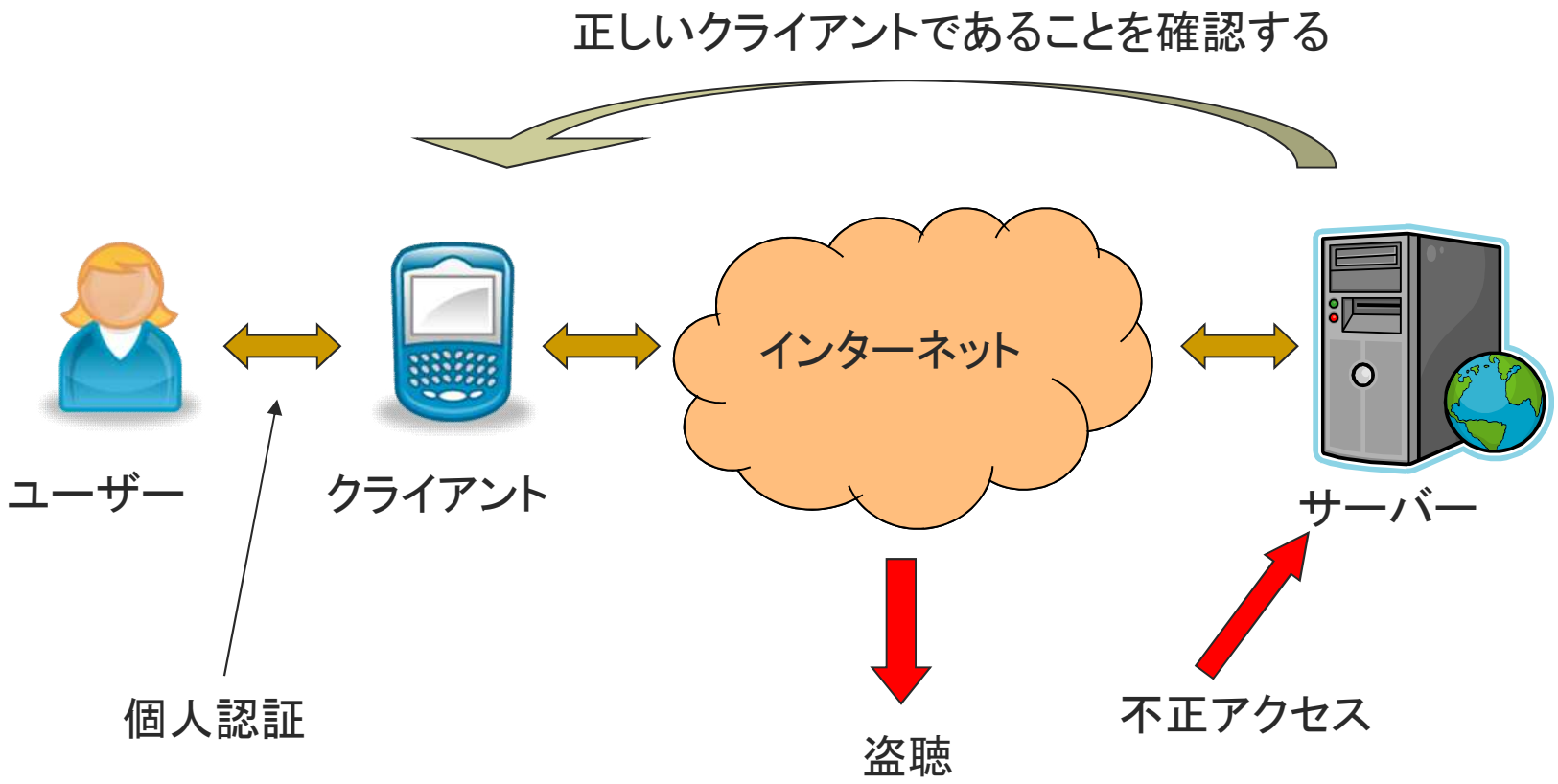
クライアント認証

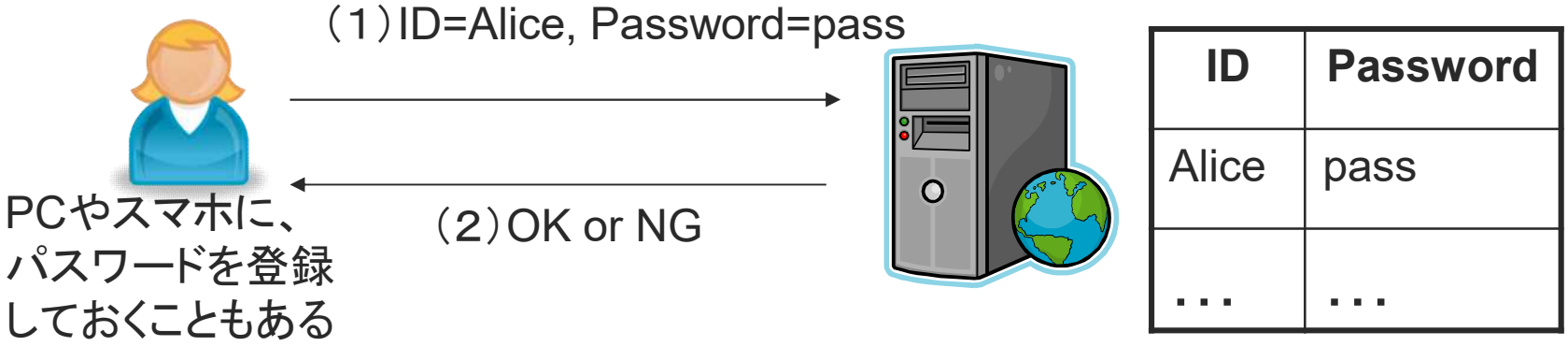
クライアント認証とは


正しいクライアントであることを確認する
インターネット
ユーザー
クライアント
サーバー
個人認証
盗聴
不正アクセス

認証方式の種類

- 名前による認証（厳密には認証でない）
  ID,グループ名,アドレス等の一致を確認
- パスワード認証方式
- ワンタイムパスワード方式
- チャレンジレスポンス方式
- 公開鍵認証方式
- （バイオメトリクス認証方式）

パスワード認証方式（基本）



☆パスワード認証方式に対する脅威、問題点

1. オンライン攻撃（通信チャンネルの盗聴）

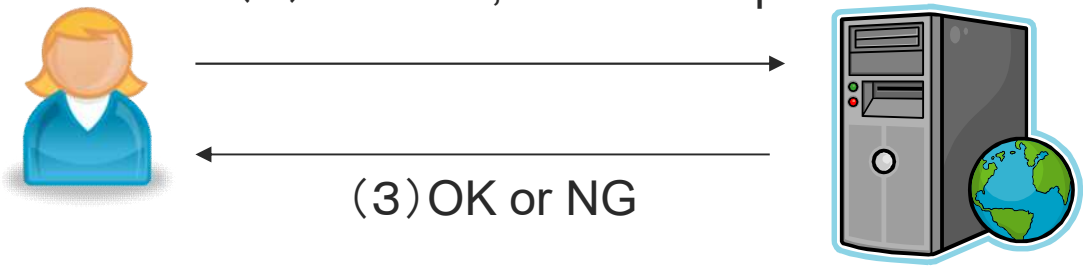
　　キーボードの盗み見、スパイウェアによる監視も

2. オフライン攻撃（サーバのデータベースの解析）

　　パソコンの紛失、盗難も同じこと

3. スケーラビリティ（ユーザ数やサーバ数に対する拡張性）

パスワード認証方式（ハッシュ）



ID	Hash
Alice	#$3aBk
…	…

（2）Hash(“pass”)を計算、照合

- オフライン攻撃に強くなる（ソルトを使用することもある）
- オンライン攻撃には無力

  - 安全なハッシュ関数を用いれば、ハッシュ値から逆算してパスワードを求めることは困難
  - 安易に推測可能なパスワードの場合、ハッシュ値の一致を確認するのは容易

パスワードソルトの利用

- パスワードハッシュ表が漏洩した場合

ID	ハッシュ値
Alice	3Eak7rv
....	
Bob	3Eak7rv
....	

- 表中に同じハッシュ値があると、同じパスワードであることが分かる
- あらかじめ、パスワードとハッシュ値の対応表を作成しておくことが可能

ID	ソルト	ハッシュ値
Alice	FjI8w	oyBb4ap
....		
Bob	5nnCi	80qvZ9e
....		

- ソルトの値（乱数）を登録時に決める
- ハッシュ値$H = Hash(Salt|Pass)$のように求める
- 同じパスワードを使用していてもハッシュ値は異なる
- 事前にパスワードとハッシュ表の対応を計算しておくことができない

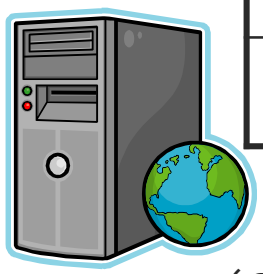
リプレイ攻撃

脆弱性を持つ例

鍵 K

（1）ID=Alice, E(K, pass)

（4）OK or NG



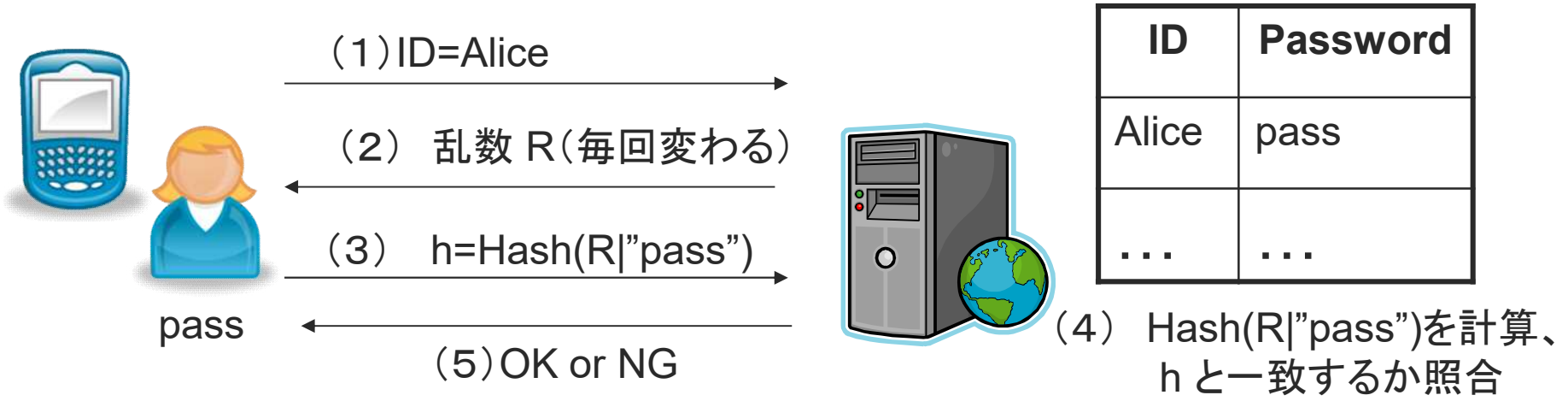
ID	Key	Hash
Alice	K	#$3aBk
…	…	…

（2）E(K,pass)を復号
（3）Hash(“pass”)を計算、照合

E(K, data)： 鍵Kによるdataの暗号化

- オンライン攻撃に強くなる？
- リプレイ攻撃に対して無力

チャレンジレスポンス方式



- オンライン攻撃（リプレイ攻撃）不可
- オフライン攻撃は可能
- ワンタイムパスワード（後述）の一つとも考えられる

チャレンジレスポンス方式(2)

鍵K

（1）ID=Alice

（2） 乱数 R（毎回変わる）

（3） s=E(K,R)

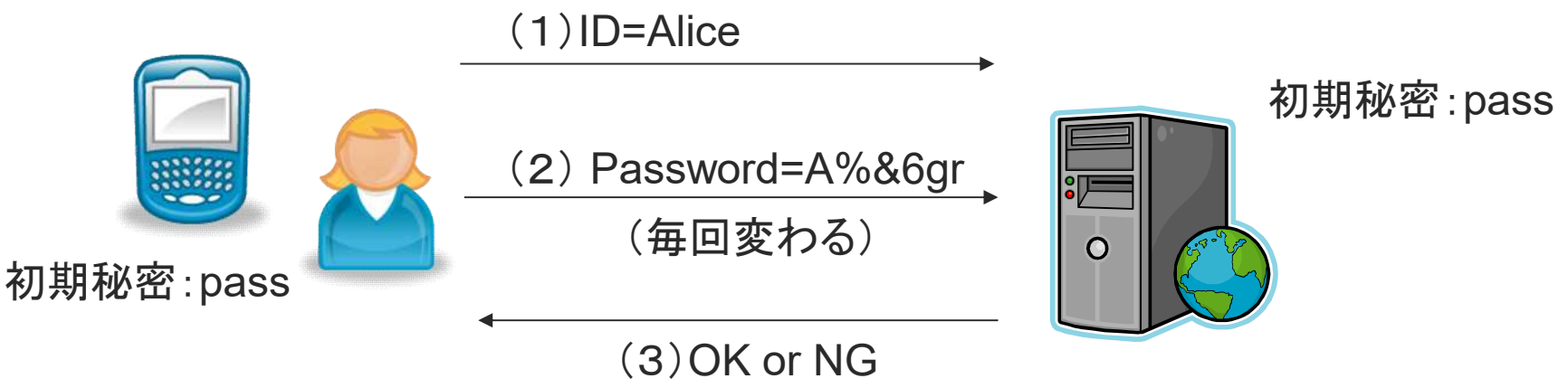
（5）OK or NG

ID	Key
Alice	K
…	…

（4） sを復号し、
Rと一致するか照合

- オンライン攻撃（リプレイ攻撃）不可
- オフライン攻撃は可能
- 鍵情報が漏洩した場合の影響大

ワンタイムパスワード方式



- オンライン攻撃（リプレイ攻撃）不可
- パスワード計算デバイスが必要
- 定期的に更新が必要な場合も
- フリーソフトウェアでは S/Keyが有名（ハッシュ関数の性質を利用）

デバイスとサーバで時刻に同期して、定期的にパスワードが変更される

ワンタイムパスワード（Lamport）

準備

$P_N = H^N(P)$

保存

N－1

1回目のログイン

$P_{N-1} = H^{N-1}(P)$

？

$H(P_{N-1}) = P_N$

P_{N-1}を保存

N－2

2回目のログイン

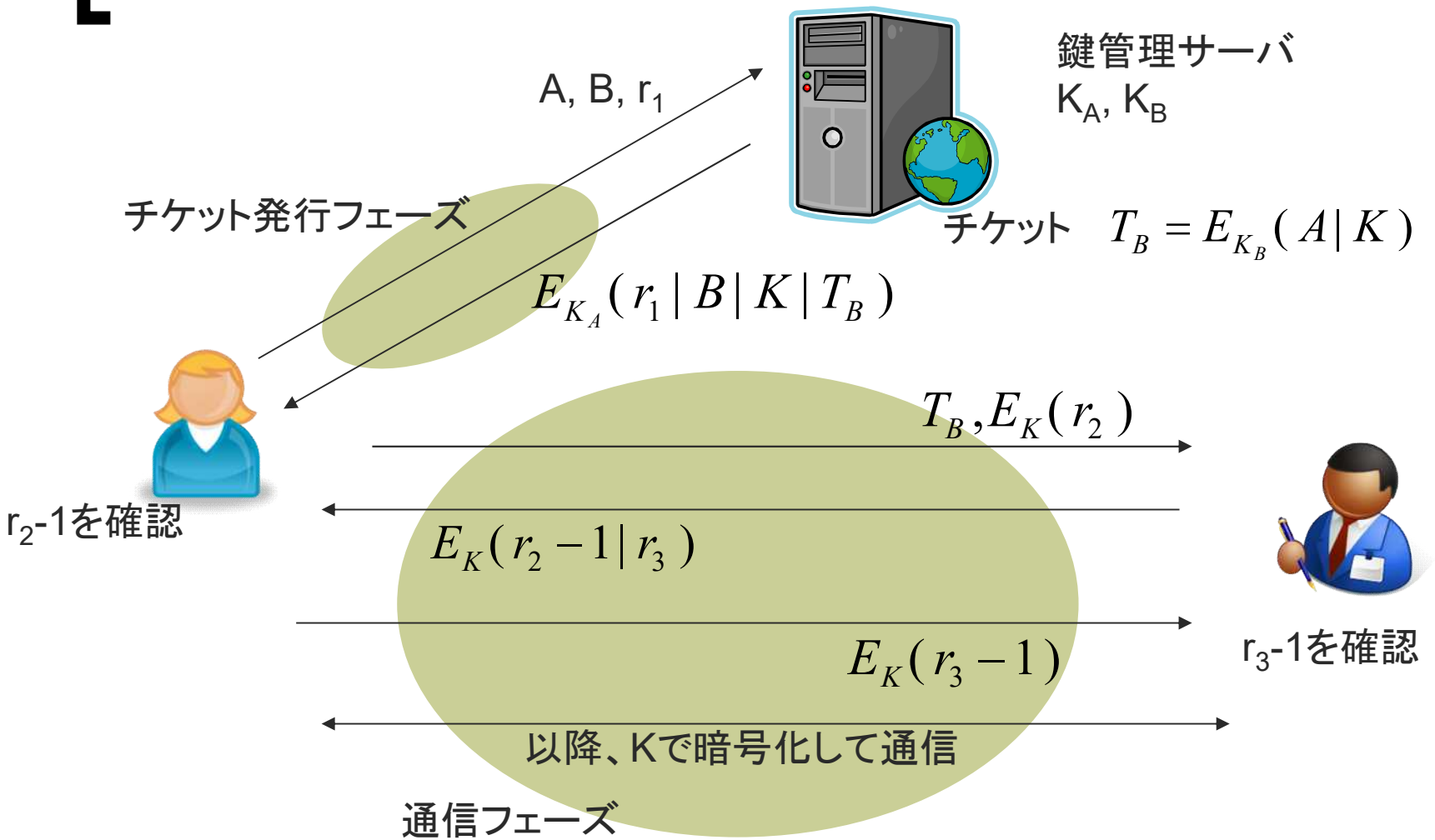
$P_{N-2} = H^{N-2}(P)$

？

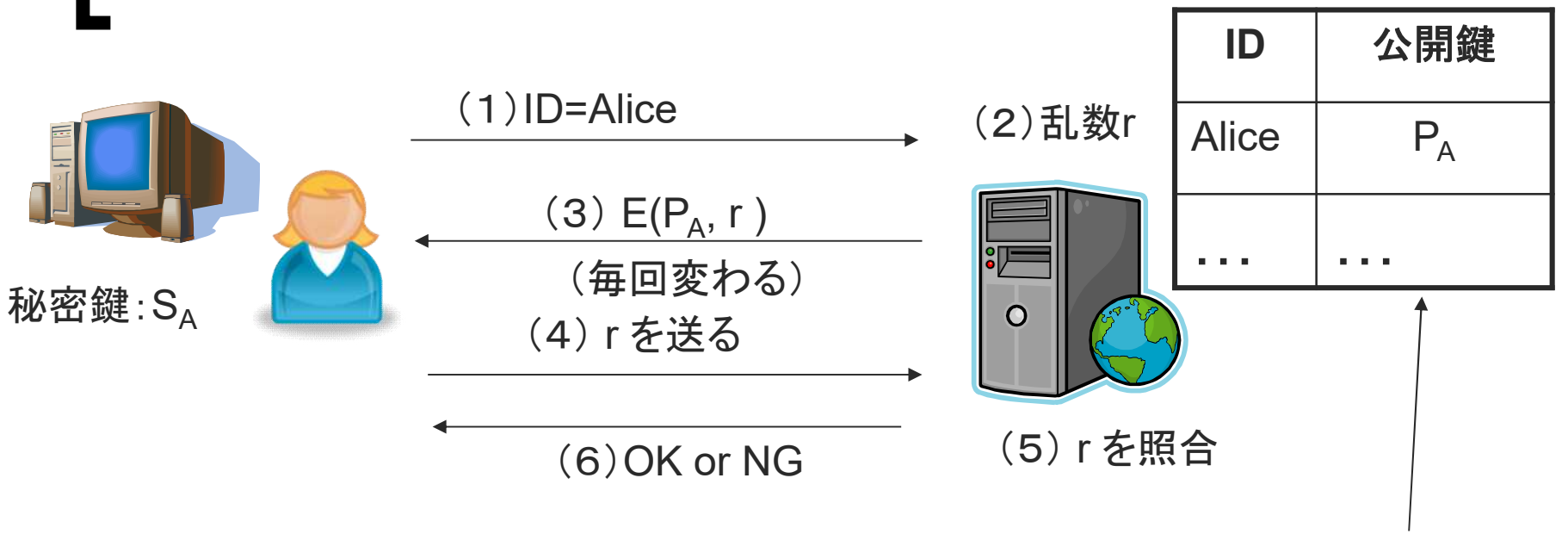
$H(P_{N-2}) = P_{N-1}$

P_{N-2}を保存

チケット方式（Kerberos）

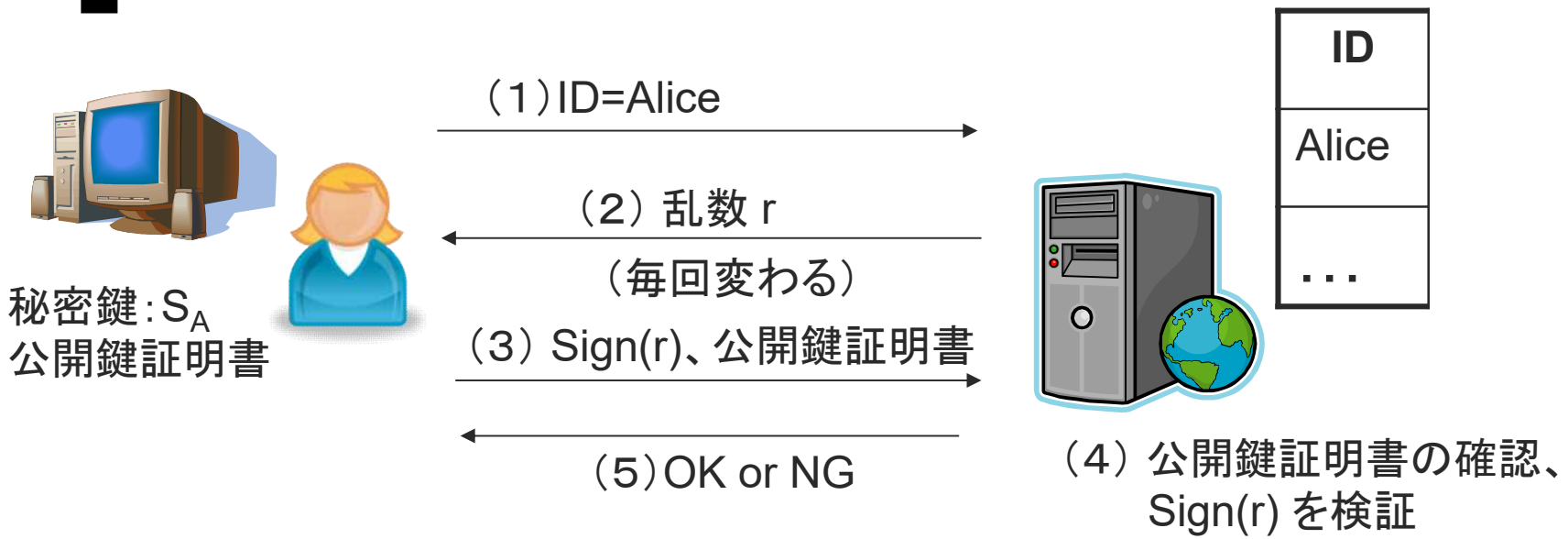


公開鍵による方式



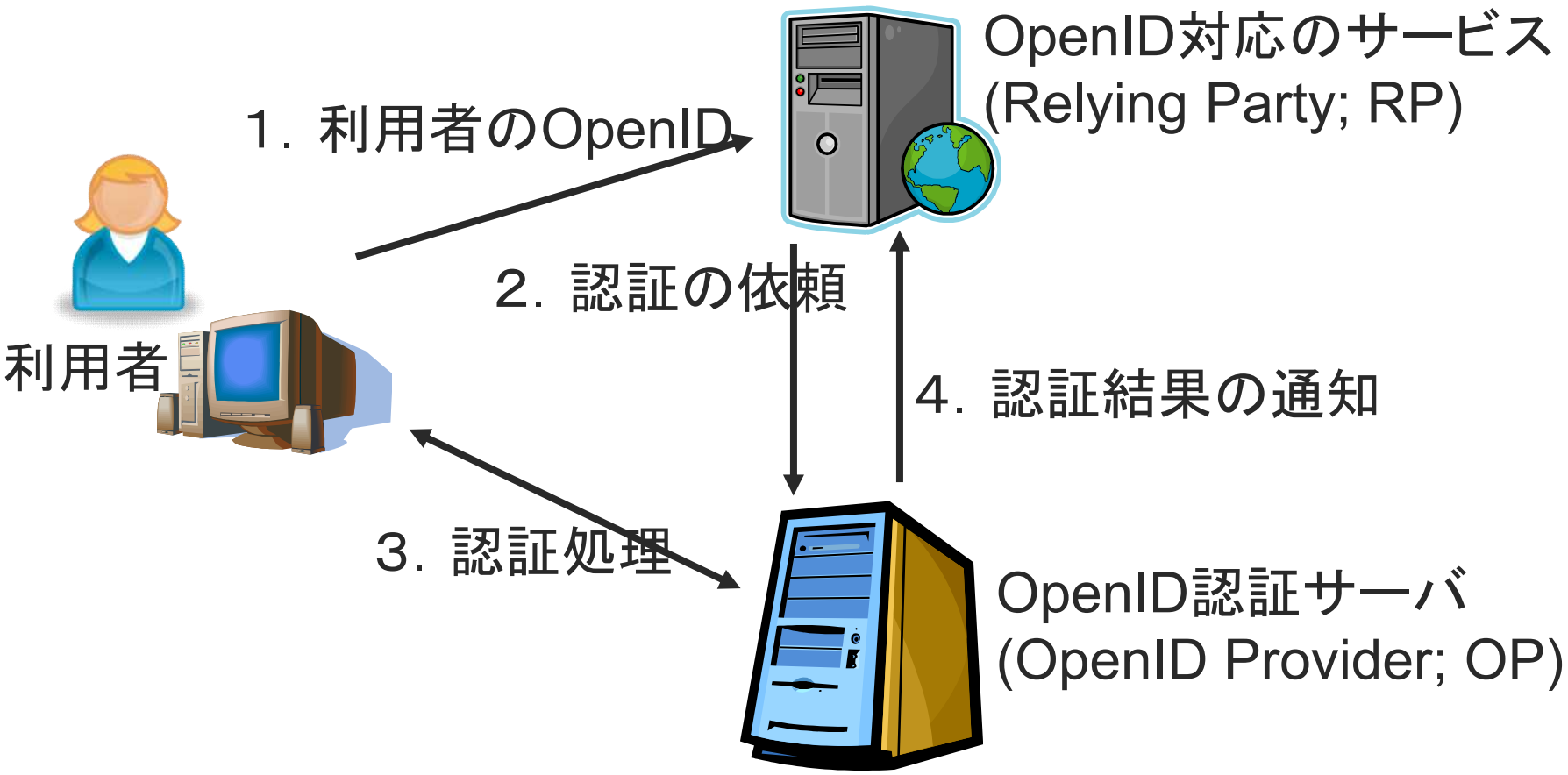
- オンライン攻撃（リプレイ攻撃）不可
- オフライン攻撃不可
- 秘密漏洩時の影響が小さい
- 計算量が多い（最近は多くの場合問題なし）

公開鍵による方式（2）



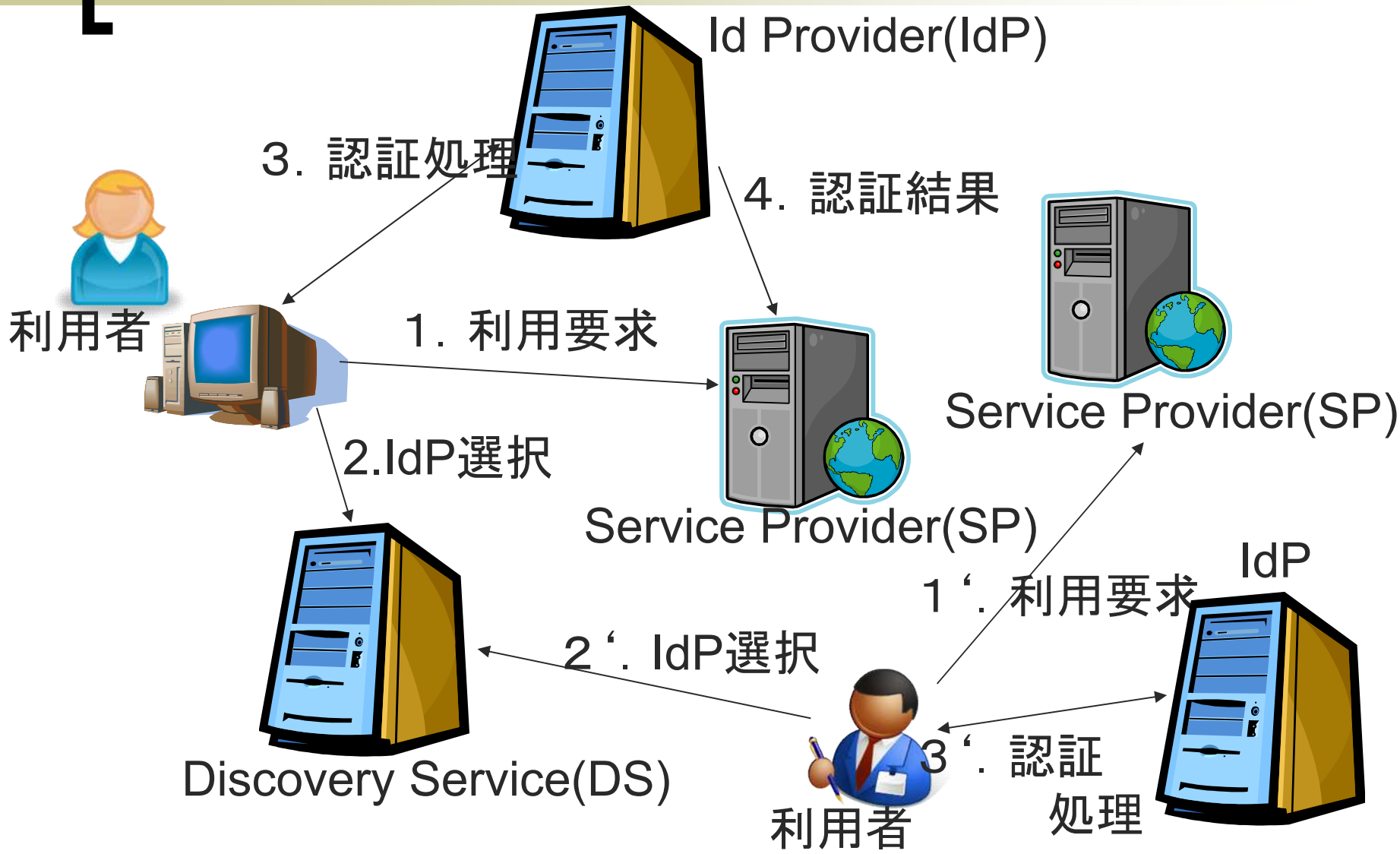
- あらかじめ公開鍵証明書を発行してもらう必要あり

OpenIDによる利用者認証

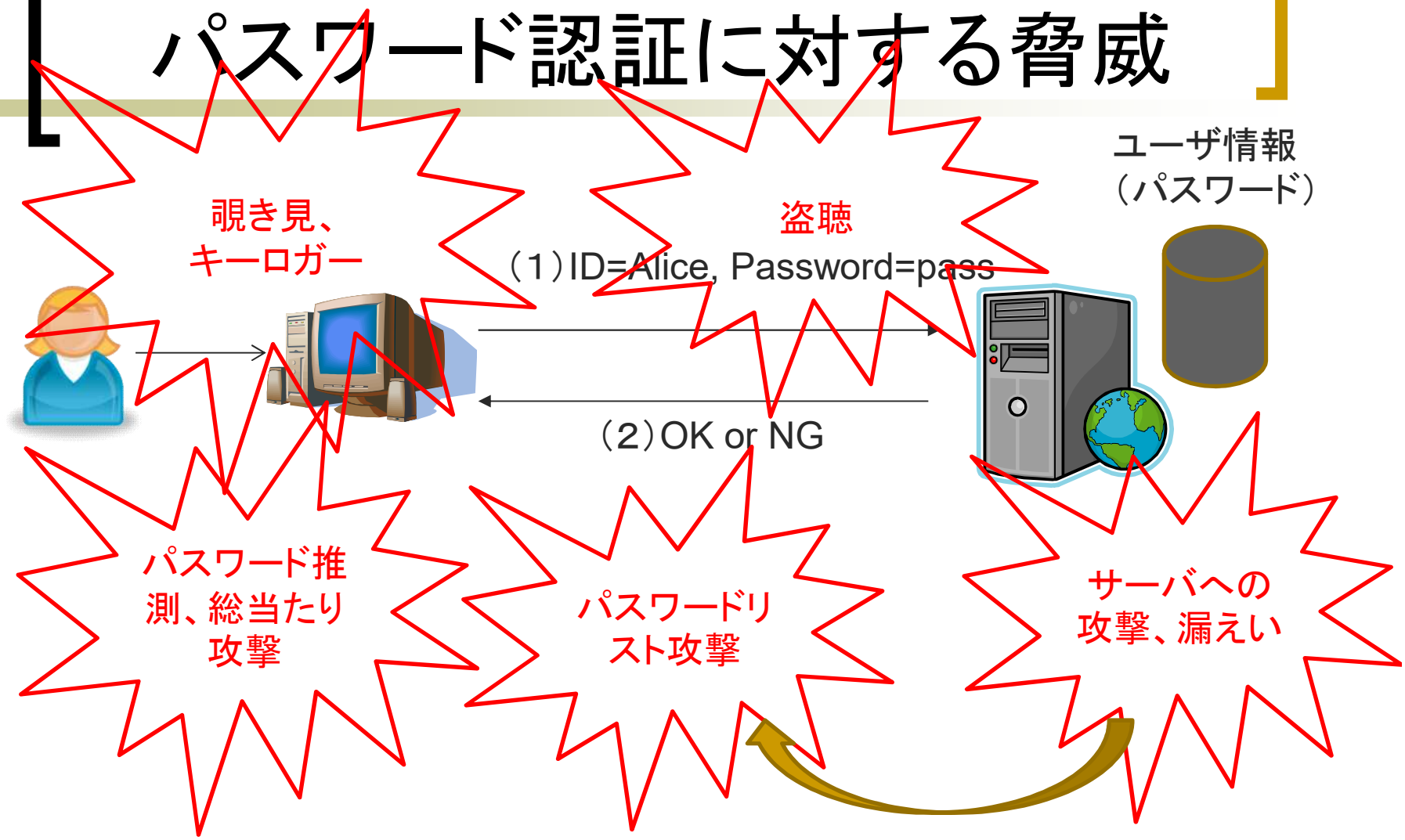


- IDの「認証」を行うだけであって、サービスの「認可」とは別
- OpenIDが使えることとRPが信頼できるかどうかは関係ない

Shibboleth（シボレス）による シングルサインオンと大学間連携



パスワード認証に対する脅威



パスワード認証は広く用いられているが、様々な脅威(本人が忘れることも含め)が存在する

安全なパスワードとは？

パスワードの安全性は、そのエントロピー*E*で見積もることができる

$$E = l \times \log_2 M \,(\text{bit})$$

*M*はパスワードに使用する文字種類数、*l*はパスワード長

パスワード推定や総当たり攻撃に対処するためには、
パスワードのエントロピーを高くすることが大事。

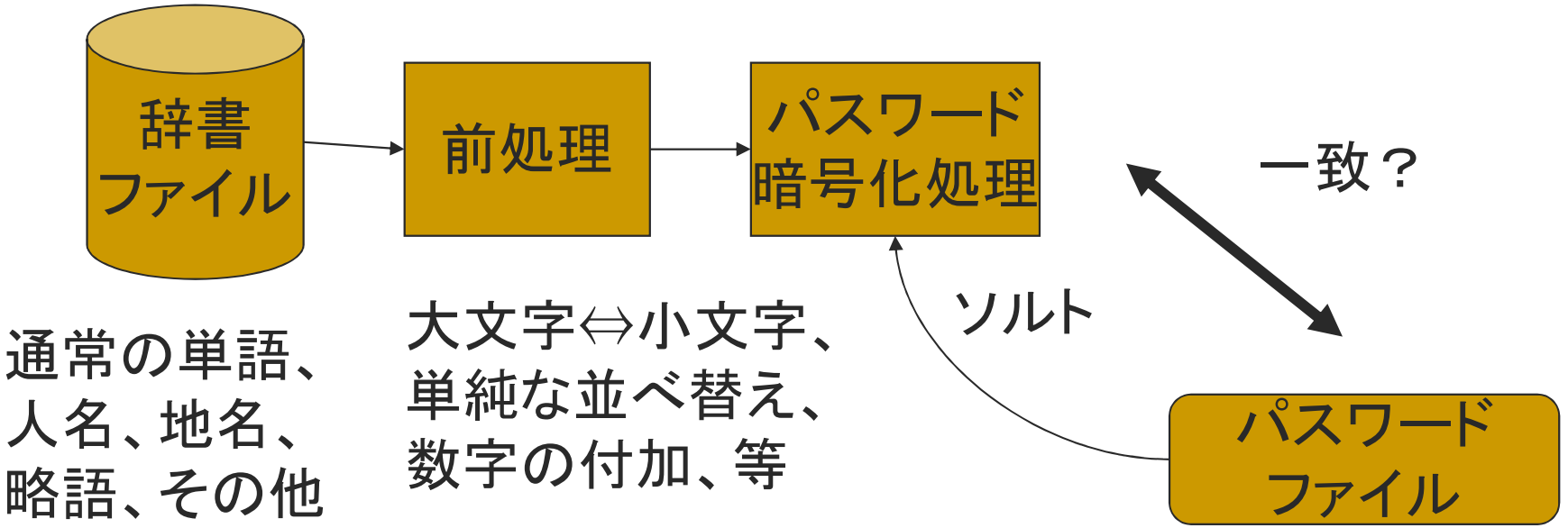
文字種類	*M*	*l*	*E(bit)*
数字のみ	10	4	13
アルファベット (小文字のみ)	26	8	38
アルファベット＋数字	62	8	48
アルファベット＋数字＋記号	96	10	66
アルファベット＋数字＋記号	96	15	99
英語の単語			20

重要なサービスでは、80ビット程度以上のエントロピーが望ましい。

ビットサイズと全数探索

事項	個数	文字数 (6bit/1文字)	ビット数	探索時間 (10^{-13}秒/1件)
地球の人口	60億	6	32	60msec
DES	7京(7×10^{16})	9	56	1.9時間
水(180cc) 分子の数	6×10^{24}	14	82	19000年
AES-128	3.4×10^{38}	21	128	100万　兆年
AES-256	1.2×10^{77}	43	256	
宇宙の 基本粒子数	10^{80}	44	265	

パスワードクラック



- **（注）英単語（60万語程度<20bit）全て対象としても計算機には楽勝**
  長さには関係なし（supercalifragilisticexpialidocious）

パスワード認証の脅威への対策

- サーバへの攻撃等によるパスワードの漏えいに対して
  サービスごとに異なるパスワードを付けること
  2段階認証も有効
- キーボードロガー等によるパスワード盗難に対して
  アンチウイルス、アンチスパイウェアソフトが有効
  安易に信頼性の定かでないソフトをインストールしない
- パスワードの盗聴に対して
  SSHやHTTPS等のセキュアプロトコルを利用
- パスワード忘れに対して
  信頼性のあるパスワード管理ツールの利用