SAMURAI Key

エンドポイント端末の認証や
データ安全性の向上ソリューション

パスワードレスで簡単にアクセスができ、アカウントの不正利用防止
さらにデータ暗号化機能搭載し、USBメモリとしてもセキュリティー力が高い
アカウント保護とデータセキュリティの完璧な組み合わせ「SAMURAI Key」

企業が直面しているエンドポイントのデータ漏洩課題

ランサムウェア

デバイスの紛失か盗難

フィッシング詐欺
などからの不正アクセス

内部からのリスク

SAMURAI Key による不正アクセスの防止

認証情報、本人確認の手段によって、知識、所持、生体認証三つの種類があります。
SAMURAI Key は、「所持」の物理認証器です。弱点となりうるパスワード、SMS 認証などの代替案として、クラウド、Web サービス、さらに PC にパスワードレスにログインできます。
多要素認証の第二認証要素とする場合、SAMURAI Key がなければ、パスワードを手に入れていても、アカウントにログインできません。パスワード漏洩によるハッキングリスクと大きな損失を防ぐことができます。

これ以上、SAMURAI Key は軍事レベルの暗号化機能、隠し領域の設計、またカスタマ可能な企業管理機能により、企業と個人の機密データを堅牢な安全性を提供します。

より安全に
不正アクセスと情報漏洩を防止
企業サーバーに経由して管理可能

より便利で
複数のサイトやクラウドで、
認証キー一つでアクセス可能

より快適に
複雑なパスワードへの依存を減らす
ユーザーの導入手順が簡単

製品特徴

1. パスワードレス認証で簡単アクセス

※　FIDO2 Level 2 に準拠中。

SAMURAI Key がなければ、パスワードを手に入れていても、アカウントにログインできません。パスワード漏洩によるハッキングリスク、大きな損失を防ぐことができます。

✓ パスワード漏洩、フィッシング詐欺などによる不正利用を防げます。

✓ Google、Microsoft、GitHub、Dropbox、Twitter、AWS、Azure、Facebook、One password、仮想通貨取引所など、百個以上のアプリケーションの認証強化が可能です。

※ FIDO 機能の使用状況は各サービスによって異なります。

✓ パスワードレス標準の FIDO2 Level 1 に準拠しました。

✓ Microsoft Entra ID（旧名Azure AD）を利用する Windows PC の認証を強化可能です。

2. 軍事レベルのデータ保護

最強のハードウェア ＆ AES 256 暗号化

✓ 現在最強の暗号アルゴリズム AES 256 bit によりディスク領域を暗号化。

✓ 悪意あるプログラムに攻撃されても、解読できません。

✓ 暗号鍵を CC EAL5+（軍事レベル）に準拠したセキュリティーチップで保護します。

紛失や盗難にあっても心配ありません

✓ 暗号秘密領域を表示させるには本人だけが知っている PIN コードを入力する必要 があります。

✓ SAMURAI Key を PC に挿すだけではディスク領域は表示されません。

※決まった手順が必要です。

3. 企業管理機能をカスタマ可能

企業サーバに経由して管理可能なカスタム版については、現在 OEM、ODM を承ります。

✓ 管理者によるリモートロック

✓ ログ管理

✓ ローカルデータの暗号化

✓ その他

製品名	Blentity - FIDO2 with Data Protector（SAMURAI Key）
接続方法	Type-C、Type-A（アダプタが付属）
読み書き速度	R：140MB/s　W：45MB/s
転送速度	USB 3.2 Gen1 (5Gbps)
暗号化アルゴリズム	Hardware-based AES XTS
寸法	76 x 20.5 x 10 mm
対応 OS	Windows 10 (バージョン21H2) 以降 / Mac OS Ventura 以降 / Linux は今後サポート予定です（Ubuntu バージョン開発中）
認証（進行中）	CE FC VCCI

本製品は OEM、ODM を承ります。お気軽に連絡してください。

お問い合わせ：info@wisecure-tech.jp

WEBサイト：https://wisecure-tech.jp