# 高機能暗号について

岡本　龍明
NTT 社会情報研究所
July 26, 2023

# もし共通鍵暗号しかないとすると

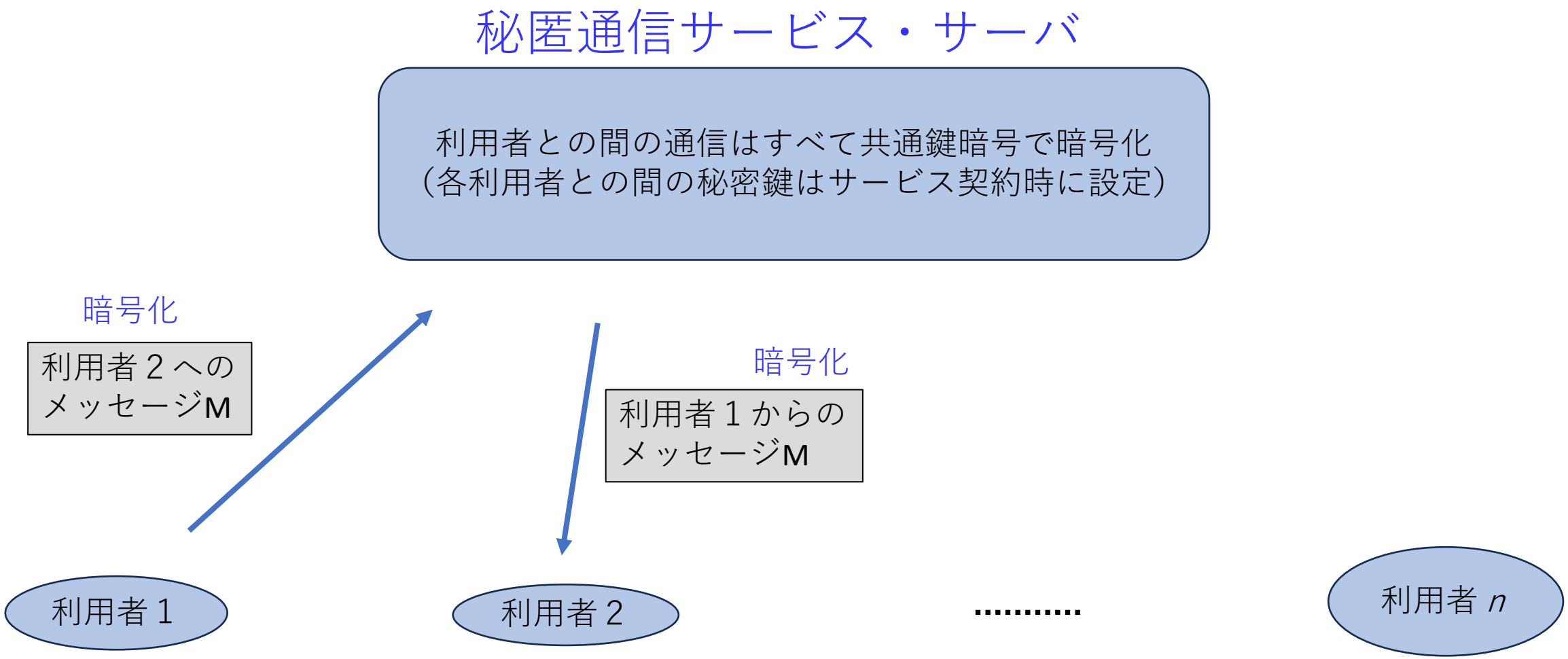
インターネットの安全性をどのように守るか？

信頼できるクラウドサービスを利用してさまざまなセキュリティ機能を実現

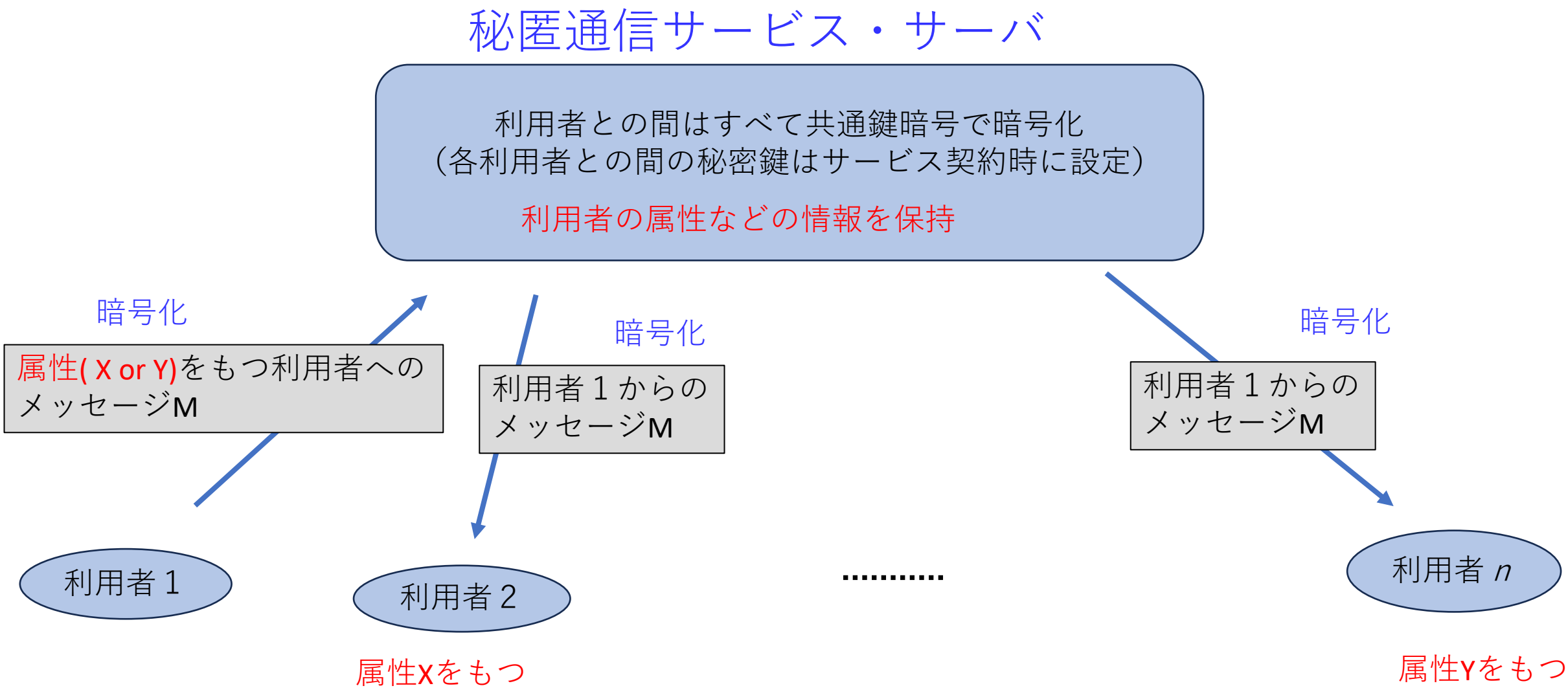
- 秘匿通信サービス
- 認証・署名サービス
- 秘密計算サービス
- データベースサービス

etc

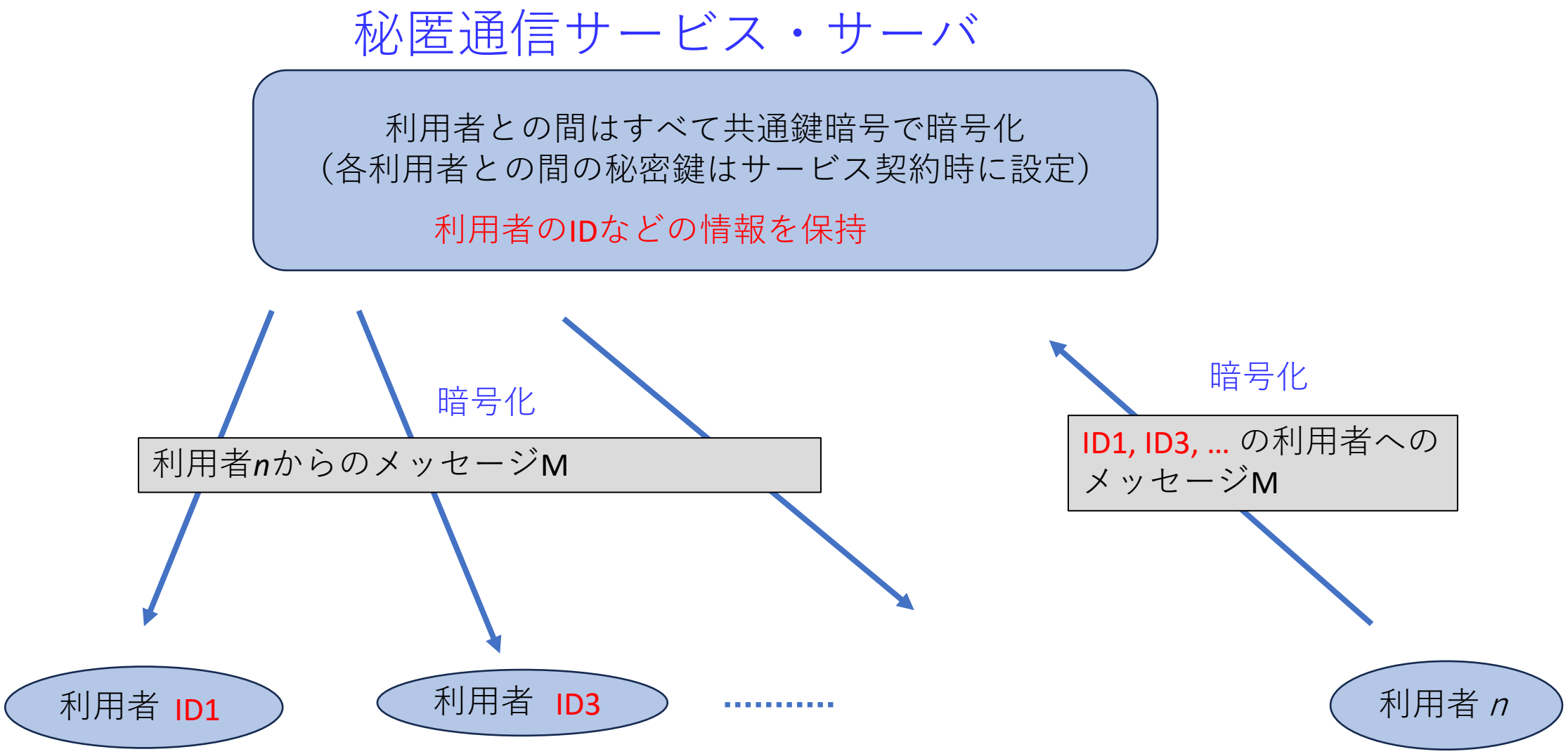
# 秘匿通信サービス（基本）


秘匿通信サービス・サーバ
利用者との間の通信はすべて共通鍵暗号で暗号化
（各利用者との間の秘密鍵はサービス契約時に設定）
暗号化
利用者２へのメッセージM
暗号化
利用者１からのメッセージM
利用者１
利用者２
.....
利用者 n

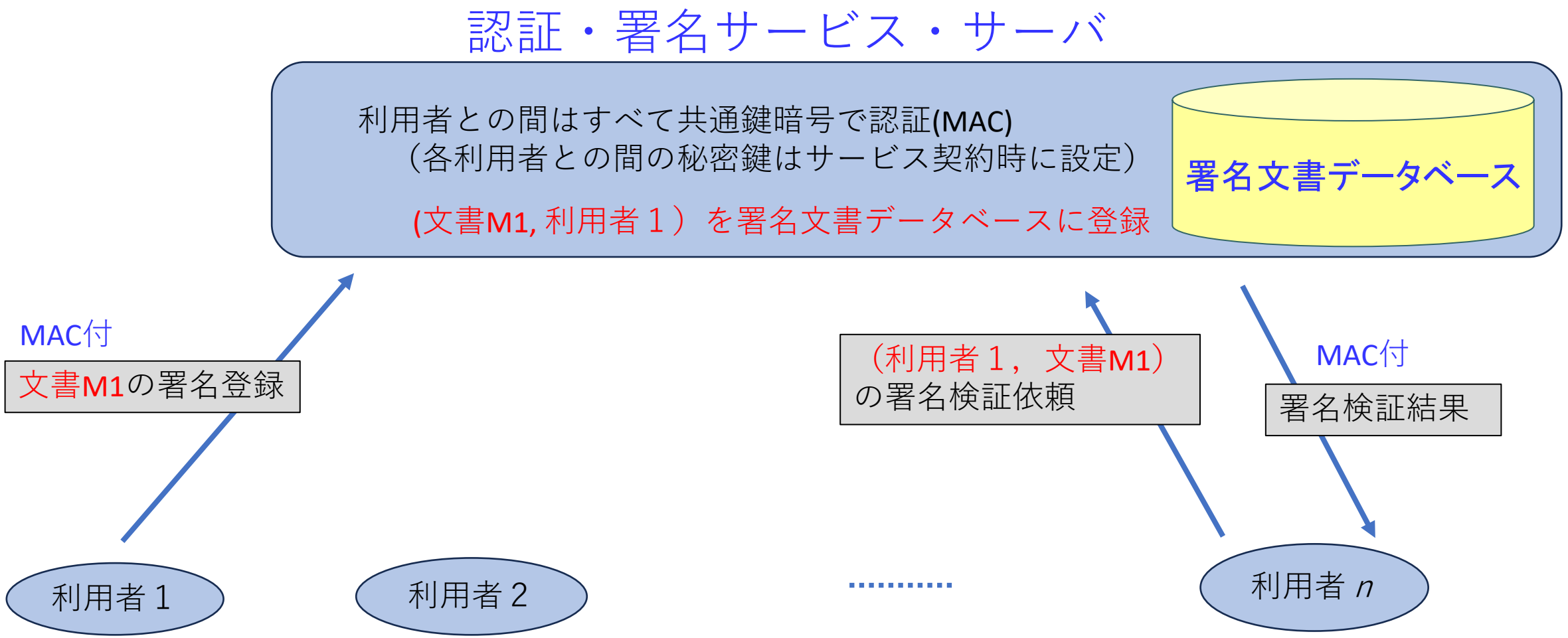
# 秘匿通信サービス（応用1）



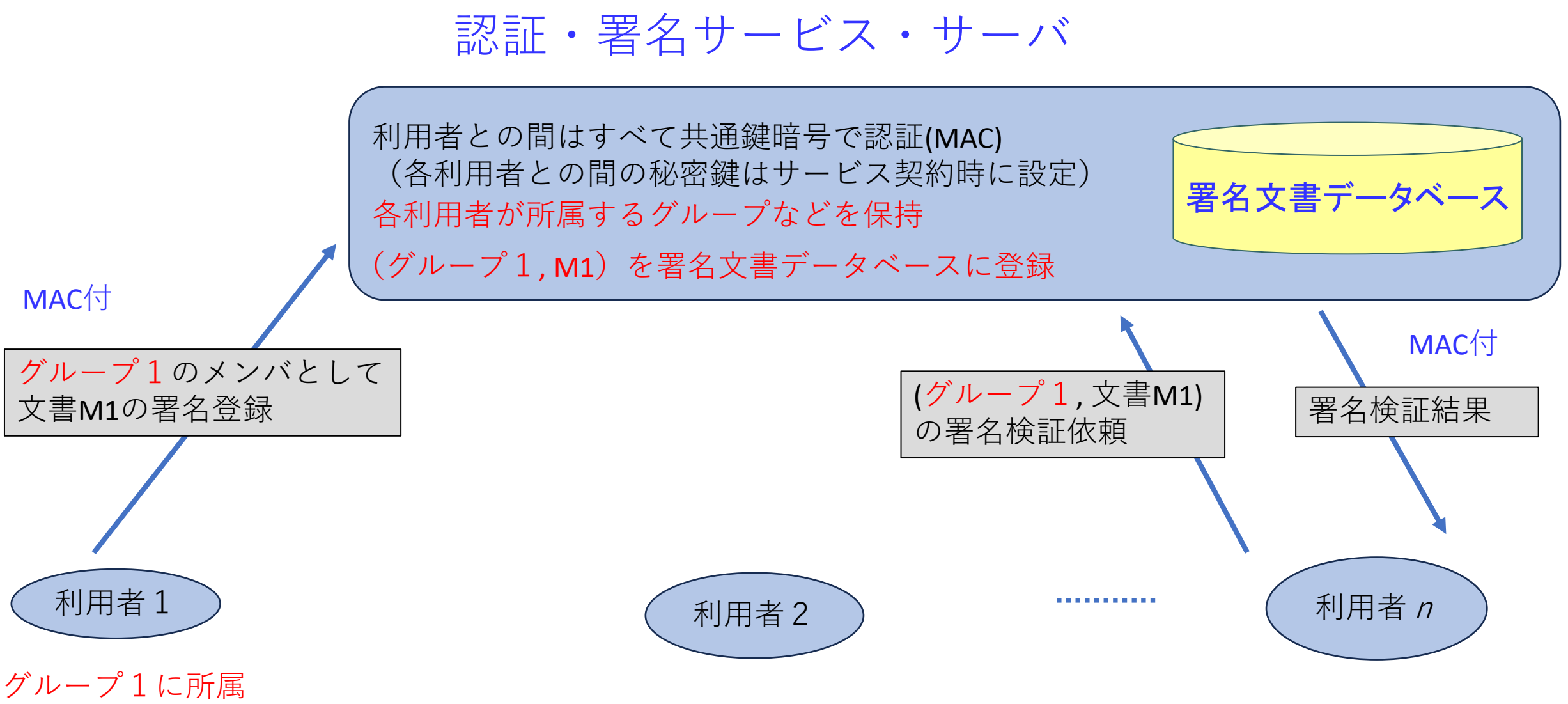
# 秘匿通信サービス（応用2）



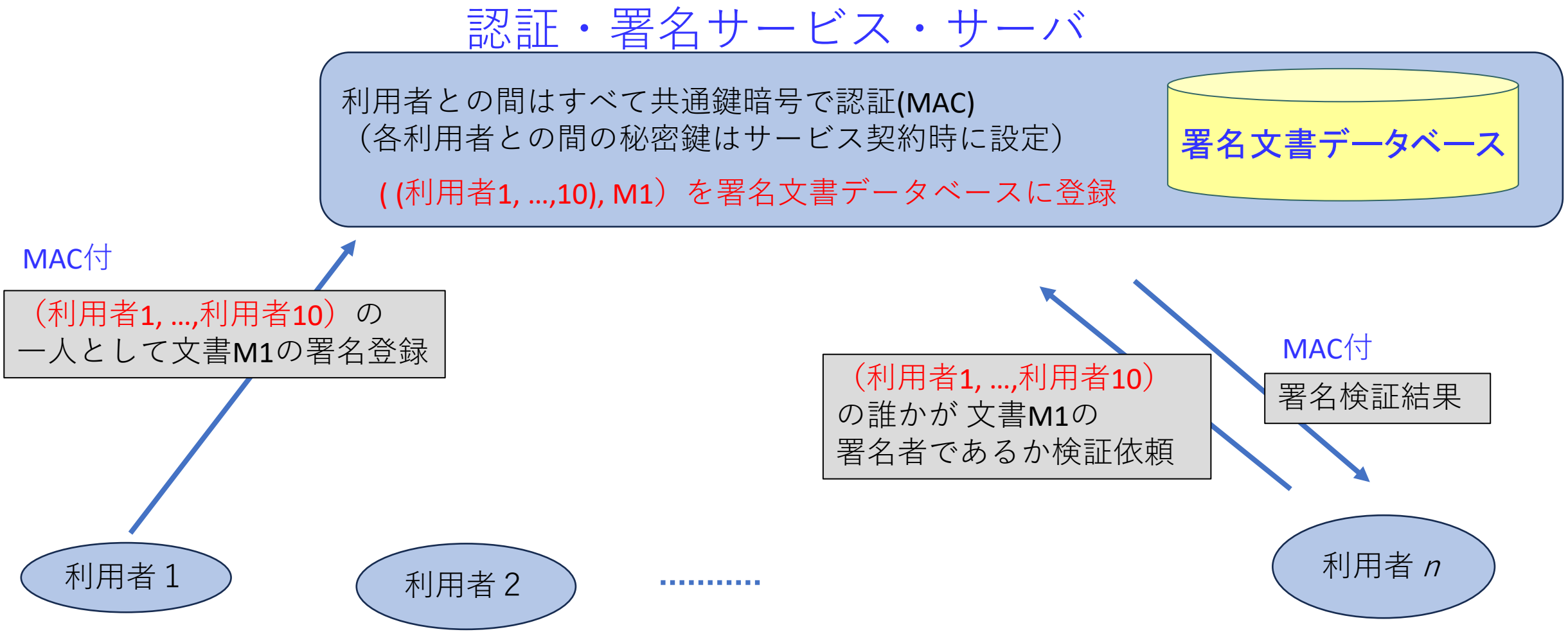
# 認証・署名サービス（基本）


認証・署名サービス・サーバ
利用者との間はすべて共通鍵暗号で認証(MAC)
（各利用者との間の秘密鍵はサービス契約時に設定）
(文書M1, 利用者１）を署名文書データベースに登録
署名文書データベース
MAC付
文書M1の署名登録
（利用者１，文書M1）
の署名検証依頼
MAC付
署名検証結果
利用者１
利用者２
.....
利用者 n

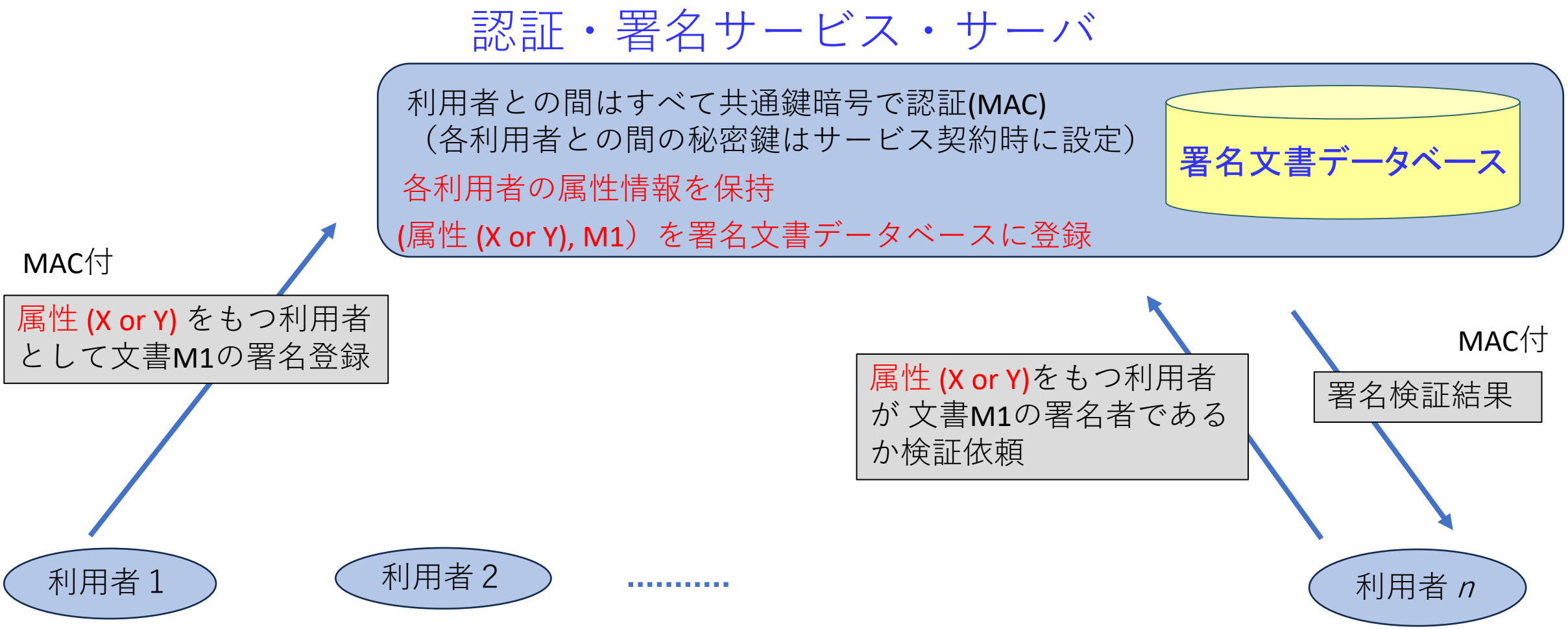
# 認証・署名サービス（応用1）



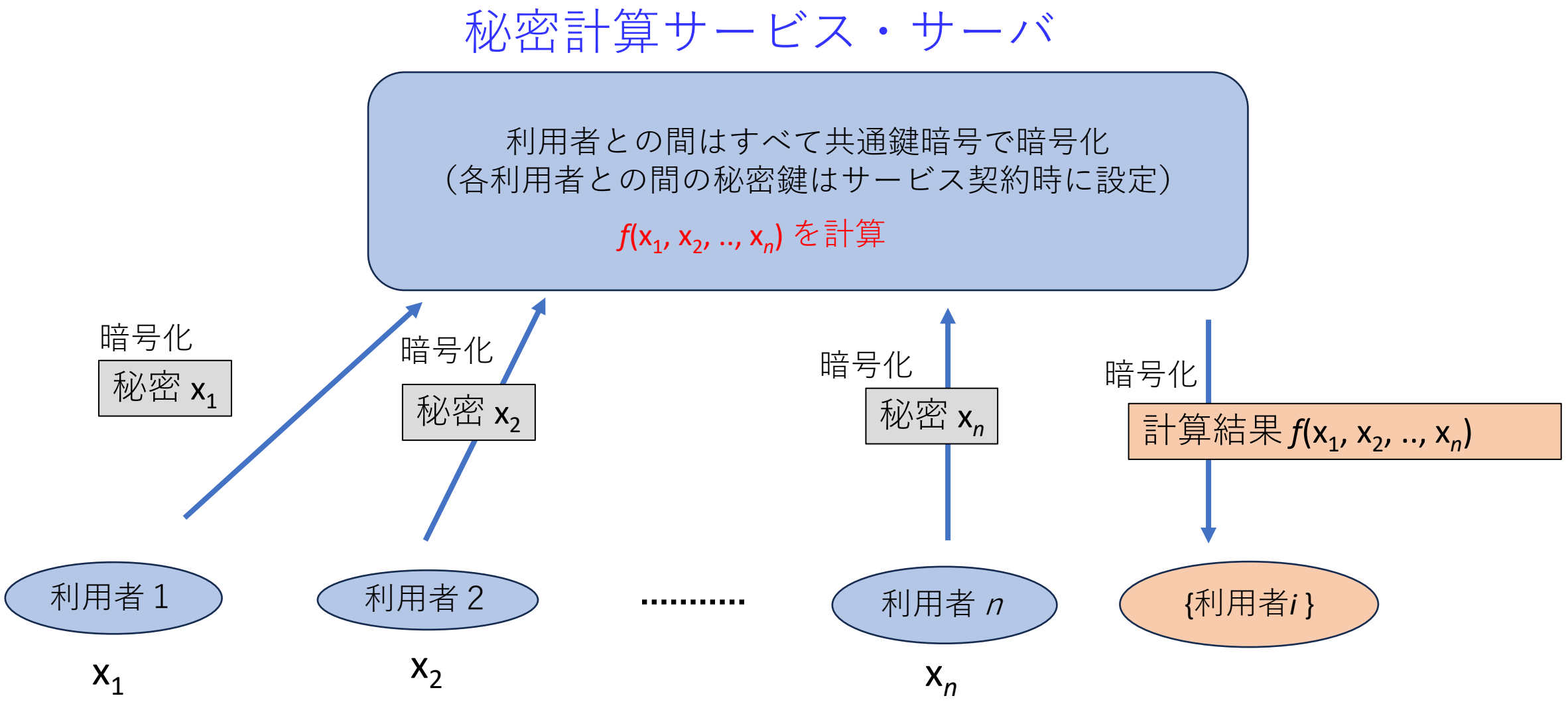
# 認証・署名サービス（応用２）



# 認証・署名サービス（応用３）



# 秘密計算サービス


秘密計算サービス・サーバ
利用者との間はすべて共通鍵暗号で暗号化
（各利用者との間の秘密鍵はサービス契約時に設定）
$f(x_1, x_2, .., x_n)$ を計算
暗号化
秘密 $x_1$
暗号化
秘密 $x_2$
暗号化
秘密 $x_n$
暗号化
計算結果 $f(x_1, x_2, .., x_n)$
利用者 1
利用者 2
.....
利用者 $n$
{利用者$i$}
$x_1$
$x_2$
$x_n$

# データベースサービス

## データベースサービス・サーバ

利用者との間はすべて共通鍵暗号で暗号化
（各利用者との間の秘密鍵はサービス契約時に設定）
検索依頼（データ$a_1$）に対して
利用者属性$q_1$がアクセス条件$f_1$を満足するか？

アクセス制御
(DBMS)

データベース

暗号化

利用者属性 $q_1$,
検索依頼

検索結果 $a_1$

利用者 1

利用者 2

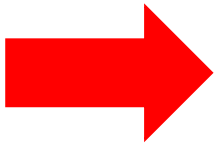
.....

利用者 *n*

# クラウドサービスによるアプローチの問題点

- クラウドに信頼性を含めてすべての機能・権限が集中
  （サービスが正しく機能するかは、クラウドの動作の正しさに全面的に依存。
  すべての利用者のプライバシー情報はクラウドが保有）
  集中／中央集権(centralized)
  → 分散／非中央集権(decentralized)

- クラウドに負荷が集中（非効率）
  → 効率化



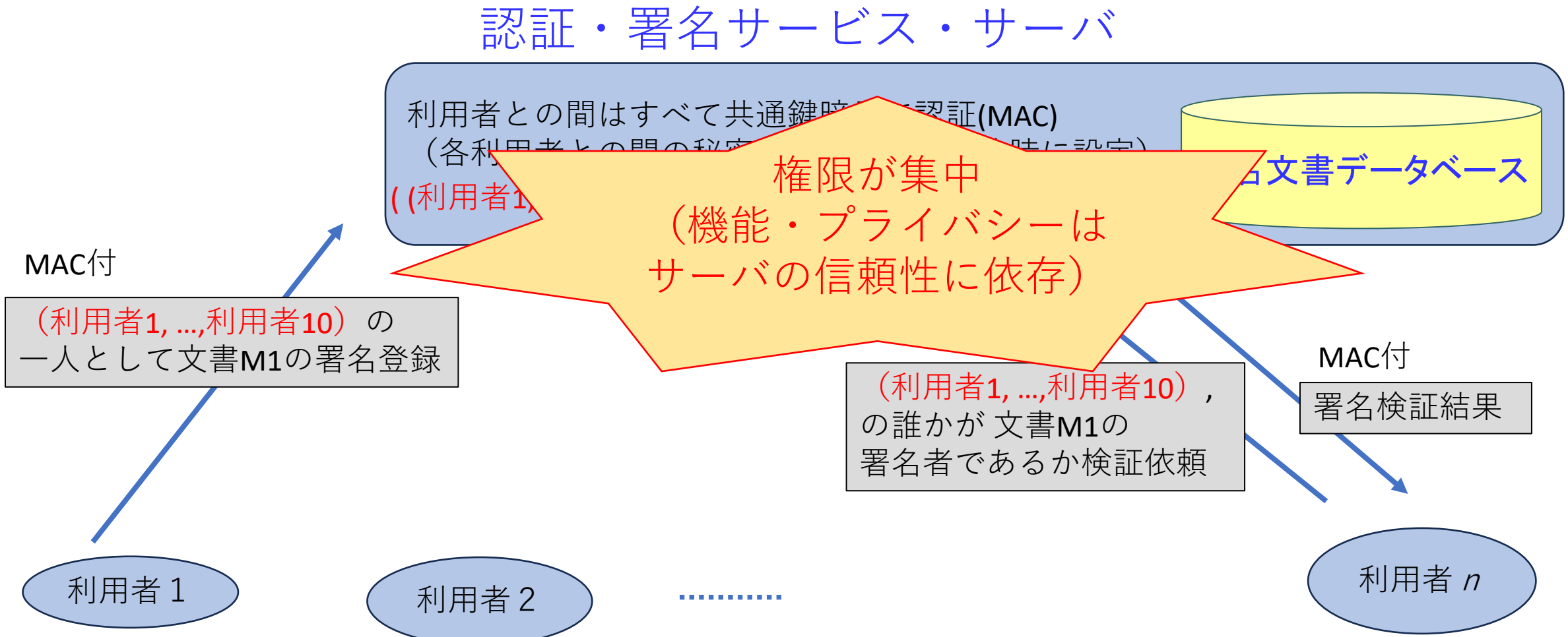
高機能暗号

# 高機能暗号

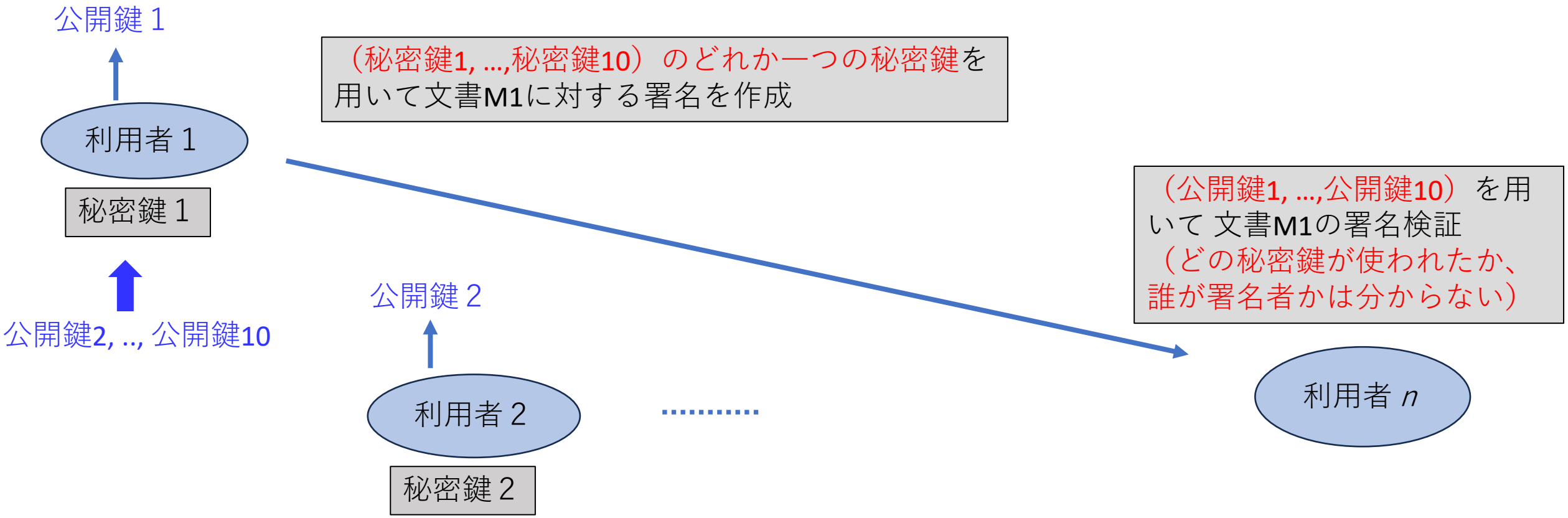
- 秘匿通信ービス → （公開鍵暗号）、プロキシ暗号、再暗号化、
  属性ベース暗号、検索可能暗号、放送型暗号
- 認証・署名サービス → （ディジタル署名）、グループ署名、
  リング署名、しきい値署名、属性ベース署名
- 秘密計算サービス → 多者秘密計算、準同型暗号、ゼロ知識証明
- データベースサービス → 属性ベース暗号、
  PIR (Private Information Retrieval) 、
  Oblivious RAM

etc

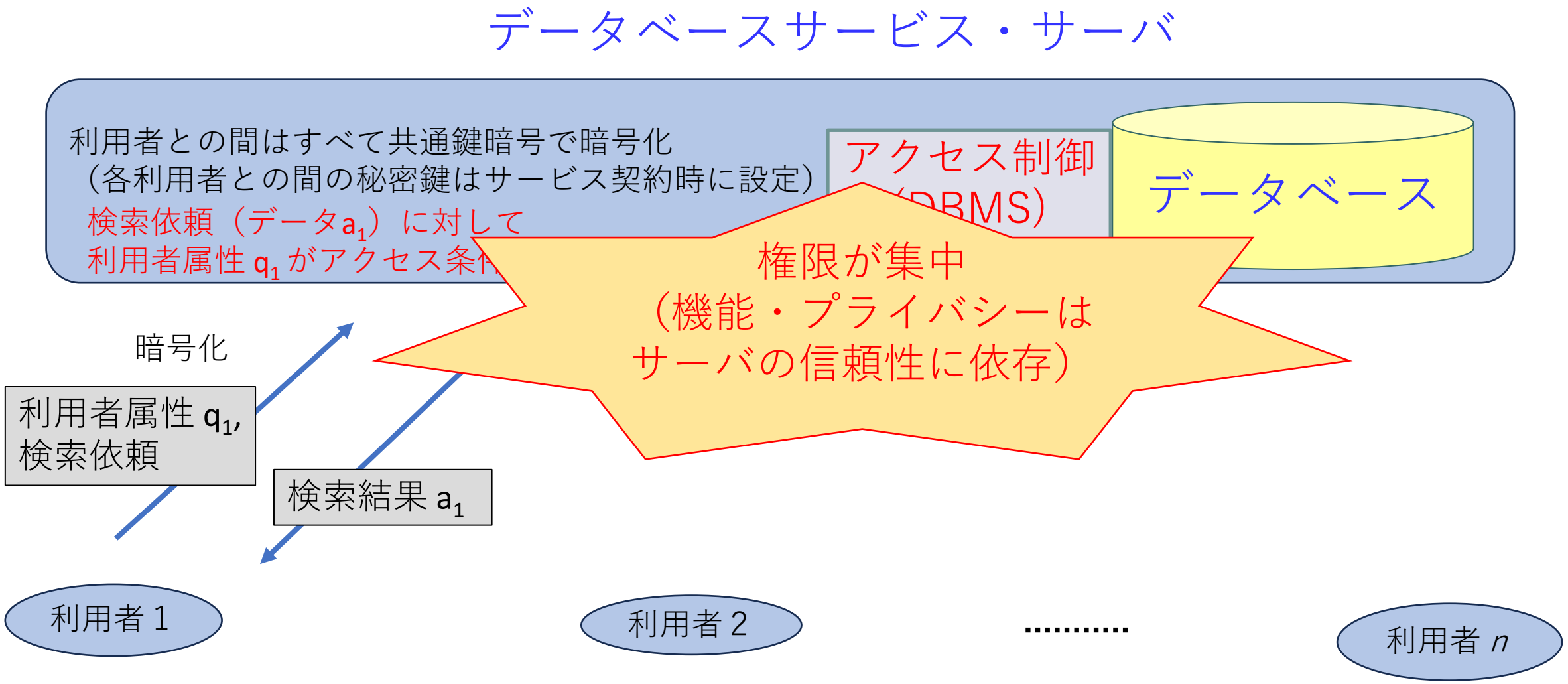
# 高機能暗号の例１：認証・署名サービス（権限の集中）



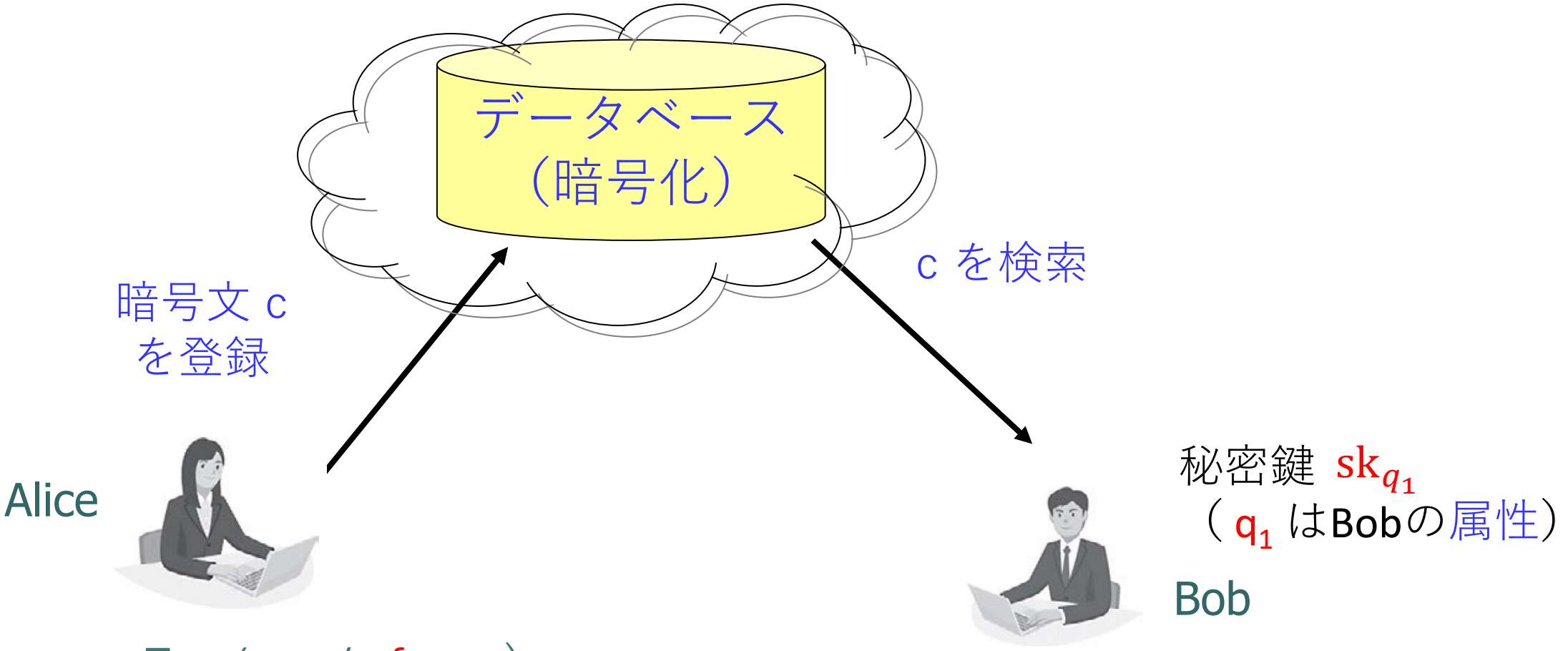
# 高機能暗号の例１：リング署名　（非中央集権化）



# 高機能暗号の例２：データベースサービス（権限の集中）



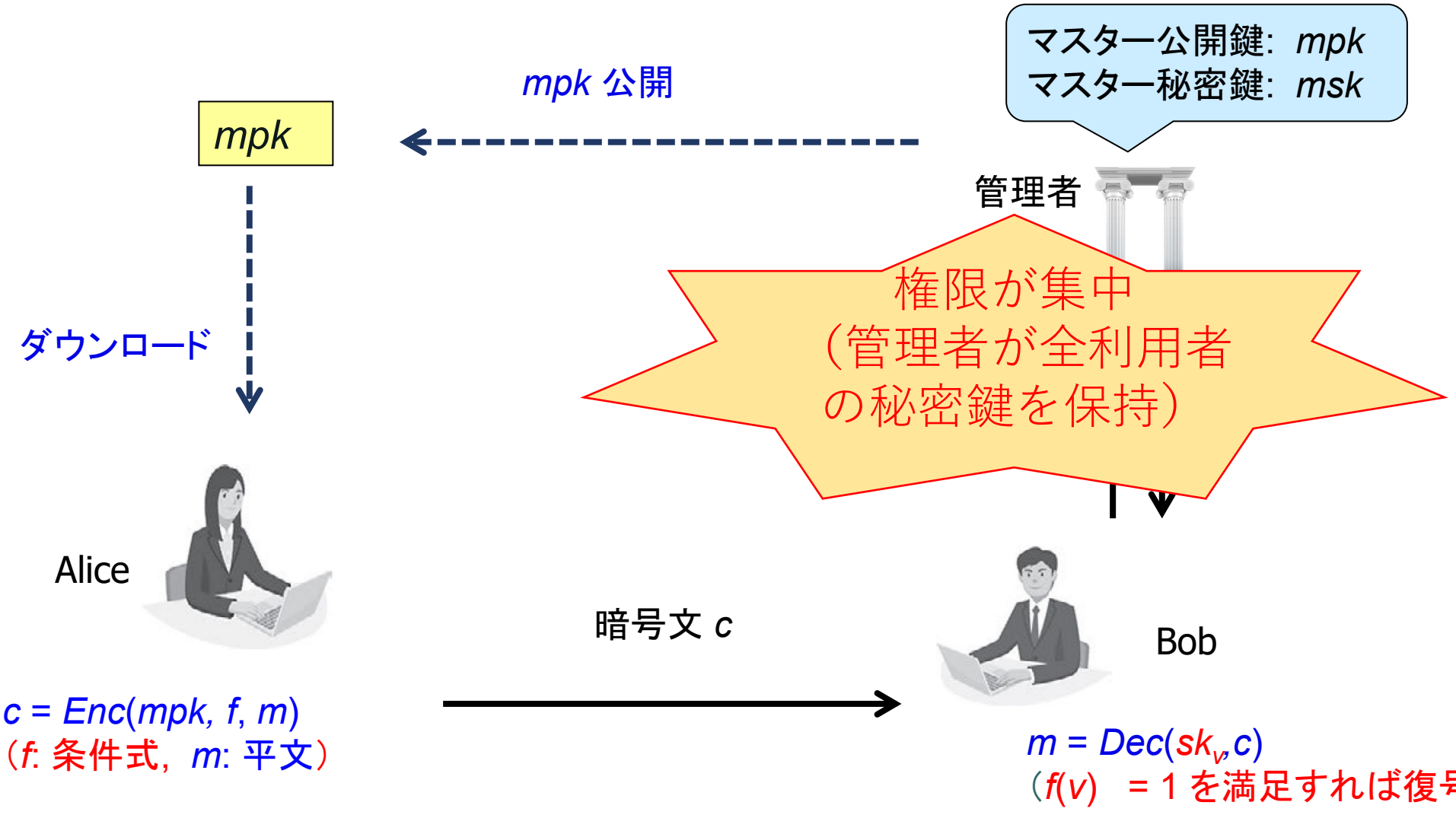
# 高機能暗号の例２：属性ベース暗号（非中央集権化）



# 研究課題

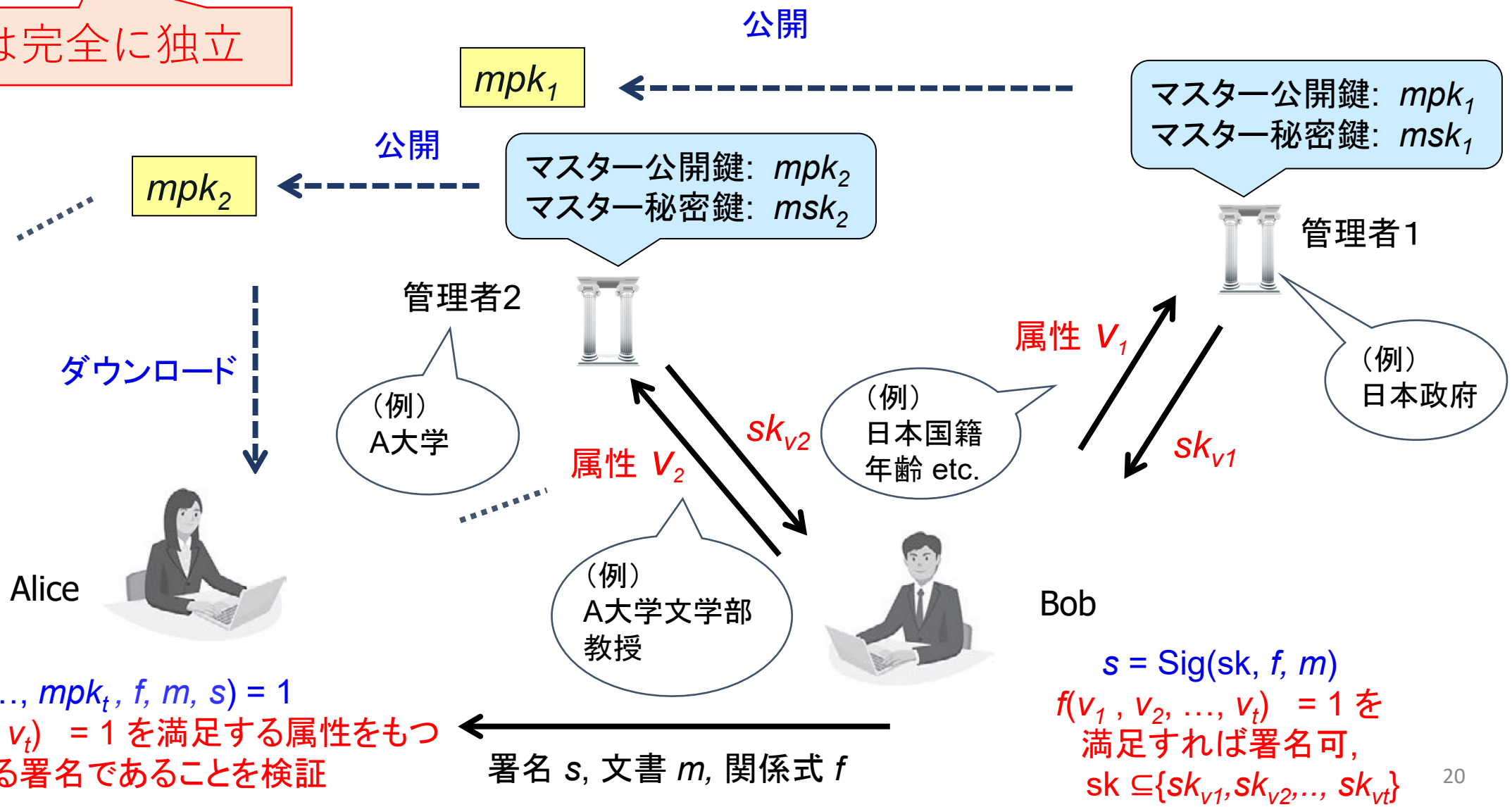
- 耐量子高機能暗号（例：LWE/SIS仮定ベース高機能暗号）
- 新しい機能への拡張（例：ブロックチェーンへの応用、Adaptor署名）
- 非中央集権化の推進（例：DMA-ABE/ABS)

# 非中央集権化の推進：
## （例）属性ベース暗号・署名（基本形）



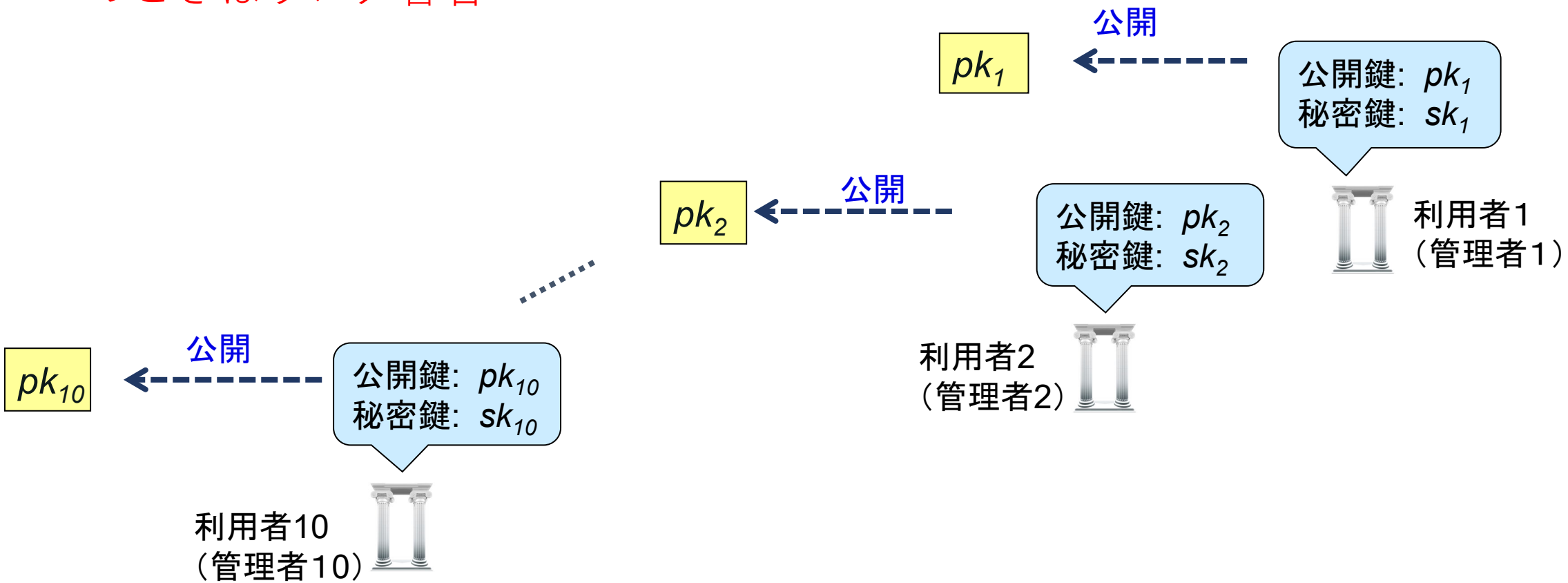
# 非中央集権化の推進：
## （例）DMA（非中央集権多管理者）属性ベース暗号・署名

各管理者は完全に独立



# 非中央集権化の推進：
## （例）DMA属性ベース署名はリング署名の一般化

$f(v_1, v_2, \ldots, v_t) = (v_1 = pk_1) \vee (v_2 = pk_2) \vee \ldots \vee (v_2 = pk_{10})$
のときはリング署名

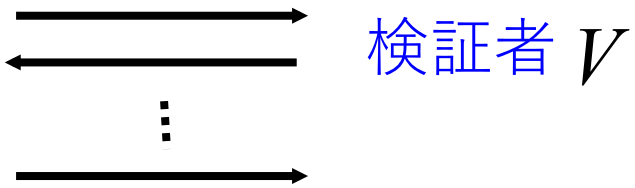


# 研究課題

- 耐量子高機能暗号（例：LWE/SIS仮定ベース高機能暗号）
- 新しい機能への拡張（例：ブロックチェーンへの応用、 Adaptor署名）
- 非中央集権化の推進（例：DMA-ABE/ABS)
- 利便性・性能向上・応用の進展（例：zk-SNARK, Doubly Efficient PIR)

# 利便性・性能向上・応用の進展：（例）ゼロ知識証明

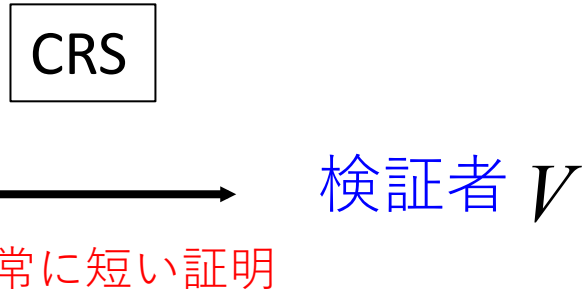
- 標準モデルでは、ゼロ知識証明は対話（4回以上）を必要とする。




- 非対話ゼロ知識証明（非標準モデル）において、標準的な仮定の下では証明サイズをある程度以上小さくできない。
- **非標準的なモデル／仮定**（CRS（共通参照情報）をシステムで共有するモデルやジェネリック群モデルなど）では、**非対話で非常に効率的な**（証明サイズが小さい）ゼロ知識証明が可能。ブロックチェーンなどで利用。

（例） zk-SNARK (Succinct Non-interactive ARgument of Knowledge)

証明のサイズが命題のサイズにかかわらず固定で非常に短い（例：群要素３つ）



# 研究課題

- 耐量子高機能暗号（例：LWE/SIS仮定ベース高機能暗号）
- 新しい機能への拡張（例：ブロックチェーンへの応用、 Adaptor署名）
- 非中央集権化の推進（例：DMA-ABE/ABS)
- 利便性・性能向上・応用の進展（例：zk-SNARK , Doubly Efficient PIR)
- 量子高機能暗号（例：量子マネー etc）

# まとめ

- 高機能暗号：様々なクラウドサービス（秘匿通信、認証・署名、秘密計算、データベースなど）に対して非中央集権化した効率的な解決策を提供

- 研究課題：
  - 耐量子高機能暗号
  - 新しい機能への拡張
  - 非中央集権化の推進
  - 利便性・性能向上・応用の進展
  - 量子高機能暗号