**地方公共団体情報システム共通機能標準仕様書【第2.1版】　新旧対照表**

| **改定後** | **現行** |
| --- | --- |
| 2.　共通機能の要件の標準について  2.1.　申請管理機能  （略）  2.1.7.　将来的なオンライン申請の在り方の検討  デジタル社会の実現に向けた重点計画（令和５年（2023年）６月９日閣議決定）においては、「品質・コスト・スピードを兼ね備えた行政サービスに向けて、アーキテクチャ設計の在り方を根本から見直す」とされ、マイナンバーカードの普及及び利用の推進に伴い、行政手続に係るデジタル化・オンライン化について、様々な取組みが行われている。例えば、公共サービスメッシュ（情報連携の基盤）については、手続時の入力を最小限にするために申請内容をあらかじめ表示することなどの利便性の高いサービスを最小限のシステム対応で実現できるよう、地方公共団体の基幹業務システムの統一・標準化を踏まえ、令和７年度（2025年度）中に新たなシステムを整備することとしている。  これらの状況を踏まえ、標準化移行期限である令和７年度（2025年度）末時点の標準化移行状況に鑑みて、令和８年度（2026年度）以降に将来的なオンライン申請の在り方について検討を進める。  （略）  2.2.　庁内データ連携機能  （略）  2.2.5.　RESTによる公開用API連携における認証認可について  　RESTによる公開用API連携において、APIを利用する基幹業務システムの認証認可を行う必要があることから、認証認可の方式について、以下のとおり規定する。  (1) 全般  ① 認証方式  client\_secret\_jwtによるJWTを用いた認証方式とする。  Client Credentials Grantで取得したOAuth2.0アクセストークンはBearerタイプとする。  なお、今後、国で統一ID基盤の整備が検討されていることから、暫定措置として、以下の認証方式の実装も可能とする。  OAuth2.0アクセストークン：Bearerタイプ  認証方式：client\_secret\_basic  API Keyについては、ガバメントクラウドでは原則認めない。認可サーバの設置が難しいオンプレミス環境等においては当面認めるが、あくまで時限的な措置とする。  ② 認証単位  業務IDもしくは独自施策システム等ID単位での認証とする。  なお、システム利用者ごとにAPIの利用可否を認可するものではない。  ③ データ形式  データ形式はJSON形式とする。  ④ 通信プロトコル  通信プロトコルはHTTP1.1以上とする。  ⑤ 通信のセキュリティ  通信のセキュリティはTLS1.2(Transport Layer Security1.2)以上とする。  (2) 認証認可サーバ  ① トークン発行方式  トークン発行方式は、Client Credentials Grantとする。  なお、アクセストークンのみの発行とし、リフレッシュトークンの発行は許容しない。  ② アクセストークンの情報取得方法  提供側業務システムは、認証認可サーバのイントロスペクションAPIを用いてアクセストークンの情報を取得すること。  ③ アクセストークンのライフサイクル（有効期限）  アクセストークンは十分に短いライフサイクル（有効期限）を設定すること。  ④ アクセストークンのスコープ  アクセストークンのスコープは、アクセストークンに割り当てられた権限の範囲を表す文字列であり、アクセストークンを送信することで提供側業務システムへのアクセスが認可されることになるが、スコープは下記のフォーマットで定義すること。  ${提供側業務システムの 業務システムID}:${リソース名}:${操作名}  なお、スコープのフォーマットに用いる文字列は、下記に示す対応に基づいて決定すること。  ・　提供側業務システムの業務システムID：「地方自治体の基幹業務システムの統一・標準化における各種IDの管理方針」の業務ID  ・　リソース名：「共通機能標準仕様書 別紙 API仕様書」のAPIコール名  ・　操作名：「共通機能標準仕様書 別紙 API仕様書」の操作種類  スコープの例を下記に示す。  ・　別紙7-1\_住登外者宛名基本情報照会API仕様書におけるフォーマット文字列：  「031:app\_submit/v10/jutogaishaatenakihonjohosyokai:Read」  ・　別紙7-2\_住登外者宛名番号付番API仕様書におけるフォーマット文字列：  「031:app\_submit/v10/jutogaishaatenabangofuban:Create」  また、利用側業務システムが複数の提供側業務システムにアクセスする場合には、提供側業務システムごとにアクセストークンを発行する。アクセストークンの権限を最小に留めるため、複数の提供側業務システムへアクセス可能なアクセストークンの発行は行わないこと。  (3) クライアント認証方式  ① クライアントタイプ  クライアントタイプはConfidential Clientとする。  ② 署名アルゴリズム  採用する認証方式：client\_secret\_jwtの標準規格に従い、対称鍵であるHS256（ハッシュ関数としてSHA-256を用いたHMAC）とする。  ③ クライアントID  クライアントを一意に識別するためのIDであり、「0-9」「A-Z」「a-z」の文字で構成される32文字の文字列とする。  ④ クライアントシークレット  クライアントを認証する際に利用し、クライアントIDの所有者であることを確認するもので、32文字以上の文字列とする。  ⑤ クライアントID管理の単位  利用側業務システムの単位でクライアントIDを発行するものとする。  (4) 利用側業務システム  ① Bearerトークンの送信方法  Bearerトークンの送信方法はAuthorization Request Header Fieldとし、Authorizationヘッダに取得したアクセストークンを設定する。なお、利用側業務システムは一度のリクエストにおいて、複数の送信方法を同時に用いてはならない。 | 2.　共通機能の要件の標準について  2.1.　申請管理機能  （略）  2.1.7.　将来的なガバメントクラウド申請管理機能の提供  デジタル社会の実現に向けた重点計画（令和４年６月７日閣議決定）においては、「品質・コスト・スピードを兼ね備えた行政サービスに向けて、アーキテクチャ設計の在り方を根本から見直す」にあたり、情報連携の基盤となる公共サービスメッシュについては、「②手続時の入力を最小限化するためにあらかじめ申請内容をプレ表示したり、関連する手続などを推奨したりするプッシュ機能等を備えたプッシュ型サービスを実現するため、地方公共団体が保有する住民情報を当該住民向けプッシュ型サービスなどに活用する仕組み（略）等を包括的に実現し、利便性の高いデジタルサービス実現を更に推進」することとしている。  具体的には「手続時の入力を最小限にするためにあらかじめ申請内容をプレ表示する機能や、関連する手続などを推奨するプッシュ機能などの利用者目線のサービスをスマートフォンでも実現できるよう、ガバメントクラウド上で必要なモジュールを整備」し、「地方公共団体基幹業務等システムの統一・標準化（データの標準化やガバメントクラウドの活用等）を見据えて、基幹業務システムとフロントサービスを提供する各機能とが、疎結合な形でAPI連携できるようにすることにより、円滑なデータ連携を可能とし、ユーザーニーズや技術動向の変化にも柔軟に対応できるようにする」こととしている。  そのため、デジタル庁において「令和４年度（2022年度）にガバメントクラウドで稼働するコンポーネントとしてプロトタイプ構築に着手し、令和５年度（2023年度）以降、地方公共団体の任意に応じて先行的に実証・活用できるように検討を進める」ものであり、マイナポータル等と標準準拠システムをつなぐための機能である申請管理機能についても、当面は令和７年をターゲットに、ガバメントクラウドにおいて標準準拠システムが利用できる申請管理機能（「ガバメントクラウド申請管理機能」という。）として、基本的な機能から、希望する地方公共団体が利用することが可能になるよう検討を進める。  基幹業務等の標準準拠システムは、「データ要件・連携要件に関する標準化基準に適合することにより、当該データの公共サービスメッシュへの連携を迅速かつ円滑に行える拡張性を有することとなる」ものであり、標準準拠システムと申請管理機能のインターフェースは本仕様に定めたものを踏まえる予定である。  標準準拠システムにおいては本仕様2.1.4.に定めるインターフェースを備えることで、標準準拠システムは追加の対応を原則行わずに、申請管理システム（総務省仕様準拠）及びガバメントクラウド申請管理機能のいずれを利用することも可能となる。  （略）  2.2.　庁内データ連携機能  （略）  2.2.5.　RESTによる公開用API連携における認証認可について  　RESTによる公開用API連携において、APIを利用する基幹業務システムの認証認可を行う必要があることから、認証認可の方式について、以下のとおり規定する。  (1) 全般  ① 認証方式  client\_secret\_jwtによるJWTを用いた認証方式とする。  client Credentials Grantで取得したOAuth2.0アクセストークンはBearerタイプとする。  なお、今後、国で統一ID基盤の整備が検討されていることから、暫定措置として、以下の認証方式の実装も可能とする。  OAuth2.0アクセストークン：Bearerタイプ  認証方式：client\_secret\_basic  API Keyについては、ガバメントクラウドでは原則認めない。認可サーバの設置が難しいオンプレミス環境等においては当面認めるが、あくまで時限的な措置とする。  ② 認証単位  業務IDもしくは独自施策システム等ID単位での認証とする。  なお、システム利用者ごとにAPIの利用可否を認可するものではない。  ③ データ形式  データ形式はJSON形式とする。  ④ 通信プロトコル  通信プロトコルはHTTP1.1以上とする。  ⑤ 通信のセキュリティ  通信のセキュリティはTLS1.2(Transport Layer Security1.2)以上とする。  (2) 認証認可サーバ  ① トークン発行方式  トークン発行方式は、Client Credentials Grantとする。  なお、アクセストークンのみの発行とし、リフレッシュトークンの発行は許容しない。  ② アクセストークンの情報取得方法  提供側業務システムは、認証認可サーバのイントロスペクションAPIを用いてアクセストークンの情報を取得すること。  ③ アクセストークンのライフサイクル（有効期限）  アクセストークンは十分に短いライフサイクル（有効期限）を設定すること。  ④ アクセストークンのスコープ  アクセストークンのスコープは、アクセストークンに割り当てられた権限の範囲を表す文字列であり、アクセストークンを送信することで提供側業務システムへのアクセスが認可されることになるが、スコープは下記のフォーマットで定義すること。  ${提供側業務システムの 業務システムID}:${リソース名}:${操作名}  なお、スコープのフォーマットに用いる文字列は、下記に示す対応に基づいて決定すること。  ・　提供側業務システムの業務システムID：「地方自治体の基幹業務システムの統一・標準化における各種IDの管理方針」の業務ID  ・　リソース名：「共通機能標準仕様書 別紙 API仕様書」のAPIコール名  ・　操作名：「共通機能標準仕様書 別紙 API仕様書」の操作種類  スコープの例を下記に示す。  ・　別紙7-1\_住登外者宛名基本情報照会API仕様書【第2.0版】におけるフォーマット文字列：  「031:app\_submit/v10/jutogaishaatenakihonjohosyokai:Read」  ・　別紙7-2\_住登外者宛名番号付番API仕様書【第2.0版】におけるフォーマット文字列：  「031:app\_submit/v10/jutogaishaatenabangofuban:Create」  また、利用側業務システムが複数の提供側業務システムにアクセスする場合には、提供側業務システムごとにアクセストークンを発行する。アクセストークンの権限を最小に留めるため、複数の提供側業務システムへアクセス可能なアクセストークンの発行は行わないこと。  (3) クライアント認証方式  ① クライアントタイプ  クライアントタイプはConfidential Clientとする。  ② 署名アルゴリズム  採用する認証方式：client\_secret\_jwtの標準規格に従い、対称鍵であるHS256（ハッシュ関数としてSHA-256を用いたHMAC）とする。  ③ クライアントID  クライアントを一意に識別するためのIDであり、「0-9」「A-Z」「a-z」の文字で構成される32文字の文字列とする。  ④ クライアントシークレット  クライアントを認証する際に利用し、クライアントIDの所有者であることを確認するもので、32文字以上の文字列とする。  ⑤ クライアントID管理の単位  利用側業務システムの単位でクライアントIDを発行するものとする。  (4) 利用側業務システム  ① Bearerトークンの送信方法  Bearerトークンの送信方法はAuthorization Request Header Fieldとし、Authorizationヘッダに取得したアクセストークンを設定する。なお、利用側業務システムは一度のリクエストにおいて、複数の送信方法を同時に用いてはならない。 |