

Kensington®

# VeriMark™ 指紋認証キー およびセキュリティキー

多要素認証とサイバーセキュリティに  
おける信頼できるブランド



## 素早く安全なアクセス

指紋認証キーと NFC セキュリティキーは、私たちのデジタル環境を保護する方法を刷新します。指紋認証キーは、ユニークな生体データを使用してパスワードなしで迅速かつ信頼性の高い認証を提供し、不正アクセスを防止します。NFC セキュリティキーは、特に PC とモバイルデバイスの両方を使用する環境において、便利さと柔軟性を提供することができます。シンプルな使用方法により、他の生体認証 オプションより低コストで導入可能です。これらのツールは、使いやすく、高い安全性を有し、機密情報を安全に保ちながら、あなたの作業を遅らせることなく設計された強力な多要素によるデータ保護を提供します。

## よくある質問

- 使用事例に見られる**セキュリティキー導入の目的**は何ですか？
- 対応するデバイスまたは **ブラウザー**はありますか？
- **Windows Hello** または **Windows Hello for Business** またはウェブ認証で利用できますか？
- ユーザーは単一または **複数** のデバイスにアクセスしていますか？
- **複数** のユーザーが、1 日の異なる時間に **同じデバイス** にアクセスしますか？
- どの **サービス** が使用されていますか？



## 業界のトレンドと研究のインサイト

### デバイスセキュリティの現状

ケンジントンは、物理的ハードウェアセキュリティを担当する 1,000 人のシニア IT 担当者を対象に、独立市場調査会社 Vanson Bourne によって実施された調査をサポートしています。1 つの重要な発見は、43% の回答者がデバイス上の会社データへの不正アクセスを最大の懸念としていることでした。次に、19% が不安定な家庭用ネットワークによる機密データの漏洩を懸念しています。セキュリティの脅威を軽減するために、生体認証または多要素認証を重要視する回答者が 30% いる中で、マルチファクター認証(MFA)を主な対応策として利用する組織も増加しています。

### 生体認証ソリューションの使用

より多くの組織が生体セキュリティソリューションの価値を認識しています。私たちの市場調査によると、回答した組織の 71% が現在、指紋認証キーまたはセキュリティキーを使用して二要素認証(2FA)を行っており、さらに 26% が近い将来にこれらの対策を実施する予定と回答しています。Kensington の VeriMark™ 製品は、パスワードレスの便利さと企業レベルの安全性を組み合わせた最先端の生体セキュリティを体現しています。現代の職場を守るリーダーとして、Kensington は TAA および GDPR に準拠したソリューションを提供し、既存のインフラに統合することで、組織が進化するサイバーセキュリティの脅威に効果的に対処できるようにします。

出展: Vanson Bourne, Device Security Research, October-November 2024

## VeriMark™ IT 2.0 による強化されたセキュリティと便利さ VeriMark™ Desktop 2.0



VeriMark™ IT 2.0 および VeriMark™ Desktop 2.0 の生体認証キーは、Windows Hello とシームレスに統合され、強化されたセキュリティと迅速で便利なアクセスを提供します。Microsoft の強化サインインセキュリティ(ESS)要件に完全に準拠しており、高度な指紋認識と最新の Windows 認証基準を組み合わせています。VeriMark™ IT 2.0 および VeriMark™ Desktop 2.0 は、安全なログイン、暗号化、オンライン保護を確保し、敏感なデータを保護しながら、シンプルなタッチでアクセスを簡素化するため、現代の IT 環境に最適です。

### 安全な認証

生体認証は、各ユーザーに固有の指紋を使用するため、非常に安全な認証方法です。

### 紛失リスクの低下

パスワードとは異なり、ユーザーは生体認証データを忘れたり紛失することはありません。

### 迅速で便利なアクセス

タッチするだけで数秒で認証可能—タイピングも不要。

## VeriMark™ Guard 2.1 によるウェブセキュリティの向上



VeriMark™ Guard 2.1 のような指紋およびセキュリティキーは、強化された保護を必要とするウェブサービスにアクセスする際の多要素認証(MFA)に最適です。FIDO® 認証ソリューションとして、生体認証または PIN 入力とハードウェアベースの認証を組み合わせ、強力なフィッシングに強いセキュリティを提供します。金融プラットフォーム、企業アプリケーション、または機密クラウドアカウントに最適な VeriMark™ Guard 2.1 は、堅牢なログイン情報の盗難に対する防御を行い、迅速でシームレスなユーザー体験を提供します。

### 高い安全性

セキュリティキーは、非常に複製や偽造が難しい強力な暗号認証を使用しており、フィッシングやソーシャルエンジニアリング攻撃に対して抵抗力があります。FIDO2、U2F、CTAP 2.1 認証デバイスとして、厳格な規制要件(HIPAA や PCI DSS など)を満たすのに役立つ最新のハードウェアベースのセキュリティ基準に対応しています。

### 使いやすさ

セキュリティキーはシンプルで使いやすく、最小限の設定で済むため、ユーザーにとって便利な選択肢です。

## パスワードなしでエンタープライズグレードのセキュリティにアクセスする



VeriMark™ NFC+ セキュリティキーは、シンプルでありながら強力なデバイス間のアクセスを提供します。ワイヤレスの便利さと堅牢な暗号化を組み合わせ、ユーザーはキーを挿入した状態でタップするか、NFCリーダーに対してキーをタップすることで認証できます。このセキュリティキーは生体認証の登録を必要とせず、共有ワークステーションでの使用や迅速なセットアップに最適です。フィッシングに強い技術と FIDO® 認証により、費用対効果の高い価格でエンタープライズグレードのセキュリティを提供し、使いやすさと企業コンプライアンスを両立させます。

### Windows Hello との統合

VeriMark™ Access は、シンプルな Plug-and-Play の指紋認証キー設定で、迅速なパスワードレスの Windows サインインを可能にします。セキュリティキーが利用できない場合、VeriMark™ Companion モバイルアプリが安全なバックアップとして機能し、アクセスを確保するためワンタイムパスワードを生成します。このソリューションは、迅速でシームレスなユーザー切り替えを必要とするマルチユーザー環境にも対応しています。

### FIDO2 機能

FIDO2 レベル 2 に認証され、CTAP2.1 をサポートするこれらのキーは、Windows、macOS、iOS、Android を含む主要なプラットフォームやブラウザで動作します。このセキュリティキーは、パスワードレスセキュリティを採用する企業向けに拡張可能なソリューションを提供します。

## 必要なとき、必要な場所、必要な方法でのセキュリティ



### 企業への展開

VeriMark™ 製品は、システム拡張が必要な企業のシステム導入のために設計されており、パスワードレス認証を実装するためのシンプルで費用対効果の高い方法を提供します。オペレーティングシステム、ブラウザ、アイデンティティプラットフォーム全体での広範な互換性を持つ VeriMark™ 製品は、既存の IT 環境にシームレスに統合することができます。基幹システムをサポート、FIDO2 および業界基準を満たし、複雑になることなくフィッシング耐性のあるセキュリティを提供します。

### GDPR および TAA 対応

GDPR、BIPA、CCPA などのプライバシー法および規制に一致するサイバーセキュリティ対策をサポートするために使用できます。米国での連邦政府機関の基準にも対応。連邦政府機関および組織にも導入可能です。

### 互換性

VeriMark™ 指紋およびセキュリティキーは、広範な互換性を考慮して設計されており、複数のプラットフォームおよびサービスで安全なパスワードレス認証を提供します。このクロスプラットフォーム機能により、VeriMark™ は便利さを損なうことなく、強力なフィッシング耐性のあるセキュリティを求める企業や個人にとって理想的なソリューションとなります。

## 主な強み 指紋 セキュリティ キーの



### 生体認証によるアクセスのコントロール

際立った利点は生体認証の所持していることだけでなく、ユーザーの指紋が一致する必要があることです。これにより、生体認証キーが紛失または盗難に遭った場合のリスクが大幅に低減されます。指紋を登録された者のみが生体認証キーの暗号解除をアクティブに行うことができます。

### 1つのデバイスに統合された MFA

指紋キーは、あなたが持っているもの(生体要素)とあなたが持っているもの(所持要素)を組み合わせます。実際には、指紋スキャンがユーザー確認ステップとして機能し、ログイン時に別の PIN やパスワードを必要としなくなります。これにより、1つのアクションでキーを解除し、認証を行いながら、複数の強力な認証要素を強制するスムーズなサインイン体験が生まれます。

### ユーザーの利便性とスピード

多くの人にとって、指紋を使用することはパスワードを入力したり、OTP コードのためにスマートフォンを確認するよりも迅速です。よく設計されたキーを使用すれば、指紋スキャンはほぼ瞬時に行われます。

### 視覚的 / 触覚的フィードバック

生体認証キーは、指紋が受け入れられたときにフィードバック(LED インジケータのような)を提供することが多く、信頼感を与えます。キーがあなたを積極的に確認したことを知ることで、安心感が得られます。

## VeriMark™ 指紋キーの主な利点

**バイOMETRICS セキュリティ:** 登録ユーザーのみがアクセスできます。

**迅速なログイン:** Touch & Go - タイピング不要。

**高いフィッシング耐性:** ハードウェアベースの認証。

**ポータブル:** 複数のデバイスで使用できます。

**基準:** GDPR に対応し、TAA に準拠しています。



## 主な強み USB NFC のセキュリ ティキー



### デバイス間の互換性

NFC 対応キーの大きな利点は、PC とモバイルデバイスの両方でシームレスに動作することです。キーを USB ポートに接続し、NFC を介してスマートフォンやタブレットにタップしてワイヤレスで認証できます。

### モバイルにおける使いやすさ

スマートフォンに USB ポートがない場合やケースが付いている場合、スマートフォンなどのデバイスでセキュリティキーを使用するのは難しいですが、NFC がその問題を解決することができます。スマートフォンにキーをタップすることは素早く行うことができ、非常に短い距離(数センチメートル以内)で通信するため、便利で安全です(傍受が難しいため)。

### 共有またはユーザーローテーション環境に最適

NFC キーは指紋を保存せず、個別の生体認証設定を必要としないため、複数の人がアクセスする必要がある環境(フロントラインの現場、研究所、または製造フロアなど)に最適です。

### 強力なセキュリティ

NFC キーは、他のハードウェアキーと同じ高レベルの暗号化セキュリティを維持します。NFC 自体は近距離通信のために設計されており、盗聴のリスクを大幅に制限します(攻撃者は使用中に物理的に数インチ以内にいる必要があるため)。

## VeriMark™ NFC+ セキュリティキーの主な利点

**デュアルインターフェース:** USB と NFC の両方で動作し、柔軟なデバイスアクセスを提供します。

**フィッシング耐性のセキュリティ:** フィッシングや資格情報の盗難に対するハードウェアベースの保護

**FIDO2 レベル 2 認証:** パスワードレス認証のための業界最高基準を満たし、CTAP2.1 に対応しています。

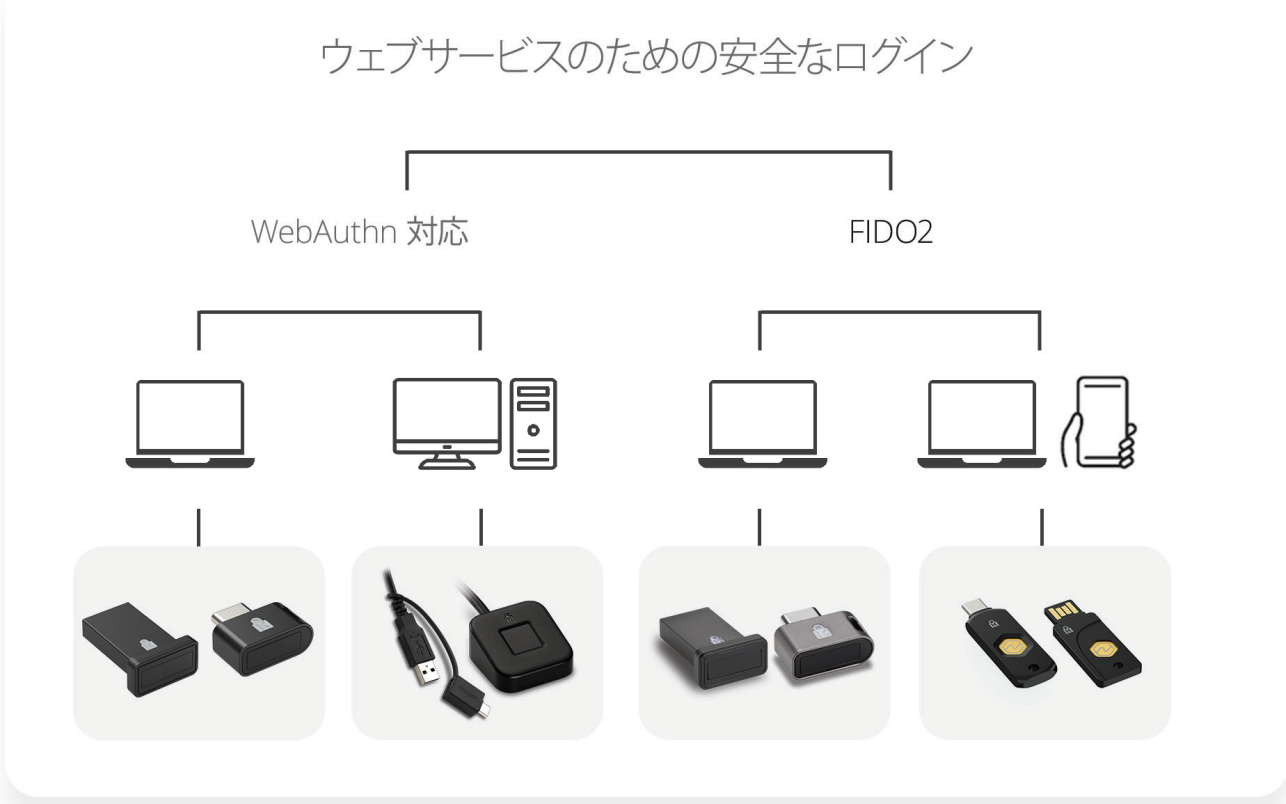
**クロスプラットフォーム:** Windows、macOS、Android、iOS、および主要なサービスとブラウザに対応しています。

**生体認証の設定は不要:** 迅速に展開可能—指紋登録は不要です





<b>Windows Hello</b>			非対応	ネイティブにはサポートされていませんが、ソフトウェア (VeriMark™ Access)を通じてアクセス可能です。 + 付属のモバイルアプリ
<b>Microsoftの強化サインインセキュリティ</b>	Windows 11 を通じてサポートされています。	Windows 11 を通じてサポートされています。	非対応	非対応
<b>FIDO2 &amp; FIDO U2F</b>	非対応	非対応	 FIDO2 レベル 1	 FIDO2 レベル 2
<b>CTAP</b>	非対応	非対応	CTAP2.1 をサポートし、CTAP2.0 との互換性があります	CTAP2.1 をサポートし、CTAP2.0 との互換性があります
<b>デバイス</b>				
<b>オペレーティングシステム</b>				
<b>Google, Amazon, Apple, Microsoft のサービス</b>				
<b>ウェブサービス</b>				
<b>パスワードマネージャー</b>				





VeriMark™ IT 2.0  
指紋キー



VeriMark™  
デスクトップ 2.0  
指紋キー



VeriMark™  
Guard 2.1 指紋  
セキュリティキー



VeriMark™ NFC+  
セキュリティキー

項目 #	USB-C® : K64705WW USB-A : K64740WW	K64741WW	USB-C® : K65051WW USB-A : K65050WW	USB-C® : K64739WW USB-A : K64738WW
認定	 Windows Hello <small>Microsoft Enhanced Sign-In Security (ESS)</small>	 Windows Hello <small>Microsoft Enhanced Sign-In Security (ESS)</small>	 FIDO U2F FIDO2	 FIDO U2F FIDO2
オペレーティングシステム				
キータイプ				
接続タイプ	USB-C® または USB-A	USB-A と USB-C® アダプター	USB-C® または USB-A	USB-C® または USB-A と NFC
Windows Hello	対応	対応	非対応	ネイティブにはサポートされていませんが、ソフトウェアを通じてアクセスできます (VeriMark™ Access)
FIDO	WebAuthn 互換	WebAuthn 互換	FIDO U2F および FIDO2 レベル 1 認証済み	FIDO U2F および FIDO2 レベル 2 認証済み
CTAP	N/A	N/A	CTAP2.1 プロトコルに 対応	CTAP2.1 プロトコルに 対応
パスキー	生体認証を通じて 互換性があります	生体認証を通じて 互換性があります	生体認証を通じて 互換性があります	NFC または Tap-and-Go を通じて 互換性があります
指紋認証タイプ	Match-in-Sensor™	Match-in-Sensor™	Match-in-Sensor™	N/A
データスコア	キーの指紋テンプレートデータ	キーの指紋テンプレートデータ	キーの指紋テンプレートデータ	N/A
本人拒否率	2%	2%	2%	N/A
他人受入率	0.001%	0.001%	0.001%	N/A
可読性	365 度	365 度	365 度	N/A



VeriMark™ NFC+ USB-C® セキュリティキーは、ウェブベースのサービス全体でデジタルセキュリティを強化するために設計されています。この NFC 対応 USB-C® セキュリティキーは、FIDO2 レベル 2 の認証を受けており、一般ユーザーと企業ユーザーの両方に対して安全で便利なクロスプラットフォーム認証を提供します。ハードウェアベースの MFA を使用してパスワードの脆弱性を排除することで、フィッシングやアイデンティティ盗難に対する企業レベルの保護を提供します。

- FIDO2 レベル 2 認証済みセキュリティ
- FIDO C TAP2.1 プロトコルサポート
- USB-C® + NFC デュアルインターフェース
- シンプルさと補完的なソフトウェア
- クロスプラットフォームの互換性
- コンパクトでポータブル



他にも利用可能



より詳しい情報はこちら  
[kensington.com/solutions/product-category/why-biometrics/](https://kensington.com/solutions/product-category/why-biometrics/)

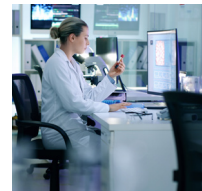


## 指紋キー – 理想的な使用ケースと目的

指紋キーは、生体認証とハードウェアベースのセキュリティを組み合わせています。個々のアイデンティティの保証が重要な環境に最適です。

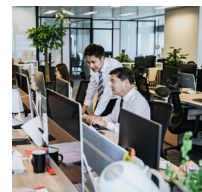
## NFC キー – 理想的な使用ケースと目的

NFC キーは Tap-and-Go 認証を提供し、モバイルファースト、マルチユーザー、または消費者向けの環境に最適です。



### ヘルスケア

- 患者記録への安全なアクセス(HIPAA 準拠)。
- 医療機器や端末への不正アクセスを防止します。
- 共有ワークステーションを使用する臨床医のための生体認証ログイン。



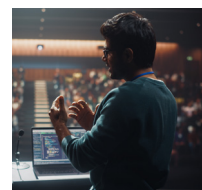
### 金融と銀行業

- 取引プラットフォームや金融ダッシュボードへの安全なアクセス。
- 高リスク環境での資格情報の盗難を防止します。
- 規制要件を満たします(例:PCI-DSS、GDPR)。



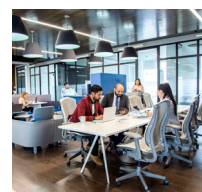
### 政府および公共部門

- 連邦機関で生体認証 MFA に使用されます。
- FIDO2 および Windows Hello for Business に対応しています。
- TAA 準拠のハードウェアを必要とする機関に最適です。



### 教育

- 教師やスタッフは安全なログインのために指紋キーを使用します。
- 共有コンピュータラボでの不正アクセスを防ぎます。



### 企業 IT

- 特権アクセス管理に使用されます。
- パスワードリセットによるヘルプデスクの負担を軽減します。
- 監査証跡と集中アクセス制御をサポートします。



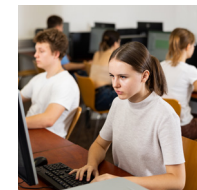
### 小売および販売時点

- POS 端末のためのタップ認証。
- スタッフアカウント間の迅速な切り替え。
- 不正な取引を防ぎます。



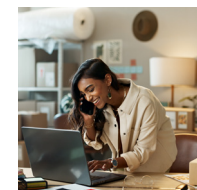
### 輸送および物流

- ドライバーは NFC キーを使用してルート計画ツールにアクセスします。
- フリート管理システムへの安全なログイン。
- 過酷な環境に最適(IP68 防水等級)。



### 教育

- 学生は共有デバイスにログインするためにタップします。
- IT 管理者は、生体認証の登録を必要とせずにアクセスを管理します。



### 消費者および中小企業

- 個人デバイスのためのパスワードなしログイン。
- 非技術者向けの簡単なセットアップ。
- Apple ID、Google、Microsoft などと互換性があります。



### 公共部門 - 現場作業

- モバイルワーカーのための Tap-and-Go ログイン。
- 指紋登録や PIN の暗記は不要です。
- オフラインで、かつプラットフォームを超えて動作します。



すべての仕様は、予告なしに変更される可能性があります。お住まいの地域によっては製品を販売していない場合があります。Kensington® および Kensington, The Professionals' Choice™ は ACCO Brands の商標です。その他の登録商標 および未登録の商標は、それぞれの所有者の財産です。© 2026 Kensington Computer Products Group, a division of ACCO Brands. k26\_4506

問い合わせ先 : 1-855-692-0054 | [sales@kensington.com](mailto:sales@kensington.com)

# Kensington

The Professionals' Choice™