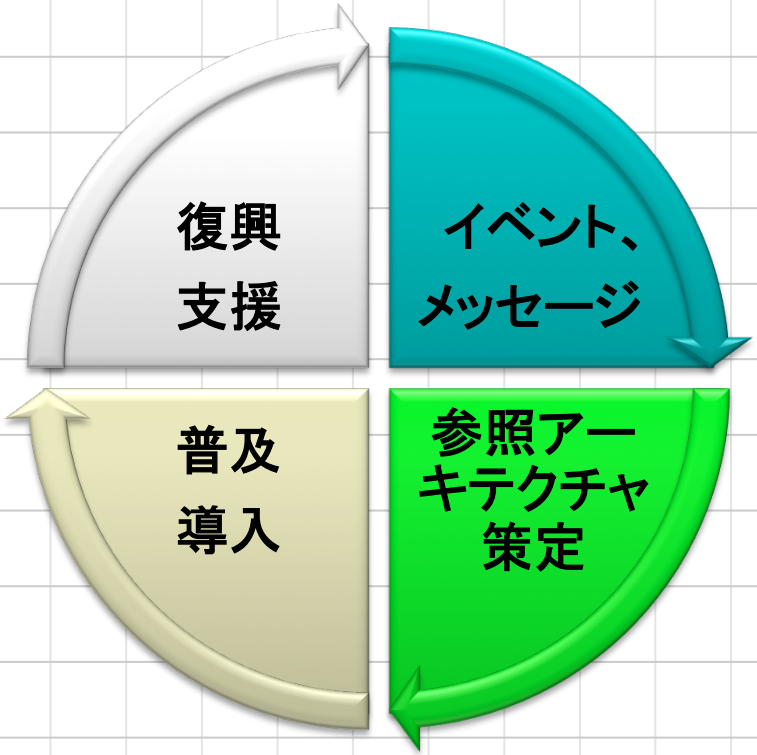
Project ICHIGANの目指す新しい自治体ITアーキテクチャのあり方

2012年3月8日　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

2012/3/24 新宿合宿

2012/2/16 デブサミ

2012/1/28 新宿合宿

竹洞陽一, 吉田裕之

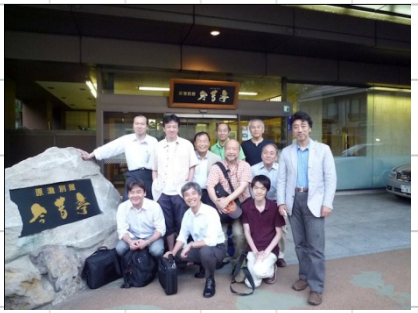
2011/10/19 モデリングForum

2011/9/27 中間報告会@NII

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

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。

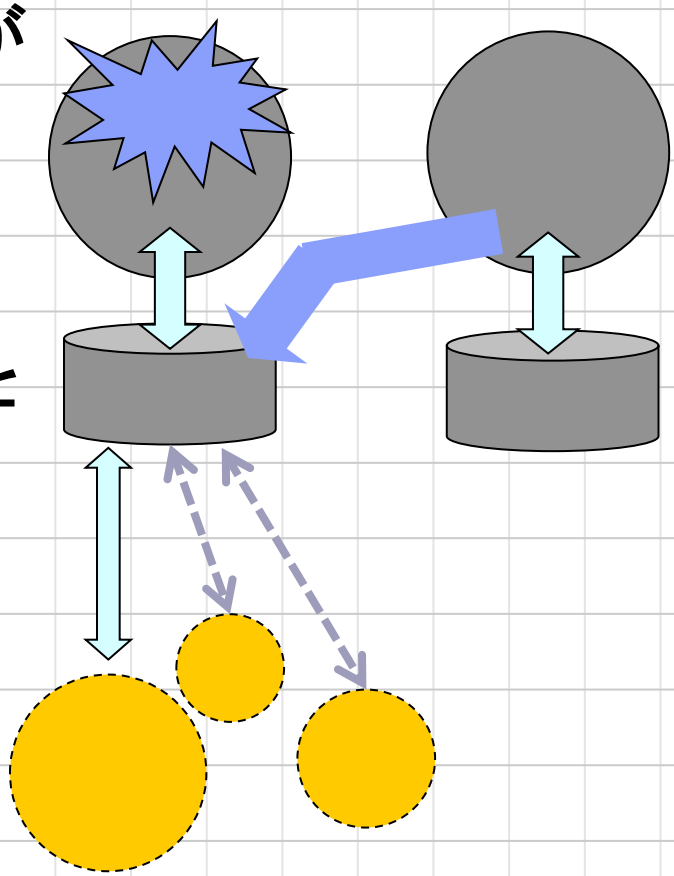
ICHIGAN 参照アーキテクチャ (ICHIGAN Reference Architecture)

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・モデルとは、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3つのポイント

- 地域間でのシステムの柔軟な連携
  - –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（カップリング）が可能となるようにする
- 体制やモードの区別に応じた対応
  - –業務も運用もシステム自体も、平常時、警戒期、応急期、復旧期といった区別とそれらの移行に対応できるようにする
- 有事システムとの柔軟な連携
  - –避難所管理システム、安否確認システム等の被災時システムと通常時システムとの接続が容易になるようにする

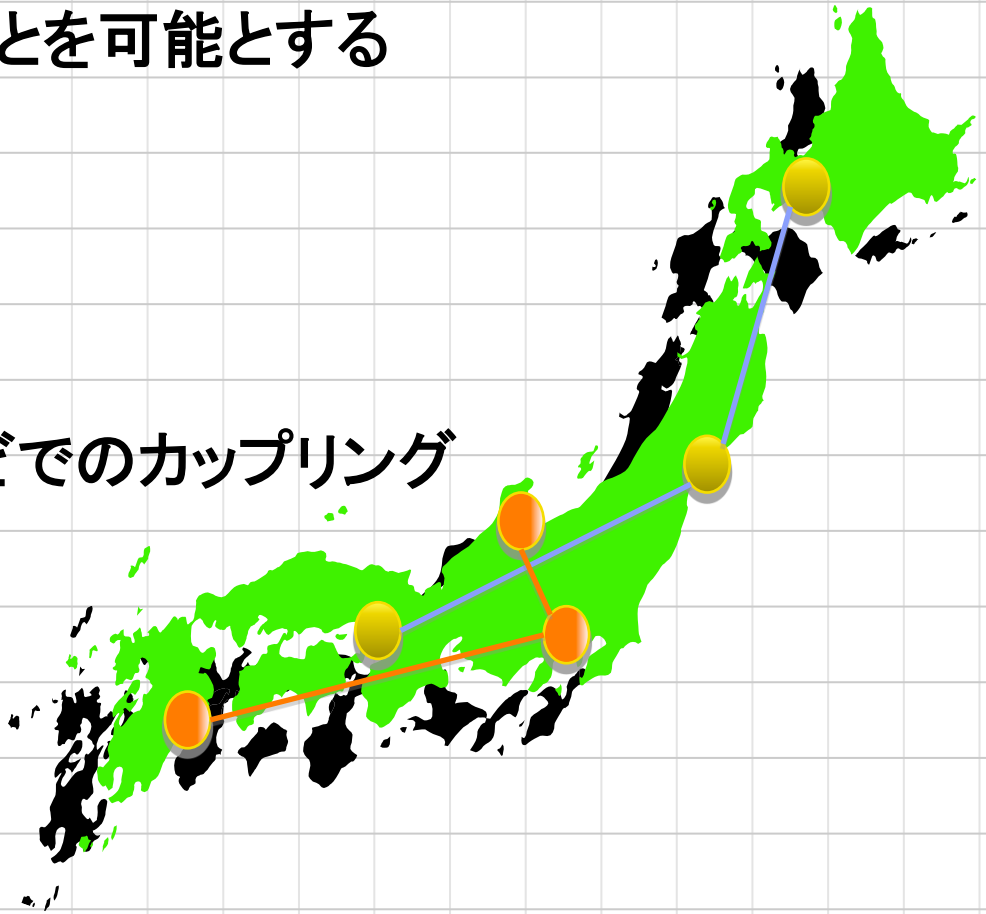


ICHIGAN RAが考えるシステム運用

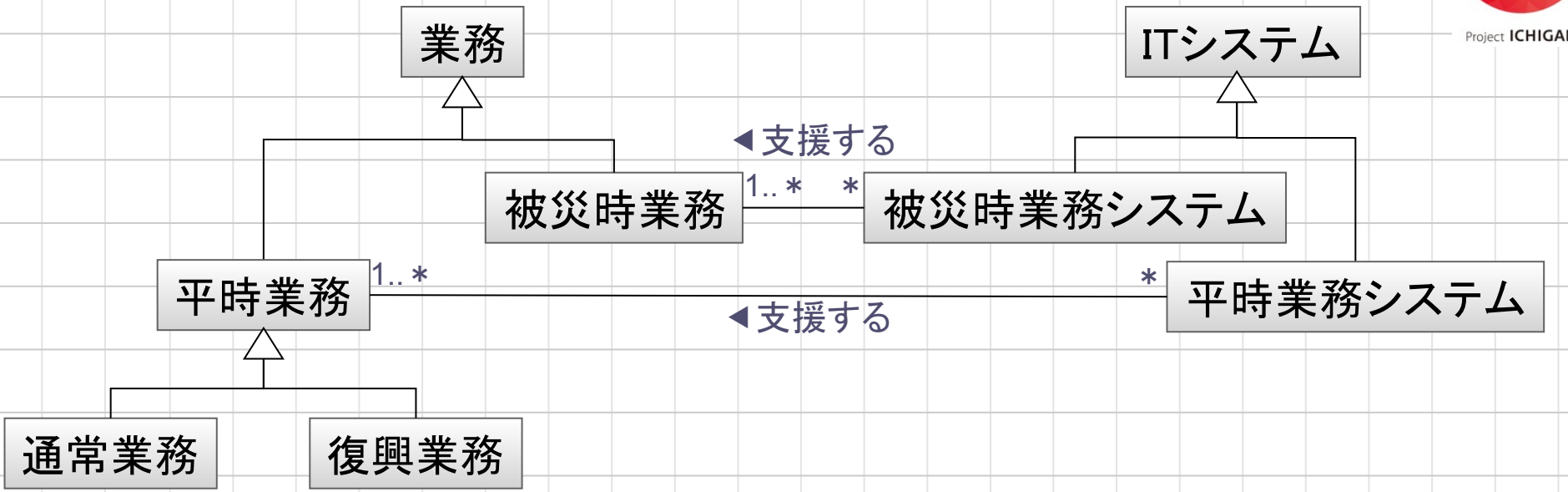
Project ICHIGAN

複数（2ないし3）の地方自治体どうし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

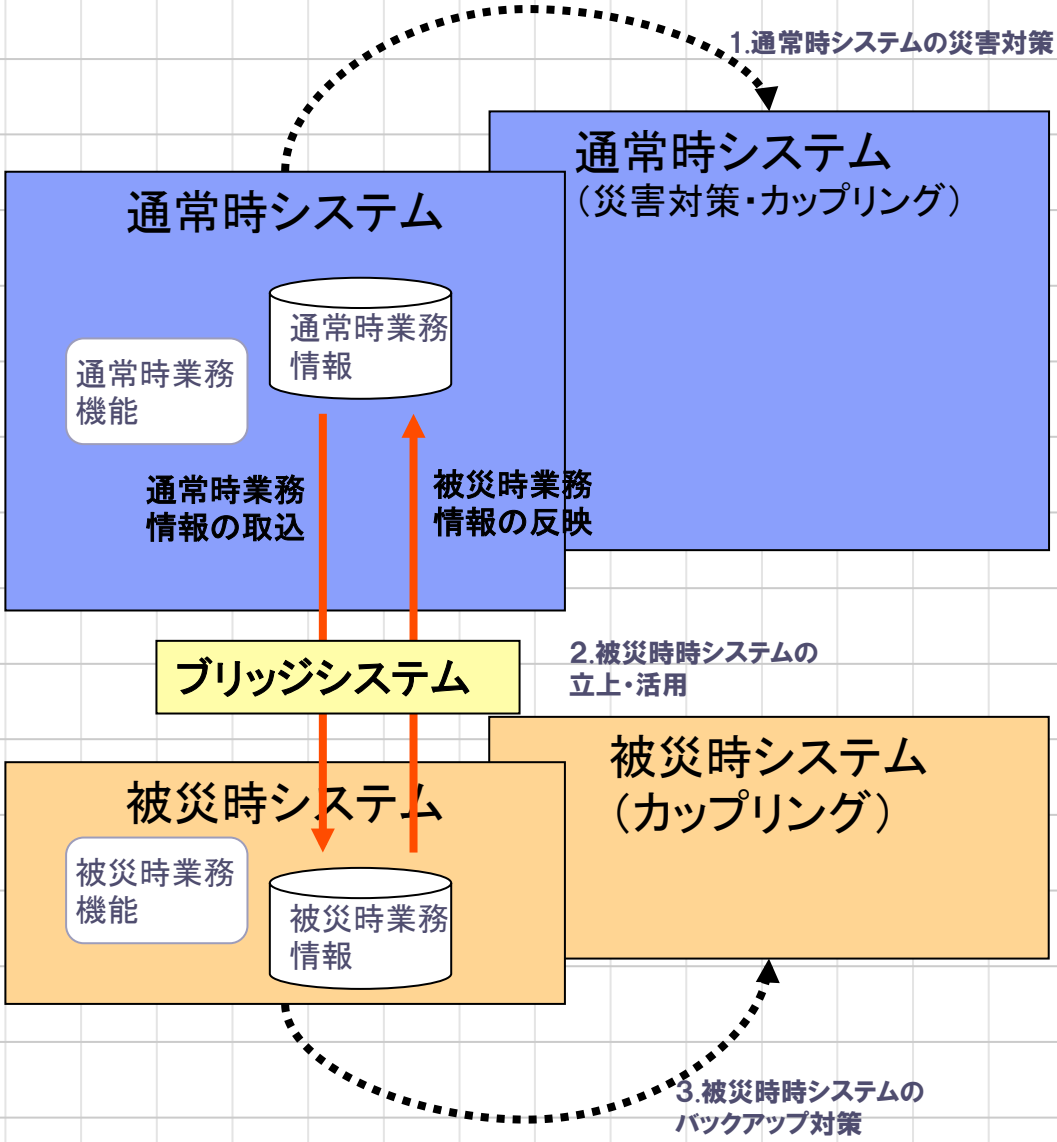


平時業務・被災時業務

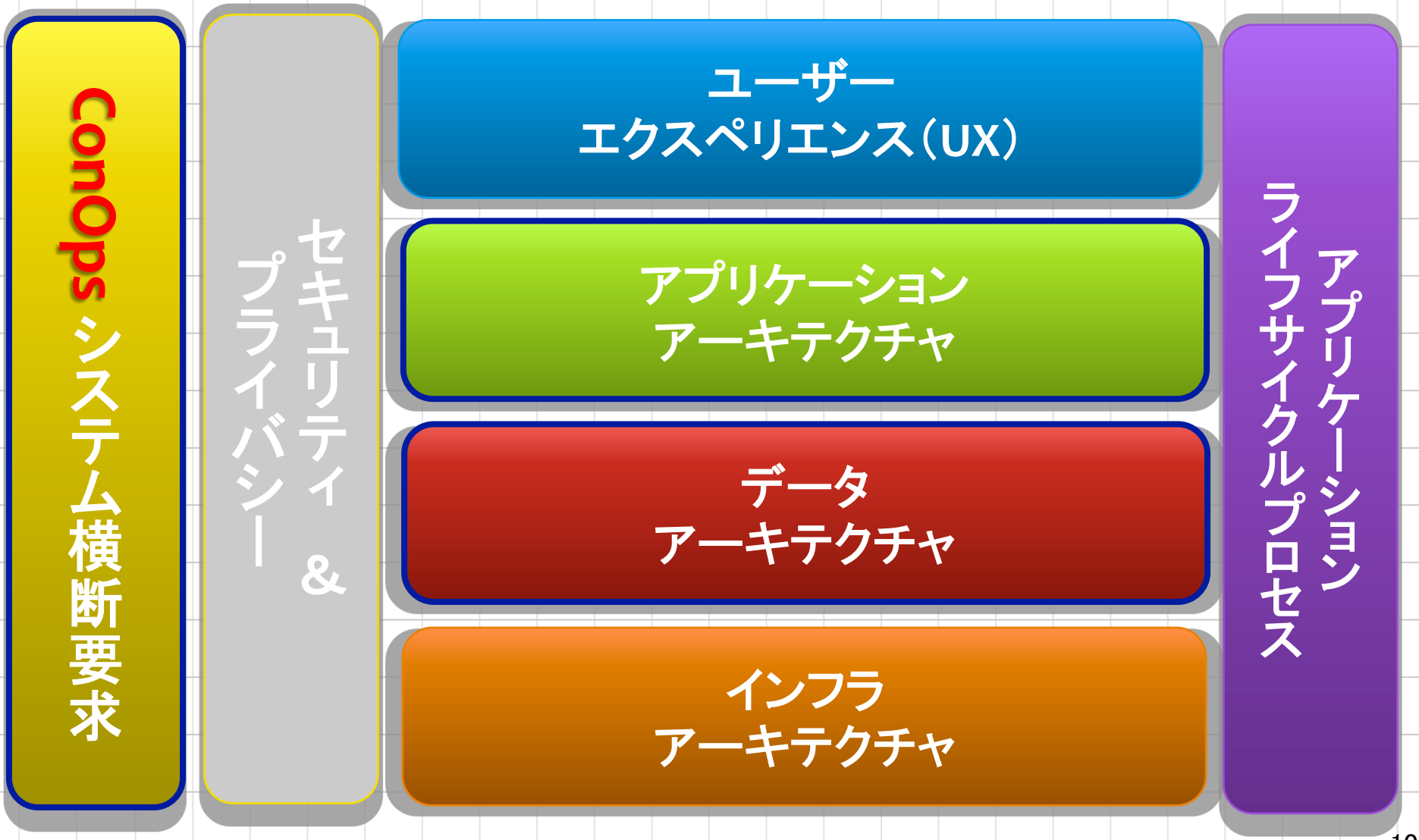


- 「平時業務」とは、主として平時に住民サービスを提供する業務であり、通常業務と復興業務に分類される。
- 「復興業務」とは、復興期に地域復興のために特別に遂行される業務である。復興業務ではない平時業務は「通常業務」である。
- 通常業務は、被災時において遂行リソース（人員・電力・通信等）が不足すると、平時とは異なる業務モードで遂行されることがある。
- 「被災時業務」とは、主として被災時に特別に遂行される業務であり、平時には訓練や支援システムの準備・保守以外の作業は遂行されない。

想定するアーキテクチャのイメージ



ICHIGAN参照アーキテクチャ（RA）



ICHIGAN参照アーキテクチャとは？

- 実装のためのアーキテクチャそのものではない
  - アーキテクチャ例を示し，その背景となる考え方を示す
  - 従ってすぐにそのまま利用できるアーキテクチャとはなっていない
  - 個別自治体で適宜カストマイズしながら利用することを前提.
- 実装アーキテクチャを作るための枠組みである
  - アーキテクチャの考え方
  - アーキテクチャの定義例
  - アーキテクチャの書き方
  - アーキテクチャの指定方法

ICHIGAN
参照アーキテクチャ成果物

- アーキテクチャ 分析ガイド
- アーキテクチャ 分析チェックリスト
- アーキテクチャ 構築ガイド
- アーキテクチャ 参考定義例・技術例
- アーキテクチャ 参考実装（UX）

システム横断要求=運用構想ConOps

Project ICHIGAN

- コンセプト・オブ・オペレーション　ConOps
  - 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

ConOps目次(IEEE1362の例)をICHIGAN用にカスタマイズ

1. スコープ(Scope)
   1.1 プロジェクト名
   1.2 本書の概要
   1.3 システムのオーバービュー(System overview)
3. 現行システム(Current system)または場面・状況(Situation)
4. 本質的な変更(Nature of Change)と正当性(Justification) → 想定する業務環境の定義（Needs/Gap）
5. 提案システムのコンセプト(Concepts for the proposed system)
   5.1 背景・目的・範囲
   5.2 ポリシーと制約
   5.3 提案システムまたは場面・状況の説明
   5.4 オペレーションモード
   5.5 ユーザーとその他関係者
   5.6 支援環境
6. 運用シナリオ（Operational scenarios)
7. 影響の要約(Summary of impacts)
8. 提案システムの分析(Analysis of the proposed system)

参考資料：

IEEE Std 1362-1998, IEEE Guide for Information Technology - System Definition - Concept of Operation Document,

IEEE Std 1362-1998 非公式翻訳（メタボリクス　山田正樹氏)

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？

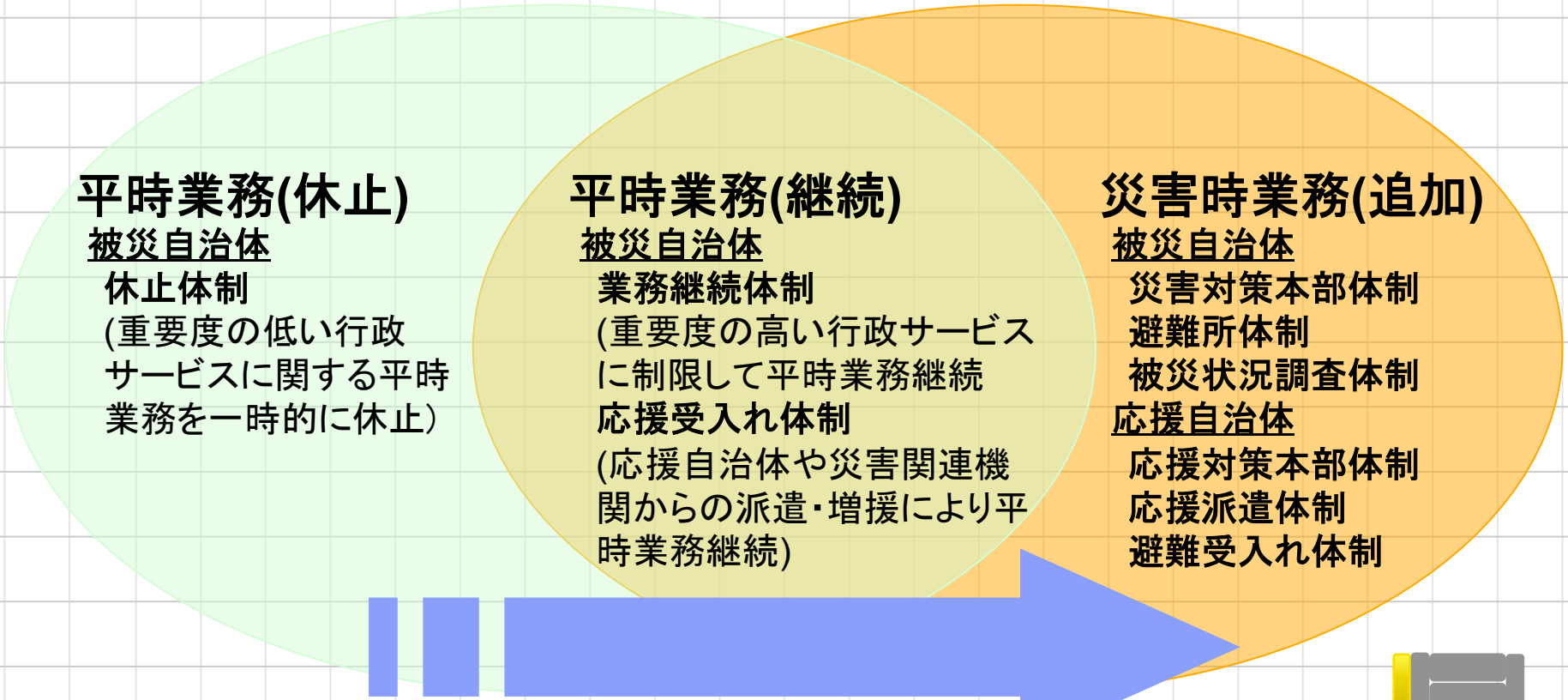
欧米の公的機関では、緊急時対応計画のシステム調達に関して、災害時のシナリオを想定した運用構想を作成している

- 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？

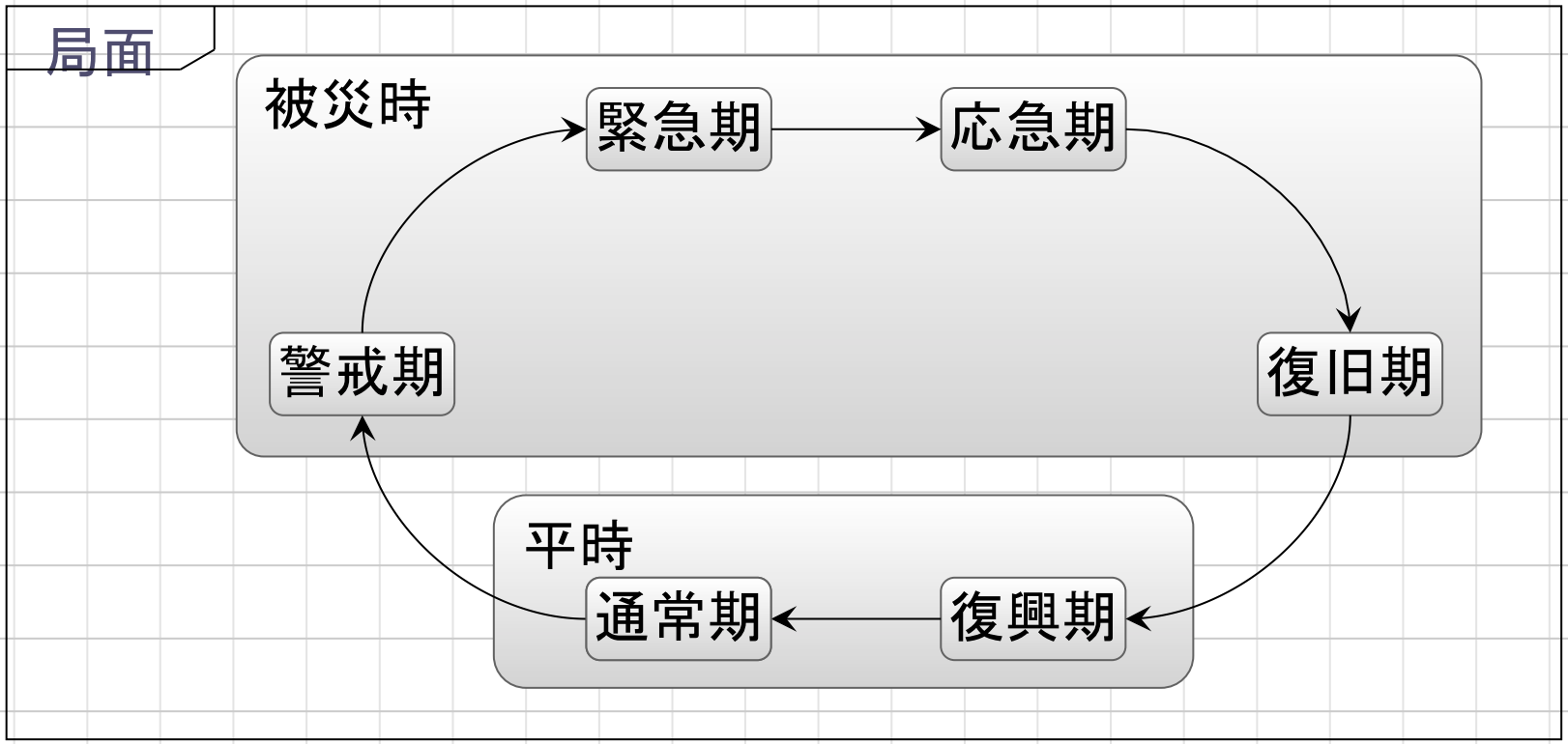
被災自治体は、災害対策本部体制/避難所体制へ、
応援自治体は、救援体制/避難者受入れ体制へ、組織の編成を変える



局面

- 通常期：災害による被害が無い状態。自治体業務の観点から災害発生以前の状況に完全に戻った状態。
- 警戒期：災害の発生が予期され、住民の避難、職員の待機、システムの移行準備などが行われる状態。
- 緊急期：災害が発生し、人命救助、被害状況の把握などが最優先される状態。
- 応急期：通常業務の再開が求められ、重要なもののみ不十分なリソースで遂行する状態。
- 復旧期：業務を通常期と同様に遂行できるように準備を進めている状態。
- 復興期：通常業務を災害発生以前と同様に遂行することに加えて、地域復興のための特別な業務を遂行している状態

局面の遷移



- 警戒期～復旧期をまとめて「被災時」と呼び、通常期・復興期を「平時」と呼ぶ

【注】
- この遷移は標準的な順序関係だけを規定している。実際には、警戒期から通常期に戻るなど、途中をスキップした遷移がありうる。

自治体システムは、災害時の組織体制に適合した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。

- 本番サービス・モード(Production Service mode)
  - 通常モード(Normal mode)
  - 能力縮小モード(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)
- 開発・テストモード(Development and Test mode)
- 訓練モード(Training mode)
- 保守モード(Maintenance mode)

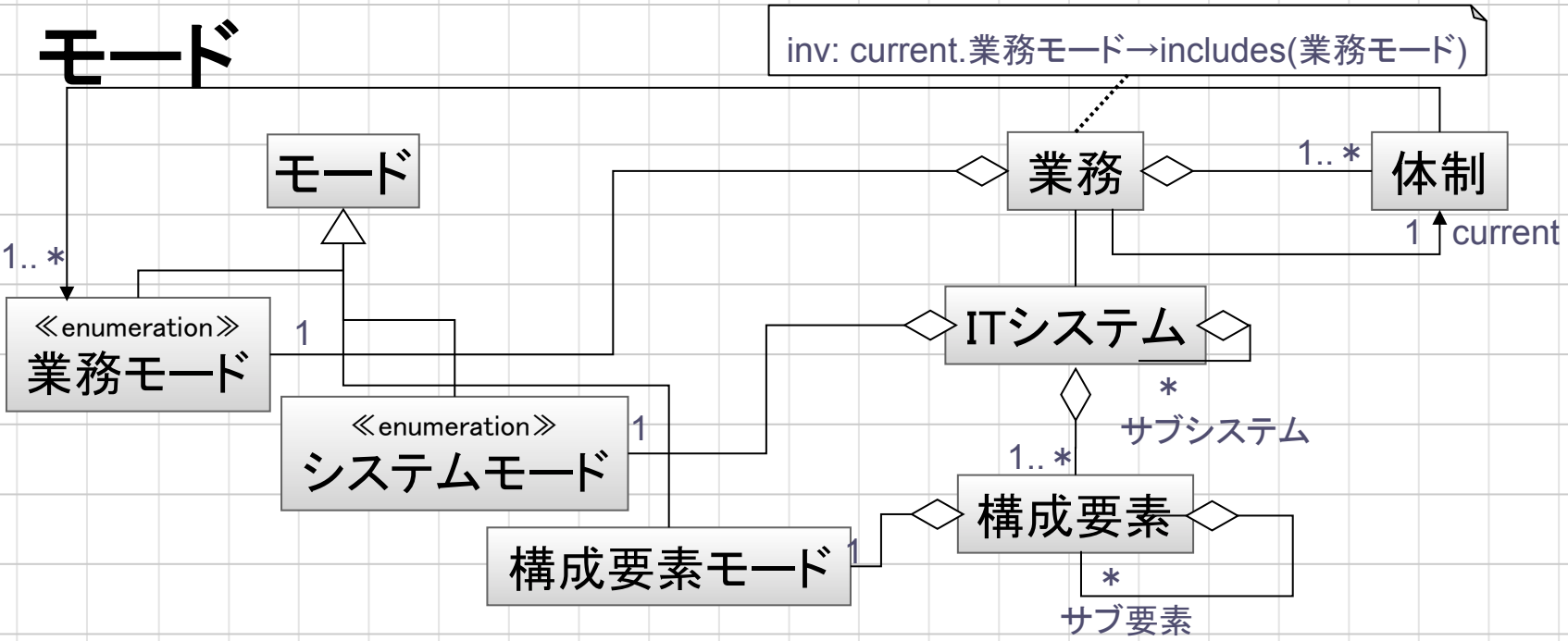
・・・・・・など

- 接続モード/オンライン-オフライン(Online-Offline mode)
  - クライアント接続モード
  - 外部システム接続モード
  - 平時システム接続モード（災害時システムのみ）
  - 災害時システム接続モード（平時システムのみ）
- UIモード(User Interface mode)
  - テキスト・モード
  - グラフィック・モード
  - 音声モード　他
- システム運転モード(IT system operation mode)
  - 自動運転モード
  - 手動運転モード

・・・・・・など

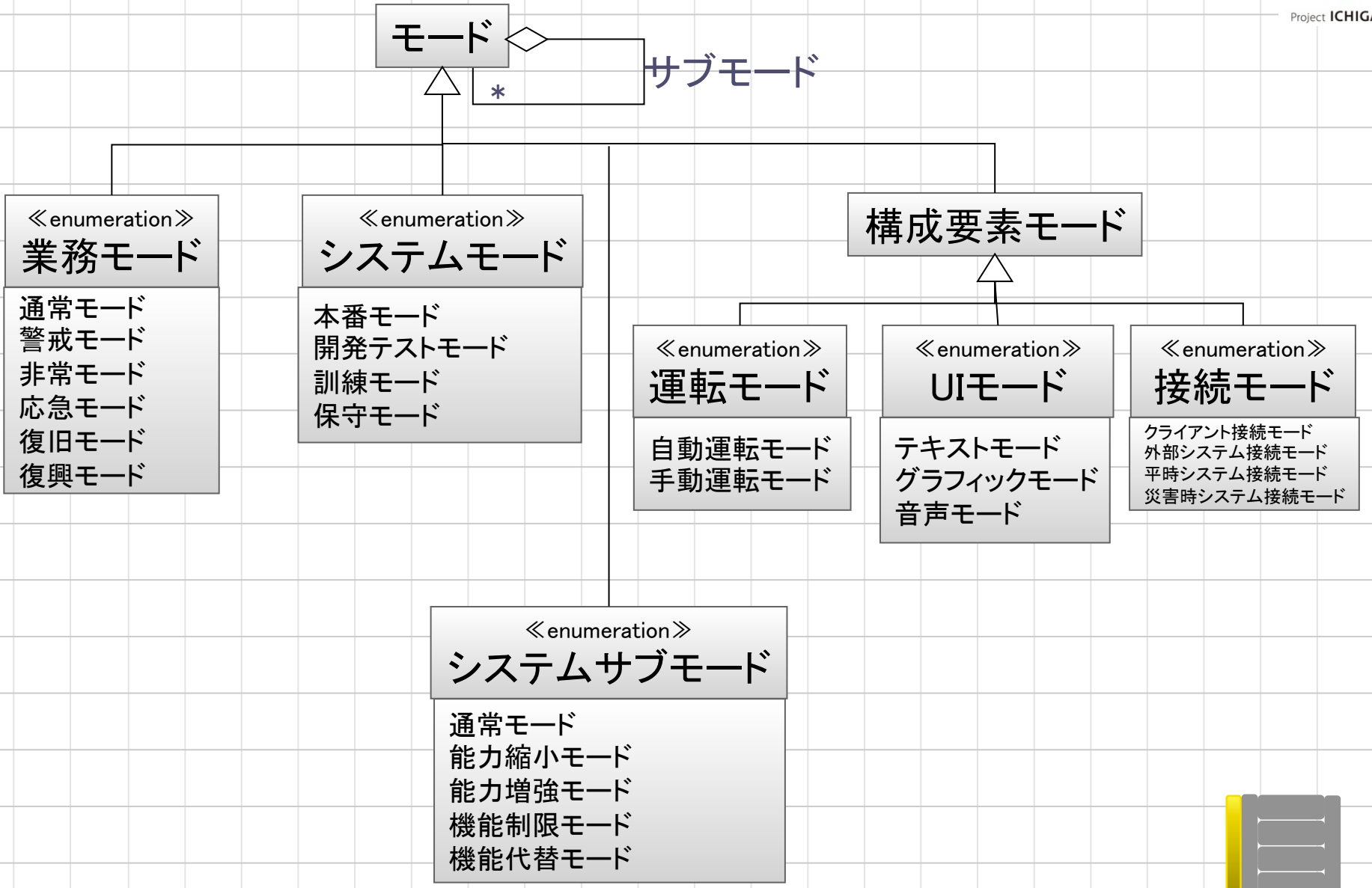
災害局面の場面・状況により変化する組織体制と業務に対応できる自治体システムのモードを手動または自動で切り替える機能を提供する必要がある。

モード



- 「モード」とは、災害対策の観点での業務・ITシステムの状態である。
- ITシステムは「サブシステム」や「構成要素」に分割できる。
- 現時点で業務をどの体制で遂行するかは、業務のモードによって規定されている。

モード


モード
サブモード
*
≪enumeration≫
業務モード
通常モード
警戒モード
非常モード
応急モード
復旧モード
復興モード
≪enumeration≫
システムモード
本番モード
開発テストモード
訓練モード
保守モード
構成要素モード
≪enumeration≫
運転モード
自動運転モード
手動運転モード
≪enumeration≫
UIモード
テキストモード
グラフィックモード
音声モード
≪enumeration≫
接続モード
クライアント接続モード
外部システム接続モード
平時システム接続モード
災害時システム接続モード
≪enumeration≫
システムサブモード
通常モード
能力縮小モード
能力増強モード
機能制限モード
機能代替モード

業務モードとシステムモードの関係の例

戸籍謄本業務	戸籍謄本平時システム	戸籍謄本被災時システム
通常モード	本番モード[デフォルト] 訓練モード[訓練時] 保守モード[保守時]	待機モード[デフォルト] 準備モード[警戒期]
非常モード	待機モード[デフォルト]	待機モード[デフォルト]
応急モード	縮退モード[デフォルト]	本番モード[デフォルト]
復旧モード	開発テストモード[テスト時] 本番モード[可能な場合]	本番モード[デフォルト]

ICHIGAN RAは、応急期の場面と状況に対応する災害時システムのモード から取り組んでいる

Project ICHIGAN

局面	場面	状況	組織の運営体制	情報システムのモード
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（本番サービス・通常モード） 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等のに移行する（本番サービス・機能代替モード）
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－データセンター復旧、データ不整合、避難所ネットワーク低品質	災害対策本部体制 避難所運営体制	復旧した平時システムで重要な行政サービスの業務を継続する（能力縮小モード、機能制限モード） 災害時システムを立ち上げ、ネットワーク品質が悪い避難所において、タブレットやスマホンで災害時アプリとデータを利用する（クライアント接続オフライン・モード） 平時システムや災害関連機関と連携する（平時システム／外部システム接続・オンライン・モード:） データ不整合があるため、例外やエラー発生時にシスオペが対応する（システム手動運転モード）
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）

ライフサイクルとビジネスアクターを軸に、ハイレベルな業務シナリオを整理

Project ICHIGAN

		局面					
		警戒期	緊急期 (24時間？)	緊急期⇒応急期 (48時間？)	応急期 (避難所生活、仮設住宅に移動するまで)	応急期⇒復旧期	復旧期
業務領域	被災住民記録						
	被災者基本台帳						
	安否確認						
	被災者支援						
	犠牲者 遺族管理						
	避難所 物資管理						
	避難所管理						

【Conops/AAチームのお勧め】
・緊急期から応急期への遷移におけるシナリオ
・災害対策本部の設置シナリオ

赤字は、Ⅱに関連すると思われる業務シナリオ。
一覧対象の業務シナリオとする。

ビジネスアクター	被災自治体職員	・災害対策本部の設置（readyness確認、被災者支援システムの立上、データバックアップ、データ移行など）	・災害規模／被害状況を確認する ・被害状況や避難所の情報を住民に提供する ・支援自治体、警察などに支援要請	・被災者支援用システムの立上（データ移行などの発生、ネットワーク回線の確保、システム設置場所／電源の確保など） ・避難者の本人確認 ・被災者の安否確認 （セキュリティモードの切り替え） （通常時システムは継続稼働している前提）	・被災者支援用システムの利用（例えば） ・安否情報（所在地含む）の公開 ・支援物資の調達／配送 ・医療サービスの手配／提供（感染症、常備薬、妊婦など） ・傷病者情報と避難者情報の連携 【UXモードの切り替え】 ・支援用システムの調達	・被災者支援用システムの通常時システムへの遷移（データ移行などの発生）	
	支援自治体職員		・被災自治体（カップリング自治体）の状況を確認する ・支援要請を受けて、支援準備を行う	・支援業務実施のための準備 （セキュリティモードの切り替え） （ネットワーク回線の確保など）	・被災者支援用システムの利用 【UXモードの切り替え】	・カップリング状態から、通常モードへの戻し（セキュリティ、UXモードの切り替え）	
	被災自治体住民（住民票あり）		・被害状況の確認 ・自治体からの指示の確認 ・避難所へ避難する	・避難所に避難する ・安否情報を提供する （セキュリティモードの切り替え）	・被災者支援用システムの利用 ・安否情報を確認する	（仮設住宅への移動） ・被災者支援用システムの利用縮退	
	被災自治体居住者（住民票なし）		同上）	・避難所に避難する ・安否情報を提供する	・被災者支援用システムの利用 ・安否情報を確認する	（仮設住宅への移動） ・被災者支援用システムの利用縮退	
	医療機関	TBD）	TBD）	・避難者の傷病情報の収集 ・傷病者情報を自治体に提供する	・傷病者情報と避難者情報の連携	TBD）	TBD）
	警察・消防・自衛隊		・自治体の要請に応じて被災者救助を行う	・被災者救助の継続	N/A）	N/A）	N/A）
	契約企業		N/A	N/A）	・支援用システムの構築 ・仮設住宅、瓦礫処理などの受注	N/A）	N/A）
	支援団体・ボランティア		N/A	N/A）	N/A）	N/A）	N/A）
	日本国政府		・被災自治体の被害状況を確認する ・自衛隊などへ出動要請を行う	N/A）	N/A）	N/A）	N/A）

インフラストラクチャ・アーキテクチャ

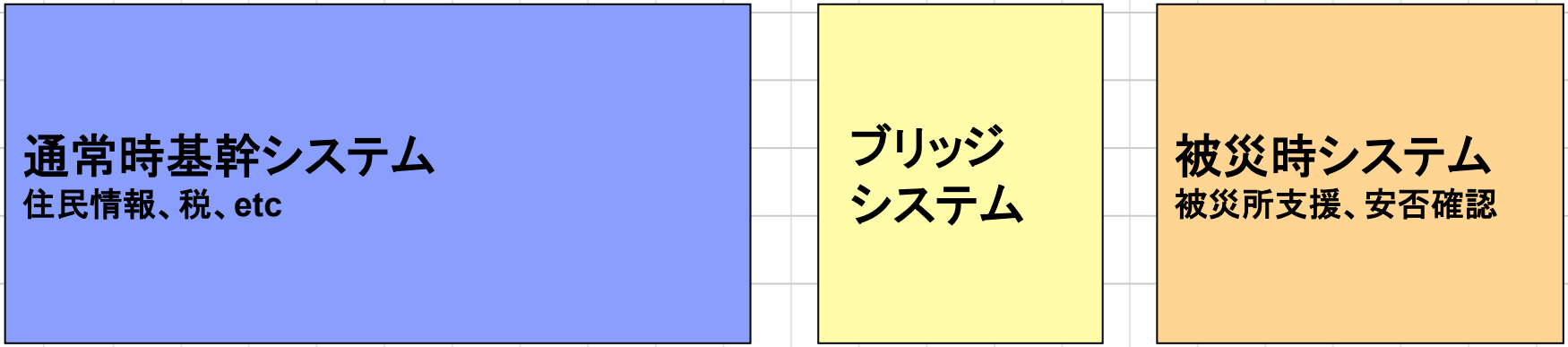
Project ICHIGAN

- 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
- 自治体のカップ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

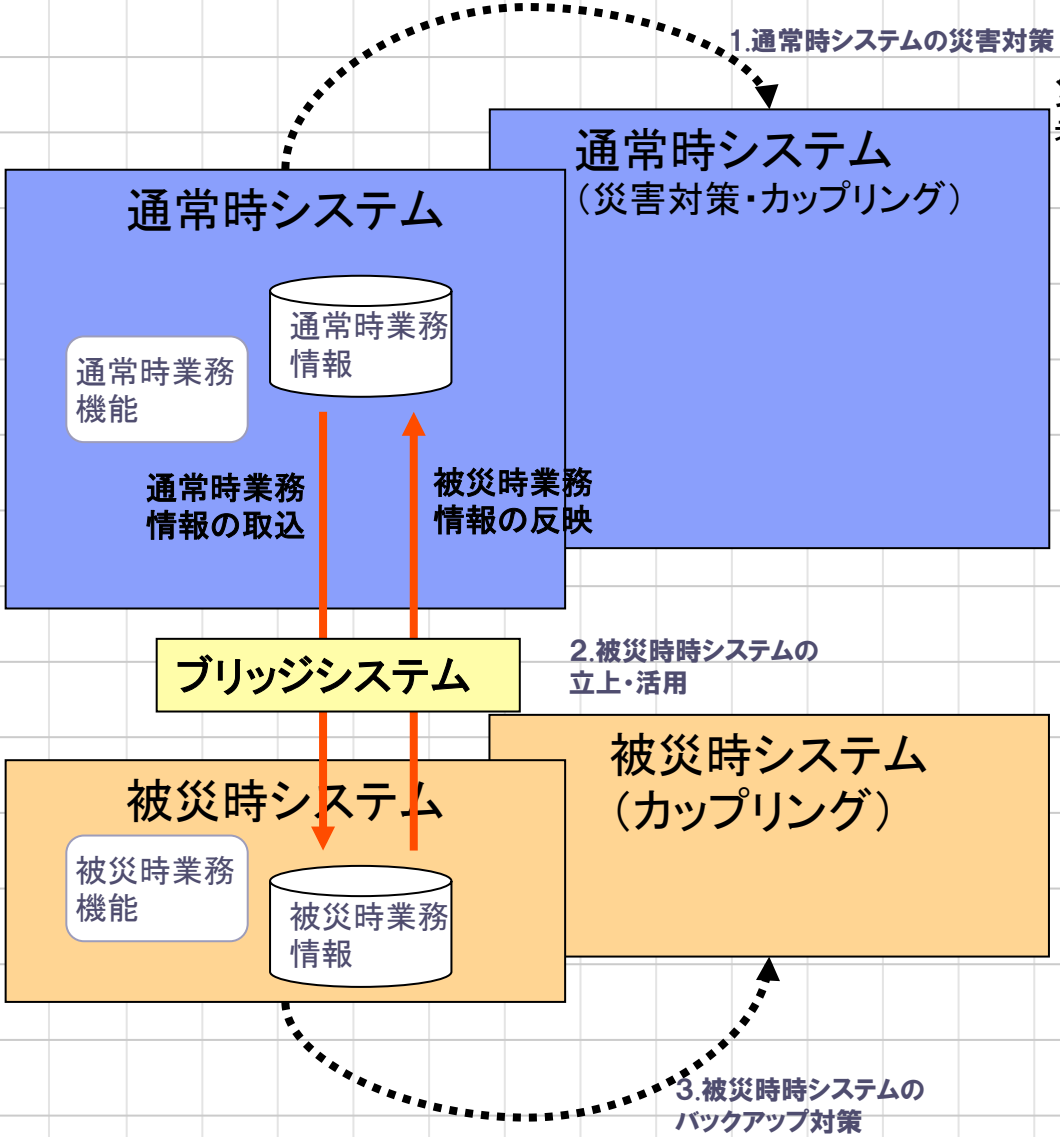
アプリケーション・アーキテクチャ概要
アプリケーション・スコープの定義



- 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



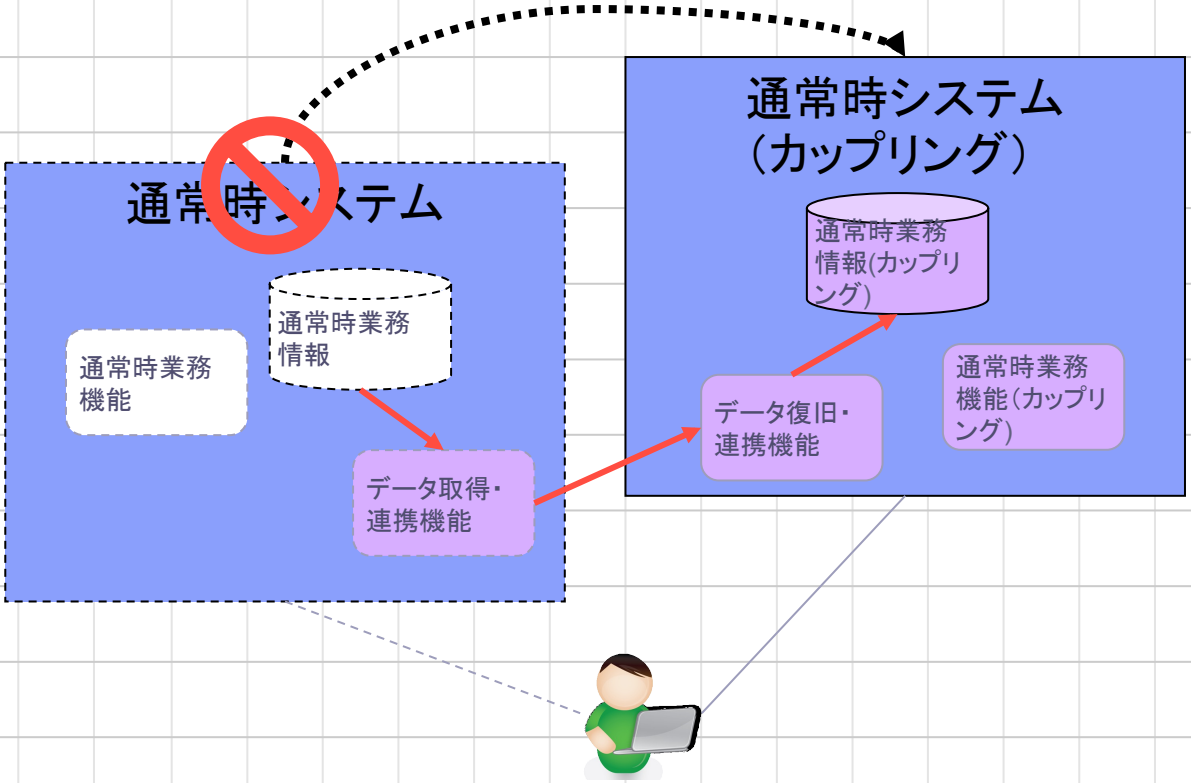
災害発生時において、以下の三つのシナリオを考慮したアーキテクチャーを検討する:

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



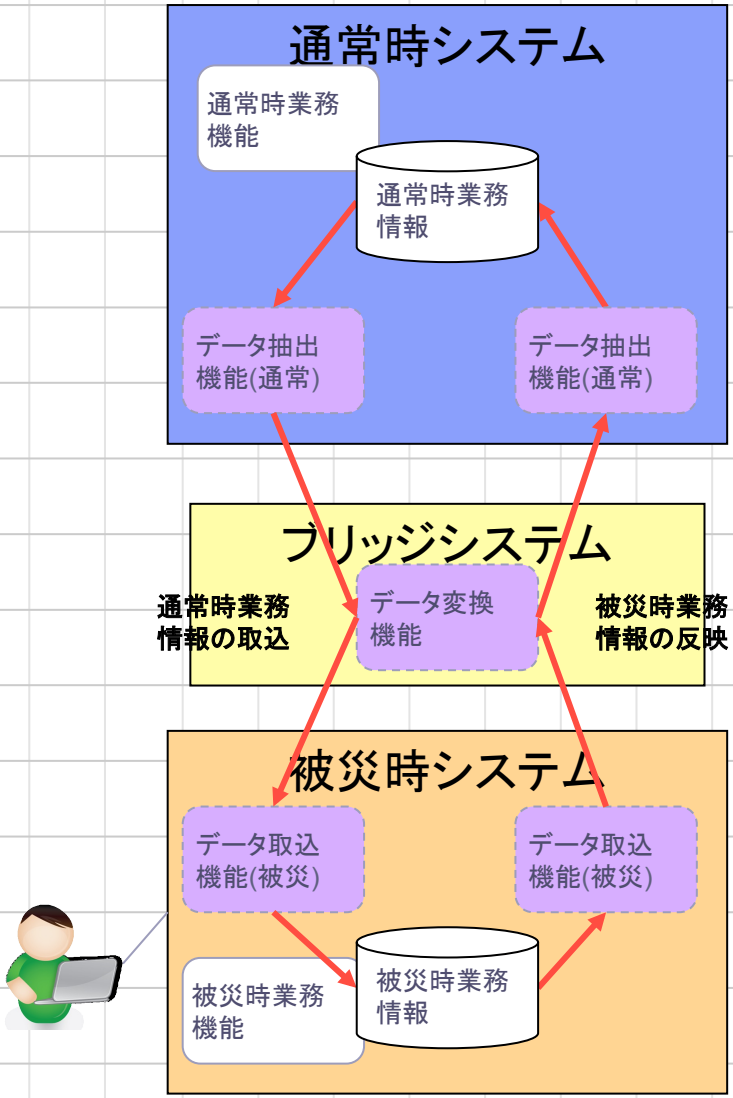
通常時システムが災害により被害を受けた時の、バックアップシナリオを想定する。

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<u>復旧／カップリング方式をパターン化</u>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

ICHIGANデータ・アーキテクチャの特徴

- 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

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

・避難所情報入力
・支援要望入力
・安否入力

災害現場

・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）

ICHIGANデータアーキテクチャに関わる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

Project ICHIGAN

- 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
- **Deferred Authentication**
- マイナンバー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

＜サンプルケース＞前提とする災害シナリオ
台風19号による災害

Project ICHIGAN

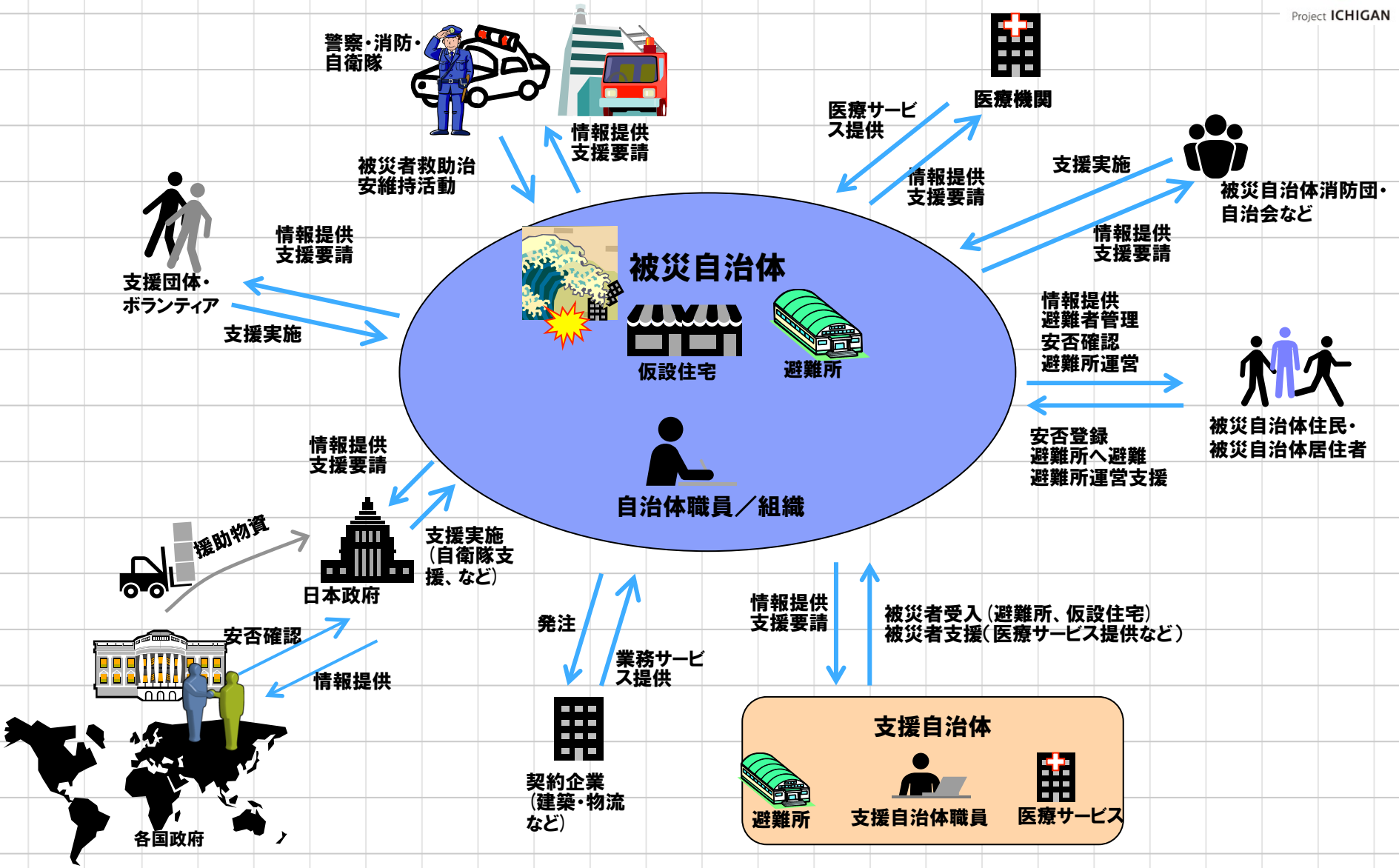
日時	状況				局面	システム
9/20	紀伊半島に台風が48時間後に上陸する可能性が大				警戒期	
	自治体長がカップリング先（北海道）へのシステムを切り替え宣言					
	避難命令が発令され、住民の避難が始まる				緊急期	
9/22	台風が上陸、甚大な被害 （町役場も水没）					
	対象	死者・行方不明	けが	家を失くした人		
	全体	5,000人	20,000人	100,000人		
	人口1万人のA町	500人	2,000人	10,000人		
9/25	避難所の開所				応急期	
翌年 1/01 ～	避難所から仮設住宅への移住 避難所の閉所				復旧期	

＜サンプルケース＞前提とする災害シナリオ
台風19号による災害　～　システムの状況

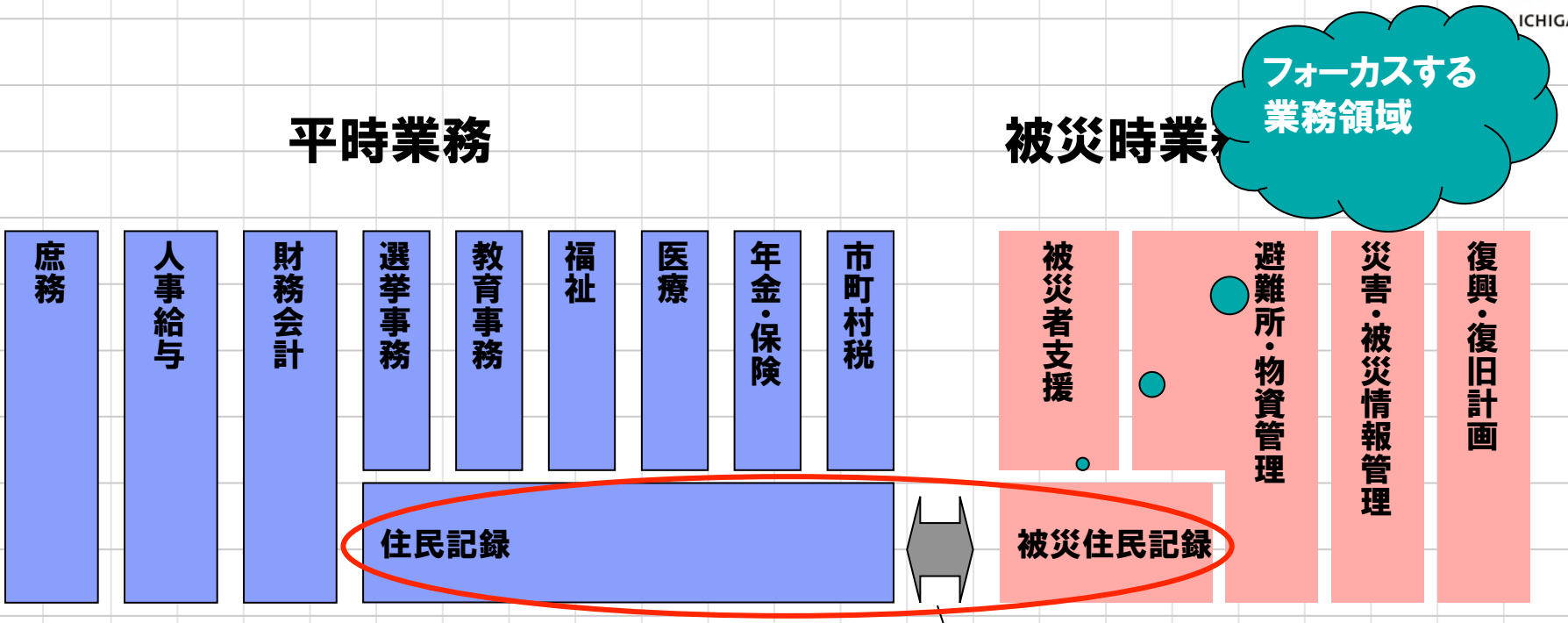
Project ICHIGAN

日時	住民台帳管理システム （通常業務システム）	局面	被災者台帳管理業務システム （被災時システム）
通常	町役場のコンピュータ室にシステムは設置・稼動 カップリング先システムと同期できている 災害を想定した訓練が行われている	通常期	稼動環境を確保済み(SaaS) 災害を想定した訓練が行われている
9/20	システム稼動状況は変わらない	警戒期	状況は変わらない
	カップリング先（北海道）のシステムに切り替え後、町役場のシステムは遮断する		平時システムからのデータ移行の準備を行う
	カップリング先（北海道）のシステム上で稼動	緊急期	被災時システムは稼働していない データ移行作業を実施？
9/22	町役場のシステムも水没 （電源、ネットワークダウン）		
9/25	電源、ネットワークは、徐々に復旧していく 町役場のシステムは、使用できない カップリング先のシステムを利用	応急期	オフラインモードでシステムは稼動（ネットワーク・オフライン） ネットワーク復旧後、システムはデータ複製を実施 ⇒オフライン業務はないのでは？
翌年 1/01 ～	電源、ネットワークの復旧は完了 カップリング先のシステムを利用 町役場のシステムは、再構築し、カップリング先（北海道）より移行	復旧期	

ビジネス・コンテキスト


警察・消防・
自衛隊
情報提供
支援要請
被災者救助治
安維持活動
医療サービ
ス提供
医療機関
情報提供
支援要請
支援実施
被災自治体消防団・
自治会など
情報提供
支援要請
情報提供
支援要請
支援団体・
ボランティア
支援実施
被災自治体
仮設住宅
避難所
情報提供
避難者管理
安否確認
避難所運営
安否登録
避難所へ避難
避難所運営支援
被災自治体住民・
被災自治体居住者
自治体職員／組織
情報提供
支援要請
援助物資
日本政府
支援実施
（自衛隊支
援、など）
安否確認
情報提供
各国政府
発注
業務サービ
ス提供
契約企業
（建築・物流
など）
情報提供
支援要請
被災者受入（避難所、仮設住宅）
被災者支援（医療サービス提供など）
支援自治体
避難所
支援自治体職員
医療サービス

業務領域スタック定義(案)



被災時業務のうち、平時業務の拡張(類似のUIを持つなど)と整理すべきものと、被災時のみの臨時業務となるものの整理が必要と思われる。

住民・被災住民情報、固定資産情報などの連携が必要

業務領域(業務ユニット)定義

- サンプル事例の対象業務は、平時業務は「住民基本台帳」業務、被災時業務は「被災者基本台帳」業務とする。

L1	L2	L3				
平時業務	総務・企画・消防部門					
	住民記録	1.住民基本台帳	2.印鑑登録	3.外国人登録	21.戸籍	30.住登外管理
	選挙事務	4.選挙人名簿管理				
	教育事務	20.就学				
	市町村税	5.固定資産税	6.個人住民税	7.法人住民税	8.軽自動車税	9.収滞納管理
	財務会計	50.財務会計				
	人事・給与	52.人事給与				
	庶務	51.庶務事務	52.文書管理			
	共済・貸付					
	消防事務					
	民生・労働・衛星関係					
	福祉	12.障害者福祉	15.児童手当	16.生活保護		
	年金・保険	10.国民健康保険	11.国民年金	14.介護保険		
	医療	13.後期高齢者医療	17.乳幼児医療	18.ひとり親医療	19.健康管理	
	清掃業務					
	環境保全業務					
	商工農林水産部門					
	土木・建築					
	その他					
被災時業務	緊急・応急時業務					
	災害・被災情報管理	災害情報管理	被災者支援情報管理			
	被災住民記録	被災者基本台帳	安否確認			
	被災者支援	犠牲者・遺族管理	被災証明	義捐・支援金管理		
	避難所・物資管理	避難所管理	仮設住宅管理	緊急物資管理		
	復旧・復興時業務					
	復旧・復興計画	復旧・復興計画				

青字：被災時業務と情報を連携する平時業務
赤字：Project ICHIGAN の議論対象とする被災時業務

選択した被災時業務「被災者基本台帳」の実施イメージ

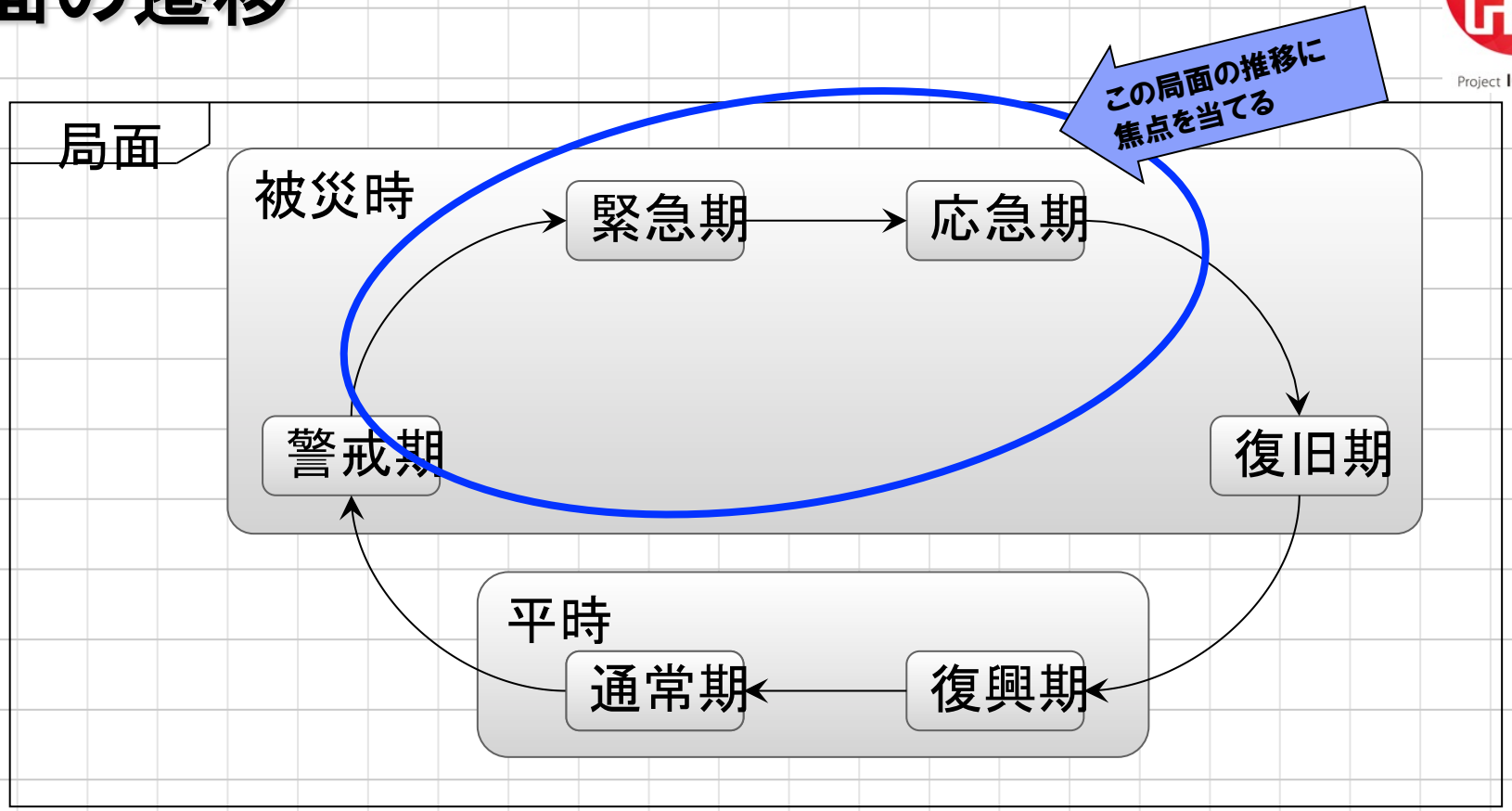
業務プロセス概要

1. 住民基本台帳に基づき、被災者台帳を作成する
    - 網羅性を確保するために、住民基本台帳をベースとする
2. 調査票を印刷し、職員が現地調査を行う
3. 調査結果をシステムに登録する
4. 戻ってこない調査票は、未確認として管理する

被災者基本台帳業務で作成された情報を元に、被災証明・罹災証明などが発行される。発行業務自体は別の業務ユニットとして定義されているため、発行業務自体の深い議論は実施しない。業務ユニット間の情報連携に焦点を当てて議論を進める。

- 罹災証明：固定資産台帳に基づいて、証明書を発行する。
- 被災証明：東日本大震災の時は、本人確認なく発行していた事例がある。証明書発行対象は、住民に限らない。

局面の遷移



- 警戒期～復旧期をまとめて「被災時」と呼び、通常期・復興期を「平時」と呼ぶ

議論点：
復興期は平時か？

【注】- この遷移は標準的な順序関係だけを規定している。実際には、警戒期から通常期に戻るなど、途中をスキップした遷移がありうる。

局面と業務モードの関係の例(平時業務)

Project ICHIGAN

	住民基本台帳業務(平時業務)		住民基本台帳システム(平時システム)	
通常期	通常モード	平時の住民サービス。	通常モード	平時のシステム稼働。
警戒期	警戒モード (縮退)	<体制変更の宣言で警戒期に遷移> 体制変更に伴うモード変更(警戒態勢) 窓口業務縮退 自治体職員が実施主体	(通常モード) カップリング前後でモード遷移が発生する (代替モード) サーバ@カップリング先 端末@被災自治体	・移行準備を行う ・準備完了後、カップリング先自治体に移動 ・被災時システムに移行するデータの抽出 「状況」が変化したことに伴うモード遷移
緊急期	非常モード	住民基本台帳業務に関する住民サービス停止(異動申請、証明書発行など)	代替モード	システムを利用した住民サービス実施は想定しない。
応急期	応急モード	カップリング自治体職員が実施主体	代替モード? サーバー、端末共に、カップリング自治体で、稼働する。	応急期から復旧期への遷移において、通常モードへの戻し作業が発生する
復旧期	通常モード	平時の業務体制・プロセスに復旧する。 主体は被災自治体		
復興期	通常モード			

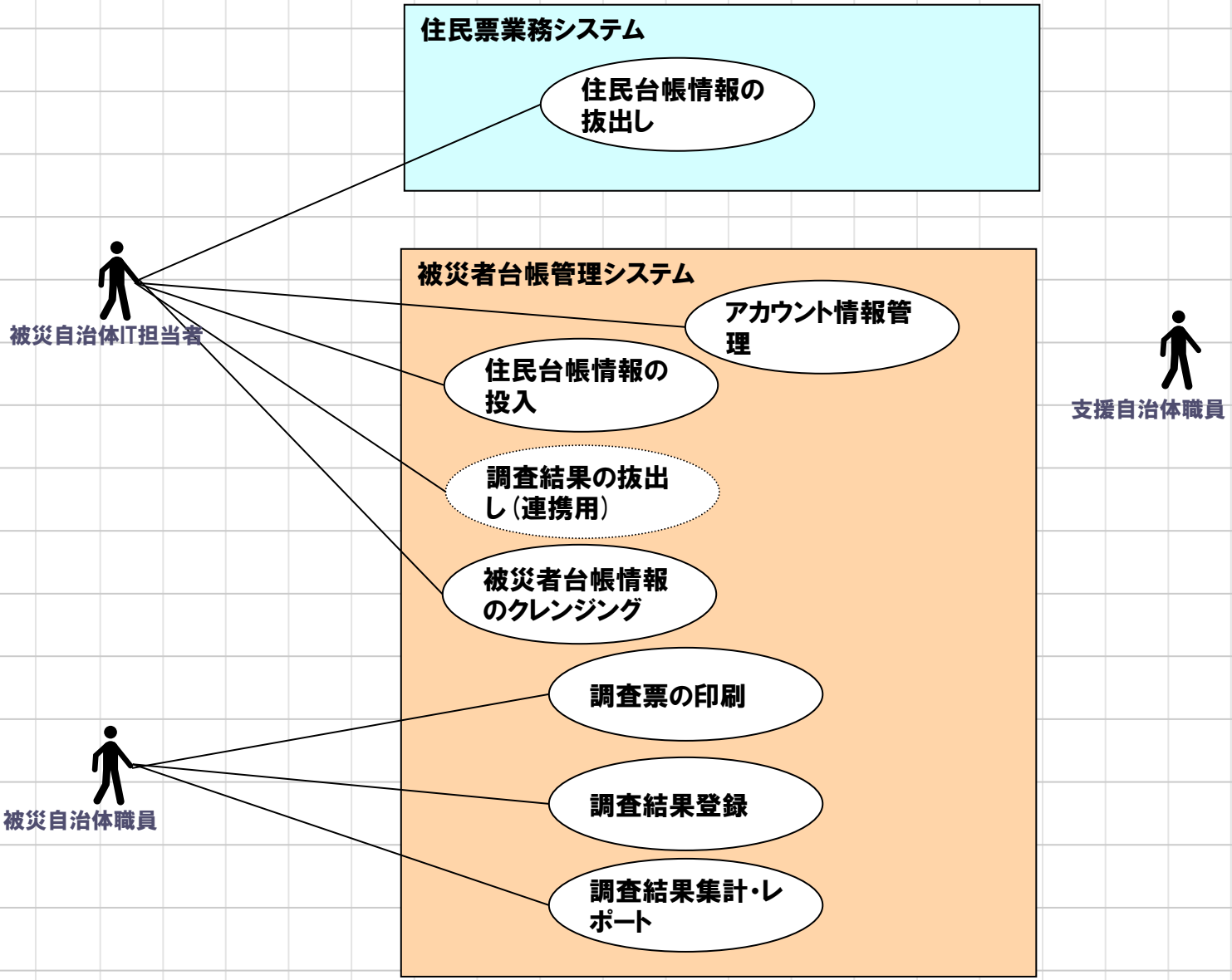
局面と業務モードの関係の例(被災時業務)

自自治体の住民台帳をベースに、世帯単位で状況確認

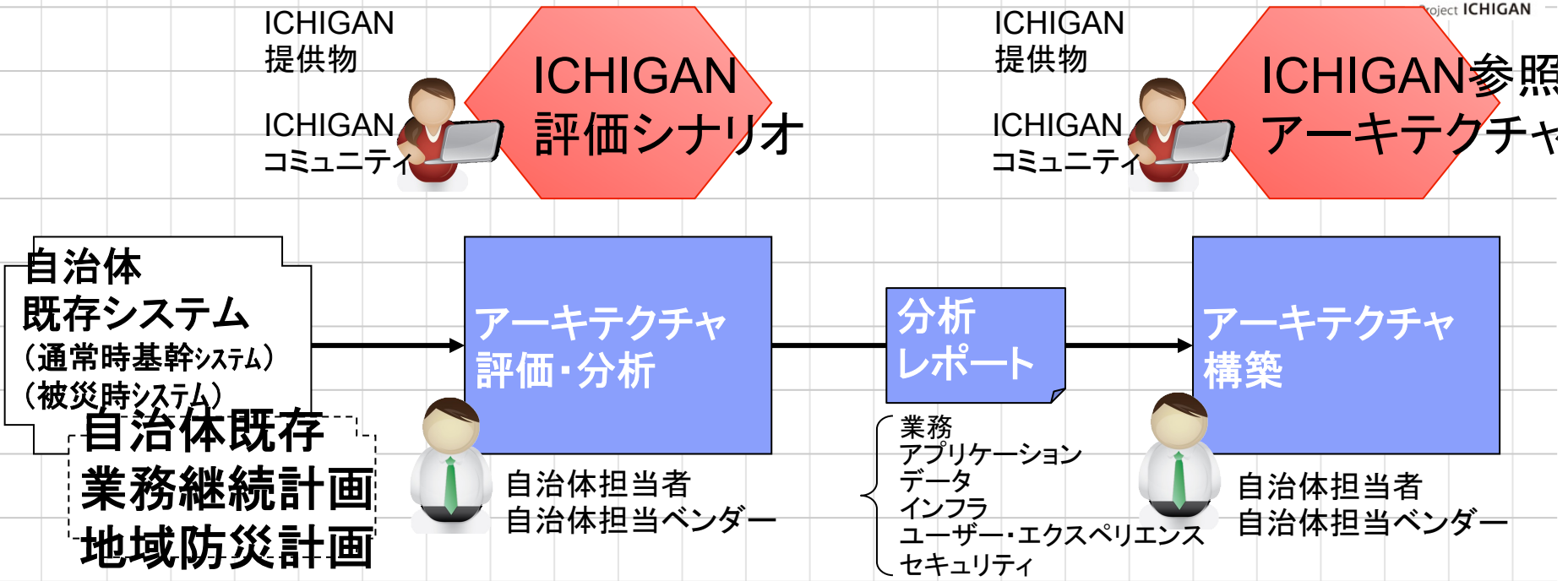
緊急期：緊急事態の対応を始めた時点で、緊急期に入る。(避難も含む)

	被災者台帳管理業務(被災者時業務)		被災者台帳管理業務システム(平時システム)	
通常期	訓練モード (準備モード)	(平時に何らかの作業は発生している)		
警戒期	準備確認モード	体制の確認。住民台帳が最新であることを確認する。ネットワークなどの準備の確認。 住民基本台帳に基づいた調査票を印刷する。	準備モード	平時システムからデータを移行。 住民基本台帳、家屋台帳／固定資産情報などから被災者台帳を作成する。
緊急期	緊急モード	住民避難を働きかけた時点で緊急期に入る。自治体職員が世帯の被災状況を確認する。調査票をベースに現地調査を実施。データ入力が開始される。 (安否確認は緊急期の実施も必要)	本番モード	ユーザーによる情報更新・参照処理。(自治体本体で実施する業務であり、情報は一か所で更新される)
応急期	実施モード	自治体職員が世帯の被災状況を確認する。 被災証明・罹災証明発行業務に情報を連携する。	本番モード	調査票に基づく調査は継
復旧期	制限モード	被災証明・罹災証明発行業務に情報を連携する。		被災証明・罹災証明発行システムにデータを連携する必要がある。
復興期				

ユースケース図


住民票業務システム
住民台帳情報の抜出し
被災者台帳管理システム
アカウント情報管理
住民台帳情報の投入
調査結果の抜出し（連携用）
被災者台帳情報のクレンジング
調査票の印刷
調査結果登録
調査結果集計・レポート
被災自治体IT担当者
被災自治体職員
支援自治体職員

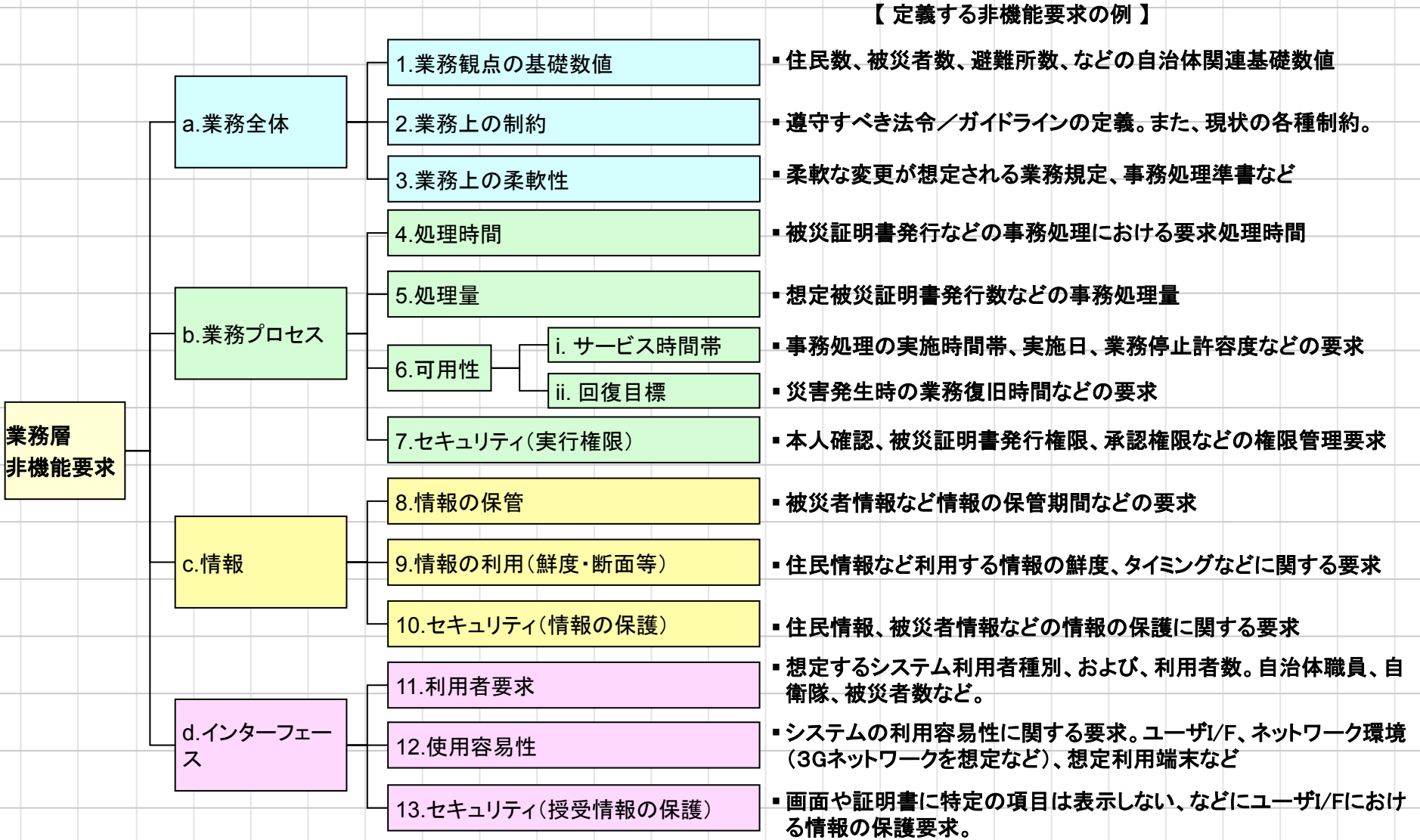
ICHIGAN参照アーキテクチャの使い方



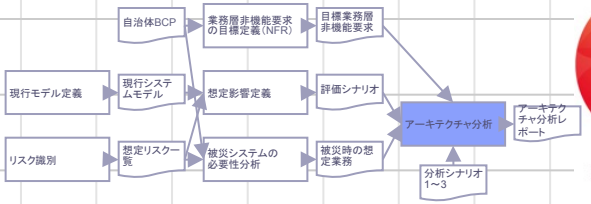
- 自治体の既存の業務・システムとBCPを前提として、以下の活動の実施を想定する。
  - ICHIGANで定義したシステム評価シナリオに基づき、既存の業務・システムの災害対策および業務継続性対応状況の評価を行う。
  - 評価結果に基づき、業務・システムのアーキテクチャの改訂を行う。
    検討にあたり、ICHIGAN参照アーキテクチャを活用することが可能である。
- 上記の活動の主担当として、自治体担当者、および、自治体の担当ベンダーを想定する。

アーキテクチャ分析の流れ
業務層非機能要求定義　～ 分析の枠組み

- ICHIGANで提案する、業務層非機能要求分析の枠組みの詳細を以下に示します。

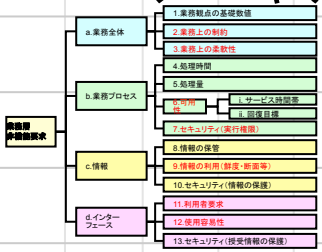


アーキテクチャ分析の流れ



Project ICHIGAN

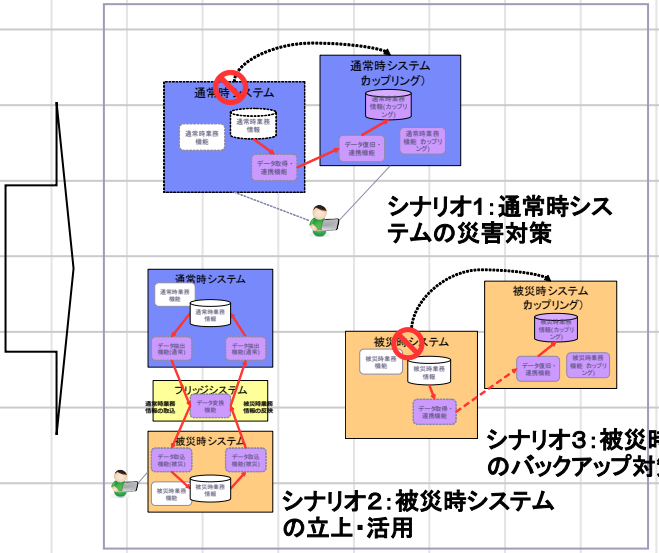
- これまでの分析結果から得られた各種要求の実現について、想定される対策のパターン(分析シナリオ:詳細は後述)に基づき以下のような詳細な分析作業を実施し、分析レポートとしてまとめます
  - 対応状況分析
  - 業務層非機能要求詳細化
  - アーキテクチャの精査



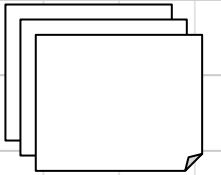
目標業務層非機能要求

評価シナリオ

業務ユニット定義



分析シナリオ



分析レポート

仕様書成果物の目次案

Project ICHIGAN

ICHIGANとしての仕様書成果物

概要
・目的
・用語の定義
・業務の概要
・情報システム化の範囲

機能要件
・情報システムの要件
　機能
　画面
　帳票
　情報・データ
　外部インタフェース

非機能要件
・規模・性能要件
（規模、性能）
・信頼性等要件
（信頼性、拡張性、上位互換性、
システム中立性、事業継続性）
・情報セキュリティ要件
（権限、情報セキュリティ対策）
・ユーザビリティ

システム稼働環境
　全体構成、
　ハードウェア構成、
　ソフトウェア構成、
　ネットワーク環境、
　アクセシビリティ）

テスト要件

移行要件
　移行、教育

運用要件
　情報システムの操作・監視等
　データ管理
　運用施設・設備

保守要件
　ソフトウェア保守
　ハードウェア保守

自治体での調達仕様書

調達仕様書

表紙
・調達件名

作業の概要
・目的
・用語の定義
・業務の概要
・情報システム化の範囲
・作業内容・納入成果物

機能要件
・情報システムの要件（機能、画面、帳票、情報・データ、外部インタフェース）

非機能要件
・規模・性能要件（規模、性能）
・信頼性等要件（信頼性、拡張性、上位互換性、システム中立性、事業継続性）
・情報セキュリティ要件（権限、情報セキュリティ対策）
・システム稼働環境（全体構成、ハードウェア構成、ソフトウェア構成、ネットワーク環境、アクセシビリティ）
・テスト要件
・移行要件（移行、教育）
・運用要件（情報システムの操作・監視等、データ管理、運用施設・設備）
・保守要件（ソフトウェア保守、ハードウェア保守）
・作業の体制及び方法（作業体制、開発方法、導入、瑕疵担保責任）
・特記事項

業務・システム最適化計画等の関係書類

以下の資料をベースに検討
「情報システムに係る政府調達の基本指針」実務手引書
http://www.soumu.go.jp/main_content/000141665.pdf

今後ともご支援をよろしくお願いします

Project ICHIGAN