社団法人　情報処理学会　研究報告
IPSJ SIG Technical Report

2006－DSM－40（25）
2006／3／29

広域 ID 連携および属性認証システムを利用した 非匿名性ネットワークの提案と評価

長谷川智矢[1]　小松愛美[1]　浦田昌和[2]　市川本浩[3]　石島辰太郎[4]

[1] 東京都立科学技術大学 工学部 電子システム工学科

[2] NTTサービスインテグレーション基盤研究所　[3] エーティーエル システムズ

[4] 首都大学東京 システムデザイン学部

インターネットの普及と接続環境の整備に伴い利用環境の社会的基盤としての役割が増しつつある．基盤化に伴い多様な利用形態が増しつつある．利用形態の多様化や変化に伴い従来ではあまり考慮されていなかったサービスの提供や利用およびリソースの共有や交換において，インターネットの特徴のひとつである匿名性が問題となりつつある．本稿では，インターネット利用における匿名性の問題点を述べ，提案する非匿名性ネットワークの必要性・特徴について述べる．非匿名性ネットワーク構築法として，広域ID連携及び属性認証の仕組みを提供するInternet2/MACE Shibboleth[1]を適用した．適用における構築法の検討と効果を検証する．

Proposal and Assessment for a Non-anonymous network with Identity Federation and Attribute-based Authorization through Shibboleth

Tomoya Hasegawa[1], Aimi Komatsu[1], Masakazu Urata[2], Motohiro Ichikawa[3], Shintaro Ishijima[4]

[1]Department of Electronic Systems Engineering, Faculty of Engineering, Tokyo Metropolitan Institute of Technology

[2]NTT Service Integration Laboratories [3]ATL Systems

[4]Faculty of System Design, Tokyo Metropolitan University

The Internet is increasing a role of the social infrastructure with maintaining of spread and communication environment. Various usages are increasing with the infrastructure. Currently, necessity is arising for problems of anonymous usages of the Internet in resource sharing and exchanges, and offering new unconventional services with diversification and change of usages. In this paper, we will describe these problems, and discuss "Non-anonymous network" needs and requirements. Then we will propose, and assessment our system with Identity Federation and Attribute-based Authorization through Internet2 Middleware Architecture Committee for Education (MACE) Shibboleth [1].

1.はじめに

インターネットは当初，研究用のネットワークとしてスタートしたが，今日では大学での研究活動や企業のビジネスに不可欠なものになってきており，一般家庭においても電子メールやショッピング等，利用が拡大している．インターネットを利用することにより，時間や距離に依存せず，低価格でサービスを利用できるようになった反面，利用者やサービス提供者の住所や氏名が相手に分からないといった匿名性に起因した犯罪への利用が問題となってきている[2]．自殺支援サイトやフィッシング詐欺等は，その一例である．また，大学内外や産学公の連携を支える情報インフラとして，情報ネットワークは必要不可欠であり，匿名性を廃しながら安全かつ信頼性の高いネットワークが求められている．しかしながら，匿名性を廃し単に実名で利用する場合，次のような問題がある．インターネット上のサービスは，匿名利用もしくは事前に個人情報を登録しておき利用時に認証を行う　（＝個人を特定する）形態に分類できる．しかしながら，サービス利用時に認証を行う方式の場合，認証主体とサービス提供者が同じであり，誰がどういったサービスを利用したかがサービス提供者に分かってしまい，購入

履歴等の個人情報がサービス提供以外の目的に利用される可能性がある．サービス提供者においても，個人情報を安全に管理する必要があり，運用コストが増加する．また，複数のサービスを利用する場合，個人情報を複数のサイトに登録する必要があるため，個人情報が偏在し漏洩の危険性が高くなる．

そこで本研究では，利用者の匿名性を廃し利用者を識別可能であり，かつ，個人情報の取扱いに配慮した非匿名性ネットワークの構築方法について研究を行い，実証実験を通してその有効性を確認することを目的とする．

本稿では、まず提案する非匿名性ネットワークの構成法について述べ、次に今回採用したソフトウェアである“Shibboleth”について解説する。その後、Shibboleth を使った非匿名性ネットワークの評価を行い、最後にまとめと課題について述べる。

2.非匿名性ネットワーク

2.1 非匿名性ネットワークの定義

前項で述べた問題点を解決するため，非匿名性ネットワークが満たすべき要件を以下に示す．

(1)通常は利用者情報，及び，その行為を特定するための情報を分散管理する等，利用者の特定を困難とし，問題発生時には，ネットワーク管理者等の特定の権限を持った管理者が情報を集約することで，利用者の特定が可能であること

(2)利用者のプライバシーに配慮し，サービスの利用履歴情報，及び，住所・氏名等の個人情報が適切に管理されること．

2.2 非匿名性ネットワークの構成法

利用者を特定する技術として ID・パスワード認証やバイオメトリクスといった認証技術がある．これらの認証情報と履歴情報（認証ログ，アクセスログ等）を使うことで利用者の特定が可能となる．しかし，認証主体とサービス提供者が同一の場合、前項で述べたような購入履歴等のプライバシー情報の管理の問題や、個人情報をサービス毎に登録しておくことが必要となる．そこで，非匿名性ネットワークを実現するための技術として，近年注目されている広域 ID 連携の技術に着目した．広域 ID 連携システムにおいては，個人情報を管理し認証を行う Identity Provider (IdP) と，サービス提供を行う Service Provider (SP) に役割が分離されており，SP に対する個人情報の扱いについても配慮されている．また，IdP の認証ログ，SP のアクセスログを集約することで利用者の特定も可能と考えられる．本研究では米国 Internet2 プロジェクトで開発され米国や欧州の大学や行政・研究機関での利用が進んでいる Shibboleth[1] を採用しネットワークを構築した．

3．Shibboleth

3.1 概要

Shibboleth[1] はプロジェクトの名称であり，次世代インターネット研究開発コンソーシアム（Internet2）教育向けミドルウェア・アーキテクチャ評議会（Middleware Architecture Council for Education, MACE）において研究が進められている．その内容は学術教育組織間で，特にウェブリソースの共有を行うために必要となるアクセス制御や複数組織間でのアクセス制御情報の交換に関するものである．

3.2 特徴

Shibboleth は組織同士で連盟 (federation)をつくる．所属する組織にログインしたあとは，関連する組織のサイトにシングルサインオンでアクセスできる．ログイン時に払いだされた識別子 NameIdentifier により組織（ドメイン）を越えたアクセスを可能としている．NameIdentifier により，認証による認可情報の参照や交換が可能となる．NameIdentifier により属する組織の認証システムと分けられていることで，組織の認証システムを変更することなく組織を越えた広域のシングルサインオンを行うことができる．

最大の特徴として，アクセスするリソースを選択できるという機能がある．所属する組織で参照・交換可能な情報とアクセスするサイトが要求する許可用の情報を比較し，マッチしたリソースのみにアクセスすることができる．このとき使用される情報を属性情報 （Attribute）と呼ぶ．属性情報は，所属する組織により定められ，氏名や大学，所属するドメイン名等幅広く定義することができる．本機能により，リソース提供側はアクセス希望側の情報を必要に応じて知ることができる．また，利用側としても所属する組織単位ではあるが，属性情報の参照の範囲制御できるため，ネットワーク上の非匿名性・匿名性の操作を行うことができる．そのため，プライバシーにも配慮したネットワークを構築することができる．

Shibboleth の構成は，主にリソースの存在する Service Provider (SP)，SP に対して NameIdentifier を払い出す Identity Provider (IdP), 複数の IdP が存在する場合，所属する組織の IdP を選択する WAYF (Where Are You From?) の３つから成っている．

国外では InCommon (USA)や SWITCH (SWISS), SDSS (UK)といった機関で実証実験や研究が盛んである．

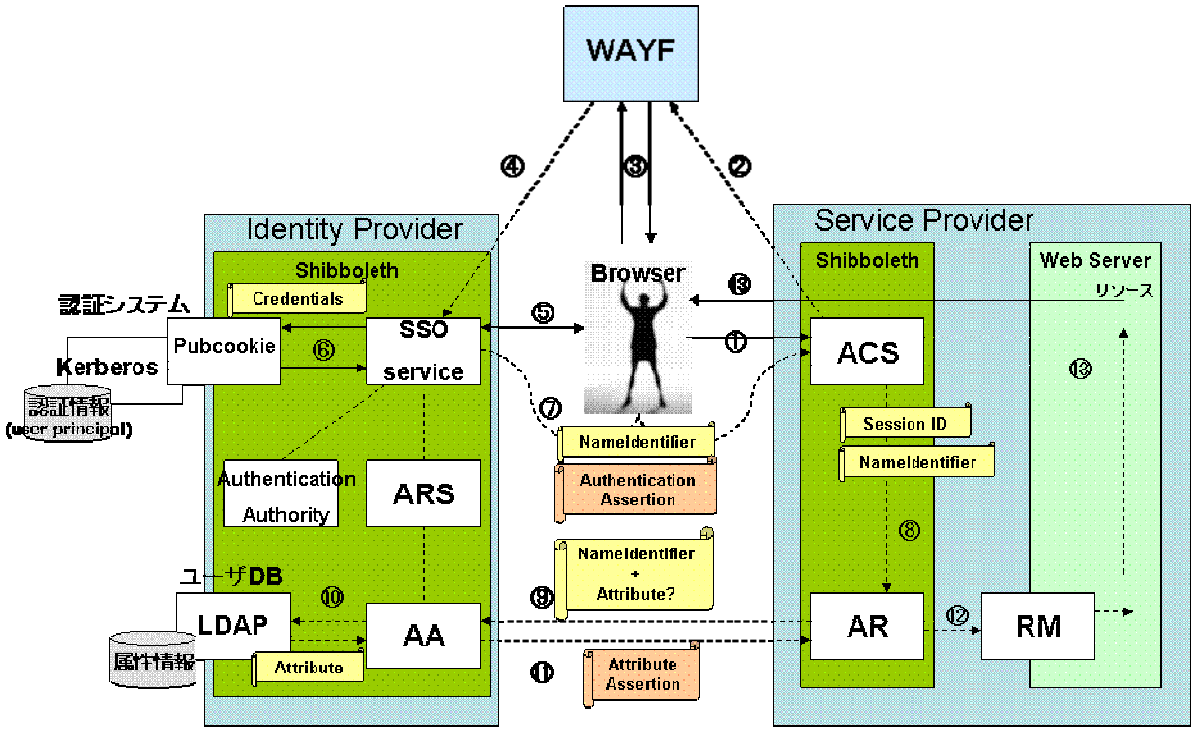

図 1：Shibboleth の処理フロー

3.3 Shibboleth の認証メカニズム

利用者が Shibboleth に管理されている Service Provider (SP)へアクセスした場合の動作を説明する．Shibboleth の処理フローを図 1 に示す．

3.3.1 Shibboleth 認証 1

利用者はアクセスしたい SP へウェブブラウザでアクセスする①．1 度目のアクセスであった場合，SP 側の Assertion Consumer Service (ACS)は Where Are You From? (WAYF)へアクセスをリダイレクトさせる②．WAYF は，複数 IdP が存在する場合，その選択の仲介を行う．利用者はブラウザを通し所属する組織の IdP を選択する③．その選択により，IdP へリダイレクトされる④．

3.3.2 Shibboleth 認証 2

利用者のアクセスが IdP へリダイレクトされると，シングルサインオンサービス (SSO service)により利用者の認可情報が確認される．本実証実験では，認証システムの利用者認証に Kerberos，シングルサインオン機能に Pubcookie を用いる⑥．ウェブブラウザに保存されている cookie を確認し，まだ利用者認証が終わっていないと判断されると，認証画面が表示される⑤．入力された利用者 ID とパスワードは，認証システムに問い合わされ，認証結果を得る⑥．

3.3.3 Shibboleth 認証 3

利用者が正しく認証されると，SSO service から NameIdentifier，Authentication Authority から認可情報 （Authentication Assertion）が払い出される⑦．SP 側の ACS はその情報を受け取ると，Authentication Assertion から Session ID を生成し，NameIdentifier と共に，同 SP 内の Attribute Requester (AR)へ渡す⑧．AR は，NameIdentifier の属性情報を IdP の Attirbute Authority (AA)へ問い合わせる⑨．

3.3.4 Shibboleth 認証 4

AA では，NameIdentifier から利用者 ID を求め利用者・データベースから属性情報 (Attribute)を取り出す⑩．このとき，Shibboleth では属性情報参照ポリシー設定ファイル (arp.site.xml)より属性情報の参照範囲の制御が可能となる．取り出された属性情報は SP の AR へと送られる⑪．その後，属性情報は同 SP 内の Resource Manager (RM)に渡され⑫，リソース利用に必要な属性情報を満たしているならば，利用者へリソースアクセスが可能となる⑬．

3.3.5 Shibboleth 構成

IdP が SP に対してどの属性情報を参照・交換可能とするかといったポリシーを，IdP の Attribute Release Policies （ARPs）に記述し，その属性情報を受取った SP 側でどの属性情報を上位アプリケーションに通知するかのポリシーを，SP の Attribute Acceptance Policies (AAPs)に記述

する．Shibboleth は ID 連携及び属性認証の仕組みを提供し, 利用者認証やシングルサインオンのためのメカニズムについては, 標準的な技術と連携可能である（可能なように設計してある）.

今回の非匿名性ネットワークでは, 標準的な技術であり，Shibboleth との連携が可能な以下の仕組みを採用した.

- 利用者認証：Kerberos
- 利用者情報のリポジトリ：LDAP
- SSO 機能：Pubcookie

なお，単純に Shibboleth を適用した構成では, 利用可能なアプリケーションは, ブラウザを利用した Web ベースのアプリケーションを想定している．グリッド・コンピューティングにおける GridShib[3] の取り組み，P2P ファイル共有システム LionShare[4] での適用等，Web ベースのアプリケーション以外への適用が進みつつある.

4.評価

構築した非匿名性ネットワークは利用履歴情報であるログを集約することで利用者の特定が可能である．利用履歴の追跡が可能か実験し，評価を行った.

次に，SP 間で遷移したときに，個人情報が保護されているかの確認を行うために，HTTP ヘッダの情報と SP のログ情報を集め評価を行った.

最後に, 様々な利用形態に沿ったアクセス制限を行い, 非匿名性ネットワークの可用性を評価した.

4.1 利用主体の特定可能性の評価

非匿名性ネットワークは, 利用履歴情報であるログを集約することで利用主体を特定可能で, 利用主体の追跡が可能か確認する．また，集約をしなければ，個人情報が守られることも確認する.

利用主体がアクセスする SP として，一つ目は要求する属性項目に非匿名性の高い設定をしたブログを用い, 二つ目は要求する属性項目に非匿名性の低い設定をした動画ダウンロードサイトとした．この二つ属性情報の異なる要求の SP にアクセスし，ログ情報をそれぞれ集約する．各 SP の要求する属性項目を以下の表 1 に示す.

表 1 ：各 SP の要求する属性項目

	SP1	SP2
要求する属性項目	eduPersonPrincipalName 大学内のユニーク ID (メールアドレス) (e.g. qu0001@tmit.xxx)	eduPersonAffiliation 役職 (e.g. student, staff, faculty, menber)
	surname 苗字 (e.g. Gakusei)	PostalAddress 住所 (e.g. Tokyo, Niigata)
	givenname 名前 (e.g. Kazuko)	eduPersonScopedAffiliation 所属ドメイン (e.g.student@ tmit.xxx)

実験には，qu0001 という ID を持つ利用主体を用いた．この利用主体の属性項目とその内容を表 2 に示す.

表 2：qu0001 の登録した属性情報

属性情報の項目	登録した属性情報
eduPersonPrincipalName	qu0001@tmit.xxx
surname	Gakusei
givenname	Kazuko
eduPersonAffiliation	student
PostalAddress	Tokyo
eduPersonScopedAffiliation	student@tmit.xxx

各 SP には，以下の図 2 および 3 のようにアクセスを行った.

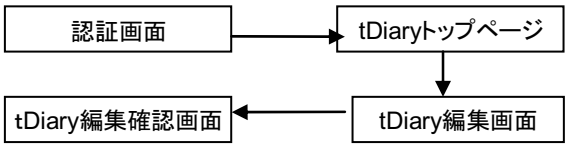

図 2：SP1（ブログ）へのアクセス手順

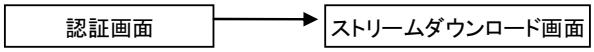

図 3：SP2（動画ダウンロードサイト）へのアクセスの手順

図 4 および 5 に動画ダウンロードサイトへのアクセスの集約したログ情報の一部を示す.

```
<NameIdentifierFormat="urn:mace:shibboleth:1.0:nameIdentifier"
NameQualifier="urn:mace:shibboleth:metro:tmit">_2f738487ba70679e50cf6bde244b657

xx.xx.18.74 - - [16/Feb/2006:04:49:17 +0900]
"GET /video-library HTTP/1.1" 302 415
xx.xx.18.74 - - [16/Feb/2006:04:49:27 +0900]"
POST/Shibboleth.sso/SAML/POST HTTP/1.1" 302 229
xx.xx.18.74 - - [16/Feb/2006:04:49:30 +0900]
"GET/video-library/NGC-TheSecretLifeOfCats.wmv HTTP/1.1" 304 -
```

図 4：SP のログ情報

```
2006-02-16 04:49:27,034 INFO
Shibboleth-TRANSACTION : Authentication
assertion issued to provider
(https://sp1.tmit.xxx/shibboleth) on behalf of principal
(qu0001). Name Identifier:
(_2f738487ba70679e50cf6bde244b6571).
Name Identifier Format:
(urn:mace:shibboleth:1.0:nameIdentifier).
```

図 5：IdP のログ情報

それぞれに同じ NameIdentifier が表示されていることから，利用主体の ID と行動履歴を結びつけることができる．この他のログ情報より，利用主体の属性項目を知ることができる．これらの情報より利用主体を特定することができる．また，個

別のログ情報のみでは，SP では行動履歴，IdP では利用主体の ID，属性情報のみしか分からないために利用主体を特定することはできない．このために，個人情報を保護することができる．ブログへのアクセスにおいても同様の結果を確認した．よって，利用主体の特定に，要求する属性項目は影響しない．

4.2 匿名性と非匿名性の操作性の評価

提案する非匿名性ネットワークにおける，匿名性と非匿名性の操作性について評価を行うため，SP 間を遷移したときの HTTP ヘッダ，SP 側の Shibboleth ログ情報を集約した．

SP1
New session
(ID: **_13cd824ef6c2ff2ca4b987c0e0e26ad3**) with
(applicationId: default) for principal from
(IdP:urn:mace:shibboleth:metro:tmit.xxx)
at (ClientAddress: xxx18.126) with
(NameIdentifier: **_d73face90b614baf5a7c78cbe9ce557b**)

SP2
New session
(ID: **_e73956b8924acd5d83a3b0858504249a**) with
(applicationId: default) for principal from
(IdP:urn:mace:shibboleth:metro:tmit.xxx)
at (ClientAddress: xxx.18.126) with
(NameIdentifier: **_116e0e79fc4e5df125b9d1567a13a7d6**)

図 6：SP 側のログ

SP 1
"_shibstate_89d1883123dfe21108933e643ddafebac1be5028=
https%3A%2F%2Fsp1.tmit.xxx%2Fvideo-library;
_shibsession_89d1883123dfe21108933e643ddafebac1be5028=
_13cd824ef6c2ff2ca4b987c0e0e26ad3;
_saml_idp=dXJuOm1hY2U6c2hpYmJvbGV0aDptZXRybzp0bWl0LXVuZXQub2NuLm5lLmpw"
student student@tmit.xxx - - - -

SP2
"_shibstate_c94d71b7044ee2eb9c5690ac4d4ebc0a1279b604=
https%3A%2F%2Fsp2.tmit.xxx%2Ftdiary;
_shibsession_c94d71b7044ee2eb9c5690ac4d4ebc0a1279b604=
_e73956b8924acd5d83a3b0858504249a;
_saml_idp=dXJuOm1hY2U6c2hpYmJvbGV0aDptZXRybzp0bWl0LXVuZXQub2NuLm5lLmpw"
- - kazuko gakusei - qu0001@tmit.xxx

shibstate_SP の識別名：ブラウザのリンク先
saml_idp：IdP を示す Handle
shibsession_SP の識別名：ブラウザ（ユーザ）と SP のセッションを示す Handle

図 7：HTTP ヘッダに含まれる cookie

図 6 より，IdP から払い出された利用者 ID を示す NameIdentifier が異なる．そのため，SP 側では，ブラウザ(利用者)とのセッション Handle (shibsession SP の識別名)も新しく生成された．

SP2 にアクセス，認証完了後にSP1 へと遷移した．しかし，図7 より，異なるSPにアクセスをすると同セッションが行われていることがわかった．この結果から，Shibbolethを採用した非匿名性ネットワークではIdP－SP間，ブラウザ(利用者)－SP間のセッションをSPごとに独立させることにより匿名性を確保していることが明らかとなった．

4.3 アクセス制限の可用性の評価

提案する非匿名性ネットワークにおいて，様々な利用形態に沿ったアクセス制限を行えるか，その可用性について評価を行った．その際，属性情報の異なる利用者を 7 人，要求する属性情報の項目が異なるサービスを 4 つ想定した(表 3)(表 4)．サービスには，大学が実際に提供するサービスを想定した属性情報によるアクセス制限がかけられている．これらの条件から 28 通りのアクセス結果を取得した(表 5)．

表 3：利用者の属性情報

ユーザ名	ユーザ ID	役職	所属ドメイン	住所
ユーザ 1	qu0001	student	tmit.xxx	Tokyo
ユーザ 2	qu0002	student	tmit.xxx	Tokyo
ユーザ 3	fa0001	faculty	tmit.xxx	-
ユーザ 4	st0001	staff	tmit.xxx	Tokyo
ユーザ 5	st0002	staff	tmit.xxx	-
ユーザ 6	abc123	student	aiit.xxx	Tokyo
ユーザ 7	abc456	student	aiit.xxx	-

表 4：アクセスサイトの制限

	サイト 1 (AND)	サイト 2 (AND)	サイト 3 (AND)	サイト 4 (AND)
eduPerson Affiliation 役職	student	student or faculty	faculty	-
eduPersonScoped Affiliation 所属ドメイン	tmit.xxx	tmit.xxx	tmit.xxx	tmit.xxx or Tokyo
PostalAddress 住所	Tokyo	-	-	

表 5：アクセス結果

	ユーザ ID	サイト 1	サイト 2	サイト 4	サイト 3
ユーザ 1	qu0001	○	○	×	○
ユーザ 2	qu0002	×	○	×	○
ユーザ 3	fa0001	×	○	○	○
ユーザ 4	st0001	×	×	×	○
ユーザ 5	st0002	×	×	×	○
ユーザ 6	abc123	×	×	×	○
ユーザ 7	abc456	×	×	×	×

この結果から，Shibboleth を採用した非匿名性ネットワークでは，アクセス制限として，
・条件を全て満たしている (AND).
・複数の条件のうち，１つでも満たしている

（OR）.
が適用可能であり，
・条件と等しくない (NOT).
については，本実験では，Shibboleth の認証モジュールが Apache のモジュールを使用したため，Apache のモジュールの記述法の制約を受け確認することができなかった.

5.まとめと考察

今回構築した非匿名性のネットワークにおいて, ログ解析に一般的に用いられているサイトのアクセスログと比較すると，各 SP のログ情報だけでは，利用した時間，どこからアクセスしたなどの履歴情報は，現状と変わらない．しかしながら，利用主体の属性情報が分かることで，利用者がサイトにアクセスした目的の推測等が可能である．したがって，参照・交換可能とする属性情報の範囲の取り決めと規約が重要な要素となる．系として履歴情報を集約することで IdP において認証をどのように確実に行い，さらに SP で属性を要求することで利用主体がサイトにアクセスできる属性を持っているかが分かる．よって，構築したネットワークは, 高いセキュリティを確保しつつ利用主体の特定を行う要件を満たしていると考えられる．個人情報保護の観点では，SP ごとに払いだされる NameIdentifier が独立しているため, 利用主体を特定することが困難な仕組みとなっている．NameIdentifier が独立する単位は連盟内で IdP, SP が共有する規約の設定ファイルである metadata.xml 内の Provider ID に依存している．属性情報の参照・交換についても IdP の属性情報参照ポリシー設定ファイルである arp.site.xml において同様に Provider ID 単位となっている．したがって，非匿名性ネットワークは個人情報の保護にも配慮したネットワークといえる.

以上より, 本実証実験で定義した非匿名性ネットワークの要求条件
・利用者の特定可能性の確保
・個人情報の保護
の 2 点が満たされていることが明らかとなった．よって，Shibboleth を採用した非匿名性ネットワークは個人情報の取扱いに配慮した非匿名性ネットワークの実現方法として有効である.

６．今後の課題

今回の実験により, 構築したシステムの利用履歴情報を利用することで, 技術的には利用主体が識別可能であり, 行動履歴を追跡可能であることを確認できた．しかしながら，実際の大学間や産学連携のためのネットワークに適用するには, 信頼できる組織の集合である連盟に規約やネットワークの運用ポリシーを規定する必要がある.

参考文献

[1] Shibboleth Project: http://shibboleth.internet2.edu/
[2] 警察庁サイバー犯罪統計資料: http://www.npa.go.jp/cyber/statics/index.html
[3] GridShib: http://gridshib.globus.org/
[4] LionShare: http://lionshare.its.psu.edu/main/