External Supplier Control Obligations

復旧計画

2021 年 10 月付け第 11.0 版

1.定義：

「危機」	とは、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は幹部レベルの介入を必要とするものを指します。
「インシデント」	とは、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。
「復旧計画」	ビジネスサービス、ビジネスプロセス、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
「破壊的なイベント」	原因に関わらず、サプライヤーが復旧および復旧力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
「復旧時間目標」	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業務再開までの目標時間を指します。

2.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、計画のスコープ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その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分類には、少なくとも以下の点を考慮する必要があります。 ▪ 事業運営を維持できなくなるような複数の拠点における建物の滅失。 ▪ 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人的リソースの喪失。 ▪ 潜在的なサイバーイベントや非サイバーイベントによりサービスが利用できなくなる可能性、および Barclays へのサービス提供に対する潜在的な影響。 ▪ テクノロジーサービスの単一の同時復旧（データセンター損失時）。 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。	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
	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。	
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、サービスを Barclays に提供するために不可欠な依存関係を定義し、文書化して、サプライヤーがて季節な復旧力を備えていることを確認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： ▪ すべてのテクノロジーとデータの損失 ▪ 重要な下請業者（Barclays へのサービスの提供において重要な下請業者）のサービスが利用できなくなる可能性 ▪ 労働力の喪失（建物の滅失および/または人員の喪失。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） 適切な復旧力があり、必要なサービスレベルを満たしていることを実証するために、ビジネス復旧プランを通じてテストと検証を実行し、サービスが Barclays が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必要があります。	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、事業復旧計画を維持しなければなりません。 事業復旧計画には、Barclays に提供するサービスへの影響を軽減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	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
	▪ 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。	
4.統合テスト	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しなければなりません。 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、またはサービスに重大な変更がない限り、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.インシデント/危機管理手順	サプライヤーはインシデント/危機を Barclays に上申する手順を含めたインシデントおよび危機管理手順を文書化するものとします。インシデントおよび危機管理手順は 12 ヶ月ごとのサプライヤーのテストと検証が問題なく行われた後に承認されるものとします。 手順にはインシデント/危機が発生してから終結するまでのライフサイクルを通じて、その管理と取り扱いに必要とされる最低限の活動と成果を定義するものとします。サプライヤーは以下の人物を指名するものとします： (i) 手順の承認者であり、手順が目的に適合したものであることを確認する責任を負う個人 (ii) 危機に関する役割ごとの一次連絡先と二次連絡先（一次連絡先が不在の場合）。	サプライヤーはインシデントまたは危機が起きた場合、サービスの取扱いや管理手順について明確な考えを持つものとします。サプライヤーと Barclays は、インシデントおよび危機の状況についての上申プロセスについて共通の理解を持つものとします。 サプライヤーはテストと検証を実施し、インシデントおよび危機が発生した時に、関係する個人/チームがそれを管理するのに十分なスキル、知識、組織を有していることを保証するものとします。

管理対象	管理内容	本件が重要である理由
6.インシデント/危機後の報告	サービス混乱後、通常の事業活動レベルまでサービスが回復してから 4 暦週以内にインシデント/危機後報告書を Barclays に提出するものとします。 報告書には少なくとも以下の検討項目を含むものとします： ▪ インシデントまたは危機の根本原因 ▪ 完了済みの是正措置および再発を防止するために継続に実施されている改善措置 ▪ サプライヤーに通知された Barclays の顧客への影響	インシデント/危機後報告は、適時に問題が特定/是正され、教訓を学んだことを Barclays に保証する上で必要です。
7.システム復旧計画	サプライヤーは、Barclays の復旧力分類 0～3 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）、および相当の復旧時間目標（RTO）と復旧時点目標（RPO）を設定しなければなりません。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、復旧力対策としてアクティブ/パッシブ構成で設計されているものに関しては、すべての要素が有効に動作していることを確認するために、SRP の検証には、復旧された環境がより長い期間維持されて BAU 運用されることが必要となります。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。
8.データ整合性復旧計画	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。
9.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。
10.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 の規定する復旧力分類要件 0～3 を満たしていることを示さなければなりません。	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、

管理対象	管理内容	本件が重要である理由
	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。 テストが該当する復旧力分類の最小復旧力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。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。	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。
11.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。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。
12.プラットフォームとアプリケーションの再構築/改善計画	サイバー攻撃などの破壊的なイベントからの復旧をサポートするため、サプライヤーは、復旧力分類 0～1 のサービスを Barclays に提供するために必要な各技術サービス/システムのプラットフォームおよびアプリケーション再構築/改善計画を策定し、少なくとも 12 ヵ月に 1 回、レビュー、承認およびテストを実行するものとします。	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ます。

管理対象	管理内容	本件が重要である理由
	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。	

3.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、Barclays により規定されている適切な復旧分類に関して、そのサービスが以下に規定されている復旧時間目標（RTO）を達成するよう徹底するものとします：

		ERMF - Risk Impact Assessment	Exceptional Impact	High Impact	Moderate Impact	Low Impact	Insignificant Impact
		Resilience Category	0	1	2	3	4
		Resilience Type	Continuous	Highly Resilient	Resilient	Recover	Suspend / Backup Only
Disruption Event	Application	RTO for Application Recovery (non-data events)	Up to 1 hour	Up to 4 hours	Up to 12 hours	up to 24 hours	No planned recovery
		RPO	Up to 5 minutes	Up to 15 mins	Up to 30 mins	Up to 24 hours	No planned recovery