RESOURCE CENTER

エンド・ツー・エンドの暗号化が知識ゼロへの道を開く – ホワイトペーパー

Bitwarden、ゼロ知識暗号化によるパスワード管理を実現

Get the full interactive view at
https://bitwarden.com/ja-jp/resources/zero-knowledge-encryption-white-paper/

bitwarden

As more of our daily and professional lives move online, both personal and company security depends on all of us. Cyber attacks and data breaches unfortunately continue, with password management often cited as an easy step to mitigate risk.

But how can you trust a company to keep all of your secrets secret? The answer lies in end-to-end encryption, which lays the groundwork for applications with 'zero knowledge' architectures.

In a recent article on Tech Radar, author Christian Rigg noted,

> Zero knowledge refers to policies and architecture that eliminate the possibility for a password manager to access your password.

While this is a perfect explanation of zero knowledge for a broad audience, security experts will differ in the interpretation of zero knowledge. We know we want zero knowledge in terms of safely handling encrypted passwords with password managers, but what exactly does that mean?

強力なエンドツーエンドの暗号化から始める

セキュアなアーキテクチャーの基礎は、暗号化、特にエンド・ツー・エンドの暗号化から始まる。ビットワーデンでは、
お客様がビットワーデンクライアントに機密データを入力すると、すぐに暗号化します。データをデバイスに保存する前に、暗号化されます。
暗号化されていないVaultデータというものは存在しません。ただし、
Bitwardenクライアントで電子メールアドレスとマスターパスワードを入力し、情報を閲覧している場合は例外です。

そこから、すべてのVaultデータは、Bitwardenクラウドまたはセルフホスト Bitwardenサーバーに送信される際も暗号化されたままです。
他のクライアントとデータを同期する際、固有の電子メールアドレスとマスターパスワードが再入力されるまで、
データは暗号化されたままです。

つまり、Bitwardenはお客様のパスワードを見る**ことが**できず、
お客様の電子メールとマスターパスワードによってエンドツーエンドで暗号化されます。マスターパスワードは保存されず、
アクセスすることもできません。

データ保管庫のデータには、Bitwardenは業界標準のAES 256ビット暗号を使用しています。マスターパスワードには、PBKDF2 SHA-256が使用され、Vaultデータを暗号化する鍵が導き出されます。Bitwardenのセキュリティについて詳しくは、
セキュリティFAQをご覧ください。

当然のことながら、エンド・ツー・エンドの暗号化で重要なのは、復号化するための鍵である。これがエンド**ユーザーのみに**留まる限り、
ソリューションは知識ゼロのアーキテクチャーへと進むことができる。

ソフトウェアやサービス・プロバイダーが暗号化を推進しながらも、キーを保持するケースもある。このようなケースは、
ソフトウェアやサービス・プロバイダーが技術的にデータを解読する能力を持っているため、我々の観点からはゼロ知識とは認められない。

Give users key control for zero knowledge encryption

When users have control of the encryption key, they control access to the data, and can provide encrypted data to a password manager without the password management company having access to, or knowledge of, that data.

This is the fundamental premise on which well-designed password managers work. They facilitate strong and unique passwords that only you can access. Doing so requires zero knowledge of the secret data, and therefore users must control the encryption key. We refer to this as zero knowledge encryption.

But there is information beyond the secret Vault data that might be shared with a software or service provider. For example, an email address might serve as a unique customer identifier. One could claim that this isn't zero knowledge, and that would be correct.

At a minimum, zero knowledge must pertain to secret data. In the case of a password manager, that means all information within the password Vault. At the same time, it is important to recognize the realities of software, services, and users, and that in order for a commercial relationship to exist, their likely needs to be some knowledge exchanged between parties.

In the world of password managers, that line can get blurry. For example there are some password managers (not Bitwarden) that retain unencrypted URLs and websites for which you store passwords. While they claim that this benefits users, ultimately it provides these companies with detailed information on which websites users visit, when they do so, and every log in.

Bitwarden takes a more conservative view of what constitutes sensitive data, and therefore encrypts all of the information in your Vault, including the websites you visit, even the names of your individual items and folders. We use the term zero knowledge encryption because only you retain the keys to your Vault, and the entirety of your vault is encrypted. Bitwarden cannot see your passwords, your websites, or anything else that you put in your Vault. Bitwarden also does not know your Master Password. So take good care of it, because if it gets lost, the Bitwarden team cannot recover it for you.

Zero trust as a protective mindset

The zero trust model initially emerged as a way for organizations to get beyond the traditional thinking of internal and external threats to their IT operations. Today, companies need to protect from threats coming from both inside **and** outside. Zero Trust models often use technologies like identity and access management, encryption, multi-factor authentication, and permissions to operate.

Of course, between password managers and users adopting software or services, there is likely going to be at least **some** element of trust between the two parties. The password management provider trusts that the user will not violate the terms of service, and the user trusts that the password management provider will live up to their stated offering. However, everyone is better off if the boundaries of required trust are limited, so that even the possibility of sensitive data being compromised is eliminated altogether, hence the zero trust model.

While we stand by to support our customers with a trusted relationship, we can reduce the reliance on implied trust through the Bitwarden self-hosted offering. This deployment enables businesses with greater flexibility and control over their infrastructure. Running your own Bitwarden instance could be on an airgap network, further reducing risks by being disconnected from the internet.

At Bitwarden we take this trusted relationship with our users seriously. We also built our solution to be safe and secure with end-to-end encryption for all Vault data, including website URLs, so that your sensitive data is "zero trust" secure.

Understand and adopting safe encryption practices

We want our users to be well-informed on security practices in general, and with the benefits Bitwarden provides. With encryption, seek a complete end-to-end encryption architecture where only the end user retains the key, and make sure all sensitive data is encrypted using that architecture.

For many, it is easier to understand zero knowledge than end-to-end encryption, and we like easy! But we also understand the intricacies of these terms and aim to maintain clear definitions. We hope this article helps clarify our philosophy and approach.

知識ゼロの暗号化ソリューションを今すぐ試してみたい方は、こちらから無料のBitwardenアカウントにサインアップできます。