野村総合研究所

企業内アイデンティティ管理について

2014年12月17日 (水)

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

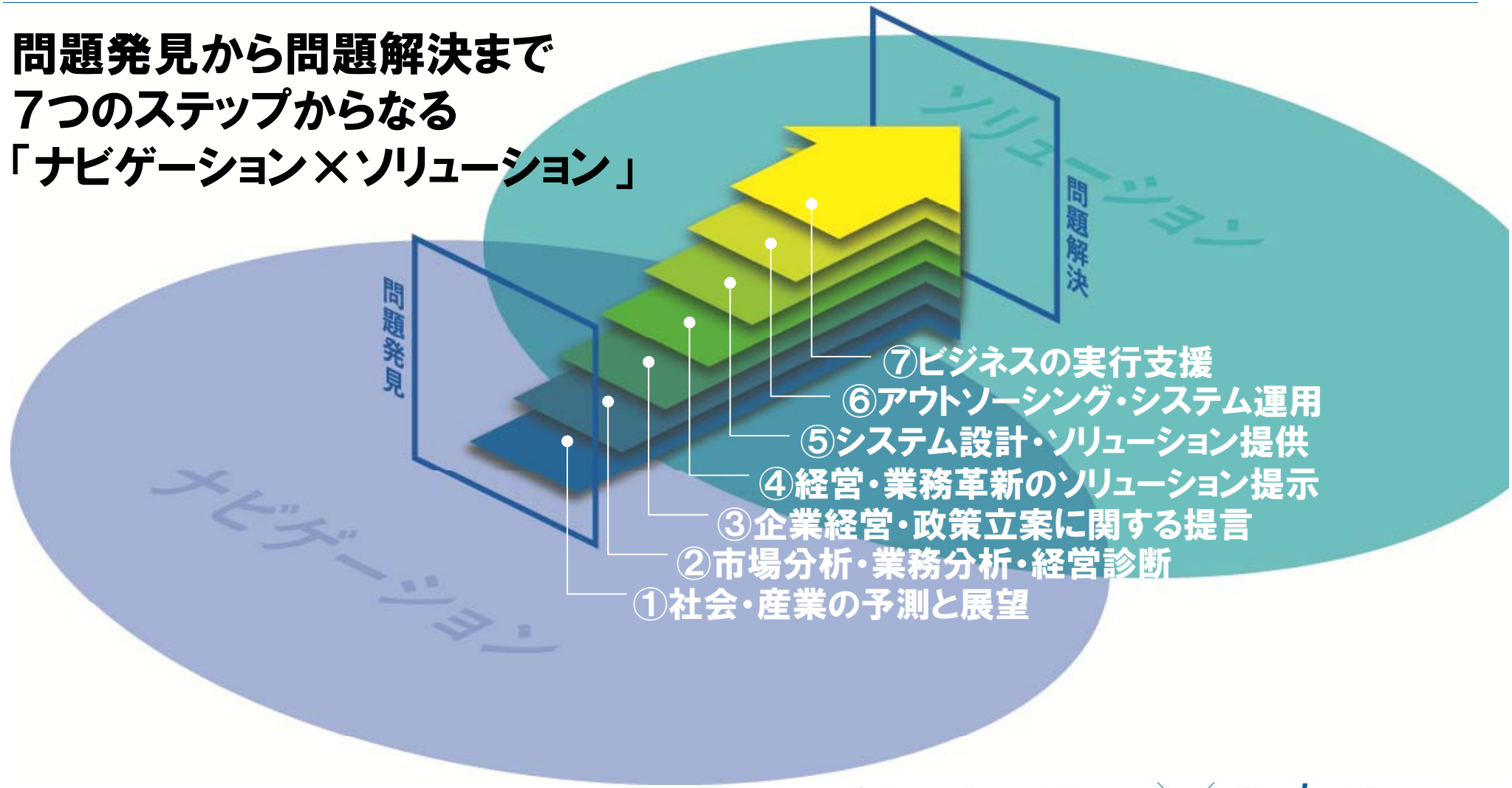
堀崎　修一

〒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

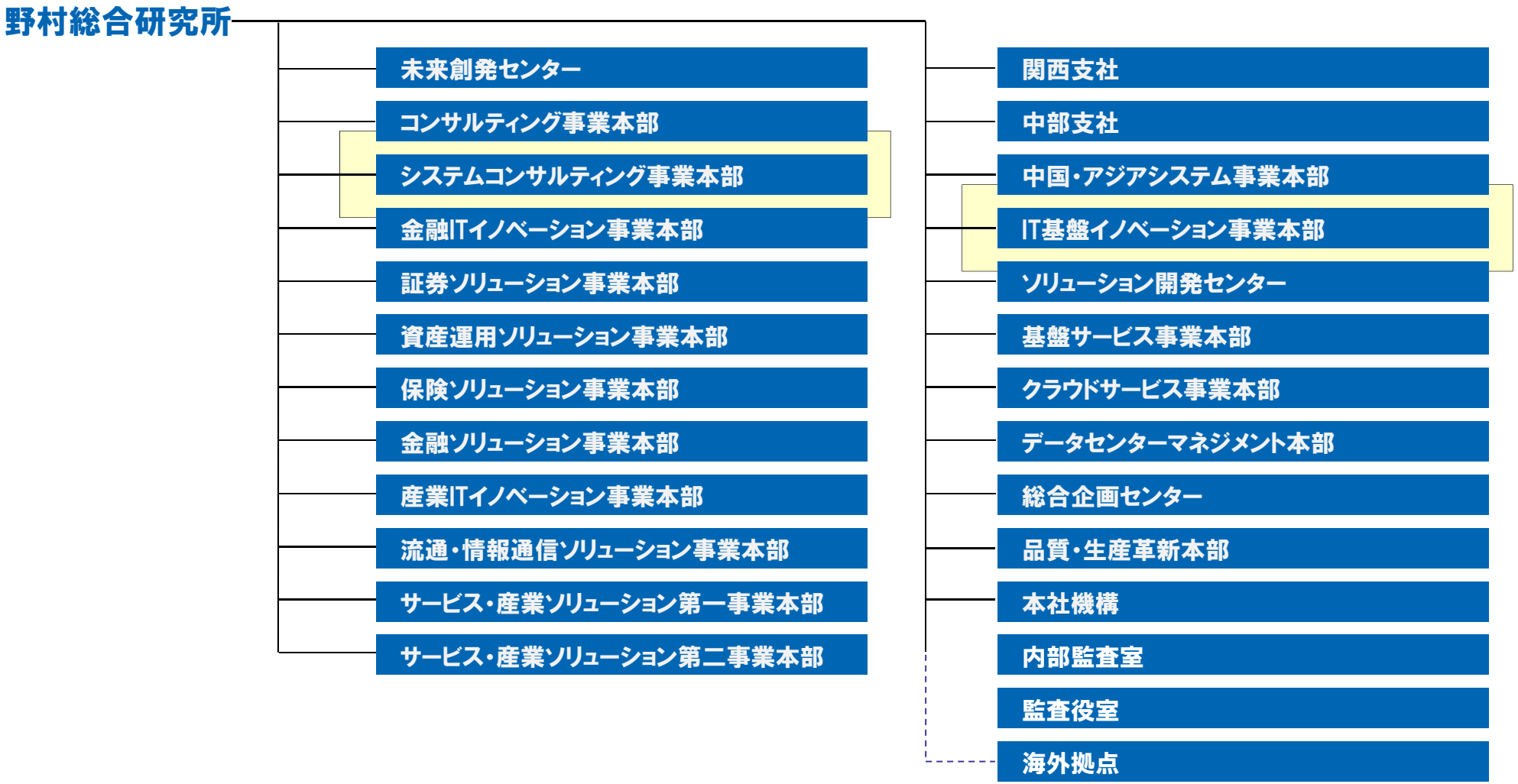
- 金融ＩＴコンサルティング部
- 産業ＩＴコンサルティング部
- 社会ＩＴコンサルティング部

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



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

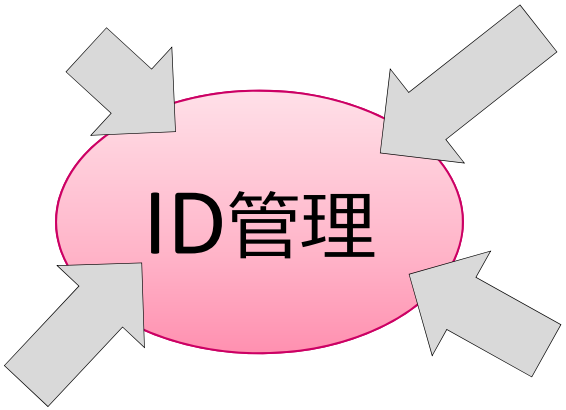
- グループ企業間あるいはグローバル規模でのコワーク、システム利用頻度の増加
- 企業合併（M&A)、多様な人材登用、活用　・・・　あるとき急にユーザーが増える！
- 社内認証基盤統合、社内システムの統合　・・・　急に運用管理対象となるシステムが増える！

２．企業内アイデンティティ管理への要求（２つの方向性）

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。

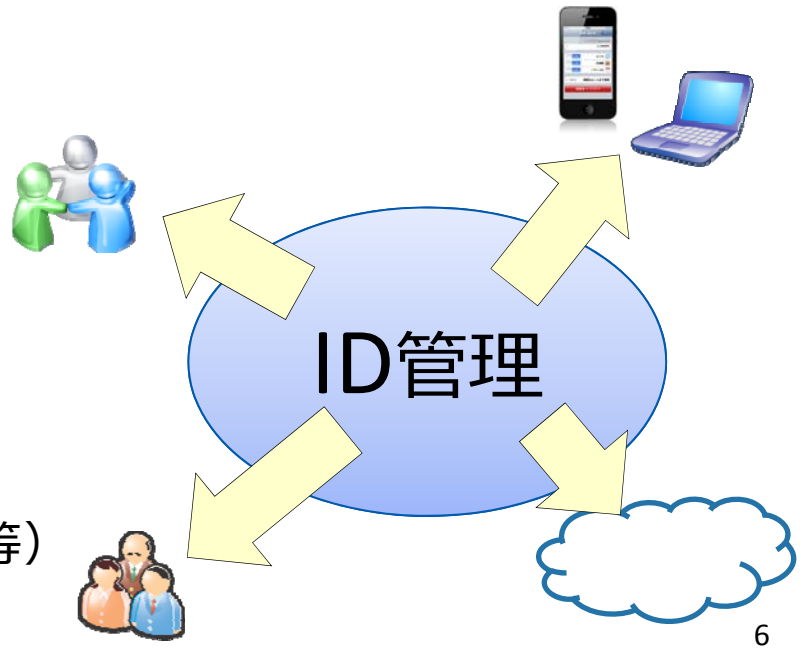
■規制・ルール遵守強化の方向

- パスワードポリシーの強化
- 退職者、契約切れ派遣社員などのＩＤの速やかな削除
- ＩＤの追加、変更、削除、権限付与といったフローによる承認（対監査性の向上）
- 監査ログ、監査レポートの対応

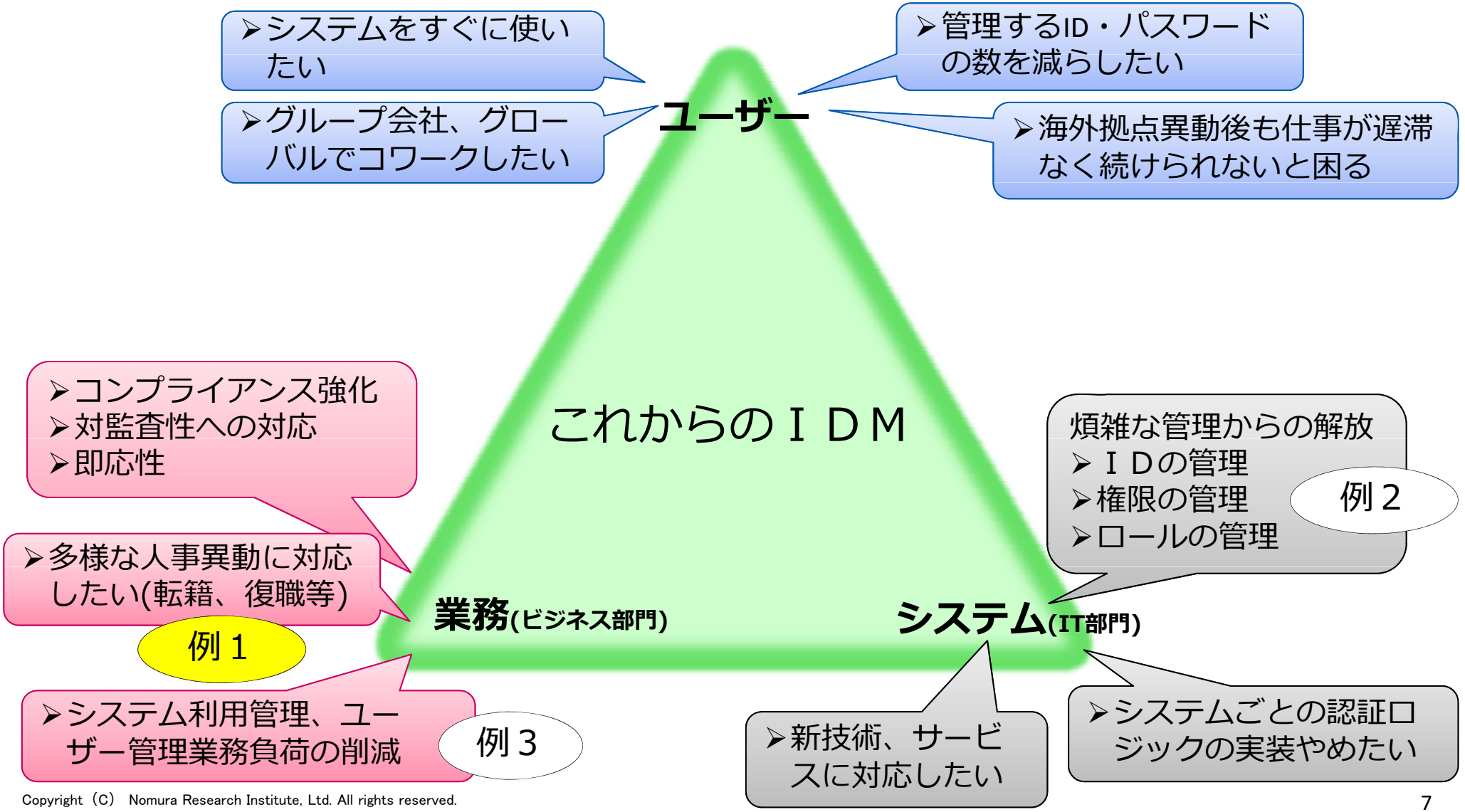


■利用拡大の方向

- システムの派遣社員、パートナー、グループ企業、グローバルなどへの利用範囲拡大
- グループ企業・グローバルでの人材流通を支えるＩＤMの必要性
- 様々な端末でのシステム利用（モバイル、スマートフォン、タブレット）
- クラウドサービスの活用（Office365,salesforce等）



3．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つの視点で考える

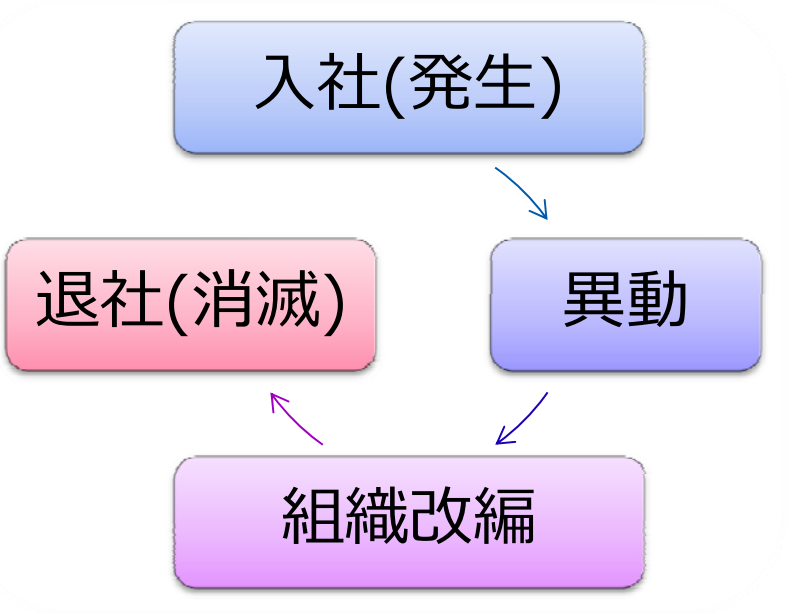


3．企業内アイデンティティ管理検討における重要なポイント

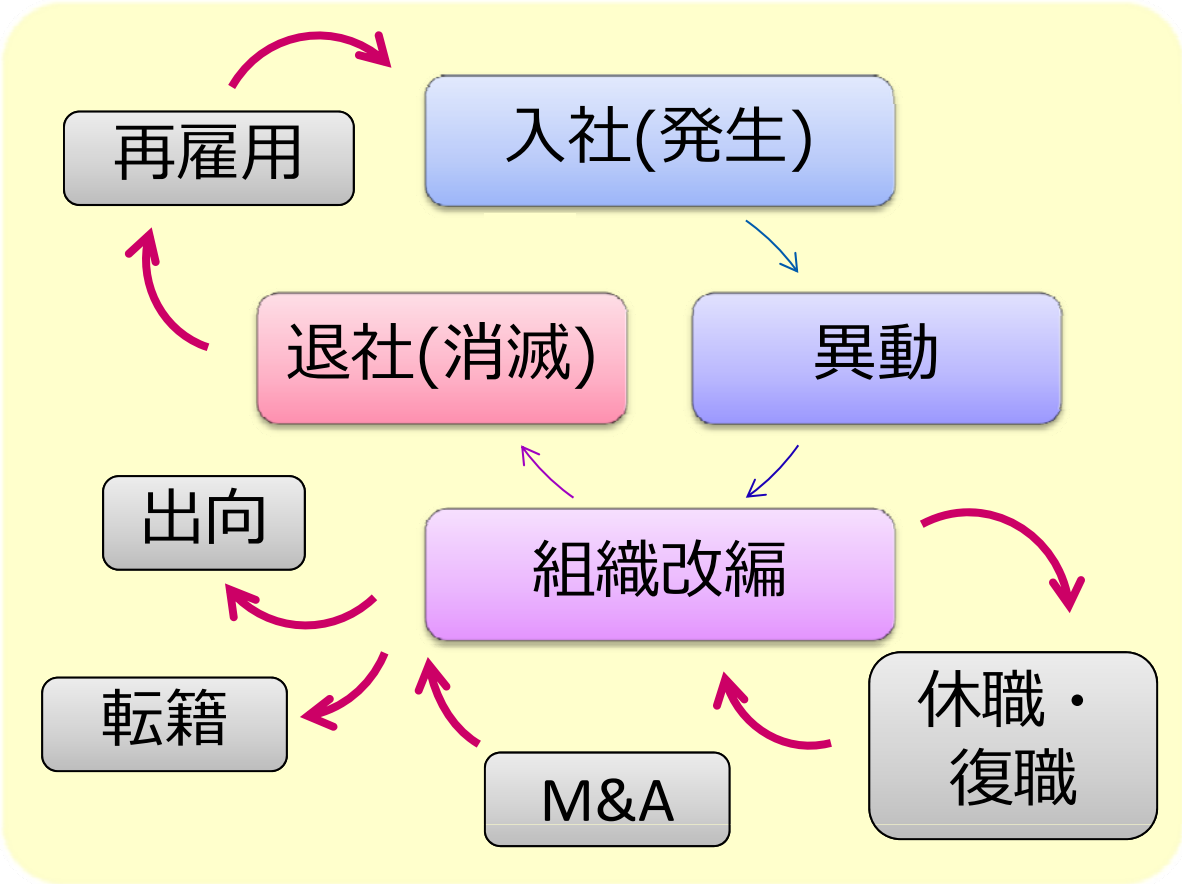
3.1　IDのライフサイクル管理

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



3．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
3.1　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

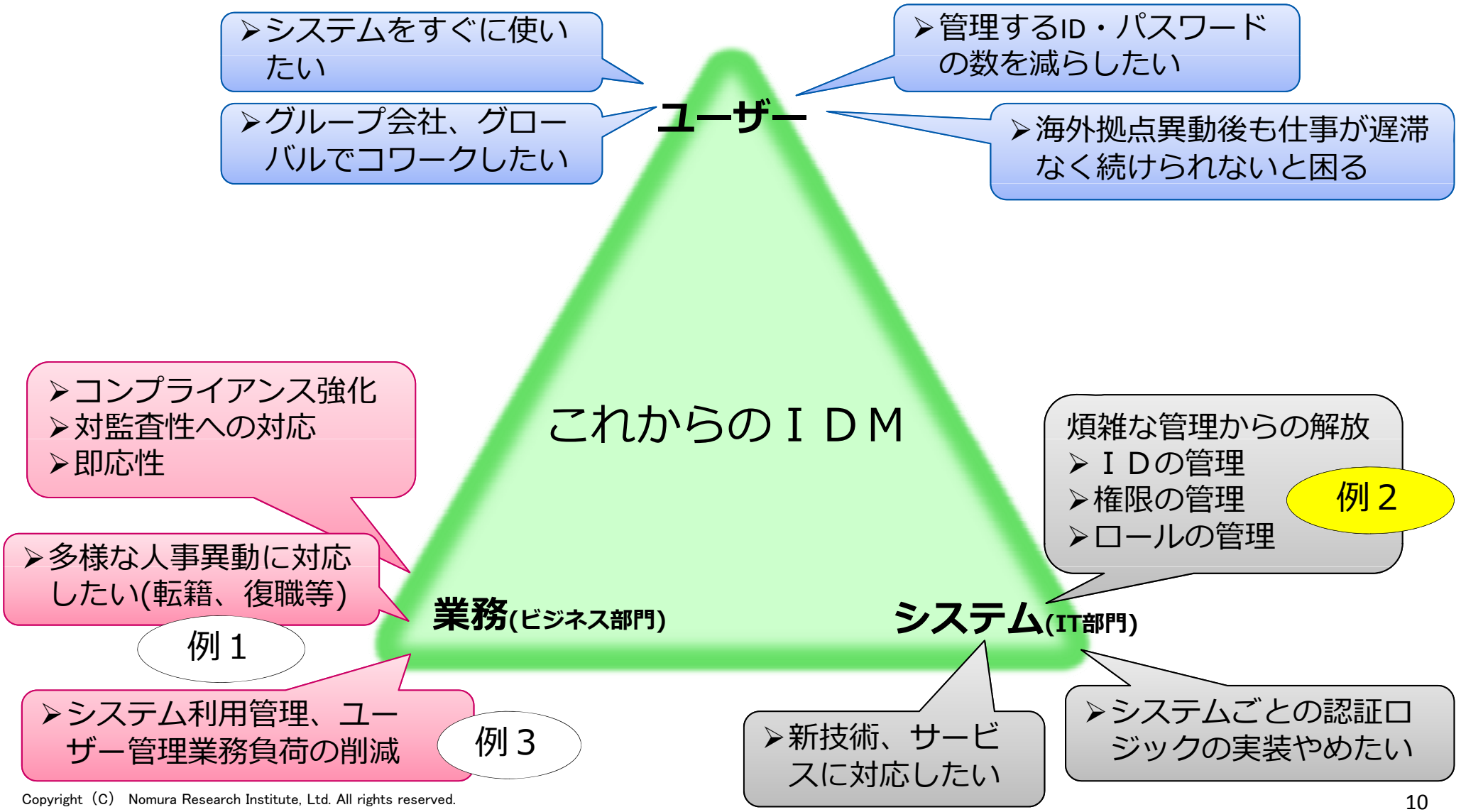
■ 人事イベントをキーにライフサイクル管理を検討した例

人事イベント	利用中のEnterprise ID	新Enterprise IDの発番有無
雇用	–	あり
異動(拠点内)	廃止しない	なし
休職・復職	廃止しない	なし
退職	廃止しない	
異動(別拠点)	廃止しない	
	人事によるIDの引き継ぎが可能な場合、変更無	
転籍	廃止しない	
	人事によるIDの引き継ぎが可能な場合、変更無	
退職・再雇用	廃止しない	
	人事によるIDの引き継ぎが可能な場合、変更無	
出向	廃止しない	
	人事によるIDの引き継ぎが可能な場合、変更無	
兼務	廃止しない	あり
	人事によるIDの引き継ぎが可能な場合、変更無	なし

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

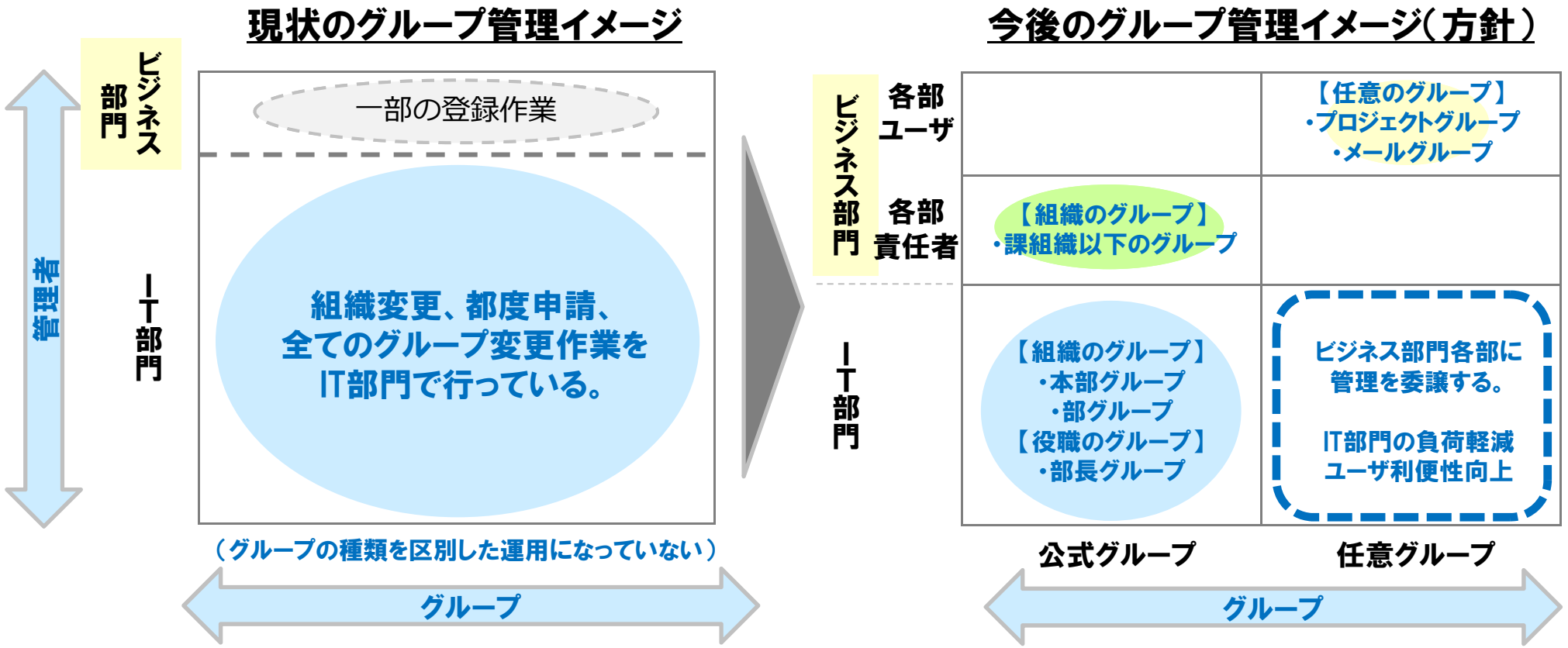
人事以外のイベント	利用中のEnterprise ID	新Enterprise IDの発番有無
不正利用	停止	なし
パスワード流出	停止	なし

3．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



3．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
3.2　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

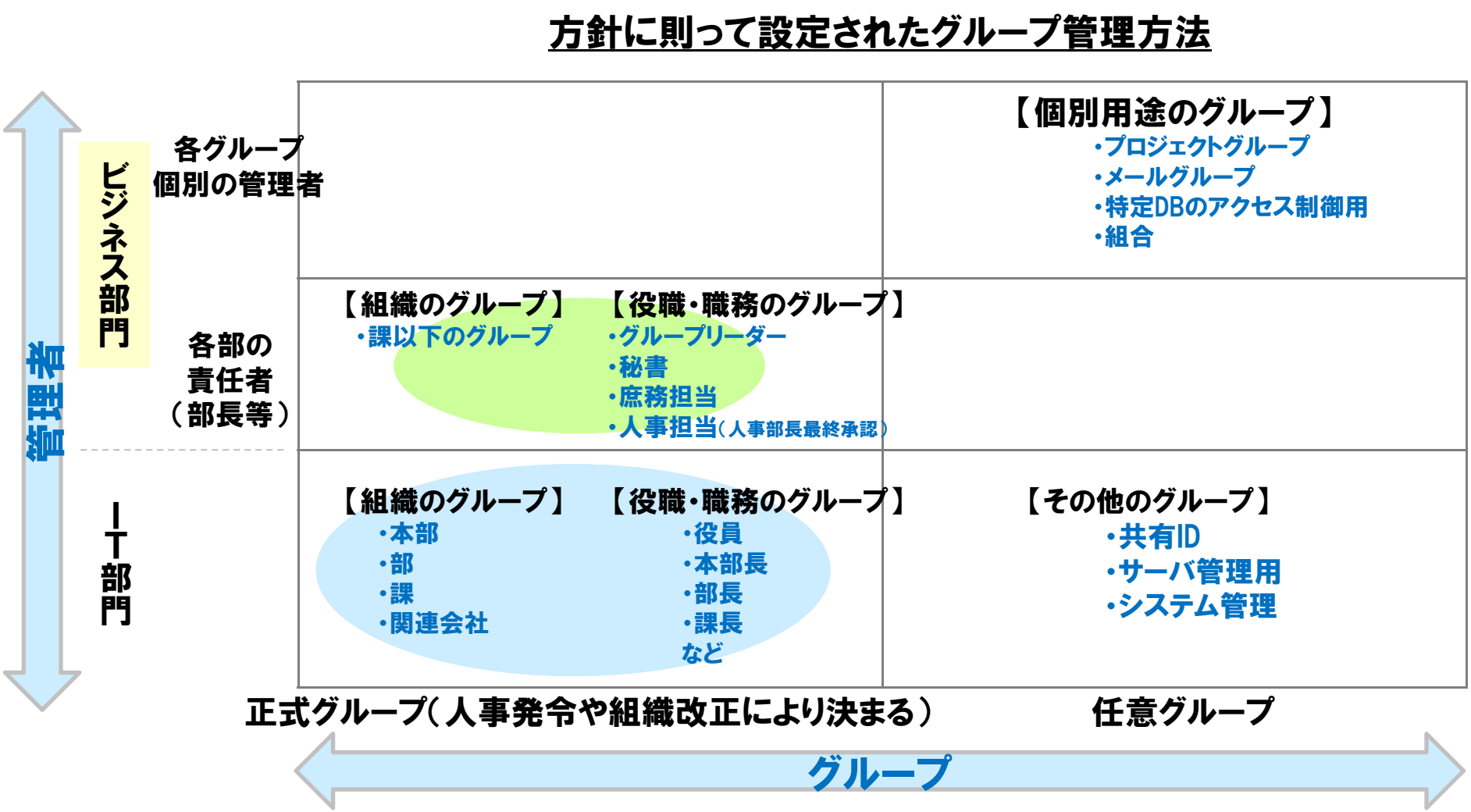
■ 管理の委譲によりビジネス部門にもIT部門にもメリットのある管理方法を探っていく。



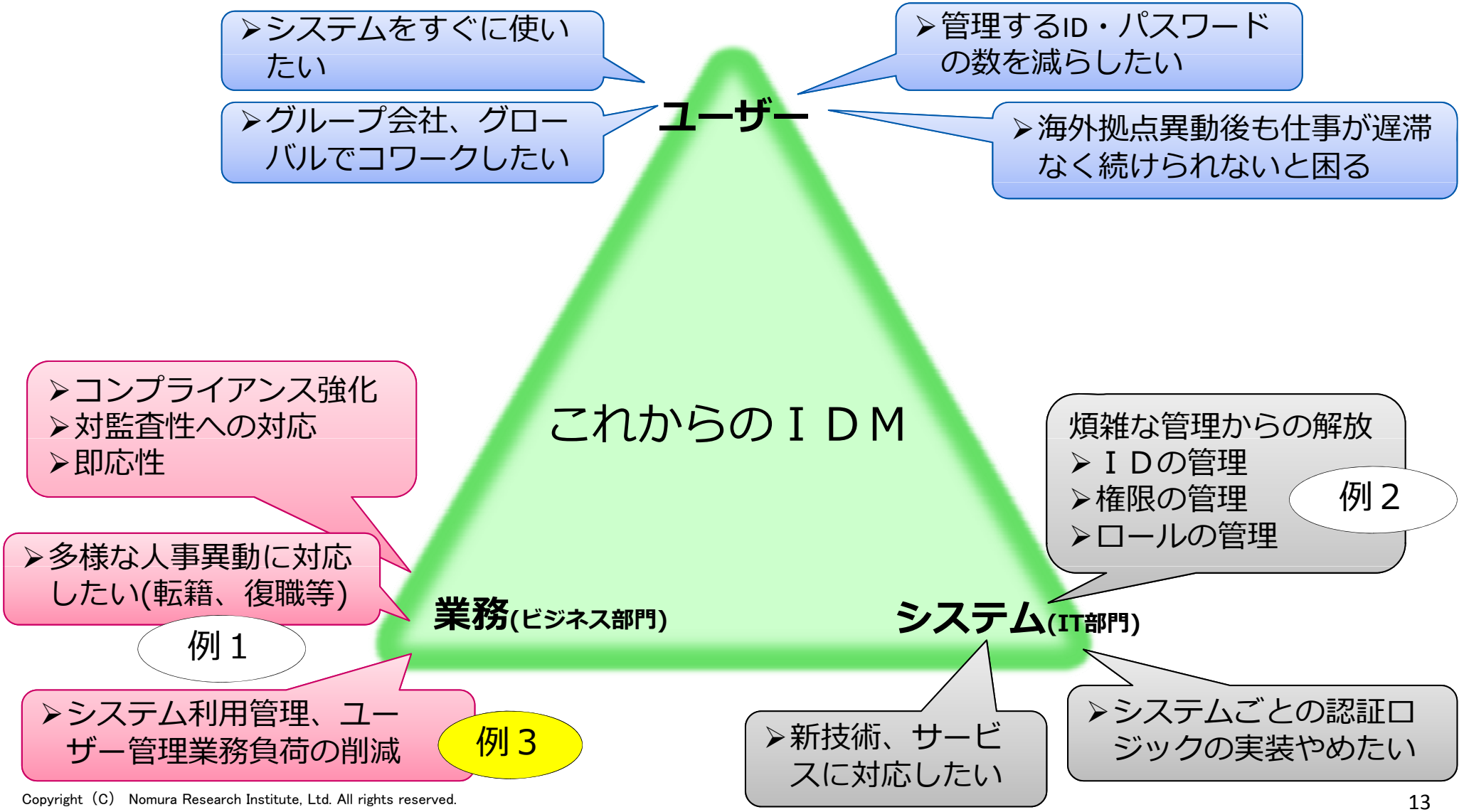
3．企業内アイデンティティ管理検討における重要なポイント

3.2　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



3．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



3．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

3.3　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	利用ﾜｰｸﾌﾛｰ名	作業担当	登録パターン
1	Windows(AD)	ﾕｰｻﾞ・ｸﾞﾙｰﾌﾟ登録	専用ﾜｰｸﾌﾛｰｼｽﾃﾑを用いた申請	User-ID申請W/F	IT部門（運用担当）	①
		ﾄﾞﾗｲﾌﾞｱｸｾｽ権	専用ﾜｰｸﾌﾛｰｼｽﾃﾑを用いた申請	OA関連申請W/F	IT部門（運用担当）	②
		（定期異動時）	所管部門が管理(ﾕｰｻﾞ申請なし)	－	IT部門（運用担当）	⑥
2	グループウェア	ﾕｰｻﾞ・ｸﾞﾙｰﾌﾟ登録	専用ﾜｰｸﾌﾛｰｼｽﾃﾑを用いた申請	User-ID申請W/F	IT部門（外部ｵﾍﾟﾚｰﾀ）	①
		ﾉｰﾂDBｱｸｾｽ権	専用ﾜｰｸﾌﾛｰｼｽﾃﾑを用いた申請	OA関連申請W/F	IT部門（運用担当）	②
		（定期異動時）	所管部門が管理(ﾕｰｻﾞ申請なし)	－	IT部門（外部ｵﾍﾟﾚｰﾀ）	⑥
3	新グループウェア（クラウド）	ﾕｰｻﾞ・ｸﾞﾙｰﾌﾟ登録	専用ﾜｰｸﾌﾛｰｼｽﾃﾑを用いた申請	OA関連申請W/F	IT部門（運用担当）	②
		ｱｸｾｽ権				
4	人事システム		所管部門が管理(ﾕｰｻﾞ申請なし)	－	人事部	⑥
5	経理システム　※J-SOX対象		専用ﾜｰｸﾌﾛｰ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		専用ﾜｰｸﾌﾛｰ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		専用ﾜｰｸﾌﾛｰ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		専用ﾜｰｸﾌﾛｰ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		専用ﾜｰｸﾌﾛｰｼｽﾃﾑを用いた申請	ﾌﾟﾛｸﾞﾗﾑ統制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

3．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

3.3　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)	ﾕｰｻﾞ・ｸﾞﾙｰﾌﾟ登録	統合認証ポータルの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）	
		ﾄﾞﾗｲﾌﾞｱｸｾｽ権			
		（定期異動時）			
2	グループウェア	ﾕｰｻﾞ・ｸﾞﾙｰﾌﾟ登録			
		ﾉｰﾂDBｱｸｾｽ権			
		（定期異動時）			
3	新グループウェア（クラウド）	ﾕｰｻﾞ・ｸﾞﾙｰﾌﾟ登録			
		ｱｸｾｽ権			
4	人事システム		所管部門が管理(ﾕｰｻﾞ申請なし)	人事部	⑥
5	経理システム　※J-SOX対象		統合認証ポータルの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

４．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（２～４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

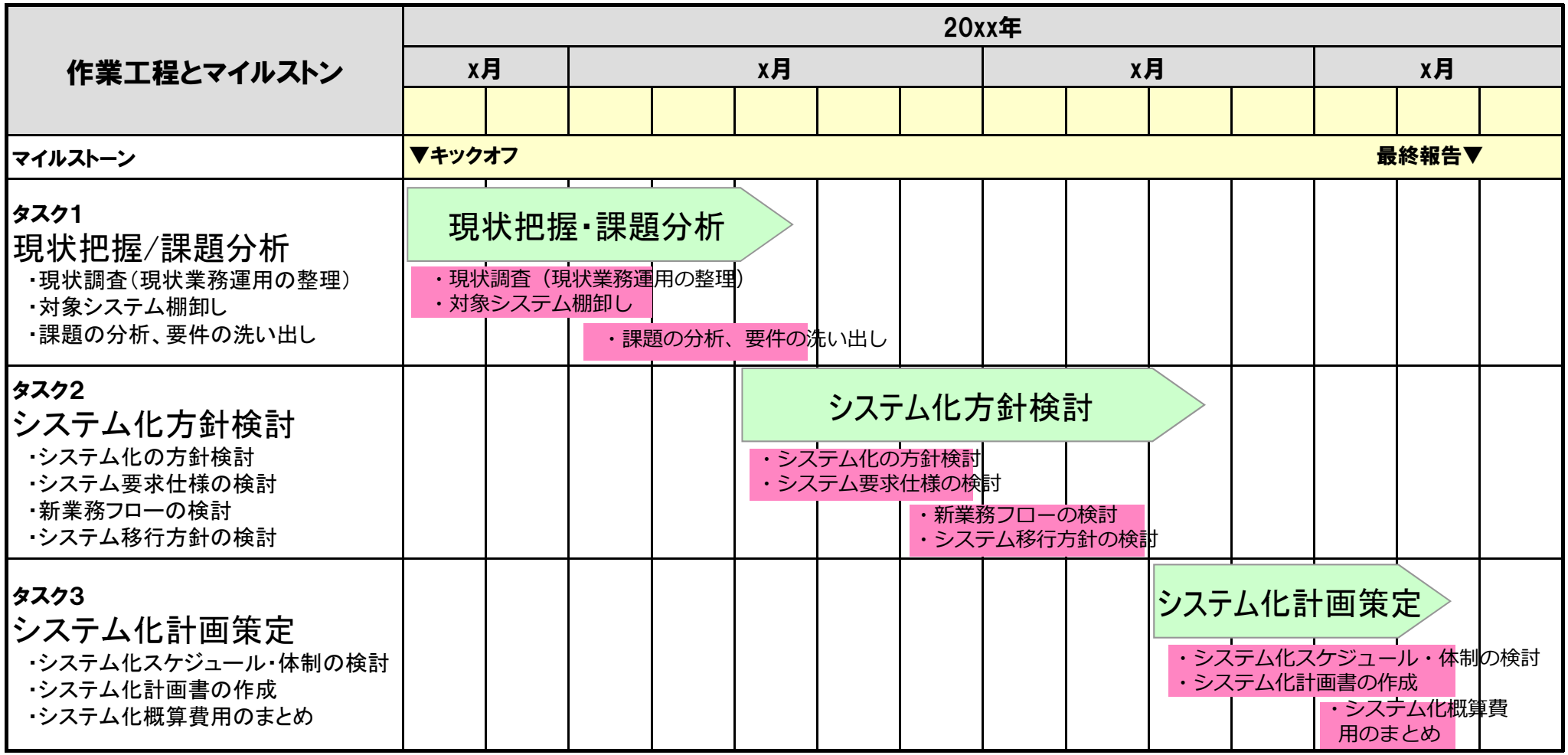
■ベンダ調達を行うことによって、以下のメリットが得られる。

- ●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（４～１２ヶ月）

要件定義（詳細） → 設計～導入

４．IDM導入にあたっての検討の進め方
スケジュールの一例



5．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（２つの方向性）
- 規制・ルール遵守強化の方向
- 利用拡大の方向

■ 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.