稲城市住基ネットセキュリティ対策基準

平成14年７月30日
市　長　決　裁

（目的）

第１　この基準は、住民基本台帳法（昭和42年法律第81号）、稲城市電子計算組織管理運営規程（昭和61年稲城市訓令第４号。以下「規程」という）及び住民基本台帳ネットワークシステムのセキュリティ対策基準（平成14年総務省告示第334号）に定めるもののほか、住民基本台帳ネットワーク（以下「住基ネット」という。）の適正かつ円滑な運営を図るため並びに機密性、正確性及び持続性の維持（以下「セキュリティ」という。）を確保するために必要な事項を定めることを目的とする。

（定義）

第２　この基準において、次の各号に掲げる用語の意義は、それぞれ当該各号に定めるところによる。

⑴　条例　稲城市個人情報保護条例（平成15年稲城市条例第25号）をいう。

⑵　電子計算組織　条例第２条第７号に規定する電子計算組織をいう。

⑶　サーバー　ネットワークを通じて端末装置又は他の電子計算組織からの要求に基づき処理をする電子計算組織

⑷　ファイヤーウォール　ネットワークにおいて、外部からの不正侵入を防御する電子計算組織

⑸　ネットワーク機器　ネットワークを構成する機器類のうち、サーバー、端末装置及びファイヤーウォールを除くもの

⑹　コンピュータウイルス　電子計算組織に侵入して、データの破壊、流出等何らかの不正な動作を行う目的で作成されたプログラム

⑺　ワクチンソフト　電子計算組織内のウイルスの検出、駆除及び感染防止をするプログラム

（住基ネット統括者）

第３　住基ネットの対策を総合的に実施するため、住基ネット統括者（以

下「統括者」という。）を置き、副市長をもって充てる。

（住基ネット副統括者）

第４　統括者を補佐するため、住基ネット副統括者（以下「副統括者」という。）を置き、電子情報を担当する部長をもって充てる。

（住基ネット管理者）

第５　住基ネットを確保するため、住基ネット管理者（以下「管理者」という。）を置き、電子情報を担当する課長をもって充てる。

（住基ネット運用管理者）

第６　住基ネットを利用している課においてセキュリティ対策を実施するために住基ネット運用管理者（以下「運用管理者」という。）を置き、住民情報を担当する課長をもって充てる。

（暗証番号管理者）

第７　暗証番号及び操作識別カード（以下「暗証番号等」という。）による対策を行うため、暗証番号管理者を置き、住民情報を担当する課長をもって充てる。

２　暗証番号管理者は、暗証番号等に関する運用基準を作成し、厳正に管理運用しなければならない。

（個人情報の保護）

第８　住基ネットでは、法で定める本人確認情報以外の個人情報を扱ってはならない。

２　管理者及び運用管理者（以下「管理者等」という。）は、個人情報の漏えい、滅失及びき損の防止その他の個人情報の適切な管理のために必要な措置を講じなければならない。

３　住基ネットを電子計算組織と結合する場合は、個人情報の保護及び確保のために必要な措置を講じなければならない。

（会議）

第９　セキュリティ対策を行うため、稲城市住民基本台帳ネットワーク会議（以下「会議」という。）を置く。

２　会議は、次に掲げる事項を掌理する。

⑴　住基ネットの対策の決定及び見直し

⑵　前号の対策の実施状況の確認

⑶　監査の実施

⑷　教育及び研修の実施

３　会議は、次に掲げる者をもって組織する。

⑴　統括者

⑵　副統括者

⑶　管理者

⑷　暗証番号管理者

⑸　運用管理者

⑹　住民情報を担当する部長

４　会議に議長を置き、統括者をもって充てる。

５　議長は、会議を代表し、会務を総理する。

６　会議に副議長を置き、副統括者をもって充てる。

７　副議長は、議長を補佐し、議長に事故あるときは、その職務を代理する。

８　議長は、前項のうち重要と認められる事項を審議する場合は、稲城市個人情報保護運営審議会の意見を聴くものとする。

９　議長は、必要と認めるときは、関係職員の出席を求め、その意見を聴くことができる。

１０　会議の庶務は、電子情報を担当する課において処理する。

（関係部署に対する指示等）

第１０　統括者は、会議の結果を踏まえ、関係部署の長に対し指示し、又は行政委員会等に対し必要な措置を要請することができる。

（電子計算組織との結合）

第１１　管理者は、住基ネットを電子計算組織と結合する場合は第８の３に規定する措置のほか、次の事項を守らなければならない。

⑴　住基ネットは、電子計算組織から独立したネットワークとすること。

⑵　端末装置は共用しないこと。

（電算室等の管理）

第１２　管理者は、サーバー、ファイヤーウォール及びネットワーク機器

（以下「サーバー等」という。）の設置室並びに住基ネットのデータ、情報等の保管室（以下「電算室等」という。）の管理並びに電算室等への入退室の管理に関し、必要な措置を講じなければならない。

２　電算室等に入退室できる者は、管理者から事前に許可を得た者のみとする。

３　管理者は、入退室管理簿を作成し、入退室するものに記録させなければならない。

（入退室管理に係る指示）

第１３　統括者は、適切な入退室の管理が行われているかどうか、管理者等から報告を聴取し、必要に応じて調査を行い、及び必要な指示を行うものとする。

（機器の管理）

第１４　管理者は、住基ネットで使用する機器の管理に当たっては、次の事項を遵守しなければならない。

⑴　不正利用及び不正操作を防止する措置を講じること。

⑵　決められた機器及びプログラム以外は、組み込まないこと。

⑶　サーバー等は、対策を施した電算室に設置すること。

⑷　サーバー等は、対策を施したラックに収容し、決められたもの以外による操作を防止すること。

⑸　住基ネットで使用する機器、プログラム及び磁気媒体を住基ネット構成管理簿（様式第１号）に記載し、構成内容に変更が生じた場合は、速やかにその旨を記録すること。

⑹　ネットワーク構成に関するドキュメントを作成し、構成内容に変更が生じた場合は、速やかに所要の修正を行うこと。

⑺　ファイヤーウォールに使用するプログラム等は、最新のものを使用すること。

⑻　ファイヤーウォールの設定データは、必ず複製をとり、障害等発生時には速やかに回復できるようにすること。

（データ等の管理）

第１５　管理者等は、データ、プログラム及びドキュメントを定められた

場所に保管し、取扱い及び管理に関し必要な措置を講じなければならない。

（暗証番号等）

第１６　管理者等は、機器を操作するもの（以下「操作者」という。）の異動等により暗証番号等の設定、取消し又は変更の必要が生じたときは、速やかに暗証番号管理者に修正を依頼しなければならない。

２　管理者等は、操作者の異動等により不要となった操作識別カードを回収し、暗証番号管理者に返還しなければならない。

３　暗証番号管理者は、暗証番号管理上の理由等から暗証番号等の設定、取消し又は変更の必要が生じたときは、管理者等と協議するものとする。

４　操作者は、暗証番号をみだりに書き留め、若しくは他に漏えいし、又は操作識別カードを他人に貸与する等のデータの保護に支障をきたす行為をしてはならない。

５　操作者は、交代又は離席時には業務を終了し、及び操作識別カードを抜き取り、暗証番号等を不正利用されないよう厳正な運用を行わなければならない。

６　管理者等は、操作識別カードを施錠できる場所に保管し、盗難又は不正に利用されないよう厳正な管理を行わなければならない。

（端末装置の運用）

第１７　操作者は、管理者の許可なく次の事項を行ってはならない。

⑴　決められた機器以外を住基ネットに接続すること。

⑵　端末装置に組み込まれているプログラムを変更し、又は削除すること。

⑶　端末装置に新たなプログラムを追加すること。

⑷　その他セキュリティの確保に支障をきたすおそれのある行為を行うこと。

（住民基本台帳カードの管理）

第１８　運用管理者は、交付前の住民基本台帳カード（以下「住基カード」という。）の盗難その他住基ネットのセキュリティの確保に支障をきたすおそれのある行為を防止するため、使用しないときは施錠できる場所

に保管する等の対策を講じなければならない。

２　運用管理者は、住民から住基カードを回収した場合は、住基カードに記録されている個人情報を再取得できない状態にした上で廃棄処分しなければならない。

（ウイルス）

第１９　操作者は、入手した磁気媒体又は磁気記録を使用する場合は、事前にワクチンソフトを使用しウイルスに感染していないことを確認しなければならない。

２　操作者は、磁気記録を発信する場合は、事前にワクチンソフトを使用し、端末機等がウイルスに感染していないことを確認しなければならない。

３　運用管理者は、ウイルスに感染した磁気記録を入手したこと、又は磁気媒体が感染していることが判明した場合は、ネットワークの接続を遮断し、管理者に感染の経緯を報告するとともに、ウイルスに感染した磁気記録を入手元に連絡しなければならない。

４　管理者は、ウイルス感染した旨の報告を受けた場合は、速やかに運用管理者に連絡し、感染の拡大を防がなければならない。

（操作履歴の記録）

第２０　管理者は、操作履歴を記録し、不正な行為が行われていないかどうか確認しなければならない。

２　管理者は、7年前まで遡って解析できるよう保管しなければならない。

（調査）

第２１　管理者が、住基ネット及び市の保有する情報の適正利用に係る維持管理を目的とした調査を行う場合は、職員はこれに協力しなければならない。

（不正アクセス行為）

第２２　管理者は、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）を遵守し、ネットワークを通じた不正侵入又は暗証番号等の不正利用その他の不正なアクセス行為（以下「不正アクセス行為」という。）を受けないよう対策を講じなければならない。

２　管理者は、不正アクセス行為を受けたときの対応マニュアルを作成しなければならない。

３　運用管理者は、住基ネット又は住基ネットと結合している電子計算組織が不正アクセスを受けたときは、管理者に報告しなければならない。

（外部委託）

第２３　管理者等は、住基ネットに係る個人情報業務を外部に委託しようとするときは、あらかじめ、次の事項を行わなければならない。

⑴　委託を受けようとする者における当該受託に係る情報の保護に関する管理体制について確認すること。

⑵　個人情報に関する委託内容について稲城市個人情報保護運営審議会の承認を経ること。

（委託契約書への記載事項）

第２４　個人情報を処理する事務を外部に委託するときは、その委託契約において次に掲げる事項について定めなければならない。

⑴　個人情報の秘密保持の義務に関すること。

⑵　再委託の禁止に関すること。

⑶　個人情報の目的外使用及び第三者への提供の禁止に関すること。

⑷　個人情報の複写及び破棄に関すること。

⑸　事故発生時の報告義務に関すること。

⑹　前各号に違反した場合における契約解除等及び損害賠償に関すること。

⑺　個人情報の帰属及びプログラムの所有権に関すること。

⑻　その他必要と認めること。

（受託者の管理状況の調査）

第２５　管理者等は、必要に応じて外部委託に係るセキュリティ対策の実施状況に関する調査を実施するものとする。

（故障発生時の措置）

第２６　保守作業の実施にあたっては、実施者は、管理者の指示に基づき行うものとする。

（障害対策マニュアル）

第２７　管理者は、システムの障害発生時における作業手順を定めた障害対策マニュアルを作成し、対処するものとする。

（災害又は緊急時における対応）

第２８　運用管理者は、災害又は緊急事態が発生した場合は、直ちに管理者に連絡し、その指示により対処するものとする。

（火災の防止）

第２９　管理者等及び職員は、火災によるシステムの構成機器又は関連設備の損傷を防止するため、煙感知器その他の検知装置及び消火設備その他の保安設備を活用し、火災による被害の拡大を防がなければならない。

２　前項の火災が発生した場合は、運用管理者は、直ちに被害の状況を管理者に報告しなければならない。

（地震及び落雷時の対応）

第３０　管理者等は、比較的大規模な地震若しくは落雷による停電その他の災害により、システムの構成機器若しくは関連設備の損傷又はデータ破壊が生じるおそれのあるときは、直ちにシステムを終了し、端末装置の電源を切断するものとする。

２　前条第２項に定めた規定は、前項の場合に準用する。

（委任）

第３１　この基準に定めるもののほか、必要な事項は、市長が別に定める。

付　則

この基準は、平成14年８月５日から施行する。

付　則

この基準は、平成19年４月１日から施行する。ただし、第２第１号、第２第２号、第８第８項及び第22第２号は、平成15年７月１日から適用し、第８第10項は、平成18年４月１日から適用する。

付　則（平成24年３月30日市長決裁）

この基準は、市長決裁日から施行し、平成23年４月１日から適用する。

付　則

この基準は、令和３年４月１日から適用する。