### ntfs-mft

NTFSマスターファイルから、ファイルパスおよびファイル名、ファイルサイズ、ディスク割り当てサイズ、ファイルの作成・変更・アクセス日時、ディレクトリかどうか等の情報を取得します。取得したデータをもとに、全体のファイルおよびフォルダー構造を分析したり、削除されたファイルやフォルダーを抽出したり、ADS（Alternate Data Stream）による隠蔽情報を探索することができます。

#### 構文

ntfs-mft [zipcharset=CHARSET] [zippath=ZIPFILE\_PATH] FILE\_PATH

必須パラメーター

**FILE\_PATH**

NTFSマスターファイルのパス。ファイルパスにワイルドカード（\*）を使用すると（例：D:\data\NTFS\*）、パターンに一致するすべてのファイルを一度に取得できます。zippathオプションと併用する場合は、ZIPファイル内に含まれるNTFSマスターファイルのパスを指定してください。

オプションパラメーター

**zipcharset=CHARSET**

ZIPエントリのエンコーディング形式（デフォルト：utf-8）。下記ドキュメントに登録されているPreferred MIME NameまたはAliasesを使用してください：<https://www.iana.org/assignments/character-sets/character-sets.xhtml>

**zippath=ZIPFILE\_PATH**

ZIPファイルのパス

#### 説明

出力されるフィールドの内容は、以下の表を参照してください。

出力フィールド

|  |  |  |
| --- | --- | --- |
| フィールド | 型 | 説明 |
| no | 整数 | ファイル番号 |
| file\_name | 文字列 | ファイル名 |
| file\_path | 文字列 | ファイルパス |
| file\_size | 整数 | ファイルサイズ |
| alloc\_size | 整数 | 割り当てサイズ |
| in\_use | ブール | 使用中かどうか |
| is\_dir | ブール | ディレクトリかどうか |
| link\_count | 整数 | 当該ファイルを参照するハードリンク数 |
| created\_at | 日付 | $FILE\_NAME属性の作成日時 |
| modified\_at | 日付 | $FILE\_NAME属性の変更日時 |
| access\_at | 日付 | $FILE\_NAME属性のアクセス日時 |
| mft\_modified\_at | 日付 | $FILE\_NAME属性のMFT変更日時 |
| std\_created\_at | 日付 | $STANDARD\_INFORMATION属性の作成日時 |
| std\_modified\_at | 日付 | $STANDARD\_INFORMATION属性の変更日時 |
| std\_access\_at | 日付 | $STANDARD\_INFORMATION属性のアクセス日時 |
| std\_mft\_modified\_at | 日付 | $STANDARD\_INFORMATION属性のMFT変更日時 |
| is\_readonly | ブール | 読み取り専用かどうか |
| is\_hidden | ブール | 隠しファイルかどうか |
| is\_system | ブール | システムファイルかどうか |
| is\_archive | ブール | アーカイブ属性かどうか |
| is\_device | ブール | デバイスファイルかどうか |
| is\_normal | ブール | 通常ファイルかどうか |
| is\_temp | ブール | 一時ファイルかどうか |
| is\_sparse | ブール | スパースファイルかどうか |
| is\_reparse | ブール | リパースポイントかどうか |
| is\_compressed | ブール | 圧縮ファイルかどうか |
| is\_offline | ブール | オフラインファイルかどうか |
| is\_indexed | ブール | インデックスファイルかどうか |
| is\_encrypted | ブール | 暗号化ファイルかどうか |
| lsn | 整数 | ログシーケンス番号 |
| seq | 整数 | シーケンス |
| file\_ref | 整数 | ファイルリファレンス |
| parent\_file\_ref | 整数 | 親ファイルリファレンス |
| parent\_no | 整数 | 親ファイル番号 |

#### 使用例

ファイルパスを指定して取得

ntfs-mft D:\data\NTFS\test\_MFT

zippathオプションで指定したZIPファイル内のNTFSマスターファイルを取得

ntfs-mft zippath=D:\data\NTFS.zip NTFS\test\_MFT

削除された隠し属性ファイルの一覧を取得

ntfs-mft D:\data\NTFS\test\_MFT | search not(in\_use) and not(is\_dir) and is\_hidden