1.1 概要

コンピュータ・システムの信頼性を高めるためには，さまざまなエラーや障害などによる停止や影響を最小限に抑え，不正な処理を防止する機能が必要です．本書ではサーバの信頼性について，障害への対策とセキュリティの両面から考えていきます．

障害に対する対策は，障害を防止する，あるいは，障害時の影響を抑えるための措置をとっておくことから，障害が発生したならば，すぐに検出・検知し，回避策，対策をとり復旧することです．さらに，こうした障害の経験をそれ以降の運用管理で活かすためのログ分析および障害対策の更新も重要な処理です．

また，セキュリティ対策は，接続してくる相手やアクセスを認証して，正当ならば許可し，不正な場合は除外する仕組み，さらに，送受信するデータをセキュアに処理するための仕組みです．

なお，本書ではサーバ・システム単体としての対策を，姉妹書「Linux高信頼サーバ構築ガイド－クラスタリング編」ではネットワーク上のクラスタリング・システムとしての対策を，それぞれ解説しています．

1.2 高信頼サーバとは

信頼性の基準は，総務省の「情報通信ネットワーク安全・信頼性基準」や，経済産業省の「情報システム安全対策基準」や「システム監査基準」などで規定されています．信頼性の高いサーバとはRASIS（Reliability，Availability，Serviceability，Integrity and Security；信頼性，可用性，保守性，保全性，および機密性）に代表される仕組みを装備した，システム停止から完全フリーかまたは停止時間が短く，その停止による通常処理への影響が非常に小さい，セキュリティや障害に対する耐性が強い，サーバ・システムです．

サーバ・システムを含むネットワークを評価する具体的な基準は，性能やコスト，障害，品質などになります．このうち，信頼性に関するものは，性能や障害，そして品質です．性能面では，通信や接続のレスポンス，機能性やサービス性などがあります．障害停止に関しての評価は時間という数値で表します．一般のシステム評価ではMTBF(*1.1)やMTTR(*1.2)などが使用されます．さらに，品質面では，接続品質（呼損率や遅延）や伝送品質（伝送損失，伝送エラー，ノイズ），稼働品質（平均稼働・停止時間），処理

品質（処理遅延，エラー）などがあります．

また，フォールト・トレランス（Fault Tolerance）で表される障害への耐性は，ネットワーク（またはシステム）内の障害に対し，ユーザにその影響を全く与えない（狭義のフォールト・トレランス）か，もしくはほとんど与えない（影響を一部に限定する：フェール・ソフト）程度の故障/障害に対する防御能力のことです．

そのため，処理系や回線などの二重化や階層化，などで防御すると同時に，障害検出から障害部分の切り離し/迂回/代替，そして復旧までを自動的かつ素早く行うようにします．また，障害の前兆を監視し重度化を抑止する，特にネットワークではトラフィックの輻輳（ふくそう）を抑止するために，リモート監視も重要です．

なお，障害やセキュリティはソフトウェアとハードウェア，そして，運用管理の面から考える必要があります．

1.3 信頼性のポイント

前述のように信頼性のポイントとなるのは，フォールト・トレランス，セキュリティ，トラブル対応です．

1.3.1 フォールト・トレランス

フォールト・トレランス（Fault Tolerance）は耐故障性で，ネットワーク（またはシステム）内の故障に対し，ユーザにその影響を全く与えない（狭義のフォールト・トレランス）か，もしくはほとんど与えない（影響を一部に限定する：フェール・ソフト）程度の故障/障害に対する防御能力のことです．

処理系の二重化

フォールト・トレランスを実現するための構成手法には，以下のような三つの手法があります．

●デュプレックス（duplex）構成

1台が稼働し，別の1台が障害で停止するまでスタンバイ機となる．

スタンバイ機はプライオリティの低い別業務に使用されることもある．

(*1.1) Mean Time Between Failures；平均故障間隔

(*1.2) Mean Time To Repair；平均復旧時間