エンタープライズ
ロール管理解説書
（第３版）

特定非営利活動法人　日本ネットワークセキュリティ協会
標準化部会　アイデンティティ管理　ワーキンググループ

2016年6月2日

目次

あいさつ

本書は「エンタープライズロール管理」について、その基礎となる考え方や実施の意義、ID 管理システムを導入するにあたって同時に検討すべき「ロール管理」について、実用的な導入指針（ガイドライン）を示している。本書の作成にあたったワーキンググループには、ID 管理製品やロール管理製品の開発・販売ベンダ、導入経験のある SIer・コンサルタント等が多数参加しており、特定の製品に偏向しないことを留意しつつも、ロール管理を導入するユーザ、SIer 等にとって有用となる知識・ノウハウを持ち寄った。

その結果、本書はロール管理とは何か？から始まり、ID 管理におけるロール管理の重要性を解説し、実際のロール管理の実装ステップをステップごとに解説をおこなっている。また、ロール管理はその運用が重要になるため運用のガイドラインとなるものを解説した。

第 2 版ではロール管理の仮想企業導入事例を追加し、読者がロール管理のプロジェクトを進めるためのイメージができるものを追加した。

第 3 版においては、導入部分を見直し、ロール管理の失敗例の追加、ロール管理のあるべき姿の検討を行い、ロール管理の全体像についてより理解しやすい内容とした。

これから、ロール管理を導入検討する人には、プロジェクトの推進の準備として、また、現在 ID 管理やロール管理システムを導入中の人にとっては、現在のプロジェクトをよりよくするためのチェック、ヒント集として、活用していただけると考えている。

なお、本書は「日本ネットワークセキュリティ協会（ＪＮＳＡ）」の「アイデンティティ管理ワーキンググループ」にて複数年に渡って検討した内容となっており、ワーキンググループに参加いただいたすべての方々のご協力に深く感謝する。

また、この分野について詳細に書かれた書籍がほとんど出版されておらず、その意味でも本書の内容は多くの企業に役立つ内容となっている。

本書があらゆる企業において、ロール管理の適切な導入・運用に貢献できれば幸いである。

特定非営利活動法人　日本ネットワークセキュリティ協会
標準化部会　アイデンティティ管理　ワーキンググループ
リーダ　宮川 晃一

はじめに

全社的なアクセス権の制御を適切かつ効率的に行うことを目的として、ロール管理の考えを取り入れ実践している企業は多い。しかし、実際にはこの目的を実現できていないケースも多く、ロール管理を適切かつ効率的に行うことは難しいのが現状である。

ロールを利用したアクセス制御の仕組み自体は難しいものではないため、各種のアクセス管理製品に仕組みとして実装はされているが、それらを利用して、ロール管理を適切かつ効率的に実現するためには、管理対象となっているロール自体がどのようなものであるか？どのような種類があるのか？を理解し、また、どのように設計し、どのように運用すべきかを理解し、かつ、実践する必要がある。

本ガイドラインは、実際の組織におけるロール管理のあるべき姿を追求し、そもそもロールとは何か、ロールの種類、ロールの構造はどうあるべきか、ロールの設計および運用はどう行うべきか？をまとめたものである。

第 1 章においては、ロールの定義とロール管理の目的及び前提条件を明らかにする。この章では、更に、実際のロール管理において陥りがちな問題をいくつか例示し、そうした問題の回避するための考え方が本ガイドラインの第 2 章以降のどの部分に記述されているかを示す。

第 2 章においては、ロール管理のあるべき姿として、ロールの種類とその関係・構造を提示し、その導入および運用の各段階の概要を示す。

第 3 章においては、ロール管理の導入段階で行う現状調査・企画、ロール設計、実装方式設計、実装・移行・展開といった各フェーズのガイドラインとして　それぞれにおいて行うタスクを定義し、各タスクの目的、前提条件、留意事項、作業内容、成果物を定義する。

第 4 章においては、ロール管理の運用段階でのガイドラインとして、ロールのライフサイクルを定義し、そのライフサイクルイベント毎に行うべきロールの運用作業について定義する。

第 5 章においては、「仮想企業におけるロール管理導入事例」として、簡単ではあるが第 3 章をベースに実際にロールの導入がどのように行われるか？を仮想事例として紹介している。

第1章
ロールの定義とロール管理の失敗例

本章では、まず、ロールの定義とロール管理の目的及び前提条件を明らかにする。その後、ロール管理を実施する際に陥りがちな「ロール管理の失敗例」を取り上げ、後続章で示すロール管理に関するガイドラインのどの記述がそうしたロール管理の失敗の予防に役立つかを示す。

1.1. ロールの定義とロール管理の目的及び前提条件

本節では、本書が扱うロールの定義とロール管理の目的を整理し、また、そこから導き出されるロール管理の前提条件を明確化する。

1.1.1 ロールの定義とロール管理の目的

本項では、以下の 2 つを対比することでロールの定義及びロール管理の目的を明確化する。

① 実世界における、実在の人（＝本書では「ユーザ」と表記）と、そのユーザが割り当てられた職務及び権限

② 情報システムにおける、そのユーザが利用するアカウントと、そのアカウントに割り当てられたアクセス権

企業においては、正社員や派遣社員と言った従業員だけではなく、その企業を支えるグループ会社の人、サプライチェーンに関わる別企業の人といった様々な人が、役職や組織、業務規定などにより職務・権限が割り当てられる。こうした職務を遂行するためには様々なリソースの利用が必要となり、情報システムが普遍化した今日においては情報システムもそうしたリソースの重要な一部である。情報システムでは一般的にリソースの利用の可否を「アクセス権」という形で定義し、情報システムを利用するためには各ユーザが利用するアカウントが適切なアクセス権を有する必要がある。これを図示すると下図の通りとなる。

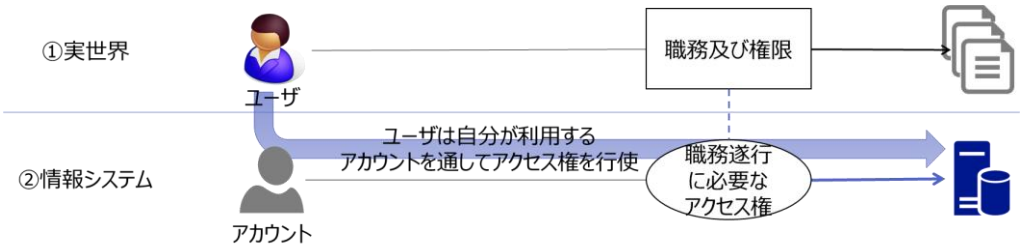


図 1.1 ユーザ・職務の関係とアカウント・アクセス権の関係

上図に示した、ユーザ（とそのユーザが利用するアカウント）とアクセス権の関係を、原始的に管理する方法は、ユーザとアクセス権を 1 対 1 で管理する方法である。これを例示すると下図の通りとなる。

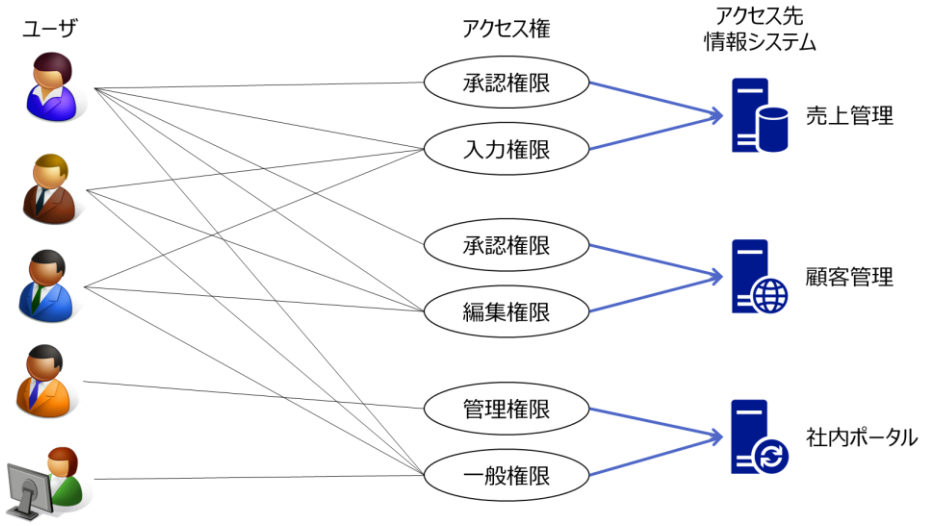


図 1.2　ユーザ（とそのユーザが利用するアカウント）とアクセス権を 1 対 1 で管理している状態

しかし、こうしたユーザとアクセス権の関係は固定されたものではない。ユーザとアクセス権の関係は、下図に示す通り「ユーザと職務の関係」及び「職務とその職務遂行に必要なアクセス権の関係」により成り立つ。この 2 つの関係はそれぞれ人事異動や組織改編、職務遂行のために利用する情報システムの新規導入などにより変化する。

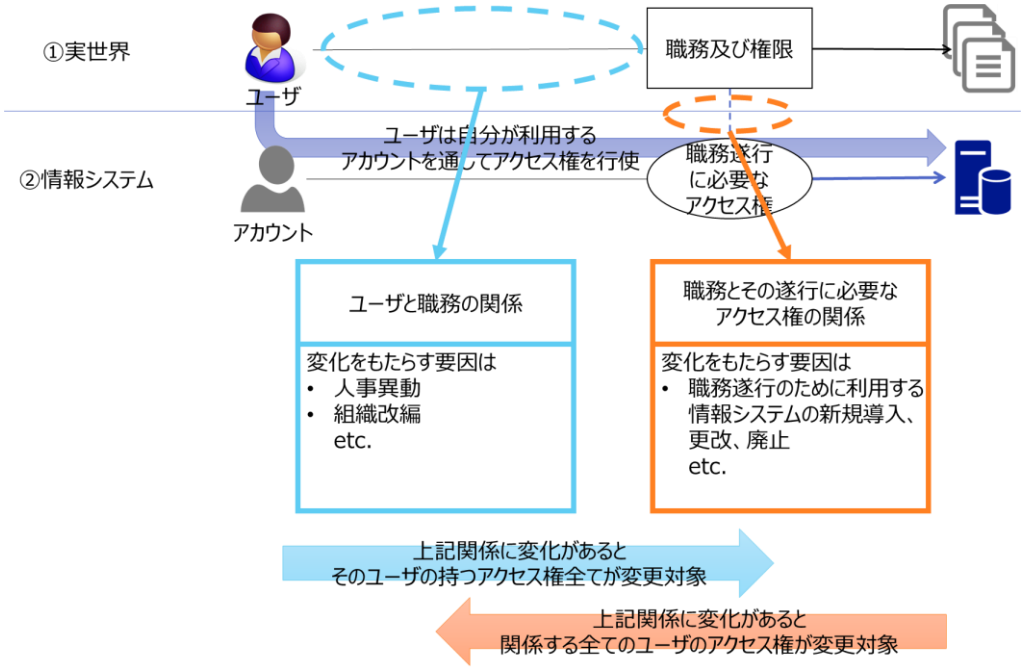


図 1.3　ユーザと職務の関係及び職務とその遂行に必要なアクセス権の関係（ロールを介さない場合）

ユーザとアクセス権を 1 対 1 で管理している場合は、いずれの関係における変化もその影響範囲は変化が生じる対象に関連する全てのユーザとアクセス権の割り当てに及ぶ。そのため、その変化

に応じてユーザにアクセス権を都度付与・剥奪することは、実施不可能なほど複雑で手間のかかる作業になってしまう。「図 1.2　ユーザ（とそのユーザが利用するアカウント）とアクセス権を 1 対 1 で管理している状態」に示した例で、人事異動及び新システム導入が起こった場合のアクセス権の変更の一例を下図に示す。下図においては水色の線は「ユーザと職務の関係」の変化、オレンジの線は「職務とその職務遂行に必要なアクセス権の関係」の変化を示す。

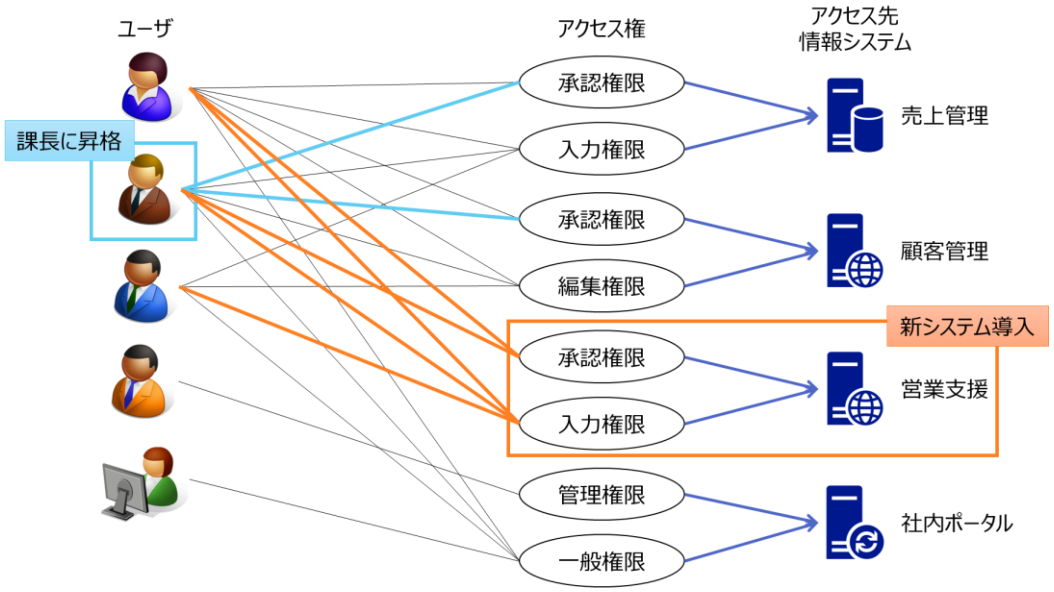


図 1.4　関係に変化が生じた場合のユーザと割り当てるアクセス権の変更箇所

上述のような変化に対して管理の煩雑さを抑制しつつ適切な管理を実施するためには、職務を遂行するために必要な「各種情報システムに対するアクセス権の組み合わせ」を抽出し、その組み合わせを仲立ちとして、ユーザにアクセス権を割り当てる必要がある。これを図示すると下図の通りとなる。

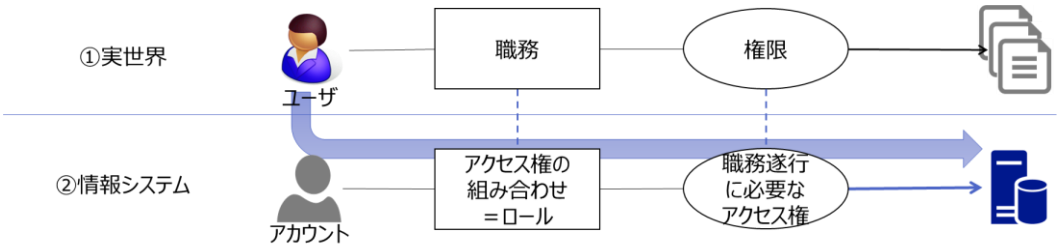


図 1.5　ロールを仲立ちとしたユーザ・職務の関係とアカウント・アクセス権の関係

本書ではこの「職務遂行に必要な各種情報システムに対するアクセス権の組み合わせ」をロールと定義する。前掲の「図 1.2　ユーザ（とそのユーザが利用するアカウント）とアクセス権を 1 対 1 で管理している状態」についてロールを仲立ちさせると下図の通りとなる。

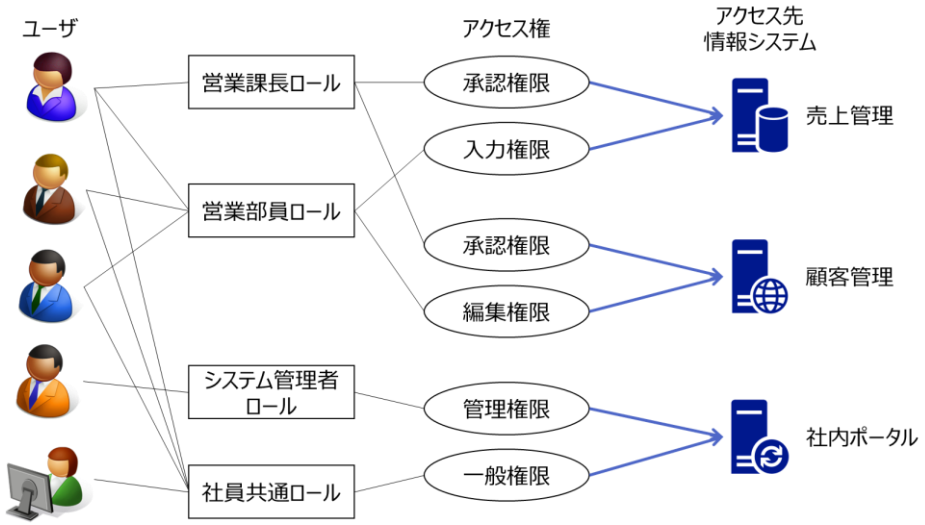


図 1.6　ユーザ（とそのユーザが利用するアカウント）とアクセス権をロール管理している状態

ロールを介した管理においてもユーザとアクセス権の関係は「ユーザと職務の関係」及び「職務とその職務遂行に必要なアクセス権の関係」により成り立つが、下図に示す通り、この 2 つの関係の間にロールを介する。ロールを介することで、この二つの関係の一方における変化の影響範囲はロールまでに限定される。「ユーザと職務の関係」における変化の影響範囲はユーザとロールの関連づけの変更までとなり、「職務とその職務遂行に必要なアクセス権の関係」の変化の影響範囲はアクセス権とロールの関連づけの変更までとなる。

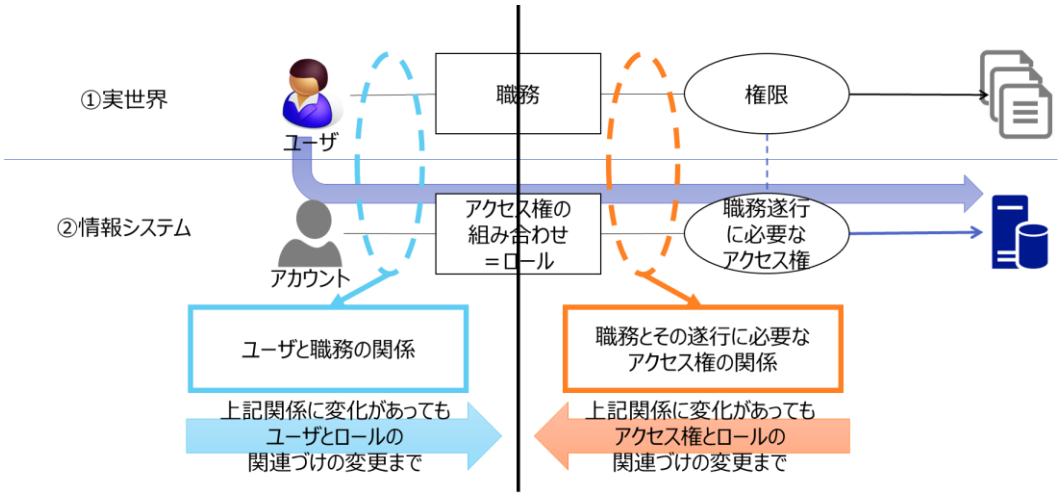


図 1.7　ユーザと職務の関係及び職務とその遂行に必要なアクセス権の関係（ロールを介す場合）

変更箇所が限定されるため、前掲の「図 1.4　関係に変化が生じた場合のユーザと割り当てるアクセス権の変更」と同様の具体例においてロール管理を採用する場合に生じる変更箇所を下図に示す。必要な設定内容が大幅に減っていることが分かる。

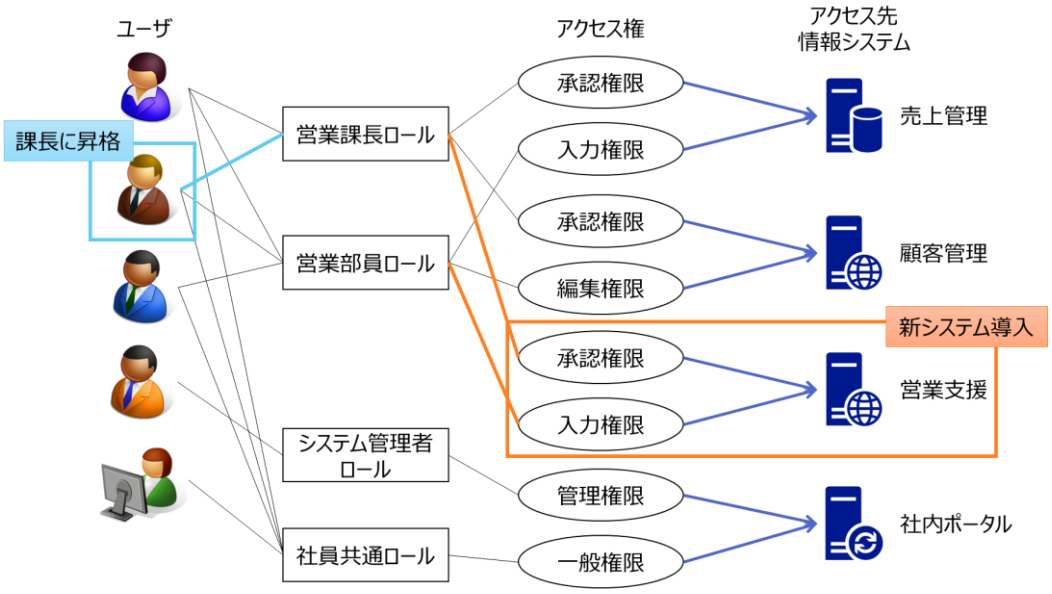


図 1.8　関係に変化が生じた場合のロールに生じる変更箇所

ロールを仲介することでユーザと職務の関係性や職務の遂行に必要なアクセス権に変化が生じた場合にもその変化が及ぶ箇所を最小化することが出来、効率的な管理が可能となる。このように、ロール管理の目的は「アカウントとアクセス権の対応を適切かつ効率的に実現すること」である。

なお、情報システムにおけるロールの概念がどのように生まれてきて、どのように定義されているのかについても触れておくことにする。

ロールは、情報セキュリティの分野で RBAC(Role-Based Access Control: ロールベース・アクセス制御)という概念の中に早くから登場し実装されている。RBAC は、ユーザ単位にリソースへのアクセス権限を個別に割り付けるのではなく、業務上の必要性によって定められるロールに基づいて（ロールを介して）リソースへのアクセス権限を一纏めに割り付け、アクセス制御を実現するモデルである。リソースへのアクセス権限をロールで束ねることにより、数多くのユーザおよび様々なリソースに対して横断的なアクセス権限管理を実現し、その運用・管理を容易にすることができる。

RBAC についての主な参考文献・参照先は以下の通りである。

- Ferraiolo, D.F. and Kuhn, D.R. (10 月 1992 年). “Role Based Access Control”. 15th National Computer Security Conference. pp. 554-563
- Sandhu, R., Coyne, E.J., Feinstein, H.L. and Youman, C.E. (8 月 1996 年). “Role-Based Access Control Models” (PDF). IEEE Computer (IEEE Press) 29 (2): 38-47.
- http://csrc.nist.gov/groups/SNS/rbac/ (NIST)
- “ Role-Based Access Control”　ISBN 1-58053-370-1　David F. Ferraiolo, D. Richard Kuhn, and Ramaswamy Chandramouli

1.1.2　ロール管理の前提条件

上述の通り、ロールはアカウントに対して割り当てるため、ロール管理を実施するためにはユーザに割り当てるアカウントが識別されている必要がある。これはすなわち ID 管理が実施されていることと同義である。ID 管理を実施し、各情報システムにおけるアカウントを識別し、各アカウントを割り当てたユーザの情報が管理されていることは、ロール管理を行うための前提条件となる。

1.2. 陥りがちなロール管理失敗例

前節に記述したとおり、ロール管理を行うことで「アカウントとアクセス権の対応を適切かつ効率的に実現すること」ができる。しかしながら、ロール管理を行っていながらも、何らかの原因で適切なロール管理のメリットを活かしきれずに、この目的を果たせていないケースが少なくない。本節では陥りがちなロール管理の失敗例を挙げ、そうした失敗例を改善する上で必要な事項が本書のどの記述内容に相当するかを示す。

1.2.1. 似たもの同士ロール

■　ロール管理失敗例概説

必要なロールの粒度について、十分な検討を行わずにその時に必要な条件を満たすようにロールを作った結果、類似のロールがいくつも必要になってしまう例。

■　症状例

田中さんは、A 社の IT 部門で各部署が利用するアプリケーションのアクセス権を管理している。あるとき田中さんは、新しく導入する営業支援ソフトウェア（以下 SFA）を担当するプロジェクトチームから、営業部長から提示されたリストに含まれる 100 名弱の営業部員がこの SFA にアクセス出来るようにしたい、との要望を受けた。

もともとファイルサーバへのアクセスを制御するために、人事情報及び営業部に所属する非正社員を管理する DB に基づき営業部に所属するユーザを含める営業部ロールが定義してあったので、そのロールを構成するユーザと営業部長からのリストを比較してみたが、10 名弱の食い違いが生じた。

食い違いが生じた理由について営業部長に確認を求めたが返答がなく、プロジェクトチームからは要望の実現可否の回答を急かされる状況だったため、田中さんは新しく SFA 用ロールを定義し、当該100名弱のアカウントがそのロールに含まれるようにした。人事情報に基づくロールとは食い

違いが生じており、田中さんは四半期に一度の人事異動時には SFA 用のロールのメンテナンスを手動で行うことにした。

SFA 導入から数ヶ月後、顧客管理ツール（以下 CRM）の更改を担当するプロジェクトチームから田中さん宛に、更改に伴う CRM のアクセス権管理を田中さんに引き継ぎたい旨の連絡があった。CRM はそれまでロール管理対象外であったので、これを機にロール管理を行おうと考え、田中さんは CRM 利用予定ユーザの一覧を、営業部ロールに含まれるユーザや SFA 用のロールに含まれるユーザと比較してみたが、やはり 10 名弱がどちらとも食い違っている状態だった。

田中さんは仕方なく CRM 用のロールを新しく作った。SFA 用ロールと同様に人事情報に頼ることが出来ないため、田中さんはこのロールのメンテナンスも手動で行うことにした。

他の部門でも同様に、人事情報とは若干食い違うアクセス要件を満たそうとした結果、各ロールの一部のメンバが違うロールがアプリケーション別に増えていき、田中さんは人事異動の度にそれらのロールの正しい構成ユーザは誰なのかを各方面に確認し、それを実際のロールに手動で反映するという作業に追われるのであった･･･。

■ ガイドライン参照ポイント

2.1 ロールのあるべき姿

2.3.1 組織型ロール管理のポイントについて

3.1.2 現状調査・企画

3.1.3 ロール設計

3.2.1 ビジネスロールとその付与ルールの調査時に直面する課題

3.4.4 組織型ロール設計

4.2 ロール管理運用の観点

4.3.1 トリガイベントが最初に組織型ロールに影響を及ぼすケース

1.2.2. 増殖していくロール

■ ロール管理失敗例概説

ロールの要否について、確認する術が定義されないまま必要なロールを作った結果、使われているのかどうかが分からないが、無くなったときの業務影響を恐れて決して消すことが出来ないロールがどんどん増えていく事態になってしまう例。

■ 症状例

高橋さんは、A 社の IT 部門でロールの運用を担当している。今日もロールの申請書が 2 通回ってきた。ここのところ毎日のようにロール申請があり、ひどい時には 1 日に数十通の申請書が回ってくる。今回の申請は、2 通とも新規ロール作成の申請であり、申請理由の欄には、いずれも「新規プロジェクト発足の為」と記載されている。「ロールの新規追加申請は毎日のように来るが、削除申請は見たことが無いな。業務に支障がでるから追加の申請書は来るけど、削除申請は、しなく

ても困らないからだろうな。」と、高橋さんは思った。

ある日、高橋さんはどんどん増え続けるロールに、このままではまずいと思い、不要なロールを削除しようとしたが、

- このロールは何に使っているロールだろうか、わからない。
- そもそもロールの責任者が明確でないので、削除してよいかを誰に確認すればいいのだろう。
- ルールでは使用しなくなったロールは削除申請することになっている。こちらの勝手な判断で、ロールを削除してまずいことが起こったらどうしよう。

高橋さんは、ロールを削除することを諦めた。その結果、何が必要なロールで、何が不要なロールかを誰も判断できなくなり、ロール数は 2 万個を超えた･･･。

■ ガイドライン参照ポイント

2.2.3 ロールの運用について

2.3.3 プロジェクト型ロール管理のポイントについて

3.2.4 ロールデータの元データとその維持管理体制の定義時に直面する課題

3.4.6 プロジェクト型ロール設計

3.5.2 ロール運用設計

4.2 ロール管理運用の観点

4.3.2 トリガイベントが最初にプロジェクト型ロールに影響を及ぼすケース

1.2.3. メンバ不明ロール

■ ロール管理失敗例概説

ロールに含まれるメンバ要否について、確認する術が定義されないまま必要とされるメンバをロールに追加していった結果、メンバの適・不適が分からずアクセス権の管理が実質的に出来ていない事態になってしまう例。

■ 症状例

佐藤さんは、A 社の IT 部門で各部署が利用するアプリケーションのアクセス権を管理している。あるとき、佐藤さんは、既存アプリケーションシステム（以下 A システム）を担当するプロジェクトチームから、異動に伴う管理者権限メンバ 1 名追加の依頼を受けた。

A システムは基幹系システムの一部であり、該当する管理者権限ロールは、「基幹系システム管理者権限ロール」として、1 つにまとめられている。基幹系システムと呼ばれるシステムは、A システム、B システム、C システム及び D システムの集合体であり、D システムは既に廃棄されている。また、該当するプロジェクトチームも解散している。

佐藤さんが「基幹系システム管理者権限ロール」の所属メンバを確認したところ、50 名を超えるメンバが所属していたが、既に廃棄されたシステムも含まれる関係上、50 名を超えるメンバの権限要否の判断ができない状況であった。佐藤さんは、依頼を受けるまま、該当ロールにメンバを追加し、登録完了の連絡を A システム担当プロジェクトチームへ行った。

こうした作業を繰り返した結果、ロールメンバの妥当性判断がよりいっそう困難な状況となっていくのだった･･･。

■ ガイドライン参照ポイント

2.2.3 ロールの運用について

1.2.4. 使用目的が不明なロール

■ ロール管理失敗例例概説

ロールの設計において命名規則が定義されていない、または、命名規則が定義されていても、ロール名称がロールの使用用途を表現できていないことにより、人事異動や組織改編、プロジェクトの改廃、業務フローの変更など、あらゆる「変化」に対応できず、ロールに割り当てられた権限が不適切なまま残り、ロール管理運用が非効率となってしまう例。

■ 症状例

鈴木さんは、A 社の IT 部門で各部署が利用するアプリケーションのアクセス権を管理している。あるとき鈴木さんは、財務会計システムを更新できるロールのメンバ追加依頼を受けた。財務会計システムを更新できる権限は、経理課に属するメンバのみであったが、決算期の応援メンバとして経理課の経験がある総務課の B さんを追加して欲しいという依頼だった。鈴木さんはこれまで使用していた経理課ロールにBさんを追加することができないため、新たに「経理課２」というロールを作成し、経理システムにマッピングした。

また、同じような依頼が他部門からもあり、〇〇課２、△△課３という、ロールの使用用途が名前から判別できないロールが増えていった。

その結果、不適切な権限が残ったままとなるロールが散見され、また、棚卸し時のロール要／不要の判断、ロールメンバの妥当性判断が困難な状況となっていった･･･。

■ ガイドライン参照ポイント

2.2.1 ロールの設計について

3.4.4 組織型ロール設計

4.2 ロール管理運用の観点

第2章
ロール管理の概要

ロールのあるべき姿

ロールは、第1章で説明したように、アカウントとアクセス権の中間に入り、アクセス権の管理を柔軟にコントロールする。ただし、作成したロールは設計時のまま固定されるわけではなく、組織変更やシステム変更の影響を受け運用時に変更が必要となる。

ロールの設計によっては、第1章で説明したような「失敗例」を作りこんでしまう可能性がある。そのため、そうした変更に対応できる、ロールのあるべき姿を考慮しておく必要がある。

例えば、最初に承認者のための「承認者ロール」を作成し、アプリケーション側の権限として「承認画面 A 用権限」を設定した。その後、新しい職務として監査担当が必要となり、「監査者ロール」を作成した。アプリケーション側の権限としては「承認者ロール」と同一であったため、同じ権限を設定した。さらに、アプリケーション側で新しい権限「承認画面 B 用権限」が作成された。この時、「承認者ロール」と「監査者ロール」の両方にマッピングしなければならなかったが、「監査者ロール」については名前から推測できなかったため、設定が忘れられてしまった。また、このままでは監査担当に必要な権限がないため、アプリケーションを正常に利用できなくなり、新しい「監査者承認ロール」が監査担当用に作成された。これは、「監査者ロール」の役割があいまいであったため手をつけることができず新しいロールを作るという、その場しのぎの判断がされたためであった。その後「監査者ロール」は消すに消せず残ることになり、結果として「使用目的が不明なロール」というロール管理の失敗例を生み出すことになった。

本来ならロール自体の変更時には、「ユーザと職務の関係」と「職務とその職務遂行に必要なアクセス権の関係」の両方の視点で変更箇所を確認する必要がある。しかし、それぞれの変更箇所がわかりにくい構造の場合、前述のような「ロール管理の失敗例」を生みだしてしまう。

これらを回避するためには、アカウント側とアプリケーション側の意図を把握しやすい仕組み作りが重要である。その方法として、ロールを3層の構造とする。

具体的には、ロールをビジネスロール、アプリケーションロール、IT ロールという構成にわける。ロールをアカウント側とアプリケーション側に分離し、さらにシステム上で扱いやすくするため中間にクッションとしてのロール導入する。これより変更個所を局所化でき、変更があった側のみで対応できる管理しやすい構造を作ることができる。（図 2.1　ロールの 3 層構造）

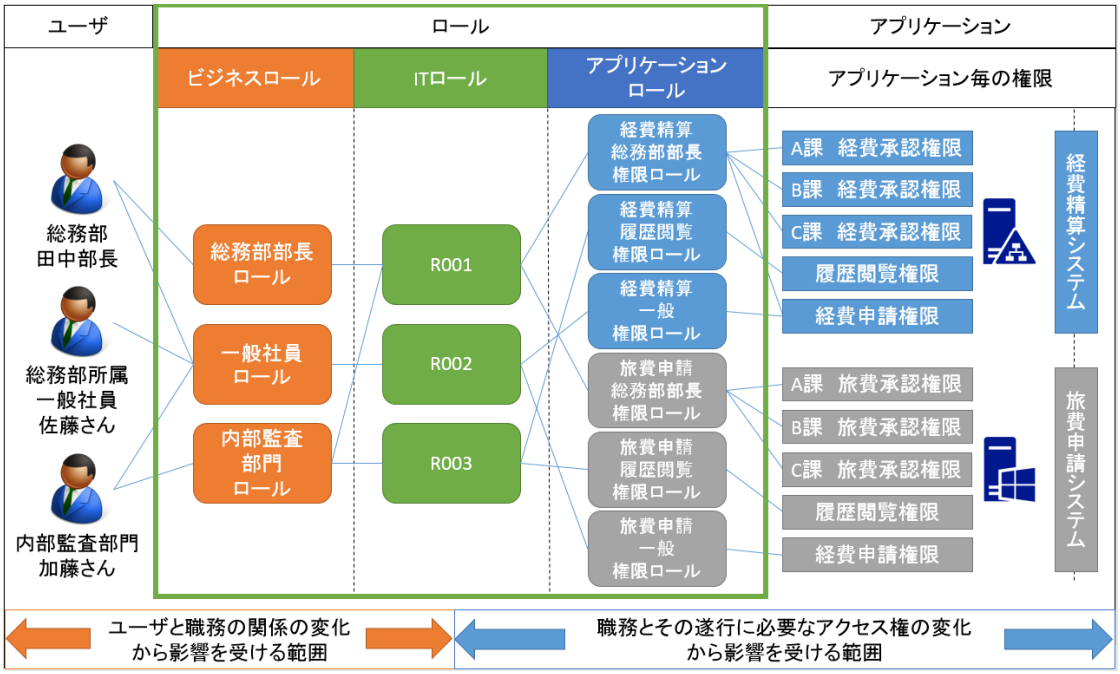


図 2.1　ロールの 3 層構造

・　ビジネスロール

ビジネスロールとは、職務を区分するためのロールである。日常業務上の役割の概念に最も近く、職制などと関連付けられる。例えば、課長ロールや部長ロールといあった職位に対応付けられるものや、経理ロール・営業ロールといった職種・部門に対応づけられるものが考えられる。

・　アプリケーションロール

アプリケーションロールは、アプリケーションのリソースへのアクセス権限を直接対応付けるロールである。アプリケーションのリソースの管理者が、アプリケーションロールを定義し、各種アクセス権限に対応付ける。例えば、入力、参照、承認権限などの権限と直接関連付けられるロールが考えられる。

・　IT ロール

IT ロールはビジネスロールとアプリケーションロールの中間に位置するロールで複数のアプリケーションロールを束ねる。例えば、事務処理の承認が許可された権限がある複数のビジネスロールと事務処理の承認処理ができる複数のアプリケーションロールを組み合わせたロールが考えられる。

2.2. ロール管理の導入におけるポイント

第１章で説明した「失敗例」にならないようにするためには、管理しやすい状態を保つことが重要となる。そのためには、「設計」「実装」「運用」といったロール管理における各工程で管理のしやすさを意識する必要がある。結局のところすべての工程が関連しており、どこかの工程で問題を作りこんでしまうと後になって修正するのが難しくなってしまうためである。

本節では、ロール管理における各工程で意識しておくポイントについてまとめておく。詳細については第３章以降を参考にしていただきたい。

2.2.1. ロールの設計について

ロールはシステムの基盤的な役割を担うためライフサイクルは長い。設計時の状態で運用され続けることはまれであるため、今後の変更を考慮に入れて設計する必要がある。そのため、設計の核としてはロールを３層構造にすることを推奨する。

また、ロールの役割に沿った名前を付けることもポイントになる。これによりロールがなんのために作られているのかがわかり運用しやすくなる。逆に良い名前が決まらないときは存在意味が曖昧な場合が多いので、失敗例の「似たもの同士ロール」などの発生原因となりやすい。ロール作成時になにをどこまで管理するのかの方針も十分検討していただきたい。

ただ、実際に３層構造を意識して設計しなさいと言われても、なにから手を付けてよいかわからない場合には、ビジネスロールを整理するところから始めるとよい。具体的には次の方針で進める。

■進め方

以下に設計の進め方について簡単にまとめておく。詳細については第３章「ロール管理導入指針」を参考にしていただきたい。

１．ビジネスロールの設計（アカウント側の整理）

まずは、アカウント側であるビジネスロールを整理する。業務の種類に分割して進めると設計しやすくなる。企業に存在する業務・役割などを割り当てるとよい。具体的には３種類「組織型ロール、ライン型ロール、プロジェクト型ロール」に分けて設計することをお勧めする。

A)　組織型ロール

組織型ロールとは、人事情報などで定義されるユーザの属性によって定義できるロールである。

B)　ライン型ロール

ライン型ロールとは、複数の組織が関係する業務に使用する。存在する業務フローを意識してロールを実装する。

C)　　プロジェクト型ロール

プロジェクト型ロールとは、期限付きの業務（プロジェクト）を行う場合などに使用する。組織に跨ったユーザからメンバが構成されることも多く、人事情報や組織情報からは自動で抽出しにくいものになる。

２．アプリケーションロールの設計（システムアクセス権限の設計）

次にアプリケーション側のロールを整理する。アプリケーションで必要な権限をアプリケーションの実装に合わせて設計する。これはアプリケーション固有なロールとなるため、その中で最適化されるように設計することが重要である。

３．IT ロールの設計（マッピング）

最後に、上記で作成したビジネスロールとアプリケーションロールを関連付ける。その関連が IT ロールとなる。お互いの影響を IT ロールがクッションになることによって、運用しやすい柔軟なロール管理を可能とする。「図 2.2　ロールのマッピング」のように表を作成してマッピングすると関連付けやすくなる。

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

図 2.2　ロールのマッピング

2.2.2. ロールの実装について

設計したロールを実際にシステムへ反映させるには、アプリケーションロールはアプリケーション側でそれに相当するもので実装し、ビジネスロールと IT ロールは ID 管理を担当するシステムで

実装することを想定している。

ビジネスロールと IT ロールの管理にシステムを使わず運用者の手作業のみで対応しようとすると、工数増大や設定ミスによる不具合の原因になる。そのため、これらの管理には ID 管理製品を使って実装することを検討していただきたい。ID 管理製品はロール管理の自動化などの以下のメリットが得られるためロール管理を行う上で最適なシステムとなる。

- ID 管理基盤には「ライフサイクル管理」「属性情報管理」「プロビジョニング」などの機能があり、これらを活用することでロール管理の運用負荷を下げることが可能になる。例えば、ユーザの属性変更に合わせて自動的にロールの割り当てを行うことが可能になる。
- ID 情報管理の証跡と対応付けたロール管理の証跡把握など、他の運用面でもメリットを得ることができる。

一方で設計したロールによっては自動化することが難しい場合もある。その場合は、無理に自動化して ID 管理システムの運用を複雑化させるより、例外と割り切り手動での対応も検討してほしい。手動にしたほうが結果として運用が簡単になる場合もある。ただし、例外を都合のよい処理にしないために内容を明確化して、ルール化しておくことが重要になる。

2.2.3. ロールの運用について

ロールの設計・実装は一度行えば完了というわけではなく、業務上の役割の変更などによって改修する可能性がある。そのため、柔軟に対応できるような管理方法にしておく必要があり、ここまでにそれらについて述べてきた。

しかし、設計・実装を注意深く行っても運用時に問題を引き起こしてしまうこともある。具体的には、第 1 章で述べた「メンバ不明ロール」もこの工程で作り込みやすい。これは、設計で決めたロールの粒度を運用者の認識不足で粒度感が違うメンバをロールに追加・削除してしまうことから発生する。このようにしないためには、「設計段階の方針を徹底する」ことが重要になる。

また、運用を続けているうちにロール内容が業務とかけ離れてしまうことがある。これは作業の結果が実態に即しているのか確認していないことから発生する。このようにしないためには、「棚卸」作業を定期的に実施することが重要になる。

実際の原因は運用だけでなくその上位工程の場合もある。ただ、ロールを一番壊しやすいのが運用時である。そのためにも運用について設計・実装時から意識し、ロールを管理しやすい体制を維持しなければならない。具体的な運用の方法については「第 4 章ロール管理の運用」を参照してほしい。

2.3. ビジネスロールのポイント

ロールの設計においてはビジネスロールから整理することを推奨した。しかし、この時に方向性を誤ると第1章で説明した「失敗例」に陥りやすくなるので、種類の選択は重要になる。そのため、本節では設計時に理解しておいてほしい各種類のポイントについて説明していく。

2.3.1. 組織型ロール管理のポイントについて

組織型ロールとは、人事情報などで定義されるユーザの属性によって定義できるロールである。ユーザが所属している組織情報や、ユーザの職位情報によって権限が分けられる業務に使用する。組織情報をロールにする場合には、組織ツリー階層を維持した形でロールが作成される。

組織型ロールの例として、以下のようなロールが考えられる。

- 組織ロール（総務部ロール、システム開発課ロール、全社ロール、・・・）
- 職位ロール（幹部社員ロール、部長職ロール、主任以上ロール、・・・）
- 社員種別ロール（正社員ロール、派遣社員ロール、協力会社社員ロール、・・・）
- 拠点ロール（A事業所ロール、B事業所ロール、・・・）
- 職責ロール（営業ロール、SEロール、開発者ロール、運用者ロール、・・・）
- 上記を組み合わせたロール

■ 組織型ロールの特徴

組織型ロールは、企業全体で一意に定められた人事情報や組織図から作成できるため、Top Downで作成し易く、また、ロールを自動作成し易いという特徴がある。

■ 組織型ロールの考慮点

組織型ロールで特に組織ロールを実装する場合には、以下の考慮が特に必要である。

- 組織階層をどの階層レベルまでロールにする必要があるか。（課レベルまで、係レベルまで等）人事情報として保持している階層以下のレベルまでロールにする必要がある場合には、実装しにくくなりメンテナンスが大変になる。
- 組織変更にどう対応するかを考慮した上でロールを実装する必要がある。ユーザが所属している組織コードを使って、自動化できるのであれば比較的メンテナンスは容易となる。また、引き継ぎ期間や兼務の扱いについても考慮する必要がある。
- 組織ロールは入れ子（ロールの中に他のロールを含める構造）となる場合が多く、複雑になるため、上位の権限の継承も考慮する。また、部ロールを作成する場合、部に属する全ての人に与える権限か、部直属の人のみに与える権限かというように、権限の範囲を考えておく必要がある。
- 組織をベースにしていても、不適切な権限付与になってしまう場合もあるため注意が必要である。また、組織そのものの上下関係、包含関係をどのように表

現するのかも課題となる。

■ 組織型ロールの利用例

組織型ロールの利用例として、「Web 認証サーバ」の例を示す。統合認証サーバでは、認証情報としてユーザ情報、認可情報として ACL（アクセス制御リスト）を管理する。

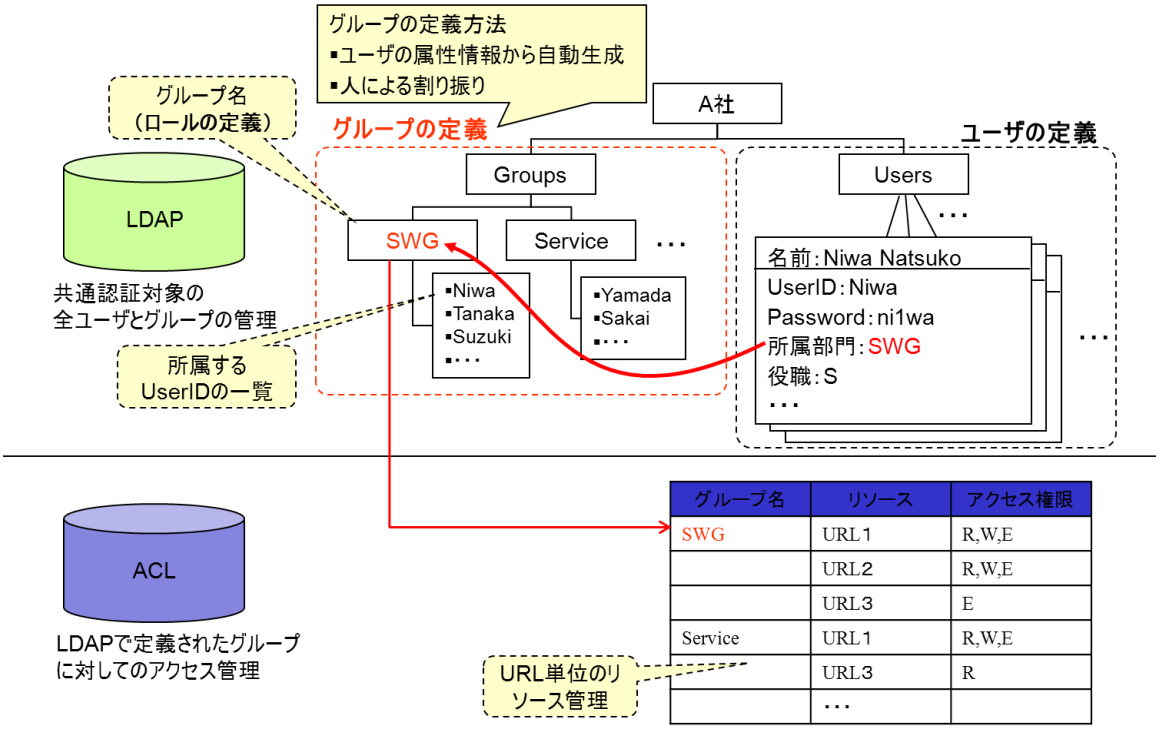


図 2.3　組織型ロールの利用例「Web 認証サーバ」

また、組織型ロールの利用例として、ファイルサーバの権限設定例を示す。人事情報からロールメンバを自動メンテナンスし Active Directory のセキュリティグループに配信する。ファイルサーバの権限をセキュリティグループに対して与えることにより、メンテナンスが自動化される。

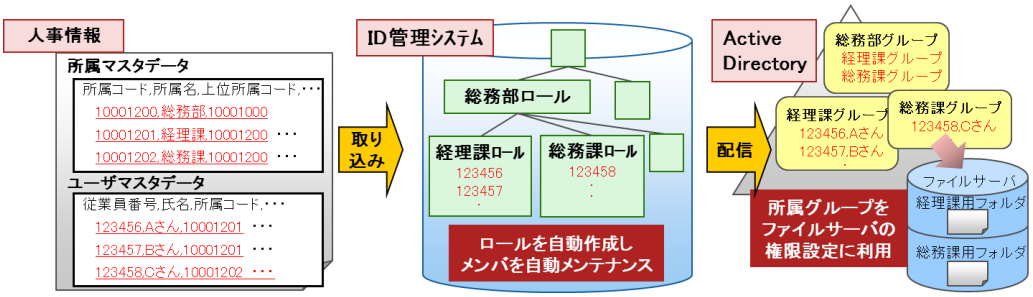


図 2.4　組織型ロールの利用例「ファイルサーバ」

2.3.2. ライン型ロール管理のポイントについて

ライン型ロールとは、複数の組織が関係する業務に使用され、各組織の業務上の役割に応じて、業務フローを意識してロールを実装する。また、組織や職位とは関係せず、入力者ロールや承認者ロールのように、○○をする人というロールもある。

■　ライン型ロールの特徴

ライン型ロールの特徴として、以下のようなものがある。

- ロールと権限が密接に関連している。
- 業務システムごとに独立したロールが必要となる場合が多い。
- 業務そのものに変更がない限り変更は少ない。
- SoD（Segregation of Duties：職務分掌）が求められることが多い。
- それぞれの組織内でさらに権限が分かれることが多い。
- 組織型ロールとプロジェクト型ロールの両方の特徴を持つ。
- 基幹業務で使用されることが多い。

■　ライン型ロールの考慮点

ライン型ロールを実装する場合には、以下の考慮が必要である。

- 業務フローを意識するため、業務分析が不可欠である。
- SoD に抵触しないよう留意しながら実装する必要がある。
- ロールと職位は必ずしも対応するとは限らない。業務上の役割をロールとして実装するため、部長には必ず承認者ロールを付与するとは限らず、組織の役割として一般社員に承認者ロールを付与する場合も考えられる。

■　ライン型ロールの利用例

ライン型ロールの利用例としては、基幹業務における、申請者ロール、審査者ロール、支払者ロール、承認者ロールなどが該当します。

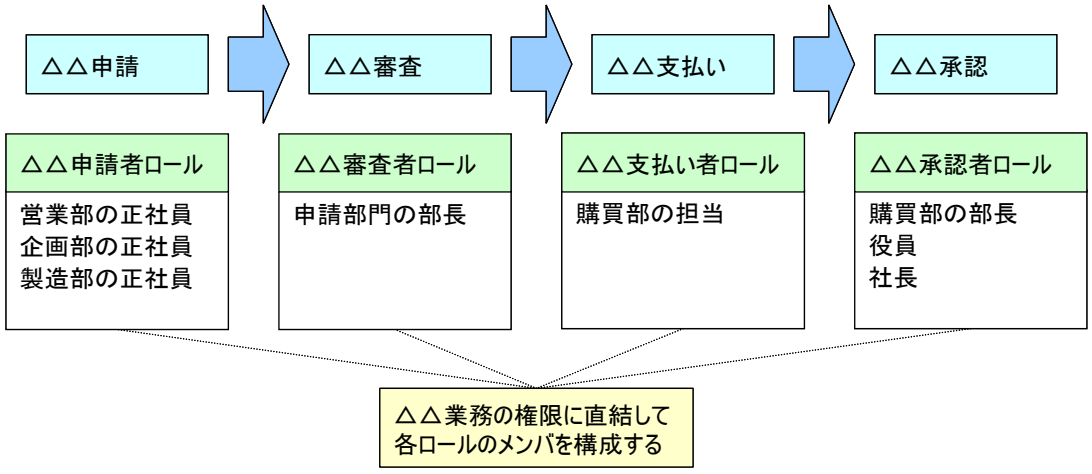


図 2.5　ライン型ロールの利用例「基幹業務ライン」

2.3.3. プロジェクト型ロール管理のポイントについて

プロジェクト型ロールとは、期限付きの業務（プロジェクト）を行う場合などに使用し、組織に跨ったユーザからメンバが構成されることも多く、人事情報や組織情報からは自動で抽出できない。その反面、ロールの自由度は高くなる。プロジェクトメンバのみにアクセス権限を与えたい場合に使用するロールであるため、プロジェクト専用のロールを作ることがある。

■ プロジェクト型ロールの特徴

プロジェクト型ロールは、日常業務上プロジェクトを順次実行していくような部門もあり、Top Down で作成することは難しい。また、ロールメンバのメンテナンスは手動で行うことが多い。

■ プロジェクト型ロールの考慮点

プロジェクト型ロールを実装する場合には、以下の考慮が必要である。

- ロールのメンテナンスが手動となることが多く、全てのプロジェクト型ロールを特定の部門のみで管理することは難しいため、ロールオーナを定め、ロールの管理を権限委譲する必要がある。ロールオーナに与えられる権限は、ロールメンバの管理、サブロール（子ロール）の作成・削除、ロールの持つ権限の管理などである。

- 複数部門の多くの人がロールの管理を行うため、不要なロールがいつもでも放置されてロールが増え続ける傾向が強く、全体の統制が効かない可能性が高い。よって、ロールの作成・改廃基準を作成するなど、ロール管理ルールを定めることが重要である。なお、職務分掌の観点から、ロールの管理責任と実作業実施を分離することも考慮する必要がある。

■ プロジェクト型ロールの利用例

プロジェクト型ロールの利用例としては、ファイルサーバのプロジェクト共有フォルダのアクセス権限管理などに使用される。

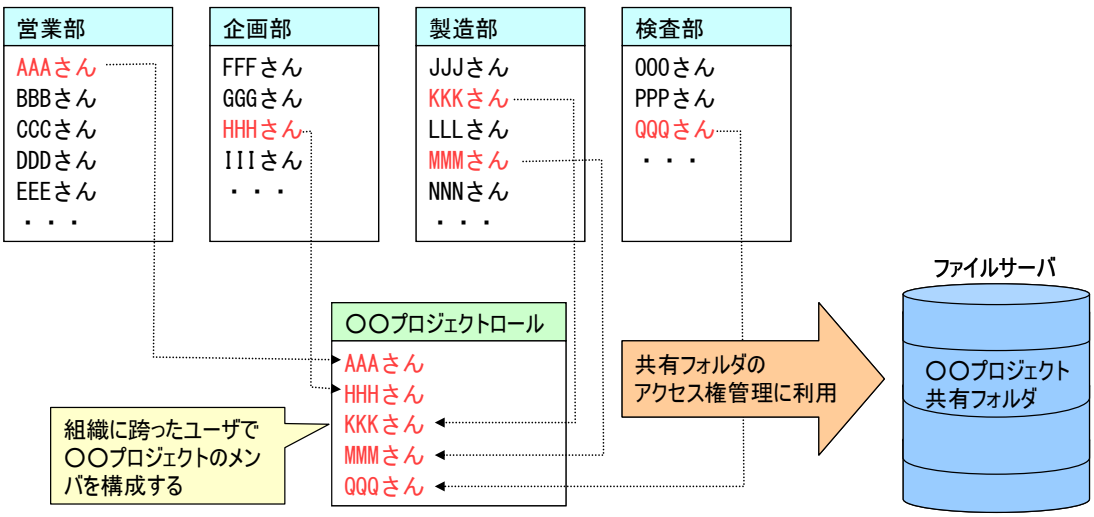


図 2.6　プロジェクト型ロールの利用例「ファイルサーバ」

第3章
ロール管理導入指針

3.1. ロール管理導入の流れ

前章までで、ロール管理とは何か、そして ID 管理におけるロール管理の重要性について説明してきた。この後は、ロール管理の導入を実際に進める過程の全体像を説明してから、それらの過程における課題やその解決の進め方について掘り下げて説明していく。

本節では、ロール管理導入過程の全体像（概要）について説明する。

3.1.1. 導入全体の流れ

ロール管理導入過程の全体は、以下に示す流れになる。

(1) 現状調査・企画
(2) ロール設計
(3) 実装方式設計
(4) 実装・移行・展開

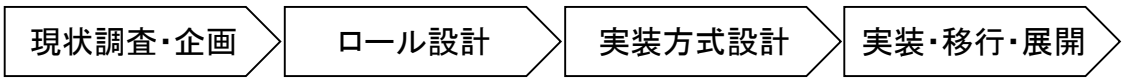


図 3.1 ロール管理導入全体の流れ

まず、ロール管理に関する現状がどうなっているのか、調査・確認する必要がある。そして、ロール管理導入の目的と目指すべき目標像を明確化する。

次に、現状調査の結果と目指すべきロール管理の目標像を踏まえて、どんなロールを用いるのかを検討・設計する。そして、これら設計したロールを用いて、ロール管理をどのように実装・運用するのかを検討・設計する。

最後に、設計したロール管理の実装・移行・展開をどのように進めるべきかを計画し、それを実施する。

これら導入過程の各フェーズにおいて、どのようなタスクが必要となるかについて、概要を以下に説明する。

3.1.2. 現状調査・企画

ロール管理に関する現状を調査し、企画するフェーズにおいては、以下に挙げるタスクが必要となる。

(1) 組織調査
(2) 職務分掌調査
(3) ライン型（定型・部署別）業務調査
(4) プロジェクト型（期間限定・部署横断）業務調査
(5) 対象システム調査
(6) 対象法規制調査
(7) 目的・目標像の明確化

3.1.3. ロール設計

現状調査の結果と目指すべきロール管理の目標像を踏まえて、どんなロールを用いるのかを検討・設計するフェーズにおいては、以下に挙げるタスクが必要となる。

(1) 組織型ロール設計
(2) ライン型ロール設計
(3) プロジェクト型ロール設計
(4) システムアクセス権限設計
(5) IT ロール設計

3.1.4. 実装方式設計

設計したロールを用いて、ロール管理をどのように実装・運用するのかを検討・設計するフェーズにおいては、以下に挙げるタスクが必要となる。

(1) プロビジョニング方式設計
(2) ロール運用設計
(3) ロール管理対象範囲の確定

3.1.5. 実装・移行・展開

設計したロール管理の実装・移行・展開をどのように進めるべきかを計画し、それを実施するフェーズにおいては、以下に挙げるタスクが必要となる。

(1)　実装・移行・展開の計画

(2)　実装・移行・展開の実施

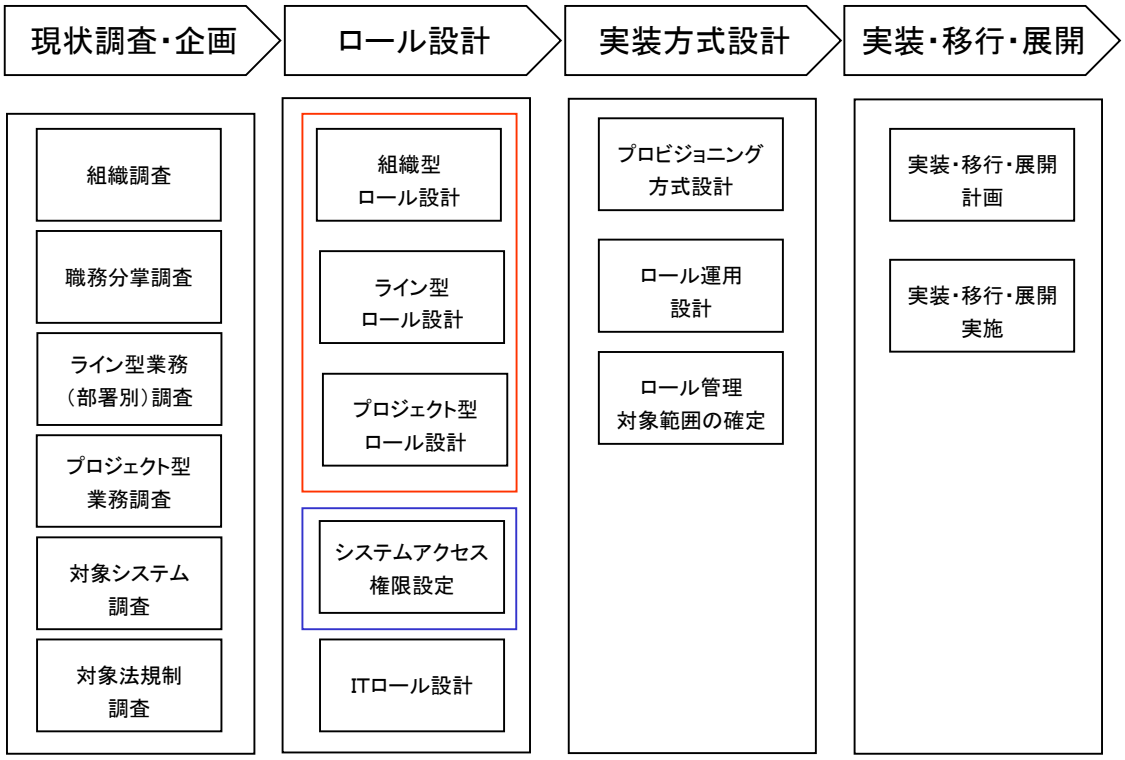


図 3.2　ロール管理導入過程のフェーズおよびタスク

■ **各工程の概要**

各工程の概要を以下に示す。

表 3.1　各工程の概要と成果物例

工程名	概要	成果物例
現状調査・企画フェーズ		
組織調査	ロール設計に必要なインプットとなる組織体制・階層等を洗い出す。	・調査メモ
職務分掌調査	ロール設計に必要なインプットとなる職務分掌を洗い出す。	・調査メモ
ライン型業務調査	ロール設計に必要なインプットとなるライン型業務のロールを洗い出す。	・調査メモ
プロジェクト型業務調査	ロール設計に必要なインプットとなるプロジェクト型業務のロールを洗い出す。	・調査メモ
対象システム調査	ロール設計に必要なインプットとなる対象システムに現在設定されている権限情報を洗い出す。	・調査メモ
対象法規制調査	ロール設計に影響をあたえる法規制について調査する。	・調査メモ
目的・目標像の明確化	ロール管理実装における目的・目標像を明確化する	・ロール管理導入計画
ロール設計フェーズ		
TopDown 型モデリング	工程ではない。	
BottomUp 型モデリング	工程ではない。	
ハイブリッド型モデリング	工程ではない。	
組織型ロール設計	組織型ロールを設計する。	・ロール設計書
ライン型ロール設計	ライン型ロールを設計する。	・ロール設計書
プロジェクト型ロール設計	プロジェクト型ロールを設計する。	・ロール設計書
システムアクセス権限設計	システムアクセス権限の設計をする。	・ロール設計書
IT ロール設計	IT ロールの設計をする。	・ロール設計書

実装方式設計フェーズ		
プロビジョニング方式設計	ロールを対象システムに配布する方法について検討・設計をする。	・プロビジョニング方式設計書
ロール運用設計	ロールのライフサイクルの検討とそれに伴う運用の検討を行う。	・ロール運用設計書
ロール管理対象範囲の確定	ロール管理を行うシステムの対象範囲を決定する。	・検討メモ
実装・移行・展開フェーズ		
実装・移行・展開計画	ロール管理システムについての実装・移行・展開計画を立案する。	・移行展開計画書
実装・移行・展開実施	ロール管理システムの実装・移行・展開を実行する。	・（特に定義せず）

3.3節以降において、各タスクの目的と前提条件、期待される成果物と具体的な作業について記述する。

3.2. ロール管理導入における課題

前節では、ロール管理導入過程の全体像（概要）について、説明した。この後は、ロール管理導入過程における課題やその解決の進め方について掘り下げて説明していく。

本節では、ロール管理導入の検討を進めようとした時に、どのような課題に直面するかについて、例を挙げて説明する。後節以降で説明する導入過程の各フェーズにおいては、本節で説明する課題を意識しながら検討を進める必要がある。

3.2.1. ビジネスロールとその付与ルールの調査時に直面する課題

現状調査・企画フェーズにおいて、ビジネスロールとして何があるか、およびそのビジネスロールを付与する際のルールに関する調査を進める時には、以下に挙げる課題に直面する。

(1) ビジネスロールは組織に応じて様々である。
(2) ビジネスロールの定義が曖昧な場合がある。
(3) 兼務や委任/代行が多く、それに伴いビジネスロール付与ルールの例外が多く存在する場合がある。
(4) 委任か代行かにより、責任の所在が異なり、ロールの扱いを変えなければならない場合がある。

これらの課題を踏まえて調査・検討を進める必要がある。

3.2.2. システム権限とその付与ルールの調査時に直面する課題

現状調査・企画フェーズにおいて、システム権限として何があるか、およびそのシステム権限を付与する際のルールに関する調査を進める時には、以下に挙げる課題に直面する。

(1) システム権限および権限付与ルールはシステムに応じて様々である。
(2) 例外的な権限付与が実施されている場合がある。

これらの課題を踏まえて調査・検討を進める必要がある。

補足）システム実装上の制約により、システム上での権限付与（設定）はロールを用いて行うことができず、ユーザごとに行わなければならない場合がある。このようなシステム個別の実装対応は、ロール管理実装の外で個別インタフェース実装の仕方として埋めるべき部分であり、ロール管理実装の中では詳しく論じない。

3.2.3. アクセス制御の全体ポリシーの確認時に直面する課題

現状調査・企画フェーズにおいて、アクセス制御の全体ポリシーに関する確認を進める時には、以下に挙げる課題に直面する。

(1) 実際のビジネスロールやシステム権限付与が、全体ポリシーと不整合を起こしている場合がある。
(2) 全体ポリシーが実態に合っているかを確認するために、アクセス制御対象となる情報資産すべての棚卸しが必要になる場合がある。

これらの課題を踏まえて確認・検討を進める必要がある。

3.2.4. ロールデータの元データとその維持管理体制の定義時に直面する課題

ロール設計フェーズにおいて、ロールデータの元データをどのデータソースのものにするか、およびその維持管理体制の定義を進める時には、以下に挙げる課題に直面する。

(1) ロールデータの元データが存在しない、あるいは存在しても維持管理が実施できていない場合がある。
(2) 維持管理の組織への割り当てが難航する場合がある。

これらの課題を踏まえて検討・定義を進める必要がある。

補足）ロールデータの元データの維持管理が実施できていない場合として、単純に実施できていない場合の他に、データのオーナ＝維持管理責任者が明確に定められていない、あるいは、名目的に定められていても実質的にはガバナンスが利いておらずデータの整合が取れていないなどの場合がある。

3.2.5. IT ロールのスコープ定義時に直面する課題

ロール設計フェーズにおいて、IT ロールのスコープ定義を進める時には、以下に挙げる課題に直面する。

(1) IT ロールとして共通管理する範囲や粒度の落としどころの調整が難しい。

これらの課題を踏まえて検討・定義を進める必要がある。

補足）共通管理する意味のない特殊なロールは、IT ロールとして管理するスコープには含めずシステム個別に管理する、という整理の仕方もある。（例えば、組織横断の一時的なプロジェクト業務担当などの場合。）

3.2.6. IT ロール付与ルールとその例外の定義時に直面する課題

ロール設計フェーズにおいて、IT ロールを付与する際のルール、およびその例外の定義を進める時には、以下に挙げる課題に直面する。

(1) IT ロール付与ルールの例外をどこまで認めるか、セキュリティ・ガバナンスと運用のバランスを取る必要がある。

これらの課題を踏まえて検討・定義を進める必要がある。

表 3.2 ロール管理導入における課題

タスク	課題
ビジネスロールおよびビジネスロール付与ルールの調査	● ビジネスロールは組織に応じて様々である。 ● ビジネスロールの定義が曖昧な場合がある。 ● 兼務や委任/代行が多く、それに伴いビジネスロール付与ルールの例外が多く存在する場合がある。 ● 委任か代行かにより、責任の所在が異なり、ロールの扱いを変えなければならない場合がある。
システム権限および権限付与ルールの調査	● システム権限および権限付与ルールはシステムに応じて様々である。 ● 例外的な権限付与が実施されている場合がある。
アクセス制御の全体ポリシーの確認	● 実際のビジネスロールやシステム権限付与が、全体ポリシーと不整合を起こしている場合がある。 ● 全体ポリシーが実態に合っているかを確認するために、アクセス制御対象となる情報資産すべての棚卸しが必要になる場合がある。
ロールデータの元データおよび維持管理体制の定義	● ロールデータの元データが存在しない、あるいは存在しても維持管理が実施できていない場合がある。 ● 維持管理の組織への割り当てが難航する場合がある。
IT ロールのスコープ定義	● IT ロールとして共通管理する範囲や粒度の落としどころの調整が難しい。
IT ロール付与ルールおよび例外の定義	● IT ロール付与ルールの例外をどこまで認めるか、セキュリティ・ガバナンスと運用のバランスを取る必要がある。

まとめ

1. ロール管理導入の検討を進める時の課題として、表 3.2 に挙げるものが存在する。
2. ここに挙げた課題を踏まえて調査・検討・設計を進める必要がある。

3.3. 現状調査・企画フェーズ

このフェーズでは、ロール管理を行うにあたって、ロール設計のインプットとなる情報の調査を行う。また、ロール管理を企画するにあたって、ロール管理導入の目的や目指すべき目標像を明確化する。

3.3.1. 組織調査

(1) 目的

本タスクの目的はロール設計を行う上で重要なインプットとなる組織体制・階層を洗い出すことにある。

表 3.3 目的

	目的	具体的内容
1	組織情報の取得	組織体制図の調査。職位等の階層情報の調査。体制図に記述されていない委員会組織や部署内のチームレベルの体制等についての調査。同時に人事異動・組織変更のタイミングなどを調査する。 また、組織内の雇用形態や関連する規程についても調査を行う。

(2) 前提条件

本項目の前提となるインプット情報は下記の通りである。

表 3.4 前提となるインプット情報

	インプット情報	利用方法／必要性
1	社内組織図、人事課、部署内体制図、関連規程	（ベース資料）。

(3) 留意事項

本項目の留意事項は以下の通りである。

表 3.5 留意事項

	項目	内容
1	調査の粒度	あまりに細かい体制までを調査した場合に、組織の延べ数が膨大になる可能性がある。 あくまで、ロール＝権限のベース、であるため業務遂行上の権限が異なる組織情報を洗い出すことに留意する。

(4) 具体的な内容

下記のような情報を収集する。

表 3.6 収集する情報

	作業項目	作業内容
1	組織・部署構成調査（役職・階層含む）	社内組織図、部署内の体制図などを収集し、それぞれの組織の名称、業務内容の概要などをまとめる。 また、組織の上下関係（レポートライン）、役職・階層に関わる情報についても調査を行う。
2	拠点等調査	組織が複数拠点ある場合には、業務としての組織とは別に拠点ごとの組織体制・役職等がある場合が多いため、それらの情報について調査を行う。
3	雇用形態等調査	組織内の人員としては正社員、契約社員、嘱託、派遣、パート、委託先といった雇用形態が考えられ、それぞれで権限が異なる場合も多いので、それらの雇用形態について調査を行う。
4	関連社内規程調査	組織、人事に関連する社内規程について調査を行う。特に、組織図には記載されないが、社内規程で定めらる組織（○○委員会等）に注意する。

(5) 成果物

本段階の成果物は以下の通りである。

表 3.7 成果物一覧

	成果物	内容
1	調査メモ（組織）	組織の一覧、組織図等。

3.3.2. 職務分掌調査

(1) 目的

本タスクの目的はロール設計を行う上で重要なインプットとなる職務分掌を洗い出すことにある。

表 3.8 目的

	目的	具体的内容
1	職務分掌情報の調査	職務分掌は、組織内・組織間をまたがる業務において、誰が（どこが）どのような業務を行っているのか？また、申請・承認などの権限はどうなっているのかを調査し、最終的にロールに反映することを目的とする。

(2) 前提条件

本項目の前提となるインプット情報は下記の通りである。

表 3.9 前提となるインプット情報

	インプット情報	利用方法／必要性
1	職務分掌表 業務フロー 業務マニュアル・手順書 社内帳票 関連社内規程 ヒアリング 関連業務システムのアクセス権限情報	業務における権限、もしくは、業務における作業内容が記述されているため。 それらの資料がない場合には、現場へのヒアリングを通して、必要な情報を得る。

(3) 留意事項

本項目の留意事項は以下の通りである。

表 3.10 留意事項

	項目	内容
1	調査の粒度	あまりに細かいレベルまで調査した場合に、調査の工数・負荷が膨大になる可能性がある。
2	情報の正確性	職務分掌表、業務フロー、手順書等に書かれた情報が正確であるとは限らず、実際の現場では違う形・権限で行われているか、システム上の権限との齟齬がある場合がある。

(4) 具体的な内容

下記のような情報を収集する。

表 3.11 収集する情報

	作業項目	作業内容
1	職務分掌調査	インプットを収集・調査し、各業務における職務権限情報を抽出する。 また、各権限を保有する組織・階層などについても調査をしておく。

(5) 成果物

本段階の成果物は以下の通りである。

表 3.12 成果物一覧

	成果物	内容
1	調査メモ（職務分掌）	職務分掌の一覧。

3.3.3. ライン型業務調査

(1) 目的

本タスクの目的はロール設計を行う上で重要なインプットとなるライン型業務のロール情報を洗い出すことにある。

表 3.13 目的

	目的	具体的内容
1	ライン型業務の調査	ライン型業務は、組織内・組織間をまたがる業務において各組織・担当者の作業内容・権限が決まる。 それらの作業内容・権限がロールのインプットとなるため、それを調査する。

(2) 前提条件

本項目の前提となるインプット情報は下記の通りである。

表 3.14 前提となるインプット情報

	インプット情報	利用方法／必要性
1	業務フロー 業務マニュアル・手順書 関連帳票 ヒアリング 業務システムのアクセス権限情報	業務における権限、もしくは、業務における作業内容が記述されているため。 それらの資料がない場合には、現場へのヒアリングを通して、必要な情報を得る。

(3) 留意事項

本項目の留意事項は以下の通りである。

表 3.15 留意事項

	項目	内容
1	調査の粒度	あまりに細かいレベルまで調査した場合に、調査の工数・負荷が膨大になる可能性がある。
2	情報の正確性	業務フロー、手順書等に書かれた情報が正確であるとは限らず、実際の現場では違う形・権限で行われているか、システム上の権限との齟齬がある場合が

		ある。

(4) 具体的な内容

下記のような情報を収集する。

表 3.16 収集する情報

	作業項目	作業内容
1	ライン型業務調査	インプットを収集・調査し、各業務における職務権限情報を抽出する。 また、各権限を保有する組織・階層などについても調査をしておく。

(5) 成果物

本段階の成果物は以下の通りである。

表 3.17 成果物一覧

	成果物	内容
1	調査メモ（ライン型業務）	業務フロー、権限、役割等についてのメモ

3.3.4. プロジェクト型業務調査

(1) 目的

本タスクの目的はロール設計を行う上で重要なインプットとなるプロジェクト型業務のロール情報を洗い出すことにある。

表 3.18 目的

	目的	具体的内容
1	プロジェクト型業務の調査	プロジェクト型業務は、既存の組織の枠にとらわれずにプロジェクトチームを結成し、そのプロジェクトチームにおいて一定期間行われる業務である。そのため、既存の組織図等には表れないことが多い。それらのプロジェクトにおける役割・権限をベースとしたロールを抽出することを目的とする。

(2) 前提条件

本項目の前提となるインプット情報は下記の通りである。

表 3.19 前提となるインプット情報

	インプット情報	利用方法／必要性
1	プロジェクト体制図 ヒアリング	組織内に存在するプロジェクトのタイプを洗いだし、それぞれのタイプごとにプロジェクトの体制・プロジェクト内の役割等を洗い出す。

(3) 留意事項

本項目の留意事項は以下の通りである。

表 3.20 留意事項

	項目	内容
1	調査の粒度	プロジェクトの数が少なければ、全てを調べても構わないが、プロジェクトの数が多い場合には、プロジェクトタイプごとに典型的なプロジェクトについて調査をする、もしくはサンプリングによる調査をするようにしたほうがよい。

(4) 具体的な内容

下記のような情報を収集する。

表 3.21 収集する情報

	作業項目	作業内容
1	プロジェクトタイプ洗い出し	組織内においてどのようなタイプのプロジェクトのタイプがあるかを調査する。 例) ・毎年実施する○○委員会のようなもの ・特定顧客案件対応プロジェクト ・社内向け/社外向け
2	プロジェクト体制確認	プロジェクトタイプごとに、典型的なプロジェクトについてプロジェクト体制図の閲覧、ヒアリング等を通じて、プロジェクトチーム内の権限・役割について調査・整理をする。

(5) 成果物

本段階の成果物は以下の通りである。

表 3.22 成果物一覧

	成果物	内容
1	調査メモ（プロジェクト型業務)	プロジェクト型業務における、権限、役割等についてのメモ

3.3.5. 対象システム調査

(1) 目的

本タスクの目的はロール設計を行う上で重要なインプットとなる対象システムに現在設定されている権限情報を洗い出すことにある。

表 3.23 目的

	目的	具体的内容
1	対象システム調査	ロール管理の対象システムにおける現在のアクセス権限管理情報の内容を洗い出す。 また、現状のロールの運用管理がどのように行われているかを調査する。

(2) 前提条件

本項目の前提となるインプット情報は下記の通りである。

表 3.24 前提となるインプット情報

	インプット情報	利用方法／必要性
1	業務システムのアクセス権限情報	現行のシステムにおけるロールのため。
2	現状のロール管理運用についての資料	現状のロールの運用管理状況を確認するため。

(3) 留意事項

本項目の留意事項は以下の通りである。

表 3.25 留意事項

	項目	内容
1	不要権限の存在	実際のシステムにおいて ・ロール自体が不要（使用されていない）な場合 ・ID に不必要なロールを付与されている場合 が存在するため、ロールだけではなく、実際に利用されているかどうか？に留意すること

(4) 具体的な内容

下記のような情報を収集する。

表 3.26　収集する情報

	作業項目	作業内容
1	アクセス制御方式・アクセス権限管理方法の調査	システムの実装によって、アクセス制御方式・アクセス権限管理方法が異なるため、それぞれの対象システムについて調査を行う。 アクセス制御を行うための元となっている情報としては以下のようなものがある。 ・グループ/ロール（ID とは別の情報） ・ID に紐づく属性（ID が保有する情報の一部） ・ID も文字列上に表現されるもの（ID に組織コードが埋め込まれている等） また、業務ロジックから独立したアクセス制御システムだけでなく、プログラム中にロジックとして組み込まれるアクセス制御もあるため、注意する必要がある。
2	ロールの洗い出し	各システムのアクセス制御に利用されている権限情報を抽出する。
3	運用管理状況調査	各システムにおけるロールの運用管理状況を調査する。具体的には、下記の項目を調査する。 ● 現状行われているロール管理業務 ● ロールの運用フロー ● 運用管理体制 ● ロールの変更・更新のタイミング、頻度、工数 ● 認識されている問題点

(5)　成果物

本段階の成果物は以下の通りである。

表 3.27　成果物一覧

	成果物	内容
1	調査メモ（対象システム現状ロール）	対象システムごとのアクセス権限情報についてのメモ

3.3.6. 対象法規制調査

(1) 目的

本タスクの目的は法規制が対象組織のロールに与える影響を調査することにある。

表 3.28 目的

	目的	具体的内容
1	対象法規制の調査	対象組織が遵守すべき法令・基準等を調査し、それらを遵守するにあたって必要な対象組織内の体制等を洗い出す。

(2) 前提条件

本項目の前提となるインプット情報は下記の通りである。

表 3.29 前提となるインプット情報

	インプット情報	利用方法／必要性
1	遵守対象法令	社内の体制に影響をあたえるため。

(3) 留意事項

本項目の留意事項は以下の通りである。

表 3.30 留意事項

	項目	内容
1	業界ガイドライン・認証等	法令だけでなく、対象組織が属する業界の業界内ガイドライン、ISMS・プライバシーマーク・QMS などの認証・認定についても留意すること。

(4) 具体的な内容

下記のような情報を収集する。

表 3.31 収集する情報

	作業項目	作業内容
1	遵守対象法令の確認	遵守対象となる法令・業界ガイドライン等を確認する。
2	遵守対象法令による社内体制への影響の確認	対象法令・業界ガイドライン等において社内体制として定義されているもの、遵守する上で必要な体制を洗いだし、対象組織における現状との比較を行う。

(5) 成果物

本段階の成果物は以下の通りである。

表 3.32 成果物一覧

	成果物	内容
1	調査メモ（法規制・コンプライアンス）	法規制・コンプライアンス遵守に関連する体制等についてのメモ

3.3.7. 目的・目標の明確化

(1) 目的

本タスクの目的は、当該組織においてロール管理を導入するにあたっての目的と目指すべき目標像を明確化することである。

表 3.33 目的

	目的	具体的内容
1	現状の課題・問題点の把握	現状調査の結果から、現状の課題・問題点を整理し明確化する。
2	目的の明確化	課題・問題点から、ロール管理を実装することによって得られる最終的な効果を検討し、明確化する。
3	目標像の明確化	目的（最終的な効果）を得るために必要となるロール管理の実装におけるポイントとそれをどの程度実現するかについて、目標像を明確化する。

(2) 前提条件

本項目の前提となるインプット情報は下記の通りである。

表 3.34 前提となるインプット情報

	インプット情報	利用方法／必要性
1	現状調査メモ（各種）	課題・問題点の明確化のため

(3) 留意事項

本項目の留意事項は以下の通りである。

表 3.35 留意事項

	項目	内容
1	目標における実現レベルの明確化	目標としてロール管理実装におけるポイントを検討する際において、そのポイントにおける実現レベルを出来る限り具体化、ロール管理を実装することにより、どのようなシステム・運用管理になるか、の観点で具体化すること。
2	目的と目標の関係	目標はあくまで目的である最終的に得られる効果を生み出すために必要であるものとして、因果関係が考えられるものとすること。 ロール管理システム自体の導入が目的化しないようにすること。

(4) 具体的な内容

下記のような内容を検討する。

表 3.36 検討内容

	作業項目	作業内容
1	課題・問題点の把握	現状調査の結果から、現状のロール管理の運用における課題・問題点を整理し明確化する。
2	目的の明確化	問題点から、ロール管理を実現することにより、得るべき効果を検討し、ロール管理導入の目的を明確化する。
3	目標像の明確化	目的を実現するために必要となる、ロール管理導入における目標像を明確にする。
4	実現イメージの作成	ロール管理の導入後のシステム・運用管理業務の実現イメージを作成する。

(5) 成果物

本段階の成果物は以下の通りである。

表 3.37 成果物一覧

	成果物	内容
1	ロール管理導入計画	ロール管理における目的・目標像、実現イメージなどを計画としてまとめた文書

3.4. ロール設計フェーズ

このフェーズでは、現状調査・企画フェーズの結果に基づき、ロール設計を行う。

ロールを設計する手法は、そのアプローチにより大きく以下の 2 つに分けられる。

(1) Top Down 型モデリング

業務の改革に基づくシステム導入・見直しに伴い、「あるべき論」からロール定義の具体化を進める。

(2) Bottom Up 型モデリング

既に「実際に運用を回している」業務における「実際の権限設定」からロール定義の具体化を進める。

それぞれの手法を杓子定規に適用すると、「検討した結果のロール定義」が「実際に運用可能なロール定義」になっているかは見直さなければならない場合があり、注意が必要である。そこで、両方を組み合わせた「ハイブリッド型モデリング」と呼ぶ手法を取る場合もある。

なお、以下のようなプロジェクト型ロールの設計手法については、本節に記載するどの方法によっても適切な設計ができない場合もあるので、議論の余地がある。

- 組織に期限付きで割り当て実行する業務に付随するロール
- 専門家を集めたチーム内のロール
- 「定型」業務が無いプロジェクトに対するロール

以降では、まず、ロール設計の手法として、「Top Down 型モデリング」と「Bottom Up 型モデリング」、そして 2 つの混合である「ハイブリッド型モデリング」について説明する。その後、ロールの種類ごとの設計ステップについて説明していく。

3.4.1. Top Down 型モデリング

(1) モデリング手法の特徴

ロール定義の基になる組織上の役割や職務、ならびにそれらに関する規程類から、本来あるべきロール定義を導出する設計手法である。

具体的には、組織情報、人事情報、権限管理規程、職務分掌規程(segregation of duties)などを基に、本来あるべきロールを定義し、そのロールに本来付与されるべきアクセス権限の組み合わせを対応付ける、というアプローチで、ロール定義の具体化を進める。

なお、職務分掌規程には、一つの業務プロセスにおける実行者と承認者の両方の職務権限を同一者が保有することを禁止する規定があるはずである。これは近年の SOX 法への対応などにおいては重要な項目であり、組織情報／人事情報のみから設計する場合には見逃しがちなポイントなので、注意されたい。

Top Down 型のロール定義の進め方を、具体的なケースを想定して説明する。

一般的な組織で部長／課長／担当者のような階層構造となっている場合は、組織におけるそれぞれの役職に応じて職務や権限が付与されるので、組織および役職に応じたロール定義が導出できるはずである。また、職務分掌規程から同一者が保有してよい職務権限の範囲が制限される場合は、それを踏まえてロールを分割する。例えば、職務分掌規程にて、見積の作成権限と承認権限を同一者に付与してはならないルールが存在する場合は、見積の作成と承認を別のロールとして定義し、それぞれの権限が同一のロールに対応付けられないようにする。

一方で、組織や役職などに応じて決まる本来の職務とは異なる職務を担わざるを得ない事情が存在する場合もある。例えば、組織改編や人事異動の際に、以前に担っていた職務の適切な引き継ぎ先が無く、仕方なくその職務を継続して担っている場合など。そのような場合は、組織および役職などから導出したロール定義だけをそのまま適用しても、実際に必要となる権限が付与されないことになるので、それに付加的に、本来のあるべき姿とは異なる個別の権限を対応付けたりする必要が生じる。

Top Down 型では、事実として行われている例外は考慮せずにモデル化し、その後に現実的に運用可能なように修正を加えるというアプローチを取ることになる。

⑵ モデリングに必要な情報

ロール定義の基になる組織上の役割や職務、ならびにそれらに関する規程類からロール設計を行うので、それらに関する既存の定義情報はあるだけ収集し、参考にすることが必要となる。特に企業内の組織であれば、以下のような情報、ソース、属性が必要である。

■ 組織・人事情報

情報ソース：全社ディレクトリ情報・人事データベース・社内電話帳など

例１） 全社ディレクトリ上のユーザ属性情報
- 所属組織（事業部、センター、部、グループ、組織コード）
- 管理職／専門職（Individual Contributor）
- 決裁権限の有無
- 雇用形態（社員／コントラクターなど）
- 職位、階級、肩書き、役職
- 職務、職種　（営業／SE／法務など）
- 勤務事業所、勤務場所コード、住所
- 有資格・免許情報
- 国籍、市民権
- 座席位置
- 電話番号
- メールアドレス
- 上長、Report To
- 所属長
- 部下
- 所属プロジェクト、タスク、チーム

例２） 組織コード表

例３） 組織構成図

例４） レポーティングライン図

■　業務についての情報

情報ソース：業務フロー定義書

例１）　J-SOX 法への適合にあたり整備したものなど

情報ソース：規程・ガイドライン類

例１）法律、省令、自主規制、自社ガイドラインなど

例２）社内の業務情報の取り扱い基準、権限定義情報

例３）職務分掌規程、一覧

　　規制、ガイドラインで定められた分掌規程

例４）業務情報取り扱い基準、権限定義情報

　　決裁権限情報

　　承認者条件規程

情報ソース：業務マニュアル類

例１）業務フロー

　　業務上の役割、定義

　　フロー上に定義された役割

(3)　モデリング手法の適性

ロールに対応付けられるリソースおよび権限の関係が固定的である場合は、すなわち成熟した組織、業務、役割であり変更が少ない、あるいは、基になる属性が適正に管理できていることを意味する。このような場合には、Top Down 型モデリングでロール定義を導出する方法が適切である。

3.4.2. Bottom Up 型モデリング

(1) モデリング手法の特徴

実際に担当している業務や、実際に付与されているアクセス権限を基に、現実に即したロール定義を抽出する設計手法である。具体的には、実際に稼動しているアプリケーション上で実際に設定されているアクセス権限から、同一の権限の組み合わせを付与されているユーザのグループを見出し、ユーザとアクセス権限の組み合わせを対応付けるためのロールを定義する、というアプローチで、ロール定義の具体化を進める。

Bottom Up 型のロール定義の進め方を、具体的なケースを想定して説明する。

アプリケーションのアクセス権限設定情報の記録が資料として存在する場合は、それをマスタ情報として、同一権限および類似権限を付与されているユーザのグループの抽出を行うことができる。ただし、マスタ情報として扱うことができるのは、当該情報が適切にメンテナンスされ、かつ最新の状態である場合に限られる。適切に維持されていない場合には、資料上の情報からロール定義を抽出するだけでは足りず、実際のアプリケーション上のアクセス権限設定を調査する必要が生じる。とりわけ、アクセス制御処理がロジックとしてコーディングされている場合には、設定だけではなくアプリケーションロジックも調査する必要が生じることがある。

一方、記録が資料として存在しない場合は、いわゆるリバースエンジニアリング的な調査が必要になることもある。

また、アプリケーションの機能として実装されておらず、オフラインで運用として実施している業務までを含めたロール定義を行う場合は、アプリケーションの設計や設定に加えて、オフラインの業務運用プロセスも調査する必要が生じる。例えば、帳票入力業務において、入力実施時に出力された帳票類を第三者がチェックすることで、相互牽制を運用として実施している場合など。

Bottom Up 型では、多くの場合、完全に同一の権限を付与されているユーザのグループを抽出することは難しいので、ほぼ同一であるグループとして纏め、それに対応するロールを定義し、ユーザごとの差分の権限をどう対応付けるかを後から決めるというアプローチを取ることになる。

いずれの場合も、得られる結果は「実際の権限設定」をロール定義として表現し直すだけであり、多くの場合、膨大な数のロール定義に陥ることが懸念される。また、リバースエンジニアリングによる場合は、それをもってロール定義として良いかどうかは再考が必要であろう。

⑵ モデリングに必要な情報

実際の業務における権限設定からロール定義を抽出する方法であるので、業務およびリソース類への権限設定の情報を収集することが必要となる。

具体的には以下のような情報、ソース、属性が必要である。

■ リソース類に関する情報

情報ソース：システム情報

例１）ファイルサーバ上の ACL

ユーザ・グループとフォルダへのアクセス権限（R/W/D/U）

例２）情報共有ツールなどのアクセス権限リスト

グループウェアのアクセス権限

グループウェア内の権限（ロールの定義として存在している可能性あり）

例３）ワークフローシステム

承認権限回想情報、承認経路情報、決裁権限情報

例４）文書管理システム

ACL など

例５）既存 ID 管理システム（LDAP、Active Directory など）

実ディレクトリデータ

例６）既存業務アプリケーション

実 ID 設定、ロジック内に記載される権限割付

⑶ モデリング手法の適性

ロールに対応付けられるリソースおよび権限の関係が流動的である場合は、すなわち成熟していない組織、業務、役割であり変更が多い、あるいは、基になる属性が適正に管理されていない／できないことを意味する。このような場合には、Bottom Up 型モデリングでロール定義を抽出する方法が適切である。

3.4.3. ハイブリッド型モデリング

(1) モデリング手法の特徴

Top Down 型モデリングと Bottom Up 型モデリングの組み合わせによる設計手法をハイブリッド型モデリングと呼ぶ。

Top Down 型と Bottom Up 型のどちらを先に実行するかは、以下の 3 つの点による。

- 対象となる業務の種別
- 入手可能な資料
- ロール定義の目的

例えば、業務改善が目的で、ロール定義を見直すのであれば、「組織と業務の現状(As-Is)」を調査し（すなわち Bottom Up 型モデリングに準じた調査を行い）、その一方で業務改善の観点から「あるべき論(To-Be)」を検討し（すなわち Top Down 型モデリングの基になる検討を行い）、それらの比較からロール定義を見直すことが効果的だろう。

一方、十分に成熟した組織や業務であれば、Bottom Up 型モデリングと Top Down 型モデリングは高いレベルで一致することが期待される。このような場合には、大枠の導出は Top Down 型モデリングを用い、例外の抽出のために Bottom Up 型モデリングを用いることが効率的だろう。

いずれのモデリング手法でも、例外にこだわると膨大なロール定義に陥りがちなので、例外は設計の対象から外し、例外処理を付加するプロセスを別途確立する（例外としての証跡を残すなど）といった工夫が必要である。

3.4.4. 組織型ロール設計

(1) 目的

本タスクの目的はビジネスロールの中でも組織型ロールを設計することである。

表 3.38 目的

	目的	具体的内容
1	組織型ロールの設計	ビジネスロールの中の組織型ロールを設計する。 組織ロールは、対象組織の組織体制をベースにしたロールであり、現状調査の組織調査の結果を主なインプットとして作成する。 具体的には拠点、部署、役職・職位、雇用形態などがベースとなるロールである。

(2) 前提条件

本項目の前提となるインプット情報は下記の通りである。

表 3.39 前提となるインプット情報

	インプット情報	利用方法／必要性
1	調査メモ（組織）	拠点、部署、役職・職位、雇用形態についての組織ロールを洗い出すのに使用する。
2	調査メモ（職務分掌）	場合によるが、職務権限のベースが組織、役職・職位、雇用形態による場合があるため、その場合に組織ロールとして切り出す場合がある。
3	調査メモ（対象システム現状ロール）	設計したロールと現状システムにおける、組織ベースのロールについてすり合わせる。
4	ロール管理計画	ロール管理導入の目標・実現イメージとの摺合せを行う。

(3) 留意事項

本項目の留意事項は以下の通りである。

表 3.40 留意事項

	項目	内容
1	ロールの粒度	あくまで、ロール＝権限のベース、であるため業務遂行上の権限が異なる組織情報をロールとして定義するようにする。 最低限、個人以外の権限の最小単位を表現できるものを設計する必要がある。
2	ロール同士の関係	部署の場合、部→課→係のように上下関係があるものなどロール間に依存関係がある場合があり、その場合には、その関係についても設計情報として記述する。
3	現状システムの組織型ロールとの調整	現状システムに設定されているアクセス権限の中で組織としての権限が設定されているものを網羅するかどうかを決定する必要がある。
4	ロールの運用	ロールの設計情報として、ロールの作成タイミング、作成者、所有者、所属 ID 変更の申請タイミング・申請者・承認者等を決定しておく必要がある。
5	例外メンバの取り扱い	ロールのメンバについては、可能であれば例外のメンバと正規メンバを区別可能なように設計したほうが、運用管理が行いやすい。 例）「ロール A_正規」と「ロール A_例外」で分けるなど
6	ロール運用上の役割定義	ロールの運用を行うにあたって必要となる役割としては、下記のようなものがある。 ・ロールオーナ ・ロール監査担当 ・ロールオペレータ これらの役割は、内部統制の権限分離の観点から兼務が出来ないようにすることが望ましい。
7	メンバの決定方法	ロールメンバの決定はロールオーナが決定する場合が多いが、組織型ロールについては人事データにより決定されることが多い。

(4) 具体的な内容

下記のような内容を設計する。

表 3.41　設計内容

	作業項目	作業内容
1	ロール定義	組織、職務分掌の調査メモより、組織型ロールを設計する（トップダウン）。 また、ロールメンバの条件・例外対応についても定義を行う。
2	現状システムアクセス権限すりあわせ	トップダウンで設計したロールと現状システムアクセス権限を摺合せ、ロールの粒度を確認する。
3	ロール間関係定義	設計したロール間の関係（上下関係、包含関係等）を整理する。 例）部・課の関係、ある職位以上、などの関係等
4	ロール運用情報定義	ロール運用に関する情報を定義する。

(5) 成果物

本段階の成果物は以下の通りである。

表 3.42　成果物一覧

	成果物	内容
1	ロール設計書（組織型ロール）	組織型ロールの一覧および説明

3.4.5. ライン型ロール設計

(1) 目的

本タスクの目的はビジネスロールの中でもライン型ロールを設計することである。

表 3.43 目的

	目的	具体的内容
1	ライン型ロールの設計	ビジネスロールの中のライン型ロールを設計する。ライン型ロールは、組織の業務プロセスに関係するロールであり、主にシステムの機能（入力・作成、実行、承認）等に関する機能に関するロールを設計する。

(2) 前提条件

本項目の前提となるインプット情報は下記の通りである。

表 3.44 前提となるインプット情報

	インプット情報	利用方法／必要性
1	調査メモ（ライン型業務）	ライン型業務ロールを洗い出すのに使用する。
2	調査メモ（職務分掌）	場合によるが、職務分掌においてライン型業務の職務分掌を定義している場合もあるため。
3	調査メモ（対象システム現状ロール）	設計したロールと現状システムにおける、ライン型業務のロールについてすり合わせる。
4	ロール管理計画	ロール管理導入の目標・実現イメージとの摺合せを行う。

(3) 留意事項

本項目の留意事項は以下の通りである。

表 3.45 留意事項

	項目	内容
1	ロールの粒度	あくまで、ロール＝権限のベース、であるため業務遂行上の権限が異なる業務権限をロールとして定義するようにする。最低限、個人以外の権限の最小単位を表現できるものを設計する必要がある。
2	ロール同士の関係	ライン型業務においては、一つの業務の流れの中で複数のロールが設定される（例：○○業務の入力権限と承認権限、等）。また、ロール間における職務分離の関係もありうる（申請権限と承認権限の分離など）。このようにライン型ロールにおいては、ライン型業務ごとにロールが複数設定されることが多いため、それらを意識して設計する必要がある。
3	現状システムのライン型ロールとの調整	現状システムに設定されているアクセス権限の中でライン型業務の権限が設定されているかを確認する必要がある。
4	ロールの運用	ロールの設計情報として、ロールの作成タイミング、作成者、所有者、所属 ID 変更の申請タイミング・申請者・承認者等を決定しておく必要がある。
5	例外メンバの取り扱い	ロールのメンバについては、可能であれば例外のメンバと正規メンバを区別可能なように設計したほうが、運用管理が行いやすい。 例）「ロール A_正規」と「ロール A_例外」で分けるなど
6	ロール運用上の役割定義	ロールの運用を行うにあたって必要となる役割としては、下記のようなものがある。 ・ロールオーナ・ロール監査担当・ロールオペレータ これらの役割は、内部統制の権限分離の観点から兼務が出来ないようにすることが望ましい。
7	メンバの決定方法	ロールメンバの決定は業務フロー等により決定される場合、ロールオーナにより決定されることが多い。

(4) 具体的な内容

下記のような内容を設計する。

表 3.46　設計内容

	作業項目	作業内容
1	ロール定義	ライン型業務の調査メモより、ライン型ロールを設計する（トップダウン）。 また、ロールメンバの条件・例外対応についても定義を行う。
2	現状システムアクセス権限すりあわせ	トップダウンで設計したロールと現状システムアクセス権限を摺合せ、ロールの粒度を確認する。
3	ロール間関係定義	設計したロール間の関係を整理する。 例：ロール間における職務分離等
4	ロール運用情報定義	ロール運用に関する情報を定義する。

(5) 成果物

本段階の成果物は以下の通りである。

表 3.47　成果物一覧

	成果物	内容
1	ロール設計書（ライン型ロール)	ライン型ロールの一覧および説明

3.4.6. プロジェクト型ロール設計

(1) 目的

本タスクの目的はビジネスロールの中でもプロジェクト型ロールを設計することである。

表 3.48 目的

	目的	具体的内容
1	プロジェクト型ロールの設計	ビジネスロールの中のプロジェクト型ロールを設計する。 プロジェクト型ロールは、対象組織におけるプロジェクト（期間限定の一時的な組織・チーム）をベースにしたロールであり、現状調査の組織調査およびプロジェクト型業務調査の結果を主なインプットとして作成する。

(2) 前提条件

本項目の前提となるインプット情報は下記の通りである。

表 3.49 前提となるインプット情報

	インプット情報	利用方法／必要性
1	調査メモ（組織）	組織の中にプロジェクトとして扱うべき組織がある場合がある。
2	調査メモ（プロジェクト型業務）	プロジェクト型業務の内容。
3	調査メモ（対象システム現状ロール）	設計したロールと現状システムにおける、プロジェクト型業務ベースのロールについてすり合わせる。
4	ロール管理計画	ロール管理導入の目標・実現イメージとの摺合せを行う。

(3) 留意事項

本項目の留意事項は以下の通りである。

表 3.50 留意事項

	項目	内容
1	ロールの粒度	あくまで、ロール＝権限のベース、であるため業務遂行上の権限が異なるプロジェクト型業務情報をロールとして定義するようにする。 最低限、個人以外の権限の最小単位を表現できるものを設計する必要がある。
2	ロール同士の関係	プロジェクト型ロールはプロジェクトに一つということではなく、プロジェクト内においても複数の業務があることがあるため、そのあたりを留意する。
3	現状システムのプロジェクト型ロールとの調整	現状システムに設定されているアクセス権限の中でプロジェクト型業務としての権限が設定されているものを網羅するかどうかを決定する必要がある。
4	ロールの運用	ロールの設計情報として、ロールの作成タイミング、作成者、所有者、所属 ID 変更の申請タイミング・申請者・承認者等を決定しておく必要がある。
5	例外メンバの取り扱い	ロールのメンバについては、可能であれば例外のメンバと正規メンバを区別可能なように設計したほうが、運用管理が行いやすい。 例）「ロール A_正規」と「ロール A_例外」で分けるなど
6	ロール運用上の役割定義	ロールの運用を行うにあたって必要となる役割としては、下記のようなものがある。 ・ロールオーナ ・ロール監査担当 ・ロールオペレータ これらの役割は、内部統制の権限分離の観点から兼務が出来ないようにすることが望ましい。
7	メンバの決定方法	ロールメンバの決定はロールオーナが決定する場合が多い。

(4) 具体的な内容

下記のような内容を設計する。

表 3.51　設計内容

	作業項目	作業内容
1	ロール定義	組織、プロジェクト型業務の調査メモより、プロジェクト型ロールを設計する（トップダウン）。 また、ロールメンバの条件・例外対応についても定義を行う。
2	現状システムアクセス権限すりあわせ	トップダウンで設計したロールと現状システムアクセス権限を摺合せ、ロールの粒度を確認する。
3	ロール間関係定義	設計したロール間の関係（上下関係、包含関係等）を整理する。 例）ロール間の関係等
4	ロール運用情報定義	ロール運用に関する情報を定義する。

(5) 成果物

本段階の成果物は以下の通りである。

表 3.52　成果物一覧

	成果物	内容
1	ロール設計書（プロジェクト型ロール）	プロジェクト型ロールの一覧および説明

3.4.7. システムアクセス権限設計

(1) 目的

本タスクの目的はシステムアクセス権限を設計することである。

表 3.53 目的

	目的	具体的内容
1	システムアクセス権限設計	実際のシステムにおけるアクセス権限を設計する。

(2) 前提条件

本項目の前提となるインプット情報は下記の通りである。

表 3.54 前提となるインプット情報

	インプット情報	利用方法／必要性
1	調査メモ（各種）	各種の調査メモをベースにシステムのアクセス権限情報のベースとする。
2	調査メモ（対象システム現状ロール）	現状システムに設定されているアクセス権限を確認する。
3	ロール管理計画	ロール管理導入の目標・実現イメージとの摺合せを行う。

(3) 留意事項

本項目の留意事項は以下の通りである。

表 3.55　留意事項

	項目	内容
1	現行システムにおけるアクセス権限の例外の扱い	現行システムのアクセス権限において、例外が存在している場合が多く、それを見分ける必要がある。
2	不要なアクセス権限	現行システムにおいて、不要となっているアクセス権限が存在している場合があるため、気をつける必要がある。
3	ビジネスロールの考慮	システムのアクセス権限を決定する際には、システムの用途・目的等により、どのビジネスロールを採用するかについて留意する。

(4) 具体的な内容

下記のような内容を設計する。

表 3.56　設計内容

	作業項目	作業内容
1	システムアクセス権限設計	システムアクセス権限の設計を行う。
2	ロール運用情報定義	ロール運用に関する情報を定義する。

(5) 成果物

本段階の成果物は以下の通りである。

表 3.57　成果物一覧

	成果物	内容
1	システムアクセス権限設計書	システムアクセス権限の一覧および説明

3.4.8. IT ロール設計

(1) 目的

本タスクの目的はビジネスロールとシステムアクセス権限の関係を定義する IT ロールを設計することである。

表 3.58 目的

	目的	具体的内容
1	IT ロールの設計	ビジネスロールとシステムアクセス権限から IT ロールの設計を行う。

(2) 前提条件

本項目の前提となるインプット情報は下記の通りである。

表 3.59 前提となるインプット情報

	インプット情報	利用方法／必要性
1	ロール設計書（各種）	ビジネスロール（組織型、ライン型、プロジェクト型）の情報。
2	システムアクセス権限設計書	システムアクセス権限の情報。

(3) 留意事項

本項目の留意事項は以下の通りである。

表 3.60 留意事項

	項目	内容
1	ロール運用	ビジネスロールとシステムアクセス権限の関係が同じ場合でも、ビジネスロールの運用が異なる場合には別 IT ロールとなる場合もあるので注意する。

(4) 具体的な内容

下記のような内容を設計する。

表 3.61　設計内容

	作業項目	作業内容
1	IT ロール設計	ビジネスロールとシステムアクセス権限の関係を IT ロールとして定義する。 具体的には、ビジネスロールに紐づくシステムアクセス権限をまとめ、ロール運用を考慮したうえで、IT ロールを定義する。

(5) 成果物

本段階の成果物は以下の通りである。

表 3.62　成果物一覧

	成果物	内容
1	IT ロール設計書	IT ロールの一覧および説明

3.5. 実装方式設計フェーズ

このフェーズでは、ロール管理を行うにあたって、ロール設計のインプットとなる情報の調査を行う。

3.5.1. プロビジョニング方式設計

(1) 目的

本タスクの目的はロール情報のプロビジョニングをどのように実装するかの設計を行うことにある。

表 3.63 目的

	目的	具体的内容
1	プロビジョニング方式設計	設計されたロールについて、レポジトリで定義されたロールをどのように対象システムに連携するか（プロビジョニングするか）を決定する。

(2) 前提条件

本項目の前提となるインプット情報は下記の通りである。

表 3.64 前提となるインプット情報

	インプット情報	利用方法／必要性
1	ビジネスロール設計書	ロール情報
2	IT ロール設計書	ロール情報
3	システムアクセス権限設計書	対象システムのアクセス権限情報
4	ロール管理計画	ロール管理導入の目標・実現イメージとの摺合せを行う。

(3) 留意事項

本項目の留意事項は以下の通りである。

表 3.65 留意事項

	項目	内容
1	プロビジョニング方式	対象システムによって、プロビジョニング方式が異なる。
2	プロビジョニングのトリガ	プロビジョニングが行われるトリガとなるイベントを意識する。 特に、レポジトリ側、対象システム側の双方で対応できる必要があるため留意する。
3	エラー処理	プロビジョニングが何等かの原因で失敗した場合に、エラーの検知、データの整合性確保、再処理の方法等について留意する。

(4) 具体的な内容

下記のような内容を設計する。

表 3.66 設計内容

	作業項目	作業内容
1	プロビジョニングのトリガの洗い出し	プロビジョニングが実行されるトリガとなるイベントを洗い出す。
2	プロビジョニング内容の特定	プロビジョニングのイベントごとに、どのようなロール情報を対象システムへ送信するのかを特定する。
3	プロビジョニング実装方式の検討	対象システムごとにイベントごとのプロビジョニングの実装方式を検討する。 エラー処理等についてもここで検討する。

(5) 成果物

本段階の成果物は以下の通りである。

表 3.67 成果物一覧

	成果物	内容
1	プロビジョニング方式設計書	プロビジョニング方式を記述する。

3.5.2. ロール運用設計

(1) 目的

本タスクの目的はロール管理の運用設計を行うことにある。

表 3.68　目的

	目的	具体的内容
1	ロール運用設計	ロール管理としてのロールの運用の設計を行う。 ロールのライフサイクル、運用フロー・運用タスクの設計を行う。

(2) 前提条件

本項目の前提となるインプット情報は下記の通りである。

表 3.69　前提となるインプット情報

	インプット情報	利用方法／必要性
1	ビジネスロール設計書	ロール情報
2	IT ロール設計書	ロール情報
3	システムアクセス権限設計書	対象システムのアクセス権限情報
4	調査メモ（各種）	ロールのライフサイクル、管理についての情報
5	ロール管理計画	ロール管理導入の目標・実現イメージとの摺合せを行う。

(3) 留意事項

本項目の留意事項は以下の通りである。

表 3.70 留意事項

	項目	内容
1	ライフサイクルとイベント	運用は何らかのトリガによって発生するため、ロール自体のライフサイクルと日常のトリガに留意する必要がある。 また、ライフサイクルとしては以下のようなものがある。 例）新規作成、メンバ変更（追加・削除）、ロール定義変更、ロール削除
2	運用フロー	プロビジョニングが行われるトリガとなるイベントを意識する。 特に、レポジトリ側、対象システム側の双方で対応できる必要があるため留意する。
3	例外処理	プロビジョニングが何等かの原因で失敗した場合に、エラーの検知、データの整合性確保、再処理の方法等について留意する。
4	コンプライアンス	ロールはシステム上の権限に直結しているためアクセス管理の重要な一要素となる。従って J-SOX 対応のみならず、不正アクセス禁止法等においても重要であるため、それらへの対応に留意する必要がある(例：定期棚卸など)。
5	ロールの種類ごとに異なる運用フロー	同じロールの運用業務であっても、ロールの種類が異なると、運用フローが異なる場合もあることに留意する。 例）組織型ロールとプロジェクト型ロールの作成・変更のフローなど。

(4) 具体的な内容

下記のような内容を設計する。

表 3.71 設計内容

	作業項目	作業内容
1	ライフサイクル定義（イベント洗い出し）	ロール管理における運用を洗い出すため、ロール自体のライフサイクルから、その中でのイベントを洗い出す。
2	運用フロー定義	洗いだされたイベントごとに運用フローを検討する。
3	運用タスク定義	運用フローで定義された運用タスクの内容を定義する。

(5) 成果物

本段階の成果物は以下の通りである。

表 3.72 成果物一覧

	成果物	内容
1	ロール運用設計書	ロール運用について記述する。

3.5.3. ロール管理対象範囲の確定

(1) 目的

本タスクの目的はロール管理を行う対象システムの範囲を確定することである。

なお、本タスクは、今フェーズより以前のフェーズにおいて実施される場合もある。

表 3.73 目的

	目的	具体的内容
1	ロール管理対象範囲の確定	統合的なロール管理を行う対象範囲を確定する。 具体的には、統合 ID 管理を行う範囲の中で、統合ロール管理を行う範囲の確定を行う。

(2) 前提条件

本項目の前提となるインプット情報は下記の通りである。

表 3.74 前提となるインプット情報

	インプット情報	利用方法／必要性
1	ビジネスロール設計書	ロール情報
2	IT ロール設計書	ロール情報
3	システムアクセス権限設計書	対象システムのアクセス権限情報
4	プロビジョニング方式設計書	プロビジョニング方式の実現可能性・工数等の情報
5	ロール運用設計書	ロール運用に関する情報。

(3) 留意事項

本項目の留意事項は以下の通りである。

表 3.75 留意事項

	項目	内容
1	プロビジョニング方式	対象システムによってロール情報のプロビジョニングが技術的に可能か、工数的に可能かどうか、等の検討によって対象範囲を検討する必要がある。
2	対象範囲外となるシステムについて	対象範囲外となるシステムについては、当該システムにおいてロール管理・運用をどのようにするかを再度確認する必要がある。

(4) 具体的な内容

下記のような内容を検討する。

表 3.76 検討内容

	作業項目	作業内容
1	対象範囲の検討	ロール管理対象範囲の確定を行う。

(5) 成果物

本段階の成果物は以下の通りである。

表 3.77 成果物一覧

	成果物	内容
1	検討メモ	プロビジョニング範囲検討のメモ

3.6. 実装・移行・展開フェーズ

このフェーズでは、ロール管理の実装・移行・展開を行う。

3.6.1. 実装・移行・展開の計画

(1) 目的

本タスクの目的はロール管理の実装・移行・展開を計画することである。

表 3.78 目的

	目的	具体的内容
1	ロール実装・移行・展開計画	ロール管理の実装・移行・展開計画。 プロビジョニングの実装、現行ロールから新ロールへの変更、運用の変更等の移行および展開の計画を立案する。

(2) 前提条件

本項目の前提となるインプット情報は下記の通りである。

表 3.79 前提となるインプット情報

	インプット情報	利用方法／必要性
1	ビジネスロール設計書	ロール情報
2	IT ロール設計書	ロール情報
3	システムアクセス権限設計書	対象システムのアクセス権限情報
4	プロビジョニング方式設計書	プロビジョニングの実装等についての情報
5	ロール運用設計書	ロールの運用等の情報
6	調査メモ（ロール管理対象範囲の確定）	移行・展開の範囲の情報

(3) 留意事項

本項目の留意事項は以下の通りである。

表 3.80 留意事項

	項目	内容
1	実装・移行・展開方式	ロール管理の対象範囲への実装・移行・展開を、一度にやってしまうのか、何回かに分けて段階的に行うのかによって、考慮することが異なる。
2	新ロールへの変更	対象範囲全体（レポジトリ、対象システム）において新ロール全体が整合している必要があるため、それら新ロールを現ロールからどのように変更する（切り替える）のかに留意する必要がある。
3	運用開始タイミング	どのタイミングから新ロールでの運用を開始するかを移行・展開方式と合わせて検討する必要あり。
4	利用者への周知	ロールは利用者にも密接に関わるため、稼働後の混乱を減らすため、利用者への周知についても留意する必要がある。

(4) 具体的な内容

下記のような内容を検討する。

表 3.81 検討内容

	作業項目	作業内容
1	実装・移行・展開方式の決定	実装・移行・展開方式をどのようにするかを決定する。
2	実装・移行・展開作業タスクの洗い出し	実装・移行・展開に必要な作業の洗い出しを行う。
3	ロール切り替え方式の検討	新ロールへの切り替えの方法について検討する。
4	利用者への周知計画	利用者への周知についての計画を検討する。

(5) 成果物

本段階の成果物は以下の通りである。

表 3.82 成果物一覧

	成果物	内容
1	実装・移行・展開計画書	実装・移行・展開についての計画書。

3.6.2. 実装・移行・展開の実施

(1) 目的

本タスクの目的はロール管理の実装・移行・展開を実施することである。

表 3.83 目的

	目的	具体的内容
1	ロール実装・移行・展開実施	実装・移行・展開計画書に基づき、実装・移行・展開を実施する。

(2) 前提条件

本項目の前提となるインプット情報は下記の通りである。

表 3.84 前提となるインプット情報

	インプット情報	利用方法／必要性
1	ビジネスロール設計書	ロール情報
2	IT ロール設計書	ロール情報
3	システムアクセス権限設計書	対象システムのアクセス権限情報
4	プロビジョニング方式設計書	プロビジョニングの実装等についての情報
5	ロール運用設計書	ロールの運用等の情報
6	調査メモ（ロール管理対象範囲の確定）	実装・移行・展開の範囲の情報
7	実装・移行・展開計画書	実装・移行・展開計画書

(3) 留意事項

本項目の留意事項は以下の通りである。

表 3.85 留意事項

	項目	内容
1	実データの投入・検証	実装・移行・展開においては、ロールの定義はもちろんのこと、各ロールへのロールメンバの登録も行うことになり、当然のことながら、システムのアクセス権限に関わる部分が変更されていることになる。 したがって、それらのデータの投入を行った後に、現場業務が適切に実行可能の検証が必要となる。

(4) 具体的な内容

下記のような作業を実施する。

表 3.86 実施作業

	作業項目	作業内容
1	実装・移行・展開の実施	実装・移行・展開計画書に基づき、実装・移行・展開を実施する。

(5) 成果物

本段階の成果物は以下の通りである。

表 3.87 成果物一覧

	成果物	内容
1	(特に規定せず)	

第4章
ロール管理の運用

4.1. ロール管理の適正な運用の重要性

ロールを利用することで、リソースへのアクセス権限管理を効率化でき、リスクを低減できることは、本書の冒頭にも述べた通りである。

しかしながら、ロール自体あるいはロールのメンバは、例えば人事異動や組織改編、プロジェクトメンバの変更、業務フローの変更など、様々な変化にさらされる。こうした変化に適切なタイミングで対応できるように運用しなければ、逆に権限が不足することによる業務の停止や、過剰な権限が付与されていることによる情報漏洩といったリスクが増してしまう。

そのため、ロールの適正な運用を設計し実装・実施することは、ロールを利用することによるメリットの最大化のために欠かせない。

4.2. ロール管理運用の観点

本節ではロール管理の運用を行う上で、考慮すべき観点について記述する。

ロール管理運用は以下 3 つの観点から整理する必要がある。

(1) ロールのライフサイクル

(2) ロール管理運用フロー

(3) ロール管理のアクタとその役割

以下の項ではそれぞれの観点について説明する。

4.2.1. ロールのライフサイクル

本項では、ロール管理運用の観点の一つである、ロールのライフサイクルについて記述する。

その中で、ロールのライフサイクルに関与する、ロール定義の基になる情報とロール管理運用のトリガとなるイベントについて記述する。そして、ロールのライフサイクルの中で生じるロール管理運用の各種操作や棚卸しについて記述する。

ロールは、人事情報やプロジェクト情報などに基づいて定義する。そのため、これらの情報に追加・変更・削除が生じると、それをトリガのイベントとして、ロール管理の運用が生じる。

ロールとそのロール定義の基になる情報、およびその情報に変更が生じるトリガとなるイベントの例を、いくつか下表に示す。

表 4.1　ロール定義の基になる情報、およびロール管理運用のトリガとなるイベント（例）

ロール	ロール定義の基になる情報	ロール管理運用のトリガイベント
組織型ロール（ビジネスロール)	人事情報、組織情報	人事異動の発令、組織改編の発令
プロジェクト型ロール（ビジネスロール)	プロジェクト情報（プロジェクトの業務、構成員などを含む)	新しいプロジェクトの開始申請の承認、プロジェクトメンバの変更申請の承認
アプリケーションロール	アプリケーションの業務要件、ユースケース	新しいアプリケーションの追加、既存アプリケーションの入れ替え

*：上表に見られる通りビジネスロールとアプリケーションロールについては最初のトリガとなるイベントが生じうる。一方 IT ロールは、最初のトリガに対応してビジネスロールあるいはアプリケーションロールに生じたロール管理運用をトリガとして、従属的にロール管理運用が生じる。このため、上表には IT ロールが含めていない。ロール管理運用におけるそうした運用フローは 4.2.2 ロール管理運用フローに詳述する。

また、上記ロール定義の基になる情報に変更が生じる際には、必要な権限を持つ人がその変更を承認する。そのため、その承認を行うアクタ及び承認のプロセスも観点として考慮する必要がある。

上記のとおり、トリガとなるイベントが発生すると、ロール管理の運用が生じる。

ロールが作成されてから削除されるまでのライフサイクルの中で、ロール管理に関して発生する運用の操作を以下に挙げる。

- 作成
- 変更
  - ロール定義の変更
  - ロールに割り当てられた権限の変更
  - ロールメンバの変更
  - ロールオーナ*の変更
- 削除
- 棚卸し
  - ロール要否の棚卸し
  - ロールに割り当てられた権限の棚卸し
  - ロールメンバの棚卸し
  - ロールオーナ*の棚卸し

*：ロールオーナの定義については 4.2.3 ロール管理運用におけるアクタとその役割で記述した。

このロールライフサイクルの状態遷移を図に示すと図 4.1 の通りである。

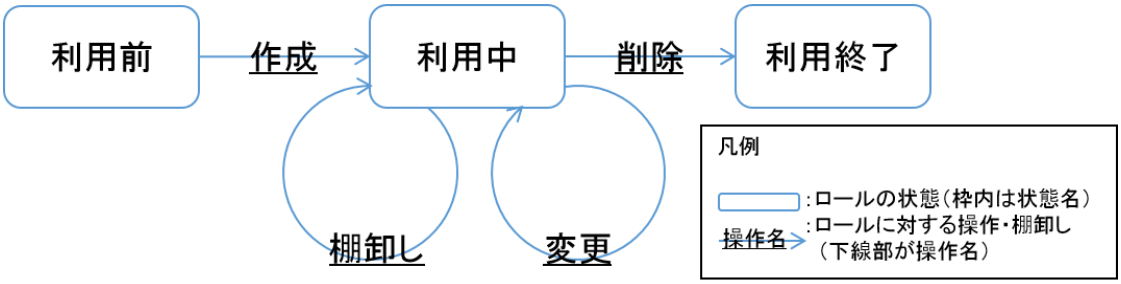


図 4.1　ロールのライフサイクル

上記のとおり、ロール管理の運用は、ロールのライフサイクルに関する以下の観点で考慮し整理する必要がある。

・　ロール定義の基になる情報とその承認プロセス
・　ロール管理運用が生じるトリガとなるイベント
・　ロールライフサイクルにおけるロール管理運用の各種操作

4.2.2. ロール管理運用フロー

ロール管理運用においては、前項に記述した通り、トリガとなるイベントが生じると、それに応じてロール管理運用を実施する。本項では、ロール管理運用を実施する際の運用フローを記述する。

本書のこれまでの章で記述してきた通り、ビジネスロール、アプリケーションロール、IT ロールは相関している。そのため、いずれかのロールについて設計変更及びそれに基づく操作あるいは棚卸しを実施した場合、そのロールに関係する別のロールについても設計の変更及び操作や棚卸しの実施要否を判断し、必要に応じて設計の変更やそれに基づく操作あるいは棚卸しを実施しなければならない。

ロールの管理運用はこのように連鎖的に生じるため、以下の項目を意識する必要がある。

- 最初のトリガとなるイベント（以降「トリガイベント」とする）
- トリガイベントが最初に影響するロール
- 上記ロールに生じた変更が従属的に影響するロール（あるいはさらにそのロールの変更が影響する別のロール）

トリガイベントは、組織変更や人事異動、新しいプロジェクトの開始などビジネス側で生じるケースと、新しいアプリケーションの利用などアプリケーション側で生じるケースがある。前者の場合、直接変更が生じるロールはビジネスロールとなり、後者の場合、直接変更が生じるロールはアプリケーションロールとなる。それぞれのケースの運用フローを下表に示す。

なお、IT ロールはビジネスロールとアプリケーションロールの仲立ちを担うため、ビジネスロールあるいはアプリケーションロールに生じた変更による影響を受けて IT ロールが変更されることはあるが、IT ロールに直接変更が生じるトリガイベントが発生することはない。

表 4.2　トリガイベントがビジネス側で生じるケースのロール管理運用フロー

No.	フロー概要
1	ビジネスロールの操作や棚卸しを行うトリガイベントが発生する
2	トリガイベントについて、ビジネスロール設計の変更要否を判断し、必要があればビジネスロールの設計を変更する
3	トリガイベントについてビジネスロール設計に基づいて、ビジネスロールに対する操作や棚卸しを実施する
4	上記ビジネスロールに対する操作や棚卸しの結果、IT ロールあるいはアプリケーションロール設計の変更要否を判断し、必要があれば各ロール設計を変更する
5	IT ロールあるいはアプリケーションロールの設計に基づいて、IT ロールやアプリケーションロールに対して必要となる操作や棚卸しを決定し実施する

表 4.3　トリガイベントがアプリケーション側で生じるケースのロール管理運用フロー

No.	フロー概要
1	アプリケーションロールの操作や棚卸しを行うトリガイベントが発生する
2	トリガイベントにおいて、アプリケーションロール設計の変更要否を判断し、必要があればアプリケーションロールの設計を変更する
3	トリガイベントにおいて、アプリケーションロールの設計に基づいて、アプリケーションロールに対して必要となる操作や棚卸しを決定し実施する
4	変更されたアプリケーションロールについて、ビジネスロールや IT ロール設計の変更要否を判断し、必要があれば各ロールの設計を変更する
5	変更されたビジネスロールや IT ロール設計に基づいて、各ロールに対する操作や棚卸しを実施する

上記のとおり、ロール管理運用においては、

・　トリガイベントが生じる場所（ビジネスかアプリケーションか）

・　トリガイベントによって生じる直接的及び連鎖的に生じるロールの変更

を考慮する必要がある。

以上の運用フローを、下記の背景の下に発生するトリガイベントがビジネス側で生じる場合のロール管理運用を例にとって、具体的に下表に示す。

背景：

従来、営業部配下に営業１課と営業２課があったが、事務処理が増えつつあった。各営業課員の事務処理負担軽減のため、組織改編に際して営業に関する事務処理を横断的に担当する「営業サポート課」を新設することになり、組織改編が発令された。

組織改編前後の組織図と業務上の社内システム利用を図示すると、下図の通りとなる。

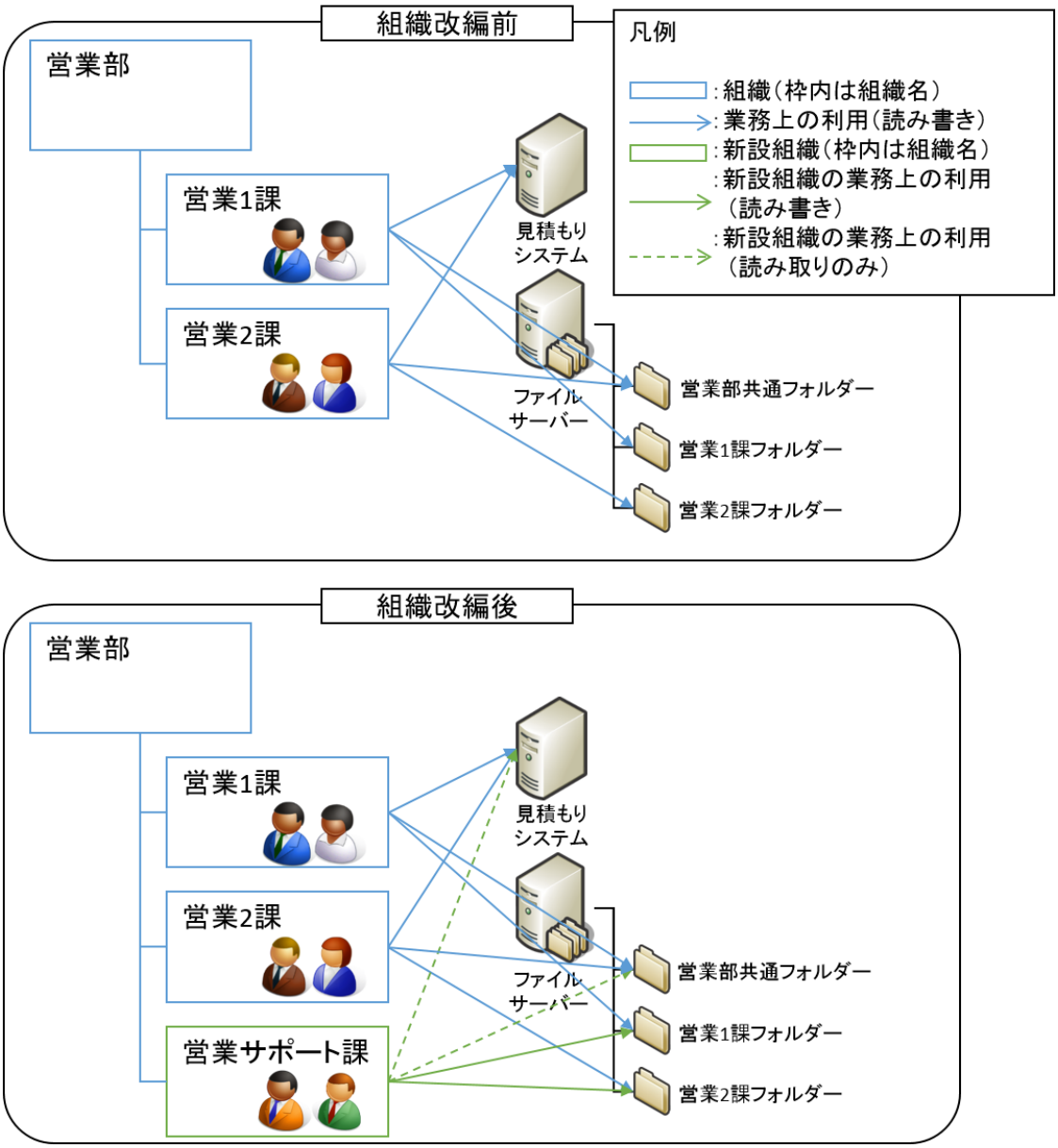


図 4.2　組織改編前後の組織図と業務上の社内システム利用

表 4.4　前述の背景の例におけるロール管理運用フローと具体的なタスク

No.	具体的なタスク	決定者もしくは操作者
1	－（イベントの発生時にはタスクは生じない）	－
2	新設する営業サポート課の業務内容を決定する営業部長が、営業サポート課の業務内容について、業務上社内システムを利用する必要があることを考慮し、「営業サポート課」のビジネスロール新設が必要と判断。また当該ロールのメンバは正社員や派遣社員などの雇用形態とは無関係に「営業サポート課」の課員とすることを判断。 上記判断を受けて、ビジネスロールの設計に「営業サポート課」ビジネスロールを追加。	営業部長
	営業サポート課の課長が、「営業サポート課」ビジネスロールのメンバとなるべき具体的な課員を判断。	営業サポート課課長
3	営業部長の判断を受けて、ビジネスロールの操作を行う担当者が「営業サポート課」ビジネスロールを作成。 また、営業サポート課課長の判断を受けて「営業サポート課」のメンバに適切な課員を登録。	ビジネスロールの操作を行う担当者
4	営業サポート課の業務内容に基づき、業務に関係する各アプリケーションのオーナが、「営業サポート課」ビジネスロールに割り当てるべき必要なアクセス権限を以下のように判断。 A) 見積もりに関する情報を利用することから、見積もりシステムへの読み取り権限 B) 営業 1 課及び 2 課双方の情報を利用することから、ファイルサーバ上の双方のフォルダへの読み取り権限 C) 営業部に所属するので、営業部共通フォルダへの読み取り権限	業務で利用する各アプリケーションのオーナ
	各アプリケーションのオーナが、営業サポート課の業務遂行に必要な上記 A～C のアクセス権限を与えるためのロールを確認したところ、以下の IT ロールが既存 ・ 営業情報読み取り IT ロール： 営業部以外の各部長及び課長に、営業関係情報の読み取りを許すため設けてあった IT ロール。見積もりシステム、営業部共通フォルダ及び各営業課のフォルダに対して読み取り権限を持つ のため、「営業情報読み取り」IT ロールのメンバを決定する営業部長の許可の元、「営業サポート課」ビジネスロールを「営業情報読み取り」IT ロールのメンバとする設計に変更	業務で利用する各アプリケーションのオーナ（左記では見積もりシステム及びフォルダのオーナ） 及び 「営業情報読み取り」IT ロールの要否及びメンバを決定する営業部長（営業に関する情報読み取り用の IT ロールであるため）

	上記 IT ロールだけでは、営業 1 課フォルダ及び営業 2 課フォルダへの書き込み権限が不足するため、各フォルダオーナの許可の元、「営業サポート課」ビジネスロールを以下のロール ・　営業 1 課フォルダ読み書きアプリケーションロール ・　営業 2 課フォルダ読み書きアプリケーションロール のメンバとする設計に変更	アプリケーションのオーナ（左記ではフォルダのオーナ）
5	4 の設計に基づき、IT ロールの操作を行う担当者が、「営業サポート課」ビジネスロールを「営業情報読み取り」IT ロールのメンバに追加	IT ロールの操作を行う担当者
	4 の設計に基づき、アプリケーションロールの操作を行う担当者が、「営業サポート課」ビジネスロールを「営業 1 課フォルダ読み書き」アプリケーションロール及び「営業 2 課フォルダ読み書き」アプリケーションロールのメンバに追加	アプリケーションロールの操作を行う担当者

組織改編前後のビジネスロール、IT ロール、アプリケーションロールの関係を図示すると、下図の通りとなる。

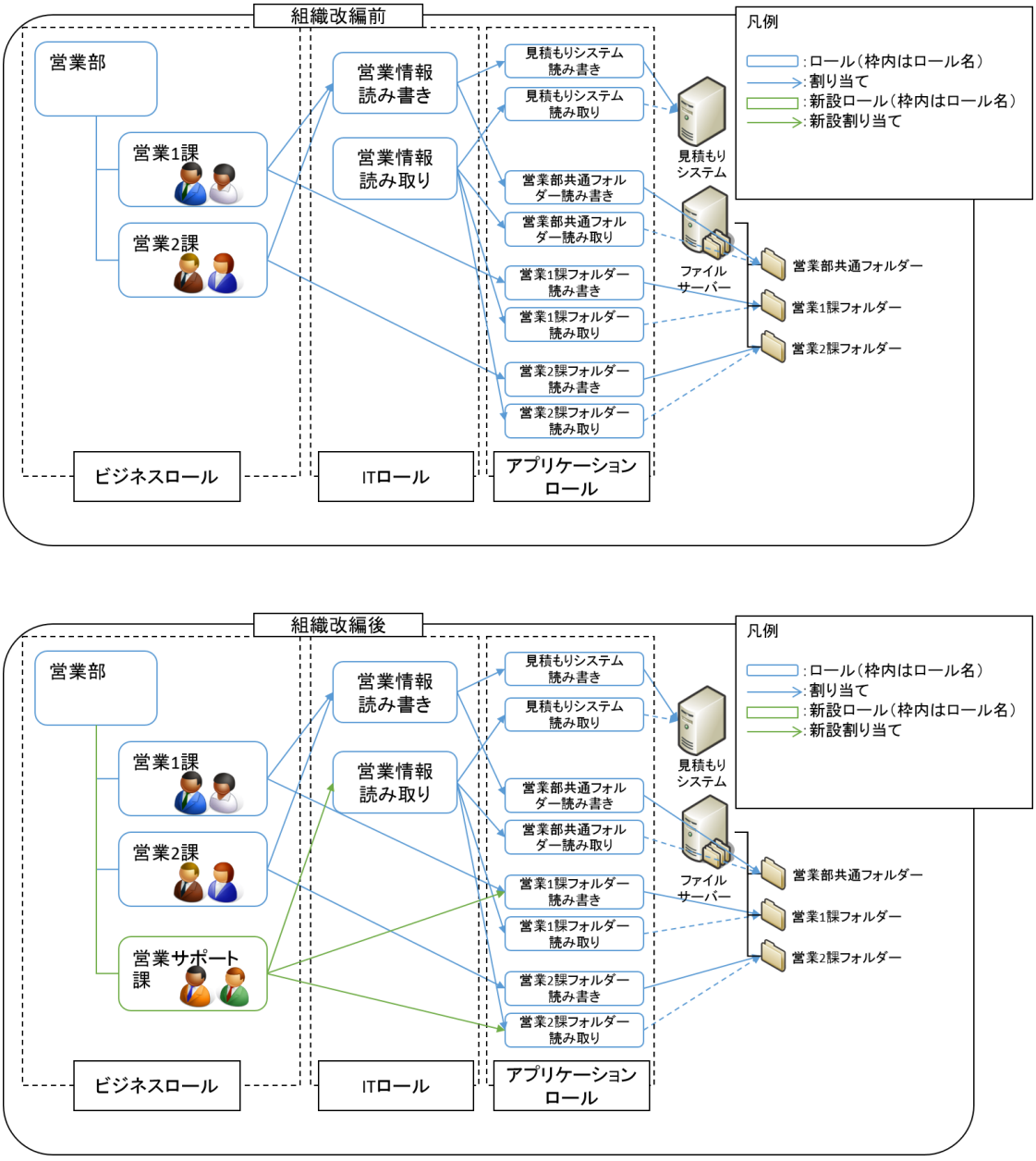


図 4.3　組織改編前後のビジネスロール、IT ロール、アプリケーションロールの関係

4.2.3. ロール管理運用におけるアクタとその役割

ロール管理運用は前項に記述した運用フローに沿って行われる。本項ではそのフローにおけるアクタとその役割について記述する。

組織が新設される場合を例にとって、ロール管理運用フローの各タスクを 4.2.2 に示したが、各タスクの決定者あるいは操作者をアクタと定義し、その役割を一般化すると下表の通りである。

表 4.5　アクタとその役割

アクタ	役割	表 4.4 前述の背景の例におけるロール管理運用での具体的な決定者・操作者
ビジネスオーナ	ビジネスプロセスや職務分掌についての決定権限を持つ。用意すべきビジネスロールを決定する。また、各ロールが行う業務の範囲とそのメンバ条件を決定し、ビジネスロールの設計を承認する。	営業部長
ビジネスロールオーナ	ビジネスロールに所属するメンバの決定権限を持つ。IT ロールオーナを兼務することもある。	営業サポート課課長
ビジネスロールメンバ	ビジネスロールに所属するメンバ。実際の従業員に相当し、そのビジネスロールに割り当てられた権限の範囲内で業務を遂行する。	営業サポート課課員
ビジネスロールオペレータ	ビジネスオーナが決定するビジネスロールを用意する。また、ビジネスロールオーナが決定するビジネスロールのメンバの追加/削除を行う。	ビジネスロールの操作を行う担当者
アプリケーションオーナ	アプリケーションなどのリソースについての決定権限を持つ。リソースに用意すべきアプリケーションロールを決定する。また、ビジネスロールあるいは IT ロールに割り当てるリソースへのアクセス権限を決定し、アプリケーションロールの設計を承認する。	業務で利用する各アプリケーションのオーナ（例では見積もりシステム及びフォルダのオーナ）
アプリケーションロールメンバ	アプリケーションロールの所属するメンバ。ビジネスロールあるいは IT ロールを割り当てる。	「営業サポート課」ビジネスロール（「営業 1 課フォルダ読み書き」アプリケーションロール及び「営業 2 課フォルダ読み書き」アプリケーションロールのメンバとして）
アプリケーションロールオペレータ	リソースオーナの決定に基づき、アプリケーションロールを用意する。また、指定されたビジネスロールあるいは IT ロールを指定されたアプリケーションロールへ割り当てる。	アプリケーションロールの操作を行う担当者
IT オーナ	ビジネスロールとアプリケーションロールを仲立ちする IT ロールの要否及び必要な場合に用意すべき IT ロールを決定し、IT ロールの設計を承認する。ビジネスオーナが兼務することもある。	「営業情報読み取り」IT ロールの要否及びメンバを決定する営業部長（営業に関する情報読み取り用の IT ロールであるため）
IT ロールオーナ	IT ロールに割り当てるビジネスロールの決定権限を持つ。ビジネスロールオーナを兼務することもある。	「営業情報読み取り」IT ロールの要否及びメンバを決定する営業部長（営業に関する情報読み取り用の IT ロールであるため）

IT ロールメンバ	IT ロールに所属するメンバ。ビジネスロールを割り当てる。	「営業サポート課」ビジネスロール（「営業情報読み取り」IT ロールのメンバとして）
IT ロールオペレータ	IT オーナの決定に基づき、IT ロールを用意する。また、指定されたビジネスロールを指定された IT ロールへ割り当てる。	IT ロールの操作を行う担当者

ロール管理運用では、「4.2 ロール管理運用の観点」で示したライフサイクルの各操作及び棚卸しの運用フローにおいて、これらのアクタを考慮する必要がある。

4.3. トリガイベント分類ごとのロール管理運用ガイドライン

本節では、まず、トリガイベントの発生場所とそれが影響を及ぼすロールタイプにより、ロール管理運用を以下 4 つのパターンに分ける。

- トリガイベントがビジネス側で生じるケース
  - (1) トリガイベントが最初に組織型ロールに影響するケース
  - (2) トリガイベントが最初にプロジェクト型ロールに影響するケース
  - (3) トリガイベントが最初にライン型ロールに影響するケース
- トリガイベントがアプリケーション側で生じるケース
  - (4) トリガイベントが最初にアプリケーションロールに影響するケース

その上で、上記 4 つのパターンに対して、前節に記述したロール管理運用の観点を適用した結果を、以下の流れに沿って記述し、ロール管理運用ガイドラインとして示す。

- ロール設計の基になる情報及びその情報に変更が生じるトリガイベント
- トリガイベントごとのロール管理運用概要
- トリガイベントごとのロール管理運用詳細（フロー、タスク及びアクタ）

4.3.1. トリガイベントが最初に組織型ロールに影響を及ぼすケース

本項では、組織型ロール管理運用のガイドラインを以下の項目ごとに示す。

- ロール定義の基になる情報及びその情報に変更が生じるトリガイベント
- トリガイベントごとのロール管理運用概要
- トリガイベントごとのロール管理運用詳細（フロー、タスク及びアクタ）
  (1) 組織改編発令
  (2) 人事異動発令
  (3) 人事情報に含まれない人員の入社・異動・退社

4.3.1.1. ロール定義の基になる情報及びその情報に変更が生じるトリガイベント

組織型ロールのロール定義の基になる情報、その情報に変更が生じるトリガイベント、ならびに変更時の承認プロセスを下表に示す。

表 4.6 組織型ロールの基になる情報、変更が生じるイベント、ならびに変更時の承認プロセス

基になる情報	左記情報に関して生じるイベント	左記情報変更時の承認プロセス
組織情報（役職、雇用形態、拠点自体の情報も含む)	組織改編	組織情報の承認プロセスに従う
人事情報（人員及び各人員の組織や役職、雇用形態などへの所属情報)	人事異動	人事情報の承認プロセスに従う
人事情報に含まれない人員の所属情報	人事情報に含まれない人員の入社・異動・退職	以下の申請・承認フローで運用する。 ・申請者：左記人員本人もしくは代理 ・承認者：所属する組織の管理者

4.3.1.2. トリガイベントごとのロール管理運用概要

組織型ロールについてロール管理運用の最初のトリガイベント及びそれにより生じる操作・棚卸しを下表に示す。

表 4.7　組織型ロールのライフサイクルのトリガイベント及びそれにより生じる操作・棚卸し

<table>
<tr><th>トリガイベント</th><th>左記イベントにより生じる組織型ロール管理運用</th><th>左記ロール管理運用に伴って生じるアプリケーションロール及びITロール管理運用</th><th>補足</th></tr>
<tr><td rowspan="6">組織改編発令</td><td>ロールの作成</td><td rowspan="6">・ ロールの作成
・ ロールの定義の変更
・ ロールに割り当てる権限の変更
・ ロールに割り当てられたビジネスロールの変更
・ ロールの削除
・ ロール要否の棚卸し
・ ロールに割り当てられた権限の棚卸し
・ ロールに割り当てられた組織型ロールの棚卸し
・ ロールオーナの棚卸し</td><td rowspan="6">組織型ロールに相当する組織や役職などが新設や廃止、既存組織などの業務内容や責任範囲の変更が行われる。これにより、組織型ロールの要否及び定義と必要な権限が変化する。
これに伴って、組織型ロールを割り当てるアプリケーションロールやITロールについても、作成、定義や権限の変更、割り当てる組織型ロールの変更、削除が行われる。（不要なこともある）</td></tr>
<tr><td>ロールの定義の変更</td></tr>
<tr><td>ロールに割り当てる権限の変更</td></tr>
<tr><td>ロールに割り当てる権限の棚卸し</td></tr>
<tr><td>ロールの削除</td></tr>
<tr><td>ロールの要否の棚卸し</td></tr>
<tr><td rowspan="4">人事異動発令</td><td>ロールメンバの変更</td><td rowspan="3">－</td><td rowspan="5">組織型ロールのメンバやロールオーナが変更時には、アプリケーションロールや IT ロールの変更は不要。</td></tr>
<tr><td>ロールメンバの棚卸し（後述の人事情報に含まれていない人員も棚卸し対象に含む）</td></tr>
<tr><td>ロールオーナの変更</td></tr>
<tr><td>ロールオーナの棚卸し</td><td rowspan="2">－</td></tr>
<tr><td>人事情報に含まれない人員の入社・異動・退社</td><td>ロールメンバの変更</td></tr>
</table>

4.3.1.3. トリガイベントごとのロール管理運用詳細（フロー、タスク及びアクタ）

組織型ロール管理運用フローにおけるタスクとそのアクタを下表に示す。なお、組織型ロール管理運用フローはそのトリガによって大きく 3 つに分かれるため、それぞれについて表を分けて記述する。

表 4.8　組織改編発令に伴う組織型ロール管理運用フローにおけるタスクとそのアクタ

No.	フロー概要	タスク	アクタ
1	ロールの操作や棚卸しを行うトリガイベントが発生する	・ 組織改編の発令をトリガとする場合は、本項内「4.3.1.1 ロール定義の基になる情報及びその情報に変更が生じるトリガイベント」に記述の通りの承認プロセスを行う	本項内「4.3.1.1 ロール定義の基になる情報及びその情報に変更が生じるトリガイベント」の承認プロセスを参照
2	トリガイベントにおいて、事前に定められたビジネスロール設計の変更要否を判断し、必要があればビジネスロールの設計を変更する	・ 以下を確認する ➢ 自分が管轄する組織や役職、雇用形態、拠点の新設や廃止有無 ➢ 設計済みの各組織型ロールの業務内容変更有無 ・ 棚卸しを兼ねているので、組織情報上変更が加わっていない組織に基づく組織型ロールについても確認する ・ 新設や廃止の場合や業務内容が変わる場合にはロール設計（組織型ロール）変更を行う*1	組織を管轄する立場の人員（ビジネスオーナとして。例　営業部配下の営業課を管轄する営業部部長）
		・ 組織型ロールが作成される場合、具体的なメンバを確認し、ロール設計（組織型ロール）に反映する	組織のメンバを管理する立場の人員（ビジネスロールオーナとして。例　営業1課の課員を管理する営業 1 課課長）
3	トリガイベントについてビジネスロール設計に基づいて、ビジネスロールに対する操作や棚卸しを実施する	・ 人事異動や組織改編発令日に、人事情報及びロール設計（組織型ロール）に基づいて、組織型ロールの作成、ビジネスロールメンバの変更、ビジネスロールオーナの変更、削除を実施する	ビジネスロールオペレータ

4	上記ビジネスロールに対する操作や棚卸しの結果、IT ロールあるいはアプリケーションロール設計の変更要否を判断し、必要があれば各ロール設計を変更する	・ 上記ビジネスロール設計の変更に伴い組織型ロールに割り当てるべき権限を変更するか確認する ➢ 変更する場合にはロール設計（アプリケーションロール）変更を行う ・ 棚卸しを兼ねているので、各アプリケーションロールについて、以下を確認する ➢ 不要なアプリケーションロールの有無 ➢ アプリケーションロールの権限 ➢ 適切な組織型ロールの割り当て ➢ アプリケーションロールのオーナ	アプリケーションオーナ
		・ 上記ビジネスロール設計の変更に伴い組織型ロールに割り当てるべき権限を変更するか確認する ➢ 変更する場合にはロール設計（IT ロール）変更を行う ・ 棚卸しを兼ねているので、各 IT ロールについて、以下を確認する ➢ 不要な IT ロールの有無 ➢ IT ロールの権限 ➢ 適切な組織型ロールの割り当て ➢ IT ロールのオーナ	IT オーナ
5	IT ロールあるいはアプリケーションロールの設計に基づいて、IT ロールやアプリケーションロールに対して必要となる操作や棚卸しを決定し実施する	・ 人事異動や組織改編発令日にロール設計（アプリケーションロール）に基づいて、指定された組織型ロールあるいは IT ロールを適切なアプリケーションロールに割り当て実施する	アプリケーションロールオペレータ
		・ 人事異動や組織改編発令日にロール設計（IT ロール）に基づいて、指定された組織型ロールを適切なアプリケーションロールに割り当て実施する	IT ロールオペレータ

*1：ロール設計（組織型ロール）変更時には業務内容及び割り当てる権限の調査・調整が必要になることが多い。そのため、人事情報や組織改編発令日前に情報を入手し、設計を改める必要がある。運用設計を行う際にはこのリードタイムも考慮に入れる必要がある

*2：ビジネスロール設計の変更と同様に、ロール設計（IT ロール）及びロール設計（アプリケーションロール）変更時には、ビジネスロールが必要とする権限及び既存ロールの調査・調整が必要になることが多い。そのため、人事情報や組織改編発令日前に情報を入手し、設計を改める必要がある。運用設計を行う際にはこのリードタイムも考慮に入れる必要がある

上表のロール管理運用フローを例示すると下図のとおり。

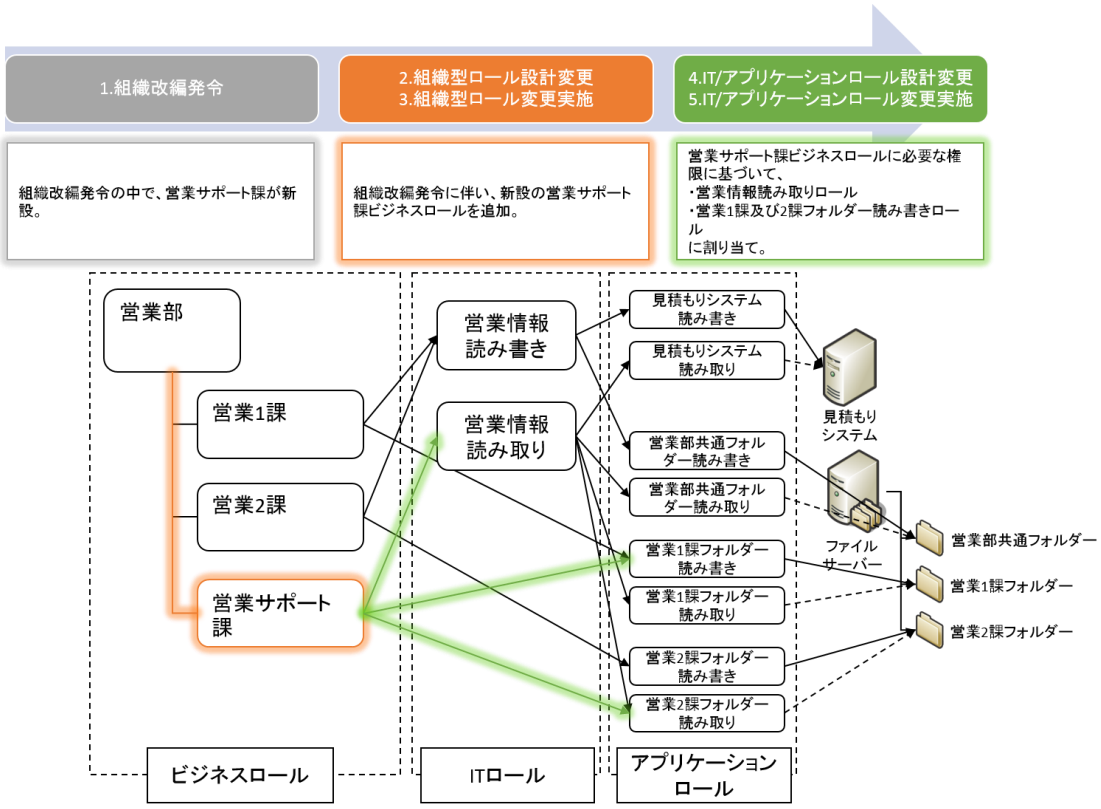


図 4.4　組織改編発令に伴う組織型ロール管理運用フローの例

表 4.9　人事異動発令に伴う組織型ロール管理運用フローにおけるタスクとそのアクタ

No.	フロー概要	タスク	アクタ
1	ロールの操作や棚卸しを行うトリガイベントが発生する	・ 組織改編の発令をトリガとする場合は、本項内「4.3.1.1 ロール定義の基になる情報及びその情報に変更が生じるトリガイベント」に記述の通りの承認プロセスを行う。	本項内「4.3.1.1 ロール定義の基になる情報及びその情報に変更が生じるトリガイベント」の承認プロセスを参照
2	トリガイベントにおいて、事前に定められたビジネスロール設計の変更要否を判断し、必要があればビジネスロールの設計を変更する	・ 以下を確認する ➢ 自分が管轄する組織の管理者が変更有無 ・ 棚卸しを兼ねているので、組織情報上変更が加わっていない組織についても確認する ・ 組織の管理者変更の場合には、ロール設計（組織型ロール）上のロールオーナ変更を行う	組織を管轄する立場の人員（ビジネスオーナとして。例　営業部配下の営業課を管轄する営業部部長）
		・ 以下を確認する ➢ 自分がロールオーナを務める組織型ロールのロールメンバに追加や削除の要否 ・ 棚卸しを兼ねているので、棚卸しを兼ねているので、人事情報上変更が加わっていない場合も、適切な組織型ロールに所属しているか確認する ・ 人事情報に含まれない人員のロールメンバについても棚卸しを実施する ➢ 追加や削除する場合は、ロール設計（組織型ロール）変更を行う	組織のメンバを管理する立場の人員（ビジネスロールオーナとして。例　営業1課の課員を管理する営業 1 課課長）
3	トリガイベントについてビジネスロール設計に基づいて、ビジネスロールに対する操作や棚卸しを実施する	・ 人事異動発令日に、人事情報及びロール設計（組織型ロール）に基づいて、ビジネスロールオペレータが組織型ロールメンバの変更、ロールオーナの変更を実施する。 ➢ 人事情報に含まれない人員も不要な場合はここで削除する。	ビジネスロールオペレータ
4	―	―	―
5	―	―	―

上表のロール管理運用フローを例示すると下図のとおり。

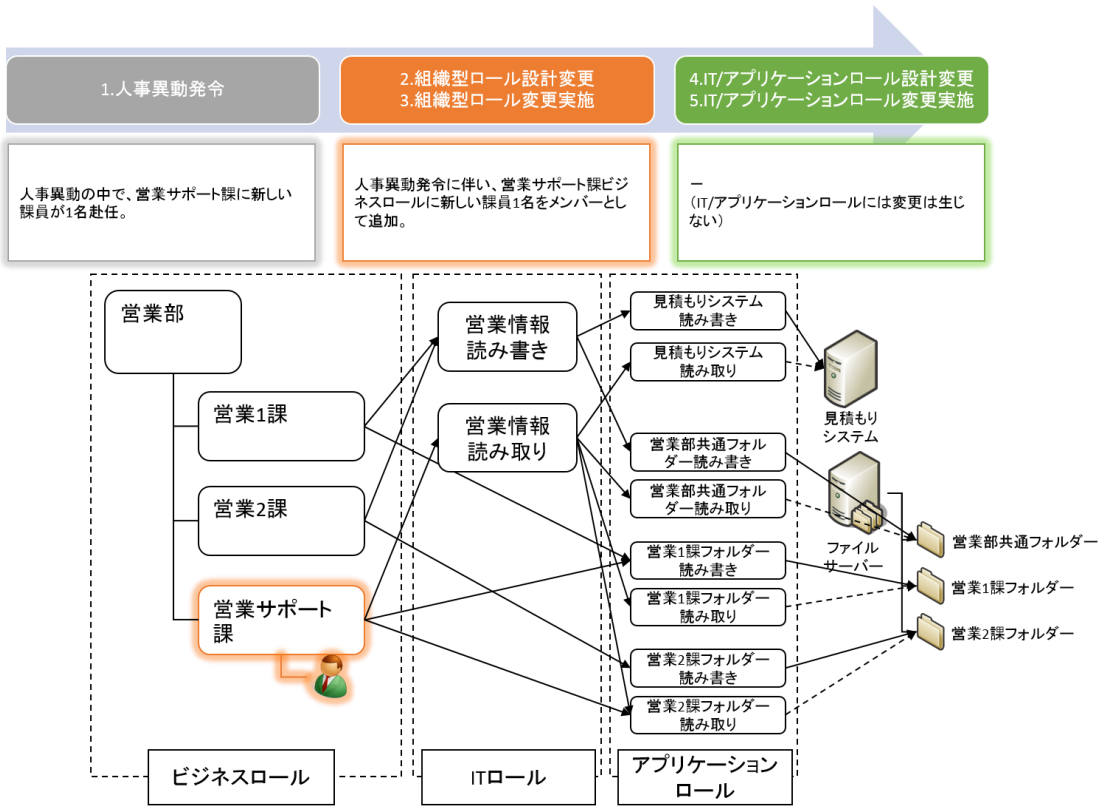


図 4.5　人事異動発令に伴う組織型ロール管理運用フローの例

表 4.10　人事情報に含まれない人員の入社・異動・退社に伴う組織型ロール管理運用フローにおけるタスクとそのアクタ

No.	フロー概要	タスク	アクタ
1	ロールの操作や棚卸しを行うトリガイベントが発生する	・ 人事情報に含まれない人員の入社・異動・退社をトリガとする場合は、本項内「4.3.1.1 ロール定義の基になる情報及びその情報に変更が生じるトリガイベント」に記述の通りの承認プロセスを行う。	本項内「4.3.1.1 ロール定義の基になる情報及びその情報に変更が生じるトリガイベント」の承認プロセスを参照
2	トリガイベントにおいて、事前に定められたビジネスロール設計の変更要否を判断し、必要があればビジネスロールの設計を変更する	・ 以下を確認する ➢ 自分がロールオーナを務める組織型ロールのロールメンバに追加や削除の要否	組織のメンバを管理する立場の人員（ビジネスロールオーナとして。例　営業1課の課員を管理する営業 1 課課長）
3	トリガイベントについてビジネスロール設計に基づいて、ビジネスロールに対する操作や棚卸しを実施する	・ 人事情報に含まれない人員の入社・異動・退社に伴うビジネスロールメンバの変更をビジネスロールオーナが承認した後に、ビジネスロールオペレータがそうした人員をメンバに追加あるいは削除する。	ビジネスロールオペレータ
4	―	―	―
5	―	―	―

上表のロール管理運用フローを例示すると下図のとおり。

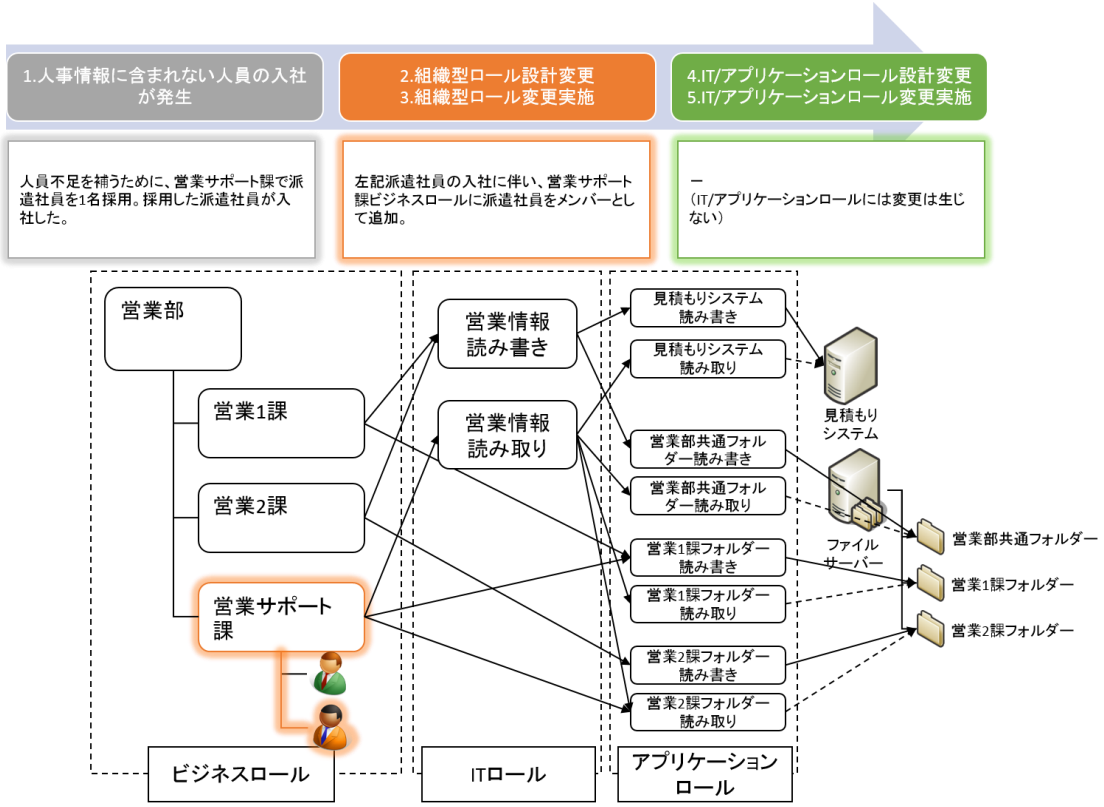


図 4.6　人事情報に含まれない人員の入社・異動・退社に伴う組織型ロール管理運用フローの例

4.3.2. トリガイベントが最初にプロジェクト型ロールに影響を及ぼすケース

本項では、プロジェクト型ロール管理運用におけるガイドラインを以下の項目ごとに示す。

- ロール定義の基になる情報及びその承認プロセス
- トリガイベントごとのロール管理運用概要
- トリガイベントごとのロール管理運用詳細（フロー、タスク及びアクタ）

4.3.2.1. ロール定義の基になる情報及びその情報に変更が生じるイベント

プロジェクト型ロールのロール定義の基になる情報及びその情報に変更が生じるイベント、変更時の承認プロセスを下表に示す。

表 4.11 プロジェクト型ロール定義の基になる情報及び変更が生じるイベントと変更時の承認プロセス

ロール定義の基になる情報	左記情報に変更が生じるイベント	左記情報変更時の承認プロセス
プロジェクトに関する以下情報 ・ プロジェクトの要否 ・ プロジェクトの役割 ・ プロジェクトの管理者*	プロジェクト自体の変更 ・ プロジェクトの開始 ・ プロジェクトのステータスの変更（例　準備フェーズから実行フェーズへの変更など） ・ プロジェクト管理者の変更 ・ プロジェクトの終了	以下の申請・承認フローで運用する。 ・申請者：当該プロジェクト関係者 ・承認者：当該プロジェクトの管理者（＝ビジネスロールオーナ）及び当該プロジェクトを管轄するビジネスオーナ
	プロジェクト自体の棚卸し	ー
プロジェクトに関する以下情報 ・ プロジェクトメンバ	プロジェクトメンバ変更	以下の申請・承認フローで運用する。 ・申請者：当該プロジェクト関係者 ・承認者：当該プロジェクトの管理者（＝ビジネスロールオーナ）
	プロジェクトメンバの棚卸し	ー

*：プロジェクトの管理者とは、プロジェクトメンバの決定権を持つ者を指す。

4.3.2.2. トリガイベントごとのロール管理運用概要（フロー）

前項に述べたトリガイベントごとのプロジェクト型ロール管理運用フローの概要を下表に示す。

表 4.12　トリガイベントとプロジェクト型ロール管理運用フロー概要

トリガイベント	左記イベントにより生じるプロジェクト型ロール管理運用	左記ロール管理運用に伴って生じるアプリケーションロール及び IT ロール管理運用	補足
プロジェクト自体の変更	ロールの作成	・ ロールの作成 ・ ロールの定義の変更 ・ ロールに割り当てる権限の変更 ・ ロールに割り当てられたビジネスロールの変更 ・ ロールの削除	プロジェクトの開始、終了及びその間のステータスの変更により、プロジェクト型ロールの要否及び定義と必要な権限が変化する。 これに伴って、プロジェクト型ロールを割り当てるアプリケーションロールや IT ロールについても、作成、定義や権限の変更、割り当てるプロジェクト型ロールの変更、削除が行われる。（不要なこともある）
	ロールの定義の変更		
	ロールに割り当てる権限の変更		
	ロールオーナの変更		
	ロールの削除		

プロジェクトメンバの変更	ロールメンバの変更	―	プロジェクト型ロールのメンバ変更時には、アプリケーションロールや IT ロールの変更は不要。
定期的なプロジェクト自体の棚卸し時 （棚卸しの結果、変更が生じた場合は、上記「プロジェクト自体の変更」に準ずる）	プロジェクト型ロールの要否の棚卸し	・ ロールの要否棚卸し ・ ロールに割り当てる権限の棚卸し ・ ロールに割り当てられたプロジェクト型ロールの棚卸し ・ ロールオーナの棚卸し	プロジェクトの要否、役割、割り当てる権限、及び管理者についての変更（特に不要な場合の削除）は、適切なタイミングで申請されない（あるいは全く申請されない）ことが多いため、定期的な棚卸しを実施する
	プロジェクト型ロールの定義の棚卸し		
	プロジェクト型ロールに割り当てられた権限の棚卸し		
	プロジェクト型ロールオーナの棚卸し		
定期的なプロジェクトメンバの棚卸し時 （棚卸しの結果、変更が生じた場合は、上記「プロジェクトメンバの変更」に準ずる	プロジェクト型ロールメンバの棚卸し	―	プロジェクトメンバの変更（特に削除）は、適切なタイミングで申請されない（あるいは全く申請されない）ことが多いため、定期的な棚卸しを実施する

4.3.2.3. トリガイベントごとのロール管理運用詳細（フロー、タスク及びアクタ）

プロジェクト型ロール管理運用フローにおけるタスクとそのアクタを下表に示す。なお、プロジェクト型ロール管理運用フローはそのトリガによって大きく 4 つに分かれるため、それぞれについて分けて記述する。

表 4.13　プロジェクト自体の変更が承認された時のルール管理運用フローにおけるタスクとそのアクタ

No.	フロー概要	タスク	アクタ
1	ロールの操作や棚卸しを行うトリガイベントが発生する	・ プロジェクトの開始、ステータスの変更、管理者の変更、終了をトリガとする場合は、本項内「4.3.2.1 ロール定義の基になる情報及びその情報に変更が生じるイベント」に記述の通りの承認プロセスを行う	本項内「4.3.2.1 ロール定義の基になる情報及びその情報に変更が生じるイベント」の承認プロセスを参照
2	トリガイベントにおいて、事前に定められたビジネスロール設計の変更要否を判断し、必要があればビジネスロールの設計を変更する	・ 以下を確認する ➢ 設計済みのプロジェクト型ロールへの変更有無 ・ プロジェクトの開始、終了の場合やプロジェクトの役割が変わる場合にはロール設計（プロジェクト型ロール）変更を行う	プロジェクトを管轄する立場の人員（ビジネスオーナとして。例 営業部配下のプロジェクトを管轄する営業部部長）
		・ プロジェクト型ロールが作成される場合、具体的なメンバを確認し、ロール設計（プロジェクト型ロール）に反映する	プロジェクトの管理者（ビジネスロールオーナとして。例 プロジェクトマネージャー）
3	トリガイベントについてビジネスロール設計に基づいて、ビジネスロールに対する操作や棚卸しを実施する	・ プロジェクト自体の変更が承認された日に、上記で変更されたロール設計（プロジェクト型ロール）に基づいて、プロジェクト型ロールの作成、メンバの変更、ビジネスロールオーナの変更、削除を実施する	ビジネスロールオペレータ

4	上記ビジネスロールに対する操作や棚卸しの結果、IT ロールあるいはアプリケーションロール設計の変更要否を判断し、必要があれば各ロール設計を変更する	・ 上記ビジネスロール設計の変更に伴いプロジェクト型ロールに割り当てるべき権限を変更するか確認する ➢ 変更する場合にはロール設計（アプリケーションロール）変更を行う ・ 棚卸しを兼ねているので、各アプリケーションロールについて、以下を確認する ➢ 不要なアプリケーションロールの有無 ➢ アプリケーションロールの権限 ➢ 適切なプロジェクト型ロールの割り当て ➢ アプリケーションロールのオーナ	アプリケーションオーナ
		・ 上記ビジネスロール設計の変更に伴いプロジェクト型ロールに割り当てるべき権限を変更するか確認する ➢ 変更する場合にはロール設計（IT ロール）変更を行う ・ 棚卸しを兼ねているので、各 IT ロールについて、以下を確認する ➢ 不要な IT ロールの有無 ➢ IT ロールの権限 ➢ 適切なプロジェクト型ロールの割り当て ➢ IT ロールのオーナ	IT オーナ

5	IT ロールあるいはアプリケーションロールの設計に基づいて、IT ロールやアプリケーションロールに対して必要となる操作や棚卸しを決定し実施する	・ プロジェクト自体の変更が承認された日にロール設計（アプリケーションロール）に基づいて、指定されたプロジェクト型ロールあるいはITロールを適切なアプリケーションロールに割り当て実施する	アプリケーションロールオペレータ
		・ プロジェクト自体の変更が承認された日にロール設計（IT ロール）に基づいて、指定されたプロジェクト型ロールを適切なアプリケーションロールに割り当て実施する	IT ロールオペレータ

上表のロール管理運用フローを例示すると下図のとおり。

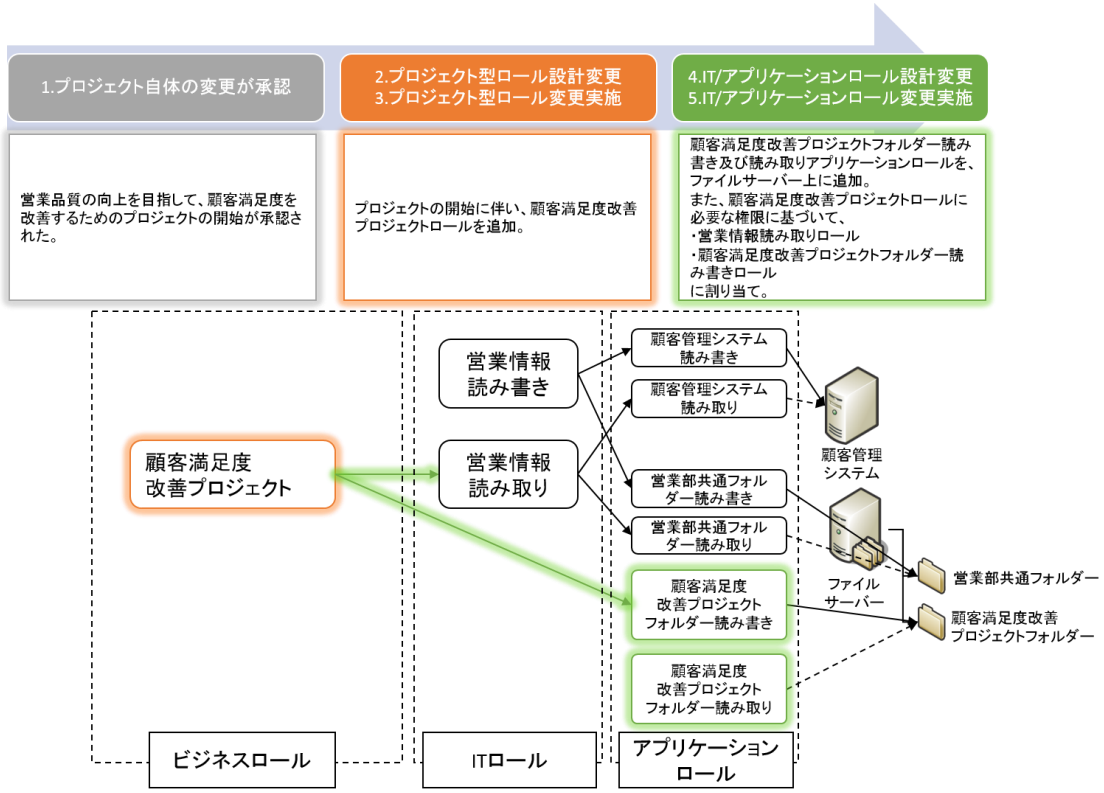


図 4.7　プロジェクト自体の変更が承認された時のロール管理運用フローの例

表 4.14　プロジェクトメンバの変更が承認された時のロール管理運用フローにおけるタスクとそのアクタ

No.	フロー概要	タスク	アクタ
1	ロールの操作や棚卸しを行うトリガイベントが発生する	・ プロジェクトメンバの変更をトリガとする場合は、本項内「4.3.2.1 ロール定義の基になる情報及びその情報に変更が生じるイベント」に記述の通りの承認プロセスを行う。	本項内「4.3.2.1 ロール定義の基になる情報及びその情報に変更が生じるイベント」を参照
2	トリガイベントにおいて、事前に定められたビジネスロール設計の変更要否を判断し、必要があればビジネスロールの設計を変更する	・ 追加あるいは削除対象のメンバを確認し、ロール設計（プロジェクト型ロール）に反映する	プロジェクトの管理者（ビジネスロールオーナとして。）
3	トリガイベントについてビジネスロール設計に基づいて、ビジネスロールに対する操作や棚卸しを実施する	・ プロジェクトメンバの変更が承認された日に、上記で変更されたロール設計（プロジェクト型ロール）に基づいて、プロジェクト型ロールのメンバの変更を実施する。	ビジネスロールオペレータ
4	―	―	―
5	―	―	―

上表のロール管理運用フローを例示すると下図のとおり。

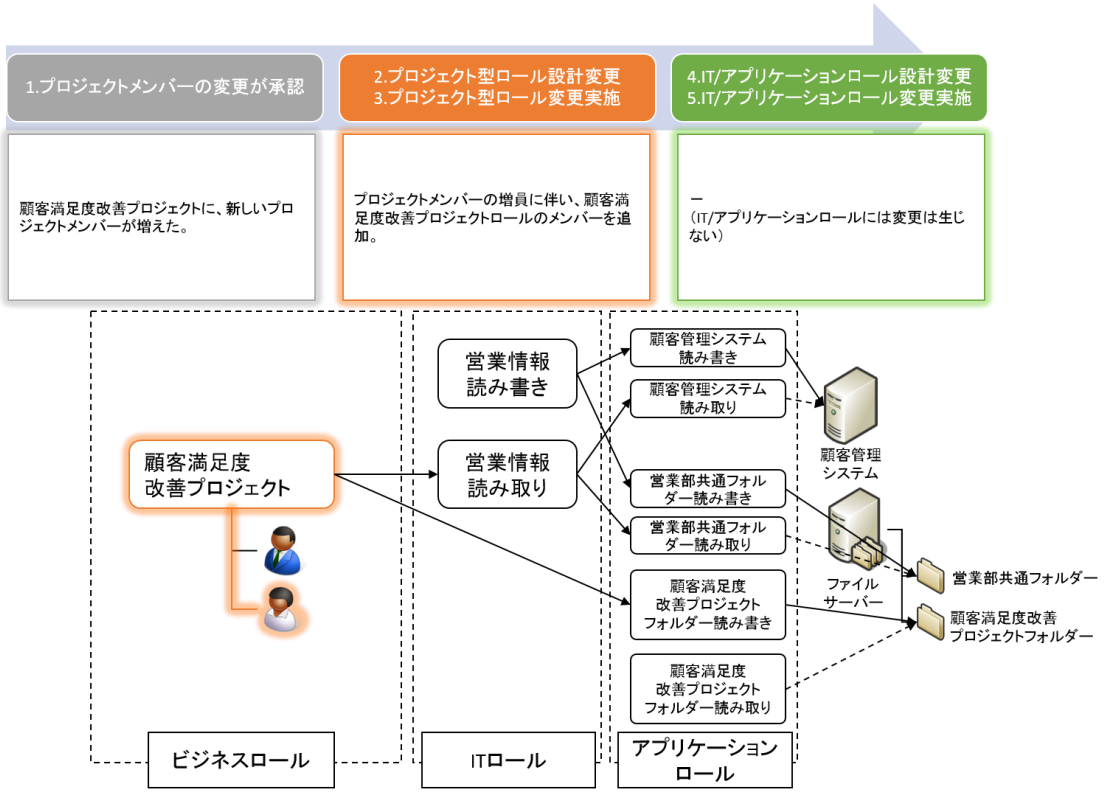


図 4.8　プロジェクトメンバの変更が承認された時のロール管理運用フローの例

表 4.15　定期的なプロジェクト自体の棚卸し時の運用フローにおけるタスクとそのアクタ

No.	フロー概要	タスク	アクタ
1	ロールの操作や棚卸しを行うトリガイベントが発生する	－ （定期的に行われるため、トリガイベント発生時のタスクはない）	－
2	トリガイベントにおいて、事前に定められたビジネスロール設計の変更要否を判断し、必要があればビジネスロールの設計を変更する	・ プロジェクトを管轄する立場の人員が、ロール設計（プロジェクト型ロール）に定義してあるプロジェクト型ロールについて以下を確認する ➢ ロールの要否 ➢ ロールに割り当てられた権限 ➢ ロールのオーナ	プロジェクトを管轄する立場の人員（ビジネスオーナとして。）
3	－	・ －	－
4	上記ビジネスロールに対する操作や棚卸しの結果、IT ロールあるいはアプリケーションロール設計の変更要否を判断し、必要があれば各ロール設計を変更する	・ 棚卸しを兼ねているので、各アプリケーションロールについて、以下を確認する ➢ 不要なアプリケーションロールの有無 ➢ アプリケーションロールの権限 ➢ 適切なプロジェクト型ロールの割り当て ➢ アプリケーションロールのオーナ	アプリケーションオーナ
		・ 棚卸しを兼ねているので、各 IT ロールについて、以下を確認する ➢ 不要な IT ロールの有無 ➢ IT ロールの権限 ➢ 適切なプロジェクト型ロールの割り当て ➢ IT ロールのオーナ	IT オーナ
5	－	－	－

*：No.2 及び 4 の棚卸しの結果変更が必要なことがわかった場合は、プロジェクト自体の変更が生じたと見なす。その場合の各タスク、アクタは、「表 4.13　プロジェクト自体の変更が承認された時のルール管理運用フローにおけるタスクとそのアクタ」を参照。

表 4.16　定期的なプロジェクトメンバの棚卸し時の運用フローにおけるタスクとそのアクタ

No.	フロー概要	タスク	アクタ
1	ロールの操作や棚卸しを行うトリガイベントが発生する	― ・　（定期的に行われるため、トリガイベント発生時のタスクはない）	―
2	トリガイベントにおいて、事前に定められたビジネスロール設計の変更要否を判断し、必要があればビジネスロールの設計を変更する	・　以下を確認する ➢　自分がロールオーナを務めるプロジェクト型ロールのロールメンバの追加や削除の要否	プロジェクトの管理者（ビジネスロールオーナとして。）
3	―	―	―
4	―	―	―
5	―	―	―

*：No.2の棚卸しの結果変更が必要なことがわかった場合は、その内容に応じてプロジェクトメンバの変更が生じたと見なす。その場合の各タスク、アクタは、

表 **4.14　プロジェクトメンバの変更が承認された時のロール管理運用フローにおけるタスクとそのアクタ**」を参照。

4.3.3. トリガイベントが最初にライン型ロールに影響を及ぼすケース

本項では、ライン型ロール管理運用におけるガイドラインを以下の項目ごとに示す。

- ロール定義の基になる情報及びその承認プロセス
- トリガイベントごとのロール管理運用概要
- トリガイベントごとのロール管理運用詳細（フロー、タスク及びアクタ）

4.3.3.1. ロール定義の基になる情報及びその情報に変更が生じるイベント

ライン型ロールのロール定義の基になる情報及びその情報に変更が生じるイベント、変更時の承認プロセスを下表に示す。

表 4.17 ライン型ロール定義の基になる情報及び変更が生じるイベントと変更時の承認プロセス

ロール定義の基になる情報	左記情報に変更が生じるイベント	左記情報変更時の承認プロセス
業務に関する以下情報 ・ 業務の要否 ・ 業務の役割 ・ 業務の管理者*	業務自体の変更 ・ 複数の組織をまたがる新しい業務の開始 ・ 業務の役割の変更 ・ 業務管理者の変更 ・ 業務の終了	以下の申請・承認フローで運用する。 ・申請者：当該業務関係者 ・承認者：当該業務の管理者（＝ビジネスロールオーナ）及び当該業務を管轄するビジネスオーナ
	業務自体の棚卸し	ー
業務に関する以下情報 ・ 業務担当メンバ	業務担当メンバ変更	以下の申請・承認フローで運用する。 ・申請者：当該業務関係者 ・承認者：当該業務の管理者（＝ビジネスロールオーナ)
	業務担当メンバの棚卸し	ー

*：業務の管理者とは、業務担当メンバの決定権を持つ者を指す。

4.3.3.2. トリガイベントごとのロール管理運用概要（フロー）

前項に述べたトリガイベントごとのライン型ロール管理運用フローの概要を下表に示す。

表 4.18　トリガイベントとライン型ロール管理運用フロー概要

トリガイベント	左記イベントにより生じるライン型ロール管理運用	左記ロール管理運用に伴って生じるアプリケーションロール及び IT ロール管理運用	補足
業務自体の変更	ロールの作成 ロールの定義の変更 ロールに割り当てる権限の変更	・ ロールの作成 ・ ロールの定義の変更 ・ ロールに割り当てる権限の変更 ・ ロールに割り当てられたビジネスロールの変更 ・ ロールの削除	業務の開始、終了及びその間の業務の役割の変更により、ライン型ロールの要否及び定義と必要な権限が変化する。 これに伴って、ライン型ロールを割り当てるアプリケーションロールや IT ロールについても、作成、定義や権限の変更、割り当てるライン型ロールの変更、削除が行われる。（不要なこともある）

業務担当メンバの変更	ロールメンバの変更	―	ライン型ロールのメンバ変更時には、アプリケーションロールや IT ロールの変更は不要。
定期的な業務自体の棚卸し時 （棚卸しの結果、変更が生じた場合は、上記「業務自体の変更」に準ずる）	ライン型ロールの要否の棚卸し ライン型ロールの定義の棚卸し ライン型ロールに割り当てられた権限の棚卸し ライン型ロールオーナの棚卸し	・ ロールの要否棚卸し ・ ロールに割り当てる権限の棚卸し ・ ロールに割り当てられたライン型ロールの棚卸し ・ ロールーオーナの棚卸し	業務の要否、役割、割り当てる権限、及び管理者についての変更（特に不要な場合の削除）は、適切なタイミングで申請されない（あるいは全く申請されない）ことが多いため、定期的な棚卸しを実施する。
定期的な業務担当メンバの棚卸し時 （棚卸しの結果、変更が生じた場合は、上記「業務担当メンバの変更」時に準ずる）	ライン型ロールメンバの棚卸し	―	業務担当メンバの変化（特に削除）は、適切なタイミングで申請されない（あるいは全く申請されない）ことが多いため、定期的な棚卸しを実施する

4.3.3.3. トリガイベントごとのロール管理運用詳細（フロー、タスク及びアクタ）

ライン型ロール管理運用フローにおけるタスクとそのアクタを下表に示す。なお、ライン型ロール管理運用フローはそのトリガによって大きく４つに分かれるため、それぞれについて分けて記述する。

表 4.19　業務自体の変更が承認された時のロール管理運用フローにおけるタスクとそのアクタ

No.	フロー概要	タスク	アクタ
1	ロールの操作や棚卸しを行うトリガイベントが発生する	・ 業務の開始、ステータスの変更、管理者の変更、終了をトリガとする場合は、本項内「4.3.3.1 ロール定義の基になる情報及びその情報に変更が生じるイベント」に記述の通りの承認プロセスを行う。	本項内「4.3.3.1 ロール定義の基になる情報及びその情報に変更が生じるイベント」の承認プロセスを参照
2	トリガイベントにおいて、事前に定められたビジネスロール設計の変更要否を判断し、必要があればビジネスロールの設計を変更する	・ 以下を確認する ➢ 設計済みのライン型ロールへの変更有無 ・ 業務の開始、終了の場合や業務の役割が変わる場合にはロール設計（ライン型ロール）変更を行う	業務を管轄する立場の人員（ビジネスオーナとして。例　営業部配下の業務を管轄する営業部部長）
		・ ライン型ロールを作成する場合、そのメンバを確認し、ロール設計（ライン型ロール）に反映する	業務の管理者（ビジネスロールオーナとして。例　見積書発行業務を管理している営業サポート課主任）
3	トリガイベントについてビジネスロール設計に基づいて、ビジネスロールに対する操作や棚卸しを実施する	・ 業務自体の変更が承認された日に、上記で変更されたロール設計（ライン型ロール）に基づいて、ライン型ロールの作成、メンバの変更、ビジネスロールオーナの変更、削除を実施する。	ビジネスロールオペレータ

4	上記ビジネスロールに対する操作や棚卸しの結果、IT ロールあるいはアプリケーションロール設計の変更要否を判断し、必要があれば各ロール設計を変更する	・ 上記ビジネスロール設計の変更に伴いライン型ロールに割り当てるべき権限を変更するか確認する ➢ 変更する場合にはロール設計（アプリケーションロール）変更を行う ・ 棚卸しを兼ねているので、各アプリケーションロールについて、以下を確認する ➢ 不要なアプリケーションロールの有無 ➢ アプリケーションロールの権限 ➢ 適切なライン型ロールの割り当て ➢ アプリケーションロールのオーナ	アプリケーションオーナ
		・ 上記ビジネスロール設計の変更に伴いライン型ロールに割り当てるべき権限を変更するか確認する ➢ 変更する場合にはロール設計（IT ロール）変更を行う ・ 棚卸しを兼ねているので、各 IT ロールについて、以下を確認する ➢ 不要な IT ロールの有無 ➢ IT ロールの権限 ➢ 適切なライン型ロールの割り当て ➢ IT ロールのオーナ	IT オーナ

5	IT ロールあるいはアプリケーションロールの設計に基づいて、IT ロールやアプリケーションロールに対して必要となる操作や棚卸しを決定し実施する	・ プロジェクト自体の変更が承認された日にロール設計（アプリケーションロール）に基づいて、指定されたライン型ロールあるいはIT ロールを適切なアプリケーションロールに割り当て実施する	アプリケーションロールオペレータ
		・ プロジェクト自体の変更が承認された日にロール設計（IT ロール）に基づいて、指定されたライン型ロールを適切なアプリケーションロールに割り当て実施する	IT ロールオペレータ

上表のロール管理運用フローを例示すると下図のとおり。

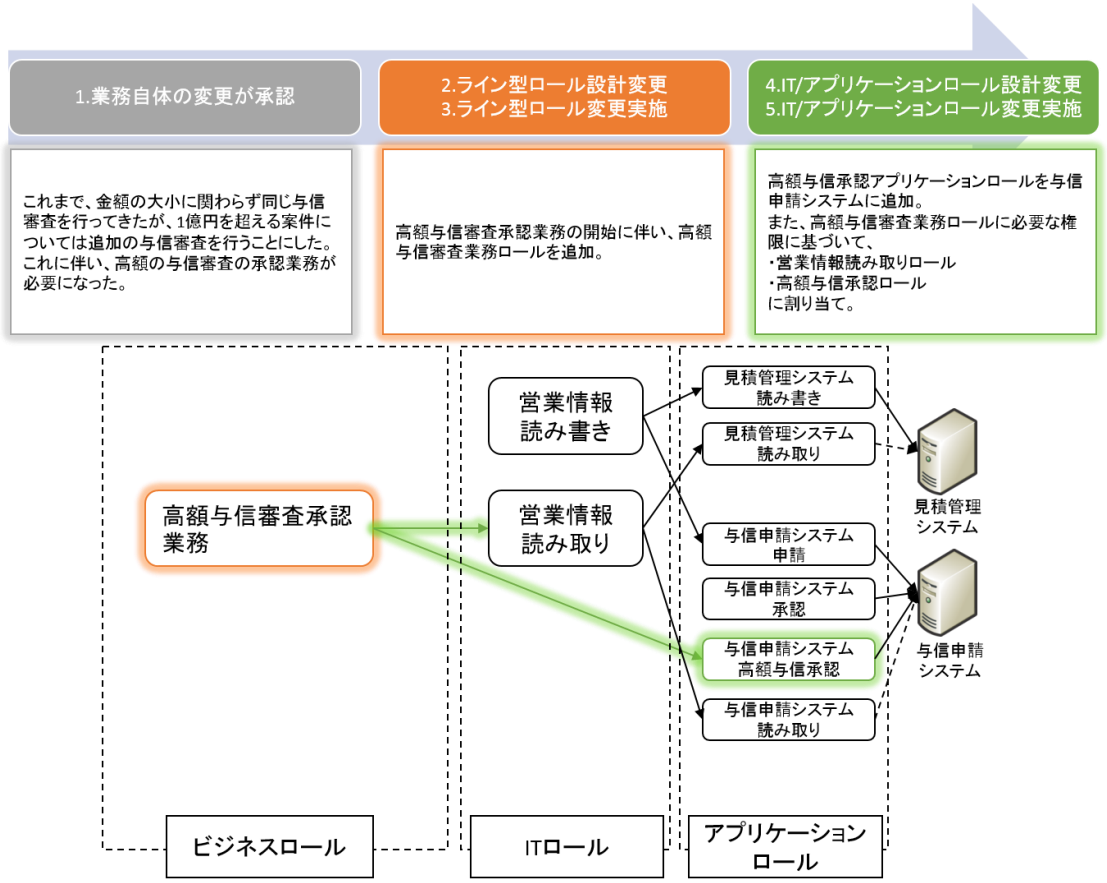


図 4.9　業務自体の変更が承認された時のロール管理運用フローの例

表 4.20　業務担当メンバの変更が承認された時のロール管理運用フローにおけるタスクとそのアクタ

No.	フロー概要	タスク	アクタ
1	ロールの操作や棚卸しを行うトリガイベントが発生する	・ 業務担当メンバの変更をトリガとする場合は、本項内「4.3.3.1 ロール定義の基になる情報及びその情報に変更が生じるイベント」に記述の通りの承認プロセスを行う。	本項内「4.3.3.1 ロール定義の基になる情報及びその情報に変更が生じるイベント」を参照
2	トリガイベントにおいて、事前に定められたビジネスロール設計の変更要否を判断し、必要があればビジネスロールの設計を変更する	➢ ライン型ロールが新設される場合、そのメンバを確認し、ロール設計（ライン型ロール）に反映する	業務の管理者（ビジネスロールオーナとして。）
3	トリガイベントについてビジネスロール設計に基づいて、ビジネスロールに対する操作や棚卸しを実施する	・ 業務担当メンバの変更が承認された日に、上記で変更されたロール設計（ライン型ロール）に基づいて、ビジネスロールオペレータがライン型ロールのメンバの変更を実施する。	ビジネスロールオペレータ
4	－	－	－
5	－	－	－

上表のロール管理運用フローを例示すると下図のとおり。

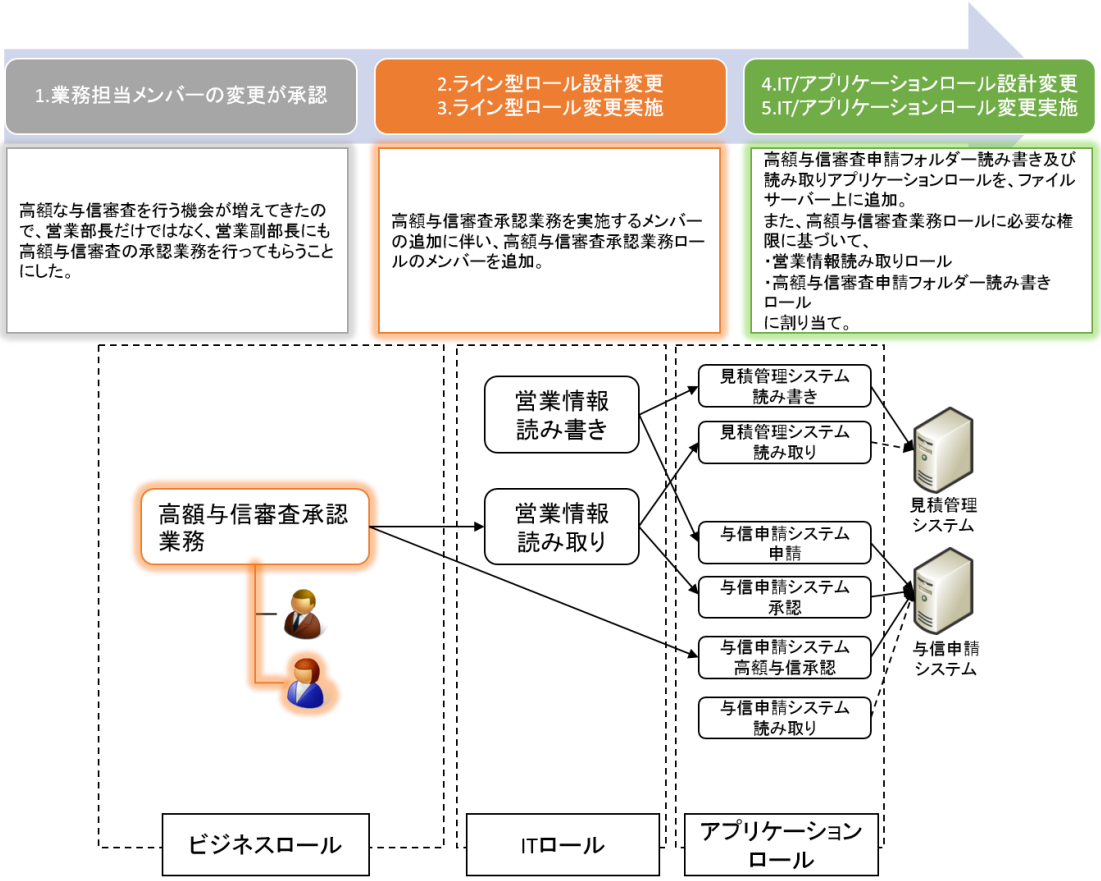


図 4.10　業務担当メンバの変更が承認された時のロール管理運用フローの例

表 4.21　定期的な業務自体の棚卸し時の運用フローにおけるタスクとそのアクタ

No.	フロー概要	タスク	アクタ
1	ロールの操作や棚卸しを行うトリガイベントが発生する	－ （定期的に行われるため、トリガイベント発生時のタスクはない）	－
2	トリガイベントにおいて、事前に定められたビジネスロール設計の変更要否を判断し、必要があればビジネスロールの設計を変更する	・ 業務を管轄する立場の人員が、ロール設計（ライン型ロール）に定義してあるライン型ロールについて以下を確認する ➢ ロールの要否 ➢ ロールに割り当てられた権限 ➢ ロールのオーナ	業務を管轄する立場の人員（ビジネスオーナとして。）
3	－	・ －	－
4	上記ビジネスロールに対する操作や棚卸しの結果、IT ロールあるいはアプリケーションロール設計の変更要否を判断し、必要があれば各ロール設計を変更する	・ 棚卸しを兼ねているので、各アプリケーションロールについて、以下を確認する ➢ 不要なアプリケーションロールの有無 ➢ アプリケーションロールの権限 ➢ 適切なライン型ロールの割り当て ➢ アプリケーションロールのオーナ	アプリケーションオーナ
		・ 棚卸しを兼ねているので、各 IT ロールについて、以下を確認する ➢ 不要な IT ロールの有無 ➢ IT ロールの権限 ➢ 適切なライン型ロールの割り当て ➢ IT ロールのオーナ	IT オーナ
5	－	－	－

*：No. 2 及び 4 の棚卸しの結果変更が必要なことがわかった場合は、その内容に応じて業務自体の変更が生じたと見なす。その場合のフロー概要と各タスク、アクタは「表 4.19　業務自体の変更が承認された時のロール管理運用フローにおけるタスクとそのアクタ」を参照。

表 4.22　定期的な業務担当メンバの棚卸し時の運用フローにおけるタスクとそのアクタ

No.	フロー概要	タスク	アクタ
1	ロールの操作や棚卸しを行うトリガイベントが発生する	― ・　（定期的に行われるため、トリガイベント発生時のタスクはない）	―
2	トリガイベントにおいて、事前に定められたビジネスロール設計の変更要否を判断し、必要があればビジネスロールの設計を変更する	・　以下を確認する ➢　自分がロールオーナを務めるライン型ロールのロールメンバの追加や削除の要否	業務の管理者（ビジネスロールオーナとして。）
3	―	―	―
4	―	―	―
5	―	―	―

*：No.2の棚卸しの結果変更が必要なことがわかった場合は、その内容に応じて業務担当メンバの変更が生じたと見なす。その場合のフロー概要と各タスク、アクタは「表 4.20　業務担当メンバの変更が承認された時のロール管理運用フローにおけるタスクとそのアクタ」を参照。

4.3.4. トリガイベントが最初にアプリケーションロールに影響を及ぼすケース

4.3.4.1. ロール定義の基になる情報及びその情報に変更が生じるイベント

アプリケーションロールのロール定義の基になる情報及びその情報に変更が生じるイベント、変更時の承認プロセスを下表に示す。

表 4.23 アプリケーションロール定義の基になる情報及び変更が生じるイベントと変更時の承認プロセス

ロール定義の基になる情報	左記情報に変更が生じるイベント	左記情報変更時の承認プロセス
アプリケーションに関する以下情報 ・ 業務要件 ・ ユースケース	アプリケーション自体の変更 ・ 新しいアプリケーションの利用開始（システム化されていない業務がシステム化されるケース） ・ 利用中のアプリケーションの置き換え・機能変更 ・ 既存アプリケーションの利用終了（システム化されていた業務が非システム化されるケース）	新しいアプリケーションの利用開始や、既存アプリケーションの置き換え、利用中止の承認プロセスに従う
アプリケーションに関する以下情報 ・ 利用者	アプリケーションの利用者の変更	アプリケーションの利用者は、ビジネスロールあるいは複数のビジネスロールを束ねる IT ロールにより定義する。従って、本項以前の各項に記述したビジネスロールの承認プロセスを参照

4.3.4.2. トリガイベントごとのロール管理運用概要（フロー）

前項に述べたトリガイベントごとのアプリケーションロール管理運用フローの概要を下表に示す。

表 4.24　トリガイベントとアプリケーションロール管理運用フロー概要

<table>
<tr><th>トリガイベント</th><th>左記イベントにより生じるアプリケーションロール管理運用</th><th>左記ロール管理運用に伴って生じるビジネスロール及び IT ロール管理運用</th><th>補足</th></tr>
<tr><td rowspan="5">アプリケーション自体の変更</td><td>ロールの作成</td><td rowspan="5">・ ロールの作成
・ ロールの定義の変更
・ ロールに割り当てる権限の変更
・ ロールを割り当てるアプリケーションロールの変更
・ ロールの削除</td><td rowspan="5">アプリケーションの利用開始、終了及びその間のアプリケーションの機能変更などにより、アプリケーションロールの要否及び定義と必要な権限が変化する。
これに伴って、アプリケーションロールに割り当てられるビジネスロールや IT ロールについても作成、定義や権限の変更、割り当てるアプリケーションロールの変更、削除が行われる（不要なこともある）</td></tr>
<tr><td>ロールの定義の変更</td></tr>
<tr><td>ロールに割り当てる権限の変更</td></tr>
<tr><td>ロールオーナの変更</td></tr>
<tr><td>ロールの削除</td></tr>
<tr><td>アプリケーション利用者の変更</td><td colspan="3">－*1</td></tr>
<tr><td>アプリケーションロール自体の棚卸し時</td><td colspan="3">－*2</td></tr>
<tr><td>定期的なアプリケーションメンバの棚卸し時</td><td colspan="3">－*1</td></tr>
</table>

*1：アプリケーションの利用者はビジネスロール（あるいは IT ロール）で定義される。そのため、アプリケーションの利用者の変更はすなわちアプリケーションロールに割り当てられるビジネスロール及びビジネスロールのメンバの変更になる。ビジネスロールのアプリケーションロールへの割り当て、及びビジネスロールのメンバ変更及び棚卸しの運用については、本項以前の各項に記述したビジネスロール管理運用を参照

*2：アプリケーションロールの要否は、各ビジネスロールの棚卸しにおいてアプリケーションロールへの割り当てを確認する際に実施してするため、ここで独立して実施しない。ビジネスロール管理運用における、アプリケーションロールの棚卸しについては、本項以前の各項の「運用フローにおけるタスクとそのアクタ」における棚卸し時の運用フローとタスクを参照

4.3.4.3. トリガイベントごとのロール管理運用詳細（フロー、タスク及びアクタ）

アプリケーションロール管理運用フローにおけるタスクとそのアクタを下表に示す。

表 4.25　アプリケーション自体の変更時のロール管理運用フローにおけるタスクとそのアクタ

No.	フロー概要	タスク	アクタ
1	アプリケーションロールの操作や棚卸しを行うトリガイベントが発生する	・ アプリケーションの利用開始、置き換え、利用終了をトリガとする場合は、本項内「4.3.4.1 ロール定義の基になる情報及びその情報に変更が生じるイベント」に記述の通りの承認プロセスを行う。	本項内「4.3.4.1 ロール定義の基になる情報及びその情報に変更が生じるイベント」の承認プロセスを参照
2	トリガイベントにおいて、アプリケーションロール設計の変更要否を判断し、必要があればアプリケーションロールの設計を変更する	・ 以下を確認する ➢ 設計済みのアプリケーションロールへの変更有無 ・ アプリケーションの利用開始や利用終了の場合や置き換えや機能変更によりアプリケーションロールに変更が必要な場合にはロール設計（アプリケーションロール）変更を行う	アプリケーションを管轄する立場の人員（アプリケーションオーナとして。例　各アプリケーションを管轄するシステム部部長）
3	トリガイベントにおいて、アプリケーションロールの設計に基づいて、アプリケーションロールに対して必要となる操作や棚卸しを決定し実施する	・ アプリケーション自体の変更を実施する日に、上記で変更したロール設計（アプリケーションロール）に基づいて、アプリケーションロールの作成、メンバの変更、アプリケーションロールオーナの変更、削除を実施する。	アプリケーションロールオペレータ

4	変更されたアプリケーションロールについて、ビジネスロールや IT ロール設計の変更要否を判断し、必要があれば各ロールの設計を変更する	・ 以下を確認する ➢ 上記アプリケーションロール設計の変更に伴い、アプリケーションロールに割り当てを追加あるいは解除すべきビジネスロールの有無 ・ ビジネスロールの有無と割り当てに応じて、ビジネスロールを変更する場合にはロール設計（組織型ロール、プロジェクト型ロール、ライン型ロール）変更を行う	ビジネスオーナ
		・ 以下を確認する ➢ 上記アプリケーションロール設計の変更に伴い、アプリケーションロールに割り当てを追加あるいは解除すべき IT ロールの有無を確認する ・ IT ロールの有無と割り当てに応じて、IT ロールを変更する場合にはロール設計（IT ロール）変更を行う	IT オーナ
5	変更されたビジネスロールや IT ロール設計に基づいて、各ロールに対する操作や棚卸しを実施する	・ アプリケーション自体の変更が実施される日に、上記で変更するロール設計（組織型ロール、プロジェクト型ロール、ライン型ロール）に基づいて、ビジネスロールの作成、メンバの変更、ロールオーナの変更、削除を実施する。	ビジネスロールオペレータ
		・ アプリケーション自体の変更が実施される日に、上記で変更するロール設計（IT ロール）に基づいて、IT ロールの作成、メンバの変更、ロールオーナの変更、削除を実施する。	IT ロールオペレータ

上表のロール管理運用フローを例示すると下図のとおり。

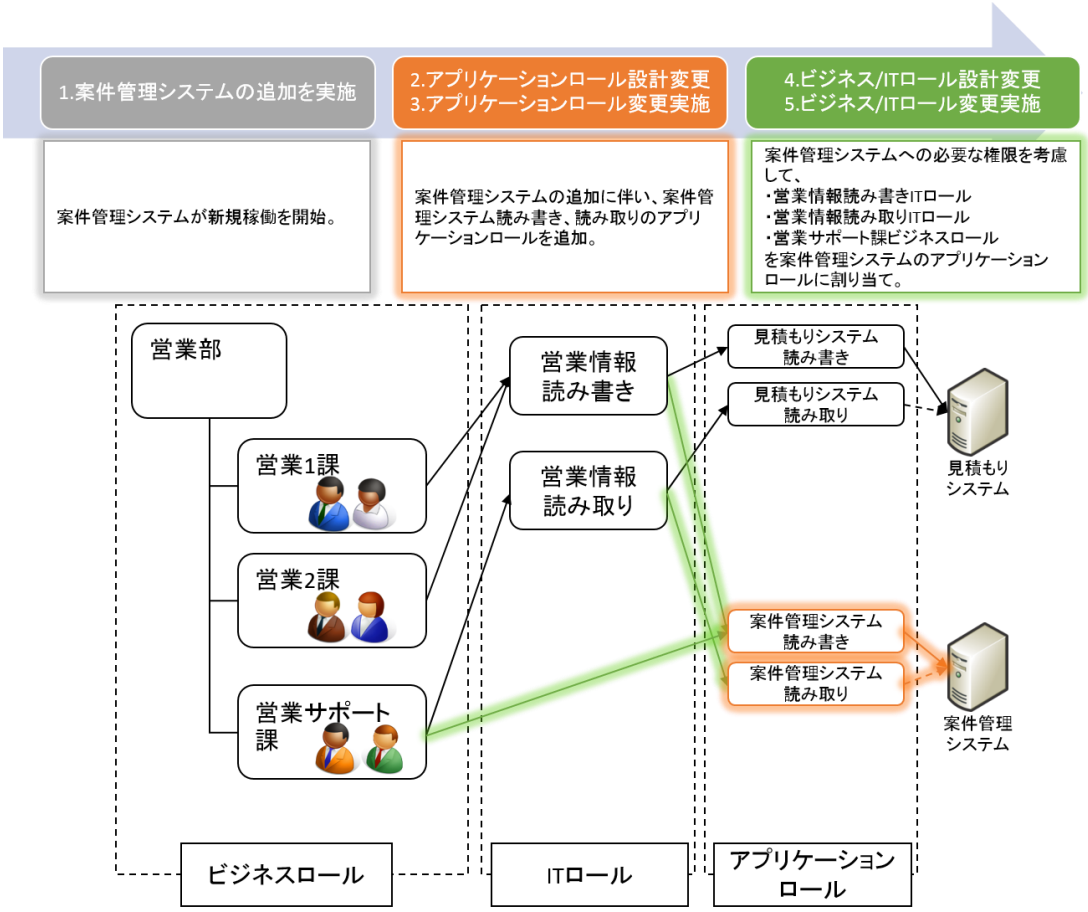


図 4.11　アプリケーション自体の変更時のロール管理運用フローの例

まとめ

ロール管理運用においては、以下項目を考慮する

- ロール定義の基になる情報とその承認プロセス
- ロール管理運用が生じるトリガとなるイベント
- ロールライフサイクルにおけるロール管理運用フロー、タスクとアクタ

ロール管理運用が生じるトリガとなるイベントは、ビジネス側、アプリケーション側で生じる可能性があり、それによって運用フローが変わる。また、ビジネス側でトリガとなるイベントが生じた場合にも、ロールタイプによって上記項目が異なるので留意する。

第5章
ロール管理の仮想企業導入事例

5.1. 金融業の仮想企業におけるロール管理導入事例

本節では、ロール管理の導入事例として、金融業（クレジットカード会社）の仮想企業における事例を説明する。

本仮想企業事例は、本 WG 出版書籍「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」の 6.1 節に記載の事例をベースにしている。

5.1.1. 金融業の仮想企業事例の全体像

最初に、金融業の仮想企業事例の全体像を整理しておく。

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

表 5.1　金融業（クレジットカード会社）仮想企業のプロフィール

業種		金融 (カード会社)
従業員数		3,000 （正社員:2,000名　非正社員:1,000
IDユーザ数		3,000
課題	コンプライアンス	監査対応
	情報漏えい対策	必要
	法制度/業界ガイドラインからの要	SOX、J-SOX、PCI DSS、GLBA、BASEL II
	その他	CoBIT, ITIL
	シェアードサービス	あり
社内体制	ISMS	あり
	CoBIT	あり
	ガバナンス体制	内部統制対策室設置
情報システム		・財務系システム（RDBMS） ・情報系システム（LDAP） ・Active Directory ・CRMシステム（パッケージ・ソフト） ・物理入退館システム ・メインフレーム ・データ分析ツール など
ハードウェア		Windows、Linux、商用UNIX、メインフレー
IDM対象範囲		B to E（社内システムユーザ対象）
IT運用者数		50名程度
情報の分類	オーナ 決定権者	存在する CIO
その他		自社内にコールセンタあり

J カードは、ID／アクセス管理およびロール管理に関して、以下の課題を抱えていた。

- 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

そこで J カードは、これらの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。

5.1.2. 本事例でロール管理導入にあたり意識したポイント

J カードは、ロール管理導入にあたり、以下に挙げた点を意識し検討を進めた。

- 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」（IT 業者の開発・保守用 ID）、「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）」

5.1.3. 本事例のスコープ

本事例では、以下の範囲に焦点を絞り、以降の説明を記述する。

- 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・企画およびロール設計までの部分を説明する。

5.1.4. 現状調査

J カードではロール管理を導入するにあたり、まずはロール管理に関する現状がどうなっているかの調査・確認を行った。

5.1.4.1. 組織調査

J カードでは、業務遂行上の役割分担の基礎になる組織体制・階層の構造を把握するために、各種規程などに明示された組織や役職情報の調査・確認を行った。それに加え、規程に明示されていない実際の業務遂行時の運用についても調査・確認を行った。

調査・確認の手掛かりとしては、以下のものを利用した。

- 社内組織図（組織規定より）
- 役職一覧（役職規程より）
- 決裁権限一覧（役職規程より）
- 稟議規程（稟議規程より）
- 雇用形態一覧（人事部へのヒアリングより）
- 業務フロー・手順（各業務規程及びマニュアルより）

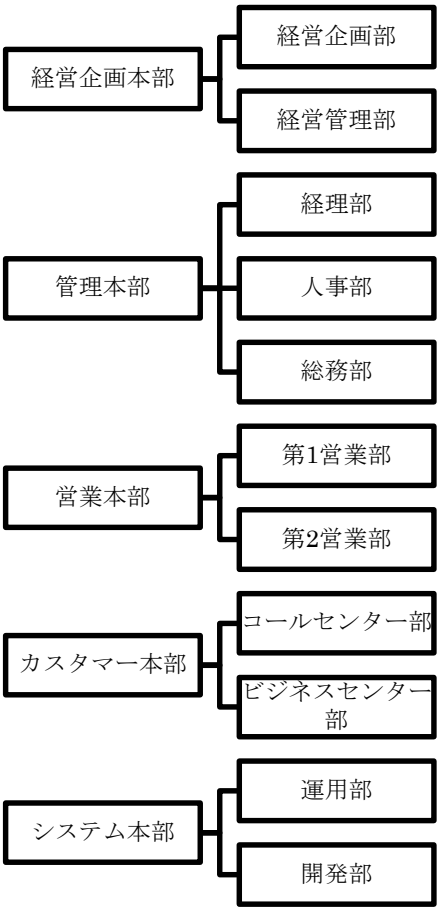
その上で、現場ヒアリングを行い、これらの手掛かりが組織体制・階層の構造を把握するための情報として妥当であることを評価した。

調査・確認の観点としては、以下の点に着目し整理した。

- 組織構成だけでは無く、階層・役職・拠点・雇用形態に関わる情報
- 組織の階層構造と、権限の範囲及び権限の継承の関係
- 兼務時の扱い
- 通常の組織図では表現されていないレポートラインの有無
- 上記いずれについても、権限の範囲を洗い出すために必要とされる以上に細かく分けすぎないこと
- 人事異動時の対応、引き継ぎ期間

調査の結果、組織体制・階層の構造は以下に整理したとおりであることが把握でき、調査メモとしてまとめた。

- 組織図



- 役職一覧

役職名	管理職扱いの有無
本部長	○
副本部長	○
部長	○
副部長	○
ゼネラルマネージャー*1	○
副ゼネラルマネージャー*1	○
課長	○
マネージャー*2	○
主任	×
アシスタントマネージャー	×

*1：ゼネラルマネージャーは部長職相当

*2：マネージャーは課長職相当

- 雇用形態

雇用形態名	人事発令の対象（正社員扱い）
正社員	○
出向受け入れ社員	○
派遣社員	×
契約社員	×
パート･アルバイト	×

- 運用に関するメモ
  - 人事発令の対象とならない従業員は、各部の部長決裁により採用され業務に従事する。
  - 人事異動時は、前任者が引き継ぎ期間として 2 週間のあいだ人事異動後も異動前と同等の権限を保持し、後任者の円滑な業務遂行を援助する。

5.1.4.2. 職務分掌調査

J カードでは、IT システム上で職務分掌が特に求められる業務としてどのような業務があるかを把握する ため、実際の業務上の権限や職務分掌はどうなっているかの調査・確認を行った。

調査・確認の手掛かりとしては、以下のものを利用した。

- 他の調査フェーズの成果物
- 職務分掌表
- 業務フロー・手順
- 社内規程
- 各種帳票類

その上で、現場ヒアリングを行い、職務分掌を洗い出した。

調査・確認の観点としては、以下の点に着目し整理した。

- 組織内、組織間、会社間での職務分掌
- 役割、職位、雇用形態に応じた職務分掌
- 申請、承認、実施など、業務プロセス上の職務分掌
- 各種稟議のプロセス
- カードの申込受付、発行、送付
- 本人確認、審査、与信、決済、請求、回収
- 顧客個人情報／決済情報の参照、変更

- 特権分掌
- IT システムの運用管理上の職務分掌
- IT システムの開発、テスト、運用、監視のプロセス上の職務分掌
- セキュリティ上の職務分掌
- 監査の分掌
- 影響度の大きい業務や権限の複数人実行

これらの観点については、以下に挙げる「職務分掌の原則」も踏まえ整理を進めた。

- 職務分掌の原則
  - 職務分掌が求められる業務における「申請（代行）」、「承認（代行）」、「実施」は、それぞれ別の組織／人物が行う。
    「承認」は、当該業務のリスク影響度の大きさにより、必要に応じて多段とする。
    同様に、「実施」は、必要に応じて複数人による作業とする。
  - IT システムの「開発」、「テスト」、「運用」、「監視」は、それぞれ別の組織／人物が行う。
  - IT システムを構成するネットワーク、サーバ（OS）、仮想環境などの「インフラ」、「アプリ」、「データ」の運用管理は、それぞれ別の組織／人物が担う。
  - データセンタやコンピュータ室の「物理セキュリティ」と「システムセキュリティ」は、別の組織／人物が担う。
  - 「監査」は、各種組織から独立の第三者組織が担う。

また、以下に挙げるような職務分掌の分け方が為されているかどうかの確認も行った。

- 職務分掌の分け方
  - ライン、組織、会社を分ける
  - 役割、職位、雇用形態による区分を変える
  - 別ラインの管理職上位者による承認、予算管理部門の承認
  - オペレーション会社による実施
  - 派遣社員は正社員が代行申請、等

以下に挙げる業務は、特に職務分掌が求められる業務として、注意深く調査・確認を行った。

- 職務分掌が求められる業務
  - 財務会計にかかわる業務
  - カードの申請受付、発行、送付
  - カード利用申請者の本人確認、審査、与信
  - カード利用による決済、請求、回収
  - 顧客個人情報／決済情報の参照、変更
  - IT システムやセキュリティの特権を用いた運用管理

調査・確認の結果、本事例のスコープの範囲では、以下に挙げる代表的な職務分掌の要件が存在することが分かった。また、課題もあることが分かった。

- 代表的な職務分掌の要件

業務	職務分掌	備考（課題）
経費精算	①申請： 経費利用者本人、あるいは所属部門の代行者（正社員）、 ②部門承認： 経費利用者本人の所属部門の部門長あるいは部長クラス（申請者が部門長の場合は、部門長の上長が部門承認を 代行）、 ③経理部承認： 経理部の当該部門担当者（マネージャークラス以上）	・②部門承認は、本来は部長クラスの職務だが、マネージャークラスが担っている部門も存在する。 ・③経理部承認は、本来はマネージャークラス以上の職務だが、主任・担当クラスが担っている場合もある。 ・上記の課題に対するシステム上の制約は掛けられていない。
営業管理（顧客管理）	①申請： 当該データの顧客担当者本人、あるいは所属部門の代行者（正社員）、 ②部門承認： 顧客担当者本人の所属部門の部門長あるいは部長クラス（部門長が申請者になることは無い）、 ③営業本部・顧客管理担当承認（二段）：営業本部・顧客管理担当の担当者と、その上位職位者（部長クラス以上）	・②部門承認は、本来は部長クラスの職務だが、マネージャークラスが担っている部門も存在する。 ・③営業本部・顧客管理担当承認の二段目は、本来は部長クラス以上の職務だが、マネージャークラスが担っている場合もある。 ・上記の課題に対するシステム上の制約は掛けられていない。

5.1.4.3. ライン型（定型・組織別）業務調査

J カードでは、ライン型業務としてどのような業務が存在し、その中でどのような役割や権限が存在するかを把握するため、以下を手掛かりに調査を開始した。

- 業務フロー
- 業務マニュアル・手順書
- 関連帳票
- 業務システムのアクセス権限情報

しかし、手掛かりとして利用した業務フロー、手順書等に記載された情報が実状と合っているとは限らず、実際の現場では異なるフローや手順で業務が実施されている可能性もある。そのため、調査ではシステム担当に対するヒアリングや現場確認を行い、フローや手順の実状の確認も行った。

その際、ライン型業務として以下の点に着目した。

・権限を保持する組織、階層の関係

・業務の管理オーナ（管理部門など）

調査の結果、代表的な業務およびその中での役割・権限として以下に挙げるものが存在した。
また、あるべき姿と実状とのずれが発生していることも判明した。

- 代表的な業務

業務名	概要	業務フロー	関連システム	関連部署
経費精算システム	経費申請	申請者→部門長→運用担当者	経費精算システム 会計システム ActiveDierctory	全部署 経理部 （管理部門：経理部）
営業管理システム	顧客管理	申請者→部門長→営業部担当→営業部承認者	営業管理	営業部 （管理部門：営業部）
システム利用申請	システムへのユーザ登録・変更・削除を管理	申請者→部門長→情報システム部担当者	ID 管理システム	全部署 情報システム部 （管理部門：情報システム部）

- 役割と権限

システム	対象者	役割	権限	備考（課題等）
経費精算システム	社員（本人あるいは代行者）	経費の利用を申請する	申請	
経費精算システム	部長職以上	部門に所属している社員の業務を承認する	部門長の承認権限	本来は部長職以上だが、マネージャークラスが承認している部門もある
経費精算システム	経理部の担当者	業務の最終的な承認をする	経理部の承認権限	本来はマネージャークラス以上に承認を行わせたいが、業務が回らないため、役職に関係なく承認者を割り当てている
営業管理システム	社員（本人）	担当する顧客管理用のデータ更新を申請する	申請	
営業管理システム	部長職以上	部門に所属している社員の顧客管理データ更新を承認する	部門長の承認権限	
営業管理システム	営業部の担当者	営業部として申請内容をチェックする	営業部担当者の承認権限	
営業システム	営業部の部長職以上	業務の最終的な承認をする	営業部承認者の承認権限	
システム利用申請	マネージャー以上	担当範囲のユーザのシステム利用申請を実施する	申請	本来はマネージャークラス以上に申請を行わせたいが、業務が回らないため、一部の部門では役職に関係なく申請者を割り当てている
システム利用申請	部長職以上	部門に所属している社員のシステム利用申請を承認する	部門長の承認権限	
システム利用申請	情報システムの担当者	システム利用申請の最終的な承認をする	運用担当者の承認権限	

5.1.4.4. プロジェクト型（期間限定・組織横断）業務調査

J カードでは、プロジェクト型業務としてどのようなものがあるかの洗い出しを、以下の観点で実施した。

- 組織単位ではなく組織横断で実施する業務
- 構成メンバも組織横断となっていること
- 期限付きか、期限無しか（期限無しの場合は定期開催の業務）

上記に該当する業務をリストアップして分類し、各分類で代表的なプロジェクトをサンプルケースとして詳しく調査した。

Ｊカード社　プロジェクト型業務　洗い出し

- ①-1）新規カード入会キャンペーンプロジェクト　（不定期開催）
- ①-2）他社タイアップ売り上げ増キャンペーン　（不定期開催）
- ②-1）顧客満足度向上プロジェクト（定期開催）
- ②-2）個人情報保護・セキュリティ向上タスク　（定期開催）

サンプルプロジェクトについて以下の情報を収集し、プロジェクトの中でどのような役割や権限が存在するかを整理した。

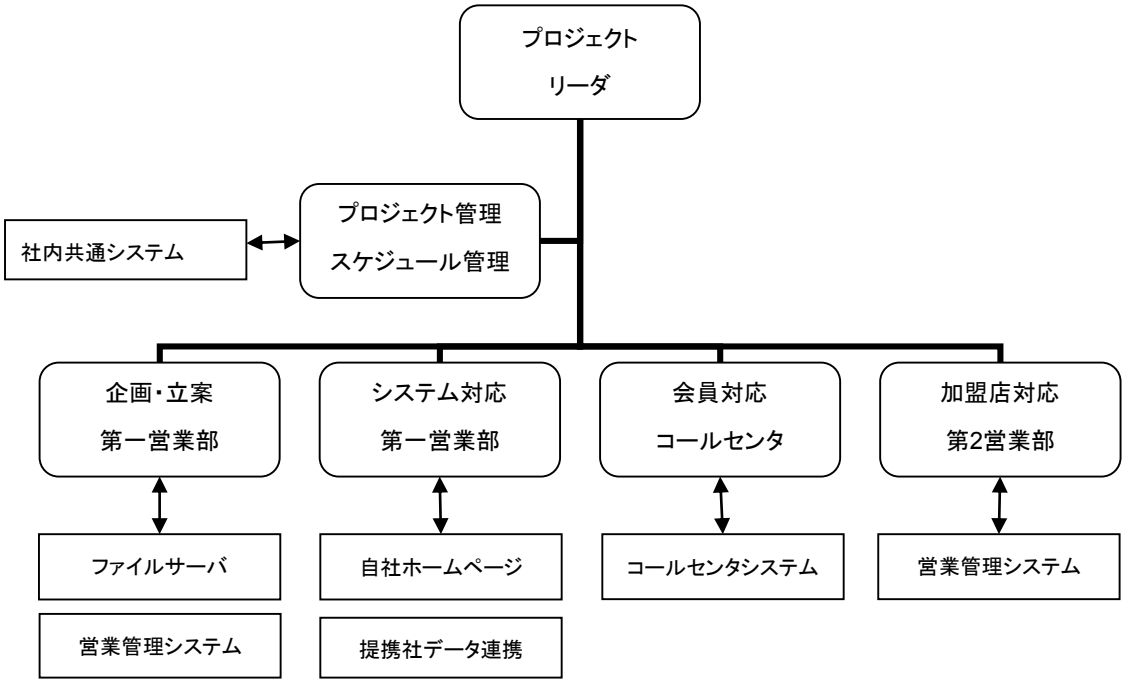
- プロジェクト体制図
- 業務内容の確認
- 業務の処理の流れと、処理に関係する人
- プロジェクトで使用するシステムのリストアップ

代表的なサンプルプロジェクトとして、①-2)と②-2)について調査を実施した。

調査結果は以下に整理したとおりであった。

①他社タイアップ売り上げ増キャンペーン の業務調査

プロジェクト体制図と利用システム



プロジェクト期間（ロールの有効期間）： 201X 年 YY 月～ 201X 年 ZZ 月

業務内容

- キャンペーン内容企画
- 宣伝
- 顧客情報管理
- 問い合わせ対応
- 加盟店対応
- システム対応
- 経理・購買
- アルバイトなど臨時増員

業務詳細（役割と権限）

プロジェクトリーダ：

プロジェクトに関わる全ての業務について決定権限、承認権限を持つ。

プロジェクト管理チーム：

プロジェクトの実施に伴う事務局機能（スケジュール管理、備品準備、経費精算、人員補充など）を担う。

プロジェクトで情報共有に利用するグループウェアの管理や、メールの一斉同報のためのグループメンバ登録も担当している。

企画・立案チーム：

キャンペーンの具体的な内容について企画・立案し、リーダの承認を得た上で、提携社との連携交渉、広報・宣伝活動、各チームへの作業依頼などを行う。

システム対応チーム：

キャンペーン宣伝用 Web ページの開発と、キャンペーンの内容により追加の機能開発を行う。提携社とは、キャンペーンの情報交換　（どのユーザがキャンペーンに該当するサービスをどれだけ利用したかなど）が必要となるため、そのための仕組みを開発する。

会員対応チーム：

カード会員からのキャンペーンに関する問合せに備え、コールセンタシステム用の応答情報の作成および入力を実施する。また、コールセンタメンバへのキャンペーン情報の一斉送信による教育なども実施する。

加盟店対応チーム：

キャンペーンについての通知と、加盟店からの問合せ対応を実施する。

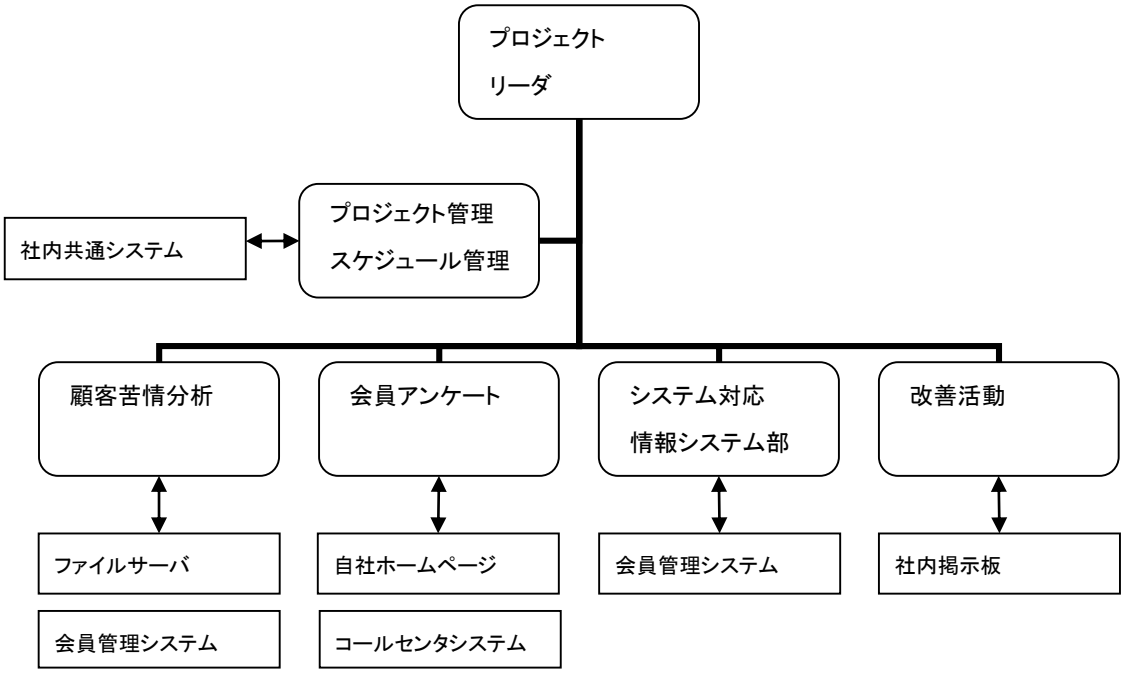
現状の課題

プロジェクトメンバのグループウェア（情報共有システム）に対するアクセス権限付与は、プロジェクト管理チームが一人ひとりについて手動で設定しており、作業量が多く、かつ反映までに時間が掛かっている。

プロジェクト終了時に権限の削除作業は行っておらず、監査で不備を指摘される可能性がある。

②顧客満足度向上プロジェクト

プロジェクト体制図と利用システム



プロジェクト期間　　期限は無し。定期開催。ただしメンバ変更が発生する

業務内容

- お客様苦情報告書の調査
- 満足度アンケートの企画・実施・集計
- 満足度向上企画　（コールセンタ向け、一般社員向け、加盟店向けの研修など）

業務内容詳細（役割と権限）

プロジェクトリーダ：

プロジェクトに関わる全ての業務について決定権限、承認権限を持つ。

プロジェクト管理チーム：

プロジェクトの実施に伴う事務局機能（スケジュール管理、備品準備、経費精算など）を担う。

プロジェクトで情報共有に利用するグループウェアの管理・権限追加や、メールの一斉同報

のためのグループメンバ登録も担当している。

苦情分析チーム：

コールセンタに寄せられる苦情・意見を集約し登録してあるグループウェア（情報共有システム）上の登録内容を調査・分析する。

会員アンケートチーム：

会員情報システムからランダムに抽出したカード会員に対して、はがきまたはメールにてアンケートを送付し、回収・整理・分析を行う。

改善活動チーム：

苦情・アンケートの分析結果から、チームで検討した要改善点を全社に通知し、改善のための活動を推進する。

システム対応：

改善活動チームからの依頼を受け、システムの改善を検討・実施する。

現状の課題

顧客満足度向上プロジェクトは、長期に繰り返し実施されるため、各担当者の交代が発生する。会員情報システムや苦情情報へのアクセス権限は、プロジェクト事務局がユーザごとに設定しており、担当者の交代時の権限削除まで手が回っていない。

担当を外れても顧客苦情情報へのアクセスが可能なままになっているなど、権限管理の不備が指摘されている。

5.1.4.5. 対象システム調査

J カードでは、ロール管理対象となるシステムにおける権限付与の状況を確認するために、各システムのアクセス権限管理方法と実際に付与されている権限の調査を実施した。

アクセス権限管理方法としては管理方式、運用方式の明確化を行った。

・管理方式（RBAC,メニュー制御等）

・運用方式（個人ごとに権限付与、所属により自動決定等）

調査・確認の手掛かりとしては、以下のものを利用した。

- 他の調査フェーズの成果物
- システム設計書、
- 運用手順、
- 各種帳票類

その上で、現場ヒアリングを行い、権限付与状況の整理を実施した。

調査・確認の観点としては、以下の点に着目し整理した。

- グループやロール
- ID に紐づく属性情報
- ID の文字列内に表現されるもの（ID に組織コードや役割を含むもの等）
- アクセス制御に関するシステム設定
- プログラム中にコーディングされているアクセス制御

調査結果は以下に整理したとおりであった。（ここでは代表的なものを記載）

各システムのアクセス権限管理・運用の状況

	システム	管理部署	権限運用	権限管理における課題
1	経費精算システム	経理部	利用者権限：所属に権限が付与される。 管理者権限：管理者による登録	利用者権限：個人に付与している権限の棚卸 管理者の権限の妥当性の確認手法の確立
2	営業管理システム	営業部	担当営業のみが参照、更新可能。 管理職は自部門の情報を参照、更新可能。	情報によっては共有したい情報もあるが現在は担当営業しか見ることができない。
3	ActiveDirectory ファイルサーバ	情報システム部	所属単位にグループを作成し権限付与。 モバイル利用者は別OUにて管理	モバイル利用者、PC権限含めた管理方式の統一
4	コールセンターシステム	コールセンター	個人単位にメニュー権限をアプリにて付与。 権限設定については申請票のエクセルをワークフローに添付し承認後、情報システム部にて設定	組織異動時の棚卸、権限の再設定の負荷軽減
…				

システム・ロール・権限の関係の整理

	ユーザ1 営業部長	ユーザ2 総務課長	ユーザ3 営業担当	ユーザ4 総務担当	ユーザ5 コールセンタ担当
AD、ファイルサーバ	○	○	○	○	○
営業管理システム	○		○		
経費精算システム	○	○	○	○	○
コールセンターシステム					○

		ユーザ1	ユーザ2	ユーザ3	ユーザ4	ユーザ5
権限	AD、ファイルサーバ	更新、削除、参照	更新、削除、参照	更新、参照	更新、参照	更新、参照
	営業管理システム	承認、参照		登録、参照		
	経費精算システム	申請、承認	申請、承認、管理	申請	申請、管理	申請
	コールセンターシステム					登録

5.1.4.6. 対象法規制調査

J カードでは、ロール管理にかかわる法規制についても、あらためて調査・確認を行った。

J カードはクレジットカード業であるため、考慮すべき法規制として、以下に挙げる法令や自主規制を含む業界ルール／自社ルールを調査対象とした。

J カードは原則として国内消費者および加盟店向けの事業を担当するため、国際的な企業において考慮すべき法規制の調査は不要であるものとした。（国際的な企業の場合、関連国／地域における法規制への適合を意識する必要がある。）

作業内容

- 関連法令／自主規制の調査
- 前段までの成果物の法規制観点でのレビュー

作業実施上の注意点

法令だけでなく、組織が取得している認証（ISMS、QMS 等）、業界団体のガイドライン、組織が加盟している団体のガイドライン等にも注意を払った。

対象とした法令／自主規制など

- J-SOX
- 割賦販売法
- 貸金業法
- PCIDSS
- 犯罪収益移転防止法
- 個人情報保護法／プライバシーマーク／WebTrust
- ブランド内ルール／Ethics
- 信用情報機関との取り決め
- グループ会社内における個人情報／信用情報の取り扱いルール
- 取得済、取得予定の認定制度

その他の考慮点

- 法令などで定義される取得／認定資格の要否、ならびに各社員が保持している資格とその有効期限などの管理に関しても考慮した。資格有無／期限の管理は、ロール棚卸運用でのチェック項目になるため、運用設計で考慮すべき申し送り事項とした。
- 職務分掌の調査上、「申請」、「承認」、「実施」の分権の実現に当たり、「二人以上で行う作業」、「同一担当者が実施してはならない作業」など、ロール設計に影響を及ぼす事項を洗い出した。

- 外部委託先等の社員に付与するロールを定義する場合の条件を明確化した。例えば、外部委託先の社員による業務の承認は、外部委託先の管理者による承認を得た上で、委託元の管理者が承認すること等。

成果物

- 調査メモ（法規制・コンプライアンス）
- 職務分掌にかかわる要是正点（特に、「申請」、「承認」、「実施」の分権が実現できているかの確認が重要）
- 法務、業務企画などの社内プロセス主管部署による成果物レビュー結果の反映
- 倫理規定を所轄する部署による成果物レビュー結果の反映
- 法規制対応の観点での運用設計の確認または申し送り事項
- 外部委託先等の関連会社へ依頼すべき事項

調査・確認の結果、営業管理システムにかかわる法規制がロール設計に影響を及ぼす点は、以下のとおりであった。

- 個人情報の取扱いに関する適正な権限付与の確認が必要
  - 担当顧客情報の新規登録から、参照、変更、削除に至る業務を担うユーザ（営業部の担当者、管理職、部門長、ならびに営業部外の社員）に付与される各ロールは、業務上必要最小限の情報のみを登録／参照／変更／削除可能であるように定義できていること
  - 担当者が不在の際に代行処理が必要である場合は、代行処理に関するルールが内部規程で定義されており、その定義通りに運用されるロール定義・付与になっていること
- 監査ロールの定義に関する確認が必要
  - 当該システムにおけるデータへのアクセスに関するログ等が適切に記録され、それを管理する監査目的のロールが業務目的のロールとは別に定義されていること

5.1.5. ロール設計

J カードでは、ロール管理に関する現状調査の結果と、ロール管理導入の目的や目指すべき目標像を踏まえ、ロール設計の検討を行った。

5.1.5.1. 組織型ロール設計

組織型ロールの設計では、組織体制における役割分担に応じて、組織、役職、雇用形態などをベースとした権限管理を行うためのロールを定義する。

J カードでは、現状調査フェーズにおける以下の成果物をインプットとして、組織型ロールの設計を行った。

- 調査メモ（組織）
- 調査メモ（職務分掌）
- 調査メモ（対象システムのアクセス権限管理の状況）

これらのインプットから、以下に示す手順で組織型ロールを設計した。

1. ロールの抽出とメンバの定義
2. ロール間の関係整理
3. ロールの運用整理

以降で、各手順の詳細を説明する。

1. ロールの抽出とメンバの定義

ここでは、調査メモの分析から抽出したロールとそのメンバの決定方法を説明する。

ロールを抽出するために、まずトップダウン型モデリングを使って、調査メモ（組織）から以下の方針を導き出した。

- 各組織（本部、部）に相当するロールが必要
- 組織をまたいだ役職ごとのロールが必要
- 組織をまたいだ雇用形態区分ごとのロールが必要
- 各組織内で役職ごとにロールを分けると細分化しすぎるため、調査メモ（対象システムのアクセス権限管理の状況）を分析し、要否を判断

・ 各組織内で雇用形態区分ごとにロールを分けると細分化しすぎるため、調査メモ（対象システムのアクセス権限管理の状況）を分析し、要否を判断

一方、調査メモ（対象システムのアクセス権限管理の状況）から、以下のことが読み取れた。

・ ファイルサーバの権限管理用に組織ごとのグループを作成・利用
  - ファイルサーバの権限管理用の組織ごとのグループは、調査メモ（組織）に記載した組織の単位と合致
  - ファイルサーバの権限管理用には、組織ごとの管理職メンバのみで構成するグループも利用
・ 経費精算システムでは、経理部という組織のメンバ全員に対してチェック権限を付与
・ 経費精算システムでは、各組織の副部長以上の役職者に対して当該組織内での経費申請に対する承認権限を付与
・ コールセンタシステムでは、雇用形態区分によるスーパバイザとオペレータの権限分離を実施
・ 会員管理システムでは、雇用形態区分によるスーパバイザとオペレータの権限分離を実施
・ 派遣社員、契約社員、パート・アルバイトは人事発令の対象外となり、その管理は各組織に委任

以上を踏まえて、当初導き出した方針を再検討し、以下の結論になった。

・ 組織図に記載された各部に相当するロールは必要
・ 組織図に記載された各本部に相当するロールは不要
・ 組織をまたいだ役職ごとのロールは不要
・ 組織をまたいだ雇用形態区分ごとのロールは不要
・ 各部内で、役職に関して以下の 3 種類に分けたロールが必要
  - 部長相当職
  - 管理職
  - 上記以外
・ 各部内で、雇用形態区分に関して以下の 2 種類に分けたロールが必要
  - 正社員
  - 非正社員

このように抽出した組織型ロールとそのメンバの定義を下表に示す。

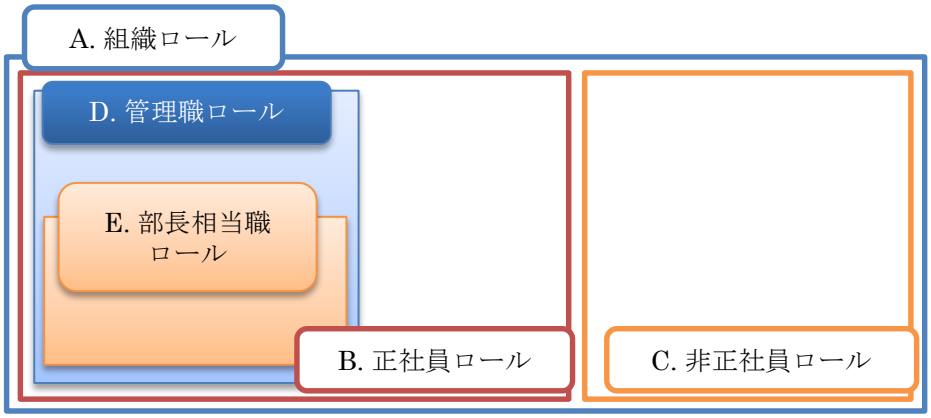
	組織型ロール	メンバ
A	部ロール	当該部の全構成員
B	部の正社員ロール	当該部の全構成員の中で、正社員扱いする構成員
C	部の非正社員ロール	当該部の全構成員の中で、正社員扱いしない構成員

D	部の管理職ロール	当該部の全構成員の中で、管理職相当の役職にある社員
E	部の部長相当職ロール	当該部の全構成員の中で、部長職相当の役職にある社員

2. ロール間の関係整理

ここでは、前項で定義した組織型ロールのロール間の関係を整理した内容を説明する。

上述のロール間に成立する包含関係は下図の通りとなるため、個別にロールメンバを設定せずにロールの入れ子によってロールメンバを設定した。



3. ロールの運用整理

ここでは、組織型ロールの運用について、以下の 2 点に関して定義した内容を説明する。

- ロール運用上の役割
- ロール運用におけるロール自体の操作とロールメンバの操作タイミング

組織型ロールの運用上の役割とその担当者を下表に示す。なお、組織型ロールが部単位で定義されることから、上述の 5 種類の組織型ロールにおいては下表の役割は共通となる。

運用上の役割	左記役割の説明	担当者
ビジネスロールオーナ	ビジネスロールに所属するメンバの決定権限を持つ	各部の部長及び副部長
ビジネスロールメンバ	ビジネスロールに所属するメンバ	各組織型ロールのメンバとして定義された構成員
ビジネスロールオペレータ	ビジネスロールのメンバの追加・削除を行う	各部の部長及び副部長からの委任を受けて、当該部のロールメンバの追加削除を行う当該組織の構成員

ロール運用におけるロール自体の操作とロールメンバの操作タイミングを下表に示す。

	組織型ロール	ロール自体の操作タイミング	ロールメンバの操作タイミング
A	部ロール	人事発令時	人事発令時*1
B	部の正社員ロール	人事発令時	人事発令時*1
C	部の非正社員ロール	人事発令時	契約社員、派遣社員、パート･アルバイトの入社の前日及び退社の翌日*2
D	部の管理職ロール	人事発令時	人事発令時*1
E	部の部長相当職ロール	人事発令時	人事発令時*1

*1：当該部から他部に異動するメンバについては、2 週間後にロールメンバから削除する。

*2：契約社員、派遣社員、パート・アルバイトは部長決裁により入退社が決まるため、人事発令は待たない。

5.1.5.2. ライン型ロール設計

ライン型ロールの設計では、ライン型の業務（業務フロー）における役割分担に応じて権限管理を行うためのロールを定義する。例えば、業務上の承認権限や実行権限などが対象となる。

J カードでは、調査で取得した以下のインプットを主に利用して、ライン型ロールの設計を行った。

・調査メモ

・対象システムのアクセス権限管理の状況

これらのインプットから、次のような手順でライン型ロールの設計を進めた。

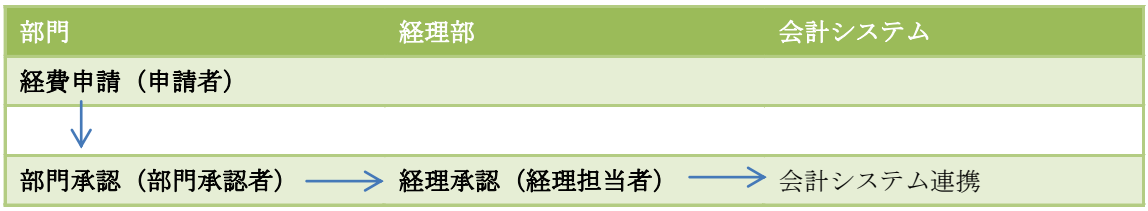
１：ライン型ロールの整理・定義

２：ロール間の関係を整備

３：運用上で必要なロールの確認

以降では、調査した業務の「経費精算システム」を例に取って、ライン型ロールの設計内容を説明する。

「経費精算システム」の概要



１：ライン型ロールの整理・定義

「経費精算システム」のロールを洗い出し定義した。抽出する際には次のポイントを意識した。

・個人以外の権限の最小単位の表現を目指す。

・業務フローの詳細レベルでのアクタが、ロールのベースになる場合が多い。

・アクタに「組織上の肩書き」がある場合、組織ロールと混同されることがあるが、業務フロー上のロールを定義する。

それらを意識して抽出したライン型ロールは以下のようになった。

・申請者ロール

・部門長経費承認者ロール

・経理承認者ロール

２：ロールの関連を整備

抽出したロールの整合性をチェックするために他ロールや権限などと比較して整理を行った。

ライン型ロールの区分は職位に対応するとは限らず、実際の職務に対応したものになるので、以下のように職務分掌との違いなどに注目して整理した。

・申請者ロールは職務分掌上「社員（正規社員＋契約社員）」となる。

・部門長経費承認者ロールは職務分掌上「部長」権限以上となる。しかし、この承認権限は「経費精算」業務に依存しているため、権限の範囲が変わる可能性がある。そのため、「経費精算」業務固有のロールにする必要がある。

・経理承認者ロールは経理部署の担当者に割り当てられる。担当者には特に組織上の肩書きは関係なく、選択された社員がその権限を有することになる。

３：運用上で必要なロールの確認

- 「経費精算システム」では、経理承認者ロールや経費部門長承認者ロールの割り当てを行うための運用担当者が必要となる。この役割は、このシステムの担当部署の部長以上に権限が割り当てられる。業務には直接関係しないため、運用のための「経費精算システム運用ロール」も必要となる。

■成果物

以上をまとめ、次のようなライン型ロールを定義した。

ライン型ロール	業務の役割	備考（職務上の権限）
申請者ロール	申請を行う人	社員
部門長経費承認者ロール	部門の申請を承認する人	部門の部長以上 ※このシステム固有にする必要がある
経理承認者ロール	部門承認を承認する人 （最終承認）	経理部の担当者 （運用者に割り当てられた人）
※運用ロール		
経費精算システム運用ロール	ロール管理を行う人	経理部門の部長以上

5.1.5.3. プロジェクト型ロール設計

プロジェクト型ロールの設計では、プロジェクト型の業務における役割分担に応じて権限管理を行うためのロールを定義する。

ここでは具体例として、5.1.4.4 でサンプルケースとして調査した代表的なプロジェクト：「他社タイアップ売上増キャンペーン」に関するプロジェクト型ロール設計を説明する。

J カードでは、当該プロジェクトの業務調査の結果に基づき、各種システムで必要となる権限をフレークダウンし、プロジェクトリーダ、プロジェクト管理チーム、その他チームのメンバそれぞれに対して付与する必要のある権限を整理した。

メンバが担う役割の種類	社内共通システム（経費精算、購買、メール他）	グループウェア情報共有システム（プロジェクト用）	営業管理システム（顧客・加盟店情報）	コールセンタシステム
プロジェクトリーダ	申請・承認	管理者権限	参照	承認
プロジェクト管理	申請・内容確認	管理者権限	参照	参照
企画・立案	申請	編集	参照	参照
システム対応	申請	編集	参照	——
会員対応	申請	編集	参照	変更申請
加盟店対応	申請	編集	参照	——

プロジェクト型ロールには、どのプロジェクトにも共通で必要になるプロジェクト定型ロールと、プロジェクトごとに必要になるプロジェクト固有ロールがあることが分かった。

プロジェクト定型ロール
- プロジェクトリーダロール
- プロジェクト管理ロール　（PMO ロール）

プロジェクト固有ロール（「他社タイアップ売上増キャンペーン」プロジェクトの場合）
- 企画・立案ロール
- システム対応ロール
- 会員対応ロール
- 加盟店対応ロール

プロジェクト型ロール	業務の役割	備考（職務上の権限）
プロジェクトリーダロール	プロジェクトに関わるあらゆる承認処理、参照・更新権限	管理職と同等
プロジェクト管理ロール	プロジェクトに関わる人事、経理、購買処理の申請・参照・代行承認	一般社員
プロジェクト固有ロール	プロジェクト固有の情報共有のための権限	一般社員

当該プロジェクトのプロジェクト固有ロールは、通常業務上で既に付与されている権限の範囲で対応可能な部分が多く、追加付与が必要な権限は主にプロジェクト内部向けのグループウェア情報共有システムにおける編集権限であることが判明した。
また、コールセンタシステムの権限は、プロジェクト固有ロールの中では企画・立案ロールと会員対応ロールに限り付与すべきものであることが分かった。

5.1.5.4. システムアクセス権限設計

システムアクセス権限設計では、最少権限（Least Privilege）の原則に従い、各システムで設定されているアクセス権限の見直しと再設計を行う。

J カードでは、下記の情報をインプットとして、アクセス権限設計を行った。
- 各種調査メモ

- 対象システムのアクセス権限管理の状況

インプットとなる情報から、以下の手順で設計を進めた。

1. 権限付与方針の整理
2. システム権限一覧の作成

＜権限付与方針の整理＞

各システムの権限について見直しを行い、権限付与の方針を以下のとおりに整理した。

No	システム名	使用メンバ	利用者権限の種類	利用者権限の与え方
1	経費精算システム	社員	申請権限・上司承認権限・チェック権限	申請権限：社員 上司承認権限：所属の管理職 チェック権限：経理部
2	ファイルサーバ Active Directory	全員（派遣社員・契約社員を含む）	フルコントロール・書き込み・読み取り・モバイル使用権限	所属／プロジェクト単位にセキュリティグループを作成し権限を付与。職位を考慮。 モバイル使用権限は個別申請とし、ユーザ毎に設定。
3	コールセンタシステム	コールセンタ部	個人単位のメニュー権限、承認権限	スキル（対応可能業務）に応じた権限をパターン化し個人に付与。 承認権限は SV（スーパーバイザー）に付与
4	会員管理システム	ビジネスセンタ部	個人単位のメニュー権限、承認権限	同上
5	営業管理システム	第１営業部	申請権限・上司承認権限限	申請権限：第一営業部 承認権限：第一営業部管理職
6	グループウェア	全員（派遣社員・契約社員を含む）	ロールで各機能に対する更新・参照権限などを設定	社員種別、所属、職位に応じてロールを定義

＜システム権限一覧の作成＞

システム権限一覧の例を以下に示す。（前頁の 1～3 のシステム）

① 経費精算システム

No	所属	職位	権限			
			申請権限	上司承認権限	チェック権限	管理者権限
1	経理部	課長以上	○	○	○	○（システム担当者のみ）
2		一般社員	○	×	○	○（システム担当者のみ）
3	経理部以外	課長以上	○	○	×	×
4		一般社員	○	×	×	×

② ファイルサーバ・Active Directory

No	所属／プロジェクト	職位	権限				
			各部門フォルダ	各部門管理職フォルダ	部門外フォルダ	プロジェクトフォルダ	モバイル使用権限
1	コールセンタ部	課長以上	R/W	R/W	×	×	△
2		一般社員	R/W	×	×	×	△
3	ビジネスセンタ部	課長以上	R/W	R/W	×	×	△
4		一般社員	R/W	×	×	×	△
5	第１営業部	課長以上	R/W	R/W	×	×	△
6		一般社員	R/W	×	×	×	△
7	第２営業部	課長以上	R/W	R/W	×	×	△
8		一般社員	R/W	×	×	×	△
9	情報システム部　運用部	課長以上	R/W	R/W	×	×	△
10		一般社員	R/W	×	×	×	△
11		管理者	F	F	F	F	F
12	情報システム部　開発部	課長以上	R/W	R/W	×	×	△
13		一般社員	R/W	×	×	×	△
14	プロジェクトメンバ	－	×	×	×	R/W	×
15	プロジェクトメンバ以外	－	×	×	×	×	×

F：フルコントロール、W：書き込み、R：読み取り、△：個別申請

③ コールセンタシステム

No	所属	業務種別	スキル	権限								
				インバウンド業務					アウトバウンド業務		管理者権限	
				新規契約受付	契約変更受付	各種問合せ受付	苦情受付	承認権限	入金催促	新規顧客開拓	運用管理権限	システム管理権限
1	コールセンタ部	スーパバイザ	SV	○	○	○	○	○	○	○	×	×
2		オペレータ	1	○	×	×	×	×	×	×	×	×
3			2	○	○	×	×	×	×	×	×	×
4			3	○	○	×	×	×	×	○	×	×
5			4	○	○	○	×	×	×	○	×	×
6			5	○	○	○	×	×	○	○	×	×
7			6	○	○	○	○	×	○	○	×	×
8		運用管理者（個人に付与)	－	×	×	×	×	×	×	×	○	×
9	情報システム部	システム管理者（個人に付与)	－	×	×	×	×	×	×	×	×	○
10	その他の所属	－	－	×	×	×	×	×	×	×	×	×

例外への対応

対応業務権限で例外がある場合には、スキルパターンを追加して対応することにした。

5.1.5.5. IT ロール設計

IT ロール設計では、個々の ID を持つユーザが付与されているビジネスロールそれぞれに対して、どのようなシステムアクセス権限が設定されているのかをまとめ、IT ロールとして定義する。

J カードでは、まず、ビジネスロールを縦軸に、システムアクセス権限を横軸にした表を作成し、各ビジネスロールがどのようなシステムアクセス権限を持つべきかを、これまでのロール設計の内容から定義した。その後、ビジネスロールごとにどのような IT ロールとしてシステムアクセス権限をまとめられるかを検討し、IT ロールを定義していった。

この時、下記の点に注意する必要があった。

- ビジネスロールは「業務上の役割」の定義であり、原則として変更されることはない。
- システムアクセス権限も、実際のシステム上での定義であるため、原則として変更されることはない。
- システムアクセス権限の定義が、例えば組織での役割に対するものなのか、あるいはライン型業務での役割に対するものなのか（システムがライン型業務用のものなのか）等を確認することにより、どのビジネスロールに対して、どのシステムアクセス権限を設定するべきかを判断する。
- ビジネスロールは、定義された役割が重複することがあり、重複する役割は統合することで、IT ロールの定義を進めていく。

J カードが IT ロール定義を進めた手順をまとめると、以下のとおりである。

① ビジネスロールを列挙する（表の縦軸）
② システムアクセス権限を列挙する（表の横軸）
③ ビジネスロールとシステムアクセス権限を対応付ける
④ ビジネスロールの中で統合するものを検討し、統合元に対応付けられていたシステムアクセス権限を、統合先のシステムアクセス権限として対応付ける
⑤ IT ロールを定義する（命名する）

Ｊカードでは、下記のロールを統合した。

ライン業務：経費精算業務

- 申請者ロール→各組織の正社員、非正社員全てのロールに統合
- 部門経費承認者→各部門の課長相当職以上（管理職）のロールに統合
- 経理承認者→経理部の正社員のロールに統合

ライン業務：営業管理

- 申請→第１営業部の正社員ロールに統合
- 承認→第１営業部の管理職ロールに統合

最終的に、Ｊカード社による IT ロールは、別添「J カード IT ロール定義表」のようになった。

以上

［編者］

特定非営利活動法人 日本ネットワークセキュリティ協会（JNSA）
標準化部会 アイデンティティ管理 ワーキンググループ

本ワーキンググループはアイデンティティ管理の必要性の啓蒙および導入指針の提示による普及促進、アイデンティティ管理分野の市場活性化を目的として、2005 年に JNSA の政策部会にて「内部統制におけるアイデンティティ管理 WG」として発足した。2007 年度には「内部統制におけるアイデンティティ管理解説書」第 1 版を発行。2008 年度には、標準化部会「セキュリティにおけるアイデンティティ管理 WG」として活動を継続し、「内部統制におけるアイデンティティ管理解説書」第 2 版を発行 2009 年度には「JNSA 賞 WG の部」を受賞している。2010 年度には「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」の初版を発行し、WG 名称を「アイデンティティ管理 WG」と変更して活動を継続。現在に至る。

【WGリーダ】

宮川 晃一　　日本ビジネスシステムズ株式会社

【主要執筆者】

貞弘 崇行　　株式会社アイピーキューブ

木村 慎吾　　株式会社インテック

齊藤 光司　　KPMG コンサルティング株式会社

酒井 美香　　日本 IBM システムズ・エンジニアリング株式会社

桑田 雅彦　　日本電気株式会社

南 芳明　　日本ベリサイン株式会社

今堀 秀史　　富士通関西中部ネットテック株式会社

福原 幸一　　富士通関西中部ネットテック株式会社

中島 浩光　　サブスクライバ（株式会社マインド・トゥー・アクション）

【ワーキングメンバ】

富士榮 尚寛　伊藤忠テクノソリューションズ株式会社

新嘉喜 康治　伊藤忠テクノソリューションズ株式会社

深澤 聡　　SCSK 株式会社

工藤 達雄　　NRI セキュアテクノロジーズ株式会社

内田 健一　　NEC ソリューションイノベータ株式会社

駒沢 健　　NTT コムウェア株式会社

杉村 耕司　　株式会社 NTT データ

山田 達司　　株式会社 NTT データ

深谷 貴宣　　KPMG コンサルティング

篠原 信之　　株式会社シグマクシス

後藤 厚宏　　情報セキュリティ大学院大学（教授）

塩田 英二　　TIS 株式会社

小林 智恵子　東芝ソリューション株式会社

栃沢 直樹　　トレンドマイクロ株式会社

飯塚 昭　　日本オラクル株式会社

後藤 兼太　　日本電気株式会社

見上 昌成　　日本ビジネスシステムズ株式会社

安納 順一　　日本マイクロソフト株式会社

村田 裕昭　　日本マイクロソフト株式会社

小野寺 匠　　日本マイクロソフト株式会社

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

佐藤 公理　　マカフィー株式会社

大竹 章裕　　株式会社ラック

（会社名　五十音順）　　以上