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

2012年度 アイデンティティ管理WG
成果報告

＜標準化部会＞
日本ビジネスシステムズ株式会社
宮川　晃一

2013年 6 月 7日

WG活動報告内容

1．ID管理におけるトラストフレームワークの
　　エンタープライズにおける活用

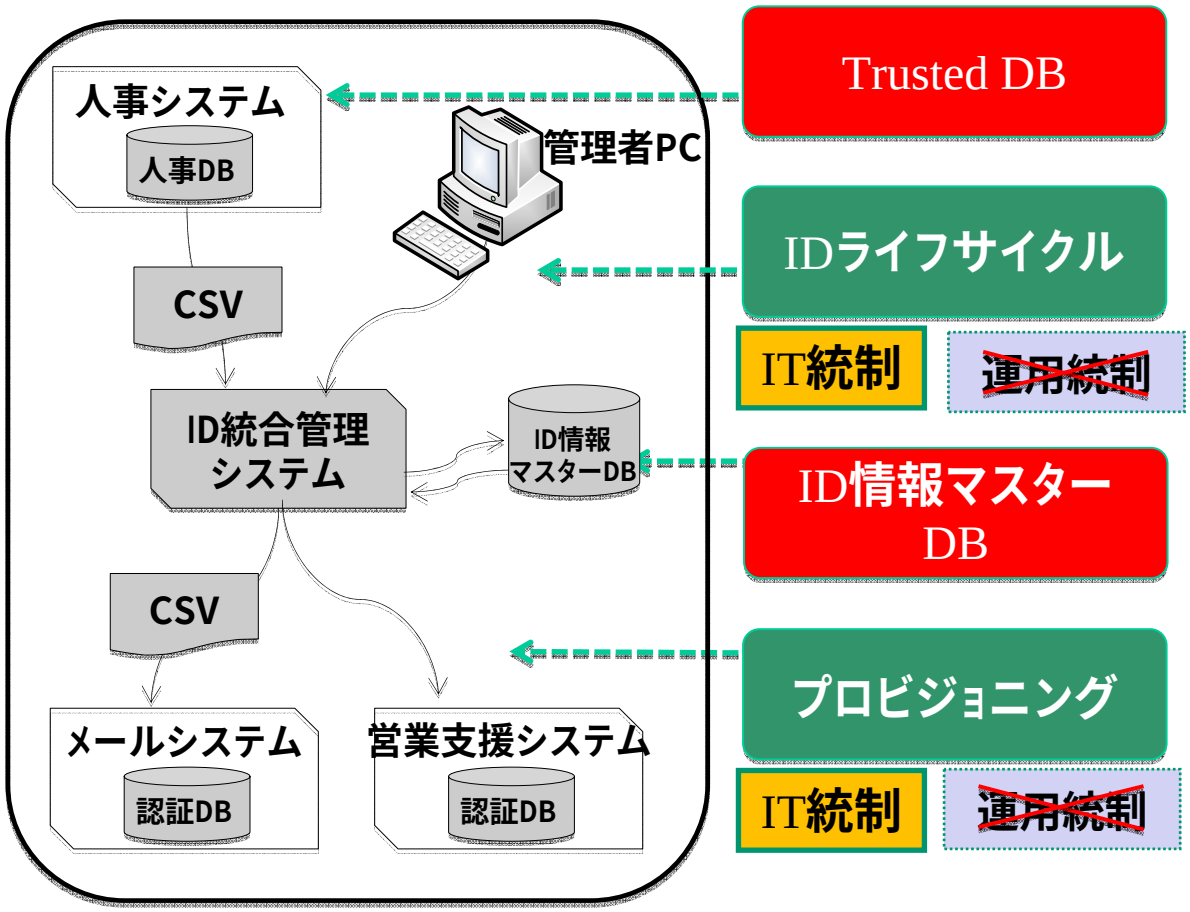
2．エンタープライズロール管理

3．＜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

4．今年度のテーマについて

１．ID管理における
トラストフレームワークの
エンタープライズにおける活用

1-1. 認証基盤　システム構成



1-2. IDライフサイクル管理のポイント

①発行＝間違いなく本人にIDを発行する

(運用例)
社員証を確認して、ID通知書を手渡しする。

身元保証

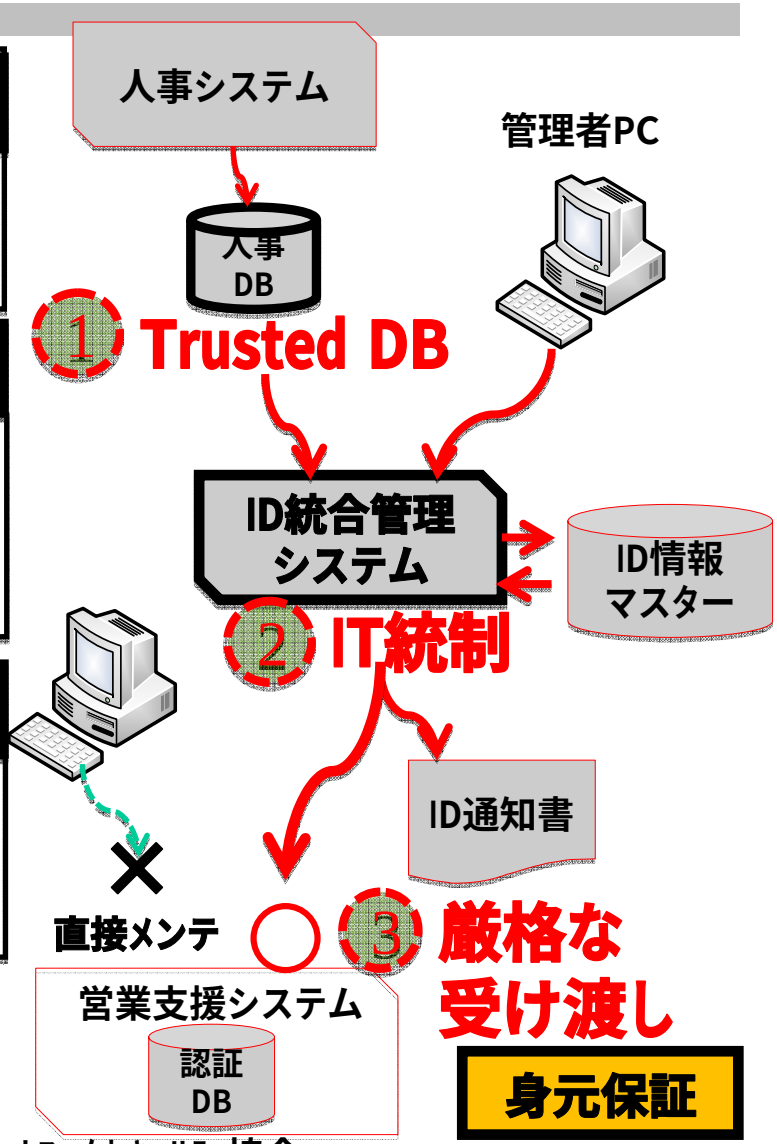
②利用＝IDを利用しているのは間違いなく本人

(運用例)
パスワード有効期限～定期変更。
ID有効期限設定～更新処理。ログ参照。

身元保証

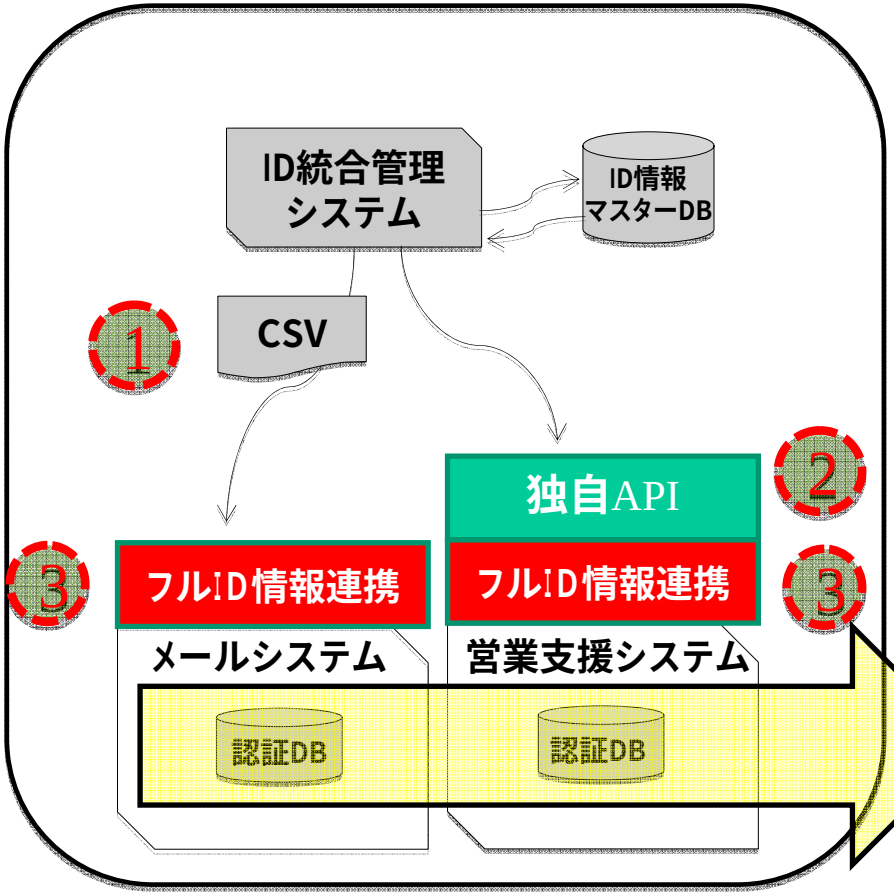
③削除＝迅速かつ漏れなくIDを削除する

(運用例)
源泉DB有りのID情報→自動連携
源泉DBなしのID情報→有効期限



1-2. IDライフサイクル管理のポイント

1-3. プロビジョニングの特徴～Classic認証基盤の場合

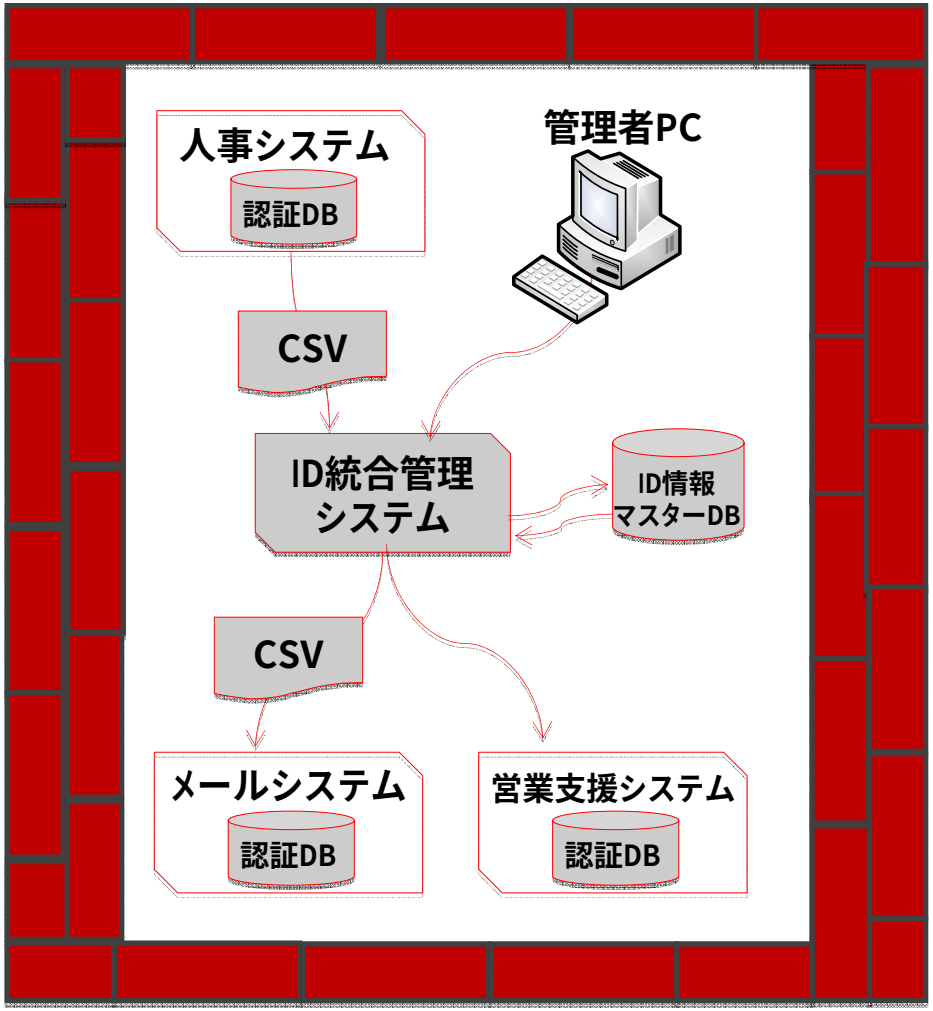


Classic認証基盤での プロビジョニングの特徴

1. CSV連携
2. 独自API連携
3. フルID情報連携

ローカル認証

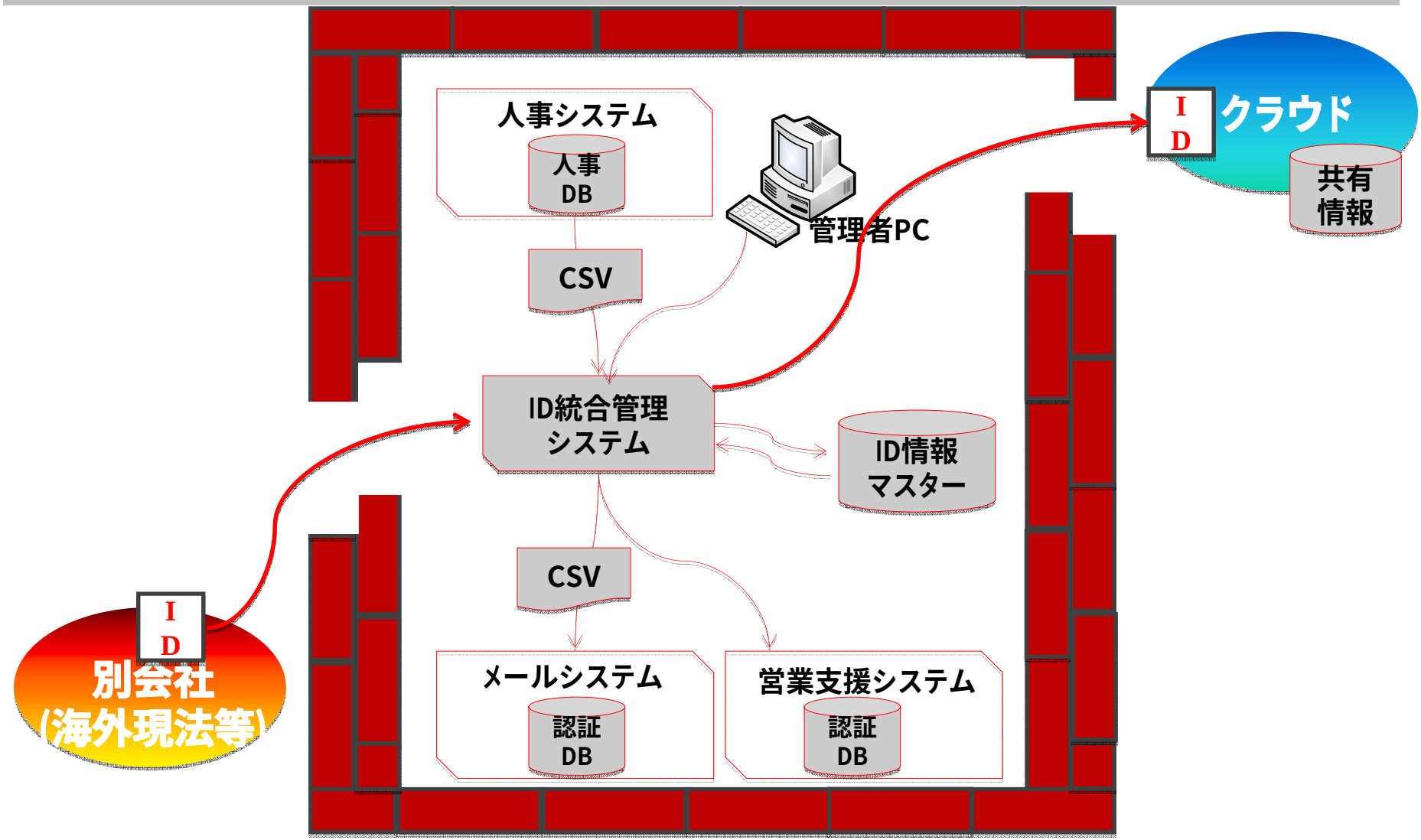
1-4. ITリソースのボーダレス化



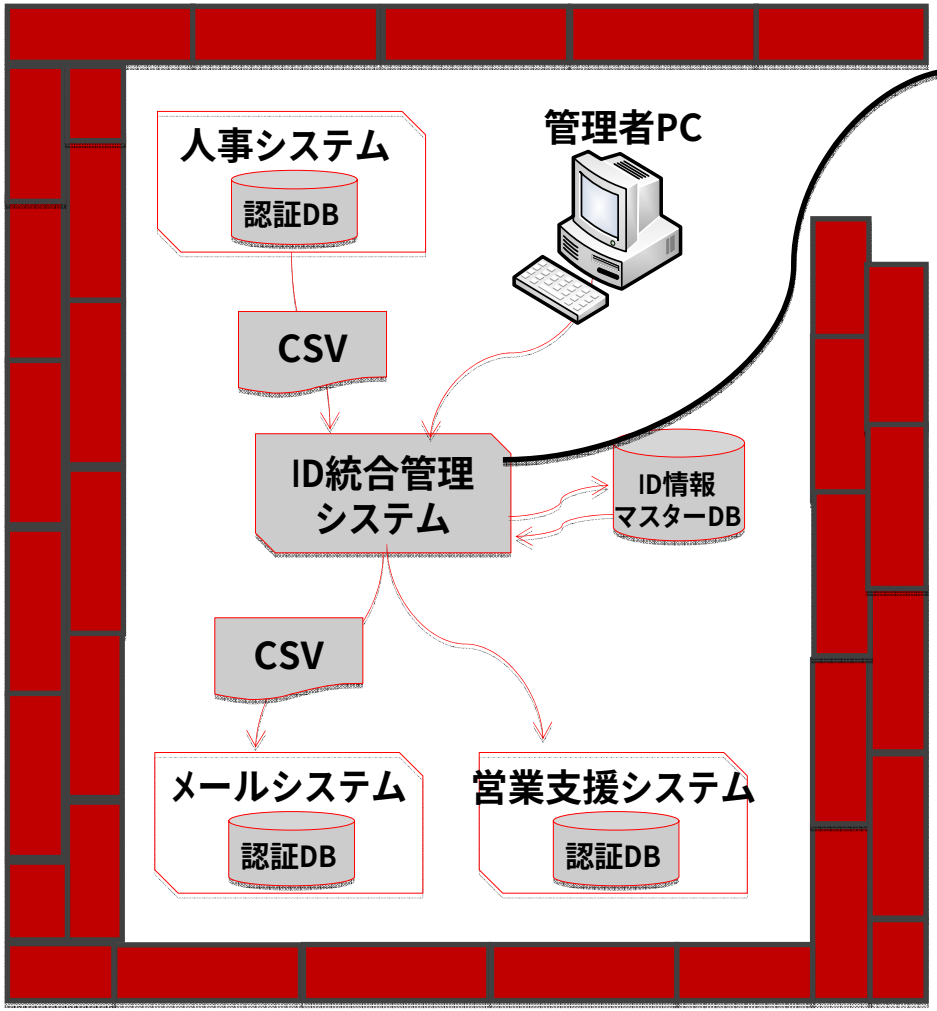
クラウド

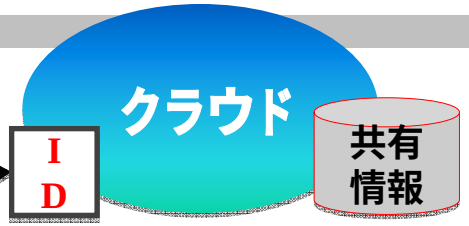
別会社
(海外現法等)

1-4. ITリソースのボーダレス化



1-5. クラウドサービス利用時の不安



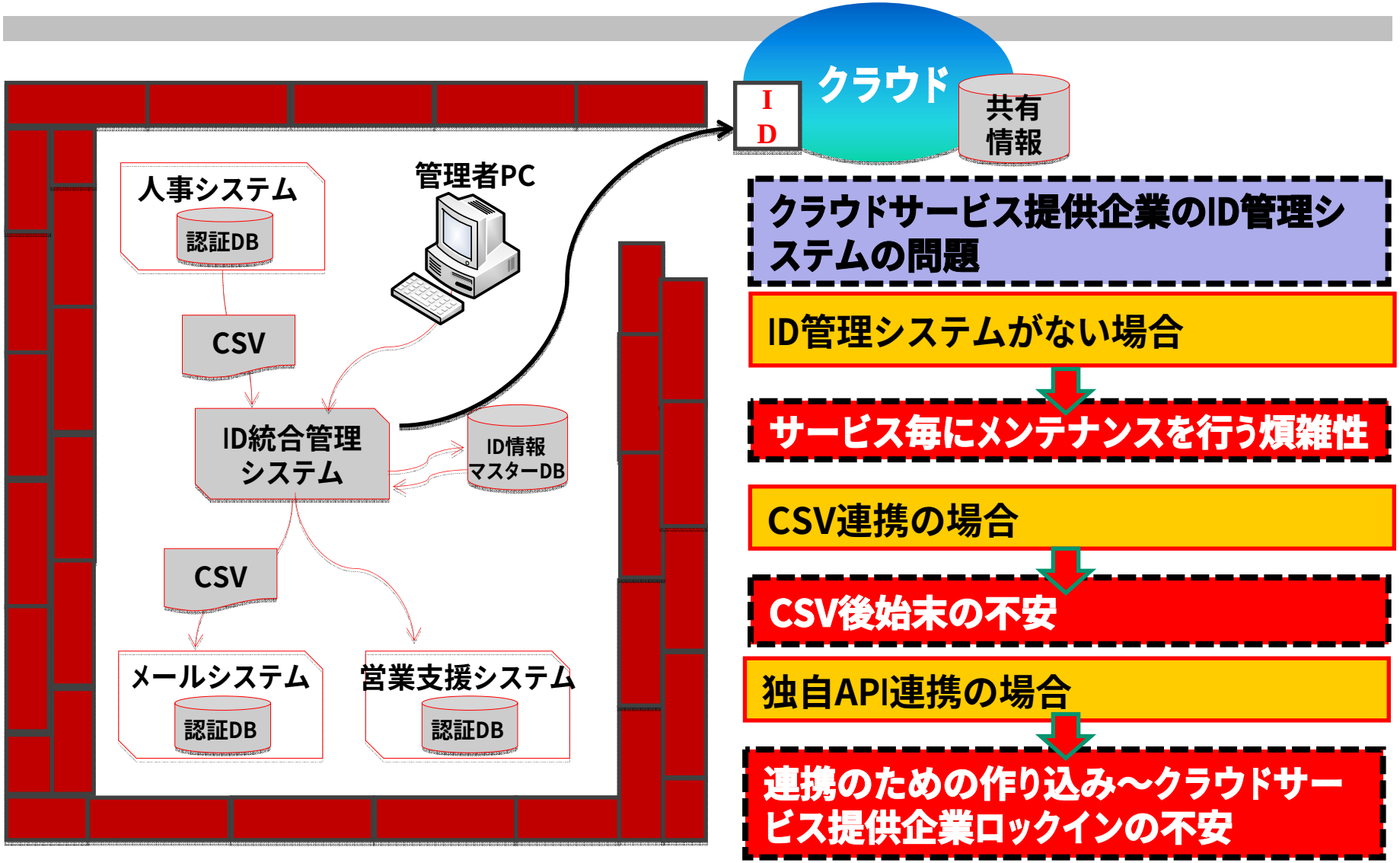


クラウドサービス提供企業にフルID情報(Credential含む)を預ける

- 情報セキュリティマネージメントの外部組織依存による統制(コントロール)の限界
- クラウドサービス提供企業のサービスレベル説明 (透明性)が欠如している場合がある
- クラウドサービス提供企業の技術の脆弱性の把握や客観的な検証が困難な点
- クラウドサービス提供企業のコスト削減に伴う情報管理の品質低下懸念

クラウドサービス提供企業からID情報(Credential含む)が漏洩することの不安

1-5. クラウドサービス利用時の不安



クラウドサービス提供企業のID管理システムの問題

ID管理システムがない場合

サービス毎にメンテナンスを行う煩雑性

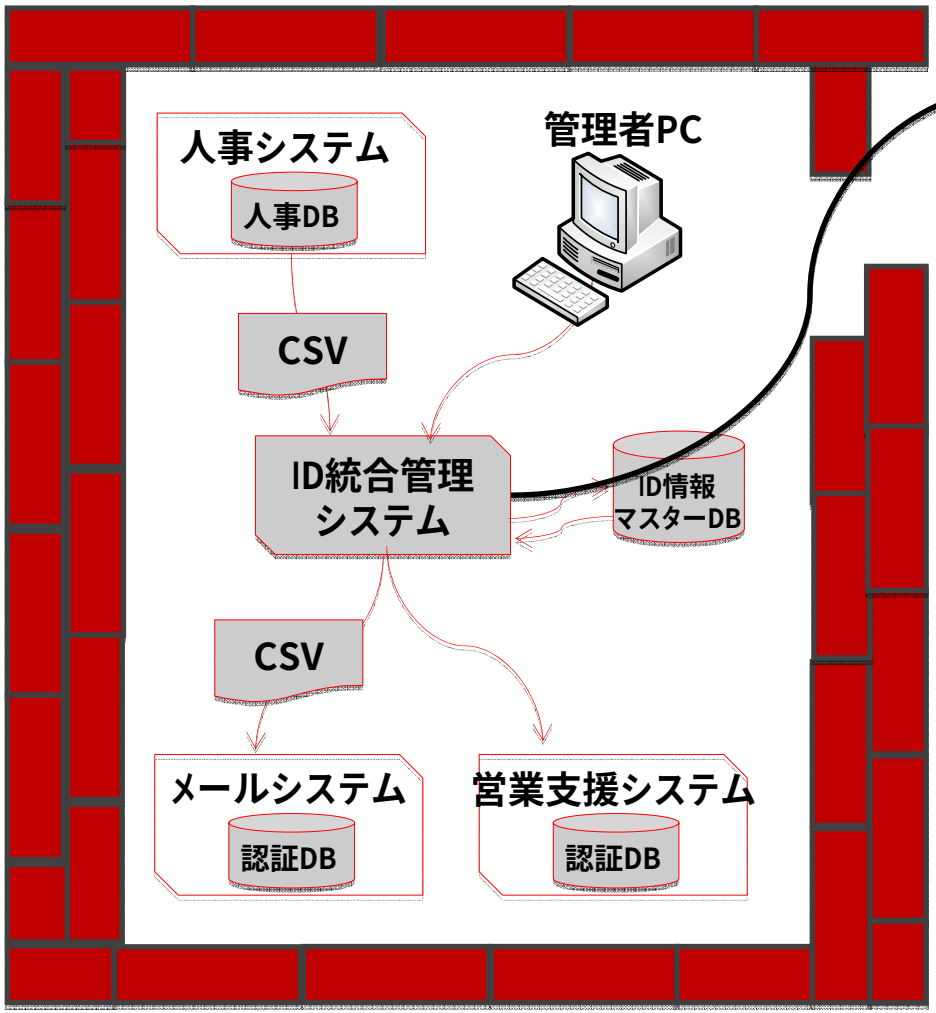
CSV連携の場合

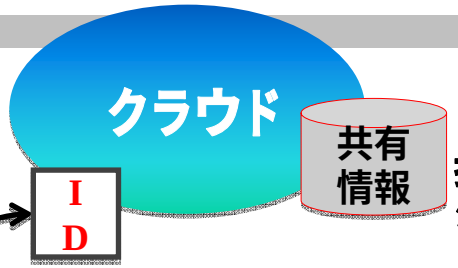
CSV後始末の不安

独自API連携の場合

連携のための作り込み～クラウドサービス提供企業ロックインの不安

1-6. 取引先との情報共有時の不安





＊クラウドサービス提供企業にID管理システムがあると仮定

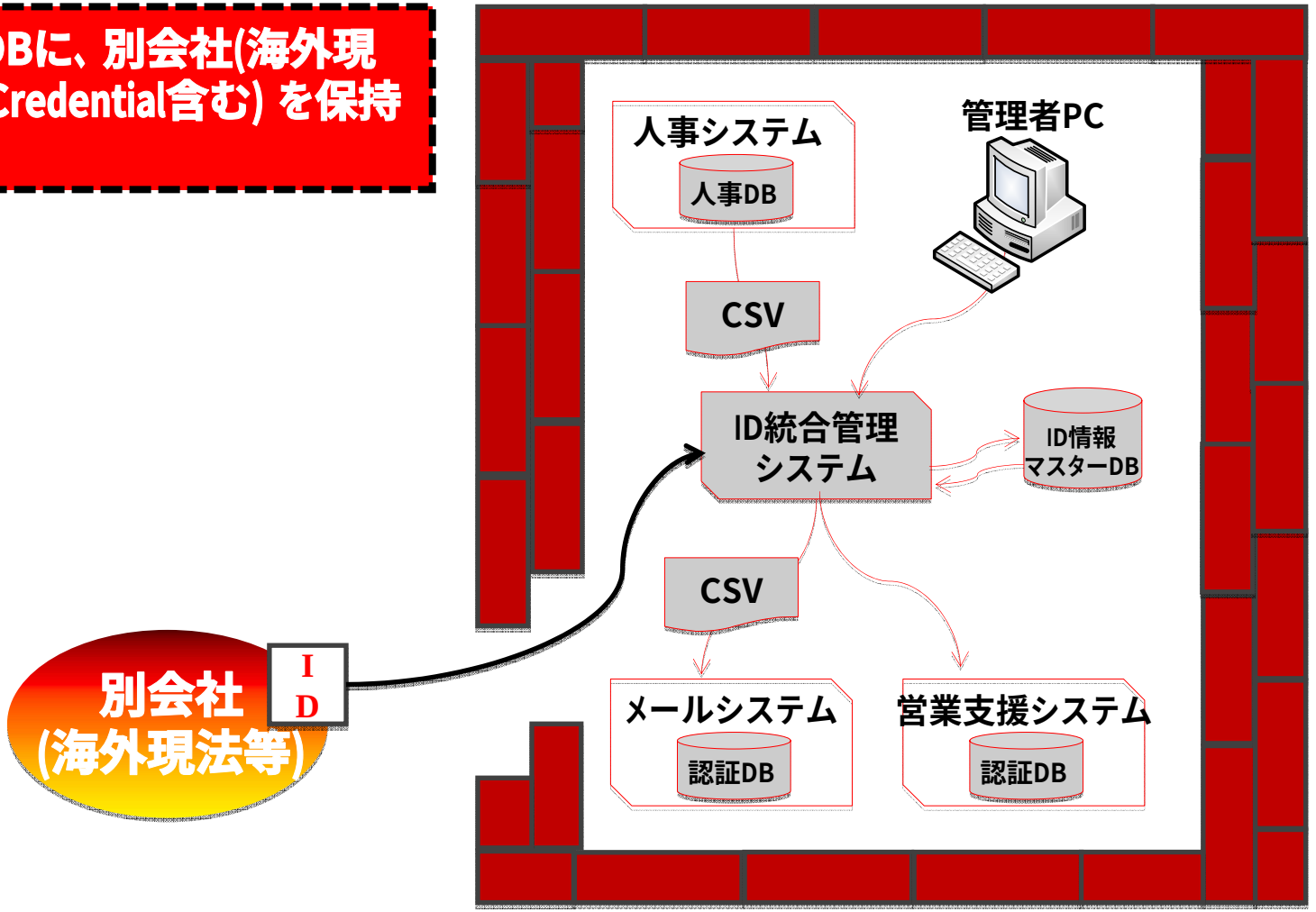
情報(機密情報含む)を共有する企業と認証･認可ルールを共有する

情報を共有する企業で運用ルールが異なる。ID情報ライフサイクル管理(特にTrusted DBの存在と、ID情報の厳格な受け渡し)が適切に行われていない企業が存在する可能性あり

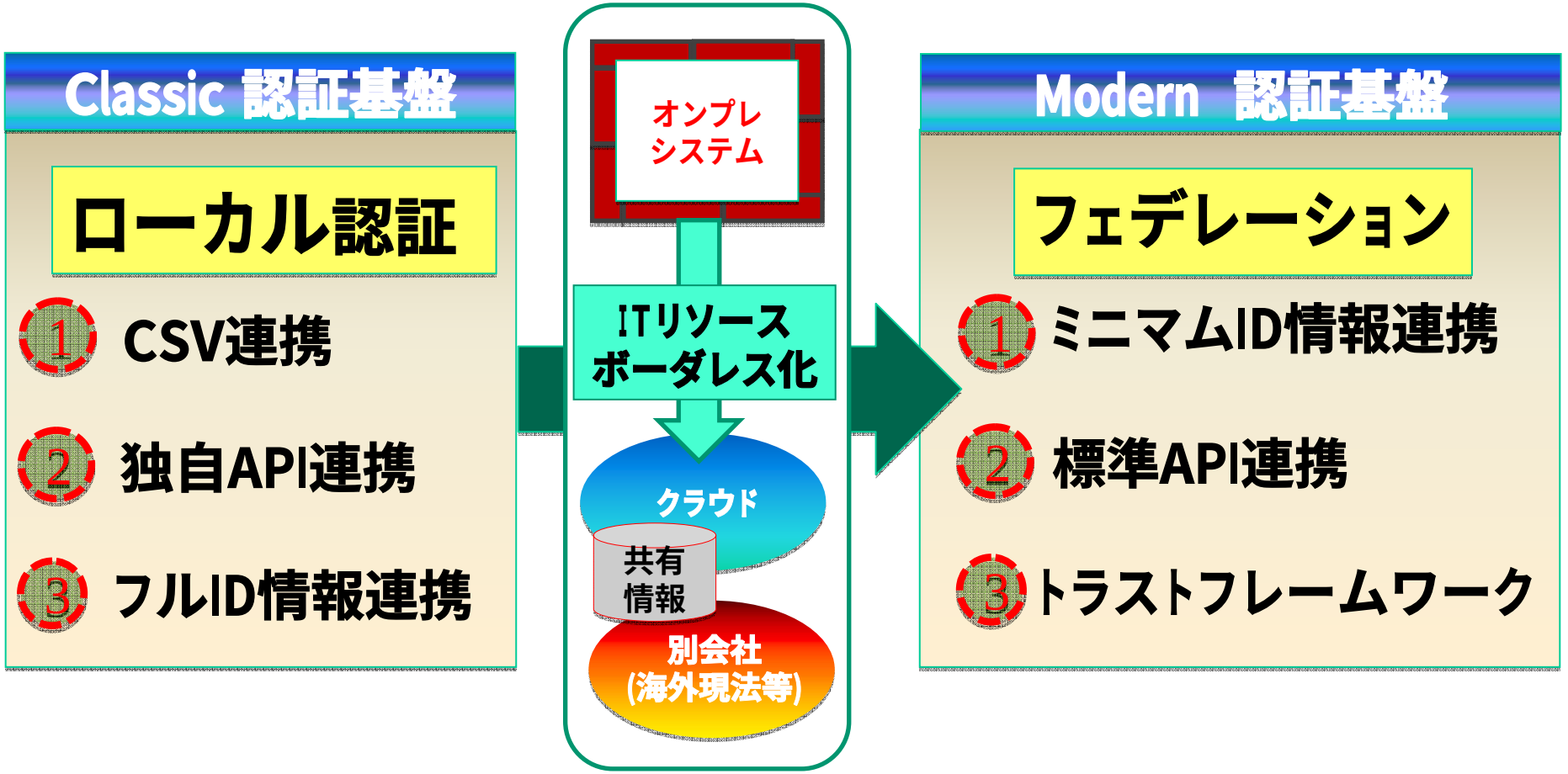
ID情報ライフサイクル管理が適切に実施されていない企業から、共有情報(機密情報含む)が漏洩することの不安

1-7. 別会社への情報公開時の不安

ID情報マスターDBに、別会社(海外現法等)のID情報(Credential含む) を保持することのリスク



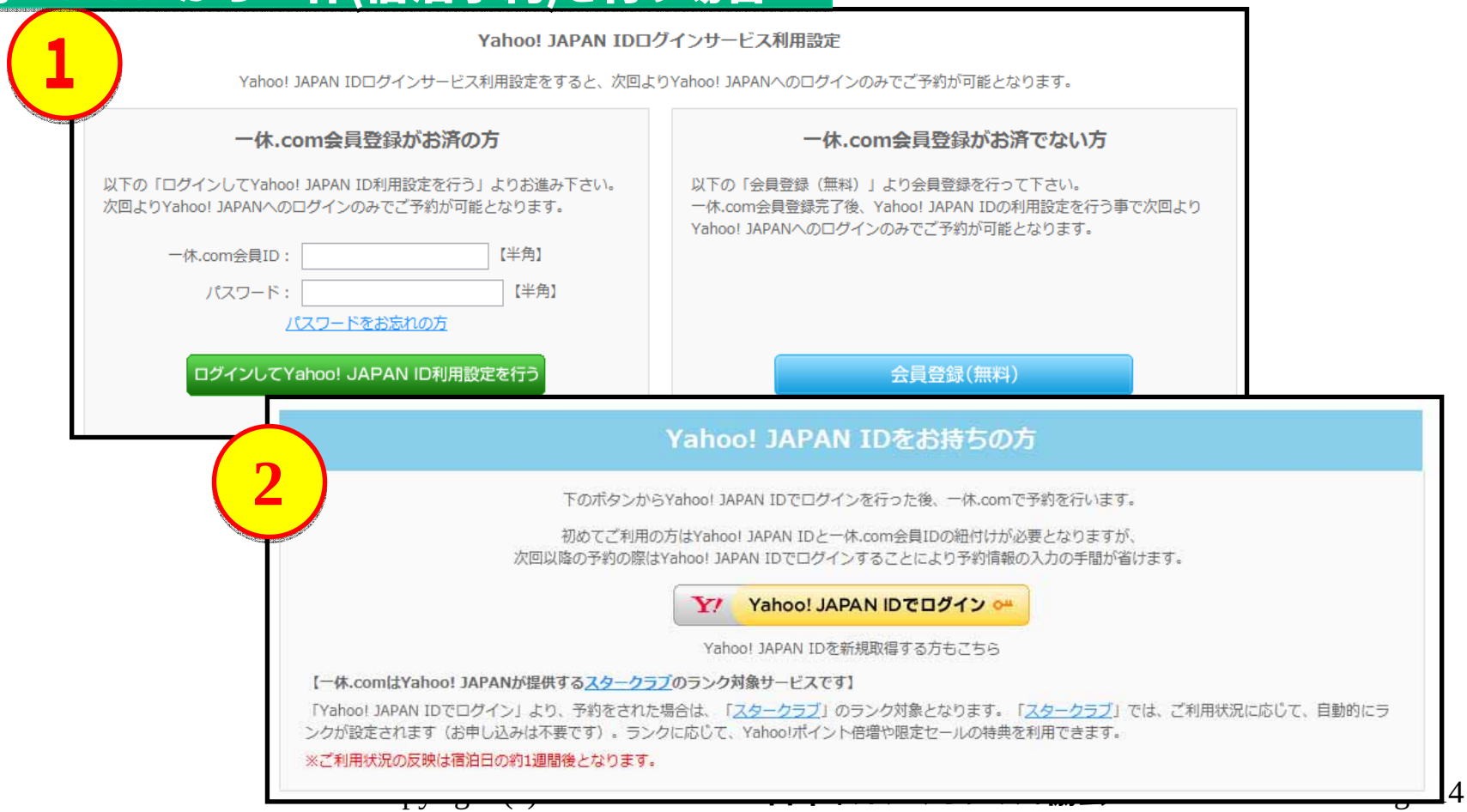
1-8. Classic認証基盤からModern認証基盤へ



1-9. フェデレーションのエンタープライズ利用

コンシューマ市場でのフェデレーション利用例

例：Yahoo! から一休(宿泊予約)を行う場合



1-9. フェデレーションのエンタープライズ利用

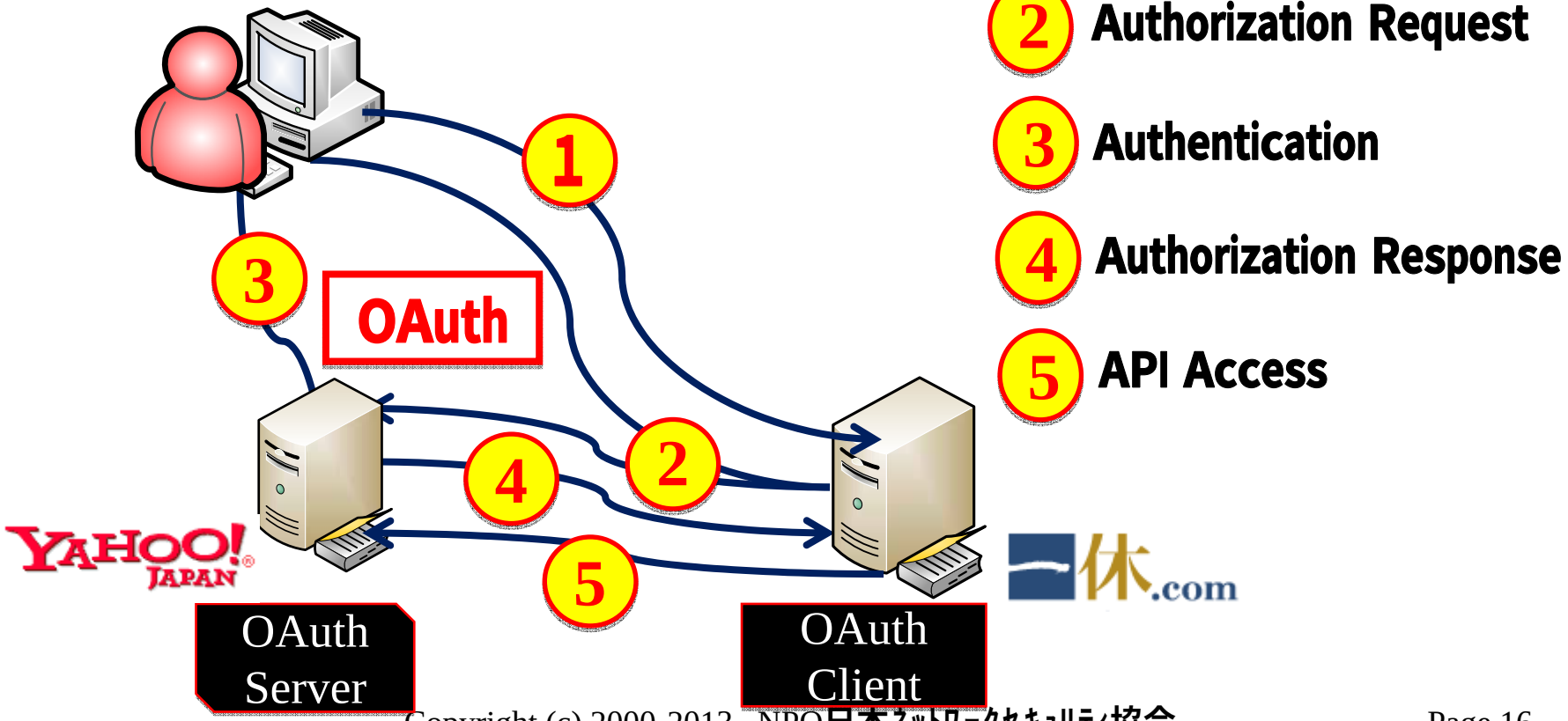
コンシューマ市場でのフェデレーション利用例

例：Yahoo! から一休(宿泊予約)を行う場合

1-10. フェデレーションのエンタープライズ利用

コンシューマ市場でのフェデレーション利用例

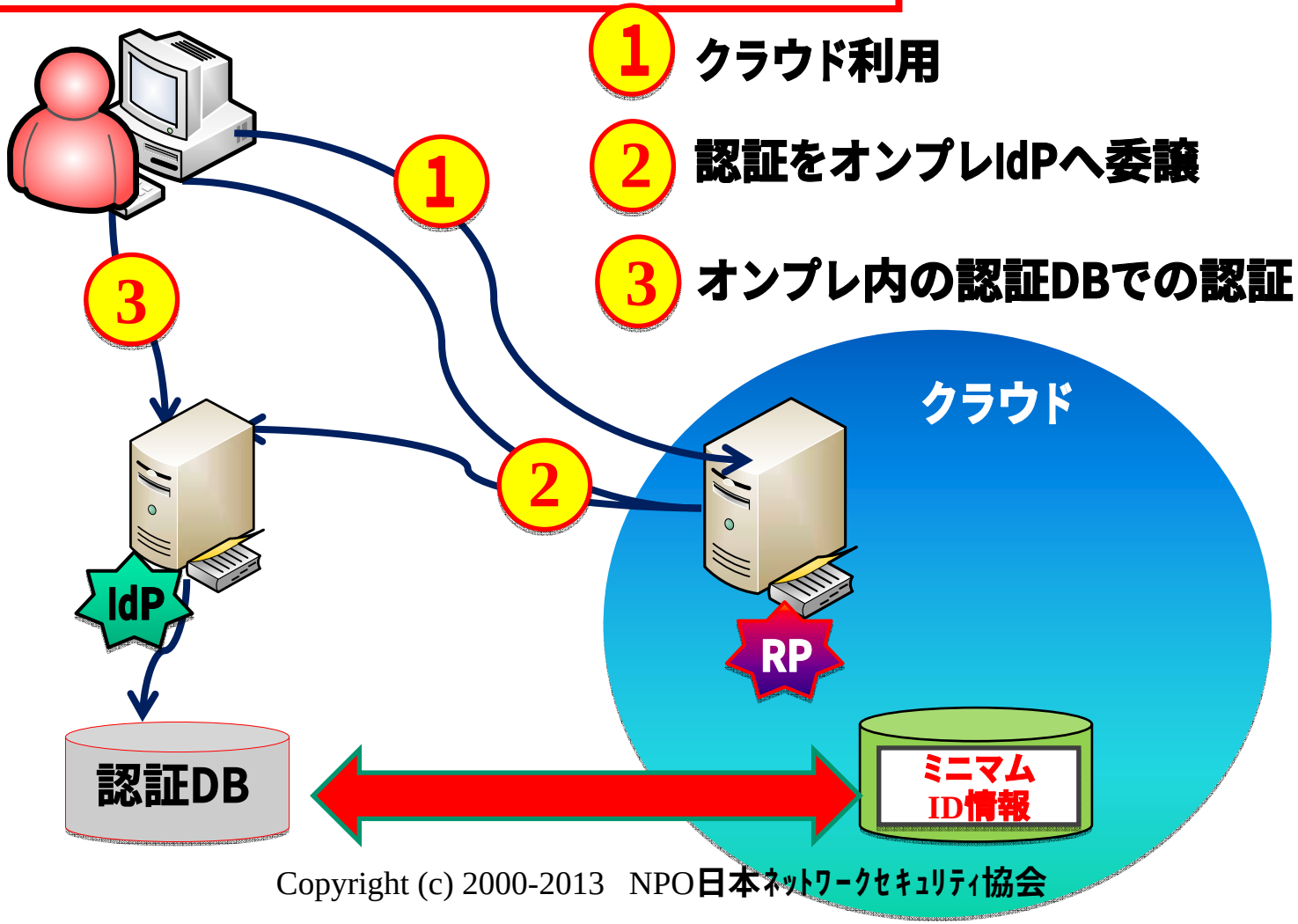
APIベースの認可情報委譲による
シングル・サインオン



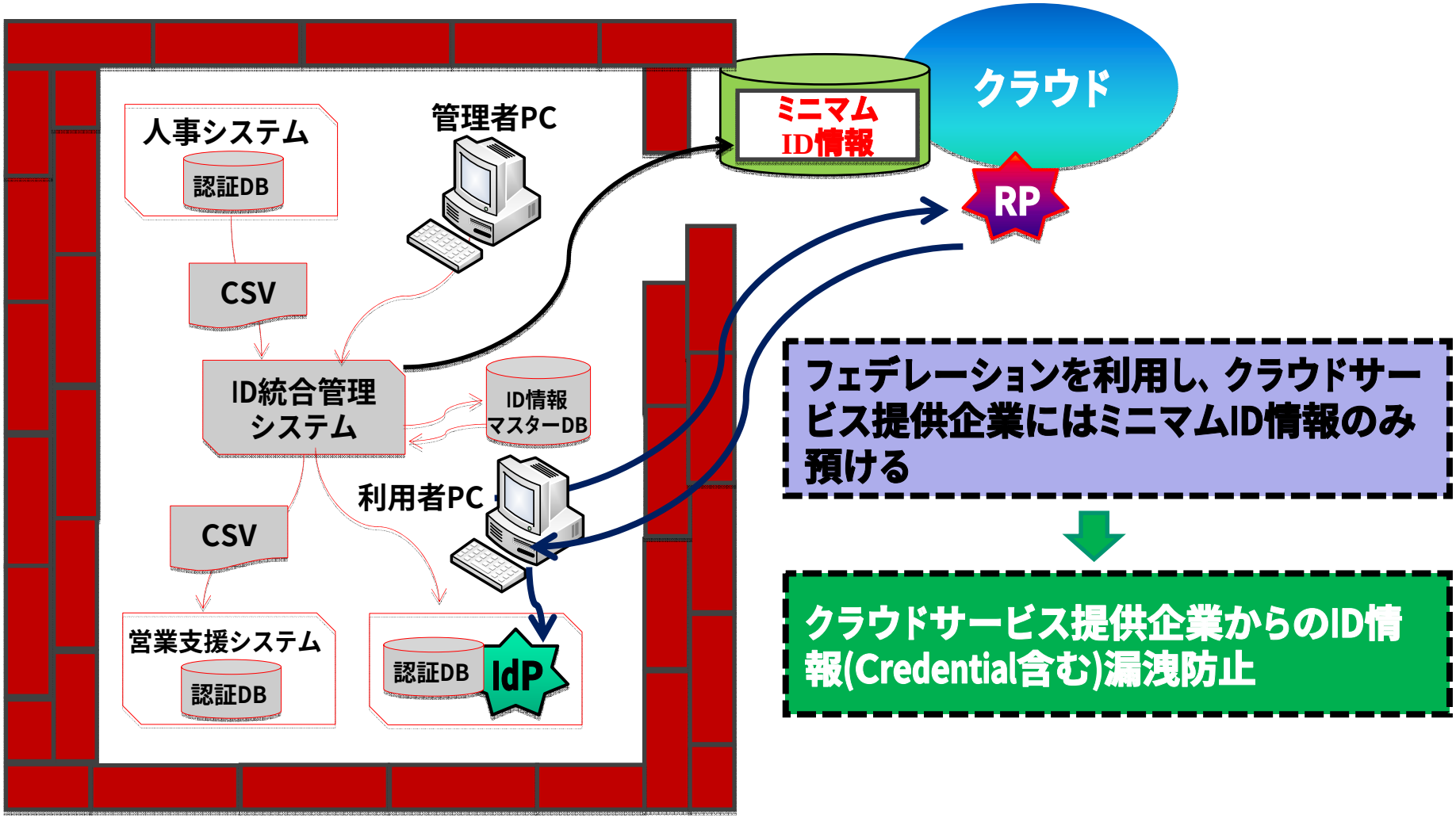
1. Initiate
2. Authorization Request
3. Authentication
4. Authorization Response
5. API Access

1-10. フェデレーションのエンタープライズ利用

エンタープライズ市場でのフェデレーション利用



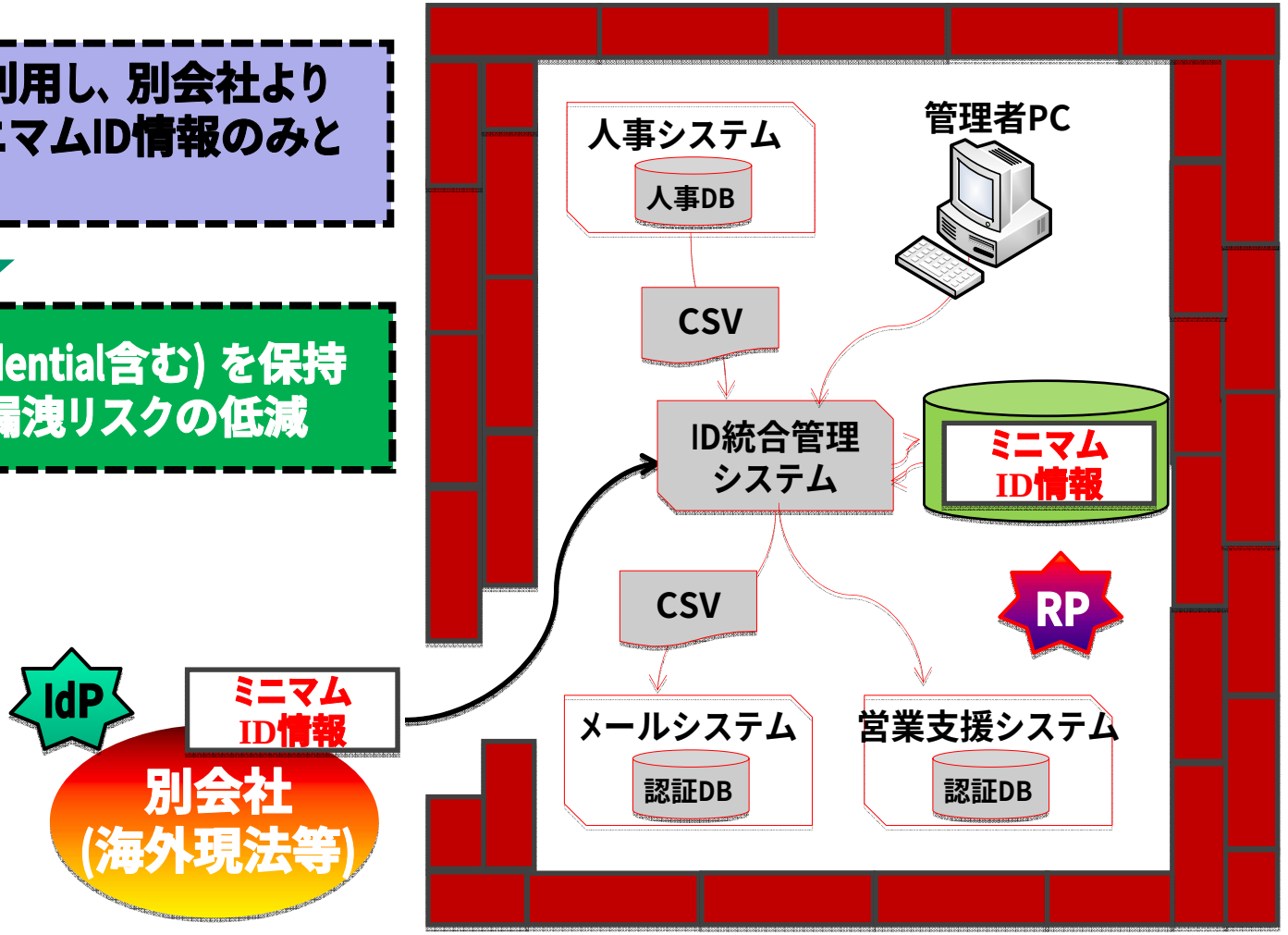
1-11. ミニマムID情報連携



1-11. ミニマムID情報連携

フェデレーションを利用し、別会社より預かるID情報はミニマムID情報のみとする

他社のID情報(Credential含む) を保持した状況での情報漏洩リスクの低減



1-12. 標準化API連携

標準化API連携のメリット

エンタープライズクラウド利用の場合プロビジョニングが必要なサービスは多い。

↓

プロビジョニングとフェデレーション併用による属性プロバイディング。

↓

クラウドサービス連携のインターフェースが統一されることによるコストメリット。
　～クラウドサービス毎に連携機能を開発したり、オプション製品を購入せずに済む。
～　ベンダーロックインの回避

クラウドサービス提供企業でのCSV後始末処理の不安回避。

↓

RESTベースのSCIMが有力候補

1-12. 標準化API連携

RESTの特徴

・Representational State Transfer の略。

・2000年、カリフォルニア大学 Roy Fielding 博士の論文で紹介。

・ネットワーク上のソフトウェア構成「クライアント＆サーバ型」にいくつかのルール(制約)を設けたもので、この制約に従った API が「RESTful API」と呼ばれている。

・そのシンプルさや拡張性の高さが受け入れられ、Facebook, Twitter, Microsoft、国内ではcybozu 等、多くの事業者がサービス機能へのアクセス手段としてRESTFul API を提供している。

・多くが、広く認知されているHTTP上で実装されている（HTTPの開発ツールは多くのデバイス上で存在するため、PC,スマホ,タブレット等さまざまなデバイスで容易に開発）。

・扱う情報を「リソース」として定義し、URIで一意に識別

・「リソース」をシンプルな操作で扱う
Create(POST),Read(GET),Update(PUT),Delete(DELETE)

1-12. 標準化API連携

SCIMの特徴

・System for Cross-domain Identity Management の略。

・GoogleやSalesforce.com、Cisco(WebEx)、Vmwareといったサービス事業者が仕様策定に関与し、現在は IETF Working Group で活動中で、Ver1.0、Ver1.1が internet-draft として公開されており 、Ver2.0を策定中。

・ＲＥＳＴfulなHTTPベースのＷｅｂＡＰＩ。

・シンプルで拡張しやすいスキーマ。

・JSONによるデータ表現。

・5つのオペレーション。

オペレーション	説明
ＧＥＴ	リソースの取得
ＰＯＳＴ	リソースの新規作成・一括更新
ＰＵＴ	リソースの更新（全置換）
ＰＡＴＣＨ	リソースの更新（部分的な更新）
ＤＥＬＥＴＥ	リソースの削除

1-13. トラストフレームワーク

トラストフレームワークとは

電子政府を推進する多くの国、地域で「電子政府認証ガイドライン」が策定されている。
その中で認証の**保証レベル(LoA：Levels of Assurance)**が定義され、各手続きサービスのリスク評価の結果から求められる**認証の保証レベル(LoA)**に従って、適切な認証方式が選択できるようになっている。

〔トラストのそもそもの目的〕RPがサービスを提供する場合にIDPを評価する。
〔何故、必要か？〕フェデレーションのように、完全な分散環境でサービスを提供する場合、RPがIDPを制御できない以上、IDの品質について何らかの評価が必要であるため。

米国政府の動き

2003	**米国 大統領府行政管理予算局(OMB)**は、電子認証に関わるガイダンス、OMB M-04-04を発行し、レベル1～4の**認証の保証レベル(LoA)**について詳しい解説を行った。
2004	このOMB M-04-04を補完することを目的として、**米国国立標準技術研究所(NIST)**は、電子認証に関するガイダンス(NIST Special Publication 800-63-1)を発行した。
2009	民間認証機関のさらなる活用、連携を図り認証に係るコストを削減する観点から、CIOカウンシルの下に設置されたICAMが、Trust Framework Provider Adoption Process(TFPAP)を取りまとめた。
2010	National Insutitute of Satndards and Technology(NIST)は、市民/民間が安全にサイバー空間で暮らしていくためのアイデンティティ基盤構築のための国家戦略文書として、National Strategy for Trusted Identity in Cyberspace(NSTIC)を発表した。

1-13. トラストフレームワーク

日本政府の動き

2010

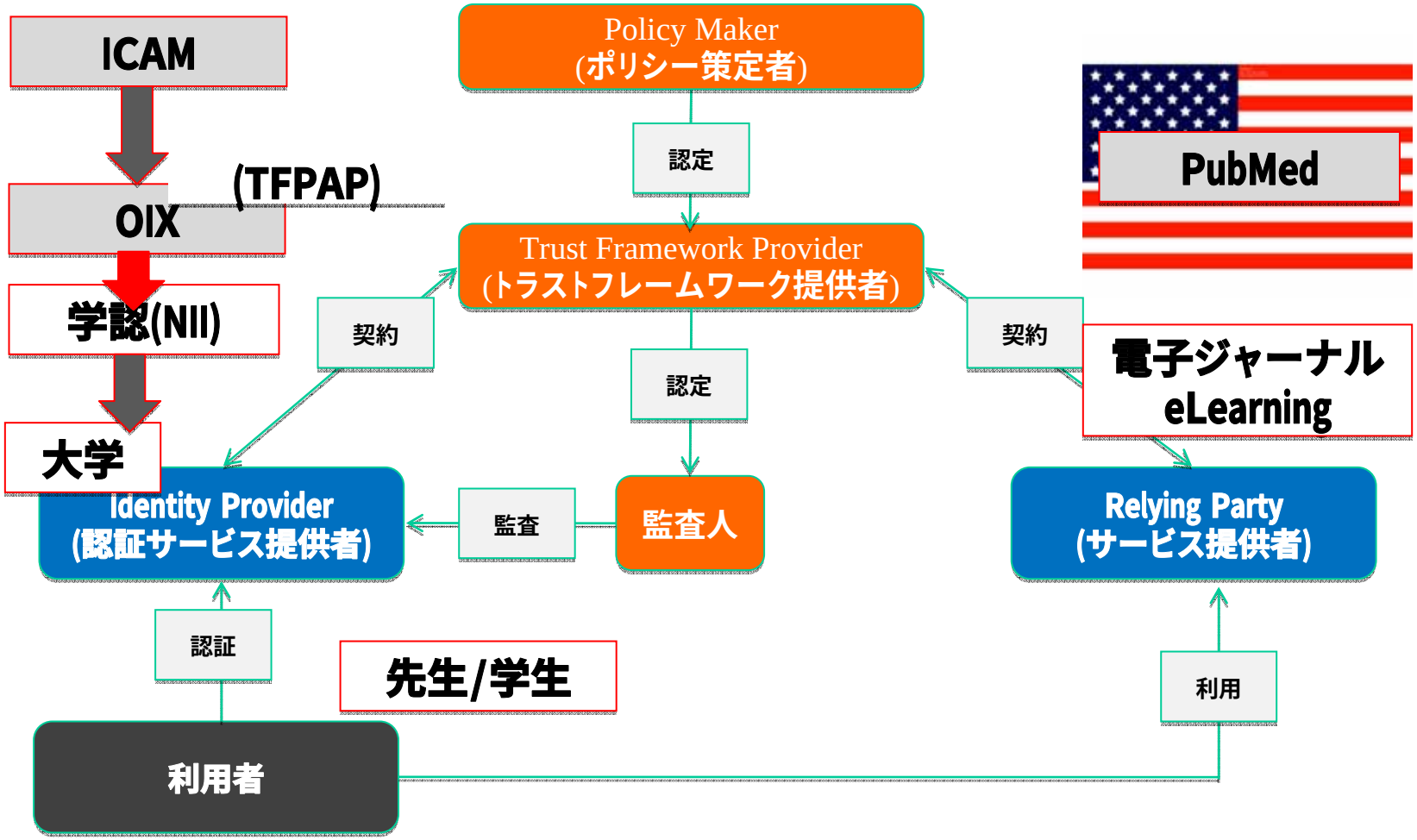
内閣官房情報セキュリティセンター(NISC)は、日本の電子政府における認証方式の設計にあたり活用可能な「ものさし」を確立することを目的として「オンライン手続におけるリスク評価及び電子署名・認証ガイドライン」を策定した。

保証レベル(LoA：Level of Assurance)

＜主な対策基準＞

保証レベル	登録	発行・管理	トークン	認証プロセス	署名等プロセス
レベル4	**（窓口）** ・写真付き身分証明1種の提示 ・申請情報の台帳照合 ・重複登録ではないことの確認	・手渡し、本人限定受取郵便、によるトークン発行	・レベル3の基準に加え、耐タンパ性が確保されたハードウェアトークンを利用すること	・レベル3と同等の基準	・電子政府推奨暗号リストに記載の署名方式 ・電子署名用の証明書の用途は電子署名限定
レベル3	**（窓口）** ・写真付き身分証明1種（or他2種）の提示 ・申請情報の台帳（又は公的証明書）照合 **（郵送 or オンライン）** ・申請書に対する電子署名 ・申請情報の台帳（又は公的証明書）照合	・レベル4の方法に加え、書留郵便、書留郵便＋ダウンロード、電子署名＋ダウンロード、によるトークン発行	・レベル2の基準に加え、複数の認証要素を利用すること	・レベル2と同等の基準に加え、フィッシングの脅威に対する耐性	・電子政府推奨暗号リストに記載の署名方式
レベル2	**（窓口）** ・写真付き身分証明1種（or他2種）の提示 **（郵送 or オンライン）** ・申請情報に他機関の登録情報（クレジットカード番号等）を含めて申告	・レベル3の方法に加え、分割配付（一方を郵送）、メール通知後のダウンロード、によるトークン発行	・認証情報の推測確率が16384分の1未満であること	・レベル1と同等の基準に加え、盗聴、セッション・ハイジャック、中間者攻撃の脅威に対する耐性	
レベル1	**（窓口 or 郵送 or オンライン）** ・身元確認は不要 ・メールアドレスの到達確認	・レベル2の発行方法に加え、電子メールによる送付、ダウンロード、によるトークン発行	・認証情報の推測確率が1024分の1未満であること	・オンライン上の推測、リプレイ攻撃の脅威に対する耐性	

1-14. 学認(学術系トラストフレームワーク)



1-14. 学認(学術系トラストフレームワーク)

トラスト(学認アンケートで問われていること(抜粋))

1.Governance

■組織の成熟度 IdPの運用規模等に関する質問

Q1-5. IdP を運用する上での根拠規則や内規が定められていれば記入してください。

(回答のポイント)

・IdPの運用が組織によってオーソライズされていること。
・組織がセキュリティについてのポリシー、運用規則を定め、文書化され、それに従った運用をしていること。

1-14. 学認(学術系トラストフレームワーク)

トラスト(学認アンケートで問われていること(抜粋))

2.Privacy

■個人情報保護に関する質問

Q4-1. IdP から送信される個人情報について、関係する法令その他に従うように運用されていますか？具体的に規定はありますか？

(回答のポイント)

- 法令を遵守していること。
- より良いのは、『学内外にプライバシーポリシーを開示している。』、『新たな SP のサービスを利用するときには、書面またはオンラインで利用者許諾を得ないと利用できないように運用している。』

1-14. 学認(学術系トラストフレームワーク)

トラスト(学認アンケートで問われていること(抜粋))

3.Technical

■ Identity管理、パスワード管理関する質問

Q2-1. 利用者IDは、学務データや人事データ等、組織にとって信頼できるデータベースから作成されるように定めていますか？

(回答のポイント)

- ID情報は人事DB、教務DB等、組織の中で「Trusted DB」が源泉となること。
- Trusted DB から作ることができないID情報は、作成にあたって組織(部レベル)の承認行為があるなど責任の所在が明確であること。

1-14. 学認(学術系トラストフレームワーク)

トラスト(学認アンケートで問われていること(抜粋))

3.Technical

■ パスワード管理に関する質問

Q2-7. 利用者IDのライフサイクル管理、特に停止や廃棄についてどう規定されていますか？

Q3-2. IdP では，同一 ID でのアクセスが同一人物からによること を保証するための方策を講じなければならないとされています。

Q3-2-1. 特に、ID とクレデンシャルの配布や管理によってこれを保証する方法を記入してください。

(回答のポイント)

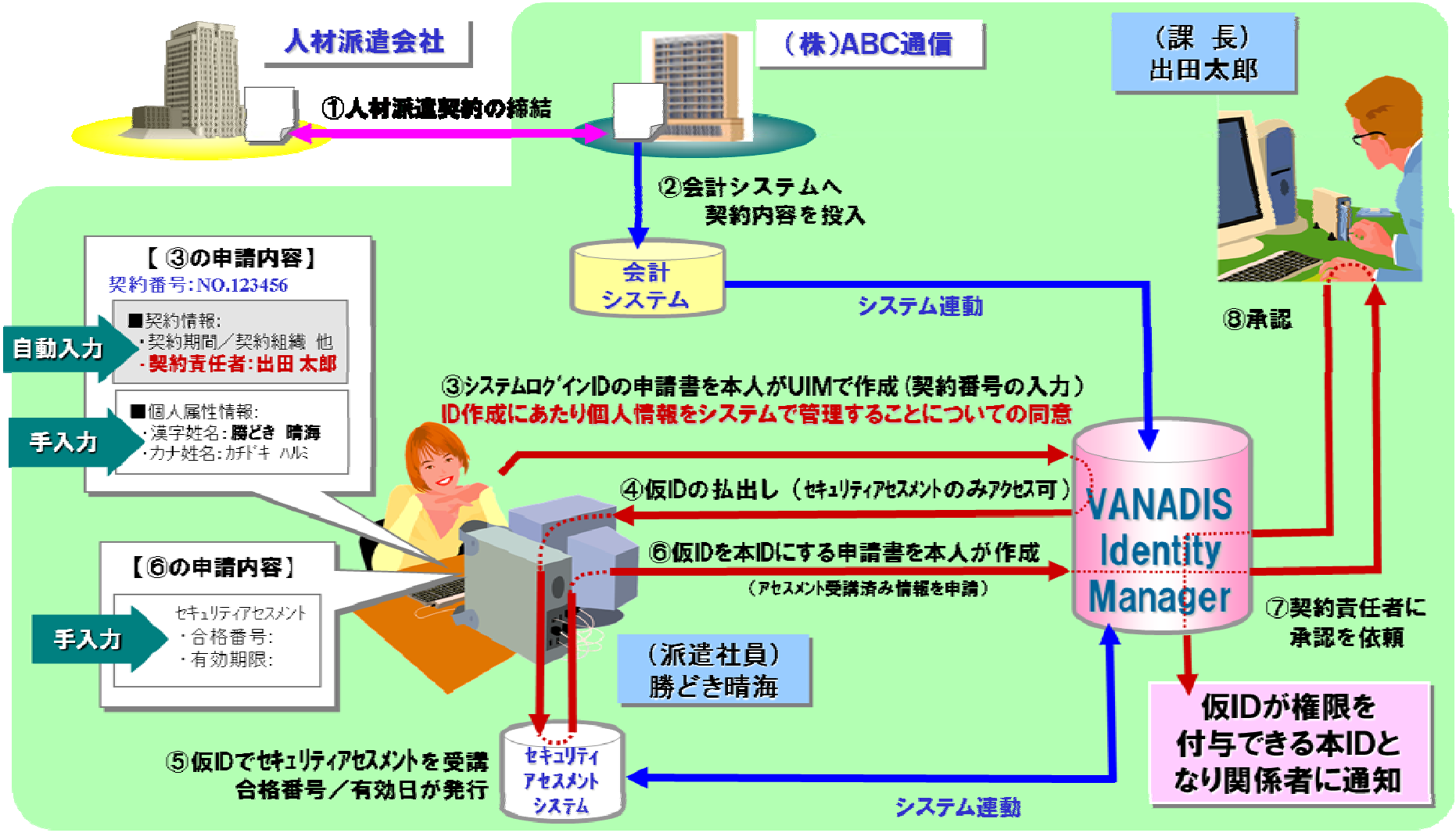
・利用者IDのＤＢは、管理部局である人事または学務において適切に管理され、**IDのライフサイクル管理**もその一環として管理されていること。

・利用者が組織を去った場合、担当部局によって失効作業が行われる体制になっていること。

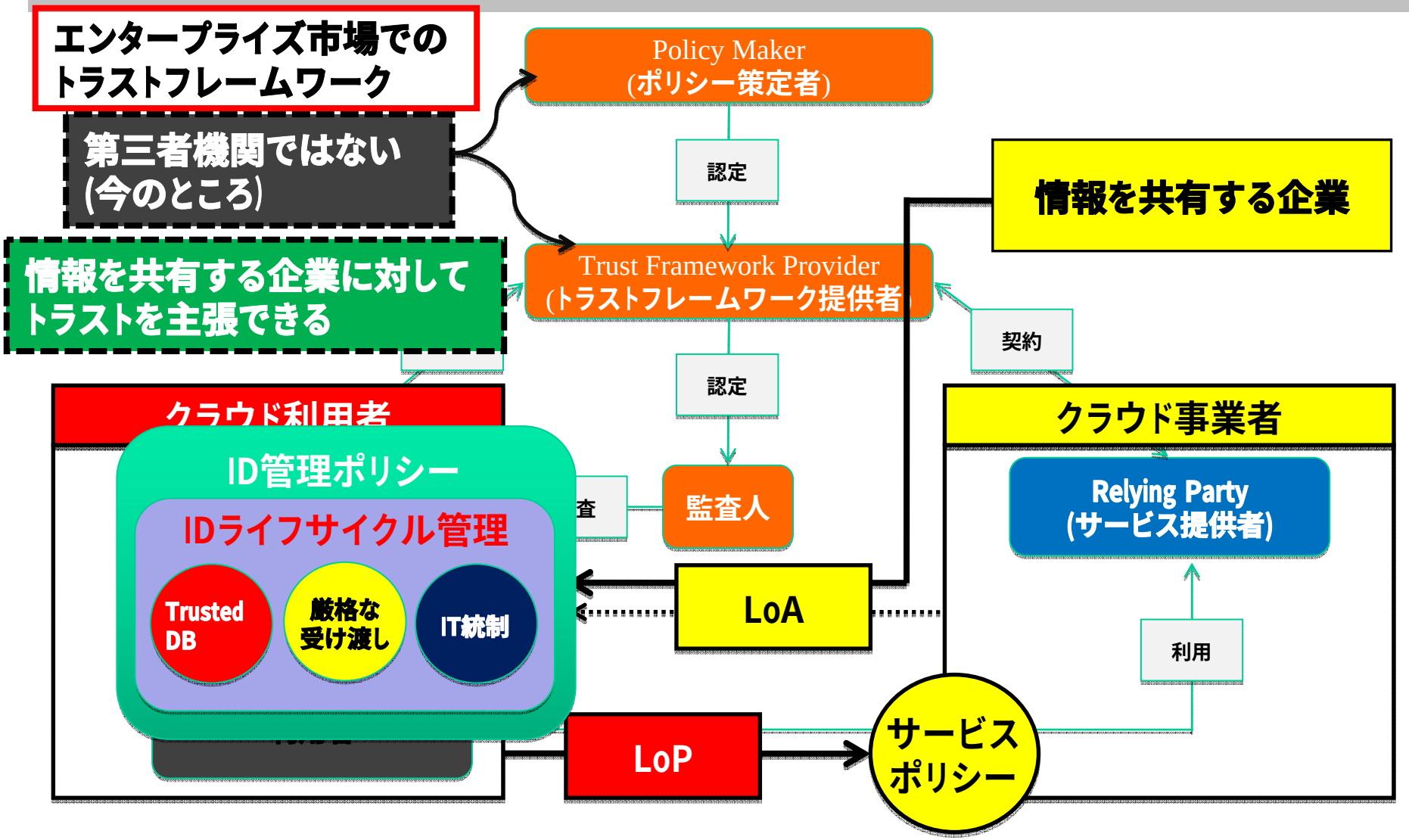
・IDとパスワードの配布は、職員証・学生証を用いて本人確認を行った上で、書面で行っていること。

1-15. 厳格なIDライフサイクル管理運用の事例

NTTデータ様の場合(派遣社員のID発行処理)

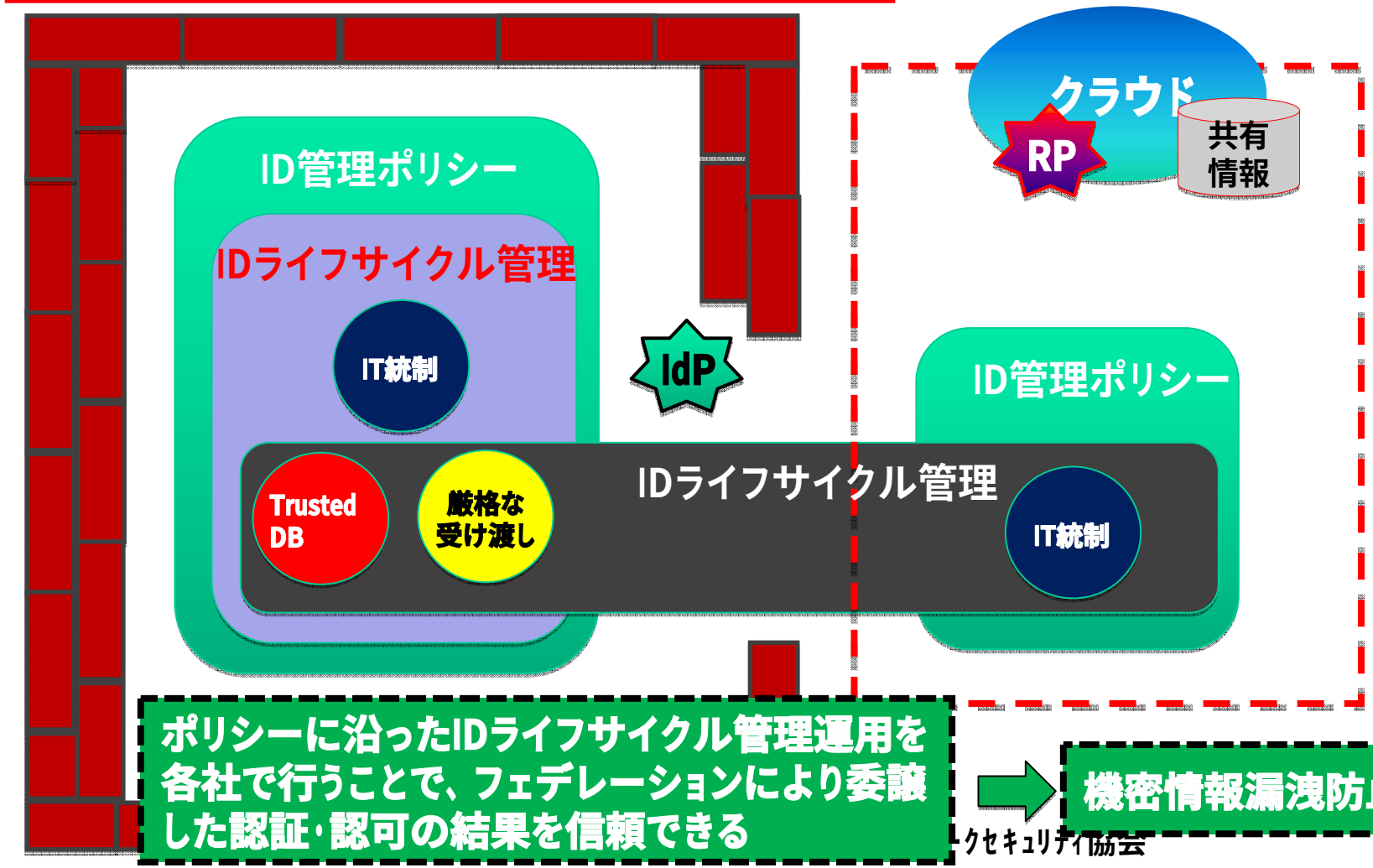


1-16. エンタープライズでのトラストフレームワーク



1-16. エンタープライズでのトラストフレームワーク

エンタープライズ市場でのトラストフレームワーク



ポリシーに沿ったIDライフサイクル管理運用を各社で行うことで、フェデレーションにより委譲した認証・認可の結果を信頼できる

→ 機密情報漏洩防止

1-16. エンタープライズでのトラストフレームワーク

提案

〔ID管理ポリシーの策定〕
各企業は、ID管理システム導入時に策定するID情報メンテナンスに関わる運用設計があれば、ID管理ポリシーを作成することができる。

〔学認のような第三者機関はない〕
エンタープライズ市場では学術市場での学認のような、第三者機関としてのPolicy MakerやTFP(Trust Framework Provider)は存在せず、ITリソースのボーダレス化に遭遇すると、会社間の力関係により親会社等が作成したポリシーの遵守を強制される場合も多々ある。

〔各企業の作成したID管理ポリシーは通用する〕
IDライフサイクル管理の①Trusted DBと③IDの厳格な受け渡し部分は誰もが認めるトラストの構成要素であり、適切なIDライフ サイクル管理を理解し、自社用に作成しておけば、他社との情報共有を行う場合、ポリシー作成者が他社でも、そのまま適用できるはずである。

1-17. まとめ
フェデレーションとトラストフレームワーク関係

フェデレーション活用

↓

余分なID情報(Credential含む)の保持回避

↓

認証処理が委譲される

↓

〔正しい認証認可の前提〕ID管理運用が適切に行われている

↓

ID運用ポリシーの策定とその遵守についての説明責任発生

↓

ID統合管理システムによる厳格なIDライフサイクル管理の実施

↓

他社との情報共有時、自社で作成した運用ポリシーの適用

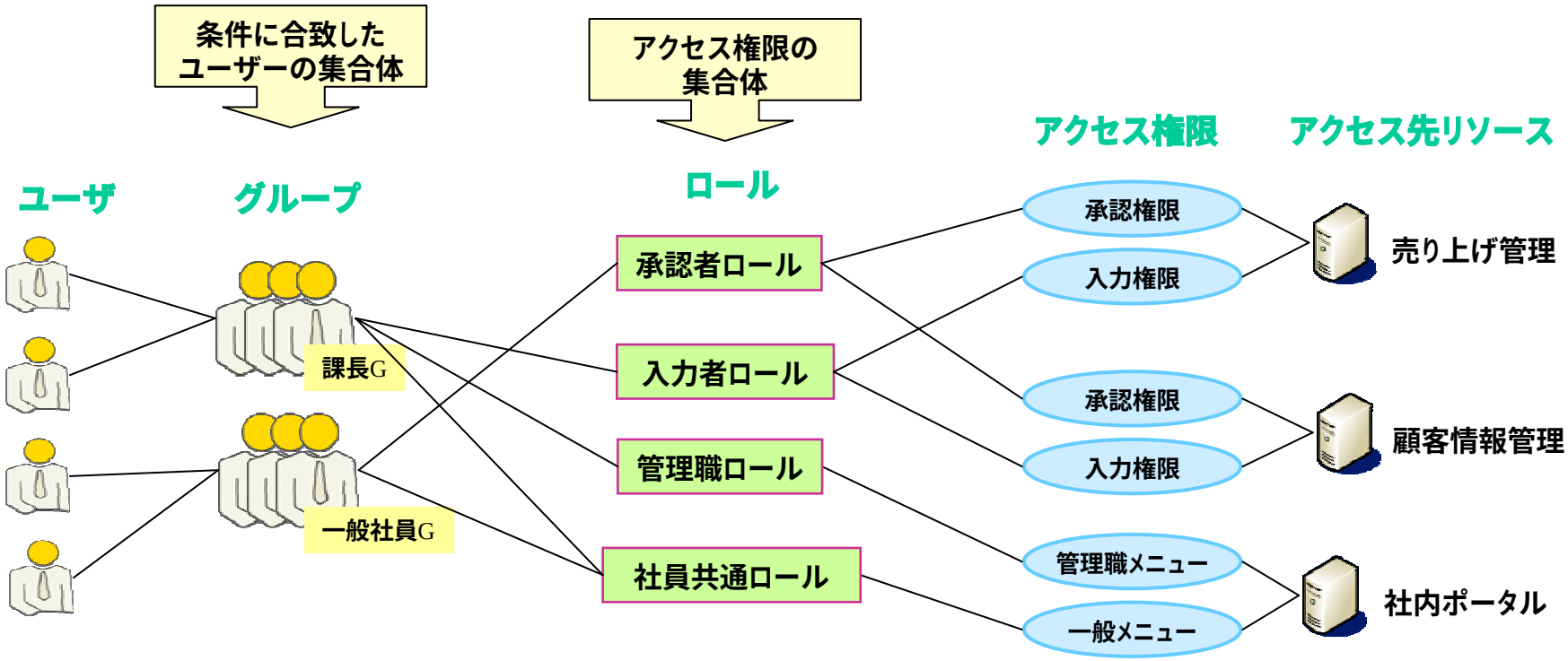
↓

トラストの確立＆維持

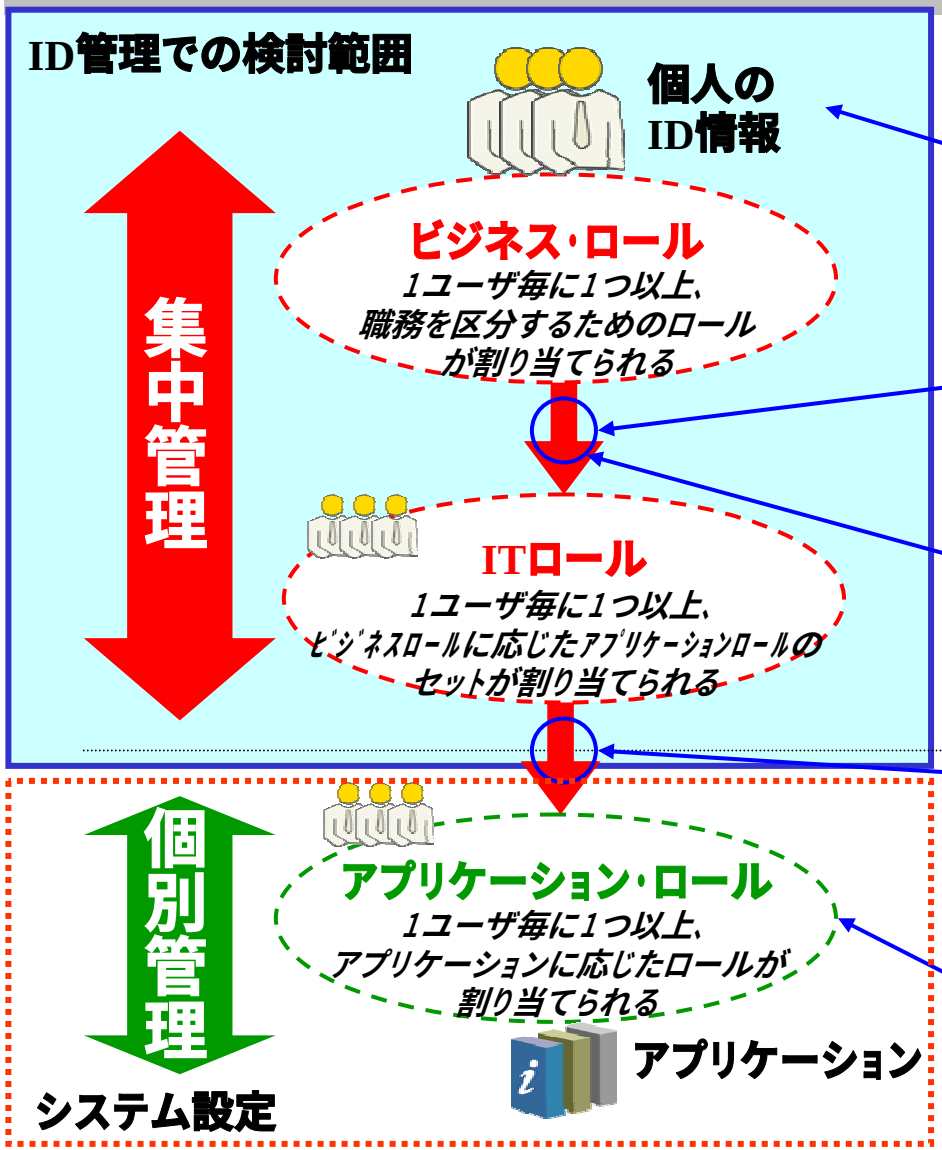
2. エンタープライズロール管理

2－1．ロール管理とは何か？
①ID管理におけるロールとは

ロールとは職務権限/役割に応じた、リソースへのアクセス権の集合体です。
アクセス権はアクセス先リソース（オブジェクト）とオペレーションから構成され、
ユーザーないしはグループは、ロールの割り当てを経てアクセス権を獲得する。
RBAC (Role-based access control:ロールベース・アクセス制御)は、個々のユーザ/グループ単位での割り当てではなくロールに基いてリソースへのアクセスをコントロールするモデルです。
リソースへのアクセス権をロールで束ねることで、システム横断的なアクセス権管理を実現し、以降の運用を容易することが可能となる。



2－1.ロール管理とは何か？
②ロールの分類とID管理での検討範囲



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ロールにマッピングされる。

ビジネスロールは直接的にアプリケーションロールにマッピングすることもできる。

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。

2－1．ロール管理とは何か？
③ロール定義例

以下にビジネス･ロールからITロールへのマッピングを定義した例を示す。
ここでは所属企業/職制によるビジネス･ロールを定義し、業務単位のアクセス先リソースでのアプリケーション･ロールからITロールを定義している。
更に業務フローごとの職責ロールなども定義の対象となる。

ビジネス･ロール			T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	R001	×	○	○	○	×	×	×	○	○	○	○	○	○	×
		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	R009	×	○	○	×	○	×	×	○	○	○	○	○	×	×
		協力会社社員	R010	×	○	○	×	×	×	×	○	×	×	×	×	×	×
			ACL	ACL001	ACL002		ACL003	ACL004	ACL005	ACL006	ACL007	ACL008	ACL009		ACL010	ACL011	ACL012

2－2．成果物の紹介

「エンタープライズロール管理」

第1章 ロール管理とは
- 1.1 ロール管理の定義
- 1.2 ロール管理の意義

第2章 ロール管理導入指針
- 2.1 ロール管理導入の流れ
- 2.2 ロール管理導入における課題
- 2.3 現状調査･企画フェーズ
- 2.4 要件定義フェーズ

第3章 ロール管理の運用
- 3.1 ロール管理の適正な運用の重要性
- 3.2 ロール管理運用の観点

＊ダウンロードはこちらから
http://www.jnsa.org/result/2013/std_idm.html

３．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

3－1．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 POD
インプレスR&D libura PRO

３－１．書籍の紹介

第1章　アイデンティティ管理（ID管理）とは
第2章　ID管理の意義
第3章　IT内部統制におけるID管理の位置付け
第4章　クラウド環境におけるID管理の位置付け
第5章　グローバルビジネス環境におけるID管理
第6章　ID管理システム導入指針
第7章　ID管理システムにおける仮想企業導入事例
第8章　ID管理アンチパターン
第9章　ID管理に関するFAQ

用語集

４. 今年度のテーマ

４－１．今年度のテーマ

１．ロールマネジメントの検討（継続テーマ）
　　成果物改定

２．アイデンティティとプライバシー勉強会
　　有識者の方との懇談を予定

３．特権IDの検討

４．openID　ファウンデーションジャパン EIWG の連携

５．その他テーマ

　　＊現在、新規メンバー募集中！　６／１４（金）まで！

4－2．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式会社
2	富士榮　尚寛	伊藤忠テクノソリューションズ株式会社
3	稲吉　英宗	伊藤忠テクノソリューションズ株式会社
4	木村 慎吾	株式会社インテック
5	駒沢 健	NTTコムウェア株式会社
6	前園　暁子	NTTコムウェア株式会社
7	篠原　信之	株式会社シグマクシス
8	小林 智恵子	東芝ソリューション株式会社
9	丹羽　奈津子	日本IBM株式会社
10	酒井美香	日本アイ・ビー・エム　システムズ・エンジニアリング株式会社
11	桑田 雅彦	日本電気株式会社
12	中村 有一	日本電気株式会社
13	半澤　敦	日本電気株式会社
14	大竹 章裕	株式会社ネットマークス
15	栃沢 直樹	トレンドマイクロ株式会社

	氏名	所属
16	岩田　洋一	富士通株式会社
17	今堀　秀史	富士通関西中部ネットテック株式会社
18	福原　幸一	富士通関西中部ネットテック株式会社
19	恵美　玲央奈	株式会社富士通ソーシアルサイエンスラボラトリ
20	安納　順一	マイクロソフト株式会社
21	中島　浩光	株式会社マインド・トゥー・アクション
22	南　芳明	日本ベリサイン株式会社
23	川田　晋嗣	セコムトラストシステムズ株式会社
24	酒井　寛	セコムトラストシステムズ株式会社
25	貞弘　崇行	JBSソリューションズ株式会社
26	讃井 崇喜	日本アイ・ビー・エム システムズ・エンジニアリング株式会社
27	山田　達司	株式会社ＮＴＴデータ　技術開発本部
28	江川　淳一	エクスジェン・ネットワークス株式会社
29	大平　祐介	エクスジェン・ネットワークス株式会社
30	森田 陽一郎	日本電気株式会社
31	石川 祐輔	三菱電機株式会社
32	淺海 美哉	ソニー株式会社

計３２名（順不同）