

別紙:RPAガバナンスの構成要素

大項目		小項目	概要	参考	ポイント	解説	対応方法(例)	備考							
a	戦略	a-1	RPAに対する経営者の理解	経営者もRPAの特徴、活用することの価値、経営へのインパクト等を理解する。	【COBIT】 APO02	(1)	RPA等といったデジタルテクノロジーについて、経営者自身も積極的に理解しようとしていること。	全社レベルでRPA導入を進めていくための意思決定を行うには、その前提として、経営者自身もRPAの特徴や効果等を理解していることが必要不可欠である。これはRPAだけに限らず、デジタルテクノロジー全般に言えることである。また経営幹部等は、経営者がRPAを理解できるよう、その働きかけを行うことが求められる。	・デジタルテクノロジーの進展は早いことから、経営層に対して、RPAを含むデジタルテクノロジーに関する教育を定期的に行う。 ・経営層向けの教育には、RPAやその他のデジタルテクノロジーの概要説明だけでなく、必要に応じて外部の協力を得ながら、自社における適用分野、他社事例(成功例・失敗例)、デモ等も含め、より具体的な検討方針を決定する機会とする。						
						(2)	時間削減といった短期的な効果だけでなく、高付加価値業務へのシフトや採用難等といった人材や労働にかかわる経営課題解決のツールになると理解していること。	時間削減は最も分かりやすいRPA導入効果である。その様な分かりやすい効果だけでなく、創出された時間で高付加価値業務へシフトすることや、ルーティンワークをRPAに置き換えることで採用難に対応する等、時間削減がもたらす効果についても理解しておく必要がある。特に後者は、前者に比べわかり辛いものの、重要性は非常に高いことに留意する。RPAは要素技術でありツールであることから、この様な広い視野を持っていないと、RPA導入自体が目標・目的と化してしまう可能性がある。	・経営層向けのRPA教育では、新聞等で取り上げられているような労働時間削減などの定量的で分かりやすく短期的に得られるコスト効果のみを強調するのではなく、今後訪れるであろう労働人口減少時代において永続的に成長させていくことやRPAを導入しない場合の競争力への影響といった中長期的効果も合わせて説明する。						
						(3)	企業経営のプラットフォームとなるのか、単なるデジタルツールの1つなのか、RPAの位置付けを検討すること。	RPAの位置付けは企業によって異なる。一部の企業ではRPAはマクロの延長といった単なるデジタルツールの1つとしてとらえているが、効果を上げている企業においては、内外の環境変化に対する即応性を高めるツールや、システム全体の効率性向上・リスク低減を図るツール等、企業経営のプラットフォームとして位置付けている。	・経営層向けのRPA教育では、RPAは新たなデジタルツールの1つということだけではなく、働き方を変革するためのツール、組織内外の環境変化に対する即応性を高めるためのツール、システム全体の柔軟性向上・効率性向上・リスク低減を図るツールにもなりうる等、必要に応じ事例を交えながら、企業経営のプラットフォームとなりうることを説明し、啓発する。 ・RPAの位置付けとして、個人利用の業務範囲と責任内においてマクロの延長のような使い方をするか、ロボットにIDを付与し、人(従業員)と同じまたは人(従業員の代わりとするのか、ロボットをシステムと同等に扱う(ロボットの処理は正しいことを前						
						(4)	RPAを導入しない場合の中長期的な影響、リスクについても理解していること。	ROIが高くない等といった理由で全社レベルでのRPA導入が見送られるケースがあるが、中長期的視点で欠けている場合がある。RPA導入が成功している企業は、時間削減といった短期的な効果はRPA導入対象の優先度検討のインプット程度とし、RPAを全社導入しない中長期的な影響やRPAが定着化するまでの期間等、中長期的視点での検討を重視している。	・経営層向けのRPA教育では、「a-1(2)」にてRPAの中長期的な視点での期待効果を理解させた上で、RPAを導入しない、またはうまく導入が進まない場合に、それらの効果を得られないことが、中長期的に経営にどのような影響をおよぼす可能性があるかも併せて説明する。						
		a-2	RPA導入目的・目標・方針	企業ミッションを踏まえ、RPAをどのような効果を得るために導入し、活用するかの目的を明確化する。	【COBIT】 EDM02、EDM04、APO02、APO05 【監督指針】 Ⅲ-3-7-1-2-(6)-①	(1)	RPA導入によって解決すべき経営課題や、達成すべき短期的および中長期的な目標が明確化されていること。	RPA導入効果を図るため、ROIを利用することがあるが、RPAの導入効果は業務時間の削減のみではない。付加価値を生まない単純作業の時間を削減することで、注力すべき高付加価値業務に対して、RPA導入前より時間を割けるようになること、採用難等の人材確保面の経営課題を解決できるツールになり得ること等のメリットがある。これらの点を踏まえ、RPA導入によって解決すべき経営課題や、達成すべき目標を明確化することが望まれる。また、達成すべき目標として、時間削減といった短期的な目標だけでなく、人員の再配置等といった中期的な目標も検討されていることが望まれる。	・RPA導入によって解決すべき経営課題をRPA導入の目的を実現するために達成すべき目標について定め、組織全体に共有する。 ・RPAの導入効果を図り継続的な改善を行うため、「効率化」などの定性的な目標だけでなく、「XX時間削減」などの定量的な目標を設定する。 ・設定する目標には、単純に今ある業務をロボットに置き換えることのみを検討するのではなく、「XX%の業務を全てロボットに置き換える」、「XX人の人員の再配置を行う」など「a-1(2)」に記載の内容を踏まえ、中長期的な目標も設定する。 ・設定した目標を従業員に周知する際は、単に業務の置き換えや人員削減だけでは従業員のモチベーションダウン等、誤った捉え方をされる可能性があるため、「採用難等、労働人口の不足に備える」などの背景や理由も合わせて説明する。						
						(2)	会社としての明確な導入方針が定められていること。	RPAの導入は通常の情報システムの導入と比較して容易なため、各部門が独自に導入することも可能である。しかし、各部門が個別のRPAツールを導入し、個別のルールで利用する場合、全社的なガバナンスが機能しない状況に陥る恐れがある。そのため、会社として、RPAを導入する領域や規模、導入のロードマップ等、RPAの導入方針を定めることが必要である。	・RPA導入目標を実現するため、トップダウンで進めるのかボトムアップで進めるのか、特定業務領域から進めるのか全業務領域を対象に進めるのか、いつまでにどの様な状態にするのか等、アプローチやロードマップを含む導入方針を定め、組織全体に共有する。						
							a-3	RPAにかかわるリスク認識と対応方針	RPA導入により生じるリスクを認識し、そのリスクに対応するため、RPAガバナンスを整備する方針を明確化する。	【COBIT】 EDM03、APO01、APO12 【監督指針】 Ⅲ-3-7-1-2-(1)-①、Ⅲ-3-7-1-2-(2)-①、Ⅲ-3-7-1-2-(2)-②、Ⅲ-3-7-1-2-(6)-②	(1)	RPA導入によって生じるリスクを認識すること。	RPAは人が端末上で行う作業をソフトウェアロボットが代替で実行する自動化ツールであり、その利便性などのメリットが強調されるが、人ではなくロボットが行うことにより新たに生じるリスクが存在する。RPAを適用する業務や利用範囲に応じ、内部統制のリスクやセキュリティのリスクなど、どのようなリスクがあるかを識別することが求められる。	・PoC等のRPAの検証を行う期間を設け、その中でセキュリティや内部統制上どの様なリスクがあるのかも合わせて検証し、想定されるリスクを洗い出す。 ・リスクの洗い出しは、客観的視点が必要であるため、必要に応じて、知見のある社内の有識者(セキュリティ担当、リスク管理担当、内部統制担当等)や外部専門家を交えた検討を行う。 ・洗い出したリスクは、顕在化した場合に致命的になるものからそうでないものまでさまざまなものがあるため、頻度(頻繁に起こりうるか等)や影響度(顕在化した場合、事業に重大な影響をおよぼすか等)からそれぞれのリスクの重要度を検討(まずは識別したリスクを許容できるか否か整理)する。 ・RPA導入・利用におけるリスクは、後々顕在化するとその改善に多大なコストがかかったり、場合によっては導入自体見直しになりかねないため、PoCの期間等、早いタイミングで検討を行う。	
											(2)	RPA導入・利用におけるリスク対応方針や、経営が従業員に求める管理方針・ルール等が定められていること。ただし、認識したリスクに対し過度にならないこと。	リスクに対し過度にガバナンスを整備すると、RPAの利点である柔軟性が失われることにもつながるため、リスクに対する対応方針(許容、低減、回避等)を定め、リスク対応方針に沿った管理方針や管理ルール等を整備することが望まれる。その際、リスクを過度に評価してRPAの利用促進を妨げるのではなく、リスクに応じて必要となるガバナンスを整備していくことが重要となる。	・検討したリスクの重要度に応じ、その対応方針(許容、低減、回避等)を検討する。ただし、RPA本格導入前の場合は、ルール検討のインプットレベルの対応方針となるため、ハイレベルな検討に留める。 ・リスクとその対応方針の検討は、場合によっては保守的となり、過度なものとなる可能性があるため、RPAを適用する業務範囲や権限を限定的なものとする場合やロボットが停止した際の業務影響が著しく小さい場合は、管理の対象外にする等、緩和的なルールも視野に検討する。 ・リスクや対応方針の検討は判断が要求されるものであるため、必要に応じて知見のある社内の有識者や外部専門家を交えた検討を行う。 ・リスクはRPAの導入状況や利用環境等の変化によって変わるため、リスクの洗い出しと対応方針の検討を継続的に行うプロセスを整備する。	

大項目	小項目	概要	参考	ポイント	解説	対応方法(例)	備考	
a	戦略 (続き)	a-4 取締役会や経営会議における議論	RPAの導入方針やリスク対応方針について、経営層で議論し、合意する。	【COBIT】 EDM01、EDM05、APO08 【監督指針】 Ⅲ-3-7-1-2-(1)-①、Ⅲ-3-7-1-2-(2)-①、Ⅲ-3-7-1-2-(6)-①	(1) 経営会議や取締役会等で、RPA導入方針やそれに伴うリスク対応方針が議論されていること。	RPAは人が端末上で行うあらゆる作業をロボットが自動で行うことが可能であり、RPAを導入することで生じるリスクは、あらゆる業務プロセスや事業に影響する可能性がある。そのため、経営会議や取締役会等において、経営層に対してRPAの導入方針やRPA導入によるリスクが共有され、リスクを低減する施策や環境、会社として保有するリスク等のリスクの対応方針が議論されていることが望ましい。	・RPA導入に向けてどのように活用・浸透させていくのか等の方針とRPA導入に伴うリスクを定期的に経営会議等で議論する。例えば、推進組織の体制・各部門の役割・責任について、利用ツールの選定方針、予算の割り当てや、「a-3」で検討したリスクについて経営層に共有し、対応方針について議論する。	
				(2) 経営会議や取締役会等で、RPA導入方針、RPAガバナンス整備状況、RPA導入による効果等のステークホルダーへの公開が議論されていること。	RPAガバナンスにおいて、ステークホルダーのニーズを充足することが重要であるため、会社としてのRPA導入方針や利用方針、定期的なモニタリングによるRPAガバナンスの整備、管理状況、得られている効果等について、社内への情報共有や株主総会・IR活動などによるステークホルダーへの公開について、経営会議や取締役会等で議論されていることが望ましい。	・RPA導入方針や得られている効果について、ポータルサイト等を利用した全社的な共有や、ホームページ、プレスリリース等を利用した社外への公開について経営会議等で議論する。		
b	組織	b-1 RPA導入・利用における責任の所在	RPAを導入することに対する経営者の役割・責任やRPAガバナンスを機能させる責任を負う担当役員の設置を明確化する。	【COBIT】 EDM01、APO07 【監督指針】 Ⅲ-3-7-1-2-(1)-③	(1) RPA導入・利用における経営者の役割・責任が明確化されていること。	RPAを導入し、利用する組織の経営者に対する役割・責任が明確化されていないと、目的や有事が発生した際の責任が曖昧になり、結果として組織全体に影響をおよぼす可能性があるため、RPAの管理方針等にて明確に定めることが望まれる。	・RPA導入方針に従い、どのような役割と責任が経営者に求められるかを関係者と議論し、決定する。例えば以下のようなRPA導入・利用にかかわる役割と責任が経営者に求められる。 ・決定したRPA導入・利用における経営者の役割と責任は、管理方針や管理ルールに定義するし、組織全体に周知する。	
				(2) RPAガバナンスを機能させる責任を負う担当役員が選任されており、またその役割が明確化されていること。	RPAガバナンスを機能させる責任を負う担当役員には、例えば、RPAガバナンスの整備と維持・管理、RPA導入状況の把握、RPA導入によるリスクの管理、RPAのセキュリティ管理などの役割が求められる。RPAの管理方針等にてこれらの役割を明確にし、RPAガバナンスの担当役員を明確化することが望まれる。なお、RPAガバナンスの担当役員として、経営企画部門、業務改革部門、デジタル推進部門、情報システム部門などの担当役員が選任される場合が多い。	・RPA導入方針に従ったRPA利用の推進し、RPAガバナンスの構築とそのガバナンスを機能させる役割を負う担当役員を選任する。 ・RPAガバナンスを機能させる責任を負う担当役員には、RPAのメリットや位置付け、リスク等を正しく認識している者から選任する。または、必要な教育を実施する。 ・RPAガバナンスを機能させる責任を負う担当役員およびその役割と責任は、管理方針や管理ルールに定義する等により明確化し、組織全体に周知する。		
		b-2 全社的な管理体制	RPAガバナンスを機能させるために必要となる全社的な体制とその役割・責任を明確化する。	【COBIT】 EDM01、APO01	(1) 各組織形態(集権型・分散型・連邦型)のメリット・デメリットを理解し、組織に応じたRPAガバナンスの形態を組成し、必要となる推進・管理部門を設置すること。	RPAガバナンスを機能させる体制は、以下のような集権型、分散型、連邦型に大別される。RPAの導入状況や将来的な利用拡大を考慮し、どのような管理体制を目指すのか、それぞれのメリット・デメリットを踏まえ、検討し、必要となる推進部門や管理部門を整備する必要がある。 - 集権型: 全社的な戦略・方針に従いRPAを導入し、全社的な推進組織がRPAのツール基盤、開発・運用体制、管理ルールを整備・管理しているようなガバナンス形態 - 分散型: 各事業部門が個別にRPAツールを選定・導入し、維持・管理しているようなガバナンス形態 - 連邦型: RPAの導入や利用は各事業部門の判断にて実施しているが、全社的な推進組織が管理ルールの策定・展開、RPAシステムの提供、開発支援など一程度関与しているようなガバナンス形態	・RPA導入の目的や目標・方針に応じ、RPA導入や管理に関する全社横断的な推進・管理組織を設置する(集権型、連邦型)か、各部門にてRPAの導入や管理をしていく(分散型)かを決定する。 ・RPAガバナンスを機能させるために必要となる管理体制の検討においては、短期的に必要な管理体制と合わせて中長期的な目標に応じた将来的な利用拡大を考慮した管理体制も合わせて検討し、将来的な基盤の変更や移行も考慮した体制整備計画を策定する。 ・決定した管理体制を組織全体に周知し、集権型や連邦型の場合は推進・管理部門を設置する。	
					(2) 推進・管理部門には、ロボット利用状況の把握やセキュリティレビュー等、会社として一定レベルの管理水準を担保するための機能を持たせること。または推進・管理部門を設置しなくとも、各部門で不適切なロボットの利用がなされないための仕組みを整備すること。	推進・管理部門を設置する場合は、管理ルールに反した不適切なロボットの利用を予防・発見し、会社として一定レベルの管理水準を担保するため、ロボット利用状況の把握やセキュリティレビュー等の機能を持たせることが望まれる。また、分散型の場合など推進・管理部門を設置しない場合は、同等の役割を持った管理者の設置を求めることが望まれる。	・推進・管理部門を設置する場合は、各事業部門におけるロボットの適用業務の範囲やセキュリティの順守状況などの監視を含む役割を定義し、必要となるリソースを確保する。 ・分散型の場合など推進・管理部門を設置しない場合は、ロボットの適用業務の範囲やセキュリティの順守状況などの監視を含む役割を持った管理者を各事業部内に設置し、適切な権限と責任を持った者を任命する。	
		b-3 利用部門と開発部門の役割・責任	RPAを導入して利用する部門や開発部門の役割・責任について明確化する。	【COBIT】 EDM01、APO01	(1) RPAを導入して利用する部門やロボットを運用する部門の役割と責任を明確化すること。	自部門の業務にRPAを導入し利用する部門は、ロボットにより自動化する部分も含めて、当該業務の結果に責任を負うことが一般的である。具体的には、業務予定に従いロボットを確実に実行すること、ロボットの処理に誤りがいないことを確認すること、ロボットの処理に異常や遅延が発生した場合のリカバリを行うことなどが求められるため、その役割と責任を管理ルール等で明確に定めておく必要がある。また、ロボットの運用管理を行う部門を利用部門とは別に設置する場合は、その役割分担も明確に定めることが求められる。	・RPAのユーザー部門等、RPAを導入して利用する部門やロボットを運用する部門の役割・責任を明確化する。特にユーザー部門側で開発を行わない場合(ユーザー部門が開発を内部・外部へ委託する場合)、個々の開発において、ユーザー部門と開発側との責任分界点を十分に考える。また役割・責任は、責任者、管理者、担当者等、職階の違いも検討する。 ・情報セキュリティやSOX等、関連する社内ルールへの順守も、ユーザー部門に責任があることを明確化する。	
					(2) ロボットを開発する部門の役割と責任を明確化すること。	ロボットの開発は、通常の情報システムのように利用部門と合意した要件に従い、設計・構築、テストを工程順に行うのではなく、開発やテストをしながら設計や要件の見直しを繰り返しながら行われという特徴がある。このような特徴やRPA利用部門との役割分担を考慮し、要件定義やテスト、リリース判定、本番利用開始後の障害対応や維持・管理などについて、ロボット開発部門の役割と責任を管理ルール等で明確に定めておく必要がある。	・ロボットを開発する部門の役割・責任を明確化する。特にユーザー部門と開発側との責任分界点を十分に考える。また役割・責任は、責任者、管理者、担当者等、職階の違いも検討する。 ・上手く開発が進まない原因はユーザー側(開発依頼側)にある場合がある。よって要件定義やテスト等、ユーザー側が十分に関与するよう明確化する。	
					(3) ロボットの開発者、利用者、運用者の分離、ロボットの実行可能権限とその作業の承認権限の分離等、職務分離が検討されていること。	RPAの利用形態によっては、適切な承認プロセスを経ないでロボットが開発される、リリースされる、実行されるというリスクがある。これらリスクが顕在化しないよう、ロボットの開発を行う開発者、ロボットのリリースを行う運用者、ロボットの起動を行う利用者を分離することを検討することが望ましい。また、情報システムへ申請を起票するロボットを作成する場合において、当該申請を承認する権限を保有する承認者にはロボットの実行権限を持たさないなど、システムで設計された権限の分離を侵さないように考慮することが必要である。	・現在のRPA利用形態において、未承認のロボットの開発、リリース、利用といったリスクがあるか検討する。もしその様なリスクがあるのであれば、各職務の分離を行う。 ・上記職務の分離は、ルールだけでなく、それを順守できるよう技術的な対応も検討する。	

大項目	小項目	概要	参考	ポイント	解説	対応方法(例)	備考
c 人材	c-1 RPA人材の育成	RPAガバナンスを機能させるために必要な人員やロボットの開発・運用に必要な人材を確保するための育成や採用方針、外部委託先の活用方針を明確化する。	【COBIT】 APO07、APO10、BAI08 【監督指針】 Ⅲ-3-7-1-2-(6)-⑥	(1) RPAの概念やRPA導入目的・目標を理解させる取り組みが行われていること。	RPA推進部門、RPAシステム運用部門、ロボット開発部門、ロボット利用部門などのRPA関連組織の従業員（外部委託先を含む）に対して、RPAの概要や当該組織のRPA導入目的・目標や各部門の役割に応じて必要な内容の教育を定期的の実施することが望まれる。	・RPAに関連する組織、従業員に対し、RPAの概要、目的・目標、利用手続き等の教育・説明会・研修等を定期的に行う。 ・教育には、概要や手続きだけではなく、必要に応じて外部専門家の協力を得ながら、他部門や他社の適用実績における事例や、デモ等も含める。	
				(2) ロボットの開発や運用に必要な人的リソース（質・量）が洗い出され、その育成や採用、外部委託先の選定等が行われていること。	ロボットの開発や運用を行うために必要なリソースを質（スキル、知識）と量（人数）の両面で計画的に確保する必要がある。業務の重要度に応じて、ロボットで処理異常が発生した場合の保守体制を整備する必要がある。	・ロボットの開発、運用を行うためのリソースについて、自社内で育成するのか、新たに従業員を採用するのか、外部委託するのかを検討し、決定する。 ・自社内で育成を行う場合は、立ち上げ時は必要に応じて外部委託先の協力を得ながら進め、徐々にスキルを移管していくような移行計画を策定する。 ・ロボットの処理で異常が発生した場合に、迅速に復旧する必要があるような重要な業務がある場合、自社内でロボットの修正を持った要員を確保するか、ロボットの運用を外部に委託する場合は迅速に対応してもらえる契約内容とする。	
				(3) ロボット開発や運用の内製化を目指す場合、必要となるスキルが明確化され、内製化に向けた開発スキルの教育計画や育成やロボット開発ナレッジを蓄積する仕組みが整備されていること。	RPA導入当初は、ロボットの開発は専門知識・スキルを持つ外部委託先を活用する場合が多い。ただし、RPA適用範囲拡大、運用の内製化、開発コストなどの観点から、将来的な開発の内製化を図る場合は、必要となるスキルの明確化、内製化の範囲、社内体制の整備、人材の育成・採用、外部委託先からの知識・スキル移管、開発ナレッジの蓄積や最新技術動向の把握などを計画的に実施することが望まれる。なお、RPAの導入や運用を行うために必要となるスキルには、RPAツールにかかわる知識だけでなく、BPRのスキル、情報システムやセキュリティのスキルなども含まれることも考慮する必要がある。	・内製化する必要があるか否か、内製化のメリット・デメリットを踏まえ、検討する。 ・いつまでに内製化を目指すのか検討する。そしてそれに向けた課題及び対応方針を検討の上、内製化に向けた具体的な計画を策定する。 ・策定した計画に基づき、体制整備や人材育成、各種部品やナレッジを共有する仕組みを構築する。	
	c-2 RPAの導入目的やリスク認識の醸成	RPA導入の目的や導入により生じるリスク、それに対応するための管理ルール等を認識させる。	【COBIT】 APO07 【監督指針】 Ⅲ-3-7-1-2-(4)-⑩	(1) 全ての従業員またはロボットが行う業務に関わる従業員に対し、RPAの導入方針や管理ルールに関する教育を実施していること。	RPAを安心安全に利用していくには、全ての従業員またはロボットが行う業務に関わる従業員に対して、RPA導入戦略や導入方針、RPA導入によるリスク、ロボット管理ルールや取り扱いの注意事項などを教育する必要がある。RPA単独での研修開催が難しい場合は、情報セキュリティ研修やコンプライアンス研修等にRPAに関わる内容を追加する方法も考えられる。	・RPAの開発に関する教育だけでなく、リスクやルール等に関する教育も含む、RPAに関する教育プログラムを策定する。なお教育は、1度実施して終わりではなく、継続的かつ段階的に行なうよう検討する。 ・策定したプログラムに基づき、教育を実施する。	
				(2) 従業員へ伝えるRPAの導入方針には、ロボットによる自動化、効率化、コスト削減だけでなく、RPAの活用によりビジネス、組織、従業員、プロセスをどのように変革させていくかの戦略や目的を含めること。	RPA利用部門の従業員にとって、ロボットの導入は人員削減などネガティブなイメージもあるため、ロボットの利用の促進やRPA適用業務の拡大が現場レベルで計画通りに進まない恐れがある。社会、業界がどのように変化していき、それに合わせて組織や人、プロセスをどのように変革する必要があるのか、また会社としておよび個人としてどのようなメリットがあるのかを従業員に伝える必要がある。	・RPA普及に向け、従業員に対してメッセージを伝える。なお当該メッセージは、動機付けになるよう検討する。また場合によってはモチベーションダウンにつながる可能性があるため、慎重に検討する。	
	d プロセス	d-1 ロボットの重要度・リスク度合いの評価	【COBIT】 EDM03、APO12、DSS06 【監督指針】 Ⅲ-3-7-1-2-(3)-①、Ⅲ-3-7-1-2-(4)-⑤	(1) ロボットの重要度やリスク度合いの定義やその判断基準が明確化されていること。	例えば機密性・可用性・完全性の観点等から業務にRPAを適用することのリスクを考慮し、そのリスクに応じたロボットの重要度の管理分類やその判断基準を定義することが望まれる。	・ロボットが停止または誤処理をした際のリスクに応じて、「最重要」、「重要」、「一般」というような重要度の管理分類を定義する。 ・業務の特性や重要性、異常発生時の業務影響度、取り扱うデータの機密性、アクセスする情報システムや権限などの観点から、各ロボットをどの重要度に分類するか判断基準を定める。	
				(2) 重要度やリスク度合いに応じたロボットの管理水準・管理ルールが明確化されていること。	重要度やリスク度合いを考慮せずに一律で同じ管理ルールを適用する場合、リスクの低いロボットにも過剰な管理ルールを求めることとなったり、逆にリスクの高いロボットに対し簡易的なルールしか求めなかったりすることが懸念される。そのため、ロボットの各重要度分類に対し、そのリスクに応じて求める管理水準や管理ルールを定めることが望まれる。	・ロボットの重要度の定義に従い、例えばロボットの重要度が「最重要」、「重要」に該当するもののみを重点的に管理（リリース・変更時の成果物の提出と確認、リリース後のモニタリング等）する。 ・ロボットの障害対応についても、「最重要」と「重要」は監視や障害対応体制の整備を求めるような管理ルールとする。	
				(3) ロボットの重要度やリスク度合いを評価する手続きが明確化されていること。	ロボットの特徴として、開発しながら業務範囲などの要件を具体化していくことや、リリース後も業務や操作するシステムの変更に合わせて頻繁にロボットプログラムの変更を行うことがある。その変更により、ロボットの重要度やリスクが変動してしまう場合があるため、開発起案時に加えリリース時にも、またリリース後も定期的に、そのリスクや重要度を評価するプロセスを定めることが望まれる。	・ロボットの重要度の判断基準に従い、開発起案時に評価を行い、当該ロボットのリリース時にも重要度の判定を行う。 ・ロボットの重要度分類が把握できるよう、ロボット管理台帳等を作成し、管理する。 ・リリース後も定期的にロボットの重要度に変更はないか、リスクに変動はないか等の評価やモニタリングを実施する。	
	d-2 RPAシステムの選定・導入	RPAを適用する業務領域に求められるロボットの信頼性や管理機能などから、RPAツールや基盤を選定し、導入するプロセスを明確化する。	【COBIT】 BAI02、APO01	(1) 新たな業務領域へのRPAの適用について、検討や承認プロセスが定められていること。	新たな部門へのRPA導入など、新たな業務領域へのRPA適用を検討する場合、そのリスクを検討・評価し、適用を承認するフローや承認者が明確となっていることが望まれる。なお、信頼性、大量処理、レスポンスなどの要求が高い自動化については通常の情報システムの導入を、スプレッドシートのみなど単一アプリケーションのみの操作の場合は当該アプリケーション機能を利用した自動化の実現などを合わせて検討することが望まれる。	・新たな部門へRPAを導入する場合、RPA導入活動を推進している管理者または責任者に承認を得るプロセスを構築する。 ・業務の自動化を検討する際、RPAの適用のみを前提とせず、業務の特性や利用するアプリケーション等により、場合によっては情報システムの導入の検討、アプリケーション機能を利用した自動化、業務プロセスの見直し等も併せて検討する。	
				(2) RPA適用が承認された業務領域について、その重要度や取り扱うアプリケーション、将来的な拡張予定などに応じて、ロボットに求める信頼性、性能、管理機能などの要件を明確化し、RPAツールや基盤を選定し、導入する手続きが定められていること。	RPA適用が承認された業務領域について、既存の基盤上でロボットを開発するか、要件が適合しないため新たなRPAツールや基盤を選定・導入するかを検討するプロセスを整備することが望まれる。ロボット管理サーバーや端末の導入は、通常の情報システムの導入プロセスに従い実施することが考えられる。	・業務で利用するアプリケーションや情報システムとRPAツールの親和性を検証した上で新たに導入するRPAツールを選定する。 ・スモールスタートから将来的にロボットの台数を拡張していく等の想定をしている場合、ロボットを一元管理可能なサーバー型への移行可否やその機能も考慮し、基盤導入を検討する。 ・RPAツールや基盤を選定する際は、メンテナンスの容易性や、ロボットの運用を見据えた管理機能等を検討する。その際、クラウド版RPAツールがある場合は、拡張性や管理負荷等の観点も踏まえ、選択肢のひとつとすることも検討する。 ・ロボット管理サーバーやロボットを利用する端末を導入する際は、既定の関連情報システムの導入プロセスがあれば、それに従い実施する。既定の導入プロセスが存在しない場合は、申請方法、セキュリティチェック等の導入プロセスを明確化する。	・必要に応じて、e-1の「RPAツールに対する要求事項」の考え方と整合を取ること考えられる。
				(3) 新たなRPAシステムを導入する場合は、ロボット管理サーバーやロボット端末などの運用、保守の管理体制や手順を定めるプロセスとしていること。	新たなRPAシステムを導入する場合は、ロボット管理サーバーやロボット端末などを運用し、保守するための管理体制の整備や管理手順の作成を行う必要がある。導入期間中にそれらを整備するプロセスとすることが望まれる。特にロボット管理サーバーが障害等で停止した場合は、複数のロボットやその業務へ影響することとなるため、将来的な体制強化も考慮しつつ、そのリスクに応じた運用、保守の体制を整備することが望まれる。	・新たなRPAシステムを導入する場合、ロボット管理サーバー、ロボット端末、開発したロボットに対し、それぞれの運用、保守にかかわる役割と責任を明確化する。 ・運用、保守にかかわる定期的なオペレーション、不定期に発生するオペレーションを洗い出し、必要な手順を整備する。	

大項目	小項目	概要	参考	ポイント	解説	対応方法(例)	備考
d プロセス (続き)	d-3 ロボットの開発・変更	ロボットを企画する際の考慮事項、開発標準の適用、整備すべきドキュメントなど、ロボットを開発する際に順守すべき事項や、ロボットリリース時のテスト・承認プロセスを明確化する。	【COBIT】 APO11、BAI03、BAI06、BAI07 【監督指針】 Ⅲ-3-7-1-2-(6)-③、Ⅲ-3-7-1-2-(6)-⑤	(1)	業務標準化等も含めた要件検討や開発の優先順位付けなど、ロボットを企画する際の手続きが明確化されていること。	ロボットを企画する際は、業務フロー全体の見直しや標準化、リスクや効率性を意識した自動化範囲の決定などを行った上で要件を検討し、最終的にはROI算定等により優先順位を付けて開発対象とするプロセスを定めることが望まれる。 ・ロボット企画時には、業務主管部門が業務フロー全体を見渡した上で、主管業務のうち、どの業務にRPAを適用するか、また、どのような作業を自動化し、どのような作業は人間に行わせるかを検討し、RPAの適用計画を策定する。 ・RPA導入だけでなく、業務標準化や廃止等、RPA導入以外の方法も検討する。 ・ロボットの開発着手にあたっては、ROIだけでなく、以下のような観点も踏まえ優先順位付けを行う。 - 社内での横展開が可能か - RPA適用による定量的、定性的効果が高い等	
				(2)	開発標準などのロボット作成時に守るべきルールやリリースまでに整備すべきドキュメントなど、ロボットを開発する際に順守すべき事項が明確化されていること。	・開発者による品質のばらつきを抑制するため、ロボット開発における工程と工程毎の整備すべき成果物やコーディングルールなどの標準的な開発ルールを定め、それを順守することが必要である。また、RPAの開発は一般的なシステム開発と異なり、開発期間が短期間となることや、開発手法についてもウォーターフォール型ではなくアジャイル型の開発手法を用いることが一般的であることに留意する。ただし、重要度/リスク度合いの高いロボットにおいては、スピード感より品質等を重視する必要があることに留意する。 ・RPAツールや利用するシステムの特性等を加味した開発標準を策定し、社内へ展開する。また展開だけでなく、開発されたロボットの品質レビュー、順守状況のモニタリング、改善プロセスも合わせて検討する。 ・通常のシステム開発との違いを踏まえた開発工程を検討し、それぞれの工程で作成する成果物を明確化する。開発工程と成果物については、通常のシステム開発のものをベースに簡易的なものとして例えば以下のような成果物のテンプレートを整備する。なお重要度/リスク度合いの高いロボット開発の場合は、レビューを厚くする等といった考慮を行う。 - ロボット要件定義書 - ロボット仕様書 - ロボットテスト計画書兼結果報告書 - リリース判定チェックリスト	RPAはその特性上、通常のシステムと違い頻繁に変更が入る可能性がある。またエンジニアが開発したものをユーザーが保守するようなことも考えられる。そのためロボットの保守性は重要となる。
				(3)	エラー処理のテストの実施、RPA利用部門も参画したテストの実施、テスト環境でのテストの場合は本番環境との違いの考慮、本番環境でのテストの場合は本番システムへの影響の考慮など、ロボットをテストする際のチェック項目や留意事項が明確化されていること。	・エラー処理のテストの実施やRPA利用部門も参画したテストの実施など、ロボットをテストする場合のチェック項目を明確化したチェックシート等を整備することが望まれる。また、テスト環境と本番環境の違いを踏まえたテスト計画の策定や、本番環境を使ってテストをする場合の実行後の本番システム内のテストデータの削除など、テスト環境に応じた留意事項を明確にすることが望まれる。 ・通常のシステム開発同様、正常系だけでなく、異常系のテストも行う。特にRPAの場合ユーザー開発を行う場合もあり、またシステム環境の変更等によって止まる場合があることから特に留意する。 ・システムを操作するようなロボットのテストは、原則テスト環境のシステムを使ってテストを行う。その際、例えば以下の通り、テスト環境と本番環境との違いを十分に考慮する。(テスト環境では正常に動いたが、本番環境では動かない等といったことも起こりうる可能性がある。) - 画面解像度 - 端末のスペック - RPAツールのバージョン - 権限 等 ・やむを得ず、本番環境を利用したテストを行わざるを得ない場合、データを元の状態に戻せることを条件に、本番環境のシステムを使ったテスト実施を許容することも検討する。なお許容する場合、テスト完了後(リリース前)にデータが元に戻されていることを確実にするプロセスも合わせて検討する。データを元に戻せない場合は、参照系の操作やデータ入力もドラフトまで等、適用範囲を制限する。	
				(4)	ロボットをリリースする際の承認者や承認時の確認項目などが明確化されていること。	・開発・テストが完了したロボットを本番利用する前のリリース手続きとして、リリースの承認者やロボットのリリースを判定するチェックシートなどを整備し承認時の確認項目を明確にすることが望まれる。承認時の確認項目としては、テスト結果の確認、ドキュメントの整備状況の確認、要件定義時からの設計変更有無の確認、テスト済みロボットの確実なリリース手順の確認などが考えられる。 ・リリースするにあたって、必要となる工程が完了し、特段問題がないこと、また本番運用にかかわる各種ドキュメント類がそろっていることを確認した上でリリースする。なお重要度/リスク度合いの高いロボットのリリースについては、リリース時のレビューを強化する等といった対応を行う。 ・上記リリース時に確認すべきことをチェックリスト化しておく。 ・デグレーション等が発生しないよう、例えば2名体制でリリース作業をしたり、リリース手順を明確化する等といった対応を行う。また業務に影響を及ぼさないよう、リリースのタイミングについてもよく検討する。	
				(5)	リリース済みのロボットを改修する場合の役割や手続きが明確化されていること。	・ロボットの改修も基本的には新規開発時と同等の手続きとなるが、軽微な変更や障害対応による緊急の変更などがあることも考慮し、必要な手続きやその役割を明確化することが望まれる。 ・ロボットを改修する際は、原則ロボットの新規開発に準じて行う等、改修手続きを検討する。 ・ただし、障害対応等の緊急を要する場合、テスト完了後、RPA推進部門の管理者、およびユーザー部門の管理者の口頭承認を得たのちにリリースを行い、事後に正式な承認を得る等といった対応を取ることも検討する。	
	d-4 ロボットの運用・管理	ロボットを安全かつ安定的に稼働させるために、ロボットの運用・管理プロセスを明確化する。	【COBIT】 BAI09、BAI10、DSS01～04 【監督指針】 Ⅲ-3-7-1-2-(1)-④、Ⅲ-3-7-1-2-(5)-⑧、Ⅲ-3-7-1-2-(9)-①、Ⅲ-3-7-1-2-(9)-④、Ⅲ-3-7-1-2-(10)-①、Ⅲ-3-7-1-2-(10)-②、Ⅲ-3-7-1-2-(10)-⑥	(1)	ロボットの運用にかかわる定例、非定例のオペレーションを明確化し、その手続きを定めること。	・ロボットの起動、処理結果確認などの定例オペレーションや、ロボットの臨時実行、実行スケジュールの変更、バックアップ取得、ロボット用IDのパスワード変更などの非定例オペレーションを明確化し、作業実施～確認まで一連の手続きを定めることが望まれる。 ・サーバー側、デスクトップ側の定例、非定例作業を洗い出し、定例・非定例オペレーションとして明確化する。なお網羅的に洗い出した作業以外のものは、非定例オペレーションとして位置付ける。 ・定例オペレーションについて、作業手順を定めると共に、作業実施、結果の確認までの一連の手続きを策定する。なお策定する作業手順は、十分なレビューや必要に応じて試行を行う。加えて手続き策定にあたっては、作業ミス、漏れといったリスクが低減できることに留意する。 ・非定例オペレーションについて、作業申請・承認、実施、実施結果の確認まで、一連の手続きを策定する。なお手続き策定にあたっては、未承認の作業実施、作業ミス、漏れ等といったリスクが低減できることを検討する。	
				(2)	ロボットが停止するリスクを低減するための予防的な対策を講じること。	・ロボットが利用するシステムの画面レイアウトの変更やバージョンアップ等、ロボットの動作に影響を与える可能性のある情報は事前に把握する仕組みを構築する。事前に改修可能な場合は改修し、事前に改修ができない場合は影響があるロボットの利用者への注意喚起と当該ロボットの保守要員を増員する等の対応を検討する。	

大項目	小項目	概要	参考	ポイント	解説	対応方法(例)	備考
d	d-4	ロボットの運用・管理 (続き)	【COBIT】 BAI09、BAI10、DSS01～04 【監督指針】 Ⅲ-3-7-1-2-(1)-④、 Ⅲ-3-7-1-2-(5)-⑧、 Ⅲ-3-7-1-2-(9)-①、 Ⅲ-3-7-1-2-(9)-④、 Ⅲ-3-7-1-2-(10)-①、 Ⅲ-3-7-1-2-(10)-②、 Ⅲ-3-7-1-2-(10)-⑥ (続き)	(3)	ロボットの処理で異常や遅延が発生した際に、自動的に通報される仕組みまたは人が検知して連絡する手続きを定めること。	ロボットの処理の異常や遅延について、どのような基準で異常や遅延と判断するかを定義し、当該業務の重要度に応じて、自動的に通報される仕組みや人が即時または事後で検知して連絡する手順や監視・連絡体制を整備することが望まれる。なお、事前に想定されるイレギュラーケースについては、ロボットの処理に異常時対応フローを組み込むことを推奨するが、想定外の異常が発生することもある。	・対象となるロボットを洗い出し、各ロボットの異常や遅延の定義(いわゆる障害の定義)、対応方法(リトライ、担当者に連絡等)を検討する。担当者に連絡する対応を取る場合は、連絡先等も作成する。前述の定義検討において、金融機関の場合は、どの場合を事務リスクとするか、システムリスクとするか検討する。その際、リスク管理部門に相談したり、また易きに流れないように注意する。 ・上記を踏まえた対応フローを作成する。その際、その内容や影響に応じて、関連部門へ適時に連絡したり、エスカレーションするフローとなることに留意する。(RPAにかかわる障害対応と危機対応の境目に留意する。)
				(4)	再発が想定されるロボットの処理の異常や遅延について、原因分析や恒久対応を行う手続きを定めること。	発生したロボットの処理の異常や遅延の再発が想定される場合は、投入データ確認やリトライ実行等の対応手続きの作成やロボットの変更を行うなど、原因分析や根本解決に向けた手続きを定めることが望まれる。また、必要に応じてロボットの品質についても見直す必要がある。	・処理の異常や遅延等のインシデントを記録し、定期的にそれら内容を分析し、類似する障害の未然防止策や再発防止策を検討する。必要に応じ、関係者に対し横展開を行う。 ・異常が発生したロボットについて、開発標準等のルール通りに実装がされているか、例外処理は適切に実装されているか等、実装内容を確認した上で必要に応じて改修を行う。場合によっては、開発標準自体の見直しも検討する。
				(5)	ロボットが利用できなくなることを想定したコンティンジェンシープランが策定されていること。	ロボットの異常が修復できない場合やロボット管理サーバーが停止するなど、ロボットが同時に使用できなくなるまたはロボットが長期間利用できなくなることも想定し、特に止まった場合の影響が大きい業務に対しては、代替手段なども含めたコンティンジェンシープランを策定することが望まれる。また、策定したコンティンジェンシープランは、定期的にその有効性を確認し、見直すことが望まれる。	・ロボットが利用できない場合の対応策として、リトライ方法に加え、手作業による代替手段を検討する。特にその様な場合の影響が大きいロボットについては、顧客への連絡等、関係者への連絡を含めたコンティンジェンシープランを策定しておく。なお策定した代替手段やコンティンジェンシープランは、定期的にその有効性を確認し、必要に応じて見直しを行う。 ・高い可用性が求められるロボットが多くなると、同時多発的にロボットが利用できない自体が発生した場合、危機的な状況に陥る可能性がある。そのため、状況に応じて堅牢性の高い基盤にロボットを移行することを検討する。また何事も絶対はないため、同時多発的な停止を想定し、復旧優先度等も検討しておく。場合によっては、全社で策定しているBCPの対象シナリオにも加えることを検討する。 ・極めて高い可用性が求められる業務に対しては、RPAの適用を制限することも検討
				(6)	ロボット端末、RPAツール、ロボットなどRPAにかかわる構成情報が管理されていること。	どのようなロボット端末、RPAツール、ロボットを利用しているかを特定し、台数、管理者、バージョン、ライセンスなども含めた管理台帳等を整備し、管理することが望まれる。	・RPAツールがインストールされている端末、ツールの種類、ライセンスの種類、バージョン等について管理責任者、担当者を明確にし、台帳管理を行う。また、当該台帳が適切に管理されているかを確認するために定期的にモニタリングを行う。 ・RPAツールによってはexe形式のインストール不要なものが存在する。この様な形式のものは、上記台帳から漏れる可能性があるため、その様な形式のツール導入は禁止にするようなルールを策定する。またRPAベンダーと基本契約を結ぶ場合は、exe形式の製品は出荷しないような条項を入れることも検討する。
	d-5	セキュリティ管理	【COBIT】 APO13、DSS05 【監督指針】 Ⅲ-3-7-1-2-(4)-③、 Ⅲ-3-7-1-2-(4)-⑥、 Ⅲ-3-7-1-2-(5)-①	(1)	内部不正やサイバー攻撃によるセキュリティリスクに応じて、RPAに対して求めるセキュリティ管理要件やセキュリティ対策を検討・実装する手続きを明確化すること。	セキュリティ管理要件は、ロボット端末、ロボット管理サーバー、ロボットが取り扱うデータ、ロボットが操作する情報システムなどについて検討し、定めることが望まれる。求めるセキュリティ管理要件として、設置場所、パッチ適用、マルウェア対策ソフトの導入、端末内に保存するデータの保護、ログの取得・分析、ロボット端末がウイルスに感染した際の対応整備、リスク分析などがある。また、セキュリティ対策の検討には、情報システム部門などのセキュリティの専門知識を有する部門が関与するプロセスとすることが望まれる。	・ロボット端末については、社内の端末管理ルールに従う。 ・ロボット管理サーバーについては、社内のシステム管理ルールに従い、人のアクセス制限等、セキュリティが担保された区画(サーバールーム等)に設置する。 ・ロボット管理サーバーを設置する際には、社内の情報セキュリティ部門が定める情報セキュリティ方針に従い、セキュリティ審査等の審査を経た上で利用を開始する。 ・ロボット管理サーバーへの論理的なアクセスについては、アクセスログを保管し、許可されていないアクセスがされていないかを定期的に確認する。 ・ロボットが扱うデータについては、情報の取り扱いに関する社内ルールに従い、情報の重要度や管理レベルに応じた扱いをする。
				(2)	ロボットの改ざんやロボットの不正実行などを防止するため、ロボットへのアクセスは必要最小限な者に限定するための手続きを明確化すること。	ロボット管理サーバーやロボット端末へ不正にアクセスされると、ロボットを悪用した不正な業務を実行される恐れがある。そのため、ロボットへのアクセス(端末・サーバーへの物理的なアクセス、OSやアプリケーションへの論理的なアクセス)や各種操作権限(高権限の利用制限、リリース権限の限定、実行権限の限定など)について適切に管理し、モニタリングすることが望まれる。	・ロボット端末の利用に際しては、離席時の画面ロック徹底やログインID・PWを貼り出さないこと等、社内の端末管理ルールに従い、利用する。 ・ロボット端末の管理者権限は、社内の端末管理ルールに従い、ユーザー部門には開放しない。 ・ロボット管理サーバーの利用に際して、管理者権限はサーバー運用部門内のみの利用として、ユーザー部門へ開放しない。 ・ロボット管理サーバーでは、論理的なアクセス履歴を取得し、許可されていないアクセスがないかどうか、定期的にチェックする。

	大項目	小項目	概要	参考	ポイント	解説	対応方法(例)	備考		
d	プロセス (続き)	d-5	セキュリティ管理 (続き)	【COBIT】 APO13、DSS05 【監督指針】 Ⅲ-3-7-1-2-(4)-③、 Ⅲ-3-7-1-2-(4)-⑥、 Ⅲ-3-7-1-2-(5)-① (続き)	(3)	情報システムなどにアクセスするためにロボットが使用するIDやパスワードは、管理者を定め、不正に使用できないように管理する手続きを明確化すること。	ロボットが使用するIDは、ロボット実行者自身のIDを使用する場合と、ロボット専用のIDを作成する場合がある。ロボット実行者自身のIDを使用する場合は、ロボットプログラム内への記載禁止やログへの出力禁止など、他者が閲覧できないように管理する必要がある。ロボット専用のIDの場合は、その管理者を定め、ロボットの実行以外の手段で当該IDを使用できないようにパスワードの管理や利用状況のモニタリングを行うことが求められる。	・情報漏洩やロボットの不正利用に繋がるため、ロボット実行者自身のIDを使用する場合も、ロボット専用IDを使用する場合も、原則ID・PWのロボットプログラム内への記載は禁止する。 ・ロボット専用IDを使用する場合、当該IDの管理者を定める。またその場合は、ロボット専用ID管理者の職務権限以下の権限を付与することより、各IDの権限設定を適切に管理する必要がある。 ・ロボット実行者自身のIDを使用する場合は、各利用者が社内ルールに従い、ID・PWの漏洩を防止するよう努める。 ・共有のロボット専用IDを使用する場合は、利用時に個人を特定できるよう、ID利用者を利用の都度、管理簿へ記録したり、踏み台サーバーを用意し、自動で利用者を特定できるような仕組みを整備する。 ・ロボット専用IDを使用する場合(個人割り当て・共有ともに)は、ロボットの実行以外に不正利用される危険があるため、ロボット実行以外に使用されていないことを定期的にチェックする。 ・ロボットが出力するログに対するセキュリティを担保すること。		
					(4)	ロボットが取り扱うデータに対するアクセス制御や管理手続きを明確化すること。	ロボットが取り扱うデータとして、情報システムからダウンロードするデータファイル、それを加工した作業ファイル、処理完了後の出力ファイルなどがある。それらのファイルは、データの機密性に応じて閲覧可能な者のみがアクセスできる領域に保存する必要がある。異常が発生などにより、ロボットが途中で停止した場合のロボットが処理中のファイルの保存間所も考慮が必要である。	・ロボットが操作対象システムからダウンロードするデータについては、ロボットが使用するIDの権限設定において、ロボット実行者の職務権限に応じて、適切に制限し、ロボット実行者の職務権限上、アクセス不可の情報はダウンロードできないよう制限する。 ・ロボットが加工した作業ファイルや、処理完了後の出力ファイルは、原則ロボット端末のローカル環境への保存はせず、社内の共有フォルダ等、アクセス制限がされている環境へ保存する。 ・ロボット実行中に停止する場合に備えて、ロボットプログラム内にロールバック処理(処理途中でエラーが発生した場合、処理を巻き戻す処理)を組み込む等、処理途中のデータが出力されないよう制限する。		
		d-6	各種法令・内部統制・コンプライアンス 対応	RPAを適用する業務が各種法令・内部統制・コンプライアンスに該当するか否かを明確化し、ロボットで行う処理がそれらに対応するよう設計・運用するプロセスを明確化する。	【COBIT】 MEA03	(1)	各種法令、内部統制、コンプライアンスなどに影響をおよぼすロボットかどうかの基準や判断する手続きを明確化すること。	個人情報の取り扱い、内部統制にかかわる承認処理などを行うロボットを作成し、利用する場合は、各種法令、内部統制、コンプライアンスの範囲内でのロボットの処理や業務プロセスとする必要がある。そのため、どのようなロボットを開発・利用する場合にその考慮が必要かの基準を明確にし、その開発を許可する場合の手続きを整備することが望まれる。なお、関連会社、子会社、事業所等の海外拠点でRPAを適用する場合は、現地の法令や個人情報の取り扱いにおいて順守すべきルール等を確認し、それらに対応することが求められる。	・ロボット開発を開始する前に、開発するロボットが各種法令や内部統制、コンプライアンス等に関する業務に利用するものか確認する。 ・当該業務に使用する場合、実際に当該業務に影響をおよぼすものか確認する。例えば、以下の様な視点で確認することが考えられる。 - 法令上求められるデータの記録にかかわるものか、誤った記録や上書きを予防・発見できるか - 外部に提出したり公表するデータについて、ロボットの誤処理を予防・発見できるか - エラーニング受講やオンラインテスト等、人が必ず行わなければならないものを自動化するの か 等 ・上記の様に、明確に影響度を分析できない可能性がある場合、ルール上に利用禁止事項として明確化したり、確認する仕組みを構築する。	・必要に応じて、d-1の「ロボットの重要度・リスク度合い」の考え方と整合を取ることも考えられる。
						(2)	各種法令、内部統制、コンプライアンスなどに影響をおよぼす可能性のあるロボットの利用を許可する場合、RPAの管理体制や管理ルールはそのリスクを踏まえたものとする。	各種法令、内部統制、コンプライアンスなどに影響をおよぼす可能性のあるロボットに対しては、ロボットで行う処理や取り扱うデータ、ログの網羅性や正確性を確実にするため、ロボットのテストや監視の強化や処理結果を人が確認するなど、追加的な管理ルールを定めること、またそれを実現するための管理体制を整備することが求められる。	・各種法令や内部統制、コンプライアンス等に影響するロボットについては、ロボットの処理結果を確認する手続きや開発時の有識者の参画等、リスク低減策を検討する。ロボット開発の承認者は、それらリスク低減策等を加味し、開発可否を決定する。(上記ロボットの処理結果を確認する手続きは、それ自体もロボットに行わせる方法も考えられる。) ・ロボットをリリースする際には、有識者によるレビューが行われているか、処理結果を確認する手続きが業務マニュアル上明確化しているか等、上記リスク低減策の実施状況を確認の上、リリース承認を行う。	
		d-7	導入効果や管理状況の モニタリング	RPA導入による効果やリスクへの対応状況、ロボットの管理状況をモニタリングするためのプロセスを明確化する。	【COBIT】 APO04、APO06、MEA01～03 【監督指針】 Ⅲ-3-7-1-2-(3)-③、 Ⅲ-3-7-1-2-(4)-⑨	(1)	RPA導入目標(KPI)とその達成状況をモニタリングする仕組みが整備されていること。	RPAを導入すること自体が目的となり、自動化が限定的なロボット、処理異常が頻発するロボット、使用されていないロボットが改善されないままとならないように、企画時に立てたKPI等の目標に対するロボットの導入効果を定期的に測定し、目標の達成状況を評価することが望まれる。導入効果として、業務時間削減といった定量的な効果に加え、自動化による品質の向上や人の付加価値業務へのシフトによる業務創造効果などの定性的な効果も合わせて評価することが望ましい。	・各ロボットの導入効果を明確化するだけでなく、測定方法を予め検討しておく。その上で、導入後に導入効果の測定を行う。など導入効果は、すぐに効果が出るものと、時間がかかるものがあることに留意する。また効果が出ていない場合、利用部門には効果を上げるためのアクションプランを策定してもらう。 ・時間削減等といった効果が十分に出ていなくても、業務ストレスが緩和されている等といった見えにくい効果が出ている場合がある。このため、例えばアンケート等によって、見えにくい効果を確認することも検討する。 ・時間が削減できていたとしても、付加価値業務へのシフト等が行われていないと意味がない場合がある。効果測定においては、その様に付加価値業務へのシフト状況等も確認する。	
						(2)	各RPA利用部門でのロボットの導入状況や、各ロボットの重要度・リスク度合いを定期的に確認する仕組みが整備されていること。	許可されていないロボットが開発され、利用されていないことを確認するため、管理台帳等を整備し、各RPA利用部門のロボットの導入状況や各ロボットの重要度・リスク度合いの再評価を定期的に実施することが望ましい。	・どこにどのようなロボットが開発・利用されているか把握できるよう、ロボット管理台帳を作成する。 ・当該管理台帳は、更新漏れ等を定期的に確認し、実態と一致するよう維持管理を行う。なおその際、ロボットの重要度やリスク度合いについても再確認する。 ・全社RPA管理部門は、RPA利用部門が実施したロボット管理台帳の確認結果を収集し、それら結果の確認を行う。その際、重要度やリスク度合いの高いロボットがどこにあるのか、どの程度増えたのか確認する。また特段変更のない台帳については、形式的な確認となっている可能性があるため、必要に応じて回答したRPA利用部門にインタビュー等を行う。	

大項目	小項目	概要	参考	ポイント	解説	対応方法(例)	備考		
d	プロセス (続き)	d-7 導入効果や管理状況のモニタリング (続き)	RPA導入による効果やリスクへの対応状況、ロボットの管理状況をモニタリングするためのプロセスを明確化する。 (続き)	【COBIT】 APO04、APO06、 MEA01～03 【監督指針】 Ⅲ-3-7-1-2-(3)-③、 Ⅲ-3-7-1-2-(4)-⑨ (続き)	(3)	各RPA利用部門に対して、ロボットの開発・運用における管理ルールの順守状況を定期的に評価し、モニタリングする仕組みが整備されていること。	RPAを導入して時間が経つにつれて、利用者の増加・変更やロボットの増加により、管理ルールが守られなくなるおそれがあるため、ロボットの開発・運用において管理ルールが順守されていることを定期的に評価し、全社的なRPA推進・管理部門等が評価結果を確認することが望まれる。	・RPA導入状況(RPAツールの特性、ロボットの総数、重要度及びリスク度合いの高いロボットの数、インシデント発生状況等)を踏まえ、RPA利用部門に対しRPA管理ルール順守状況の確認を行う必要があるか検討する。 ・RPA管理ルール順守状況の確認を行う必要があると判断される場合、評価実施部門を検討すると共に、どのような手順で確認を行うか、評価アプローチも検討する。なお評価アプローチは、全ロボットを確認するのではなく、全体的なリスク傾向より部門毎に評価優先度を検討し、優先度の高い部門から評価、必要に応じてロボット自体の評価を行う(いわゆるリスクアプローチ)。 ・上記評価を行うにあたり、RPA管理ルール等から、各部門に求める管理水準を抽出し、評価シートを作成する。なお評価においては、順守していない事項があった場合、代替的・補完的な取り組みを行っているか確認し、それらが前述の各部門に求める管理水準を満たしているか検討を行う。 ・評価結果より、ルール未順守事項の改善を各部門に要請すると共に、それら評価結果を取りまとめ、既存の管理ルール改善箇所の抽出も行う。 ・これら一連の取り組みを手続き化し、モニタリングの仕組みとして確立する。	・本RPA管理ルール順守状況の確認は、会社として一定の管理水準を満たすための必要かつ重要な機能であることに留意する。 RPA導入が進み、ロボット数が増えれば増えるほど、その必要性、重要性は増す。 ・金融機関においては、システムリスク管理の中で類似の取り組みを行うことが当局から求められている。言い換えると、RPAに関しても同様の取り組みを行うことが求められる可能性が高い。
					(4)	技術発展や法制度変更などの外部環境の変化も踏まえ、全社的なRPAガバナンスの状況を内部監査や外部監査で評価し、必要に応じてRPAガバナンスの見直しを行っていること。	RPA技術の向上、AIやIoTなどの新たな技術・サービスの発展、法制度の変更、ビジネスや業務プロセスの変化等に対応するため、整備したRPAガバナンスは継続的に見直す必要がある。そのため、全社的なRPA推進・管理部門によるRPAの導入効果や管理状況のモニタリングも含め、全社的なRPAガバナンスの状況を内部監査や第三者評価で評価し、必要に応じて管理体制、管理ルール等のRPAガバナンスの見直しを行うことが求められる。	・定期的に以下の内容について確認し、RPA管理ルールや体制の改善箇所を検討、改善を行う。 - RPAにかかわる各種課題、インシデント内容 - 内部監査や外部監査指摘事項 - 他社におけるRPA失敗事例、インシデント事例 - 新たに採用した技術、もしくは採用予定の技術が既存のRPA管理ルール等によおよぼす影響 等 ・自社のみで改善箇所の検討を行うのが難しい場合、第三者評価を受ける等、社外専門家の知見を活用することも検討する。	
e	基盤	e-1 RPAツールに対する要求事項	利用するRPAツールについて、どのような要件が必要かを検討し、RPAツールを選定する。	【COBIT】 BAI03 【監督指針】 Ⅲ-3-7-1-2-(5)-⑤	(1)	さまざまなアプリケーションやテクノロジーとの親和性が高いこと。	RPA適用業務の拡大に伴うロボットが操作するアプリケーションや情報システムの対象の増加や将来的なOCRやAIなどのテクノロジーとの連携も視野に入れ、それらとの親和性の高いRPAツールを選定しておくことが望まれる。	・RPAルールに標準で準備されている機能類が業務で利用するアプリケーションの自動化と合致しているか、また機能類の豊富さを確認、検証する。 ・情報システムや、Web操作を行う場合、利用する端末の環境に影響されやすい画像認証や座標の記録ではなく、要素を認識して操作を自動化可能かどうかを検証する。 ・RPAツールとして、OCRやAIとの連携機能が付随しているか、または機能の追加を検討しているか等、将来的な利用方針を踏まえて検討する。	
					(2)	ロボット管理機能や異常時の通報機能、ログの出力機能など、ロボットの実行や管理を支援する機能が実装されているまたは拡張可能なこと。	より多くの業務やより重要な業務へロボットの利用を拡大するためには、変更・リリース管理、構成管理、アカウント管理、ログ管理、障害管理、セキュリティ管理など、通常の情報システムに求められるようなコントロールが必要となる。その際、RPAツールの機能で実現できない場合、人手による管理や管理システムの導入などが必要となり、想定していた効率化やコスト削減ができなくなる可能性がある。特に、デスクトップ型で小規模に導入を開始する場合は、ロボット管理サーバーを導入し、サーバー型に移行可能かを機能面やコスト面も含めて考慮しておくことが望まれる。	・RPAツールの選定時、特にロボットを重要な業務への適用を検討または予定している場合、例えば以下のような機能が実装されているかの観点で選定する。 - ロボットの開発、変更、リリース、利用における職務分離が可能か。 - 開発されたロボットのバージョン管理が可能な機能はあるか。 - ロボットの実行履歴や、設定変更履歴等、必要に応じたログの記録、管理が可能か。 - ロボットの実行状況の確認、スケジュール実行の設定、管理が可能か。等 ・デスクトップ型で一部の組織や部門でスモールスタートし、将来的に組織横断の横展開等でロボットの利用拡大を検討している場合、サーバー型へ移行が可能かを検討する。	
	(3)	RPAツールの脆弱性情報やセキュリティパッチが定期的に提供されること。	RPAツールにセキュリティ脆弱性があり、その脆弱性をついたサイバー攻撃によりロボット端末やロボット管理サーバーへの不正アクセスを受けると、ロボットが操作可能な情報システムへの二次攻撃の発生など被害が拡大する恐れがある。そのため、脆弱性情報やそのセキュリティパッチが定期的に提供されるRPAツールを選定することが望まれる。	・RPAツールの脆弱性情報やセキュリティパッチが定期的に提供されるか確認する。 またそれらの情報提供方法や、適用方法について確認する。					
		e-2 ロボットが操作するシステムに対する要求事項	ロボットが操作する社内または社外のシステムについて、どのような要件が必要かを検討し、ロボット操作対象とするシステムを決定する。	【COBIT】 BAI03	(1)	ロボットによるアクセスがルールやライセンスで制限されていないこと。	社内システムの場合、ロボットによる高速アクセスがシステムと与える影響、ロボット用IDの不正利用防止、アプリケーションのライセンス規約などを加味したルールを定め、その範囲内で利用する必要がある。また、外部のシステムの場合、利用規約などでロボットによるアクセスが制限されていないかを確認する必要がある。	・ロボットによる社内システムへのアクセスについて、当該システムへのロボットによる高速アクセスにより業務に影響が発生しないか、ロボット用IDを利用する場合はライセンス規約違反等が発生しないか確認する。必要に応じてロボットがアクセス可能な時間帯を制限したり、ロボットが操作可能な機能を制限する(参照権限のみ)等のルールを定める。 ・ロボットによる外部システムへのアクセスについて、特にロボット用IDを利用する場合は当該情報システムの利用規約等を確認する。	・新規開発する情報システムについては、アプリケーションレベルでアクセスログや操作ログを取得することを検討する。本ログは、RPAを安全に利用する上で必要となるだけでなく、例えばプロセスマイニング等を行う上でも有効となる。
(2)					アプリケーションレベルでのアクセスログや操作ログが取得可能であること。	情報システムへのロボットによるアクセスや操作を許可する場合には、不正使用の防止や誤操作の特定・復元のため、アプリケーションレベルでアクセスログや操作ログが取得可能であることが望まれる。特にロボット用IDを発行する場合は、ロボットの不正実行や当該IDを人が不正に利用したことを検知・特定するため、ログのモニタリングが必要となる場合がある。	・ロボットがアクセスする情報システムについて、アプリケーションレベルでのアクセスログや操作ログが取得されているか確認する。 ・アクセスログ、操作ログが取得されていない場合、その情報システムの特性(機密情報や高い完全性が求められるデータを保持する等)を踏まえ、ログの必要性を検討の上、ログの取得を行えるようシステム改修を行う。 ・アクセスログ、操作ログが取得されている場合、ロボットIDを用いた不正アクセスや不正操作を発見できるだけの項目があるか、ログ保存期間が適切か確認し、もし不足しているのであれば、システム改修を行う。 ・アクセスログ、操作ログは、取得しているだけでなく、定期的にその内容を確認する。なお確認は、ただ単に見て確認するのではなく、例えば申請書と照合する等、不正アクセス、操作を発見するための手続きを策定する。		

大項目	小項目	概要	参考	ポイント	解説	対応方法(例)	備考	
e	e-2	ロボットが操作するシステムに対する要求事項(続き)	【COBIT】 BAI03 (続き)	(3)	ロボットの誤処理やテスト処理で更新されたデータを特定し、修正するための機能が実装されていること。	ロボットの操作により誤ったデータが入力された場合に、それを識別し、データを個別に修正する機能が必要となる。また、本番の情報システムに対してロボットのテストを行う場合は、テスト処理によるレコードの追加や情報の更新をテスト後に戻すことが必要となる。	・システムに誤ったデータを入力してしまった場合、削除等、データを元に戻すことが可能なシステムを確認する。その内容を踏まえ、本番の情報システムを用いたロボットのテストについては、データを戻すことを条件に、本番の情報システムを用いたテストの実施を許容する。	・新規開発する情報システムにおいては、削除等、データを元に戻せる機能を実装することを検討する。
				(4)	システムの変更ににより、ロボットが行う業務に重大な影響をおよぼす可能性がある場合は、当該システムの管理部門と連携し、事前に対応の検討が可能であること。	ロボットの操作に影響を与える画面レイアウトの変更や出力ファイル形式の変更が操作対象の情報システム側で予告なく行われるとロボットの処理が異常となり、業務が停止する恐れがある。業務への影響やシステムへの変更頻度を考慮したうえで、必要に応じ、システムの管理部門と連携し事前に対応可能な仕組みを整備することが望まれる。	・ロボットがアクセスする情報システムについて、いつ、どのようなシステム変更が行われるか把握する。それに加え、当該情報システムに変更がある場合、ロボットの稼働に影響があるか否か検討する。必要に応じ、システムの管理部門とシステム変更内容について確認する場を設ける。 ・システム変更の頻度が多く、ロボットが停止する可能性が高い場合、その部分についてはRPAの適用可能性可否を検討する。	
	e-3	インフラ環境に対する要求事項	【COBIT】 BAI03～05	(1)	ロボット端末やロボット管理サーバーには、社内の端末や情報システムと同様のシステム管理にかかわるルールやセキュリティにかかわるルールが適用されること。	ロボット端末やロボット管理サーバーに対しても、求められる信頼性、性能、セキュリティなどに応じて、社内の端末や情報システムと同様のシステム管理ルールやセキュリティ管理ルールが適用され、ファンシリティ管理、バックアップ管理、ログ管理、セキュリティ管理等の対策が求められる。特にサイバーセキュリティリスクに関して、マルウェア対策ソフトの導入やネットワークの通信制限などの対策が求められる。	・ロボット端末やロボット管理サーバーのOSやDB、物理セキュリティ、論理セキュリティ等は、既存のIT・システムの管理ルールを提供する。 ・RPAの特性を踏まえると、例えばロボット端末がマルウェアに感染したとしても、そのことに気付くのが遅れる可能性がある。よってRPA導入を進めるにあたり、サーバーセキュリティ対策(特に内部対策)を確認し、必要に応じて改善する。	
				(2)	ロボット端末へのアクセスを物理的・論理的に制限するとともに、そのログをモニタリングすること。	ロボット端末へアクセスできる人の限定やOSの特権管理者アカウントの利用制限など、ロボット端末へのアクセスを制限する必要がある。加えて、ロボット端末へのアクセスログを取得し、必要に応じモニタリングすることが望まれる。また、ロボット端末の設置場所への入退制限や施錠による持ち出し制限など、物理的なアクセス制限も求められる。	・ロボット端末へのアクセスは、限定された者のみがアクセスできるよう制限する。 なお複数人が共有IDでロボット端末へアクセスする場合は、利用管理簿等に利用状況を記録する。ロボット端末への不正アクセス・操作を予防できない場合は、ログを取得し、定期的に利用管理簿と照合を行う。 ・ロボット端末として仮想デスクトップ環境を準備し、仮想デスクトップ上でロボットを稼働させ、許可された者のみがリモート接続で利用する。 ・ロボット端末の特権管理者アカウントは、RPA利用者が利用できないよう制限する。 ・(製品によってはロボット端末の画面が開いた状態でないと稼働しないものがあるため、そのような場合は)ロボット端末をセキュリティが確保されたエリア等に設置、保管する。	
				(3)	RPAツールを導入している端末を特定・把握し、ロボットの動作に影響をおよぼすような保守計画を把握する仕組みがあること。	許可しないロボットの開発や実行を防止するため、RPAツールを導入している端末を特定し、把握しておくことが望まれる。また、ロボット端末のOSのパッチ適用や端末内のアプリケーションのバージョン更新など、ロボットの動作に影響をおよぼすような保守計画が社内ですべて事前に連携されるなどのプロセスを整備することが望まれる。	・各端末へのRPAツールのインストールを制限する。またインストールする場合は、管理者の承認を必要とし、また必ずどの端末にインストールしたか記録する。 ・ロボット端末のOSのパッチ更新やOffice製品のバージョンアップ等、保守計画を確認する。それに加え、それら保守内容のロボットの稼働に影響があるか否か検討する。必要に応じ、端末管理を行っているインフラ担当者や当該保守内容について確認する場を設ける。	・RPAツールのインストール状況の管理方法(台帳管理)は、d-4・(5)を参照
				(4)	処理件数増加や高速・大量通信への対応等、ロボット端末やネットワークのスケーラビリティが高いこと。	RPA適用業務の拡大に合わせて、ロボット端末の増加やネットワークの増強が可能であることが望まれる。特に、頻繁に使用する情報システムとロボット端末のネットワークは、大量の通信の発生やネットワークによるレスポンスの影響等を考慮して設計することが望まれる。	・ロボット開発を行う際、当該ロボットが操作する情報システムへのアクセス数やどの程度増加するか把握する。また大量データの伝送等を行うかも確認する。それら結果を踏まえ、情報システムやネットワークのパフォーマンスへの影響を確認する。万一パフォーマンスへ影響をおよぼす場合、当該ロボットの開発を制限したり、基盤増強等を検討する。 ・情報システムへのアクセス数やレスポンスタイム、CPU使用率、メモリ使用率等を定期的に確認する。またネットワークのトラフィック量を定期的に確認する。万一パフォーマンスが悪化している場合、それがロボットによるものか確認し、必要に応じてロボットの開発を抑制したり、基盤増強等を検討する。	・新規開発する情報システムについては、RPA利用も視野に入れたスケーラビリティを検討する。

【お問い合わせ先】
PwCあらた有 限 責 任 監 査 法 人
RPAガバナンス担当
jp_aarata_rpa_gov@pwc.com

UiPath株式会社
ソリューション本部バリューデザイン部
jp-value-design-div@uipath.com

© 2019-2020 PricewaterhouseCoopers Aarata LLC. All rights reserved.
PwC refers to the PwC network member firms and/or their specified subsidiaries in Japan, and may sometimes refer to the PwC network.
Each of such firms and subsidiaries is a separate legal entity. Please see www.pwc.com/structure for further details.

© 2019-2020 UiPath Inc., UiPath SRL, UiPath K.K.

This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.