FUJITSU Server PRIMERGY
FUJITSU Server PRIMEQUEST

FUJITSU

Windows Server 2008/2008 R2 Active Directory 運用管理の考え方

第 2.2 版

2014 年　9 月

富士通株式会社

Copyright 2011-2014 FUJITSU LIMITED

はじめに

本書は、Microsoft® Windows Server® 2008またはMicrosoft® Windows Server® 2008 R2 Active Directory®の運用管理における考え方について記載しています。
システムの認証基盤を担うActive Directory®では、「止まることのない」「安定した」運用が求められます。本書では、これらの要件を満たすために必要となる運用管理タスクや管理者の役割、その他考慮すべきポイントを紹介します。Active Directory®運用開始前の計画フェーズで利用することを想定して記載しています。なお、Active Directory®の安定稼働のためには運用以前に適切な設計構築を行うことも重要です。設計の考え方については、「Active Directory 設計指南書」を参照してください。

本書の目的

本書を読むことによって以下の事項が達成できることを目標としています。

- Active Directory®の運用管理の概要と考え方を理解できること

本書を利用するにあたっての前提知識

以下の技術情報についての知識が必要となります。

- Active Directory®の基礎知識

参考資料

本書以外の Windows Server 技術情報は、以下のサイトで公開しています。

・Windows システム構築ガイド
http://jp.fujitsu.com/platform/server/primergy/technical/construct/

本書では、以下の略称を使用しています。

略称	意味
AD	Active Directory
DC	Domain Controller

本書では、製品名を以下のように表記しています。

正式名称	略称
Microsoft® Windows Server® 2003	Windows Server 2003
Microsoft® Windows Server® 2008	Windows Server 2008
Microsoft® Windows Server® 2008 R2	Windows Server 2008 R2

Copyright 2011-2014 FUJITSU LIMITED

注意事項

- 本ドキュメントを輸出または第三者へ提供する場合は、お客様が居住する国および米国輸出管理関連法規等の規制をご確認のうえ、必要な手続きをおとりください。
- 本書に記載されたデータの使用に起因する、第三者の特許権およびその他の権利の侵害については、当社はその責を負いません。

Copyright 2011-2014 FUJITSU LIMITED

改版履歴

改版日時	版数	改版内容
2008.10	1.0	新規作成
2009.9	2.0	Windows Server 2008 R2 に対応
2011.7	2.1	留意事項の追加
2014.09	2.2	2.2.1 ユーザ/コンピュータアカウントの管理 - 「②パスワード有効期限の管理」を追加

Copyright 2011-2014 FUJITSU LIMITED

目次

1 AD 運用管理計画の考え方 1
1.1 AD 運用管理計画の重要性 1
1.2 AD 運用管理計画を立てる際の考慮点 1
1.3 AD 運用管理計画策定の進め方 2
1.3.1 運用管理要件の定義 2
1.3.2 運用管理タスクの決定 4
1.3.3 運用体制の計画 5
2 AD 運用管理で必要となるタスク 8
2.1 継続したサービス提供に必要なタスク 8
2.1.1 状態監視 9
2.1.2 保守 10
2.2 効率的なオブジェクト管理に必要なタスク 11
2.2.1 ユーザ/コンピュータアカウントの管理 11
2.2.2 DNS/WINSレコード管理 13
2.2.3 その他のオブジェクト管理タスク 13
2.3 障害から復旧するために必要なタスク 16
2.3.1 バックアップ 16
2.3.2 障害発生時の対応 17
2.3.3 障害発生パターンと復旧シナリオ 18
2.3.4 バックアップ・リストアの留意事項 20
おわりに 22
付録 1 Authoritative Restore を利用したリストアイメージ 23
付録 2 Sysvol フォルダのサイズとリストア時の DC 間複製時間について 24

Copyright 2011-2014 FUJITSU LIMITED

図表目次

図 1 運用管理計画策定の進め方 2
図 2 AD 運用管理の目的と方針の例 3
図 3 運用管理タスクの決定 4
図 4 管理者配置の例 7
図 5 AD 運用管理におけるタスク 8
図 6 Active Directory 管理センターのグローバル検索画面 12
図 7 パスワードが無効になる前にユーザーに変更を促すポリシーの設定画面 13
図 8 パスワード忘却時の作業例 14
図 9 バックアップのタイミング 16
図 10 障害発生パターンと復旧方法 19
図 11Active Directory Recycle Bin 無効時の動作イメージ 21
図 12Active Directory Recycle Bin 有効時の動作イメージ 21
図 13Authoritative Restore によるリストアイメージ 23
図 14 グループポリシーオブジェクトファイルの構成 24

表 1 配置する AD 管理者の例 5
表 2 継続した AD サービス提供に必要なタスク 8
表 3 状態監視に関する運用管理イメージ 10
表 4 保守に関する運用管理イメージ 11
表 5 ユーザ/コンピュータアカウントの管理に関する運用管理イメージ 11
表 6 パスワード有効期限の運用管理イメージ 12
表 7DNS/WINS レコード管理に関する運用管理イメージ 13
表 8OU の分け方 14
表 9 その他のオブジェクト管理に関する運用管理イメージ 14
表 10 バックアップに関する運用管理イメージ 17
表 11 障害レベルの定義例 17
表 12 障害発生時の対応に関する運用管理イメージ 18

Copyright 2011-2014 FUJITSU LIMITED

1 AD 運用管理計画の考え方

AD の運用管理において、検討・考慮すべきポイントは、お客様の環境・規模・要件により細部は異なりますが、大筋は共通しています。これらの共通ポイントを抑えて運用管理計画を立てることで、安定稼働が実現できます。

1.1 AD 運用管理計画の重要性

AD は認証基盤として、システムの重要な役割を担っています。万一、障害などで認証サービスが停止すると新規にクライアントの認証ができず、ファイルサーバやアプリケーションが利用できなくなります。最悪の場合、業務を全て停止させることになります。継続して認証サービスを提供するためには、信頼性・可用性・セキュリティを考慮した構成設計と、運用管理計画が重要です。

1.2 AD 運用管理計画を立てる際の考慮点

AD 運用管理計画では、次の 3 つのポイントを考慮して計画を進める必要があります。

正常時

① 継続した AD サービスの提供

継続した AD サービスの提供を行うため、常時 AD の監視を行うことが重要になります。監視項目として、AD 特有のイベントログはもちろん、他のサーバと同様に OS のイベントログやハードウェア故障、ウイルス検知も必要になります。

② 効率的なオブジェクト管理

AD では、ユーザアカウントをはじめとする AD データベースのオブジェクト管理タスクが多く発生します。多数のユーザアカウント管理を行う場合は、アカウント管理ツールを利用するなど、お客様の環境や体制に合わせてオブジェクトを効率よく管理する仕組みを検討します。

障害発生時

③ システムに障害が発生した際の迅速な復旧

AD に障害が発生して停止した場合、迅速な復旧が求められます。事前にあらゆる障害パターンを想定し、障害の切り分けから復旧までの手順を確立することで迅速な復旧が期待できます。

AD の運用管理では、継続した認証サービスを提供することが重要であり、障害が発生した際には迅速に復旧できるように計画します。加えて、管理性の向上も考慮することで、より良い AD の運用管理が実現します。

本節で紹介した”AD 運用管理における 3 つの考慮すべきポイント”を踏まえて、実際の運用管理計画策定の進め方を次節で紹介します。

Copyright 2011-2014 FUJITSU LIMITED

1.3 AD 運用管理計画策定の進め方

AD の運用管理における目的と方針を明確に決定し、その目的と方針に従って「いつ」「どこで」「誰が」「何を」「どのように」すべきか具体的に決定します。また、決定事項に対して「なぜ」そう決定したかを明確にしておくことで、システム設計の見直しや、管理の引き継ぎがスムーズに行えます。詳細につきましては各章を参照してください。

図 1 運用管理計画策定の進め方

1.3.1 運用管理要件の定義

はじめに、AD 運用管理の目的と方針を決定します。AD 運用管理においてベースとなる重要な定義であり、明確に定義する必要があります。

- 運用管理の目的決定
  運用管理の目的では、最終的に目指すべき運用管理の体制やシステム構成を見据えて決定します。明確な目的を立てるためには、次の内容が含まれていることが望ましいと言えます。

  - 運用管理において重要視するもの
  - 最終的な運用管理イメージ

- 運用管理の方針決定
  運用管理の方針では、運用管理の目的を達成するための具体的な定義を行います。方針の決定には、「何を」運用管理の要件とするか、「どのレベルまで」運用管理の範囲とするか検討が必要になります。

Copyright 2011-2014 FUJITSU LIMITED

以下に「停止しない AD 運用管理」を目指す場合に掲げる目的と方針の例を紹介します。

◎運用管理目的

システムが 24 時間 365 日止まることのないよう監視・保守を行い、ハードウェア故障やシステム障害による業務停止を事前に察知して対処する。万が一、障害が発生した場合は迅速に復旧作業を行い、システム停止による業務停止時間を最小限に留める

◎運用管理方針

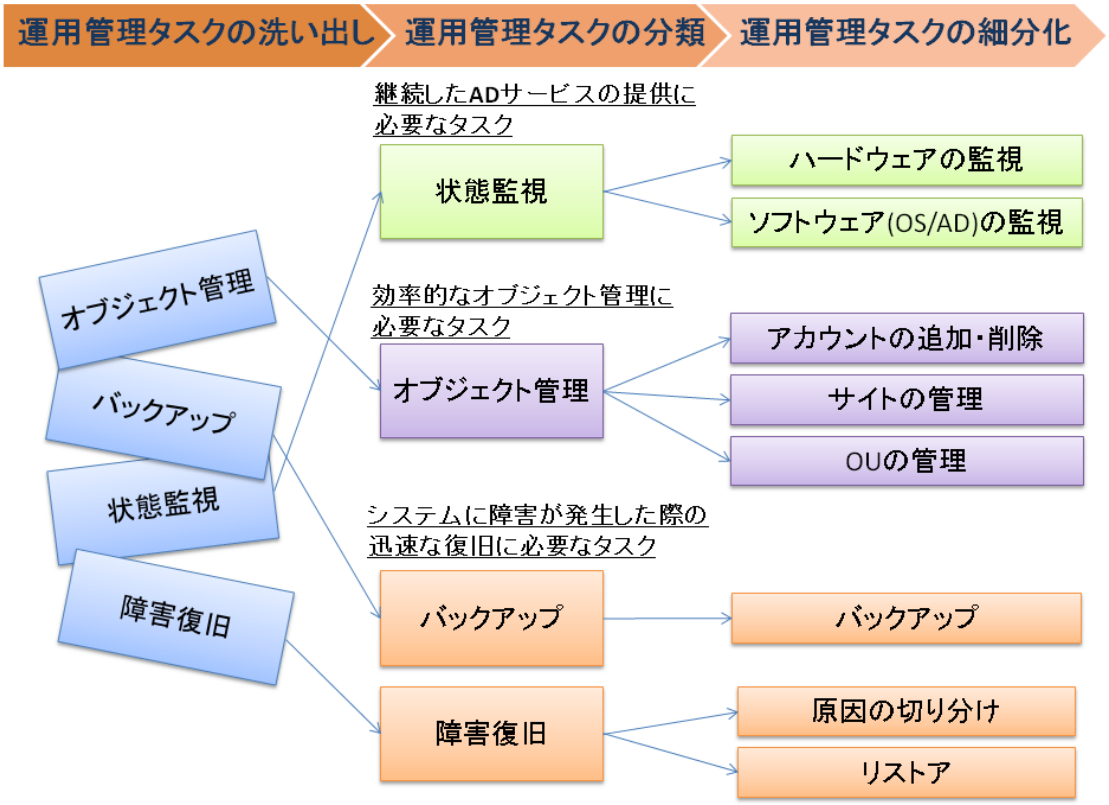
要件	要件の分類	方針
信頼性	障害対策	・イベント監視ツールを利用して常に監視 ・障害発生時には自動的に管理者へ通知 ・障害パターンを想定した復旧方法を確立
	システムの整合性	・AD データベースの定期診断 ・時刻同期の定期確認
可用性	リブートによる サービス停止	・他サーバのリブートを考慮した設計 ・業務時間外にリブートを計画
	バックアップ	・障害時の迅速な復旧を考慮したバックアップ・リストア方法の確立
セキュリティ	ウイルス感染対策	・ウイルス対策ソフトウェアにより感染を防止 ・毎日ウイルス定義ファイルを更新
	情報漏洩	・共有ファイルに対するアクセス権が正しく付与されていることを定期的に確認
	不正アクセス	・管理者権限を特定のメンバにのみ付与

図 2 AD 運用管理の目的と方針の例

Copyright 2011-2014 FUJITSU LIMITED

1.3.2 運用管理タスクの決定

運用管理の目的と方針が決定したら、AD の運用管理で必要となるタスクを決定します。以下のフローに従って設計を進めていきます。



(※)AD 運用管理タスクの一例を紹介しています。

図 3 運用管理タスクの決定

- 運用管理タスクの洗い出し
  AD の本番運用を想定して、運用管理タスクを挙げていきます。運用管理要件の定義を基盤に、必要なタスクを挙げていきます。安全かつ安心して AD の運用管理を行うためには、「1.2 章 AD 運用管理計画を立てる際の考慮点」で紹介した 3 つの考慮点を基にしたタスクを含めます。

- 運用管理タスクの分類
  洗い出した運用管理タスクを整理します。図 3 の例では、運用管理タスクが発生するタイミングで分類しています。このように分類することで、運用管理タスクに過不足がないか確認できます。

- 管理タスクの細分化
  タスクを可能な限り細分化します。運用管理タスク項目を列挙することにより管理すべき項目が明確になり、容易に管理者へタスクを分担できます。

(※)それぞれの AD 運用管理タスクの中で特に考慮すべき項目については、第 2 章で詳細を紹介します。

Copyright 2011-2014 FUJITSU LIMITED

1.3.3 運用体制の計画

運用管理の目的と方針が決定したら、AD の運用管理で必要となるタスクを決定します。以下のフローに従って設計を進めていきます。用管理体制の計画では「どこに」、「どのような」役割の管理者を配置し、各管理者は AD の運用管理において「何を」すべきか決定します。
以下に運用管理体制を決定するまでの流れを紹介します。

・ 管理部門(管理者)の配置計画
運用管理タスクを実施する上で、どこにどのような役割の管理部門(管理者)を配置すべきかを検討します。ここでは、AD の運用管理で一般的に考えられる管理者役割を紹介します。
実際に管理体制を組む場合、複数の役割を一つの管理部門（または管理者）が兼務するケースが多く見られます。以下で紹介する管理者役割を参考に、お客様の環境に合わせて体制を決定してください。

表 1 配置する AD 管理者の例

管理者役割		配置
		役割の詳細
AD 管理者	エンタープライズ管理者	中央（本社／データセンター）に配置。EnterpriseAdmins グループに所属する。
		・ AD の運用・管理に関するすべての決定権を持つ。 ・ AD の設定・設計の変更・拡張に関して最終的な決定権を持つ。 ・ AD 全体に影響を与える操作 （スキーマ拡張、ドメイン追加、サイト構成など）の実行権を持つ。 ・ AD の障害発生時には陣頭指揮を取り、トラブル解決に努める。
	ドメイン管理者	中央（本社／データセンター）に配置。必要に応じて拠点ドメインにも配置。Domain Admins グループに所属する。
		・ 担当するドメインの運用・管理に関するすべての決定権を持つ。 ・ 担当するドメインの設定・設計の変更・拡張に関して最終的な決定権を持つ。 ・ 必要ならば、管理権限の一部をサーバ／システム管理者や部門管理者へ委任できる。 ・ ドメインに影響を与える操作 （DC 追加、信頼関係構築など）の実行が可能。 ・ 担当するドメインの障害発生時には陣頭指揮を取り、トラブル解決に努める。
	部門管理者（OU 管理者）	中央（本社／データセンター）および各拠点に配置。適宜必要な権限（グループに追加）を与えられる。
		・ 担当する部門のユーザアカウント、コンピュータアカウント、セキュリティグループの作成、変更、削除を行う。 ・ 担当する部門利用者へ提供するネットワークリソース（共有フォルダや共有プリンタ、アプリケーション）の公開設定やアクセス権の設定を行う。

Copyright 2011-2014 FUJITSU LIMITED

管理者 役割	配置 役割の詳細
ネットワーク 管理者	中央（本社／データセンター）に配置。必要に応じて拠点にも配置。 適宜必要な権限（グループに追加）を与えられる。
	・ 物理ネットワークの運用、管理、保守業務を主に担当し、AD 管理者と協同でシステム管理にあたる。 ・ ネットワークの設定（TCP/IP の設定）の運用・管理。 ・ ネットワークサービス（DNS、DHCP、WINS）の運用・管理。 ・ ネットワークセキュリティの確保。
監視管理者	中央（本社／データセンター）に配置。適宜必要な権限（グループに追加）を与えられる。
	・ AD ネットワークリソースの監視に関する各種設定を行う。 ・ AD ネットワークリソースの監視を行う。 ・ 障害発生時には、原因の追求のための情報収集を行い、各担当管理者へ連絡をする。
サーバ／システム 管理者	中央（本社／データセンター）または各拠点に配置。適宜必要な権限（グループに追加）を与えられる。
	・ DC、各種リソースサーバのハードウェア、OS の管理、保守を主に担当する。 DC サーバの管理、保守は必要に応じて「ドメイン管理者」と兼務可能。 ・ 中央や各拠点に配置されている DC、リソースサーバのハードウェア、OS、リソースの管理 ・ 利用者へ提供するネットワークリソース（共有フォルダや共有プリンタ、アプリケーション）の公開設定やアクセス権の設定を行う。
キッティング センター(※)	中央（本社／データセンター）に配置。適宜必要な権限（グループに追加）を与えられる。
	・ 利用者が利用するコンピュータをセットアップし、各拠点へ配送する。 ・ 配送したハードウェアの資産管理を行う。 ・ ソフトウェアのライセンス管理を行う。
ヘルプデスク(※)	中央（本社／データセンター）に配置。適宜必要な権限（グループに追加）を与えられる。
	・ 利用者からの障害報告、質問などを電話やメール、Web システムで受付け、問合せに対応する。 ・ 障害発生時には、各管理者や関係部門との連絡の取次ぎを行う。

(※)本書ではキッティングセンター、ヘルプデスクは記載範囲外とします

以下に管理者配置の例を紹介します。

Copyright 2011-2014 FUJITSU LIMITED

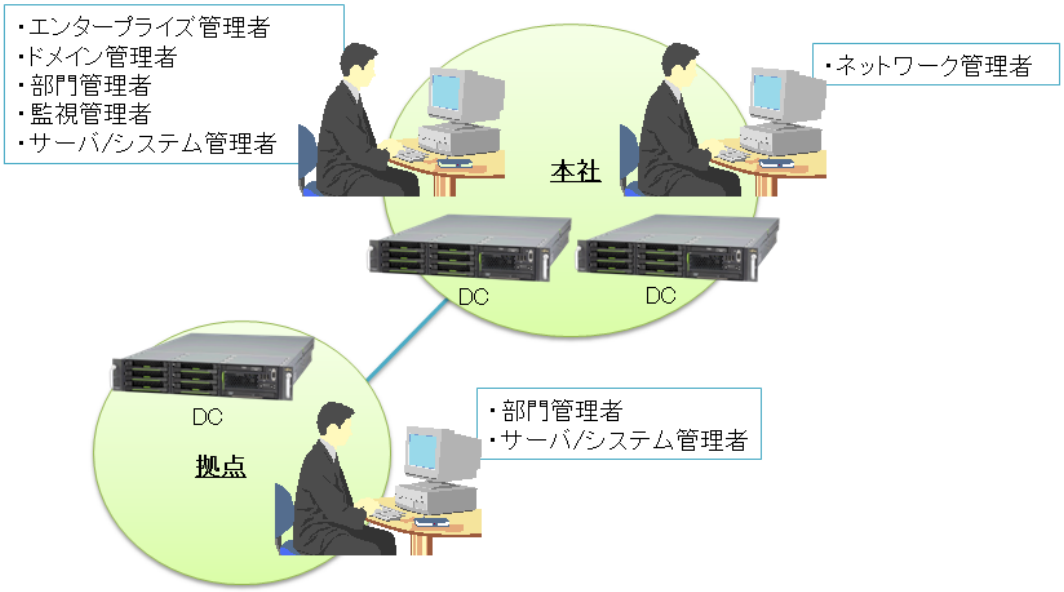


図 4 管理者配置の例

・ 運用管理タスクの振り分け
細分化したタスクと管理者の配置が決定した後に、どのタスクを「いつ」「誰が」「どのように」行うか決定します。タスクを適切な管理者へ振り分けることが重要になります。
なお、タスクを複数の管理者が連携して行う場合は、管理者間の関係や連絡方法も併せて決定しておくと、運用時にスムーズな連携を期待できます

Copyright 2011-2014 FUJITSU LIMITED

2 AD 運用管理で必要となるタスク

AD の運用管理では、図 5 に示すように一般的なサーバで必要な運用管理タスクに加えて、AD 固有の運用管理タスクがあります。本章では、安全かつ安心して AD を運用管理するために、必要となる代表的なタスクを紹介します。

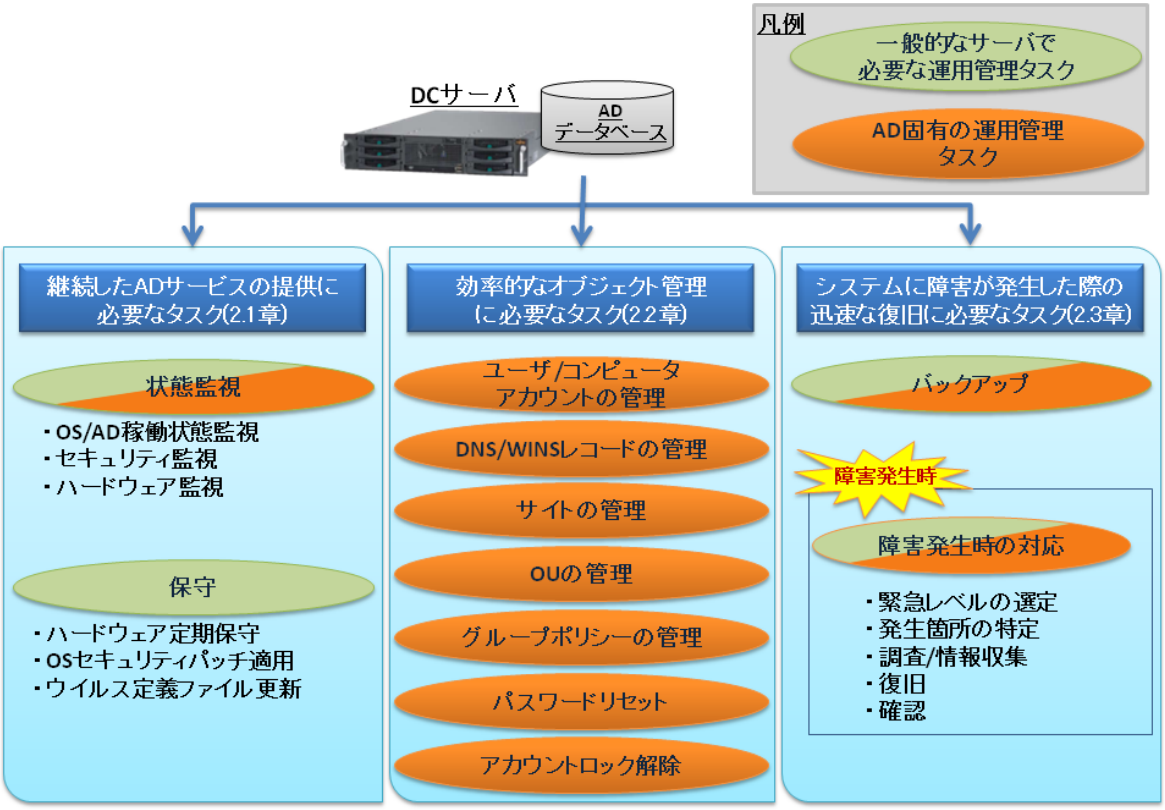


図 5 AD 運用管理におけるタスク

各運用管理タスクの詳細につきましては、以下を参照してください。

2.1 継続したサービス提供に必要なタスク

AD サービスを継続して提供するためには、下記の「状態監視」、「保守」タスクが重要になります。各項目について詳細を紹介します。

表 2 継続した AD サービス提供に必要なタスク

大項目	小項目
状態監視(2.1.1 章)	OS/AD 稼働状態監視
	セキュリティ監視
	ハードウェア監視
保守(2.1.2 章)	ハードウェア定期保守
	OS セキュリティパッチ適用
	ウイルス定義ファイル更新

Copyright 2011-2014 FUJITSU LIMITED

2.1.1 状態監視

AD の運用管理においては、サーバやシステムがダウンしないよう常に監視を行うことが重要になります。
また、事前に故障の予兆を検出し対処することで、トラブルを回避することができます。
以下に監視を行う上で特に考慮すべきタスクについて紹介します。

① OS/AD 稼働状態監視

システムが正常に稼働しているかを監視します。監視する方法としては、OS 標準機能を利用する方法とシステム監視ツールを利用する方法があります。どちらの方法でも、障害発生時には管理者へメールを送信するなど、管理者へアラートを上げる構成にすることをお勧めします。

【OS 標準機能を利用した監視】

AD に関するイベントログを「イベントビューア」を利用して監視します。イベントビューアに出力されるイベントログを通じて、AD の異常を検知できます。
イベントログでは、一般的なサーバと同様に「アプリケーション」「セキュリティ」「システム」を中心に監視を行います。AD 環境ではこれに加えて「ディレクトリサービス」「DNS サーバ」のイベントログを監視します。
特定のイベントに絞って自動監視する場合は、「タスクスケジューラ」を利用して、「警告」、「エラー」など特定のイベントログの発生時に、以下の方法で管理者へ通知が可能です。

- 管理者へメール送信
- デスクトップ画面にポップアップを表示
- 特定プログラムの実行

その他にも、イベントログを他のサーバに転送できる「イベントフォワーディング」機能を使用して、複数サーバのイベントログを集中監視できます。

また、データベース内のオブジェクトに対するアクセス監視を強化する場合など、多数のイベントログの保存が必要な場合は、データ量の肥大化に注意が必要です。イベントログには記録できる最大ログサイズがあり、既定では最大サイズを超えると、古い情報が上書きされます。最大ログサイズに達した際の動作設定やイベントログのバックアップ間隔の検討が必要になります。

【監視ツールを利用した監視】

大量に発生するイベントログをリアルタイムに監視したい場合や、OS の標準機能で監視できない項目を監視対象とする場合は、監視ツールを利用した高度な監視を行います。OS の標準機能で監視できない項目の例として、以下ものがあります。

- 複数台サーバのイベント統合監視
- 常駐プロセスの稼働監視
- 性能監視(CPU、メモリ、ディスクなどの使用状況の自動監視)

お客様の要件に合わせて、監視ツールの導入を検討してください。富士通がお勧めする監視ツールとして、以下のものがあります。詳細は以下の URL を参照してください。

- FUJITSU Software Systemwalker Centric Manager
  http://systemwalker.fujitsu.com/jp/centricmgr/
- マイクロソフト「System Center 2012 R2」
  http://www.microsoft.com/ja-jp/server-cloud/products/system-center-2012-r2/

② セキュリティ監視

セキュリティ監視では、サードパーティ製のウイルス対策ソフトを利用してウイルス感染の有無をチェックします。ウイルススキャンはサーバに負荷がかかるため、比較的利用者の少ない深夜などに実行することをお勧めします。富士通がお勧めする製品としては、以下のものがあります。詳細は URL を参照してください。

- トレンドマイクロ「ウイルスバスター コーポレートエディション」 (セキュリティ対策)
  http://jp.trendmicro.com/jp/products/enterprise/corp-family/corp/

Copyright 2011-2014 FUJITSU LIMITED

③　ハードウェア監視

サーバ運用においては、老朽化などに起因するハードウェア故障を考慮しなければなりません。管理者はハードウェアの状態を監視して、稼働状況やパフォーマンス低下など、各ハードウェアデバイスの異常を早期に検出する必要があります。

富士通 PC サーバ PRIMERGY では、標準添付ソフト「ServerView Operations Manager」を利用することで、故障の予兆検知から管理者への通知までリアルタイムに行うことができます。また、システム全体の統合管理を行う際は、富士通ミドルウェア「Systemwalker Centric Manager」の導入をご検討ください。各製品の詳細は以下の URL を参照してください。

・ServerView Operations Manager/Agents (PRIMERGY サーバ監視)
http://jp.fujitsu.com/platform/server/primergy/serverview/

・FUJITSU Software Systemwalker Centric Manager (システム統合管理)
http://systemwalker.fujitsu.com/jp/centricmgr/

表 3 状態監視に関する運用管理イメージ

タスク	作業担当者	作業タイミング
OS 稼働状況	サーバ/システム管理者	毎日
AD 稼働状況	ドメイン管理者	毎日
セキュリティ監視	サーバ/システム管理者	毎日
ハードウェア監視	サーバ/システム管理者	毎日

2.1.2 保守

保守作業は、サーバが正常に稼働し滞りなくサービスを提供するため必要なタスクです。保守作業はハードウェアや OS システムに関連するタスクが多く、一般的なサーバと共通したタスクが多くあります。保守においては以下のタスクについて検討してください。

④　ハードウェア定期保守

ハードウェアの保守では、ハードウェアの定期点検やバックアップメディアなど消耗品の交換などがあります。ハードウェアの点検では、あらかじめチェックリストなどを作成することにより、確認漏れを防止することができます。また、どれくらいの頻度で作業を行うかを決定します。

⑤　OS セキュリティパッチ適用

OS のセキュリティパッチ適用は、全てのサーバで必要な作業になります。ここで注意すべき点は、セキュリティパッチ適用後にリブートを必要とするケースがあることです。DC をリブートする際は、サイト内にグローバルカタログ(GC)の役割を持つ DC が一台以上動いているように計画します。リブートするタイミングを夜間などの認証要求が少ない時間帯に計画することで、ユーザや業務への影響を最小限に抑えることが可能です。また、クライアントを含めた AD 全体のセキュリティパッチ適用を集中管理・効率化するために、Microsoft® Windows Server Update Services(WSUS)を導入するケースが増えています。詳細は以下の URL を参照してください。

・マイクロソフト「Windows Server Update Services の概要」
http://technet.microsoft.com/library/hh852345.aspx

⑥　ウイルス定義ファイル更新

導入したウイルス対策ソフトの「ウイルス定義ファイルの更新」、「ウイルススキャン」が主な作業になります。また、ウイルス感染時の対策やマニュアルを用意し、手順を確立しておく必要があります。

Copyright 2011-2014 FUJITSU LIMITED

表 4 保守に関する運用管理イメージ

タスク	作業担当者	作業タイミング
ハードウェア定期保守	サーバ/システム管理者	毎月
OS セキュリティパッチ適用	サーバ/システム管理者	毎月
ウイルス定義ファイル適用	サーバ/システム管理者	毎日

2.2 効率的なオブジェクト管理に必要なタスク

AD の運用では、オブジェクト(ユーザ/コンピュータ)の追加などのタスクが発生します。効率的なオブジェクト管理を行うために、管理ツール導入の検討や、オブジェクト管理を「いつ」「誰が」「どのように」行うか決定します。

2.2.1 ユーザ/コンピュータアカウントの管理

AD の運用において、オブジェクトの管理はさまざまな機会に発生するタスクです。

① ユーザ/コンピュータアカウントの登録・変更・削除

新入社員の受け入れ、社員の退職など定期的に発生する場合や、部署異動など不定期に発生する場合が考えられます。

表 5 ユーザ/コンピュータアカウントの管理に関する運用管理イメージ

タスク	作業担当者	作業タイミング
ユーザ/コンピュータアカウントの登録	ドメイン管理者	新入社員受入時 新規コンピュータ導入時
ユーザ/コンピュータアカウントの変更	ドメイン管理者	組織変更時 部署移動時
ユーザ/コンピュータアカウントの削除	ドメイン管理者	社員の退職 コンピュータのリース切れ

少人数の場合は手動で短時間に登録できますが、数百人以上の規模になると、以下に紹介するツールを利用して作業を自動化することをお勧めします。

(1) スクリプトを利用

スクリプトを利用することで、大量にあるオブジェクトの作成/変更/削除などの操作を一括して行えます。サンプルスクリプトが以下 URL で公開されていますので、必要に応じて参照してください。

・マイクロソフト 「スクリプト センター」
http://www.microsoft.com/japan/technet/scriptcenter/scripts/ad/default.mspx

(2) メタディレクトリ製品を利用

社内には、多くの場合 AD 以外にもユーザ情報を管理しているシステムが存在します。このような複数のユーザ情報を連携し、一元管理するためのしくみとしてメタディレクトリがあります。ユーザ情報のマスタである人事データベースから必要な情報を定期的に吸い上げ、AD のアカウント情報に反映するといったしくみを構築することができます。メタディレクトリ製品として以下のものがあります。詳細は以下の URL を参照してください。

・「LDAP Manager®」(ID 管理)
http://jp.fujitsu.com/group/fst/services/ldapmgr/
・「FUJITSU Security Solution PMaid™ IDMaster V5」(ID 管理)
http://jp.fujitsu.com/group/kcn/services/products/networkapl/product-pmaid-idm.html

Copyright 2011-2014 FUJITSU LIMITED

・マイクロソフト「System Center 2012 R2」
http://www.microsoft.com/ja-jp/server-cloud/products/system-center-2012-r2/

(3) その他オブジェクト管理製品を利用

サードパーティ製のツールを利用することで、オブジェクトの管理を簡素化できます。オブジェクト管理製品の一つとして、AD アカウントを一括作成/更新する「Account Agent」があります。オブジェクト管理製品を利用することで、AD アカウント管理にかかる手間と時間を大幅に削減できます。詳細は以下 URL を参照してください。

・Account Agent (AD アカウント一括作成/更新)
http://jp.fujitsu.com/group/fst/services/accountagent/

② パスワード有効期限の管理

一般的にユーザアカウントのパスワードの有効期限は、セキュリティ方針により決定され、セキュリティ強化の観点からパスワードを定期的に変更することを推奨します。
AD でのユーザアカウントのパスワードの有効期限は、既定で 42 日に設定されており、パスワード有効期限切れの 5 日前にユーザへ通知されます。ドメイン管理者や部門管理者は、自部門のセキュリティ方針に従ってパスワード有効期限を管理します。

表 6 パスワード有効期限の運用管理イメージ

タスク	作業担当者	作業タイミング
パスワードの有効期限管理	ドメイン管理者 部門管理者	セキュリティ方針変更時

以下に、パスワードの有効期限が切れるユーザを確認する方法と、パスワード有効期限のユーザへの通知日数を変更する方法を紹介します。

【パスワードの有効期限が切れるユーザを確認する方法(※)】
パスワードの有効期限が切れるユーザを確認するには、「Active Directory 管理センター」のグローバル検索を使用します。検索条件に「指定日数以内にパスワードの有効期限が切れるユーザー」と「日数」を設定することで、指定した日数以内にパスワードの有効期限が切れるユーザを検索表示できます。
※ Windows Sever 2008 R2 で利用可能な方法です。Windows Server 2008 では利用できません。

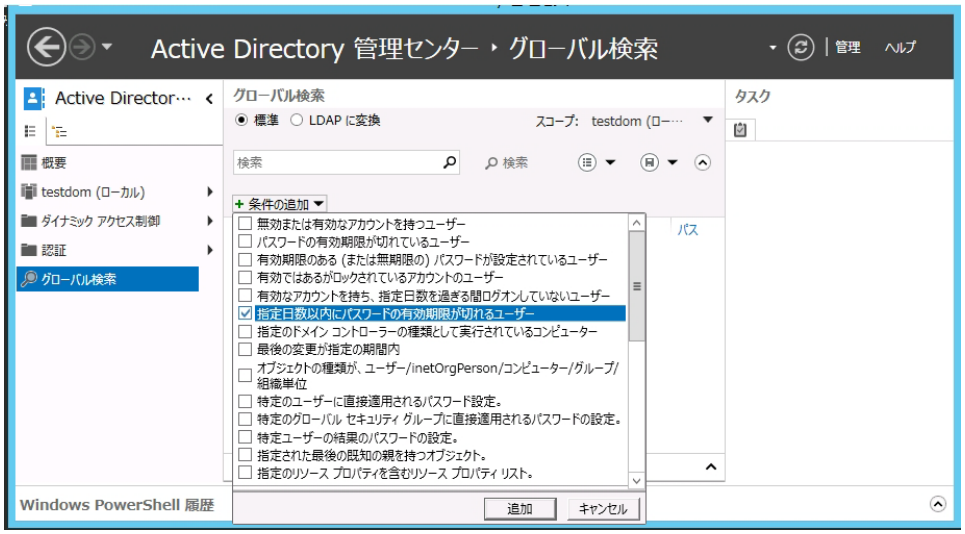


図 6 Active Directory 管理センターのグローバル検索画面

Copyright 2011-2014 FUJITSU LIMITED

【パスワードの有効期限切れ通知日数を変更する方法】
パスワードの有効期限が切れる前にユーザへ通知する日数を変更するには、以下の「グループポリシー」を設定します。

[コンピューターの構成]-[Windows の設定]-[セキュリティの設定]-[ローカルポリシー]-
[セキュリティオプション]-[対話型ログオン:パスワードが無効になる前にユーザーに変更を促す]

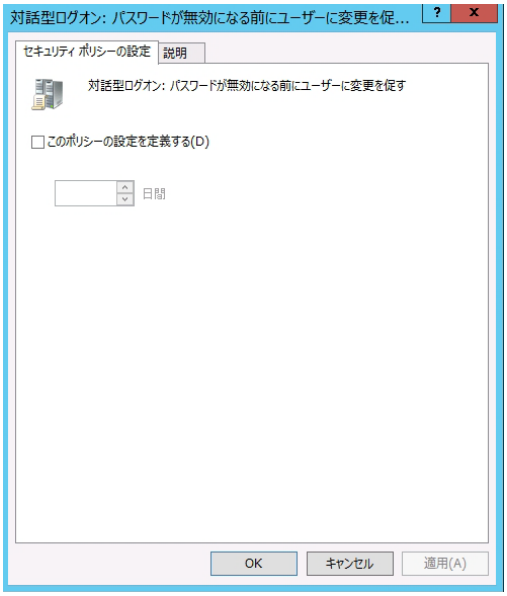


図 7 パスワードが無効になる前にユーザーに変更を促すポリシーの設定画面

なお、グループポリシーを利用する際のタスクについては「③グループポリシーの管理」を参照してください。

2.2.2 DNS/WINS レコード管理

AD において、DNS は必須コンポーネントです。AD では DNS の管理も重要なタスクの一つです。DNS の管理では、静的レコードの追加/変更/削除のタスクが発生します。名前解決に WINS を利用している場合は、WINS の静的レコードの管理も必要になります。

表 7DNS/WINS レコード管理に関する運用管理イメージ

タスク	作業担当者	作業タイミング
DNS/WINS 静的レコードの追加/変更/削除	ネットワーク管理者	サーバ導入/移動/廃棄時 ネットワーク構成変更時

2.2.3 その他のオブジェクト管理タスク

A オブジェクトの管理として、「ユーザ/コンピュータアカウント」、「DNS/WINS レコード」の管理について紹介しましたが、その他にも以下のタスクについて考慮する必要があります。

① サイトの管理

サイトの管理では新会社設立や事務所の移動時などサーバ設置場所の変更時、ネットワーク構成変更時にサイトの追加・変更・削除が必要になります。サイト構成の見直しでは、サイト間の通信速度やサイト内のクライアント数を参考に以下の項目の見直しが必要になります。

・サイトリンクの定義

Copyright 2011-2014 FUJITSU LIMITED

・リンクコストによる重みづけ
・複製タイミングの見直し

② OU の管理

必要に応じて、OU の追加・変更・削除を行います。構成設計の段階で、なるべく変更が発生しないように考慮することをお勧めします。下表に、主な OU の分け方のパターンを示します。

表 8OU の分け方

OU の分け方	説明
管理体系	A 部と B 部を一箇所で管理している場合など、業務上の組織でなく管理単位で OU を分割する。
業務の組織構造	組織構造をそのまま OU 構造とする。注意点として組織変更による影響が大きいことが挙げられる。
地理的構造	地理的な構造を OU 構造とする方法。管理体制も拠点毎に分かれる場合などに適する。
オブジェクト種別単位	ユーザオブジェクト、コンピュータオブジェクト、といったオブジェクト単位に OU 分割する方法。人事異動による管理工数削減のため、ユーザオブジェクトについてよく使用されるパターン。

③ グループポリシーの管理

グループポリシーを利用することでユーザが操作可能な範囲を限定したり、特定の設定を強制したりするなど一貫した管理が可能です。管理においては、グループポリシーの追加/変更/削除が主なタスクになります。どのグループポリシーをどの範囲に適用するか判断できる管理者が必要であり、追加/変更/削除を行う際は、事前に計画・検証を行うことを推奨します。

④ パスワードリセット・アカウントロック解除

AD を利用した認証システムにおいて、ユーザがアカウントロック、またはパスワード忘却のためログインできないケースが考えられます。
このようなケースを想定して、迅速に対応できるよう管理体制を整える必要があります。図 8 の、問合せを総合的に受け付ける窓口が存在するケースでは、ドメイン管理者と問合せ窓口の間で運用手続きを定義しておくことでスムーズな対応が可能になります。

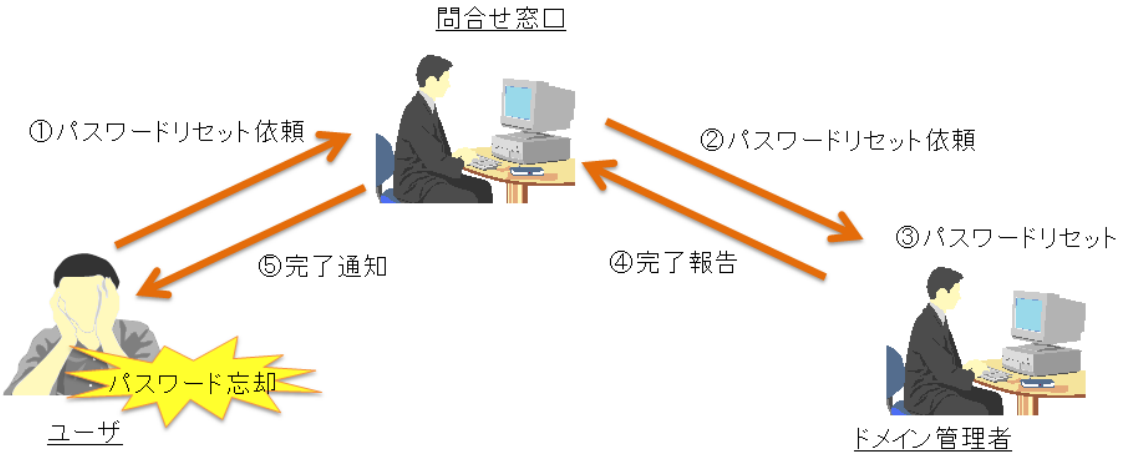


図 8 パスワード忘却時の作業例

表 9 その他のオブジェクト管理に関する運用管理イメージ

Copyright 2011-2014 FUJITSU LIMITED

タスク	作業担当者	作業タイミング
サイトの管理		
サイトの追加/変更/削除	ドメイン管理者	ネットワーク構成変更時
OU の管理		
OU の追加/変更/削除	ドメイン管理者 部門管理者	組織変更時
グループポリシーの管理		
グループポリシーの追加/変更/削除	ドメイン管理者 部門管理者	管理体制変更時
パスワードリセット・アカウントロック解除		
パスワードリセット	ドメイン管理者 部門管理者	ユーザ問い合わせ時
アカウントロック解除	ドメイン管理者 部門管理者	ユーザ問い合わせ時

Copyright 2011-2014 FUJITSU LIMITED

2.3 障害から復旧するために必要なタスク

AD の障害に備えて定期的にバックアップを行い、障害発生時には早急に障害の原因を特定して復旧作業を行う必要があります。本章では障害対策(バックアップ)から障害が発生した際の復旧作業までに必要となるタスクを復旧シナリオと併せて紹介します。

2.3.1 バックアップ

バックアップは、データベース全損など障害発生時のシステム復旧を行うために必要な重要タスクです。既存システムに最適なバックアップ手法を選択して実行する必要があります。
また、業務時間外にバックアップを実行するなど、取得タイミングにも考慮が必要です。

【バックアップ方式】
Windows Server 2008/2008 R2 では、以下の方式で AD のバックアップが可能です。

① サーバ全体バックアップ
サーバ全体バックアップは、Windows Server 2008/2008 R2 の標準機能「Windows Server バックアップ」を利用してサーバ上のデータ全てをバックアップします。特別な理由がない限り、この方式でバックアップを取得することを推奨します。

② システム状態バックアップ
コマンドプロンプトで wbadmin コマンドを実行することで、システム状態のバックアップができます(※)。システム状態は以下の情報を含みます。

・レジストリ
・COM＋クラス登録データベース
・システムファイルなど、ブートファイル
・証明書サービスデータベース
・Active Directory ドメインサービス
・SYSVOL
・クラスタサービス情報
・Microsoft Internet Information Service(IIS) meta directory
・Windows ファイル保護(WFP)のあるシステムファイル

(※)Windows Server 2008 R2 では、Windows Server バックアップのウィザードを使用したシステム状態のバックアップ取得も可能です。

【バックアップの頻度】
バックアップは、サーバ全体のデータを毎日取得することを推奨します。その他にも、ハードウェアの構成変更や OS セキュリティパッチ適用などシステムの変更前後でも、バックアップを取得することをお勧めします。

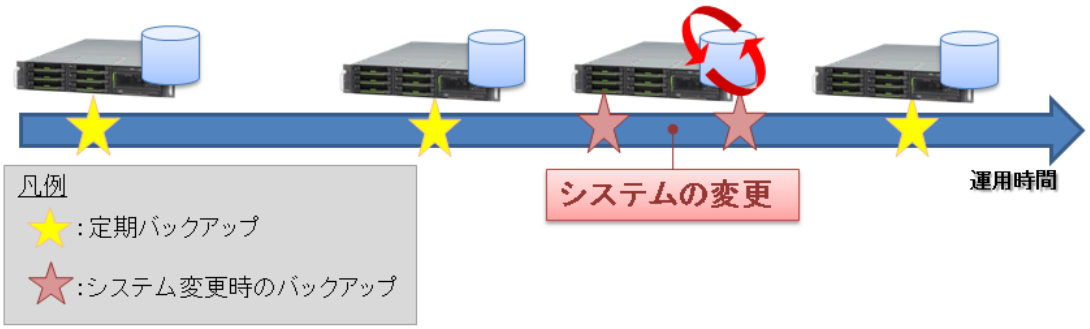


図 9 バックアップのタイミング

Copyright 2011-2014 FUJITSU LIMITED

【バックアップを取得する DC】
バックアップを取得する DC の選定は、管理体制・サーバ配置などを考慮の上、検討してください。また運用設計の段階で十分な検証を行い、お客様の環境・運用に合わせたリストア手順を確立します。なお、複数台構成のドメインにおいて何れかの DC でバックアップを取得する場合、FSMO の役割を持つ DC でバックアップを取得しておくとリストア手番が簡単です。

【その他のバックアップソフトウェアの選定】
AD データベースは、Windows Server バックアップを利用してバックアップすることが可能ですが、テープ媒体でデータを保存する場合は、サードパーティ製のバックアップソフトウェアを利用します。詳細は以下の URL を参照してください。

・「バックアップソフトウェア ARCserve®」 (テープ装置へのバックアップ)
http://software.fujitsu.com/jp/arcserve/index.html

表 10 バックアップに関する運用管理イメージ

タスク	作業担当者	作業タイミング
バックアップ	サーバ/システム管理者	毎日 システム変更時

2.3.2 障害発生時の対応

AD の障害は、発生箇所や原因がさまざまであり、障害レベルも軽度のものから緊急を要するものまであります。障害発生時は、障害レベルに合わせた適切な復旧を行うことが重要になります。基本的に、AD の障害時は以下の手順で復旧作業を進めます。

① 障害レベルの判断
発生した障害によるサーバの状態や、ユーザへの影響度を見て障害レベルを判断します。以下に障害レベルの定義例を紹介します。

表 11 障害レベルの定義例

障害レベル	障害状況
S	◎業務停止◎ システムが完全に停止し、全ユーザが利用できない。
A	◎一部業務停止◎ 一部のシステムが停止し、一部のユーザが利用できない。
B	◎縮退運用◎ 業務を縮小して稼働している。業務の継続は可能だがパフォーマンスなどに影響あり。
C	◎業務に影響なし◎ 障害が発生しているが業務に影響なし。

障害レベルに応じて、システムを利用するユーザに対して障害状況や復旧目処などをアナウンスすることを検討します。

② 発生箇所の特定
障害発生箇所の特定を行います。

③ 調査/情報収集
詳細な障害原因の調査を開始します。イベントログや情報収集ツールを利用することにより障害の原

Copyright 2011-2014 FUJITSU LIMITED

因を特定し、対応策を立てます。

④　復旧

調査結果や収集した情報を基に復旧作業を開始します。ハードウェアの故障であれば故障部品の交換を行い、AD データベース破損などソフトウェアの障害であればリストアを検討します。想定される障害復旧シナリオ例を、「2.3.3 章　障害発生パターンと復旧シナリオ」で紹介します。

⑤　確認

復旧作業完了後に、障害箇所が正常に動作しているか確認を行います。また、新たな問題が発生していないかを併せて確認する必要があります。

表 12 障害発生時の対応に関する運用管理イメージ

タスク	作業担当者	作業タイミング
障害レベルの判断	ドメイン管理者 監視管理者	障害発生時
発生箇所の特定	ドメイン管理者 監視管理者	障害発生時
調査/情報収集	ドメイン管理者 監視管理者	障害発生時
復旧	ドメイン管理者 監視管理者	障害発生時
確認	ドメイン管理者 監視管理者	復旧作業完了後

2.3.3 障害発生パターンと復旧シナリオ

障害の発生パターンをあらかじめ予測し、復旧シナリオを用意しておくことで迅速な復旧が期待できます。本章では、以下の 3 パターンの障害が発生することを想定した復旧シナリオを紹介します。

Copyright 2011-2014 FUJITSU LIMITED

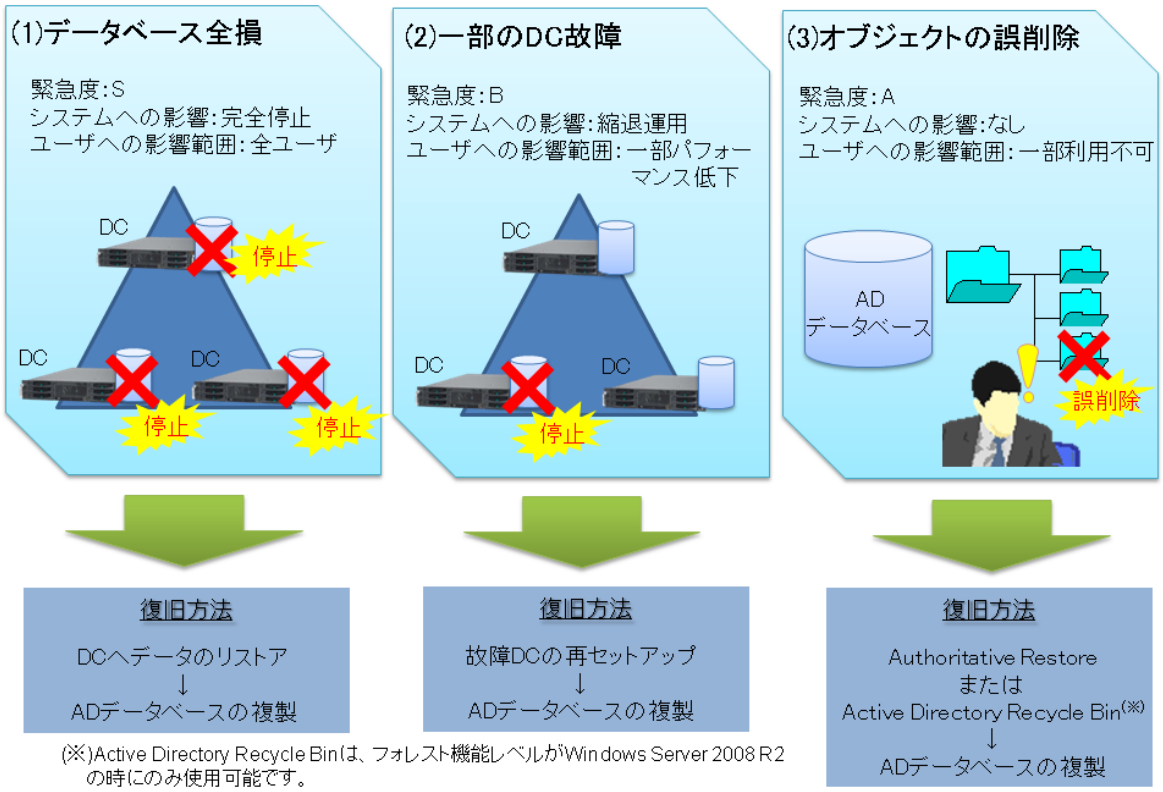


図 10 障害発生パターンと復旧方法

① データベース全損

データベース全損とは、主に災害などで全 DC サーバが停止した状態であり、最も緊急度が高いと言えます。このような場合、「Windows Server バックアップ」を利用して取得したバックアップイメージファイルから全データのリストアを行うことでシステムを復旧させます。
2 台目以降の DC サーバの復旧は、サーバの再セットアップを行った後に復旧した DC と AD データベースの複製を行うことで完了します。

② 一部の DC 故障

複数台の DC で構成される環境において一部の DC が障害で停止した場合、ドメインユーザは他の正常稼働している DC で認証を行うことができます。したがって、認証サービスのパフォーマンスが低下する可能性はありますが、業務が停止することはありません。
復旧作業はリストアではなく、サーバの再セットアップを行います。サーバの再セットアップ後に AD データベースが複製され、再度認証サービスの提供を開始できます。

③ オブジェクトの誤削除

AD データベース内のオブジェクトを誤って削除した際は、Authoritative Restore(権限のある復元)を利用してリストアします。通常の方法で AD データベースのリストアを行った場合、リストアした情報は古い情報とシステムが認識するため、他の DC が持つデータベース情報に上書きされます。しかし、Authoritative Restore によってリストアした場合、リストアしたデータベースのデータが最新の情報と認識され、他の DC の AD データベースへ複製されます。
Authoritative Restore を利用したリストアについては「付録 1 Authoritative Restore を利用したリストアイメージ」を参照してください。
また、Windows Server 2008 R2 では AD の新機能として「Active Directory Recycle Bin」が追加されました。Active Directory Recycle Bin が有効な場合、Authoritative Restore を使用せずに迅速にオブジェクトの復旧が可能です。オブジェクト回復には、「Windows PowerShell」または「LDAP ユーティリティ」を使用します。Active Directory Recycle Bin を利用したリストアイメージ、および

Copyright 2011-2014 FUJITSU LIMITED

Authoritative Restore との比較については、以下を参照してください。

・新機能 Active Directory Recycle Bin で AD 運用はどう変わる？
～Windows Server 2008 R2 移行・導入・運用の豆情報～
http://primeserver.fujitsu.com/primergy/software/windows/os/wins2008/w2008r2/01-01.html

2.3.4 バックアップ・リストアの留意事項

バックアップ・リストアを行う際には、以下の留意事項を考慮の上、計画を立ててください。

- 「Windows Server バックアップ」では、バックアップ格納先としてテープを利用できません。
- セキュアチャネル更新期間(Windows Server 2008/2008 R2 の既定では 30 日)以前のデータを復元する際は、セキュアチャネルのリセットを行う必要があります。
- 「Tombstone の有効期間(※)」を過ぎた古いバックアップイメージからはリストアできません。
- Sysvol フォルダ容量が大きい場合、リストア時の複製処理に時間がかかり、認証サービス開始に時間を要することがあります。
  詳細は「付録 2 Sysvol フォルダのサイズとリストア時の DC 間複製時間について」を参照してください。

Windows Server 2008 では、上記に加えて以下の留意事項も考慮してください。

- スケジュールバックアップは、内蔵、外付けハードディスクにバックアップ可能です。
  DVD や、共有フォルダにはバックアップすることはできません。
- スケジュールバックアップで、バックアップ先に指定されたディスクは、1度フォーマットされます。
  バックアップ先にデータが格納されている場合は、別のディスクに格納してください。
- システム状態のバックアップは、Wbadmin コマンドを使用して、コマンドラインで取得します。
  「Windows Server バックアップ」の GUI を使用したバックアップでは取得できません。

(※) Tombstone の有効期間
AD の管理コンソールからオブジェクトの削除操作を行った場合、そのオブジェクトは即時にデータベースから削除される訳ではありません。削除されたオブジェクトは「Tombstone の有効期間」と呼ばれる期間に入り、オブジェクト自体はデータベースから削除されませんが、ほとんどの属性が削除されます。この期間を過ぎると、オブジェクトはデータベースから完全に削除されます。
Windows Server 2008 R2 において、Active Directory Recycle Bin が有効な場合、削除されたオブジェクトはまず、「削除されたオブジェクトの有効期間」と呼ばれる期間に入ります。この期間のオブジェクトは、すべての属性値が保持されるため、削除前の状態に完全復元できます。
「削除されたオブジェクトの有効期間」が終了すると「Tombstone の有効期間」に入り、これらの異なる 2 つの期間を経て、オブジェクトはデータベースから完全に削除されます。
Windows Server 2008/2008 R2 では、「削除されたオブジェクトの有効期間」、「Tombstone の有効期間」共に、既定で 180 日が設定されています。これらの値は変更可能です。

Copyright 2011-2014 FUJITSU LIMITED

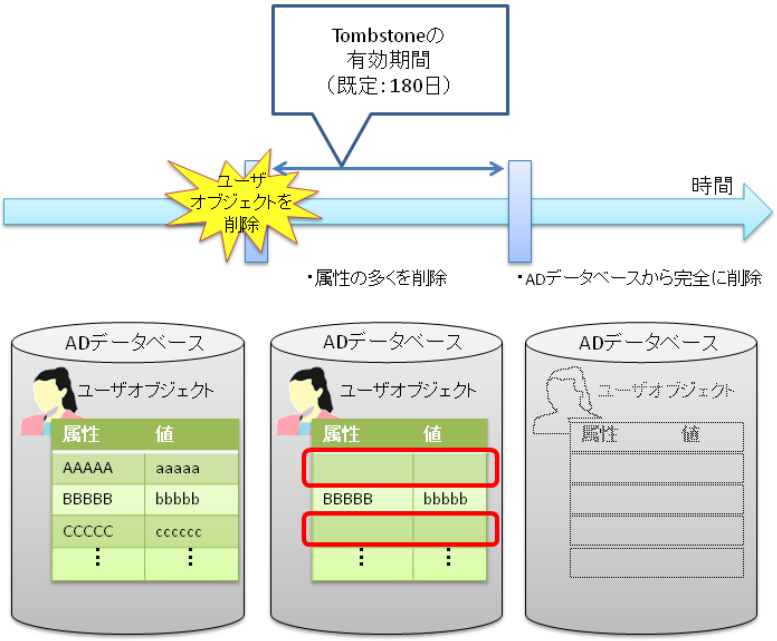


図 11Active Directory Recycle Bin 無効時の動作イメージ

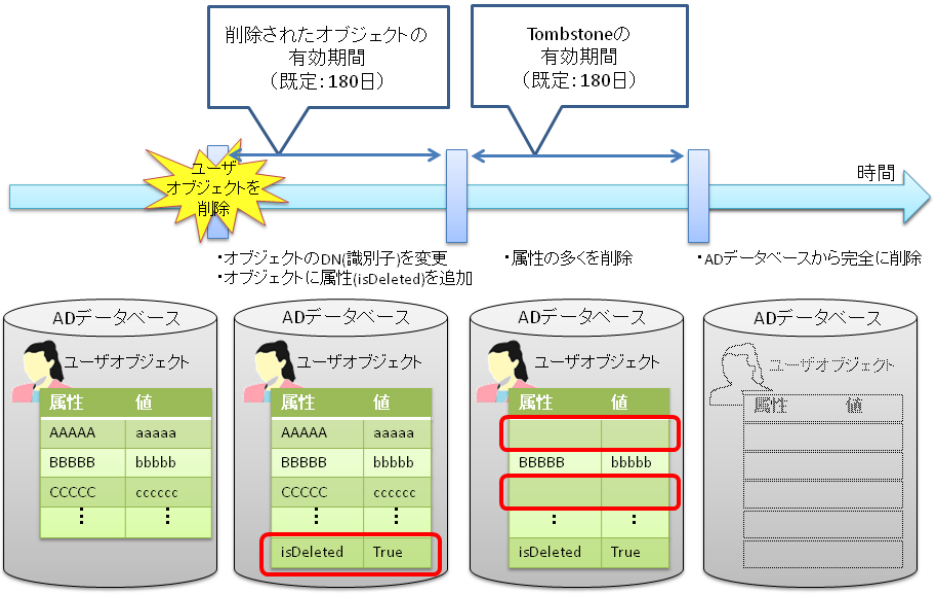


図 12Active Directory Recycle Bin 有効時の動作イメージ

Copyright 2011-2014 FUJITSU LIMITED

おわりに

AD を安定稼働させるためには、以下のポイントを考慮した、運用管理計画が重要になります。

- 運用管理要件を明確に定義する
- システムの異常や障害を早期に発見する監視方法を設計する
- 効率よくオブジェクトを管理するしくみを検討する
- あらゆる障害パターンを想定して、障害発生時に迅速な復旧方法を計画する

Copyright 2011-2014 FUJITSU LIMITED

付録 1 Authoritative Restore を利用したリストアイメージ

Authoritative Restore で AD のデータベースを復元すると、復元したデータベースが最新情報と認識され、他の DC に複製されます。図 13 に Authoritative Restore を利用したリストアイメージを紹介します。

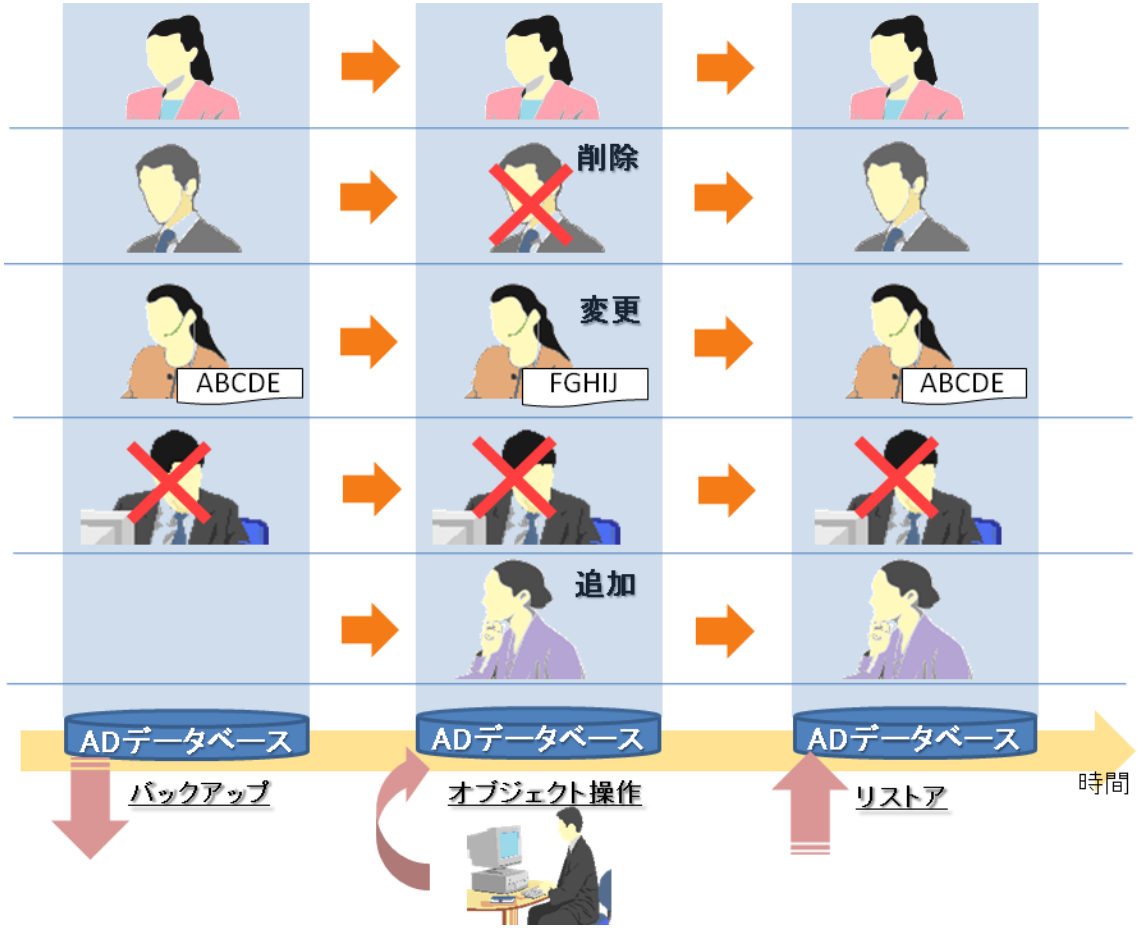


図 13Authoritative Restore によるリストアイメージ

① バックアップ後に何も操作を行っていないオブジェクトは、そのまま残る。
② バックアップ後に削除されたオブジェクトは、復元される。
③ バックアップ後に変更された属性は、復元される。
④ バックアップ前に削除されていたオブジェクトは、削除されたままとなる。
⑤ バックアップ後に追加されたオブジェクトは、削除されない。

Authoritative Restore では、DC を「ディレクトリサービス復元モード」で再起動し、システム状態を復元する必要があります(※)。システム状態の復元後に、コマンドプロンプトから「ntdsutil」コマンドを使用して Authoritative Restore を実行します。

(※)通常起動してディレクトリサービスを停止しても、Authoritative Restore はできません。

Copyright 2011-2014 FUJITSU LIMITED

付録 2 Sysvol フォルダのサイズとリストア時の DC 間複製時間について

リストア時の DC 間複製は、DC 間での初期同期処理が含まれます。同期が完了するまでは、Sysvol 共有が有効とならないため、DC として機能しません。同期の完了は、イベントの ID13516 で確認できます。リストア時の DC 間複製時間は Sysvol フォルダのサイズに応じて増加します。Sysvol フォルダのサイズは、グループポリシーオブジェクトの数に大きく影響を受けます。

Windows Server 2003 以前ではグループポリシーで使用する ADM ファイルが Sysvol フォルダに格納されるため、Sysvol フォルダが肥大化傾向にありました。富士通の事例でも、Sysvol フォルダのサイズが約 100MB あり、同期に 2 時間程度かかった例があります。
Windows Server 2008/Windows Vista 以降では、グループポリシー管理用テンプレートの実装が ADMX/ADML ファイルを使用する方式に変更され、同時に Sysvol フォルダに格納する仕様ではなくなったため、基本的には Sysvol フォルダが肥大化しないよう改善されています。

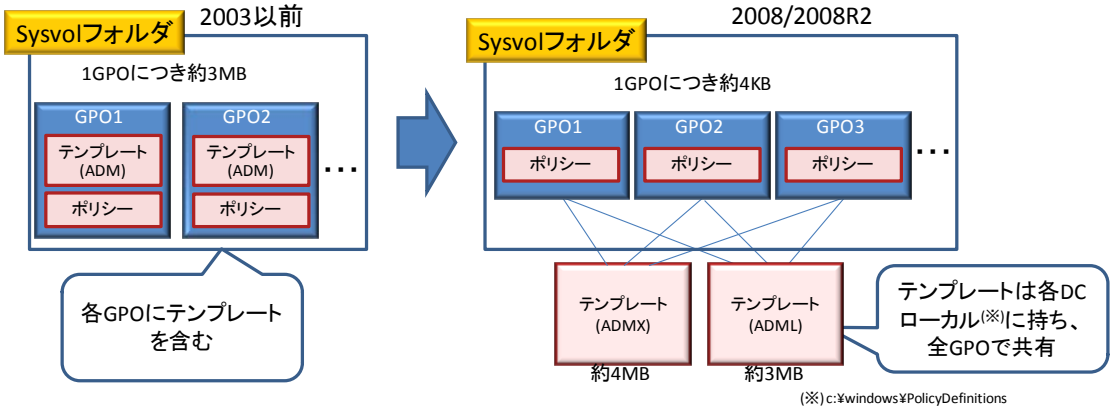


図 14 グループポリシーオブジェクトファイルの構成

但し、以下の場合は Windows Server 2008 以降でも Windows Server 2003 以前と同様に Sysvol フォルダ容量に注意が必要です。

- セントラルストアを構成し ADMX ファイルの集中管理を行う場合
  セントラルストアを構成した場合は、Sysvol フォルダ配下に ADMX ファイルを配置するため、容量を把握した上で復旧計画を考えます。
  ADMX ファイル、セントラルストアについての詳細は以下を参照してください。

  ・マイクロソフト「グループ ポリシー管理での ADMX ファイルの使用に関するステップ バイ ステップ ガイド」
  http://technet.microsoft.com/ja-jp/library/cc709647(WS.10).aspx

- 2003 ドメインから 2008/2008 R2 ドメインへ DC をアップグレードしている場合
  既存の ADM ファイルは、Sysvol フォルダに残るため、その容量を把握した上で復旧計画を考えます。

Copyright 2011-2014 FUJITSU LIMITED

PC サーバ FUJITSU Server PRIMERGY につきましては、以下の技術情報を参照願います。

・PC サーバ FUJITSU Server PRIMERGY（プライマジー）
http://jp.fujitsu.com/platform/server/primergy/
・FUJITSU Server PRIMERGY 機種比較表
http://jp.fujitsu.com/platform/server/primergy/products/lineup/select-spec/
・FUJITSU Server PRIMERGY サーバ選定ガイド
http://jp.fujitsu.com/platform/server/primergy/products/lineup/select-model/

PC サーバ FUJITSU Server PRIMERGY のお問い合わせ先。

・PC サーバ FUJITSU Server PRIMERGY お問い合わせ
http://jp.fujitsu.com/platform/server/primergy/contact/

基幹 IA サーバ FUJITSU Server PRIMEQUEST につきましては、以下の技術情報を参照願います。

・基幹 IA サーバ FUJITSU Server PRIMEQUEST（プライムクエスト）
http://jp.fujitsu.com/platform/server/primequest/
・FUJITSU Server PRIMEQUEST 製品ラインナップ
http://jp.fujitsu.com/platform/server/primequest/products/

基幹 IA サーバ FUJITSU Server PRIMEQUEST のお問い合わせ先。

・本製品のお問い合わせ
http://jp.fujitsu.com/platform/server/primequest/contact/

Copyright 2011-2014 FUJITSU LIMITED

商標登記について

- Microsoft、Windows、Windows Server、Hyper-V、Active Directory、Windows PowerShell は、米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。
- ARCserve は、米国 CA, Inc.社の商標です。
- 記載されている会社名、製品名は各社の登録商標または商標です。
- 記載されている会社名、製品名等の固有名詞は各社の商号、登録商標または商標です。
- その他、本資料に記載されている会社名、システム名、製品名等には必ずしも商標表示を付記しておりません。

免責事項

このドキュメントは単に情報として提供され、内容は予告なしに変更される場合があります。また、発行元の許可なく、本書の記載内容を複写、転載することを禁止します。
このドキュメントに誤りが無いことの保証や、商品性又は特定目的への適合性の黙示的な保証や条件を含め明示的又は黙示的な保証や条件は一切無いものとします。富士通株式会社は、このドキュメントについていかなる責任も負いません。また、このドキュメントによって直接又は間接にいかなる契約上の義務も負うものではありません。このドキュメントを形式、手段（電子的又は機械的）、目的に関係なく、富士通株式会社の書面による事前の承諾なく、複製又は転載することはできません。

Copyright 2011-2014 FUJITSU LIMITED

FUJITSU