サイトを越えるサービス連携における認証・認可，プライバシ情報保護技術

斉藤嗣治[*1]　石井章夫[*2]

[*1] 日本電気(株)　[*2] 富士通(株)

近年，電子政府や電子商取引などの分野では，サービス利用者にとって利便性の高いワンストップサービスを実現するために，インターネット上に存在するさまざまなサービスを連携させ，複合的な Web サービスとして動作させることが求められている．

現状では，個々のサイトがサービス単位で認証・認可，プライバシ情報を扱っており，運用・管理ルールが統一されていない．これら複数サイトのサービスを連携させる際には，個々のサイトでの運用・管理ルールによる利用者の利便性が低下する可能性，サービス管理者の煩雑な管理作業が増大する可能性がある．

本稿では，これらサービス連携における認証・認可，プライバシ情報の扱いの課題を解決することで，より付加価値の高いサービスを提供するために開発した技術を紹介する．

サービスの認証，認可，プライバシ情報の扱いの位置づけと，サービス連携における課題

現状，インターネットの普及に伴い，B2C（企業と一般消費者の取り引き），B2B（企業間取り引き），G2C（行政と住民の手続き）にて，文具などのオフィス用品やパソコン，書籍などの物品販売から，航空チケットの手配やホテルの予約サービス，部品や原料などの調達，行政手続きなど多岐にわたる分野で，インターネット上のサービスが提供されている．インターネット上のサービスでは，不正なサービス利用者を排除し，サービスで利用するプライバシ情報を正しく提供するために，サービス利用者が本人であることを判断し証明する「認証」を行い，プライバシ情報を扱う際には，個人情報保護法の配慮をしつつ，プライバシ情報の漏洩を防止し，サービス利用者が要求するサービス処理を行う際には，サービス処理の使用許可をサービス利用者の利用権限に基づいて判断する「認可」をしている．これら，認証・認可の処理は，サービスを提供する個別サイトの運用・管理ルールに基づいているのが現状である．

そこで，複数のサイトで提供されるサービスを連携し，サービス利用者に付加価値の高いサービスを提供する場合における，「認証」「プライバシ情報の漏洩防止」「認可」の現状と課題を示す．

(1) 異なるサイト間の認証

サービス利用者の「認証」には，さまざまな手段が提供されている．その認証手段には，ID・パスワードによる認証，より認証レベルを強化した IC カードを利用した認証や，公開鍵証明書を利用した認証などさまざまである．IC カードを利用するには IC カードリーダというハードウェアが必要であるため，実際には特定のサービスでしか利用されておらず，ID・パスワードによる認証が主流である．

これらサイトごとにさまざまな認証手段を提供するサービスを連携させる場合，次の点を考慮して，サービス利用者の利便性を低下させないようにする必要がある．

- サービス利用者に統一的な認証手段を提供可能にする．
- 連携するサービスごとにサービス利用者をインタラクティブに認証することなく，サービス利用者の 1 回の認証で複数のサービスを利用することを可能にする．その際，一度認証した認証情報を連携するサービスへ引き継ぐことで複数サービスでの認証を可能とする．ただし，この認証情報で，個々のサービスに登録されているユーザ情報（プライバシ情報）を名寄せにより統合することを防止できるようにする．

(2) 異なるサイト間のプライバシ情報の交換

サービス利用者は，ユーザ登録にてプライバシ情報をサービス提供者へ提供する必要がある．提供するプライバシ情報には，物品の送り先となる住所・氏名，支払い

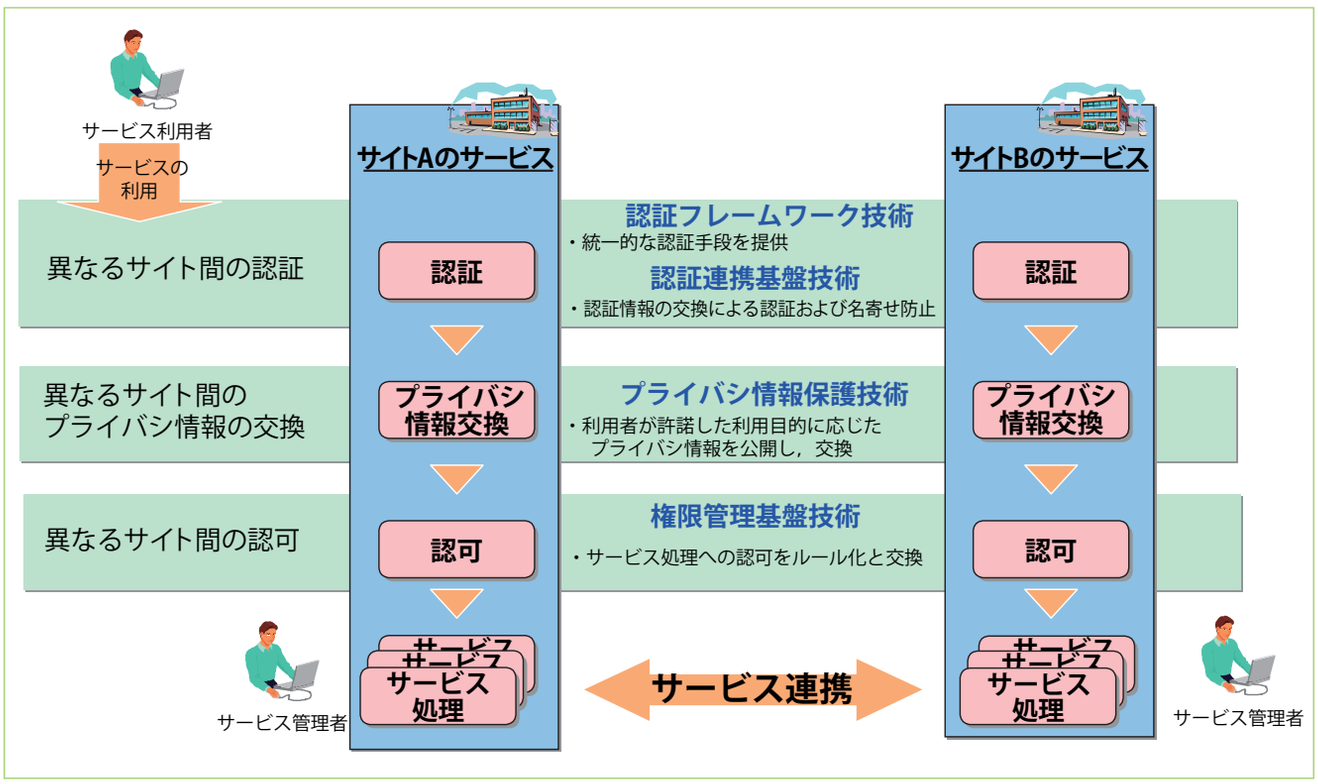

図 -1　サービス連携時の認証，プライバシ情報交換，認可の位置づけ

の決済情報，サービス提供者がマーケティングに利用するための情報となる性別，生年月日，嗜好などが含まれる．サービス提供者は，ユーザ登録時に発行したユーザ ID およびパスワードから，サービス利用者を識別，認証することによって本人確認を行い，プライバシ情報を利用してサービス利用者により魅力的なサービスの提供を行っている．

このユーザ登録では，個人情報保護法の基本原則に基づき，プライバシ情報の利用目的の特定と，本人の同意を基本としているため，サービス利用者にとって，サービスごとにプライバシ情報の利用許諾を与える必要があり，このプロセスが負担となっている．

複数サイトのサービスが連携する場合，サービスの提供，およびサービスの連携の局面において，サービス提供者におけるプライバシ情報の利用目的と，サービス利用者のプライバシ情報の利用許諾意思との間の調整を行い，サービス利用者の意図したプライバシ情報の公開のみを保証することが必要である．

(3) 異なるサイト間の認可

サービス利用者の「認可」では，サービス提供者がサービス利用者に対してどのような権限があるのかを管理し適切なサービスを提供しなければならない．サービス提供者は，サービス利用者のアクセス制御情報（権限情報）の管理を実施しているが，現状，サービス利用者の権限情報は，サービス利用者の ID 情報に関連付けられており，サイト内のプラットフォームごとアプリケーションごとに個別に管理されている．このため，サービス提供者は，サイト内で利用者の登録，削除の操作が発生するたびにそれに伴う ID 情報と権限情報のマッピングを手作業で行っている状況である．

複数サイトのサービスが連携する際の認可でも，他サイトからのサービス利用者に対しても適切なサービスを提供することが必要である．サービス提供者は他サイトのアクセス制御に対しても考慮しなければならず，複数のアプリケーションで使用される利用者の権限情報を一元的に管理する手法，サイトをまたがった利用者に対しても権限情報の整合性を維持する手法が必要となる．

これらの課題を解決するため，本稿では**図 -1** に示す異なるサイト間の認証，異なるサイト間のプライバシ情報の交換，異なるサイト間の認可に必要となる技術を紹介する．

- 異なるサイト間の認証では，統一的な認証手段を提供できる「認証フレームワーク技術」，サービス間の認証情報の交換による認証および名寄せを防止する「プライバシ保護型認証連携基盤技術」
- 異なるサイト間のプライバシ情報の交換では，利用者が許諾した利用目的に応じたプライバシ情報の公開，交換を行う「プライバシ情報保護技術」
- 異なるサイト間の認可では，サービス処理への認可をルール化と交換する「権限管理基盤技術」

統一的な認証手段を提供可能とする「認証フレームワーク技術」

認証フレームワーク技術は，異なるサイト間の認証において，連携するサービス同士で認証手段を統一するために，個々のサービスを柔軟な認証手段に対応可能にする．

従来の認証手段は，個別に開発されたアプリケーションやサービスが用意している方法に基づいており，統一的な認証手段を提供する技術が存在しなかった．そこで，次の４つの認証手段を切り替えたり，変更するためのメカニズムとして認証フレームワークを考案した．

- ID/ パスワード
- IC カード（PKCS#11）
- 公開鍵証明書（PKCS#12）
- Windows 提供のもの（Crypto API）

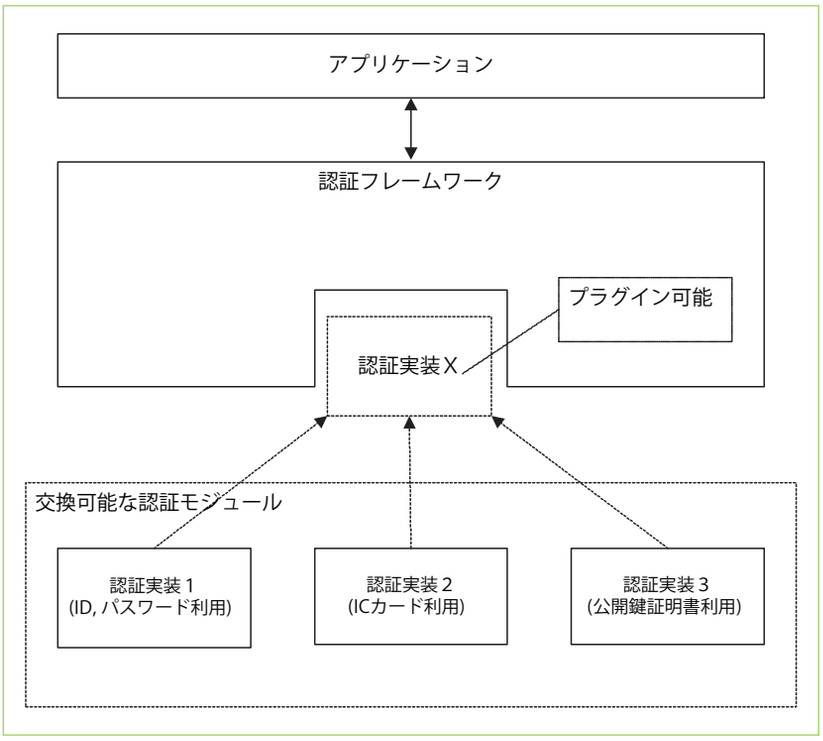

図 - 2　認証フレームワークのメカニズム

図 -2 は，その認証フレームワークのメカニズムを示している．アプリケーションが認証を使用する際に準拠すべきアプリケーションインタフェースを規定し，このフレームワークに準拠した認証手段の実装（認証実装 X）を交換するだけで対応する認証方式を容易に変更することが可能となる．

このアプリケーションインタフェースとなる認証フレームワークは，Java の JAAS（Java Authentication and Authorization Service）という機構を用いて実現している．

サービス間の認証情報の交換による認証および名寄せを防止する「プライバシ保護型認証連携基盤技術」

プライバシ保護型認証連携基盤技術は，異なるサイト間の認証において，サービス間の認証情報の交換を可能とし（認証連携機能），認証情報による複数サービスに登録されているプライバシ情報の名寄せを防止する（名寄せ防止機能）技術である．

従来認証はさまざまな技術仕様により提供されていたことで，認証情報の相互交換をするには個々のケースで連携手段を開発する必要があった．開発して認証情報を交換することにより，プライバシ情報の名寄せが可能となってしまう課題があった．

（1）認証連携機能

サービス間の認証情報を交換可能とする「認証連携機能」を実現できる標準仕様としては，OASIS（Organization for the Advancement of Structured Information Standards）が策定した SAML（Security Assertion Markup Language） や，Liberty Alliance が策定した Liberty ID-FF（Identity Federation Framework），または，Microsoft などが中心となり策定した WS-Federation といった仕様があり，複数の類似な仕様が乱立している状態である．しかし，SAMLv2.0 は，Liberty ID-FF1.2 仕様がベースであり，また，WS-Federation と Liberty ID-FF 仕様の相互変換を可能とする仕様が作成されるなど次第に統一化が進んでいくものと考えられる．

認証連携機能では，仕様の包含関係などを考慮し，Liberty ID-FF1.2 仕様を中心とし，サービス連携時の認証情報の受け渡しについては，WS-Security を中心とし Liberty ID-FF1.2 に対応可能とした．

（2）名寄せ防止機能

名寄せを防止するには，他のサービスで提供される認証情報の伝播を防ぐ必要があり，認証用の ID を隠蔽することで情報の連鎖を切る方法が必要である．

名寄せ防止機能は，Liberty ID-FF1.2 仕様のうち，仮 ID や匿名 ID の機能を利用することで実現した．具体的には，サービス利用者に認証サーバ内で統一的な ID を発行し，サービスごとに異なる仮 ID を発行させる．認証サーバでは，統一的な ID および仮 ID の紐付けを行う．認証情報を交換する際，連携元のサービスは，認証サーバから異なる仮 ID を受け取り，連携先のサービスへ受

個人情報保護法に定める公開すべき項目	P3P
取得する個人情報の利用目的	○
当該個人情報取扱事業者の氏名または名称	○
利用目的の通知，開示，訂正・追加・削除，利用停止，第三者提供停止の求めに応じる手続き	○
当該個人情報取扱事業者が行う保有個人データの取扱いに関する苦情の申出先	○
認定個人情報保護団体の名称および苦情の解決の申出先	○
第三者提供を行う旨	○
第三者への提供を利用目的とすること	○
第三者に提供される個人データの項目	○
第三者への提供の手段または方法	×
本人の求めに応じて当該本人が識別される個人データの第三者への提供を停止すること	○
個人データを共同利用する旨	×
共同して利用される個人データの項目	○
共同して利用する者の範囲	○
利用する者の利用目的	○
当該個人データの管理について責任を有する者の氏名または名称	○
手数料の額	×

表 -1
サービス提供者が公開すべき項目と P3P の関係

け渡す．連携先サービスでは受け取った仮 ID を認証サーバに問い合わせる方式を考案した．これにより，仮 ID が割り当てられたサービス以外ではユーザを特定することができないため，名寄せを防止することが可能となった．

利用者が許諾した利用目的に応じたプライバシ情報の公開，交換を行う「プライバシ情報保護技術」

プライバシ情報保護技術は，異なるサイト間のプライバシ情報の交換において，連携するサービスごとにプライバシ情報の利用目的と，サービス利用者のプライバシ情報の利用許諾意思との間の調整を行い，サービス利用者の意図したプライバシ情報の公開のみを保証する技術である．

現状，Web サービスの世界では，プライバシ情報の取扱いに関する情報を利用者に開示するには，Web サイト上にプライバシポリシーを掲載する方法が一般的である．通常，プライバシポリシーは，人間の読める文書の形式で掲載されるものであるが，サービス利用者側のブラウザで機械処理を可能とすることを目的として，XML 形式で記述フォーマットを定めた仕様である P3P（Platform for Privacy Preferences）に従い提示する方法がある．しかし，**表 -1** に示すとおり，個人情報保護法と P3P で表現できる項目を比べると，P3P だけでは充足していないため，サイト上に人間の読める文書の形式で掲載するなどの対応を取る必要がある．

そこで，サービス提供者の利用目的と，サービス利用者の利用許諾意思を，それぞれ作成して保存しておき，両者があっているか判断することを特徴とするプライバシ情報公開技術を開発した．その機能要件について述べる．

（1）サービス提供者におけるプライバシ情報の利用目的ポリシーの作成機能

提供するサービスの内容と，サービスの提供の際に利用するプライバシ情報の内容，およびその利用目的を記述した，サービス提供者におけるプライバシ情報の利用目的ポリシーを作成し，サービスにおいて保存する（**図 -3**）．

（2）サービス利用者におけるプライバシ情報の利用許諾意思ポリシーの作成機能

利用するサービスの内容と，サービスの利用の際に利用を許諾するプライバシ情報の内容，およびその利用目的を記述した，サービス利用者におけるプライバシ情報の利用許諾意思ポリシーを作成し，保存する（**図 -4**）．作成したポリシーはサービス利用者の利用する端末，もしくはサービス利用者が信頼するプライバシ情報公開調整サービスに保存する．

（3）プライバシ情報の利用目的ポリシーと利用許諾意思ポリシーの調整機能

プライバシ情報の利用目的ポリシーと利用許諾ポリシー間の調整を行い，調整結果を返す機能である（**図 -5**）．ポリシーが適合すればプライバシ情報をサービス提供者に提供し，ポリシーが適合しない場合はプライバシ情報をサービス提供者に提供しない．調整は，プライバシ情報自体を保存しているサービス利用者の利用する端末，もしくはサービス利用者が信頼するプライバシ情報公開調整サービスで行う．

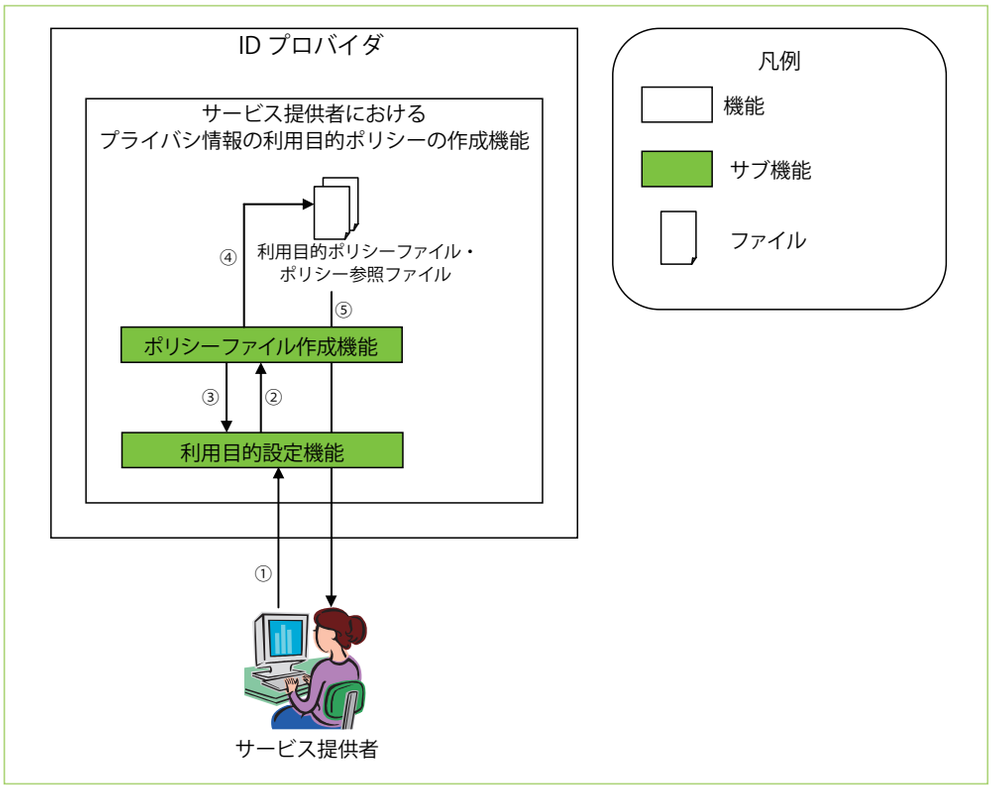

図 -3
プライバシ情報の利用目的ポリシーの作成機能

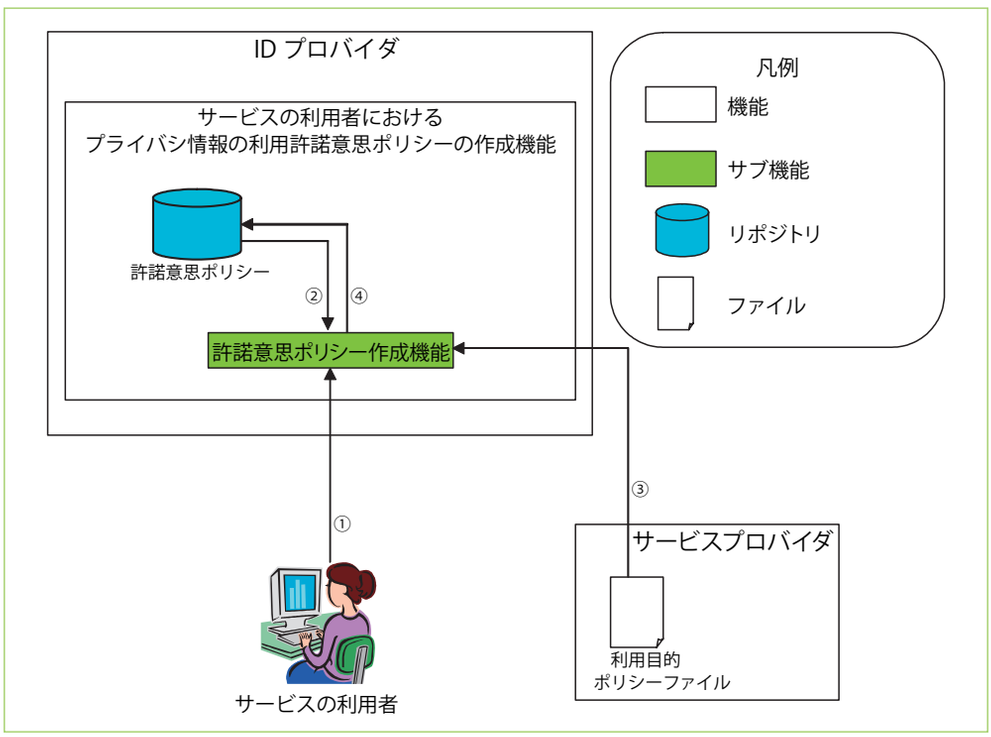

図 -4
プライバシ情報の利用許諾意思ポリシーの作成機能

サービス処理への認可をルール化と交換する「権限管理基盤技術」

権限管理基盤技術は，異なるサイト間の認可において，複数のアプリケーションで使用されるサービス利用者の権限情報を一元的に管理する手法，サイトをまたがったサービス利用者に対しても権限情報の整合性を維持する手法である．

従来のシステムにおいてもアクセス制御機能は存在している．しかし，そのアクセス制御機能はアプリケーションごとに実装されていることが多く，さらにそのアクセス制御に使用するアクセス制御ルールもアプリケーション固有のフォーマットであった．このような状況では，アクセス制御の管理者（サービス提供者）は，アプリ

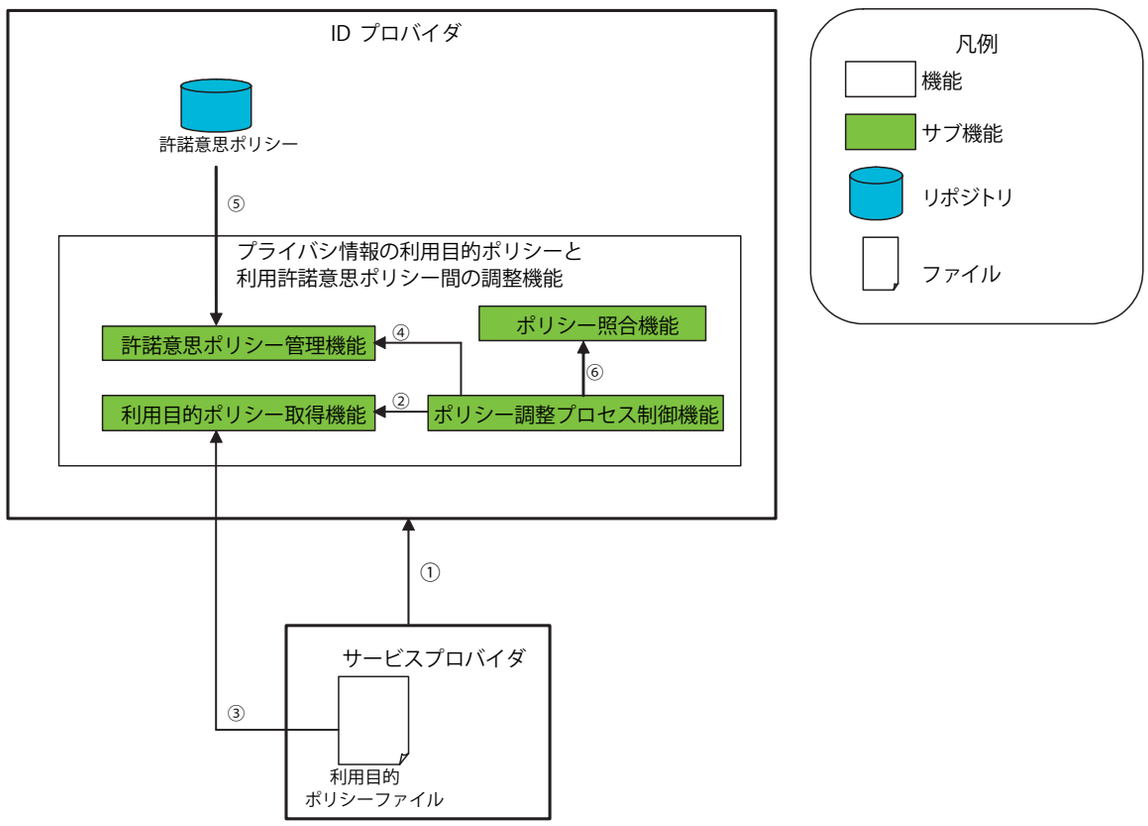

図 -5　利用許諾意思ポリシーの調整機能

ケーションごとにアクセス制御ルールを設定しなければならず，さらに，アプリケーションが連携する環境においては，システム全体でアクセス制御ルールに不整合が発生しないように細心の注意を払ってアクセス制御ルールを設定しなければならない．つまり，サービス提供者は，アクセス制御ルールの管理作業に煩雑で手間がかかるという問題点がある．具体的には，**図 -6** に示すように，サービス提供者がサービスのアクセス制御ルールを変更する際，住所変更サービスに対しては住所変更アクセス制御ルールを反映し，図書館利用サービスに対しては図書館利用アクセス制御ルールを反映しなければならない．サービス提供者はサービスごとに違う反映操作をするため手間がかかる．

サービス提供者の負担を軽減させる課題に対し，アクセス制御ルールの記述に統一定義した共通フォーマットを使用し，記述されたアクセス制御ルールをまとめて一元管理する解決策をとった．解決策を実現するために，権限情報提供技術と権限情報同期技術を開発した．

（1）権限情報提供技術

権限情報提供技術では，サイト内のアクセス制御ルールの管理および判定を実現する．この実現に必要な取り組みとして，アクセス制御ルールの標準化，統合的なアクセス制御ルールの管理がある．

（1-1）アクセス制御ルールの標準化

アクセス制御ルールを標準化するにあたり，基本となる考え方を以下に示す．

- アクセス制御ルールは，標準化された言語（XACML）を採用して共通化する．その際，汎用性・拡張性も考慮する．XACML 採用の理由を本稿末の参考情報に記す．
- アクセス制御は，サイト内で統一した判定基準（XACML）を採用する．
- 各アプリケーション向けインタフェースは，統一化して提供する．
- 通信プロトコルは，相互接続に向けて標準化された仕様（SOAP）を採用する．

（1-2）統合的なアクセス制御ルールの管理

アクセス制御ルールを管理するにあたり，基本となる考え方を以下に示す．

- サイト内のアクセス制御ルールは，1 つの管理コンソールから操作できるようにする．
- すべてのアプリケーションに対して統合的（一元的）に編集し，一括したアクセス制御の変更ができるようにする．

図 -7 に権限情報提供技術の実現例を示す．アクセス制御ルールを共通化し一元管理にする．また，住所変更サービスや図書館利用サービス等に対しては権限管理基

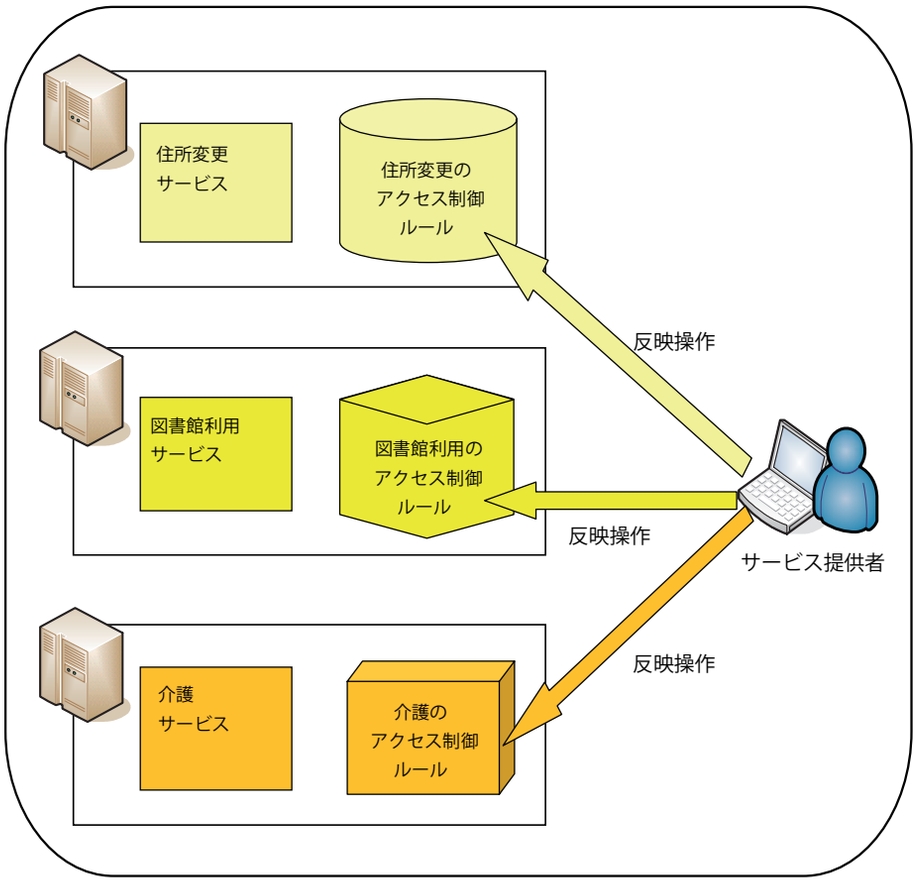

図 -6
サービス提供者が直面している問題点

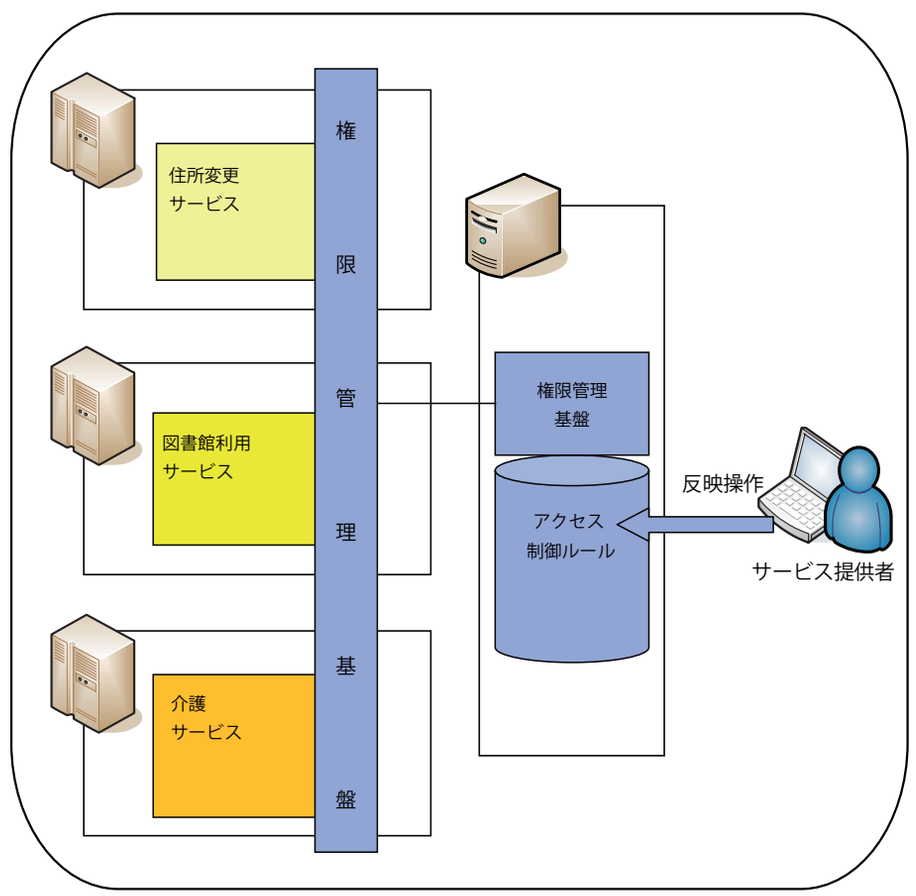

図 -7
権限情報提供技術の実現例

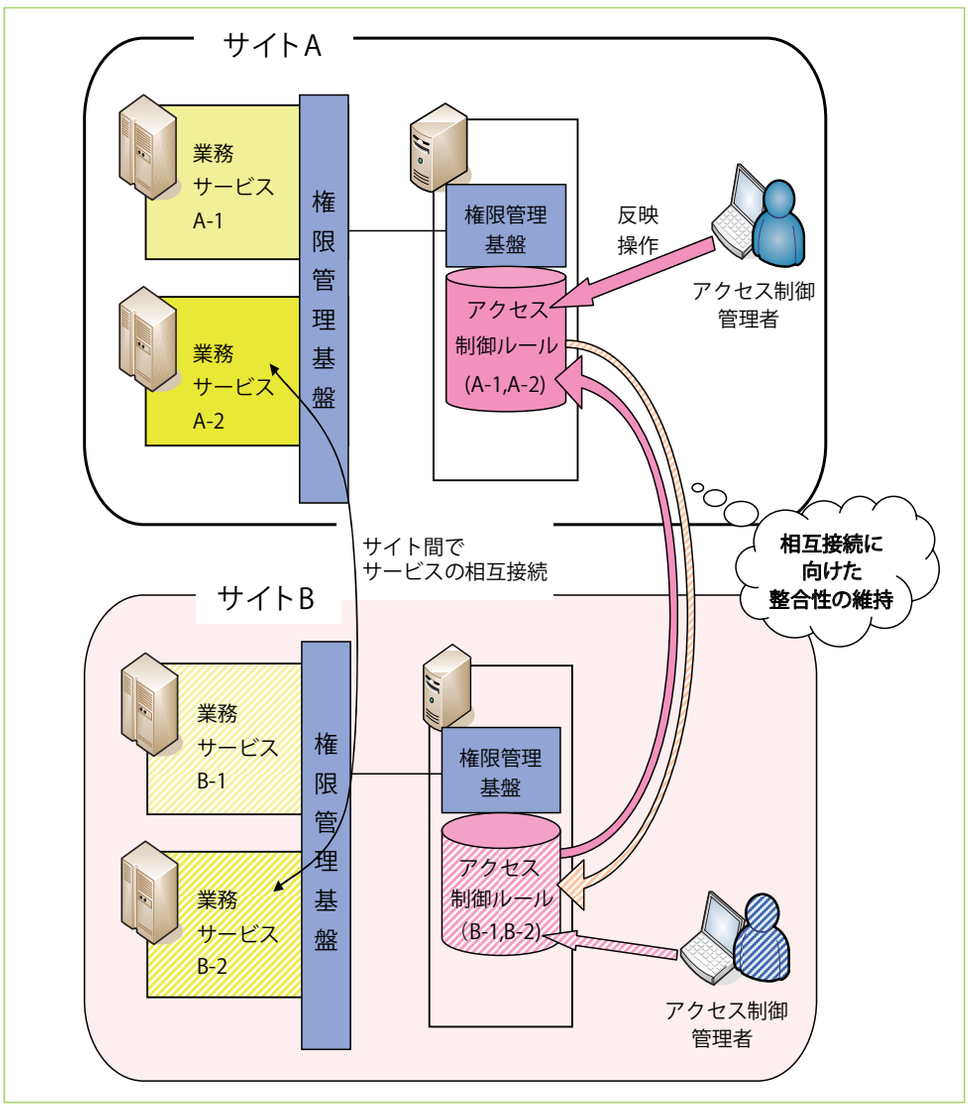

図 -8　権限情報同期技術の実現例

盤を提供し，共通化したアクセス制御ルールによる判定を可能にする．サービス提供者がアクセス制御ルールの反映操作にかける手間が削減される．

（2）権限情報同期技術

権限情報同期技術では，サイト間のアクセス制御ルールの管理および判定を実現する．この実現に必要な取り組みとして，権限情報の連携，権限情報の整合性の維持がある．

（2-1）権限情報の連携

権限情報は，他サイトで定義された権限情報に対しても適用できるように，サイト間で受け渡す際に変換する．

（2-2）権限情報の整合性を維持

権限情報は，他サイトで定義された権限情報に対しても適用できるように，自サイトの権限情報と他サイトの権限情報との関連に必要な情報の保持および管理ができるようにする．

図 -8 に権限情報同期技術の実現例を示す．サイト A の業務サービス A-2 とサイト B の業務サービス B-2 が連携する際，他サイトからの利用者に対してもアクセス制御すべきである．サイト A から受け渡す権限情報は，サイト B のアクセス制御ルールに適合させるように変換し，サイト B でアクセス制御を実施する．この際，変換する権限情報は，サービス提供者が管理しなければならない．

謝辞　本研究は，（独）情報通信研究機構からの委託研究開発「異なる運用ポリシーや異なるアーキテクチャのサービスが連携し，高付加価値サービスを提供できるためのサービス連携基盤技術の研究開発」の成果の一部である．ここに記して謝意を表する．

[参考情報]

アクセス制御を実現する上で，アクセス制御の機能性，拡張性，将来性から，標準化された規約を実装する方針とした．

アクセス制御およびアクセス制御ポリシーに関しては，これまでもいくつかの規約が標準化される動きがあるが，ここでは，その中でも代表的な XACML と EPAL をあげる．それぞれの詳細については各 Web サイトの情報を参照されたい．

（1）XACML（eXtensible Access Control Language）

XACML は OASIS で規格化が進められている XML ポリシー言語である．

http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml

（2）EPAL（Enterprise Privacy Authorization Language）

EPAL は W3C で規格化が進められている XML ポリシー言語である．IBM によって設計されたものである．

http://www.w3.org/Submission/2003/SUBM-EPAL-20031110/

右の表では XACML と EPAL との機能比較について示す（引用元：Anne Anderson. “A Comparison of EPAL and XACML” Sun Microsystems (July 12, 2004), http://research.sun.com/techrep/2005/smli_tr-2005-147/TRCompareEPALandXACML.html）．

上記のとおりに，機能性においては XACML が優れていると判断する．また，業界動向および将来性においても XACML が優れていると判断する．よって，権限管理基盤ではアクセス制御・認可決定のコア技術として XACML を利用するものとする．

機能	EPAL	XACML
決定要求（Decision Request）	✓	✓
ネストしたポリシー	未サポート	✓
ポリシーの参照	未サポート	✓
ルール	✓	✓
アルゴリズムや優先の結合	✓	✓
ボキャブラリー	✓	未サポート
属性値	✓	✓
属性マッピング	✓	✓
属性検索	✓	✓
XML 属性値	未サポート	✓
階層化エンティティ	✓	✓
複数の属性を持つ主体者（Subject）	✓	✓
複数の主体者（Subject）	未サポート	✓
目的（Purpose）属性	✓	✓
エラー処理	✓	✓
ターゲットやプレ条件	✓	✓
条件（Condition）	✓	✓
改訂番号	✓	✓
データ型	✓	✓
関数（Function）	✓	✓
責務（Obligation）	✓	✓
複数のレスポンス	未サポート	✓

（平成 19 年 3 月 28 日受付）

斉藤嗣治
t-saito@dh.jp.nec.com

1998 年，北陸先端科学技術大学院大学情報科学研究科修士課程修了，同年 NEC 入社．以来，主に，QoS，セキュリティ，認証連携に関する研究に従事．

石井章夫
ishii.akio@jp.fujitsu.com

1987 年名古屋大学理学部物理学科卒業．同年富士通入社．UNIX 関連技術動向調査，各種ミドルウェア（OLTP，LDAP ディレクトリ，電子証明書発行ミドルウェア）開発，標準化動向（SAML，XACML，SPML）調査などに従事．