

Appendix 1. RPA関連リスクとコントロールのポイント

フェーズ	分類	項番	リスクの概要	リスクの種類			コントロールのポイント	参考(関連基準)
				可用性	完全性	機密性		
開発・変更	1 起案	1 開 1-1	承認を得ずにロボット開発が行われる等、リスクの高い業務でロボットが利用され、結果として業務に影響をおよぼす事象が発生する。		✓	✓	・開発するロボットの重要度/リスク度合いを定義し、開発起案時に開発する予定のロボットの重要度やリスク評価を行う。  ・それら評価結果をもとに、承認者による承認を得た後に開発を行う。  ・なお適用禁止の業務やロボットの利用制限等を予め決めておくことも望まれる。 (例:非常に高い可用性が求められる業務への適用は禁止等)	【COBIT】 APO12、BAI02 【監督指針】 Ⅲ-3-7-1-2-(3)-① Ⅲ-3-7-1-2-(6)-③
		2 要件定義・設計	1 開 2-1	要件定義が不十分等、業務要件に合致しないロボットを開発してしまう。	✓	✓	✓	・通常のシステム開発と同様、要件定義を行う。ただし、RPAは通常のシステムと違い、開発規模等が小さいため、通常のシステム開発より簡易的なものも許容可能だと考えられる。  ・ユーザー自身で開発し、ユーザー自身で利用するロボットは、いわゆる表計算ソフトのマクロの延長と捉えられる場合がある。その場合、対外的な影響有無や、後続の業務プロセス上のコントロール有無によっては、割愛することも検討する。
	3 開発	1 開 3-1	可読性の低いロボットを開発し、保守が困難となる。	✓			・通常のシステム開発同様、ロボットの開発標準等を定め、それらについての教育を実施し、当該標準に基づき開発を行うようにする。  ・なおRPAは、ユーザー自身が開発する場合があるため、ロボットの開発標準等は開発経験のないユーザーにも分かりやすいものである必要がある。  ・開発経験がない、または浅い者が開発する場合、コードレビューを行い、当該レビューを通してOJTで教育することも考える。	【COBIT】 APO07 APO11 【監督指針】 Ⅲ-3-7-1-2-(6)-③
		2 開 3-2	画像マッチングを多用したロボットを開発してしまい、システム変更等によってロボットが異常終了する可能性が高くなる。	✓			・原則、画像マッチングを禁止する。またそれをロボットの開発標準等に規定する。  ・場合によっては、RPA製品の選定時に画像マッチング以外の方法に強い製品を選定する。	【COBIT】 APO11 【監督指針】 Ⅲ-3-7-1-2-(6)-③
		3 開 3-3	開発者にロボットがアクセスするシステムのIDを貸与し、それらIDが不正に利用され、機密情報等が漏洩する。			✓	・開発者には、開発するロボットの用途に応じた最低限のIDを発行する。  ・機密性の高い情報を扱うロボット等、リスクの高いロボット開発を行う場合は、セキュリティの確保されたエリアや端末等で開発を行う。	【COBIT】 APO13、DSS05 【監督指針】 Ⅲ-3-7-1-2-(6)-③
		4 開 3-4	開発したロボットファイルや設定ファイルに直接記載されたID/PWが不正利用され、会計データや業務処理に影響をおよぼす。			✓	・ロボットファイルや設定ファイルには、ロボットが利用するID/PWの記載を禁止する。またそのことを開発標準等に規定する。  ・ID/PWは、ロボット実行の都度、人に入力させたり、システム等で集中管理したりすることで、ロボットファイルに直接記載しないロボット開発を行う。	【COBIT】 APO11、APO13、DSS05 【監督指針】 Ⅲ-3-7-1-2-(6)-③
	4 テスト	1 開 4-1	ロボットが要件定義通りに開発されていないことが発見されないことで、業務で利用する際、誤った処理が行われ、業務に影響をおよぼす。	✓	✓	✓	・通常のシステム開発同様、テストを行う。ただし、RPAは通常のシステムと違い、開発規模等が小さいため、通常のシステム開発より簡易的なものも許容可能だと考えられる。	【COBIT】 APO11、BAI03、BAI07 【監督指針】 Ⅲ-3-7-1-2-(6)-⑤
		2 開 4-2	本番環境のシステムとは異なる環境下でテストを行ったため、本番時に想定外の障害が発生する。	✓	✓	✓	・本番環境とテスト環境を同じ環境に整備しテストを行う。  ・本番環境とテスト環境に差異がある場合、差異を明確にし、テストへの影響を明確化した上でテストを行う。	【COBIT】 APO11、BAI03、BAI07 【監督指針】 Ⅲ-3-7-1-2-(6)-⑤
		3 開 4-3	本番環境のシステムを利用したロボットのテストにて、テストデータを当該システムに入力してしまい、業務に重大な影響をおよぼす。		✓		・本番環境を利用したロボットのテストを行う場合、ロボット実行後業務に影響を与えないよう、登録や更新をしたデータの回復を行う。  ・上記の対応が困難な場合、本番環境においてテストを行う場合には、システムへの入力や登録を行わないようロボットを制御した上でテストを行う。  ・テストを行えない部分については、初回本番稼働時等で確認を行い、業務への影響を及ぼさないよう注意しながら、ロボットの品質を確認する。	【COBIT】 APO11、BAI03、BAI07 【監督指針】 Ⅲ-3-7-1-2-(6)-⑤
	5 リリース	1 開 5-1	未承認のロボットを業務に使用し、業務に影響をおよぼす事象が発生する。	✓	✓	✓	・ロボットの開発者、運用者を職務分離する。  ・ロボットのリリースは、利用者によるテスト実施、およびテスト結果の承認を経た上で、運用者がリリースを行う。  ・リリース承認にあたっては、ロボットの重要度やリスク度合いに応じた審査項目を定義し、審査項目を満たすことを確認した上でリリースを行う。	【COBIT】 BAI06、BAI07 【監督指針】 Ⅲ-3-7-1-2-(6)-③
		2 開 5-2	ロボットをリリースする際にデグレージョンが発生し、業務に影響をおよぼすおそれがある。		✓		・ロボットファイル、および設定ファイル等の最新版は管理台帳等を利用して管理を行う。  ・ロボットのプログラムの変更を行う際は、処理概要等を記載するロボットの設計書等に記録して管理する。	【COBIT】 BAI10
	6 保守	1 開 6-1	ロボットの不具合が適切に修正されず、誤った処理結果が訂正されない。		✓		・ロボットの不具合を把握する仕組みを定め、ロボットの修正を行う際の手続き、体制を定める。	【COBIT】 DSS01、DSS02、 DSS03、 DSS04
		2 開 6-2	ロボットが操作するシステムや周辺環境の変化、RPAツールの仕様変更等が生じることで、ロボットの処理停止や異常処理が発生する。	✓	✓		・ロボットが操作するシステム、アプリケーションや周辺環境の変更計画を収集し、開発者や利用者へ情報共有を行う。  ・RPAツールの最新バージョンを導入する際、動作確認を行った上でバージョンアップの判断を行う。	【COBIT】 BAI06
		3 開 6-3	ロボットへの影響が考慮されないまま、RPA基盤やロボット端末へのパッチ適用や設定変更が行われることにより、RPA基盤やロボット端末が正常に動作しなくなることで、業務へ影響をおよぼす事象が発生する。	✓	✓		・RPA基盤やロボット端末へのパッチ適用や設定変更を行う際、RPA基盤やロボットへの影響をテストした上で、利用を開始する。	【COBIT】 BAI06
運用	1 ロボットの 実行	1 運 1-1	未承認のロボット実行スケジュール登録や誤設定により、不適切なタイミングでロボットが実行され、業務に影響をおよぼす事象が発生する。	✓	✓		・ロボットの実行スケジュール登録は、利用者がスケジュール登録を申請し、運用者が承認した上で、本番環境へ反映する。運用者がスケジュール登録を行い際には、2名体制で作業を行う等、作業ミスを防止する。	【COBIT】 DSS01
		2 運 1-2	本来スケジュールに則り、自動で実行されるべきロボットが、利用者により手動実行されることで、リソースの圧迫や異常終了、誤処理が発生し、業務へ影響をおよぼす。		✓		・スケジュールで実行すべきロボットと利用者が手動で実行すべきロボットは分離して管理し、スケジュール実行すべきロボットは、利用者が手動実行できないように設定を行う。	【COBIT】 DSS01
		3 運 1-3	利用者が誤ったロボットを実行したり、二重に実行したりすることで、異常終了や誤処理が発生する。	✓	✓		・利用者が実行できるロボットは、業務上必要な最低限のものとする。  ・ロボット利用手順書等を作成し、ロボットの処理内容や利用上の禁止事項等を利用者に周知する。	【COBIT】 DSS01
	2 オペレー ション管理	1 運 2-1	RPA基盤やロボット端末に対する定例作業の作業漏れや作業ミスにより、業務へ影響をおよぼす事象が発生する。	✓			・定期保守や月次処理等、定型的に行う作業が明確化され、RPA基盤にかかわる定例作業一覧等を作成し整理されていること。  ・各定例作業における作業の確認、実施、結果確認まで一連の手続きがRPA基盤にかかわる定例作業手順書等を作成し整理されていること。	【COBIT】 DSS01
		2 運 2-2	RPA基盤やロボット端末に対する非定例作業について、未承認または誤った作業を実施し、業務に影響をおよぼす事象が発生する。	✓	✓		・非定例作業を行う場合に必要な承認手続きを定めること。  ・作業を行う際には、2名体制で作業を行う等、作業ミスを防止する。	【COBIT】 DSS01
	3 ロボットが 使用する データ・ システムの 管理	1 運 3-1	ロボットから出力されたファイルやデータが改ざんされ、業務に影響をおよぼす事象が発生する。		✓		・ロボットが生成するデータは、原則アクセスが制限されているロボット端末内の領域やファイルサーバー等に保存する。	【COBIT】 DSS05 【監督指針】 Ⅲ-3-7-1-2-(4)-⑥、⑦、⑧
		2 運 3-2	ロボットが取り扱う入力ファイルや操作する各システム・アプリケーションのデータが不正に差し替えられ、ロボットの実行や処理は正常に実施されたものの、結果として不正な処理となり、会計データや処理の信頼性が損なわれる。		✓		・ロボットが生成するデータやロボットが利用するインプットファイルや情報は、原則アクセスが制限されているロボット端末内の領域やファイルサーバー等に保存する。	【COBIT】 DSS05 【監督指針】 Ⅲ-3-7-1-2-(4)-⑥、⑦、⑧
		3 運 3-3	ロボットが取り扱うファイルやデータが、当該ファイルやデータの重要度に応じた取り扱いをされないことにより、社外秘とすべきデータが漏洩する。			✓	・情報の重要度、リスク度合いに応じた取り扱いを行うルールを定めること。  ・ロボットで取り扱う情報に応じて、ロボットの仕様や開発方法を定義し、ロボット開発標準等へ定めること。	【COBIT】 DSS05 【監督指針】 Ⅲ-3-7-1-2-(4)-⑥、⑦、⑧

フェーズ	分類	項番	リスクの概要	リスクの種類			コントロールのポイント	参考(関連基準)
				可用性	完全性	機密性		
運用 (続き)	4 リソース管理	1 運 4-1	ロボットに十分なリソースが与えられていないために、ロボットの実行遅延、異常終了が発生する。	✓			・RPA基盤、ロボットの稼働状況、異常終了を定期的に監視すること。 ・RPA基盤のリソースを管理する対象項目(例:CPU占有率やHDD容量)、注意を促す基準を定めること。 ・基準を超過した場合、必要となる対策を検討し、対策を講じること。	【COBIT】 BAI04
	5 構成管理	1 運 5-1	RPA製品のライセンス切れによりロボットを利用できなくなる。	✓			・利用するRPAツールの特性に応じたライセンス管理方法が定められていること。 ・有効期限が到来するライセンスについて、一定期間前に該当するライセンスを把握する手続きを定めること。	【COBIT】 BAI09
		2 運 5-2	各ロボット端末で利用できるRPAツールのバージョン、アプリケーション、台数等が把握できず、障害等の影響範囲が特定できない。	✓			・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作成し、管理すること。	【COBIT】 BAI09
	6 障害・問題管理	1 運 6-1	ロボットの処理が不完全・不正確に実施されたことが検知されず、業務に影響をおよぼす事象が発生する。		✓		・ロボットの実行状況を監視し、異常発生を適時に把握、通知する仕組みを構築する。 ・異常を検知した場合の手続き、連絡体制を定める。 ・利用者からロボットの異常等について問い合わせる窓口を設置する。	【COBIT】 DSS02 【監督指針】 Ⅲ-3-7-1-2-(10)-①
		2 運 6-2	大量のアラートが検出され、対応が必要なアラートに対処できない。		✓		・検知すべきアラートのレベルを定義し、不要なアラートは検出されないような仕組みを構築すること。	【COBIT】 DSS02 【監督指針】 Ⅲ-3-7-1-2-(10)-①
		3 運 6-3	ロボットの停止等、異常な処理が発生しても適切に復旧対応されない。	✓	✓		・障害のレベルに応じた報告/連絡態勢、指示命令系統が定められていること。 ・暫定対応、原因分析、恒久対応など障害発生からクローズまでの一連の手続きが定められていること。 ・発生した障害の影響を極小化するための体系的な仕組みが整備されていること。 ・障害発生状況、原因調査結果、各対応等の記録を残す手続きが定められていること。 ・障害発生を未然防止するための障害内容の分析、対策検討を行う手続きが定められていること。(例:過去の障害発生の傾向、キャパシティ管理の結果分析など) ・未対応の障害の有無について、定期的にモニタリングを行うこと。	【COBIT】 DSS02 【監督指針】 Ⅲ-3-7-1-2-(10)-②、③、④、⑤、⑦
		4 運 6-4	発生した異常事象に対して、根本原因が究明されず、同様の障害が再度発生してしまう。	✓	✓		・再発が想定される異常事象について、投入データの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。	【COBIT】 DSS03 【監督指針】 Ⅲ-3-7-1-2-(10)-⑥
	7 バックアップ	1 運 7-1	災害やシステム障害により、ロボットが保有する入力データや処理状況のデータ等の消失が発生し、業務に影響をおよぼす。	✓	✓		・バックアップの取得対象、取得サイクル、取得世代、保管場所、保管期間等を定め、定期的にバックアップを取得し、正常に取得されていることを確かめること。	【COBIT】 DSS04 【監督指針】 Ⅲ-3-7-1-2-(9)-⑥
		2 運 7-2	災害やシステム障害により、ロボット実行ファイルデータの消失をすることでRPAを利用した業務の復旧に時間を要する。	✓			・重要度に応じ、ロボットのバックアップの取得対象、取得サイクル、取得世代、取得バージョン、保管場所、保管期間等を定め、定期的にバックアップを取得し、正常に取得されていることを確かめること。 ・復旧時のバージョン管理を含めたリストア手順を定めること。	【COBIT】 DSS04 【監督指針】 Ⅲ-3-7-1-2-(9)-⑥
	8 モニタリング	1 運 8-1	管理ルール、開発標準等に従わないロボットが利用され、業務に影響をおよぼす。	✓	✓	✓	・すべてのロボットの利用者、関係者に対し、定期的に管理ルールの順守状況を確認すること。 ・すべてのロボットを定期的に棚卸し、利用されていないロボットを削除する仕組みを整備すること。	【COBIT】 MEA02 【監督指針】 Ⅲ-3-7-1-2-(4)-⑨
		2 運 8-2	ロボットが不正に変更され、業務に影響をおよぼす。	✓	✓	✓	・ロボットの変更履歴を把握できる仕組みを整備すること。 ・SOX業務等に利用しているロボットは、その変更履歴を把握し、定期的に変更の妥当性を確かめること。	【COBIT】 BAI06
	9 コンティンジェンシープラン	1 運 9-1	障害等でロボットが利用できなくなった場合に代替手段がなく、業務を継続することができない。	✓			・利用者はロボットが障害や誤処理で長時間利用できない場合を想定したコンティンジェンシープランを策定すること。 ・RPA基盤やロボット端末の損壊・停止に備えてコンティンジェンシープランを策定すること。 ・策定したコンティンジェンシープランは定期的に見直す仕組みを整備すること。	【COBIT】 DSS04 【監督指針】 Ⅲ-3-7-1-2-(5)-⑧ Ⅲ-3-7-1-2-(9)-①、③、④
	10 外部委託管理	1 運 10-1	外部委託によるRPAの不正利用が発生し、対外的な影響をおよぼす。	✓	✓	✓	・外部委託先管理のルールがRPAにも適用されていること、またはルールの周知徹底がされていることを確認し外部委託先を選定する。(特にユーザーが通常業務で利用するデータを外部委託先のロボ開発者に受け渡す場合、注意すること)	【COBIT】 APO10 【監督指針】 Ⅲ-3-7-1-2-(2)-② Ⅲ-3-7-1-2-(8)-①、②、③、④
アクセス 制限・ セキュリティ 管理	1 特権IDの管理	1 ア 1-1	RPA基盤の特権ユーザーIDやユーザー権限の変更ができる等の高権限ユーザーIDの使用が制限されていない場合、ユーザーID・権限の不正な追加や基本設定の更新が行われる等、結果として会計データや処理の信頼性が損なわれてしまう。		✓	✓	・RPA基盤の初期管理者IDのPWを導入時に変更すること。 ・RPA基盤の初期管理者IDを利用した未初認のアクセスがないか、定期的にモニタリングを行う。 ・特権ID、高権限IDの利用する場合は一時貸出等の手続きを定め、利用を制限する。	【COBIT】 DSS05 【監督指針】 Ⅲ-3-7-1-2-(5)-③
	2 ユーザーIDの登録・変更・削除・棚卸	1 ア 2-1	職務に対し、適切な権限が付与されていない場合、権限を保持している人員によるロボットの不正実行や不適切な設定変更等が行われ、結果として会計データや処理の信頼性が損なわれてしまう。			✓	【RPA管理サーバーOS/DBのID】 ・ロボット管理サーバーへのアクセス権の付与を行う場合必要な申請手続きを定義し、職務に対して適切な権限を付与し、管理する。 ・ロボット管理サーバーへの権限登録の際は、登録作業者とは別の担当者が当該権限について正しく登録されているかを確認する。 【ロボット端末のID】 ・ロボット端末へのログインIDは、ロボット利用者の職務に応じた権限とし、ログインした者が特定できるよう個人毎に発行する。 ・ロボット端末を共用利用する場合は利用者が特定できるよう利用状況を管理する。 【ロボットがアクセスする情報システムやアプリケーションのID】 ・ロボットがアクセスする情報システム等へログインする場合、情報システムへのログインがロボットによるものなのか、人によるものなのか見分けられるような仕組みを構築する。 ・ロボットがアクセスする情報システムの仕様等により、情報システムへのログインがロボットによるものなのか人によるものなのか判断ができない場合は、不正利用を予防または発見できる対策を講じる。またはロボットの権限を制限する等の対策を講じる。	【COBIT】 DSS05 【監督指針】 Ⅲ-3-7-1-2-(5)-③
		2 ア 2-2	不要になったユーザーIDが残存し、悪用されることで不正アクセスが行われる。		✓	✓	・RPA基盤、ロボットが操作するシステム、ロボット端末のユーザーIDは、不要になった場合、適宜に削除するまたは、当該IDの管理者に削除の申請をすること。 ・RPA基盤、ロボットが操作するシステム、ロボット端末のユーザーIDを定期的に棚卸すること。	【COBIT】 DSS05 【監督指針】 Ⅲ-3-7-1-2-(5)-③
		3 ア 2-3	IDの不正利用が発見できず、業務へ影響をおよぼす。			✓	・管理対象となるIDについて、アクセスログ、操作ログを一定期間保存する等、事後的に不正利用を検知できる仕組みを整備する。	【COBIT】 DSS05 【監督指針】 Ⅲ-3-7-1-2-(5)-③
	3 共有IDの管理	1 ア 3-1	共有IDを利用する場合、不正なアクセスや操作が行われた場合に個人を特定できない。		✓	✓	・IDは原則個人に対し1IDを付与することとする。 ・共有IDを利用する場合は、台帳を利用して一時貸出をする等、個人が特定できること。	【COBIT】 DSS05 【監督指針】 Ⅲ-3-7-1-2-(5)-③
	4 ユーザーIDの貸出	1 ア 4-1	正当な理由に基づき貸し出されたユーザーIDが悪用され、不正操作が行われる。		✓	✓	・IDの一時貸出手続きを定め、承認の上、IDの貸し出しを行う。 ・IDの貸し出し終了後、運用者は当該IDのPWを変更する。	【COBIT】 DSS05 【監督指針】 Ⅲ-3-7-1-2-(5)-③
	5 PW管理	1 ア 5-1	パスワードが漏えいしたり推測されたりすることで、不正にアクセス・操作され、会計処理に影響をおよぼすおそれがある。		✓	✓	・管理ルール上、文字数、文字種、有効期限等のパスワードポリシーを制定すること。 ・パスワードポリシーに沿った設定をシステム上行うこと。	【COBIT】 DSS05 【監督指針】 Ⅲ-3-7-1-2-(5)-③

フェーズ	分類	項番	リスクの概要	リスクの種類			コントロールのポイント	参考(関連基準)
				可用性	完全性	機密性		
アクセス制限・セキュリティ管理(続き)	6物理アクセス管理	1ア 6-1	RPA基盤が外部から不正アクセスされ、業務に影響をおよぼす事象が発生する。	✓			・RPA基盤の設置場所は、アクセスが制限される場所とし、ICカードでの入退館・入退室や監視カメラを利用して常時監視等を行う。  ・RPA基盤は施錠可能なラック等に設置し、その鍵は適切に管理する。  ・RPA基盤を冗長化し、一部が故障してもロボット実行に影響が出ない構成にする。  ・クラウド環境にRPA基盤を構築する場合、クラウド提供事業者における設備の管理状況等を確認した上で、事業者を選定する。	【COBIT】 DSS05
		2ア 6-2	ロボット実行中に画面がロックされないまま放置されたロボット端末に不正侵入され、ロボットの不正実行や処理中のアプリケーションの不正操作等により、業務に影響をおよぼす。	✓	✓	✓	・画面ロックしても実行可能なロボットを利用し、処理を行う。  ・画面ロックすると利用できないロボットの場合、実行中、ロボット端末から離れないことをルールとして定めること。また、離れる場合、画面ロックや施錠できるラック等セキュリティの確保された環境へ設置し、ロボット端末が不正に利用されないよう対策を定めること。  ・財務情報や個人情報等、極めて重要な情報を操作するロボットについては、ロボット端末はユーザーがログインできないロボット専用端末とし、施錠できるラック等セキュリティの確保された環境に設置し、原則人が触らない。  ・ロボット端末の利用には、ID/PWの入力を要するように設定する。	【COBIT】 DSS05
		3ア 6-3	RPA基盤の不正利用が発見できない。	✓	✓	✓	・RPA基盤の設置場所で取得した監視カメラの映像や入退室ログ等を定期的にモニタリングし、不正な侵入を検知する仕組みを整備する。	【COBIT】 DSS05
	7セキュリティ対策	1ア 7-1	RPA基盤やロボット端末にマルウェアが侵入し、端末が乗っ取られることで、本番データの改ざんや本番アプリケーションへの不正操作が行われることで、業務へ影響をおよぼす。		✓	✓	・ロボット端末のマルウェア感染や不正な遠隔操作等を防ぐために、IPSの導入や、振る舞い検知等を行っており、またシグネチャや定義ファイルは最新のものに更新している。  ・ロボット端末のマルウェアが侵入し乗っ取られた際の被害の拡大を防ぐため、ロボット端末がアクセス可能な社内システムの権限等は必要最低限のものとする。	【COBIT】 DSS05 【監督指針】 Ⅲ-3-7-1-2-(4)-③ Ⅲ-3-7-1-2-(5)-⑤

【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.