OAuth入門

2012年4月24日
辻口 鷹耶

オープンソース・ソリューション・テクノロジ株式会社
http://www.osstech.co.jp/
お問い合わせ info@osstech.co.jp

Copyright © 2012 Open Source Solution Technology, Corp.

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

Copyright © 2012 Open Source Solution Technology, Corp.

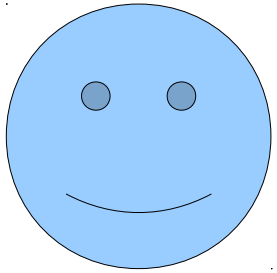
OAuthについて

Copyright © 2012 Open Source Solution Technology, Corp.

OAuthの背景

OAuth登場以前は。。。

ユーザ



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

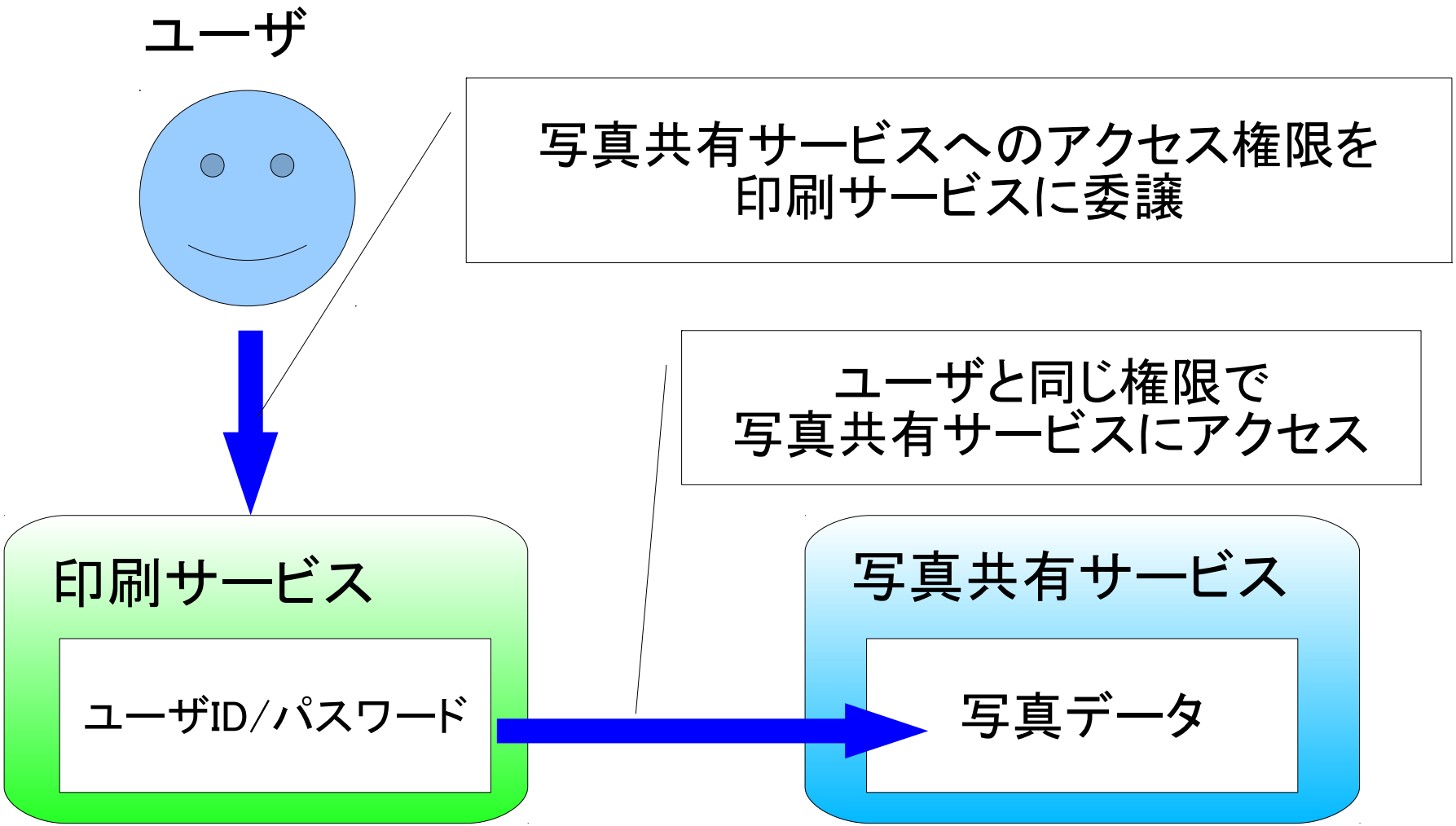
印刷サービス

写真共有サービス

写真データ

Copyright © 2012 Open Source Solution Technology, Corp.

OAuthの背景

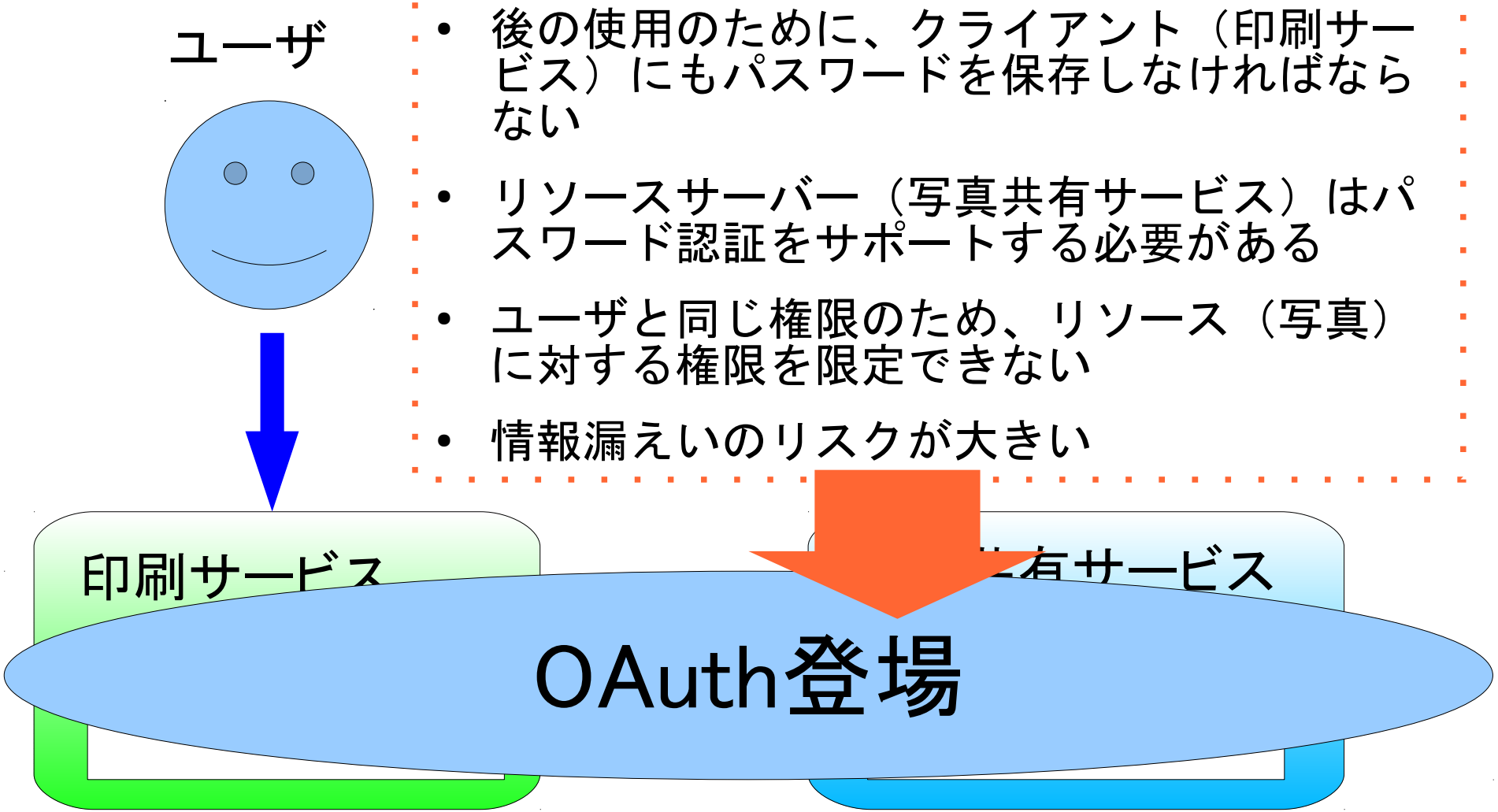


Copyright © 2012 Open Source Solution Technology, Corp.

OAuthの背景

アクセス権限の委譲の問題点：

- 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



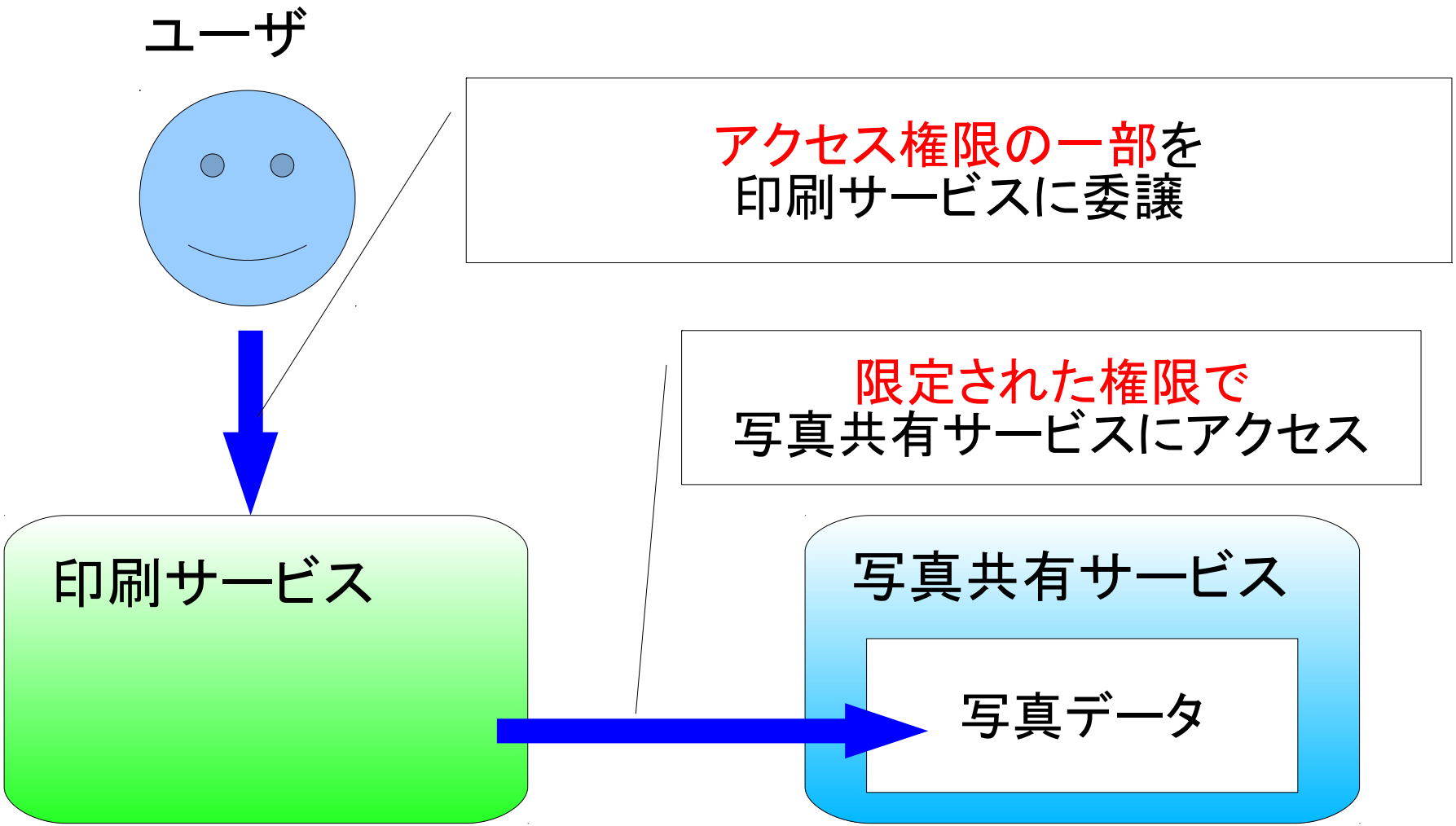
Copyright © 2012 Open Source Solution Technology, Corp.

OAuthとは

- クライアント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プロトコル
- 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

Copyright © 2012 Open Source Solution Technology, Corp.

OAuthを利用すると



Copyright © 2012 Open Source Solution Technology, Corp.

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。

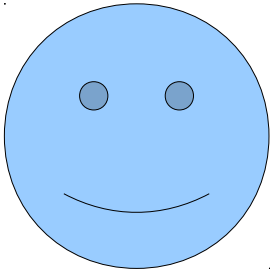
- 認可サーバー

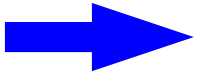
  リソースオーナーの認証し、アクセストークンをクライアントに発行するサーバーです。

Copyright © 2012 Open Source Solution Technology, Corp.

OAuthでの役割（例：Facebook）

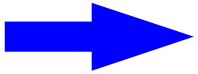
Facebookユーザ





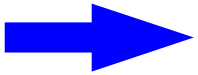
リソースオーナー

Facebook
連携アプリ



クライアント

Facebook

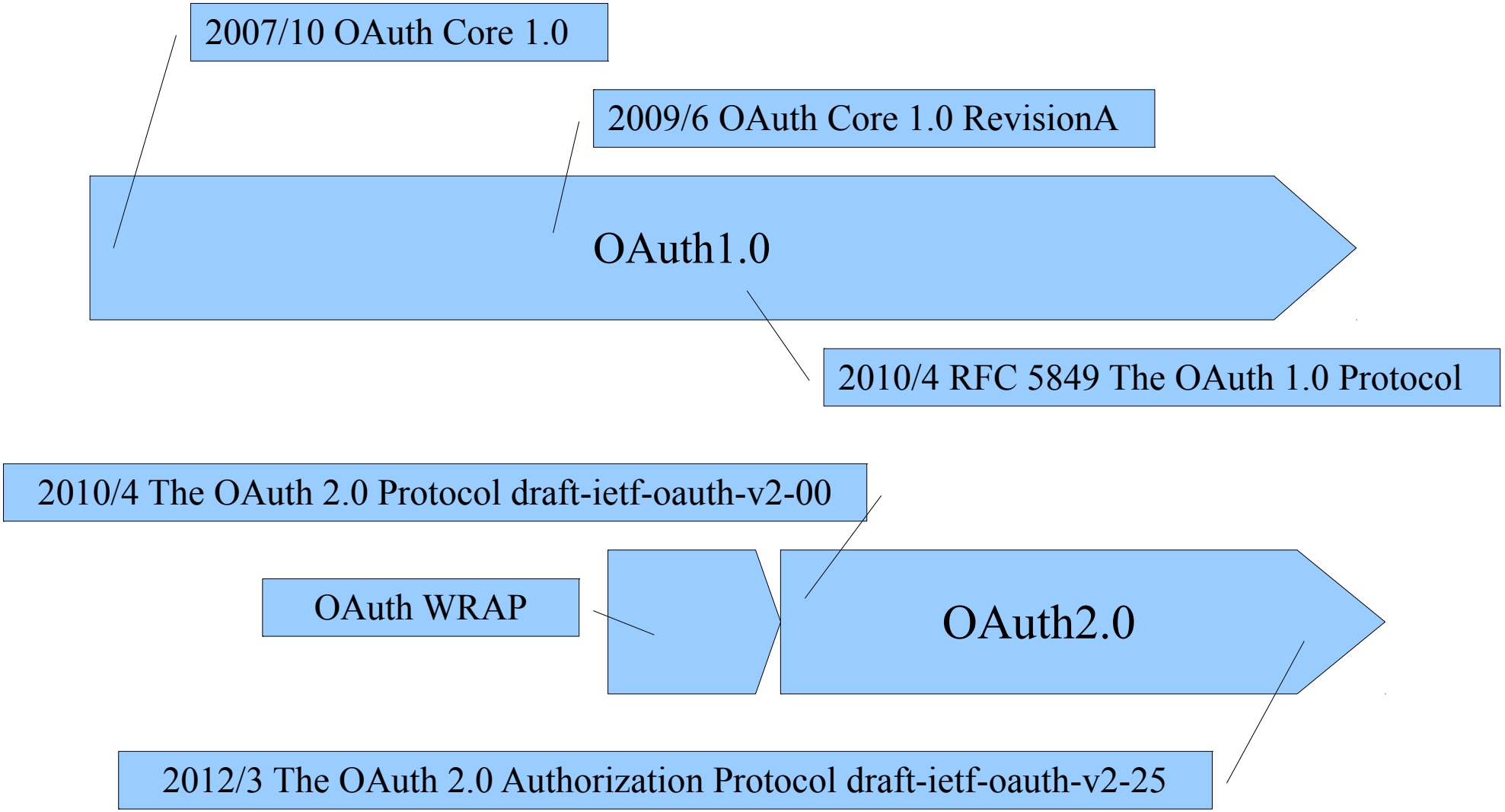


認可サーバー

リソースサーバー

Copyright © 2012 Open Source Solution Technology, Corp.

OAuthの歴史



Copyright © 2012 Open Source Solution Technology, Corp.

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。

Copyright © 2012 Open Source Solution Technology, Corp.

OAuth2.0では

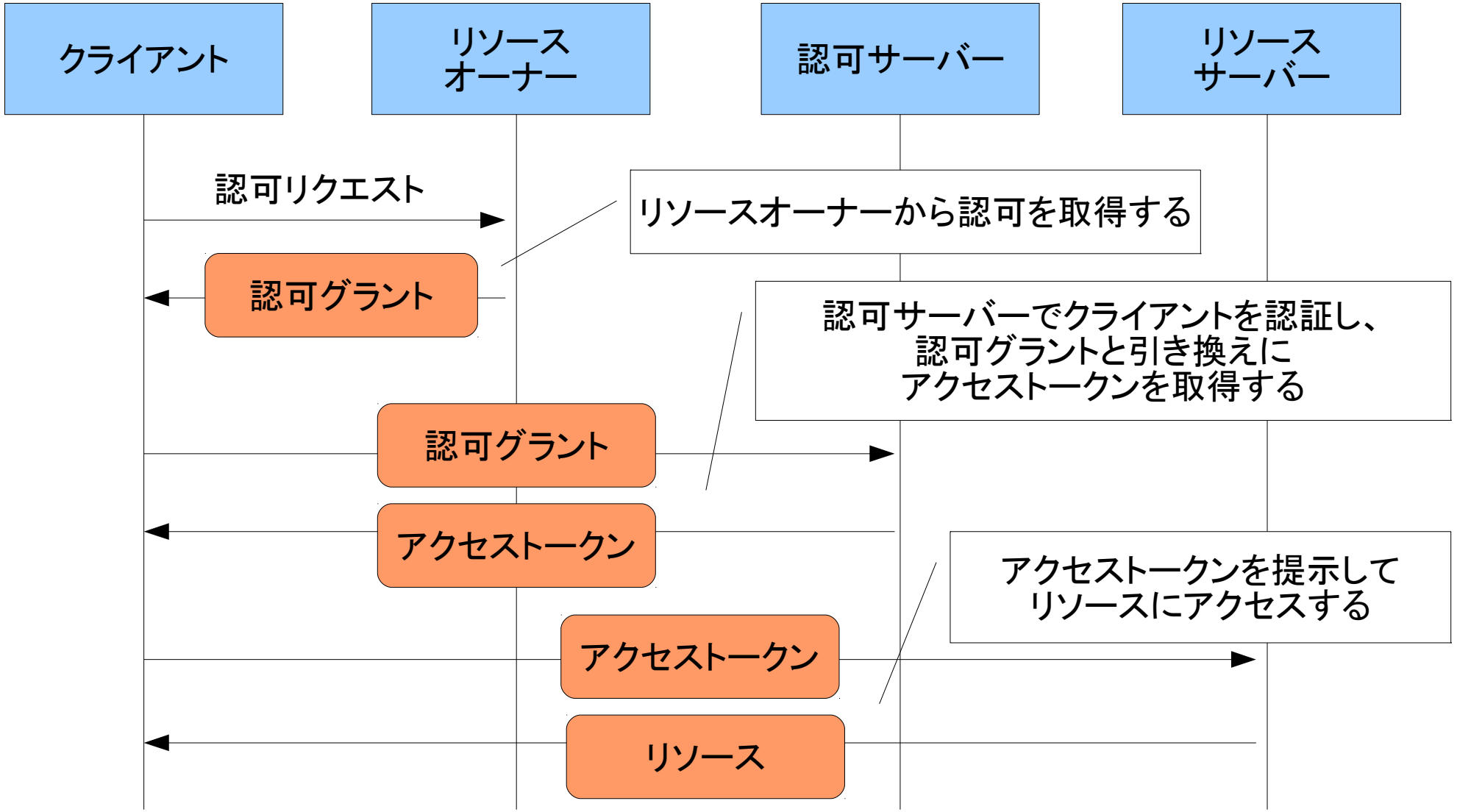
- 署名と複雑な認証
  - → 独自の暗号化は行わず、HTTPSを利用してセキュリティを確保。
- WEBアプリケーション以外で上手く機能しなかった
  - → WEBアプリケーション以外のフローも仕様化された。
- スケールしにくい
  - → 長期間有効なアクセストークンを発行するのではなく、一時的なトークンを発行して認可状態を継続できるようになった。
  - → サーバーは認可サーバーとリソースサーバーに役割が分離された。

Copyright © 2012 Open Source Solution Technology, Corp.

プロトコル概要
(OAuth2.0)

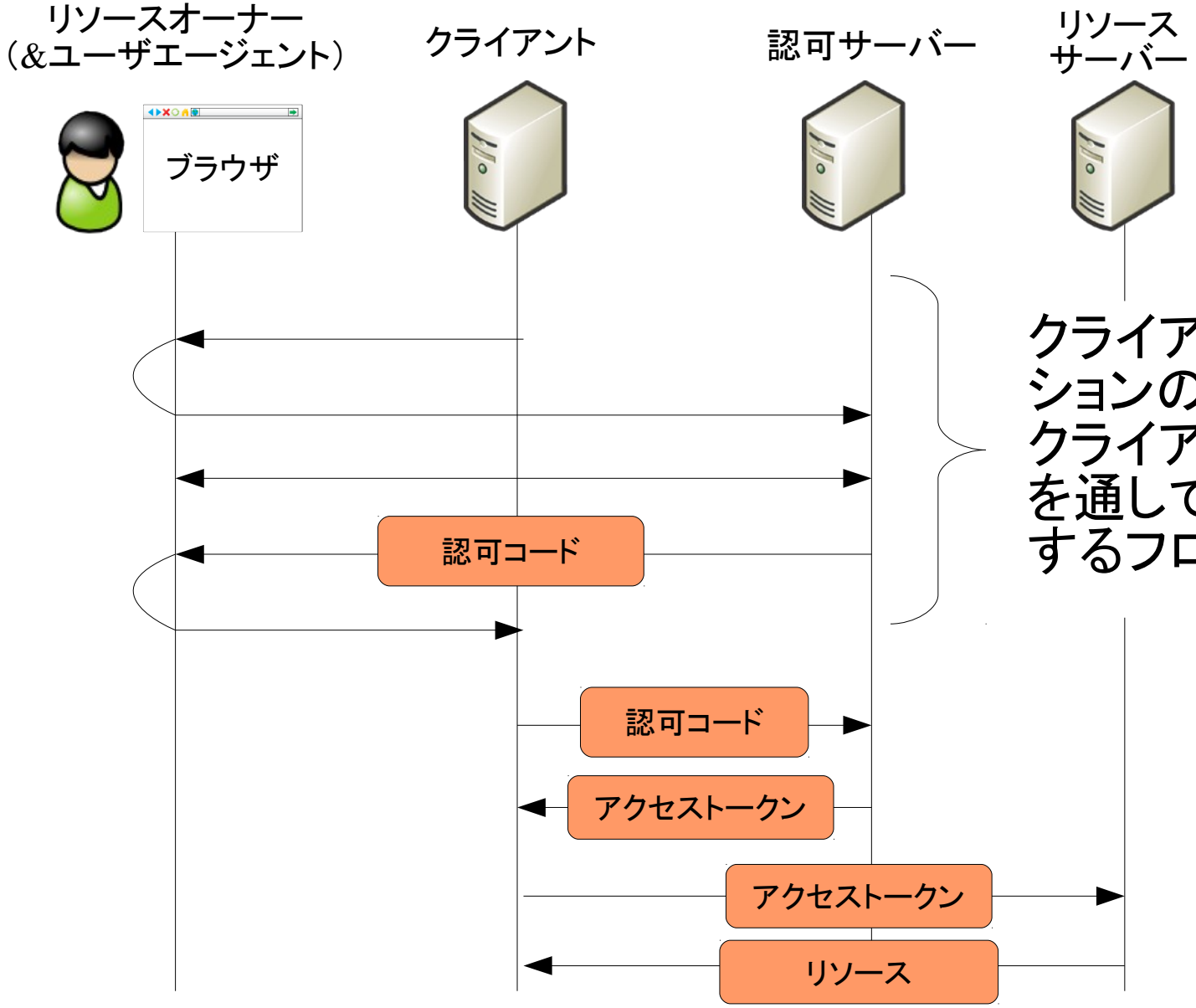
Copyright © 2012 Open Source Solution Technology, Corp.

基本フロー



Copyright © 2012 Open Source Solution Technology, Corp.

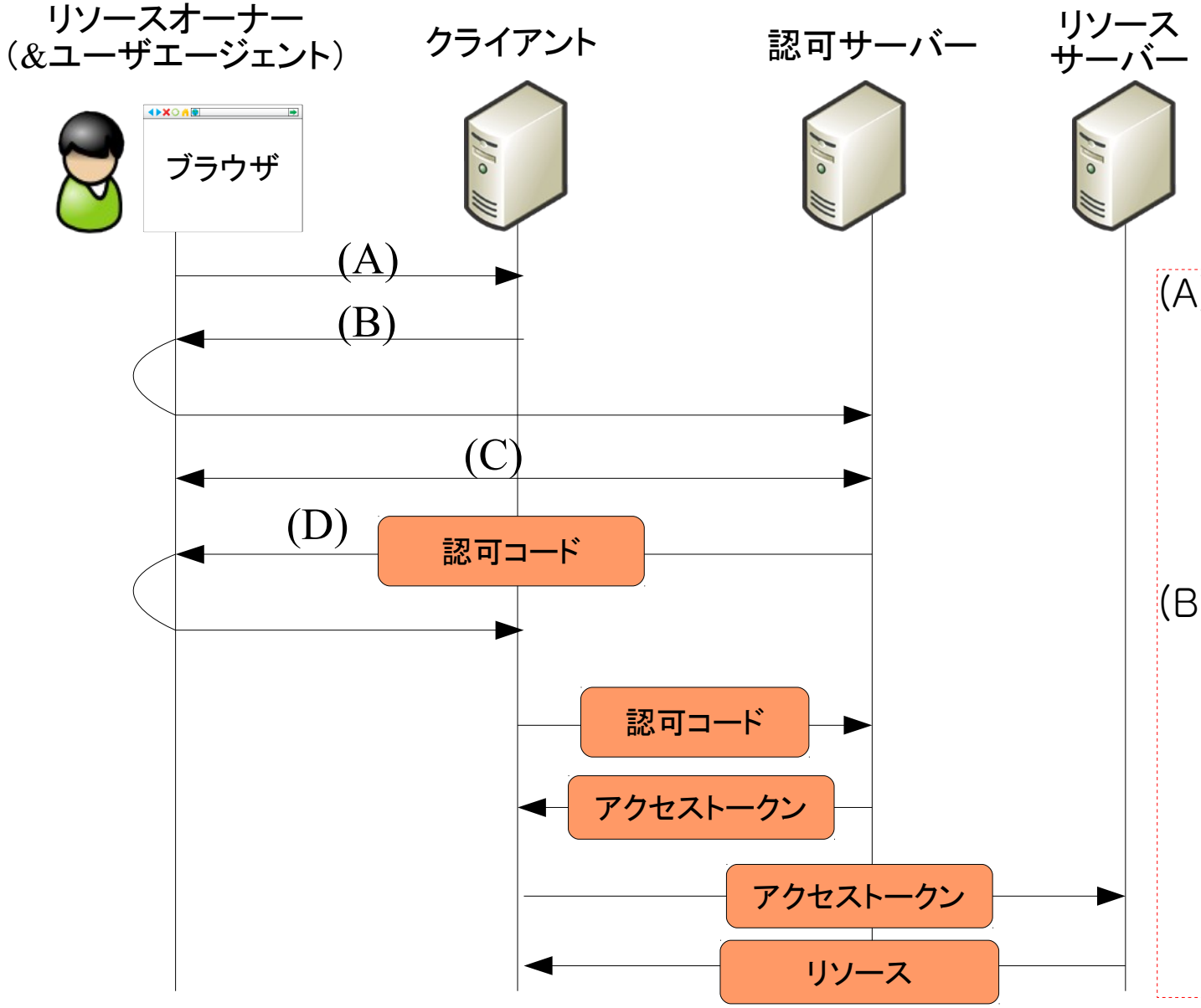
フロー(認可コード)



クライアントがWEBアプリケーションのケースでは、
クライアントは認可サーバーを通して認可グラントを取得するフローとなっている。

Copyright © 2012 Open Source Solution Technology, Corp.

フロー(認可コード)



(A)クライアントへのアクセス等

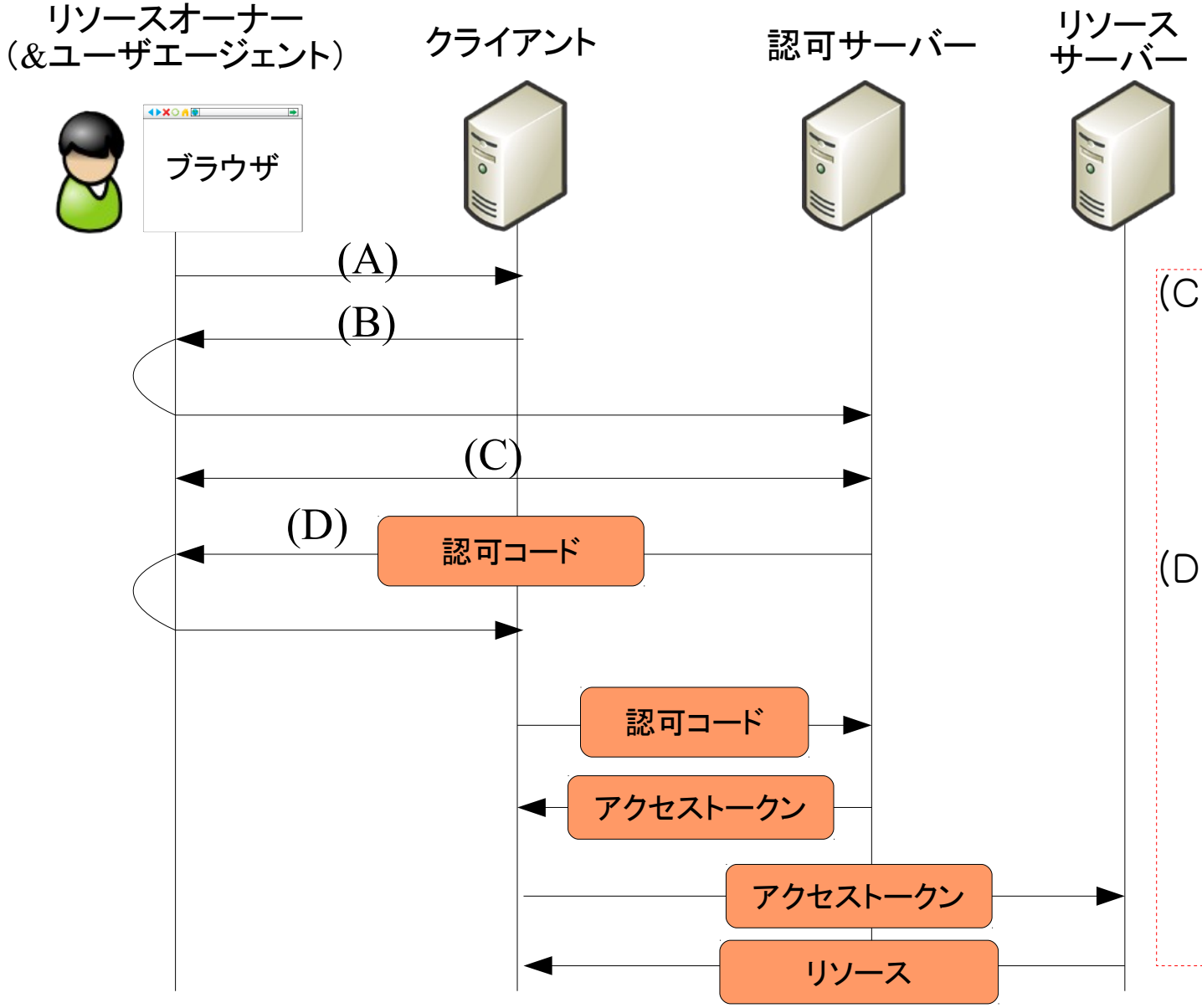
リソースオーナーの操作によりリソースへアクセスする必要性の発生します。

(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。

Copyright © 2012 Open Source Solution Technology, Corp.

フロー(認可コード)



(C)認可

認可サーバーはリソースオーナーを認証し、アクセスの許可/拒否をたずねます。

(D)認可コード返却

アクセスが許可された場合、認可サーバーはユーザーエージェントをクライアントにリダイレクトします。その際、認可コードをURLに付加します。

Copyright © 2012 Open Source Solution Technology, Corp.

OpenAMにおけるOAuth

Copyright © 2012 Open Source Solution Technology, Corp.

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

Copyright © 2012 Open Source Solution Technology, Corp.

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

Copyright © 2012 Open Source Solution Technology, Corp.

設定

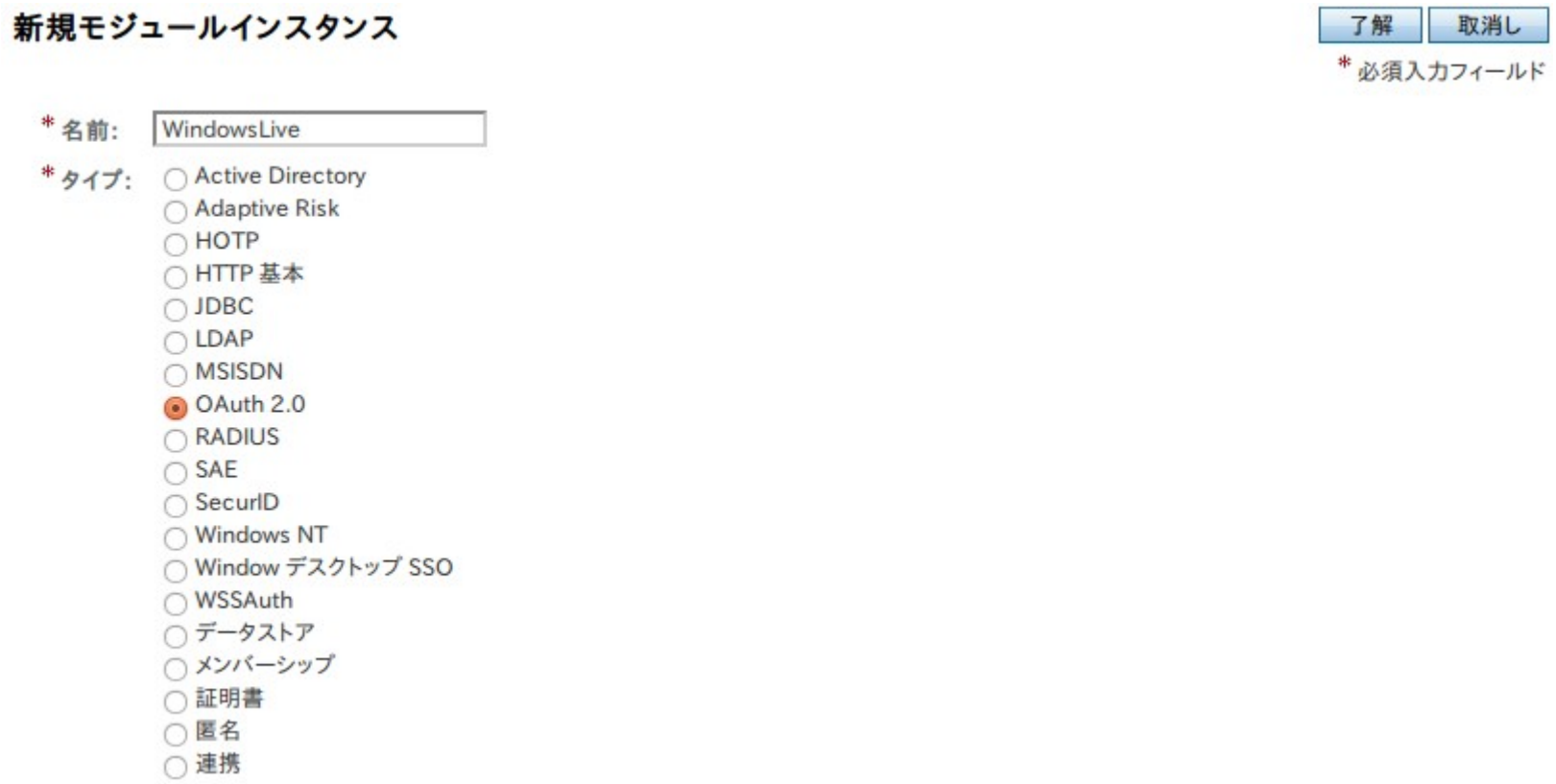
- OAuthプロバイダにOpenAMをアプリケーションとして登録する

※例はWindows Liveアカウントで認証する際のものです

Copyright © 2012 Open Source Solution Technology, Corp.

設定

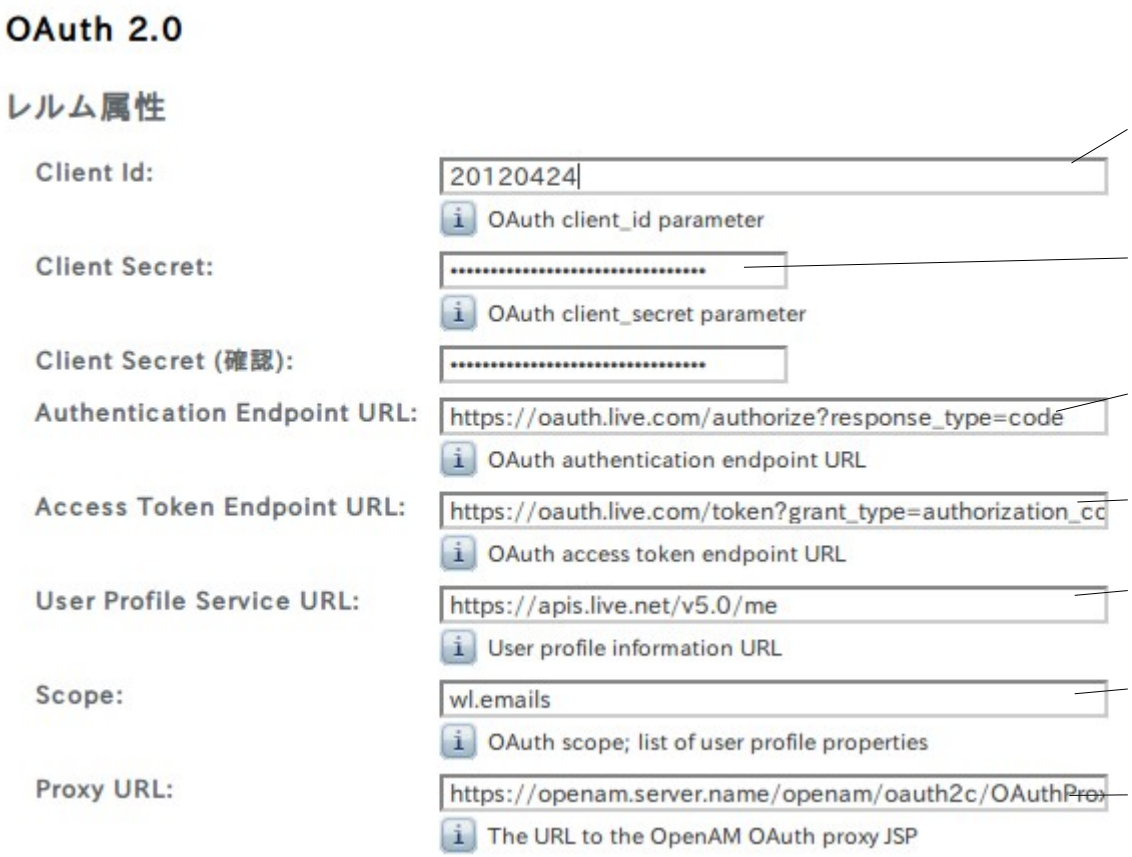
- OpenAMの管理コンソールでOAuth認証モジュールを作成する



Copyright © 2012 Open Source Solution Technology, Corp.

設定

- OAuth認証モジュールの設定を行う



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

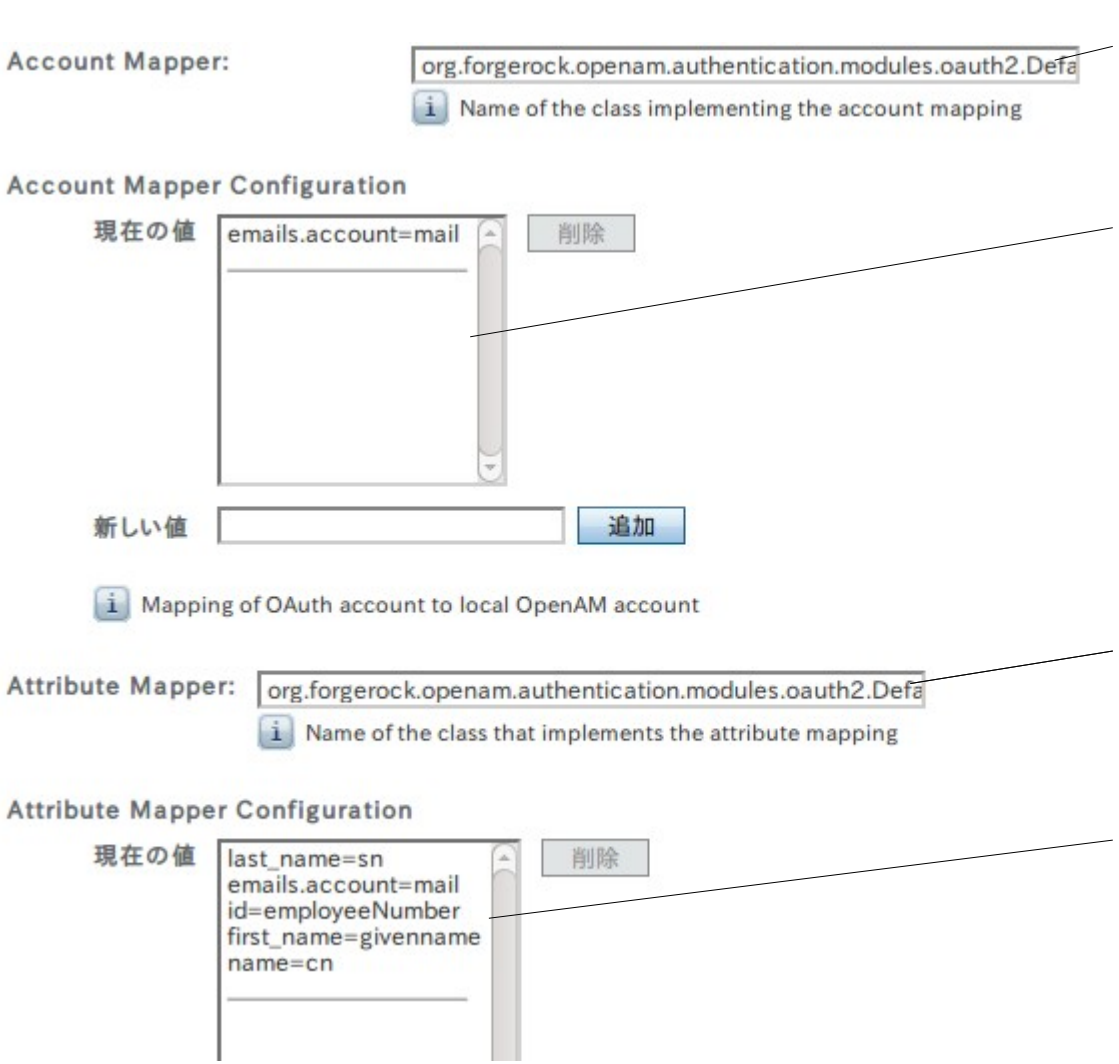
ユーザ情報の要求範囲

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す

Copyright © 2012 Open Source Solution Technology, Corp.

設定



OAuthアカウントをOpenAMに
マップするクラス

OAuthアカウントをOpenAMに
マップする際にキーとなる属性

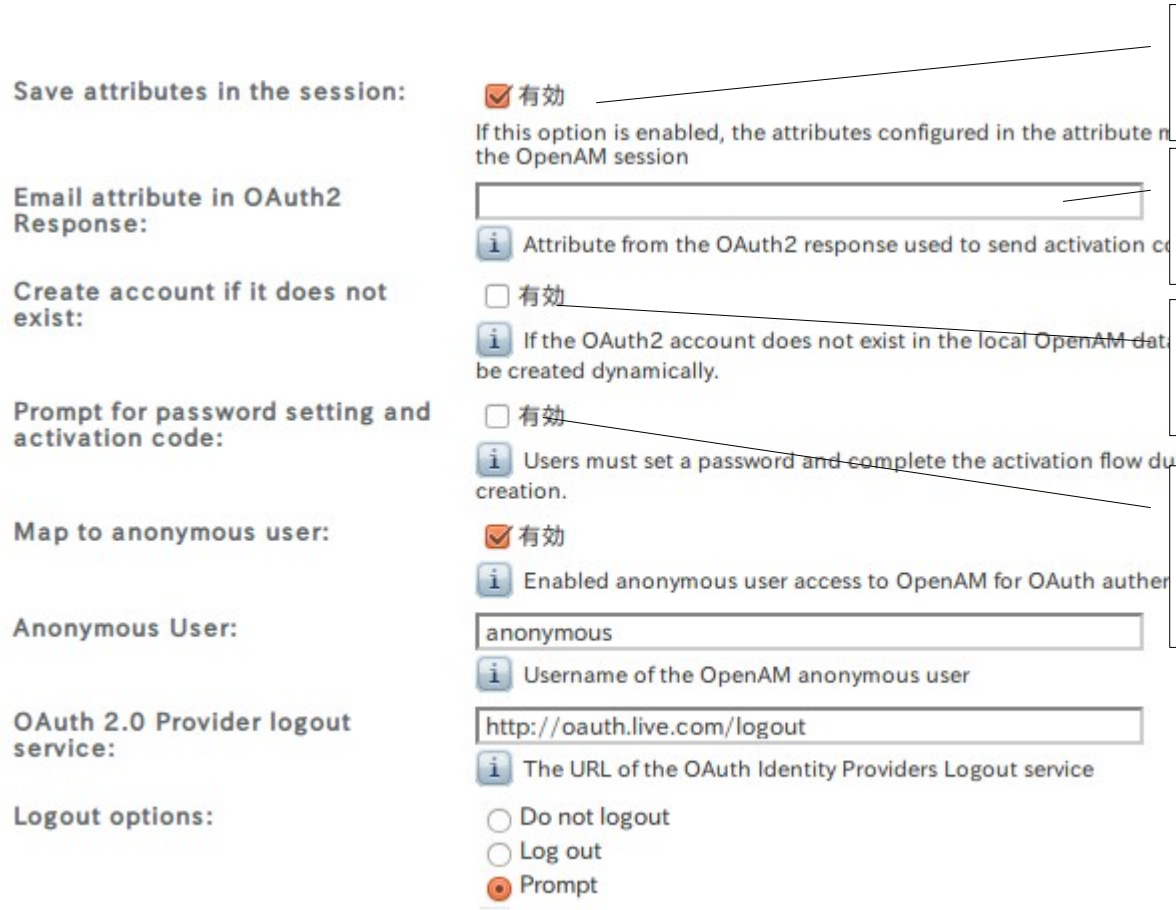
OAuthアカウント属性をOpenAMに
マップするクラス

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す

Copyright © 2012 Open Source Solution Technology, Corp.

設定



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

OAuthプロバイダのプロファイルのうちEmailに該当する属性

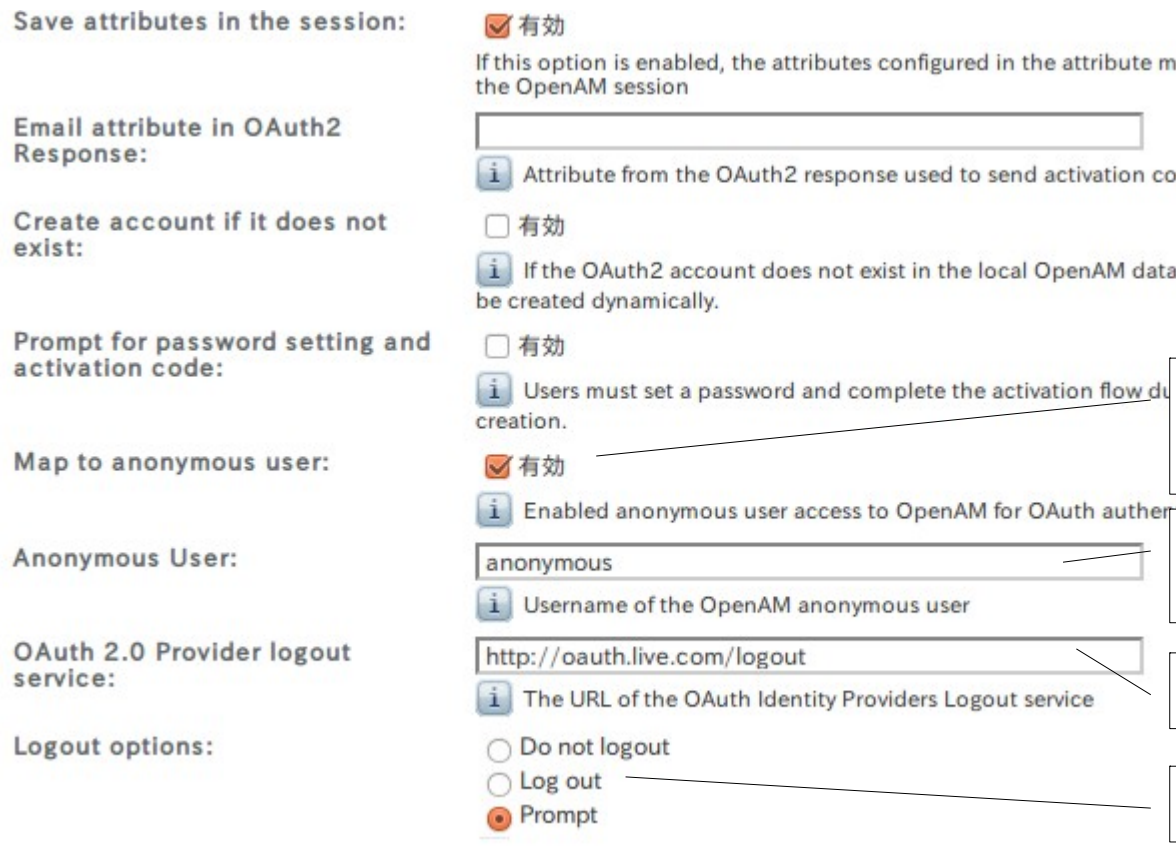
ユーザがデータストアに存在しない場合に自動でアカウントを作成するか

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

※例はWindows Liveアカウントで認証する際のものです

Copyright © 2012 Open Source Solution Technology, Corp.

設定



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

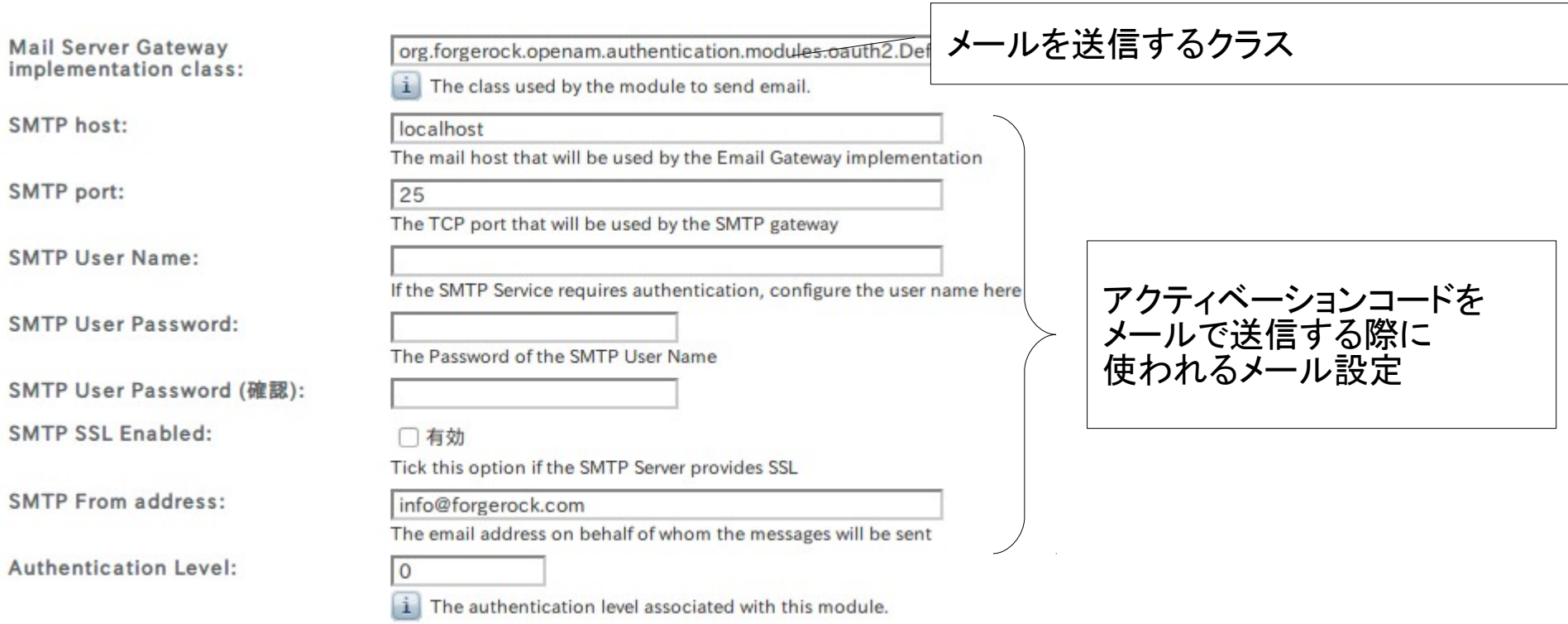
OAuthプロバイダのログアウトのURL

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

Copyright © 2012 Open Source Solution Technology, Corp.

設定

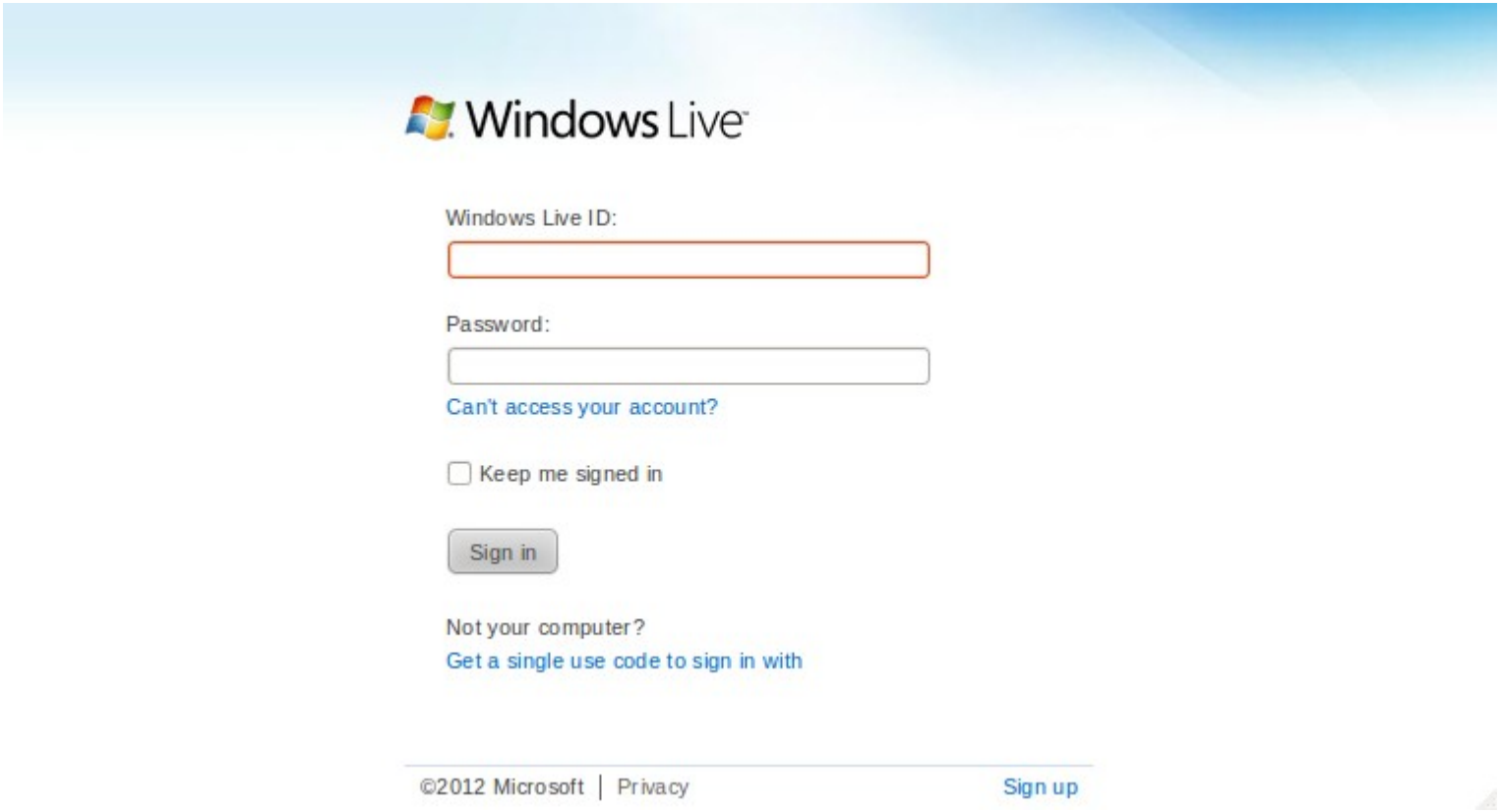


※例はWindows Liveアカウントで認証する際のものです

Copyright © 2012 Open Source Solution Technology, Corp.

デモ

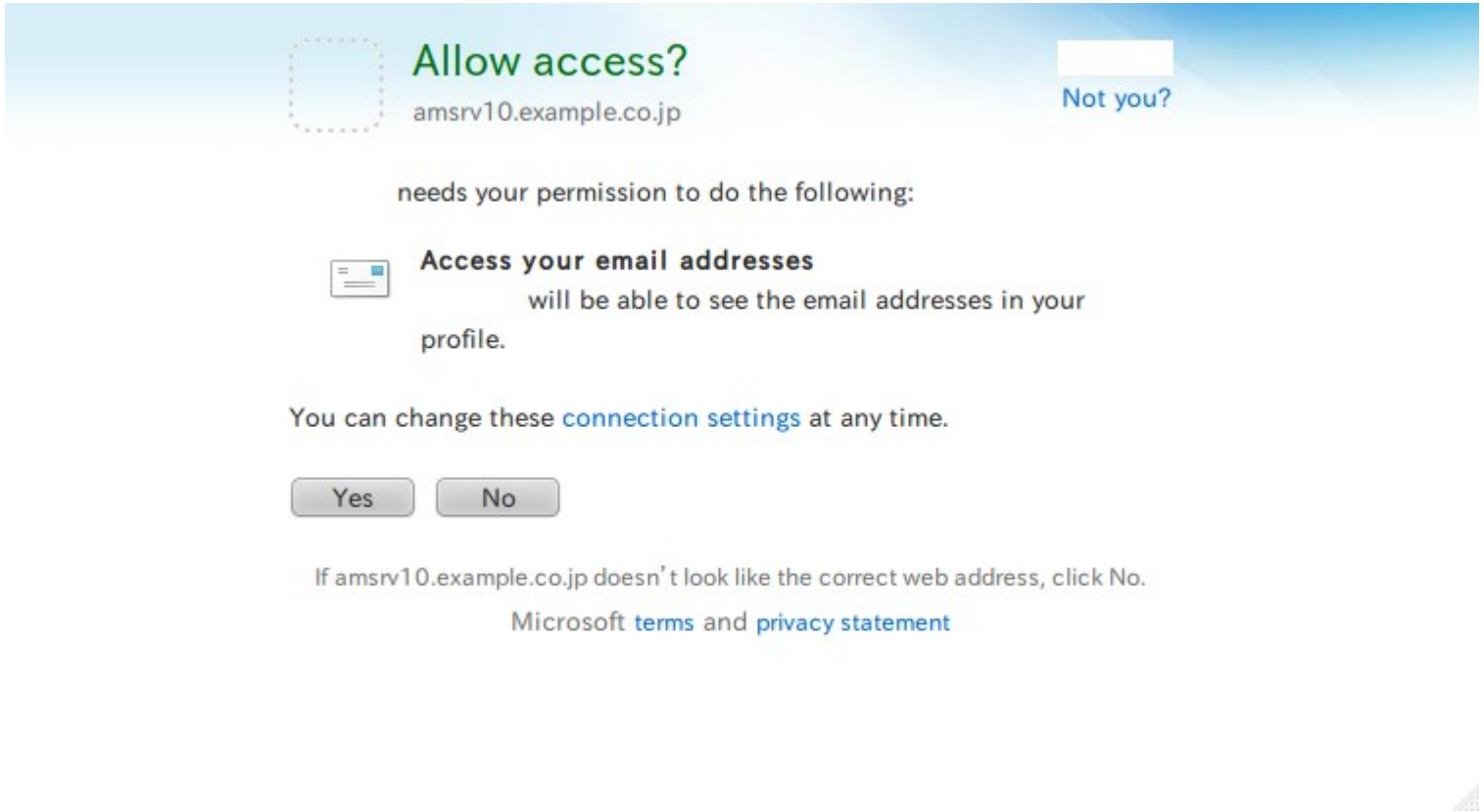
- OpenAMにアクセス⇒Windows Liveの認証画面へ



Copyright © 2012 Open Source Solution Technology, Corp.

デモ

- アクセスの許可を問われる



Copyright © 2012 Open Source Solution Technology, Corp.

デモ

- 認証成功

※ここでは匿名ユーザにマップしています

Copyright © 2012 Open Source Solution Technology, Corp.

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

Copyright © 2012 Open Source Solution Technology, Corp.

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？

Copyright © 2012 Open Source Solution Technology, Corp.

参考文献

- OAuth Community Site

  ⇒OAuthの仕様

  http://oauth.net/

- Introducting 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

Copyright © 2012 Open Source Solution Technology, Corp.

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

Copyright © 2012 Open Source Solution Technology, Corp.

オープンソース・ソリューション・テクノロジ株式会社
http://www.osstech.co.jp/
お問い合わせ *info@osstech.co.jp*

Copyright © 2012 Open Source Solution Technology, Corp.