今後の認証基盤で必要となる関連技術の動向

株式会社オージス総研
テミストラクトソリューション部
八幡 孝

統合認証ソリューション ThemiStruct

ThemiStruct-WAM

シングルサインオン
認証基盤ソリューション

ThemiStruct-IDM

ID管理ソリューション

ThemiStruct-CM

電子証明書発行・管理
ソリューション

ワンタイムパスワードソリューション

ThemiStruct-OTP

システム監視ソリューション

ThemiStruct-MONITOR

ThemiStruct（テミストラクト）
Identity Platform AWS対応版

クラウド、IoT時代の
“All in one”
認証プラットフォーム

ビジネスのデジタル変容トレンドへの対応

ビジネスのデジタル変容の概念

モバイル、クラウド、
ソーシャルの活用

ビジネスプロセス
の自動連携

ユーザー情報の
活用と分析

多様なデバイスの
連携、活用

- ユーザー毎に最適化されたサービスの提供
- 業務効率の向上、提供スピードの向上

認証基盤の適応分野の広がり、要求の拡大

クラウド活用、モバイル活用など、要求が拡大

守りの認証基盤から 攻めの認証基盤へ

社内システムの認証基盤（BtoE）	✓ 内部統制への対応 ✓ 開発コスト抑制 ✓ ユーザー（社員）の利便性の向上	✓ 信頼できるユーザー、端末からのクラウド利用 ✓ スマホ活用への対応
取引先システム提供の認証基盤（BtoB）	✓ 信頼できる組織、ユーザーの認証 ✓ システムの安全な外部公開 ✓ 提供側によるID管理	✓ 難しい初期設定の回避 ✓ 利用者側の多ID問題の解決
顧客向けサービスの認証基盤（BtoC）	✓ ユーザー利便性の確保 ✓ セルフサービスによる利用 ✓ 大量ユーザー、アクセス対応 ✓ ピーク性のあるアクセス対応	✓ スマホファースト、スマホ完結 ✓ 提携先アプリとのSSO、連携

ビジネスのデジタル変容への必要性が高まる

社内システムの認証基盤（BtoE）

取引先システム提供の認証基盤（BtoB）

- ✓ ゲートウェイ方式の認証基盤が得意とする対象。
- ✓ クラウド活用、モバイル活用の広がりにより、フェデレーション方式が併用されるように。

顧客向けサービスの認証基盤（BtoC）

- ✓ フェデレーション方式（アイデンティティ連携対応）の認証基盤が得意とする対象。

ビジネスのデジタル変容への対応はBtoC から BtoE へと浸透していく

認証基盤に求められること

クラウドの活用	クロスドメイン環境への対応
モバイルの活用	Webアプリもネイティブアプリも
ソーシャルの活用	簡単なユーザー登録とシングルサインオン

認証基盤に求められるようになること

ビジネスプロセスの自動連携	API利用時のアクセス管理
ユーザーの情報やデータの活用と分析	ユーザー意思に基づく情報やデータの提供
多様なデバイスの活用	デバイスの登録関連付け

アイデンティティ連携技術への対応が必要となる

ビジネスのデジタル変容への対応

- クロスドメイン環境への対応
- API利用時のアクセス管理
- Webアプリもネイティブアプリも
- ユーザー意思に基づく情報やデータの提供
- 簡単なユーザー登録とシングルサインオン
- デバイスの登録関連付け

認証基盤のアイデンティティ連携の技術への対応

アイデンティティ連携とは

エンティティ と アイデンティティ

アイデンティティ
＝ 属性の集合

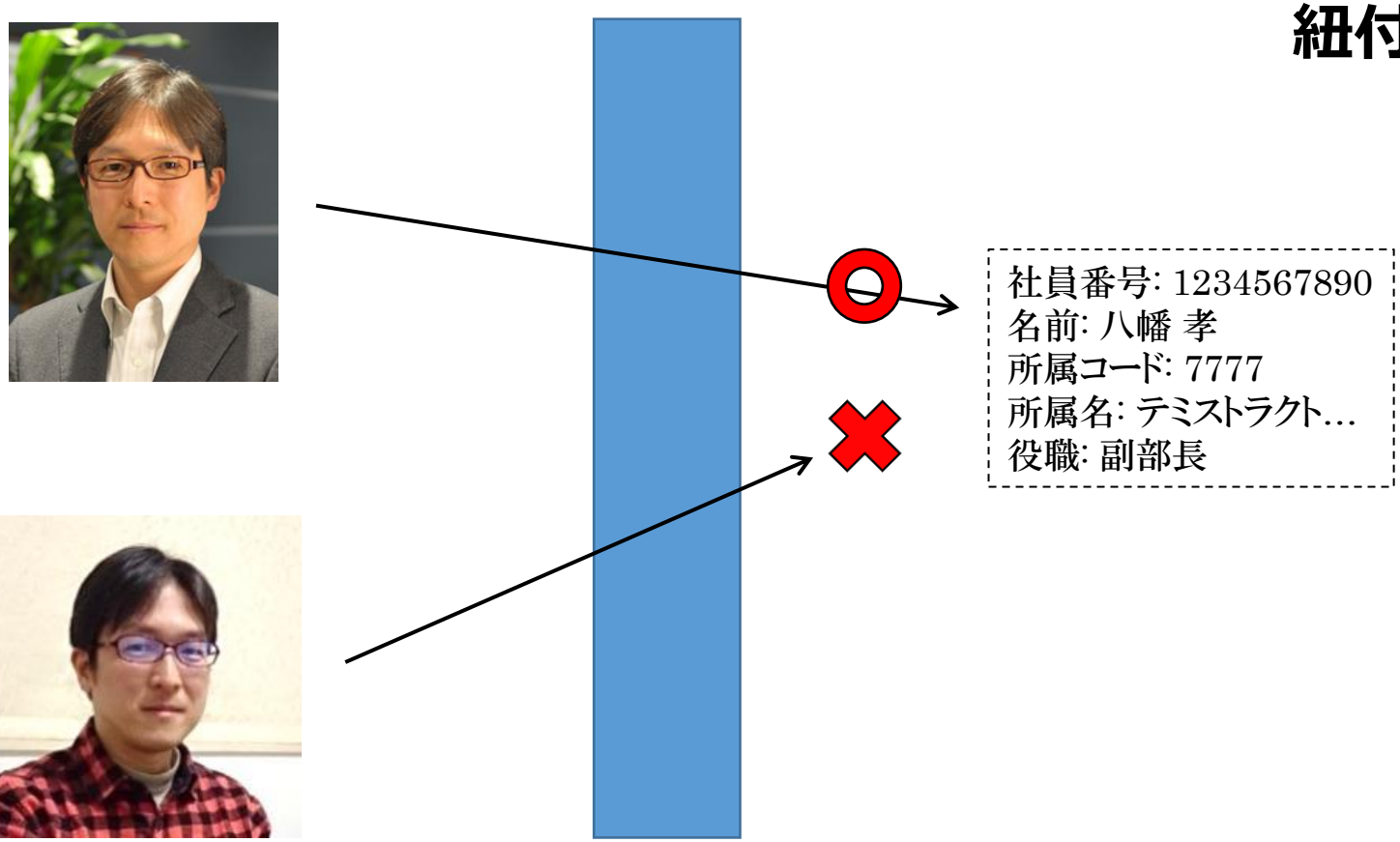
エンティティ（実体）

身長が160cmくらい
黒い髪
メガネをかけている
関西弁を話す
…

社員番号: 1234567890
名前: 八幡 孝
所属コード: 7777
所属名: テミストラクト…
役職: 副部長

認証とは？

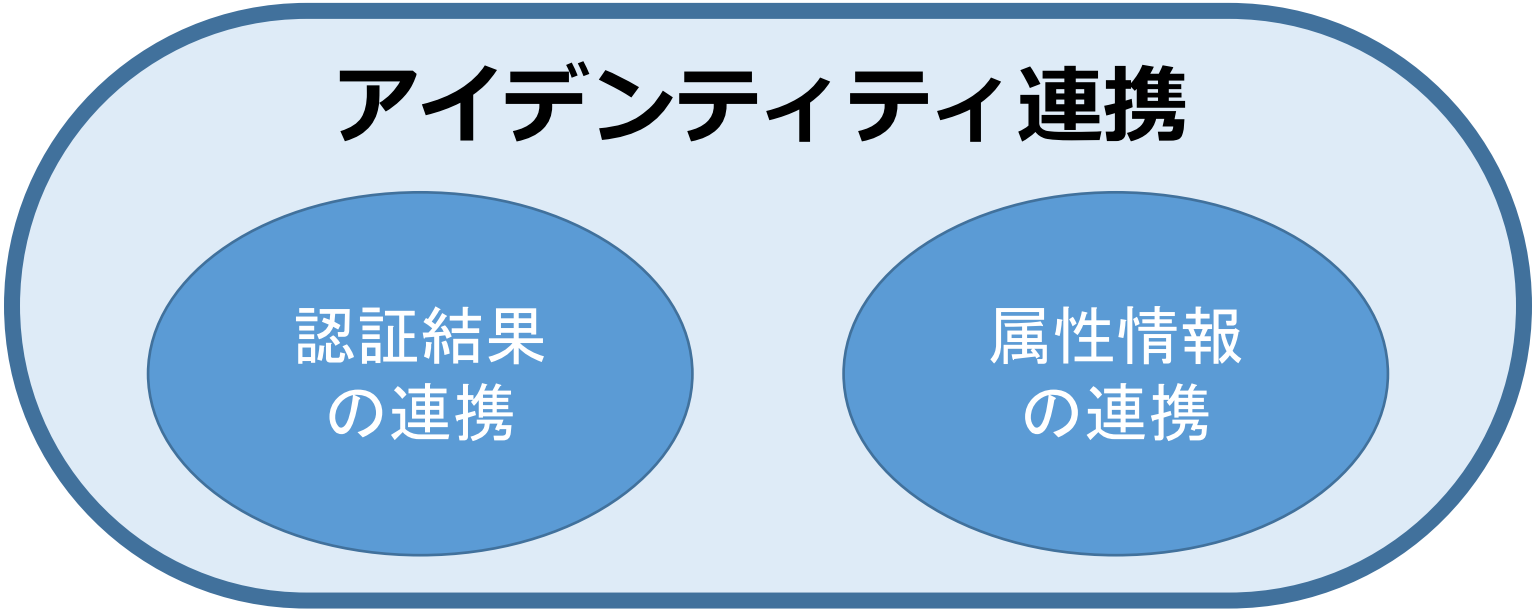
アクセスをしている主体を、
システムが認識しているアイデンティティと、
本人だけが知っている情報、本人だけ所有する情報を用いて
紐付ける



アイデンティティ連携とは

ID連携とは、異なる組織間でユーザのID（アイデンティティ）データを連携し、サービスの質の向上を図る仕組みのことです。

経済産業省 ホームページより引用
http://www.meti.go.jp/policy/it_policy/id_renkei/



アイデンティティ連携技術標準

アイデンティティ連携の技術群

アイデンティティ連携の技術群

- 標準化団体 OASIS で策定
- ユーザーの認証、認可、属性に関する情報をネットワーク上でやり取りするための技術標準
- XMLベース

  - Assertions and Protocols
  - Bindings
  - Profiles
  - …

  http://saml.xml.org/saml-specifications

アイデンティティ連携の技術群

- IETF oauth wg で策定
- HTTPベースのAPI, リソースへのアクセス許可を取得するための技術標準
- ユーザー同意のもと、制限された権限で許可が可能。

  - RFC 6749 The OAuth 2.0 Authorization Framework
  - RFC 6750 The OAuth 2.0 Authorization Framework: Bearer Token Usage
  - RFC 7636 Proof Key for Code Exchange by OAuth Public Clients
  - RFC 7662 OAuth 2.0 Token Introspection
  - …

  https://datatracker.ietf.org/wg/oauth/documents/

アイデンティティ連携の技術群

- OpenID Foundation で策定
- アイデンティティ情報（認証結果、属性情報）を、安全にかつ、ユーザーの同意、制御の下で、交換するための技術標準
- OAuth 2.0 上に構築
- RESTベースのプロトコル、JSONベースのデータ構造

  - OpenID Connect Core
  - OpenID Connect Discovery
  - OpenID Connect Dynamic Client Registration
  - …

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

アイデンティティ連携の技術群

SCIM

- IETF scim wg で策定
- アイデンティティ情報の参照やプロビジョニングを、クラウドサービス間、クラウドサービスと企業間などで行なうための技術標準
- RESTベースのプロトコル、JSONベースのデータ構造

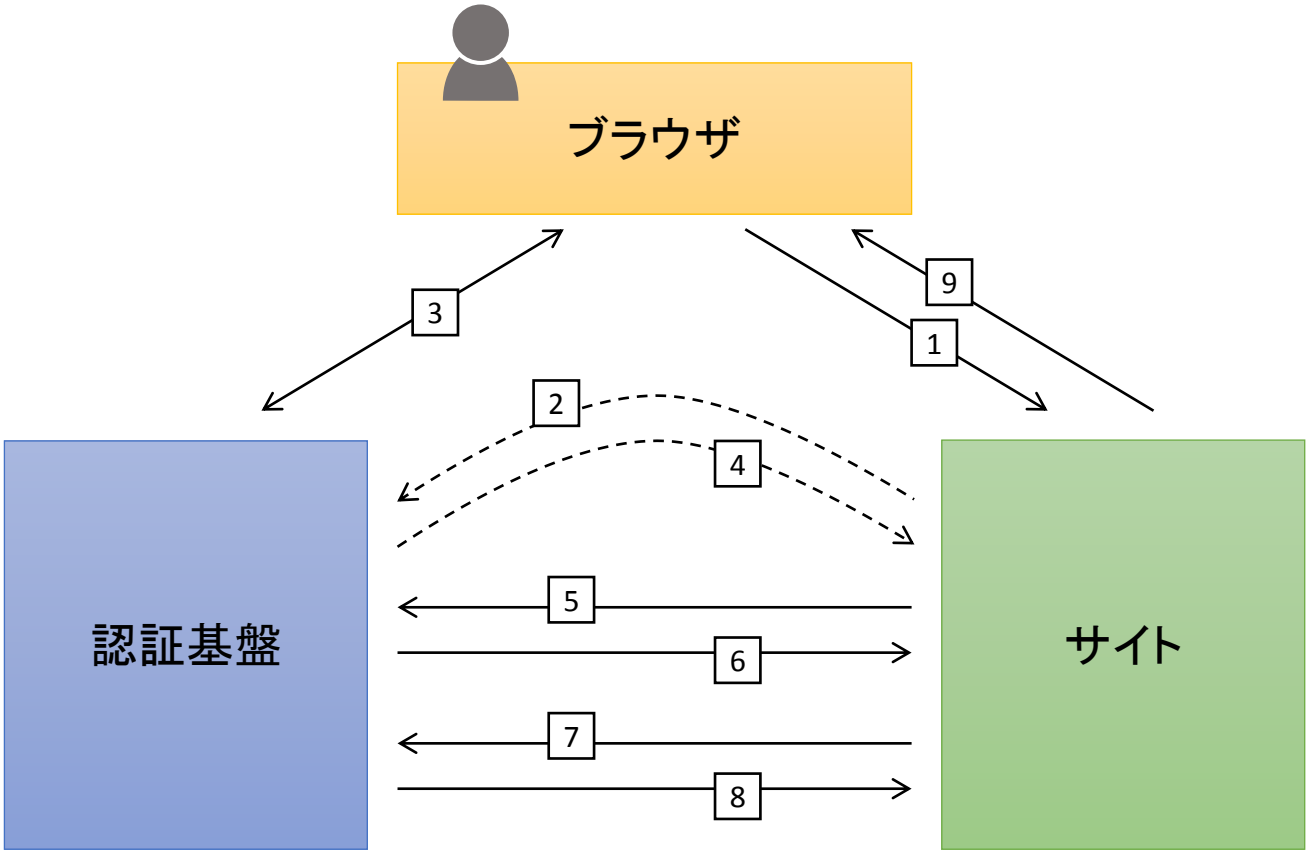
- RFC 7643 System for Cross-domain Identity Management: Core Schema
- RFC 7644 System for Cross-domain Identity Management: Protocol
- …

https://datatracker.ietf.org/wg/scim/documents/

アイデンティティ連携技術でどう対応するか？

クロスドメイン環境でのシングルサインオン 1

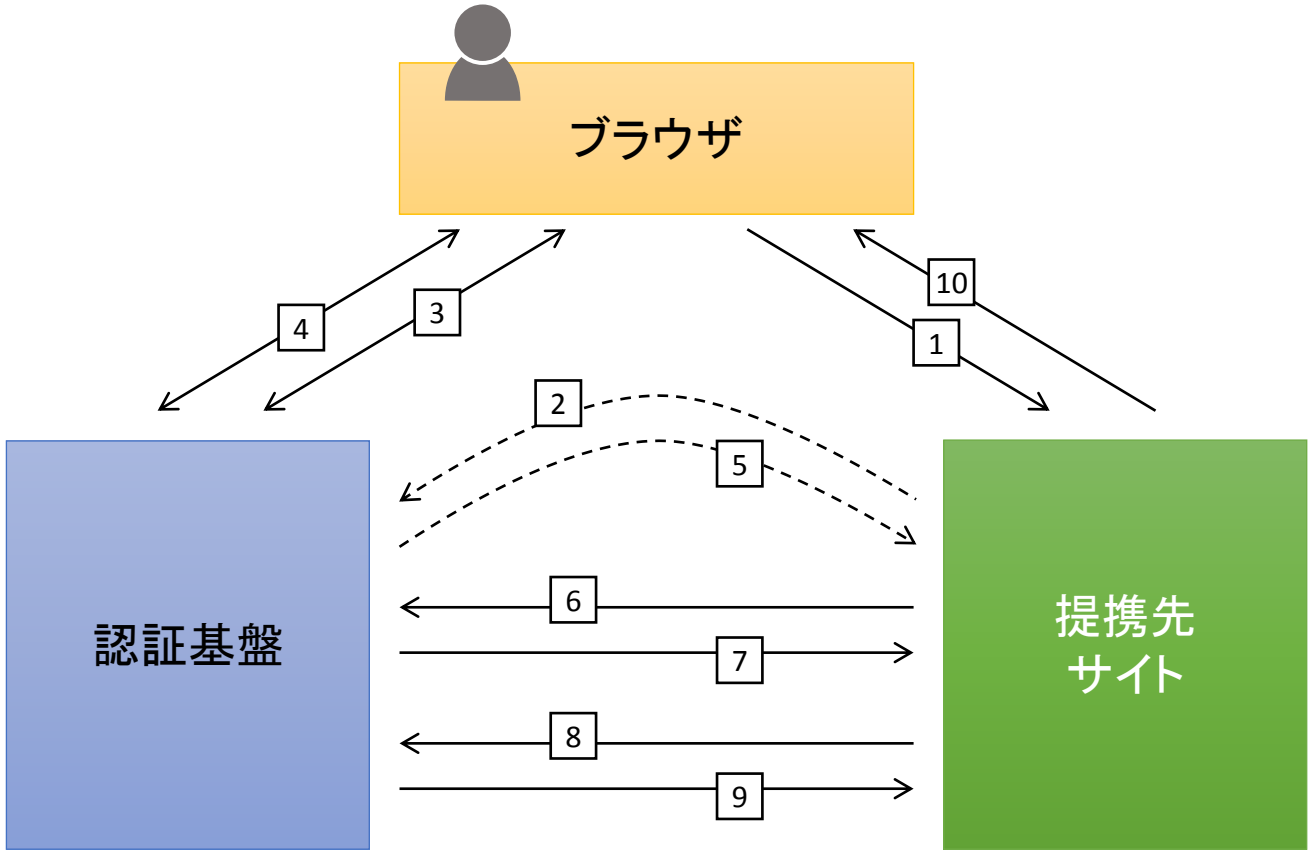
OpenID Connect



1. サイトへアクセス
2. 認証要求を送信
3. ユーザーを認証
4. 認可コードを応答
5. 認可コードを使ってトークンを要求
6. IDトークン(認証結果)とユーザー情報アクセス用トークンを応答
7. ユーザー情報を要求
8. ユーザー情報を応答
9. サイトコンテンツを応答

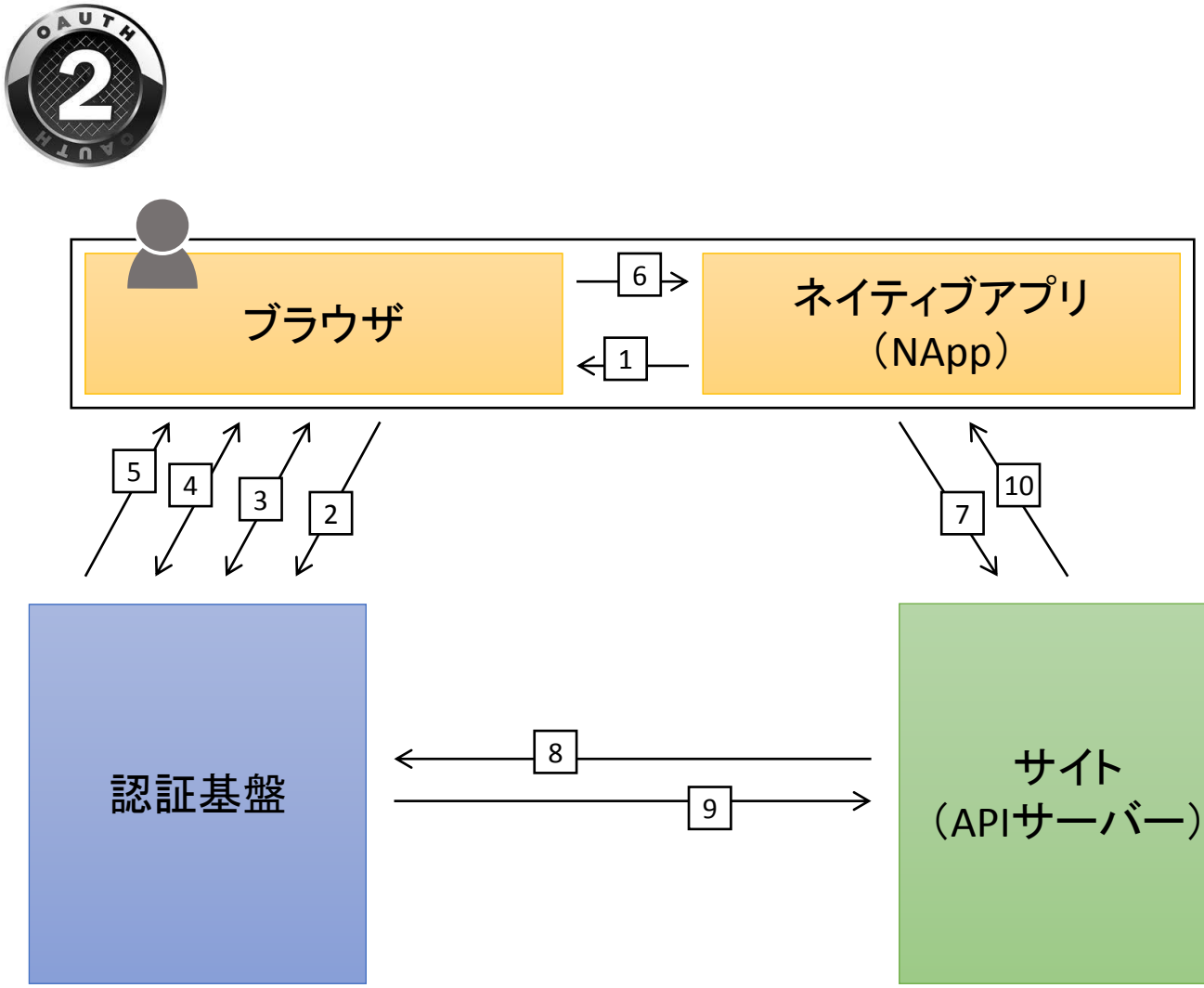
クロスドメイン環境でのシングルサインオン 2

OpenID Connect



1. サイトへアクセス
2. 認証要求を送信
3. ユーザーを認証
4. ユーザーの同意を取得
5. 認可コードを応答
6. 認可コードを使って
   トークンを要求
7. IDトークン(認証結果)
   とユーザー情報アクセ
   ス用トークンを応答
8. ユーザー情報を要求
9. ユーザー情報を応答
10. サイトコンテンツを
    応答

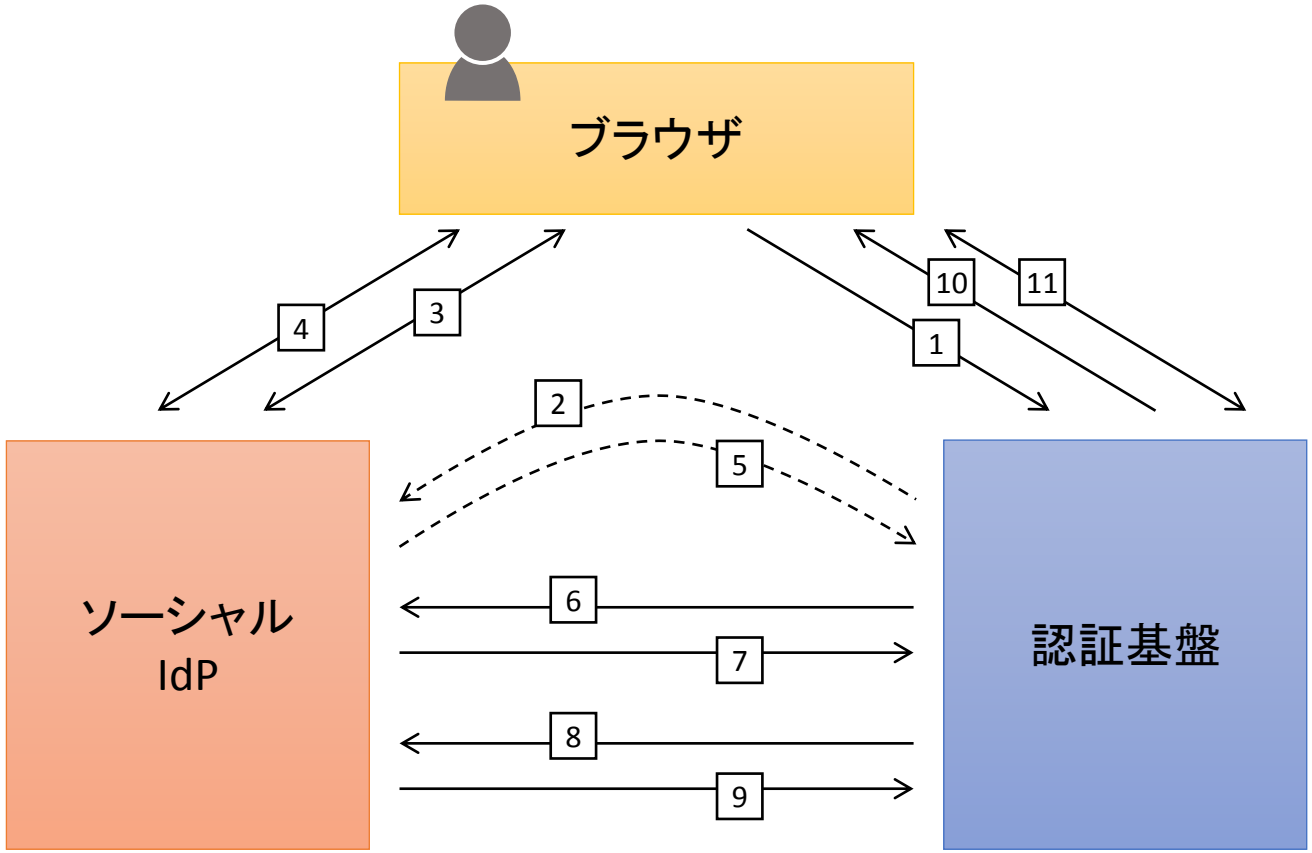
モバイル活用への展開（ネイティブアプリ対応）



1.NAppでログイン操作、ブラウザを起動
2. ブラウザからアクセス許可要求を送信
3. ユーザーを認証
4. ユーザーの同意を取得
5. APIアクセス用トークンを応答
6. アクセストークンをネイティブアプリへ送る
7. APIへアクセス
8. アクセストークンの情報を要求
9. アクセストークンの情報を応答
10. APIの実行結果を応答

ソーシャルIDを使った登録

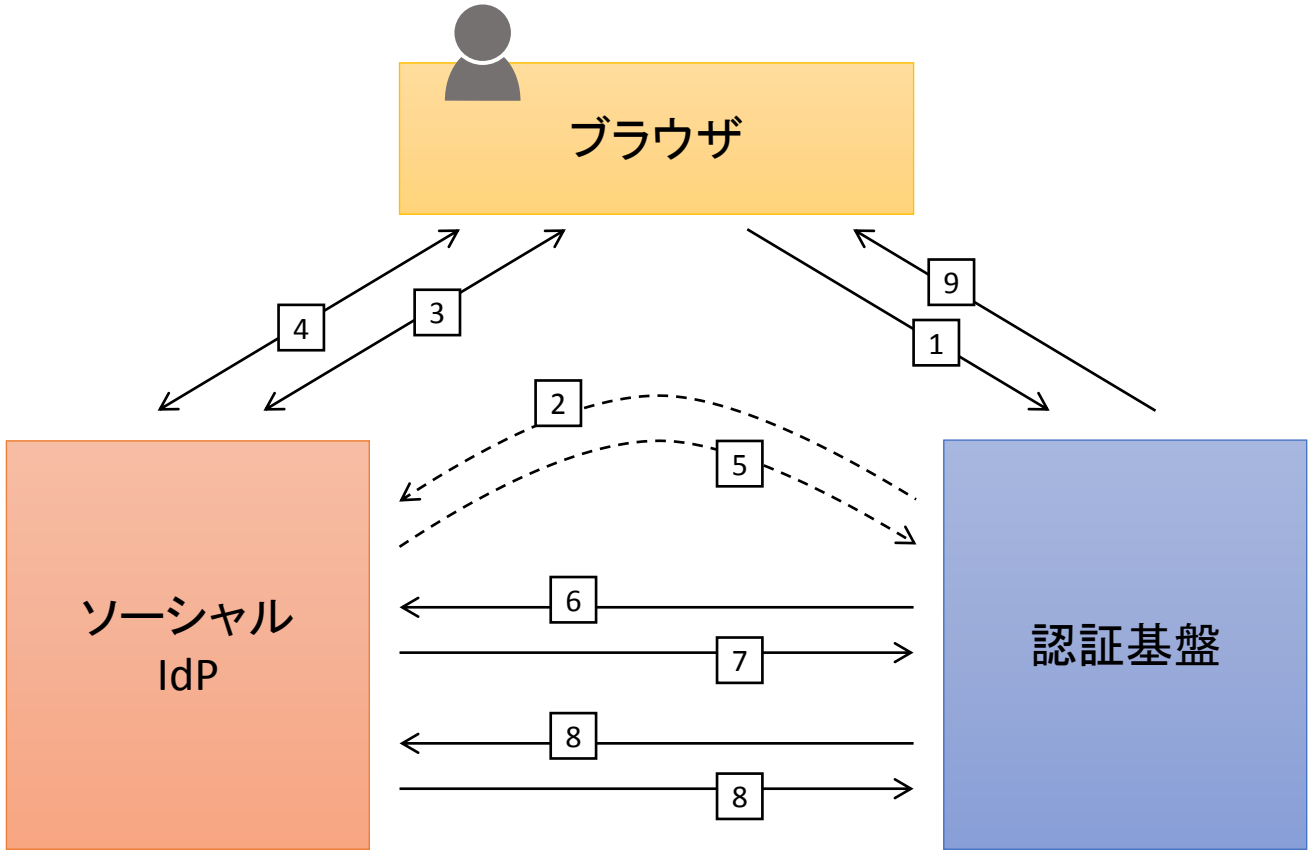
OpenID Connect



1. 「○○で登録」機能へアクセス
2. 認証要求を送信
3. ユーザーを認証
4. ユーザーの同意を取得
5. 認可コードを応答
6. 認可コードを使ってトークンを要求
7. IDトークン(認証結果)とユーザー情報アクセス用トークンを応答
8. ユーザー情報を要求
9. ユーザー情報を応答
10. ユーザー登録画面にソーシャルIdPから受け取った基本属性を埋め込んで応答
11. 不足情報を追記して登録を完了

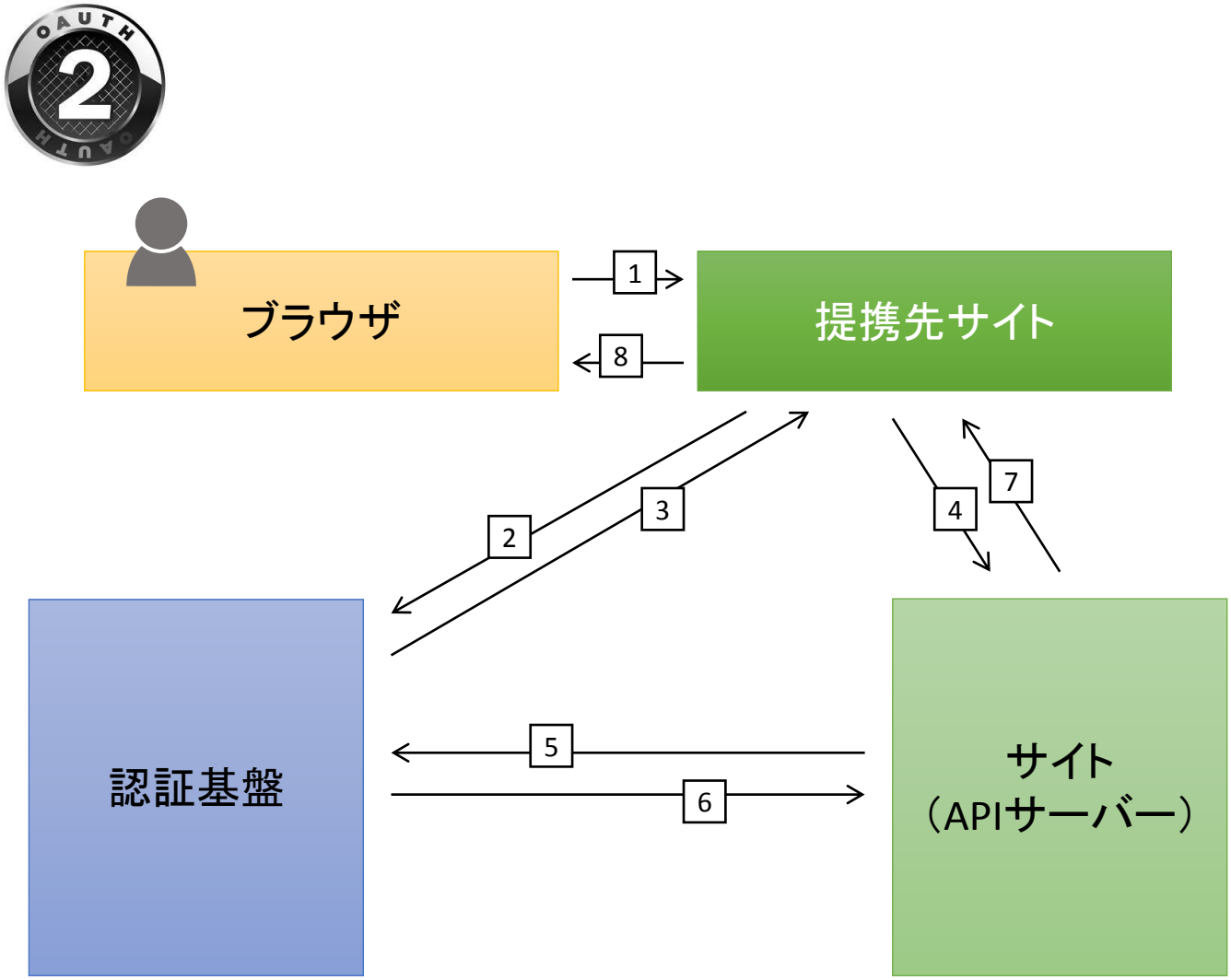
ソーシャルIDを使ったシングルサインオン

OpenID Connect



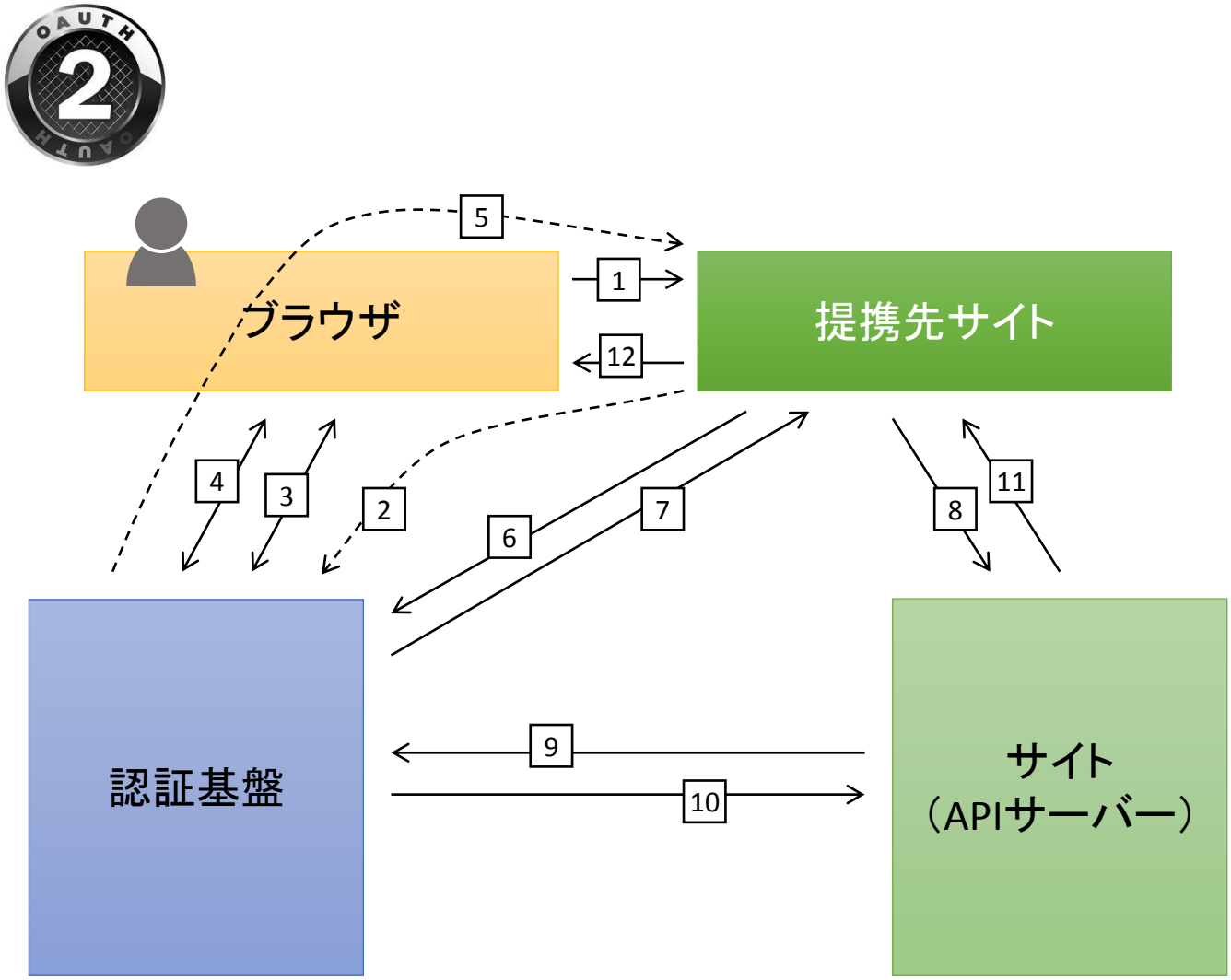
1. 「○○でログイン」機能へアクセス
2. 認証要求を送信
3. ユーザーを認証
4. (ユーザーの同意を取得)
5. 認可コードを応答
6. 認可コードを使ってトークンを要求
7. IDトークン(認証結果)を応答
8. （ユーザー情報を再取得して最新化）
9. 認証完了、次の処理へ

バックエンドでのAPI連携 1



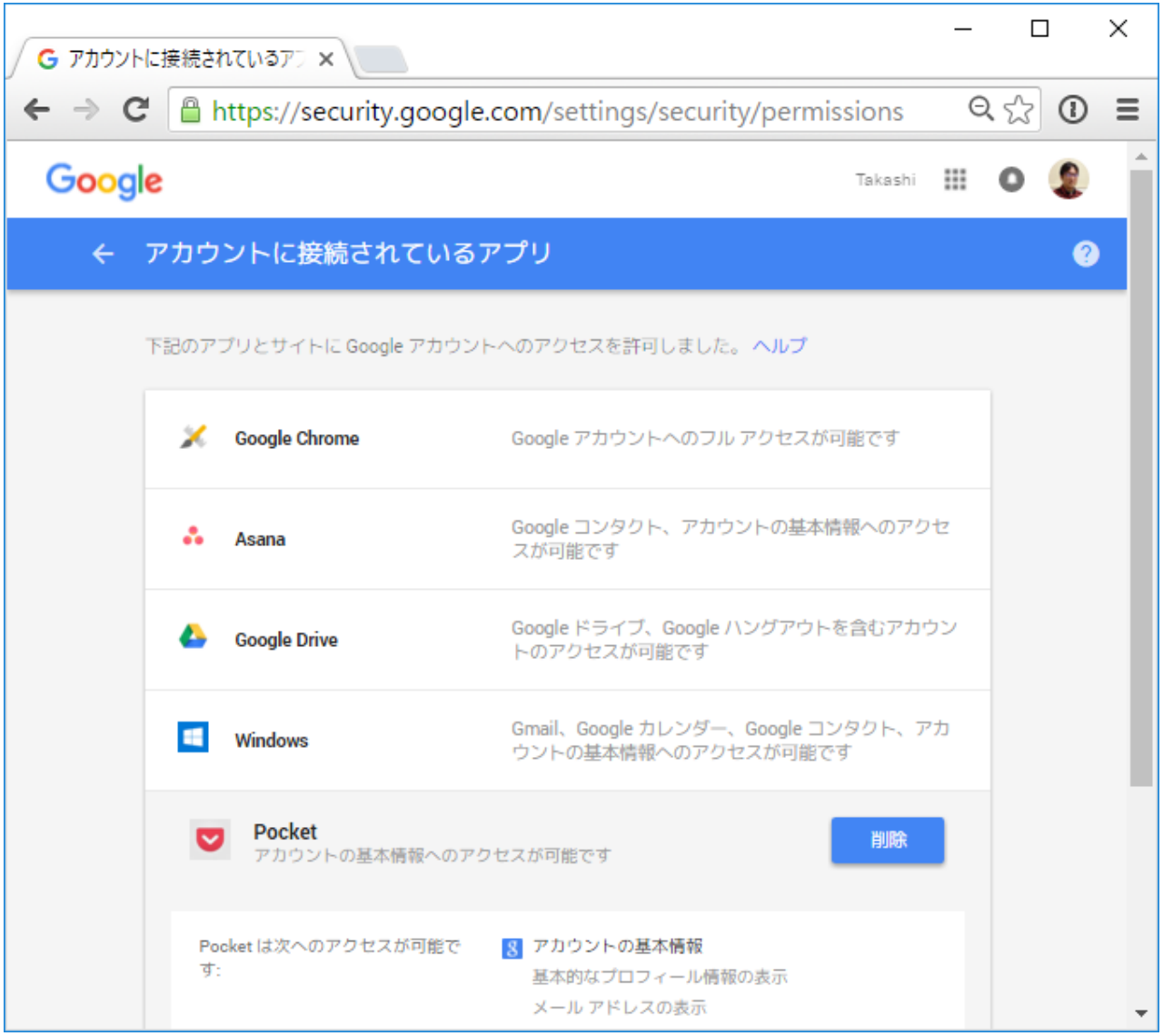
1. 提携先サイトへアクセス
2. 提携先サイトがAPIアクセス用トークンを要求
3. APIアクセス用トークンを応答
4. APIへアクセス
5. アクセストークンの情報を要求
6. アクセストークンの情報を応答
7. APIの実行結果を応答(実行は提携先サイトの権限で)
8. 提携先サイトがコンテンツを応答

バックエンドでのAPI連携 2



1. 提携先サイトへアクセス
2. 提携先サイトがアクセス許可要求を送信
3. ユーザーを認証
4. ユーザーの同意を取得
5. 認可コードを応答
6. 認可コードを使ってトークンを要求
7. APIアクセス用トークンを応答
8. APIへアクセス
9. アクセストークンの情報を要求
10. アクセストークンの情報を応答
11 APIの実行結果を応答(実行はユーザーの権限で)
12. 提携先サイトがコンテンツを応答

ユーザーの同意の取得、同意の取り消し



デバイスの認証、アクセス許可

- OAuth 2.0 Device Flow？それとも？

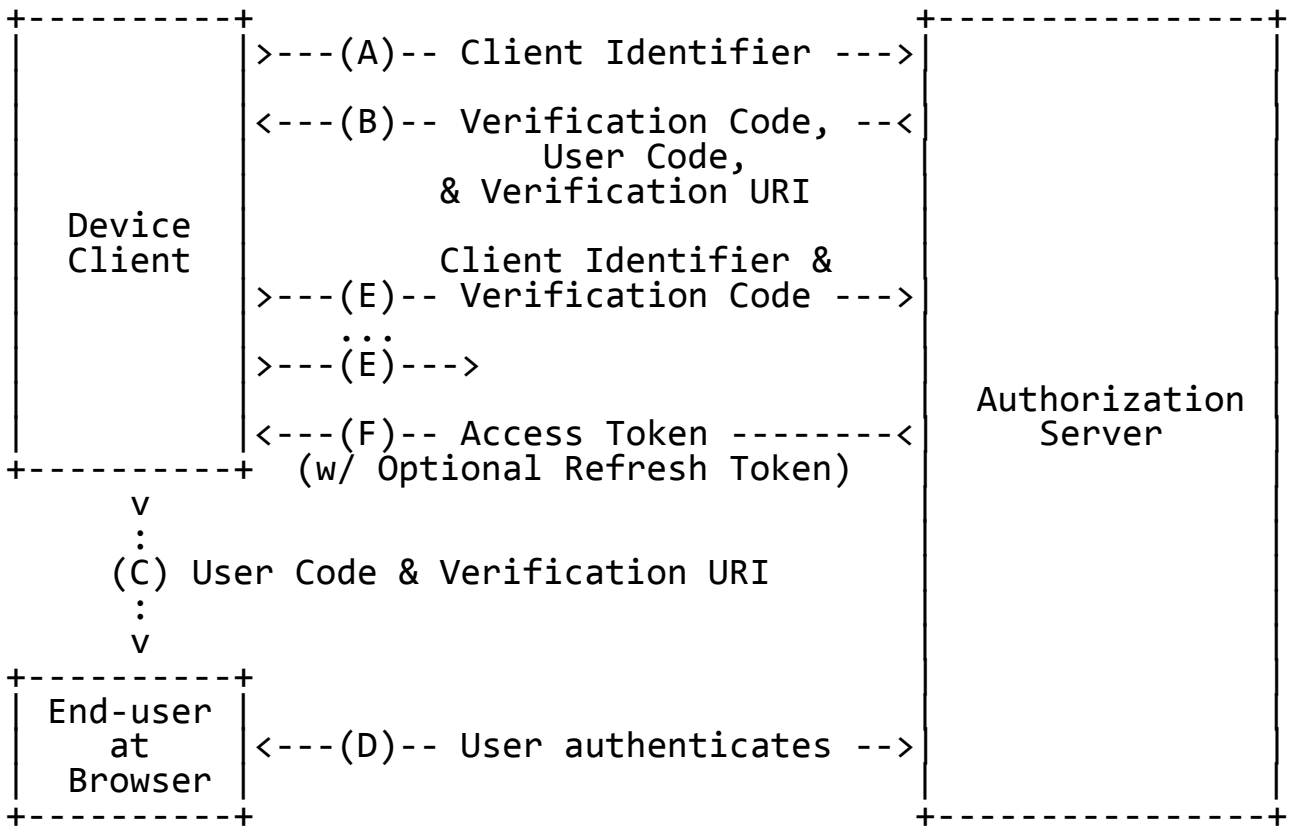


Figure 1: Device Flow.

OAuth 2.0 Device Flow draft-ietf-oauth-device-flow-01 より引用
https://tools.ietf.org/html/draft-ietf-oauth-device-flow-01

まとめ

まとめ

- ビジネスのデジタル変容という潮流の中にある
- 認証基盤に求められることが変わる
- アイデンティティ連携技術への対応が不可欠である
- BtoC向けのみならず、BtoB, BtoEも変化が必要となる

ご清聴ありがとうございました

ThemiStruct
テミストラクト

【お問い合わせ先】
株式会社オージス総研
TEL: 03-6712-1201 / 06-6871-7998
mail: info@ogis-ri.co.jp

OGIS-RI