外部サプライヤー管理義務

技術リスク

2021 年 10 月付け第 11.0 版

1.老朽化の管理	継続的なサポート手配を確保する	サプライヤーは、直接または間接を問わず、製品にセキュリティ脆弱性がある場合を含め、Barclays へのサービス提供に使用する IT 資産のサポート提供能力に周知の変更がある場合、これを Barclays に直ちに知らせ、これらの IT 資産の適時のアップグレードまたは撤去を行うものとします。	サポート対象外となるハードウェア・ソフトウェア資産、または旧式のハードウェアやソフトウェアに依存する技術サービスに関する記録および/または手続きが不十分である場合、許容できないパフォーマンス、不安定性、セキュリティの脆弱性、ビジネスの喪失、および過大な移行コストが発生する場合があります。
2.インシデント処理	インシデントの記録、分類、解決	サプライヤーは、すべての運営上のインシデントが一次連絡先において、あるいは適時の適切な上申により、適切に識別、記録、優先、分類され、速やかに解決されるよう IT システムおよびサービスの運営に関するインシデント処理体制を構築するものとします。これには、重大インシデントの速やかかつ効果的な処理のための堅牢なプロセスを設けることが含まれます。	技術インシデントが適時に報告されない場合、または十分な説明がされない場合、あるいは必要な是正措置が取られなかった場合、回避できたはずのシステム/サービスの中断またはデータの破損や消失が発生する場合があります。重大インシデントは、これらがビジネスに重大なリスクを呈するインシデントであること、また深刻な機能停止、評判の喪失、財務上の影響、中核ビジネスプロセスへの影響などの重大な結果を招きかねないため、強化・緊急対応が必要となります。
3.問題の管理	技術的問題の特定、評価/分析、および解決	サプライヤーは、根本原因分析を通じてかかる問題が特定、記録され、インシデントの再発の可能性と影響を最小限にするための効果的な解決策が講じられる、重大な技術インシデントの原因となった問題を適時調査するための体制を構築するものとします。また、サプライヤーは、頻度の高い、発生件数の多い反復インシデントの原因を特定、解決するために、定期的なインシデントの事前分析を行うものとします。	技術サービスの提供に影響を与えるインシデントの発生原因となった問題が適時に特定、解決されない場合、回避することができたはずのシステム/サービス中断またはデータの破損や消失が発生する場合があります。
4.変更管理	厳格な変更管理の実施	サプライヤーは、Barclays へのサービス提供に使用されるすべての IT 要素が、以下の目標をすべて考慮した厳格な変更管理体制下に管理されていることを確認するものとします： 1.適切な許可なしの変更は禁止 - 実施前に承認を得る必要がある 2.変更開始者、責任者、承認者と実施者の間の	技術サービスへの不正な変更または不適切な変更を防止するための変更プロセスが不正または不十分な場合、サービスの中断、データの破損、データの消失、プロセスエラーまたは不正が発生する場合があります。

		責務の分離 3.関連するリスクレベルに従った変更計画および変更管理 4.変更においては、影響を受ける技術要素のパフォーマンスおよび/または容量に対する潜在的な影響を十分に考慮する 5.変更においては、実施前にその変更に関連する技術的およびビジネス上のテストを受け、必要に応じ、その証拠を保存する 6.変更は実施後にテストされ、想定外の影響なしに成功裏に実現されていることを徹底する	
5a.技術復旧力	システム復旧計画 (SRP)	サプライヤーは、Barclays の復旧力カテゴリー 0〜3 を達成するために必要な各技術システム/サービス、および相当の復旧時間目標(RTO)と復旧時点目標(RPO)のためのシステム復旧計画(SRP)を備えている必要があります。計画は、少なくとも 12 ヶ月に 1 度、正確性を確認しなければなりません。 **注:** 復旧分類−0〜1 の技術システム/サービスで、復旧力対策のためにアクティブ/パッシブ構成で設計されているものに関しては、すべての要素が効果的に動作することを確認するため、システムの復旧環境を延長し、BAU として動作させて SRP を検証することが必要です。これは事実上、プロダクションクロスオーバー (PCO) イベントです。	システム復旧計画が不十分である場合、インシデント発生後にビジネスまたは顧客に提供する技術サービスにおいて許容できない損失が発生する場合があります。復旧関連文書を更新し、実践し続けることで、復旧計画を常にビジネスニーズに整合したものにすることができます。
5b.技術復旧力	データ整合性復旧計画 (DIRP)	サプライヤーは、Barclays の復旧分類 0〜1 を達成するため、必要とされる技術システム/サービスごとに、データの整合性および復旧計画 (DIRP) を備えている必要があります。計画は、少なくとも 12ヶ月に 1 度、正確性を確認しなければなりません。	データの損失は、悪意ある手段で発生する可能性があるため、私たちが直面する最大の脅威の 1 つです。 これはシステム障害でも発生する可能性があります。このシナリオのための計画を立てることは非常に重要であり、データのソースと依存関係を特定して理解する上で役立ちます。

5c.技術復旧力	データセンターの多様性	サプライヤーは、Barclays の復旧力カテゴリー0～3を達成するために必要な各技術システム/サービスは、データセンター間の復旧力を備えており、データセンターが単一のイベントによって同時に影響を受けるリスクを軽減するために十分に離れていることを確認するものとします。	データセンターは代替電源、ネットワークリンクなどを備え、単一のイベントによってデータセンターが同時に影響を受けるリスクを軽減するために、十分に離れた場所に設置する必要があります。
5d.技術復旧力	SRP の検証	サプライヤーは、システム復旧計画（SRP）のテストと検証を行い、技術システム/サービスが復旧して Barclays の規定する復旧分類要件 0～3 を満たしていることを示す必要があります。 復旧力対策としてアクティブ/パッシブ構成で設計されている、復旧分類要件 0 ～1 を達成するために必要な各技術システム/サービスについては、能力および完全な統合機能性（プロダクション・クロスオーバー）を証明するのに十分な期間、文書化された SRP に従ってパッシブ環境を構築し、BAU 本番環境として使用する必要があります。 検証頻度要件は、関連する復旧分類（レジリエンスカテゴリー）によって決定する必要があります。 - 復旧分類 0: SRP の検証は 12 ヶ月ごと、PCO は 3 ヶ月ごとに実施する必要があります。 - 復旧分類 1: SRP と PCO の検証は 12 ヶ月ごとに実施する必要があります。 - 復旧分類 2-3: SRP の検証は 24 ヶ月ごとに実施する必要があります。 いずれかのテストで該当する復旧力分類の最低復旧力要件を達成できなかった場合は、サプライヤーは速やかに Barclays に通知し、詳細に示した改善計画（実施すべき措置および対応完了日を含	サプライヤーが提供する技術システムは、Barclays のカスタマー・ジャーニーに影響を与える可能性があります。Barclays の事業運営をサポートするサプライヤーが、テストされた適切な復旧計画を備えていることを保証することは非常に重要であり、サプライヤー管理に適切なガバナンスを運用する上で Barclays に対する規制上の義務でもあります。 プロダクション・クロスオーバー（PCO）とは、アクティブ/パッシブ構成されたシステムのパッシブ・インスタンスが期待された通りに動作し、BAU 運用で必要とされるレベルまで動作するかどうかを検証する方法です。また PCO は、上流または下流のシステムに依存していても期待通りに機能し続けることができるかどうかを検証します。

		む）を提供するものとします。サプライヤーは、PCOを実施する前に通知するものとします。	
5e.技術復旧力	DIRP の検証	サプライヤーは、復旧中のデータの整合性を証明するために、Barclays の復旧分類 0～1 を達成するため、必要とされる各技術システム/サービスにごとに、データの整合性および復旧計画(DIRP)をテストし、検証する必要があります。検証は 12 ヶ月ごとに実施する必要があります。 いずれかの計画で該当する復旧力分類の最低復旧要件を達成できなかった場合は、サプライヤーは速やかに Barclays に通知し、詳細に示した改善計画（実施すべき措置および対応完了日を含む）を提供するものとします。	データは、様々な意味で悪影響を受ける可能性がある重大な要素です。データが正確で有効であることを実証するために、その復元、復旧、再作成のための文書化された計画を実施するものとします。
6.パフォーマンスと容量の管理	Barclays の技術ニーズに沿っていること	サプライヤーは、定められたビジネスニーズに沿って、Barclays へのサービス提供に使用されるすべての主要 IT 要素のパフォーマンスと容量の適切なレベルを定義するものとします。また、サプライヤーは、主なコンポーネントに適切な警告と閾値を設定することで、閾値への違反の可能性に警告を発し、またこれらを定期的に見直すことで、サービス提供が Barclays のニーズに沿ったものであることを徹底するものとします。	IT リソースのパフォーマンスおよび/または能力レベルを監視し、現在および将来の要件に沿うための対策が不十分、またはそれを維持することができない場合は、技術サービスにおいて許容できない低下および/または中断およびビジネス損失が発生する場合があります。 ビジネス/取引先のニーズの定義および/または文書が不十分な場合、技術サービスにおいて許容できないパフォーマンスおよび事業場の損失が発生する場合があります。

管理エリア	管理対象	管理内容	本件が重要である理由

7.技術アプリケーション開発	再現可能な品質保証の実施	サプライヤーは、Barclays へのサービス提供に使用されるそのすべてのシステムおよびサービスは、厳格で、徹底した、かつ再現可能な品質保証プロセスを受けていることを示すことができるよう徹底するものとします。これにはピアレビューまたは自動化ツールによる機能テストおよび非機能テスト、静的アプリケーションセキュリティテスト、コード品質保証が含まれますが、これらに限定されません。	テストおよび品質保証システムおよびサービスが不十分な場合、技術サービスおよびビジネスプロセスにおける機能性の想定外の重大な損失に到ることがあります。
	ビジネス成果の受け入れ	サプライヤーは 1 回限りまたは継続ベースで相互に受け入れ可能なビジネス成果の定義に合意するものとします。その定義により、IT システムおよびサービスの新規または更新リリースが Barclays に供給され、また Barclays により承諾されます。 これらの定義のフォームには、システムおよびサービスの十分な機能面および非機能面を記載する必要があり、既存のシステムマニュアル、詳細な相互合意要件を記載した文書、ユーザーストーリー、使用事例またはその他の適切なフォームなど、相互に合意された適切なフォームを採用することがあります。 サプライヤーは、Barclays と協力し、ビジネス成果が、全体または相互に合意された部分において、1 回限りまたは継続ベースで、Barclays のこれらの事前に合意済みの定義のビジネス受け入れに基づいて、必ず受け入れられるよう徹底するものとします。	システムの機能的および非機能的行動についての不十分な合意は、想定された Barclays のシステム行動からの逸脱に到ることがあり、ビジネスと事業運営プロセス上のリスクに到る恐れがあります。
8.システムおよびデータのバックアップに関する取り決め	適切で効果的なバックアップと復元プロセスの運用	サプライヤーは、Barclays へのサービス提供において使用されるすべての IT システムとサービスが Barclays のニーズに沿って運用され、定期的にその効果を証明するために十分なバックアップと復元プロセスが設けられていることを徹底するものとします。	ビジネスデータバックアップ体制が欠如している場合または不十分である場合、システム/サービスの中断、データの消失または不適切なデータの開示が発生する場合があります。

	安全でセキュアであり、信頼性の高いバックアップメディアの確保	サプライヤーは、Barclays へのサービス提供に関連するすべてのバックアップメディアを、それらのメディアの処理および保管に関する取り決めと共に、いかなる時にも安全かつ信頼できるように保つものとします。	ビジネスデータバックアップ体制が欠如している場合または不十分である場合、システム/サービスの中断、データの消失または不適切なデータの開示が発生する場合があります。
9.設定管理	生産環境の分離	サプライヤーは、Barclays に提供したプロダクションサービスには、非プロダクション要素への依存性がなく、安全でないまたは信頼できないサービスの提供が回避されるよう徹底するものとします。	既定の所有権およびサードパーティ依存性などの技術要素（ハードウェアおよびソフトウェア）の登録エントリーが不適切な場合、安全でないまたは信頼できないサービスやデータが発生する場合があります。プロダクションサービスの提供において非プロダクション要素を使用することは、それらがプロダクション標準に構築されていない、あるいはこうした標準により管理されないリスクを生みます。
	設定詳細の記録と維持	サプライヤーは、Barclays へのサービス提供に使用されるすべての対象設定項目の完全かつ正確な登録エントリーを維持管理するものとします（所有権および上流部門/下流部門の依存性/マッピングを含む）。サプライヤーは、データの正確性と整合性を継続的に維持するための管理体制を備えている必要があります。	不適切または不完全な登録エントリー（他の設定項目への関連する依存性/マッピングと合わせ）は、非効果的なインシデントおよび変更の影響評価の結果として安全でないまたは不安定なサービスおよびデータが発生するおそれがあります。
10.ハードウェア資産マネジメント	ハードウェア資産詳細の記録と維持	サプライヤーは、資産のライフサイクルを通してハードウェアの資産データの記録および継続的な保守を保証するための管理を実施するものとします。 サプライヤーは、Barclays へのサービス提供において使用される、すべての IT ハードウェア資産の完全で正確な登録エントリーを維持管理するものとします。	既定の所有権およびサードパーティ依存性などの技術ハードウェア資産の登録エントリーが不適切な場合、安全でないまたは信頼できないサービスやデータが発生する場合があります。ハードウェア資産の消去および処分を安全に行えなかった場合、財務上、風評上、規制上の損害が発生する場合があります。
	資産の廃棄	すべての資産処分については、関連する Barclays セキュリティ標準の要件に沿って、正	サプライヤーは、資産が正しく処分されたかどうかの正式な確認（銀行データの安全な破棄を含む）を取得し、記録する

		式な廃棄プロセスに従い、すべての Barclays データを完全に消去し、安全に処分するものとします。	ことが重要です。ハードウェア資産の消去および処分を安全に行えなかった場合、財務上、風評上、規制上の損害が発生する場合があります。
	資産の喪失	すべての「紛失・盗難資産」は適切に調査し、見つからなかった場合には Barclays に報告し、リスクの承認を得るものとします。	サプライヤーは、紛失資産を徹底的に調査し、見つからなかった場合には Barclays に報告し、リスクの承認を得ることを保証するための管理体制を備えていることが重要です。ハードウェア資産を紛失し、消去および処分を安全に行うことができなかった場合には、財務上、風評上、規制上の損害が発生する場合があります。

管理エリア	管理対象	管理内容	本件が重要である理由
11.ソフトウェア資産マネジメント	ソフトウェア資産/インストール詳細の記録と維持。ソフトウェア資産ライセンシング	サプライヤーは、Barclays へのサービス提供において使用されるすべての対象 IT ソフトウェア資産およびそのインストールの完全で正確な登録エントリーを維持管理するものとします（所有権を含む）。サプライヤーは調達から処分（およびインストールから取り外し）まで、データの正確性と完全性を維持管理するものとします。また、サプライヤーはソフトウェアの使用が常に既定のライセンス条件に沿ったものであるよう徹底するものとします。	既定の所有権などの技術ソフトウェア資産の登録エントリーが不適切な場合、安全でないまたは信頼できないサービスやデータが発生する場合があります。権原に照らしたソフトウェアの使用を管理できない場合、財務上、風評上、規制上の損害が発生する場合があります。

技術復旧力の定義

復旧時間目標(RTO)	RTO とは、予想外のサービスの不具合または中断から合意されたサービスレベルでのオペレーション再開までの目標時間を指します。
復旧時点目標(RPO)	RPO とは、復旧プロセスの開始時点における利用できるデータの目標ステータスを指します。回復状況において許容できる最大のデータ損失尺度です。

プロダクション・クロスオーバー(PCO)	PCO とは、アクティブ/パッシブ構成で設計されたシステムの代替 (DR) インスタンスを有効にし、これを本番用のインスタンスとして長期間使用して、完全な機能と能力を検証することです。
システム復旧計画	システム復旧計画とは、システムまたは不具合のあったコンポーネントを運用状態に戻す方法の技術的な要素および詳細を定義した文書を指します。
データ整合性および復旧計画	データの整合性および復旧計画とは、システム障害や悪意により失われたデータを復旧するための手順を記載した文書を指します。 計画は、関連するオプションを含むシナリオに対応する必要があります（例: 他のシステムからのデータ再生、テープアーカイブからのデータ復元、またはデータの再作成など）

Barclays の復旧分類マトリックスによる復旧力要件

復旧分類	0	1	2	3
復旧時間目標(RTO)	最高 5 分	最高 4 時間	最高 12 時間	最高 24 時間
復旧時点目標(RPO)	最高 5 分	最高 15 分	最高 30 分	最高 24 時間