KINGSTON IRONKEY™

ハードウェアベース vs ソフトウェアベースの暗号化

主な違いを理解し、自分のニーズに合った最適なオプションを知る

データセキュリティに関する終わりのない戦いにおいて、ハードウェア暗号化とソフトウェア暗号化の違いは、セキュリティがどこに組み込まれ、実際の使用環境においてどれだけ危険にさらされるかに集約されます。暗号化機能が組み込まれている USB ドライブと SSD は、データがどれだけ安全に保護されているか、そしてそれが周囲のシステムにどれだけ依存しているかを決定します。

ハードウェア	VS	ソフトウェア
暗号化キーの処理 暗号化キーは、ハードウェア内部で生成され、ドライブ内に安全に保存されます。		**暗号化キーの処理** ユーザーのパスワードは暗号化キーとして使用され、暗号化キーはシステムメモリ内に保存されます。
総当たり攻撃の防止 総当たり攻撃を防ぐために、一定回数の以上の試行が行われるとドライブが自動的にデータを消去するよう設計されています。これにより、ドライブが紛失したり、盗難されたりした場合でも、機密データが漏洩することはありません。		**総当たり攻撃の防止** ブルートフォースアタックの影響を受けやすい場合、コンピュータは入力の試行回数を制限しますが、ハッカーはコンピュータのメモリにアクセスして試行カウンターの値をリセットすることができます。
ソフトウェアまたはドライバの要件 ホストシステムにドライバやソフトウェアをインストールする必要はありません。		**ソフトウェアまたはドライバの要件** ソフトウェアやドライバのインストールが必要で、オペレーティングシステムとの互換性は状況に応じて異なります。
暗号化リソース ドライブ自体に組み込まれた専用の暗号化プロセッサを使用します。		**暗号化リソース** ホストコンピュータの CPU とシステムのリソースを使用して、データを暗号化および復号化します。
ホストシステムの依存性/脆弱性 セキュリティ機能はデバイス内部で独立しており、信頼できないコンピュータやウイルス感染したコンピュータに接続した場合でも保護された状態を保ちます。		**ホストシステムの依存性/脆弱性** セキュリティはホストオペレーティングシステムに依存し、コンピュータがマルウェアに感染するとリスクが高まります。
暗号化の状態 設計上、暗号化は常時有効になっており、削除したり回避したりすることはできません。		**暗号化の状態** 暗号化は有効にしたり、無効にしたりでき、設定ミスが起こる可能性があります。
パフォーマンスへの影響 暗号化処理はハードウェアプロセッサ側で処理されるため、パフォーマンスへの影響は最小限に抑えられます。		**パフォーマンスへの影響** 暗号化が CPU のリソースと共有されるため、パフォーマンスに悪影響を及ぼす可能性があります。
複数のフォームファクタに対応する 暗号化は、特定の USB または SSD ドライブに関連付けられます。		**複数のフォームファクタに対応する** ほとんどすべてのストレージメディアに実装可能です。

ソフトウェア暗号化は柔軟性がありますが、ハードウェア暗号化はセキュリティ機能が独立して機能し、システムレベルのリスクを軽減します。2 つの暗号化のデータ保護方法とアクセス制御方法をを理解することで、ワークフローとリスクプロファイルに最適なセキュリティレベルを選択できます。

www.kingston.com/ironkey