長時間の電源障害時のデータ保全について

テッド アイブス

White Paper #10

Legendary Reliability™

Revision 1

要約

コンピュータテクノロジの進歩にもかかわらず、電源障害は常にコンピュータやサーバで起こるダウンタイムの主な原因になっています。無停電電源装置（UPS）によるコンピュータシステムの保護はトータルソリューションの一部ですが、UPS電源管理ソフトウェアを活用することも、長時間の電源障害に伴うデータの破損を防止するために欠かすことができません。このホワイトペーパーでは、多様なソフトウェア構成について説明し、アップタイムの確保を目的とする最適な方法を提示します。

背景

長時間の電源障害は、いつでも起こる可能性があります。電源障害が発生してしまうと、保護されていないコンピュータに対しては、必要なシャットダウンを行うことはできません。もともと、コンピュータやサーバのオペレーティングシステムは、「ハードシャットダウン」と呼ばれる不意の電源断に対処するようには設計されていません。そのため、メモリの保存、各種アプリケーションやサービスの停止など、コンピュータのシャットダウンは所定のプロセスによって実行する必要があります。通常、このプロセスを「正常なシャットダウン」と呼びます。一方、ハードシャットダウンは結果的にデータの消失やデータの破損を引き起こし、電源が回復した後でも、復旧に膨大な時間を要する可能性があります。

無停電電源装置（UPS）は、被害をもたらす電源障害からシステムを保護し、短時間の電源障害であれば、ユーザが作業を中断することなく続行できるため、サーバの可用性が向上します。UPSのバックアップ時間を超えるような長時間の電源障害が発生したとしても、システムにUPSシャットダウンソフトウェアがインストールされていれば、UPSのバッテリが完全に放電する前に、UPSと通信してシステムの正常なシャットダウンが自動的に行われます。

はじめに

長時間におよぶ電源障害の原因は、局地的な落雷による変圧器の破損から、広域の電力供給網の断線まで多岐にわたります。常に、ハードシャットダウンによるデータの破損からコンピュータシステムと保存データを守るため、適切な手段を講じる必要があります。長時間の電源障害でデータが破損する要因の1つは、データの操作中に生じるアプリケーションやオペレーティングシステムの異常終了です。ドキュメント、重要なファイルシステム構造（ファイルアロケーションテーブルなど）、動的なアプリケーションデータなどが、この異常終了の被害を受ける可能性があり、電源が回復した後でも、オペレーティングシステムやアプリケーションでは破損したテーブルの修復が試行されるため、「復旧までの時間」が長引くケースもあります。

また、コンピュータのハードドライブについても考慮することが必要です。ハードドライブ業界では、最近の10年間で「ヘッドクラッシュ」（異常終了すると、何らかの原因でハードドライブの読み込み/書き込みを行うヘッドがディスク面に接触し、表面を損傷すること）を防止するテクノロジが着実に進歩してきました。ハードドライブテクノロジは他の側面でも進歩しましたが、実際には、それがデータ破損の潜在的な原因となっています。より高いレベルの性能を実現するために、情報を一時的にメモリに書き込み、実際のディスクへの書き込みを後で行う、キャッシュ技術を利用するハードディスクコントローラが広く採用されています。ここで電源障害が発生するとキャッシュ内の情報は失われ、データファイルやデータの破損につながる可能性があります。

企業や政府でこの問題が大きく取り扱われることはありませんが、技術の進歩にかかわらず電源障害によるデータの破損は、現在でもIT業界の課題として広く認識されています。このことは、以下の業界関係者の意見からも**明らかです。**

「インターネットサービスプロバイダ、データセンタ、無線通信ネットワーク、オンライントレーダ、コンピュータチップメーカ、医療研究センタなど、電力の影響を大きく受ける顧客には、一瞬の停電が深刻な事態につながる可能性もあります。このよう

な顧客の場合、**データの破損**、基板の破損、コンポーネントの損傷、ファイルの破損、顧客の喪失など、**電源障害による被害は甚大です**」

-『Electrical Power Interruption Cost Estimates for Individual Industries, Sectors, and U.S. Economy（電源障害が個別産業、産業分野、米国経済に与えるコストの概算）』
2002年2月、U.S. Dept. of Energy Office of Power Technologies

「**電源障害の後に発生する起動障害の大半は、ファイルの破損**、またはハードディスクの損傷が原因です。最新の高性能システム構成でも、これを修復する手立てはありません」
- MCSE Microsoft® Windows® XP Professional Readiness Review
Exam 70-270、Section 70-270.04.03.002、2001年11月28日

「ネットワークやコンピュータ機器への電力供給が絶たれる電源障害。サーバやワークステーションでは、この障害が原因となり、システムおよびネットワークのクラッシュ、PCのロックアップ、**重要なデータの破損や損失**などが発生する可能性があります」
-「Power Protection Basics（電源保護の基本）」、2002年3月、『Contingency Planning Management Magazine』

「**システムおよびそのデータは、電源障害が原因で破損する恐れがあります。**UPSは電源障害からシステムを保護することができます。UPSは通常、緊急時にシステムを正常終了するために十分な電力を供給します」
-『Special Publication 800-34 Contingency Planning Guide for Information Technology Systems（臨時増刊800-34情報技術システムの災害対策ガイド）』
National Institute of Standards and Technology、2002年6月

UPS電源管理ソフトウェアの推奨構成

[構成1] 1台のコンピュータを1台のUPSで保護する場合

この構成では、各コンピュータはそれぞれ専用のUPSに保護され、UPSとコンピュータは、シリアルケーブルかUSBケーブルを介して通信します。UPS電源管理ソフトウェアをコンピュータにインストールしておくと、長時間におよぶ電源障害が発生した場合、システムは自動的に正常終了します。この場合、UPSに接続されているコンピュータでUPSを管理します。この構成が最も単純であり、サーバ、ワークステーションを問わず、多様な場所で利用されています。

図1 – 1台のコンピュータを1台のUPSで保護する場合

[構成2]　2、3台のコンピュータを1台のUPSで保護する場合

この構成では、複数のコンピュータをより大型のUPS（通常、1台で1500VA以上）に接続します。UPSのシリアルポートに直接接続するのは1台のコンピュータのみで、残りのコンピュータは、シリアルポートをUPSに増設する拡張カードに接続します。この構成では、コンピュータすべてを正常終了することができますが、UPSの管理はUPSに直接接続されているコンピュータで行います。

なお、USB規格では、1度に通信できる対象は1台のシステムに限られるため、この構成ではUSB接続を使用できない点にご注意ください。この方法では、最大24台のコンピュータを接続（デイジーチェーン方式を使用）できますが、追加ケーブルが必要になるため、APCではこの方法を推奨しません。

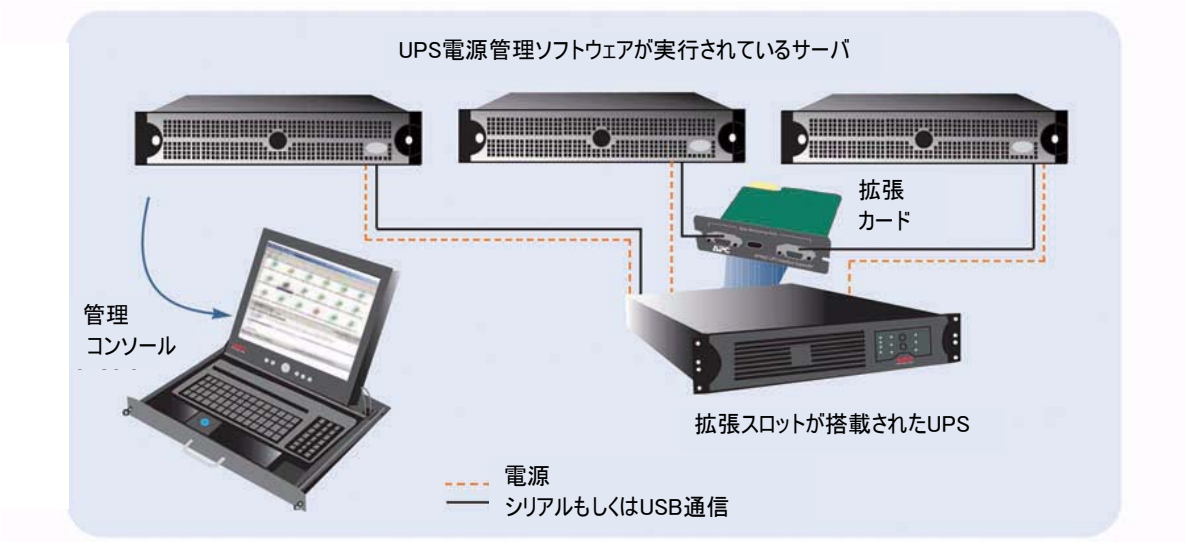

図2－2、3台のコンピュータを1台のUPSで保護する場合

[構成3] 3台以上のコンピュータを1台のUPSで保護する場合

最近では、LAN上でUPSを直接管理する手法が注目されています。この場合、UPS自体にネットワーク管理カード（リアルタイムオペレーティングシステムとハードウェアウォッチドッグチップ付き）が搭載されているために、サーバベースの管理は必要ありません。この方法を使用した構成例としては、APCのInfraStruXureアーキテクチャが挙げられます。この構成では、管理機能はUPS自体に組み込まれるため、コンピュータにインストールされたソフトウェアに必要なものはシャットダウン機能のみになります。

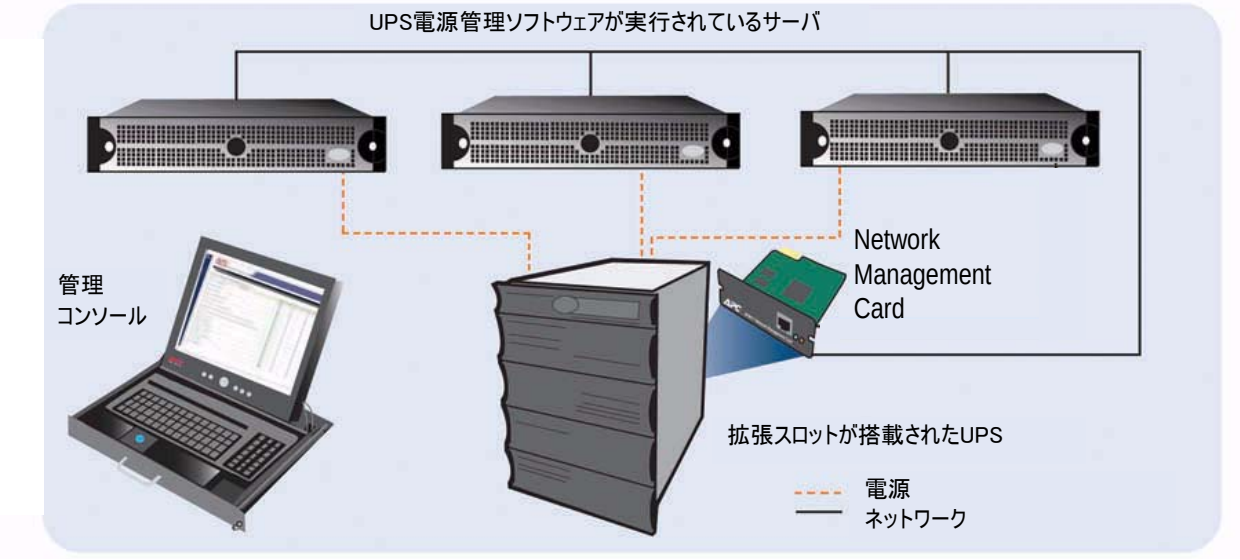

図3 － 3台以上のコンピュータを1台のUPSで保護する場合

オペレーティングシステムの多様なシャットダウン

Microsoft Windows®などの最新オペレーティングシステムでは、電源管理機能も一層発達し、新しいシャットダウン方法が組み込まれています。従来、電源管理機能はラップトップユーザの要件に対応するように発達してきましたが、それに加えてUPS電源管理ソフトウェアを使用することで、長時間の電源障害後に発生する復旧時間を抑えることもできます。

シャットダウン

これは従来から利用されてきた方法で、コンピュータのオペレーティングシステムでは、UPSのシャットダウンソフトウェアからシャットダウンコマンドを受け取り、アクティブなプロセスを順番に終了してからコマンドを終了します。たとえば、Windows®システムでは、画面上に「電源を切断する準備ができました」というメッセージが表示される状態になります。

シャットダウンと「電源オフ」

これは前述の方法と類似していますが、オペレーティングシステムはこのプロセスの最後で、実際に電源をオフにするようにコンピュータに命令します。そのため、システムは完全に停止し、電力の消費もなくなります。また、この方法は、前述の構成2を使用した環境でも有用です。1台のコンピュータを完全に停止することで、残りのコンピュータの起動時間を延長できるためです（この方法は「負荷制限」とも呼ばれます）。シャットダウンと「電源オフ」機能では、BIOSで自動的な「電源オフ」を有効に設定しなければならない場合もあります。

休止

休止プロセス（たとえば、最新のMicrosoft Windows®オペレーティングシステムに導入されています）は、前述の方法に類似していますが、一層高度で有用な手順が加わります。

1. 最初に、すべての開いているファイルを含め、コンピュータのデスクトップの状態が保存されます。これは、すべてのRAM情報を1つの大きなファイルとしてハードディスクに保存することで実現します。
2. 続いて、システムがシャットダウンされ、電源が切れます。
3. 電源が回復するか、オペレーティングシステムが起動されると、ハードディスクから再びRAM情報が読み込まれます。
4. デスクトップ、開いているすべてのファイル、およびアプリケーションが、休止に入る前と同じ状態で表示されます。

シャットダウン前に、作業中の状態とマシンの状態が保存されるという点で、この機能は他の方法よりも優れています。このような理由から、APCではこの方法をUPS電源管理ソフトウェアのシャットダウン方法として推奨しています。

スタンバイ

コンピュータは「スタンバイ」モードの状態であっても電源は完全には切断されません。コンピュータは一部のコンポーネント（モニタ、I/Oチップなど）への電力供給を停止した低電力消費状態になります。そのため、DRAMの更新などが継続的に行われ、コンピュータは「スタンバイ」モードから復帰すると、通常では、スタンバイモードに入る直前の状態に直ちに戻ります。使用するコンピュータでスタンバイモードを指定する場合、長時間の電源障害の発生時にシステムを正常終了できるように、選択したUPSでシステムをスタンバイモードから復帰することが重要です。システムがスタンバイ状態のままでは、最終的にUPSのバッテリが完全に消耗し、システムへの電源供給が完全に絶たれてしまう可能性があります（「ハード」シャットダウンの状態）。

最良の方法

√ 長時間稼動が可能なUPS／発電機を導入する

商用電源の信頼性に関する調査データは限られています。しかし、商用電源の信頼性について、それぞれ、AT&T ベル研究所とIBMによる2つの意義深い調査が米国で実施されています。

また、米国American Power Conversionでは、800万台におよぶUPSシステムの導入実績がありますが、これらのシステムのほとんどで電源障害が確認されています。米国での2つの調査結果はAPCの経験を裏付けており、以下に重要事項を整理します。

通常の環境で、ITシステムの故障原因となる電源障害の年間平均回数はおよそ15回です。詳細は以下のとおりです。

- 停電の90%は発生から5分未満で復旧（10%は5分以上継続）
- 停電の99%は発生から1時間未満で復旧（1%は1時間以上継続）
- 累積時間の合計では停電は年間100分に達する

この情報は停電の発生率が非常に高いフロリダなど、米国内でも、その地理的な位置や環境で大幅に異なります。さらに、建物自体の条件も加味すると、停電の発生率は最大で3倍にも跳ね上がる可能性があります。当該データは日本や西ヨーロッパにも当てはまるとみられます。

10%の停電が5分以上、1%の停電が1時間以上におよぶことから、ダウンタイムのコストが高い場合には、長時間実行可能なUPSか発電機、あるいはその両方の導入が得策であると考えられます。

√ ネットワーク機器をUPSで保護する

アプリケーションの可用性は、アプリケーションへのアクセスに使用するネットワーク機器の可用性かに左右されます。アプリケーションの可用性を確保する上で、ハブ、ルータ、スイッチといったネットワーク機器の電源保護が重要であるにもかかわらず、これらは見過ごされがちです。さらに、前述の構成3の方式でUPSのシャットダウンソフトウェアが実行されている場合、UPSのシャットダウンソフトウェアからの通信が正常に実行されるように、停電中でもネットワークは機能していなければなりません。つまり、ネットワークが保護されていないとコンピュータを正常終了することができません。

√ シャットダウンに必要な時間をサーバごとに確認する

オペレーティングシステムを正常にシャットダウンするために必要な時間はシステムによって異なります。たとえば、多くのアカウントが登録されている電子メールサーバにはシャットダウンまでに最大20分を要するものもあります。UPS電源管理ソフトウェアの設定時には、このようなコンピュータ特有の要件に配慮し、正しく設定してください。

結論

保護されたコンピュータであっても、シャットダウンソフトウェアがインストールされていなければ、UPSの働きは起こりうる結果を先延ばしするだけに過ぎません。いかなる構成や最良の方法を採用したとしても、またいかなる特定のUPS製品を使用したとしても、シャットダウンソフトウェアのインストールという要件を見過ごされることのないようAPCは強く提言します。シャットダウンソフトウェアをインストールし、構成することは、一見小さな取り組みですが、UPSの実行時間を超えるような長時間の電源障害が起きた場合には、このような小さな取り組みが大きな成果を実現します。

参考文献

『Monitoring of Computer Installations for power line disturbances（電源障害時のコンピュータのモニタリングについて）』、Allen/Segall共著、IBM、IEEE PES Winter conference、1974年

（1969～1970年の38ヶ月間のモニタリングデータを基に調査実施）

『The Quality of US Commercial AC Power（米国商用AC電源の品質）』、Goldstein/Speranza共著、ATT Bell Labs、Intellec conference、1982年

（1977～1979年に米国24ヶ所で調査実施）

『Power Quality Site Surveys: Facts, Fiction, and Fallacies（電力品質のサイト調査：事実、フィクション、誤った議論）』、Martzloff著、IEEE Transactions on Industry Applications、Vol 24、No 6

著者について

テッド アイブスは、製品ラインマネージャで、ウエストキングストンにあるAPC本社のデバイス管理部門に勤務しています。APCのネットワーク管理カードとPowerChuteソフトウェア製品を担当しています。