Ⅰ.生体認証の一般的な問題点

- 生体認証デバイスと認証サーバ間に、生体認証データを奪取するために、悪意のある中間者が入り込む可能性がある (主に以下の３経路)
  - 生体認証デバイス上でのタッピング (盗聴)
  - 生体認証デバイスが接続されたクライアント端末上でのデータ盗聴
  - 認証デバイスと認証サーバ間の通信データ盗聴

Ⅱ.生体認証と LR-AKE を組み合わせた場合

- **利点**
  - 生体認証情報と、LR-AKE のクライアント認証情報を使ったユーザ認証となるために、二要素認証となる。
  - 生体認証データが奪取されても、クライアント認証情報が奪取されなければ、中間者攻撃は成り立たない
  - 仮に、クライアント認証情報が奪取されても、その後に、LR-AKE 認証を行っていれば、奪取されたクライアント認証情報は意味のないものとなる
- **LR-AKEとの連携について**
  - 生体認証を生体認証サーバに対して行い、OK であれば、その固有 ID を取得（LR-AKEのパスワードと同義）
  - その取得した固有 ID を要素として、LR-AKE 認証を実行する