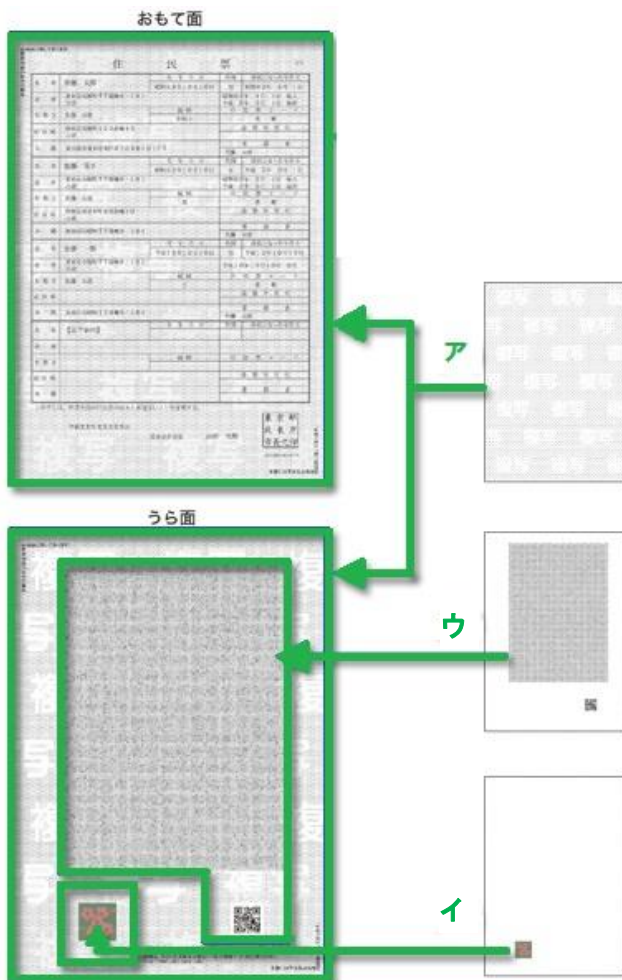


8. セキュリティ対策(詳細)

	コンビニ事業者	地方公共団体情報システム機構	新宿区
管理するシステム等	ECセンター キオスク端末(端末)	証明書交付センター	既存住基システム 証明書自動交付システム
物理的な措置 (主なもの)	○端末は施錠されており、端末保守員以外の者は開錠できません。	○証明書交付センターのサーバは、セキュリティの確保されたデータセンターに設置され、入退室管理を厳格に行っています。	○サーバの設置室は施錠されているほか、あらかじめ許可した者以外の入室を禁止しています。
技術的な措置 (主なもの)	○証明書データは、ECセンターで保持しないほか、発行後速やかにセキュリティソフトによって端末から自動的に消去されます。 ○ECセンター内のサーバは、外部及び内部ネットワークから隔離されたエリアに設置します。 ○パスワードにより、端末保守員以外の者は端末のプログラムへのアクセスができません。	○ネットワークには、閉域性の確保された専用回線及び行政専用のネットワーク(LGWAN)回線を使用し、第三者からのアクセスを排除します。 ○専用回線及びLGWAN回線におけるデータ通信は、SSL(データの盗取や改ざん等を防止するための暗号化通信の方法)による安全化措置がとられます。	○ウイルス対策のソフトウェアを導入し、ウイルスをチェックするファイルを定期的に更新します。 ○ファイアウォールを設置し、不正プログラム等のシステムへの侵入を防止します。
その他の措置 (主なもの)	○個人番号カード取り忘れ防止のため、カードを取り外さないと証明書発行画面まで進めません。 ○証明書取り忘れ防止のため、端末の音声・画面で警告します。 ○証明書を取り忘れた場合は、コンビニの従業員が遺失物として警察に届け出ます。	○証明書の偽造・改ざんを防止するために、証明書に以下ア～ウの措置(※)が施されています。 ア けん制文字 イ スクランブル画像 ウ 偽造防止検出画像	○新宿区情報セキュリティポリシー及び新宿区個人情報保護条例等に基づき、個人情報の適切な管理運用を行っています。

(※) 証明書の偽造・改ざん防止措置



ア けん制文字(偽造防止措置)

証明書をコピーした場合は「複写」という文字が浮かびあがるため、証明書の提出を受けた先で、原本か否かの見分けがつかます。

イ 偽造防止検出画像(偽造防止措置)

証明書の裏面に、専用の器具を使うことで確認できる、隠れた「潜像画像」が印刷されており、これはコピーすると欠落する性質があるため、証明書の提出を受けた先で、原本か否かの見分けがつかます。

ウ スクランブル画像(改ざん防止措置)

証明書のうら面に印刷されている「スクランブル画像」をスキャナで読み込み、専用のサイトで確認すると、スクランブルを解除した画像(証明書発行時のおもて面の元画像)がパソコン上に表示されます。

証明書の提出を受けた先で、パソコン上に表示された画像と、提出された証明書のおもて面の内容とに相違がないか見比べ、証明書の内容の改ざんの有無を確認できます。