令和６年３月１日
法務省民事局

戸籍又は除かれた戸籍の副本等の電気通信回線を通じた送信の方法等に関する技術的基準

戸籍法施行規則（昭和２２年司法省令第９４号。以下「規則」という。）第７５条第５項の規定に基づく戸籍又は除かれた戸籍の副本の電気通信回線を通じた送信の方法、規則第７５条の３第４項の規定に基づく戸籍又は除かれた戸籍の副本に記録されている情報の電気通信回線を通じた提供の方法、規則第７６条第５項に基づく受付帳情報の電気通信回線を通じた送信の方法及び規則第７８条の２第６項に基づく届書等情報の電気通信回線を通じた送信の方法に関して法務大臣が定める技術的基準は以下のとおりである。

第１　目的

戸籍法（昭和２２年法律第２２４号）第１１８条第１項の電子情報処理組織において、電気通信回線その他の電気通信設備の利用における安全性及び信頼性を確保するため、戸籍又は除かれた戸籍の副本（規則第７５条第１項及び第２項（第４項において準用する場合を含む。）に規定する副本をいう。）の電気通信回線を通じた送信の方法（規則第７５条第５項）、外務大臣に対する戸籍又は除かれた戸籍の副本に記録されている情報の電気通信回線を通じた提供の方法（規則第７５条の３第４項）、受付帳情報の電気通信回線を通じた送信の方法（規則第７６条第５項）及び届書等情報の電気通信回線を通じた送信の方法（規則第７８条の２第６項）に関する技術的基準を定めることを目的とする。

第２　定義

１　戸籍情報連携システム

戸籍副本データ管理センター、市町村、管轄法務局等に設置される電子計算機、端末機、電気通信関係装置（ファイアウォールを含む。以下同じ。）、電気通信回線、プログラム等により構成されるシステムであって、戸籍又は除かれた戸籍の副本、受付帳情報及び届書等情報を送受信し、当該副本等の保存及び管理を行う機能を有し、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）に基づく行政機関等との情報連携や市町村の戸籍情報システム（戸籍法第１１８条第１

項に規定する市町村長の使用に係る電子計算機。本基準において、外務大臣の使用に係る戸籍情報連携システムから情報の提供を受けるためのシステムを含む。以下同じ。）との情報連携を行うもの

2　戸籍情報連携システムサーバー群

戸籍副本データ管理センターに設置され、戸籍又は除かれた戸籍の副本、受付帳情報及び届書等情報の送信を受け、市町村の戸籍情報システムとの情報連携及び当該副本を保存するために動作する一連の電子計算機群で、戸籍情報連携システム内の役割に応じてセグメントごとに複数台で構成されるもの

3　戸籍事務内連携サーバー

市町村及び外務省に設置する電子計算機又は端末機であって、戸籍情報システムと戸籍情報連携システムとの間で連携される情報の送信を行うもの

4　管轄法務局等

戸籍又は除かれた戸籍の副本を送信する市町村を管轄する法務局若しくは地方法務局又はその支局

5　管轄法務局等端末

管轄法務局等に設置され、市町村から送信された戸籍又は除かれた戸籍の副本の管理を行う管轄法務局等の使用に係る端末機

6　ファイアウォール

ネットワークにおいて不正侵入を防御する電子計算機又は同等の機能及び効果を有するソフトウェア

7　データ

戸籍情報連携システムにおいて送信され、記録され又は保存される情報

8　プログラム

電子計算機を機能させて戸籍情報連携システムを作動させるための命令を組み合わせたもの

9　ファイル

磁気ディスク（これに準ずる方法により一定の事項を確実に記録しておくことができる物を含む。以下同じ。）に記録されているデータ及びプログラム

10　ドキュメント

戸籍情報連携システムの設計、プログラム作成及び運用に関する記録及び文書

11　重要機能室

電子計算機、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

びにその室の空気調和をする空気調和機及びその付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

ア　戸籍情報連携システムのセキュリティ（正確性、機密性及び継続性を維持することをいう。以下同じ。）を確保するため、戸籍情報連携システムの企画、開発及び運用に関する責任体制並びに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の確立を図ること。

イ　市町村長及び外務大臣（以下「市町村長等」という。）は、戸籍情報システムのセキュリティを確保するため、戸籍情報システムのうち、戸籍情報連携システムに情報を送信し又は戸籍情報連携システムから情報を受信する機能に係る部分の企画、開発及び運用に関する責任体制を明確にすること。また、戸籍事務内連携サーバーの防災及び防犯に関して、通常時及び非常時の責任体制の確立を図ること。

(2) セキュリティ対策に関する連絡調整

戸籍情報連携システムのセキュリティ対策に関し、市町村長等と連絡調整を行う場の設置その他の適切な措置を講ずること。

(3) 緊急時連絡体制の整備

戸籍情報連携システムの運用に際し、異常な状態を早期に発見し、市町村長等に連絡することができるよう体制の整備を図ること。

２　規程の定め等

戸籍情報連携システムの運用に関する規程を定めるとともに、戸籍情報連携システムの設計書、操作手順書、緊急時における作業手順書等を作成すること。

３　人事、教育、研修等

(1) 要員管理

法務大臣及び市町村長等は、戸籍情報連携システムの運用に必要な職員の配置、交替等の人事管理を適切に行うこと。

(2) 教育及び研修

ア　戸籍情報連携システムを運用する職員に対して、戸籍情報連携システムの操作及びセキュリティ対策についての教育及び研修を実施するために、教育及び研修に関する計画を策定し、その実施体制を確立すること。

イ　市町村長等に対し、教育及び研修に関する技術的な協力を行うこと。

(3) 問合せ窓口の設置

戸籍情報連携システムの適切な運用を確保するため、操作等に関する問合せ窓口を設置すること。

4　戸籍情報連携システムの監査

(1) 監査の実施

法務大臣は、戸籍情報連携システムの企画、開発及び運用の各段階におけるセキュリティ対策について監査を実施し、その結果に基づき、戸籍情報連携システムの改善に努めること。

市町村長等は、戸籍情報システムのうち、戸籍情報連携システムに情報を送信し、又は戸籍情報連携システムから情報を受信する機能に係る部分の企画、開発及び運用の各段階におけるセキュリティ対策について監査を実施し、その結果に基づき、戸籍情報システムの改善に努めること。

(2) 監査の体制の確立

市町村長等は、法務大臣の実施する監査に必要な協力を行い、その結果に基づき戸籍情報連携システムの運用の改善に協力すること。

5　緊急時体制

(1) 作動停止時における事務処理体制

ア　戸籍情報連携システムの構成機器、関連設備又はソフトウェアの障害等により戸籍情報連携システムの全部又は一部が作動停止した場合の行動計画、市町村長等との連絡方法等について、市町村長及び外務大臣と相互に密接な連携を図り、これらの事項を定めること。

イ　アにおいて定めた行動計画、連絡方法等に基づき、適切な対応を図ることができるよう、市町村長等と相互に密接な連携を図り、教育及び研修を行うこと。

(2) データの漏えいのおそれがある場合の事務処理体制

ア　データの漏えいのおそれがある場合の行動計画（戸籍情報連携システムの全部又は一部を停止する基準の策定を含む。）、市町村長との連絡方法等について、市町村長等と相互に密接な連携を図り、これらの事項を定めること。

イ　アにおいて定めた行動計画、連絡方法等に基づき、適切な対応を図ることができるよう、市町村長等と相互に密接な連携を図り、教育及び研修を行うこと。

第４　戸籍情報連携システムの環境及び設備

1　建物及び重要機能室

(1) 建物及び重要機能室の保全等

ア　戸籍情報連携システムサーバー群を管理する建物及び重要機能室（以下「建物等」という。）は、国内に設置すること。

イ　重要機能室の壁、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。

ウ　重要機能室への侵入を検知するための措置を講ずること。

エ　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。

オ　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を容易に行うことができるよう配慮すること。

イ　重要機能室は、その場所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　重要機能室は、緊急事態発生の際の連絡設備を設けるなど、連絡体制を整備すること。

エ　重要機能室は、他の部屋と区別して専用の部屋とすること。

オ　重要機能室において常時利用する出入口は、不特定多数の人が利用する場所を避け、限定すること等により、侵入の防止を容易に行うことができるよう配慮すること。

カ　電子計算機及び電気通信関係装置は厳重に固定し、磁気ディスク及びドキュメントは専用保管庫により施錠保管すること。

2　障害の防止等

(1) 電気的・機械的障害の防止等

戸籍情報連携システムの構成機器又は関連設備の電気的・機械的障害の発生を防止し、これら障害の発生の検知及びこれらの障害が発生した場合の対策を図るため、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

戸籍情報連携システムの構成機器の水又は蒸気による障害の発生を防止し、これら障害の発生の検知及びこれらの障害が発生した場合の対策を図るため、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、火災による戸籍情報連携システムの構成機器又は関連設備の損傷を防止し、火災の発生の検知及び火災が発生した場合の対策を図るため、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) 地震対策

地震による建物等又は戸籍情報連携システムの構成機器若しくは関連設備の損傷の防止及び地震が発生した場合の対策を図るため、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

空気調和設備は、その容量に配慮し、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

戸籍情報連携システムの構成機器及び関連設備には、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

動物その他による障害を防止し、これらの障害の発生を検知し、及び障害が発生した場合の対策を図るため、必要な措置を講ずること。

3　ネットワーク設備

(1) 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、戸籍情報連携システムサーバー群、戸籍事務内連携サーバー及び管轄法務局等端末を結ぶ電気通信回線は、地方公共団体及び国相互間の通信用に設けた行政事務専用の回線を使用すること。

(2) 必要な伝送速度の確保

戸籍情報連携システムサーバー群、戸籍事務内連携サーバー及び管轄法務局等端末を結ぶ電気通信回線は、データを円滑に送信し、又は伝送するために必要な伝送速度を確保すること。

第5　戸籍情報連携システムの管理

1　入退室管理

(1) 入室資格の付与

重要機能室に入室する権限を有する者を限定すること。また、重要機能室に入退室する者に鍵を貸与する際には、その者が入室する権限を有することを確認すること、生体情報等による主体認証によって重要機能室に入退室する者が入室する権限を有することを確認することなどにより、入退室の管理を適切に行うこと。

(2) 鍵等の管理

ア　重要機能室の出入口の鍵は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。

イ　生体情報等の管理方法を定めること。

(3) 搬出入物品の確認

重要機能室への搬出入物品は、重要機能室に入室する権限を有する者が内容を確認すること。

(4) 事務室の管理

重要機能室の出入口の鍵等を管理する事務室における盗難、損壊等を防止するため、職員が不在となる時の事務室の施錠等、必要な措置を講ずること。

2　ソフトウェア開発等の管理

(1) 設計の実施

ア　戸籍情報連携システムの開発又は変更を行う際には、戸籍情報連携システムのセキュリティを高める設計を行うこと。

イ　戸籍情報連携システムの開発又は変更を行う際には、必要機能を明確にし、将来の規模の拡大等を考慮した設計を行うこと。

(2) 戸籍情報連携システムの試験の実施

戸籍情報連携システムの開発又は変更を行った場合には、その試験を適切に実施すること。また、試験の実施に当たっては、ファイルの安全を確保するため、別途試験環境を用意することその他の適切な措置を講ずること。

(3) 戸籍情報連携システムの開発等に際してのエラー及び不正行為の防止

ア　戸籍情報連携システムの開発又は変更を行う際には、戸籍情報連携システムの開発又は変更の計画を策定すること、戸籍情報連携システムの開発又は変更の責任者を指定すること、プログラムの作成、変更又は廃止を責任者の承認を得て行うことなどエラー及び不正行為の防止のための手続を明確にすること。

イ　戸籍情報連携システムの開発又は変更の各段階で使用するドキュメントの様式を標準化すること。

ウ　戸籍情報連携システムの変更に応じてドキュメントを更新し、責任者が確認すること。

3　戸籍情報連携システムの管理

(1) アクセス権限の限定

戸籍情報連携システムの運用に関係する者に対して、電子計算機、端末機、電気通信関係装置、電気通信回線、ファイル等に関し、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における不正行為又は電子計算機への不正アクセス行為に対して戸籍情報連携システムを保護するため、

戸籍情報連携システム及び戸籍事務内連携サーバー間等の必要な部分にはファイアウォールを設置し、通信制御を行うこと。

(3) 電気通信関係装置の管理

エラー及び不正行為により電気通信関係装置の不当な運用が行われないようにするため、電気通信関係装置の管理に当たっては厳重な確認を行うなど、管理権限がある者以外の者による操作を防止するための措置を講ずること。

(4) 通信相手相互の認証

戸籍情報連携システムと戸籍事務内連携サーバーとの間の通信については、通信相手相互の認証を行うこと。

(5) データの暗号化

戸籍情報連携システムサーバー群、戸籍事務内連携サーバー及び管轄法務局等端末それぞれの間の通信については、交換するデータの暗号化を実施すること。

(6) 模擬攻撃の実施

ネットワーク経由の模擬攻撃を適宜実施し、その実施結果に基づき必要な措置を講ずること。

(7) 情報収集等

セキュリティ対策に関する情報を収集して分析を行い、必要な措置を講ずること。

(8) 時刻の正確性確保

不正行為の追跡、セキュリティを侵害された場合における証跡の解析等を容易にするため、重要機能室内の機器を正確な時刻に同期するための必要な措置を講ずること。

4　端末機操作の管理

(1) 端末機の管理

端末機の取扱いは、当該端末機の管理を行う責任者の指示又は承認を受けた者が行うこと。

(2) 端末機の操作者の確認

端末機の取扱いに際しては、暗証番号又はこれと同等以上のものと認められる方法により、操作者が正当なアクセス権限を有していることを確認すること。

(3) 暗証番号等の取扱い

暗証番号等の管理方法を定め、操作者は当該管理方法を遵守すること。

(4) ファイルに対する利用制限

端末機の操作者ごとに利用可能なファイルを設定する等、ファイルの

利用を制限する方法を定めること。

(5) 操作履歴の記録等

ア　戸籍情報連携システムを操作した履歴を磁気ディスクに記録し、法令を遵守していることを監査する等、その利用の正当性について確認すること。

イ　戸籍情報連携システムを操作した履歴は、不当な消去や改ざんを防止するため、管理権限がある者以外の者による操作を防止するための措置を講ずること。

(6) 複数回のアクセス失敗に対する機能

端末機には、複数回のアクセスの失敗に対し、当該端末機へのアクセス権限を一定の間取り消す機能等を設けること。

5　電子計算機の管理

(1) 秘密鍵の厳重な管理

戸籍情報連携システム及び戸籍事務内連携サーバーにおいて、通信相手相互の認証及び市町村から送信する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、安全な方法により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。

(2) 他のソフトウェアの作動禁止

戸籍情報連携システム及び戸籍事務内連携サーバーでは、戸籍情報連携システムの管理及び運用に必要なソフトウェア以外のソフトウェアを作動させないこと。

6　磁気ディスクの管理

(1) 保管場所

磁気ディスクは、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) 持ち出し及び返却の確認等

ア　磁気ディスクの盗難の防止等のため、その保管位置を指定し、持ち出し及び返却の措置を講ずること。

イ　重要な磁気ディスクは他の磁気ディスクと判別することができるようにすること。

7　構成機器及び関連設備等の管理

(1) 管理方法の明確化

ア　戸籍情報連携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、関連設備等の管理方法を明確にすること。

イ　利用するハードウェア、ソフトウェア及び磁気ディスクの種類、数量等を文書等で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、これを関係職員に周知し、管理しているハードウェア、ソフトウェア又は磁気ディスク以外の物を使用しないこと。

(2) 保守の実施

戸籍情報連携システムの構成機器及び関連設備の保守を定期に、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) 稼動状況の監視

構成機器の稼動状況を監視し、必要に応じ、市町村長に状況を通知すること。

(4) 不正プログラムの混入防止等

戸籍情報連携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、戸籍情報連携システムの運用に関係する者に周知すること。

8　データ、プログラム、ドキュメント等の管理

(1) データ等の取扱い及び管理

ア　データ、プログラム及びドキュメントについては、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、これらの取扱い及び管理の方法を明確にすること。

イ　データ、プログラム及びドキュメントの内容については、最新の状態にしておくこと。

ウ　データ、プログラム及びドキュメントを変更した場合については、変更者及び版数の管理を行うこと。

エ　戸籍情報システムと戸籍情報連携システム間のデータの送受信については、データの特性に応じ、即時処理通信（情報送信元から情報を送信し、直ちに情報受信先に受信される通信をいう。以下同じ。）又は大量データ等の一括処理通信から適切な送信方法を選択し、その管理を行うこと。

オ　プログラムの改ざん、消去等を防止するために、プログラムの登録及び抹消は、責任者の指示又は承認を受けた者が行うこと。

カ　データ、プログラム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。

キ　戸籍情報連携システムサーバー群、戸籍事務内連携サーバー及び管

轄法務局等端末に保管される重要なデータについては、暗号化を実施すること。

ク　市町村長は、法務大臣からデータ、プログラム及びドキュメントの返却又は廃棄を求められたときは、これに応じること。

(2) 戸籍情報システムと戸籍情報連携システム間のデータ送信方法の管理

ア　大量データ等の一括処理通信について、処理途中におけるデータの更新を防止する制御や、更新対象の情報について、更新が完了するまでの間は閲覧できないようにする制御を行うこと。

イ　大量データ等の一括処理通信について、送信処理が途中で中断しても再送信が可能な仕組みを実施すること。

ウ　大量データ等の一括処理通信について、戸籍情報システムと戸籍情報連携システム間の双方において、適切にデータの受渡しが可能となるように送受信手順を確立すること。

(3) 帳票の管理

ア　重要な印字済みの帳票の受渡し及び廃棄の方法を定めること。

イ　事務室の出力装置から出力する場合のデータの漏えいを防止するため、必要な措置を講ずること。

9　障害時等の対応

(1) 障害の早期発見

戸籍情報連携システムの障害箇所を発見するための機能を整備すること。

(2) 早期回復のための代替機能等の整備

ア　重要なファイルについては、他の磁気ディスクに複製することとし、必要に応じ、複製された磁気ディスクと当該ファイルを記録した磁気ディスクとは別に保管すること。

イ　障害が発生した時に、複製された重要なファイル等を基に速やかに戸籍情報連携システムを回復させるための機能を整備すること。

(3) 不正アクセスの早期発見

不正アクセスを早期に発見するための機能を整備すること。

(4) 不正アクセスが判明した場合の対応

不正アクセスが判明した場合、市町村長等と連絡調整を行い、被害状況の把握、被害拡大を防止するための措置等必要な措置を講ずること。

10　委託等を行う場合の措置

(1) 委託先事業者等の社会的信用の確認等

戸籍情報連携システムの開発、変更、運用、保守等について委託等を行うときは、委託先事業者等の社会的信用及び能力を確認すること。また、

市町村長は、戸籍情報連携システムの運用について委託等を行うときは、委託先事業者等の社会的信用及び能力を確認するとともに、管轄法務局等の長に報告を行うこと。

(2) 委託先事業者等に対する監督

ア　委託先事業者等に対し、この基準と同様の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エラー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。

イ　委託先事業者等がこの基準に適合したセキュリティ対策を実施していないと認められる場合には、当該委託先事業者等に係る契約を解除すること。また、管轄法務局等の長は、市町村の委託先事業者等が、この基準に適合したセキュリティ対策を実施していないと認められた場合には、当該市町村長に対し、当該委託先事業者等に係る契約を解除することを助言又は勧告すること。

(3) 再委託等の制限

委託先事業者等が委託業務の一部を第三者に委託する場合等の制限、事前申請及び承認に関する事項について、委託先事業者等との間で定めを置くこと。また、管轄法務局等の長は、必要に応じ、市町村の委託先事業者等が委託業務の一部を第三者に委託する場合等の制限、事前申請及び承認に関する事項について、市町村長が委託先事業者等との間で定めを置くに当たり、助言又は勧告すること。

(4) 委託先事業者等の分担範囲等の明確化

戸籍情報連携システムの開発、変更、運用、保守等に複数の委託先事業者等が関係する場合は、分担して行う範囲及び責任の範囲を明確にするとともに、作業上必要な情報交換を行うことができるような措置を講ずること。

第６　既設ネットワークとの接続

１　既設ネットワークとの接続条件

市町村長は、戸籍情報連携システムと戸籍情報システムとの間の通信を確保するため、既設ネットワークと戸籍事務内連携サーバーとを接続する場合は、既設ネットワークにおいて、次のようなセキュリティ対策を講ずること。

(1) 体制の整備等

ア　既設ネットワークのセキュリティを確保するため、既設ネットワークの開発及び運用に関する責任体制及び連絡調整体制を明確にするこ

と。

イ　既設ネットワークにおいて、個人情報の漏えいのおそれがある場合の事務処理体制を確立すること。

(2) 電気通信回線上の盗聴等の防止

電気通信回線は専用回線を用い、又はそれに準じた通信データの盗聴、改ざん、滅失・き損及び操作否認の防止についての必要な対策を講ずること。この場合において、電気通信回線はデータを円滑に送信し、又は伝送するために必要な伝送速度を確保すること。

(3) ファイアウォールによる通信制御

既設ネットワークと戸籍事務内連携サーバーとの間にファイアウォール、不正侵入検知（ＩＤＳ）、不正侵入防御（ＩＰＳ）等を利用した確実な不正侵入対策を講じ、戸籍情報連携システム上の処理又は既設ネットワーク上の処理に係る通信のみが可能となるよう通信制御を行うこと。

(4) 電気通信関係装置の保護等

既設ネットワークに係る電気通信関係装置等は、既設ネットワークの管理責任者以外の者による操作を防止するための措置を講ずること。

(5) 機器の接続

既設ネットワークの管理責任者は、ネットワークに機器を接続するための手続、方法等を定め、接続状況を適切に管理すること。

(6) 外部との接続

ア　既設ネットワークの管理責任者は、既設ネットワークを外部ネットワークに接続するための手続、方法等を定め、接続及び運用に関する業務を総括的に管理すること。

イ　既設ネットワークと外部のネットワークを接続する場合は、既設ネットワークと外部のネットワークとの間にファイアウォール、不正侵入検知（ＩＤＳ）、不正侵入防御（ＩＰＳ）等を利用した確実な不正侵入対策を講じ、厳重な通信制御を行うこと。

２　既設ネットワークとの接続状況についての連絡調整

管轄法務局等の長は、既設ネットワークとの接続状況について市町村長と連絡調整を行うこと。また、市町村長は、既設ネットワークにおいて個人情報の漏えいのおそれがある場合は、管轄法務局等の長と連絡調整を行うこと。