
Kingston
TECHNOLOGY
USB ドライブが
今の時代にも意味が
ある理由は？
#KingstonIsWithYou

USB ドライブが今の時代にも意味がある理由は？

まえがきと目次

世界の企業データ全体の 60% がクラウドに保存されている[1]デジタル時代の今、発売開始から 30 年近くたったストレージ技術手法が今でも通用するのかを論じることは、少し奇妙に思われるかもしれません。しかし、この普及型ストレージ技術は、発売以来大きく進化を遂げており、今後も発展し続ける見込みです。

USB ドライブが、ファイル、ドライブ、アプリケーションをつなげる標準的な手段に過ぎなかった時代は、もう昔のことです。現在のソリューションは転送速度が大幅に向上しただけでなく、多くの状況に必要な信頼性と安全性に優れた、ポータブルメディアとも機能します。今ではクラウドストレージソリューションでもほぼ同じ利点を提供できるようになったようですが、それでも USB ドライブを使うことに意味があるのはなぜでしょうか？

この e ブックでは、クラウドが支配的な状況の中で、USB フラッシュドライブがどのような用途に役立つかをご説明します。業界の主なエキスパート数名から得た重要な知見を裏付けとして使用しながら、現在、企業・団体などで USB ドライブが使用されている理由についてご説明し、ソフトウェア暗号化との比較、独立ストレージ環境、エンドポイントでのデータセキュリティなどについて論じます。

USB ドライブが今の時代にも意味がある理由は？

寄稿者

このｅブックは、IT と新興技術の業界エキスパート 3 名の力を得て、作成されました。

Rafael Bloom

彼は、テクノロジー製品、マーケティングコミュニケーション、事業開発の上級職としてキャリアを重ねました。彼のアドバイザリー業務は、収益源の構築と維持を主な目標として、技術的および規制上の変化による組織、製品、コミュニケーションの新たな課題に焦点を当てています。この非常に多様な業務には、情報ガバナンス、コンプライアンスを視野に入れた設計、データプライバシーや、アドテック、モバイルおよび 5G、人工知能、機械学習などの新技術に関する技術顧問が含まれています。

Tomasz Surdyk

Tomasz 氏は政府自治体内の IT セキュリティに関して 24 年以上の経験を持ち、情報セキュリティ、個人データおよびサイバーセキュリティなどの分野で第一人者となっています。これまでに、行政機関で機密情報や個人データを処理する ICT システムおよびネットワークの検査に携わってきました。また、NATO と EU のセキュリティクリアランスを取得しています。数年間にわたり、企業情報や個人データの保護強化用セキュリティソリューションの実装を専門とする企業を経営しています。

David Clarke

David は、トムソン・ロイターによる「英国におけるソーシャルメディア、リスク管理、コンプライアンス、レグテックの分野で最も影響力のある思想的リーダーおよび思想家トップ 30」で上位 10 名に入るインフルエンサーとして認められており、Kingston Technology による世界的専門家のトップ 50 のリストにも入っています。David はこれまで、グローバル FTSE100 社のセキュリティ・サービス・デリバリーのグローバル責任者やセキュリティ・インフラストラクチャの責任者など、複数のセキュリティ管理職を歴任してきました。

USB フラッシュドライブの登場

20 年以上前に最初のユニバーサルシリアルバス（USB）ドライブが市場に登場した時、その幅広い互換性によって、コンピュータ技術の分野の流れは大きく変わりました。2000 年に最初の USB フラッシュドライブがリリースされると、多くの人々が複数のデバイスを操作できるようになったため、USB はすぐに進化し、より高速なデータ転送速度、USB 3.0 ポート、大容量などが提供されるようになりました。

それ以降、モバイルデータストレージやセキュリティのニーズに対応する技術が大きく進化を遂げています。注目を集めているのは、非常に特殊な用途を念頭に設計されている現世代の USB ドライブです。企業から見ると、リモートワークやハイブリッドワークの増加や、クラウドサービスの利用の増加、サイバーセキュリティの問題の深刻化などによって、効果的なソリューションの必要性がますます高まっています。これに加えて、規制要件を順守した方法でデータを保管する必要があります。分散した複雑なシステムが「オンプレミス」とクラウドで実行されることで、この圧力がさらに悪化することもよく起こっています。

さらに、文書、メール、写真、動画、メタデータなどの構造化データや非構造化データの量の増大という問題があります。これらはすべて、企業で変化し続けるストレージ要件を一層複雑にします。

しかし、クラウドストレージがこれらの問題にすべて対応できるとしたら、現在のビジネス環境で USB ドライブを使用する意味はあるのでしょうか？

> 過去に使用されていた USB ドライブは、たいてい使い捨てで、パフォーマンスが低く、セキュリティも弱かったため、多くの人々に、もう時代遅れでつまらないものと考えられています。- Rafael Bloom

需要の増大に対応するポータブルストレージ

USB ドライブをポータブルストレージの道具として使用する旧来の方法は消えつつありますが、高性能 USBドライブを、データ保護や機密保護を多層化する個人用の安全なローカルバックアップとして利用する方法が出現しました。これは、人事記録、財務データ、医療記録、知的財産（IP）保護、個人を特定できる情報（PII）全般など、規制対象とされるデータにとって、非常に重要な意味を持ちます。また、この世代のデバイスはデータ転送速度、ストレージ、バックアップ、セキュリティ機能が強化されているため、次の用途に応用できます。

- 手渡しが必要な規制情報
- 現場や遠隔地への配達や印刷が必要な法務および財務関係の書類
- ランサムウェアの脅威がある、危険な環境すべて
- ネットワークでアクセスできない場所へ持ち込んで印刷

暗号化 USB の提供で業界をリードする Kingston Technology は、Kingston IronKey™ S1000 などのソリューションをリリースして進化する需要に対応し続けています。これはクラス最高の暗号化 USB ドライブで、XTS-AES 256 ビットの暗号化や、強固な改ざん防止機能付きの独立した暗号化チップなどを活用した機密データ保護機能により、厳格な基準に対応しています。また、FIPS 140-2 レベル 3 認証取得済みです。つまり、暗号ハードウェアの一種として効果を発揮することが、米国政府によって正式に検証されているため、より安心なデータ保護を求める企業組織に最適です。

このようなハードウェア暗号化 USB ドライブでは、データの場所がクラウドかオンプレミスかに関係なく、一括型の安全なデバイス管理ソリューションが可能です。ソフトウェア不要で使いやすく、コンプライアンスに沿った暗号化データストレージですので、IT 担当者の貴重な時間を無駄にせず、迅速かつ効率的に実装可能なソリューションを設計できます。

需要の増大に対応するポータブルストレージ

サードパーティのクラウドサービスから独立して、長期的にデジタル資産を保護するために USB ドライブを活用するもうひとつの例として、バックアップとアーカイブがあります。クラウドでも大容量のデータを転送できますが、企業の独自知的財産は、インターネットから分離して安全に保管できる、暗号化セキュア USB ドライブに機密情報として保管しておくほうがよいでしょう。

企業がデータを論理的および物理的に管理下に置きたい状況は必ず発生します。暗号化ドライブを使用する場合は特にそうです。また、HDD や SSD 上のストレージが暗号化できない場合もあります。Kingston IronKey D300S のような外付けの暗号化 USB ドライブを使用すれば、この問題は解決されます。この USB フラッシュドライブには、128 ビットのデータブロックを暗号化できるブロック暗号、XTS 256 ビットの AES（高度暗号化標準）ハードウェア暗号化が施されています。これ以上のデータの暗号化が必要になった場合、AES は、前のモードより優れた強固なデータ保護を提供できる XTS ブロック暗号モードを使用します。

> 私の意見では、USB フラッシュドライブは依然として使用されており、データセキュリティに欠かせない要素です。特に、デバイス間で迅速に情報を移動するため、そして適切な保管と保護のために使用されています。- Tomasz Surdyk

暗号化：ハードウェアベースとソフトウェアベースの比較

データの暗号化の方法については、ハードウェア暗号化がソフトウェア暗号化よりも管理しやすく安全であると言っても差支えないでしょう。これは、暗号化プロセスが、ホストシステムの他の部分とは分離されているため、傍受や突破が難しいためです。集中型のデバイスレベル管理を用いて、イントラネット LAN やインターネット接続を介したドライブ制御が可能になり、これは以下の場合に非常に優れたツールになります。

- 暗号化された個別／グループ USB の使用に関するポリシーの制定と施行
- データが組織を出入りするたびに正確に追跡する、ファイル移動の監査
- 重要なデータを転送する際にリモートでコンテンツをバックアップ可能
- USB の紛失または侵害の場合にリモートでデバイスを無効化
- リモートパスワードを忘れた場合にリセットを実行

このように認証済みドライブを正しく管理すれば、機密データのコピーや共有のリスクを最小限に抑えることができます。さらに、現在のハードウェア暗号化 USB ドライブには、ファイルやメッセージが受取人以外にアクセスや読み取りされないよう防ぐ、多くのセキュリティ機能が追加されています。

> 私は、ハードウェア暗号化がソフトウェア暗号化よりも優れていると考えています。ハードウェアおよびソフトウェア暗号化の手法は、ブルートフォース攻撃（総当たり攻撃）に対する脆弱性で大きな違いがあります。ハードウェア暗号化デバイスの場合は、このような攻撃に容易に屈服しません。
>
> - Tomasz Surdyk

暗号化：ハードウェアベースとソフトウェアベースの比較

低価格なためソフトウェア暗号化を検討する企業も見受けられますが、これは目先の利益に目を奪われすぎかもしれません。ソフトウェアベースのソリューションでは、ホストデバイスの暗号化リソースを他のプログラムと共有するため、安全性のレベルはそのコンピュータによって決定されてしまいます。また、頻繁なソフトウェア更新が必要なため、保守を怠ると脆弱になります。ソフトウェア暗号化 USB ドライブは、パスワードを推測するブルートフォース攻撃を無制限に受ける場合があり、短時間に何百もの文字の組み合わせを試すソフトウェアベースの辞書攻撃には対抗できません。

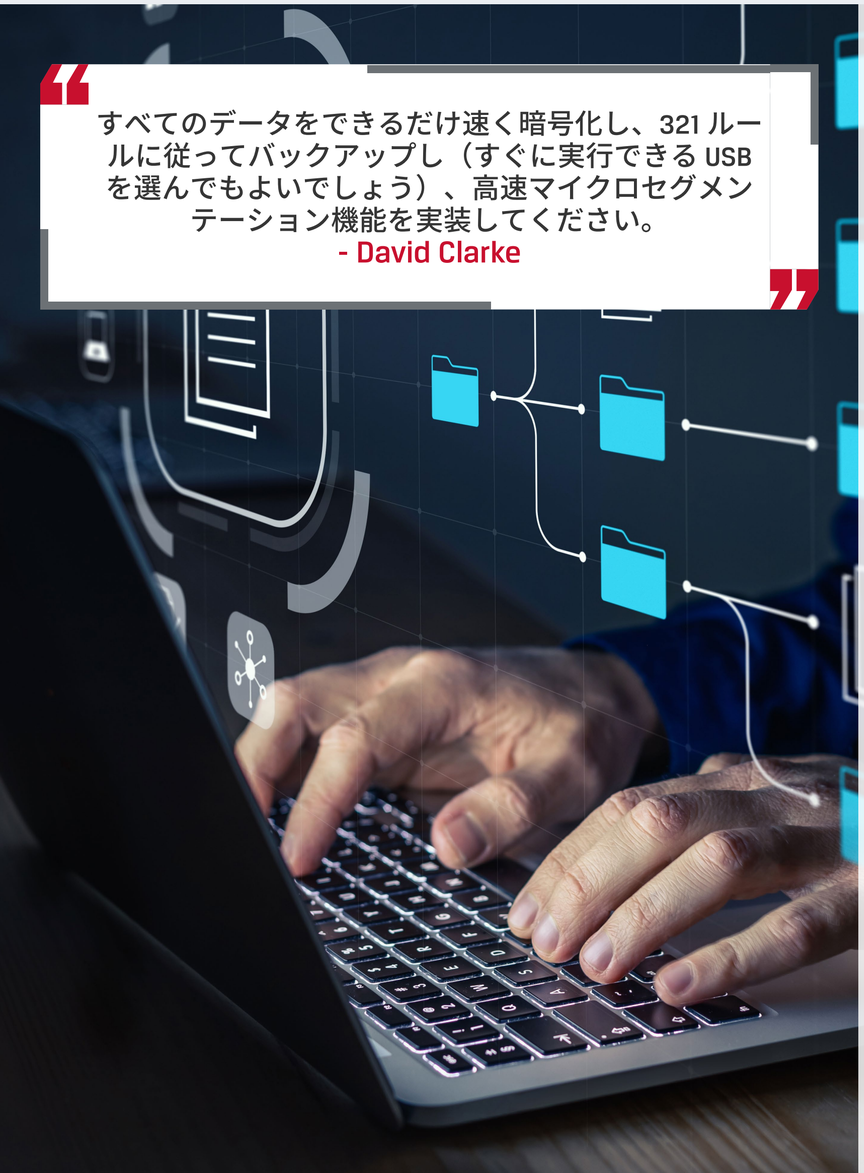
さらに、ソフトウェア暗号化は解除可能な暗号化手法でもあります。ソフトウェア暗号化ドライブを持っている従業員が、データをコピーして USB ドライブをフォーマットしてしまえば、暗号化は解除されます。その後、データファイルをコピーしてドライブに戻し、さまざまなプラットフォームや OS 上で認証の手間なしに使用することができます。

前に述べたとおり、ハードウェア暗号化では、物理的な「暗号化」と、それに続くデータの保存は、ホストシステムから独立して行われます。これにより、システムがたとえ侵害されていたとしても、もう一枚の壁で防衛できます。

これは特に金融、医療、政府自治体などの業界にとって見逃せません。医療保険の携行性と責任に関する法律（HIPAA）や PCIDSS (クレジットカード業界データセキュリティ基準)などの規制で、機密情報の暗号化について厳格な要件が設けられているためです。

強固なハードウェア暗号化デバイスによってこれらの規制を順守すれば、企業は高額な罰金、訴訟、壊滅的な企業イメージの損傷のおそれを回避することができます。安価な一般の USB ドライブよりも、ハードウェア暗号化ドライブは高くつきますが、侵害に遭った場合の法務費用は、数時間の法律相談だけでドライブ数百個分の費用になる場合があります。

機密データの保護のニーズ拡大



> すべてのデータをできるだけ速く暗号化し、321 ルールに従ってバックアップし（すぐに実行できる USB を選んでもよいでしょう）、高速マイクロセグメンテーション機能を実装してください。
> - David Clarke

機密データの紛失や盗難の防止については、それぞれの組織が、デバイスに確実に適切なセキュリティ機能を付ける義務があります。また、数多くのサイバー攻撃の脅威が進化を続けているため、デジタル成熟度やユーザー自身による末端でのデータ管理スキルが、依然として高いリスク要因のままであることを考慮することも重要です。組織内部からの脅威には、データ管理からの逸脱や USB ストレージデバイスの紛失、安全でない環境へのデータの転送、暗号化されていない USB ドライブの使用、パスワードの共有などがあり、そのすべてがエンドユーザの注意義務および努力の不足が原因です。これらはすべて、適切な研修、教育、適正な USB ドライブソリューションによって予防できます。

事前に計画を立てよく訓練された連絡体制は、会社の存続を揺るがしかねない危機への対処にも重要な役割を果たします。現在のサイバー脅威は、企業の弱点を標的に狙っています。

暗号化 USB 計画を構築する最良の時期は、それが必要になる前であり、暗号化 USB ドライブとそのポリシーを全社的な総合セキュリティ戦略に組み込む必要があります。暗号化 USB の計画を施行せず、ガイドラインもない場合、基準とするものがなくなり、企業は規制順守違反など、あらゆるレベルのリスクにさらされます。たとえば一般データ保護規則（GDPR）では、記事 32 で機密データに暗号化が必要であると具体的に言及しています。

> 企業は、全データセットの重要度や機密レベルを記載した明確なデータマップを用意し、最重要データに最優先に対応する計画を立て、データへの接続を物理的になくすか、データソースを外部から見られない場所に置く必要があります。迅速に関連システムを隔離可能にすることが重要です。そして、文書化した計画を立て、訓練を行うことは必須です。
> - Rafael Bloom

> ユーザーは機密データを処理します。これを紛失した場合の責任は重大で、会社のイメージや安全に大きな悪影響を与えます。機密データを保護するために、データ暗号化など各種セキュリティソリューションを使用する必要があります。- Tomasz Surdyk

機密性の高い金融データの保護

セキュリティ的な意味合いに加えて、データストレージおよびバックアップソリューションが従わなければならないコンプライアンス標準もあります。これらの規則には、データ保持スケジュールを管理し施行する必要など、様々な業界に共通するものがある一方で、企業データのクラウドへの移行などは、業界に応じて扱いがかなり異なります。

金融サービスなど多くの業界では、適切なデータ管理義務を定めた規制が実施されています。銀行では特に、初期はサードパーティのストレージやバックアップを使用したがらない傾向が非常に強く、今でも多くの銀行がデータインフラのすべてを所有することにこだわっています。

金融機関はまた、サーベンス・オクスリー法（SOX）や一般データ保護規則（GDPR）など、増加し続けるデータセキュリティ規制および標準を順守する義務があります。しかし、モバイルで働く従業員や請負業者が増加するに従い、データ漏洩のリスクや、法律や標準で定められた義務を順守できないリスクも高まっています。

実際には、もしモバイルで働く従業員が、自分が持ち運んでいるデジタルアイデンティティ、ポータブルワークスペース、顧客の記録、財務データなどの保護を怠ったら、コンプライアンスへの努力は簡単に水の泡になります。このため、多くの企業では、従業員がどこにいようとも、デジタルアイデンティティやアプリケーションを保護するため、Kingston IronKey 暗号化 USB ドライブなどのモバイルセキュリティソリューションへ移行しています。

> 全体的な傾向として、IT の設置場所がますます分散していく状況や、クラウドインフラの拡張性の高さを考慮すると、多くの業界や多数の中小企業は、もはや冷却装置付きのサーバールームの管理を考えていないことが容易に理解できます。
> - Rafael Bloom

患者の医療データへの安全なアクセス

医療業界でもまた、データセキュリティが今まで以上に重要になっています。2021 年にはデータ侵害によって 4567 万件の患者情報が流出し、患者情報の盗難リスクが高まっています。これは年間の合計数としては 2015 年以降もっとも大きな数字です[2]。データストレージとバックアップの点から見ると、患者データは、医療提供者が患者を安全に扱えるようにするための重要で包括的な医療情報です。

これには、患者の医療履歴、検査、写真、X 線写真などを記載した電子健康記録（EHR）ファイルや、支払い記録、患者の保険、未払い料金などを記載した事務ファイルなとがあります。モバイルで働くスタッフの増加や、医療市場の拡大に直面し、大きな変革が進行しているため、現在の医療提供者がデータセキュリティに懸念を感じているのは不思議ではありません。

さらに、リスクを予測せず、医療保険の携行性と責任に関する法律（HIPAA）や経済的および臨床的健全性のための健康情報技術に関する法律（HITECH）などの厳格な義務を守れない場合、医療データの漏洩が非常に高額の損失になる場合もあり、患者、パートナー、規制当局者の信頼もさらに揺らぐことになります。

暗号化 USB ドライブの中でも Kingston IronKey シリーズなどを使用したソリューションでは、医療組織が一台の端末から、数個～数千個のドライブに対してパスワード、アプリケーションの使用、回復などのポリシーを設定できます。保存したデータに安全にアクセスするために、ドライバや他のソフトウェアをインストールする必要のない、ユーザーフレンドリなソリューションのため、モバイルや現場などで働くスタッフは、患者のサポートに役立てることができます。ユーザーや管理者はどんな場所にいても、容易かつ迅速にデータを見ることができます。

> 特にランサムウェアが成長産業になりつつあり、機密データを扱う組織は、極端な圧力下でも業務を継続する方法を検討しなければなりません。
> - Rafael Bloom

クラウドストレージの未来における USB ドライブの役割

> クラウドデータストレージは、現在および将来も利用されるでしょう。しかし私は、暗号化 USB ドライブによって、データを物理的に保護することがもっとも安全だと主張します。クラウドで何が起きているか、ユーザーが完全に制御することはできません。しかし、暗号化 USB ドライブではデータを制御して、自分で保護し保存できます。私たち以外は、それらの媒体にアクセスすることはできません。
> - Tomasz Surdyk

ここまで、USB ドライブの利点を明らかにしてきましたが、それではクラウドストレージの未来で、USB ドライブはどのような役割を果たすのでしょうか？

10 年前には、データを便利に保存して運ぶ主要な道具として、USBドライブの需要は膨大でした。しかし、ハイブリッドな勤務形態の登場や、チームの各員がばらばらな場所で働くことが増えた影響で、クラウドは多くのデバイスから素早くかつ簡単にアクセスでき、情報を保管できるようになりました。かつてフラッシュドライブは、ファイルの移動を便利に行えるという独自性から、非常に人気がありました。現在は、クラウドストレージサービスが、さらに簡単にファイルを移動できるようにしています。

ただし、クラウドストレージには多くの制限があります。ネットワーク接続が必要で、いつどのようにファイルのバックアップや転送が行われたかわかりません。そのため、セキュリティ面での懸念が増えます。会社がクラウドを使用するように義務付けた場合、データのアクセス経路までを管理できるとは限りません。したがって、個人用または公共の Wi-Fi 接続を使用して VPN にアクセスするだけで、ハッキングのリスクが発生します。さらに、クラウドサービスは攻撃する側にとって魅力的で、マルウェアの大半（61%）がクラウドアプリケーションによって配布されています[3]。

> おそらく、クラウドを利用できないときに何が起きるか、データを 100% 利用可能にしておかなければならない場合のシナリオ、長期ストレージにより発生する脆弱性などについて検討しておくことが賢明でしょう。- David Clarke

クラウドストレージの未来における USB ドライブの役割

一方で USB 暗号化は、デバイスのハードウェア経由またはソフトウェア経由で実行することができます。ハードウェアで行われソフトウェアに依存しない暗号化は、サイバー攻撃対策にもっとも効果的な手段です。データ漏洩の対策として優秀で、複雑さのないソリューションであり、データ保護では究極のセキュリティによって厳格なコンプライアンス標準にも対応できますので、組織が安心して脅威を管理し、リスクを軽減できます。

ハードウェア暗号化 USB ドライブは自己完結型ですので、ホストコンピューター上に何らかのソフトウェアを置く必要がありません。ソフトウェアの脆弱性がないため、ブルートフォース攻撃、スニッフィング、およびメモリハッシュ攻撃の心配がありません。ソフトウェア暗号化 USB ドライブはまた、ユーザーが任意のコンピュータ上でドライブをフォーマットして暗号化を無効にし、保護されていない方法で機密データの保存に使用するリスクも抱えています。

ハードウェア暗号化 USB ドライブであれば、データを安全に保存できる、優れた物理的手段ともなります。ユーザーまたは管理者が情報アクセス基準を設定でき、既存のローカルエンドポイントソリューションと統合できます。このため、クラウドストレージでは対応不可能か、効果的なソリューションにならないような多くの状況で、便利で低価格のソリューションとなります。これにはたとえば、ネットワークに接続していないデバイスからデータを保存する必要がある場合、プライバシーを守る必要がある場合、オフライン時でもアクセスする必要がある場合などがあります。

> 私たちは組織が日常的に使用する頻度の高さに応じて、データを「ホット」（頻繁に使用）または「コールド」（それほど頻繁に使用しない）に分けて考えがちです。しかし、もし業務継続性や高パフォーマンスが組織全体や業務に必須な部門またはプロセスにとって重要であれば、「コールド」データをクラウドに置き、「ホット」データはローカルの USB ストレージを多用するのが効率的でしょう。
>
> - Rafael Bloom

サマリー

未来のイノベーションの到来を予見することは不可能ですが、弊社では、あらゆるモバイルデータ保護要件に対応するさまざまな暗号化ソリューションを備え、受賞歴のある USB ドライブ製品を提供できます。使いやすい PIN 保護用の英数字キーパッドを搭載した USB ドライブから、最高レベルの暗号化と改ざん防止機能で FIPS 140-2 レベル 3 認証取得済みの製品や、セキュリティを犠牲にしない SuperSpeed USB 3.1 技術まで、Kingston IronKey 製品は、強力で効果的なデータ移動とモバイルデータストレージソリューションをお約束する USB ドライブによって、データの課題に対応するように設計されています。

データストレージに関するあらゆる局面で、専門分野を持つエキスパートチームがサポートし、お客様のニーズに最適なストレージソリューションを見つけるよう、確実に支援します。

暗号化 USB プランの策定でも、お客様のビジネスに最適な USB ドライブの選定でも、セキュリティポリシーの制定や施行でも、弊社には機密情報を安全に保護し、新しい規制を順守するスキルと技術があります。きめ細かくパーソナライズされたサービスを提供することで、お客様のデータストレージの優先順位に合った製品を確実にご提供し、前例のない速さで変化するビジネス世界にも対応できるようにします。

Kingston について

35 年の実績を持つ Kingston は、企業が直面するモバイルデータの課題を特定し、解決する知識を有しており、組織をリスクにさらすことなく従業員が安全に業務に従事できるようにします。

1. Statista - https://www.statista.com/statistics/1062879/worldwide-cloud-storage-of-corporate-data
2. SC Magazine - https://www.scmagazine.com/analysis/breach/breaches-exposed-45-67m-patient-records-in-2021-largest-annual-total-since-2015
3. Infosecurity Magazine - https://www.infosecurity-magazine.com/blogs/cloud-services-top-of-mind-phishers

#KingstonIsWithYou