bitwarden | ヘルプセンターの記事

PASSWORD MANAGER > BITWARDEN SEND

暗号化を送信する

ヘルプセンターで表示:
https://bitwarden.com/help/send-encryption/

暗号化を送信する

Sendsは、プレーンテキストやファイルを含む、誰にでも敏感な情報を送信するための安全で一時的なメカニズムです。「Sendについて」の記事のメモによれば、Sendは**エンドツーエンド暗号化**されているということです。つまり、暗号化（以下で説明）と復号化はクライアント側で行われます。あなたがSendを作成するとき：

1. 新しい128ビットの秘密鍵がSendのために生成されます。
2. HKDF-SHA256を使用して、秘密鍵から512ビットの暗号化キーが導出されます。
3. 派生キーは、ファイル/テキストデータとメタデータ（名前、ファイル名、メモなど）を含むSendをAES-256で暗号化するために使用されます。

> **Tip**
> Sendを保護するために使用されるパスワードは、Sendの**暗号化や復号化には関与していません。**
> パスワードは純粋に認証方法であり、パスワードで保護されたSendは、
> パスワードの認証が成功するまで復号化からブロックされます。

4. 暗号化されたSendは、
   BitwardenがSendの復号化のために識別するための一意のIDを含むBitwardenのサーバーにアップロードされますが、
   暗号化キーは**含まれません。**

解剖学を送る

Sendsは、ユニークなSend IDと派生した暗号化キーから構築されたSendリンクを開くことで復号化されます。

```
https://vault.bitwarden.com/#/send_id/encryption_key
```

これにはいくつかの要素が含まれています：

コンポーネント	例
プロトコル	https://
ドメイン	vault.bitwarden.com
アンカー/フラグメント/ハッシュ	アンカー/フラグメント/ハッシュは、URLのsend idとsend keyを含んでいます。 例のリンクでは、これは`#/send_id/encryption_key`として表されています。

アンカー/フラグメント/ハッシュはサーバーに送信されません。この情報は、ブラウザ内でローカルに使用され、IDを識別し、Sendを復号化します。

復号を送信します

Sendリンクにアクセスするとき：

1. ウェブブラウザは、Bitwardenサーバーから Sendアクセスページを要求します。

2. Bitwardenサーバーは、ウェブ保管庫クライアントとしてSendアクセスページを返します。

3. ウェブ保管庫クライアントは、Send IDと暗号化キーを含むURLフラグメントをローカルで解析します。

4. ウェブ保管庫クライアントは、解析されたSend IDに基づいてサーバーからデータを要求します。
   暗号化キーは**決して**ネットワークリクエストに含まれません。

5. Bitwardenサーバーは暗号化されたSendをウェブ保管庫クライアントに返します。

6. ウェブ保管庫クライアントは、暗号化キーを使用してSendをローカルで復号化します。

> **Tip**
> あなたのSendがパスワードで保護されている場合、Sendの復号化は**認証によってブロックされます**。
> サーバーはパスワードを検証し、パスワードが正しい場合のみSendを返します。これは、
> 復号化に使用されるパスワードと混同してはなりません。

セキュリティを送る

Bitwarden Sendリンクを送信する際に、追加のセキュリティのために取ることができるオプションの手順があります:

1. Sendにパスワードを追加し、パスワードを別のチャンネルで共有してください。

2. キー（最後のスラッシュより前のすべて）を除いたリンクをSendし、キーは別のチャンネルでSendしてください。

3. 上記の両方のオプションを活用してください。

> **Tip**
> Send URLを再構築するときは、Send IDと暗号化キーの世界を含めるようにしてください。
>
> 例: `https://vault.bitwarden.com/#/send/send_id/encryption_key`