ネットワーク上のトラブルを未然に防止するデジタル・タイムスタンプ・システム

9 産業と技術革新の基盤をつくろう

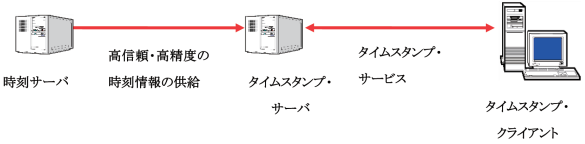
キーワード　情報セキュリティ／情報ネットワーク／ソフトウェア

研究概要

ネットワーク上のデジタル・データの作成日時や内容の改ざんを防止し、係争時には第三者に対して、データの作成日時・内容を証明するための技術としてデジタル・タイムスタンプ・システムがある。近年、e-文書法に対応して領収書等の発行日時の保証、メールの送受信の日時証明、Web上のトランザクションの日時証明、法律上のデータの改ざん防止等のため、タイムスタンプ・システムの重要性が増している。

タイムスタンプ・システムには幾つかの方式が提案され運用されているが、第一には(RFC3161として)国際標準化もされているデジタル署名に基づくシステムを適用する。

この国際標準では、ネットワーク上のクライアント・システムとサーバ・システムのデータのやり取りの順序とそのフォーマットを定めているのみであり、システムとして運用する際には、クライアントにおいてどのようなデジタル・データを選択/構成してサーバにタイムスタンプ付与を依頼するかがポイントとなる。



タイムスタンプ・サーバとタイムスタンプ・クライアントの間のプロトコルは、例えばRFC3161で定められたTime-Stamp Protocol(TSP)を想定する。
タイムスタンプ・クライアントとしては、エンド・ユーザが使う一般のPC、メール・サーバ、Webサーバ、ストレージ・サーバ等が想定される。多くの場合、タイムスタンプ・クライアントは、何等かのサービスを提供するサーバとして動作しながら、タイムスタンプ・サービスにおいてはクライアントとして動作することになる。

今後の展開やメッセージ

これまで作成した幾つかのプロトタイプ・システムを元に、実運用するシステムの構築を実現していく。

研究者情報

堀田 英一 教授・Ph.D.
基礎教育部　数理基礎教育課程
所属研究所：情報技術AI研究所

京都大学理学部卒(数学専攻)。九州大学工学部修士課程修了(応用数学専攻)。日本電信電話公社入社、オランダ数学・計算機科学研究所客員研究員、アムステルダム自由大学よりPh.D.取得(計算機科学専攻)、NTTソフトウェア研究所主任研究員を経て、2006年本学教授就任。

研究者情報URL
https://kitap01.kanazawa-it.ac.jp/researcherdb/researcher/RAGAAH.html