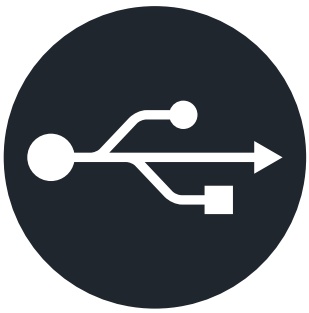
エンドポイントセキュリティ対策で 妥協をせずに

# USB ドライブへのアクセスを許可する

#KingstonIsWithYou #KingstonIronkey

# はじめに

1996 年 1 月にリリースされた公式 USB 1.0 仕様は、周辺機器ベンダーとエンドユーザーにとって同様に均一性、利便性、多用途性の新時代の到来を告げるものでした。27 年後も、USB は各リビジョンとの下位互換性を維持し、サーバーからスマートフォンに至るまでコンピューターハードウェアインターフェイスの基礎として存続しています。



USB のプラグアンドプレイのシンプルさと速度の向上により、USB ポータブルストレージは普遍的なストレージの 1 つとして進化しました。しかしこのような利便性には、データセキュリティ面で代償が伴います。今日の世界では、ホストコンピューターのエンドポイント保護や適切なデータセキュリティの実践など、適切なツールを使用する必要があります。ポータブル USB ストレージの使用に対して無頓着なユーザーは、エンドユーザーに損失を与え、組織や政府全体を危険にさらす可能性のあるデータ侵害に、自分自身や他人をさらすことになります。

ホスト環境の保護に加えて、USB ドライブはパスワード保護とオンデバイスのハードウェア暗号化によって保護される必要があります。これにより、非常に堅牢な侵入対策ができます。USB ドライブをより安全に使用するためのベストプラクティスをいくつか紹介するとともに、USB ドライブ全般について詳しく説明します。

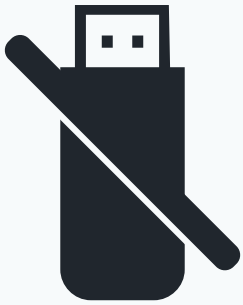
組み合わせたアプローチが理想的ですが、最も重要なのは暗号化の堅牢性と USB ドライブ自体のハードウェアコンポーネントです。これらの機能は金融から、医療、製造、国防まで幅広い分野で有用です。また、ネットワークアクセスが利用できないか、脆弱であるか、非実用的であるリモート作業でも役割を果たします。

USB ハードウェア暗号化ドライブは、さまざまな認証評価で利用可能であり、さまざまなセキュリティ機能を提供します。それらの属性とカスタマイズの機会を調査することにより、あらゆる種類の機密性の高い環境で地位を確保しているため、スタンドアロンソリューションとしての適合性もより明確になります。

# ポートオーソリティ：USB ストレージとエンドポイント管理データ損失防止ソフトウェアの出会い

何十年にもわたって、ウイルス対策およびマルウェア対策アプリケーションは、ダウンロードと接続されたデバイスを自動的にスキャンし、疑わしいコンテンツを報告または処理するという、最も基本的なレベルでの保護を提供してきました。次世代アンチウイルス（NGAV）ソフトウェアによる保護は、ここから一歩前進しています。NGAV は、継続的に更新されるウイルスのシグネチャのデータベースだけに依存するのではなく、未知の脅威を特定して軽減できる機械学習機能と動作検出機能を追加します。

しかし利用できるツールはこれだけではありません。ユーザー周辺機器などからの攻撃に対する対策が必要な方には、USB ポートなどのアクセスポイントへあらゆる種類のアクセスを拒否できる、エンドポイント管理データ損失防止（DLP）ソフトウェアがあります。



「すべてのポートをブロック」するセキュリティに対する姿勢は確かにリスクを排除することができ、状況によっては望ましい場合もありますが、そのようなポリシーは多くの場合、望ましくない結果をもたらす非常に鈍い手段であることが判明する可能性があります。

しかし、一部の IT 管理者は、ユーザーマシンで USB ポートを開く要求を拒否することを好みます。これは、これらのエンドポイントで USB ポートを開くと、エンタープライズファイアウォールを介した直接アクセスが可能になるためです。このような注意は理解できますが、USB ストレージへのアクセスを有効にする場合、特定の前提条件が守られていれば、この権限を与えることがセキュリティ上の大きな問題になる必要はありません。

必須の要件は、アンチウイルス／アンチマルウェアソリューション上で脅威検出スキャンを行う機能や、すべてのユーザーエンドポイントを中央で監視・管理できる機能のあるエンドポイント管理アプリケーションスイートです。

通常、このような基本的なアプローチはさまざまな形で、McAfee MVision、Sophos Intercept X、Symantec Endpoint Security、Trend Micro Smart Protection、WinMagic SecureDoc など多くの人気ベンダの統合ソリューションに実装されています。

# ホワイトリストの細かい調整


USB ストレージデバイスのセキュリティを確保する場合、利用する方法は必要な保護レベルによって異なります。シンプルでありながら効果的なアプローチには、各ベンダ ID（VID）と製品 ID（PID）の値を活用して、USB ストレージデバイスをホワイトリストに入れる方法があります。すべての USB 周辺機器について言えることは、各メーカー固有の VID は一定ですが、PID は新製品がリリースされるたびに変わるということです。

ホワイトリストの場合、メーカーの VID のみを使用すると、そのメーカーがこれまでに製造したすべての USB デバイスが許可されるため、セキュリティを確保するには範囲が広すぎます。PID はそれをさらに絞り込み、特定のモデルのみにホストシステムへのアクセスを許可することを要求します。

これは改善ではありますが、まだ理想的ではありません。USB ストレージデバイスが広く普及しており、認可されたモデルと一致するデバイスをユーザーが自分用に購入できるためです。これらのことを念頭に置き、Kingston Technology は USB ストレージデバイスのセキュリティを強化するためのオーダーメイドのソリューションを提供します。

カスタマイズプログラムを通じて利用できる、組織に固有のカスタム PID プロファイルを作成し、さまざまな Kingston 暗号化 USB フラッシュドライブに適用できます。カスタム PID の付いたデバイスを展開する企業は、ホワイトリストを簡素化できるだけでなく、セキュリティを大幅に強化することもできます。一致するカスタム PID がない場合、従業員が独自に購入した一見同一のデバイスであってもアクセスが拒否されます。

カスタム PID を使用すると、IT 管理者は新しい USB ストレージデバイスを迅速かつ簡単に稼働させることができますが、より詳細な代替方法は、ほとんどの Kingston 暗号化 USB ドライブに搭載されている個々のデバイ

スのシリアル番号を使用することです。この設定には、エンドポイント管理スイートを使用して、それぞれ固有のデバイスのシリアル番号を登録する必要があります。まず最初に、IT スタッフによるプロセスが必要なため、Kingston から各注文ごとのシリアル番号一覧を提供できます。この一覧は常に英数字データで、順番にソートされていません。この手法を選択すると、個々のドライブの所有者に応じた非常に柔軟なポリシー運用が可能になり、さらに、IT 部門が捜査を行う場合、非常に有益なデバイス来歴追跡を正確に行えるようになるという長所もあります。一部の Kingston ドライブには、電子スキャン用に筐体にシリアル番号とバーコードが含まれていますが、企業向けに筐体にバーコードとシリアル番号を追加するようにカスタマイズできるドライブもあります。これらのアイテムはドライブの追跡に使用できます。

原則的に、エンドポイント管理システムは、ポートのブロックとホワイトリストのための VID/PID へのアクセスを提供します。Kingston では、USB ストレージデバイスの使用を促進する際に、お客様のご事情に合わせてカスタマイズされたポリシーを実現できるように、これらの機能の多種多様な活用方法を提供しています。適切な識別方法を確立することで、おおざっぱな「すべてのポートをブロックする」という方針は単純すぎるだけでなく、不要になります。

## リモートユーザー向けの安全でコンプライアンスに沿ったソリューション

セキュリティの面で、ホワイトリストによるデバイス管理は問題の半分のみを取り扱うにすぎません。言い換えると、これはソリューションの半分にすぎません。

USB ストレージデバイスはその利便性とシンプルさにより、スムーズなデータ転送を実現するために可搬性が鍵となる多くの企業や機関にとって不可欠なものとなっています。ほとんどの環境では規制準拠や IT 品質管理などの理由で、データ移動のような作業用にスタッフに暗号化 USB メモリを携帯させることが必要です。パスワード保護とデバイスの暗号化を組み合わせて利用することで、ポータブルストレージには、デバイスの紛失、盗難、または潜在的に脆弱な状況に放置された場合に、機密データへのアクセスを防止するための保護手段が提供されます。


暗号化技術はさまざまであり、これは万能のソリューションではありません。ソフトウェアとハードウェアの暗号化ソリューションを比較すると、最も大きな違いが明らかになってきます。ではどちらが良いのでしょうか？それは個々のニーズによって異なりますが、より踏み込んだ質問は、「どちらがより安全でしょうか?」と尋ねることです。

ソフトウェア暗号化は基本的に、小規模な運用で済む一部の分野を満足させるだけの、低予算の選択肢です。また、データ転送が機密でなく、ポリシー遵守の方が重視される企業に適している方法です。

しかし、ソフトウェア暗号化の便利さは、アキレス腱でもあります。コンピュータに依存するクライアント側アプリケーションでして暗号化を実行する必要があるためです。したがって、必然的に、ソフトウェア暗号化ストレージデバイスの安全性はホストコンピューターと同じ程度にとどまります。

コンピューターのメモリにアクセスできるハッカーが暗号化/復号化キーを「盗聴」できるため、侵害の危険も高まります。暗号化されたファイルにアクセスしてコピーできる場合、パスワードによるアクセス保護は必要ないため、ドライブ上のデータはブルートフォース攻撃の対象になる可能性があります。

ソフトウェアベースの暗号化では、ソフトウェアの更新が時々必要になる可能性があり、IT スタッフの負担が増えるため、実装が複雑になる可能性があることに注意してください。特に大きな短所として、異なるプラットフォームでドライブを利用する際に問題が発生し、いらいらした従業員がソフトウェア暗号化機能を完全に削除してしまうことがあります。ドライブのユーザーは、暗号化されたドライブのデータをコンピュータに一旦コピーし、ドライブを非暗号化ドライブにフォーマットし直してから、データをドライブにコピーして戻すことができます。この時点で、データは安全ではなくなり、漏えいに対して完全に脆弱になります。USB ドライブのセキュリティが実質的に無効になる可能性があるため、データプライバシー法および規制の遵守を目的としてこれは容認できません。

# オンチップ暗号化：強力かつ高速なソリューション

対照的に、ハードウェア暗号化された USB ドライブは、実際のドライブに暗号化を管理する専用プロセッサが組み込まれているため、コンピューターとは独立して機能します。ブルートフォースパスワード攻撃に対する保護を備えた常時オンの暗号化プロセスを備えています。暗号化されたデータにはアクセスできず、コピーすることもできません。

Kingston のエンタープライズおよびミリタリーグレードのハードウェア暗号化 USB ドライブは、XTS モードで AES 256 ビット暗号化を利用しています。世界各国で認可を受けている暗号化技法の AES 256 ビットでは、堅牢なデータ保護を提供しています。XTS モードは、暗号化/復号化プロセスの異なる段階で 2 つの個別のキーを利用することにより、データを 2 回暗号化するのと同様の効果をもたらします。

使用時には、暗号化キーはドライブコントローラーの乱数生成器から導出され、ユーザーのパスワードでロックが解除されます。認証はデバイスの暗号化ハードウェア内で行われるため、暗号化キーやその他の重要なセキュリティ機能は、BadUSB、コールドブート攻撃、悪意のあるコード、ブルートフォース攻撃などの一般的な侵害から保護されます。

ハードウェア暗号化の最も直接的な利点の 1 つは、暗号化タスクをホストコンピューターに負担させないため、ドライブのパフォーマンスがソフトウェアで暗号化されたドライブよりも大幅に優れていることです。すべてはドライブ内で行われます。

Kingston IronKey D500S などのハードウェア暗号化 USB ドライブは、工場出荷時から暗号化されている、パスワードで保護されたデバイスです。使用する際、最初はかきこみ防止が施されたランチャーボリュームのみが見えます。これにパスワードの認証とメイン暗号化ストレージボリュームのアンロックに使用するアプリケーションが含まれています。この手順により、ホスト PC にドライバーやソフトウェアをインストールする必要が一切なくなります。

さらに、Kingston のハードウェア暗号化 USB ドライブは、デバイス内でのファームウェアの操作を防止するデジタル署名されたファームウェアを備えています。この追加セキュリティ層によって、USB デバイスファームウェア特有の脆弱性を悪用する BadUSB などの攻撃から保護します。これにより、ホストコンピューター上でコマンドが秘密裏に実行されたり、悪意のあるコードが実行されたりする可能性があります。

もちろん、「すべてのポートをブロックする」アプローチは、BadUSB 侵害のリスクを減らせますが、なぜそのような時代遅れの慣行で生産性を犠牲にするのでしょうか？上で強調したように、ハードウェア暗号化 USB ドライブを導入するための簡単な調達および実装の手順が整備されていれば、ポータブルストレージデバイスを使用しながらも、安全な環境を維持できます。

# リモートワークでのセキュリティ維持とコンプライアンス

リモートワーカーが会社の安全な作業環境から遠く離れ、保護を受けられない今、戦略を見直し、新たな目線で優先度を考える必要があります。


リモートでのセキュリティプランについて言えば、従業員のノートパソコンの USB ポートをブロックするメリットはあるのでしょうか？従業員がインターネット経由でサーバーにアクセスしてドキュメントをアップロードまたは取得するようになるだけです。外出時は、セキュリティと信用性の低い Wi-Fi アクセスポイントなどのオープンインターネットアクセスしか利用できず、そのためにさまざまな危険を招き、漏えいの可能性が増大します。スプーフィングによるデータ傍受や監視、中間者（MitM）攻撃、ネット

ワーク盗聴などの脅威は、サイバー犯罪者が利用できる、ますます巧妙化したハッキング手法のほんの一部にすぎません。VPN さえも侵害されています。

組織のインターネットへのネットワーク接続は単なるエンドポイントであり、本質的に暴露されているため、非常に脆弱で標的を絞られた侵入口になります。リモートアクセスに公開することは、特に機密データに関してはセキュリティ上のリスクが伴います。

パスワードで保護され、ハードウェアで暗号化された USB ドライブをリモートワーカーに委託することで、潜在的なネットワークの脆弱性を効果的に排除できます。しかしこのようなデバイスを提供するには、入手可能な USB メモリについて詳しく調査し、それぞれのリモートワーク環境のニーズに合うかを検討する必要があります。これには、ドライブ容量や、シリアル番号がログに記録されているかなど、多くの考慮事項があり、簡単には選択できません。これはデバイス自体の物理的な構造に関係します。

# 改ざん防止の保護手段：確かなオプション

ここでの主な問題は、ハードウェアで暗号化された USB ドライブが改ざん防止できるかどうかです。このような干渉に対してデバイスがどの程度安全であるかは、FIPS 140-3 などの規格に反映されています。FIPS 140-3 には、暗号化手法を使用せずにドライブの物理構造の復元力を精査するいくつかのレベルがあります。


関連する FIPS-197 認定は、ハードウェア暗号化属性と、データセキュリティ要件がミリタリーグレードレベルではないエンタープライズ向けモデルである IronKey Vault Privacy 50 シリーズや Vault Privacy 80 外付け SSD などのデバイスのみを監視します。これらのドライブは安価ですが、物理ドライブの改ざんに対する保護がありません。

FIPS 140-3 レベル 3 認定（申請中）では、デバイスの改ざんを暴露するために使用される手法はミリタリーグレードとして認められています。Kingston は、これらの FIPS 140-3 レベル 3 ドライブを世界中の企業、政府、軍に供給しています。

内部にエポキシを使用してセキュリティに必要なすべての駆動回路をコーティングし、内部コンポーネントをケースに接着することで、さらなる防御壁が作成されます。金属製のケースを開こうとしても非常に困難で、最終的には内部のチップや他のコンポーネントが壊れてしまい、ドライブが機能しなくなります。この硬くて不透明なエポキシを所定の位置に配置すると、重要なコンポーネントを改ざんすることはほぼ不可能な作業になります。Kingston IronKey D500S や S1000 などのデバイスには、この追加のセキュリティ対策が含まれています。

これらのデバイス保護は物理的対策のみに限定されず、Kingston IronKey S1000 は改ざん防止を別のレベルに引き上げます。IronKey S1000 では、内部暗号チップにより物理的改ざんを検出可能で、デバイスに電源が入るとただちにドライブが使用不能になります。ハードウェアで暗号化された USB ストレージ デバイスに依存して機密ファイルにアクセスし、転送することは、スムーズなリモート操作を促進し、現場でのセキュリティを効果的に保証する実用的な措置です。

USB ドライブのハードウェアとセキュリティ機能を必ず調べて、特定のニーズやユースケースに対応しているかどうかを確認してください。ケースバイケースでそれぞれの USB メモリを検討してください。信用のある認定制度を意思決定の指針として役立てることができます。優先順位が何であれ、Kingston は、一般的なコンプライアンスから最も厳しいミリタリー仕様に至るまで、あらゆる種類の環境に対応する幅広いハードウェア暗号化 USB ドライブ ソリューションとカスタマイズ オプションを手頃な価格で提供しています。

# 安全第一：ネットワークがなくても問題はありません

現在、オフィスに国境はなく、在宅勤務が普及し続けるにつれて、リモートアクセスの脆弱性の問題が多くの企業で注目を集めています。多くの人がこれらの課題に初めて直面しており、この増大する傾向に対応するより安全な方法を探しています。

さまざまな業界におけるこのようなニーズのサポートに関して、ハードウェア暗号化 USB ストレージデバイスはすでに十分に確立しており、いくつかの理由でネットワーク経由のデータ転送が非実用的であるか、望ましくない場合にセキュアなソリューションを提供します。

金融業界では、規制当局は企業の行動とコンプライアンスをチェックするためにデータを頻繁に要求します。投資や市場取引など極秘のバンキング活動について正確な詳細情報が記載されている機密文書を伝送する際に、ネットワークを使用することは、曝露の危険があまりにも高く、考えられません。シンプルで効果的な解決策は、この情報をハードウェア暗号化された USB ドライブで配信することです。

医療環境では、安全な USB ドライブを使用してファイルを転送することが日常的に行われています。このやり方はまた、医師やコンサルタントがファイルを分析する際、調査のために参照する際、医療研究のために症例を提示する際などに便利です。さらに、医療用画像処理装置などのネットワークへのアクセスがないか、ネットワークにアクセスすると安全でないプロプライエタリシステムに関して、実用的なニーズがあります。準拠したハードウェア暗号化 USB ドライブを利用することで、ファイルを簡単に転送して他の場所で使用できます。

## 注意事項

✓ **規制準拠した安全なドライブを使用し、**仕様を確認して各実装のニーズに合ったドライブを調達してください。

✗ **ランダムな、または個人所有デバイスの業務使用（BYOD）ポリシーを承認しないでください** – どの企業にとっても、暗号化されていないドライブを失うことは、財務損失および評判失墜の点であまりにも大きな代償です。

✓ **エンドポイント管理スイートを展開し、**独特のホワイトリスト機能を提供するハードウェア暗号化 USB ドライブを使用してください。

✗ **何事も成り行き任せにしないでください。**– 施設内およびリモート作業環境の要件を適切に評価してください。

✓ **セキュリティの問題についてスタッフを教育し**てください。会社をセキュリティ侵害から守り続けることが彼ら自身の利益になります。

✗ **セキュリティ対策の負担をあまりかけないようにしてください。**ユーザーが影に隠れて IT ソリューションを利用し始めます。全員対象のポリシーがどんな場合にも適用されるからと言って、すべての状況で適切なわけではありません。職場は変化しており、適切なソリューションを選択することで、新しいポリシーを策定し、施行することができます。

この状況では、Kingston IronKey Keypad 200（KP200）が真価を発揮します。OS に依存しないドライブであるため、パスワードを入力するためのランチャーボリュームはありませんが、その代わりに、どのプラットフォームでも使用できるようにデバイスをアンロックする英数字キーパッドが付属しています。さまざまな用途に使えるハードウェア暗号化 USB メモリですので、製造分野でも使用できます。たとえば運用技術（OT）プラットフォームによる機械制御用に、IT 研究開発分野で作成されたアプリケーションを安全に移行できます。Linux も使用する混合プラットフォーム運用の場合、KP200 は利用可能な最も簡単な安全なソリューションの 1 つです。

ハードウェア暗号化された USB ストレージデバイスは、法執行機関でも重要な役割を果たします。事件ファイルや画像などの証拠を保護し、現場の調査員、捜査陣、法科学チームなどと安全に受け渡しができます。Kingston では、外部ケースに内部シリアル番号とバーコードを印刷して提供できますので、さらに利点があります。ドライブを支給して記録にまとめると、シンプルかつ容易に追跡できます。手操作でシリアル番号を記録するのと同様に容易で、バーコードをスキャンするのと同様に迅速ですので、監査や在庫管理が容易になります。これは、Kingston IronKey D500S、D500SM、および S1000B/E ドライブに標準として搭載されている機能ですが、Kingston カスタマイゼーションプログラムの一部として他のハードウェア暗号化モデルでも利用できます。

# セキュリティとストレージのモビリティ：最高水準

パスワード保護、ハードウェア暗号化、改ざん防止セーフガード、きめ細かなエンドポイントのホワイトリスト追加、ミリタリーグレードの FIPS 140-3 レベル 3 認証（申請中）、および一目でわかるログ記録は、Kingston USB ドライブの既製の機能であり、すぐに利用できます。

これらの堅牢なセキュリティ防御機能により、USB ドライブとそのデータはホスト環境において安全な状態を維持します。書面のスペックが素晴らしいからといって、何も調べずに適当にモデルを選んでも、組織が厳密な要件を持っている場合、理想的な解決策になるとは限りません。

独立系メーカーであるKingstonは、顧客のニーズを満たすために幅広いオプションを提供しています。Kingston Customisationプログラムを通じて、シームレスなユーザーエクスペリエンスを提供するように設計された高度なソリューションを利用できます。

セキュアなカスタマイズは、ホワイトリスト用の独自の USB PID を組織に提供するだけではありません。ランチャーアプリケーションのセキュリティプロファイルもカスタマイズ可能で、連絡先や会社詳細から、パスワードのヒントの有効化やパスワード試行回数上限の決定まで、15 種類の設定から選べます。社外向けに、企業ブランド（共通ロゴ）を印刷したり、企業専用のドライブにブランドカラーなどさまざまな色をお選びいただくことができます。最小注文数は 50 ドライブで、これらすべての機能が組み合わさって理想的に統合され、簡単にデバイスを実装できます。

安全な USB ストレージに適したエンドポイント管理アプリケーションがまだ導入されていない場合でも、多数の Kingston ドライブを管理したい組織が利用できる、管理ソリューション（パスワードをリモートでリセットするオプションなど）が用意されています。

USB の普及性と利便性により、USB はさまざまな有望な新興技術を超えて存続しており、多くのタスクでは USB ストレージの即時性と利便性が重宝されています。すぐに利用でき、常に安全に保護された USB ドライブは、すぐに評価できるシンプルなソリューションを提供します。

リモート環境でのネットワークデータ侵害を心配したくないなら、どうすればいいのでしょうか？Kingston IronKey ハードウェア暗号化 USB ストレージ デバイスなら、その答えを手のひらの上でお届けします。

Kingston がどのように役立つかについて詳しくは、kingston.com/ironkey にアクセスするか、より具体的な質問については、Encrypted USB の専門家に問い合わせてください。

**#KingstonIsWithYou #KingstonIronkey**