RPAガバナンスの重要性と構築のポイント

新型コロナウイルス感染症（COVID-19）の影響下においても、RPA（Robotic Process Automation）は重要なテクノロジーとみなされています。本稿では、今後ニューノーマルが形成される中でも、企業にとってより欠かせないテクノロジーとなっていくであろうRPAについて、固有のリスクと顕在化した場合に発生し得る問題、またそれらに対応するためのガバナンス構築について、ポイントを挙げながら解説します。

1. RPA導入の動向

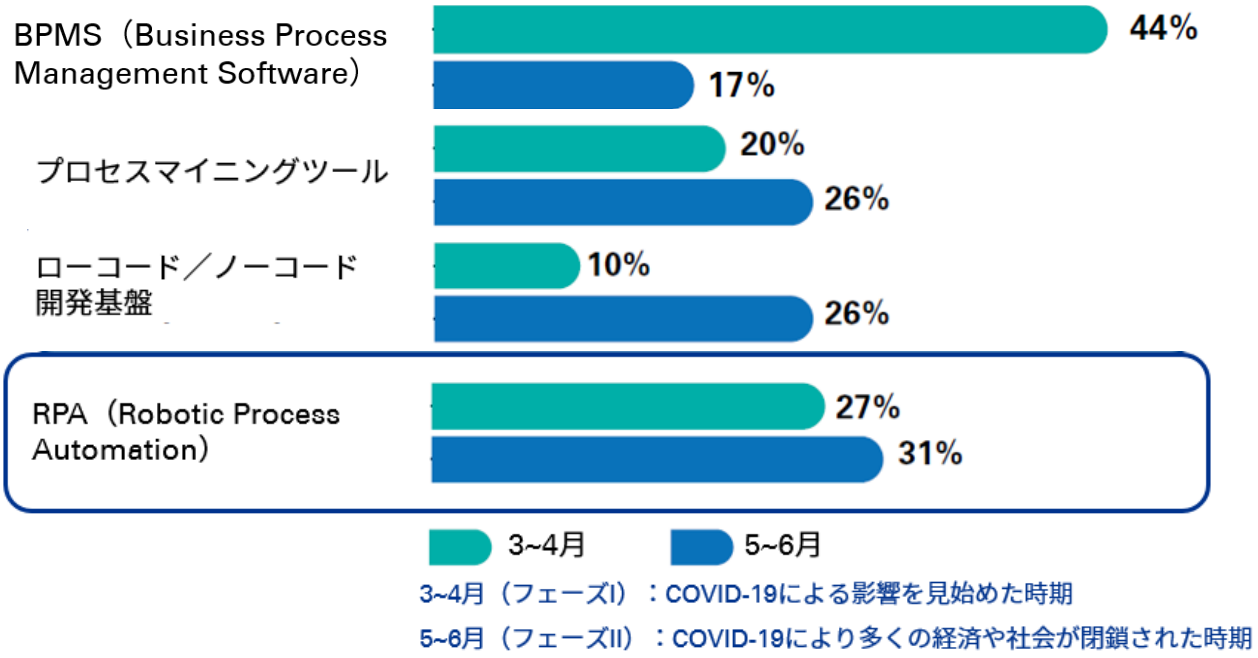
昨今のCOVID-19感染の拡大に対して、多くの金融機関がテクノロジーを用いて人・場所に依存しない業務環境の構築に取り組み、ビジネスの維持・継続に努めています。このテクノロジー活用の流れは一過性のものではなく、COVID-19が終息した社会においても、ニューノーマル（新常態）を形成していくものと予想されます。

RPAは、従前より大手金融機関を中心に導入が進んでいる代表的なテクノロジーであり、経理業務や審査業務等さまざまに活用されています（図表1参照）。また、金融庁が2020年6月に公開した「金融機関のITガバナンス等に関する調査結果レポート」によると、地域銀行においても、RPAを導入済である銀行が70%を超える結果となっています。さらに、KPMGとHFS Researchが実施した調査レポート「2020 Global Emerging Technology Survey Report」によると、グローバル企業において、COVID-19による経済や社会への影響が出始めた2020年5月から6月においても、RPAは引き続き「重要な自動化投資」として考えられていたことがわかります（図表2参照）。これらのことからも、金融機関におけるRPAの導入は今後も維持・拡大することが想定されます。

【図表1　RPAのユースケース例】

利用業務／ 成果（例）	実施処理（例）
住宅ローン申込書作成・登録 1件当たりの処理時間を70分から15分へ削減	✓OCRによる情報読み取り （住民票や重要事項説明書等の添付資料をテキスト化） ✓読み取り情報の申込書への転記 ✓申込内容のシステムへの転記
アンチ・マネーロンダリング（AML） 審査プロセスの合理化	✓顧客・取引先データの収集 ✓収集したデータの審査システムへのアップデート
会計伝票の起票および照合業務 プロセス全体の70%を自動化	✓証憑データのメール受領 ✓計上用データの作成 ✓会計システムへの転記 ✓承認者への計上申請

【図表2　コロナ影響下における最も重要な自動化投資先】



出典：「2020 Global Emerging Technology Survey Report」を基にKPMG作成

2. RPA固有のリスク

RPAの導入により、業務の効率化や品質向上を実現できる一方で、固有のリスクが生じます（図表3参照）。
例えば、人が使用するIDとは別にロボット専用のIDを作成した場合、ロボット専用のIDの管理が疎かとなり、IDが不正に使用されてしまう可能性があります。その際、RPAのログ取得の設定が不足している等の原因で、後から不正な操作をした人物の特定が困難になることも想定されます。
また、RPA導入の目的の1つとして業務の自動化がありますが、導入後に当該業務を手作業で実施する機会が減ることや、担当者の異動時の引継ぎ漏れ等により、自動化以前の業務がブラックボックス化する可能性があります。
さらに、RPAによる業務の自動化により要員配置を変更した場合、RPAによる処理が何らかの理由で完了しなかった際に要員の知識不足もしくはパワー不足により、適切な対応が行えず、業務が滞る可能性も考えられます。
RPAを全組織に展開していく際は、既存のIT統制の目線でのみ考えず、これらのRPA固有のリスクに対処するための仕組みを整備することが重要となります。

【図表3　RPA固有のリスク例】

リスク	内容
誤処理	ロボットによる処理操作の誤りにより、間違った結果となるリスク。OCRでテキストの読み取りを行うような場合は、特に留意が必要となる。
ブラックボックス化	RPA導入に伴い、既存の業務内容が暗黙知となるリスク。
職務分掌の不遵守	IDの発行者と承認者が分離されない等、本来あるべき職務分掌が徹底されない状況となるリスク。
野良ロボットの発生	未把握のロボットが作成され、セキュリティホールとなるリスク。現場主導でRPAを導入する際にはより注意を要する。
既存統制無効化	ロボットが既存の統制を無効化するリスク。
ロボットIDの悪用	ロボットのIDが不正利用され、外部攻撃・内部不正に繋がるリスク。
処理の未遂	ロボットによる処理が完了せず、業務が未完了となる、または停止するリスク。

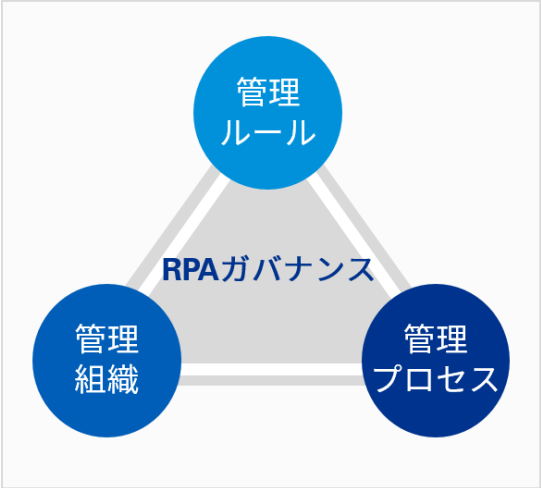
3. RPAガバナンスの重要性

RPA固有のリスクに対処するための仕組みを整備しないままRPAの展開を進めた場合、先に挙げたRPA固有のリスクが顕在化しやすくなる他にも、RPAの導入で逆に非効率となるような問題や、コンプライアンスに係る問題が発生する可能性があります。例えば、RPAを導入する際に全社で共通して取得するべきログを定める等、RPAの開発規約類を規定していないことで、開発後に取得が必要なログが判明し、修正のための手戻りが発生するといった問題が起こる可能性があります。また、RPAを導入してよい対象業務を定めていなかったことにより、個人情報を扱うRPAでIDを不正に利用し個人情報を持ち出すような、コンプライアンスに係る問題が発生することも考えられます。

RPA固有のリスクを確実にコントロールしていくためには、RPA固有のリスクに対処するためのガバナンスの整備が重要となります。RPAガバナンスでは、管理ルール、管理組織、管理プロセスの3つの要素が必要と考えます（図表4参照）。 RPA固有のリスクに対応したガバナンスを整備するためには、これら3つの要素について、RPA固有のリスクに対処するための見直しを行う必要があります。

ガバナンスに必要な3つの要素

【図表4　RPAのガバナンスに必要な3要素】



管理ルール	RPA固有のリスクへのコントロールを考慮した、全社で守るべき 規定（統制）の整備
管理組織	RPAの実質的な管理部門や統括部門の設定／決定および役割（職掌）整備
管理プロセス	全体管理・最適化を考慮した、各種管理プロセス（フロー）の具体化および管理の枠組み整備

まず1点目は、「管理ルール」です。全社的なRPAの取扱いを規定することで、野良ロボットの抑止、ロボット用IDの適切な設定や管理、想定外の業務へのRPAの適用禁止等が期待できます。
2点目は、「管理組織」です。実質的な管理部門や全社的な統括部門を決定し、各部のRPA導入に対する相談窓口や管理ルール・管理プロセス整備を所管する組織を決定する必要があります。
そして3点目は、「管理プロセス」です。RPAの台帳整備・棚卸や、RPA固有のリスク評価等、管理ルールの目的を実現するための具体的なプロセスを定める必要があります。
なお、公益財団法人　金融情報システムセンター（FISC：The Center for Financial Industry Information Systems）発行の「RPA導入にあたっての解説書」では、RPAに係る問題点とその対応策が解説されており、RPAガバナンスの整備事項を整理するうえで参考になります。
RPAは、業務担当者による利用が比較的容易であり、組織に一度導入されれば加速度的に利用が拡大することが想定されるため、RPAの全社展開を見据えて、なるべく早い段階でRPA固有のリスクに対応したRPAガバナンスを整備しておくことが重要になります。

4. RPAガバナンス整備のポイント

RPA固有のリスクに対応したRPAガバナンスを整備するにあたり、考慮すべきポイントとして、以下の3点が挙げられます。

ポイント（1）導入対象製品

導入対象となる製品が、サーバ上で稼働する（いわゆる“サーバ型”）か、利用者のPC端末上で稼働する（いわゆる”デスクトップ型”）かによって、統制が変わる可能性があります。例えば、サーバ型のRPAであればシステム部門が所管するIT統制に馴染みやすく、デスクトップ型のRPAであれば各部が所管するEUC統制に馴染みやすい等、組織の既存の統制の枠組みをRPAに当てはめるうえでの考慮が必要になります。

ポイント（2）導入対象業務

RPAの導入を禁止する業務をあらかじめ定めておくことも必要です。例えば、前述したように、個人情報を扱う業務にはRPAの導入を禁止することも考えられます。また、SOX対象業務にRPAを導入する場合には監査の対象となりますので、より厳密な管理や、RPAに対する経営者の考え方の整理等、監査に耐え得る対応が必要になります。あらかじめSOX対象業務へは導入を認めない、またはSOX対象業務については通常の業務よりもモニタリングに係るルールを厳しくする等、対象業務の重要性に応じて管理の軽重をつけることが必要です。

ポイント（3）既存の統制とのバランス

RPAのガバナンスを整備するにあたっては、必ずしもRPA固有の統制をゼロから作成する必要はありません。既存の統制と照らし合わせ、RPA固有リスクへの対処が必要な箇所にフォーカスして、RPA独自のルール・組織・プロセスを整備することが一般的です。RPA独自の統制を整備する際は、既存の統制と比較して過度な統制になっていないことも、統制の実行性を担保するうえで重要な視点になります。

5. おわりに

RPAガバナンスは、RPAの利用価値を最大化するための枠組みです。RPA固有のリスクへの対応はRPAを安全に利用するために重要である一方で、リスク対応を偏重すれば、業務担当者による短期間での業務自動化の実現といったRPAの利点を享受できない可能性があります。また、RPAガバナンスは一度整備したら終わりではありません。ニューノーマルにおけるテクノロジー活用の流れの中で今後AI等新技術との連携により、想定されるリスクも変動していくことが想定されます。想定されるリスクの大きさに応じて統制の強度を分ける等、リスクベースアプローチに基づくRPAガバナンスを構築し、継続的にアップデートすることにより、ニューノーマルにおいてもRPAを安全かつ有効に利用することができるものと考えます。

KPMGコンサルティング株式会社
マネジャー　酒田 道博

KPMGコンサルティング株式会社

03-3548-5111
kc@jp.kpmg.com

home.kpmg/jp/kc