blancco
technology group

WHITE PAPER

クラウドおよびデータセンターにおけるデータ消去

- 適切なデータ消去 -

適切でないデータ消去

企業のサーバーまたはその他のITインフラストラクチャから機密データを削除しなければならない場合が数多くあります。しかし、削除されたデータは本当に消えているのでしょうか？　サイバー攻撃者がアクセスすることはできるかもしれません。単なる削除ではデータは永遠になくなるわけではありません。　認定されたデータの消去がビジネスにとって不可欠です。それは、最も機密性の高い機密データの整合性を保護し、それが悪意のある人にわからないようにするためです。

2014年11月にソニーはサイバー攻撃で100テラバイトのデータを失い、その後、同社はずさんな記録管理について多くの批判を受けました。　最も有害なファイルには、スタジオの幹部間での何万もの電子メールが含まれており、これがソニー・ピクチャーズの内部の仕組みを露呈させ、大衆とメディアの間で深刻な反発を招きました。　企業のサーバーから電子メールが定期的に削除されていれば、ソニーはそのような否定的な意見や企業の評判の深刻な損害は生まれていなかったでしょう。

一般的なファイル削除コマンドは、データを本当に削除するわけではありません。　データが存在するディスクセクタへのポインタを削除するだけです。　このような「削除された」データは、一般的なソフトウェアツールを使って簡単に復元できます。　そのため、多くのCIOやITプロフェッショナルは、これから発生するセキュリティ上の危険性を認識していますが、常に正しい予防策を講じているとは限りません。

従業員記録や顧客情報、また、知的財産など、ほんの数例だけでも、膨大な量の機密データがデータセンターとクラウド環境の両方に保存されています。　データ侵害が発生するか否かが問題ではなく、それはいつか発生するという問題です。

これは、eBay、Home Depot、Texas Health and Human Servicesなど、顧客を失った小売業者、ヘルスケアプロバイダー、金融機関、さらには政府機関の数を見ると明白です。

そして、米国政府の人事管理局（OPM）による8億の社会保障番号の最新の違反も重要です。　管轄区域、国境、国境を越えて、規制当局はセキュリティ違反に対する監視と罰金の両方を増やしています。　そして、消費者から企業、政府機関に至るまで、顧客は組織がデータをどのように管理しているかについてより注意を払っています。

単なるデータ削除だけでは、もはや不十分です。　必要なのは、機密情報を完全に消去して消去を検証できるエンタープライズクラスのソフトウェアによって達成される、認定されたデータの消去です。　認定されたデータ消去は、組織が独自のデータセンターを運用したり、パブリッククラウドにデータを保存したり、他の企業にクラウドベースのデータストレージを提供したりする場合でも、強力なエンタープライズセキュリティに対する増大する要件を満たします。

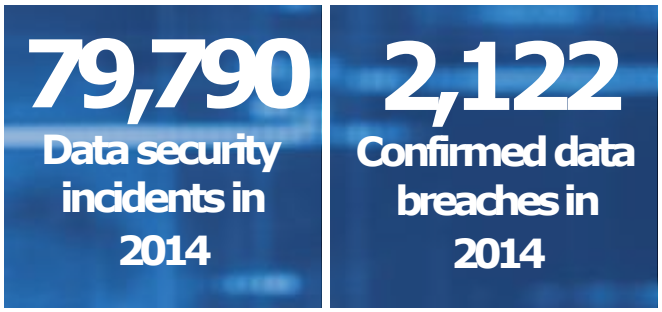
効果的なデータ消去管理（Data Erasure Management: DEM）には、ITセキュリティ戦略全体に適合し、データとブランドを保護するのに役立つ、綿密に計画された信頼できるDEMソフトウェアを活用した自動化アプローチが必要です。その方法は次のとおりです。

消去に対しての競争

多くの企業は、特定のデータを消去する必要性を長い間認識しています。　しかし、一部の企業は、データ消去管理を、ITインフラストラクチャ全体およびデータセキュリティポリシーの不可欠な要素として見落としています。
しかし、以下に概説するいくつかのイベントにより、それは変化し始めています。

サイバー攻撃:

データの侵害は誰もが標的にされたています。
実際に、2014年に79,790件の文書化された情報セキュリティインシデントと2,122件のデータ侵害があったとVerizonにより確認されています。
さらに恐ろしいことは、これらの攻撃は洗練されたプレイヤーによって、より一層行われているということです。
ソニーの侵害の背後には北朝鮮政府がいるとされ、また、中国政府は2015年春に米国内国歳入庁（IRS）から400万人の米国納税者の記録を盗んだと非難されています。

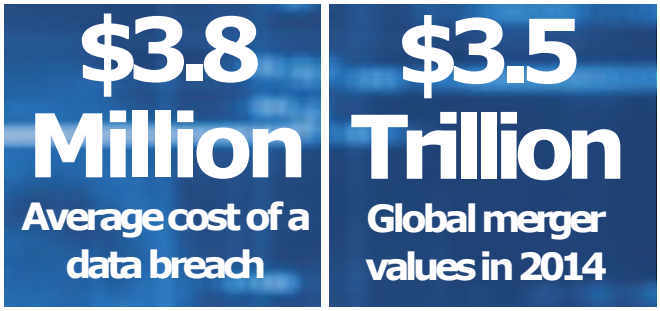


Source: Verizon

また、盗まれたデータの経済的負担が高まっています。Ponemon Instituteが報告しているように、データ侵害の平均コストは2014年に380万ドルであり、1レコードあたり約150ドルになります。

これは2013年から23パーセント増加しています。

この失われたデータの根本的な原因は、
人的ミス（25%）、
犯罪行為（47%）　です。



Source: Ponemon Institute

規則：

データ侵害に直面して、
政府は規制を強化しています。
カリフォルニア州や
マサチューセッツ州など、米国の州と同様に、少なくとも75カ国にデータ保護法があります。

企業は、SOXおよびHealth Insurance Portability and Accountability Act（HIPAA）からペイメントカード業界データセキュリティ基準（PCI DSS）まで、一般および業界固有の規制とガイドラインの両方に準拠する必要があります。

2015年に提案された政権の消費者プライバシー権利章典では、業界がデータに関する行動規範を確立し、米国連邦取引委員会（FTC）の監督下にあるプライバシー委員会を作成することを義務付けていました。

また、2017年には欧州連合（EU）は1995年のデータ保護指令の見直しを完了し、いわゆる「忘れられる権利」やデータ記録からの消去などの市民の権利を強化しています。

さらに重要なのは、サーバーがEUの外にあったとしても、EU市民データを処理するクラウドサービスを持つ企業には規則が適用されるということです。

その他の関連ガイドラインには、国際標準化機構（ISO）および国際電気標準会議（IEC）によって発行されたISO / IEC 27001およびISO / IEC 27040が含まれます。 これらの規格では、再利用または廃棄前の記憶媒体の上書きなど、データの保護方法に関する規則が定められています。

また、これらの規格はG-Cloudなどの政府調達取引所への参加を希望する企業に対する規則や認定資格になることもあります。

FedRAMPプログラムを通じてクラウド環境を活用したいと考える米国の機関にも同様の規則があります。

企業の統合:

企業の買収、売却、および適切なサイジングにおいても、データ消去への関心を高めています。

Thompson Reutersによると、2014年の世界規模の合併額は、2013年比で47%増の3兆5000億ドルを突破しています。

企業が合併すると、データセンターも統合され、物理的および仮想のITリソースの移動、または廃止されたときに、データが保護や消去されていることを証明する必要があります。

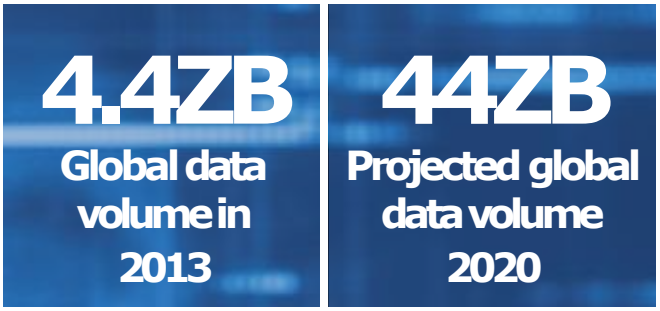
データの増加：

データ消去の必要性の最も重要な要因の1つは、データの爆発的な増加です。

世界のデータ量は、2013年の4.4ゼタバイト（ZB）から、2020年には44ZBに急増するとIDCは予測しています。

44兆ギガバイトという驚異的な数字です。

それらのデータはクラウドやデータセンターに存在します。



Source: IDC

仮想化：

データの増加などの要因により、企業はクラウドと仮想化を推進しています。Ciscoによると、2018年までにクラウドで4分の3以上のサーバーワークロードが処理されると予測しています。

データセンター全体のワークロードは2013年から2018年の間にほぼ2倍になり、クラウドのワークロードは約3倍になります。

高度な仮想化を反映して、クラウド内の物理サーバーあたりのワークロードは5.2から7.5に増加するでしょう。

仮想マシン（VM）が移行され、廃棄する際には、関連するすべてのデータをホスト元の物理サーバーまたはストレージから消去する必要があります。 また、VMには物理サーバーと同じレベルのセキュリティが必要です。しかし、VMの消去には、同じハードウェア上で実行されている他のアクティブなVMに影響を与えてしまうことなく、消去を実行するという技術的な課題があります。

Now You See It, Now You Don't

データ消去管理（DEM）は多くの企業にとって目新しいものですが、データライフサイクル全体における、「作成→保存→使用→編集→消去」という一般的な構成要素のひとつです。

どのようにデータを消去するのかと言う、データライフサイクル全体を考慮せず、データを作成するべきではありません。

これは、データが存在しうる全てのITインフラ上（物理サーバー、仮想サーバー、物理ディスク、論理ドライブ、さらにはPC、ラップトップ、タブレット、スマートフォンなど）において言えることです。

データの消去は、ITインフラの種類に関係なく必要です。

あなたの会社は、以下のいずれかの状況に当てはまりませんか？

- 独自のオンプレミスデータセンターを運用
- 占有データセンターを扱うサービスプロバイダーの利用
- コロケーションデータセンターの利用
- パブリッククラウドへのデータ保存
- 一部のリソースを外部に配置するハイブリッドクラウドの利用
- 物理的環境と仮想環境の任意の組み合わせ

クラウドとデータセンターの両方において、データ消去が必要となる5つの重要な背景があります。

ここではそれぞれの概要を説明します。

機器のEnd-of-Life：

サーバー、ストレージデバイス、その他のIT資産が償却されると、転売または廃棄されます。

どちらの場合も、そのIT資産に含まれているデータは、すべて消去される必要があります。

データ移行：

データがある場所から別の場所に、つまり、"老朽化したサーバーから新しいサーバー"に、"ある仮想マシンから別の場所"に移動されるたびに、元のデータの場所を消去する必要があります。

情報のEnd-of-Life：

多くの企業は、キャンペーンなどのプロジェクトのために、特定期間をカバーする仮想マシンをその業務で利用します。

プロジェクトが完了したら、仮想マシンを削除するだけではなく、そのマシンに存在する情報を完全に消去しなくてはなりません。

クラウドプロバイダーとデータ消去

企業が自社のIT環境をクラウドプロバイダに引き渡す時、企業の多くはクラウド上の彼らのデータは自社環境と同じく、保護されたままであると考えています。しかし、使用中のデータが安全であることだけでなく、仮想環境からすべての使用済みデータが完全に消去されていることを確認する必要があります。

それが故に、クラウドプロバイダーが、データ消去という新たなサービスをSaaS、もしくはIaaSとして提供し始めています。

クラウドのお客様が、仮想マシンまたはvAppを削除すると、 VMware ESXi、vCenter Server、Microsoft Hyper-Vなどの一般的なソリューション上で、適切なデータ消去管理ソフトウェアを導入しているクラウドプロバイダでは、ホストレベルで安全に消去されます。

特定の仮想マシンをデータストアにグループ化しているクラウドプロバイダーにおいては、効果的なデータ消去管理ソフトウェアは、論理ユニット番号と同じようにデータストア全体を消去できます。

顧客からのデータ消去要求:

EUなどの管轄区域では、「忘れられる権利」規則により、消費者からデータを削除するよう求められた場合は、それに従う必要があります。単にレコードを削除するだけでは、消費者からの再三の要求に頭を悩まされ、不十分かもしれません。

適合な消去が行われたことを証明するために、認証されたレポートを含む監査証跡が存在しなければなりません。

災害復旧後:

大規模な災害時には、データはディザスタサイトにおいて一時的に回復されます。実際の顧客データがテストで使用される障害回復演習でも同じことが言えます。

どちらの場合でも、本番システムの復旧後にリカバリディスクに残っているデータはすべて消去する必要があります。

セカンダリサイトからデータを消去することが重要です。

多くの企業は、データを暗号化しておけば保護されているため、これらの移行時点ではデータの消去は必要ないという、誤った認識をしています。

しかし、暗号化はデータの保護には効果的ですが、暗号化キーは盗まれる可能性があり、暗号化されたデータを復号することができます。「inside job」が現実的に存在することを常に忘れないでください。

データへの侵害に気づくのに数週間または数ヶ月かかることがあります。

Verizonによると、カードスキマーによるカードの不正利用の場合、36%が数日で発見され、18%は数週間かかり9%は数か月にかかるということです。

適切なデータ消去管理ソリューションの検討

ファイルの削除がファイルの消去と同じではないのと同じように、あらゆるデータ消去管理（Data Erasure Management:DEM）ソリューションが同じ仕組みではありません。効果的なDEMソリューションは、次の機能と利点を提供します。

コンプライアンス：

DEMソリューションは、機密データの保護と法令遵守の両方を保証するための、データ消去に関するすべての主要な国際政府および業界標準を満たすことが認定されている必要があります。

レポート：

監査にあたり、改ざんが不可能な消去レポートを発行して、重要な移行点でデータが完全に消去されたことを証明するレポートが必要です。レポートには、シリアル番号、仮想マシン名、LUN IDなどの特定のハードウェアの詳細、および実際の消去プロセスを実行した人とそれにかかった時間が表示される必要があります。

汎用性：

優れたDEMソリューションは、ファイル、ディスク、論理ユニット番号、サーバー、仮想マシン、およびストレージシステムからデータを消去するための監査可能なプロセスを提供する必要があります。

自動化：

最後に、ソリューションは、組織のニーズに合わせた消去の自動化を提供する必要があります。セルフプロビジョニングを実行している内部の従業員が仮想マシンまたはLUNを消去できなかった場合、データは脆弱になります。 忙しいIT管理者がサーバーを正しく消去できなかった場合、あなたのデータは危険にさらされてしまうためです。消去の自動化により、確実に情報資産が確実に保護されるようになります。

違反が検出されない時間が長くなればなるほど、暗号化されたデータが危険にさらされるようになります。

データ消去管理は、データセキュリティに対する包括的で絶対的な防御方法の不可欠な要素になります。このアプローチによって、ファイアウォール、ウイルス対策、データの暗号化などのセキュリティ対策に、データの消去という保護層が追加されます。

攻撃がファイアウォールを通過すると、ウイルス対策ソフトウェアがそれを検知する可能性があります。

マルウェアがウイルス対策を回避した場合は、データの暗号化によって漏洩を防ぐことができます。

不要なデータについては、使用済みデータが完全に消去されるデータ消去管理導入した場合、攻撃者が盗むことができるデータはそこには存在しません。

ディスク消去

ディスク消去は、ストレージエリアネットワーク（SAN）から解放されているドライブと同様に、ホスト外のディスクをサニタイズするために必要で、搬送経路によるリスクの懸念により、現地ローカルでのデータ消去が必要です。また、解放されているドライブを消去するには、外部のホスト/ブートデバイスと、ドライブとホスト間の接続が必要です。

シナリオは次の通りです。

返品許可（RMA）保証ドライブ：

故障したディスクを消去すると内容が削除されるため、ドライブをOEMに返送して保証交換することができます。

データ消去は、OEMではなくデータセンターが担当します。

ドライブのバックログ：

過去に使用済みドライブの消去が行われたことがない場合、データセンターに消去が必要な廃棄ドライブの在庫がある可能性があります。

サービス終了サーバー用のドライブ交換：

解放されているドライブを交換することは、サニタイズ前のドライブを使用しているサーバーの廃止を促進する一般的なプロセスです。 しかし、それは損なわれていないデータを持つドライブを解放することになります。

効果的なデータ消去ソフトウェアを使用すると、接続されているすべてのドライブを高速で同時に消去できます。 ディスクレベルで消去アプライアンスから実行して、管理者によって指定されたRMAドライブからデータを削除できます。管理者は、さまざまな消去標準から選択できます。

（図1参照）

The process should take about one minute per gigabyte to simultaneously erase SCSI, SAS, STAT, Fibre Channel (FC)

SCSI、SAS、STAT、ファイバチャネル（FC）、およびIDE/ATAドライブを同時に消去するには、1 GBあたり約1分かかり、また、SSDにも対応する必要があります。

消去ソフトウェアは、消去レポートを管理コンソールまたは資産管理データベースに自動的に送信します。

その後、コンソールはレポートを検証し、消去を確認してレポートを保存します。

Blancco Drive Erase （サーバーの消去）

Blancco Drive Eraserは、内部接続されているすべてのドライブの消去が可能です。

ローカルまたはリモートで消去を実行でき、利便性が高いです。

また、ハードウェア属性とデータ消去に関する監査可能なレポートを発行することも可能です。

また、ディスクの保護された領域と再マッピングされたセクターを検出し、消去できないものにフラグを立てます。

そしてそれは、シリアルATA、SAS、SCSI、FCディスクのような広範囲のハードウェアのデータ消去が可能です。

ディスク消去シナリオ:

図1. 解放されたドライブの消去

サービスの終了:

ハードウェアのサポートが終了すると、データセンターはデータを保護し、規制を遵守するためにサーバー/ストレージアレイのすべての情報を安全に消去する必要があります。これにより、健全なディスクのリサイクルまたは再販が可能になり、「グリーン」オペレーションと利益の両方が促進されます。

ホスティング契約の終了：

既存の顧客がホスティングサービスを終了したときに、ホスト環境でサーバーを再利用するには、消去が必要です。

データセンターの再配置：

データセンターは頻繁に移動または拡張するため、安全に消去しないとサーバーの移動が必要になり、転送中にデータが失われる可能性があります。

リース終了：

ハードウェアのリース終了時に、ストレージシステムをリース会社に返送する前にデータを消去する必要があります。

サーバー消去では、管理者はCDまたはUSBから、あるいはネットワーク経由で消去ソフトウェアを起動します。 （図2を参照）

ソフトウェアはドライブを識別し、消去を実行した後に、管理コンソールまたはメモリースティックにレポートを送信します。

Blancco Drive Eraseは、x86サーバーとx64サーバー、さらにRAIDサーバーと非RAIDサーバーを消去します。 内蔵RAIDコントローラを搭載したサーバーの場合、ソフトウェアはRAIDを「破壊」し、すべての内蔵ドライブを管理者が選択した消去規格まで消去する可能です。 また、SPARCアーキテクチャ上でもデータ消去が可能です。

File Erasure

多くのデータセンターは、冗長性のために同じデータを複数コピーし、保存しています。 PCI DSSなどの規格では、特定の間隔でファイルレベルのデータの削除を要求しているため、ネットワーク上で対象ファイルや重複ファイルを消去するための集中管理された方法が必要です。 Windows分散ファイルシステム（DFS）環境では、アップタイムを維持するために、データの消去を冗長システムとミラーシステム間で同時に実行する必要があります。 ほとんどの場合、消去ツールはサーバーノードレベルでは見えないはずです。

ファイル消去シナリオ:

図2. リモートでのサーバー消去

PCI DSS コンプライアンス:

PCI DSSにおいては、クレジットカード情報は、5年以上保存するべきではありません。 この場合、時間またはイベントごとに特定のファイルをターゲットとする消去ソリューションが必要です。

データ整理：

ファイルの消去はデータ全体のメンテナンスの一部であり、冗長データが不必要に保存されないようにするため、ITコストとデータ盗難の可能性が増大する可能性があります。

データ流出：

機密データが、許可されていないシステムまたはアプリケーションに誤ってコピーされる可能性があります。 そのデータは単に削除されるのではなく、完全に消去されなければなりません。

効果的なデータ消去ソリューションは、時間またはイベントごとに、または管理者によってフラグが立てられたときにファイルを破壊する可能性があります。 （図3を参照）

管理者は、中央のインターフェースからどのルールと保存領域を適用するかを選択します。

このツールでは、監視を完全な制御のためのサービスとして許可し、すべての消去アクティビティをログに記録する必要があります。

また、すべてのWindowsまたはUNIXの削除コマンドを置き換えることができます。
管理者がネットワーク上の場所に関係なく特定のファイルを消去できるように、MicrosoftのWindows Serverのファイル分類基盤（FCI）や他の文書管理システムとの互換性もあります。

LUNの消去

データセンターは、仮想ストレージシステム構成を再構築せずに安全に再利用できる必要があります。
これを実現するには、ストレージアレイをオフラインにできないアクティブな環境で、論理ユニット番号（LUN）などの論理ドライブを消去できる集中管理ツールが必要です。
LUNの消去は稼働環境を保って行われるため、ダウンタイムは発生しません。
そのため、消去作業によってデータセンターの生産性が低下することはありません。

LUNの消去は、LUNが構成されているオペレーティングシステム、またはターゲットのLUNを表示して複数のユニットを同時に消去できる外部接続サーバーから実行されます。
LUNの消去は、米国国防総省などの政府機関と取引を行う企業にとって非常に重要です。
LUNを消去する機能がない場合、ストレージアレイ全体を取り外して物理ドライブを消去する必要があります。
LUN消去のシナリオ：

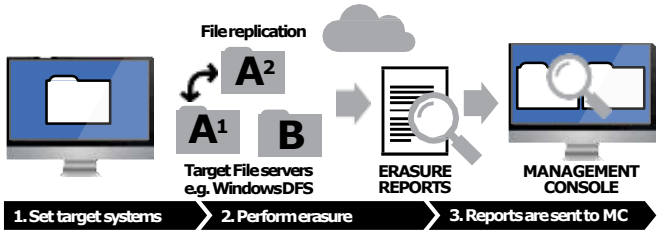


図 3. ファイルレベルでの安全なデータ消去

LUNのホスティング、削除、または移行の終了：

ユーザーがLUNを大規模に移行したり、クラウド利用を終了した際には、LUNを再利用するにあたり、ホストでの消去が必要です。そうすることでLUNを安全に新しいユーザーに再割り当てることが可能になります。

これは、ストレージとしてLUNを使用する物理サーバーと、特定のLUNに専用のストレージを持つVMの両方に当てはまります。

災害復旧テスト:
惨事復旧テストの後、LUNデータの重複コピーを消去する必要があります。
データ消去ソリューションは、中央のインターフェースからソフトウェアの並列インスタンスを起動することによって、複数のLUNの同時破壊をサポートする必要があります。
（図4参照）

ソフトウェアは、Windows、UNIX、またはLinuxシステムが論理ディスクまたはドライブ上の書き込み可能領域全体をセクタ単位で上書きすることによって検出できる物理または論理ユニットを消去する必要があります。

仮想化環境の消去

ビッグデータが増加し、VMware vSphere、Citrix XenServer、Microsoft Hyper-Vなどの仮想化環境へ移行するにつれて仮想化環境上のデータを消去する必要がでてきます。 データ消去ソリューションは、データセンターの運用や事業活動に影響を与えずに、データの上書きを実施する必要があります。 他の仮想マシンや物理ホスト上のアクティビティに影響を与えることなく、アクティブ環境の仮想マシンを消去することが必要です。
仮想マシン消去シナリオ：

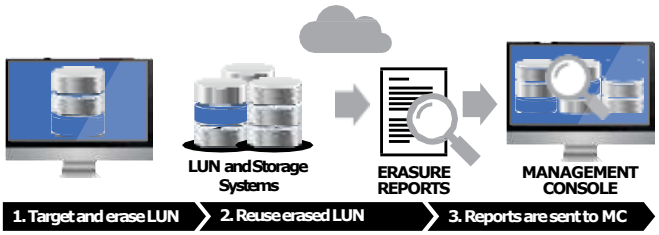


図4. アクティブ環境でのLUNの消去

VMware vCenter Serverとの統合：

VMWare vCenter Serverは、VMwareベースのデータセンターで物理ホストサーバーとVMの両方を管理するための標準ツールです。
管理者が仮想マシンを右クリックしてデータストアから消去できるように、消去ソリューションをvCenterと統合する必要があります。

ESXiプラットフォームでのVMのホスティング、削除、または移行の終了：

VMが削除されたり、データセンター内の場所が変更されたりした場合は、VMを的確に消去する必要があります。
ホストを再起動せずにこれを達成できるはずです。
消去ソリューションをVMware ESXiレベルでインストールすることで、VMware vSphereのVMを手動で消去できます。
VMDK、VMSD、VMX、VMXFなど、ターゲットのVMに関連付けられているすべてのファイルを消去する必要があります。

VM Ware vCloud Director上のVMのホスティングの終了、削除、または移行：

VMware vCloud Directorを介してアクセスされたVMは、多くの場合、データセンター内で削除または移行されます。

vCloud Directorユーザーインターフェイスを介したシームレスな統合とアクセスにより、「delete」コマンドを使用して、アクティブシステム内のVMまたはvApp上のすべてのデータを破棄できます。

自社開発ポータルからの消去：

VMware ESXiホストを実行しているユーザーは、vCloud Directorの代わりに自社開発のポータルを使用してVMを展開することがよくあります。

この場合、Blancccoのデータ消去ソフトウェアをESXiホストにインストールし、自社開発のポータルから実行することができます。

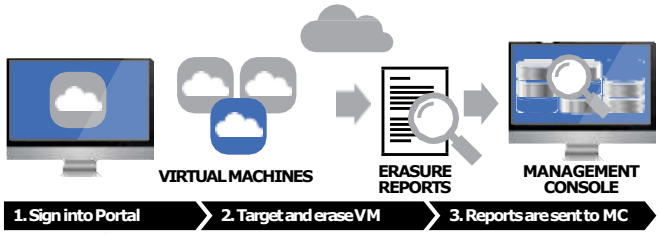


図 5. 仮想環境のデータ消去

最終見解

急増する仮想環境やクラウド環境の管理、複数の政府規制へのコンプライアンスの認識、データ漏洩に対する顧客情報と知的財産の保護を効果的に、データ消去によって強化することができます。

また、データ消去の提案により、ビジネスを拡大する企業は多岐にわたります。

グローバルなワイヤレスディストリビュータは、仮想マシンの効果的な廃棄を確実にするためにデータの消去に目を向けました。

米国の主要な通信プロバイダーは、連邦政府とのビジネスクリティカルな契約を維持するための消去ソリューションを導入しています。

また、ヨーロッパの大手データセンタープロバイダは、データの消去を競争上の差別化要因として活用し、新規顧客の獲得につなげています。

米国の大手ITプロバイダは、データ消去管理の優位性を提案し、ITインフラの保護を航空宇宙業界のリーダーに提供しています。

サイバーセキュリティ、ITインフラ管理、政府の規制、および顧客の期待に対する評価の変化が、企業データの保護に新たな負担をかけています。

また、データ消去管理は、データ資産の保護、ブランドの保護、およびビジネスの成功に向けた企業の位置付けなど、データセキュリティに不可欠な要素となってきています。