HITACHI
Inspire the Next

エストニアの秘密計算と制度的な整理について

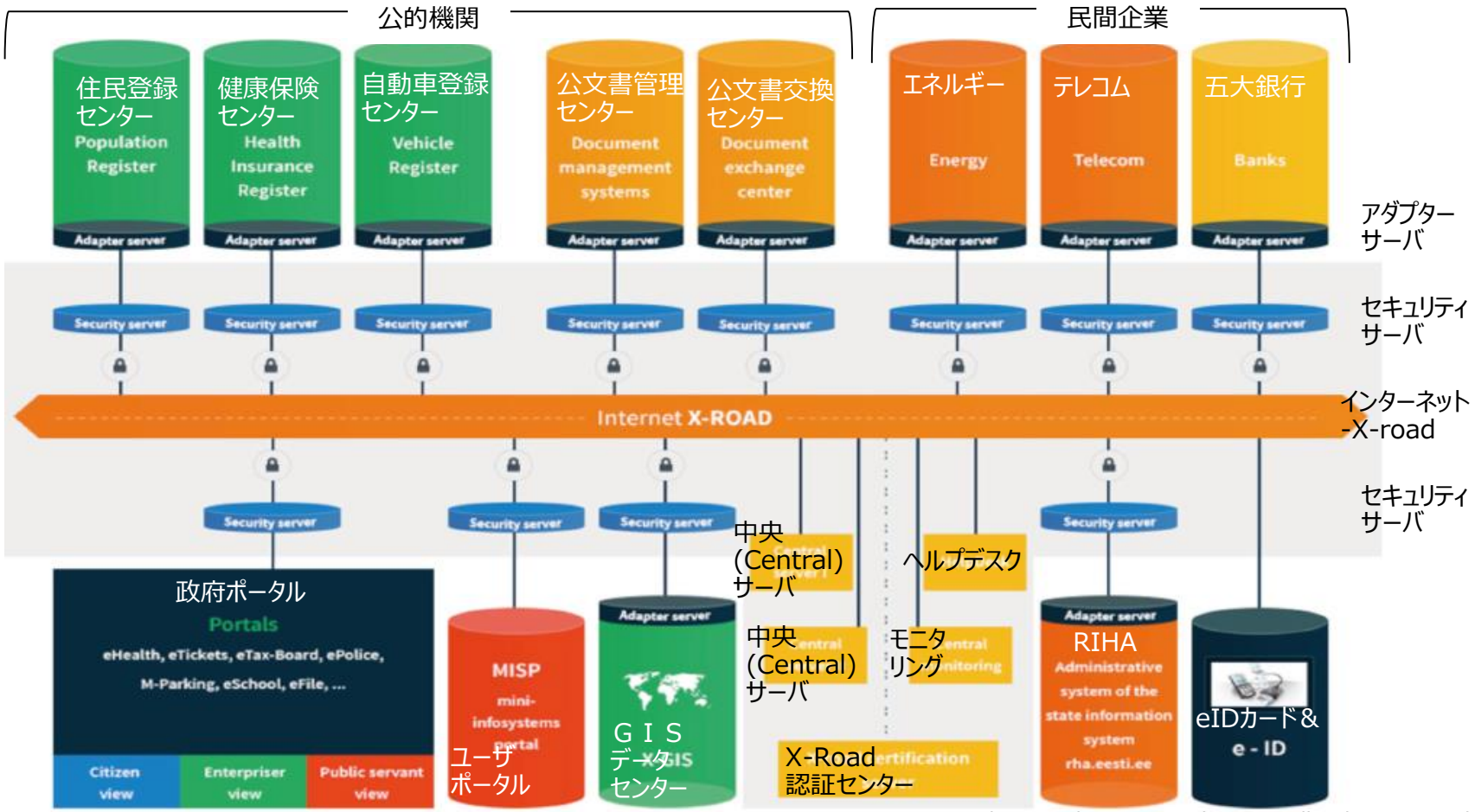
2019年3月7日

日立コンサルティング
美馬正司

CTBERNETICA

HITACHI
Inspire the Next

- 1997年に設立されたエストニアのIT企業であり、セキュリティ関連のソリューション等を保有。
- 百数十名の技術オリエンティッドな会社であり、１割以上が博士号所有。
- X-Roadというエストニア政府のデータ交換基盤の開発に携わっている。



出典：X-ROAD FACTSHEET, https://www.ria.ee/public/x_tee/X-road-factsheet-2014.pdf

Sharemind

HITACHI
Inspire the Next

- CYBERNETICAによって開発された秘密分散を用いたMPC
- Sharemindの特徴は以下の通り。
  - 分散アプリケーションサーバアーキテクチャ
  - 1,000以上の計算プロトコルを実装
  - 大規模並列安全マルチパーティ計算操作をSecreCというプログラミング言語で実装
  - 出力プライバシーの実装（閾値制御、差分プライバシー）
- 2017年からIntel SGXを用いた”Sharemind HI”をリリースし、従来のものは”Sharemind MPC”と呼んでいる。

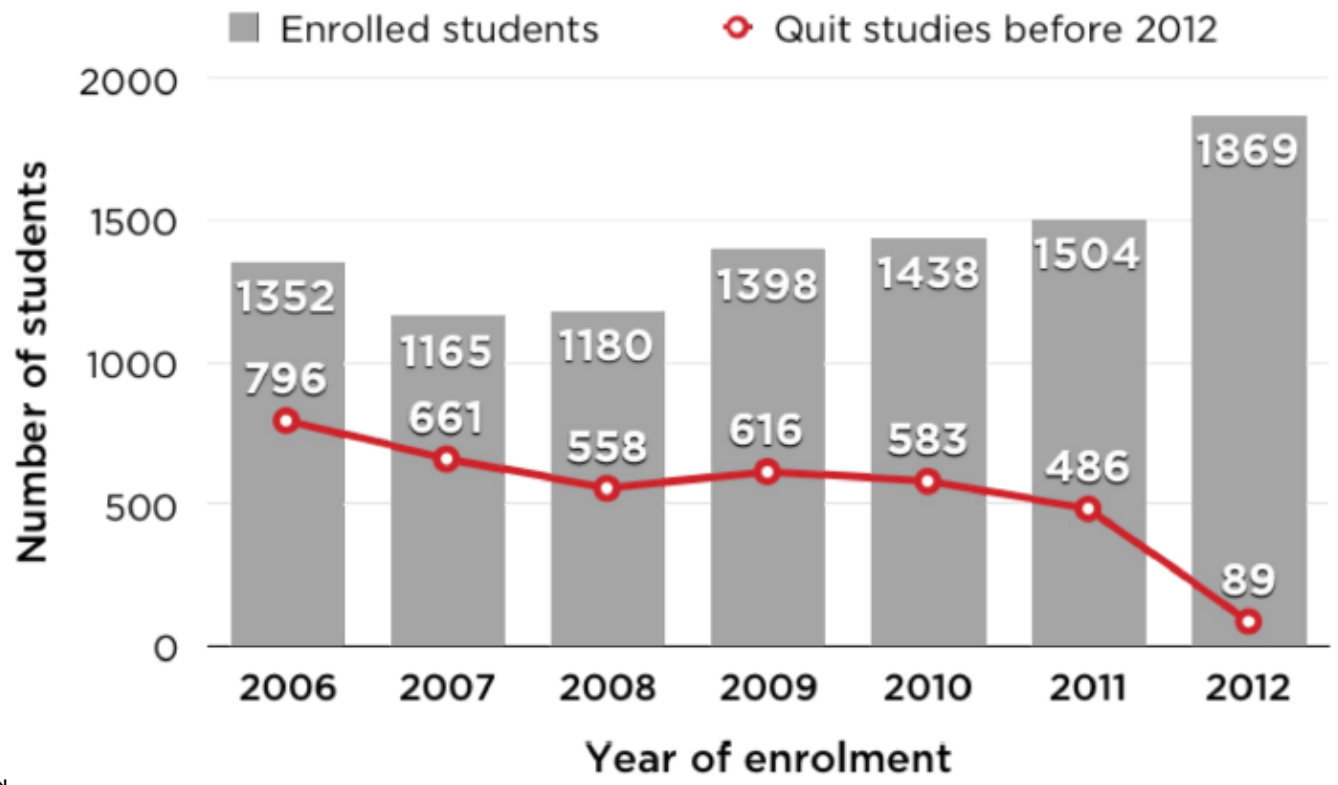
	Sharemind MPC	Sharemind HI
Technology	Purely cryptographic technology	Cryptography with trusted hardware
Performance	Low to medium performance overhead	Minimal performance overhead
Deployment	Multi-node application server (three servers needed)	Single-node application server (one server with special CPU)
Usage Model	Analytical tools and SDK available	Tailor-made applications only
Requirements	Deployable in any data centers or private/public clouds	Requires modern processor hardware to run

出典：CYBERNETICA資料

実装事例：PRIST project

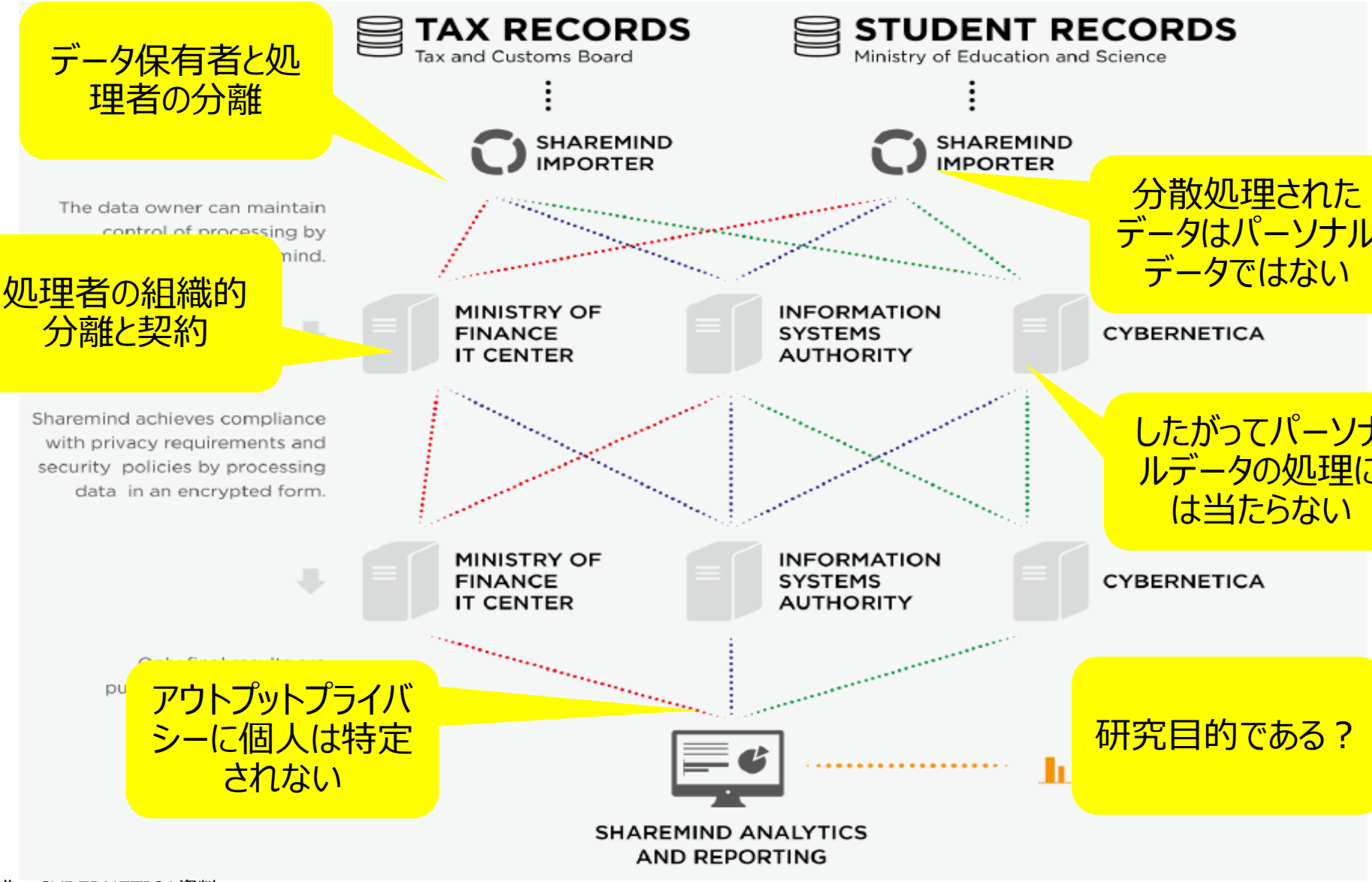
HITACHI
Inspire the Next

- EUのファンドで2013～15年に行われたプロジェクト
- IT系の大学生の卒業率が低下しており、これが大学時の就業と関係があるのではないかという仮説を秘密計算により検証
- 国税庁の持つ1,000万の納税データと、文部科学省の持つ60万の教育データを国民Idを用いて突合して分析
- 結論として相関は見られず、景気の停滞とともに卒業率は回復した模様



出典：CYBERNETICA資料

制度的な論点（１）



データ保有者と処理者の分離

処理者の組織的分離と契約

分散処理されたデータはパーソナルデータではない

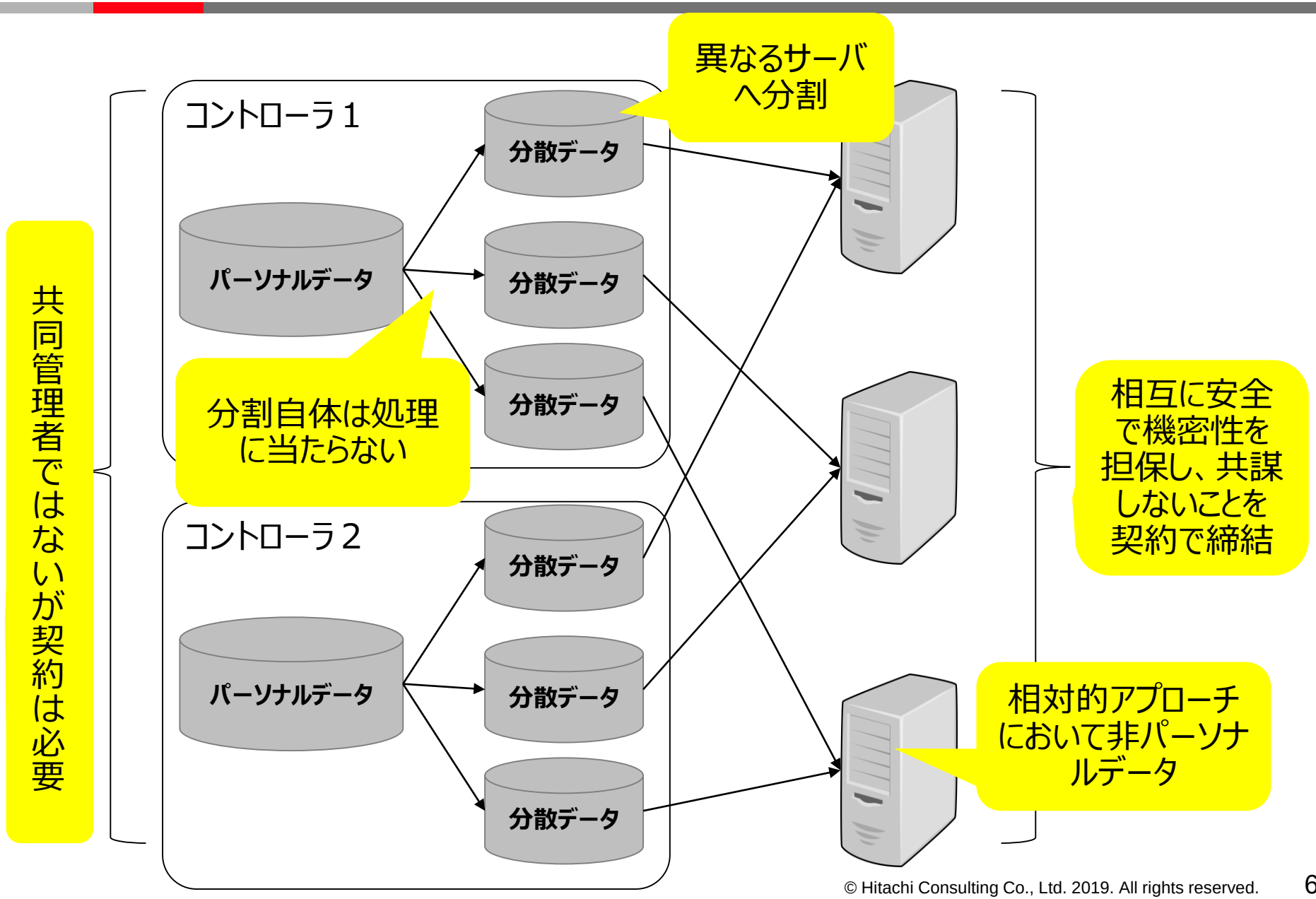
したがってパーソナルデータの処理には当たらない

アウトプットプライバシーに個人は特定されない

研究目的である？

出典：CYBERNETICA資料

制度的な論点（２）



その他

HITACHI
Inspire the Next

- GDPR施行前はDPAによりパーソナルデータの処理に当たらない、という判断
- GDPR下では、明確ではないが相対的アプローチでは同様の解釈が可能
- サーバが三か所に分かれているのは処理能力のためで、２者の共謀防止の意図ではない模様
- 技術だけでなく、プロセスも含めてDPAとは密にやり取りをしており、その結果としての判断
- クラウドにサーバを置くなら、それぞれ異なるクラウドであることが必要
- 秘密計算で何を実現するかのアカウンタビリティも重要

HITACHI

Inspire the Next