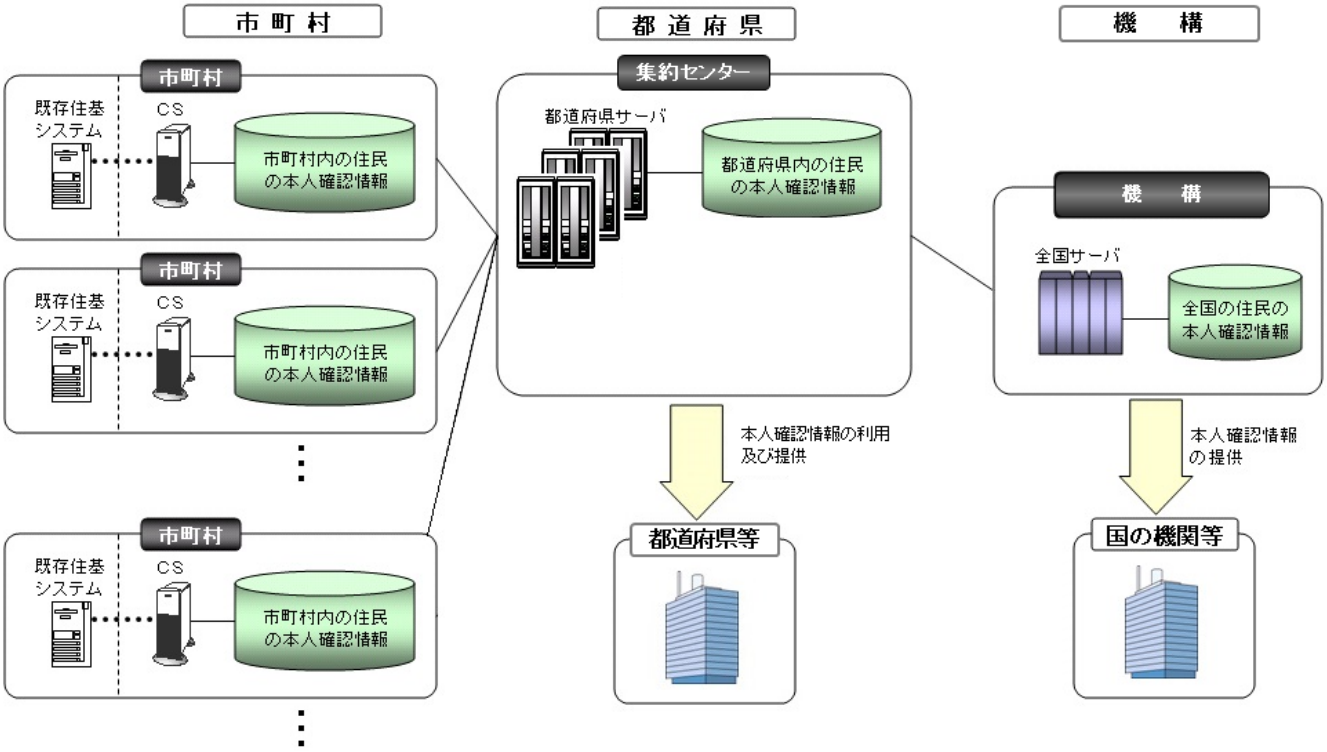
住民基本台帳ネットワークシステムの概要

1　概要

住民基本台帳ネットワークシステム（以下「住基ネット」という。）は、全国の地方公共団体を専用回線で結び、市町村ごとに運用されていた住民基本台帳（住民票を各市町村でまとめたもの。）に関するシステムをネットワーク化することにより、全国共通の本人確認を可能とするシステムで、平成 14 年８月から運用が開始されています。



市町村において住民の異動が発生すると、既存住基システムから CS へ異動情報が通知され、CS の情報が更新されます。同様に、異動情報が CS から都道府県サーバへ、都道府県サーバから全国サーバへ通知されることで、都道府県サーバと全国サーバの情報が更新されます。

2　用語の説明

機構	地方公共団体情報システム機構のことで、住民基本台帳法に基づき住基ネットの開発や運用管理等を行う機関。
既存住基システム	住基ネットの構築以前から各市町村で運用されていた住民基本台帳に関するシステム。
CS（コミュニケーションサーバ）	各市町村が管理するサーバ。市町村ごとに異なる既存住基システムの情報を統一化し、住基ネットに接続するためのもの。
都道府県サーバ	各都道府県が管理するサーバ。都道府県等が住基ネットの情報を利用等するためのもので、現在は機構に対し集約センターでの一括管理を委託。
全国サーバ	機構が管理するサーバ。国の機関等に住基ネットの情報を提供等するためのもの。

3　導入の主なメリット

・これまで住民が申請等する際に必要だった住民票の写しの提出を省略することが可能となりました。
・市町村間で住基ネットを通じて住民の異動情報をやりとりすることが可能となりました。
・国の機関及び都道府県等において、住民の現況を確実かつ迅速に把握することが可能となりました。

（別添1）事務の内容

次ページ図を参照

（備考）

1. 本人確認情報の更新に関する事務
1-①.市町村において受け付けた住民の異動に関する情報を、市町村CSを通じて都道府県サーバに通知する。
1-②.都道府県サーバにおいて、市町村より受領した本人確認情報を元に都道府県知事保存本人確認情報ファイルを更新する。
1-③.機構に対し、住民基本台帳ネットワークを介して、本人確認情報の更新を通知する。

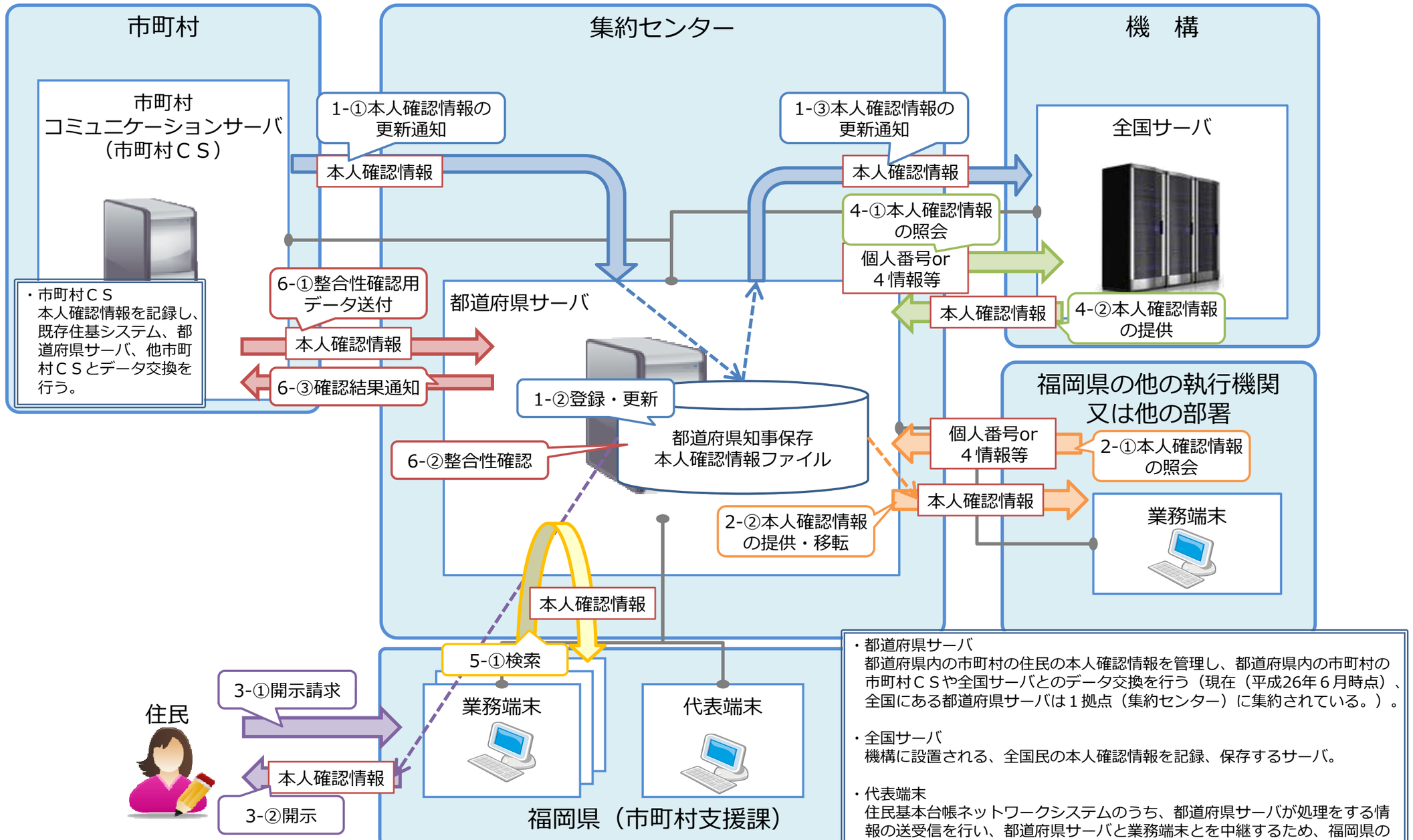
2. 福岡県の他の執行機関への情報提供又は他の部署への移転
2-①.福岡県の他の執行機関又は他の部署において、個人番号又は4情報等をキーワードとした本人確認情報の照会を行う。
2-②.福岡県知事において、提示されたキーワードを元に都道府県知事保存本人確認情報ファイルを検索し、
照会元に対し、当該個人の本人確認情報を提供・移転する。
※検索対象者が他都道府県の場合は全国サーバに対して検索の要求を行う。
※福岡県の他の執行機関又は他の部署に対し、住民基本台帳ネットワークシステムに係る本人確認情報を一括して提供する場合（注1）には、福岡県知事又は照会元において、都道府県サーバの代表端末又は業務端末を操作し、媒体連携（注2）により行う。
（注1）福岡県の他の執行機関又は他の部署においてファイル化された本人確認情報照会対象者の情報（検索条件のリスト）を元に都道府県サーバに照会し、照会結果ファイルを提供する方式を指す。
（注2）媒体連携とは、一括提供の方式により本人確認情報の提供を行う場合に、情報連携に電子記録媒体を用いる方法を指す。

3. 本人確認情報の開示に関する事務
3-①.住民より本人確認情報の開示請求を受け付ける。
3-②.開示請求者（住民）に対し、都道府県知事保存本人確認情報ファイルに記録された当該個人の本人確認情報を開示する。

4. 機構への情報照会に係る事務
4-①.機構に対し、個人番号又は4情報等をキーワードとした本人確認情報の照会を行う。
4-②.機構より、当該個人の本人確認情報を受領する。

5. 本人確認情報検索に関する事務
5-①.4情報の組み合わせを検索キーに、都道府県知事保存本人確認情報ファイルを検索する。

6. 本人確認情報整合
6-①.市町村CSより、都道府県サーバに対し、整合性確認用の本人確認情報を送付する。
6-②.都道府県サーバにおいて、市町村CSより受領した整合性確認用の本人確認情報を用いて都道府県知事保存本人確認情報ファイルの整合性確認を行う。
6-③.都道府県サーバより、市町村CSに対して整合性確認結果を通知する。



・都道府県サーバ
都道府県内の市町村の住民の本人確認情報を管理し、都道府県内の市町村の市町村ＣＳや全国サーバとのデータ交換を行う（現在（平成26年６月時点）、全国にある都道府県サーバは１拠点（集約センター）に集約されている。）。

・全国サーバ
機構に設置される、全国民の本人確認情報を記録、保存するサーバ。

・代表端末
住民基本台帳ネットワークシステムのうち、都道府県サーバが処理をする情報の送受信を行い、都道府県サーバと業務端末とを中継するため、福岡県の本庁舎に設置する電子計算機。

・業務端末
住民基本台帳ネットワークシステムのうち、都道府県サーバ及び代表端末にネットワークで接続し業務を行う電子計算機及びこれに接続するプリンタ及び業務に必要な認証を受けるため、生体情報に不可逆演算処理を施した情報を読み取る機能を有する装置。

住民基本台帳ネットワークシステムに係る本人確認情報の管理及び提供等に関する事務におけるリスク対策の骨子

Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策

プロセス	リスク	主な対策　（詳細は全項目評価書を参照）
2．県が本人確認情報の更新のために市町村ＣＳを通じて特定個人情報を県サーバに入手する （P.12）	リスク1：県が必要な特定個人情報以外の情報の入手を行ってしまうリスク	○誤って更新対象者以外の住民の情報を県が入手することの防止 ・本人確認情報を更新する際の特定個人情報の入手経路は、マスター（既存住基システム）に直結した市町村CSからに限られている。 ・更新する対象者が真正なる本人であり、かつ、変更内容が正確であるかどうかは市町村が変更事項の受付時に厳格に審査している。 ○更新対象者について、必要な情報以外を県が入手することの防止 ・県が市町村から入手することのできる情報項目は、法令で限定されておりそれ以外の情報項目は入手しない。
	リスク2：県が特定個人情報を入手する際に他者に情報を詐取・奪取されるリスク	・県のサーバと市町村 CS 間は全て専用回線でつながれている。
	リスク3：県が入手した特定個人情報が不正確であるリスク	○市町村が特定個人情報を入手する際の本人確認 ・住民の異動情報の届出等を受け付ける市町村の窓口において、対面で身分証明書（個人番号カード等）の提示を受け、本人確認を行う。 ○個人番号の正確性確保 ・個人番号の正確性は、市町村が厳格に管理、審査しているマスター（既存住基システム）に直結する市町村 CS から入手することとなっている。 ○特定個人情報の更新情報の正確性確保 ・県のサーバが本人確認情報の更新情報を受け取る際論理チェックを行う（例えば、現存する住民に対して転入を異動事由とする更新が行われようとした場合や、転居を異動事由とする更新の際に住所以外の更新が行われようとした場合に当該処理をエラーとする。）。 ・入手元である市町村CSにおいて、項目（フォーマット、コード）のチェックを実施する。
	リスク4：特定個人情報を入手する際に県が特定個人情報を漏えい・紛失するリスク	○機構が作成・配付する専用のアプリケーションを（＊）用いることにより、入手の際の特定個人情報の漏えい・紛失の防止に努める。 ○県のサーバと市町村 CS とを接続するネットワーク回線に専用回線を用い、送信情報の暗号化を実施するなどの措置を講じる。 ○市町村 CS から県サーバへの特定個人情報の更新は、操作者の人為的なアクセスが介在せず、全て自動処理で行う。 ＊都道府県サーバのサーバ上で稼動するアプリケーション。 都道府県内の市町村の住民の本人確認情報を管理し、都道府県内の市町村 CS や全国サーバとのデータ交換を行う。 データの安全保護対策、不正アクセスの防止策には、最新の認証技術や暗号化技術を採用し、データの盗聴、改ざん、破壊及び盗難、端末の不正利用及びなりすまし等を防止する。
3．県が特定個人情報を使用する （P13～P.14）	リスク1：県サーバが保有する特定個人情報を、職員が使用目的を超えて紐付け又は担当事務に必要のない情報まで紐付けを行うリスク	○宛名システムや他の県の事務処理の庁内システムと県サーバは、直接接続はしない（県サーバからの情報の提供は全て媒体を通じて行い、取得情報は他の目的には使用できないよう厳格に媒体の管理を行う）。
	リスク2：権限のない者（元職員、アクセス権限のない職員等）が不正に特定個人情報を使用するリスク	○ユーザ認証の管理 ・生体認証による操作者認証を行う。 ○アクセス権限の発行、失効の管理（本庁） ・申請内容確認後、市町村支援課がシステムへの登録、削除を行い管理簿へ登載する。 ○アクセス権限の発行、失効の管理（出先） ・出先業務端末設置所属毎に管理者を置き、管理者が登録・削除を行い管理簿へ登載。登載内容に誤りがないか市町村支援課で確認。 ○アクセス権限の管理 ・操作者の業務に応じた必要最小限のアクセス権限を付与し、アクセス権限がある職員を管理簿で管理する。 ○特定個人情報の使用の記録 ・操作履歴を記録し、定期的に抽出して不正操作がないことをシステム管理を受託した業者が確認。 ・操作履歴の確認により本人確認情報の検索に関して不正な利用の疑いがある場合は、利用管理簿等との整合性の確認や利用所属への聞き取りを行う。
	リスク3：職員が特定個人情報を住基法、住基条例で利用が認められている事務以外に使用するリスク	○システムの操作履歴を記録し、不適切な利用を行っていないかシステム管理を受託した業者が随時確認する。 ○毎年度一部の操作履歴を抽出し、当該利用が目的外利用でないか、使用した職員以外の職員に任じて点検させる。
	リスク4：県サーバが保有する特定個人情報のファイルを職員が不正に複製するリスク	・管理権限を持つ市町村支援課の特定職員以外は、システム制約により情報の複製はできない。

4．県が必要に応じて特定個人情報ファイルの取扱いの委託を行う （P.14～P.15） 【委託先①】 ・地方公共団体情報システム機構（J-LIS） →都道府県サーバの運用及び監視の委託 【委託先②】 ・日本電気株式会社九州支社（NEC） →代表端末及び業務端末等の機器の運用支援、システム障害時の復旧作業等の委託	・委託先が特定個人情報を不正に入手することや不正な使用を行うリスク ・委託先が特定個人情報を不正に他者に提供するリスク ・委託先が特定個人情報の保管・消去を行う際に特定個人情報の漏えいが発生するリスク ・委託先が委託契約終了後に特定個人情報を不正に使用するリスク ・委託先が再委託を行う場合に再委託先で上記と同様の事態を生じるリスク	○情報保護管理体制の確認 ・県ネットワークの運用管理や県サーバの運用監視の委託業者の選定については、必要な社会的信用と能力を設定し、選定経過の記録を残す。 ○特定個人情報ファイルの閲覧者等の制限 ・委託業者に名簿を提出させ作業者を限定するとともに、アクセス権限を業務に必要な最小限のものとしている。 ・操作履歴により、不正な使用がないことを確認する。 ○特定個人情報ファイルの取扱いの記録 ・アクセスログや媒体授受の取扱記録を上書きせずに残している。 ○特定個人情報の提供のルール ・委託先から他者への特定個人情報の提供を一切認めない契約としている。 ・システム管理業者は検索ログを確認できる権限を持つため、そのログの個人情報について、市町村支援課が随時調査する。 ○特定個人情報の消去のルール ・県管理基準で、個人情報が記載された媒体を破棄する際、書類はシュレッダ、電子記録媒体は職員立会いの下内容を読み取れないようにすることが規定されており、システム管理の委託業者に徹底する。 ○委託契約書中の特定個人情報ファイルの取扱いに関する規定 ・目的外利用の禁止、個人情報の閲覧者の制限、個人情報の利用・提供の制限、個人情報の複写又は複製の禁止、再委託における条件、個人情報の保護に関する研修の実施及び当県職員による個人情報の状況の随時調査の実施を契約書に明記している。 ○再委託先による特定個人情報ファイルの適切な取扱いの確保 ・直接本人確認情報にアクセスする業務は再委託を禁止する。再委託先には、その他すべての項目につき委託先と同様の安全管理措置を義務付け、委託先は再委託先の安全管理措置に対する管理監督を義務付ける。
5－1．県が特定個人情報を全国サーバへ提供する （P.15～P.16）	リスク1：（故意又は過失により）県が特定個人情報の不正な提供・移転を行うリスク	・提供の記録（提供、移転の日時、操作者等）をシステムで上書きすることなく管理、保持している。
	リスク2：県が情報の安全が保たれない不適切な方法で特定個人情報の提供・移転を行うリスク	・全国サーバへ特定個人情報の提供は相互認証を実施している。
	リスク3：正当な全国サーバ以外の誤った相手方に特定個人情報を提供・移転してしまうリスク	
5－2．県担当部署（市町村支援課）が他の執行機関や他部署への提供・移転を行う （P.15～P.16）	リスク1：（故意又は過失により）県担当部署（市町村支援課）職員が特定個人情報の不正な提供・移転を行うリスク	・提供・移転（行えなかった場合も含む。）の記録（提供、移転の日時、操作者等）をシステムで上書きすることなく管理、保持している。
	リスク2：県担当部署（市町村支援課）職員が情報の安全が保たれない不適切な方法で特定個人情報の提供・移転を行うリスク	・福岡県の他の執行機関及び部署への提供・移転の際に、媒体への出力が必要な場合は、逐一出力の記録を残す。
	リスク3：県担当部署（市町村支援課）職員が誤った特定個人情報又は正当な他の執行機関や他部署以外の誤った相手に特定個人情報を提供・移転してしまうリスク	・他の機関に提供しようとする特定個人情報の正当性を逐一個人番号で照合するため、誤って他人の情報を提供することはない。（個人番号での称号ができないものは、住所・氏名・生年月日・性別の完全一致で照合する。） ・フラッシュメモリを用いた提供については、提供相手と直接対面し、相手が持参した媒体にデータを格納することで提供している。電子メールを用いた提供については、庁内ネットワークのメールシステムで、相手からの提供依頼時に相手が定めたパスワードを提供データに施し送付することとしている。
6. 情報提供ネットワークシステムとの接続		・接続しない。
7．県が行う特定個人情報の保管・消去 （P.17～P.18）	リスク1：県が保有する特定個人情報が、他者に漏えい又は他者による滅失・毀損に遭うリスク	・県サーバ集約センターにおいて、サーバ設置場所、記録媒体の保管場所を施錠管理し、監視カメラで入退室者の特定管理を行っている。また、ウイルス対策ソフトの定期的パターン更新等を行っている。
	リスク2：更新すべき特定個人情報が更新されず、古い情報のまま保管され続けるリスク	・市町村の住民基本台帳で本人確認情報の変更があった場合には住民基本台帳ネットワークシステムを通して本人確認情報の更新が行われる仕組みとなっているため、古い情報のまま保管されることはない。
	リスク3：消去すべき特定個人情報が保管期限後も消去されずにいつまでも存在するリスク	・修正前の本人確認情報は保存期間経過後システム的に消去する。 ・磁気ディスクの廃棄時は、要領・手順書等に基づき、内容の消去、破壊等を行うとともに、その記録を残す。また、専用ソフトによるフォーマット、物理的粉砕等を行うことにより、内容を読み出すことができないようにする。 ・帳票については、福岡県文書管理規程等に基づき、定められた期間のみ保管するとともに、廃棄時には裁断、溶解等、当該文書に記録された情報の漏えいを防止するために必要な措置を講じるものとする。

Ⅳ　その他のリスク対策

1．監査の実施 （P.19）		○自己点検 ・年に 1 回、住民基本台帳ネットワークシステムの端末を設置している全所属に対し、セキュリティ対策に係るチェックリストを配布し、自己点検を実施する。 ○監査 ・利用所属の一部を抽出して、外部監査事業者による監査を実施し、監査結果を踏まえて体制や規定を改善する。
2. 職員に対する教育・啓発 （P.19）		・年に1回、住基ネットの初任者等を対象に、住民基本台帳ネットワークシステムの操作方法や禁止事項等の研修を行う。また、別途住基ネットを利用する全所属を対象に、セキュリティ対策に関する研修会を行う。