

Knowledge Emergence Infrastructure by Convergence of Real World and IT

30 September, 2009

Systems Development Laboratory, Hitachi, Ltd.

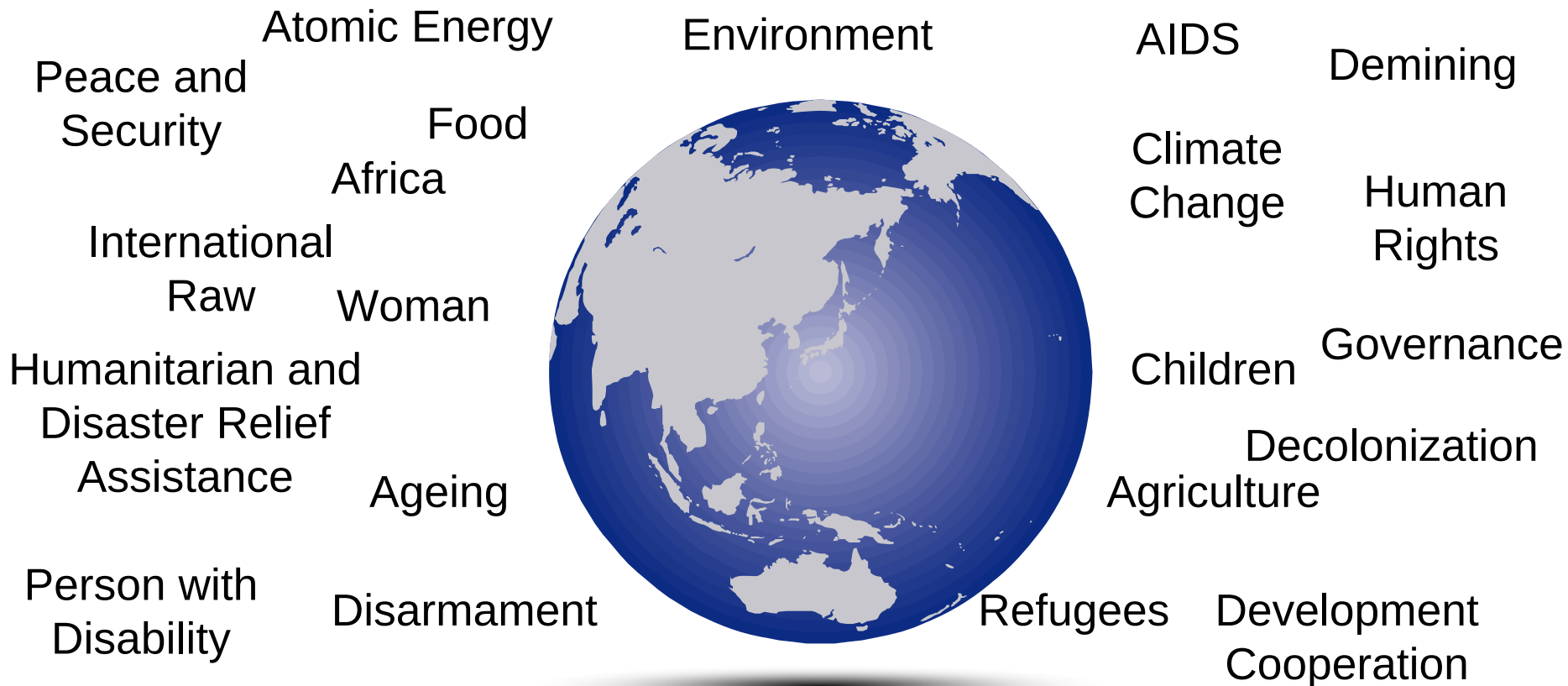
Akira Maeda

Contents

1. Social Innovation Induced by IT
2. KaaS: Knowledge as a Services
3. Information Security for KaaS
4. Conclusions

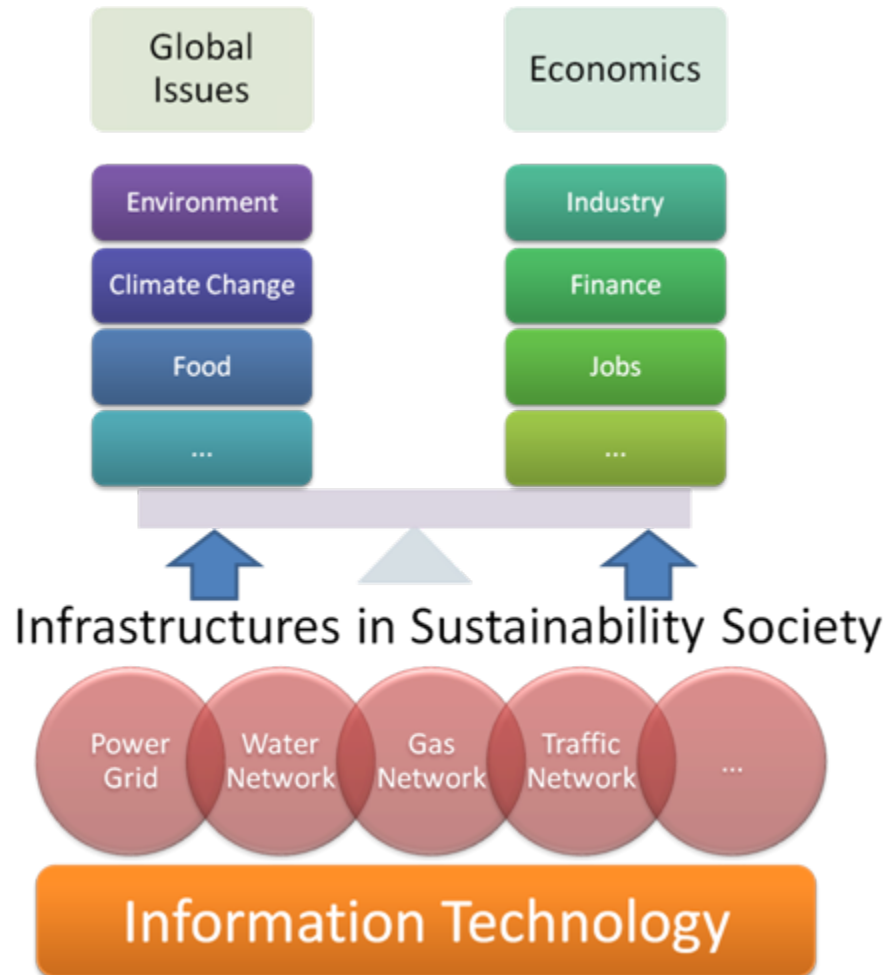
21 global issues grappled by the United Nations

<http://www.un.org/en/globalissues/>



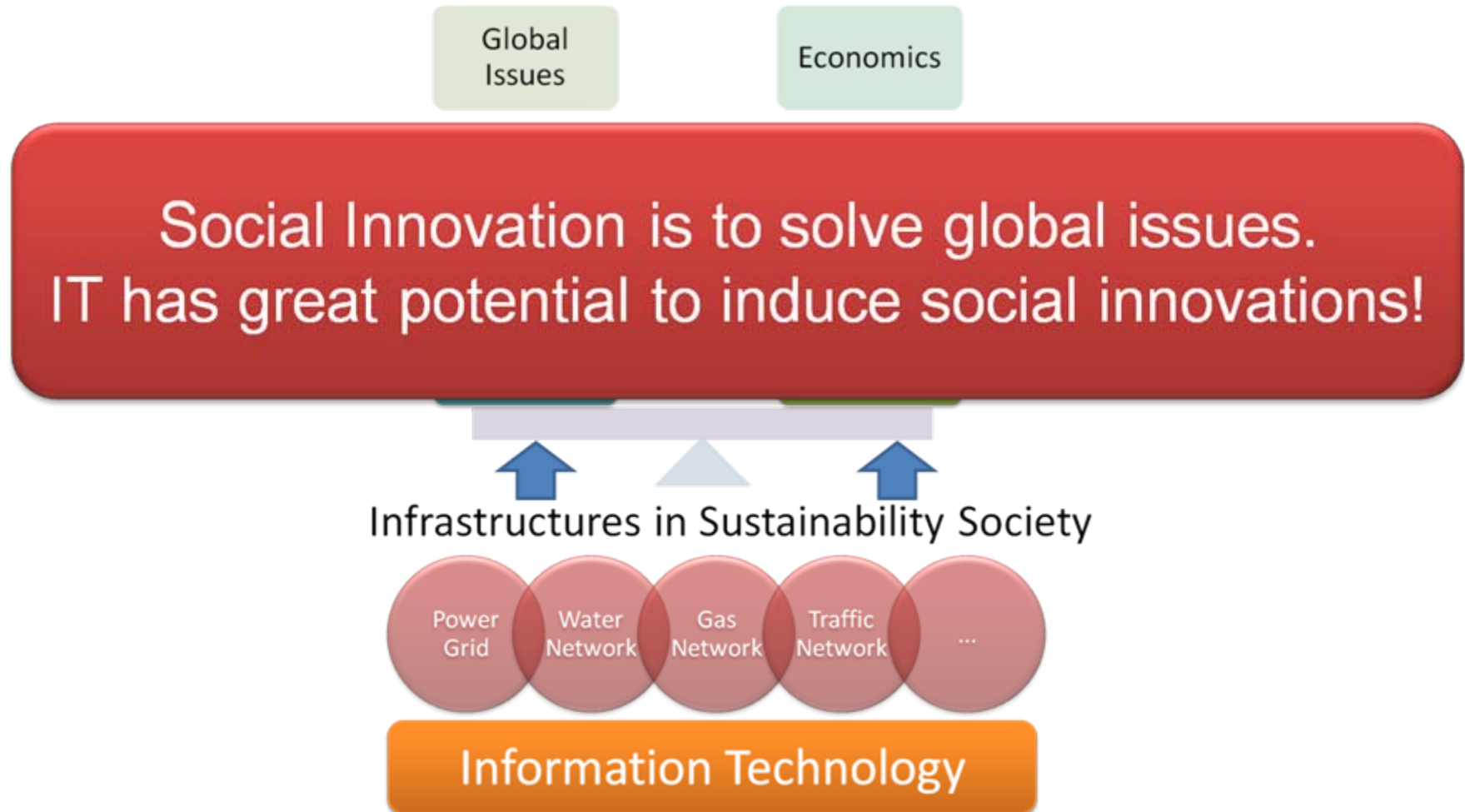
1-2. Reasonable Approach to Tackle Global Issues

- It is important to improve efficiency of activity in daily life to harmonize issues.
- Social Infrastructures that support daily life should be “globally” optimized.
- IT plays a roll for a **infrastructure of infrastructures**.



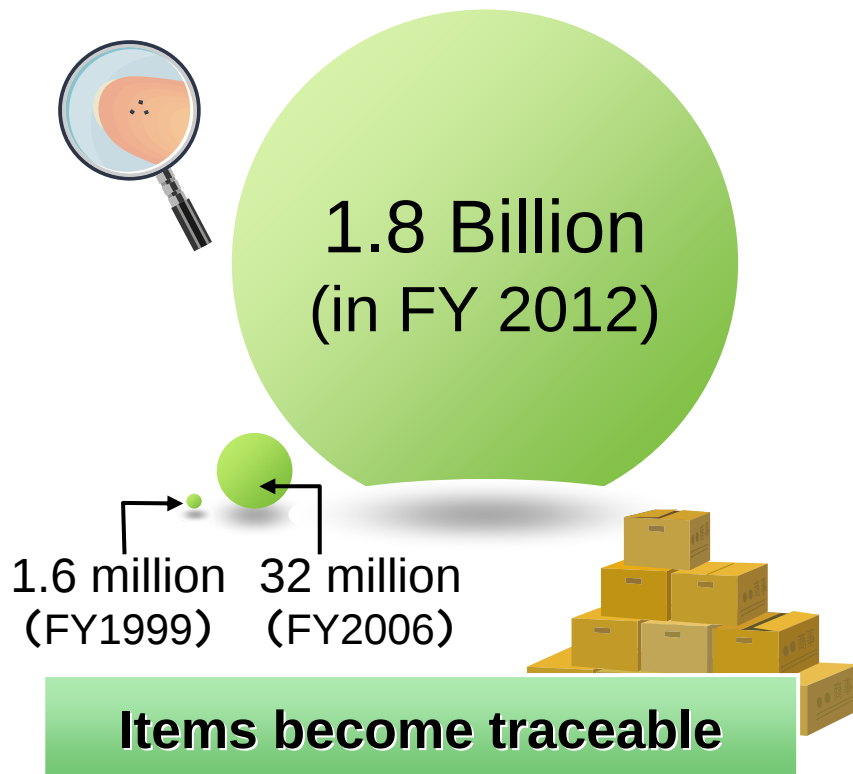
1-2. Reasonable Approach to Tackle Global Issues

- It is important to improve efficiency of activity in daily life to harmonize issues.
- Social Infrastructures that support daily life should be “globally” optimized.
- IT plays a roll for a **infrastructure of infrastructures**.

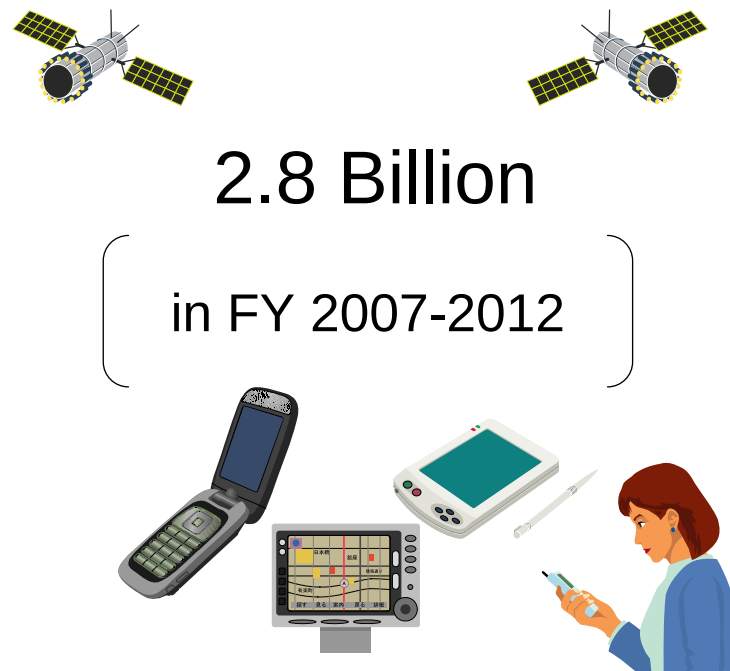


1-3. Upcoming Information-Explosion Era

Produced RFID (Japan)



Shipped GPS cell phones (W/W)

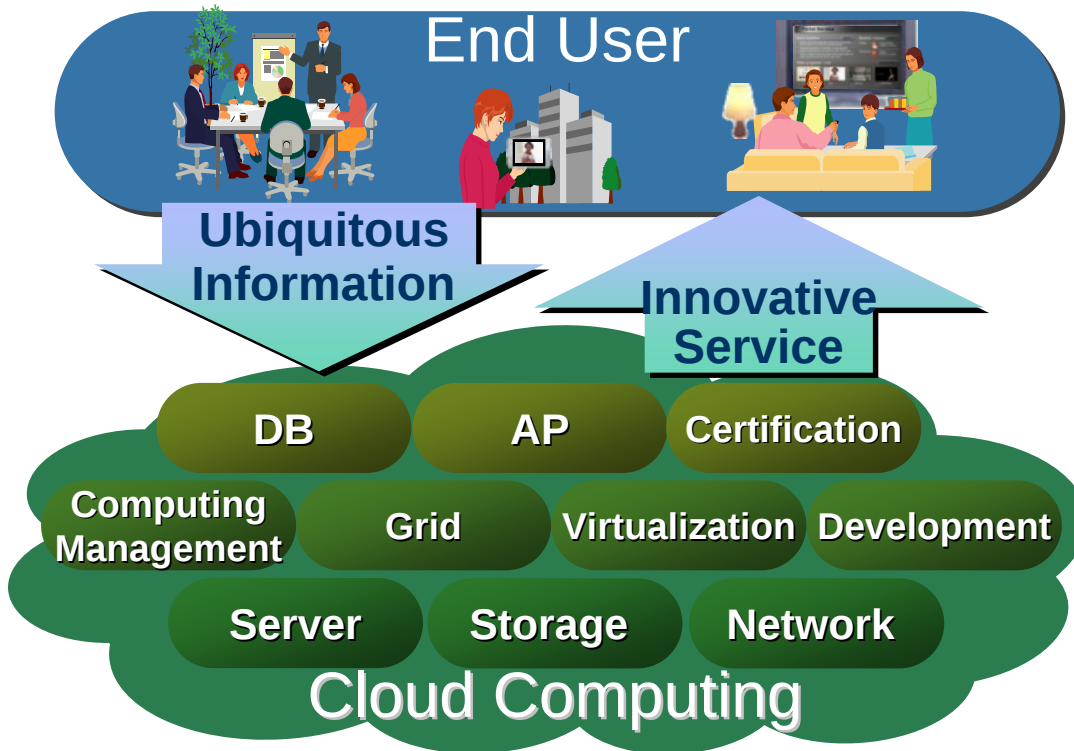


Reference: Yano Research, Parks Associates

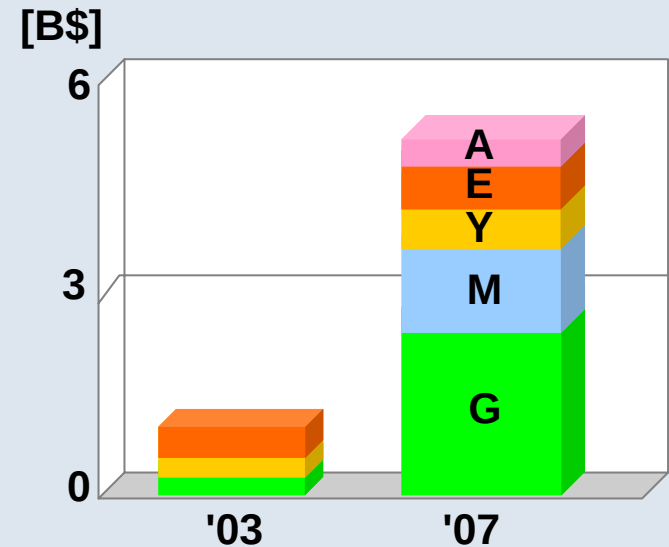
Newly evolutionary services will be available by storing and using massive amount of real world data

1-4. The Cloud yet to Come

Cloud absorbing huge amount of ubiquitous data will gain ability to generate even more evolutionary services. The cycle will go on.



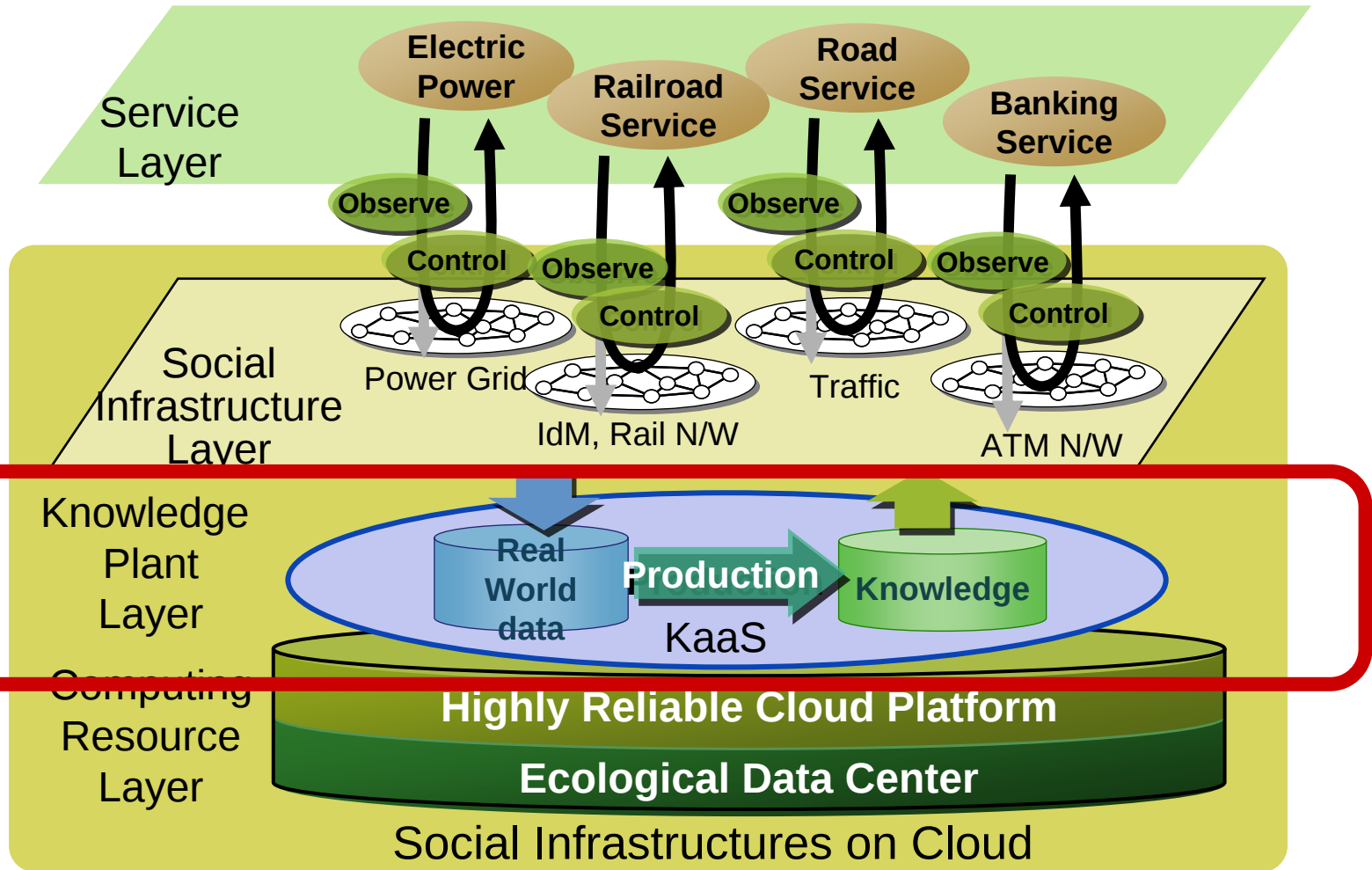
Expenditure for Datacenter



Cloud computing enables service providers to acquire valuable information and store them in the black box

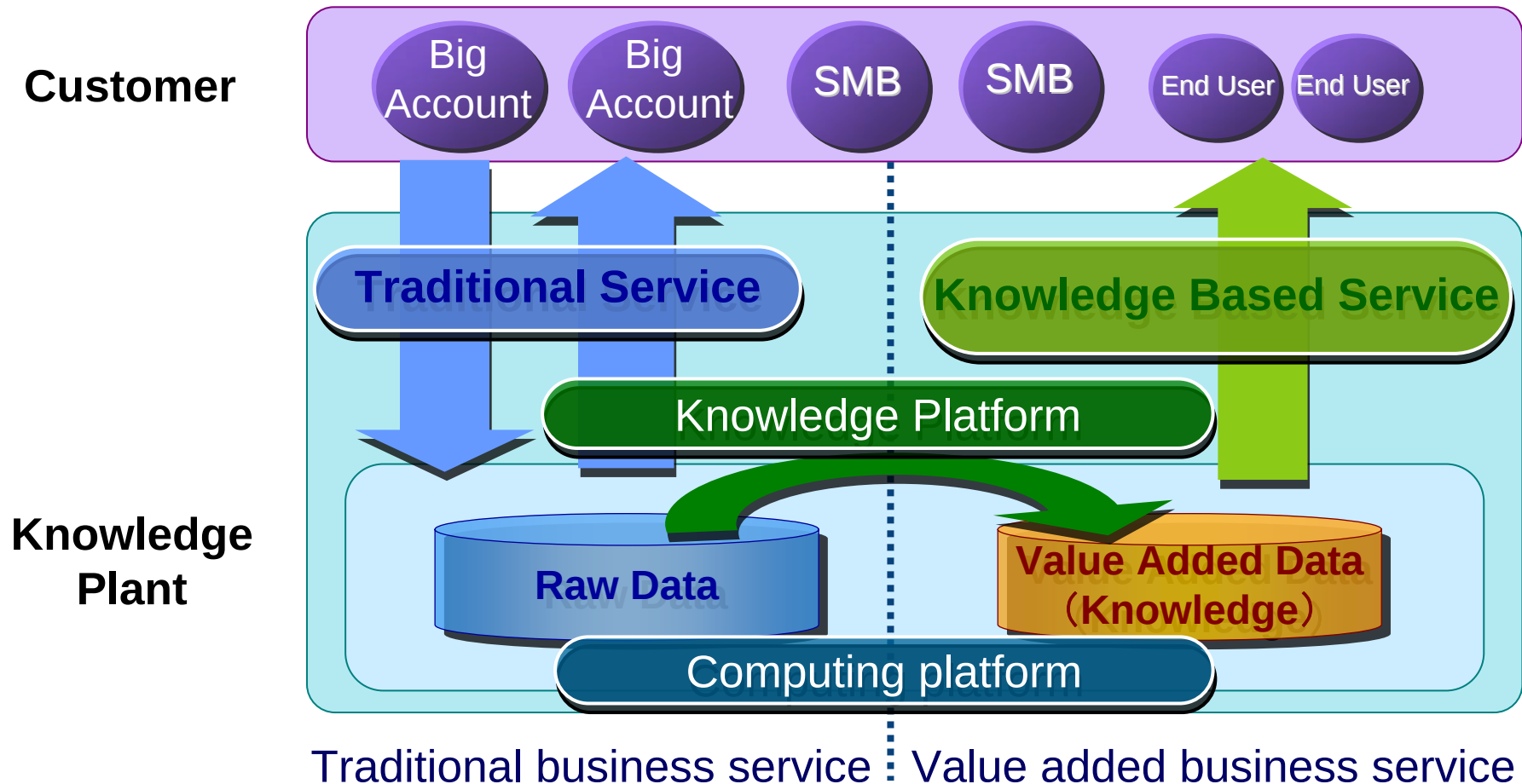
1-5. Social Infrastructures on Cloud

Today's
Topic



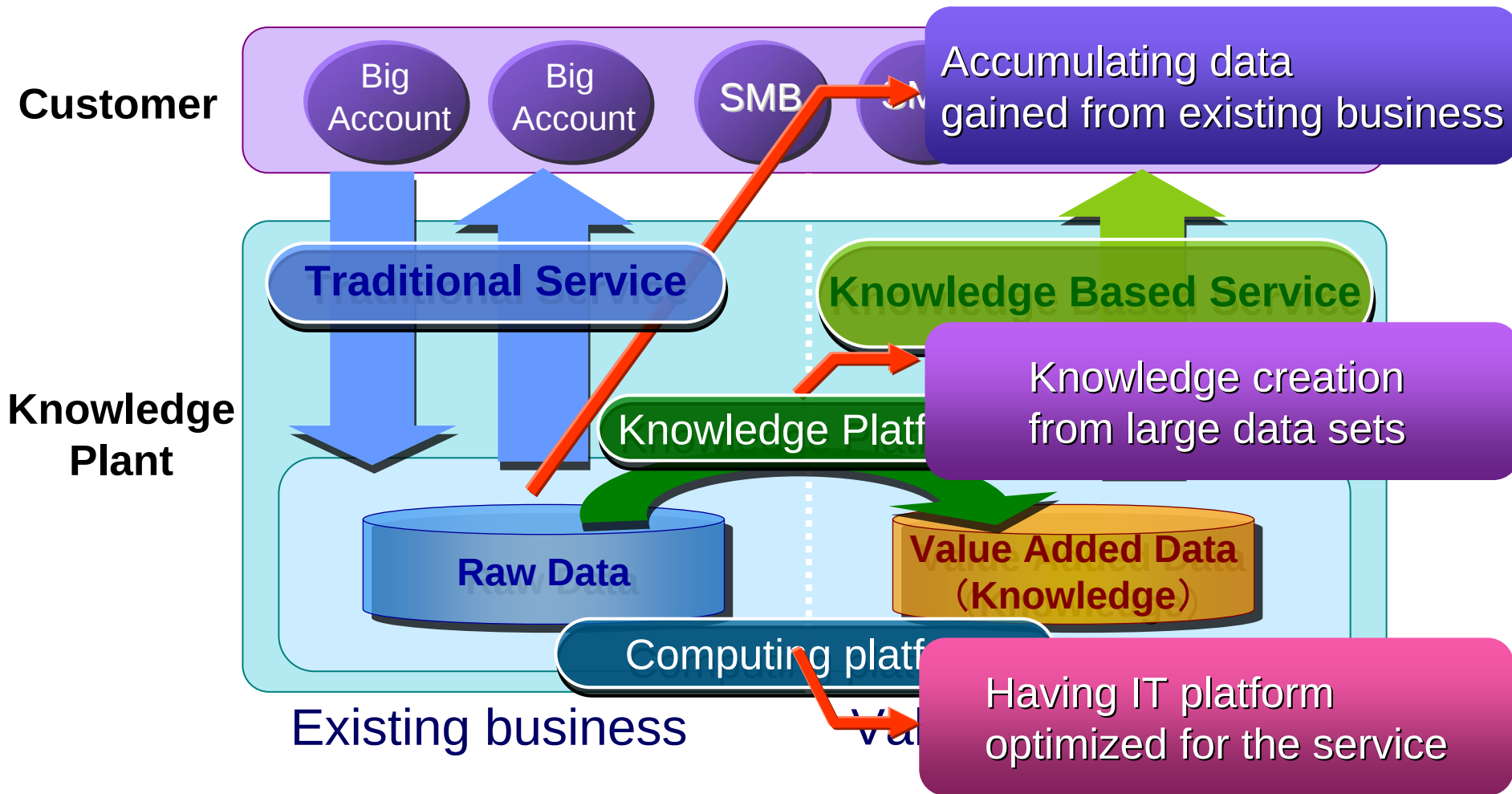
Social Infrastructures on cloud computers enable to observe, optimize and control real world

2-1. Toward Innovation: A New Business Growth Model



**“KaaS (Knowledge as a Service) business model”
is one of the keys for IT service business to grow**

KaaS business model characteristics



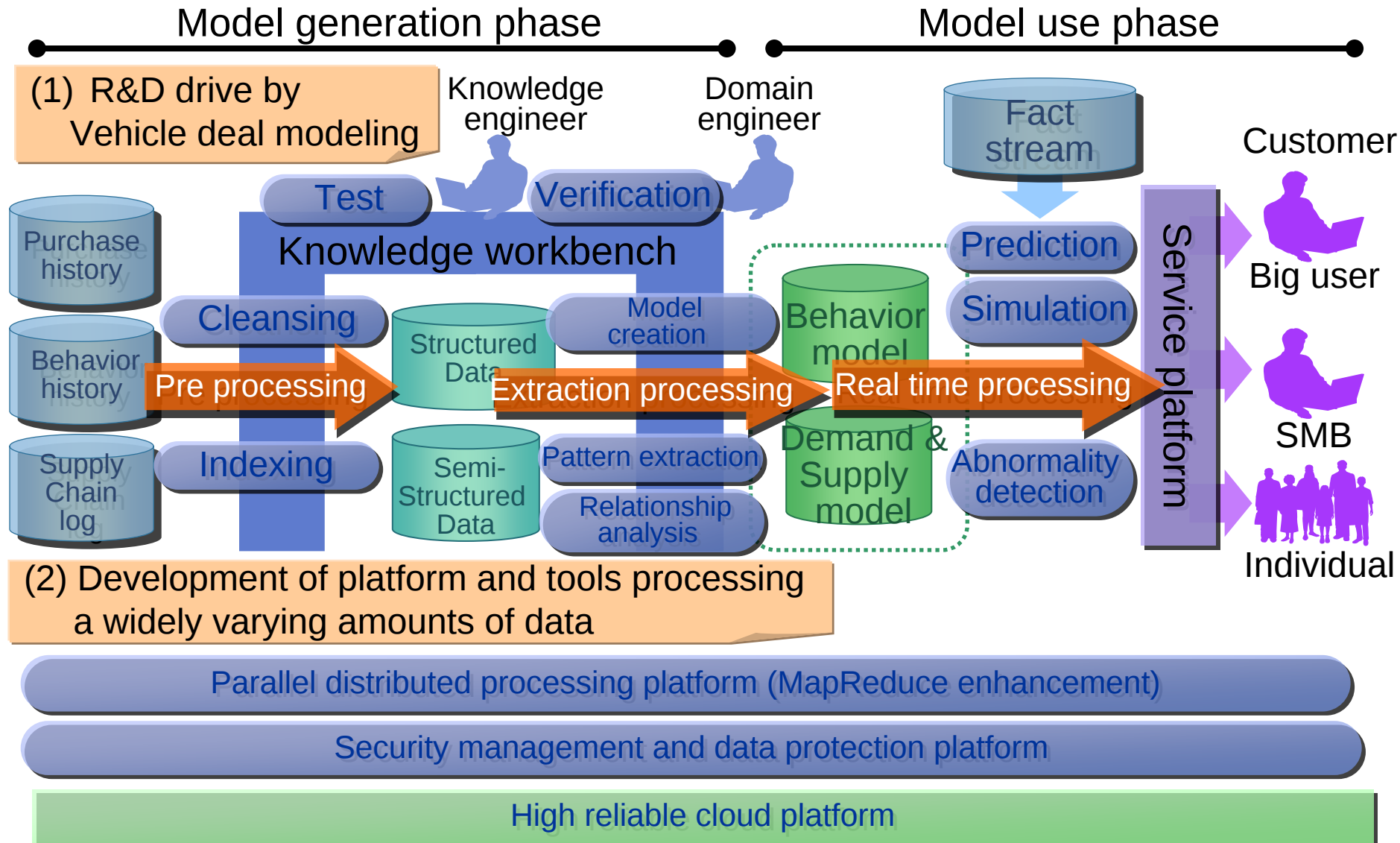
Knowledge Platform

- Data processing/structuring technology based on the real business data characteristics
- Continuous business/future trend prediction methodology and simulation technology
- Provide a service business platform by enabling new technological components to be plugged in

Computing Platform

- Essentially new datacenter architecture for the real business data to be processed in a highly effective manner
- Adoption of emerging electronics technologies to enable ultra-low electricity consumption per operation
- A datacenter to be regarded and controlled as if it were a single computer

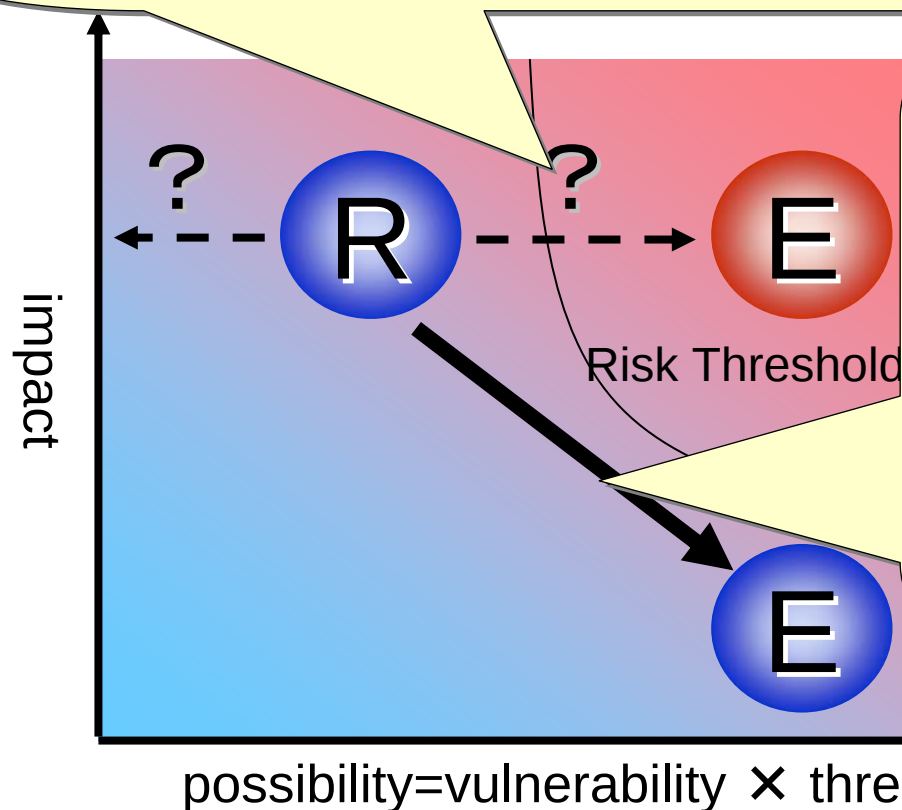
2-4. KaaS Overview and Research Approach



3-1. Risk Management Strategy for Cloud Security

Clarify and keep service level agreement of security

- Guidelines for ASP/SaaS information security measures of MIC(*1)
- SLA Guideline for SaaS of METI (*2)
- Information Security Management System(*3)



Transform outsourced data to secure by Technology

(1) Hide all of secret information

Private Information Processing

•Server-aided Computation

•Cancerable Biometrics

(2) Hide only identifiable information to person

Anonymization

•ID management and field isolation

•K-aonymization

$\text{Risk} = \text{impact} \times \text{possibility}$

R: Risk of in-house data

E: Risk of out-sourced data

(*1) Ministry of Internal Affairs and Communications

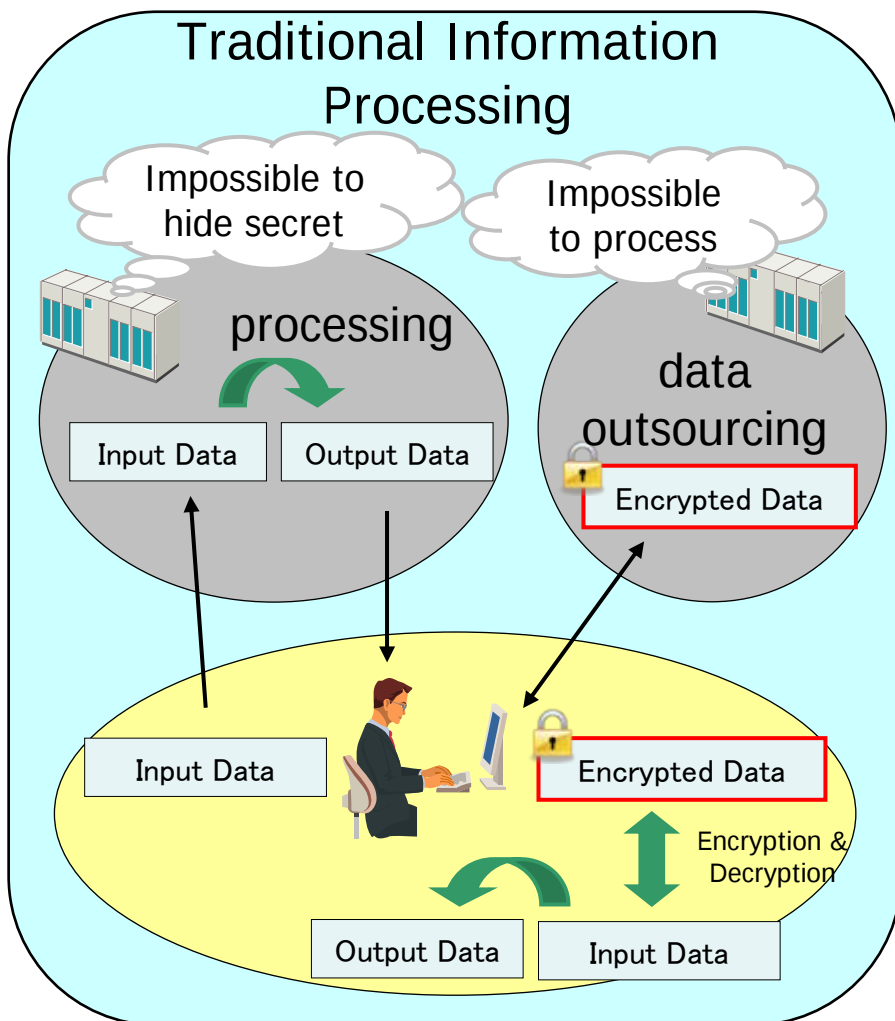
(*2) Ministry of Economy, Trade and Industry

(*3) ISO/IEC 27001

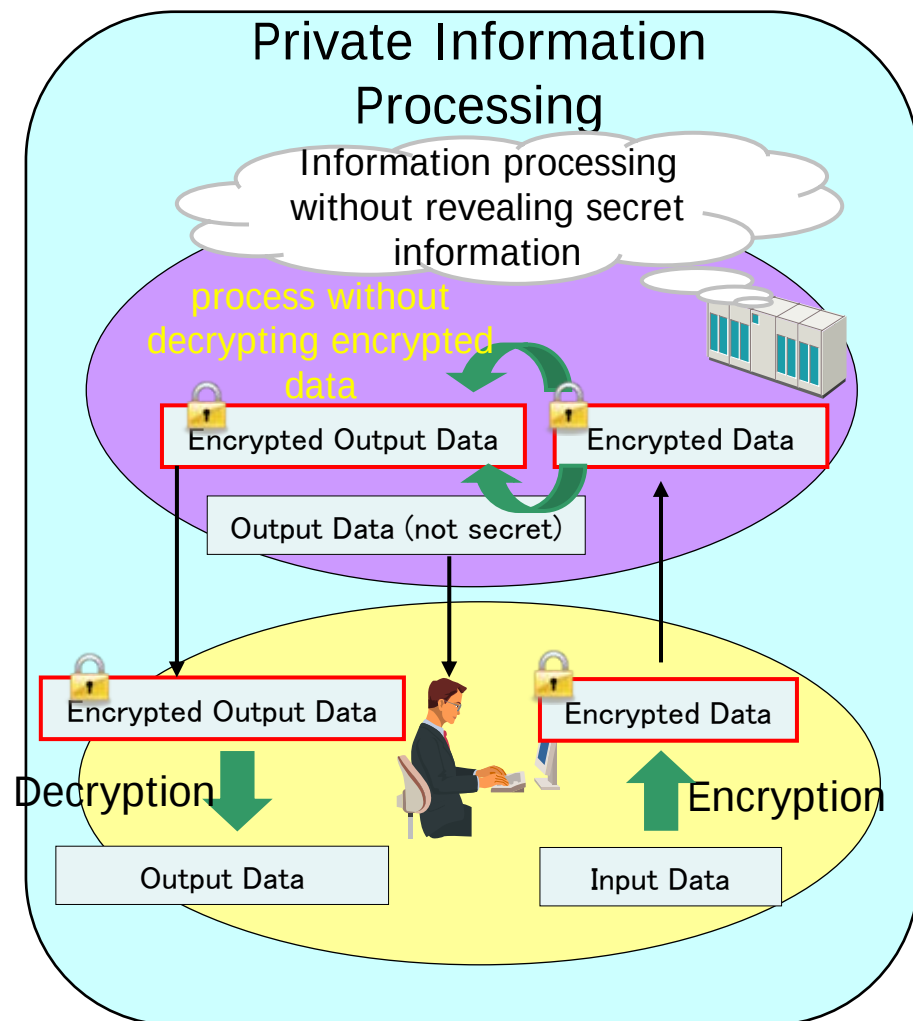
3-2. Private Information Processing

Private Information processing (PIP) is a computing paradigm, which can process without decrypting encrypted data

Traditional Information Processing



Private Information Processing

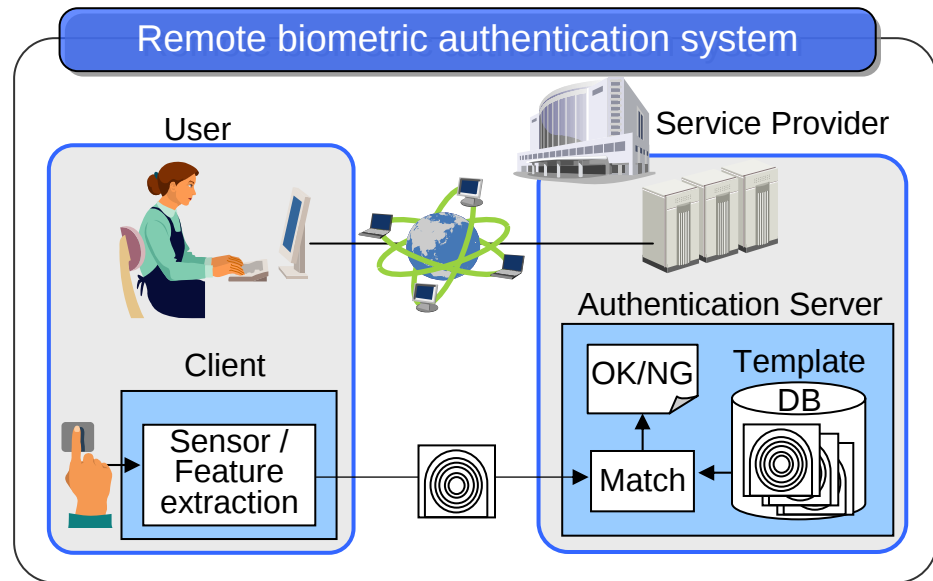


■ Expectation for remote biometrics

- Expansion of the network society
- Needs for rigorous and convenient user authentication over networks
- Maturity of biometric technologies (e.g. fingerprint, vein, iris, face, etc...)

■ Issues of remote biometrics

- Biometric features are
 - **Unchangeable / Irrevocable**
 - Personal / sensitive information
- Centralized control of templates
 - Risk of mass leakage
 - **Internal fraud**
- Privacy issues
 - User's anxiety about giving his/her biometric information to the remote server



Necessity of strict protection of biometric templates

3-3. Cancelable Biometrics: Overview

■ Cancelable biometrics

- The biometric authentication scheme with template protection
 - in which biometric features are encrypted, and matched without decryption

■ Features

(1) Privacy protection:

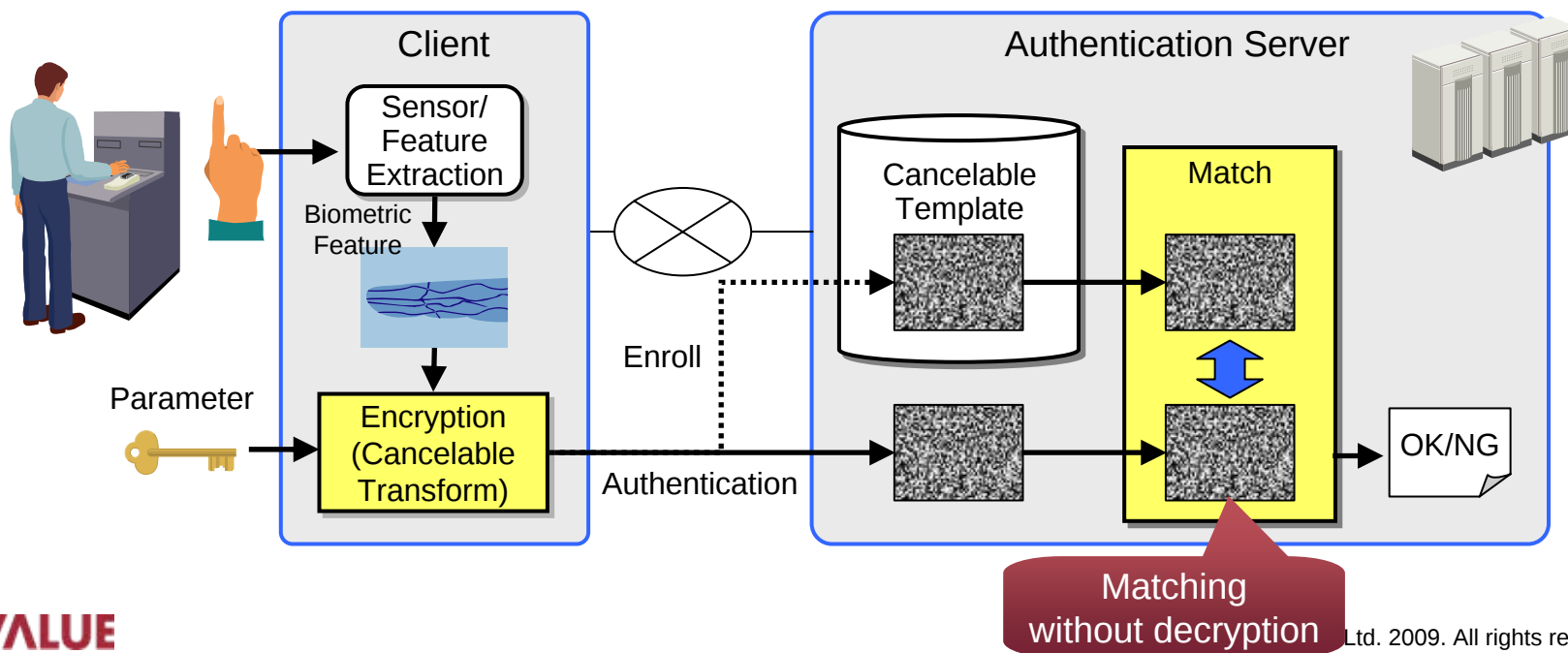
- The server can perform the authentication process without knowing the biometric features

(2) High security:

- It is impossible to reuse leaked templates for impersonation.

(3) Cancelable:

- Even if the biometric templates are leaked, they can be canceled by re-encryption.



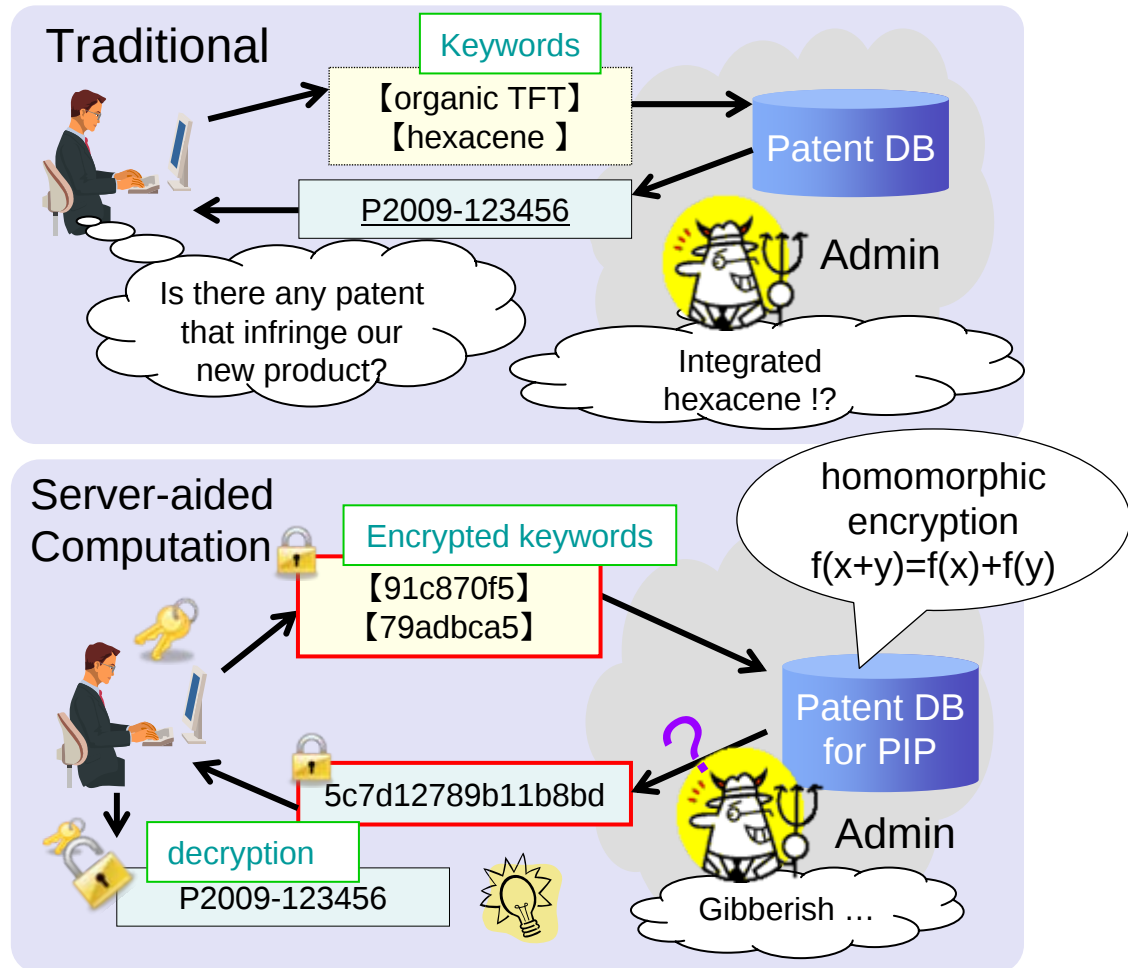
A PIP model using “*homomorphic encryption*”

【Example: patent search】

Disclose keywords
closely related to secret
to service provider

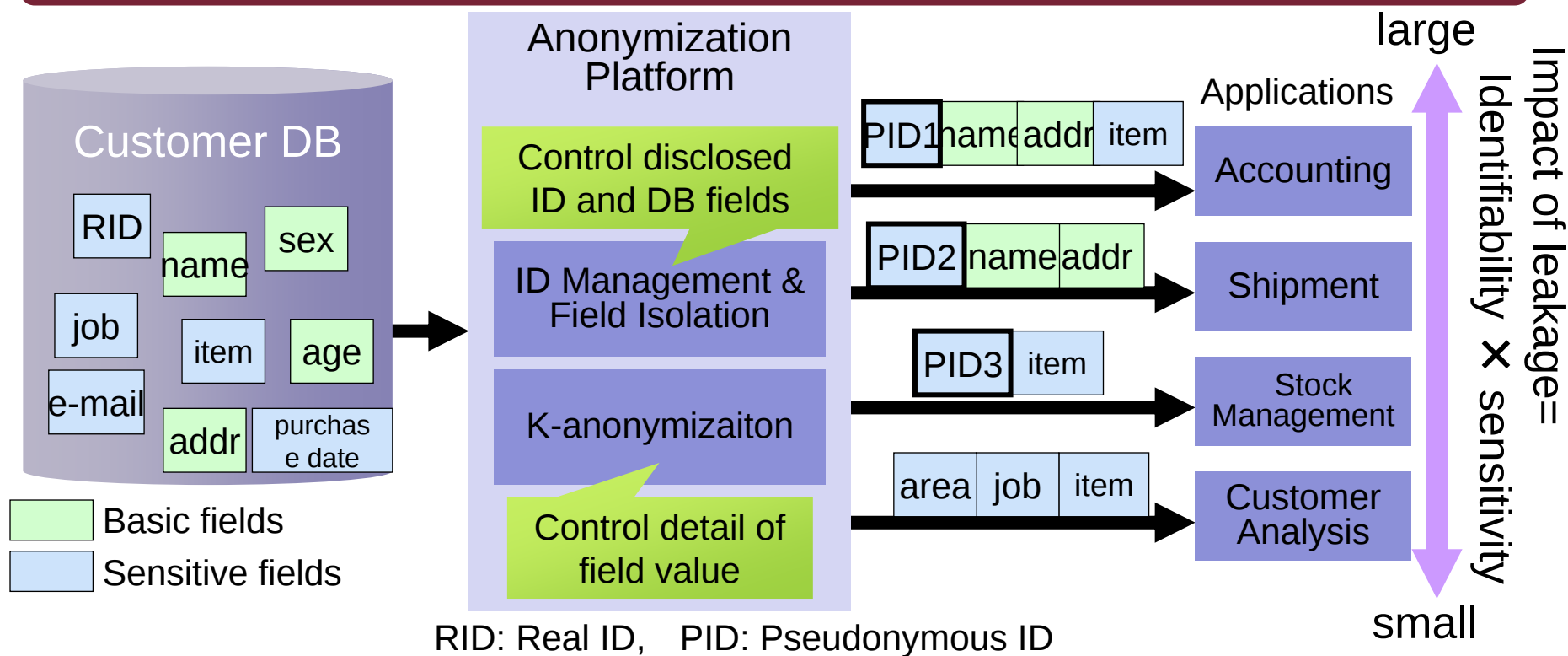


Search database of clear
text with **encrypted
keywords**. Server
administrator can not
know any information
from search process.



3-5. Anonymization for Personal Data

Control personal ID, DB field, detail of field value according to identification risk of personal data and property of applications



Hiding ONLY leakage between person and information enable go together safety and usability of personal data

3-5. Anonymization: K-anonymization

Exclude identification risk in personal data
with minimum information loss

ADDR	AGE	SEX	HOME TOWN	MARRIAGE
Tokyo	30	M	Akita	Yes
Chiba	25	F	Osaka	No
Saitama	30	M	Tokyo	No

Personal Data

Anonymization

Outsourcing
of customer
analysis

Identification Risk
Evaluation

- Safety cells
- Un-safety cells

Generalize
un-safety field
values

ADDR	AGE	SEX	HOME TOWN	MARRIAGE
Tokyo	30	M	Akita	Yes
Chiba	25	F	Osaka	No
Saitama	30	M	Tokyo	No

Safety

Satisfy k-anonymity

Un-Safety

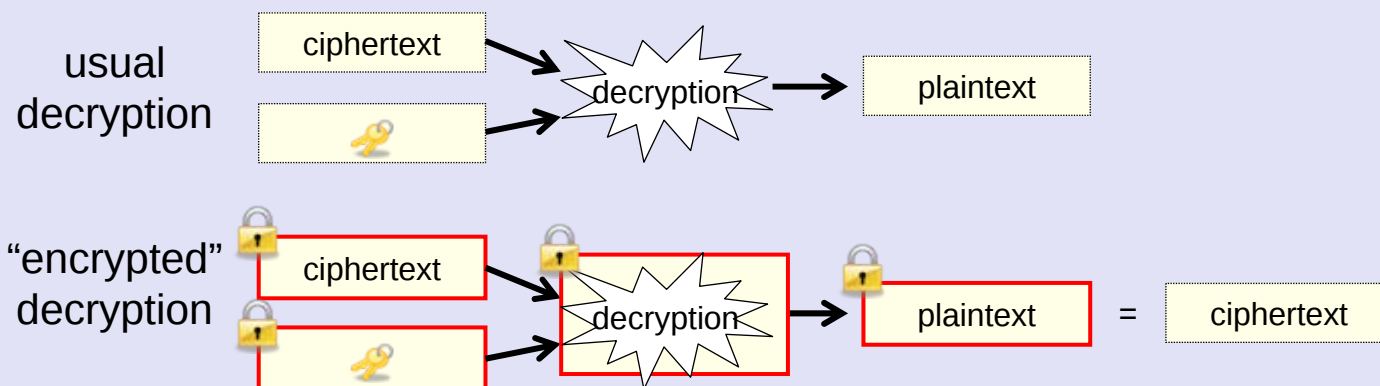
Not satisfy k-anonymity if
it is used with safe cells

3-6. Directions of Future Works

■ Research for common technology for any applications

- **Fully** homomorphic encryption settles arbitrary transaction
- Tremendously slow; $10^{12}+$ times
- Challenge: boost its performance to the practical level

Fully homomorphic encryption is based on “encrypted” decryption



■ Research for application specific technology

- Authentication services: cancellable biometrics
- Patent search: PIR based on traditional homomorphic encryption
- Customer analysis: k-anonymization

Social Innovation for Sustainable Society

Intelligent Information
Processing

×

Real World Data

KaaS: Knowledge as a Service

