4. 信頼性等要件

設計・開発業者は、以下の信頼性要件、拡張性要件、上位互換性要件、システム中立性要件及び事業継続性要件を踏まえ拠点 LAN の設計を行っている。受注者においても、以下の要件を前提に作業を行うこと。

4.1. 信頼性要件

（1） 可用性

機器及び回線の冗長化による可用性確保はしない。稼働率や故障率は「10.1.3. 利用拠点LANに関するSLA項目」にて定めている。

（2） 完全性

障害等により導入機器の設定情報が消失した場合に備え、「2.8.2. 納入機器　表 2.8-2 納入機器及び納入期限　項番 6」に示すとおり、適宜バックアップを取得する。

（3） 機密性

ログイン通信が盗聴されないよう、導入機器へのリモートログインにあたっては SSH による暗号化を実装する。

4.2. 拡張性要件

導入完了以降、端末、サーバ及びネットワーク機器が導入機器毎に 2 台まで増加することを想定しているため、導入機器毎に空きポートを 2 つ用意する。

4.3. 上位互換性要件

導入機器のファームウェア等を更新した際、更新前にサポートしているプロトコル仕様や設定ファイルに対して互換性を有すること。

4.4. システム中立性要件

従前または今後の調達における導入機器との相互接続性を確保するため、原則として国際規格及び日本工業規格等のオープンな規格に準拠していること。

4.5. 事業継続性要件

「10.1.3. 利用拠点LANに関するSLA項目」にて定めるサービスレベルを満たすこと。

5. 情報セキュリティ要件

設計・開発業者は、以下の権限要件及び情報セキュリティ要件を踏まえ拠点 LAN の設計を行っている。受注者においても、以下の要件を前提に作業を行うこと。

5.1. 権限要件

表 5.1-1　利用者とアクセス権限

項番	機能	利用者の区分	アクセス権	補足
1	導入機器管理機能	拠点 LAN 保守担当者	更新可	導入したネットワーク機器の設定変更や機能診断など管理作業の実施を想定

5.2. 情報セキュリティ対策

表 5.2-1　リスクと対策

項番	リスク区分	リスクの概要と対策
1	不正ログイン	拠点 LAN 保守担当者以外の者がログインして、管理者権限により不正に機器の設定を変更されることのないよう、パスワードによる認証機能を利用する。
2	リモートログイン通信の盗聴	拠点 LAN 保守担当者が機器にリモートログインをする際、その通信を盗聴され、管理者パスワード及び設定情報が漏洩しないよう、SSH によるリモートログイン通信の暗号化を利用する。