

JP-LINK勉強会（初級編）

“スマートシティをもっとシンプルに”
自治体が主導する行政DXへの挑戦

2021年12月9日

2022年1月24日

2023年1月16日

JP-Linkビジネス編 データ連携における市場

1



海外の事例（エストニア）

電子保険記録システム

全国の医療機関のICTシステムと接続。個人情報、医療記録、来院情報、病歴等を医師が閲覧できる。

電子画像管理システム

すべての病院とつながる、X線写真などのデータバンク。電子保険記録システムとも接続し、経年での観察など診察に活用。

電子予約システム登録

オンラインでの病院予約が可能。

電子処方箋システム

eIDカードを提示することで薬を受け取れる。

eKool

生徒の成績評価、指導内容、休校や宿題、試験結果などを、アプリケーションを通じて蓄積、先生、保護者、生徒の間で共有されるツール。



EHIS（エストニア教育情報システム）

教育機関、教職員、生徒に関するデータベース。卒業書類の有効性の確認や教育政策の決定にも活用。

SAIS(入学情報システム)

大学などへの入学願書の提出がオンラインで行える。他のデータベースや試験システムと接続され、過去の成績や試験結果などの証明が不要。

キャッシュレス

eIDカードのハンディキャップ、年齢等の情報に基づき、自動的に金額が引き落とされる。



E-Residency

海外にいながら法人登記ができ、エストニアの企業としてEU市場でのビジネス機会が得られる。



電子開議

オンラインによる開議。海外からの参加が可能。電子署名により投票。

投票

インターネットによる国政投票への参加。どこにいても選挙に参加が可能。

税金

ポータルサイトから電子署名を行うことで税金額を確定。申告から3日程度で還付金が振り込まれる。

警察

バトカー搭載のシステムから運転免許証、車両所有者、車両保険、武器登録などへのデータへアクセス。

住民登録

住民登録台帳が電子化され、居住届、出生届、証明書コピー申請が可能。

法人登記

オンラインによる法人登記申請、変更手続き。

出典：各種資料より内閣府作成

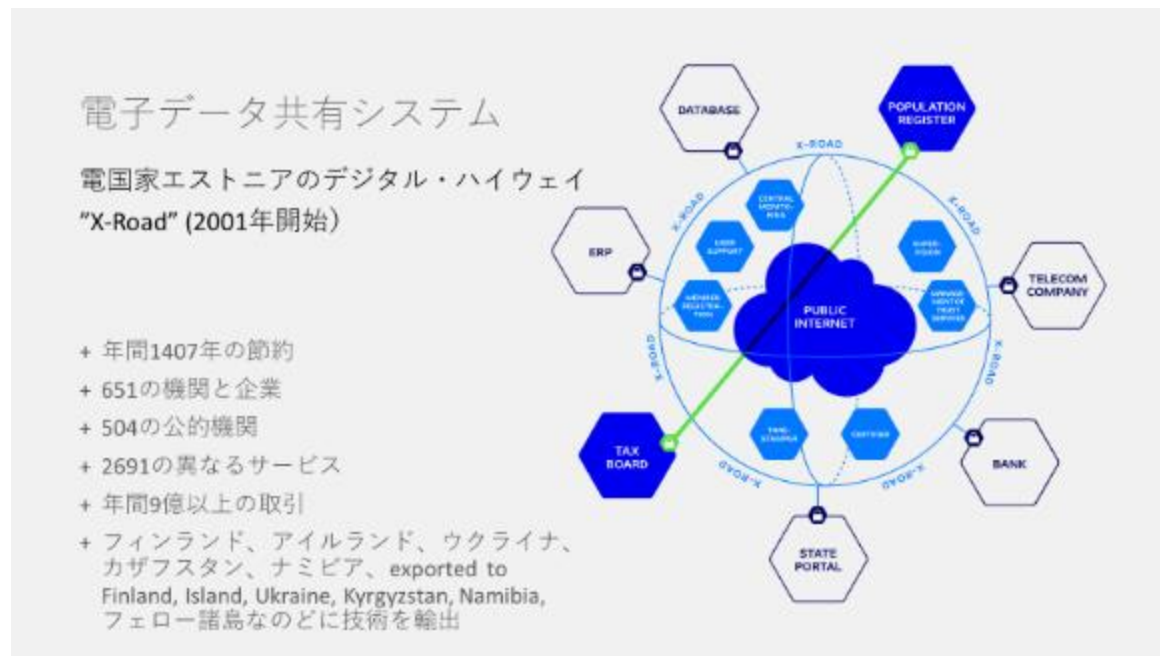
29

出展：内閣府「スーパーシティ」構想について

Confidential

エストニアで有名な2つのデジタルツール

オープンソースのデータ連携基盤 X-Road



利便性の高い国民ID



基本このままデジタルツールを日本にもってきても使えない

実際は、エストニアのデータ連携はX-Road + 国民IDだけではない
(日本では間違った認識も多い)

X-Roadを活用してデータトラフィック



ひと月あたりのX-Roadアクセス数
1.75億回/月（130万人の人口）

一人135回/月程度の利用

714 機関や企業
166 公共部門機関
CA 52000 間接的なX-ロードサービスの利用組織
1591 情報システムのインターフェース
178 メンバーによってインストールされたセキュリティサーバ

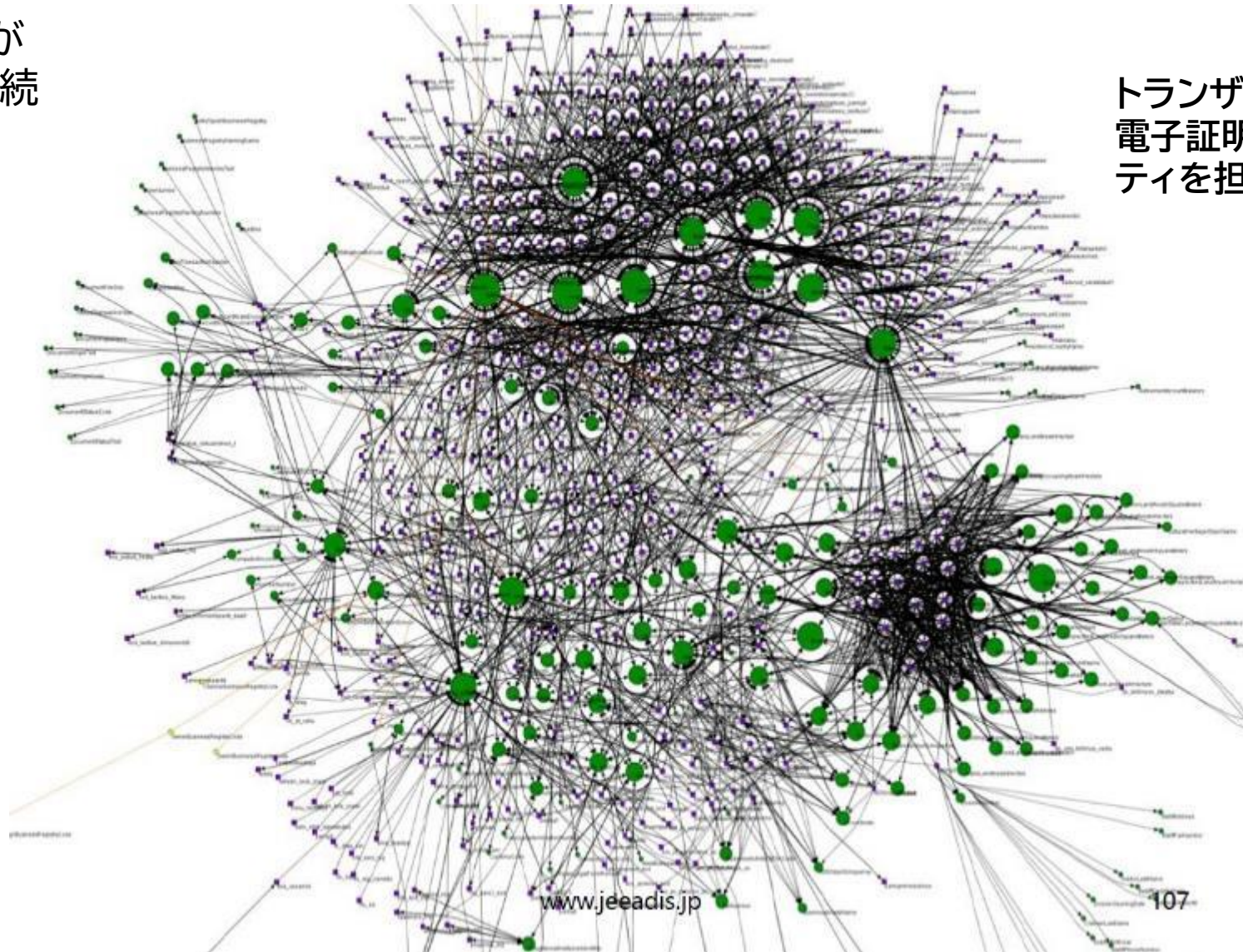
<https://www.x-tee.ee/factsheets/EE/#eng>

X-Roadをベースに各DBがつながる世界

各企業や行政のDBが
Peer to Peerで接続

サービス連携
データ連携

トランザクションごとに ログが残り、
電子証明書を活用してトレーサビ
リティを担保。



デジタル活用に関してはEU圏でTopクラスに

データ活用ができる環境だからこそ
ベンチャー企業の活動が活発
(大きくなるとエストニアから
EUやUSへお引越し。。。)

デジタルハリウッドやSkypeなど
エストニアからUSで活躍

日本が1.3億人で約7社のユニコーン
130万人の国でも約7社のユニコーン

(デジタルネイティブな若者と
データ活用の環境)

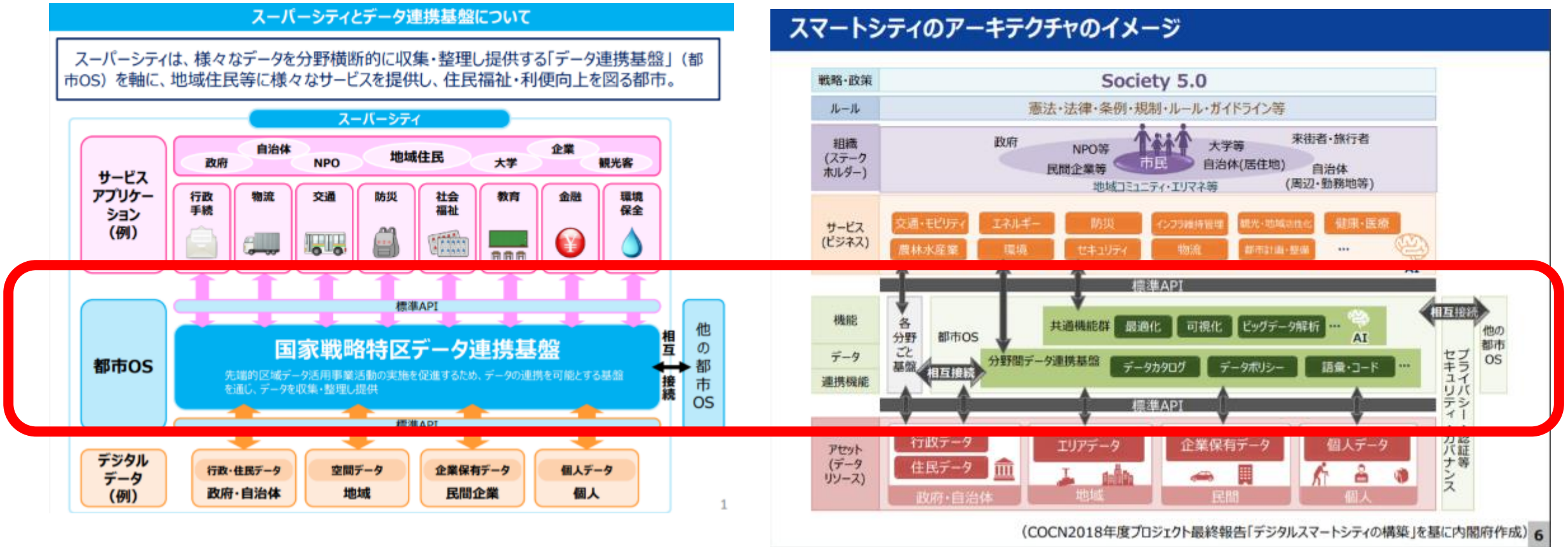
図表2：先進国内の起業活動指数順位とVC投資額の比較（欧州のみ抜粋）



注：TEA（Total Early-Stage Entrepreneurial Activity）指数＝総合起業活動指数は、起業活動の活発さを表す指標で、一定の基準を満たした起業家が、成人人口に占める割合。それを経済発展段階に応じて3分類し、先進国の中で順位化したものの中から、図表では欧州各国のみを抜粋。TEAに関して2017年値がない国は2016年値で代替
出所：「Global Entrepreneurship Monitor」、「Venture Capital in Europe & Israel」を基に三井物産戦略研究所作成

デジタル活用に関して日本は

日本では、海外の事例をもとにデータ連携や都市OSの活用を目指してスマートシティやスーパーシティに向けて重要な位置づけを行っています。



スーパーもスマートも都市OS上に構築されている

世界で使われている都市OSと呼ばれているもの

- SynchroniCity
- FIWARE
- X-Road
- IndiaStack
- IES-City

など他にも各国で取り組まれている

日本で利用されているのは
FIWARE/X-Roadだが都市OSの一部

日本も独自でデータ連携基盤を
作る会社もあるが・・・

表 7.1-4 海外スマートシティアーキテクチャの参考ポイント

アーキテクチャ	概要	参考ポイント	関連章
SynchroniCity ³⁵	スマートシティに関する欧州のIoTパイロットであり、現在20都市が参加した大規模な取組。	・都市OSの各機能群における構成要素とその定義 ・最小限相互運用メカニズム(Minimal Interoperability Mechanisms, MIMs)における、API、データモデルの考え方 ・認証系API、データマネジメント系API ・アーキテクチャ維持組織の機能	7.2 都市OSの機能説明 7.3 外部連携 9.1.1 アーキテクチャの維持発展を可能とする各種取組
FIWARE ³⁶	FI-PPPが次世代インターネット技術における欧州の競争力強化と、社会・公共分野のスマートアプリケーション開発を支援するために、開発した基盤ソフトウェア。	・都市OSの各機能群における構成要素とその定義 ・認証系API、データマネジメント系API	7.2 都市OSの機能説明 7.3 外部連携
X-Road ³⁷	エストニア政府が整備した安全なデータ交換のためのプラットフォーム。	・アーキテクチャ維持組織の機能	9.1.1 アーキテクチャの維持発展を可能とする各種取組
IndiaStack ³⁸	インド政府が生体認証技術を活用した個人を一意に識別する番号としてAadhaarを開発、Aadhaarを活用するデジタルインフラとしてのAPI群(e-KYC、e-Sign等)を含めた総称。	・個人に関する認証(個人認証)	7.2.2 認証
IES-City ³⁹	NIST(National Institute of Standards and Technology; 米国国立標準技術研究所)が主導して定めたコンセンサスフレームワーク。	・相互運用ポイントであるPivotal Points of Interoperability(PPI)の考え方	7.3 外部連携

世界で言われる都市OS：X-Road型とFIWARE型の得意分野

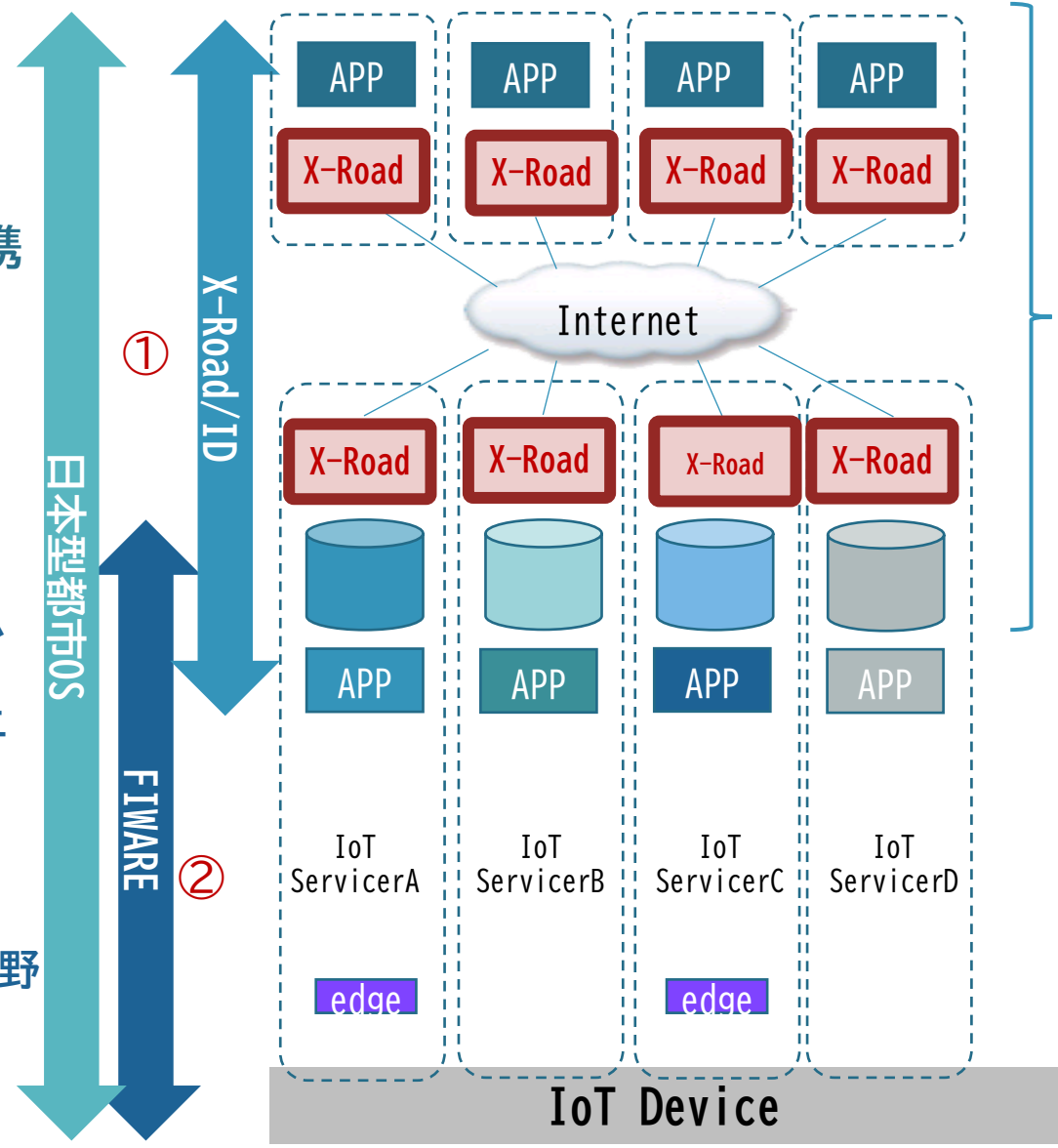
X-Road/IDの領域

- 法人間/個人間のデータ連携
- 監査証跡の確保
- 個人の許諾ベースの情報活用

FIWAREの領域

- IoTサービスプラットフォーム
- IoT領域の標準化からStart
- IoTシステム開発の生産性向上
- IoT Systemの相互運用性
- データ収集・蓄積・仲介
Context Broker

データモデルをターゲットした分野
向けに準備



- X-Roadは組織データやデータベースをPtoPで共有する基盤
- オープンソースで汎用性が高く住民サービスを構築する際に使われる手法

- FIWAREはIoTのためのデータ共有の基盤
- 柔軟性の高いデータモデルで統合管理が可能

データの流通を可能にするために、標準的なデータモデルと、オープンな共通APIを準備

各モジュールを組み合わせて開発が可能

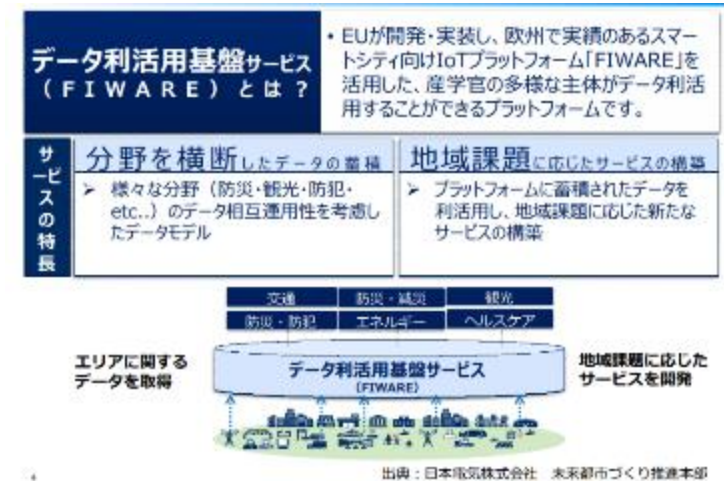
用途によるデータ連携基盤のサービス例



住民サービス
X-Road

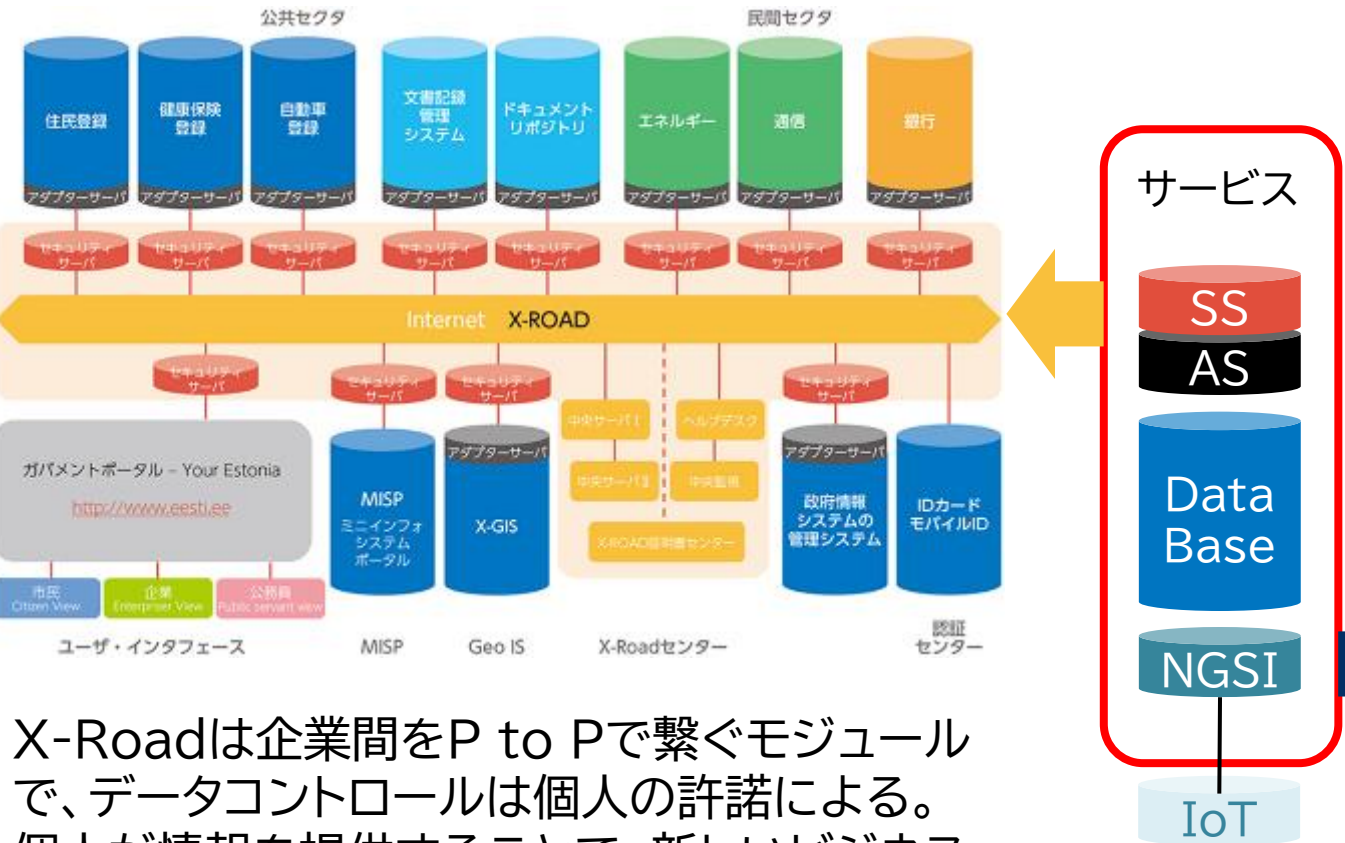
利用目的が違うので
共存を検討

都市開発
FIWARE



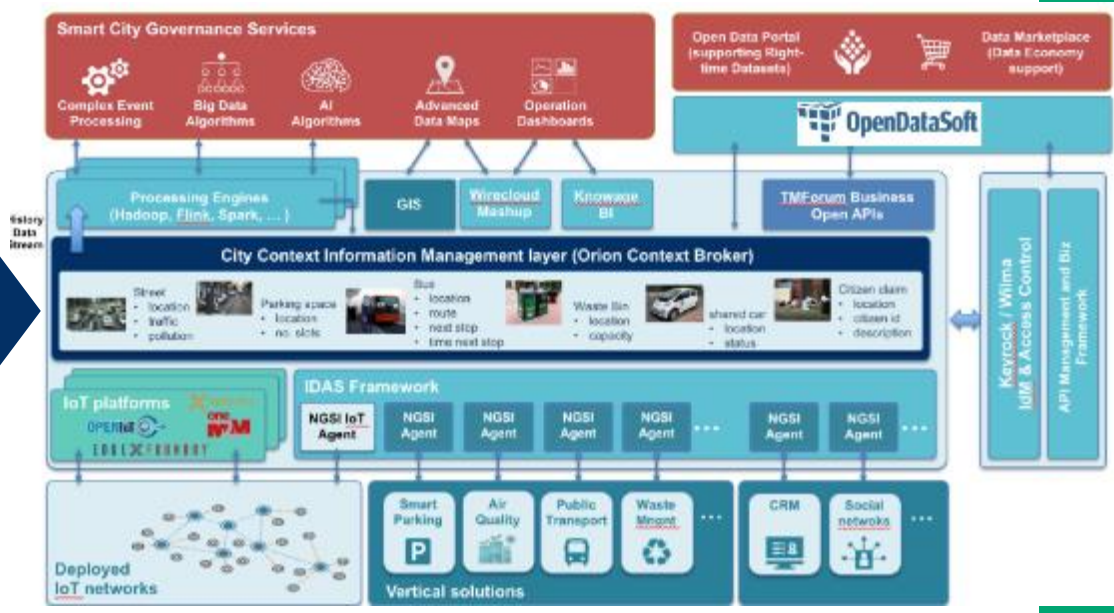
混在するデータ連携基盤は共存できる可能性を模索@CSPFC

サービス上で、複数のデータ連携基盤は共存可能(CPU/メモリの物理リソースは掛かります。)
何を介してデータを連携させるかはサービスの状況次第



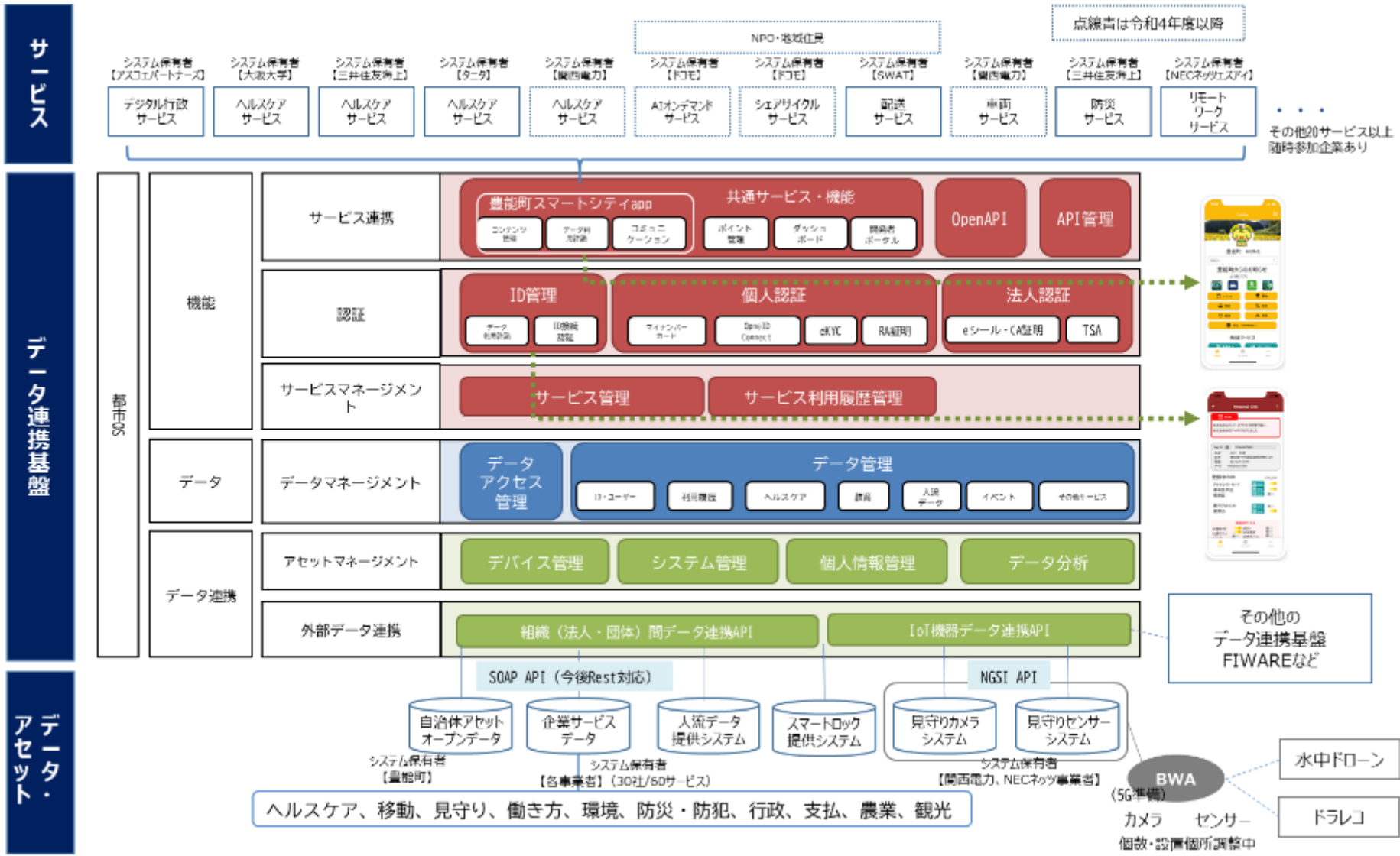
X-Roadは企業間をP to Pで繋ぐモジュールで、データコントロールは個人の許諾による。個人が情報を提供することで、新しいビジネス策定

FIWAREはContext Broker(データ仲介)が入りデータコントロールを行う。誰が管理するかを考えて、運用を行う形式が取れる。Context Broker中心に新しいビジネス策定が可能。



CSPFのデータ連携基盤を都市OS的に表現

難しすぎるので、とりあえず都市OSとして使える！という感じです。



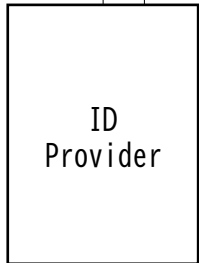
CSPFのデータ連携基盤をもう少し柔軟に

利用規約に同意して
dアカウントでログイン

ドコモより
dアカウント連携
8000万人ユーザー



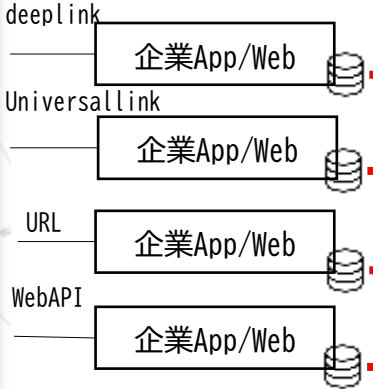
IDをお持ちでない場合
IDプロバイダーで
ID作成



TRSTDOCK社
ドコモ
DP社等

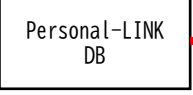
IDをお持ちの場合
ログイン
=ID認証(OIDC)

IDをお持ちの場合
ログインデータはJP-Linkで共有

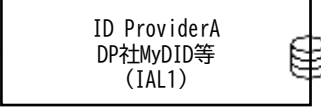


各自治体向けUAX-Linkには基本的なAPIで接続

マスターID (ID利用不可: 割振りナンバー)
・IDリスト (変換テーブル)
・JP-Link設定ファイル



OpenID Connect
OpenID Connect



JP-Linkでデータ連携

データ連携・共有
はJP-LINKで、必要
とする企業(RP)間
でのみと連携

企業(RP)と
Persona-LINK間では
必要なテーブル
を共有・連携

ID Providerとは、OIDCでの
認証・やり取り以外のデー
タを連携する必要がある場
合のみJP-LINK利用

マルチID エストニア ID認証の事例（行政機関）

日本ではエストニアやシンガポールなど国民IDのみで、サービスができると考えている方が多いが実際は色々なIDを活用してログインするマルチオーセンティフィケーションが主流。

国民ポータルログイン画面

Secure authentication for e-services EESTI РУССКИЙ

Riigi Autentimisteenus

ID-card Mobile-ID Bank link EU citizen

Bank link ※銀行のIDでもログイン可能

You need to be a client of supported bank to log in. To enter the portal using a bank link, select your bank. You will be redirected to your bank's authentication service.

Swedbank SEB LHV Luminor coop | Park

※他EU国の国民IDでもログイン可能
For European Union citizen

Requires a valid eID of one of the supported countries. Select your country. You will be redirected to your country's identity provider for authentication.

Select your country

- Belgium
- Germany
- Italy
- Luxembourg
- Spain

[Return to service provider](#)

e-Tax ログイン画面

Private client Business client Contacts and about us Accessibility Help Enter e-MTA

Republika EESTI Riigi Teenused In English

Income, expenses, supply, profit Excise duties, assets, gambling Customs, trade in goods Registration, business Taxation, payment of taxes

Business client's main page

03.09.2019 ETCB launches updated e-MTA self-service system
Estonian Tax and Customs Board (ETCB) e-services are now available at the e-MTA environment that has an improved UI/UX withdrawal from ETCB

Current topics
Upgraded desktop of e-MTA environment
UK's withdrawal from EU

Select a method for signing in

- ID-card
- Mobile-ID
- Smart-ID
- Internet bank
- eIDAS

For authentication with Smart-ID, please enter your personal identification code. Afterwards, follow the instructions on the screen. You will receive a confirmation code by SMS or email. Click "Sign in".

Country

Legend:

- 政府発行の国民ID
- Smart-ID:民間発行のユニバーサルID
- 銀行のID
- 他EU国の国民ID

Sign in

REPUBLIC OF ESTONIA TAX AND CUSTOMS BOARD

Customer support
880 0814 e-customs services
880 0815 e-tax services
[All contact data, etc.](#)

マルチID エストニア ID認証の事例（民間企業）

統合IDはSingle Sign On(SSO)と同様の発想だがSSOはユーザー側の利便性は上がるが、サービス提供者側への負担が大きい。結果多くの国は国民IDを主とするものの、マルチログインを採用している。（本人確認済みIDの活用方法を組み立てる方が、ID統合よりも大切）

銀行 ログイン画面

通信会社 ログイン画面

マルチオーセンティフィケーション

The collage displays login interfaces from Swedbank, SEB, LHV, and other providers. A central legend identifies the authentication methods:

- 政府発行の国民ID (Government-issued national ID)
- Smart-ID:民間発行のユニバーサルID (Smart-ID: Private universal ID)
- 銀行のID (Bank ID)
- 独自ID (Unique ID)

改めてサービス・データ連携を考えてみる



全てが繋がり、シームレスで効率よく安全に住民サービスが提供される世界

調剤

病院

救急

免許

家族

改めてサービス・データ連携を考えてみる(採択前総務省へ提案)

■ 活用するデータとサービス【データ・サービス相関表】

各サービスは分野毎に以下に整理しました。今期はまず各社が他社のデータをどのように活用できるのかを検討し令和4年度以降にサービスを利用者に対してシームレスにつなげるかを進めます。自治体はデータ連携基盤、ID管理(個人情報管理)、住民向けインターフェースが無償で提供され、行いたいサービス(以下)から有償・無償を確認しながら、サービスパッケージを構築する事ができます。(サービスは随時追加されていきます)

サービス		分野	都市OS	データ	分野	区分	ストア先(管理者)	住民	自治体
住民サービス統合アプリ(豊能スマートシティapp) 高齢者・子供見守りサービスの提供	豊能町推奨のサービスや豊能町配信サービスを統合するサービス	⑯その他	JP-Link	サービス利用履歴	⑯その他	③パーソナルデータ(匿名加工情報等) D 利用履歴	OZ1	無料	無料
	見守りカメラ、ビーコン/スマホ活用した位置情報	②セキュリティ・見守り	Symphonict	映像、センサー、位置情報、時間	②セキュリティ・見守り	③パーソナルデータ(匿名加工情報等) A センシングデータ	NECネットエスアイ	未定	有償
	OTTADE!(BLE)による位置情報	②セキュリティ・見守り		センサー、位置情報、時間	②セキュリティ・見守り	④非パーソナルデータ A センシングデータ	関西電力	無償	有償
	スマートロック利用による位置情報	②セキュリティ・見守り	JP-Link	開閉データ	②セキュリティ・見守り	④非パーソナルデータ A センシングデータ	Bitkey	有償	無償
	救急タグによる健康状態見守りサービス	②セキュリティ・見守り	JP-Link	既往歴、治療中、アレルギー、投薬、障害、術歴、介護認定、認知症、血液型	②セキュリティ・見守り	③パーソナルデータ(匿名加工情報等) D 医療データ	豊能町	無償	有償
	ウェアラブルによる健康状態見守りサービス	⑧健康・医療	Symphonict	BLE位置情報	⑧健康・医療	④非パーソナルデータ D センシングデータ	(未定:NECネットエスアイ)	無償	無償
	郵便局員・銀行員による巡回見守りサービス	②セキュリティ・見守り		—	②セキュリティ・見守り	②パーソナルデータ(個人情報) D アンケート	日本郵政/池田泉州銀行	有償	無償
高齢者及び希望住民ヘルスケアサービスの提供	ココカラダイアリーによる生活習慣見守り	⑧健康・医療	調整中	運動・食事・睡眠	⑧健康・医療	③パーソナルデータ(匿名加工情報等) D センシングデータ	三井住友海上	無償	無償
	豊能町住民の国保健診データのAI分析/生活習慣病発症予測システム	⑧健康・医療	JP-Link	健康診断データ、ウェアラブル端末データ	⑧健康・医療	③パーソナルデータ(匿名加工情報等) D 医療データ	大阪大学	有償	有償
	スマホ活動量計測サービス	⑧健康・医療	JP-Link	活動量	⑧健康・医療	③パーソナルデータ(匿名加工情報等) A センシングデータ	OZ1	無償	無償
	体重計・血圧計・活動量計などで健康見守りサービス	⑧健康・医療	JP-Link	身体、活動量	⑧健康・医療	③パーソナルデータ(匿名加工情報等) A センシングデータ	タニタ	無償	有償
	住民定期健康診断	⑧健康・医療	(JP-Link)	匿名化国保健診	⑧健康・医療	③パーソナルデータ(匿名加工情報等) D 医療データ	豊能町	—	—
	リビングラボ・公民館への施設サービス	⑫行政	(JP-Link)	施設利用	⑫行政	④非パーソナルデータ D 利用者履歴	豊能町	無償	無償
	ヘルスケアパスポート(医療履歴管理)	⑧健康・医療	(JP-Link)	医療データ	⑧健康・医療	②パーソナルデータ(個人情報) D 医療データ	TIS	無償	有償
	遠隔問診	⑧健康・医療	(JP-Link)	医療データ	⑧健康・医療	②パーソナルデータ(個人情報) D 医療データ	各病院	—	—
	就学生を中心とした子供をカメラ、センサーを利用して位置情報を計測	②セキュリティ・見守り	Symphonict	カメラ、センサー	②セキュリティ・見守り	③パーソナルデータ(匿名加工情報等) A センシングデータ	NECネットエスアイ	無償	有償
子育てしやすい環境整備サービス提供	子育てシェアサービス(子守代行サービス)	②セキュリティ・見守り	JP-Link	サービス利用者	②セキュリティ・見守り	③パーソナルデータ(匿名加工情報等) D 登録者情報	AsMama	無償	無償
	子育て支援サービスのプッシュ・レコメンデーション	⑫行政	JP-Link	豊能町行政サービス	⑫行政	②パーソナルデータ(個人情報) D 行政申請データ	アスコエパートナーズ	無償	有償
	スマートロックを活用した共働き家庭の買い物・家事代行支援サービス	②セキュリティ・見守り	JP-Link	開閉データ	②セキュリティ・見守り	④非パーソナルデータ A センシングデータ	Bitkey	有償	無償
	子育て保育サービス	②セキュリティ・見守り	JP-Link	担当者スケジュールデータ	②セキュリティ・見守り	②パーソナルデータ(個人情報) D 登録者情報	地元企業(NPO)	無償	有償

改めてサービス・データ連携を考えてみる

買い物困難者支援サービス	買い物困難者など向けキッチンカー・移動販売カーの配備	⑤観光・地域活性化	JP-Link	位置、時間、サービススケジュール	⑤観光・地域活性化	④非パーソナルデータ A センシングデータ	三井住友海上	有償	無償
	地元農家などからの野菜提供	⑤観光・地域活性化	JP-Link	野菜売買、位置情報	⑤観光・地域活性化	④非パーソナルデータ B 購買情報	YACYBER	無償	無償
	買い物困難者への買い物代行	⑤観光・地域活性化	JP-Link	サービス利用者	⑤観光・地域活性化	②パーソナルデータ(個人情報) D 登録者情報	CaSY	有償	無償
	地域通貨による決済サービス	⑬支払い	JP-Link	購買履歴	⑬支払い	④非パーソナルデータ B 購買情報	フィノバレー/ (Digital Platform)	無償	有償
	地元スーパーなどによる商品供給	⑦物流	(JP-Link)	商品	⑦物流	④非パーソナルデータ B 購買情報	地元商店	有償	無償
インターネット・旅行による間接住民を増やすサービスの提供	旅行希望の若者と地元農家や企業でのお仕事/宿泊のマッチングサービス	⑤観光・地域活性化	JP-Link	サービス利用者	⑤観光・地域活性化	②パーソナルデータ(個人情報) D 登録者情報	おてつだび	無償	無償
	AIオンデマンド交通による町内移動支援サービス	⑥交通・モビリティ	JP-Link		⑥交通・モビリティ	④非パーソナルデータ A センシングデータ	Docomo / SWAT	有償	有償
	デジタル通貨による町内サービス決済	⑬支払い	JP-Link		⑬支払い	④非パーソナルデータ B 購買情報	フィノバレー/ (Digital Platform)	無償	有償
	農家や林業者など仕事の確保と宿泊場所の調整	⑤観光・地域活性化	JP-Link	職業データ・宿泊地情報	⑤観光・地域活性化	②パーソナルデータ(個人情報) D 登録者情報	豊能町	無償	無償
地域通貨による地域経済の活性化サービス	地域通貨をベースに移動、買い物などの支払い、健康増進などのポイントに利用	⑬支払い	JP-Link	購買、サービス利用者	⑬支払い	④非パーソナルデータ B 購買情報	フィノバレー/ (Digital Platform)	無償	有償
AIオンデマンド交通による住民移動手段サービスの提供	豊能スマートシティapp及び現状の1次交通などのデータを分析し最適な車両配備	⑥交通・モビリティ	JP-Link	地図、経路	⑥交通・モビリティ	④非パーソナルデータ C 地理空間データ	SWAT	—	有償
	豊能スマートシティappの利用履歴・(予約履歴)を含めて行動分析	⑥交通・モビリティ	JP-Link	利用履歴	⑥交通・モビリティ	④非パーソナルデータ D 利用履歴	OZ1	—	無償
	AIオンデマンドバスで利用者を目的地に効率良く配送・利用者のデータ管理	⑥交通・モビリティ	JP-Link	地理空間データ・利用履歴	⑥交通・モビリティ	④非パーソナルデータ C 地理空間データ	Docomo / SWAT	—	
	電動自転車利用者のデータ管理	⑥交通・モビリティ	調整中	利用者履歴	⑥交通・モビリティ	③パーソナルデータ(匿名加工情報等) D 利用者履歴	Docomo ShareBike	—	有償
	dポイント利用者の移動・行動履歴を可視化し都市計画に利用	⑥交通・モビリティ	—	利用者履歴	⑥交通・モビリティ	③パーソナルデータ(匿名加工情報等) D 利用者履歴	Docomo Datawise	—	有償
	EV車などの利用履歴管理	⑥交通・モビリティ	調整中	利用者履歴	⑥交通・モビリティ	④非パーソナルデータ D 利用者履歴	関西電力	—	有償
	自動運転EV車	⑥交通・モビリティ		センシングデータ	⑥交通・モビリティ	④非パーソナルデータ A センシングデータ	Docomo/ZMP	—	有償
	運転手サービス(空いている運転手のマッチング)	⑥交通・モビリティ	(JP-Link)	登録者情報	⑥交通・モビリティ	③パーソナルデータ(匿名加工情報等) D 登録者情報	地元NPO/阪急バスなど	無償	無償
	町の状況供給バランスの計画作成	—	—	—	—		テクノガウス	—	有償
	太陽光発電による電力需給予測	⑩環境・エネルギー	JP-Link	設備配置、発電量	⑩環境・エネルギー	④非パーソナルデータ A センシングデータ	エコスタイル	—	有償
カーボンニュートラルに向けた豊能町の環境整備	EV車など給電	⑩環境・エネルギー	JP-Link	設備配置、利用履歴	⑩環境・エネルギー	④非パーソナルデータ A センシングデータ	エネゲート	—	有償
	Google EIE活用により二酸化炭素排出量・太陽光発電によるエネルギー換算のシュミレーション	⑩環境・エネルギー	—	地図、CO2排出量シュミレーション	⑩環境・エネルギー	④非パーソナルデータ C 地理空間データ	Google	—	無償
	デジタル行政窓口サービス	⑫行政	JP-Link	行政窓口サービス	⑫行政	②パーソナルデータ(個人情報) D 申請者情報	アスコエパートナーズ	無償	有償
	AI弁護士による住民のお悩み相談	⑫行政	JP-Link	住民相談	⑫行政	②パーソナルデータ(個人情報) D 利用者履歴	ロボットコンサルティング	無償	無償

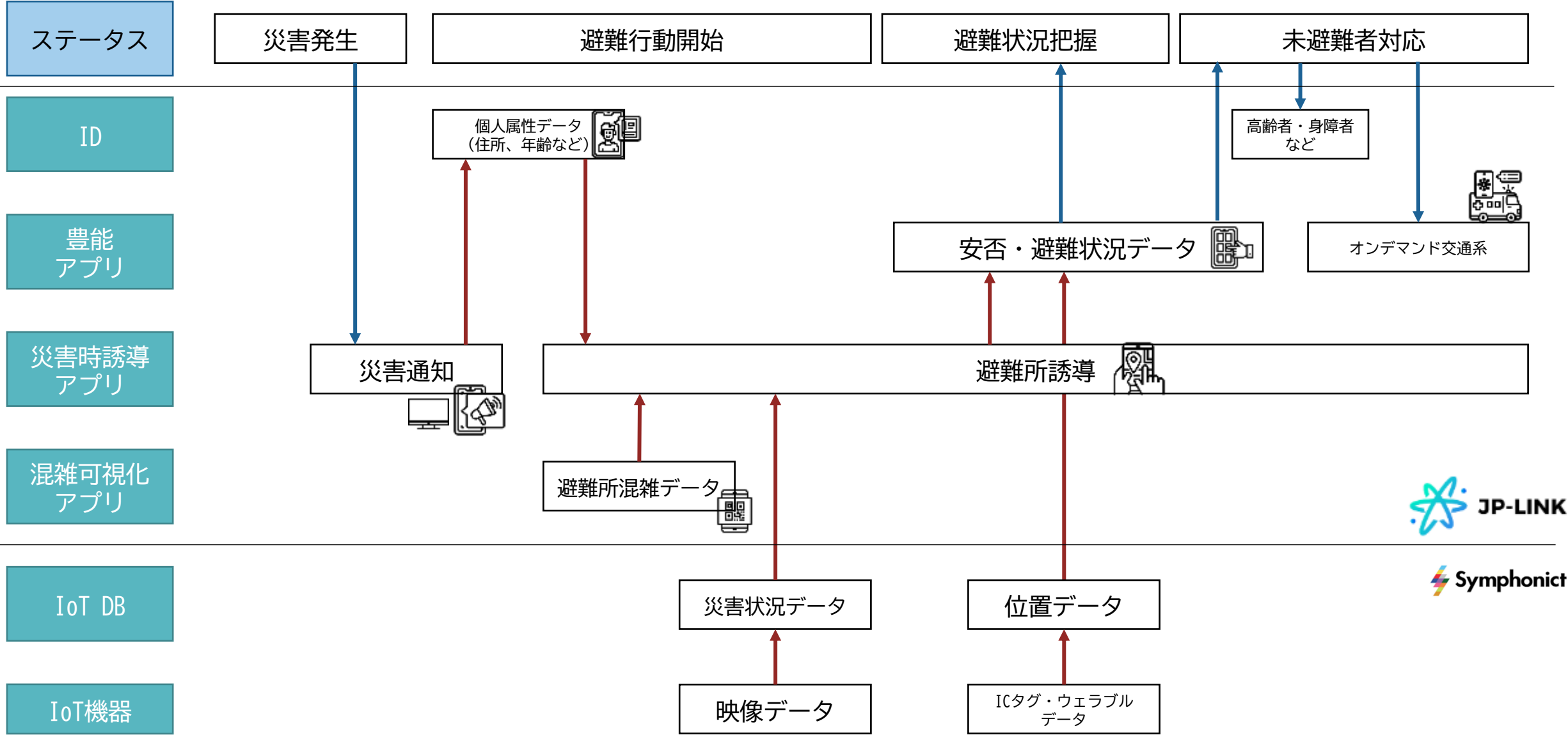
改めてサービス・データ連携を考えてみる

災害時避難支援による環境整備	避難時に避難所への誘導を行うサービス	①防災	JP-Link	地図、経路、避難所	①防災	④非パーソナルデータ C 地理空間データ	三井住友海上	無償	無償
	避難所の混雑状況の可視化サービス	①防災	JP-Link	人口密度、避難所	①防災	④非パーソナルデータ C 地理空間データ	VACAN	無償	無償
	AIオンデマンドバスなどによる被災者救済サービス	⑥交通・モビリティ	JP-Link	地理空間データ・利用履歴	⑥交通・モビリティ	③パーソナルデータ(匿名加工情報等) A センシングデータ	Docomo / SWAT	未定	未定
	ウェアラブルによる被災者の位置情報把握サービス	②セキュリティ・見守り	Symphonict	被災者位置情報	②セキュリティ・見守り	③パーソナルデータ(匿名加工情報等) A センシングデータ	(未定:NECネットエスアイ)	無償	無償
	見守りカメラによる被災状況把握サービス	②セキュリティ・見守り	Symphonict	映像、センサー、位置情報、時間	②セキュリティ・見守り	④非パーソナルデータ A センシングデータ	(未定:NECネットエスアイ)	無償	有償
デジタルインフラによるIT弱者の解消環境整備		⑩環境・エネルギー	Symphonict	設備配置、サービス利用者	⑩環境・エネルギー	④非パーソナルデータ A センシングデータ	NECネットエスアイ	—	—
	デジタルデバйд教育	⑪教育		施設利用	⑪教育	③パーソナルデータ(匿名加工情報等) D 登録者情報	Code for Osaka/Docomo/OZ1	無償	有償
	NoCodeによるアプリケーション開発(プログラミング教育)	⑪教育		施設利用	⑪教育	③パーソナルデータ(匿名加工情報等) D 登録者情報	OZ1/NoCodeJapan	無償	有償
都市環境整備	ドラレコを活用した舗装道路の修繕箇所の計測	③インフラ維持管理		映像、センサー、位置情報、時間	③インフラ維持管理	④非パーソナルデータ A センシングデータ	関西電力	—	有償
	ドラレコ、ドローンによる建物・道路の劣化状態をAI分析	③インフラ維持管理		映像、センサー、位置情報、時間	③インフラ維持管理	④非パーソナルデータ A センシングデータ	三井住友海上	—	有償
	水中ドローンによる放流渠内部点検	③インフラ維持管理		映像、センサー、位置情報、時間	③インフラ維持管理	④非パーソナルデータ A センシングデータ	NECネットエスアイ	—	有償
デジタル教育による就学生のIT活用人材の育成	デジタル教科書の提供	⑪教育		教科書利用		③パーソナルデータ(匿名加工情報等) D 利用者履歴	Libry	無償	有償
	Learning Mangement systemによる就学度の管理	⑪教育		教育関連相互		③パーソナルデータ(個人情報) D 利用者履歴	eKool	無償	有償
	デジタルコンテンツ配信サービスの提供	⑪教育		サービス利用者		④非パーソナルデータ D 利用者履歴	EduTech	無償	有償
		⑪教育		利用者履歴		③パーソナルデータ(匿名加工情報等) D 利用者履歴	スクールエージェント	—	有償
		⑪教育		利用者履歴		④非パーソナルデータ D 利用者履歴	iTeachers	無償	無償
	NoCodeによるアプリケーション開発(プログラミング教育)	⑪教育		利用者履歴		④非パーソナルデータ D 利用者履歴	NoCodeJapan	無償	有償

令和4年度以降または本予算外

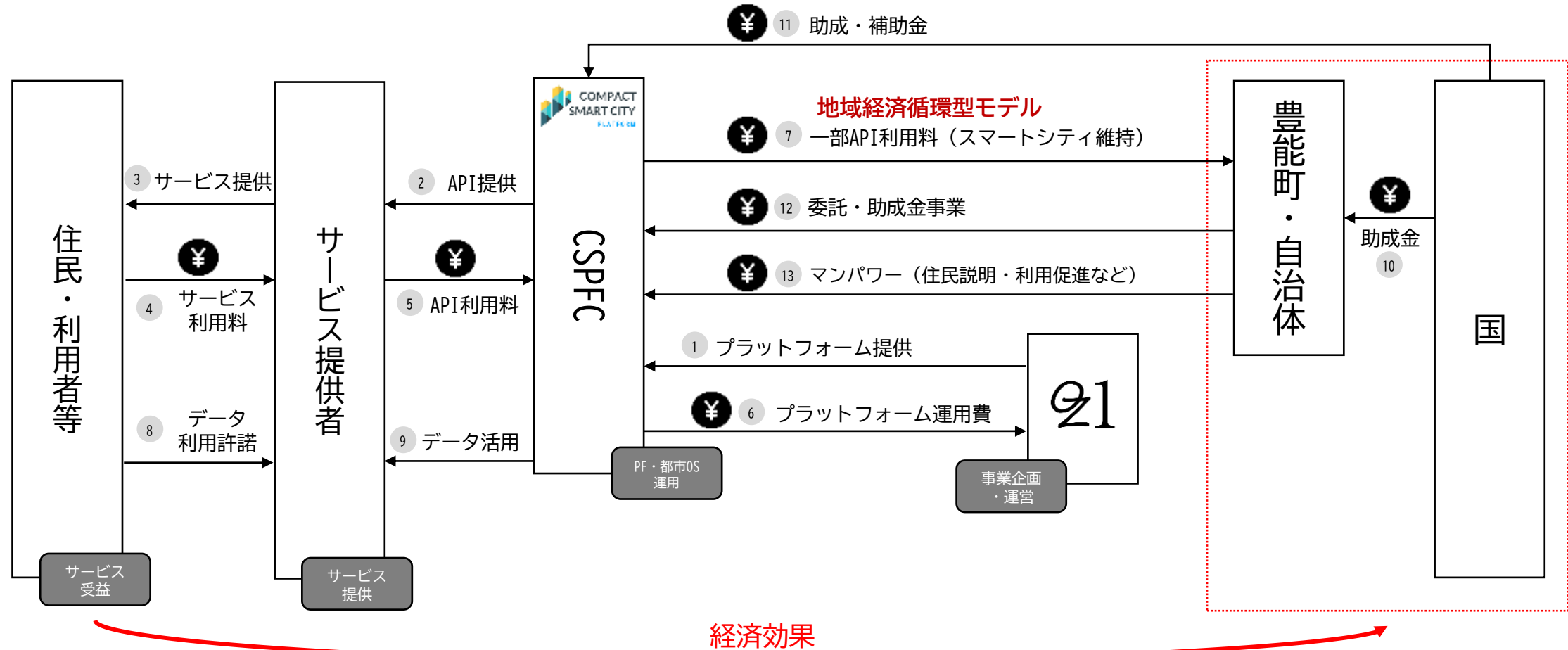
改めて、サービス連携を考えてみましょう

改めてサービス・データ連携を考えてみる(災害対策での例)



デジタルの地産地消ビジネスモデル（スマートシティで広がる格差是正）

スマートシティを支援するIT企業の8割は東京本社で、スマートシティが広がると東京都が潤う仕組みを是正が必要。地域経済循環率とスマートシティの維持



デジタルの地産地消ビジネスモデル(企業負担も軽減)

- CSPFCはでJP-Linkを無償配布します
- API利用料金的に、アクセスログに対して10円を課金します
無償化も出来るが、自治体に還元するため課金します
自治体およびアカデミックは無償で利用が可能です
- 10円課金
アクセスログに対して月額10円で一旦検討します
みなさんが1回300円で住民サービスをして10円
300円を10回使ってもらっても10円
*自治体スマートシティ維持コストの状況に合わせて、金額変更する可能性は有ります。

企業負担を軽減し、サービス提供自治体の収益につながるモデル



JP-Linkテクニカル編 JP-Linkを使うには（基礎）

Security ServerとAdapter Serverの技術サポート問い合わせ先：
OZ1 (techoz1@oz1.life)

Confidential

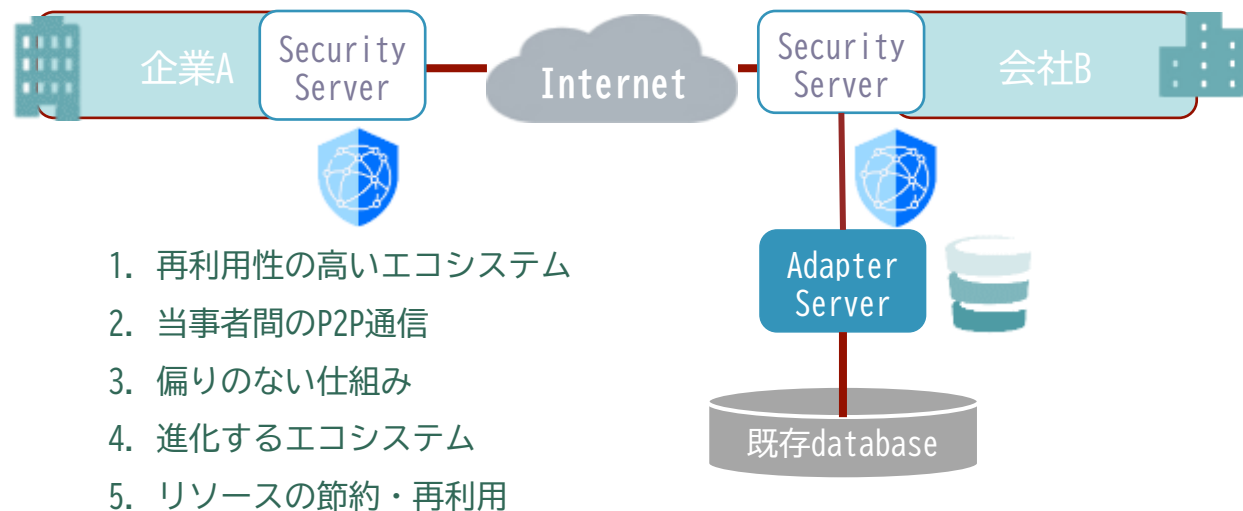
JP-LINKの特長

JP-LINKとは

JP-Linkは、インターネットを利用したセキュアな
法人間データ連携プラットフォームです

P2Pで通信を行う**分散アーキテクチャー**な所のセンターです
すべてのデータを保存することを行いませんの情報連携基盤です

PKI等の標準技術を用いてセキュアかつスケーラビリティを
実現しています



JP-LINKの強み

どんな会社でも規模
を問わず接続可能

- ・モジュール導入企業同士であれば、設備を追加せずにデータ連携が可能

VPN・専用線不要

- ・インターネットを利用したデータ連携
- ・証明書を使用した強度の高い暗号化通信

通信の改ざん・
なりすまし防止

- ・法人用の電子証明書を使用した電子署名
- ・タイムスタンプによる通信時間の証明

既存システムの制約なく
そのまま導入可能

- ・マルチプラットフォーム対応
- ・マルチDBMS対応
- ・マルチベンダー対応

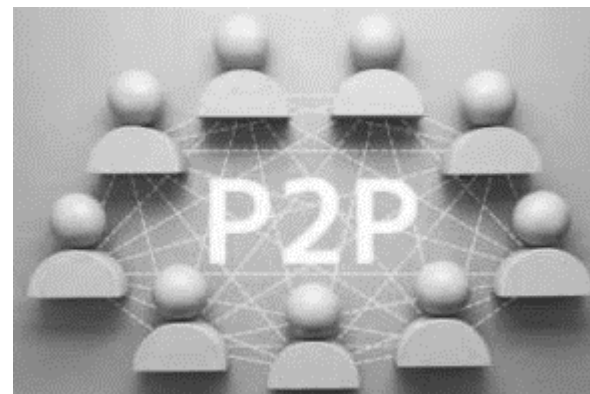
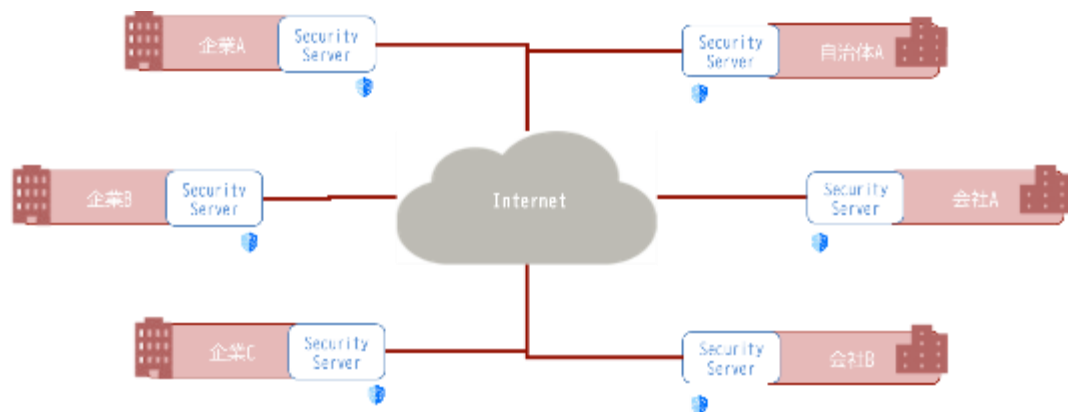
***PKI:「Public Key Infrastructure」**の略で、公開鍵暗号技術と電子署名を使って、インターネット上で安全な通信ができるようにするための環境のことを言います。
この公開鍵・秘密鍵は認証局が本人確認の上、電子証明書とともに発行するものです。

当事者間のP2P通信

通信が必要な相手に必要な検索を許可する仕組み

Peer to Peer (P2P) :

複数のコンピューター間で通信を行う際のアーキテクチャのひとつで、対等の者（Peer、ピア）同士が通信をすることを特徴とする通信方式、通信モデル、あるいは通信技術の一分野を指す



P2Pメリット

高スケーラビリティ
低コスト
耐障害性の高さ

P2Pデメリット

実装の困難さ
動作確認の困難さ
セキュリティ制御の困難さ
削除制御の困難さ
通信相手特定の困難性

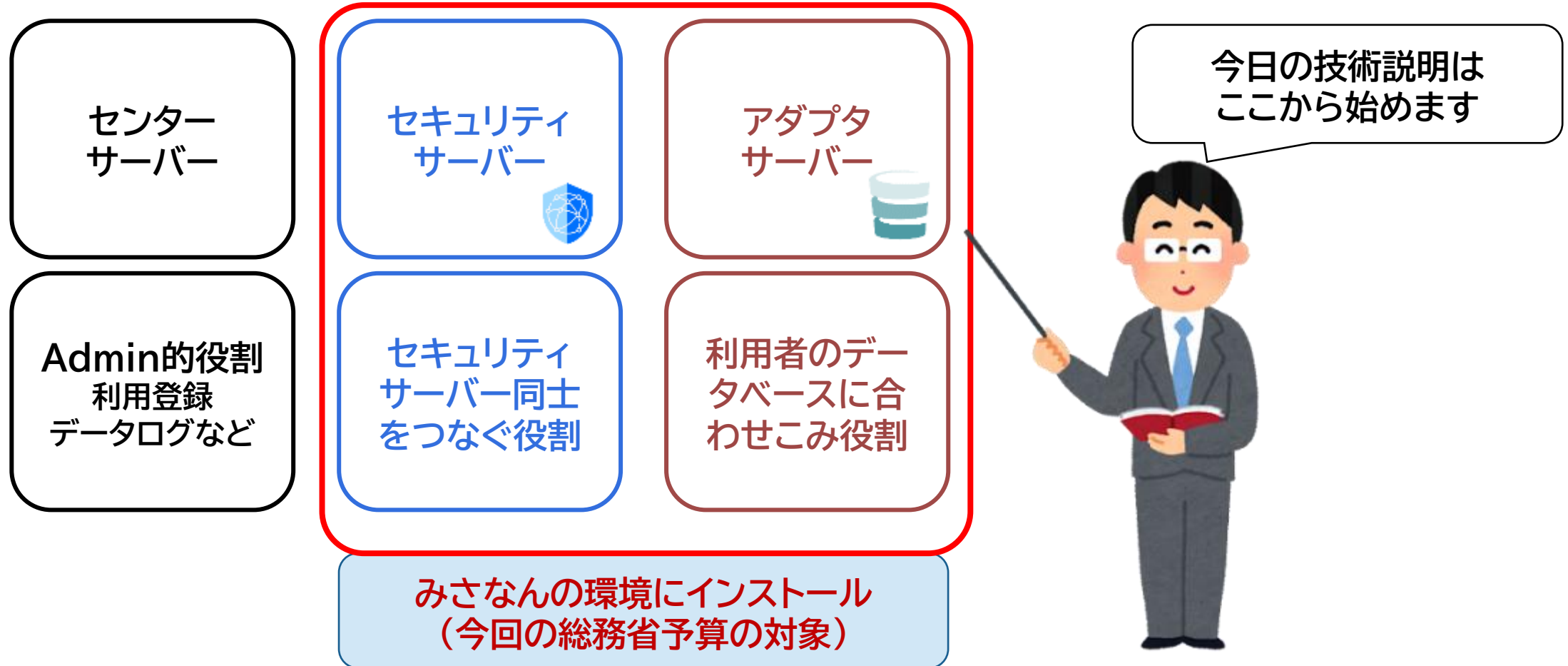


JP-LINK はデメリットを解消した、P2Pネットワークを提供します
中央で一極集中してデータを集めるデータベースは作りません

そもそもJP-LINKって？

JP-LINKはX-Roadをベースにした日本向け仕様にカスタムしたデータ連携基盤です

JP-LINKは大きく**3つの機能**で構成されてます（もちろん、他にも色々な機能があります）



エストニアでのデータのコピーを作らないサービス事例 法人登記クラウド

登記申請者： 法人登記ポータルにアクセスして申請

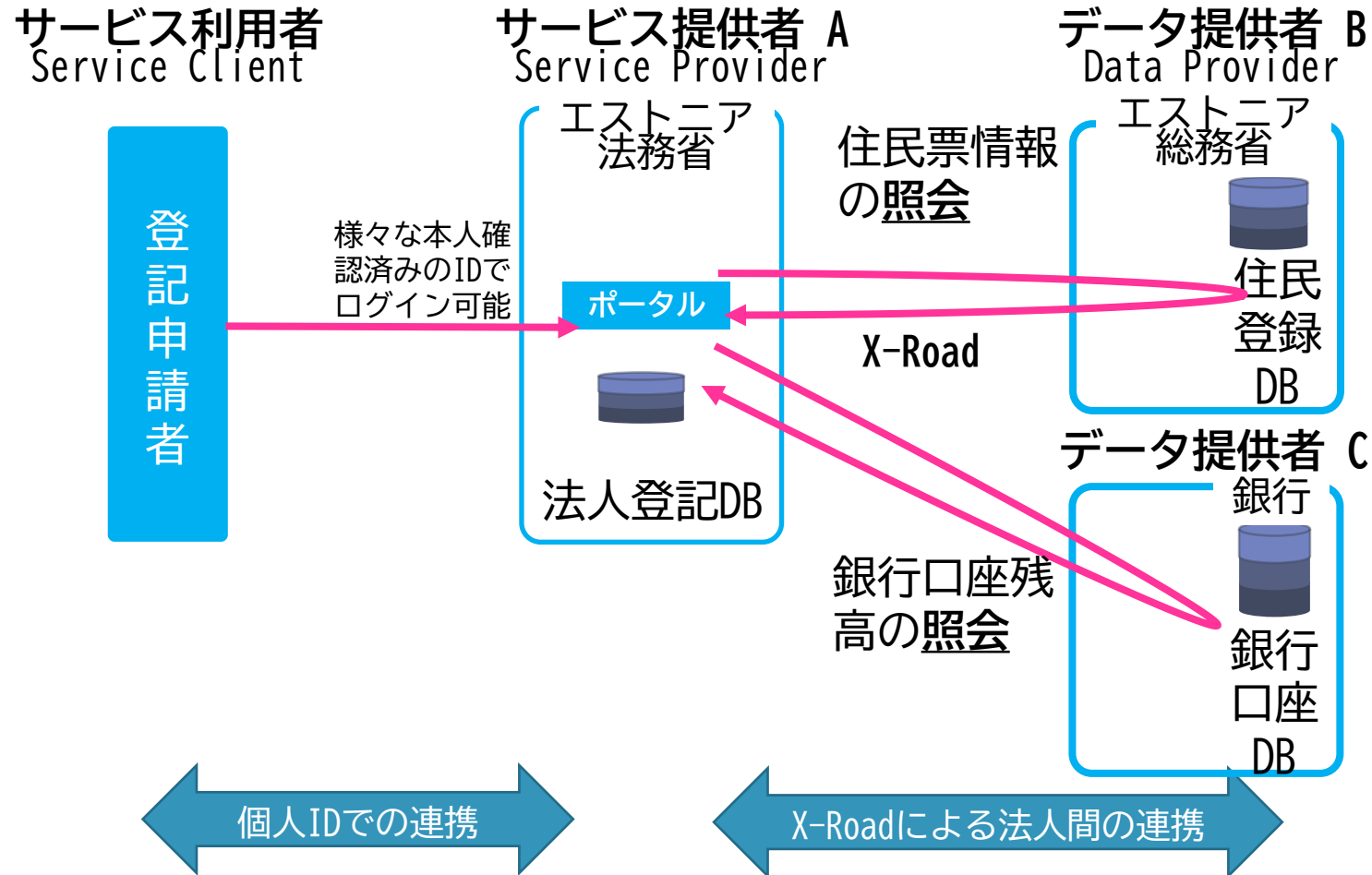
(個人IDと個人の認証、署名を利用)

法務省： 法人登記ポータルを運営、サービス

(サービスプロバイダーは法務省)

法務省： 住民票、銀行口座残高をX-Roadを通じてデータプロバイダーへ照会

(データプロバイダーは総務省と銀行)



参考：
エストニアには「**once only (一度きり)**」という原則があり、同じ情報を複数個所に入力させず、保存された一か所に対して、アクセスが許可された人や組織が参照することで無駄にコピーや同期の手間をとらずに正確な情報の利活用をするという方針があります。

セキュリティサーバーの主な役割

JP-LINKのネットワークに参加するために、**既存システムのデータベースにセキュリティサーバー**を追加します
参加企業間でピアツーピア（P2P）で送信されるメッセージの認証と検証を行います

セキュリティサーバー同士が接続先を認識しているので、細かな設定は不要です

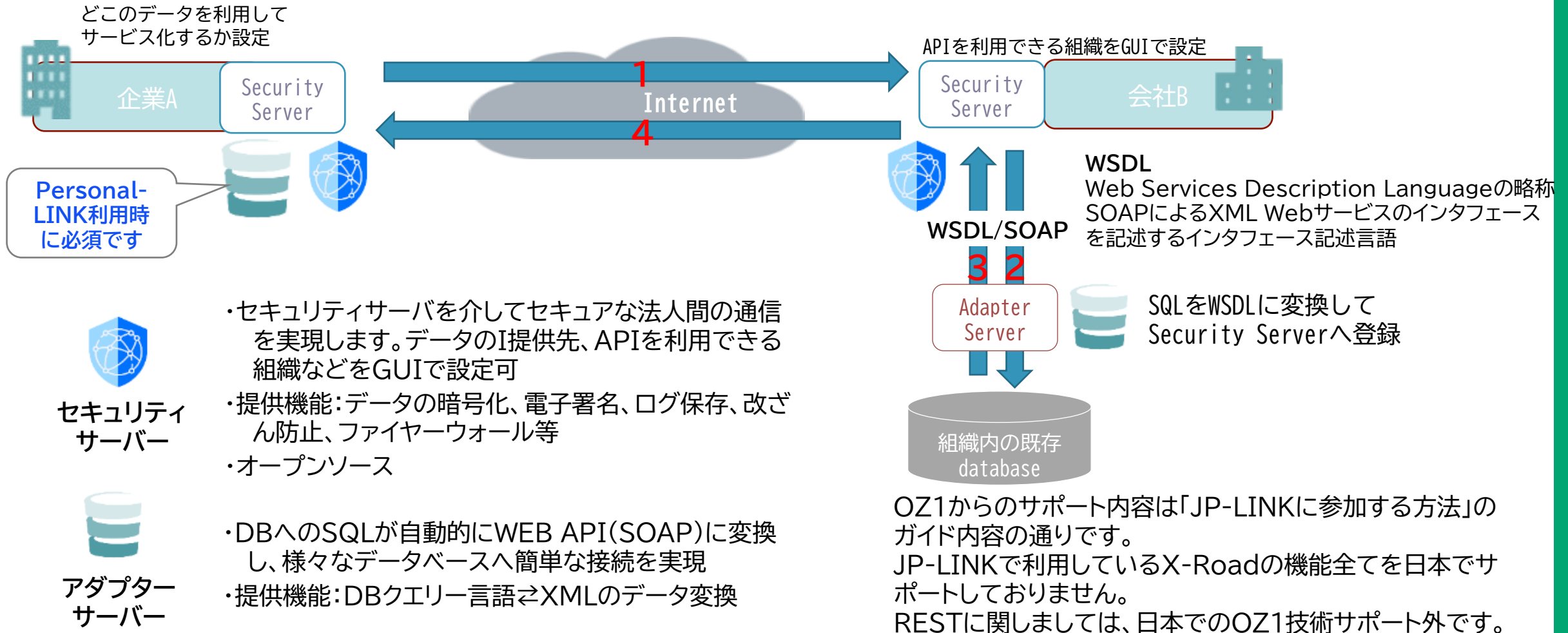


サービスプロバイダーの場合、セキュリティサーバーは独自の情報システムへのアクセス制御も提供します

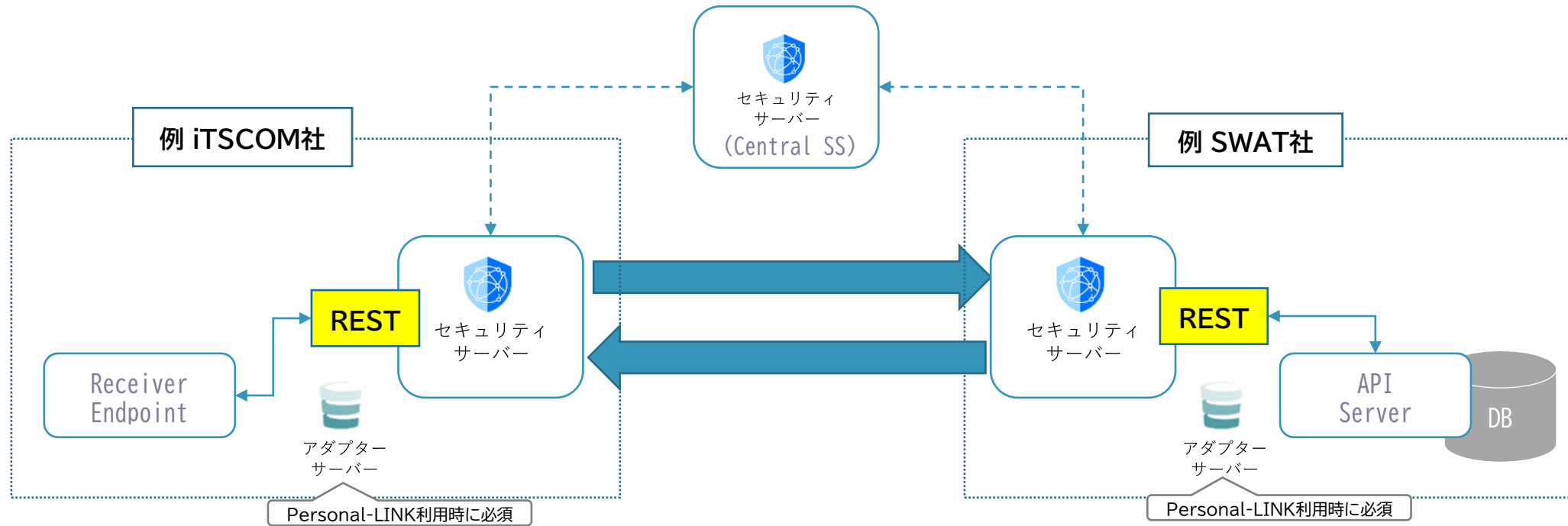
JP-LINKでのデータ交換フロー

JP-LINKでは、データ連携はWEB APIを介して実現します。現在SOAPによるWeb APIのみサポート

注意) Security ServerはWSDLでの登録に加え、v7以降RESTでの登録を受け付ける機能を持ちますが、OZ1から技術サポートを行っておりません。現在、開発チームの方でサポートの検討を行っておりますが、サポートの時期等に関する情報は提供できません



REST API 利用イメージ ※REST通信は令和4年度案件はOZ1サポート対象外



下記X-Road公式ドキュメンテーションでは、RESTサービス利用に関する記載はございませんので、ご確認の上、設定および利用のご判断をお願いいたします。

(SOAPを追加する箇所と合わせて確認いただくと分かりやすいかもしれません。)

REST ※OZ1サポート対象外のため、接続検証等についてAPI提供先にご連携をお願いいたします

[https://github.com/nordic-institute/X-Road/blob/develop/doc/Manuals/ug-ss x-road 6 security server user guide.md#612-rest](https://github.com/nordic-institute/X-Road/blob/develop/doc/Manuals/ug-ss%20x-road%206%20security%20server%20user%20guide.md#612-rest)

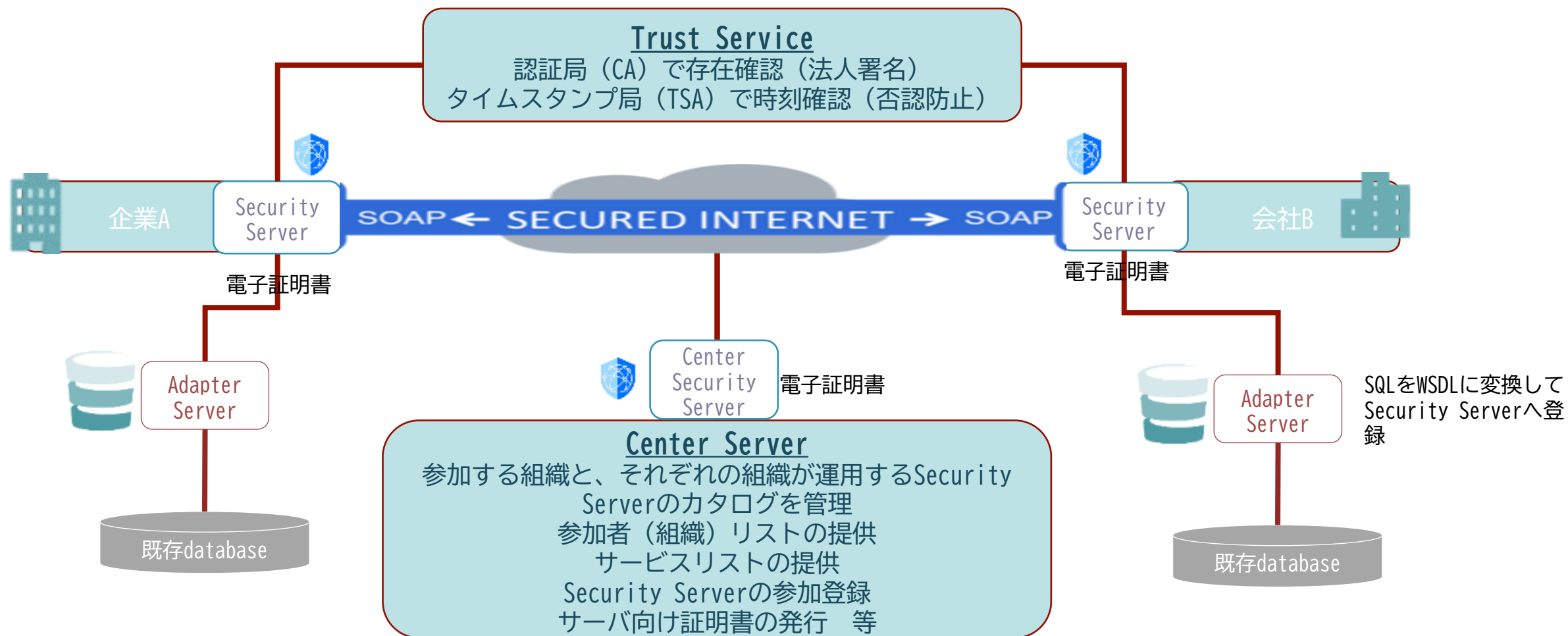
SOAP

[https://github.com/nordic-institute/X-Road/blob/develop/doc/Manuals/ug-ss x-road 6 security server user guide.md#611-soap](https://github.com/nordic-institute/X-Road/blob/develop/doc/Manuals/ug-ss%20x-road%206%20security%20server%20user%20guide.md#611-soap)

注: RESTを設定しているSecurity Serverでも、Adapter Serverの利用やSOAPの通信部分はOZ1より技術サポート可能です。

JP-LINKでのセキュリティの実現

PKIアーキテクチャを利用してセキュアな環境を実現しています



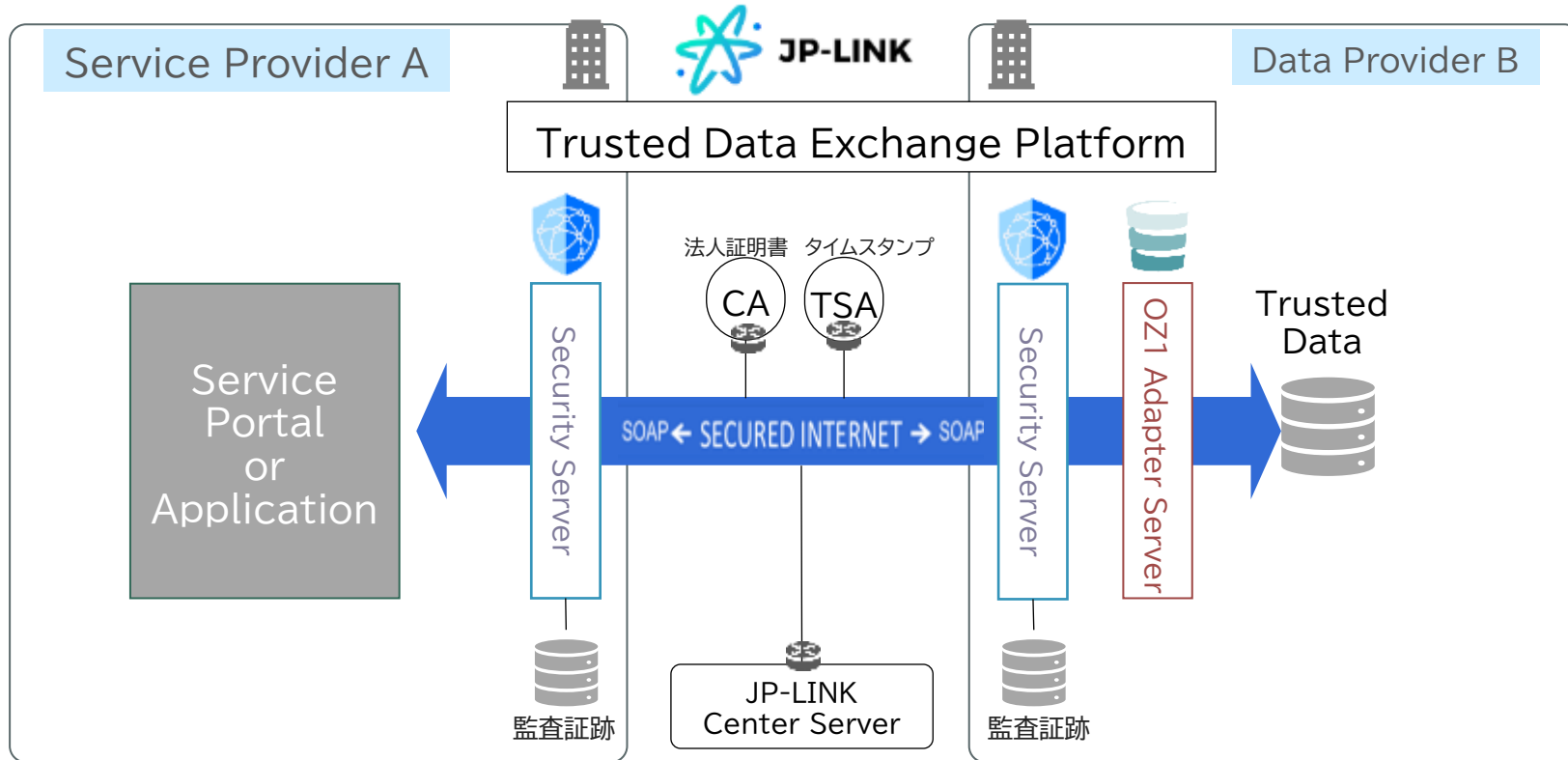
*PKI:「Public Key Infrastructure」の略で、公開鍵暗号技術と電子署名を使って、インターネット上で安全な通信ができるようにするための環境のことを言います。
この公開鍵・秘密鍵は認証局が本人確認の上、電子証明書とともに発行するものです。

上記は双方がユーザへのサービス提供者（データ利用者）兼、データ提供者の例

JP-Linkはデータ提供者とサービス提供者の組み合わせで実現

ユーザへのサービス提供者(データ利用者)

データ提供者



P2Pで実現されるJP-Linkは複数の「ユーザへのサービス提供者(データ利用者)Service Provider」と「データ提供者 Data Provider」の組み合わせで実現されるネットワークです。

データ提供者がサービス提供者を兼務することは問題ありません。

また、サービスをリクエストする主体をサービスクライアントと呼びます。

CA : 認証局、電子証明書を発行
TSA:タイムスタンプ局、時間を証明

JP-LINK FAQ よくある質問

Q サービス作成や参加のために大規模な開発や変更が必要とならないの？

A 現在提供中のサービスを変えずに、モジュールを追加導入し、設定することでつながります
WebAPI開発経験者なら1-3日でインストールから設定まで可能です

Q サービスをたくさん開発し続けなければならないの？

A 一度作成したサービス、ならびにデータ提供の仕組みは、提供先を追加定義するなどのアレンジで再活用可能です。

Q 参加するには何をしなきゃいけないのか？

A モジュールをどこに追加するのか、参加方法、サービスの定義の仕方などのポイントをお伝えします。SOAPでの定義になります。

モジュールのインストール方法、信頼されるネットワークへの参加方法は中級編の技術セッションでお伝えします

詳しくは、JP-Link勉強会(中級編)

参考 サービス・データ連携を考えてみる

役に立つサービスの検討

サービスを実現するため他社のどのデータを活用するか？

1. 実現したいサービスは何か？費用を頂く場合には誰がどのくらいの費用を出しても欲しいサービスは何か？

解決したい課題は何か？

誰のどのようなニーズにこたえることで喜んでもらえるか？

他社に実現していただくサービスは？自社で実現するサービスは？

例)糖尿病が増えると自治体および家族にどのようなコスト負担が予想されるか？

糖尿病慢性化を防ぐと自治体および家族でどのようなコストなど負担軽減が実現されるか？

2. 活用するデータはどこにどのようなデータがあるか？

自身で持つデータの明示と他社のデータの把握

3. どの相手とどのデータをやり取りするか？

4. どのような形式でやり取りするか？業界標準は何か？

5. どのような呼び出しで、どのような引数にしたらどのような値が返るようにするか？

サービス例:各サービスを利用時に住民情報を再入力させないで済ませるために、同じデータの再利用を行う

当初は個人情報にかからないデータで検討

次年度以降で個人の許諾に基づく個人情報を含むデータのやり取りによるサービス実現の検討へ

⇒ データのやり取りの際に信頼できるデータ連携基盤を活用

JP-LINKに参加する方法

Security Serverインストール・セットアップの流れ

1. はじめに と 要件
2. JP-LINKメンバーコードを取得
3. ソフトウェア情報
4. セキュリティサーバーをインストール
5. セキュリティサーバーをセットアップ
6. CSRを送信

注：CSR（Certificate Signing Request）とは、SSL/TLS サーバー証明書を発行するための証明書署名要求のこと

7. 証明書をインポート



2 ページ後に 1 – 3 の内容を記載いたします。

4 – 7 の具体的手順は中級編で解説します。

JP-LINK構築・運用のためのポータルサイトとして**JP-LINKポータル**を提供し、より管理しやすくするように準備中です。

JP-LINKポータル Dashboardイメージ

Dashboadを使えば、JP-Linkの設定プロセスと対応内容が簡単、便利に把握できるようになる予定です。
当面はDashboadを使わず、インストール、運用を行います。

7. 証明書をインポート

The screenshot shows the JP-LINK Dashboard interface. The browser address bar displays 'https://www.example.com/'. The dashboard title is 'My Environment > Dashboard'. The left sidebar contains a navigation menu with items: Dashboard, X-Road members, Security Servers, SS-Certificates, Subsystems, Adapter Servers, Databases, Data Services, Applications, and Settings. The main content area is divided into three tabs: 'X-Road Member Code Settings', 'Security Server Settings', and 'Adapter Server Settings'. The 'Security Server Settings' tab is active, showing a list of items: Security Servers (2), SS-Certificates (4), Subsystems(App) (3), and Subsystems(DB) (2). Below the tabs, there is a section titled 'Applications' with three sub-sections: 'Member code Requests' (1), 'SS-Certificate Requests' (4), and 'Access Permission Requests' (1). Callouts point to specific features: '7. 証明書をインポート' points to the 'SS-Certificates' item in the left sidebar; '2. メンバーコードを取得' points to the 'Member code Requests' section; '6. CSRを送信' points to the 'SS-Certificate Requests' section; and 'アクセス許可の要求' points to the 'Access Permission Requests' section.

X-Road Member Code Settings		Security Server Settings		Adapter Server Settings	
X-Road members	1	Security Servers	2	Adapter Servers	2
		SS-Certificates	4	Databases	2
		Subsystems(App)	3	Data Services	6
		Subsystems(DB)	2		

Applications	
Member code Requests	1
SS-Certificate Requests	4
Access Permission Requests	1

2. メンバーコードを取得

6. CSRを送信

アクセス許可の要求

JP-LINKに参加する方法 1-3

2のメンバーコードの申請・取得と3の条件でポートを開けたVM上のOS環境をご準備ください

1. はじめにと要件

JP-LINKの使用を開始するには、セキュリティサーバーを設定する必要があります。Security Serverは、ネットワーク内の他のメンバーと通信するための安全な方法を提供します。

セキュリティサーバーの主な役割は、メンバー間でピアツーピアで送信されるメッセージの認証と検証を提供することです。サービスプロバイダーの場合、セキュリティサーバーは独自の情報システムへのアクセス制御も提供します。

2. メンバーコードを取得

JP-LINKに参加するには、メンバーとして承認されるためにメンバーコードの取得が最初に必要なになります。

各メンバーが機能するために一意のメンバーコードを持っている必要があります。コードを生成するために、以下の情報をOZ1 (techoz1@oz1.life)へ送信してください。

1. 管理者のeメールアドレス
2. 組織名
3. 追加情報 (任意)

3. ソフトウェア情報

セキュリティサーバーの要件：Ubuntu 18.04 LTSx86-64の場合 もしくはRHELの場合次ページに記載

開くポート：

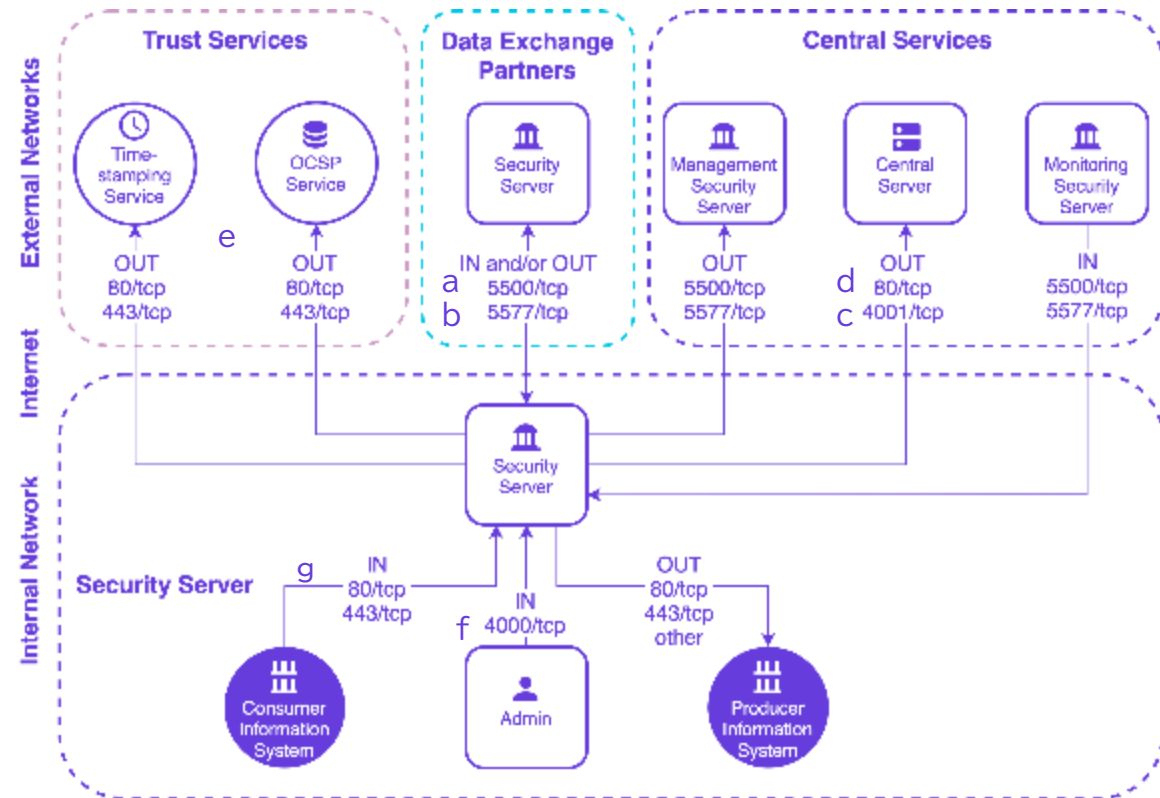
- a. セキュリティサーバー間のメッセージ交換のためのTCP5500インバウンド/アウトバウンド
- b. セキュリティサーバー間のOCSPサービス要求のTCP5577インバウンド/アウトバウンド
- c. 中央サーバーとの通信用のTCP4001アウトバウンド
- d. グローバル設定をダウンロードするためのTCP80アウトバウンド
- e. タイムスタンプサービスおよびOCSPサービスとの通信用のTCP80 / 443アウトバウンド
- f. セキュリティサーバーのユーザーインターフェイスにアクセスするためのTCP4000インバウンド (ローカル)
- g. 情報システム接続用のTCP80 / 443インバウンド/アウトバウンド (ローカル)

4-7の具体的手順は中級編 JP-LINKに参加する方法で解説します。

4. セキュリティサーバーをインストール
5. セキュリティサーバーをセットアップ
6. CSRを送信

注：CSR (Certificate Signing Request) とは、SSL/TLS サーバー証明書を発行するための証明書署名要求のこと

7. 証明書をインポート



セキュリティサーバーの要件(Ubuntuの場合)

セキュリティサーバをインストールするための
VM上のOS(UbuntuもしくはRHEL)環境を
ご用意ください

推奨される最小ハードウェアパラメータ：

- サーバーのハードウェア（マザーボード、CPU、ネットワークインターフェイスカード、ストレージシステム）は、一般的にUbuntuでサポートされている必要があります。
- 64ビットのデュアルコアIntel、AMD、または互換性のあるCPU。AES命令セットのサポートを強くお勧めします。
- 2CPU以上
- 4 GB以上のRAM
- 10 GB以上の空きディスク容量（OSパーティション）、20～40 GBの空きディスク容量（/varパーティション）
ストレージの空き状況は監視してください
- 100Mbps以上のネットワークインターフェイスカード
- 必要に応じて、ハードウェアトークンを使用するためのインターフェイス

ソフトウェアと設定の要件：

- インストールおよび構成されたUbuntu18.04LTSオペレーティングシステム
- セキュリティサーバーがファイアウォールやNATによって他のネットワークから分離されている場合、セキュリティサーバーとの間の必要な接続が許可されます。オペレーティングシステム（DNS、NTP、SSHなど）の機能と管理に必要な補助サービスの有効化は、このガイドの範囲外です。
- セキュリティサーバーにプライベートIPアドレスがある場合は、対応するNATレコードをファイアウォールに作成する必要があります。

セキュリティサーバーの要件(RHELの場合)

セキュリティサーバをインストールするための
VM上のOS(UbuntuもしくはRHEL)環境
をご用意ください

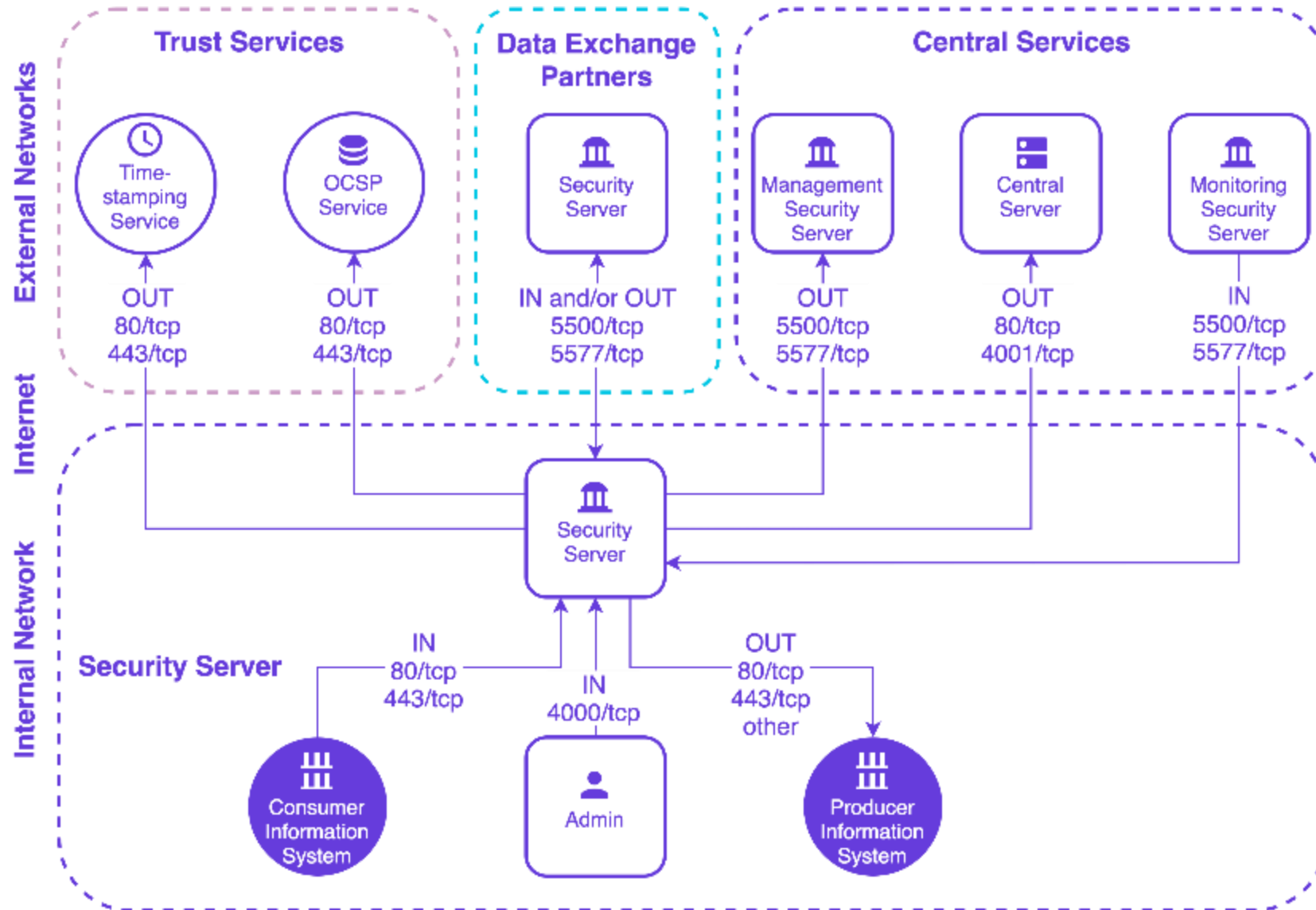
推奨される最小ハードウェアパラメータ：

- サーバーのハードウェア（マザーボード、CPU、ネットワークインターフェイスカード、ストレージシステム）は、一般的にRHELでサポートされている必要があります。
- 64ビットのデュアルコアIntel、AMD、または互換性のあるx86-64 CPU。
- 2CPU以上
- 4 GB以上のRAM
- 10 GB以上の空きディスク容量（OSパーティション）、20～40 GBの空きディスク容量（/varパーティション）
ストレージの空き状況は監視してください
- 100Mbps以上のネットワークインターフェイスカード
- 必要に応じて、ハードウェアトークンを使用するためのインターフェイス

ソフトウェアと設定の要件：

- インストールおよび構成されたRHEL（7.3以降、8.0以降）オペレーティングシステム
- セキュリティサーバーがファイアウォールやNATによって他のネットワークから分離されている場合、セキュリティサーバーとの間の必要な接続が許可されます。オペレーティングシステム（DNS、NTP、SSHなど）の機能と管理に必要な補助サービスの有効化は、このガイドの範囲外です。
- セキュリティサーバーにプライベートIPアドレスがある場合は、対応するNATレコードをファイアウォールに作成する必要があります。

参考: Security Server 通信フロー ubuntuの場合 (X-Road7)

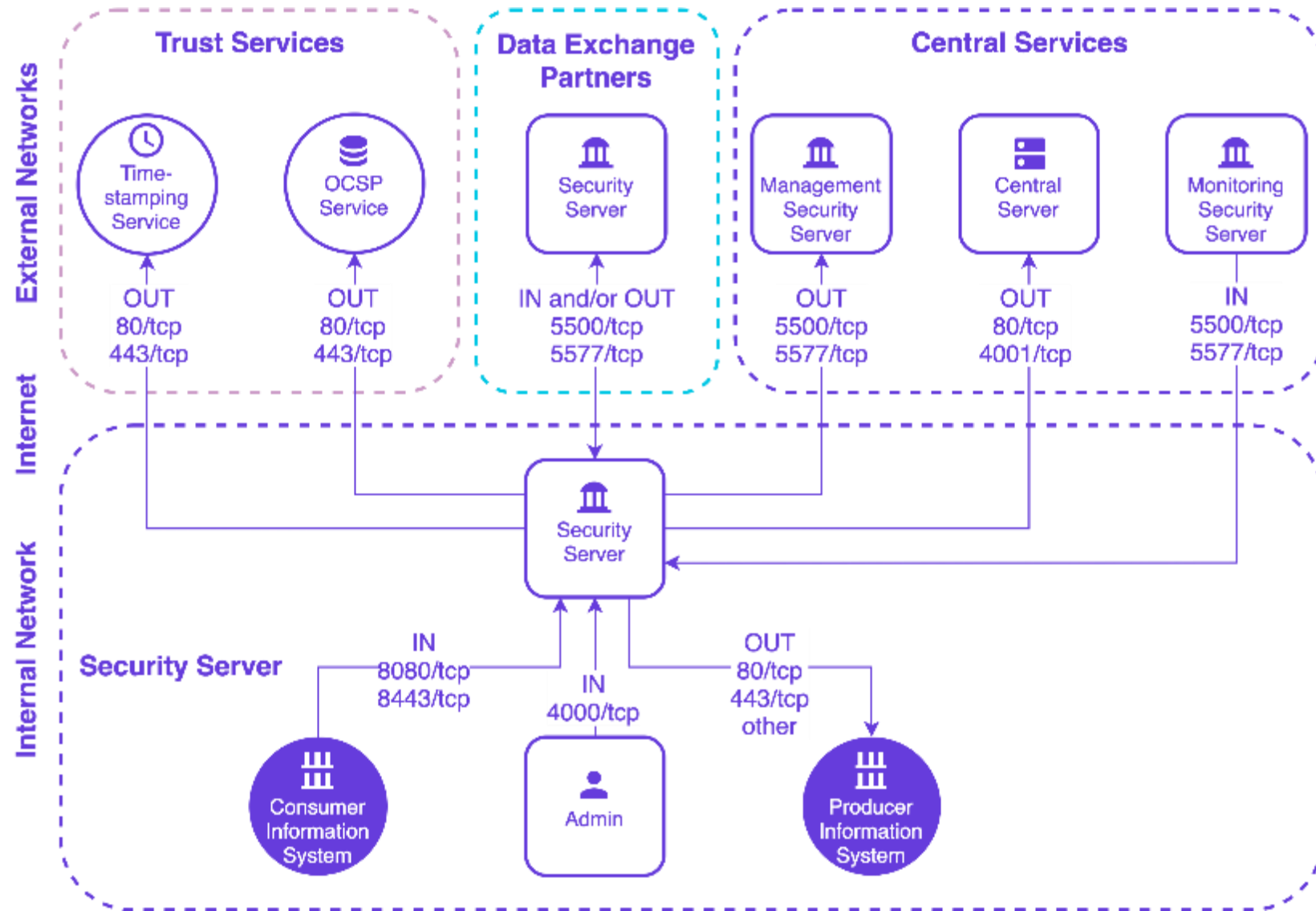


出典: https://github.com/nordic-institute/X-Road/blob/master/doc/Manuals/ig-ss_x-road_v6_security_server_installation_guide.md

参考: Security Server 通信フロー ubuntuの場合 (X-Road7)

Connection Type	Source	Target	Target Ports	Protocol	Note
Out	Security Server	Central Server	80, 4001	tcp	
Out	Security Server	Management Security Server	5500, 5577	tcp	
Out	Security Server	OCSP Service	80 / 443	tcp	
Out	Security Server	Timestamping Service	80 / 443	tcp	
Out	Security Server	Data Exchange Partner Security Server (Service Producer)	5500, 5577	tcp	
Out	Security Server	Producer Information System	80, 443, other	tcp	Target in the internal network
In	Monitoring Security Server	Security Server	5500, 5577	tcp	
In	Data Exchange Partner Security Server (Service Consumer)	Security Server	5500, 5577	tcp	
In	Consumer Information System	Security Server	80, 443	tcp	Source in the internal network
In	Admin	Security Server	4000	tcp	Source in the internal network

参考: Security Server 通信フロー RHELの場合 (X-Road7)



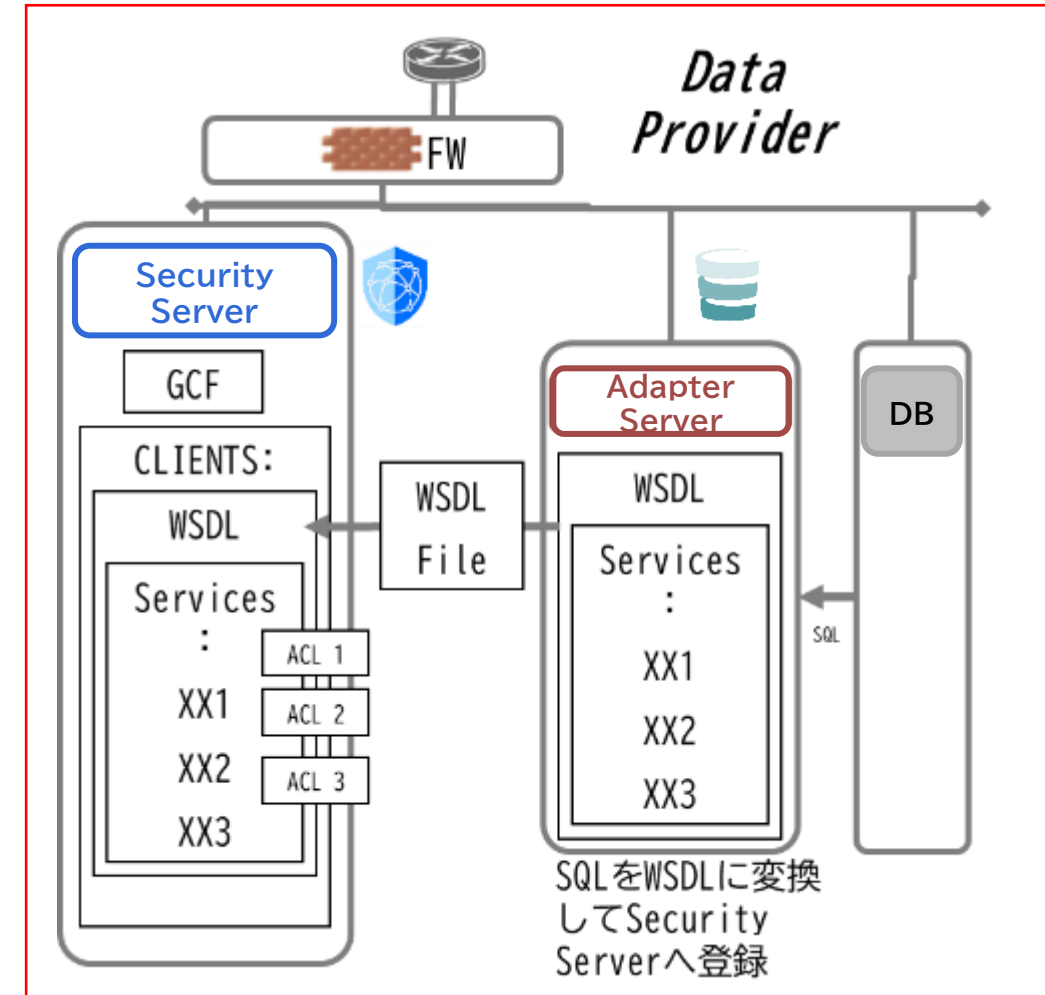
出典: https://github.com/nordic-institute/X-Road/blob/master/doc/Manuals/ig-ss_x-road_v6_security_server_installation_guide_for_rhel.md

参考: Security Server 通信フロー RHELの場合 (X-Road7)

Connection Type	Source	Target	Target Ports	Protocol	Note
Out	Security Server	Central Server	80, 4001	tcp	
Out	Security Server	Management Security Server	5500, 5577	tcp	
Out	Security Server	OCSP Service	80 / 443	tcp	
Out	Security Server	Timestamping Service	80 / 443	tcp	
Out	Security Server	Data Exchange Partner Security Server (Service Producer)	5500, 5577	tcp	
Out	Security Server	Producer Information System	80, 443, other	tcp	Target in the internal network
In	Monitoring Security Server	Security Server	5500, 5577	tcp	
In	Data Exchange Partner Security Server (Service Consumer)	Security Server	5500, 5577	tcp	
In	Consumer Information System	Security Server	8080, 8443	tcp	Source in the internal network
In	Admin	Security Server	4000	tcp	Source in the internal network

データ提供側(Data Provider)における基本的な準備

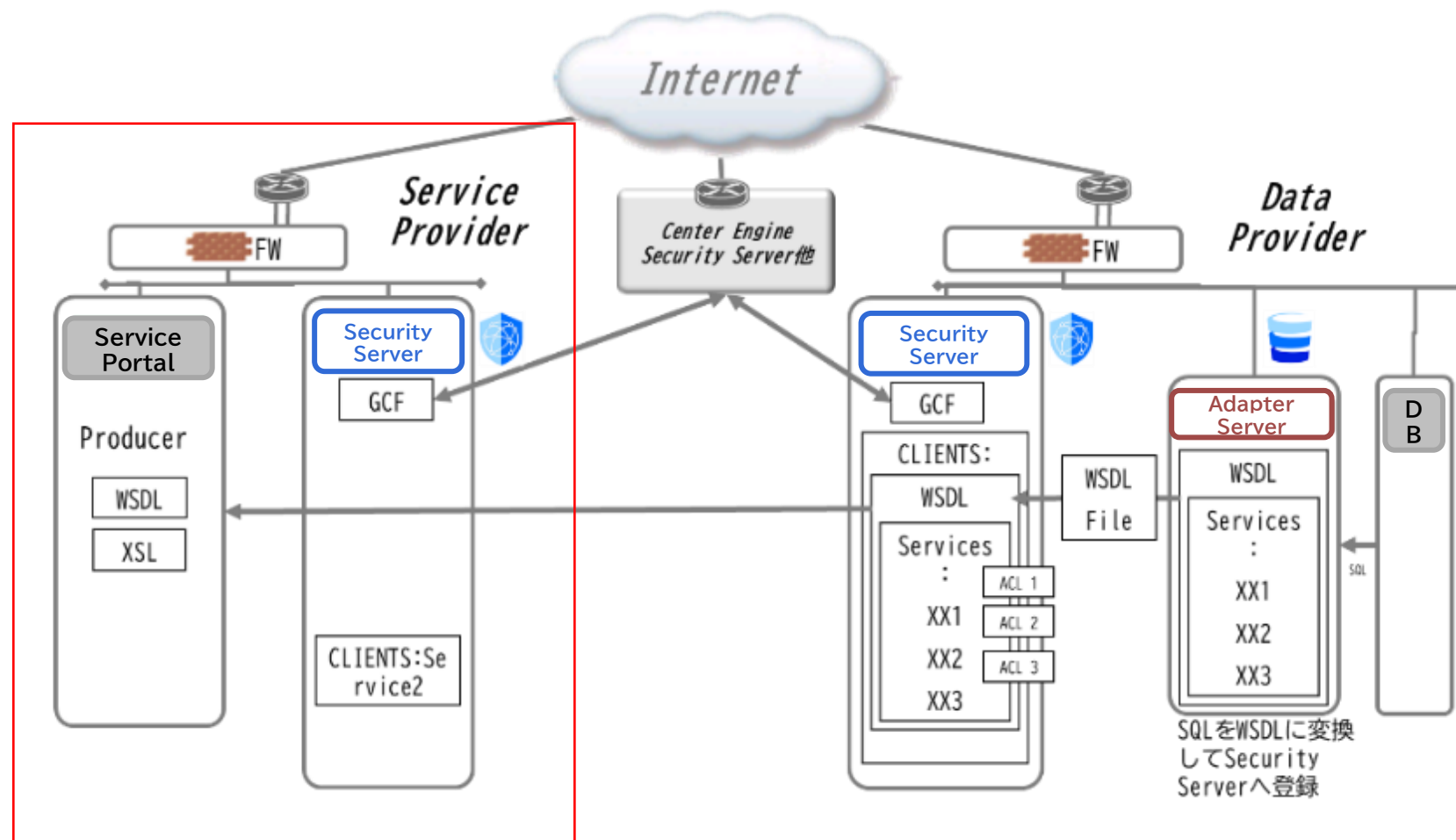
1. センター(OZ1)にネットワーク上の登録を依頼
(CLIENTSとなります)
2. 誰にどのような検索を許可するか相手先
(Service Provider) との調整の上で決めます
3. どのDBにどのような検索をかけるか決めます
(SQL文の定義)
4. Adapter ServerにおいてSQL文を登録します
5. Adapter Serverにおいて自動的にSQL文をWSDLに変換されます
6. Security Serverにおいて変換されたWSDL文を登録します
7. Security Serverにおいて登録したWSDLをどの組織の
Security Serverやアプリケーションにサービスを公開する
か、アクセスを許可するか権限設定、登録します。



サービス提供側(Service Provider)における基本的な準備

1. CLIENTSとしてSecurity Serverに宣言、登録
2. センター(OZ1)にサービス(CLIENTS)をネットワーク上へ登録依頼
OZ1へMember Name,
Member Class, Member Code,
Subsystem Codeを伝達
3. WEB Application ServerにおいてSOAPで自身のSecurity Serverを通じて相手先のSecurity Serverへのアクセスを記述

JP-LINK連携図 データ交換リクエストの流れ



WEB Application ServerにおけるサービスのSOAPでのサンプル記述例

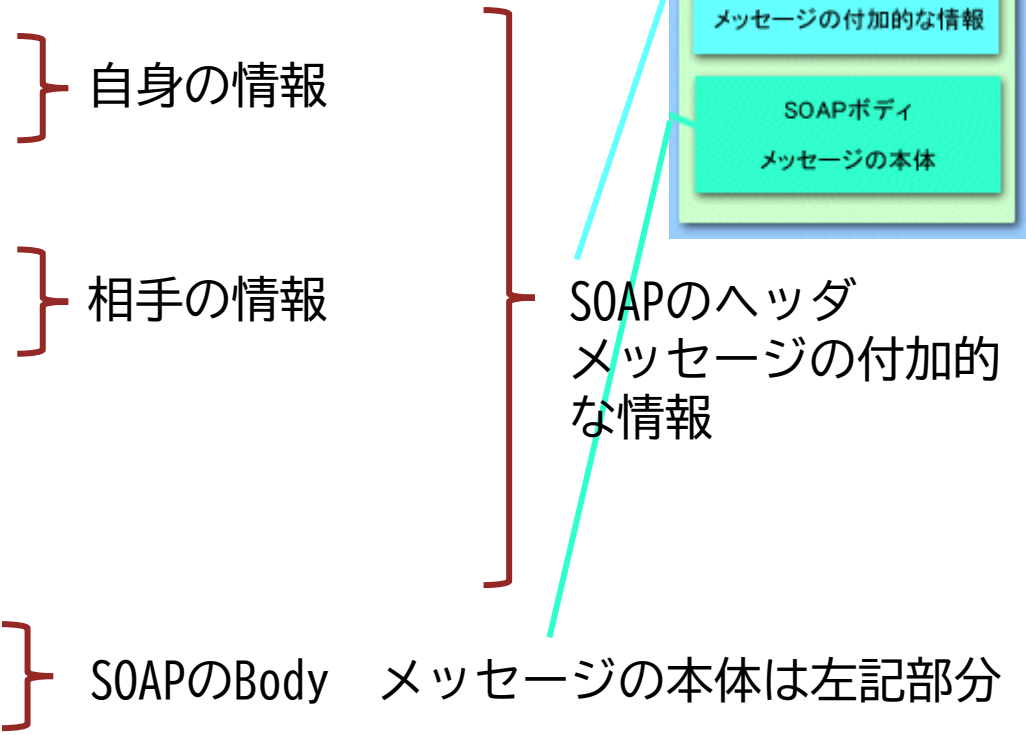
最低限で記述しやすいSOAPでの記述

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:xro="http://x-road.eu/xsd/xroad.xsd" xmlns:iden="http://x-road.eu/xsd/identifiers">
  <soapenv:Header>
    <!-- 自身のセキュリティサーバーの情報 -->
    <xro:client iden:objectType="SUBSYSTEM">
      <iden:xRoadInstance>参加しているネットワーク名</iden:xRoadInstance>
      <iden:memberClass>メンバークラス</iden:memberClass>
      <iden:memberCode>メンバーコード</iden:memberCode>
      <iden:subsystemCode>サブシステムコード</iden:subsystemCode>
    </xro:client>

    <!-- 相手先のセキュリティサーバーの情報 -->
    <xro:service iden:objectType="SERVICE">
      <iden:xRoadInstance>参加しているネットワーク名</iden:xRoadInstance>
      <iden:memberClass>メンバークラス</iden:memberClass>
      <iden:memberCode>メンバーコード</iden:memberCode>
      <iden:subsystemCode>サブシステムコード</iden:subsystemCode>
      <iden:serviceCode>利用したいサービスコード</iden:serviceCode>
      <iden:serviceVersion>サービスのバージョン</iden:serviceVersion>
    </xro:service>

    <!-- 任意設定項目：主に監査ログに残す各種タグ情報 -->
    <xro:id>ID11234</xro:id>
    <xro:userId>EE1234567890</xro:userId>

    <!-- 通信プロトコルのバージョン情報：基本的に固定 -->
    <xro:protocolVersion>4.0</xro:protocolVersion>
  </soapenv:Header>
  <soapenv:Body>
    <prod:{利用したいサービスコード} xmlns:XXX={XML名前空間:仕様にしたがって指定の値を登録}>
      <!-- 以下は利用サービスごとに指定されたパラメーターに従って設定 -->
      <!-- 例：<prod:name>Test</prod:name>等々 -->
    </prod:{利用したいサービスコード}>
  </soapenv:Body>
</soapenv:Envelope>
```



細かいAPIの定義は自信と相手先の定義程度の最低限で、あたかもAPIが自動生成されているかのような単純明快かつ柔軟な形
データの内容に関するルールや定義はないので、業界内での標準を踏まえて相手先と調整して定義の上でやり取りしてください

SOAPでの返事記述例

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:iden="http://x-road.eu/xsd/identifiers" xmlns:xro="http://x-
road.eu/xsd/xroad.xsd">
  <soapenv:Header>
    <!-- 自身のセキュリティサーバーの情報 -->
    <xro:client iden:objectType="SUBSYSTEM">
      <iden:xRoadInstance>参加しているネットワーク名</iden:xRoadInstance>
      <iden:memberClass>メンバークラス</iden:memberClass>
      <iden:memberCode>メンバーコード</iden:memberCode>
      <iden:subsystemCode>サブシステムコード</iden:subsystemCode>
    </xro:client>

    <!-- 相手先のセキュリティサーバーの情報 -->
    <xro:service iden:objectType="SERVICE">
      <iden:xRoadInstance>参加しているネットワーク名</iden:xRoadInstance>
      <iden:memberClass>メンバークラス</iden:memberClass>
      <iden:memberCode>メンバーコード</iden:memberCode>
      <iden:subsystemCode>サブシステムコード</iden:subsystemCode>
      <iden:serviceCode>利用したいサービスコード</iden:serviceCode>
      <iden:serviceVersion>サービスのバージョン</iden:serviceVersion>
    </xro:service>

    <!-- 任意設定項目：主に監査ログに残すために存在する各種タグ情報 -->
    <xro:id>ID11234</xro:id>
    <xro:userId>EE1234567890</xro:userId>

    <!-- ハッシュ値 -->
    <xro:requestHash
algorithmId="http://www.w3.org/2001/04/xmlenc#sha512">wUsvsGAfUM0z08keb4XCfWyfUGAw9In9TraZ4zrfbg7egwrxdoZrJhphGYJ/qwphbFJZ/ub8eYy5hF3IMnoWd
Q==</xro:requestHash>

    <!-- 通信プロトコルのバージョン情報：基本的に固定 -->
    <xro:protocolVersion>4.0</xro:protocolVersion>
  </soapenv:Header>
  <soapenv:Body>
    <ts1:{利用したいサービスコード} xmlns:XXX={XML名前空間:仕様にしたがった指定の値}>
      <!-- レスポンスデータ -->
      <!-- 例：<ts1:message>Hello Test! Greetings from adapter server!</ts1:message> -->
    </ts1:{利用したいサービスコード}>
  </soapenv:Body>
</soapenv:Envelope>
```

} Bodyは左記部分

参考 セキュリティサーバー展開オプション

C.1一般

セキュリティサーバーには、複数の展開オプションがあります。最も簡単な選択は、ローカルデータベースを備えた単一のセキュリティサーバーを使用することです。これは通常、ほとんどの場合は問題ありませんが、展開を調整する理由は複数あります。

C.2ローカルデータベース

最も簡単な展開オプションは、ローカルデータベースで単一のセキュリティサーバーを使用することです。開発とテストの目的で他のものが必要になることはめったにありませんが、本番環境では要件がより厳しくなる可能性があります。

C.3リモートデータベース

セキュリティサーバーでリモートデータベースを使用することが可能です。このオプションは、データベースの状態を外部化する必要がある場合の開発およびテストで使用されることがあります。

セキュリティサーバーは、AWSRDSやAzureDatabaseforPostgreSQLなどのさまざまなクラウドデータベースをサポートしています。この展開オプションは、クラウドネイティブデータベースの使用が最初の選択肢であるクラウド環境で開発を行う場合に役立ちます。

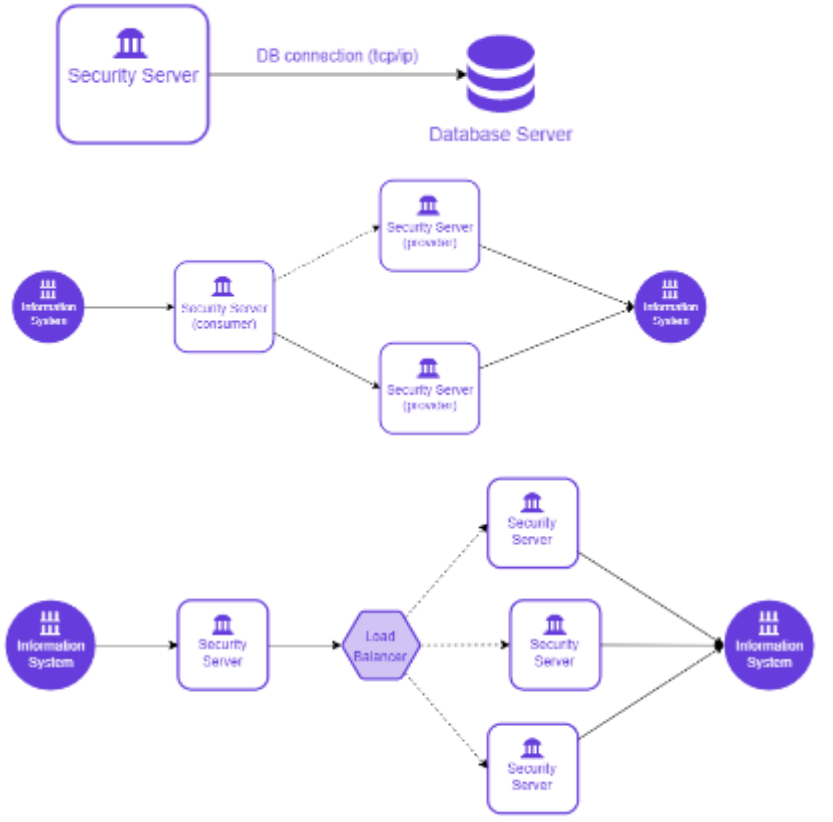
C.4高可用性のセットアップ

実動システムでは、単一障害点が発生することはめったに受け入れられません。セキュリティサーバーは、いわゆる内部負荷分散メカニズムを介してプロバイダー側の高可用性セットアップをサポートします。セットアップは、同じメンバー/メンバークラス/メンバーコード/サブシステム/サービスコードが複数のセキュリティサーバーで構成され、最も高速に応答するサーバーに要求をルーティングするように機能します。この展開オプションは、パフォーマンス上の利点を提供するのではなく、冗長性を提供するだけであることに注意してください。

C.5ロードバランシングの設定

ビジーな本番システムでは、高可用性に加えてスケーラブルなパフォーマンスが必要になる場合があります。これらの問題の両方に同時に対処するための外部負荷分散メカニズムをサポートしています。選択したアルゴリズムに基づいてリクエストをルーティングするために、セキュリティサーバークラスターの前にロードバランサーが追加されます。

展開	開発者	製品
ローカルデータベース	●	
リモートデータベース	●	
高可用性のセットアップ		●
負荷分散の設定		●



参考 ドキュメント

随時更新していきます。ご確認されたい方はご用命ください。

JP-LINKの技術仕様

- 1 はじめに
 - 1.1 概要
 - 1.2 設計目標
- 2 システム・コンポーネント
 - 2.1 センター・サーバ
 - 2.2 セキュリティ・サーバ
 - 2.3 情報システム
 - 2.4 タイムスタンプ局
 - 2.5 認証局
 - 2.6 コンフィギュレーション・プロキシ
 - 2.7 運用モニタリング・デモン
- 3 プロトコルとインターフェイス
 - 3.1 JP-LINKメッセージ・プロトコル
 - 3.2 コンフィギュレーション・ダウンロード・プロトコル
 - 3.3 メッセージ転送プロトコル
 - 3.4 サービス・メタデータ・プロトコル
 - 3.5 署名付きドキュメントのダウンロード
 - 3.6 マネージメント・サービス・プロトコル
 - 3.7 OCSPプロトコル
 - 3.8 タイムスタンプ・プロトコル
 - 3.9 セキュリティ・サーバのユーザー・インターフェイス
 - 3.10 センター・サーバのユーザー・インターフェイス
 - 3.11 運用モニタリング・データの保存
 - 3.12 運用モニタリング・クエリ
 - 3.13 運用モニタリング・プロトコル
 - 3.14 運用モニタリングJMX
 - 3.15 環境モニタリング・プロトコル
 - 3.16 環境モニタリングJMX
- 4 テクノロジー・マトリックス
- 5 配置ビュー
- 用語の定義
 - EIDAS
 - OCSP
 - PKCS10
 - SOAP
 - TSP
 - WSDL

JP-LINK セキュリティ・サーバ・ユーザーガイド

- 1 はじめに
 - 1.1 X-Road セキュリティ・サーバ
 - 1.2 X-Road のコンセプト
 - 1.3 用語の定義
 - ASIC
 - CRON
 - [INI] file
 - JDBC
 - JSON
 - JMX
 - Zabbix Gateway
 - Zabbix JMX
 - Zabbix API
- 2 ユーザー管理
 - 2.1 ユーザーのロール(役割)
 - 2.2 ユーザーの管理
- 3 セキュリティ・サーバの登録
 - 3.1 セキュリティ・サーバ所有者用の署名用鍵と証明書の設定
 - 3.1.1 署名用鍵の作成
 - 3.1.2 署名用 CSR の作成
 - 3.1.3 ローカル・ファイル・システムから証明書のインポート
 - 3.1.4 セキュリティ・トークンから証明書をインポートする
 - 3.2 セキュリティ・サーバの認証用鍵と証明書の設定
 - 3.2.1 認証用鍵の作成
 - 3.2.2 認証用鍵のための CSR の作成
 - 3.2.3 ローカル・ファイル・システムから認証用証明書のインポート
 - 3.3 X-Road 監督機関においてセキュリティ・サーバを登録する
 - 3.3.1 認証用証明書の登録
- 4 セキュリティ・サーバ・クライアント
 - 4.1 セキュリティ・サーバのクライアントの状態
 - 4.2 セキュリティ・サーバにクライアントの追加
 - 4.3 セキュリティ・サーバ・クライアントの署名用鍵と証明書の設定
 - 4.4 X-Road 監督機関にセキュリティ・サーバ・クライアントを登録する
 - 4.4.1 セキュリティ・サーバ・クライアントの登録
- 4.5 セキュリティ・サーバからクライアントの削除
 - 4.5.1 クライアントの登録を解除する
 - 4.5.2 クライアントを削除する
- 5 セキュリティ・トークン、鍵、および証明書
 - 5.1 セキュリティ・トークン、鍵、および証明書の状態
 - 5.2 証明書の登録状態
 - 5.2.1 署名用証明書の登録状態
 - 5.2.2 認証用証明書の登録状態
 - 5.3 証明書の有効性状態
 - 5.4 証明書の有効化と無効化
 - 5.5 認証用鍵と証明書の設定と登録
 - 5.6 証明書の削除
 - 5.6.1 認証用証明書の登録を解除する
 - 5.6.2 証明書または CSR 通知の削除
 - 5.7 鍵を削除する
- 6 X-Road サービス
 - 6.1 WSDL を追加する
 - 6.2 WSDL の更新
 - 6.3 WSDL の有効化と無効化
 - 6.4 WSDL のアドレスの変更
 - 6.5 WSDL の削除
 - 6.6 サービス・パラメータの変更
- 7 アクセス権
 - 7.1 サービスのアクセス権の変更
 - 7.2 サービス・クライアントの追加
 - 7.3 サービス・クライアントのアクセス権の変更
- 8 ローカル・アクセス権グループ
 - 8.1 ローカル・グループを追加する
 - 8.2 ローカル・グループのメンバーの表示と変更
 - 8.3 ローカル・グループの説明を変更する
 - 8.4 ローカル・グループの削除
- 9 クライアント情報システムとの通信
- 10 システム・パラメータ

JP-LINK: セキュリティ・サーバのアーキテクチャ

- 1 初めに
 - 1.1 概要
 - 1.2 用語の定義
- 2 コンポーネント・ビュー
 - 2.1 プロキシ
 - 2.2 メッセージ・ログ
 - 2.3 メタデータ・サービス
 - 2.4 運用モニタリング・サービス
 - 2.5 運用モニタリング・バッファ
 - 2.6 Signer
 - 2.7 データベース
 - 2.8 ユーザー・インターフェイス
 - 2.9 サプレット・エンジン
 - 2.10 コンフィギュレーション・クライアント
 - 2.11 パスワード・ストア
 - 2.12 SSCD
 - 2.13 環境モニタリング・サービス
 - 2.14 モニター
- 3 インターフェース
 - 3.1 管理サービス
 - 3.2 コンフィギュレーションのダウンロード
 - 3.3 メッセージ・プロトコル
 - 3.4 メッセージ転送プロトコル
 - 3.5 サービス・メタデータ・プロトコル
 - 3.6 署名された文書のダウンロード
 - 3.7 TSP
 - 3.8 OCSP
 - 3.9 運用モニタリング・プロトコル
 - 3.10 運用モニタリング・データの保存
 - 3.11 運用モニタリング・クエリ
 - 3.12 環境モニタリング・プロトコル
 - 3.13 環境モニタリング JMX

参考 SOAPとは？

SOAP:Simple Object Access Protocol

SOAP は標準プロトコルです。元々、異なる言語および異なるプラットフォームで構築されたアプリケーションが通信できるようにすることを目的に設計されました。これはプロトコルなので、組み込みのルールが適用され、複雑さとオーバーヘッドが増大し、ページのロード時間が長くなる可能性があります。しかし、これらの標準は組み込みのコンプライアンスも提供するため、エンタープライズシナリオに適しています。組み込みのコンプライアンス基準には、セキュリティ、原子性、一貫性、分離、および耐久性（ACID）が含まれます。ACID は、信頼性の高いデータベース・トランザクションが確実に行われるようにする一連のプロパティです。

一般的な Web サービスの仕様は次のとおりです。

- Web サービスセキュリティ (WS-Security)**: トークンと呼ばれる一意の識別子を通じてメッセージを保護および転送する方法を標準化します。
- WS-ReliableMessaging**: 信頼性の低い IT インフラストラクチャを介して転送されるメッセージ間のエラー処理を標準化します。
- Web サービスアドレッシング (WS-Addressing)**: ルーティング情報をネットワーク内の奥深くに保持するのではなく、SOAP ヘッダー内のメタデータとしてパッケージ化します。
- Web サービス記述言語 (WSDL)**: Web サービスの機能、およびそのサービスの開始と終了の場所を記述します。

SOAP API に送信されたデータ要求は、HTTP (Web ブラウザの場合)、SMTP (電子メールの場合)、TCP などの任意のアプリケーション・レイヤー・プロトコルを介して処理できます。しかし、要求が受信されると、SOAP メッセージは XML ドキュメント (人間も機械も読み取り可能なマークアップ言語) として返信される必要があります。完了した SOAP API への要求はブラウザでキャッシュできないため、API に再送信しない限り、後でアクセスすることはできません。