Shibbolethを用いたインタークラウドシステムのための認証基盤の設計

相澤 孝至[1,a)]　棟朝 雅晴[1]　Courtney Powell[1]

概要：本稿では，全国各地に分散配置されたクラウドシステムを連携させ，一体的なインタークラウドシステムとして相互運用するための認証基盤の設計について述べる．本認証基盤では，認証連携技術であるShibboleth および代理証明書リポジトリを利用する事により，既存のクラウドシステムの設計を変更することなく，インタークラウドシステムを構成するクラウドシステムに対するシングルサインオンを実現する．本稿ではまた，本認証基盤の設計を検証するために構築した実験環境上での実証実験についても報告する．

1. はじめに

クラウドコンピューティングにおいて，仮想化技術に基づくIaaS（Infrastructure as a Service）型のサービス提供形態はその中でも注目されている方式の1つであり [1]，全国各地の研究機関や様々な企業で構築されている．ビジネスとして大規模なクラウドシステムによるサービスが行われているが，利用条件，利用料金，ネットワーク遅延，セキュリティポリシーなどの問題から，研究機関における要求に全て合致させることは困難である．そのため，多くの研究機関で独自のクラウドシステムが構築されている．ただ，予算上の制約などから，それぞれのシステムの規模は比較的小規模なものに留まることが多く，クラウドコンピューティングによるスケールメリットがいかされていないという問題がある．そこで，それぞれの研究機関に導入されたクラウドシステムを連携させ，大規模なインタークラウドシステムとしての利用が進められている．

これらのインタークラウドシステムの運用では，複数の異なる組織が運用する資源を一度の認証手続きで利用可能とするシングルサインオンを実現することが重要な課題となる．クラウドシステム上でシングルサインオンを実現する要素技術は従来より提案されている．しかし，実運用を既に提供している組織の資源間でシングルサインオンを実現するためには，各組織の異なる運用方法や既存ユーザーの利用方法に適した要素技術の選択，組織間の運用ポリシーの調整が必要であり，認証基盤の設計やシステム配備，運用方法を確立することは難しい．従って，既存のクラウドシステムの設計を変更することなくシングルサインオンを実現する認証基盤が求められている．

本稿ではインタークラウドシステムのための認証基盤の設計について述べる．インタークラウドシステムでは，シングルサインオンによりコミュニティクラウドあるいはプライベートクラウドへのアクセスを可能とすることを目指している．これを実現するための，本認証基盤でシングルサインオンを実現するための機構は，分散したアカウント管理システムを連携するための技術であるShibboleth[2] [3] および，代理証明書リポジトリ [4] を用いて設計されている．ユーザーは，各クラウドシステム上の一組織（情報基盤センター等）から発行されるインタークラウドシステムを利用するためのアカウント（インタークラウドアカウント）を用いて，インタークラウドシステム上のクラウドシステムにシングルサインオンすることが可能である．本認証基盤の設計を検証するため，認証基盤のプロトタイプシステムを構築し，実証実験を行った．本稿では実証実験についても報告する．

以後，2節ではインタークラウドシステムの概要について述べ，3節では認証基盤の設計を示し，4節では実証実験について報告する．最後に5節ではまとめと今後の計画について述べる．

1　北海道大学大学院情報科学研究科
北海道札幌市北区北14条西9丁目
a)　takashi.cbt197ne66@ist.hokudai.ac.jp

ⓒ 2013 Information Processing Society of Japan

2. インタークラウドシステムの概要

インタークラウドでは，全国各地に分散配置されたクラウトシステムを連携させ相互運用することにより，クラウドシステム間での柔軟な資源の融通したり，複数クラウドシステムの資源を組み合わせたサービスの提供したりとユーザの利便性を高めることを目的としている．

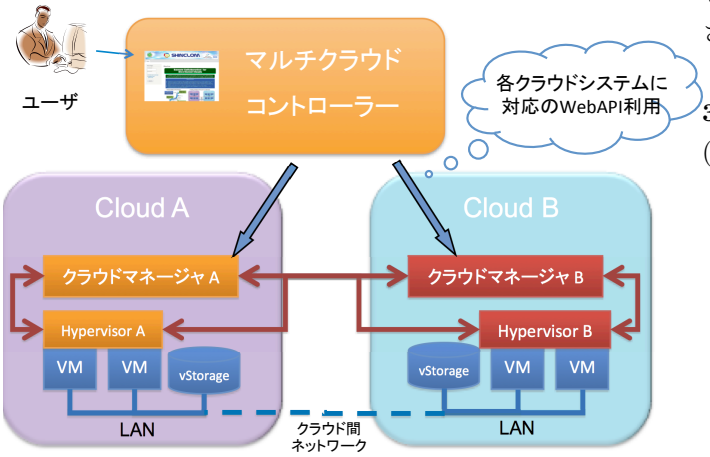

図 1 インタークラウドシステムの概要

図のようにユーザはマルチクラウドコントローラーの Web ブラウザを通して，各研究機関のクラウドシステムを操作することができる [5]．マルチクラウドコントローラーを通して，仮想マシンの起動や制御などの各クラウドシステムの計算機資源の操作・管理だけでなく，異なるクラウドシステムの計算機同士の通信や資源共有なども行うことができる．クラウドシステムでは，基本的に管理コンソールで実施可能な機能はすべて API が公開されており，各クラウドシステムに対応した WebAPI[6] を用いて，マルチクラウドコントローラーからクラウドシステムの操作が行われている．現在，Scalr[7] や RightScale[8] といった商用を目指したマルチクラウドコントローラーが開発・提供されているほか，SHINCLOM(Simple Heterogeneous INter-CLoud Manager)[9] といった学術向けマルチクラウドコントローラーの開発・提供もされている．また，ITU-T が公開している FG Cloud Technical Report[10] ではインタークラウドのいくつかのモデルやユースケースが取り上げられるなど，インタークラウドの国際標準化の検討が行われている．

インタークラウドシステムのユーザーが利用する手順を示す．インタークラウドシステム上の資源を利用するためには，利用したいクラウドシステムの組織に対して申請を行い，利用が認められる必要がある．インタークラウドアカウントを取得したユーザは，認証ポータル上でサインオン手続きを行い，本アカウントを用いて各クラウドシステムの組織に対して，利用申請を行う．申請が許可されたユーザに対しては，許可されたクラウドシステムへのアクセスが可能となる．

3. 認証基盤の設計

本節では，2 節であげたインタークラウドシステムを構成する組織が運用するクラウドシステムに対してシングルサインオンを実現するための認証基盤への要求要件を定義し，次にこの要求要件を満足するために採用した要素技術，さらに認証基盤アーキテクチャについて述べる [11]．

3.1 要求要件

(1) 機能性

- **シングルサインオン**：インタークラウドシステムを構築する各クラウドシステムはそれぞれ独立して運用されており，現在，ユーザはクラウドシステム毎に異なるユーザーアカウント（ローカルアカウント）やパスワード（APIKey や SecretKey）を用いてクラウドシステムにアクセスしている．これに対して，インタークラウドシステムでは，インタークラウドシステム上で有効な共通アカウント（インタークラウドアカウント）を用いることにより，インタークラウドシステムを構成している全てのクラウドシステムへのアクセスができる必要がある．
- **委譲**：インタークラウドシステムでは，ユーザが複数のクラウドシステムを利用する事が想定される．そのため，ユーザがあるクラウドシステムにアクセス後，さらに別のクラウドシステムへアクセスすることを認証手続き（APIKey や SecretKey の入力）を行うことなく実現できる必要がある．
- **様々な種類の IaaS 環境**：インタークラウドシステムを構成するクラウドシステムの IaaS クラウドソフトウェアは多岐にわたる．代表的な IaaS クラウドソフトウェアとしては，Eucalyptus[12]，OpenStack[13]，OpenNebula[14]，CloudStack[15] などがある．様々な種類の IaaS 環境に対応した認証基盤が必要である．

(2) 運用性

- **許可**：インタークラウドシステム上で提供される資源は，インタークラウドシステムのユーザに占有されるわけではなく，資源を運用する組織の多くのローカルユーザからも利用される．そのため，インタークラウドシステム上で認証されたユーザが資源を利用するための許可については，クラウドシステムを運用する組織が制限できる必要がある．
- **アカウント管理負荷分散**：インタークラウドシステムのユーザ数は単一組織内のユーザ数に比べて多いため，インタークラウドシステムのためのアカウント管理システムを新たに構築して運用することは多く

ⓒ 2013 Information Processing Society of Japan

の運用コストを必要とする．そのため, アカウント管理を複数組織に分散することにより, 管理負荷の分散を図る必要がある．

- **安定運用**：インタークラウドシステムの認証基盤には，インタークラウドを構成する各クラウドシステムの運用と同等の安定性および継続性が求められる．そのため，認証基盤を実現する要素技術やソフトウェアは，成熟した技術かつ可能な限り利用実績のあるソフトウェアである必要がある．またアカウント管理システムは，既に安定運用されているシステムを最大限に活用する必要がある．

(3) 利便性

- **ユーザインタフェース**：インタークラウドシステムのユーザが持つ分散計算環境を利用するための知識のレベルは多岐にわたることが想定されるため, シングルサインオン手続きは, 高度な知識や技術を持たないユーザにとっても簡便である必要がある．
- **複数クライアント環境**：インタークラウドシステムのユーザの利用環境（OS 等）は多岐にわたるため, より多くの環境からシングルサインオンが可能である必要がある．

3.2 要素技術

インタークラウドシステムでは，インタークラウドシステムを構成するクラウドシステムへのアクセス，ユーザ管理支援や先端ソフトウェア運用基盤の Web ポータルの利用に必要な認証が，3.1 節で示した要求要件を満たしつつ，シングルサインオンにより実現される必要がある．本認証基盤の設計では，これらの要求要件を満足するために，Shibboleth および代理証明書リポジトリを用いて認証基盤を実現することとした．具体的には，Shibboleth は分散管理されるインタークラウドアカウントを用いてユーザ管理支援や先端ソフトウェア運用基盤の Web ポータルを利用する際の認証に用いられる．証明書の発行や操作も Web ポータル上で提供されており，このための認証にも Shibboleth が用いられる．また，代理証明書リポジトリはインタークラウドアカウントと各クラウドシステムのローカルアカウントを対応づけるために用いられる．

本節では，以後，インタークラウドシステムの認証基盤を実現するために用いられた要素技術として，Shibboleth, 代理証明書リポジトリ，ユーザインターフェースについて述べる．

3.2.1 Shibboleth

インタークラウドシステムの認証基盤を実現する上で, インタークラウドアカウントの管理方法は重要な課題である．各クラウドシステムを利用するためのローカルアカウントは, 各資源の運用組織のアカウント管理システムにより管理されているため, これらの他にさらにインタークラウドアカウント用のアカウント管理システムを運用することは効率が悪い．そのため, 本認証基盤では, インタークラウドに資源を提供する組織が運用する既存のアカウント管理システム上にインタークラウドアカウントを登録するとともに, これらのアカウント管理システムは分散して存在するため, Shibboleth 認証連携技術を用いて分散したアカウント管理システムを連携させる．Shibboleth は Security Assertion Markup Lan- guage(SAML) [16] を用いて Web 認証処理を連携させる技術である．Shibboleth では, ネットワーク上でサービスを提供するサービスプロバイダ（SP）それぞれがユーザアカウントを管理するのではなく, ユーザが SP 上でサインオンする際に,SP がユーザのアカウントを管理するアイデンティティプロバイダ（IdP）に認証処理を依頼することで複数の組織間で連携した認証を実現している．LDAP[17] や Kerberos[18] などによる組織ごとに異なるアカウント管理システムを Shibboleth の IdP として統一的に連携運用することにより, 運用性に関する要件のうち, アカウント管理負荷分散を満足することができる．また,Shibboleth は Internet2 で開発され, 米国の研究教育機関間の認証連携サービスを提供している InCommon[19] において利用されている．また, 日本でも国立情報学研究所（NII）を中心とした「学術認証フェデレーション」（学認:GakuNin）[20] が立ち上がっており,NII と大学関係者による「学認タスクフォース」が立ち上がっている．このような実績をもつため, 運用性の安定運用に関する要件を満足する．

3.2.2 代理証明書リポジトリ

代理証明書リポジトリは，代理証明書を代理発行するシステムのことである．代理証明書とは，あるエンティティが別のエンティティを代理認証するための枠組みである．ユーザの持つクライアント証明書から作成され，新たに作成された秘密鍵と公開鍵を含み，ユーザの秘密鍵により署名されている．認証時には，代理証明書の秘密鍵を除いた部分が遠隔資源に送付され，Public Key Infrastructure（PKI）[21] に基づく認証処理が行われる．ユーザは，代理証明書を生成する際に一度だけユーザの秘密鍵を復号化するためのパスワレーズを入力するが，代理証明書中の秘密鍵は暗号化されていないため，その後の認証ではパスフレースを入力する必要がない．

インタークラウドシステムの認証基盤を実現する上で，インタークラウドアカウントと各クラウドシステムのローカルアカウントを対応づけることは重要である．本認証基盤では，代理証明書を用いることにより，インタークラウドアカウントと各クラウドシステムのローカルアカウントを結びつける．代理証明書を用いた認証方法は，グリッドコンピューティングにおける認証・暗号通信・シングルサインオンを実現するための仕組みである GSI（Grid Security Infrastructure）[22] [23] のシングルサインオンと委譲を実

ⓒ 2013 Information Processing Society of Japan

現するために使われている．以上の理由により，代理証明書リポジトリを用いることで運用生の安定運用に関する要件も満たすことができる．

3.2.3 ユーザインタフェース

ユーザの利便性を向上させるためには，より使い易いユーザーインタフェースを提供することが重要である．インタークラウドシステムの認証基盤では，インタークラウドシステム上のクラウドシステムにシングルサインオンするための認証ポータルとインタークラウドシステムのクラウドシステムを操作するためのクラウド管理ポータルを運用する．認証ポータルは ShibbolethSP を用いて，クラウド管理ポータルは学術向けマルチクラウドコントローラー SHINCLOM と連携することで実現している．図 2 は，クラウド管理ポータル画面を示す．ポータルを利用することで，WebAPI に精通していないユーザでもクラウドシステムの操作を安心して行うことができる．また，WebAPI に精通したユーザに対しては，クラウド管理ポータルで表示される APIKEY と SECRETKEY を使ってクラウドシステムを操作することも可能である．

図 2 クラウド管理ポータル画面

3.3 認証基盤のアーキテクチャ

インタークラウドシステム認証基盤は，表 1 に示す組織が運用するシステムから構成される．図 3 は，各機関が運用するシステムの関係を示す．インタークラウドシステム認証基盤では，アカウント作成，クラウドシステムの利用申請から，審査・選定を経て，資源利用の許可のための構成情報を一元管理している．

3.3.1 資源提供機関

資源提供機関は，インタークラウドシステムに対して計算機やネットワーク，ストレージなどを提供する組織である．図 4 のように，資源提供機関はプロジェクトという単位でユーザを管理する．

プロジェクトは，仮想マシン，スナップショット，テンプレート，データディスク，および IP アドレスなどの計算機資源を制限することができる．各クラウドシステム管

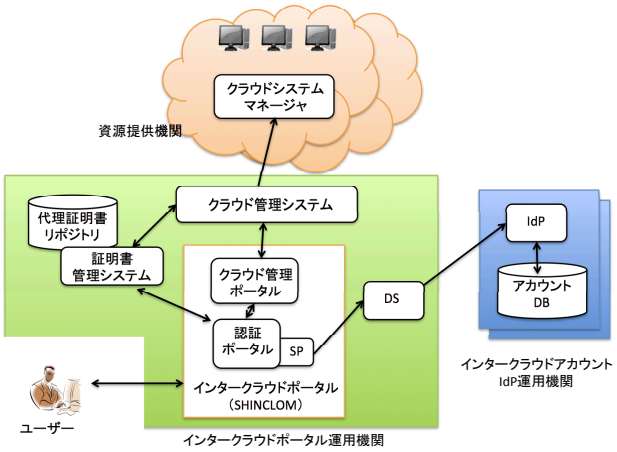

図 3 認証基盤のアーキテクチャ

運用機関	役割
インタークラウドポータル運用機関	インタークラウドシステム環境にシングルサインオンするための認証ポータルとクラウドシステムを操作・管理するためのクラウド管理ポータルを運用する．
インタークラウドアカウント IdP 運用機関	インタークラウドシステム環境にシングルサインオンするためのアカウントを発行・管理する．
資源提供機関	インタークラウドシステムのユーザに対して計算機やネットワーク，ストレージ等の資源を提供する．

表 1 認証基盤運用機関

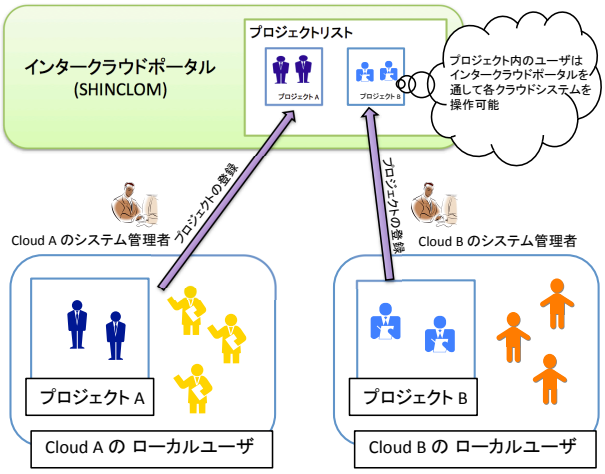

図 4 プロジェクトを用いたユーザ管理

ⓒ 2013 Information Processing Society of Japan

理者がインタークラウドシステムで利用する資源を制限することができ,3.1 節の運用性の許可を満たす．本認証基盤では，このプロジェクトというユーザ管理を使いシングルサインオンを実現する．具体的には，各資源提供機関はインタークラウドポータル運用機関に対してあらかじめプロジェクトを登録する．インタークラウドポータル運用機関からプロジェクトに登録しているユーザに対して認証ポータルで認証したユーザとの照合を代理証明書を用いておこなうことができ，プロジェクト内のユーザはシングルサインオンを行うことができる．

3.3.2 インタークラウドポータル運用機関

インタークラウドポータル運用機関は，インタークラウドシステムにユーザがシングルサインオンするための Web ポータル（認証ポータル）を提供し，シングルサインオンで得た情報をもとに各クラウドシステムを操作する Web ポータル（クラウド管理ポータル）も提供する組織である．認証ポータルは，Shibboleth による Web 認証フェデレーションから代理証明書を扱うための Web インターフェースを提供する．

具体的には，認証ポータルは Shibboleth SP として実装されており，ユーザ認証をユーザのインタークラウドアカウントを管理する Shibboleth IdP に依頼する．また，Shibboleth DS は, 認証を受けるアカウントを管理する Shibboleth IdP に認証処理を転送する役割を持つ．インタークラウドシステム上のユーザにはインタークラウドシステムの利用を申請する以前にインタークラウド ID と呼ばれる番号が割り当てられている．

クラウドシステム上では，代理証明書を生成することができ，生成された代理証明書は代理証明書レポジトリに保存される．代理証明書は生成時に有効期間を設定することにより万一漏出した場合の影響範囲を限定する事ができる．ユーザは，認証ポータル上で 1 時間単位で最大 168 時間（1 週間）まで有効期間を設定できる．例えば，有効期間を 24 時間と指定した場合，24 時間以内は認証手続きなしで各クラウドシステムにアクセスできる．インタークラウドポータル用ソフトウェアは，インタークラウドシステム向けに特化したインターフェースが必要なため，あたらに開発したものを用いる．また，代理証明書リポジトリには MyProxy[24] を用いる．

クラウド管理ポータルでは認証ポータルで得た SAML 情報と代理証明書をもとに，各クラウドシステム上のアカウントと認証したユーザの照合を行う．許可されたユーザに対して発行される APIKey と SecretKey を利用して，利用したいクラウドシステムに合わせた WebAPI を用いてクラウド操作を行う．図 5 は，クラウド管理ポータルが行う動きについて述べる．クラウド管理ポータルから各クラウドシステムを操作するソフトウェアは，新たに開発したものを用いる．

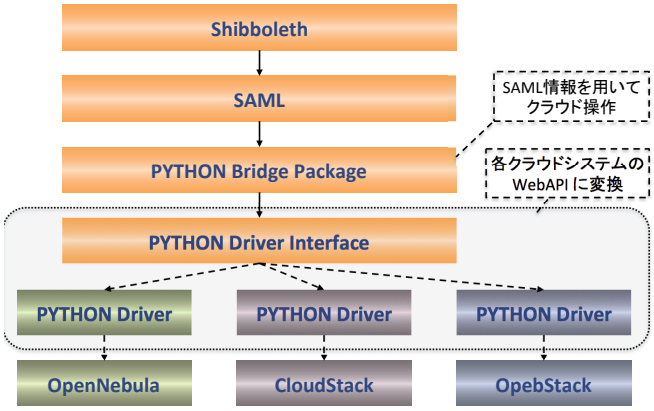

図 5 各クラウド基盤ソフトウェアに対応したクラウド操作

インタークラウドポータル運用機関では，代理証明書を用いることにより，インタークラウド ID と各クラウドシステムのローカルアカウント（APIKEY と SecretKey）を対応付ける．具体的には，以下の手順で対応付けが行われる．

(1) 資源提供機関は，ローカルアカウント作成時にユーザのインタークラウド ID を申請情報として得るため，ローカルアカウント作成後，代理証明書を生成し代理証明書リポジトリに登録する．インタークラウド ID と代理証明書の対応情報を作成する．
(2) インタークラウドポータル運用機関は資源提供機関のプロジェクトリストから，ユーザの代理証明書と APIKey/SecretKey 情報を得ることができる．
(3) インタークラウドポータル運用機関は，定期的に資源提供機関のプロジェクト情報から代理証明書と APIKey/SecretKey の情報を入手し，手元のインタークラウド ID と代理証明書の対応情報を照合することにより，インタークラウド ID と APIKey/SecretKey の対応付けを行うことができる．

これらの処理は，スクリプトを用いた自動処理が可能であり，資源提供機関における代理証明書の生成などの処理に要する負荷を抑さえることができる．また，インタークラウドシステム認証基盤では各組織に役割があり，インタークラウドポータル運用機関と認証許可の役割は完全に分離されている．そのため，インタークラウドポータル運用機関はフェデレーションにつきひとつだけ設置するものなのではなく，複数設置（連携）可能である．

3.3.3 インタークラウドアカウント IdP 運用機関

インタークラウドアカウント IdP 運用機関は，インタークラウドアカウントの認証機能を提供する組織である．本機関では，自らが運用するアカウント管理システム（アカウント DB）にインタークラウドアカウントを登録する．アカウント DB は Shibboleth IdP と連携しており，Shibboleth IdP は，Shibboleth SP から要求されたインタークラウドア

ⓒ 2013 Information Processing Society of Japan

カウントの認証を行い，認証結果を Shibboleth SP に返す．

4. 実証実験

本稿で示した認証基盤の実証実験を行うため，北海道大学，北見工業大学から構成される認証基盤実験環境を構築した．本節では，本環境上での実験結果について述べる．

4.1 動作試験

本実験環境では，図 6 に示すように，北海道大学がインタークラウドポータル運用機関の役割を持ち，認証ポータル，クラウド管理ポータル，代理証明書リポジトリ，Shibboleth DS を運用する．また，北見工業大学は，インタークラウドアカウント IdP 運用機関および資源提供機関としての役割を持ち，各自が運用するユーザアカウント管理システム（アカウント DB）と連携した Shibboleth IdP（IdP），クラウドシステムを運用する．表 2 は，実証実験に用いたソフトウェアの一覧を示す．

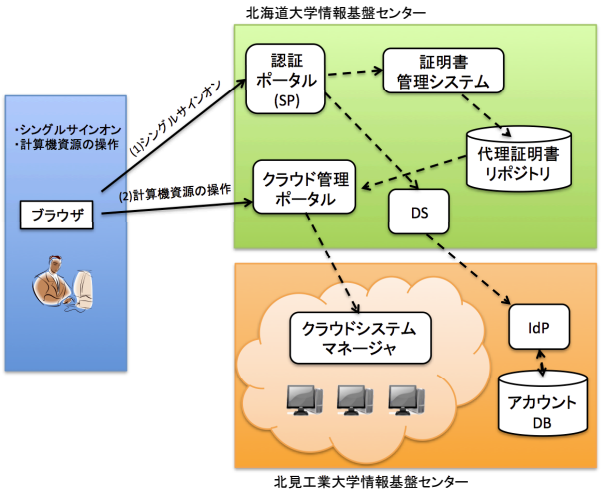

図 6 実証実験環境

システム名	ソフトウェア名
代理証明書リポジトリ	MyProxy 4.2
Shibboleth SP Shibboleth IdP Shibboleth DS	Shibboleth SP 2.5.2 Shibboleth IdP2.4.0 Shibboleth DS1.2.1
クラウドマネージャ	CloudStack4.1

表 2 認証基盤ソフトウェア一覧

本実証実験の結果，本環境上でユーザによる以下の操作が可能であり，本認証基盤により，インタークラウドシステムを構成するクラウドシステムへのシングルサインオンが可能であることが確認された．図 7 は認証時のユーザ画面を示す．

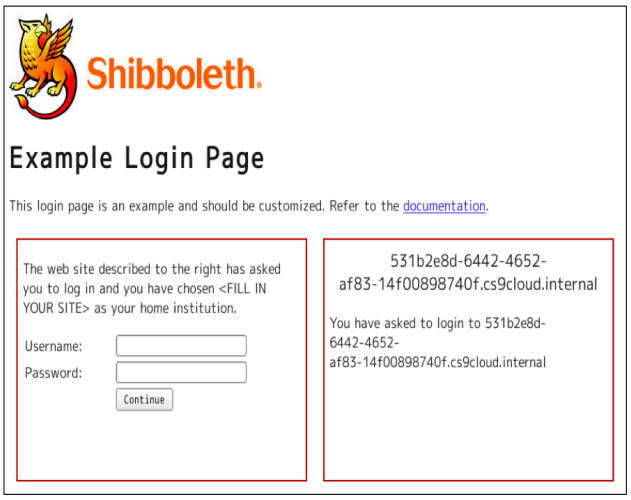

図 7 認証時のユーザ画面例

- Shibboleth 認証連携を用いた認証ポータル上のサインオン
- 認証ポータル上でのクラウドシステムの操作

Shibboleth に関する実験では，まず北海道大学内にテスト用の IdP を構築することにより，認証ポータル運用機関，インタークラウドアカウント IdP 運用機関間の連携動作を確認した．次に，北見工業大学に IdP を構築して北海道大学のシステムとの連携試験を行った．クラウドシステムとインタークラウドポータル運用機関に関する実験では，まず北見工業大学のクラウドシステムを構築し，CloudStack の WebUI からプロジェクト管理アカウントとプロジェクトの作成を行った．次に，インタークラウドポータル上でプロジェクトの登録を行った．

4.2 ユーザの利用例

ユーザの利用例として，シングルサインオンを行ってクラウドシステムの操作するまでの手順を示している．図中，実線矢印はユーザの処理，点線矢印はシステムの処理を意味する．

- ユーザは Web ブラウザで認証ポータルにサインオンする．この際，ユーザは自分のアカウントを管理するインタークラウドアカウント IdP 運用機関を Shibboleth DS 上で選択し，インタークラウドアカウントとパスワードを入力する．認証ポータルはユーザが指定した Shibboleth IdP にユーザの認証処理を依頼する．Shibboleth IdP から提供される「eduPersonTargetedID」属性をもとに，代理証明書リポジトリに対して代理証明書のダウンロードを行い，クラウド管理ポータルに代理証明書を受け渡す．
- ユーザはクラウド管理ポータルから各クラウドシステム上の計算機資源の操作を行う．具体的には，認証ポータルから受け取った代理証明書と SAML 情報を

ⓒ 2013 Information Processing Society of Japan

もとに，プロジェクトリストを用いて，ローカルアカウントとの対応付けを行う．その後，ローカルアカウント（APIKey と SecretKey）を用いて各クラウドシステムに対応した WebAPI でクラウドシステムの操作が行われる．そのため，ユーザが APIKey，SecretKey を入力する必要はない．

5. まとめと今後

本稿では，既存のクラウドシステムの設計を変更することなく，インタークラウドシステム上でシングルサインオンを実現するための認証基盤の設計およびプロトタイプシステムによる実証実験について述べた．今回の実証実験では，北海道大学と北見工業大学の 2 拠点でのテスト検証であった．今後，本運用と同仕様のシステムを用いた運用試験を多拠点で実施し，異なる IaaS 環境のクラウドシステムに対して認証実験を開始する予定である．また，本認証基盤とグリッド認証技術である GSI 技術を用いることで，計算資源に対してもシングルサインオンを行えるシステムを構築していく予定である．

謝辞
本研究の実施にあたり, クリエーションライン（株）との共同研究「マルチクラウド構築・運用技術に関する研究及びコントローラの開発」，および，学際大規模情報基盤共同利用・共同研究拠点の支援を受けました.

参考文献

[1] 新井利明, 山口宣宏, 関口知紀, 矢崎武己, クラウドコンピューテングを支える基盤技術,IT プラットフォーム,2010.
[2] *Internet2: Shibboleth.* http://shibboleth.internet2.edu/.
[3] Morgan, R. L., Cantor, S., Carmody, S., Hoehn, W. and Klingenstein, K.: Federated Se- curity: The Shibboleth Approach, EDUCAUSE Quarterly, Vol. 27, No. 4 (2004).
[4] 奥野琢人. グリッドコンピュータと pki. Technical report, 日本ネットワークセキュリティ協会, 2005.
[5] インタークラウドに向けたシステムアーキテクチャの提案 (クラウド). 電子情報通信学会, 2011.
[6] クラウドサービス api で仮想マシンを制御. itpro.
[7] *Scalr – Cloud Management Solutions for Private, Public Clouds.* http://www.scalr.com/.
[8] *Cloud Computing Management Platform by RightScale.* http://www.rightscale.com/.
[9] Courtney Powell, Masaharu Munetomo, Takashi Aizawa: Towards a User Deployable Service-oriented Autonomic Multi-cloud Overlay Infrastructure for Sky Computing, Proceedings of the 2013 International Conference on Grid Cloud Computing and Applications.
[10] *FG Cloud Technical Report.* http://www.itu.int.
[11] 高性能分散計算環境のための認証基盤の設計. SACSIS,2012, 合 田 憲 人. 東 田. 学. 坂 根 栄 作. 天 野 浩 文. 小 林克 志 棟 朝 雅 晴 江 川 隆 輔 ¿建 部 修 見 鴨 志田. 良和 滝澤. 真一朗 永 井. 亨 岩 下 武 史 石 川 裕.
[12] *The Eucalyptus Cloud.* http://www.eucalyptus.com/eucalyptus-cloud/iaas/.
[13] *OpenStack Open Source Cloud Computing Software.* http://www.openstack.org/.
[14] *OpenNebula - Open Source Data Center Virtualization.* http://opennebula.org/.
[15] *OpenStack Open Source Cloud Computing Software.* http://cloudstack.apache.org/.
[16] *OASIS: Security Assertion Markup Language(SAML) Specification*, 2004. http://www.oasis-open.org/committees/security/.
[17] Gerald Carter. LDAP-設定・管理・プログラミング-. オーム社, 2003.
[18] JasonGarman. *Kerberos.* オーム社, 2004.
[19] InCommon: InCommon, http://www.incommon.org/.
[20] 学術認証フェデレーション.
[21] 小松文子 (編): PKI ハントフック, ソフトリサーチセンター (2004).
[22] Welch, V., Siebenlist, F., Foster, I., Bresna- han, J., Czajkowski, K., Gawor, J., Kesselman, C., Meder, S., Pearlman, L. and Tuecke, S.: Se- curity for Grid Services, Proc. of the 12th IEEE International Symposium on High Performance Distributed Computing (2003).
[23] Welch, V.: Globus Toolkit Version 4 Grid Security Infrastructure: A Standards Perspective, http://www.globus.org/toolkit/docs/4.0/security/GT4-GSI-Overview.pdf (2005).
[24] Novotny, J., Tuecke, S. and Welch, V.: Initial Experiences with an Online Certificate Reposi- tory for the Grid: Myproxy, Proc. of the Tenth International Symposium on High Performance Distributed Computing (HPDC-10) (2001).

ⓒ 2013 Information Processing Society of Japan