藤沢市個人情報保護制度運営審議会答申第８７０号

２０１７年（平成２９年）8月１０日

藤沢市長　鈴木　恒夫　様

藤沢市個人情報保護制度
運営審議会会長　畠山　関之

所管する情報処理システムの運用管理に係るコンピュータ処理について
（答申）

２０１７年（平成２９年）７月２６日付けで諮問（第８７０号）された所管する情報処理システムの運用管理に係るコンピュータ処理について次のとおり答申します。

１　審議会の結論

藤沢市個人情報の保護に関する条例（平成１５年藤沢市条例第７号。以下「条例」という。)第１８条の規定によるコンピュータ処理を行うことは適当であると認められる。

２　実施機関の説明要旨

実施機関の説明を総合すると，本事務の実施に当たりコンピュータ処理を行う必要性は，次のとおりである。

(1) 諮問に至った経過

社会保障・税番号制度は，「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」（以下「番号法」という。）等に基づき，複数の機関に存在する個人情報を同一人の情報であることの確認を行うための基盤であり，社会保障・税制度の効率性・透明性を高め，国民にとって利便性の高い公平・公正な社会の実現を目的とした制度である。

この番号制度の導入により，２０１７年（平成２９年）７月１８日から，国・都道府県・市町村等の情報保有機関間の情報連携の試行運用が開始されるとともに,「情報提供等記録開示システム」（以下「開示システム」という。）の試行運用も開始されることとなった。

開示システムは,番号利用法附則第６条第３項に基づき国が設置するもので,情報提供ネットワークシステム（番号法第２条第１４項）や公的個人認証サービス等と連携しつつ，３つの事務（情報提供等記録表示，自己情報表示，お知らせ情報表示）において，開示システムを利用する国民等（以下「利用者」という。）に対し，情報を表示するための機能を有する。

開示システムの運用開始にあたり，自己情報表示及びお知らせ情報表示につい

て，本市の「情報連携中間サーバーシステム」（以下「中間サーバー」という。）」にて新たなコンピュータ処理を行うことになるため，藤沢市個人情報の保護に関する条例第１８条に基づき，藤沢市個人情報保護制度運営審議会に意見を求めるものである。

(2) コンピュータ処理について

ア　コンピュータ処理の必要性

中間サーバーにおけるコンピュータ処理については，２０１５年（平成２７年）８月２８日付けで個人情報保護制度運営審議会に諮問し（第７６３号），９月１０日付でコンピュータ処理を行うことは適当との答申を得ている。今回の諮問では，開示システムの運用開始に伴い，中間サーバーにて追加される新たなコンピュータ処理について諮問するものである。

(ｱ)　自己情報表示

自己情報表示とは，情報保有機関で保有する情報連携用の特定個人情報を，開示システムの利用者に開示する機能である。

開示システムは，利用者から自己情報の提供要求を受け付けると，情報提供ネットワークシステムを経由して情報保有機関へ送信する。情報保有機関は，開示システムから自己情報提供要求を受信すると，中間サーバーに保存されている情報連携用の特定個人情報を，利用者が提供要求した自己情報として，情報提供ネットワークシステムを経由し開示システムへ通知する。開示システムは，その内容を利用者フォルダーに保存するとともに，当該情報を開示システムに接続された利用者の端末に表示する。

なお，個人ごと，かつ特定個人情報ごとに，自己情報提供用添付ファイル（特定個人情報に関連する個人情報として特定個人情報（連携対象）と併せて提供される添付ファイル。氏名，住所，性別，生年月日の基本４情報は含まない。）を登録することも可能である。

また，開示システムに自己情報を提供した状況について，必要に応じて個人番号利用事務実施者が確認を行うことも可能である。

自己情報表示については，番号利用法附則第６条第３項及び附則第６条第４項第１号の規定に基づき，新たなコンピュータ処理を行う必要がある。

(ｲ)　お知らせ情報表示

お知らせ情報表示は，情報保有機関からのお知らせ情報（個人番号利用事務に関してのお知らせ情報に限る）を，お知らせ対象とする利用者に対し，送信する機能である。（お知らせ情報の中で，利用者に対し，お知らせ情報用の添付ファイルを添付したり，選択式の回答を求めることもできる。）

地方公共団体の場合，中間サーバーから，情報提供ネットワークシステムを経由して，開示システムに送信する。

開示システムは送信を受けたお知らせ情報を，該当の利用者フォルダーに保存するとともに，開示システムに接続された端末に表示する。

また，情報保有機関は，開示システムに「お知らせ情報の状況確認依頼」を行うことで，お知らせの閲覧状況や，利用者からの回答結果を取得する。

お知らせ情報表示については，番号利用法附則第６条第３項及び附則第６条第４項第２号の規定に基づき，新たなコンピュータ処理を行う必要がある。

イ　コンピュータ処理をする個人情報

(ｱ) 自己情報表示

１.情報提供用個人識別符号，２.団体内統合宛名番号，３.特定個人情報（番号法別表第２に基づき本市が提供する特定個人情報に限る。資料４「特定個人情報名及び特定個人情報の項目名」のとおり。）

※なお，「３.特定個人情報」については，番号法等の改正により，取り扱う特定個人情報及び項目に追加・削除・変更が生じる可能性があることから，今後情報連携の対象となる特定個人情報及び項目を含めて包括的に諮問したい。

(ｲ) お知らせ情報表示

１．情報提供用個人識別符号，２.団体内統合宛名番号

なお，お知らせ情報表示機能を使用して通知を利用者に送信する場合，平成２９年５月２６日付け内閣官房番号制度推進室からの事務連絡により，４情報（氏名，住所，性別及び生年月日）等の個人を特定する情報については掲載不可とされている。

ウ　安全対策について

(ｱ) 中間サーバーについて

中間サーバーは庁内には設置せず，クラウドの積極的な活用により共同化・集約化を図るために地方公共団体情報システム機構が全国２か所に用意する中間サーバー・プラットフォームを利用する。なお，全国全ての地方公共団体が，この中間サーバー・プラットフォームを利用する。

ａ　中間サーバー・プラットフォームにおける安全対策については，次のとおり。

(a) 中間サーバー・プラットフォームはデータセンターに設置されており，データセンターへの入館及びサーバ室への入室を厳重に管理するとともに，有人監視及び施錠管理を行う。

(b) 設置場所はデータセンター内の専用の領域とし，他テナントとの混在によるリスクを回避する。

(c) ＵＴＭ（コンピュータウイルスやハッキングなどの脅威からネットワークを効率的かつ包括的に保護する装置）等を導入し，アクセス制限，侵入検知及び侵入防止を行うとともに，ログの解析を行う。

(d) 特定個人情報を管理するデータベースを地方公共団体ごとに区分管理（アクセス制御）しており，中間サーバー・プラットフォームを利用する団体であっても他団体が管理する情報には一切アクセスできないようにする。

(e) ウイルス対策ソフトを導入し，パターンファイルの更新を行い，導入しているＯＳ及びミドルウェアについて，必要に応じてセキュリティパッチの適用を行う。

(f) 中間サーバー・プラットフォームの保守・運用を行う事業者においては，特定個人情報に係る業務にはアクセスができないよう管理を行い，業務上，特定個人情報へはアクセスすることはできない。また，運用に携わる職員及び事業者に対し，運用規則やセキュリティについての研修等を実施する。

b　中間サーバー接続端末の利用にあたっては，操作者を限定するために，端末にログオンする際の職員の生体認証登録を行う。また，システムにログインするためのＩＤとパスワードを設定することで不必要な情報へのアクセスを防止するとともに，アクセスログを取得することにより，不適切な操作を防止する。ウイルス対策ソフトを導入し，パターンファイルの更新を行う。また，ワイヤーロックを使用し，端末の盗難を防止する。

c　日常的な安全対策として，条例，藤沢市情報セキュリティポリシー及び藤沢市コンピュータ管理運営規程を遵守する。

(ｲ) 開示システムについて

開示システムについて国が実施している主な安全対策については，次のとおりである。

a　特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。）における安全対策

(a) 利用者フォルダー開設に当たって，利用者が初期設定に係る事務の手続を行う場合の本人確認は，個人番号カードを用いた公的認証システムを利用し，電子証明書により本人の申請ということを確認する。このことにより，本人以外の情報を受け付けないようシステムで制御することで，本人以外の情報の入手を防止する。

(b) 開示システムと接続先との通信時においては，サーバ証明書を用いた認証を行い，なりすましを防止する。

(c) 開示システムが保有する各種設定ファイルにより，接続先のなりすましを防止するとともに，その設定ファイルについては，改ざん検知システムによる保護を行う。

(d) 外部公開コンテンツ（開示システムの入力画面等）の改ざん防止対策を講じる。

(e) 偽サイトへの誘導（フィッシング）対策として公開 Web サーバに電子証明書を使用し，サーバ認証を実施する。

(f) メールに関するなりすまし対策として，開示システムから利用者への送信メール以外は中継しないようメールサーバで設定する。また，開示システム内部からの不正なメール送信の防止対策として，外部向けのメール送信サーバにＳＭＴＰ認証を導入する。

(g) 初期設定終了後も，開示システムにログインする際には，公的個人認証サービスに確認を行い，使用されている証明書が失効されていないことの確認を行う。

(h) 通信の安全を確保し，盗聴等を防ぐために暗号化通信を行う。使用

する暗号アルゴリズムは，最新の「電子政府推奨暗号リスト」に記載された暗号アルゴリズムから，想定されるリスクに対して最適な選定を行う。

b　特定個人情報の使用における安全対策

(a)　システムを利用する必要がある職員を特定し，個人ごとにユーザIDを割り当てるとともに，IDとパスワードによる認証を行う。

(b)　ＯＳや管理ソフトにより運用端末へのアプリケーションのインストールを制限する。

(c)　システムにアクセスできる端末を制限する

(d)　システムへのアクセスログ，システムでの操作ログの記録を行い，操作者個人を特定できるようにする。

(e)　定期的に操作ログをチェックし，不正とみられる操作があった場合，操作内容を確認する。

c　情報提供ネットワークシステムとの接続における安全対策

(a)　情報提供ネットワークシステムとの間の通信は専用線によって行われ，かつ通信自体は暗号化される。

(b)　マルウェア対策としてサーバ装置（仮想マシンを含む）及び運用者端末には，マルウェア対策ソフトウェアを導入し，マルウェア検出用不正プログラム定義ファイル等の最新化を図るため適宜更新を行う。

d　特定個人情報の保管・消去における安全対策

自己情報表示は一時的な保管であり，利用者参照後，ログアウト時に開示システムにおいて自動的に消去され，また，お知らせ情報に関しては，個々の情報保有機関において設定した保存期間経過後，開示システムにおいて自動的に消去されることから，古い情報のまま保管され続けるリスクはない。

(3) 実施時期

２０１７年（平成２９年）７月１８日から

(4) 提出書類

資料１　システム連携図及び特定個人情報の流れ
資料２　中間サーバーにおけるコンピュータ処理及び諮問の範囲
資料３　個人番号利用事務実施課一覧
資料４　特定個人情報名及び特定個人情報名項目名
資料５　関係法令〈抜粋〉
資料６　個人情報取扱事務届出書

3　審議会の判断理由

当審議会は，コンピュータ処理を行うことについて，次に述べる理由により，審議会の結論のとおりの判断をするものである。

(1) コンピュータ処理を行うことについて

ア　コンピュータ処理を行う必要性について

実施機関では，コンピュータ処理を行う必要性について，次のように述べ

ている。

(ｱ) 自己情報表示におけるコンピュータ処理の必要性

自己情報表示とは，情報保有機関で保有する情報連携用の特定個人情報を，開示システムの利用者に開示する機能である。

開示システムは，利用者から自己情報の提供要求を受け付けると，情報提供ネットワークシステムを経由して情報保有機関へ送信する。情報保有機関は，開示システムから自己情報提供要求を受信すると，中間サーバーに保存されている情報連携用の特定個人情報を，利用者が提供要求した自己情報として，情報提供ネットワークシステムを経由し開示システムへ通知する。開示システムは，その内容を利用者フォルダーに保存するとともに，当該情報を開示システムに接続された利用者の端末に表示する。

なお，個人ごと，かつ特定個人情報ごとに，自己情報提供用添付ファイル（特定個人情報に関連する個人情報として特定個人情報（連携対象）と併せて提供される添付ファイル。氏名，住所，性別，生年月日の基本４情報は含まない。）を登録することも可能である。

また，開示システムに自己情報を提供した状況について，必要に応じて個人番号利用事務実施者が確認を行うことも可能である。

自己情報表示については，番号利用法附則第６条第３項及び附則第６条第４項第１号の規定に基づき，新たなコンピュータ処理を行う必要がある。

(ｲ) お知らせ情報表示におけるコンピュータ処理の必要性

お知らせ情報表示は，情報保有機関からのお知らせ情報（個人番号利用事務に関してのお知らせ情報に限る）を，お知らせ対象とする利用者に対し，送信する機能である。（お知らせ情報の中で，利用者に対し，お知らせ情報用の添付ファイルを添付したり，選択式の回答を求めることもできる。）

地方公共団体の場合，中間サーバーから，情報提供ネットワークシステムを経由して，開示システムに送信する。

開示システムは送信を受けたお知らせ情報を，該当の利用者フォルダーに保存するとともに，開示システムに接続された端末に表示する。

また，情報保有機関は，開示システムに「お知らせ情報の状況確認依頼」を行うことで，お知らせの閲覧状況や，利用者からの回答結果を取得する。

お知らせ情報表示については，番号利用法附則第６条第３項及び附則第６条第４項第２号の規定に基づき，新たなコンピュータ処理を行う必要がある。

以上のことから判断すると，コンピュータ処理を行う必要性があると認められる。

イ　安全対策について

実施機関が２説明要旨(2)ウ(ｱ)ａ(a)から(f)まで，ｂ及びｃ，(ｲ)ａ(a)から(h)まで，ｂ(a)から(e)まで，ｃ(a)及び(b)並びにｄにおいて示す安全対策は，次のとおりである。

(ｱ) 中間サーバーにおける安全対策

実施機関では，中間サーバーは庁内には設置せず，クラウドの積極的な活用により共同化・集約化を図るために地方公共団体情報システム機構が全国２か所に用意する中間サーバー・プラットフォームを利用する，としている。なお，全国全ての地方公共団体が，この中間サーバー・プラットフォームを利用する，とのことである。

また，中間サーバー・プラットフォームにおける安全対策については，次のとおりとしている。

ａ　必要最小限の担当者以外の者がデータにアクセスできないようにするための措置　(ｱ)a(d)，(ｱ)ｂ

ｂ　ネットワークへの不正アクセスを防止するための措置　(ｱ)a(c)，(ｱ)ｂ

ｃ　ネットワークを通じた情報漏えいを防止するための措置　(ｱ)a(e)

ｄ　実施機関の安全対策を確認できるようにするための措置　(ｱ)a(a)，(b)

ｅ　その他受託者の安全対策を高めるための措置　(ｱ)a(f)

ｆ　日常的な安全対策　(ｱ)ｂ及びｃ

(ｱ) 開示システムにおける安全対策

ａ　必要最小限の担当者以外の者がデータにアクセスできないようにするための措置　(ｲ)ｂ(a)，(c)及び(d)

ｂ　ネットワークへの不正アクセスを防止するための措置　(ｲ)ａ(b)，(c)，(f)及び(g)及び(h)並びに(ｲ)ｃ(a)及び(b)

ｃ　ネットワークを通じた情報漏えいを防止するための措置　(ｲ)ａ(d)及び(e)並びに(ｲ)ｂ(b)及び(c)

ｄ　データを確実に消去するための措置　(ｲ)ｄ

ｅ　日常的な安全対策　(ｲ)ａ(a)及び(ｲ)ｂ(e)

以上のことから判断すると，安全対策上の措置が施されていると認められる。

以上に述べたところにより，コンピュータ処理を行うことは適当であると認められる。

以　上