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

JNSA　2013年度活動報告会

「 2013年度 アイデンティティ管理WG 成果報告 」

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）

2014 年　6月　10日（火）　ベルサール神田

ＷＧ活動報告内容

１．２０１３年度の活動内容

２．エンタープライズID連携トラストフレームワーク
　　ポリシー検討

３．エンタープライズロール管理

４．今年度の活動テーマ

１．2013年度の活動内容について

２０１３年度活動内容について

２０１３年度は以下のテーマで議論をいたしました。

1．エンタープライズID連携トラストフレームワーク
　　ポリシー検討

2．特権ID管理

3．エンタープライズロール管理

4．IDとプライバシー（勉強会）

5．ID管理ソリューション比較軸検討（IT&IDイベント用）

２０１３年度活動内容について

また、各種セミナー協力、他団体連携を行いました。

１． ID & IT Management Conference 2013 (2013/9/18,9/20)　**協力**

２． Japan Identity & Cloud Summit 2014 (2014/1/14, 1/15)　**協力**

３．OpenID ファンデーション・ジャパン　EIWG　協力
『OpenID ConnectとSCIMのエンタープライズ利用ガイドライン』公開

４．経済産業省　ID連携トラストフレームワーク　検討委員会 協力

５．ID連携トラストフレームワークアイデアソン(2014/1/27)　**参加**

６．シンポジウム「アイデンティティ連携が生み出す社会」 参加

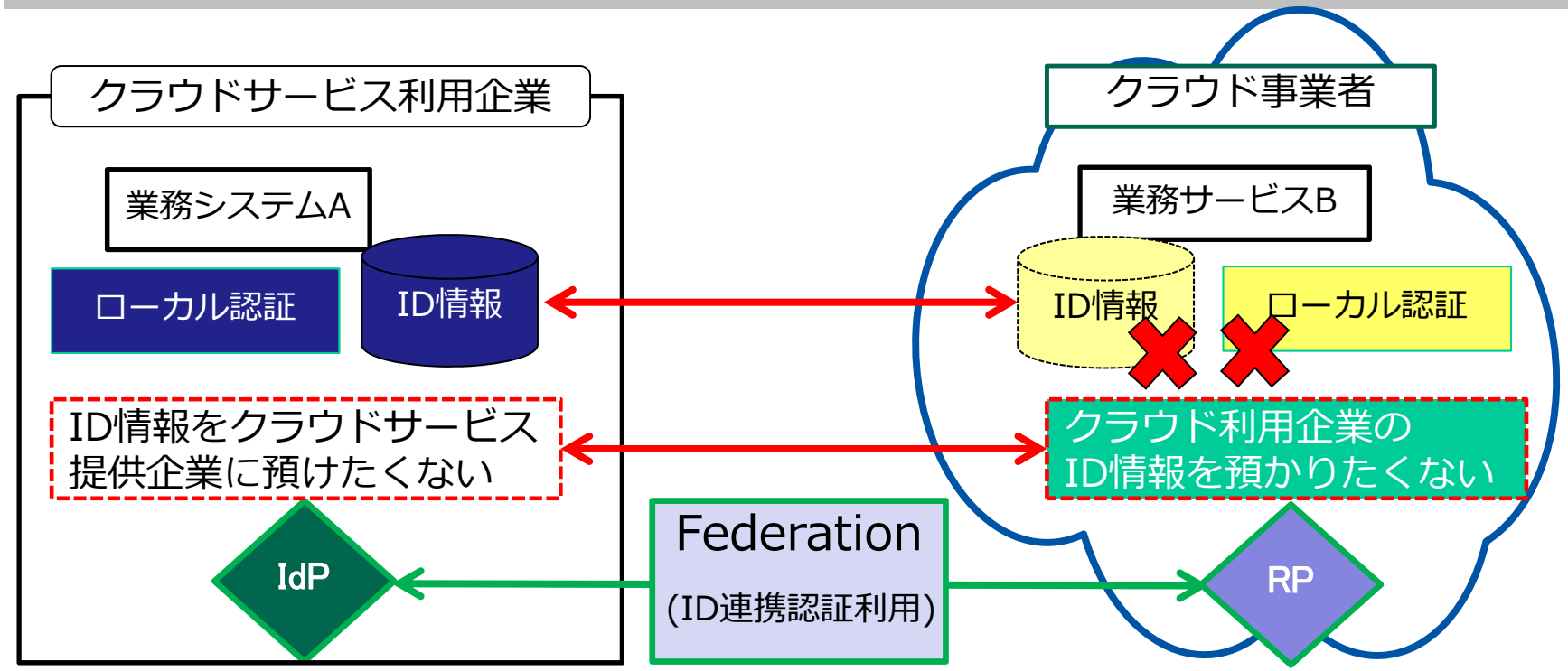
(2014/3/14)

２．エンタープライズID連携トラストフレームワークポリシー検討

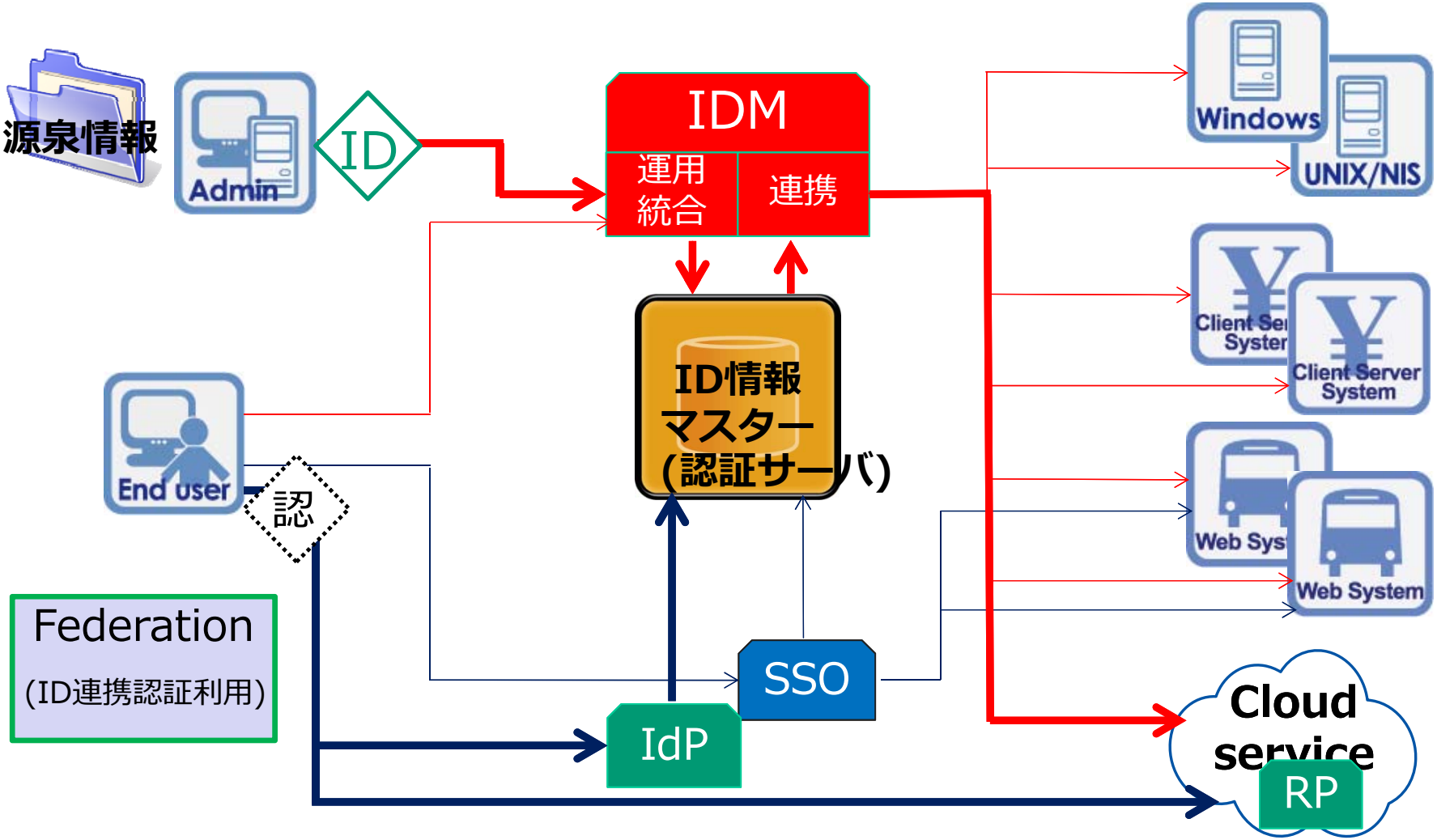
「トラスト確立のための共通ポリシーを考える」
～トラストを主張できるポリシーとは～

1. クラウド利用時の認証基盤システム

①ローカル認証⇒フェデレーションの認証利用

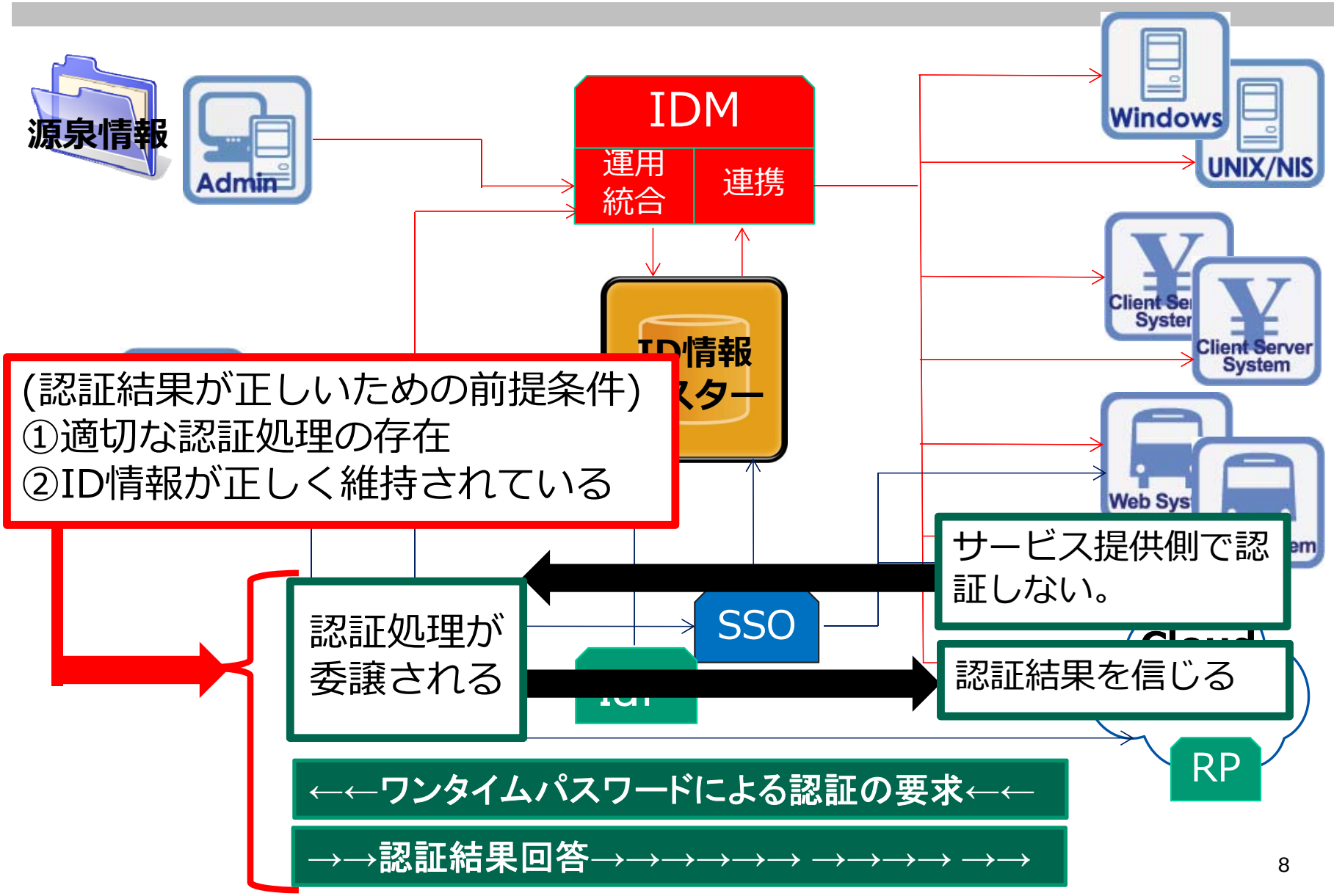


1. クラウド利用時の認証基盤システム
②システム構成



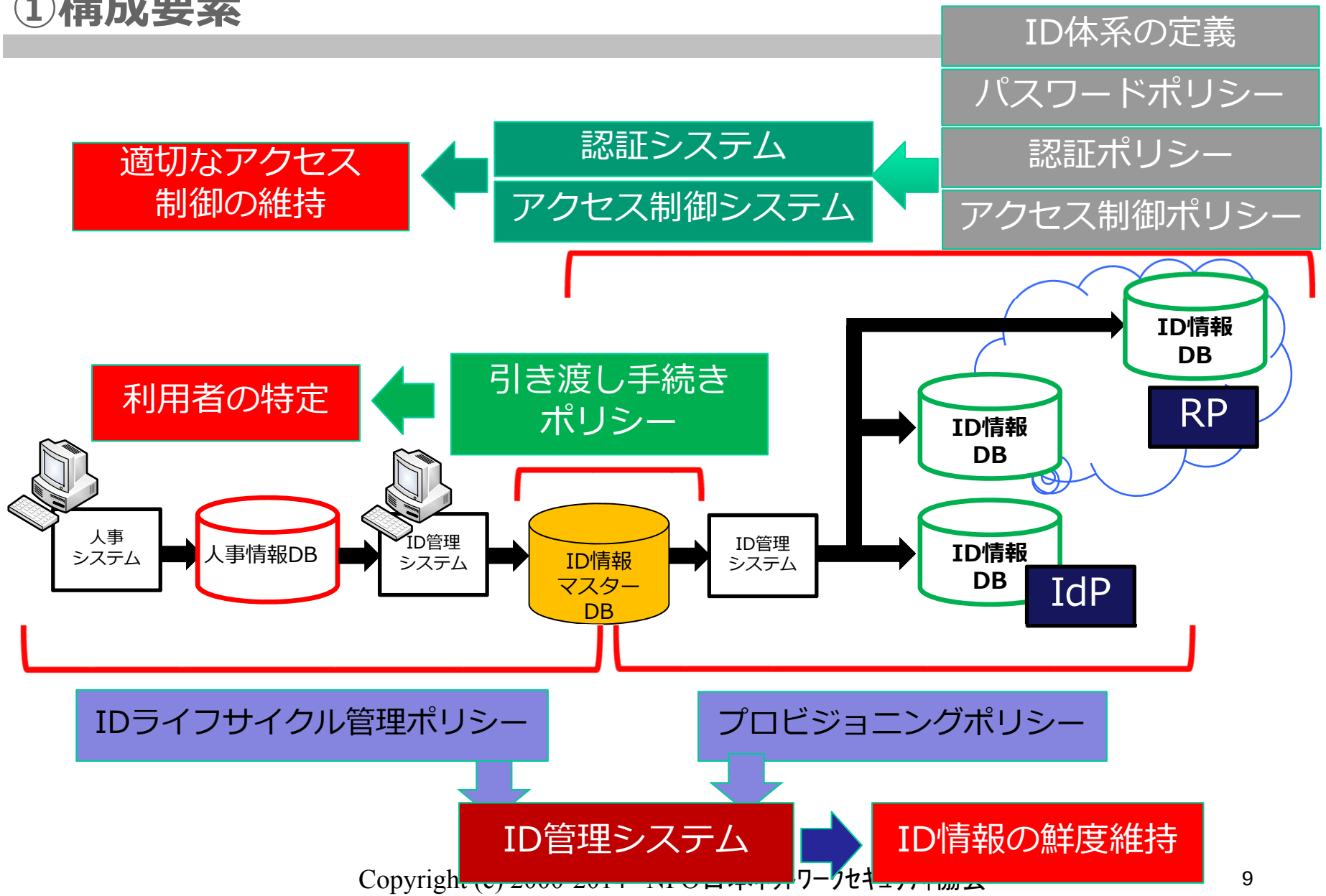
1. クラウド利用時の認証基盤システム

③フェデレーションが維持される前提条件



2. ID情報と認証結果の正当性

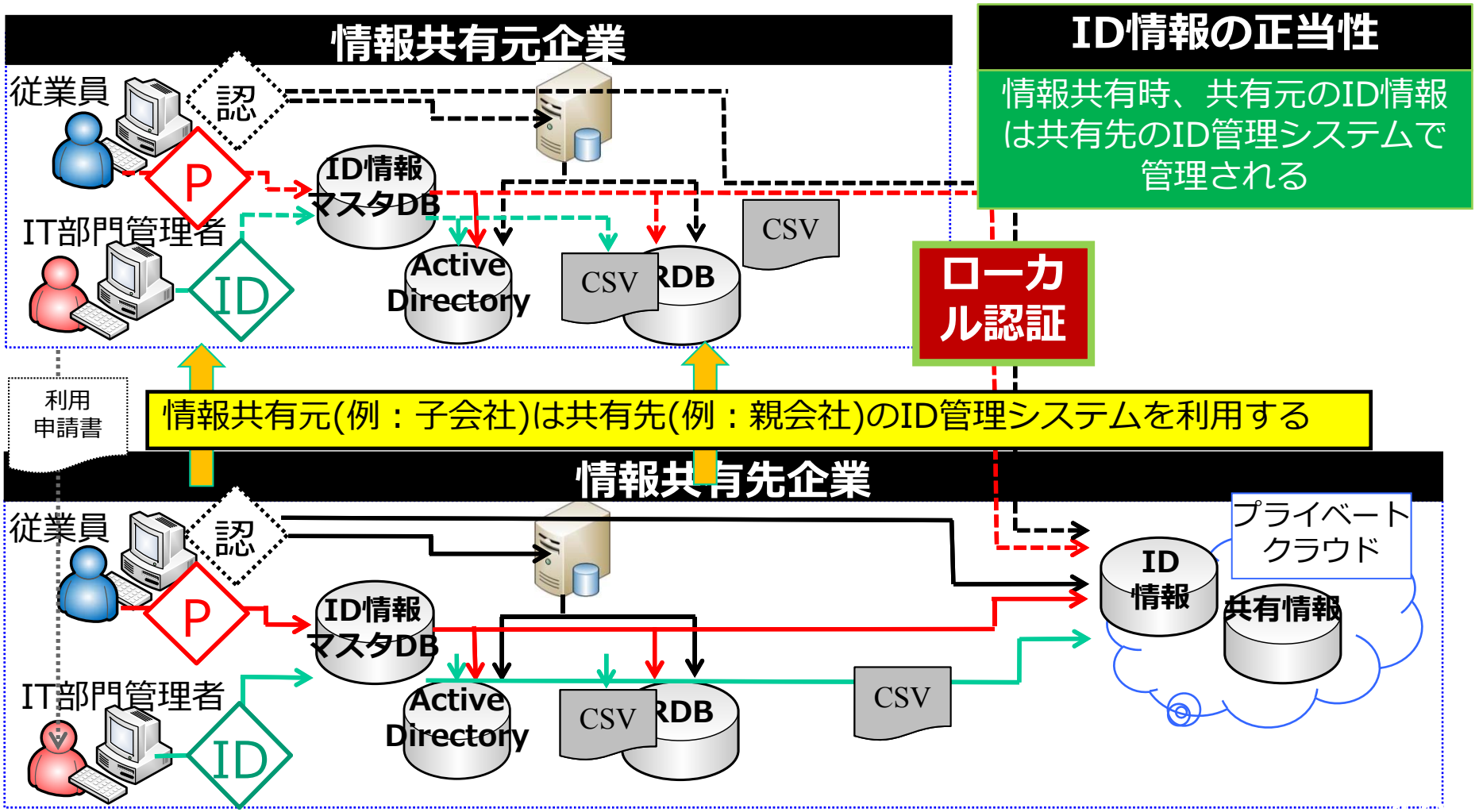
①構成要素



2. ID情報と認証結果の正当性

②情報共有時のID情報の正当性の説明責任

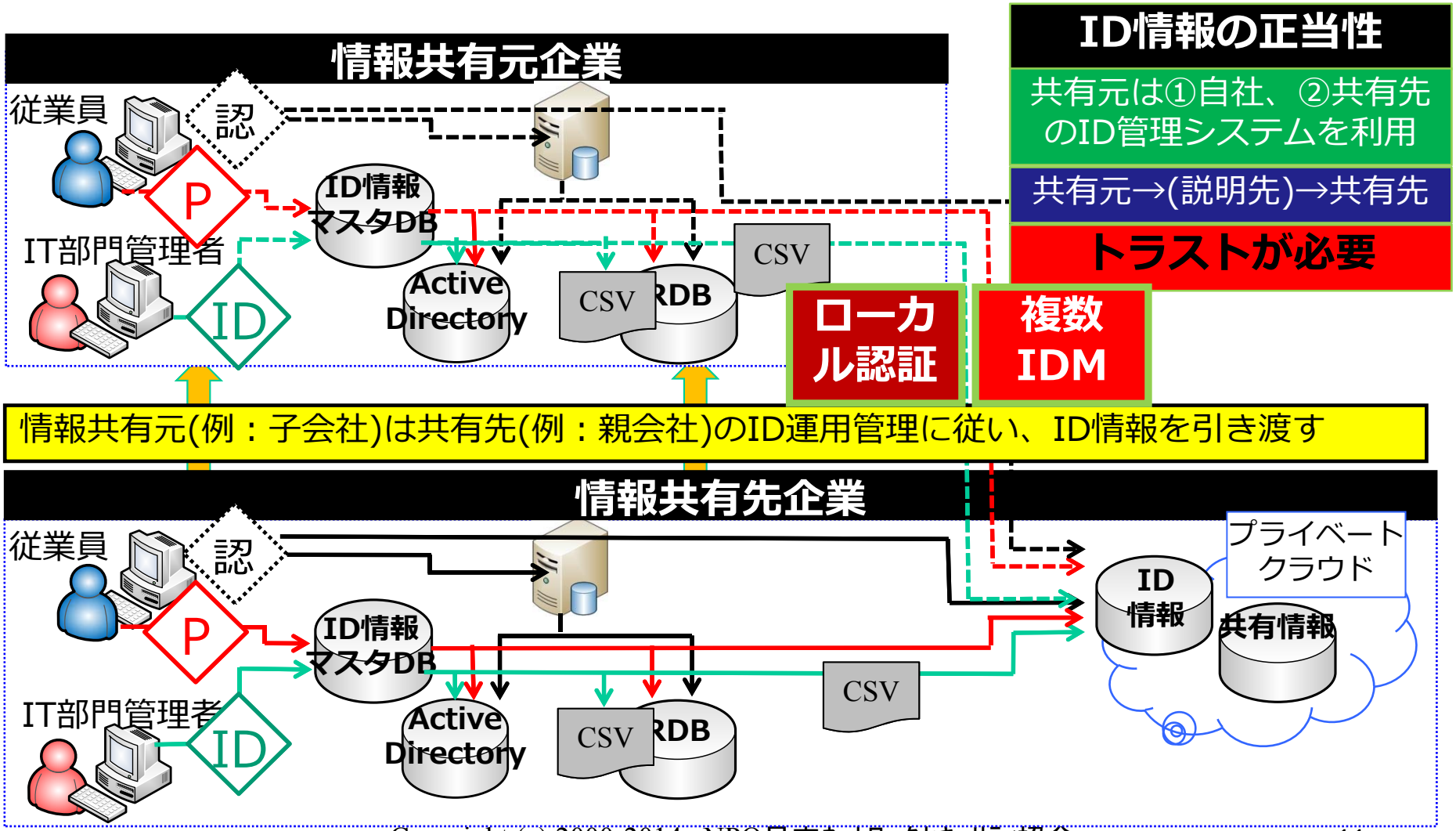
(1) 情報共有(プライベートクラウド/フェデレーションなし/申請書)



2. ID情報と認証結果の正当性

②情報共有時のID情報の正当性の説明責任

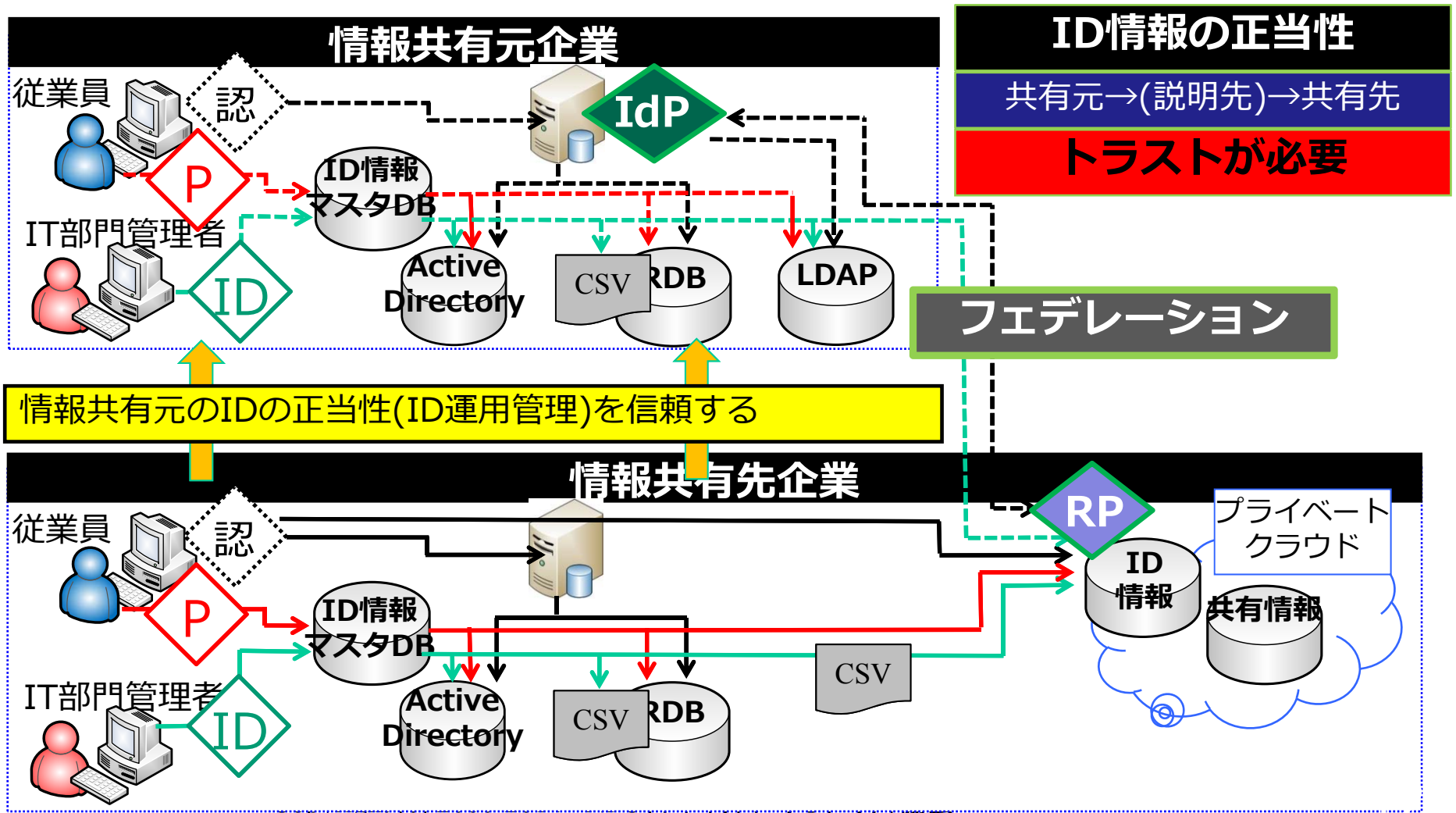
(2) 情報共有(プライベートクラウド/フェデレーションなし)



2. ID情報と認証結果の正当性

③情報共有時の認証結果の正当性の説明責任

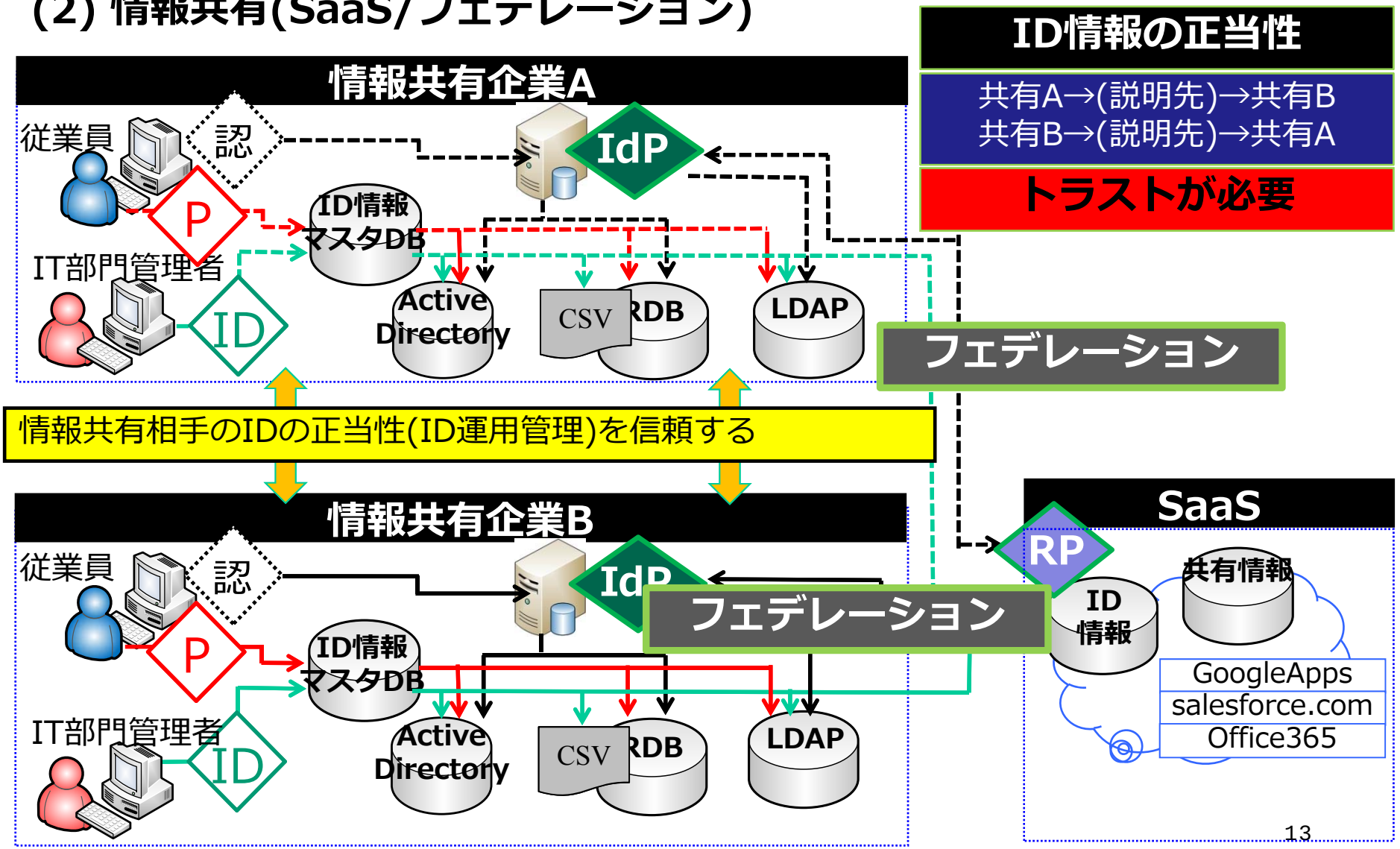
(1) 情報共有(プライベートクラウド/フェデレーション)



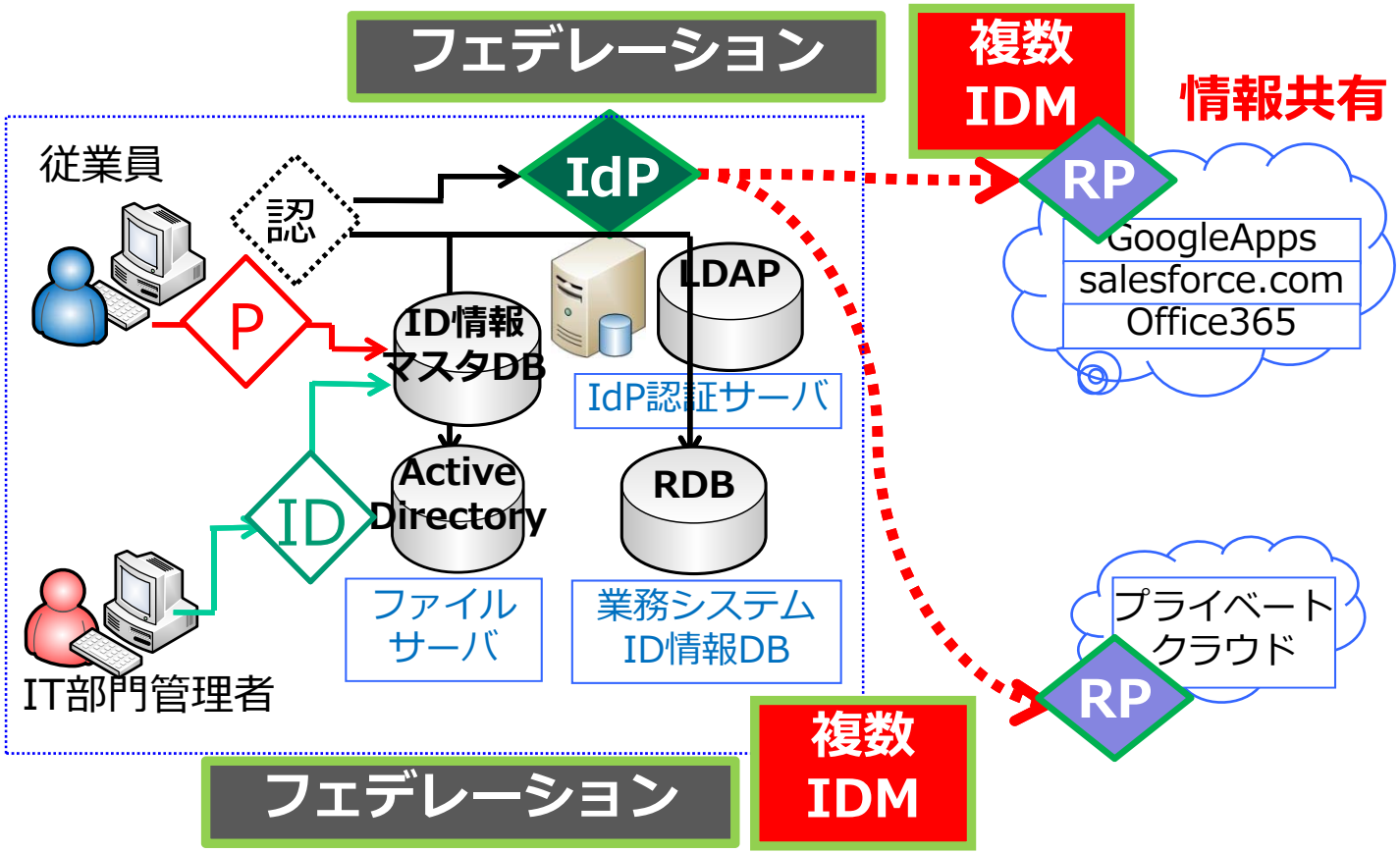
2. ID情報と認証結果の正当性

③情報共有時の認証結果の正当性の説明責任

(2) 情報共有(SaaS/フェデレーション)



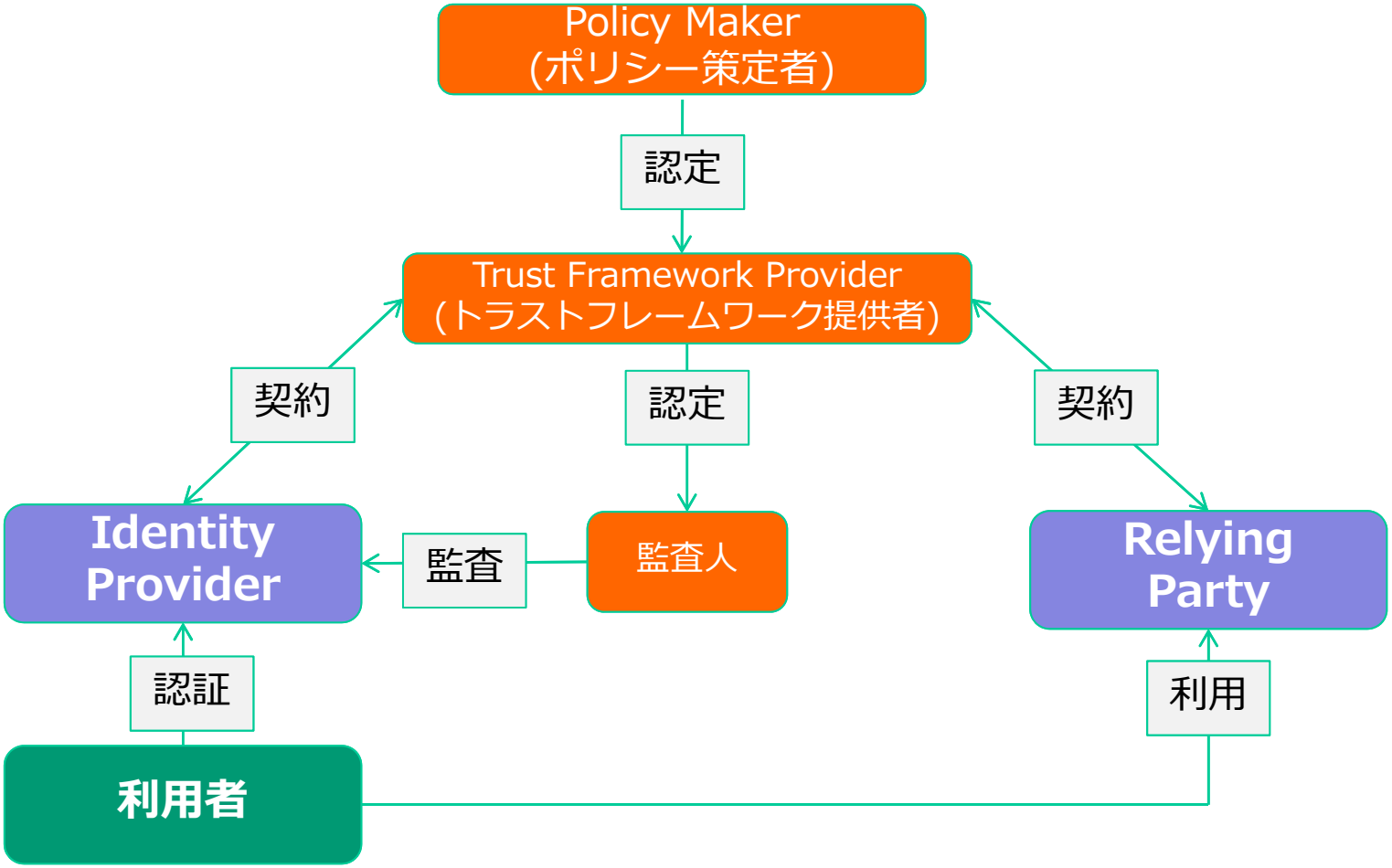
2. ID情報と認証結果の正当性
④まとめ



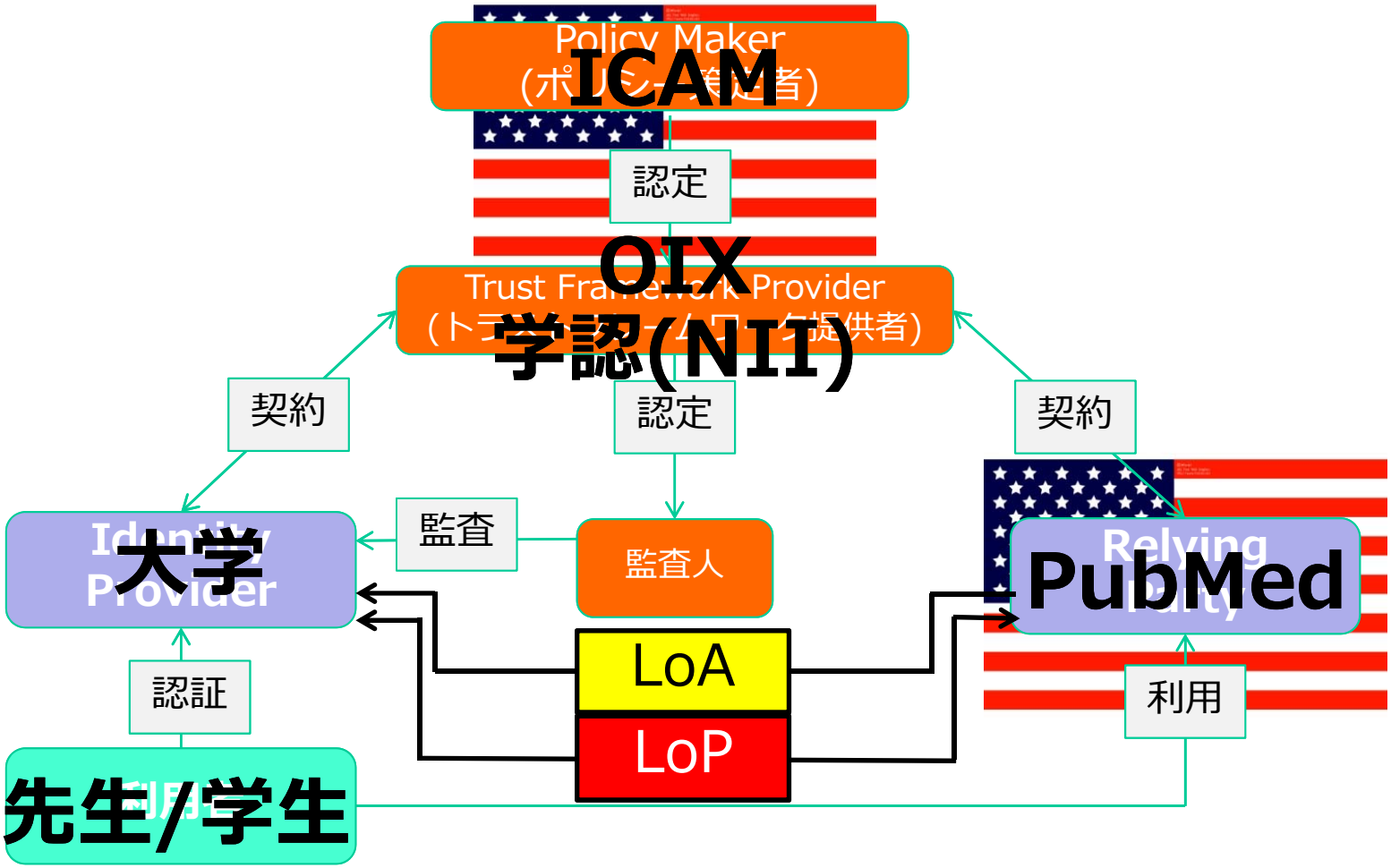
ID情報と認証結果の正当性

企業→(説明先)→株主様	共有元→(説明先)→共有先
J-SOX	**トラスト**

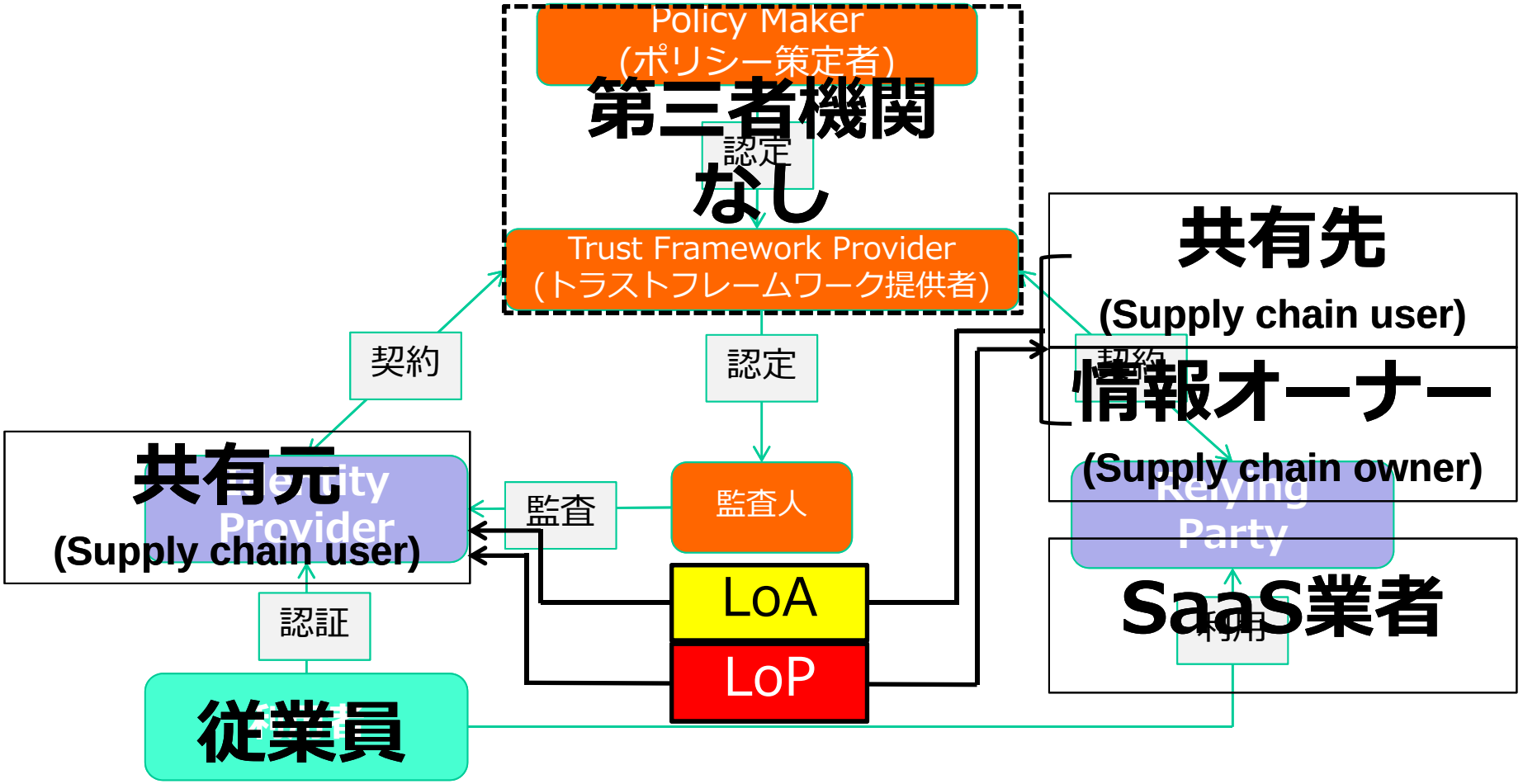
3. トラストフレームワーク
①基本モデル



3. トラストフレームワーク
②学認モデル



3. トラストフレームワーク
③エンタープライズ環境での現状



4. ポリシーを主張することでトラストを築く

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、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ました。

参考資料を参照ください。

(ポイント)

1.多額の投資や多くの運用負荷がかからないリーズナブルなレベル。

2.以下の規定を参考にした。

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

３．エンタープライズロール管理

１．ロール管理の成果　全体像（２０１３年度）

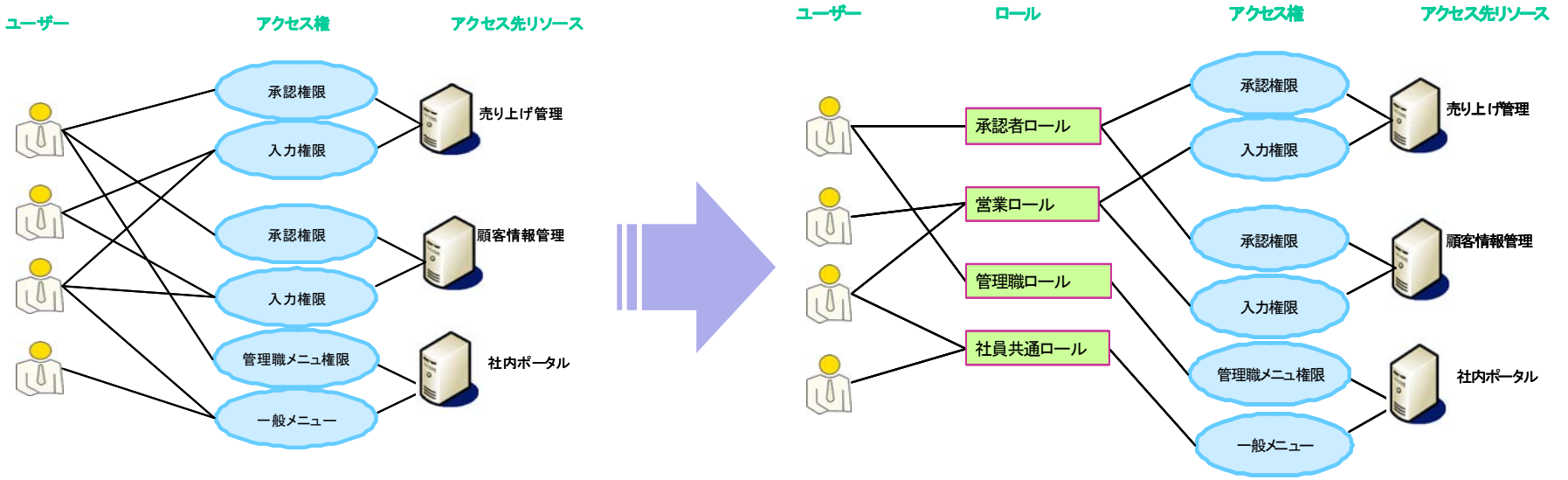
- 前年度の成果物として、
  「エンタープライズロール管理解説書
  （第1版）」を作成
  - http://www.jnsa.org/result/2013/std_idm.html

- 2013年度は、ケーススタディの章を追加

2．エンタープライズロール管理解説書　目次

3．ロール管理とは

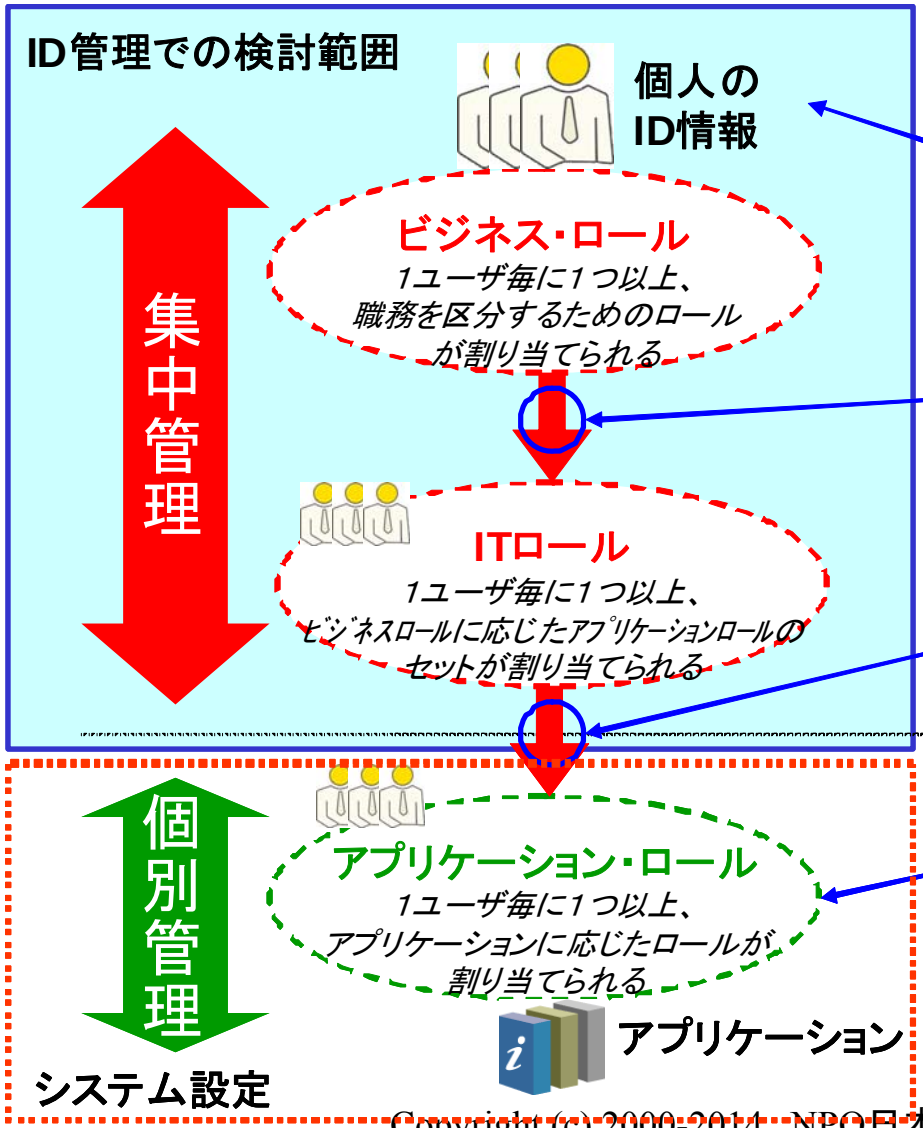
ロール管理により、
個別のユーザに対する個別のアクセス権の管理から、
ユーザ集合に対するアクセス権集合の管理へ



ロールが無い状態

ロールにより整理されている状態

4. ロールの分類とその関係



ID情報をアプリケーションに対し直接的に割り当てると、管理性や拡張性が失われるため、レイヤーを用いて管理する

ビジネスユーザはビジネス・ロールを持ち、ITロールまたはアプリケーションロールにマッピングされる。

ITユーザはITロールを持ち、ITロールはアプリケーション・ロールにマッピングされる。

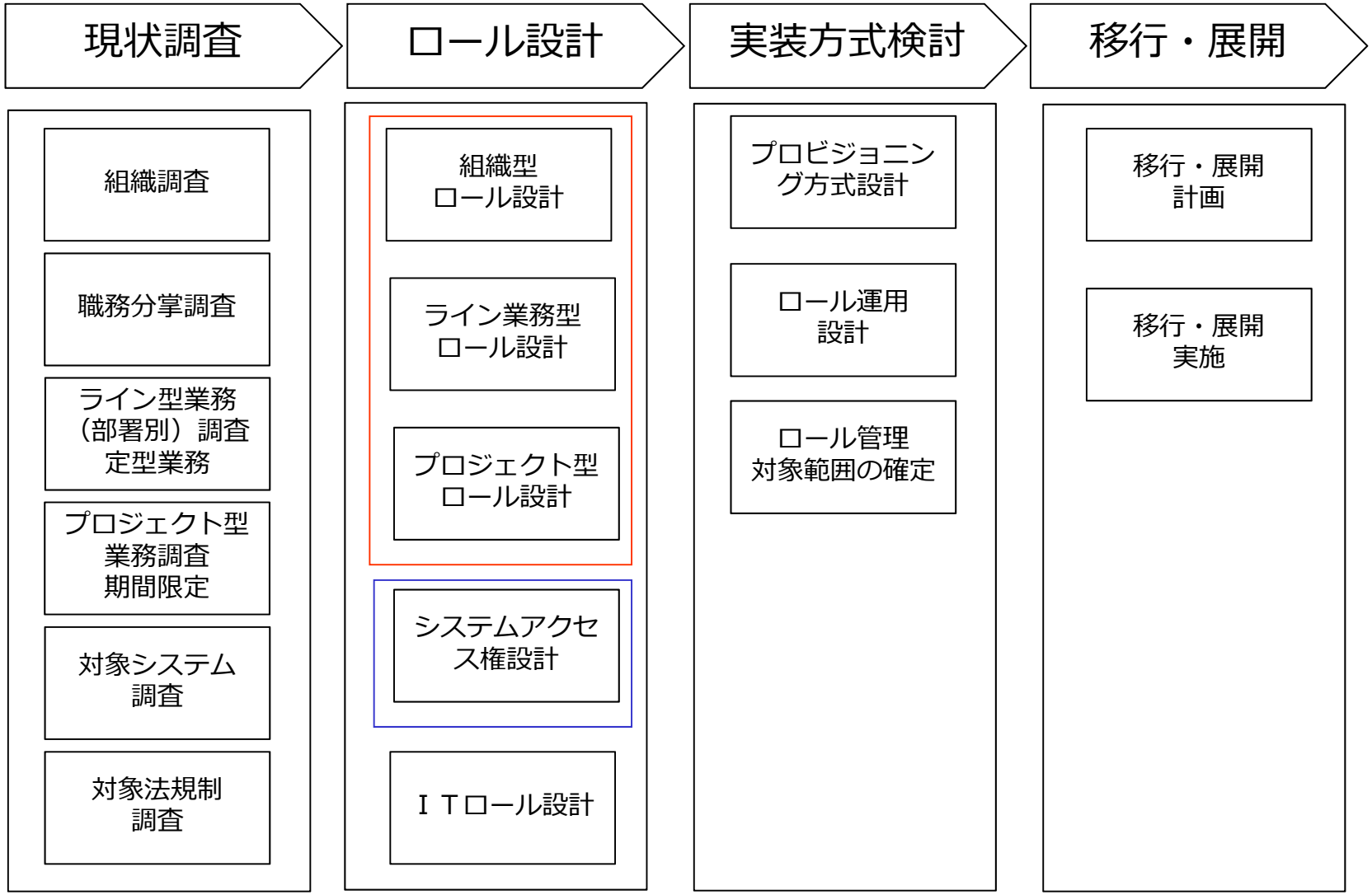
アプリケーション管理者はアプリケーション・ロールを定義し、それぞれのシステム権限にマッピングする。

5.【参考】３階層のロール間の関係例

アプリケーション・ロール

ビジネス・ロール			ITロール	認証		社内システム												
				認証基盤		ポータル					メール	社内電話帳	会議室予約	スケジュール	各種申請		管理メニュー
所属企業コード	分類	職制		パスワード初期化アカウントロック解除	パスワード変更	トップメニュー	管理職用メニュー	一般職用メニュー	出向者用メニュー	グループ企業用メニュー					申請	承認	
00:本社	一般	役員	R001	×	○	○	○	×	×	×	○	○	○	○	○	○	×
		管理職		×	○	○	○	×	×	×	○	○	○	○	○	○	×
		一般社員	R002	×	○	○	×	○	×	×	○	○	○	○	○	×	×
		出向者	R003	×	○	○	×	×	○	×	×	○	×	×	○	×	×
	システム部	運用管理者	R004	○	○	○	○	○	○	○	○	○	○	○	○	○	○
		ヘルプデスク	R005	○	○	○	○	○	○	○	○	○	○	○	○	○	×
01:グループ企業	スタッフ	管理スタッフ	R006	×	○	○	×	×	×	○	○	○	○	○	○	○	×
		一般スタッフ	R007	×	○	○	×	×	×	○	○	×	×	×	○	×	×
		受入出向者	R008	×	○	○	×	○	×	○	○	○	○	○	○	×	×
02.その他企業	その他	受入出向者	R009	×	○	○	×	○	×	×	○	○	○	○	○	×	×
		契約社員		×	○	○	×	○	×	×	○	○	○	○	○	×	×
		協力会社社員	R010	×	○	○	×	×	×	×	○	×	×	×	×	×	×
			ACL	ACL001	ACL002		ACL003	ACL004	ACL005	ACL006	ACL007	ACL008	ACL009		ACL010	ACL011	ACL012

6．ロール管理導入のプロセスとタスク



7. ロール管理ケーススタディーの目次

第4章　ロール管理の仮想企業導入事例

4.1. 金融業の仮想企業におけるロール管理導入事例

4.1.1. 金融業の仮想企業事例の全体像

4.1.2. 本事例でロール管理導入にあたり意識したポイント

4.1.3. 本事例のスコープ

4.1.4. 現状調査

4.1.5. ロール設計

- 対象組織は、カスタマ本部（コールセンタ部、ビジネスセンタ部）、営業本部、情報システム部に範囲を絞る。
- 対象情報システムは、ファイルサーバ、グループウェア、経費精算システム、コールセンタシステム、会員管理システム、営業管理システムに範囲を絞る。
- 導入過程のうち、現状調査およびロール設計までの部分を説明する。

8．仮想企業事例の全体像

JNSA

仮想企業の概要：

- ●クレジットカード会社「Jカード」
- ●顧客の個人情報／決済情報を取り扱っている
- ●従業員数：3,000人、うち非正規社員：1,000人（コールセンタ等）
- ●IT運用者が50人

ID/アクセス管理およびロール管理の課題：

- ●非正規社員の管理が適正に実施できていない
- ●ID／アクセス管理プロセスの標準化ができておらず、
  管理作業がすべて手作業で運用工数が増大、属人的な管理になっている
- ●特権ID（システム管理者）の管理が適正に実施できていない
- ●ロール定義が存在せず、管理基準や判断ルールが不明確になっている

課題を解決するために、ERP上で定義された「職責」をベースに、
ロール定義およびロール管理システム導入の検討に取り掛かった

９．【参考】事例企業がロール管理導入にあたり意識した点

- 管理プロセス・基準のルール化
- PCIDSSなどの基準への対応
- 「職務分掌」
- 「監査」の観点
- 特権IDの管理
  - ✓IT運用管理者、ITベンダ
  - ✓「共有ID」、「メンテナンスID」(保守・開発用等)
  - ✓「一時ID」
- 「ロールメンテナンス運用」のし易さを考慮
- 「兼務」、「引き継ぎ期間」など、日本特有の要件
- 「例外（個別設定）」

詳細は「エンタープライズロール管理（第2版）」を参照ください

４．今年度のテーマ

今年度のテーマ（案）

１．ロールマネジメントの検討（継続テーマ）
　　成果物改定
２．特権IDの検討（継続テーマ）
３．書籍改定作業（第２版）
４．アイデンティティとプライバシー勉強会
５．各種セミナー協力、他団体活動協力
６．その他テーマ

＊現在、新規メンバー募集中！　６／１３（金）まで！

ＪＮＳＡ事務局まで！

WGメンバー紹介

	氏名	所属
1	宮川　晃一	日本ビジネスシステムズ(株)
2	木村　慎吾	(株)インテック
3	川田　晋嗣	セコムトラストシステムズ(株)
4	齋藤　雅浩	富士通(株)
5	南　芳明	(株)シマンテック
6	貞弘　崇行	JBSソリューションズ(株)(日本ビジネスシステムズ(株))
7	大竹　章裕	(株)ネットマークス
8	富士榮　尚寛	伊藤忠テクノソリューションズ(株)
9	恵美　玲央奈	(株)富士通ソーシアルサイエンスラボラトリ
10	篠原　信之	(株)シグマクシス
11	宮島 秀彰	富士ゼロックス情報システム(株)
12	今堀　秀史	富士通関西中部ネットテック(株)
13	福原 幸一	富士通関西中部ネットテック(株)
14	小林 智恵子	東芝ソリューション(株)
15	山田　達司	(株)NTTデータ
16	中島 浩光	(株)マインド・トゥー・アクション
17	江川　淳一	エクスジェン・ネットワークス(株)
18	稲吉　英宗	伊藤忠テクノソリューションズ(株)
19	栃沢 直樹	トレンドマイクロ(株)

	氏名	所属
20	長内　仁	NTT ソフトウェア(株)
21	安納 順一	日本マイクロソフト(株)
22	邦本　理夫	(株)日立システムズ
23	塩田　英二	TIS(株)
24	酒井美香	日本IBMシステムズ・エンジニアリング(株)
25	桑田　雅彦	日本電気(株)
26	淺海 美哉	ソニー(株)
27	佐藤公理	マカフィー(株)
28	岩田　洋一	富士通(株)
29	岩渕 琢磨	情報セキュリティ大学院大学(学生)
30	西中 芳幸	インタセクト・コミュニケーションズ(株)
31	新嘉喜　康治	伊藤忠テクノソリューションズ(株)
32	後藤厚宏	情報セキュリティ大学院大学(教授)
33	後藤 兼太	日本電気(株)
34	杉村 耕司	(株)NTTデータ
35	中林 聖裕	(株)ディアイティ
36	森田 陽一郎	日本電気(株)

計３６名（順不同）

書籍の紹介

書籍名：<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

出版社：インプレスR&D NextPublishing

形態：電子書籍、Ondemand Print(POD)

販売： Amazon
　　インプレスR&D libura PRO

http://www.amazon.co.jp/dp/4844395866

ご参考資料

トラストを主張できるポリシー案

①ID体系の定義

〔ID管理対象者の明確化〕

(例)ID情報マスターDBで管理しているID管理の対象者は①正社員、
②非正社員、③ゲストアカウントです。

〔ユニークIDによる管理〕

(例)各ユーザに一意のIDを割り当てています。

②パスワードポリシー

〔パスワードポリシーの説明〕

(例)パスワードポリシーは以下の通りです。

・IDと同一のパスワード、生年月日、password、会社電話番号等、自分の車のナンバー等の推測されやすいパスワードは利用しない

・数字と英字混在し7文字以上であること

・ユーザが新しいパスワードを設定する時に最後に使用した４つのパスワードと同じものは使用できないetc.

〔定期的なパスワード変更〕

(例)長期にわたって同じパスワードを使用し続けないよう、３か月ごとに変更する運用を行っています。

〔初期パスワードの変更〕

(例)初期パスワードはユーザ毎に一意の値に設定し、初回使用後に直ちに変更する運用を行っています。

〔パスワードリマインダーの運用〕

(例)パスワードリマインダーはユーザーが保持している携帯電話のメールアドレスに対してパスコードを送信する方式を併用しています。

③認証ポリシー

〔社内の認証システムの存在〕

(例)社内の各アプリケーションの認証はアプリケーションが保持するID情報DBでのローカル認証方式やLDAP、Active DirectoryのID情報DBでの外部認証方式を利用しています。

(例)社内の各アプリケーションの認証はシングルサインオンシステムを利用してセキュアかつ効率的に行われています。

〔フェデレーション技術の存在〕

(例)クラウドサービスを利用する場合、フェデレーション技術を利用します。

(例)SAMLのIdPとOpenID ConnectのOPのしくみを保持しています。

〔多要素認証システムの存在〕

(例)IDの不正使用防止の本人特定の方法として、アプリケーションによってはパスワードによる認証だけではなく、ワンタイムパスワードによる多要素認証を行っています。

③認証ポリシー

〔パスワードの有効性の維持〕

(例)システムやデータへのアクセス権を不正利用されないように各アプリケーションの認証システムでは以下の機能を実装しています。

①ログオン中のタイムアウト
②ユーザーにログオン履歴情報の提供
③パスワード入力失敗回数制限
④エラーメッセージからのパスワード推測防止
etc.

④アクセス制御ポリシー

〔アクセス制御システムの存在〕

(例)アクセス制御はID情報マスターDBのユーザ情報や組織情報等をベースにロール情報と紐付けされ、適切に管理され、各アプリケーションのアクセス制御システムで実装しています。

〔アクセス権限の見直しタイミング(通常運用外)〕

(例)人事異動や組織変更以外にも以下の状況でアクセス権限の変更を行っています。

①長期出張、長期留学、長期休暇

②新システム稼働時

⑤IDライフサイクル管理ポリシー

〔IDライフサイクル管理の存在〕

(例)ID管理の対象者毎に、適切なIDの登録、変更、削除に関する依頼手続及びメンテナンス手続きを行っています。

〔ID管理責任者とID管理担当者の役割分担〕

(例)ID管理責任者とID管理担当者を明確化し、それぞれに対してID管理システムでの適切なオペレーション権限を付与しています。

〔ID情報の鮮度を保つしくみの存在〕

(例)人事異動や組織変更の情報が、迅速かつ適時、ID情報DBに反映できるIDライフサイクル管理とプロビジョニングのしくみを保持し、ID情報は常に最新の情報に更新されています。

⑤IDライフサイクル管理ポリシー(正社員)

〔Authoritative Sourceの存在〕

(例)正社員のID情報、組織情報は人事情報DBをAuthoritative Sourceとしています。

〔ID管理システムによるメンテナンス内容〕

(例)システム部署のID管理担当者は、人事異動や組織変更の内容を、ID管理システムを利用して、ID情報マスターDBに対して、CSVファイルで反映します。

〔ID管理責任者の確認作業〕

(例)システム部署のID管理責任者は上記のCSVファイルの内容に関して適切かどうか、メンテナンスが行われる前に確認しています。

〔特に厳格に実施されている無効化処理〕

(例)退職に伴うID情報の無効化処理や組織変更に伴う該当グループ情報からのメンバー削除処理は特に厳格、適切に行っています。

〔特に厳格に実施されている無効化処理～棚卸処理〕

(例)削除されるべきID情報やメンバー情報が残存していないことを確認するため棚卸処理を3か月毎に行っています。

⑤IDライフサイクル管理ポリシー(非正社員)

〔管理手続きの存在〕

(例)非正社員のID情報は、受け入れる部署の業務アシスタントが、ワークフローシステムを利用して、登録、変更申請処理を行い、受け入れる部署の業務責任者が最終承認/否認処理を行います。

〔ID管理シテムによるメンテナンス内容〕

(例)システム部署のID管理担当者は、最終承認された登録、変更情報をID管理システムを利用して、ID情報マスターDBに対して、CSVファイルで反映します。

〔ID管理責任者の確認作業〕

(例)システム部署のID管理責任者は上記のCSVファイルの内容に関して適切かどうか、メンテナンスが行われる前に確認しています。

〔特に厳格に実施されている無効化処理〕〕

(例)無効化処理は登録時に設定される有効期限日をトリガーに自動的に行われます。

〔特に厳格に実施されている無効化処理～棚卸処理〕

(例)無効化されるべきID情報や削除されるべきメンバー情報が残存していないことを確認するため棚卸処理を3か月毎に行っています。

⑤IDライフサイクル管理ポリシー(ゲストアカウント)

〔管理手続きの存在〕

(例)ゲストアカウントのID情報は、訪問される部署の業務アシスタントが、ワークフローシステムを利用して、登録申請処理を行い、訪問される部署の業務責任者が最終承認/否認処理を行います。

〔ID管理シテムによるメンテナンス内容〕

(例)システム部署のID管理担当者は、最終承認された登録情報をID管理システムを利用して、ID情報マスターDBに対して、CSVファイルで反映します。

〔ID管理責任者の確認作業〕

(例)システム部署のID管理責任者は上記のCSVファイルの内容に関して適切かどうか、メンテナンスが行われる前に確認しています。

〔特に厳格に実施されている無効化処理〕

(例)無効化処理はゲストが退社した時に受付業務担当者が行っています。

⑥プロビジョニングポリシー

〔ID管理シテムによるプロビジョニング〕

(例)ID情報マスターDBの情報はID管理システムにより、アプリケーションが保持するID情報DBや外部認証用のLDAP、Active DirectoryのID情報DBに適時、連携されています。

〔プロビジョニングポリシーの存在〕

(例)プロビジョニングにより連携されるID情報は、アプリケーション毎に必要最低限の情報であることがポリシーにより定義されています。

〔クラウドサービスに対するプロビジョニング〕

(例)フェデレーション技術を利用することで、クラウドサービスに対しては必要最低限の情報をプロビジョニングしています。

⑦引き渡し手続きポリシー

〔正当なIDの保持者であることの確認〕

(例)IDを保有者に引き渡す際に、本人であることについて厳重な確認作業を行っています。

(例)初回認証時(IDをActivateにする時)は、以下の方法で保有者が本人であることの再確認を行っています。

・通常の認証とは別な手段による認証（本人のみが知る情報など）の入力を必須にする

(例)ID利用申請を行う際に、本人が申請に必要な情報を正当に保有していることの確認を行っています。

〔本人の情報確認の補完〕

IDを保有者に引き渡す際に、本人であることの確認を補完する手段を有しています。(要求されるLoAのレベルにより必要な場合がある)

⑦引き渡し手続きポリシー

〔本人がIDの保有に対する意思を持っているかの確認〕

悪意のある第三者が申請やActivateを行い、本人の取得と同時に搾取し、行使をすることを回避します

(例)本人がID申請／保有を意図していない場合の否認表明手段を確保すると共にID失効手段を確保しています。

(例)ID発行時、本人の意思を確認します。

〔発行するIDと権限の定期的な棚卸〕

ID保有者の上長など、ID保有者以外による保有事実の確認と付与される権限範囲の確認を行っています。

(例)ID保有者の上長による棚卸（引き渡し時、運用開始後定期的に）

(例)ID保有者の上長に対する権限変更時の承認プロセス

(例)ID保有者の上長によるID失効手段の確保

⑦引き渡し手続きポリシー(エンプラ適用で考慮必要な内容)

〔正当なIDの保持者であることの確認〕
IDを保有者に引き渡す際の、本人であることの確からしさの設定

(例)ID引き渡す時は、以下の方法で行っています。(選択)
(1)メールによる通知
(2)郵送による通知
(3)自宅への郵送（本人限定郵便を含む）
(4)さらに異経路による通知の組み合わせ
(5)出頭、手交

(例)初回IDを認証時(Activateにする時)は、以下の方法で保有者が本人であることの再確認を行っています。
・通常の認証とは別な手段による認証（本人のみが知る情報など）の入力を必須にする

(例)本人が申請に必要な情報を正当に保有していることの確認を行っています。
・適切な第三者の認証情報に依存して、IDの発行／引き渡しを行う

〔本人がIDの保有に対する意思を持っているか〕
悪意のある第三者が申請を行い、本人の取得と同時に搾取し、行使をすることを回避する

(例)本人がID申請／保有を意図していない場合の否認表明手段を確保すると共にID失効手段を確保しています。
・本人が意思を表明することで、正式なID発行を行う手続き
・Activateする手続きを付加し、第三者による搾取を回避

⑦引き渡し手続きポリシー(エンプラ適用で考慮必要な内容)

〔本人の情報確認の補完〕
IDを保有者に引き渡す際に、本人であることの確認手段を補完することでIDの本人確認レベルを向上（LOAのレベルによっては必要）

(例) ID引き渡す時は、以下の方法で行っています。(選択)
(1)メールによる通知によるメールアドレスの確認
(2)郵送による事業所所在の確認
(3)自宅への郵送（本人限定郵便）による居住の確認（本人確認）
(4)出頭、手交による確認

(例)初回IDを認証時(Activateにする時)は、以下の方法で保有者が本人であることの再確認を行っています。
・通常の認証とは別な手段による認証（本人のみが知る情報など）の入力を必須にする

組織の中での上長の活用

トラスト･フレームワークにおける身元確認スキームの応用

⑧その他

〔新規クラウドサービスに対するLoP評価〕

(例)新規にクラウドサービスと連携する場合はクラウドサービスのSLAを確認して、クラウドサービス事業者の中で、ID情報が適切に管理されるか否かについて評価します。

〔新規システム追加時の設定変更規定〕

〔ログシステムの併用〕

(例)システムへのアクセス履歴を取得し、システムを監査証跡とし保持しています。また、アクセス記録を定期的にチェックし、不当なアクセスなのかどうかを調査していることをユーザに周知しています。

〔特権ID管理システムの併用〕

(例)特権ユーザIDに関するアクセス権が、職務の実行に必要な最小限の特権に制限されています。

〔定期的な監査の併用〕

〔個人情報保護法への対応〕

〔リモートアクセスの制御〕