知的財産保護に関するタイムスタンプの利用（しくみの説明）

弁理士　　椿　豊

【基礎知識】

（１）文書のハッシュ値化（ダイジェスト化）とは

数学により、どんな元データでも 64 文字（sha256 の場合）のハッシュ文字列にすることが可能。元データが同じならば、何度やっても同じ文字列になる。元データが違えば、ハッシュ文字列も異なる（可能性としては低いが同じになることもある）。ハッシュ文字列を元データに戻すことは不可能。

例：

「こんにちは」→

125aeadf27b0459b8760c13a3d80912dfa8a81a68261906f60d87f4a0268646c（64 文字）

（１００頁の PDF ファイル）→

2752af13357fad290269985d4d11df3f0c8adaf8667f3f0fbdcb41c9c820ff59（64 文字）

（２）公開鍵、秘密鍵とは

元データを暗号化するためのもの。ペアの公開鍵、秘密鍵を使う（鍵と言うが、実体は暗号化するための文字列）。「秘密」鍵を使って暗号化すると、「公開」鍵で元のデータに戻すこと（復号化）ができる。「公開」鍵を使って暗号化すると、「秘密」鍵で元のデータに戻すことができる。

秘密鍵は誰にも公開しない実印のようなもの。公開鍵は一般公開し、誰でも入手可能。

「秘密」鍵で暗号化された暗号文が送られてきたとき、ペアの「公開」鍵で復号できれば、秘密鍵の所有者がその秘密鍵（実印）を使って暗号化した文だな…、と推測することができる（秘密鍵の実印的な機能）。

【タイムスタンプで日時の立証が可能である仕組み】

（３）タイムスタンプ付与時

（３－１）タイムスタンプを押したい文書を、利用者のＰＣでハッシュ値化する。

例

（１００頁の PDF ファイル）→

2752af13357fad290269985d4d11df3f0c8adaf8667f3f0fbdcb41c9c820ff59（64 文字）

（３－２）ハッシュ値を利用者のＰＣから、タイムスタンプ局のサーバに送る。

（３－３）タイムスタンプ局のサーバは、ハッシュ値に日時情報を付加する。

例

2752af13357fad290269985d4d11df3f0c8adaf8667f3f0fbdcb41c9c820ff59 2022-02-17-18-02-41

（３－４）サーバは、ハッシュ値＋日時情報を「秘密鍵」で暗号化する。これがタイムスタンプトークンと呼ばれる。
例
2752af13357fad290269985d4d11df3f0c8adaf8667f3f0fbdcb41c9c820ff59 2022-02-17-18-02-41 →
ZuBuLVKPgANfLHAULf7iUWWjLtH2ApsBuExxLiudnEjVTfWGaj38iisjwBQdLiFUpLZ9T42VaYEAxycd

（３－５）サーバは、タイムスタンプトークンを利用者の PC に返す。

（３－６）利用者の PC では、タイムスタンプトークンが元の文書とセットで保存される。

（４）タイムスタンプ確認時
（４－１）タイムスタンプの真偽を確認したい文書を、利用者のＰＣがハッシュ値化する。上記（３－１）と同じハッシュ値となる。
例
（１００頁の PDF ファイル）→
2752af13357fad290269985d4d11df3f0c8adaf8667f3f0fbdcb41c9c820ff59（64 文字）
（４－２）タイムスタンプトークンを、タイムスタンプ局の「公開鍵」で復号化する。上記（３－３）と同じハッシュ値と日時が得られる。得られなければ、そのタイムスタンプ局が暗号化したタイムスタンプトークンではない（そのタイムスタンプ局の秘密鍵で暗号化されたものではない）とわかる。
例
ZuBuLVKPgANfLHAULf7iUWWjLtH2ApsBuExxLiudnEjVTfWGaj38iisjwBQdLiFUpLZ9T42VaYEAxycd →
2752af13357fad290269985d4d11df3f0c8adaf8667f3f0fbdcb41c9c820ff59 2022-02-17-18-02-41
（４－３）上記（４－１）と（４－２）のハッシュ値
「2752af13357fad290269985d4d11df3f0c8adaf8667f3f0fbdcb41c9c820ff59」が一致すると、タイムスタンプ局がその文書についてのタイムスタンプトークンを発行したことがわかる（異なれば、それは違う文書のタイムスタンプトークンである）。タイムスタンプトークンに含まれている日時である、「2022-02-17-18-02-41」がタイムスタンプ局が証明した日時(その文書が存在した日時）であると証明される。

【知財管理への応用】
（５）知財管理への応用

（５－１）他社から権利行使を受けたくない自社技術について、その技術についての先使用権の発生要件を記載した資料を作り、タイムスタンプ（特許法７９条「特許出願の際現に」の立証）を付与する。資料には、「日本国内においてその発明の実施である事業をしている又はその事業の準備をしている」ことを示す事実、「実施又は準備をしている発明及び事業の目的の範囲内」は何であるかを広めに記載しておく。

これまで先使用権は立証が困難であることが指摘されてきたが、タイムスタンプによって立証の容易化を図る。

（５－２）発明内容を他社にプレゼンする前に、事前にその発明内容を記載した文書（望ましくは特許明細書的な文書）を作成し、タイムスタンプを付与する。守秘義務違反、冒認出願などされないための資料とする。相手に資料を渡す時も、タイムスタンプを付与したものを渡すことで、牽制力になる。

（５－３）商標などの周知性の立証、著作権の発生・帰属の立証などに使うことができる。

（５－４）タイムスタンプは日時を立証するものであり、公開の事実を証明するものではない。発明が公知であることなどを立証するためには、公知となった事実（販売、インターネット公開など）が客観的に示されている資料を準備し、それにタイムスタンプを付与する。単に事実を述べるのではなく、公開された発明や技術的思想が何であるかを「広めに」書いておく（変形例、バリエーションなどを書いておく）とよりよい。

以上