

企業内でのオープンソース活用による最新認証連携と あるべき姿



2015年2月26日 (木)

株式会社野村総合研究所
システムコンサルティング事業本部
ITアーキテクチャーコンサルティング部

堀崎 修一

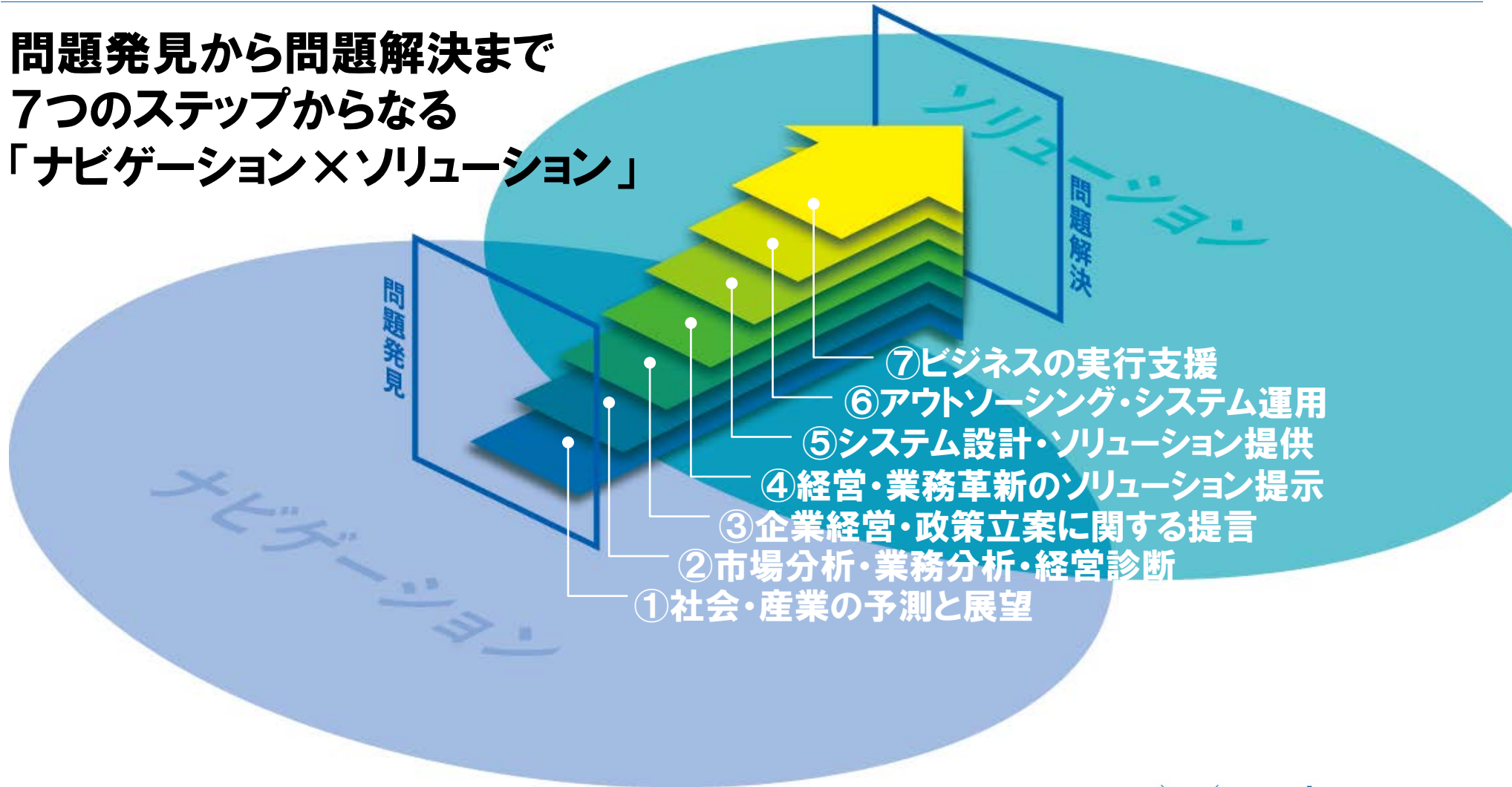
〒100-0005
東京都千代田区丸の内1-6-5 丸の内北口ビル

目次

- シスコンのご紹介（システムコンサルティング事業本部のご紹介）
- IDMが注目される背景
- 企業内アイデンティティ管理への要求
- 企業内アイデンティティ管理のあるべき姿
- 企業内アイデンティティ管理検討における重要なポイント
- IDM導入にあたっての検討の進め方
- まとめ

システムコンサルティング事業本部のご紹介 NRIのDNA「ナビゲーション×ソリューション」

問題発見から問題解決まで 7つのステップからなる 「ナビゲーション×ソリューション」



Navigation × Solution

システムコンサルティング事業本部のご紹介 ナビゲーションからソリューションへの橋渡し

マネジメント コンサルティング

- 事業戦略/事業再編/
新事業開発
- M&A/企業再生/
ファイナンス戦略
- 組織開発/人材戦略/
次世代人材育成
- ビジョン/
経営計画策定/CSR
- マーケティング/
ブランド戦略
- 新興国戦略
- PPP/公企業改革/
インフラ事業戦略
- 政策立案/政策評価
- 地域再生/
チェンジマネジメント
- 社会システム構築/
実証実験
- 業務改革

システムコンサルティング

システムコンサルティング事業本部

(約200名)

ITマネジメント
コンサルティング部

ITアーキテクチャー
コンサルティング部

システムデザイン
コンサルティング部

IT刷新プロジェクト部

戦略IT研究室

金融
IT
コン
サル
ティ
ン
グ
部

産業
IT
コン
サル
ティ
ン
グ
部

社会
IT
コン
サル
ティ
ン
グ
部

ソリューション

金融ITソリューション

証券ITソリューション
資産運用ITソリューション
銀行ITソリューション
保険ITソリューション

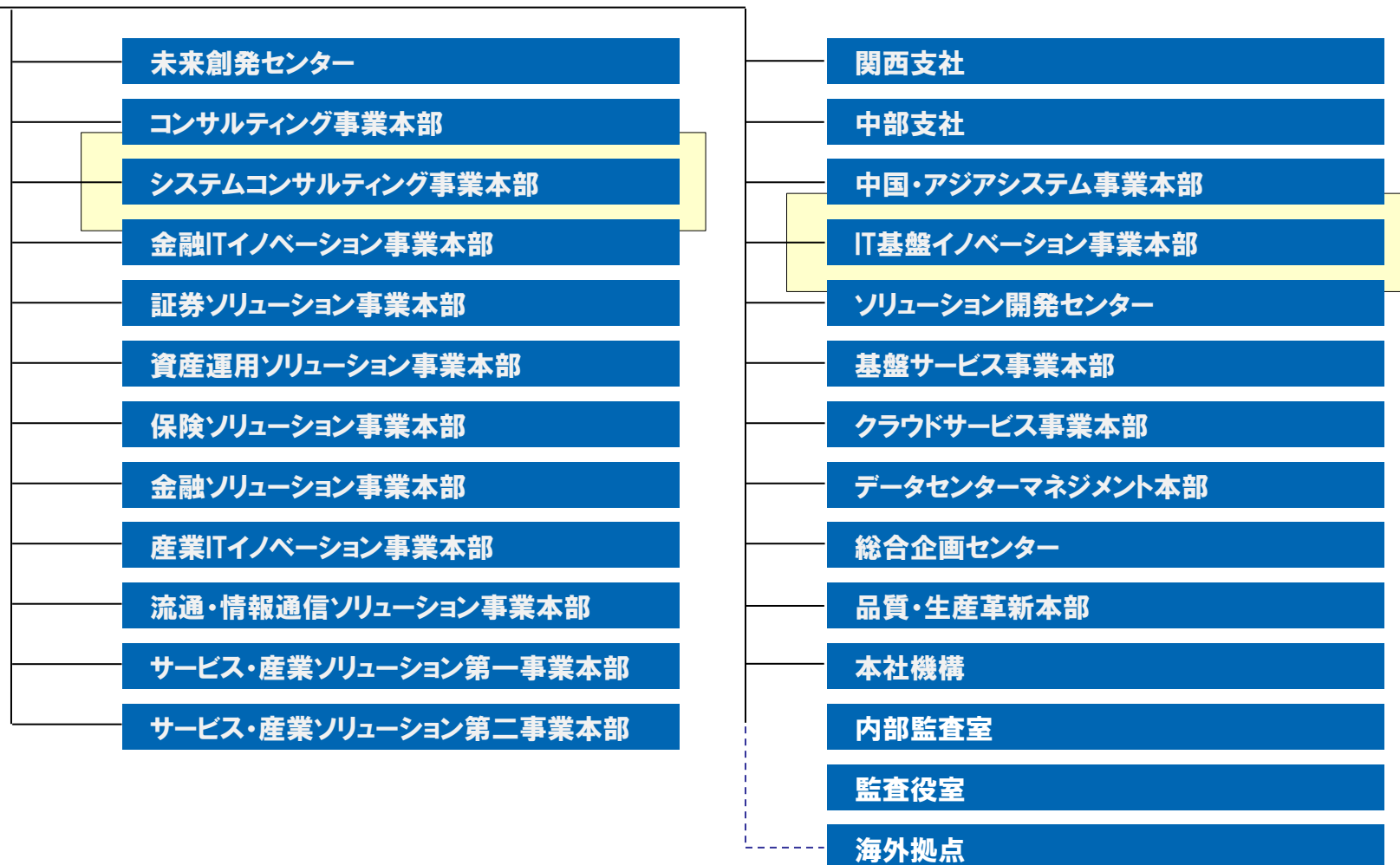
産業ITソリューション

流通ITソリューション
産業ITソリューション
ヘルスケアITソリューション

IT基盤サービス

基盤ITソリューション
システム運用ソリューション
先端技術ソリューション

野村総合研究所



1. IDMが注目される背景

企業内のID管理作業は年々複雑化し作業も高負荷に、人手では限界に来ている。

■ 常に求められる業務の効率化

- ID管理の効率化
 - ・・・ 人事異動の時期のたびに疲弊する運用管理者
- 現行認証基盤の複雑化
 - ・・・ 度重なるシステムの改変、改良で維持管理も高負荷

■ 法規制への対応

- 内部統制、コンプライアンス強化
 - ・・・ ID作成手順の見える化、そしてトレースできるように
- 個人情報保護
 - ・・・ アクセス権管理の強化、対応にも作業負荷が顕著に

■ IT環境の変化

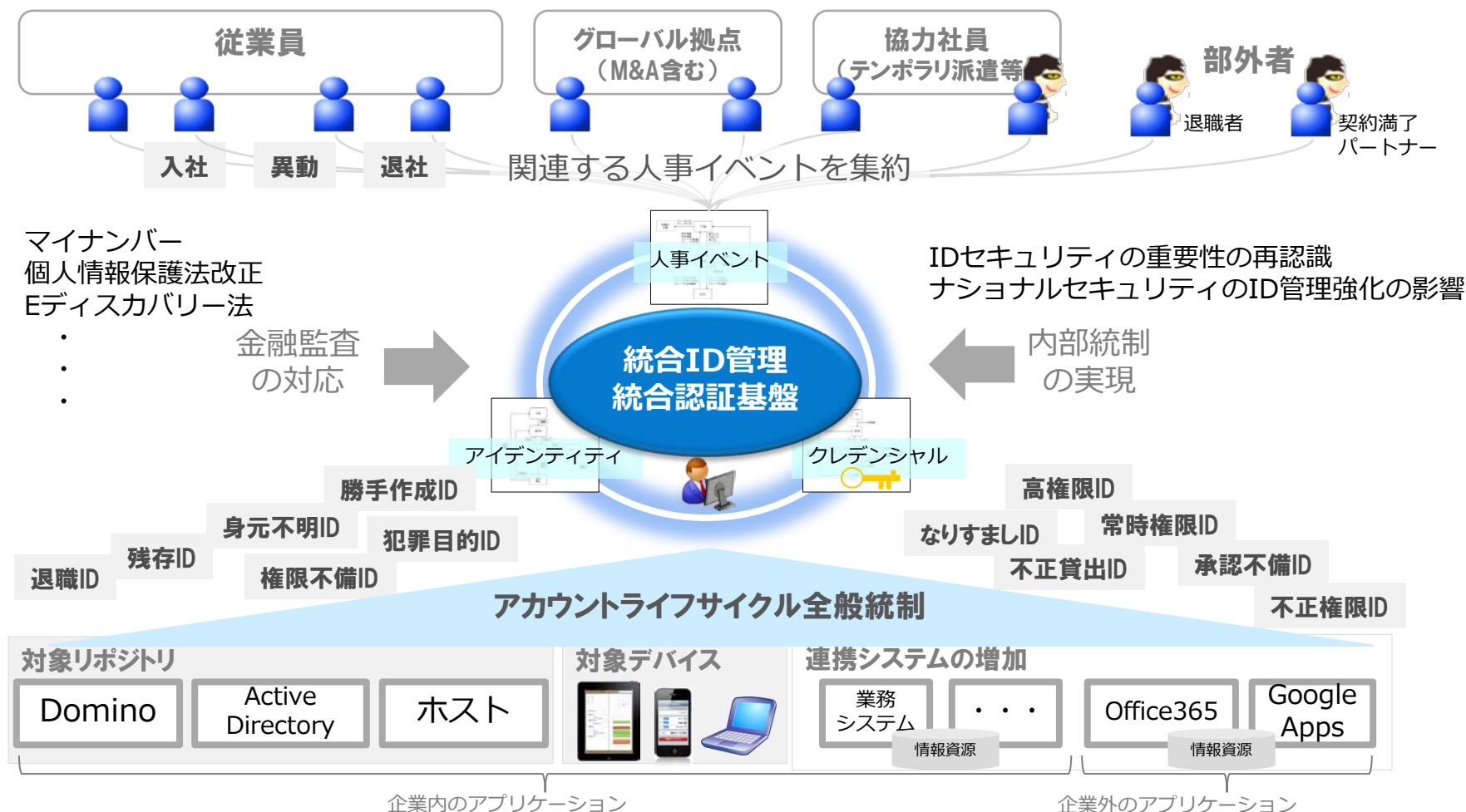
- SaaSの台頭、クラウドサービス利用の一般化
 - ・・・ Office365、GoogleApps等の利用
- モバイル端末、スマートフォン、タブレットの利用
 - ・・・ モバイル利用の促進、要求、管理手法
- 多段認証の要求（生体認証の追加等）

■ 事業変化への対応

- グループ企業間あるいはグローバル規模でのコワーク、システム利用頻度の増加
- 企業合併（M&A）、多様な人材登用、活用
 - ・・・ あるとき急にユーザーが増える！
- 社内認証基盤統合、社内システムの統合
 - ・・・ 急に運用管理対象となるシステムが増える！

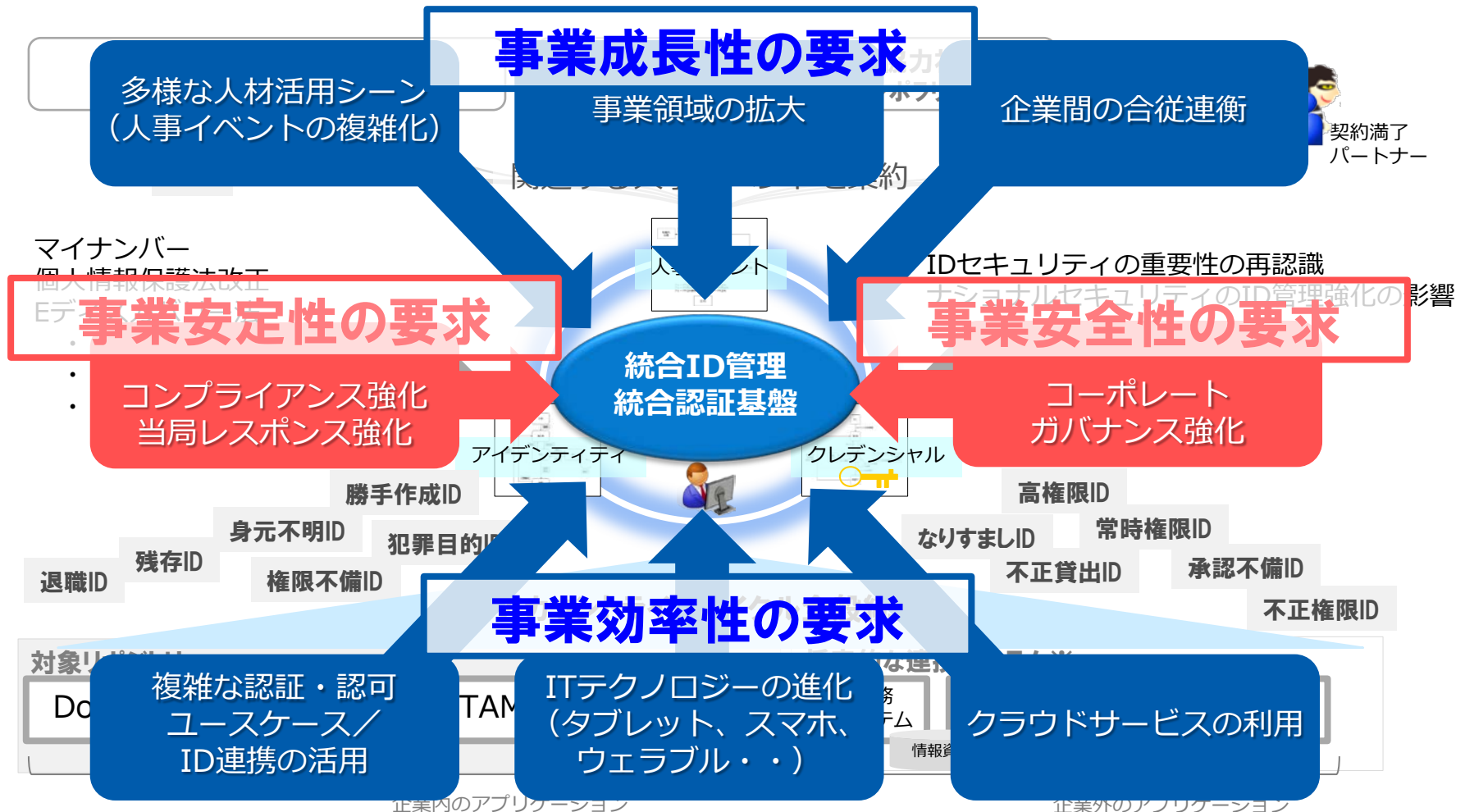
2. 企業内アイデンティティ管理への要求

グローバル化の流れとコンプライアンス強化の流れがID管理強化を求めている。

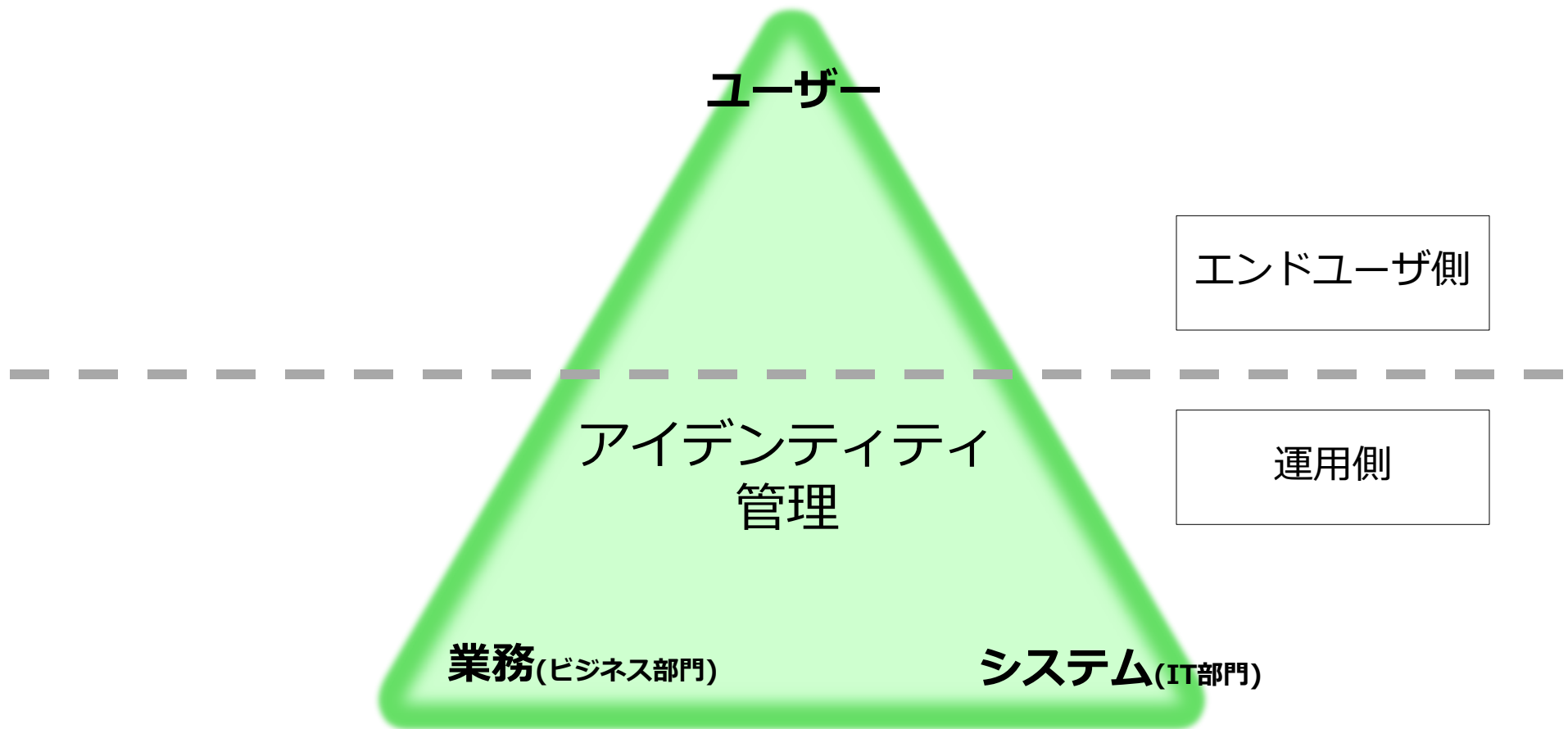


2. 企業内アイデンティティ管理への要求

グローバル化の流れとコンプライアンス強化の流れがID管理強化を求めている。

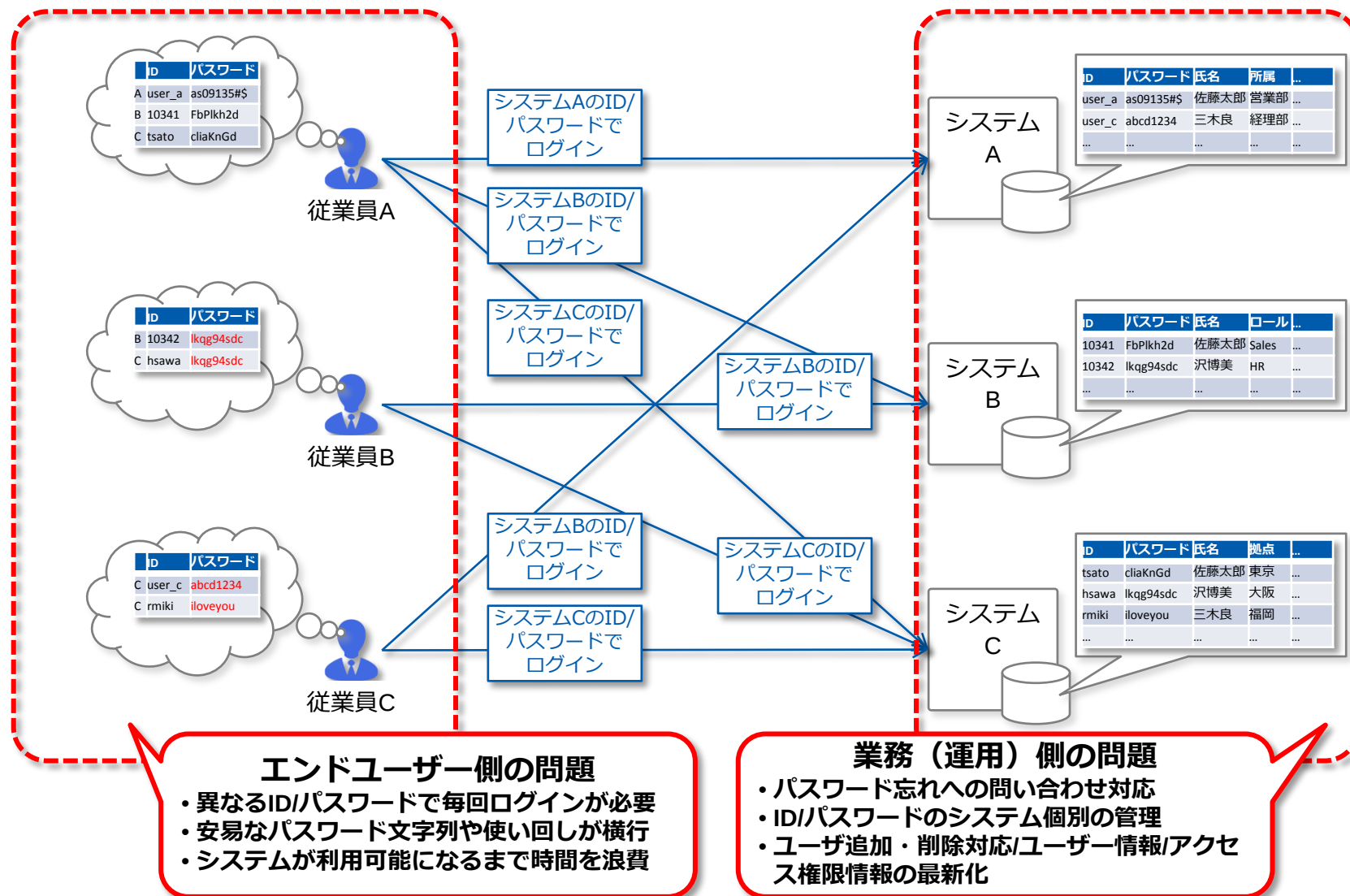


3. 企業内アイデンティティ管理のあるべき姿 業務、システム、ユーザーの3つの視点

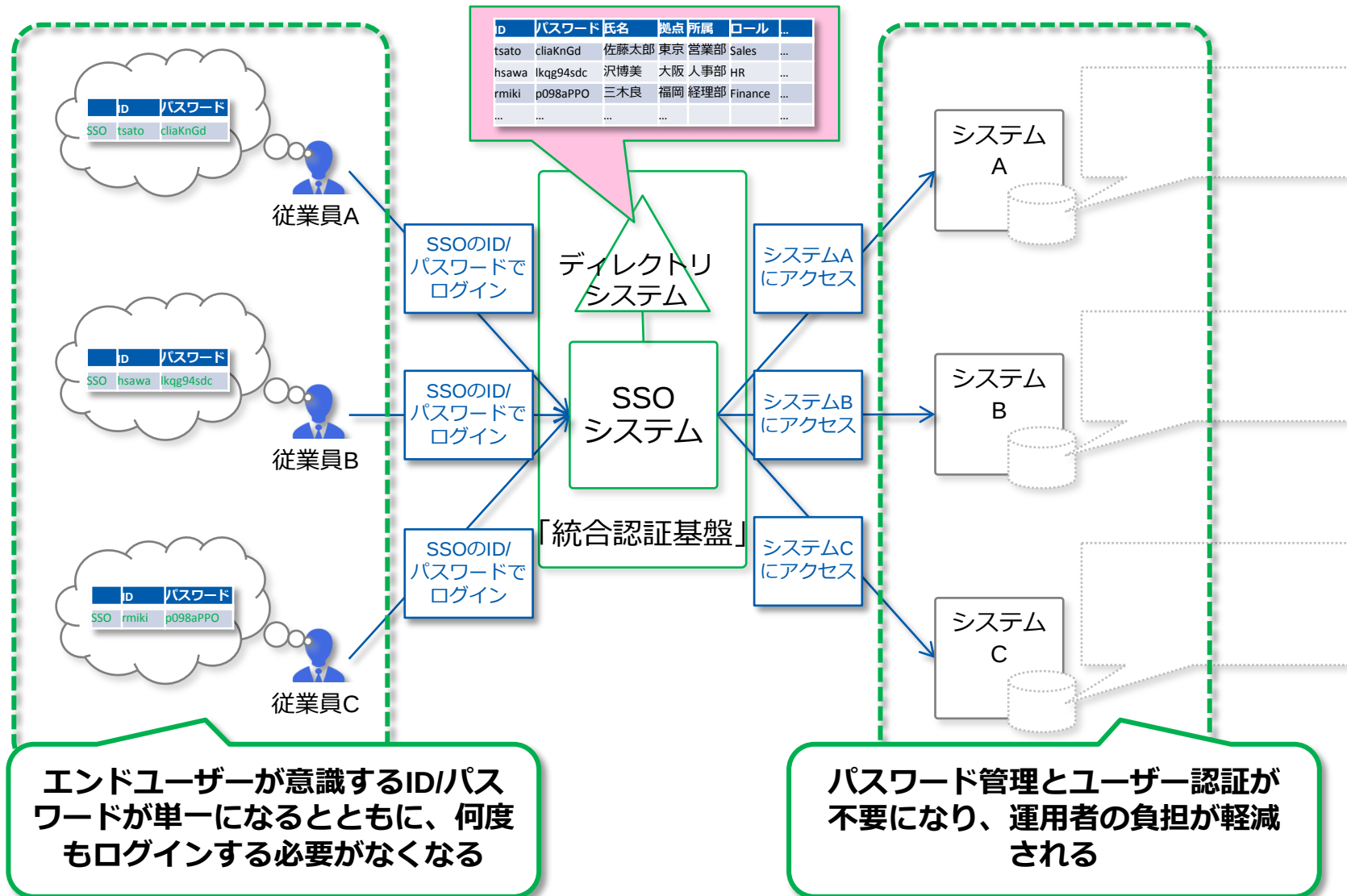


3. 企業内アイデンティティ管理のあるべき姿

ユーザー情報/アクセス権限情報の散在はユーザー/業務の双方にとって問題となる

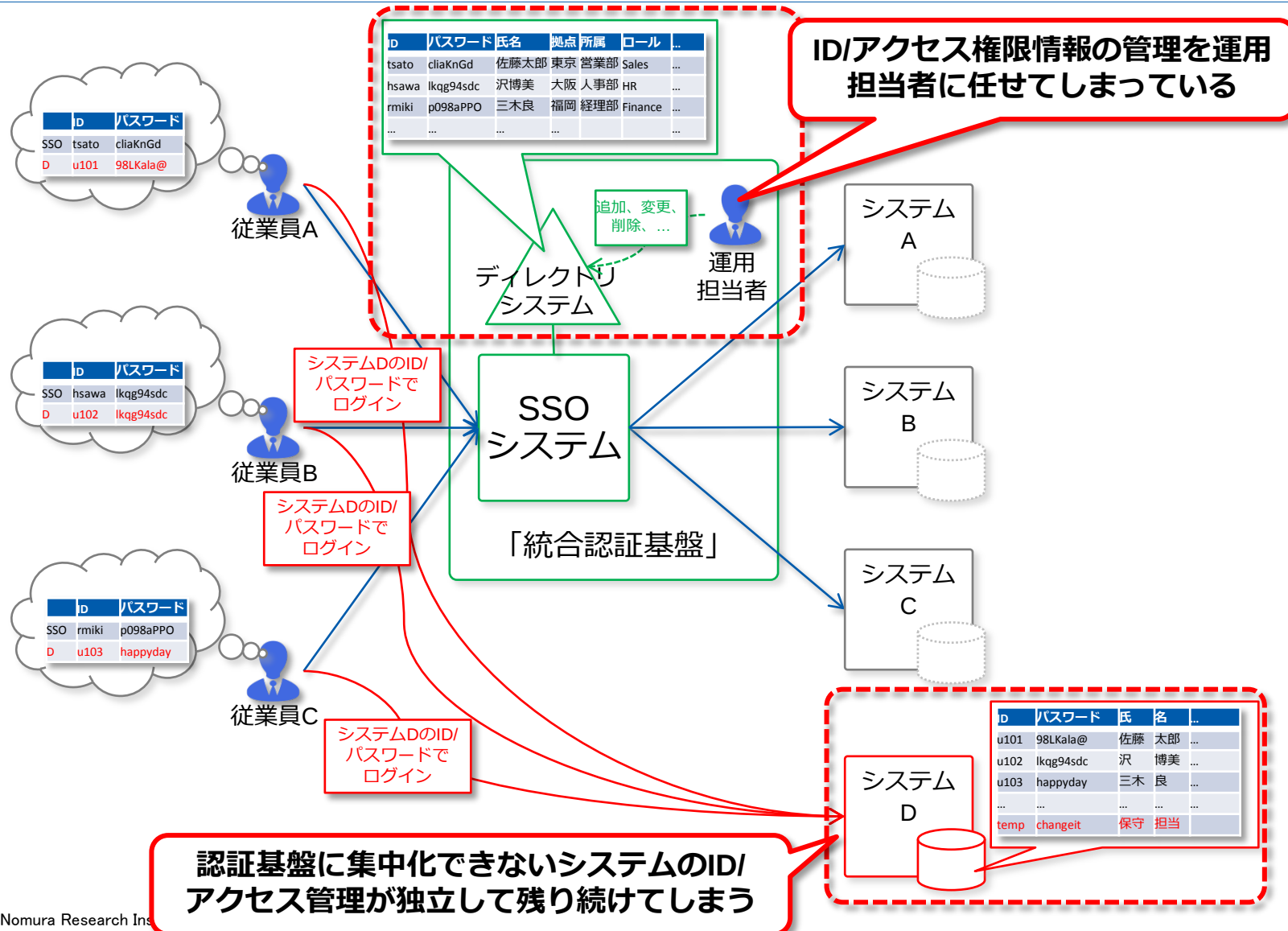


3. 企業内アイデンティティ管理のあるべき姿 ユーザー認証を一元化する「認証基盤」の登場



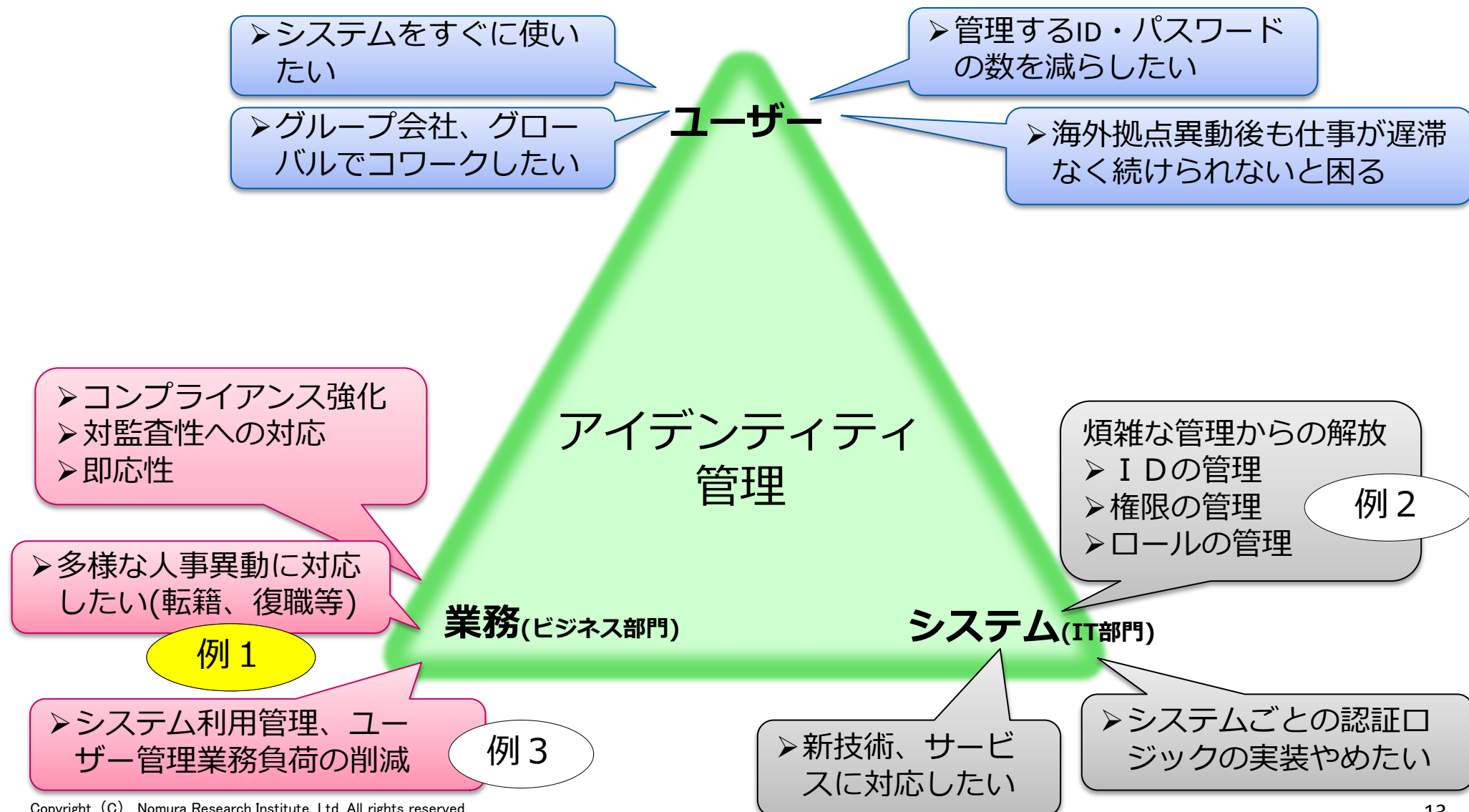
3. 企業内アイデンティティ管理のあるべき姿

「認証基盤」だけでは組織全体のID/アクセス権限を管理しきれない





4. 企業内アイデンティティ管理検討における重要なポイント 業務、システム、ユーザーの3つの視点で要件を検討・定義する

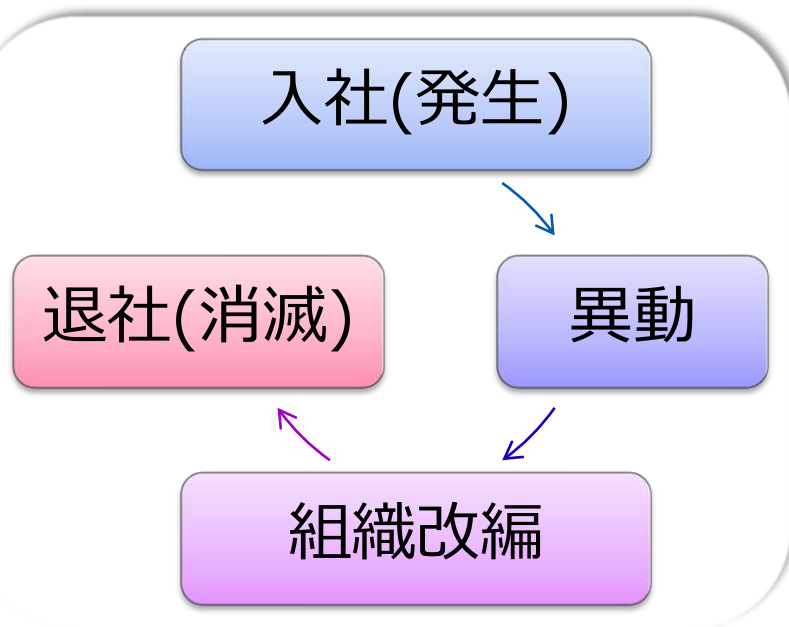


4. 企業内アイデンティティ管理検討における重要なポイント

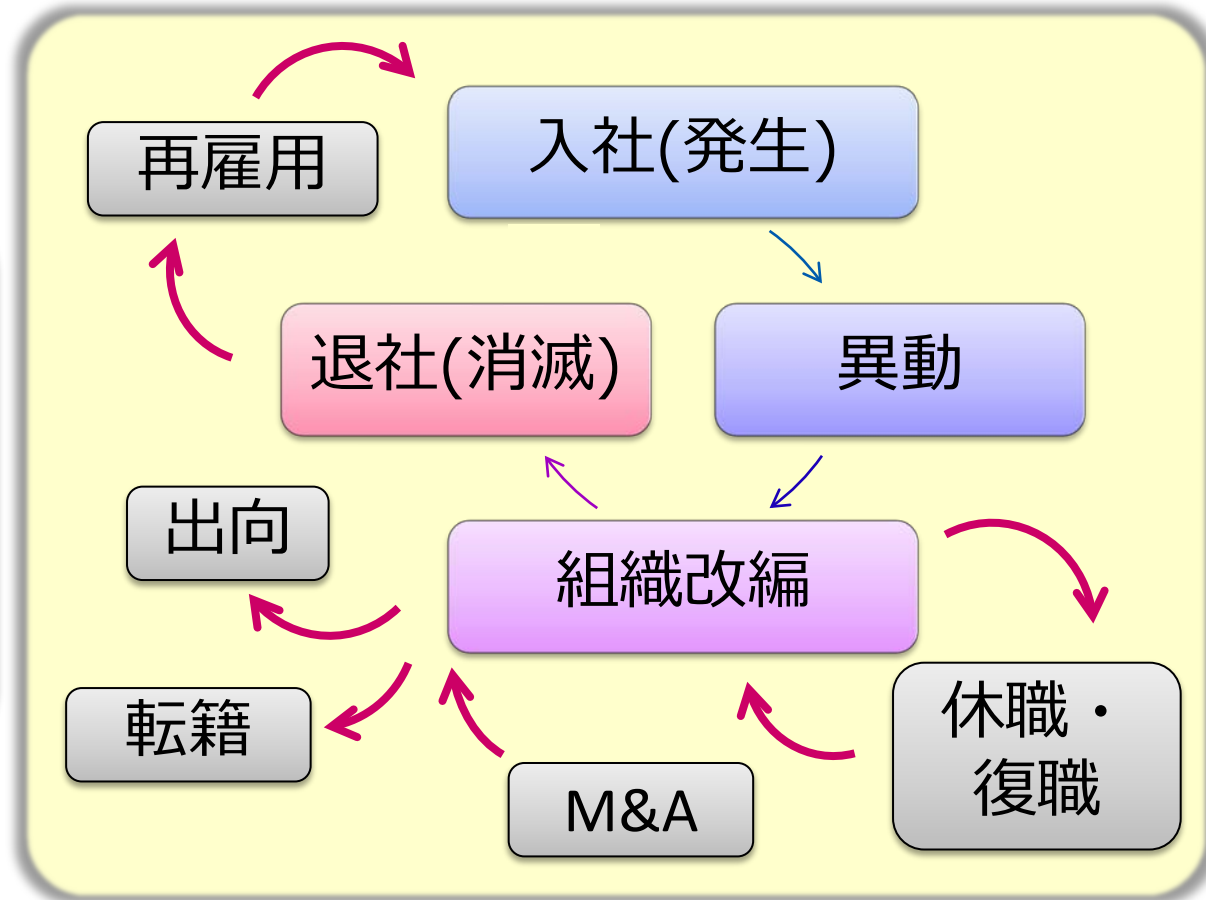
4.1 IDのライフサイクル管理

ライフサイクルは多様性が増している、現状をしっかりと把握する必要がある

従来の IDライフサイクル



複雑化するIDライフサイクル



4. 企業内アイデンティティ管理検討における重要なポイント

4.1 IDのライフサイクル管理

ライフサイクルは多様性が増している、現状をしっかりと把握する必要がある

■ 人事イベントをキーにライフサイクル管理を検討した例

業務プロセス定義済み ライフサイクル対象外		登録（受入）		変更																削除			
		本社		Prj.	本社												Prj.		人	本社	Prj.	他	
		人事採用	部門採用	Prj採用	部署異動	拠点移動	職位変更	再雇用 （シニア）	再雇用 （役員）	／出向 ／帰任	転籍	兼務	／休職 ／復職	組織改正	改姓	兼務	その他	PM変更	PMリセッ ト	退職	PM離脱	PM完了	システ ム利用 削除
職員	会社全体																						
パートナ ー	契約派遣社員																						
	顧客																						
	パートナー会社																						
	ベンダー																						
	その他																						
システ ム管理	ヘルプデスク																						
	グローバル拠点 システム管理者																						
	本社システム管理者																						

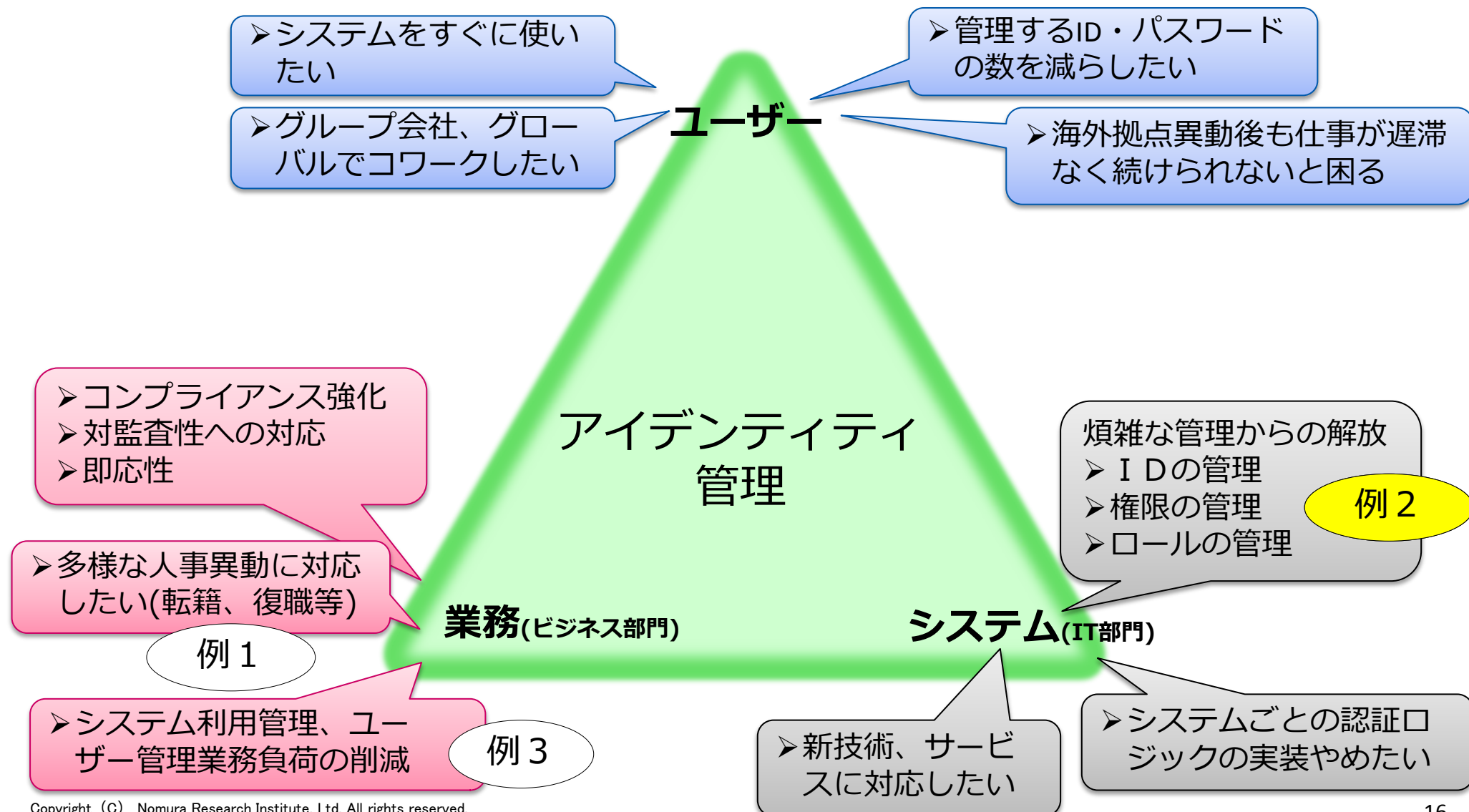
ステークホルダー（例）

- 人事部門
 - グループ会社の人事
 - 出向先の人事
- 業務部門
 - グローバル拠点のIT

ステークホルダー（例）

- 人事部門
 - グループ会社の人事
 - 出向先の人事
- 業務部門
 - グローバル拠点のIT

4. 企業内アイデンティティ管理検討における重要なポイント 業務、システム、ユーザーの3つの視点で要件を検討・定義する



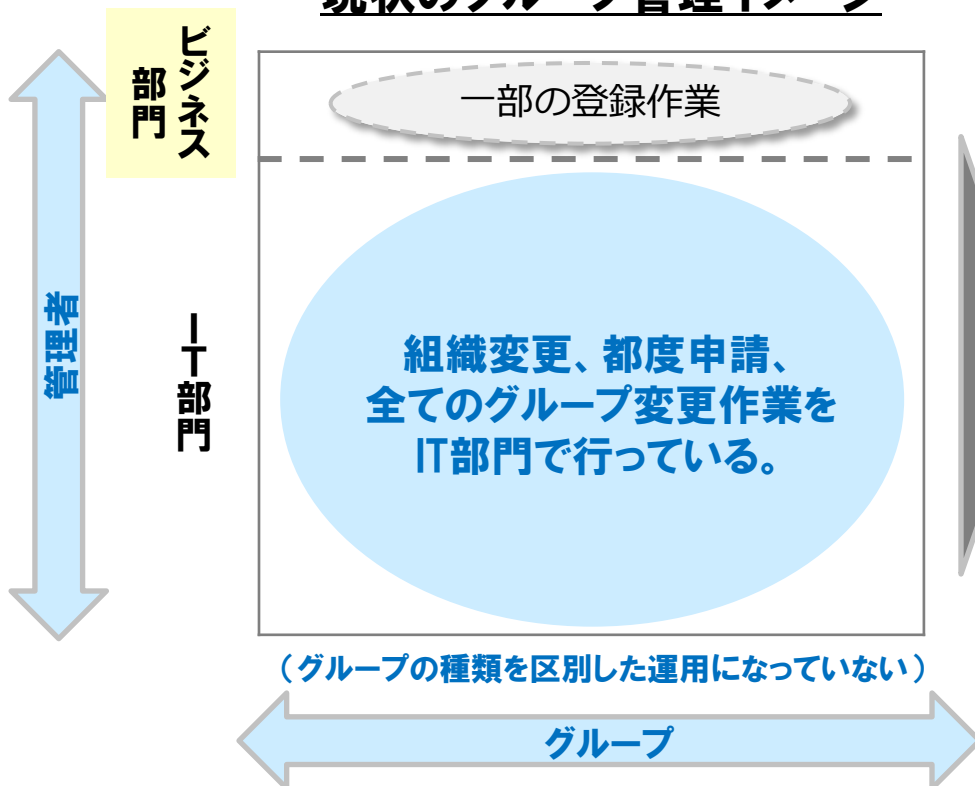
4. 企業内アイデンティティ管理検討における重要なポイント

4.2 認証・認可（ロール）情報の管理

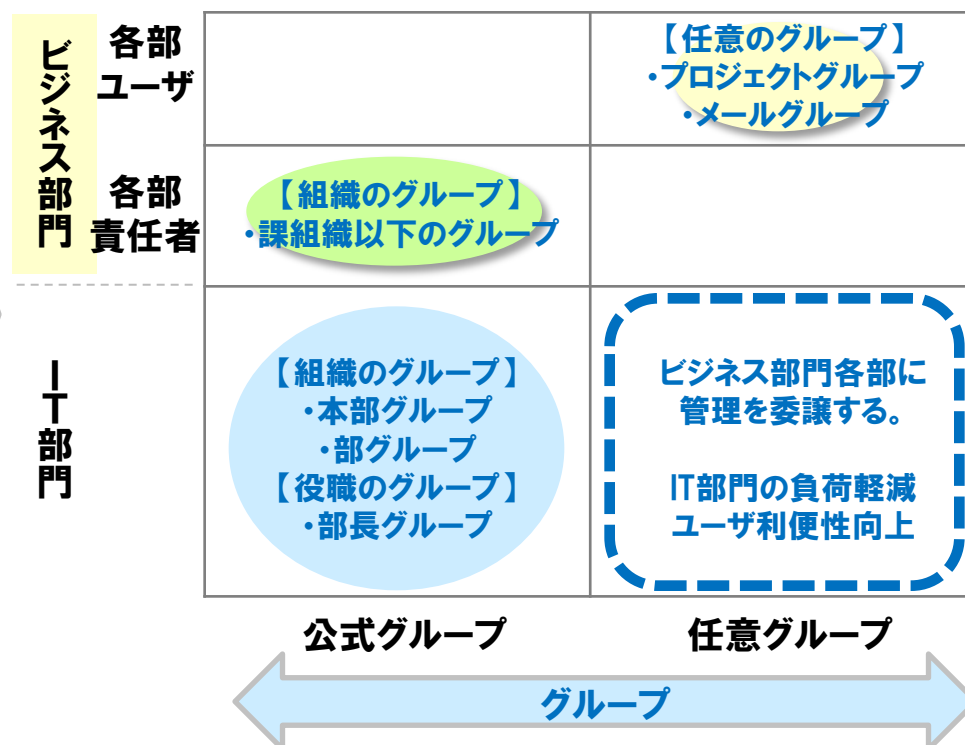
認証・認可情報についても十分な現状整理と、納得のいく管理方針決めが大切

- 管理の委譲によりビジネス部門にもIT部門にもメリットのある管理方法を探っていく。

現状のグループ管理イメージ



今後のグループ管理イメージ(方針)

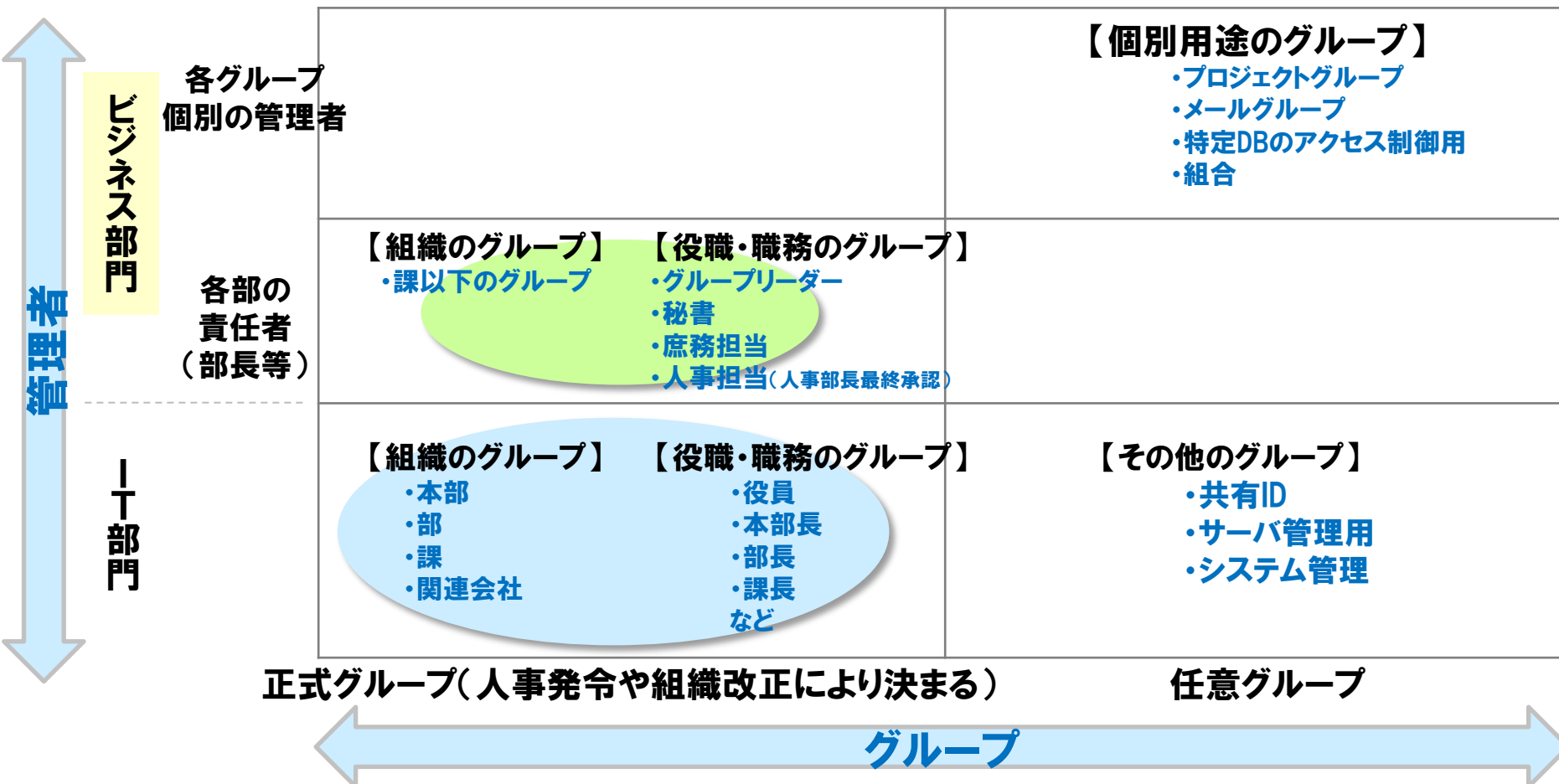


4. 企業内アイデンティティ管理検討における重要なポイント

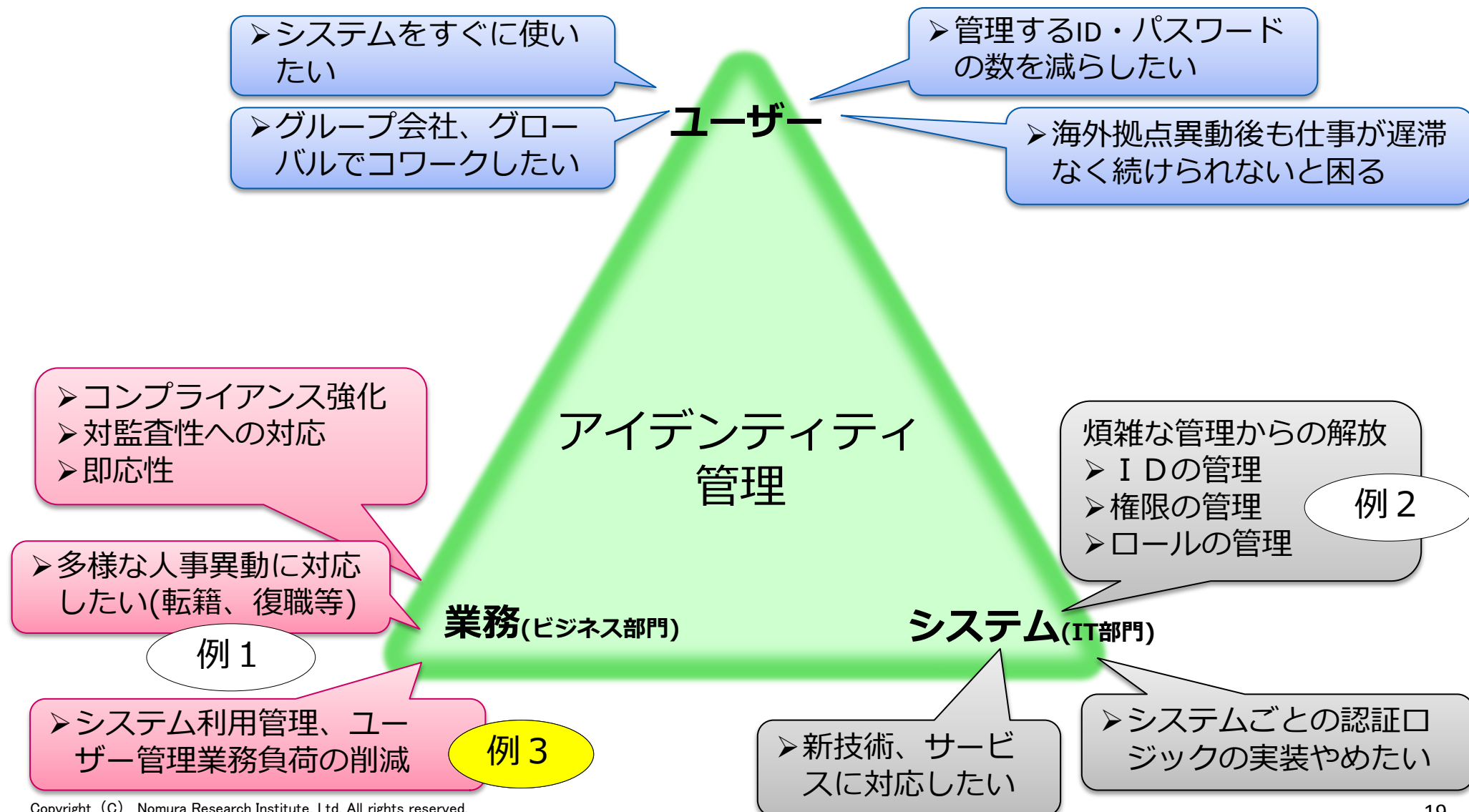
4.2 認証・認可（ロール）情報の管理

管理の委譲によりビジネス部門にもIT部門にもメリットのある管理方法に

方針に則って設定されたグループ管理方法



4. 企業内アイデンティティ管理検討における重要なポイント 業務、システム、ユーザーの3つの視点で要件を検討・定義する



4. 企業内アイデンティティ管理検討における重要なポイント

4.3 ユーザー登録・管理の主管を巡る攻防

管理の集中と分散のライン引きは、自由度を求めるビジネス部門との対話が大切

No.	システム名	申請方法	利用ワーク名	作業担当	登録パターン
1	Windows(AD)	1-ザ・グループ登録	専用ワークシステムを用いた申請	User-ID申請W/F	IT部門（運用担当）
		ドライブアクセス権	専用ワークシステムを用いた申請	OA関連申請W/F	IT部門（運用担当）
		（定期異動時）	所管部門が管理(1-ザ申請なし)	－	IT部門（運用担当）
2	グループウェア	1-ザ・グループ登録	専用ワークシステムを用いた申請	User-ID申請W/F	IT部門（外部オペレータ）
		メールDBアクセス権	専用ワークシステムを用いた申請	OA関連申請W/F	IT部門（運用担当）
		（定期異動時）	所管部門が管理(1-ザ申請なし)	－	IT部門（外部オペレータ）
3	新グループウェア（クラウド）	1-ザ・グループ登録 アクセス権	専用ワークシステムを用いた申請	OA関連申請W/F	IT部門（運用担当）
4	人事システム	所管部門が管理(1-ザ申請なし)	－	人事部	⑥
5	経理システム ※J-SOX対象	専用ワークシステムを用いた申請	アクセス権管理W/F	経理部	③
6	図面管理システム ※J-SOX対象	専用ワークシステムを用いた申請	アクセス権管理W/F	AAA事業本部	③
7	G連結会計システム ※J-SOX対象	専用ワークシステムを用いた申請	アクセス権管理W/F	財務部	③
8	e-ラーニング	専用ワークシステムを用いた申請	User-ID申請W/F	IT部門（運用担当）	①
9	重要文書管理システム	利用者が直接所管部門に申請	－	総務部	⑤
10	サービス管理システム	利用者が直接所管部門に申請	－	AAA事業本部	⑤
11	開発プログラム管理システム	専用ワークシステムを用いた申請	プログラム統制DB	IT部門（運用担当）	④
12	地図情報システム	各部門内部で申請・登録 （各部門に権限委譲）	－	各部署責任者	⑦
13	書類・図面検索システム	利用者が直接所管部門に申請	－	BBB事業本部	⑤
14	文書管理システム	利用者が直接所管部門に申請	－	IT部門（運用担当）	⑤

4. 企業内アイデンティティ管理検討における重要なポイント

4.3 ユーザー登録・管理の主管を巡る攻防

管理の集中と分散のライン引きは、自由度を求めるビジネス部門との対話が大切

No.	システム名	申請方法	作業担当	登録パターン
1	Windows(AD)	統合認証ポータルワークフローを用いた申請 (一元的に登録、各システムへID連携)	IT部門 (IDM/SSO基盤システムによる自動登録)	
	1-ザ・グループ登録 ドライブアクセス権 (定期異動時)			
2	グループウェア			
	1-ザ・グループ登録 ノートDBアクセス権 (定期異動時)			
3	新グループウェア (クラウド)			
	1-ザ・グループ登録 アクセス権			
4	人事システム	所管部門が管理(1-ザ申請なし)	人事部	⑥
5	経理システム ※J-SOX対象	統合認証ポータルワークフローを用いた申請 (一元的に登録、各システムへID連携)	IT部門 (IDM/SSO基盤システムによる自動登録)	
6	図面管理システム ※J-SOX対象			
7	G連結会計システム ※J-SOX対象			
8	e-ラーニング			
9	重要文書管理システム			
10	サービス管理システム			
11	開発プログラム管理システム			
12	地図情報システム			
13	書類・図面検索システム	利用者が直接所管部門に申請	BBB事業本部	⑤
14	文書管理システム	利用者が直接所管部門に申請	IT部門 (運用担当)	⑤

5. IDM導入にあたっての検討の進め方

システム化計画フェーズの充実した検討がプロジェクトの成否を左右します

- システム化計画フェーズは管理対象となるシステム数、拠点リージョン数によって増減します。

システム化計画フェーズ(2～3ヶ月)

現状把握
/課題分析

システム化
方針検討

システム化
計画策定

- IDMを実現するうえで、**最も重要なフェーズ**。ユーザ企業主体で如何に要求事項を整理し、ベンダーへ正確に伝えることが出来るかによって、**完成するシステムの出来が大きく左右される**

- ID管理に関わる業務・システムの可視化
- 現行業務・システムの問題点・要望事項の抽出
- スケジュール、体制、概算費用、期待効果のまとめ

ベンダ調達フェーズ(1～2ヶ月)

RFP提示

評価基準
策定

提案書作成

提案評価
・契約

- ベンダ調達を行うことによって、以下のメリットが得られる。

- 自社リソースで実施するには負荷が高いパッケージのFit & Gap分析を提案ベンダに依頼できる
- 競争原理が有効に機能し、各社から安価な提案を引き出せる（場合によっては戦略的価格を引き出すことが可能）
- パッケージ優劣のみならず、ベンダーの力量も評価できる
- システム化計画フェーズで算出した概算費用の精緻化が可能

システム導入フェーズ (3～12ヶ月)

要件
定義(詳細)

設計～導入

5. IDM導入にあたっての検討の進め方 スケジュールの一例

作業工程とマイルストーン	20xx年											
	x月		x月				x月				x月	
マイルストーン	▼キックオフ											最終報告▼
タスク1 現状把握/課題分析 ・現状調査（現状業務運用の整理） ・対象システム棚卸し ・課題の分析、要件の洗い出し	現状把握・課題分析 ・現状調査（現状業務運用の整理） ・対象システム棚卸し ・課題の分析、要件の洗い出し											
タスク2 システム化方針検討 ・システム化の方針検討 ・システム要求仕様の検討 ・新業務フローの検討 ・システム移行方針の検討	システム化方針検討 ・システム化の方針検討 ・システム要求仕様の検討 ・新業務フローの検討 ・システム移行方針の検討											
タスク3 システム化計画策定 ・システム化スケジュール・体制の検討 ・システム化計画書の作成 ・システム化概算費用のまとめ	システム化計画策定 ・システム化スケジュール・体制の検討 ・システム化計画書の作成 ・システム化概算費用のまとめ											

6. まとめ

■ IDMが注目される背景

- 業務の効率化
- 法規制への対応
- IT環境の変化
- 事業変化への対応

■ 企業内アイデンティティ管理への要求

- 事業成長性の要求・・・事業拡大、事業提携、M&A…（等を起因とするユーザの多様性拡大）
- 事業効率性の要求・・・運用効率向上、ID連携、デバイスの多様化、クラウドサービス利用
- 事業安定性の要求・・・コンプライアンス強化、監査対応

■ 企業内アイデンティティ管理のあるべき姿

- 認証基盤＋アイデンティティ管理

■ 企業内アイデンティティ管理検討における重要なポイント

- 業務（ビジネス部門）、システム（IT部門）、ユーザーの3つの視点で要件を検討する
 - 多様化しているIDライフサイクルをきちんと把握
 - 現状の認証・認可情報、そして仕組みを十分に整理し、納得いく管理方針を
 - ID管理の集中、分散のライン引きはビジネス部門と対話を重ねて納得のいくゴールを

NRI

未来創発

Dream up the future.