標準化部会
デジタルアイデンティティWG

エンタープライズ認可（Authorization）入門のご紹介

2025/7/25

WGリーダー　貞弘　崇行
伊藤忠テクノソリューションズ株式会社

概要

デジタルアイデンティティWGでは、近日中に「エンタープライズ認可（Authorization）入門」を公開します。

企業や組織において重要なデジタル資産（情報、システム）を守るためには、アイデンティティや認証の適切な管理だけでなく、認可の適切に管理も必要です。

そのための第一歩として、まずは用語や概念の整理を目指した資料になっています。この資料の概要をご紹介し、ポイントとなる事項について解説いたします。

デジタルアイデンティティWGの紹介

活動の目的

「デジタルアイデンティティWGの目的」

本WGは“デジタルアイデンティティ”全般を広く議論する場として、
今年度で設立20年目を迎えました。

本WGでは、デジタルアイデンティティの課題等について議論し、導入指針や各種報告書の提示、執筆活動・セミナー・勉強会等での啓蒙活動および普及促進、関連他団体との連携による市場活性化等を目的として活動を行っています。

メンバー紹介：
https://www.jnsa.org/active/std_idm.html

成果物：
https://www.jnsa.org/result/digitalidentity/index.html

本WGの歴史

年	成果物等	WG名称
2005	WG設立	内部統制におけるアイデンティティ管理WG
2006	合宿実施（三浦マホロバツインズ）	
2007	内部統制における アイデンティティ管理解説書（第１版）	
2008	内部統制における アイデンティティ管理解説書（第２版）	
2009		
2010	クラウド環境における アイデンティティ管理ガイドライン （企業向け調査レポート）	セキュリティにおけるアイデンティティ管理WG
2011		
2012	改定新版　クラウド環境におけるアイデンティティ管理ガイドライン（書籍） エンタープライズ ロール管理解説書（第１版）	
2013	OpenID ConnectとSCIMの エンタープライズ利用ガイドライン	アイデンティティ管理WG
2014	エンタープライズ ロール管理解説書（第2版）	
2015	１０周年記念セミナー！ エンタープライズ ロール管理解説書（第3版）	
2016	エンタープライズにおける特権ID管理 解説書（第１版）	
2017	ID管理システム導入における現状把握チェックリスト（第１版） クロスボーダー時代のアイデンティティ管理セミナー!	
2018	内部統制における アイデンティティ管理解説書（第２版）	
2019	クレデンシャルの歴史（読み物）	
2020	Software Design 11月号特集（雑誌）	デジタルアイデンティティWG
2021	Enterprise Identity Day！ 標準化部会セミナー！	
2022	今さら聞けない暗号技術＆認証･認可（書籍） 改定新版　エンタープライズにおける特権ID管理ガイドライン（解説編） ミニウェビナー＆Youtube 「？？？とアイデンティティ」	
2023	改定新版　エンタープライズにおける特権ID管理ガイドライン（実践編）	

これまでの成果物（出版、報告書）

https://www.jnsa.org/result/digitalidentity/index.html

▶ ・2023/5/8

報告書 ニュージーランド政府による"Identification Management Standards"に関する考察
==NIST SP800-63 "Digital Identity Guidelines"との比較結果等==

▶ ・2023/3/31

報告書 【改定新版】特権ID管理ガイドライン　解説編

▶ ・2023/3/6

関連書籍発売 「Software Design　今さら聞けない認証・認可」が再編集されて別冊シリーズで発売されました。
技術評論社さんのページにリンクします。

▶ ・セミナー 2023/5/25開催　YouTube JNSAChannelで公開中！セミナーページからどうぞ

セミナー｜デジタルアイデンティティWGミニウェビナー 「？？？とアイデンティティ」

2021/11/26

セミナー資料　2021年11月26日（金）開催
「Enterprise Identity Day　再考！！エンタープライズ・アイデンティティ～ゼロトラストセキュリティの礎を確立する～」

▶ ・執筆 「Software Design」2020年11月号
特集1「今さら聞けない認証・認可ーセキュアなIAMを実現するために覚えておきたいこと」
技術評論社さんのページにリンクします。

▶ ・読み物 「クレデンシャルの歴史」

▶ ・報告書 「ID管理システム導入における現状把握チェックリスト （第１版）」

▶ ・出版書籍 「＜改訂新版＞クラウド環境におけるアイデンティティ管理ガイドライン」
Amazonにリンクします

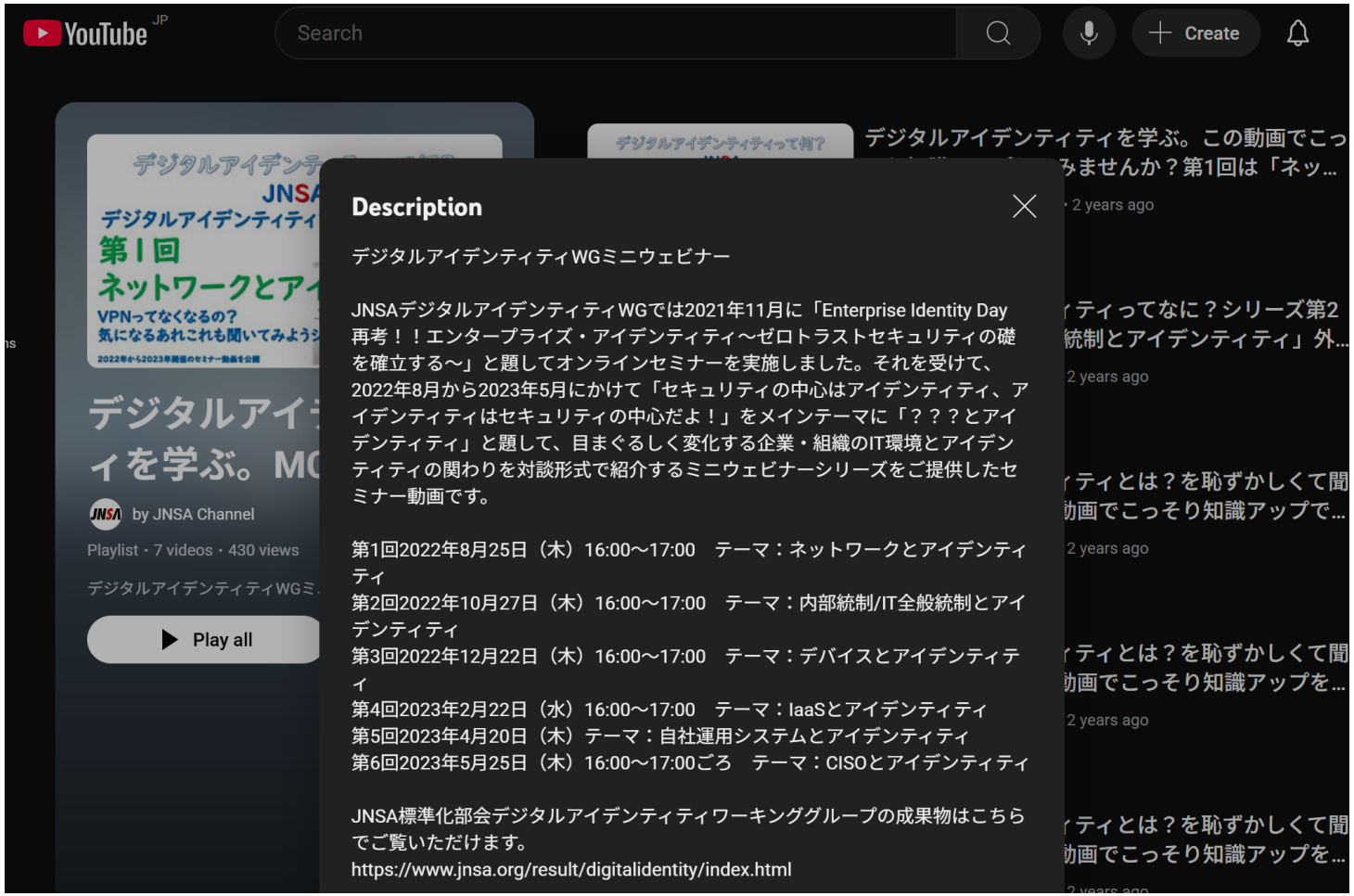
▶ ・報告書 「OpenID ConnectとSCIMのエンタープライズ利用ガイドライン」
（JNSAとOpenID Foundation Japanとの共同執筆）

▶ ・報告書 「エンタープライズにおける特権ID管理解説書（第１版）」

▶ ・報告書 「エンタープライズロール管理解説書（第３版）」

これまでの成果物（ミニウェビナー）

https://www.youtube.com/playlist?list=PL1nvarmw8MRuJfxf8nrBf-Zv4hqEqUlhm



エンタープライズ認可（Authorization）入門

目次構成

目的・ねらい・対象想定読者

- 目的・ねらい
  - 日本の企業・組織における認可管理の高度化を促進する
  - 認可に関する用語・概念を整理し、共通理解を助け、認可の高度化にむけたコミュニケーションのハードルを下げる。

- スコープ
  - 企業・組織において業務に利用されるシステム・ITサービス

- 想定読者
  - セキュリティ管理者・ITリスク管理者
  - Enterprise Architecture担当、社内システム共通基盤担当部門

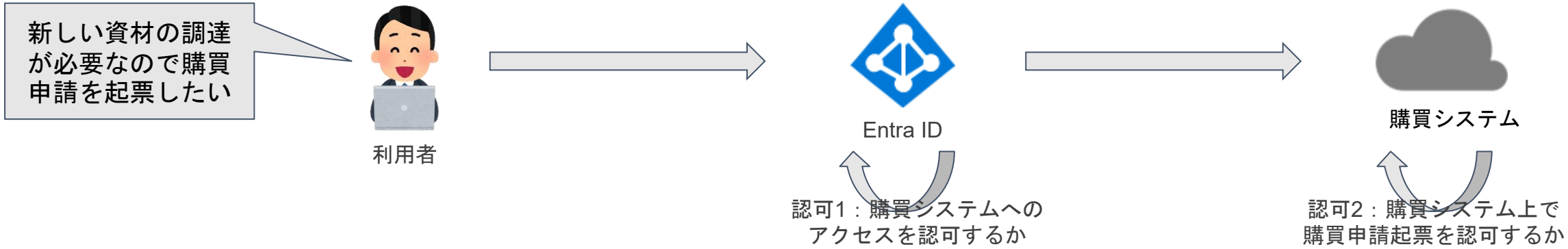
認可の例と本資料の構成

デジタル資産を守る最後の砦である認可だが、適切な認可を実現するためには適切な箇所で適切な考え方に基づいた認可を実施する必要がある。例えば、ある利用者がEntra IDで保護されている購買システムにアクセスして購買申請を起票するケースを考えてみる。

このケースでは以下2箇所での認可を通して、購買申請の起票を認可したと考えられる。

認可1（Entra IDにて）：利用者の所属部署やアクセス状況（場所など）に基づく購買システムへのアクセスの認可*

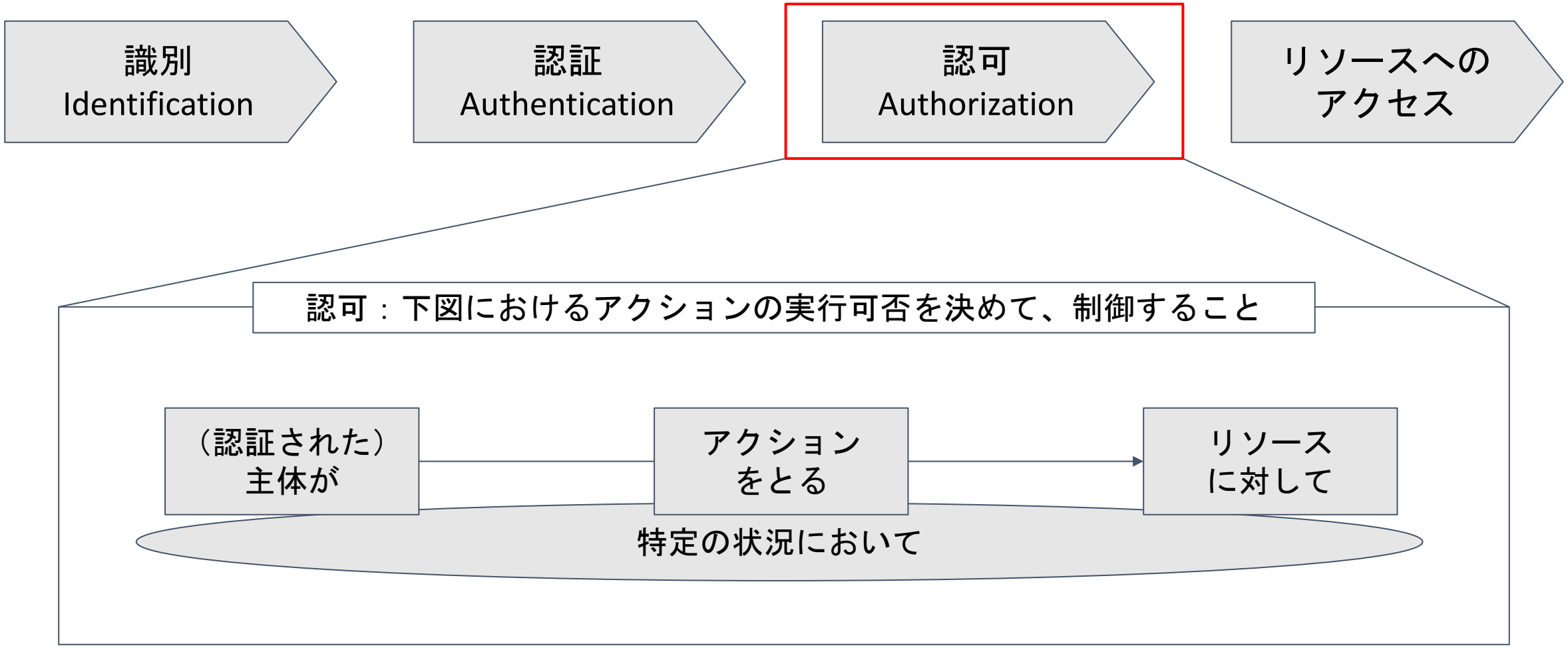
認可2（購買システムにて）：業務上の役割に基づく購買システム上で購買申請起票の認可



本資料では、まず「2. 認可とは」にて認可の定義を整理する。上述の認可1や認可2で用いられることが多いロールや属性に基づくアクセス制御などの考え方については、本資料「3.関連用語や概念との関係」で整理している。さらに、適切な認可を行うために必要なコンポーネントとそこでの考え方の組み合わせ方は、本資料4章、5章で整理している。

*：Entra IDは、利用者の認証を行った後に認証連携先へのアクセスを認可する。ここでは、この認可を指す。

認可とは（図示）1/2

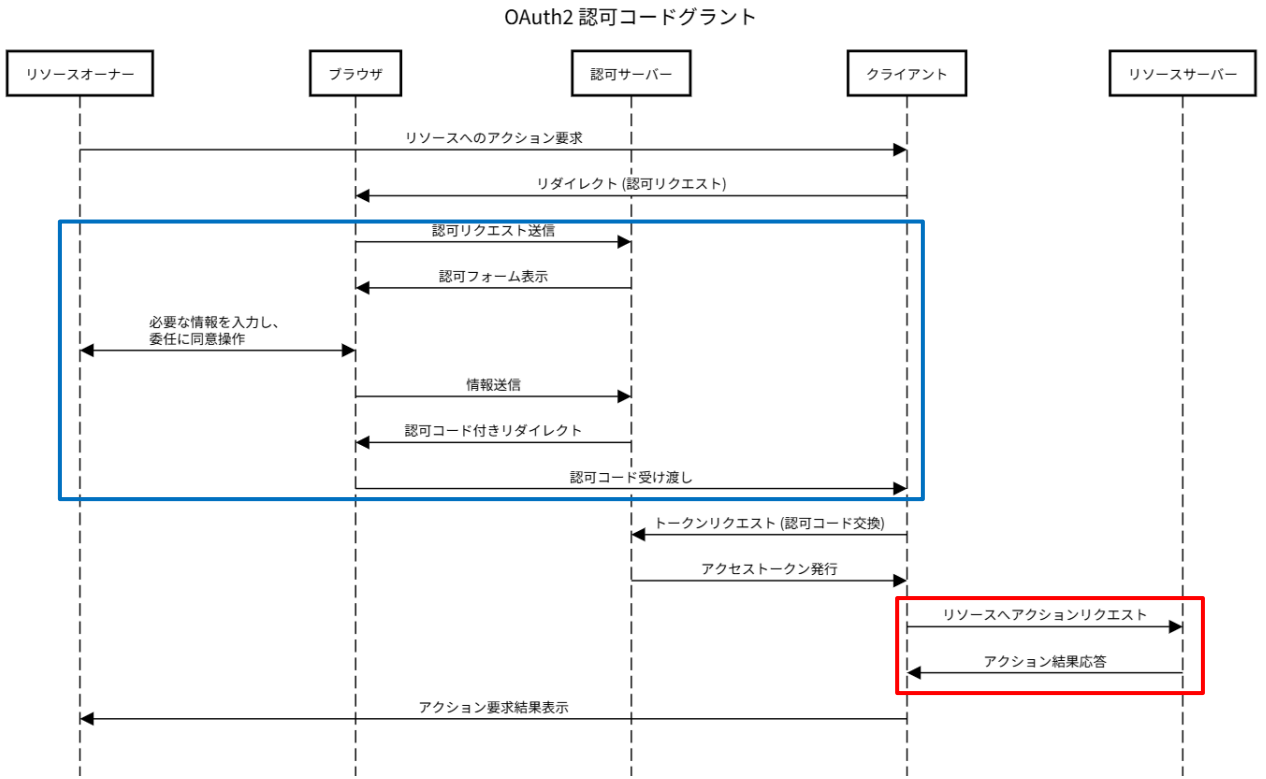

識別
Identification
認証
Authentication
認可
Authorization
リソースへの
アクセス
認可：下図におけるアクションの実行可否を決めて、制御すること
（認証された）
主体が
アクション
をとる
リソース
に対して
特定の状況において

OAuth2における認可の定義 1/3

- OAuth2は「認可フレームワーク」とされる。
- しかし、OAuth2での「認可」は本資料における認可の定義とは異なり、「委譲すること」という意味を持つ。
  - Clientとはリソース所有者の「認可」の元でリソース所有者の代わりに保護されたリソースのリクエストを行うアプリケーションのことです。（RFC 6749 1.1 Rolesより。原文は以下）
    - An application making protected resource requests **on behalf of** the resource owner and with its **authorization**.
  - RFC 4949においても「主体がリソースへアクセスするために与えられる承認」と定義されている（原文は以下）
    - 1a. (I) An approval that is granted to a system entity to access a system resource
- いくつか、OAuth2について説明するサイトでも、「委譲すること」の意味で使われているケースが散見される。（下表赤字部）
  - 認可とは、**第三者のアプリケーションに、自分のアカウントを用いたWebサービスAPIへのアクセス権限を委譲すること**を言います。
  - 認証されたユーザーが、どのリソースやデータにアクセスできるかを決めるプロセスです。
  - 認可（Authorization）は、特定のユーザーがシステム上のリソースにアクセスする権限があるかどうかを確認するプロセス
  - クライアントはリソースオーナーの**認可を得て、リソースオーナーの代理として保護されたリソースに対するリクエストを行う**役割。

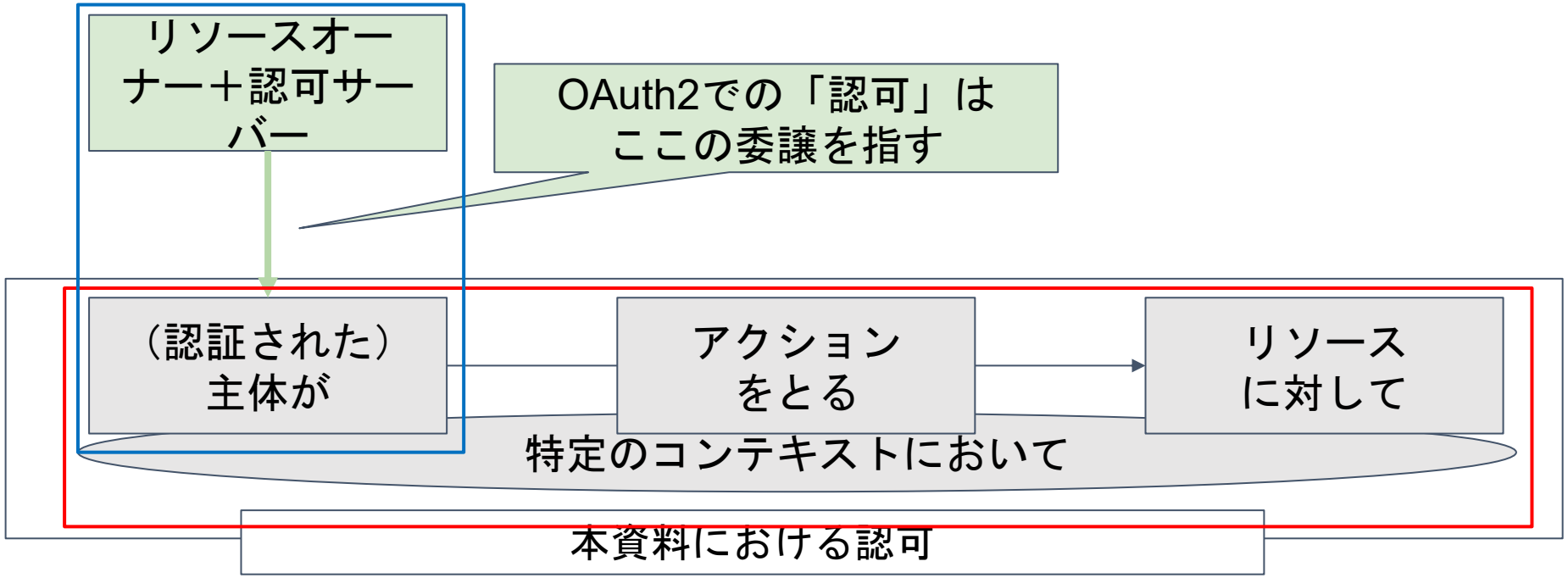
OAuth2における認可の定義 2/3

- OAuth2の一般的なシーケンス（認可コードフロー）は右図の通り。
  - クライアント、リソースオーナー、などについてはRFC 6749 1.1 Rolesを参照
- 本資料における「認可」の定義を踏まえると、リソースに対してアクションを実行する主体はクライアントである。
- そのため、本書における「認可」が適用されるのは右図赤枠部となる。
- 一方、前述の「委譲すること」は右図青枠部で行われている。



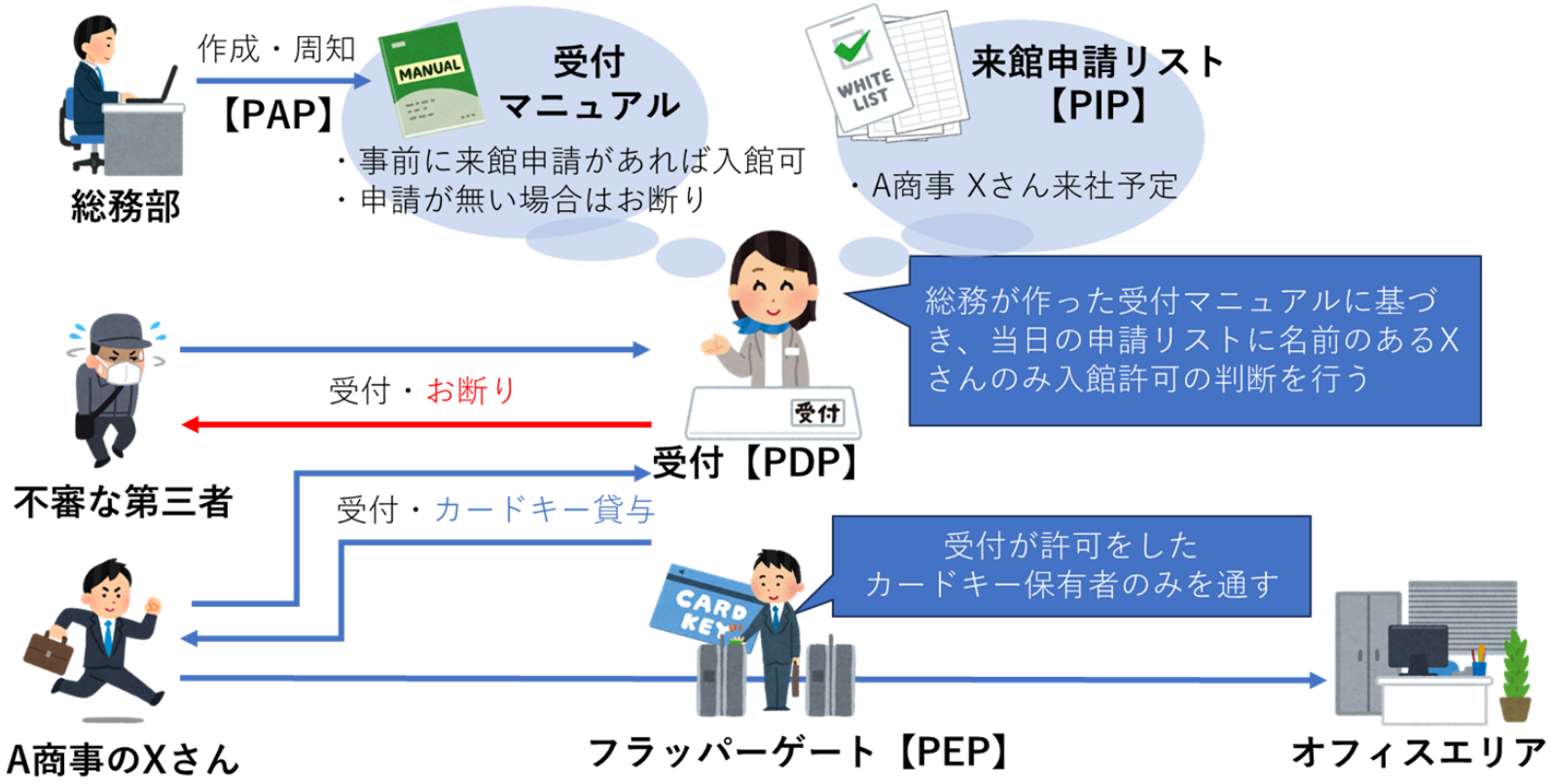
OAuth2における認可の定義 3/3

- OAuth2での「委譲することを認可」を本資料での認可の定義に当てはめると下図の通りとなる。
  - 下図における赤枠と青枠はシーケンス上の赤枠と青枠を示す



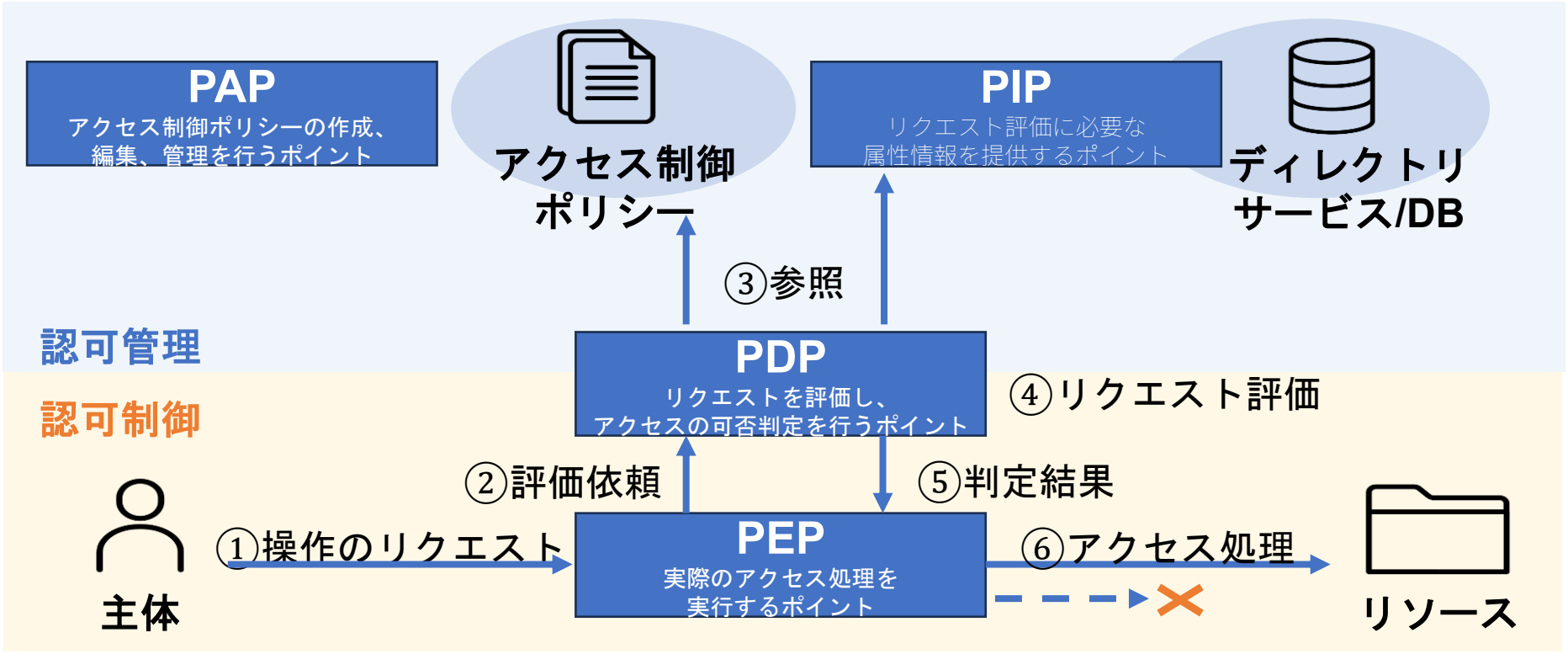
アナログ世界における認可

「認可」の概念モデルと聞くとハードルが高くとも、アナログ世界にも同じ概念は存在する。
例えば来社対応を想像した時、受付担当者は訪問者をフラッパーゲートを通す（認可）かの判断を、訪問者の身元情報（認証）を確認した上で、事前に取り決めた受付マニュアル（アクセス制御ポリシー）に照らし合わせながら判断している。



PxP概念モデル

前述したPxPの各用語について、図示したものが以下の通り。
アクセス元（主体）からリクエスト先（リソース）へのアクセス（アクション）に適正なコントロールを適用するためには、各PxPのコンポーネントによりアクセスの可否判定および判定結果に基づくアクセス処理を行う必要がある。



アクセス制御の流れ

①アクセス元がアクション（閲覧や編集等）をリクエスト

②リクエスト内容の諾否について評価を依頼

③事前に取り決めたアクセス制御ポリシーを参照

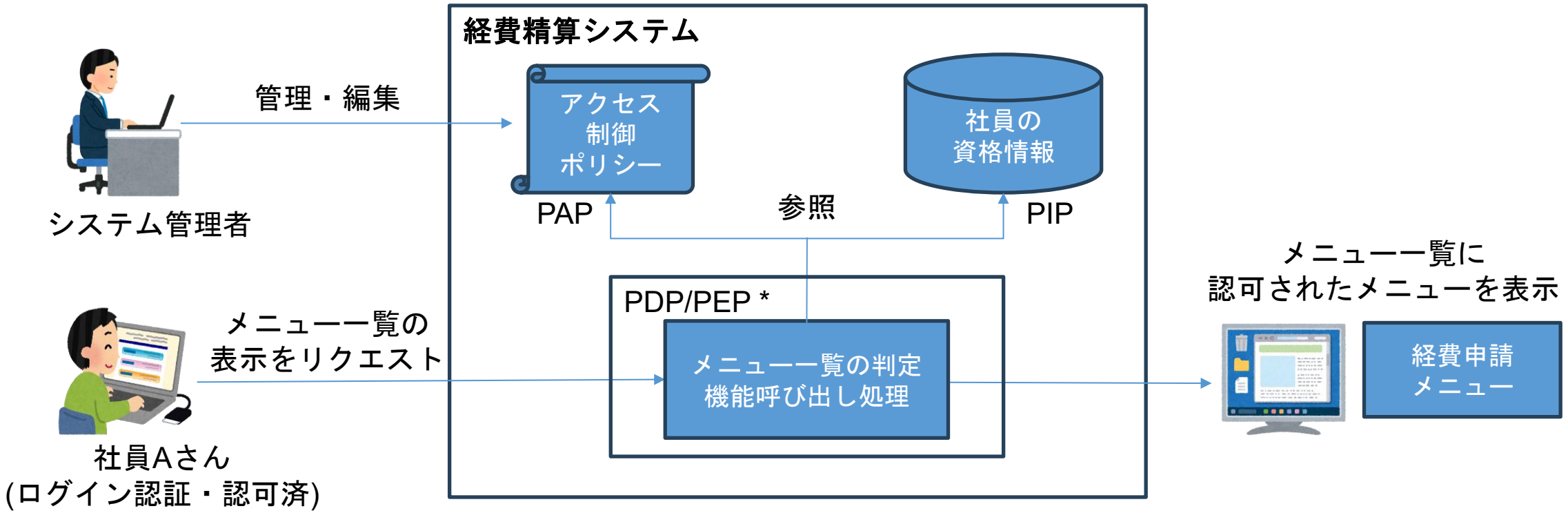
④参照結果を基に、リクエストの許可または拒否を判定

⑤判定結果を回答

⑥判定結果に基づき、主体からリソースに対してコントロールを適用

システム内の認可モデル（構成要素）

前述の経費精算システムの各種認可制御を実現するために、ユーザーの役職を格納するためのデータベース（社員の資格情報）や、どの機能を使う際にどういった条件を満たす必要があるのかを定めたルール（アクセス制御ポリシー）、実際にその機能を提供していいかどうかを判定するための内部判定機能といったシステム構成をすることで、適切な認可制御を行う構成を実現している。以下の図では、経費精算システム利用におけるメニュー一覧表示のステップにフォーカスして記載している。



*システム構成によっては、PDP/PEPが同一コンポーネント上で実装されており、分離されていないケースも存在する

ご意見、お問い合わせ、WG参加など

事務局まで