

WIPO PROOFの仕組み

WIPO PROOF は、RFC 3161 タイムスタンププロトコルに準拠した世界最高水準のPKI (Public Key Infrastructure: 公開鍵基盤) 技術を用いてタイムスタンプトークン (「WIPO PROOF トークン」) を生成します。

WIPO PROOF へのアクセス

- 1 ユーザは WIPO PROOF の Web アプリケーションにブラウザ経由で接続します (URL: wipoproof.wipo.int、各種最新ブラウザ対応)。

WIPO PROOF トークンの要求

- 2 電子ファイル (任意のファイル形式) を選択します。
注: WIPO PROOF でトークンを要求するには WIPO ユーザ アカウントが必要です。
- 3 ユーザ側のブラウザで、ファイルのハッシュ値 (各ファイル固有の値で電子データの指紋に例えられる情報) が、高度な一方方向ハッシュ関数アルゴリズム「SHA-2 (256ビット)」により生成されます。
注: ファイルが WIPO PROOF にアップロード (送信) されることはありません。ユーザがファイルを保有したままの状態での処理が行われます。
WIPO PROOF へは、ユーザ側のブラウザで生成されたハッシュ値のみがアップロードされます。

WIPO PROOF トークンの発行

- 4 WIPO PROOF が、システム監査の検証を経た高信頼性のシステム (業界標準に完全準拠) を用いて、ファイルのハッシュ値に時刻情報を付します (「タイムスタンプ」)。タイムスタンプの時刻情報は、UTC (協定世界時) と同期したハードウェアベースの時刻ソースから取得されます。
- 5 FIPS-140 レベル 3 認証を受けた不正アクセス対抗型の HSM (ハードウェアセキュリティモジュール) 装置に格納された秘密鍵を用いて、ハッシュ値に対して署名処理を行い、デジタル署名を作成します。デジタル署名の正当性を証明するための公開鍵を付します。
- 6 WIPO PROOF トークンをダウンロードします。このタイムスタンプトークンは、トークンが作成された日時にその電子ファイルが確かに存在していたことを証明する改変不可能な証拠になります。

WIPO PROOF タイムスタンプトークンの発行

