

〇〇〇〇システム実施手順書（雛型）

〇〇〇〇システムの安全管理対策は、「相模原市情報セキュリティ対策に関する規程」及び「情報セキュリティ対策基準」に定める事項のほか、以下の実施手順により行うものとする。

1 情報資産の管理

（１）情報資産の分類

ア 機密性による分類

分類	分類基準	該当
機密性 3	行政事務で取り扱う情報資産のうち、個人情報（公知の情報は除く。）及び機密情報等、情報漏えいにより市民の権利が侵害される、又は業務の遂行に多大な影響を及ぼすおそれがある情報資産	
機密性 2	行政事務で取り扱う情報資産のうち、機密性 3 に相当する機密性は有しないが、直ちに一般に公表することを前提としていない重要な情報資産	<input checked="" type="radio"/>
機密性 1	機密性 2 又は機密性 3 以外の情報資産	

イ 完全性による分類

分類	分類基準	該当
完全性 2	行政事務で取り扱う情報資産のうち、改ざん、誤びゅう又は破損により、市民の権利が侵害される又は行政事務の適確な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報資産	<input checked="" type="radio"/>
完全性 1	完全性 2 以外の情報資産	

ウ 可用性による分類

分類	分類基準	該当
可用性 2	行政事務で取り扱う情報資産のうち、滅失、紛失又は当該情報資産が利用不可能であることにより、市民の権利が侵害される又は行政事務の安定的な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報資産	<input checked="" type="radio"/>
可用性 1	可用性 2 以外の情報資産	

※分類が異なる情報が複数記録されている場合は、最高度の分類を記載してください。

（２）管理責任

本システムに係る情報資産の管理は、〇〇〇〇課長が管理責任を有する。

2 物理的セキュリティ対策

(1) サーバ等の管理

管理項目		管理策
サーバ名		〇〇サーバ・・・〇台 〇〇サーバ・・・〇台
設置場所		に設置
電源の確保状況		
停電対策	無停電源電源装置 (UPS)	<電池交換時期> 直近交換実施時期…〇〇年〇月 次回交換予定時期…〇〇年〇月 <対象機器> <停電補償時間> 〇〇分 <出力容量> 〇〇k v a 以上
	自家発電機 ※推奨事項	有 (発電可能時間：〇〇時間)・無
過電流対策		例) 雷サージ機能付きの UPS を使用
機器の定期保守	実施の有無	
	周期	定期保守は年〇回 (〇月及び〇月) 実施

(2) クライアントP Cの管理

管理項目	管理策
設置場所	に設置
認証方法	

(3) 可搬記録媒体の管理

管理項目	管理策
現物確認	3 か月に 1 回以上は現物を確認する。 <可搬記録媒体管理台帳の保管場所>
持ち出し許可	外部に持ち出す際は、〇〇課長に許可を得る。 <可搬記録媒体持出台帳の保管場所>

(4) プリンタ等の管理

管理項目	管理策
設置場所	に設置

(5) 管理区域の管理

管理項目	管理策
管理区域	<p>を管理区域とする。</p> <p>※事務室内に管理区域を設定している場合は、客観的に管理区域であることが分かるよう、明示すること。</p>
入退出管理方法	<p>例) IC カード</p> <p>※カードの貸出管理簿による入退出管理を行っている</p>
空調管理	例) サーバ室内の温度は 25℃を超えないよう温度管理を行う。
耐震対策	例) サーバは専用ラックに収納し、スタビライザーにより固定。
防火対策	例) 消火器の設置場所・・・〇〇〇〇〇

(6) 通信回線及び通信回線装置の管理

管理対象	管理策
通信回線	<通信回線装置に関する文書の格納場所> _____

(7) 記憶装置を有する情報機器等の廃棄

管理対象	管理策
サーバ、パソコン、ネットワーク機器等	<p>統括情報セキュリティ管理者が指定する場所で、当該機器から電磁的記録媒体を取り外し、データ消去又は、物理的な破壊を行う。</p> <p>※機器をリースしている場合は、契約期間終了後に買取又は無償譲渡し物理破壊を行うか、データ消去後リース会社へ返却することとする。</p>

(8) クライアントパソコンにおける認証

管理項目	管理策
認証方法	<p>例) パスワード及び IC カード</p> <p>※情報システムへのログインに際し、複数の認証情報の入力を行わなければなりません。なお、基幹系の場合は、多要素認証が必須です。</p>

3 人的セキュリティ対策

(1) 教育の実施

ア セキュリティ教育

管理項目	内容
教育の実施予定日	○月
実施責任者	○○○○課長
教育実施者	現システム担当者
受講対象者	新規システム担当者
実施内容・テキスト	例) 本手順書及び情報セキュリティポリシー
教育の効果測定方法	受講者へのインタビューを中心に実施 運用時における理解度チェック

イ 運用管理教育

管理項目	内容
教育の実施予定日	○月
実施責任者	○○○○課長
教育実施者	現システム担当者
受講対象者	新規システム担当者
実施内容・テキスト	例) 運用手順マニュアル

(2) 情報セキュリティインシデントの報告

情報セキュリティインシデントを認知した場合、危機管理手順書を基に対応を行う。

<危機管理手順書格納場所>

電子媒体	
紙媒体	

※危機管理手順書は、常時閲覧できる場所へ保管するものとし、同手順書を保存しているサーバ等が利用不能状態時を想定して、紙媒体を常置する。

<情報セキュリティインシデント記録台帳格納場所>

4 技術的セキュリティ対策

(1) バックアップ管理

ア システムバックアップ管理

管理項目	管理策
実施時期	システム修正時（バージョンアップ含む）
実施手順	自動（ソフト名： ）・手動（手順書格納場所： ）
媒体の種類	
媒体保管場所	
バックアップ ツール名	

イ データバックアップ管理

管理項目	管理策
実施範囲	例）フルバックアップ / 差分バックアップ
実施周期	
実施手順	自動（ソフト名： ）・手動（手順書格納場所： ）
保存期間	〇〇年間分
媒体の種類	
媒体保管場所	
世代管理	例）3世代管理
バックアップ ツール名	

(2) システム運用に関する各種記録等の保管

管理項目	作業記録の保管場所
定期保守作業記録	
システム変更作業記録	
システム仕様書	
システム構成図	
ネットワーク構成図	
障害記録	

(3) ログ取得等

管理項目	保存期間	項目の種類	取得方法
アクセスログ	〇年	例）ログイン ID、ログイン日時、操作内容	
〇〇ログ	〇年		
ログが取得できなくなった場合の対応	例）保守事業者にも速やかに連絡する。（連絡先は危機管理手順書参照）		

(4) 外部ネットワークとの接続制限

外部ネットワークとの接続の有無	有 ・ 無
-----------------	-------

※外部ネットワークと接続がある場合は、必ずDX推進課へ相談し、「外部機関接続申請書」をご提出ください。

(5) アクセス制御

ア 職員による庁外からのアクセス等の制限

庁外からのアクセスの有無	有 ・ 無
--------------	-------

※庁外からのアクセスがある場合は、必ずDX推進課へ相談し、「外部機関接続申請書」をご提出ください。

イ ID及びパスワードは、次のとおり管理する。

(7) 利用者ID

区分	管理方法
ID管理	
パスワード管理	

(イ) 管理者ID（特権ID）

区分	管理方法
ID管理	
パスワード管理	

(6) 情報システム開発・保守等に関連する資料等の整備・保管

管理項目	保存期間	作業記録の保管場所
開発に関連する資料	システム稼働期間	
保守に関連する資料	システム稼働期間	
テストに関連する資料	〇〇年	

(7) 情報システム変更管理

管理対象	管理策
変更管理履歴	<情報システム変更管理履歴の格納場所>

(8) 不正プログラム対策

区分		内容
不正プログラム対策ソフト	サーバ	種類：Windows Defender ライセンス数：〇〇ライセンス 更新方法：D×推進課からネットワークを通じて配信 更新頻度：毎日
	クライアント	種類：Windows Defender ライセンス数：〇〇ライセンス 更新方法：D×推進課からネットワークを通じて配信 更新頻度：毎日
セキュリティホールへの対応		例) 定期保守時に保守業者から OS のアップデート及びセキュリティパッチの適用について説明を受け、必要な対応を行う。

以 上

【改訂履歴】

[illegible]