A Large-Scale Data Clean Room Case Study in Japan: Confidential Computing and Privacy Regulations

Acompany Co., Ltd.

Confidential Computing Summit 2026
June 24, 2026

Key Points of This Session

CC: Confidential Computing

Regulation

- **Japan's laws are changing** — CC is expected in guidelines
- Japan's CC market is expected to expand

Technology & Case

- Our Data Clean Room (DCR) works under current law
- Adopted by a **Fortune Global 500** company — **40M users**

Who We Are

Acompany

Japan's Confidential Computing Startup

TODAY'S PRESENTERS

Takao Takenouchi

VP of Public Affairs / Strategic Alliance

20 years in this field. Now bridges technology and law to advance PETs and confidential computing.

PRESENTS

Law & policy

Takeharu Kondo

Co-founder / Chief R&D Officer

Leads R&D taking TEE and confidential computing production-ready, now focused on confidential AI.

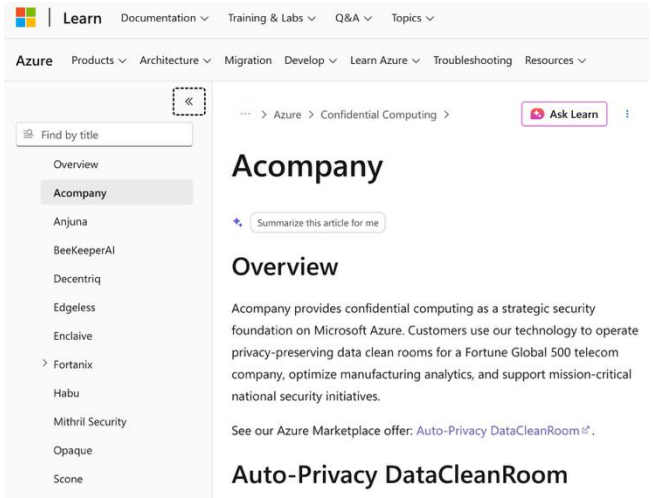
PRESENTS

Technology & case study

Acompany's Strengths

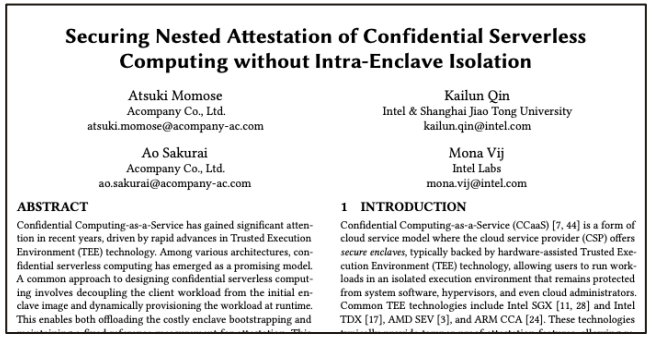
Trusted in both the technology and the community of Confidential Computing

Azure CC Partner



Source: https://learn.microsoft.com/en-us/azure/confidential-computing/partner-pages/acompany

Joint research with Intel Labs



Securing Nested Attestation of Confidential Serverless Computing without Intra-Enclave Isolation

Atsuki Momose
Acompany Co., Ltd.
atsuki.momose@acompany-ac.com

Kailun Qin
Intel & Shanghai Jiao Tong University
kailun.qin@intel.com

Ao Sakurai
Acompany Co., Ltd.
ao.sakurai@acompany-ac.com

Mona Vij
Intel Labs
mona.vij@intel.com

ABSTRACT

Confidential Computing-as-a-Service has gained significant attention in recent years, driven by rapid advances in Trusted Execution Environment (TEE) technology. Among various architectures, confidential serverless computing has emerged as a promising model. A common approach to designing confidential serverless computing involves decoupling the client workload from the initial enclave image and dynamically provisioning the workload at runtime. This enables both offloading the costly enclave bootstrapping and

1 INTRODUCTION

Confidential Computing-as-a-Service (CCaaS) [7, 44] is a form of cloud service model where the cloud service provider (CSP) offers *secure enclaves*, typically backed by hardware-assisted Trusted Execution Environment (TEE) technology, allowing users to run workloads in an isolated execution environment that remains protected from system software, hypervisors, and even cloud administrators. Common TEE technologies include Intel SGX [11, 28] and Intel TDX [17], AMD SEV [3], and ARM CCA [24]. These technologies

Source: https://eprint.iacr.org/2025/727

CCC Member

CONFIDENTIAL COMPUTING CONSORTIUM

Deployment at a Fortune Global 500 company

Spark Your Journey
KDDI

Source: https://en.acompany.tech/news/kddi-acompany-partnership

Acompany Leads Japan's Confidential Computing Community

- In Japan, Acompany founded an industry group, the Privacy Tech Association.
- We lead technical outreach and policy advocacy

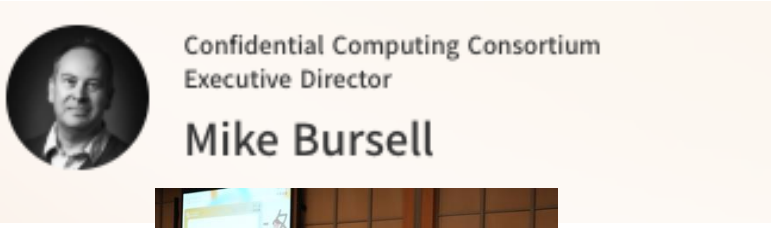
Member Companies

Acompany, EAGLYS, LayerX, JMDC, Hakuhodo DY holdings, Tomorrow, Together KDDI, TOPPAN, Deloitte. デロイト トーマツ, Orchestrating a brighter world NEC, CCC, 大和総研 Daiwa Institute of Research, NTT東日本, Digital Garage, Rakuten, docomo InsightMarketing, 日本総研 The Japan Research Institute, Limited, SoftBank, FUJITSU

Community Activity

Technical Outreach

- Held a hybrid event on CC with around 500 participants
- Featuring a message by Mike Bursell of the CCC



Policy Advocacy

- Proposed updates to Japan's privacy laws and security guidelines

  → More details later

Challenge & Solution: Technology and Law

Main theme: Japan's laws are changing and its CC market is set to expand — so CC is becoming part of the rules.

THE CHALLENGE

Companies couldn't share data across organizations — exactly what AI needs

Technology

Our DCR works under current law — Fortune Global 500, 40M users

→ **Next: Kondo**

Policy

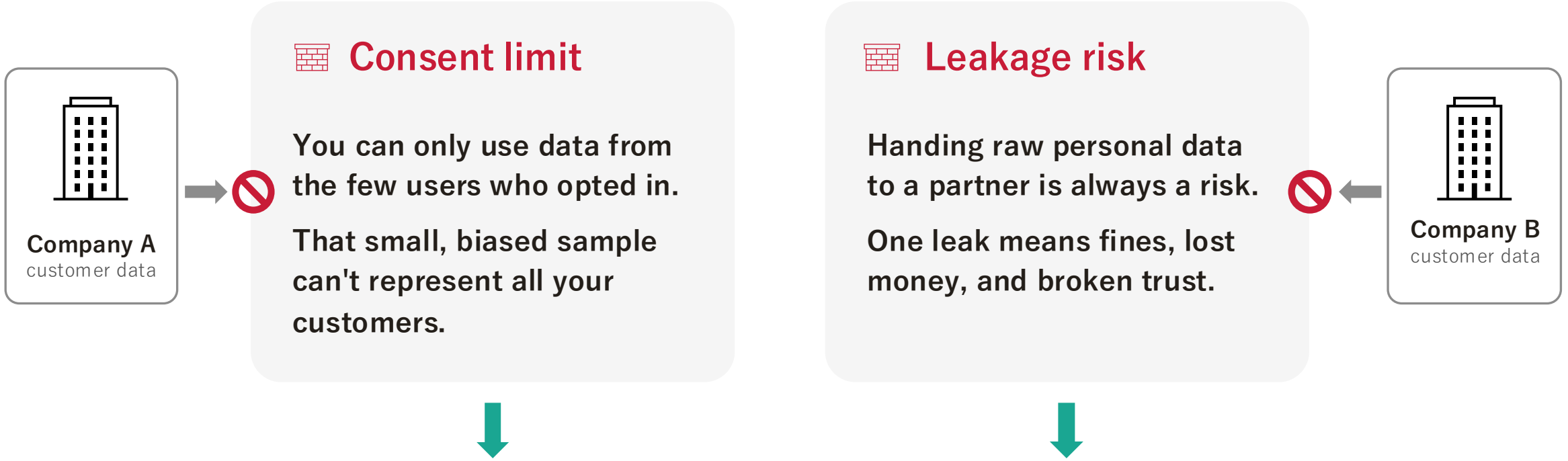
As the law advances, CC is set to enter official guidelines

→ **Later: Takenouchi**

Data Clean Room in Practice

Two walls block data sharing between companies

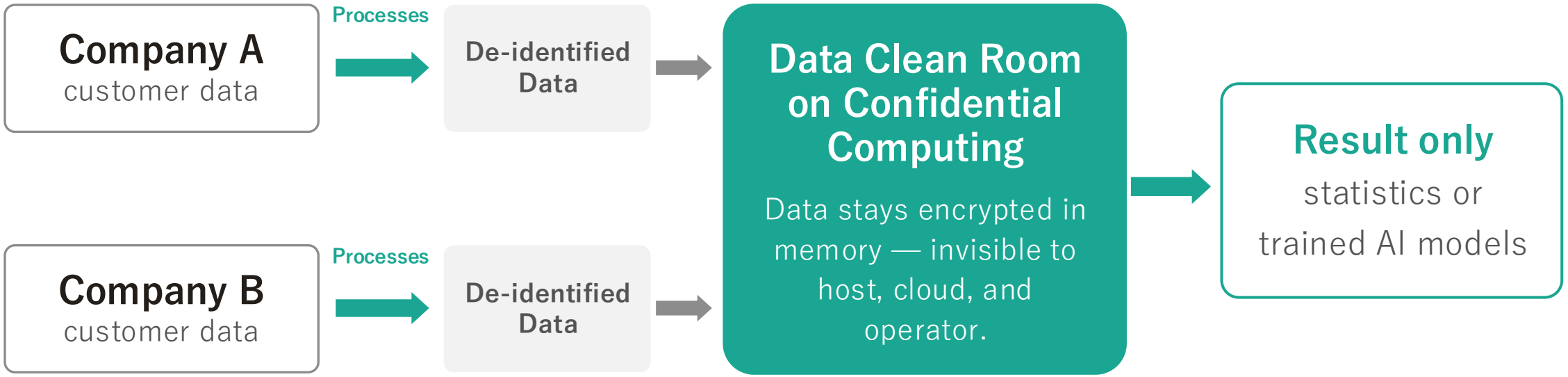
You need other companies' data to understand customers better — but consent and leakage risk stand in the way.



A Data Clean Room removes both walls at once.

With a Data Clean Room, you can leverage data without revealing it

1. Each company processes customer data as de-identified data
2. Analysis runs in Confidential Computing (CC)



Minimize the risk of re-identifying personal data

1. **Apply k-anonymity, salted hashing, and differential privacy to turn data into de-identified data**
2. **Run data matching and statistical/AI processing in CC to minimize re-identification risk**

De-identification

Apply k-anonymity, salted hashing, and differential privacy to produce de-identified, processed data.

Confidentiality

Processing inside the clean room keeps the analysis that follows data matching confidential.

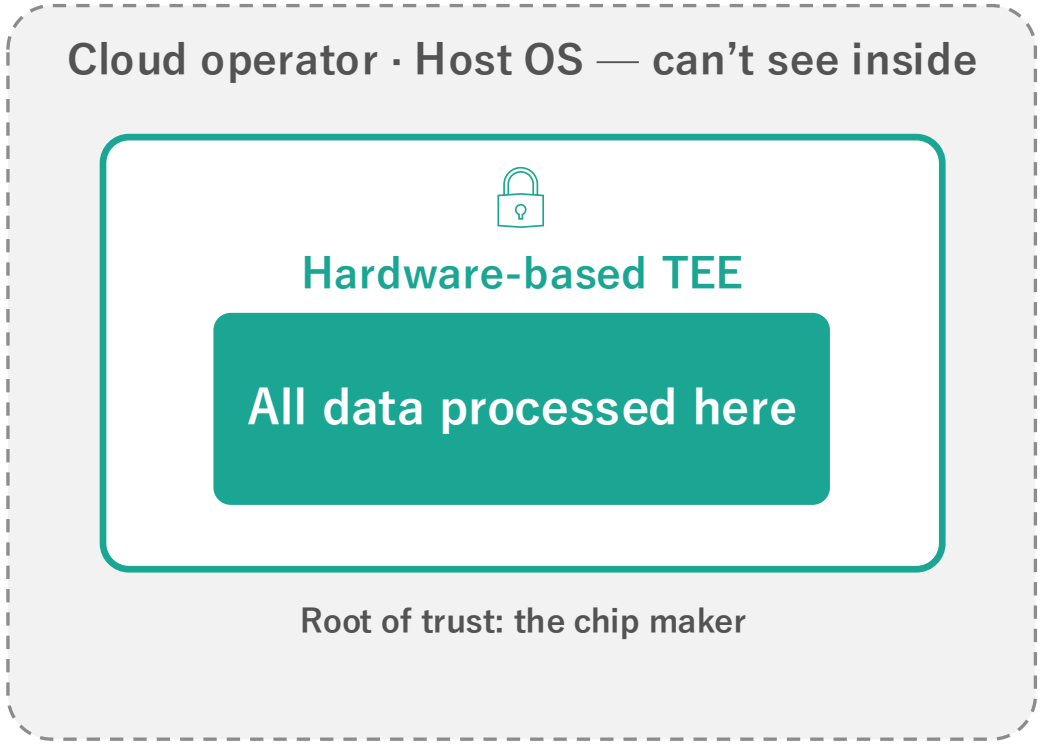
Verifiability

Remote Attestation lets external parties verify that the processing was agreed on in advance.

The clean room enforces these guarantees in code, before anyone can see a result.

Security rooted in the hardware

Your data runs inside a hardware-based TEE, so not even cloud providers or the host OS can access it while in use.



Hardware-based TEE

Runs inside Intel SGX. Memory is encrypted and hidden from the host OS.

Remote attestation

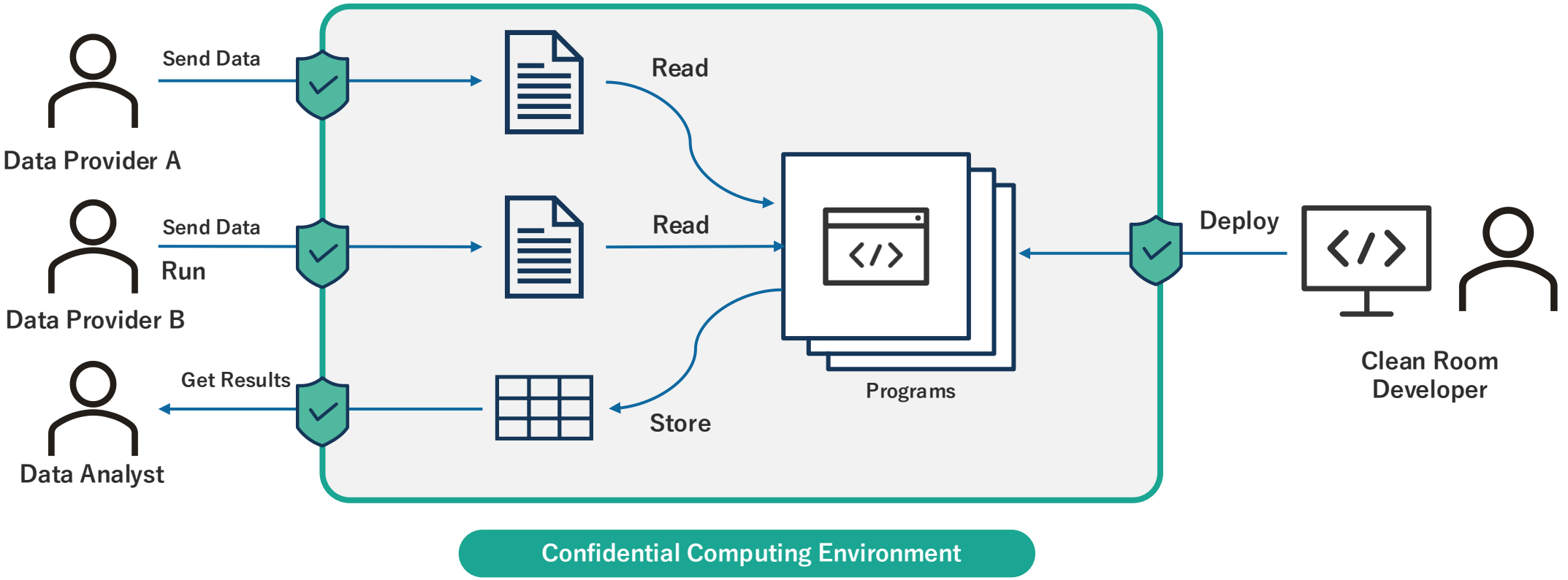
Before sending data, the enclave proves which code is running — and that it has not been changed.

No data retention

All data is deleted after use. Each session uses new keys.

Composed of entities with three roles

- Data Provider: Holds the data to be fed into the clean room
- Clean Room Developer: Develops and deploys the programs that run inside the clean room
- Data Analyst: Runs the clean room programs and receives the results



The whole exchange is four commands

Each entity interacts with the data clean room through a single CLI tool

1 **Deploy the room (clean room developer)**

```
apc cleanroom deploy --name cross_table_app \
   --source ./function --handler handler.run \
   --encrypted-files ./encrypted_files.yaml
```

2 **Send encrypted data (each data provider)**

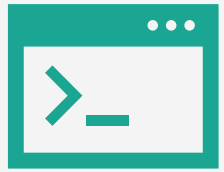
```
apc cleanroom data cp ./inputs/input_a \
   cross_table_app:input_a
```

3 **Run (analyst)**

```
apc cleanroom run cross_table_app
```

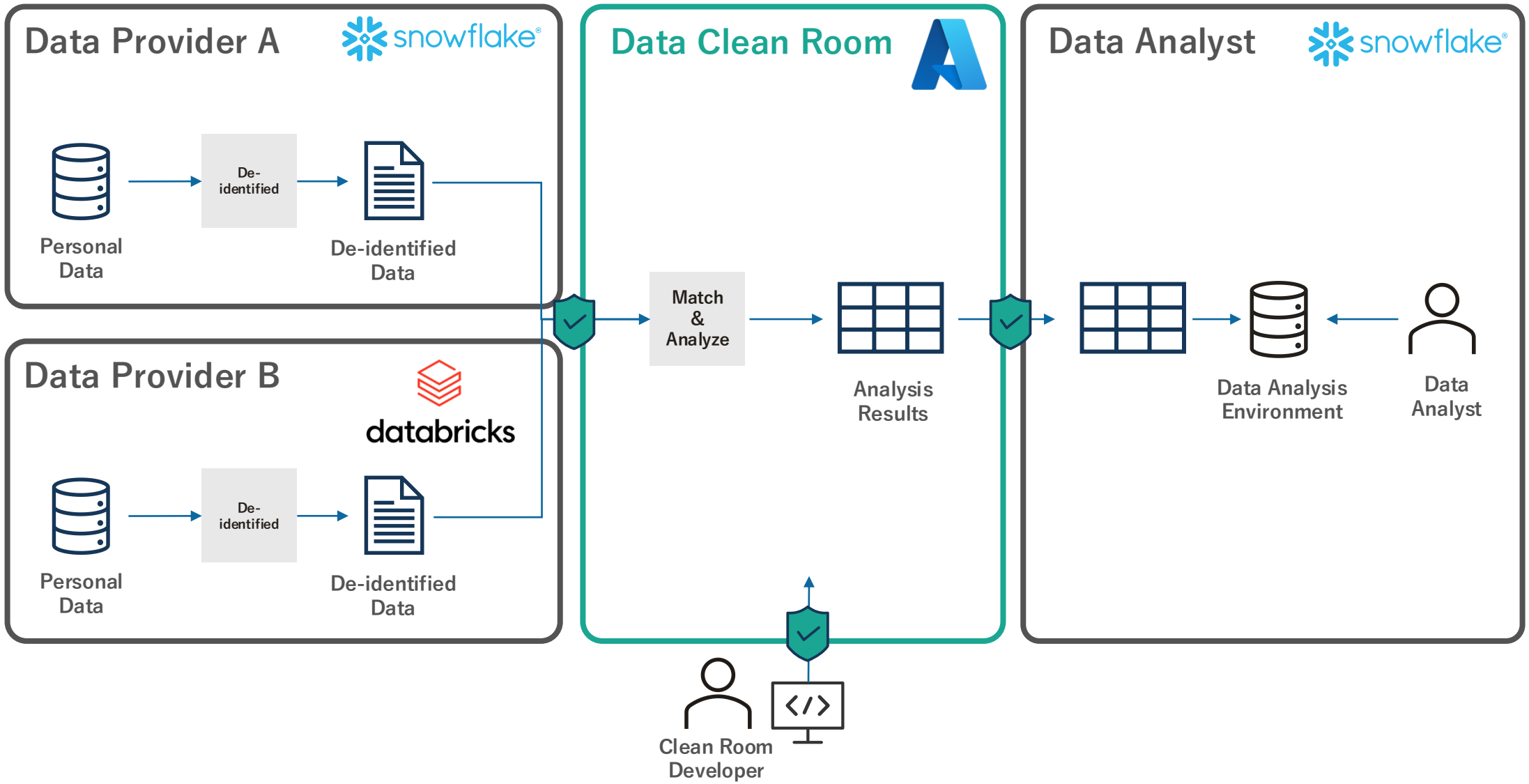
4 **Retrieve (analyst)**

```
apc cleanroom data cp \
   cross_table_app:output ./output
```



One CLI tool.
Four commands.
A complete data clean room exchange.

Example Implementation Using Snowflake, Databricks & Azure



Already running in production

- **Fortune Global 500 company KDDI** runs its data collaboration on our Data Clean Room
- It combines its **40M-user data** with partner data for cross-tabulation, driving smarter sales and marketing

Spark Your Journey KDDI

Location Data

Attribution Data

Partner Company

POS Data

Purchase Data

Data Collaboration Platform

date	place	age	Interest
6/3	Tokyo	29	Hobby
6/3	Tokyo	26	PC
6/4	Osaka	35	Book
6/5	Kyoto	35	Book

Revenue Contribution

Acquisition of new customers

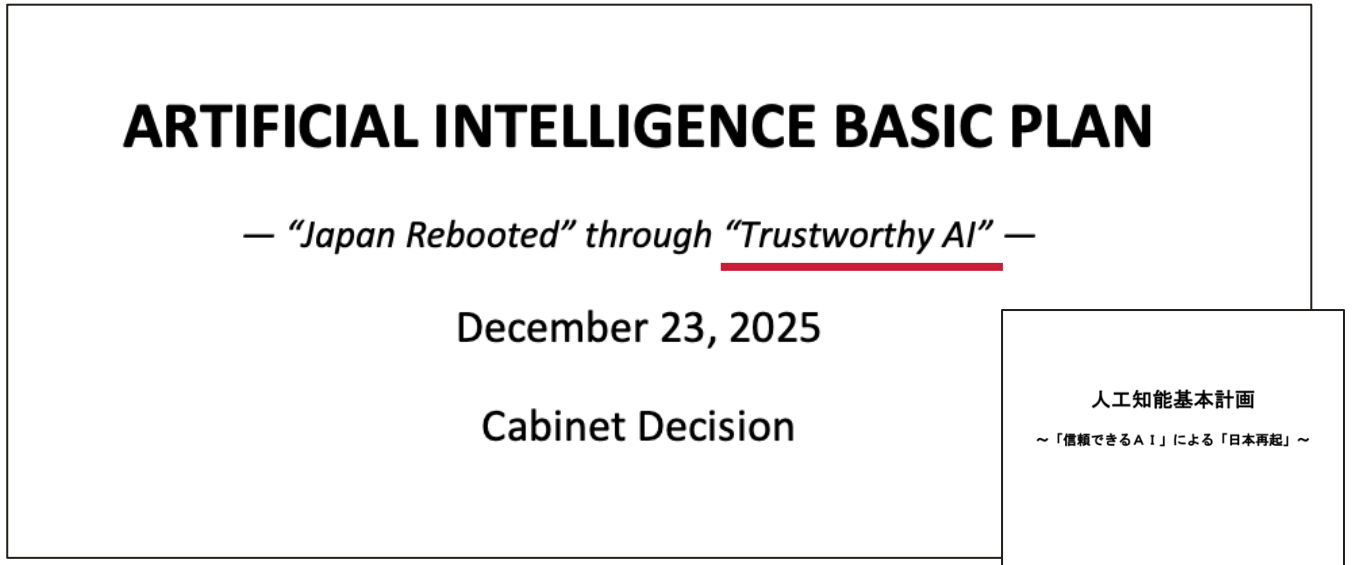
Shop optimization

Japan’s
Regulatory Landscape for CC

Japan's Regulatory Developments for CC

- The Japanese government aims to realize "Trustworthy AI"
- Trustworthy AI requires Confidential AI — and Sovereign AI
- To realize this, Acompany is advancing how CC and the law fit together, through the industry group

The Japanese Government's AI Strategy



Source:
https://www8.cao.go.jp/cstp/ai/ai_plan/ai_plan.html
https://www8.cao.go.jp/cstp/ai/ai_plan/aiplan_eng_20260312.pdf

This **trustworthiness is a core pillar of Japan's globally respected brand**

We will actively apply AI to pressing challenges, accumulate experience as data, and share it across organizations to **create "Trustworthy AI" that is a reliable presence for the world.**

Our Action 1: Amendment of Japan's Privacy Law (APPI)

- Acompany takes part in this discussion, highlighting the value of Confidential Computing
- Now that the amendment has passed, we plan to get CC included in the official guidelines *1

We proposed CC

Source: https://privacytech-assoc.org/news/25-0107

PETs, including CC, heading into the rules

As a result, a supplementary resolution in the Diet recommended PETs, including CC

Privacy Enhancing Technologies (PETs) is a promising technology

Kiyoshi Sawaki, Secretary-General, Personal Information Protection Commission

By building in the latest PETs as guardrails, we can drive data use and strengthen Japan's AI competitiveness.

Akiko Murakami, Director of AISI Japan

*1: As of June 2026, the amendment has cleared the lower house and is now before the upper house.

Our Action 2: Recommending CC in Critical-Infrastructure Guidelines

- Japan's critical-infrastructure guidelines have recommended protecting data in use since 2023.
- But the text was outdated — so our organization requested an update, and it was agreed.

Current text

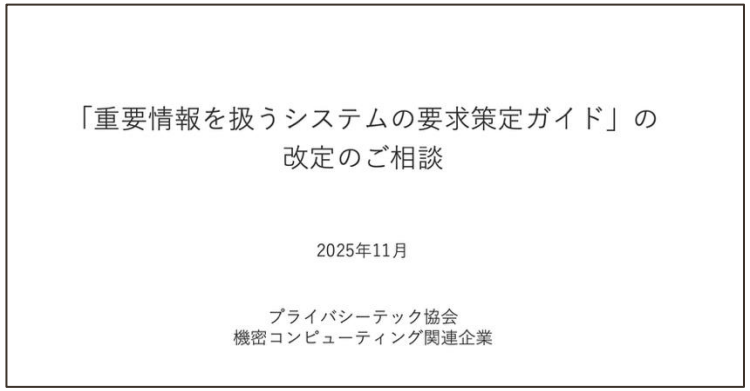
Ensuring encryption of data in use

Even if an attacker targets the hardware, or a privileged operator acts maliciously, the contents of data in memory cannot be read.

Source: https://www.ipa.go.jp/digital/kaihatsu/system-youkyu.html

We are proposing revision

We submitted a formal opinion, together with CC companies


「重要情報を扱うシステムの要求策定ガイド」の
改定のご相談

2025年11月

プライバシーテック協会
機密コンピューティング関連企業

Conclusion

Takeaways

In Japan, CC and the law are coming together — and the market is opening up.
Let's build Japan's safe AI infrastructure, powered by Confidential AI — **together.**

Chip vendors — grow the market with us

Cloud / Data Center — offer Confidential VMs in Japan

Frontier models — host your models in Japan

Policymakers — let's shape the rules together

Takao Takenouchi

VP of Public Affairs & Strategic Alliance

Email: takao.takenouchi@acompany-ac.com

Takeharu Kondo

Co-founder & CRDO

Email: takeharu.kondo@acompany-ac.com