電子文書における署名とタイムスタンプ

宮崎一哉*

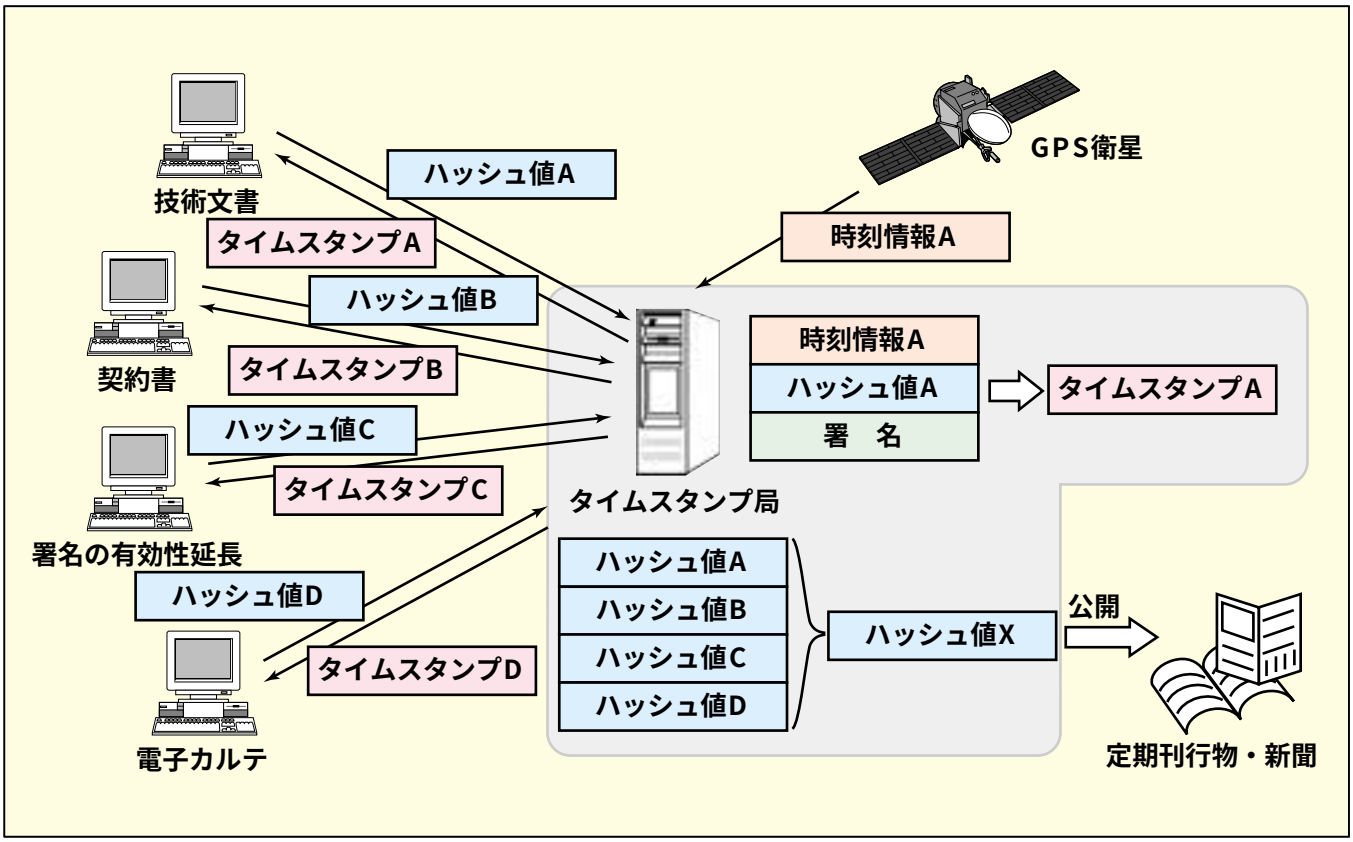
要　旨

近年，業務の電子化やインターネット上での電子商取引が盛んに行われるようになり，これに伴って，電子文書が急激に増加している。ところが，電子文書は紙ベースの文書と比較して複製や加工が極めて容易であるため，いつ，だれが，何を作成したか，すなわち，真正性を保証することが難しい。PKI(Public Key Infrastructure：公開かぎ(鍵)基盤)の発展と電子署名法の成立によって電子文書の真正性を保証する枠組みが技術面・法制度面の両面から整いつつあるが，そこで中心となるディジタル署名は，“いつ”を保証する手段を持たないばかりか，時間の経過によって“だれ”及び“何”をも保証できなくなるという問題を抱えている。

これを解決する一つの手段がタイムスタンプである。

タイムスタンプは，電子文書のある時刻における存在と，その時刻以降，電子文書が改ざんされていないことを保証する仕組みである。タイムスタンプは，通常，信頼のおける第三者機関であるタイムスタンプ局によって発行される。このとき，タイムスタンプには可能な限り正確な時刻を利用するほか，ハッシュ値を定期刊行物や新聞などの大衆メディアに公開することにより，タイムスタンプ自体の信頼性を高めることができる。

ディジタル署名の標準拡張仕様や医用画像情報の標準署名フォーマットにタイムスタンプが採用されるなど，現在，タイムスタンプに対する注目度は高まっており，今後，幅広い分野において利用されることが予想される。



タイムスタンプの概要

タイムスタンプ局に対してタイムスタンプを取得したい電子文書のハッシュ値を送付すると，タイムスタンプ局は，ハッシュ値と時刻情報を結合し，タイムスタンプ局の署名を付けたデータをタイムスタンプとして送り返す。正確な時刻情報はGPS(Global Positioning System)衛星などから取得する。タイムスタンプ局は，定期的にハッシュ値を定期刊行物や新聞などの大衆メディアに公開することにより，サービスの信頼性を高める。

*情報技術総合研究所