

# **Symantec Backup Exec™ 11d Active Directory エージェント による Microsoft® Active Directory のクイックリカバリ**

Microsoft Windows® 2000 Server および  
Windows Server 2003 での使用

White Paper: Enterprise Solutions

# Symantec Backup Exec 11d Active Directory エージェントによる Microsoft Active Directory の クイックリカバリ

## 目次

概要 .....	3
従来の Active Directory リカバリプロセス .....	4
Active Directory の用語 .....	5
Active Directory バックアップとリカバリの改善 .....	5
Active Directory エージェントの利点 .....	6
他のソリューションとの主要な相違点 .....	8
Backup Exec 11d による Active Directory のリカバリ .....	9
Active Directory エージェントの要件 .....	9
Active Directory ドメインコントローラの要件 .....	10
Backup Exec 11d メディアサーバーの要件 .....	10
一般的な要件とベストプラクティス .....	10
まとめ .....	12

## Symantec Backup Exec 11d Agent for Active Directory による Microsoft Active Directory クイックリカバリ

### 概要

Microsoft Active Directory は、Windows ベースのシステムを導入するあらゆる規模の Windows 環境において、組織と経営の基盤となっています。Microsoft Exchange や SharePoint® Portal Server など、Active Directory に依存するアプリケーションがインストールされている環境において、Active Directory は標準のディレクトリサービスとなっています。このような理由から Active Directory が幅広く普及しているため、Active Directory の包括的なデータ保護と迅速なリカバリの必要性が高まっています。

データやシステムの損失の最大の原因は、人為的なミスとハードウェア/ソフトウェアの障害です。Active Directory においては、オブジェクトが誤って変更、削除、また誤ったスクリプトによって属性が書き換えられることなどのデータ損失があります。その他にもハードウェア障害によって破損することもあります。ユーザーアカウントが誤って削除された場合、そのユーザーは何時間、あるいは何日も生産性が失われるばかりでなく、企業のリソースにアクセスすることができなくなります。さらに、Active Directory に依存しているマイクロソフト社のアプリケーションが Active Directory のダウンタイムによるリスクを増大させます。Active Directory のデータが損失、破損の影響は、Windows 環境全体に波及し、Microsoft Exchange、SQL Server、SharePoint にも影響を与えます。

Active Directory で実際にリカバリが必要とされる情報の大部分は、消失、削除、破損、または書き換えされたユーザーアカウント、オブジェクト、および属性です。こういった情報が迅速にリカバリされなければ、「小さな障害」が大惨事になる可能性があります。しかし、個々のユーザーアカウント、オブジェクト、各属性等が消失または破損した場合に、Active Directory 全体をリカバリすることは、管理の時間と労力の観点から実用的な策とは言えません。

Active Directory の従来のリカバリソリューションは通常、次の 2 つのカテゴリに分類されます。

- 既存のバックアップとは別に管理される Active Directory のバックアップを必要とするスタンドアロンユーティリティ
- Windows オペレーティングシステムに無料で提供されているコマンドラインユーティリティ

Symantec Backup Exec 11d が提供する Active Directory エージェントは、小さな障害からリカバリする時間を大幅に削減し、従業員の生産性の向上や、大惨事にいたる可能性の低減、さらに従来の方法による Active Directory の保護とリカバリによる悪影響の緩和に役立ちます。

## Symantec Backup Exec 11d Agent for Active Directory による Microsoft Active Directory クイックリカバリ

### 従来の Active Directory リカバリプロセス

削除されたユーザーアカウントや失われた属性などの Active Directory のデータを Microsoft Ntdsutil などの標準ツールを使用してこれまでリストアしてきた管理者は、従来のリカバリプロセスにかかる時間とフラストレーションがどれほどのものかを理解しています。従来の Active Directory リカバリツールを使って Active Directory データをリカバリしようとする、管理者や企業は次のような問題に直面します。

- Active Directory の Authoritative Restore は、Ntdsutil などのコマンドラインシステムツールを利用する必要がある。
- システム状態のフルリストアを実行する必要があるため、ダウンタイムが増大する。
- Authoritative Restore を実行するにはドメインコントローラをネットワークから切断する必要があるため、リカバリの実行中、ユーザーはネットワークリソースにアクセスできなくなる。
- ドメインコントローラは最低 2 回再起動する必要がある、ダウンタイムとリスクが増大する。
- フルリカバリの終了後、レプリケーションにより冗長性を確保している Active Directory は、ディレクトリの大部分がインバウンドとアウトバウンドで複製されるのを待つ必要がある、ダウンタイムがさらに増大する。

データが破損または削除された場合、Active Directory の Authoritative Restore を実行する従来のリカバリでは、重要なドメインコントローラ上で時間のかかる再起動を複数回行うばかりでなく、複雑なコマンドラインユーティリティを使用することになります。このプロセスは次のとおりです。

1. Active Directory リカバリモードで再起動する(F8)。
2. システム状態をリストアする。
3. ネットワークケーブルを取り外す。
4. 再起動する。
5. コマンドラインユーティリティ Ntdsutil を使用して、リカバリするオブジェクトを取り出す。
6. ネットワークに接続する。
7. アウトバウンドとインバウンドのレプリケーションが実行されるのを待つ。

## Symantec Backup Exec 11d Agent for Active Directory による Microsoft Active Directory クイックリカバリ

### Active Directory の用語

**Active Directory**—リソースの検索と管理を行うための、ネットワークベースで分散型、階層型、および複製されたオブジェクトストアとサービス。

**Active Directory Application Mode (ADAM)**—Active Directory の軽量版。

**属性**—Active Directory オブジェクトのプロパティ(例: CN = Bob)。

**削除されたオブジェクトストア**—Active Directory から削除されたオブジェクトを格納するコンテナ。

**ドメインコントローラ**—Active Directory データベースを格納し、セキュリティ認証要求(ログイン、アクセス権のチェックなど)に対応する。

**GUID**—Global Unique Identifier の略。

**オブジェクト**—リソース、サービス、または人。Active Directory では、オブジェクトは階層型で編成される。

**SID**—Security Identifier の略(固有)。

**廃棄 (Tombstone)**—オブジェクトが削除用にマークされていることを示す Active Directory のインジケータ。

**廃棄 (Tombstone) の有効期間 (Tombstone lifetime)**—あるオブジェクトが削除されるまで、削除されたオブジェクトストアに残される日数。

### Active Directory バックアップとリカバリの改善

Active Directory エージェントのライセンスは、ドメインコントローラごとに、個別のアドオンコンポーネントとして付与されます。これには、ドメインコントローラ上にある Active Directory 以外のデータを保護するための Windows システムエージェントライセンスも含まれます。

Active Directory エージェントは、誤って削除または変更した Active Directory データをわずか数秒か数分でリカバリできます。この新しいエージェントでは、Active Directory または Active Directory Application Mode (ADAM) のオブジェクトと属性をリストアできます。この場合、Authoritative Full Restore や 非 Authoritative Full Restore を実行する必要はなく、再起動も不要です。

通常、Windows 2000 または Windows 2003 の Active Directory ドメインコントローラのシステム状態のフルバックアップは、ローカルまたはネットワーク経由で簡単に実行できます。この Active Directory エージェントのきめの細かいオンラインリストア機能を使用すると、ユーザー、組織単位、プリンタなどの選択したオブジェクトを、これらのオブジェクト内の個々の属性レベル、ディレクトリの特定のセクション、あるいは Active Directory 全体でさえリカバリすることができます。

## Symantec Backup Exec 11d Agent for Active Directory による Microsoft Active Directory クイックリカバリ

このとき、Active Directory ドメインコントローラをオフラインにする必要はありません。

Active Directory バックアップとリカバリプロセスは比較的シンプルです。

1. バックアップする Active Directory ドメインコントローラのシステム状態コンポーネントを選択する。
2. 詳細なリストアを実行するためのチェックボックスが選択されていることを確認する(デフォルトで有効)。
3. バックアップを開始する。
4. Active Directory ドメインコントローラのバックアップを生成した Backup Exec 11d ヘルプブラウズする。
5. リカバリするオブジェクトまたは属性を選択する。
6. リストアを開始する。

### Active Directory エージェントの利点

機能	説明	利点
オンラインリカバリ (再起動不要)	<ul style="list-style-type: none"> <li>Active Directory をオンラインの状態、Active Directory の重要な情報をリカバリ。</li> <li>リストアのために Active Directory サービスモードで再起動する必要はない。</li> <li>Windows Server 2003 Active Directory 環境で、「Tombstone(廃棄)済み」オブジェクトの再生をサポートする。</li> <li>Windows Server 2003 Active Directory 環境で、再生する「Tombstone(廃棄)済み」オブジェクトの SID 情報と GUID 情報を保持する。</li> </ul>	<ul style="list-style-type: none"> <li>高速で、容易なリカバリ。</li> <li>失われた、または壊れた Active Directory オブジェクトをリストアするために、重要なドメインコントロールを再起動する必要はない。</li> <li>ドメインコントローラが失われても、ネットワークユーザーに影響がない。</li> <li>元の ID、および他の Active Directory オブジェクトへの正しいリンクで、削除されたオブジェクトを復元できる。ID を再作成して、古いリンクを削除する必要もない。</li> </ul>
詳細なリカバリ (Granular Recovery)	<ul style="list-style-type: none"> <li>個々の属性レベルまで細かく、削除されたユーザーアカウント、プリンタ、組織単位など Active Directory オブジェクトをリストアする。</li> <li>Active Directory 全体をリストアせずに、個々のオブジェクトをリストアする。</li> <li>構成パーティションなど、ほとんどの Active Directory パーティションのオブジェクトをリストアする。</li> </ul>	<ul style="list-style-type: none"> <li>リカバリしたい Active Directory オブジェクトだけを、いつでもリストアできる。</li> <li>個々のオブジェクトのリカバリは、Active Directory 全体のリカバリよりも高速にできる。</li> <li>最も重要な Active Directory オブジェクトを高速にリカバリする機能が向上する。</li> </ul>
ディザスタ リカバリのフルサ ポート	<ul style="list-style-type: none"> <li>Active Directory、SYSVOL、COM+ データベース、Windows レジストリ、システムファイルなど、すべてのシステム状態コンポーネントの完全バックアップをサポートする。</li> </ul>	<ul style="list-style-type: none"> <li>システム状態と Active Directory のディザスタリカバリを完全にサポートし、ドメインコントローラのリカバリを迅速かつ容易に実行する。</li> </ul>

## Symantec Backup Exec 11d Agent for Active Directory による Microsoft Active Directory クイックリカバリ

### Active Directory エージェントの利点（続き）

機能	説明	利点
バックアップとリストアのパフォーマンス	<ul style="list-style-type: none"> <li>データベースとオブジェクトレベルのリカバリに個別のジョブを実行する必要がない。</li> </ul>	<ul style="list-style-type: none"> <li>システム状態のハイパフォーマンスバックアップにより、個々の Active Directory オブジェクトレベルのリカバリのメリットを享受。</li> </ul>
管理の容易性	<ul style="list-style-type: none"> <li>Windows データを保護するために設計された使いやすい直感的なインターフェースを提供する。</li> </ul>	<ul style="list-style-type: none"> <li>トレーニングと管理にかかるコストを削減できる。</li> </ul>
Active Directory Application Mode (ADAM) のサポート	<ul style="list-style-type: none"> <li>ADAM オブジェクトのバックアップとリカバリに対応する。</li> <li>ADAM のオンラインバックアップとリストア。</li> </ul>	<ul style="list-style-type: none"> <li>同じ Granular Recovery Technology (GRT) を使用して、他の Active Directory オブジェクトと同様、容易に ADAM オブジェクトをリストアできる。</li> <li>ADAM をオフラインにしたり、重要なドメインコントローラを再起動することなく、ADAM オブジェクトをリストアできる。</li> </ul>
一元管理	<ul style="list-style-type: none"> <li>Active Directory のバックアップとリカバリを一元管理する。</li> <li>Active Directory 環境全体のバックアップを管理する集中管理コンソール。</li> <li>Microsoft Exchange、SharePoint、SQL Server などユーザー環境全体の Active Directory の保護と個々のオブジェクトのリカバリを統合する。</li> </ul>	<ul style="list-style-type: none"> <li>ドメインコントローラに及ぶことなく、すべてのリストア操作を一箇所から実行できる。</li> <li>ドメインコントローラのローカルとリモートからのバックアップを一箇所で管理、コントロールできる。</li> <li>Active Directory とその他のバックアップをユーティリティを使用せず、1 つの製品を使用してスケジューリングおよび管理できる。</li> </ul>
メディアに依存しない	<ul style="list-style-type: none"> <li>ディスクまたはテープにバックアップできる。<sup>1</sup></li> <li>D2D2T (ディスク -to- ディスク -to- テープ) ステージングを自動化できる。<sup>1</sup></li> </ul>	<ul style="list-style-type: none"> <li>Active Directory を保護するためにほとんどすべてのバックアップデバイスを使用できる。</li> <li>Active Directory バックアップは、まずクイックリカバリのためにディスクへ、その次にオフサイトディザスタリカバリプロテクションのためにテープへ段階的にステージングできる。</li> </ul>
組み込み暗号化	<ul style="list-style-type: none"> <li>非常に強力な 128/256 ビット AES 暗号化により、企業の Active Directory の機密データを保護する。追加料金は不要。<sup>2</sup></li> </ul>	<ul style="list-style-type: none"> <li>Active Directory バックアップ情報をオンサイトとオフサイトの両方に安全に、確実に格納する。</li> </ul>

<sup>1</sup> テープバックアップから個々の Active Directory オブジェクトをきめ細かくリカバリするためには、2 段階のリストアプロセスが必要です。Backup Exec は、このプロセスを自動化し、リストアするデータをまず保存した後、そのデータを対象のリストア先に書き込みます。

<sup>2</sup> 詳細なリカバリ機能を有効にしている場合、暗号化されたバックアップをディスクにバックアップすると自動的に復号されます。そして、長期のデータ保護またはディザスタリカバリの目的でテープに移すときに暗号化されます。

## Symantec Backup Exec 11d Agent for Active Directory による Microsoft Active Directory クイックリカバリ

### 他のソリューションとの主要な相違点

他のソリューションとは異なり、Active Directory エージェントは Active Directory がインストールされている Windows のシステム状態と ADAM のバックアップと連携します。Windows のシステム状態をバックアップする場合、Active Directory をコンポーネントとして含みます。

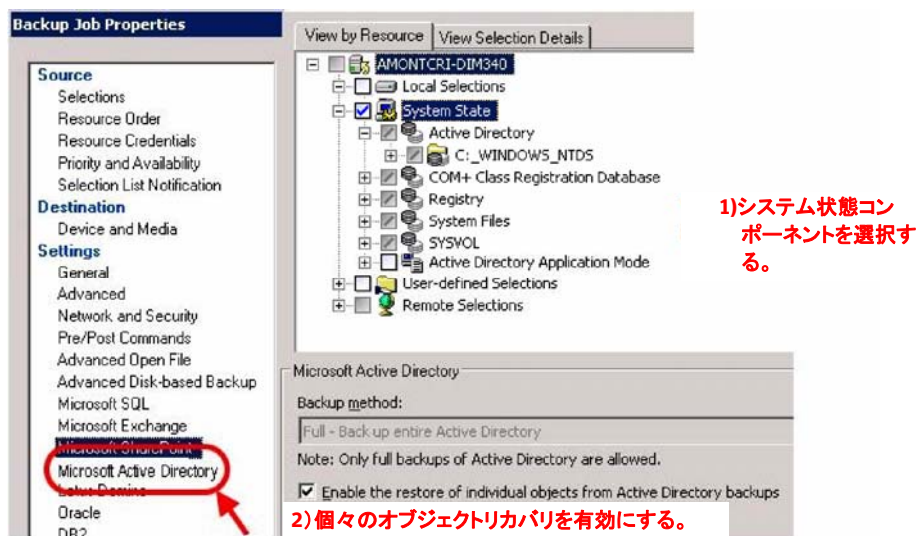


図 1. システム状態のシングルパスバックアップ

個々の Active Directory オブジェクトと属性をリストアするには、[リストアジョブのプロパティ]ビューの [選択リスト] タブからオブジェクトや属性を選択します。また、個々の ADAM オブジェクトと属性をリストアするには、個々の ADAM オブジェクトと属性を選択します。複数の ADAM インスタンスをバックアップする場合、各インスタンスは ADAM ノードの下に表示されます。Active Directory の完全なシングルパスバックアップ(図 1 を参照)は、次のように実行します。

1. バックアップする Active Directory ドメインコントローラの [システム状態] コンポーネントを選択する。
2. 詳細なリストアを実行するためのチェックボックスが選択されていることを確認する(デフォルトで有効)。
3. バックアップを開始する。

## Symantec Backup Exec 11d Agent for Active Directory による Microsoft Active Directory クイックリカバリ

Backup Exec 11d による Active Directory のリカバリ

データの破損または削除のために ユーザー情報のリカバリを実行する場合、リカバリは以下の簡単な 3 つの手順で済みます。

1. Backup Exec 11d が作成した、ドメインコントローラのバックアップへブラウズする(図 2 を参照)。
2. リストアするオブジェクトまたは属性を選択する。
3. リストアを開始する。

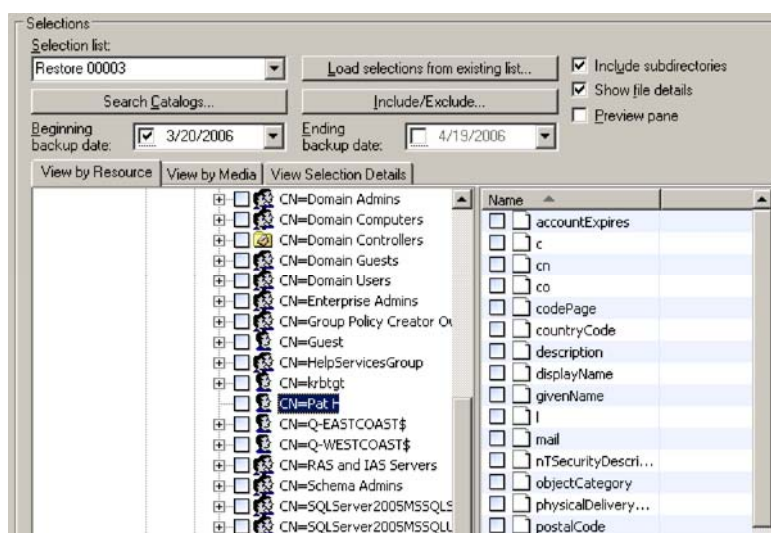


図 2. リストアする Active Directory オブジェクトの選択

### Active Directory エージェントの要件

上記以外に Active Directory オブジェクトをきめ細かくリカバリするために Backup Exec を設定する手順はありませんが、Active Directory エージェントを使用して個々のオブジェクトと属性をリストアするには次の要件を満たす必要があります。

### Active Directory ドメインコントローラの要件

Active Directory をインストールするコンピュータでは、次のいずれかの Windows オペレーティングシステムを使用する必要があります。

- Windows 2000 Server Service Pack 4(注: Windows 2000 ドメインコントローラ上の Active Directory Deleted Objects コンテナからオブジェクトを再生することはできません。リストア中、オブジェクトは Backup Exec により再作成される必要があります。削除されたオブジェクトが同じドメインに存在する場合、Windows Server 2003 ドメインコントローラ上で Backup Exec

## Symantec Backup Exec 11d Agent for Active Directory による Microsoft Active Directory クイックリカバリ

Remote Agent により、削除されたオブジェクトを個別にリストアすることをお勧めします。)

- Windows Server 2003 Service Pack 1 以降
- Windows Server 2003 R2

### Backup Exec 11d メディアサーバーの要件

リストアジョブを実行するメディアサーバーでは、minifilter ドライバをサポートする Windows オペレーティングシステムのバージョンを使用します。以下の Windows オペレーティングシステムが minifilter ドライバをサポートします。

- Windows 2000 Server Service Pack 4/Windows 2000 Rollup Package 1
- Windows Server 2003 Service Pack 1 以降
- Windows Server 2003 R2

※個々のオブジェクトリカバリを実行するために、x64 Windows 2003 Active Directory ドメインコントローラは x64 バージョンの Backup Exec 11d によって保護することをお勧めします。

### 一般的な要件とベストプラクティス

- バックアップを作成するときには[Active Directory のバックアップで個々のオブジェクトのリストアを有効にする]オプションが選択されていることを確認します。このオプションが選択されている場合に限り、Active Directory や ADAM のフルバックアップから個々の属性とプロパティをリストアできます。このチェックボックスは、[バックアップジョブのプロパティ] ダイアログボックスの Microsoft Active Directory セクションにあります。
- バックアップがディスクベースで行われる場合、リストアにかかる時間はテープにバックアップするときよりもはるかに短縮されます。テープからリストアするには、テープからのデータをコピーする、一時的なハードディスク領域を作成する必要があります。テープからリストアする時間が長くなるのは、選択した属性とプロパティを抽出するためにバックアップセット全体を読み取る必要があるためです。一時的なハードディスク領域の指定は、Backup Exec の [ツール] > [オプション] > [リストア] メニューから行えます。Backup Exec はそこに、テープからリストアするとき、リストアしたいオブジェクトや属性を一時的に保管します。この場所は Backup Exec サーバー上のローカルパスである必要があり、バックアップする Active Directory データベース全体を格納するために十分な空きディスク容量が必要です。このテンポラリデータはリストアが完了すると自動的に削除され、このディスク領域は再利用されます。
- 個々の Active Directory または ADAM のオブジェクトや属性をテープから 64 ビットコンピュータにリストアするには、64 ビットのオペレーティングシステムが動作しているメディアサーバーにテープを移します。

## Symantec Backup Exec 11d Agent for Active Directory による Microsoft Active Directory クイックリカバリ

- ディスクへのバックアップフォルダをバックアップ先デバイスとして使用するには、ディスクへのバックアップフォルダのバックアップ先設定が Backup Exec メディアサーバーのローカル NTFS ボリュームにある必要があります。
- Active Directory エージェントのランセンスが付与され、インストールされている Windows 2000 または 2003 Active Directory ドメインコントローラのシステム状態の完全バックアップを作成しておく必要があります。Backup Exec の以前のバージョンで作成されたバックアップ、または Active Directory エージェントを使わずに作成されたバックアップは、オブジェクトをきめ細かくリストアするためには使用できません。
- Active Directory がインストールされているコンピュータで、Windows システムエージェントが実行されている必要があります。
- 「廃棄済み」オブジェクトを Active Directory Deleted Objects コンテナから再生できるのは、以下の場合です。
  - オブジェクトの廃棄 (tombstone) の有効期間が経過していない。つまり、廃棄済みのオブジェクトを再生するために利用できる Active Directory バックアップの使用期限が限られていることを意味します。リストア時、設定した廃棄の有効期間よりも古いバックアップからオブジェクトをリストアする場合、再生は期待できません。
  - オブジェクトが Deleted Objects コンテナからパーズされていない。
  - Windows Server 2003 Service Pack 1 ドメインコントローラにリストアしようとしている。

**注:** Windows 2003 Server Service Pack 1 では、廃棄の有効期間が 60 日から 180 日に変更されました。これにより、廃棄オブジェクトをバックアップから再生できる期間が延長されました。シマンテックでは、バックアップを行うすべての Windows Server 2003 ドメインコントローラに Service Pack 1 をインストールすることをお勧めします。マイクロソフト社のコマンドラインユーティリティ Ntdsutil を使用すると、この設定を変更できます。

## Symantec Backup Exec 11d Agent for Active Directory による Microsoft Active Directory クイックリカバリ

### まとめ

IT 企業は、その環境における重要なデータの保護とリカバリをいかに効率的に実行するかについて、日々奮闘し続けています。特に、機密データになるほどその傾向は顕著です。Active Directory は、マイクロソフト社の他のアプリケーション (Microsoft Exchange や SharePoint など) が依存する Windows ベースのシステムや基盤を持つ企業にとって重要なコンポーネントの一つとなりました。Microsoft Active Directory の従来のリカバリソリューションは、Active Directory の最も一般的なリカバリに必要な機能、特に、個々のオブジェクトのリカバリ機能を提供していません。Active Directory エージェントは革新的な新しいテクノロジーを提供し、IT 管理者はいつでも、必要な Active Directory データを高速かつ簡単にリカバリできます。特に、ユーザー、属性、コンポーネントなど Active Directory の重要なデータは、システムを再起動することなく、わずか数秒か数分でリカバリできます。



Copyright ©2007 Symantec Corporation. All rights reserved. SymantecとSymantecロゴは、米国におけるSymantec社およびその関連会社の登録商標です。その他の会社名、製品名は各社の登録商標または商標です。製品の仕様・価格は、都合により予告なしに変更することがあります。本ホワイトペーパーの記載内容は、2007年4月現在のものです。英語版の翻訳です。

---

## 株式会社シマンテック

〒107-0052 東京都港区赤坂1-11-44 赤坂インターシティ

[www.BackupExec.com/jp](http://www.BackupExec.com/jp)