

ヒアリング評価基準

| 評価観点 | | 評価基準 | 配点 | 比重 | 配点方法等 | |
|------|---------------------|---|---|------|-------|---|
| No | 評価項目 | 評価項目 | | | | |
| 1 | 提案する新ネットワークの構成/構築体制 | <p>・管理体制が不十分で設計、構築後の確認不足があり仕様通りになっていない。</p> <p>・インシデント発生後、対応計画がなく、状況説明がない。そのため、年単位で解決されないインシデントが多々積み上がった</p> | <p>(1) 提案する新ネットワークは、他社との違い（特徴）があるか、現行より簡素化できるか。</p> <p>(2) 新ネットワークを導入した際の効果(都産技研へのメリット)は何か。</p> <p>(3) 上記(1)と(2)は、根拠などが示されて理論的に説明されているか。</p> <p>(4) 構築時に、障害や遅れが生じた際のサポート・バックアップ体制など、企業として人員を増加して期限内に完了できる体制があるか。</p> <p>(5) 受注者側の連携体制（チーム間での情報共有等）について明確化できているか。連携が取れているか</p> <p>(6) 類似業務の実績があるメンバで体制が構成されているか</p> <p>(7) プロジェクトマネージャ、プロジェクトメンバは業務に対する知識が十分であるか</p> | 60点 | 20.0% | <p>・絶対評価とする</p> <p>・配点</p> <p>A : 非常に良い (100%配点)</p> <p>B : 良い (75%配点)</p> <p>C : 普通 (50%配点)</p> <p>→必要最低限の記載があるレベル</p> <p>D : 悪い (25%配点)</p> <p>E : 非常に悪い (0点)</p> |
| 2 | 運用・管理の効率化(デモ含む) | <p>・端末に、IEEE802.1x認証の証明書を展開するために、端末を一度MACアドレス認証により産技研ネットワークに参加させる必要がある。</p> <p>・ネットワーク機器専用のコマンドの知識がないと設定や調査が行えない。</p> <p>・機器の設定が本部と支所で方式が違う。</p> <p>・管理している端末の接続場所が特定できず、端末がどの場所にあるか解らない。</p> | <p>(1) デモンシナリオは、業務を考慮したシナリオになっているか。</p> <p>(2) 運用・管理をする統合管理の画面やメニューの構成が直観的か、マニュアルを参照しなくても操作できるか、ショートカット機能が使えて操作負担を軽減できるか。GUIでも操作が完結できるか。</p> <p>(3) 統合管理の一画面における情報量が適切でみやすいか。画面構成に一貫性があるか。画面のフォントの大きさなどは変更できるか。</p> <p>(4) 統合管理は、画面上で管理している機器の設定を行えるか。</p> <p>(5) 統合管理は、機器の障害を検知した場合に、画面にアラートが上がるか。また管理者にメールが送られているか。</p> <p>(6) 画面上で、拠点毎や拠点間など分けて表示ができるか。また、拠点を跨った機器をグループ化して、グループ単位表示および一括設定や監視ができるか。</p> <p>(7) 統合管理は、管理している機器をクリックなどしてステータスが表示できるか。機器交換時にネットワークに接続するだけで自動設定ができるか。</p> <p>(8) APIやプログラム言語で機器の設定や管理の自動化ができるか。</p> <p>(9) 統合管理は、操作に不慣れな職員の運用・管理業務を補助するような機能があるか。設定ミス防止する機能があるか。</p> | 110点 | 36.7% | 同上 |

| 評価観点 | | 評価基準 | 配点 | 比重 | 配点方法等 | |
|------|--------------------|--|--|------|-------|------|
| No | 評価項目 | 現行ネットワークおよびプロジェクト進行上の課題 | | | | 評価項目 |
| 3 | セキュリティ対策 (デモ含む) | <ul style="list-style-type: none"> ・セキュリティの設定が製品毎で管理や確認が煩雑。 ・産技研ネットワークへの接続する際の検疫システムが運用できていない。 ・不正な端末の産技研ネットワークへの接続の発見に時間がかかる。 ・インシデントレスポンスの切り分けの際、端末での操作を把握できていない ・デジタル化の推進に伴い、SaaSをアカウントに応じたアクセス制御ができず、個人アカウントも利用できてしまう。 Microsoft365を運用しているが機能を活かしきれていない。 | <ul style="list-style-type: none"> (1)デモンナリオは、業務を考慮したシナリオになっているか。 (2)セキュリティ設定は、一箇所で設定でき管理できるようになっているか。GUIでも操作が完結できるか。 (3)セキュリティ設定の画面やメニューの構成が直観的か、マニュアルを参照しなくても操作できるか、ショートカット機能が使えて管理者の操作負担を軽減できるか (4)一画面における情報量が適切でみやすいか。画面構成に一貫性があるか。画面のフォントの大きさなどは変更できるか。 (5)操作に不慣れな職員の運用・管理業務を補助するような機能があるか。設定ミスを防止する機能があるか。 (6)不正端末を検知して、通信遮断または隔離用VLANに自動で移動できるか。また管理者にメールを送れているか。 (7)SaaS毎に制御ができ、個人アカウントの利用許可・拒否、オンラインストレージへのアップロード・ダウンロードが、自宅、産技研内などの場所ごと制御できているか。不正なダウンロードやアップロードを行った端末を特定することができるか。 (8)外部ソリューションと連携して、セキュリティを強化できる機能があるか。 (9)操作に不慣れな職員の運用・管理業務を補助するような機能があるか。設定ミスを防止する機能があるか。 | 110点 | 36.7% | 同上 |
| 4 | 追加提案 | | 都産技研に有用な提案(コスト削減や人員削減など)であって、他事業者との比較優位性があるか。 | 20点 | 6.7% | 同上 |

300点 100.0%