藤沢市個人情報保護制度運営審議会答申第５１４号

２０１２年9月１３日
（平成２４年）

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　鬨之

所管する情報処理システムの運用管理事務に係るコンピュータ処理について（答申）

２０１２年8月２９日付けで諮問（第５１４号）された所管する情報処理システムの運用管理事務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

現在，情報システム（職員情報ポータルや住民記録，税システム等）の運用に当たっては，「藤沢市コンピュータシステム管理運営規程」第１９条及び「藤沢市情報セキュリティポリシー＜対策基準・基本編＞」第７項（３）に基づき，指紋認証による端末ログイン時及びスクリーンセーバ解除時の利用者権限確認というセキュリティ対策（アクセス制御）を施している。

この指紋認証による利用者権限確認については，個人情報保護制度運営審議会（平成１８年２月９日開催，答申番号：１７３号及び平成２０年９月１１日開催，答申番号３４４号）で承認を得た上で生体認証システムを構築し，これまで運用してきた。

指紋認証は，指先の皮膚の状態（指荒れ、乾燥指など）により認証が困難となる場合があるが，他の生体認証を追加導入するには，新たに別のシステムを構築する

必要があったため，代替策として，ID・パスワードの入力により，利用者の認証を行ってきた。しかし，この運用を継続することは，確実な本人認証という生体認証システムの導入目的に反するものであり，セキュリティの低下に繋がりかねない。

この度，昨今の技術の進展に伴い，指紋情報と指静脈情報を同一のシステムで取り扱え，かつ，同一の管理が可能となったため，指静脈認証を追加するものである。

静脈情報については新たに利用者から収集し，コンピュータ処理を行うこととなるため，条例第１８条コンピュータ処理の制限に基づき，個人情報保護制度運営審議会に諮問するものである。

(2)　生体認証の必要性

不正な端末操作を防ぐためには，厳格な本人認証が不可欠となるが，ＩＤ・パスワードによる認証やカードなどの持ち物認証では，紛失や盗難による，なりすましの危険性が高くなる。

対して，指紋や顔，静脈，瞳の虹彩といった生物個体が持っている特性を利用した生体認証は，紛失や盗難の恐れがなく，限りなく確実な本人認証をすることができる。さらに，複数の生体認証方式を導入することによって，利用者の身体的な状態に左右されることなく認証を行うことが可能となる。

機微な情報を取り扱う市の業務において，セキュリティを確保するために生体認証は重要であり，その運用には，コンピュータの処理及び管理が必要である。

(3)　コンピュータ処理する個人情報

これまで取り扱ってきたア・イに加え，新たにウの情報を取り扱う。

ア　指紋情報

指紋の特徴点とリレーション

※　リレーションとは

特徴点と他の特徴点との間を横切る「隆線」の数の情報のこと。

→特徴点の情報に付加することで照合精度を向上させる。

イ　管理情報

職員番号，氏名

ウ　指静脈情報

指静脈の位置情報

(4)　実施時期

２０１２年１０月（予定）

(5)　データの管理

データの管理については，ＩＴ推進課コンピュータ室内に設置の生体情報を管理するサーバで行う。

なお，コンピュータ室への入退室については，入室できる人員を制限し指紋による個人認証を行うとともに，監視カメラにより厳重な管理を行っている。

(6)　セキュリティ対策

生体認証システムでは，生体情報の紋様や構造そのものを画像として扱うのではなく，特徴点や位置情報をデータとして認識するものであり，データから静脈及び指紋を復元または再生することはできない。また，生体情報読み取り装置とサーバ間のデータのやりとりは暗号化して通信する仕組みとなっているため，たとえ悪意のある者に通信を傍受されたとしても悪用されるおそれはないと言える。

なお，本システムの運用にあたっては，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に基づき，個人情報の保護並びに安全対策を図っていく。

(7)　提出資料

資料１　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，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。

不正な端末操作を防ぐためには，厳格な本人認証が不可欠となるが，ＩＤ・パスワードによる認証やカードなどの持ち物認証では，紛失や盗難による，なりすましの危険性が高くなる。

対して，指紋や顔，静脈，瞳の虹彩といった生物個体が持っている特性を利用した生体認証は，紛失や盗難の恐れがなく，限りなく確実な本人認証をすることができる。さらに，複数の生体認証方式を導入することによって，利用者の身体的な状態に左右されることなく認証を行うことが可能となる。

機微な情報を取り扱う市の業務において，セキュリティを確保するために生体認証は重要であり，その運用には，コンピュータの処理及び管理が必要である。

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。

(2)　安全対策について

実施機関では，次の安全対策を講じている。

ア　データの管理については，ＩＴ推進課コンピュータ室内に設置の生体情報を管理するサーバで行う。

イ　コンピュータ室への入退室については，入室できる人員を制限し指紋による個人認証を行うとともに，監視カメラにより厳重な管理を行っている。

ウ　生体認証システムでは，　生体情報の紋様や構造そのものを画像として扱うのではなく，特徴点や位置情報をデータとして認識するものであり，データから静脈及び指紋を復元または再生することはできない。

エ　生体情報読み取り装置とサーバ間のデータのやりとりは暗号化して通信する仕組みとなっているため，たとえ悪意のある者に通信を傍受されたとしても悪用されるおそれはないと言える。

オ　本システムの運用にあたっては，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に基づき，個人情報の保護並びに安全対策を図っていく。

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