初めての「Registry Viewer」

2015年2月22日

セクタンラボ

Registry Viewerについて

- Registry Viewerは，Windows上で動作するフォレンジックツールです。
  - 有償ツールのため，USBドングルを接続しないと機能制限された「Demo Mode」での起動となりますが，基本操作の学習用とであれば十分に使えます。

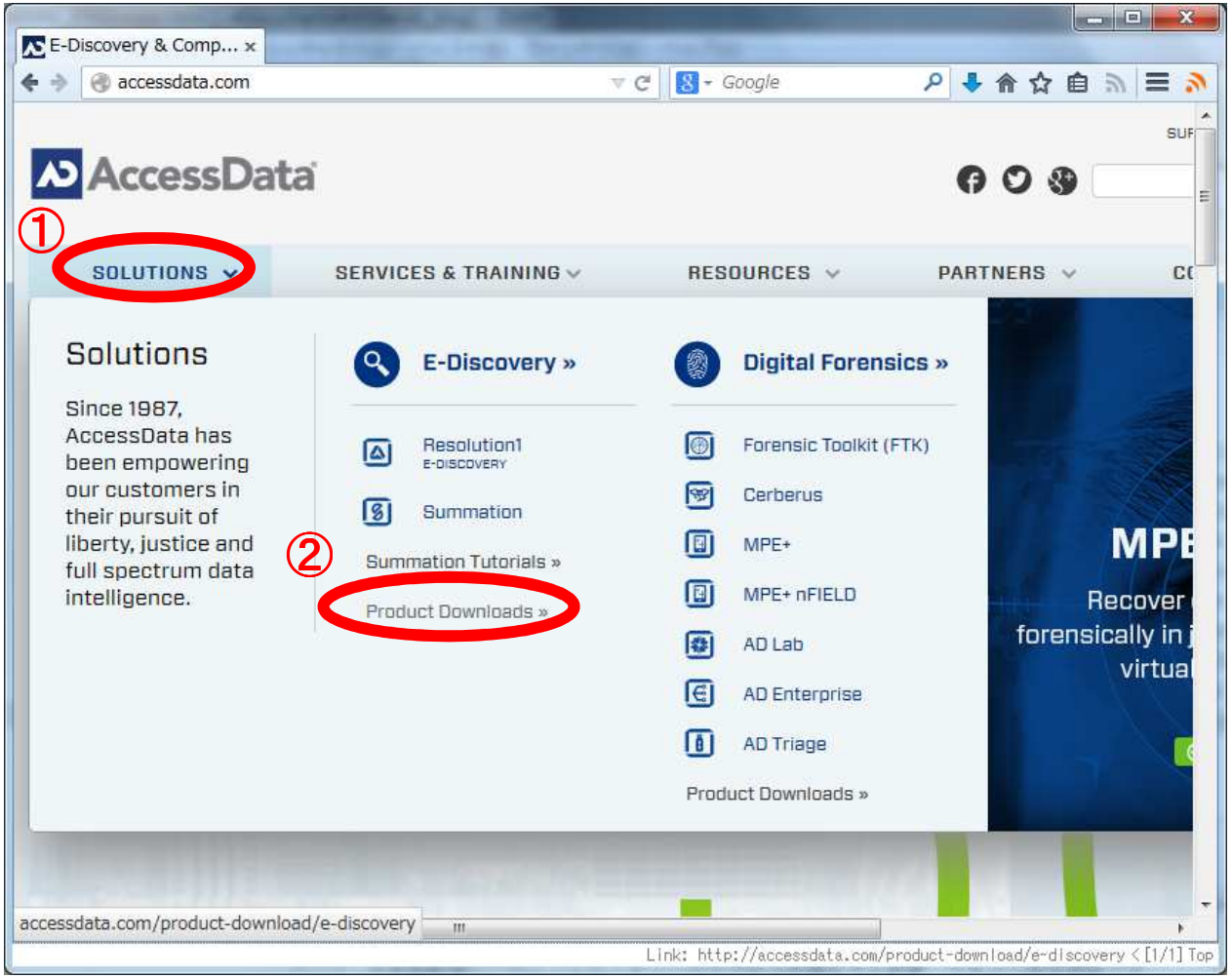
- FTK Imagerなどでエスクポートしたレジストリファイルを読み込み，解析する機能を有しています。
  - OS標準の「レジストリエディタ」では表示されない，レジストリキーの更新日時も表示されます。
  - 一部のレジストリキーに対しては，解析結果を表示する機能もあります。
    （ROT13形式に変換されたデータの復号など）

- 本資料では，Registry Viewerの基本的な操作方法を記載します。

ダウンロードとインストール

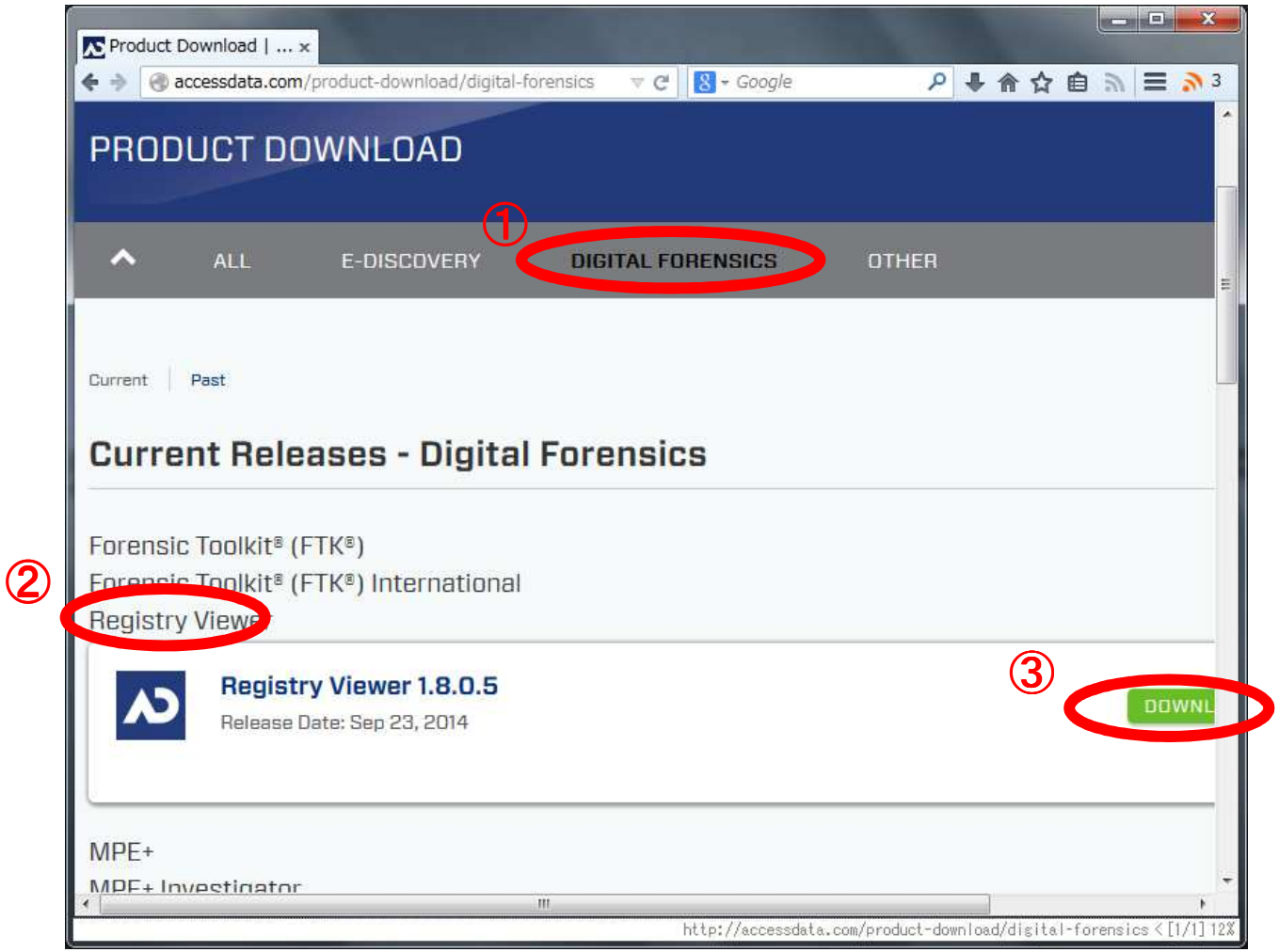
ダウンロード（1）

- AccessData社のWEBサイト（http://accessdata.com/）にアクセスし，上部メニュー「SOLUTIONS」-「Product Downloads」をクリック



ダウンロード(2)

- [DIGITAL FORENSICS]をクリックし，フォレンジック製品一覧の中から「Registry Viewer」をクリックし，「DOWNLOAD」をクリック

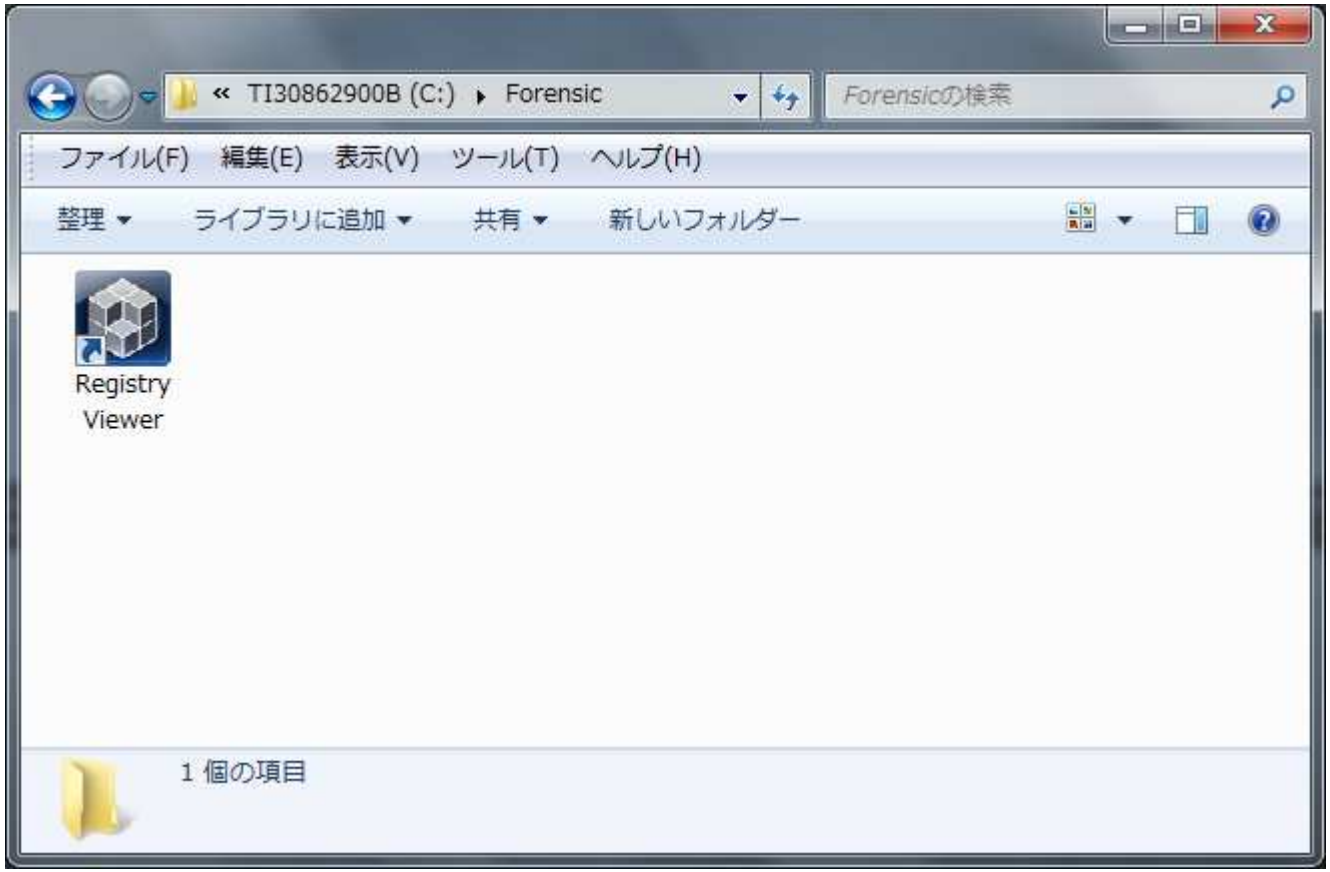


インストール

- 通常版は，インストーラーの指示どおりにクリックするだけで，難しいことは何もないので割愛します。

起動（1）

- デスクトップに作成されたショートカットなどから「Registry Viewer」を実行します。



起動（2）

- エラーメッセージが表示されたら，「いいえ」をクリック
  - 「ライセンス認証用のUSBドングルが見つからないため，ネットワーク上のライセンス認証サーバを指定しますか」という趣旨のメッセージです。

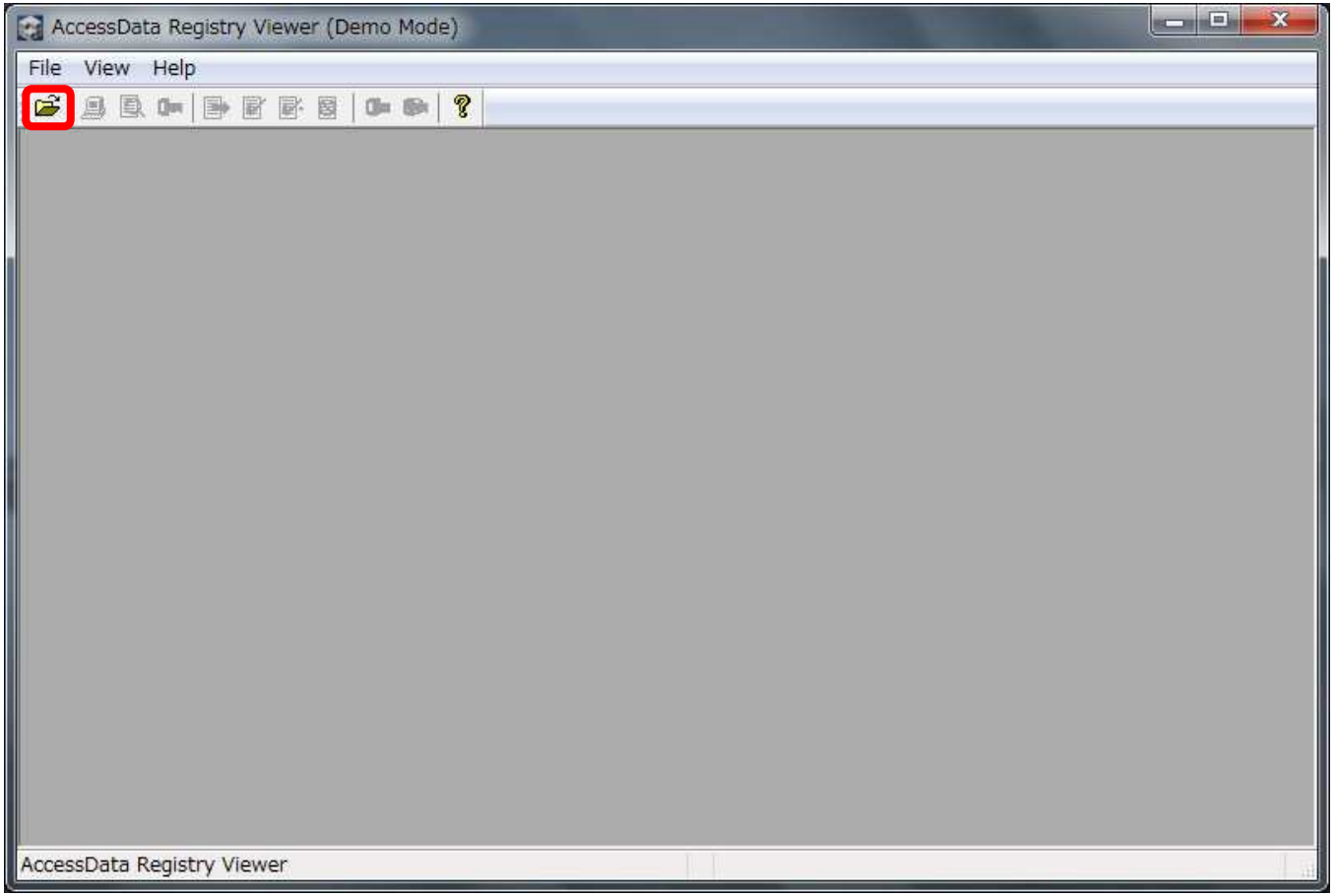
起動（3）

- メッセージが表示された「OK」をクリックすると，Registry Viewerが起動します。
  - 「Demo Modeで起動します」という趣旨のメッセージです。

基本操作

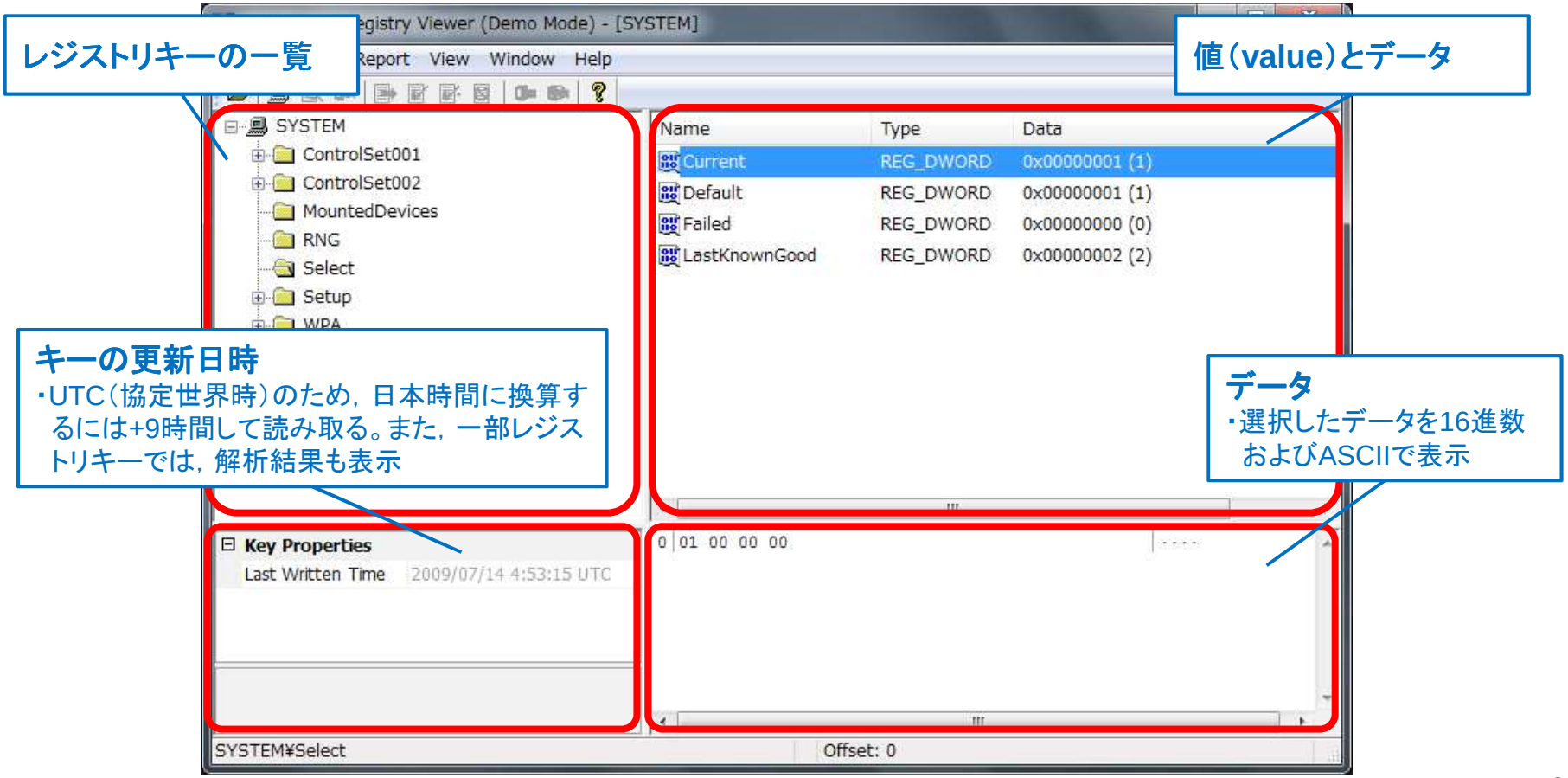
レジストリファイルの閲覧

- ツールバーから「Open」をクリックして閲覧したいレジストリファイルを選択，またはレジストリファイルを，「Registry　Viewer」のウィンドウにドラッグアンド



画面構成

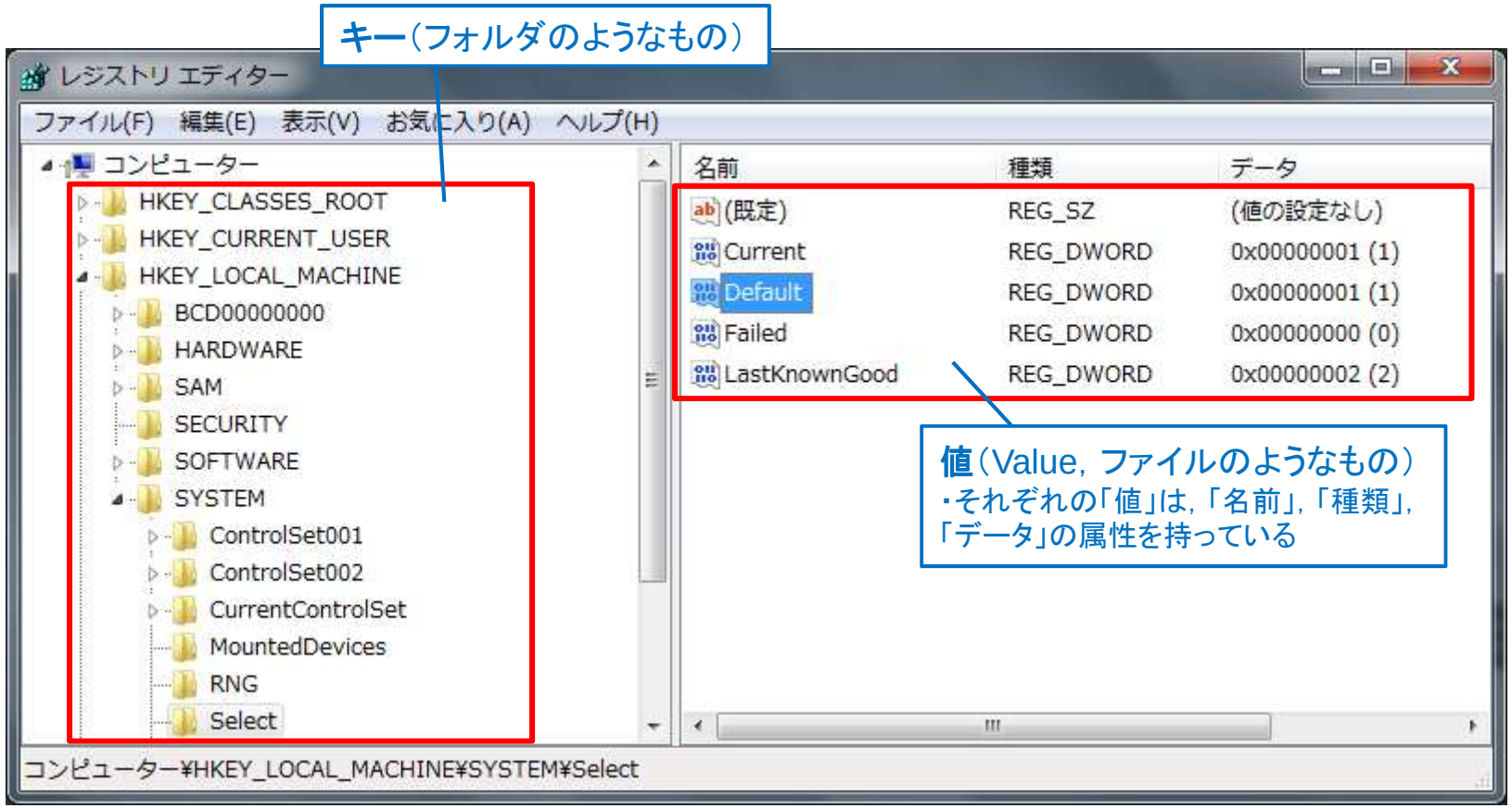
- 画面上部は，OS標準の「レジストリエディタ」とほぼ同じです。
- 画面下部に，レジストリキーの更新時間や，データの16進数が表示されます。



（参考）レジストリの基本

レジストリの概要

- レジストリとは，Windowsのシステム設定およびアプリケーション設定を記録するデータベースです。「キー」と「値」で構成されます。
- 「キー」は，最終更新日時を保有しており，直下の「値」が追加・削除・更新されると，タイムスタンプが更新されます。（「値」は，タイムスタンプを保有していません）



レジストリファイル

- レジストリは，複数のレジストリファイルとして保管されています。
  - OS起動時に各ファイルが読み込まれ，レジストリハイブ*1として構成されます。OS終了時・アプリケーション終了時に変更内容がファイルに保存されます。
- FTK Imagerなどでエクスポートしたレジストリファイルを，Registry Viewerで解析します。

◆ レジストリハイブとレジストリファイル

レジストリハイブ	レジストリファイルの場所
HKEY_LOCAL_MACHINE¥SAM	C:¥Windows¥System32¥config¥SAM
HKEY_LOCAL_MACHINE¥SECURITY	C:¥Windows¥System32¥config¥SECURITY
HKEY_LOCAL_MACHINE¥SOFTWARE	C:¥Windows¥System32¥config¥SOFTWARE
HKEY_LOCAL_MACHINE¥SYSTEM	C:¥Windows¥system32¥config¥SYSTEM
HKEY_USERS¥ (ユーザーのSID)	C:¥Users¥*【ユーザー名】*¥NTUSER.DAT

*1 レジストリ内部で構成される，レジストリキーのグループのこと。

自動構成されるレジストリハイブ

- **一部のレジストリハイブは，複数のレジストリファイルなどの情報を組み合わせて自動構成されます。**

◆ 複数のレジストリファイル等から自動構成されるレジストリハイブ

レジストリハイブ	説明
HKEY_CLASSES_ROOT	エクスプローラーを使用してファイルを開くときに，正しいプログラムを起動するための情報が格納される。
HKEY_CURRENT_CONFIG	システムの起動時に，ローカル コンピューターにより使用されるハードウェア プロファイルに関する情報が格納される。
HKEY_CURRENT_USER	現在ログオンしているユーザーの構成情報が格納される。

参考情報

- 上級ユーザー向けの Windows レジストリ情報（Microsoft）
  - http://support.microsoft.com/kb/256986/ja
- Windows OS入門：第5回　システム設定を集中管理するレジストリ（@IT）
  - http://www.atmarkit.co.jp/ait/articles/1501/22/news143.html
- Insider‘s Computer Dictionary ハイブ（hive）（@IT）
  - http://www.atmarkit.co.jp/icd/root/82/63063482.html