

A Proposal of a Simple and Secure Statistical Processing System using Secret Sharing

Kiyomi Shirakawa*, Ken Nakamatsu, Koji Chida***, Satoshi Takahashi*** and
Yutaka Abe******

*** Hitotsubashi University / National Statistics Center,
kshirakawa@ier.hit-u.ac.jp**

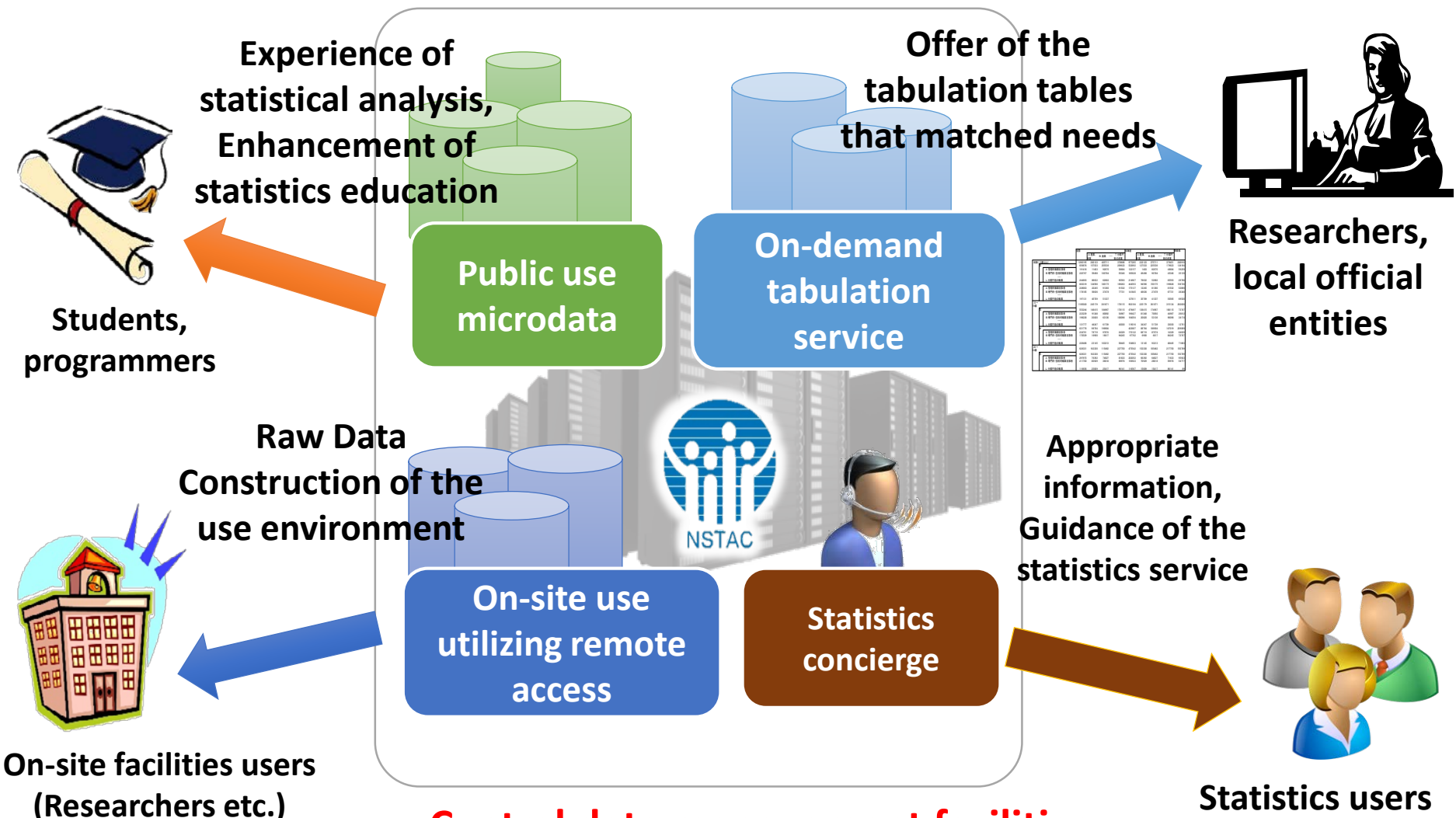
**** Takumi Information Technology Corporation,
ken.nakamatsu@takumi-it.co.jp**

***** NTT Secure Platform Laboratories,
{chida.koji, takahashi.s} @lab.ntt.co.jp**

****** National Statistics Center,
yabe3@nstac.go.jp**

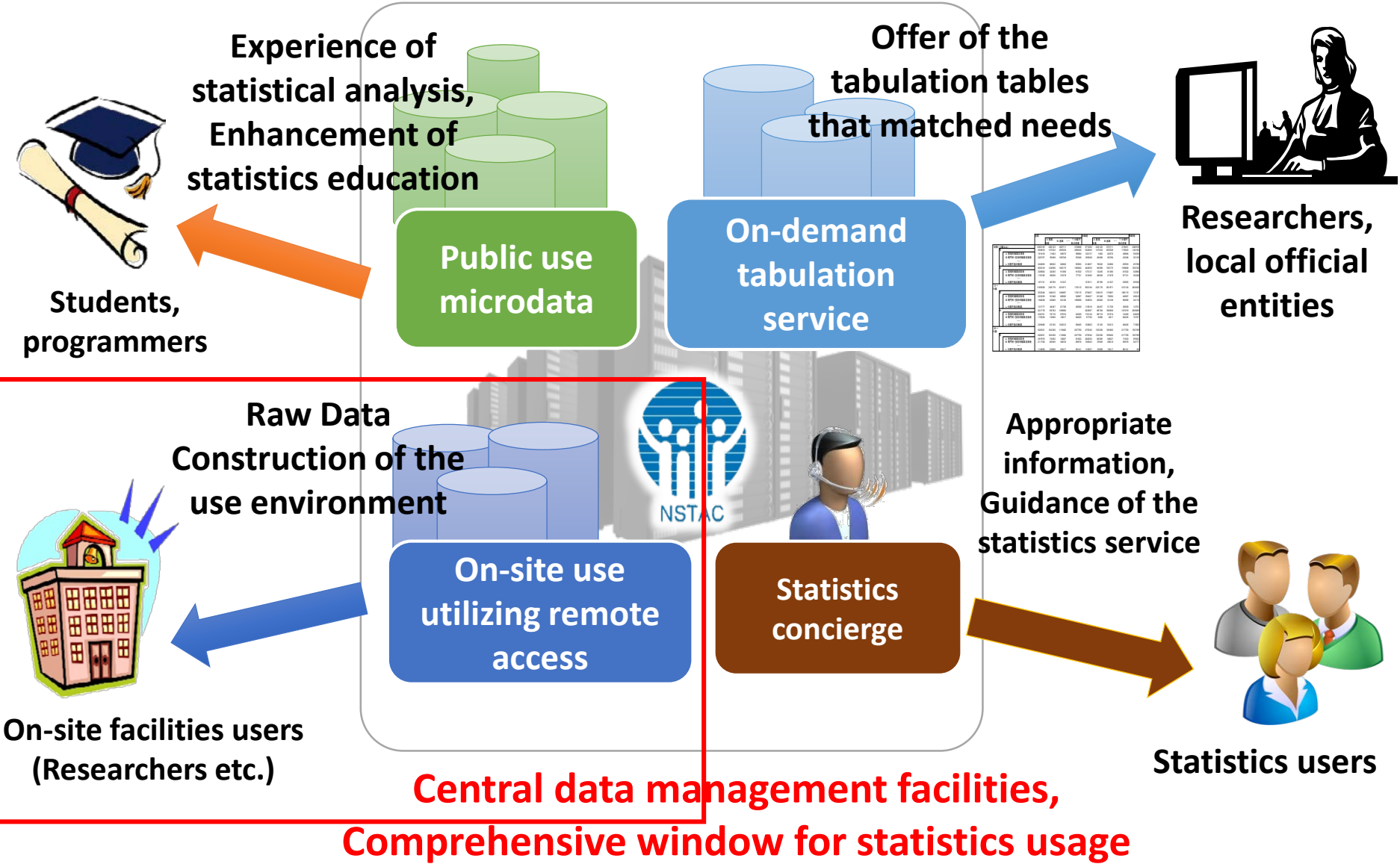
- 1. Four challenges of the National Statistics Center (NSTAC)**
- 2. Outline of τ -ARGUS**
- 3. What's Secure Computation?**
- 4. Demonstration**
- 5. Conclusions and Future works**

1. Four challenges of the NSTAC



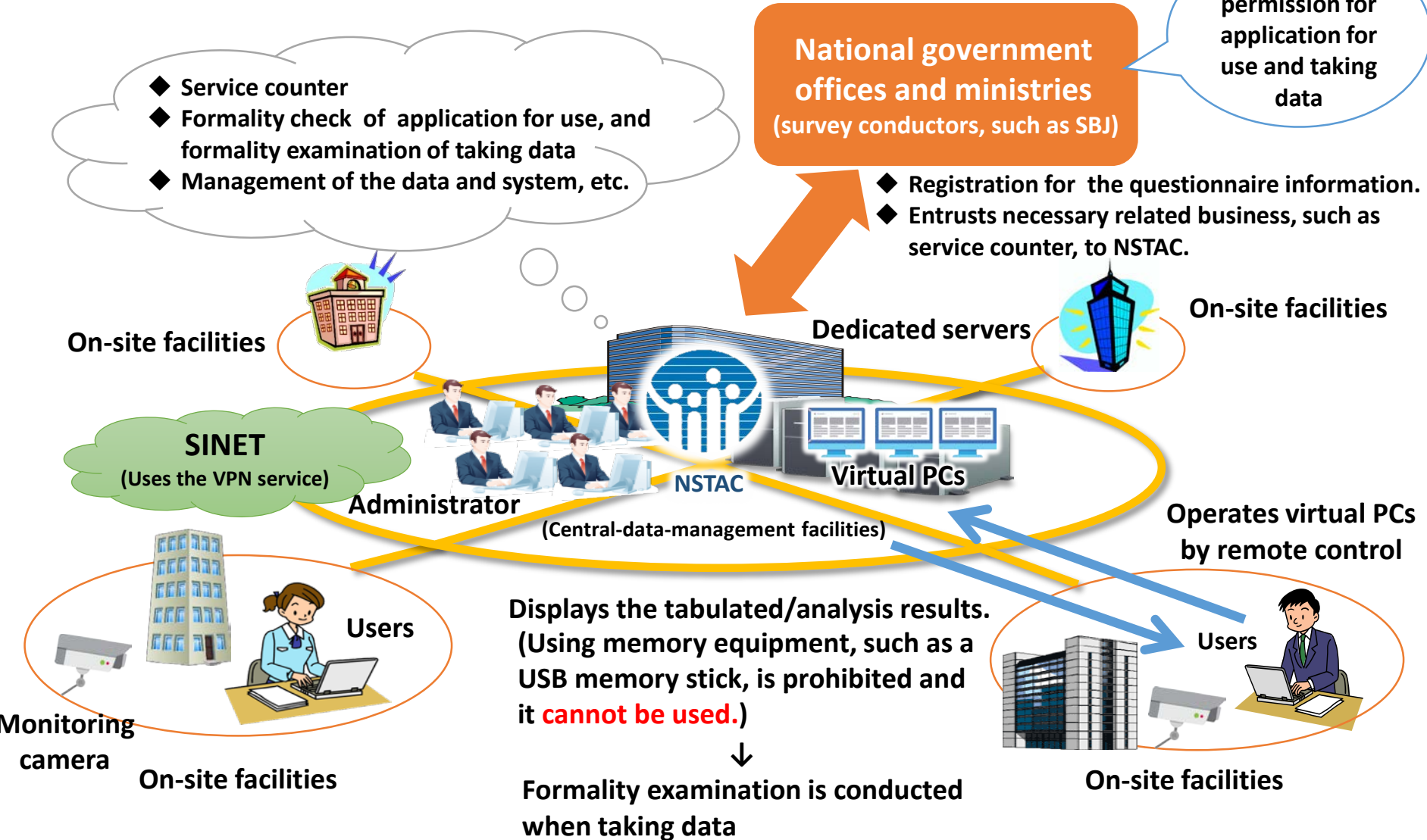
**Central data management facilities,
Comprehensive window for statistics usage**

1. Four challenges of the NSTAC



On-site use of statistical microdata

Conceptual Diagram of on-site use utilizing remote access



On-site use of statistical microdata

Merits of on-site use

Present (provide with DVD)

Use condition

It must be the use of microdata in research deemed to provide a public-benefit.

Security

Researchers are responsible for ensuring security at large.

Application

User needs to obtain permission by submitting an application for use including the detailed design of tabulation and analysis.

Micro-data

Only the minimum information required for the designed analysis is provided.



Exploratory and creative research is **difficult.**

Future (on-site use)

Use condition

It must be the use of microdata in research deemed to provide a public-benefit.

Security

Facility installation personnel are responsible for ensuring a secure environment.

Application

User burden is reduced by simplifying the application for use.

Micro-data

All the information is available for use.



Exploratory and creative research is **possible.**

On-site use of statistical microdata

Merits of on-site use

Present (provide with DVD)

Future (on-site use)

However, we would like to consider a benefit of off-site users.

Application
User needs to obtain permission by submitting an application for use including the detailed design of tasks for analysis.

Micro-data
Only the minimum information needed for the designed analysis is provided.

Application
User burden is reduced by simplifying the application for use.

Micro-data
Maximum information is available for use.

solution

Secure Computation System
+
SDC software τ-ARGUS

difficult.

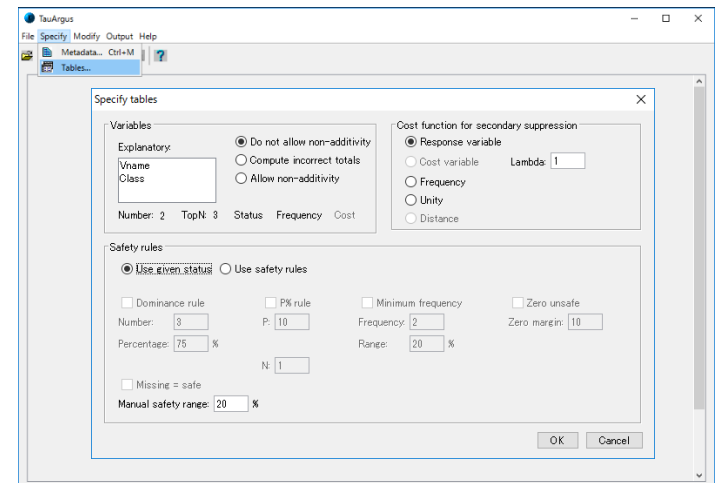
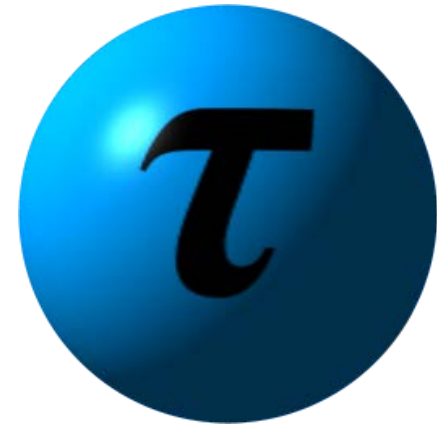
possible.

2. Outline of τ -ARGUS

τ -ARGUS is general-purpose confidential processing software that can protect statistical tables by GUI operation.

The latest τ -ARGUS is version 4.1.5.

- The primary confidential method
 - (n, k) rule
 - $p\%$ rule
 - Minimum frequency rule
- The secondary suppression method
 - Hypercube/GHMITER method
 - Optimal method
 - Modular approach
 - Network






<http://neon.vb.cbs.nl/casc/tau.htm>

Result of empirical analysis

The verification subject is Table #2 (Two-or-more-person Households and Workers' Households from the 2009 National Survey of Family Income and Expenditure) in the special tabulation by the Institute of Economic Research, Hitotsubashi University (Kinoshita and Sakashita, 2014).



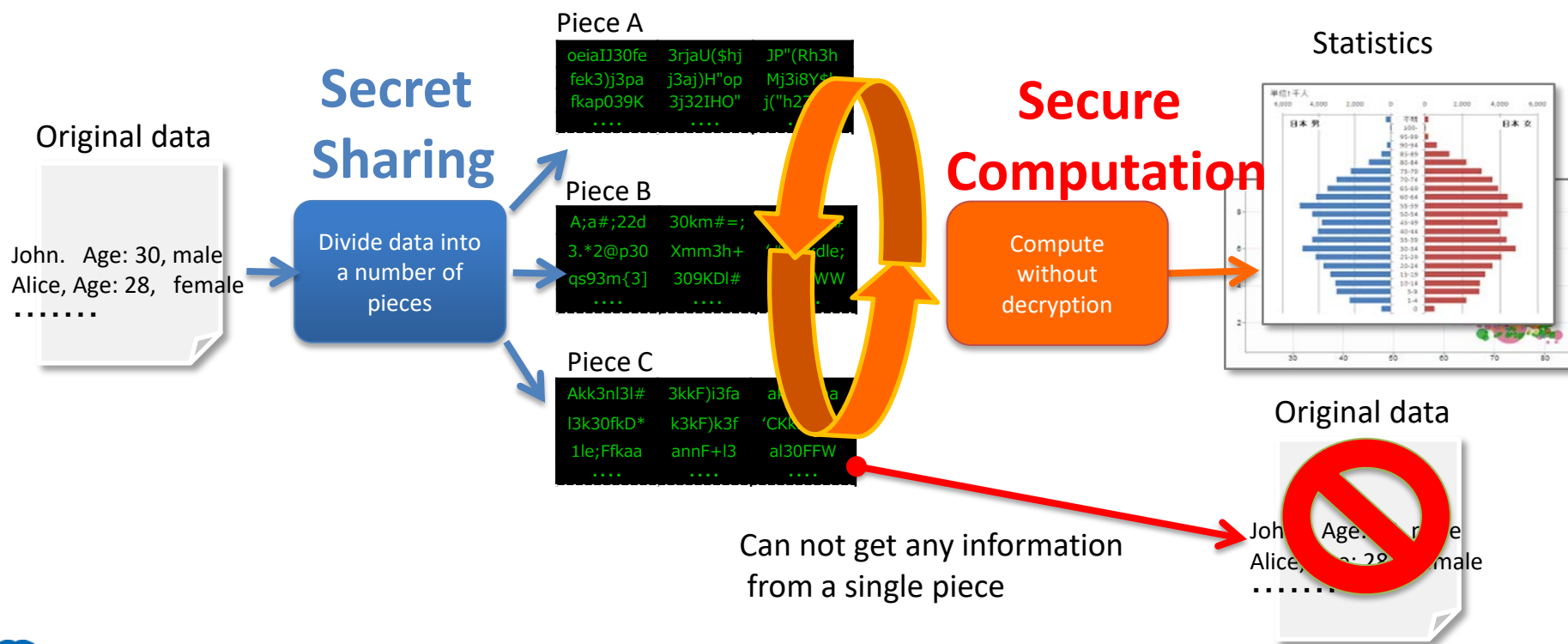
 min. freq. rule  p% rule  secondary suppression



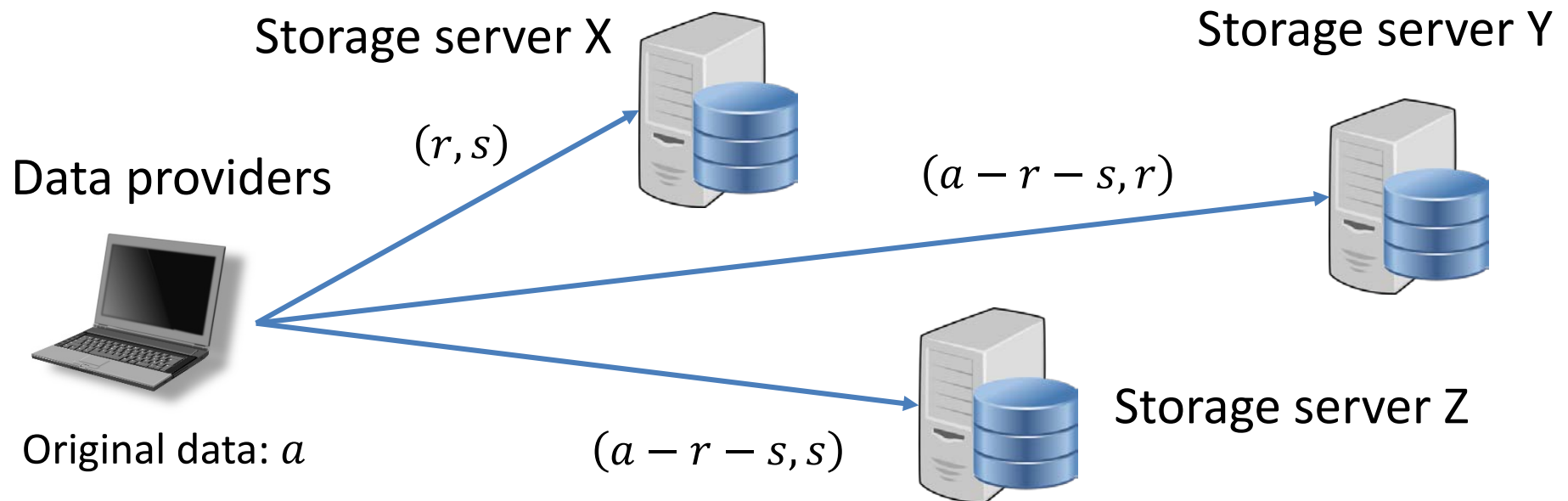
Innovative R&D by NTT

3. What's Secure Computation?

- Store secret data with both **confidentiality and availability**.(Secret sharing)
- Conduct statistical analysis **without decrypting data**.



- Data providers generate n (e.g., $n = 3$) fragments and send them to each storage server individually
 - Secure: The original data can be kept secret even if stored data in a storage server is leaked
 - High available: The original data can be restored even if up to $n - t$ (e.g., $t = 2$) storage servers are crashed

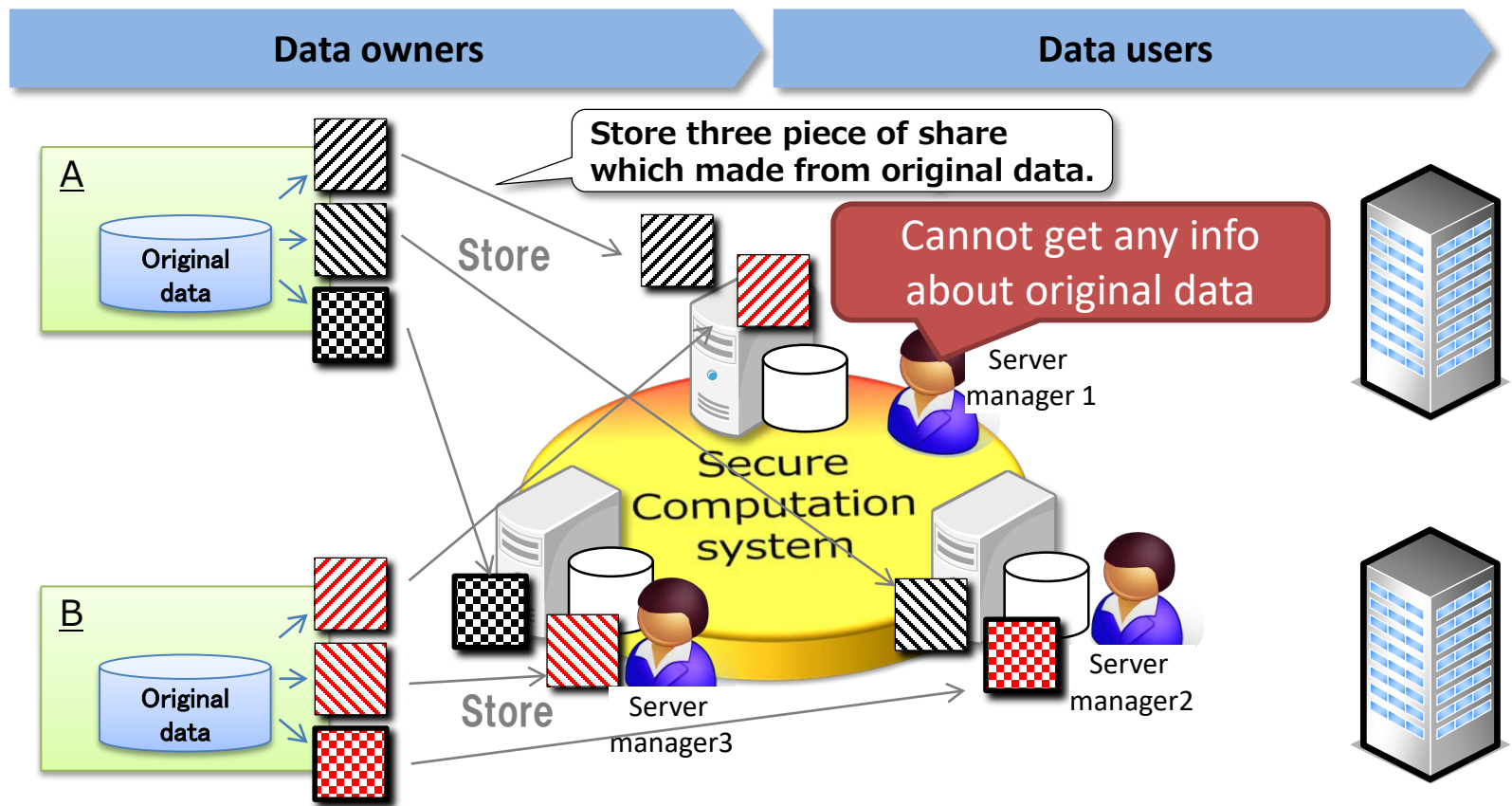


Protection of original data by Secure Computation



Never disclose original data to server manager.

→ The data is protected by Secret Sharing in Secure Computation.

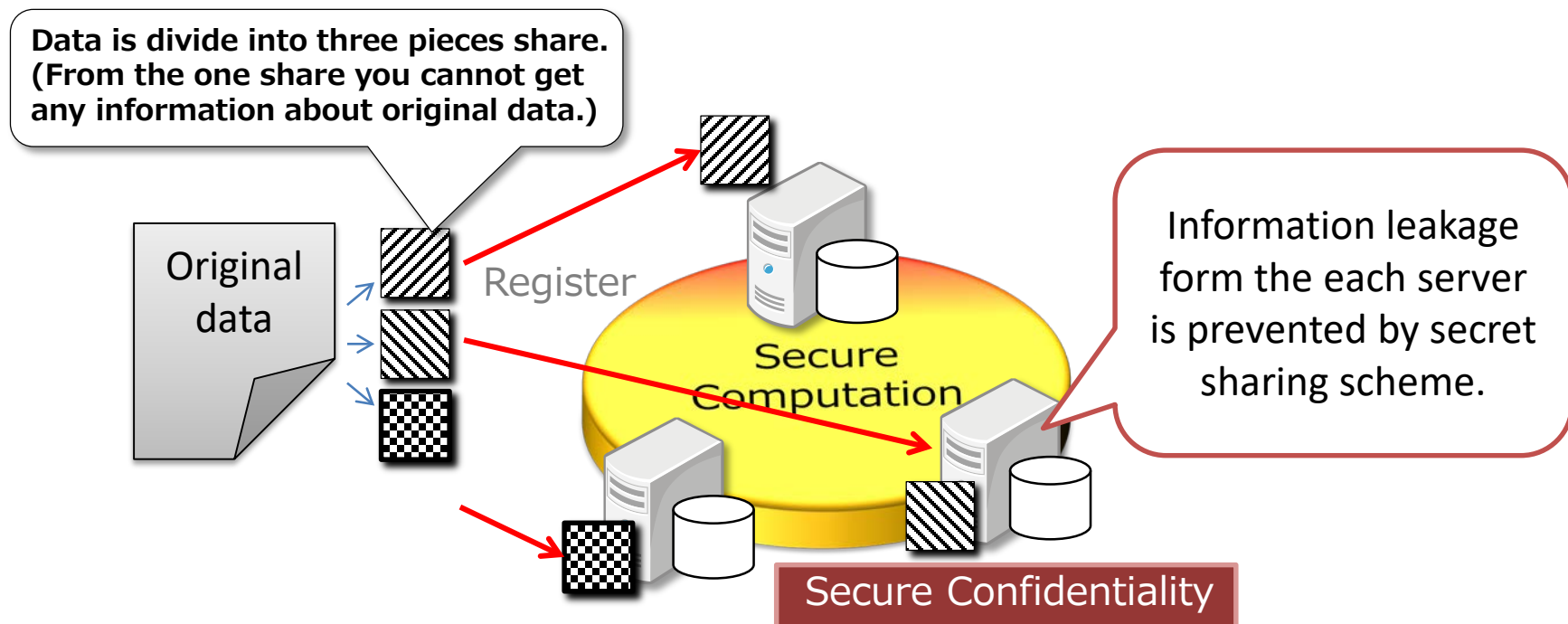


Cooperation between τ -ARGUS and Secure Computation

“Data registration”



- The data is registered to the secure computation system in the following flow.
→The Registered data's safety is ensured by the secret sharing scheme does not cause encryption compromise.

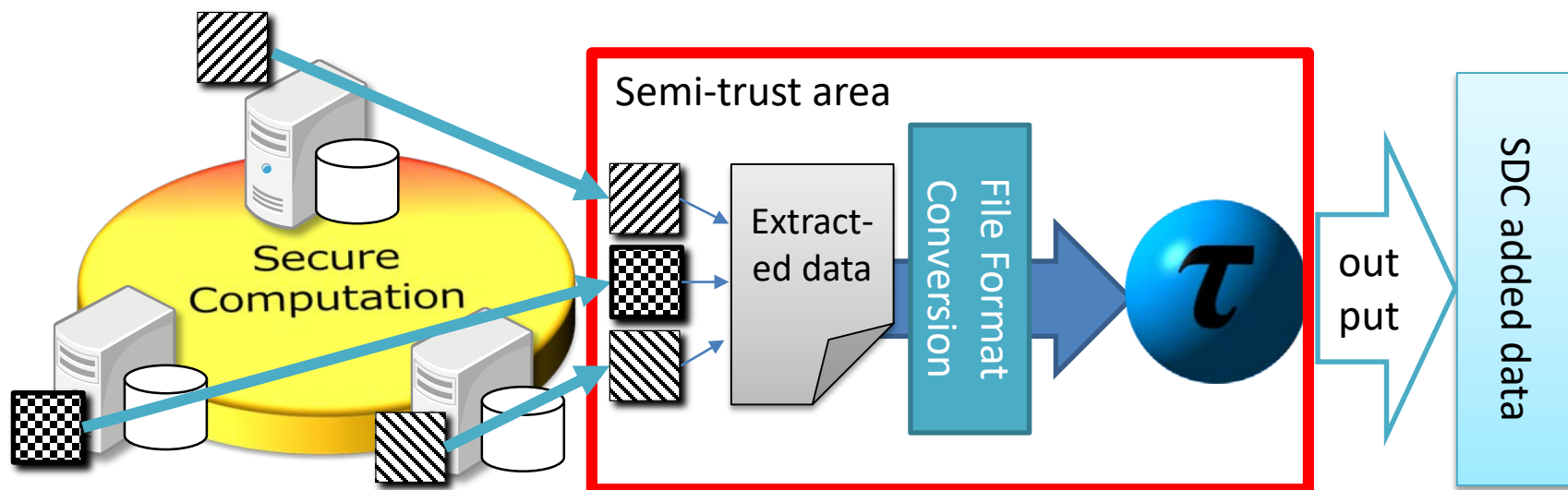


Cooperation between τ -ARGUS and Secure Computation

“Data output”



- The flow for outputting the summary table with SDC from the secure computation system which the data is registered safely.
→ Addition of SDC using τ -ARGUS is carried out on “semi-trust area”.



4. Demonstration



- Please see a demonstration Cooperation between “Secure Computation” and “ τ -ARGUS”.
- The demo scenario is as follows
 - ① Output a summary table using Secure Computation.
 - ② Write the summary table to csv file.
 - ③ **Convert file format from csv, to the τ -ARGUS required.**
 - ④ **Input the data to τ -ARGUS the add SDC.**

5. Conclusions and Future works



- Conclusions
 - We performed the making of the table using encrypted files and the suppression verification by the function of τ -ARGUS.
 - The usefulness of τ -ARGUS by applying the suppression rules suitable for the statistical tables was confirmed.
 - Showed demonstration of Cooperation between “Secure Computation” and “ τ -ARGUS”.
- Future works
 - The feature of this research is to make automatic processing by a concatenate secure computation system with τ -ARGUS which has a tabulation function.
 - We will consider changing the language of τ -ARGUS into Japanese.