文書番号：MOE10-業仕様-3002

平成１５年度

流通サプライチェーン全体最適化情報基盤整備事業

（業務連携支援システム基本設計）

基本設計書

「運用条件書・運用設計書」

平成 16 年 3 月

日本電気株式会社

改版履歴

日付	版数	改版内容
2004 年 1 月 31 日	初版	新規

基本設計書作成責任者
日本電気株式会社　：曽根田　雄一

検　印

目 次

１．システム運用条件

本システムは、以下の３つの形態での利用を想定している。

- 大企業が利用（主に大手企業が自社システムと本システムを接続して利用する）
- 中小企業が利用（主に中小企業が本システムを自社システムとして利用）
- ASP 方式(主に中小企業が ASP 業者の提供する本システムを利用する)

本設計書では、多数の企業が接続することから最も運用条件を厳しくする設定する必要のある ASP サイトの運用条件を記載する。また、大手企業、中小企業および Web クライアントについては各社の運用要件が異なることが想定されるため、ASP 方式を原則として各社にて個別に運用条件を定めるものとし、本仕様書では必要な場合にのみ推奨条件を記載するものとする。

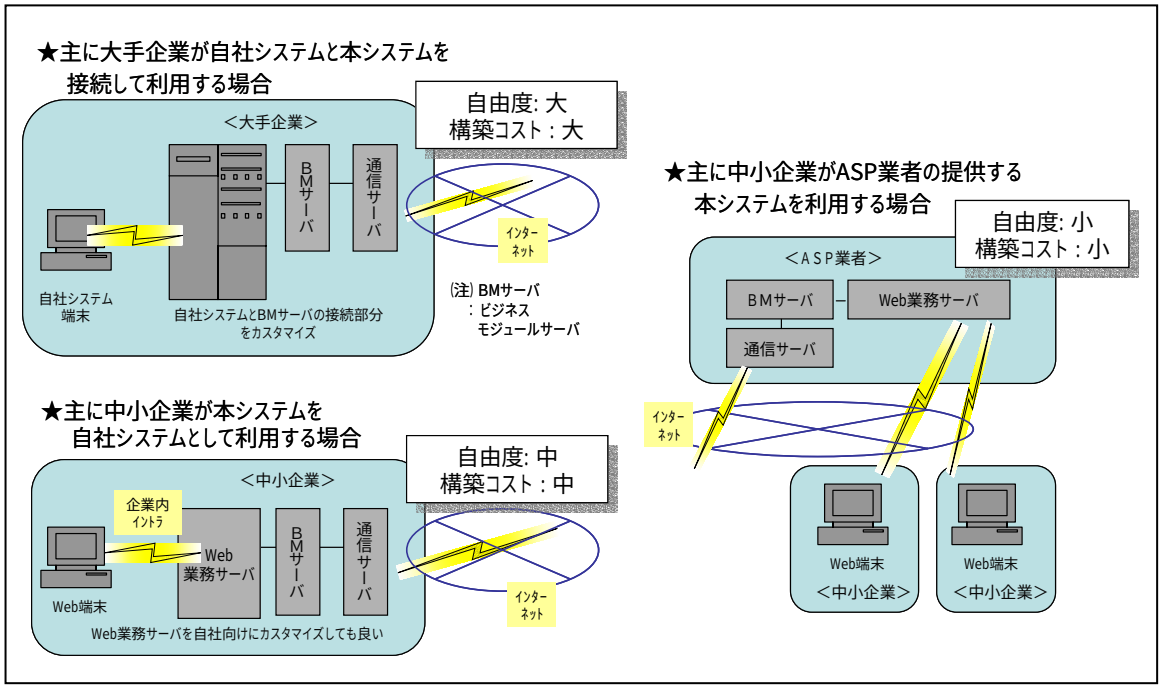

図 1.1 本システムの構成形態

1.1 運用時間

（1） 前提条件

流通業における受発注業務を行う本システムでは、複数の企業から接続されるため、システムダウンが発生すれば運営企業の業務が中断、取引機会の損失、企業イメージの低下、信用の失墜などの様々な影響が発生する可能性

がある。このような業務上の影響を最小限にするために高信頼性のシステムを構築する必要があり、本システムでは、運用時間として 24 時間 365 日を運用要件とする。

（2） 運用時間

ASP サイトの運用時間は 24 時間 365 日を基本とする。

ただし、以下のようなシステムメンテナンスや臨時メンテナンスについては計画停止することも可能とする。

- システムメンテナンスのための月１回半日程度、環境設定や資産移行、定期保守を目的とした計画停止
- アプリケーションのバージョンアップやハードウェアの増強などのサイト運営で必要な計画停止

1.2 許容停止時間

（1） 前提条件

多数の会員が SCM の業務サービスとして ASP サイトを利用するため、高可用なシステムであることが求められ、停止時間を最小限に留める必要がある。このため、ハードウェアレベルのシステム復旧時間およびデータの調査時間として最低限必要である時間から許容停止時間を２時間以内と考える。

（2） 許容停止時間

ASP サイトの許容停止時間は２時間以内とする。

ただし、以下については許容停止時間に含めないものとする。

- システムメンテナンスなどの計画停止時間
- データセンタに接続されている外部ネットワーク、大手企業および中小企業の基幹システム、Web クライアントに関する障害は、ASP サイトの許容停止時間に含めないものとする。

1.3 定期作業

（1） 前提条件

重要性の高い業務データを管理し、高可用システムを維持するためには、システムの二重化、クラスタ切り替え、ログ管理等について適切な運用を行

う必要がある。また、人為的ミスを防ぐため可能な限り、運用作業の自動化が望ましい。

（2） 定期作業

ASP サイトの安定運用を目的として、下記の作業を定期的に実施する。

- 定期的にバックアップを実施する。バックアップサーバ等を利用したオンラインバックアップを想定する。
- ログのクリーンアップや一定保存期間を経過したデータを削除する。なお、本作業については運用コストを考慮してジョブ制御と連動して自動で行われるものとする。
- ホットスタンバイとなっているクラスタ（二重化）構成機器については定期的に系切り替えを実施する。ただし、一部の機器についてはその性質上、系切り替えを実施しない運用も可能とする。
- 各種サーバおよびネットワーク機器等のハードウェア機器の点検を定期的に実施する。
- 各種サーバ等のパスワードを定期的に変更する。
- 各種サーバの処理時間およびスループットを定期的に収集する。

1.4 運用体制

ASP サイトはデータセンタにて運用することを前提とし、データセンタが提供するサービス、設備を活用することとする。

運用体制としては、運用監視機能と連動し、障害を迅速に検知可能な体制を 24 時間確保するとともに、障害通知から一次切分～エスカレーション、復旧までの業務停止時間を最小限にとどめるために必要な体制であることを要件とする。これらの要件を満たすため ASP サイトについては下記の体制にて運用を行うものとする。

また、本システムと自社システム間の連携を実施する企業については、運営上必要な臨時メンテナンスや障害発生時の対応のため、連絡窓口としてのシステム管理者（運用 SE）を設置し、サイト運営責任者とのやりとりを行う。

また、エンドユーザからの問い合わせに対応するため、ヘルプデスクを設置する。

表 1.2 ASP サイトの運用体制

担当	役割
サイト運営責任者	ASP サイト（データセンタ）の運営責任者。
運用ＳＥ	運用監視員（運用オペレータ）への作業指示とサイト運営責任者とのやりとりを行う運用側の窓口。 システム運用上必要となる作業の企画や立案も含めて実施する。
運用監視員 （運用オペレータ）	データセンタにて運用ＳＥの指示によりシステムのオペレーションや運用作業の全般を行う。 データセンタでのハードウェアおよびソフトウェアの障害監視を担当。 24 時間 365 日体制で障害監視を行う。
保守センタ	障害通知を受けて、原因調査および対応を行う。必要に応じて、保守契約締結先であるハードウェアまたはソフトウェアベンダへの障害調査および障害対応を依頼する。
SW/HW ベンダ	ASP サイトとの保守契約に基づき、保守センタからの問合せ、障害調査および障害対応を行う。
ヘルプデスク	エンドユーザからの問合せ対応を行う。 原則として、平日 9：00 から 17：00 までの対応を想定する。

1.5 セキュリティに関する運用について

CA サーバの管理やウィルスチェック等のセキュリティに関する運用については「セキュリティ設計書」に基づくものとする。

２．システム運用設計

２.１ ハードウェア

システム構築にあたり、運用条件を満たすためには複数のサーバを設置する必要がある。これらのサーバの中でも特に重要性の高いサーバにおいては、システムの一部に何らかの障害が発生した場合でも、システムを停止しても継続処理できるフォールトトレラント性が要求される。たとえば、電源ユニット、ハードディスクなどで障害が発生するとシステムの運用に重大な支障をきたす可能性が高い。対応策として、デバイスを二重化しておく、ハードディスクやメモリエラーなどを検出し、エラー訂正技術などによって自動的にこれを訂正する機能を組み込み、などがある。

中でも高信頼性を実現するために用いられる技法のひとつにクラスタリングがある。ハードウェア、ソフトウェアの組み合わせで、複数のハードウェアを用意し、障害の発生時に処理を他サーバが引き継ぐような構成になっている。その形態には、クラスタ構成、パラレル構成などがある。

表 ２.１フォールトトレラントシステムの構成

クラスタ構成	２台以上のサーバを用意し、１つのグループ（クラスタ）を構成する。クラスタ内のサーバ１台に以上が発生した場合、他のサーバが業務を引き継ぐ形態をいう。
パラレル構成	２台以上のサーバを用意し、同一の環境を構築する。ロードバランサなどを用いて処理要求を各サーバに振り分ける。あるサーバで異常が発生した場合には、これをロードバランサが検知し、異常の発生したサーバへの処理要求の割付を中止する。

以上のような手法を利用し、フォールトトレラントシステムを構築するために最適な機器構成を選択する。

本システムにおいては、WWW サーバにパラレル構成を採用し、二重化による可用性の向上と、ロードバランサによる負荷分散機能で急激なアクセス増加時におけるレスポンスの向上を図る。また、WWW サーバ以外のサーバにおいてはクラスタ構成を採用し、二重化することによってシステムの可用性を向上させる。また、監視端末においては、サーバの設置場所と同じ場所に１台、別の場所に同機能の監視端末を１台設置することで二重化し、無停止運転を実現させる。

以下に信頼性、拡張性の観点から各サーバの構成に必要な要件について述べる。

2.1.1 信頼性・拡張性と適用範囲

本サイトにおける信頼性・拡張性要件の適用範囲を以下の通りとする。

基本方針として、サーバ系は各サーバの高可用性に加え、流通サプライチェーンというミッションクリティカルな業務に直接関係するサーバに関しては更なる信頼性・拡張性を追求する。ネットワーク系についても上記要求を満たす構成とする。

表 2.2 ハードウェア運用要件一覧

		冗長化/負荷分散	高速化
サーバ	WWW/BM ｻｰﾊﾞ	ロードバランサによる複数台化（ホットスタンバイ用ロードバランサの設置）	SSL アクセラレータによる暗号/復号処理の専用装置化（ホットスタンバイの SSL アクセラレータを設置）
		サイト共通ページ（静的コンテンツ）用サーバの分離	帯域制御装置による HTTP リクエストの安定化
	DB ｻｰﾊﾞ	クラスタ構成による多重化	AP サーバ/DB サーバの GB-SW 接続 (AP サーバ/DB サーバの FC 接続)
			ディスクアレイの高速化、FC 接続
	通信サーバ	クラスタ構成による多重化	
	認証サーバ	クラスタ構成による多重化	
	CA サーバ	クラスタ構成による多重化	
	Mail ｻｰﾊﾞ & (内)DNS ｻｰﾊﾞ	クラスタ構成による多重化	
	(外)DNS ｻｰﾊﾞ	ホットスタンバイの設置	
WAN	ISP 接続	ISP 接続ルートを多重化	
LAN	ﾙｰﾀ/HUB/ｹｰﾌﾞﾙ	経路の二重化	
	FireWall	クラスタ構成による多重化	

2.1.2 サーバ高可用性

運用条件である 24 時間 365 日のサーバ運用を実現するため、サーバや各機器について下記のような冗長構成とし、仮にハードウェア障害が発生した場合でもサービスを停止せずに運用を継続できる構成とする。

- CPU、内臓ディスクを冗長構成とすることで単一障害点を除去する
- LAN、SCSI、ファイバチャネル等のインタフェースカードを二重化する
- ディスクアレイのコントローラおよびディスクアレイ本体を二重化する

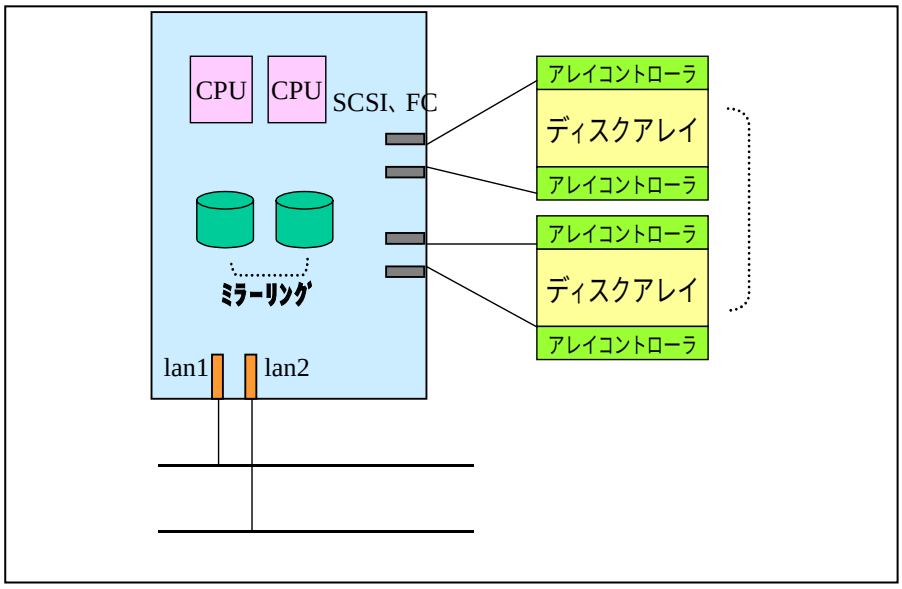

図 2.3 サーバ高可用性の構成例

（1） CPU 障害の対応

CPU を二重化し、CPU 障害が発生した場合でもサーバのオートリブートによって CPU を切り離して、継続して縮退運転を行うことのできる構成とする。

（2） 内蔵ディスク障害の対応

ディスクを二重化（ミラーリング）し、内蔵ディスク障害が発生した場合でも、片系のディスクで継続運用が可能な構成とする。また、システムを停止することなく、故障したディスク装置を交換してミラーリングの再同期が可能な構成とする。

（3） LAN 障害の対応

ルータ／HUB／ケーブル等のネットワーク機器を二重化し、LAN 環境の構成機器に障害が発生した場合でも、待機系機器に切り替わることで通信を続行可能な構成とする。

（4） SCSI 障害・FC インタフェース障害の対応

SCSI／FC インタフェースを二重化することで、障害発生時にも片系の装置でディスクアクセスを継続可能な構成とする。

（5） ディスク障害の対応

RAID 機能、ホットスペア機能を有したディスク装置を採用することで、ディスク障害が発生した場合でも継続してディスクアクセスが可能な構成とする。

（6） アレイコントロール障害の対応

多重化構成とすることで、障害発生時にも片系のアレイコントローラでディスクアクセスを続行可能な構成とする。

（7） ディスクアレイ本体停止の対応

多重化構成とすることで、障害発生時にも片系のディスクアレイでディスクアクセスを続行可能とする。また、障害復旧についてはシステムを停止することなく、故障したディスクアレイを交換して、ミラーリングの再同期が可能な構成とする。

2.1.3 WWW／BM（ビジネスモジュール）サーバの信頼性・拡張性の向上

WWW／BM サーバの信頼性・拡張性を実現するため、以下を満たす構成とする。

- ロードバランサによる負荷分散／冗長化構成
- SSL アクセラレータによる HTTPS（SSL）処理の高速化
- データベースサーバのフェールオーバ時の障害対応機能

2.1.3.1 ロードバランサによる負荷分散／冗長化構成

ロードバランサを設置することで以下の要件を満たす構成とする。

- ロードバランサを使用して WWW／BM サーバを複数台設置し、負荷分散／冗長化を行う。
- ロードバランサ本体も冗長化（ホットスタンバイ）構成とする。

（1） 負荷集中時のレスポンス低下への対応

ロードバランサにより複数の WWW／BM サーバに対して負荷分散を行うことが可能になり、WWW／BM サーバでのレスポンス低下を緩和する。

（2） WWW／BM サーバの障害発生時の対応

障害発生時には、障害の発生していない WWW／BM サーバのみを利用し、WWW／BM サーバからの応答が中断することを回避する。

また、ロードバランサ自身の障害も考慮して、ロードバランサの二重化（ホットスタンバイ）を行う。

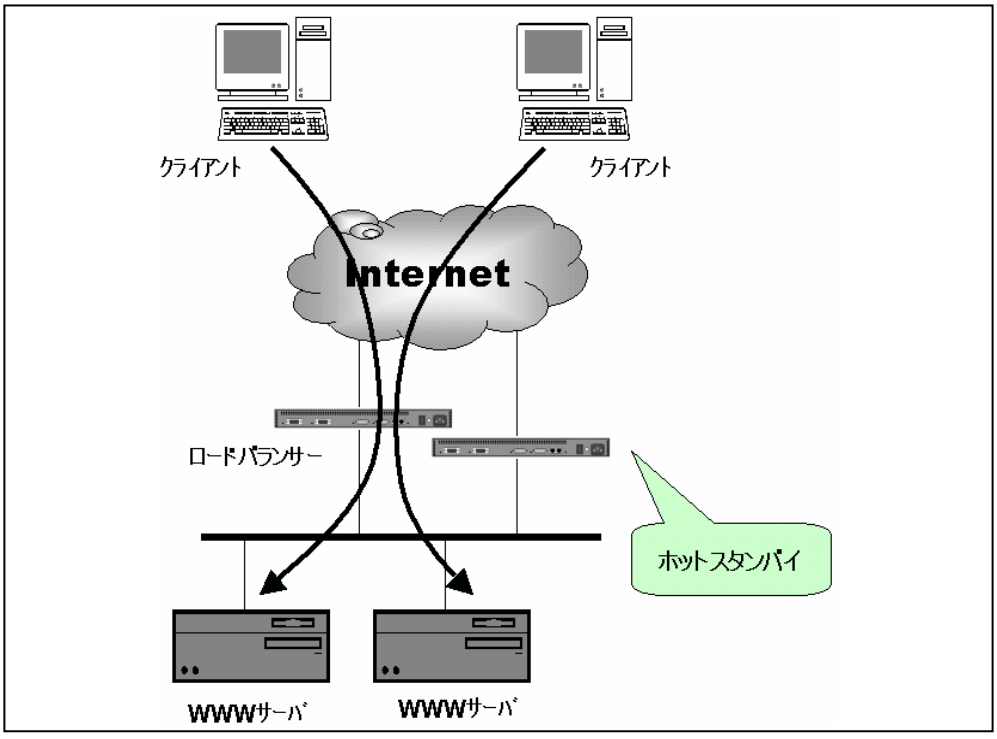

図 2.4 WWW サーバの構成例

2.1.3.2 SSL アクセラレータによる HTTPS（SSL）処理の高速化

SSL アクセラレータを設置することで以下の要件を満たす構成とする。

- SSL アクセラレータによって HTTPS（SSL）処理を高速化する。
- SSL アクセラレータによりロードバランサの負荷分散の精度を向上する。
- SSL アクセラレータとロードバランサを使用することでセッションの保持を行う。
- SSL アクセラレータ本体も冗長化構成を行う。

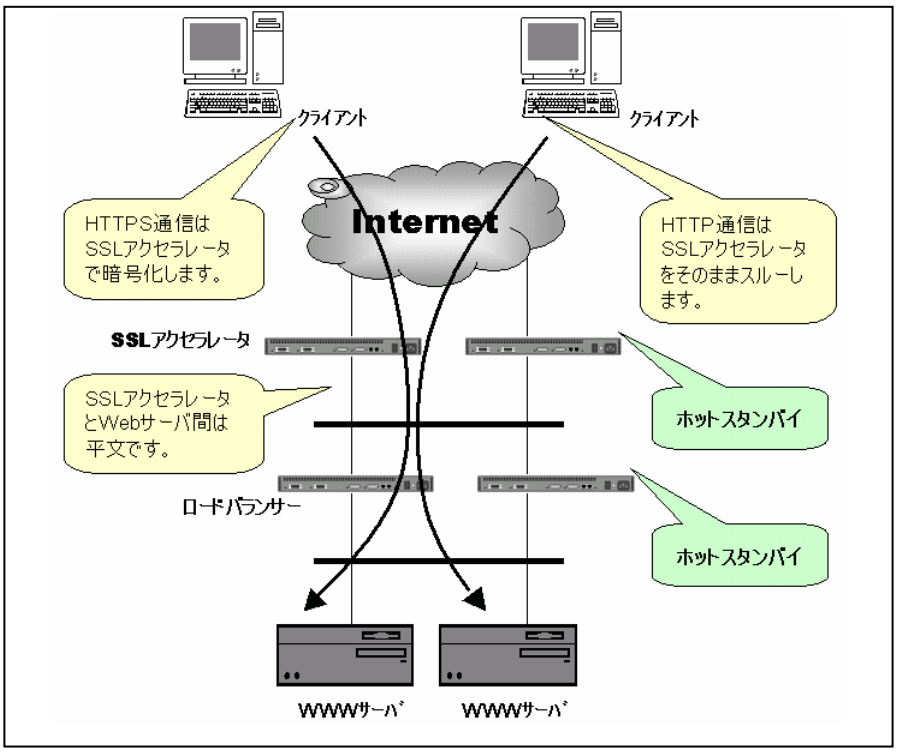

図 2.5 SSL アクセラレータの設置例

（1） 高速化

HTTP の暗号化処理を専用機（SSL アクセラレータ）で行い、WWW サーバの処理能力の低下防止と HTTPS の高速化を実現する。

（2） 負荷分散の精度向上

SSL アクセラレータを利用することによってロードバランサでは平文にて通過する。このため、クライアントが Proxy 経由でアクセスした場合でも端末単位での振り分けが可能となり、負荷分散の精度が向上する。

（3） セッション保持

SSL アクセラレータとロードバランサを組み合わせることで Cookie 情報を元にセッションの保持を行うことができる構成とする。

（4） 信頼性向上

SSL アクセラレータの障害を考慮し、二重化（ホットスタンバイ）することで障害発生に備える。

2.1.3.3 データベースサーバのフェールオーバ時の障害対応機能

障害が発生し、データベースサーバのフェールオーバが必要な場合に、BM サーバとして適切な処理が実施できるように以下の要件を満たす構成とする。

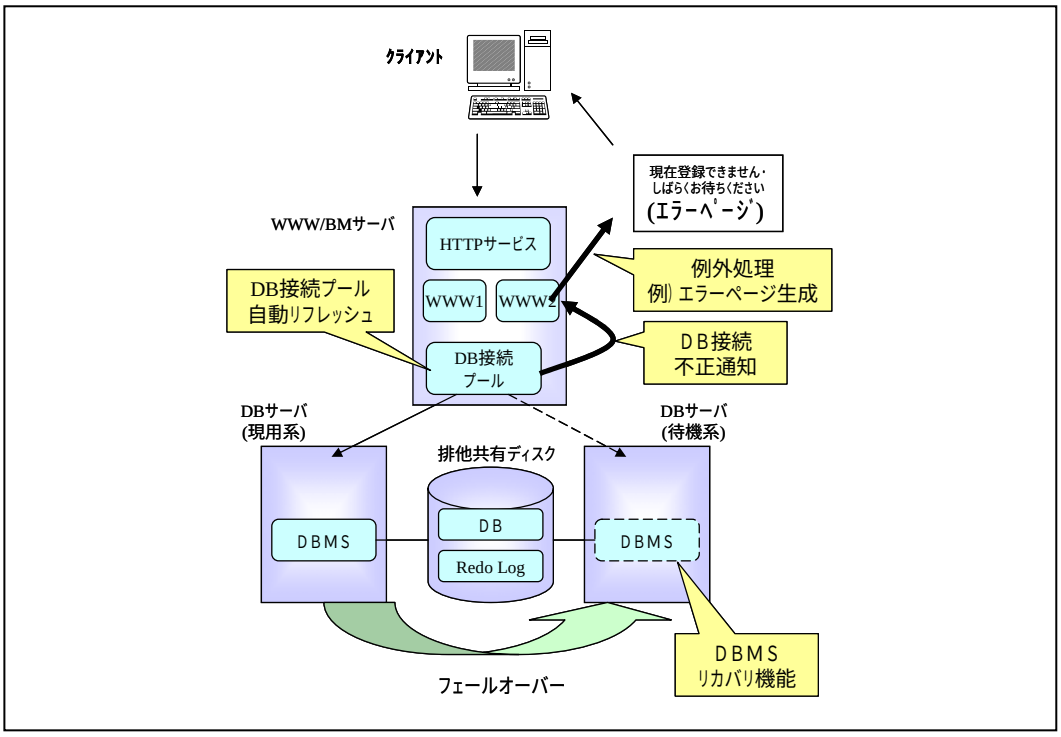

図 2.6 フェールオーバの対応

（1） データベース接続プール自動リフレッシュ機能

障害によってフェールオーバが発生した場合、接続プールの自動リフレッシュ機能によって、接続プールを保持してデータベース接続を正常な状態に保つことが可能な構成とする。

（2） データベース接続不正通知

フェールオーバによって一時的にデータベース接続ができない場合、データベース接続プールの自動リフレッシュ機能からデータベース接続不正との旨のメッセージを返却する機能を保持する必要がある。

（3） AP 例外処理

データベース接続プールからの不正通知を受信し、BM サーバにてエラーページを表示するなどの適切な対応ができる構成とする。

（4） DBMS リカバリ機能

フェールオーバが発生した場合、DBMS のリカバリ機能と連携してトランザクションデータを保護する。コミットされていないデータはロールバックされ、トランザクションとしての一貫性が保証される構成とする。

2.1.4 データベースサーバの信頼性・拡張性

データベースサーバの信頼性・拡張性を確保するため、以下の要件を満たす構成とする。

- クラスタ化によるフェールオーバ構成
- サーバ間通信をファイバチャネルで多重化接続することで、高速化／信頼性を向上する

2.1.4.1 クラスタ化によるフェールオーバ構成

データベースをクラスタ化にすることで以下の要件を満たす構成とする。

- クラスタ構成により、障害発生時は自動的にフェールオーバさせることで停止時間の短縮を図る。
- 仮想アドレス機能を利用し、クライアントからはどのマシンで処理されているかを考慮する必要のない構成にする。

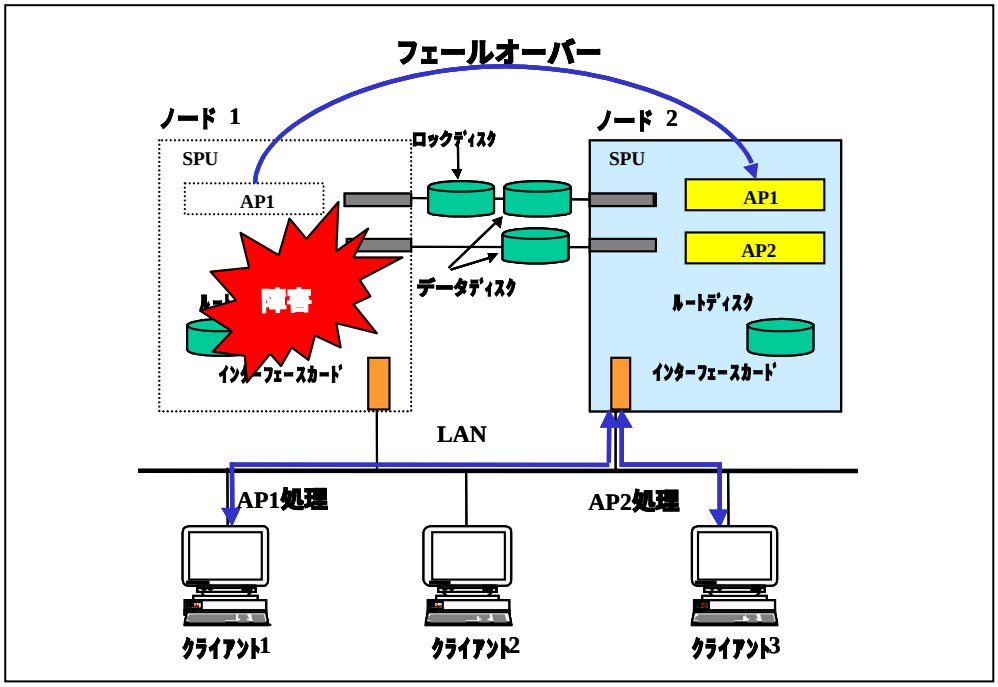

図 2.7 データベースサーバのクラスタ構成例

（1） マシン停止の対応

AP１をノード２で自動的に起動し、処理を再開させることができる構成にする。

但し、マシン停止時の処理を継続するのではなく、クライアント（BM サーバ）からの再要求で正常に接続可能となる構成とする。

（2） アプリケーション障害の対応

ノード１で再起動しても動作しないアプリケーション障害が発生した場合、（1）と同様にノード２で自動的に起動し、処理を再開させることができる構成とする。

なお、フェールオーバ処理ではデータベースシステムの整合性チェックを行う必要があるため、クラスタリングの一般的な復旧時間として 30 分程度の停止時間を要することは許容する。

2.1.4.2 多重化ファイバチャネル接続

サーバ間接続については以下の要件を満たす構成とする。

- ファイバチャネル技術により、サーバ間通信、ディスクアレイ接続の高速化を図る。
- 装置間をファイバチャネルハブで多重接続することで、高速化、信頼性の向上を図る。
- 高性能ディスクアレイ装置を利用し、大容量データの格納、高速アクセスを可能にする。

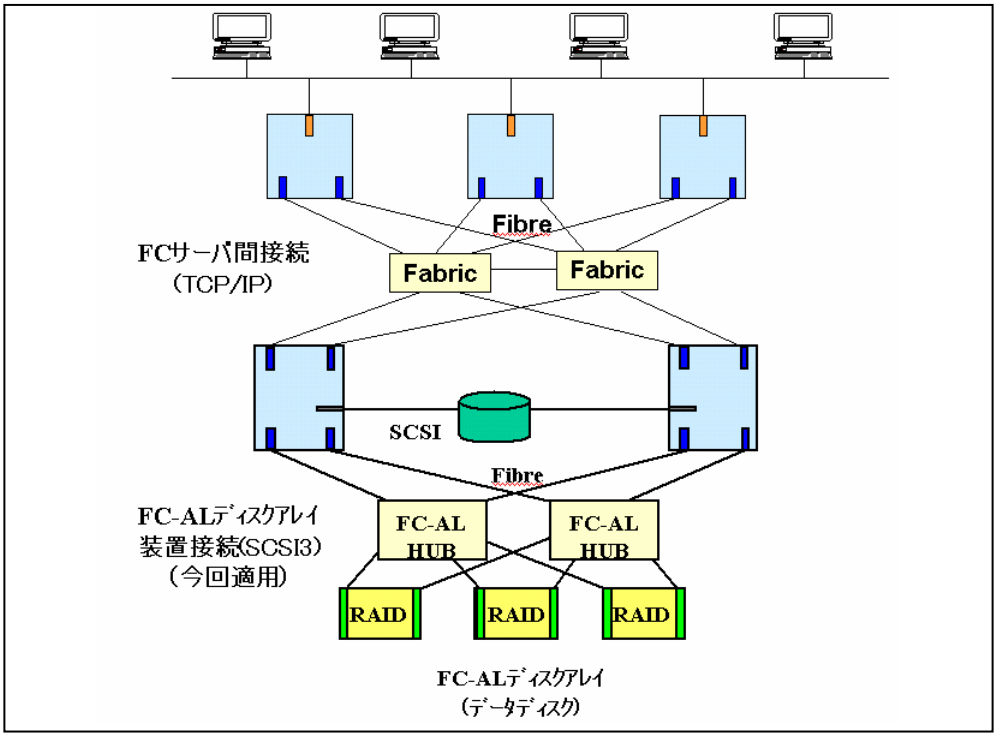

図 2.8 多重化ファイバチャネル接続の構成例

（1） ファイバチャネル間接続

ディスク I/O および内部サーバ間通信を高速化するためファイバチャネルを利用することを原則とする。また、ファイバチャネルハブを二重化、カスケード接続することにって通信のリカバリを高速に実行できる構成とする。なお、他の構成との状況からファイバチャネルに代わり、1000BASE/SX を使用することも可能とする。

（2） FC-AL ディスクアレイ装置接続

FC-AL ハブを中継することにより、複数のディスクアレイへのパスを集約し、マシン側と接続することが可能な構成とする。

（3） 高性能ディスクアレイ装置

ファイバチャネル接続に対応した高性能ディスクアレイ装置を設置する。要件としては、大容量ディスクを搭載可能、かつ、1 コントローラあたり 64M～1GB の大容量キャッシュを搭載可能である、高速ディスクアクセスが可能な装置とする。

2.1.5 メールサーバの信頼性・拡張性

他の主要サーバと同様にメール中継サーバを二重化し、プライマリメールサーバに障害が発生した際にもメール配信がストップしない構成とする。

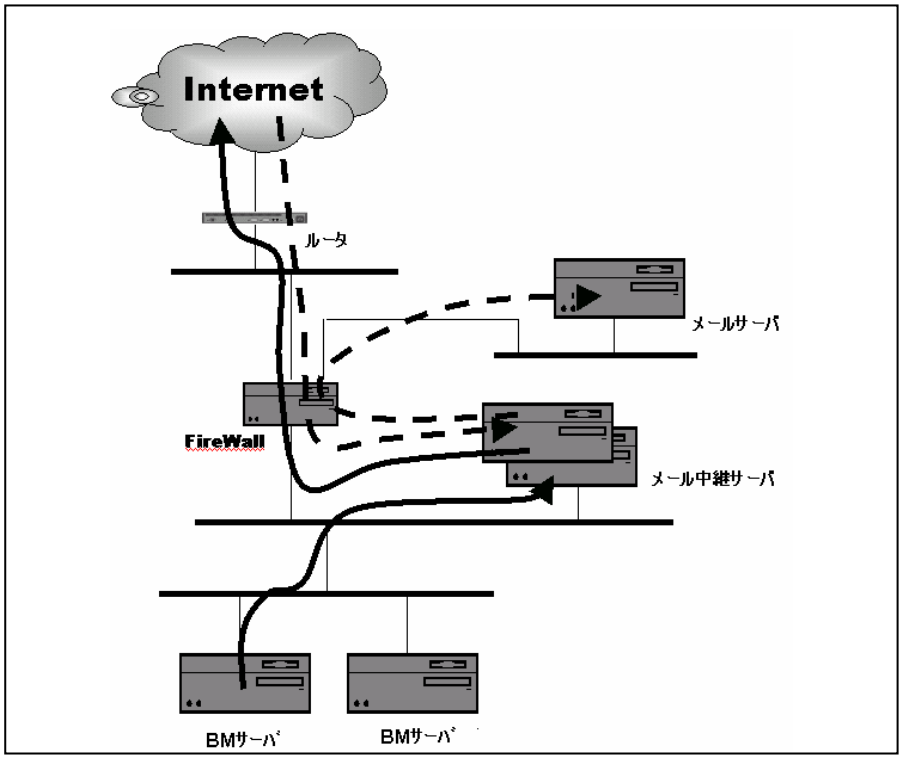

図 2.9 メール中継サーバの多重化構成

（1） メール配信（BM サーバ⇒外部）

メール中継サーバを二重化することによって、プライマリメール中継サーバで障害が発生した場合でも、セカンダリメール中継サーバが処理を代行す

ることで、ＢＭサーバから送信されたメールを継続して配信することができる構成とする。

（２） メール受信（外部⇒メールサーバ）

メールサーバに障害が発生した場合でも、外部から受信したメールをメール中継サーバに保持することができる構成とする。また、メール中継サーバを二重化することによって、プライマリメール中継サーバで障害が発生した場合は、セカンダリメール中継サーバが処理を代行する。

２.１.６ 通信サーバの信頼性・拡張性

（１） クラスタ切り替え

ハードウェアおよび通信サーバのクラスタ機能により、現用系がハードウェア障害やネットワーク障害で停止した場合でも待機系で継続運用が可能となる構成とする。なお、障害発生からフェールオーバ完了までに、障害検知、リソース切り替えおよび旧待機系サーバ上のサービスの起動等が必要であり、フェールオーバが完了するまで一定時間が必要となる。フェイルオーバ完了までの時間については実装するハードウェアの性能等を勘案して適切な時間に設定する。

さらに、通信サーバ上のプロセスが停止した場合でも上記と同様に、ハードウェアおよび通信サーバのクラスタ機能によって待機系で継続して運用することができる構成とする。なお、大手企業および中小企業に設置されている通信サーバの信頼性確保については、各社にて定めるものとする。

（２） ASP サイトの通信サーバからの再送制御

クラスタ切り替えおよび障害復旧を自動化するためにはクラスタ切り替えが完了するまでの間、送信元の通信サーバからデータを再送する必要がある。このような理由から高い耐障害性が求められるASPサイトの通信サーバについては、クラスタ切り替えが完了するまでの間、障害発生によって送信に失敗したデータを再送できる構成および設定とする必要である。

（３） データベース

通信サーバにて利用するデータベースについては、業務用データベースの構成に準じた構成とする。

2.1.7 CA サーバの信頼性・拡張性

CA サーバについては、セキュリティ方針によって外部の CA サーバを利用される場合も想定される。以下は CA サーバを内部にて管理する場合の構成についての要件を記述するものである。

（1） クラスタ構成

CA サーバも高可用性を実現するため、通信サーバと同様のコールドスタンバイのクラスタ構成とする。

（2） 鍵管理

秘密鍵は FIPS 140-1 レベル 3 相当の HSM（ハードウェア・セキュリティ・モジュール）製品にて管理することにし、安全性を十分に確保する。ただし、セキュリティ方針によって、適切なセキュリティを確保できると判断される構成であれば、上記レベルに達していない構成も可能とする。

（3） データベース

データベースについては業務用データベースと同様の高可用性を実現できる構成とする。

2.1.8 FireWall の二重化（ホットスタンバイ）

FireWall については二重化構成として、ホットスタンバイ機を設置し、現用系のハードウェア障害やネットワーク障害が発生した場合でも待機系を利用して運用を継続することができる構成とする。

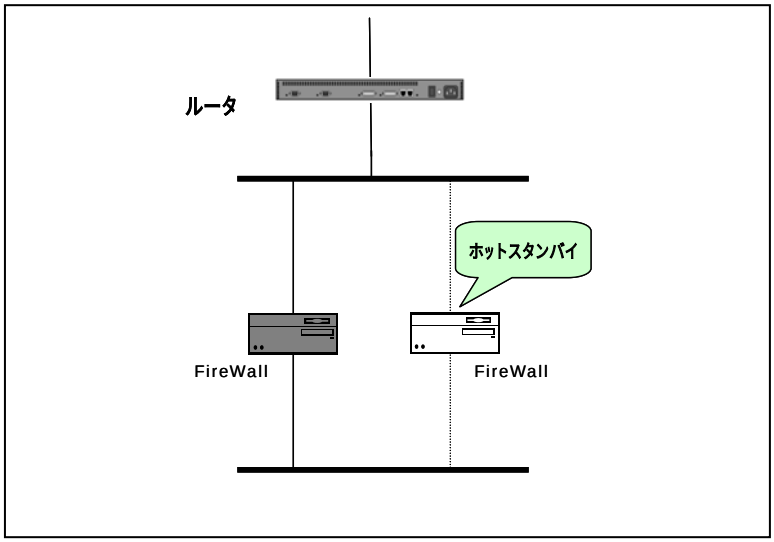

図 2.10 FireWall の二重化構成例

2.2 データセンタ

2.2.1 設置要件

システムを運用するサーバの安全性を維持するために、サーバが設置されている施設、設備面における施設環境、冗長化構成、入退出のあり方などの運用環境について規定する必要がある。

要件については「セキュリティ設計書」にて記述する。

2.3 運用管理

データセンタでの24時間365日運転を前提としたシステム運用要件は以下の通りとする。なお、運用管理を実現するために必要な保守契約は締結することとし、以下の内容については保守契約を締結していることを前提として記載する。

なお、FireWall、IDS、ウィルスチェック、CAサーバ等のセキュリティ関連の運用については、別紙「セキュリティ設計書」にて記載する。

表 2.11 運用要件一覧

	対象								機能
	www /BM	CA	DB	連携	DNS	Mail	NW 機器	FW	
構成管理	●	●	●	●	●	●			各ﾉｰﾄﾞの HW、SW 構成管理
障害管理	●	●	●	●					HW 監視、障害通報
	●	●	●	●	●	●	●	●	ﾉｰﾄﾞの死活監視
	●	●	●	●	●	●	●	●	SNMP ﾄﾗｯﾌﾟ監視
	●	●	●	●	●	●			OS の障害監視(syslog など)
	●	●	●	●	●	●			ﾐﾄﾞﾙｳｪｱ、ﾃﾞｰﾀﾍﾞｰｽの障害監視
	●	●	●	●	●	●			業務ﾒｯｾｰｼﾞ監視
性能管理	●	●	●	●	●	●			ﾉｰﾄﾞの各種資源の使用状況監視
	●	●	●	●	●	●			ﾉｰﾄﾞの各種資源の統計情報収集
	●	●	●	●	●	●			ﾉｰﾄﾞの各種資源の閾値監視
							●		ﾈｯﾄﾜｰｸ性能監視、統計情報収集
ﾌﾟﾛｾｽ管理	●	●	●	●	●	●			ｱﾌﾟﾘｹｰｼｮﾝ、ｻｰﾋﾞｽの死活監視
ｼﾞｮﾌﾞ管理	●	●	●	●					ｼﾞｮﾌﾞﾈｯﾄﾜｰｸの設定
	●	●	●	●					ｼﾞｮﾌﾞの自動ｽｹｼﾞｭｰﾘﾝｸﾞ、自動運転
	●	●	●	●					ｼﾞｮﾌﾞの稼動状況監視
ﾊﾞｯｸｱｯﾌﾟ管理	●	●	●	●	●	●			OS 領域のﾊﾞｯｸｱｯﾌﾟ、ﾘｽﾄｱ
	●	●	●	●	●	●			利用者領域のﾊﾞｯｸｱｯﾌﾟ、ﾘｽﾄｱ
			●						ﾃﾞｰﾀﾍﾞｰｽのﾊﾞｯｸｱｯﾌﾟ、ﾘｽﾄｱ
	●	●	●	●	●	●			媒体管理(世代管理)
ﾃﾞｰﾀﾍﾞｰｽ管理			●						ﾃﾞｰﾀﾍﾞｰｽ構成管理
			●						ﾃﾞｰﾀﾍﾞｰｽ性能管理
			●						ﾌﾗｸﾞﾒﾝﾃｰｼｮﾝ解消、再編成
ｻｰﾋﾞｽ管理	●	●				●			ｱﾌﾟﾘｹｰｼｮﾝ、ｻｰﾋﾞｽの死活監視

●：適用項目　　無印：対象外項目

2.3.1 障害監視

（1） 障害管理の役割分担

障害管理は以下の役割分担で行う。

表 2.12 障害管理の役割分担

作業項目	サイト 運営管理者	運用 SE	運用監視員 (運用ＯP)	保守センタ	アウトプット
HW 監視					
監視			◎	◎	
調査・処置		○		◎	
報告・管理	○	○	○	◎	メンテナンスレポート
死活監視					
監視			◎		
調査・処置		◎		◎	
報告・管理	○	◎	○	◎	メンテナンスレポート 障害報告書／障害管理台帳
ﾒｯｾｰｼﾞ監視					
監視			◎		
調査・処置		◎			
報告・管理	○	◎	○		障害報告書／障害管理台帳
巡回監視					
監視					
調査・処置					
報告・管理					メンテナンスレポート 障害報告書／障害管理台帳

◎・・・作業項目の内容を主体となって行う担当者。

○・・・作業主体の担当者からの作業依頼・報告を受けて、作業を行う担当者。

障害報告の際は、HW はメンテナンスレポート、SW は障害報告書で、各担当者からサイト運営責任者に報告する。サイト運営責任者および運用 SE は障害報告の内容を障害管理台帳に記載して情報管理を行う。

（2） ハードウェア障害通報

通常運用時の障害監視については、導入したハードウェアの管理機能に応じて以下の方式を単独もしくは組合せて実施することとする。

① 監視センタの管理機能による死活監視

ハードウェア障害が発生し、マシンダウンが発生した場合には運用監視員に自動通報される。運用監視員はマシンの動作状況から障害の状況を確認する。

運用監視員は、ハードウェア障害が確認された場合には保守センタ宛てに通報し、保守センタによって復旧作業を行う。なお、監視は 24 時間体制で行うこととする。

② 運用監視員による巡回監視

運用監視員が巡回にて各機器の状態を確認する。

各ランプの点灯が通常状態でない場合、運用監視員から保守センタに通報し、保守センタにて復旧作業を行う。

巡回は運用マニュアルに従って日々、固定時刻に実施する。

③ ハードウェア障害の自動通報機能による監視

ハードウェア障害が発生した場合、保守センタに自動通報される。保守センタは通報を確認後、復旧作業を行う。

監視は 24 時間体制で実施する。

（3） ハードウェア障害通知における復旧までのプロセス

① 各監視方法で異常が検出された場合、運用監視員はハードウェア／ソフトウェアの切り分けを行った後、サイト運営管理者、運用 SE、保守センタに対して障害が発生したことを通知する。

② ハードウェア障害の場合、保守センタは、サイト運営管理者の承認後、故障ハードウェアを交換・動作確認後に運用 SE に対して動作確認を依頼する。なお、障害切り分けのために必要に応じて保守契約ベンダに対して問合せを行う場合もある。

③ 運用 SE は運用マニュアルに基づいて動作確認を行う。

④ 運用 SE は動作確認完了後、サイト運営責任者に障害報告書を提出するとともに障害管理台帳に記録する。

⑤ 保守センタは障害復旧後、メンテナンスレポートをサイト運営責任者に提出

する。

（4） 死活監視／SNMP トラップ

監視対象である各サーバに対して、Ping 送信することによってサーバの死活を監視する。Ping 送信の応答が規定回数以上ない場合には SNMP トラップで運用監視員宛てに通知する。復旧は保守センタにて運用マニュアルに従って対応する。

（5） 死活監視・SNMP トラップにおける復旧までのプロセス

① 死活監視／SNMP トラップにより異常が発生した場合、監視サーバから運用監視員に自動で障害通報が行われる。

② 運用監視員はハードウェア／ソフトウェア障害の切り分けを行って、サイト運営管理者、運用 SE、保守センタに対して障害通知を行う。ハードウェア障害は、障害通知に準じた処置を行う。

③ 障害切り分けにより通知を受けた担当者（運用 SE または保守センタ）は原因調査を行い、サイト運営管理者の承認の後、障害対応を実施する。

④ 運用 SE は運用マニュアルに基づいて動作確認を行った後、サイト運営責任者に対して障害報告書を提出し、障害管理台帳に記録する。

（6） メッセージ監視

ＯＳ、ミドルウェア、業務ログのメッセージ監視を行い、障害発生時には運用監視員宛てに障害通報を行う。メッセージ監視については、フィルタリング機能を利用することで監視対象メッセージを選別することとする。また、業務ログについては業務要件に基づいてあらかじめ規定したルールに従ってメッセージを監視する。

障害発生時の復旧は、運用監視員が運用マニュアルに従って対応する。

2.3.2 性能監視

（1） 使用状況、統計情報監視

運用要件一覧に記載されている監視対象である各サーバについて、定期的に使用状況を収集する。毎月、動作指標を集計し、サイト運営責任者に報告する。

（2） 閾値監視

監視対象サーバに対して定期的で動作状況を取得し、超過した動作指標についてはアラーム通知を行う。閾値を超過した場合、運用監視員では運用マニュアルに従って対応する。

WWW サーバ、ビジネスモジュールサーバ、データベースサーバなどのミッションクリティカルな業務に関するサーバは、全ての動作指標を監視する。また、性能要件から判断して負荷が低いと考えられる一部サーバ（メール・DNS サーバなど）については、一部の動作指標（例えば、ディスク使用量のみ）のみを監視対象とし、それ以外の項目は定期的な報告のみとする運用も可能とする。なお、監視項目については運用状況の変化によって見直しが必要であるため、定期的に監視項目を再検討するものとする。

（3） レスポンス測定

アプリケーション等のレスポンスについては、必要に応じてテストプログラムを作成し、レスポンスデータを取得する。レスポンス測定の周期や保存間隔などは運用マニュアルにて規定する。

集計した性能レポートに基づいてサイト運営責任者は性能分析を行い、チューニングや設備投資の計画立案を行う。

（4） 性能レポート

採取したデータセンタ内のサーバ性能情報は、毎月、サイト運営管理者が定めた１日分の動作指標を集計して性能レポートとして提出する。

① 毎月のレポートについては運用監視員が作成し、サイト運営管理者、運用 SE に提出するものとする。

② サイト運営管理者、運用 SE は、性能レポートに基づいて現状分析を行い、性能に問題がある場合には、アプリケーション等のチューニングや機器増設等の施策立案を行う。

2.3.3 プロセス管理

プロセス管理は、ジョブ管理機能を利用して定期的に監視ジョブを起動することでプロセスの死活を検出する。

異常が検出された場合にはデータセンタにて運用マニュアルに基づいて対応を行う。

2.3.4 ジョブ管理

（1） 自動運転

ジョブ情報は最も信頼性の高いデータベースサーバ上で一元管理することでサーバ間のジョブネットを実現する。ジョブは事前にスケジュールされた情報に基づいて自動運転を行う。

（2） 稼動監視

障害監視にてジョブの異常終了を検出した場合には、データセンタにて運用マニュアルに従って対応を行う。

定時監視のための確認メッセージやオペレーションのための指示メッセージは、前述のメッセージ監視を利用する。障害が検知された場合には運用監視員は運用マニュアルに従って対応を行う。

（3） ジョブ起動

ジョブの起動方法としては用途に応じて以下のいずれかを選択することが想定される。よって、ジョブ管理プログラムとしては以下と同等の機能を有したシステムである必要がある。

- 自動起動

  起動条件を持たない定時ジョブに適用する。起動条件（例えば、先行ジョブで作成されたファイルの利用など）を持つジョブに適用する場合は、本ジョブにて条件を満たさない場合の処置（先行ジョブのファイルが作成が未完了の場合は処理をスキップして終了するなど）を組み込む必要がある。

- オペレータ起動

  オペレータの起動判断（例えば、バックアップ媒体の装填など）が必要なジョブに適用する。オペレータに起動条件を判断させるための手段として、前述のメッセージ監視を利用することもできる。

- トリガー起動

  先行ジョブの終了以外に起動条件を持ち、その条件を自動判断できるジョブに適用する。例えばオンライン処理などからの起動を指示することが可能である。トリガーとしてはファイルの作成／削除／更新やイベントの通知を考慮する必要がある。

2.3.5 バックアップ管理

（1） バックアップ運用

バックアップ運用は前述のジョブ管理機能を利用し、運用ジョブに組み込んで実施する。バックアップの失敗はジョブの異常終了としてデータセンタに通知される。異常発生時の復旧は、運用監視員にて運用マニュアルに従って対応する。

バックアップはＯＳ毎にドメインを構成し、ネットワークバックアップを実施することで集約化を実現する。

バックアップ装置としては大容量の媒体を利用することとし、媒体交換作業を効率化することとする。なお、バックアップ媒体については耐用年数もしくはバックアップ媒体に障害が発生した場合に交換を行うものとする。本運用は、老朽媒体の交換を含め運用監視員もしくは保守センタが運用マニュアルに従って対応する。

（2） ドメイン構成

バックアップの効率化およびセキュリティの観点からバックアップドメインを以下の基準にて分割する。

- FireWall の内外で、バックアップドメインを分割する。
- データベースサーバのような性能の確保やバックアップ時間に制約のあるサーバは単一サーバ単一ドメインとして構成し、自身のローカルバックアップを実施する。

2.3.6 データベース管理

（1） 性能監視

データベースは運用開始後の初期状態から本格的に稼動後の安定運用期などの各データ状態によって、最適なアプリケーションの処理方法が異なる。このため、アプリケーションの性能監視と合わせてデータベースの性能監視を定期的に実施する必要がある。

性能監視にて問題が発覚した場合には、アプリケーションの改善やハードウェアの設備増強などをサイト運用管理者にて検討する。

（2） 再編成

表やインデックス等のデータベース構成要素のフラグメンテーション解消のため、定期的に各構成要素の再編成が必要になる。本作業については運用監視員が運用マニュアルに従って対応する。

また、インデックスの再編成などについては前述のジョブ管理機能を利用して定期的に運用ジョブから実行することもできる。

2.3.7 サービス管理

（1） サービス管理

サービス管理は、サービス管理ツールの自動レスポンス測定機能を利用して、初期導入時のチューニングまたは本番後に性能問題が発生した場合に実施する。ここで、サービスとは複数のプロセスが強調して実現する一つの機能を示す。

各サーバのサービス（WWW、データベースなど）ごとにアクセスを行い、サービスの死活・性能監視を行う。

サービスに問題が発生した場合には、運用監視員が運用マニュアルに従って対応する。