MEIJI UNIVERSITY

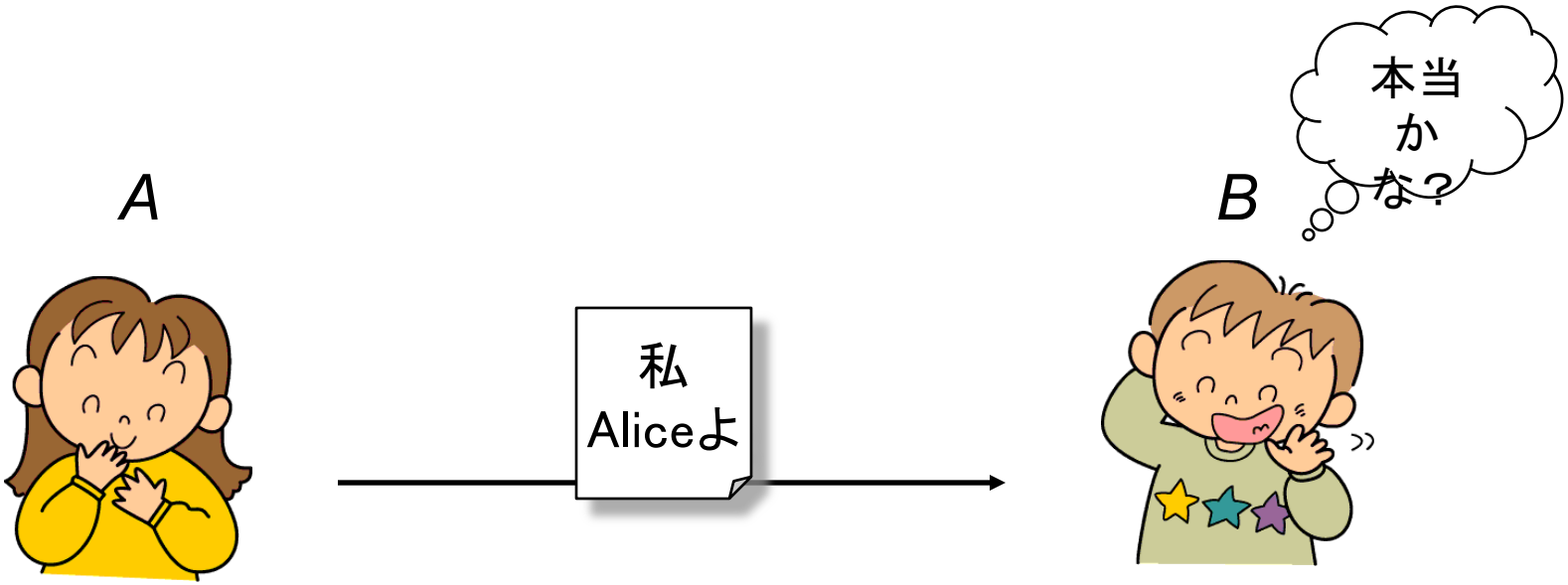
認証技術

ネットワークと情報セキュリティ7

菊池浩明

問題 「認証」

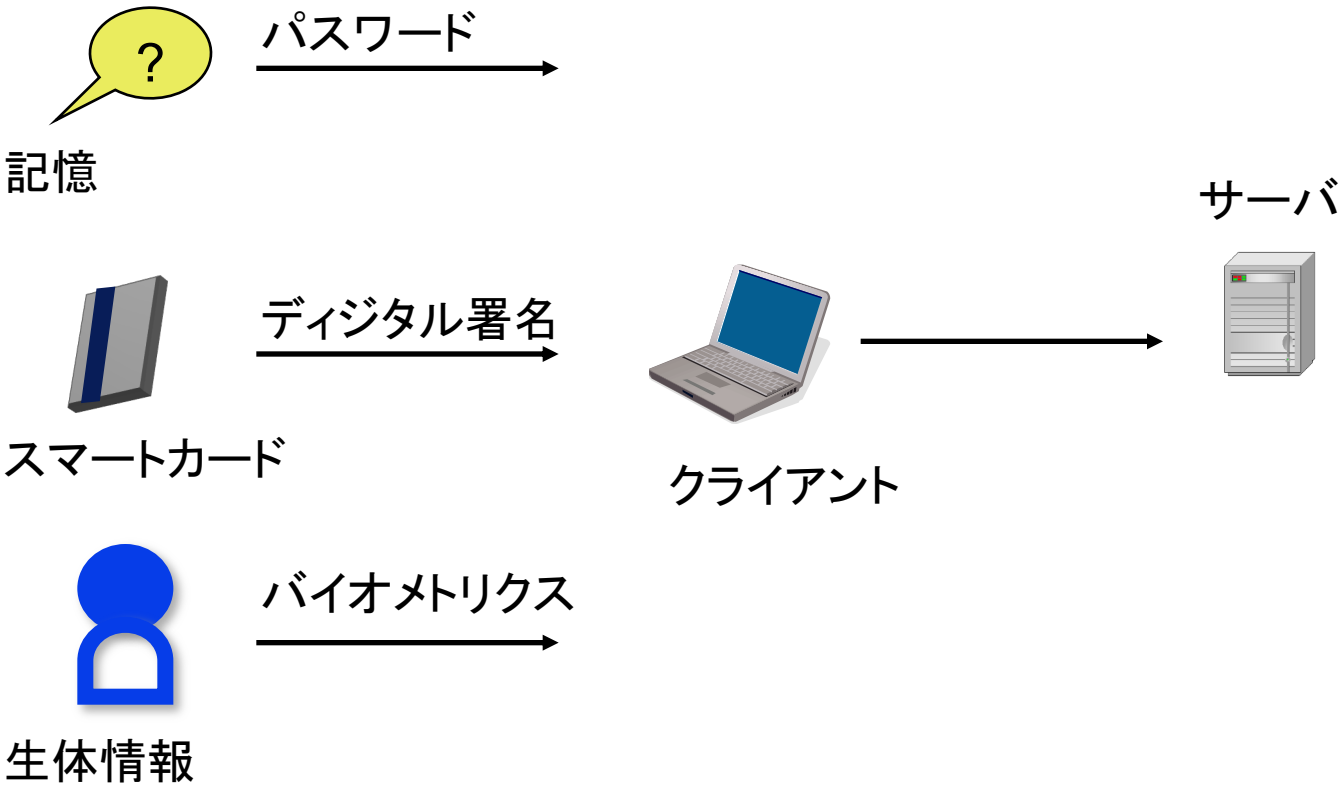
- 本物であることの証明



ユーザ認証の方法

- *What you know*
  - 暗証番号, パスワード
- *What you have*
  - トークン(Token), Key, Smart Card
- *What you are*
  - 虹彩，声紋，指紋，筆跡

ユーザ認証と本人認証


?
パスワード
記憶
サーバ
ディジタル署名
スマートカード
クライアント
バイオメトリクス
生体情報
本人認証
認証プロトコル

本人認証の課題

認証手段	安全性	認証手段 所持	登録情報 の修正
パスワード			
耐タンパー デバイス			
バイオメトリクス			

脅威1:　盗聴

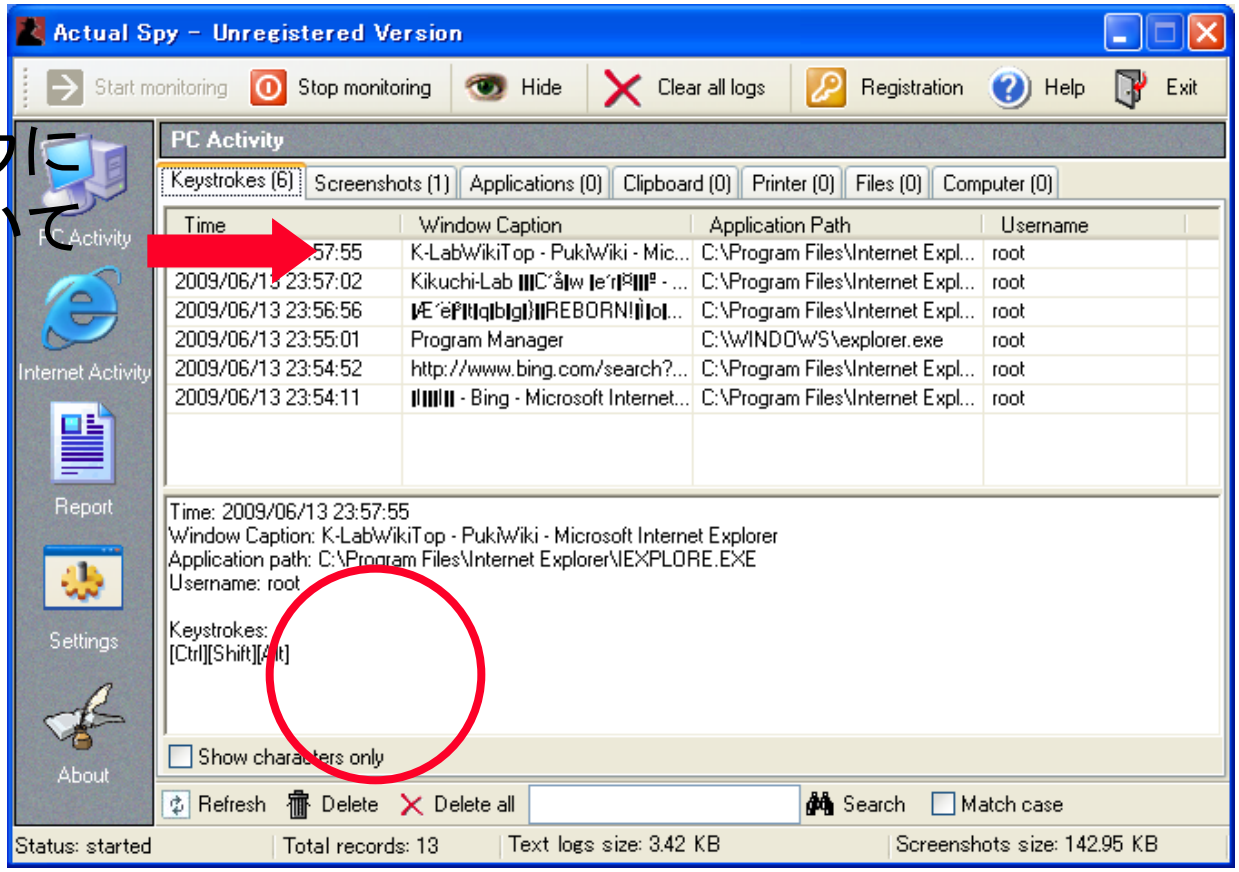
- オンライン攻撃
  - ネットワークのパケットを盗聴する
  - WireShark (パケットキャプチャーソフト)

password

ID	パスワード
ハリー	Rabiosa
ロン	open123

脅威2: Keyloger

全ウィンドウについて



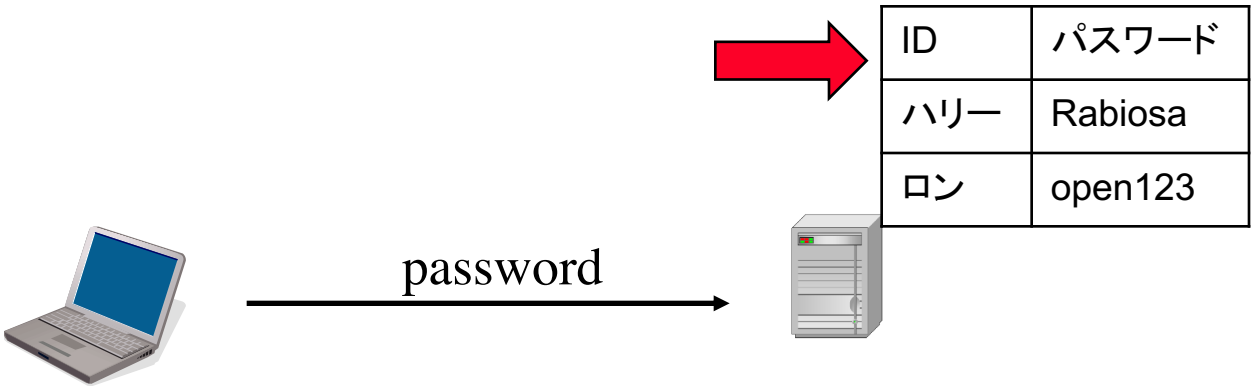
全てのストロークが記録

脅威3: ソーシャルエンジニアリング

- プライベート情報からの推測
  - Griffith and Jakobsson
    - » Public record to infer individual's mothers' maiden names
- 詐欺
  - 「営業2課の菊池だけど，今顧客先で，至急私のパスワードを初期化してくれないか？」
- ショルダーハッキング
  - 覗き込み盗聴

脅威4： 内部犯

- オンライン攻撃
  - ネットワークを流れるオンラインのパケットを盗聴する
- オフライン攻撃
  - サーバに格納されているファイルをオフラインで解析する



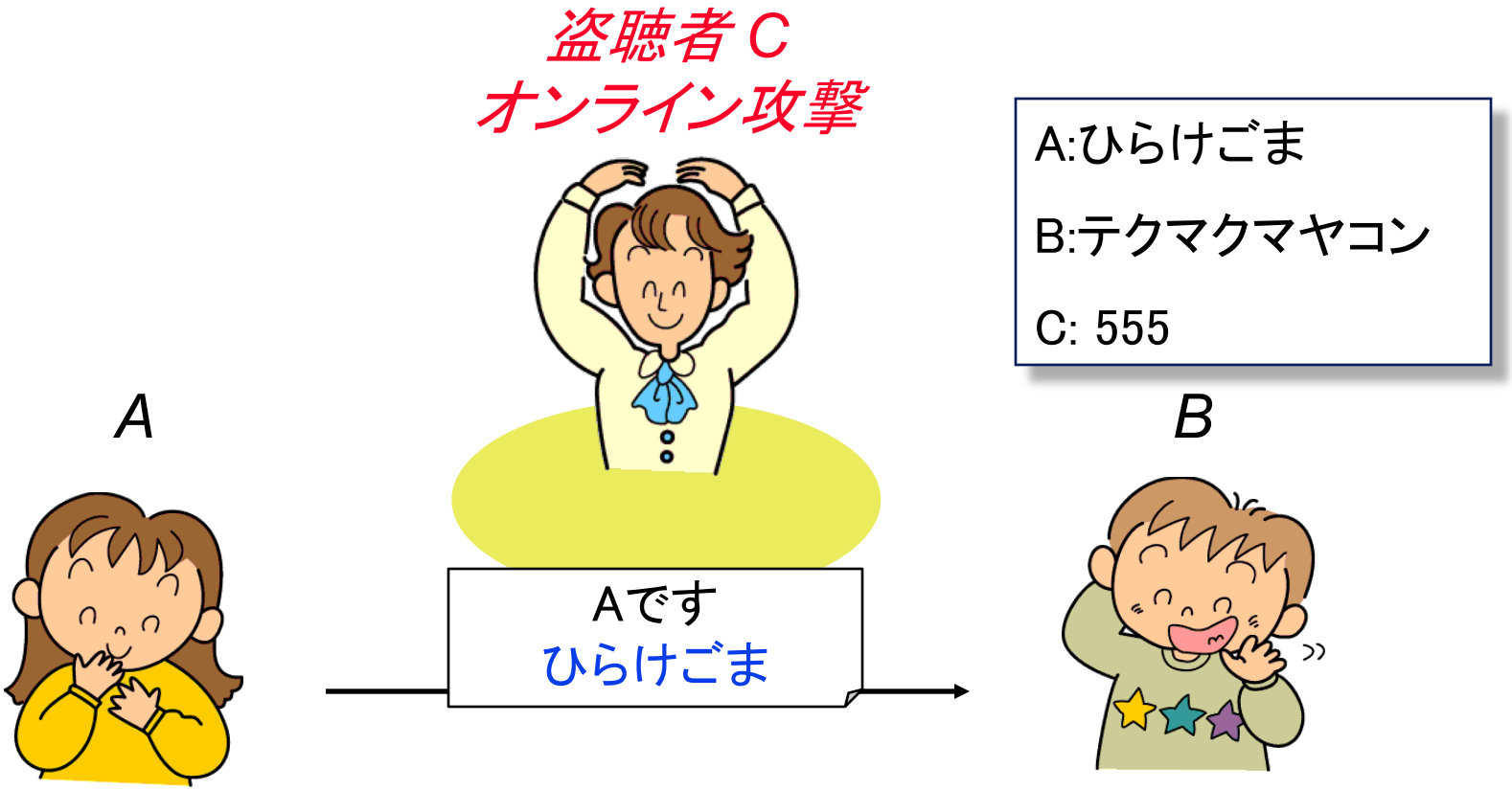
認証プロトコル

認証プロトコル

- ユーザ認証技術
  1. パスワード
  2. ワンタイムパスワード
  3. チャレンジレスポンス
  4. 鍵管理プロトコル, チケット
  5. Open ID

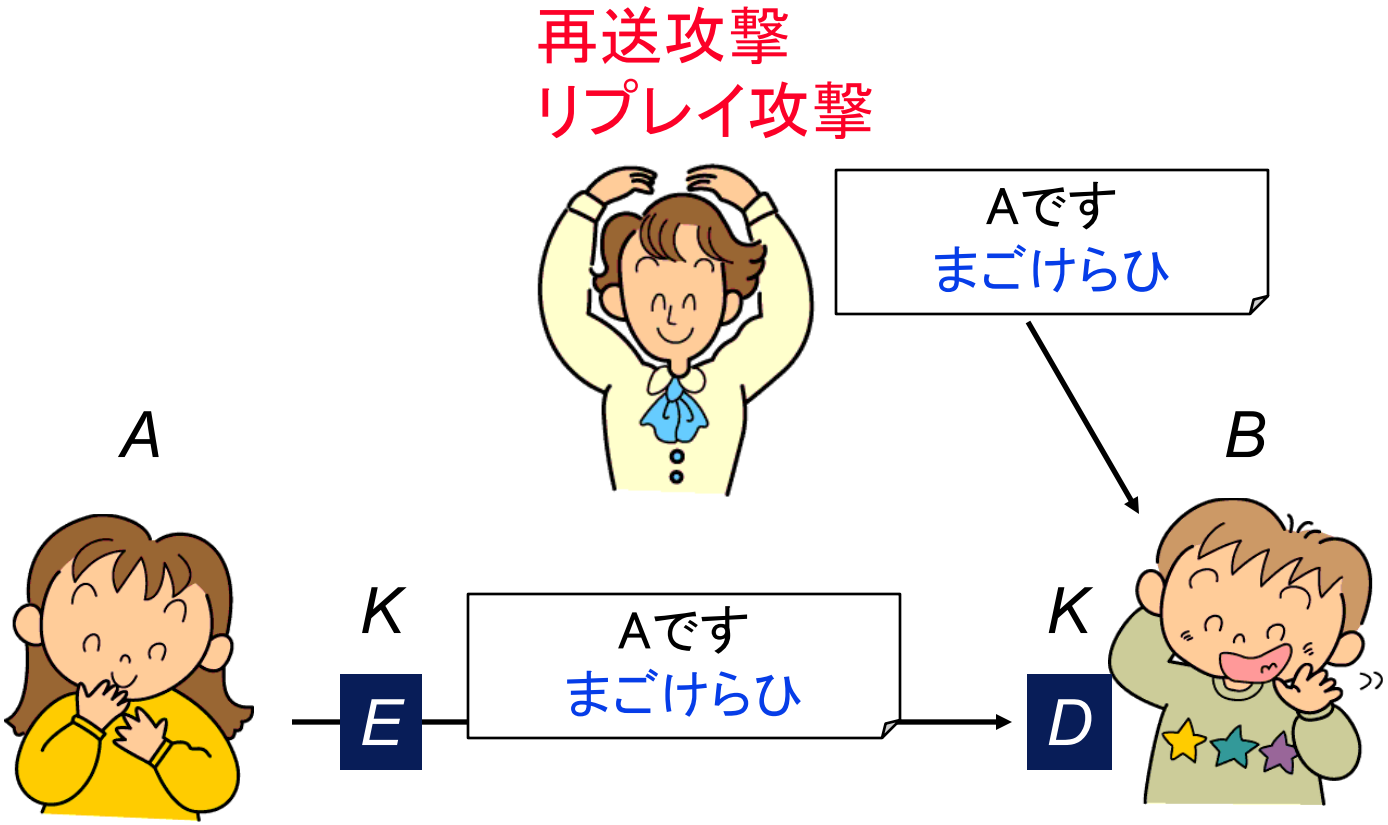
1. パスワード認証

- PIN



暗号化

- パスワードの暗号化



オンライン攻撃への対策

- 使い捨てパスワード (One-Time Password)
  1. Token Based
  2. Hash Chain Based
- Challenge-Response プロトコル

使い捨てパスワード

- RSA Secure ID

t_1

$x_1 = H(t_1 \| ID)$

t_1

$x_1 = H(t_1 \| ID)$

ID, x_1

2. 使い捨てパスワード（登録）

A　　*one-time password*　　*B*

秘密 *k*

$x_1 = h(k)$

$x_2 = h(x_1)$

$x_3 = h(x_2)$

$x_4 = h(x_3)$　　登録 x_4 ⟶　　A: x_4

h; 一方向性ハッシュ関数

2. 使い捨てパスワード （認証）

A　　B

秘密　k

$x_1 = h(k)$　　A, x_1 →　x_1

$x_2 = h(x_1)$　　A, x_2 →　x_2　　=? $x_2' = h(x_1)$

$x_3 = h(x_2)$　　A, x_3 →　x_3　　=? $x_3' = h(x_2)$

$x_4 = h(x_3)$　　登録 x_4 →　A: x_4 =? $x_4' = h(x_3)$

登録と比較

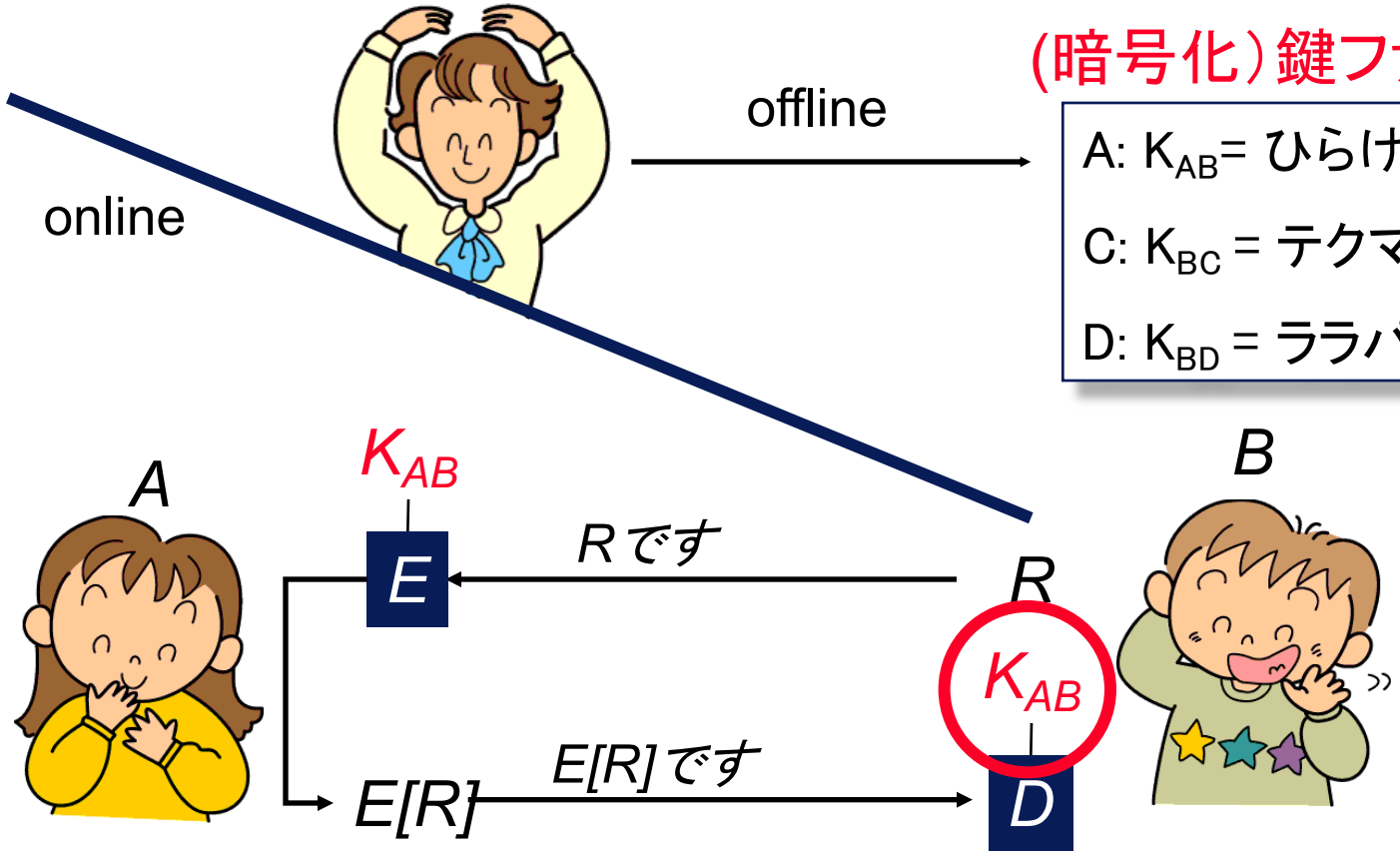
内部犯対策

- 「塩」
  - サーバに格納する秘密情報を撹乱する乱数
  - パスワードが同じでも格納情報xは異なる

x_1 = H(塩1, パスワード)
x_2 = H(塩2, パスワード)

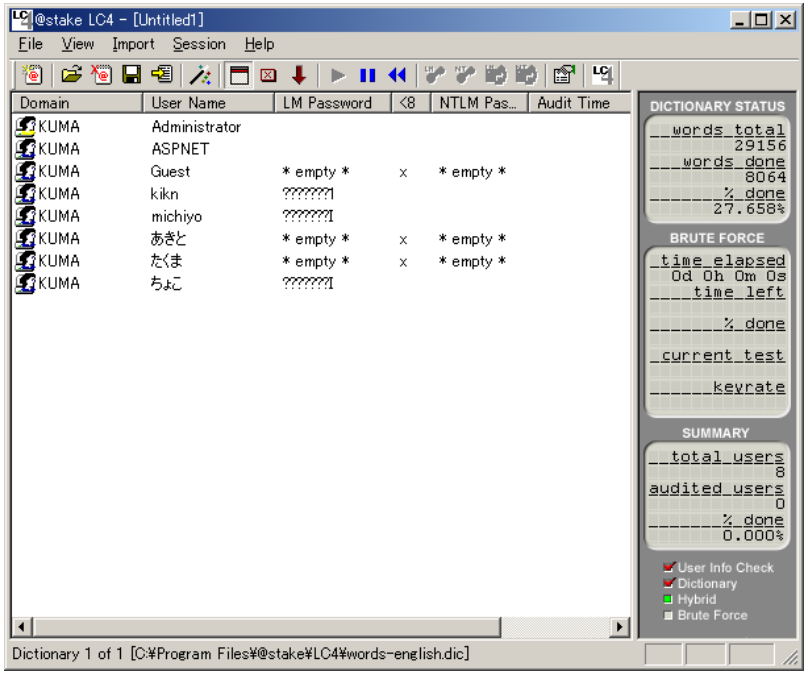
問題点2. オフライン攻撃

- 共通鍵（パスワード）データベースの解析



パスワードクラック

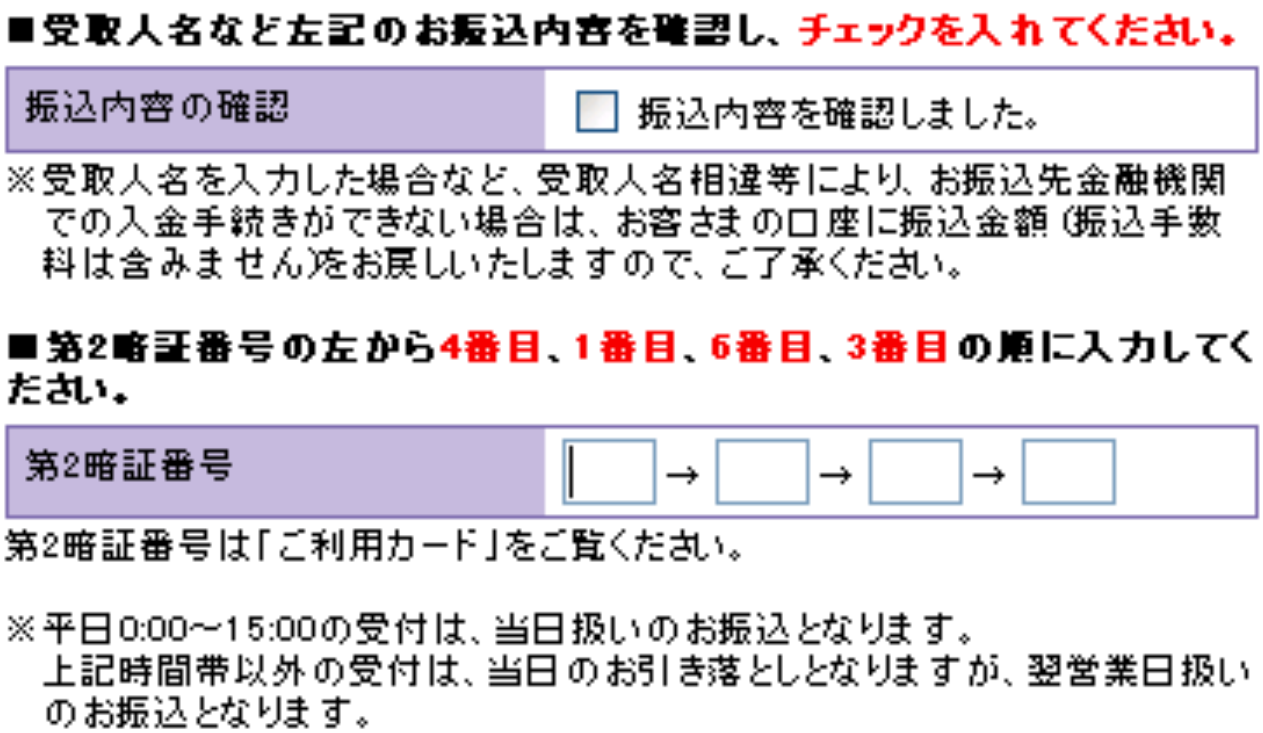
- LC4 @stake
  - LOptCrack
  - Windows NT/2000/XP 解析
  - /Winnt/System32/Config/SAM（パスワード）
  - 辞書攻撃（23万語）
  - ハイブリッド（数字の組み合わせ）
  - 総当り攻撃
  - Sniffer (ネットワーク上のデータについて解析）



http://www.atstake.com/products/lc/

Keylogger 対策

- 第2暗証番号



■受取人名など左記のお振込内容を確認し、チェックを入れてください。

振込内容の確認	☐ 振込内容を確認しました。

※受取人名を入力した場合など、受取人名相違等により、お振込先金融機関での入金手続きができない場合は、お客さまの口座に振込金額（振込手数料は含みません）をお戻しいたしますので、ご了承ください。

■第2暗証番号の左から4番目、1番目、6番目、3番目の順に入力してください。

第2暗証番号	□ → □ → □ → □

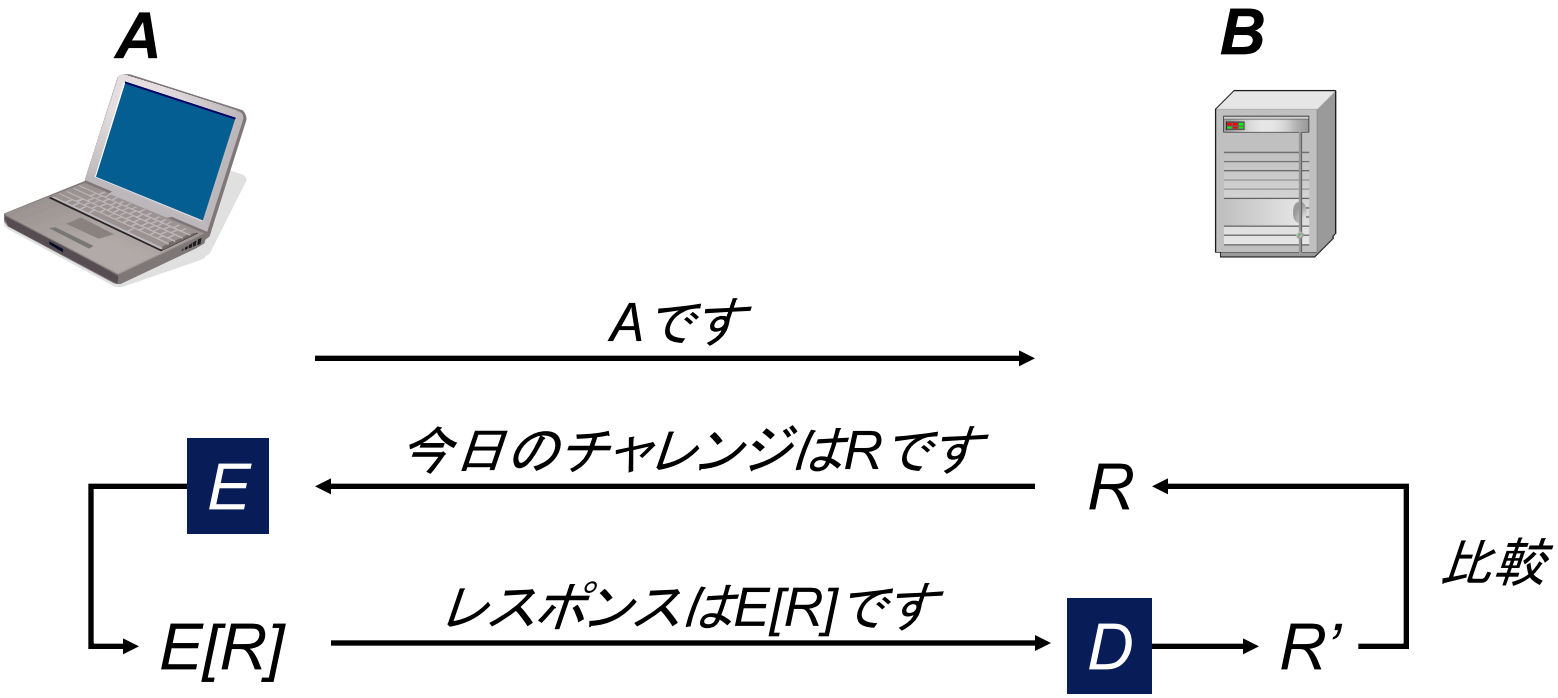
第2暗証番号は「ご利用カード」をご覧ください。

※平日0:00～15:00の受付は、当日扱いのお振込となります。
上記時間帯以外の受付は、当日のお引き落としとなりますが、翌営業日扱いのお振込となります。

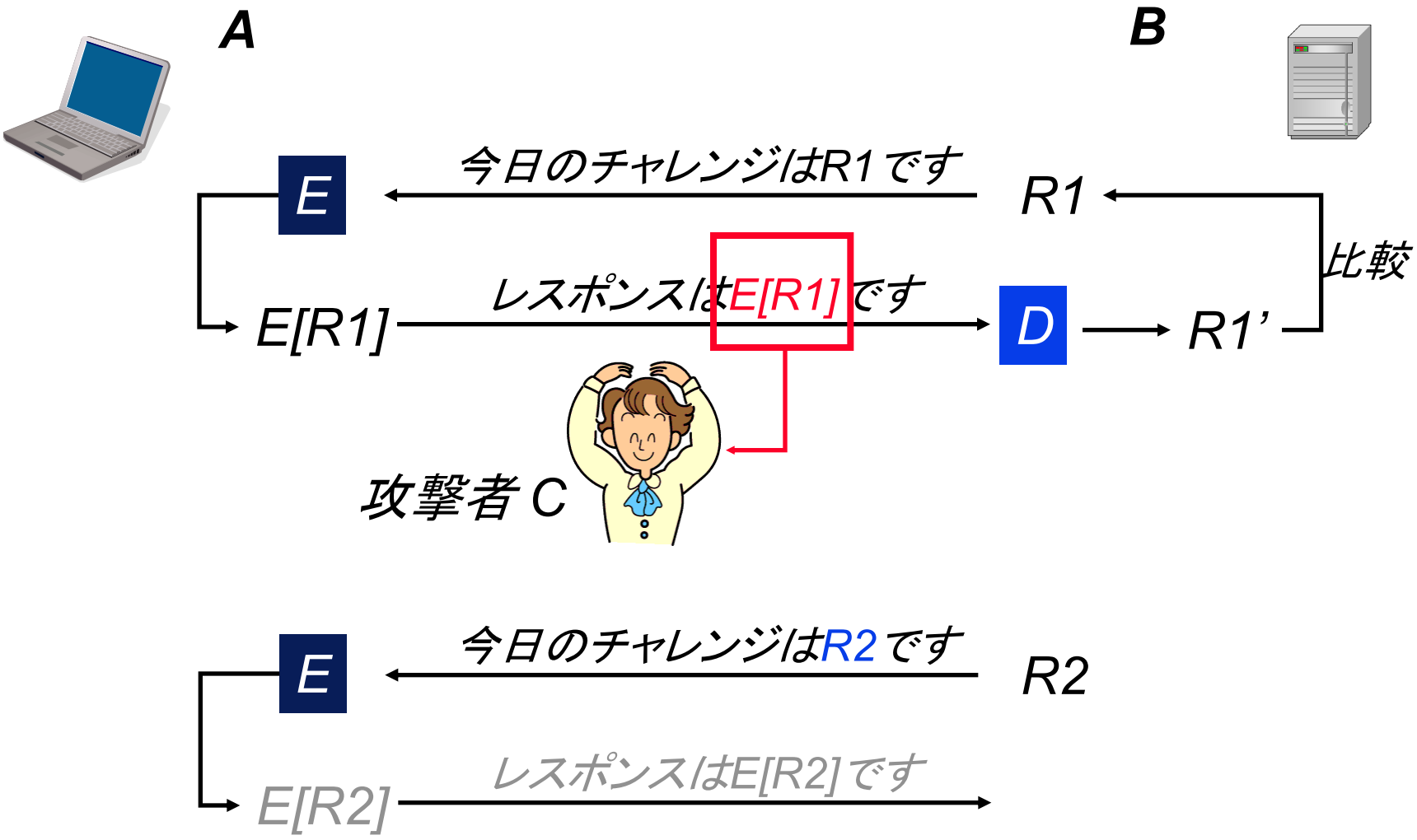
認証の課題

- 盗聴
- 再送攻撃
- 内部犯
- スケーラビリティ

3. チャレンジアンドレスポンス

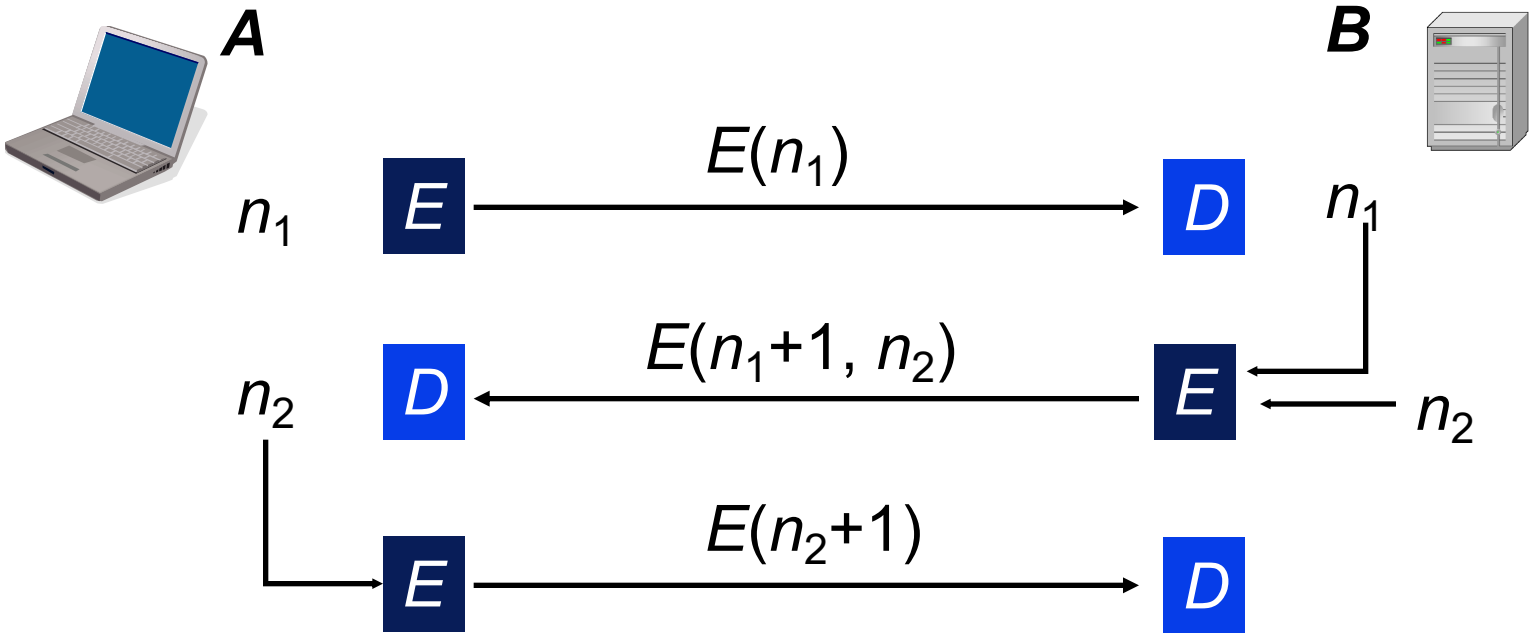


再送攻撃への耐性


A
B
E
今日のチャレンジはR1です
R1
比較
E[R1]
レスポンスはE[R1]です
D
R1’
攻撃者 C
E
今日のチャレンジはR2です
R2
E[R2]
レスポンスはE[R2]です

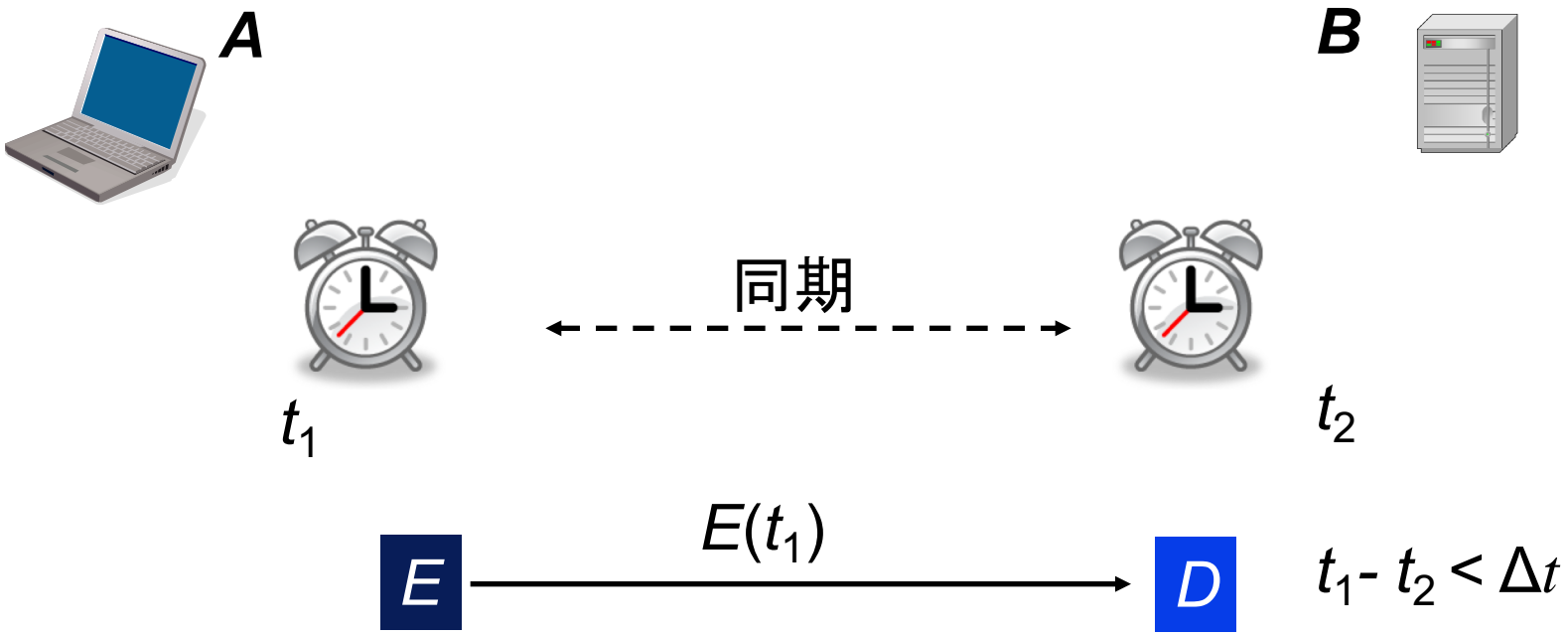
(1) “nonce” ナンス 一度きりの乱数

- **n**umber used **once**
  - 相手が再送していないことを保証する「フレッシュ」な乱数 n_1



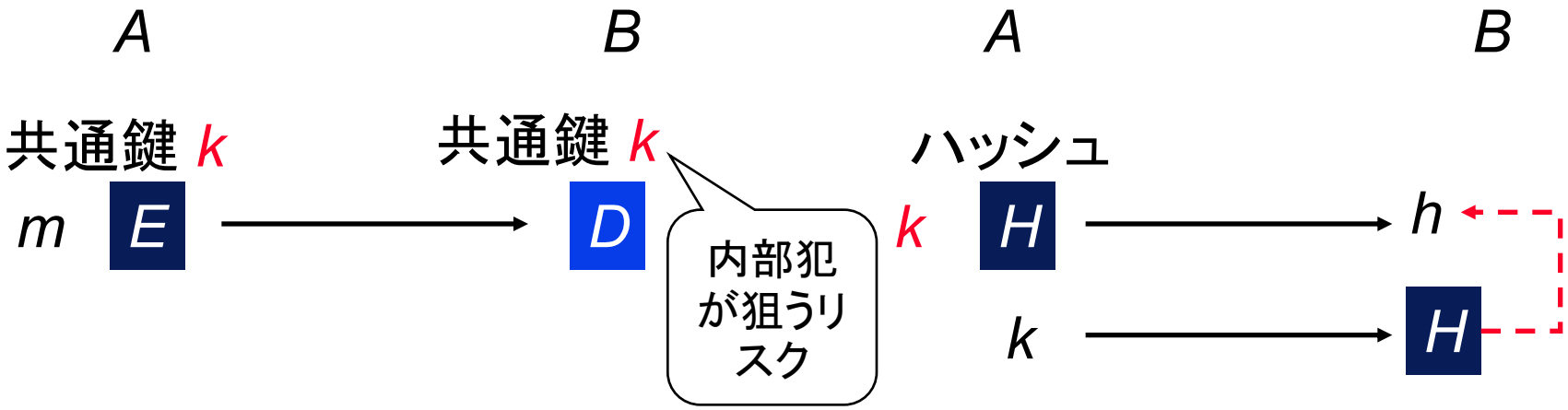
(2) “time stamp” 時刻の信頼

- time stamp （時刻印) t_1



CHAPとOTPどちらが安全か?

- CHAP（チャレンジレスポンス）
- OTP (一方向性パスワード)

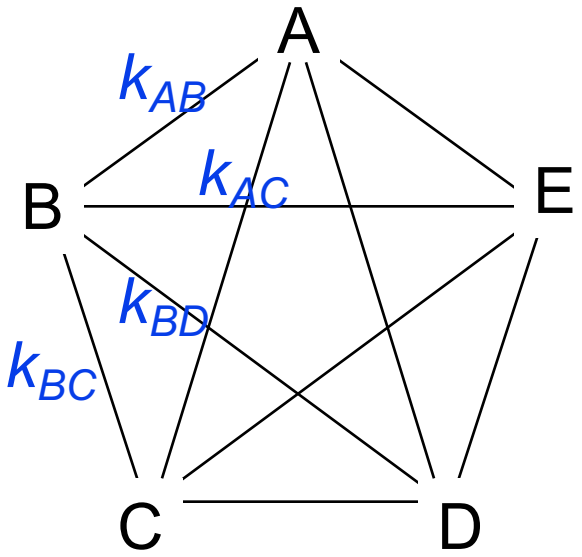


- shared secret（秘密共有型認証）

問題点1. スケーラビリティ

- スケーラビリティ
  - scalable
    - (a) 拡大縮小が可能な，システムが拡張可能な，拡張性のある
  - ユーザ数の増加に対してサービス提供側のコストが小さいこと

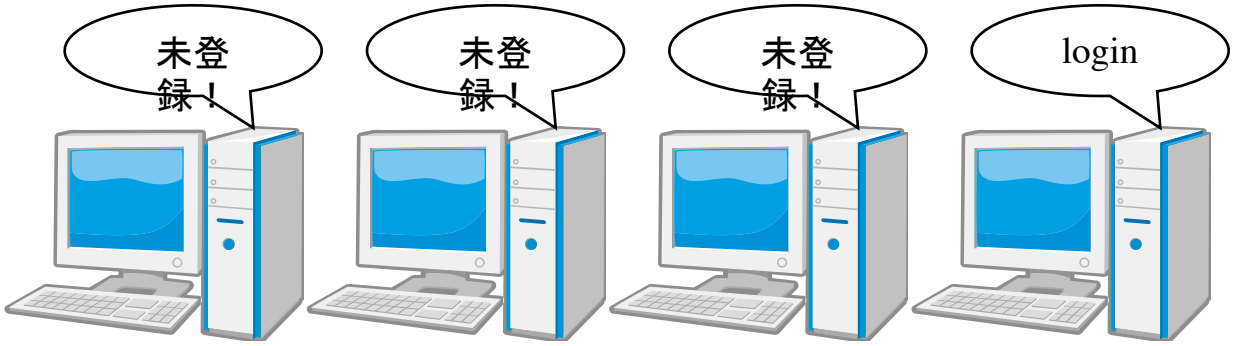
- 共通鍵の総数



$$\binom{n}{2} = \frac{n(n-1)}{2}$$

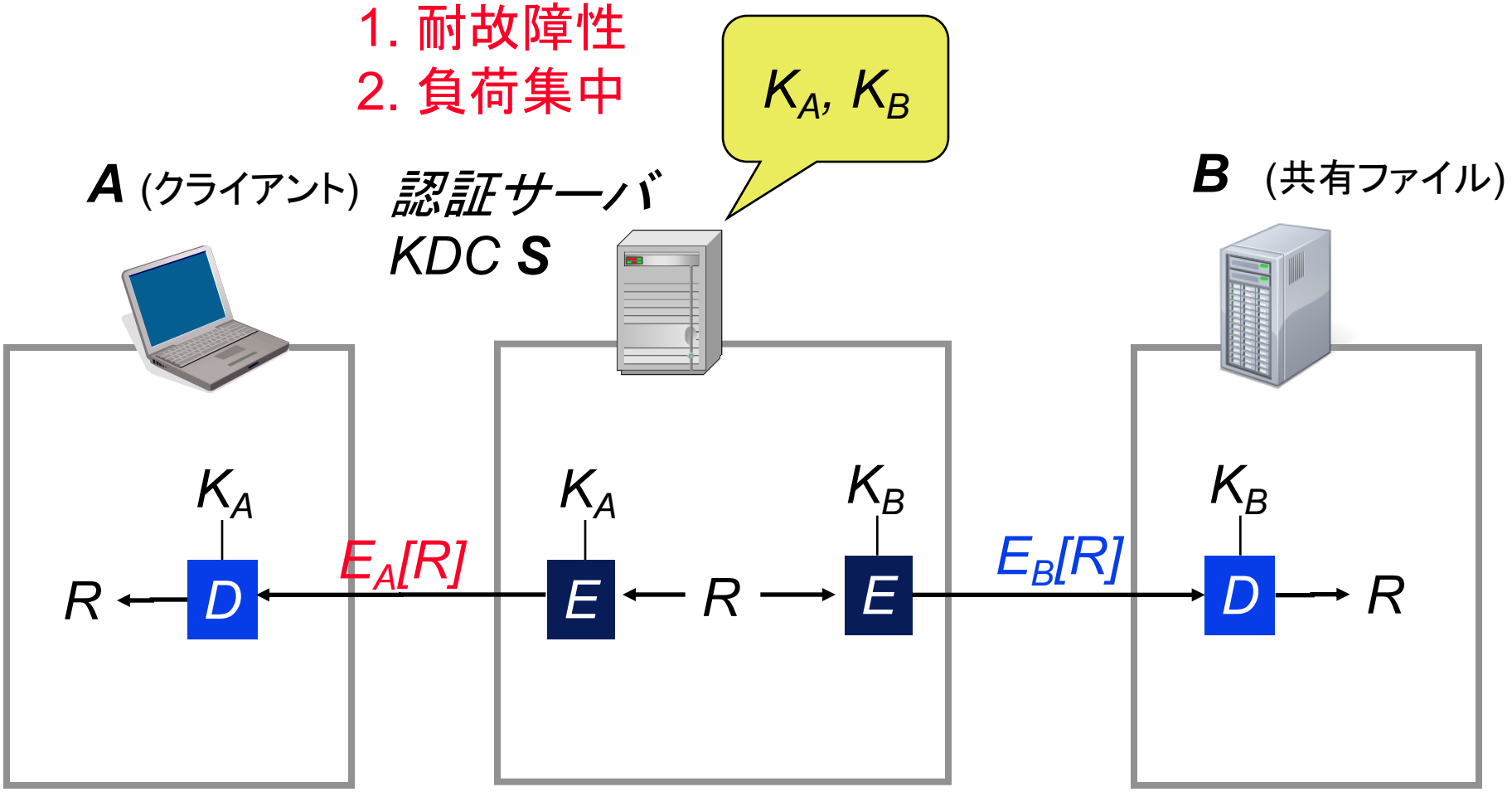
一元的なユーザ登録の必要性

- 例）キャンパスネットワーク

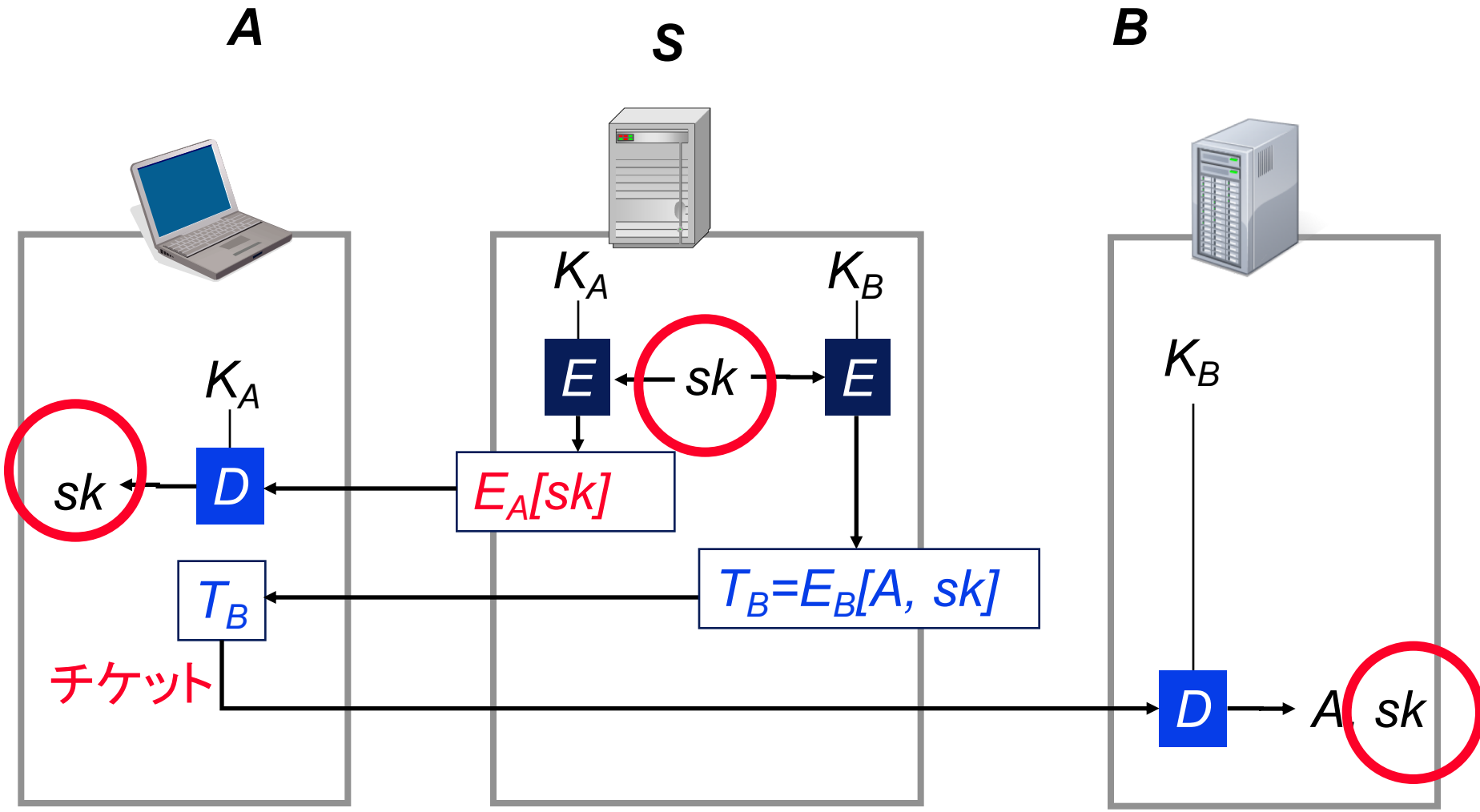


4. 第三者認証の原理

問題点
1. 耐故障性
2. 負荷集中



第三者認証「チケット」



Needham - Schroeder

- プロトコル

  A→S: N_1 ナンス

  S→A: $E_A(N_1, B, sk, T_B=E_B(sk, A))$

  A→B: $T_B=E_B(sk, A)$ チケット(ticket), $E_{sk}(N_2)$

  B→A: $E_{sk}(N_2-1, N_3)$

  A→B: $E_{sk}(N_3-1)$

  - チケット $T_B=E_B(sk, A)$ (Bしか復号できない)
  - セッション鍵 sk (一度きりの秘密情報)

Windows Domain認証

- MIT Kerberos 認証システム
- Active Directory
  - Windows 2000以降
  - Key Distribution Center (KDC)
  - クロスレルム（領域）認証

M12.1 HERAKLES, KERBEROS

http://www.perseus.tufts.edu/Herakles/cerberus.html

5. Open IDの原理

Client A

RP (Replying Party)
OpenID利用サイト

Aは未登録

OP (OpenID Provider)
OpenID登録サイト

A登録済み

OPのAです →

Aを知っている？ →

← Aの身元を保証します

← 会員サービスをどうぞ

Open ID

Client **A**

RP (Replying Party)
OpenID利用サイト

OP (OpenID Provider)
OpenID登録サイト

login: OPのA

A, M

コンテンツMの
ハッシュを計算

リダイレクト
http 302 “moved temporarily”

http://OP&RP&A

password

Aの認証

RPへ繋ぐ確認

承認

リダイレクト

コンテンツ M

演習： 認証プロトコルと性能

プロトコル	盗聴耐性	再送攻撃耐性	オフライン攻撃耐性	スケーラビリティ
パスワード	×	×	×	×
ワンタイムパスワード(ハッシュ関数)				
チャレンジレスポンス (nonce)				
チケット (KDC)				
OpenID				

まとめ

- ユーザ認証には，パスワードなどの（　　）によるもの，（　　）などのデバイスによるもの，虹彩などの（　　）がある．
- 単純なパスワードの暗号化は（　　）攻撃に弱い．
- 再送攻撃に対して一度きりの乱数（　　）が効果的である．
- （　　）は，内部犯やオフライン攻撃に対して頑強である．
- 大規模な環境でもスケーラビリティのある認証方式は（　　）である．