リリースから10年以上経過したサービスのOIDC化の事例

2024年 8月 28日

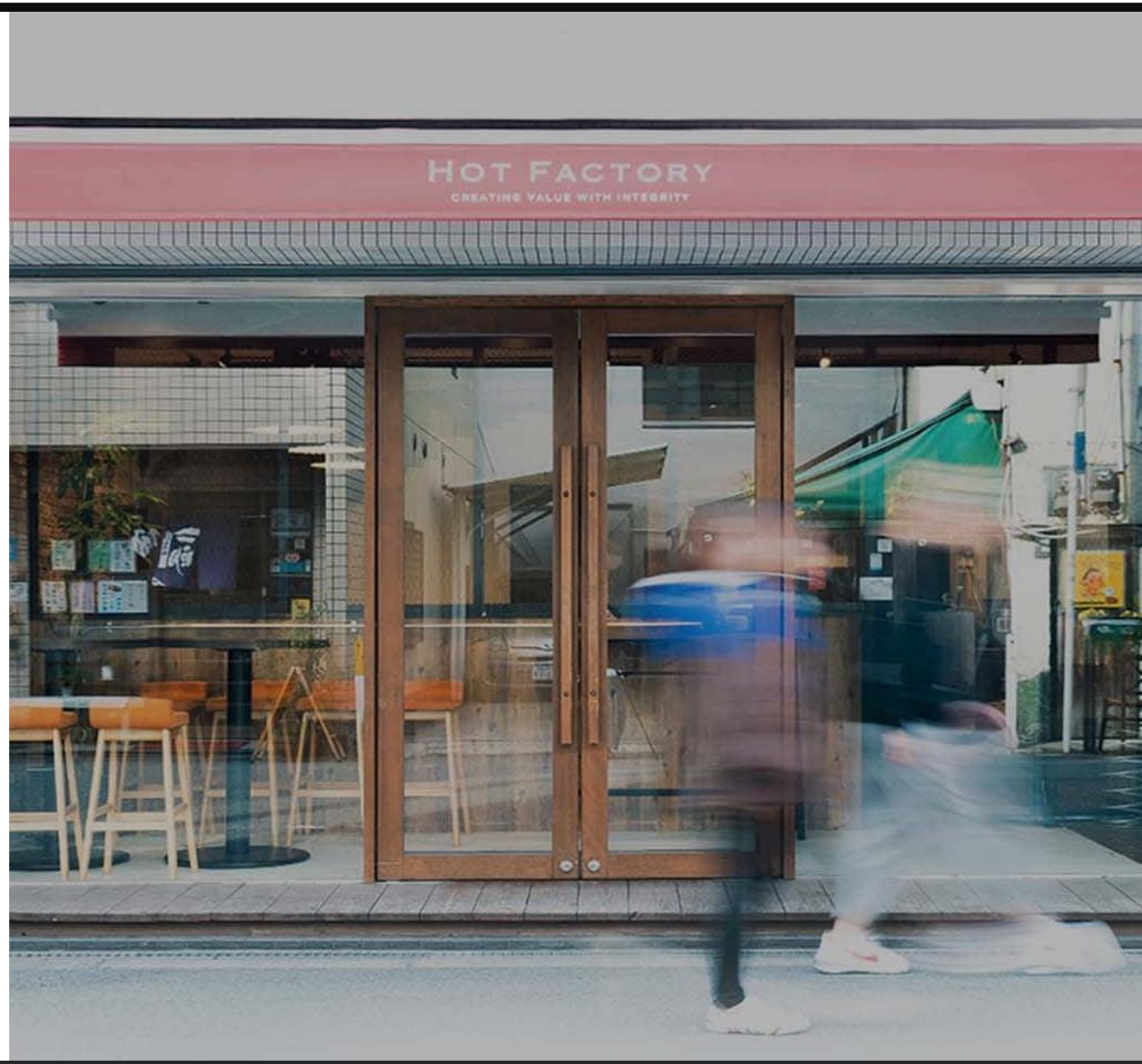
株式会社ホットファクトリー
取締役 CTO　福岡 秀一

株式会社ホットファクトリー

HOT FACTORY
CREATING VALUE WITH INTEGRITY

デザイン力もあるシステム開発会社

会社名	株式会社ホットファクトリー
創立	2002年10月
代表者	代表取締役 早田泰三
取締役	粟津孝博・福岡秀一・山下太郎・藤井純一
従業員数	75名
オフィス	大阪本社、東京、札幌、北広島、九州
事業内容	インターネットホームページの企画、立案、制作、 メンテナンス業務、Webシステムの開発・構築、 インターネットに関するコンサルティング業務、 通信販売等の事務局運営及びコールセンター業務、 広告代理業、レンタルサーバサービスの提供、飲食事業　等



本日のテーマ

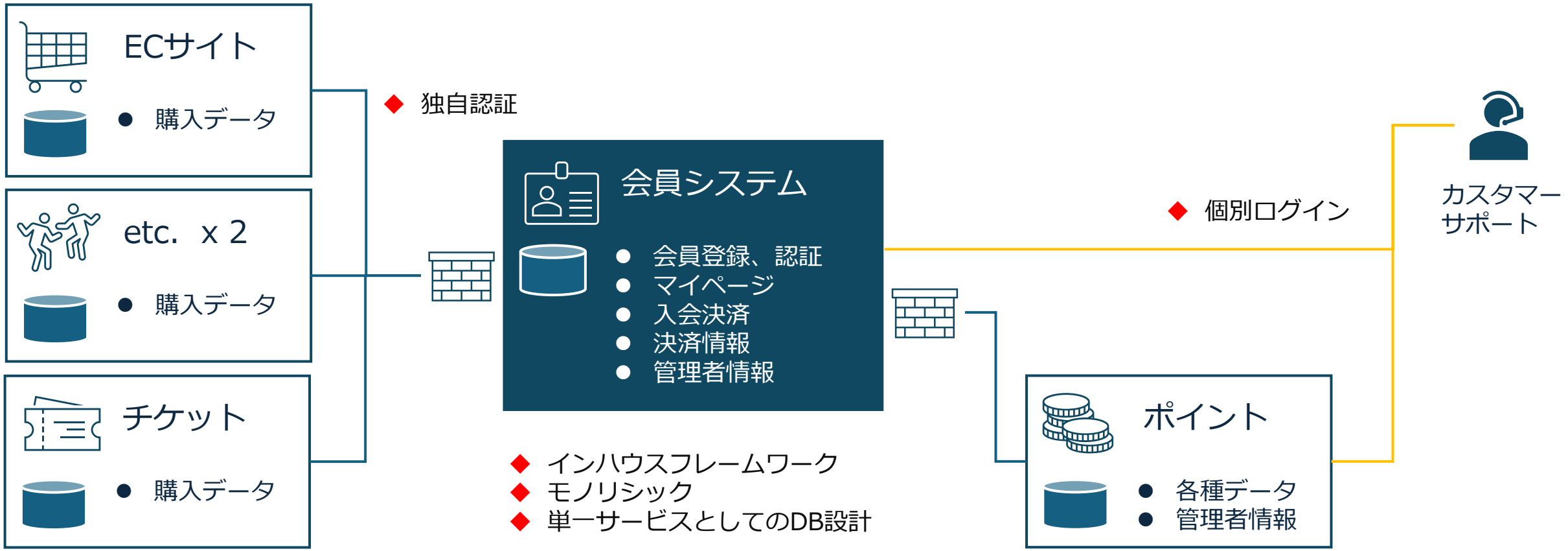
HOT FACTORY
CREATING VALUE WITH INTEGRITY

- 新旧システムの概要
- OIDC化するに至った背景とスケジュール
- 理想と現実のギャップ、Authleteさんとの出会い
- スコープ管理、コミュニケーションについて
- 運用して気づいたこと
- まとめ

旧システム概要図

HOT FACTORY
CREATING VALUE WITH INTEGRITY

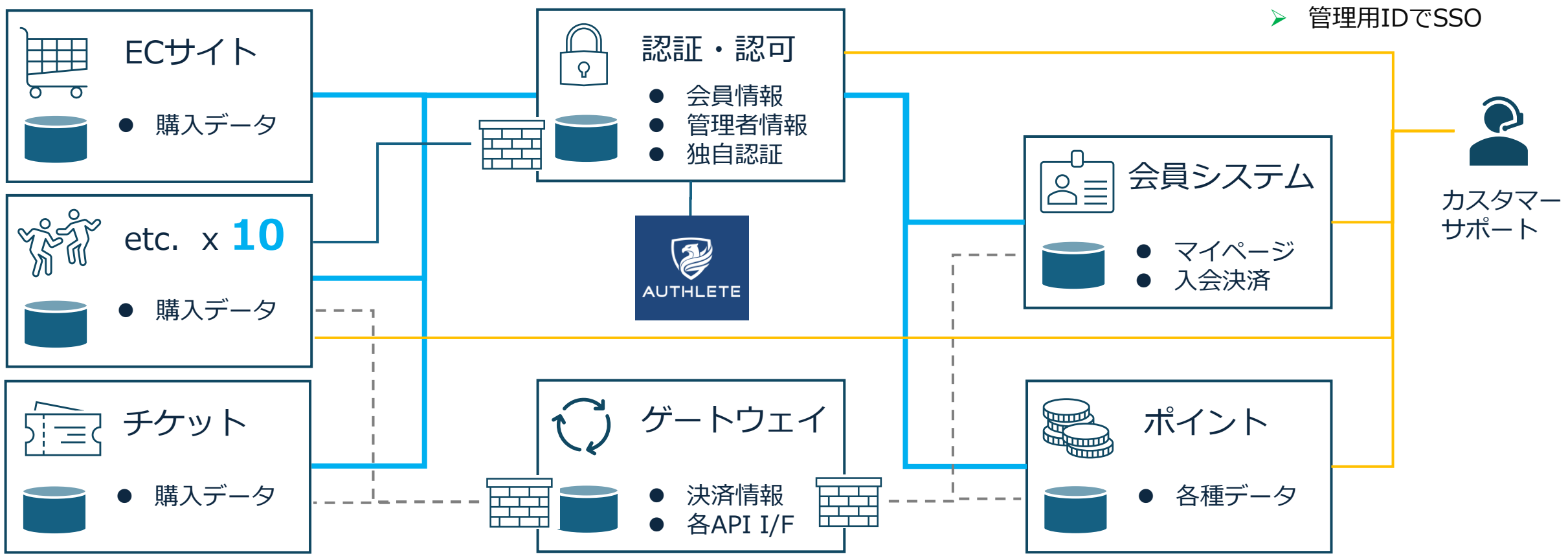
- ✓ 認証を担っていたのは 2006年に構築導入した会員システム
- ✓ 外部サービスとの認証は独自認証、シングルサインオンはできない
- ✓ オペレーションの管理画面もシステム毎にログインして利用



現在のシステム概要図

HOT FACTORY
CREATING VALUE WITH INTEGRITY

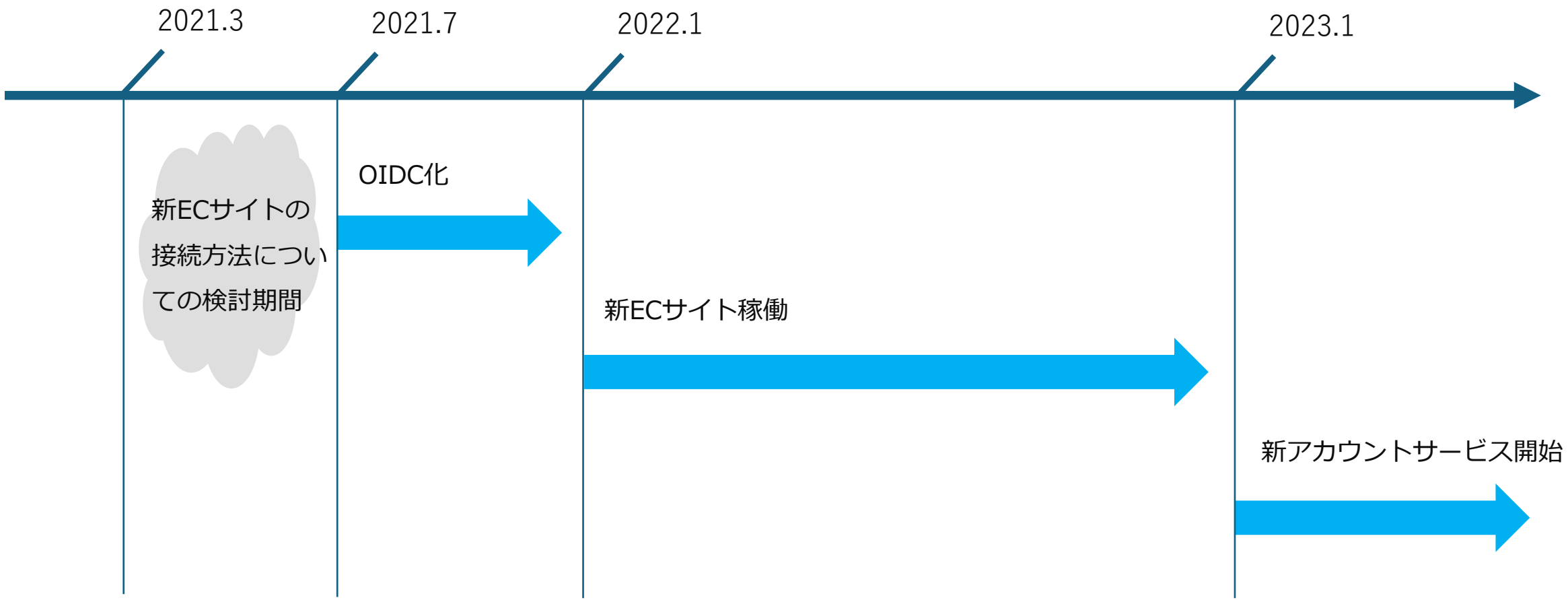
- ✓ 機能単位でシステムを分割し、個々に最適な環境で再構築
- ✓ オペレーションの管理画面も管理者用IDで統合
- ✓ 連携先も 10 を超える規模



背景とスケジュール感

HOT FACTORY
CREATING VALUE WITH INTEGRITY

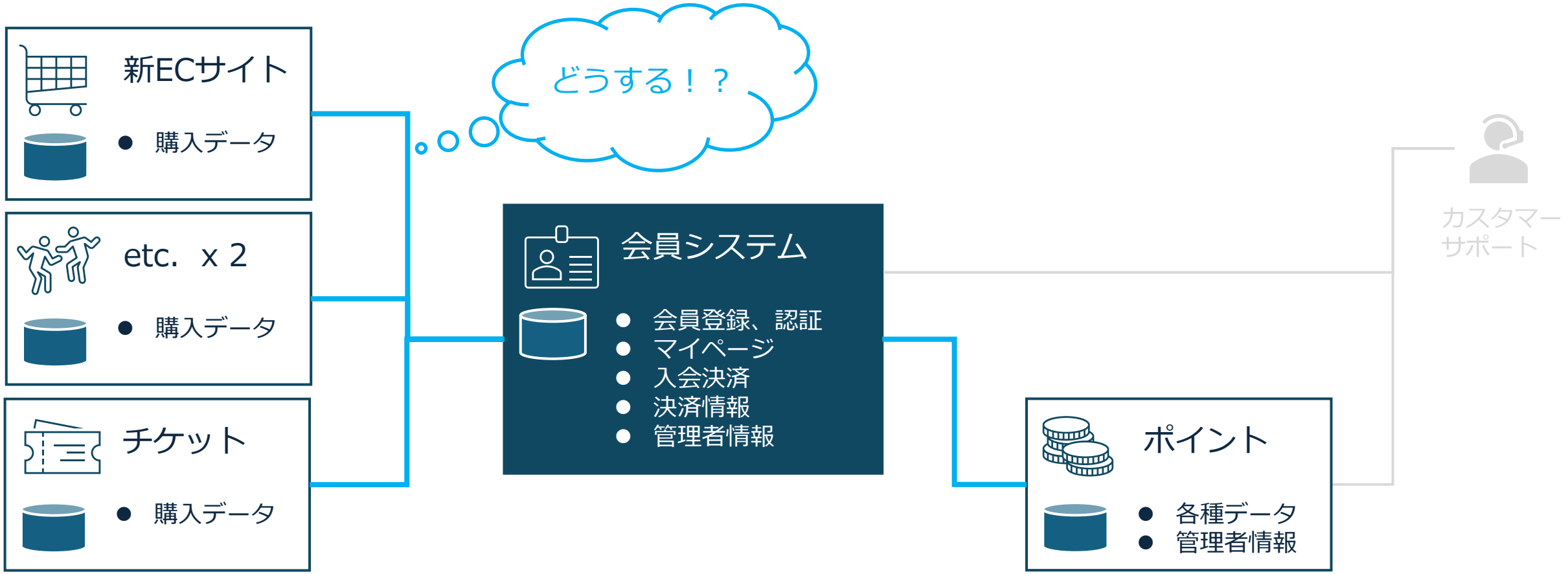
- ✓ ECサイトのリプレイスに伴い、新ECサイトの接続はOIDCが必須（OIDC化のリミット）
- ✓ 2023年には新しいアカウントサービスを開始し、接続先が急増する（モダン化のリミット）



制約事項

HOT FACTORY
CREATING VALUE WITH INTEGRITY

- ✓ 会員情報を外部システムに移管することはNG
- ✓ 会員番号を採番しなおすことはNG（番号に対する思い出、物理カードの再発行のコスト増、などなど）



理想と現実

HOT FACTORY
CREATING VALUE WITH INTEGRITY

- ✓ サービスとシステムのバランスをとりながら要件を整理する時間がない
- ✓ OIDC化のメリットは理解しつつも、限られた時間の中での最適解を模索するしかない

	幸せな理想	厳しい現実
システム	✓ モダナイゼーション ✓ 拡張性と柔軟性 ✓ 接続先とのデータ連携の柔軟性	✓ レガシー ✓ モノリシックで拡張性が乏しい ✓ OIDCの独自実装は難易度が高い
サービス	✓ シームレスな体験 ✓ 連携先が増えることでのビジネス機会 ✓ 新アカウントサービスの最大化	✓ EC販売でのトラブルは避けたい ✓ 将来的な構想を検討する時間的猶予 ✓ 規約などの法務面の時間的猶予
カスタマーサポート	✓ ユーザー情報の一元管理 ✓ 履歴が追跡しやすくなりサポートの向上	✓ UI/UX が大きく変わるのは避けたい ✓ 運用が変わるのは避けたい
周辺サービス	✓ 一般的なプロトコルでの接続で学習コスト低 ✓ プロファイルを活かしたサービス設計	✓ OIDCに対応する時間的猶予 ✓ 上記に伴うサービス設計の検討

Authleteさんとの出会い

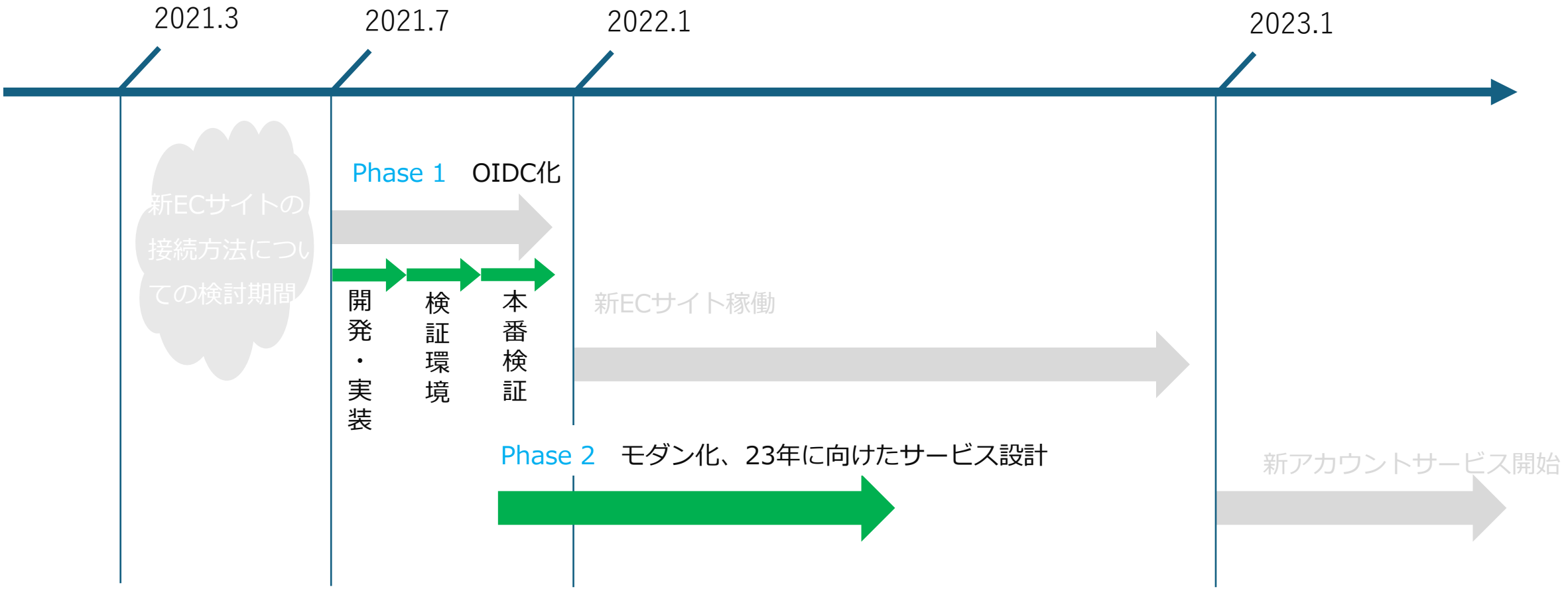
HOT FACTORY
CREATING VALUE WITH INTEGRITY

- ✓ Authleteさんが私たちにとっての最適解（自社技術との親和性、制約事項、短納期）
- ✓ OIDCの認証認可だけを新設

スコープの調整

HOT FACTORY
CREATING VALUE WITH INTEGRITY

- ✓ Phase 1　OIDC化に向けた必要最小限の実装
- ✓ Phase 2　モダン化と23年のサービス設計の両立



Phase 1 必要最小限とはいえ・・・

HOT FACTORY
CREATING VALUE WITH INTEGRITY

◆ Authleteの組み込み

- ✓ 特に苦労しなかった

◆ OIDCのプロファイリング（前回 6/18 の勉強会をご参照）

- ✓ Authleteの管理画面に選択肢は網羅されている
  - 各種トークンの有効期限
  - スコープとクレーム
  - 認証フロー
  - 暗号化方式
  - などなど・・・

◆ 既存の会員システムが動いている状態での UI / UX も含めたサービス設計

- ✓ ECサイトの要件に絞った検討
- ✓ 基本的な実装（欲を出さない）
- ✓ 23年に向けて再検討を行う前提

Phase 2 に向けてのアプローチ

HOT FACTORY
CREATING VALUE WITH INTEGRITY

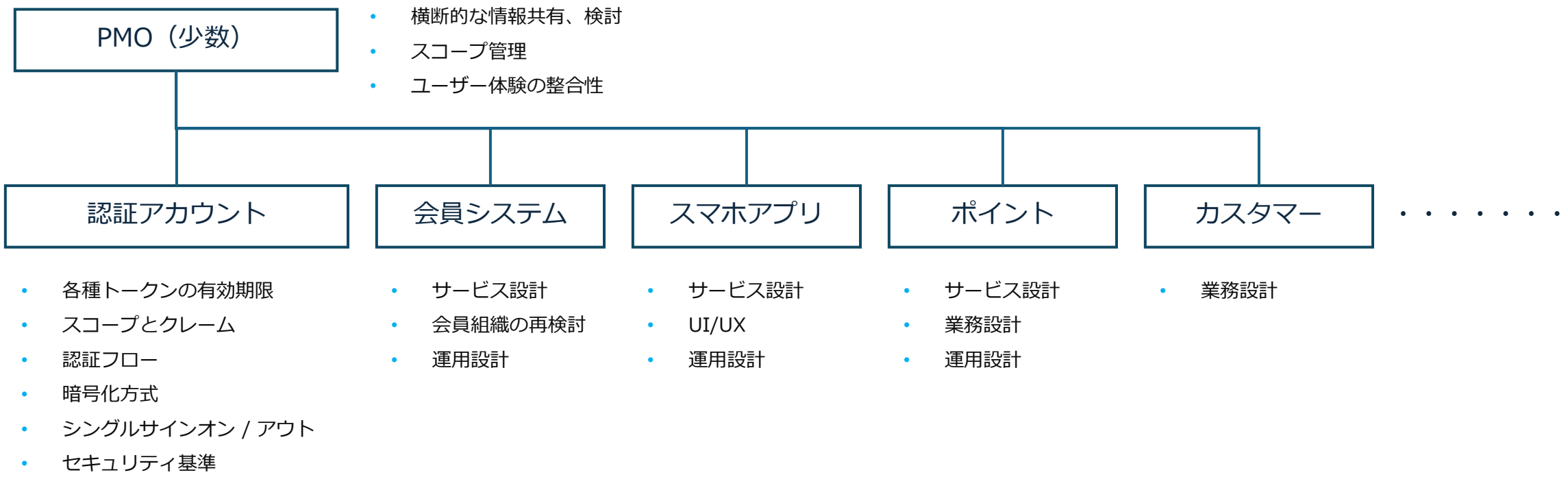
- ✓ あるべき理想との向き合い方を時間をかけて整理
- ✓ 既に動くモノがあることで、サービス設計に集中できる環境にもなっていた

	幸せな理想	アプローチ
システム	✓ モダナイゼーション ✓ 拡張性と柔軟性 ✓ 接続先とのデータ連携の柔軟性	✓ 機能単位でのシステム分割 ✓ 各システムで管理する情報の再設計 ✓ 最適な環境の選定 ✓ データの移行計画
サービス	✓ シームレスな体験 ✓ 連携先が増えることでのビジネス機会 ✓ 新アカウントサービスの最大化	✓ UI/UXの整理 ✓ 収集、共有するプロファイルの設計 ✓ 規約の見直し
カスタマーサポート	✓ ユーザー情報の一元管理 ✓ 履歴が追跡しやすくなりサポートの向上	✓ 運用が変わる <<< 新システムでのメリット ✓ 運用の変化点を速やかに共有 ✓ 横断的にデータにアクセスできる環境
周辺サービス	✓ 一般的なプロトコルでの接続で学習コスト低 ✓ プロファイルを活かしたサービス設計	✓ 既に公開しているOIDCでイメージ ✓ 旧認証をいつまでサポートするか

Phase 2 を実現するためのコミュニケーション

HOT FACTORY
CREATING VALUE WITH INTEGRITY

- ✓ 適切な単位で分科会を設けて進行
- ✓ 横断的な検討と判断にはビジネスジャッジができる人が必須



運用して気づいたこと

HOT FACTORY
CREATING VALUE WITH INTEGRITY

1 周辺サービスが OIDC に対応できないことがある

- 周辺サービスも年代物。
- 対応するコストが見合わない、など。

アプローチ

- ✓ 旧認証方法をサポート
- ✓ 新認証認可サービスに旧認証を再実装

要検討

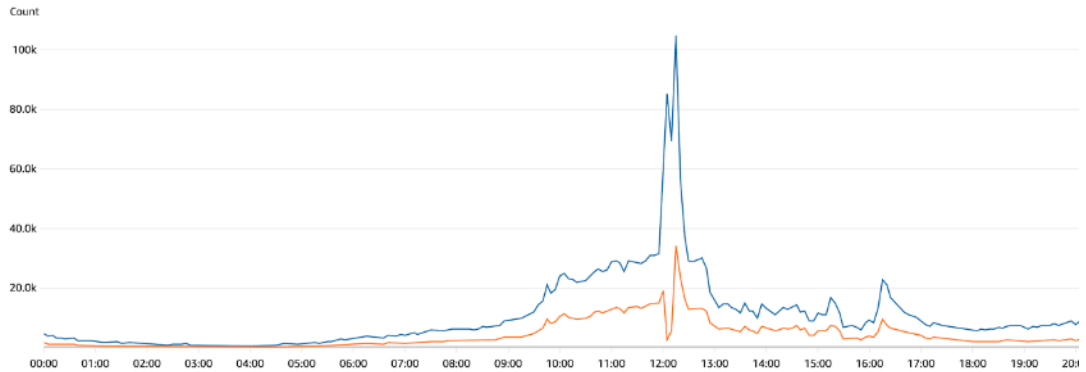
- ◆ SSOができない
- ◆ UI / UX の統一感（フィッシングサイト）
- ◆ サポートの煩雑さ

運用して気づいたこと

HOT FACTORY
CREATING VALUE WITH INTEGRITY

2 エンタメ特有のピークが極端

- 平時とピークで10倍以上の差
- 極狭い時間帯に集中
- Authlete の RPS に直撃



アプローチ

- ✓ トークンの有効期限などの検討
- ✓ キャッシュの検討
- ✓ オンデマンドオプション

イントロスペクション・レスポンスのキャッシング

概要

場合によっては、Authleteのイントロスペクション・エンドポイントからのレスポンスをキャッシュすることが、リソース・サーバーのAPIのレスポンス性能の改善につながります。
設定例

1. お客さまの環境の認可サーバーあるいはリソース・サーバーに、Redisなどのキャッシュ・サーバーをインストールします。
2. Authleteからのイントロスペクション・レスポンスをキャッシュするように設定します。

まとめ

- 全てのPhaseを通して、ビジネスメンバーが参加することの必要性
- コミュニケーションは少人数で「決める」体制を作る
- スコープは適切な範囲を見極める（周辺サービスへの配慮、チームリソース、スケジュール）
- タスクが積み上がった場合は最初のコンセプトに立ち返る（やれそうなこと <<< 最悪の事態を想定）
- Authleteさんは大体の要求に応えられる

最後に

HOT FACTORY
CREATING VALUE WITH INTEGRITY

エンジニア積極採用中！

ちょっと話を聞いてみたいと思ったら・・・カジュアル面談から！