別表第一（第一条関係）
別表第1の適用に関する通則
一　認証単位は業務ID若しくは独自施策システム等ID単位の認証とする。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。
二　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
三　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。
四　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。
五　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。
六　クライアントタイプはConfidential Clientとする。
七　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。
八　クライアントIDは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。
九　クライアントシークレットは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。
十　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。
十一　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。

概要

本資料はOAuth2.0アクセストークン発行を実施するためのAPI仕様について記述したものである。
「地方公共団体情報システムの標準化に関する法律第７条第１項に規定する各地方公共団体情報システムに共通する基準のうち電磁的記録において用いられる用語及び符号の相互運用性の確保その他の地方公共団体情報システムに係る互換性の確保に関する標準を定める命令（令和8年デジタル庁・総務省令第８号）」の「文字要件」で定めた標準仕様に従う必要がある。
本APIでサポートするHTTPメソッドはPOSTとする。

提供可能なAPIコールについて

提供するAPIコールは、以下のとおりである。

No.	APIコール名	操作種類	概要
1	oauth/v1/token	Create	OAuth2.0アクセストークン発行を実施する。

APIコールにおける補足事項

■通信プロトコル
本APIを利用する際の通信プロトコルは、HTTP1.1以上を採用する。
■要求元認証
本APIの要求元認証は、認証方式：client_secret_jwtで行う。

シーケンス図

