

OpenID 認証 2.0

～概論～

社内勉強会 - www.feedforce.jp

suzuki@feedforce.jp

OpenID認証は
エンドユーザーが管理する
Identifierを証明する方法を
提供します。

本日の予定

- 特徴
- 用語
- 概観と実例
- セキュリティ
- おまけ

特徴

- 「オープン」
- 「秘密情報の保護」
- 「分散的」
- 「HTTP」
- 「拡張」

「オープン」

「秘密情報の保護」

「分散的」

「HTTP」

「擴張」

用語

- Identifier
- User-Agent
- Relying Party
- OpenID Provider
- OP Endpoint URL
- OP Identifier
- User-Supplied Identifier
- Claimed Identifier
- OP-Local Identifier

Identifier

User-Agent

Relying Party
(=RP)

OpenID Provider (=OP)

OP Endpoint URL

OP Identifier

User-Supplied Identifier

Claimed Identifier

OP-Local Identifier

概観と実例

- 認証の手続きの概観
- Yahoo! JAPANとFastladderの例

(7) 照合
(2) 発見

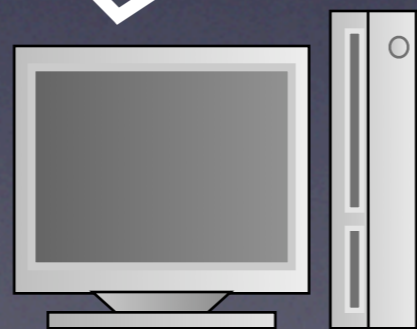
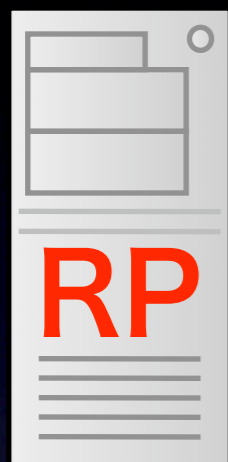
(5) ユーザー
を認可

(3) 関連づけ
(任意)

(6) 承認/却下

(1) 開始

(4) 認証要求



開始

The image shows a login interface with the following elements:

- Email address:** A text input field.
- Password:** A text input field.
- Sign in:** A button.
- forgot your password?:** A blue link.
- Sign in with OpenID:** A section highlighted by a red dashed box, containing:
 - OpenID field:** A text input field containing "yahoo.co.jp".
 - Sign in / Create Account:** A button.
- or:** A separator text.
- Sign In with a Yahoo! ID:** A yellow button with the Yahoo! logo.

A red arrow points from the bottom of the red dashed box to the "Sign in / Create Account" button.

入力してボタンをクリック！！

正規化

yahoo.co.jp



http://yahoo.co.jp/

発見

```
$ curl -LI http://yahoo.co.jp/
HTTP/1.1 302 Found
...
Location: http://www.yahoo.co.jp/index.html
...
HTTP/1.1 200 OK
...
X-XRDS-Location: http://open.login.yahoo.co.jp/openid20/www.yahoo.co.jp/xrds
...
```

```
$ curl -i http://open.login.yahoo.co.jp/openid20/www.yahoo.co.jp/xrds
HTTP/1.1 200 OK
...
Content-Type: application/xrds+xml

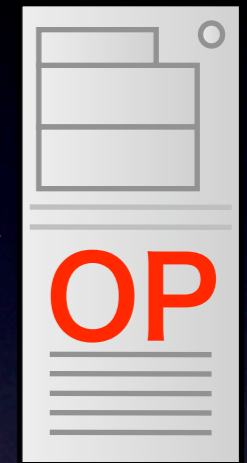
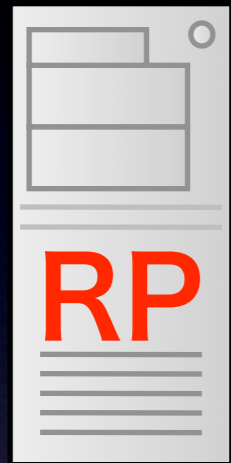
<?xml version="1.0" encoding="UTF-8"?>
<xrds:XRDS
  xmlns:xrds="xri://$xrds"
  xmlns:openid="http://openid.net/xmlns/1.0"
  xmlns="xri://$xrd*($v*2.0)">
  <XRD>
    <Service priority="0">
      <Type>http://specs.openid.net/auth/2.0/server</Type>
      <URI>https://open.login.yahooapis.jp/openid/op/auth</URI>
    </Service>
  </XRD>
</xrds:XRDS>
```

関連づけ (任意)

Diffie-Hellman鍵共有

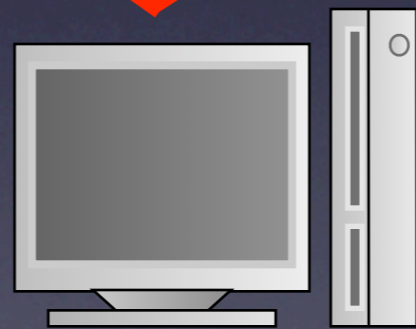


認証要求



<OP Endpoint URL>+<認証要求パラメータ>

- openid.ns
- openid.mode
- openid.claimed_id
- openid.identity
- openid.assoc_handle
- openid.return_to
- openid.realm



ユーザー認可

Yahoo! JAPAN ID:

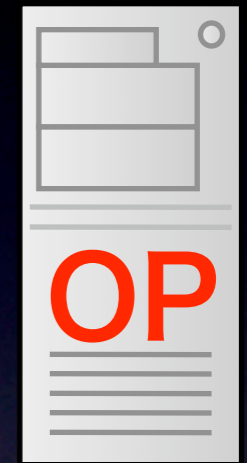
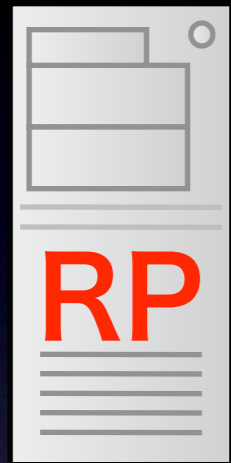
パスワード:

次回からIDの入力を省略
最長で2週間ログイン状態を維持できます。
共用のパソコンではチェックを外してください。

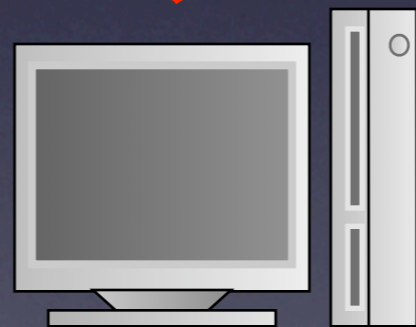
 ログイン

モード: [標準\(http\)](#) | [SSL\(https\)](#)

承認 or 却下



承認 or 却下



- openid.ns
- openid.mode
- openid.op_endpoint
- openid.claimed_id
- openid.identity
- openid.return_to
- openid.response_nonce
- openid.invalidate_handle
- openid.assoc_handle
- openid.signed
- openid.sig

照合

- 戻りURL
- nonce
- 発見した情報
- 署名

Create New Account

Note: If you already have a Fastladder account, [link your OpenID to your Fastladder account](#).

OpenID `https://me.yahoo.co.jp/a/Ya_JyXB8ZPujNdvm800HJ837_LRI7UJ11__x#7c4d5`

User ID

User ID may contain a-z, 0-9, and dashes.

I have read and agreed to the [Terms of Service](#) and [Privacy Policy](#).

Create Account

照合成功 => 認証完了

(7) 照合
(2) 発見

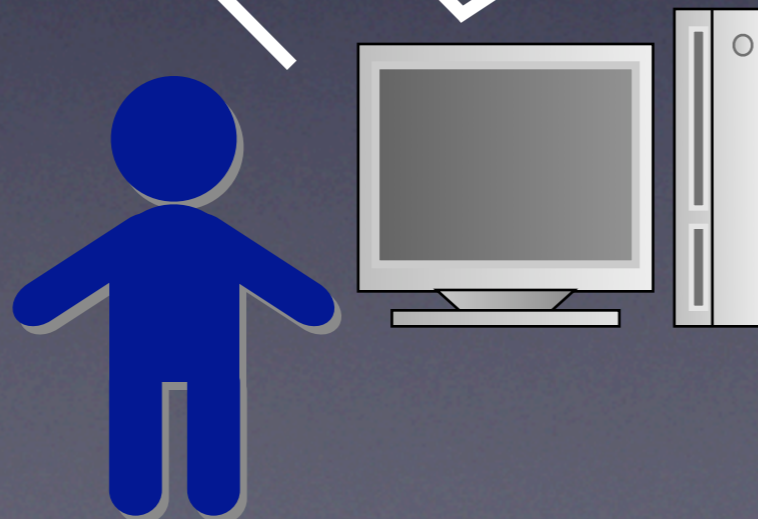
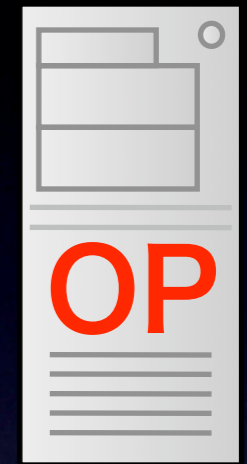
(5) ユーザー
を認可

(3) 関連づけ
(任意)

(6) 承認/却下

(1) 開始

(4) 認証要求



実例

- OPはYahoo! JAPAN
- RPはFastladder
- いくつかの始め方を紹介
- Identifierに注目

実例

- OP Identifierで始める
- OP-Local Identifierで始める
- HTMLのURLで始める
- Yadis IDで始める

OP Identifier

- <http://fastladder.com>
- yahoo.co.jp

OP-Local Identifier

- <http://fastladder.com>
- [https://me.yahoo.co.jp/a/
Ya_JyXB8ZPujNdvm800HJ837_LRI
7UJII_x](https://me.yahoo.co.jp/a/Ya_JyXB8ZPujNdvm800HJ837_LRI7UJII_x)

HTMLのURL

- <http://fastladder.com>
- <http://lab.koshigoe.jp/openid2.html>

Yadis ID

- <http://fastladder.com>
- <http://id.koshigoe.jp>

セキュリティ

- 攻撃の予防
- User-Agent
- UI
- DoS攻撃
- 信頼性/評価

盗聴の予防

中間者攻撃の予防

Proxyの予防

User-Agent

UI

DoS攻撃

信賴性/評價

おまけ

- 参照
- OPとRPの対応状況
- 日本での活動
- 関連情報

<http://openid.net/developers/specs/>

<http://openid.net/Libraries>

http://www.atmarkit.co.jp/fsecurity/index/index_openid.html

OPとRP

- OP

- Yahoo! JAPAN
- はてな
- Livedoor
- Blogger
- など

- RP

- Fastladder
- はてな
- LiveJournal
- など

日本での活動

- アイデンティティ飲み会
- Liberty Alliance 技術セミナー
- openid-ja
- ブログで議論

おしまい