5.14.統合ディレクトリ

5.14.1.統合ディレクトリの定義

統合ディレクトリは、各府省が個別に保有するアカウント情報のマスター・データベース機能を提供する。人事・給与情報システムや府省共通の職員等利用者共通認証基盤(GIMA)とデータ連携を行い、アカウント情報のマスター・データを保持する。統合ディレクトリに格納されたアカウント情報は、統合アカウント管理機能やディレクトリ連携機能により府省内の個別ディレクトリへ配布される。

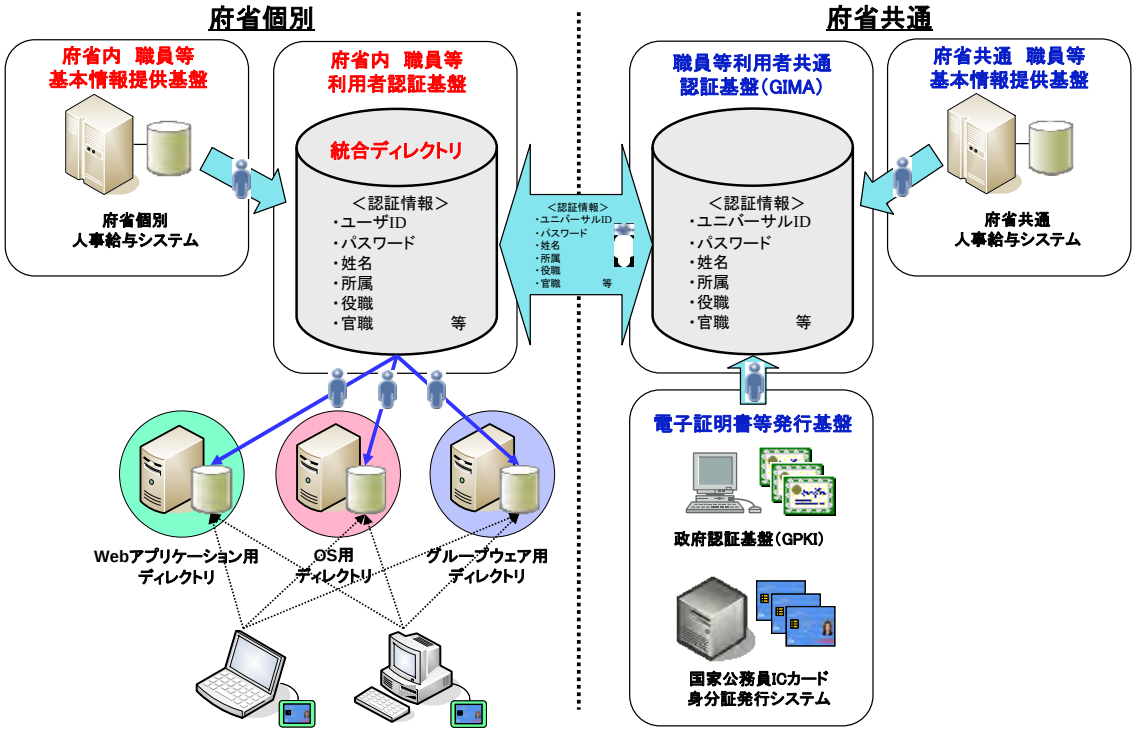

図 5.14-1 統合ディレクトリと職員等利用者共通認証基盤(GIMA)の関係

統合ディレクトリの機能・サービス	
機能・サービス	定義
統合ディレクトリ	府省ごとに構築されるアカウント情報のマスター・データベース機能を提供する。Web アプリケーションやグループウェアを利用する際のアカウント情報を一元的に管理するための基盤機能であるとともに、職員情報のディレクトリとして職員の検索にも対応する。 各種ディレクトリに格納するアカウント情報のマスターとなるデータを格納するため、人事異動の際には最新の組織・職員情報に更新する必要があり、人事給与システムや府省共通の職員等利用者共通認証基盤(GIMA)とデータ連携を行う。 [参考] 人事給与システムは、各府省が個別に構築したシステムと、業務・システム最適化計画に基づき府省共通で構築したシステムが存在する。現在は府省個別のシステムから、府省共通のシステムへ移行している段階であり、各府省の移行状況に応じて、統合ディレクトリが連携すべきシステムを選定する必要がある。 職員等利用者共通認証基盤(GIMA：Government Identity Management for Authentication)は、府省共通業務アプリケーション及び府省内業務アプリケーションを利用するためのアカウント情報を管理し、認証・認可・監査ログ取得機能を提供する。 ■職員等利用者共通認証基盤(GIMA)が提供する機能 ①アカウント情報の管理と提供 ②主体認証機能及び利用認可機能の提供 ③アクセス証跡情報(上記①、②に関するログ情報)の記録と提供 職員等利用者共通認証基盤(GIMA)は、人事給与システムの人事情報をオンラインにより取り込み、業務アプリケーションにおけるアカウント情報の管理業務を効率化する。 府省内のアカウント情報を一元的に管理する仕組みを既に保有している府省においては、既に保有しているこの仕組みを府省内職員等利用者認証基盤として活用し、府省内業務アプリケーションに対し、GIMA と同等の機能を提供する。 職員等利用者共通認証基盤(GIMA)とのデータ連携に必要な連携仕様書が整備されているので、必要に応じて参照すること。

5.14.2.統合ディレクトリの機能要件・非機能要件

機能要件（認証情報としてパスワードを想定）		
1	基本	統合アカウント管理機能やディレクトリ連携機能と連携して、アカウント情報を一元的に管理する仕組みを実現すること。
2	基本	アカウント情報を保管し、一元的に管理するためのリポジトリ(データ保管)機能を提供すること。リポジトリには、利用者に関する次のような情報を格納できること。 ●Identifier : 利用者を識別する ID(ユーザ ID 等) ●Credential : 認証に使用するデータ(パスワード等) ●Common Profile : 利用者に関するデータ(所属や官職等)
3	加点	リポジトリには、利用者に関する次のような情報を格納できること。 ●Application Profile : アプリケーションが利用するデータ
4	加点	府省個別の人事給与システムとデータ連携が行えること。
5	基本	アカウント情報をインポート/エクスポートできる機能を有すること。
6	基本	外部システムとのデータ連携のインタフェースが提供されていること。
7	基本	アカウント情報に対する操作を、監査ログとして記録することができること。
8	加点	監査ログはレポートとしてわかりやすい形式で表示できること。

非機能要件（個別の要件がある場合のみ記述）		
可用性	加点	サーバの冗長化やクラスタ・ソフト、レプリケーション等の技術により可用性を高める構成を採用すること。
セキュリティ	基本	認証を受けた管理者のみが、アカウント情報にアクセスできる仕組みを有すること。
	基本	管理者の役割や管理対象の範囲に応じて、適切なアクセス権を設定してアカウント情報を保護することができること。
	基本	取得した監査ログはアクセス制御を徹底して改ざんを防止すること。
	加点	通信の暗号化が可能なこと。
パフォーマンス	基本	「約 5 万」のアカウント情報を管理することとなり、人事異動の際には短期間に大量のユーザ属性を更新することが求められる。事前に性能要件を明確にし、十分な処理能力をもった構成とすること。
拡張性	加点	対象とするシステムや利用者の増加に伴い、ユーザ ID の増加が予想されるため、処理能力の柔軟な増強ができる構成とすること。
バックアップ	基本	リポジトリに保管されたアカウント情報のデータのバックアップを取得すること。

関連する技術	
ディレクトリサービスアクセスプロトコル	LDAP:LDAP(Lightweight Directory Access Protocol)は、ディレクトリ・サービスに接続するために使用される標準プロトコル。LDAP V3 が規定されている。
ディレクトリサービスデータ交換形式	LDIF:LDIF(LDAP データ交換フォーマット:LDAP Data Interchange Format)は、LDAP のアカウント情報を交換する際に用いるファイル・フォーマットである。
データベースアクセス技術	JDBC:JDBC(Java Database Connectivity)は、Java プログラムから RDB へアクセスするための API。ディレクトリが RDB のケースでは利用が想定される。

・物理構成モデルのセグメントに対応する項目:S1～S6