



ID一元管理を実現する - OpenIDの紹介 (OpenID Authentication1.1)

2007年12月07日

XMLコンソーシアムDay

セキュリティ部会 林 正樹(富士通株式会社)



OpenID?? とは

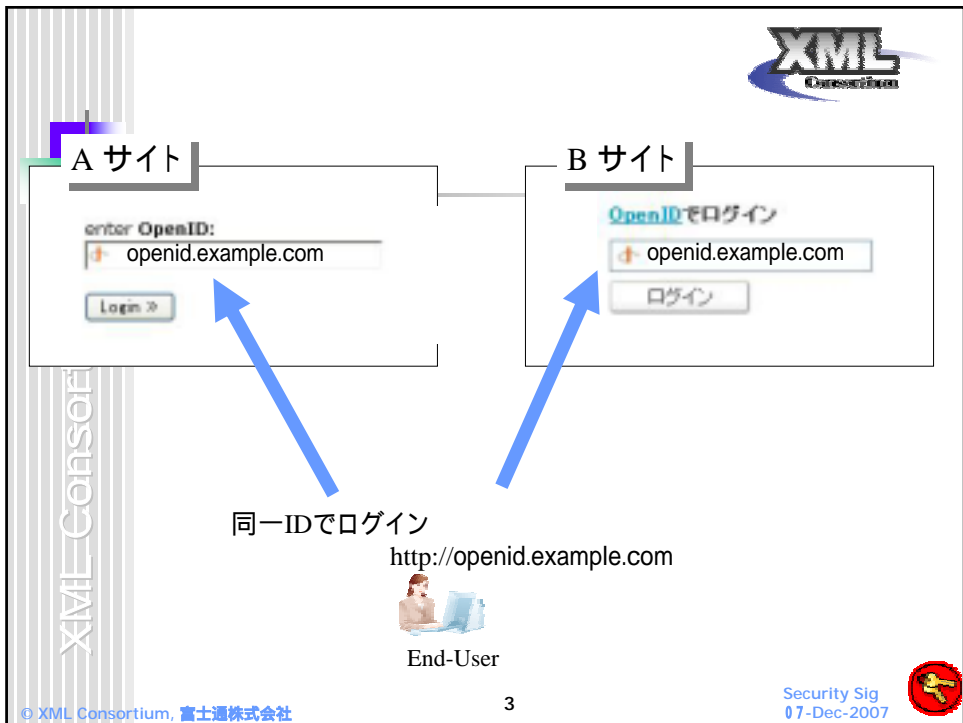
2005年秋 Six apart社のBrad Fitzpatric氏によって提唱

IDとしてURLを利用した一元管理する認証技術

OpenIDの仕様は、The OpenID Foundationで策定
(<http://openid.net>)

現在の仕様: OpneID Authentication 1.1





How do I get an OpenID ?

OpenID.net

How do I get an OpenID?

Surprise! You may already have one. If you use any of the services listed below, you already have your own OpenID.

- id.me**
openid.id.me/
- LiveDoor**
profile.livedoor.com/
- LiveJournal**
username.livejournal.com
- Orange (France Telecom)**
http://openid.orange.fr/
- Drupal**
username.drupal.com
- Technorati**
technorati.com/people/technorati/
- Yves**
member.yves.com
- WordPress.com**
username.wordpress.com

Well Known & Simple Providers

If you don't have an OpenID yet, here are a few which are generally recommended for various members of the community. In the end you should choose a provider from a company which you trust, see reader the list just perfect and plan to evolve it into a more useful tool.

- id.me**
id.me is the free, easy way to manage your online identity with OpenID.
- myID.net**
Free OpenID Provider with support for groups and three languages.
- myOpenID**
Secure, free, instant OpenID service by Sphero.
- myVidooop**
Free OpenID Provider that integrates perfectly with security features, customization, and service integration.

If you're more curious about the technology, you can also have more about the features that some of the popular providers offer.

All Providers

For a list of more OpenID Providers, check the list on the site. We don't make any guarantee about the providers listed, though most are quite good!

© XML Consortium

XML Consortium

OpenID.ne.jp

1回のみ登録と1つのアカウントでOpenIDを認証するすべてのサイトに、すぐ登録することが出来ます。

海外サイト一覧 (英語)

- MailChimp http://www.mailchimp.com
- Hungry http://www.hungry.com/usa
- Zicomm.com http://www.zicomm.com/usa
- Ma.gnolia.com http://ma.gnolia.com/signin
- Stir http://stir.kia.com/oc/openid/one
- Opnity.com http://www.opnity.com
- Wikivote http://wikivote.org/en/Special:OpenIDLogin
- Twitter http://twitter.com
- Woojab http://www.wojab.com
- LiveJournal http://www.livejournal.com/openid
- Wikipedia http://www.wikipedia.org/(日本語)
- Bohannon.com http://bohannon.com
- State http://state.com
- Rufus http://rufus.mediamt.edu
- Doory http://doory.com
- Widensity http://www.widensity.com
- TakeEverything! http://www.takeeverything.com
- Wiki http://wiki.kibot.net
- asentyls http://asentyls.org
- I want my OpenID http://wantmyopenid.org
- multipedia http://www.multipedia.com/openid.php
- DeadJournal http://www.deadjournal.com/openid
- RadCarly.com http://www.radcarly.com
- NeedBark http://www.needbark.net
- People Aggregator http://www.peopleaggregator.com
- Planet.org http://www.planet.org
- OpenID Enabled http://www.openidenabled.com
- Client http://client.com

国内サイト (日本語対応)

- Chob http://www.chob.jp
- LiveJournal http://www.livejournal.com/openid
- Zicomm.com http://www.zicomm.com/usa
- Mobile Top Weblog http://www.smart.com/mobiletop
- Place Drops http://www.placedrops.com/ask/login
- FreeStyleWeb http://fsweb.jp/
- Hara In http://www.hara.in
- アイドナー http://aidner.jp
- Stack Stack Doka http://stack.kayshaya.jp/

© XML Consortium, 富士通株式会社

07-Dec-2007

XML Consortium

米国の全国紙 USA Today に掲載

Technology cuts down on Web registrations (2007年3月15日)

Technology cuts down on Web registrations

By Lee Ann Szymanski

OPENING DOOR TO OPENID

OpenID technology lets consumers use the same user name and password for hundreds of websites that require a sign-in.

	2006	2007 (1)
Digital users (in millions)	75	200-250
OpenID-enabled sites	1,200	10,000-15,000
New sites added daily	20-25	40-50

1-estimate, Source: ianRain

© XML Consortium, 富士通株式会社

07-Dec-2007



The State of OpenID

Scott Kveton氏 (Board Member, OpenID Foundation)から



XML Consortium

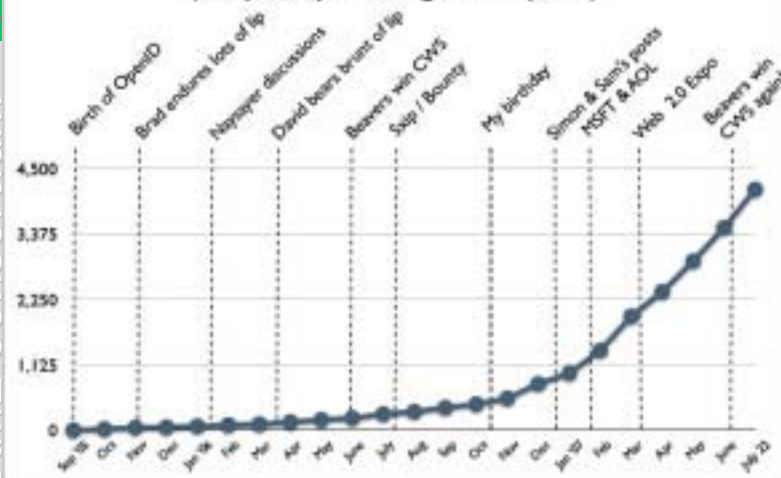
~120 million OpenID's

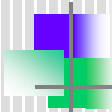
(including **every** AOL and LiveJournal user)



Total Relying Parties

(aka places you can login with OpenID)





OpenID Authentication1.1 (Abstract)

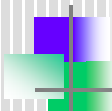
OpenID Authenticationは、End Userが所有しているIdentity URLを証明する方法を提供。

ConsumerやIdentity Providerになるため特別な認可は不要

JavaScriptや特別なbrowsersを必要としない

・AJAX styleのsetupを使った認証方法が可能。

profile情報の交換方法については、拡張機能(Extentions)として仕様策定が進められている。



Terminology

End User

Consumerに対して、自分のIdentityを証明しようとするユーザ
(Serviceの利用者)

Identifier

Identifier = URL

OpenID Authentication protocolのすべてのフローはEnd Userが所有しているURLを証明すること。

Claimed Identifier

Consumerによって、立証されていないIdentifier

Verified Identifier

Consumerによって立証されたIdentifier

(IDPと連携してClaimed IdentifierをConsumerが立証)



Terminology (続き)

Consumer

Claimed Identifierの立証を必要としている Web Service
(OpenIDの認証に対応したWeb Serviceを提供)

Identity Provider

OpenID認証サーバ. IDP、Serverと呼ばれている。

ConsumerがClaimed Identifierを立証してもらうために、問い合わせる相手。

End UserとIDPの認証方法については、仕様の範囲外

User-Agent

End Userのweb browser。

特別なPlug-insやJavaScriptは不要。



OpenID 認証の仕組み

Transforming a HTML Document into an Identifier

ConsumerがIDPを知る方法

Claimed Identifier (URL)が示すHTMLドキュメント
にIDPの情報(タグ)を追加

Claimed Identifier(URL)とIDPはhostが別でも構わない





Transforming a HTML Document into an Identifier

End UserのID
(Identifier: <http://example.com>)

IDP
<http://openid.example.com>



← End UserのIDを証明



Transforming a HTML Document into an Identifier

End UserのID
(Identifier: <http://example.com>)

IDP
<http://openid.example.com>



← End UserのIDを証明

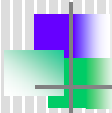


Claimed Identifier (<http://example.com>)
のHTMLドキュメントに以下のタグを追加

```
<head>  
<link rel="openid.server" href=http://openid.example.com/>  
...  
</head>
```



Delegating Authentication

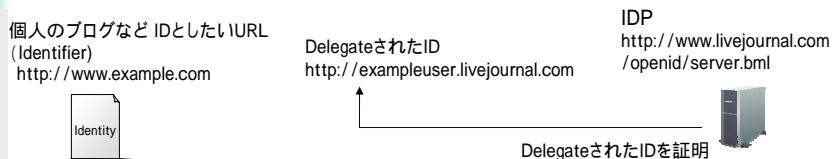
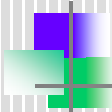


Delegating Authenticationとは
IDとして、個人のブログなどのURLを利用することが可能

Delegating Authenticationを使うメリット
OpenIDとして使う Server (IDP)が変わった場合でも
Delegateする相手を変えるだけで、変更を吸収することが
可能
OpenID Identityを何年も変わらず保持することが可能



Delegating Authentication



Claimed Identifier (http://example.com)
のHTMLドキュメントに以下のタグを追加

```
<head>
<link rel="openid.server"
ref="http://www.livejournal.com/openid/server.bml">
<link rel="openid.delegate" href="http://exampleuser.livejournal.com/">
...
</head>
```



Smart Mode / Dumb Mode



XML Consortium

ConsumerとIDP間の認証手続きの方法

Smart Mode

(the highly recommended mode)

ConsumerとIDP間で、最初に行われる認証手続

共通鍵の生成とセッション保持(state full)

IDPからの認証結果情報の確認処理に利用

Dumb Mode(stateless)

共通鍵とセッションを保持しない(stateless)

IDPからの認証結果情報後に、再度認証確認を行う

必要あり

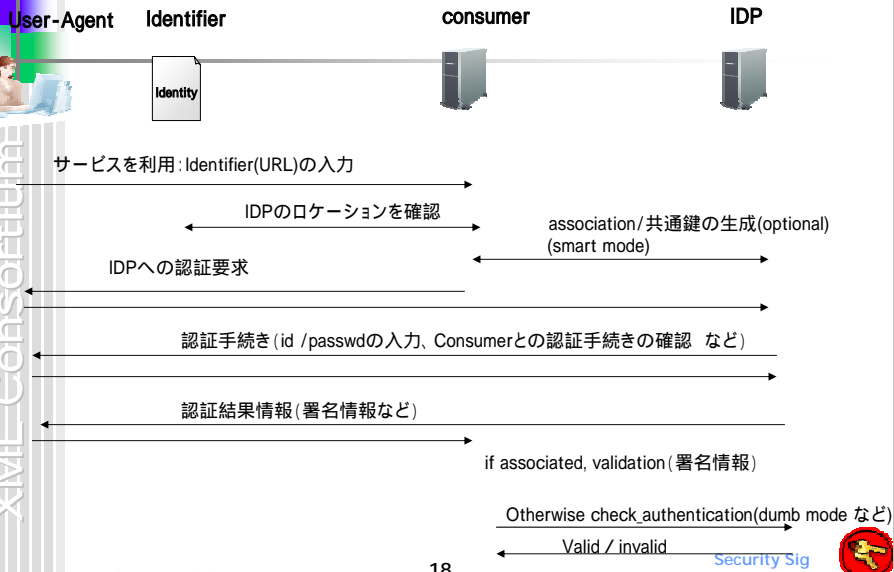
check_authentication



シーケンス



XML Consortium



トレース情報(at User-Agent)



User-Agent
FireFox

Identifier
http://profile.livedoor.com/hayashi_masaki



Consumer
PlaceEngine
<http://www.placeengine.com/>

IDP
<http://auth.livedoor.com>



サービスを利用: Identifier(URL)の入力 (User Agent Consumer) (20)



```
POST /auth/login HTTP/1.1
Host: www.placeengine.com
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.2; ja; rv:1.8.1.7) Gecko/20070914 Firefox/2.0.0.7
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
Accept-Language: ja,en-us;q=0.7,en;q=0.3
Accept-Encoding: gzip,deflate
Accept-Charset: Shift_JIS,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Referer: http://www.placeengine.com/auth/login
Cookie: _pe_session_id=e851bf379c9a30b62295c64025eed95b
Content-Type: application/x-www-form-urlencoded
Content-Length: 80
```

openid_url=http://3A%2F%2Fprofile.livedoor.com%2Fhayashi_masaki&login=Login+%C2%BB





IDPへの認証要求 (User Agent Consumer) (21)

HTTP/1.1 302 Found
 Date: Sat, 06 Oct 2007 01:47:48 GMT
 Server: lighttpd/1.4.10
 Content-Type: text/html; charset=utf-8
 Set-Cookie: _pe_session_id=e851bf379c9a30b62295c64025eed95b; path=/
 Cache-Control: no-cache
 Location: http://auth.livedoor.com/openid/server?openid.mode=checkid_setup&openid.return_to=http%3A%2F%2Fwww.placeengine.com%2Fauth%2Fcomplete%3Fnonce%3DfLHNGcbd&openid.trust_root=http%3A%2F%2Fwww.placeengine.com%2F&openid.identity=http%3A%2F%2Fprofile.livedoor.com%2Fhayashi_masaki&openid.assoc_handle=1191600403%3AwjZT4Vi9ufygMfQza2oK%3Af2ef1522fb
 Connection: close
 Transfer-Encoding: chunked

XML Consortium



IDPへの認証要求(request) (User Agent IDP) (29)

GET
 /openid/server?openid.mode=checkid_setup&openid.return_to=http%3A%2F%2Fwww.placeengine.com%2Fauth%2Fcomplete%3Fnonce%3DfLHNGcbd&openid.trust_root=http%3A%2F%2Fwww.placeengine.com%2F&openid.identity=http%3A%2F%2Fprofile.livedoor.com%2Fhayashi_masaki&openid.assoc_handle=1191600403%3AwjZT4Vi9ufygMfQza2oK%3Af2ef1522fb HTTP/1.1
 Host: auth.livedoor.com
 User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.2; ja; rv:1.8.1.7) Gecko/20070914 Firefox/2.0.0.7
 Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
 Accept-Language: ja,en-us;q=0.7,en;q=0.3
 Accept-Encoding: gzip,deflate
 Accept-Charset: Shift_JIS,utf-8;q=0.7,*;q=0.7
 Keep-Alive: 300
 Connection: keep-alive
 Referer: http://www.placeengine.com/auth/login
 Cookie: auth_sid=5df29c4847f0544e3a97108b3e18734a

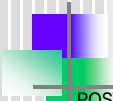
XML Consortium





トレース情報

認証手続 (User Agent IDP)(56)



XML Consortium

POST /login/index HTTP/1.1

Host: member.livedoor.com

User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.2; ja; rv:1.8.1.7) Gecko/20070914 Firefox/2.0.0.7

Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5

Accept-Language: ja,en-us;q=0.7,en;q=0.3

Accept-Encoding: gzip,deflate

Accept-Charset: Shift_JIS,utf-8;q=0.7,*;q=0.7

Keep-Alive: 300

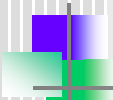
Connection: keep-alive

Referer:

http://member.livedoor.com/login/?next=http%3A%2F%2Fauth.livedoor.com%2Fopenid%2Fapprove%3Freturn_to%3Dhttp%3A%2F%2Fwww.placeengine.com%2Fauth%2Fcomplete%253Fnonce%253DfLHNGcbd%26identity%3Dhttp%3A%2F%2Fprofile.livedoor.com%2Fhayashi_masaki%26assoc_handle%3D1191600403%3AwjZT4Vi9ufygMfQza2oK%3Af2ef1522fb%26trust_root%3Dhttp%3A%2F%2Fwww.placeengine.com%2F&sv=auth

Cookie: mem_sid=ab61ac9455df7e7fc778b9ca0ae1896f

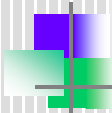
Content-Type: application/x-www-form-urlencoded



XML Consortium

next=http%3A%2F%2Fauth.livedoor.com%2Fopenid%2Fapprove%3Freturn_to%3Dhttp%3A%2F%2Fwww.placeengine.com%2Fauth%2Fcomplete%253Fnonce%253DfLHNGcbd%26identity%3Dhttp%3A%2F%2Fprofile.livedoor.com%2Fhayashi_masaki%26assoc_handle%3D1191600403%3AwjZT4Vi9ufygMfQza2oK%3Af2ef1522fb%26trust_root%3Dhttp%3A%2F%2Fwww.placeengine.com%2F&sv=auth&livedoor_id=hayashi_masaki&password=hayashi





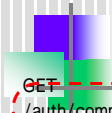
認証結果情報 (User Agent IDP)(73)

HTTP/1.1 302 Found
Date: Sat, 06 Oct 2007 01:48:15 GMT
Server: Apache/1.3.37 (Unix) mod_perl/1.29

Location:

http://www.placeengine.com/auth/complete?nonce=fLHNGcbd&openid.mode=id_res&openid.identity=http://profile.livedoor.com/hayashi_masaki&openid.return_to=http://www.placeengine.com/auth/complete%3Fnonce%3DFLHNGcbd&openid.assoc_handle=1191635295:STLS.8k6eljbA52Yh6zquicCz:e29bfba967&openid.signed=mode,identity,return_to&openid.invalidate_handle=1191600403:wjZT4Vi9ufygMfQza2oK:f2ef1522fb&openid.sig=L8moFbSXcULy3U3aSmbicd8DBJk%3D

Content-Type: text/plain
Vary: Accept-Encoding,User-Agent
Content-Encoding: gzip
Content-Length: 20



認証結果情報(response) (User Agent Consumer)(77)

GET

/auth/complete?nonce=fLHNGcbd&openid.mode=id_res&openid.identity=http://profile.livedoor.com/hayashi_masaki&openid.return_to=http://www.placeengine.com/auth/complete%3Fnonce%3DFLHNGcbd&openid.assoc_handle=1191635295:STLS.8k6eljbA52Yh6zquicCz:e29bfba967&openid.signed=mode,identity,return_to&openid.invalidate_handle=1191600403:wjZT4Vi9ufygMfQza2oK:f2ef1522fb&openid.sig=L8moFbSXcULy3U3aSmbicd8DBJk%3D HTTP/1.1

Host: www.placeengine.com
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.2; ja; rv:1.8.1.7) Gecko/20070914 Firefox/2.0.0.7
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9;text/plain;q=0.8,image/png,*/*;q=0.5
Accept-Language: ja,en-us;q=0.7,en;q=0.3
Accept-Encoding: gzip,deflate
Accept-Charset: Shift_JIS,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Referer: http://auth.livedoor.com/openid/approve?return_to=http://www.placeengine.com/auth/complete%3Fnonce%3DFLHNGcbd&identity=http://profile.livedoor.com/hayashi_masaki&assoc_handle=1191600403:wjZT4Vi9ufygMfQza2oK:f2ef1522fb&trust_root=http://www.placeengine.com/





最後に今後の動向



OpneID Authentication2.0 (Draftxx)

Updated Initiation and Discovery

Supports OP Identifiers

XRI - XRDS のサポート

URL - Yadisプロトコルの使用 :XRDS

HTML-Base discovery

multiple Ops for a single Identifier

supported extensions

セキュリティの強化

replay attacksの強化 : nonce

new association type :HMAC-SHA256

new association session type:DH-SHA256

