

Title	社会制度のゴール指向分析
Author(s)	山本, 修一郎
Citation	
Issue Date	2007-09-07
Type	Presentation
Text version	publisher
URL	<a href="http://hdl.handle.net/10119/8264">http://hdl.handle.net/10119/8264</a>
Rights	
Description	北陸先端科学技術大学院大学 21世紀COEシンポジウム 「検証進化可能電子社会」 = JAIST 21st Century COE Symposium “Verifiable and Evolvable e-Society”, 開催：2007年9月6日～7日，開催場所：キャンパス・イ ノベーションセンター東京 国際会議室(1F)，2007年 9月7日（金），「JAIST-COE シンポジウム：法令工学 の可能性と展望」発表資料

IN+ELLIGEN+

# 社会制度のゴール指向分析

平成19年9月7日

株式会社NTTデータ  
システム科学研究所 所長

フェロー 工学博士 山本修一郎



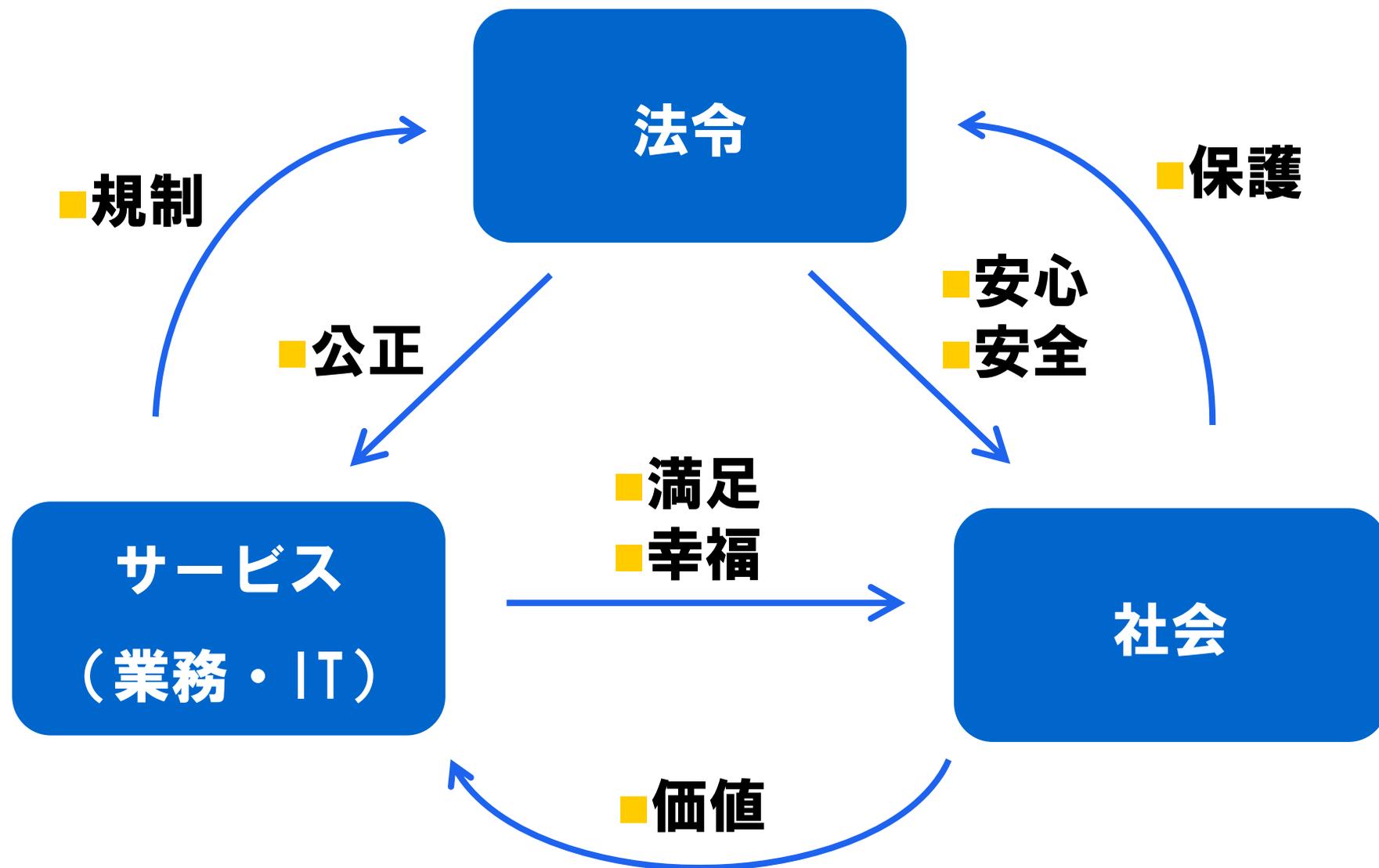
なぜ法令工学が必要なのか？

なぜゴール指向が有効なのか？

どんな研究事例があるのか？

# 1 法令工学がなぜ必要なのか？

(参考)システム要求管理技法—ゴール指向による, ソフト・リサーチ・センター, 2007





これからの20年で、情報システムはますます社会に**“溶け込む”**存在となるだろう。

それにつれて情報システムの**社会的な影響**が増し、安全性や信頼性、相互接続性などの**非機能要件**の部分がより重要になってくる。

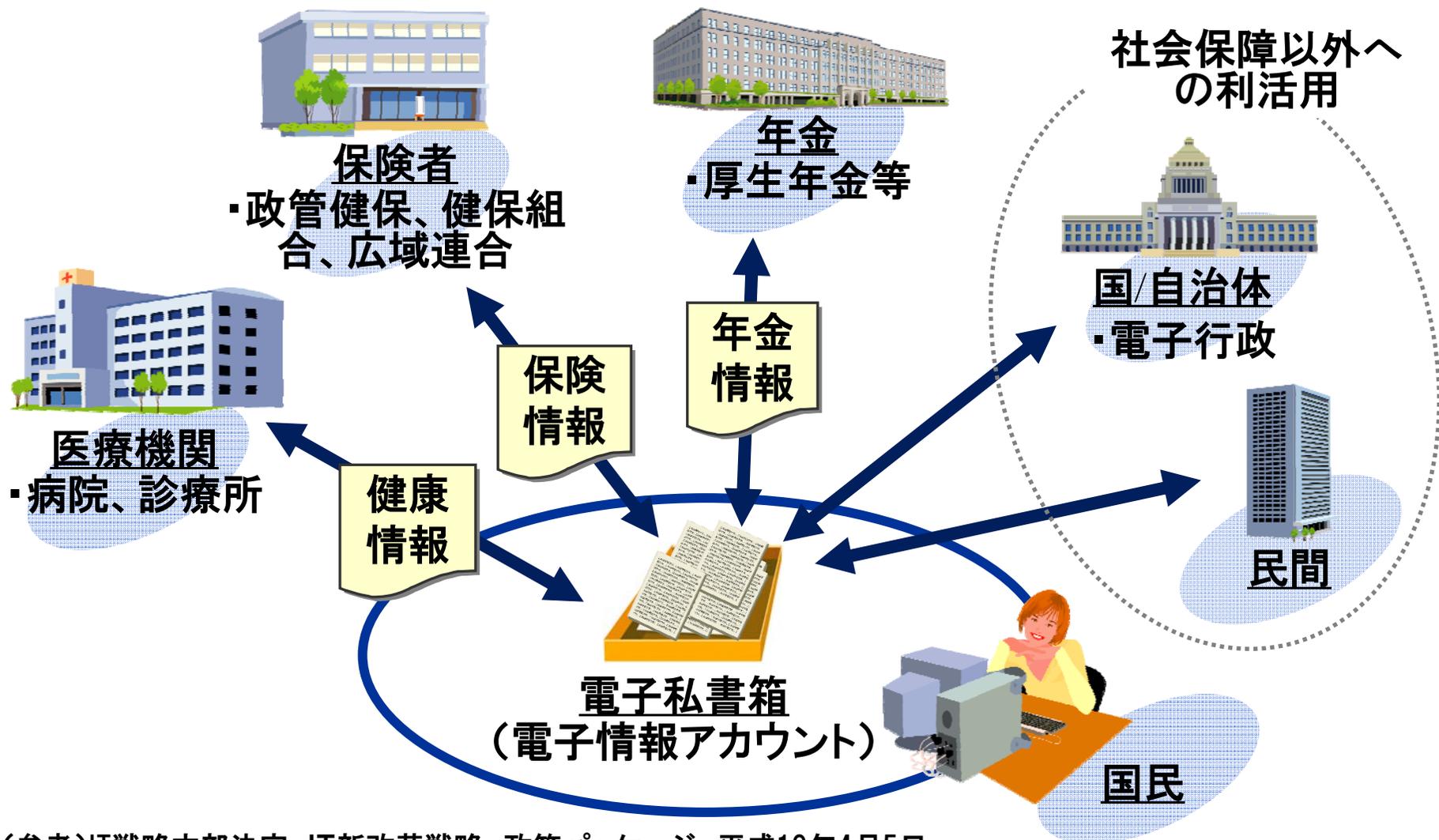
これまでの情報システムでは想定しなくて済んだ事態を考慮しなければいけない可能性も高い。

例えば、**社会制度**を含めた**情報社会のアーキテクチャ**を意識する必要がある出てくるはずだ。おそらく、システム開発は現在よりも、**いっそう複雑**になるだろう。

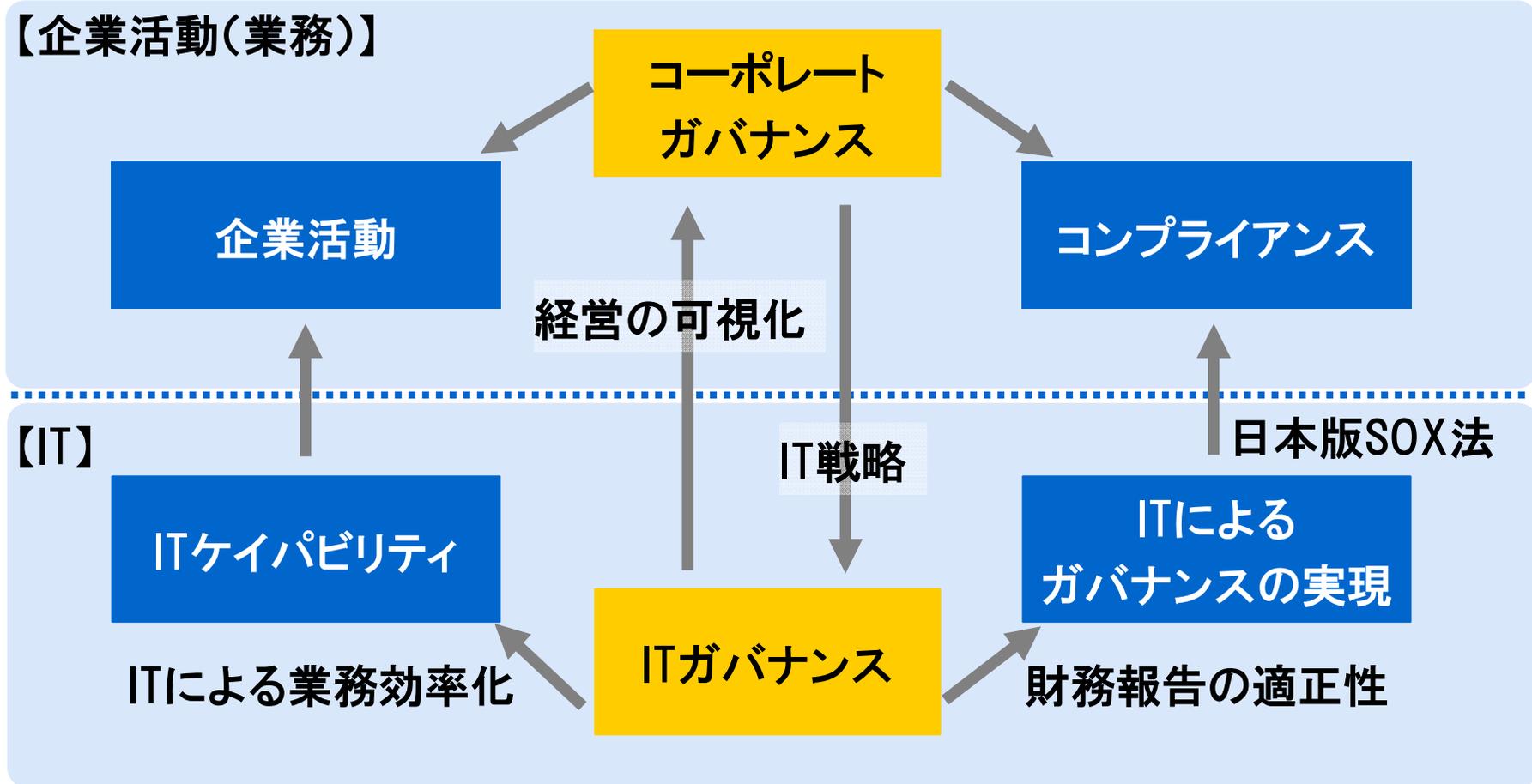
社会に対する**リスク・マネジメント**なども考慮したシステムの開発が必要だ。

参考:「企業システムの開発に”EA2.0”が必要」日経コンピュータ  
2007年1月22日号 p.55

電子私書箱は、自らの情報を一元化し、自らの意思で利活用できる仕組み



(参考)IT戦略本部決定, IT新改革戦略 政策パッケージ, 平成19年4月5日



- COBIT: リスクを強化したITガバナンス成熟度

- 日本版COSOフレームワークに「ITへの対応」追加
- 情報システムに関する内部統制の整備・運用

(注)COBIT:Control Objectives for Information and related Technology  
 COSO:the Committee of Sponsoring Organization of the Treadway Commission

## 2 ゴール指向とは

(参考)システム要求管理技法—ゴール指向による, ソフト・リサーチ・センター, 2007

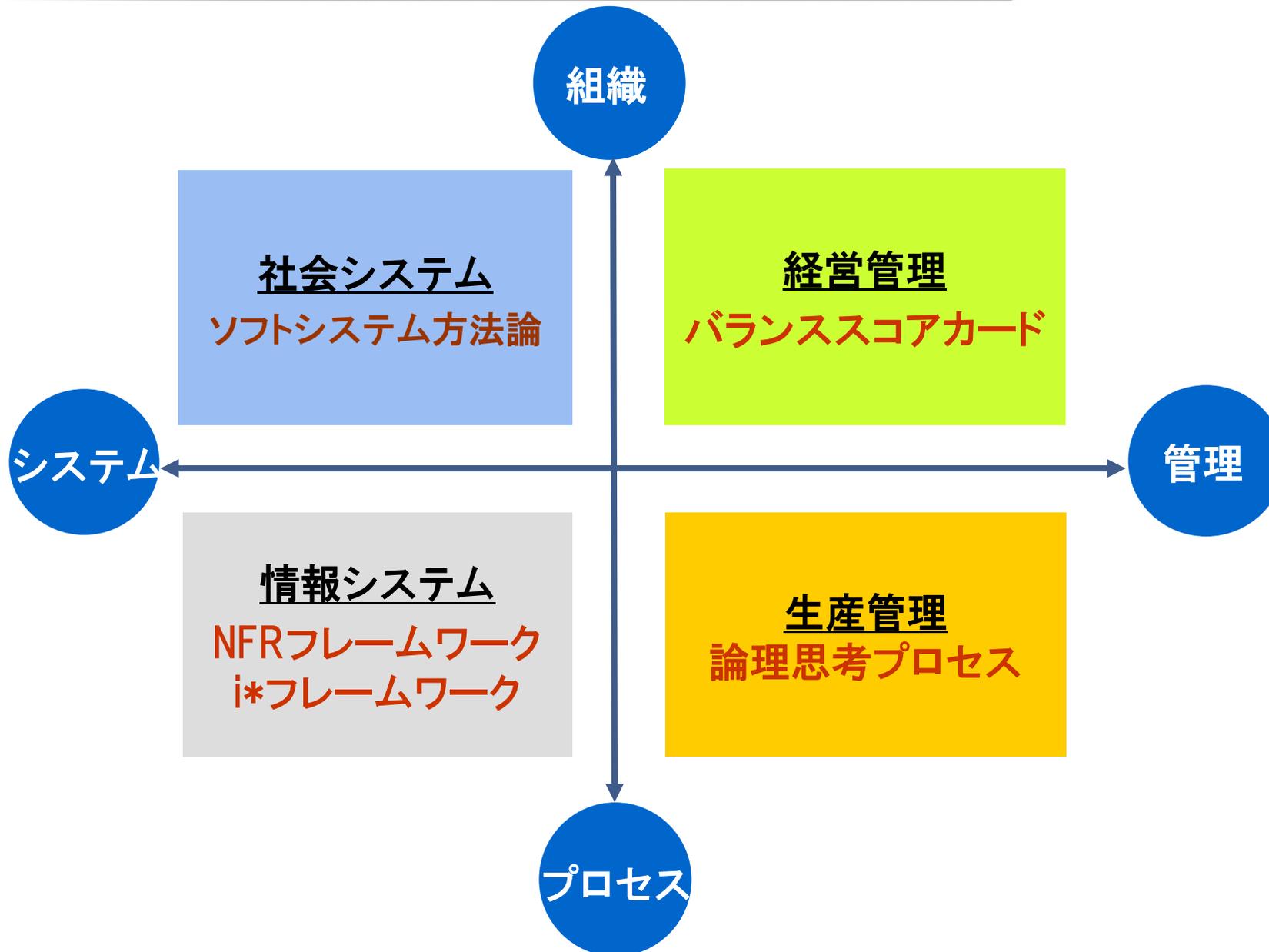


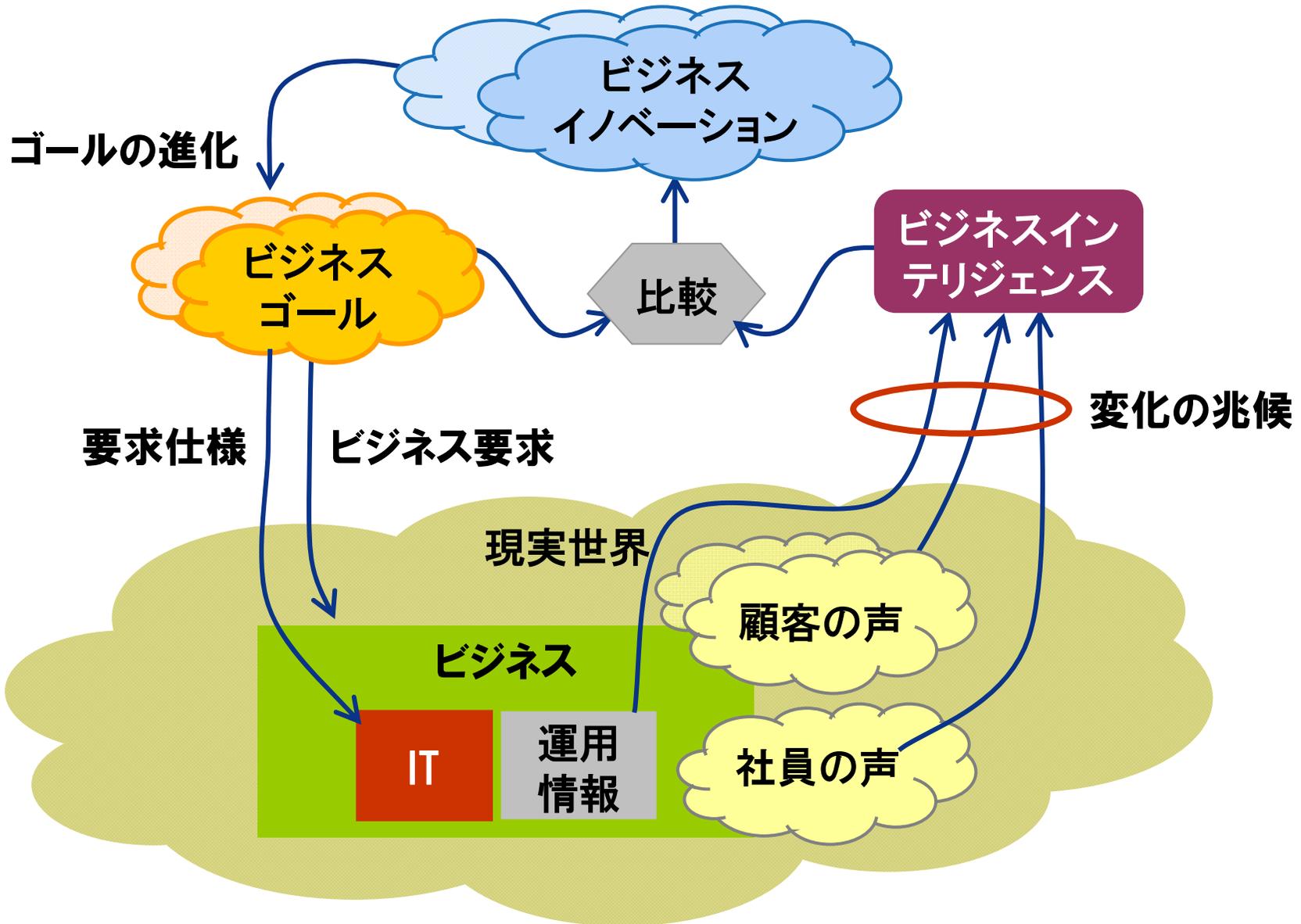
## ■ ゴール

人間活動やITシステムが達成すべき成果としての目標

## ■ ゴール指向手法

人間活動やITシステムの目標とその実現手段や前提条件などとの依存関係を合理的に定義することによりゴールのマネジメントを容易化する

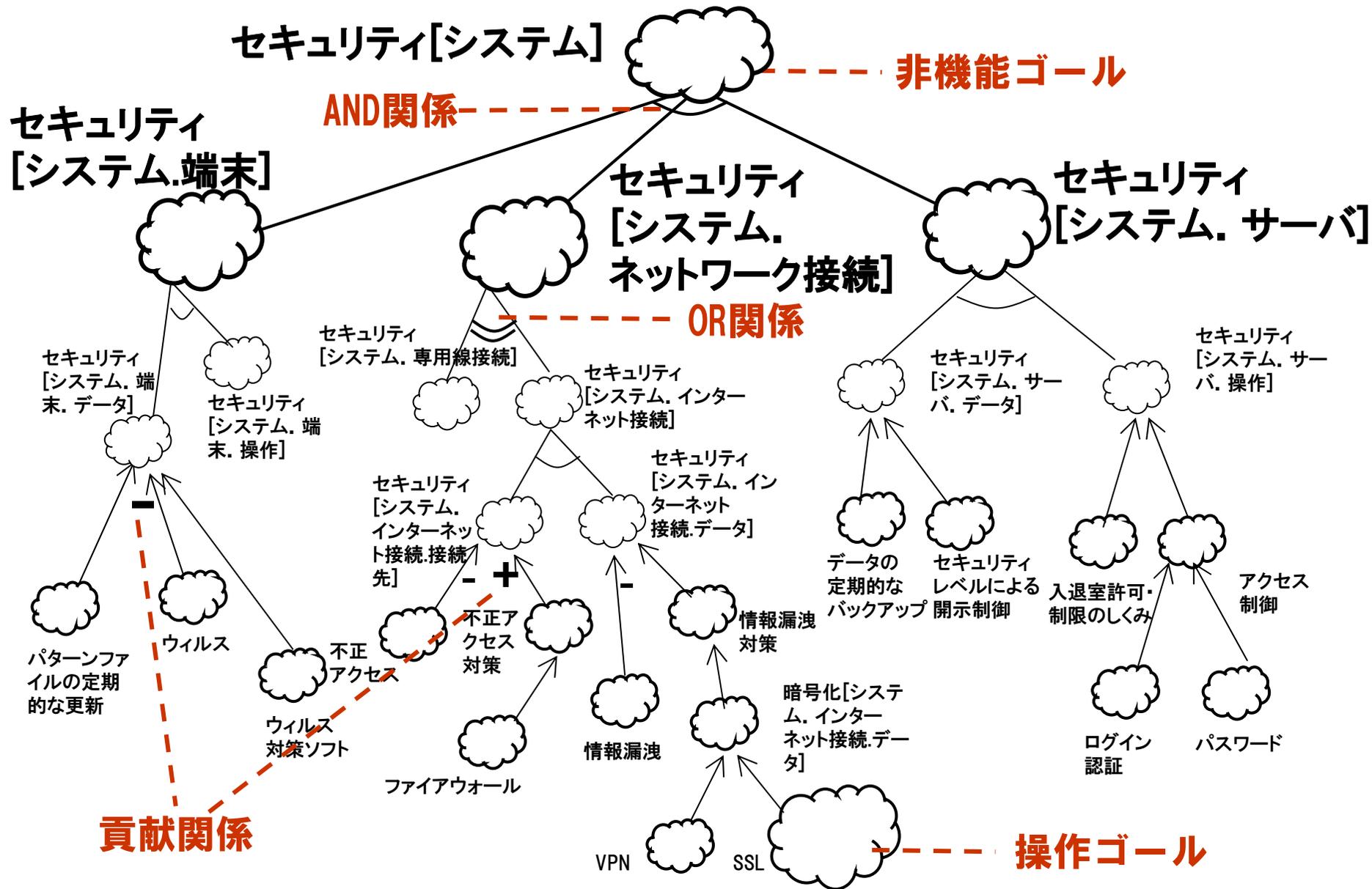




(参考)M.M. Lehman and L.A. Belady, Program Evolution -Process of Software Change, Academic Press, 1985

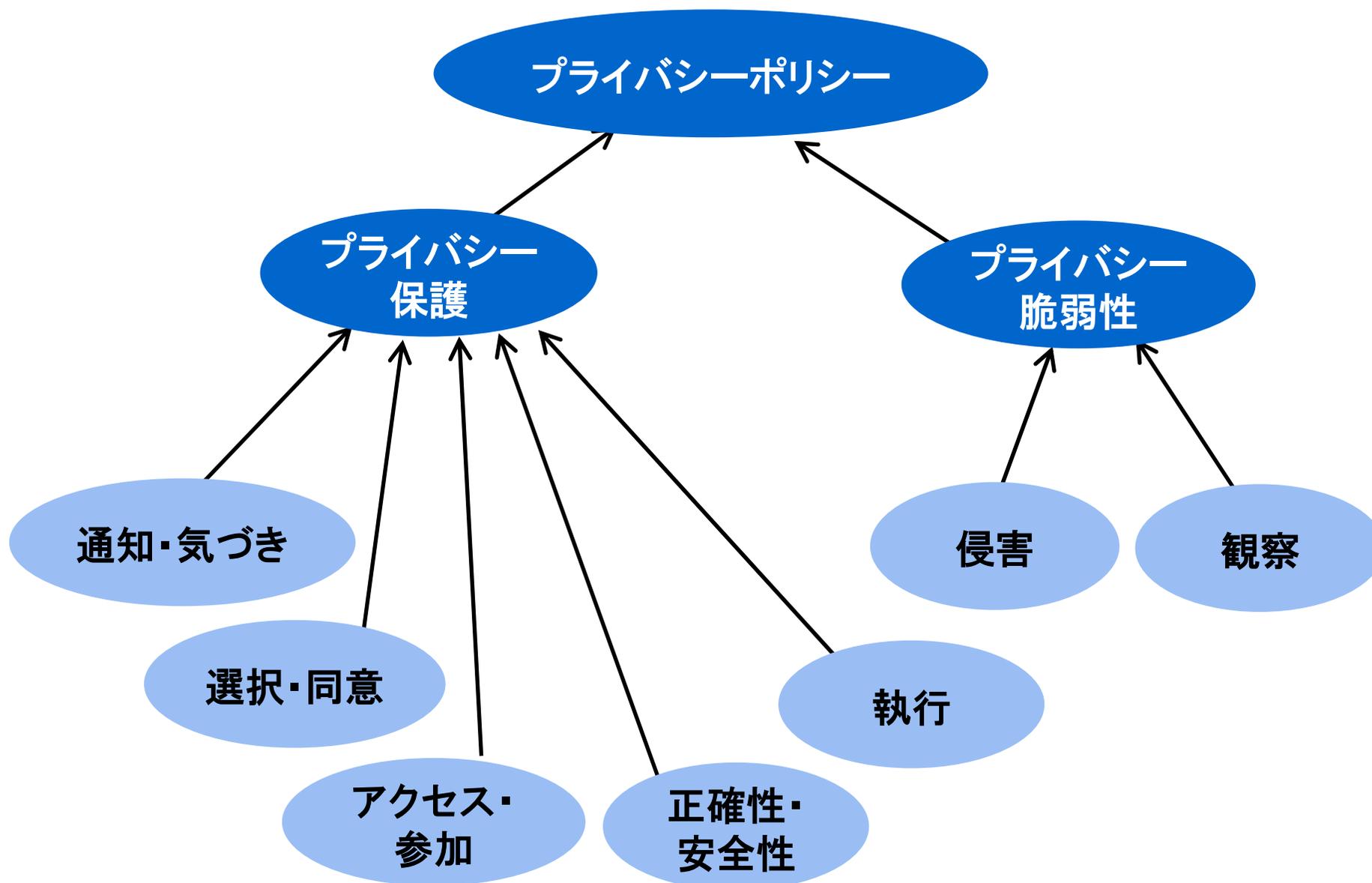
# 3 研究事例

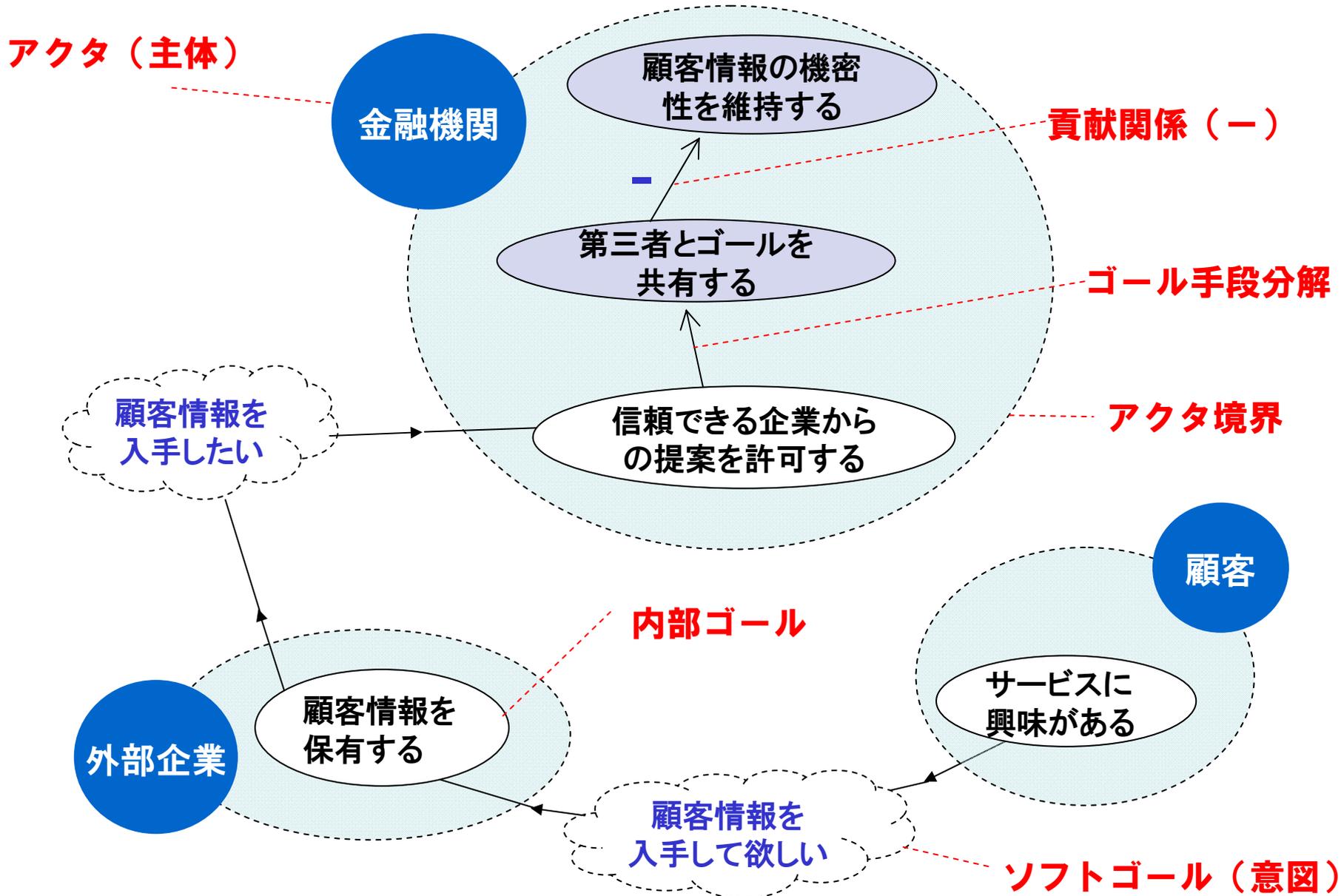
(参考)システム要求管理技法—ゴール指向による, ソフト・リサーチ・センター, 2007



手順	内容
標本の決定	GLBAの対象である9つの金融機関の40のプライバシーポリシードキュメントを抽出
Goal Mining	<ul style="list-style-type: none"> <li>・「動詞」に着目してプライバシーポリシーのゴールを同定</li> <li>・5個のプライバシー記述要素を抽出</li> </ul> Actor、Action word、Subject type、conditions /constraints /circumstance
Goalの洗練	<ul style="list-style-type: none"> <li>・Goal Setの曖昧さ、冗長さ、矛盾の解消</li> <li>・経験則によるGoalの洗練</li> </ul> 経験則の体系化 -ゴールの意味、用語、用法の統一
プライバシー保護と脆弱性の分類	<ul style="list-style-type: none"> <li>・プライバシーポリシーの記述を分類</li> <li>-プライバシー保護とプライバシー脆弱性</li> <li>・分類不能なゴールもある</li> </ul>
ポリシーコンフリクトの同定	i*フレームワークにより、ゴール間の意味的関連性、ステークホルダー間の整合性を確認
読みやすさの評価	プライバシーポリシーを理解できる教育レベルをドキュメントごとに評価 理解には高学歴が必要なものも多い

Anton, A. Earp, J., Bolchini, D., and Jensen, C., Financial Privacy Policies and the Need for Standardization, IEEE Security & Privacy, pp.36-45, 2004





## ゴールレイヤ

プライバシーを保護した  
電子タグビジネスの実現

電子タグ利用者との  
良好な関係の構築

安全な電子タグシステム  
の構築と運用

利用者の認知

利用者の同意

a. 電子タグシステム  
の啓発活動

b. 電子タグシステム  
の存在明示

c. プライバシー情報  
の利用承諾

d. 電子タグシステムへの  
参加選択権付与

e. プライバシー  
情報のセキュリティ確保

f. プライバシー情報  
の適切な管理

g. プライバシー情報  
の濫用禁止

## プランレイヤ

1. 利用者に対  
する説明及び  
情報提供

2. 電子タグタグ  
の社会的利益  
に関する情報  
提供

3. 電子タグ  
タグ装着の  
明示

4. 電子タグ  
リーダーの  
存在の明示

5. 電子タグ  
リーダーの動作  
状況の明示

6. 利用者による  
電子タグ内情報  
の確認

7. プライバシー情報  
利用目的の本人通知

8. プライバシー情報  
の目的外利用の承諾

9. 利用者の同意の  
ない追跡の禁止

10. 電子タグタグ  
の不活性化の  
選択権付与

11. 利用者へ  
の電子タグ利用  
強要の禁止

12. 電子タグ不  
利用による機  
会損失の禁止

13. プライバシー  
情報の正確性確保

14. プライバシー  
情報の損失、毀損、  
改竄、漏洩の防止

15. プライバシー  
情報の第三者開示禁止

16. 情報  
管理者の  
設置

17. 利用者へ  
のプライバ  
シー情報の開  
示

18. 消費者の  
要求以外の条  
件でのプライバ  
シー情報照会  
の禁止

19. 電子タグタグ  
情報とプライバ  
シー情報  
DBとの照会規  
制

ガイドラ  
インを公表

啓発活動  
プログラム  
を実施

電子タグ  
リーダーマッ  
プ

電子タグ存在  
を明記

動作状況表示可  
能な電子タグリー  
ダー

電子タグ内情報  
の確認システム

電子タグサービス  
への参加手続を提  
供

プライバシー情報  
利用承諾システ  
ム

電子タグサービス  
不参加手続を提  
供

Kill Tag

Faraday  
Cage

ID読取  
制御

ID読取防  
御

ID配信  
暗号化

情報照会  
制御

照会結果  
監視

DBアクセ  
ス監視

DBアクセ  
ス制御

処理論理  
制御

個人情報管理  
体制を確立

SSL

Soft Block  
ing

Re-  
Encryption

利用者へのプライバ  
シー情報開示システ  
ム

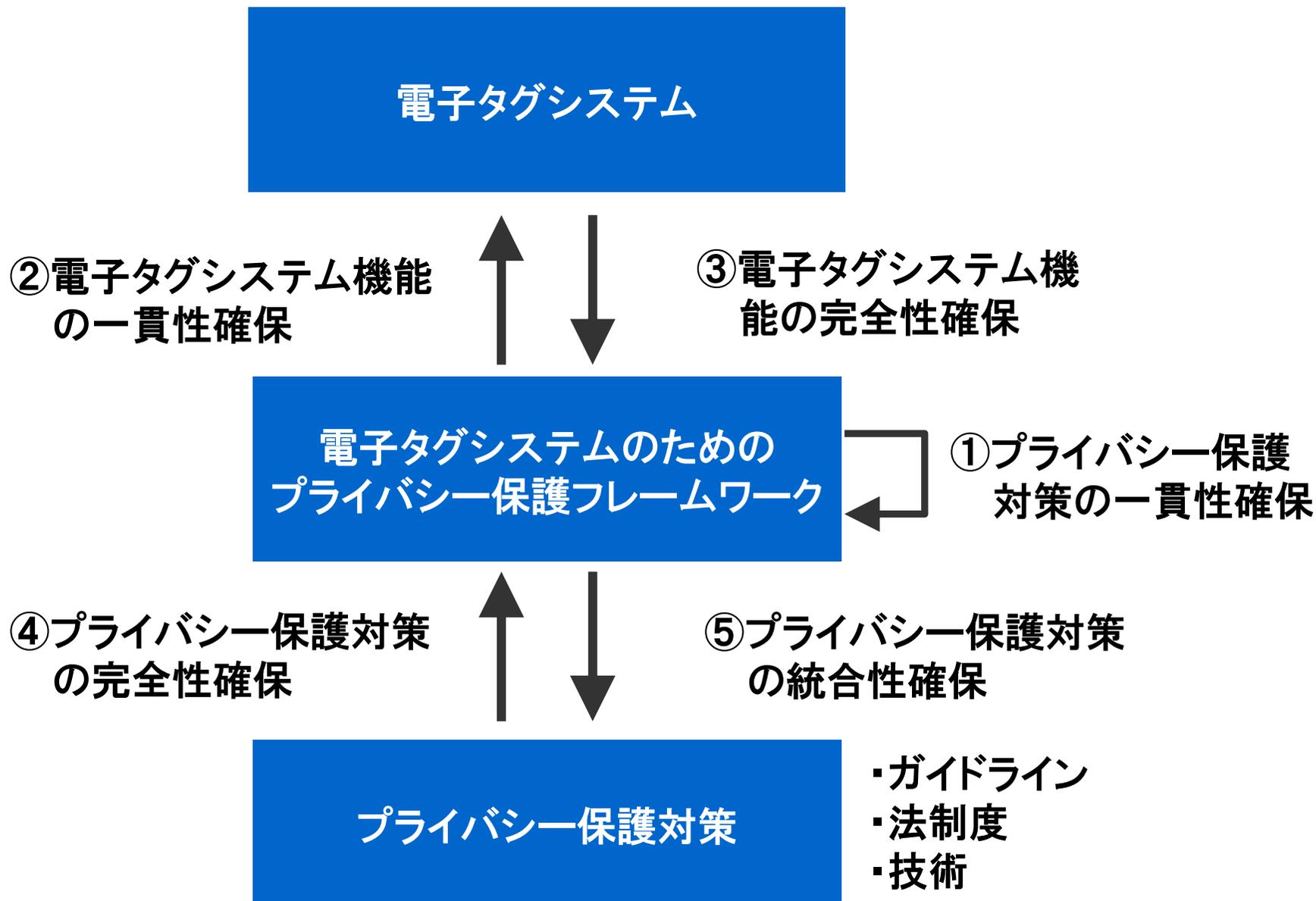
Hash Lock

Bloker Tag

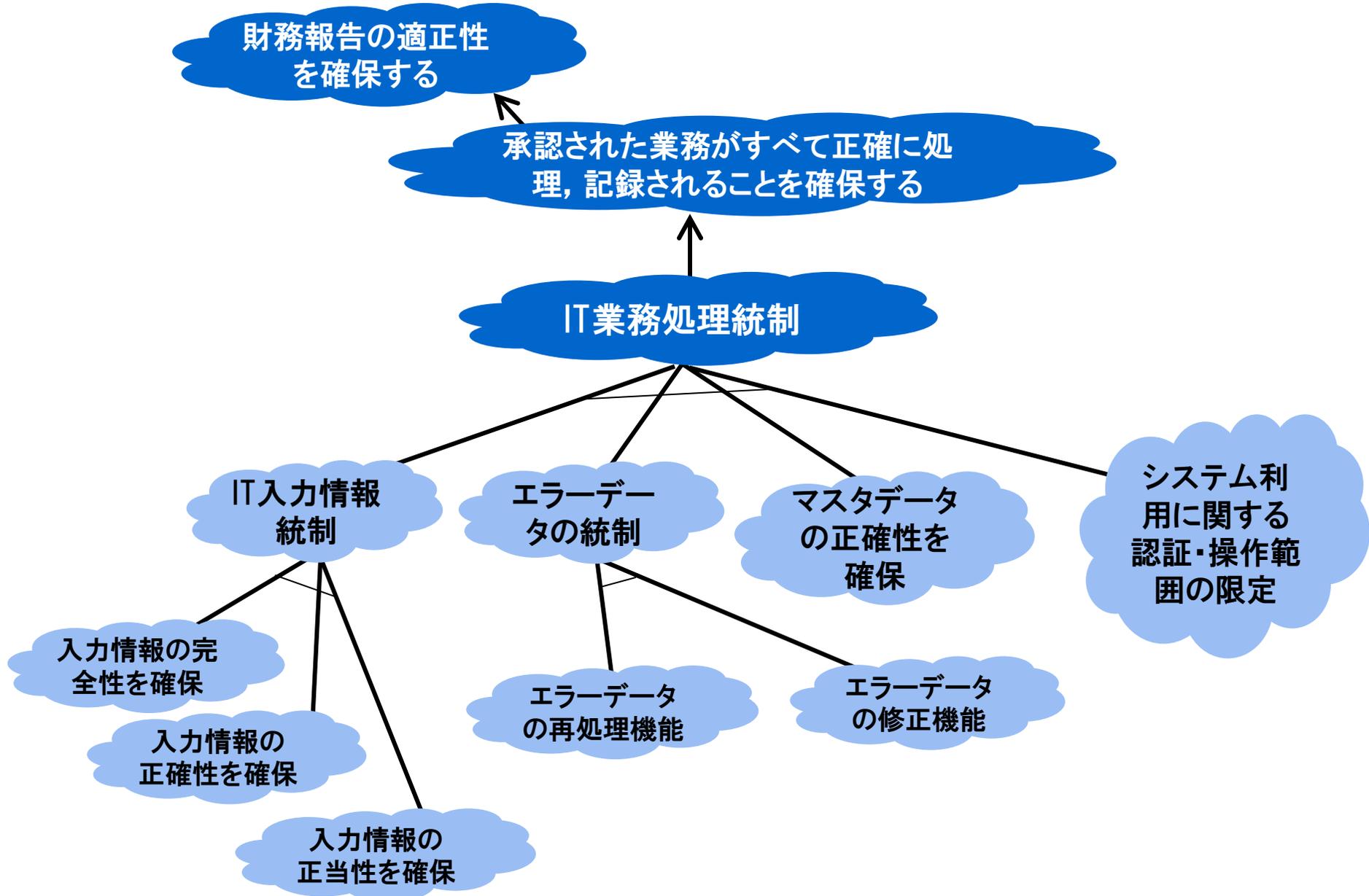
Active  
Jamming

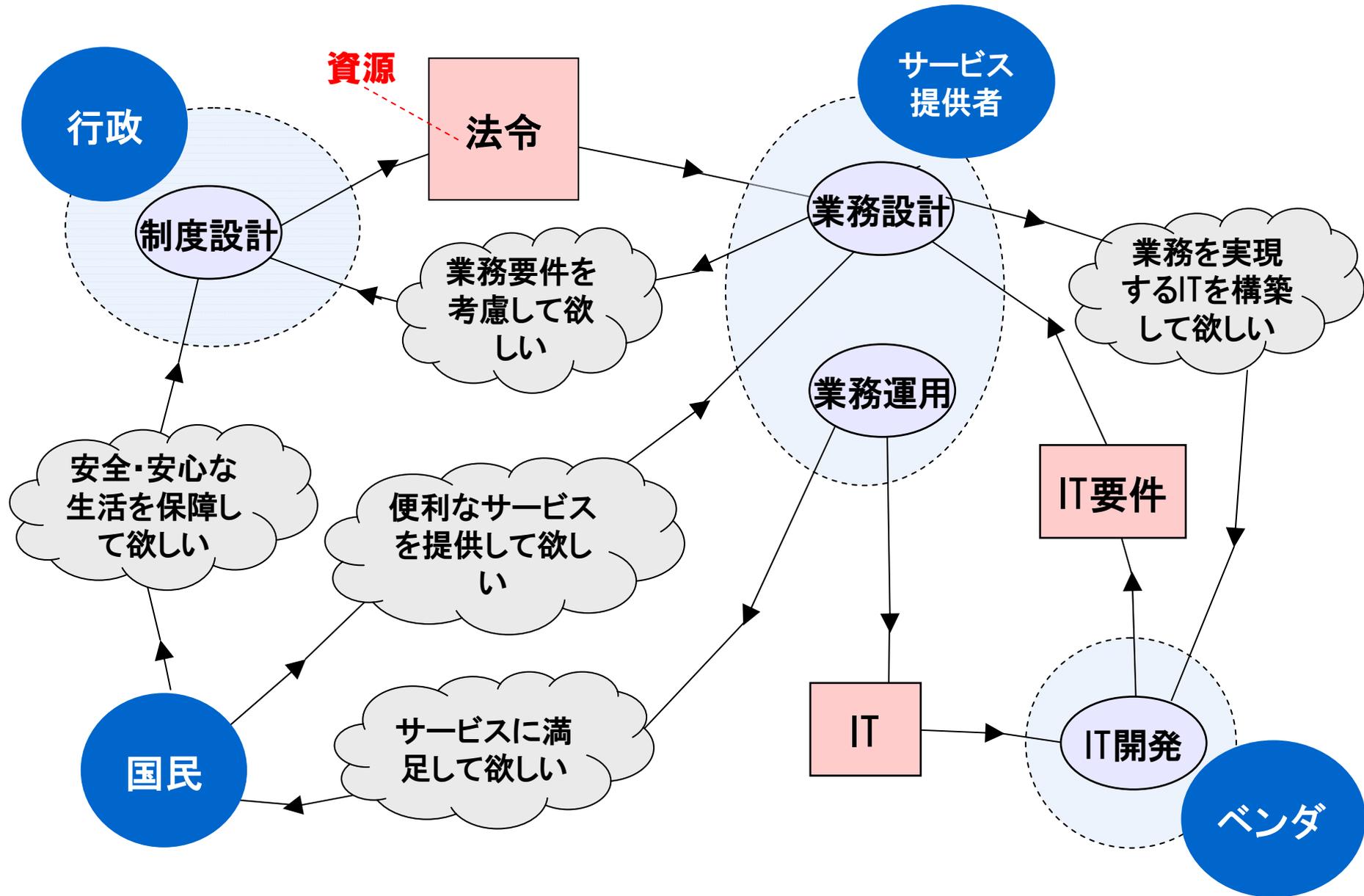
Silent Tree  
Walking

## アクションレイヤ



# 【事例】 IT業務処理統制





# Insight for the New Paradigm

---

未来のしくみを、ITでつくる。

株式会社NTTデータ