### hive-file

レジストリハイブファイルから、ユーザーアカウントやグループ、セキュリティポリシー、OS情報、USBデバイス、プログラム利用履歴などの情報を照会します。

#### 構文

hive-file [zipcharset=CHARSET] [zippath=ZIPFILE\_PATH] FILE\_PATH

必須パラメーター

**FILE\_PATH**

レジストリファイルのパス。ファイルパスにワイルドカード（\*）を使用すると（例：D:\data\registry\*）、パターンに一致するすべてのファイルを一括で照会できます。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レジストリハイブ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）。次の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

ハイブファイルおよび出力されるフィールドの内容については、以下の表を参照してください。

ハイブファイル

|  |  |  |  |
| --- | --- | --- | --- |
| ファイル | 用途 | レジストリパス | 抽出情報 |
| SAM | アカウント・接続履歴 | HKEY\_LOCAL\_MACHINE\SAM | ユーザーアカウント、グループ |
| SECURITY | セキュリティポリシー・権限 | HKEY\_LOCAL\_MACHINE\Security | セキュリティポリシー |
| SOFTWARE | インストールプログラム | HKEY\_LOCAL\_MACHINE\Software | OSバージョン、OSインストール日、OSインストールディレクトリ、所有者アカウント |
| SYSTEM | システム設定 | HKEY\_LOCAL\_MACHINE\System | ホスト名、タイムゾーン、システムシャットダウン時刻、USBデバイスなど |
| NTUSER.DAT | ユーザー設定 | HKEY\_USERS.DEFAULT | 最近開いたファイル一覧 |

出力フィールド

|  |  |  |
| --- | --- | --- |
| フィールド | 型 | 説明 |
| key | 文字列 | サブキー |
| type | 文字列 | タイプ |
| name | 文字列 | レジストリ名 |
| value | オブジェクト | レジストリデータ |
| last\_written | 日付 | 最終更新日時 |

#### 使用例

ファイルパスを指定して照会

hive-file D:\data\registry\SYSTEM

zippathオプションを指定して照会

hive-file zippath=D:\data\registry.zip registry\SYSTEM

Windows OS情報の確認

hive-file D:\data\registry\SOFTWARE | search key=="ROOT\\Microsoft\\Windows NT\\CurrentVersion"