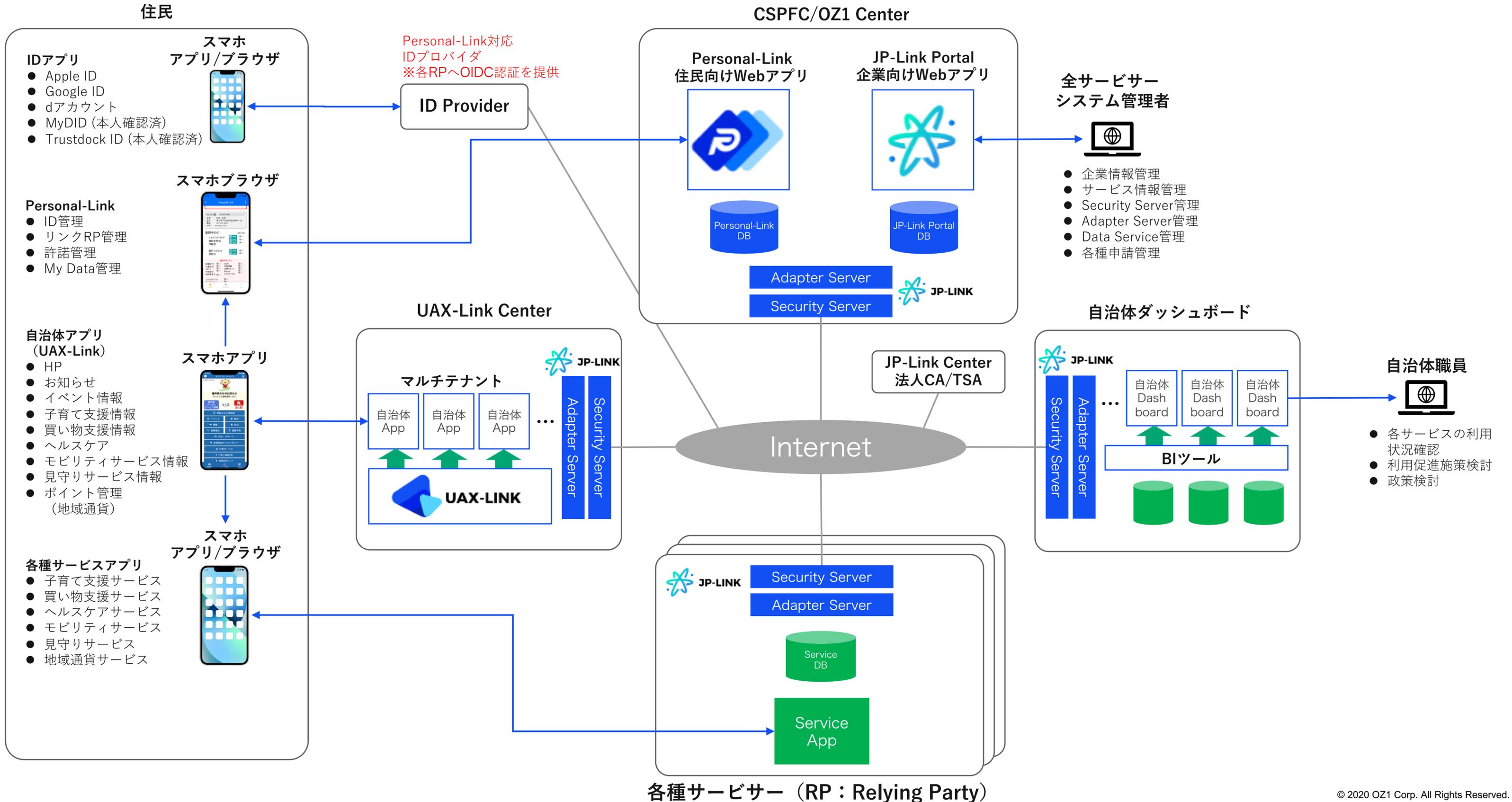
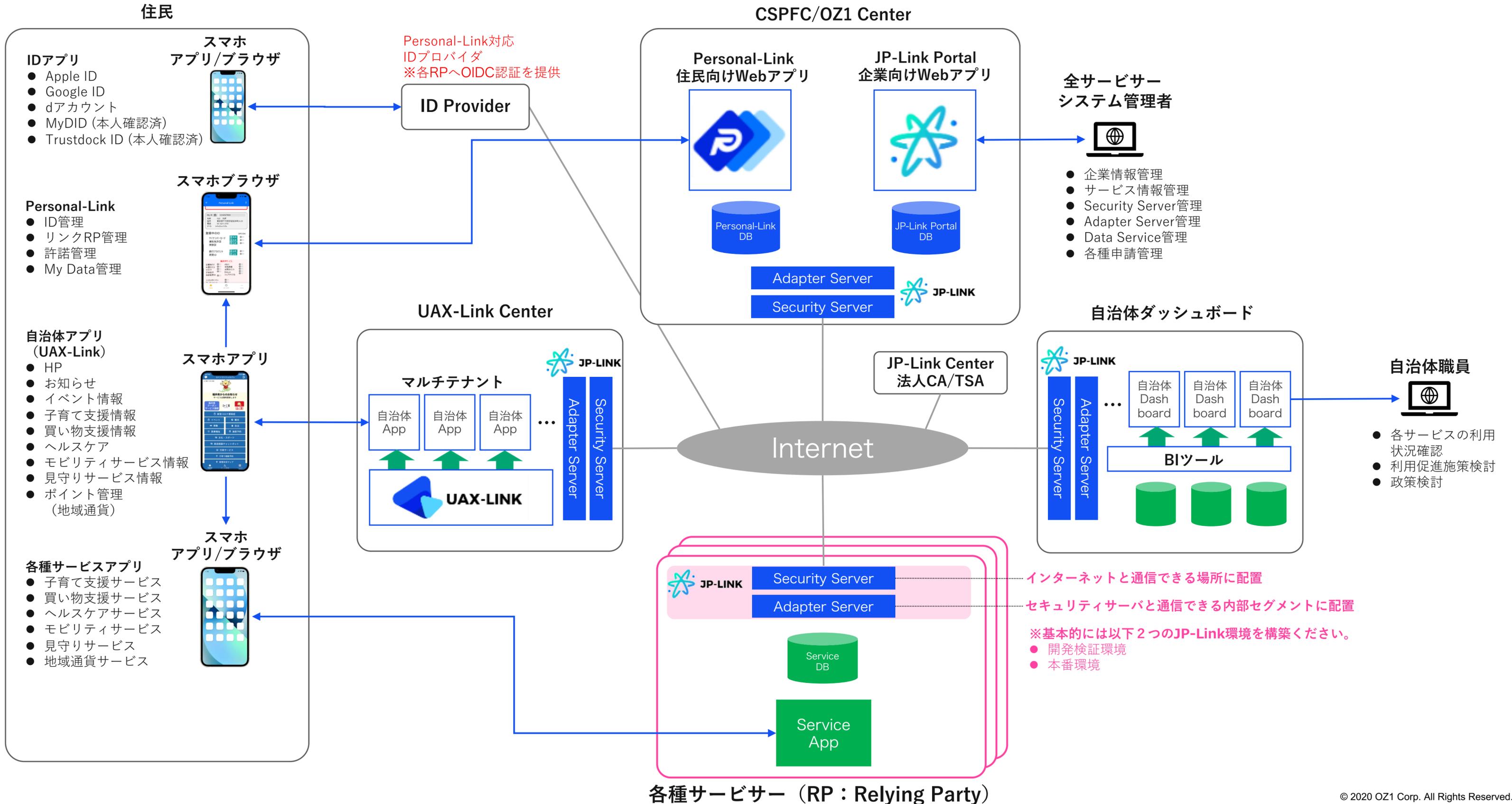


コンパクトスマートシティプラットフォーム（都市OS） 接続仕様概要



JP-Link アーキテクチャ 及び 環境構築 及び 設定／実装概要



セキュリティサーバ動作環境

	Ubuntu	Red Hat Enterprise Linux (RHEL)
OSバージョン	Ubuntu 20.04 or 22.04 LTS x86-64	RHEL 7.3以上、RHEL 8以上
メモリ	4GB 以上	4GB 以上
ストレージ	・OSパーティション10GB以上の空き容量 ・他パーティション(/var 配下) 20GB 以上	・OSパーティション10GB以上の空き容量 ・他パーティション(/var 配下) 20GB 以上

セキュリティサーバポート構成 (インターネットと通信できる場所に配置)

解放するポート	用途
TCP5500 インバウンド/アウトバウンド	セキュリティサーバ間のメッセージ交換のため
TCP5577 インバウンド/アウトバウンド	セキュリティサーバ間のOCSPサービス要求用
TCP4001 アウトバウンド	中央サーバとの通信用
TCP80 アウトバウンド	グローバル設定をダウンロードするため
TCP80 / 443 アウトバウンド	タイムスタンプサービスおよびOCSPサービスとの通信用
TCP4000 インバウンド (ローカル)	セキュリティサーバのユーザーインターフェイスにアクセスするため
TCP80 / 443 インバウンド/アウトバウンド (ローカル)	情報システム接続用
TCP8080/8443 インバウンド/アウトバウンド (ローカル)	(RHEL のみ)情報システム接続用
TCP80/8085/8003 アウトバウンド	アダプターサーバとの通信用

セキュリティサーバ導入手順 (概要)

項番	項目	作業時間の目安 ※1
1	JP-LINKのメンバーコードの取得(OZ1へ依頼)	5分
2	動作環境の準備	各社VM環境作成工数
3	セキュリティサーバのインストール	30分
4	セキュリティサーバの初期セットアップ	10分
5	CSRをOZ1へ送信する ※2	5分
6	証明書のインポート	5分
7	内部通信方式 (HTTP or HTTPS) の選択	5分
8	OZ1テストサービスとの疎通確認	10分
	合計	70分

アダプターサーバ動作環境

	Ubuntu
OSバージョン	Ubuntu 20.04.3 LTS (64-bit server)
メモリ	4GB RAM 以上
ストレージ	50GB 以上

アダプターサーバポート構成(イントラネットでセキュリティサーバとイントラDBとの通信できる場所へ配置)

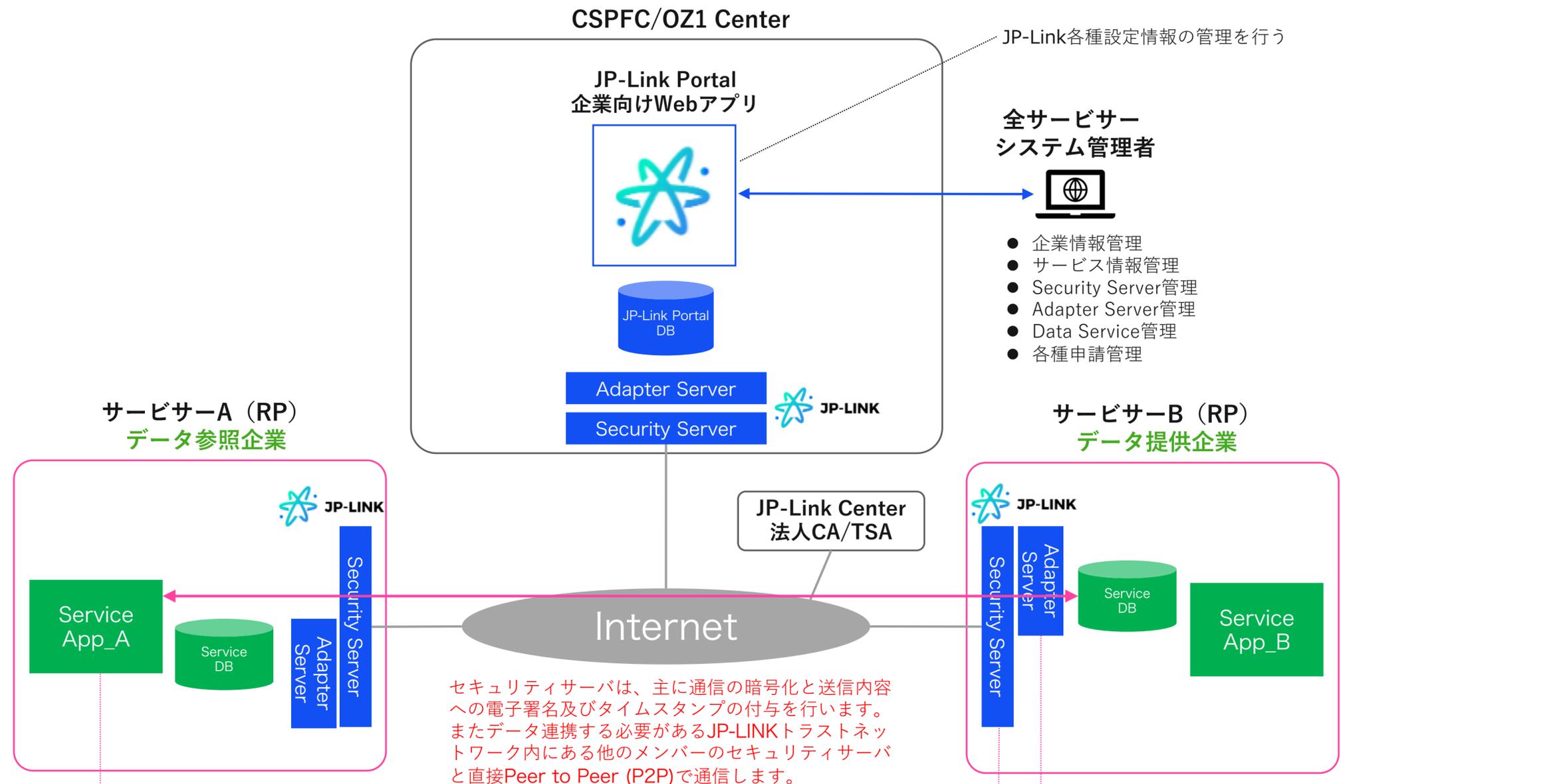
解放するポート	用途
TCP80 / 443 インバウンド	アダプターサーバのユーザーインターフェース接続用
TCP80/8085/8003 インバウンド	セキュリティサーバとの通信用
(TCP5432 アウトバウンド)	データベースとの接続・通信のためにデータベースごとに設定されるTCPポートのアウトバウンド (PostgreSQLの場合、デフォルトポートは5432) ※他のRDBMSの場合は各標準ポート等を設定。

アダプターサーバ導入手順 (概要)

項番	項目	作業時間の目安 ※1
1	動作環境の準備	各社VM環境作成工数
2	Adapter Server のインストール	20分
3	Adapter Serverでのサービスの作成	20分
4	セキュリティサーバへのサービスの登録及びアクセス権設定 (セキュリティサーバ側作業)	10分
	合計	50分

※1) サービサー (RP) 側で実施を想定。OZ1とのやりとりを除く。上記は本プロダクト導入経験があるエンジニアの標準工数で担当の技術スキルに応じて工数が前後する場合がある。詳細については、p.11 「JP-Link/Personal-Link 実装関連ドキュメント」をご参照。

※2) CSR (Certificate Signing Request) とは、セキュリティサーバ証明書を発行するための証明書の署名要求のこと
最短で翌営業日夕刻以降の証明書の返信。なお、申請時に登記簿謄本の提供が必要です。



JP-Link各種設定情報の管理を行う

全サービサーシステム管理者



- 企業情報管理
- サービス情報管理
- Security Server管理
- Adapter Server管理
- Data Service管理
- 各種申請管理

サービサーA (RP)
データ参照企業

サービサーB (RP)
データ提供企業

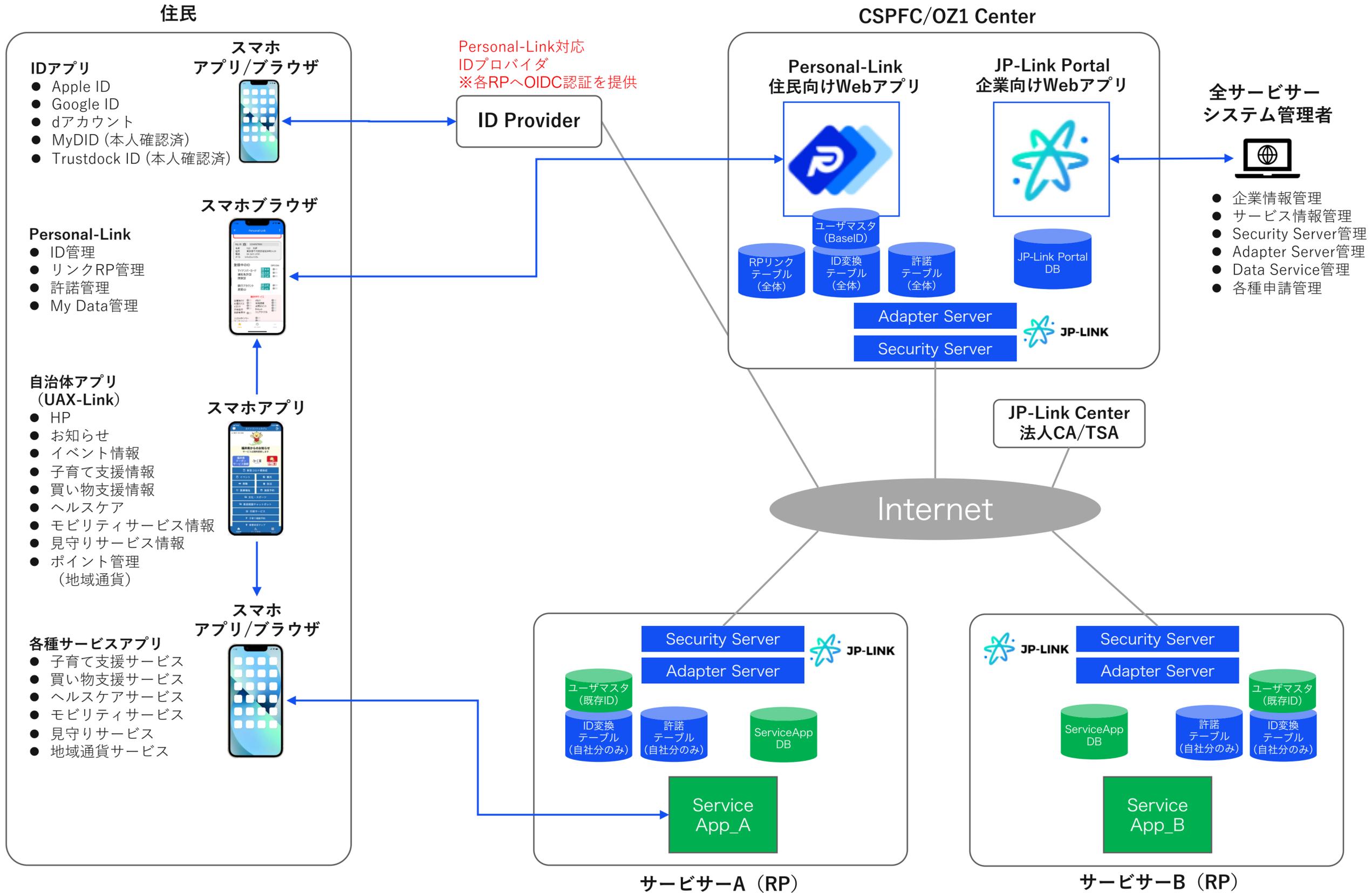
セキュリティサーバは、主に通信の暗号化と送信内容への電子署名及びタイムスタンプの付与を行います。またデータ連携する必要があるJP-LINKトラストネットワーク内にある他のメンバーのセキュリティサーバと直接Peer to Peer (P2P)で通信します。

- Service App実装概要**
サービサーBのデータサービスに対するリクエスト／レスポンスの処理を実装します。
- 自社Security Serverに対してサービサーBのデータサービスへのリクエストを送信実装
 - サービサーBからのレスポンス処理実装

- Adapter Server設定概要**
データサービスの作成を行います。
- 接続するRDBMSの設定
 - データサービスのカテゴリー (Sub System Code) の定義
 - データ操作API (Data Service) の名称の定義

- Security Server設定概要**
作成したデータサービスの設定と連携するサービサーの特定のアプリケーションに対するアクセス権の付与を行います。
- Adapter Serverで定義した情報の設定
 - アクセス権の付与

Personal-Link アーキテクチャ 及び 実装概要



住民

IDアプリ

- Apple ID
- Google ID
- dアカウント
- MyDID (本人確認済)
- Trustdock ID (本人確認済)

スマホアプリ/ブラウザ



スマホブラウザ



Personal-Link

- ID管理
- リンクRP管理
- 許諾管理
- My Data管理

自治体アプリ (UAX-Link)

- HP
- お知らせ
- イベント情報
- 子育て支援情報
- 買い物支援情報
- ヘルスケア
- モビリティサービス情報
- 見守りサービス情報
- ポイント管理 (地域通貨)

スマホアプリ



スマホアプリ/ブラウザ



各種サービスアプリ

- 子育て支援サービス
- 買い物支援サービス
- ヘルスケアサービス
- モビリティサービス
- 見守りサービス
- 地域通貨サービス

Personal-Link対応 IDプロバイダ ※各RPへOIDC認証を提供

ID Provider

許諾

CSPFC/OZ1 Center

Personal-Link 住民向けWebアプリ



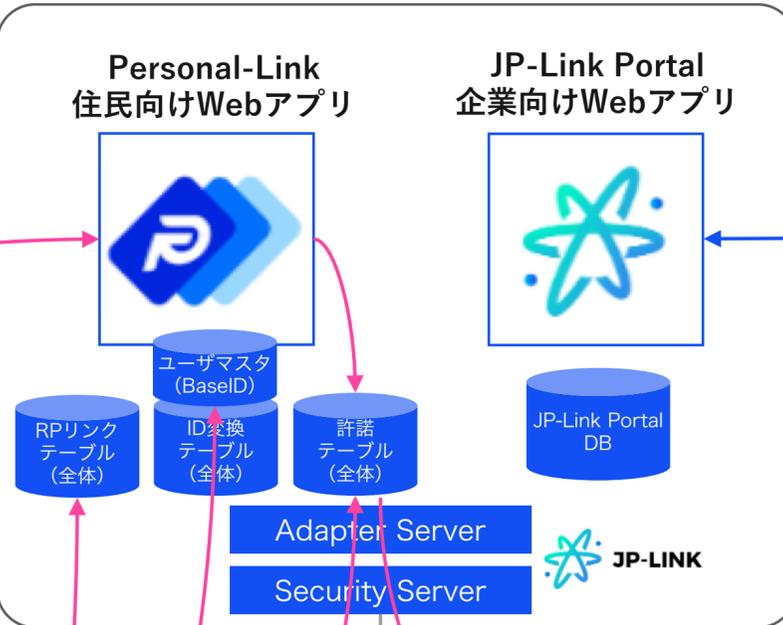
JP-Link Portal 企業向けWebアプリ



全サービスシステム管理者



- 企業情報管理
- サービス情報管理
- Security Server管理
- Adapter Server管理
- Data Service管理
- 各種申請管理



JP-Link Center 法人CA/TSA



Personal-Link対応ID実装 (サービスA/B共通)

- Personal-Link対応IDのリンク実装 (BaseID取得/ID変換テーブル実装含む)
- Personal-Link対応IDによるログイン実装
- Personal-Link対応IDによる新規登録実装

個人データ取得実装 (サービスA)

- ユーザへの許諾依頼実装
- サービスBへの個人データサービスリクエスト実装
- 上記レスポンス処理実装

サービスリンク 情報書込み

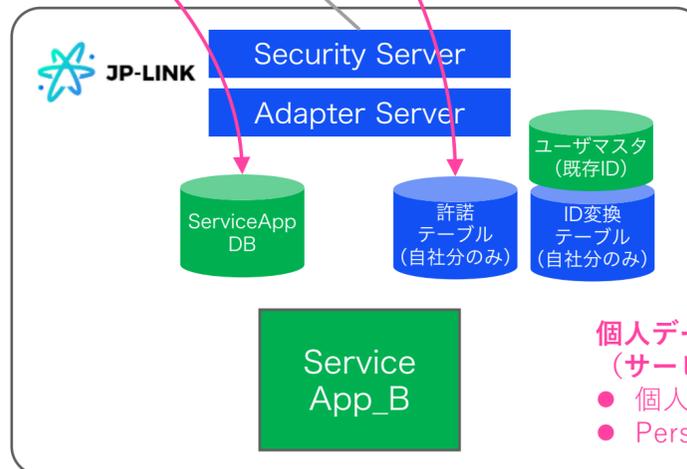
個人データ取得



サービスA (RP) 個人データ参照企業

許諾依頼

許諾情報反映



サービスB (RP) 個人データ提供企業

個人データ提供実装 (サービスB)

- 個人データ連携サービス作成/設定
- Personal-Linkからの許諾情報反映

JP-Link／Personal-Link 実装関連ドキュメント

JP-Link関連

- JP-Link_SecurityServer_Installation_Guide_v1.1(ja)
- JP-Link_SecurityServer_User_Guide_v1.1(ja) ※1
- JP-Link_AdapterServer_Installation_guide_v1.3(ja)
- JP-Link_AdapterServer_User_guide_v1.4(ja) ※1

Personal-Link関連 ※1

- 01_Personal-Link：許諾ベースのデータ連携プロセス概要☒1.3
- 02_Personal-Link：許諾ベースのデータ連携プロセス詳細（RP実装範囲フローチャート）v1.0
- 03_Personal-Link実装関連テーブル定義書v1.0
- 04_Personal-Link実装API仕様
 - API仕様_BaseID照会_v1.0
 - API仕様_ID完了通知_v1.0
 - API仕様_ID連携完了通知_v1.0
 - API仕様_UL-PL_ID変換TBL登録_v1.0
 - API仕様_UL-PL_ID連携管理TBL登録_v1.0
 - API仕様_UL-PL_ユーザーマスタTBL登録_v1.0
 - API仕様_許諾情報登録_v1.0

※1 落札後の企業とのNDA締結後に開示または一般社団法人コンパクトスマートシティプラットフォーム協議会参加企業に開示

※2 【IDプロバイダ関連】 Personal-Link対応IDプロバイダーのOIDC実装は、IDプロバイダーの仕様書を参照のこと

EoF