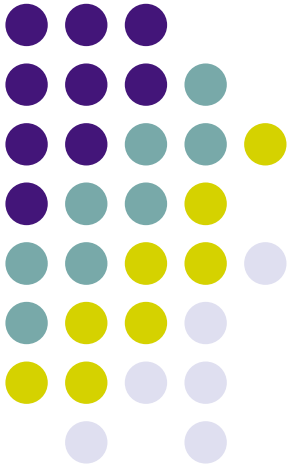
マイナンバーシンポジウムin栃木＠とちぎ福祉プラザ
平成24年9月29日

マイナンバー制度とプライバシー
ー技術的な課題ー

宇都宮大学大学院
情報システム科学専攻
渡辺　裕

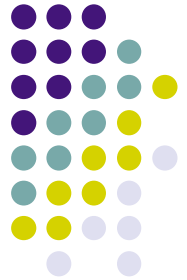


社会保障・税の共通番号

- 社会保障を受ける権利を守る
- 社会保障・税制面での適切な政策遂行
- 効率的な社会保障給付
- 利便性の高い行政サービス提供
- 災害時でも安心できる社会保障サービスの提供

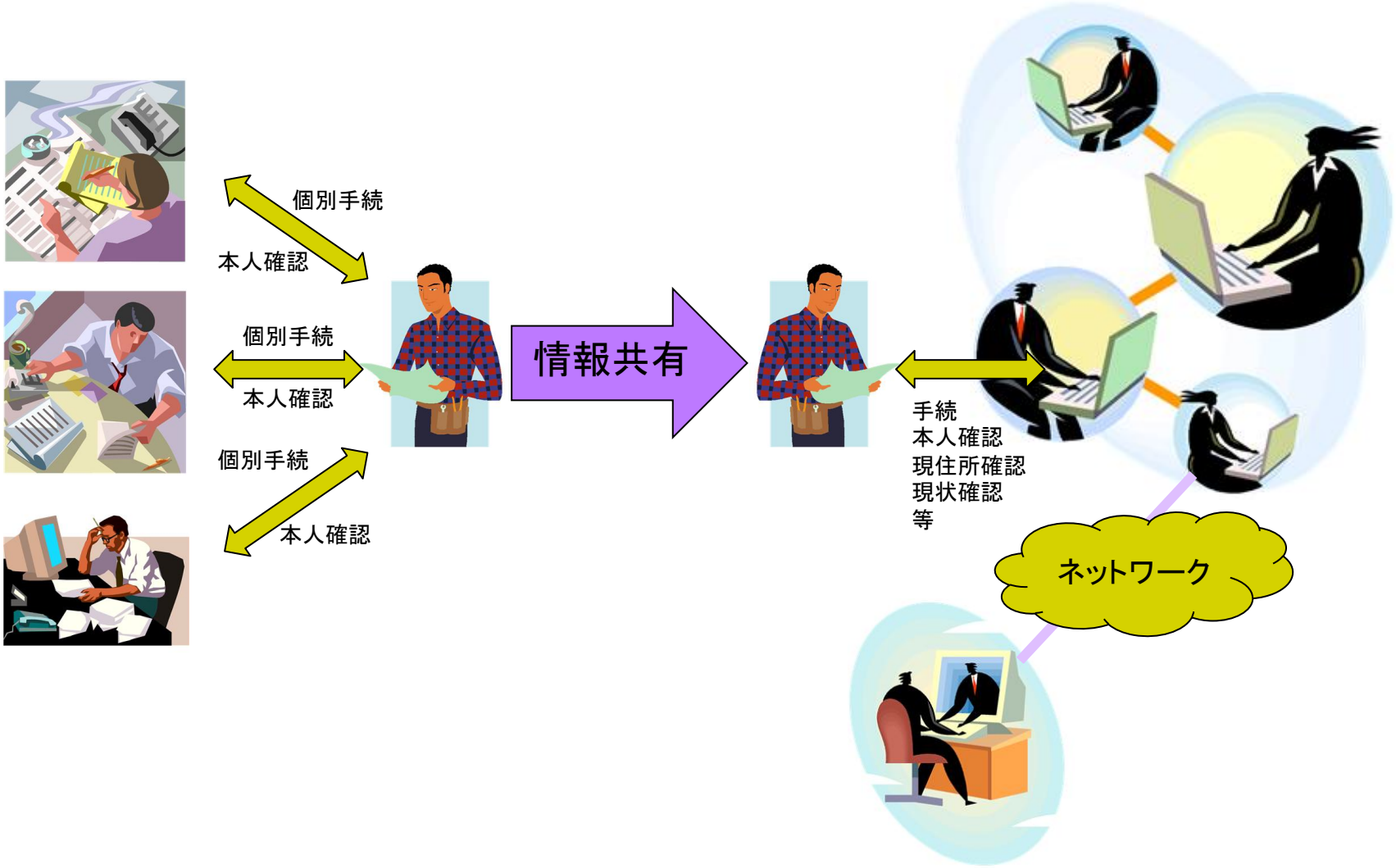
- 番号利用
  年金、医療、介護、福祉、労働、税務

番号制度の利用

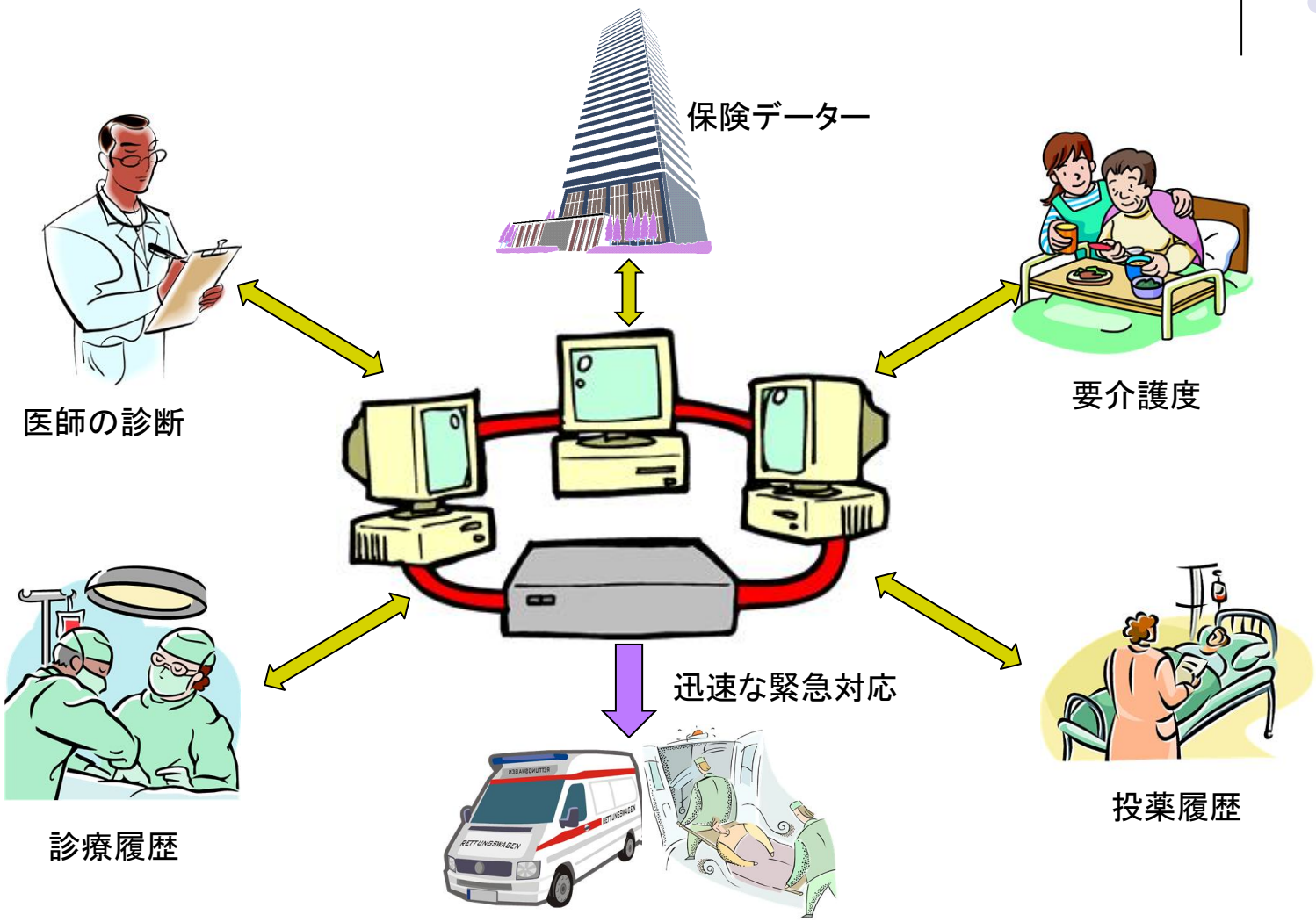


- 税と社会保障制度の融合
- 企業における従業員の税・社会保険料徴収業務の効率化
- 医療データの蓄積利用、介護情報との連携
- 行政手続きの処理状況の確認
- 自己情報の適切な管理確認
- 選挙投票等への応用

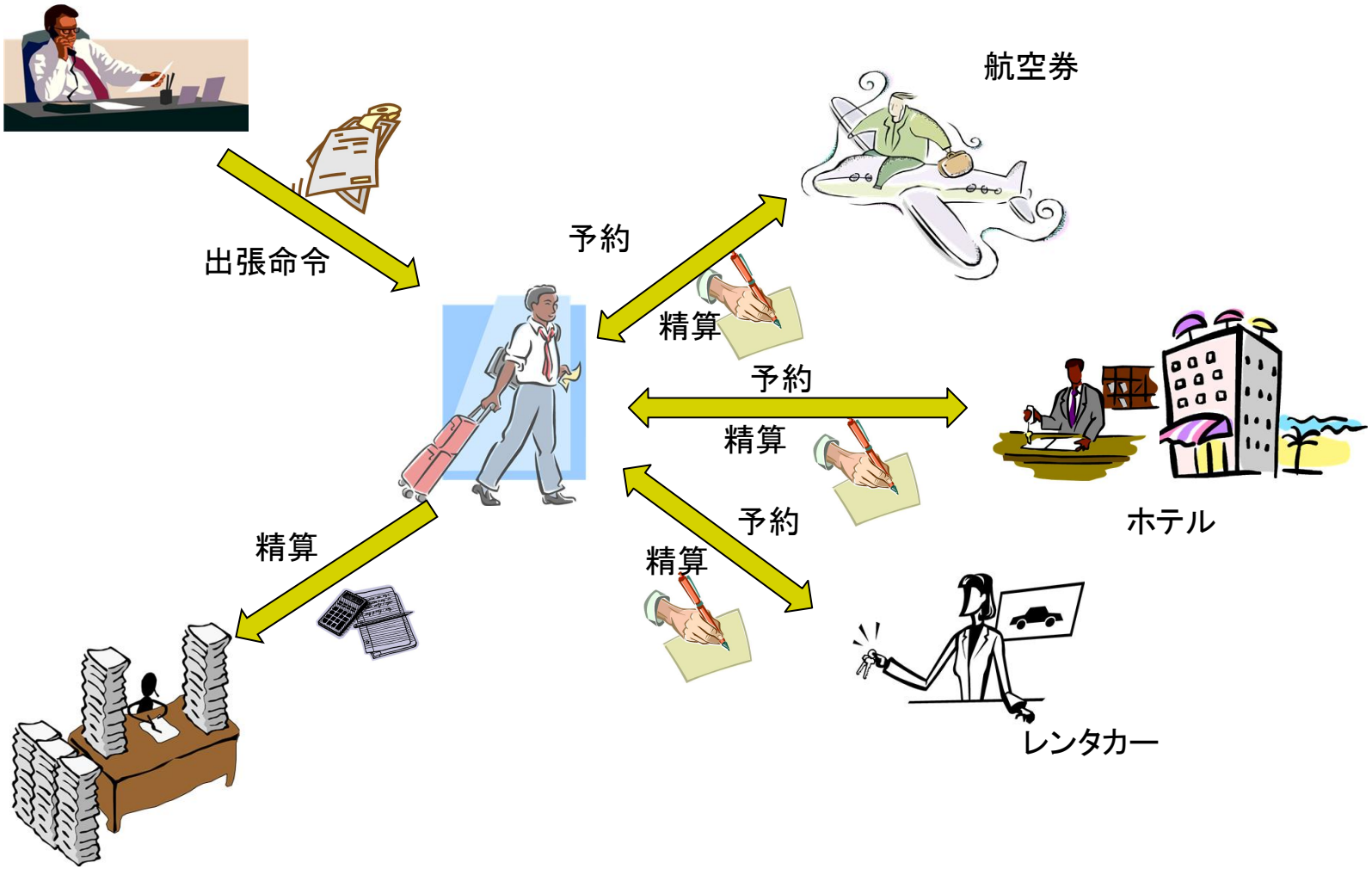
情報共有による利便性の向上



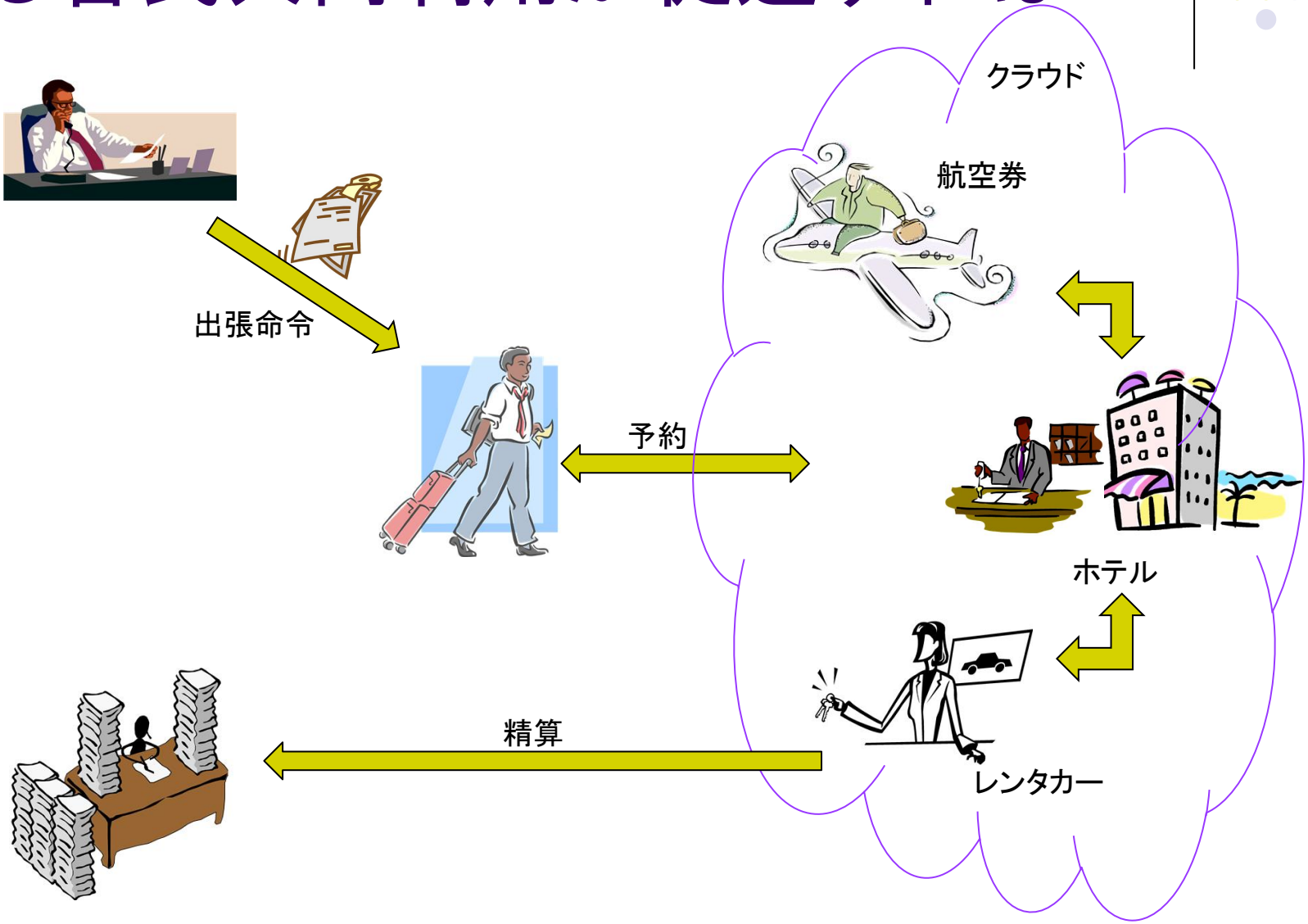
医療･介護の情報連携



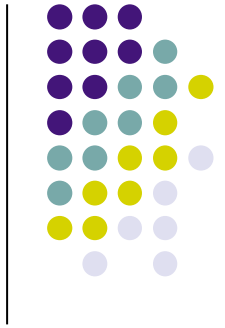
もし官民共同利用が促進すれば



もし官民共同利用が促進すれば



個人情報



- 個人情報とは、特定の個人(人間)を識別することができる情報
- 情報技術の進展により様々な個人情報データのコンピューターによる集積が進んでいる
  - 集積された情報が無制限に利用できると、個人のプライバシーに関わる内容が第三者に容易に把握されてしまう
  - クレジットカードの利用状況、出身校、勤務先、家族構成、通院歴など各種のデータの結合により、私生活の状況が把握される
  - 個人情報の取扱いに関心が高まり、規制が必要とされ、法制度の整備が行われている

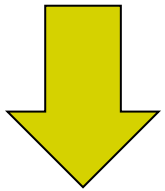
個人情報の項目

基本的事項	氏名、住所、性別、生年月日・年齢、電話番号、識別番号、国籍
家庭生活等	親族関係、婚姻歴、家庭状況、住居状況
社会生活等	職業、職歴、地位・役職、学業・学歴、資格、賞罰、成績・評価、趣味
経済活動等	資産・収入・借金・預金・カード決済などの信用状況、納税額、公的扶助、取引状況

- 上記情報でかつ個人を特定できる場合
- 上記いずれかでも、個人を特定することができなければ、個人情報には該当しない
- 生体情報については、個人特定性が強まっている

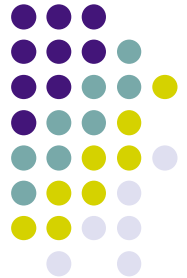
Googleの規約改訂

- 60を超えるGoogleのサービスのすべてに、同じプライバシーポリシーが適用される
- インターネットの法律が変わった？



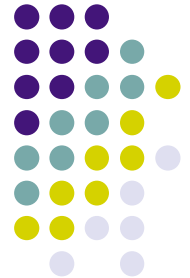
- サービス間をまたいだ個人情報交換への対処
- SNS等へのユーザーの投稿や「いいね！」ボタンを押した情報により検索結果や広告表示を行う

Googleが収集する個人情報



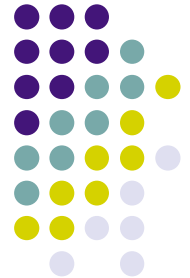
- ユーザが提供する情報
  - Google アカウント登録時の氏名、メール アドレス、電話番号、クレジットカードなどの個人情報
- サービス利用時に収集される情報
  - ハードウェアモデル、オペレーティングシステムのバージョン、端末固有の ID、電話番号などのモバイルネットワーク情報
  - Google サービスを利用時のログ：情報検索キーワード、電話のログ情報等
  - 現在地情報
- 新しいサービスの開発、ユーザに合わせてカスタマイズしたコンテンツの提供を可能とする。
  - 端末の ID や電話番号をアカウントと関連付ける。
  - 特定のサービスから取得した個人情報を、他のサービスから取得した情報と結びつける。
- ユーザの居住国以外にあるサーバーで個人情報を処理する場合もある。

規約改定で何が変わるのか？



- 新しく使うGoogleのサービスが最初からユーザに最適化される
- 全く興味の無い広告が表示される事が無くなる。（広告主にとって広告の無駄うちが無くなる；数打ちゃ当たるから少数精鋭へ）

Googleのストリートビュー

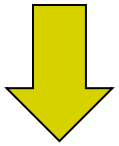


- 必ずしもプライバシー・肖像権などの諸権利との関係を十分に整理し、社会的合意を形成した上で提供されてきたとはいい難い
- 十分な社会的合意を形成するための一層の努力が強く求められる
- プライバシー・肖像権に対する考え方は、時代や技術動向により常に変化するため、今後サービスを取り巻く情勢に変化があった場合には再検討が必要になる

利用者視点を踏まえたICTサービスに係る諸問題に関する研究会　第一次提言(案)　平成21年6月

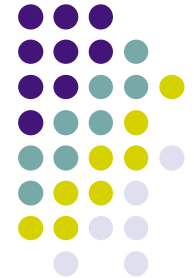
プライバシー

- 個人の私生活に関する事柄（私事）や私事が他から隠されており干渉されない状態を要求する権利



- Privacy refers to the right to self-determination.
  - 自己の明確化に関する権利
- The right of individuals to ‘know what is known about them’, be aware of stored information about them, control how that information is communicated and prevent its abuse.
  - 知られていることを知る権利
  - 蓄積されたその人に関する情報を知ること
  - 情報の伝達を制御でき、悪用を防ぐこと

ISO15001 （JIS Q 15001）

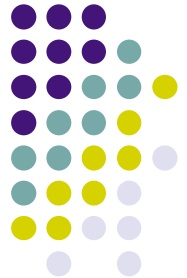


- 個人情報保護マネジメントシステム：PMS (Personal information protection management systems)
- 個人情報を適切に扱うための管理システム
  - それを実践するための計画を立て（Plan）
  - それを実行し（Do）
  - 個人情報保護が適切に行われているかどうかを定期的または必要に応じて評価し（Check）
  - 改めるべき点があれば改善する（Action）
- 品質管理システムISO 9001、環境管理システムISO 14001、情報セキュリティマネジメントシステムISO/IEC 27001と同じ手法

アイデンティティ

- アイデンティティ
  - 人の属性情報の集合
- アイデンティファイア
  - いわゆるユーザ名、パスワード

アイデンティティ管理
IdM: identity management

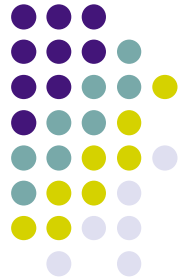


- 利用者のアイデンティティ情報（ユーザーID、ユーザー権限、ユーザープロファイル）の設定を継続的に追加・変更・削除すること
- 管理内容；
  - 利用者を特定するための識別・認証情報
  - 利用できる機能や範囲を定める利用権限情報
  - 利用者の行動や履歴を把握するプロファイル情報
- 可能になるサービス
  - 特定の利用者のみにサービスを提供する
  - 利用者ごとにサービス内容を変更（パーソナライズ）する

アイデンティティ管理の3要素

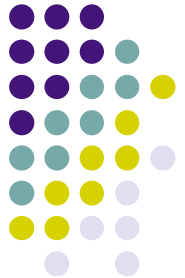
- 認証：Authentication
  - あるサービスが、ユーザーを特定する行為
- 認可：Authorization
  - あるサービスが、特定のユーザーに対し、特定のリソースの利用許可を判断する行為
- 属性交換：Attribute Exchange
  - あるサービスが、ほかのサービスに対し、特定のユーザーの属性情報を提供すること

セキュリティ関連の標準機関



- 国際標準
  - ISO：国際標準化機構
  - ITU-T：国際電気通信連合
- 地域の団体
  - ETSI：欧州電気通信標準化機構
- 国内団体
  - NIST：アメリカ国立標準技術研究所
- 特定分野
  - OASIS：構造化情報標準促進協会（電子ビジネス標準策定）
  - リバティアライアンス（アイデンティティ管理技術の技術標準策定）
  - IETF（インターネットの技術標準策定）
  -
  -

標準化の動向



- 技術的重要課題として、アイデンティティ管理技術が注目されており、ITU-T、ISO/IEC等において精力的な標準化活動が行われている。
  - アイデンティティ連携
    - パートナー間でアイデンティティ情報を関連付ける技術
  - 認証連携
    - 組織をまたがるシングルサインオン
  - IDプロビジョニング
    - アカウントの配布機能の拡張
  - 属性情報交換
    - 信頼するパートナ間での属性情報の共有

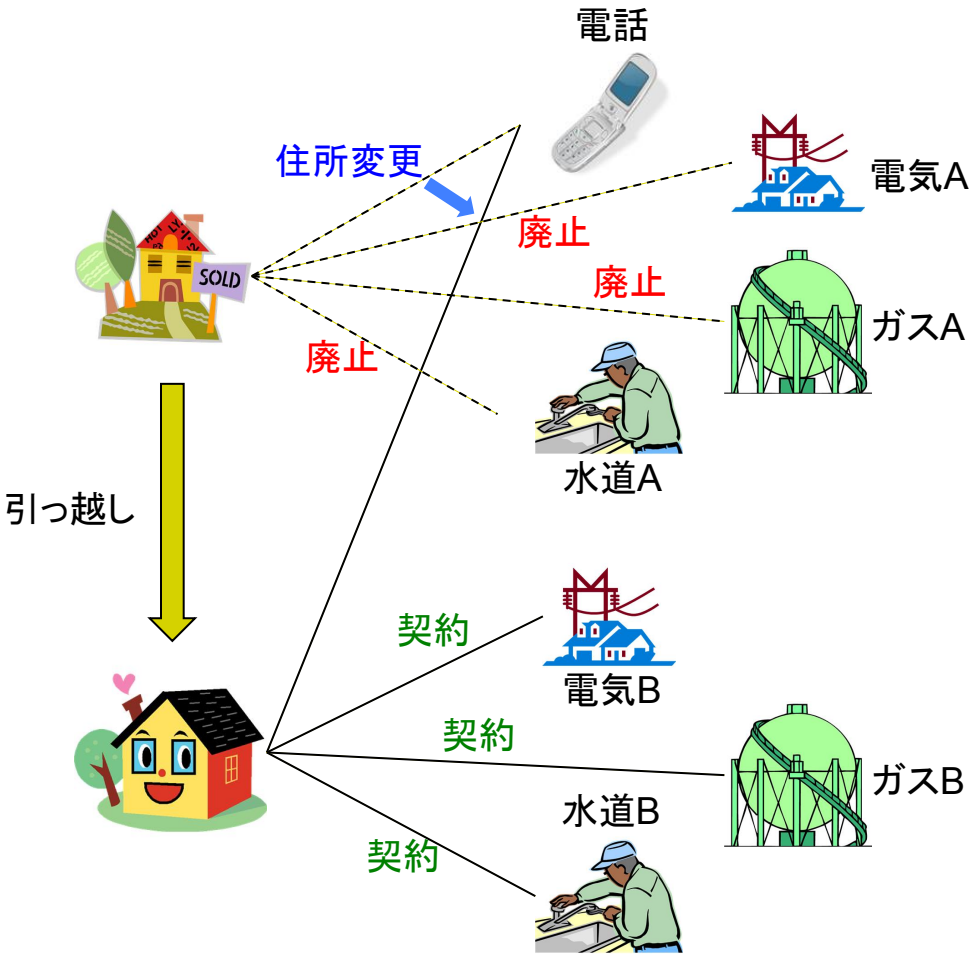
リバティアライアンス

- プライバシを保護した安心安全なアイデンティティ管理の実現
- 150以上の企業・組織・団体が参加

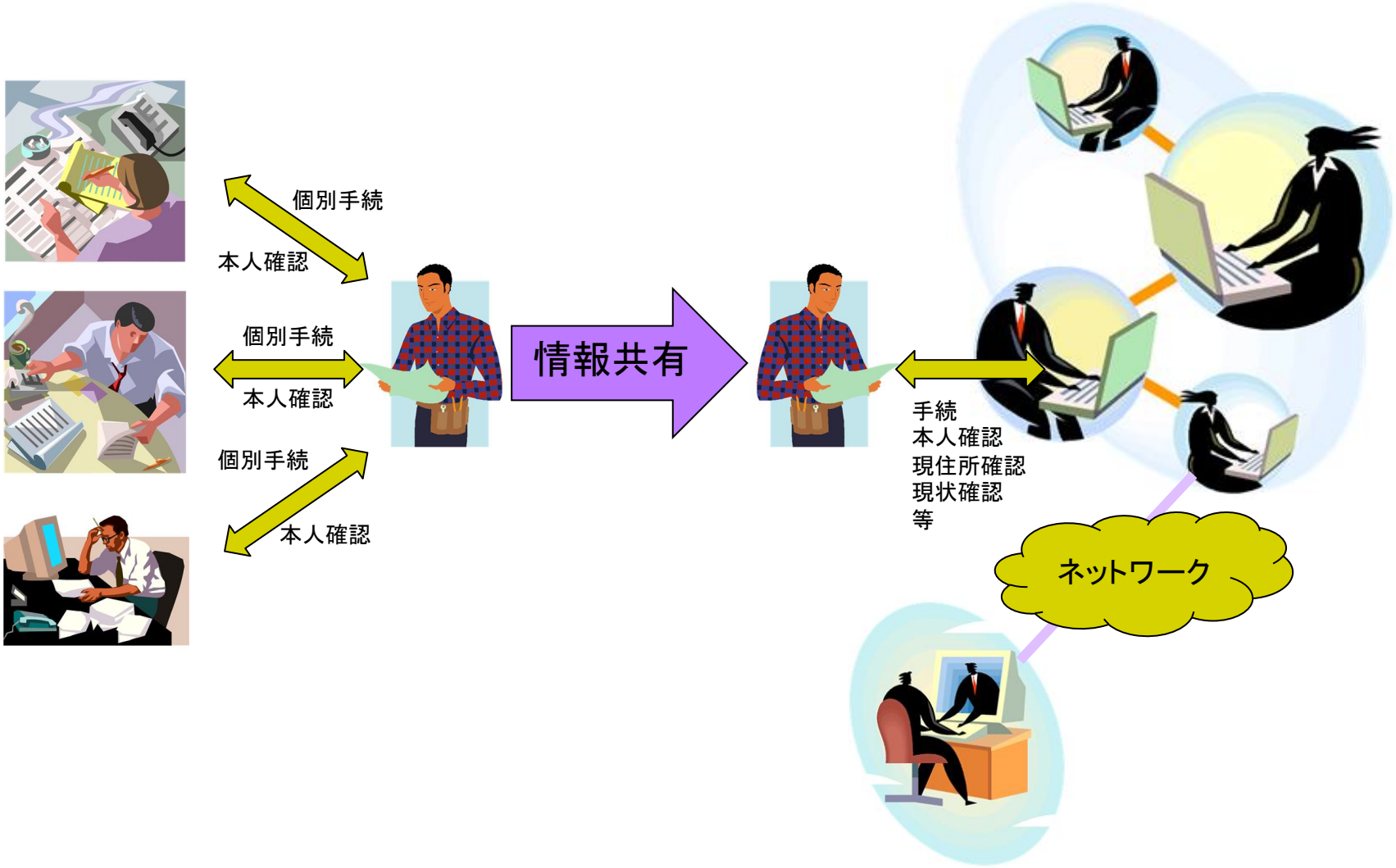
理事会のメンバー

これまでのアイデンティティ管理

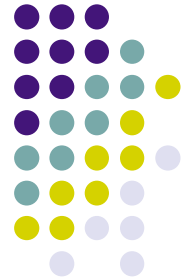
- 引っ越しをした場合には、電話、電気、ガス、水道など、それまでに関係を持っていたすべてのユーザープロファイルを、別個に変更する必要がある
- サービスがサービスを提供する上ですべて作成したユーザー情報は、各所に拡散している
- これらの情報は、相互に関係を持つことは無く、個々のサービスごとに管理される



これからのアイデンティティ管理

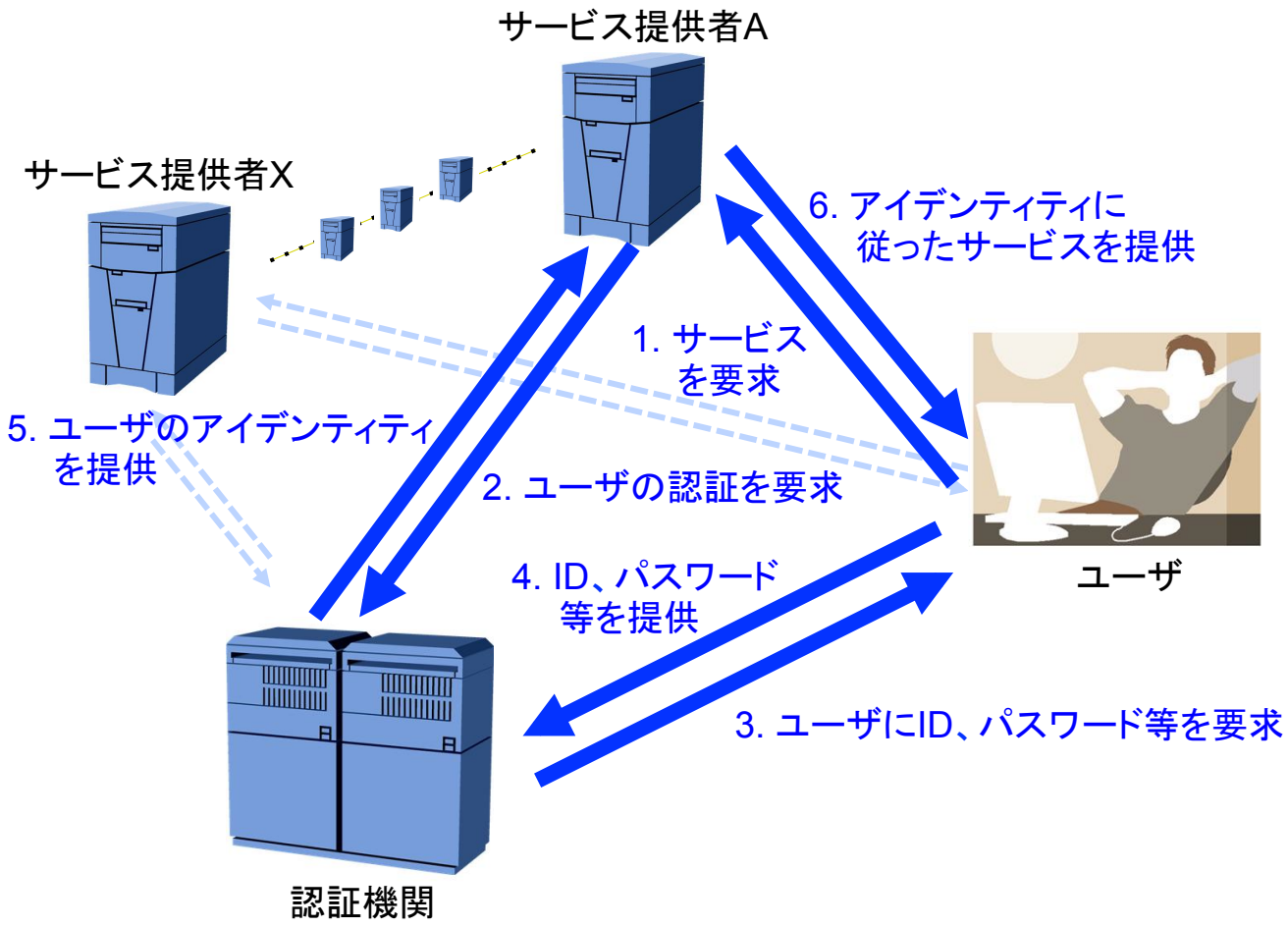


SAML:
Security Assertion Markup Language



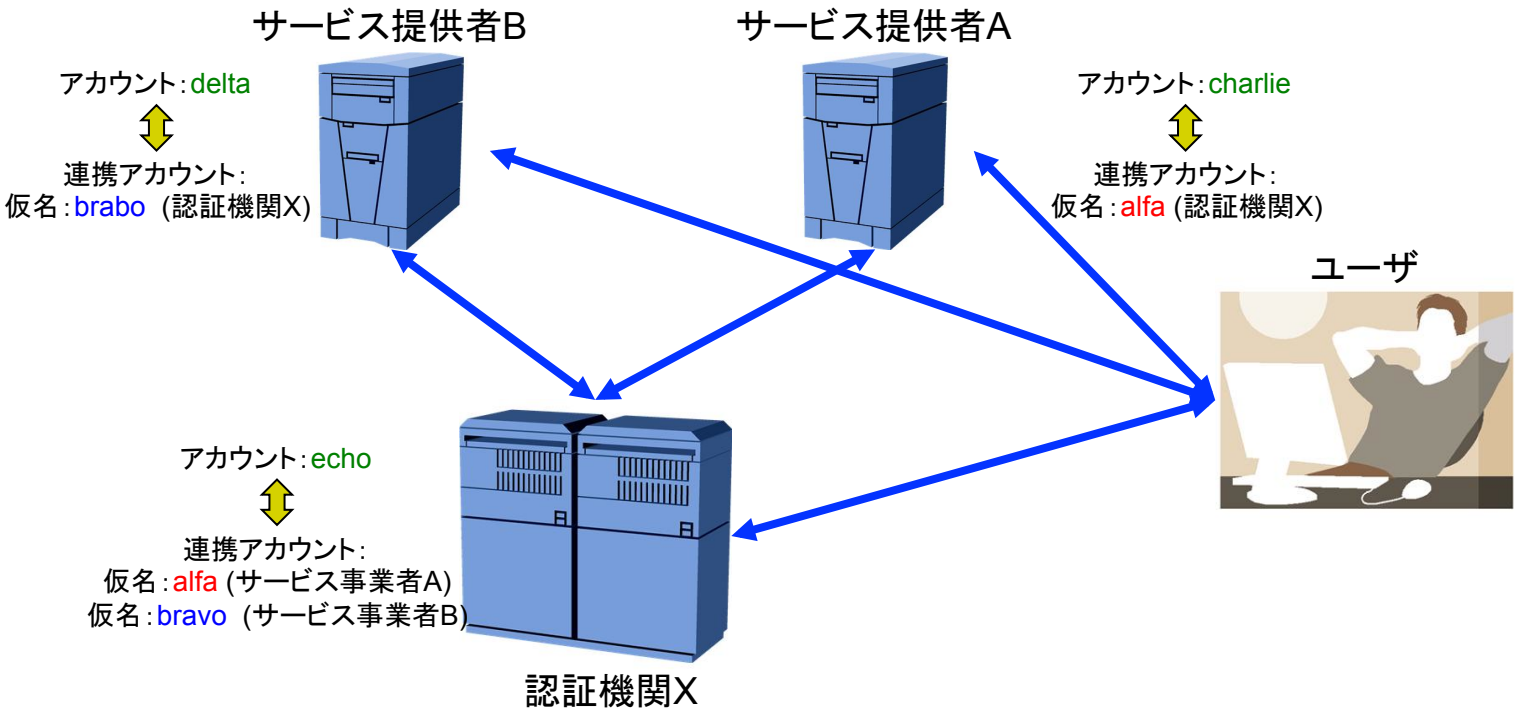
- 標準化団体OASISによって策定された一度の認証で複数のサービスが利用できるシングルサインオン(SSO：Single Sign-On)を実現する仕様
- ITU-Tも勧告化（X.1141: Security Assertion Markup Language）
- プライバシー保護機能を具備
  - 仮名の利用による名寄せの防止

シングルサインオン


サービス提供者A
サービス提供者X
6. アイデンティティに
従ったサービスを提供
1. サービス
を要求
5. ユーザのアイデンティティ
を提供
2. ユーザの認証を要求
4. ID、パスワード
等を提供
ユーザ
3. ユーザにID、パスワード等を要求
認証機関

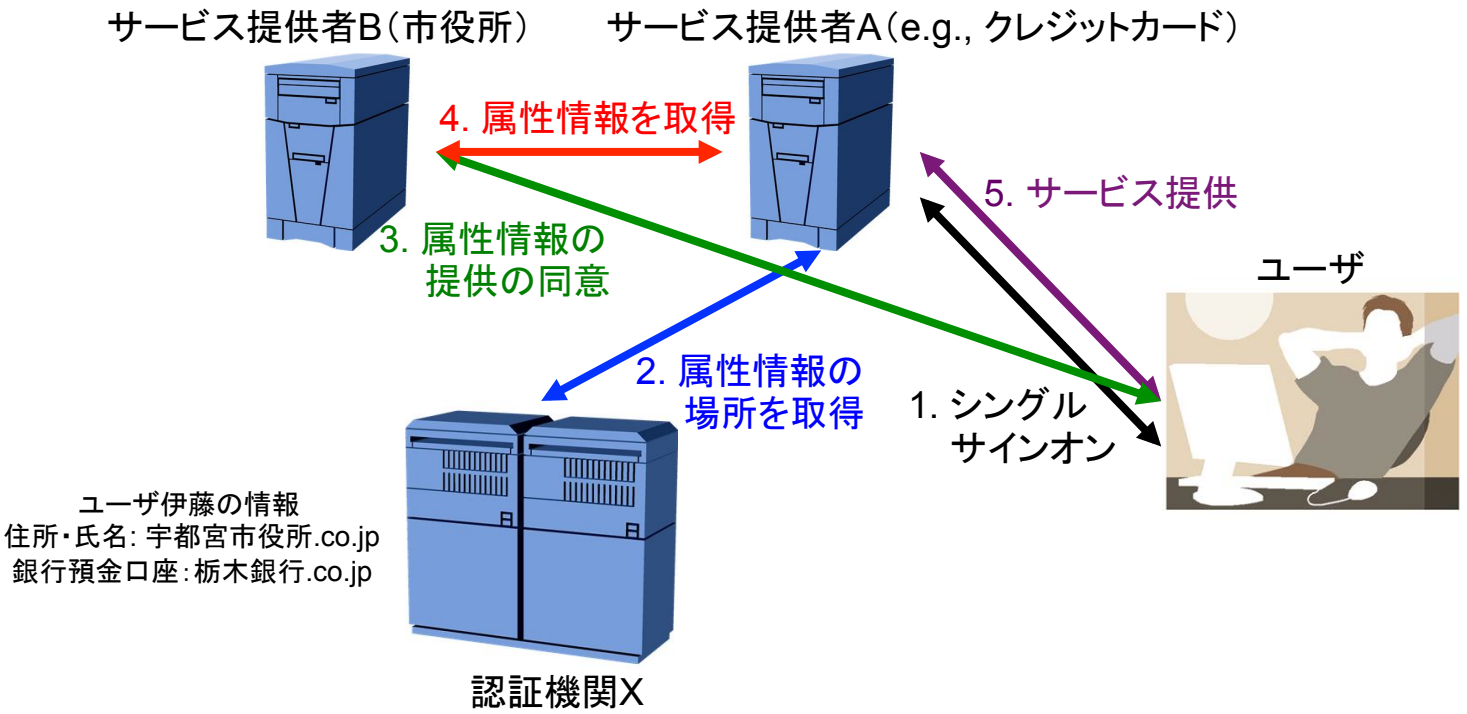
仮名を使ったアカウント連携

- 個人を特定不能な仮名の利用によるプライバシー保護
  - 仮名の利用により実アカウント名の流出を防
  - 事業者の結託による名寄せの防止



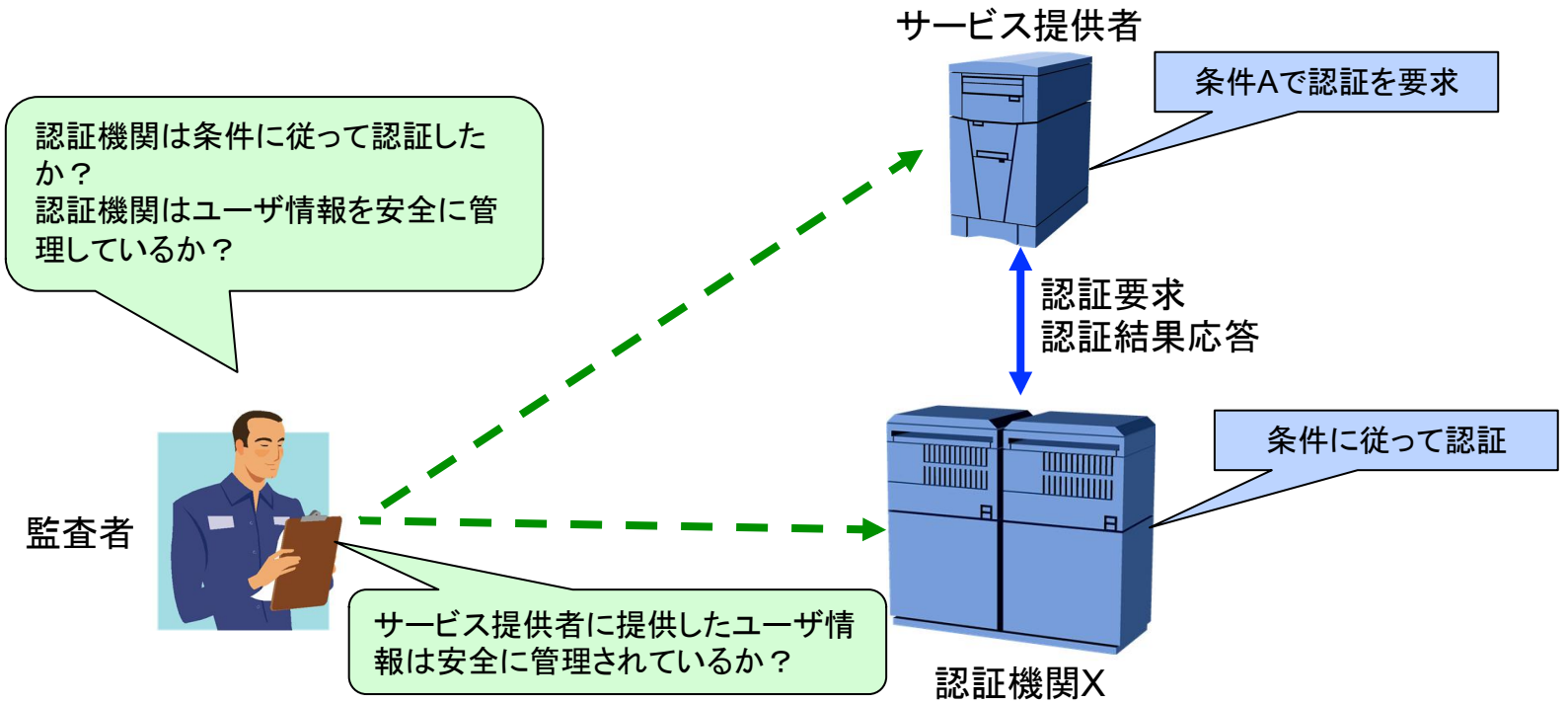
Liberty ID-WSF:
属性情報の安全な交換・利用

- サーバに登録されている属性情報をサービス業者間で直接交換し、ユーザのサービス登録や利用時の手間を省いたり、サービスのパーソナライズを図る。
- 仮名アイデンティティ連携及び情報提供の同意取得機能でプライバシ保護



IAF: Identity Assurance Framework
第三者の評価

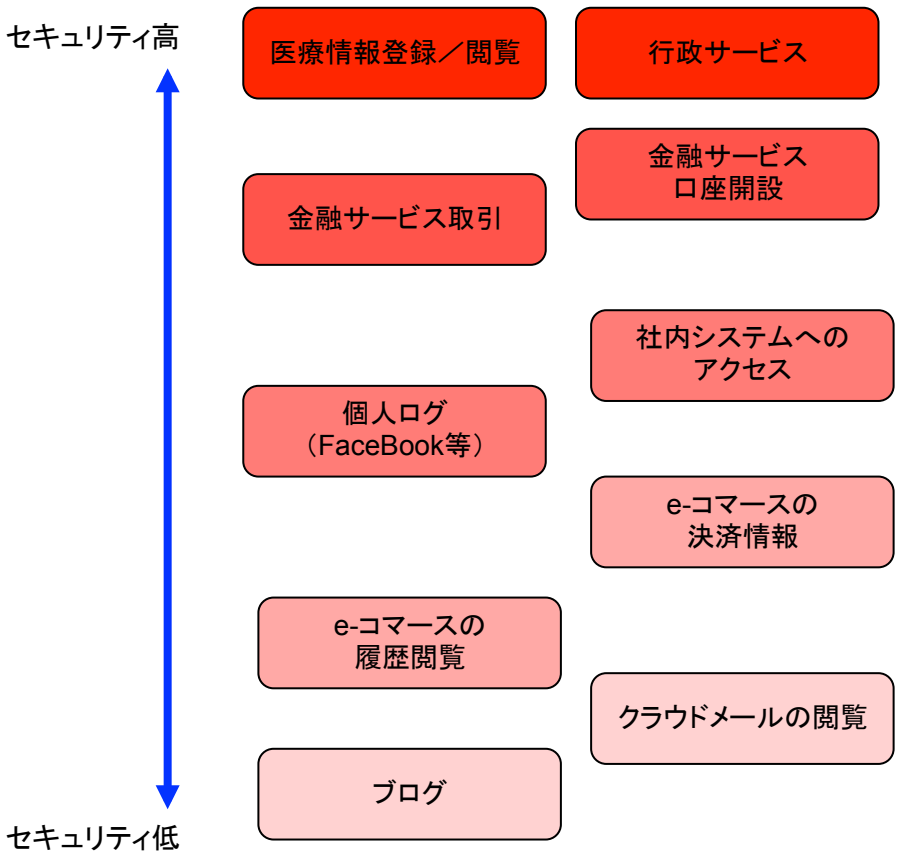
- 事業者がユーザー・アイデンティティを管理、運用するのにふさわしいことを監査する。



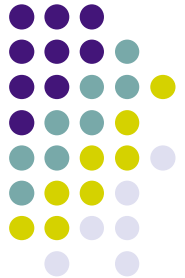
アイデンティティ保証レベルの規定

- アイデンティティの機密性の高さ
- アイデンティティを保護する上での重要度
- 優先順位

kantara INITIATIVE™



海外での事例



- 英国:
  - 各種電子政府システムへのシングルサインオン。登録済ID:800万。
- 米国:
  - NY州の公立学校(約700校)システムのシングルサインオンを実現。教師1万人が登録済。
  - 一般調達局(GSA)で政府システム間の連携標準技術として採用
- フィンランド:
  - オンライン納税や公的文書の一元管理
- ノルウェー:
  - 個人情報にアクセスする政府系マイページポータルサービス
- イタリア:
  - 運転免許更新サイトへのシングルサインオン
- オーストリア:
  - 市民認証カードによるオンラインバンキングのユーザ認証
- ニュージーランド:
  - 電子政府サービスに省庁を越えてシングルサインオン

出典:NTT情報流通プラットフォーム研究所資料

マイナンバー制度の導入の技術課題

- ディレクトリ
  - ネットワーク上のユーザ情報やネットワーク資源一元管理。ITU-T勧告X.500
- アクセスコントロール
  - アクセス／ポリシー制御。OASISで標準化-XACML（eXtensible Access Control Markup Language）ITU-T勧告X.1142
- プロビジョニング
  - アカウント情報の作成・追加・修正・停止・削除。OASISで標準化SPML（Simple Provisioning Markup Language）
- 認証・認可
  - 複数サイト間で、認証情報を安全に交換する。OASISで標準化SAML（Security Assertion Markup Language）ITU-T勧告X.1141
- アイデンティティ連携／サービス連携
  - 連携アイデンティティサービス。LibertyのID-WSF