情報セキュリティ技術: 個人識別

情報社会とセキュリティ
2024 年度前期
佐賀大学理工学部 只木進一

個人識別: Personal Identification

- 認証: authentication
  - 本人であることを確かめる
  - authenticate: to prove that something is genuine, real, or true.
- 認可: authorization
  - 権限があることを確かめ、許可する
  - authorize: to give official permission to something, or for somebody to do something.

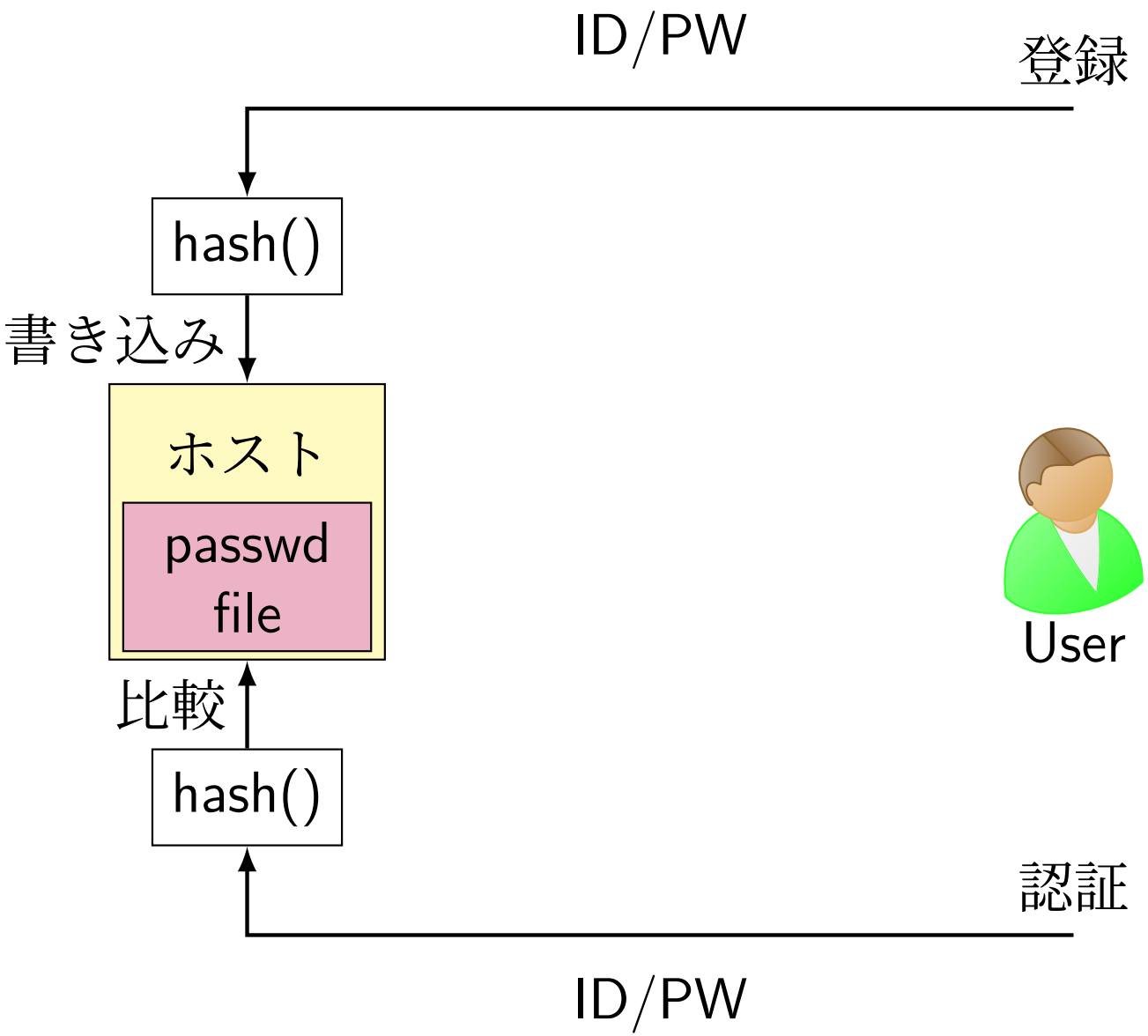
認証の要素

- 本人の記憶
  - パスワード、秘密のワード
- 持ち物
  - IC カード、スマートフォン、乱数表
- 本人そのもの
  - 指紋、虹彩、静脈、顔

ローカル認証

- コンピュータ内にパスワードファイルを保持
  - ユーザが入力したパスワードを一方向暗号化 (hash 化) して保存
- 保存している暗号化済み文字列と比較
- hash 関数
  - データを一定の長さの文字列に変換
  - 異なるデータは、実効的に異なるハッシュ値に
  - MD5、SHA-1、SHA-256 などがある
- 暗号化していても、パスワードファイルを盗まれると、時間をかけて解析される

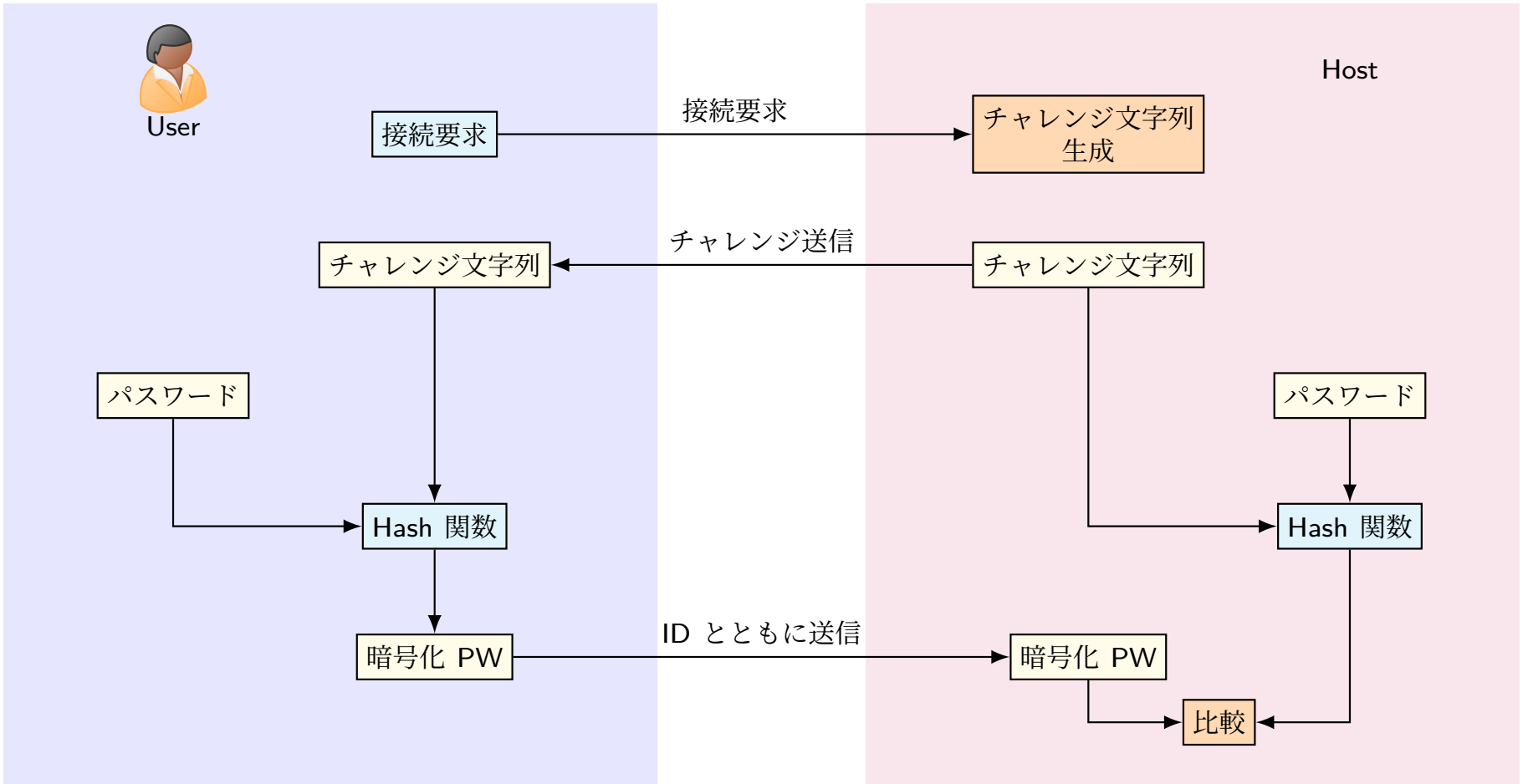
ローカル認証



リモート接続時の暗号化

- SSH (Secure Shell) を用いて、通信そのものを暗号化
  - 公開鍵暗号を利用した SSL/TLS
- ID とパスワードが通信回線を流れる際に、簡易な暗号化を行う
  - CHAP 認証: Challenge Handshake Authentication Protocol

CHAP 認証: Challenge-Handshake Authentication Protocol

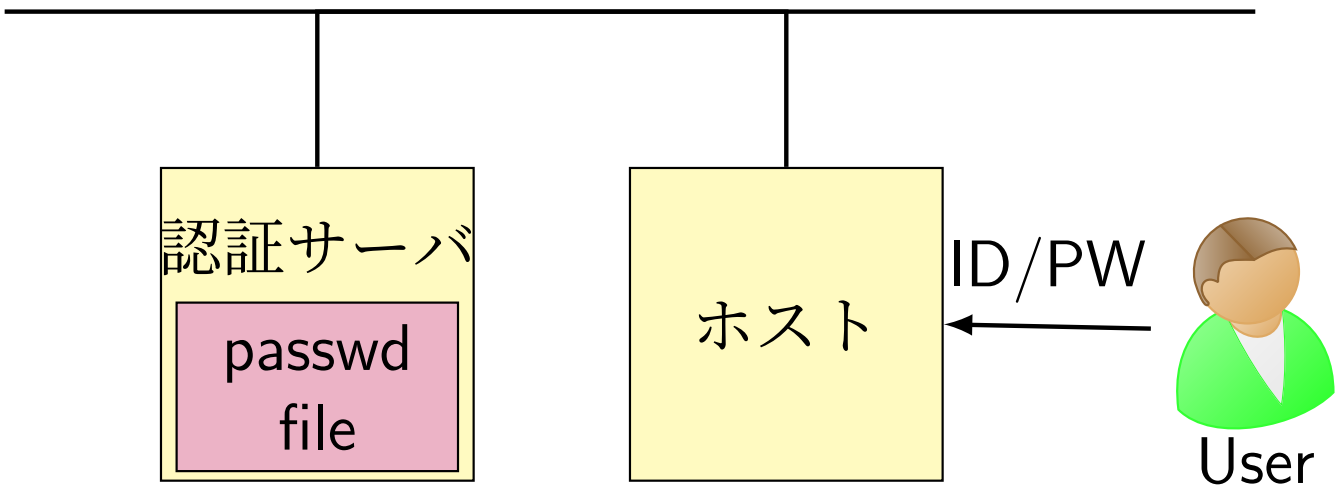


質問

ホスト側でパスワードを平文、つまり暗号化せずに保持しておいたほうが、比較は簡単にできます。パスワードを平文で保持している場合の危険性を考えましょう。

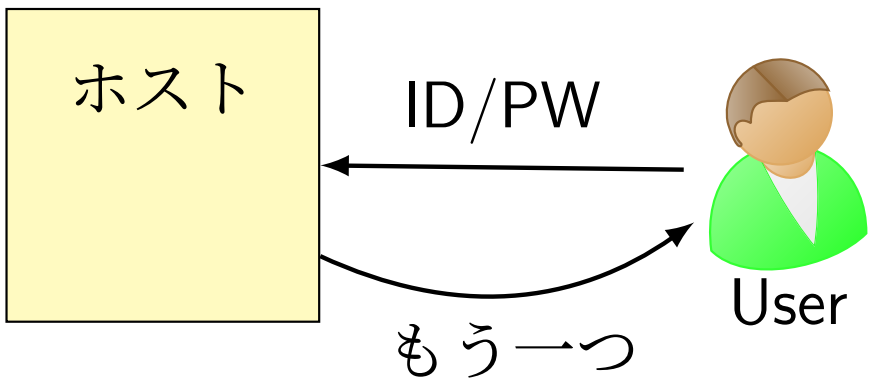
ネットワーク認証

- ネットワークで接続したコンピュータ群に共通の認証を提供
- LDAP (Lightweight Directory Access Protocol)
  - LDAP サーバに情報を集約
  - Windows では、AD (Active Directory) と呼ぶ
- 現在では、SSL/TLS を用いてサーバ・クライアント間の通信暗号化を実施



多要素認証: Multi-factor authentication

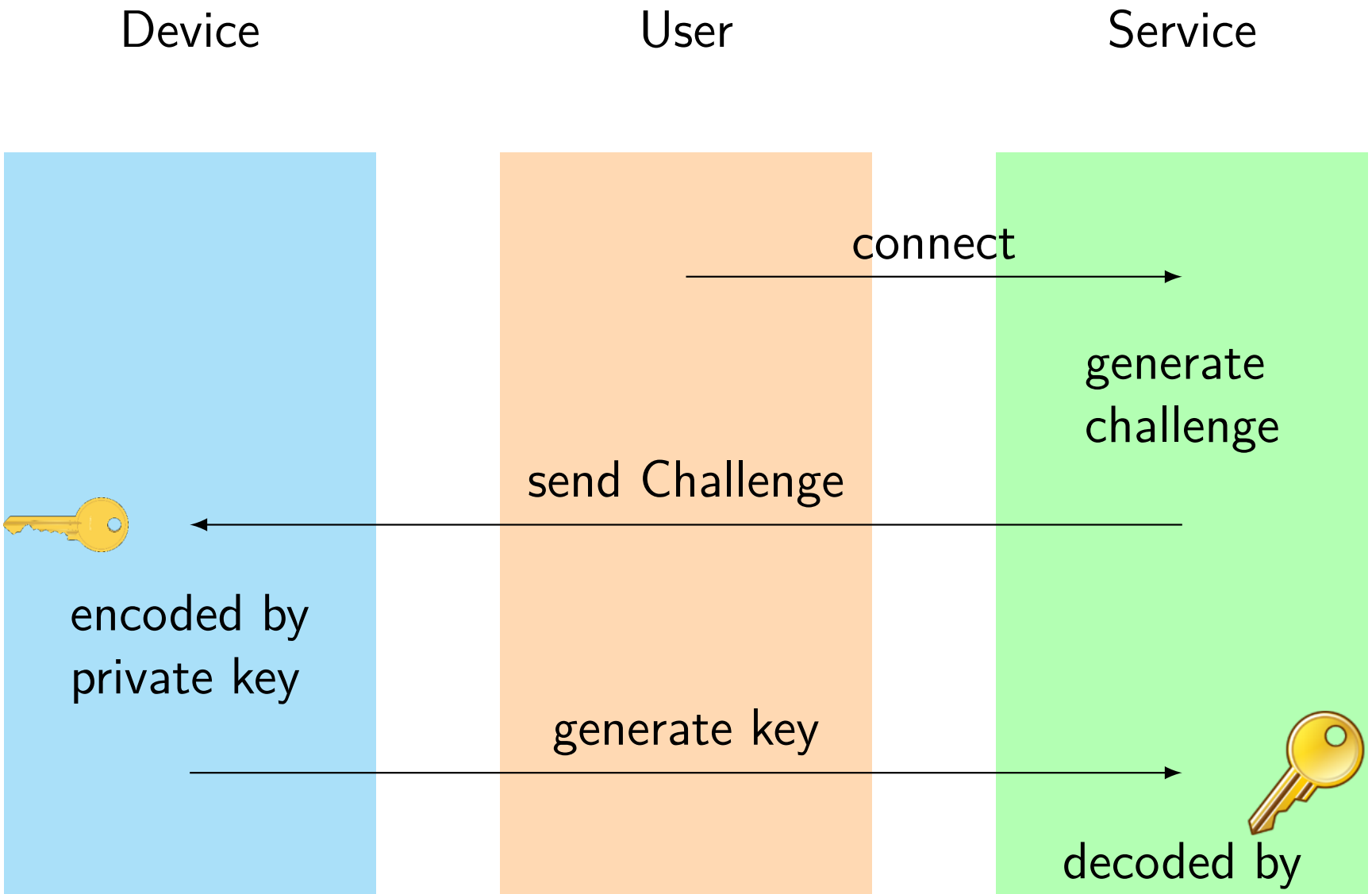
- 認証の要素を複数用いることで、認証強度を上げる
- 例: パスワード認証とともに
  - スマートフォンへショートメッセージとして、番号を送る
  - スマートフォンの認証アプリを用いて、確認する
- Microsoft365 で使用



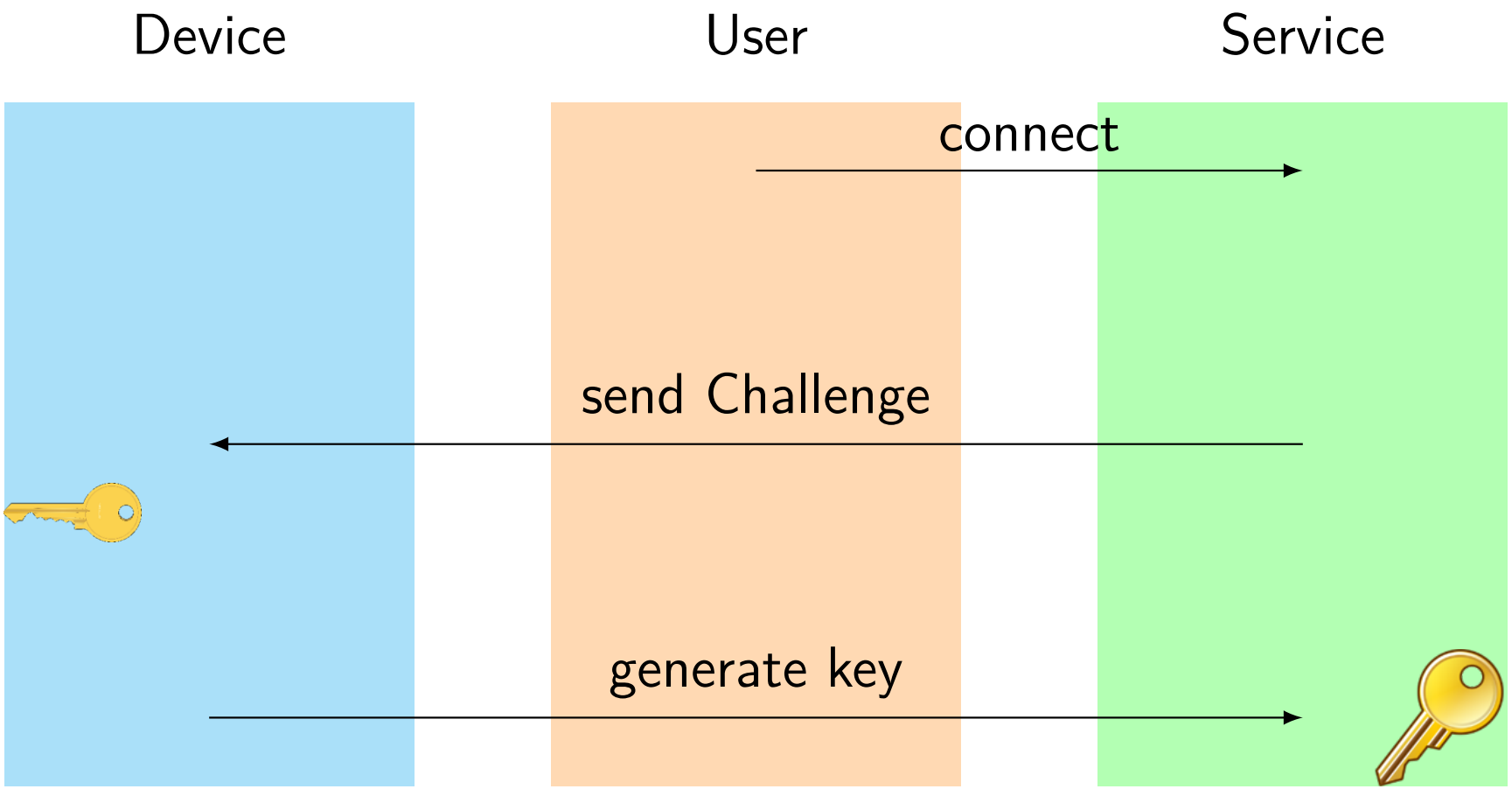
FIDO: Fast Identy Online

- パスワードを使わず、ユーザが持つ認証デバイスを使う方式
- 登録時
  - 認証デバイスで秘密鍵と公開鍵を生成
  - 公開鍵をオンラインサービスに登録
- ログイン時
  - サービスがチャレンジ文字列を認証デバイスに送信
  - 認証デバイスの秘密鍵でチャレンジ文字列に署名して返送
  - サービス側が公開鍵で復号できれば、認証成功
- 認証デバイスが課題

FIDO registration



FIDO login



質問

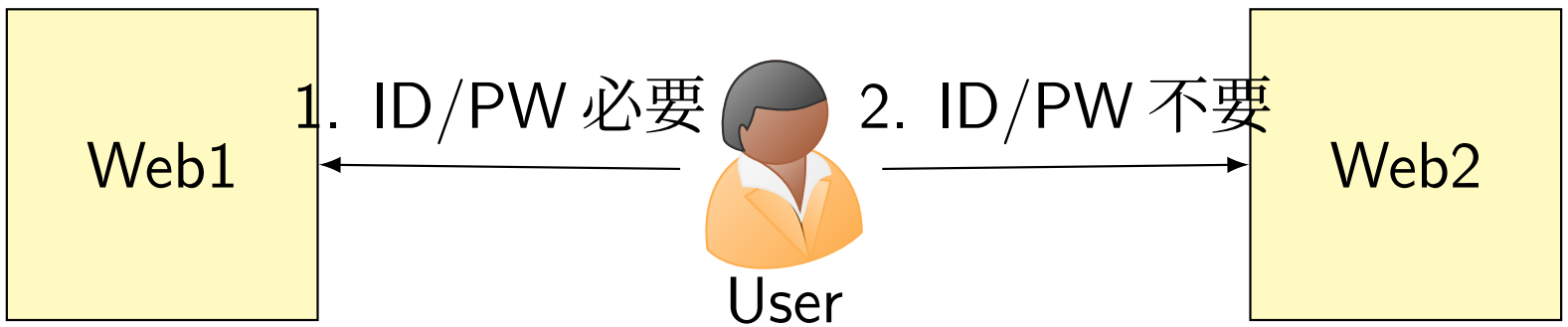
多数のシステムにログインする必要がある人を考えます。その人が必要とするシステム毎にログインを求めるとすると、その人はどんなパスワードを設定するでしょう？

Web 型情報システムの普及

- 情報システムの Web 化
- 組織内に多数の Web 型情報システム
- システム毎に認証すると
  - システム毎に異なる ID とパスワード
  - 利用者にとっては煩雑
  - 各システムの開発者は、認証の仕組みを実装
  - システム毎に ID とパスワードを管理
  - ID/パスワード漏洩リスク

SSO: Single Sign-On

- 複数の Web 型情報システムに、一度のログインでアクセスできる仕組み
- 一度認証に成功すると、他の情報システムでは再度の認証をしない



質問

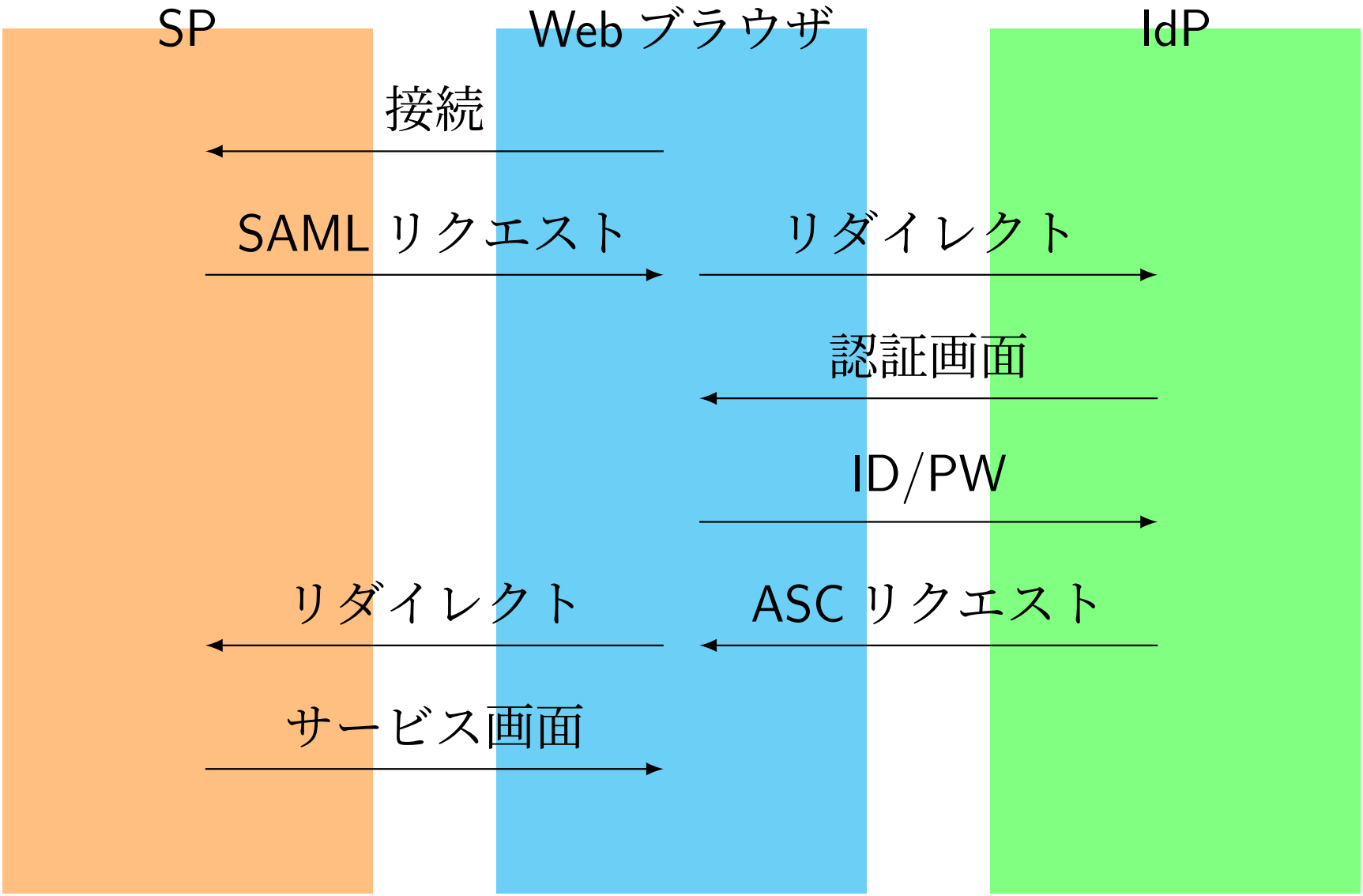
シングルサインオンは、利用者の利便性を向上させるだけではなく、セキュリティ強化にも役立ちます。どのような点でセキュリティ強化になるのでしょうか。

SSO の利点

- 各システムの開発者は、外部の認証システムを利用できる。
  - システム構築が容易となる。
- パスワード等の認証情報は、集中した認証サーバだけが保有
  - 各情報システムは、認証情報 (パスワード) を保有しない
  - 各情報システムには、メールアドレスや所属等の必要な情報だけを送信する。
  - セキュリティレベル向上
- 利用者は、複数のサービスを同一 ID、パスワードで利用できる。
  - 最初にログイン処理を行うと、他の情報システムへ入っても、認証を求められない。
  - ユーザ利便性向上

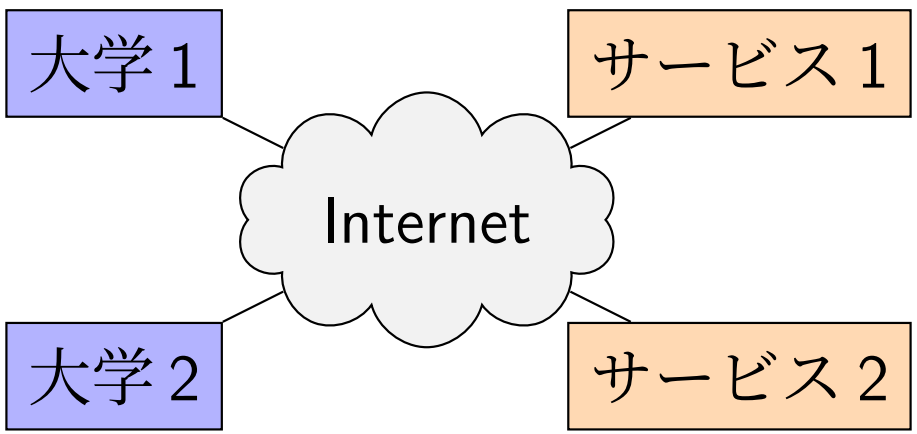
Shibboleth 認証

- サービス提供者:SP (Service Provider)
- 認証提供者:IdP (Identity Provider)
- SP に接続すると、認証要求を IdP に送信
- ユーザは、IdP で認証を受け、認証済み情報を SP へ送信
  - 重要: 認証情報は SP には渡らない
- SP と IdP が直接に情報交換しない
  - 認証済であることは、Web ブラウザが保持


SP
Web ブラウザ
IdP
接続
SAML リクエスト
リダイレクト
認証画面
ID/PW
リダイレクト
ASC リクエスト
サービス画面

認証連携

- SP と IdP が相互に信頼した組織を作る (federation)
- 「学認」: 大学等の IdP と、学術サービスの SP
- `https://www.gakunin.jp/`
- SP の例
  - 学術雑誌
  - オンライン教育
  - 学割



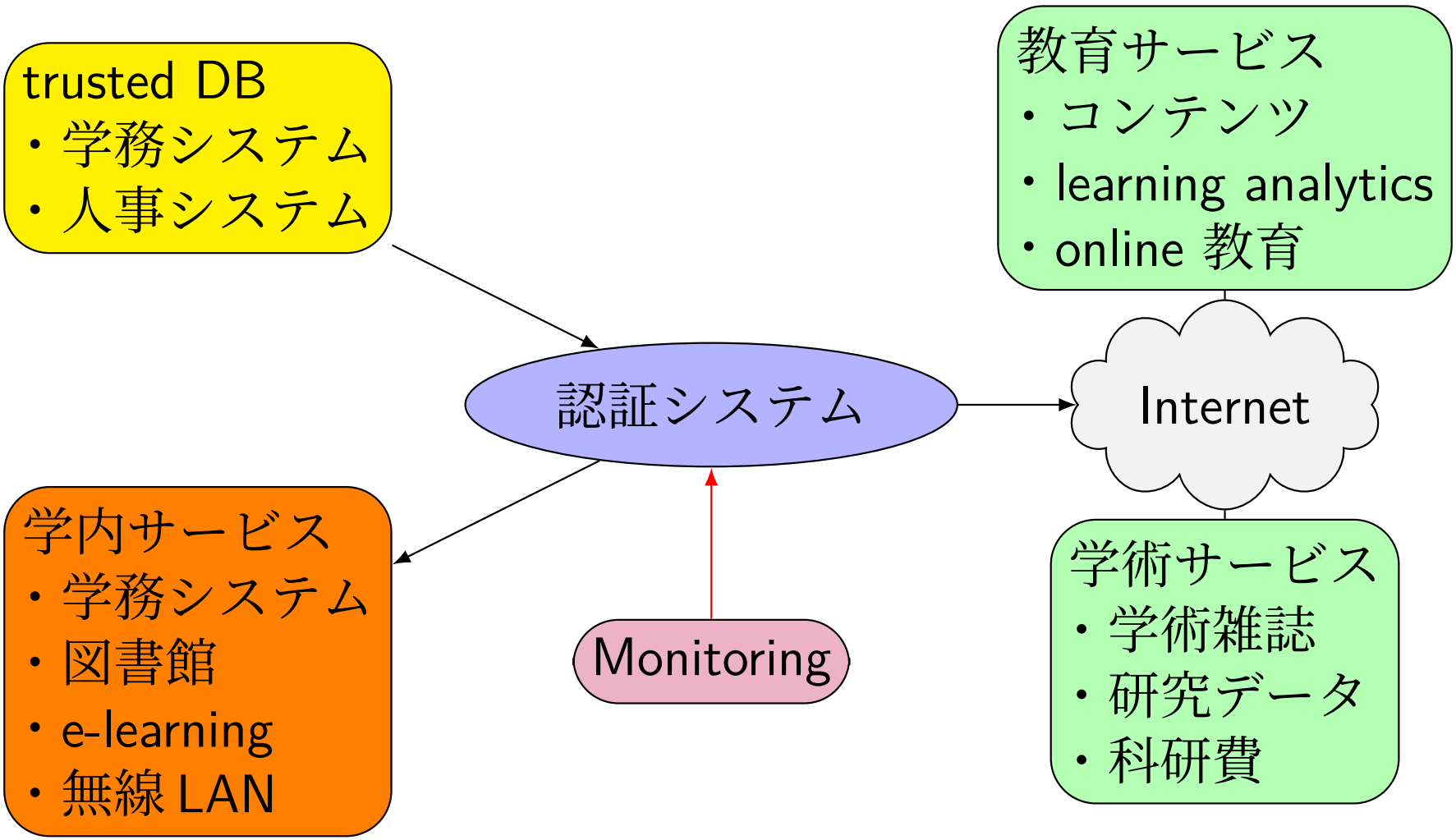
認証連携の活用

- eduroam
  - https://www.eduroam.jp/
  - 訪問先大学でも、自大学の ID で無線を利用
  - ゲスト ID 発行の抑制

認証連携を可能にするには: フェデレーション内の水準維持

- 認証情報の確度
  - 正しい情報に基づいているか
  - 適切な頻度で「棚卸し」されているか
  - 大学ならば、人事システム・教務システムとの連携
- 管理運営体制
  - 人的体制が整備され機能しているか
  - 規則類が整備され、それに基づく運用になっているか

認証システム構成


trusted DB
・学務システム
・人事システム
教育サービス
・コンテンツ
・learning analytics
・online 教育
認証システム
Internet
学内サービス
・学務システム
・図書館
・e-learning
・無線 LAN
Monitoring
学術サービス
・学術雑誌
・研究データ
・科研費

認証システムを導入・運用するには

- 技術的側面
  - 標準的技術の選択
  - ベンダーソリューションの活用
  - クラウドサービス: IDaaS
- 仕組み・体制
  - 利点とコストの確認
  - 組織全体としての体制・規則整備

課題

組織内で認証情報を統合して運用することは、利便性向上とともにセキュリティ強化としても重要です。一方で、なかなか実行に移せない組織も少なくありません。実行するために重要な点は何でしょうか。