

別紙 1

番号	理想	問題	課題
1	誰が見ても分かりやすく、誰が担当になっても運営できるネットワーク等整備	機器の都度追加等により、ネットワーク全体として見た時に最適化されていない。	ネットワーク全体の見直しと最適化
2		ネットワーク構成等がブラックボックス化されている。	ネットワークの見える化
3		ネットワーク機器で耐用年数が過ぎているスイッチ等機器がある。	スイッチ等の更新
4		ネットワークや端末を含む情報システムに関することが、適切に引き継がれずに組織として共有されていない。	業務が属人化しない環境の構築
5		ネットワークや端末を含む情報システムに関することが、担当者個人の能力に頼ってしまっている状態である。	最低限の知識で容易に管理対応できる環境の構築
6		端末へのソフトウェア等インストールする際に、容易に各端末へ配信できず、個別での対応や、業者へ依頼している。	職員が容易に各端末へ配信等できる環境の構築
7		資産管理ソフト（Asset View）を導入しているが、三層対策に伴う外部記憶媒体の管理目的で主に導入使用しているため、ネットワークや端末を含む情報システム資産管理が適切にできておらず、把握できていない（運用できていない）。	情報システム資産の洗い出しと再整理。
8			ネットワークの見える化と合わせた、情報システム資産管理方法の抜本的な見直し
9		職員の権限等について、全庁的な認証基盤（ActiveDirectory 等）等による管理をしておらず、各システムの権限は、各システムごとに管理しているため、人事異動に伴う権限変更などに時間を要してしまう。	一元管理できるよう、統一的な権限管理環境の構築。
10	職員減少下にあっても、最少人数で、品質と持続性の高い業務環境を確保するため、セキュリティや利便性、先進性、可用性の観点からのネットワーク等整備	インターネット接続系での業務やサービスが増えているが、 α モデルにより手間がかかっている。	現状使用しているシステムと、今後を踏まえて α' 及び β' モデル等の検討
11		主に共有フォルダやメールサーバ等を含む仮想基盤の耐用年数が過ぎている一方で、災害時やテレワーク等を見据えてのクラウド化の検討ができていない。	サーバのクラウド化や、本クラウド化活用検討も含めての更新
12		共有ファイルサーバの統一的なルールもなく、階層もバラバラとなっているため、必要な情報に辿り着くのに時間を要する。	統一的なルールや制限等仕組みの構築
13			ファイル等データ管理の抜本的な見直し。
14		無線利用において、本庁の会議で使用する2部屋（LANポート有）にアクセスポイントがないため、通信が安定しない。	アクセスポイントの設置

15	急速に変化するサイバー空間を巡るリスクも踏まえた情報セキュリティ対策	本庁において、停電時は非常用電源に切り替わるが、切り替わるラグが数秒発生する。サーバ類についてはUPSを設置しているが、ルータやスイッチ等は電源が切れてしまう。	停電時から非常用電源に切り替わるにおいても業務が継続できる環境の構築
16		外部持ち出し用の端末や環境がないため、出張時は自前の端末等を使用している。	出張時に使用できる、セキュリティを確保した端末や、作成した資料等のデータを受け渡しできる仕組みの構築。
17		端末のユーザー管理については、少数のユーザーを使用している	1人1ユーザー体制の構築
18		境界防御に頼っている。	ゼロトラストアーキテクチャの考えに基づくセキュリティ導入の検討
19		ファイルサーバーのバックアップ環境がオンプレミスのため、庁内でのインシデントや災害発生時にバックアップ含めて被害を受ける可能性がある。	オンプレミスとクラウドで分けるなど、BCPを考慮した冗長構成の構築。