松戸市情報セキュリティポリシー

目次

第１章　総則

第１節　目的及び定義

（目的）

第１条　このセキュリティポリシーは、松戸市情報システム管理運営規則（平成１９年松戸市規則第６６号。以下「管理規則」という。）第８条の規定に基づき、情報セキュリティ対策について必要な事項を定めるものとする。

（定義）

第２条　このセキュリティポリシーにおいて、次の各号に掲げる用語の意義は、当該各号に定めるところによる。

(1) 市の機関　市長、教育委員会、選挙管理委員会、公平委員会、監査委員、農業委員会、固定資産評価審査委員会、水道事業管理者、病院事業管理者、消

防長及び議会をいう。

(2) 電子情報　本市が保有する情報のうち電子計算機処理するものをいう。

(3) 情報資産　電子情報（当該電子情報の記録媒体を含む。）、電子計算機、ネットワーク（情報システムを相互に接続し、電子情報を交換するための仕組みをいう。以下同じ。）等をいう。

(4) 情報システム　電子計算機、端末装置、通信回線等により電子情報を処理する仕組みをいう。

(5) 情報セキュリティ　情報資産の機密性、完全性及び可用性を維持することをいう。

(6) ネットワーク管理者　管理規則第４条第４項に規定するネットワーク管理者をいう。

(7) システム管理者　管理規則第４条第５項に規定するシステム管理者をいう。

第２節　管理体制

（市の機関の責務）

第３条 市の機関は、このセキュリティポリシーに定めるところにより、情報セキュリティを確保するために必要となる対策を講じなければならない。

２　市の機関において情報システムを管理運営する場合には、セキュリティ対策を確実に実施するため、セキュリティポリシーに基づき、具体的な対策の手順書を策定するものとする。

（統括管理者の任命等）

第４条　市長は、情報セキュリティ対策に必要な組織体制の整備を行うものとする。

２　セキュリティポリシーを全般的に統括するため、情報セキュリティ統括管理者（以下「統括管理者」という。）を置き、副市長をもって充てる。

３　統括管理者の職務を補佐するため、情報セキュリティ副統括管理者（以下「副統括管理者」という。）を置き、総務部長をもって充てる。

４　セキュリティポリシーの実施状況を監理するため、情報セキュリティ管理者（以下「セキュリティ管理者」という。）を置き、別表に掲げる者をもって充てる。

５　業務所管課におけるセキュリティポリシーの実施について、その徹底を図るため、情報セキュリティ実施責任者を置き、業務所管課長をもって充てる。

６　情報セキュリティ実施責任者の職務を補佐するため、業務所管課に情報セキュリティ担当者を置き、情報セキュリティ実施責任者が指定したものをもって充てる。

（実施状況の報告）

第５条　市の機関は、セキュリティポリシーの実施状況を定期的に点検し、その結果を委員会（管理規則第５条に規定する情報システム運営委員会をいう。以下同じ。）に報告しなければならない。

２　委員会は、前項の規定による報告を受けた場合には、その内容の確認及び評価を行い、必要があると認めたときは、当該機関におけるセキュリティポリシーの遵守状況を監査し、その結果を統括管理者に報告するものとする。

３　統括管理者は、前項の規定による委員会の調査結果に基づき、必要があると認めた場合には、セキュリティポリシーの見直しを行うものとする。

（職員の責務）

第６条　職員（非常勤職員及び臨時職員を含む。以下同じ。）は、セキュリティポリシーの重要性を認識し、これを遵守しなければならない。

第２章　対策基準

第１節　電子情報等

（電子情報の管理）

第７条　業務所管課長は、電子情報を作成し、又は取得した場合には当該電子情報を適正に管理するものとする。

（重要媒体の管理）

第８条　業務所管課長は、重要電子情報を内容とする記録媒体（以下「重要媒体」という。）のうち取り出し可能なものについては、重要媒体を安全な場所に保管するとともに、その保管記録を作成しなければならない。

２　業務所管課長は、内容の確定した重要媒体については、新たな書込みを防止するための措置を講じなければならない。

３　業務所管課長は、重要媒体の送付等を行う場合には、重要媒体の複製の防止及び物理的保護のための措置を講じなければならない。

（重要媒体の廃棄）

第９条　業務所管課長は、重要媒体を廃棄しようとする場合には、廃棄の方法、日

時、担当者、電子情報の消去方法等について書面によりセキュリティ管理者の許可を得なければならない。

２　業務所管課長は、前項の場合において、重要媒体に記録されている電子情報を復元不可能な方法により消去しなければならない。

第２節　物理的対策

（管理区域）

第１０条　システム管理者は、重要電子情報を処理する電子計算機を一般事務を行う場所から区分できる場所（以下「管理区域」という。）に設置するよう努めるものとする。

２　システム管理者は、管理区域への不正な立ち入りを防止するため、適切な措置を講じるものとする。

（機器搬入等）

第１１条　システム管理者は、管理区域に新規に情報システムを構成する機器（以下「情報機器」という。）を搬入しようとする場合及び管理区域から既存の情報機器を搬出しようとする場合には、稼働中の情報システムに対する影響について、事前に確認するものとする。

２　システム管理者は、情報機器の搬入及び搬出に際しては、職員を立ち会わせるものとする。

（電源）

第１２条　システム管理者は、停電又は電圧異常により業務処理に支障が生じるおそれのある情報機器については、非常用電源を設置するなど、当該情報機器を適切に停止するよう努めるものとする。

（配線）

第１３条　ネットワーク管理者は基幹系ネットワーク及び情報系ネットワーク（以下「庁内ＬＡＮ」という。）の配線について、システム管理者は所有するネットワークの配線について、損傷等のために必要な措置をとるとともに、定期的に点検を行わなければならない。

２　業務所管課長は、ネットワーク管理者の許可を得ずに庁内ＬＡＮの配線を変更し、又は追加してはならない。

（盗難防止）

第１４条　業務所管課長は、情報資産の盗難防止のため、適切な措置を施さなければならない。

第３節　人的対策

（業務所管課長の遵守義務）

第１５条　業務所管課長は、情報資産が無権限者により使用されることのないよう適切に管理しなければならない。

（情報資産の管理）

第１６条　職員は、業務所管課長が必要と認めた場合を除き、業務以外の目的で情報資産の使用及び外部への持ち出しを行ってはならない。

（ＩＣカード管理）

第１７条　職員は、当該職員に貸与されたＩＣカード（情報システムへのアクセス権限の認証のために用いるカードをいう。）について、適切に管理しなければならない。

（ＩＤ・パスワード管理）

第１８条　職員は、ＩＤ・パスワード（情報システムへのアクセス権限の認証のために用いる符号で、当該職員に付与されたものをいう。）について、適切に管理しなければならない。

（研修等）

第１９条　セキュリティ管理者、業務所管課長及びネットワーク管理者（以下「セキュリティ管理者等」という。）は、職員に対し、セキュリティポリシーの研修を行うものとする。

２　職員は、前項の研修に参加し、知識及び技術の習得に努めなければならない。

（遵守義務の明示）

第２０条　セキュリティ管理者等は、非常勤職員又は臨時職員に対し、その発令時又は雇用契約時にセキュリティポリシーの遵守義務を明示しなければならない。

（外部委託時の措置）

第２１条　市の機関は、情報システムの構築、保守等を外部事業者に委託する場合には、委託契約書中に次に掲げる事項を明記しなければならない。

(1) セキュリティポリシーを遵守すること。

(2) 電子情報の目的外利用及び第三者への提供を禁止すること。

(3) 情報システムに障害が発生した場合の損害賠償に関すること。

(4) その他情報セキュリティの確保のために必要な事項

２　業務所管課長は、外部委託事業者において必要な情報セキュリティ対策が確保されていることを定期的に確認し、必要に応じ、前項の契約に基づき措置しなければならない。

第４節　技術的対策

第１款　情報資産管理

（アクセス履歴等）

第２２条　セキュリティ管理者は、情報資産へのアクセス履歴を記録するよう努め、その窃取、改ざん、消去等を防止するとともに、一定期間保存し、必要に応じ当該履歴を分析するものとする。

２　セキュリティ管理者は、ネットワーク構成図、情報システム仕様書等を無権限者が閲覧できないよう留意し、保管しなければならない。

（処理状況の確認等）

第２３条　システム管理者は、情報システムに係る入出力データの処理状況を常時確認するとともに、定期的にバックアップしなければならない。

（庁内ＬＡＮへの接続）

第２４条　職員は、ネットワーク管理者が指定した情報機器以外の機器を庁内ＬＡＮに接続してはならない。

第２款　アクセス管理

（管理者権限による接続）

第２５条　ネットワーク管理者は、管理者権限による情報システムへの接続時間を情報システムの管理運営上、必要最小限としなければならない。

（外部ネットワークとの接続）

第２６条　ネットワーク管理者は、情報機器を外部ネットワークに接続する場合には、事前に当該外部ネットワークの構成、運用状況、使用機器等を詳細に検討し、既存の情報システムに影響が生じないことを確認しなければならない。

２　セキュリティ管理者等は、外部ネットワークとの接続により情報システムの安全性が脅かされる事態が生じた場合には、速やかに当該接続を物理的に切断しなければならない。

第３款　情報機器管理

（開発環境と運用環境の分離等）

第２７条　システム管理者は、システム開発、保守及びテスト環境とシステム運用環境を分離しなければならない。

２　システム管理者は、システム開発・保守計画の策定時に手順を明確にしなければならない。

３　システム管理者は、移行の際、情報システムに記録されている情報資産の保存を確実に行い、移行に伴う情報システムの停止等の影響が最小限になるよう配慮しなければならない。

（電子情報の消去）

第２８条　セキュリティ管理者は、記録媒体を有する情報機器の修理又は廃棄を外部事業者に委託しようとする場合には、事前に当該記録媒体内の電子情報を全て消去しなければならない。

２　セキュリティ管理者は、前項の電子情報を消去することが困難な場合には、当該外部事業者に守秘義務を課さなければならない。

第４款　ウイルス対策

（ウイルスの侵入防止）

第２９条　ネットワーク管理者及びシステム管理者は、情報機器へのコンピュータウイルスの侵入を防止するため、適切な措置を実施しなければならない。

２　職員は、自己の使用する情報機器へのウイルスの侵入を防止するため、適切な措置を実施しなければならない。

第５款　不正アクセス対策

（不正アクセスの防止）

第３０条　セキュリティ管理者等は、情報システムへの不正アクセス（不正アクセス行為の禁止等に関する法律（平成１１年法律第１２８号）第３条第２項に規定する不正アクセス行為その他無権限者によるアクセス行為をいう。）を防止するため、適切な対策を実施しなければならない。

２　セキュリティ管理者等は、不正アクセスへの対策を実施するにあたっては、警察等関係機関との緊密な連携に努めなければならない。

（記録の保存等）

第３１条　統括管理者及びセキュリティ管理者等は、サーバ等に攻撃を受け、当該攻撃が不正アクセス等の犯罪の可能性がある場合には、攻撃の記録を保存しなければならない。

（情報システムの停止）

第３２条　セキュリティ管理者等は、不正アクセスにより情報システムが重大な影響を受けると認めた場合には、統括管理者に報告するとともに、情報システムを停止しなければならない。

（職員の義務）

第３３条　職員は、情報システムに対する不正アクセスを行ってはならない。

第５節　運用対策

（運用状況の監視）

第３４条　セキュリティ管理者等は、情報システムを正常に稼動させるため、情報システムの運用状況を常時監視しなければならない。

２　セキュリティ管理者等は、前項の監視により得られた記録を安全な場所に保管し、その盗難、改ざん、消去等を防止しなければならない。

（監視権限）

第３５条　セキュリティ管理者は、職員による情報システムへのアクセス及び電子メールの送受信について、監視権限を有する職員及び監視項目を定め、職員に周知しなければならない。

（遵守状況の把握等）

第３６条　セキュリティ管理者は、セキュリティポリシーの遵守状況及び運用上の支障の有無を常に把握しなければならない。

２　セキュリティ管理者は、セキュリティポリシーの運用上の問題点を発見した場合には、速やかに統括管理者に報告しなければならない。

（端末等の利用状況調査）

第３７条　統括管理者及び統括管理者が指名した者は、不正アクセス、不正プログラム等の調査のために、職員が使用しているパソコン等の端末、記録媒体のアクセス記録、電子メールの送受信記録等の利用状況を調査することができる。

（違反者への対応）

第３８条　職員は、セキュリティポリシーに対する違反行為を発見した場合、直ち

に業務所管課長に報告をしなければならない。

２　業務所管課長は、セキュリティポリシーに違反した職員の行為を確認した場合には、セキュリティ管理者に報告するとともに、適切な処置を行うものとする。

（点検計画）

第３９条　業務所管課長は、セキュリティポリシーの実施状況について、定期的又は必要に応じ自己点検を実施しなければならない。

２　業務所管課長は、自己点検の時期、方法、対象範囲等について計画を定めなければならない。

（点検結果の活用）

第４０条　業務所管課長は、自己点検の結果に基づき、実施手順の改善を図らなければならない。

（緊急時対応計画）

第４１条　セキュリティ管理者等は、情報システムに障害が発生した事態に対処するため、被害拡大の防止、情報システムの復旧、再発防止等の措置に関する緊急時対応計画を定めなければならない。

２　セキュリティ管理者等は、所管する該当情報システムの緊急時対応計画を関係職員に周知しなければならない。

（障害の調査及び報告）

第４２条　システム管理者は、情報システムに障害が発生した場合には、その内容、原因、影響の範囲等について調査し、セキュリティ管理者及びネットワーク管理者に報告しなければならない。

（障害の拡大防止）

第４３条　セキュリティ管理者等は、前条の場合において、情報資産の保護のため特に必要と認めたときは、統括管理者に報告するとともに、情報システムを停止するものとする。

（復旧措置）

第４４条　セキュリティ管理者等は、情報システムを復旧する場合には、再発防止のための暫定的措置を講じるとともに、復旧後必要と認められるまでの間、再発の有無を監視しなければならない。

（再発防止措置）

第４５条　セキュリティ管理者等は、情報システムに発生した障害について再発防止措置を講じるとともに、そのリスク分析を実施し、当該措置の有効性を検証しなければならない。

（法令遵守）

第４６条　職員は、職務の遂行において使用する情報資産を保護するために、次に掲げるもののほか関係法令を遵守し、これに従わなければならない。

(1) 地方公務員法（昭和２５年法律第２６１号）

(2) 著作権法（昭和４５年法律第４８号）

(3) 不正アクセス行為の禁止等に関する法律（平成１１年法律第１２８号）

(4) 個人情報の保護に関する法律（平成１５年法律第５７号）

(5) 松戸市個人情報の保護に関する条例（昭和６３年松戸市条例第１０号）

（懲戒処分）

第４７条　セキュリティポリシーに違反した職員及びその監督責任者は、その重大性、発生した事案の状況等に応じて、地方公務員法による懲戒処分の対象とする。

第３章　雑則

（適用除外）

第４８条　このセキュリティポリシーは、学校教育法（昭和２２年法律第２６号）第２条第１項の規定により、市が設置する学校において専ら教育用に用いる情報機器には適用しない。

（補則）

第４９条　このセキュリティポリシーに定めるもののほか、必要な事項は別に定める。

附　則

（施行期日等）

１　このセキュリティポリシーは、平成１９年１１月２６日から施行する。

２　松戸市情報セキュリティポリシー（平成１６年４月１日施行）は、廃止する。

附　則

このセキュリティポリシーは、平成２２年４月１日から施行する。

附　則

このセキュリティポリシーは、平成２２年７月５日から施行する。

附　則

このセキュリティポリシーは、平成２５年４月１日から施行する。

別表（第４条第４項関係）

市の機関名	セキュリティ管理者
市長	総務部長
消防長	消防局長
選挙管理委員会	事務局長
監査委員	事務局長
農業委員会	事務局長
公平委員会	書記長
固定資産評価審査委員会	書記
議会	事務局長
教育委員会	生涯学習部長
病院事業管理者	管理局長
水道事業管理者	水道部長