外部サプライヤー管理義務

復旧計画

2022 年 10 月付け第 12.0 版

1.定義：

「**危機**」	通常の BAU 構造および/またはリソースを超えた対応を必要とする破壊的または風評上のイベントで、意思決定および調整に幹部レベルの介入を必要とするものを指します。
「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。
「**インシデント**」	日々の事業活動の一貫として、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。
「プロダクション・クロスオーバー」	プロダクション・クロスオーバーは、技術システムが代替環境（DR）にフェイルオーバーし、長期間にわたって生産機能を実行する場合に使用される用語です。
「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。
「復旧力分類」	サービスに復旧力要件を適用するために使用される格付けを指します。 これには、RTO、RPO、検証要件および頻度が含まれます。

2.復旧力重大度表：

サプライヤーのサービスは、Barclays の復旧力分類（0～4）のいずれかに分類されます。 高い回復分類（すなわち小さい数字）では、サービスの重要度に応じたより高いレベルの回復または復旧が必要なります。サプライヤーは、契約サービスに関して Barclays が規定する適切な復旧力分類に関して、そのサービスが以下に規定されている復旧時間目標（RTO）および復旧時点目標（RPO）を達成するよう徹底するものとします：

	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
	復旧力の種類	継続運用	高い復旧力	復旧力	復旧	保留/バックアップのみ
破壊的なイベント（アプリケーション）	RTO目標（非データ/サイバーイベント）	1時間以内	4時間以内	12時間以内	24時間以内	復旧計画なし
	RPO目標（非データ/サイバーイベント）	5分以内	最高15分	最高30分	24時間以内	復旧計画なし

3.管理：

管理対象	管理内容	本件が重要である理由
1.破壊的なイベントの復旧計画の要件	Barclaysは、契約サービスの復旧力分類を定めるものとします。 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。 破壊的なイベントの規定については、少なくとも以下の点を考慮する必要があります。 ▪ 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）。 ▪ 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）。 ▪ 技術サービスの損失（データセンターの損害、すべての技術サービスに影響を与えるクラウドサービスプロバイダーの損害など）。 ▪ 重要な（サービスまたは消耗品を取り扱う）下請業者の損失。 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。 サプライヤーは、さまざまな重大度の要因が検討、テスト、検証されていることを実証しなければなりません。	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
2.復旧計画に含めるための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、12 ヵ月ごとに維持および確認しなければなりません。 考慮すべき依存関係： ▪ 技術およびデータ（社内および外注業者から提供）。 ▪ 重要な下請業者（Barclays へのサービスの提供に不可欠な下請業者）。 ▪ 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）。	サービスプロバイダーは、Barclays にサービスを提供する際の依存関係を理解する必要があります。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、すべての依存関係はビジネス復旧計画の一部に含められるものとします。
3.復旧計画要件の検証	サプライヤーは、合意された破壊的なイベントについて、ビジネス復旧計画を維持する必要があります。 ビジネス復旧計画には、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を考慮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分類要件に満たない場合、サプライヤーは速やかに 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。	テストと検証は、サービスの設計と計画が本来の目的通りに機能しており、すべての依存関係を含んでおり、合意されたレベルのサービスが提供されていることおよびそのサービスが Barclays によって規定されている復旧力要件を満たしていることを Barclays に対して保証するために実行されます。

管理対象	管理内容	本件が重要である理由
4.統合テスト	復旧力分類 0～1 の場合、サプライヤーは Barclays の要請に応じて、サプライヤーと Barclays 双方の総合的な復旧力/継続性を検証するための統合テストに参加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。
5.システム復旧計画	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/サービスに関するシステム復旧計画（SRP）、および対応する復旧時間目標（RTO）と復旧時点目標（RPO）を策定する必要があります。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。	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。
6.データ復旧計画	復旧力分類 0～1 の場合、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/サービスに関するデータ復旧計画を策定する必要があります。計画は少なくとも 12 ヵ月ごと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	データの損失は重大な脅威の 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	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/サービスが、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、さまざまな可用性ゾーンでサービスを利用できる必要があります。 復旧力分類 0～1 の場合、サービスは、クラウドリージョンの全体にわたって復旧力を備えている必要があります。	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複数の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。

管理対象	管理内容	本件が重要である理由
8.システム復旧計画の検証	サプライヤーはシステム復旧計画をテストおよび検証し、技術システム/サービスが復旧できること、ならびに復旧力重大度表で定義されている復旧時間目標および復旧時点目標を達成できることを証明する必要があります。 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、復旧力分類 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、文書化されたシステム復旧計画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。 アクティブ/アクティブ構成で設計されたサービスの場合、1 つのアクティブな環境が失われたときでも（処理リソースのシナリオ削減）運用継続が可能なことを検証で証明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。 -復旧力分類 0：PCO によって年に 4 回以上 SRP 検証を実行する必要があります。 -復旧力分類 1：PCO によって年に 2 回以上 SRP および PCO 検証を実行する必要があります。 -復旧力分類 2：少なくとも 12 ヵ月ごとに SRP 検証を実行する必要があります。 -復旧力分類 3：少なくとも 24 ヵ月ごとに SRP 検証を実行する必要があります。 該当する復旧力分類の最小復旧要件をテストが満たさない場合、サプライヤーは速やかに Barclays に通知し、詳細な改善計画（実施すべき措置および対応する完了日を含む）を提出する必要があります。	サードパーティ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ードパーティーが、テストされた適切な復旧力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の 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。
9.データ復旧計画の検証	復旧力分類 0～1 の場合、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/サービスのデータ復旧計画をテストおよび検証し、復旧プロセスによってデータを運用状態に復元できることを証明する必要があります。少なくとも 12 ヵ月ごとに検証を実行する必要があります。 計画が該当する復旧力分類の最小復旧要件に満たない場合、サプライヤーは速やかに Barclays に通知し、詳細な改善計画（実施すべき措置および対応する完了日を含む）を提出するものとします。	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示すために、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。

管理対象	管理内容	本件が重要である理由
10.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	復旧力分類 0～1 の場合、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/サービス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） • 復旧計画を実行するためのツールの依存関係 計画が該当する復旧力分類の最小復旧要件に満たない場合、サプライヤーは速やかに Barclays に通知し、詳細な改善計画（実施すべき措置および対応する完了日を含む）を提出するものとします。	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。