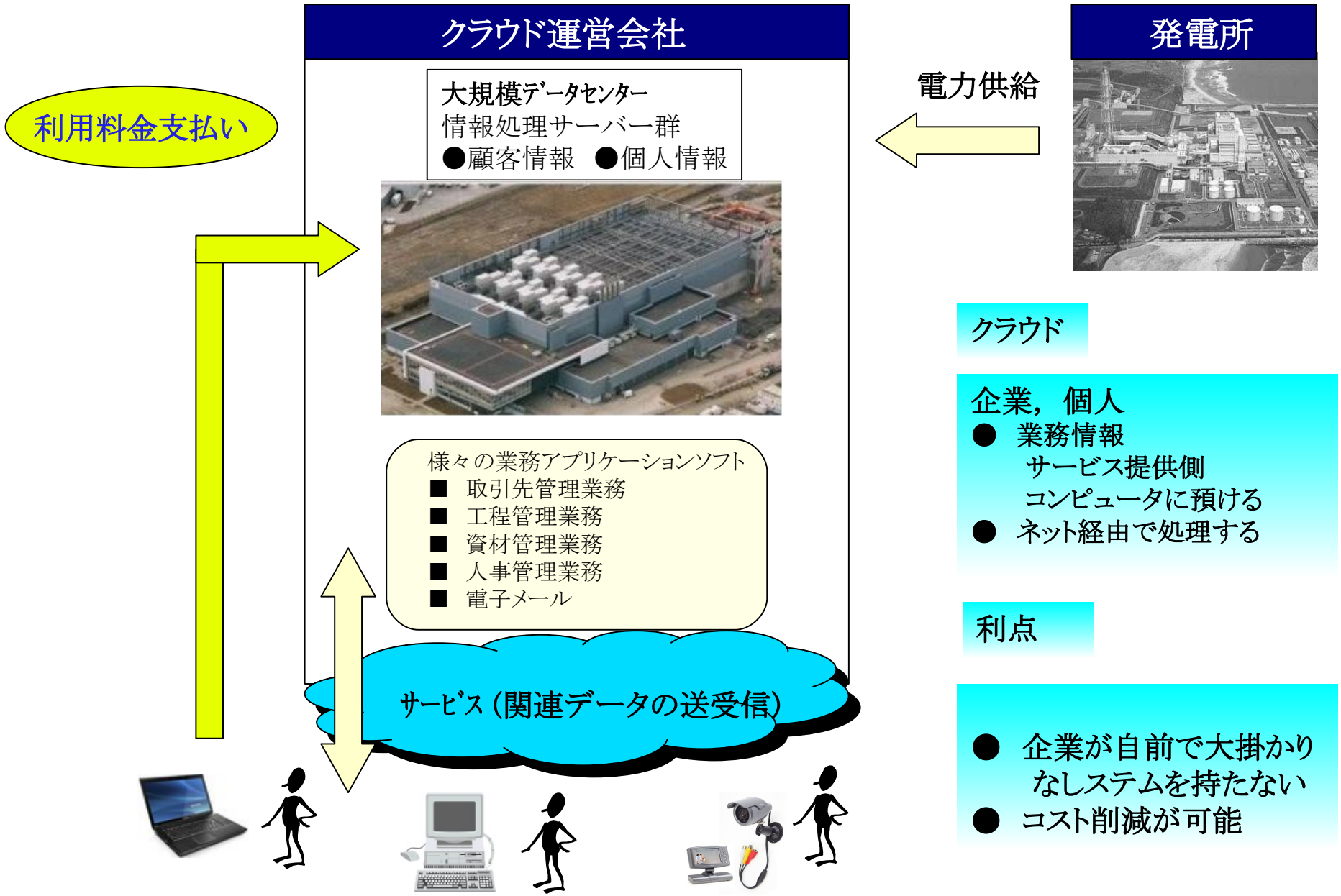
AA&S

クラウドコンピューティングとIDベース暗号との融合による安全性の向上と、データ、サービス連携技術の開発

Advanced Algorithm & Systems

クラウドコンピューティングシステム



クラウド

企業，個人

- 業務情報
  サービス提供側
  コンピュータに預ける
- ネット経由で処理する

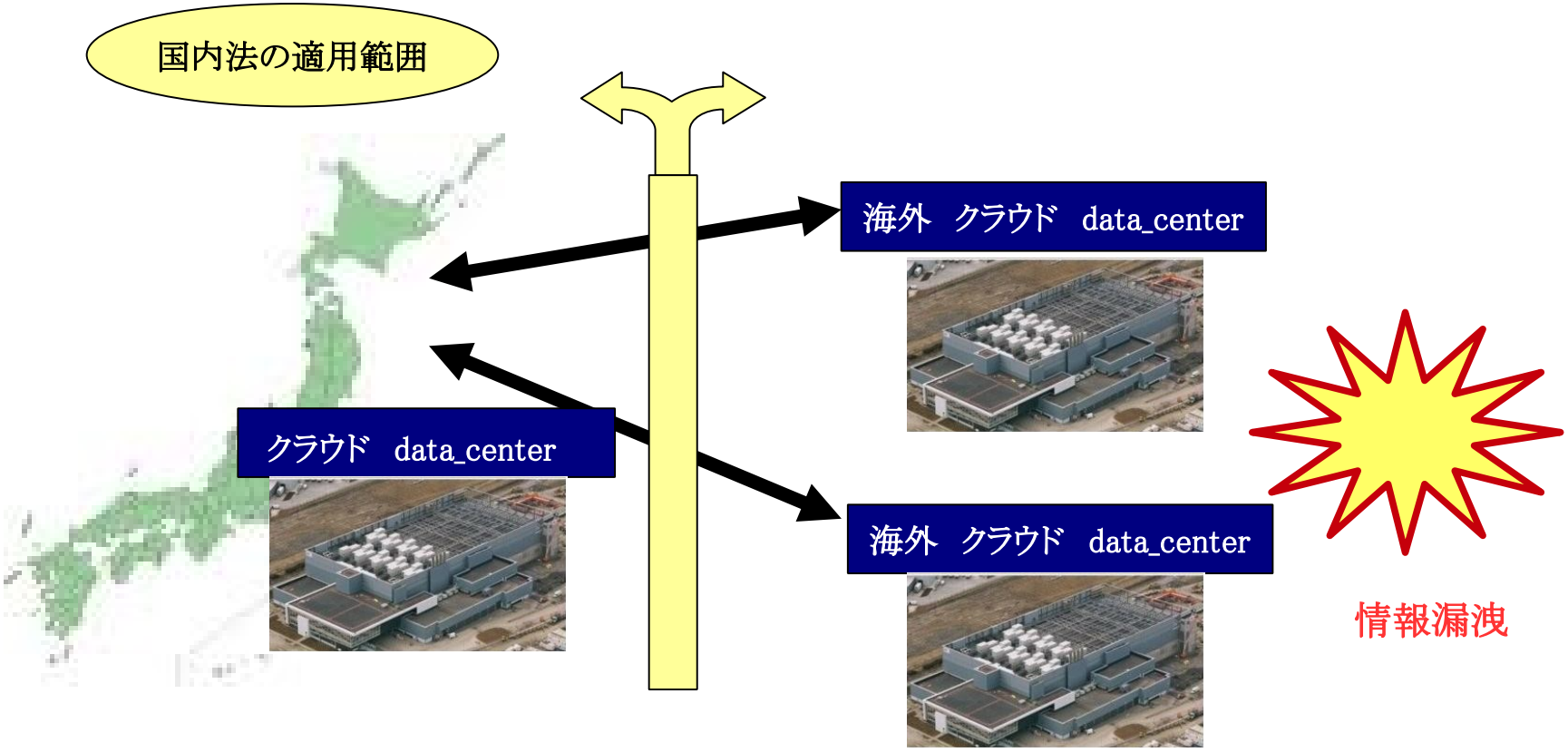
利点

- 企業が自前で大掛かり
  なしステムを持たない
- コスト削減が可能

クラウドコンピューティングシステム

問題点　　クラウドを運用する場合、電力料金の安い海外のデータセンタを利用することが多くなる。
海外のデータセンタで情報漏洩が発生した場合、 国内法は適用されない。

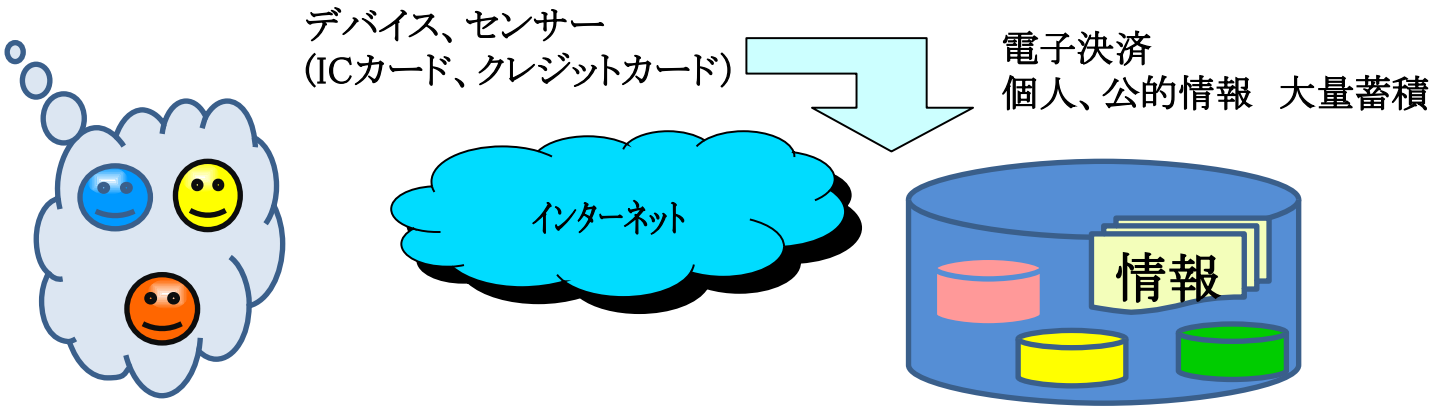
対策　　クラウドの安全性を仮定しない、情報セキュリティシステムの導入。



個人の情報の安全性と経済的活用

個人の情報

個人情報	個人を識別する情報	姓名、生年月日、住所、電話番号
ライフログ情報	購買情報	お金の支払いに関する情報
	閲覧情報	どんなWebページ、テレビを見たか
	行動履歴	どこに行ったか
	健康履歴	体重、体温変動の記録、食の記録、定期健康診断の記録
公的モニタ情報	介護履歴	体重、体温変動の記録、食の記録、介護の記録
	監視履歴	監視カメラの記録
	環境データ	気温、湿度、風向、風速、空調電力



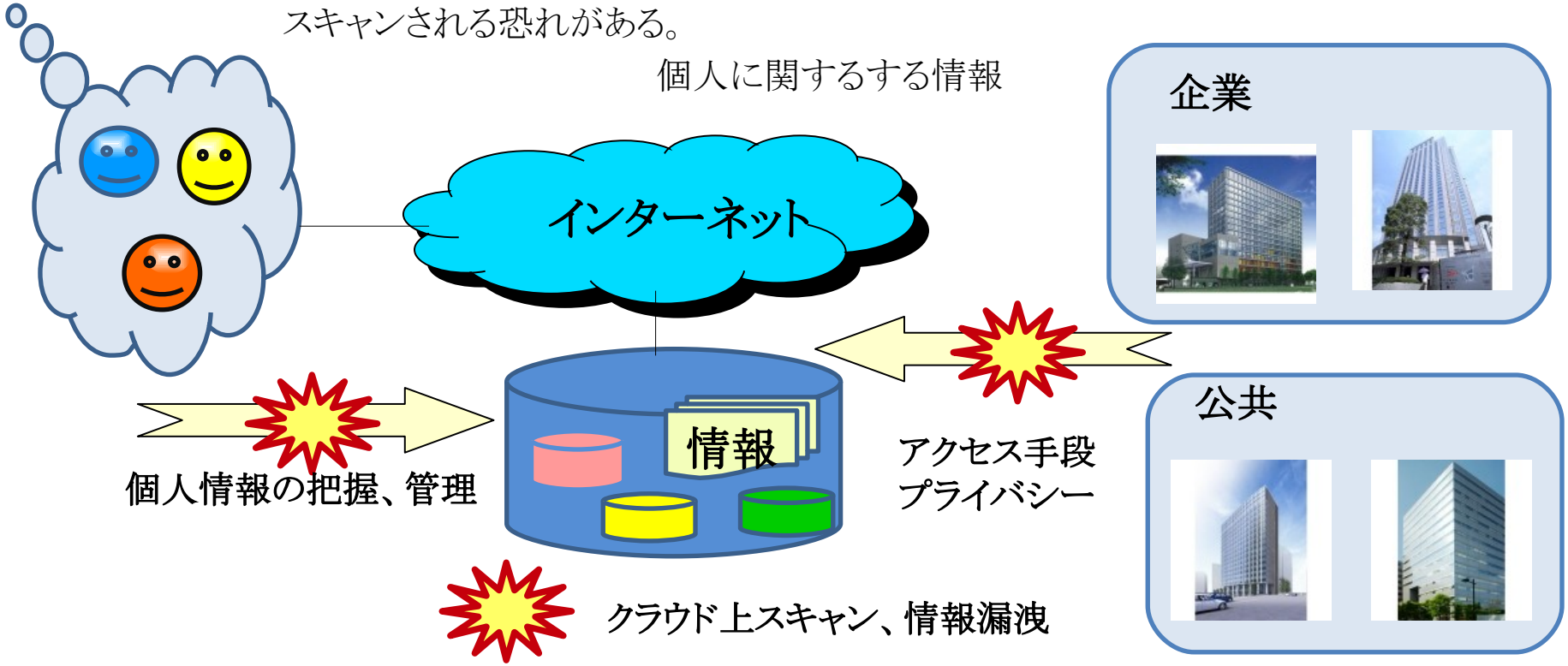
個人の情報の安全性と経済的活用

課題

- 個人に関するする情報を把握、管理することができない。
- 企業がクラウドに蓄積された情報をアクセスする手段がない
- 個人に関するする情報の利用に対する対価を分配できない。

個人の情報の利用が進んでいない理由

- 個人に関するする情報を細かくセキュリティ管理して企業に提供できない。
- プライバシイの多く含まれる、個人に関するする情報をクラウドに蓄積するとスキャンされる恐れがある。



クラウド上メタデータを活用したシステム技術の概要

AA&S

Web2.0技術を活用したメッセージ交換・データ蓄積型のクラウドサービスの構築技術

基本機能

- メタデータを活用したデータ整理と格納
- タグ付加サポート
- タグを利用した検索・ネット経由での活用
- 各種入出力ディバイスやアプリケーションに依存しないアプリケーション開発用のREST　API

セキュリティ機能

- Attributeベース関数クラスの使用による細かいアクセス制御の設定
- IDを利用した鍵交換、権限委譲方式の採用
- タグ(キーワード)により、暗号化したままの検索機能
- XMLベース

付加機能

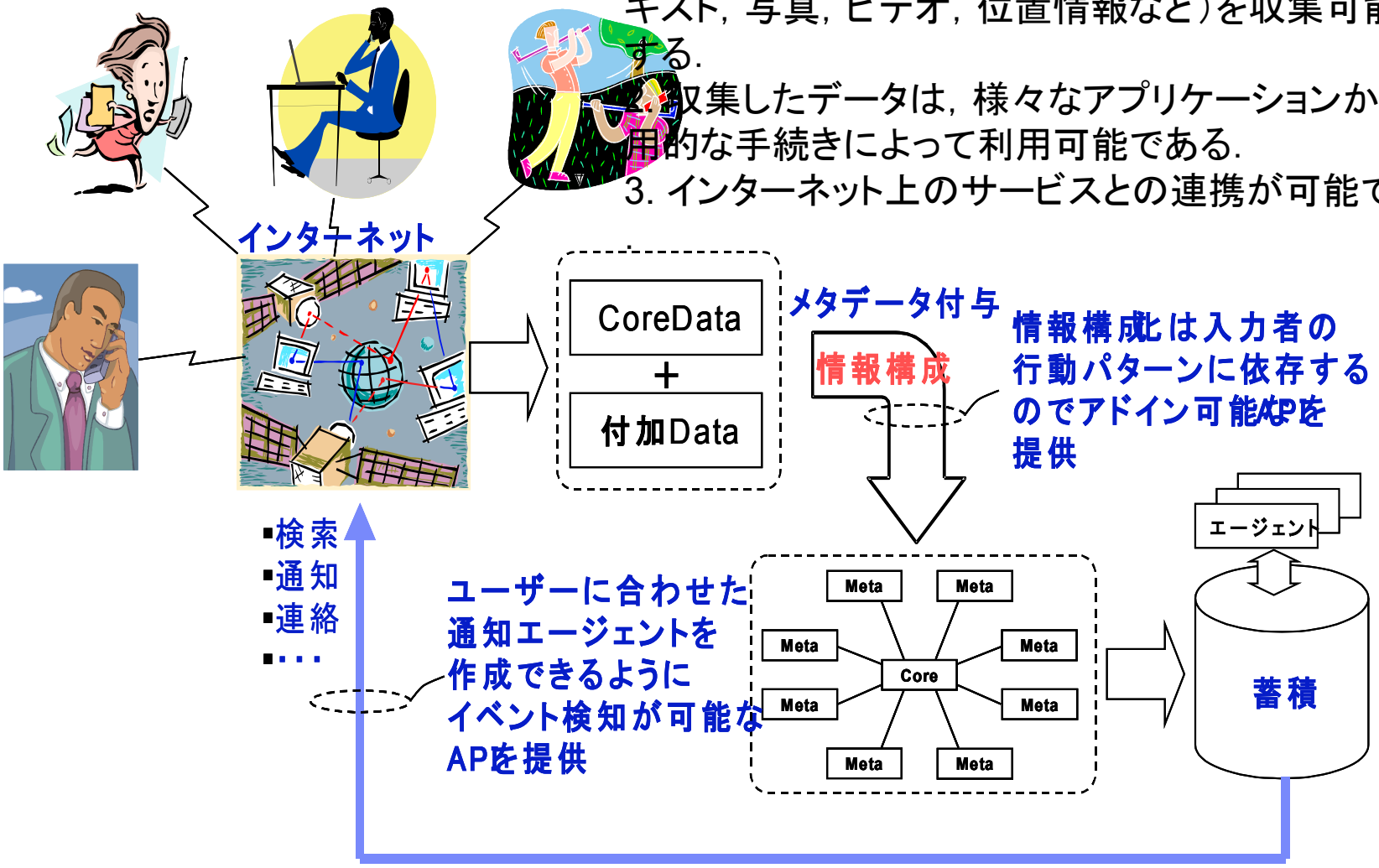
- テキスト・画像等の多様な情報を扱う
- インターネットサービス(youTube , Flickrなど)を活用できる配信・検索機能

実世界データ利用サービス

関係者外秘

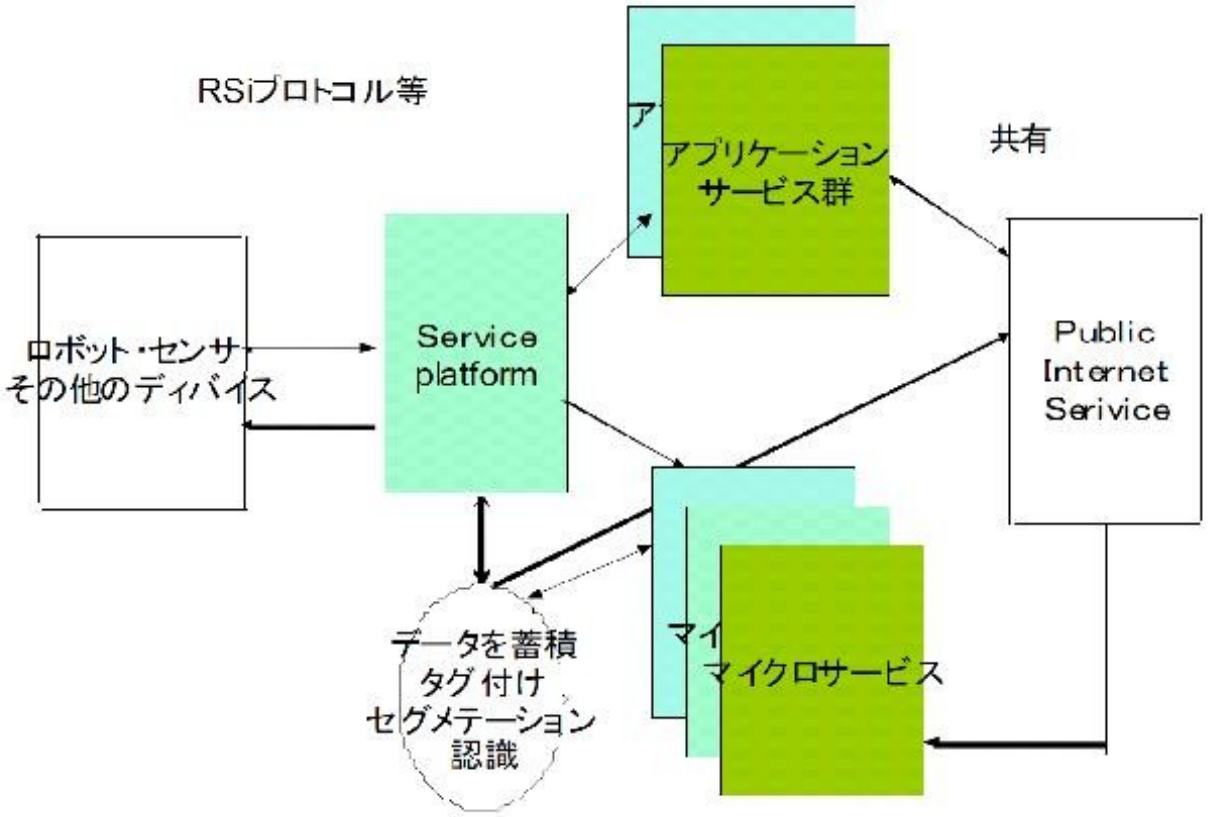
図2：メタデータ付きデータの蓄積と取り出し

1. 様々なデバイス（携帯電話，PC，ICタグ，センサ，ロボットなど）から，多様なデータ形式のデータ（テキスト，写真，ビデオ，位置情報など）を収集可能にする．
2. 収集したデータは，様々なアプリケーションから汎用的な手続きによって利用可能である．
3. インターネット上のサービスとの連携が可能である



実世界データ利用サービスのアーキテクチャー

本アーキテクチャにより、入力デバイスに依存せず従来バラバラに保管されていた情報の一元管理が可能になる



A本社

個人の情報

アクセス

企業

公共、医療、介護

店舗　POS

個人利用

B本社

店舗　POS

インターネット

セキュリティ管理センター

クラウド運営会社　iDC

情報バンク

家計簿アプリ

Webアプリ

監視モニター
環境モニター

クラウド上メタデータを活用したシステム技術の概要

AA&S

- ***産総研の開発したCFE暗号方式の特徴***
  - 従来のPKI方式だと，データが権限分増えてしまうが，新方式だとデータ自身が暗号化されるので，データ量は小さいままである．
  - 個人が設定した小さい単位で安全性を担保することが出来るので，アプリケーション等で企業が利用するまで，情報が漏えいする等の危険性が激減する．

- ***適用した場合の利点***
  - 個人情報やプライバシーの保護
    マイクロサービスが取得するライフログの公開範疇のコントロールによる個人情報・プライバシーなどの考慮が可能となる。
  - ポリシーの設定によるきめの細かいデータへのアクセス管理が可能となる。