すること。
- (3 4) 本学担当者との協議の上、設定すること。