

# 野田市個人情報の保護に関する管理基準

## 第1 総則

### 1 目的

この基準は、野田市における個人情報の保護に関する法律（平成15年法律第57号。以下「個人情報保護法」という。）第66条に規定する保有個人情報の安全管理のため、また、行政手続における特定の個人を識別するための番号の利用等に関する法律（平成25年法律第27号。以下「番号利用法」という。）第12条に規定する個人番号の適切な管理のために必要な措置について定めることを目的とする。

### 2 定義

用語の意義は、個人情報保護法及び番号利用法の例による。

## 第2 管理体制

### 1 総括保護管理者

- (1) 総括保護管理者を置き、副市長をもって充てる。
- (2) 総括保護管理者は、各実施機関における保有個人情報（個人番号及び特定個人情報を含む。以下同じ。）の管理に関する事務を総括する任に当たる。

### 2 副総括保護管理者

- (1) 副総括保護管理者を置き、総務部長をもって充てる。
- (2) 副総括保護管理者は、総括保護管理者を補佐する任に当たる。
- (3) 保有個人情報を複数の部署で取り扱う場合の各部署の任務分担及び責任の明確化を行う。

### 3 部保護管理者

- (1) 保有個人情報を取り扱う室及び部（以下「部等」という。）に、部保護管理者を置き、各部等の長をもって充てる。
- (2) 部保護管理者は、部等における保有個人情報を適切に管理する任に当た

る。

#### 4 保護管理者

- (1) 保有個人情報を取り扱う課等に、保護管理者を置き、各課等の長をもって充てる。
- (2) 保護管理者は、課等における保有個人情報の適切な管理を確保する任に当たる。
- (3) 保護管理者は、保有個人情報を取り扱う職員（以下「事務取扱担当者」という。）並びにその役割を指定する。
- (4) 保護管理者は、事務取扱担当者が取り扱う保有個人情報の範囲を指定する。
- (5) 保護管理者は、保有個人情報を情報システムで取り扱う場合、情報政策課長と連携して、その任に当たる。
- (6) 保護管理者は、次に掲げる組織体制を整備する。
  - ① 事務取扱担当者がこの基準に違反している事実又は兆候を把握した場合の保護管理者への報告連絡体制
  - ② 保有個人情報の漏えい、滅失又は毀損等（以下「漏えい等」という。）事案の発生又は兆候を把握した場合の職員から保護管理者への報告連絡体制
  - ③ 保有個人情報の漏えい等の事案の発生又は兆候を把握した場合の対応体制

#### 4 保護担当者

- (1) 保有個人情報を取り扱う課等に、保護担当者を置き、各課等の長の補佐又は保護管理者が指定する者をもって充てる。
- (2) 保護担当者は、保護管理者を補佐し、課等における保有個人情報の管理に関する事務を担当する。

#### 5 監査責任者

- (1) 監査責任者を置き、総務課長をもって充てる。
- (2) 監査責任者は、保有個人情報の管理（情報セキュリティに関する事項を除く。）の状況について監査する任に当たる。

## 6 保有個人情報の適切な管理のための委員会

総括保護管理者は、保有個人情報の管理に係る重要事項の決定、連絡・調整等を行うため必要があると認めるときは、関係職員を構成員とする委員会を設け、定期的に又は随時に開催する。

## 第3 教育研修

### 1 教育研修の実施

- (1) 総括保護管理者は、保有個人情報の取扱いに従事する職員（派遣労働者を含む。以下同じ。）及び保有個人情報を取り扱う情報システムに関する事務に従事する職員（派遣労働者を含む。以下同じ。）に対し、保有個人情報の取扱いについて理解を深め、保有個人情報の保護に関する意識の高揚を図るための啓発その他必要な教育研修を実施する。
- (2) 総括保護管理者は、保護管理者及び保護担当者に対し、各課等の現場における保有個人情報の適切な管理のための教育研修を実施する。
- (3) 保護管理者は、当該課等の職員に対し、保有個人情報の適切な管理のための教育研修への参加の機会を付与する等の必要な措置を講ずる。

## 第4 職員の責務

- 1 職員は、個人情報保護法、番号利用法及び野田市情報セキュリティポリシーの趣旨にのっとり、関連する法令等の定め並びに総括保護管理者、副総括保護管理者、部保護管理者、保護管理者及び保護担当者の指示に従い、保有個人情報を取り扱わなければならない。
- 2 職員は、保有個人情報の漏えい等の事案の発生又は兆候を把握した場合及び事務取扱担当者がこの基準に違反している事実又は兆候を把握した場合は、速やかに保護管理者に報告しなければならない。

## 第5 保有個人情報の取扱い

### 1 アクセス制限

- (1) 保護管理者は、保有個人情報の秘匿性等その内容に応じて、当該保有個

個人情報にアクセスをする権限（以下「アクセス権限」という。）を有する職員とその権限の内容を、当該職員が業務を行う上で必要最小限の範囲に限る。

- (2) アクセス権限を有しない職員は、保有個人情報にアクセスしてはならない。
- (3) 職員は、アクセス権限を有する場合であっても、業務上の目的以外の目的で保有個人情報にアクセスしてはならず、アクセスは必要最小限としなければならない。

## 2 複製等の制限

職員が業務上の目的で保有個人情報を取り扱う場合であっても、保護管理者は、次に掲げる行為については、当該保有個人情報の秘匿性等その内容に応じて、当該行為を行うことができる場合を必要最小限に限定し、職員は、保護管理者の指示に従い行う。

- ① 保有個人情報の複製
- ② 保有個人情報の送信
- ③ 保有個人情報が記録されている媒体の外部への送付又は持出し
- ④ その他保有個人情報の適切な管理に支障を及ぼすおそれのある行為

## 3 誤りの訂正等

職員は、保有個人情報の内容に誤り等を発見した場合には、保護管理者の指示に従い、訂正等を行う。

## 4 媒体の管理等

職員は、保護管理者の指示に従い、保有個人情報が記録されている媒体を定められた場所に保管するとともに、必要があると認めるときは、耐火金庫等への保管、施錠等の保有個人情報等の漏えい等を防止するための措置を講ずる。また、保有個人情報が記録されている媒体を外部へ送付し又は持ち出す場合には、原則として、パスワード等（パスワード、ICカード、生体情報等をいう。以下同じ。）を使用して権限を識別する機能（以下「認証機能」という。）を設定する等のアクセス制御のために必要な措置を講ずる。

## 5 誤送付等の防止

職員は、保有個人情報を含む電磁的記録又は媒体の誤送信・誤送付、誤交付又はウェブサイト等への誤掲載を防止するため、個別の事務・事業において取り扱う個人情報の秘匿性等その内容に応じ、複数の職員による確認やチェックリストの活用等の必要な措置を講ずるものとする。

## 6 廃棄等

職員は、保有個人情報又は保有個人情報が記録されている媒体（端末及びサーバに内蔵されているものを含む。）が不要となった場合には、保護管理者の指示に従い、当該保有個人情報の復元又は判読が不可能な方法により当該情報の消去又は当該媒体の廃棄を行う。特に、保有個人情報の消去や保有個人情報が記録されている媒体の廃棄を委託する場合（二以上の段階にわたる委託を含む。）には、必要に応じて職員が消去及び廃棄に立ち会い、又は写真等を付した消去及び廃棄を証明する書類を受け取るなど、委託先において消去及び廃棄が確実に行われていることを確認する。

## 7 保有個人情報の取扱状況の記録

(1) 保護管理者は、保有個人情報の秘匿性等その内容に応じて、台帳等を整備して、当該保有個人情報の利用及び保管等の取扱いの状況について記録する。

(2) 保護管理者は、特定個人情報の取扱状況を確認する手段を整備して、当該保有個人情報の利用及び保管等の取扱状況について記録する。

## 8 外的環境の把握

保有個人情報が、外国（民間事業者が提供するクラウドサービスを利用する場合においてはクラウドサービス提供事業者が所在する外国及び個人データが保存されるサーバが所在する外国が該当する。）において取り扱われる場合、当該外国の個人情報の保護に関する制度等を把握した上で、保有個人情報の安全管理のために必要かつ適切な措置を講じなければならない。

## 9 個人番号の利用の制限

保護管理者は、個人番号の利用に当たり、番号利用法があらかじめ限定的に定めた事務に限定する。

## 10 特定個人情報の提供の求めの制限

職員は、個人番号利用事務又は個人番号関係事務（以下「個人番号利用事務等」という。）を処理するために必要な場合その他番号利用法で定める場合を除き、個人番号の提供を求めてはならない。

#### 1 1 特定個人情報ファイルの作成の制限

職員は、個人番号利用事務等を処理するために必要な場合その他番号利用法で定める場合を除き、特定個人情報ファイルを作成してはならない。

#### 1 2 保有個人情報の収集・保管の制限

職員は、番号利用法第19条各号のいずれかに該当する場合を除き、他人の個人番号を含む個人情報を収集又は保管してはならない。

#### 1 3 取扱区域

保護管理者は、個人番号及び特定個人情報を取り扱う事務を実施する区域（以下「取扱区域」という。）を明確にし、物理的な安全管理措置を講ずる。

### 第6 情報システムにおける安全の確保等

#### 1 アクセス制御

(1) 保護管理者は、保有個人情報（情報システムで取り扱うものに限る。以下第6（12を除く。）及び第7において同じ。）の秘匿性等その内容に応じて、認証機能を設定する等のアクセス制御のために必要な措置を講ずる。

(2) 保護管理者は、(1)の措置を講ずる場合には、パスワード等の管理に関する定めを整備（その定期又は随時の見直しを含む。）するとともに、パスワード等の読取防止等を行うために必要な措置を講ずる。

#### 2 アクセス記録

(1) 保護管理者は、保有個人情報の秘匿性等その内容に応じて、当該保有個人情報へのアクセス状況を記録し、その記録（以下「アクセス記録」という。）を一定の期間保存し、定期的に又は随時に分析するために必要な措置を講ずる。

(2) 保護管理者は、アクセス記録の改ざん、窃取又は不正な消去の防止のために必要な措置を講ずる。

#### 3 アクセス状況の監視

保護管理者は、保有個人情報等の秘匿性等その内容及びその量に応じて、当該保有個人情報等への不適切なアクセスの監視のため、保有個人情報等を含む又は含むおそれがある一定量以上の情報が情報システムからダウンロードされた場合に警告表示がなされる機能の設定、当該設定の定期的確認等の必要な措置を講ずるものとする。

#### 4 管理者権限の設定

保護管理者は、保有個人情報の秘匿性等その内容に応じて、情報システムの管理者権限の特権を不正に窃取された際の被害の最小化及び内部からの不正操作等の防止のため、当該特権を最小限とする等の必要な措置を講ずる。

#### 5 外部からの不正アクセスの防止

保護管理者は、保有個人情報を取り扱う情報システムへの外部からの不正アクセスを防止するため、ファイアウォールの設定による経路制御等の必要な措置を講ずる。

#### 6 不正プログラムによる漏えい等の防止

情報政策課長は、不正プログラムによる保有個人情報の漏えい等の防止のため、ソフトウェアに関する公開された脆弱性の解消、把握された不正プログラムの感染防止等に必要な措置（導入したソフトウェアを常に最新の状態に保つことを含む。）を講ずる。

#### 7 情報システムにおける保有個人情報の処理

職員は、保有個人情報について、一時的に加工等の処理を行うため複製等を行う場合には、その対象を必要最小限に限り、処理終了後は不要となった情報を速やかに消去する。保護管理者は、当該保有個人情報の秘匿性等その内容に応じて、随時、消去等の実施状況を重点的に確認するものとする。

#### 8 暗号化

保護管理者は、保有個人情報の秘匿性等その内容に応じて、暗号化のために必要な措置を講ずる。職員は、これを踏まえ、その処理する保有個人情報について、当該保有個人情報の秘匿性等その内容に応じて、適切に暗号化を行う。

#### 9 記録機能を有する機器・媒体の接続禁止

- (1) 保有個人情報の漏えい等の防止のため、USBメモリ等の記録機能を有する機器・媒体（以下「可搬記録媒体等」という。）の情報システム端末等への接続を禁止する。
- (2) 保護管理者は、業務に支障が出ると判断した場合に限り、可搬記録媒体等の情報システム端末等への接続の許可を副総括保護管理者に願い出ることができる。
- (3) 副総括保護管理者は、業務に支障が出ると判断した場合に限り、可搬記録媒体等の情報システム端末等への接続を許可することができる。

#### 1 0 端末の限定

保護管理者は、保有個人情報の秘匿性等その内容に応じて、その処理を行う端末を限定するために必要な措置を講ずる。

#### 1 1 端末の盗難防止等

- (1) 保護管理者は、端末の盗難又は紛失の防止のため、端末の固定、執務室の施錠等の必要な措置を講ずる。
- (2) 職員は、保護管理者が必要があると認めるときを除き、端末を外部へ持ち出し、又は外部から持ち込んで서는ならない。

#### 1 2 閲覧防止

職員は、端末の使用に当たっては、保有個人情報が当該職員以外の者に閲覧されることがないように、使用状況に応じて情報システムからログオフを行うことを徹底する等の必要な措置を講ずる。

#### 1 3 入力情報の照合等

職員は、情報システムで取り扱う保有個人情報の重要度に応じて、入力原票と入力内容との照合、処理前後の当該保有個人情報の内容の確認、既存の保有個人情報との照合等を行う。

#### 1 4 バックアップ

保護管理者は、保有個人情報の重要度に応じて、バックアップを作成し、分散保管するために必要な措置を講ずる。

#### 1 5 情報システム設計書等の管理

保護管理者は、保有個人情報に係る情報システムの設計書、構成図等の文

書について外部に知られることがないように、その保管、複製、廃棄等について必要な措置を講ずる。

## 第7 電子計算室等の安全管理

### 1 入退管理

- (1) 情報政策課長は、保有個人情報を取り扱う基幹的なサーバ等の機器を設置する室その他の区域（以下「電子計算室等」という。）に立ち入る権限を有する者を定めるとともに、用件の確認、入退の記録、部外者についての識別化、部外者が立ち入る場合の職員の立会い又は外部電磁的記録媒体等の持込み、利用及び持ち出しの制限又は検査等の措置を講ずる。また、保有個人情報を記録する媒体を保管するための施設を設けている場合においても、必要があると認めるときは、同様の措置を講ずる。
- (2) 情報政策課長は、必要があると認めるときは、電子計算室等の出入口の特定化による入退の管理の容易化、所在表示の制限等の電子計算室等の安全を管理するための措置を講ずる。
- (3) 情報政策課長は、電子計算室等への入退室を管理するため、立入りに係る認証機能を設定するとともに、電算機室（管理区域）入退室許可申請書兼管理台帳（以下「入退室許可申請書兼管理台帳」という。）等により入退室の状況を把握しなければならない。
- (4) 保護管理者は、課等の業務の処理において、電子計算室等へ立ち入る必要がある場合には、入退室者を指定の上、情報政策課長に対し、入退室許可申請書兼管理台帳を提出しなければならない。

### 2 電子計算室等の管理

- (1) 情報政策課長は、外部からの不正な侵入に備え、電子計算室等に施錠装置、警報装置、監視設備の設置等の措置を講ずる。
- (2) 情報政策課長は、災害等に備え、電子計算室等に、耐震、防火、防煙、防水等の必要な措置を講ずるとともに、サーバ等の機器の予備電源の確保、配線の損傷防止等の措置を講ずる。

## 第8 保有個人情報の提供及び業務の委託等

### 1 保有個人情報の提供

- (1) 保護管理者は、個人情報保護法第69条第2項第3号及び第4号の規定に基づき保有個人情報を提供する場合には、個人情報保護法第70条の規定に基づき、原則として、提供先における利用目的、利用する業務の根拠法令、利用する記録範囲及び記録項目、利用形態等について提供先との間で書面を取り交わす。
- (2) 保護管理者は、個人情報保護法第69条第2項第3号及び第4号の規定に基づき保有個人情報を提供する場合には、個人情報保護法第70条の規定に基づき、安全確保の措置を要求するとともに、必要があると認めるときは、提供前又は随時に実地の調査等を行うことにより当該措置状況を確認してその結果を記録するとともに、改善要求等の措置を講ずる。
- (3) 保護管理者は、番号利用法で限定的に明記された場合を除き、個人番号及び特定個人情報を提供してはならない。

### 2 業務の委託等

- (1) 保護管理者は、保有個人情報の取扱いに係る業務を外部に委託する場合には、個人情報の適切な管理を行う能力を有しない者を選定することがないように、必要な措置を講ずる。また、契約書に、次に掲げる事項を明記するとともに、委託先における責任者及び業務従事者の管理及び実施体制、個人情報の管理の状況についての検査に関する事項等の必要な事項について書面で確認する。
  - ① 個人情報に関する秘密保持、目的外利用の禁止等の義務
  - ② 再委託の制限又は事前承認等再委託に係る条件に関する事項
  - ③ 個人情報の複製等の制限に関する事項
  - ④ 個人情報の安全管理措置に関する事項
  - ⑤ 個人情報の漏えい等の事案の発生時における対応に関する事項
  - ⑥ 委託終了時における個人情報の消去及び媒体の返却に関する事項
  - ⑦ 法令及び契約に違反した場合における契約解除、損害賠償責任その他必要な事項

- ⑧ 契約内容の遵守状況についての定期的報告に関する事項及び委託先における委託された個人情報の取扱状況を把握するための監査等に関する事項
- (2) 保有個人情報の取扱いに係る業務を外部に委託する場合には、取扱いを委託する個人情報の範囲は、委託する業務内容に照らして必要最小限でなければならない。
  - (3) 保護管理者は、保有個人情報の取扱いに係る業務を外部に委託する場合には、委託する保有個人情報の秘匿性等その内容に応じて、委託先における責任者及び業務従事者の作業の管理体制及び実施体制や個人情報の管理の状況を確認する。
  - (4) 保護管理者は(3)のほか、個人番号利用事務等の全部又は一部を外部に委託する際には、委託先において、番号利用法に基づき野田市が果たすべき安全管理措置と同等の措置が講じられるか否かについて、あらかじめ確認するとともに、必要かつ適切な監督を行う。
  - (5) 委託先において、保有個人情報の取扱いに係る業務が再委託される場合には、委託先に(1)の措置を講じさせるとともに、再委託される業務に係る保有個人情報の秘匿性等その内容に応じて、委託先を通じて又は委託元自らが(3)の措置を実施する。保有個人情報の取扱いに係る業務について再委託先が再々委託を行う場合以降も同様とする。
  - (6) 個人番号利用事務等の全部又は一部の「委託を受けた者」が再委託をする際には、委託をする個人番号利用事務等において取り扱う特定個人情報の適切な安全管理が図られることを確認した上で再委託の諾否を判断する。
  - (7) 保有個人情報の取扱いに係る業務を派遣労働者によって行わせる場合には、労働者派遣契約書に秘密保持義務等個人情報の取扱いに関する事項を明記する。
  - (8) 保有個人情報を提供し、又は業務委託する場合には、漏えい等による被害発生リスクを低減する観点から、提供先の利用目的、委託する業務の内容、保有個人情報の秘匿性等その内容などを考慮し、必要に応じ、特定

の個人を識別することができる記載の全部若しくは一部を削除し、又は別の記号等に置き換える等の措置を講ずる。

## 第9 安全管理上の問題への対応

### 1 事案の報告及び再発防止措置

- (1) 保有個人情報の漏えい等の事案の発生又は兆候を把握した場合、事務取扱担当者が取扱規程等に違反している事実又は兆候を把握した場合等、安全管理の上で問題となる事案の発生又は発生のおそれを認識した場合に、その事案の発生等を認識した職員は、直ちに当該保有個人情報を管理する保護管理者に報告する。
- (2) 保護管理者は、被害の拡大防止又は復旧等のために必要な措置を速やかに講ずる。ただし、外部からの不正アクセスや不正プログラムの感染が疑われる当該端末等のLANケーブルを抜くなど、被害拡大防止のため直ちに行い得る措置については、直ちに行う（職員に行わせることを含む。）ものとする。
- (3) 保護管理者は、事案の発生した経緯、被害状況等を調査し、総括保護管理者に報告する。ただし、特に重大と認める事案が発生した場合には、直ちに総括保護管理者に当該事案の内容等について報告する。
- (4) 総括保護管理者は、(3)の規定に基づく報告を受けた場合には、事案の内容等に応じて、当該事案の内容、経緯、被害状況等を市長に速やかに報告する。
- (5) 保護管理者は、事案の発生した原因を分析し、再発防止のために必要な措置を講ずる。

### 2 法に基づく報告及び通知

保有個人情報の漏えい等が生じた場合であって個人情報保護法第68条第1項の規定による個人情報保護委員会への報告及び同条第2項の規定による本人への通知を要する場合には、1で定める事項と並行して、速やかに所定の手続を行うとともに、個人情報保護委員会による事案の把握等に協力する。

### 3 公表等

- (1) 総括保護管理者は、事案の内容、影響等に応じて、事実関係及び再発防止策の公表、当該事案に係る保有個人情報の本人への対応等の措置を講ずる。
- (2) 総括保護管理者は、公表を行う事案については、当該事案の内容、経緯、被害状況等について、速やかに個人情報保護委員会に情報提供を行う。

## 第10 監査及び点検の実施

### 1 監査

監査責任者は、保有個人情報の適切な管理を検証するため、第2から第9に規定する措置（情報セキュリティに関する事項を除く。）の状況を含む保有個人情報の管理の状況について、定期に及び必要に応じて監査を行い、その結果を総括保護管理者に報告する。

### 2 点検

保護管理者は、課等における保有個人情報の記録媒体、処理経路、保管方法等について、定期に及び必要に応じて点検を行い、必要があると認めるときは、その結果を総括保護管理者に報告する。

### 3 評価及び見直し

総括保護管理者、保護管理者等は、監査又は点検の結果等を踏まえ、実効性等の観点から保有個人情報の適切な管理のための措置について評価し、必要があると認めるときは、その見直し等の措置を講ずる。

## 第11 出資法人等に対する指導等

野田市は、出資法人、指定管理者及び業務委託先事業者に対して、その業務運営における自主性に配慮しつつ、個人情報の保護に関し必要な指導、助言を行う。

## 第12 補則

この基準に定めるもののほか、野田市の保有する個人情報の保護に関し必要な事項は、市長が定める。