ＢＣＰ対応の大学情報バックアップサービスの構築

稗田 隆, 岡山 聖彦, 河野 圭太, 内田　純平

岡山大学　情報統括センター

hieda-t@okayama-u.ac.jp

概要：大学では情報を各自でバックアップしているが、大規模災害により元データとバックアップデータが同時に喪失する危険性のあるシステムが多数存在している。このため、大学内の重要データを一元的に集約管理、遠隔地に設置した装置間で常時レプリケーションを行う情報バックアップサービスを構築した。バックアップ対象を基幹システム、各研究室の運用サーバ類、個人利用のＰＣ類等とし、多様な情報収集手段を提供している。

1 はじめに

岡山大学では、大規模災害により大学内の元データと保存しているバックアップデータが同時に喪失する危険性のあるシステムが多数存在していた。このため、大学内の重要データを一元的に集約保管し、遠隔地に設置したバックアップストレージ装置間で常時レプリケーションを行う情報バックアップサービスを構築した。

一方、岡山県は大規模災害に対して最も発生頻度の少ない安全な地域であるため、バックアップサービスの利用促進策が必要である。このため、基幹系システム、各研究室の個別サーバ類、個人利用のＰＣ類を含めた全学情報を一元的に、簡便にバックアップするための機能を実装し、利用者の利便性を確保した。また、情報保持者の了解のもとでの情報の２次利用の手段を実装した。システム構成では、バックアップ情報の重複排除機能、圧縮機能、合成バックアップ機能を実装した。

2　BCP 対応ﾊﾞｯｸｱｯﾌﾟｻｰﾋﾞｽの開発方針

岡山大学内の総ての情報に対して大規模災害発生時確実に情報を保存するサービスを提供する。本サービスでは、災害時の対応に遠隔地のデータセンターに情報を保持する。また、災害時のシステム復旧時間の短縮のため、システムと利用者情報を一括して保存する。

なお、本ＢＣＰ対応バックアップサービスは、長期間の情報保存サービスではなく、多世代の情報を保持するサービスであり、一般的な情報のバックアップサービスとは異なる。

以下、各機能の開発方針を示す。

2.1 バックアップ対象情報

学内の基幹系業務情報（約 340TB）、システムログ関連(約 10TB)、及び学内の個別サーバ群、学内 PC 群（約 70TB）をバックアップ対象情報とする。合計 420TB の情報を、最低 5 世代保持する。

2.2 データの保存方式

5 世代のバックアップ情報は単純計算で 2PB 以上となるが、①情報の重複排除機能、②情報の圧縮機能、③仮想の世代管理機能としての合成バックアップ機能により大幅な保存情報量を削減する。

情報の重複排除機能[1]は、保存情報をブロック単位で管理し、重複ブロックを削除することで大幅な情報量の削減を行う技術である。通常のバックアップ情報では 10 倍以上の情報の圧縮が期待できる。一方、動画情報など重複情報と判断されない情報も多数存在することから、重複排除によるデータ圧縮量は低めに見積る必要がある。(図 1)

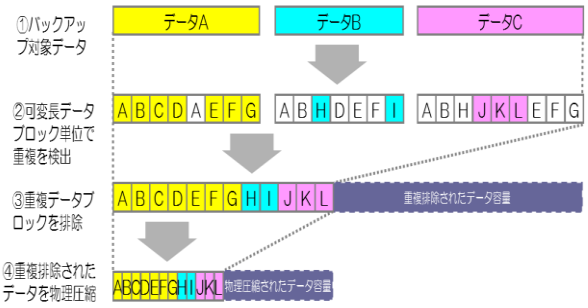

図.1 重複排除と圧縮の効果イメージ(NEC 資料)

合成バックアップ機能[2]は、フルバックアップ情報と、差分情報を用いて、仮想的に各世代のフルバックアップディレクトリを生成する機能である。総ての世代のフルリストアを高速に実行可能である。本機能により、対象システムからのフルバックアップは最初に一回のみであり、常に差分情報の取得で運用可能である。なお、古くてリストアに必要ない情報は自動削除する。

2.3 データセンターの活用

本学に設置したストレージ装置と、外部の BCP 対応のデータセンターに同一のストレージ装置と、情報のリストアを実施可能なサーバを設置する。これにより、常に２拠点間で同一の情報の保持と、相互のリストア動作を可能とする。

2.4 バックアップ情報の安全性

バックアップ情報の漏えい対策のためにバックアップ情報の暗号化、外部データセンター転送時の情報の自動暗号化を実施する。また、外部データセンターとは SINET を利用し、安全、安心と通信コストの大幅な効率化を実現する。

外部データセンターに設置するストレージ装置等は本学からの遠隔運用を行い、学内との一元運用とし、第三者によるアクセスは禁止する。

2.5 バックアップ情報の活用

本システム内のバックアップ情報は全学の情報資産である。これを大学経営に効率的に活用する手段を提供する。具体的には、バックアップ情報を任意の粒度でリストア可能とする情報管理サーバを設置する。今後、利用方法を含め明確化を進める。

2.6 運用監視機能の充実

バックアップ失敗、リストア失敗等のリスクを最小にするために GUI を基本とした運用監視機能を実装する。特に、リストア機能に関しては定期的なリストア試験を実施し、情報の完全性を確認する機能を実現する。

3　BCP 対応ﾊﾞｯｸｱｯﾌﾟｼｽﾃﾑの構成

3.1　ﾊﾞｯｸｱｯﾌﾟｼｽﾃﾑの構成

２章に沿ったシステム概略図を図.２に示す。一部を除き、情報のバックアップ処理に必要な基本装置は２重化以上で構成し、バックアップサービスの無停止を実現した。

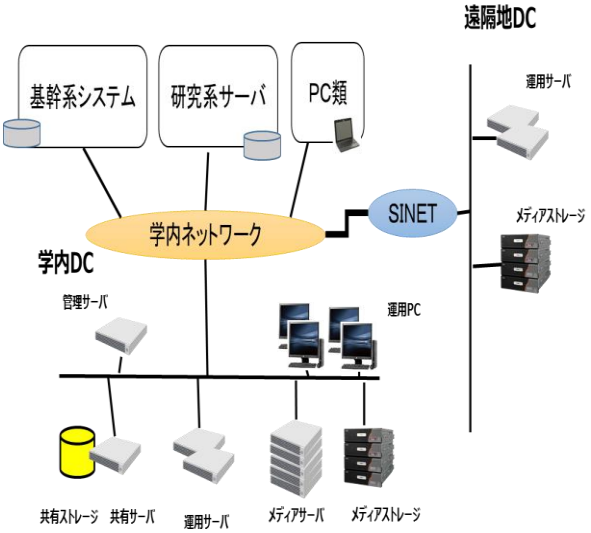

図.２　システム概略図

3.2　DDNS による動的 IP アドレスの管理

DDNS とは、DNS データベースを動的に更新する技術[3]である。接続ごとに DNS レコードを更新することで一意のホスト名を常時接続環境の PC に対して付与するサービスが DDNS である。

運用サーバは、バックアップ対象装置をホスト名(FQDN)で識別(特定)する。一般的に、バックアップ対象としてはサーバ機器が多く、これらの機器の IP アドレスは固定されているので、ホスト名と IP アドレスの紐づけは、hosts ファイルあるいは DNS で静的に管理すればよい。これに対し、本サービスでは、バックアップ対象装置(通常の PC 類)を対象とし、これらの装置の IP アドレスは DHCP サーバにより動的に配布し固定されていないため、ホスト名と IP アドレスの紐づけを静的に管理することができない。

バックアップ対象装置については DDNS サービスを提供する。具体的には、DDNS 機能を持つローカル DNS サーバを運用サーバ内に用意し、バックアップ対象装置は DHCP サーバから IP アドレスの配布を受ける度に、ローカル DNS サーバに対して自身のホスト名と IP アドレスの組を登録する(こ

の動作を DNS Update という)。

一方、運用サーバによるバックアップ動作が必要になった場合、バックアップ対象装置のホスト名をキーとしてローカル DNS サーバに IP アドレスを問い合わせる。ローカル DNS サーバは、その時点で保持している(問い合わせのあったホスト名に対する)IP アドレスを返す。このため、IP アドレスが固定されていない場合でも、クライアント機器が正しく DNS Update を行っていれば、運用サーバはホスト名により常に同じバックアップ対象にアクセスすることが可能となる。

具体的な動作は以下の通り。(図. 3 参照)

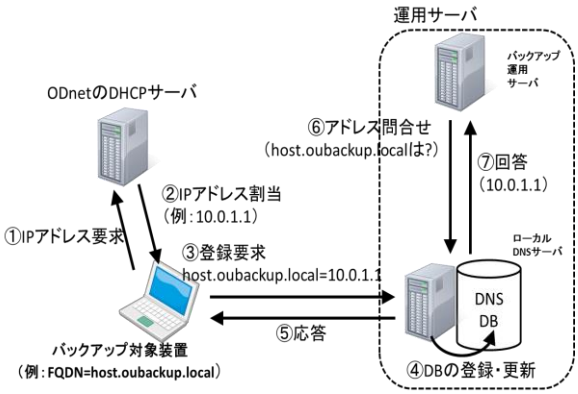

図. 3　DDNS による動的更新の流れ

(1) バックアップ対象装置

バックアップ対象装置は、起動時やスリープからの復帰時など、DHCP サーバから IP アドレスの配布を受ける度に、ローカル DNS サーバに対して自身の FQDN(hostname.oubackup.local)と IP アドレスの登録要求メッセージを送信する。なお、マイクロソフトのサイト[4]によれば、DHCP による IP アドレスのリースが変更または更新された際にも、同様の登録要求が行われる。

(2) ローカル DNS サーバ

バックアップ対象装置からの登録要求を受け付けて、登録要求メッセージに含まれる FQDN と IP アドレスの組を自身の DB に登録する。これ以外の動作は、通常の DNS サーバと同様である。

運用サーバ上の仮想マシンとして動作する Linux サーバに、DNS サーバの標準的なパッケージである bind をインストールして、DDNS 機能をサポートするローカル DNS サーバを新規導入した。プライベートなドメインとして"oubackup.local"を導入し、このドメインに対する DNS Update を受け付けて、ホスト名と IP アドレスの組を登録する。ローカル DNS サーバは、学内からの登録および問い合わせのみを受け付ける。

また、oubackup.local 以外のドメインに対する問い合わせは、すべて本学認証ネットワークシステム(ODnet)の DNS サーバにフォワードしている。

4 バックアップ動作の流れ

4.1　情報のバックアップ時の動作

図 4 に情報のバックアップの流れを示す。

バックアップ対象システムには、バックアップクライアントソフトウェアを実装し、差分増分バックアップ（前日からの差分バックアップ）を行う。情報は、メディアサーバによりソフトウェア的な重複排除を、メディアストレージによる、ブロック単位での情報（複数のシステムのバックアップ情報）に対して再度重複排除と情報の圧縮処理を行う。

完了した情報で発生したメディアストレージ間の差分を外部データセンターへレプリケーションし、情報の整合性を確保する。

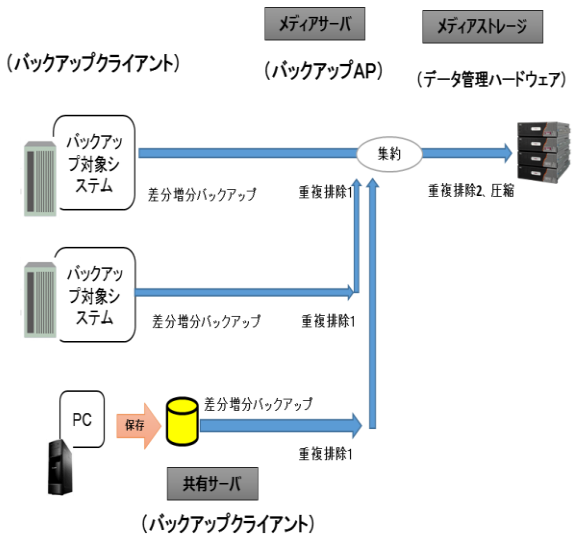

図.4　バックアップ情報の処理イメージ

4.2　情報のリストア時の流れ

リストア処理は、大学内と外部データセンターに設置したメディアストレージのいずれかを指定して、運用サーバから実行する。

管理サーバはメディアストレージ内の保持情報を任意に指定して運用サーバ、共有ストレージ、あるいはUSB接続DKへのリストアを実施する。本機能は情報のリストア試験にも用いる。

4.3　ﾊﾟﾌﾞﾘｯｸｸﾗｳﾄﾞｽﾄﾚｰｼﾞｼｽﾃﾑへの情報の転送

今後バックアップ情報の増加、あるいは本サービスで想定している期間を超えたバックアップ情報の保持（例えば、１年以上の情報保持）への対応のため、ストレージ型のパブリッククラウドサービスへのバックアップ情報の連携機能と、情報の管理機能（転送情報の管理、一定期間後の自動削除機能など）を提供する。

5 利用者による情報のバックアップ処理

全学情報に対してバックアップサービスを提供する。

以下、利用方法の概要を示す。

5.1 基幹系業務システムのバックアップ運用

基本方針は、バックアップクライアントソフトウェア(以下 CS と略す)をバックアップ対象システムにインストールする。CSにより、ポリシーに従ったバックアップ処理を実行する。（図.5）

本サービスではバックアップ実行時のバックアップ対象システムの性能低下の影響をバックアップ未実行時の１割以下と規定していることから、CSによる重複排除は実施していない。

①基幹系業務システムへのCS搭載が可能な場合

バック対象アップシステム上で CS による差分増分バックアップを実行する。

②基幹系業務システムへのCS搭載が不可の場合

バックアップ対象ファイルへのメディアサーバからのアクセス許可を設定し、メディアサーバから差分増分バックアップを実行する

5.2 学内ｻｰﾊﾞ、学内 PC の情報のﾊﾞｯｸｱｯﾌﾟ運用

学内設置のサーバ、PC バックアップのために、IPアドレスと共有エリアのユーザ管理機能を利用する。

(1)動的IPアドレスで運用する場合、DDNSを使用するために以下設定を行う。

①DNSの動的更新機能の有効化

②ドメインとして"oubackup.local"を指定

③プライマリ DNS サーバをのローカル DNS サーバに指定し、セカンダリ DNS サーバとして ODnet の DNS サーバを指定

(2)共有ストレージのユーザ管理を、本学統合認証管理システムの物品管理機能と連携して運用し、バックアップ対象システムに物品 ID を付与して共有エリアを提供している。

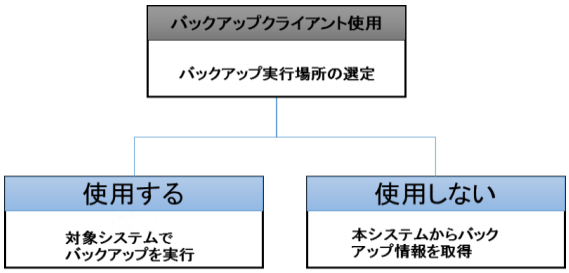

図.5　基幹系業務のバックアップ処理

(3)学内サーバ、学内 PC は以下の各方式から選択してバックアップを実行する。(図,6)

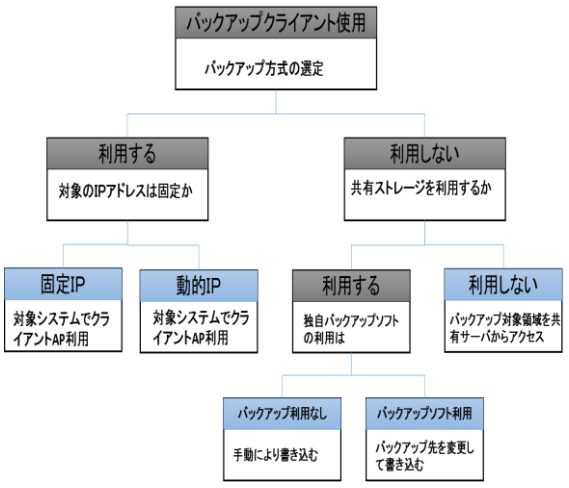

図.6　学内サーバ、学内 PC のバックアップ処理

① 提供された共有ストレージ（物品 ID ごとに 10GB の領域)に対して、人手等によるバックアップ情報の書き込みを行い、バックアッ

プする。

② バックアップ対象システムに付与された共有ストレージをネットワークドライブ等として利用し、利用中のバックアップソフト等によりバックアップを実行する。なお、独自のバックアップソフトによりバックアップを行っている場合、バックアップ格納先を本共有ストレージに変更することで遠隔地への二次バックアップが実現できる

③ 共有サーバにバックアップ対象フォルダへのアクセスを許可することで、共有サーバの CS がバックアップを実行する。すでにＮＡＳ等を利用したバックアップを実行している場合、ＮＡＳに対して共有サーバからのアクセス許可行うことで、二次バックアップが実行される。

④ バックアップ対象システムへの CS の搭載可能な場合は、CS によるバックアップを実行する。この場合は特に、差分増分バックアップ情報量により CPU 負荷、ネットワーク負荷等の増加への対応が必要である。

5.3 利用者によるリストア処理

利用者によるリストア処理は提供しない。

リストア処理は、大規模災害時を除き利用者からの申請に基づきシステム管理者が実施する。リストア情報は、利用者の要求に沿って可搬型媒体や、既存システム、共有ストレージにて提供する。

6 性能に関する実測値例

実際のバックアップ処理の性能値を例示する。なお、性能値はシステム条件、バックアップ条件、ネットワーク条件等で大きく変化するため一例として提示している。

(1)バックアップ性能（バックアップ対象システムからメディアサーバ間のスループット）: 約 22 MB/秒（1 週間の全バックアップ動作の平均値）

(2)PC から共有ストレージへの書込み性能：80MB/秒～9MB/秒　（環境で大きく変化）

(3) レプリケーション性能（メディアストレージ間のデータ転送速度）：　最大 47 MB/秒　（上限 500Mbps の制限による）

管理サーバ上の転送速度の例を図.7 に示す。

(4) メディアストレージからのリストア処理：24MB/秒　（約 100GB のリストアの例）

(5)差分増分バックアップ容量：全システム容量の約２％　（例:2.1TB に対して差分情報は約 40GB）

(6)メディアストレージの圧縮率：14.3 倍　（全バックアップ情報量 260TB に対して保存容量 18.2TB）

なお、バックアップ処理は 5 台のメディアサーバによる負荷分散で行っている。現状の各サーバの CPU 利用率は 3～4%であるが、2 台のサーバのメモリ使用率は 90%を超えている。

図.7　一週間のレプリケーションの速度例

7 運用機能と考察

7.1 運用画面

BCP バックアップサービス全体は統合された環境で運用、制御を行っている。実際の運用画面の例を図.8～図.9 に示す。

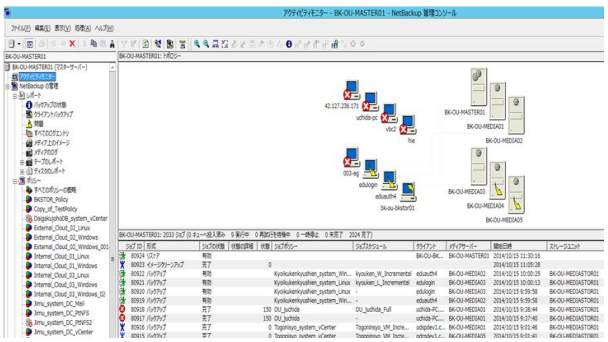

図.8　バックアップの動作管理画面の例

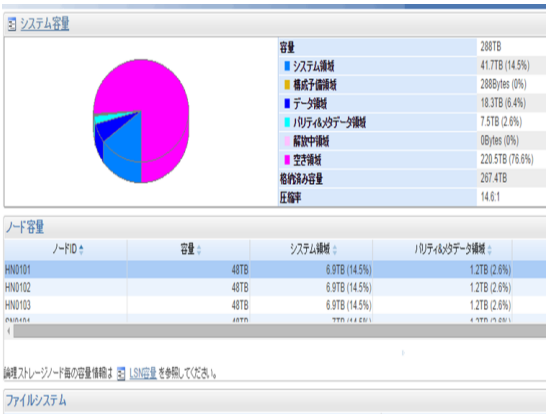

図. 9　システムの容量監視画面の例

7.2 考察

現在の BCP 対応バックアップでは、合成バックアップ機能により 30 日間の仮想的なフルバックアップを保持している。バックアップ情報を任意の日付を指定してリストア可能であり、リストアに要する時間は性能に関する実測値からバックアップと同等のスループットであり、満足できる性能と考える

重複排除と圧縮機能、差分増分バックアップと合成バックアップの活用により実際にメディアストレージに保存が必要となる情報は約 14 分の 1 である。現在、本学における基盤システムと個別サーバ類の約 175 システムをバックアップ対象として運用しているが、30 世代で必要とする差分情報は約 50TB である。(図. 10 参照)　ハードウェアの実保存容量は 3TB 程度であることから、現在のハードウェア資源を前提とすれば、３年、1,000 世代程度の仮想フルバックアップを保持可能である。長期間の情報の更新履歴保存は BCP 対策以上の利用者サービスを提供できる。

なお、合成バックアップに伴うカタログ情報は、30 世代(30 日)で約 100 GBであり、3 年で 3.6TB が必要になる。

図. 10　メディアストレージの容量推移

8 さいごに

岡山大学では、BCP 対応に特化した全学の情報バックアップ環境を構築した。現在は運用開始後で今後 PC や個別サーバ等を追加していく段階である。今後、バックアップ情報の増加に伴い、より重複排除機能、合成バックアップ機能の優位性が増し、大量の情報が保存されると考えている。

また、PC 利用者は共有フォルダへの情報の書き込み等の単純な処理により、大規模災害時においても情報の喪失を防ぐ確実な安全が確保できる。

今後は、バックアップ対象システムの損壊時に業務実行に必要となる仮想環境を整備し、実際の大規模災害発生時においてスムーズに業務を再開する環境整備、安否確認等の緊急処理に必要な情報の即時提供の運用環境の高度化を進めていく必要がある。

参考文献

[1]日本電気 HP, HS8-40 http://jpn.nec.com/istorage/product/backup/hs/hs8_40/index.html

[2]ｼﾏﾝﾃｯｸ HP, Symantec Backup Exec ｱﾄﾞﾊﾞｲｻﾞｰ, http://www.symantec.com/region/jp/beadviser/b-14.html

[3] P. Vixie, S. Thomson, Y. Rekhter and J. Bound, "Dynamic Updates in the Domain Name System (DNS UPDATE)", RFC2136, 1997.

[4] ﾏｲｸﾛｿﾌﾄ HP, 動的更新、http://msdn.microsoft.com/ja-jp/library/cc784052%28v=ws.10%29.aspx