研究会報告

ＣＩＡフォーラム研究会報告

# Robotics Process Automation（ＲＰＡ）に係る自己点検（ＣＳＡ）の実践

研究会No.ｄ１（ＣＳＡの事例研究会）

ＣＩＡフォーラムは、ＣＩＡ資格保持者の研鑽及び相互交流を目的に活動する、一般社団法人日本内部監査協会（ＩＩＡ－ＪＡＰＡＮ）の特別研究会である。各研究会は、担当の座長が責任をもって自主的に運営し、研究期間、目標成果を設定し、研究成果を発信している。

当研究報告書は、ＣＩＡフォーラム研究会No.ｄ１が、その活動成果としてとりまとめたものである。報告書に記載された意見やコメントは、研究会の「見解」であり協会の見解を代表するものではなく、協会がこれを保証・賛成・推奨等するものでもない。

## エグゼクティブサマリー

近年、活用が飛躍的に拡大しているロボティック・プロセス・オートメーション（Robotic Process Automation：ＲＰＡ）により、従来は人が行っていた単純作業の自動化が可能になる。ＲＰＡはユーザー部門で手軽に実装できるがゆえにシステム部門の関与が無い場合も多く、利用実態の網羅的な把握や管理が難しく、内部監査人が気づいたときには仕様やメンテナンスができなくなった“野良ロボット”の課題に直面していることも少なくない。ＲＰＡの期待効果はローコストでの生産性向上であるが、ＲＰＡに関連するリスクは、無計画な導入、無秩序な実装と過剰な権限付与による展開等、戦略、オペレーショナル、セキュリティリスク等多様である。ＲＰＡの実装で得られた手続の省力化により、人的ミスが減少するメリットがある一方で、場合によってはこれまでの内部統制を毀損するリスクも生じてしまう。業務の効率化と内部統制をバランスよく両立するためには、適正なリスク評価と予防的・発見的統制が重要になる。

ＲＰＡの利用ルールを整備・運用、継続的に改善する仕組みとして、ＣＳＡ（Control Self-Assessment：自己点検）[1]の手法が有用と考えられる。１線で適時にＣＳＡを実践することにより、スモールスタートやアジャイル開発を重視した上で、必要な内部統制の実装が後回しにされないようにすることが必要である。

今回の研究では、スモールスタートの段階から着手すべきユーザー部門によるＣＳＡ、リスク評価及びコントロールの整備・見直し・運用等の基本的内部統制の実装、内部監査の実践ポイントについて、ケーススタディを使って考察し、その内容をとりまとめた。

[1] Control Self Assessmentの一般的な日本語訳は「統制自己評価」であるが、本稿では実務に即して「自己点検」とする。

## はじめに

労働人口減少への対応、働き方改革、ウィズコロナ時代の在宅勤務や業務プロセス改革の手段として、近年、人工知能（ＡＩ）やディープラーニング、その他関連技術と並んで、活用が飛躍的に拡大しているＲＰＡは労働生産性を向上する“デジタルレイバー（仮想知的労働者）”として、世界中の多くの企業・組織で導入と利活用が加速している。一方でＲＰＡ特有のリスクとその内部統制、内部監査に関する事例を詳述する文献がまだ少なく、内部統制や内部監査の実務家の方々におかれては、何をどこまで確認すべきか悩むのではないだろうか。ＲＰＡの最大の強みはスモールスタート、手軽に実装ができることであるが、その後、メンテナンスもしていない（管理者不在の）“野良ロボット”が組織の至るところで生じていることもよく聞く。今回の研究では、今後ますます活用範囲を広げるＲＰＡについて、スモールスタートの段階から着手すべきユーザー部門によるＣＳＡ、リスク評価及びコントロールの整備・見直し・運用等の基本的内部統制の実装、内部監査の実践ポイントについて、ケーススタディを使ってとりまとめた。

ＲＰＡと言ってもその種類や規模、用途はさまざまであるため、紹介するケーススタディは、業種や規模を問わず汎用性があり、かつ、初歩的な利用形態を踏まえるものとした。また、ケーススタディは架空会社での想定であるが、当フォーラムのメンバーの関与先で実際に起きている事実も含め、実践的内容とした。共感をいただければ幸いである。

また、本研究成果は、ＣＳＡを中心とした１線ないし２線の目線や取り組み内容にフォーカスし、読者である内部監査人に関連する監査テーマや監査手続作成時の気づきを得られるような構成とした。具体的には、まず、ＲＰＡについて俯瞰し、次いで、ケーススタディ会社の紹介、ＣＳＡの実践、ＣＳＡを踏まえたリスク評価の実践、ＣＳＡを踏まえたＲＰＡコントロールルールの作成・運用、今後の展開について述べる。

**＜目次＞**



## １．ＲＰＡについて

### １－１．利用目的や効果

ＲＰＡは、これまで人間のみが対応可能と想定されていた作業を人間に代わって実施できるルールエンジンやＡＩ、機械学習等を含む認知技術を活用して代行・代替する取り組みを指す[2]。特に我が国では、労働生産人口の減少に備え、働き方改革を実現するためのソリューションの１つとしてＲＰＡが注目されてきた。概念自体は2010年代初頭からあるものの、我が国では2017年に政府が公表した「未来投資戦略2017」等の中で明記された「第４次産業革命」への対応等を契機として、官民で広く利活用が進められるようになった。総務省の調査では2017年当時で国内の14.1％

[2] 総務省によると、ＲＰＡはこれまで人間が行ってきた定型的なパソコン操作をソフトウェアのロボットにより自動化するものである。具体的には、ユーザー・インターフェース上の操作を認識する技術とワークフロー実行を組み合わせ、表計算ソフトやメールソフト、ＥＲＰ（基幹業務システム）など複数のアプリケーションを使用する業務プロセスをオートメーション化するものとされている（https://www.soumu.go.jp/menu_news/s-news/02tsushin02_04000043.html）。

の企業が導入済み、6.3％が導入中、19.1％が導入を検討中と回答し、当時の市場規模は31億円だったのに対し、2021年度には100億円規模になると予測していた[3, 4]。2021年度以降も中期的に成長は継続し、2023年度のＲＰＡ市場規模は事業者売上高ベースで1,520億円、そのうちＲＰＡツール製品は520億円、ＲＰＡ関連サービスが1,000億円まで拡大すると予測されている[5]。ＲＰＡは比較的低コストかつ短期間で導入できるという特長があることから、ＲＯＩ（投資収益率）に見合わないなどの観点からシステム化が見送られてきた領域でも活躍の機会がある。具体的な適用業務としては、帳簿入力や伝票作成、ダイレクトメールの発送業務、経費チェック、顧客データの管理、ＥＲＰ（Enterprise Resource Planning：統合基幹業務システム）、ＳＦＡ（Sales Force Automation：営業支援システム）へのデータ入力、定期的な情報収集など、主に事務職の人たちが携わる定型業務で生産性向上等の成果が出ていることが最近の総務省の調査で明らかになっている[6]。

## １－２．主な利用形態

ＲＰＡの利用範囲、利用方法はさまざまなケースやタイプがある。例えば、総務省が定義するＲＰＡには３つのタイプがある[7]。それによると、ＲＰＡには３段階の自動化レベルがあるとされ、現在のＲＰＡの多くは定型業務（クラス１）に対応しているとされている。次期レベルの「クラス２」は、ＡＩと連携して非定型業務でも一部は自動化されるもので、「クラス３」は、より高度なＡＩと連携することで、業務プロセスの分析や改善だけでなく意思決定までを自動化できるとされている。

ＲＰＡは、ツールの種類について、大きく「デスクトップ型」「サーバー型」「クラウド型」があり、どのツールを選択するかにより、統制の考え方、費用対効果、維持管理の難易度が変わる（図表１）。

**＜図表１＞ＲＰＡツールの種類（ｄ１チームまとめ）**

| | デスクトップ | サーバー | クラウド |
|---|---|---|---|
| **ツールのインストール** | ＰＣ端末 | 自社サーバー | SaaS |
| **主な特徴** | ・スモールスタート<br>・費用が低く抑えられる<br>・ＰＣ端末１つで手軽に始められる | ・１台で複数のロボットの稼働が可能<br>・自社サーバー内にＲＰＡを作成するため、情報漏えい等のセキュリティ対策が容易 | ・運用や保守の手間がかからない<br>・費用が低く抑えられる |

[3] 総務省「メールマガジン『M-ICTナウ』働き方改革：業務自動化による生産性向上」https://www.soumu.go.jp/menu_news/s-news/02tsushin02_04000043.html

[4] グローバルレベルで見ると、世界のＲＰＡ市場は飛躍的に成長し、ガートナー社の最新予測によると、世界のロボティック・プロセス・オートメーション（ＲＰＡ）ソフトウェアの売上は、2021年には18億ドルを超え、ＲＰＡ市場は2024年まで２桁の成長率を維持すると予想している。出典：Robotic Process Automation Revenue to Reach $2 Bn ¦ Press releases, Gartner, Sep. 21, 2021, https://www.gartner.com/en/newsroom/press-releases/2020-09-21-gartner-says-worldwide-robotic-process-automation-software-revenue-to-reach-nearly-2-billion-in-2021

[5] 株式会社矢野経済研究所プレスリリース「ＲＰＡ市場に関する調査を実施（2020年）」2020年12月７日、https://www.yano.co.jp/press-release/show/press_id/2599

[6] 総務省「メールマガジン『M-ICTナウ』」Vol.21、2018年５月第２号、ＩＣＴトピック「ＲＰＡ（働き方改革：業務自動化による生産性向上）」

[7] 総務省「情報通信統計データベース」、「ＲＰＡ（働き方改革：業務自動化による生産性向上）」https://www.soumu.go.jp/menu_news/s-news/02tsushin02_04000043.html

今回のケーススタディではクラス１の「定型業務」で「デスクトップ型」を利用したよくいわれる“スモールスタート”を前提とした。このツールを題材に取り上げた理由は、少ない投資で手軽にできるため、中小企業でも、また大企業の一部門でもよく見られる方式であると同時に、一度現場（１線）で導入されると、２線や３線からは見えにくい形式だからである。

### １－３．主なリスク

ＲＰＡの導入・開発・利活用におけるリスクとしては、主に以下のようなものがあげられる（図表２）。ただし、ＲＰＡの利用形態によって、想定リスクは大きく異なる。

特に、経理業務でＲＰＡを導入する場合は、財務報告に係る内部統制評価（以下、Ｊ－ＳＯＸ）上のリスクにも対応する必要がある。例えば、ロボットの処理実行結果を人が目視確認するケースと、ロボットの処理実行結果を人が確認しない（システムに近いような利用形態）ケースを比べると、後者の場合、ＲＰＡ仕様にコントロールが規定され、これが実装されているかを確認する必要がある。ある事業会社（以下、ケーススタディ会社）での実践例については第２章以降を参照されたい。

**＜図表２＞ＲＰＡ導入・利活用に係る主要なリスク（ｄ１チームまとめ）**

| 分類 | リスク事象 |
|---|---|
| **組織・戦略リスク** | 経営計画に準拠しない開発や導入 |
| | 費用対効果がない |
| | ＲＰＡ人材の不足 |
| | 災害時にロボット起動ができない（事業継続リスク） |
| | 導入・利活用に係る体制・職務権限の不備 |
| **オペレーショナルリスク** | 業務要件に合致しないロボット開発 |
| | 無秩序な開発 |
| | 設定ミス・処理の不具合の多発 |
| | 保守コストが多額 |
| | ロボット処理のブラックボックス化・“野良ロボット”化 |
| **セキュリティリスク** | 個人情報、機密情報の漏えい |
| | サイバー攻撃 |
| | 不正ログイン、ロボットの悪用 |

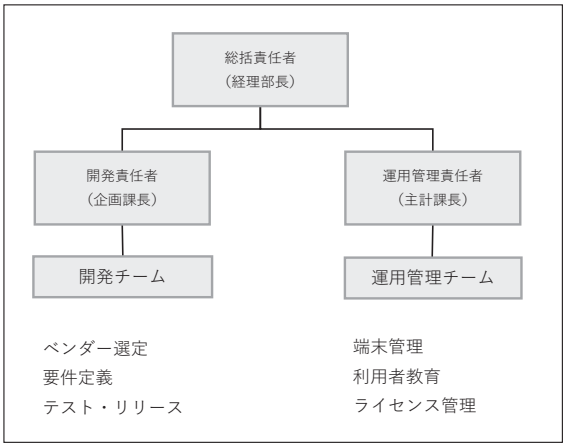
## ２．ケーススタディの紹介

ケーススタディ会社では、経理業務の生産性を向上するため、ＲＰＡを導入し、活用を始めることにした。経理部内にＲＰＡのツール選定、対象業務の要件定義、開発計画の策定、設計、実装・テストを行う担当を設け、運用体制は、以下のような体制を整備した（図表３）。

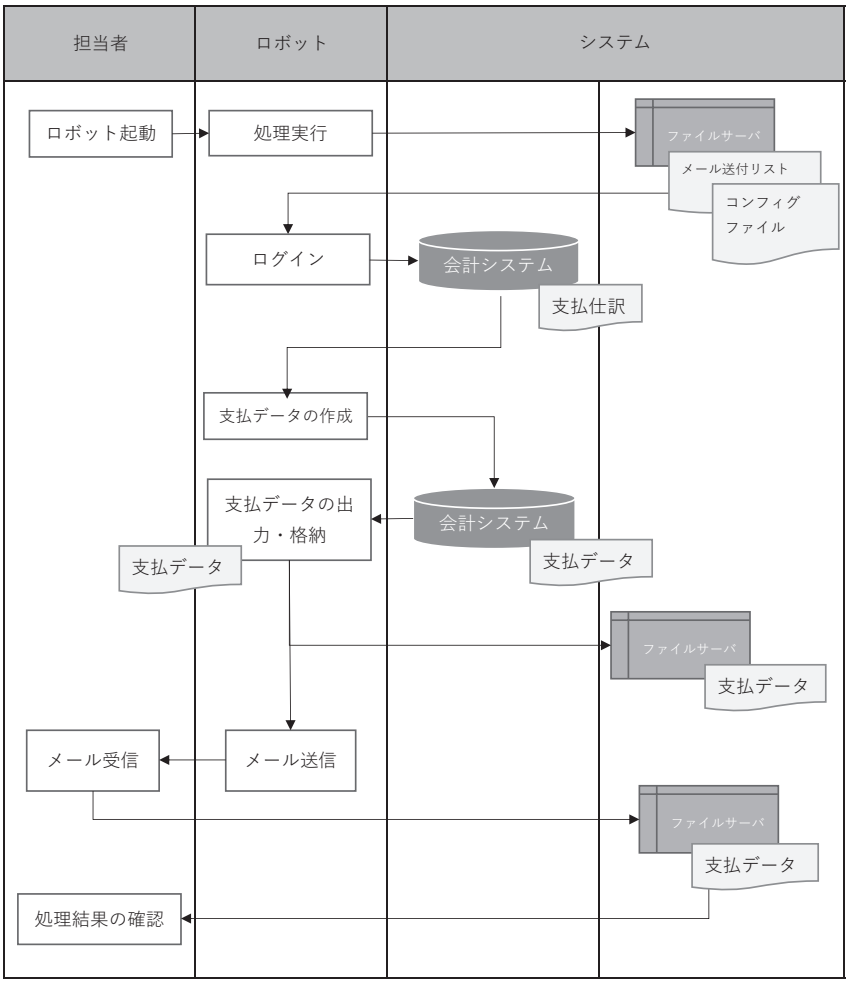
具体的なＲＰＡの活用範囲は、経理業務の中でも、債務管理、資金管理、固定資産管理の単純な入出力処理で活用することにした。例えば、これまで経理部員が作成していた支払データをＲＰＡ（支払データ作成ロボット）が作成する手順（シナリオ）を作成（図表４）し、以下のように実装した。

① 支払担当者がＲＰＡ専用端末上でＲＰＡツールを立ち上げて起動処理を行うと、あらかじめ組み込んだコマンド情報に基づき、支払データ作成ロボットが会計システムにログインする（見た目には支払

**＜図表３＞ＲＰＡの管理体制図と各担当での主な業務**



＜図表４＞支払データ作成におけるロボットのフロー図




担当者が何も操作せずにカーソルが動き出す)。

② 支払データ作成ロボットはログインした会計システム上で、「支払データの生成」ができるメニューに入り、処理ボタンを押下することで、支払データを生成する。

③ 支払データ作成ロボットはデータの生成が完了すると、サーバーの所定場所へダウンロードするボタンを押下する。支払データは自動で所定の場所へ格納される。

④ 上記の処理が完了すると、支払担当者に結果がメールで送付される。

このシナリオではメールを受け取った人間（支払担当者）が成果物をチェックする工程は別にある。ロボットの成果物を人の目を介さないでそのままファームバンキング上で後続処理するシナリオにすることも可能である。ロボットが作業だけをするのか、それとも、確認や承認（統制）までするのかにより、想定リスクが異なり、検討すべき内部統制も異なる。

ケーススタディ会社では、この経理業務ロボットの導入により、定量的効果として、ＲＯＩ（（ＲＰＡ化による定量効果―ＲＰＡ化費用）÷ＲＰＡ化費用×100％）が300％超えると試算し、業務時間の短縮による人件費削減ができるとの見通しをもった。また、定性的な効果としては、業務の自動化による人的ミスの削減、より付加価値の高い業務に要員をシフトできるなどの効果もあると見込んだ。

導入から１年が経過し、経理部長がＲＰＡの開発・運用管理活用状況を確認したところ、実はコンプライアンス部門や内部統制評価部署への相談もなくこのロボットが作られていたことや、ほかにも開発したロボットのほとんどが未稼働、もしくは想定通りに利用されていないことがわかった。

## ３．ＲＰＡの自己点検の実践

### ３－１．ＣＳＡの有用性・有効性

ＣＳＡはＲＰＡと相性が良いリスクマネジメントツールといえる。ＲＰＡはＥＵＣ（エンド・ユーザー・コンピューティング）と同

様、ユーザー部門での制度設計や運用が求められる一方、ＥＵＣよりもツールが多く、その扱いにはシステムの専門知識・スキルが求められることから、ＩＴリテラシーが低いユーザー部門だと、ＲＰＡナレッジが一部の人材に偏り、ＲＰＡがブラックボックス化する恐れがある。これを避けるには、「ＣＳＡ（自己点検)」を公制度化することである。ＣＳＡを組織の公式な制度にしておくことで、実効的なＲＰＡマネジメントができ、加えて、ＣＳＡをユーザー部門のナレッジ蓄積や引継ぎツールとしても活用できる。ユーザー部門が、そのＣＳＡの項目作成にあたっては、ＲＰＡの特性を踏まえるとともに、ＣＯＳＯ（Committee of Sponsoring Organizations of the Treadway Commission：トレッドウェイ委員会支援組織委員会）フレームワーク、ＩＳＯ27001（情報セキュリティマネジメントシステム)、ＣＯＢＩＴ（Control objectives for information and related technology）のようなグローバルなフレームワークに加えて、経済産業省の「システム監査基準」や「システム管理基準」等を参考にした。ケーススタディ会社での実践例については、第３－２節を参照されたい。

## ３－２．ＣＳＡの実践例

ケーススタディ会社では、２つのフォーマットを用いてＣＳＡを実施することにした。１つは、部内のＲＰＡの洗い出しをするための「現物調査票」（図表５）である。「現物調査票」は点検後、「ＲＰＡ管理台帳」として用いることを想定し、主な用途や管理者、ロボットの重要度を入力することにした。

ロボットの重要度を設定する目的は、最適な管理を行うためである。具体的には、重要性の高いロボットは開発から運用・保守までの管理は厳しくし、重要性の低いロボットは簡素にする。

重要度の判断基準としては、経理業務という特性上、Ｊ－ＳＯＸ対応を重視した。次に、個人情報保護規制（ＧＤＰＲ（一般データ保護規則)、個人情報保護法等）や不正競争防止法等のコンプライアンス対応が重要と考え、図表６のような重要度判断基準を整備した。重要性の判断基準の整備においては機密性、完全性、可用性の各観点でリスクを「最重要」「重要」「一般」等のレベル分けを行い、管理することが望ましいとされている[8]。ケーススタディ会社の図表１で示したロボットの場合、重要度は「Ｂランク：重要」に該当する。ＲＰＡの開発、利用、廃棄のライフサイ

**＜図表５＞現物調査票**

| # | 項目 | 仕様 | 仕様 | 仕様 |
|---|---|---|---|---|
| 1 | RPA製品名 | Uipath | Uipath | Uipath |
| 2 | 製品タイプ | デスクトップ型 | デスクトップ型 | デスクトップ型 |
| 3 | ロボットＩＤ | ロボットA | ロボットB | ロボットC |
| 4 | 主な用途 | 支払データ作成 | 固定資産台帳登録 | マスター登録 |
| 5 | 個人情報有無 | 個人情報　有 | 個人情報　有 | 個人情報　有 |
| 6 | 重要度 | | | |
| 7 | 開発者 | | | |
| 8 | 利用者 | | | |
| 9 | 運用管理者 | | | |
| 10 | 稼働年月 | | | |
| 11 | Ver. | | | |
| 12 | リリース日 | | | |
| 13 | 利用形態 | | | |
| 14 | 端末所有者 | | | |
| 15 | 接続ススステム名 | | | |
| 16 | 外部接続 | | | |
| 17 | リモート利用 | | | |
| 18 | 廃棄日 | | | |



[8] ＰｗＣあらた有限責任監査法人「ＲＰＡガバナンス構築のためのガイドライン（第２版)」第３章２（エ）ＲＰＡガバナンス構築「ロボットの重要度／リスク度合いの定義」

＜図表６＞重要度判断基準

| ランク | 定義 |
|---|---|
| Ａランク<br>最重要 | ・Ｊ－ＳＯＸ評価対象システムに接続し、ロボットによる処理が「重要な統制（キーコントロール）に該当する<br>・Ｊ－ＳＯＸ評価対象システムに接続し、ロボットの処理結果を人が確認していない（ロボットの正確性がそのまま業務の正確性になる） |
| Ｂランク<br>重要 | ・ロボット専用ＩＤを利用してロボットを実行している<br>・個人情報や機密情報を含むデータを取り扱っている<br>・ロボットが止まると人がリカバリーできない、決算遅延を招きかねない |
| Ｃランク<br>一般 | ・上記に属さない |

クルは早く、改廃やプログラムの変更も多いため、開発者や利用者、Version管理の情報も入れるようにした。

２つ目は「自己点検チェックリスト」（図表７）である。これはＲＰＡのライフサイクル（企画・導入、開発、運用、保守）に沿ってオペレーショナルリスクへの対応を中心に検証できるようにした。自己点検チェックリストの作成に際しては、ＰｗＣあらた有限責任監査法人「ＲＰＡガバナンス構築のためのガイドライン（第２版)」のAppendix１「ＲＰＡ関連リスクとコントロールのポイント」が参考になる。

ケーススタディ会社での実践例では、開発・導入時にリスク評価を実施していなかったことや、自然災害や機器故障等の障害対応、セキュリティ面で「×（未実施)」が多いことがわかった。

オフサイト（書面）による点検実施後に、気になる点について、インタビューや現物を確認した。ケーススタディ会社のインタビューでは以下のようなことも把握できた。

① ＲＰＡ導入決裁書と異なる運用であった。決裁時、本来開発したシナリオを使えば導入後３年間で数億円のコスト削減効果があると記載されていたが、実際にはＲＰＡは利用されていなかった。未使用の理由はＲＰＡを使うと作業が遅いということであった。また、接続先の会計システムの仕様変更により、ロボットが異常終了することや、ログインすらできないケースもあり、利用しなくなったケースも多かった。

② 開発リスクや開発目的、使用する資源、開発期間、効果等を明示した開発依頼書はなかった。

③ ＲＰＡは開発用ＰＣと運用用ＰＣがあり、それぞれ端末用の共有ＩＤで動かすことができる。ロボットを使用しない者も運用用実機のＩＤとパスワードを知っている状態であった。

④ 開発用のＩＤは外部委託先に貸与されており、そのＩＤを利用すれば、社内のネットワーク、会計システムにアクセスすることが可能であった。

⑤ 作業しかしないＲＰＡに承認権限まで付与していた。

⑥ ＲＰＡソフトウェアの脆弱性情報は入手していなかった。

⑦ ＲＰＡソフトウェアの操作ログは分析していなかった。

⑧ リモートデスクトップの機能を使い、遠隔地で操作ができることがわかった。

⑨ ＢＣＰがなかった。

⑩ 開発用のＰＣのローカルディスクには機密情報が多数残されていた。シナリオを実装するときに使ったデータとのことであった。

＜図表７＞自己点検チェックリストの一部事例

| No. | 大項目 | 中項目 | 小項目 | 評価ポイント | 点検結果 |
|---|---|---|---|---|---|
| 1 | プロセス | 開発・利用部門の役割・責任 | 職務分離 | ロボットを開発する人、リリースを行う運用管理者、利用する人を分離しているか | × |
| 2 | プロセス | 開発・利用部門の役割・責任 | 外部委託先の選定 | ロボットの開発、運用、保守が自前でできていない場合、外部委託先を選定し、契約内容には運用支援や保守に関する仕様が明示されているか | ○ |
| 3 | プロセス | リスク評価 | ロボットのランク付け | ロボットの導入時に、業務の重要性やロボット停止時の影響度、取り扱うデータ（個人情報、マイナンバー、顧客情報）の機密性等に応じてロボットをランク付けし、重要性に応じて管理する仕組みはあるか | × |
| 4 | プロセス | リスク評価 | 関係部署への相談・リスクチェック | ロボットを開発する前に、個人情報保護法等の法令、内部統制、コンプライアンスに関係する業務かについて関係部署による以下のチェックを受けているか<br>・業務オーナー及びシステム所管部署への説明、相談、承認<br>・コンプライアンス部門、内部監査部門への確認 | × |
| 5 | プロセス | リスク評価 | 関係部署への相談・リスクチェック | ロボットの操作に影響を与えることがないように、接続するシステム側の管理部門と当該システムの変更等の内容について確認する場を設けているか | × |
| 6 | プロセス | リスク評価 | 関係部署への相談・リスクチェック | ロボット開発を行う際に、ロボットが操作する情報システムへのアクセス数や通信の発生等のネットワークインフラへの影響を評価し、検討結果を記録しているか | × |
| 7 | プロセス | 選定・導入 | ツール要求事項 | 現在使用しているＲＰＡツールには、将来的なＤＸ対応を考慮し、ＯＣＲやＡＩとの連携機能が付与していることを確認しているか | ○ |
| 8 | プロセス | 選定・導入 | ツール要求事項 | 利用しているＲＰＡツールの脆弱性情報、セキュリティパッチは定期的に提供されているか。それらを確認する社内担当者をアサインしているか | × |
| 9 | プロセス | 選定・導入 | 計画 | デスクトップ型のスモールスタートの場合、将来的な利用拡大計画が検討され、機能面、リスク、コストに関して経営層の説明や合意は受けているか | ○ |
| 10 | プロセス | 選定・導入 | 開発手順 | ロボットを新たに企画する場合の手順は文書化しているか（要件検討、有識者の確認、開発工程の明確化、成果物明確化等） | × |

## ４．ＣＳＡを踏まえたリスク評価の実践

### ４－１．リスクの洗い出し・評価

ケーススタディ会社の場合、経理部門の業務内容や組織特性を踏まえ、図表８に示すリスク評価基準（影響度・発生可能性）に基づき、ＲＰＡリスクを把握することにした。

### ４－２．リスク評価結果

ＣＳＡに基づくリスク評価結果は図表９のように整理した。会計システムにログインで

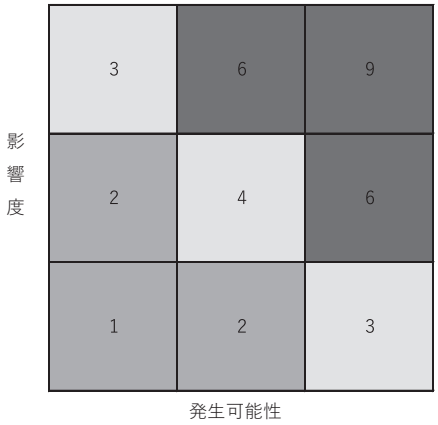
＜図表８＞リスク評価基準

**影響度：**

| レベル | 説明 |
|---|---|
| 大 | 報道等により、企業ブランドを傷つける<br>社外に対する損害賠償が発生する |
| 中 | 損害賠償はないものの、部内の経費予算を超える支出が発生 |
| 小 | 上記以外。開発、運用保守経費の無駄の発生、作業生産性の悪化が生じている |

**発生可能性：**

| レベル | 説明 |
|---|---|
| 大 | リスクがすでに顕在化 |
| 中 | ３年以内にリスクが顕在化すると予測 |
| 小 | ３年超えて発生するか、発生する見込みがない |




＜図表９＞リスク評価結果サマリー

| リスク | 影響度 | 発生可能性 | 重要度 |
|---|---|---|---|
| 経営資源を無駄に利用しているリスク | 1 | 3 | 3 |
| 無断開発により、接続側のシステムが誤作動するリスク | 3 | 2 | 6 |
| ＰＲＡのＩＤを使い、業務処理をする、情報を不正に盗み出す、漏えいする、不正利用するリスク | 3 | 2 | 6 |
| 開発ＩＤで本番データを滅失や破壊するリスク | 3 | 2 | 6 |
| 情報漏えいやデータ持ち出しがあっても特定できないリスク | 3 | 2 | 6 |
| ソフトウェアを攻撃したウイルス感染 | 1 | 2 | 2 |
| 外部委託先からの不正アクセス | 3 | 1 | 3 |
| 自然災害トラブル、ネットワーク障害、ＲＰＡの故障等で利用ができなくなり、業務遂行ができなくなるリスク | 1 | 1 | 1 |

きてしまうことに対して、内部統制評価を行う部署、情報システム部門、コンプライアンス部門に相談をしていなかったためにロボットを通じて財務情報の不正取得ができることや、ロボットＩＤの共用等による不正や経理処理の誤謬のリスクが高いということを踏まえて重要度を判断した。

## ５．ＣＳＡを踏まえたＲＰＡコントロールルールの作成・運用

### ５－１．システム部門との連携

ＲＰＡは１線であるユーザー所管とはいうものの、実態はシステム開発や運用保守管理に近く、システム部門との連携が重要である。例えば、ロボット側の処理が接続先の本番システムに接続、処理することで、トラフィック量が増え、想定外の負荷を与え、システムがダウンすることもある。そのため、ＲＰＡツールの種類、接続方法や環境等をあらかじめシステム部門に相談し、当該システム部門が有する開発標準に基づき、開発を行う必要がある。とはいえ、システム開発標準をそのまま準用することは、アジャイル開発が強みのＲＰＡには負荷が高すぎる懸念もある。ケーススタディ会社では、第５－２節で示すようなポイントで、ルールを整備することとした。

### ５－２．全般のポイント

#### （１）管理体制と手順の整備

ＲＰＡを適正に管理するために推進責任者や担当者の配置等の体制が必要である。ケーススタディ会社の場合においても、前述のＣＳＡの結果、責任者やチームの組成は漠然とできていたものの、ＲＰＡの実装経験のある者が限られ、開発と運用の職務分離ができていなかったことが浮き彫りになっていた（図表７）。また、スモールスタートやアジェイル志向を重視し、開発申請やテスト・リリースの承認記録に係るルールがなかったため、１線と２線が協働し、ＲＰＡ開発・運用に係る管理体制や手順を文書化することとした。

図表10は新たに作成した「ＲＰＡ管理ポリシー兼ルールブック」の目次構成である。ＲＰＡは通常のシステムとは異なるものの、通常のシステムと同様のルールを設定しないと、管理できないこともわかった。ただし、後続で触れるように、それぞれの管理項目において、ＲＰＡの重要度に応じて、濃淡をつけることがポイントになる。

## ５－３．導入計画・開発ルールのポイント

### （１）導入計画

導入企画から実装まで１線内で完結してしまうと組織全体としてはブラックボックスになりやすいため、短期・中長期導入計画の策定やＲＰＡツールやベンダーの選定時における“リスク評価手続”において２線が適切に支援、関与する仕組みが必要である。

稟議時に費用対効果の目標やその測定方法を定めないと、あとで検証ができないという論点はシステム開発と同じである。ＲＰＡの場合、ＲＯＩや投資回収期間が指標として利用されているが、ＲＯＩを設定したところで、ＲＰＡの場合、300％という数値を見ることも多分にあり、適正な目安を設定できない懸念がある。ケーススタディ会社では、一定金額以下の投資の場合には、投資回収ではなく、人為的ミスの削減数等の定性的な効果による検証を行うルール設定とした。

一方、悩ましいのはテストやリリース承認手順である。ＲＰＡはプログラム言語不要のツールで、システム開発経験がなくても実装できるものの、プログラムであることに変わりはないため、一定の開発テストが必要である。テストをどこまで行うかはシステムと同様、検討が必要となる。重厚なテストにしすぎないように、ロボットの重要度でメリハリをつけ、ロボットが仕様通りに動作すること（ブラックボックステスト）や、セキュリティ上の違反がないことを確認する程度のテ

**＜図表10＞ケーススタディ会社における「ＲＰＡ管理ポリシー兼ルールブック」の目次構成**

| No. | 目次 | 主な規定内容・ポイント |
|---|---|---|
| 1 | ガイドラインの目的 | |
| 2 | 準拠規程 | 情報管理やシステム管理系の手順との相互関係 |
| 3 | 適用範囲 | ＲＰＡツールの種類や内部利用範囲 |
| 4 | 用語の定義 | ＲＰＡ、ロボット、端末、デスクトップ型、サーバー型、クラウド型等の言葉の定義 |
| 5 | 推進・管理体制 | 総括、開発、運用の各責任者、担当者、機能 |
| 6 | ロボットの重要度 | 図表６参照 |
| 7 | 外部委託先の管理 | 開発保守ベンダーの選定、契約管理 |
| 8 | 導入 | 導入計画、企画稟議、開発承認、関連部署への相談、テスト・リリース |
| 9 | 運用管理 | 手順書・フローの管理、ライセンス管理 |
| 10 | セキュリティ管理 | 端末管理、ＩＤ管理、アクセス管理 |
| 11 | 廃止 | 廃止手続 |
| 12 | 異常対応・ＢＣＰ | 障害対応、トラブル対応 |
| 13 | モニタリング | ＲＰＡの棚卸、ＣＳＡ |
| 14 | 手順の管理 | |

スト項目とするとともに、重要性の低いロボットはテストの詳細計画、実施までは必須としない等の管理の濃淡をつけたルール設定とした。

## ５－４．保守・運用ルールのポイント

### （1）ＩＤ管理

ロボットの利用形態で、個人ＩＤでロボットを利用するか、ロボット専用ＩＤで利用するかにより、そのリスクは異なるのは前述の通りである。特にスモールスタート会社の場合、ＲＰＡツールの利用ライセンスを限定することから、ロボット専用ＩＤを共用するケースがある。ケーススタディ会社においても、ＲＰＡソフトウェアをインストールした端末に専用ＩＤを持たせるものの、利用者がそのＩＤを“共用”する形態であった。デスクトップ型でロボット専用ＩＤを付与して利用しているケースは、ほとんどがこのＩＤ共有をすることになる。この場合、操作ログをみても、そもそものＲＰＡ利用者を特定できない。ＲＰＡの簡易性と内部統制との間でどうバランスをとるかが難しい。ケーススタディ会社では、ＲＰＡを利用できる担当者を絞ることで共用によるリスクを抑える方法とした。

### （2）アクセスコントロール

ロボットはデジタルレイバーであり、従業員と同様である。よって、任された職務に応じてアクセス権を付与する必要がある。ケーススタディ会社ではＲＰＡは図表４の通り、作業者レベルの処理でしか利用しないため、承認権限を付与する必要はないにもかかわらず、第３－２節で示したように、ロボット専用ＩＤに承認権限を付与していた。この場合、ロボットに過剰な権限を付与してあるので、承認権限を有しない個人ユーザーがロボット専用ＩＤを利用し、本来は行うべきでない処理プロセスを行うリスクが内在することになる。ケーススタディ会社では、ロボット専用ＩＤによる作業ログの収集と分析により、ロボットの処理内容の妥当性を事後的にモニターするルール設定とした。

### （3）ロボット端末の現物管理

ＰＣ１つでロボットが生成できるため、端末の管理が重要である点については、通常のＰＣ管理とは変わらない。ケーススタディ会社においては、開発用の端末と運用の端末を分けており、特に、開発用の端末は外部委託先に貸与し、ＲＰＡの実装、会計システムの開発環境にログインし、テスト等を委託していたため、アクセス権の設定が重要なポイントであった。運用端末は夜間作業を行うこともあるため、施錠したボックスに格納し、セキュリティエリアで利用することにした。

## ５－５．廃止ルールのポイント

会計システムに接続している未稼働のロボットや、システム側の仕様変更で利用できなくなったロボット等、ロボットの停止・廃棄を適正に管理しないと、“野良ロボット”が増殖する要因になるため、その廃止手続きをあらかじめ定めておくことも有用である。管理手法としては、ロボットの操作ログを取得し、ロボットの稼働率をモニターし、稼働がないロボットを強制的に廃止登録する方法や、業務の見直しやプロセス変更と合わせてロボットの改廃の要否判断を行うことをルール化し、廃止に該当すれば台帳登録する等、廃棄予定ロボットの把握・検出ルールを設定した。

## ５－６．その他課題と留意点

ロボットは人間と異なり、定型業務の場合は抜け・漏れ等の処理ミスが出ることはないものの、自然災害時やサイバーテロ等のアクシデントによる異常停止はありうるため、ＢＣＰの検討も重要になる。また、“野良ロボット”防止のためにも文書（ＲＰＡの業務フローやテスト記録、仕様書）は必要であるが、

あまり厳格にルール化してしまうとＲＰＡの良さが生かせないジレンマもある。ケーススタディ会社では、文書化をどこまで行うのか、リリース承認記録をどこまで求めるかにつき、画一的な基準が整備できず、運用管理者と開発管理者の合議で決め、あとはＣＳＡやモニタリングで運用をみて改善要否を判断するという運用でカバーすることにした。

このほか、ＲＰＡ製品は日々技術が進化し、製品が多様化し、ライセンス契約の見直しも多い。また、接続元のシステム改修の都度、ロボットの異常停止も増え、その都度、人手による処理がある。ソフトウェアのバージョンアップテストもユーザー側で対応しなければならないため、ユーザー部門にＩＴリテラシーのある要員の確保は必要である。

デジタルレイバーの管理者がいなければ、結局は未稼働や“野良ロボット”化が進むリスクは大きいことを実感することになる。

## ６．今後の展開

### ６－１．ＲＰＡの内部統制評価及び内部監査

前章までに、１線（ユーザー部門）と２線（主にシステム部門）が協働で、コントロール及びルール設計を行うポイントについて紹介した。本章では、実効性のあるＲＰＡガバナンスの構築において、ＣＳＡやリスク評価の結果に基づくコントロールの整備・運用を客観的に評価・監査する３線による内部監査について提言したい。

ケーススタディ会社においては、後述する１線からの申告がない限り、監査部門がＲＰＡの利用状況を把握できなかったのが実態である。現場のＲＰＡの利用状況を適時に監査部門が把握する仕組みを構築することが最初の課題ではないだろうか。

Ｊ－ＳＯＸの一環でシステム調査を制度化している場合、その中でＲＰＡについてもアンケートしているケースも見られる。ただし、後述の通り、Ｊ－ＳＯＸ制度では重要プロセスベースで評価対象範囲を判断するため、ＲＰＡが重要プロセスに組み込まれていない限り、監査部門がリスク感度を持ってＲＰＡリスクを検証することはほとんどない。

ケーススタディ会社ではＲＰＡに限らず、経理ＤＸを加速度的に進めているため、定期的に１線、２線（情報システム部）、３線（監査部）でテクノロジー情報交換会を開催し、実装予定のテクノロジーとそのリスクについて情報交換していた。監査部門はこの場面でＲＰＡリスクを把握し、監査テーマに取り上げることになった。ケーススタディ会社で実践した監査の着眼点は第６－３節を参照されたい。

### ６－２．Ｊ－ＳＯＸ対応

一般的に、経理部門でのＲＰＡ利用はＪ－ＳＯＸにも影響すると見られる。影響度の判断のポイントは２点ある。１つ目は、ＲＰＡによる処理が“重要な統制”かどうかである[9]。例えば、ロボットは会計システムに自動ログインし、人を介在せずに会計システム上で処理を行うが、処理結果は人が見ている場合、ロボットの処理そのものが重要な統制にはなりえず、影響度は低いと見る。２つ目は、重要なプロセスに関与しているかどうかである。売上・売掛金・棚卸資産の３勘定に関連する会計処理でＲＰＡが利用されていない場合や、決算ＰＬＣと呼ばれる引当金等の判断や計上プロセスにＲＰＡが活用されていない場合も、影響度は低いと見る。業務プロセスに係る内部統制に影響しないのであれば、Ｉ

[9] ＰｗＣあらた有限責任監査法人「ＲＰＡガバナンス構築のためのガイドライン（第２版）」第４章３にある「図17 ＳＯＸ対応検討フロー（例）」は、ＲＰＡ導入におけるＳＯＸ影響度を判断するうえで参考になる。

Ｔ全般統制（ＩＴＧＣ）の評価範囲にも含まれないとの見方になるため、ＲＰＡのプログラム変更管理、インフラ管理、アクセス管理、運用管理等のＩＴ統制に係る論点はＪ－ＳＯＸの評価対象外という整理になる。

一方で経理業務や決算実務でＲＰＡを利用している限り、全社的内部統制、全社的な観点から評価を受けることが適切な決算財務報告プロセスに対応した内部統制を実装すべきとの会計監査人やコンサルタントもいる。ケーススタディ会社においては、監査法人との協議において、会計システムに接続し、自動処理を行うＲＰＡについて、ＩＴＧＣの評価項目に準じて評価を行うこととし、第５章で記載したようなＩＤ管理やアクセスコントロール、開発・変更管理等の整備・運用状況を評価することにした。

## ６－３．内部監査の着眼点

ＮＰＯ法人日本システム監査人協会発行の『情報システム監査実践マニュアル』によれば、ＲＰＡの特徴として、「部門が個別で導入を進め、組織として統制がとりづらくなる点」、「業務整理を行わないまま開発着手し、業務シナリオが属人化する弊害」、「接続する周辺アプリケーションの環境変化により異常停止するリスク」、「要員の異動によりＲＰＡがブラックボックス化する恐れ」の４点をあげている。これらを踏まえ、ＲＰＡにおけるＩＴガバナンス（戦略方針、組織体制、役割など）を確認するとともに、ＲＰＡの監査ポイントを「企画フェーズ」「開発フェーズ」「運用・利用フェーズ」「保守フェーズ」「事業継続管理」「人的資源管理」の６分野でまとめている。どのポイントもシステム監査の観点と大差がない。

多くの内部監査組織では業務監査とシステム監査を分ける傾向が強く、システム監査側からすれば、ＲＰＡはＥＵＣと変わらないという考え方で、業務側で見るべきと整理しているところもあれば、業務監査側としては、ＲＰＡはシステムだと認識し、評価対象外とし、ＲＰＡ管理がシステム監査と業務監査双方の間で論点漏れとなる懸念がある。

ここで、ケーススタディ会社における監査対応例を紹介したい。業務監査とシステム監査を合わせた“テーマ監査”として取り組むこととし、ＣＳＡの結果と監査部門でのリスク評価を踏まえ、３つのテーマを重点として設定することにした。

１つは、利用されていないＲＰＡについて、投資回収できない“減損リスク”について検証することとした。監査プログラムの主な着眼点としては、開発稟議や導入決裁時の意思決定の適切性、効果の測定方法の明確化と測定の有無、効果が出ていない場合の原因分析の妥当性や改善着手状況とした。

２つ目は、セキュリティリスク対応である。監査プログラムの主な着眼点としては、在宅勤務に対応したリモートによるロボット操作等も踏まえたネットワーク管理や、ロボットＩＤによるアクセスログや作業ログの収集分析状況について精査することとした。

３つ目は、ＲＰＡ実装の最大の目的となる業務の効率性・生産性の向上についてである。監査プログラムの主な着眼点としては、ロボット稼働率と、導入効果の測定（経理要員の残業時間の削減）・モニタリングの妥当性と、ミス・ロス等の業務の正確性指標とのバランス、余剰になった人員や時間の活用の適切性を検証することとした。

このほかにも、開発と運用の職務分離等の管理体制に関するテーマ設定や、ベンダー選定や保守委託等の外部委託先管理や契約管理、ライセンス管理、ＲＰＡ人材の要員確保、研修等も着手すべき論点になりうる。他の監査テーマと同様、ＣＳＡ結果や監査部門でのリスク評価を踏まえた上で、定期的に行うことが必要と考えられる。

## おわりに（実効性のあるＲＰＡガバナンスとは）

ＣＳＡケーススタディを踏まえ、当研究会で、実効性のあるＲＰＡガバナンスについて必要になることは以下の３つの条件だと考えている。

１．ＲＰＡの理解促進
２．ＲＰＡがもたらす“処理の自動化”に対する組織リスク許容度の醸成と共有
３．２線、３線の適正な牽制

１．の「ＲＰＡの理解促進」については、現場やユーザー部門、いわゆる１線でＲＰＡの活用が急拡大の一方で、２線、３線でのＲＰＡツールの理解度は進んでおらず、システムの一部だと思っている監査人も多いのではないか。ＲＰＡツールは急速に進化し、自社の組織やプロセスに実装されているため、監査側もＣＳＡを利用して、自社のＲＰＡ棚卸状況を把握し、その概要や用途等を把握することが求められる。

２．の「ＲＰＡがもたらす“処理の自動化”に対する組織リスク許容度の醸成と共有」とは、１．に関連するものであるが、“自動化”がもたらすリスクシナリオは多種多様である。ＣＳＡを通じてＲＰＡの棚卸が完了し、実態を把握すると、「人を介しない自動処理で本当に大丈夫なのか」「不正利用される懸念はないのか」等、“自動化”がもたらす効用よりもリスクを過大評価することもある。結果として、ＲＰＡの実装を阻害し、享受できるメリットも少なくなる。ＲＰＡの最大の期待効果は生産性の向上であり、多くの場合、管理手続きの省力化が争点になるなど、内部統制の実装と利益相反する場面が多い。このようなケースにおいて、生産性と統制のバランスをみて、リスク対応案の優先順位をつけ、統制を実装できるようになるのは短期的な取り組みや座学では難しい。組織のリスク許容度、リスクカルチャーも影響する。定期的なＣＳＡを繰り返し行い、結果を蓄積することで、ＲＰＡの固有リスク、統制リスクを把握し、それらのリスクに濃淡をつけ、その時々に応じて合理的なリスク対応案を設定していくことが必要だと考える。

最後に３．の「２線、３線の適正な牽制」については、１線のＣＳＡはあくまで自己点検であるため、バイアスがかかることが多い。２線、３線が本来の役割に基づき、１線の内部統制の整備、運用に積極的に関与し、自己点検結果を利用した内部統制の見直しや高度化を推進する機能があってこそ、１線のＣＳＡに適度な緊張感が生じ、正確で客観的な事実把握（リスクとコントロールの把握）につながる。ＲＰＡに限らず、ＣＳＡの推進と有効化には、２線、３線の適正な牽制が極めて重要となる。

**＜ＣＩＡフォーラム研究会No.ｄ１（ＣＳＡの事例研究会）メンバー＞**

（五十音順・敬称略）

| 氏名 | 勤務先・所属 |
|---|---|
| 斎藤　淳一（座長） | ホウライ株式会社 |
| 伊東　映仁 | 元 独立行政法人農業・食品産業技術研究機構 |
| 鈴木　茂臣 | 元 住友商事株式会社 |
| 谷口　英明 | シミックホールディングス株式会社 |
| 廣兼　玲子 | |

（メンバーの氏名、勤務先・所属は、2024年７月現在）