乙第１３号証

# 情報提供ネットワークシステム
# 接続運用規程

## 施行準備版

## 第 2.0 版

平成 28 年 7 月

総務省

改訂履歴

| 日付 | 改訂内容 |
| --- | --- |
| 平成28年３月 | 施行準備版　第1.0版　作成 |
| 平成28年７月 | 施行準備版　第2.0版　作成 |

# 1　はじめに

## 1.1　本規程の目的

本規程は、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（平成 25 年法律第 27 号。以下「番号法」という。）に基づき、総務大臣が設置及び管理を行う情報提供ネットワークシステムへの情報照会者及び情報提供者その他の関係する者が有する情報システムの接続及びその後の使用に関する手続並びに必要となる情報セキュリティ対策等の情報提供ネットワークシステムに接続して行う運用に関して遵守すべき基本事項を定め、情報提供ネットワークシステムを使用した情報連携の円滑かつ安定的な運用を確保することを目的とする。

## 1.2　本規程の適用対象者

本規程の適用対象者は、以下の情報提供ネットワークシステムと接続する機関等とする。

- 情報照会者等
- 情報連携事務等の所管府省
- 情報照会者等の所管府省
- 集約機関
- 取りまとめ都道府県
- 住民基本台帳ネットワークシステム運営主体
- 情報提供等記録開示システム運営主体
- 監視・監督システム運営主体

## 1.3 本規程の位置付け

本規程は、番号法の規定及び「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並びに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」（平成 27 年総務省告示第 401 号。以下単に「技術的基準」という。）に基づき、情報提供ネットワークシステムへの接続、その後の運用及び接続の停止からなるライフサイクルにおいて、遵守すべき基本事項を規定した文書であり、情報提供ネットワークシステムに接続して行う運用（以下「接続運用」という。）に関して依拠すべき文書の一つとして位置付ける。

本規程を含む接続運用に関する規程の体系を「図 1-1：接続運用に関する規程の体系」に示す。

本規程における規定事項は、下図に示す文書及び設計関連文書に業務・システムの両面から準拠することを前提としている。また、その他の法令及び所管府省等からの通知等があった際には、当該通知等に準拠する。

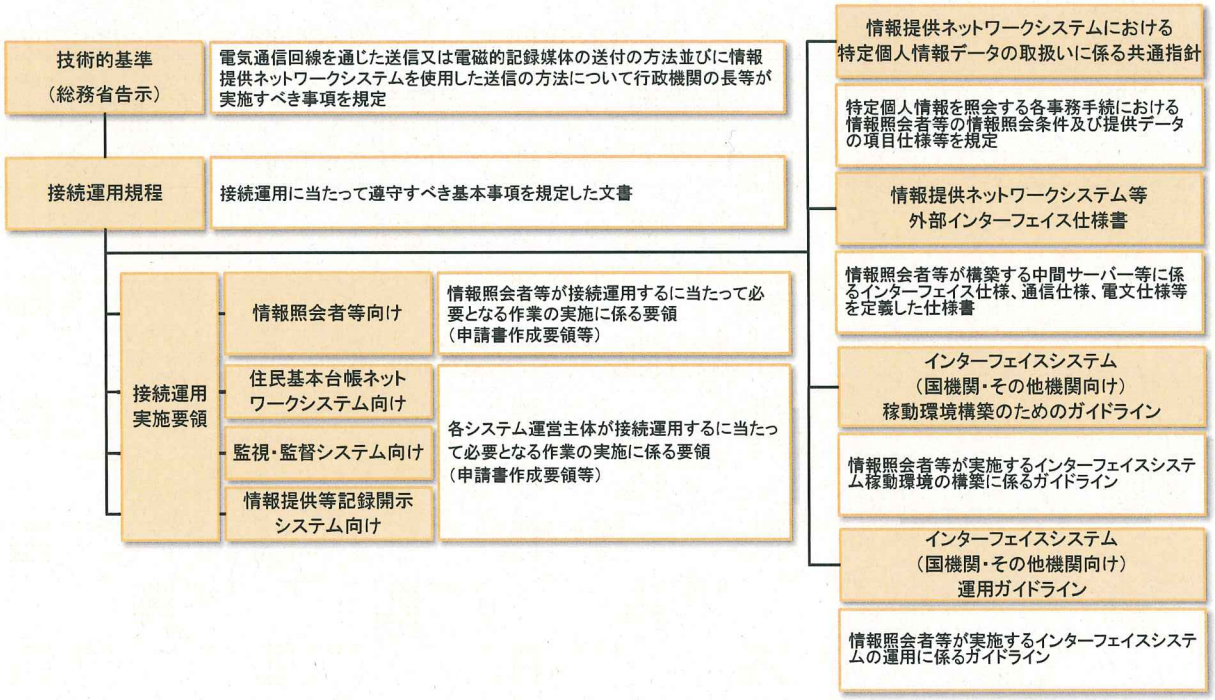


**図 1-1：接続運用に関する規程の体系**

また、本規程で定める接続運用に当たって必要な作業に係る実施要領として接続運用実施要領を別途定める。接続運用実施要領は、情報照会者等が中心となって実施する接続運用に係る要領を示す情報照会者等向けに加え、情報提供ネットワークシステムに接続する住民基本台帳ネットワークシステム、監視・監督システム及び情報提供等記録開示システムの各運営主体と情報提供ネットワークシステムとの間で実施する接続運用に係る要領を示した各システム向けの接続運用実施要領を定める。

各運営主体においては、接続運用規程及び接続運用実施要領に従って接続運用を行う。

なお、番号法に関する各種政策の見直し、制度改正等の変更により、記載事項等の見直しを行う必要が生じた場合は、接続運用に関する規程の構成又は内容の改訂を行う。施行準備版については、番号法附則第２条に基づき準備行為として策定するものであり、今後施行までに総合運用テストを踏まえ、必要に応じて見直しを行う。

## 2.7　安全管理措置

本項では、番号法第 24 条の規定及び技術的基準に基づき、接続運用に当たって接続機関が実施すべき安全管理措置について定める。なお、情報照会者等の所管府省、集約機関及び取りまとめ都道府県については、取りまとめ対象となる情報照会者等の安全管理措置の内容についても、適切な安全管理措置が講じられていることを確認する。

安全管理措置の適用対象となる機関及び関係システムを「表 2-8：安全管理措置の適用対象となる機関及び関係システム」に示す。「別紙２：安全管理措置一覧及び自己点検表」における「担当者等」は、「2.1　責任体制」に示す担当者等に加え、情報連携事務等の実施担当者を含むこととする。

**表 2-8：安全管理措置の適用対象となる機関及び関係システム**

| 適用対象となる機関 | 適用対象となる関係システム | 概要 |
|---|---|---|
| 各情報照会者等 | インターフェイスシステム、中間サーバー等及び既存システム | 左記の情報システムにおいて共通的に遵守すべき事項を「別紙２：安全管理措置一覧及び自己点検表」のとおり規定 |
| 集約機関 | インターフェイスシステム及び中間サーバー等 | |
| 住民基本台帳ネットワークシステム運営主体 | 住民基本台帳ネットワークシステム | |
| 情報提供等記録開示システム運営主体 | 情報提供等記録開示システム及びインターフェイスシステム | |
| 監視・監督システム運営主体 | 監視・監督システム | |

当該安全管理措置は、「図 2-12：各関係システムのライフサイクルの各段階に各接続機関が講ずべき安全管理措置」に示すとおり、各接続機関の所管する関係システムが情報提供ネットワークシステムに接続を開始し、その後の運用及び保守等の運営を経て、接続の停止に至るまでのライフサイクルの各段階に応じて講ずべき措置を定めるものである。

具体的には、接続開始に向けて、安全管理措置一覧に掲げる措置事項について、自己点検を実施し、具体策の検討及び措置を講じた上で、接続申請を行う。また、接続開始後の運営においても、安全管理措置に関する自己点検等の計画の策定、実施、実施結果及び計画の評価並びに改善を定期的に行うこととする。

なお、情報提供ネットワークシステム運営主体は、各接続機関の所管する情報システムの接続時における自己点検状況等を確認し、その後も定期的なフォローアップを行うこととする。

各機関において実施した安全管理措置の自己点検及び実施結果の評価の内容は、「様 02-06：安全管理措置確認結果報告書」に確認結果を添付して、情報提供ネットワークシステム運営主体に報告する。

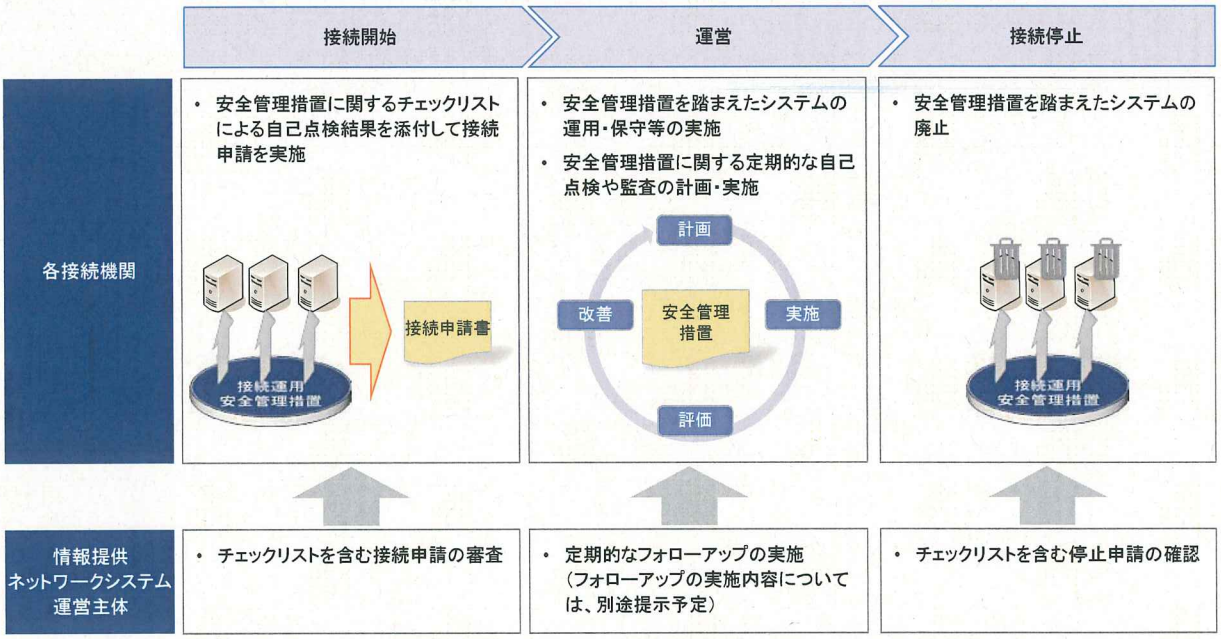


**図 2-12：各関係システムのライフサイクルの各段階に各接続機関が講ずべき安全管理措置**

### 2.7.1 安全管理措置の自己点検方法

各接続機関は、安全管理措置の一覧に基づき、自己点検を実施する。自己点検に係る対応を「表 2-9：安全管理措置の自己点検方法」に示す。各接続機関は、これを用いて自己点検を実施するとともに、自己点検の結果を情報提供ネットワークシステム運営主体に報告することとする。下表で規定する点検頻度に加えて、安全管理措置一覧に示す事項に関連する変更を実施する場合は、各接続機関において該当事項の自己点検を実施する。

安全管理措置一覧に掲げる事項は、重点報告事項とそれ以外の事項に区分する。重点報告事項は、技術的基準で規定する事項に加え、情報提供ネットワークシステムの円滑かつ安定的な運用において重要と認められる事項とし、それ以外の事項は、原則として各接続機関において取り組むべき情報セキュリティ対策の水準確保に係る事項とする。

情報提供ネットワークシステム運営主体によるフォローアップは、重点報告事項を中心に行うこととする。

表 2-9：安全管理措置の自己点検方法

| 項番 | 項目 | 定期点検 | 随時点検 |
|---|---|---|---|
| 1 | 点検頻度 | ・１年に１回 | ・接続申請時<br>・基本計画策定時（ただし、接続申請時を除く。） |
| 2 | 点検事項 | ・安全管理措置の全事項 | |
| 3 | 報告頻度 | ・１年に１回 | ・点検実施の都度による |
| 4 | 報告対象事項 | ・安全管理措置の重点報告事項 | ・安全管理措置の全事項 |
| 5 | 点検単位・方法 | ・「別紙２：安全管理措置一覧及び自己点検表」を用いて機関単位で点検を実施 | |
| 6 | 取りまとめ・提出 | ・「2.3.1　情報提供ネットワークシステム運営主体及び情報照会者等の間の連絡」の規定に沿って実施 | |
| 7 | 実施状況の確認等 | ・情報照会者等の所管府省、取りまとめ都道府県又は集約機関は、点検結果について、内容の不備や確認項目がある場合には、情報照会者等に見直し又は確認を依頼<br>・情報照会者等の所管府省、取りまとめ都道府県又は集約機関は、点検実施状況の確認及び必要に応じた督促を実施 | |

# 安全管理措置一覧及び自己点検表

| # | 項目 | 安全管理措置<br>（最終案） | 重点報告事項 | 自己点検 | |
|---|---|---|---|---|---|
| | | | | 自己点検結果 | 特記事項 |
| | 1 安全管理措置の基本的枠組み | | | | |
| | 1.1 組織・体制の整備 | | | | |
| 1 | (1) 情報セキュリティに関する管理体制の整備 | 情報提供ネットワークシステムに関係する情報システム(以下、「関係システム」と総称する。注１）のセキュリティを確保するため、関係システムに係る企画、開発及び運用保守に関する責任体制を整備すること。 | ○ | | |
| 2 | (2) 監視体制の整備 | 各接続機関は、関係システムに係る情報セキュリティインシデントなどの異常な状態を早期に発見することができる体制を整備すること。 | ○ | | |
| | 1.2 対策推進計画の策定 | | | | |
| 3 | (1) 対策推進計画の策定 | 各接続機関は、関係システムを含む情報セキュリティ対策を総合的に推進するための計画（以下「対策推進計画」という。）を策定すること。また当該計画には以下を含めること。<br>・情報セキュリティ対策基準<br>・情報セキュリティに関する教育<br>・担当者等における情報セキュリティ対策実施状況の点検<br>・情報セキュリティ監査<br>・情報システムに関する技術的な対策を推進するための取組<br>・前各号に掲げるもののほか、情報セキュリティ対策に関する重要な取組 | | | |
| | 1.3 情報セキュリティ関係規程の運用 | | | | |
| 4 | (1) 情報セキュリティ対策に関する実施手順の整備・運用 | 各接続機関は、自機関における情報セキュリティ対策に関する実施手順を整備し、当該実施手順に基づく運用を着実に実施すること。 | ○ | | |
| | 1.4 教育 | | | | |
| 5 | (1) 教育実施計画の策定及び教育の実施 | 各接続機関は、情報セキュリティ対策に係る教育について、対策推進計画に基づき教育実施計画を策定し、当該計画に基づき担当者等に対し教育を実施すること。 | ○ | | |
| | 1.5 情報セキュリティインシデントへの対処 | | | | |
| 6 | (1) 情報セキュリティインシデントに備えた体制の整備 | 各接続機関は、関係システムの情報セキュリティインシデントを認知した際、認知した者からの報告窓口を整備するとともに、関係者への報告手順（所管府省等との情報共有手順を含む。）を整理すること。 | ○ | | |
| 7 | | 各接続機関は、関係システムの情報セキュリティインシデントに備え、緊急連絡先、連絡手段、連絡内容を含む緊急連絡網を整備すること。 | ○ | | |
| 8 | (2) 情報セキュリティインシデントの認知時における対処 | 各接続機関は、関係システムの情報セキュリティインシデントが発生した際は、速やかに被害の拡大防止等を図るための応急措置の実施及び情報セキュリティインシデントからの復旧に係る措置を行うこと。 | ○ | | |
| 9 | (3) 情報セキュリティインシデントの原因調査・再発防止 | 各接続機関は、関係システムの情報セキュリティインシデントが発生した際は、その原因を調査するとともに再発防止策を検討し、当該再発防止策を実施すること。 | ○ | | |
| | 1.6 情報セキュリティ対策実施状況の点検 | | | | |
| 10 | (1) 年度点検計画の策定・実施手順の整備 | 各接続機関は、対策推進計画に基づき、担当者等の情報セキュリティ対策実施状況の年度点検計画を策定するとともに、点検実施手順を整備していること。 | | | |
| 11 | (2) 点検の実施 | 各接続機関は、年度点検計画に基づき、担当者等の情報セキュリティ対策実施状況の点検を実施している、又は実施を予定していること。 | | | |

| # | 項目 | 安全管理措置<br>（最終案） | 重点報告事項 | 自己点検 | |
|---|---|---|---|---|---|
| | | | | 自己点検結果 | 特記事項 |
| 12 | (3) 点検結果の評価・改善 | 各接続機関は、点検結果を全体として分析・評価し、点検の結果により明らかになった問題点について、必要な改善を行っている、又は行うことを予定していること。 | | | |
| | 1.7 見直し | | | | |
| 13 | (1) 情報セキュリティ関係規程の見直し | 各接続機関は、関係システムの情報セキュリティの運用及び自己点検・監査等の結果等を総合的に評価するとともに、情報セキュリティに係る重大な変化等を踏まえ、対策推進計画、情報セキュリティ対策に関する実施手順等について定期的に必要な見直しを行っている、又は行うことを予定していること。 | | | |
| | 2 外部委託 | | | | |
| | 2.1 外部委託 | | | | |
| 14 | (1) 外部委託に係る規程の整備 | 各接続機関は、外部委託に係る委託先の選定基準等を含む規程を整備すること。 | | | |
| 15 | (2) 外部委託に係る契約 | 各接続機関は、関係システムについて外部委託を実施する際には、選定基準及び、事前申請・承認等を含む選定手続に従って委託先を、以下の事項を踏まえて選定すること。<br>(ア) 委託時の委託先事業者等の能力の確認<br>(イ) 委託先事業者等へのセキュリティ対策の実施指示<br>(ウ) 委託先事業者等でのセキュリティ対策の実施状況の監督<br>(エ) 委託先事業者等の不正行為防止措置 | ○ | | |
| 16 | (3) 外部委託における対策の実施 | 各接続機関は、契約に基づき、関係システムの委託先における情報セキュリティ対策の履行状況を確認すること。 | ○ | | |
| 17 | | 各接続機関は、関係システムについて委託した業務において、情報セキュリティインシデントの発生を認知した場合は、委託先に契約に基づく必要な措置を講じさせること。 | | | |
| 18 | | 各接続機関は、関係システムについて委託した業務の終了時に、委託先において取り扱われた情報を確実に返却又は抹消させること。 | | | |
| 19 | (4) 外部委託における情報の取扱い | 各接続機関は、関係システムの委託先への情報の提供等において、以下の事項を遵守すること。<br>(ア) 委託先に情報を提供する場合、提供する情報を必要最小限とし、あらかじめ定められた安全な受渡し方法により提供すること。<br>(イ) 提供した情報が委託先において不要になった場合は、これを確実に返却又は抹消させること。 | | | |
| | 3 情報システムのライフサイクル | | | | |
| | 3.1 情報システムに係る文書等の整備・管理 | | | | |
| 20 | (1) 情報提供ネットワークシステムに係る設計文書等の管理 | 各接続機関は、情報提供ネットワークシステム運営主体から提供された設計文書、マスターデータ等の各種資材について、必要な者のみが閲覧可能とするよう措置を講じるなど秘密保持に係る適切な措置を行うこと。 | ○ | | |
| 21 | (2) 情報システムに係る文書の整備 | 各接続機関は、関係システムの情報セキュリティ対策を実施するために必要となる文書として、以下を網羅した文書を整備すること。<br>(ア) システムを構成するサーバー装置及び端末関連情報<br>(イ) システムを構成する通信回線及び通信回線装置関連情報<br>(ウ) システム構成要素ごとの情報セキュリティ水準の維持に関する手順 | ○ | | |
| 22 | (3) 情報システムに係る文書の情報の取扱い | 各接続機関は、関係システム関連文書について、保管、使用、複写、消去、廃棄などの取扱いに係る規程を定め、当該規程に基づき適切に管理すること。 | ○ | | |

| # | 項目 | 安全管理措置<br>（最終案） | 重点報告事項 | 自己点検 | |
|---|---|---|---|---|---|
| | | | | 自己点検結果 | 特記事項 |
| | 3.2 情報システムのライフサイクルの各段階における対策 | | | | |
| 23 | (1) 情報システムの運用・保守時の対策 | 各接続機関は、関係システムの運用・保守において、情報システムに実装されたセキュリティ機能を適切に運用すること。 | | | |
| 24 | | 各接続機関は、不正な行為及び意図しない関係システムへのアクセス等の事象が発生した際に追跡できるように、運用・保守に係る作業についての記録を管理すること。 | ○ | | |
| 25 | (2) 情報システムの更改・廃棄時の対策 | 各接続機関は、関係システムの更改又は廃棄を行う場合は、当該情報システムに保存されている情報について、当該情報の格付及び取扱制限を考慮した上で、以下の措置を適切に講ずること。<br>(ア) 情報システム更改時の情報の移行作業における情報セキュリティ対策<br>(イ) 情報システム廃棄時の不要な情報の抹消 | | | |
| 26 | (3) 情報システムについての対策の見直し | 各接続機関は、関係システムの情報セキュリティ対策について新たな脅威の出現、運用、監視等の状況により見直しを適時検討し、必要な措置を講ずること。 | ○ | | |
| | 3.3 情報システムの運用継続計画 | | | | |
| 27 | (1) 情報システムの運用継続計画の整備 | 各接続機関は、必要に応じ、関係システムの運用継続計画を策定すること。特に、情報提供ネットワークシステムと直接接続する関係システム及びインターフェイスシステム（以下「直接接続関係システム」と総称する。）については、その策定について十分検討を行うこと。その際、非常時における情報セキュリティに係る対策事項を検討すること。 | | | |
| 28 | (2) 情報システムの運用継続計画の整合的運用の確保 | 各接続機関は、関係システムの運用継続計画の教育訓練や維持改善を行う際等に、非常時における情報セキュリティに係る対策事項が運用可能であるかを確認すること。 | | | |
| | 4 情報システムのセキュリティ要件 | | | | |
| | 4.1 施設・設備の要件 | | | | |
| 29 | (1)情報システムを設置する施設・設備の対策の基準の決定 | 各接続機関は、関係システムの特性及び以下の内容を踏まえて、関係システムを設置する施設・設備の基準を定めること。<br>(ア) 許可されていない者が容易に立ち入ることができないようにするための、施錠可能な扉、間仕切り等の施設の整備、設備の設置等の物理的な対策<br>(イ) 許可されていない者の立入りを制限するため及び立入りを許可された者による立入り時の不正な行為を防止するための入退管理対策 | | | |
| 30 | | ◆ 各接続機関は、直接接続関係システムを設置する施設・設備において、以下の対策を講じること。<br>・建物・室の壁・窓・ドア等を外部から破壊されないための措置<br>・不正な侵入を検知するための措置<br>・電力及び電気通信回線の切断等を防止するための措置<br>・外に設置された関連設備に対する不当な接触を防止するための措置<br>・外部に所在情報を明らかにしないための措置<br>・火災、地震、水害その他の災害等により建物及び関連設備の損傷を防止するための措置<br>・異常事態発生時において緊急連絡を行うための措置 | ○ | | |
| 31 | (2) 情報システムを設置する施設・設備における入退室管理 | ◆ 各接続機関は、直接接続関係システムを設置する施設・設備における入退室管理、鍵管理、搬出入物品管理を行う措置を講じ、管理台帳等により適切に管理すること。また、入室する権限を有する者が不在となる時の施錠等、必要な措置を講ずること。 | ○ | | |

| # | 項目 | 安全管理措置<br>（最終案） | 重点報告事項 | 自己点検 | |
|---|---|---|---|---|---|
| | | | | 自己点検結果 | 特記事項 |
| | 4.2 情報システムのセキュリティ機能 | | | | |
| 32 | (1) 主体認証機能の導入 | 各接続機関は、関係システムが取り扱う情報へのアクセスを管理するため、識別及び主体認証を行う機能を設け、適切に主体認証を行うこと。 | ○ | | |
| 33 | | 各接続機関は、関係システムにおいて、主体認証情報の漏えい等による不正行為を防止するための措置及び不正な主体認証の試行に対抗するための措置を講ずること。 | | | |
| 34 | (2) アクセス制御機能の導入 | 各接続機関は、関係システムが取り扱う情報へのアクセスを、主体によって制御する必要がある場合、当該システムにアクセス制御を行う機能を設け、適切にアクセス制御を行うこと。 | ○ | | |
| 35 | | 各接続機関は、関係システムへのアクセス制御機能の導入に当たり、情報セキュリティの強度や利便性を考慮の上、利用者及び所属するグループの属性に基づくアクセス制御だけでなく、利用時間帯や利用端末ごとの制御等、アクセス制御機能に求める情報セキュリティ上の要件を定めること。 | | | |
| 36 | (3) 権限管理機能の導入 | 各接続機関は、関係システムの管理を実現するための権限に係る管理の機能を設け、適切に権限管理を行うこと。 | ○ | | |
| 37 | | 各接続機関は、関係システムに権限管理機能を導入するに当たり、管理者権限を悪意ある第三者等によって、不正に窃取された際の被害を最小化するための措置及び、内部からの不正操作や誤操作を防止するための措置を講ずること。 | | | |
| 38 | (4) 識別コード・主体認証情報の付与管理 | 各接続機関は、関係システムに係る全ての識別コードの適切な付与及び主体認証情報の適切な管理のための措置を講ずること。 | ○ | | |
| 39 | (5) ログの取得・管理 | 各接続機関は、関係システムが正しく利用されていることの検証及び不正侵入、不正操作等がなされていないことの検証を行うため、ログを取得すること。 | ○ | | |
| 40 | | 各接続機関は、関係システムにおいて、ログとして取得する情報項目、ログの保存期間、要保護情報の観点でのログ情報の取扱方法、及びログが取得できなくなった場合の対処方法等について定め、適切にログを管理すること。 | | | |
| 41 | | 各接続機関は、関係システムにおいて取得したログについて、必要に応じて、悪意ある第三者等からの不正侵入、不正操作等の有無について点検又は分析を実施すること。 | | | |
| 42 | (6) 暗号化機能・電子署名機能の導入 | 各接続機関は、関係システムで取り扱う情報の漏えいや改ざん等を防ぐため、暗号化を行う機能の必要性の有無を検討し、必要があると認めたときは、当該機能を設けること。 | | | |
| 43 | (7) 暗号化・電子署名に係る管理 | ◆ 各接続機関は、直接接続関係システムにおいて暗号及び電子署名を適切な状況で利用するため、暗号化のために選択されたアルゴリズムの危殆化に関する情報を定期的に入手すること。また、暗号化及び電子署名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。 | ○ | | |
| | 4.3 情報セキュリティの脅威への対策 | | | | |
| 44 | (1) ソフトウェアに関する脆弱性対策の実施 | 各接続機関は、関係システムを構成するサーバー装置、端末及び通信回線装置の設置又は運用開始時に、当該機器上で利用するソフトウェアに関連する公開された脆弱性についての対策を実施すること。 | | | |
| 45 | | 各接続機関は、関係システムを構成するサーバー装置、端末及び通信回線装置上で利用するソフトウェアに関連する脆弱性情報を入手した場合には、セキュリティパッチの適用又はソフトウェアのバージョンアップ等による情報システムへの影響を考慮した上で、ソフトウェアに関する脆弱性対策計画を策定し、措置を講ずること。 | | | |

| # | 項目 | 安全管理措置<br>（最終案） | 重点報告事項 | 自己点検 | |
|---|---|---|---|---|---|
| | | | | 自己点検結果 | 特記事項 |
| 46 | | 各接続機関は、関係システムを構成するサーバー装置、端末及び通信回線装置上で利用するソフトウェア及び独自に開発するソフトウェアにおける脆弱性対策の状況を定期的に確認し、脆弱性対策が講じられていない状態が確認された場合は対処すること。 | | | |
| 47 | (2) 不正プログラム対策の実施 | 各接続機関は、関係システムを構成するサーバー装置及び端末にシステム構成の状況に応じて、不正プログラム対策のための措置を講ずること。 | ○ | | |
| 48 | | 各接続機関は、関係システムへの想定される不正プログラムの感染経路の全てにおいて、不正プログラム対策ソフトウェア等により対策を講ずること。 | | | |
| 49 | | 各接続機関は、関係システムにおける不正プログラム対策の状況を適宜把握し、必要な対処を行うこと。 | | | |
| 50 | (3) サービス不能攻撃対策の実施 | 各接続機関は、関係システムについて、サービス提供に必要なサーバー装置、端末及び通信回線装置が装備している機能又は民間事業者等が提供する手段を用いてサービス不能攻撃への対策を行うこと。 | | | |
| 51 | | 各接続機関は、関係システムについて、サービス不能攻撃を受けた場合の影響を最小とする手段を備えた情報システムを構築すること。 | | | |
| 52 | | 各接続機関は、関係システムについて、サービス不能攻撃を受けるサーバー装置、端末、通信回線装置又は通信回線から監視対象を特定し、監視すること。 | | | |
| 53 | (4) 標的型攻撃対策の実施 | 各接続機関は、関係システムについて、標的型攻撃による組織内部への侵入を低減する対策（入口対策）を講ずること。 | | | |
| 54 | | 各接続機関は、関係システムにおいて、内部に侵入した攻撃を早期検知して対処する、侵入範囲の拡大の困難度を上げる、及び外部との不正通信を検知して対処する対策（内部対策）を講ずること。 | | | |
| | 5 情報システムの構成要素 | | | | |
| | 5.1 端末・サーバー装置等 | | | | |
| 55 | (1) 端末の導入時の対策 | 各接続機関は、関係システムの端末について、端末の盗難、不正な持ち出し、第三者による不正操作、表示用デバイスの盗み見等の物理的な脅威から保護するための対策を講ずること。 | | | |
| 56 | | 各接続機関は、関係システムの端末について、多様なソフトウェアを利用することにより脆弱性が存在する可能性が増大することを防止するため、業務に不要なソフトウェアの利用を禁止していること。 | | | |
| 57 | (2) 端末の運用時の対策 | 各接続機関は、関係システムの端末において利用を認めるソフトウェア及び利用を禁止するソフトウェアについて定期的に見直しを行うこと。 | | | |
| 58 | | 各接続機関は、関係システムの端末で利用されている全てのソフトウェアの状態を定期的に調査し、不適切な状態にある端末を検出等した場合には、改善を図ること。 | | | |
| 59 | (3) 端末の運用終了時の対策 | 各接続機関は、関係システムの端末の運用を終了する際に、端末の電磁的記録媒体の全ての情報を抹消すること。 | | | |

| # | 項目 | 安全管理措置<br>（最終案） | 重点報告事項 | 自己点検 | |
|---|---|---|---|---|---|
| | | | | 自己点検結果 | 特記事項 |
| 60 | (4) サーバー装置の導入時の対策 | 各接続機関は、関係システムのサーバー装置について、サーバー装置の盗難、不正な持ち出し、第三者による不正操作、表示用デバイスの盗み見等の物理的な脅威から保護するための対策を講ずること。 | | | |
| 61 | | 各接続機関は、障害や過度のアクセス等によりサービスが提供できない事態となることを防ぐため、関係システムについて、将来の見通しも考慮し、サービス提供に必要なサーバー装置を冗長構成にするなどにより可用性を確保すること。 | | | |
| 62 | | 各接続機関は、多様なソフトウェアを利用することにより脆弱性が存在する可能性が増大することを防止するため、関係システムにおいて業務に不要なソフトウェアの利用を禁止していること。 | | | |
| 63 | | 各接続機関は、通信回線を経由して関係システムのサーバー装置の保守作業を行う際に送受信される情報が漏えいすることを防止するための対策を講ずること。 | | | |
| 64 | | ◆ 各接続機関は、直接接続関係システムのサーバー装置について、電気的、機械的障害及び水、蒸気、温湿度変化、転倒等の設備・環境に起因する障害の発生を防止するための対策を講じること。 | ○ | | |
| 65 | (5) サーバー装置の運用時の対策 | 各接続機関は、関係システムにおいて利用を認めるソフトウェア及び利用を禁止するソフトウェアについて定期的に見直しを行うこと。 | | | |
| 66 | | 各接続機関は、関係システムのサーバー装置の構成やソフトウェアの状態を定期的に確認し、不適切な状態にあるサーバー装置を検出等した場合には改善を図ること。 | | | |
| 67 | | 各接続機関は、関係システムのサーバー装置上での不正な行為、無許可のアクセス等の意図しない事象の発生を監視する措置を講ずること。ただし、サーバー装置の利用環境等から不要と判断できる場合はこの限りではない。 | | | |
| 68 | | 各接続機関は、関係システムのサーバー装置について、情報のバックアップを取得するなど、サーバー装置を正常な運用状態に復元することが可能になるよう、必要な措置を講ずること。 | | | |
| 69 | (6) サーバー装置の運用終了時の対策 | 各接続機関は、関係システムのサーバー装置の運用を終了する際に、サーバー装置の電磁的記録媒体の全ての情報を抹消すること。 | | | |
| 70 | (7) 情報システムの適切な維持・管理 | ◆ 各接続機関は、直接接続関係システムに機器を接続するための手続、方法等を定め、構成機器の管理方法を定めること。 | ○ | | |
| 71 | | ◆ 各接続機関は、直接接続関係システムの構成機器等の台帳管理を実施し、現況と一致するよう適切に構成管理を実施すること。 | ○ | | |
| 72 | | ◆ 各接続機関は、直接接続関係システムのサーバー装置について、電気的、機械的障害を防止するため、適切に保守を実施すること。 | ○ | | |
| 73 | (8) 情報システムで用いる外部電磁記録媒体の対策 | 各接続機関は、関係システムにおいて用いるUSBメモリ等の外部電磁的記録媒体を用いた情報の取扱いに関して、マルウェア等が存在しないこと等を確認する運用としていること。 | ○ | | |
| | 5.2 通信回線 | | | | |
| 74 | (1) 通信回線の導入時の対策 | 各接続機関は、関係システムが接続される自機関外との通信回線構築時に、政府共通ネットワーク、総合行政ネットワークその他の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用いること。自機関内の通信回線を構築する際には、情報セキュリティインシデントによる影響を回避するために、通信回線に対して必要な対策を講ずること。 | ○ | | |

| # | 項目 | 安全管理措置<br>（最終案） | 重点報告事項 | 自己点検 | |
|---|---|---|---|---|---|
| | | | | 自己点検結果 | 特記事項 |
| 75 | | 各接続機関は、関係システムが接続される通信回線において、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。 | ○ | | |
| 76 | | 各接続機関は、関係システムが接続される通信回線において、サーバー装置及び端末のアクセス制御及び経路制御を行う機能を設け、適切にアクセス制御及び経路制御を行うこと。 | ○ | | |
| 77 | | 各接続機関は、関係システムを通信回線に接続する際に、通信内容の秘匿性の確保が必要と考える場合は、通信内容の秘匿性を確保するための措置を講ずること。 | ○ | | |
| 78 | | 各接続機関は、通信回線へ関係システムを接続する際に、当該情報システムが接続を許可されたものであることを確認するための措置を講ずること。 | ○ | | |
| 79 | | 各接続機関は、関係システムが接続される通信回線に係る通信回線装置について、物理的な保護措置を講ずるなどして、第三者による破壊や不正な操作等が行われないようにすること。 | | | |
| 80 | | 各接続機関は、関係システムが接続される通信回線について、当該通信回線の継続的な運用を可能とするための措置を講ずること。 | | | |
| 81 | | 各接続機関は、関係システムが接続される通信回線については、原則、インターネット回線の通信と分離すること。インターネット回線を接続する必要がある場合には、関係システムが接続される通信回線及び当該システムの情報セキュリティを確保するための措置を講ずること。 | ○ | | |
| 82 | | 各接続機関は、関係システムが接続される自機関内通信回線と自機関外通信回線との間で送受信される通信内容を監視するための措置を講ずること。 | ○ | | |
| 83 | | 各接続機関は、関係システムが接続される通信回線に係る通信回線装置が動作するために必要なソフトウェアを定め、ソフトウェアを変更する際の許可申請手順を整備すること。ただし、ソフトウェアを変更することが困難な通信回線装置の場合は、この限りでない。 | | | |
| 84 | | 各接続機関は、関係システムが接続される通信回線の保守又は診断のために、通信回線装置に対して行われるリモートアクセスに係る情報セキュリティを確保すること。 | | | |
| 85 | (2) 通信回線の運用時の対策 | 各接続機関は、関係システムが接続される通信回線について、経路制御及びアクセス制御を適切に運用し、通信回線や通信要件の変更の際及び定期的に、経路制御及びアクセス制御の設定の見直しを行うこと。 | ○ | | |
| 86 | | 各接続機関は、関係システムが接続される通信回線に係る通信回線装置が動作するために必要なソフトウェアの状態を定期的に調査し、許可されていないソフトウェアがインストールされているなど、不適切な状態にある通信回線装置を認識した場合には、改善を図ること。 | | | |
| 87 | | 各接続機関は、関係システムが他の情報システムと通信回線を共有している場合において、情報セキュリティの確保が困難な事由が発生した場合には、関係システムを保護するため、当該通信回線とは別に独立した閉鎖的な通信回線に構成を変更すること。 | | | |
| | 5.3 その他 | | | | |
| 88 | (1) 電子メールの導入時の対策 | 各接続機関は、接続運用に係る電子メールを送受信する場合には、それぞれの自機関が運営し、又は外部委託した電子メールサーバにより提供される電子メールサービスを利用すること。 | ○ | | |
| 89 | | 各接続機関は、電子メールサーバーが電子メールの不正な中継を行わないように設定すること。 | | | |
| 90 | | 各接続機関は、電子メールクライアントから電子メールサーバーへの電子メールの受信時及び送信時に主体認証を行う機能を備えること。 | | | |
| 91 | | 各接続機関は、電子メールのなりすましの防止策を講ずること。 | | | |

| # | 項目 | 安全管理措置<br>（最終案） | 重点報告事項 | 自己点検 | |
|---|---|---|---|---|---|
| | | | | 自己点検結果 | 特記事項 |
| 92 | (2) 時刻管理(NTP)の対策 | 各接続機関は、関係システムの構成要素（サーバー装置・端末等）のうち、時刻設定が可能なものについては、「接続運用規程 2.9.1 時刻同期」に準じ、当該構成要素の時刻を同期させ、ログに時刻情報も記録されるよう、設定すること。 | ○ | | |

（注1）中間サーバー等のほか、個別の事務に関する処理を行う既存システム、機関別符号の生成の際に連携する住民基本台帳ネットワークシステム、情報提供等の記録の開示機能等を有する情報提供等記録開示システム、情報連携に係る監視及び監督等を行う監視・監督システム等を指す。

（注2）「◆」の項番（#30、31、43、64、70、71、72）については、集約機関がある情報照会者等については、対象外となるもの。

【自己点検に係る記載要領】

1 「自己点検結果」欄は、各接続機関において該当するすべての関係システムについて、各接続機関で定める措置を実施済みであるもの、又は、今後生じうる事象について措置を検討し、発生時に速やかに対応可能であるものについては「○」を、機関で定める措置が未実施であり、今後措置を実施する予定であるものは「△」を、機関におけるシステムの状況から見て該当しないもの、又は、集約機関が接続機関として措置を行う事項であり、情報照会者等において実施しないものは「ー」を記入する。

2 「特記事項」欄は、「自己点検結果」欄において「△」を記入した場合、その措置の実施予定時期を、「ー」を記入した場合点検の対象外とした理由を記入する。