

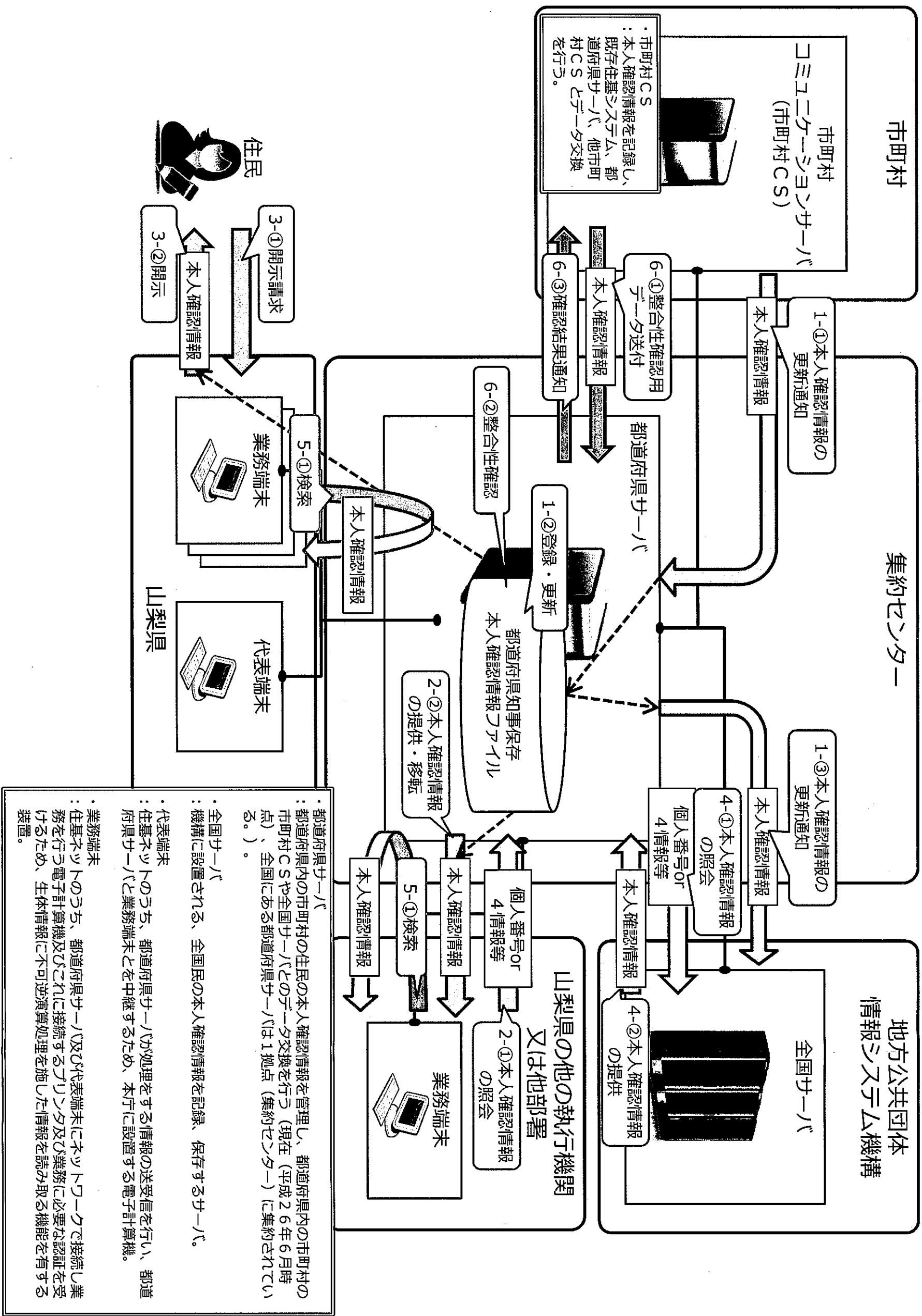
## 住民基本台帳ネットワークシステムに係る本人確認情報の管理及び提供等に関する事務 全項目評価書の概要

<p>I 基本情報</p> <ul style="list-style-type: none"> <li>○ 事務の内容、システムの概要については、別図のとおり。</li> <li>○ 他のシステムとの接続 情報提供ネットワークシステム等、他のシステムとは接続しない。</li> <li>○ 情報提供ネットワークシステムによる情報連携 実施しない。</li> </ul>	<p>県から受領した本人確認情報を元に機構保存本人確認情報 ファイルを更新する。</p> <p>【提供先2】 山梨県他の執行機関</p> <ul style="list-style-type: none"> <li>・ 提供先における用途</li> <li>他の執行機関への情報提供が認められる事務(住民基本台帳法別表第6)の処理に用いる。</li> </ul> <p>【提供先3】 住民</p> <ul style="list-style-type: none"> <li>・ 提供先における用途</li> <li>開示された情報を確認し、必要に応じてその内容の全部又は一部の訂正、追加又は削除の申出を行う。</li> </ul> <p>【提供先1】 山梨県他の部署</p> <ul style="list-style-type: none"> <li>・ 移転先における用途</li> <li>住民基本台帳法別表第5及び山梨県住民基本台帳法施行条例に掲げる、本人確認情報の利用が認められた事務の処理に用いる。</li> </ul>	<p>システム上、本人確認情報更新の際に論理チェックを行う。</p> <ul style="list-style-type: none"> <li>・ 入手の際に特定個人情報が入り、紛失するリスク</li> <li>市町村CSと専用回線で接続。情報の暗号化の実施</li> </ul> <ul style="list-style-type: none"> <li>○ 特定個人情報の使用におけるリスク対策</li> <li>・ 目的を超えた紐づけ等が行われるリスク・対策</li> <li>都道府県サーバと宛名システム、庁内システムとの接続は行わない。</li> <li>・ 権限のない者によって不正に使用されるリスク・対策</li> <li>生体認証による操作者認証を行う。</li> <li>操作者一覧表を作成し、アクセス権限を適切に管理する。</li> <li>・ 従業者が事務外で使用するリスク・対策</li> <li>操作履歴を記録し、不正な操作の疑いがある場合は、ヒアリングを実施し、業務上不要な検索等がないことを確認する。</li> <li>・ 特定個人情報ファイルが不正に複製されるリスク・対策</li> <li>システム上、管理権限のある職員以外の複製を行えない仕組みとする。</li> </ul>
<p>II 特定個人情報ファイルの概要</p> <ul style="list-style-type: none"> <li>○ 対象となる本人の範囲 山梨県内の住民(転出等により住民票から削除された者を含む。)</li> <li>○ 記録される項目 個人番号、4情報(氏名、性別、生年月日、住所)、転出入情報</li> <li>○ 特定個人情報ファイルの保有開始日 平成27年7月予定</li> <li>○ 特定個人情報の入手・使用 県内の市町村から、市町村CSを通じて入手する。 使用方法は別図に示すとおり。</li> <li>○ 特定個人情報ファイルの取扱いの委託</li> </ul> <p>【委託事項1】</p> <ul style="list-style-type: none"> <li>・ 委託内容 都道府県サーバの運用・監視に関する業務</li> <li>※ 委託する業務は、直接本人確認情報に関わらない(直接本人確認情報にアクセスできず、閲覧、更新、削除等を行わない)業務を対象とする。</li> <li>・ 委託先 地方公共団体情報システム機構</li> <li>・ 再委託 書面による事前承諾がある場合に限り可能</li> </ul> <p>【委託事項2】</p> <ul style="list-style-type: none"> <li>・ 委託内容 代表端末等機器の運用管理に関する業務</li> <li>※ 委託する業務は、直接本人確認情報に関わらない(直接本人確認情報にアクセスできず、閲覧、更新、削除等を行わない)業務を対象とする。</li> <li>・ 委託先 株式会社 YSK e-com</li> <li>・ 再委託 原則として禁止。やむを得ず再委託をする場合は、県の事前承諾を要する。</li> </ul> <ul style="list-style-type: none"> <li>○ 特定個人情報の提供・移転</li> </ul> <p>【提供先1】 地方公共団体情報システム機構</p> <ul style="list-style-type: none"> <li>・ 提供先における用途</li> </ul>	<p>県から受領した本人確認情報を元に機構保存本人確認情報 ファイルを更新する。</p> <p>【提供先2】 山梨県他の執行機関</p> <ul style="list-style-type: none"> <li>・ 提供先における用途</li> <li>他の執行機関への情報提供が認められる事務(住民基本台帳法別表第6)の処理に用いる。</li> </ul> <p>【提供先3】 住民</p> <ul style="list-style-type: none"> <li>・ 提供先における用途</li> <li>開示された情報を確認し、必要に応じてその内容の全部又は一部の訂正、追加又は削除の申出を行う。</li> </ul> <p>【移転先1】 山梨県他の部署</p> <ul style="list-style-type: none"> <li>・ 移転先における用途</li> <li>住民基本台帳法別表第5及び山梨県住民基本台帳法施行条例に掲げる、本人確認情報の利用が認められた事務の処理に用いる。</li> </ul> <ul style="list-style-type: none"> <li>○ 特定個人情報の保管・消去</li> <li>・ 集約センターにおいて、施設管理・入室管理を行っている部屋に設置したサーバ内に保管する。サーバへのアクセスはID/パスワードによる認証が必要。</li> <li>・ 代表端末は施設管理・入室管理がされた部屋に保管し、業務端末・記録媒体を施設管理された部屋に保管する。</li> <li>県の代表端末・業務端末へのアクセスはID/パスワード・生体認証が必要。</li> <li>・ 消去方法 都道府県知事保存本人確認情報ファイルに記録されたデータをシステムにて自動判別し消去する。</li> </ul>	<p>システム上、本人確認情報更新の際に論理チェックを行う。</p> <ul style="list-style-type: none"> <li>・ 入手の際に特定個人情報が入り、紛失するリスク</li> <li>市町村CSと専用回線で接続。情報の暗号化の実施</li> </ul> <ul style="list-style-type: none"> <li>○ 特定個人情報の使用におけるリスク対策</li> <li>・ 目的を超えた紐づけ等が行われるリスク・対策</li> <li>都道府県サーバと宛名システム、庁内システムとの接続は行わない。</li> <li>・ 権限のない者によって不正に使用されるリスク・対策</li> <li>生体認証による操作者認証を行う。</li> <li>操作者一覧表を作成し、アクセス権限を適切に管理する。</li> <li>・ 従業者が事務外で使用するリスク・対策</li> <li>操作履歴を記録し、不正な操作の疑いがある場合は、ヒアリングを実施し、業務上不要な検索等がないことを確認する。</li> <li>・ 特定個人情報ファイルが不正に複製されるリスク・対策</li> <li>システム上、管理権限のある職員以外の複製を行えない仕組みとする。</li> </ul> <ul style="list-style-type: none"> <li>○ 特定個人情報ファイルの取扱いの委託におけるリスク・対策</li> <li>・ 特定個人情報ファイルの閲覧者・更新者の制限</li> <li>作業者を限定するために、委託作業者の名簿を提出させる。</li> <li>・ 特定個人情報の提供ルール</li> <li>委託先から他者への特定個人情報の提供は一切認めないことを契約上明記する。</li> <li>地方公共団体情報システム機構は、日次、月次、年次で目的外利用及び提供についてセキュリティチェックを行い、当県は、月次で書面により、「セキュリティ確認結果報告」の報告を受けている。</li> <li>代表端末等機器の運用管理に関する業務委託においては、受託者に特定個人情報を提供しない。</li> <li>・ 特定個人情報の消去のルール</li> <li>委託契約書に、保管期間の過ぎた特定個人情報をシステムにて自動判別し、消去する等の措置をとる旨を規定する。</li> <li>・ 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</li> <li>目的外利用の禁止</li> <li>特定個人情報の閲覧者・更新者を制限 等</li> <li>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</li> <li>再委託する業務は、直接本人確認情報に関わらない業務とする。</li> </ul>
	<p>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</p> <ul style="list-style-type: none"> <li>○ 特定個人情報の入手におけるリスク対策</li> <li>・ 目的外の入手が行われるリスク・対策 入手手段は、市町村CSからの本人確認情報更新要求の際に通知される場合に限定される。</li> <li>市町村の住基所管課職員を対象とした研修会等において、厳格な本人確認を行うよう周知する。</li> <li>・ 不適切な方法で入手が行われるリスク・対策 入手元を市町村CSに限定する。</li> <li>・ 入手した特定個人情報が入り、不正であるリスク・対策</li> </ul>	

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 全項目評価書の概要

<ul style="list-style-type: none"> <li>○ 特定個人情報の提供・移転におけるリスク対策             <ul style="list-style-type: none"> <li>・ 不正な提供・移転が行われるリスク・対策</li> <li>・ 特定個人情報の提供・移転を行う際に、提供・移転の記録をシステム上で記録し、7年間分保存する。</li> </ul> </li> </ul> <p>操作者に付与する権限の範囲は、当該操作者がその業務を行うために必要な範囲に限っており、権限のない者はアクセスできない仕組みとする。</p> <ul style="list-style-type: none"> <li>・ 不適切な方法で提供・移転が行われるリスク・対策</li> </ul> <p>全国サーバと都道府県サーバ間の通信では相互認証を実施しているため、認証できない相手方への情報の提供はなされないことがシステム上で担保される。</p> <p>県他の執行機関への情報提供等のため、媒体へ出力する必要がある場合には、逐一出力の記録が残される仕組みを構築する。</p> <ul style="list-style-type: none"> <li>・ 誤った情報を提供・移転してしまうリスク、誤った相手に提供・移転してしまうリスク・対策</li> </ul> <p>システム上、照会元から指定された検索条件に基づき得た結果を適切に提供・移転することを担保する。</p> <ul style="list-style-type: none"> <li>○ 情報提供ネットワークシステムとの接続におけるリスク対策             <ul style="list-style-type: none"> <li>・ 情報提供ネットワークシステムとは接続しない。</li> </ul> </li> <li>○ 特定個人情報の保管・消去におけるリスク対策             <ul style="list-style-type: none"> <li>・ 特定個人情報の漏えい・滅失・毀損リスク・対策</li> <li>・ 安全管理体制、安全管理規程の整備、安全管理体制・規程の職員への周知については、十分に整備・周知している。</li> </ul> </li> </ul> <p>集約センターにおいては、監視カメラを設置してサーバ設置場所への入退室者を特定し、管理する。</p> <p>県では、代表端末及び媒体記録を、入退室記録をとって保管している部屋に保管し、業務端末を設置した執務室は職員が退庁時に施錠する。</p> <p>ウイルス対策ソフトの定期的パターン更新を行う。</p> <ul style="list-style-type: none"> <li>・ 特定個人情報古い情報のまま保管され続けるリスク・対策</li> <li>・ 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、住民ネットワークを通じて本人確認情報の更新が行われる仕組みとなっているので、古い情報のまま保管されることはない。</li> <li>・ 特定個人情報が消去されずにいつまでも存在するリスク・対策</li> </ul>	<p>住民票の記載の修正前の本人確認情報(履歴情報)及び消除者の本人確認情報は、住民基本台帳法施行令に定める保存期間を経過した後にシステム的に消去する。</p>	
	<p>IV その他のリスク対策</p> <ul style="list-style-type: none"> <li>○ 自己点検             <ul style="list-style-type: none"> <li>・ 年に1回、担当部署内において実施している自己点検に用いるチェック項目に、「評価書に記載どおりの運用がなされていること」に係る内容を追加し、運用状況を確認する。</li> </ul> </li> <li>○ 監査             <ul style="list-style-type: none"> <li>・ 年に1回、組織内に置かれた監査担当により自己監査を実施し、監査結果を踏まえて体制や規定を改善する。</li> </ul> </li> <li>○ 従業者に対する教育・啓発             <ul style="list-style-type: none"> <li>・ 住民ネットワーク操作を対象にした研修を毎年度当初に実施。</li> </ul> </li> </ul> <p>住民ネットワークの利用について必要な知識の習得及びセキュリティに関する意識の向上を図り、その記録を残す。</p>	
	<p>V 開示請求、問合せ</p> <ul style="list-style-type: none"> <li>○ 特定個人情報の開示・訂正・利用停止請求             <ul style="list-style-type: none"> <li>・ 請求先 山梨県総務部市町村課行政選挙担当</li> <li>・ 来庁し、又は郵送で、書面により開示、訂正等を請求</li> </ul> </li> </ul>	

【別図】 事務の内容



・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  
：住基ネットのうち、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、本庁に設置する電子計算機。

・業務端末  
：住基ネットのうち、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。