資料３－４

ITU-TにおけるID管理の状況
～ ITU-T SG13とFG-IdMを中心に ～

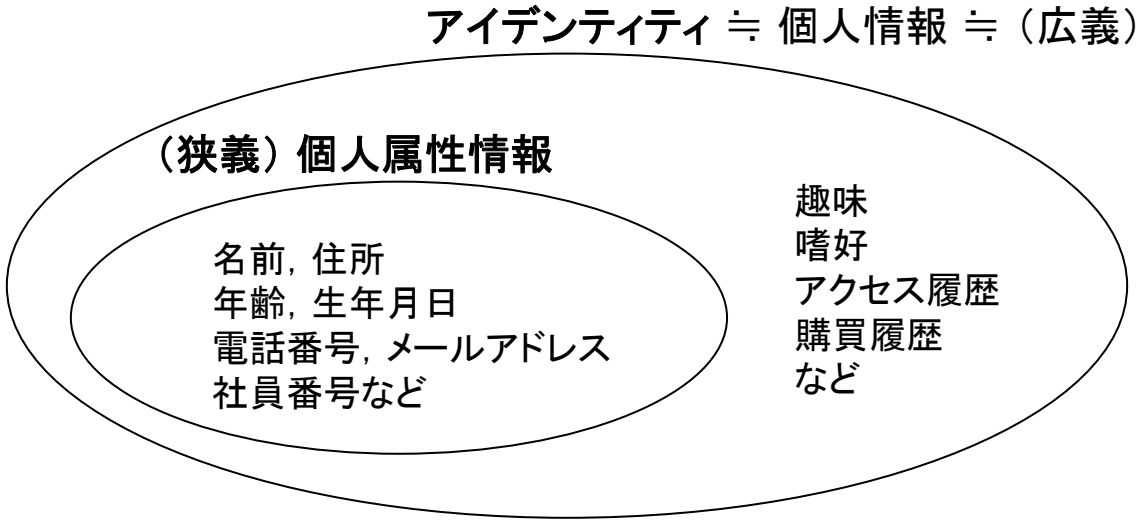
2007年12月20日

KDDI株式会社　中尾　康二
日本電気株式会社　江川　尚志

1. ID管理（IdM）とは何か

アイデンティティ(人)とは

- 個人を特徴付ける属性情報の集合
  - (狭義)属性情報:
    - 名前, 住所, 電話番号, メールアドレス, その他
  - (広義)属性情報
    - 趣味, 嗜好, アクセス履歴, その他

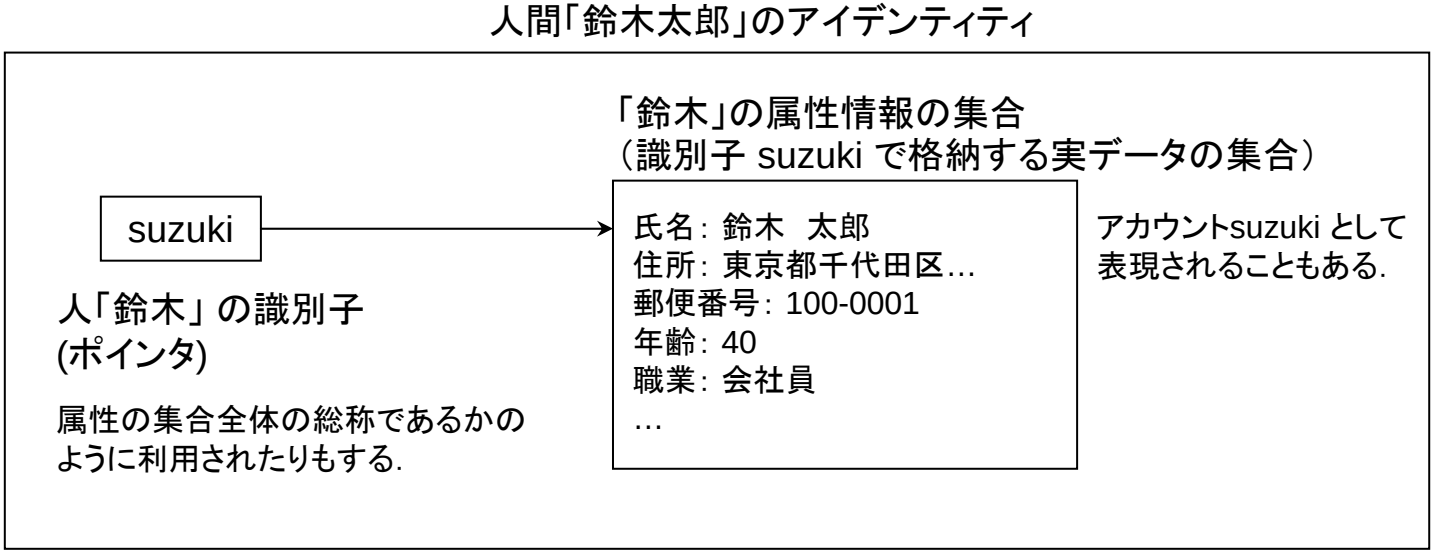


属性情報の狭義・広義の
明確な定義づけはない

＊アイデンティティ管理では, 主に「人」のアイデンティティが対象.
(ただし, 人と関連付けられる「物」もアイデンティティの1つ.
従って「物」の情報化が主であるNIDとは直接には競合しない(注意は必要))

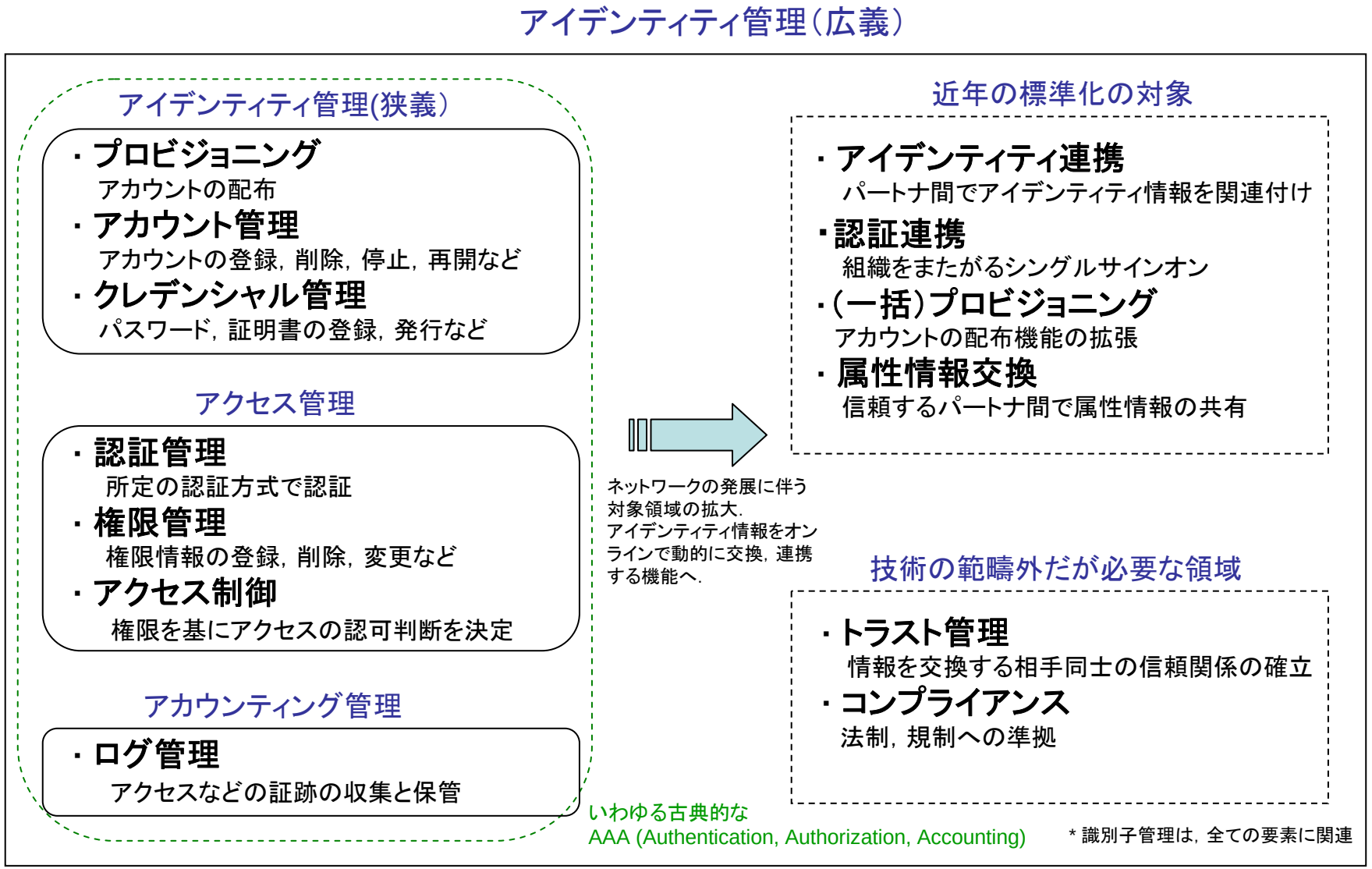
IDの2つの定義

- 一般に，人の IDは以下の両方の省略形として利用されることが多い.
  - **Id**entity（アイデンティティ）→「アイデンティティ管理」と呼ばれる領域
    - 上記，Identifierを包括した，人の属性情報の集合（既出）
  - **Id**entifier（アイデンティファイア：識別子）
    - アイデンティティへの参照情報（ポインタ）.
      - いわゆる”ID/Password” のIDはこれに相当.
    - 本「識別子」という意味で用いながらも，その管理対象である「アイデンティティ」を指すこともあり.



＊「ID管理」という時，”Identity” **なのか** “Identifier” **なのか注意が必要.**

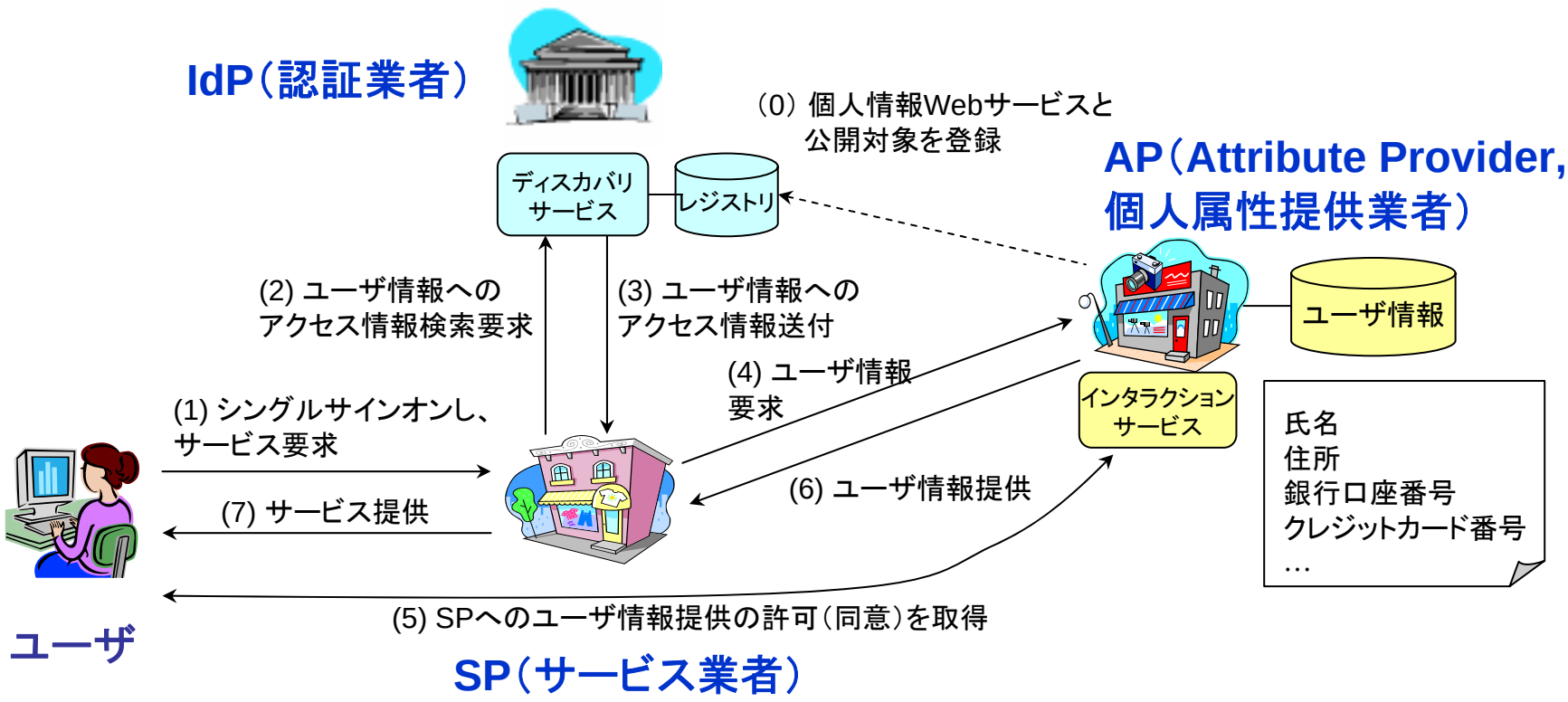
アイデンティティ管理の対象領域



ID管理の例：Liberty ID-WSF

個人情報の安全な交換と活用

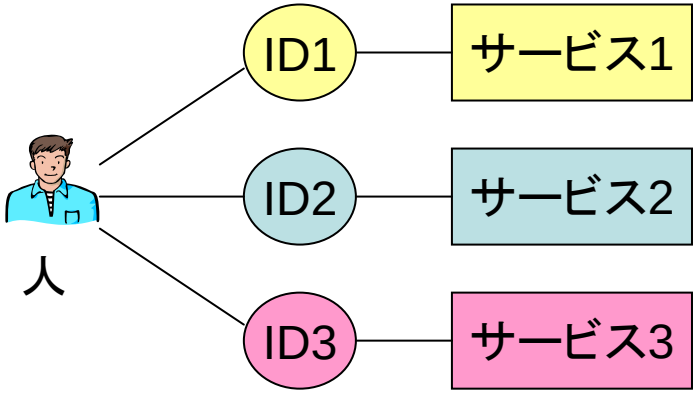
- サーバに登録されている個人情報をサービス業者間で直接交換し、ユーザのサービス登録や利用時の手間を省いたり、サービスのパーソナライズを図る。



*ID-WSF: Identity Web Service Framework

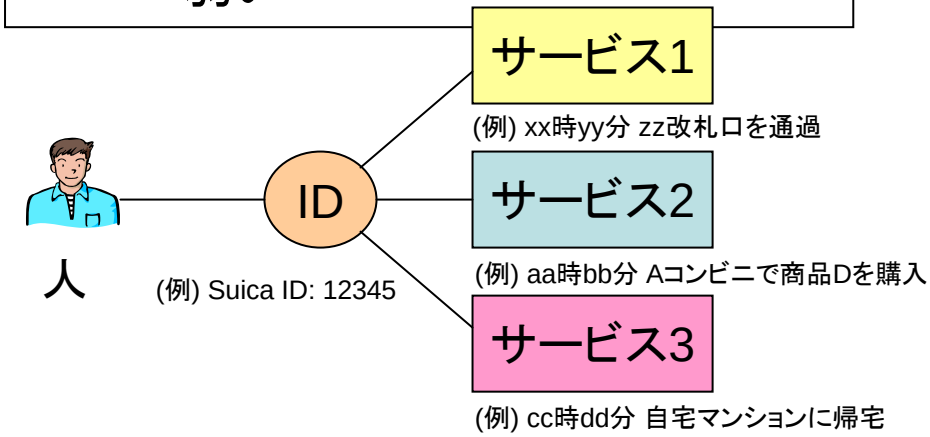
ID管理の課題例: トラッキングによるプライバシ漏洩

- ローカルID（識別子）
  - 有効範囲が限定的で、独立性が高い



・各IDは、人の各サービスにおける行動しか追跡できないので、
プライバシ漏洩リスクは低い

- グローバルID（識別子）
  - 有効範囲が広く、独立性が弱い



・共通化されたIDは、人の全てのサービスにおける行動を追跡可能とし、プライバシ漏洩リスクは高い
・ID自体がランダムな番号であっても漏洩リスクは同じ
・いずれかの情報から本人確度が高くなると全ての情報が本人と関連付けられてしまう

cf) http://java-house.jp/%7Etakagi/paper/iccard-world-2004-takagi.pdf

ID管理の基本目標: 第1回FG-IdM会合より（1）

通信事業の価値の源泉は、人々を結びつけることにある。
「私の娘は、Skypeで友達の家と常時接続し、空間を共有している。
これはもはや電話の置き換えではないのだ。
新しいSocial Networkのツールであり、ここに通信の価値がある」
（Lee Dryburgh, Bittech社　社長）
では、誰と誰を、いつ、どのような手段で結びつけるべきか？

- 解くべき課題
  - 属性を広告 (advertise) する方法
  - 広告されている属性を見つける方法 (discovery)
  - 強固な認証との結合(MSISDN, E.164, 名前、住所等)

「隣の寿司屋」で通信が出来るようにする方法は？
「この技術課題の解決法を知っている人間」を見つける方法は？

ID管理の基本目標: 第1回FG-IdM会合より（2）

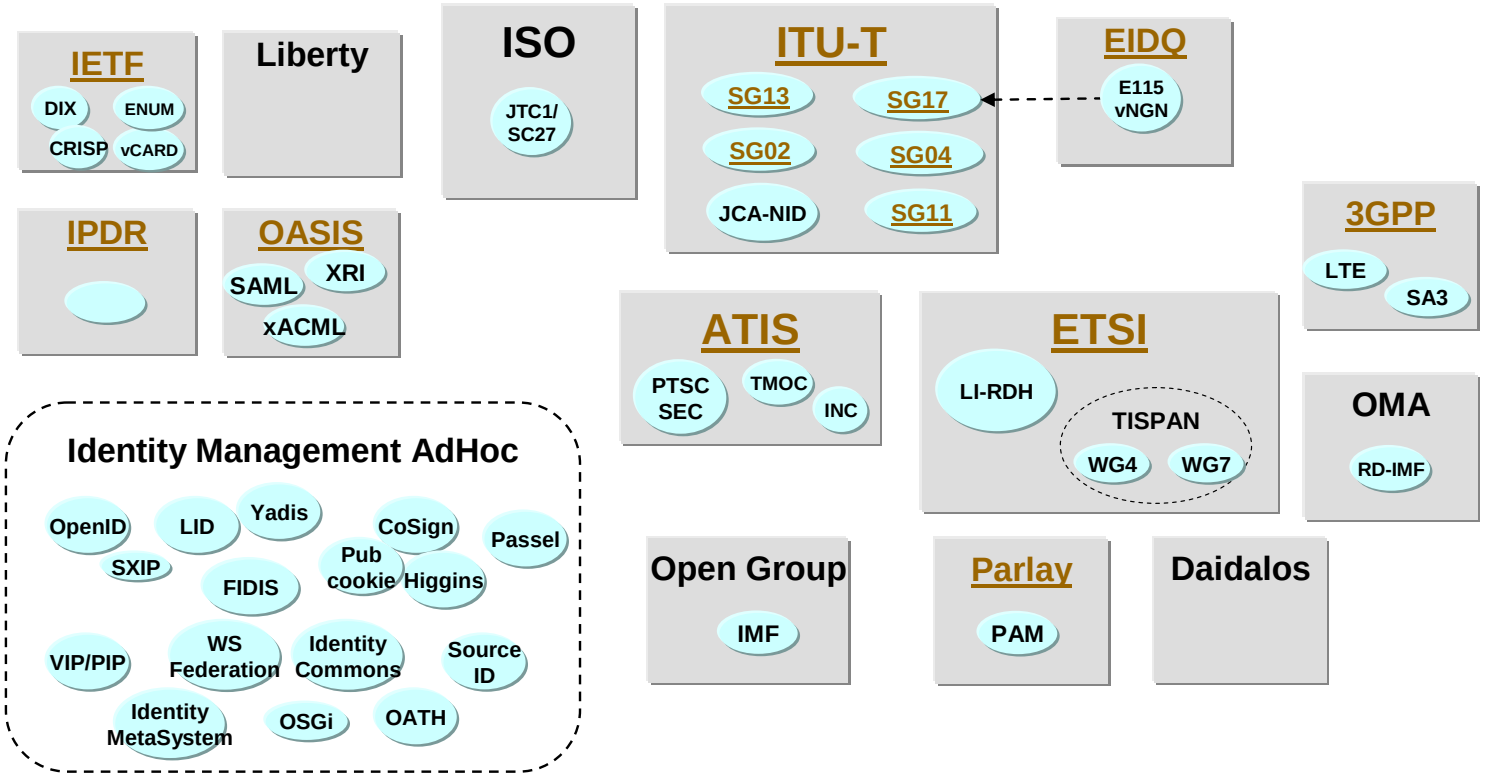
- 通信オペレータが持つ能力
  - 地理的位置情報の特定
  - コンタクトのためのIDや属性の特定
  - IDをSIM等で「アンカー」すること
  - ユーザ情報の提供 (ホーム/オフィス、利用端末、移動速度など)
  - ユーザのネットワーク (バディリストなど)の保管と広告

これらを、プライバシを守りつつ管理し、コンテキストに合わせて利用可能とすることがID管理の目標

GoogleのFON（無線LANホットスポット）への出資（2006/02）

無線LANへの接続を用いてユーザの位置情報を把握し、それに基づくターゲット広告を行うシステムを確立するためとの憶測あり

アイデンティティ管理関連団体



* ITU-T Y.IdMsec仕様 から抜粋

FG-IdM第１回会合冒頭での各種団体活動レビュー

- ITU-T SG13, SG 17 & ISO SC27 (IdM), Dick Brackney (USA), Tony Rutkowski (VeriSign)
- Content Industry standard identifier activities , Norman Paskin (ISO)
- Handle System , [Norman Paskin] (www.handle.net)
- 3GPP IDM , Martin Euchner (Siemens), Frederick Hirsch (Nokia)
- A NGN Overview:from an IdM perspective , Tony Rutkowski (VeriSign)
- Identity Federation and Web Services, Liberty Alliance, Fulup Ar Foll (SUN)
- CardSpace and Identity Metasystem, Mike Jones (Microsoft)
- OpenID: Making the Web Suck Less!,David Recordon (VeriSign)
- Interoperable Identifiers in Next Generation Networks, Ajay Madhok (AmSoft)
  OASIS XRI (i-names) and XDI
- Higgins Project, [Paul Trevithick, Project Technical Lead]Higgins, Tony Nadalin (IBM)
- JCA-NID Overview, [Pierre-André Probst] (OFCOM Switzerland)
- Object identifiers (OIDs) and Registration Authorities,Olivier Dubuisson (France Telecom) , OID (Object Identifier Registry)
- Identity Commons overview, Kaliya Hamlin (Identity Woman)
- Privacy and Rights Management, Mary Rundle (Berkman Center for Internet and Society at Harvard Law School and Stanford Center for Internet and Society)

2. ITU-TにおけるID管理検討の現状

ITU-T Study Groups

- **SG 2** Operational aspects of service provision, networks and performance
- **SG 3** Tariff and accounting principles including related telecommunications economic and policy issues
- **SG 4** Telecommunication management
- **SG 5** Protection against electromagnetic environment effects
- **SG 6** Outside plant and related indoor installations
- **SG 9** Integrated broadband cable networks and television and sound transmission
- **SG 11** Signalling requirements and protocols
- **SG 12** Performance and quality of service
- **SG 13** **Next generation networks**
- **SG 15** Optical and other transport network infrastructures
- **SG 16** Multimedia terminals, systems and applications
- **SG 17** **Security, languages and telecommunication software**
- **SG 19** Mobile telecommunication networks
- **TSAG** Telecommunication Standardization Advisory Group

www.itu.int/ITU-T

ITU-TでのID管理検討

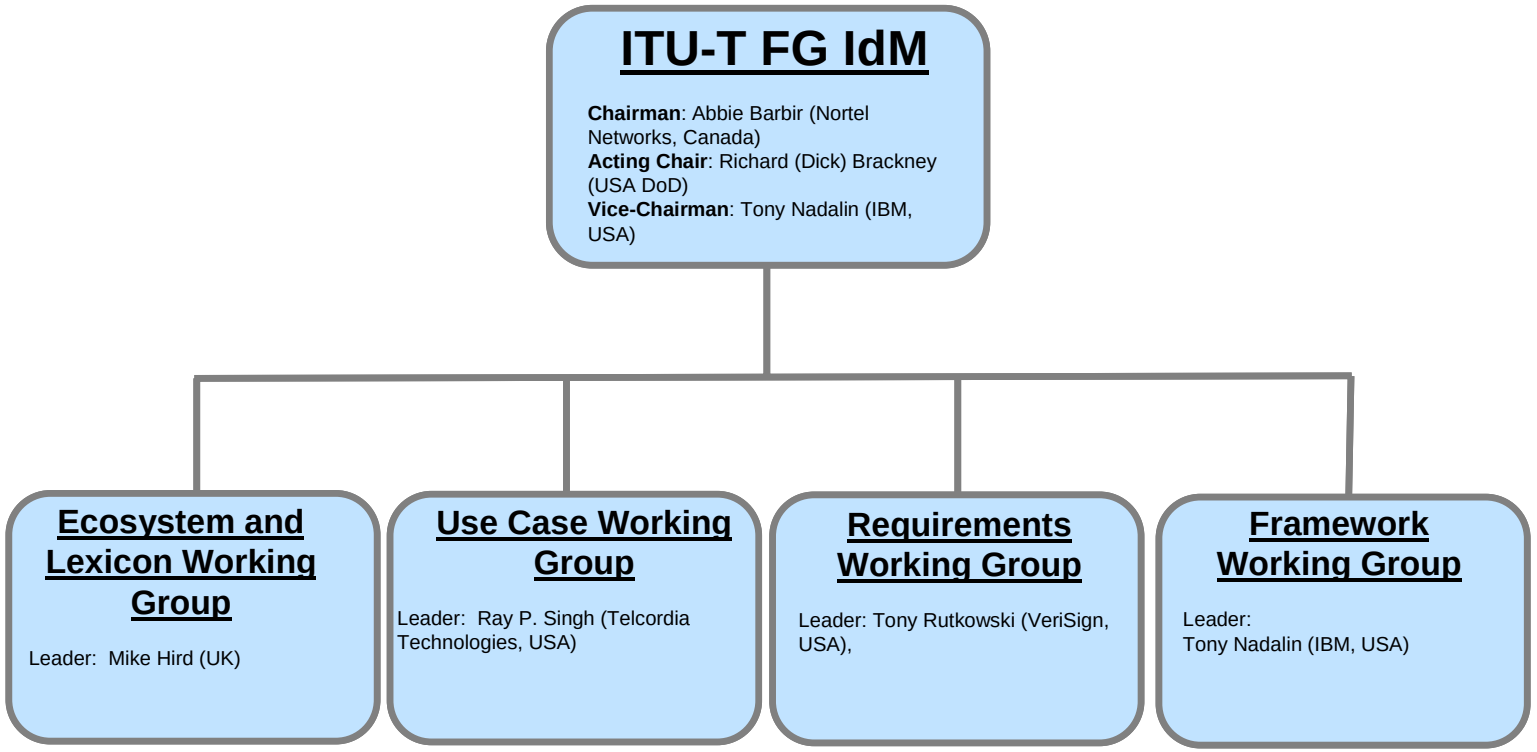
- SG13 Q15 (NGN security)
  NGNでのIdM (Identity Management) を規定するY.IdMsec (NGN Identity Management Security) を2006年10月より検討
- FG-IdM (Focus Group on Identity Management)
  SG17配下で2007年2月よりIdM全般を検討

  これら2つの活動の中心人物はいずれも米国国防総省(DoD)のRichard (Dick) Brackney氏 (ISO/IEC JTC1 SC27 WG5の中心人物でもある)

- (JCA-NID)
  RFID等のタグとそれを支える網機能を検討
  （モノの情報化）

FG IdM – Overview（2/9）

- FG IdM Organization and Structure



FG-IdM: WG構成とリーダー

- 議長: Abbie Barbir (Nortel, カナダ); SG17 Q6ラポータ
- 副議長 Dick Brackney (DoD, 米); Y.IdMsecエディタ
- 副議長 Tony Nadalin (IBM、米); Higginsプロジェクト関係者

- Use Cases Working Group (ユースケース)
  - Sergio Fiszman (Nortel, 加)
  - Ray Singh (Telcordia, 米); Q15/13関係者
  - Mike Jones (Microsoft、米); Card Space関係者
  - David Recordon. (Verisign、米); Open IDの中心人物
- Requirements Working Group (要求条件)
  - Tony Rutkowski (Verisign、米); 弁護士、FCCやITUの役職を歴任
  - Jiwei Wei (Huawei Technologies、中); Q9/17副ラポータ
- Framework Working Group (フレームワーク)
  - Tony Nadalin (IBM、米); Higginsプロジェクト関係者
  - Amardeo Sarma (NEC、独); Daidalosプロジェクト関係者、元SG10議長
- Living List and Lexicon Working Group (他の活動調査および用語集)
  - Mike Hird (英); 商務省のコンサルタント; 用語集担当
  - Kaliya Hamlin (Identity Woman、米); Open Space担当のコンサルタント、他団体の調査担当
  - Karen Mulberry (Neustar, 米); SG2関係者

FG-IdM: ユースケースWG

- ユースケースを集めて分析し、以下の分野についてその問題の概要、基本的な情報の流れを示したダイアグラム、必要とされる要求条件と能力、既存の解決手法、本FGが取り組むべき既存の手法の抜け(gap) を記述
  - ID資源のディスカバリ
  - ID資源のフェデレーション間・Circle of Trust間相互運用性
  - 情報交換に用いる機構の相互運用性
  - IDの確からしさの尺度の相互運用性
  - 透明性と通知
  - 物の管理との統合
  - ID管理のセキュリティとアイデンティティ・パターン
  - トークンの変換
  - 静的なトラストモデルと動的な選択
  - 権限委譲
  - メタデータモデル
- 実際には、最初の7項目のみ作業が進んでいる
- 第3回会合(5月)で完成予定だったが、その後の電話会合でも完全には完成できず、第4回会合に持ち越し。第4回会合後は特別な理由がない限り改変しない予定。本分析は要求条件やフレームワークの議論のベースになるため

FG-IdM: 要求条件WG

- ユースケースの分析と、法的な枠組みに基づき下記を作成
  - 各種IdMに共通な要求条件
    前提とするアーキテクチャモデル、プロビジョニング、ディスカバリ、IDプロバイダ間やプロバイダのフェデレーション間での相互運用性、監査、脅威とリスクの軽減、パフォーマンス、信頼性、可用性
  - 要求条件を実現する上で現在欠けているソリューション
    共通的なIdMアーキテクチャモデルとIdMレイヤ、グローバルなディスカバリ、グローバルなIDサービスの相互運用性、グローバルなID保証 (identity assurance) の相互運用性、透明性と通知、オブジェクト管理との統合、異なる法制度間での要求条件の違いの調停
- 現在は目次のみ。次回東京会合で中身が議論される見込み
  - 上記目次内容は、エディタが独自に作成したドラフトであるため、今後大幅に変わる可能性が少なくない

フレームワークWG

- ユースケース分析に基づき、IdMのアーキテクチャや必要な能力を分析、記述
- まだユースケース分析が完了していないためペンディング中
  - 第1回会合のフリーディスカッションをまとめたメモのみ
- アーキテクチャ
  - 各種IdMフレームワーク間でのディスカバリ、ID情報交換等の相互運用性に配慮つつ機能ブロック図を作成
- 各種IdMフレームワークの不足 (gap) を分析し、必要な機能を記述。必要な機能としては下記を想定。
  - 典拠のあるディスカバリやID情報の交換（保証の尺度を含む）
  - エンティティの証明書、識別し、属性やバインディングなど
  - IDプロバイダやプロバイダのフェデレーション間での特権管理の相互運用性
  - ID管理に伴う脅威とリスク、およびその軽減策

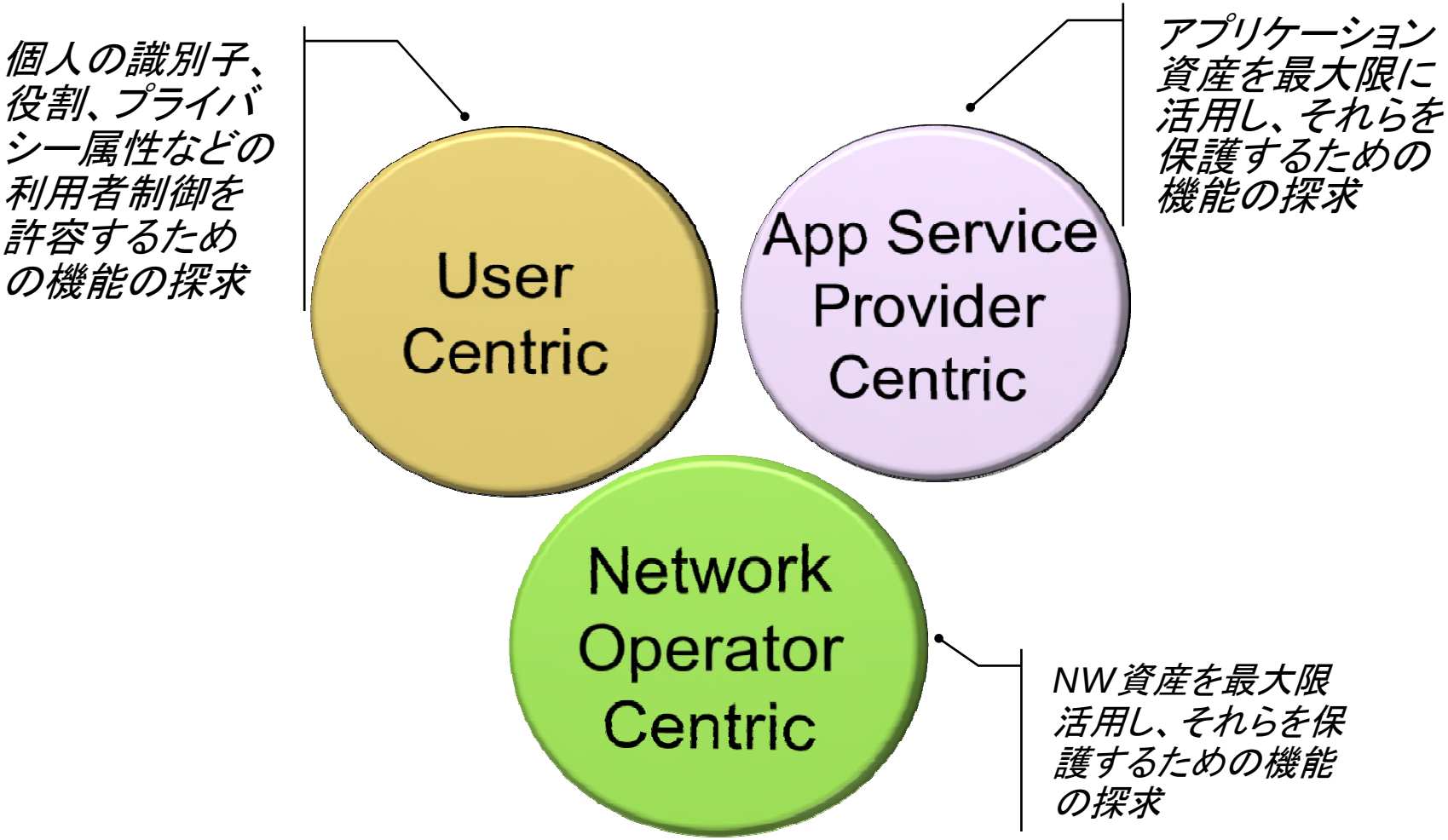
Lexicon and Ecosystem WG

- 用語の定義 (lexicon)
  - 定義が合意できた用語(terminology) と合意できていない用語 (lexicon) についての文書を作成

- 他のID管理の団体との関係を整理 (ecosystem)
  - 現在調査済の団体: ITU-T, 3GPP, IETF, ISO, Liberty Alliance, OASIS, OMA, W3C, ETSI TISPAN, FDIS, Guide, Higgins, その他各種業界団体など26団体

ユースケースとギャップ分析（1/7）

Current View of IdM Landscape



ユースケースとギャップ分析（2/7）

Current View of IdM Landscape

- User-centric
  - エンドユーザ視点でこれまで開発されたIdMのモデル、及びこれらのエンドユーザのための最適化
- Application-centric
  - アプリケーションの要求事項のために最適化されたIdMモデル（例：アプリケーションリソースへのアクセス保護）
  - 歴史的に、企業ユースケースによって推進されているIdMの実装 (e.g., SAML, Shibboleth, WS-Federation)
  - しかしながら、これらの実装はその他の広い利用に拡大され、カスタマイズされ得る。

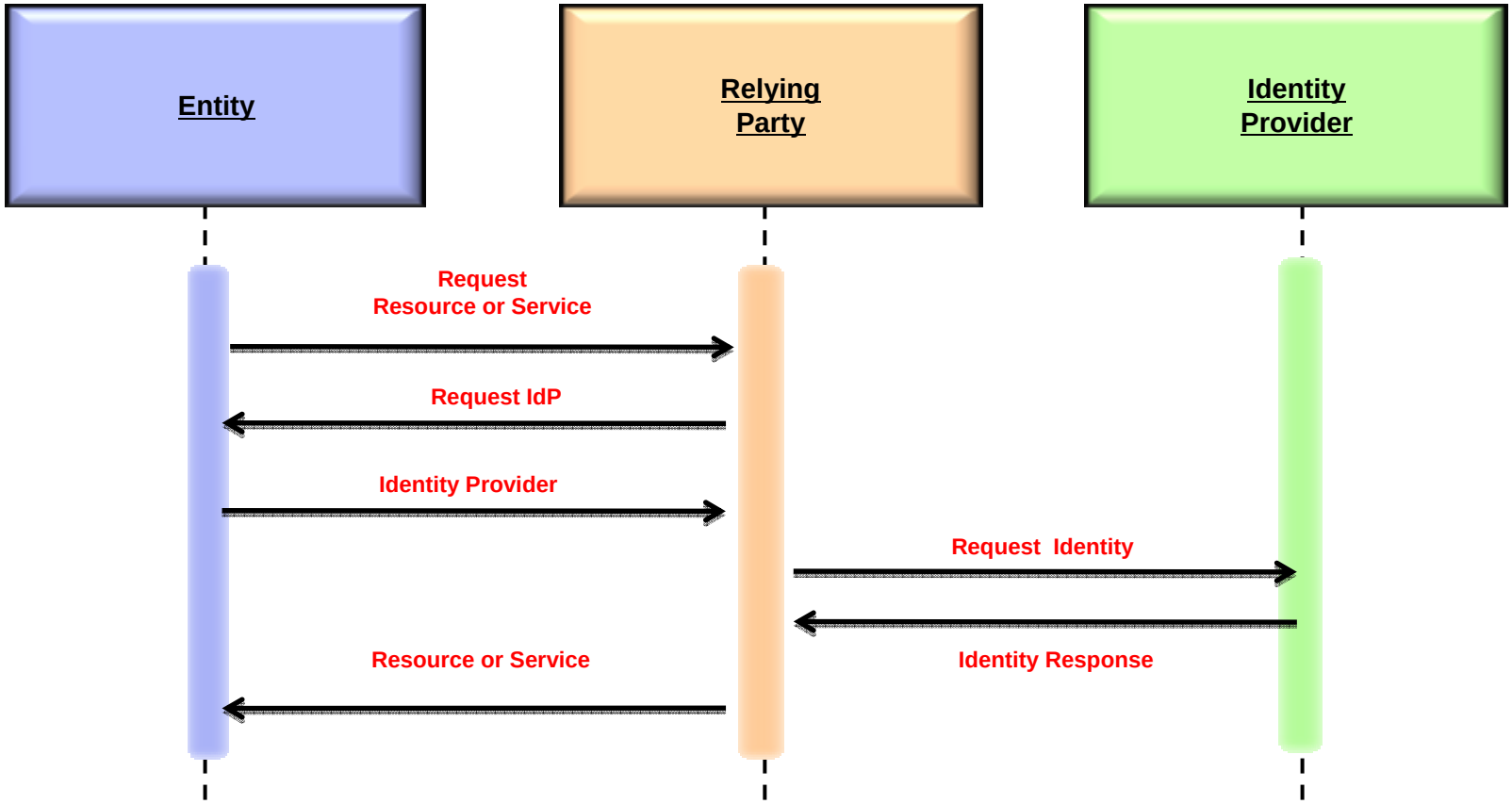
ユースケースとギャップ分析 (3/7)

Current View of IdM Landscape

- Network-centric
  - ネットワークやネットワーク提供者のために最適化されたIdMモデル (e.g., NGN providers and operators)
  - NGNのための、ネットワークや機器依存したものに焦点が当てられている。ここで、サービスの詐欺や窃盗などの点も考慮している。
- この3つのモデルの境界は曖昧であるが。
  一般に:
  - どのようなIdMの実施(配備)では、この3つのモデル(user, application, network)の要素が典型的に含まれている
  - どのような既存のIdMの実施においても、これらの3つのモデルに沿った形で具体的に配備(実施)できる。

ユースケースとギャップ分析（4/7）

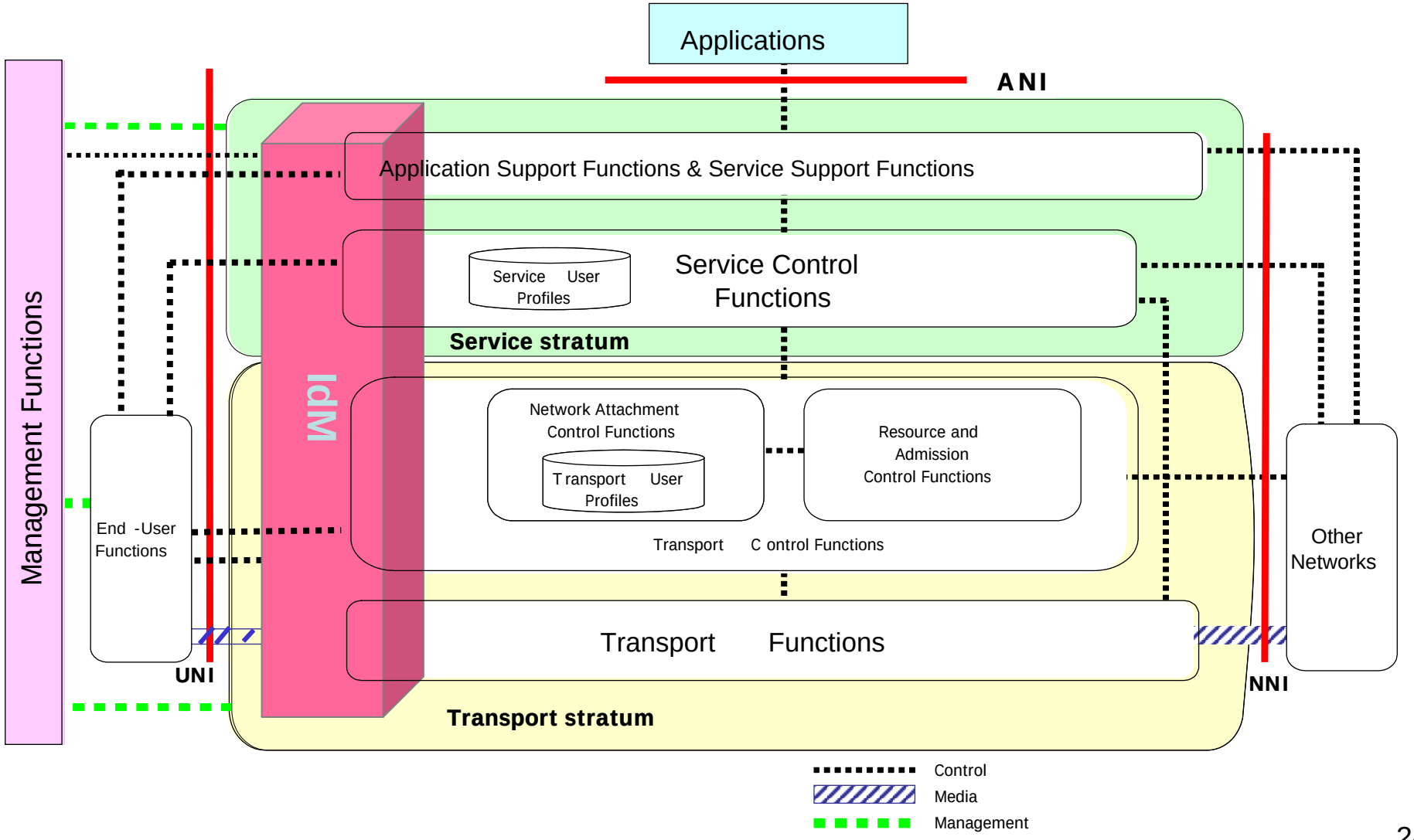
General IdM Architectural Model



- IdM 検索レスポンスメカニズムは、良い構造にて構築されることが望ましく、すでに公知または関与する事業者が知ることができるプロトコル及びプロファイルを用いることが望ましい。

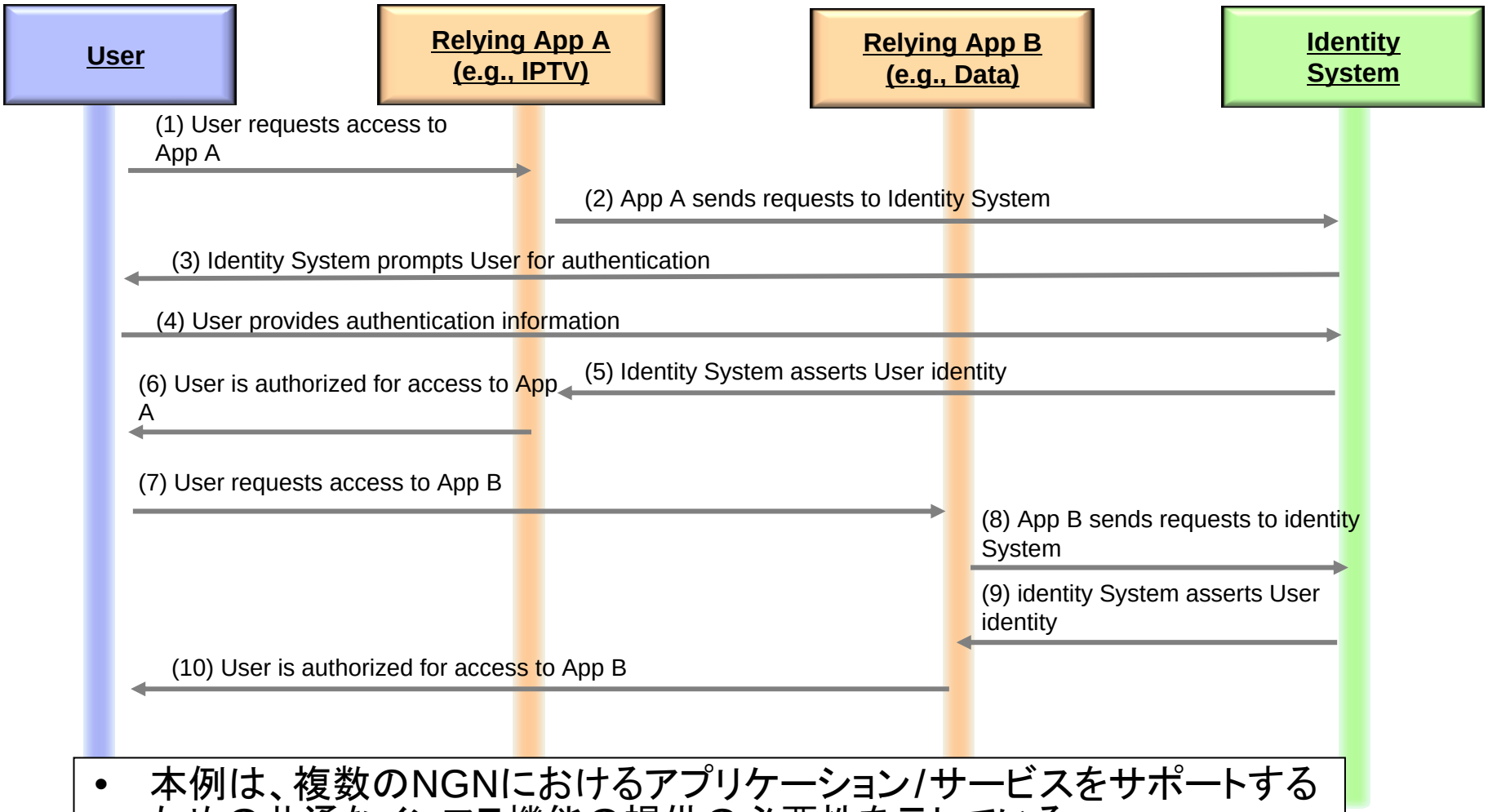
ユースケースとギャップ分析（5/7）

Integration of IdM in NGN Architecture



ユースケースとギャップ分析（6/7）

ユースケース例：NGNにおいて複数アプリケーションをサポートするための共通のIdMシステム利用

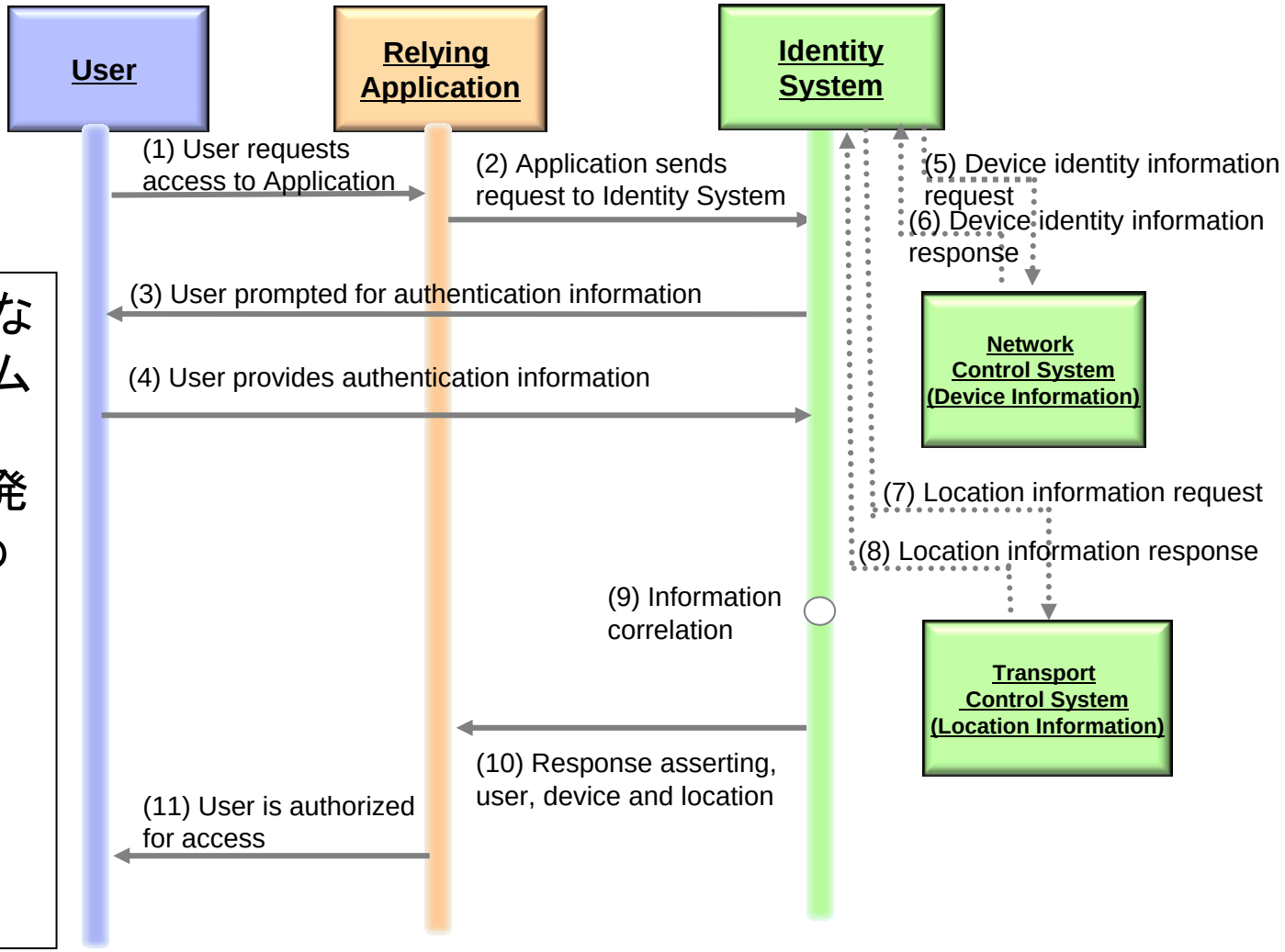


- 本例は、複数のNGNにおけるアプリケーション/サービスをサポートするための共通なインフラ機能の提供の必要性を示している。

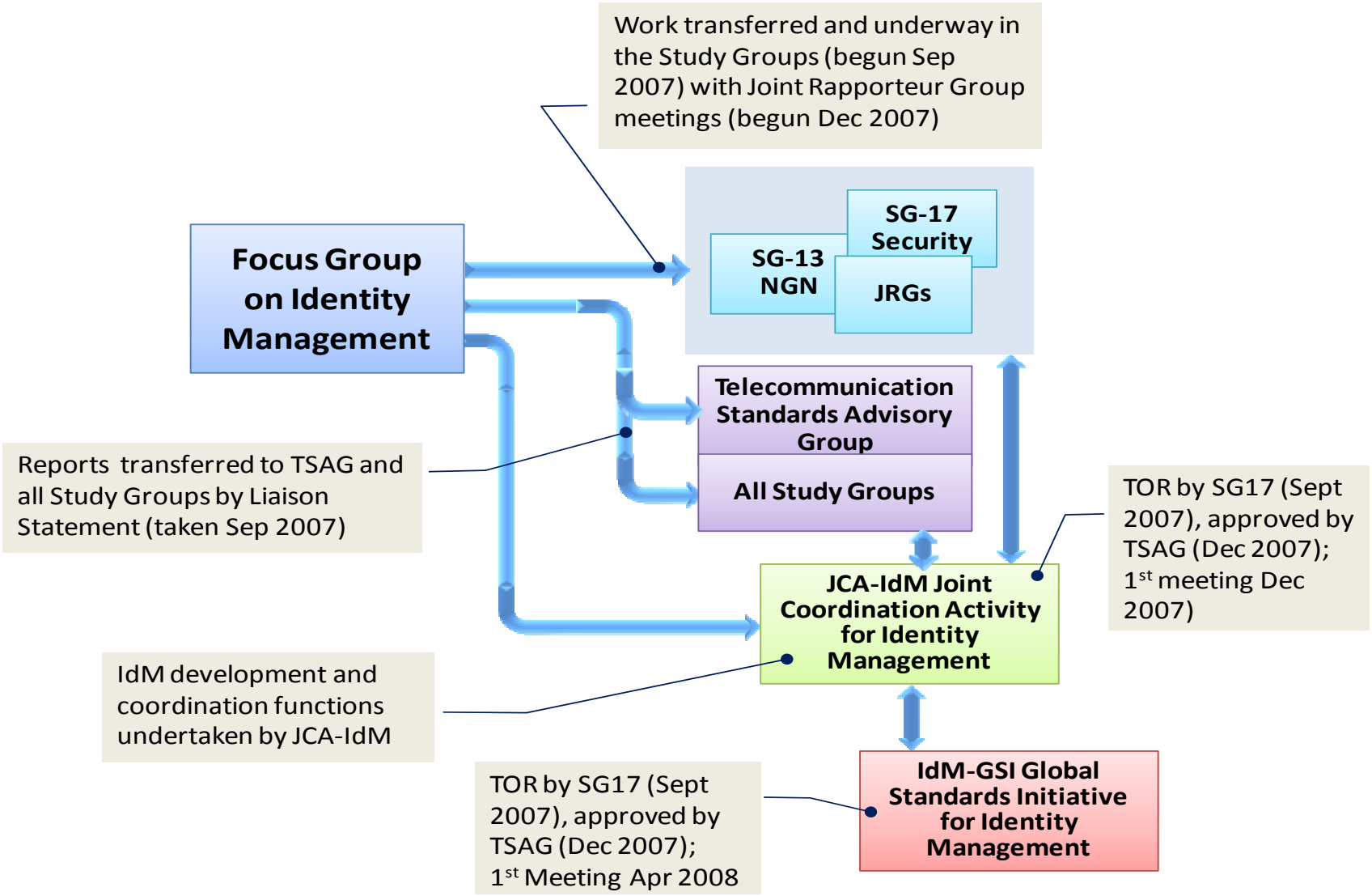
ユースケースとギャップ分析（7/7）

ユースケース例：通信レイヤを跨る情報の収集

- NGNにおける異なるレイヤ、システムに置かれているIdentity情報を発見、収集するための例示



ITU-T における今後の活動



今後の展望

技術的な重要課題として、アクセス管理（制御）を含めた、Identityの管理に関わ
技術が注目されており、ITU-T、及びISO/IECで精力的に取り組まれつつある。

＜標準化の方向＞ → 今後の認証基盤の確立に影響

- **アイデンティティ連携**
  パートナ間でアイデンティティ情報を関連付け
- **認証連携**
  組織をまたがるシングルサインオン
- **（一括）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属性情報の共有

IdM技術は、今後のいろいろな技術と何らかの関係を保有していくことは
間違えないと考える。

Thank you for listening Q&A