別紙１

導入・構築時の情報セキュリティ対策

１　アクセス制御について

（１）受注者は、特権が付与されたアカウントを作成し、これによりシステム接続する際は、強化された認証技術（多要素認証等）を用いること。

（２）受注者は、サービスに影響を与える操作の特定と誤操作を抑制するため、手順書を作成すること。また、誤操作を認識可能なアラート等の実装を検討すること。

（３）受注者は、外部サービス（ソフトウェア・アプリケーション提供サービスやクラウドサービス等）上で構成される仮想マシンに対して適切なセキュリティ対策を行うこと。

２　設計・設定及び開発

（１）受注者は、想定される脅威やリスクに対するセキュリティ対策を検討し、その内容を踏まえたセキュリティ対策を行うこと。

（２）受注者は、監査及びデジタルフォレンジックに必要となるログ等の情報（デジタル証拠）について、府の監査の実施や漏洩等の事業の原因究明のため、府の指示に基づき可能な限り情報提供を行うこと。

（３）受注者は、外部サービス上に他ベンダーが提供するソフトウェア等を導入する場合は、そのソフトウェアの当該サービス上におけるライセンス規定を確認し、規定に違反することなく適切に運用ができるようにすること。

別紙２

運用・保守時の情報セキュリティ対策

１　利用方針

（１）受注者は府と責任分界点について協議を行い、府と合意を得た上で運用すること。
（２）受注者は、府と協議の上、利用承認を受けた外部サービスを利用すること。
（３）受注者と府は協議の上、情報セキュリティインシデント発生時の連絡体制を構築し、双方で共有すること。

２　教育

（１）受注者は利用する外部サービスの手順書を定め、職員に周知すること。
（２）受注者は、情報セキュリティリスクとその対策について職員に共有をはかること。

３　アクセス制御

（１）受注者は、リソース設定を変更するユーティリティプログラムを使用する場合は、その機能の確認と利用できる者を制限すること。
（２）受注者は、不正な利用を監視（業務時間外の利用等を外部サービスに対するアクセスログで確認等）すること。

４　暗号化

（１）受注者は、外部サービス上に情報資産（データ）を保存する場合、暗号化の仕組みや暗号化に使用する鍵の管理方法について確認し、必要に応じて府へ共有すること。
（２）受注者は、鍵管理機能を利用する場合、鍵の生成から廃棄に至るまでのライフサイクルにおける仕組みについて、府に報告を行い、リスクがないことの説明を行うこと。

５　不正プログラム対策、脆弱性管理

（１）脆弱性管理の手順について、受注者と府は協議を行い、受注者が書面を作成の上、府の合意を得ること。

別紙３

更改・廃棄時の情報セキュリティ対策

１　利用終了時における対策

（１）受注者は、移行計画書又は終了計画書を作成すること。

２　取り扱った情報の移行・廃棄

（１）受注者は、外部サービスで利用する全ての情報について、適切に移行及び削除されるよう管理すること。

（２）受注者は府と協議の上、取り扱う情報の機密性（資料４　情報管理レベル）に応じて移行もしくは廃棄方法を決定すること。（暗号化消去及び廃棄証明書の提出等。）データ廃棄の詳細については仕様書「１８．センター運営のための要件（３）カ」によるものとする。

（３）受託者は上記（１）（２）の内容について文書を作成し、府の承認を得ること

（４）受注者は、装置等の資源を処分・廃棄する場合、セキュリティを確保した対応となるよう、その方針及び手順について、文書で府に提出し承認を得ること。（受注者が利用者に提供可能な第三者による監査報告書や認証等を取得している場合、その監査報告書や認証等の提出をもって変えることもできる。）

３　利用のために作成したアカウントの廃棄

（１）受注者は、作成した利用者の各アカウントを削除すること。

（２）受注者は、利用したシステム管理者特権アカウントを削除（又は返却）すること。

（３）受注者は、利用者のアカウント以外に特殊なアカウントがある場合は、関連情報（資格情報等）含めて廃棄すること。

（別紙４）

［参考］情報管理レベル

業務実施に当たり、府民等から各種情報を収集することが想定される。それらの情報については情報セキュリティ要綱に定める区分に従って保管・運用すること。

区分	想定される情報	保管が想定されるシステム
機密性３	・氏名 ・住所 ・電話番号 ・メールアドレス ・通話録音データ ・録音メモ ・過去の問い合わせ内容や対応履歴 ・申出本人による要配慮個人情報（持病等） ・問合せ内容 ※例示であり、これ以外の情報も機密性３に該当する場合あり	・電話交換機 PBX 内（録音データ） ・府民の声システム ・応対履歴システム ・お問合せフォーム ・音声認識システム ※例示であり、それ以外のシステムも含まれる可能性あり。
機密性２	・法人の取引先名 ・企業の今後の事業方針 ・法人固有の技術に関する情報 ※例示であり、これ以外の情報も機密性２に該当する場合あり	同上
機密性１	・機密性３、機密性２に該当しない情報	同上

※機密性３：業務で取り扱う情報のうち、個人情報・法令秘情報等、秘密保全の必要性が高い情報

※機密性２：業務で取り扱う情報のうち、行政機関の保有する情報の公開に関する法律(平成 11 年法律第 42 号) 第５条各号における不開示情報に該当すると判断される蓋然性の高い情報を含む、公表することを前提としていない情報

※機密性１：公表済みの情報や公表しても差し支えない情報等、機密性２情報又は機密性３情報以外の情報