External Supplier Control Obligations

復旧計画

2024年10月付け最終第14.0版

1. 定義：

破壊的なイベント	原因に関わらず、サプライヤーが復旧の実施および復旧に関する計画と機能を通じて緩和することを選択したインシデントの影響の記録を指します。 **サイバーイベント、自然災害、人為的災害などの傷害が発生すると、組織の業務が中断される場合があります。**
インシデント	日々の事業活動の一環として、復旧計画を発動することで管理される破壊的なイベントを指します。
復旧計画	サービスを運用ステータスに戻すために実行する手段と措置を詳述した文書を指します。これらは事業継続計画（またはこれに類似した用語）と呼ばれる場合があります。
復旧計画	ビジネスサービス、業務プロセス、および基盤となる依存関係の復旧のプロセスまたは計画を指します。
復旧時間目標	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業務再開までの目標時間を指します。
復旧時点目標	復旧時点目標（RPO）とは、「復旧プロセスの開始時点におけるデータの可用性の目標状態」として定義されています。回復状況においてビジネスで許容できる最大のデータ損失の尺度です。
復旧力分類	復旧力分類は、Barclaysが重大度と影響に基づいてサービスに復旧力要件を適用するために使用する評価です。復旧力分類は、RTO（Recovery Time Objective：復旧時間目標）、RPO（Recovery Point Objective：復旧時点目標）、検証頻度の要件の向上に役立ちます。
許容できない被害	お客様/消費者/クライアント、金融市場、またはBarclaysの安全性と健全性の観点から、サービスの中断が許容できなくなる時点。
リソースの依存関係	ビジネスサービスを提供するために必要な依存関係（テクノロジー、サードパーティサービス、人員）。

2. 復旧力重大度表：

サプライヤーのサービスに対し、特定の復旧力分類（0~4）が割り当てられます。これは、サービスが中断した際にBarclaysに与える影響に基づいて、Barclaysがサプライヤーに求める復旧目標を反映したものです。復旧力分類が高い（数値が小さい）ほど、Barclaysにとってのサービスの重要度に応じて、より高いレベルの復旧力と回復力が求められます。サプライヤーは、契約サービスに関してBarclaysが規定する該当の復旧力分類に対して「復旧力重大度表」に記載されている復旧要件を達成するよう徹底するものとします。「復旧力重大度表」は、復旧力分類に基づいて適用可能なコントロールを示したものです。コントロール要件の詳細は、セクション3（**コントロール**）をご覧ください。

リスク影響評価	非常に高い影響	高い影響	中程度の影響	低い影響	非常に低い影響
復旧力分類	0	1	2	3	4
RTOターゲット	1時間以内	4時間以内	12時間以内	24時間以内	計画されているリカバリはありません
RPOターゲット	5分以内	最高15分	最高30分	24時間以内	計画されているリカバリはありません

技術テストの頻度	復旧力分類0	復旧力分類1	復旧力分類2	復旧力分類3	復旧力分類4
システム復旧計画の検証	年に2回以上	年に2回以上	12ヵ月に1回以上	24ヵ月に1回以上	計画されているリカバリはありません
データ復旧計画の検証	本番環境と同様の環境での計画の年次検証	デスクトップウォークスルーによる年次検証	12ヵ月に1回以上	任意	計画されているリカバリはありません
プラットフォームおよびアプリケーションの再構築計画の検証	デスクトップウォークスルーによる年次検証	デスクトップウォークスルーによる年次検証	任意	任意	計画されているリカバリはありません

サプライヤー管理の適用範囲	復旧力分類0	復旧力分類1	復旧力分類2	復旧力分類3	復旧力分類4
1.復旧計画に含めるためのリソース依存関係マッピング要件	✔	✔	✔	✔	O
2. 破壊的なイベントに対する復旧計画の要件	✔	✔	✔	✔	O
3. 事業復旧計画および検証要件	✔	✔	✔	✔	O
4. 統合テスト要件	✔	✔	O	O	O
5. システム復旧計画および検証要件	✔	✔	✔	✔	O
6. データ復旧計画および検証要件	✔	✔	O	O	O
7. データセンターの多様性およびクラウドサービスプロバイダーの要件	✔	✔	✔	✔	O
8. プラットフォームおよびアプリケーションの再構築計画の要件	✔	✔	O	O	O

✔= 必須	O= 任意

レビュー中に問題が特定された場合、または管理のテスト中に要件を満たせなかった場合、当該サプライヤーはBarclaysに速やかに（通常は10日以内に）それを通知し、合意した日までに問題を是正する必要があります。

3. 管理：

サプライヤーは、該当する業界のベストプラクティスと適用される規制要件に沿って運用と技術の復旧力要件を管理するポリシーと基準文書でサポートされている、復旧力（事業継続および災害復旧）に対する構造的アプローチを有している必要があります。復旧力に対する構造的アプローチは、経営陣が監督し、有効性について毎年レビューおよび評価しなければなりません。

管理対象	管理内容	本件が重要である理由
1. 復旧計画に含めるためのリソース依存関係マッピング要件	サプライヤーは、Barclaysにサービスを提供する上で重要なリソース依存関係を定義し、文書化する必要があります。これらの依存関係は、適切に維持され、12ヵ月ごと、または重要な変更が発生した際に見直す必要があります。 考慮すべきリソース依存関係： ▪ 技術およびデータ（社内および下請業者から提供）。 ▪ 重要な下請業者（Barclaysへのサービスのパフォーマンスと提供に重大な影響を与える可能性がある下請業者）。 ▪ 労働力（人員の喪失。作業エリアの復旧戦略または在宅勤務能力の有無については考慮しない）。	サプライヤーはBarclaysにサービスを提供するために、リソースの依存関係を理解し、文書化するものとします。リソースの依存関係は、サプライヤーのビジネス復旧計画の一部を構成し、これらがインシデントの影響を軽減し、Barclaysにサービスを提供できなくなる状況を回避するために考慮されるようにしなければなりません。
2. 破壊的なイベントに対する復旧計画の要件	サプライヤーは、復旧計画の範囲で破壊的なイベントを定義し、合意されたサービスレベルおよび対応する復旧時間目標内で確実にサービスを提供するために必要な計画のレベルを定義する必要があります。サプライヤーは、破壊的なイベントが現在のリスク/脅威の状況を反映したものであり、その重大度と妥当性が評価され、業界の洞察およびインテリジェンスによる洞察によって裏付けられていることを確認する必要があります。 最低条件として、サプライヤーは計画の範囲に以下の破壊的なイベントを含める必要があります。 ▪ Barclaysへのサービス提供に影響を与える複数の拠点における建物の損失（建物および関連するインフラストラクチャが使用できない状態）。 ▪ データの破損、サイバーイベントやBarclaysへのサービス提供に対する潜在的な影響を含むデータ損失シナリオ。 ▪ 合意されたサービスレベルの提供に影響を与える可能性のある労働力の不足（世界的な流行病の発生、地政学的イベント、重要な国家インフラストラクチャの障害など）。 ▪ 技術サービスの喪失（データセンターまたはクラウドサービスプロバイダーリージョンの喪失など）。 ▪ 重要な（サービスまたは消耗品を取り扱う）下請業者の喪失。	Barclaysは、重大な破壊的イベントを回避および/または適時に復旧するために（すなわち適切な復旧力を備えるために）、商業的（およびリスク主導型）要件を設けています。Barclaysは、混乱が発生した場合、サービスへの影響（顧客、財務および/または風評上の影響）が最低限に抑えられることを保証されており、またその利害関係者に保証することができるものとします。

管理対象	管理内容	本件が重要である理由
	破壊的なイベントは、計画とテストに情報を提供し、長期的な変化を確認するために、毎年継続的にレビューする必要があります。	
3. 事業復旧計画および検証要件	サプライヤーは、定義された破壊的イベントに対する復旧計画を維持し、復旧目標を達成する必要があります。 復旧計画には、Barclaysに提供するサービスへの影響を軽減および/またはサービスの利用停止を延期するための詳細な復旧手順とサプライヤーの対応を記述する必要があります。 少なくとも以下の点に対処する必要があります。 ▪ 実行可能な回避策 ▪ 意思決定プロトコル ▪ 最小限の実行可能なサービスレベルを再開/維持するためのコミュニケーションとビジネスの優先度設定 ▪ 依存関係 合意されたサービスレベルを提供できること、およびそのサービスがBarclaysの規定する復旧力分類要件を満たしていることを実証するため、12ヵ月ごと、または重要な変更が発生した際に、復旧計画をテストおよび検証しなければなりません。 計画が合意されたレベルのサービスまたは適切な復旧力分類要件に満たない場合、サプライヤーは速やかに（通常は10日以内に）Barclaysに通知し、詳細な改善計画（講じる措置および対応する完了日を含む）を提供するものとします。	企業は、文書化された復旧計画を策定して、その計画が意図したとおりに機能し、合意されたサービスレベルが提供可能であること、サービスがBarclays規定の復旧要件を満たすことを示すためにすべての依存関係が含まれていることをBarclaysに保証するために検証を完了することが求められます。

管理対象	管理内容	本件が重要である理由
4. 統合テスト要件	Barclaysとサプライヤーサービス間の相互依存性がサービス復旧に関して理解されるように、Barclaysの要請に基づき、また相互に合意された日に、サプライヤーは統合テストに参加して、サプライヤーとBarclaysの両方の総合的な復旧力/継続性を検証する必要があります。 Barclaysは、前回の統合テストで重大な欠陥が明らかになった場合またはサービスの中断をもたらしたインシデントが発生した場合を除き、2年に1度以上、このテストを要請することはありません。	合同演習は、適切な復旧計画のためのプロトコルが実行されており、効果的なコミュニケーション戦略が適用されていることを確認するほか、サプライヤーとBarclaysが共同で業務の中断を管理してBarclaysの顧客やより広範囲の金融システムへの影響を最小限に抑えるために役立ちます。 Barclaysは、サードパーティのサービスプロバイダーと連携して事業継続テストを実施することが規制により義務付けられています。
5. システム復旧計画および検証要件	サプライヤーは、システムの中断後にシステムを動作状態に戻すために必要なアクションを詳述したシステム復旧計画を有している必要があります。定義されたBarclaysの復旧力分類の要求に従い、定義された復旧時間目標と復旧時点目標内でシステムを復旧できることを（証拠付きで）実証するために、これらの計画をテストおよび検証する必要があります。 アクティブ/パッシブ構成で設計されたシステムでは、パッシブ環境がアクティブになり、機能と完全な統合機能を実証するのに十分な期間、BAUの本番環境として使用できる必要があります。（最低1週間） アクティブ/アクティブとして設計されたサービスの場合、検証では、システムのノード、インスタンス、または可用性ゾーン（クラウドホストの場合）が失われた状態でも（最低60分）継続的に動作できることを証明する必要があります。 検証頻度の要件は、システムの復旧力分類によって定義されます。「復旧力重大度表」を参照してください	システム復旧計画がないか不十分である場合は、インシデント発生後にBarclaysまたはその顧客に提供され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。

管理対象	管理内容	本件が重要である理由
6. データ復旧計画および検証要件	サプライヤーは、Barclaysへのサービス提供をサポートするために必要な、各技術システムに関するデータ復旧計画を有している必要があります。計画は少なくとも12ヵ月ごと、または重要な変更が発生した際にその精度を確認するものとし、以下を最低限考慮するものとします。 ▪ データソースおよびフロー（上流および下流） ▪ バックアップおよびレプリケーションソース ▪ 復元後のデータ同期要件 サプライヤーは、Barclaysへのサービス提供をサポートするために必要な各技術システムのデータ復旧計画をテストおよび検証し、復旧プロセスにより、必要とされる復旧時点目標内で、データを期待される運用状態に復元できることを（証拠をもって）証明する必要があります。	データの損失は、Barclaysが直面する重大な脅威の1つであり、悪質な行為またはシステム障害によって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。
7. データセンターの多様性およびクラウドサービスプロバイダーの要件	サプライヤーは、Barclaysへのサービス提供をサポートするために必要な各技術システムが、データセンターの全体にわたって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地理的に十分に離れていることを確認するものとします。 技術システムがクラウドサービスプロバイダーによってホスティングされている場合、可用性ゾーン（AZ）の停止を軽減するために、さまざまなAZでシステムを利用できる必要があります。重要なシステムは、クラウドサービスプロバイダーリージョンの障害から復旧する能力を実証する必要があります。	技術システムは、データセンターの停止を防ぐために、複数のデータセンターに導入する必要があります。これはクラウドサービスプロバイダーによってホスティングされているシステム（リージョン障害）にも適用されます。

管理対象	管理内容	本件が重要である理由
8. プラットフォームおよびアプリケーションの再構築計画の要件	サプライヤーは、Barclaysへのサービス提供をサポートするために必要な各技術システムのプラットフォームおよびアプリケーションの再構築計画を維持し、少なくとも12ヵ月ごと、または重要な変更が発生した際にレビュー、承認、テストを受ける必要があります。 これらの計画は、従来の復旧/復元オプションを使用できず、システムを「ベアメタル」から再構築する必要がある状況を対象としています。 計画では、以下を考慮する必要があります。 ▪ オペレーティングシステム/基盤ソフトウェア ▪ アプリケーションの導入と設定 ▪ セキュリティ管理/設定 ▪ システム-エコシステムの依存関係と再統合 ▪ データ要件（データ復旧計画） ▪ 復旧計画を実行、調整するためのツールの依存関係 ▪ 管理プレーンの復旧（例Active Directory） 計画の妥当性は、実現可能性を実証するために、少なくとも机上での演習によって証明されなければなりません。	技術サービスおよびサポートの合意には、サイバー/データ整合性イベントに関する適切な復旧計画が含まれることが重要です。