高可用性（HA）システム フレームワークと応用
High-Availability System Frameworks and Their Applications

関　悦夫 E. Seki
小林　茂 S. Kobayashi
吉羽　宏 H. Yoshiba
掛札　榮昭 H. Kakefuda
伊達　俊彦 T. Date
松原　宗志 N. Matsubara
加藤　信行 N. Kato
田岡　一詩 H. Taoka
木下　善貴 Y. Kinoshita
浅野　俊明 T. Asano
小松　智 S. Komatsu

高可用性（HA：High Availability）システムの設計を効率化するために，HAシステムのフレームワークに基づく設計支援を導入した。フレームワークとは，システム構成，およびサービス引継ぎなどのシステムのふるまいを類型化したものである。各フレームワークに類するシステムの開発を，HAシステム設計支援機能における典型システムのサポートと，ドキュメントによるガイドの提供により支援する。当社は従来からさまざまなHAシステムを開発し，その経験を通して業種，業務や規模に応じたフレームワークを見いだしてきた。ここではHAシステム フレームワークの概要と，五つのシステム事例を紹介する。

To improve the efficiency of the design phase of high-availability (HA) systems, we have introduced a framework-based design method. An HA system framework is an abstract and typical system design. It includes information about the system composition and system behavior such as the taking over of services. For each framework, a template for the HA system development facility is provided as well as documentary guidance. Toshiba has developed many HA systems and determined various HA system frameworks according to the type of industry or business as well as the system scale.

In these papers, the concept of an HA system framework is explained and some actual HA systems are described.

HAシステム フレームワーク概要
General Description of HA System Framework

1 まえがき

当社は，これまでプラント制御システムや基幹業務などの多数のシステム開発を行い，HAシステム構築技術を蓄積してきた。これらのシステムは，従来，主としてミニコンやオフコンなど当社独自のサーバを用いて構築してきたが，最近では，オープン化・ダウンサイジングの流れに対応して，UNIX(注1)サーバ（OS：Solaris(注2)，AIX），あるいはPCサーバ（OS：WindowsNT®(注3)）などのオープンサーバ上で構築することが多くなっている。

HAシステムでは，さまざまな障害のケースも含めてシステムの動作を考慮しなければならないため，設計が複雑になる。HAシステムの構築におけるソフトウェア開発を容易にするために，現在，各社からHAサポート ソフトウェアが提供されているが，それによっても設計の困難さは単純には解決されない。しかし，これまでのシステム構築の経験から，HAシステムにはいくつかの類型があることが認識されてきた。

HAシステム フレームワークは，その類型を抽出し，既存のノウハウと成果物を最大限に活用することを目的としている（図1）。

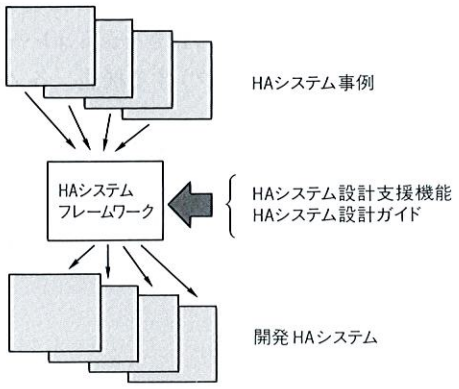


図1．フレームワークの抽出と適用　HAシステム事例から抽出したフレームワークに，目的システムの固有値を設定し，設計情報を生成する。
Extraction and application of HA system framework

（注1）UNIXは，X/Openカンパニーリミテッドがライセンスしている米国ならびに他の国における登録商標。
（注2）Solarisは，米国SunMicrosystems社の商標。
（注3）WindowsNTは，Microsoft社の商標。

2 HAシステムのフレームワークとは

HAシステムの設計では，可用性の確保の上で，システムのどこが弱点となるかを見極め，その障害を回避・復旧する方式を決定する必要がある。そのときに考慮しなければならない主要な問題は，HA戦略の策定と，機能・性能やコストなどの諸要件間のトレードオフである。

HA戦略とは，障害発生時のバックアップ処理をはじめとする，高可用性の実現のためのシステム動作・運用を規定するものである。当社HAサポート ソフトウェアでは，この戦略を記述したものを“HAシナリオ スクリプト”と呼び，専用に開発したプログラミング言語で記述する。HAシナリオ スクリプト作成時の主な設計項目には，例えば次のものがある。

(1) システム立上げ時のサービスの実行状態
(2) 監視／検出する障害要因
(3) 各種障害検出時の処理
(4) サービスの起動／停止／引継ぎの各タイミングでの処理

HAシステムにおいて，トレードオフの必要を生ずる要件パラメータには，例えば次のものがある。

(1) 連続稼働時間，所要復旧時間
(2) 稼働時性能
(3) データの一貫性や保全性
(4) 運用の容易性
(5) 各種コスト

HAシステムの形態は，上述の問題にシステム構成（ハードウェア，ネットワーク，ミドルウェア，アプリケーションなど）を加えた，全体の相互関連を見ながら設計されなければならない。従来は，システムエンジニアやアプリケーションの開発者が，経験を通して見いだしたノウハウに基づいて，HAシステムを構築していた。

しかし，HAシステムの形態はすべてがまったく異なるものではなく，業種／業務／規模によって，いくつかの類型的なシステム形態がある。例えば，自治体の窓口業務システム，営業情報支援システム，製造・販売統合システムなどである。これらのシステムでは，HAシステム設計上のポイントとなる事項について特定の処理となる場合が多い。

これらの類型的システムに関するノウハウを定式化したものが，HAシステム フレームワークである。

3 HAシステム フレームワークの目的

HAシステム フレームワークを作成するには，まずシステム事例を収集して，それらの解析結果を基に類型を抽出し，それぞれのフレームワークを作る。これらを評価用システムの構築に適用し，細部の改善を行って完成度を高めていく。また，既存のフレームワークでうまく表現できない新たな形態のシステムについては，随時，フレームワークのレパートリ追加を行う。

このようにして，HAシステム構築のノウハウをHAシステム フレームワークとして集約しておくことによって，システムの高可用性を，より容易に，かつより確実に実現することが可能になる。これはシステムの設計・開発者だけでなくユーザにとっても，次のようなメリットがある。

(1) システム構築期間およびコストの削減が可能である。
(2) 洗練された定型的な処理手順を利用することにより，設計ミスによって二次障害を生ずるなどのリスクを低減できる。
(3) 標準的なシステム構成の採用により，固有の作り込みを少なくでき，システムの拡張性を高められる。

4 HAシステム フレームワークを用いた設計手順

HAシステム フレームワークは，当社のHAサポートソフトウェアの一部である，システム設計支援機能と密に関連している。設計支援機能では，業種／業務／規模ごとに各フレームワークに対応した，HAシナリオ スクリプトの雛(ひな)型を用意している。この雛型をHAテンプレートと呼び，その中のシステム固有のパラメータを設定することによって，目的のシステム用のHAシナリオ スクリプトを作成できる。

HAシステム フレームワークを用いて，実際のHAシステムを設計する手順は次のようになる。

(1) 業種／業務／規模を選択する　目的のシステムが属する業種／業務／規模を選択する。
(2) システム要件を抽出する　機能・性能・可用性などのシステム要件を抽出する。
(3) システム形態を決定する　ハードウェア，ネットワーク，ミドルウェア，アプリケーションなどのシステム構成とHA戦略を，設計ガイドの事例と解説に基づき決定する。
(4) HAテンプレートを選択する　HAシステム設計支援ツール上で，目的のシステム構成とHA戦略から成るHAテンプレートを選択する。
(5) HAシナリオ スクリプトを完成する　HAテンプレートの中の，システム固有のパラメータを設定して，HAシナリオ スクリプトを完成する。

5 あとがき

HAシステム構築をより確実，より容易にする，HAシステム業種／業務／規模別フレームワーク技術の概念を述べた。

現在，この技術をUNIXサーバ，およびPCサーバの，マルチプラットホーム上で適用している。今後は，異機種を結合したクロスプラットホームでのHAシステム実現などの機能強化と並行し，HAシステムフレームワークの充実を図り，多様なシステム形態に柔軟に対応できるHAシステム構築支援機能を提供していく予定である。

（関／小林）

気象情報配信システム
Meteorological Data Switching System

1 まえがき

気象庁は，各種観測データや予報データなどを全国の気象台や測候所などと交換し，外部にも発表している。気象データを送受信するシステムでは，近年の観測・予報技術の高度化，多様化に伴うデータ量の増大により，処理の高速化が要求されている。また，予報データや地震津波関連の緊急データを扱う24時間連続運転リアルタイムシステムのため，システムの信頼性が高いことも必須(す)条件である。

気象データの送受信を行う東京L-ADESS（東京・地方中枢気象資料自動編集中継装置）では，他の地方L-ADESSに先駆けて回線の高速化およびシステムの更新が計画された。当社では，UNIXサーバとHAミドルウェアを用いて複合系システムを構築した。オープンサーバを用いたHAシステムの一例として，以下にその概要を紹介する。

2 システムの位置づけ

気象庁は，図2に示すような，気象データ送受信用のシステムを整備している。東京管区内の場合，地方気象台や測候所などに集められた観測データは，東京L-ADESSに送信され，全国の気象データを集めるC-ADESS（気象資料総合処理システム）に送られる。

一方，東京で作成される予報の基礎データは，C-ADESSから東京L-ADESSに送られて，地方気象台などへ送信される。地震津波関連のその他のデータもL-ADESSを経由して送受信される。

以上からわかるように，L-ADESSのシステムダウンは気象データの交換を停止させることになるので，HAシステムの導入が要求される。

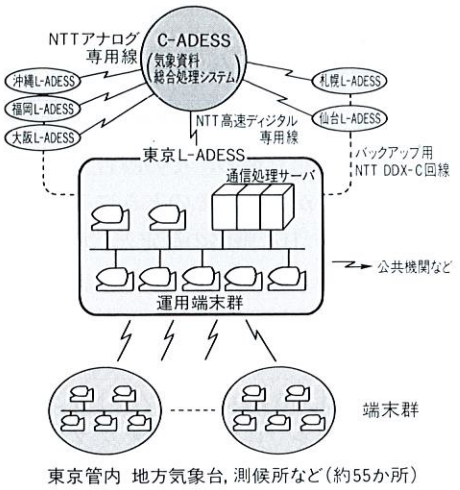


図2．東京L-ADESSの位置づけ　C-ADESSと端末群の中間に位置し，気象データの伝送において重要な役割を果たしている。

Conceptual configuration of meteorological data switching systems

3 システムの構成

図3に示すように，汎(はん)用のUNIXマシンを中心にシステムが構成される。通信処理など，主要な処理をするサーバ（以下，通信処理サーバと呼ぶ）には，高速CPUを搭載したUNIXサーバUX7000を採用し，HAミドルウェアおよび切換機などを用いて，ホットスタンバイ方式の複合系システムを構成している。通信処理サーバとLANで接続された運用系の端末には，UNIXワークステーションAS8000およびAS4035を採用している。

東京L-ADESSの運用上の操作は，運用部で行う。システムの変更・調整などは保守部，各種テーブルの変更・管理などは，テーブルメンテナンス部でそれぞれ行う。気象庁本庁に設置されている東京L-ADESSは，地方の各L-ADESSのシステム状態およびその収容回線をも監視する役割があり，全国L-ADESS監視部で各L-ADESS運用部との通信を行い，その状態を把握，表示する。

4 システムの特長

システムの特長は，以下のとおりである。

4.1 サーバの二重化

通信処理サーバは，ホットスタンバイ方式により二重化されている。通信処理サーバは，RAS（Reliability, Availability, Serviceability）カードおよび専用のEthernet(注4)を通じて相互監視を行い，運用系の障害時には待機系と運用系との切換えを自動的に行う。この際，切換え前の運用系の各処理の

(注4)　Ethernetは，富士ゼロックス㈱の商標。

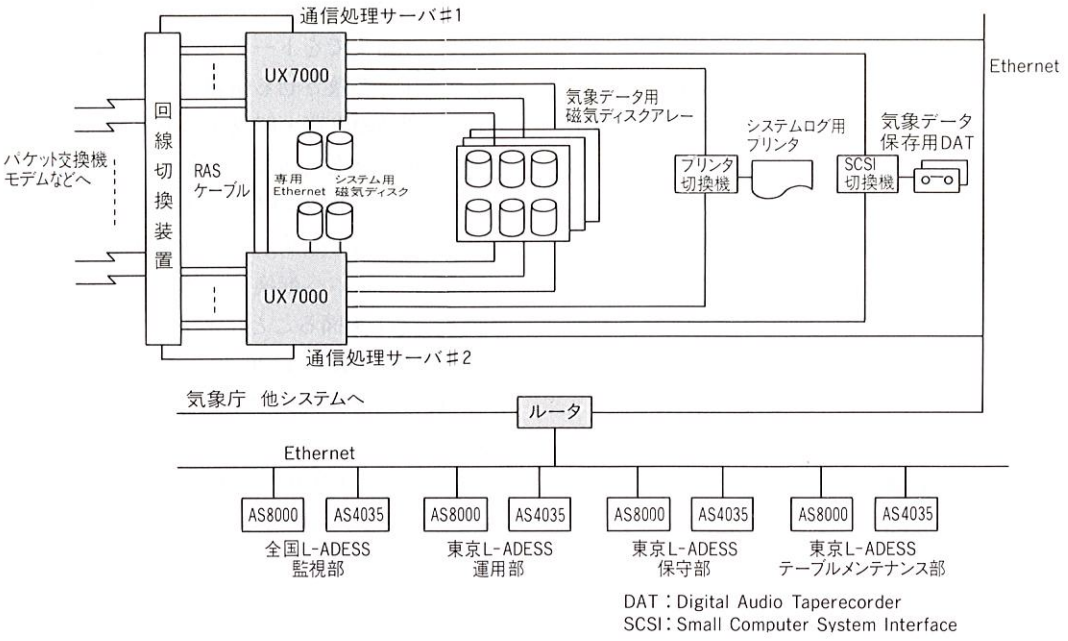


図3．東京L-ADESSの構成　ホットスタンバイ方式のUNIXサーバとUNIXワークステーションの運用端末群から成る，サーバ／クライアント方式を採っている。

Configuration of Tokyo L-ADESS

状態，データは共有のディスクアレーを通じて新しい運用系に引き継がれ，処理の連続性が保たれるようになっている。また，システムログ用プリンタや回線切換装置などのハードウェア資源も，サーバの運用系／待機系の変換に従い自動的に切り換えられる。IP（Internet Protocol）アドレスもつねに自動的に運用系に引き継がれるため，クライアントなどからは，IPアドレスの変更を意識する必要はない。

ソフトウェアやテーブルの変更作業，回線増設作業および保守作業なども，運用系／待機系の切換え（非障害時モード），システムからの切離しを行うことにより，システムの停止を伴わず作業可能となる。

4.2　磁気ディスク装置の二重化

通信処理サーバがおのおのもつシステム用磁気ディスク装置，共有する気象データ用ディスクアレーは，汎用ミドルウェアを用いて二重化されており，運用系磁気ディスクの障害時には，自動的に待機系磁気ディスクに切り換わる。運用系端末群についても，同様の方法でシステム用，データ用の磁気ディスク装置が二重化されている。

4.3　監視機能

運用部では，システムを構成する各装置を監視しており，ワークステーションに表示された模式的な構成図上に，正常（オンライン）・障害・オフラインの別を色分けして示している。通信処理サーバの運用系・待機系・障害などの状態も，同画面上の色分けで表示している。障害発生時には画面上の色の変化に加えて，チャイムなどで報知し，現業者の迅速な対応を可能としている。システムに収容される各回線の状態も監視されており，運用部のワークステーションに色分け表示されている。

なお，気象庁本庁に設置されている東京L-ADESSは，地方のL-ADESSシステムおよび収容回線の状態をも監視する役割がある。

全国L-ADESS監視部は，各地方L-ADESSの運用部との通信により，各装置・回線の状態を把握し，構成図上に色分け表示する。

4.4　ユーザインタフェース

運用部の各装置の状態などを表示する画面と回線の状態を表示する画面で，通信処理サーバの切換え・切離しなどのシステム制御や回線制御，詳細データの表示・出力指示などが，マウス操作によって可能となっている。通常の運用ではコマンドの入力などが不要なため，現業者の負担軽減に寄与している。

4.5　ソフトウェア配布機能

気象庁本庁は，各地方のL-ADESSを管理する立場にあるので，必要に応じて，東京L-ADESSからの遠隔操作により，ソフトウェアやテーブルの変更を同時に行えることが望ましい。汎用のソフトウェア配布用ミドルウェアを導入することにより，この機能を実現した。

4.6　省スペース化

汎用のUNIXサーバおよびワークステーションを中心としたシステム構築と，システム・回線監視機能で，従来の専用の監視盤の代わりに，ワークステーションを使うことで，省スペース化を実現した。

5 あとがき

気象システムでは，従来から培ってきた高信頼性・リアルタイム性に加えて，気象データ量の増加・回線の高速化に伴う処理の高速化，ユーザインタフェースの高度化，標準化などが要求されている。当社では，オープンサーバにHAミドルウェアを組み合わせることで，この要求を実現した。気象システムの構築にあたっては，従来からの技術に新しい技術をどう適応させるかが，最重要課題となろう。

（吉羽）

ロジスティクス情報システム
Logistics Information System

1 まえがき

ロジスティクスに課せられた一つの命題として，生産と物流を同期化させ，総在庫の圧縮を図るとともに，タイムリな物のデリバリにより顧客サービスの向上を図ることが挙げられる。これは経営効率と顧客満足度（CS）を同時に向上させ，ビジネスを拡大するための大きなステップとなる。これを実現するためにはビジネス形態に合致した情報システムの構築が不可欠となる。

㈱ダスキンでは，レンタル商品出荷業務などを担う全国物流センタと，レンタル商品の製造業務を担う工場に，当社のグローバル ネットワークサーバ GS シリーズを利用した物流管理システムと生産管理システムを構築・展開している。さらに本部スタッフ向けに，全国物流センタ／新製品製造工場の各種出荷・製造実績などをリアルタイムに収集・表示させること，および本部情報の全国配信などを目的に，当社エンタープライズ サーバ ES シリーズを利用した経営情報システムを構築している。また，双方のシステム連携によるロジスティクス情報システム（以下，LIS と略記）の構築により，レンタル商品の製造から出荷，回収，廃棄までのスルーした機能を実現している。

ここでは，HA システムを採用した LIS について紹介する。このシステムでは，PC サーバ，PC クライアントで構成されているシステム間の連携，24 時間自動運行などの高い信頼性が要求されている。

2 ロジスティクス情報システム

LIS は，㈱ダスキンのレンタルビジネス（家庭用モップ，業務用マットなどのレンタル）における，商品開発資材の調達，貯蔵および製品の開発・生産，保管，販売（レンタル），回収，廃却までをトータルなものの流れとしてとらえ，情報の流れと合致させる情報システムであり，現場における日々の商品の出荷・回収から全国レベルでの需給バランス，生産計画の立案支援などをカバーする。

今回の LIS 導入の大きなねらいは，これまでのホスト中心のバッチ的システムから，より情報鮮度の高いリアルタイムなシステムへ転換し，物の流れと情報の流れの合一化（情物一致）を図ることにある。

LIS は，代表的な PC サーバ／PC クライアント システムで，ヒューマン インタフェースをつかさどるクライアントは当社パソコン（PC）（PV シリーズ，TECRA シリーズ）で，物流センタ／工場サーバは当社 GS シリーズで，本部基幹サーバ／コミュニケーション サーバは当社 ES シリーズで構成する。クライアントとサーバ間は LAN で接続される。

また，サーバとサーバ間は直接接続させず，LIS オペレーションセンタ内のコミュニケーション サーバを介して NTT（日本電信電話㈱）ネットワーク網（ISDN 網）で接続される（図 4）。

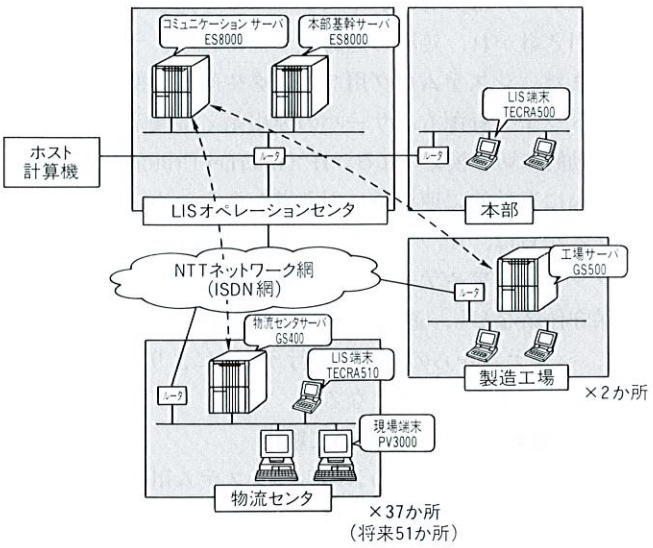


図 4．LIS 全体構成　LIS は，本部基幹サーバ，コミュニケーション サーバ，製造工場サーバ，物流センタサーバおよび PC で構成される。
Configuration of LIS

3 HA システム適用の背景とねらい

LIS では，本部基幹サーバ（1 台）と物流センタサーバおよび工場サーバ（計 39 台）間の接続用にコミュニケーション サーバを配置している。コミュニケーション サーバがなんらかの障害で停止した際，物流センタサーバ／工場サーバとの情報受配信がストップしてしまい，全国の生産物流

の統括管理機能（本部基幹サーバ）と物流センタの現場業務機能（物流センタサーバ）との双方で支障をきたすことになる。そこで，情報受配信の信頼性を上げる意味からHAシステムの適用を行った（図5）。

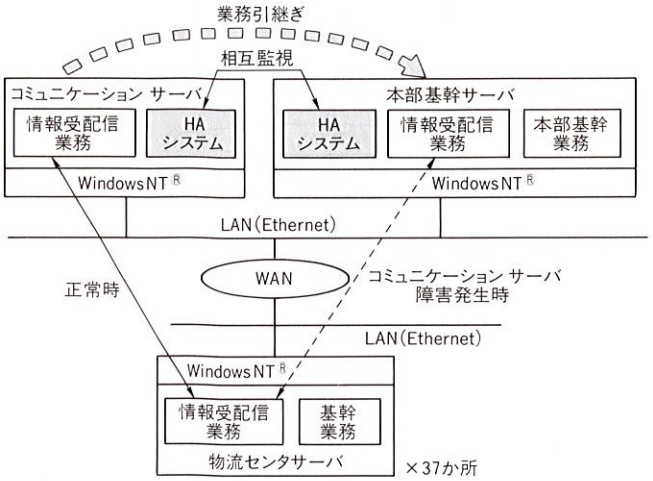


図5．LISへのHAシステム適用形態　コミュニケーション サーバにおける全国物流センタサーバ（37か所）との情報受配信処理を本部基幹サーバでバックアップする。

HA system architecture for LIS

LISに適用したHAシステムとは，コミュニケーション サーバを本部基幹サーバによって待機バックアップ可能としたシステムである。このシステムの基本的な処理形態例を示すと，通常稼働中は，コミュニケーション サーバが情報受配信業務処理を行い，本部基幹サーバがコミュニケーション サーバの稼動状況を監視し待機する。もしもなんらかの障害が原因でコミュニケーション サーバが停止した場合，待機中の本部基幹サーバがコミュニケーション サーバのLANのIPアドレスを引き継ぎ情報受配信業務処理を継続する。

4 PCサーバでのHAシステム技術

メインフレーム（ホスト）やミニコン，オフコンからUNIXサーバ，PCサーバへのダウンサイジングが進行するとともに，WindowsNT® の登場によって，PCサーバにより新たに基幹システムを構築する流れが出てきた。その流れの中でHA技術が注目を集めている。

今回LISに適用したシステムは，WindowsNT® をオペレーティング システムとするPCサーバにおいて，クラスタ（サーバ計算機を2台以上疎結合したシステム）による高可用性をサポートした“HAシステム for WindowsNT® ”である。

HAシステム for WindowsNT® では，二つのPCサーバがネットワークで接続されており，また，バックアップ方式は，相互バックアップの形態を取っている。そして，ネットワークを利用し相手のマシンの状態を監視すると同時に自マシンのアプリケーションやOS，ハードウェアの状態を監視し，自系に障害が発生した場合に他系に通知するようになっている。他系からの障害通知か正常通知のタイムアウトを検出すると，あらかじめ定めてあった手順に従い，他系の資源を引き継ぎ，他系の運用アプリケーションのバックアップを行う。これによりPCサーバシステム24時間自動運行に踏み切ることができた。

5 HAシステムの増強の将来構想

現在，LISでは，コミュニケーション サーバのバックアップとして本部基幹サーバを活用している。今後，情報受配信先である物流センタサーバが全国51か所に増えること，および情報受配信のデータの種類および利用頻度の増加が想定されることから，コミュニケーション サーバを新たに1台新設し，コミュニケーション サーバ2台によるHAシステム構築を検討中である。今年度中に，コミュニケーション サーバを2台構成とし，東日本エリア25か所，西日本エリア26か所に対しそれぞれ並行業務（情報受配信）を実施，片方で障害発生した際には，もう片方でバックアップするというHAシステムへと発展させる計画である（図6）。

これにより本部基幹サーバの負荷を低減し，本来の基幹業務サーバとしての位置付けに戻すことができる。またコミュニケーション サーバの負荷が2台に分散することで，コミュニケーション サーバそれぞれの情報受配信業務のレスポンス向上も見込まれる。

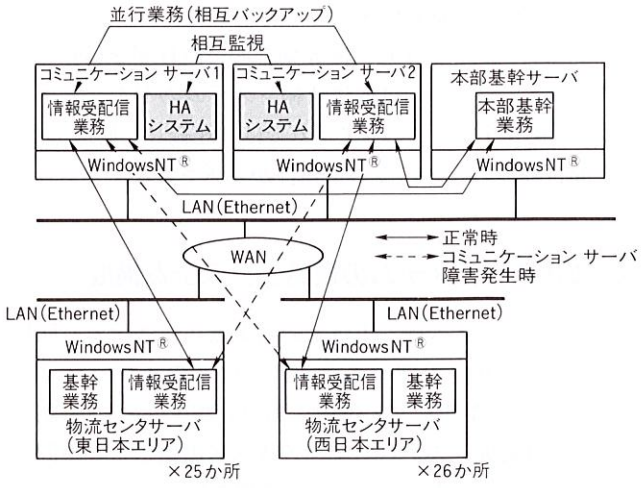


図6．LISでのHAシステム将来構想　コミュニケーション サーバを2台構成とし，それぞれ並行業務を行いながら，相互監視を実施する（相互バックアップ）。

Future plan of HA system architecture for LIS

6 あとがき

LISにおけるPCサーバHAシステム適用事例について紹介したが，基幹系システムにPCサーバを適用する場合，要所要所に高可用化を図り，システム全体の可用性を高めつつ，経済性とのトレードオフを追求することは重要テーマである。個々のシステムの可用性はRAID（ディスク高信頼化）技術やAMS（Availability Management Subsystem），冗長電源などの個別技術で順次高度化されるが，ネットワークコンピューティング時代のトータルシステムとしての高可用性達成のためには，今後もいろいろな形態でのHA技術の高度化が望まれる。そして高度化されたHA技術を基に，さらなる信頼性の高い㈱ダスキン向けLISを追求していく。

（掛札／伊達）

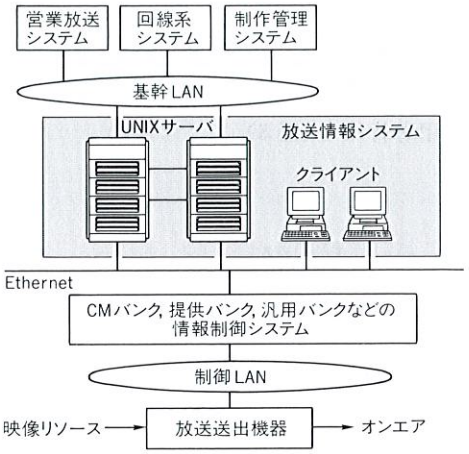


図7．放送情報システム構成　UNIXサーバとPCクライアントで構成される。

Configuration of broadcasting information system

放送情報システム
Broadcasting Information System

1 まえがき

放送業界では，映像，情報，通信が融合したサービスを目ざしている。最近では，映像のディジタル化，コンピュータネットワークのオープン化などに伴い，ほとんどの放送システムは，UNIX，Windows® などの汎用OSをベースとしたコンピュータで構成できるようになってきており，放送局におけるサーバ，クライアントなどのコンピュータの果たす役割は，重要度を増してきている。

ここでは，1997年4月，臨界副都心に新社屋を移転した㈱フジテレビジョン向け放送情報システムのHAシステムについて紹介する。このシステムでは，連続した放送送出，24時間自動運行などの高い信頼性が要求されている。

2 放送情報システムの概略とシステム構成

放送情報システムは，上位系の営業放送システム，回線系システム，制作管理システム，下位系のコマーシャル（CM），提供，番組などの情報・素材管理（バンク）・制御を行う情報制御システムおよび各放送送出機器との中間に位置しており，放送に対して一元管理されたデータにより，放送データの準備作成，緊急時の周辺送出機器の柔軟な対応など，放送運行を高信頼かつ円滑に行うことを支援するためのシステムである。

放送情報システム構成は，図7に示すように当社UNIXサーバ（UX5000）と当社クライアントPC（PVシリーズ）で構成されている。

3 HAシステムの実現方法

放送情報システムは，システム信頼性を確保するために図7のようにUX5000を二重化し運用する。二重化の形態としては，24時間停止することなくデータ処理をするというシステム要件があるため，2台のUX5000を現用系，予備系に分け，現用系はオンライン処理，予備系は待機としたホット／スタンバイ形式で運用する。また，現用系と予備系間で相互監視を行う。さらに，システム切換え時間を短縮させるため，すべての更新データは，アプリケーションにより現用系から予備系に同期更新を行い，データベースの整合性を図っている。

二重化を実現するために，このシステムではUX5000の拡張機能であるHAシステムと通信ミドルウェアのクライアント／サーバ通信プラットホーム（後述）を適用する。以下，HAシステムによる二重化の実現方式について述べる。

3.1 状態監視

二重化を実現するためには，現用系／予備系の相互動作監視および自系内の状態監視が必要である。現用系／予備系の相互監視では，HAシステムの自動検出機能，RAS機能および監視情報通信用専用回線により，他系のハードウェア故障，ソフトウェア故障を検出する。さらに専用線の障害を考慮しUX5000間で専用LANとしてプライベートEthernetを用い，通信を行うバックアップ回線も設けている（図8）。

また，自系内の監視は，HAシステムのモニタプロセス機

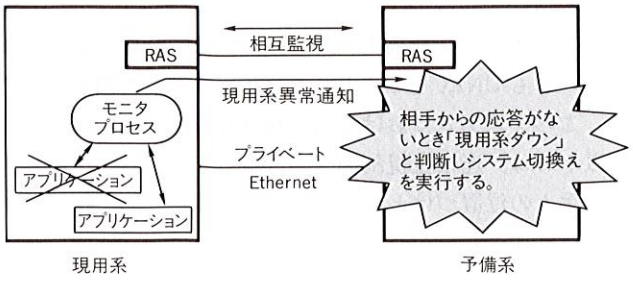


図8．システム状態監視　自系内のアプリケーションプロセスの動作を監視し異常検出を行う。

Process flow of system status monitoring

能により，自系内のアプリケーション プロセスの動作を監視し異常検出を行う。また，現用系／予備系には，同じアプリケーションが入っているため，アプリケーションのバグによっては，同時ダウンが考えられる。そのため，異常判断の重みつけを行い，システム切換えをするか否かを判断させるようにしている（図8）。

3.2　ネットワークの一本化

現用系，予備系の二重化を構成した場合，ネットワーク上のアドレスは二つ存在するため通信相手のクライアントにどちらが現用系であるかを判断させることが必要となる。しかし，HA システムの IP アドレス引継機能により，システム切換え後の予備系（現用系となる）に IP アドレスを移動させることによって，クライアントからは，1台のサーバしか存在しないように見え，サーバが切り換わったことを意識することなく継続した放送の準備作業が行える。ただし，IP アドレス引継時にいったんセッションは切断される。そのため，クライアントでは，クライアント／サーバ通信プラットホームを利用し，自動でセッションの再接続が行えるようにしている（図9）。

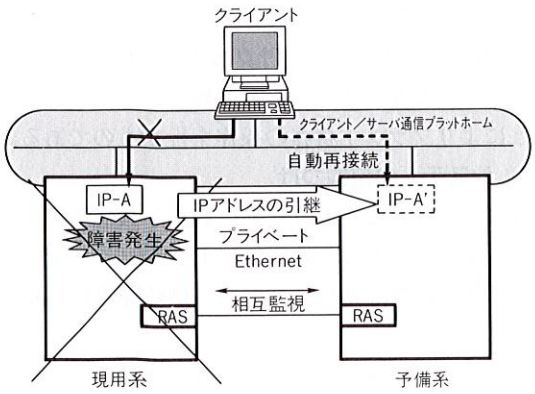


図9．ネットワークの一本化　HA の IP アドレス引継機能により，障害時，現用系の IP アドレスを予備系へ移動させる。

Process flow of dynamic IP addressing

3.3　データベースの同期更新処理

営業放送システムなどの上位系システムもしくはクライアントから現用系にデータベースの更新があったとき，現用系は，自系内のデータベースを更新したタイミングで予備系のデータベースを更新し，データの整合性を保つ処理が必要となる。このシステムでは，データベースの同期をとるための同期更新アプリケーションを開発し，それにより両系のデータベースをつねに整合性がとれるように設計した。

これにより，システム切換時間の短縮と連続した放送運行を実現している。なお，オラクル社の RDBMS（Relational Data Base Management System）の2フェーズコミット機能によるデータベース同期処理も考えられたが，直接的な処理応答を優先させるため，同期更新アプリケーションを開発した（図10）。

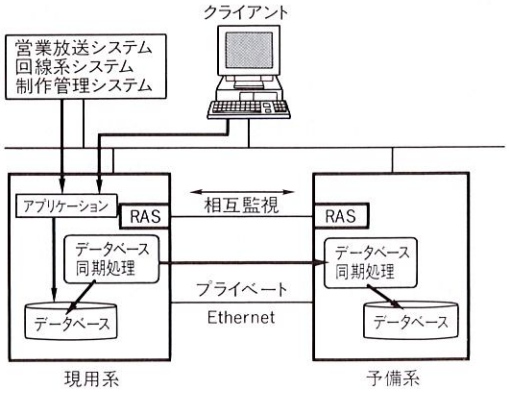


図10．データベース同期更新処理　現用系と予備系のデータベースの整合性を保つために，現用系と予備系間でデータベースの同期処理を行う。

Process flow of database synchronous updating

3.4　復旧処理（データベースの等価処理）

片系に障害が発生し，片系だけで運用している状態で，片系が復旧したときに正常な二重系に戻すには，以下の処理が必要となる。

片系を保守している間は，現用系でデータベースの更新が行われてもデータベースの同期が行われないため，保守が終了し，予備系となったタイミングで現用系のデータベースをコピーし等価とする必要がある。データベースの等価を行うため，このシステムでは，等価処理アプリケーションを開発し，復旧時両系のデータベースの整合性が取れるように設計した。データベースの等価処理が終了後，3.3節のデータベースの同期処理を開始する。なお，このアプリケーションは，オラクル社の RDBMS のデータベースコピー機能を使用した（図11）。

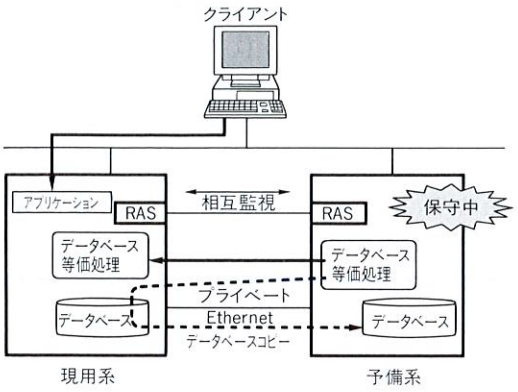


図11. データベースの等価処理　片系が復旧したとき，正常な二重系に戻すため，1台で運用中の現用系から復旧した予備系へデータベースのコピーを行う。

Process flow of database replication

4 あとがき

放送情報システムにおけるHAシステムの適用事例について述べた。

放送局では，24時間放送サービスを提供しようとしている。したがって，24時間放送サービスを提供するためには，信頼性の高いコンピュータシステムが不可欠となる。この事例では，HAシステムを利用して，連続した放送サービスを実現した。さらに，ここで培ったノウハウを基に放送事故のない高信頼・高可用システムを追及していく。

（松原／加藤）

発電用計算機システム
Computer Control System for Power Plants

1 まえがき

火力発電所，原子力発電所などの発電所では，運転監視制御用，データ管理用，業務支援用など多くの計算機システムが使用されている。この中でも運転監視制御に用いられる計算機システムは，発電プラントの状態を監視するための情報を運転員に提供し，さらに，運転員の操作によってプラント機器を制御するなど，運転に必須なシステムである。

このため，このシステムには，高い信頼性が求められ，万が一，故障が発生した場合にもその故障の影響範囲を極小化するとともに，二重化などの技術により機能の喪失を最小限にとどめるよう設計している。

近年のオープン分散化に対応し，発電用計算機システムにおいてもUNIXをOSとした分散システムを開発したので，このシステムにおける高信頼性技術について述べる。

以下では，運転監視制御用の計算機システムについて，システムの位置づけと機能，システム構成，高信頼性技術について述べる。

2 システムの位置づけと機能

発電所における計算機システムは，当初，プラント諸データの収録用のデータロガーとして導入されたが，計算機技術の進歩と監視制御の高度化要求により，プラント自動化，CRT（画像表示装置）オペレーション，警報機能の計算機化，マンマシン機能の高度化など，運転操作に直結した多くの機能を担うようになり，扱う情報量も膨大となり，また，プラントの運転に必須のものとなった。

2.1 機能

監視制御用計算機システムの代表的な機能を以下に示す。

2.1.1 プラント監視　プラント入力を定周期で監視し，警報制限値との比較を行い，警報状態になった場合には，警報窓を点灯させメッセージなどで内容を運転員に知らせる機能である。

近年の中央操作室のコンパクト化の要請により，従来制御盤上に警報窓としていたものを削除し，計算機によるメッセージだけとする場合もあり，従来に増して，計算機の重要性が増してきている。また，弁，ポンプなどのプラント機器の状態と，流量，圧力などのプロセス量を機器のシンボル，ディジタル値，トレンドなどを用いてわかりやすくCRTに表示し，運転員がプラント状態を一目で把握できるようにしている。

2.1.2 プラント自動化　運転員の管理のもとに計算機がプラント状態を判断し，自動的に運転を行うものであり，プラント起動停止操作の迅速化，高信頼化に貢献している。

2.1.3 CRTオペレーション　従来，制御盤上で行っていた手動操作をCRTを使い計算機化したもので，CRT画面上に表示された弁，ポンプなどの機器シンボルをタッチすることによりプラント機器の操作を行うものである。

2.2 システムの位置づけ

以上に述べてきたとおり運転に必須の機能を担っているため，計算機システムの機能喪失は，プラントの監視制御，操作に重大な影響を及ぼし，電力の供給障害にも結びつくことがある。

このため，計算機システムの位置づけは非常に重要なものであり，故障が発生した場合にも，機能喪失を極小化するため，機器の多重化，機能の独立性の確保などのさまざまな対応を行っている。

3 システム構成

システム全体の高信頼性を確保するため，機能の分散化を図り，図12に示す構成を採用している。

このシステム構成では，CRTを駆動しマンマシンをつかさどるオペレータステーション（OPS）と自動化，性能計算などを行うサーバに機能分散し，これらを多重化された情報LANで接続し，サーバとOPS間の表示情報，設定情報などのマンマシン情報を伝送している。プラントとの入出力は，多重化された制御LANを介してサーバが行っている。

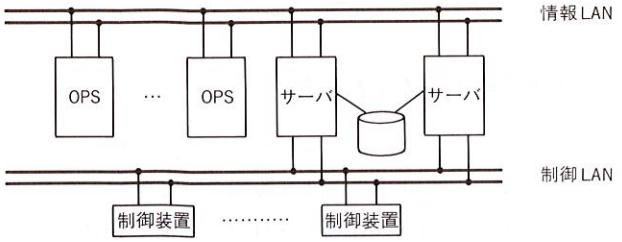


図12. 発電用監視制御計算機システム構成　CRTを駆動するOPSとサーバに機能分割し，プラント情報用の制御LANと，マンマシン情報用の情報LANで接続している。

Computer system configuration for power station

4 高信頼性技術

4.1 システム構成による高信頼化

システム構成の考えかたは，OPS間の関連を排除することによりOPSの独立性を高め，システムとしてのOPS機能の信頼性向上は，独立したOPSの数を増やすことにより，機能喪失を防止する，ということである。

OPS間の関連を排除することにより，OPSの単一故障での共倒れ現象が発生することを防止し，複数のOPSが異常となっても最低限のプラント監視，プラント操作を可能としている。OPSへデータを供給するサーバは二重化構成とし，また，制御LAN，情報LANなどのシステム共通部についても多重化構成として，ここでも単一故障がシステム全体に波及することを防止している。

また，各機器の状態を常時監視し，システム構成機器の正常異常の稼動状態はCRTに表示可能としている。機器に故障が発生した場合には，警報として運転員に通報し，即座に認識できるようにしている。これにより，運転員の誤判断，誤操作の防止につながり，システム稼働率の向上に貢献している。

4.2 OPSの高信頼化

OPSでは，CRTオペレーション，プラント監視画面表示，警報表示を担っており，他のOPSがすべて機能喪失した場合にもこれらの機能が動作可能でなければならない。このため，他のOPSとの直接的な関連を排除し，情報伝達が必要な場合にもサーバを介して通信を行うようにして，他のOPSの影響を受けないよう考慮している。

4.3 サーバの高信頼化

サーバでは，OPSへの表示データ供給，自動化機能，性能計算，ヒストリカルデータの収録，CRTオペレーションの札掛け情報管理などの機能を分担している。このため，二重化構成とし，単一故障発生時にも機能喪失しない構成としている。

二重化構成でのキーとなる技術は，二重化を構成する相手の状態を正確に把握することであり，このためハードウェアとして通常のUNIX機にはないRAS機能を装備し，動作状態をハードワイヤで伝達して，相互の動作状況を監視している。

二重化の方式は，片側がマスタとなりすべての処理を行い，マスタに異常が発生したことをスレーブ側が検出するとすべての処理を肩代わりする方式としている。

また，ヒストリカルデータ，性能計算データなどの重要なデータは，サーバの切換えが発生した場合には共有ディスクを用いて引継ぎを行い，データ喪失を防止している。

5 あとがき

発電用監視制御計算機システムは，UNIXをOSとし，監視画面を表示しCRTオペレーションを行うOPSと，自動化，性能計算などの処理を行うサーバを，情報LANと制御LANにより接続したシステムとしている。OPSは，それぞれの独立性を高め，複数台数を設置することにより機能喪失を防止し，サーバは，多重化構成として，専用の配線により相手の状態を監視し，故障を検出したときにはバックアップを行い，システムとしての高稼働率を実現している。

今後も，発電所の監視制御を行うためのキーとなるシステムとの認識のもとに，最新技術を積極的に導入し，オープンで信頼性・可用性の高いシステムの実現に努めていきたい。

（田岡／木下）

オープン分散電力系統監視制御システム TOSCAN$_{TM}$3000シリーズ

TOSCAN$_{TM}$3000 Series Open Distributed EMS/SCADA Systems

1 まえがき

電力監視制御システムは，電力系統規模の拡大と系統運

用の高度化に伴って，大規模化，高度化の一途をたどってきた。一方，システムの大規模化，とりわけソフトウェアの大規模化は，システムの保守性，拡張性の面で問題をもたらしている。そこで，電力系統監視制御機能を互いに独立した機能に分散し，そのおのおのにCPU資源を割り付け，それらをLANを利用して有機的に結合した“機能分散システム”が採用されるようになった。

電力系統監視制御システムは，情報処理システムの大きな潮流である“オープンシステム”という流れの中で電力系統監視制御システムとしての必須条件であるリアルタイム性と24時間連続運転を行うための高信頼性を堅持しつつ，変革を遂げてきている。

ここでは，“オープンシステム”という潮流の中で位置づけられる電力系統監視制御システムに関する当社のシステム構築のコンセプトについて述べる。

2 電力系統監視制御システムに求められる高信頼化技術と当社のデザインコンセプト

電力系統監視制御分野において，オープン アーキテクチャを採用した分散システムの適用が活発に行われている。当社の電力系統監視制御システムも，従来の特定アーキテクチャに依存したシステムとは異なり，オペレーティングシステム，情報通信プロトコル，データベース，ユーザ インタフェースといったシステムの根幹を標準化，汎用化している。この考えに基づいてシステムを構築することにより，より高度なヒューマン インタフェースの実現と異なるシステム間の高度な情報連携の実現，さらに最新技術を逐次システムに容易に取り込んで行ける拡張可能なシステムの提供をコンセプトとしている。

また，電力系統監視制御システムは，運用を開始してからシステムの取替えまで片時も停止することなく運転を継続する必要がある。

最近では，PCなどの一般家庭への浸透とともにますます電力の安定供給の社会的ニーズが高まってきており，電力系統の運用に直接かかわる電力系統監視制御システムの信頼性の向上が従来以上に高まってきている。

これら，電力系統監視制御システムが求めるシステム信頼性をまとめると，次のことがあげられる。

(1) 確実な障害検出（ハードウェア・ソフトウェア障害）
(2) 検出した障害の健全系への早期通知
(3) 高速なバックアップ
(4) 確実なデータの引継ぎ
(5) システム構築の容易さ
(6) システム管理の容易さ

これらの要件を満たしたシステム構成例を図13に示す。

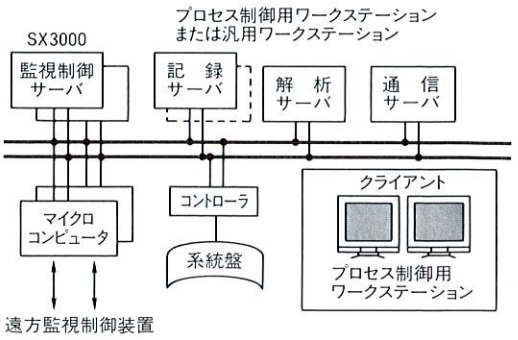


図13. TOSCAN$_{TM}$3000のシステム構成例　電力系統監視制御システムが求めるシステム信頼性を満たしている。
Example of TOSCAN$_{TM}$3000 system configuration

3 高信頼性システム形態

システムの信頼性を向上させるために，複数のサーバ計算機を結合し，運用サーバ計算機側の障害をバックアップしシステムの24時間連続運転を保証する高信頼性システムは，一般的に障害発生時のバックアップ形態（**表1**）とデータの引継ぎ形態（**表2**）により分類される。

電力系統監視制御システムの中枢である監視制御サーバでは，数秒でのバックアップが求められるために，切換え時に時間を要するバックアップ形態を採用することは実質できない。一方データの引継ぎ方法による分類は，表2のようになる。

従来のシステムは，独自アーキテクチャに基づき構成し

表1．バックアップ形態によるシステム分類
Classification of systems by form of backup

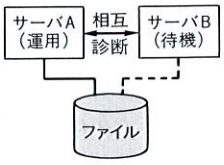
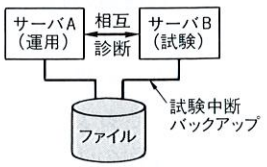
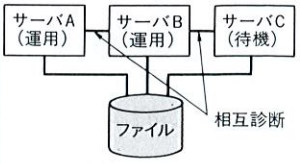
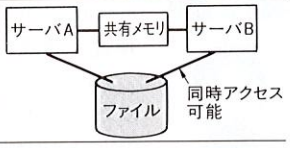
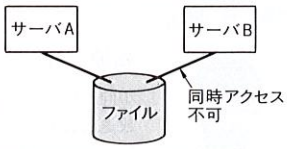
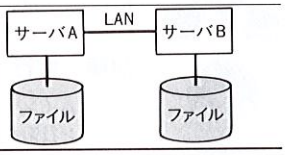
区分	説明	機能
ホットスタンバイ形態	サーバ計算機を運用と待機に分け，運用側サーバ計算機が故障したときに待機系へ切り換える方式。待機系は運用系の障害に備えているだけで，他の業務は実施できない。	
ロードシェア形態	サーバ計算機を運用と待機に分け，待機側では訓練などの別業務を実施可能とした形態。訓練などを実施中でも運転側サーバ計算機に障害が発生したときは，訓練を即時中断して運用をバックアップする形態。	
N:1バックアップ形態	一つの待機系サーバが複数の運用系サーバの障害に備えてバックアップを行う形態。	

表2．データ引継ぎ形態によるシステム分類
Classification of systems by form of data takeover

区分	説明	機能
コンカレントシェアードディスク方式	共有メモリ／共有ディスクを利用してサーバ間のデータを引き継ぐ方法。 両方のサーバからの同時アクセスが可能。	
ノンコンカレントシェアードディスク方式	共有メモリ／共有ディスクを利用してサーバ間のデータを引き継ぐ方法。 ただし両方のサーバから同時アクセスはできない。	
シェアードナッシング方式	サーバ間の共有資源をもたずネットワークなどでデータを引き継ぐ方式。	

たシステムであり，サーバ計算機間に共有ディスクなどを配置したコンカレント シェアード方式であった。

当社の電力系統監視制御システムでは，シェアード ナッシング方式を採用し，サーバのバックアップ形態としてホット スタンバイ方式，ロードシェア方式，N：1バックアップ方式のいずれの形態も可能となっている。

TOSCAN$_{TM}$3000 シリーズは，システムのもっとも重要なサーバである監視制御サーバを，ホット スタンバイまたはロードシェア方式とし，その他の分散サーバは，シングル システム形態または多数のサーバを一つのサーバでバックアップする N：1バックアップ方式を採用し，サーバの信頼性要件とコストから最適な構成を選択する方式としている。

4 TOSCAN$_{TM}$3000 シリーズの方式

当社の TOSCAN$_{TM}$3000 シリーズでは，オープン性と高可用性を実現するために，電力系統用ミドルウェアを各サーバに搭載している。高信頼性システムを構築するうえで必要となる技術は，システム構成制御機能，データ管理機能，プロセス管理機能および LAN 管理機能である（図 14）。

これらのミドルウェアを用いてアプリケーションを構築することにより，電力系統監視制御システムの要件を満足させるシステムの構築を可能としている。

4.1 シェアード ナッシング方式のデータ引継ぎ

シェアード ナッシング方式のデータ引継ぎは，図 15 に示す方式で行っている。

シェアード ナッシング方式によるデータ引継ぎでは，LAN などのネットワークを利用してデータの等価を行うために時間的に遅延が発生する。よって，非常に短時間でデータ更新をする電力系統情報入力処理は，両サーバ計算機で並行動作させてデータの欠損を防止している。これらのアプリケーション ソフトウェアの動作コントロールを，プロセス管理ミドルウェアおよび構成制御ミドルウェアが実施し，アプリケーション ソフトウェアの開発量の削減を図っている。

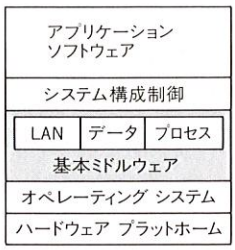


図 14．ソフトウェア概略構成　TOSCAN$_{TM}$3000 シリーズでは，オープン性，高可用性，高信頼性を実現するソフトウェア構成になっている。
Software configuration of TOSCAN$_{TM}$3000 system

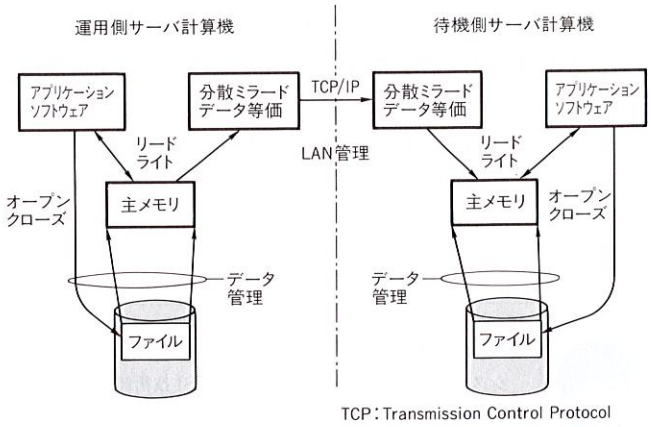


図 15．シェアード ナッシング方式データ等価構成例　電力系統情報入力処理は，両サーバ計算機で並行動作させてデータの欠損を防止させている。
Example of data replication in shared nothing system

4.2 LAN の信頼性向上

システムを構成する各種のサーバおよびクライアントは，すべて LAN に接続しているので，LAN の信頼性もシステムの重要なファクタである。当社 TOSCAN$_{TM}$3000 シリーズでは，LAN を多重化して故障に備えることを基本としてシステムを構成している。また，LAN の性能もシステム信頼性の重要なファクタの一つであるととらえ，従来のシェアード型 LAN の欠点（多数の計算機で時分割利用，トラフィック増大による性能劣化）を，克服したスイッチ形式 LAN を採用している。

LAN の故障時における自動バックアップは，LAN 管理ミドルウェアが実施し，多重化した LAN の健全ルートを探して目的の相手へ確実にデータを届けるようにしている。したがってアプリケーション ソフトウェア個々で障害時のバ

ックアップを考慮する必要はなく，アプリケーション プログラム開発を容易にしている。

これらの方式により，システムの性能と信頼性および拡張性が十分に考慮されたシステムとすることができる。

5 あとがき

以上，オープン分散電力系統監視制御システムのシステム信頼性を向上させる技術について述べた。

電力系統監視制御システムは，電力の安定供給という社会的に重要な目的のために，コンピュータの利用技術，制御技術，信頼性技術，情報処理技術，系統制御技術，情報通信技術，知識工学，人間工学といったあらゆる先端技術を駆使したシステムである。オープンシステムというキーワードのもとに情報処理システム全体が変革を遂げ続けている現在も，電力関係各位のご指導を得てよりよいシステムを構築していく所存である。 （浅野／小松）

関　悦夫　Etsuo Seki

システムインテグレーション統括部 SI 技術部部長。オープンシステムのシステムインテグレーション業務に従事。情報処理学会会員。
Systems Integration Div.

小林　茂　Shigeru Kobayashi

情報・通信システム技術研究所 開発第三担当主務。高可用性システム技術の研究開発に従事。情報処理学会会員。
Information & Communications Systems Lab.

吉羽　宏　Hiroshi Yoshiba

官公システム事業部 官公システム技術第三部。気象システムの開発に従事。。
Government & Public Corporation Systems Div.

掛札　榮昭　Hideaki Kakefuda

産業システム事業部 産業システム技術第一部主査。 産業用計算機システムの開発に従事。IEEE，情報処理学会会員。
Industrial Systems Div.

伊達　俊彦　Toshihiko Date

システムインテグレーション統括部 SI 応用技術第一部。産業分野向け SI&サービスの上流設計に従事。
Systems Integration Div.

松原　宗志　Noriyuki Matsubara

小向工場 放送制御設計部。放送局設備のシステム開発・設計に従事。
Komukai Works

加藤　信行　Nobuyuki Kato

システムインテグレーション統括部 SI 応用技術第二部。オープン技術を用いた SI システムの要件分析・設計に従事。
Systems Integration Div.

田岡　一詩　Hitoshi Taoka

府中工場 発電制御開発部部長。発電プラント向け計算機システムの設計開発に従事。
Fuchu Works

木下　善貴　Yoshitaka Kinoshita

府中工場 発電制御開発部グループ長。発電プラント向け計算機システムの設計開発に従事。
Fuchu Works

浅野　俊明　Toshiaki Asano

府中工場 電力計算機システム部主査。電力系統監視制御システムの開発・設計に従事。電気学会会員。
Fuchu Works

小松　智　Satoshi Komatsu

府中工場 電力計算機システム部主務。電力系統監視制御システムの開発・設計に従事。電気学会会員。
Fuchu Works