リクルートの利用事例から考える AWSの各サービスとセキュリティ

株式会社リクルートテクノロジーズ
インフラソリューション部
宮崎幸恵

RECRUIT リクルートテクノロジーズ

1．はじめに ～リクルートグループおよびリクルートテクノロジーズ

2．リクルートのビジネスモデルとクラウド

3．AWSで考えるセキュリティ～NW、権限、ログ

4．まとめ

1．はじめに ～リクルートグループおよびリクルートテクノロジーズ

2．リクルートのビジネスモデルとクラウド

3．AWSで考えるセキュリティ～NW、権限、ログ

4．まとめ

みやざき　　さちえ
宮崎　幸恵
株式会社リクルートテクノロジーズ
インフラソリューション部

2011年から現在まで、グループ全社向けパブリッククラウド基盤の設計、構築、運用に携わっています

リクルートグループとは、主要７事業会社＋３機能会社で構成されるグループ企業群

事業会社

リクルート
ホールディングス

リア
いカンパニー
フスタイル
ブズ
リクルートスタッフィング
リクルートマーケティングパートナーズ
スタッフサービス・ホールディングス

RECRUIT リクルートテクノロジーズ

アドミニストレーション
コミュニケーションズ

**所属会社は
リクルートテクノロジーズ**

ミッション

Missions

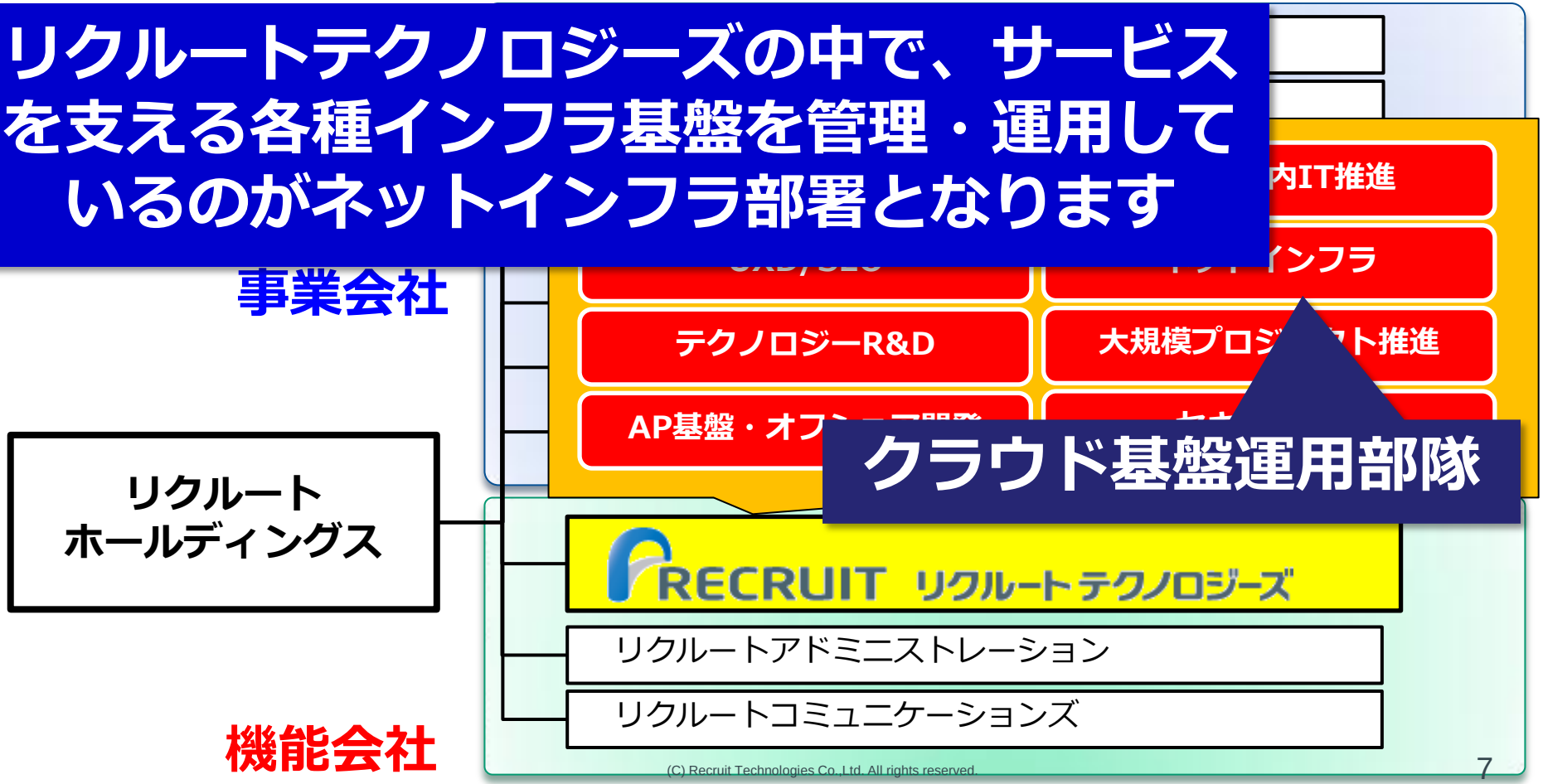
リクルートグループ各社の現在・将来のニーズを見据えて

リクルートテクノロジーズは
リクルートグループをITで牽引する企業です

http://recruit-tech.co.jp/

「リクルートグループに対して様々なソリューションを展開しています

リクルートテクノロジーズの中で、サービスを支える各種インフラ基盤を管理・運用しているのがネットインフラ部署となります



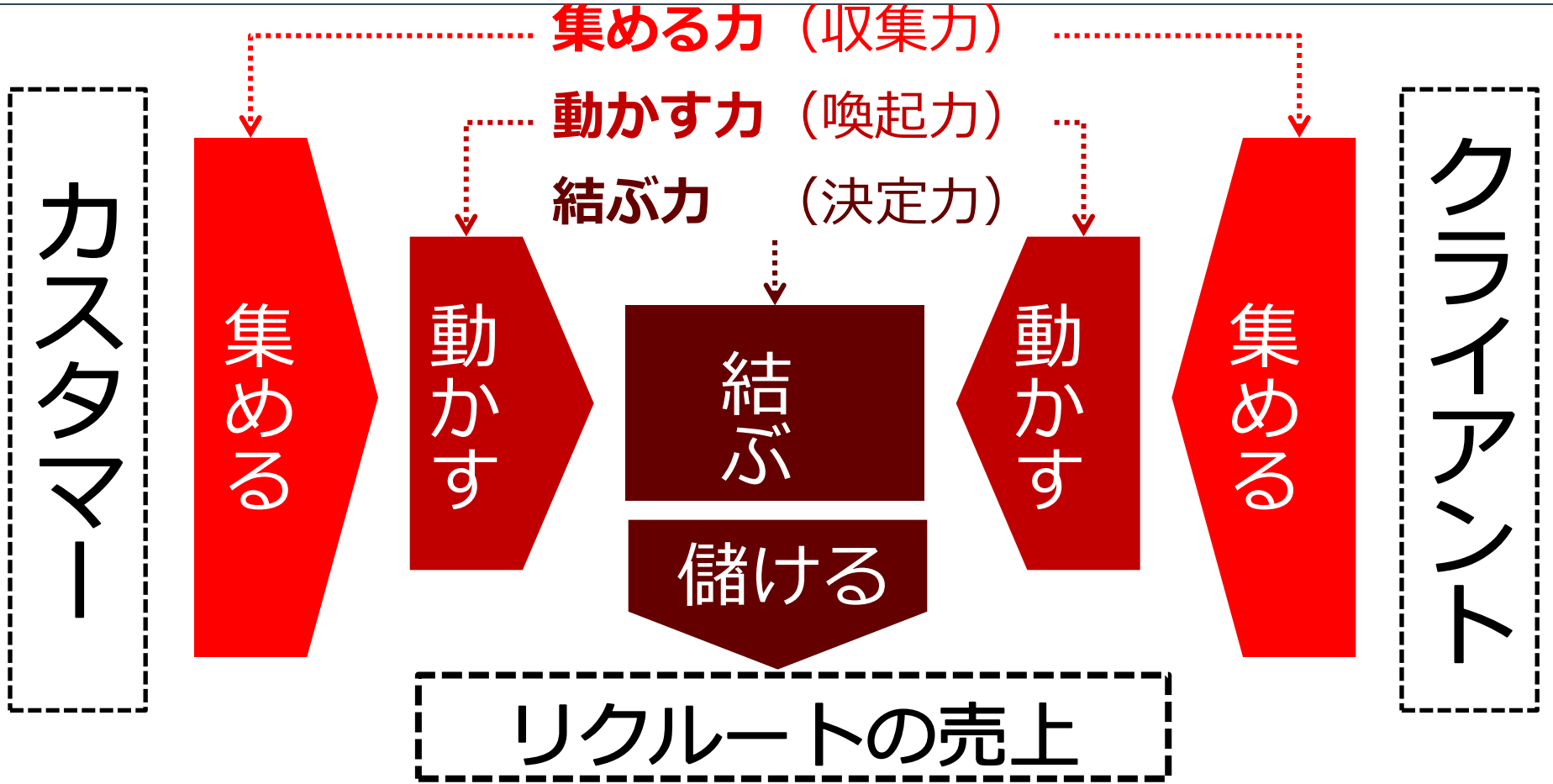
1．はじめに ～リクルートグループおよびリクルートテクノロジーズ

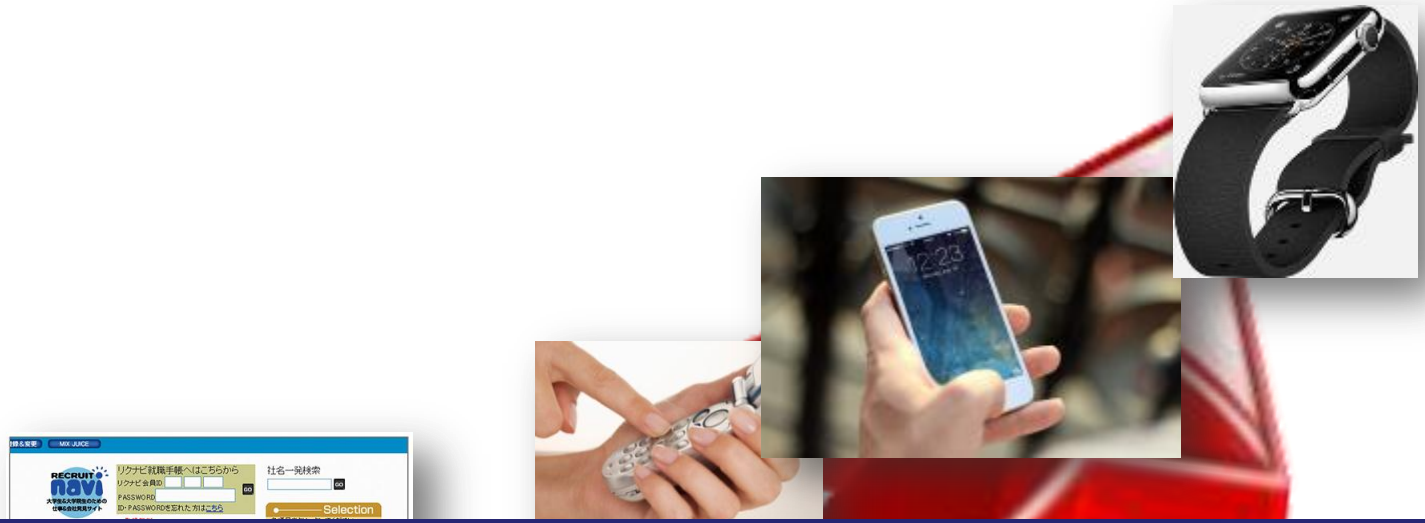
2．リクルートのビジネスモデルとクラウド

3．AWSで考えるセキュリティ～NW、権限、ログ

4．まとめ

カスタマーとクライアントを新しい接点で結び、「まだ、ここにない、出会い。」の場を創造する





紙 → ネット への展開が進む。ITの進化とともにソリューションも進化

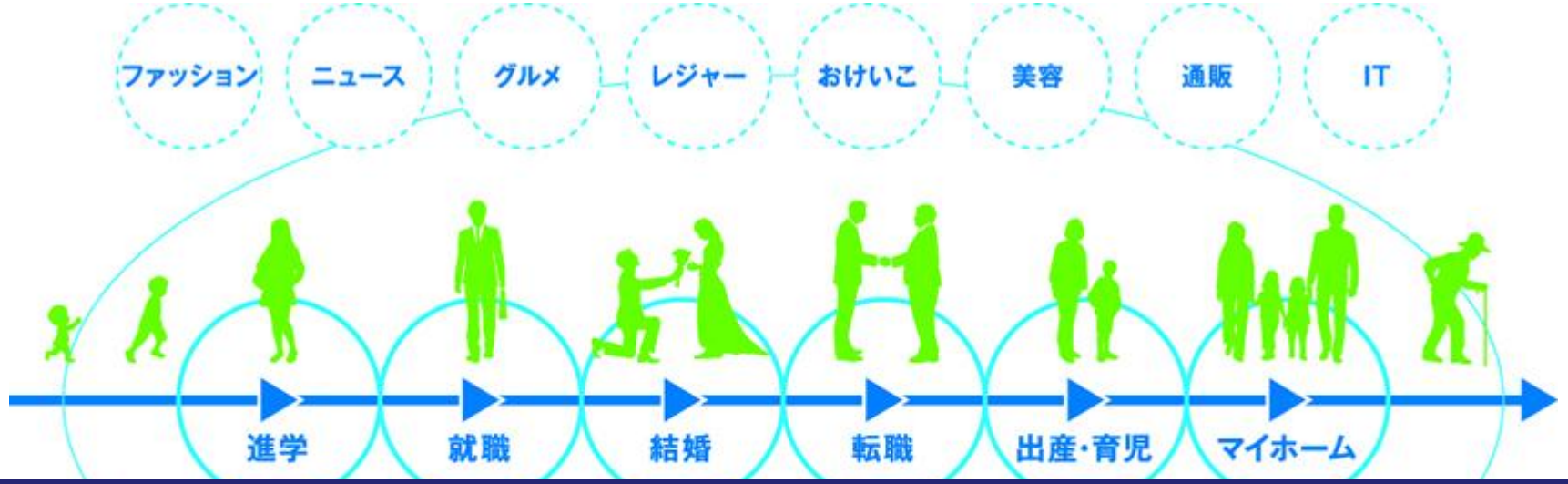
2006~2009年ごろまで4箇所 のデータセンター、 1400台 のサーバで構成

2009年にネットインフラ基盤として DCを１つに統合

2006~2009年ごろまで4箇所 1400台 のサーバで構成

年間 800億PV以上
のトラフィックを
捌くシステム基盤

2009年 DCを1つに統合



新規ビジネスへのさらに迅速な対応、需要予測の出来ないサービスの増加

オンプレミス基盤

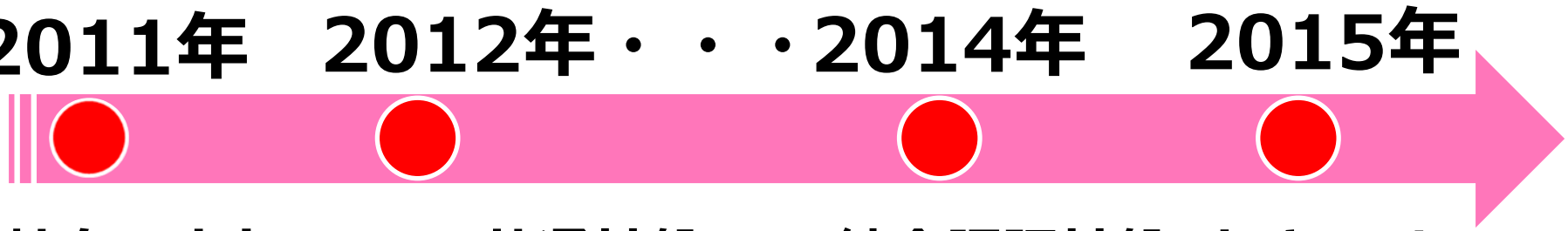
リクルートテクノロジーズが提供する中で最も大きな商用WEBサイト向けインフラプラットフォーム。

社内インフラ

主に社内ツール向けインフラプラットフォーム。
業務、経理システム等が存在。

クラウド基盤

商用Webサイト向けにパブリッククラウドを提供。

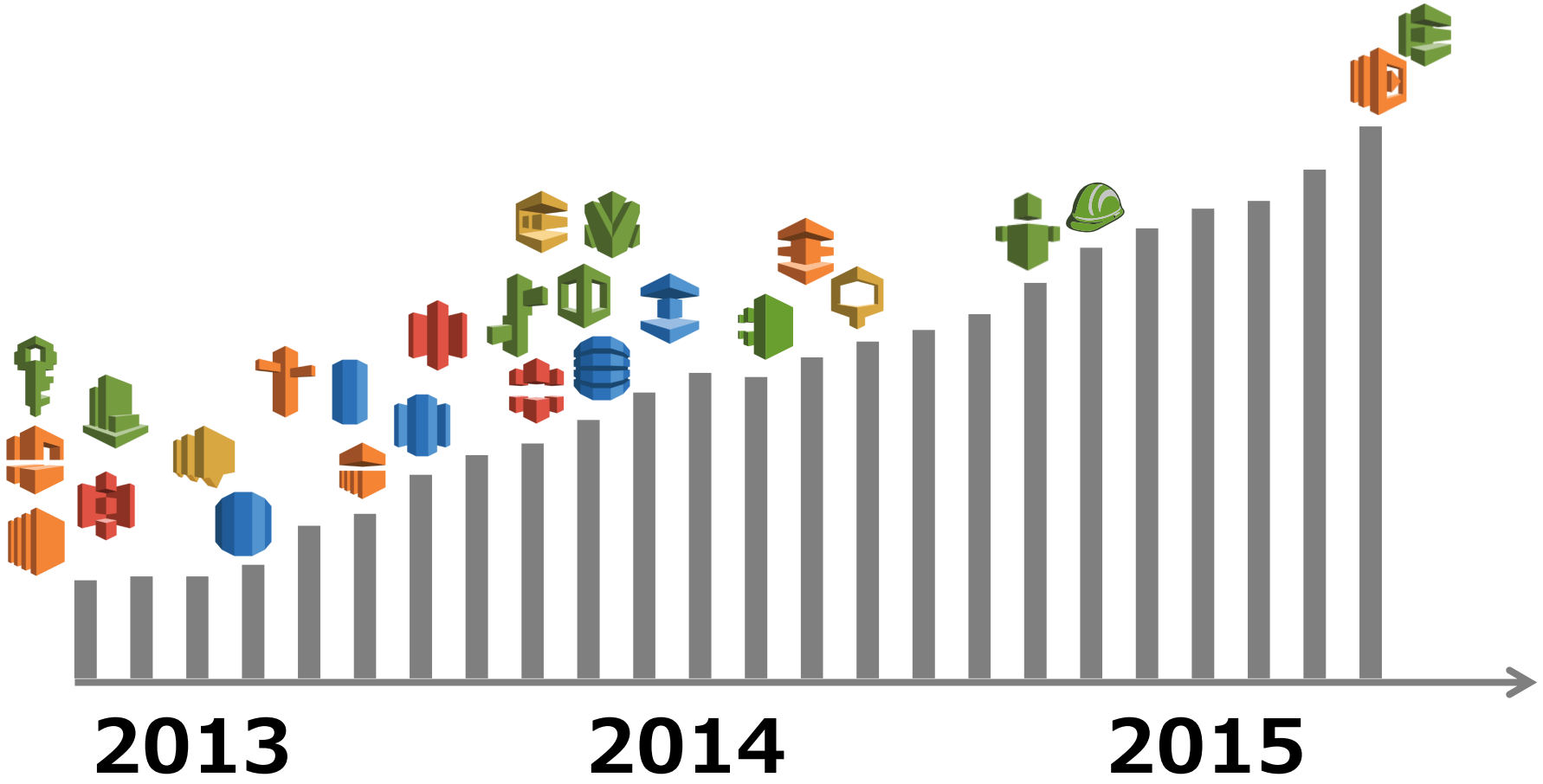


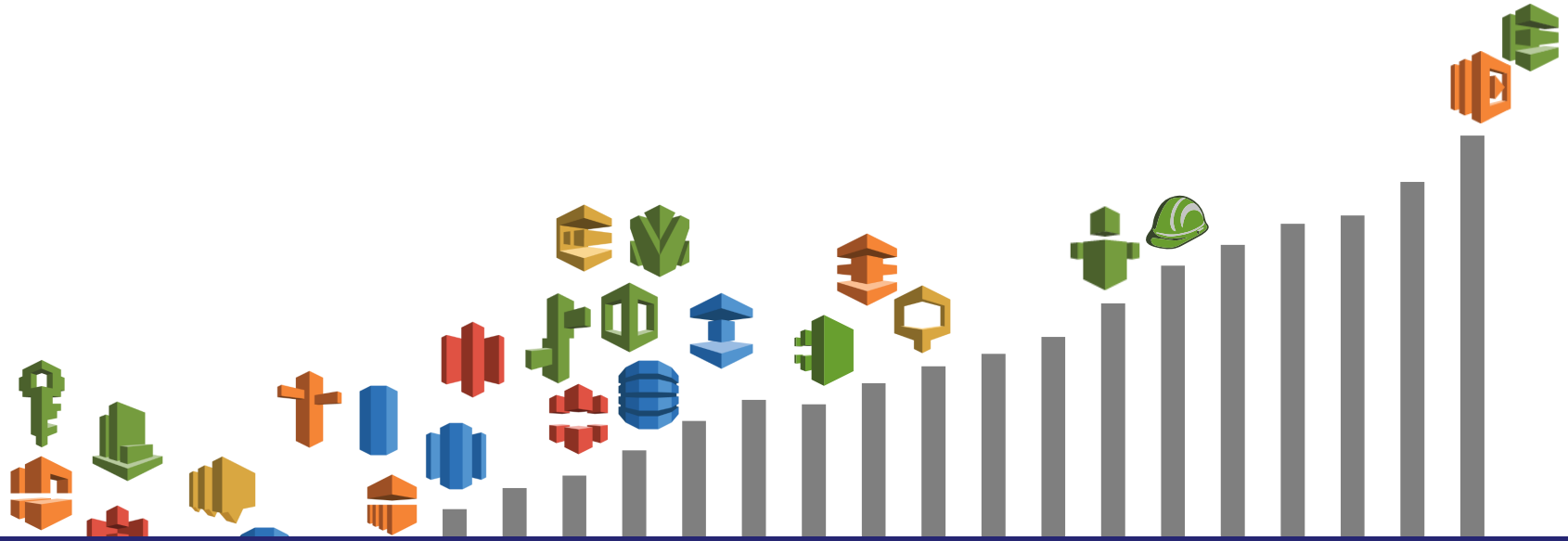
AWSの基盤としては2012年～以来アップデートしつつ拡張

・VPCでセグメント分離が可能

◎権限が制御可能

求める要件に合わせて多様なサービスを活用中





要件に合わせて数、規模とも拡大

2013 2014 2015

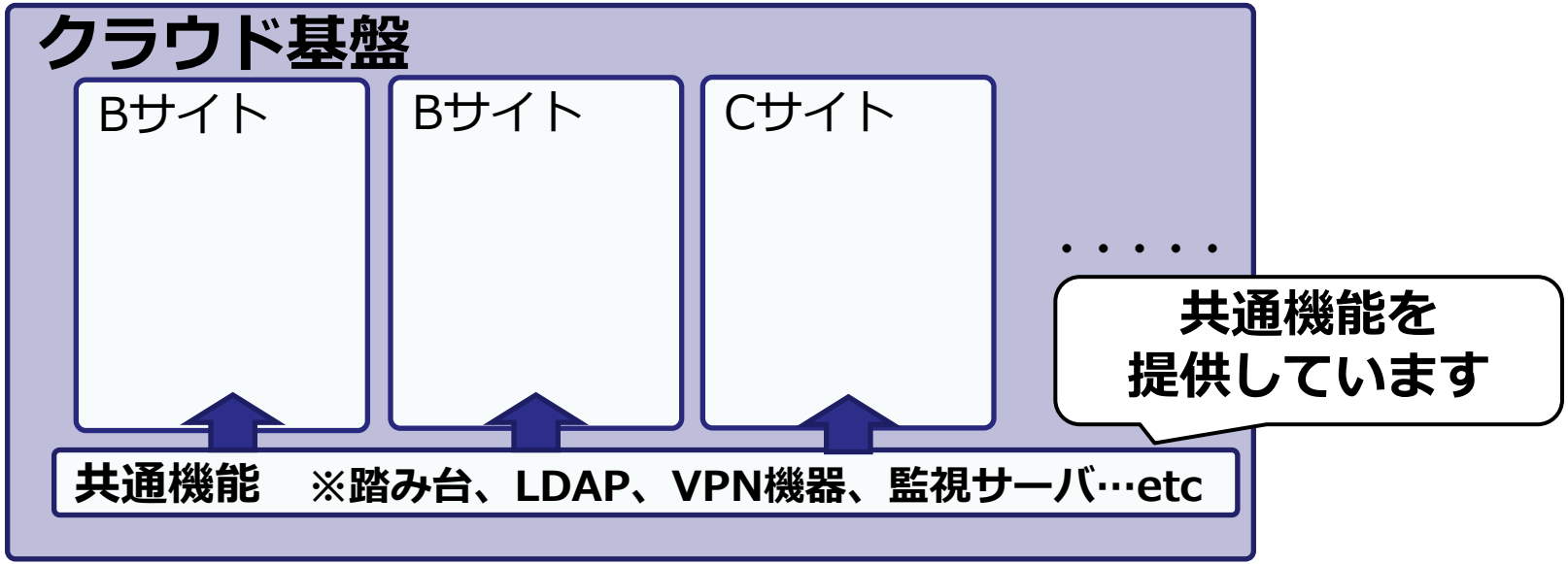
1．はじめに ～リクルートグループおよびリクルートテクノロジーズ

2．リクルートのビジネスモデルとクラウド

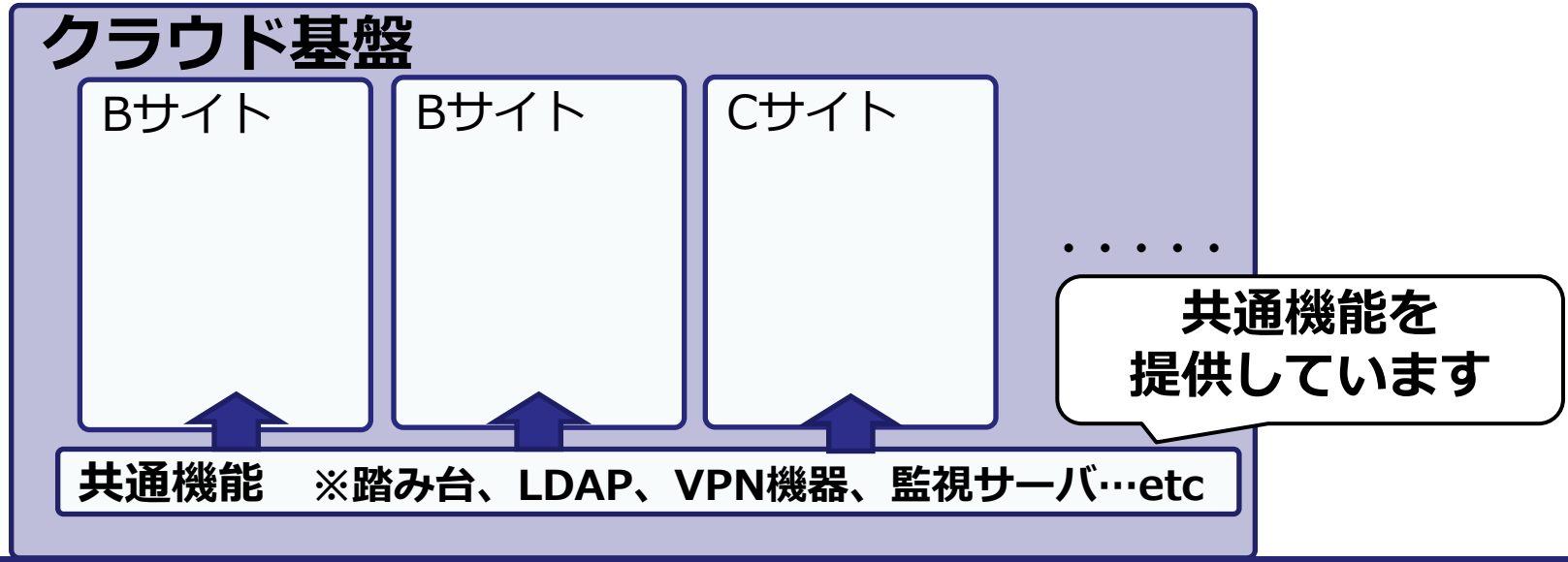
3．AWSで考えるセキュリティ～NW、権限、ログ

4．まとめ

情報をいかに守るかは
サービス基盤に課せられた使命



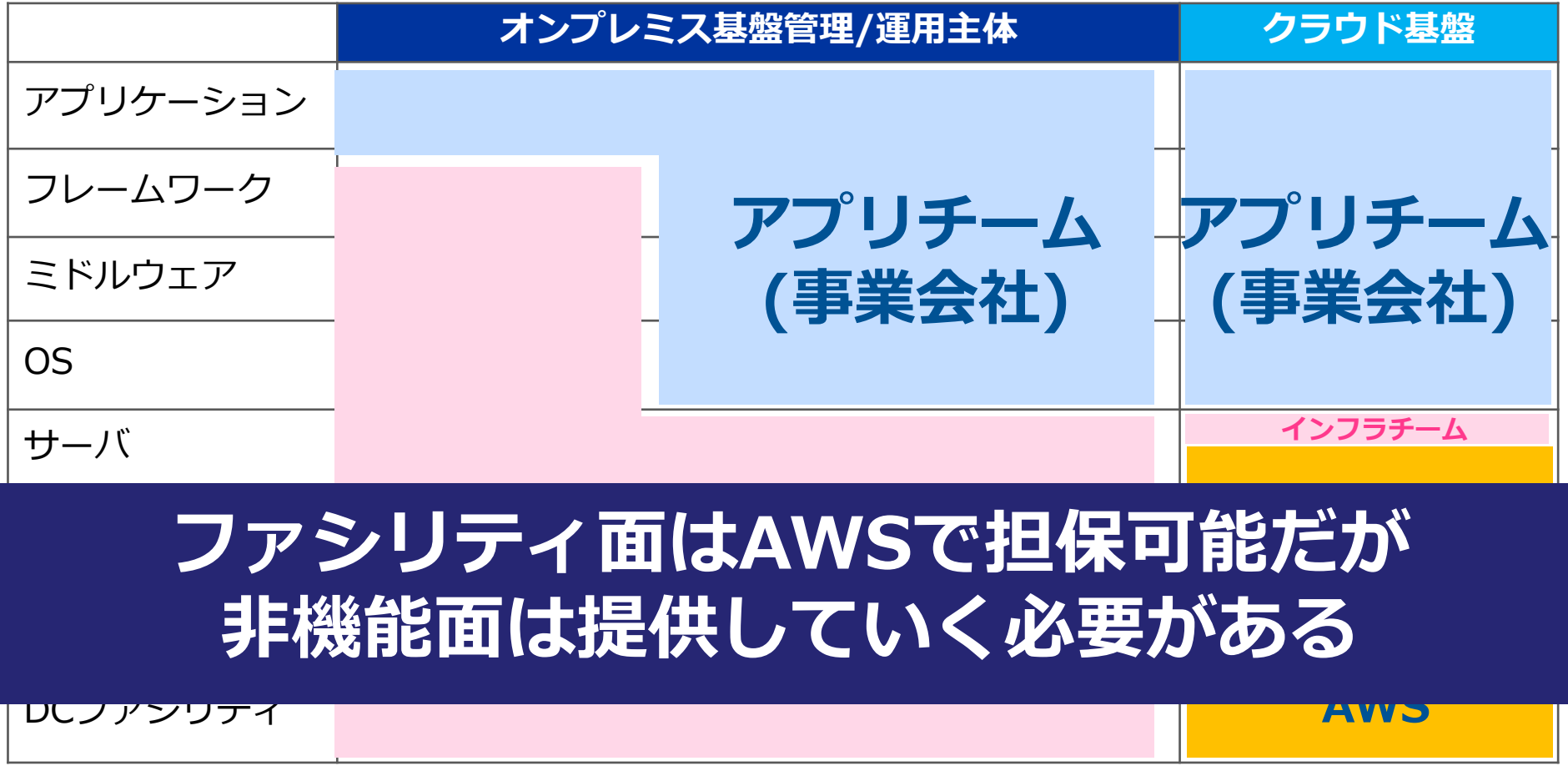
分類	機能	説明
その他	オンプレミス環境との接続	オンプレミスとの専用回線によるセキュアな接続
セキュリティ	認証/ID管理/ログ保管	サーバへの個人認証、操作ログ取得、ID管理機能を提供
運用	監視/モニタリング	監視機能、モニタリングツールの提供を実施
運用	ライセンス提供	一部MWのライセンス提供



クラウドのメリットを活かしつつ、共通機能は提供するスタイル

運用	監視/モニタリング	監視機能、モニタリングツールの提供を実施
運用	ライセンス提供	一部MWのライセンス提供


オンプレミス基盤管理/運用主体
クラウド基盤
アプリケーション
フレームワーク
ミドルウェア
OS
サーバ
ストレージ
ネットワーク
DCファシリティ
アプリチーム
(事業会社)
アプリチーム
(事業会社)
インフラチーム
インフラチーム
AWS
インフラチーム
AWS



ファシリティ面はAWSで担保可能だが
非機能面は提供していく必要がある

①仮想NW設計/ACL管理	VPC設計、オンプレミスとの連携、セキュリティグループ等の運用
②権限設計/ID管理	IAM権限設計、統合認証基盤によるID管理と運用
③ログの共通取得	操作ログの集約と保持・監査

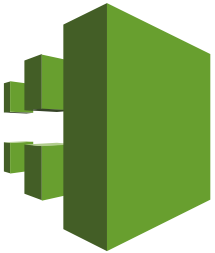
①仮想NW設計/ACL管理	VPC設計、オンプレミスとの連携、セキュリティグループ等の運用
②権限設計/ID管理	IAM権限設計、統合認証基盤によるID管理と運用

セキュリティ担保としてインフラチームではこの3項目中心に設計・運用

VPC

IAM

CloudTrail



AWSのセキュリティ3種の神器

・AWS導入当初からVPC前提で設計

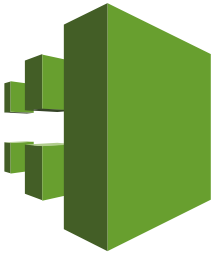
・Direct Connect、VPN、peering すべての機能を利用しているため、全体のNW構成自体は複雑

・各VPCごとの構成はセオリー通り

・AWS導入当初から利用

・権限設計は定期的に修正しながら利用

・LDAPを導入しており、SAMLでの認証連携を実装



・リリースされたリージョン順に導入

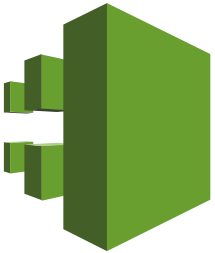
・解析ツールはいくつか試験導入済み

・サーバ操作ログ含め監査一元化を実装予定

VPC

IAM

CloudTrail



AWSのセキュリティ3種の神器

・ユーザー管理
・パスワード変更/管理
・ロック機能
・ワンタイム認証

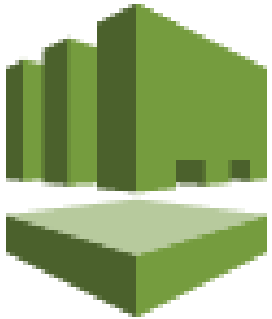
IAMの権限機能
（グループ、ポリシー）

・ユーザー管理
・パスワード変更/管理
・ロック機能
・ワンタイム認証

IAMの権限機能

IAMの基本機能以上の部分は自前構築

Directory Service



2014年10月リリース

・ユーザー管理
・パスワード変更/管
・ロック機能
・ワンタイム認証

・AWS以外の機能とも認証統合を実施したいと考えていた

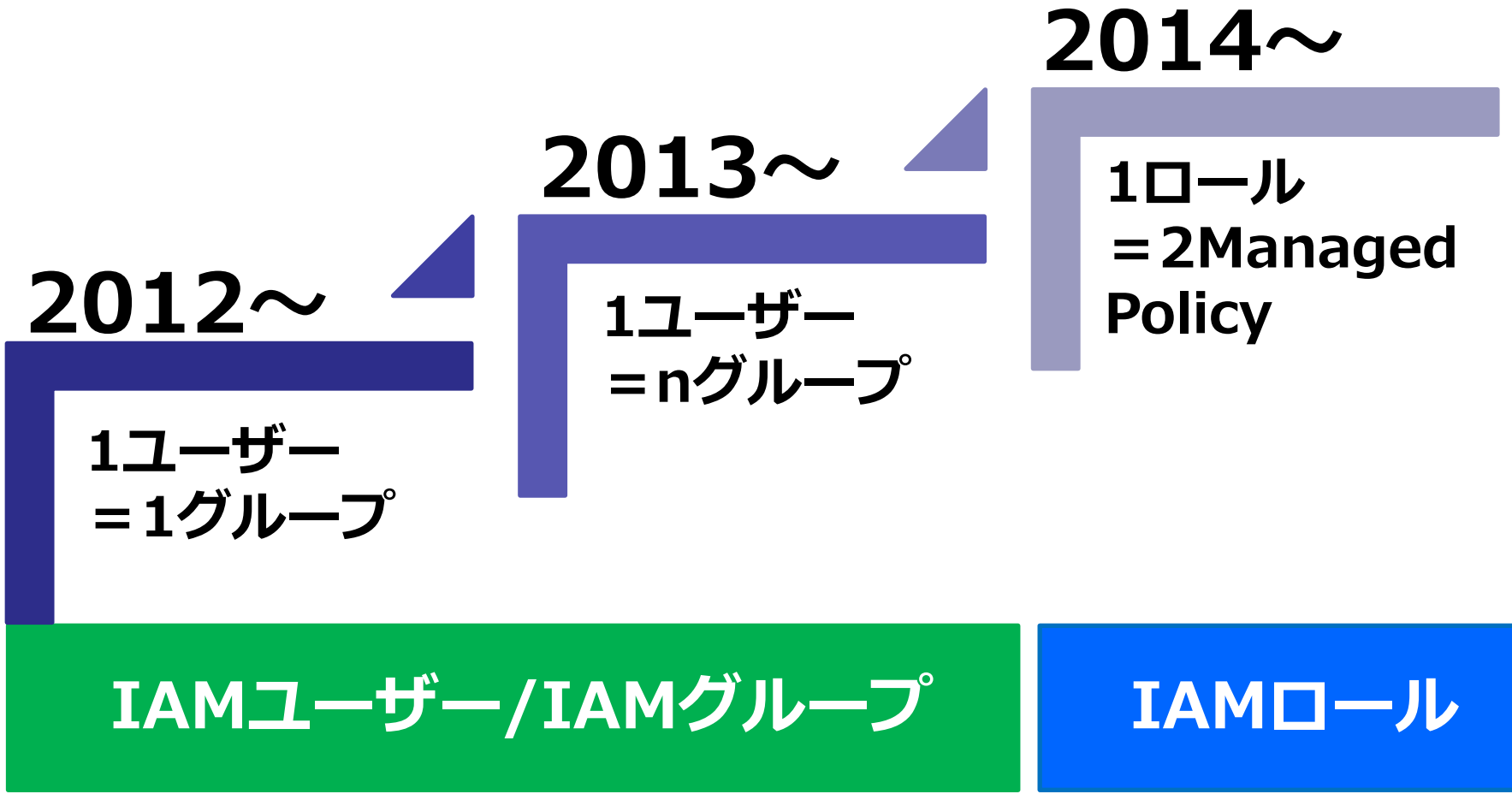
・作り込みが必要な要件があったので、カスタマイズ可能な自前構築にした

IAMの権限機能
（グループ、ポリシー）

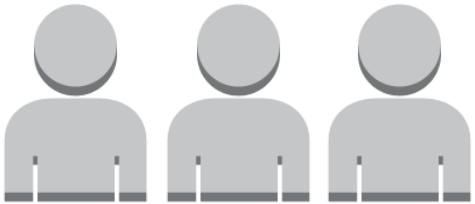
IAMの権限機能（グループ、ポリシー）

```
{
 "Statement": [
  {
   "Action": [
    “ec2:Describe*",
    "rds:Describe*",
    "rds:ListTagsForResource",
    "apa:Get*"
   "Condition": {
    "IpAddress": {
     "aws:SourceIp": ["xx.xx.xx.xx/32"]
    }
```

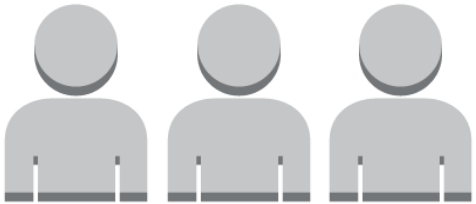
実はここが最も設計、運用が必要なところ



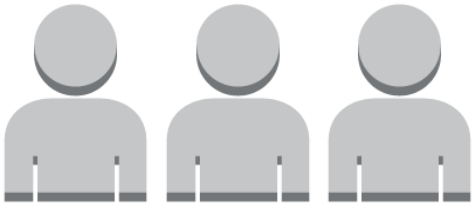
Admin
グループ



開発者
グループ



閲覧
グループ

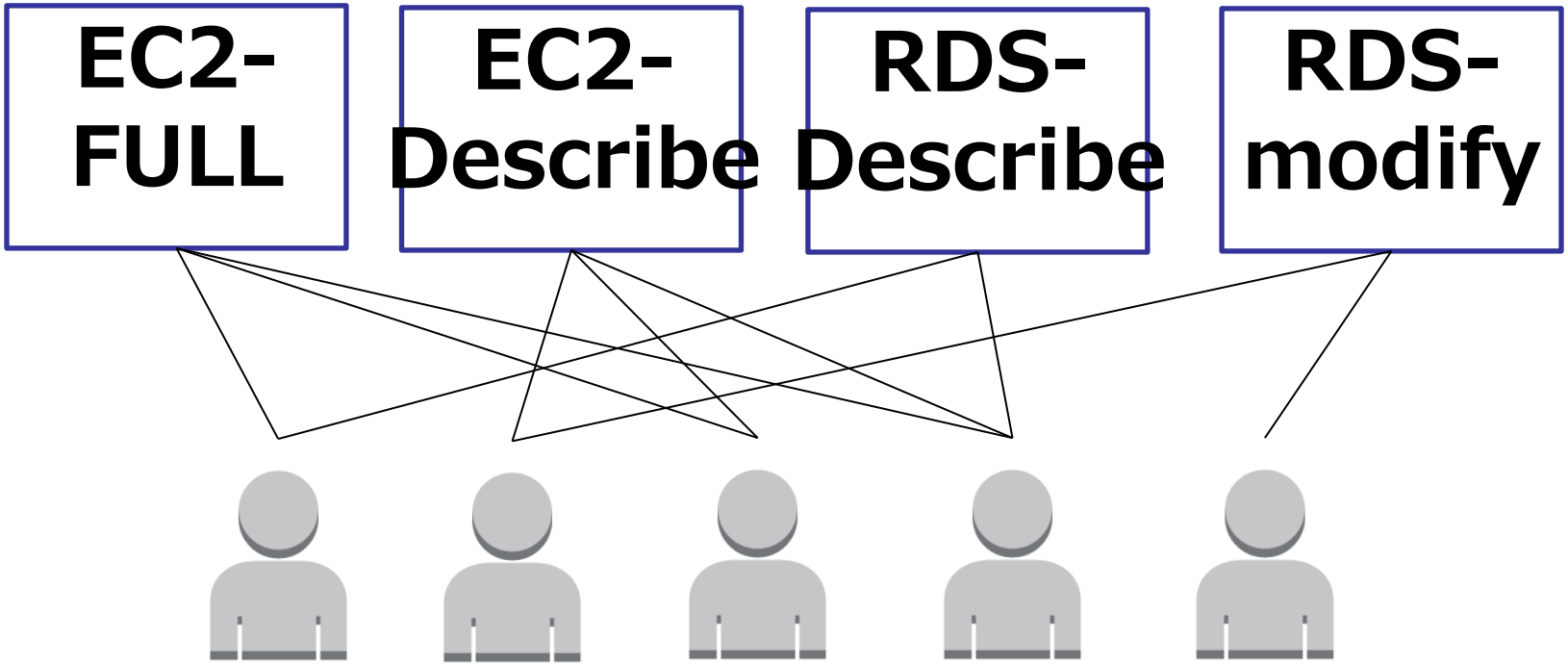


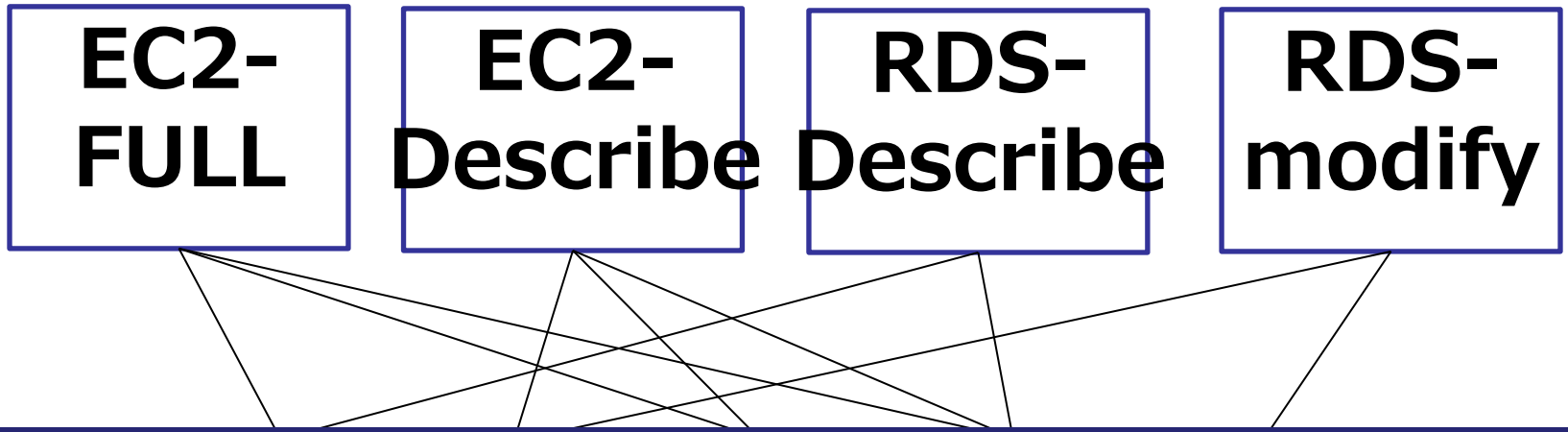
Admin
グループ

開発者
グループ

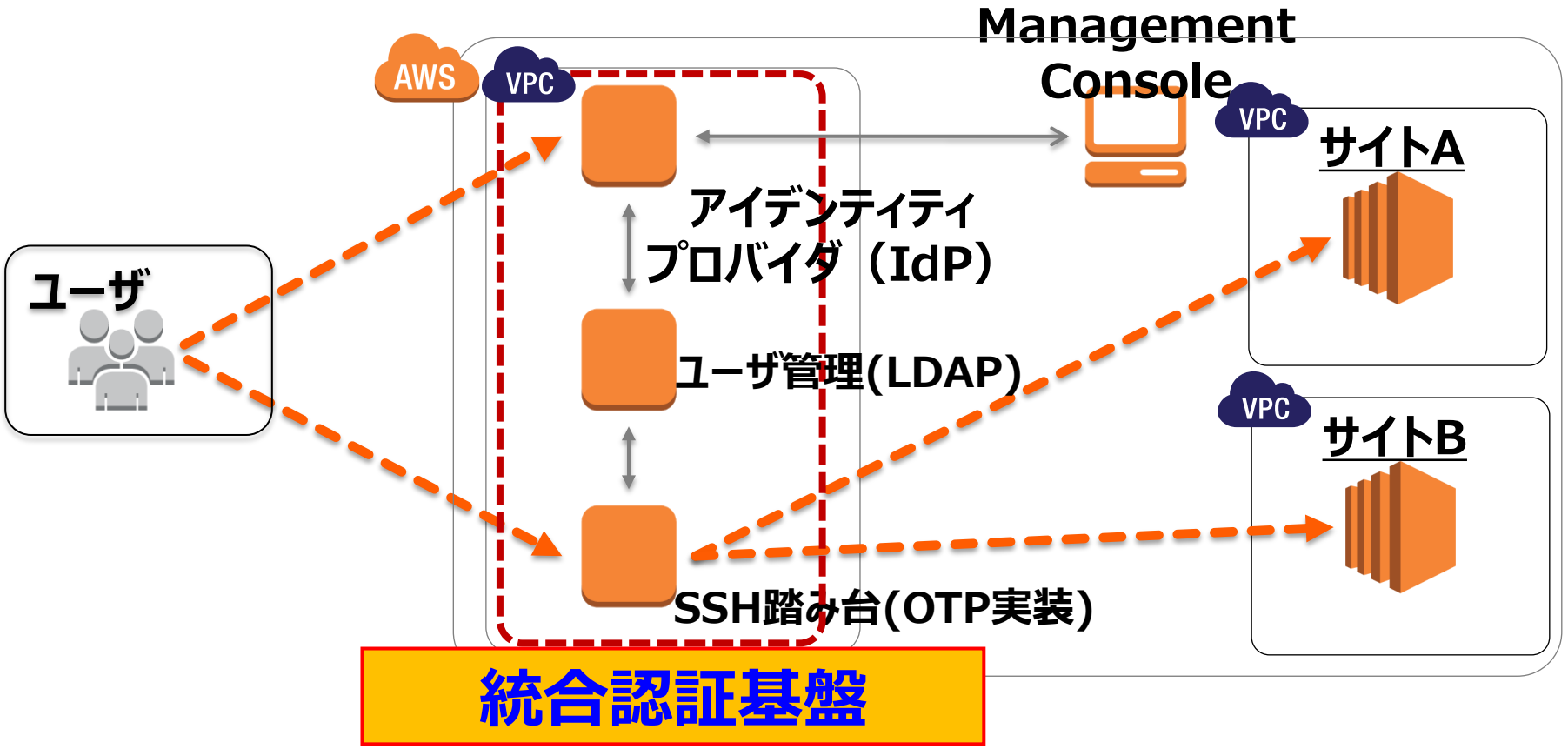
閲覧
グループ

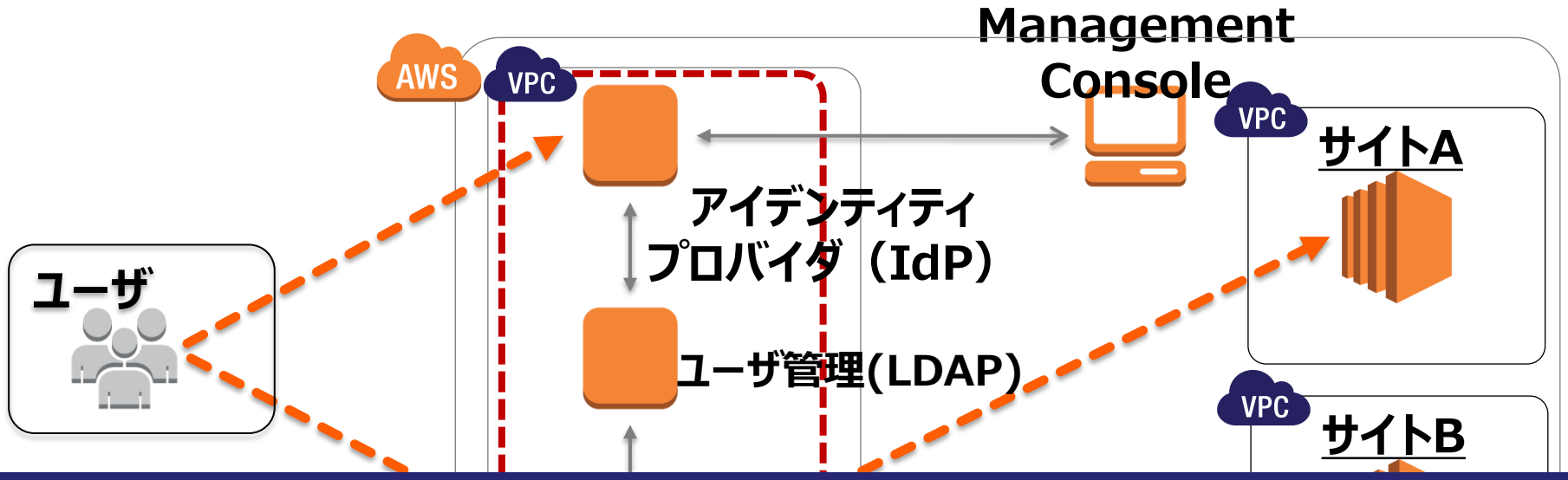
グループごとの分離設計だと
細かい権限設定が困難



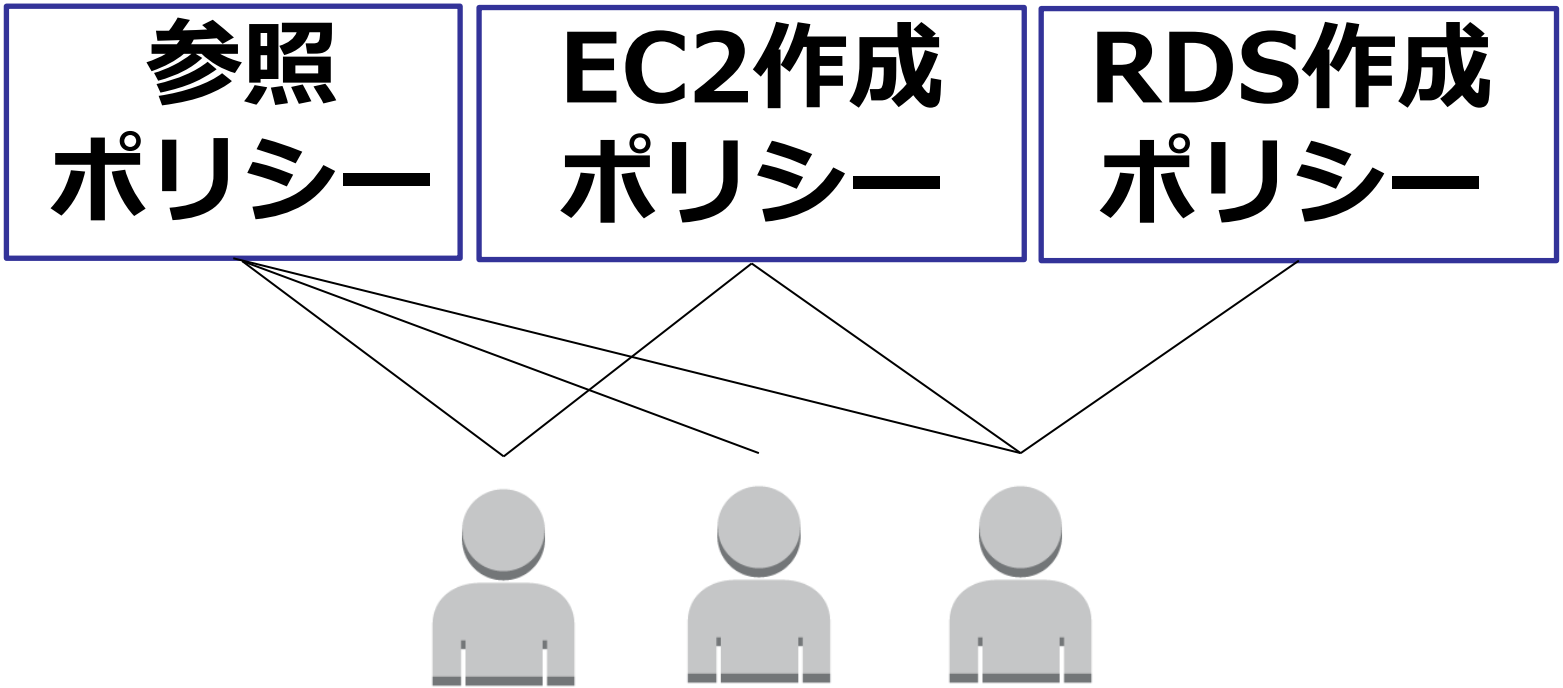


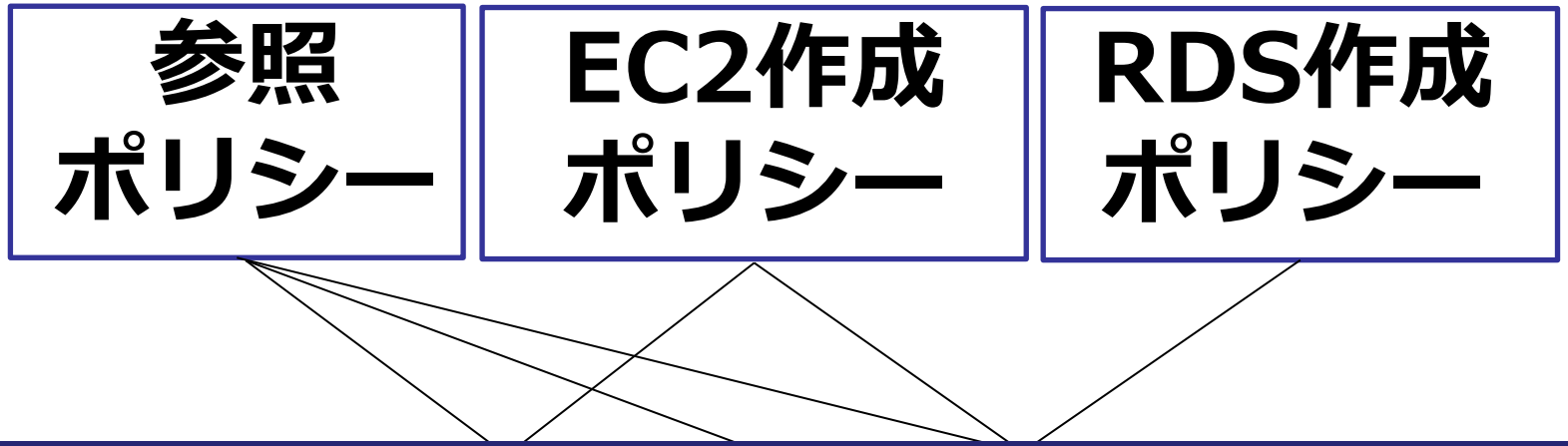
サービスと権限でグループを分離
カスタマイズ容易だがグループ管理は煩雑





2014年からはLDAPでのID管理を開始したため、現在はロールが主





利用サービスごとにポリシーを作成
問題は各サービスの関連性の把握

①ユーザー役割毎で分割	メリット：わかりやすい、管理楽 デメリット：細かい設定ができない
②サービスと権限で詳細に分割	メリット：個別対応可 デメリット：グループ管理が煩雑
③利用サービスベースで分割	メリット：①と②の両方の要望がそれなりに満たせる デメリット：各サービスの関連性を正しく理解するのが難しい

半年~1年サイクルで常に修正/更新

見直し

・ユーザー管理
・パスワード変更/管理
・ロック機能
・ワンタイム認証

IAMの権限機能

IAM権限設計に関わるアップデートを望みます

AWSのアップデート

ユーザー要望

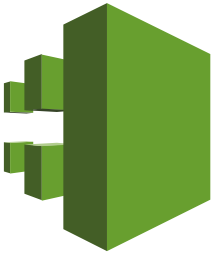
社内規定

管理方針の変更

社内環境の仕様変更

色々な要素があり、常にアップデートが必要





ベストを探し進化し続ける、それが重要

最後に

ビジョン
Vision

IT・ネットマーケティング領域において
トップレベルの専門スキルを持った人材が育ち、集い、楽しんでいる。

業界を驚かせるレベルで、
テクノロジーの開拓と、そのビジネス実装が実現している。

リクルートグループのビジネス、業界のルールを、
恒常的なイノベーションによって変革している。

各領域で共に働く仲間を募集しています！

http://recruit-tech.co.jp/recruitment/






ご清聴ありがとうございました

リクルートテクノロジーズ　検索