災害に備えたクラウド移行促進セキュリティ技術の研究開発

研究代表者	寺田 修司	株式会社日立製作所
研究分担者	甲藤 二郎	早稲田大学大学院
	菊地 浩明	東海大学
	宮内 幸司	日本電気株式会社
	中島 康之	株式会社KDDI研究所

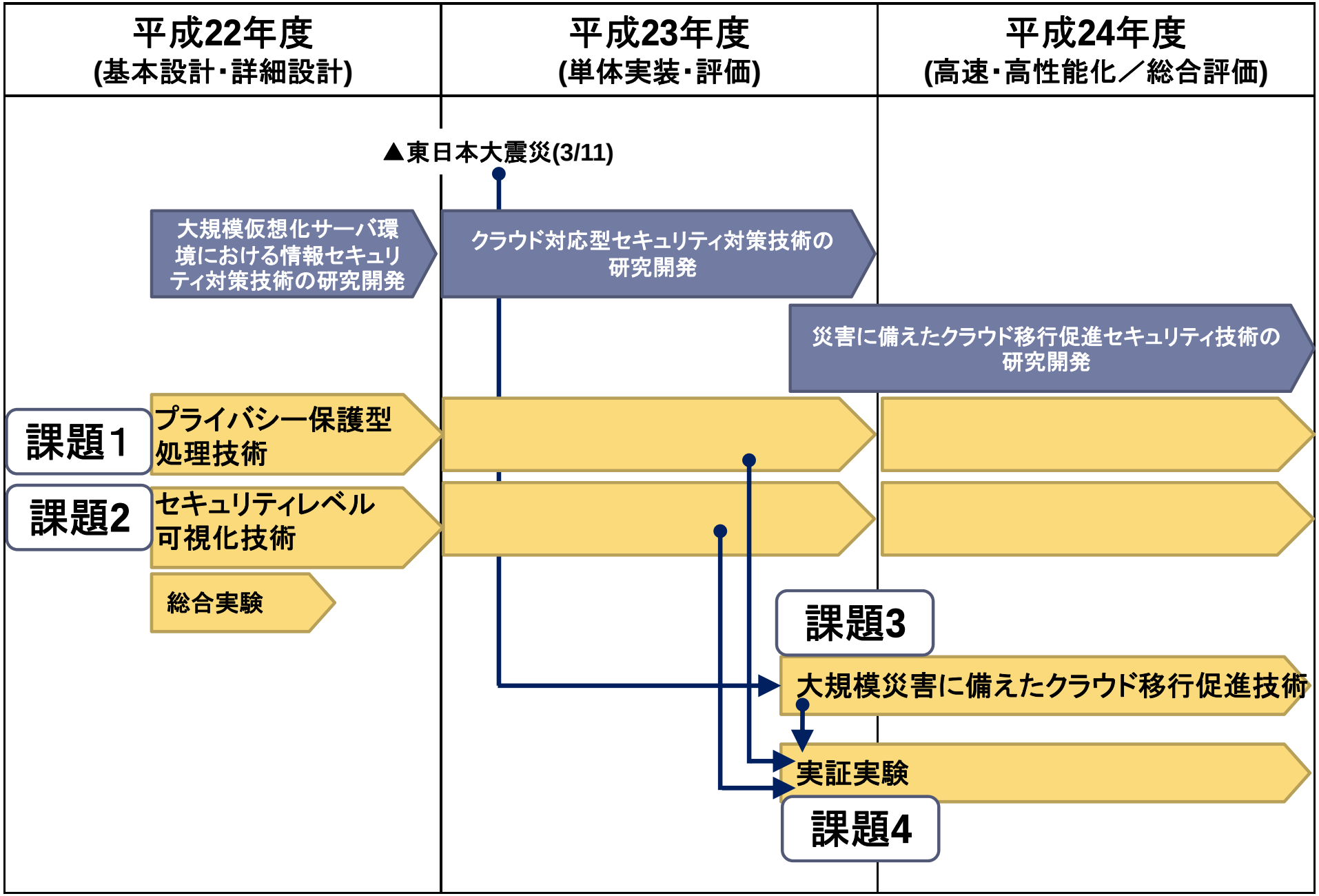
背景と目的

- クラウド環境を利活用したICTサービスの提供が進展し、国民生活や社会経済活動を支える基盤インフラとなりつつある。
- 一方、「情報漏えい」や「実態が不明な環境へ重要データを預託すること」などが不安要素として捉えられている。
- さらに、東日本大震災の影響により、大規模災害時における業務継続性を確保するクラウドを、安全・安心に構築して利用するための技術が求められている。
- 上記の利用者の不安を払しょくし耐災害性を強化するための研究開発を行う。

表：クラウドサービスにおけるセキュリティ課題

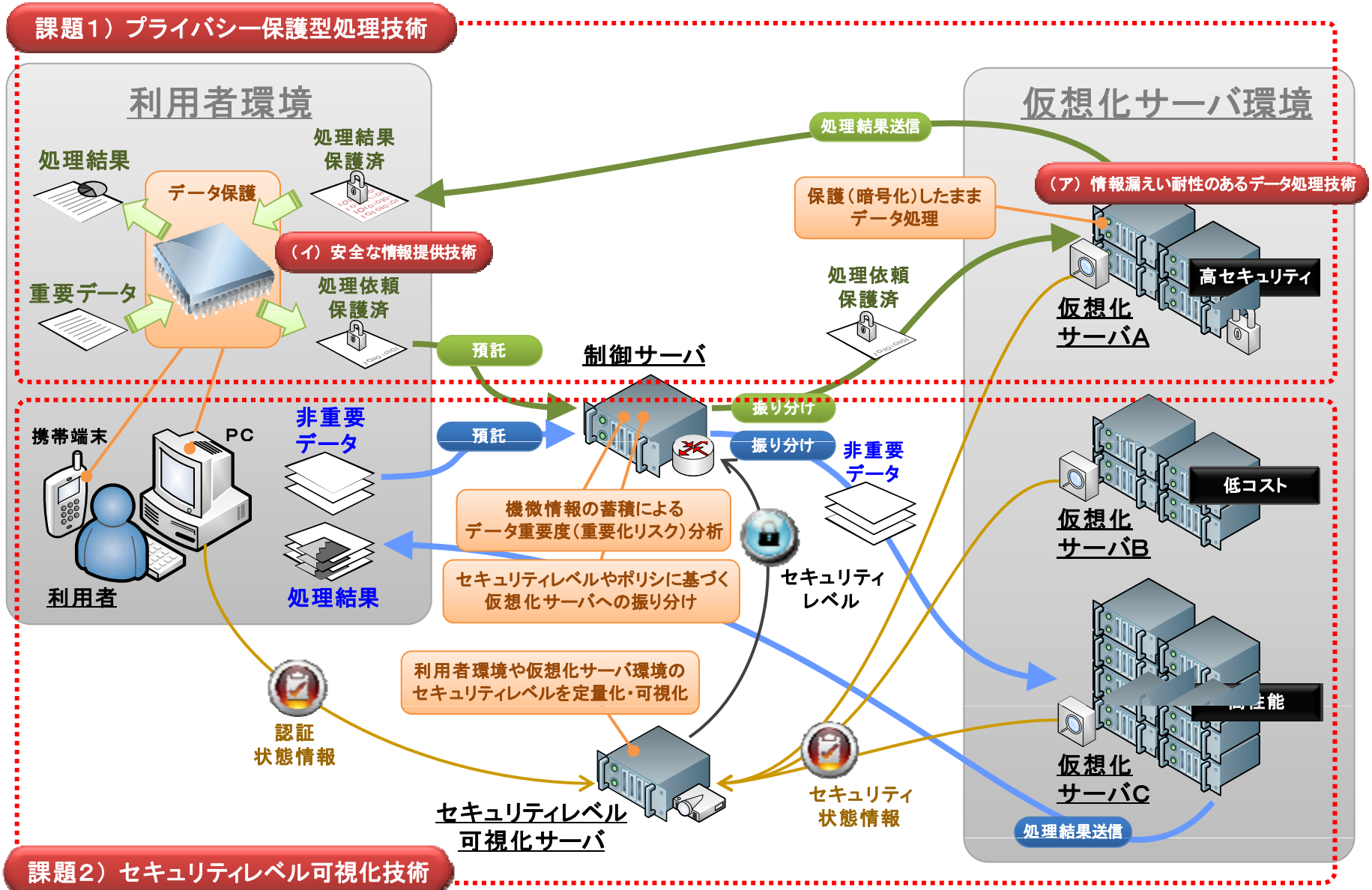
解決すべき課題	「情報漏えい」など利用者の不安要素の払しょく	大規模災害時の業務継続性の確保
データに対する対策	プライバシー保護型処理技術	大規模災害に備えたクラウド移行促進技術
システムに対する対策	セキュリティレベル可視化技術	

研究の経緯


平成22年度
(基本設計・詳細設計)
平成23年度
(単体実装・評価)
平成24年度
(高速・高性能化／総合評価)
▲東日本大震災(3/11)
大規模仮想化サーバ環境における情報セキュリティ対策技術の研究開発
クラウド対応型セキュリティ対策技術の研究開発
災害に備えたクラウド移行促進セキュリティ技術の研究開発
課題1
プライバシー保護型処理技術
課題2
セキュリティレベル可視化技術
総合実験
課題3
大規模災害に備えたクラウド移行促進技術
実証実験
課題4

研究開発全体概要

機密性の非常に高い情報処理に関してはプライバシ保護型処理技術により処理を行う。その他の情報処理については、仮想化サーバ環境のセキュリティレベル、利用者の認証レベル、利用者が発信するデータの重要度に基づき、最適な環境において処理を行う。



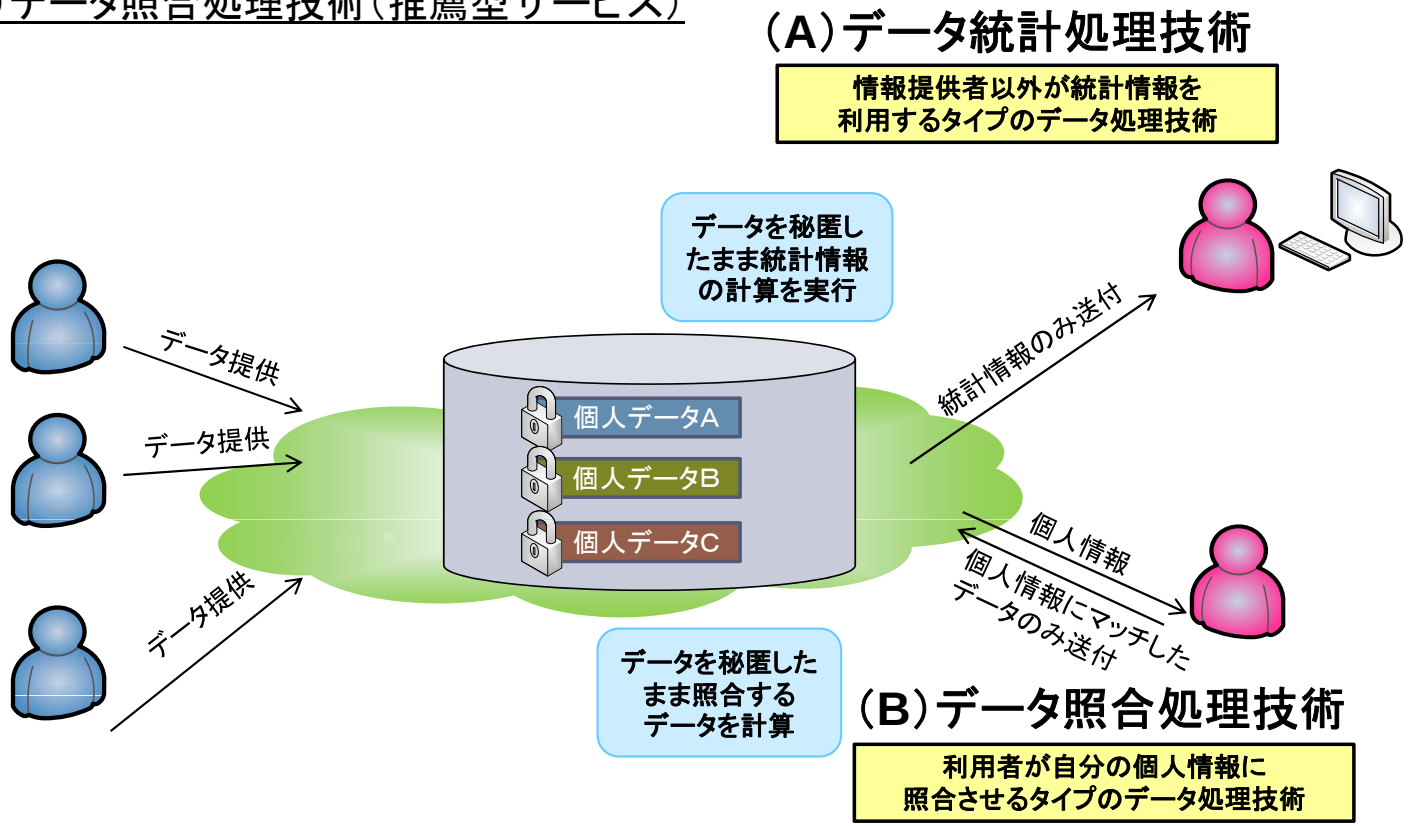
課題3)では大規模災害に備えたクラウド移行促進技術として「クラウドにおける安全なバックアップ技術の開発」などを行い、課題1)～3)で開発した技術の有効性を検証する目的で、課題4)大規模災害等に備えた実証実験を実施した。

各課題の概要

1）プライバシー保護型処理技術

ー情報漏えい耐性のあるデータ処理技術[課題 概要]

- 概要：サーバ上のデータが流出した時の被害を防止するために、情報提供者の提供するデータを秘匿したまま情報処理する技術の研究開発を行う
- クラウドで実行される主要なアプリケーションであるデータベース上での処理に着目し、データベースを利用したサービスで実行される「統計演算」、「頻度分布計算」、「推薦処理」などを暗号化したまま行うための技術を検討
- 処理時に別途個人情報の入力有無に応じて下記（A）（B）に課題を分類
  - （A）データ統計処理技術（第三者利用型サービス）
  - （B）データ照合処理技術（推薦型サービス）



1)プライバシー保護型処理技術

ー情報漏えい耐性のあるデータ処理技術　(A1) データ統計処理技術(正確性重視)

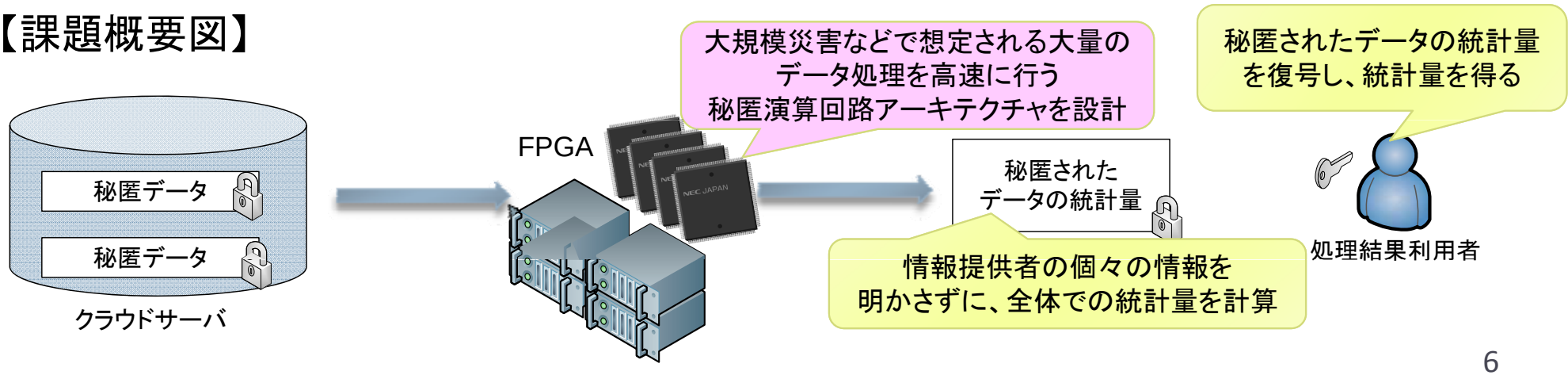
本研究開発の課題概要:
機微な情報を収集し、その統計値や頻度分布を利用したサービスが普及している。しかし、クラウドでそのようなサービスを実現する場合、収集された情報の漏えいが懸念され、サービス普及の妨げとなっている。
そこでクラウド上のデータを暗号化により秘匿したまま、統計値演算や頻度分布計算を行う技術を実現する。
特に、**高い処理精度と、高い秘匿強度を持つデータ統計処理技術**を実現する。

目標:
大規模災害時等に想定される大量のデータ処理(例えば被災者状況の統計処理)をクラウドで高速に行うための、秘匿演算回路アーキテクチャを設計。設計した回路のFPGA実装を行い、**100万件の平均演算を20秒以内**で行う。

注: FPGA (Field Programmable Gate Array) とは回路構成を設定・変更可能な集積回路のこと.

主な成果:
・100万件の暗号文を高い秘匿強度を保ちつつ処理する秘匿演算回路アーキテクチャを設計。
・**設計アーキテクチャをFPGAで実装し評価した結果、100MHz駆動で、平均20秒での処理完了を確認。**
・この結果、リソースの少ないスマートフォンでも秘匿演算できる見通しを得た。

【課題概要図】



1)プライバシー保護型処理技術

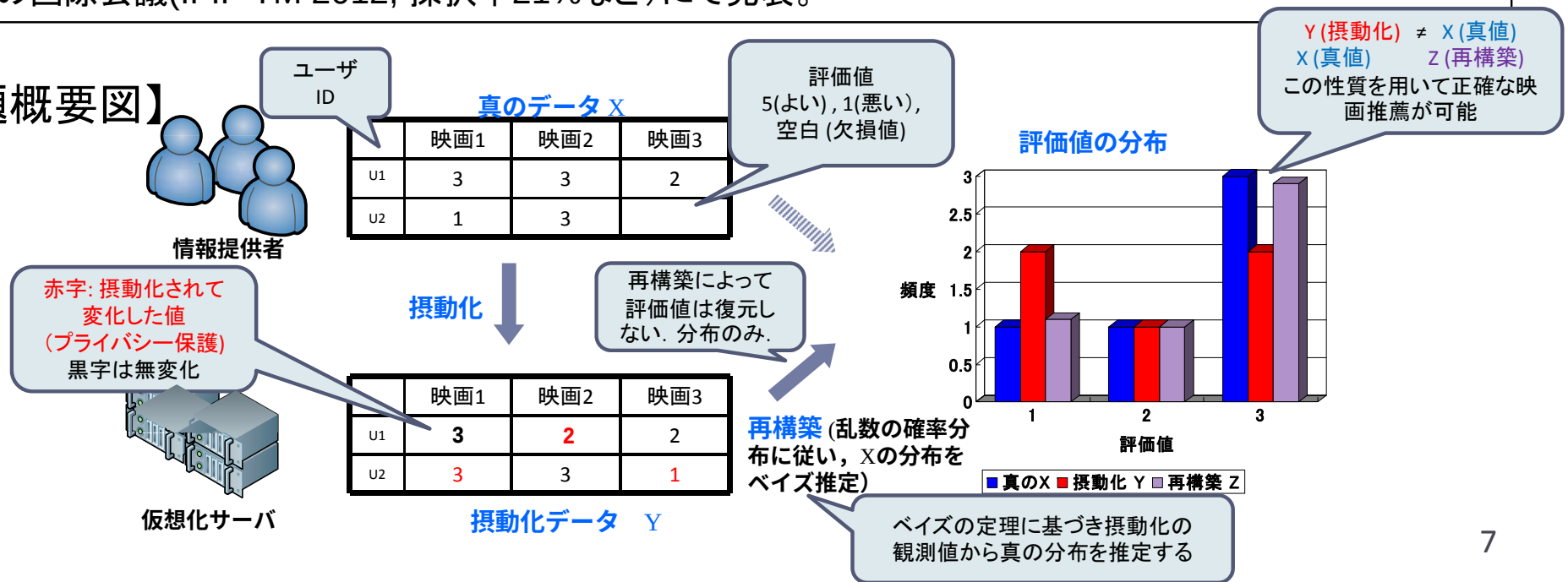
ー情報漏えい耐性のあるデータ処理技術　（A2）データ統計処理技術（速度重視）

本研究開発の課題概要：
クラウドに格納された情報にランダムノイズを加える（摂動化）ことにより、**一つ一つの情報を秘匿しつつ、平均や情報推薦などの統計処理は可能とする技術**を開発する。単一のデータレコードの摂動処理、仮想化サーバ処理、推薦処理を平均30秒以内でサービスする。

目標：
これまでに検討した改良方式の摂動化と再構築の処理速度を測定し、実現可能性を検証する。**公開データセットを用いて，再構築の精度と処理時間を測定**する。

主な成果：
・**摂動化による、未評価のアイテムに対する評価値を予測する情報推薦方式を開発。**
・代表的なパブリッククラウド(Google, Amazon)に情報推薦方式を実装し、7万人のデータセット(Jaster, MovieLens)で評価。パブリッククラウドで2.2秒以下で処理完了を確認。
・2件の国際会議(IFIP TM 2012, 採択率21%など）にて発表。

【課題概要図】



1)プライバシー保護型処理技術

ー情報漏えい耐性のあるデータ処理技術　　(B) データ照合処理技術

本研究開発の課題概要:

クラウドの管理者を信頼できない状況で，**情報利用者が自分の嗜好を秘匿したまま、他の情報提供者の評価傾向に基づいたアイテム推薦を実行すること**を目的とする．クラウドには，不特定多数の映画に関する評価値を（誰がどの評価をしたか不明な形式で）格納し、情報利用者は，自身の部分的な評価値（暗号化されている）を元に，情報提供者の評価結果との類似度を求めて，情報利用者が好むと推測される映画を出力する．

目標:

H23までにGoogle App Engine (GAE)の上に準同型性暗号(Paillier) の計算処理ソフトウェアを実装し，試験データでの基本動作を確認している．H24には，他のクラウドサービスAmazon Elastic Beanstalk (AEB)での実装と，公開データセットを用いて提案するデータ照合の処理速度と適用可能規模を評価する。**処理速度と情報推薦の精度を測定し、実用的な照合方式の改良**を行う。**ユーザインタフェースやエラー処理の整備を行い、システムの完成度を高める。**

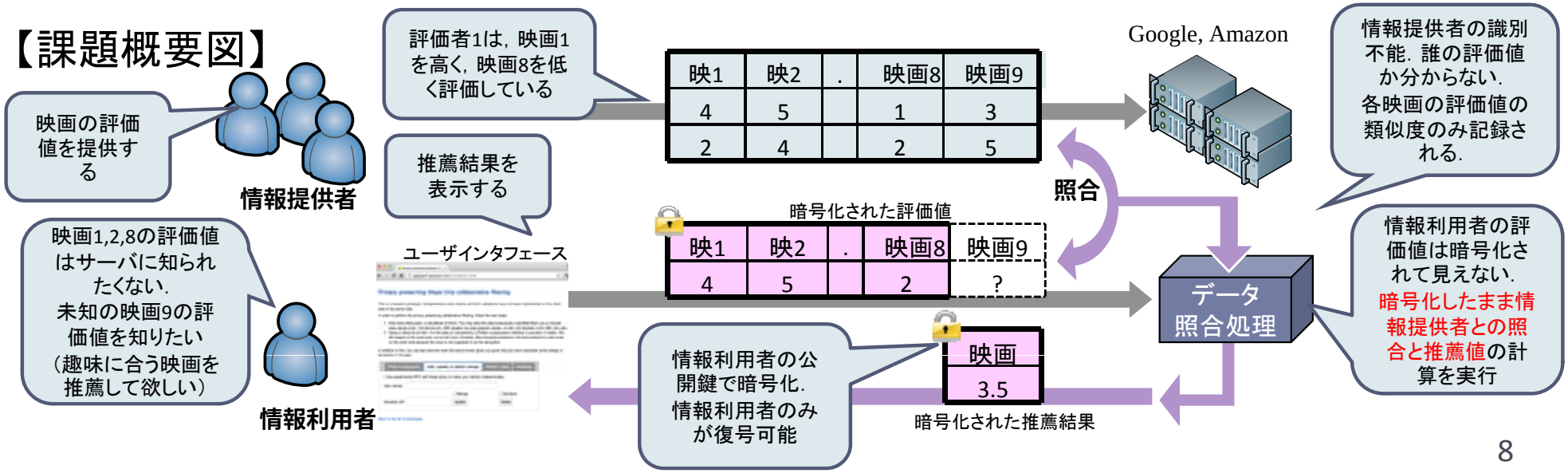
主な成果:

・クラウドでの格納方式（Google BigTableやAmazon RDB)や並列化により高速化し、処理性能を評価。

・**提案方式は，IEEE Cloudcom 2011, IFIP SEC 2011, ACM SAC　2012などの国際会議に発表し、ジャーナル論文(Springer Journal of Cloud Computing, Journal of Internet Services and Information Securityなど)に掲載**

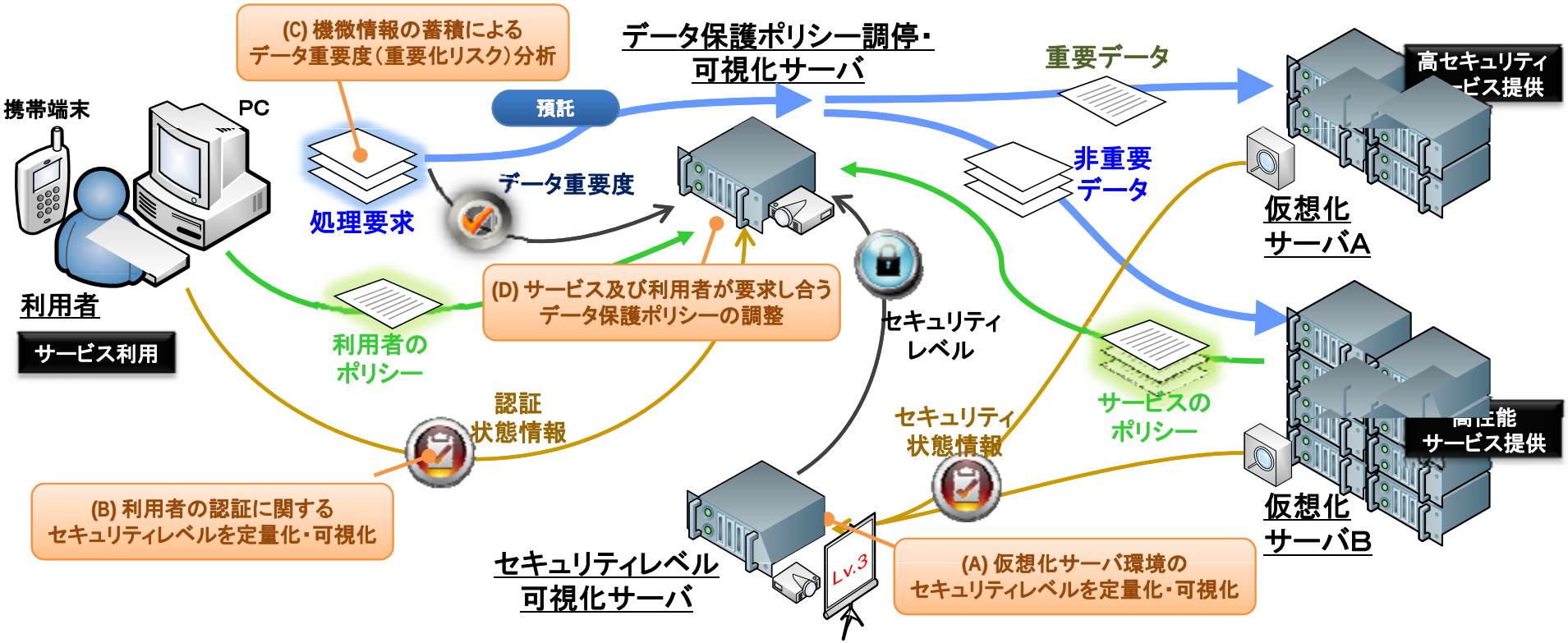
・クラウドビジネスを推進するCloud Security Allianceによる国際会議にて招待講演。

【課題概要図】



2）セキュリティレベル可視化技術[課題 概要]

- 概要：
  クラウド環境を安心・安全に利用するためのセキュリティ状態可視化技術を開発する。
  本研究開発では、クラウド環境のセキュリティレベル可視化技術を以下の4つに細分化する。
  (A) クラウド環境のサーバに関するセキュリティ対策状況の可視化技術
  (B) クラウド環境の利用者認証に関するセキュリティ対策状況可視化技術
  (C) クラウド環境に預託するデータの重要度可視化技術
  (D) 利用者とクラウド環境のデータ保護ポリシーの調停・可視化技術



2）セキュリティレベル可視化技術

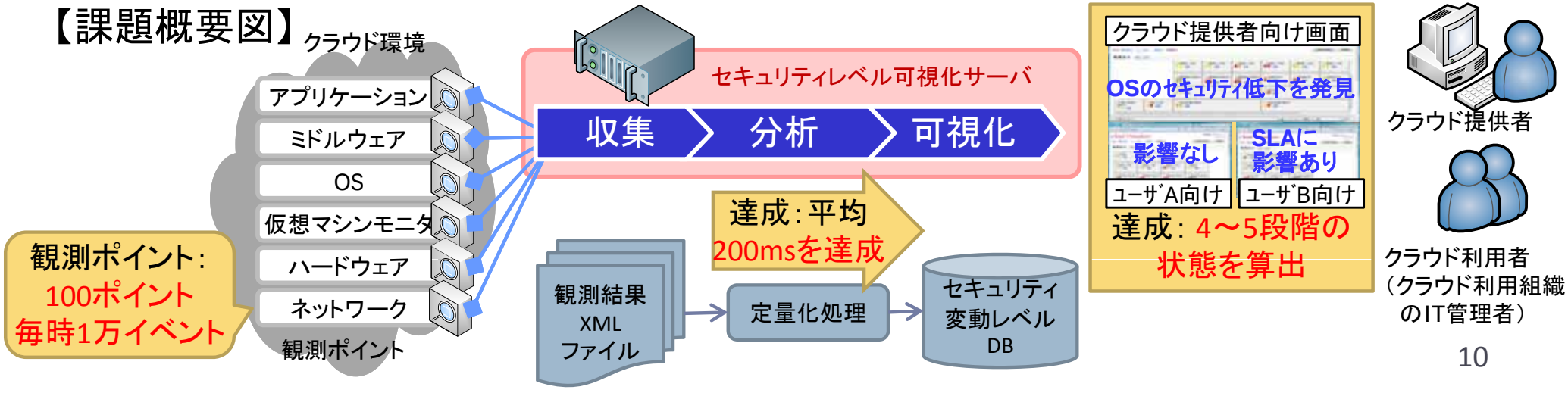
（A）セキュリティ対策状況の可視化技術

本研究開発の課題概要：
クラウドでは、クラウド提供者にITシステムの運用を任せるため、**クラウド利用者には、クラウド上の自システムの運用が適正に行われているかどうかが確認できない（不可視化）**。そのため、利用者の不安（特にセキュリティ面における不安）につながっている。
そこで、**クラウド利用者等にも、そのセキュリティ対策状況を「可視化」する技術を開発**する。

目標：
平成22年度よりクラウド環境のセキュリティ状態を分析するための情報を収集する観測ポイントを明らかにしてきた。今年度は、**観測ポイントの収集情報を精査し、100程度の観測ポイントから得られるイベント情報に基づいてセキュリティレベルを200ms以内に定量化し、セキュリティ状態を4～5段階で判定してクラウド利用者に適切に表示**する。

主な成果：
・クラウドのセキュリティ状態が変化する要因を分類し、この変化を捉えるための観測ポイントを、クラウドのシステムレイヤ毎に整理。
・**130個の観測ポイントから得られる情報をもとに、セキュリティ状態の低下箇所と影響範囲を算出し、Web表示する可視化システムを開発**。実用化に向け、運用監視オペレータにヒアリング評価し、改善内容を反映。

【課題概要図】



2）セキュリティレベル可視化技術

（B）認証に関するセキュリティ対策状況可視化技術

本研究開発の課題概要：クラウド環境では、プロバイダ同士がID連携(認証結果の受渡し)を行うことで一度の認証で複数のクラウドサービスが利用可能である(シングルサインオン)。しかし、**プロバイダ毎に認証手段(パスワード or 生体認証)、利用端末等が異なるため、プロバイダに対して第三者が不正に登録者になりすまして攻撃を行うことの難しさ(認証結果の信頼性)を評価することが困難**である。そこで**クラウド環境における認証レベルを可視化・提供する技術を確立することで、より安心・安心なクラウド環境におけるシングルサインオンを実現**する。

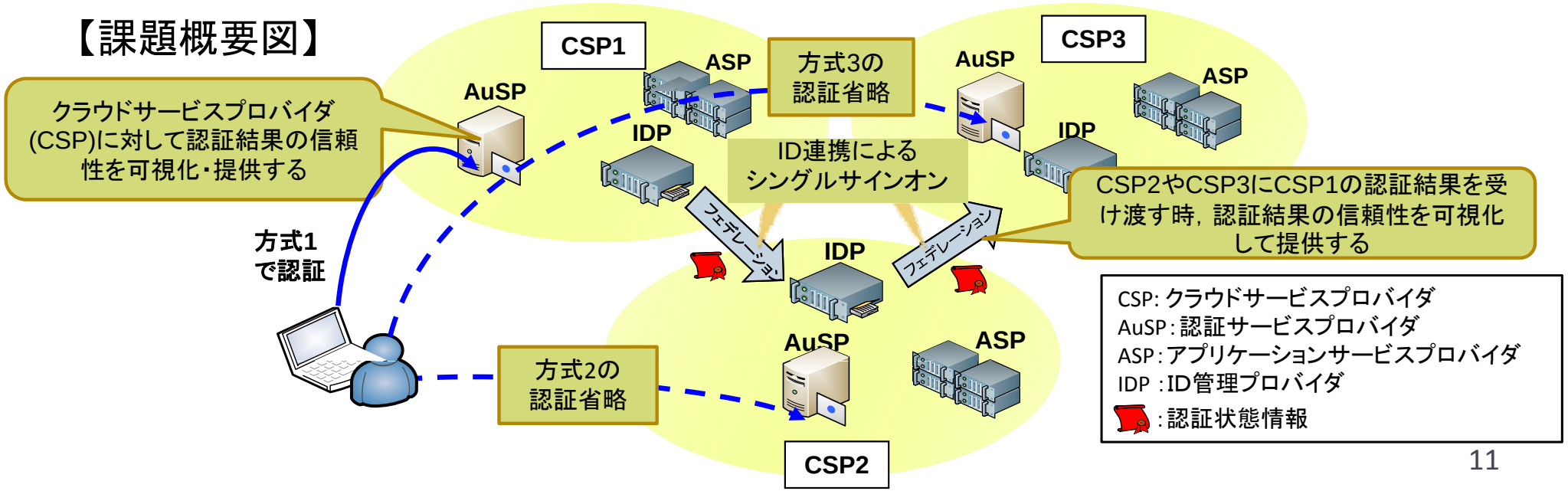
目標：**平均200ms以内でクラウド環境の認証方式の認証結果の信頼性を定量化する方法を確立**する。さらに、NIST SP800-63-1で扱われていない生体認証を認証方式とする方法を確立する。またフェデレーション(認証結果の受渡し)を受ける構成要素のセキュリティレベル分析に必要となるシステム仕様を明確化する。

主な成果：

・クラウド環境の認証方式について、認証結果の信頼性を定量化する可視化方式を開発。可視化に必要なシステム仕様を策定。

・**可視化アルゴリズムを実装し、平均10ms以内で仮想化システムの認証におけるセキュリティレベルを定量化する技術を確立**。

【課題概要図】



2）セキュリティレベル可視化技術

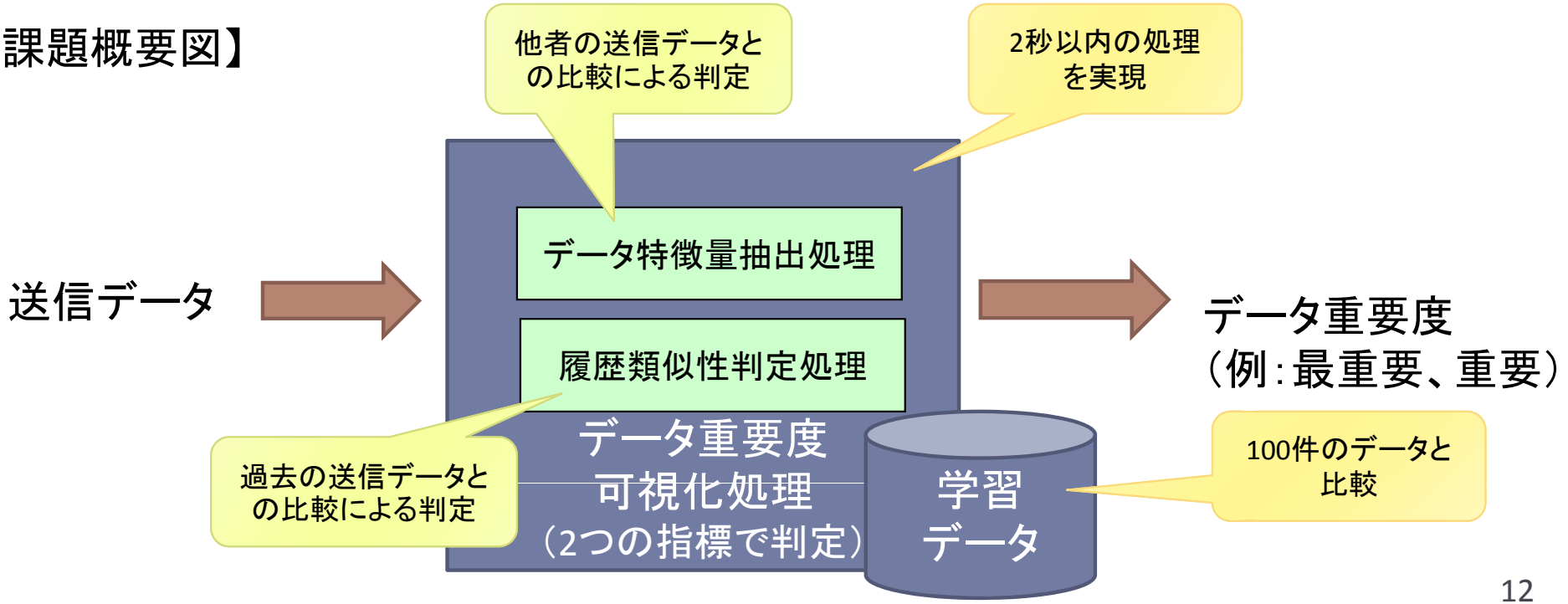
（C）データ重要度可視化技術

本研究開発の課題概要：**クラウド上でデータの重要度に応じた処理を実現するため、データの重要度を可視化する技術を確立する。**

目標：**データ特徴量抽出技術、履歴類似性判定技術の2つの基準により、重要度を総合的に判定するデータ重要度可視化システムを構築**する。**100件のデータを平均2秒以内で処理することを目標**とする。

主な成果：
- データ重要度可視化システムを実装し、性能及び機能性について評価を実施。
- **データ重要度可視化技術の処理時間は、1,000件の学習データに対し131msecの処理時間を実現**。
- **データの圧縮手法を実装し、判定確度を落とさずに、学習データのサイズを削減し、同時に速度向上を図る手法を実現**

【課題概要図】



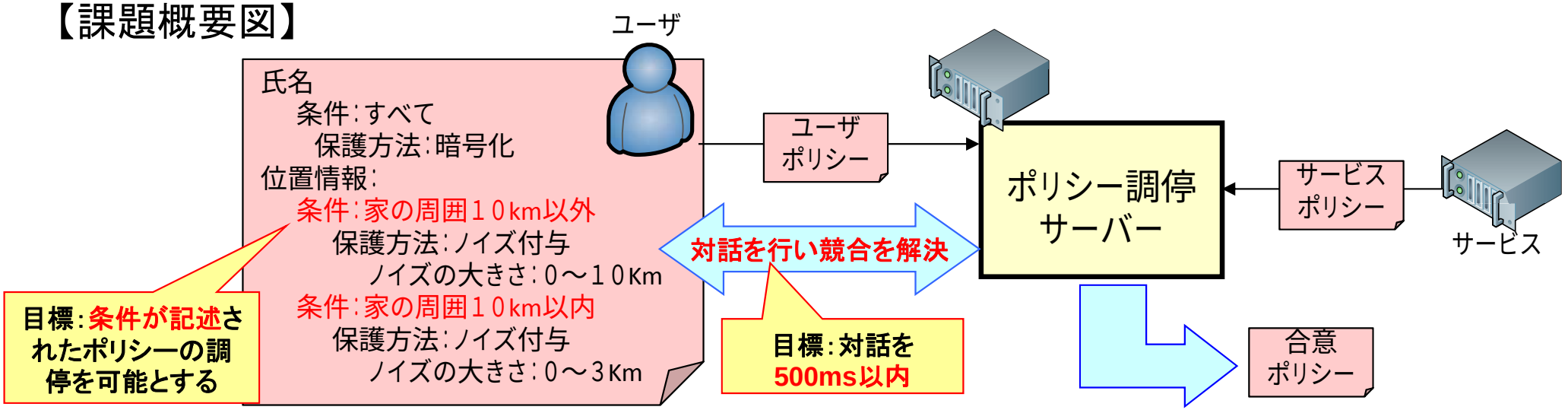
2）セキュリティレベル可視化技術
（D）データ保護ポリシーの調停・可視化技術

本研究開発の課題概要：クラウド環境は様々なセキュリティ状態のシステムが混合しているため、多様な重要性を持つユーザのデータを適切に取り扱い、安心して利用できる環境を提供することが難しい。特に**ユーザのデータ保護要件とサービスのデータ利用要件を同時に満たすことは困難**である。そこで、**2つの要件（データ保護ポリシー）の競合を解決する技術を開発**する。

目標：柔軟なデータ保護を実現するためにデータの条件ごとにデータ保護・データ利用の要件を記述できるように拡張を行い、**拡張したポリシーに対してもポリシー調停可能な技術の提案・実装・評価を行う**。**ユーザとポリシー調停システム間の対話が500ms以内で完了するように調停を可能**とする。

主な成果：
- **データ保護のユーザ条件を記述可能とし、その条件に対するポリシー調停方式を開発。ユーザとシステム間の対話が500msec以内で完了することを確認**。
- 同時に記載可能なデータ保護方法（暗号化や匿名化など）を、出力データ型が同一な組合せに制限することにより、データ保護方法の出力データ型の差から元のデータを推論される問題に対応。

【課題概要図】



3）大規模災害に備えたクラウド移行促進技術 [課題 概要]

- 概要：
  東日本大震災等の大規模災害により表面化した研究開発課題のうち即効性の高いものを選択して追加する。本研究開発では、大規模災害に備えたクラウド移行促進技術を以下の3つに細分化する。

(A) クラウドにおける安全なバックアップ技術の開発

- 東日本大震災によりバックアップの重要性が見直されているが、クラウドにおけるバックアップ手法が確立されていない。
- また、バックアップデータの安全な運用管理に負荷がかかるため、不適切な方法でバックアップが行われていることが多い。
- そこで、バックアップ手法を取りまとめガイドライン化すると共に、バックアップデータの安全な運用管理の負荷を低減する技術を開発する。

(B) 大規模災害時のクラウドサービスに適した認証基盤技術

- 東日本大震災により緊急時におけるクラウドサービスの有用性が見直されたが、機微な情報を扱うクラウドサービスについては、立ち上げの際に認証情報の登録、運用、削除など管理がボトルネックになることが多い。
- そこで、大規模災害時に緊急に立ち上げるクラウドサービスで必要とされるセキュリティ要件を取りまとめガイドライン化すると共に、大規模災害時にセキュリティレベルを不適切に下げずに迅速に認証を立ち上げるための認証基盤技術を開発する。

(C) 大規模災害時におけるクラウドを用いた安全な身元確認技術

- 東日本大震災をきっかけに、身分証がない場合に安全な身元確認の必要性が見直されたため、生体情報を使って身元確認を行う技術を開発する。

3）大規模災害に備えたクラウド移行促進技術
（A）クラウドにおける安全なバックアップ技術の開発

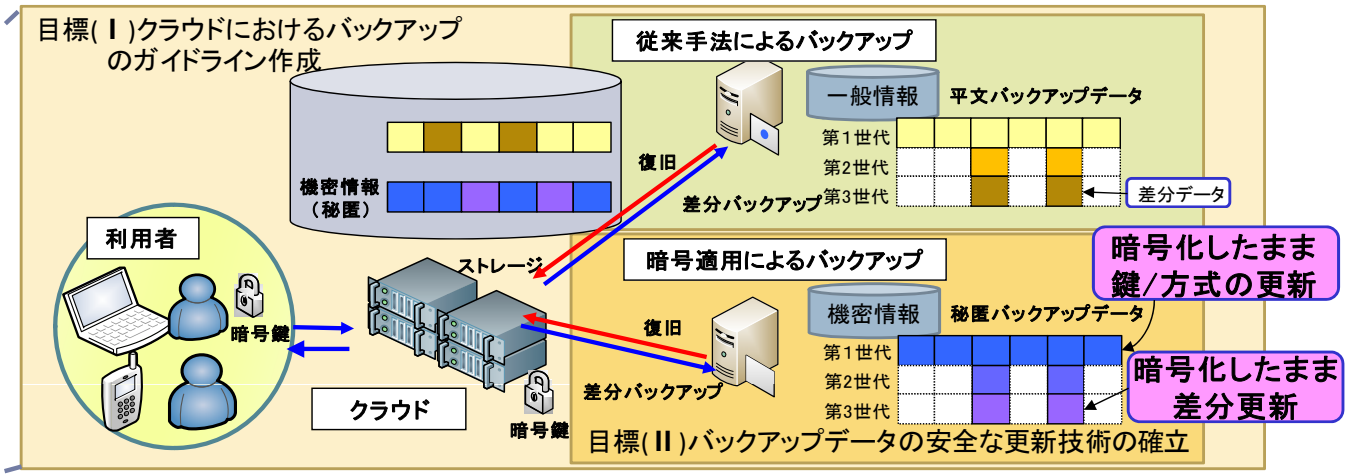
本研究開発の課題概要：
東日本大震災によりバックアップの重要性が見直されている。一方で、その確立された手法は見当たらず、またバックアップデータの暗号化を行う運用は負荷が高い。そこで、**バックアップ手法を取りまとめガイドライン化すると共に、バックアップデータの安全な運用管理の負荷を低減する技術を開発**する。

目標：
（I）大規模災害またはサイバー攻撃などからの復旧時に備えた、**クラウドにおけるバックアップを安全に行うためのガイドラインの作成**
（II）**長期間に渡るバックアップデータの高い秘匿性を維持する技術、およびバックアップデータを秘匿化したまま、差分の生じたデータを更新する技術の開発**

主な成果：
（I）東日本大震災で機能した／機能しなかったバックアップの事例を調査し、課題を整理・体系化し、**ディザスタリカバリ計画支援のガイドライン**を作成。
（II）**暗号化したバックアップデータを復号せずに差分バックアップを実現するための、差分箇所を検知・更新する技術の設計、プロトタイプ作成完了**。

【課題概要図】

ガイドラインの構成案
1. 本ガイドの目的と適用範囲
2. 最近の震災・事件から再確認されたバックアップの重要性
3. DR向けクラウドバックアップの計画プロセスの概要
4. DR向けクラウドバックアップの計画プロセスの詳細
5. DR向けクラウドバックアップの計画パターン事例
6. 付録、参考文献



DR: Disaster Recovery, 災害など致命的なシステム障害から情報システムを復旧させること

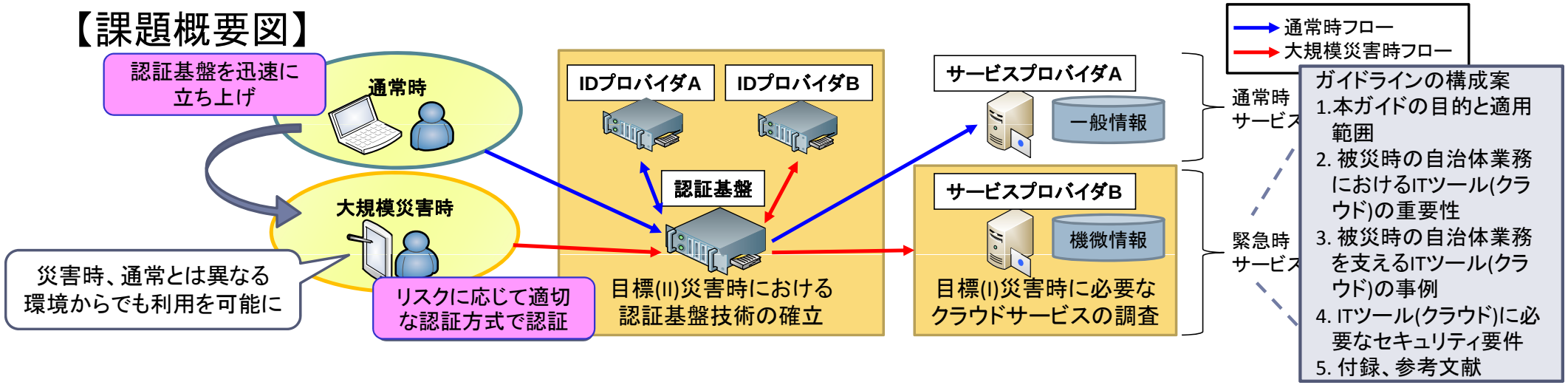
3）大規模災害に備えたクラウド移行促進技術
（B）大規模災害時のクラウドサービスに適した認証基盤技術

本研究開発の課題概要：
東日本大震災への対応でクラウドサービスの有用性が見直された一方、災害時のIT利用におけるセキュリティを考慮したガイドラインは見当たらない。また、災害対応時には通常とは異なる業務システムを、通常とは異なる環境から利用することが想定される。そこで**災害時のIT利用事例を取りまとめ、その利用について情報セキュリティを考慮してガイドライン化すると共に、リスクに応じて柔軟に認証方式を選択する認証基盤技術を開発**する。

目標：
(I)**災害時に必要となるクラウドサービスとそのセキュリティ要件をまとめガイドライン化**する
(II)**災害時のクラウドサービスに利用可能な認証機能を迅速に立上げ、業務におけるリスクに応じて認証方式を柔軟に選択する仕組みを備えた認証基盤技術を開発**する

主な成果：
(I)国内と海外の被災自治体に災害時のセキュリティの実態をヒアリングし、課題・要件を整理。防災専門家によるレビューを経て、**災害対応ICTに役立つセキュリティガイドラインを作**成。
(II)災害時の課題の一つとしてユーザ認証の安全性と利便性を両立するため、端末、認証方式、サービスのセキュリティレベルを総合的に判定し、**リスクに応じて認証方式を選択する認証基盤技術を確**立。

【課題概要図】



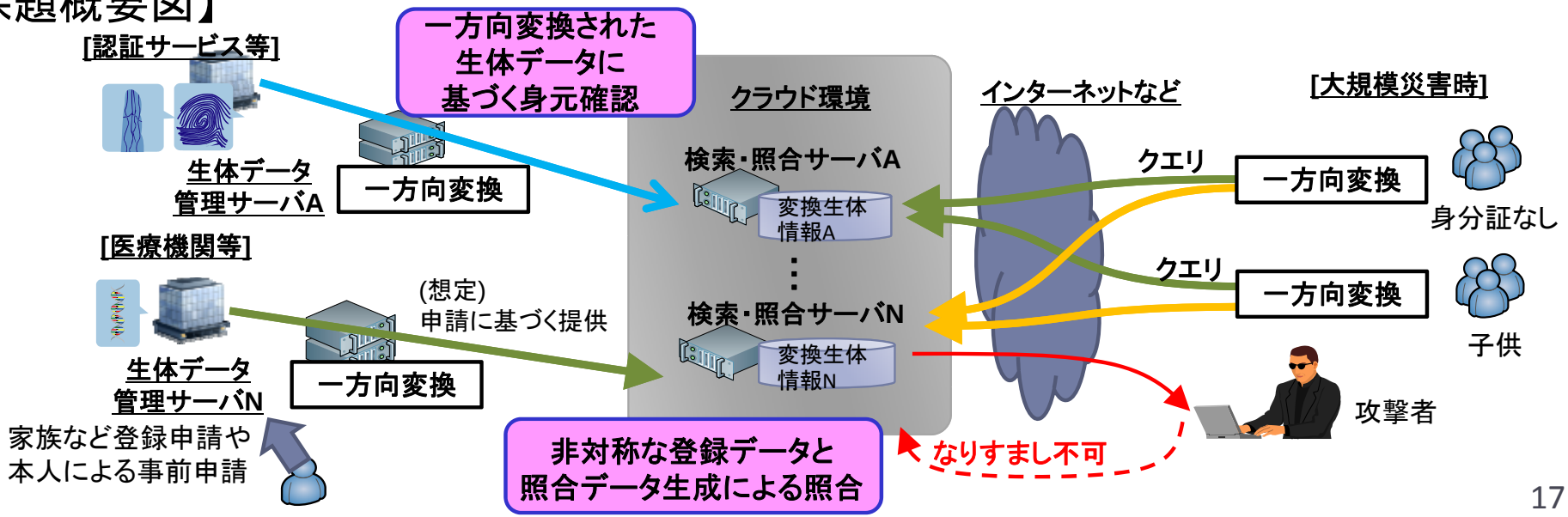
3）大規模災害に備えたクラウド移行促進技術
（C）大規模災害時におけるクラウドを用いた安全な身元確認技術

本研究開発の課題概要：
大規模災害時における被災者は、身分証等のIDカードの所持が期待できない。このため身元確認に生体情報を利用することが考えられるが、そのためには住民の生体情報を事前に保管する必要があり、プライバシー保護の観点で万全の対策が期待される。そこで、**生体情報を元に戻せない形に変換して保管し、認証時にその情報を照合することで、プライバシーを保護した安全な身元確認を行う技術を開**発する。

目標：
以下の性質を満たす**生体情報の変換・照合方式の基本設計および実装・評価**。(i)変換後の情報から元の生体情報を復元・推定できないこと**（一方向性）** (ii)クラウド上に登録された変換情報が仮に漏洩しても、それを悪用したなりすまし攻撃ができないこと**（非対称性）**

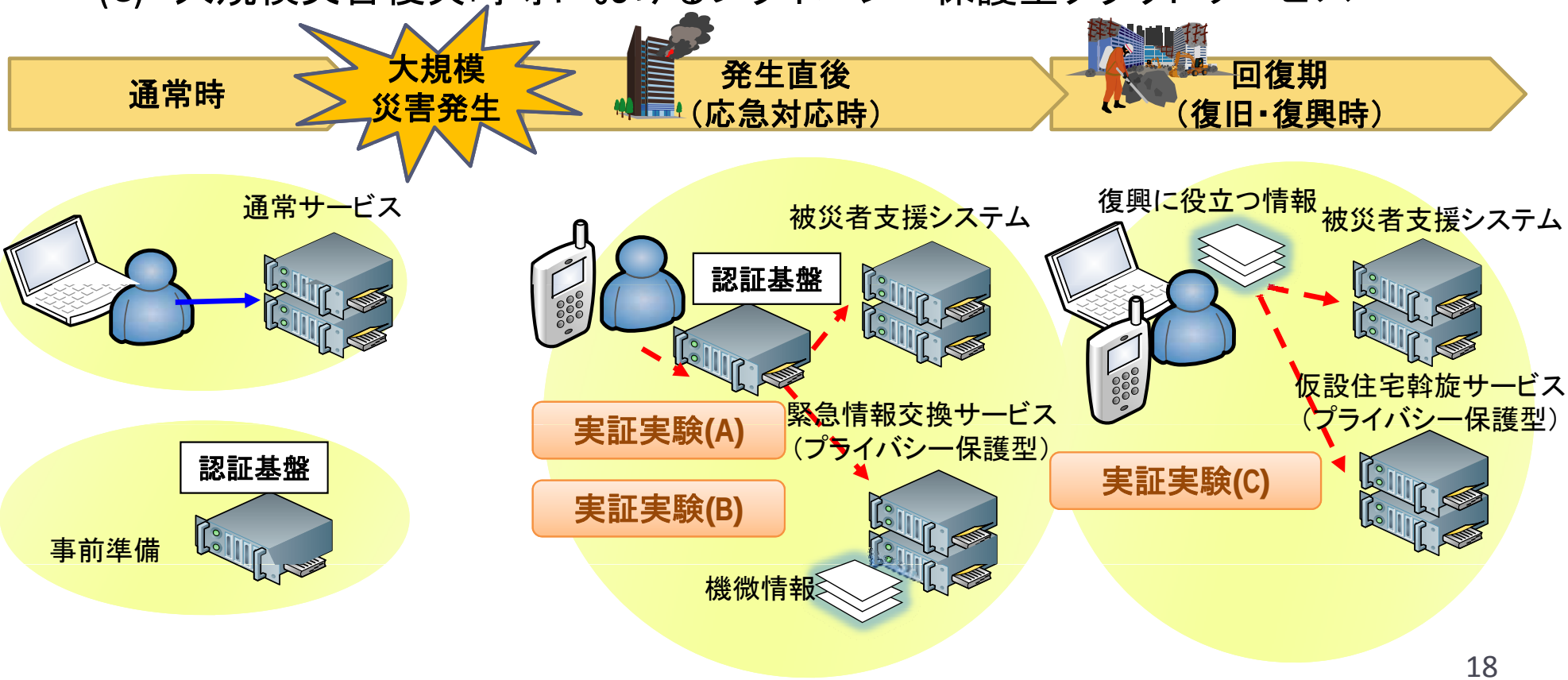
主な成果：
・**曖昧性を許す署名・検証アルゴリズム(Fuzzy Signature)を利用した、生体情報の変換・照合方式を開発**。
・安全性評価として、目標とする(i)一方向性と(ii)非対称性の両方の要件を満たすことを数学的に証明。

【課題概要図】



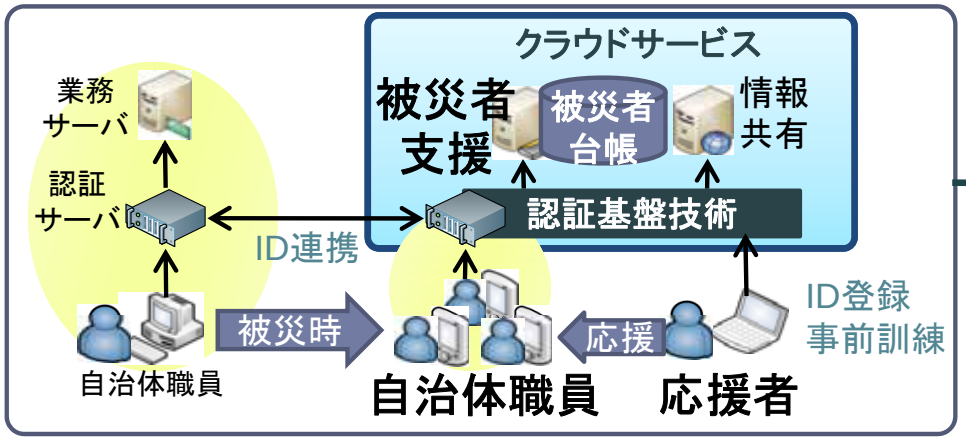
4）大規模災害等に備えた実証実験 [課題 概要]

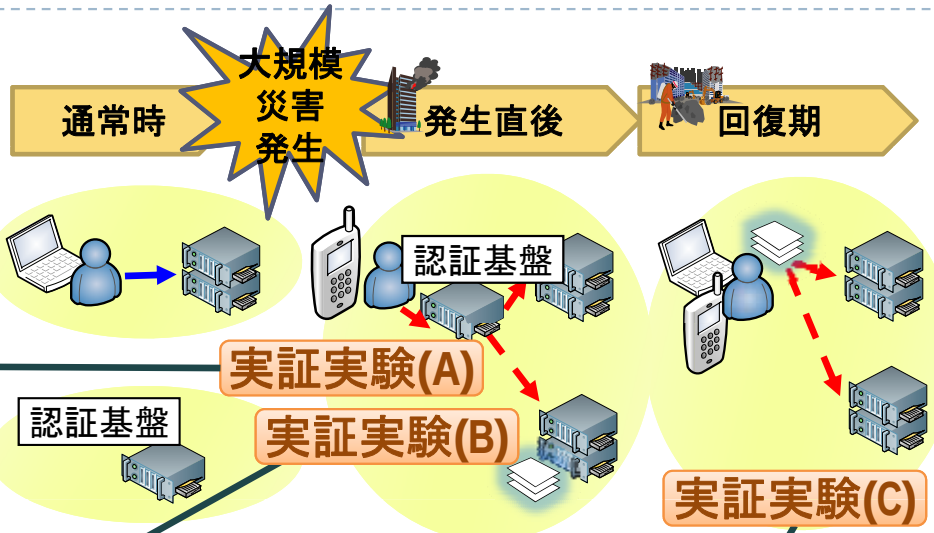
- 概要：
  大規模災害後におけるフェーズを「大規模災害発生直後」と「大規模災害からの回復期」に分け、それぞれの時点において必要となるセキュリティ技術の検証として、課題1）～3）の本研究成果に関する実証実験を、東日本大震災被災に関連する組織との連携等を考慮して行う。
  (A) 大規模災害直後における迅速かつセキュアなクラウドサービスの立ち上げ
  (B) 大規模災害発生時のクラウド型情報交換サービス
  (C) 大規模災害復興時等におけるプライバシー保護型クラウドサービス



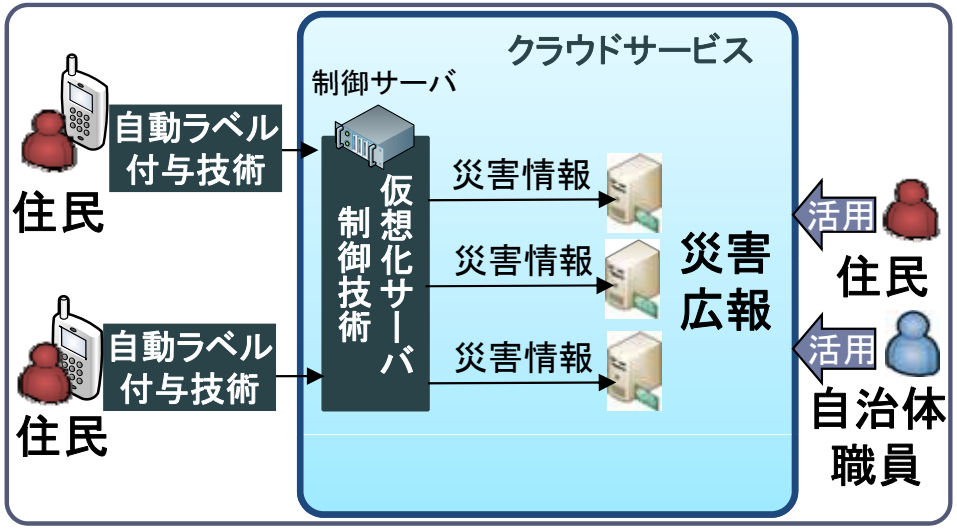
4）大規模災害等に備えた実証実験 [実証実験イメージ]

大規模災害直後における迅速かつセキュアなクラウドサービスの立上げ

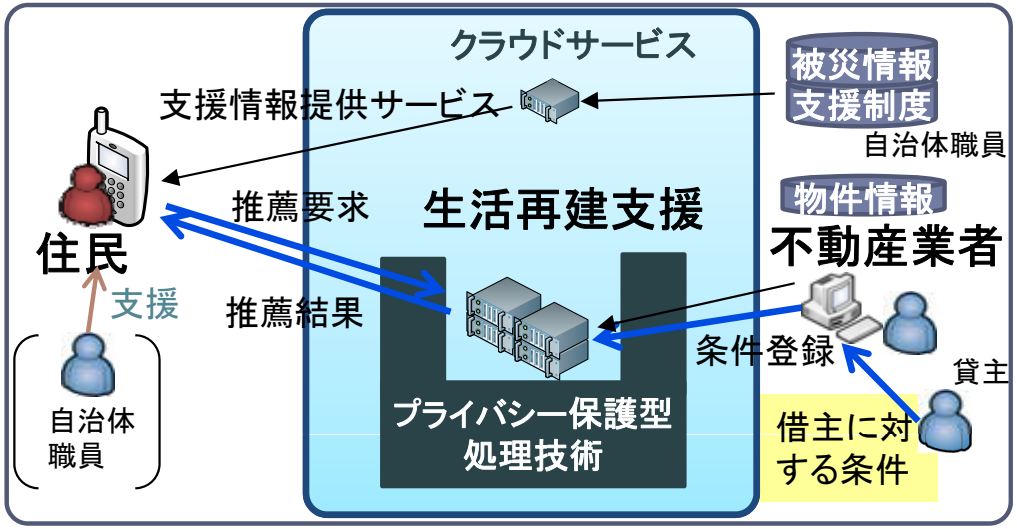




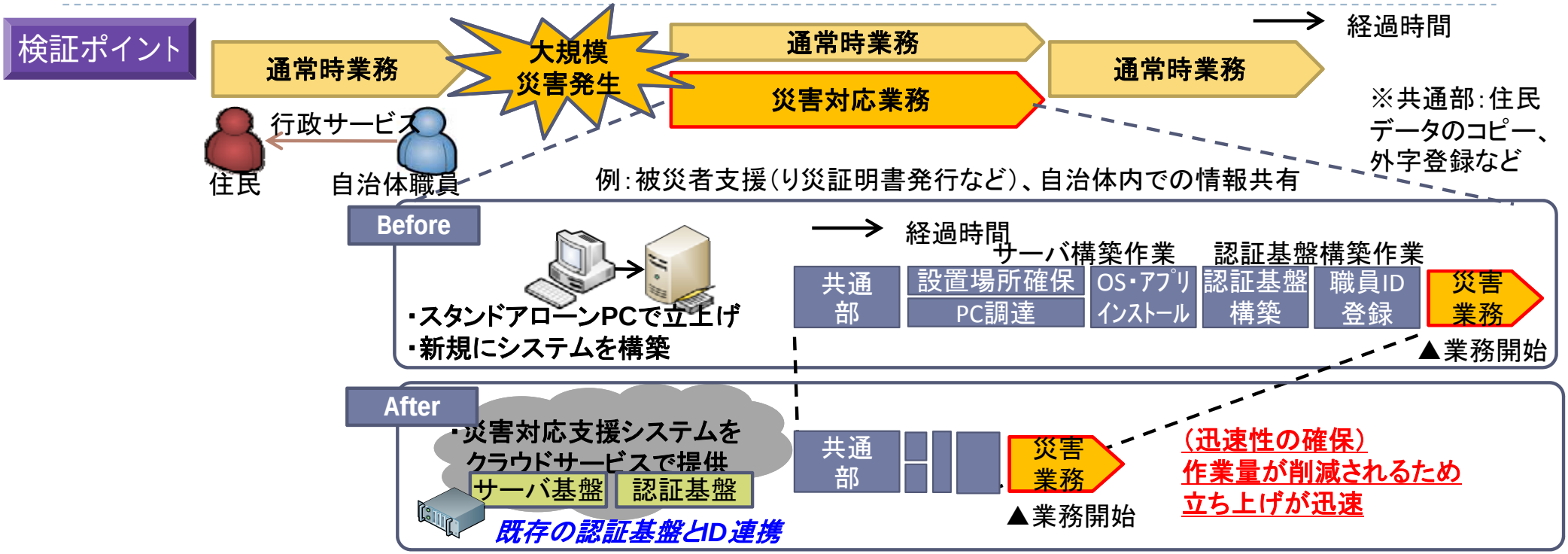
大規模災害発生時のクラウド型情報交換サービス



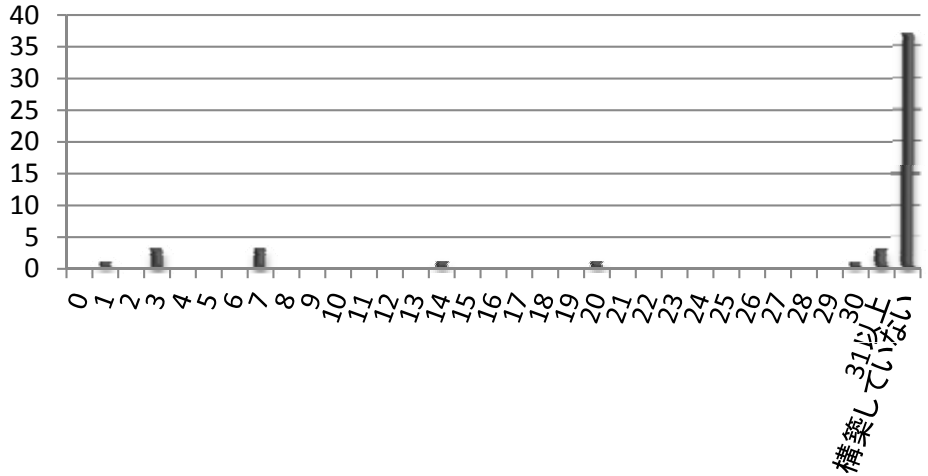
大規模災害復興時等におけるプライバシー保護型クラウドサービス



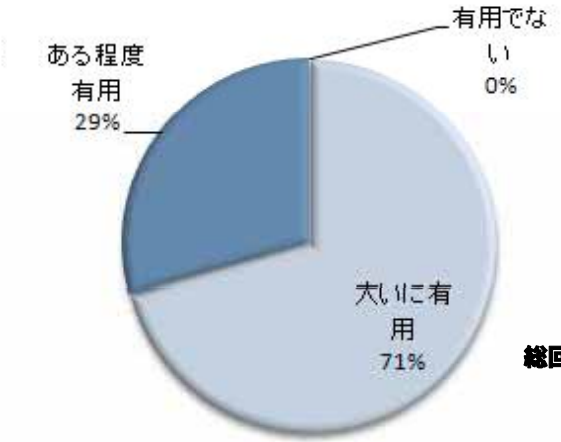
4）実証実験（A）評価結果



(Q1)東日本大震災後に災害対応の**システム構築にどのくらい日数を要し**ましたか？（対象：自治体、ベンダ）



(Q2)**クラウド上でシステムを構築**することで、災害時でも迅速に業務を立ち上げられるとしたら、どのくらい有用ですか？（対象：自治体、ベンダ）

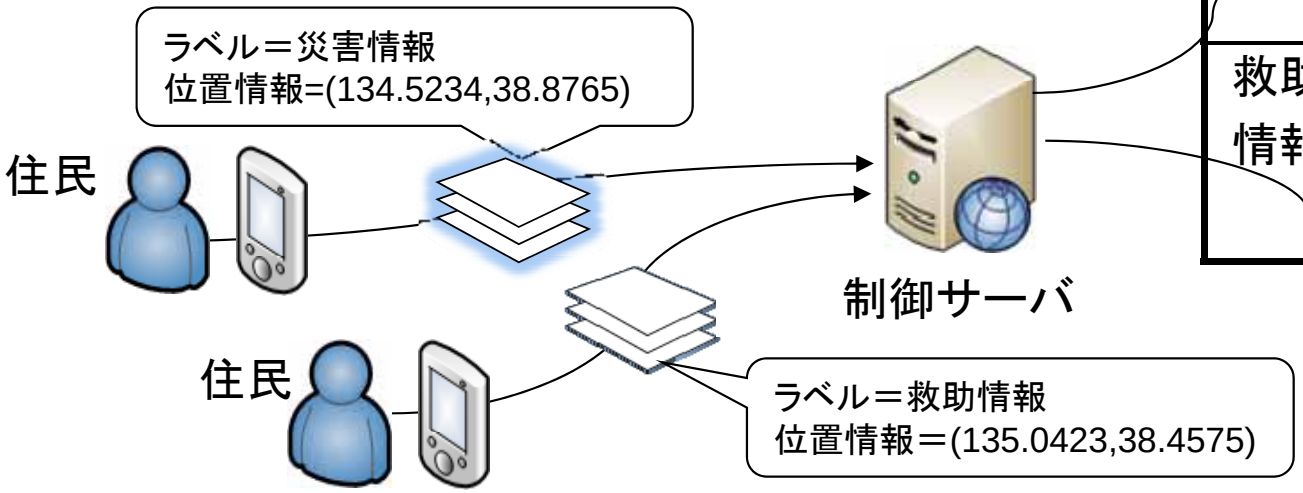


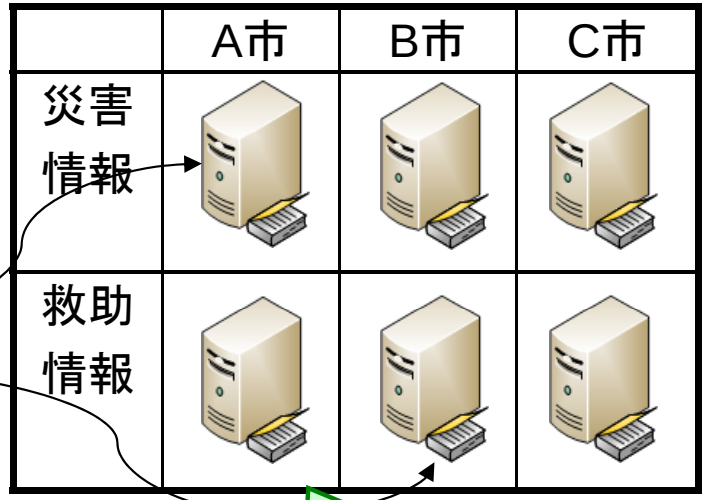
総回答人数:51人

4）実証実験（B）評価結果

検証ポイント

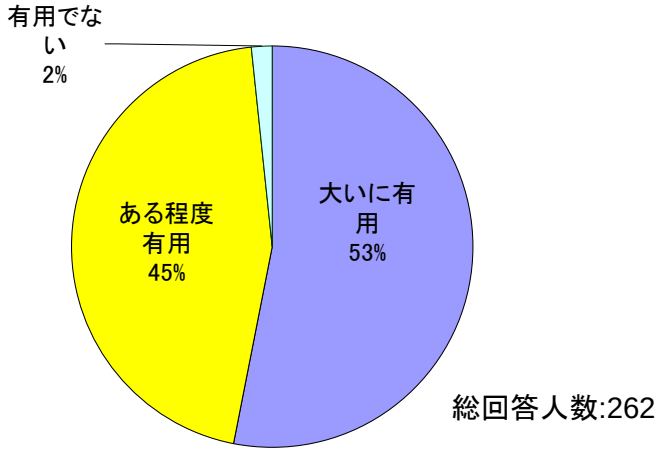
投稿データのラベルと位置情報に基づいて、適切なシステムへ振り分けることで情報収集の効率性を向上





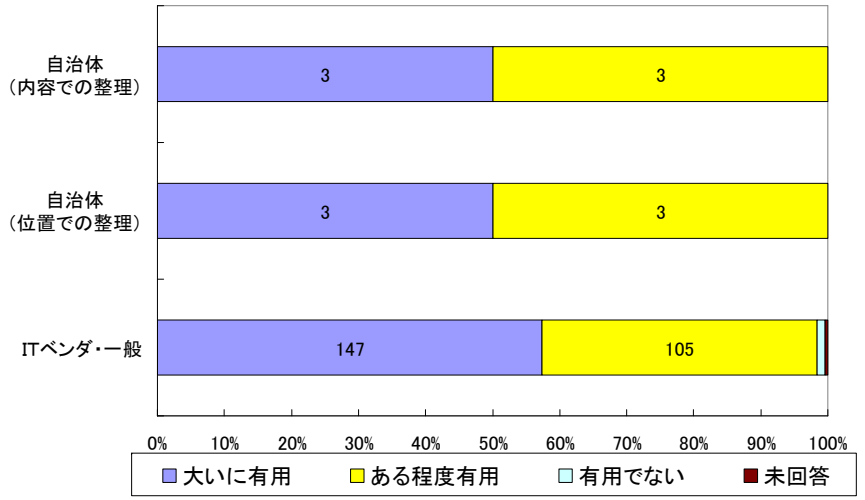
適切な自治体の適切なシステムへ情報を振り分け

(Q1)災害発生時から回復期にかけて多くの情報を収集できることは有用と思いますか？



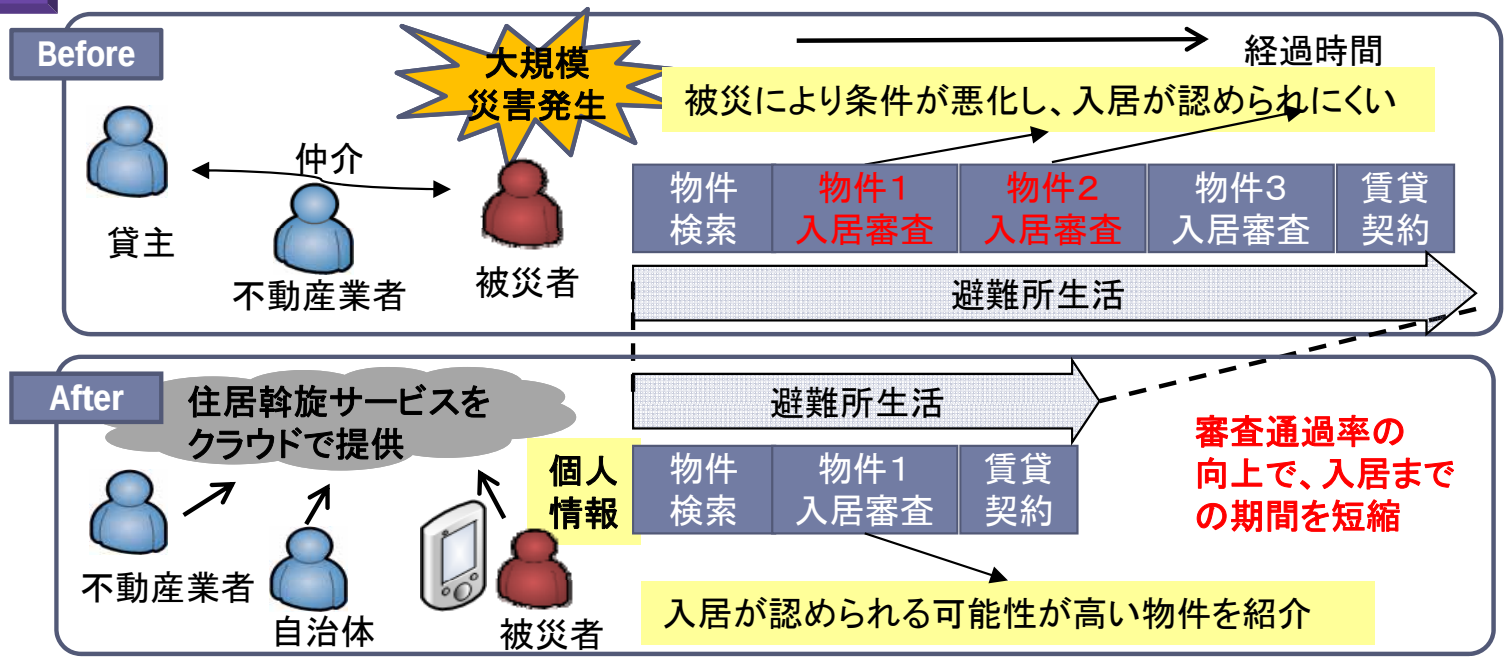
総回答人数:262

(Q2)整理された情報が収集されることは有用と思いますか？

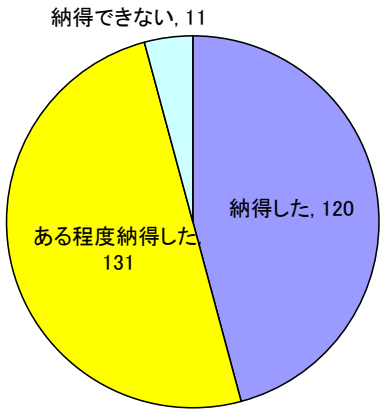


4）実証実験（C）評価結果

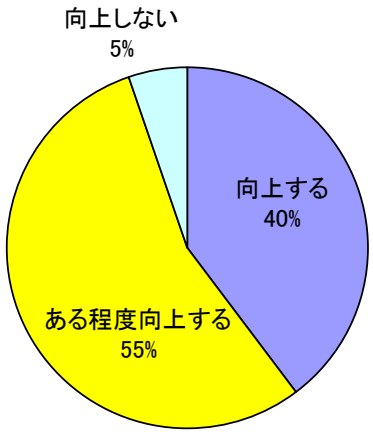
検証ポイント　災害時の賃貸住宅の斡旋を迅速化して賃貸住宅を有効活用し、被災者の生活環境の向上に資する



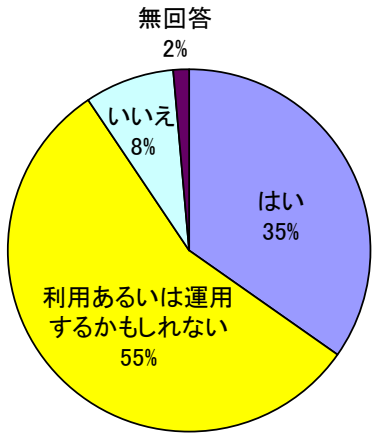
(Q1)本システムは、クラウド上のサービスからの情報漏洩を防止すると納得されましたか？



(Q2)本システムを用いてプライバシー保護が行われることにより、サービス利用時の安心感が向上すると思いますか？



(Q3)本システムが災害時にあれば、利用あるいは運用しても良いと思いましたか？



研究開発成果のまとめ

1）標準化活動

- 本研究の成果に基づいた標準化活動を以下に示す。

#	課題名	内容	標準化活動	勧告化承認状況
1	課題2）（A）セキュリティ対策状況の可視化技術 課題3）（B）大規模災害時のクラウドサービスに適した認証基盤技術	複数のIdSP*環境における複合認証の一般的枠組み	ITU-T Recommendation, X.1154:“ General framework of combined authentication on multiple identity service provider environments”	2013年4月 勧告化承認済み
2	課題2）（B）認証に関するセキュリティ対策状況可視化技術	テンプレート保護型生体認証の保護性能評価方法、 テンプレート保護型生体認証評価プロセス	ITU-T Recommendation X.1091: “A guideline for evaluating telebiometric template protection techniques“	2012年4月 勧告化承認済み

*idSP： identity service provider

2）研究開発成果の展開方針-1

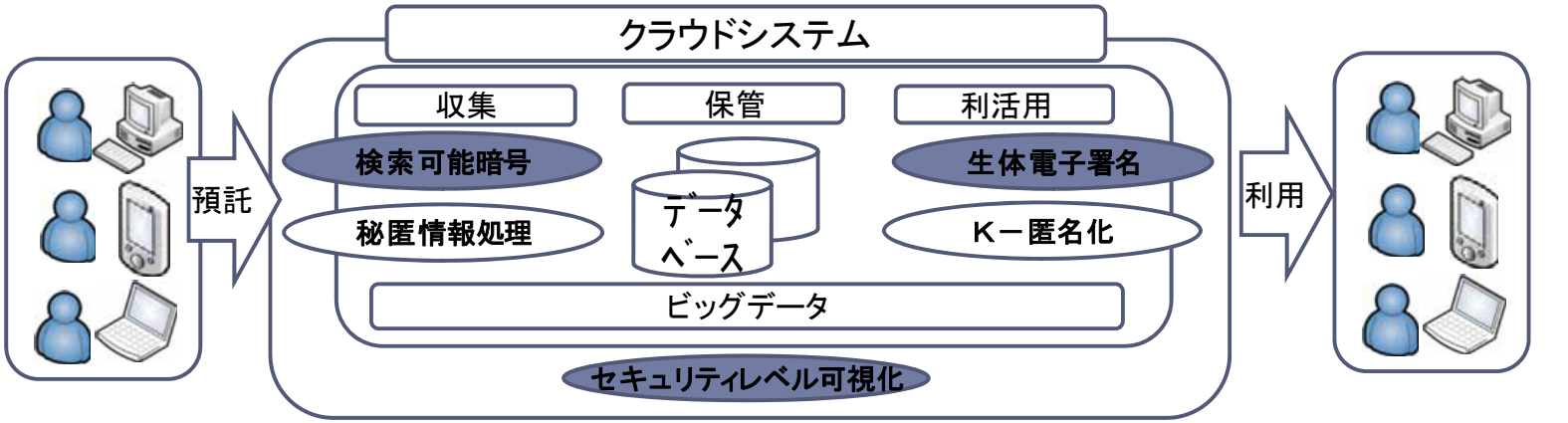
主要開発技術

①クラウド側で暗号化したまま検索処理できる**「検索可能暗号」**
②**「生体情報を用いた電子署名技術」**－ICカードやパスワードを用いずに公開鍵基盤と同様の機能を実現

情報を安心・安全に保管・流通する要素技術の開発

成果展開方針

■クラウドシステムの高信頼化・ビッグデータビジネスにおけるプライバシー保護対策への貢献を成果出口目標とし、適用分野からの業務要件をフィードバックすることで機能向上を図り、ソリューション化を推進する。



研　究	実用化検討	適　用
要素技術 ・検索可能暗号 ・生体電子署名 ・セキュリティレベル可視化	業務要件整理 機能拡充・ソリューション化推進	ソリューション展開 ・高信頼クラウド ・ビッグデータ

2）研究開発成果の展開方針-2

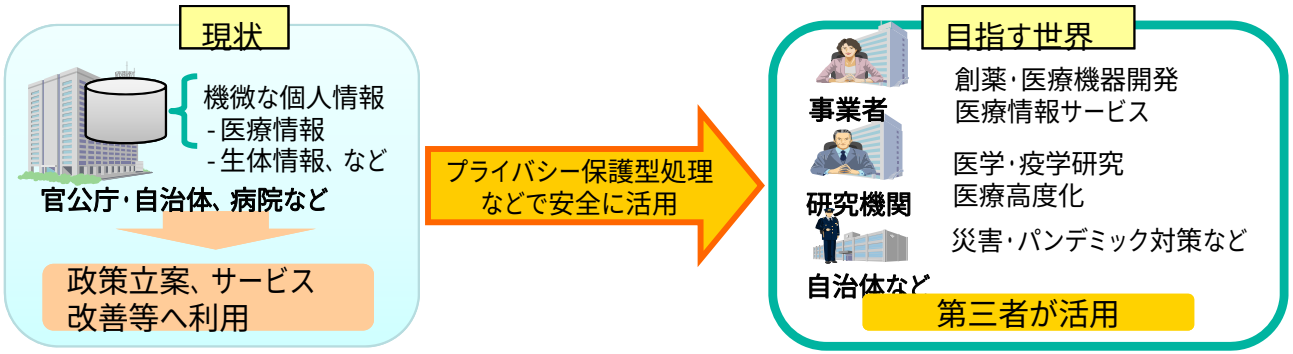
主要開発技術

①クラウド側で暗号化したまま統計演算ができる「**データ統計処理技術（正確性重視）**」の開発

②「**データ保護ポリシーの調停・可視化技術**」の開発

成果展開方針

暗号化したままでのデータ処理による医療情報や生体情報などの機微な個人情報を活用するソリューションやデータの保護と利用に関するポリシーを両立させ個人情報を活用するサービス等への研究成果展開の検討を進める。



主要開発技術

①データの重要度を判定する「**データ重要度可視化技術**」の開発

成果展開方針

データ重要度可視化技術について、ソリューションビジネス等での活用を検討する。