BARCLAYS

# 外部サプライヤー管理義務

## 技術リスク

2019 年 3 月付け第 9.0 版

| 管理エリア | 管理対象 | 管理内容 | 本件が重要である理由 |
| --- | --- | --- | --- |
| 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：<br>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 | IT リソースのパフォーマンスおよび/または容量レベルを監視し、現在および将来の要件に沿うよう維持するための対策が不十分な場合、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。また、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十分な場合、サービスの中断、データの破損、データの |

| | | | |
|---|---|---|---|
| | | 2.変更開始者、責任者、承認者と実施者の間の責務の分離<br>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<br>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<br>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<br>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 | 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。 |
| 5.サービスの継続 | 適切な回復/復旧に関する取り決めの提供と検証 | サプライヤーは、Barclays に提供する各 IT システムおよび各サービスに関する Barclays の復旧/回復ニーズを理解し、これに合意するものとします。復旧および回復計画を維持し、その正確さを確認し、サービス継続取り決めは適切に文書化され、信頼できるもので、ビジネスニーズに沿ったものであることを実践/実証するものとします。 | サービス継続計画が欠如している場合、または不十分である場合、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。 |
| 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。 | ビジネス/取引先のニーズに関する定義および/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ビジネス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。<br><br>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。<br><br>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 | 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 |

| | | | |
|---|---|---|---|
| | | 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。 | 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完全性を維持管理するものとします。 | 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、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 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（必要に応じ所有権とラベリングを含む）。サプライヤーは調達から処分まで、資産のライフサイクルを通じたデータの正確性と完全性を維持管理するものとします。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。 | 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。 |
| **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。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。 |