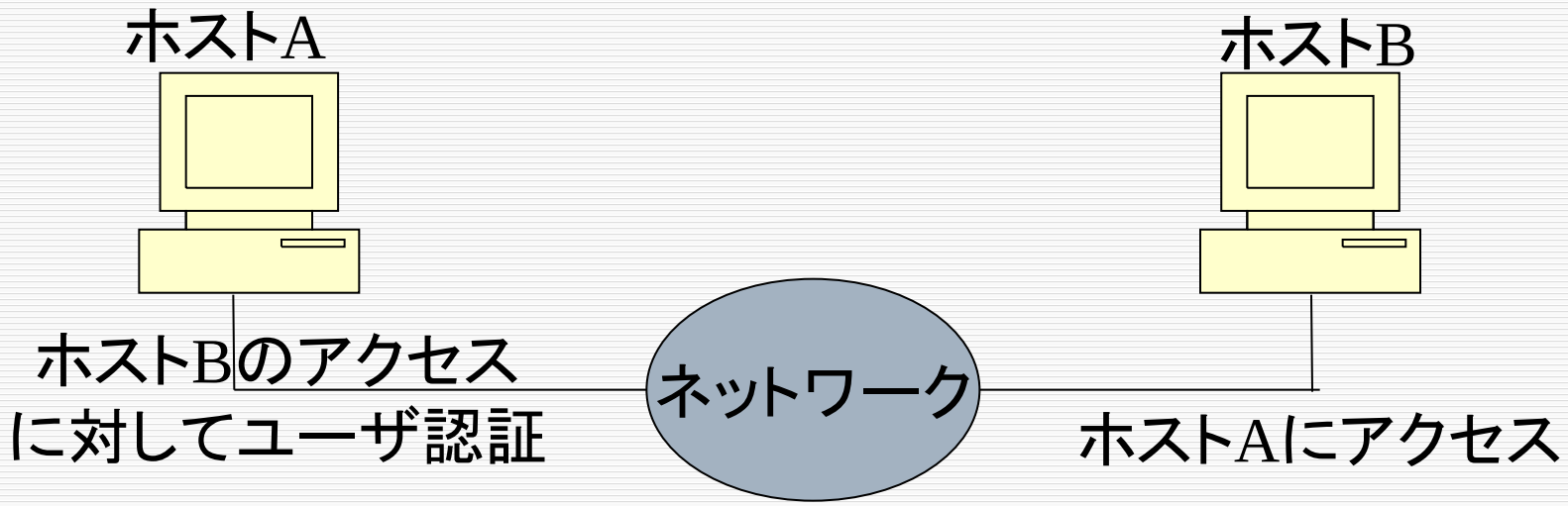
ユーザ認証

2002年9月6日

大橋 巧

ユーザ認証

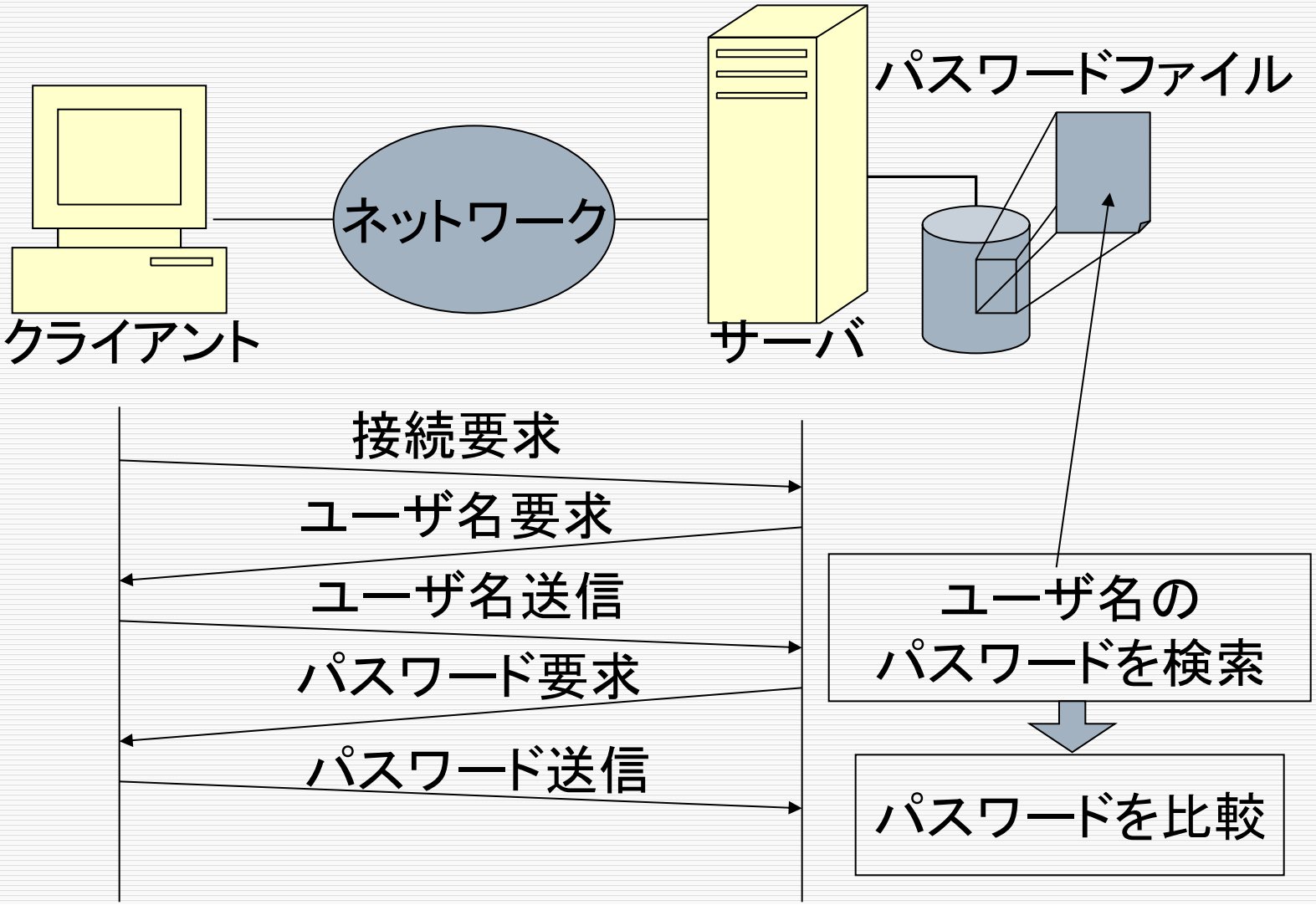
- コンピューターにログインできるユーザを限定
  - 不正行為を行うユーザを排除
- コンピュータにログインしているユーザを識別
  - 各ユーザに応じてアクセスできる範囲を限定
    - 不正なデータ改ざんを防止



ユーザ認証の方法

- パスワードファイルを用いたユーザ認証
  1. パスワードファイルにユーザ名とパスワードを保存
     - /etc/passwdなど
  2. ユーザがアクセスするとユーザ名を識別
  3. ユーザにパスワードを要求し、パスワードファイルのパスワードと比較
  4. パスワードが一致すれば正当なユーザと認証

ユーザ認証例


パスワードファイル
ネットワーク
クライアント
サーバ
接続要求
ユーザ名要求
ユーザ名送信
パスワード要求
パスワード送信
ユーザ名の
パスワードを検索
パスワードを比較

アクセス管理技術

- 電子化された情報を保護するためにユーザのアクセスを管理する技術。
  - 識別・・・アクセスを許可するユーザID
  - 認証・・・ユーザIDとパスワード
  - 権限付与・・・ユーザのアクセス可能な範囲

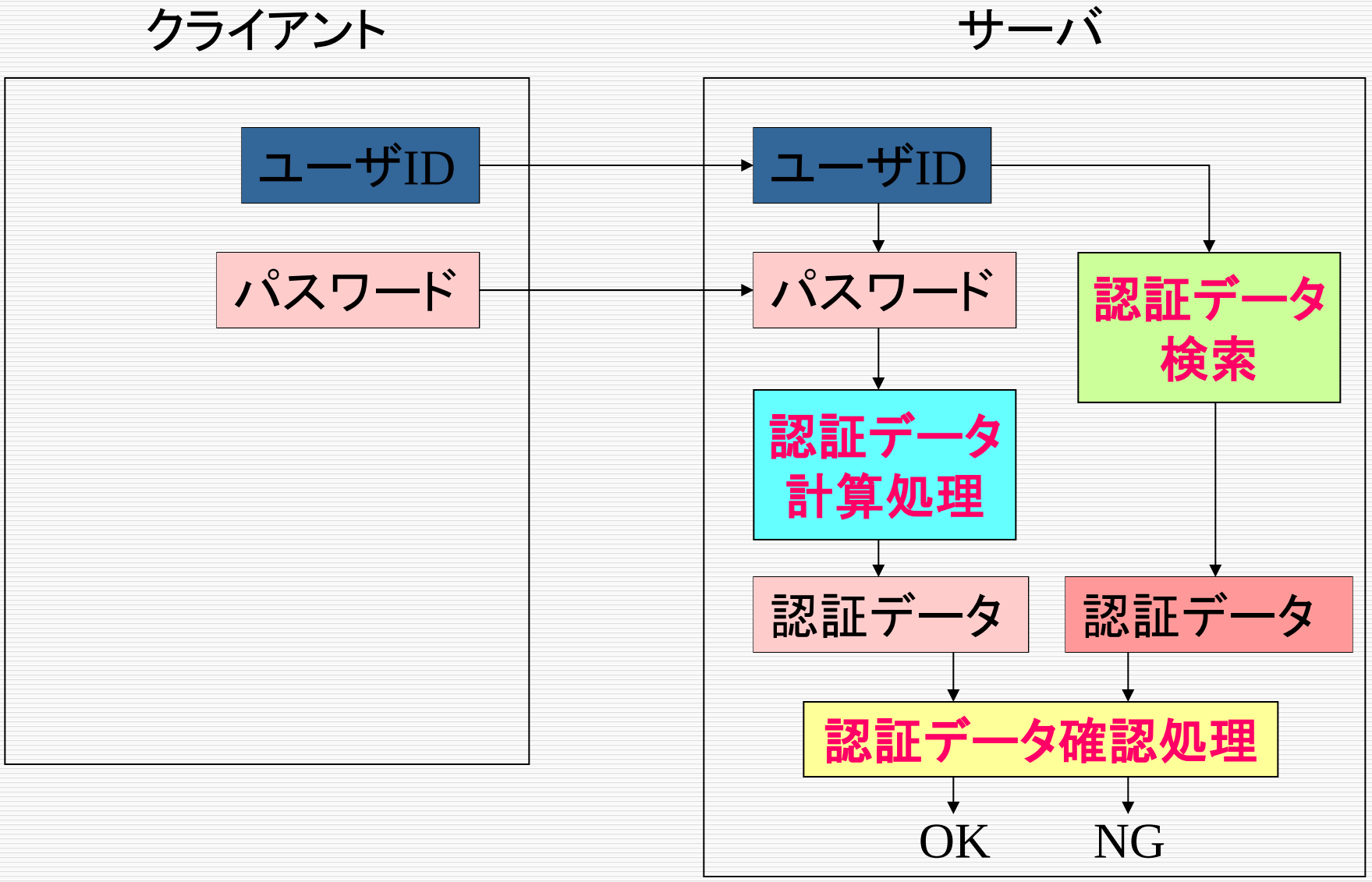
認証の種類

- パスワードファイルを用いた認証
- ワンタイム・パスワードによる認証
- S/KEYによる認証
- 暗号技術を用いた認証

パスワードファイルを用いた認証

- パスワードファイル
  - ユーザ名、ユーザIDとパスワードの組を登録したファイル。
- 認証の流れ
  - ユーザはユーザ名とパスワードを入力
  - それに応じてコンピュータはユーザIDとパスワードをパスワードファイルから探し出す
  - 登録されているパスワードと入力されたパスワードが一致すれば正当なユーザであるとみなす

認証シーケンス


クライアント
サーバ
ユーザID
パスワード
ユーザID
パスワード
認証データ
検索
認証データ
計算処理
認証データ
認証データ
認証データ確認処理
OK
NG

パスワード認証の危険要因

- ログイン時におけるパスワード漏洩
  - 偽のログインプログラムを立ち上げておき,ユーザ名とパスワードを騙し取る.(ログインシミュレーター)
- ログイン試行
  - ユーザ名とパスワードの組み合わせをしらみつぶしに試す.

盗聴の容易性

- TELNET,FTP,r系コマンド
  - パスワードを平文で流す
- 対策
  - 暗号化
    - TELNET→SSH
    - POP3→APOP
    - メール→PGP暗号化
  - ワンタイムパスワード（OTP）
    - S/KEY

ワンタイム・パスワード

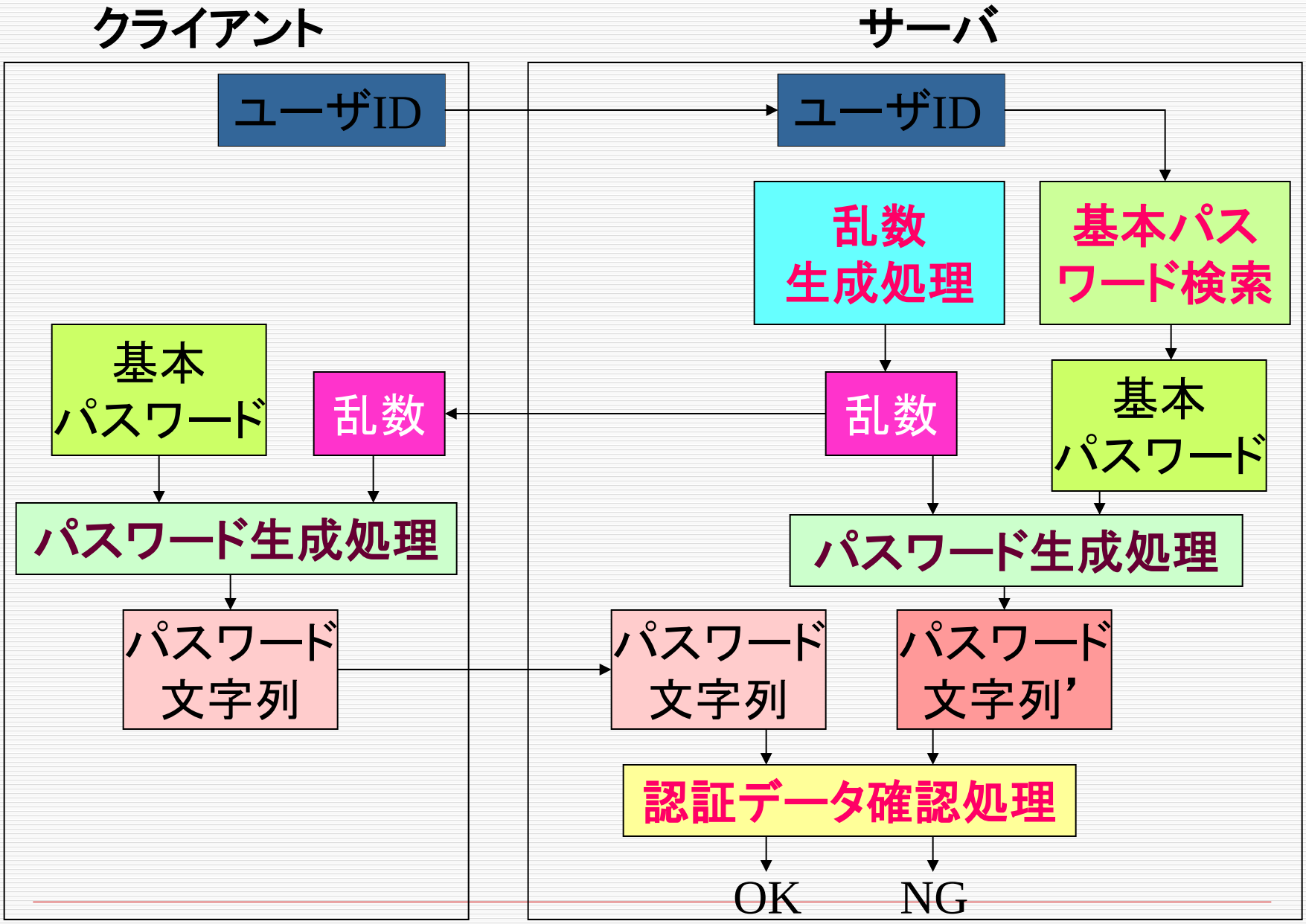
- ログインの際、ネットワーク上でパケットデータを補足されると、ユーザ名とパスワードが漏洩してしまう。

- 一度きりしか有効でないパスワードを使用する。(OTP:One Time Password)
  - チャレンジ・アンド・レスポンス方式

チャレンジ・アンド・レスポンス方式

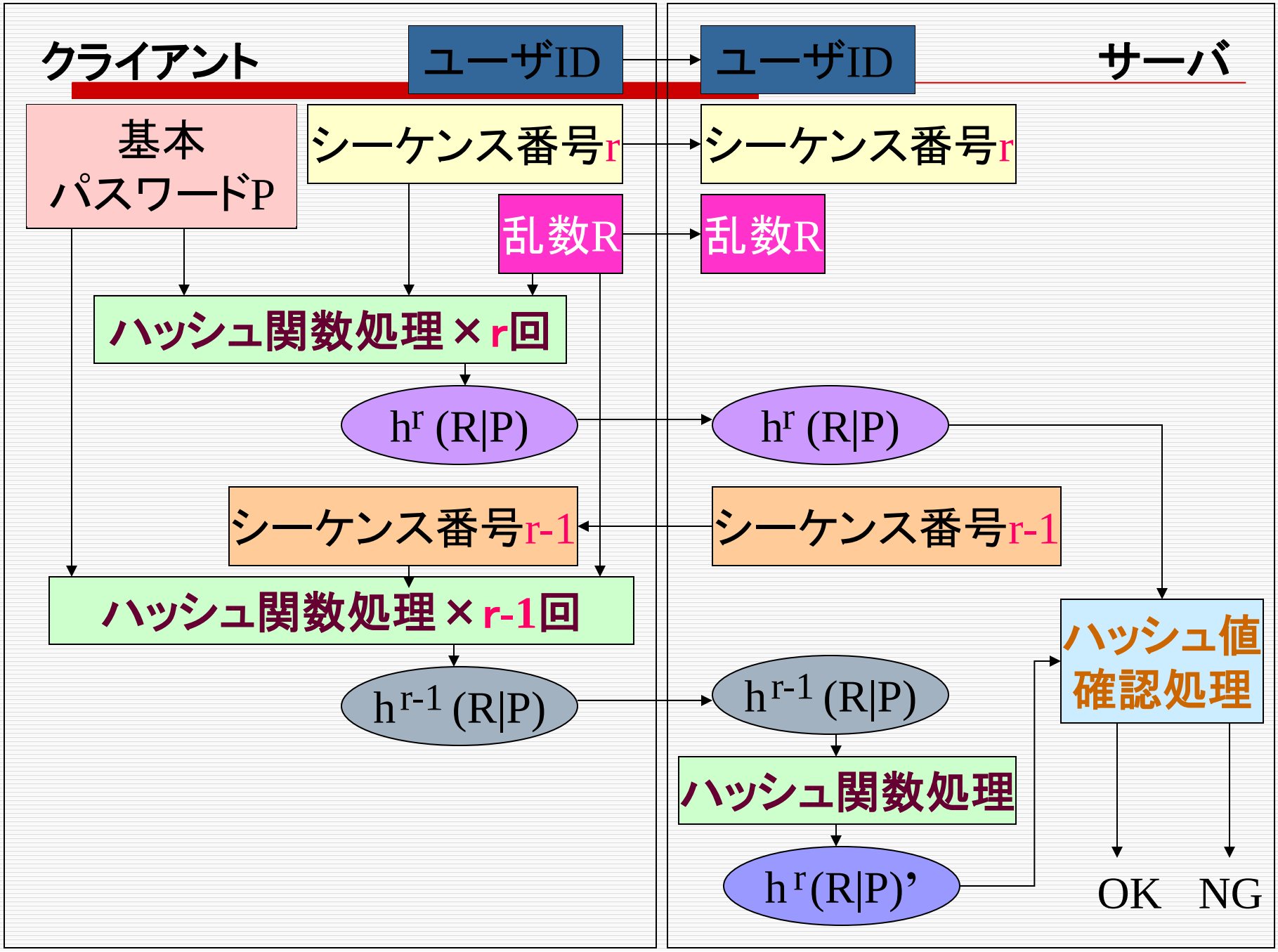
- サーバ側が送信した質問（チャレンジ）に、正しい答え（レスポンス）を返したクライアントを正規のユーザとして認証する。
- 質問と答えが毎回変わるので、リプレイ攻撃を防ぐことが可能。

認証シーケンス


クライアント
サーバ
ユーザID
ユーザID
乱数
生成処理
基本パス
ワード検索
基本
パスワード
乱数
乱数
基本
パスワード
パスワード生成処理
パスワード生成処理
パスワード
文字列
パスワード
文字列
パスワード
文字列’
認証データ確認処理
OK
NG

S/KEY

- サーバ側が基本パスワードを持たない方式。
- 複数回、ハッシュ関数を適用した値を用いる。
- サーバ側で格納される値が、ログインの度に変更される一時的なものであり、漏洩したとしてもハッシュ関数の性質からパスワードの推測が出来ない。


クライアント
ユーザID
ユーザID
サーバ
基本
パスワードP
シーケンス番号r
シーケンス番号r
乱数R
乱数R
ハッシュ関数処理×r回
hr (R|P)
hr (R|P)
シーケンス番号r-1
シーケンス番号r-1
ハッシュ関数処理×r-1回
ハッシュ値
確認処理
hr-1 (R|P)
hr-1 (R|P)
ハッシュ関数処理
hr(R|P)’
OK
NG