プライバシ保護のためのアーキテクチャ

7

小松文子 日本電気（株）
共通基盤ソフトウェア研究所

プライバシ保護技術に関する要素技術の研究とともに，実ビジネスの局面において，いかに利用し適用するかを明らかにするシステムアーキテクチャの研究が必要とされている．科学技術振興調整費による「セキュリティ情報の分析と共有システムの開発」プロジェクトでは，アイデンティティアクセス管理の領域に対して，プライバシ保護，セキュリティ保全，コンプライアンスの３つの観点から，情報のライフサイクル，プロセスモデルなどを分析しシステム要件を導出し，プライバシ保護システムとしてのアーキテクチャを策定した．このアーキテクチャでは信頼ある，ID 管理，属性管理および通信基盤のそれぞれの役割，機能および相互作用を定義している．本稿はこのプロジェクトの成果を紹介する．

背景

経済協力開発機構（OECD）は，1980 年に図 -1 に示す個人情報 8 原則を定めた．個人情報を処理するもの，と個人情報と個人との関係を表し，個人情報は個人の意思によってその利用目的が制御されると定義し，そのために関与者（主体や組織）への必要な原則を課す．一方国内では，OECD 8 原則などを基礎に 2003 年に「個人情報の保護に関する法律」が制定されるとともに，プライバシ保護を実現するシステムが強く要求されている．

本稿の構成は以下のとおりである．まず検討対象とした領域を明確にし，検討方針を示す．次に検討方針に基づき，対象領域における情報やプロセスに対するプライバシ保護要件を分析し，設計したプライバシ保護システムアーキテクチャを概説する．

1．収集制限の原則
　合法的な手段により入手し利用者への通知・同意を得る
2．データ正確性の原則
　個人情報は利用目的に即したものである
3．目的明確化の原則
　利用目的に必要な範囲で正確・完全・最新である
4．利用制限の原則
　要求された目的以外で利用してはならない
5．安全保護の原則
　紛失・破壊・修正・開示等の危険に対し，合理的な安全保護措置が必要
6．公開の原則
　個人データにかかわる開発・実施・政策は一般に公開される
7．個人参加の原則
　自己データの存在を利用者がいつでも確認できる
8．責任の原則
　管理者は上記を全うする責任を持つ

図 -1　OECD の個人情報 8 原則

プライバシ保護を必要とする領域

近年センサ技術の高度化等により，多くの「もの」が IT 情報システムにおいて識別可能となってきた．たとえば，車体，部品，商品などに IC チップを付加してその動きを追跡することが可能である．人間に対してもその振る舞いなどを観測し，統計を分析することで本人を識別することが可能となる場合もある．このような領域をコンテキストアウェアネス領域と呼ぶ．一方，個人がなんらかの組織に属し，登録され，サービスを受ける環境において，個人情報が管理されるアイデンティティ＆アクセスマネジメント（以降 IAM と呼ぶ）の領域においてもプライバシ保護が必要とされる．図 -2 にプライバシ保護が必要とされる領域について図示した．本稿では，後者の領域を対象とする．

IAM 領域は，従来トリプル A（AAA（Authentication, Authorization, Accounting））と言われた領域で，利用者の認証，権限管理と責任性を主な提供機能とする IT 領域であった．近年，本領域には，組織間連携，企業間連携が想定され，複数の組織などが相互に連携するための技術である ID 管理，連携，認証連携，サービス連携などを含み，IAM として呼ぶことが多い．これらの連携

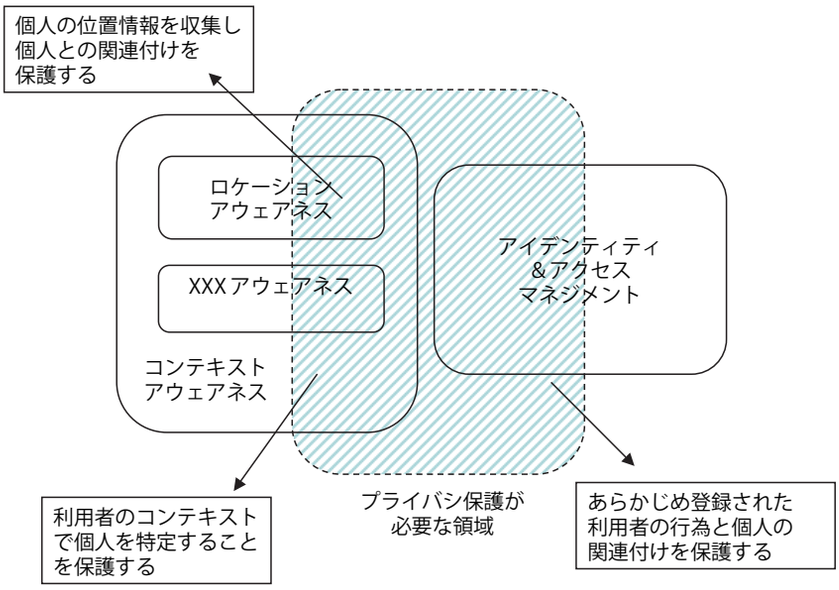

図-2 プライバシ保護が必要とされる領域

技術により利用者は複数の組織にまたがったサービスを受けることが可能となるが，結果として，プライバシ情報の拡散についての対策が大変重要な課題となっている．

アーキテクチャ検討のアプローチ

IAMにおいて利用者がサービスを受けるまでのプロセスとプライバシ情報ライフサイクルに対して，以下の3つの観点，すなわち①プライバシ保護②セキュリティ確保および③コンプライアンスの各観点からシステム要件を導出する．各観点について，以下に簡単に述べる．

■プライバシ保護の観点

ここで述べる4つの要件は，従来プライバシ保護の要件といわれてきた．これらすべての要件が必要ではなく，たとえば匿名性や偽名性は，システム要件より選択することになる．また，匿名性はリンク不能性，観察不能性を実現する要素になる．

- 匿名性 (Anonymity)
  ある者が，一意に識別されない状態．利用者が自身を識別可能にする身元情報を開示せず（あるいは開示されず）に，情報やサービスの利用ができることを保証する．
- 偽名性 (Pseudonymity)
  利用者が自身を一意に識別可能にする身元情報を公表する（あるいは公表される）ことなしに，情報やサービスを利用できる．しかし，その利用に対して責任があることを保証する．リンク不能性 (Unlinkability) を伴わない弱い匿名性 (Anonymity) といえる．
- リンク不能性 (Unlinkability)
  複数の情報をリンクすることができない状態である．たとえば，クライアントとサーバ間で送受信されるメッセージが，その盗聴者にとって1つのトランザクションとして認識できないような状態である．複数の情報やサービスを利用した場合に，第三者がそれらの利用の相互の関連性を見出せないことを保証する．
- 観察不能性 (Unobservability)
  情報そのものやサービスの利用が他人に観察されないようにすることである．

以上に加えて，追跡性（Traceability）を必要とする場合がある．追跡性は，プライバシ保護のもとになされた事実に対して後日そのプライバシ保護情報を開示し利用者などを特定できることである．

■セキュリティの確保

保護すべき情報資産が存在する場合，この情報資産に対して可用性，機密性，完全性を保つことがセキュリティ対策としての目的[☆1]である．プライバシ保護システムにおいても当然個人情報に対するセキュリティの確保が必要と考えられる．

- 可用性（availability）
  認可された利用者が，必要なときに，情報および関連する資産にアクセス可能とすること．
- 機密性（confidentiality）
  権限のある（authorized）者だけが情報にアクセスできること．
- 完全性（integrity）
  情報および処理方法が，正確であることおよび完全であることを保護すること．

■コンプライアンス要件

OECDの8原則，および国内の個人情報の保護に関する法律を考慮し，以下の3点にコンプライアンス要件を集約した．括弧内は，該当要件によって満足するOECD個人情報8原則の番号である．

①利用者によるプライバシ保護ポリシの策定と実行可否

☆1 ISMS認証基準 Ver.2.0 (JIP-ISMS100-2.0)

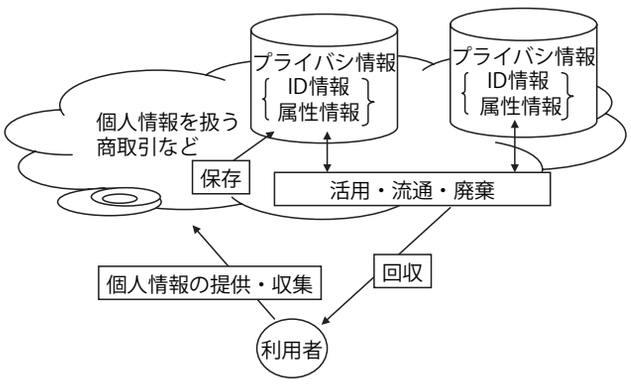

図 -3　プライバシ情報のライフサイクル

ライフサイクル	要件と対策
登録・収集	・ID の安全性対策（例：仮名 ID，匿名 ID の使用など）
活用・流通	・ネットワークの安全性，ネットワーク発信者の匿名化 ・利用者が参加するポリシ作成と実行
保存	・正当な利用者の認証およびアクセス管理，権限管理などによる情報漏えいを防ぐ ・暗号化などによる秘匿
廃棄と回収	・廃棄時個人情報が残存しない対策 ・個人情報を回収することは現実では大変困難で，提供した個人情報を追跡し，これを回収するメカニズムが必要

表 -1　プライバシ情報のライフサイクルと要件および保護対策

判断(2，3，4，7)
②利用者とサービス提供者間の合意形成(1，2，3，4，6)
③管理・保存者における情報保全(2，3，5，8)
個人と個人情報扱い者間において，ポリシをいかに合意し(②)，いかに実行(①)に移すかという点が重要となる．また，情報漏えいなどのリスクを防ぐ情報保全③が必要である．

プライバシ情報のライフサイクル

利用者がサービスを要求し，サービスを受ける場合のプライバシ情報のライフサイクルを図 -3 に示す．各ライフサイクルにおいて 3 つの観点（プライバシ保護，セキュリティ確保，コンプライアンス）からシステムへの要件を導出し，対応した保護対策を表 -1 に示す．

サービスモデルとプライバシ保護

利用者が特定のサービスを得るまでのモデルにおける関与者と関連情報を示す（図 -4）．図 -4 に示す用語について以下に定義する．

- 利用者
  プライバシ情報を保護して，サービスを利用したいと希望するユーザ
- CSP（クレデンシャル☆2 サービス提供者）
  利用者認証に利用するためのクレデンシャルを保証し，検証するために必要な処理を提供するもの
- クレデンシャル(Credential)
  利用者認証にて，利用者との結びつきを確認するために使用する情報
- AA：Attribute Authority（属性オーソリティ）
  属性情報を保存し，必要に応じて属性証明書を発行し，内容を保証する
- AC：Attribute Certificate（属性証明書）
  属性情報の内容について AA が保証した情報
- SP（サービス提供者）
  利用者の要求に対して，サービスを提供する．必要に応じて利用者認証，属性認証を行い，アクセス制御ポリシに従ってアクセス許可，不許可を判断する

☆2 クレデンシャルには，他にパスワード，ワンタイムパスワードなどがある．

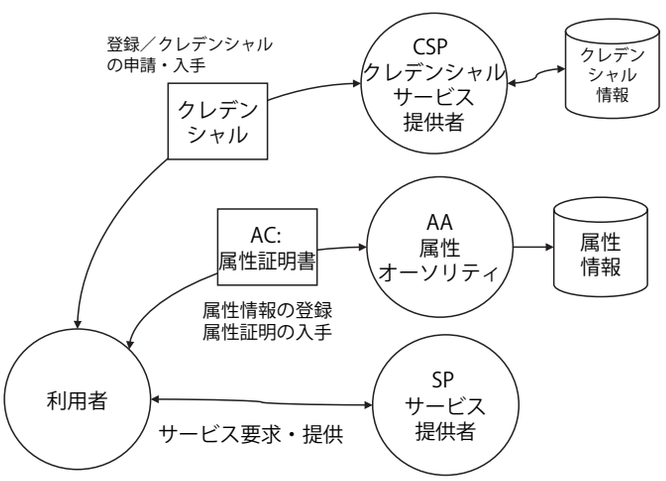

図 -4　利用者がサービスを受けるまでの関与者と情報

■サービスプロセスとサービス形態

サービスモデルを利用者とサービス提供者との関係の観点から単独のサービスモデルと連携サービスモデルに分類する．単独のサービスモデルについては，個々のプロセスに対するシステム要件を分析し，連携サービスモ

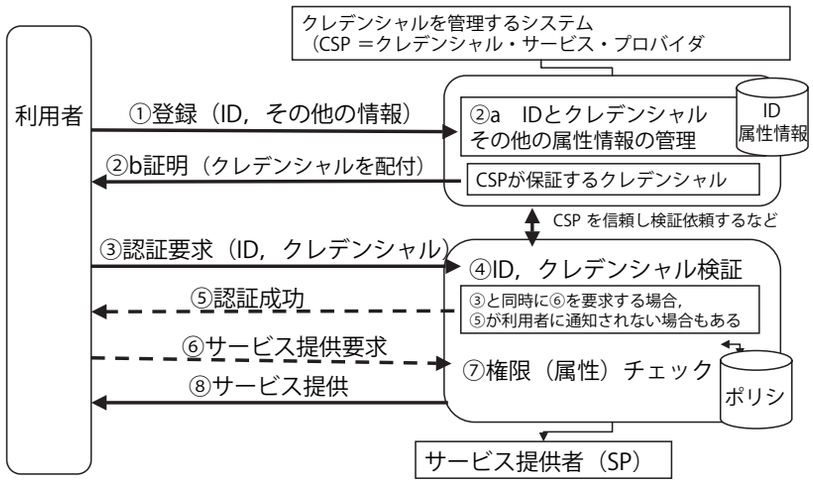

図 -5 単独のサービスプロセス

デルでは，連携要素間の関係について分析する．

■サービスプロセスとサービス形態

(1) 単独のサービスモデル

利用者と SP が 1 対 1 であるときのサービスプロセスは以下に示す①〜④のステップがあると考えられる（図 -5）．

①登録（ID 化）

利用者がサービスを受ける前に登録し，識別子を得ること．同時に本人認証や属性を証明するためのクレデンシャルや属性証明書の証明（②で示す）を受ける場合が多い．

②証明（Certification）

ID，または属性に対して内容を証明すること．公開鍵認証局，属性認証局などの第三者信頼機関（TTP：Trusted Third Party）が発行する公開鍵証明書，属性証明書などで表す．これらの証明書はクレデンシャルの 1 つである．

③認証（Authentication）

利用者認証は，利用者が提示したクレデンシャルを検証することで，クレデンシャルと本人の結びつきが正しいと検証できる場合認証が成功する．たとえば，公開鍵証明書の場合，検証者が信頼した認証局が証明書に署名していることを証明できると，そのクレデンシャルの内容を信用でき，そのクレデンシャルを本人が提示していることを共有する秘密情報などを確認できれば，相手認証が成功する．属性認証は，利用者が提示するクレデンシャルが属性を表す場合をいう．その利用者が正しく属性を保持していることを検証できるとき，属性認証は成功する．

プロセス	システム要件と対策
ID 登録	・登録情報と ID の安全な管理 ・匿名 ID，偽名 ID の利用
証明	・本人を秘匿する匿名証明書 ・属性のみを証明する属性証明書 ・証明書発行情報に対する安全な管理
ユーザ認証	・匿名 ID，偽名 ID の利用 ・ユーザ認証を行わない（属性認証のみ）
アクセス制御	・プライバシポリシの定義，利用者の参加 ・属性認証と属性情報へのアクセス管理
共通	・履歴情報に対する安全な管理

表 -2 プロセスとプライバシ保護対策

④権限管理（Authorization）とアクセス制御

エンティティ認証後，サービスを提供するために必要な権限や条件をアクセス制御ポリシに記述し，必要な権限を保持しているかを判断し，アクセスを許可または拒否する．エンティティ認証が不要の場合，属性認証のみで，アクセス制御の判断情報とする場合がある．アクセス制御判断は，利用者の属性やサービス側の属性を検証することで決定する．

表 -2 に単独のサービスモデルの各プロセスでのシステム要件対策を示す．特に，認証のプロセスにおいて，利用者認証するか（アクセス制御時に）属性だけを認証するかは，利用者またはサービス提供者からの要件による．利用者を認証する場合は，トレーサビリティ（追跡性）を確保する場合と考えられるが，利用者と保護すべきプライバシ情報である属性情報のリンク不能性，観察

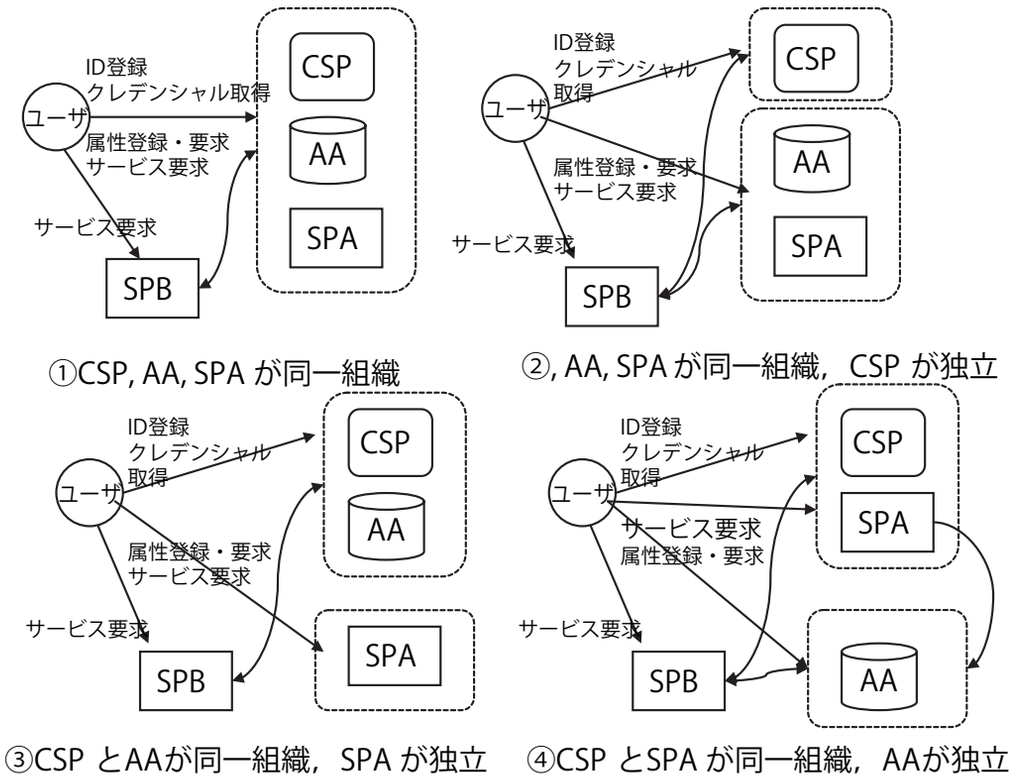

図 -6　サービス連携における構成

不能性を保証するための手段が必要となる．グループ署名技術はこの手段の 1 つとなり得る．属性認証の場合は，AC 発行において AA が追跡性を可能とする手段をとることが可能である☆3．

(2) 連携サービスモデル

複数の SP が連携し，全体として 1 つのサービスを構成するモデルである．サービスを連携させるため，ID 連携，認証連携のいずれかをとる場合が多い．連携時に必要な情報交換には，SAML☆4 アサーションを使用できる．CSP は認証事実を保証する情報を提供・保証する認証サービスを提供する．

特定の CSP に登録されている利用者が，複数の SP のサービスを要求する場合，SP はサービスに必要なクレデンシャルや属性情報を CSP や AA から得なくてはならない．CSP，AA，SP の関係を分類した（図 -6）．

① CSP，SP，AA がすべて同じ組織
② SP，AA を同じ組織（CSP は独立）
③ CSP と SP が同じ組織（AA が独立）
④ CSP と AA が同じ組織（SP が独立）
クレデンシャルサービスと属性サービスを提供するサービス基盤を，SP が利用する
⑤ CSP，SP，AA がすべて別組織の場合

いずれのケースにおいても，利用者が SP に対してプライバシ情報開示を望まない方式が要求される．したがって，CSP または，AA から SP へのやりとりを中心にシステム要件を検討する．SP は，単独のサービスモデルで述べたように，認証時にクレデンシャル，アクセス制御時に，権限情報（属性情報）を必要とする．複数の SP に対して利用者はなんらかのかたちで自分が登録された正当な権限を持つ利用者であることを宣言するが，SP にとってクレデンシャルは，CSP が保証していれば内容を検証する必要はなく，単に「認証済み」という認証状態を参照可能であればよい．また，属性認証だけで利用者認証を不要とするケースもある．次に，アクセス制御のための権限情報については，権限があるかを判断できる主体は SP であるから，サービスを提供する上で必要となる属性とともに，信頼ある属性情報（AC）として安全に受け取る必要がある．以上を考慮すると連携モデルにおけるプライバシ保護システムへの要件は，SP に対して信頼ある属性情報を安全に渡せることである．次に，必要な場合は，利用者の認証状態が信頼ある情報として参照可能であること，である．

なお，AA や CSP が集中管理されるような形態の場合は，セキュリティ確保の対策が必要である．

☆3　実用段階のシステムにおいて，属性証明書を発行する属性認証局の実装はほとんどない．
☆4　SAML：Security Assertion Markup Language．OASIS で規定された XML 上でのセキュリティ情報表現方式．

■プライバシ保護システムに必要な要件

これまで述べた分析により，プライバシ保護システムに対する要件を以下に導出した．

プライバシ情報のライフサイクル分析より

- 情報保全(情報漏えい対策)の確保
- 利用者によるプライバシポリシ設定・管理

サービスプロセス分析より

- 仮名 ID または匿名 ID の利用
- 属性認証(属性証明書)の利用
- アクセス制御ポリシとプライバシポリシの定義と利用者の参加
- 履歴情報の安全な管理

サービス連携モデル分析により

- SP，AA，CSP 間での属性情報の保持方法
- SP，CSP，AA 間のプライバシ保護情報の移動，活用制限
- 信頼ある通信路

が必要となる．

これらのうち，紙面の関係から，特に匿名認証と属性認証について述べる．

■属性認証の利用

特にサービス連携において属性認証がプライバシ保護システムに有効である．属性認証では，AA が発行する AC の識別子をもとに AA において利用者との結合が可能であるが，SP においては，属性のみを検証するため，リンク不能性を確保できる．また，SP は，特定のユーザ ID が何をしたかを観察することはできない(観察不能性)．ユーザ ID は SP に開示されないため，偽名性または匿名性を保つことができる．ユーザと SP 間では，プライバシ保護を実現できる．なお，AA において利用者と属性情報の結合情報を持つ場合には追跡性が確保されるが，保持情報に関する AA のセキュリティ要件を満たさなければならない．

■匿名 ID または仮名 ID の利用

匿名 ID には永続性がないため，SP において ID と属性との管理ができず，リンク不能性を実現できる．仮名 ID には，永続性が存在するため，仮名 ID と属性の管理が可能で安全に管理するしくみが必要となる．匿名 ID は，グループ署名を利用することでオーソリティにより ID を追跡性可能であるが，仮名 ID は，仮名 ID 管理者により保管した属性との対応をしなければ，トレースできない．匿名 ID は，SP に ID を開示せず，サービスを受けることができるが，サービスを受けるために必要な属性を管理するために，実名と配付した匿名 ID と属性の管理が必要となろう．

プライバシ保護システムアーキテクチャ

これまで述べた検討を元に，IAM 領域におけるプライバシ情報保護システムの基本設計を行いアーキテクチャ（図 -7）を策定した．複数のサブシステムから構成されるシステム構成とそれぞれの機能，役割，相互作用について定義した．

(1) 認証基盤

ID を証明する ID 認証機関と，属性を証明する属性管理機関(AA)の 2 つの信頼機関から構成される．

- ID 管理機関

  公開鍵証明書に代表されるクレデンシャルや匿名認証用グループ署名証明情報を発行する．グループ署名証明情報はグループ署名技術に基づく．クレデンシャルに公開鍵証明書を利用しない場合でも，システムコンポーネント相互接続時の相手認証や，正当性検証に利用することが可能なため，第三者信頼機関としての認証局から公開鍵証明書を入手することが必要となる．

- 属性管理機関 (Attribute Authority)

  利用者の属性情報を保管する．集中管理の脆弱性を防ぐため，複数の管理機関に分散して保管する場合もある．

(2) 通信基盤

認証基盤，サービス提供者，利用者の間で通信ネットワークを介した対話が行われる場合に使用される基盤である．対話に要求される秘匿性レベルに応じた通信ネットワークが必要とされる．次のような種類の通信が使用される．

- 通常通信

  通信路上を通過するメッセージの内容が守られない通信である．サービス要求の初期に，利用者とサービス提供者の間で発生するデータ通信に使用される．

- 認証を含む暗号化通信

  通信路上を通過するメッセージの内容が暗号化され，送信者と受信者以外には内容が理解できない通信である．受信されたメッセージ内容が，送信者によって作成されたこと，通信経路上で不正な変更が行われていないことを証明できる．インターネットにおける TLS/SSL を利用した通信に相当する．利用者やサービス提供者と各種信頼機関の間の通信に使用される．

- 匿名通信

  通信路上を通過するメッセージの送信者が識別できない (匿名化) 通信である．本通信は，onion routing などの匿名通信機能を持つネットワーク基盤で実現される．

(3) サービス提供者 (Service Provider)

利用者からの要求に対応して，サービスを提供する．サービス提供者は，利用者が提示する ID 情報や属性情

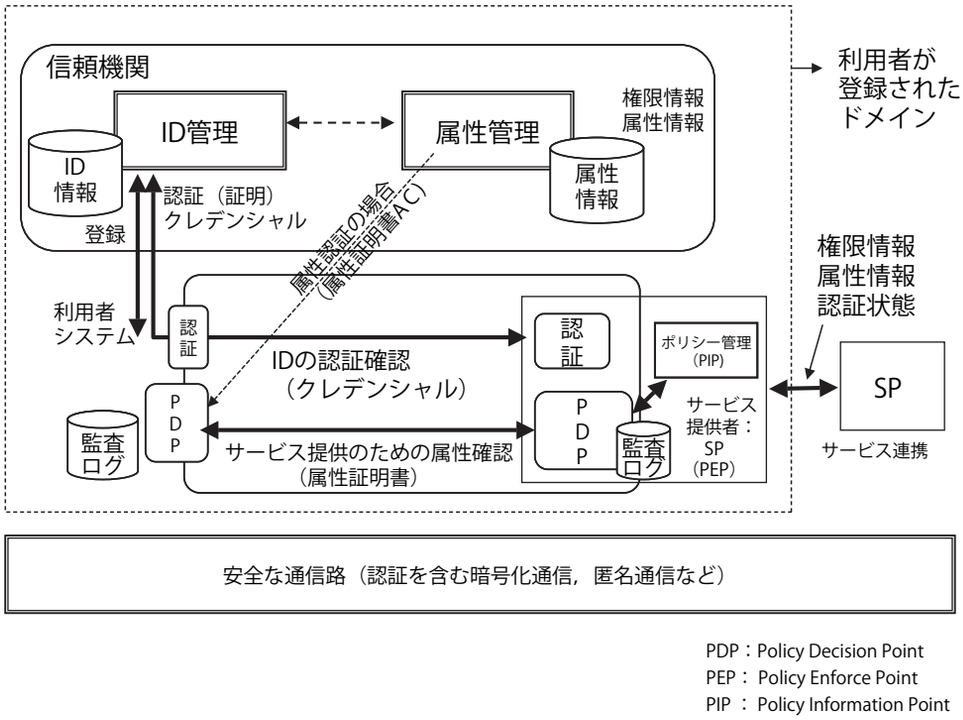

図 -7　プライバシ保護システムのアーキテクチャ

報と，サービス提供者自身のアクセス制御ポリシに基づいて，サービス提供の可否，提供レベルなどを決定する．この際，利用者がポリシに対して参加するために，利用者システム側のポリシ判断と連携する．

(4) 利用者 (User) と利用者システム

サービスの要求者である．ID 管理から配布されたクレデンシャルや，属性管理から配付された属性証明書をサービス提供者へ提示しサービスを要求し，消費する．サービス要求時，サービス提供者から属性情報の開示を求められた場合，それに応じて自身の属性情報を提示する．公開する属性情報は，プライバシポリシに基づき決定される．

課題

本研究では，要素技術としてのプライバシ保護技術をアイデンティティアクセス管理の領域におけるプライバシ保護システムとしていかに適用，利用可能かの検討を 3 つの観点（プライバシ保護，セキュリティ，コンプライアンス）より検討し，プライバシ保護システムアーキテクチャを提唱した．今後は，特に属性認証，匿名認証，および通信の匿名化に関する要素技術の実用化研究が望まれる．また，研究範囲外であったプライバシ保護と監査ログにかかわる研究や，コンテキストアウェアネス領域におけるプライバシ保護に対して本研究での成果の適用などが今後の課題と考える．

謝辞　本テーマ実行にあたって，筑波大学 岡本先生をはじめ，プロジェクトにおけるアドバイザリ委員および運営委員会の諸先生，プライバシ保護チームの研究機関の諸先生にご指導いただきましたことを感謝します．また，本稿を作成する際に協力いただいた，NEC システムテクノロジー（株）の岩西マネージャに感謝します．

参考文献
1) 属性認証ハンドブック, ECOM (Feb. 2005).
2) PRIME Architecture - Version 1, 03 August, 2005 PRIME PROJECT
3) SAML V2.0, OASIS (15 March 2005).

（平成 19 年 5 月 29 日受付）

小松文子　a-komatsu@ay.jp.nec.com
PKI 製品，サービスの開発およびセキュリティに関するコンサルテーション業務を経て，現在中央研究所にて PKI，ID 管理，認証・認可技術をはじめとしたセキュリティエンジニアリングに関する開発，研究に従事．