千葉市住民基本台帳ネットワークシステム・セキュリティ対策要綱

目次

第１章　総則

（趣旨）

第１条　住民基本台帳ネットワークシステムに関し千葉市が行うセキュリティ対策については、住民基本台帳法（昭和４２年７月２５日法律第８１号。以下「法律」という。）並びに千葉市個人情報保護条例（平成７年１０月２日千葉市条例第４２号。以下「条例」という。）及び千葉市電子情報処理規程（平成１４年１２月１２日千葉市訓令（甲）第１０号。以下「規程」という。）に定めるもののほか、この要綱の定めるところによる。

（用語の意義）

第２条　この要綱において使用する用語であって、法律、電気通信回線を通じた送信又は磁気ディスクの送付の方法並びに磁気ディスクへの記録及びその保存の方法に関する技術的基準（平成１４年６月１０日総務省告示第３３４号）又は規程において使用する用語と同一のものは、これと同一の意味において使用するものとする。

２　この要綱において「課」の意義は、千葉市事務分掌規則（平成４年千葉市規則第２号）第１条に定める課及び室（課に置かれる室を除く。）、千葉市事業所事務分掌規則（平成４年千葉市規則第３号。）別表第１に定める第一類の事業所（課を置くものにあっては課）及び第二類の事業所並びに区役所に置かれる課及び市民センター、保健所に置かれる課、児童相談所、会計室及び区役所会計室をいう。

第２章　責任体制

（情報システム管理者等）

第３条　住民基本台帳ネットワークシステムのうち千葉市が管理する部分（以下「住基ネット」という。）のセキュリティ対策を総合的に実施するため、情報システム管理者を置き、市民局長をもって充てる。

２　情報システム管理者は、住基ネットのセキュリティ対策に関し、企画調整局長及び関

係する局長と連絡調整を行うものとする。
３　情報システム管理者を補佐するため、情報システム副管理者を置き、市民局市民部長をもって充てる。

（情報システム責任者）
第４条　住基ネットの適切なシステム管理を行うため、情報システム責任者を置き、市民局市民部区政課長をもって充てる。

（情報セキュリティ責任者）
第５条　住基ネットを利用する課においてセキュリティ対策を実施するため、情報セキュリティ責任者を置き、当該課の長をもって充てる。
２　情報セキュリティ責任者は、本人確認情報、住基ネットにより出力された帳票及び住民基本台帳カードを適正に管理しなければならない。

（セキュリティ会議）
第６条　情報システム管理者は、セキュリティ会議を招集するとともに、議長を務める。
２　セキュリティ会議は、情報システム管理者のほか、次に掲げる者をもって組織する。
（１）情報システム副管理者
（２）情報システム責任者
（３）情報セキュリティ責任者
（４）企画調整局情報システム課長
３　セキュリティ会議は、次に掲げる事項を審議する。
（１）住基ネットのセキュリティ対策の決定及び見直し
（２）前号のセキュリティ対策の遵守状況の確認
（３）監査の実施
（４）教育・研修の実施
４　議長は、前項のうち重要と認められる事項を審議するときは、千葉市情報公開・個人情報保護審議会の意見を聴くものとする。
５　議長は、必要と認めるときは、関係職員の出席を求め、その意見又は説明を聴くことができる。
６　セキュリティ会議の庶務は、市民局市民部区政課において処理する。

（情報セキュリティ責任者に対する指示等）
第７条　情報システム管理者は、セキュリティ会議の結果を踏まえ、情報セキュリティ責任者に対して指示し、又は他の実施機関に対し必要な措置を要請することができる。

第３章　本人確認情報等の管理

（本人確認情報取扱者の指定）

第８条　情報セキュリティ責任者は、本人確認情報を取り扱うことができる者（以下「本人確認情報取扱者」という。）を指名するものとする。

（本人確認情報の取扱上の留意事項）

第９条　情報セキュリティ責任者は、本人確認情報を適正に管理するため、本人確認情報取扱者に対し次の各号に掲げる事項（以下「本人確認情報の取扱上の留意事項）を提示するものとする。

(1) 本人確認情報を画面表示する場合に留意すべき事項
(2) 本人確認情報の整合性を確保する場合に留意すべき事項
(3) 本人確認情報を検索・抽出する場合に留意すべき事項
(4) 本人確認情報を磁気ディスクに保管する場合に留意すべき事項
(5) 本人確認情報を帳票出力する場合に留意すべき事項

２　本人確認情報取扱者は、本人確認情報の取扱上の留意事項を遵守しなければならない。

（出力帳票の取扱上の留意事項）

第１０条　情報セキュリティ責任者は、コミュニケーションサーバから出力した帳票について、次の事項を記録するものとする。

(1) 帳票の名称
(2) 出力年月日
(3) 使用目的
(4) 申請者
(5) 数量
(6) その他必要な事項

２　情報セキュリティ責任者は、保管する帳票について、保管する数量、内訳等を記録するとともに、施錠のできる書庫等に保管し、紛失及び盗難を防止するための措置を講じるものとする。

３　情報セキュリティ責任者は、保管期間の終了等に伴い帳票を廃棄する場合は、前項の記録と突き合わせるとともに、焼却し、溶解し又は裁断することにより、記載内容が判読できないようにして、速やかに廃棄するものとする。

第４章　住民基本台帳カードの管理

（住民基本台帳カードの保管）

第１０条の２　情報セキュリティ責任者は、住民基本台帳カードの券面印刷の有無に関わらず、保管している状態及び枚数を記録し、施錠のできる場所に保管し、紛失及び盗難を防止するものとする。

２　情報セキュリティ責任者は、前項の住民基本台帳カードを紛失し又は盗難された場合は、直ちに情報システム責任者に報告するものとする。

（住民基本台帳カードの廃棄）

第１０条の３　情報セキュリティ責任者は、カード発行失敗（住民基本台帳カードへの初期データの書き込みの失敗又は券面印刷の失敗をいう。）、カード交付申請取消又はカード廃止により住民基本台帳カードを廃棄する場合は、次のとおり行うものとする。

(1) 廃棄する住民基本台帳カードはできるだけ速やかに廃棄する。

(2) 廃棄するまでの間は、廃棄する住民基本台帳カードを厳重に保管する。

(3) 廃棄する住民基本台帳カードは焼却、溶解、裁断等により券面印刷の内容が判別できないようにし、かつ、ＩＣチップを物理的に破壊する。

（住民基本台帳カードの暗証番号の管理）

第１０条の４　情報セキュリティ責任者は、本人確認情報取扱者及び住民基本台帳カード交付申請者に対し、次の事項について周知徹底するものとする。

(1) 住民基本台帳カードの暗証番号は誕生日等、容易に推測できるものを用いないこと。

(2) 暗証番号の入力は、原則として申請者自身が行うこと。

(3) 住民基本台帳カードのカードリーダライタへの抜き差しは、原則として申請者自身が行うこと。

第５章　システムの管理

（耐タンパー装置のセットアップ情報の管理）

第１１条　情報システム責任者は、耐タンパー装置用セットアップディスクを施錠できる保管庫に保管するとともに、耐タンパー装置用パスワードを適正に管理するものとする。

（システムの管理帳票）

第１２条　情報システム責任者は、住基ネットを適正に管理するために、次に掲げる帳票を作成し、変更履歴を記録するものとする。

(1) システム構成表　システムを構成するハードウェアについての一覧表

(2) システム構成図　システムを構成するハードウェアの関係を示した図

(3) 機器管理台帳　住基ネットを構成するハードウェアごとに、管理を行う上で必要となる項目を記載した台帳

(4) ソフトウェア管理台帳　住基ネットで使用するソフトウェアごとに、管理を行う上で必要となる項目を記載した台帳

(5) ネットワーク概念図　コミュニケーションサーバ及び端末機等を含めた住基ネットに関する概念的な図

(6) ネットワーク設定表　住基ネットにおけるネットワークが正常に作動するための設定を記載した表

(7) 取扱者管理台帳　本人確認情報取扱者の所属、職、氏名、権限その他必要事項を記載した台帳

（緊急時の対応）

第１３条　住基ネットのセキュリティを侵犯する不正行為が発生した場合における対応は、千葉市住基ネット緊急時対応計画書（以下「緊急時対応計画書」という。）の定めるところによるものとする。

（ハードウェア管理の留意事項）

第１４条　情報システム責任者は、ハードウェアの障害に関する対策を次のとおり実施する。

(1) 障害が発生しないよう防止対策を講じるとともに、対策が適正に実施されているか確認を行う。

(2) 職員、委託先事業者及び関係機関（以下「関係者」という。）への連絡網を整備し、障害が発生した場合の対応手順を整備するとともに、当該対応手順を関係者に周知徹底する。

(3) 障害が発生した場合には、障害状況の把握及び障害対応を行うとともに、重大な障害については、緊急時対応計画書に基づいて対応する。

２　情報システム責任者は、保守対象機器を明確にし、保守対象機器については、継続して機器が使用できるように、必要な措置を講じなくてはならない。

３　情報システム責任者は、ハードウェアの利用状況を定期的に分析し、その分析結果に基づき、ハードウェアの適正な設置を図るとともに、ハードウェアの導入を計画的に行う。

（磁気ディスクの廃棄等）

第１５条　システム管理者は、磁気ディスクを廃棄し、又は返却する場合は、当該磁気ディスクに記録された情報が、廃棄する過程において第三者に入手されることを防ぐために、物理的破壊、専用ソフトを使用したテータの上書きその他の記録された情報が読み出させない措置を講じるものとする。

２　前項の規定は、耐タンパー装置を廃棄し、又は返却する場合に準用する。

（ソフトウェア管理の留意事項）

第１６条　情報システム責任者は、コンピュータウィルス対策をコンピュータウィルス対策基準（平成７年７月７日通商産業省告示第４２９号）等に基づき行い、コンピュータウィルスに感染した場合には、速やかに適切な措置を講じるとともに、被害状況を指定情報処理機関、情報処理振興事業協会等に報告する。

２　情報システム責任者は、ソフトウェアの保守に関する管理を次のとおり実施する。

(1) ソフトウェアのバージョン管理は、指定情報処理機関の指示に従い実施するものとする。ただし、本市が個別に調達した機器に関しては、この限りではない。

(2) ソフトウェアのバックアップは、不測事態、障害に対応できるように、業務内容及び処理形態に応じて、バックアップの範囲、記録する磁気ディスク、保管方法等につ

いて定めるものとする。この場合において、バックアップしたソフトウェアと運用中のソフトウェアとの整合性・同期性について考慮するものとし、バックアップ及びリカバリ方法は、システムの変更ごとに見直しを行うものとする。

3　情報システム責任者は、指定情報処理機関一括調達ソフト、業務アプリケーションその他の指定情報処理機関が指定するソフトウェア以外で、住基ネットで使用するソフトウェアについて、性能管理を行うものとする。

（ネットワーク管理の留意事項）

第１７条　情報システム責任者は、ネットワークの障害発生の検出、障害発生時対処、障害改修までのフォローアップ、障害直後対応（二次障害防止・障害範囲拡大防止・障害の切り分け）、障害運転時対応（代替運転・縮退運転）、状況に応じた復旧作業、障害原因の調査、障害改修後対応（障害内容の報告・同様障害再発防止策立案・実施）について、必要な措置を講じるものとする。

2　情報システム責任者は、障害予測、定期診断、ログの調査・解析を行いシステムの継続性の向上に努める。

3　情報システム責任者は、ネットワークの保守に関する管理を次のとおり実施する。

(1) 円滑な運用を確保するため、ハードウェア資源の利用状況、回線トラフィック状況等を勘案して適宜、ネットワークについて見直しを行う。

(2) ネットワークの保守等のためネットワークを停止するときは、あらかじめ、セキュリティ責任者及び指定情報処理機関に通知するものとする。ただし、災害、停電等の事由により、通知するのに十分な時間が無いと判断するときには、この限りではない。

4　情報システム責任者は、性能情報及び統計資料の収集と蓄積を行うとともに、蓄積した性能情報の解析を行い、その結果に基づき、パフォーマンス上のボトルネックを検出して、ボトルネックがある場合には、改善措置を講じるものとする。

（オペレーション計画の作成）

第１８条　情報システム責任者は、情報セキュリティ責任者と協議のうえ、次の各号に掲げる計画について、作成するものとする。

(1) 要員計画　情報システム責任者は、一定期間ごとに要員配置計画を策定する。

(2) 運用計画　情報システム責任者は、通常期・ピーク時・大量データ取り扱い時のスケジュールをあらかじめ作成する。また、年次・月次・週次・日次ごとの作業項目、運用時間を決定する。

(3) バックアップの処理計画　情報システム責任者は、バックアップの処理に関して、必要な事項を定める。

(4) 緊急時対応計画　情報システム責任者は、緊急時の対応のために、緊急時対応手順の明確化、緊急時連絡体制の確認、緊急時対応手順の周知を行う。

(5) 計画の見直し等　情報システム責任者は、オペレーションに関する各計画の見直しを必要に応じて行うとともに、障害が発生する確率を下げるために、オペレーション品質の向上対策、オペレーションミスの原因分析、再現防止策の策定・実施・評価を

行う。

（ハードウェアの操作者）

第１９条　情報システム責任者は、次に掲げるハードウェアの操作について、ＩＤカード及びパスワードにより、当該ハードウェアを操作する者（以下「操作者」という。）の正当な権限を確認するとともに、その操作履歴を記録し、７年間保存するものとする。

(1) コミュニケーションサーバ

(2) 端末機

(3) 住民基本台帳カード発行端末

２　情報システム責任者は、適正な権限を持つ必要最小限の操作者を情報セキュリティ責任者の申請に基づき承認するものとする。

（オペレーティングシステムの管理方法）

第１９条の２　情報システム責任者は、コミュニケーションサーバ、端末機、住民基本台帳カード発行端末、電気通信関係装置等のオペレーティングシステムにおいて次に掲げるセキュリティ対策を行うものとする。

(1) ユーザＩＤと操作者の対応づけを行う。

(2) ユーザＩＤに付与する権限を業務上必要最低限のものとする。

(3) 操作者が業務に使用するユーザＩＤについて、業務以外の操作及び設定変更を行えないよう制限する。

(4) ユーザＩＤ及びその権限については、定期的又は必要に応じて見直しを行い不要なユーザＩＤについては、速やかに削除する。

２　情報システム責任者は、ログオンの履歴を記録することとし、定期的又は必要に応じてその履歴を確認し、不正アクセスのない事を確認するものとする。

（操作者用ＩＤカードの管理方法）

第２０条　情報システム責任者は、操作者用のＩＤカードを操作者に貸与するものとし、退職、人事異動等により操作者でなくなったものは、速やかに貸与されたＩＤカードを返却するものとする。

２　情報システム責任者は、ＩＤカードの管理簿を作成するものとする。

３　操作者は、貸与されたＩＤカードを他に貸与し、又は貸与した目的外に利用してはならない。

４　操作者は、貸与されたＩＤカードを紛失し、又は盗難されないように管理しなければならない。

５　操作者は、貸与されたＩＤカードを紛失し、又は盗難された場合は、直ちにシステム管理者に報告し、情報システム責任者は速やかに当該ＩＤカードの失効の手続きをとるものとする。

６　情報システム責任者は、貸与したＩＤカードが適正に使用されているか調査を行うものとし、ＩＤカードを貸与された操作者は当該調査に協力するものとする。

（パスワードの管理方法）

第２１条　情報システム責任者は、パスワードの有効期限を設けるものとする。

２　操作者は、パスワードに規則性のある記号及び番号又は推測可能な記号又は番号を用いてはならない。

３　操作者は、パスワードを漏えいし、又は滅失しないようにしなければならない。

４　操作者は、パスワードを定期的又は必要に応じて随時に変更するものとする。

第６章　指定施設の管理

（指定施設の管理）

第２２条　下表の左欄に掲げる施設において、当該右欄に掲げる方法による入退室管理を行うものとする。

指定施設	入退室管理の方法
重要機器室	情報システム責任者から事前に許可を得た者が、その都度、貸与された入退室管理カードを用いて入室する。この場合において、入室者は名札を着用する。また、入退室に関する記録を行い、当該記録を保存する。
端末機又は住民基本台帳カード発行端末の設置室	情報セキュリティ責任者から事前に許可を得ている者が名札を着用して入室する。

第７章　事務の委託

（セキュリティ対策の実施状況の調査）

第２３条　情報システム責任者及び情報セキュリティ責任者は、必要に応じ、委託先におけるセキュリティ対策の実施状況について調査するものとする。

第８章　委任

（委任）

第２４条　この要綱に定めるもののほか、住基ネットのセキュリティ対策に関し必要な事項は、市民局長が定める。

附　則

この要綱は、平成１４年８月５日から施行する。

附　則

この要綱は、平成１４年１２月１２日から施行する。

附　則

この要綱は、平成１５年８月２５日から施行する。

附　則

この要綱は、平成１７年４月１日から施行する。

附　則

この要綱は、平成１８年４月１日から施行する。

附　則

この要綱は、平成１９年４月１日から施行する。