JNSA
NPO 日本ネットワークセキュリティ協会
Japan Network Security Association

エンタープライズID連携トラストフレームワークにおけるポリシーのあり方

2014 年 1 月29日

アイデンティティ管理WG

本日のセッション内容

1. エンタープライズ市場での認証基盤システム概要
2. エンタープライズ市場での認証基盤整備目的の変化
3. 運用管理ポリシーの説明先
4. トラストフレームワーク
5. ポリシーを主張することでトラストを築く
6. ID情報の正当性を保つための要素

本日のパネルテーマ

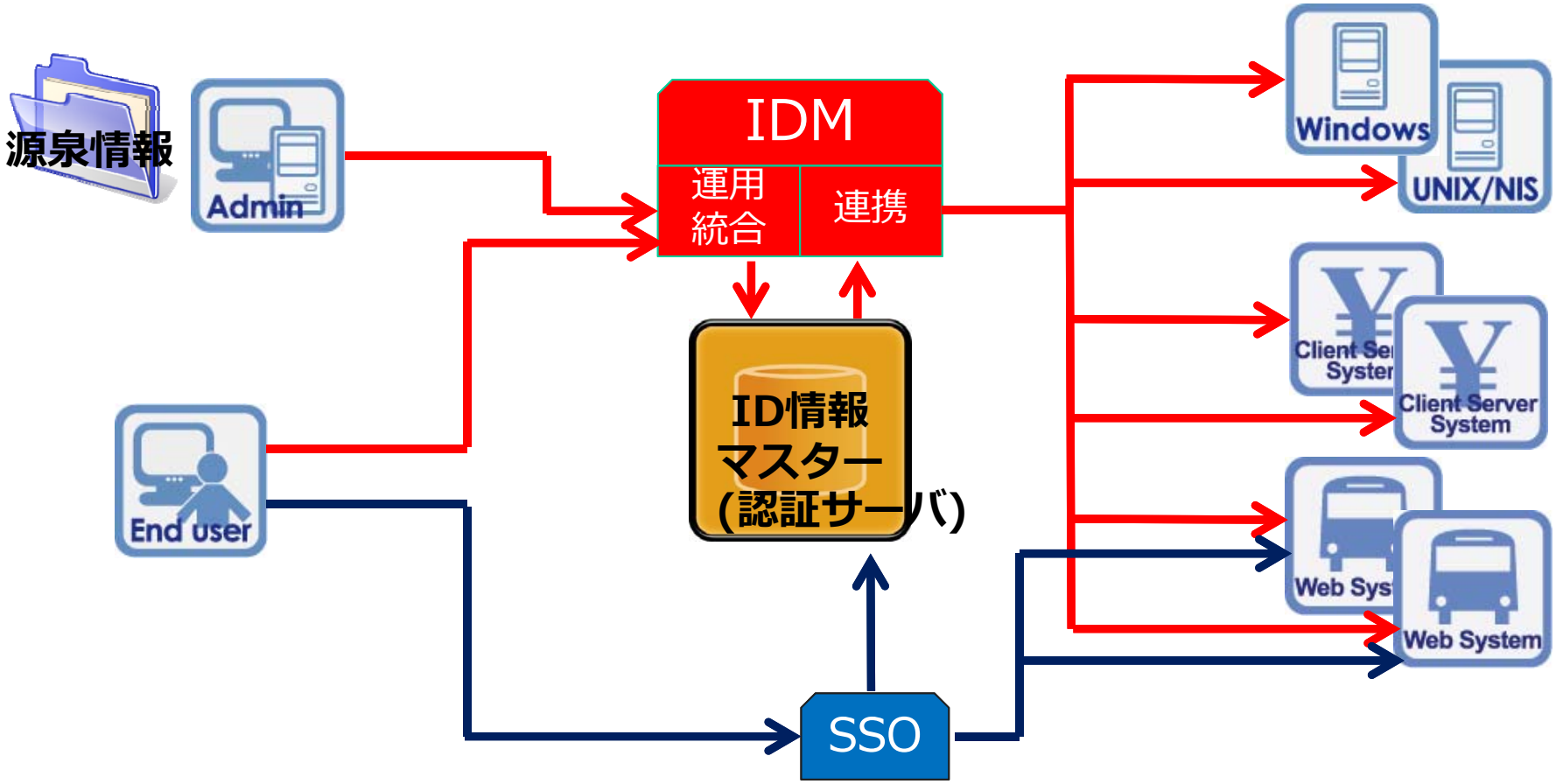
パネルディスカッション

モデレーター／パネリスト

モデレータ：
アイデンティティ管理WGリーダー
宮川 晃一　　（日本ビジネスシステムズ株式会社）

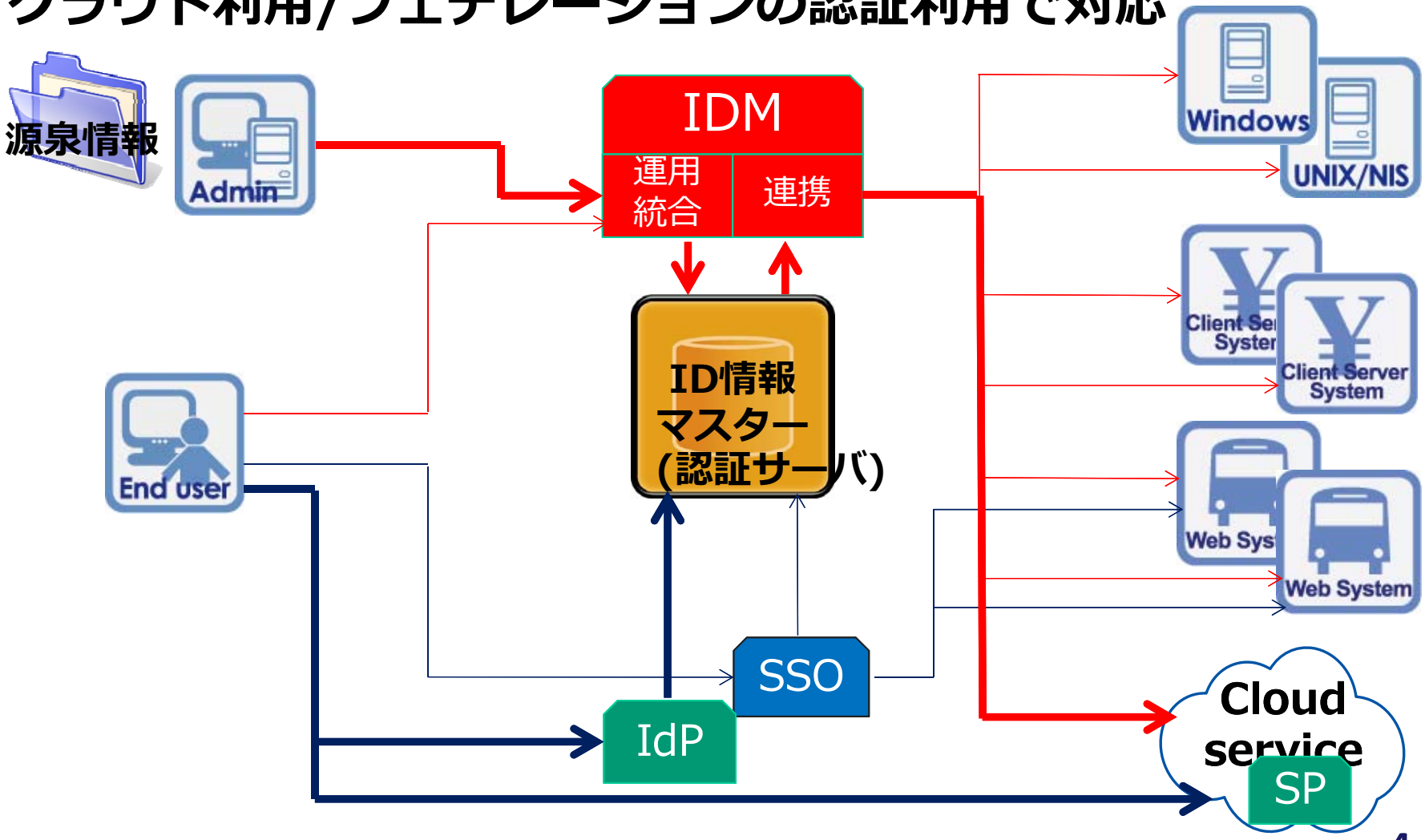
パネリスト：
南 芳明　　（株式会社シマンテック）
富士榮 尚寛　　（伊藤忠テクノソリューションズ株式会社）
中島 浩光　　（株式会社マインド・トゥー・アクション）
江川 淳一　　（エクスジェン・ネットワークス株式会社）

1. エンタープライズ市場での認証基盤システム概要



1. エンタープライズ市場での認証基盤システム概要

クラウド利用/フェデレーションの認証利用で対応



2. エンタープライズ市場での認証基盤整備目的の変化

～2002	〔認証・ID管理の効率化〕時代
クライアント・サーバシステムの増殖	
認証・ID管理・パスワードメンテの煩雑性顕著に	

2002～2006	〔セキュリティ強化〕時代
2003	個人情報保護法
2004	顧客情報漏えい事件多発

2. エンタープライズ市場での認証基盤整備目的の変化

2006～2011	〔統制強化〕時代	
2006	J-SOX(金融商品取引法)	Compliance
2009	リーマンショック	IT統制未対応
2010	Compliance is dead. →多様なステークホルダーの存在	Accountability
2011	オリンパス事件	Transparency

2. エンタープライズ市場での認証基盤整備目的の変化

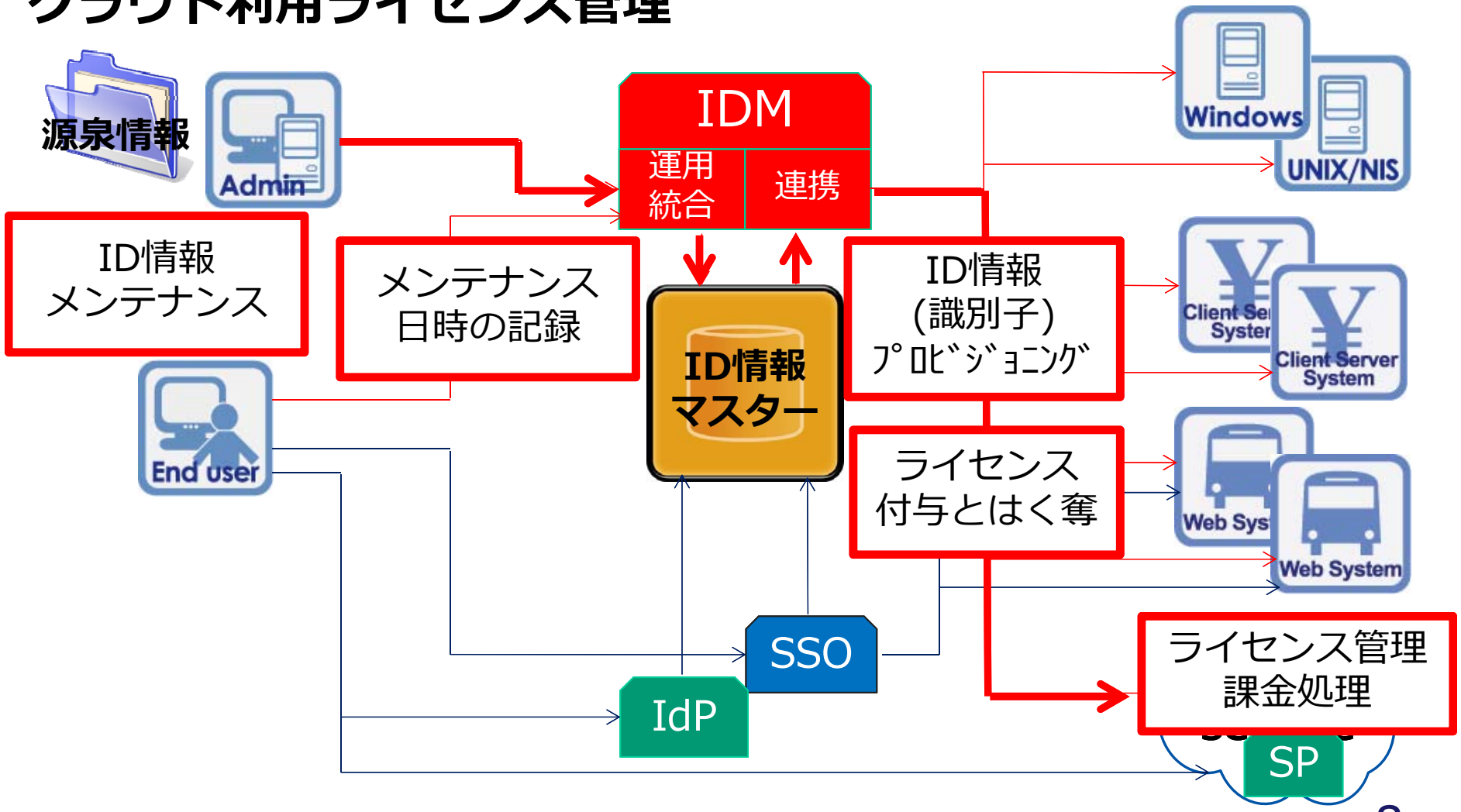
2012～	〔クラウド利用〕時代

クラウドビジネスの興隆　→クラウド利用普及前夜

クラウドサービス利用企業	・認証・ID管理の効率化 ・セキュリティ強化 **・クラウド利用ライセンス管理** **・フェデレーション対応の裏付け**
クラウドサービス提供企業	・透明性確保 （IT統制必須）

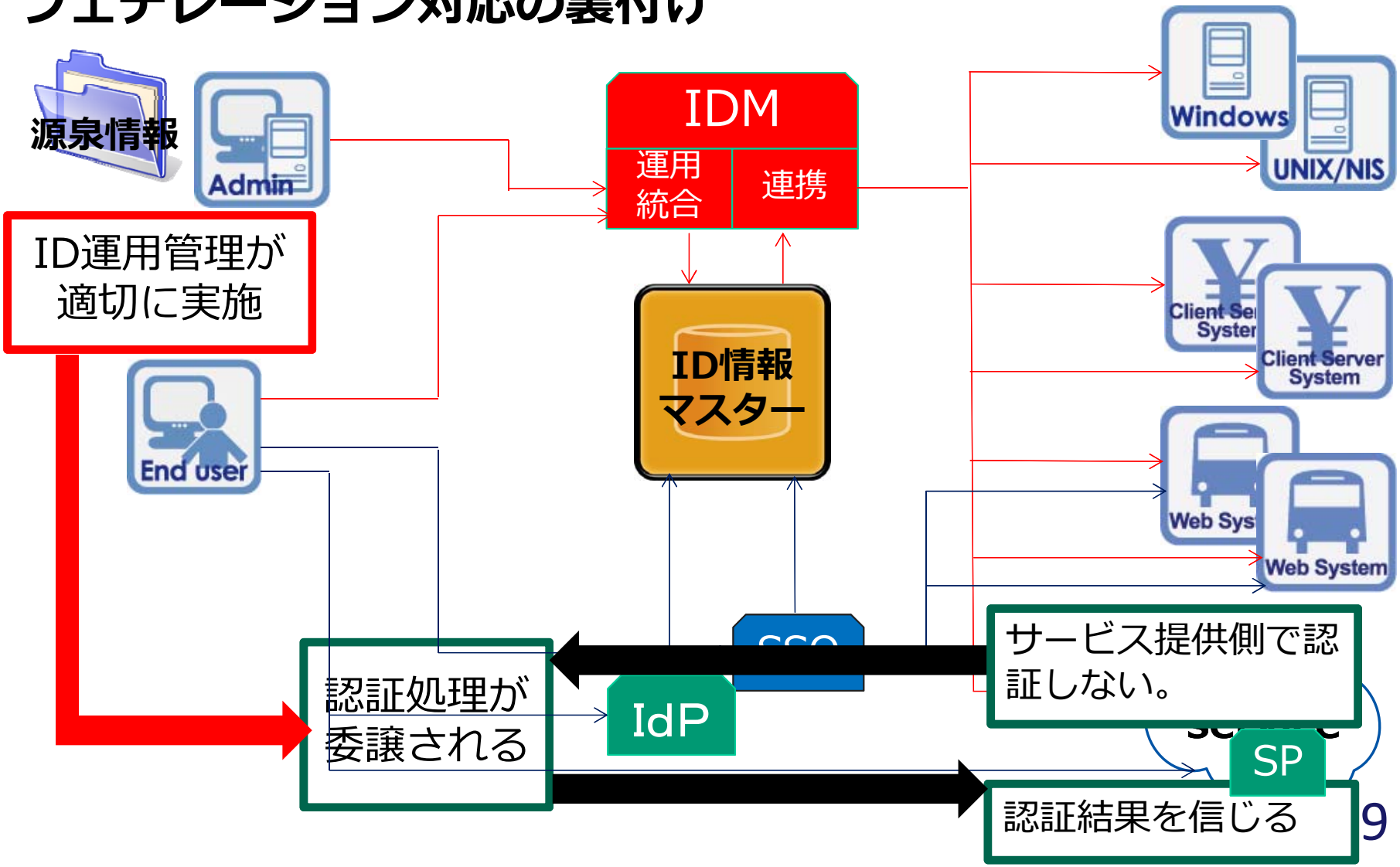
2. エンタープライズ市場での認証基盤整備目的の変化

クラウド利用ライセンス管理



2. エンタープライズ市場での認証基盤整備目的の変化

フェデレーション対応の裏付け



2. エンタープライズ市場での認証基盤整備目的の変化

クラウド利用時代 は ID運用管理が適切に実施 されている

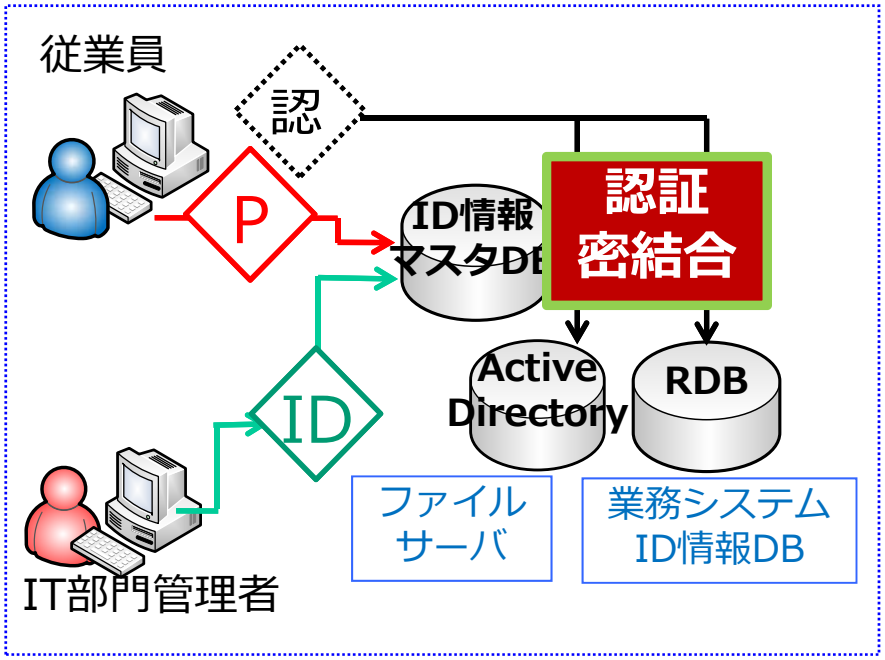
必要があり、そのために 認証基盤を整備 する。

誰が必要としているのか → 情報共有相手

何を以て適切と判断するのか → 運用管理**ポリシー**に沿った ID運用管理**システム**

3. 運用管理ポリシーの説明先

密結合完結時代

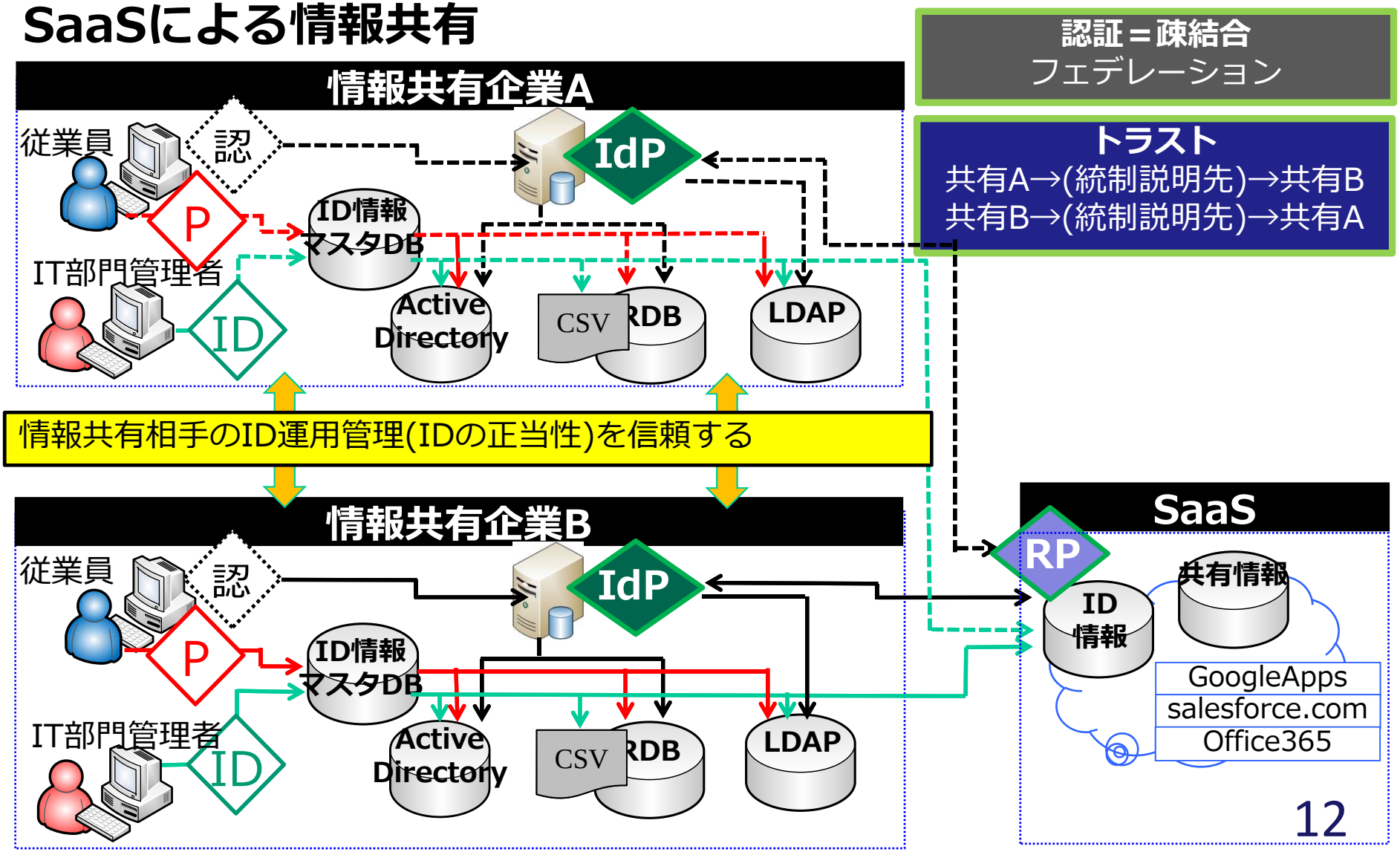


密結合完結時代

運用管理ポリシー → **J-SOX**
企業→(統制説明先)→株主様

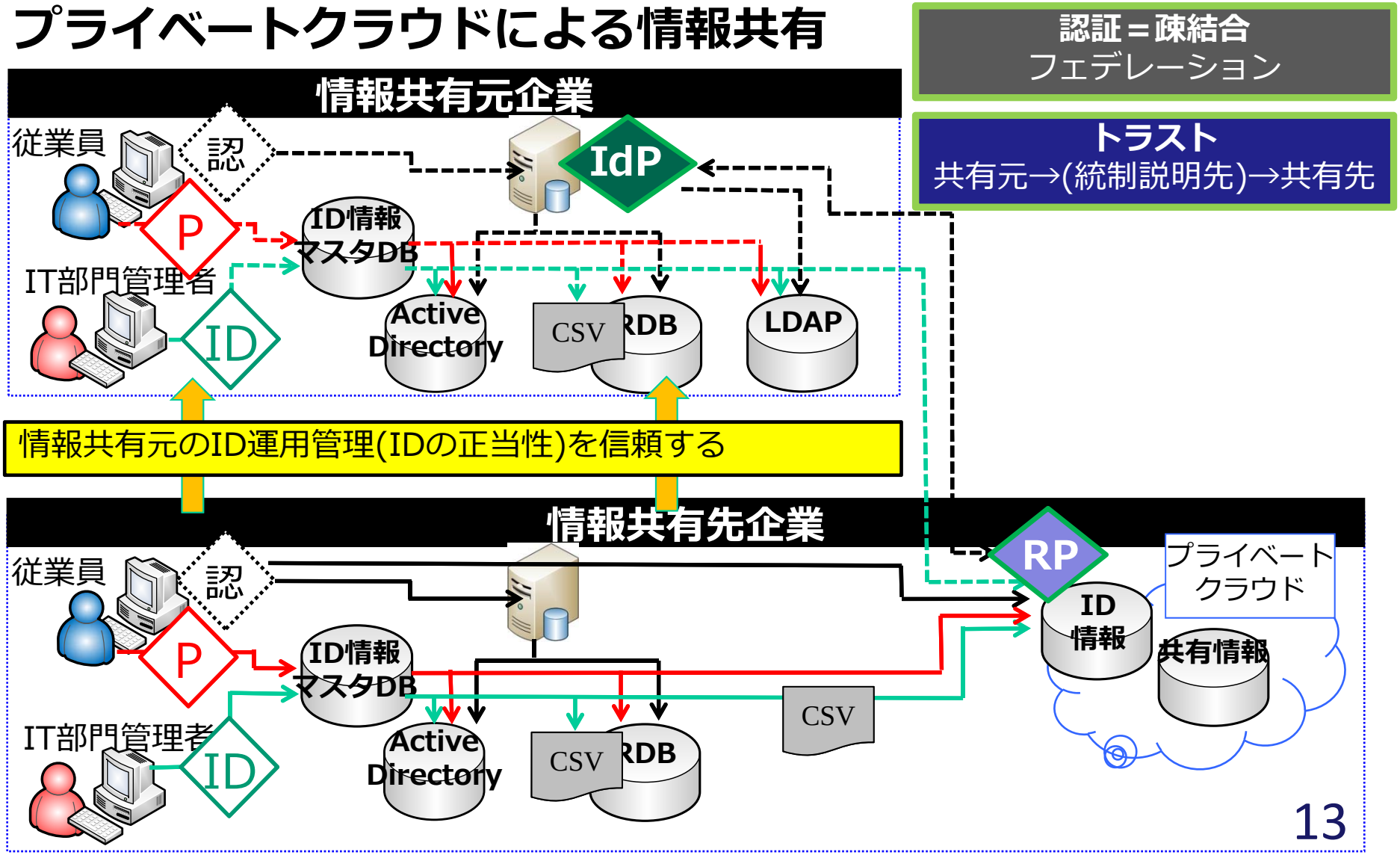
3. 運用管理ポリシーの説明先

SaaSによる情報共有



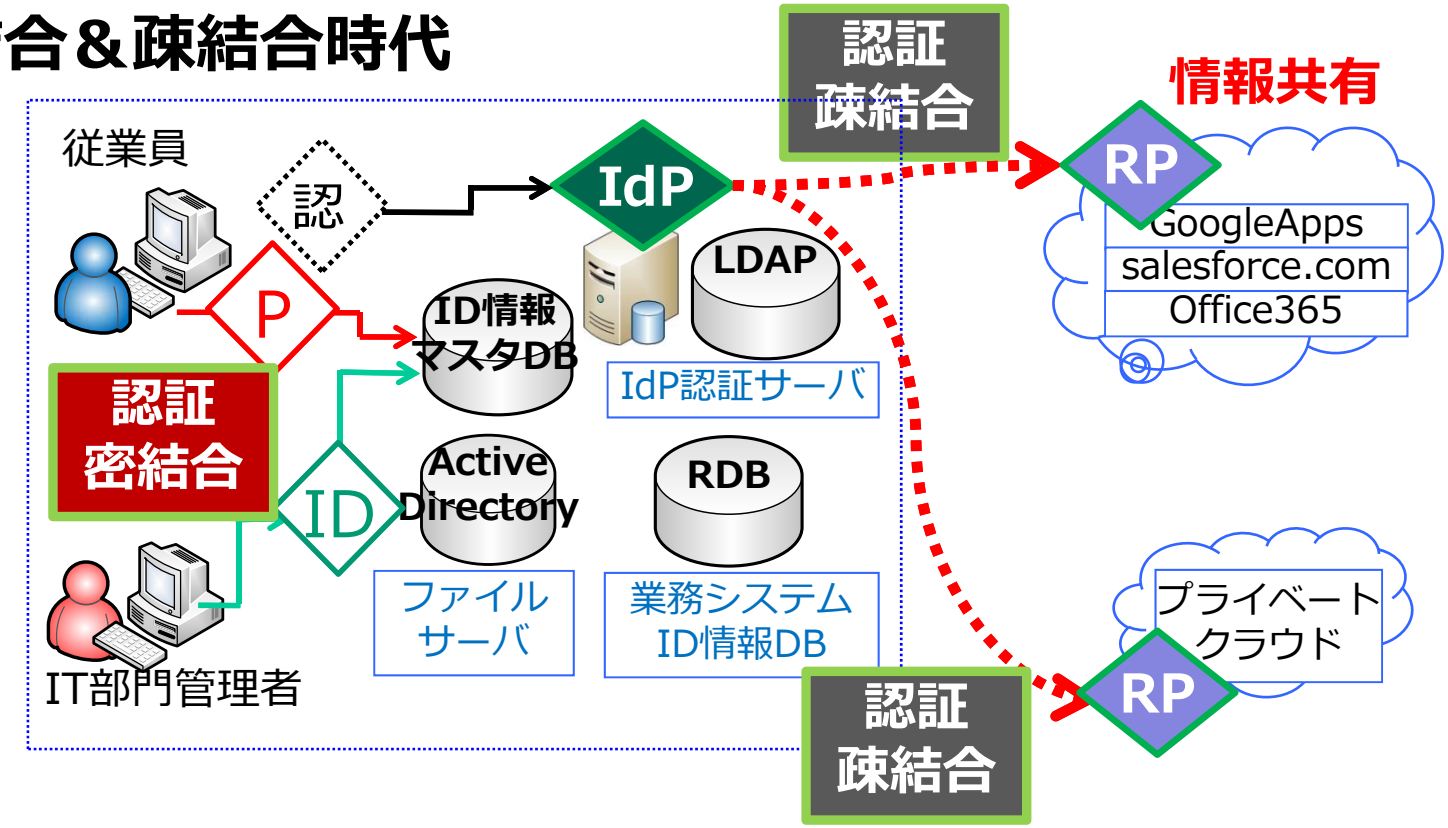
3. 運用管理ポリシーの説明先

プライベートクラウドによる情報共有



3. 運用管理ポリシーの説明先

密結合＆疎結合時代

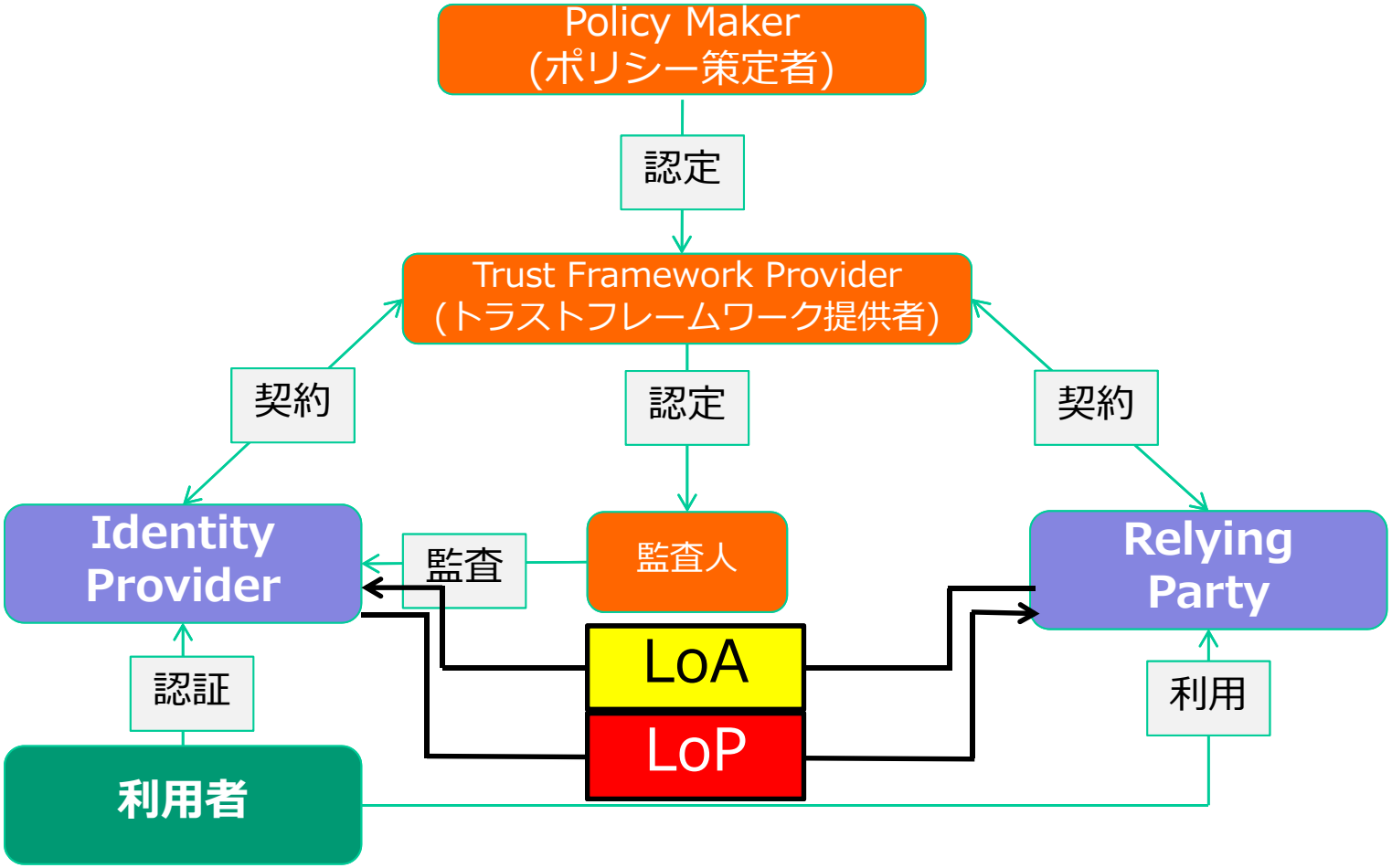


運用管理ポリシー

- 密結合＆疎結合時代
- **トラスト**
  企業→(統制説明先)→共有相手
- **J-SOX**
  企業→(統制説明先)→株主様

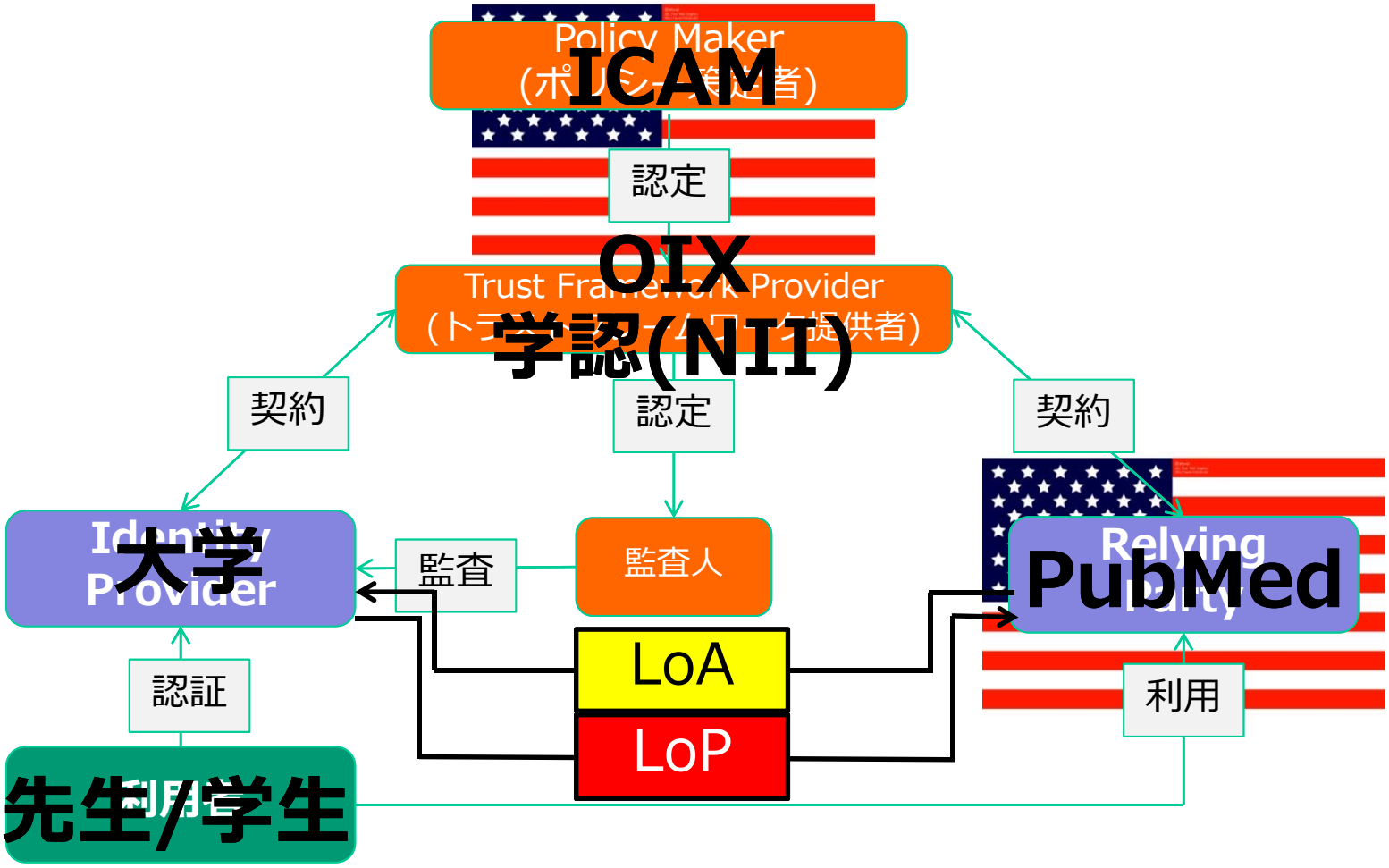
4. トラストフレームワーク

基本モデル



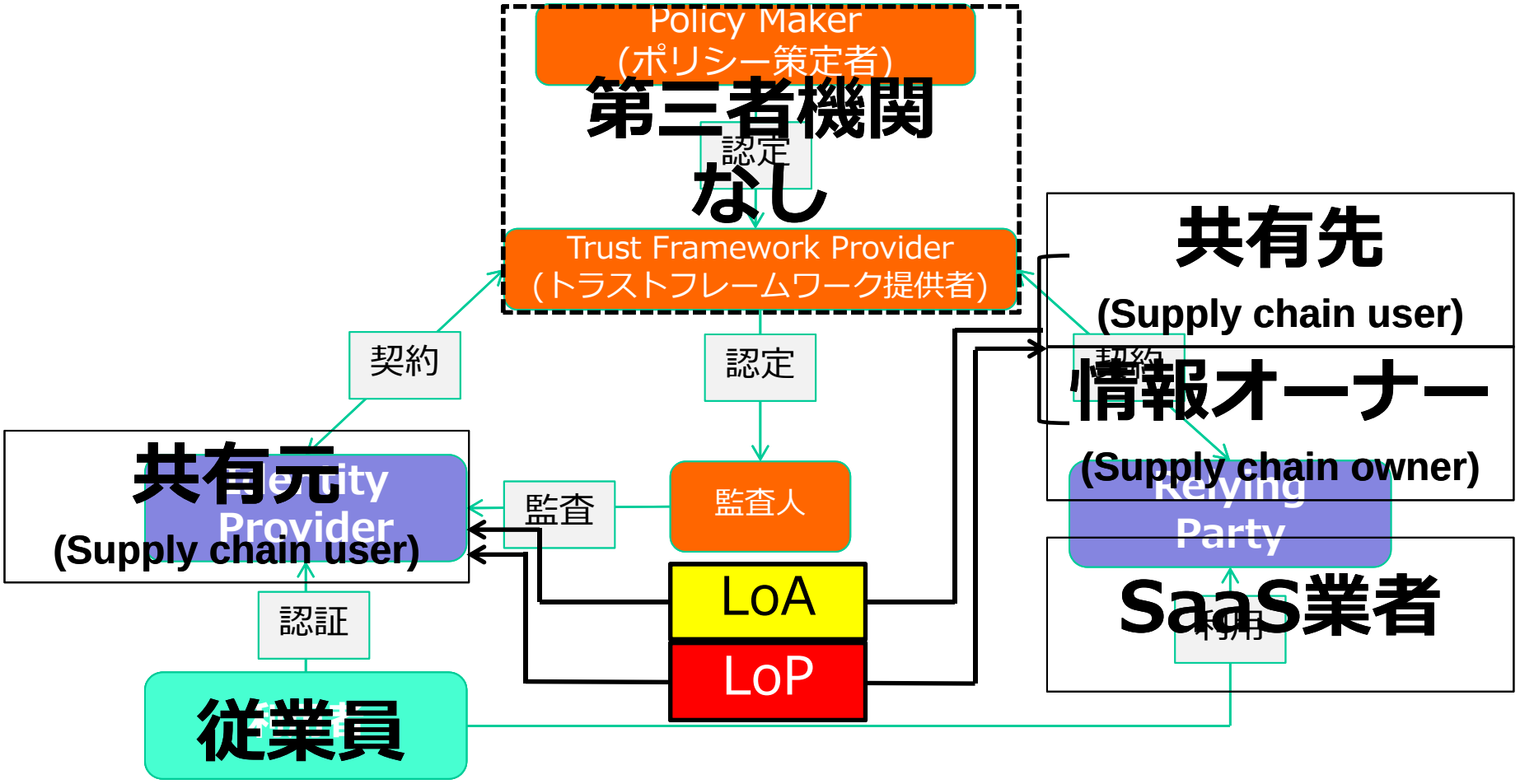
4. トラストフレームワーク

学認モデル



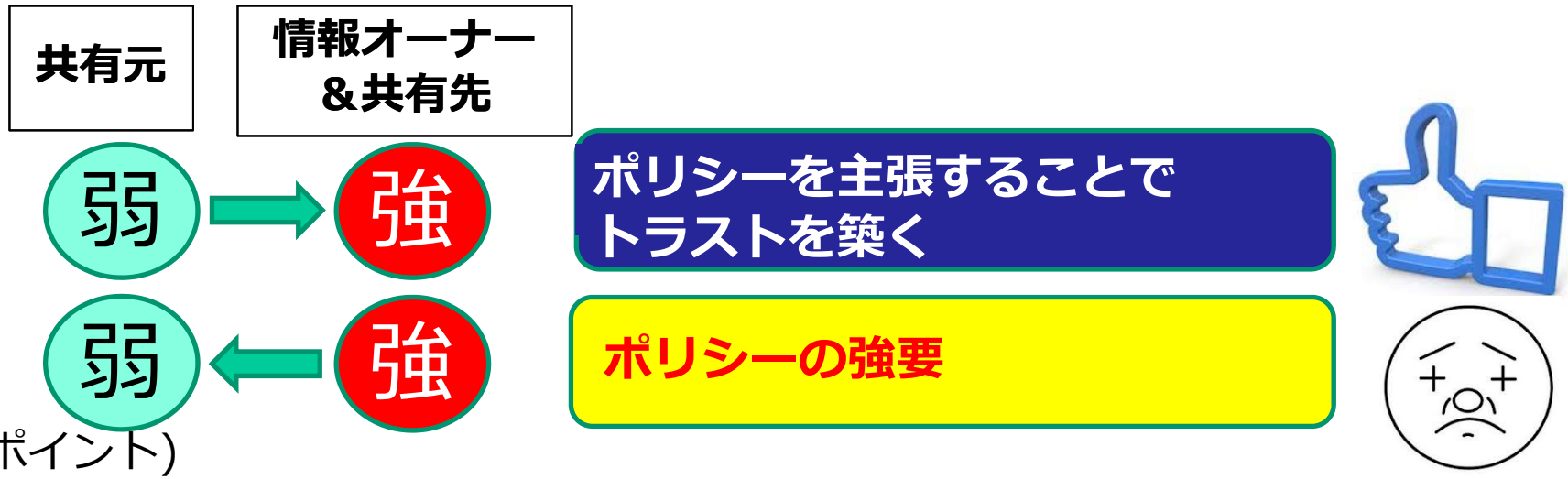
4. トラストフレームワーク

エンタープライズモデル



5. ポリシーを主張することでトラストを築く

〔IDM-WGの検討内容として〕エンタープライズ市場のトラストフレームワークにおいて第三者機関が存在しない状態で、フェデレーションを利用して情報を共有する場合、IdPでの適切な認証とアクセス制御が維持されていると主張できるポリシーの要点をまとめる



(ポイント)

1.多額の投資や多くの運用負荷がかからないReasonableなレベル。

2.以下の規定を参考にして良いとこ取りをする。

①学認運用規定

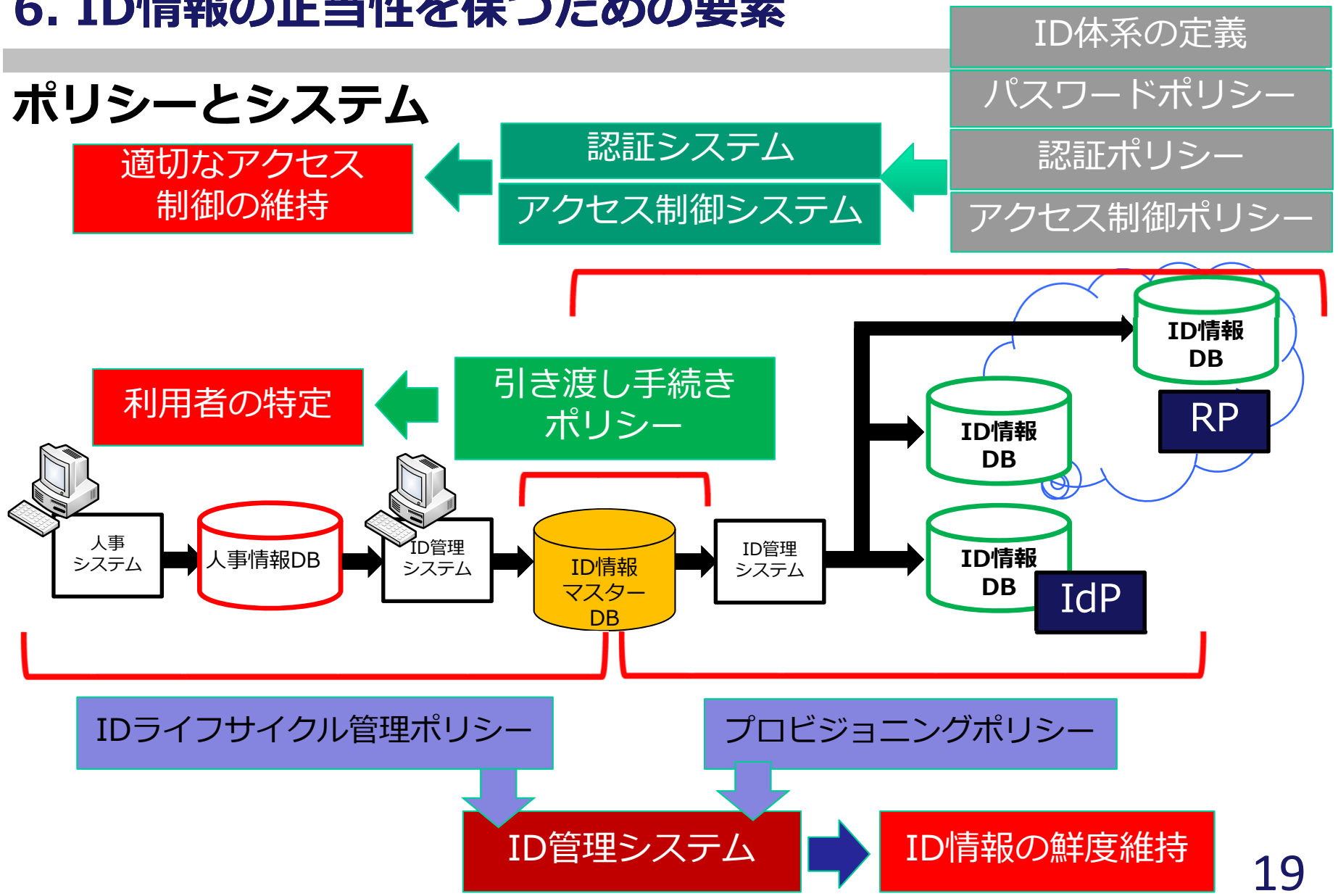
②PCIDSS (Payment Card Industry Data Security Standard)

③FISC　(Center for Financial Industry Information Systems)

④SYMANTEC PKI CP/CPS

6. ID情報の正当性を保つための要素

ポリシーとシステム

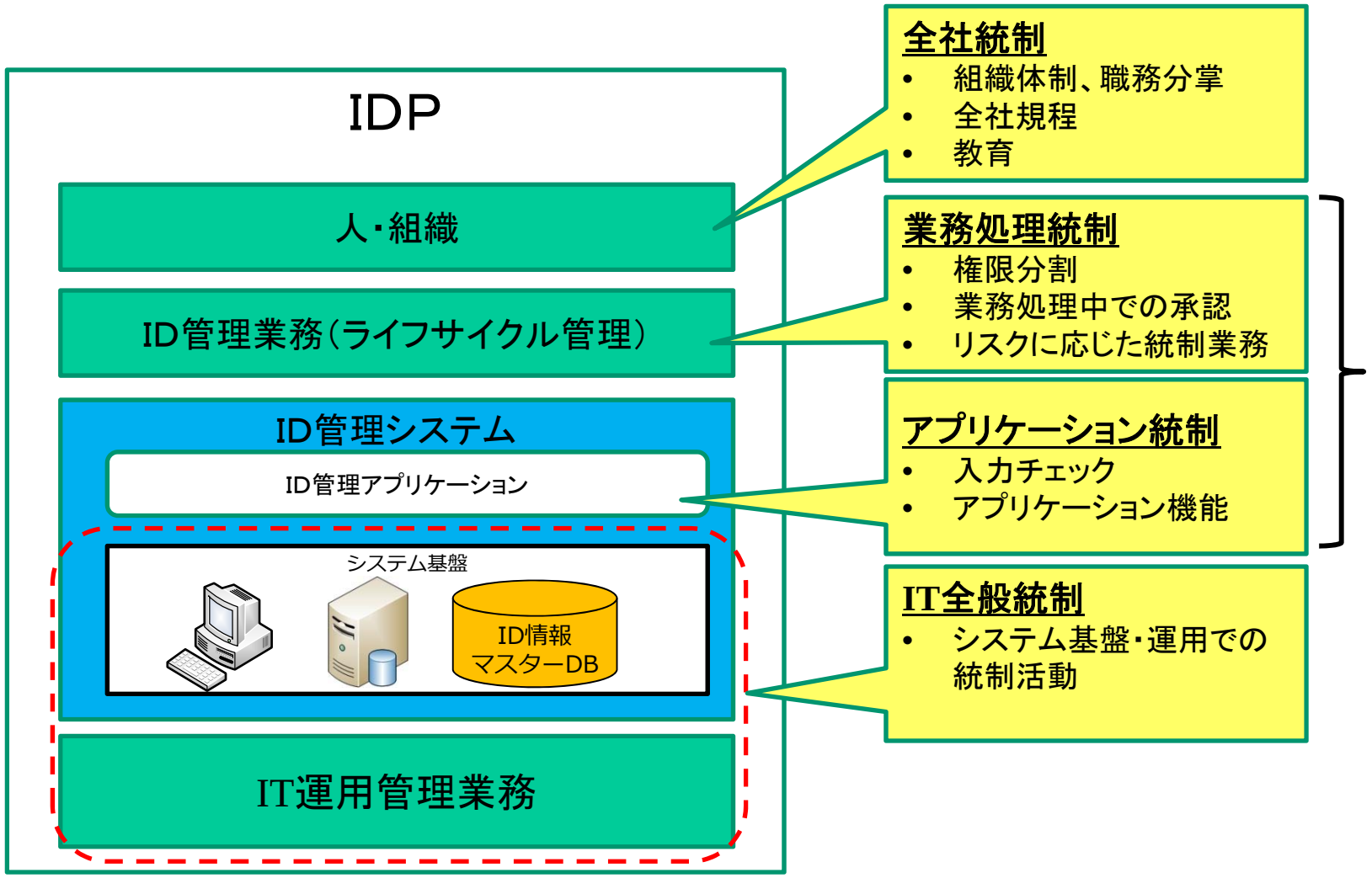


パネルディスカッションテーマ

1．エンタープライズ間でID連携を行うときの問題点とは
　　具体的なケースとして・・・・
　　・アクセス権限を維持するには
　　・エンタープライズITにおける適切なIDの引き渡し

2．トラストポリシーを内部統制モデルとして解説
　　トラストの構成要件とそれにもとづく統制活動とは

トラストポリシーを内部統制モデルとして解説したら



トラストの構成要件とそれにもとづく統制活動とは

トラスト　＝ 望ましい状態
＝ NOT（望ましくない状態）
＝ NOT（リスクが大きい状態）

どのようなリスクがトラストの何（構成要件）を侵すのか、
また、それをどう防ぐのか（統制活動）

トラストの構成要件（一部）		リスク	統制活動
ID有効性	IDが有効なIDであること	期限切れIDの利用 退職者IDの利用	IDのライフサイクル管理
ID本人到達性	IDが表す本人を唯一に特定可能であること	行為者が分からない 例）請求先が不明になる	ID登録・発行手順
ID利用者認証	IDの利用者が本人であること	IDの利用時の成りすまし	認証方式