# 情報セキュリティ文書体系

**基本方針**

| 対策基準 | 標準 名称 | 標準 内容 | 関連する利用者等 | | | | | | | | | | 手順書 | 関連資料 文書 | 関連資料 記録 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | 統括責任者 | 委員会 | ネットワーク管理者 | 主任 | システム管理者 | 主任 | 運用管理者 | 主任 | セキュリティ責任者 | 管理者 | 職員等 | 委託業務従事者 | | | |
| 第1　組織・体制 | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | ［情報セキュリティ委員会設置要綱］ | |
| 第2　情報資産の分類と管理 | 個人情報の取扱いに関する標準 | 個人情報の取得・利用・保有・提供・電子的結合の制限、個人データの取扱い | | | | | ◎ | ◎ | ◎ | ◎ | | ◎ | ◎ | ◎ | | | 個人情報取扱事務登録簿 |
| | 情報の取扱いに関する標準 | 情報の分類と取得・移送・送信・利用・保管・ﾊﾞｯｸｱｯﾌﾟ・消去・廃棄等の取扱い | | | ◎ | ◎ | ◎ | ◎ | ◎ | ◎ | | ◎ | ◎ | ◎ | | ○○○○の個人情報取扱手順書 | 個人データ収集・利用提供一覧 |
| | 情報資産の取扱いに関する標準 | 情報システム導入・変更時のリスク分析、機器・ソフト・ドキュメント・帳票等の取扱い | 承 | 諮 | ◎ | ◎ | ◎ | ◎ | ◎ | ◎ | | ◎ | ◎ | | | | 情報資産台帳（申請・承認） |
| | リスク管理標準 | 情報資産の重要性評価、脅威・脆弱性・リスク評価、セキュリティ対策の承認 | 承 | | ◎ | ◎ | ◎ | ◎ | ◎ | ◎ | | | | | | | 情報資産のリスクアセスメント（リスクの分析と評価） |
| 第3　物理的セキュリティ | コンピュータ室管理標準 | コンピュータ室の管理運用、入室許可者、作業者の遵守事項 | | | ◎ | ◎ | ◎ | ◎ | | ○ | | | ○ | ○ | | | 入室許可者、入退室記録、作業報告書 |
| | 施錠管理標準 | 施錠室、施錠キャビネット、施錠机、施錠ロッカー等の管理運用 | | | ◎ | | ◎ | | ◎ | | | ◎ | ○ | | | 記録媒体管理手順書 | 鍵管理台帳、記録媒体管理台帳 |
| | 事務室管理標準 | 事務室における機器、保管する情報と管理運用、プリンタ・コピー・FAX設置と取扱い | | | | | ◎ | ○ | ◎ | ○ | | ◎ | ○ | ○ | | ソフトウェア管理手順書 | |
| | 一般区画管理標準 | 共用スペースの管理 | | | | | ◎ | | ◎ | | | ◎ | ○ | | | ドキュメント管理手順書 | |
| | 重要機能室設置標準 | コンピュータ室、サーバ室の設置時におけるセキュリティ対策 | ◎ | | ○ | | ○ | | | | | | | | | 入出力帳票管理手順書 | |
| 第4　人的セキュリティ | | | | | | | ◎ | ◎ | | | | | | | | | |
| 1　情報セキュリティ対策の遵守義務 | | | | | | | | | | | | | | | | | |
| 2　研修・訓練の実施 | セキュリティ研修・訓練標準 | 研修・訓練計画の策定・実施・報告 | ◎ | 承 | ◎ | | ◎ | | ◎ | | | ◎ | | | | | 研修・訓練計画書、実施記録、受講者名簿 |
| 3　事故・欠陥等の報告 | | | | | | | | | | | | | | | | | 事故報告書（予兆・脆弱性含む） |
| 4　アクセスのための認証情報及びパスワードの管理 | | | | | | | | | | | | | | | | 業務概要の確認資料 | |
| | | | | | | | | | | | | | | | | ネットワークアクセスポリシー、フィルタリングシート | |
| 第5　技術的セキュリティ | ネットワーク構築管理標準 | ネットワークの構築、運用、変更、検査、停止、廃止等 | 報 | | ◎ | ◎ | | ○ | | | | | | ○ | | ネットワーク機器等技術仕様書 | 導入計画書 |
| 1　コンピュータ及びネットワークの管理 | サーバ導入管理標準 | サーバの調達、設置、変更、検査、停止、廃棄等 | 報 | | ◎ | ◎ | ◎ | ◎ | | | | | | ○ | | サーバ等技術仕様書 | セキュリティ検査報告書 |
| | 端末装置等設置標準 | 端末装置等の設置・変更・ネットワーク接続・保守・廃棄等 | | | ◎ | ◎ | ◎ | | ○ | | | ○ | ○ | ○ | | クライアントPC技術仕様書 | 保守作業報告書 |
| | | | | | | | | | | | | | | | | ログ取得・管理手順書 | ログ取得状況（サーバ，ネットワーク機器） |
| | | | | | | | | | | | | | | | | バックアップ取得・管理手順書 | バックアップ設定書、処理方法 |
| | | | | | | | | | | | | | | | | ディスク容量確認手順書 | ディスク容量確認資料 |
| | パソコン等利用標準 | 動作環境改変等の禁止事項・変更手続、保存する情報の取扱い等 | | | ◎ | ◎ | | | | | | ◎ | ◎ | | | | |
| | インターネット利用標準 | インターネット利用時の遵守事項、禁止事項等 | | | ◎ | ◎ | | | | | | ◎ | ◎ | | | インターネット利用時の遵守事項 | パソコン等環境設定変更申請書 |
| | 電子メール利用標準 | 電子メール利用時の遵守事項、文書処理、利用申請手続 | | | ◎ | ◎ | | | | | | ◎ | ◎ | | | 電子メール利用時の遵守事項 | Webアクセスフィルタリング解除依頼 |
| 2　アクセス制御 | アカウント管理標準 | ユーザIDの登録・変更・削除、ICカード発行、利用者制限 | | | ◎ | ◎ | ◎ | ◎ | ○ | | | ○ | ○ | | | ICカード管理手順書 | アカウント発行手続一覧表 |
| | | | | | | | | | | | | | | | | | アカウント登録（変更・停止・削除）申請書 |
| | | | | | | | | | | | | | | | | | ICカード発行申請書。ICカード管理DB |
| | ユーザ認証標準 | ユーザ認証システムの導入と管理、パスワードの設定・守秘 | | | ◎ | ◎ | ◎ | ◎ | ○ | | | ○ | ◎ | | | | パスワード設定・利用上の留意事項 |
| | | | | | | | | | | | | | | | | | パスワード再発行申請書 |
| | 無線LAN利用標準 | 原則利用禁止、例外時の無線LANセキュリティ対策 | 承 | | ◎ | | | | | | | | | | | | |
| | モバイルコンピューティング利用標準 | 庁舎外でのパソコン利用時の遵守事項、利用手続 | | | ○ | ○ | | | ○ | | | ○ | ◎ | | | | |
| 3　外部ネットワークとの接続制限等 | 外部ネットワーク接続管理標準 | 情報システムの外部結合時の手続、セキュリティ対策 | 承 | | ◎ | ◎ | ○ | ○ | | | | | | ○ | | アクセス制御仕様書 | 作業報告書、検査報告書 |
| 4　システム開発、導入、保守等 | システム導入標準 | 情報システムの導入（パッケージ選定・委託開発・自己開発）・廃止 | 承 | | ○ | ○ | ◎ | ◎ | ◎ | ◎ | | | | ○ | | パッケージシステム選定技術仕様書 | |
| | | | | | | | | | | | | | | | | | |
| 5　不正プログラム対策 | 不正プログラム対策標準 | コンピュータウイルス等の不正プログラム対策の実施と運用、感染時の対処、報告 | 報 | 報 | ◎ | ◎ | ◎ | | | | | ◎ | ◎ | | | | コンピュータウイルス等不正プログラム報告書 |
| 6　不正アクセス対策 | 不正アクセス対策標準 | 管理する領域と管理標準・手順、アクセス制御・権限管理・記録・分析等 | ◎ | ○ | ◎ | ◎ | ◎ | ◎ | ○ | ○ | | ○ | ○ | | | | 不正アクセス報告書 |
| 7　セキュリティ情報の収集 | セキュリティ情報収集配信標準 | 運用システム・機器・ソフト等のセキュリティ情報収集・配布・対策実施 | | | ◎ | ◎ | ◎ | ◎ | | | | | | | | セキュリティ関連情報入手先一覧表 | |
| | | | | | | | | | | | | | | | | | |
| 第6　運用 | システム運用管理標準 | 情報システムの運用と管理、データ入出力管理、資源管理、利用者支援 | 承 | | ○ | ○ | ◎ | ◎ | ◎ | ◎ | | | | ○ | | ○○○○システム管理手順書 | ○○システム業務運用計画書 | データ等受渡簿、ジョブリスト |
| 1　情報システムの監視 | | | | | | | | | | | | | | | | ○○○○システム運用手順書 | ○○○○システム運用マニュアル | 運用スケジュール表、ジョブサマリー |
| 2　セキュリティポリシー遵守状況の確認 | | | | | | | | | | | | | | | | | ○○○○システム操作マニュアル | 端末装置等操作時間延長届 |
| | | | | | | | | | | | | | | | | | ［危機管理マニュアル］ | システムログ、アプリケーションログ |
| 3　セキュリティ侵害時の対応 | 事故対応標準 | セキュリティ事故の区分と対応手順、緊急時連絡網の整備 | ◎ | ○ | ◎ | ◎ | ◎ | ◎ | ◎ | ◎ | ◎ | ◎ | ○ | | | | 緊急時連絡網 | 障害報告書、事故報告書 |
| | 緊急時対応計画標準 | 業務・情報システムサービスの継続困難な事態への対処 | ◎ | ○ | ◎ | ◎ | ◎ | ◎ | ◎ | ◎ | ◎ | ◎ | ○ | | | | 緊急時対応計画関連事項 | 訓練計画書、訓練実施報告書 |
| 4　外部委託 | 外部委託管理標準 | 委託業務の明確化、委託先の選定、委託契約、委託業務の管理、検収、違反措置 | ◎ | | ◎ | ○ | ◎ | ○ | ◎ | ○ | ○ | ◎ | | ○ | | | 業務委託仕様書、セキュリティ特記仕様書 | 再委託の承諾願、委託業務報告書 |
| 5　例外措置 | | | | | | | | | | | | | | | | | 外部委託の管理事項 | 委託契約書、覚書、誓約書（宣言書） |
| | | | | | | | | | | | | | | | | | | |
| 第7　法令遵守 | 法規制管理標準 | 情報システム基盤、個別業務に関連する法令・ガイドラインへの対応 | | | ◎ | ◎ | ◎ | ◎ | ◎ | ◎ | | | | | | | 関連法令・ガイドライン一覧表 | |
| | | | | | | | | | | | | | | | | | | |
| 第8　懲戒処分等 | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | |
| 第9　評価及び見直し | | | | | | | | | | | | | | | | | セキュリティ監査実施要領 | |
| 1　監査 | セキュリティ監査標準 | 計画策定・調達、監査実施・報告書提出、改善・フォロー | ◎ | ◎ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | | | | セキュリティ監査チェックリスト | 監査計画書、監査報告書 |
| 2　自己点検 | 自己点検実施標準 | 自己点検の実施、評価、報告、改善 | ◎ | 報 | ◎ | ◎ | ◎ | ◎ | ◎ | ◎ | ◎ | ◎ | | | | | 自己点検チェックリスト | 自己点検計画書、自己点検結果 |
| 3　情報セキュリティポリシーの見直し | 是正処置標準 | 監査報告書・事故報告書・障害報告書等に基づく是正処置 | ◎ | ◎ | ◎ | ○ | ◎ | ○ | ◎ | ○ | | | | | | | | 是正処置報告書 |
| | 予防処置標準 | 事故の予兆や脆弱性情報等に基く予防的な処置 | ◎ | ◎ | ◎ | ○ | ◎ | ○ | ◎ | ○ | | | | | | | | 予防処置報告書 |
| | 情報セキュリティ文書管理標準 | 文書の作成・承認・発行・閲覧・配布・保管・改定・廃止等 | 承 | ◎ | ◎ | ○ | ◎ | ○ | ◎ | ○ | | ○ | | | | | 情報セキュリティ文書一覧表 | 文書変更申請・承認記録 |
| | 情報セキュリティ記録管理標準 | 記録の作成・変更・保管・保護・廃棄時の承認、運用 | ◎ | | ◎ | ○ | ◎ | ○ | ◎ | ○ | | | | ○ | | | 情報セキュリティ記録一覧表 | 情報資産の棚卸し・廃棄記録 |