物理破壊 vs. 安全なデータ消去

データセンターやストレージクローゼットの近辺に、ハードディスクドライブ(HDD) やソリッドステートドライブ(SSD)が山積みになっていませんか？これらのドライブには多くの機密データが含まれているはずです。そのため、これらドライブからデータを復元できないよう直ぐにデータ消去を実施しないと、ビジネスにとってリスクになることがあります。

これらドライブはサードパーティの IT 資産処理ベンダーに回収と破壊を依頼することもあれば、施設内で破壊することもあると思います。どちらにおいても、ライフサイクル が終了したデータを保護する唯一の手段は物理破壊だけではありません。

ソフトウェアによるデータ消去も選択肢の一つです。データ消去は、データサニタイズを実現し、さまざまなデータ保護規制対応に役立ちます。

SSD の消磁と細断によるリスク

消磁はドライブの物理破壊において最も安価で簡素な手段です。消磁により、不要になった磁場を減少・排除することで、データを除去できます。しかし、SSD は磁気的にデータを保存していないため、消磁ではデータサニタイズは達成できません。

また、物理的な細断も、細断サイズが問題となります。NSA(米国家安全保障局)は、メモリチップからデータを安全に除去するには、2mm 以下のサイズに裁断することを推奨しています。しかし、一般的な業務用のシュレッダーの細断サイズは、2mm よりも大きい断片となっており、メモリに保存されたデータはそのままになります。

さらに、物理破壊では細断された IT 資産の残骸が、環境に対して有害になってしまうことがあります。IT 資産を再利用できれば、環境への配慮、そして新しいストレージデバイスの購入に必要なコストを削減できます。

データ消去によるリスク低減

データ消去はストレージデバイスのすべてのセクターに、0 と 1を使ってデータを安全に上書きするソフトウエアベースの手法です。ストレージデバイス上のデータは、上書きにより復元できなくなります。データ消去ソフトウエアは、消去プロセスの最後にデバイスのすべてのセクター上で適切に上書きが実施されたかを検証します。またデータ消去後には、監査証跡となる改ざん防止の証明書を生成します。これにより、データサニタイズを実現したことになります。また、データ消去はオンサイトもしくはリモートから実施でき、その他のデータ消去手法より高い管理性を提供します。さらに、プロセス自動化による作業時間の削減も可能です。

データが適切に上書きされたことを確認する検証プロセスと、消去後に自動生成される消去レポートにより、ソフトウエアによるデータ消去はデータサニタイズを達成するベストな手法と言えるでしょう。さらに、ソフトウェアによるデータ消去は環境に配慮した取り組みとなり、ストレージデバイスの再販価値を損なうことはありません。

Blancco Drive Eraser は、安全なデータ消去を実現し、組織は SSD および HDD の安全な再販、再利用、廃棄が可能です。

特許を取得した SSD 消去による簡素化されたプロセス

Blanccoの SSD 消去方式は特許を取得し、さまざまな SSD ベンダー間の機能の差異を吸収できるよう、、次のようなことが含まれた特別に設計になっています。

- SSD 本体がサポートするセキュリティプロトコルを使用するマルチフェーズ、そしてプロプライエタリの 消去アプローチ
- システム BIOS のフリーズロック解除とSSD内部のセキュリティ機能へのアクセスを自動化
- SSD 内部の消去プロセスの誤検知を排除するプロシージャ
- 第三者による診断と検証
- 実施した消去の証明と規制対応のための包括的な改ざん防止の消去レポート

HDD と SSD の消去に Blancco Drive Eraser を選択する理由

- 組織内の IT 管理者によるデータ消去を実現し、機密データが悪意のある第三者の手に渡ってしまうリスクを軽減
- 監査証跡となる改ざん防止の消去レポートの提供
- ソフトウエア消去によるドライブの再利用およびコスト削減
- ソフトウエア消去よる物理破壊のコスト削減
- 複数ドライブの同時消去による業務効率化
- ISO 27001 および ISO 27040 を含む、地域、国家、そして世界的なデータ保護規制・ガイドラインに準拠

Blancco Drive Eraser について詳しく知りたい方は、無償トライアルをお申し込みください。