官報
（号外）
明治二十五年三月三十一日　第三種郵便物認可
独立行政法人国立印刷局

目次



## 告示

○総務省告示第四百一号

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の規定による通知カード及び個人番号カード並びに情報提供ネットワークシステムによる特定個人情報の提供等に関する省令（平成二十六年総務省令第八十五号）第四十条、第四十一条、第四十三条、第四十四条第一項、第四十五条第二項及び第四十六条第一項の規定に基づき、電気通信回線を通じた送信又は電磁的記録媒体の送付の方法及び情報提供ネットワークシステムを使用した送信の方法に関する技術的基準を次のように定め、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附則第一条第五号に掲げる規定の施行の日から施行する。

平成二十七年十一月二十五日

総務大臣　山本　早苗

電気通信回線を通じた送信又は電磁的記録媒体の送付の方法及び情報提供ネットワークシステムを使用した送信の方法に関する技術的基準

第１　目的

この告示は、情報提供ネットワークシステム（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「法」という。）第２条第14項に規定する情報提供ネットワークシステムをいう。以下同じ。）を利用した法第19条第７号の規定による特定個人情報（法第２条第８項に規定する特定個人情報をいう。以下同じ。）の提供の求め又は提供が円滑かつ安全に行われるよう、電気通信回線を通じた送信又は電磁的記録媒体の送付の方法及び情報提供ネットワークシステムを使用した送信の方法について、行政機関の長等（法第２条第14項に規定する行政機関の長等をいう。以下同じ。）の実施すべき事項を定めることを目的とする。

第２　用語の定義

１　コアシステム

情報提供ネットワークシステムを構成するものであって、情報提供用個人識別符号（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施行令（平成26年政令第155号。以下「令」という。）第20条第１項に規定する情報提供用個人識別符号をいう。以下同じ。）を生成し、一の情報提供用個人識別符号により識別される特定の個人と他の情報提供用個人識別符号により識別される特定の個人とが同一の者であるかどうかを確認し、法第23条第３項に規定する記録に記録された特定個人情報を保存し、その他法第19条第７号の規定による特定個人情報の提供を管理するための総務大臣の使用に係る電子計算機その他の機器により構成される電子情報処理組織

２　インターフェイスシステム

情報提供ネットワークシステムを構成するものであって、コアシステムと法第19条第７号に規定する情報照会者又は情報提供者（以下「情報照会者等」という。）の使用に係る電子計算機との間で、同号の規定による特定個人情報の提供の求め又は提供に必要な処理を行うための行政機関の長等の使用に係る電子計算機その他の機器により構成される電子情報処理組織

３　情報提供等事務

情報提供等事務（法第24条に規定する事務をいう。以下同じ。）に使用するため、インターフェイスシステムに電気通信回線で接続する電子情報処理組織であって、コアシステム及びインターフェイスシステム以外のもの

４　ファイアウォール

電気通信回線において不正侵入を防御するための通信を制御する装置

5　ドキュメント
　インターフェイスシステム及び情報提供等事務に使用する他の情報システム（以下「インターフェイスシステム等」という。）の設計、開発及び運用に関する記録及び文書
6　データ
　行政機関の長等の使用に係る電子情報処理組織において通知され、記録され、保存され又は提供される情報
7　可搬記憶媒体
　行政機関の長等の使用に係る電子計算機から容易に取り外すことのできる記憶媒体（光ディスク等（光ディスク、磁気ディスク又は磁気テープをいう。）、ＵＳＢメモリ又は外付けハードディスクドライブその他これに類するもの。）
8　ファイル
　行政機関の長等の使用に係る電子計算機に内蔵される記憶媒体又は可搬記憶媒体に記録されているデータ
9　電子計算機室
　電子計算機及び電気通信関係装置を設置する室
10　可搬記憶媒体等保管室
　可搬記憶媒体及びドキュメントを保管する室
11　重要機能室
　電子計算機室、可搬記憶媒体等保管室、受電設備、定電圧・定周波電源装置等の設備を設置する室並びに電子計算機室及び可搬記憶媒体等保管室の空気調和をする空気調和機及びその附属設備を設置する室

第３　体制、規程等の整備
１　体制の整備
(1)　責任体制等の確立
　情報提供ネットワークシステムを使用して、円滑かつ安全に特定個人情報の授受を実施するとともに、インターフェイスシステム等のセキュリティを確保するため、インターフェイスシステム等の企画、開発及び運用保守に関する責任体制及び連絡体制を明確にすること。また、防災組織及び防犯組織を整備し、通常時及び非常時の責任体制及び連絡体制の確立を図ること。
(2)　監視体制の整備
　インターフェイスシステム等の運用に関し、異常な状態を早期に発見し、総務大臣に連絡することができるよう体制の整備を図ること。
２　規程等の整備
(1)　規程の整備
　インターフェイスシステム等の企画、開発及び運用保守に関する規程を整備すること。
(2)　運用等に係るドキュメントの整備
　インターフェイスシステム等に関する設計書、台帳、操作手順書及び緊急時における作業手順書等を整備し、適切に維持管理を行うこと。
３　人事、教育、研修等
(1)　要員管理
　インターフェイスシステム等の企画、開発及び運用保守に必要な職員を適切に配置するとともに、交替等の人事管理を適切に行うこと。
(2)　教育及び研修
　インターフェイスシステム等の企画、開発及び運用保守を実施する職員に対し、インターフェイスシステム等の操作、セキュリティ対策についての教育及び研修を行うための計画を策定し、その実施体制を確立するとともに、職員に対する教育及び研修を適切に行うこと。
４　セキュリティ対策
　セキュリティ対策に関する情報の収集及び分析を実施するとともに、インターフェイスシステム等の企画、開発及び運用保守の各段階におけるセキュリティ対策の点検及び評価を行い、その結果に基づきインターフェイスシステム等に関するセキュリティ対策の改善を行うこと。
５　緊急事態発生時の体制等
(1)　作動停止等発生時における事務処理体制
ア　インターフェイスシステム等の構成機器、関連設備又はソフトウェアの障害等によりインターフェイスシステム等の全部又は一部の作動停止又は異常作動の発生（以下「作動停止等発生」という。）時の行動計画、総務大臣への報告方法及び他の行政機関の長等との連絡方法等について、あらかじめ定めること。
イ　作動停止等発生時に適切な対応を行うことができるよう、他の行政機関の長等と連携を図り、行動計画、総務大臣への報告方法及び他の行政機関等との連絡方法等について教育及び研修を行うこと。
ウ　作動停止等発生時には、その旨を速やかに総務大臣に報告すること。また、インターフェイスシステム等の復旧等に必要な措置等を講じ、作動停止等発生の根本原因及び再発防止策について検討を行い、その内容について総務大臣に報告するとともに、再発防止に努めること。
(2)　不正アクセス行為発生時における事務処理体制
ア　インターフェイスシステム等への不正アクセス行為発生（以下「不正アクセス行為発生」という。）時の行動計画、総務大臣への報告方法及び他の行政機関の長等との連絡方法等について、あらかじめ定めること。
イ　不正アクセス行為発生時に適切な対応を行うことができるよう、他の行政機関の長等と連携を図り、行動計画、総務大臣への報告方法及び他の行政機関の長等との連絡方法等について教育及び研修を行うこと。
ウ　不正アクセス行為発生時には、その旨を速やかに総務大臣に報告すること。また、被害状況の把握及び被害の拡大を防止するための措置等必要な対策を講じ、総務大臣に報告すること。さらに、不正アクセス行為発生の根本原因及び再発防止策について検討を行い、その内容について総務大臣に報告するとともに、再発防止に努めること。
(3)　情報漏えい等発生時における事務処理体制
ア　法第12条に規定する措置を講ずるに当たっては、情報提供用個人識別符号及び特定個人情報の漏えいその他これに準ずる事態の発生（以下「情報漏えい等発生」という。）時の行動計画及び総務大臣への報告方法等について、あらかじめ定めること。
イ　情報漏えい等発生時に適切な対応を行うことができるよう、行動計画及び総務大臣への報告方法等について教育及び研修を行うこと。
ウ　情報漏えい等発生時には、被害状況の把握及び被害の拡大を防止するための措置等必要な対策を講じ、情報漏えい等発生の旨、被害状況及び講じた対策等について総務大臣に報告すること。また、情報漏えい等発生の根本原因及び再発防止策について検討を行い、その内容について総務大臣に報告するとともに、再発防止に努めること。
(4)　緊急事態の早期発見
　作動停止等発生、不正アクセス行為発生及び情報漏えい等発生を早期に発見するために必要な措置を講ずること。

第４　インターフェイスシステムの環境及び設備
１　建物及び重要機能室
(1)　建物等への侵入の防止等
ア　インターフェイスシステムを設置する建物及び重要機能室（以下「建物等」という。）の壁、窓、ドア等が容易に破壊されないよう必要な措置を講ずること。
イ　建物等への侵入を検知するための措置を講ずること。
ウ　電力及び電気通信回線の切断等を防止するための措置を講ずること。
エ　重要機能室の外に設置された関連設備に対する不当な接触の防止について、必要な措置を講ずること。
(2)　重要機能室の配置及び構造
ア　重要機能室の配置及び構造については、セキュリティ対策及び保守が容易に行えるよう配慮すること。
イ　重要機能室については、外部に対してその表示を行わない等、できるだけ所在を明らかにしないようにすること。
ウ　重要機能室に、緊急事態発生の際の連絡設備を設ける等、連絡体制を整備すること。
エ　電子計算機室及び可搬記憶媒体等保管室は、他の部屋と区分された、施錠可能な専用の部屋とすること。施錠可能な専用の部屋を確保できない場合は、電子計算機及び電気通信関係装置を厳重に固定し、可搬記憶媒体及びドキュメントを専用保管庫により施錠保管すること。
オ　電子計算機室及び可搬記憶媒体等保管室の常時利用する出入口を限定すること等により、侵入の防止を容易に行えるよう配慮すること。
２　障害の防止等
(1)　電気的及び機械的障害の防止等
インターフェイスシステムの構成機器又は関連設備の電気的及び機械的障害の発生を防止し、これらの障害の発生を検知し、及びこれらの障害が発生した場合の対策を行うため、必要な設備の整備等について適切な措置を講ずること。
(2)　水又は蒸気による障害の防止等
水又は蒸気によるインターフェイスシステムの構成機器又は関連設備の障害の発生を防止し、これらの障害の発生を検知し、及びこれらの障害が発生した場合の対策を行うため、必要な設備の整備等について適切な措置を講ずること。
(3)　火災による破損の防止等
建物等からの出火の防止のため、必要な措置を講ずること。また、建物等の火災によるインターフェイスシステムの構成機器又は関連設備の損傷を防止し、それらの損傷の発生を検知し、及びこれらの損傷が発生した場合の対策を行うため、必要な設備の整備等について適切な措置を講ずること。
(4)　地震による破損の防止等
地震による建物等又はインターフェイスシステムの構成機器若しくは関連設備の損傷を防止し、これらの損傷を検知し、及びこれらの損傷が発生した場合の対策を行うため、必要な設備の整備等について適切な措置を講ずること。
(5)　急激な温湿度変化等に対する措置
空気調和設備について、その容量に配慮するとともに、急激な温湿度変化等に対する措置を講ずること。
(6)　転倒、移動等に対する措置
インターフェイスシステムの構成機器及び関連設備について、転倒、移動等に対する措置を講ずること。
(7)　その他の障害の防止等
動物等によるインターフェイスシステムの構成機器及び関連設備の障害の発生を防止し、これらの障害の発生を検知し、及びこれらの障害が発生した場合の対策を行うため、必要な措置を講ずること。
３　電気通信回線の設備
電気通信回線からのデータの盗取を防止するため、インターフェイスシステムとコアシステム又は他のインターフェイスシステムとを結ぶ電気通信回線について、総務大臣が別に定める高度なセキュリティを確保した行政専用の電気通信回線を使用すること。ただし、同一の電子計算機室にある等情報の盗取の防止について必要な措置が講じられていると認められる場合については、この限りでない。
第５　インターフェイスシステムの管理
１　入退室管理
(1)　入退室及び鍵の管理
ア　重要機能室への入室者を限定すること。
イ　重要機能室の出入口の鍵を所定の場所に保管し、その管理は定められた者が行うこと。
ウ　重要機能室への入室者が入室する権限を有することを確認する方法をあらかじめ定めるとともに、重要機能室に入室しようとする者に重要機能室の出入口の鍵を貸与する際に、その者が入室する権限を有することを確認すること。
エ　重要機能室への入退室については、入退室管理台帳により適切に管理すること。
(2)　搬出入物品の確認
重要機能室へ物品を搬出入する際、重要機能室に入室する権限を有する職員に当該物品の内容を確認させること。
(3)　重要機能室の管理
インターフェイスシステムの構成機器及び関連設備等の盗難、損壊等を防止するため、重要機能室に入室する権限を有する者が不在となる時の重要機能室の施錠等、必要な措置を講ずること。
２　インターフェイスシステムの通信制御等
(1)　アクセス権限の限定
インターフェイスシステムの運用保守を実施する職員等必要な者に対してのみ、電子計算機、データ、ドキュメント、ファイル、可搬記憶媒体等に関し、必要なアクセス権限を付与すること。
(2)　ファイアウォールによる通信制御
電気通信回線に接続する電子計算機若しくは電気通信関係装置における不正行為又は電子計算機若しくは電気通信関係装置への不正アクセス行為に対して情報提供ネットワークシステムを保護するため、インターフェイスシステムとコアシステム又は他のインターフェイスシステムとの間にファイアウォールを設置し、通信制御を行うこと。ただし、同一の電子計算機室にある等、通信制御を行う必要がないと認められる場合については、この限りでない。
(3)　通信相手の認証
インターフェイスシステムとコアシステム又は他のインターフェイスシステムとの間の通信について、通信相手の認証を行うこと。ただし、同一の電子計算機室にある等、通信相手の認証を行う必要がないと認められる場合については、この限りでない。
(4)　通信の暗号化
インターフェイスシステムとコアシステム又は他のインターフェイスシステムとの間の通信について、暗号化を実施すること。ただし、同一の電子計算機室にある等、通信の暗号化を行う必要がないと認められる場合については、この限りでない。

(5)　秘密鍵の厳重な管理
　通信相手の認証及び通信の暗号化を行うために必要な秘密鍵を厳重に保護し、外部に漏えいすることを防止するための措置を講ずること。
(6)　帯域の確保
　インターフェイスシステムとコアシステム又は他のインターフェイスシステムとの接続に係る電気通信回線の通信について、情報提供等事務の処理が遅滞なく実施できるよう必要な帯域を確保すること。
3　可搬記憶媒体の管理
(1)　保管場所
　可搬記憶媒体は、保管庫等を設けることにより、できるだけ常温常湿の場所に保管すること。
(2)　持出し及び返却の確認等
　可搬記憶媒体の盗難の防止等のため、その保管位置を指定し、持ち出した場合は返却を確認すること。
(3)　廃棄
　可搬記憶媒体を廃棄する場合には、消磁、破砕、溶解その他の当該可搬記憶媒体に記録されていたファイル及びドキュメントの復元が不可能となる措置を講ずること。
(4)　不正プログラムの混入防止
　可搬記憶媒体への不正プログラムの混入防止のため、必要な措置を講ずること。
4　構成機器及び関連設備等の管理
(1)　管理方法の明確化
ア　インターフェイスシステムに機器を接続するための手続、方法等を定めるとともに、構成機器及び関連設備等の管理方法を明確にすること。
イ　使用するインターフェイスシステムの構成機器及び可搬記憶媒体の種類、数量等を体系的かつ一元的に記録管理し、現況と一致させること。また、この記録管理された内容を関係職員に周知し、記録管理しているインターフェイスシステムの構成機器又は可搬記憶媒体以外のものを使用しないこと。
(2)　保守の実施
　インターフェイスシステムの構成機器及び関連設備等の保守を定期に又は随時に実施すること。また、保守の実施に当たっては、エラーの発生及び不正行為を防止し、データを保護するため、必要な措置を講ずること。
(3)　稼働状況の監視
　緊急事態や障害を早期に発見するため、インターフェイスシステムの構成機器の稼働状況を監視すること。
(4)　不正プログラムの混入の検知等
　インターフェイスシステムにコンピュータウイルス等の不正プログラムが混入されていないかどうかを監視する措置を講じ、混入されていた場合には駆除する措置を講ずること。また、コンピュータウイルス等の不正プログラムが発見された場合の必要な措置を定め、インターフェイスシステムを運用保守する職員に周知すること。
5　ファイル、ドキュメント等の管理
(1)　ファイル及びドキュメントの取扱い及び管理
ア　ファイル及びドキュメントについて、定められた場所に保管すること、受渡し及び保管に関し必要な事項を記録すること、使用、複写、消去及び廃棄は責任者の承認を得て行うとともに、その記録を作成すること等、その取扱い及び管理の方法を明確にすること。
イ　ファイル及びドキュメントを廃棄する場合には、消磁、破砕、溶解等の措置を講ずること。
6　委託を行う場合等の措置
(1)　委託先事業者等の社会的信用等の確認
　インターフェイスシステムの開発、変更及び運用保守等について、委託を行う場合には、委託先事業者等の社会的信用と能力を確認すること。
(2)　委託先事業者等に対する監督
　委託先事業者等に対し、必要なセキュリティ対策を実施させるとともに、適切な監督を行うこと。また、委託先事業者等による不正行為を防止するため、必要な措置を講ずること。
(3)　再委託の制限等
　委託業務の一部を第三者に再委託する場合の制限、事前申請及び承認に関する事項を委託先事業者等とあらかじめ取り決めること。
(4)　秘密保持に関する措置
　委託先事業者等から、その従事者に係る秘密保持に関する誓約書を提出させる等の措置を講ずること。

第6　情報提供等事務に使用する他の情報システムとの接続等
　情報提供等事務に使用する他の情報システムについて、第3に定めるもののほか、以下に定める。
1　ファイアウォールによる通信制御
　電気通信回線に接続する電子計算機若しくは電気通信関係装置における不正行為又は電子計算機若しくは電気通信関係装置への不正アクセス行為に対して情報提供ネットワークシステムを保護するため、情報提供等事務に使用する他の情報システムとインターフェイスシステムとの間にファイアウォールを設置し、通信制御を行うこと。ただし、情報提供等事務に使用する他の情報システムとインターフェイスシステムが同一の電子計算機室にある等通信制御を行う必要がないと認められる場合については、この限りでない。
2　通信相手の認証
(1)　コアシステムとの通信
　情報提供等事務に使用する他の情報システムとコアシステムとの間の通信について、通信相手相互の認証を行うこと。ただし、同一の電子計算機室にある等通信相手の認証を行う必要がないと認められる場合については、この限りでない。
(2)　インターフェイスシステムとの通信
　情報提供等事務に使用する他の情報システムとインターフェイスシステムとの間の通信について、通信相手の認証を行うこと。ただし、同一の電子計算機室にある等通信相手の認証を行う必要がないと認められる場合については、この限りでない。
3　通信の暗号化
　情報提供等事務に使用する他の情報システムとインターフェイスシステムとの間の通信について、暗号化を実施すること。ただし、同一の電子計算機室にある等通信の暗号化を実施する必要がないと認められる場合については、この限りでない。
4　特定個人情報の暗号化
　情報提供等事務に使用する他の情報システムが情報照会者に特定個人情報を送信する場合は、当該特定個人情報の暗号化を実施すること。ただし、同一の電子計算機室にある等特定個人情報の暗号化を実施する必要がないと認められる場合については、この限りでない。
5　秘密鍵の厳重な管理
　情報提供等事務に使用する他の情報システムとコアシステム又はインターフェイスシステムとの間で通信相手の認証及び通信の暗号化を行うために、並びに情報提供等事務に使用する他の情報システムが情報照会者に特定個人情報を送信する場合に当該特定個人情報の暗号化を行うために必要な秘密鍵を厳重に保護し、外部に漏えいすることを防止するための措置を講ずること。

6　電気通信回線の設備

電気通信回線からデータの盗取を防止するため、情報提供等事務に使用する他の情報システムとインターフェイスシステムとを結ぶ電気通信回線について、総務大臣が別に定める高度なセキュリティを維持した行政専用の電気通信回線を使用すること。ただし、情報提供等事務に使用する他の情報システムとインターフェイスシステムが同一の電子計算機室にある等情報の盗取の防止について必要な措置が講じられていると認められる場合については、この限りでない。

7　帯域の確保

情報提供等事務に使用する他の情報システムとインターフェイスシステムとの接続に係る電気通信回線の通信について、情報提供等事務の処理が遅滞なく実施できるよう必要な帯域を確保すること。

8　時刻の管理

情報提供等事務に使用する他の情報システムの管理する時刻の正確性を確保するために必要な措置を講ずること。

第7　地方公共団体情報システム機構における電気通信回線等の管理

1　電気通信回線の設備等

(1)　ファイアウォールによる通信制御

コアシステムと地方公共団体情報システム機構（以下「機構」という。）の使用に係る電子計算機との間にファイアウォールを設置し、必要な通信のみが可能となるよう通信制御を行うこと。

(2)　通信相手の認証

コアシステムと機構の使用に係る電子計算機との間の通信について、通信相手相互の認証を行うこと。

(3)　データの暗号化

コアシステムと機構の使用に係る電子計算機との間でデータを送信する場合は、当該データを暗号化すること。

(4)　秘密鍵の厳重な管理

コアシステムと機構の使用に係る電子計算機との間で通信相手相互の認証及びデータの暗号化を行うために必要な秘密鍵を厳重に保護し、外部に漏えいすることを防止するための措置を講じること。

(5)　専用回線の使用

電気通信回線からのデータの盗取を防止するため、コアシステムと機構の使用に係る電子計算機とを結ぶ電気通信回線について、専用回線（接続先が固定されており、所定の伝送速度が保証されている回線をいう。以下同じ。）を使用すること。

(6)　帯域の確保

コアシステムと機構の使用に係る電子計算機とを結ぶ電気通信回線の通信について、情報提供等事務の処理が遅滞なく実施できるよう必要な帯域を確保すること。

(7)　予備の回線の設置

通信が途絶しないようにするため、コアシステムと機構の使用に係る電子計算機を結ぶ電気通信回線に予備の回線を設けること。

2　検査用符号の生成及び通知等

(1)　検査用符号の生成及び通知

機構は、情報照会者等から令第20条第2項の規定による通知を受けたときは、符号取得処理検査用符号（総務大臣が令第20条第6項の規定により通知した情報提供用個人識別符号に係る個人番号を構成する整数のうち、検査用数字（令第8条に規定される検査用数字をいう。以下同じ。）以外の各整数の総和を10で除した際に生じた剰余の数。以下同じ。）を生成し、総務大臣に対し、令第20条第4項の規定による住民票コードの通知とともに、当該符号取得処理検査用符号を通知すること。

(2)　住民票コードの通知に係る正確性の確保

機構は、情報照会者等から令第20条第2項の規定による通知を受けたときは、総務大臣に対し、同項の特定の個人に係る住民票に記載された住民票コード（当該住民票コードが変更されたものであるときは、変更される前の内容を含む。）を正確に通知すること。

第8　特定個人情報の提供の求め及び提供における留意事項

1　情報提供等個人識別符号の取得に使用する電気通信回線の設備等

(1)　ファイアウォールによる通信制御

情報照会者等の使用に係る電子計算機と機構の使用に係る電子計算機との間にファイアウォールを設置し、必要な通信のみが可能となるよう通信制御を行うこと。

(2)　通信相手の認証

情報照会者等の使用に係る電子計算機と機構の使用に係る電子計算機との間の通信について、通信相手相互の認証を行うこと。

(3)　データの暗号化

情報照会者等の使用に係る電子計算機と機構の使用に係る電子計算機との間でデータを送信する場合は、当該データを暗号化すること。

(4)　秘密鍵の厳重な管理

情報提供者等の使用に係る電子計算機と機構の使用に係る電子計算機との間で通信相手相互の認証及びデータの暗号化を行うために必要な秘密鍵を厳重に保護し、外部に漏えいすることを防止するための措置を講ずること。

(5)　専用回線の使用

電気通信回線からのデータの盗取を防止するため、情報提供者等の使用に係る電子計算機と機構の使用に係る電子計算機とを結ぶ電気通信回線について、専用回線を利用すること。

2　情報提供用個人識別符号の適切な取扱い等

(1)　情報提供用個人識別符号の適切な取扱いの確保

ア　情報照会者等は、総務大臣から令第20条第6項の規定による情報提供用個人識別符号の通知を受けたときは、速やかに、当該情報提供用個人識別符号に係る本人を識別するために当該情報照会者等が用いる番号、記号その他の符号又は個人番号（法第2条第5項に規定する個人番号をいう。以下同じ。）に正確に紐付けること。

イ　情報照会者等は、情報提供用個人識別符号の紐付けの正確性を確保するために、符号取得処理検査用符号を生成し、総務大臣から情報提供用個人識別符号とともに通知された符号取得処理検査用符号と同一のものであるかどうかを確認すること。

ウ　情報照会者等は、情報提供用個人識別符号を利用する職員等必要な者に対してのみ、当該情報提供用個人識別符号を含む特定個人情報ファイルに関し、必要なアクセス権限を付与すること。

(2)　提供の求めの対象となる特定個人情報の正確性の確保

情報提供者は、法第22条第1項の規定により特定個人情報を提供するため、当該情報提供者の使用に係る電子計算機に格納する同項の提供の求めの対象となる特定個人情報を正確かつ最新の内容に保つこと。

3　操作者の識別

情報照会者は、その職員のうち、法第19条第７号の規定による特定個人情報の提供の求めをした特定の職員を識別するための適切な措置を講ずること。

4　不正アクセス行為等による特定個人情報の不正な提供の求めの防止

(1)　不正な特定個人情報の提供の求めの防止

情報照会者は、不正アクセス行為及び不正プログラムの混入等による不正な特定個人情報の提供の求めを防ぐために必要な措置を講ずること。

(2)　特定個人情報の漏えいの防止

情報照会者等は、その使用に係る、特定個人情報（情報提供用個人識別符号を含む。）が通知され、記録され、保存され又は提供される電子情報処理組織について、インターネットの使用に用いる回線からの分離及び可搬記憶媒体の適切な管理等により、不正プログラムの混入防止措置その他の特定個人情報（情報提供用個人識別符号を含む。）の漏えい防止に必要な措置を講ずること。

5　特定個人情報の提供の求め又は提供が不適法に行われた場合

(1)　特定個人情報の提供の求めが不適法に行われた場合

情報照会者は、法第19条第７号の規定による特定個人情報の提供の求めが不適法に行われた場合（法第21条第２項各号のいずれかに該当する場合を除く。）は、提供された情報の削除等必要な措置を講じ、当該求めが行われた旨及び講じた措置について総務大臣に報告すること。また、当該情報提供の求めが生じた根本原因及び再発防止策について検討を行い、その内容について総務大臣に報告するとともに、再発防止に努めること。

(2)　特定個人情報の提供が不適法に行われた場合

情報提供者は、法第19条第７号の規定による特定個人情報の提供が不適法に行われた場合は、情報照会者に対し提供した情報の削除を求める等必要な措置を講じ、当該提供が行われた旨及び講じた措置について総務大臣に報告すること。また、当該提供が生じた根本原因及び再発防止策について検討を行い、その内容について総務大臣に報告するとともに、再発防止に努めること。

第９　情報提供ネットワークシステムへの接続等における留意事項

１　総務大臣との必要な調整等

(1)　各府省の長の所管の機関に関する調整等

情報照会者等（地方公共団体の機関を除く。）が自らの使用に係る電子情報処理組織を情報提供ネットワークシステムに接続しようとするときは、当該情報照会者等が行う事業を所管する府省を経由して、総務大臣と必要な調整等を行うこと。調整等における連絡体制及び連絡経路については、通常時及び緊急時の対応が適切に実施されるものとなるよう留意すること。

(2)　地方公共団体の機関に関する調整等

地方公共団体の機関が自らの使用に係る電子情報処理組織を情報提供ネットワークシステムに接続しようとするときは、機構を経由して、総務大臣と必要な調整等を行うこと。調整等における連絡体制及び連絡経路については、通常時及び緊急時の対応が適切に実施されるものとなるよう留意すること。

(3)　その他総務大臣との調整

情報提供ネットワークシステムと行政機関の長等の使用に係る電子情報処理組織を接続しようとするときは、あらかじめ、総務大臣と必要な調整を行うこと。ただし、(1)及び(2)の場合を除く。

２　特定個人情報保護評価の実施

(1)　特定個人情報保護評価の実施

情報照会者等は、自らの使用に係る電子情報処理組織を情報提供ネットワークシステムと接続しようとするときは、あらかじめ特定個人情報保護評価を実施すること。

(2)　総務大臣への報告

情報照会者等は、特定個人情報保護評価を変更した場合は、速やかに総務大臣に報告すること。

第10　その他

１　総務大臣が定める仕様

インターフェイスシステムについては、総務大臣の提示する指針を踏まえたものとすること。

２　その他総務大臣が定める事項

この告示に定めるもののほか、情報提供ネットワークシステムの運営に関し必要な事項は、総務大臣が定める。