Modeling Forum 2011

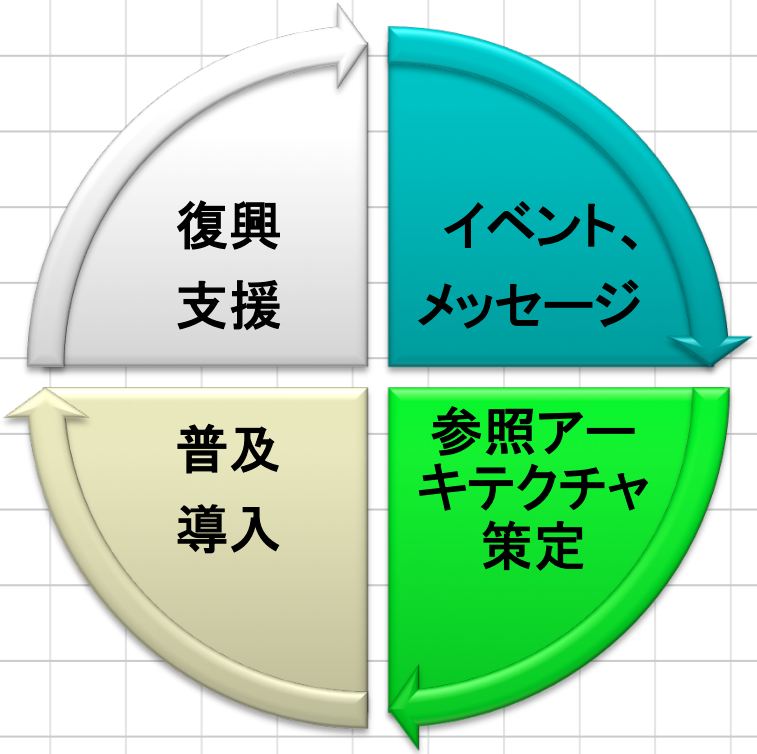
災害を念頭においたITアーキテクチャ ～Project ICHIGANの活動を通して～

2011-10-19 Project ICHIGAN 榊原 彰

Project ICHIGAN

Project ICHIGANとは

- Project ICHIGANとは、広域大災害などの危機的状況においても迅速かつ円滑に被災地域の自治体業務が再開できるよう、自治体の区分を超えて災害対策・業務継続性を考慮したITシステムを提案し、その実現を目指すための体制作りを支援する非営利のボランティアプロジェクトです。



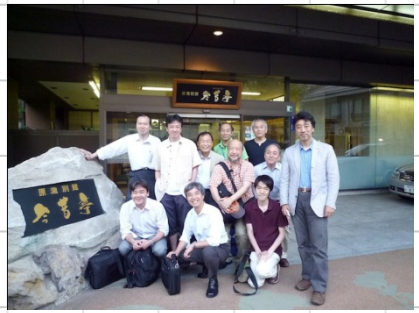
活動履歴

2011/10/19
モデリングフォーラム

2011/9/27 中間報告会

2011/9/08 CEDEC2011

2011/7/23 会津合宿



活動メンバー呼びかけ
(Webサイト、Facebook立ち上げ)

2011/5/25 キックオフ

たくさんのメンバーが趣旨に賛同し、活動に参加

鈴木章太郎, 大嶽隆児, 丸山宏, 小野沢博文, 浦本直彦, 隈元章次, …

プロジェクト発起メンバーでプロジェクトの目的や活動方法を決める

岩切晃子, 臼井公孝, 小野雄太郎, 菊間裕二, 小井土亨,今野睦, 榊原彰, 酒匂寛, 新村剛史, 鈴木雄介, 竹村司, 玉川憲, 萩本順三, 萩原正義, 羽生田栄一, 林好一, 平鍋健児, 福井厚, 細川努, 安井力 (五十音順、敬称略)

Project ICHIGAN宣言

私たちは、日本が東日本大震災から物質的かつ精神的な復興を果たすために、既成の枠組みに捉われず、以下の考えに基づき行動します。

- 私たちは、自治体システムの**新しいリファレンスモデルの開発**に取り組みます。このモデルは、特定メーカーの機種や製品に依存せず、自治体の規模にも左右されません。一貫したオープン性と柔軟性を備えます。
- 新しいリファレンスモデルに基づき構築されるシステムは、複数の自治体で共用可能です。被災によりシステムが使用不能となった自治体は、別の自治体のシステムで業務を遂行できます。新しいモデルは、**自治体業務の迅速な再開を可能にします**。
- 私たちは、この非営利活動を通じて、これからの日本社会における**新しい情報システムのあり方**を提案し、それを普遍的な価値として、世界へ向けて発信していきます。
- 私たちは、このたびの震災の被害に遭われた方々の苦難を忘れません。被災された人々と地域に貢献できるよう行動を起こします。

私たちは、Project ICHIGANの活動を通して、**夢と希望を持てる日本社会の再生**に尽くします。
そのために、ITと社会の架け橋に深く関わる者として、責任を果たし続けることをここに誓います。

ICHIGAN参照アーキテクチャ(RA)

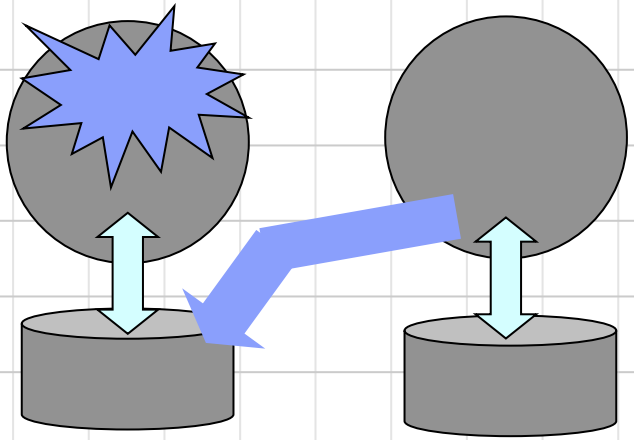
Project ICHIGAN

- 実装自体の提供ではなく、自治体システムの設計時に再利用されることを前提とした、自治体情報システムの基本構造を提供
- RA自体はベンダー技術中立。各自治体がICHIGAN RAを採用して設計を進めるにあたってどのような製品でそれらを実現するかは、ITベンダーやSIerを始めとしたシステム構築者の自由。
- APPLICやLASDECといった既存の自治体アーキテクチャ・モデルは排他的な関係ではなく、一部は概念および設計内容を共有する

ICHIGAN RAが目指すもの

- 被災地と被災をまぬがれた地域で、行政システムの相互代用が可能となるようにする

- 避難所管理システム、安否確認システム等の有事対応システムと行政システムとの接続が容易になるようにする

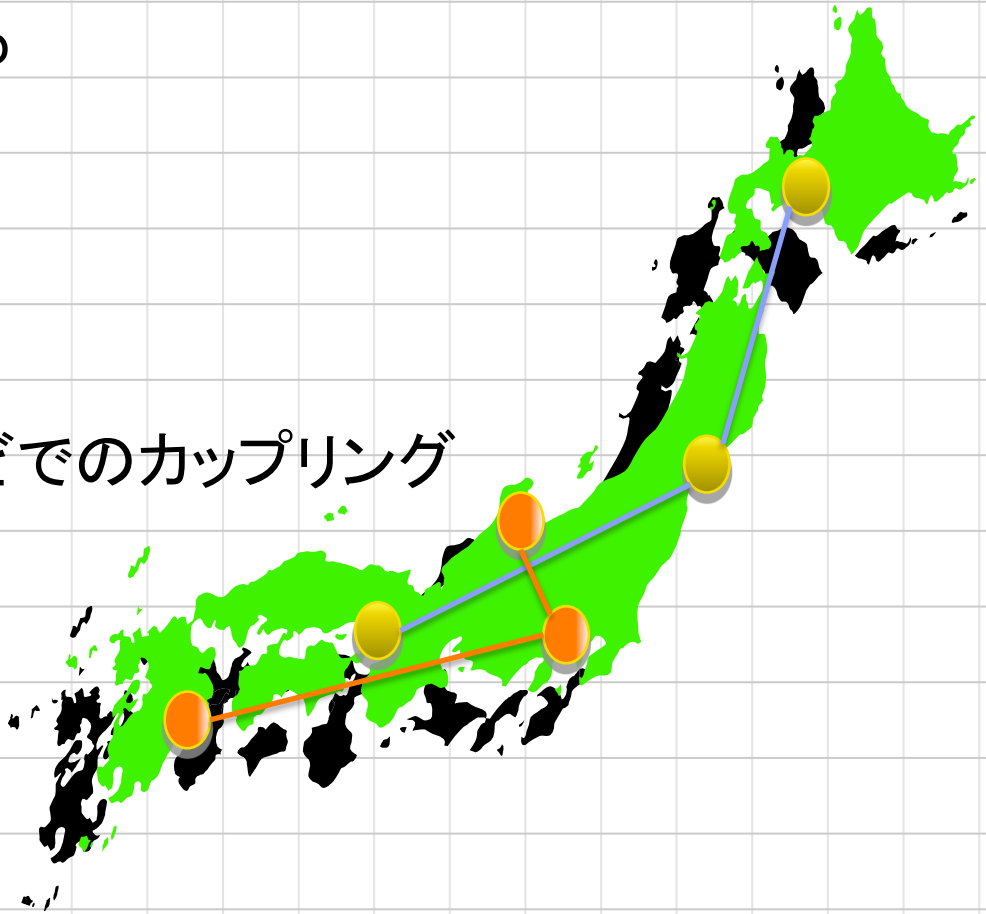


ICHIGAN RAが考えるシステム運用

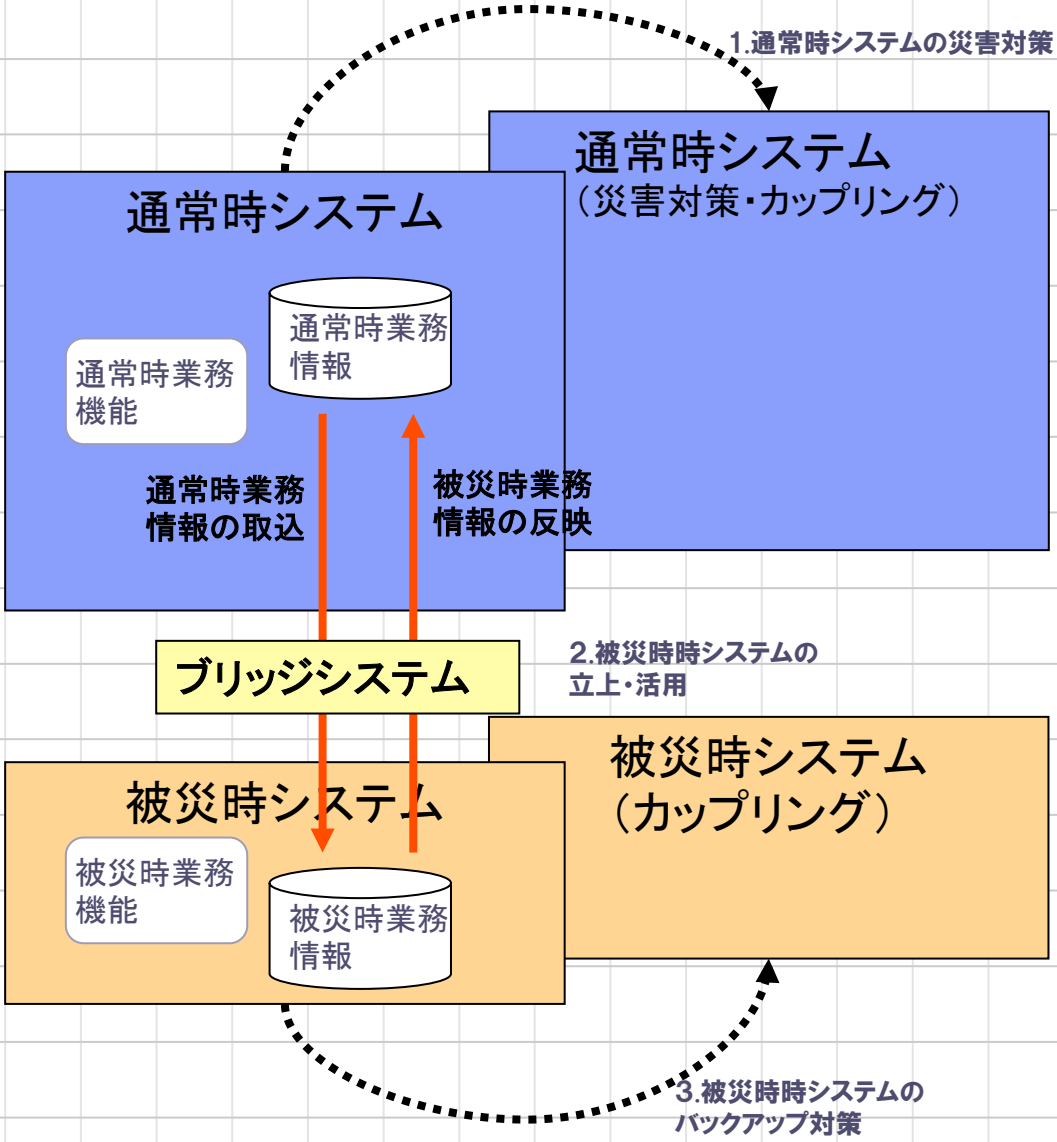
Project ICHIGAN

複数の地方自治体でネットワークを組み（ペアリングあるいはカップリング）、有事の際に、被災した自治体の業務アプリケーションの操作を他の自治体で代行してもらうことを可能とする

例えば
県レベル、市町村レベルなどでのカップリング



想定するアーキテクチャのイメージ



既存の取り組みとの違い（位置づけ）

自治体BCPガイドライン

ICHIGAN
アーキテクチャ評価
（BCPからNFR設定）

通常時基幹システム

APLIC
LASDEC

データ定義

ICHIGAN
アーキテクチャ評価

ICHIGAN
リファレンス
アーキテクチャ

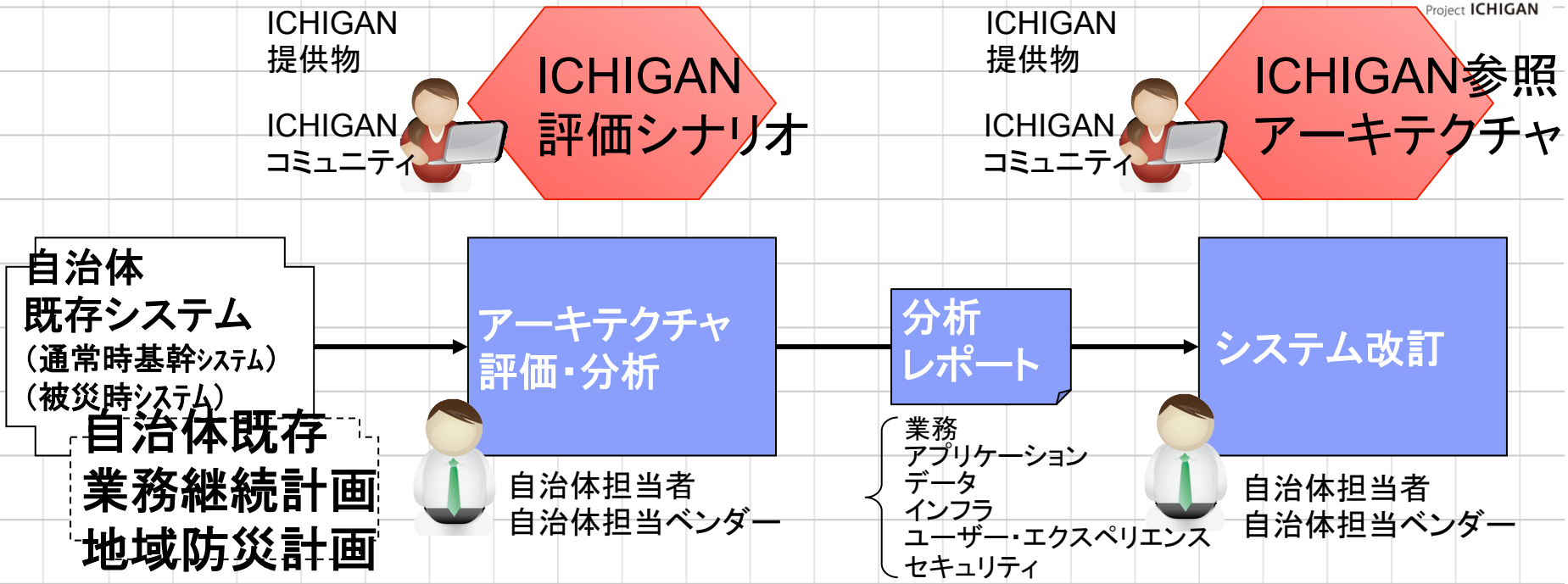
被災時システム

LASDEC被災者支援
APPLIC防災業務標準仕様

データ定義

ICHIGAN参照アーキテクチャ（RA）とは（リファレンスモデル）

ICHIGAN参照アーキテクチャの使い方



- 自治体の既存の業務・システムとBCPを前提として、以下の活動の実施を想定する。
  - ICHIGANで定義したシステム評価シナリオに基づき、既存の業務・システムの災害対策および業務継続性対応状況の評価を行う。
  - 評価結果に基づき、業務・システムの改訂を行う。検討にあたり、ICHIGAN参照アーキテクチャを活用することが可能である。
- 上記の活動の主担当として、自治体担当者、および、自治体の担当ベンダーを想定する。

システム横断要求およびConOps

Project ICHIGAN

- コンセプト・オブ・オペレーション
  - コンセプト・オブ・オペレーション（the Concept of Operation: 以下、ConOps）は、大規模・複雑なシステムを開発する際にシステムデザインそのものを管理・統制していくための「システムデザイン・マネジメント」の手法の1つ
  - システムデザイン・マネジメントでは、開発の初期段階で，顧客・ユーザーのニーズを把握するためにシステムがある時点でどのように使われるのか，局面の遷移を検討する。これはより個別のユースケースを検討していくための、場面設定と考えることが可能で、局面の遷移によって必要な業務機能の制約を定義
  - ICHIGAN RAでは、この局面の遷移に加えて、各局面で組織およびITシステムがどのようなモードで運用されるのかを定義する。
    - 警戒期
    - 緊急期
    - 応急期
    - 復興期
    - 復旧期
    - 通常期

緊急時対応計画は、災害時の行政システムを想定した運用構想があるか？

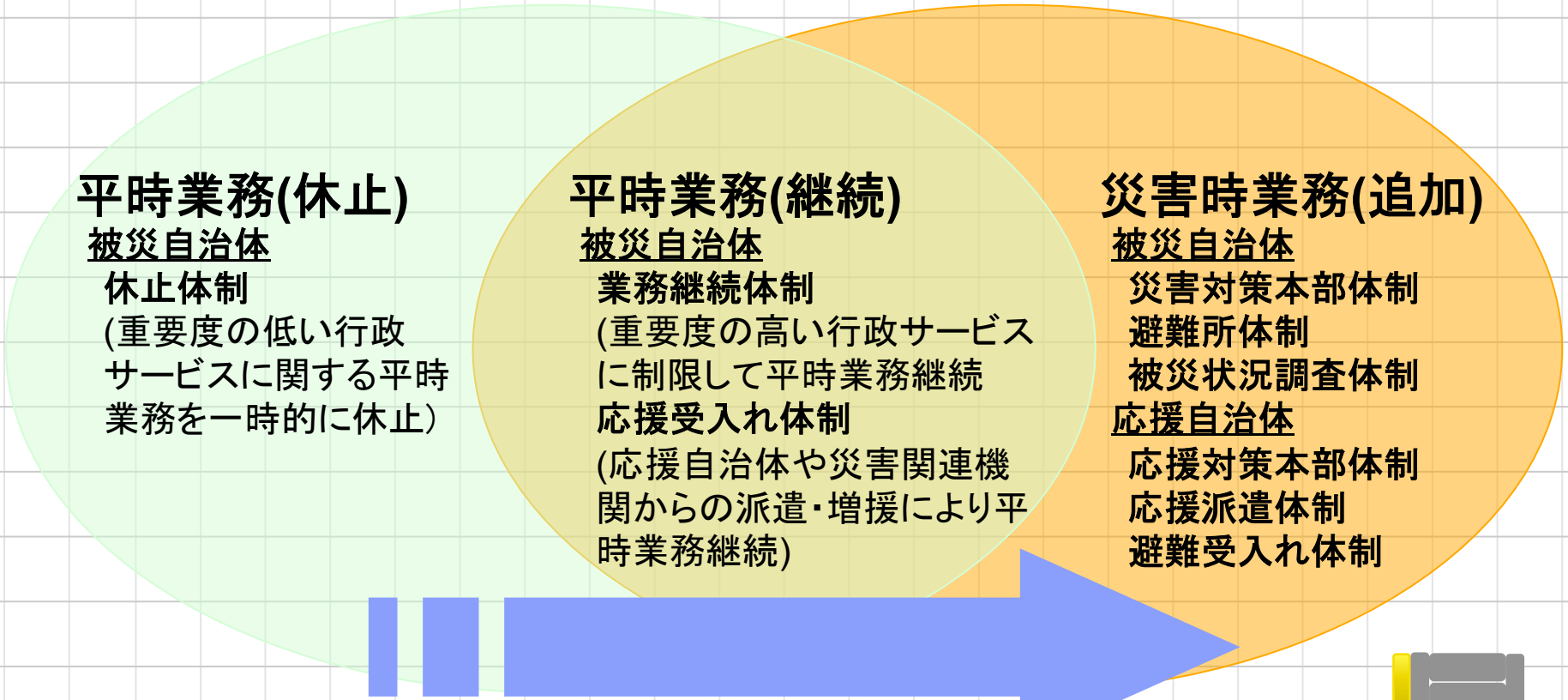
欧米の公的機関では、緊急時対応計画のシステム調達に関して、災害時のシナリオを想定した運用構想を作成している

- 新業務・システムの運用構想(ConOps:Concept of Operations)を様々な関係者が共通理解できるように、実装技術等の専門用語を使わずに利用者の視点で記述する
- 現行の課題や脅威に対応する任務必要事項(MNS:Mission Need Statements)に基づいて、新業務・システムに備えるべき能力（機能・性能）を記述する
- 災害時の局面(Phase)、場面(Situation)に起こりえる状況(Condition)を設定し、それに適用する方針(Policy)とその前提・制約条件を記述する
- 設定した局面・場面・状況に対応する組織の運営モード、システムの運用モードを定義し、シナリオと概念図を作成する

参考資料:
DHS Acquisition Instruction/Guidebook #102-01-001: Appendix F Concept of Operations, (米国国土安全保障省　調達ガイドブック)

災害時の局面、場面、状況に必要な任務と業務に適した組織体制の変更があるはず？

被災自治体は、災害対策本部体制/避難所体制へ、
応援自治体は、救援体制/避難者受入れ体制へ、組織の編成を変える



自治体システムは、災害時の組織体制に適合した運用モードが設計されているか？

モードとは、システムが提供する機能やサービスレベルの程度(Grade)をまとめて切り替え（モードチェンジ）ができるシステム仕様のセットである。

- 通常サービスモード(Normal/Full service mode)
- サービスレベル縮小モード(Degraded mode)
- 能力増強モード(Upgraded mode)
- 機能制限モード(Restricted/Limited mode)
- 機能代替モード(Alternative mode)
- 手動モード(Manual Control mode)
- 災対モード(Disastor Support mode)
- 訓練モード(Training mode)
- 開発・テストモード(Development and Test mode)
- 保守モード(Maintenance mode)

・・・・・・など

災害局面の場面・状況により変化する組織体制と業務に対応できる自治体システムのモードを手動または自動で切り替える機能を提供する必要がある。

ICHIGAN RAは、応急期の場面と状況に対応する運用モード から取り組んでいる

局面	場面	状況	組織の運営体制	情報システムの運用モード
通常期 （平穏期）	住民サービス 防災計画 防災訓練・演習	被害なし	通常体制 訓練体制	平時の行政サービスを提供している(通常サービスモード) 防災訓練・演習を実施している(訓練モード)
警戒期 緊急期 避難・救助	警報・避難勧告 捜索・救助 救急・救命 不明・犠牲者情報	組織-部分被害、災害対策関連機関との連携 IT-ネットワーク輻輳/電源喪失	災害対策本部体制 避難誘導体制 (監視体制) (警戒体制) (非常体制)	平時の自治体システムが利用できない(ネットワーク輻輳/電源喪失) 防災情報システムも機能しない 防災無線、自治体Twitter/blog等の代替モードに移行する
応急期 (救援期) 避難所生活	避難所開設・運営 避難者安否確認 調達と配給 り災・被災証明 義捐金・給付金	組織-応援、災害対策関連機関との連携 IT-復旧、データ不整合、災害時業務処理増加	災害対策本部体制 避難所運営体制	復旧した平時自治体システムで重要な行政サービスの業務を継続する(サービレベル縮小モード) 応急期の災害対策用自治体システムを立ち上げ、平時の自治体システムや災害関連機関と連携する(災対モード)
復旧期 仮設生活	仮設住宅管理 復旧事業	組織-自立 IT-通常、	災害対策本部体制 復旧本部体制	復旧事業に必要な行政サービスに対応する自治体システムを短期に立ち上げる(開発・テストモード)
復興期	復興事業	組織-自立 IT-通常	復興本部体制	復興事業に必要な行政サービスに対応する自治体システムを短期に開発・テストする(開発・テストモード)

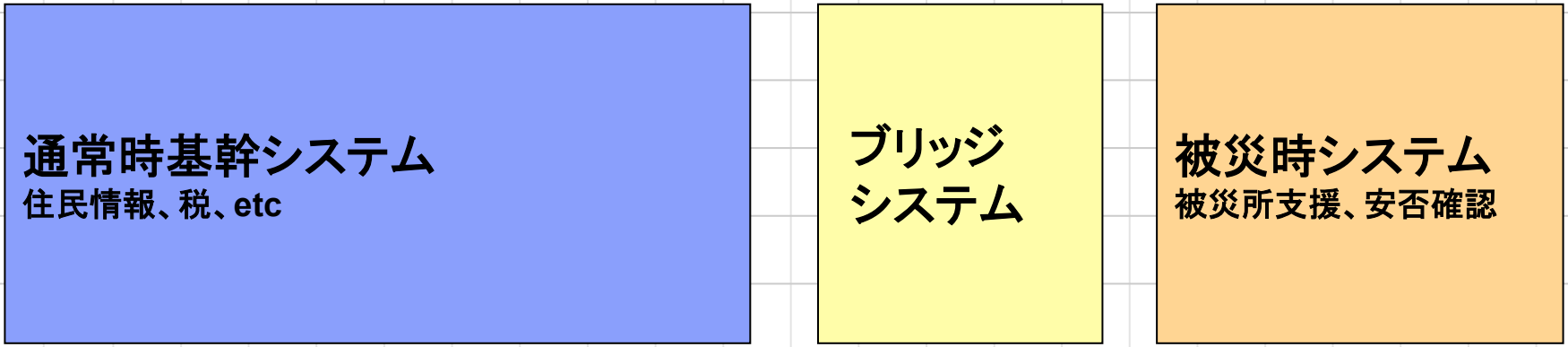
インフラストラクチャ・アーキテクチャ

- 災害時のライフラインとなる回線の確保から、ネットワーク上のシステム・サービス（いわゆるPaaSのイメージ）までをカバー
- 自治体のペアリングを前提とするため、自治体に閉じたネットワークではなく、自治体間で共有するサービスを持つネットワーク設計が必要
- 通常時の運用に加えて災害時の代替手段を各ConOps局面に応じて、優先順位をつけて定義
  - （例） 緊急期： 衛星回線に切替可能 or 自衛隊が準備している回線を使用 など
- 検討事項
  - 回線の確保
  - 帯域確保のための制約
  - ネットワーク設計
  - サービス設計
  - オンプレミス（データセンターや既存システムにおける）とクラウド等のすみ分け
  - サービス切り替えと復旧手順
  - セキュリティ設計

アプリケーション・アーキテクチャ

- 自治体業務全体の鳥瞰とICHIGAN RAスコープの定義
- 災害時において切り替え・代行が必要なサービスの定義
- 既存モデルであるAPPLIC, LASDEC等との関連・区分の定義
- オペレーションの共通化、局面・モードに応じたサービス優先順位定義
- 検討事項
  - アプリケーション・機能スタックの設計
  - ICHIGAN RAスコープ内のサービス、コンポーネント設計
  - ユースケースに応じたアプリケーション使用シナリオ
  - データモデルとの整合性
  - UX設計への要求定義
  - セキュリティ設計

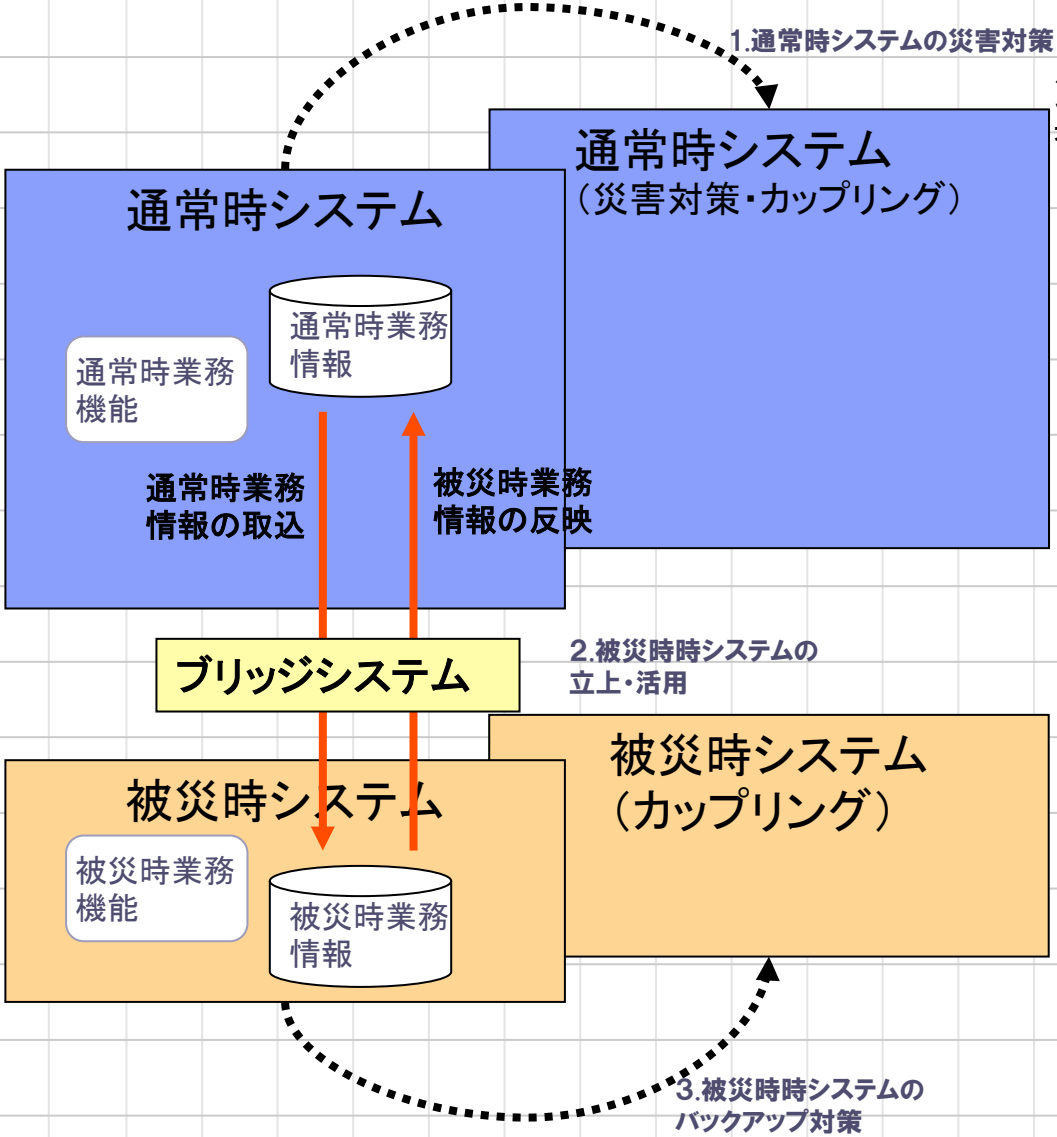
アプリケーション・アーキテクチャ概要
アプリケーション・スコープの定義



- ICHIGANにおけるアーキテクチャ分析の対象システムは、以下のシステムである。
  - 通常時基幹システム： APPLICに代表される、通常時自治体業務を支えるシステム
  - 被災時システム：LASDEC被災者支援システムやSAHANAに代表される、被災時に要求される自治体業務を支援するシステム
  - ブリッジシステム：被災時に通常時基幹システムと被災時システムとの連携を実現するシステム

- 突発的なシステム追加に対する実現可能性についても評価する。
  - 例：累積被曝量管理DBの新規開発、など

アプリケーション・アーキテクチャ概要
アプリケーション・アーキテクチャ概要の想定イメージ



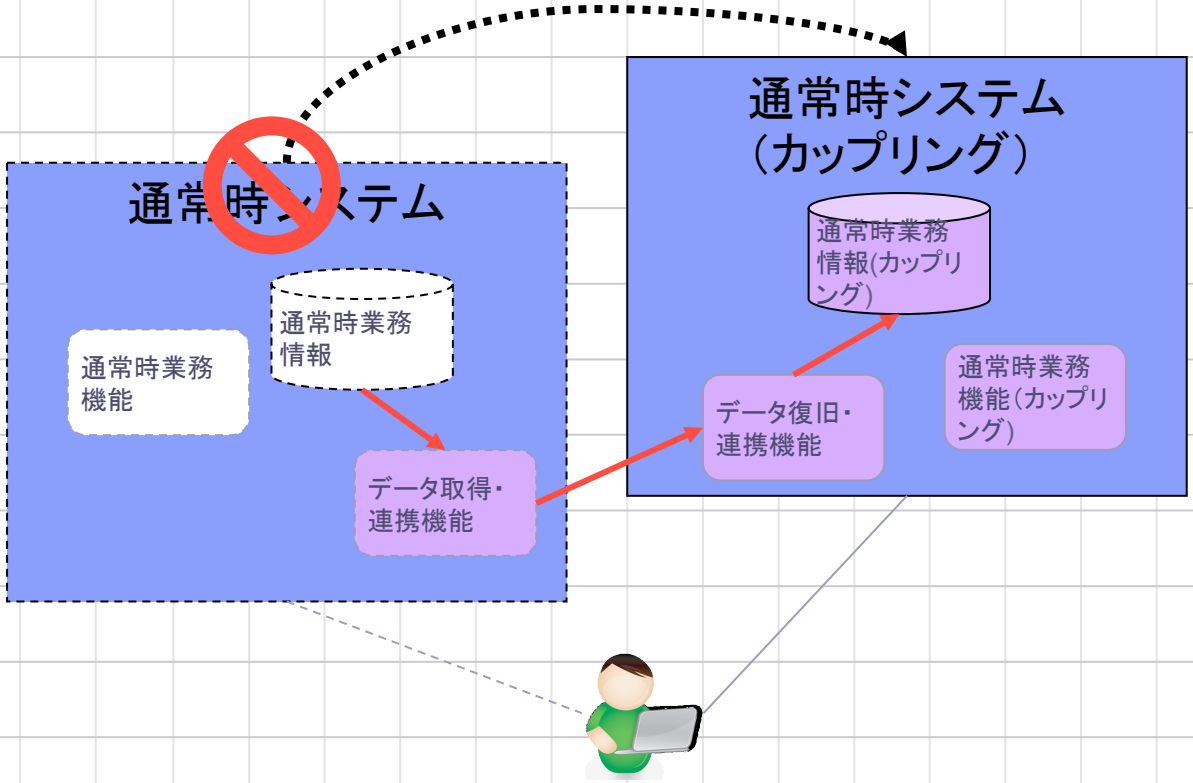
災害発生時において、以下の三つのシナリオを考慮したアーキテクチャーを検討する：

シナリオ１：通常時システムの災害対策
ホットスタンバイなどの復旧方式、カップリングなどの方式が考えられる。

シナリオ２：被災時システムの立上・活用
被災自治体内での被災時システム利用、支援自治体での被災時システム利用などが考えられる。
EXPORTファイルの連携、担当者による手動入力などが考えられる。

シナリオ３：被災時システムのバックアップ対策
被災時システムの二次災害対策なども同様に検討する。

アプリケーション・アーキテクチャ想定シナリオ
シナリオ1：通常時システムの災害対策



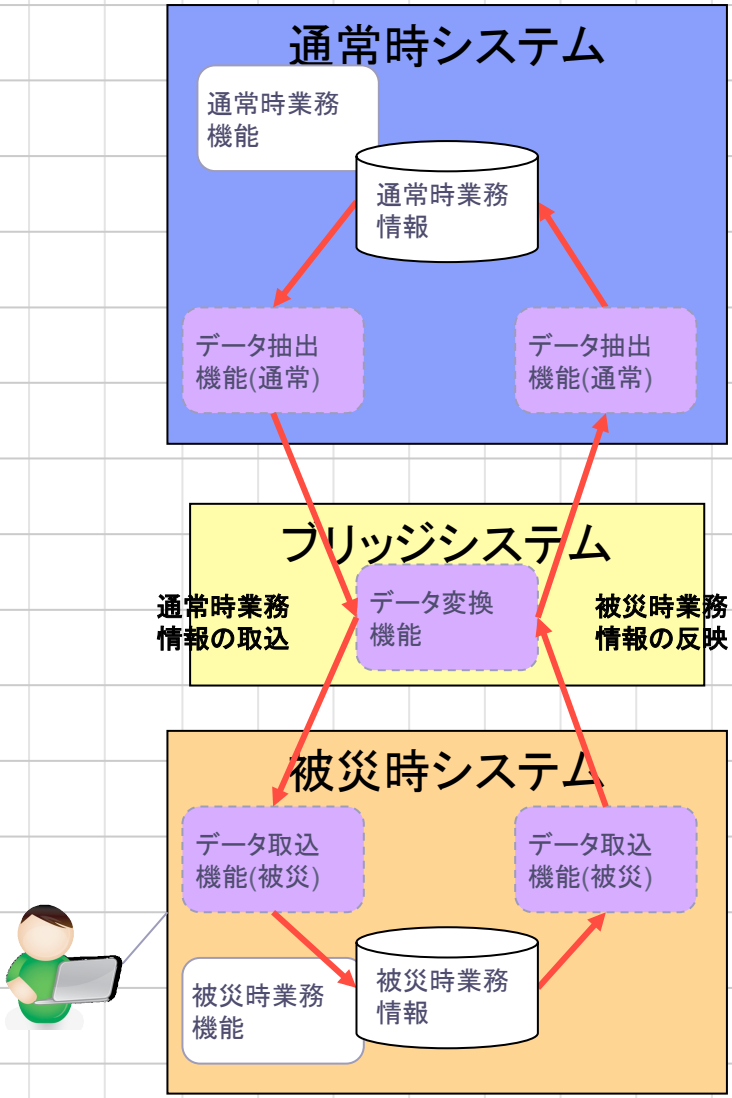
通常時システムが災害により被害を受けた時の、バックアップシナリオを想定する。

通常システムの災害対策の方法について：

- ホットスタンバイ、コールドスタンバイなどの**復旧／カップリング方式をパターン化**して検討を行う。
- 特定のデータセンターの被災など、一般的に検討される被災シナリオの適用を基本とし、大規模災害を想定した地域災害規模も考慮した検討を行う。

遠隔地でバックアップを稼動させる場合、カップリングした場合などに、必要なアプリケーション上の留意点、必要となるコンポーネント（業務機能、データ要素、プレゼンテーション機能など）の特性などについて、方式パターンごとに今後整理を行っていく予定です。(以降のシナリオにおいても同様です。)

アプリケーション・アーキテクチャ想定シナリオ
シナリオ2：被災時システムの立上・活用



被災時（応急期）のみに実施が求められる自治体業務を支える、被災時システムの立上および利用におけるシナリオを想定する。

- 被災者管理システム
- 被災所支援システム、など

通常時システムから被災時システムへの**情報連携の方式パターン**の整理が必要となる

- 住民基本台帳や税などの情報を想定する
- 方式パターン例：
  - データのExport / Import による連携
  - 印刷出力を手動でデータ転記、など
- ビジネスルールやポリシーを連携できる仕組みの必要性の検討

被災時業務で作成・更新した情報を、被災時システムから通常時システムに反映させる仕掛け

- 手作業反映、データロード、リラン、など

データ・アーキテクチャ

Project ICHIGAN

- 災害時においても最低限整合性が保障されるべきデータの定義、およびそれらを担保する機構
- サービス切り替え、モード切り替えに応じた、データ復旧手順（平常時のバックアップ手順と一対）およびデータ提供の仕組みを検討
- カップリングを前提とした際に、自治体業務を円滑に行うためのデータモデルの検討、自治体外部システムとのデータ連携の可能性を検討
- 検討事項
  - データモデル設計
  - データ物理配置設計（既存システムでのデータ配置およびクラウドベースの分散など）
  - バックアップ、リカバリー設計
  - 整合性保証のポリシー設計
  - セキュリティ設計

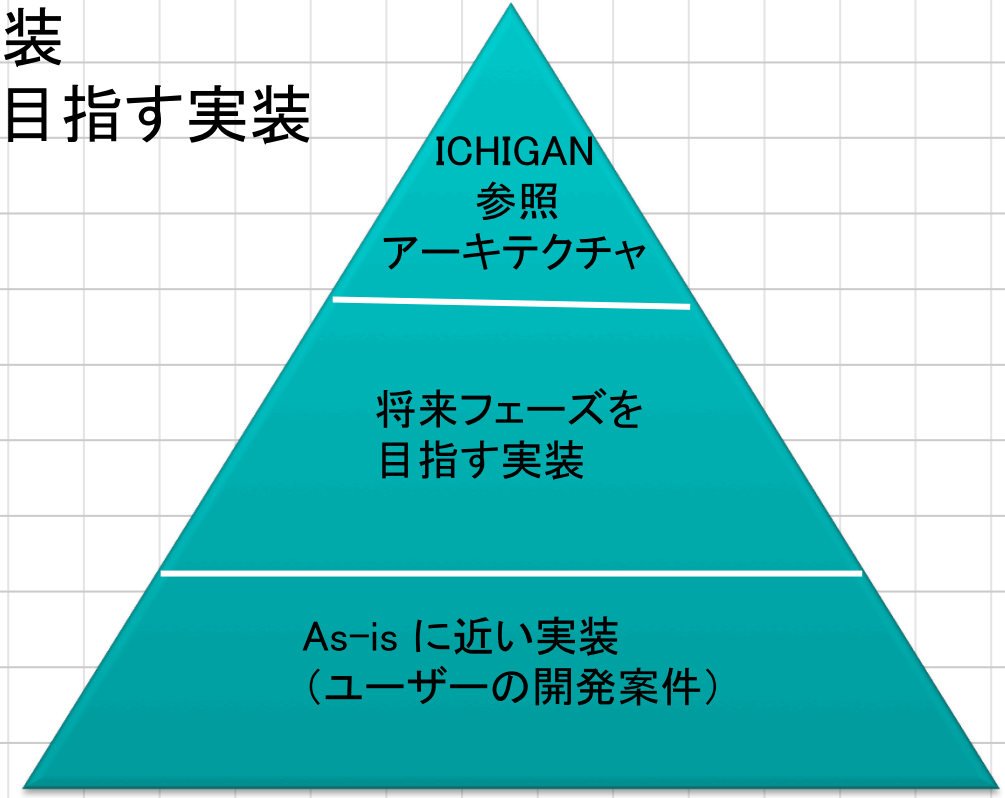
概要

- ConOps に準じて、ローカル（非ネットワーク接続）環境で動作可能であること
  - –応急期は入力データの制約条件を緩め、全てのデータの入力を可能とすること
  - –入力データは時系列に追記
  - –復旧期に入力データの精度の改善を行う
  - –転送データはテキスト形式とする
- 論理モデル
  - –現システムの登録済みデータ以外の住民の居所、避難場所、支援物資の情報などを扱う
  - –マッチング機能などの提供
  - –GIS などのメタデータ定義

To-be モデルの提供の狙い

- 先進技術を考慮した参照アーキテクチャにより、
  - –As-is に近い実装
  - –将来フェーズを目指す実装

  を可能とする



応急期データのイメージ

Project ICHIGAN

自治体システム
（通常業務データのバックアップ）

変換

メタ定義

応急期データ

XML 版

JSON 版

CSV 版

スマートフォン／タブレット

ノートPC

応急期用
デバイス

※現地ではネットワークが使えない事が前提

ローカルデータとして格納

【入力手段】

・Excel ・HTML5+LocalStorage ・ローカルアプリケーション

災害対策本部、支援組織

自治体システム（災害対策）

避難所管理

支援管理

犠牲者管理

自治体システム（災害対策データ）

変換

メタ定義

避難所や災害現場で入力した
データは、デバイス毎持参するか
媒体送付等で届ける

避難所

災害現場

・避難所情報入力
・支援要望入力
・安否入力

・支援要望入力
・安否入力
・犠牲者入力（身元判明者／身元不明者）

代表的なユースケース

- データの分散管理
- 復旧段階に応じた動作
- サービスの切り替え
- オフライン動作
- データの複製とバックアップ
- プライバシー保護
- 権限委譲

データ管理に関する ConOps の場合分け

カップリング可能

ConOps モード	最小：復旧可能条件	制限（応急期）：ネットワーク分断（役所内）	縮退（応急/復旧期）：サプライチェイン障害	代替（応急/復旧期）：代替の組織、サプライチェイン	通常
メタデータ（同期複製）	○	○ 非複製あり	○	○	○
基本データ（同期複製） 住民記録、固定資産税	ー	○ 非複製あり	○	○	○
周辺データ（非同期複製）	ー	古い	○	○	○
バックアップ（非同期）	古い	古い	古い	古い	古い
サプライチェイン	ー	古い	古い	○ 切り替え	○
監査ログ（非同期複製）	ー	○ 非複製あり	○	○	○

（遷移条件、制約の組み合わせや優先度、組織の人的な制約を定義する）

ユーザーエクスペリエンス設計

Project ICHIGAN

- アプリケーション・アーキテクチャに応じたUX定義
- ConOps局面・モードにおける最適UXの設計（CUI, GUI, Web…）
- オンライン/オフライン双方でのオペレーションを柔軟に切り替え可
- オペレーションの共通化・区分化の検討
- 検討事項
  - アプリケーション・アーキテクチャとの整合性
  - 局面・モード別最適UX設計
  - セキュリティ設計

セキュリティ＆プライバシー

- アーキテクチャ全レイヤーに共通なセキュリティ・ポリシーの定義
- ConOps局面およびモードに応じた認証方式検討
- Delayed Authentication
- 検討中の共通番号（国民ID）方式等との整合性検討
- プライバシー・データの取り扱いポリシー
- ログおよび監査・追跡性の検討
- 検討事項
  - セキュリティ・ポリシー定義
  - 認証方式・権限委譲方式
  - アプリケーション、UX、データ・アーキテクチャとの整合性

ライフサイクル・プロセス

- ICHIGAN RAを使用するライフサイクル・プロセスの定義
- ICHIGAN RAを改訂・運用するライフサイクル・プロセスの定義
- 上記プロセスにおけるキーとなる工程の設計
- ICHIGAN RA評価シナリオを使用するアーキテクチャ評価プロセス定義

ICHIGAN RA文書の構成

- ICHIGAN RA
- ICHIGAN RA利用技術ロードマップ
- ICHIGAN RA評価シナリオおよびチェックシート
- ICHIGAN RA用語集
- ICHIGAN RA著作権等IP関連文書

ICHIGAN RA本体

- コンセプト・オブ・オペレーション定義
- 想定シナリオおよびビジネス・ユースケース（ICHIGAN RAスコープ）
- 想定機能要求および非機能要求
- セキュリティ・ポリシー
- アーキテクチャ鳥瞰資料
- 各アーキテクチャ・レイヤ仕様
  - 業務機能仕様
  - 業務コンポーネント仕様
  - データ・モデル
  - データ・サービス物理仕様
  - ネットワーク仕様
  - クラウド・サービス仕様
  - ユーザー・エクスペリエンス仕様
  - 運用設計
  - …
- 他システムとの連携
- ICHIGAN RAを設計に利用するための開発プロセス
- ICHIGAN RAを改善するための運用プロセス

その他のICHIGAN RA文書

- ICHIGAN RA利用技術ロードマップ
  - –ICHIGAN RAのリリース時点では仕様に含めないが、将来適用可能な技術を取り入れた構想をRAのリリース時および更新時に併せて検討し、公開する
- ICHIGAN RA評価シナリオおよび評価チェックシート
  - –ICHIGAN RAの観点から既存システムのアーキテクチャ構成を評価するためのシナリオおよび評価ポイントをリストしたチェックシートを提供する
- ICHIGAN RA用語集
  - –ICHIGAN RAで新たに定義した用語
  - –従来から自治体システムおよび業務で使用されてきた用語
- Project ICHIGANの成果は、オープンソースと同様、社会の共有知として無償公開する予定。利用規約に関しては今後の検討事項。

今後ともご支援をよろしくお願いします

Project ICHIGAN