

所沢市訓令第 15 号

庁中一般

所沢市住民基本台帳ネットワークシステムセキュリティ規程を次のように定める。

平成14年 7 月 26 日

所沢市長 斎藤 博

所沢市住民基本台帳ネットワークシステムセキュリティ規程

目次

- 第1章 総則 (第1条・第2条)
- 第2章 組織 (第3条―第8条)
- 第3章 入退室管理 (第9条―第13条)
- 第4章 アクセス管理 (第14条―第18条)
- 第5章 情報資産管理 (第19条―第21条)
- 第6章 委託管理 (第22条―第25条)
- 第7章 教育 (第26条)
- 第8章 監査 (第27条)
- 第9章 緊急時の対応 (第28条・第29条)
- 第10章 雑則 (第30条)

附則

第1章 総則

(趣旨)

第1条 この訓令は、住民基本台帳ネットワークシステム (以下「住基ネット」という。) のセキュリティの確保に関し必要な事項を定めるものとする。

(用語)

第2条 この訓令において、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。

- (1) 本人確認情報 住民基本台帳法（昭和42年法律第81号）第30条の5第1項に規定する本人確認情報
- (2) コミュニケーションサーバ（以下「CS」という。） 都道府県知事に本人確認情報の通知及び転出確定通知を行うための電子計算機
- (3) CS端末 CSに接続ができる電子計算機
- (4) 操作者用ICカード 住基ネット業務アプリケーションの利用を可能とし、操作権限を限定するICカード
- (5) データ 住基ネットにおいて通知され、記録され、保存され、又は提供される情報
- (6) 情報資産 住基ネットに係るすべての情報並びにソフトウェア、ハードウェア、ネットワーク及び磁気ディスク
- (7) アクセス管理 操作者用ICカードを利用した、CSへの接続に係わる管理方法

第2章 組織

（セキュリティ統括責任者）

第3条 住基ネットのセキュリティ対策を総合的に実施するため、セキュリティ統括責任者を置く。

2 セキュリティ統括責任者は、総合政策部長をもって充てる。

（セキュリティ統括副責任者）

第4条 セキュリティ統括責任者を補佐するため、セキュリティ統括副責任者を置く。

2 セキュリティ統括副責任者は、セキュリティ統括責任者に事故あるとき、又はセキュリティ統括責任者が欠けたとき、その職務を代理する。

3 セキュリティ統括副責任者は、総合政策部情報統計課担任次長をもって充てる。

(システム管理者)

第5条 住基ネットの適切な管理を行うため、システム管理者を置く。

2 システム管理者は、情報統計課長をもって充てる。

(セキュリティ責任者)

第6条 住基ネットを利用する部署においてセキュリティ対策を実施するため、セキュリティ責任者を置く。

2 セキュリティ責任者は、市民課長、コミュニティ推進課長、出張所長及び市民課サービスコーナー所長をもって充てる。

(セキュリティ会議)

第7条 セキュリティ統括責任者は、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、セキュリティ統括責任者のほか、次に掲げる者をもって組織する。

- (1) セキュリティ統括副責任者
- (2) システム管理者
- (3) 管財課長
- (4) コミュニティ推進課長
- (5) 市民相談課長
- (6) 市民課長

3 セキュリティ会議は住基ネットについて、次に掲げる事項を審議する。

- (1) セキュリティ対策の決定及び見直しに関すること。
- (2) セキュリティ対策の遵守状況の確認に関すること。
- (3) 監査の実施に関すること。

(4) 教育・研修の実施に関すること。

(5) その他議長が必要と認めること。

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、所沢市情報公開・個人情報保護審議会の意見を聴くものとする。ただし、緊急の対応が必要な場合は、事後報告とすることができる。

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、総合政策部情報統計課において処理する。

(関係部署に対する指示等)

第8条 セキュリティ統括責任者は、セキュリティ会議の結果を踏まえ、関係部署の長に対し指示し、又は教育委員会等に対し必要な措置を要請することができる。

第3章 入退室管理

(入退室管理を行う室)

第9条 次に掲げる住基ネットの運用が行われる室において、それぞれのセキュリティ区分に応じた、入退室管理を行うものとする。

セキュリティ区分	室
レベル2	住基ネットのデータ、セキュリティ情報等の保管室 CS、ネットワーク機器等の設置室
レベル1	CS端末の設置室

2 それぞれのセキュリティ区分に応じた、入退室管理の方法は、次のとおりとする。

セキュリティ区分	入退室管理の方法
レベル2	・入退室を行う場合には、入退室管理者から事前に

	<p>許可を得ている者のみが入退室を行い、その都度鍵又は指紋照合電気錠の指紋照合により入退室を行う。</p> <ul style="list-style-type: none"> 指紋照合電気錠に指紋登録されていない者は、指紋照合電気錠に登録されている情報統計課職員が必要と認め、当該職員が立ち会った上で入退室できるものとする。 識別を行うために、入退室者には、名札の着用を義務付ける。また、入退室に関する記録を行う。
レベル1	<ul style="list-style-type: none"> 入退室を行う場合には、入退室管理者から事前に許可された者のみが入退室を行う。 識別を行うために、入退室者には、名札の着用を義務付ける。

(入退室管理者)

第10条 前条第2項の入退室管理者は、セキュリティ区分レベル2の室にあっては、情報統計課長、セキュリティ区分レベル1の室にあっては、市民課長、出張所長及び市民課サービスコーナー所長をもって充てる。

2 入退室管理者は、前条第1項に掲げる室について、同条第2項に定める入退室の管理を行うほか、住基ネットのセキュリティを確保するため、入退室の管理に関し、必要な措置をとらなければならない。

(鍵の管理)

第11条 第9条第1項で規定するレベル2のセキュリティ区分に係る室の鍵の管理は、管財課長が行い、指紋照合電気錠の管理は、情報統計課長が行う。

(管理簿の作成)

第12条 入退室管理者は、レベル2のセキュリティ区分に係る室については、入退室管理簿を作成し、これを保存するものとする。

2 管財課長は、レベル2のセキュリティ区分に係る室については、鍵の管理簿を作成し、これを保存するものとする。

(指示)

第13条 セキュリティ統括責任者は、適切な入退室管理が行われているかどうか、入退室管理者等から報告を聴取し、調査を行い、必要な指示を行うものとする。

第4章 アクセス管理

(アクセス管理を行う機器)

第14条 次に掲げる住基ネットの構成機器について、アクセス管理を行う。

(1) CS

(2) CS端末

2 前項のアクセス管理は、操作者用ICカード及びパスワードにより操作者の正当な権限を確認すること並びに操作履歴を記録することにより行うものとする。

(アクセス管理責任者)

第15条 前条のアクセス管理を実施するため、アクセス管理責任者を置く。

2 アクセス管理責任者は、情報統計課長をもって充てる。

(操作者用ICカード)

第16条 アクセス管理責任者は、操作者用ICカード及びパスワードに関し、次に掲げる事項を実施する。

(1) 操作者用ICカード及びパスワードの管理方法を定めること。

(2) 操作者用ICカードの種類ごとの操作者について、住基ネットを利用する部署のセキュリティ責任者と協議して定めること。

(3) 操作者用 I C カードの管理簿を作成すること。

(操作者の責務)

第 17 条 操作者は、操作者用 I C カード及びパスワードの管理方法を遵守しなければならない。

(操作履歴の記録)

第 18 条 アクセス管理責任者は、操作履歴について、7 年前までさかのぼって解析できるよう、保管するものとする。

第 5 章 情報資産管理

(情報資産管理)

第 19 条 住基ネットの情報資産の適切な管理を行うため管理責任者を置く。

2 前項の情報資産のうち、本人確認情報、C S に係る帳票及び住民基本台帳カードの管理責任者（以下「本人確認情報管理責任者」という。）は、セキュリティ責任者をもって充て、これら以外の情報資産の管理責任者（以下「情報資産管理責任者」という。）は、システム管理者をもって充てる。

(本人確認情報管理責任者)

第 20 条 本人確認情報管理責任者は、本人確認情報を取り扱うことができる者を指定するとともに、当該本人確認情報の漏えい、滅失及びき損の防止その他の当該本人確認情報の適切な管理のための必要な措置を講じなければならない。

2 本人確認情報管理責任者は、C S に係る帳票及び住民基本台帳カードの管理方法を定めるものとする。

(情報資産管理責任者)

第 21 条 情報資産管理責任者は、当該情報資産の管理方法（操作者の指定を含む。）を定めるものとする。

2 情報資産管理責任者は、本人確認情報管理責任者と協議して、住基ネットの

オペレーション計画を定めるものとする。

第6章 委託管理

(委託を受けようとする者の管理体制等の調査)

第22条 住基ネットを管理し、又は利用する部署の長は、住基ネットに係わる業務の外部委託（以下「外部委託」という。）をしようとするときは、あらかじめ、委託を受けようとする者における情報の保護に関する管理体制等について調査するものとする。

(外部委託の承認)

第23条 住基ネットを管理し、又は利用する部署の長は、外部委託をしようとするときは、委託する業務の内容、理由及び情報の保護に関する事項等について、あらかじめ、セキュリティ会議の審議を経てセキュリティ統括責任者の承認を得なければならない。

(委託契約書への記載事項)

第24条 外部委託に係る契約書には、情報の保護に関し、次の各号に掲げる事項を明記しなければならない。

- (1) 秘密保持に関すること。
- (2) 厳重な保管及び搬送に関すること。
- (3) 再委託の禁止又は制限に関すること。
- (4) 委託目的以外の利用及び第三者への提供の禁止に関すること。
- (5) 複写及び複製の禁止に関すること。
- (6) 事故発生時の報告義務に関すること。
- (7) 不要となった個人情報の速やかな返還又は処分に関すること。
- (8) 措置事項に違反した場合の契約解除及び損害賠償に関すること。
- (9) その他個人情報の保護に関し必要な事項

(受託者の管理状況の調査)

第25条 住基ネットを管理し、又は利用する部署の長は、必要に応じて受託者における当該外部委託に係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7章 教育

(教育)

第26条 住基ネットに携わるすべての職員は、セキュリティ統括責任者が行う情報セキュリティに関する教育を受けなければならない。

第8章 監査

(監査)

第27条 セキュリティ統括責任者は、住基ネットのセキュリティについて監査を定期的に行わなくてはならない。

2 監査の対象及び方法については、別に定める。

第9章 緊急時の対応

(緊急時の対応)

第28条 セキュリティ統括責任者は、住基ネットを構成するハードウェア、ソフトウェア及びネットワークの障害により住民サービスが停止する場合又は不正行為により本人確認情報に脅威を及ぼすおそれがある場合は、被害を未然に防ぎ、又は被害の拡大を防止し早急な復旧を図るため、必要な措置を講じなければならない。

(緊急時対応計画)

第29条 セキュリティ統括責任者は、緊急時の対応計画を定めるものとする。

第10章 雑則

(委任)

第30条 この訓令に定めるもののほか、必要な事項は、別に定める。

附 則

この訓令は、平成14年7月26日から施行する。