ミッションクリティカルシステムにおける RPO/RTO 短縮に向けた取り組み

Technical Approaches to Reducing RPO and RTO in Mission-Critical Systems

飯　田　　優

要　約　ミッションクリティカルな勘定系システムでは，災害時においてもデータ損失を最小限に抑え，迅速な復旧を実現することが求められる．現行 OptBAE でも災害対策を考慮しているが，データ損失の可能性や復旧時間の長さなどに改善の余地が残されていた．次期バージョンである OptBAE2.0 では，Azure への移行を契機に災害対策を見直した．東日本リージョンと西日本リージョンにまたがる構成を採用し，災害対策システムのシステム常時起動，SQL Server の AG 同期コミットモードの導入，業務ファイルのリアルタイム同期を実現した．これにより，災害対策システムへの即時切替による迅速な業務再開と，データ損失量の大幅減少を実現することができた．

Abstract　Mission-critical core banking systems must minimize data loss and enable rapid recovery during disasters. This paper describes disaster recovery enhancements implemented in OptBAE 2.0, a core banking service for regional financial institutions. Leveraging Azure cloud migration, we designed a dual-region architecture with continuous operation of disaster recovery system and real-time data synchronization. Verification testing measured switching time and data loss, demonstrating immediate system switching, rapid service resumption, and substantial data loss reduction.

1. はじめに

BIPROGY 株式会社（以後，BIPROGY）は，2022 年 1 月より地域金融機関向け共同利用型勘定系サービスとして OptBAE を提供している．OptBAE は，金融機関業務の中枢を担う勘定系システム（入出金，資金決済，口座・融資管理，利息計算などを行う基幹システム）をサービス利用型（SaaS 型）として金融機関に提供するサービスである．

勘定系システムは，システムの停止が許されないミッションクリティカルの領域に位置付けられており，地震などの災害時にも業務を継続できるよう，災害対策を講じることが必須である．OptBAE においても，本番センターから地理的に離れた遠隔地のバックアップセンターでのシステム構築，および本番データの遠隔移送を行い，災害発生時はバックアップセンターに切り替える標準的な災害対策を講じている．

災害復旧における重要な指標として，RPO（Recovery Point Objective）と RTO（Recovery Time Objective）という項目がある．RPO は障害発生時に「どの時点まで」のデータを復旧させるのかを定めた目標値であり，RTO は障害発生時に「どのくらいの時間で」復旧させるのかを定めた目標値である．いずれも値が小さいほど，事業継続性が高く災害に強いシステムと言うことができる．災害対策の理想的な目標は「RPO/RTO ともに限りなくゼロに近づけること」，すなわち災害が発生し，本番系システムが利用不可となった場合においても，利用者

視点では何事もなかったかのように業務を継続できる状態を実現することである．

現行 OptBAE では RPO/RTO を定めているが，いずれもゼロとはなっておらず，災害発生時には一部データの損失（実運用上の発生頻度は極めて低い）の可能性があり，また復旧に一定時間を要する仕組みとなっており，改善の余地があった．

BIPROGY は OptBAE の次期バージョンとして，「OptBAE2.0」を 2026 年 5 月より提供する予定である．OptBAE では災害対策の更なる強化として，災害発生時のデータ損失を限りなくゼロに抑え，バックアップセンターへの切替時間をできるだけ短縮するシステム構成を検討し，その有効性を評価した．本稿ではこの災害対策強化策について述べる．2 章では現行 OptBAE の概要と災害対策および改善点を述べた後，3 章で OptBAE2.0 における災害対策強化の取り組みについて説明する．また，4 章では災害対策強化策の妥当性確認のために行った実機検証について述べる．最後に 5 章にて今後の展望を述べる．

2. 現行 OptBAE のサービス概要と災害対策

本章では，現行 OptBAE の概要および災害対策について説明し，次期バージョンに向けての要求事項について整理する．

2. 1 現行 OptBAE サービスの概要と災害対策の仕組み

現行 OptBAE は，BIPROGY が開発した地域金融機関向け勘定系パッケージである SBI21 を，Microsoft 社の Windows Server 環境で稼働させ，データベース管理システム（DBMS）には SQL Server を使用したオープンシステムをベースとしている．

災害対策は，一般的な手法である遠隔地バックアップセンター方式（ウォームサイト方式[*1]）を採用している．この方式は，遠隔地のバックアップセンターにあらかじめシステム構築を行ったうえで，平常時には本番センターからバックアップセンターにデータの遠隔移送を行っておき，災害が発生し，本番センターの機能が停止した場合はバックアップセンターに切り替えるというものである．現行 OptBAE では，勘定系オンライン処理を行う「勘定系（オンライン）」と勘定系バッチ処理を行う「勘定系（バッチ）」を中心としたシステムを，本番センターだけでなくバックアップセンターにも配置している．本番センターには本番系システムを配置し，通常運用時に業務処理を実行する．バックアップセンターには，勘定系（オンライン）から更新データを受信するシステムと，災害発生時に業務を再開する災害対策システムを配置している．なお，災害対策システムは通常運用では待機状態としている．

OptBAE で稼働する勘定系業務アプリケーションや OS/ソフトウエアは，本番センターとバックアップセンターで同じバージョンとなるよう，両方のセンターに対してリリースや環境変更を行っている．その上で，日々更新されるデータやファイルについて，災害対策としてバックアップセンターへの転送を行っている．災害発生時はバックアップセンターに転送されたデータやファイルを使用して業務を再開する．災害対策は対象のデータやファイルの重要度によって，転送の方法や頻度を定めている．現行 OptBAE における主なデータやファイルの災害対策を表 1 に示す．

表 1　現行 OptBAE における主なデータ/ファイルの災害対策

データ/ファイル名称	データ/ファイル内容	災害対策	実現方法
勘定系オンラインデータ	オンライン処理によりリアルタイムで更新されるデータ（顧客，口座テーブルなど）	本番センターの勘定系オンライン DB 更新情報をバックアップセンターにリアルタイムで転送する	SQL Server の Always On Availability Group の非同期コミットモードによりデータを反映する
勘定系バッチデータ	勘定系オンライン DB を元にバッチ処理で使用するために加工されたデータ	毎日の夜間バッチ処理終了後，DB バックアップをバックアップセンターに複製する	データベースバックアップをストレージのレプリケーション機能でバックアップセンターに転送する
勘定系業務ファイル	勘定系 DB（オンライン/バッチ）から作られたファイル，またはユーザーから受信したファイル	1 日分の作成ファイルを 1 日 1 回の頻度でバックアップセンターに複製する	勘定系業務ファイルをストレージのレプリケーション機能でバックアップセンターに転送する

勘定系オンラインデータの災害対策について，図 1 にそのイメージを示す．通常運用では，本番センターからバックアップセンターに対して SQL Server の Always On Availability Group[1]（以後，AG 同期）の非同期コミットモードで勘定系オンライン DB の更新データをリアルタイムに転送している．なお，AG 同期には「同期コミットモード」と「非同期コミットモード」がある．同期コミットモードは，データ書き込み時に同期元と同期先の両方でトランザクションログ（データベースの更新履歴を記録するログファイル）のディスク書き込み完了を待機するため，データ整合性が担保される．一方，非同期コミットモードは，同期元でのディスク書き込み完了のみを待機し，同期先への反映は非同期で行うため，データ整合性は担保されないが高いパフォーマンスが得られる．災害発生時は，バックアップセンターの勘定系オンライン DB を災害対策システムに復元し，業務を再開する．

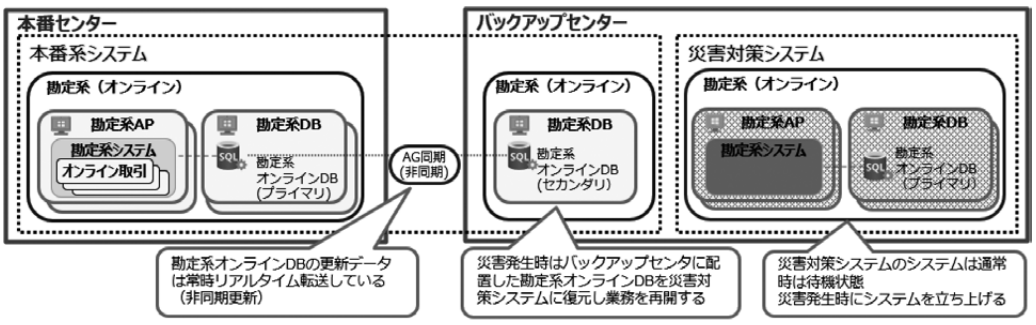

図 1　現行 OptBAE 勘定系オンライン DB の災害対策イメージ

また，勘定系バッチ DB および勘定系業務ファイルの災害対策について，図 2 にそのイメージを示す．通常運用では，夜間バッチ終了後に勘定系バッチ DB と勘定系業務ファイルをバックアップストレージに格納し，バックアップストレージのレプリケーション機能により災害対策システムに複製する運用としている．災害発生時は災害対策システムを起動し，バックアッ

プストレージから勘定系バッチ DB と勘定系業務ファイルを復元して業務を再開する．

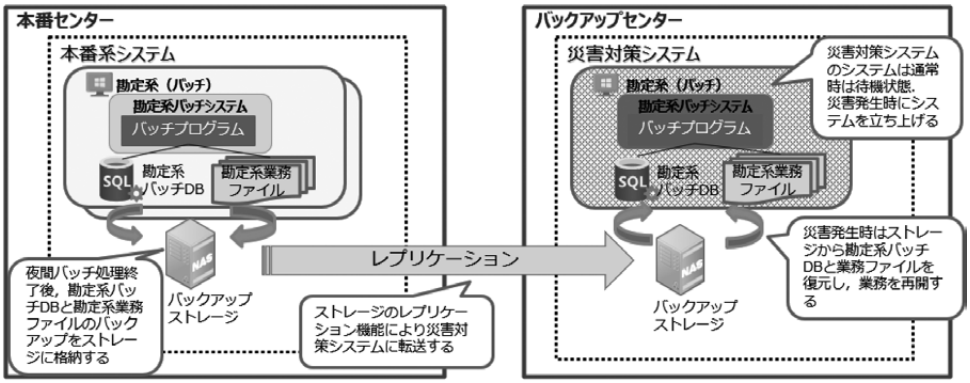

図 2　現行 OptBAE 勘定系バッチ DB・勘定系業務ファイルの災害対策イメージ

2. 2　現行災害対策の状況と次期バージョンへの要求事項

本節では，現行 OptBAE における災害対策の状況を説明し，次期バージョンに向けて整理した要求事項について述べる．

2. 2. 1　想定される災害シナリオと RPO/RTO 改善の必要性

従来の災害対策では，地震や津波などによるデータセンターの物理的な損壊を主な想定シナリオとしていた．この場合，本番センターが長期間利用不可となるため，切替先の災害対策システムでの業務継続を前提とし，本番系システムへの切り戻しは本番センターの再構築後に計画的に実施すればよい．しかし近年では，広域停電（ブラックアウト）やパンデミック時のロックダウンなど，データセンターへの物理的アクセスが制限され，一時的に運用・保守が困難となるケースも想定する必要がある．このような事態では，データセンターの設備自体は無傷であるため，災害対策システムへの切替後，アクセス制限が解除され次第，速やかに切り戻せることが重要である．また，本稿では詳細には扱わないが，近年ではサイバー攻撃も高度化しており，侵害された場合の対策も考慮を要する．

このように災害シナリオが多様化する中でも，1 章で述べたように，RPO/RTO ともに限りなくゼロに近づけることが望ましい．具体的には，災害発生時には速やかに災害対策システムへ切り替えて，データ損失を最小限に抑えるシステムが求められる．加えて，本番センター復旧後の切り戻しも円滑に実施できることが重要である．

なお，災害対策で考慮すべき重要な点として，復旧の優先順位がある．勘定系システムにおいては，オンライン処理が停止すると ATM からの出金や企業間決済など金融機関業務が全面的に停止するため，社会的影響が極めて大きい．一方，バッチ処理においては，一定の時間的余裕があるため，災害発生時にはまずオンライン処理の復旧を最優先とし，バッチ処理の復旧は後続で対応するという考え方が一般的である．

次項で現行 OptBAE における災害対策の状況と改善を要する点を述べる．

2. 2. 2　勘定系（オンライン）の現状と改善を要する点

前項で述べた考え方の通り，災害発生時には，勘定系オンライン処理を最優先で復旧しなければならない．したがって，RPO/RTO ともに短ければ短いほどよく，究極的にはゼロであることが望ましい．

現行 OptBAE における勘定系オンライン処理の災害対策では，2.1 節で述べた通り，バックアップセンターに転送された勘定系オンライン DB を災害対策システムに復元して業務を再開する方式を採用している．このため，災対切替には数時間を要する．また，現行 OptBAE ではパフォーマンスを優先し「非同期コミットモード」を採用しているため，災害が発生した場合にわずかではあるが更新データが欠損する可能性がある．

2. 2. 3　勘定系（バッチ）の現状と改善を要する点

現行 OptBAE における勘定系バッチ処理の災害対策では，2.1 節で述べた通り，1 日 1 回のバックアップをバックアップセンターに転送し，災害発生時にはこれを災害対策システムに復元して業務を再開する方式を採用している．このため，災害発生のタイミングによっては最大 1 日前の業務開始時点までデータ損失が発生する可能性がある．また，災害対策システムへの切替については，災害発生時の状況に応じて復旧方法を検討する方針としている．

したがって，勘定系バッチ処理についても，RPO/RTO を短縮することが望ましい．

2. 2. 4　災対切り戻しの現状と改善を要する点

2.2.1 項で述べたように，災害シナリオによっては，本番センターの設備が物理的に損壊していない場合が考えられるため，本番センターに速やかに切り戻しができることが望ましい．現行 OptBAE では，災害対策システムで更新されたデータやファイルを本番系システムに転送する仕組みを用意していない．このため，切り戻しを行う際には，災害対策システムで更新されたデータやファイルを本番系システムに転送する作業を要するため，数時間から数日程度システムを停止することになる．したがって，災対切り戻しについても，円滑に実施できる仕組みが求められる．

3.　OptBAE2.0 における災害対策強化の取り組み

現行 OptBAE における災害対策の現状を踏まえ，OptBAE2.0 では基盤のクラウド移行と合わせて災害対策の強化を図ることとした．災害対策の強化には，サーバーの切替方式，データベースの継続性，業務処理の再開手順，ネットワーク経路の切替など多岐にわたる検討要素がある．本稿ではその中でも特に RPO/RTO 改善に大きく寄与するサーバーの切替方式とデータベースの継続性に焦点を絞って説明する．

3. 1　クラウド環境への移行による基盤変更

OptBAE2.0 では，新規ユーザーの獲得や新たなサービス開始に備えて，システムリソースの増強などを容易に行えるクラウド（Azure）に移行する方針とした．BIPROGY では，主に地方銀行向けに提供しているオープン勘定系システム BankVision® をクラウド化した BankVision on Azure の稼働実績を通じて，金融機関向けクラウドシステムに関する運用ノウハウやセキュリティ対策の知見を蓄積してきた．こうした状況を踏まえ，OptBAE2.0 ではクラウド

環境への移行を決定した．移行の前提として，本稿の主題である災害対策の強化策を検討した．

3. 2　災害対策強化のアプローチ

2. 2 節で述べた現行 OptBAE の災害対策の状況と次期バージョンへの要求事項を踏まえ，以下のアプローチで対応することとした．

3. 2. 1　勘定系（オンライン）の改善策

OptBAE2.0 では，東日本リージョンに本番系システム，西日本リージョンに災害対策システムを配置し，両システムで常に稼働状態を保つ．また，東西リージョン間で直接勘定系オンライン DB の AG 同期を行う構成とし，平常時は西日本リージョンでは処理が動作しないよう抑止状態としておく．災害発生時は抑止状態の解除により西日本リージョンにて即座に業務を再開する．これにより，災害対策システムへの切替時間の大幅短縮が可能となる．

さらに，勘定系オンライン DB の東西間 AG 同期について，「非同期コミットモード」から「同期コミットモード」への変更を検討した．同期コミットモードによりデータベースのデータ整合性が担保されるため，災害発生時のデータ損失をゼロにすることが可能となる．一方で，同期コミットモードはオンライン取引の処理性能への懸念があるが，性能要件を満たせば採用可能と考えた．

同期コミットモードでは，東日本リージョンのトランザクションのコミット完了前に，西日本リージョンでトランザクションログ書き込み完了確認が必要となる．このため，西日本リージョンでディスク I/O 遅延やネットワーク遅延が発生した場合，東日本リージョンで実行されるオンライン処理のコミットが待たされ，障害影響が波及するリスクがある．このリスクに対して，従来の Premium SSD と比較してディスク I/O 性能の向上が期待できる Premium SSD v2 の採用により I/O 遅延の発生頻度を低減する対策を講じた[2]．また，西日本リージョンからの応答が一定時間内に返ってこない場合には一時的に東西間の AG 同期を非同期コミットモードに切り替え，東日本リージョンの DB のみでコミットを完了させる仕組みとすることで，西日本リージョンでの障害発生時においても東日本リージョンのオンライン処理を継続できるようにした．これらの対策により，同期コミットモードの採用によるリスクを許容可能なレベルまで低減し，RPO ゼロを実現しながら，平時の安定稼働を両立させることを目指した．この改善策に基づいて設計した OptBAE2.0 の勘定系オンライン DB 災害対策構成を図 3 に示す．

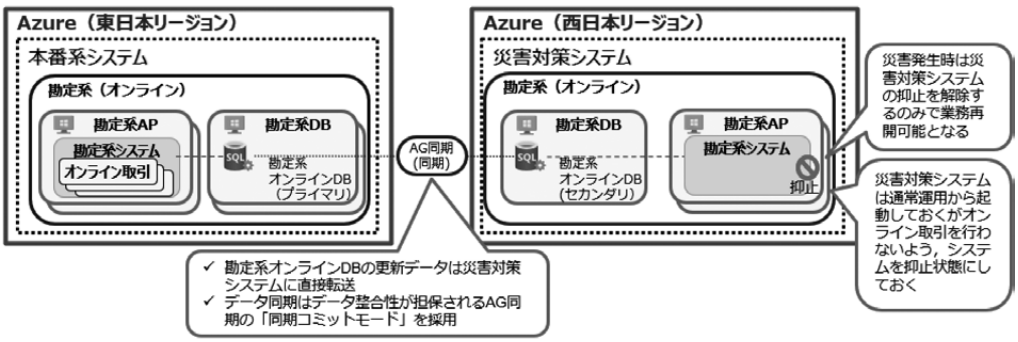

図 3　OptBAE2.0 の勘定系オンライン DB の災害対策イメージ

3. 2. 2　勘定系オンライン処理の自動切替

勘定系オンライン処理は 2 章で述べた通り復旧優先度が非常に高いため，OptBAE2.0 では東日本リージョン障害時に西日本リージョンへ自動的に切り替わる仕組みの実現を目指している．

具体的には，SQL Server の AG 機能における自動フェールオーバーを有効化することで，東日本リージョンの勘定系 DB が全て停止した際に，西日本リージョンの勘定系 DB へ自動的に切り替わるようにする．ただし，勘定系 AP と勘定系 DB が異なるリージョンに存在すると，ネットワークレイテンシー（通信の往復による待ち時間）によりオンライン処理の応答時間が大幅に遅延する．このため，勘定系 DB の東西切替をトリガーとして，勘定系 AP も東日本リージョンから西日本リージョンへ自動的に切り替わる仕組みを構築している．

3. 2. 3　勘定系（バッチ）の改善策

勘定系バッチ DB について，OptBAE2.0 では勘定系オンライン DB と同様に，東日本リージョンと西日本リージョン間で AG 同期を行う構成としたうえで「同期コミットモード」を採用することを検討した．バッチ処理は大量のデータを処理するが，コミット回数自体は多くないため，同期コミットモードによる効率への影響は限定的であると考えたからである．同期コミットモードにすることにより，勘定系バッチ DB においても災害発生時のデータ損失をゼロにすることができる．

さらに，東日本リージョンにて更新された勘定系業務ファイルを西日本リージョンにリアルタイムに複製する仕組みを導入する．業務ファイルについても同期レプリケーション（ファイル書き込み完了を両拠点で確認してから次の処理に進むファイル複製方式）により災害発生時のデータ損失をゼロとすることが理想であるが，検討段階で同期レプリケーション機能は性能要件を満たせず不採用とした．このため，非同期レプリケーションである DFS レプリケーション[3]（Windows Server の分散ファイルシステムレプリケーション機能）を採用することとした．DFS レプリケーションは非同期でファイルを複製するため，災害発生時に一部のファイルが複製途中となり破損する可能性があるが，従来の 1 日 1 回のバックアップと比較して災害発生時のデータ損失量を大幅に減少することができる．OptBAE2.0 の勘定系バッチ DB および勘定系業務ファイルの災害対策構成を図 4 に示す．

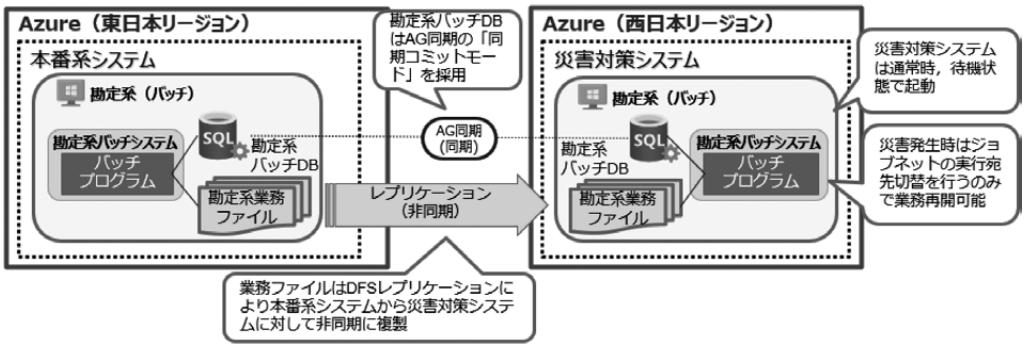

図 4　OptBAE2.0 の勘定系バッチ DB・勘定系業務ファイルの災害対策イメージ

3. 2. 4　災対切り戻しの改善策

現行 OptBAE では，災害対策システムで更新されたデータやファイルを本番系システムに転送する仕組みを用意していないため，切り戻しには数時間から数日程度のシステム停止を要した．

OptBAE2.0 では西日本リージョンが本番系システムとして稼働している際，西日本リージョンから東日本リージョンへのデータベース同期もできるようにした．また，DFS レプリケーションにより，西日本リージョンから東日本リージョンへのファイル同期もできる．そのうえで，切り戻しを行う際は災対切替と同じ処理を実施する仕組みとした．これらの対策により，本番センターの復旧後，短時間で円滑に切り戻しを実施することができる．

4.　技術的懸念事項の検証

3 章で述べた災害対策強化策は，リージョン間でのデータベース同期や業務ファイルのリアルタイム複製など，技術的に新しい取り組みを含んでいる．このような構成変更においては，システム構成の妥当性と災対切替・切り戻しの実現可能性，および RPO/RTO の改善効果を評価しなければならない．これらの検証には実機による確認が不可欠である．本章では，この実機検証について述べる．

4. 1　検証の目的と方針

本検証の目的は，3 章で検討した災害対策強化策の実現可能性を確認することである．検証は大きく二つの観点から実施した．

第一に，検討したシステム構成における処理性能への影響の確認である．東西リージョン間でのデータベース同期において同期コミットモードを採用した場合，リージョン間のネットワークレイテンシーの影響により処理性能が低下する懸念がある．このため，オンライン処理およびバッチ処理において，性能が許容範囲内に収まることを確認する．

第二に，災対切替および切り戻しの実現可能性と RPO/RTO 改善効果の確認である．RPO/RTO の改善可能性を評価するために，実機を用いて災対切替に要する時間およびデータベースと業務ファイルのデータ損失量を測定する．

これらの検証を通じて，OptBAE2.0 の災害対策強化策が技術的に実現可能であり，目標とする RPO/RTO の改善を達成できることを実証する．

4. 2　検証環境

実機検証は Azure 上に構築した検証環境にて実施した．検証環境のシステム構成は 3 章で述べた構成に準ずる．勘定系オンライン DB および勘定系バッチ DB は東西間で AG 同期（同期コミットモード）とし，業務ファイルについては DFS レプリケーションによるリアルタイム同期を実装した．検証環境の主要な構成要素を表 2 に示す．

表 2　検証環境の構成要素

サーバー名		勘定系 AP	勘定系 DB	勘定系（バッチ）
仮想マシン台数	東日本リージョン	2 台	1 台	1 台
	西日本リージョン	2 台	1 台	1 台
仮想マシンモデル		Standard E16s v5（16 コア CPU，32GB メモリ）		
OS		Windows Server 2019		
DBMS		Microsoft SQL Server 2019 Enterprise Edition		

4. 3　性能検証

本節では検討したシステム構成における処理性能への影響について検証した結果を述べる．

4. 3. 1　検証観点

オンライン処理およびバッチ処理において，同期コミットモード採用時の性能への影響を評価した．同期コミットモードではトランザクションのコミット時に東西両リージョンのログ書き込み完了を待機する仕組みとなる．また，東西両リージョン間のネットワークレイテンシーは約 12 ミリ秒[4]である．これらにより，1 トランザクションあたりの処理時間が増加し，性能低下を招く可能性があるため，その影響を評価した．

オンライン処理においては，コミット処理は原則取引成立時の 1 回のみ実施している．このため，机上検証ではコミット処理に要する時間が約 12 ミリ秒増加するのみであり，処理性能への影響は限定的との結論に至った．同様に，バッチ処理においても大量のデータをまとめて処理した後にコミット処理を行っているため，ネットワークレイテンシーの影響はバッチ全体の処理時間からすると軽微であるとの考えに至った．

これらの机上検証が妥当であることを確認するため，実機検証において同期コミットモードを採用した場合の性能を測定し，性能要件を満たすことができるかを確認した．

4. 3. 2　オンライン性能検証

オンライン性能検証では上記の代表的なオンライン取引（入金処理，出金処理，顧客照会処理）をシミュレータから繰り返し多重実行し，スループット（単位時間あたりの処理件数）および 1 トランザクション（1 取引）あたりの処理時間を測定した．

内部目標値として，スループット 200 件/秒以上，処理時間 500 ミリ秒以下を設定した．実機検証の結果，スループット 240 件/秒，処理時間 101 ミリ秒を達成し，同期コミットモードを採用した場合でも性能要件を満たすことを確認した．

オンライン処理の検証結果を表 3 に示す．この検証結果から，OptBAE2.0 において東西リージョン間で AG 同期の同期コミットモードを採用した場合でも，オンライン処理の性能要件を

表 3　オンライン性能検証結果

検証項目	目標値	結果	評価
スループット（処理時間あたりの処理件数）	200 件/秒以上	240 件/秒	達成
処理時間	500 ミリ秒以下	101 ミリ秒	達成

満たすことができることが実証された．

4.3.3　バッチ性能検証

バッチ性能検証では，現行 OptBAE において毎日夜間（0 時から明け方にかけての時間帯）に稼働しているバッチ群を実行し処理時間を測定した．内部目標値として，現行と比較して処理時間の増加が 15%以内となることとした．15%の増加であれば夜間バッチが完了すべき運用時限に十分収まると判断したためである．実機検証の結果，処理時間は 73 分（現行 OptBAE：66 分）となり，11%の増加に留まった．バッチ処理においては大量のデータをまとめて処理した後にコミット処理を行うため，東西リージョン間のネットワークレイテンシーによる影響は机上検証の通り軽微であった．

バッチ処理の検証結果を表 4 に示す．この検証結果から，OptBAE2.0 において東西リージョン間で AG 同期の同期コミットモードを採用した場合でも，バッチ処理の性能要件を満たすことができることが実証された．

表 4　バッチ性能検証結果

検証項目	目標値	結果	評価
処理時間	76 分以内（現行比 15%増以内）	73 分（現行比 11%増加）	達成

4.4　災対切替および切り戻しの検証

本節では，東日本リージョンが全面的に障害となった場合を想定し，西日本リージョンへの災対切替および切り戻しの検証結果を述べる．災対切替については，切替に要する時間の測定と，データ損失の有無の確認についても説明する．

4.4.1　検証観点

本検証における主な観点は 2 点である．1 点目は災対切替および切り戻しが正しく実施でき，切替後のリージョンにおいてオンライン処理およびバッチ処理が正常に動作することの確認である．2 点目は，4.1 節に記載したとおり RPO/RTO の改善可能性を評価するため，災対切替に要する時間の測定と，データベースおよび業務ファイルのデータ損失の有無の確認である．

4.4.2　災対切替および切り戻しの実施と評価

災対切替の検証では，西日本リージョンへの切替および東日本リージョンへの切り戻しを実施し，いずれの場合もオンライン処理およびバッチ処理が正常に動作することを確認した．

切替に要した時間は，勘定系（オンライン）と勘定系（バッチ）合わせて 11 分であった．現行 OptBAE では災対切替に数時間を要していたのに比べ，大幅に短縮できた．

データ損失量について，勘定系（オンライン）と勘定系（バッチ）に分けて述べる．

勘定系（オンライン）は，データベースの同期コミットモードの採用により，切替前後でデータの整合性が完全に保たれていることを確認した．すなわち，データベースについてはデータ損失量ゼロが達成された．

勘定系（バッチ）も，データベースについては勘定系（オンライン）と同様にデータ損失量

ゼロが達成された．勘定系業務ファイルについては，3.2.3 項で述べたように，DFS レプリケーションによる非同期レプリケーションを採用しているため，災害発生時に一部のファイルが複製途中となる可能性が想定されていた．このため，バッチ高負荷時における東西間でのファイル同期にかかる時間計測（東日本リージョンで作成されたファイルが西日本リージョンに複製されるまでの時間計測）を行った．なお，検証時にはサイズの異なる複数のファイルを用いた．もっとも大きいファイルには実運用で想定される最大級のサイズである 30GB 程度のファイルを用いた．実機検証の結果，バッチ高負荷時において 30GB 程度のファイルであれば 9 分で同期されることが確認できた．つまり，本検証条件下において勘定系業務ファイルのデータ損失量は最大 9 分間の更新分であることを確認した．

災対切替および切り戻しの検証結果を表 5 に示す．

表 5　災対切替および切り戻し検証結果

検証項目	目標値	結果	評価
災対切替動作確認	西日本リージョンへ切替後，オンライン処理およびバッチ処理が正常に動作する	正常動作を確認	達成
切り戻し動作確認	東日本リージョンへ切り戻し後，オンライン処理およびバッチ処理が正常に動作する	正常動作を確認	達成
勘定系（オンライン）切替時間	30 分以内（現行：数時間）	11 分で完了	達成
勘定系（オンライン）データ損失量（データベース）	データ損失量ゼロ	データ損失量ゼロを達成	達成
勘定系（バッチ）切替時間	30 分以内（現行：数時間）	11 分で完了	達成
勘定系（バッチ）データ損失量（データベース）	データ損失量ゼロ	データ損失量ゼロを達成	達成
勘定系（バッチ）データ損失量（業務ファイル）	30 分以内（現行：最大 1 日前の業務開始時点）	30GB 程度のファイルが 9 分で同期（データ損失量：最大9分間の更新分）	達成

4.5　検証結果の総合評価

実機検証により，OptBAE2.0 における災害対策強化策の有効性を確認することができた．同期コミットモード採用時でもオンライン処理およびバッチ処理の性能要件を満たし，実運用に耐えうる構成であることを実証した．災対切替については 11 分で完了し，データベースのデータ損失量はゼロ，業務ファイルのデータ損失量は最大 9 分間の更新分であることを確認した．この検証結果から，RTO は現行の数時間から大幅に短縮し，RPO はデータベースをゼロ，業務ファイルも大幅に短縮できるめどが立った．

以上の検証結果から，OptBAE2.0 における災害対策強化策は技術的に実現可能であり，現

行 OptBAE と比較して RPO/RTO の大幅な改善が期待できることが確認された.

5. 今後の展望と他システムへの適用可能性

本章では，OptBAE2.0 の今後の展望および他サービスへの展開の可能性について述べる.

5. 1 OptBAE2.0 サービス開始に向けて

実機検証により災害対策強化策の有効性が確認され，RPO/RTO ゼロに向けて大きく前進した．そのうえで，OptBAE2.0 は 2026 年 5 月の本番稼働を目指しており，本稿執筆時点（2025 年 12 月）では予定通りサービス開始を迎えられる見込みである．本稿で述べた災害対策強化策は，実機検証で得られた知見を活かして実装を進めており，OptBAE2.0 のサービス開始により，利用金融機関に対してより高度な事業継続性を提供できるものと考えている.

また，本取り組みは現時点でのビジネス要求や技術動向を踏まえて実現したものである．BIPROGY は今後も技術革新やビジネス環境の変化に応じて，事業継続性の更なる強化に継続的に取り組み，常にサービスを進化させていく.

5. 2 他サービスへの展開

本稿で述べた OptBAE2.0 における災害対策強化の取り組みは，OptBAE 以外のシステムへの展開も期待できる．特に，BIPROGY が主に地方銀行向けに提供しているオープン勘定系システム BankVision においても，次期バージョンである BankVision2.0 への移行が進められており，今回の災害対策強化の手法を活用する見込みである.

クラウド環境の特性を活かした災害対策の設計，特にリージョン間でのデータベース同期とファイル同期を組み合わせた手法は，ミッションクリティカルシステム全般に適用可能である．今後，BIPROGY が提供する他の金融システムにおいても，本取り組みで得られた知見を活かしていきたい.

6. お わ り に

本稿では，地域金融機関向け勘定系サービス OptBAE における災害対策強化の取り組みについて述べた．現行 OptBAE の災害対策における改善点を明らかにし，次期バージョンの OptBAE2.0 において RPO/RTO をゼロに近づけるための具体的なアプローチを示した.

金融機関における災害対策は，単なる技術的課題ではなく，社会的責任の観点から極めて重要である．本稿で述べた技術的手法は，データベース同期とファイル同期を組み合わせた災害対策の設計手法として，ミッションクリティカルシステムの災害対策を検討する際の一つの指針となり得る．災害対策の究極の目標である「RPO/RTO ともに限りなくゼロ」の実現に向けて，本稿の取り組みが同様の課題に取り組む多くの方々にとって参考となれば幸いである.

最後に，本稿の執筆にあたりご指導いただいた皆様に心より感謝申し上げる.

＊ 1 バックアップセンターで一部のシステムを稼働状態で待機させる方式．他の災害対策の方式として，常時稼働状態でシステムを待機させるホットサイト方式，設備スペースのみを確保し災害時にシステムを構築するコールドサイト方式がある.

参考文献　［1］ Always On 可用性グループとは，Microsoft Learn，2025年10月，https://learn.microsoft.com/ja-jp/sql/database-engine/availability-groups/windows/overview-of-always-on-availability-groups-sql-server?view=sql-server-ver16
［2］ Azure マネージド ディスクの種類，Microsoft Learn，2025年11月，https://learn.microsoft.com/ja-jp/azure/virtual-machines/disks-types
［3］ 分散ファイルシステム（DFS）レプリケーションの概要，Microsoft Learn，2025年7月，https://learn.microsoft.com/ja-jp/windows-server/storage/dfs-replication/dfsr-overview
［4］ Azureネットワーク ラウンドトリップ待ち時間統計，Microsoft Learn，2025年7月，https://learn.microsoft.com/ja-jp/azure/networking/azure-network-latency?tabs=APAC%2CJapan

※　上記参考文献に示したURLのリンク先は，2026年1月14日時点での存在を確認.

執筆者紹介　飯　田　　優（Masaru Iida）
2003年日本ユニシス・ソフトウェア(株)入社．金融機関向けミドルウェア「MIDMOST」や，オープン勘定系システム「BankVision®」などの開発・保守・導入を担当．2019年から現在にいたるまで，地域金融機関向け勘定系サービス「OptBAE」のサービス開発・導入・保守を担当.