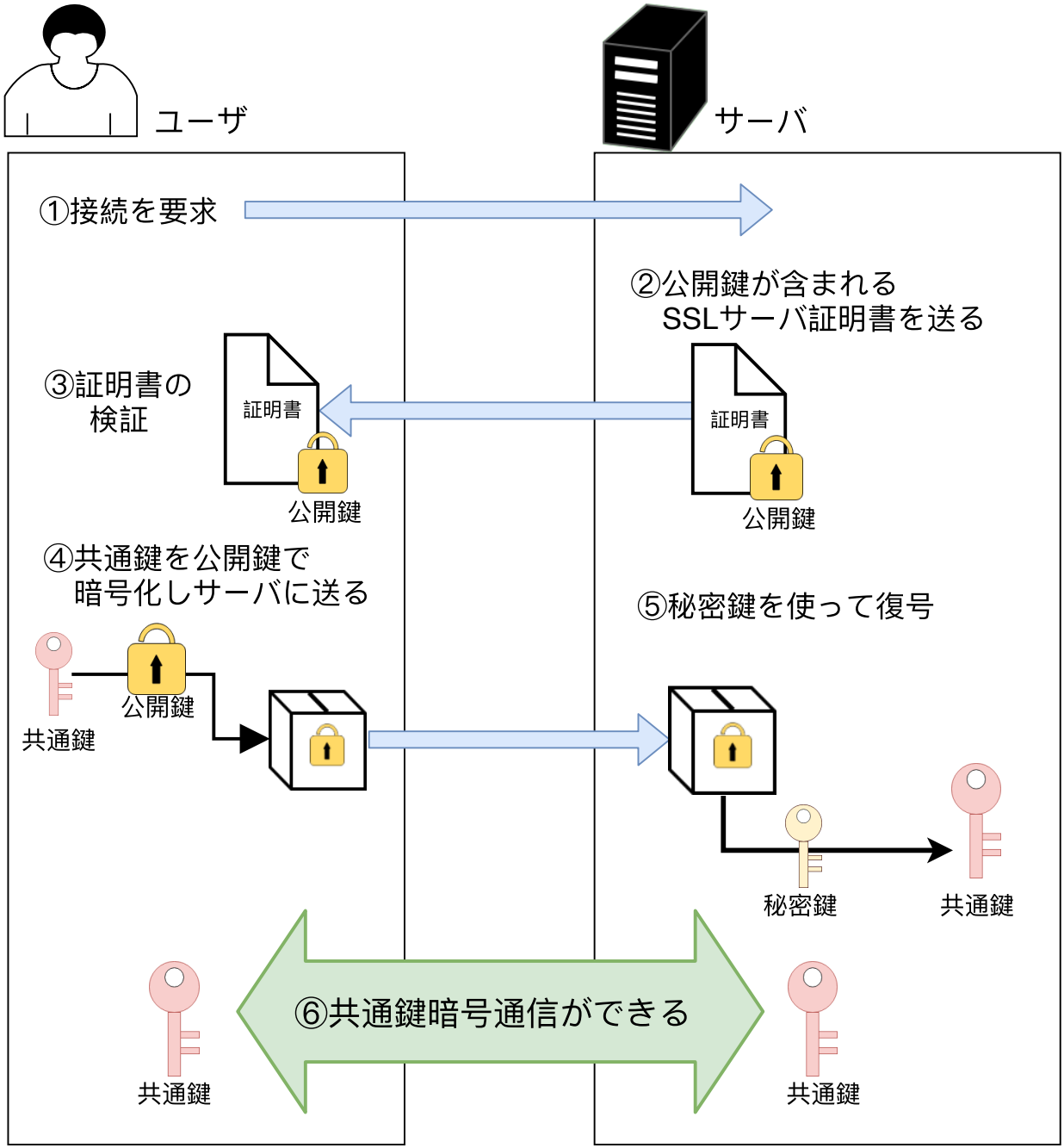
ユーザ
サーバ
①接続を要求
②公開鍵が含まれる
SSLサーバ証明書を送る
③証明書の
検証
証明書
公開鍵
証明書
公開鍵
④共通鍵を公開鍵で
暗号化しサーバに送る
公開鍵
共通鍵
⑤秘密鍵を使って復号
秘密鍵
共通鍵
⑥共通鍵暗号通信ができる
共通鍵
共通鍵