International Workshop on Information Systems for Social Innovation 2009 (ISSI 2009)

社会イノベーションを誘発する情報システムに関する国際ワークショップ

情報通信技術（ICT）は、グローバル社会を支える重要インフラとして、社会活動や経済活動に不可欠な技術になっています。ICT により、我々は、いつどこにいても、必要な情報を入手・発信することができるユビキタス環境が整いつつあります。

しかし、世界に分散しているデータやコンテンツの共有や二次利用を進めようとすると、著作権、コンプライアンスやプライバシー基準に対する国際間格差があるため、現実には様々な問題解決が必要になります。そこで、本ワークショップでは、グローバル ICT 社会の難問の一つであるコンプライアンス、プライバシー、IT リスクマネジメント、デジタル権利管理、情報セキュリティに関わる安全・安心の問題について、ヨーロッパおよび日本の研究機関で議論し、その技術的・経済的あるいは社会的・文化的な違いを明らかにしたいと考えています。

今回、国立情報学研究所（NII）は、オーストリア ウィーン工科大学との国際交流協定（MOU）の締結を契機として、同大学と既に MOU を締結しているドイツ フライブルク大学とともに本ワークショップを企画致しました。本ワークショップをきっかけに、「情報学と社会科学」の融合研究「人間・社会科学」を推進したいと考えています。

2009年 9 月

企画運営委員会

国立情報学研究所（NII）

曽根原　登 教授、越前　功 准教授、Sven Wohlgemuth 特任研究員

フライブルク大学（ドイツ）情報社会研究所

Günter Müller 教授

ウィーン工科大学（オーストリア）ソフトウェア・インタラクティブシステム研究所 所長

A Min Tjoa 教授

CONTENTS

目次

プログラム *Program*

昼　食　*Lunch break*

休　憩　*Coffee break*

15:20
〜
16:40

研究紹介
Introduction to on-going Research Activities

16:40
〜
17:50

パネルディスカッション 「社会と調和する科学技術」…… **121**
Panel discussion "Harmonizing Technology with Society"

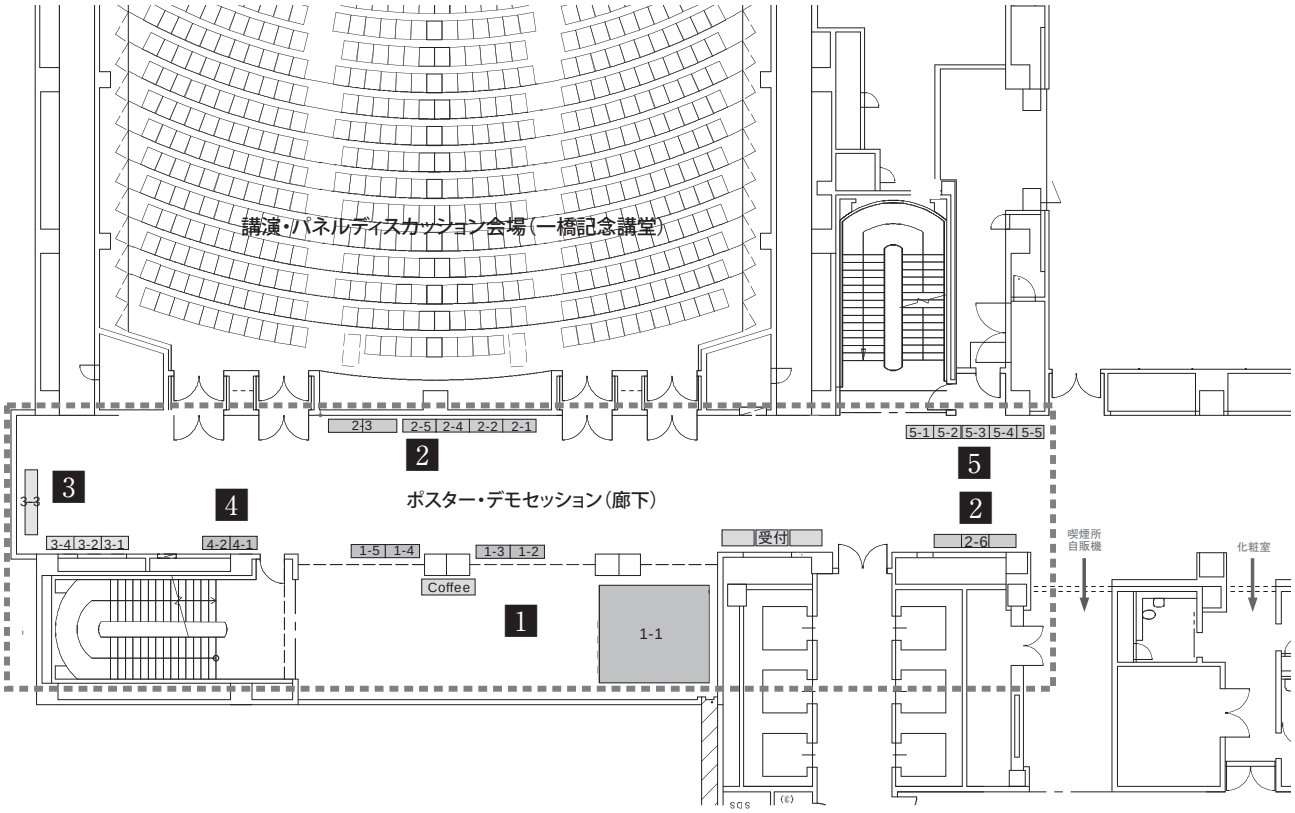
議　　長：林　紘一郎（情報セキュリティ大学院大学 学長）
モデレータ：越前　　功（国立情報学研究所 准教授）
Gerhard Schneider（フライブルク大学 チーフインフォメーションオフィサー）
Thomas Mück（ウィーン工科大学 教授）
岡部　寿男（京都大学学術情報メディアセンター 教授）
岡本　龍明（日本電信電話株式会社情報流通プラットフォーム研究所 特別研究室長）
野村　雅行（日本情報通信株式会社 代表取締役社長）
Peter Mertens（シーメンス株式会社 ゼネラルマネージャー）
持田　侑宏（フランステレコム株式会社 CTO）

17:50
〜
18:00

まとめ
Conclusion

坂内　正夫（国立情報学研究所長）

国際ワークショップ会場　案内図



ポスター・デモセッション

1　プライバシー、データ、メディアのセキュリティ技術

1－1　**Research on Re-shooting Countermeasures** … 越前　　功（国立情報学研究所 准教授）

1－2　**Extending Usability of Personal Health Records**
…… Nurul Huda（国立情報学研究所 外来研究員）

1－3　**Medical data analysis infrastructure – Attempt at the Kochi Medical School –**
…… 片岡　浩巳、畠山　　豊、奥原　義保、倉本　　秋（高知大学医学部）

1－4　**Privacy in e-Health** …… Sven Wohlgemuth（国立情報学研究所 研究員）

1－5　**Pseudonymization of Health Data**
…… Johannes Heurix（オーストリア・セキュアビジネスセンター研究員）

2　e-Science, CSI(Cyber Science Infrastructure)　研究教育情報基盤

2－1　**学術情報ネットワーク SINET3** …… 山田　茂樹（国立情報学研究所 教授）

2－2　**学術認証フェデレーションの現状** …… 山地　一禎（国立情報学研究所 准教授）

2－3　**日本における学術グリッド基盤** …… 合田　憲人（国立情報学研究所 教授）

3　IT リスク管理

4　セキュリティと社会

5　その他

講　演

相互理解が最良の安全保障

長尾　　真（国立国会図書館長）

氏名　長尾　真（ながお・まこと）
所属　国立国会図書館長


（撮影：久保真二）

学歴

1955 年　　滋賀県立膳所高等学校卒
1959 年 3 月　京都大学工学部卒
1961 年 3 月　京都大学大学院工学研究科修士課程修了
1966 年 11 月　京都大学工学博士

主要経歴

1961 年 4 月　京都大学工学部助手
1967 年 4 月　京都大学工学部講師
1968 年 11 月　京都大学工学部助教授
1969～70 年　フランス・グルノーブル客員教授
1973 年 10 月　京都大学工学部教授
1986 年 4 月　京都大学大型計算機センター長
1995 年 4 月　京都大学附属図書館長
1996 年 1 月　京都大学総長特別補佐
1997 年 4 月　京都大学大学院工学研究科長・工学部長
1997 年 12 月　京都大学総長
2004 年　　情報通信研究機構理事長に就任
2007 年～　　国立国会図書館長

専門分野

自然言語処理・画像処理、情報工学、知能情報学

研究概要

情報工学、特に画像及び言語という情報メディアを用いた知的な情報処理に関する研究において世界をリードする顕著な業績を挙げ、パターン認識、画像処理、自然言語処理、機械翻訳、電子図書館等の分野の発展及び学術振興に多大な貢献をした。

受賞

平成 5 年　IEEE Emanuel R. Piore Award
平成 6 年　京都新聞文化賞
平成 9 年　電子情報通信学会功績賞、情報処理学会功績賞、機械翻訳国際連盟（IAMT）栄誉賞、紫綬褒章受章
平成 11 年　NEC より C&C 賞、ＮＨＫ放送文化賞、英国ノッティンガム大学名誉博士
平成 17 年　日本国際賞
平成 17 年　フランス共和国よりレジオン・ドヌール勲章シュヴァリエ章
平成 20 年　文化功労者

相互理解が最良の安全保障
Mutual Understanding is the Best Way for Security

国立国会図書館長
長尾　真

1

歴史は知・情・意のサイクルを描く

古代ギリシャ	知
中世ヨーロッパ	情
ルネッサンス・フランス革命	意
19, 20世紀、科学技術の時代	知
21世紀	情？

2

情の時代、相互理解の時代

- 脳科学から心の科学の時代へ
- 知の基盤の上に花開く心の時代へ
- 情、心の時代は、相互理解が前提となる

3

信頼し合うことの大切さ

- 信頼し合うためには相互理解が必要
- 相互理解のためには対話することが必要
- 対話ができるためには相手を理解しようとする心が必要
- 相互理解、相互信頼が最も優れた安全保障である

4

言葉によるコミュニケーション

- バベルの塔の野望をこらしめるために、多言語にして民族間にコミュニケーションが出来なくしてしまった。
- 相互理解のためには言葉の壁を乗り越える努力が大切である。
- 言葉についての研究、特に情報ネットワーク時代には言語の機械翻訳の研究が大切である。

5

言葉の意味を理解

- 言葉の意味と理解は哲学の根本問題である。
- ライプニッツ、フンボルト、ソシュール、そしてウィトゲンシュタインなど多くの哲学者がこれを論じてきた。
- 特にオースチンの言語行為論やウィトゲンシュタインの言語の哲学とその背後にある心の問題などは注目に値する。

6

心のあり様の表現

- 言葉の理解はコンテキストによる。
- 日本語の場合は特に文末の付属語表現から人の心のあり様が推測される。
- 音声表現におけるアクセント、イントネーション、プロミネンスなどが発話者の心理、意図等を伝えている。
- このような言語表現の背後に存在する心理的要素を取り出す研究が大切である。

7

機械翻訳の重要性

- 人々がどの国の人とも話し合えることが大切
- 音声によるコミュニケーションのために、音声通訳システムが必要
- インターネット上での文字によるコミュニケーションのために機械翻訳システムが必要

8

機械翻訳の現状

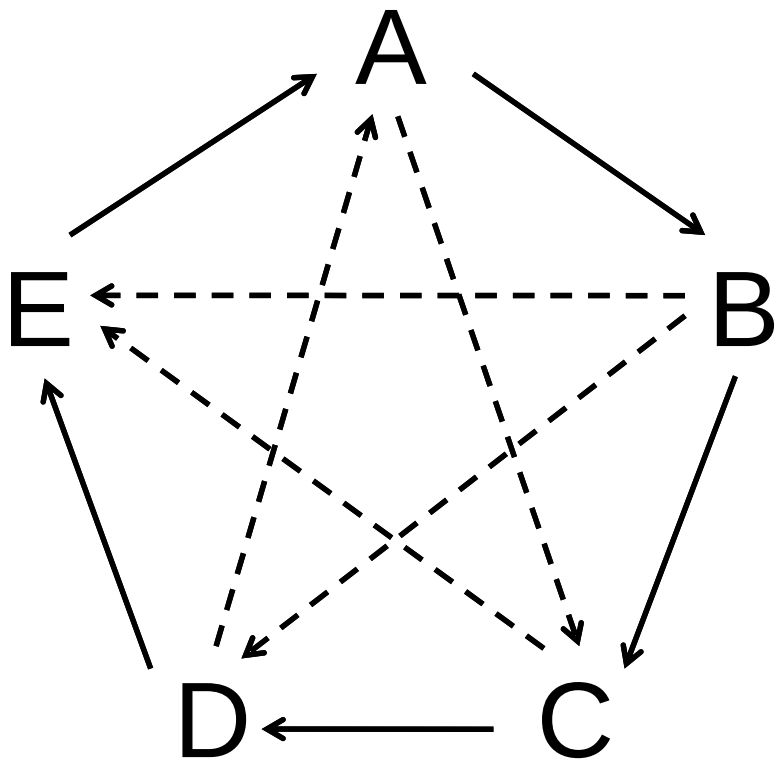
- 30～40カ国語について機械翻訳システムが作られている。
- 翻訳の品質は入力文の質による。短くて文法にかなった文であればかなりの精度で翻訳可能。
- 音声翻訳については、発話の目的があらかじめ分かっている場合に、短い発話であれば翻訳可能。

9

言語グリッドシステム

- 京都大学の石田亨教授が実験しているシステム
- 言語Aから言語Bへの翻訳システム、言語Bから言語Cへの翻訳システムの2つをカスケードにつないで言語Aから言語Cへの翻訳システムを構成する。
- 多くの翻訳システムを相互にカスケード接続することによって、それらの任意の言語間の翻訳システムを構成する。
- アジアの数言語で実験されている。

10



11

ネット情報の分析の重要性

- 社会の種々の現象に対してネット上に意見が述べられている。
- 国の政治、外交などに対してネット上に多くの意見が述べられている。
- ネット上にそれまでほとんどなかった種類の情報が突然現れ、急速に拡大する。
- こういった情報を常に分析し、対処方針をたてることが大切である。

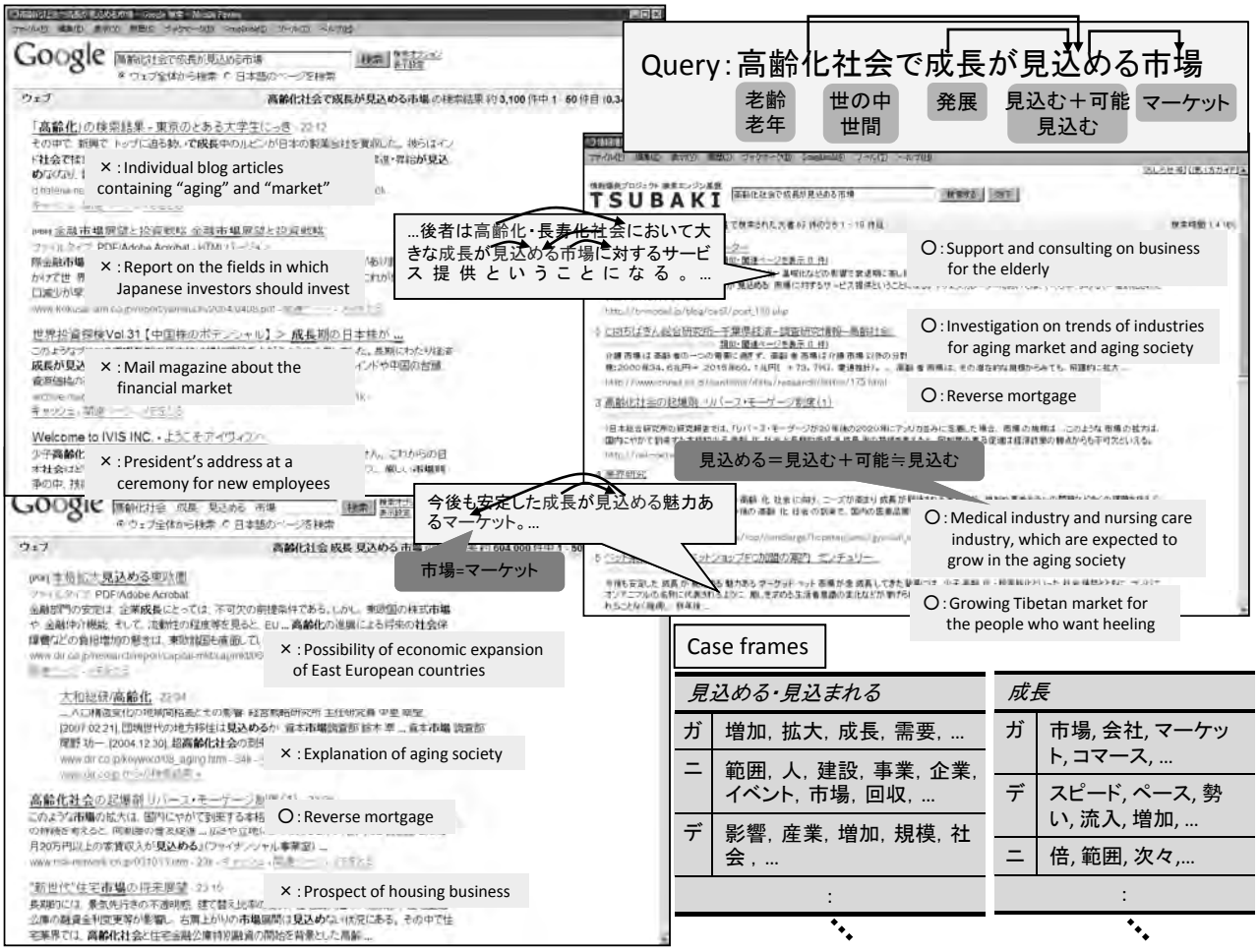
12

情報信頼性のチェックシステム

- 京都大学の黒橋禎夫教授が開発しているシステム
- インターネット情報の検索をして、出て来た情報がどの程度信頼できるものかを推定する。
- 信頼性のチェックのために次のような項目を調べる。

  (ⅰ)情報内容の信頼性

  (ⅱ)情報発信者の信頼性



WISDOM: Information Credibility Analysis System

15

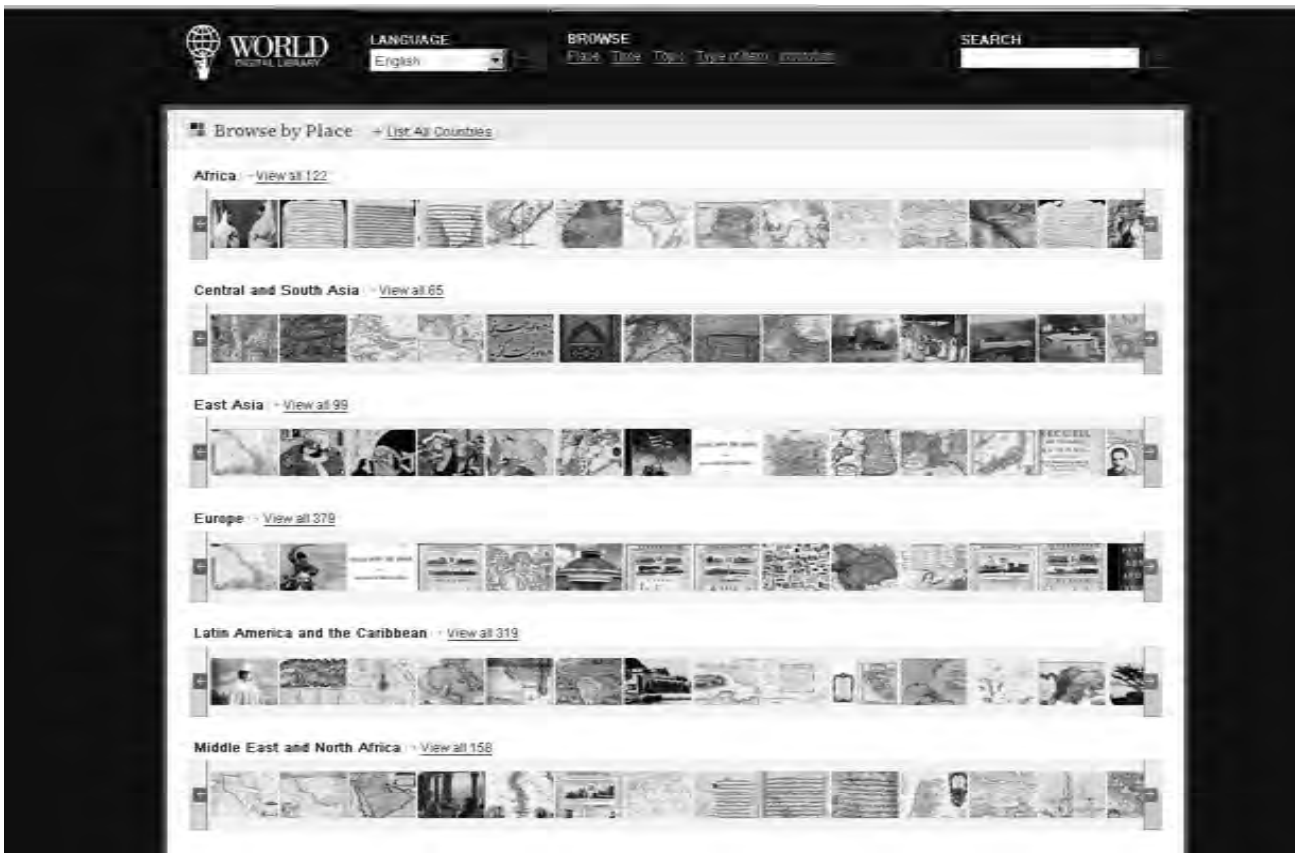
相互理解のための努力

- 相互理解のためには歴史、文化を理解することが大切
- World Digital Library は各国の文化遺産などを図や映像とそれらの解説によって紹介し、他国の文化伝統を理解するUNESCOのプロジェクト
- 国立国会図書館も参加している。

16


WORLD
DIGITAL LIBRARY
LANGUAGE
English
BROWSE
Place | Time | Topic | Type of Item | Institution
SEARCH
EUROPE
+ 379 Items
NORTH AMERICA
+ 197 Items
CENTRAL AND SOUTH ASIA
+ 65 Items
EAST ASIA
+ 99 Items
MIDDLE EAST AND NORTH AFRICA
+ 158 Items
SOUTHEAST ASIA
+ 49 Items
LATIN AMERICA AND THE CARIBBEAN
+ 319 Items
AFRICA
+ 122 Items
OCEANIA AND THE PACIFIC
+ 21 Items
6000 - 499
500 - 1499
1500 - 1699
1700 - 1799
1800 - 1849
1850 - 1899
1900 - 1949
1950 +
Home
About
Help
Contact
Legal

17


WORLD
DIGITAL LIBRARY
LANGUAGE
English
BROWSE
SEARCH
Browse by Place
+ List All Countries
Africa
View all 122
Central and South Asia
View all 65
East Asia
View all 99
Europe
View all 379
Latin America and the Caribbean
View all 319
Middle East and North Africa
View all 158

18

- インターネットを活用して各国の子ども達の共同参加教育プログラムを行ってはどうか。その時、言語グリッドシステムを用いて翻訳をする。
- 各国で電子図書館を建設し、またWorld Digital Libraryに参加して、国際的な文化の相互理解にために活用する。
- BlogやSNSが国際的相互理解のために活用されるよう努力することが大切である。

19

情報共有活動が相互理解につながってゆき、お互いの心が結ばれてゆく

これが最も確実な安全保障である。

20

講　演

Privacy and Protection of Personal Data in the EU, Transfers of Personal Data to third Countries

Hana Pecháčková（欧州委員会）

Hana Pecháčková

Hana Pecháčková is a desk officer (Legal Affairs and Policy) at the European Commission, Directorate-General Justice, Freedom and Security, in the Data Protection Unit.

She deals extensively with the processing of personal data, especially in the field of electronic communications, focusing on privacy and data protection related issues on the internet and in new technologies such as e.g. RFID and Internet of Things.

Ms. Pecháčková is also responsible for regional data protection issues and is a member of the OECD – Working Party on Information Security and Privacy. Ms. Pecháčková deals with protection of personal data and privacy related issues, among other 3rd countries, in Japan.

Within the scope of tasks entrusted to her Unit in the role of the Secretariat of the Article 29 Data Protection Working Party, Ms. Pecháčková is responsible for chairing the Technology Subgroup that deals with data protection and technology challenges. Ms. Pecháčková has been actively involved in preparing Commission's Communication on Promoting protection of personal data by privacy enhancing technologies, and monitors its proper follow-up.

Ms. Pecháčková works with other Commission services on data protection related issues such as with Directorates–General for Consumer Affairs and Information Society and Media.

She is a frequent speaker at various conferences, workshops and round-table meetings related to privacy, protection of personal data and new technologies.

Before joining the European Commission in 2005, Ms. Pecháčková worked as a legal practitioner, as an Associate in an international law firm.

BARBARA RHODE

holds a Ph. D. in Political Sciences (Kath. University Nijmegen/ NL) and a University degree in Social Science (Hamburg University/DE).

From mid/end September 2009 Barbara will be heading the Section of Science and Technology at the EU Delegation in Tokyo/Japan.

At the EU headquarters in Brussels/Belgium, she was the Adviser for International Relations to the FP7's "People" Programme (Marie Curie Grants) and the 'Small and Medium Sized Enterprise' (SME) Actions in the Directorate General for Research (DG RTD) of the European Commission.

As Head of Unit for: "Multilateral Co-operation Activities" in DG RTD she guided the EU policies on Ex-Soviet Union scientists of weapons of mass destruction (WMD) and their redirection to civilian tasks, in collaboration with the US (State Department), Japan (MoFA), Republic of Korea, Russia (RosAtom) and the countries of Eastern Europe and Central Asia.

As Head of Unit on "Ethics in Science" she negotiated rules to cope with ethical issues, i.e. human embryonic stem cells, clinical trials, animals, data protection etc. when collaborating in international research networks. Barbara represented the EC in UN and Council of Europe (CoE) bodies.

Between 1995 and 2000 she was responsible for the EU Accession negotiations for RTD with Hungary, with the Czech Republic and with Slovakia, for relations with Switzerland, with the countries of the Caucasus.

As National Expert she initiated the Social Science Programme for DG RTD.

Still in Cold War she was sent by the German Federal Ministry for Science and Technology as the West German representative to the ISSC - UNESCO 'Vienna Centre', an East-West Research Institute located in Vienna/Austria. She coordinated multi-national research projects regarding environmental policies and initiated the CoE 'Convention on Environmental Penal Law'.

Barbara started her career at the Max-Planck-Institute for International and Comparative Private Law in Hamburg/ Germany.

Lecturer at various Universities, author, co-author and editor of a number of books, many articles, co-author of a documentary film for cinema, short-version for TV, contributions to broadcast emissions and print media.

Privacy and Protection of Personal Data in the EU

Transfers of Personal Data to third Countries

European Commission
Directorate-General Justice, Freedom and Security,
Unit D5 – Data protection

International Workshop on Information Systems for Social Innovation 2009
Tokyo, Japan
30 September 2009

Goal of the presentation

- **Explain** work of the European Commission in the field of data protection and privacy
- **Outline** current data protection and privacy legislation in the EEA including basic data protection principles
- **Explain** what is necessary for transferring data to third countries: example EU – Japan, adequacy procedure
- Next steps /solutions

EC legal framework

- Article 8 of the **Charter of Fundamental Rights** of the European Union establishes the right to the protection of personal data as a **fundamental right**;

- **Directive 95/46/EC** of 24th October 1995 concerning the protection of natural persons in respect of the processing of personal data and the free movement of such data (Data Protection Directive); *currently, online public consultation on the future of privacy & data protection has been opened (*http://ec.europa.eu/justice_home/news/consulting_public/news_consulting_0003_en.htm)

- **Directive 2002/58/EC** of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications); *currently undergoing a review*

EC legal framework

- Data Protection Directive transposed into 27 MS national laws.

- Directive based on one of the principles of a functional internal market - i.e. free movement of goods, persons, services and capital.

- Based on this principle MS shall ensure that, among other things, also personal data should be able to **flow freely from one MS to another**.

Scope of Directive 95/46/EC

- Applies to **natural persons**, whatever their nationality or place of residence
- Applies to **private and public** sectors
- Applies to processing of personal data **whatever the technology used** (*technology neutral approach*)

Principles

- **Proportionality, purpose limitation**
  - Personal data must be collected for a specified, explicit and legitimate purpose
  - Not further processed in a way incompatible with those purposes
- "Rule of **privacy by design**"
- Data **minimisation**
- **Accurate** and kept **up to date**
- Data should be kept in a form which permits identification for no longer than necessary

Data processing must be *legitimate*

- Consent (freely given specific and informed indication) – *very challenging in new technologies and online services*
- Necessary for performance of a contract
- Necessary for compliance with a legal obligation of the controller
- Legitimate interests of the controller (balance of interest)
- Necessary in order to protect the vital interest of the data subject

Data Protection Authorities

- Fully **independent** supervisory bodies
- Responsible for **enforcing national legislation**
- **Powers** of investigation, intervention and to engage in legal proceedings or to bring violations to the attention of the judicial authorities

Article 29 Working Party

What is it?

•Independent advisory body composed of representatives of all EU DPAs

(http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_en.htm)

•Secretariat ensured by the European Commission (DG JLS)

What are its competences?

•It has an advisory role regarding data protection issues

•Issues opinions or recommendations on data protection which are soft law instruments (recent Opinions on search engines, online social networking, etc.)

•evaluates the level of adequate protection in 3rd countries

Transfers of Data – general issues

- Article 25 of the Data Protection Directive
- Data form EEA to third countries can be transferred **only** if the third country in question **ensures an adequate level of protection**.
- The **adequacy level is assessed in the light of all the circumstances surrounding a data transfer operation**, in particular, purpose of the operation, country of origin and of final destination, the rule of law, security measures, etc…
- If a third country does not afford an adequate level of protection, MS shall take the necessary steps to prevent any transfers
- The Commission may find that a third country ensures an adequate level of protection by reason of its domestic laws or international commitments – "**adequacy procedure**"

Adequacy – general issues

- Protection of personal data is a **fundamental right in the EU**
- Existence of **appropriate data protection rules** and **administrative capacity** in the third countries is of **horizontal importance** and a **condition for success in a number of policy areas**
- in view of **considerable benefits** it would bring, namely:

  - easier flow of personal data between the parties, **thus better business and administrative cooperation**;

  - **economy of trust**: development of e-commerce, since individuals will be more ready to buy on the internet marketplace if their data are protected and will not be abused;

  - **good governance**: respect for fundamental rights in the respective countries from undue private and public interferences

- The **level of protection has to be assessed in the light of all the circumstances** surrounding a data transfer (nature of data, duration, country of origin, country of final destination, rule of law, security measures)

Adequacy - legal steps

- The Commission has been granted the **power to determine, whether a third country ensures an adequate level of protection by reason of its domestic law or of the international commitments it has entered into** (Article 25 (6) of Directive 95/46/EC.
- In order to initiate an adequacy finding procedure, an **official request** made by the representatives of the trird country country shall be lodged to the European Commission.
- The adoption of a (comitology) Commission decision based on Article 25 (6) of the Data Protection Directive involves:
  - a proposal from the Commission
  - an opinion of the Article 29 Working Party
  - an opinion of the Article 31 Committee delivered by a qualified majority of MS
  - a thirty-day right of scrutiny for the EP (to check if the Commission has used its executing powers correctly). EP may, if it considers it appropriate, issue a recommendation.
  - the **adoption of the decision** by the College of Commissioners.

Adequacy

- The Commission may find that a third country ensures an adequate level of protection.
- The effect of such a decision is that personal data can flow from the 27 EU MS and three EEA member countries (Norway, Liechtenstein and Iceland) to that third country without any further safeguard being necessary.
- Japan has not yet been considered by the EU as a country providing an adequate level of protection with respect to the protection of personal data and fundamental rights of the persons relating to their private life.
- Therefore a transfer of data to this country from an EU country has to be carried out in pursuant to Article 26 of Directive 95/46/EC which implies a prior information/authorization by the national data protection authority.
- In order to show that the transfer provides appropriate guarantees to ensure the protection of the data subjects, this can be particularly be made by specific contractual arrangements, for instance by using the one of the standard contractual clauses models approved by the Commission.

"Adequate" 3rd countries

- The Commission's decision determining adequate protection **increases legal certainty** for companies in the EU and makes the export of personal data to the country concerned easier.
- Examples: Switzerland, Argentina, Isle of Man, the Bailiwick of Guernsey, the Safe Harbour, Canada, the Bailiwick of Jersey

Adequacy – conclusions

- The Commission launched a preliminary step to begin assessing the state of play in Japan
- Analysis has been prepared covering data protection and privacy legislation in Japan
- EU – Japan Business Dialogue Roundtable discussed personal “data protection regime”, Tokyo, 3-4 July 2008
- BDRT recommended that two authorities should work together to ensure an international equal, transparent and secure data protection regime between EU and Japan
- Commission is preparing a Progress report for the BDRT
- Commission intends to improve the co-operation in the field of the protection of personal data and data transfers and to work towards the free movement of personal data between the EU and Japan according to the highest international standards.
- The Commission is considering carrying out an in-depth analysis in order to have a complete picture of Japanese data protection laws and possibly launch an adequacy finding procedure.
- Nevertheless, this initiative should be supported by the Japanese counterpart.
- In order to initiate an adequacy finding procedure, an official request made by the representatives of Japanese shall be lodged to the European Commission.

Thank you very much for your attention!

Questions?

Web site:
http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm
or

hana.pechackova@ec.europa.eu

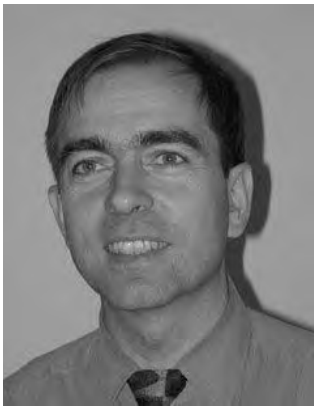
講　演

Security for Society

– Is any Technological Possibility a Desirable Solution for Democracy?

Gerhard Schneider（フライブルク大学教授 チーフインフォメーションオフィサー）

Prof. Dr. Gerhard Schneider



CIO of the University of Freiburg
Director of the Computing Center
of the University of Freiburg, Germany

From 2003 to 2008, **Prof. Dr. Gerhard Schneider** was vice rector for knowledge transfer and communication technologies of the University of Freiburg, Germany. He is now serving as CIO. At the same time Professor Dr. Schneider is the director of the computing center of the University of Freiburg, Germany.

Before his current duties the University of Göttingen, Germany has appointed him in 1999 to a C-4 professorship for applied computer science. Since 1997, he was the chief executive officer of the "Gesellschaft für Wissenschaftliche Datenverarbeitung" (Society for Scientific Data Processing) which is the corporate computing center of the University of Göttingen and the "Max-Planck-Gesellschaft" (Max-Planck Society). Before this duty, he held a C-3 professorship for decentralized information systems as well as a vice-director position of the computing center of the University of Karlsruhe, Germany.

After his PhD graduation, he received his postdoctoral lecture qualification in mathematics at the University of Essen, Germany, in 1989. At the University of Essen, he had been research assistant and assistant of the University for 12 years. Since 1989 he was the spokesman for data processing at the new founded institute of experimental mathematics In those times he has been a visiting researcher in Sydney (1985-1986), Zürich (1987 for 6 months), at Virginia Tech and at the IBM T.J. Watson Research Laboratory.

His academic career has started in 1973 at the University of Erlangen, Germany with his study of mathematics and physics. In 1978 he successfully graduated with the diploma and state examination. In addition, he received a Master of Science (M.SC.) of the University of Oxford, UK,, in 1979.

Security for Society

- Is any Technological Possibility a Desirable Solution for Democracy?

Gerhard Schneider
IT centre / Dept of Informatics
University of Freiburg
gerhard.schneider@rz.uni-freiburg.de

Albert-Ludwigs-Universität Freiburg

UNI FREIBURG

9/11 and its aftermath

Albert-Ludwigs-Universität Freiburg

UNI FREIBURG

Use technology to control everybody's life

- CCTV, bank data (SWIFT), long term storage of telephone & internet connection data,...

Legally enforce the generation of more data

Enable state agencies to correlate data

Latest example:

- 10 US$ entrance fee to the USA
- Payable with your credit card

now they know where you are

- in the country, in the world ☺
- Note: they process your credit card data (world wide)

Unwareness of risks to society

Politicians use what is available even if they promised otherwise

- example: German TollCollect originally **only** for accounting – why not use it for prosecution?

Politicians openly question classical basics

in dubio pro reo:

- should this really hold in the digital world?

is digital privacy really necessary?

- it hampers the control mania
- it does not please the music industry

Unwareness of risks to society

Albert-Ludwigs-Universität Freiburg

UNI FREIBURG

Lawyers still believe that we can hide in the enormous „sea of data“

- latest purchase in Freiburg: 8CPUs/512GB, 40K€
- enough to hold 80 bytes for every human on earth in main memory (fast access for indexing…)

German Parliament tries to block the WWW to fight child pornography

- in reality an ineffective, if not useless scheme
- which does not even address the problem
  - Why ask specialists??
- It sets up an infrastucture which can be used for all sorts of censorship (to support a crumbling old world)

Interdisciplinary cooperation

Nobody listens if technicians complain ☹

- They should stay in their labs

Team up with other disciplines:

- e.g. joint seminars
- Law and Computer Science
- Sociology and Microsystems Technology
- IT and Philosophy

Provide them with up-to-date insight

- Scare them ☺ and discuss new theories
- Think about how to advance in your own field

Various task forces at Freiburg

Three major fields of interest have evolved:

- Thinking in security terms – basic human behaviour and requirements
- New architectures for integrating security demands into society
- Technology for security vs. changes to society

Schizophrenic behaviour

Governments want to harvest data in social networks to identify terrorists

- And petty criminals (with a much higher success rate)

At the same time military warn their staff not to use social networks as classified information might leak out or may be deduced

- The Israeli army was the first to warn in public

The wife of the new MI6 boss publishes private information in facebook – jeopardizing national security

New paradigms

There is no anonymity

- if you keep data
- and do cross-correlation
- 80% of US citizens can be identified via ZIPcode, birthday and gender

Example: identify people via behavioural patterns in video recordings

- already used in court!

Use face recognition to identify people in pictures on *flickr.com*

- you may be on someone else's snapshot, proving you were in a certain location – and not where you claim to have been

Thinking security

In an emergency, will people behave the way the legal system expects them to behave?

- Looting, lyching,...

Use computer simulation like computer games to study human behaviour

- To get larger and more useful samples

TV series influencing public view of security?

- Cooperation of psychology, law, economy, humanities and IT

If you understand human behaviour – what are the right procedures / rules?

New architectures

Traditionally law experts only check the side effects of surveillance against individual paragraphs of the constitution

- The addition of various effects is not studied

Is it clever to introduce a specific security measure?

- Or should priority be given to the study of side effects and cumulative effects

What is the price/cost of not installing counter measures to certain (criminal) offences?

- E.g. is it worth it to fight any copyright violation?

New architectures

How do counter measures stop the evolution of society?

- breaking obsolete laws is part of progress
- e.g. shopping hours in Germany were once quite rigid
- scanning of books by Google may be illegal, but may be good for public knowledge

Will surveillance also modify the target?

- If a computer is hacked by a government agency,will the modified routines modify the evidence?

If the state grants anonymity in the classical world, why not in the digital world?

- I may use a public payphone without any ID, but not a mobile phone

Potential approaches / analysis

A department store may want to operate cameras to fight theft

- But why store the video for a long time?
- Or why allow security staff to monitor their girl friends?

Can we merge these contradicting requests?

- Why do we have to see the individual rather than the anonymous human on video in order to fight theft?

Potential approaches / solutions?

Digital stealth mode

I carry a device (e.g. a mobile phone)

- When I enter a department store my device receives information on the store's policy w.r.t privacy

I may agree to a contract

- store security may monitor me if it does not process/store identifiable information
- e.g. only a shadow of me will be produced by the security camera, so that my actions may still be seen, but not my face nor my clothes.

or I do not enter the store

Potential approaches

How do we make sure that the camera will always adhere to the rules?

- Use hardware specification & verification technology from computer science
- So that my device can check whether it speaks to a verified (and unmodifiable) camera

How do we introduce such verifications into the legal process?

- e.g. have laws with attached hardware specifications
- Useful side effects: if politicians want new features, prior to a firmware update a new legal process is required
- And my device will detect the change – I can then act accordingly.

International aspects

Security concerns are usually solved nationally

- Through legislation and politics
- This is pointless if we have strict rules on pro-cessing existing data – but the CIA has not

The Internet allows for international access to all available data

- International legislation is quite difficult
- Unless the legal systems do not differ too much (Japan/Germany??)

Rather than endangering its citizens should a state invest more in protecting its citizens against the curiosity of friendly states?

Summary

New threats call for new security measures

- Surveillance and storage of resulting data is seen as a security measure.

The more data are accumulated the less secure the individual is

- Society is formed by individuals!

What is the right balance?

- Introduce technical understanding in classical fields

Common issue for the Japanese and the German society

- Freiburg is looking forward to cooperating with the NII

講　演

Security and Privacy Issues in the Austrian "Patient Record" Project ELGA

Thomas Mück（ウィーン工科大学 教授）

Professor Dr. Thomas Mueck

Born in 1962 in Vienna, Austria, Thomas Mueck holds a doctorate in business informatics from Vienna University. Until 2003 he has been associate professor at Vienna University and was several years also head of the computer science and business informatics department at Vienna University. In this position, he has been involved in national and international joint projects, both governmental and industry funded.

Currently he serves as COO (operations management and controlling) of the Austrian Social Insurance for Business and continues his scientific work as an adjunct professor at Vienna University of Technology.

His current research interests include IT strategy issues as well as all technical aspects of e-health which also motivate his work on the Austrian electronic health record ELGA.

Education

1987	Doctoral graduation at the University of Vienna in Social Science and Economics
1993	Venia docendi at the University of Vienna in Computer Science

Academic Career

1995	Professor at the University of Potsdam, Germany for "Applied Informatics" Visiting professor at University of Linz
1997-2002	Professor at University of Vienna
2000-2002	Head of Department for Computer Science and Business Informatics
2003-	Professor at the Vienna University of Technology

Business Career

1983-	IT-Consultant and academic advisor
2002	Division manager IT of Austrian Federal Economic Chamber
2003-	Deputy general director of Austrian Social Insurance for Business (SVA), board member as division manager for operations management (controlling, internal organization, human resources and ICT)

Activities and Memberships

- Member of Austrian Computer Society
- Member of German Computer Society (GI e.V.)
- Representing SVA in the following organisations
    - OSSBIG (open source software for large enterprises)
    - SBA (Secure Business Austria)
    - SVD (back office spin-off of several Austrian social insurance organisations)

Privacy Issues in the Austrian EHR Project „ELGA“

Thomas Mueck
Vienna University of Technology

Outline

- eHealth study of the EU (Gartner)
- Privacy concerns (EC, Forrester)
- ELGA - Austrian eHealth Strategy (ARGE ELGA)
- Conclusion

Challenges

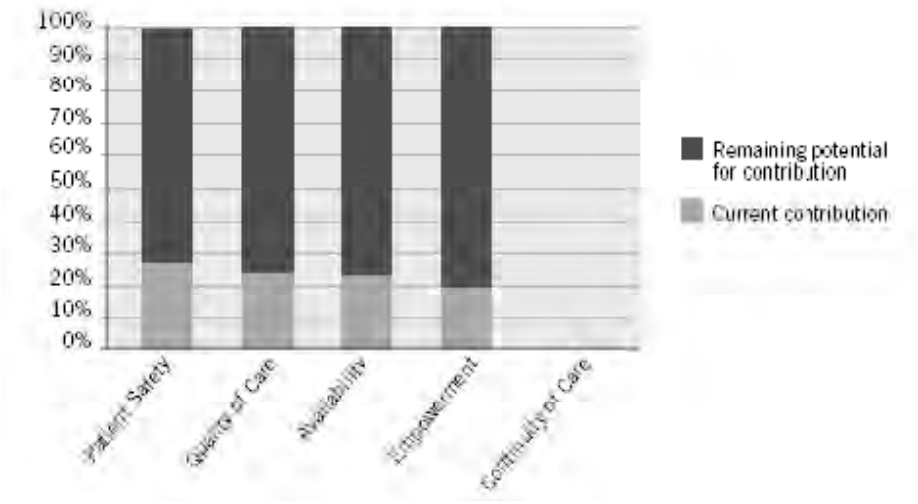
- Since the 1960s spending on healthcare has grown faster than the GDP in most EU member states.
- Spending rose from an average of 3.1% in 1960 to 8.8% in 2006.
- Forecasts indicate that spending on healthcare as a percentage of GDP will rise to around 15% by 2020.

Gartner, 2009

Political goals in healthcare

- Patient safety
- Quality
- Availability
- Empowerment
- Continuity of Care

Technology adoption



Gartner, 2009

Examples of quantified potentials

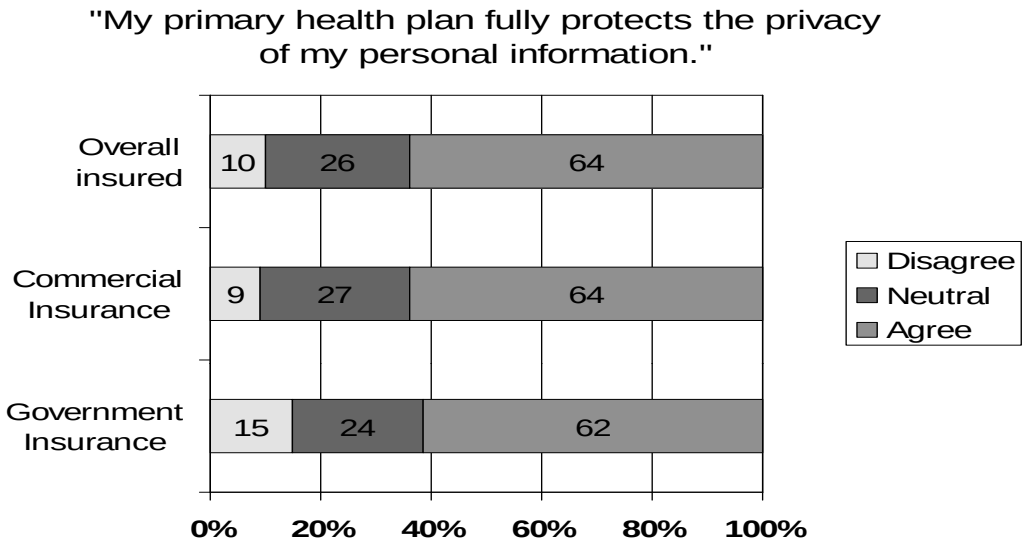
- Avoidance of **5 million yearly outpatient prescription errors** through the use of *Electronic Transfer of Prescriptions*.
- Avoidance of **100,000 yearly inpatient adverse drug events** through *Computerised Physician Order Entry* and *Clinical Decision Support*. In turn, free up **700,000 bed-days** yearly and **decreasing waiting times** (value of almost **€ 300 million**)
- Free up **9 million bed-days** yearly through use of *Computer-Based Patient Records* (value of nearly **€ 3,7 billion**)

Gartner, 2009

Privacy Concerns

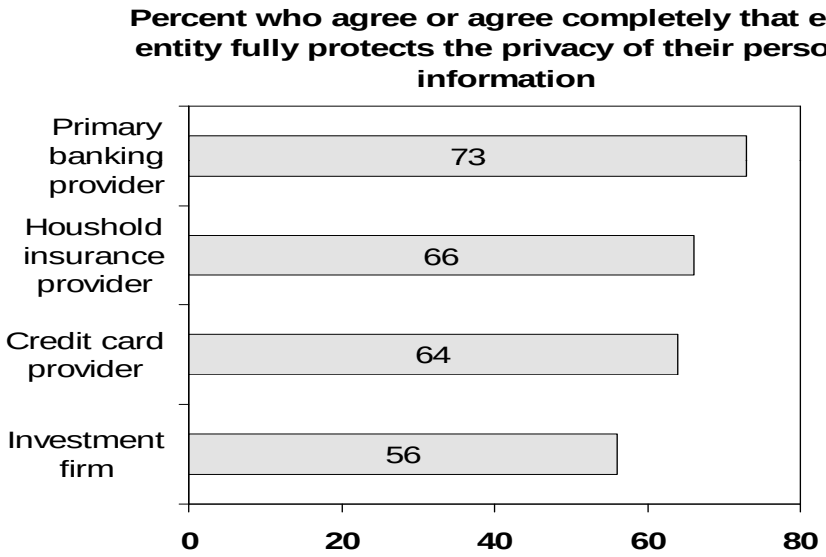
- Right of self-determination
- Identification and authentication of patients and health care professionals
- Data security
- Authorization for accessing EHR in order to read and write in EHR
- Use of EHR for other purposes
- International transfer of medical records
- Transparency
- Liability issues

Privacy Concerns - Health Insurance Portals



Forrester, 2008

Privacy Concerns - Health Insurance Portals



Forrester, 2008

ELGA Austrian eHealth Strategy

- ELGA stands for "Elektronische Gesundheitsakte" (electronic health record)
- Includes
  - prescriptions
  - referrals
  - medication history
- Decentralised electronic health record system
- Key to patient data will be the E-Card (smartcard)

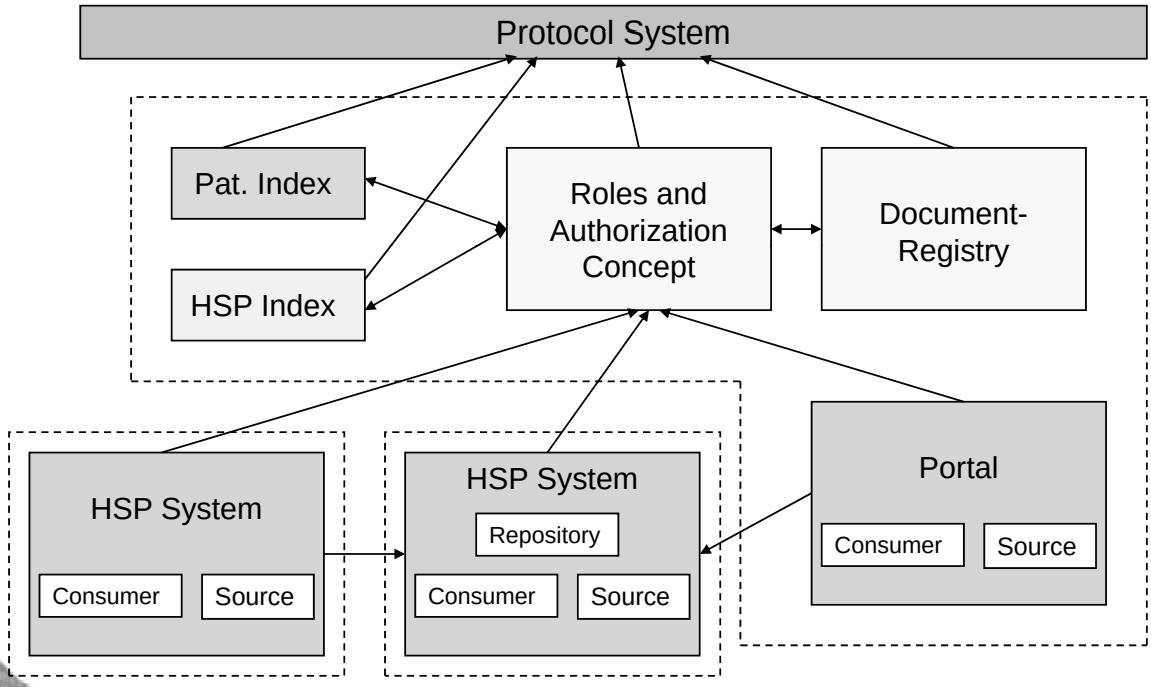
Considerations

- Already many stand-alone health care systems are put into operation at various health service providers
- Specialisation in health care → many health care service providers are consulted during one treatment
- Mobility of patients → new HSP needs information about earlier treatments
- Cross-functional consolidation of data to get consistent view on patient‘s health data nationwide

Requirements

- Decentral storage of data
- Considering data protection
- Patient‘s consent for processing his/her health records
- Only selected documents are available to HSPs
- Cost-efficiency
- Compliant to EU guidelines (Interoperability,…)
- High-quality provisioning of health data by every single HSP (7/24 h availability)

System Architecture



ELGA - Austrian eHealth Strategy

IHE IT Infrastructure Profiles

- **All systems:**
  - „ATNA Secure Node“ using SSL/TLS
- **Patient Index:**
  - „Patient Identifier Cross-Reference Manager“ (PIX)
  - „Patient Demographic Query“ (PDQ) and uses
  - „ATNA Audit Trail Node“
- **HSP Index:** „ATNA Audit Trail Node“
- **Protocol System**: „ATNA Audit Trail Node“

ELGA - Austrian eHealth Strategy

IHE IT Infrastructure Profiles II

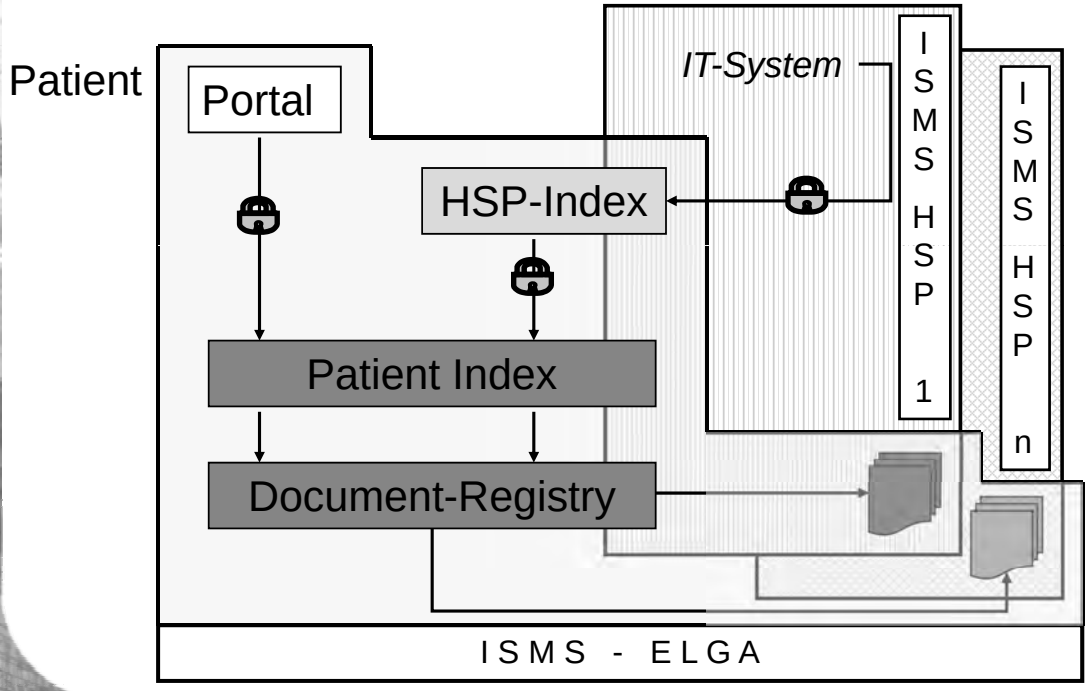
- **Authorization System:**
  - PIX, PDQ and XDR as proxy
  - uses the functions of Patient Index and Registry
  - checks and filters incoming parameters and outgoing results
- **Document Registry:**
  - „Cross Enterprise Document Sharing“
- **Portal:**
  - uses ELGA-functions through proxy interfaces

ISMS-ELGA

- **Security Concept**
  - Maintenance and improvement of security targets and security guidelines
  - Documentation of security requirements, that have to be considered while implementing the system
  - Ensure that
    - ***data integrity***
    - ***data availability***
    - ***data security***

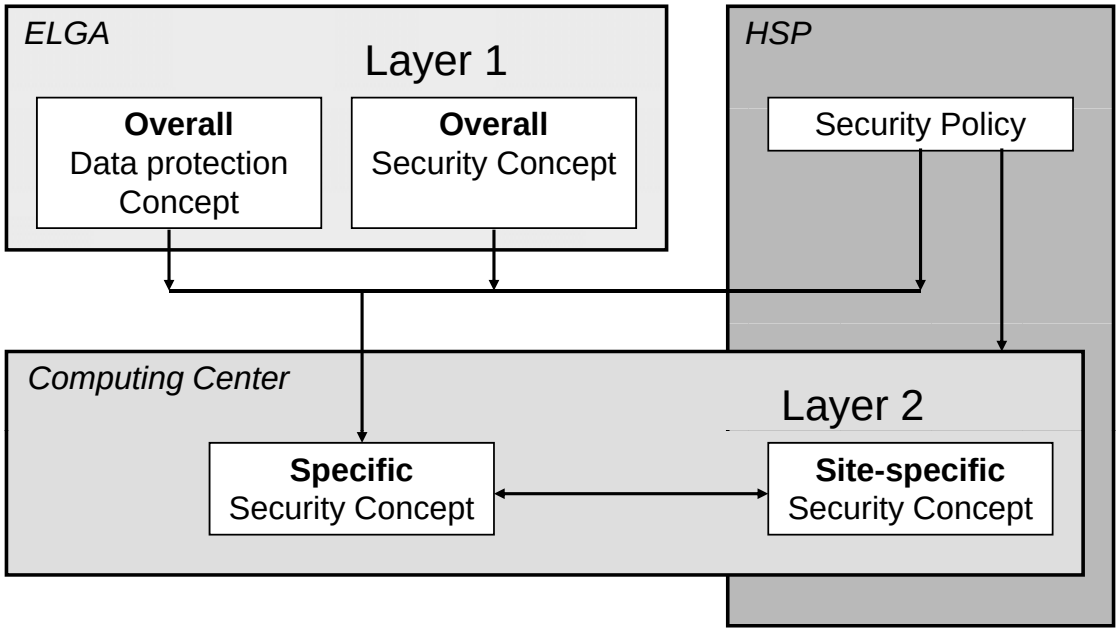
    of transferred/processed data comply with planned standards

Integration of ISMS-ELGA/ ISMS-HSP



ELGA - Austrian eHealth Strategy

Layers of ISMS Concept



ELGA - Austrian eHealth Strategy

Conclusion

Benefits from eHealth:

- Reduce medical errors and wastage of resources
- Serves increased patient and clinician demand

Privacy Concerns:

- Take concerns serious
  - *The problem is trust, not technology*.
  - Build trust in eHealth solutions

Conclusion II

ELGA System:

- Quality added value:
  - Integrated supply of data
  - Increased communication/cooperation of HSPs
  - Tool for modernizing and optimizing processes of Austrian health care system
- Privacy concerns:
  - ISMS according to ISO/IEC 2700x
  - IHE Integration Profiles

講　演

情報セキュリティが拓くネット社会の未来

岡本　龍明（日本電信電話株式会社情報流通プラットフォーム研究所 特別研究室長）

氏名　岡本　龍明（おかもと・たつあき）

所属　情報流通プラットフォーム研究所　岡本特別研究室長

学歴

1976.3　東京大学工学部計数工学科卒業

1978.3　東京大学工学系研究科計数工学専攻修士課程修了

1988.4　東京大学 博士（工学）取得

主要経歴

1978.4　日本電信電話公社入社

1978.5　横須賀通信研究所データ通信研究部　勤務

1985　　情報通信処理研究所　勤務

1989－1990　カナダ Waterloo 大学 客員助教授

1994－1995　AT&T Bell Laboratories 客員研究員

現在　日本電信電話株式会社　情報流通プラットフォーム研究所　岡本特別研究室長
　　フェロー

専門分野

暗号理論、情報セキュリティ、計算量理論

研究概要

公開鍵暗号系の各種方式、電子マネー、電子投票などの暗号プロトコルの開発及び安全性証明理論の研究に従事。

受賞

1991 年 NTT 研究開発本部長表彰・研究開発賞

1993 年 電子情報通信学会業績賞,小林記念特別賞「公開鍵認証方式に関する研究」

1997 年 電気通信普及財団賞（テレコムシステム技術賞）「理想的電子現金方式の一方法」

1998 年 科学技術庁長官賞（研究功績者賞）「効率的な電子署名方式に関する研究」

1999 年 NTT R&D フェロー

2000 年 日経 BP 技術賞「安全性を数学的に証明しただ円曲線暗号 PSEC」

2003 年 電子情報通信学会フェロー

2007 年 11 月　Certicom ECC Technology Award

2008 年 10 月　経済産業省商務情報政策局長表彰

2009 年　国際暗号学会 栄誉講演者

Inventing the Future of Network Society by Information Security

Tatsuaki Okamoto
(NTT)

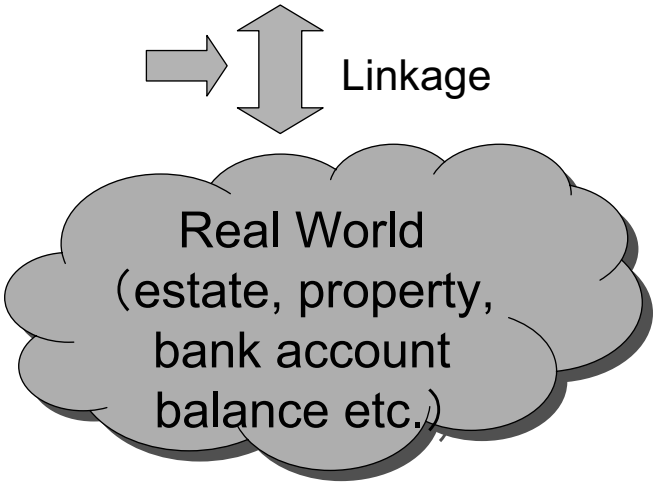
Information Security

The Role of Cryptography and Information Security

ICT systems ・・・ Virtual World

（Every information is communicated and recorded by digital data）

Cryptography and Information Security



Cryptography and Information Security

- Protecting Systems
  - Protect systems and databases from hackers to intrude and attack
- Promoting Business over Networks
  - Payment via networks (correctness)
  - Signing and contracting via networks
- Promoting Social Activities over Networks
  - Voting and auction via networks (privacy)
- Promoting Entertainment over Networks
  - Coin flipping and lottery over networks (fairness)

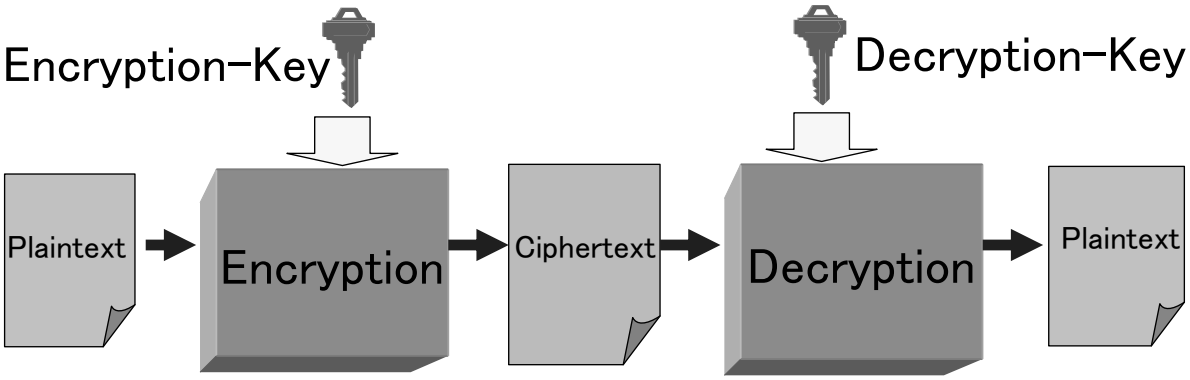
Cryptography: Key Technology in Information Security

- Basic primitives
  - Confidentiality (Encryption, Key distribution)
  - Authentication (Signatures)
- Cryptographic Protocols
  - Privacy-enhanced basic-primitives
  - Electronic voting
  - Electronic payment/money
  - Electronic contracting
  - Electronic gaming

Theoretically generalized → Multi-party protocols

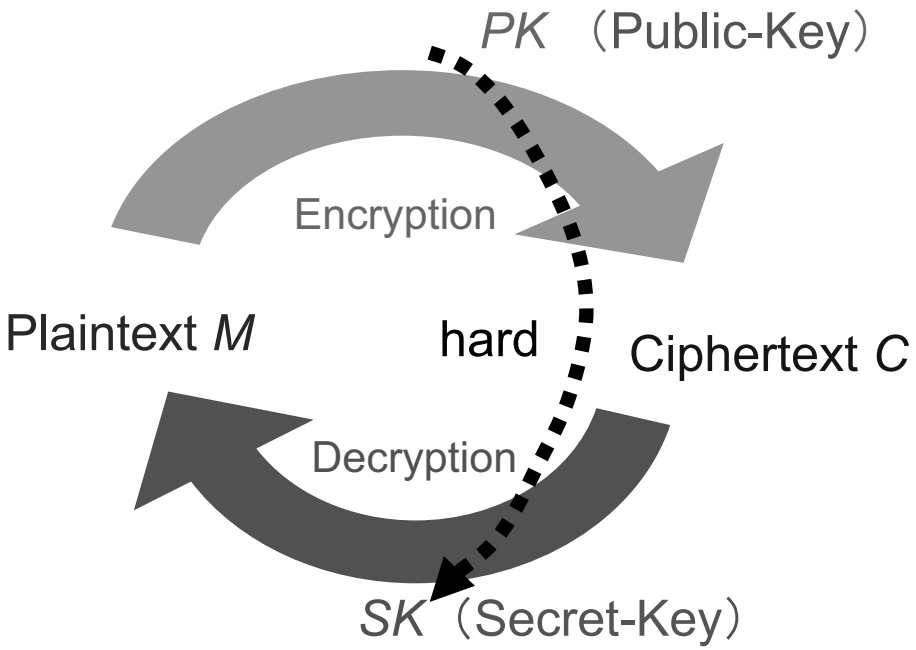
Current Technology

Symmetric and Public-key Encryption

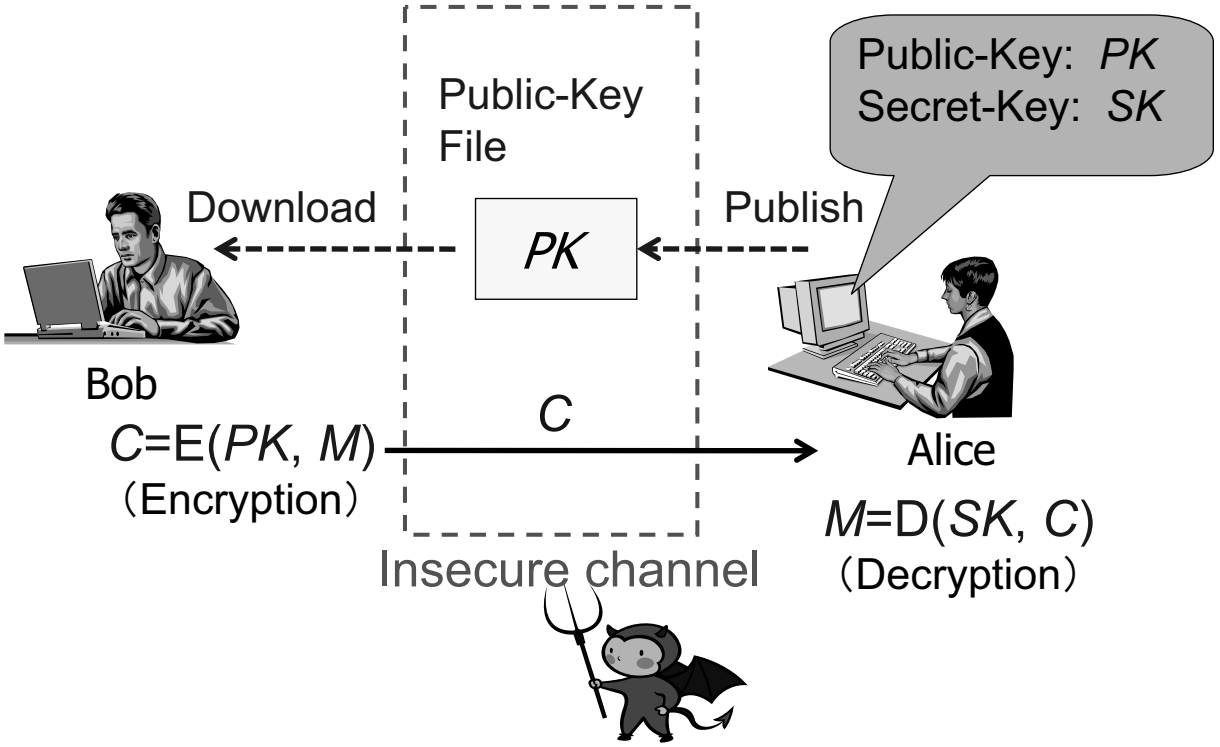


Symmetric Encryption	Encryption-Key ＝ Decryption-Key
Public-key Encryption	Encryption-Key ≠ Decryption-Key

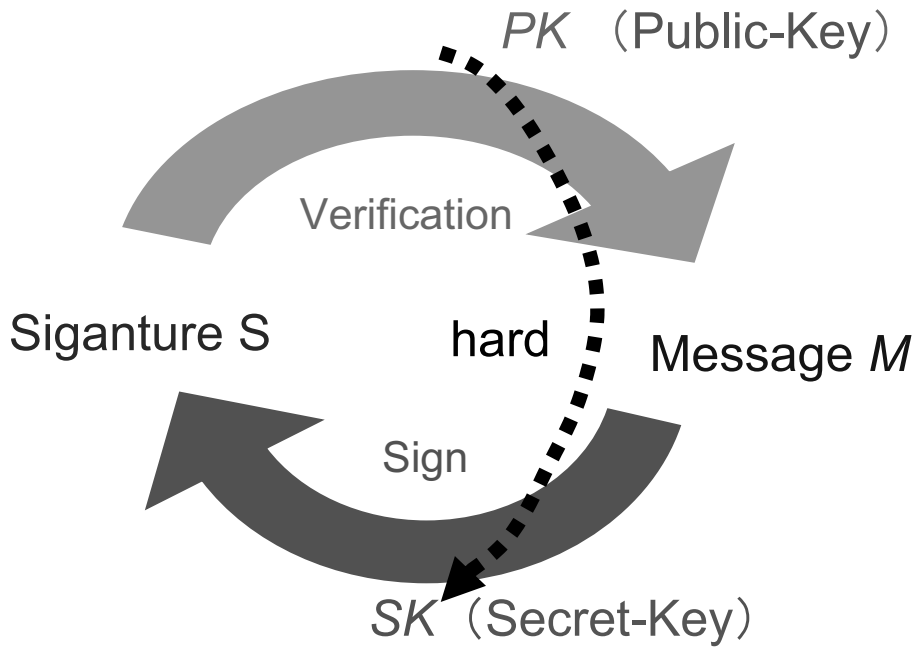
Principle of Public-key Encryption



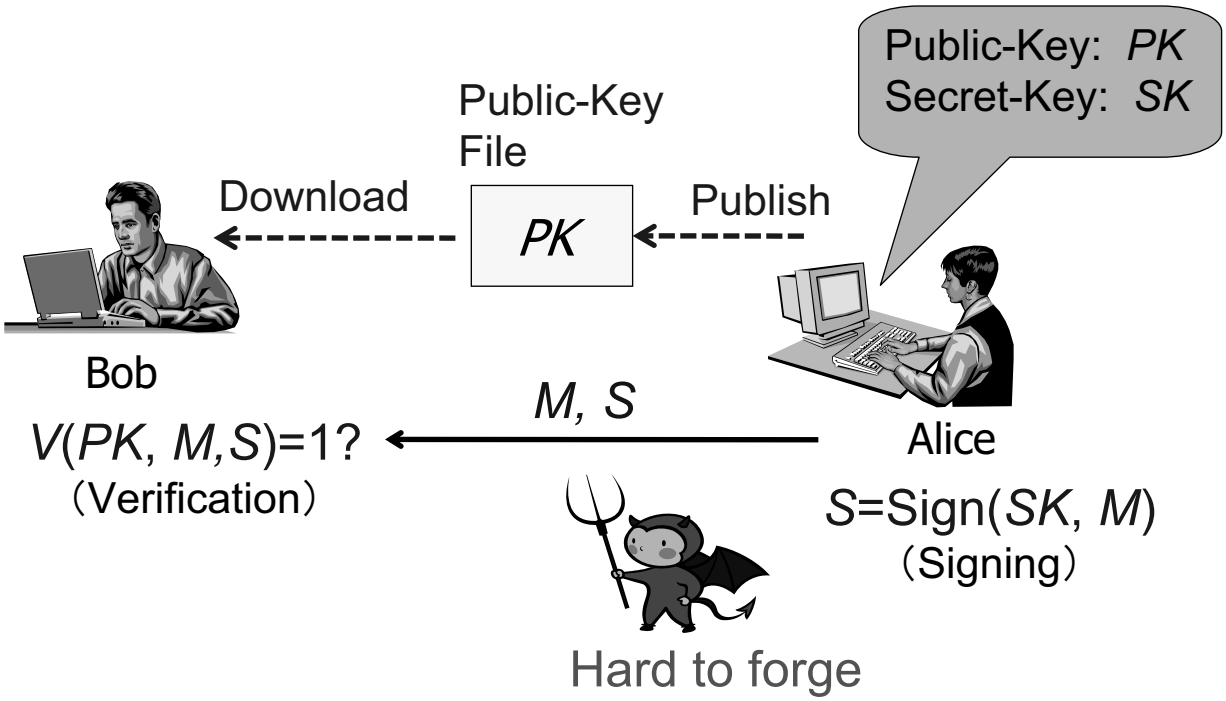
Public-key Encryption



Principle of Digital Signatures

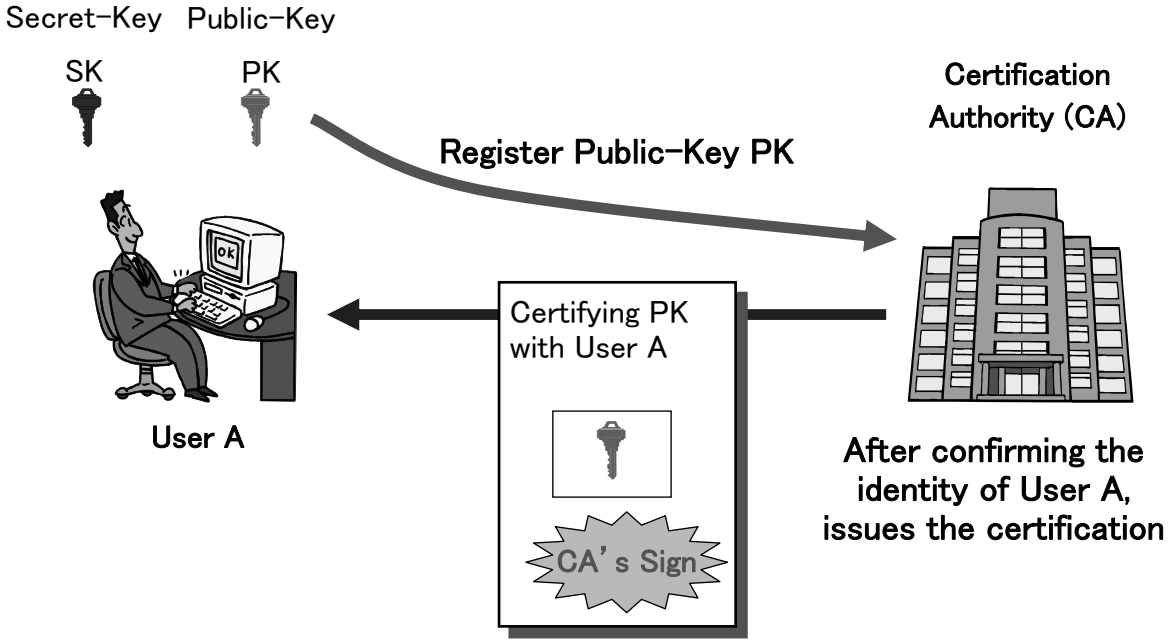


Digital Signatures



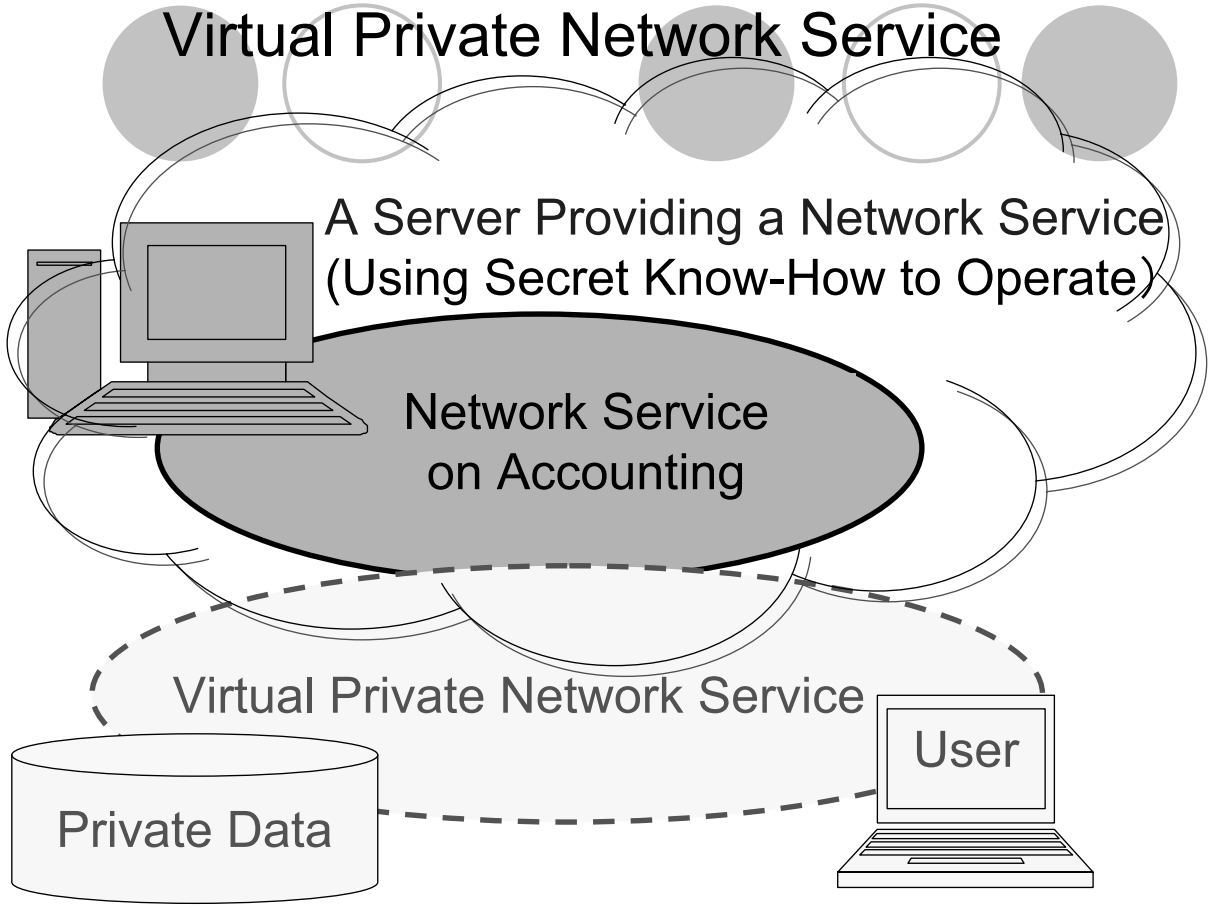
Public-Key Infrastructures (PKI)
Certification Authority (CA)

Organization to certify a public-key

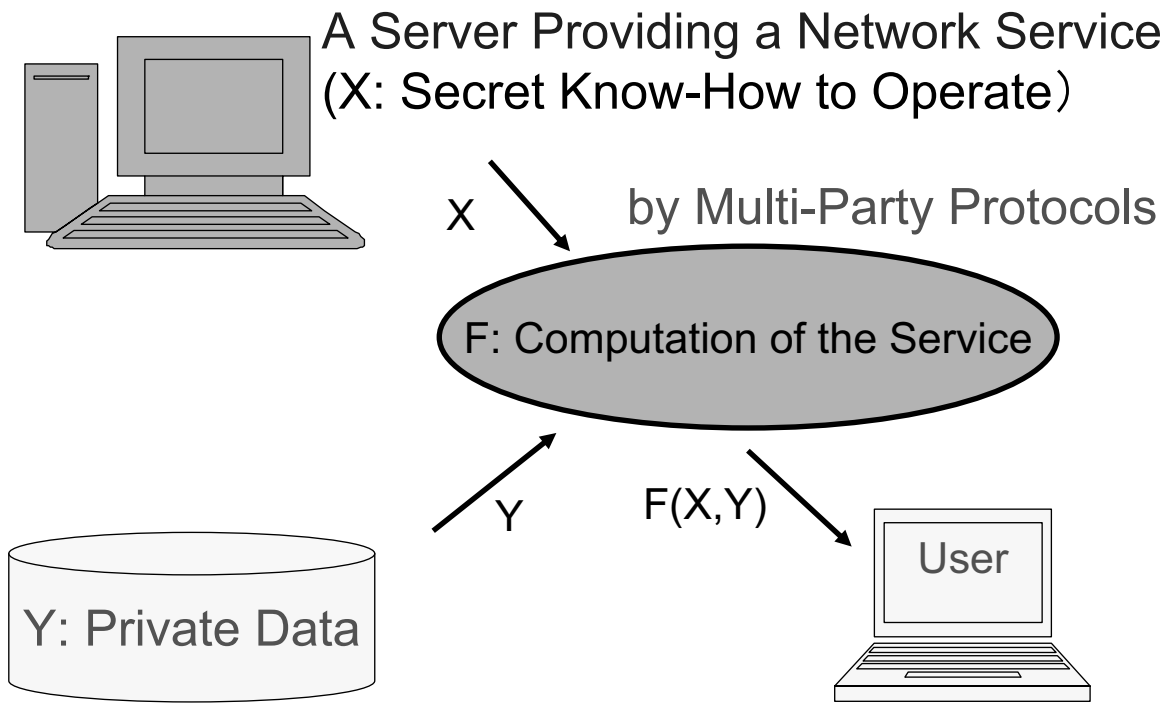


New Technology

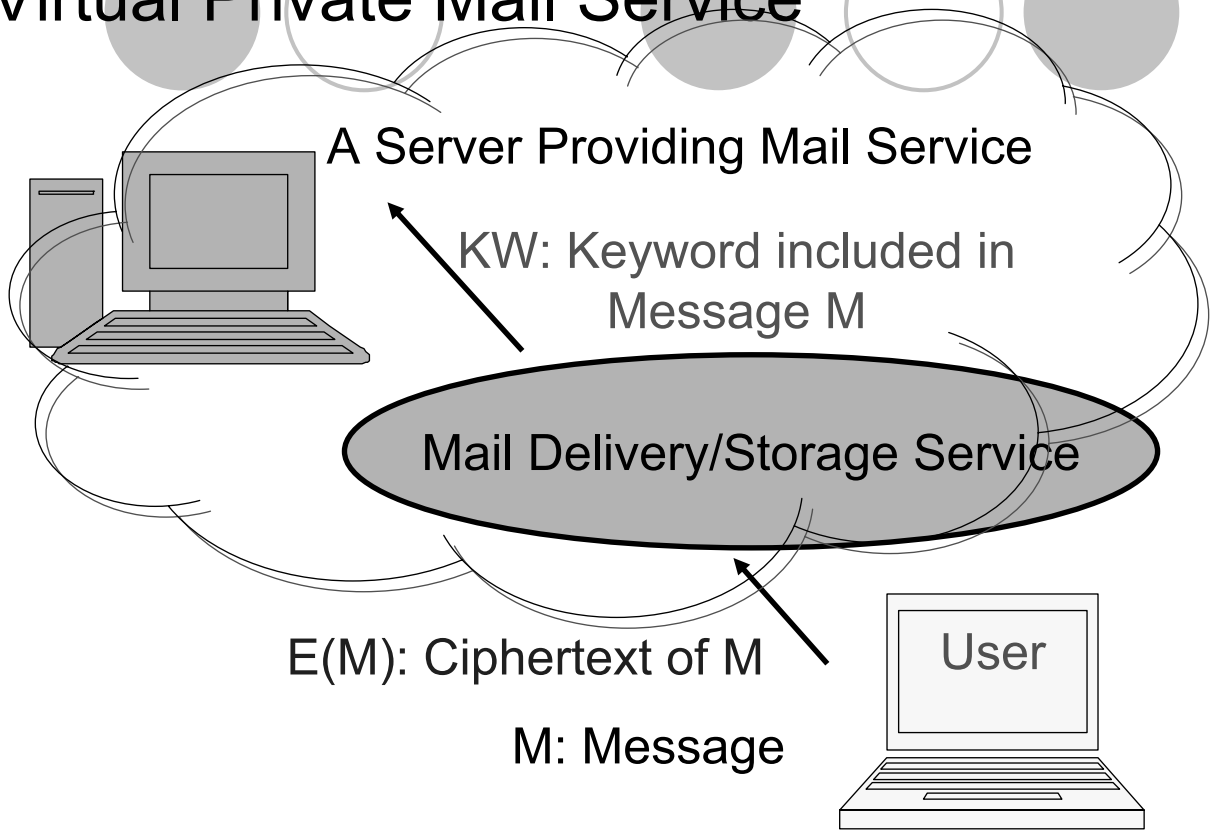
(for New Network Services like Cloud Computing)



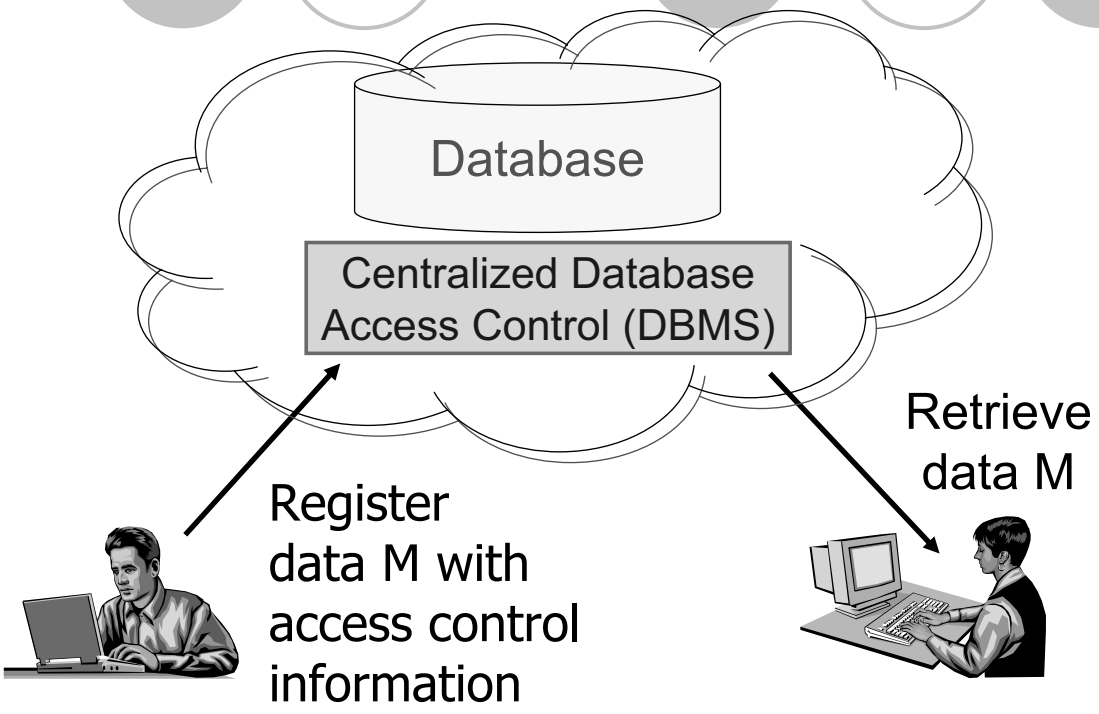
Virtual Private Network Service



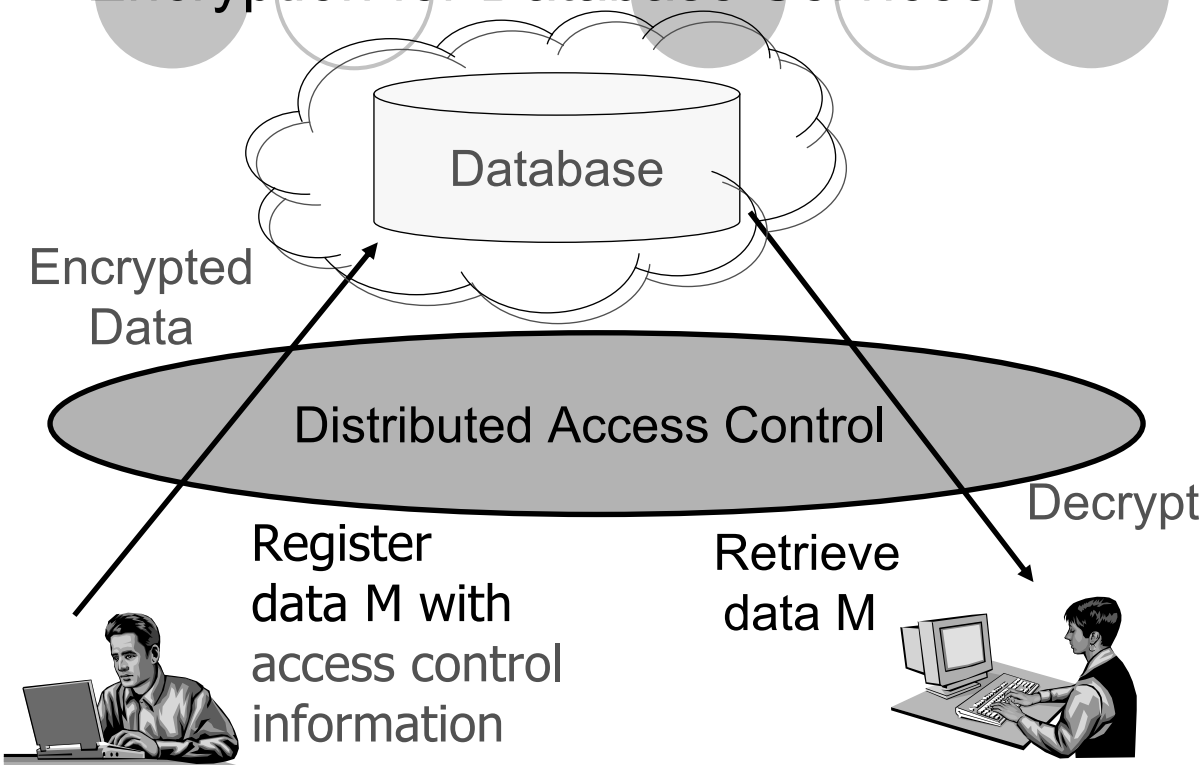
Virtual Private Mail Service



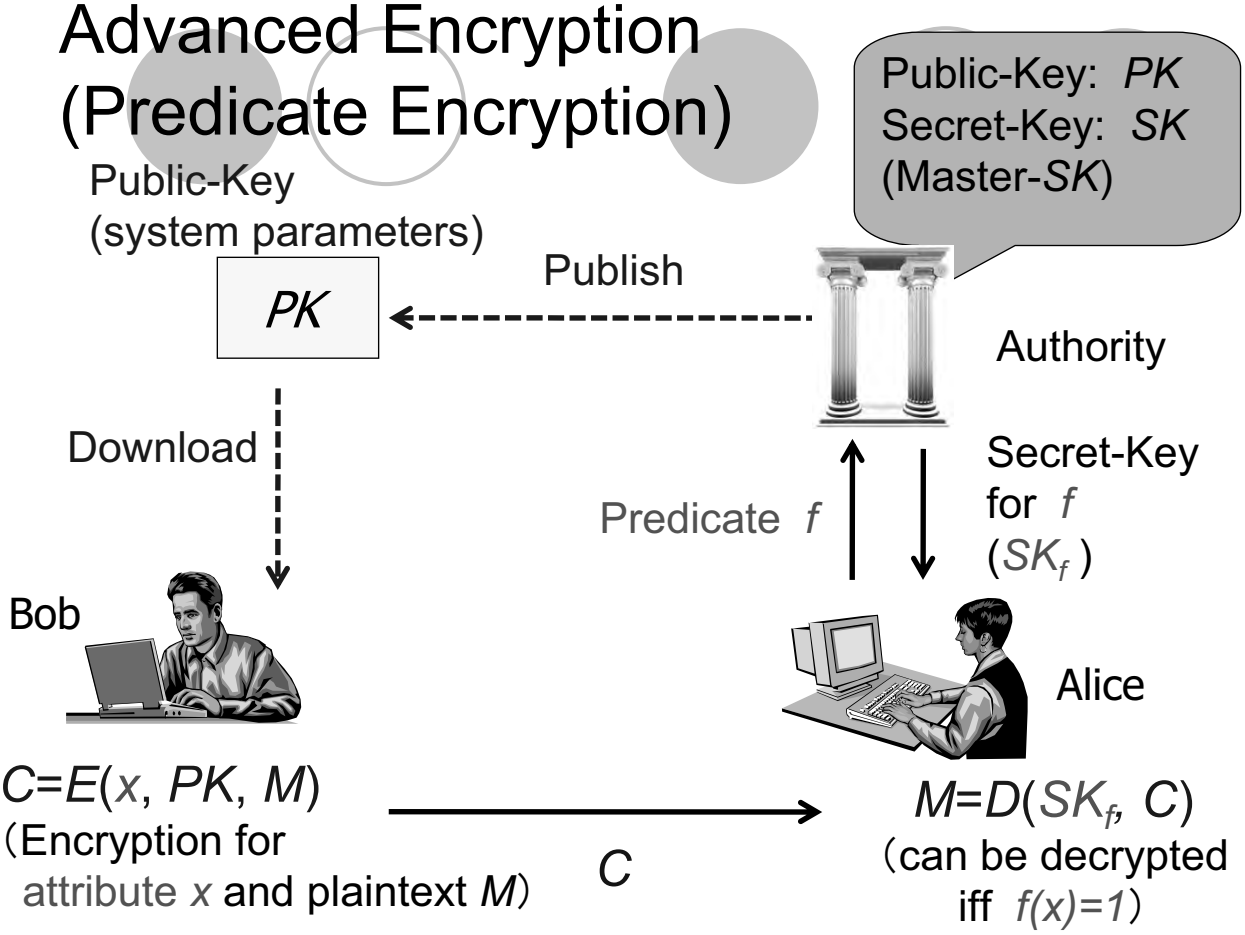
Centralized Access Control of Database Services



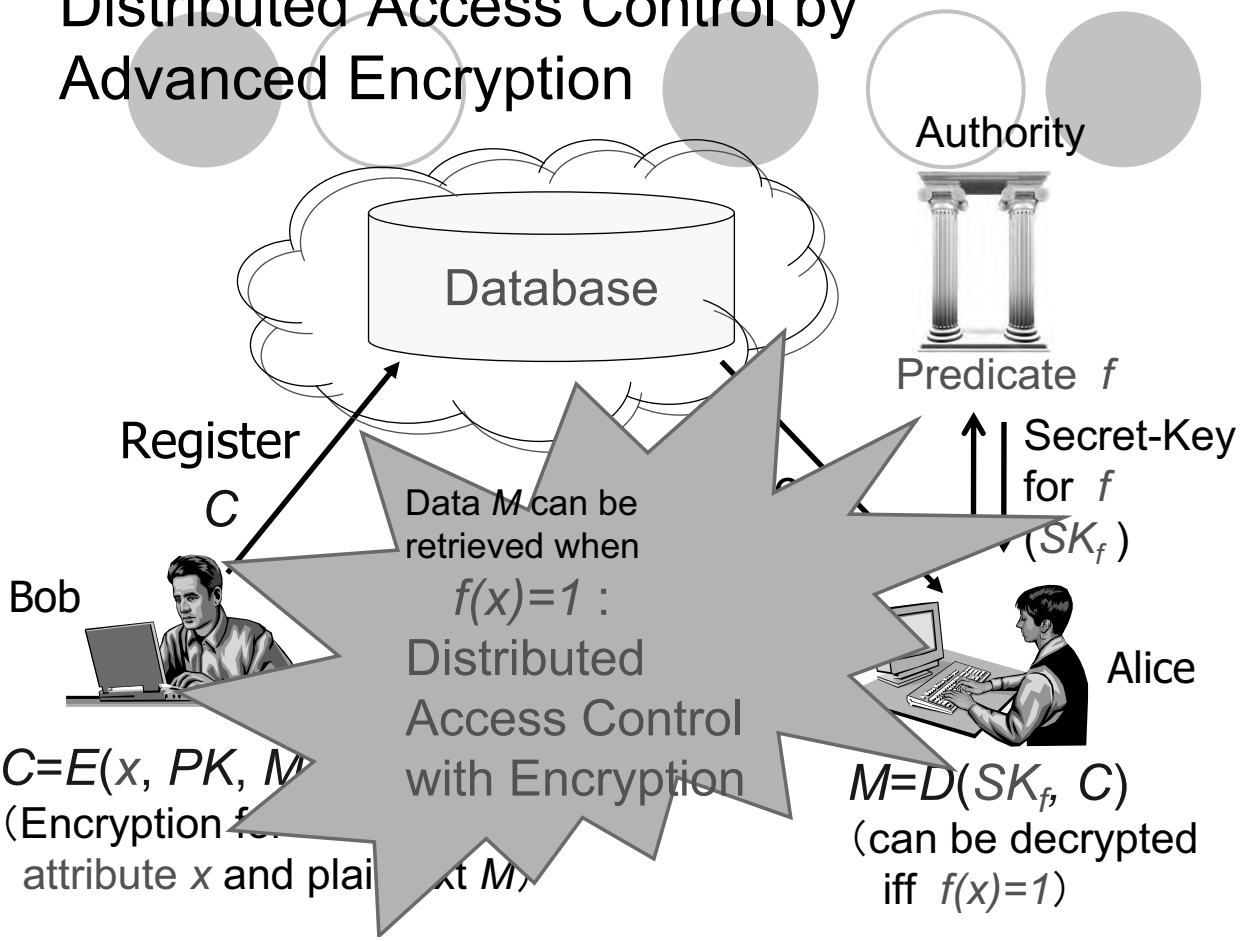
Distributed Access Control with Encryption for Database Services



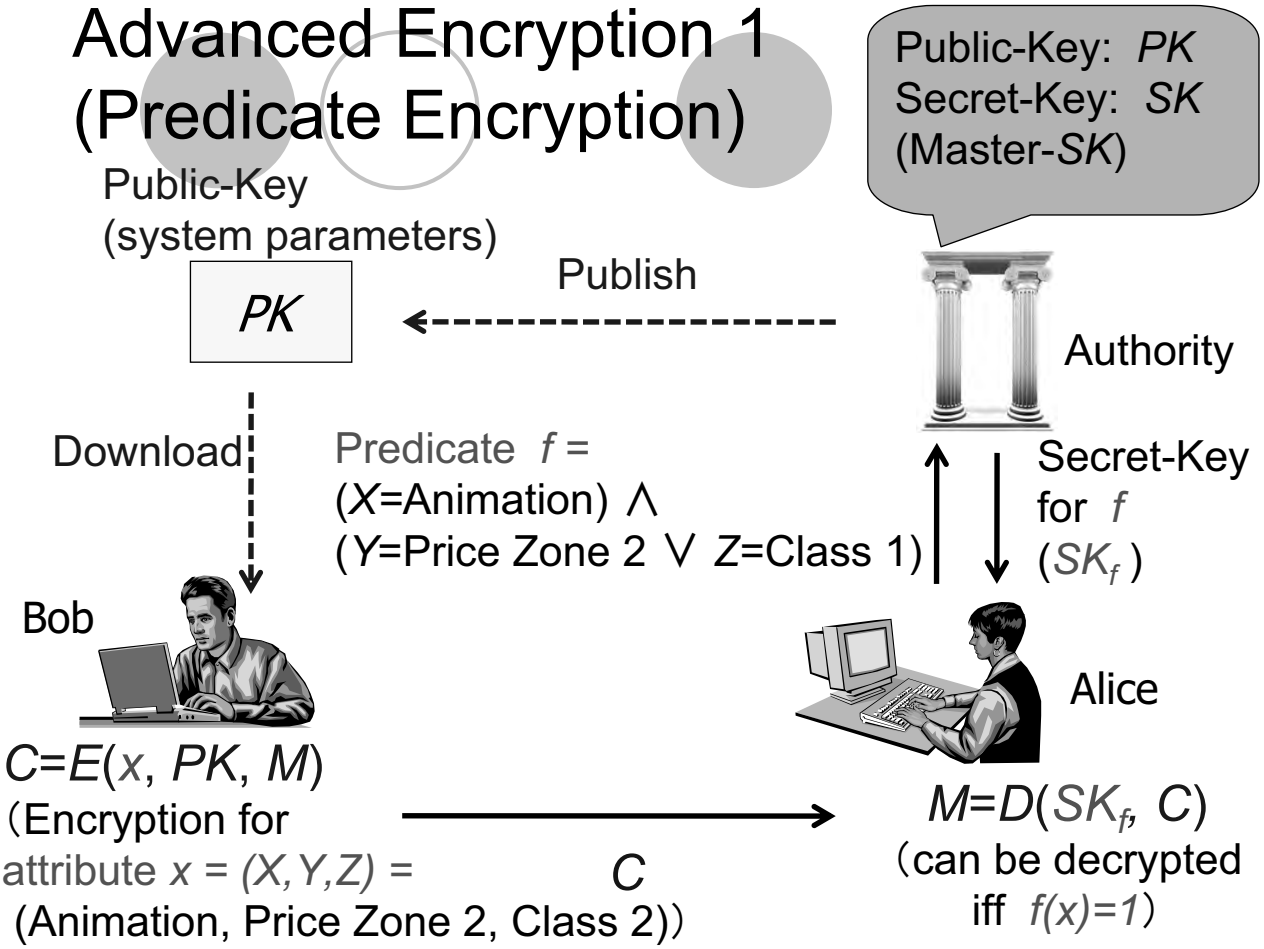
Advanced Encryption (Predicate Encryption)



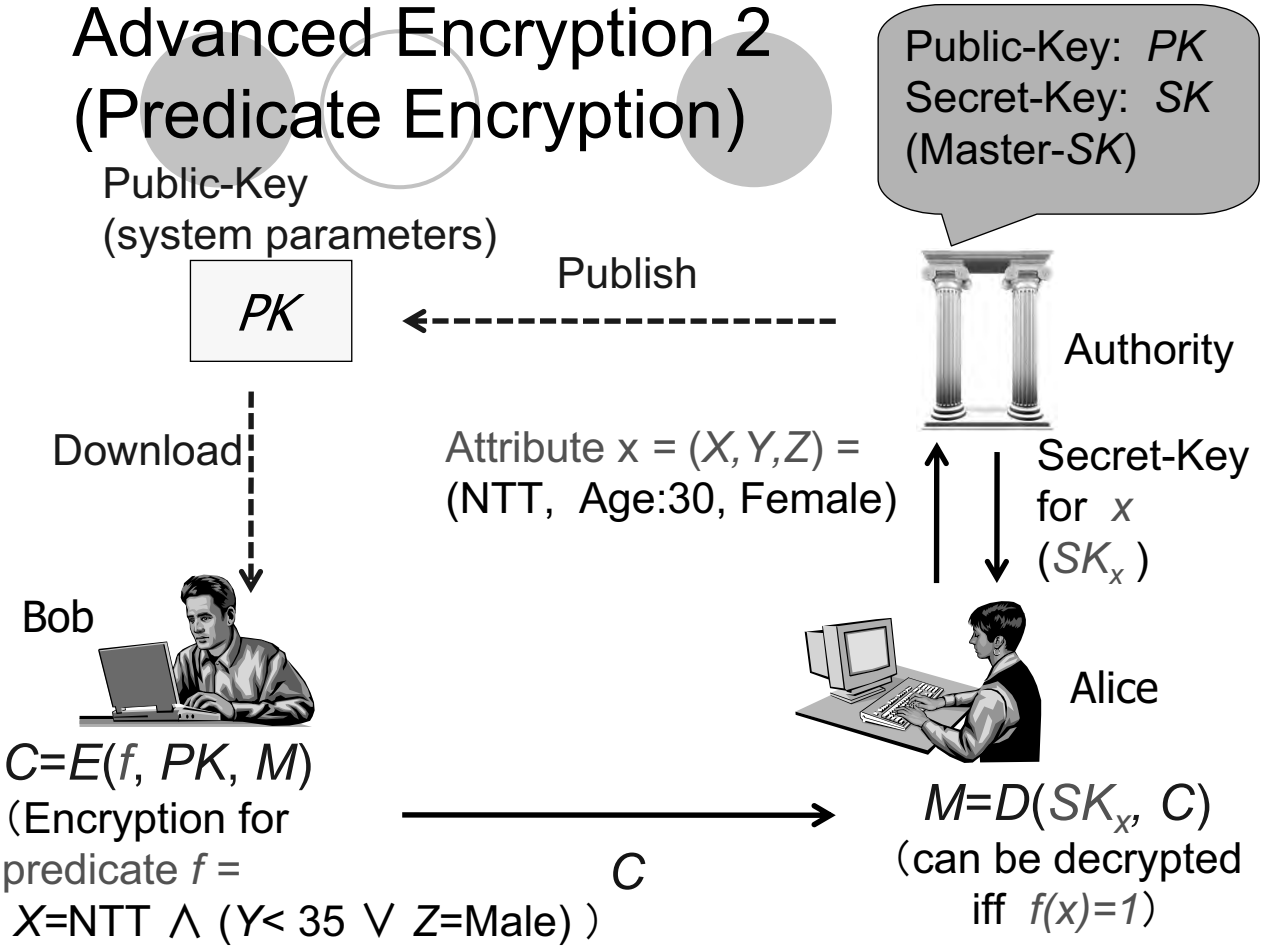
Distributed Access Control by Advanced Encryption



Advanced Encryption 1 (Predicate Encryption)



Advanced Encryption 2 (Predicate Encryption)



Summary

- How to guarantee the security in new network services like cloud computing is a key issue in promoting the services.
- New cryptographic (information security) technology guarantees and promotes secure networks services.
  - Multiparty protocols
  - Advanced encryption

講　演

実世界とITの融合による知識創発インフラストラクチャ

前田　　章（株式会社日立製作所システム開発研究所 所長）

氏名　前田　章（まえだ・あきら）
所属　株式会社日立製作所システム開発研究所　所長

学歴

昭和 53 年　東京大学理学部物理学科卒業
昭和 55 年　同大学院理学系研究科修士課程修了（物理学専攻）
工学博士（東京大学）

主要経歴

昭和 56 年　(株)日立製作所システム開発研究所入社
　　衛星・医用画像処理技術，知識情報処理技術等の開発に従事
平成 17 年 4 月より現職

専門分野

衛星画像処理、医用画像処理、ニューラルネットワーク、ファジィ、データマイニング等の研究開発を経て、現在、顧客価値の創造を実現する社会基盤・産業基盤・生活基盤・情報基盤の研究開発のマネジメントに従事

研究概要

合成開口レーダ高画質画像再生処理方式、
磁気共鳴イメージング（ＭＲＩ）画像再構成技術、
メンバシップ関数の形状をチューニングする拡張バックプロパゲーション法、
データに含まれる規則性をルール形式で抽出するデータマイニング技術の開発と実世界への適用

HITACHI
Inspire the Next

Knowledge Emergence Infrastructure by Convergence of Real World and IT

30 September, 2009

Systems Development Laboratory, Hitachi, Ltd.

Akira Maeda

Contents

uVALUE

1-1. Global Issues

HITACHI
Inspire the Next

21 global issues grappled by the United Nations

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

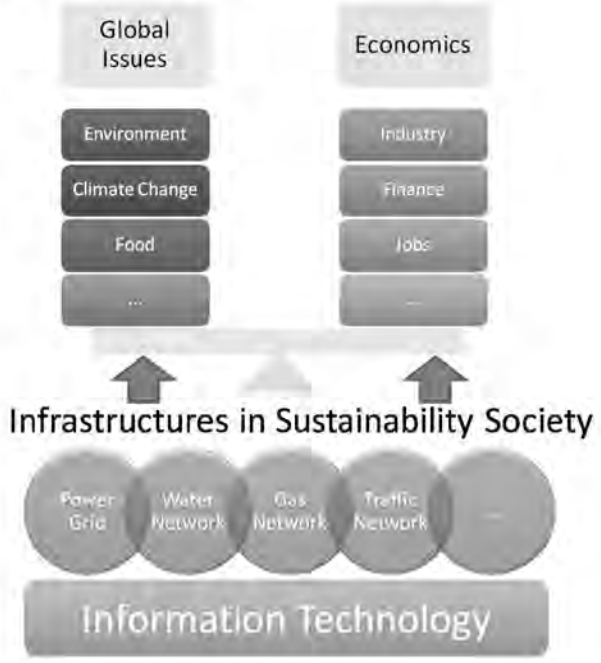
uVALUE

 1

1-2. Reasonable Approach to Tackle Global Issues

HITACHI
Inspire the Next

- 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.



uVALUE

 2

1-2. Reasonable Approach to Tackle Global Issues

HITACHI
Inspire the Next

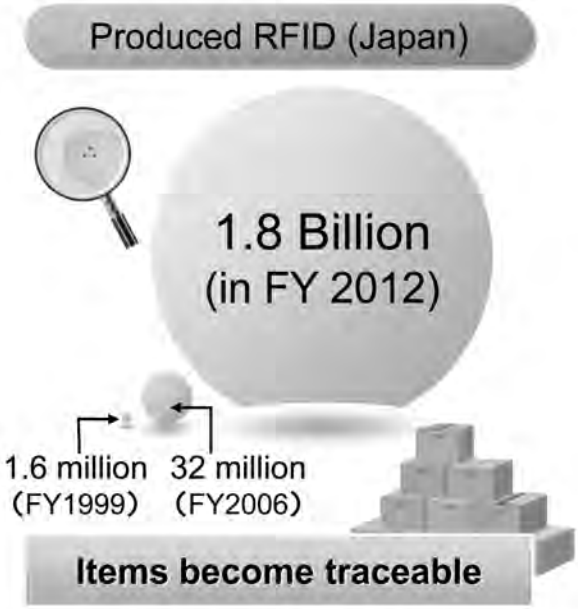
- It is important to improve efficiency of activity in daily life to harmonize issues.
- Social Infrastructures that support daily life should be "globally" optimized.
- IT plays a roll for a infrastructure of infrastructures.

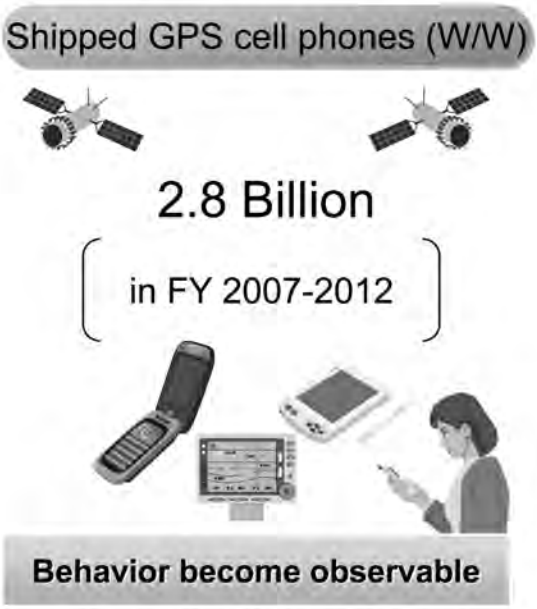
uVALUE

 3

1-3. Upcoming Information-Explosion Era

HITACHI
Inspire the Next





Reference : Yano Research, Parks Associates

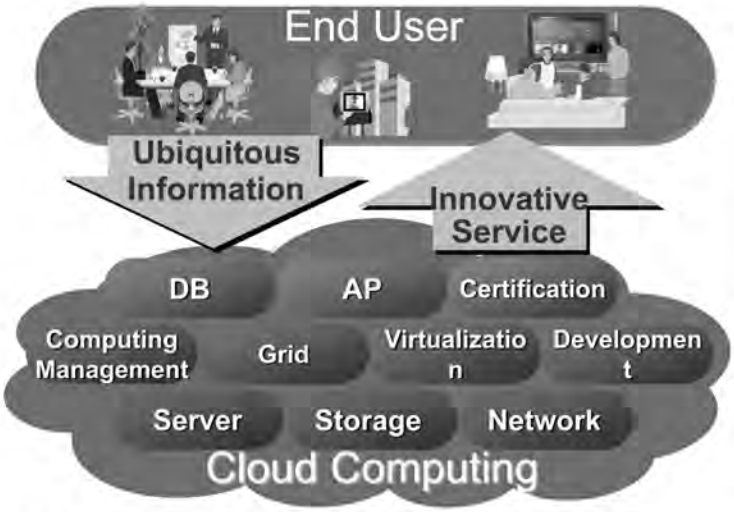
Newly evolutional services will be available by storing and using massive amount of real world data

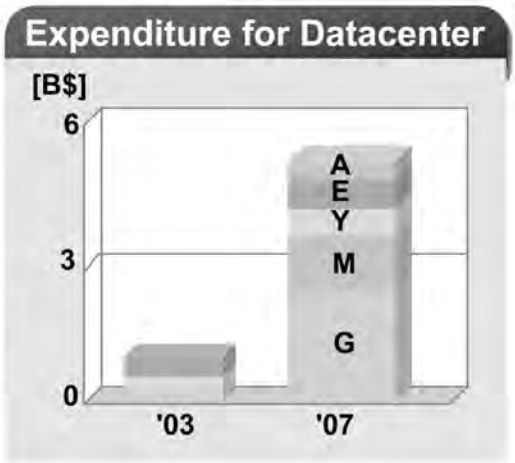
uVALUE

1-4. The Cloud yet to Come

HITACHI
Inspire the Next

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



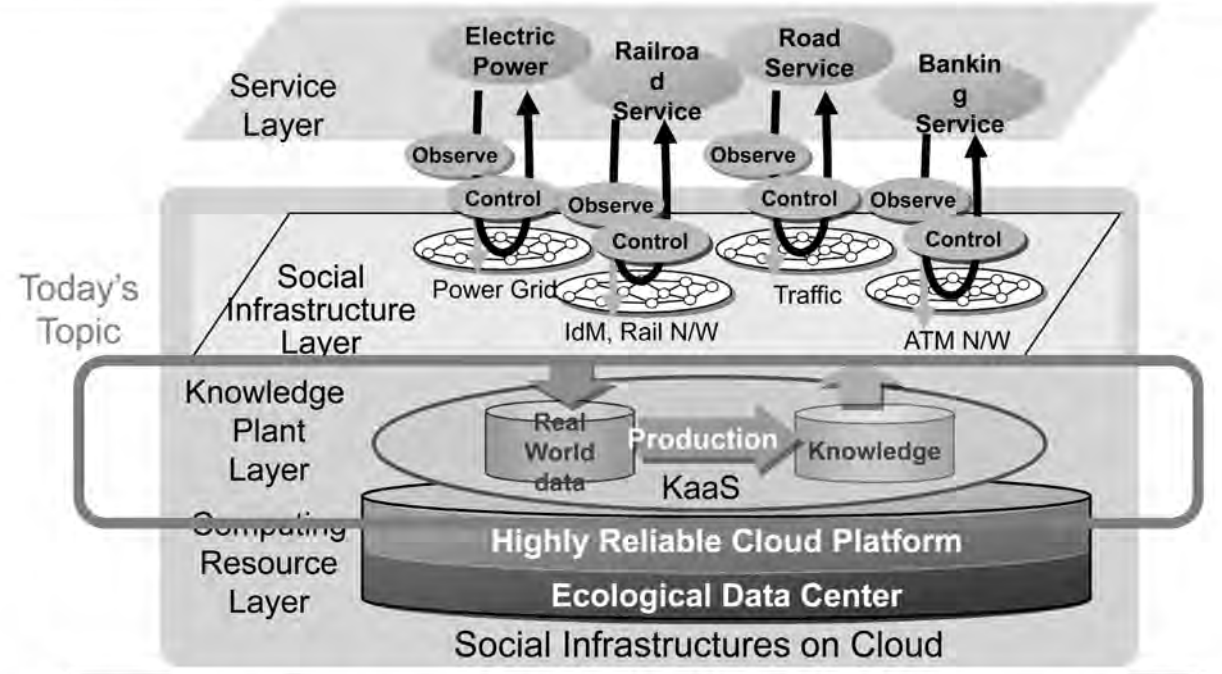


Cloud computing enables service providers to acquire valuable information and store them in the black box

uVALUE

1-5. Social Infrastructures on Cloud

HITACHI
Inspire the Next



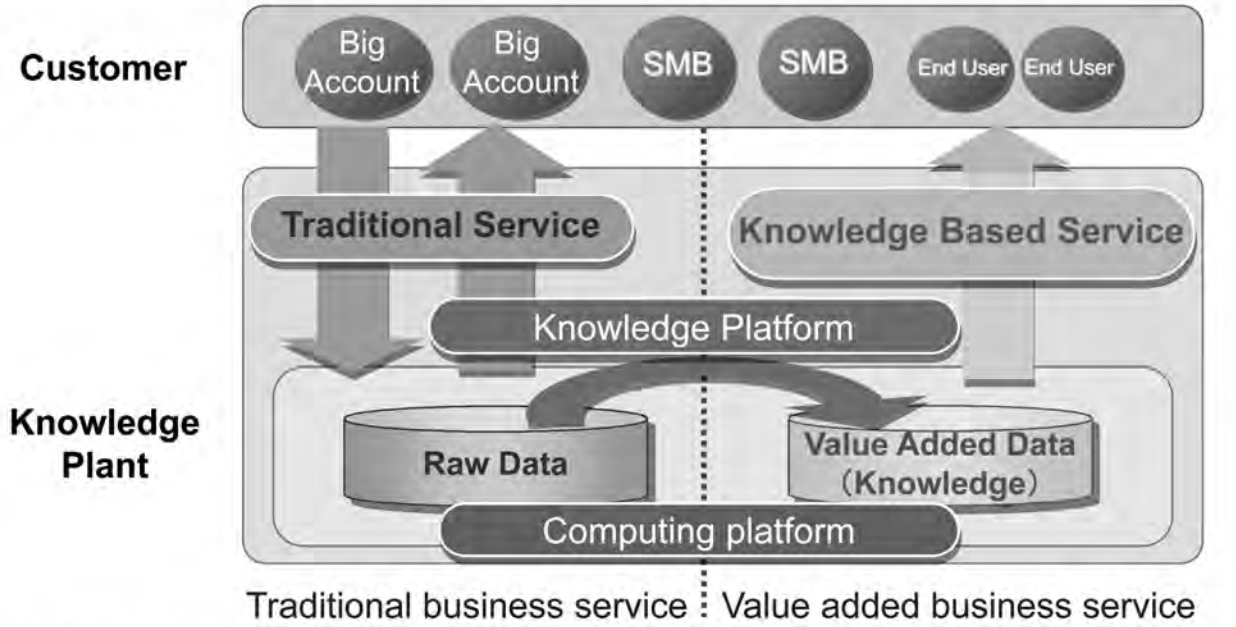
Social Infrastructures on cloud computers enable to observe, optimize and control real world

uVALUE

6

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

HITACHI
Inspire the Next



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

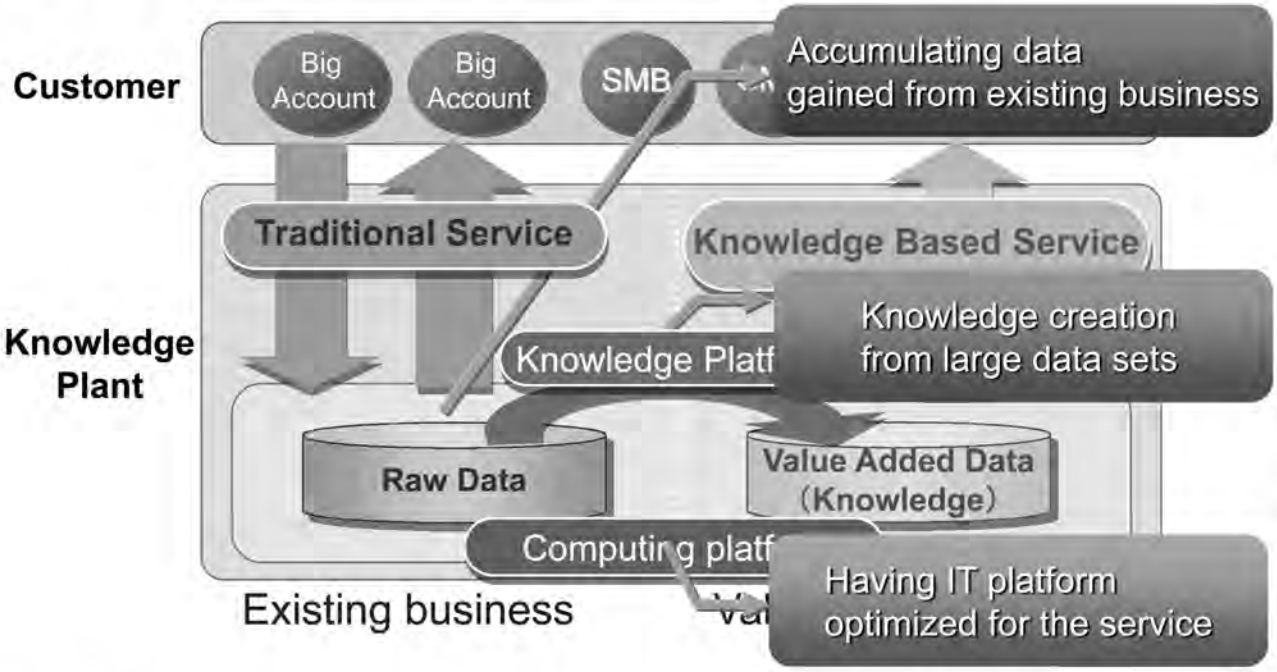
uVALUE

7

2-2. Approach to Bring KaaS to Reality

HITACHI
Inspire the Next

KaaS business model characteristics



uVALUE

 8

2-3. What to Do

HITACHI
Inspire the Next

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

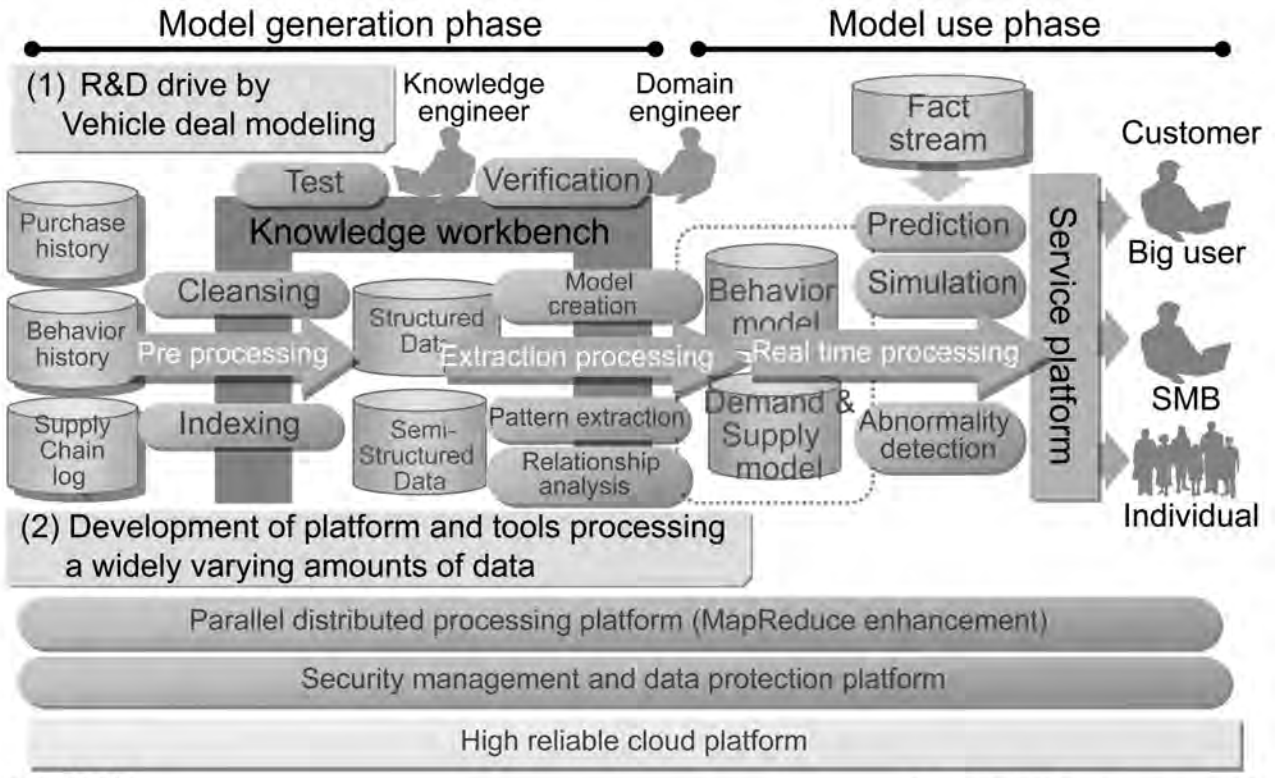
- Essentially new datacenter architecture for the real business data to be processed in a highly effective manner
- Adoption of emerging electronics technologies to enable ultra-low electricity consumption per operation
- A datacenter to be regarded and controlled as if it were a single computer

uVALUE

 9

2-4. KaaS Overview and Research Approach

HITACHI
Inspire the Next

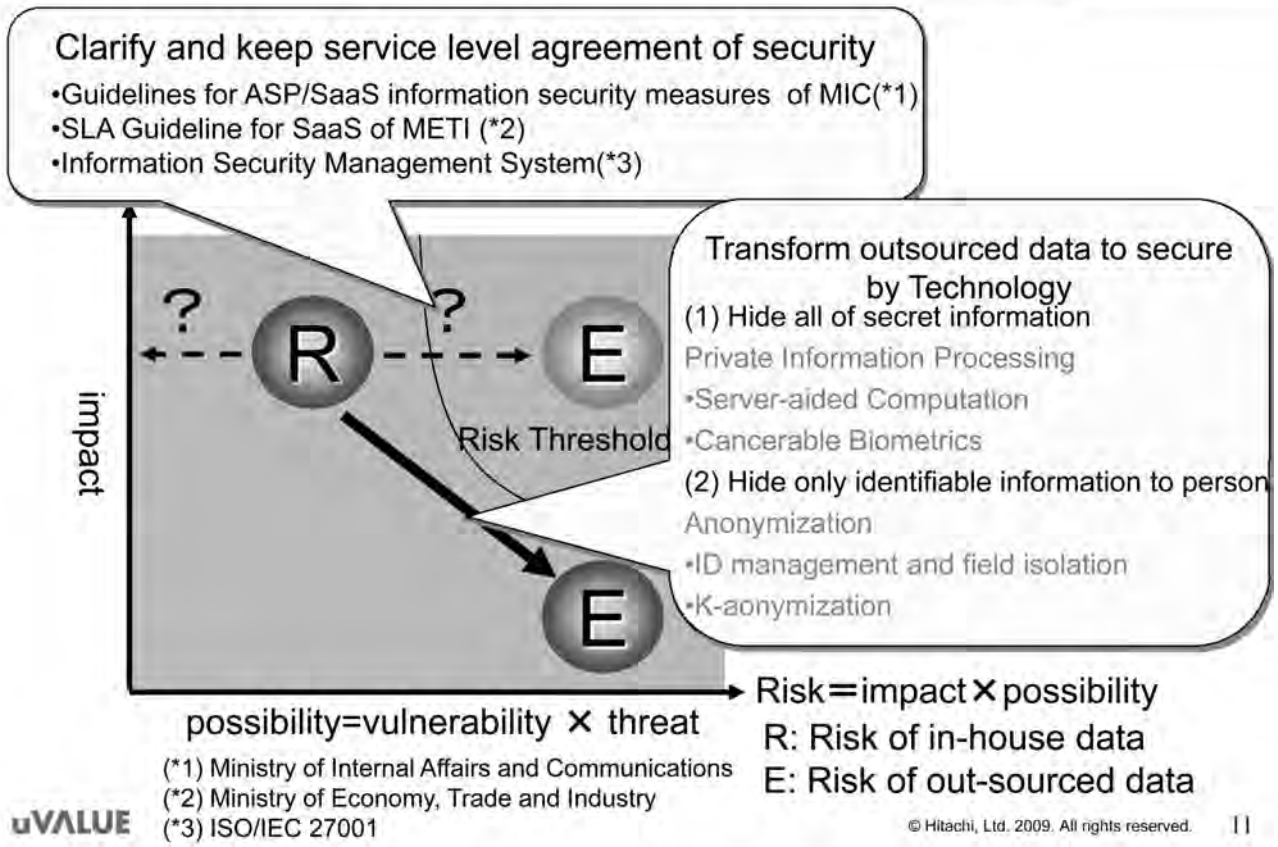


uVALUE

 10

3-1. Risk Management Strategy for Cloud Security

HITACHI
Inspire the Next



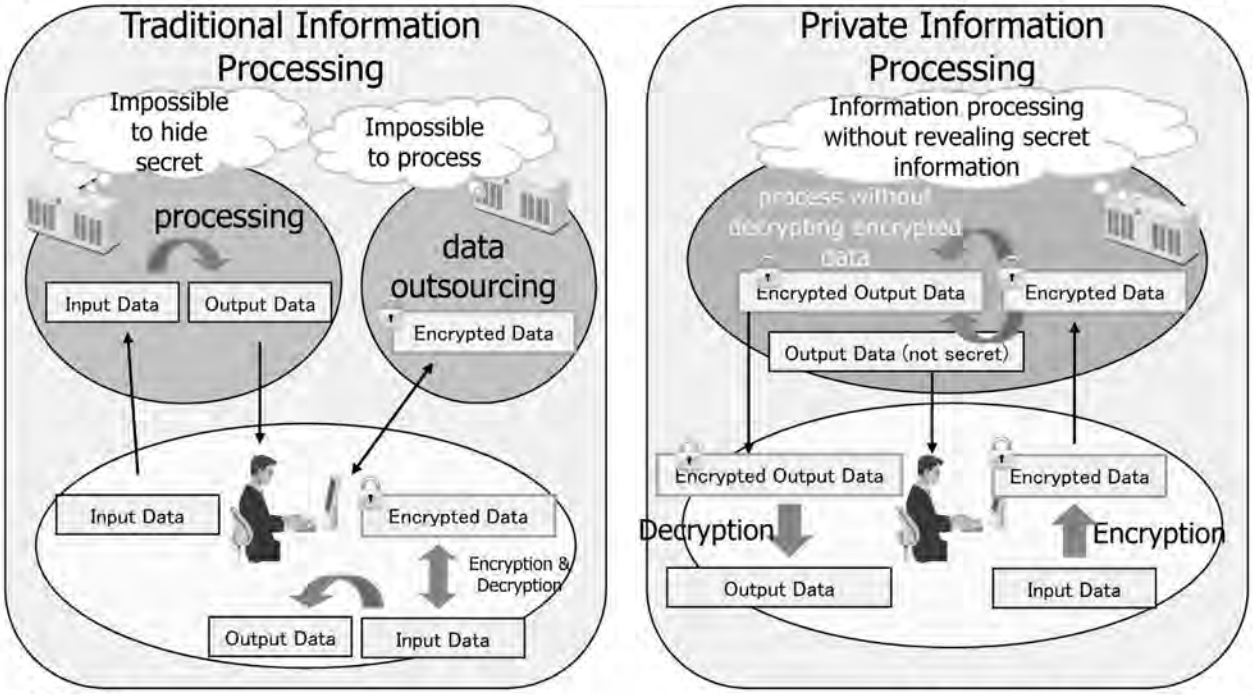
uVALUE

 11

3-2. Private Information Processing

HITACHI
Inspire the Next

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



uVALUE

 12

3-3. Practical Example: Cancelable Biometrics

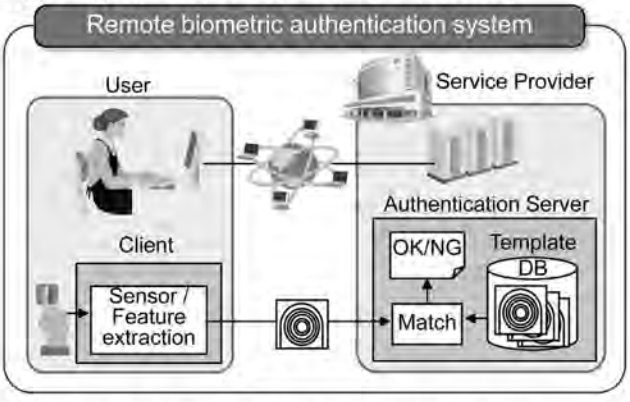
HITACHI
Inspire the Next

■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

uVALUE

 13

3-3. Cancelable Biometrics: Overview

HITACHI
Inspire the Next

- **Cancelable biometrics**

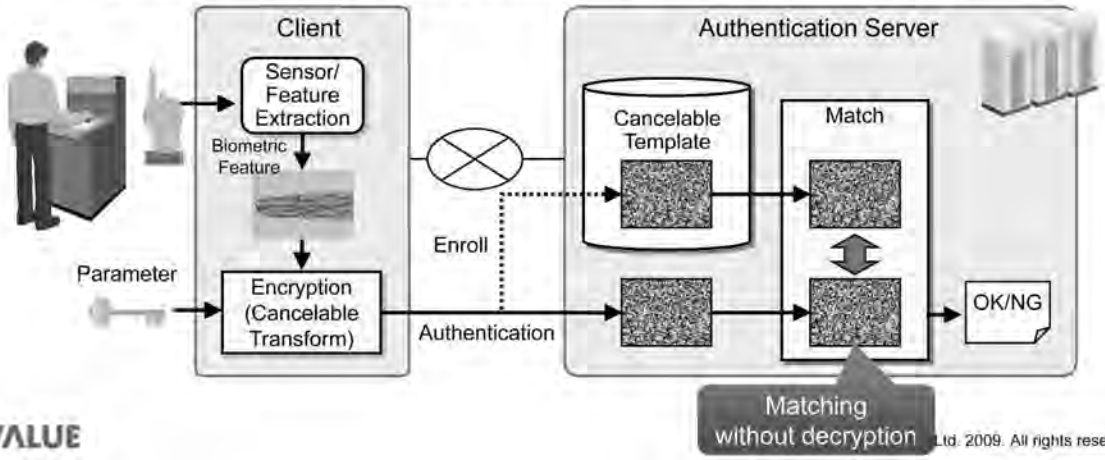
  The biometric authentication scheme with template protection
  - in which biometric features are encrypted, and matched without decryption

- **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.



uVALUE

3-4. General Approach: Server-aided Computation

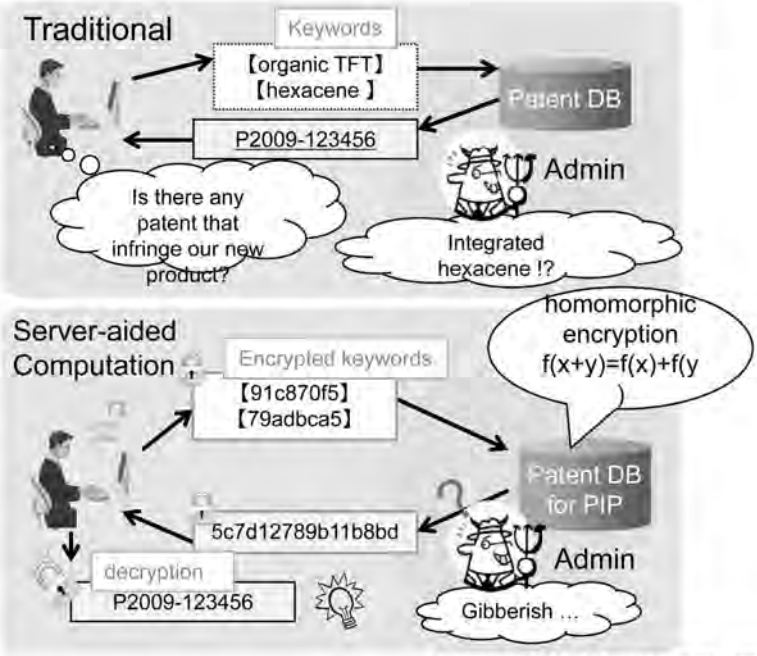
HITACHI
Inspire the Next

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.

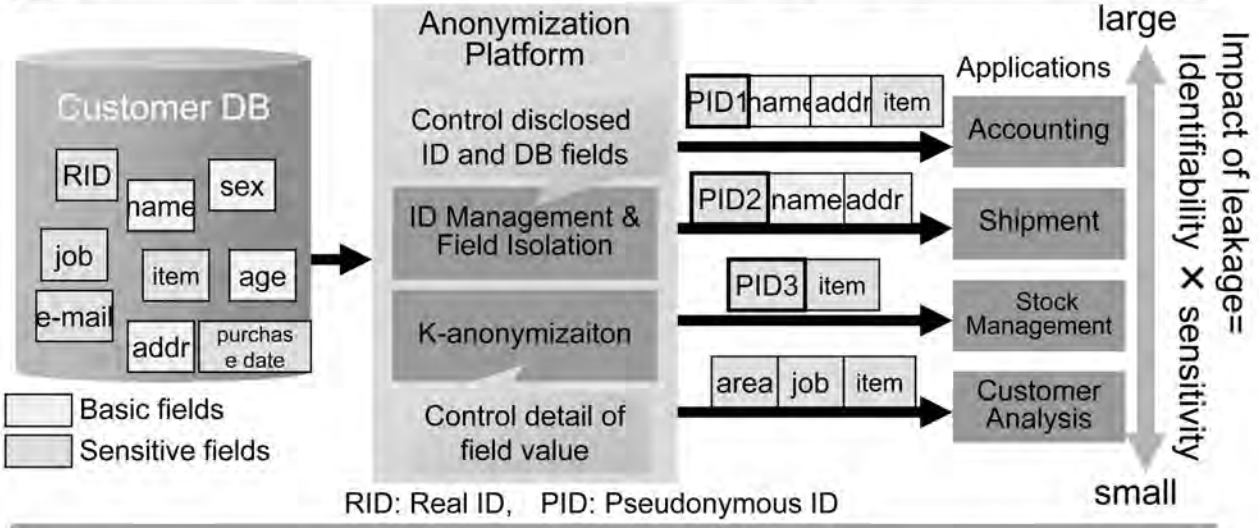


uVALUE

3-5. Anonymization for Personal Data

HITACHI
Inspire the Next

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



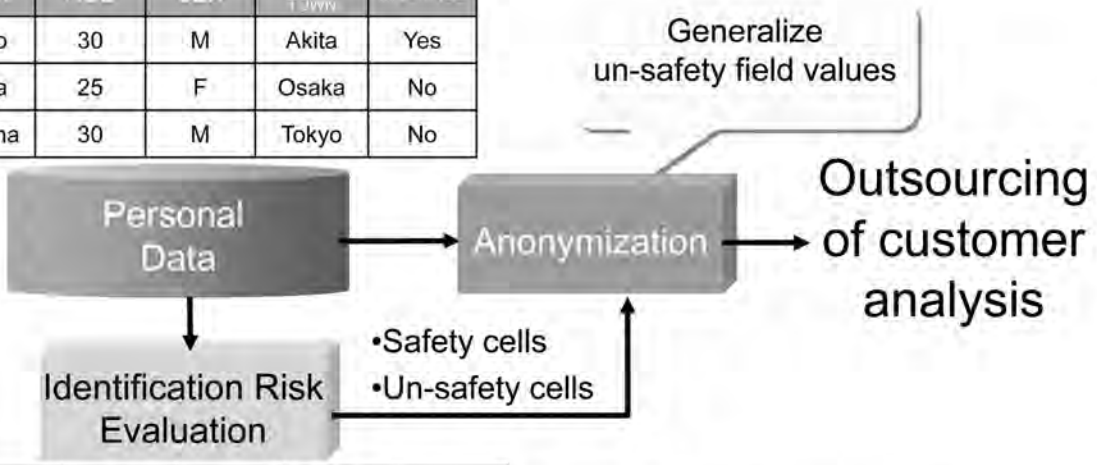
Hiding ONLY leakage between person and information enable go together safety and usability of personal data

3-5. Anonymization: K-anonymization

HITACHI
Inspire the Next

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



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

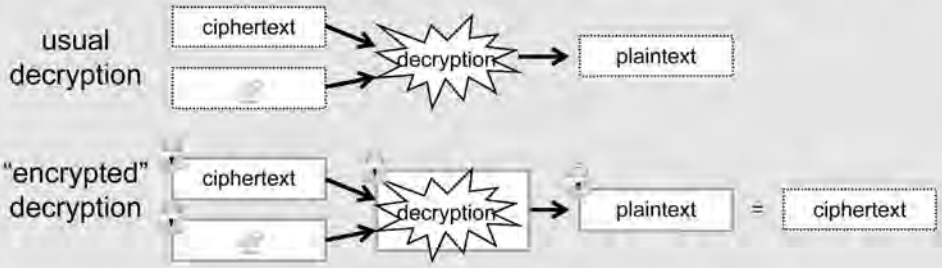
Un-Safety — Not satisfy k-anonymity if it is used with safe cells

3-6. Directions of Future Works

HITACHI
Inspire the Next

- 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



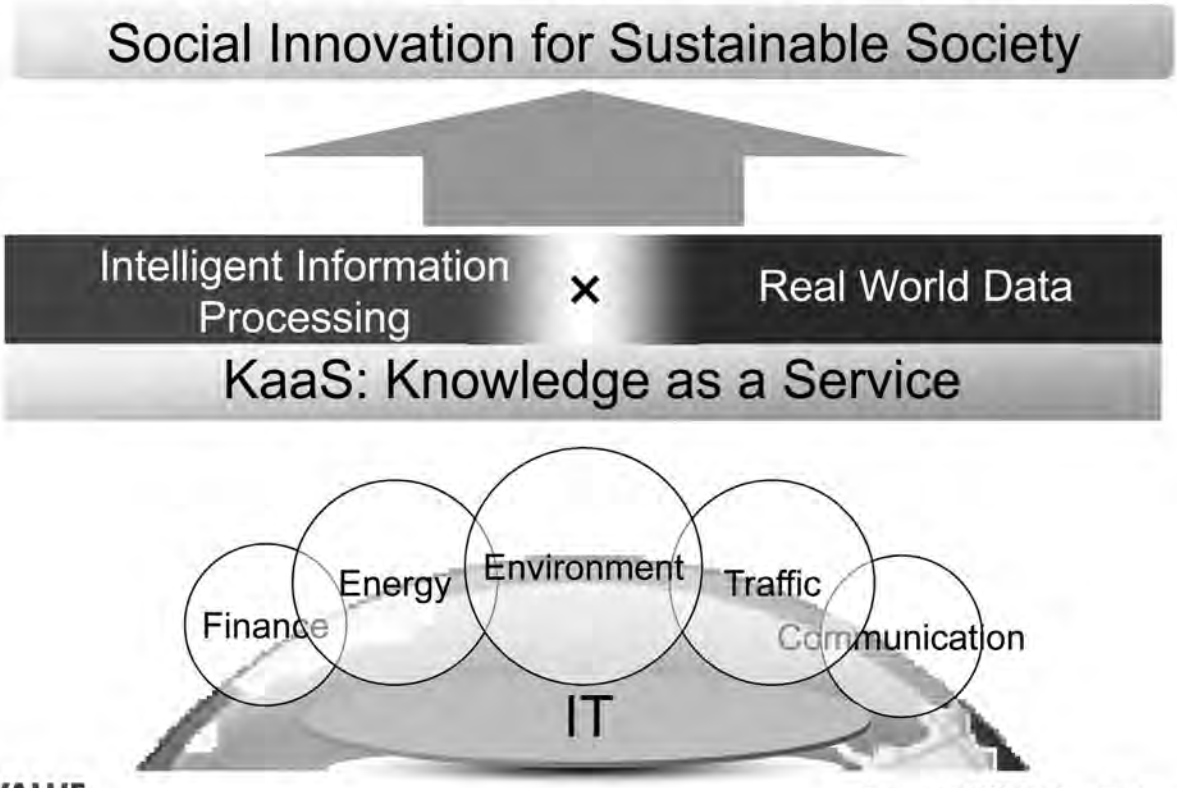
- Research for application specific technology
  - Authentication services: cancellable biometrics
  - Patent search: PIR based on traditional homomorphic encryption
  - Customer analysis: k-anonymization

uVALUE

 18

4. Conclusions

HITACHI
Inspire the Next



uVALUE

 19

講　演

地球規模の知識共有と教育機関の役割

安西　祐一郎（国立情報学研究所 顧問，前慶應義塾 塾長）

氏名　安西　祐一郎（あんざい・ゆういちろう）
所属　国立情報学研究所 顧問、慶應義塾 学事顧問、
慶應義塾大学理工学部 教授

学歴
昭和 44 年　慶應義塾大学工学部卒業
昭和 49 年　同大学大学院工学研究科博士課程管理工学専攻修了
工学博士

主要経歴
昭和 46 年　慶應義塾大学工学部助手
昭和 51～53 年　カーネギーメロン大学（米国）博士研究員
昭和 54 年　慶應義塾大学工学部専任講師
昭和 56～57 年　カーネギーメロン大学（米国）客員助教授
昭和 60 年　北海道大学文学部行動科学科助教授
昭和 63 年　慶應義塾大学理工学部電気工学科(現所属 情報工学科)教授
同大学大学院理工学研究科教授
平成 2 年　マギル大学（カナダ）客員教授
平成 5～13 年　慶應義塾大学理工学部長・大学院理工学研究科委員長
平成 13 ～21 年　慶應義塾長（学校法人慶應義塾理事長兼慶應義塾大学長）
平成 15～21 年　社団法人日本私立大学連盟会長、日本私立大学団体連合会会長
全私学連合代表（協議会議長）
平成 15 年～19 年　内閣府知的財産戦略本部員
平成 17 年～19 年　情報処理学会会長
平成 20 年～21 年　環太平洋大学協会会長
平成 21 年～　慶應義塾学事顧問
平成 21 年～　国立情報学研究所顧問

専門分野
情報科学、認知科学、知的社会基盤工学

研究テーマ
思考と学習の認知科学的研究、
ヒューマン・ロボット・コンピュータインタラクション

人間の認知、思考、学習、記憶などの情報処理過程を情報科学の方法論によって解明する認知科学、および人間と環境・コンピュータ・ロボットとのインタラクティブシステムの研究分野におけるパイオニアとして知られている。特に、人間の情報処理メカニズムの解明とその応用に関する研究を 30 年間以上にわたり続けており、情報科学、心理学、言語学、神経科学、コンピュータサイエンス、ロボティクス等にわたる知識を駆使し、人間の知性と感性のメカニズムがいかに豊かであるかを明らかにすることをライフワークとしている。また、その成果を個々の人間の能力が発揮されやすく暮らしやすい環境やシステムのデザインに役立てることを目指している。

受賞
昭和 63 年　人工知能学会業績賞
平成 17 年　フランス共和国政府教育功労賞コマンドゥール
平成 19 年　ECN (Ecole Centrale de Nantes)（フランス）名誉博士号
平成 20 年　紫綬褒章(情報学)
平成 20 年　情報処理学会功績賞
平成 21 年　延世大学（韓国）名誉博士号
ほか

Global Knowledge Sharing and Roles of Educational Institutions

Yuichiro Anzai
Senior Advisor, National Institute of Informatics
Former President, Keio University

30 September 2009, Tokyo
International Workshop on Information Systems for Social Innovation 2009
National Institute of Informatics

Change of the World and Higher Learning Environment

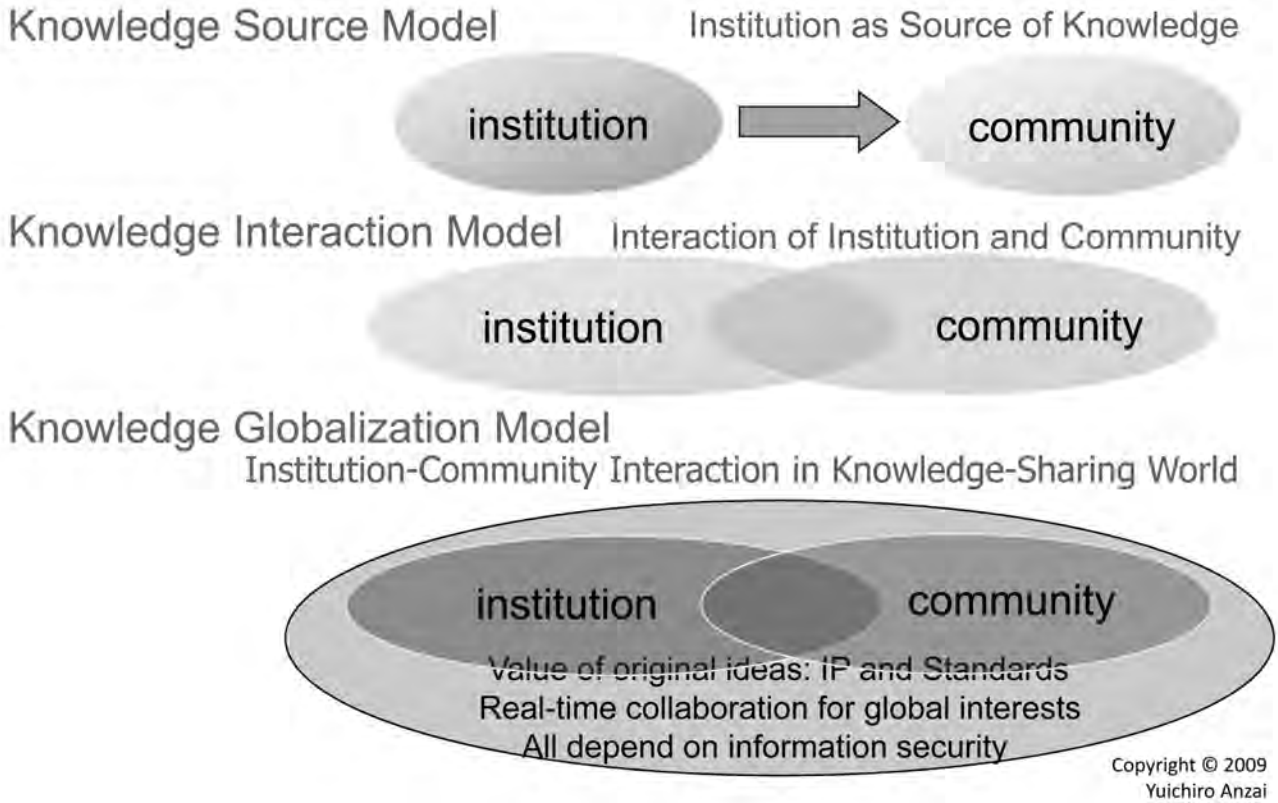
- **Increasing diversity, complexity, and necessity of thoughtful mediation in politics, economy, foreign policy and social systems; nation, ethnicity, language, culture, religion and other (increasing number of) dimensions for diversity and complexity.**
- **Increasing speed and personalizability of communication media.**
- **Increasing size and complexity of databases, or the amount and the structure of knowledge shared globally across borders.**

Change of the World and Higher Learning Environment

- People who think and act independently and collaboratively at the same time.
- Open and real-time communication for understanding each other, and for discovering and solving problems in the world.
- Creation, accumulation and distribution of knowledge logically and semantically robust enough against abuse of information, and spatio-temporally stable enough for peace, sustainability, and prosperity of our globe.

- Needs of learning environment for nurturing people who can be both independent and collaborative.
- Needs of globally distributed infrastructure for global communication and knowledge sharing based on innovative digital communication networks.

Innovation through Institution-Community Collaboration



SOI (School On Internet) Asia

-based on satellite Internet technology

24 Partner Universities in 12 Countries

Thailand
Chulalongkorn University, Asian Institute of Technology, Chulachomklao Royal Military Academy, Prince of Songkla University

Laos
National University of Laos

Myanmar
University of Computer Studies

Indonesia
Brawijaya University, Sam Ratulangi University, Hasanuddin University Kampus Tamalanrea, Institut Teknologi Bandung, Universitas Syiah Kuala

Malaysia
Universiti Sains Malaysia, Asian Institute of Medicine, Science & Technology

Vietnam
Institute of Information Technology

Philippines
Advanced Science and Technology Institute, University San Carlos

Nepal
Tribhuvan University

Cambodia
Institute of Technology of Cambodia

Bangladesh
Bangladesh University of Engineering and Technology

Mongolia
Mongolian University of Science and Technology

Japan
Tohoku University, Tokyo University of Marine Science and Technology, Japan Advanced Institute of Science and Technology, Keio University


Brawijaya University, Indonesia


Hasanuddin University, Indonesia


Sam Ratulangi University, Indonesia


Asian Institute of Technology, Thailand


National University of Laos, Laos


Advanced Science and Technology Institute, Philippines


University of Computer Studies, Yangon, Myanmar


Asian Youth Fellowship, Malaysia


Chulalonkorn University, Thailand


Institut Teknologi Bandung, Indonesia


Institute of Information Technology,, Vietnam


Universiti Sains Malaysia, Malaysia


Mongolian University of Science and Technology, Mongolia


Prince of Songklang University Thailand


Chulachomklao Royal Military Academy Thailand


Keio University Shonan Fujisawa Campus,Japan

Universitas Syiah Kuala, Indonesia

University San Carlos, Philippines


Bangladesh University of Engineering &Technology, Bangladesh


Institute of Technology of Cambodia, Cambodia

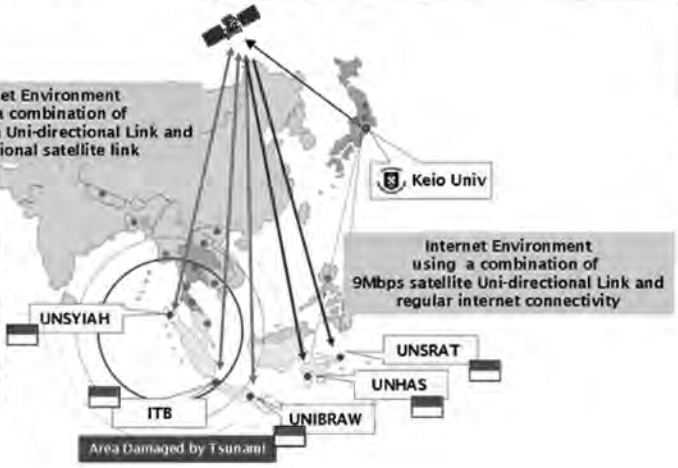

Tribhuvan University, Nepal

Understanding and Solving Real-world Problems at SOI Asia -Tsunami Disaster Recovery Project

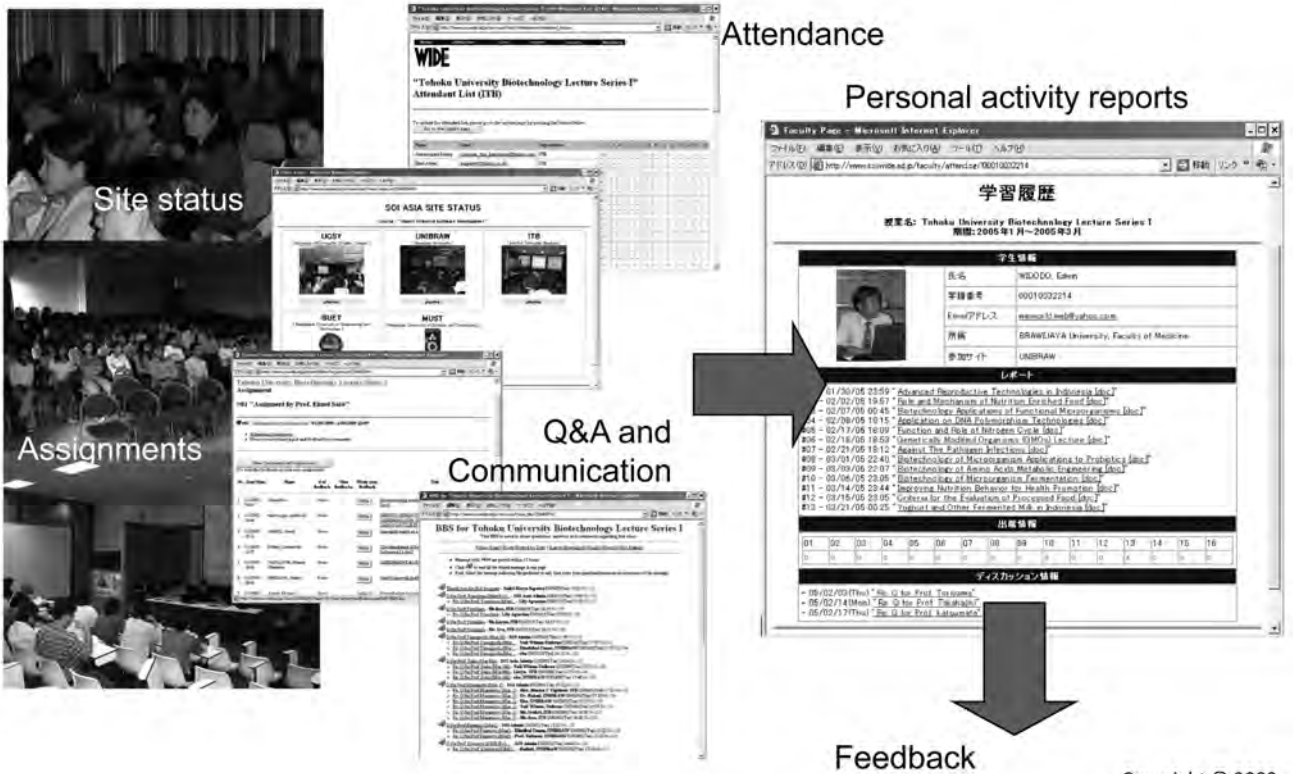
Keio University and SOI Asia assisted Universitas Syiah Kuala, the largest national university in Indonesia, by providing comm. env. for disaster recovery.

Photos by Chermg Talay Subdistrict Administration Office

Tsunami Symposium on SOI Asia network



Remote e-Learning System for SOI Asia



Industry-government-academia Collaboration for SOI Asia

Satellite Internet Infrastructure

Technology Development
Internet via Satellite
JSAT 2006~

総務省 MIC Ministry of Internal Affairs and Communications

SOI Asia Lecture Platform
IBM

Asia IT Training
2004~2005

Satellite Receiver (Product) and UDLR (Standard)

UDcast

Technology Development
Satellite and UDLR
2000~
SONY

総務省 MIC Ministry of Internal Affairs and Communications

MEXT

Content Development for Digital Media for Asia
2006
MEXT Ministry of Education, Culture, Sports, Science and Technology

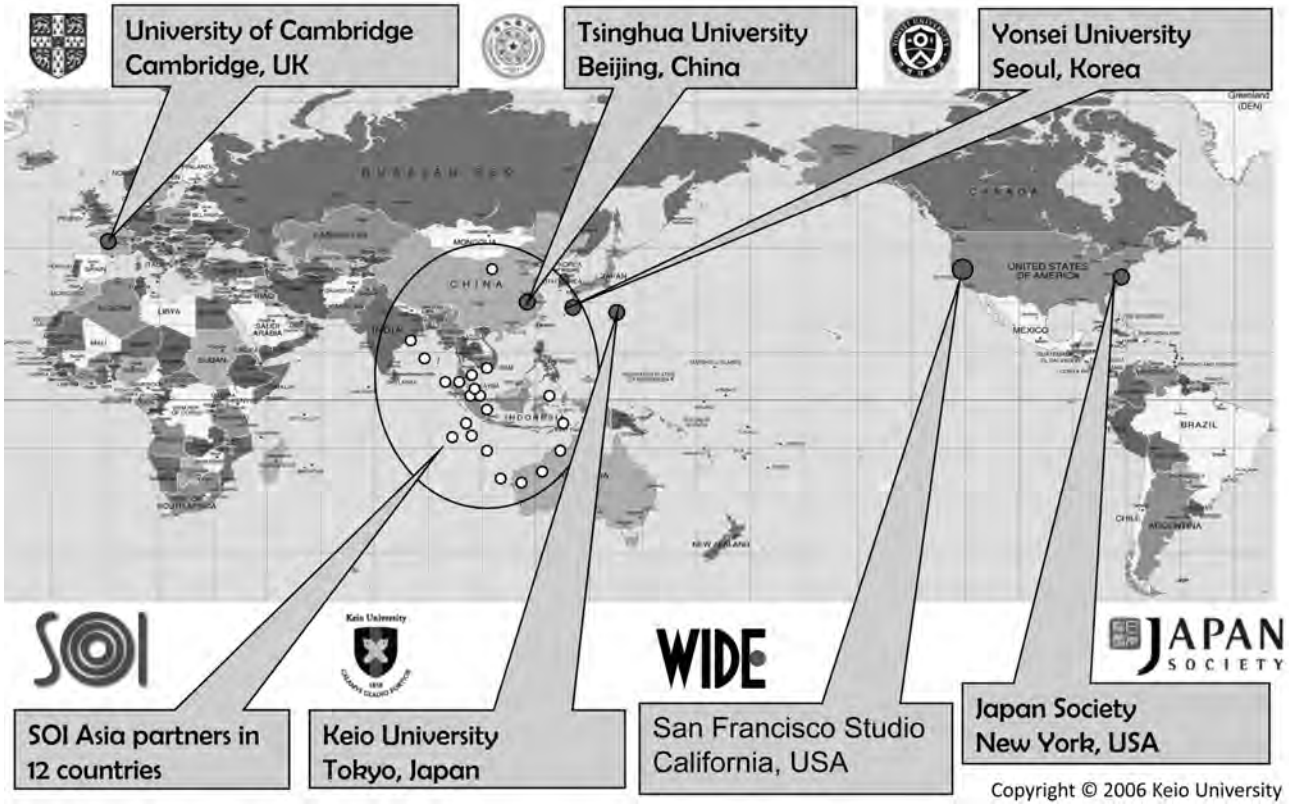
Industry/Government Partners

- Toyota Motor Corp.
- Toshiba Corp.
- NTT DoCoMo, Inc.
- Yokogawa Electric Corp.
- Matsushita Electric Industrial Co. Ltd.
- DENSO Corp.
- Fuji Xerox Co., Ltd.
- Fujitsu Ltd.
- Hitachi Ltd.
- Honda R&D Co., Ltd.
- IBM Japan, Ltd.
- KDDI Corp.
- Microsoft Corp.
- Ministry of Education, Culture, Sports, Science and Technology etc

Operator Training for SOI Asia

Annual SOI Asia Operators Workshop
(in 2005 at Brawijaya University, Indonesia, for the photo)

Global Digital Studios (as of 2006)



What are Global Digital Studios?

- Studios are:
  - ✓ Standardized digital communication spots
  - ✓ With high quality digital video/audio facilities
  - ✓ Located in key places for handling digital content
  - ✓ Connected to each other through a global digital network
  - ✓ Shared by diverse education and research communities
  - ✓ Interoperable since they adhere to the same standard
  - ✓ Autonomously operated by each partner
  - ✓ Registered as shared resources among partners.
- Partner institutions can:
  - ✓ Make use of any/all registered studios for any convenient occasion through very simple procedures.

Examples of Self-operated Global Digital Studios

Studio at Tsinghua University

Studio at Yonsei University

Studio at University of Cambridge

Studio at Japan Society

Studio at Keio University

- ✓ Location: Tokyo, Japan
- ✓ Operated by: Keio University
- ✓ DVTS and Polycom / Multipoint capable
- ✓ IPv4/IPv6
- ✓ Re-constructed in February 2006

Global Digital Studios Provide Excellent Opportunities

Creation and Distribution of Contextual Digital Content

✓ **Digital content with context, such as real-time images, video clips, audio tapes, movie programs, animation programs, sport, music, performances, scientific experiments or other scenes, books, journals, reports or other edited pages of documents, a series of digitalized pictures or photographs, promotion videos for universities, industries, governments, and so on.**

Knowledge Sharing in the Global Community

✓ **Contextual digital content could constitute an enormous portion of our body of knowledge, to be shared & used for many purposes in global & local communities.**

Research and Development

✓ **How to create, store, send, distribute, share, retrieve, edit, use, & profit from contextual digital content in a global community is an open & challenging issue for R&D in media technology, human-machine interaction, knowledge handling, business management, financing, legal systems & others.**

Benefits for Society

✓ **Industries for contextual digital content are generally labor-intensive and/or cost-inefficient; better technologies & management will produce greater benefits for society.**

Human Resources

✓ **There are very few professionals in universities, industries or governments who can design and manage contextual digital content and its large-scale platforms. Thus, universities need to take a decisive role.**

Intellectual Property Rights and Standards related to Global Knowledge Sharing

✓Copyright Protection & Promotion of Distribution

- ✓Encouraging the improvement and clarification of contractual practices in business and academia
- ✓Supporting the development of content protection schemes

✓More control over copyright infringement

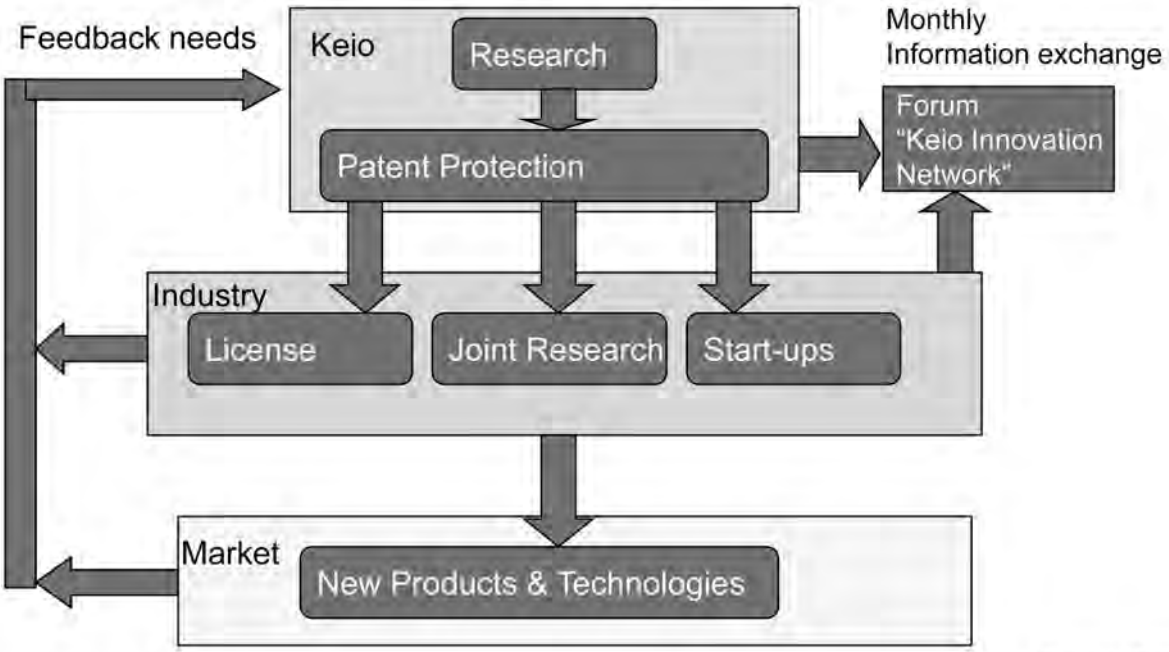
- ✓Establishment of a legal framework for dealing with trans-border copyright infringements
- ✓Stricter control over P2P-based infringements

✓Proactive efforts for international standardization

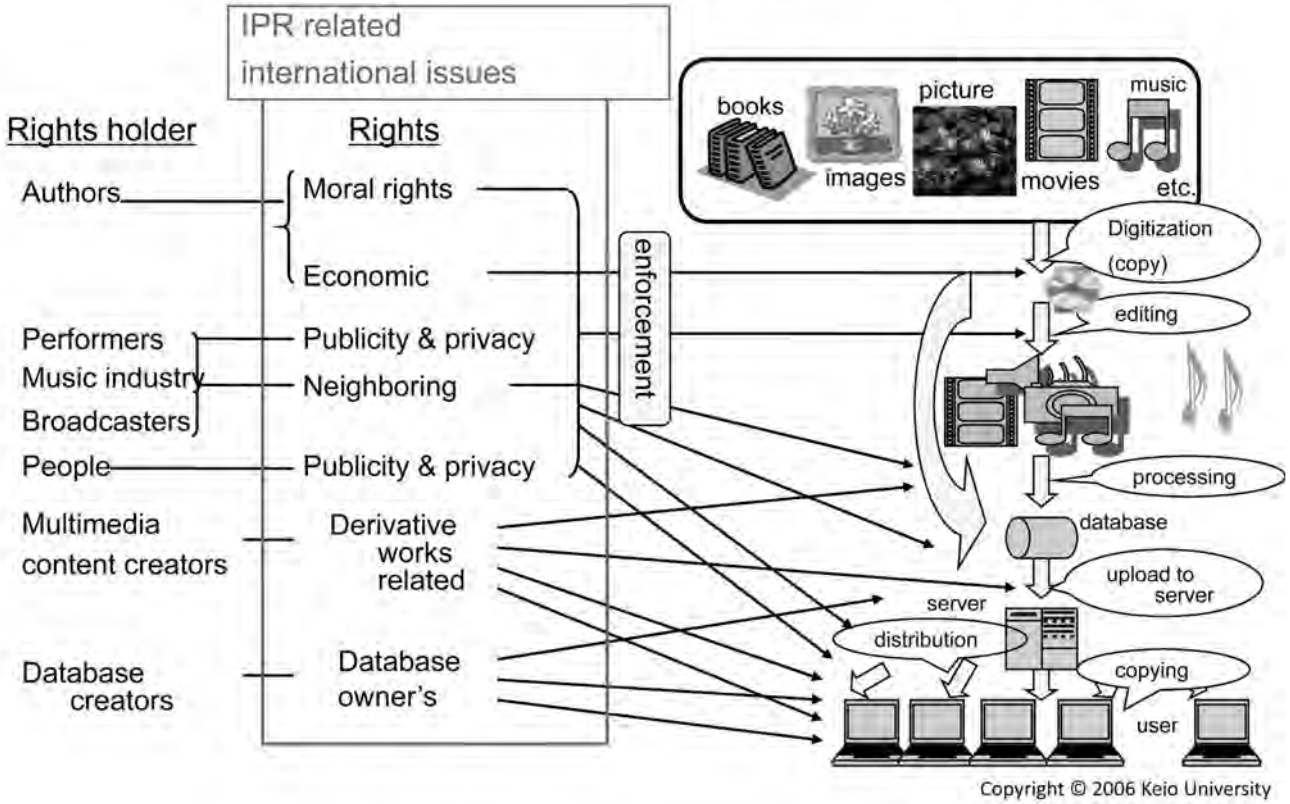
- ✓Improving awareness of the importance of standardization, including training of standardization specialists
- ✓Promoting collaborative research for the establishment of international standards

Intellectual Property Center at Keio University

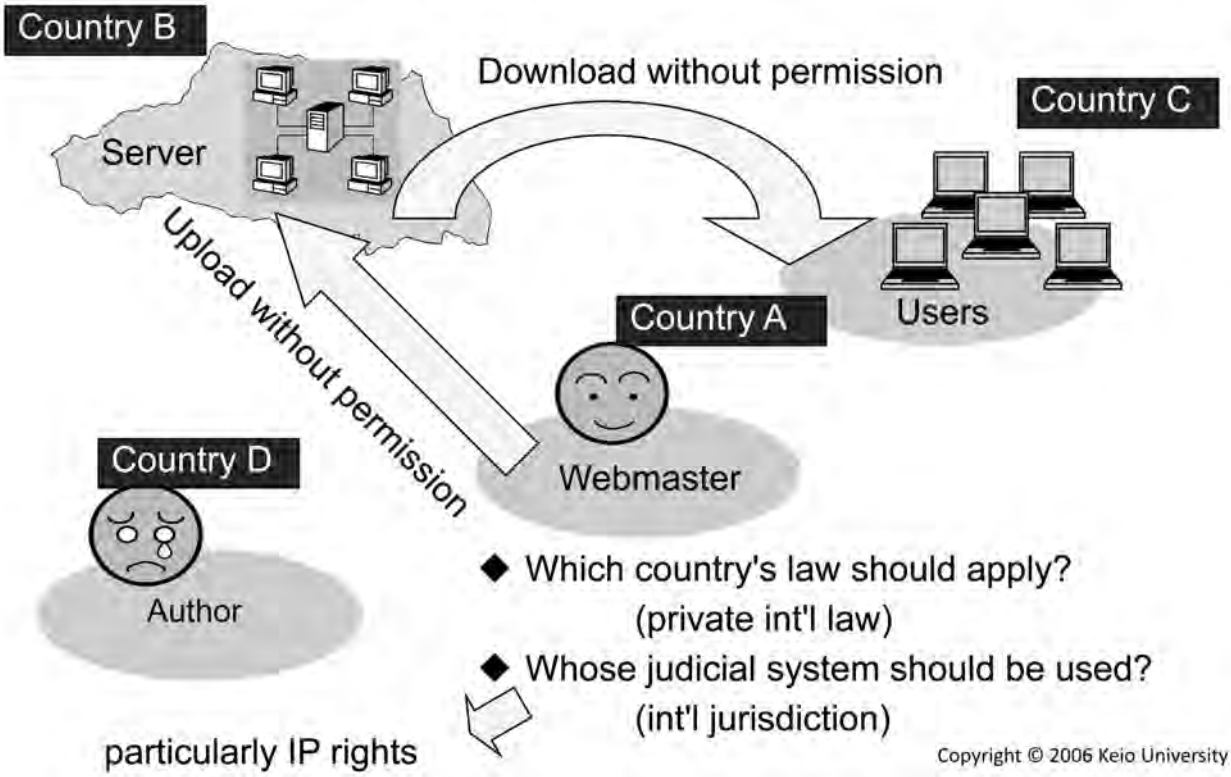
Key Mission: to convert "research results" to commercial products & technologies in order to disseminate Keio's knowledge to the public



IPR related International Issues



IPR related International Issues: An Example



- Which country's law should apply? (private int'l law)
- Whose judicial system should be used? (int'l jurisdiction)

particularly IP rights

Contribution to International Standardization: An Example

Contribution to International Digital Cinema Standard

- ✓ Approved as an international standard by DCI (Digital Cinema Initiative)
- ✓ Newest system adopting JPEG2000
- ✓ Can deliver hi-res Digital Cinema imagery (3840x2048)

4K Digital Cinema "Birthday Cake"

Content Industries and Content Management Policy

Content Industries and Content Management Policy

Different types of content go digital in different ways

- ✓**Text and Picture**
  - ✓**Text**
  - ✓**Picture**
  - ✓**Photo**
  - ✓**2D- and 3D- graphics**
- ✓**Sound**
  - ✓**Music**
  - ✓**Speech**
  - ✓**Lecture**
  - ✓**e-Learning text**
- ✓**Motion Picture**
  - ✓**Movie**
  - ✓**Video**
  - ✓**2D- and 3D-graphics**
  - ✓**e-Learning Content**
  - ✓**News**
  - ✓**Drama**
  - ✓**Animation**
- ✓**Multimedia Title**
  - ✓**TV Game**
  - ✓**Encyclopedia, Almanac**
  - ✓**Virtual Environment**

Issues in Global Knowledge Sharing: Examples

- Regulation against sending moving images **with pictures and sounds** for remote education
- Regulation against heavily repeated use **of commercial videos/films** for educational purposes
- Rapid shift to oligopolization **of copyrights and publication rights for academic products**
- Difficulty in cooperation **with content industries**
- Difficulty in coping with heavy load **to digitize paper and film products**
- Underdevelopment of secured global communication networks **with reasonable cost**
- Underdevelopment of international and domestic laws **for copyright, publication right, and distribution of information**
- Underdevelopment of protection systems **for information security**
- Difficulty in standardization **of formats and handling procedures for to-be-globally-shared materials**
- **Others**

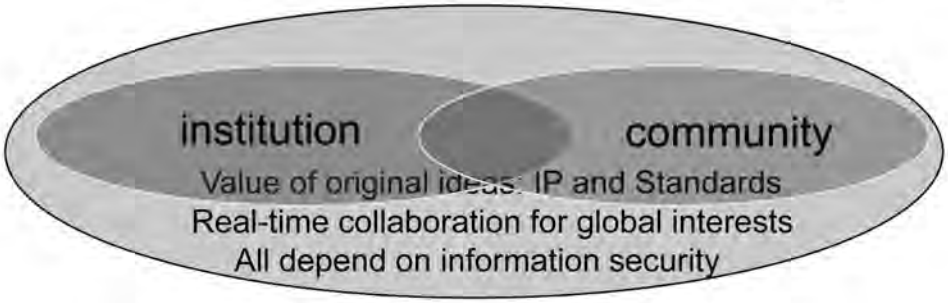
Global Knowledge Sharing: Roles of E&R Institutions

Knowledge Source Model — Institution as Source of Knowledge

Knowledge Interaction Model — Interaction of Institution and Community

Knowledge Globalization Model

Institution-Community Interaction in Knowledge-Sharing World



- **Respect for Values of Originality and Creativity**
- **Nurturing Humans with Global Knowledge, Wisdom and Sincerity**
- **Globally Significant Academic Production and Archiving**
- **Social Innovation and Contribution to Global/Local Societies**
- **Collaboration for Solving Global/Local Issues**

講　演

International Research Cooperation

– Chances and Challenges

Iris Wieczorek（ドイツ研究協会東京事務所 代表）

Dr. Iris WIECZOREK

Since February 2009 director of the Japan Office of the German Research Foundation (DFG).

Born 1967 in Hamburg, Germany.

She studied Japanese and Chinese Studies, and Computer Science at the University of Hamburg. After taking her doctoral degree at the University of Hamburg, she worked from 2000 to 2008 as a research fellow at the GIGA Institute of Asian Studies in Hamburg and as a research management officer since 2005. During her graduate and doctoral studies, she lived in Japan for several years.

Her major research interests were innovation processes and networks in the Japanese economy and society, social movements, the relationship between politics and religion in Japan in international comparison. She published numerous papers on the Japanese innovation system in international comparison. She is co-editor of the Yearbook *Japan – Wirtschaft, Politik und Gesellschaft* [economy, politics and society]

E-Mail: iris.wieczorek@dfg.de, *Website:* www.dfg.de

International Research Cooperation
Chances and Challenges

Dr. Iris WIECZOREK, Director DFG Office Japan
Tokyo, September 30, 2009

DFG

DFG: Who we are and what we do

- The Central **public funding organization** for academic research in Germany
- **Self-governing body** of science and research in Germany
- Promoting academic **excellence** on a competitive basis
- **Buttom-up** approach
- (application-oriented) **basic research**
- Serving science and the arts in **all fields**
- Advisory activities in **politics**
- Special focus on supporting **young researchers**
- Promoting **international** research cooperation
- Fostering links between **science and industry**

Dr. Iris WIECZOREK, Director DFG Office Japan
Tokyo, September 30, 2009

DFG

DFG budget

Annual Budget : 2,1 billion Euro

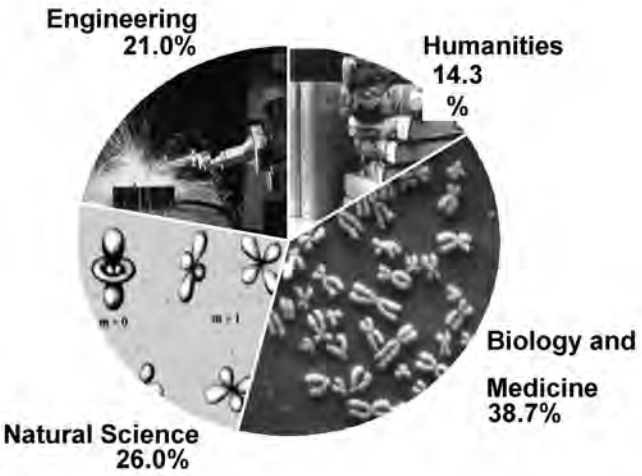
Sources of Funding

58% Federal States (Bund),

41% States (Länder), 0,4% Others

Funding Volume (2008)

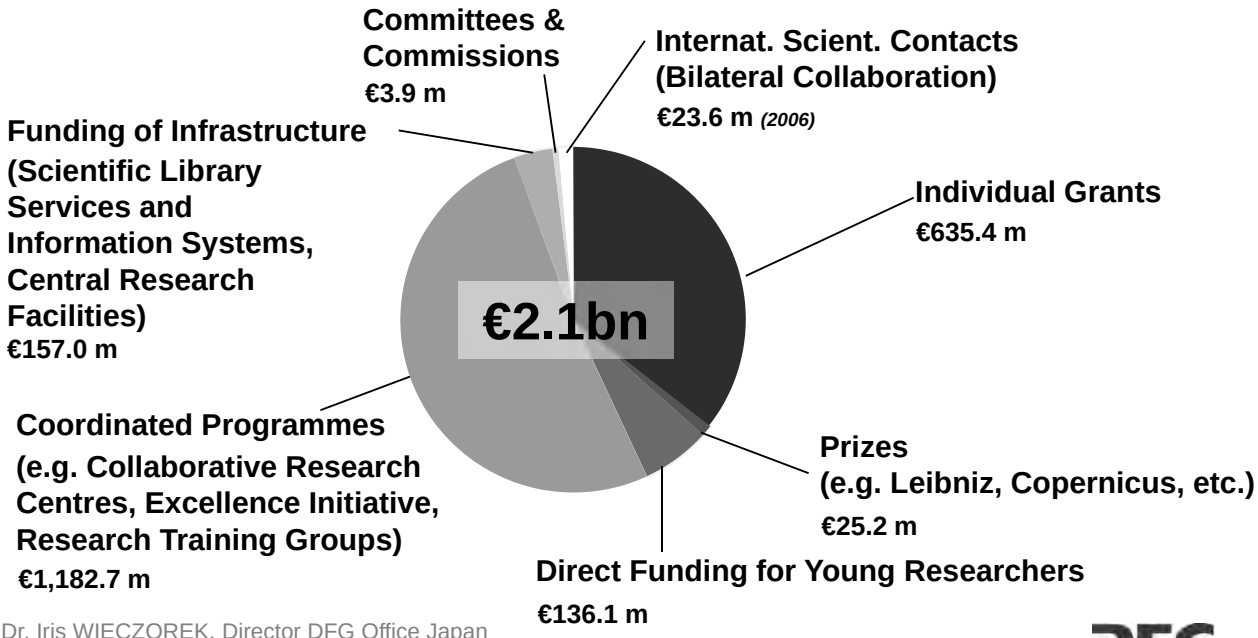
- Nearly 1.000 running programmes
- More than 20.000 projects funded



Dr. Iris WIECZOREK, Director DFG Office Japan
Tokyo, September 30, 2009

DFG

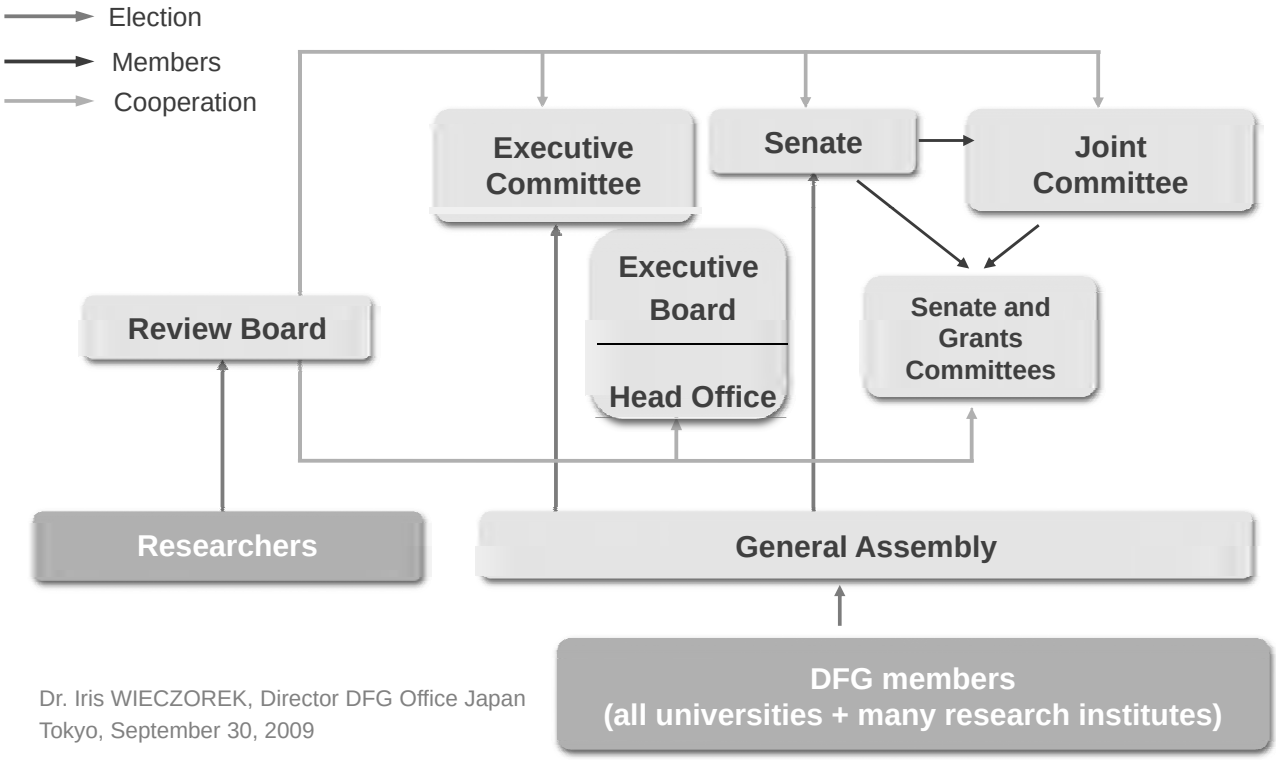
DFG Procedures and Programmes - Approvals 2007



Dr. Iris WIECZOREK, Director DFG Office Japan
Tokyo, September 30, 2009

DFG

DFG Structure and Decision making bodies



Dr. Iris WIECZOREK, Director DFG Office Japan
Tokyo, September 30, 2009

International Strategy of DFG

Supporting

- **international cooperation and activities of single researchers or whole groups of researchers**

by

- **opening all DFG programmes for international cooperation**
- **programmes with an international focus (International Research Training Groups, etc.)**
- **agreements with partner organisations, specific thematic calls (to meet demand of scientific community)**

Dr. Iris WIECZOREK, Director DFG Office Japan
Tokyo, September 30, 2009

DFG

The International DFG: Offices Abroad

Sino-German Centre
for Science Promotion
Beijing, 2000

US Liaison Offices
Washington DC, 2002
New York, 2007

Russian
Liaison Office
Moskow, 2003

Indian
Liaison Office
New Delhi, 2006

Japan
Liaison Office,
Tokyo, April 2009

Dr. Iris WIECZOREK, Director DFG Office Japan
Tokyo, September 30, 2009

DFG

What we do in Japan

- **promoting scientific collaboration; initiation of collaborative projects**
- **building an extensive network of personal and professional links**
- **contact for scientists, scientific organizations and funding bodies in Japan**
- **development of a "win-win cooperation philosophy"**
- **organizing and conducting bilateral symposia**
- **visibility & information**
  (analysis of developments of the Japanese and German Innovation System; serve as information centres)

Dr. Iris WIECZOREK, Director DFG Office Japan
Tokyo, September 30, 2009

DFG

DFG´s Japanese Partners

Japan Society for the Promotion of Science (JSPS)

- **Memorandum of Understanding on German-Japanese Graduate Externship – International Research Training Groups (2005)**
- **JSPS liasion office in Bonn** http://www.jsps-bonn.de

Programme and Application Requirements

- **Preparatory visits**
- **Joint research projects**
- **Joint seminars**

Japan Science and Technology Agency (JST)

- Joint funding scheme for the research field of **"Nanoelectronics„**
- **Joint application**, to be handed in both to DFG and JST in parallel
- **Memorandum of Understanding on Joint Research Program (15th April 2009)**

Dr. Iris WIECZOREK, Director DFG Office Japan
Tokyo, September 30, 2009

DFG

Funding Chain: Programmes for different career stages

studies	doctorate	postdoc	qualifying as a research group leader	qualifying as a professor	establishing yourself as a professor
			Emmy Noether-programme		Leader, KFO/ FOR-professor
			young investigator‘s group FOR/SFB	Heisenberg-fellowship	Heisenberg-professorship
	fellowship in research training group	research fellowship	research fellowship	research fellowship	
	position in research training group	one‘s own position (Germany)	one‘s own position (Germany)		
summer students in DFG-projects	researcher employed in DFG-project	researcher employed in DFG-project	researcher employed in DFG-project	researcher employed in DFG-project	

Dr. Iris WIECZOREK, Director DFG Office Japan
Tokyo, September 30, 2009

DFG

Thank you for your attention

for further information

- DFG: **www.dfg.de**, DFG Office Japan**:** **www.dfg.de/japan**, **japan@dfg.de**
- funded projects: www.dfg.de/**gepris/**
- Research institutions: www.dfg.de/**research_explorer/**

Dr. Iris WIECZOREK, Director DFG Office Japan
Tokyo, September 30, 2009

DFG

研　究
紹　介

i-Japan & ICT Trust

渡辺　克也（総務省総合通信基盤局電波政策課長・国立情報学研究所 客員教授）

Global Lab（グローバルラボ）3D インターネットに基づいた参加型科学の基盤

Helmut Prendinger（国立情報学研究所 准教授）

情報セキュリティに対する経済学的接近

竹村　敏彦（関西大学ソシオネットワーク戦略研究機構 助教）

a) Database Forensics
b) Pseudonymization of Health Data

Johannes Heurix（オーストリア・セキュアビジネスセンター 研究員）

Research on Re-shooting Countermeasures

越前　　功（国立情報学研究所 准教授）

Privacy in e-Health

Sven Wohlgemuth（国立情報学研究所 研究員）

i-Japan & ICT Trust

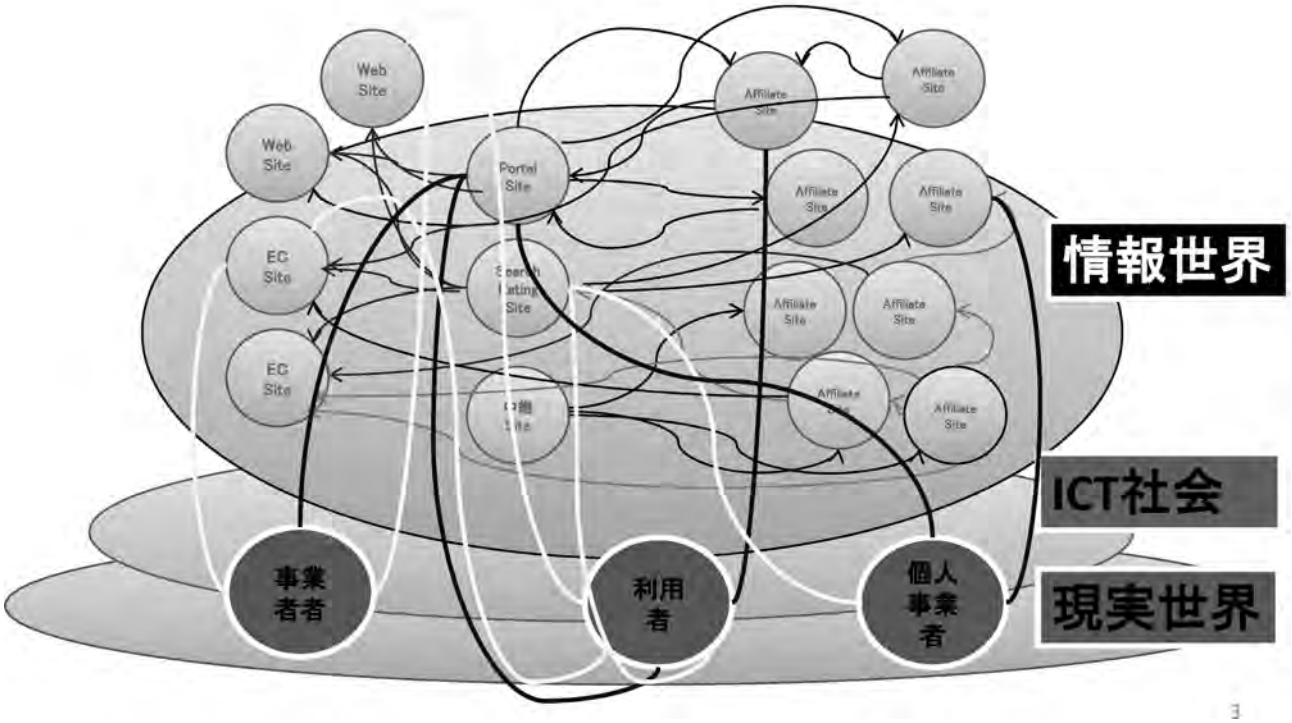
Katsuya WATANABE

Director, Radio Policy Division, Radio Department,
Telecommunications Bureau (TB),
Ministry of Internal Affairs and Communications (MIC)
Visiting Professor, National Institute Informatics(NII)

1984 Graduate of Keio University
Majored in Electronic Engineering with a Bachelor Degree
1984 Joined the Ministry of Posts and Telecommunications
2001 Director of Research & Development Office,
Information & Communications Policy Bureau, MIC
2003 Executive Director for Strategic Planning,
Communications Research Laboratory(CRL)
2004 Managing Director for Strategic Planning,
National Institute of Information & Communications Technology(NICT)
2005 Director of Telecommunication Systems Division, TB, MIC
2007 Director of Land Mobile Communications Division, TB, MIC
2008-present Director of Radio Policy Division, TB, MIC

2006-present Visiting Professor, NII

情報世界と現実世界を紐付けるICT Trust



ICT Trustへの政策課題

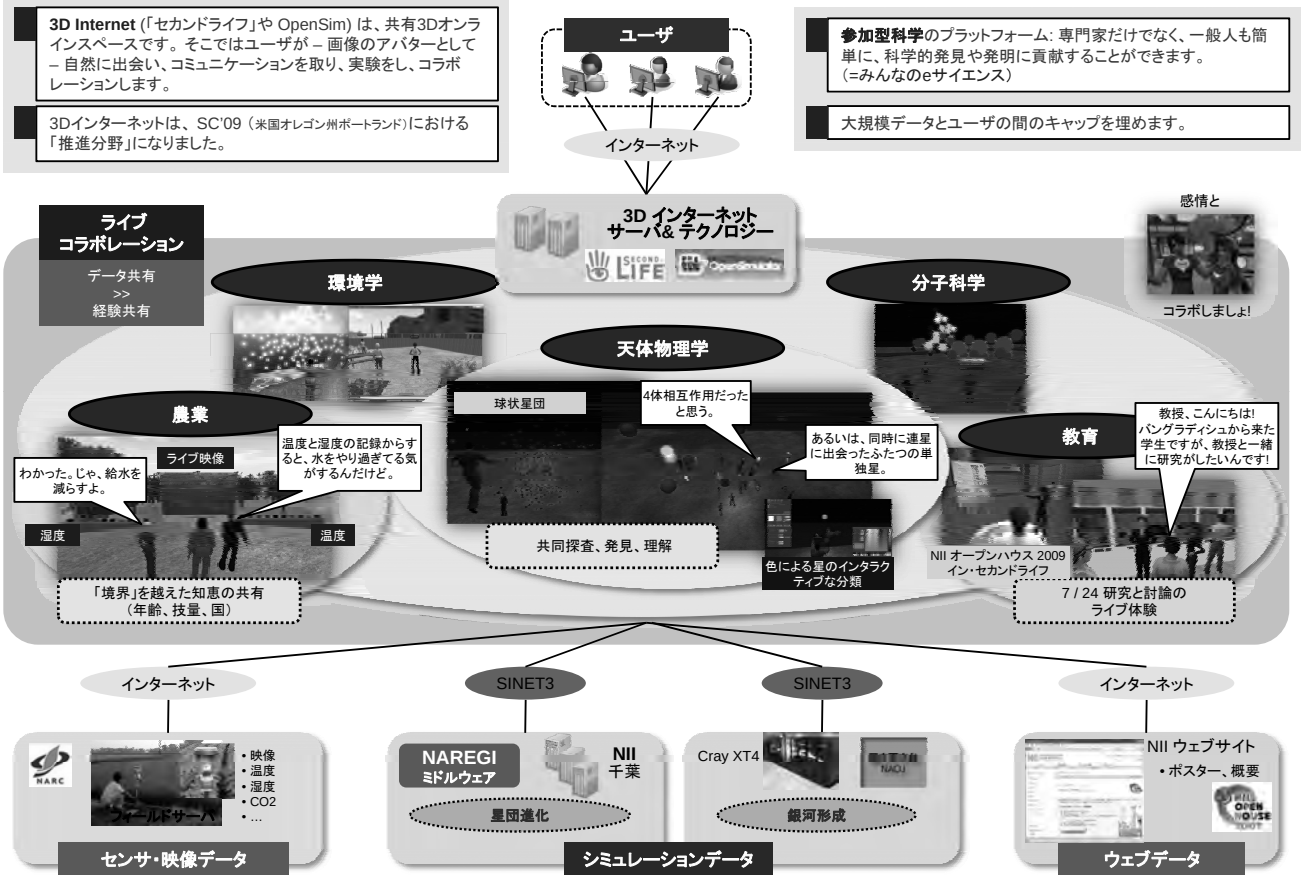
	社会への影響	新たな研究への取組	新たな制度による枠組み
○技術と市場	・情報の量の爆発的増加 ・知識サービス産業、知的情報産業へのシフト傾向	・ICTメタデータ流通プラットフォーム整備 ・メタデータ・アライアンス ・情報量爆発問題に対応できる技術の開発	・知的財産権侵害問題 ・デジタル著作権問題 ・デジタル権利のライフサイクル管理 ・流通秩序や制度設計
○情報信頼性基盤 （量から質へのパラダイムシフト） （リアルスペースとサイバースペース）	・ロボットやセンサーなど、ネットにつながる端末が桁違いに爆発 ・個人情報漏えい、ネット詐欺問題に対する不安	・情報の真贋鑑定の困難性 ・信頼のコミュニケーションモデル ・情報の収集、信頼性の分析と評価 ・信頼関係の形成、伝達、確認のメカニズム ・ネットワーク上におけるフェイス・トゥ・フェイスの情報交換	・情報信頼性の義務と責任に関する社会規範、法制度、公共政策 ・情報トラストマーク ・社会の規範、法制度、技術、市場 ・サイバースペース法
○技術と社会の調和政策 ○技術と文化の共創社会	・脱ICT社会、ポストICT社会	・サイバー・イノベーション・インフラの整備 ・情報文化力の計量学 ・技術と文化の相互作用メカニズムの解明 ・文化遺産から産業資産アーカイブの構築	・新たな社会産学連携の枠組みによる知流革命の推進 ・情報文化力戦略の提言と情報文化法制度の構築

3Dインターネットの参加型科学&コラボレーション – ライブ!

ヘルムト・プレンディンガー

3D Internet (「セカンドライフ」や OpenSim) は、共有3Dオンラインスペースです。そこではユーザが – 画像のアバターとして – 自然に出会い、コミュニケーションを取り、実験をし、コラボレーションします。

3Dインターネットは、SC'09 (米国オレゴン州ポートランド) における「推進分野」になりました。

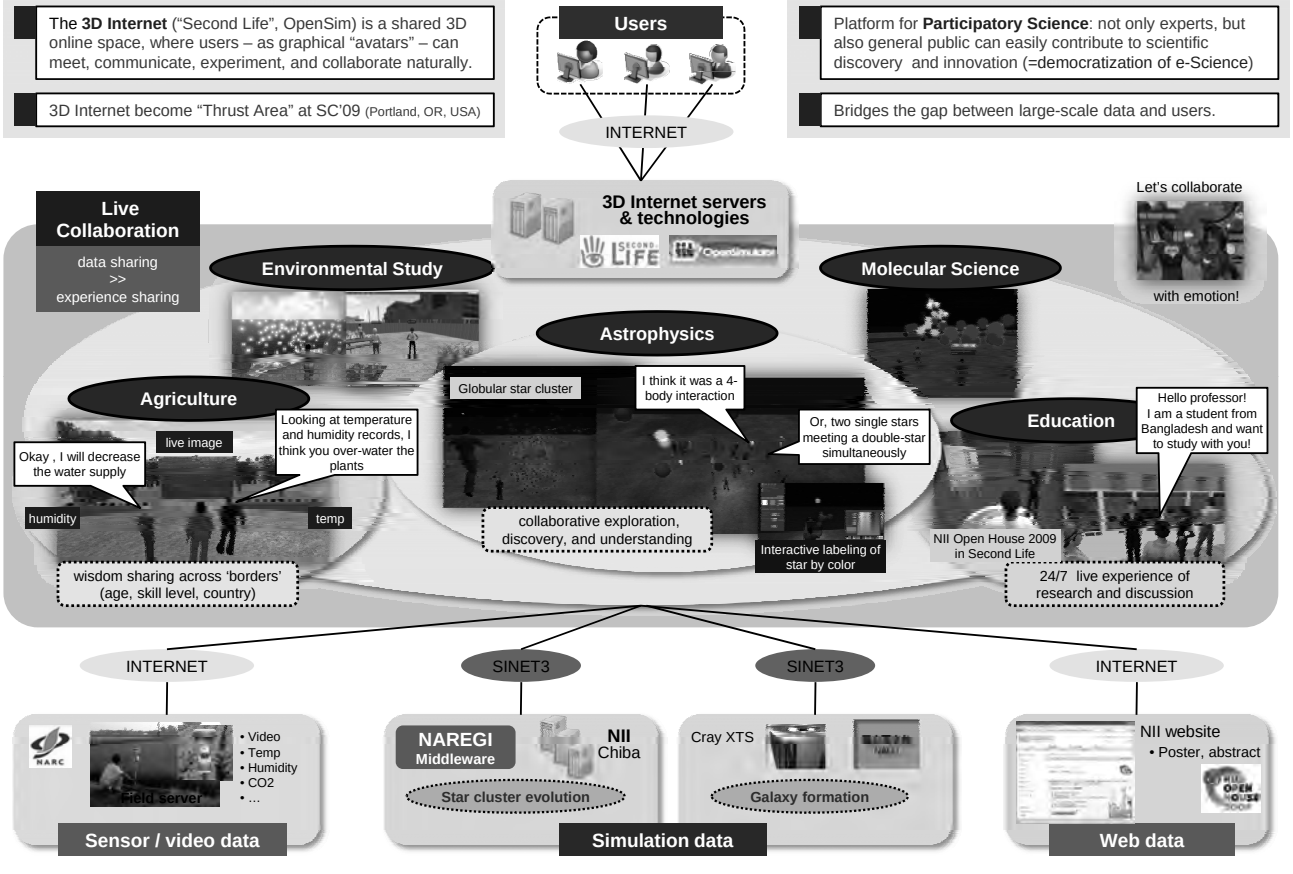


Participatory Science & Collaboration in the 3D Internet – Live!

by Helmut Prendinger

The **3D Internet** ("Second Life", OpenSim) is a shared 3D online space, where users – as graphical "avatars" – can meet, communicate, experiment, and collaborate naturally.

3D Internet become "Thrust Area" at SC'09 (Portland, OR, USA)



RISS

An Economic Approach to Issues on the Information Security

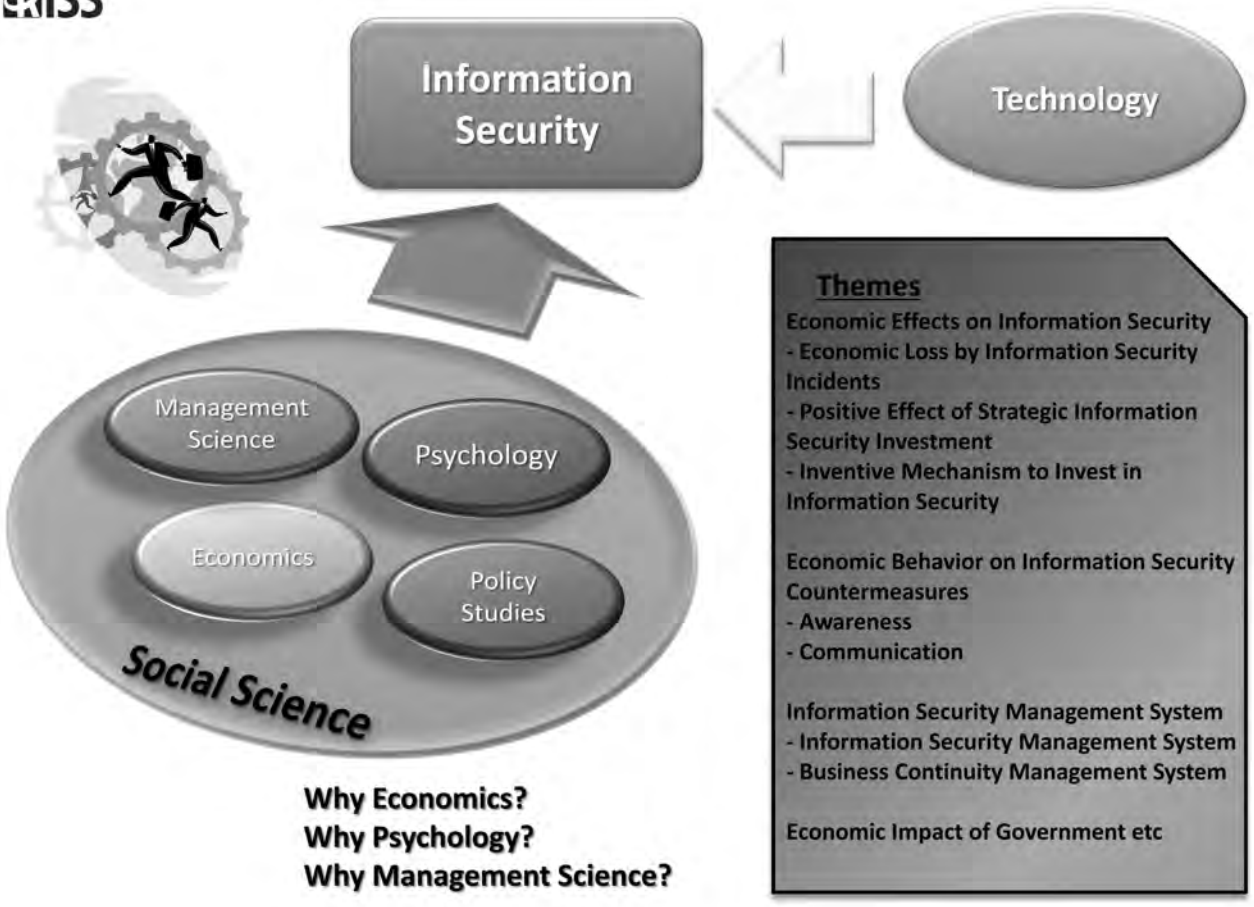
Toshihiko Takemura, Ph.D., Assistant Professor
The Research Institute for Socionetwork Strategies
takemura@rcss.kansai-u.ac.jp
http://www.rcss.kansai-u.ac.jp/~takemura/

ABSTRACT
In this work, from the viewpoint of economics, the author analyzes the interrelationship between information security countermeasures and economic activities by statistical methods. The sophisticated micro data set in this work, which includes countermeasures, (psychological) awareness on information security and various other attributes, is collected through a Web-based survey that uses sophisticated social investigation methods.

Takemura, T. (2009) "An Economic Approach to Issues on the Information Security" RCSS Discussion Paper, No.86
[URL: http://www.rcss.kansai-u.ac.jp/DPS/DPS_E.html]

THINK × ACT KANSAI UNIVERSITY

RISS



RISS

Stream of Research by Takemura Group (RISS) on Economic Aspects of Information Security

- Ukai, Y., Takemura, T. (2007) "Spam Mails Impede Economic Growth" The Review of Socionetwork Strategies, Vol.1, pp14-22
- Takemura, T. (2007) "Proposal of information security policy in telecommunication infrastructure" In: What is Socionetwork Strategies, Murata, T. & Watanabe, S. (Eds.), pp.103-127, Taga-shuppan, Tokyo (in Japanese)
- Nagaoka, H., Takemura, T. (2007) A Business Continuity Plan to Heighten Enterprise Value, Proceedings of 55th National Conference, pp.149-152 (in Japanese)
- Takemura, T., Ebara, H. (2008) "Economic Losses Caused by Spam Mails in Japan" Journal of International Development, Vol.8(1), pp.23-33
- Takemura, T., Osajima, M. (2008) "About Some Topics on Countermeasures and Policies for Information Security Incidents in Japan" GITI Research Bulletin 2007-2008 (Waseda University), pp.163-168
- Takemura, T., Ebara, H. (2008) "Economic Loss Caused by Spam Mail in Each Japanese Industry" Selected Proceedings of the First International Conference on Social Sciences (Social Sciences Research Society), Vol.3, pp.29-42
- Takemura, T., Osajima, M., Kawano, M. (2008) "Positive Analysis on Vulnerability, Information Security Incidents, and the Countermeasures of Japanese Internet Service Providers" World Academic of Science, Engineering and Technology, Vol.46, pp.688-695
- Takemura, T., Minetaki, K. (2009) "The Policies for Strategic Information Security Countermeasures Improving the Market Value" The Proceedings of 66th Conference on Japan Economic Policy Association (in Japanese)
- Takemura, T., Minetaki, K., Imagawa, T. (2009) "A Research on Worker's Awareness to Information Security" RCSS Discussion Paper, No.85 (in Japanese)
- Takemura, T.,Umino, A. (2009) "A Research on the Internet Users' Awareness to the Information Security" Telecom Journal, August 2009, pp.13-21 (in Japanese)
- Takemura, T., Minetaki, K. (2009) "An Empirical Analysis on Information Security Countermeasures" The 2nd International Conference of Social Science, Izmir, Turkey, 2009
- Takemura, T., Umino, A., Osajima, M. (2009) "Variance of Analysis on Internet Users' Awareness to Information Security" GITI Research Bulletin 2008-2009 (Waseda University), forthcoming
- Takemura, T., Minetaki, K. (2009) "An Empirical Study on the Effects of Information Security Countermeasures" The 6th Annual Forum on Financial Information Systems and Cybersecurity, Maryland, USA, October, 2009, forthcoming
- Takemura, T. (2009) "A Quantitative Study on Workers' Awareness to Information Security Using the Data Collected by Web-based Survey" The 2009 annual conference of the Applied Business and Entrepreneurship Association International, Hawaii, USA, November, 2009, forthcoming

http://www.rcss.kansai-u.ac.jp/~takemura/

RISS

Summary

Framework

Results & Implication

Economic Model & Statistical Analysis
- Economic Behavior

Data Collection
- Web-based Survey

The Research Institute for Socionetwork Strategies, Kansai University
- Database for Joint Usage/Research
http://www.kansai-u.ac.jp/riss/

Finding

- There are positive relationships between the expected effects and some management countermeasures on information security such as information sharing and education
- Human resources and information sharing are the important two factors regarding the security system in the firm
- Workers' awareness of information security is different in its attributes such as organizational attributes and the education about information security countermeasures

.....

A Keyword is "Education"

THINK × ACT
KANSAI UNIVERSITY

[SECURE] Business Austria
Science for better Security.

www.securityresearch.at

Database Forensics

Edgar Weippl
eweippl@securityresearch.at

Presented by Johannes Heurix
jheurix@securityresearch.at

Secure Business Austria

ISSI2009, NII

Introduction

[SECURE] Business Austria
Science for better Security.

www.securityresearch.at

- Importance of database forensics
  - –Critical/sensitive information stored in databases, e.g. bank account data, health data
  - –Loss caused by security incidents, corporate governance
- Aims of database forensics
  - –To find out what happened when
  - –To revert any unauthorized data manipulation operations
- Things to consider
  - –How to gain access to the system
  - –Live vs. dead system
  - –Integrity
  - –Images
  - –Data encryption
  - –Goal

[2]

Information Sources

[SECURE] Business Austria
Science for better Security.

- Files
  - MAC - (last) Modified time, Access time, Change/Create time (file attributes)
  - Timeline analysis
- Internal structures
  - SQL Server artifacts: data cache, plan cache, VLF, error logs, ….
  - Forensic tools (e.g. Windows Forensic Toolchest), automated scripts
  - Volatility, file locks
- Logical structures (index)
  - B-trees
  - Different trees for different node entry sequences

[3]

System breach suspected. What now?

[SECURE] Business Austria
Science for better Security.

- Find out if system was actually breached
  - Error logs – failed logins

```
2007-03-02 07:39:10.20 Logon       Error: 18456, Severity: 14, State: 8.
2007-03-02 07:39:10.20 Logon       Login failed for user 'sa'. [CLIENT: 192.168.1.20]
2007-03-02 07:39:10.40 Logon       Error: 18456, Severity: 14, State: 8.
2007-03-02 07:39:10.40 Logon       Login failed for user 'sa'. [CLIENT: 192.168.1.20]
2007-03-02 07:39:10.60 Logon       Error: 18456, Severity: 14, State: 8.
2007-03-02 07:39:10.60 Logon       Login failed for user 'sa'. [CLIENT: 192.168.1.20]
2007-03-02 07:39:10.80 Logon       Error: 18456, Severity: 14, State: 8.
2007-03-02 07:39:10.80 Logon       Login failed for user 'sa'. [CLIENT: 192.168.1.20]
2007-03-02 07:39:11.00 Logon       Error: 18456, Severity: 14, State: 8.
2007-03-02 07:39:11.00 Logon       Login failed for user 'sa'. [CLIENT: 192.168.1.20]
2007-03-02 07:39:11.20 Logon       Error: 18456, Severity: 14, State: 8.
2007-03-02 07:39:11.20 Logon       Login failed for user 'sa'. [CLIENT: 192.168.1.20]
2007-03-02 07:53:07.39 Logon       Login succeeded for user 'sa'. Connection: non-trusted. [CLIENT: 192.168.1.20]
```

  - Plan cache – UNION, single quotes (‘), double dashes (--)

```
SELECT * FROM ORDERS WHERE FirstName = '' UNION ALL SELECT 6666,  name, 'text', 'text',
'text', 'text', 'text', 'text','text', 'text', 'text', 'text'  from sys.sysobjects
WHERE xtype = 'U'
```

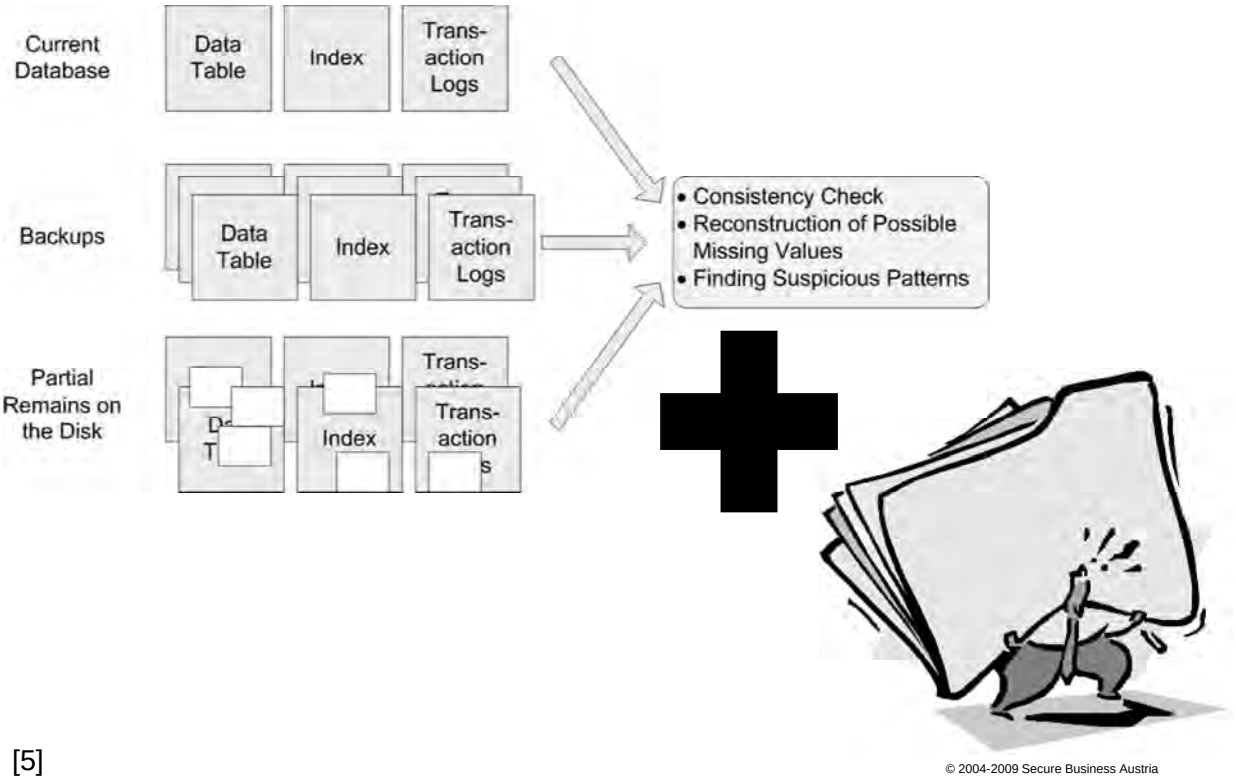
- Find out which data records were retrieved
  - Data cache – recently accessed data pages
  - Plan cache – cached database statements
  - Server state – most recently executed statement by session

Source: Kevvie Fowler – SQL Server Forensic Analysis, Addison-Wesley

[4]

Ongoing Research

[SECURE] Business Austria
Science for better Security.



[5]

[SECURE] Business Austria
Science for better Security.

Pseudonymization of Health Data

Thomas Neubauer
tneubauer@securityresearch.at

Johannes Heurix
jheurix@securityresearch.at

Secure Business Austria

ISSI2009, NII

www.securityresearch.at

Motivation

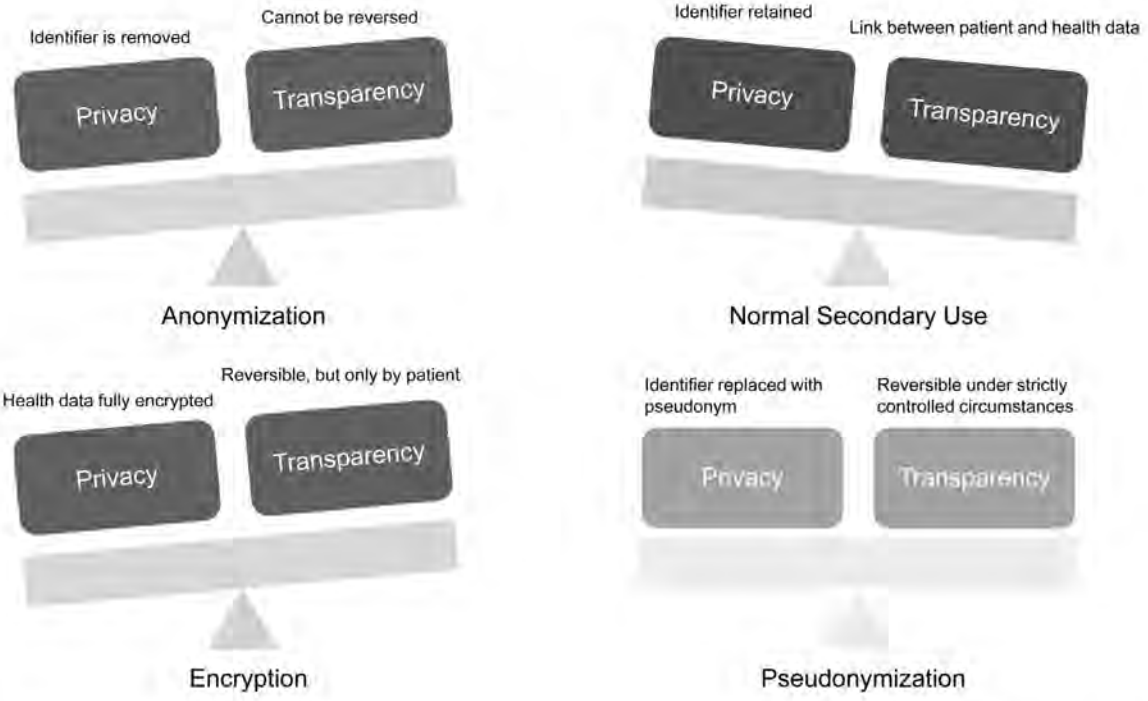
[SECURE] Business Austria
Science for better Security.

- Privacy is one of the fundamental issues in health care today, especially when digitizing medical data
  - Electronic health records (EHR) improve communication between health care providers
- With interconnected systems comes highly sensitive and personal information whose disclosure may cause serious problems for the individual
  - Insurance companies denying health coverage
  - Employers denying employment
- Laws for the protection of privacy
  - Health Insurance Portability and Accountability Act (HIPAA)
  - European Directive 95/46/EC
- Secondary use of medical data in clinical studies

[7]

Trade Off - Secondary Use

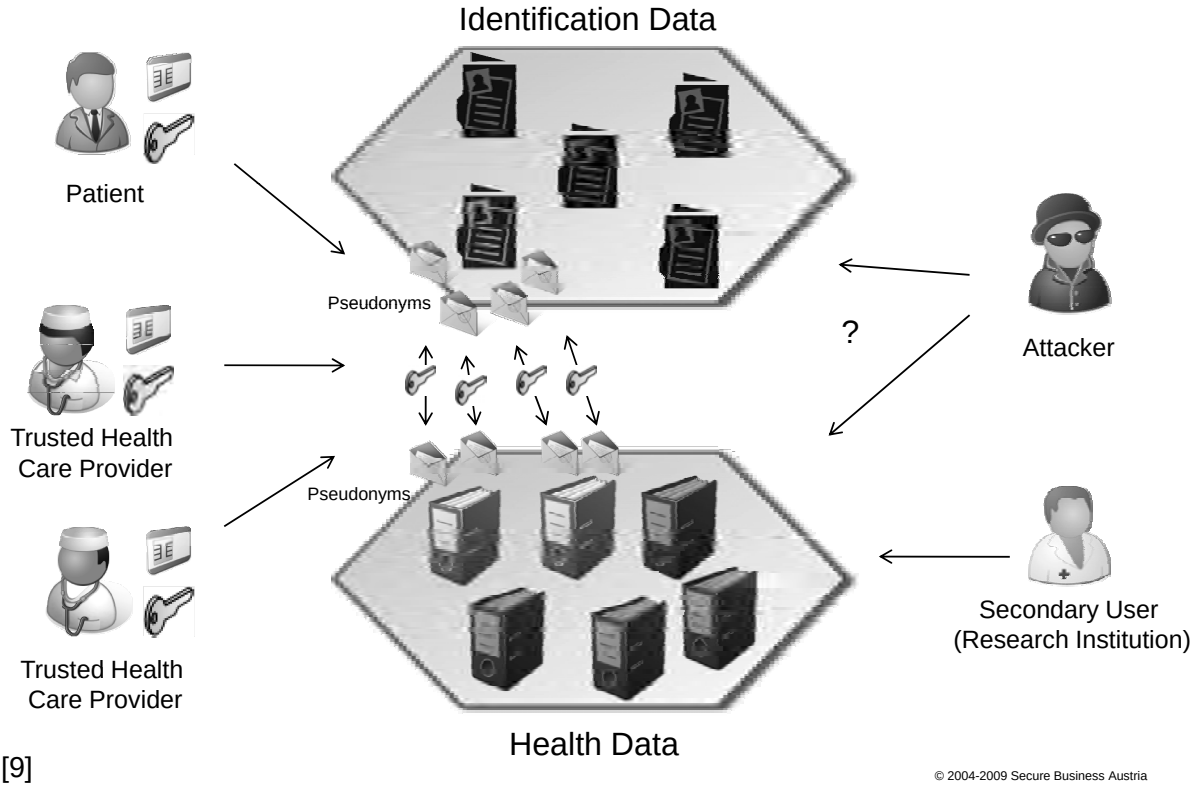
[SECURE] Business Austria
Science for better Security.



[8]

PIPE - Pseudonymization of Information for Privacy in e-Health

[SECURE] Business Austria
Science for better Security.



[9]

PIPE Benefits and Ongoing Research

[SECURE] Business Austria
Science for better Security.

- Hull-based security architecture
  - Combination of symmetric and asymmetric cryptography
  - Multiple roles supported
- Patient as data owner
  - Grants data access authorizations to trusted relatives and health care providers
- Secondary use supported
  - Secondary users gain access to health data without the ability to reconnect the pseudonymized data to the corresponding patients
- Ongoing research
  - Extension with advanced privacy-preserving query and retrieval techniques
  - Development of configurable pseudonymization workflows for different domains
  - Service-based centralized design

[10]

RESEARCH ON RE-SHOOTING COUNTERMEASURES

Isao ECHIZEN
National Institute of Informatics

Background: analog-hole problem

Conventional problem

- Originally intended to resolve security problems with analog-output terminals of digital equipment
- Resolution by replacement of digital terminals

Rise of new problem exploiting monitors and screens

- Trend of increasingly high-quality monitors and cameras makes it easy to reshoot presented content
  - -> Distribution of illegally re-shot content
    - Ex. re-shoot PC monitors with cell-phone cameras -> upload shot content
    - Ex. re-shoot theater screens -> sell pirate DVDs
      - Loss of USD 3B per year (survey of Motion Picture Association of America)

2

Conventional measures against re-shooting: use of digital watermarks

- Embed theater ID WM into digital cinema film.
- Detect WMs in pirate DVDs and identify flow of illegal distribution.

But: no control of re-shooting

3

Re-shooting countermeasure

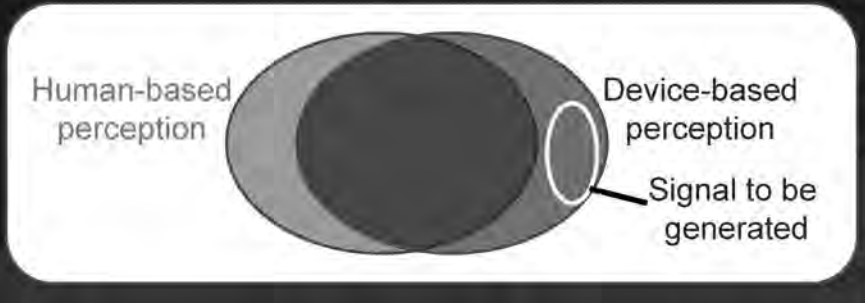
- Objective and approach -

Objective:

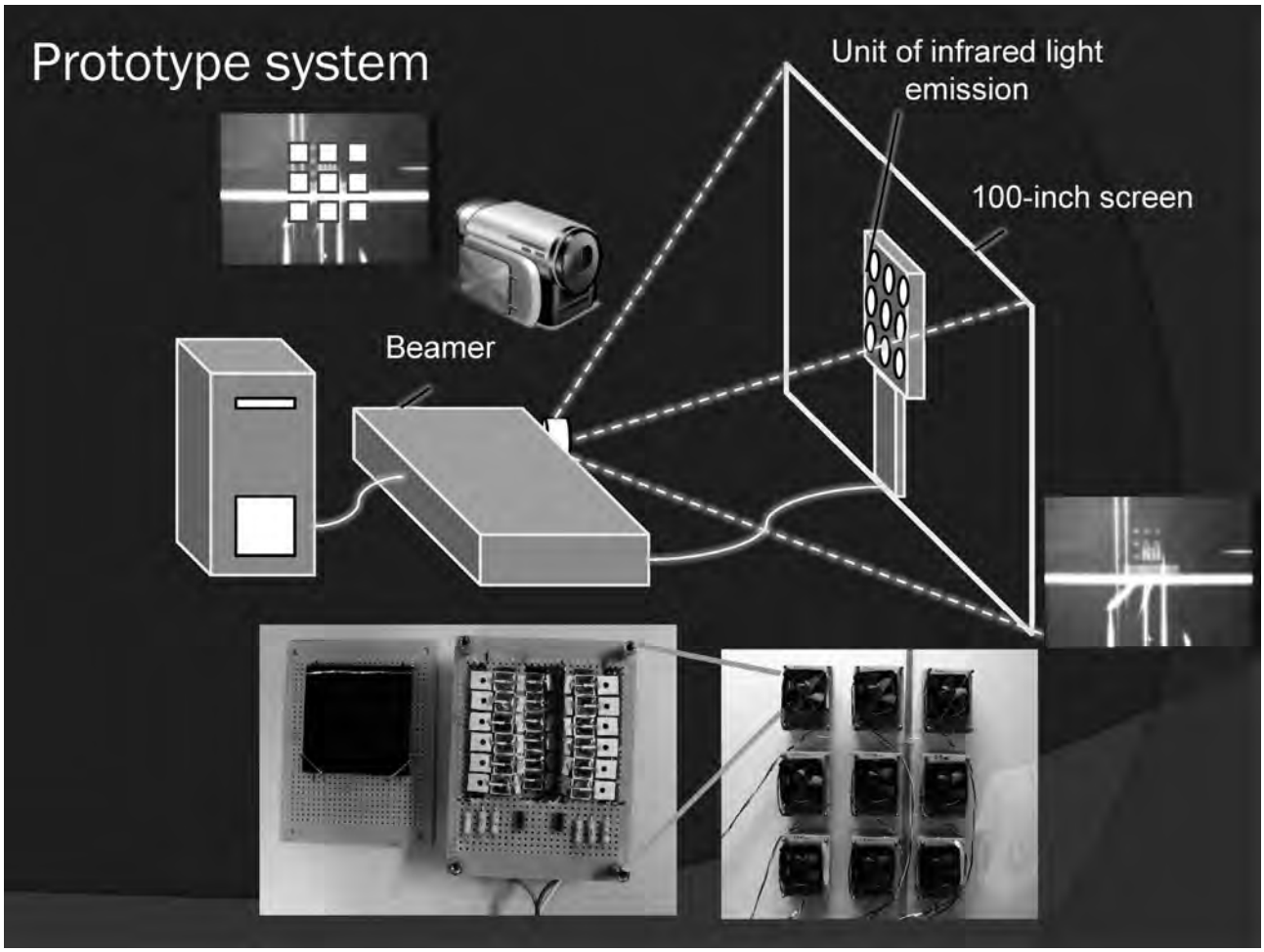
- Establish countermeasure to stop re-shooting
  - No new function is added into existing user-side device (ex. cam)

Approach:

- Use of difference between sensory perceptions of humans and devices
  - Destroy shot content using invisible signals which add noise to content shot through CCD/CMOS devices
    - Near-infrared signals: CCD and CMOS react to them



Near-infrared signals


Prototype system
Unit of infrared light emission
100-inch screen
Beamer

Privacy in e-Health

Observing Disclosure of X-Ray Images to Third Parties by Using Digital Watermarking

ISSI 2009
September 30th, 2009

Dr. Sven Wohlgemuth
Prof. Dr. Noboru Sonehara
Prof. Dr. Isao Echizen
National Institute of Informatics, Japan

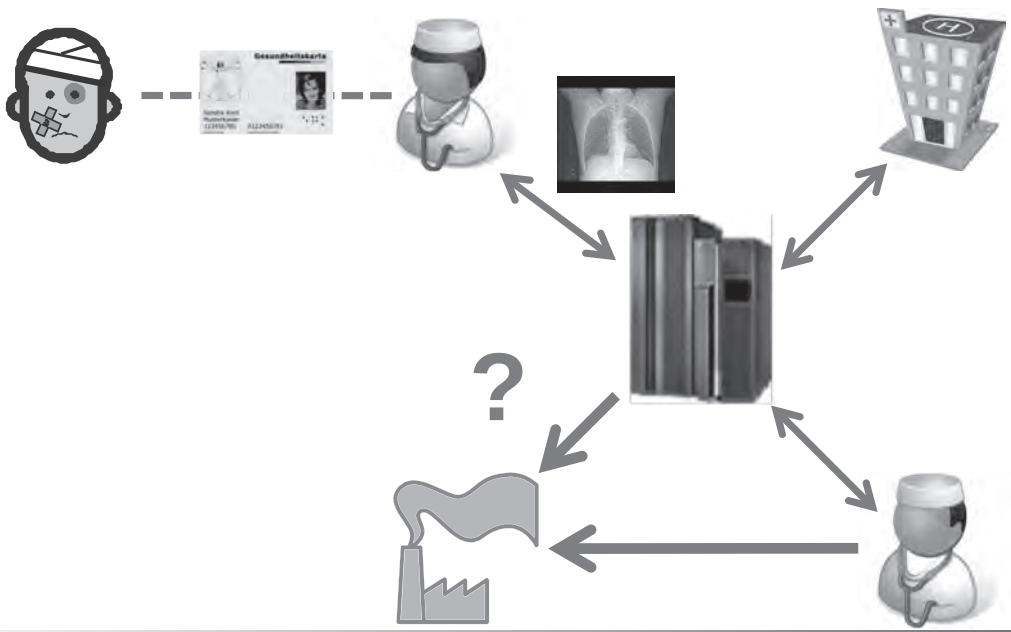
Prof. Dr. Günter Müller
University of Freiburg, Germany

Scenario: Telemedicine

National Institute of Informatics NII

Privacy promise:

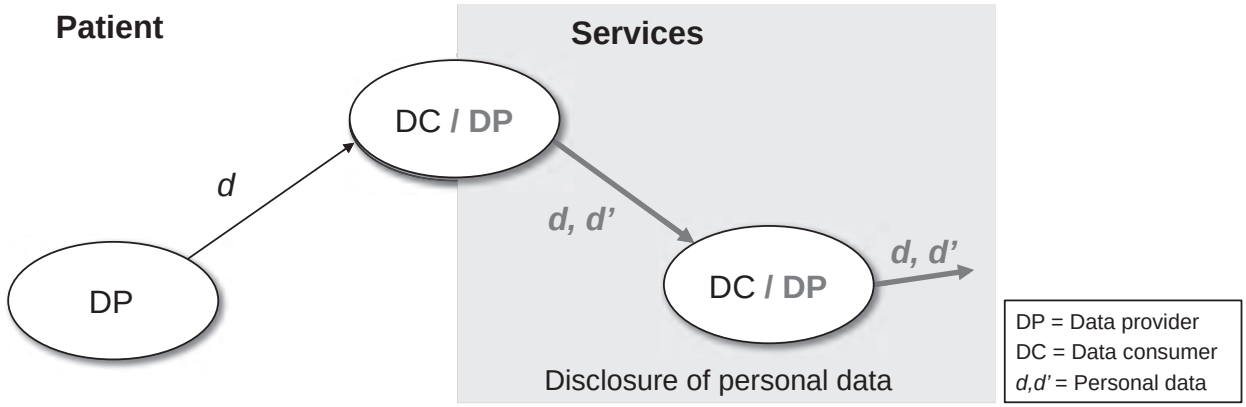
All personal data will be handled according to legislation and agreed privacy policy between users and services.



Privacy and Business Processes

Privacy legislation:

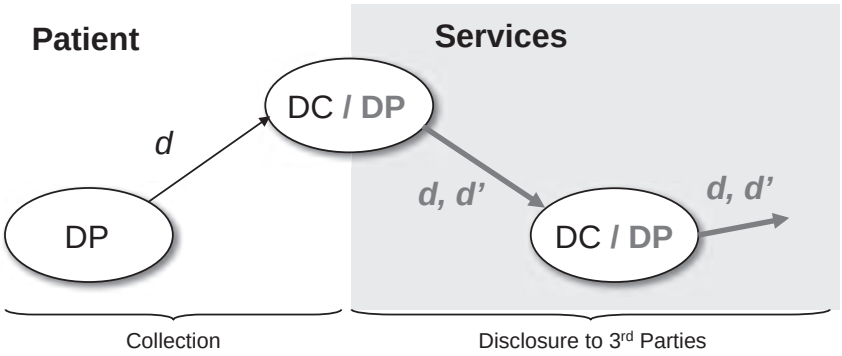
„Privacy is the claim of individuals, groups and institutions to determine for themselves, when, how and to what extent information about them is communicated to others.“
(Westin 1967, EU/Germany, Japan, HIPAA)



Pretschner, A., Hilty, M., and Basin, D. 2006.

Problem: No control for disclosure of personal data

Privacy-Enhancing Technologies: State of the Art



- Anonymity *(Anonymizer, Mix network)*
- Identity Management *(Liberty Alliance, Shibboleth, **iManager**, IBM idemix)*
- Policy language for provisions *(P3P)*
- Digital Rights Management *(Digital Privacy Management)*

- Policy languages for obligations *(IBM EPAL, NAPS)*
- Sticky policies *(HP Adaptive Privacy Management System)*
- Delegation of rights ***(DREISAM)***
  + Audit trail by digital watermarking ***(DETECTIVE)***

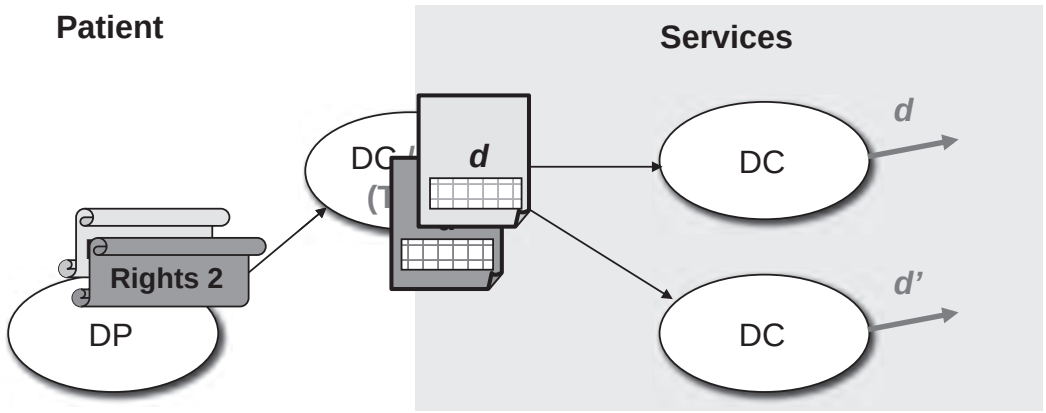
Wohlgemuth, S., 2008

DETECTIVE: Disclosure with Control

Controllable Disclosure: Authorization + enforcement by the user

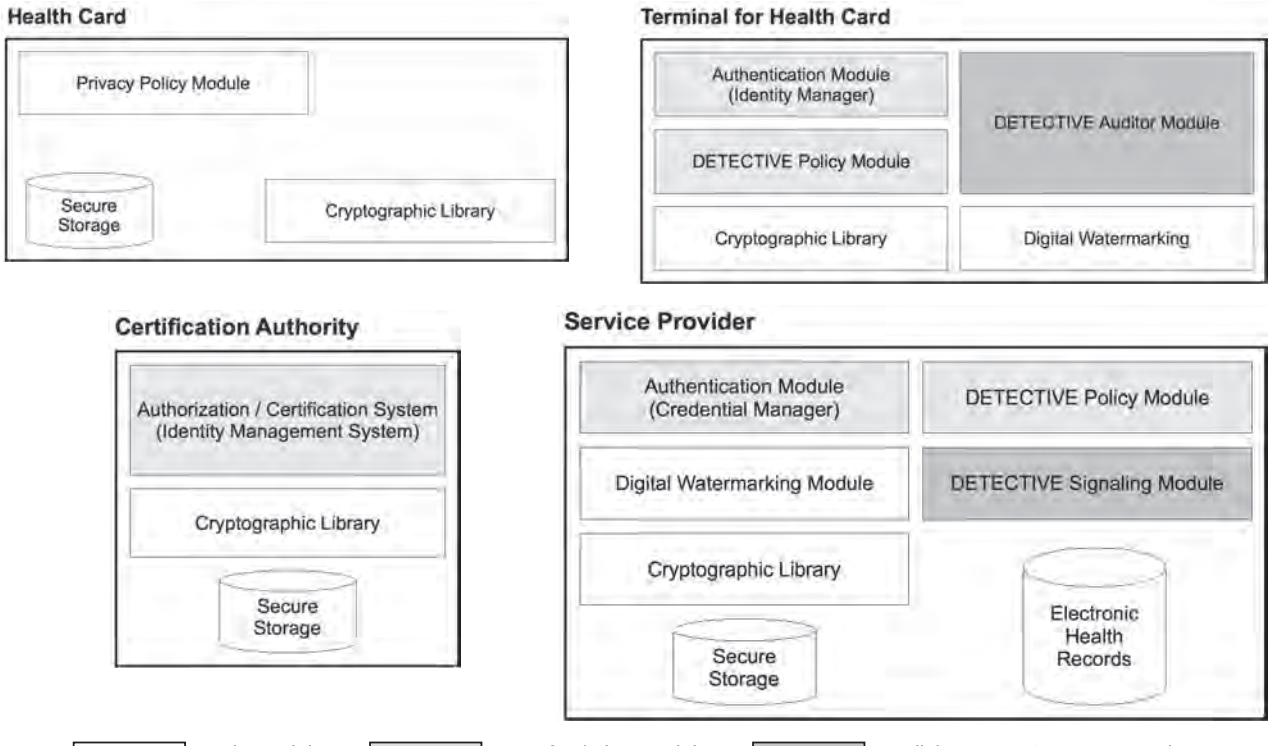
(a) Authorization: Non-linkable delegation of rights *(DREISAM)*

(b) Enforcement: Audit trail by digital watermarking *(DETECTIVE)*



Wohlgemuth, S., Sonehara, N., Echizen, I. and Müller, G., 2009

DETECTIVE: Proof-of-Concept Implementation



Dr. Sven Wohlgemuth

2009	Postdoc scholar at NII funded by DAAD (German Academic Exchange Service) Project: Enforcement of Privacy-Compliant Disclosure of Personal Data Member of ISSI 2009 organizing committee
2008	Doctoral graduation at University of Freiburg, Germany (Prof. Dr. Günter Müller) Thesis: Privacy with Delegation of Rights
2000	Diploma graduation at University of Saarbrücken, Germany (Prof. Dr. Birgit Pfitzmann, Tom Beiler) Thesis: Key Management – Object-Oriented Design and Implementation
2006/08	Member of SICHERHEIT 2008 and ETRICS 2006 conferences' organizing committee
2006-08	Founding Coordinator of working group "Privacy in Business Processes" of European Network of Excellence "Future of Identity in the Information Society (FIDIS)"
2001-06	Coordinator of German research priority programme "Security in Information and Communication Technology (SPP 1079)" funded by the German Research Foundation (DFG)
2003	doIT Software-Award 2003 by German Federal State "Baden-Württemberg" for "Usability and Security by Identity Management"

National Institute of Informatics
2-1-2 Hitotsubashi, Chiyoda-ku
Tokyo 101-8430
Japan

Phone: +81 3 4212 2594
Fax: +81 3 3556 1916
E-mail: wohlgemuth@nii.ac.jp
WWW: www.nii.ac.jp

パネル
ディスカッション

「社会と調和する科学技術」

議　　長　林　紘一郎（情報セキュリティ大学院大学 学長）

モデレータ　越前　　功（国立情報学研究所 准教授）

Gerhard Schneider
（フライブルク大学 チーフインフォメーションオフィサー）

Thomas Mück（ウィーン工科大学 教授）

岡部　寿男（京都大学学術情報メディアセンター 教授）

岡本　龍明（日本電信電話株式会社情報流通プラットフォーム研究所 特別研究室長）

野村　雅行（日本情報通信株式会社 代表取締役社長）

Peter Mertens（シーメンス株式会社 ゼネラルマネージャー）

持田　侑宏（フランステレコム株式会社 CTO）

議長

氏名　林　紘一郎（はやし・こういちろう）
所属　情報セキュリティ大学院大学学長・教授

学歴
1963 年　東京大学法学部卒業
1991 年　経済学博士（京都大学）
2004 年　博士（法学）（慶応義塾大学）

主要経歴
1963 年　日本電信電話公社入社
1969 年　データ通信本部
1973 年　経理局主計課　課長補佐
1977 年　北海道電気通信局　業務管理部長
1979 年　東京電気通信局　職員部長
1982 年　計画局総括課長
1984 年　総裁室企画室　調査役
1985 年　民営化により NTT となる
1985 年　画像電信事業部　ディジタル網部長
1987 年　国際部次長
1990 年　理事専用回線事業部長
1992 年　理事 NTT アメリカ社長
1994 年　常務理事 NTT アメリカ社長、米ネクステル社取締役
1995 年　常務理事マルチメディア推進本部本部長補佐
1996 年　同社退社
1997 年　慶應義塾大学教授（2004 年ー2005 年 同客員教授）
2004 年　情報セキュリティ大学院大学　副学長・教授
2009 年　情報セキュリティ大学院大学　学長・教授

専門分野
法と経済学

研究概要
情報セキュリティ、インターネットの自由と規律、知的財産権、
メディア法制、情報産業論、技術標準など法律学的および経済学的領域を広くカバーしている。

受賞
・「情報通信産業の生成と新産業秩序」（後に『インフォミュニケーションの時代』に吸収）
第 1 回テレコム社会科学賞、1985 年
・『ネットワーキングの経済学』 第 6 回テレコム社会科学賞、1990 年
・『情報メディア法』 電気通信普及財団特別賞、2007 年

"Harmonizing Technology with Society"

From Real to Cyber World: A Law and Economics Analysis

September 30, 2009

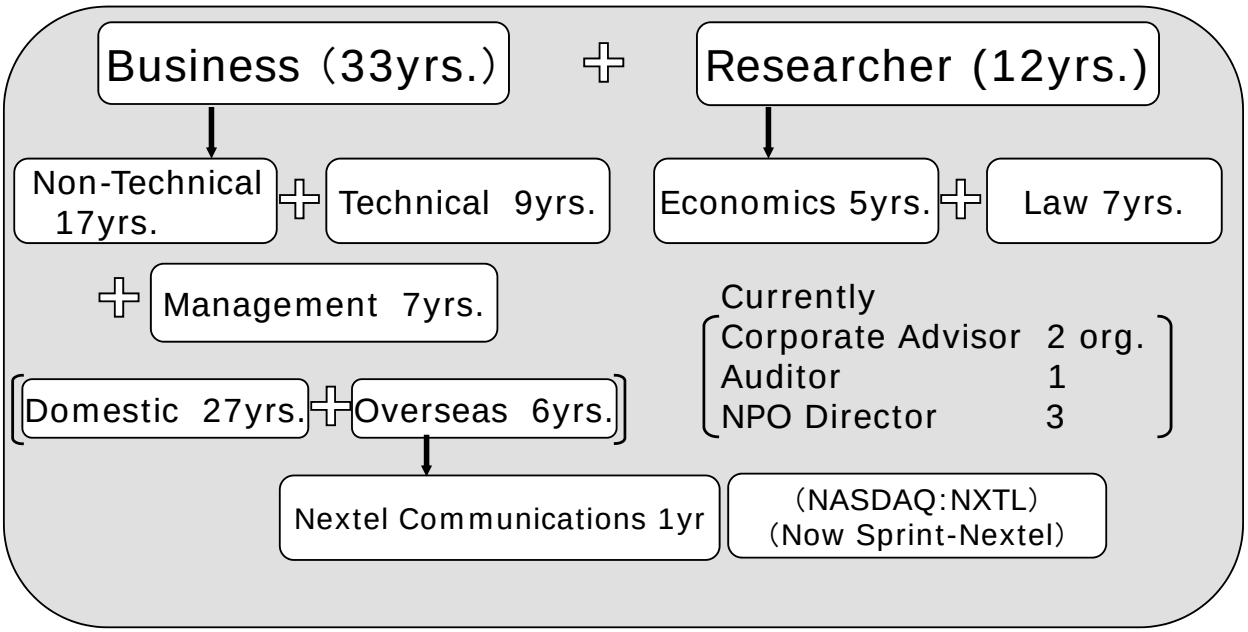
Presented to ISSI

Koichiro Hayashi, Ph.D., LL.D.

Institute of Information Security

- Established 2004
- First and only Graduate School specializing in InfoSec.
- Both Academic and Practical
- Comprehensive Study of InfoSec.
- 80%+ Students from Business
- WWW: http://www.iisec.ac.jp

Personal Career



3

Law in the Real World

- Tangible Goods: Excludable, Rivalry, Recoverable
- Alienable v. Inalienable
- Property, Contact and Liability Rules for Alienable Goods
- Freedom of Speech, Self-Decision and Privacy for Inalienable Objects
- Remedy and Sanction by Litigation, Injunction and Prosecution effective
- One Right for One Thing

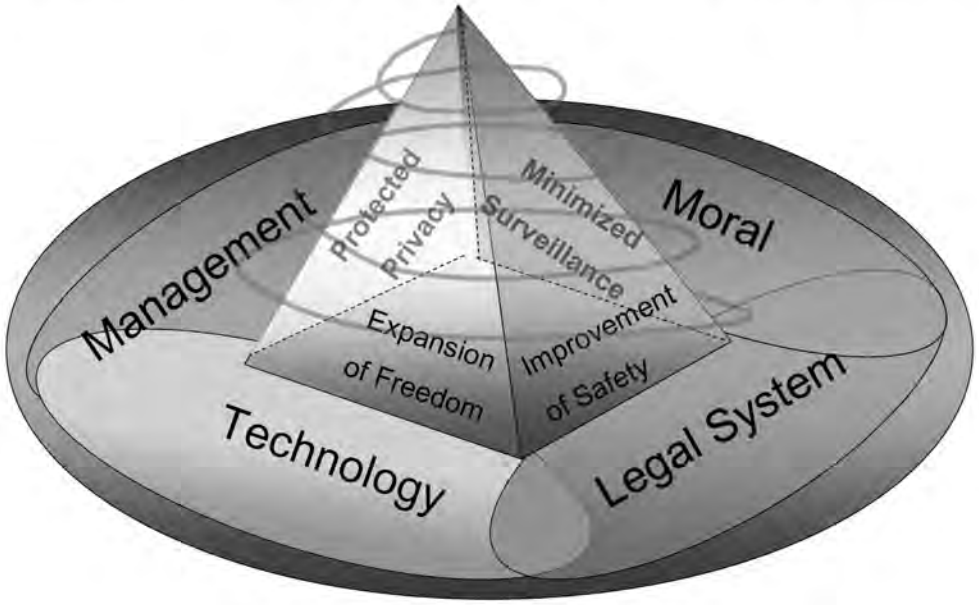
Fluctuating Law in Cyberworld

- Intangible Goods: Non-excludable, Non-rivalry, Irreversible
- Only two types of Information protected: Secret Information (SI) and Intellectual Property (IP)
- SI Protection neither comprehensive nor well-balanced
- IP Protection (especially Copyright) challenged by Digital Technology
- Personal Data as the third type?
- Multiple Rights for One Object
- CODE is Law? (Lessig [1999])

Real v. Cyber

	Real	Cyber
Subject (Actor)	Natural Person, Legal Person	+ Computer
Object	Tangible Goods	+ Intangibles
Action	Own, Exploit and Transfer	+ Attribute, Hold and License
Enforcement	Damages, Prosecution etc.	+ Injunction or Recovering Tech?
Alienability	One Right for One Thing	Multiple Rights for One Object

How to Generate a Balanced View



Original idea comes from Lessig [1999] & Tsujii [2003]

Questions

- Question-1:

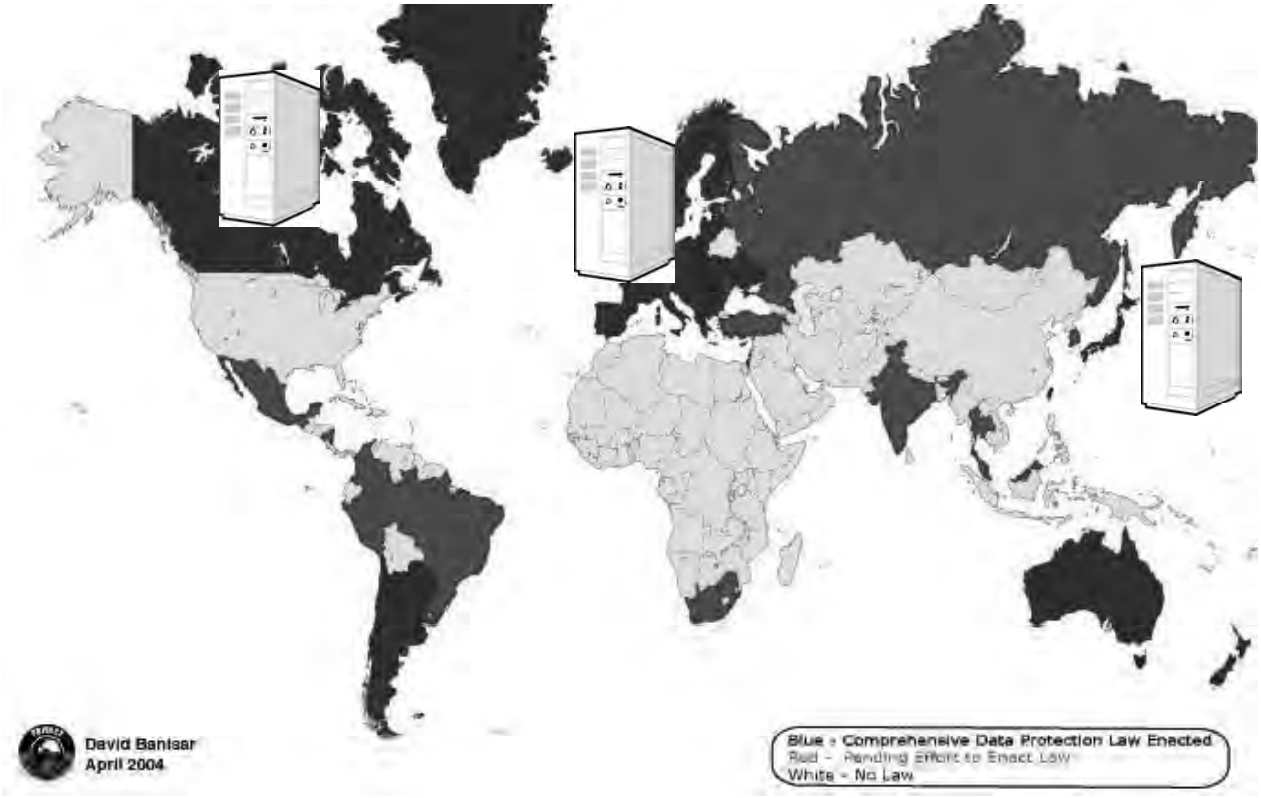
What do you think is the most important factor, if you are asked to develop or deploy a new information system for social innovation?

- Legal System?
- Management?
- Moral?
- Technology?
- ...?

- Question-2:

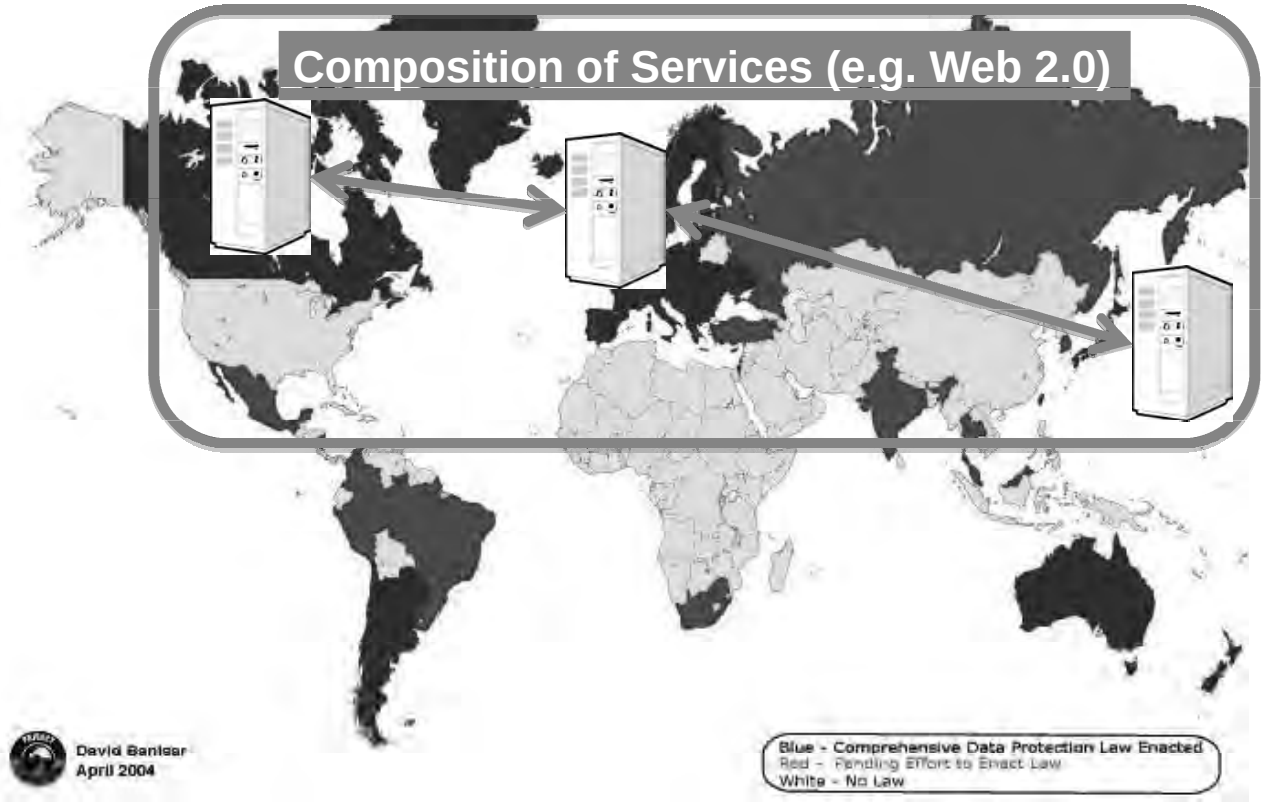
What kind of role do you expect on social scientist, when you do above?

Example: Data Protection Regulations in the World



http://www.privacyinternational.org

Social Innovation by cross-state Composition of Services



Challenge: Application of different regulations

氏名　岡部　寿男（おかべ・やすお）
所属　京都大学学術情報メディアセンター
　　ネットワーク研究部門 教授

学歴

昭和 61 年 3 月　京都大学工学部情報工学科卒業
昭和 63 年 3 月　同大学院修士課程修了
京都大学博士（工学）

主要経歴

昭和 63 年 4 月　京都大学工学部　助手
平成 6 年 7 月　京都大学大型計算機センター研究開発部助教授、ソフトウェア研究室長
平成 10 年 4 月　京都大学大学院情報学研究科助教授　通信情報システム専攻担当
平成 12 年 11 月　京都大学大学院情報学研究科助教授　知能情報学専攻担当
平成 14 年 4 月より現職

専門分野

コンピュータネットワーク

研究概要

次世代、次々世代インターネット技術により、あらゆるものがネットワーク機能を内蔵し、あらゆるところで利用可能となる、ユビキタスネットワーキング環境の実現と利用のための技術の研究を行っている。

受賞

平成 17 年 8 月 IBM Shared University Research Award 受賞
http://www.kyoto-u.ac.jp/ja/profile/intro/honor/award_b/other/2007/070808.htm

氏名　野村　雅行（のむら・まさゆき）

所属　日本情報通信株式会社（NI+C）代表取締役社長
　　工学博士

学歴

1971 年　慶應義塾大学工学部機械工学科卒業。
1973 年　名古屋大学大学院理学部数学科修士課程。

主要経歴

1973 年　日本電信電話公社（NTT）入社。
1984 年　日本電信電話公社　武蔵野電気通信研究所　研究専門調査役
1998 年　NTT マルチメディアネットワークサービス事業本部　パケット通信事業部長
1999 年　NTT コミュニケーションズ　ビジネスユーザー事業部データネットワークサービス部長
2001年　取締役ビジネスユーザー事業部　統合 IP サービス部長
2002年　取締役ブロードバンド IP 事業部長
2004 年　常務取締役ソリューション事業部長
2005 年　代表取締役副社長
2006 年　代表取締役副社長法人事業本部長
2008 年 6 月　現職。日本情報通信株式会社　代表取締役社長

～　日本電信電話公社入社後、パケット交換、フレームリレー等のデータ通信サービスの研究実用化、インターネットサービスの事業化に従事する　～

受賞

1986 年　関東地方発明協会奨励賞
1987年　テレコム旬間奨励賞、ITU 協会賞

著書

「通信プロトコル」（電気通信学会）
「パケット通信絵とき読本」（オーム社）
「やさしくわかる通信ネットワーク」（日本実業出版社）

Dr. Peter Mertens
General Manager
Technology Department
Siemens K.K.
Japan

Education:

July 2, 1986	Diplom-Physiker (Master of Physics), Friedrichs-Wilhelms Universitaet Bonn
July 1, 1991	Dr. rer. nat. (PhD) in Theoretical Physics, Phillipps-Universitaet Marburg

Professional Experience:

1991 - 1993	Siemens ZFE (Corporate Research and Development), Engineering and SW development methods SW architecture concepts for automation system
1993 - 1995	Siemens KWU (Power Generation), Erlangen, Germany Project Manager for “CAPTURE” (automatic requirements capture and engineering support database SW for combined cycle power plants.)
1995 - 1999	Siemens TS (Transportation Systems, Railway), Erlangen, Germany - Railway Engineering: Project Manager responsible for engineering processes and engineering quality management, engineering, SW and R&D planning methods in railway rolling stock engineering - SW development: Project manager of SW Initiative of TS (professional SW development program) - Manufacturing: Project and Program Manager for productivity optimization in all seven TS manufacturing plants (Benchmarking, Toyota Production System, material supply organization, improvement program, etc.)
2000 - 2001	STS (Siemens Transportation Systems), Sacramento, California (USA) Project and Product Manager responsible for developing a new generation light rail train for the American market (product management, platform development, requirements, basic design, cost reduction, supply chain, etc.)
2001 - 2005	Siemens CT (Corporate Technology), Muenchen, Germany Strategic Planning, Senior Principal Consultant, responsible for innovation capability analysis, internal planning methods, etc. - Innovation Strategy - Innovation Benchmarking - Strategy for Internationalization of R&D
Since 10/2005	Siemens K. K., Tokyo, Japan: General Manager, Head of Corporate Technology Department
03/2008 – 02/2009	Tokunin (specially assigned) Professor, SIMOT program, Tokyo Institute of Technology

SIEMENS

Data security
- Internal Activities in Siemens
- Siemens Contribution to an EU Project

Dr. Peter Mertens
Head of Corporate Technology
Siemens KK, Tokyo

Peter.mertens@siemens.com

SIEMENS

Introduction of the Author

Dr. Peter Mertens

Head of Corporate Technology, Siemens KK Tokyo

18 years of industrial experience

Experience in the Siemens Networks, Trains and Fossil Power Plant businesses as well as in Corporate Research and Technology

Experience working in Germany, the USA, and Japan

Areas of Expertise include SW engineering, project management, product management, and management of technology

Current focus is on managing R&D cooperations with partners in Japan

Academic credentials:

PhD in Physics (1991)

Publications in theoretical physics, system engineering methods, requirements engineering, management of technology, and demographic change

SIEMENS

Siemens Sectors and Divisions

Sectors

Industry

Divisions

- Drive Technologies
- Industry Automation
- Building Technologies
- Mobility
- Lighting (OSRAM)
- Industry Solutions

Energy

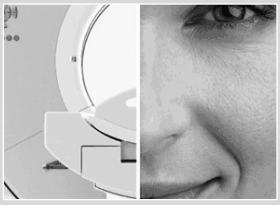
Divisions

- Fossil Power Generation
- Renewable Energy
- Oil & Gas
- Energy Service
- Power Transmission
- Power Distribution

Healthcare

Divisions

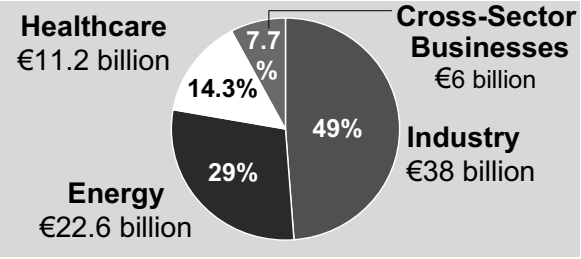
- Imaging & IT
- Workflow & Solutions
- Diagnostics



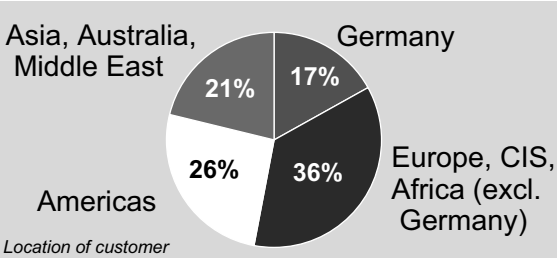
Siemens Business Numbers: Committed to profit and growth

SIEMENS

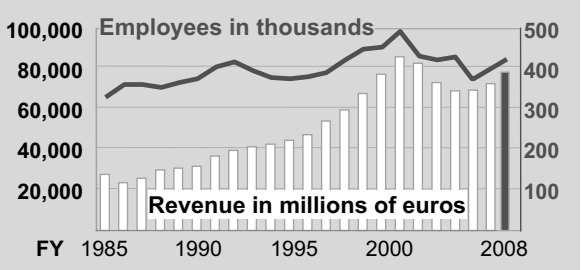
Active in three Sectors



Revenue by region



Revenue and employees



Key figures

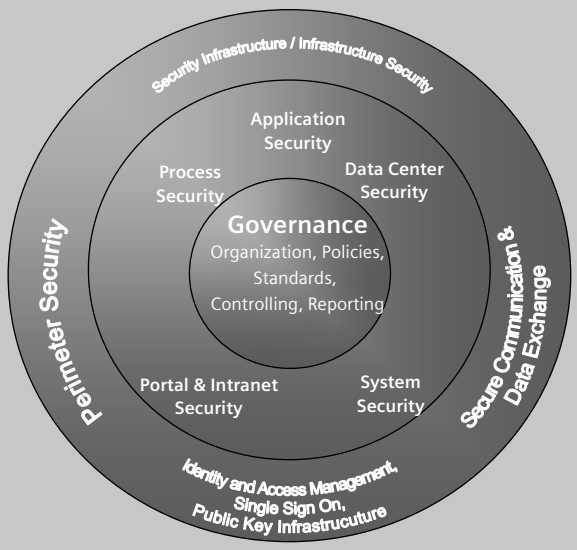
Continuing operations (in millions of euros)	FY2008	FY2007
Revenue	77,327	72,448
New orders	93,495	83,916
Income	1,859	3,909
Free cash flow	5,739	6,755
Employees	**427,000**	**398,000**

As of September 30, 2008

Siemens' data security policies and measures (examples)

SIEMENS

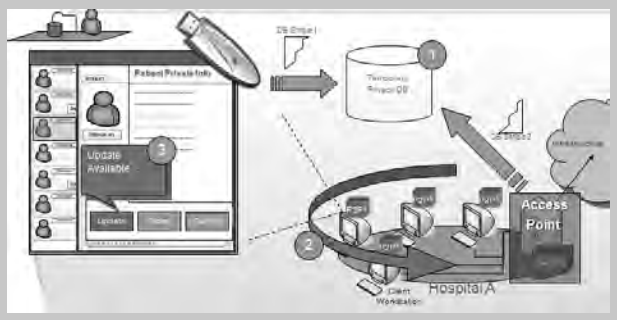
- European law makes it mandatory to implement data protection and security in a company, for example in order to protect personal data of the employees.
- Additionally, especially innovation driven companies handle large amounts of confidential data that may be targets for attacks by hackers with all kinds of motives.
- Siemens has implemented a thorough management and technical solution to make data secure. This includes data protection officers, firewalls and other technical means, and also a department that continually tests data security, for example by staging simulated attacks.



The necessity of data security in order to share important health research data

SIEMENS

- Sharing medical, especially clinical, data between institutions is sensitive because of the personal data security issues.
  So it is often difficult to share digital medical data between the general practitioner, the insurance, specialists, and hospitals.
  The introduction of a patient chip card for insurance reimbursement purposes in Germany has improved the situation somewhat, but the exchange is still limited.
- So how to exchange clinical research data not only between different institutions, but even between institutions in different countries in Europe and the US with very different data protection and security laws and cultures ?
- In the EU project "health-e-child", a thorough data security and protection policy and preparation have made it possible to internationally cooperate on a clinical database of serious but rare pediatric cases.
  Siemens is a major participant in this project and has contributed substantially to the data protection and security issue.



氏名　持田　侑宏（もちだ・ゆうこう）
所属　フランステレコム株式会社 CTO

学歴

1964年　東京大学工学部電気工学科卒
1988 年　同大学工学博士

主要経歴

1964 年　富士通研究所に入社、デジタルネットワーク用装置の研究開発に従事。
　　伝送事業部長、富士通研究所常務取締役などを経て、2007 年 6 月退任。
この間　1965-66 年ドイツミュンヘン工科大学研究滞在
　　2004-2007 年中国北京郵電大学客座教授
現在、フランステレコム（株）CTO

専門分野

デジタル伝送工学
デジタル信号処理
光通信工学

研究概要

富士通研究所にて同軸ケーブル，ミリ波導波管，光ファイバケーブルによるデジタル伝送方式･装置の研究開発，デジタル信号処理による電話回線データモデムおよび信号処理 LSI の研究開発，SDH や ATM などデジタルネットワーク装置の開発などに従事。
現在フランステレコム東京研究所で日仏間の研究交流を推進中。

受賞

IEEE および電子情報通信学会フェロー

ポスター・
デモセッション

1. プライバシー、データ、メディアのセキュリティ技術

1－1　越前　　功（国立情報学研究所 准教授）：
Research on Re-shooting Countermeasures

1－2　Nurul Huda（国立情報学研究所 外来研究員）：
Extending Usability of Personal Health Records

1－3　片岡　浩巳、畠山　　豊、奥原　義保、
倉本　　秋（高知大学医学部）：
Medical data analysis infrastructure
– Attempt at the Kochi Medical School –

1－4　Sven Wohlgemuth（国立情報学研究所 研究員）：
Privacy in e-Health

1－5　Johannes Heurix（オーストリア・セキュアビジネスセンター研究員）：
Pseudonymization of Health Data

Research on Re-shooting Countermeasures

Isao Echizen
National Institute of Informatics, Tokyo, Japan

Background: analog-hole problem

Conventional problem

- Originally intended to resolve security problems with analog-output terminals of digital equipment
- Resolution by replacement of digital terminals

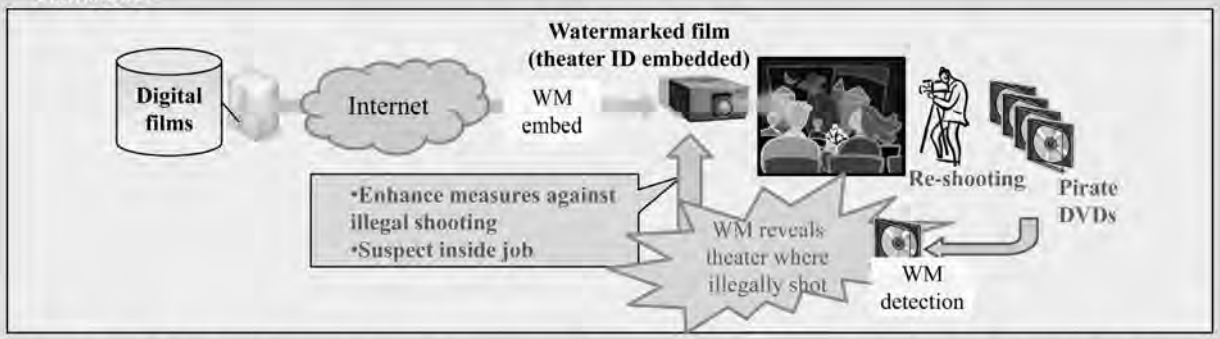
Rise of new problem exploiting monitors and screens

- Trend of increasingly high-quality monitors and cameras makes it easy to reshoot presented content -> Distribution of illegally re-shot content
  Ex. re-shoot PC monitors with cell-phone cameras -> upload shot content
  Ex. re-shoot theater screens -> sell pirate DVDs

Loss of USD 3B per year (survey of Motion Picture Association of America)

Conventional measures against re-shooting: use of digital watermarks

- Embed theater ID WM into digital cinema film
- Detect WMs in pirate DVDs and identify flow of illegal distribution ➡ But: no control of re-shooting



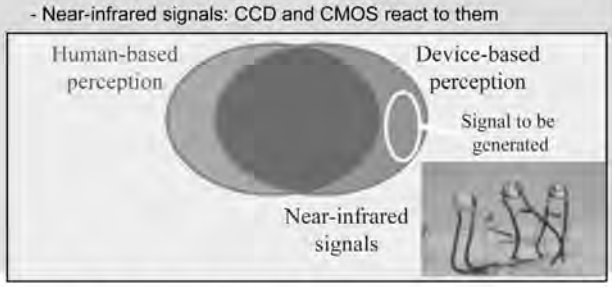
Re-shooting countermeasures based on difference between sensory perceptions of humans and devices

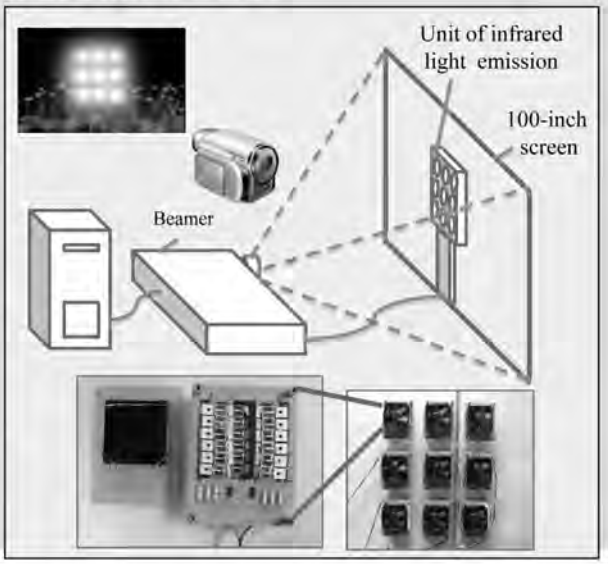
Objective

- Establish countermeasure to stop re-shooting
  No new function is added into existing user-side device (ex. cam)

Approach

- Use of difference between sensory perceptions of humans and devices
  - Destroy shot content using invisible signals which add noise to content shot through CCD/CMOS devices
  - Near-infrared signals: CCD and CMOS react to them





NII Contact: Isao ECHIZEN – Associate Professor at the Digital Content and Media Sciences Research Division
TEL : 03-4212-2516 FAX : 03-3556-1916 Email : iechizen@nii.ac.jp

Extending Usability of Personal Health Records

Md. Nurul HUDA*, Shigeki YAMADA and Noboru SONEHARA
* huda@nii.ac.jp

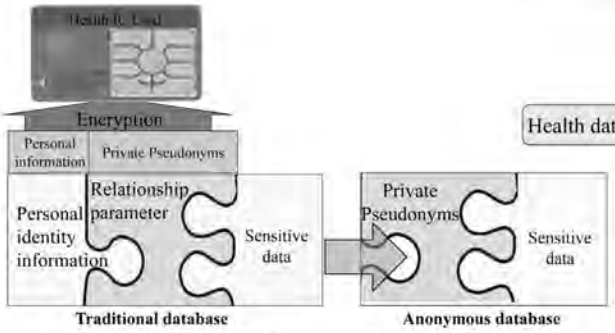


Figure 1: Concept of separating personal information from sensitive health data

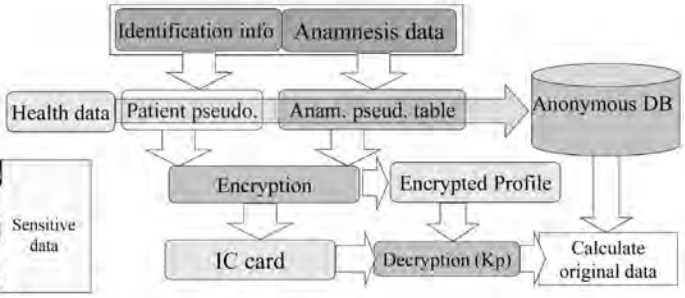


Figure 2: Database anonymization process in P³HR

Table 1: Example of anonymizing records

h = height of a domain hierarchy

Weighted hierarchical distance (WHD) of domain generalization (from height p to q)

$$WHD(p,q) = \frac{\sum_{j=q+1}^{p} \omega_{j,j-1}}{\sum_{j=2}^{h} \omega_{j,j-1}}$$

Name	T. Date	Disease
Alice	15-04-1951	Heart D.
Bob	23-07-1959	AIDS
John	09-11-1954	Heart D

Original records

Attr	Pseud
P.Pseud	010..0100
Date	+729915
Heart D.	PQR

Alice's Pseudonyms

P. Pseud	T. Date	Disease
101..1101	02-09-3459	DH
010..0100	25-01-2951	PQR
101..0111	12-12-2459	GTFD

Anonymous records

n = the number of attributes in the attribute set of anamnesis data

Av_i =availability {0,1} of i^{th} attribute

$L(v_j)$ be the domain level of v_j

Let $t = \{v_1, v_2, \ldots, v_m\}$ m≤n be a tuple, $t' = \{v_1', v_2', \ldots, v_m'\}$ be a generalized tuple of t.

Scope of secondary use (SSU) :

$$SSU(t') = \frac{\sum_{i=1}^{n} Av_i \left(1 - \sum_{j=1}^{m} WHD(L(v_j), L(v_j'))\right)}{n}$$

If N is the number of tuples in the table T,

$$SSU(T) = \frac{\sum_{i=1}^{N} SSU(t_i)}{N}$$

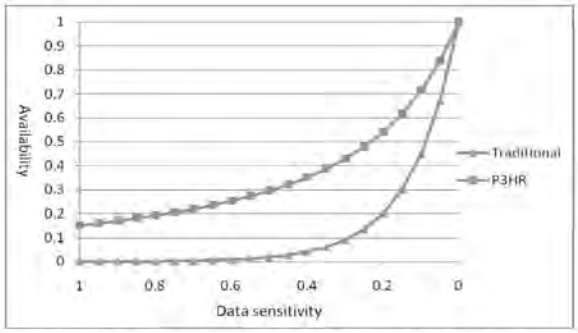


Figure 3: Data availability with change in data sensitivity

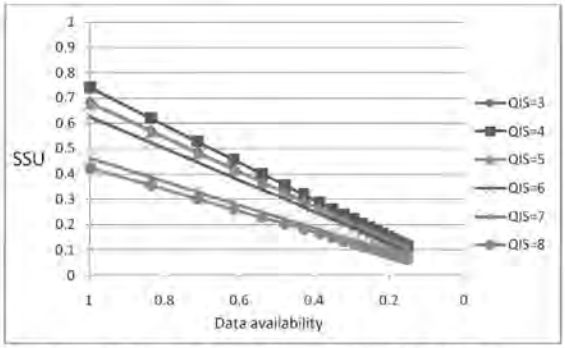


Figure 4: Scope for secondary use (SSU) in P³HR with change in data availability

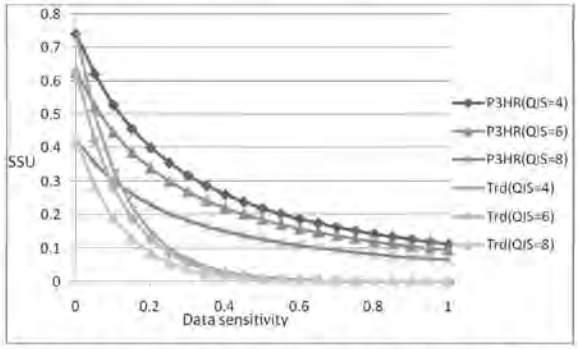


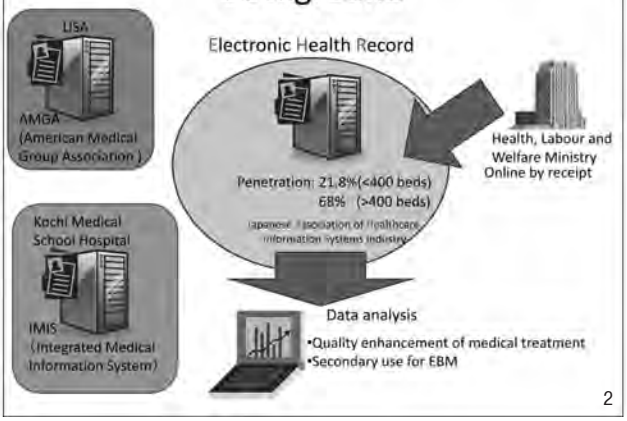
Figure 5: Comparative scope for secondary use (SSU) in P³HR and Traditional system

Medical data analysis infrastructure - Attempt at the Kochi Medical School -

Hiromi KATAOKA, Yutaka HATAKEYAMA,
Yoshiyasu OKUHARA, Shu KURAMOTO
Kochi Medical School

1

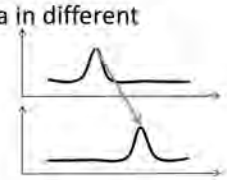
Background



2

Purpose

- Data anonymizing
  - Privacy protection
- Large variety of data type
  - Number, text, waveform data, image
- Standardization of test data in different hospitals
  - Existence of test error



3

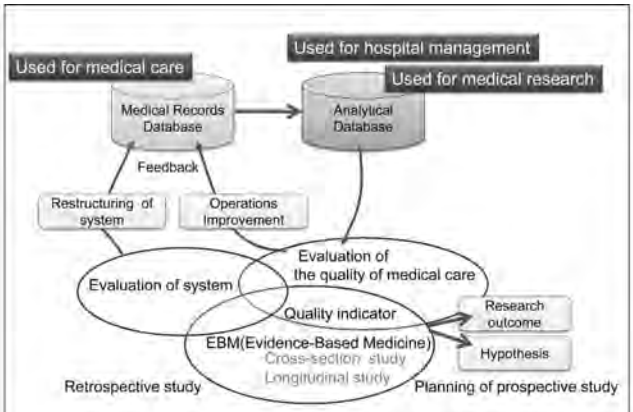


Fig1. Need for Analytical Database

4

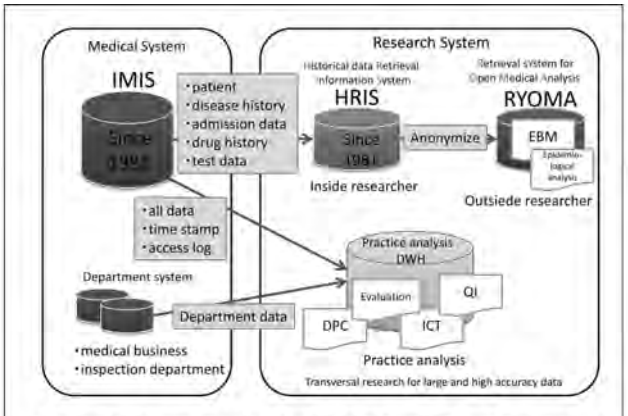


Fig.2 DWH system in Kochi Medical School Hospital

5

Process for anonymous data

- Anonymizeing for Patient ID
  - reversible mapping
- Change of date information (shifting)
  - Definition of changing date
- Data removal for few disease

Patient ID	Anonymous ID	Shifting date
0000001	1234567890	S
Removal patient → 0000002	X	X
0000003	0987654321	-1
...	...	...

6

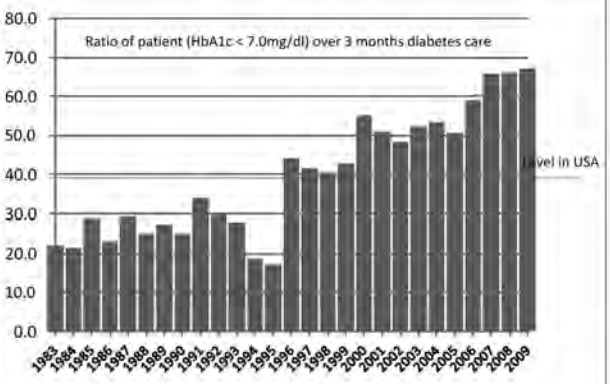


Fig.3. Ratio of control patient for diabetes care

7

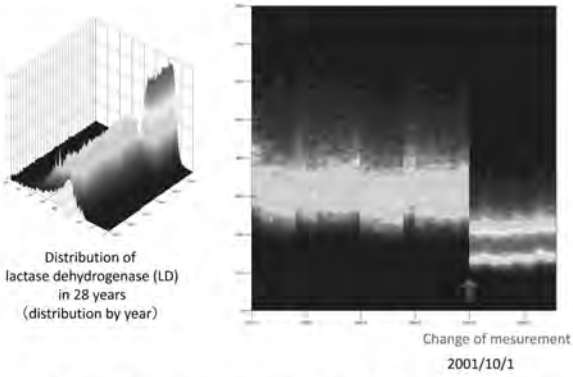


Fig.4. Standardization of test data in measurement change

8

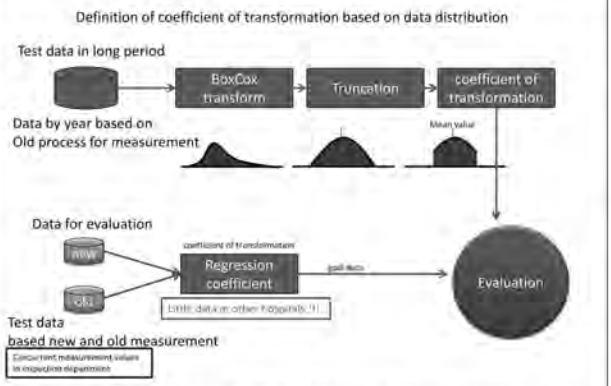


Fig.5. Proposal of normalization process

9

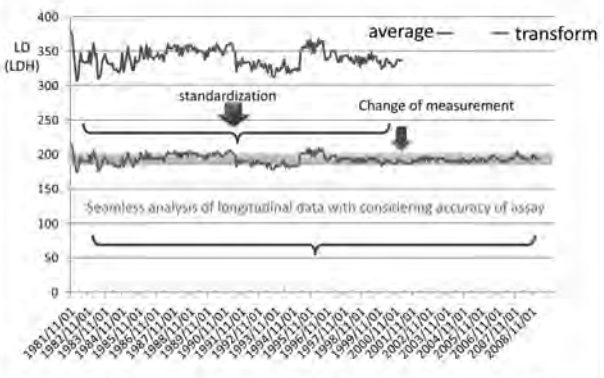


Fig.6. Sample of standardization result

10

5. Conclusion

- Infrastructure development for medical records
  - Kochi medical school hospital from 1981
- Secondary use
  - medical economics, estimation,…
- Data integration process with other hospitals
  - standardization
- Right management system of each medical data
  - Patients, hospitals, …

11

Privacy in e-Health

- Enforcement of Privacy-compliant Disclosure of Personal Data -

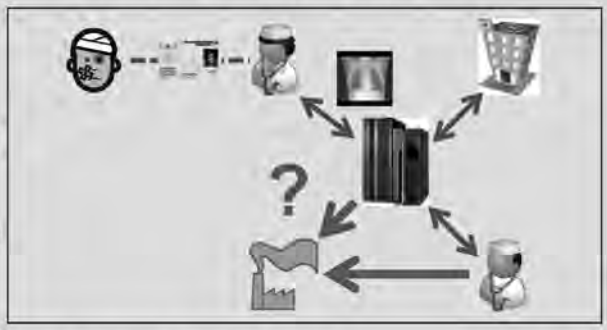
Dr. Sven Wohlgemuth Prof. Dr. Isao Echizen Prof. Dr. Noboru Sonehara Prof. Dr. Günter Müller

National Institute of Informatics, Tokyo, Japan University of Freiburg, Germany

Medical Services and Disclosure of Patients' Health Data to 3rd Parties

Service providers act as data consumers and data providers

- Availability of patients' health data by electronic health records
- Service providers (e.g. company) provide electronic health records
- Data consumers collect, use, and store the patients' personal data
- Data providers disclose / delegate personal data to service providers
- Privacy promise: Service providers handle personal data according to the agreed upon privacy policy between patients and service providers



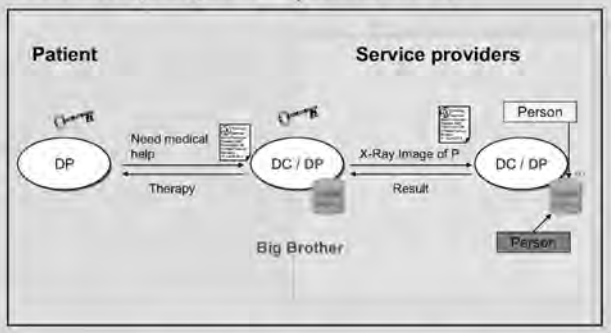
No Control on the Disclosure of Patients' Health Data

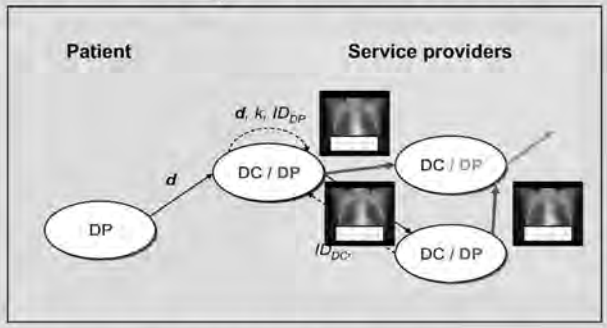
Identity Management and Delegation

- Privacy by non-linkable credentials
- All credentials and pseudonyms are based on secret key
- All-or-nothing delegation ➡ Loss of control

Digital Watermarking and Disclosure to 3rd Parties

- Copyright protection by labeling digital content
- Symmetric watermarking scheme: Both service providers get the same watermark ➡ Non-distinction of last data provider





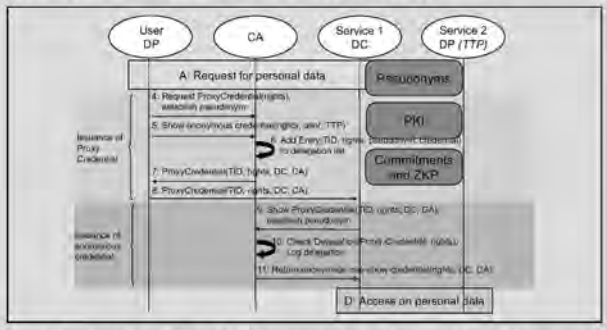
Controllable Disclosure of Patients' Health Data by DREISAM & DETECTIVE

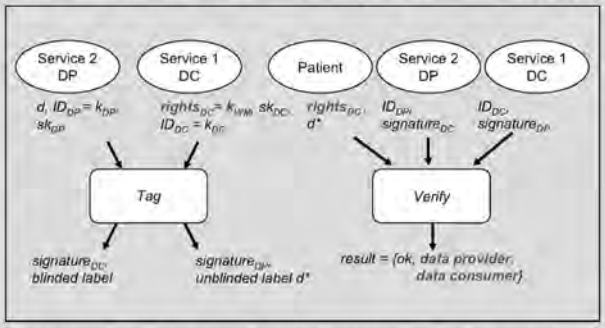
DREISAM: Non-linkable Delegation of Rights

- Authorization: Delegation of access rights to user's data
- PKI-based protocols with cryptographic commitments and zero-knowledge proof for non-linkability
- Proxy credentials instead of sharing secret key

DETECTIVE: Documenting Delegations of Personal Data

- Ex-post enforcement by identifying last data provider
- Linking the identities of data provider and consumer to disclosure by cryptographic commitments and digital watermarking
- Verification by patient due to delegated rights as watermarking key





Evaluation: Proof-of-concept implementation for medical services with electronic health records (x-ray images)

NII Contact: Dr. Sven WOHLGEMUTH – DAAD Postdoctoral Scholar at the Digital Content and Media Sciences Research Division
TEL : 03-4212-2594 FAX : 03-3556-1916 (c/o Prof. Dr. Echizen) E-mail : wohlgemuth@nii.ac.jp WWW: www.nii.ac.jp

[PIPE - Pseudonymization of Information for Privacy in e-Health]

Pseudonymization of Health Data

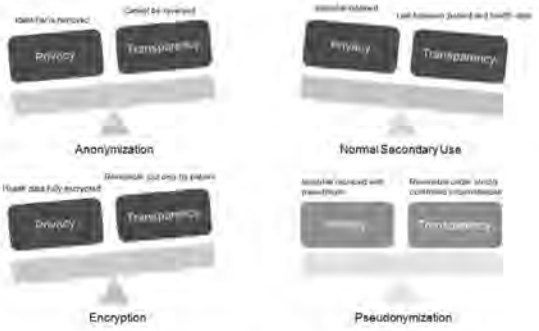
As aging and very expensive programs put more pressure on health and social care systems, the increasing use of electronic health records that promise a reduction of costs and the improvement of the quality of clinical trials brings legitimate concerns about privacy and confidentiality of the stored medical data.

[Challenges]

- Nowadays, the protection of sensitive data is more important than ever before because data is stored longer and in a centralized way.
- It is the patient's right to demand privacy (e.g. HIPAA, EC Directives, Domestic Acts).
- Disclosure of medical data can create serious problems for the patient.
- It is necessary to assure the availability of data for secondary use, e.g. for research.

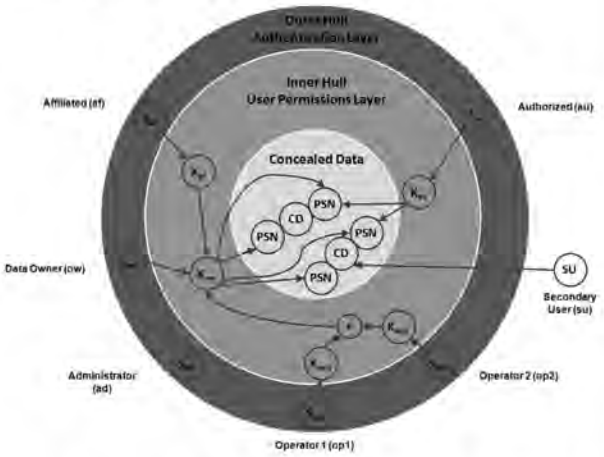
[Privacy vs. Transparency]

- Anonymization by removing identifiers allows privacy-enabled secondary use but cannot be reversed.
- Fully encrypting health data with a secret key only known to the patient ensures confidentiality but prevents secondary use of the encrypted data unless explicitly decrypted by the patient thus unconcealing her identity.
- Secondary use without privacy-enhancing measures discloses the link between patients and their health data.
- Pseudonymization severs this link which can still be reestablished under strictly controlled circumstances.



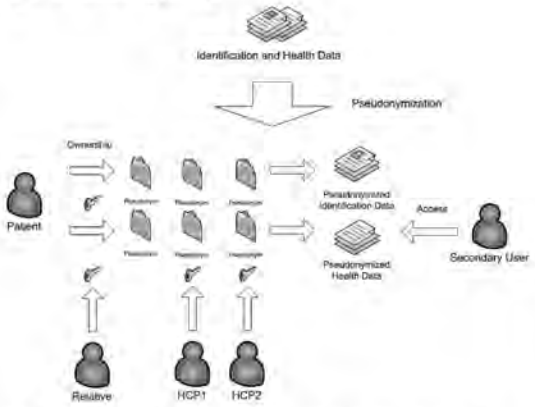
Pseudonymization retains the balance between privacy and transparency and allows privacy-preserving secondary use.

[PIPE Hull Architecture]



The three-layered hull structure supports different roles including the data owner (patient), affiliated (trusted relative), authorized (trusted health care provider), and secondary user (research institution), as well as administrative roles such as the administrator and operator.

[Pseudonyms]



Pseudonymization at the data level allows reconnecting the medical data to their corresponding patients only for explicitly authorized users.

Thomas Neubauer
Johannes Heurix
{tneubauer, jheurix}@securityresearch.at

[SECURE]
Business Austria
Science for better Security.

ポスター・
デモセッション

2. e-Science, CSI(Cyber Science Infrastructure)
研究教育情報基盤

2－1　山田　茂樹（国立情報学研究所 教授）：
学術情報ネットワーク SINET3

2－2　山地　一禎（国立情報学研究所 准教授）：
学術認証フェデレーションの現状

2－3　合田　憲人（国立情報学研究所 教授）：
日本における学術グリッド基盤

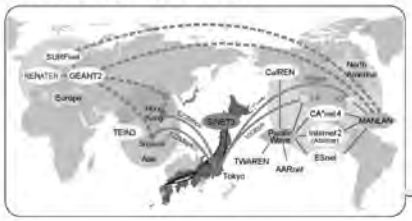
2－4　中村　素典（国立情報学研究所 教授）：
アカデミック・ クラウド・サービス・コンピューティング

2－5　山川　仁子、板橋　秀一（国立情報学研究所 音声メディアグループ）：
学術研究のための音声資源とその利用

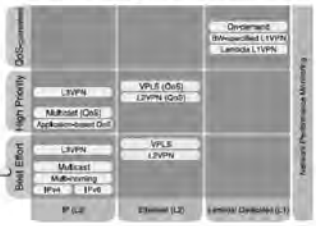
2－6　Helmut Prendinger（国立情報学研究所 准教授）：
Global Lab（グローバルラボ）：
3D インターネットに基づいた参加型科学の基盤

Science Information Network 3

Network Topology of SINET3



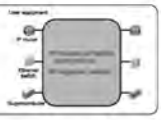
Service Categories in SINET3



SINET3 has five service categories: transfer layer, secure (VPN), quality-of- service (QoS), bandwidth-on-demand (BoD),and network performance monitoring.

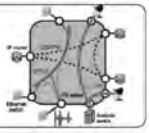
Multiple Layer Services

SINET3 is an integrated network providing all transfer layer services. Users can freely choose the best transfer layer for their applications. SINET3 enables economical service provision and flexible network resource assignment for ever-changing and unpredictable service demands.



Multiple VPN Services

A closed user group environment (virtual private network: VPN) is essential for ensuring the security of collaborative research. Users can choose from L3VPN (IP), L2VPN/VPLS (Ethernet), and L1VPN.

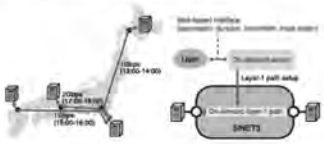


Multiple QoS Services

SINET3 provides QoS by identifying applications, VPNs, and physical/logical ports. Layer-2/3-based QoS has four priority classes: expedited forwarding (EF), network control (NC), assured forwarding (AF), and best effort (BE). Layer-1-based QoS has the smallest packet delay, no delay variance, and no packet loss.

Bandwidth-on-demand (BoD) Services

SINET3 provides bandwidth-on-demand (BoD) services on layer-1. Users can specify destination, duration, bandwidth with a granularity of 150 Mbps, and route option. The BoD server receives reservation requests, schedules accepted reservations, and triggers layer-1 path setup.



Demonstration of L1 BoD
(February 1st, 2008)

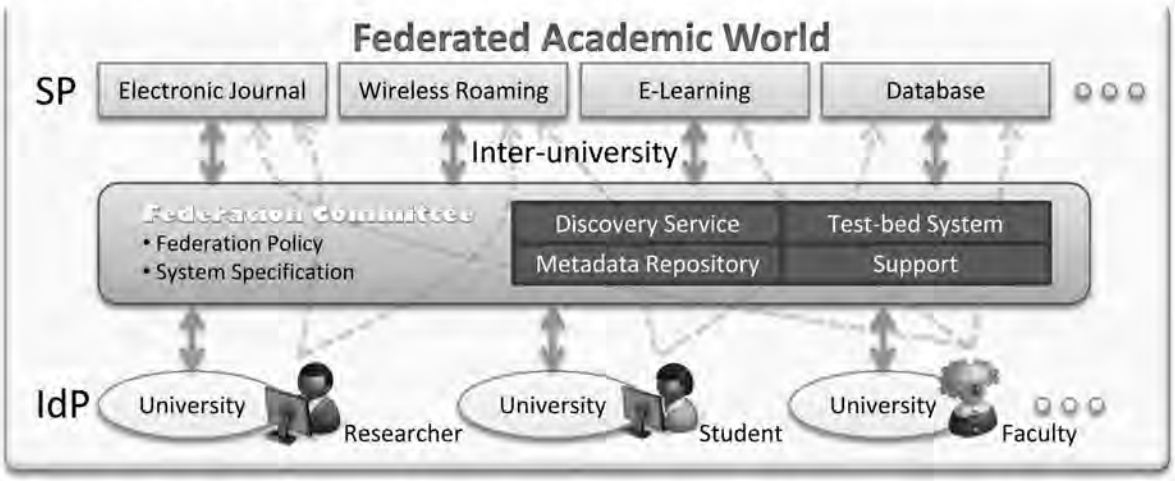
Confirmation of bandwidth reservation

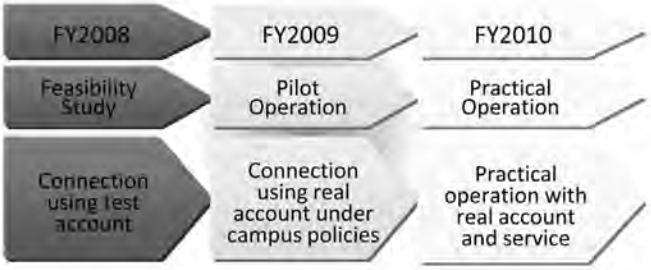
Academic Federated Access Management in Japan

Kazu Yamaji , Toshi Kataoka, Takeshi Nishimura, Masaki Shimaoka, Motonori Nakamura, Noboru Sonehara and Yasuo Okabe

[1] R & D Center for Academic Networks, National Institute of Informatics
[2] Academic Center for Computing and Media Studies, Kyoto University

We are currently promoting the federated identify management which enables a single sign-on to scholarly web resources such as electronic journals and research databases. The environment is based on SAML 2.0 standard and mainly utilizing Shibboleth middleware developed by Internet 2.





Feasibility study of this project has been done in 2008. 30 identify providers and 18 service providers joined to the experiment. Not only connection test each other but also fabric of the federation including basic policy, system architecture and specification were also discussed among participants.

Pilot Operation

Connecting to Product Level Services with Real Account

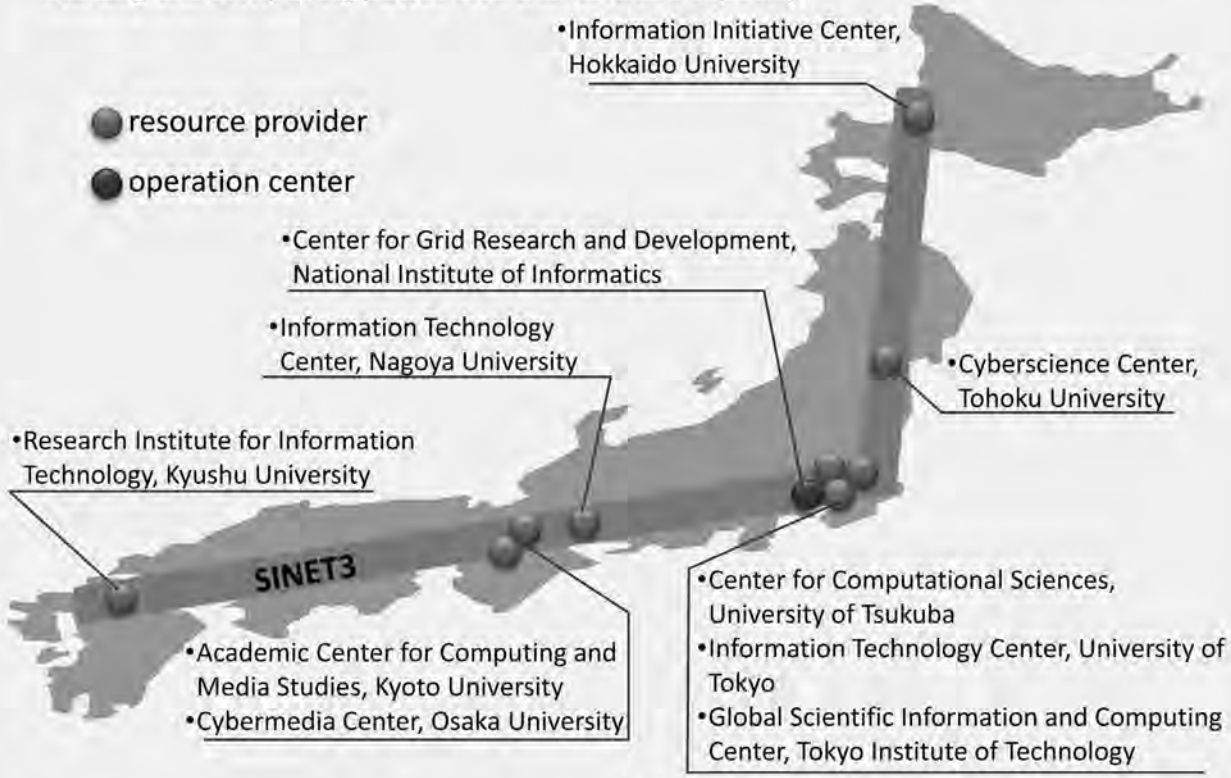
What we do this YEAR

- Documents
  - ✓ Federation Policy, System Specification
  - ✓ Benefit to University Manager, IT section and Libraries
- Event and Training
  - ✓ IdP and SP implementation
  - ✓ Setup round table for IT people and Librarians
- Recruiting
  - ✓ IdP: University, College
  - ✓ SP: Major Publishers, Domestic Services

Academic Grid Infrastructure in Japan

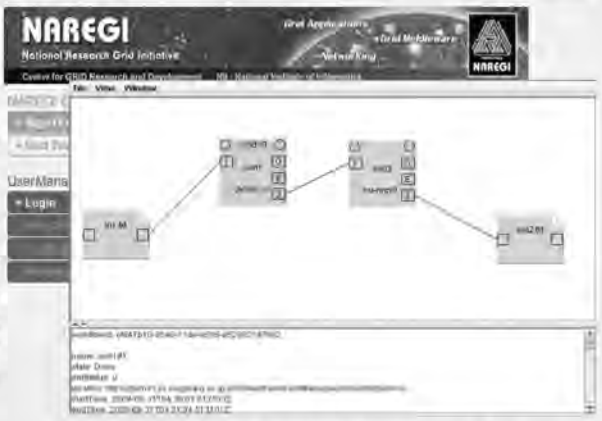
■Overview

Computer centers at nine universities and National Institute of Informatics (NII) started pilot operation of an academic grid infrastructure in Japan. The computer centers play as resource providers offering their high-performance computer systems, and NII plays as an operation center (a helpdesk, VO hosting and a certificate authority) to coordinate grid operation collaborating with the computer centers. SINET3 is used to link high-performance computing systems in the computer centers. Researchers can run their scientific applications on the academic grid infrastructure utilizing the computing power and the network capacity.



■Grid Middleware

The NAREGI middleware integrates widely distributed computing and storage resources in the grid infrastructure as a virtualized single computing environment. The NAREGI middleware is developed as open source software and available at http://middleware.naregi.org/Download/.



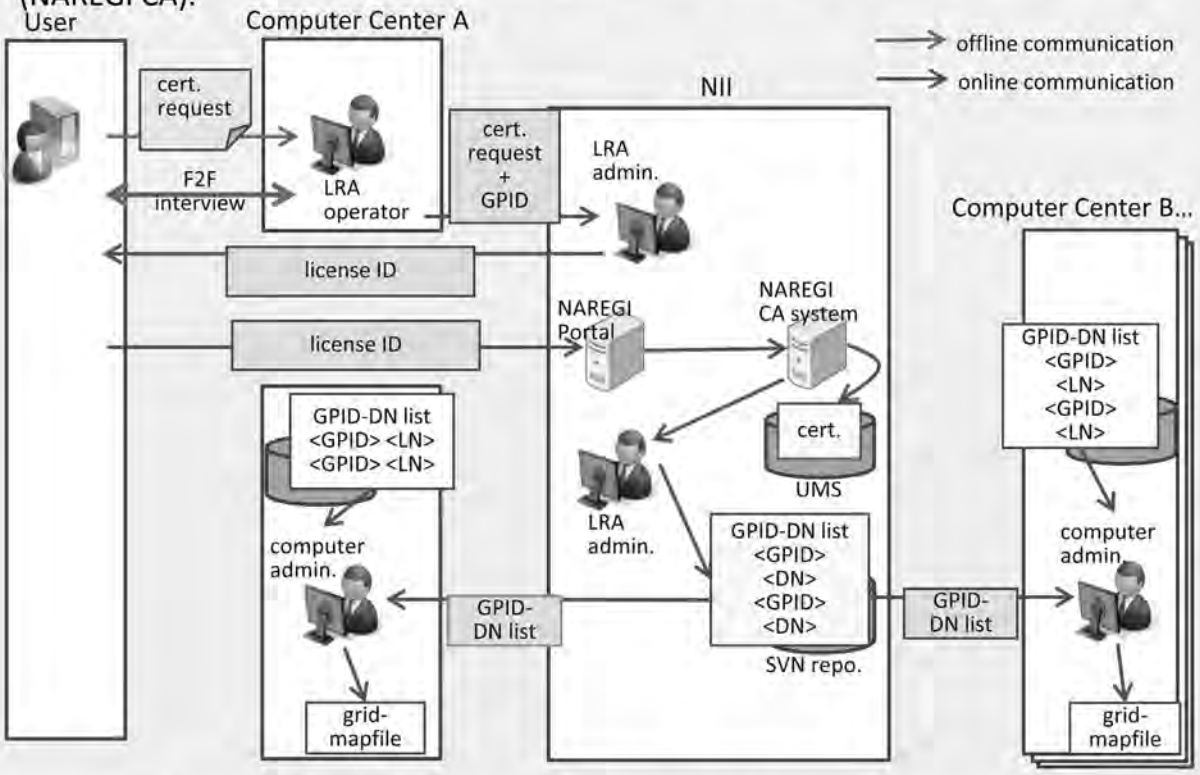
NII

Kento Aida, National Institute of Informatics

Academic Grid Infrastructure in Japan

■User Management

User Management is one of issues in grid operation. Computer centers have their own policies for user registration. PKI is now de facto standard of the user authorization method on the grid. User registration on the grid infrastructure is complicated and forces the user tedious procedures, i.e. the user needs to submit multiple application forms for accounts to multiple computer centers and apply the grid user certificate to a grid certificate authority (CA). Computer centers and NII collaborate to simplify the user registration process on the academic grid infrastructure. The user submits one application form for "the grid pack", a set of accounts of computer centers and a grid user certificate. Then, the user accounts are created in computer centers and the grid user certificate is issued from CA in NII (NAREGI CA).



A procedure for issuing a user certificate and creating grid-mapfile

■More Information: http://www.naregi.org/

NII

Kento Aida, National Institute of Informatics

Towards Constriction of Academic Application Cloud

Motonori Nakamura, National Institute of Informatics

Construct Application Platform and Improved Universal Academic Services over Cloud Server Systems with Inter-University Authentication Cooperation

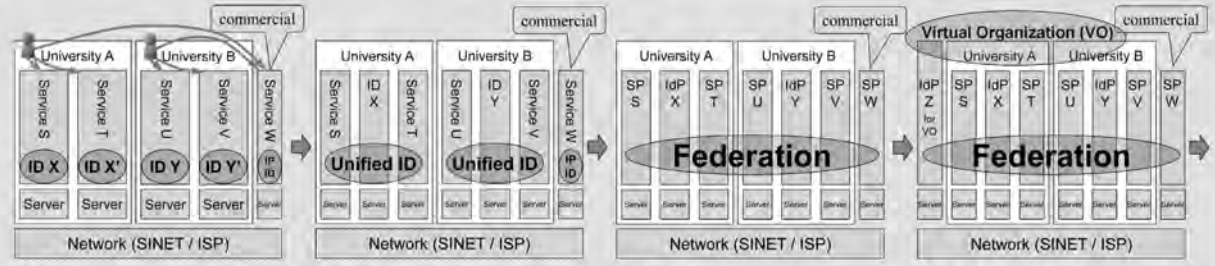
Background

- Services become infrastructure
  - Wide spread as free, Insufficient features / dependability / spam protection
- Increase of operation cost
  - Responsibility for administration, Security management, User support
- Increase of disparity on service quality between universities
  - Demand for varied service, efficiency (cost cut, personnel reduction)
- Appearance of large scale service providers
  - Retrogression to centralization (cost performance), Web2.0
- Distrust of out-sourcing services
  - Continuity, Dependability, Black-Box, Foreign entities, Confidence management

Goal

- Reduce operation cost, Improve dependability
  - Centralizing, Out-Sourcing, Scalability, Appropriate redundancy / compatibility
- Improve averaged service quality, Reduce disparity
  - High availability, Effective virus / spam protection
- Improve level of research / education by service enhancement
  - Expansion of academic service, support for inter-university activities / communities
- Activate creation of new services, Industry-Academia collaboration
  - Utilize mash-up technologies, generation of services with targeting long-tail
- Sustain / Improve technical level of operators, Training (prevent hollowing)
  - White-box, flexibility for customizing / original service (be a Service Delivery Platform)
- Construct distributed services over integrated service platform
  - Regain the initiative

Transition of Service Platform Architecture

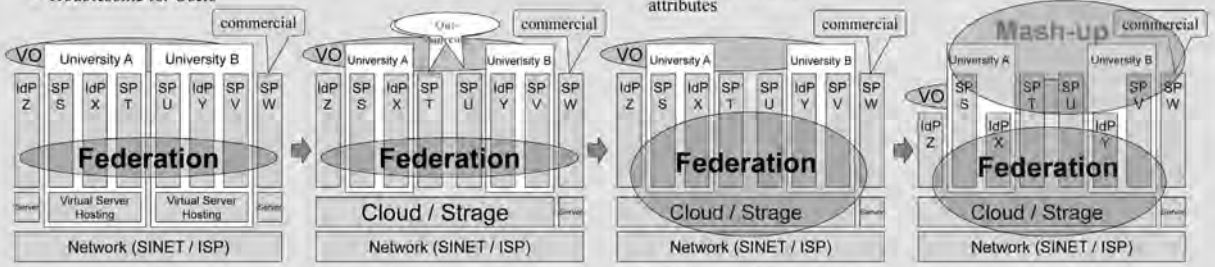


- Many Independent Services
  - Distributed Services (Downsizing)
  - Pure Client-Server Model
- Many IDs and Passwords
  - Troublesome for Users

- Unified ID management
- Single Sign On (SSO) (within an organization)
- E-Journals are still using IP-address based authentication

- Establishing Federation
  - Inter-Organization Authentication Cooperation (Including e-Journal Providers)
  - Shibboleth/SAML for disclosure control of user attributes

- IdP for Virtual Organization (VO)
  - Academic Societies
  - Research Groups
  - Inter-University Projects
- Service Sharing



- Virtualization Technology
- Platform Sharing
  - Cost Reduction

- Cloud Technology / Services
- Out-Sourcing
  - Encourage New Academic Services provided by Commercial

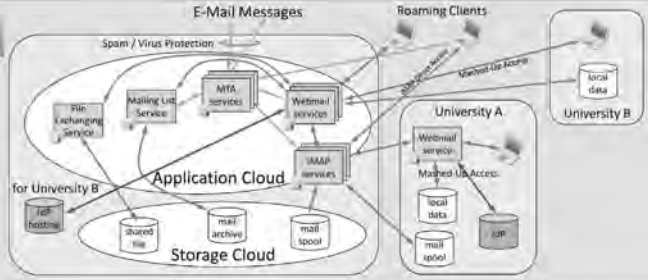
- Could/Storage/Network (VPN) as a SP in the Federation

- Mashed-up services
  - Systematic Cooperation of Applications
- Improving User Experience by application itself

Investigating Academic Service Architectures using Federation Mechanism

- Content Delivery Services
- Network Services (VPN, Roaming, etc.)
- Video Conferencing Services
- E-mail Services
- Community (VO) Supporting Services
- Computation / Storage Services

etc.



Speech Resources for Scientific Research and its Application

NII

Kimiko YAMAKAWA Shuichi ITAHASHI (NII)

NII-SRC Speech Resources Consortium

Objective?

NII has established Speech Resources Consortium (NII-SRC) so as to promote dissemination and distribution of speech resources.

NII-SRC conducts collection, distribution, investigation and research on speech resources (including speech data and software tools) necessary for developing science, education and industry related to speech.

What are we doing?

We contribute to the development of various research including speech recognition and synthesis by collecting and distributing speech corpora or speech databases which are difficult to develop individually.

Another scientific contribution by supplying valuable material for phonetics and sociolinguistics by preserving dialects and minority languages.

1. What is "Speech Corpus/Corpora"

What is corpus/corpora?

A corpus means a systematic collection of data for research with some additional information to be used for research.

(Ex.) Speech corpus, text corpus, multimedia corpus, image corpus, etc.

Variety and use of speech corpora

【Use】 Analysis, synthesis, recognition of speech; analysis of discourse and dialects; preservation of languages, etc.

【Variety】 Isolated words, continuous speech, read speech, dialogues, dialects, multilingual speech; speech by non-native speakers, infants, aged people; speech in noisy or reverberant environments.

Recording media of speech corpora

The major recording media are used though it varies according to the use or data size. DVD-R is the most common currently. On-line distribution will be available soon.

【Recording media for speech corpora】

CD-R, DVD-R, HDD, DAT, LD, etc.

Contents of speech corpora

Analysis data

Video

Transcription data

2. What is SRC?

Why speech corpora, now?

- Development of speech processing technology
- Quantitative research in linguistics-related areas
- Importance of preserving languages and dialects

Massive speech data of various kinds necessary

Problems of speech corpora

- Most corpora are developed for a project.
- It requires cost, time and labor to create.
- Expensive.
- Not open to the public.

A common framework is required for creation, collection, accumulation, distribution and sharing

Speech Resources Consortium (NII-SRC)

Launched by NII in 2006 in order to collect, manage, and distribute various speech corpora.

Currently, 31 corpora are available from NII-SRC.

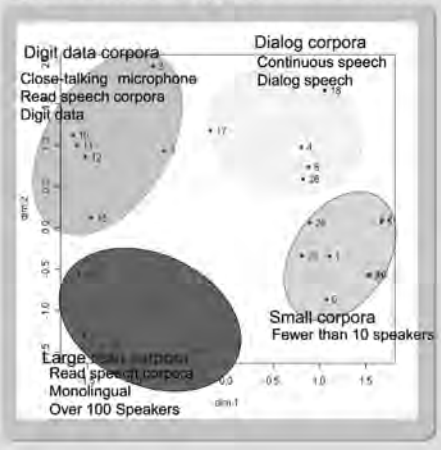
Speech-related Organizations in the World.

3. Categorization of speech corpora

Corpus attributes (8 attributes and 58 items)

Attribute		Item
Input device	7 items	Type of input device (ex. Desk-top microphone)
Input environment	5 items	Recording environment (ex. Soundproof room)
Number of speakers	10 items	Number of speakers
Speaking style	4 items	Style of speech (ex. Continuous speech)
Speech mode	5 items	Speech mode (ex. dialog, read speech)
Data mode	9 items	Other information (ex. Sampling frequency)
Language	4 items	Type of language (ex. Monolingual)
Purpose	14 items	Keyword for use or development (ex. Recognition)

4. Corpus similarity visualization



Speech Resources Consortium, National Institute of Informatics

URI: http://research.nii.ac.jp/src/eng E-mail: src@nii.ac.jp

Participatory Science & Live Collaboration in the 3D Internet

Helmut PRENDINGER (National Institute of Informatics)

NII 連絡先: Helmut PRENDINGER／ 国立情報学研究所 コンテンツ科学研究系 准教授
TEL : 03-4212-2650 FAX : 03-4212-2650 Email : helmut@nii.ac.jp

ポスター・
デモセッション

3. IT リスク管理

3－1　藤井　孝之(*1)・影山　正幸(*1)・蒲生　昌志(*2)・
金藤　浩司(*1)・椿　　広計(*1)
（*1: 統計数理研究所　*2: 産業技術総合研究所）：
化学物質のリスクトレードオフ解析

3－2　藤井　陽介・逸見　昌之・藤田　利治（統計数理研究所）：
臨床試験における療法間の統計的交互作用の評価

3－3　梶山　朋子（早稲田大学人間科学部 助手）：
子どもの情報分析力強化を支援する楽しい Web 特性学習
システムの開発

3－4　庄司　勇木（総合研究大学院大学複合科学研究科情報学専攻）：
ブロードバンド・インフラ整備における投資リスクと
公共政策

Statistical analysis in risk assessment of chemicals

Takayuki Fujii(*1), Masayuki Kageyama(*1), Masashi Gamou(*2), Koji Kanefuji(*1), and Hiroe Tsubaki(*1)

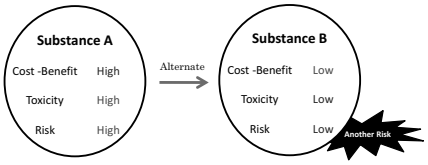
*1:The institute of statistical mathematics *2:National Institute of Advanced Industrial Science and Technology

OUTLINE

Our aim is to construct a statistical model and the inference algorithm that provide a theoretical proof for the risk assessment of chemicals. In this talk, we introduce a graphical modeling that is suitable for the representation of the causal relations with uncertainty. It becomes better combining existing statistical tools such as EM-algorism, latent variables and so on. Our approach is challenging, but substantial progress can be made.

Risk Trade-off of Chemicals

Once we find toxicity of the substance A, ….



Another risk may offset the reduction in the target risk

Risk Trade-Off

In order to promote appropriate assessment and management of chemical risks, it is necessary to construct the evaluation system which makes it possible to quantify and compare the risk of the substance and its alternative.

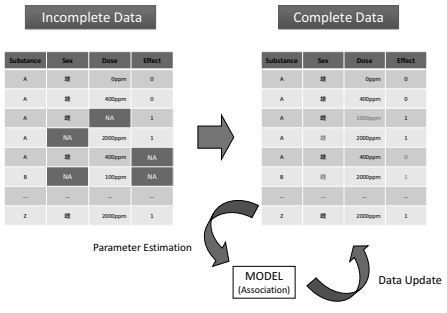
Statistical Tools

We use a graphical model to describe the relativity among the markers.

Extensions

EM algorithm is a technique for analysing the data with missing value.

EM Algorithm

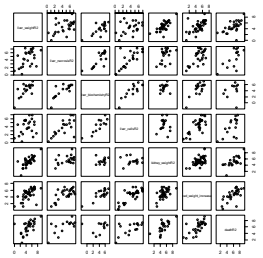


The optimal model is set for the incomplete problem.

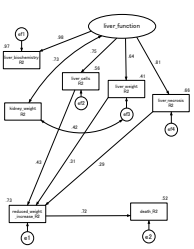
Results

The followings are some analytical Results for the chemical toxicity effect of liver and Kidney by rat's oral ingestion.

1. Scatter Plot



2. Latent Model (AIC=58.453)



Pass-Coefficient

			MLE	S.D.	Test Statistics	Prob.
Liver_necro.R2	<---	Liver function	1.559	.262	5.947	***
Liver_colliR2	<---	Liver function	1.303	.249	5.242	***
Liver_weightR2	<---	Liver function	1.109	.229	4.849	***
Weight_Inc.R2	<---	Liver_colliR2	.422	.123	3.417	***
Weight_Inc.R2	<---	Liver_weightR2	.303	.106	2.849	.004
Weight_IncR2	<---	Liver_necro.R2	.259	.120	2.158	.031
Liver_Inc.R2	<---	Liver function	2.050	.287	7.139	***
DeathR2	<---	Weight_Inc.R2	.750	.123	6.119	***

Covariance

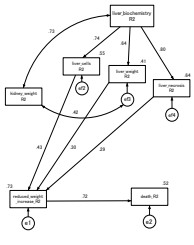
			MLE	S.D.	Test Statistics	Prob.
Kidney_weightR2	<-->	ef3	.859	.319	2.696	.007
Kidney_weightR2	<-->	Liver_function	1.120	.201	5.578	***

Variance

	MLE	S.D.	Test Statistics	Prob.
Liver function	1.000			
ef3	1.785	.427	4.179	***
ef2	1.357	.439	3.092	.002
e4	1.274	.457	2.788	.005
e1	.811	.209	3.881	***
e2	1.532	.377	4.066	***
ef1	.134	.476	.281	.779
Kidney weightR2	2.367	.452	5.240	***

The error variance of the liver biochemistry is not significant. Hence we propose the following model revision.

3. Revision of Model (AIC=56.523)



Pass Coefficient

			MLE	S.D.	Test Statistics	Prob.
Liver_colliR2	<---	Liver_biocR2	.619	.113	5.456	***
Liver_weightR2	<---	Liver_biocR2	.530	.106	4.991	***
Liver_necrosisR2	<---	Liver_biocR2	.724	.114	6.426	***
Weight_Inc.R2	<---	Liver_colliR2	.423	.121	3.497	***
Weight_Inc.R2	<---	Liver_necrosisR2	.261	.118	2.217	.027
Weight_Inc.R2	<---	Liver_weightR2	.302	.105	2.866	.004
DeathR2	<---	Weight_Inc.R2	.750	.123	6.113	***

Covariance

			MLE	S.D.	Test Statistics	Prob.
Kidney_weightR2	<-->	ef3	.860	.307	2.801	.005
Kidney_weightR2	<-->	Liver_bioc.R2	2.335	.568	4.111	***

Variance

	MLE	S.D.	Test Statistics	Prob.
Liver_biochemistryR2	4.379	1.021	4.289	***
ef3	1.784	.417	4.281	***
ef2	1.383	.425	3.252	.001
ef4	1.260	.424	3.188	.001
e1	.808	.209	3.874	***
e2	1.532	.377	4.066	***
Kidney_weightR2	2.363	.451	5.238	***

Acknowledgment

This work was supported by NEDO(The New Energy and Industrial Technology Development Organization) of Japan.

Evaluating Statistical Interaction between Various Therapy in Clinical Trials

Yosuke FUJII※1 2, Masayuki HENMI1 2, Toshiharu FUJITA1 2
1 The Institute of Statistical Mathematics, Japan; 2 The Graduate University for Advanced Studies, Japan
※ Correspondence to: 4-6-7 Minami-Azabu, Minato-ku, Tokyo, Japan E-mail: yfujii@ism.ac.jp

INTRODUCTION

●The Interaction between the mono and combination therapy

The feature of pre-marketing clinical trial for the antihypertensive drug is that not only monotherapy trials (comparative study concerning using testing antihypertensive) but combination therapy trials (comparative study concerning co-administration with other antihypertensive) is often done. It can be a practical concern to know how different the degree of efficacy or safety is between the two therapies, that is, to investigate the interaction between the two factors, the status of mono or combined and the treatment.

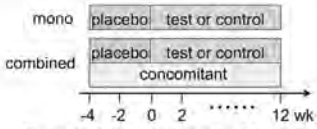


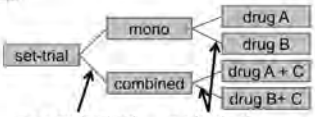
Figure 1 : Administration schedule

●Trial registration is not randomized

It should be noted that the registration in each trial (mono or combined) may be not randomized and be selective (Figure 2). The factor of selectivity may be

- ✓ background
- ✓ laboratory test values
- ✓ previous disease or contraindication disease for concomitant drug

Doctors may register the subject out of consideration of these factor. In fact, patient with experience of diuretic before trials tend to entry into combination therapy trials. If interest is on safety and efficacy difference between mono- and combined, that is interaction, the unbalance could yield bias, and that's why it should be analyzed in consideration for this unbalance.



test : drug A (ex : CCB)
control : drug B (ex :β)
concomitant : drug C (ex : diuretic)
Figure 2 : Trial registration and allocation

OBJECTIVES

We aim to evaluate the interaction between the two factors above (i.e. the status of mono or combined and the treatment) by adjusting for patients' covariates which may affect the registration in the each trial. In this poster, outcome is odds ratio about worsening of the neuropsychiatric symptoms as against before administration, included newly symptoms.

METHODS

Notation

i : patient ID ($i = 1, \ldots, n$)
S : indicator variable about the trials (0: mono, 1: combined)
T : indicator variable about drug group (0: control, 1: test)
$Y^{(st)}$: potential outcome
$\beta = (\beta_{00}\ \beta_{01}\ \beta_{10}\ \beta_{11})^T$: expectation of potential outcome, $\beta_{st} = E[Y_{st}]$
$\boldsymbol{X}$: observed covariate vector
$e_1(\boldsymbol{X}) = \Pr(S = 1|\boldsymbol{X})$: propensity score about the registration into the combi- trial
$e_2(S) = \Pr(T = 1|S)$: probability about the allocation into the test group
$m_{st}(\boldsymbol{X}) = E[Y^{(st)}|S = s, T = t, \boldsymbol{X}]$
: regression of the outcome on $\boldsymbol{X}$ in each trial and group

$e_1(\boldsymbol{X})$, $e_2(S)$ and $m_{st}(\boldsymbol{X})$ are estimated from observed data by assuming that parametric model $e_1(\boldsymbol{X};\alpha_1)$, $e_2(S;\alpha_2)$ and $m_{st}(\boldsymbol{X};\alpha_3)$. Additionally, estimated these statistics $\hat{e}_{1,i} = e_1(\boldsymbol{X}_i;\hat{\alpha}_1)$, $\hat{e}_{2,i} = e_2(S_i;\hat{\alpha}_2)$ and $\hat{m}_{st,i} = m_{st}(\boldsymbol{X}_i;\hat{\alpha}_3)$ for all i.

Average Causal Effect and Their Interaction

average causal effect about mono and combined, and their interaction

- average causal effect $\mu_s = \text{logit}(\beta_{s1}) - \text{logit}(\beta_{s0})$
- interaction $\Delta = \mu_1 - \mu_0$

Strongly Ignorable Treatment Assignment [SITA]

$(Y^{(00)}, Y^{(01)}, Y^{(10)}, Y^{(11)}) \perp S \mid \boldsymbol{X}$ ····· assumption about trial registration
$(Y^{(00)}, Y^{(01)}, Y^{(10)}, Y^{(11)}, \boldsymbol{X}) \perp T \mid S$ ··· assumption about treatment allocation

Estimator of the Average Causal Effect

■ Horovitz-Thompson form estimator [HT]

$$\hat{\beta}_{00} = \frac{1}{n}\sum_i \frac{(1-S_i)(1-T_i)Y_i^{(00)}}{(1-\hat{e}_{1,i})(1-\hat{e}_{2,i})}, \quad \hat{\beta}_{01} = \frac{1}{n}\sum_i \frac{(1-S_i)T_iY_i^{(01)}}{(1-\hat{e}_{1,i})\hat{e}_{2,i}},$$
$$\hat{\beta}_{10} = \frac{1}{n}\sum_i \frac{S_i(1-T_i)Y_i^{(10)}}{\hat{e}_{1,i}(1-\hat{e}_{2,i})}, \quad \hat{\beta}_{11} = \frac{1}{n}\sum_i \frac{S_iT_iY_i^{(11)}}{\hat{e}_{1,i}\hat{e}_{2,i}}$$

Other Type of Estimators

■ Standardized estimator [STD]

$$\hat{\beta}_{11} = \left(\sum_i \frac{S_iT_i}{\hat{e}_{1,i}\hat{e}_{2,i}}\right)^{-1}\sum_i \frac{S_iT_iY_i^{(11)}}{\hat{e}_{1,i}\hat{e}_{2,i}}$$

■ Doubly robust estimator [DR]

$$\hat{\beta}_{11} = \frac{1}{n}\sum_i \left(\frac{S_iT_iY_i^{(11)}}{\hat{e}_{1,i}\hat{e}_{2,i}} - \frac{S_iT_i - \hat{e}_{1i}\hat{e}_{2i}}{\hat{e}_{1i}\hat{e}_{2i}}\hat{m}_{11,i}\right)$$

$\hat{\beta}_{00}$, $\hat{\beta}_{01}$, $\hat{\beta}_{10}$ are derived in a similar way

CASE EXAMPLE

- Phase III clinical trial(drugs are in Figure 2)
- Sample size: 383 (mono is 199, combined is 184)
- Event: worsening of the neuropsychiatric symptoms (binary data); against before administration included newly symptoms
- Covariate: drug experience about diuretic before trials, abnormality of total cholesterol, complication of renal dysfunction
- Compare with estimate simply from 2 × 2 table(crude analysis)

Table I: 2 by 2 table [count *(row proportion)*]

trial	group	outcome: event	outcome: non-event	sum
mono	test	14 *(0.13)*	90 *(0.87)*	104
	control	18 *(0.19)*	77 *(0.81)*	95
	sum	32 *(0.16)*	167 *(0.84)*	199
comb	test	9 *(0.10)*	85 *(0.90)*	94
	control	15 *(0.17)*	75 *(0.83)*	90
	sum	24 *(0.13)*	160 *(0.87)*	184

Table II: Estimate of Average Causal Effects [translation to odds ratios]

trial	methods	odds ratios(95% CL)
mono	crude	0.67 (0.31, 1.43)
	adj: HT	0.98 (0.37, 2.64)
	adj: STD	0.98 (0.37, 2.60)
	adj: DR	1.02 (0.41, 2.53)
comb	crude	0.53 (0.22, 1.28)
	adj: HT	0.49 (0.17, 1.39)
	adj: STD	0.44 (0.16, 1.27)
	adj: DR	0.44 (0.16, 1.20)

The adjustment for mono-therapy is large, so much so that interaction is adjusted widely. However, because the population for adjustment analysis is different from one of crude analysis, we cannot simply compare adjustment with crude about average causal effects. The estimates of three adjustment methods show a similar trend.

Table III: Estimate of Interaction [translation to odds ratios]

methods	odds ratios(95% CL)
crude	※0.80 (0.25, 2.55)
adj: HT	0.50 (0.12, 2.08)
adj: STD	0.45 (0.11, 1.89)
adj: DR	0.43 (0.11, 1.66)

※ comb / mono = 0.53 / 0.67 = 0.80

CONCLUSION and FUTURE WORK

As the usual method of propensity score weighting, our method is useful in that it allows for the interaction between the two factors above and the patients' covariates, and avoids modeling the association between the outcome and the patients' covariates. The propensity score in our problem is a little more complicated, but it can be easily estimated due to the hierarchical structure of registration and treatment allocation. Our future works are below.

- Sensitive analysis : If unmeasured confounding factor is exist, estimators are …
- Non-randomized trial : If treatment allocation is non-randomized, SITA is …
- Restricted population : If interested population is restricted, estimators are …

REFERENCE

1. Bang, H., Robins, J. M. (2005). Doubly Robust Estimation in Missing Data and Causal Inference Models. *Biometrics* **61**: 962–72.
2. Lunceford, J. K., Davidian, M. (2004). Stratification and weighting via the propensity score in estimation of causal treatment effects: a comparative study. *Statistics in Medicine* **23**: 2937–60.

An Enjoyable System for Learning Website Attributes to Foster Children's Information Literacy

Tomoko Kajiyama* *Faculty of Human Sciences, Waseda University

BACKGROUND

Lights and shadows of the Internet
- large amount of and various types of information
- hard to realize risks due to both parties' anonymity
- easy and convenient, but risks need to be determined

Existing techniques to protect children from harmful websites
a) Website filtering
  - just avoid and give no chance to determine whether websites are dangerous or safe
  - enable to produce immunity in harmful websites
b) Educational contents provided by police or schools
  - seem impractical situation
  - enable to understand coping process

MOTIVATION

Problems of using existing techniques
- children cannot live in safe space permanently
- difficult to foster their information literacy
  e.g., scissors are dangerous, but
    - parents explain why they are dangerous
    - children learn how to use

What is real education about information literacy?
- experts should explain why websites are dangerous or safe
- children should access all websites to realize how to prevent traps

OBJECTIVE

Propose enjoyable system for learning website attributes to foster children's information literacy

Ring Retrieval + Risk Rating > filtering, educational contents

System gives chances
- to understanding website features and determining risks
- to foster children's information literacy and improve their decision-making ability

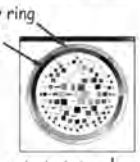
System requirement
- provide website features with various kinds of attributes
- inform websites' risk darkly
- tell children present level of their information literacy
- integrate real websites and educational contents

RING RETRIEVAL

Graphical User Interface
Category ring line up attribute names
- use for starting searches with attributes

Key ring line up attribute values
- search keys derived from the attribute values on bottom part of key rings
- adjust search keys by rotating key rings
- range of search keys are in proportion to number of key rings
- outer key ring has higher priority

"Concentric Ring View"



rotate 'color' ring

click 'atmosphere'

Display retrieved results
- arranged in concentric circles according to search key values and their priorities
- higher ranked objects are larger and shown closer to center
- details are displayed by placing cursor on image

Children can
- use enjoyable and excitedly with easy operations and reasonable screen transition
- browse and compare many websites simultaneously
- browse websites from various angle and understand their features

RISK RATING

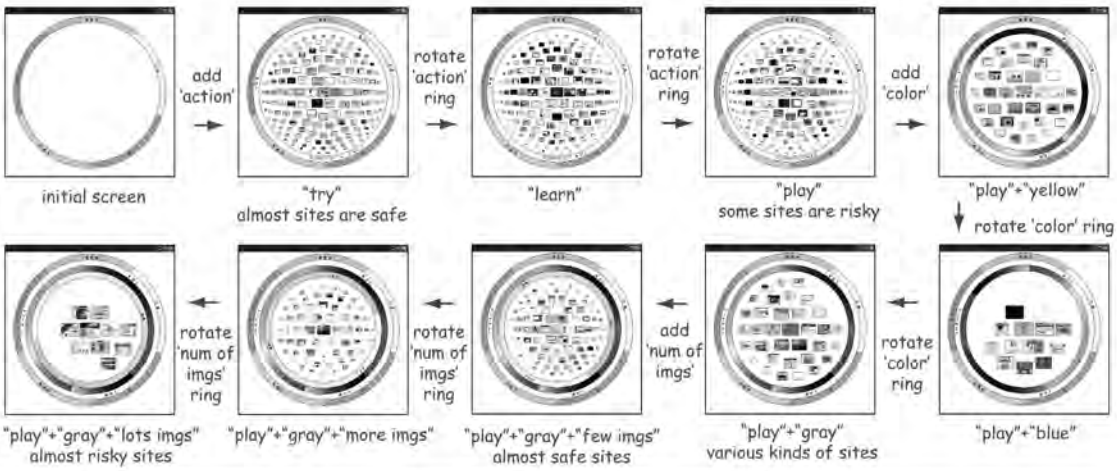
Algorithm
a) link websites with real world
  - Act on Specified Commercial Transactions
  company name, delegate's name, address, phone number, email address
b) link, text and image analysis in websites
  - html structures, writing skill, taboo words, last update, and so on

Children can
- understand risk of websites by themselves
- notice about own level of information literacy

PROTOTYPE

1,200 websites
(safe) 400 from kids' portal site
400 from general portal site
200 for over 20 like prize
(risky) 200 warning from police

Five attributes
- action (learn, try, play)
- color (two feature colors)
- atmosphere (pastel tone - dark)
- number of images (small - large)
- life cycle (short - long)



International Workshop on Information Systems for Social Innovation 2009

Investment Risks and the Public Policy to expand the broadband network in Japan

Yuki Shoji
The Graduate University of Advanced Studies

The Present Status of Broadband in Japan and the Purpose of this Presentation

In 2001, NTT started FTTH services which provide higher transmission speed and are more stable than DSL. Consequently, DSL subscribers gradually have been migrating to FTTH and in 2008, FTTH subscribers exceeded DSL subscribers. Providing FTTH services needs huge investment. Therefore, only a few operators can enter the market. In the green area of the map, NTT is the sole provider of FTTH service. In the red area, power utility companies constructed their own network and entered the markets.

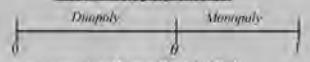
Some operators insist that NTT have to open their FTTH network to new entrants (i.e. service competition). On the contrary, NTT insists that such open network policy will harm the infrastructure competition in red areas. In this presentation, the characteristics of infrastructure competition and service competition are examined by using an economic model in order to consider FTTH competition policy.

The Cournot Model of Broadband Competition

Outline of the Model: To analyze a geometrically asymmetric competition of broadband market, the model assumes that incumbent operator and an new entrant play two stages of Cournot duopoly game in a linear uniform demand market.

Definition of the Model

Linear Duopoly Market



q_D: quantity of incumbent in [0,θ]
q_E: quantity of new entrantin [0,θ]
Demand Function: $p=a-1/\theta(q_D+q_E)$

Two stage game

First Stage: The new entrant determines service area (θ)
Second Stage: The incumbent and the entrant simultaneously determine their price and quantity produced

Cost of both firms

Marginal Cost: c_D, c_E
Fixed Cost: F0

Calculation of the Model

Profit Functions

$$\pi_D=\frac{1}{\theta}\left\{a-\frac{1}{\theta}(q_D+q_E)-c_D\right\}q_D+\frac{1-\theta}{\theta}\left\{a-\frac{1}{\theta}(q_D+q_E)-c_D\right\}q_E$$

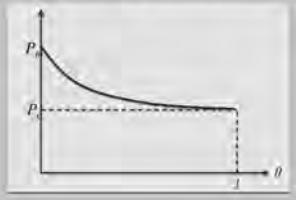
$$\pi_E=\frac{1}{\theta}\left\{a-\frac{1}{\theta}(q_D+q_E)-c_E\right\}q_E-F\cdot\theta$$

Reaction Functions

$$q_D=R_D(q_E)=\frac{-(2-\theta)}{2}q_E+\frac{\theta(a-c_D)}{2}$$

$$q_E=R_E(q_D)=\frac{-1}{2}q_D+\frac{\theta(a-c_E)}{2}$$

Relation between Price and Area Coverage

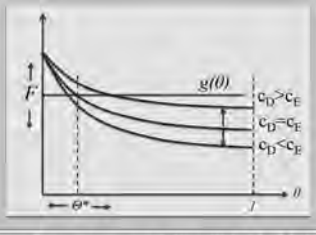


Conclusion of the Model

Decision of Entrant's Area Coverage (θ*)

$$\frac{\partial\pi_E}{\partial\theta}=\frac{(2-\theta)}{(2+\theta)^3}(a+c_D-2c_E)^2-F=0$$

$$g(\theta)=\frac{(2-\theta)}{(2+\theta)^3}(a+c_D-2c_E)^2=F$$



Entrant's area coverage (θ*) will be decided by :
Fixed Cost: F
Marginal Cost: c_D, c_E

Investment Risks and the Public Policy

Measurement of Investment Risks

There are many methodologies to measure investment risks. NPV is one of the major methodologies.

$$NPV-I=\sum_t\frac{Cf_D^t}{(1+r)^t}$$

NPV: Net Present Value I: Investment Cf: Cash Flow

In our simplified static model, the one period profits of both firms "π_i" is used as substitute for the cash flow.

Profit Function of the Stage 2 Equilibrium

$$\pi_D=\frac{\{a+\theta c_E-(1+\theta)c_D\}^2}{(\theta+2)^2}$$

$$\pi_E=\frac{\theta(a+c_D-2c_E)}{(2+\theta)^2}$$

Service Competition vs. Infrastructure Competition

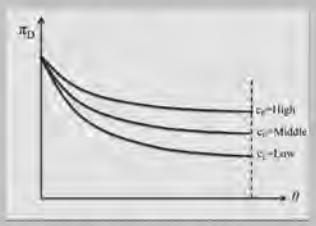
The Model shows relationship between the profit , investment and the marginal costs. The investment and marginal costs depend on whether the entrant constructs network by himself (Infrastructure Competition) or rent it from the incumbent (Service Competition).

	Investment	Marginal Cost
Service Comp.	Low	High
Infra-Comp	High	Low

Benchmark Assumptions

a=1, c_D=1, c_E(High)=1.2, c_E(Middle)=1, c_E(Low)=0.8

The Results of Simulation



The results of benchmark model imply that the low marginal cost which is realized by infrastructure competition may cause profits decline of the incumbent. This may reduce incentive of incumbent for further investment because of the risks of its return.

ポスター・
デモセッション

4. セキュリティと社会

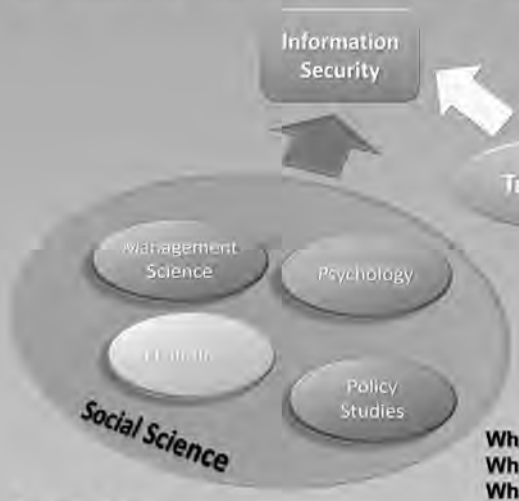
4－1　Gerhard Schneider（フライブルク大学教授チーフインフォメーションオフィサー）：
Security and Society bridging the Gap between Humanities and Technical Sciences

4－2　竹村　敏彦（関西大学ソシオネットワーク戦略研究機構 助教）：
情報セキュリティに対する経済学的接近

An Economic Approach to Issues on the Information Security

Toshihiko Takemura, Ph.D., Assistant Professor
The Research Institute for Socionetwork Strategies
takemura@rcss.kansai-u.ac.jp
http://www.rcss.kansai-u.ac.jp/~takemura/

Significance from the Viewpoint of Economics



Why Economics?
Why Psychology?
Why Management Science?

Themes

Economic Effects on Information Security
- Economic Loss by Information Security Incidents
- Positive Effect of Strategic Information Security Investment
- Inventive Mechanism to Invest in Information Security

Economic Behavior on Information Security Countermeasures
- Awareness
- Communication

Information Security Management System
- Information Security Management System
- Business Continuity Management System

Economic Impact of Government etc

ABSTRACT

In this work, from the viewpoint of economics, the author analyzes the interrelationship between information security countermeasures and economic activities by statistical methods. The sophisticated micro data set in this work, which includes countermeasures, (psychological) awareness on information security and various other attributes, is collected through a Web-based survey that uses sophisticated social investigation methods.

[URL: http://www.rcss.kansai-u.ac.jp/DPS/DPS_E.html]

Main actors dealing with the information security policy and countermeasures in Japan

	URL	Main Objective
NISC	http://www.nisc.go.jp/	Information security policy
MIC	http://www.soumu.go.jp/	Information security policy
METI	http://www.meti.go.jp/	Information security policy
CCC	https://www.ccc.go.jp/	Counter-bot measures
JADAC	http://www.dekyo.or.jp/	Countermeasures against unsolicited email
IPA	http://www.ipa.go.jp/	Countermeasures against computer viruses
JVN	http://jvn.jp/	Provision of information on vulnerabilities
JNSA	http://www.jnsa.org/	Countermeasures on network security
NPA	http://www.npa.go.jp/	Countermeasures against cyber-crimes

Framework

Economic Models
- Investigating interrelation between countermeasures and effects that firm improves market value based on the idea of intangible assets in Brynjolfsson et al. (2002)
- Examinating whether workers' awareness of information security is different in its attributes or not

Statistical Tools
- Logistic Regression Analysis
- Analysis of Covariance Structure
- Analysis of Variance Based on a Non-Parametric Method

Some Findings

- There are positive relationships between the expected effects and some management countermeasures on information security such as information sharing and education
- Human resources and information sharing are the important two factors regarding the security system in the firm
- Workers' awareness of information security is different in its attributes such as organizational attributes and the education about information security countermeasures

A Keyword is "Education"