B2B、B2C向けWebサービスにおける認証基盤のあり方

株式会社オージス総研
事業開発本部 テミストラクトソリューション部
金井　敦

本日のお話し

- Part１：それって認証なの？認可なの？ 8min
- Part２：Webサービスにおける認証・認可 7min
- Part３：認証基盤が提供する認証・認可 20min
- Part４：まとめ 5min

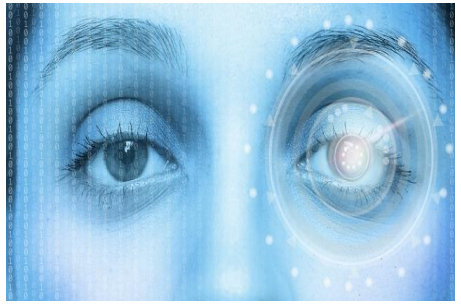
全体で40分間

Part１：
それって認証なの？認可なの？

認証について考える

◆ 認証（Authentication）

- 相手が誰であるかを確認すること。（あなた何者？）
- 相手が誰であるかを確認する手段は様々。
  - アナログでは、運転免許証、健康保険証、住民票、学生証、パスポート、名刺、知人の紹介など
  - デジタルでは、ID/パスワード、指紋、顔、ICカードなど
- 確認方法によって、本人確認の精度や確認できる情報も様々。
- Webサービスでは対面での本人確認を行うことや身分証明書の提示が（現段階では）難しいため、精度を高める方法が課題となりやすい。



認可について考える

◆ 認可（Authorization）

- 要求する権限を有しているかを確認すること。（権利ある？）
- 権限を持っているかを確認する手段は様々。
  - アナログでは、運転免許証、健康保険証、パスポート、チケット、クーポン、鍵、第三者の印鑑など
  - デジタルでは、ユーザー種別、グループ情報、ロール情報、トークンなど
- 認証と認可は異なる概念のものである。認可を行うために、認証が必要であるとは限らない。認証されたからと言って、必ず認可されるとも限らない。
  - 切符やクーポン、コインロッカーを使うのに誰であるかを名乗る必要はない
  - 取得した権限を第三者に譲渡して利用させることもあり得る
  - 相手が誰であるかを高い精度で確認できたとしても、要求を受け入れてよいかは別問題

Webサービスと認証・認可

◆ サービス利用時にユーザー登録を行いログインをして利用するWebサービスにおいて、認証と認可は必ず必要となる処理である

- Webサービスでは対面での本人確認を行うことや身分証明書の提示が（現段階では）難しいため、一般的には**ユーザー登録時に設定したパスワード情報を再提示することで認証を行う**ケースが多い。

- **認証における主な脅威は身分を偽られること（なりすまし、虚偽の申告）**であるが、パスワードを使った認証は非常に理解しやすく使いやすい反面、脅威を受けやすい。このため**認証の強度や精度を高める方法が課題となりやすい。**

- Webサービスにおいては多くの場合、誰であるかを認証してから、認証された相手に対して認可（権限）を与えたり、確認する構造であるため認証と認可が混同されやすいが、**認証されたユーザーアカウントに対して適正な権限が割り当てられ、権限の範囲でサービスを利用できる必要**がある。

- **認可における主な脅威は権限の不正取得や越権行為**であるが、他者に権限を一部委譲したくてもアカウントの単位で権限設定されているため、持っている**一部の権限やデータのみを切り出して提供することが構造的に難しい。**

Webサービスにおける認証・認可とは

◆ 店舗サービスの例