

OAuth入門



OSSTech

2012年4月24日
辻口 鷹耶

オープンソース・ソリューション・テクノロジー株式会社

<http://www.osstech.co.jp/>

お問い合わせ info@osstech.co.jp

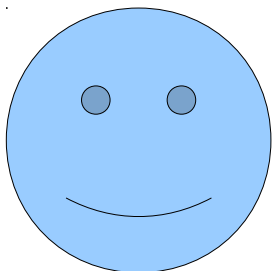
目次

- OAuthについて
 - OAuthの背景
 - OAuthの歴史
 - プロトコル概要(OAuth2.0)
- OpenAMにおけるOAuth

OAuthについて

OAuthの背景

ユーザ



OAuth登場以前は。。。。

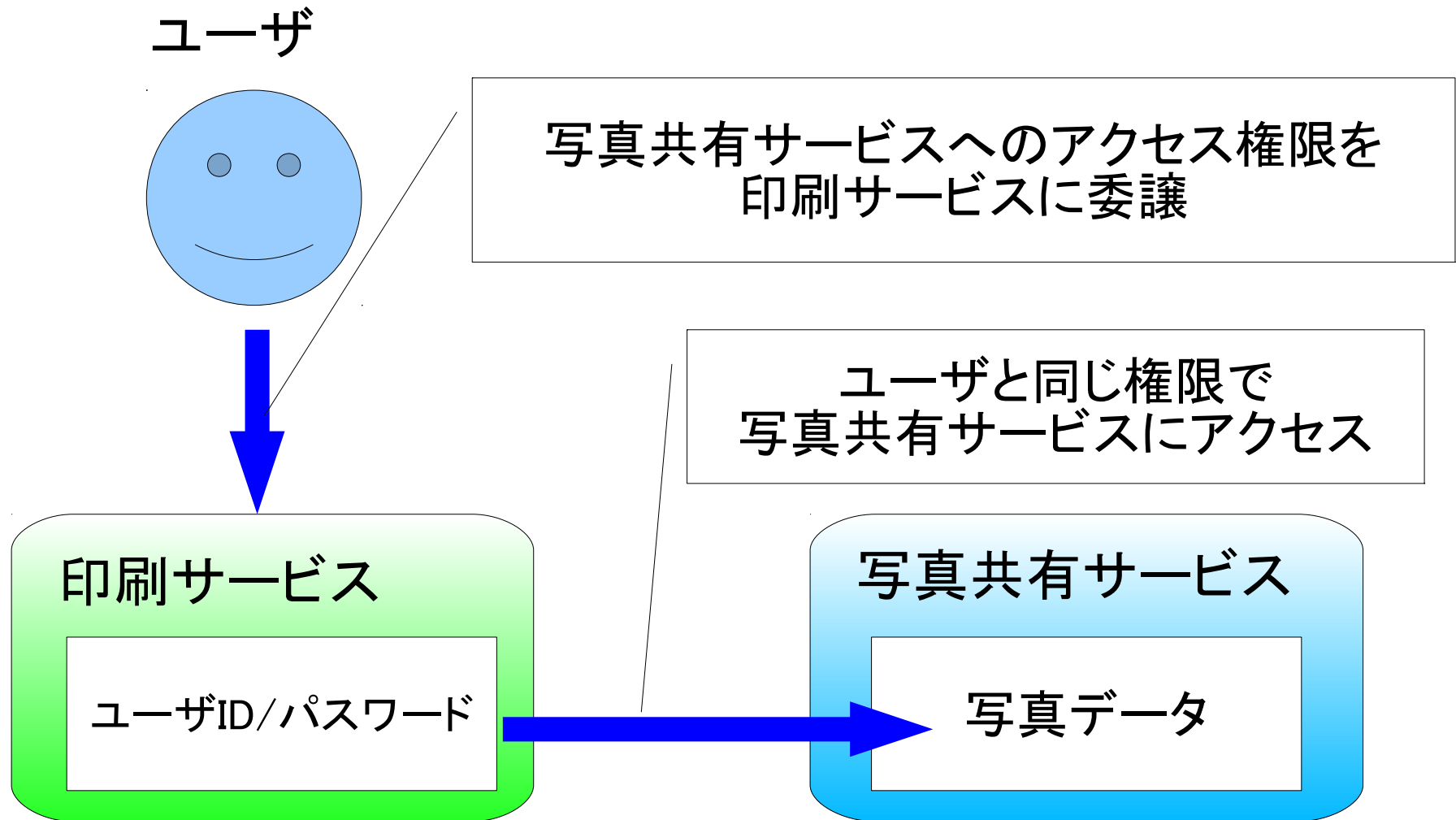
写真共有サービスにある写真を
印刷サービスで印刷したい

印刷サービス

写真共有サービス

写真データ

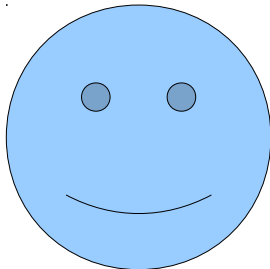
OAuthの背景



OAuthの背景

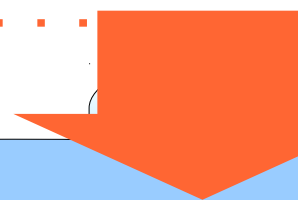
アクセス権限の委譲の問題点：

ユーザ



印刷サービス

- 後の使用のために、クライアント（印刷サービス）にもパスワードを保存しなければならない
- リソースサーバー（写真共有サービス）はパスワード認証をサポートする必要がある
- ユーザと同じ権限のため、リソース（写真）に対する権限を限定できない
- 情報漏えいのリスクが大きい



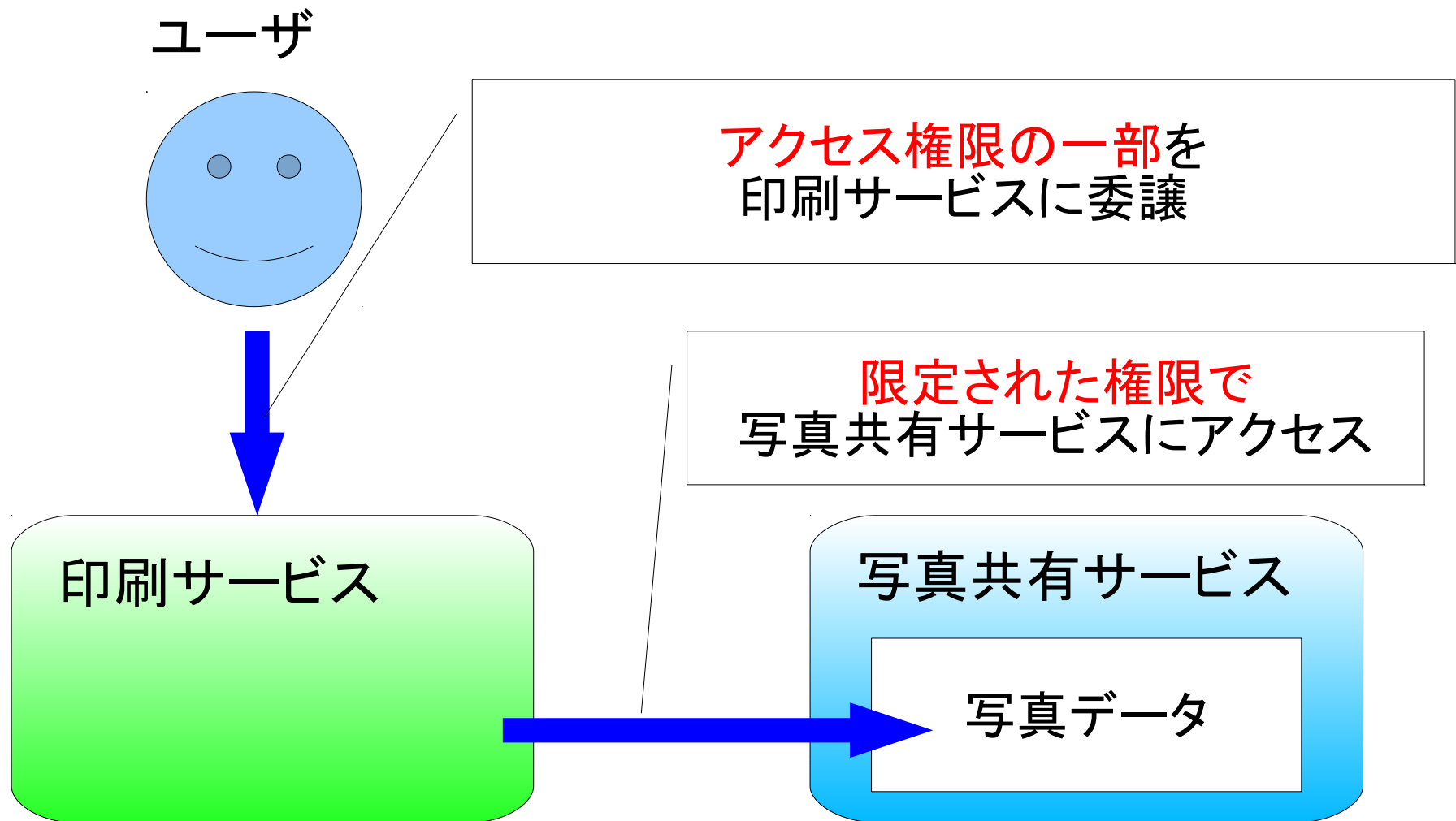
共有サービス

OAuth登場

OAuthとは

- クライアントに対してリソースオーナーが同意することで限定されたアクセス権を委譲するための認可の protocols
- パスワードを共有することなく、ユーザ（リソースオーナー）がクライアントにリソースの使用を許可することが可能になる
- アクセス権限を限定できる

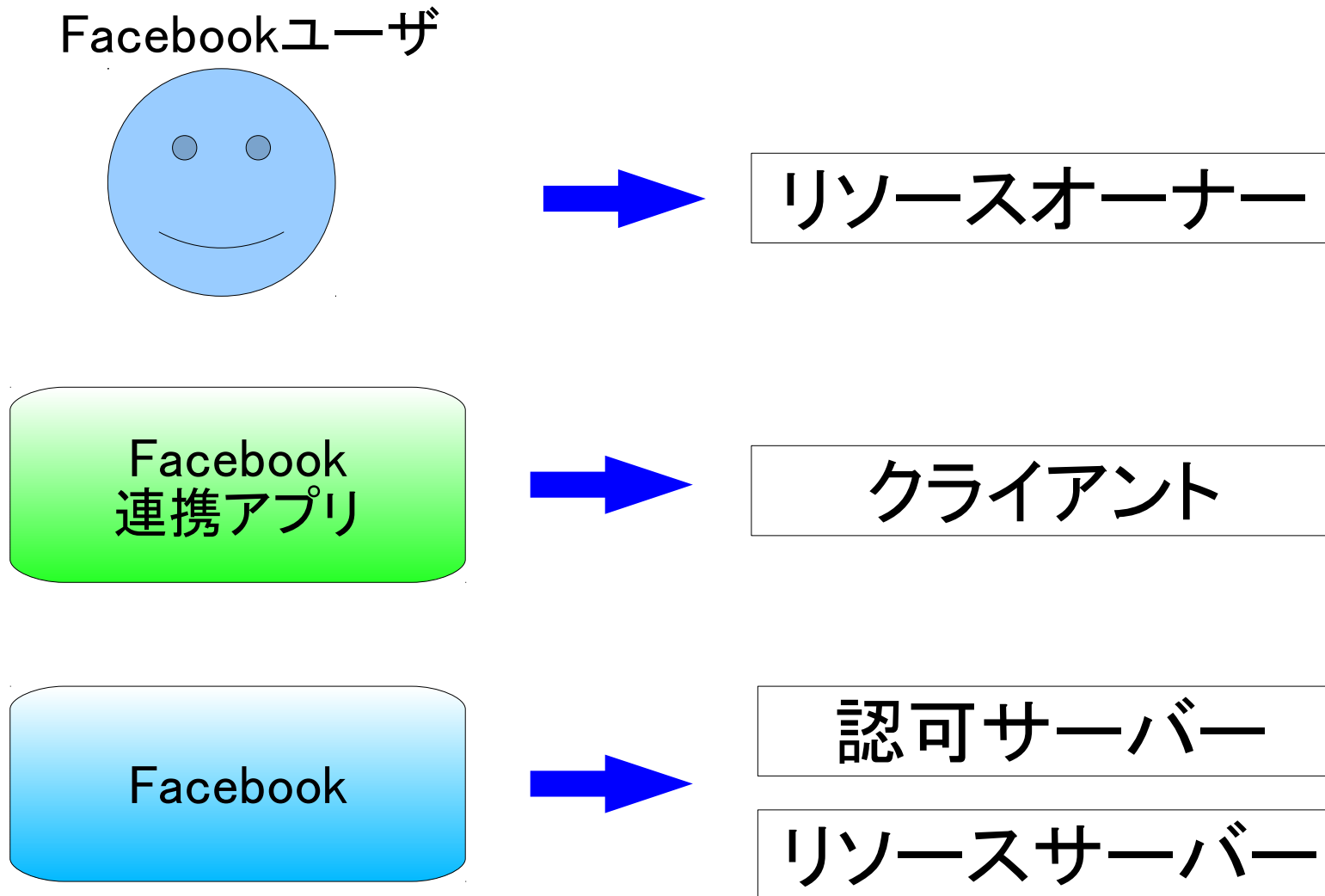
OAuthを利用すると



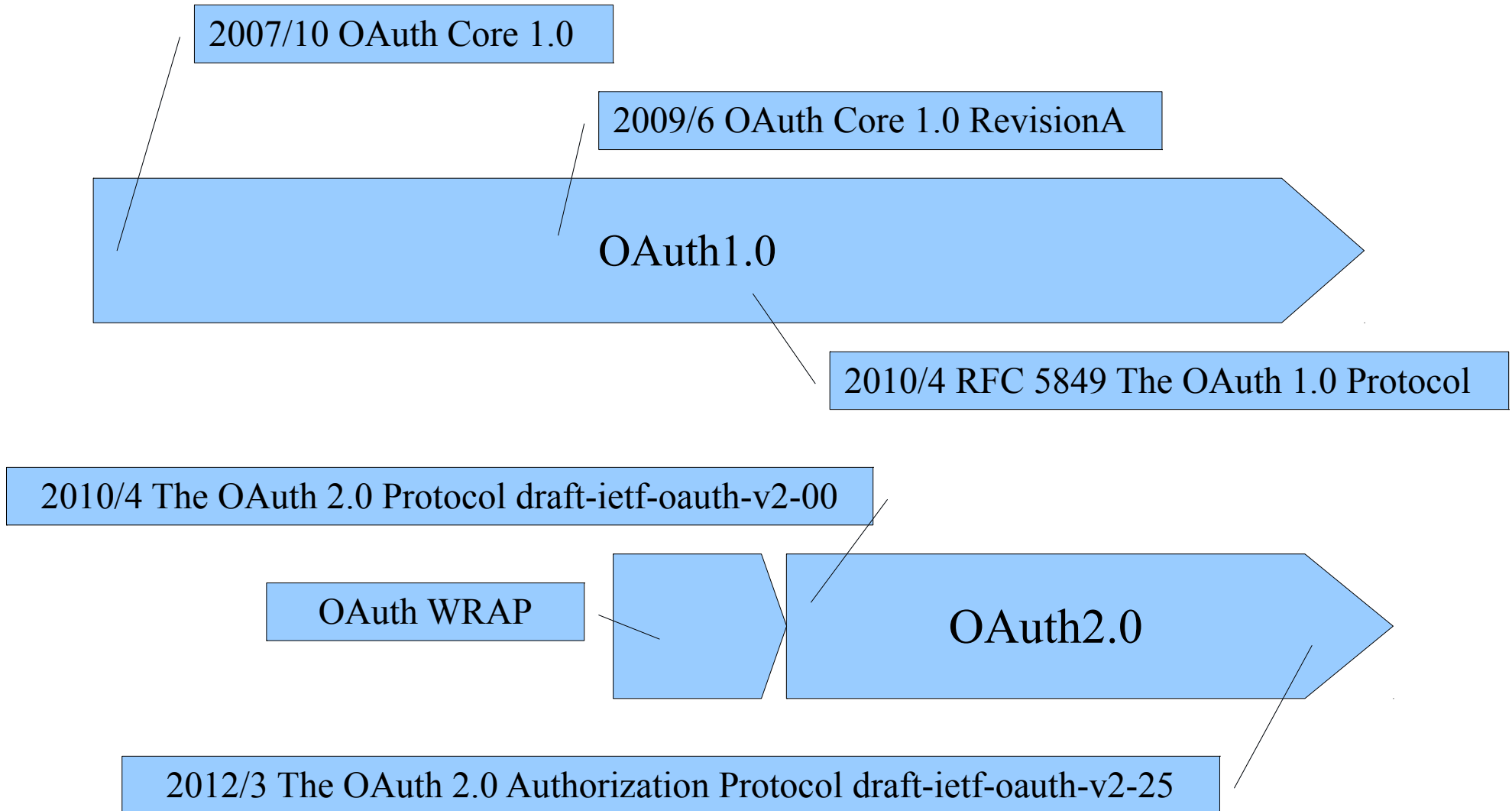
OAuthでの役割

- **リソースオーナー**
リソースの所有者です。
リソースへのアクセスを許可します。
- **リソースサーバー**
リソースを保持するサーバーです。
資格情報(アクセストークン)を提示したアクセス要求に応答します。
- **クライアント**
リソースオーナーの代理としてリソースにアクセスするアプリケーションです。
- **認可サーバー**
リソースオーナーの認証し、アクセストークンをクライアントに発行するサーバーです。

OAuthでの役割(例: Facebook)



OAuthの歴史



OAuth1.0 の課題

Eran Hammer氏の「Introducing OAuth 2.0」より

- 署名と複雑な認証

仕様で求められる暗号化手法が複雑で実装しにくい。

- WEBアプリケーション以外で上手く機能しなかった

策定当初はデスクトップアプリやモバイルデバイスのフローもあったが、すべて機能するようにマージした結果、機能しなかった。

- スケールしにくい

捨てられる一時認証情報を保持しておく必要がある。

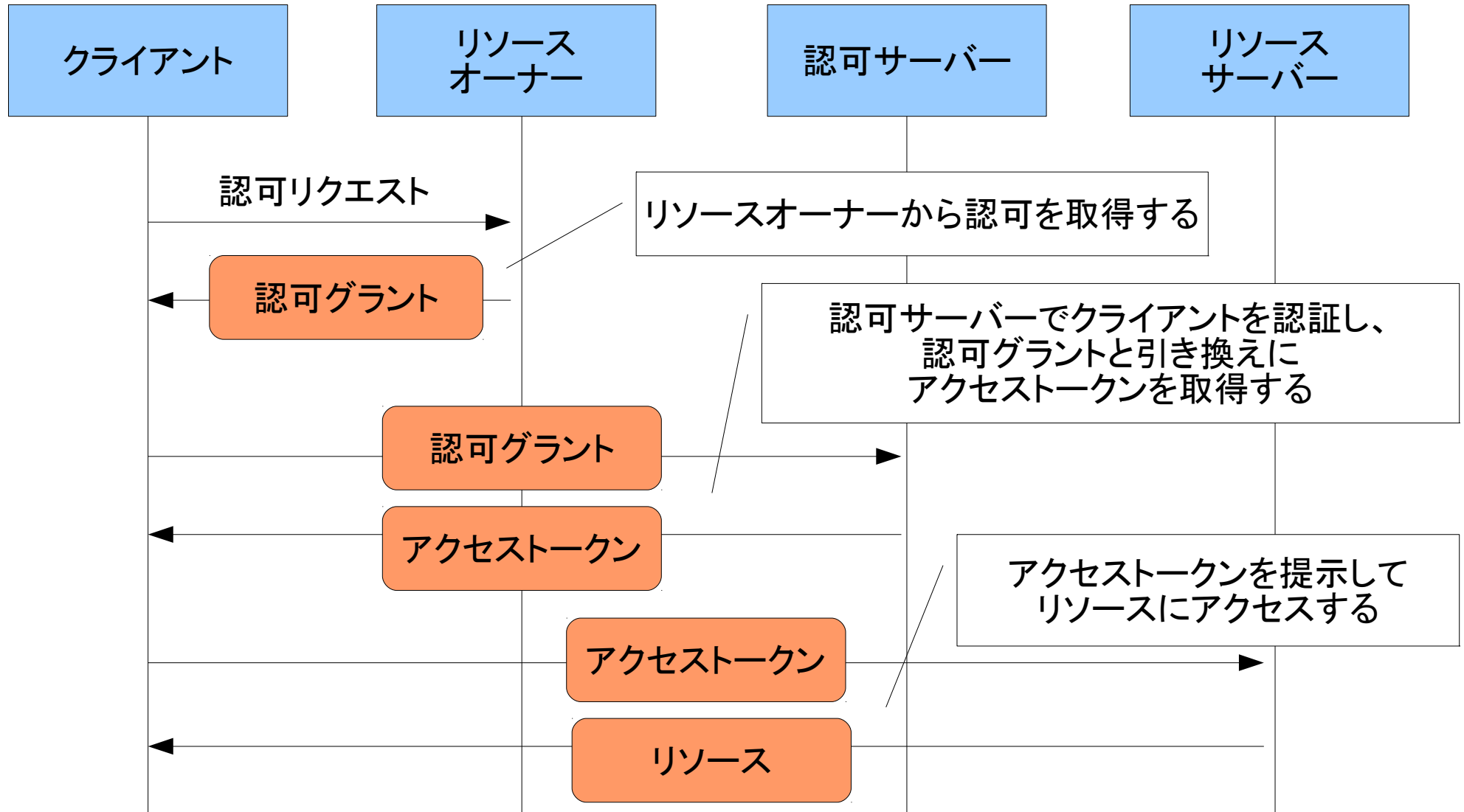
クライアントの認証情報とアクセストークンを同時に使用するため、認可サーバーとリソースサーバーを分けにくい。

OAuth2.0では

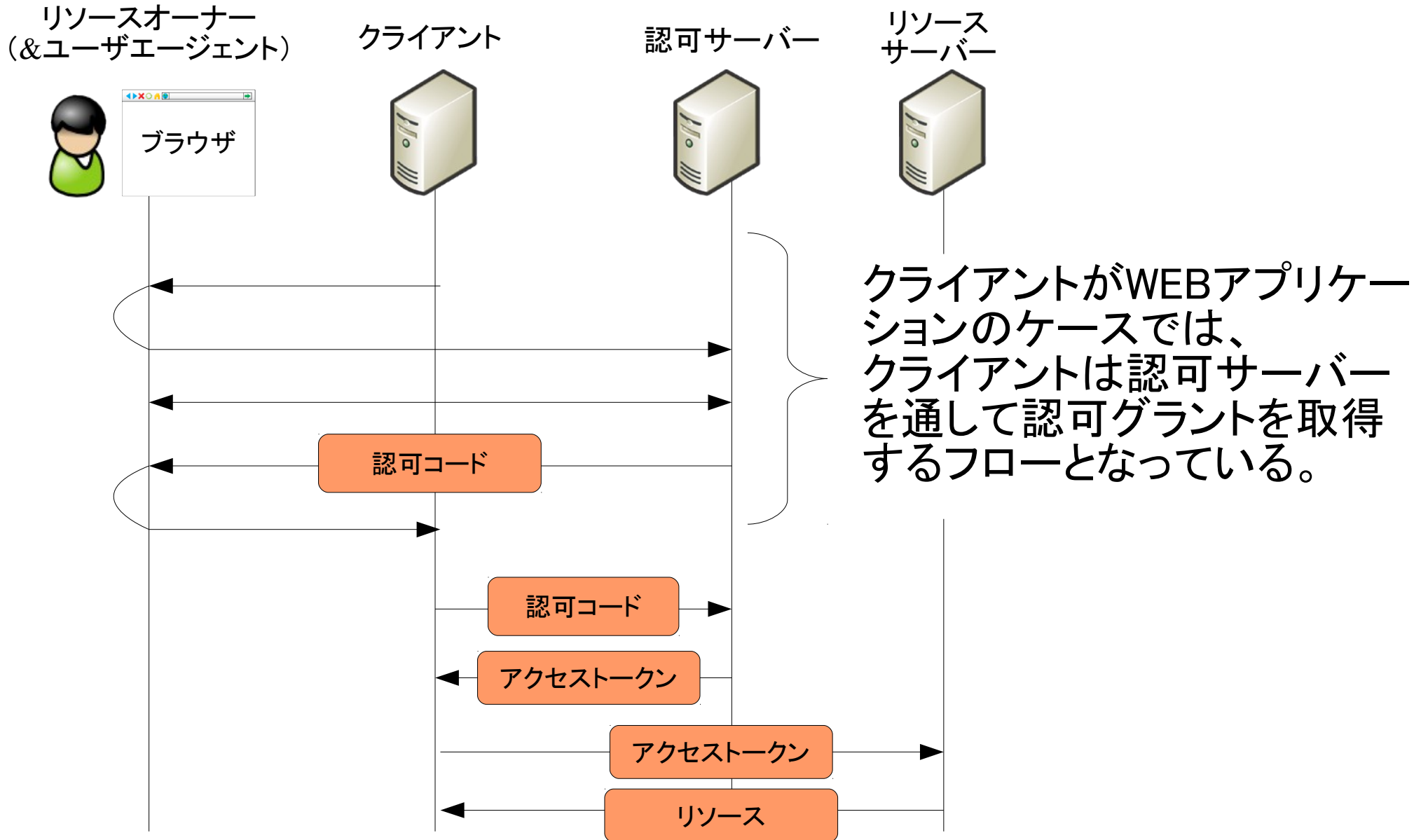
- 署名と複雑な認証
 - 独自の暗号化は行わず、HTTPSを利用してセキュリティを確保。
- WEBアプリケーション以外で上手く機能しなかった
 - WEBアプリケーション以外のフローも仕様化された。
- スケールしにくい
 - 長期間有効なアクセストークンを発行するのではなく、一時的なトークンを発行して認可状態を継続できるようになった。
 - サーバーは認可サーバーとリソースサーバーに役割が分離された。

プロトコル概要 (OAuth2.0)

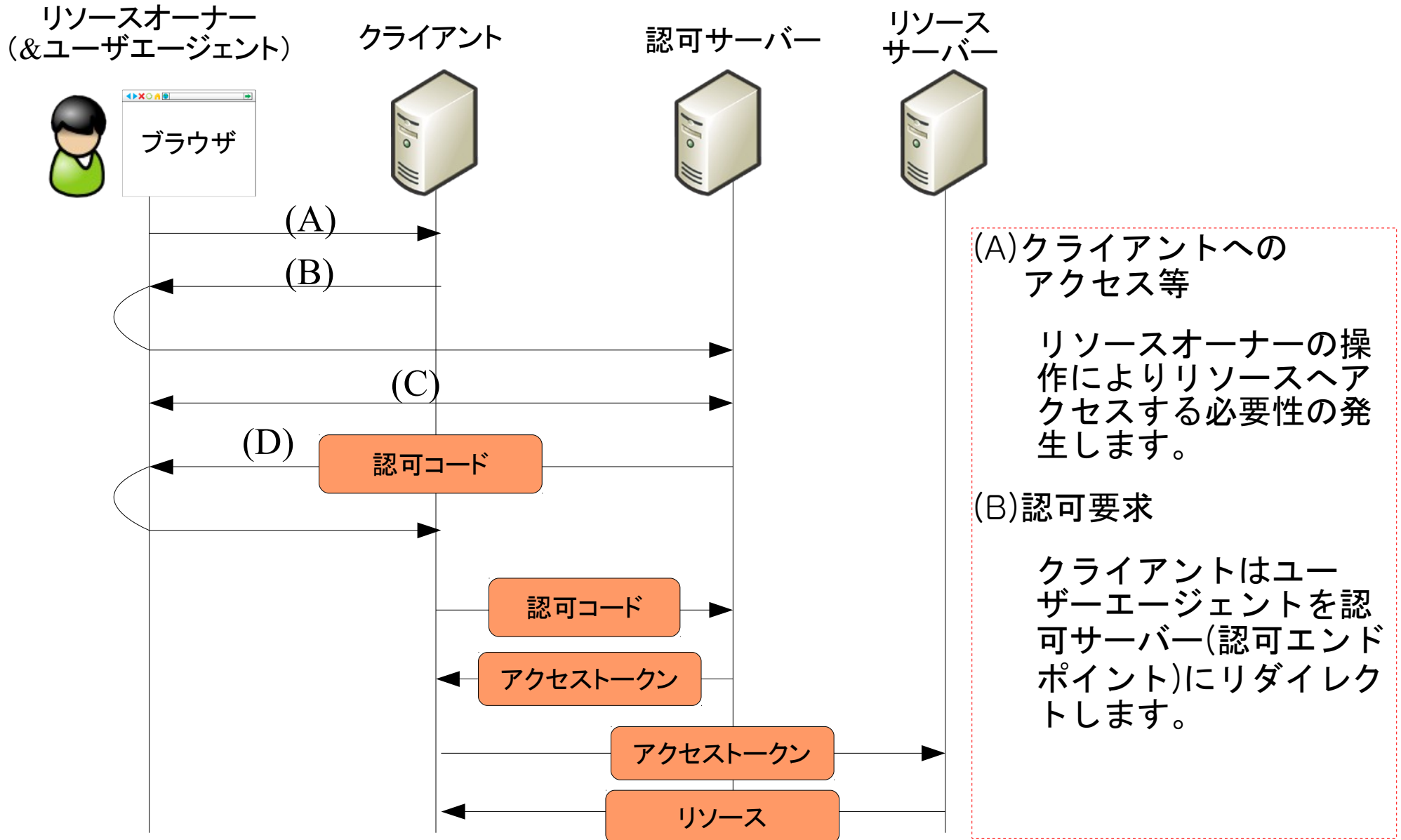
基本フロー



フロー(認可コード)



フロー(認可コード)



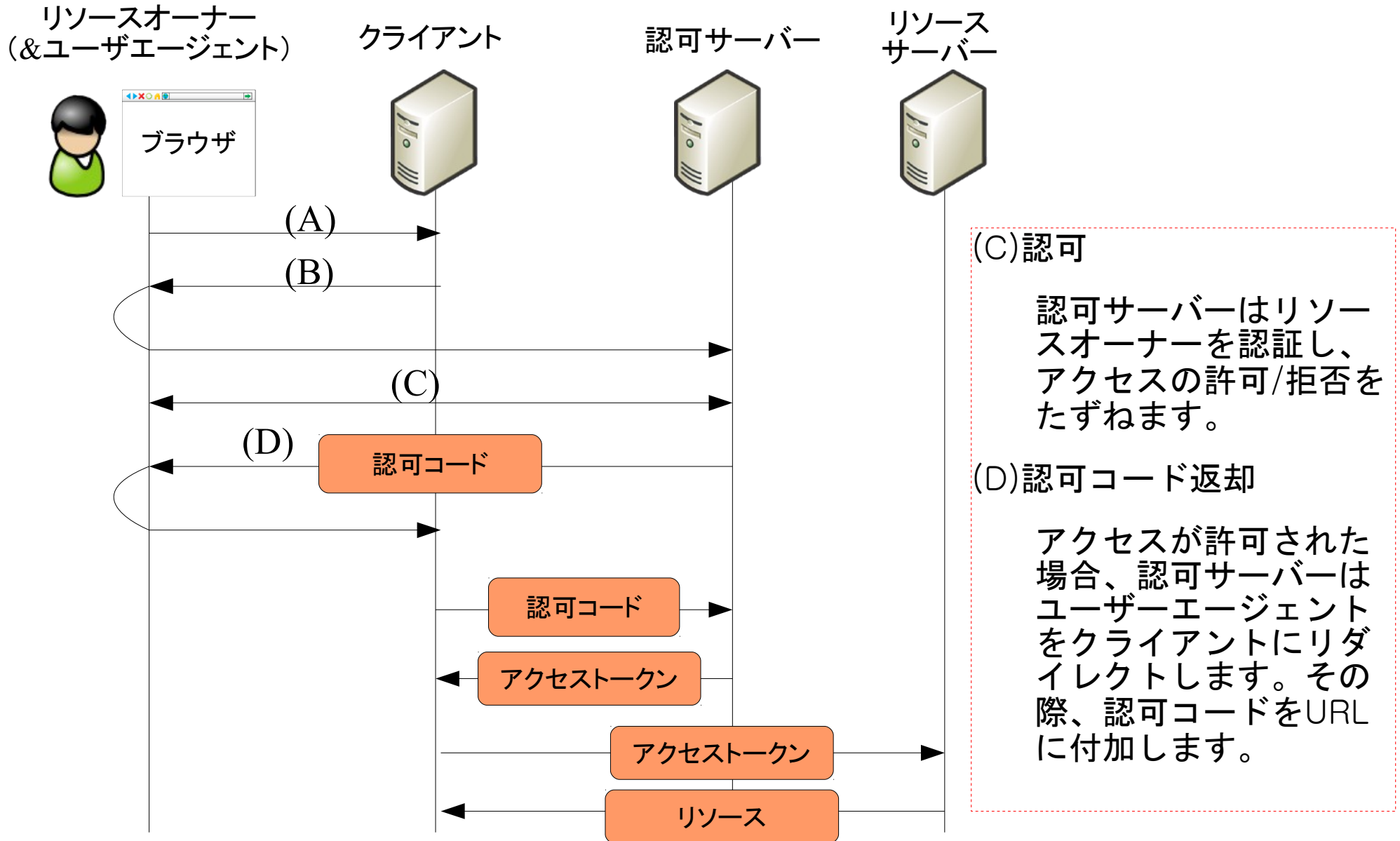
(A)クライアントへのアクセス等

リソースオーナーの操作によりリソースへアクセスする必要性の発生します。

(B)認可要求

クライアントはユーザーエージェントを認可サーバー(認可エンドポイント)にリダイレクトします。

フロー(認可コード)



OpenAMにおけるOAuth

ロードマップ

- OpenAM10.0
 - OAuth認証機能が追加された
- OpenAM10.1
 - OAuth プロバイダ機能が追加される

OAuth2.0 Authentication Module

- OAuthに対応しているサービスのユーザで認証できる認証モジュール
- OAuth2.0に対応しているサービスの例
 - Facebook
 - Google Apps
 - Windows Live etc
- 取得したユーザ情報は設定により様々な取り扱いが可能
 - データストアの既存ユーザにマッピング
 - 匿名ユーザにマッピング
 - セッション情報として保存
 - データストアに保存

設定

- OAuthプロバイダにOpenAMをアプリケーションとして登録する

Live Connect デベロッパー センター

ホーム マイアプリ ドキュメント Interactive SDK ダウンロード サポート ショーケース

oauth_demo

▶ oauth_demo

新しいアプリケーションが作成されました。使用を開始できます。新しいアプリケーションの機能をフル活用するには、[アプリケーションの設定ページ](#)に必要な情報を入力してください。

アプリケーション名:	oauth_demo
クライアント ID:	XXXXXXXXXXXX
クライアント シークレット:	XXXXXXXXXXXX

次のステップ

[Interactive SDK Web](#) サイトにアクセスして、さまざまな API を確認します。コーディングは必要ありません。
[詳細情報](#)

※例はWindows Liveアカウントで認証する際のもので

設定

- OpenAMの管理コンソールでOAuth認証モジュールを作成する

新規モジュールインスタンス

[了解](#)[取消し](#)

* 必須入力フィールド

* 名前:

- * タイプ:
- Active Directory
 - Adaptive Risk
 - HOTP
 - HTTP 基本
 - JDBC
 - LDAP
 - MSISDN
 - OAuth 2.0
 - RADIUS
 - SAE
 - SecurID
 - Windows NT
 - Window デスクトップ SSO
 - WSSAuth
 - データストア
 - メンバーシップ
 - 証明書
 - 匿名
 - 連携

設定

• OAuth認証モジュールの設定を行う

OAuth 2.0

レム属性

Client Id:
 OAuth client_id parameter

Client Secret:
 OAuth client_secret parameter

Client Secret (確認):

Authentication Endpoint URL:
 OAuth authentication endpoint URL

Access Token Endpoint URL:
 OAuth access token endpoint URL

User Profile Service URL:
 User profile information URL

Scope:
 OAuth scope; list of user profile properties

Proxy URL:
 The URL to the OpenAM OAuth proxy JSP

OAuthプロバイダから提供されるクライアント識別子

OAuthプロバイダから提供されるクライアントのパスワード

認可コードを提供するサーバーのURL

アクセストークンを提供するサーバーのURL

ユーザ情報を提供するサーバーのURL

ユーザ情報の要求範囲

OAuthサーバーからOpenAMへリダイレクトさせる際のURL
サーバー名以外は固定

※例はWindows Liveアカウントで認証する際のもので

設定

Account Mapper:

i Name of the class implementing the account mapping

OAuthアカウントをOpenAMに
マップするクラス

Account Mapper Configuration

現在の値

OAuthアカウントをOpenAMに
マップする際にキーとなる属性

新しい値

i Mapping of OAuth account to local OpenAM account

Attribute Mapper:

i Name of the class that implements the attribute mapping

OAuthアカウント属性をOpenAMに
マップするクラス

Attribute Mapper Configuration

現在の値

OpenAMにマップする属性

※例はWindows Liveアカウントで認証する際のもので

設定

Save attributes in the session:

有効

If this option is enabled, the attributes configured in the attribute map are saved in the OpenAM session

セッションにOAuthプロバイダから取得した属性を保存するか

Email attribute in OAuth2 Response:

i Attribute from the OAuth2 response used to send activation code

OAuthプロバイダのプロファイルのうちEmailに該当する属性

Create account if it does not exist:

有効

i If the OAuth2 account does not exist in the local OpenAM data store, the account can be created dynamically.

ユーザがデータストアに存在しない場合に自動でアカウントを作成するか

Prompt for password setting and activation code:

有効

i Users must set a password and complete the activation flow during dynamic profile creation.

自動でアカウントを作成する場合にパスワードを設定しアクティベーションコードをメールで送付するか

Map to anonymous user:

有効

i Enabled anonymous user access to OpenAM for OAuth authentication

Anonymous User:

i Username of the OpenAM anonymous user

OAuth 2.0 Provider logout service:

i The URL of the OAuth Identity Providers Logout service

Logout options:

Do not logout

Log out

Prompt

※例はWindows Liveアカウントで認証する際のものです

設定

Save attributes in the session: 有効
 If this option is enabled, the attributes configured in the attribute mapper will be saved into the OpenAM session

Email attribute in OAuth2 Response:
 Attribute from the OAuth2 response used to send activation code emails.

Create account if it does not exist: 有効
 If the OAuth2 account does not exist in the local OpenAM data store, an account will be created dynamically.

Prompt for password setting and activation code: 有効
 Users must set a password and complete the activation flow during creation.

Map to anonymous user: 有効
 Enabled anonymous user access to OpenAM for OAuth authentication.

Anonymous User:
 Username of the OpenAM anonymous user

OAuth 2.0 Provider logout service:
 The URL of the OAuth Identity Providers Logout service

Logout options:
 Do not logout
 Log out
 Prompt

存在しないユーザを匿名ユーザにマップするか

匿名ユーザの名称

OAuthプロバイダのログアウトのURL

ログアウトの動作を指定

※例はWindows Liveアカウントで認証する際のものです

設定

Mail Server Gateway implementation class:
i The class used by the module to send email.

SMTP host:
 The mail host that will be used by the Email Gateway implementation

SMTP port:
 The TCP port that will be used by the SMTP gateway

SMTP User Name:
 If the SMTP Service requires authentication, configure the user name here

SMTP User Password:
 The Password of the SMTP User Name

SMTP User Password (確認):

SMTP SSL Enabled: 有効
 Tick this option if the SMTP Server provides SSL

SMTP From address:
 The email address on behalf of whom the messages will be sent

Authentication Level:
i The authentication level associated with this module.

メールを送信するクラス

アクティベーションコードを
メールで送信する際に
使われるメール設定

※例はWindows Liveアカウントで認証する際のものです

デモ

- OpenAMにアクセス⇒Windows Liveの認証画面へ



The screenshot shows the Windows Live sign-in interface. At the top, the Windows Live logo is displayed. Below it, there are two input fields: one for the Windows Live ID and one for the password. A 'Sign in' button is located below the password field. There are also links for 'Can't access your account?' and 'Not your computer? Get a single use code to sign in with'. At the bottom, there is a copyright notice for Microsoft and a 'Sign up' link.

Windows Live™

Windows Live ID:

Password:

[Can't access your account?](#)

Keep me signed in

Sign in

Not your computer?

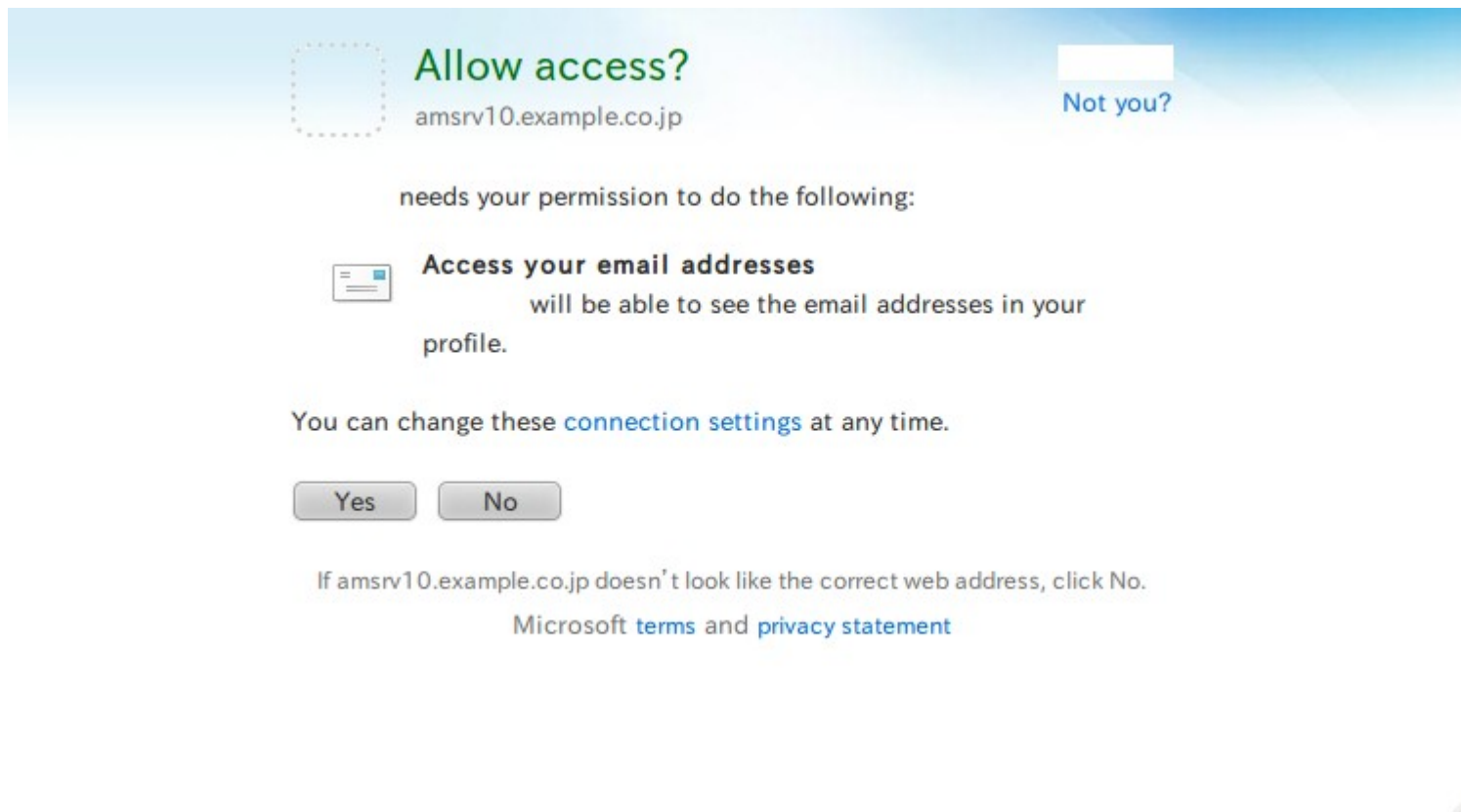
[Get a single use code to sign in with](#)

©2012 Microsoft | [Privacy](#)

[Sign up](#)

デモ

- アクセスの許可を問われる



デモ

- 認証成功



anonymous

保存 リセット

* 必須入力フィールド

名:	<input type="text" value="anonymous"/>
* 姓:	<input type="text" value="anonymous"/>
* フルネーム:	<input type="text" value="anonymous"/>
パスワード:	編集
電子メールアドレス:	<input type="text"/>
電話番号:	<input type="text"/>
住所:	<input type="text"/>
パスワードリセットオプション:	編集
汎用 ID:	id=anonymous,ou=user,dc=opensso,dc=java,dc=net

※ここでは匿名ユーザにマップしています

OAuth認証の使いどころ

- OAuthプロバイダはFacebookやtwitterといったSNSが多い
- OAuth認証モジュールの特徴は、OAuthプロバイダのアカウントをOpenAMに取り込める所
 - 不特定多数のユーザを対象としたサービスに向いている
 - 教育機関や企業にはSNSとの連携は難しい

OAuth認証の使いどころ

- OAuth認証を利用すれば、OAuthプロバイダがもつ情報を利用できる
- OpenAMのデータストアに持つ必要がなくなりデータの一元管理が可能になる？

参考文献

- OAuth Community Site

⇒OAuthの仕様

<http://oauth.net/>

- Introducing OAuth2.0

⇒OAuth2.0策定の背景

<http://hueniverse.com/2010/05/introducing-oauth-2-0/>

- OAuth 2.0 Authentication (Facebook, Google, MSN, etc)

⇒OAuth認証モジュールの概要

<https://wikis.forgerock.org/confluence/display/openam/OAuth+2.0+Authentication+%28Facebook,+Google,+MSN,+etc%29>

参考文献

- OAuth 2.0 (Live Connect Developer Center)

⇒Windows LiveのOAuthの仕様

<http://msdn.microsoft.com/en-us/library/live/hh243647.aspx>

- Scopes and permissions (Live Connect Developer Center)

⇒Windows Liveのscopeの仕様

<http://msdn.microsoft.com/en-us/library/live/hh243646.aspx>



OSSTech

オープンソース・ソリューション・テクノロジー株式会社

<http://www.osstech.co.jp/>

お問い合わせ info@osstech.co.jp