【セキュリティポリシー適合チェックリスト】

1．自治体機密性２（※１）以上の情報資産の利用		市情報セキュリティポリシー等
1.1	（利用範囲）業務での利用を目的としていますか	対策基準4.2オ(1)
1.2	（権限）情報へのアクセス権限及び利用権限を適切に定めていますか	対策基準4.2オ(2)
1.3	（送信、USB等による持出し）神戸市の許可を得て暗号化対策（CRYPTREC 暗号リストの「電子政府推奨暗号リスト」※２に記載されている方式を利用すること）の上で送信等する運用になっていますか	対策基準4.2オ(3) 対策基準4.2キ(1)④
2．自治体機密性２以上の情報資産の運搬		
2.1	（USB等）情報を媒体等で運搬する場合、必要最低限の情報のみを鍵付きのケース等に入れて運搬し、利用後は当該情報を速やかに削除する運用になっていますか	対策基準4.2キ
3．適正な回線の使用		
3.1	適正な回線（閉域イーサネット、専用線、IP-VPN等の閉域網）を使用していますか（※３）	対策基準6.3.5
3.2	インターネットVPNを使用して、システムまたは外部サービスを利用しますか（※３）	対策基準6.3.5
3.3	インターネット回線（TLS 通信）を使用する場合、TLS回線のバージョンは、1.2以上を使用していますか	仕様書11(2)
3.4	インターネット回線（TLS 通信）を使用する場合、利用するシステムまたは外部サービスで、ファイアウォール、WAF、IP アドレス制限、多要素認証等の付加的なセキュリティ対策が実施されていますか（※３）	対策基準6.3.5
3.5	Web会議,監視カメラや対策基準8.1.14の特定用途機器で、インターネット回線を利用する場合は、TLS通信を使用していますか	仕様書11(2)
4．執務区域外における遵守事項（モバイル端末等）		
4.1	（情報漏えい対策）端末の盗難防止や覗き見防止（フィルター装着等）を行っていますか	対策基準7.1.1オ(3)(4)
4.2	（個人情報）大量の保有個人情報又は要配慮個人情報を取扱わないこととしていますか	対策基準7.1.1オ(2)
4.3	（データ保存先）原則として端末内にデータを保存しないこととしていますか	対策基準7.1.1オ(6)
4.4	（印刷）原則として自治体機密性２以上の情報の印刷を行えないようになっていますか	対策基準7.1.1オ(8)
4.5	（紛失・盗難対策）パスワードによる端末ロックの設定および管理システム（MDM）を導入していますか	対策基準6.4.4エ
5．外部の者（市民等。委託業務従事者を除く。）が利用するシステム（※４）		
5.1	（市のネットワークとの分離）市のネットワークと物理的に分離していますか	対策基準8.1.10ア
6．外部サービス（クラウドサービス）（※委託事業者がクラウドサービスを利用する場合を含む）		
6.1	外部サービス要件の必須項目を満たしていますか。	外部サービス要件
7．情報資産・機器の廃棄等		
7.1	機器内部の記憶装置から 全ての情報を消去の上、復元不可能な状態にする措置を講じるよう仕様等に記載していますか	対策基準4.2ケ、6.1.7
8．ログの取得等		
8.1	各種ログ及び情報セキュリティの確保に必要な記録を取得、1年以上保存するようになっていますか	対策基準8.1.7ア
8.2	システム開発・保守に関連する資料及びシステム関連文書を適正に整備・保管していますか	対策基準8.3.7ア

※１　「神戸市情報セキュリティポリシー（対策基準4.1.1 機密性）」参照
※２　電子政府推奨暗号リスト
　　https://www.cryptrec.go.jp/list/cryptrec-ls-0001-2022r1.pdf
※３　3.1、3.2、3.4のいずれかの要件を満たすこと
※４　「委託契約仕様書　６（５）システムの整備」に規定する「相談用システム」を指します