（添付資料－4）

セキュリティ遵守事項

受託者は、導入･運用に係るセキュリティを維持するために下記事項を遵守しなければならない。

1 情報資産管理

(1) 帳票及び可搬記憶媒体（以下「媒体」という。）の管理は、次のとおり行うこと。

① 担当者が利用する媒体を適切に管理させること。

② 個人情報等が含まれる媒体については、利用制限について定めるとともに、次に掲げる取扱いを遵守すること。

ア 施錠可能なロッカー、キャビネット等に保管すること。

イ 利用者は、必要最小限の者に限定すること。

ウ 格納された情報を複写する場合は、情報セキュリティ責任者の許可を得ること。

エ 媒体の廃棄にあたっては、読み取りが完全に不可能な措置（磁気処理による消去又は裁断等）を講じること。

オ その他、個人情報の保護等の観点から、厳格な取扱いを行うこと。

③ その他

ア 職務時間内外にかかわらず、媒体を放置しないこと。

イ 媒体を保管する書庫等は、利用しない場合、必ず施錠すること。

(2) システム機器の管理は、次のとおり行うこと。

① システム機器に関する管理体制と管理責任を、あらかじめ明確にしておくこと。

② システム機器の移送時には、情報システム機器内に格納されている情報が保護されるよう、対策を講じること。

③ システム機器の盗難防止対策を講じること。

④ 情報システム機器に、地震による機器の転倒等を防止する方策を講じること。

⑤ 停電対策として、サーバ等には無停電電源装置（ＵＰＳ）を設置すること。

(3) 住民に公開する情報資産は完全性を確保すること。

2 ガイダンスドキュメント

(1) システム管理者向けの管理者マニュアルには、次の項目を記載すること。

① 管理者用機能

② 管理機能の操作手順

③ 管理機能と権限についての注意事項

④ 安全な環境を維持するための前提条件

(2) 利用者向けの利用者操作マニュアルには、次の項目を記載すること。

① 利用者用機能

② 利用時の操作手順

③　利用者が使用可能な機能と権限についての注意事項
④　安全な運用に必要な利用者の責任

3　テスト

(1) テスト計画を作成し、セキュリティ機能の正常動作を確認すること。
セキュリティ機能については、特に以下の機能を想定している。
①　暗号化
②　電子証明書等の認証
③　不正侵入検知
④　不正改ざん検知
⑤　ウィルスチェック
⑥　サーバ室の入退室管理
(2) テスト実施時には、試験計画書を作成すること。
(3) テスト結果により、セキュリティ機能が仕様どおり動作したことを確認すること。
(4) セキュリティ機能をすべてテストしたことについて、承認を得ること。
(5) システムの導入が既存システムに影響を及ぼさないことを確認すること。
(6) 本番データをテストデータとして使用しないこと。
(7) 業務上やむを得ず本番データを使用する場合は、利用範囲と利用目的を明確にし、当該本番データ管理部門の情報セキュリティ責任者の許可を得ること。許可を受ける場合にはテスト手順を作成し、次の保護対策を講じること。
①　テストデータの管理は管理責任者を定め、管理責任者が行うこと。
②　テスト完了後、テストで使用した本番データを削除すること。

4　運用操作手順

(1) システムの運用手順の作成・管理に関する実施体制と管理責任を明確にすること。
(2) システム運用手順の作成及び改正には、システム管理者の承認を得ること。
(3) システム関連のドキュメントは、安全に保管すること。
(4) システム運用手順には、正確に運用を実行するため、少なくとも次の項目について、適切な指示を記載しておくこと。
①　ファイルの取扱いについて
②　運用スケジュールについて
③　他のシステムとの相互依存について
④　エラー発生時の処理及び運用について
⑤　システムのアクセス制限について
⑥　運用上または技術的な問題が発生した場合の連絡体制について
⑦　重要なデータの管理とその出力について
⑧　失敗したジョブ出力の安全な処分について
⑨　システムが故障した場合の対応について
⑩　運用変更がある場合の手順のメンテナンスについて
⑪　システムログの分析について

⑫　アクセス履歴の記録と確認について
⑬　システムの監視について

5　システムの変更･管理

(1) システムを変更する場合、変更内容・スケジュール・影響等に係る計画書を作成すること。
(2) システム変更にあたっては、システム担当者の意見を聞くこと。
(3) システム変更を行う前に、テスト環境において正常動作を確認すること。
(4) システム変更にあたり、当該システムの運用者以外の者が作業にあたる場合には、事前調整の上、その作業者のシステムへのアクセス権限を、必要な部分に限定すること。
(5) オペレーティングシステム及びアプリケーションソフトウェアの更新に当たり、バージョン管理を行うこと。緊急時対策用に古いバージョンを保持しておき、更新前の実績のある状態を復元できるようにしておくこと。
(6) 実施した変更について、履歴管理を行うこと。

6　事故管理手順

(1) システム運用における事故管理の手順を明確にし、文書化しておくこと。
(2) 事故管理の手順書には、必ず次の項目を記載すること。
　① システムの故障時の対応
　② システムの機能低下によるサービスの損失への対応
　③ データの完全性または不確実性に起因するエラー発生への対応
　④ 外部機関を含めた連絡体制
　⑤ 復旧後の動作確認
(3) 事故の発生、調査結果、回復手段及び再発防止対策について記録し、保存すること。

7　データのバックアップ

(1) データのバックアップの手順書を作成し、管理ミスを最小化すること。
(2) 重要な業務のデータは定期的にバックアップすること。
(3) バックアップの世代管理を行うこと。
(4) バックアップデータを可搬記憶媒体に保管する場合、その媒体を厳重に管理すること。
　① バックアップデータが格納された媒体は、施錠可能な場所に保管すること。
　② バックアップデータが格納された媒体について、保管台帳を作成し、定期的な点検を行うこと。

8　システム保守

(1) システムの定期保守についての手順書を作成すること。手順書には、定期保守後のセキュリティ機能の正常動作を確認するための手順を記載すること。

(2) システムの保守について記録し、履歴を保管すること。
(3) システムの保守作業終了後は、必ずシステム管理者に作業終了の報告を行い、承認を得ること。
(4) システムの保守時には、重要なデータを保護する等の措置を講じること。