

Shibboleth試行運用実験と 分散ストレージ



名古屋大学情報基盤センター

名古屋大学IdP

- **全学的なユーザ認証基盤と接続**
 - 名古屋大学ID/パスワードでログイン可能
 - 全構成員がログイン可能
 - 人事労務課・学務部からデータ入手
 - 月に1回程度, 内容を更新(異動など)
- **IdPサーバ**
 - CPU: Xeon 3.80GHz (4コア)
 - OS: CentOS 5.4
 - メモリ: 4GB
- **Cambridge Journals Onlineなどの電子ジャーナルとの接続**
- **試行運用するための要項の作成**
 - 情報連携統括本部会議で承認



試行運用実験

試行運用実験

UPKI-Fed試行運用実験 - Mozilla Firefox

ファイル(E) 編集(E) 表示(V) 履歴(S) ブックマーク(B) ツール(I) ヘルプ(H)

http://w3serv.itc.nagoya-u.ac.jp/UPKI-Fed/

UPKI-Fed試行運用実験

UPKI-Fedとは

本実験は国立情報学研究所が中心となり、全国の約30の教育研究機関と情報サービス提供機関が組織する学術認証フェデレーション(UPKI-Fed)の試行運用を行なうものです。UPKI-Fedに参加する機関のうち、情報サービスを提供する機関をSP(S)機関をIdP(ID Provider)といいます。UPKI-Fedでは、どのSPが提供するサービスの情報サービスを行う機関のIdPがユーザ認証を行ないます。

UPKI-Fed試行運用実験の期間

2010年1月1日～2010年2月28日

実験参加者の募集期間は、2009年12月17日～2010年2月21日です。

UPKI-Fed試行運用実験で採取される情報

本実験では、UPKI-Fedにおける運用上の課題を抽出し、検討することを目的とします。そのため、

- アクセスした参加者のユーザID
- 参加者の所属学部
- コンピュータのIPアドレス、ドメイン名
- アクセス日時

Nagoya University Shibboleth IdP - Mozilla Firefox

ファイル(E) 編集(E) 表示(V) 履歴(S) ブックマーク(B) ツール(I) ヘルプ(H)

nagoya-u.ac.jp https://shib.itc.nagoya-u

名古屋大学

名古屋大学ID
(Nagoya University ID):

パスワード
(Password):

Login

注意: 全学IDではログインすることはできません

- ただいま、Shibbolethによる学術認証フェデレーションの試行運用実験中です。詳細は <http://w3serv.itc.nagoya-u.ac.jp/UPKI-Fed/>を御覧下さい。
- 本実験にご協力いただける方は上記のURLから「同意書」を印刷し、「実験者控」に署名の上、情報基盤センター 平野 へ送付してください。

試行運用の参加者

- (アクセスできるSPのほとんどが電子ジャーナルなので)附属図書館から教員へ案内を送付
- 同意書への署名・返送
 - 農学部・工学部等から6名が同意書を返送
 - 同意書を返送しないで利用している人も多数

利用可能なSP

- Science Direct
- SpringerLink
- Web of Knowledge
- EndNote Web
- OvidSP
- Cambridge Journals Online
- Pathology Images
- CiNii

サービスプロバイダ(SP)へのアクセス方法と渡される情報

現在、名古屋大学からは下記のSPにアクセスすることができます。Internet ExplorerやFireFoxなどのWebブラウザでそれぞれのURLにアクセスし、名古屋大学のIdPでユーザ認証を受けることによりSPが提供するサービスをご利用できます。名古屋大学のIdPでユーザ認証を受ける場合には、名古屋大学IDとそれに対応するパスワードを入力してください。

- **Science Direct**
 1. 画面右上の「Athens/Institution Login」をクリック
 2. 「Otherwise, please choose your institution's location.」から「Japanese Research and Education(UPKI-Fed)」を選択して「Go」をクリック
 3. 画面左下の「Nagoya University」をクリック
- **SpringerLink**
 1. 画面左上の「Institutional Login」をクリック
 2. 「1. Select your country:」から「Japan」を選択
 3. 「2. Select your Institution:」から「Nagoya University」を選択
 4. 「ログイン」をクリック
- **Web of Knowledge**
 1. 「Shibboleth authentication」をクリック

結果(1/3)

- 実施期間：2010年1月1日～2月28日
- 実ユーザ数：73人
- IdPへのログイン回数：179回
- SPへのアクセス回数：1,457回

結果(2/3)

アクセス回数の分布

アクセス回数	人数
1	37
2	21
3	5
4	4
5	1
6	1
10	1
12	1
14	1
22	1

SP別アクセス回数の分布

SP	アクセス回数
SpringerLink	832
GiNii	208
Science Direct	170
Web of Knowledge EndNote Web	116
OvidSP	77
Microsoft DreamSpark	35
Cambridge Journals Online	10
Pathology Images	6
FReCS MCU	3

←未接続

←未告知

結果(3/3)

部局別・身分別アクセス回数の分布

部局	教員・研究員	院生	学部学生	事務職員	図書系職員
教育学部・教育発達科学研究科		3	1		
経済学部・経済学研究科	1	1			
理学部・理学研究科	2	3	2		
工学部・工学研究科	9	6	7	1	
農学部・生命農学研究科	3				1
医学部・医学系研究科	2	3	1		
多元数理科学研究科	1				
国際開発研究科		6			
国際言語文化研究科		2			
環境学研究科	1	5			
情報科学研究科	3	5			
地球水循環研究センター	1				
附属図書館					1
情報基盤センター	1				
情報連携統括本部				1	

アンケートの結果(1/2)

回答数：5

- 全体的に考えて使い勝手は良かったですか？
 - 大変使いやすかった：1人
 - どちらかといえば使いやすかった：2人
 - どちらとも言えない：2人
- 使い勝手が良かった点は何ですか？
 - 学外からのアクセスも学内と同様に行うことができ、必要な状況で迅速に必要な論文等の情報を得ることができました。
 - 名古屋大学IDで複数サーバーにアクセス出来る点。
「なんだっけ」，にならない。
- 使い勝手が悪かった点は何ですか？
 - FirefoxでアドオンのZoteroを使用してProxyを記憶させていると，附属図書館のEZProxyと干渉する。

アンケートの結果(2/2)

- 今後も使いたいと思いますか？
 - はい：5人
 - いいえ：0人
- EZProxyとShibbolethのどちらが使いやすいと思いますか？
 - どちらかといえばEZProxyのほうが使いやすい：1人
 - どちらともいえない：1人
 - どちらかといえばShibbolethのほうが使いやすい：1人
- 他に使いたいサービスはなんですか？
 - JST文献情報提供サービス
- 自由記述
 - 学外での業務が増えており、時間と場所の制約なく文献調査ができ、文献が入手できた点でたいへん有用と感じました。継続と適応journalの拡大を希望します。
 - 今後利用が進む場合、Shibbolethで利用出来るものとそうでないものがあると結局面倒は残るのかなとも思いました。

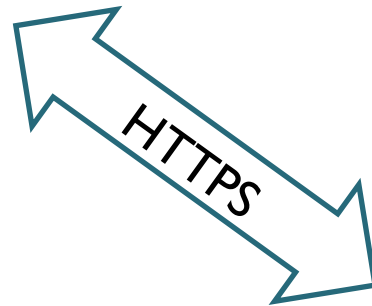


Shibboleth認証付き 分散ストレージ

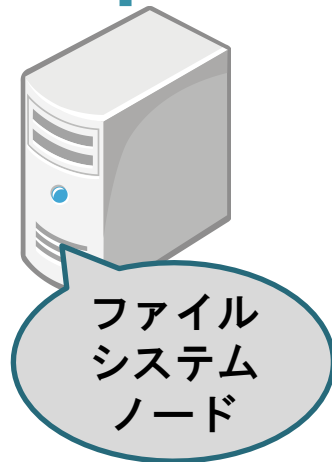
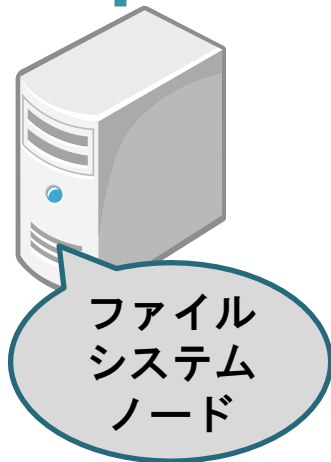
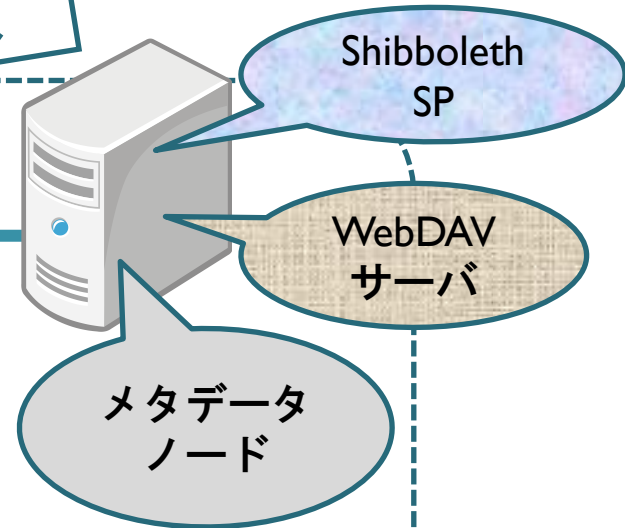
概要

- WebDAVによる分散ストレージ
 - Windows, MacOS X, Linuxなど多くのプラットフォームからアクセス可能
 - GUIおよびCUIのクライアント多数
- Gfarm上にZope/Ploneをインストール& Zope/PloneのWebDAVサーバ
 - ファイルシステムノードを地理的に分散することにより, 対障害性・対災害性の向上
 - 地理的に近いファイルシステムノードから読み書きすることにより, パフォーマンス向上
- Zope/PloneをShibboleth化

構成(1/2)



Gfarmによる分散ストレージ



構成(2/2)

Shibboleth

←SSO

Apache + mod_ssl

←HTTPS

WebDAV

←分散ストレージの公開

Zope/Plone

←コンテンツに対する
アクセスコントロール

Gfarm

←分散ストレージ

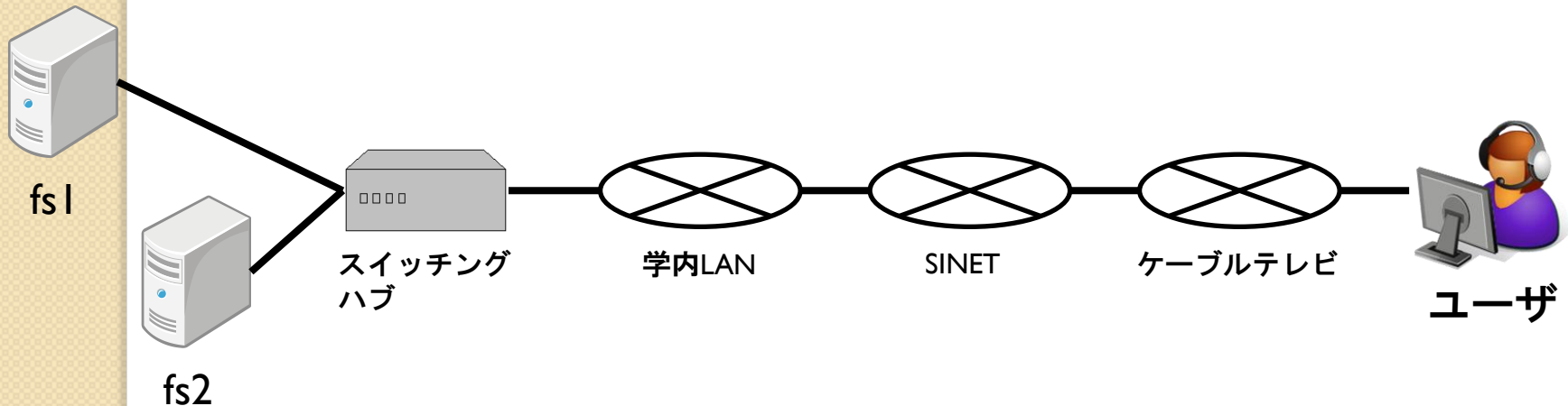
WebDAVフォルダに対するアクセス制限



- PloneのコンテンツとしてWebDAV用のフォルダを作成
- ユーザIDと所属機関を指定して，アクセスコントロールを行うことが可能

実験環境

- 名古屋大学に設置した2台のサーバ
 - fs1: メタデータサーバ, ファイルシステムノード, Shibboleth SP, Zope/Plone サーバ
 - fs2: ファイルシステムノード
- fs1とfs2はGigabit ethernetで同一のスイッチングハブを介して接続
- 実験で用いるデータ
 - 60個のファイルと25個のフォルダからなる150MBのデータ



実験内容

- ユーザビリティとパフォーマンスの評価
 - 書き込み時間
 - 分散ストレージ化されたファイルシステムに対する、WebDAVフォルダへの書き込み時間とsftpによる書き込み時間を比較
 - 自宅からアップロード(ケーブルテレビ→商用回線→SINET3→学内LAN)
 - レプリケーションの時間
 - fs1からfs2へのレプリケーション時間
 - 耐障害性
 - fs1(Zope/Ploneが稼働)のファイルシステムノードを停止した状態でWebDAVフォルダにアクセス

結果

- **書き込み時間**
 - クライアント
 - WebDAV クライアント: CarotDAV
 - sftp クライアント: FileZilla
 - **書き込み時間: 約20分 (WebDAV, sftp とも)**
- **レプリケーションの時間**
 - 5分程度
- **耐障害性**
 - Zope/PloneのコンテンツおよびWebDAVフォルダへの読み書きが可能

考察

- 書き込み時間はsftpと同程度
 - 実用上の問題無し
- レプリケーション時間は5分程度
 - 今回のデータ(150MB)では問題無し
 - 大規模化した場合には、負荷分散や更新分のみのレプリケーションなどが必要
- 耐障害性
 - Gfarmのファイルシステム内にZope/Ploneをインストールすることにより、堅牢性が向上