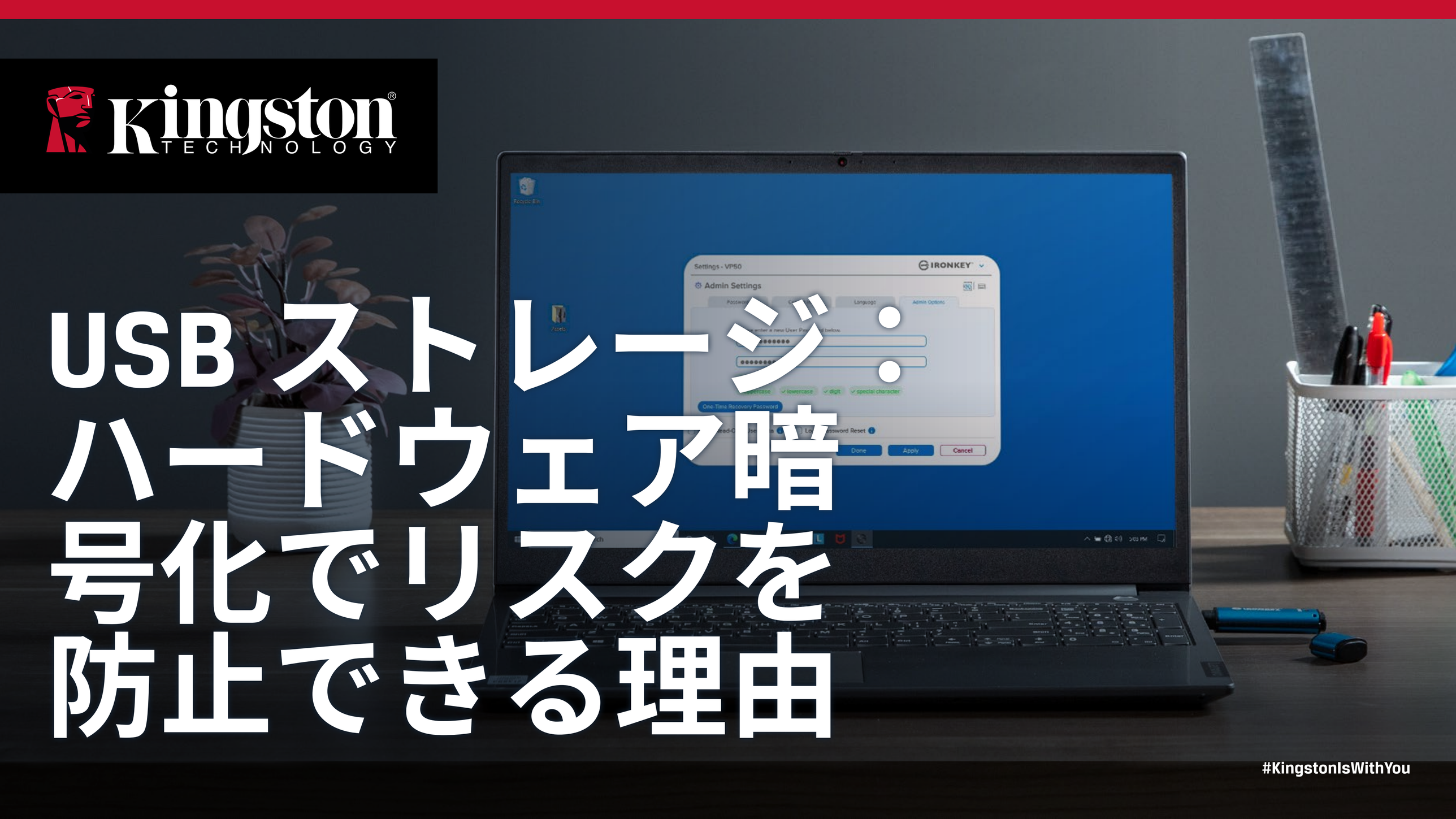
Kingston
TECHNOLOGY
USB ストレージ：
ハードウェア暗
号化でリスクを
防止できる理由
#KingstonIsWithYou

USB ストレージ：ハードウェア暗号化でリスクを防止できる理由

まえがきと目次

サイバーセキュリティはこれまで以上に企業の関心を集めていますが、非常に多くの企業でサイバーセキュリティの脅威に関する情報と対策が不足しています。UpCity 社によれば、新型コロナウイルスのパンデミック開始以来、多くの企業がリモートまたはハイブリッドワークモデルに移行しましたが、米国ではわずか 50% の企業がサイバーセキュリティ計画を実施中で、32% はサイバーセキュリティ計画を更新していません。また、サイバー攻撃の頻度は増加する一方で、全世界でランサムウェア攻撃を受けた企業の数は 2020 年に 37%、2021 年に 66% 増加しています[1]。

サイバーセキュリティの侵害は、企業に壊滅的な影響を与える可能性があります。サイバー攻撃による金銭的な損害に加えて、データ、安全、評判などを失うことで、短期的にも長期的にも多くの面で悪影響があります。

サイバーセキュリティ攻撃でよく使われる手段のひとつが、USB ドライブです。USB ドライブは機器に差し込むだけですぐ使えるという手軽さが理由で、多くの企業のあらゆる場所で使用されるようになりました。しかし、まさにその手軽さのせいで、USB ドライブは攻撃に対して非常に脆弱です。ひとつのドライブを置き忘れるか、盗まれるだけで、悪意のある何者かが機密データにアクセスできてしまう可能性があります。この点で暗号化は、個人や組織が USB ドライブを安全に使用し、それに伴うリスクを軽減する上で、重要な役割を果たすことができます。この e ブックでは、主に次の疑問への回答が得られます。

- 暗号化 USB がサイバー攻撃対策で重要な理由は？
- 組織が自ら脆弱性を高めがちな個所は？
- どんな対策が可能か？

目次	ページ

USB ストレージ：ハードウェア暗号化でリスクを防止できる理由

寄稿者

このｅブックは、IT およびエマージングテクノロジー業界の主導的な方々と、弊社の技術専門家が協力し、作成されました。

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。

Pasi Siukonen

Pasi は、Kingston 製品の広報、マーケティング、フィールドセールス、テクニカルサポート、カスタマーサービスなど、Kingston の各部門をサポートする専門家チームのリーダーを務めています。彼は主にフラッシュと SSD の製品ラインに注力しています。

コモディティと暗号化ドライブの違い

コモディティ（非暗号化）ドライブは非常に簡単にアクセスして使用できる一方で、ハードウェア暗号化ドライブには物理的およびデジタル的なセキュリティが複数のレイヤーで追加されており、ずっと安全な USB ストレージになっています。コモディティ非暗号化ドライブは容易に入手でき、低価格で持ち運びが簡単ですが、ユーザーにとって便利な分、機密データを盗みたい人、マルウェアやランサムウェアを企業ネットワークに忍び込ませたい人などの不正行為者にとっても好都合です。USB は非常によく使用されているため、サイバー攻撃の機会も多くあります。コモディティドライブに伴うリスクは主に2つあります。

- **ランサムウェア攻撃：**これは USB を使用する攻撃で、マルウェアを企業ネットワークに侵入させ、企業の情報やシステムを暗号化して、元に戻すことと引き換えに金銭（身代金）を要求します。これは BadUSB が原因であることが多く、マルウェアの中でも特に目立つタイプとなっています。
- **データの盗難：**適切なセキュリティ対策をせずに紛失、盗難、放置されたドライブがひとつあるだけで、不正行為者は、顧客情報、ソースコード、機密性の高い財務および業績データなど、ドライブに保存されたデータに容易にアクセスできます。

BadUSB とは攻撃の一種で、保護されていないファームウェアの入った USB ドライブの脆弱性を悪用し、悪意あるソフトウェアでプログラムすることがあります。サイバー犯罪者にとってはこの悪意あるツールは非常に普及して入手しやすい一方で、ツールはまだ一般的にはそれほど知られていないため、この攻撃は非常に容易です。コモディティドライブのファームウェアをハッキングファームウェアと置き換えるだけで、USB ドライブがキーボードのふりをし、大抵はスクリプトを実行してファイアウォールを攻撃できます。多くのサイバー攻撃は、悪意があるかないかにかかわらず、社内の不用心な人によって実行されますので、企業が暗号化ドライブを使用することは非常に大切です。暗号化ドライブは、この攻撃を予防するため、保護されたデジタル署名付きファームウェアを活用しますので、サイバー犯罪者が成功するチャンスを減らします。

> インフラの再構築コストと、身代金要求や恐喝に払う金額は、USB の管理コストより巨額です。
> - David Clarke

暗号化 USB を使用する理由

暗号化ドライブは、ドライブの内部と、接続中のデバイスに保存されたデータを保護することに特化して設計されていますので、どんな組織の IT 備品としても価値の高いツールです。サイバーセキュリティ攻撃はますます巧妙化していますが、暗号化ドライブの機能を利用すれば、このデバイスを悪用したいサイバー犯罪者の先を行くことができます。Kingston IronKey™ ハードウェア暗号化製品シリーズのように、強力な XTS モードの AES 256 ビット暗号化、頑丈な改ざん防止ケース、デジタル署名付きファームウェア、仮想キーボード、複雑なパスワードまたはパスフレーズモードなどの機能が、ユーザーをあらゆる攻撃から完全に保護するため、長年にわたって開発され追加されています。

多くの企業では、サイバーリスクの理解が不十分であることが多く、コモディティドライブにはさまざまな脆弱性が伴うにも関わらず、それを採用してしまいます。脆弱性を高める要因には、入手しやすさ、低価格、ソフトウェア暗号化の使用の他に、フラッシュドライブの社内承認プロセスの不在などがあります。多くの場合、ISO27001、GDPR、SOC2、WISP 政府ベストプラクティスなどの各種 IT およびサイバーセキュリティ標準を順守するための、社内のベストプラクティスやプロセスもありません。そのため、リスクは証拠ではなく意見によって評価され、多くの企業が攻撃に脆弱なままになります。

一部では、既存のソフトウェア暗号化ツール付きのコモディティドライブを使用していますが、多くのソフトウェア暗号化ドライブはインターネット上で誰にでも入手できる無料または有料ツールでハッキングできてしまうため、結局はコスト節減になりません。ソフトウェア暗号化は、ユーザーが手間を省くため、またはサポートされていない OS プラットフォームでドライブを使用するために、ドライブを再フォーマットするだけでドライブから取り除くことができます。ハードウェア暗号化 USB の暗号化は常時有効で、無効にできないため、目的に合致しています。また、ドライブの真正性と完全性を保証するため、改ざん防止、開封防止構造で、デジタル署名付きファームウェアを使用しています。IronKey VP50 のような暗号化ドライブにはさらに、パスワード試行回数の制限（総当たり攻撃防止）と仮想キーボード（キーロギングおよびスクリーンロギングの防止）のふたつの機能が追加されており、不用心なユーザーからパスワードを引き出そうとする不正行為者への対策の業界ベストプラクティスに準拠しています。

> IronKey ドライブが、ファームウェアに改ざんが行われたことを検知すると、ドライブが作動不能になり、起動しないため、サイバーセキュリティが向上します。- Pasi Siukonen

リスクの高い人

実際に、USB のアクセスを管理できない企業はすべてリスクにさらされています。そして多くの場合、どんなリスクかさえ正確に認識していません。しかし、特定の企業がサイバー攻撃の魅力的で脆弱な標的になるには、要因があります。

医療および金融セクターの企業は、そのデータがサイバー犯罪者にとって非常に魅力的なだけでなく、組織や顧客に重大な影響を与えます。英国では 2017 年に国民保健サービス（NHS）を狙ったサイバー攻撃で、19,000 件以上の予約がキャンセルされ、成果が失われて 9200 万ポンドの出費となり、データとシステムの復旧にもコストがかかりました。これに影響を受けた患者が医療サービスを利用できなかっただけでなく、NHS は、事前のサイバー攻撃警告に対して、迅速かつ十分な対応ができなかったことで多くの批判を浴びました。すべての企業にサイバーセキュリティに関して最新かつ良質な情報を得ている必要がありますが、とりわけ特殊な分野のデータなど、機密性の高い情報を取り扱う組織は、サイバーリスクに関する警戒を倍増する必要があります。

総被害額で測った場合の企業の価値が高いほど、不正行為者の報酬も大きいため、企業がサイバー攻撃で直面するリスクも大きくなります。しかしこれは、小規模な企業がサイバーセキュリティに無関心でもよいという意味ではありません。大企業は攻撃側に魅力ある標的ですが、サイバー攻撃に対応するリソースと専門スタッフも持っています。一方、多くの中小企業（SMB）には、専門のサイバーセキュリティチームがなく、上級管理職が USB 管理の例外にされやすいため、深刻な被害を特に受けやすい傾向があります。いくつかの調査では、実際に中小企業がサイバー攻撃の標的になることが多いと示されています。

上級管理職の地位にある従業員のリスクはさらに高くなります。このような人々は追跡しやすく、多くの場合、社内で重役特権がありますので、USB 管理手続きなどのサイバー対策が適用されず、サイバー犯罪者にとっておいしい獲物になりやすいからです。この点で、常時有効な暗号化ドライブを使用し、サイバーセキュリティに対する適切な情報を徹底させ、ベストプラクティスおよびプロセスに従うことには、リスクを軽減し、攻撃から保護する大きな効果があります。

> 最近の侵入の多くは、社内の人に進んで、または知らないうちに手伝わせることが得意な不正行為者によって行われています。- David Clarke

リスクの高い人

> 企業や組織は十分なサイバーセキュリティ攻撃対策を行っていません。 - David Clarke

企業にとって、サプライチェーンはもうひとつの潜在的に脆弱な個所であり、サプライチェーンへの攻撃は非常によく発生しています。2013 年に、米国の小売業者の Target が、小売業界史上有数の規模のデータ漏洩の被害を受け、4000 万人以上の顧客のデビットカードおよびクレジットカードの情報が流出しました。Target 自体はサイバーセキュリティへの関心が高く、攻撃の 6 か月前に大規模なサイバーセキュリティシステムを導入したばかりでしたが、攻撃者は Target のサードパーティサプライヤに潜入し、そこから Target のメインデータネットワークへのアクセスに成功しました。Target に対して合計 90 件の訴訟が起こされ、同社は漏洩への対応で 6100 百万ドルを失いました。同社はこの攻撃に直接の責任がなかったものの、サプライチェーンのサイバーセキュリティにこのような弱点があるだけで、財務と企業イメージの両面で傷つきました。

従業員が煩雑な操作の抜け道を探すことも、脆弱性の原因になります。このような抜け道では、従業員が日常業務の生産性を上げることはできますが、多くの場合、パスワード管理などの基本的なセキュリティプロセスやベストプラクティスを見過ごしがちです。NCSC や CISA のガイダンスは十分に明快ですが、多くの場合、特に IT やサイバーセキュリティをよく知らないチームメンバーにとって、実際に施行することは大変です。専門のサイバーセキュリティチームはもちろん役に立ちますが、ハードウェア暗号化ドライブなどの適切なツールを従業員に配布することは、従業員の抜け道探しのリスクの軽減にたいへん有効です。

> 最近のハードウェア暗号化 USB ドライブは、既存のサイバーセキュリティポリシーへの適応や統合がしやすく、各種インターフェイス（グラフィック、キーパッド、タッチスクリーン）から幅広いオペレーティングシステムまでをサポートし、あらゆる組織のニーズに対応する容量があります。
> - Pasi Siukonen

組織がサイバー攻撃のリスクを軽減する方法

組織から見れば、エンドポイントを保護し、データを保護するために実行できることはたくさんあります。GRC（ガバナンス、リスク、コンプライアンス）サイバーセキュリティが不十分の場合、失敗しやすいため、プロセスをよく知って従うことが、企業が自己防衛をする上でますます重要になっています。堅牢なエンドポイントセキュリティソフトウェアを導入することでも、多くのサイバー攻撃を無力化できます。ただし、セキュリティ脆弱性の修正にできるだけ迅速に対応する必要があります。

> 強制的な暗号化ポリシーを採用するかどうかは、データのバックアップ実行を選択するかどうかにも関連するため、リスク管理にとって非常に重要な問題です。
> - Pasi Siukonen

しかし個人レベルでは、暗号化ハードウェアによってサイバーセキュリティ攻撃に対する脆弱性は大幅に軽減します。リモートおよびハイブリッドワークが普及し持続していることや、特に昨年のサイバー攻撃が増加したことによって、企業のあらゆる階層の従業員が企業データを確実に安全に取り扱い、転送し、読み取ることが、今まで以上に大切になりました。ユーザーはハードウェア暗号化 USB を使用することによって、持ち運びやすさや簡単操作などのフラッシュドライブの利点を活用し続けられるだけでなく、データ、金銭、企業イメージなどの損失のリスクを大幅に軽減できます。ハードウェア暗号化ドライブは、さまざまな攻撃から機密データを保護するように設計されています。サイバー犯罪者は新しい攻撃方法を編み出すに従って、暗号化ドライブもそれらの新しい課題に対応するように進化します。

サイバー攻撃対策の総コストは多額になる場合もあります。実際に、全社的な暗号化ドライブの採用と使用には、関与度の高い承認とセットアップが必要ですが、恐喝関連コストや、企業イメージ低下による売上損失などの金銭的な節約も長期的には大きい場合があります。漏洩の場合の訴訟関連コストだけでも、ハードウェア暗号化 USB ドライブによるコスト増加分を回収できます。

> Kingston のポートフォリオでは、優れた暗号化 USB ソリューションを提供するために長期的に尽力していますので、企業は、業界標準の強化ハードウェア暗号化、エンドポイントポリシー準拠の設計、デバイス管理機能などのセキュリティの構成に対応できます。- Pasi Siukonen

結論

Kingston では常にサイバーセキュリティ分野の開発に努力し、IronKey 暗号化ドライブを最新の要件に確実に適合させ、規模の大小を問わず企業や組織のサイバーセキュリティのニーズに対応しています。サイバーセキュリティはますますグローバルな関心事になっていますが、弊社では企業が適切なツールと知識を自由に活用することで、今後の課題に対応する態勢を十分に整えながら、企業自身と従業員と顧客を守ることができると確信しています。

Kingston について

35 年以上の実績を持つ 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。

#KingstonIsWithYou

1. https://www.techtarget.com/searchsecurity/news/252516423/Sophos-66-of-organizations-hit-by-ransomware-in-2021