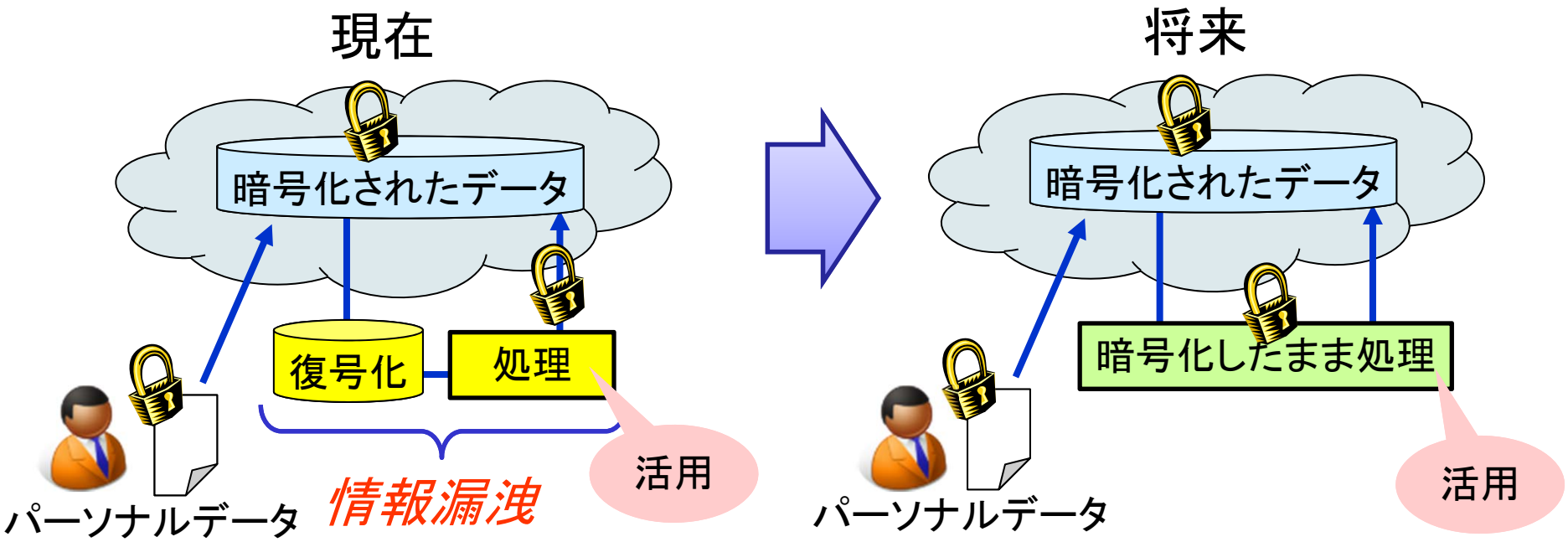
情報を守るICTのジレンマ（一例）

ビッグデータの利活用で便利で豊かな社会を築くためには
パーソナルデータの保護が重要

ジレンマ

暗号化すると使えない、暗号化しないと使えない

取り組むべき課題：
データを暗号化したまま処理（暗号化情報処理）

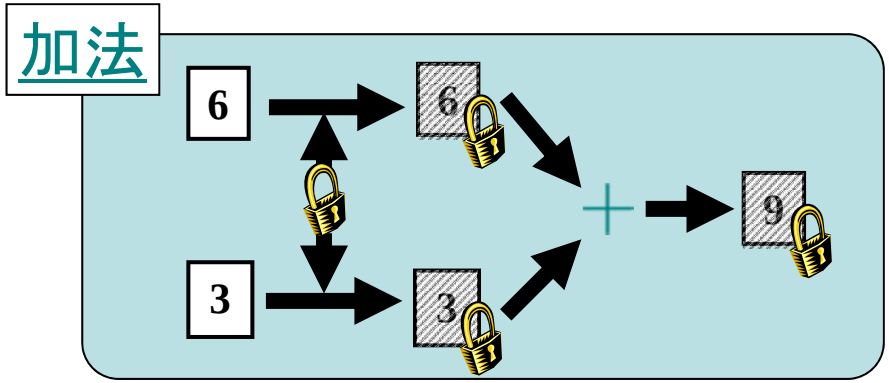


暗号化情報処理－完全準同型暗号

暗号化されたデータを、復号することなく検索や計算を可能とし、安全性と利便性を両立

「完全準同型暗号」

- 2つの暗号文同士の加減乗除をとると、それらの隠れた平文同士の加減乗除の暗号文となる特殊な暗号



技術的課題：
- 自由な演算
- ビッグデータでの性能
- 安全性評価

完全準同型暗号 (Fully Homomorphic Encryption)
データを暗号化したままの状態で、もとのデータの加算と乗算の演算が行える暗号方式。2009年に米IBM社の暗号研究者、クレイグ・ジェントリーが格子理論を利用して、初めて完全準同型暗号の開発に成功した。（http://www.nict.go.jp/press/2013/01/21-1.html）

夢の実現例ーブレイン・プロバイダ

ノーベル賞受賞者の記憶、知識、分析、判断などを暗号化してクラウドに蓄積