提出時刻の改ざんを防止するTimeStampシステム”S3”の開発

木澤 寛厚

1. はじめに

菊池研究室では、3 年生を対象に Java ゼミナールを行っている。毎週、宿題が出題されるが、期限内に出したと言い張ったり、期限後に秘密に修正するなどの不正行為の懸念があった。

そこで、本研究では、S. Haberらが提案したLinking Protocol[1]を用いたTime Stampシステムを開発した。本稿では、本システムの実装と試験運用について報告する。

2. Time Stamp

Time Stamp は、デジタルデータが特定時刻に存在していたことと、その時刻以降、データが改ざんされていないことを証明する技術である。

Linking Protocol とは、Time Stamp 生成機関が複数の Time Stamp を相互に関連付けるリンク情報を生成し、これを基に Time Stamp を生成する方式である。リンク情報は、

$L_1=H(h_1,L_0)$,

$L_2=H(h_2,L_1)$,

：

$L_n=H(h_n,L_{n-1})$

と定義される。L_nを定期的に公開しているので、文章の順序を変更してしまうとリンク値が変わってしまう。そのため、サーバは不正を行なうことが出来ない。

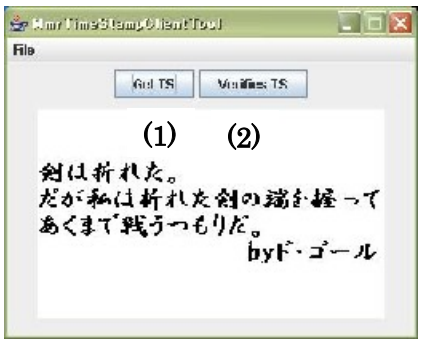
3. システム

本プログラムは、Time Stampサーバ S、クライアント C、情報公開サーバS_pの三つで構成されている。

3.1 Time Stamp サーバ S

ハッシュ h_i を受け取り、それに時刻情報t_iとデジタル署名を付加して返す。同時に、リンク情報Li=H(hi,Li-1)を生成しサーバ上に保存する。

3.2 クライアント C



(1)Time Stamp 取得ボタン

(2)Time Stamp 検証ボタン

図 1. クライアントツール

クライアントは、Time Stampの要求と検証を行う。実行画面を図 1 に示す。Time Stampを要求するには、対象ファイルのハッシュ値h_iをサーバ S に送り、返ってきたデータ(h_i, σ_i,L_i)をTime Stampファイル(.tst)として保存する。検証は、検証するファイルのTime Stampのデジタル署名 σ_i、リンク情報 L_i をチェックし、Time Stampファイル中のハッシュと検証するファイルのハッシュ h_i を比べて実行される。改ざんが無ければ、検証に成功し時刻が証明される。

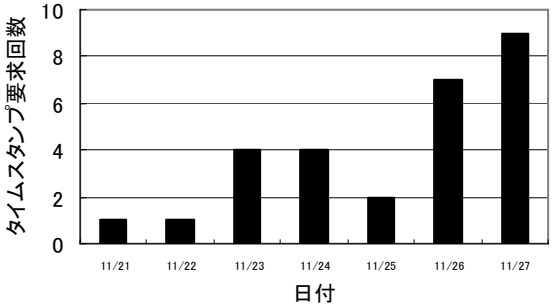
3.3 情報公開サーバS_p

Linking Protocol では、定期的にリンク情報を公開しなければならない。情報公開サーバはそのための Web サーバである。クライアントから要求に対して、サーブレットで公開情報を提供する。

4. 運用実験

4.1 実験結果

2006 年 11 月 21 日から、菊池研究室にて、3 年生 21 人に対して運用を行った。図 2 は、実行期間中に Time Stamp を



要求した回数の推移である。なお、Time Stamp を押し直した人もカウントされている。

図 2. 一週間の人数の推移

週の中盤と最後にアクセスが増加し、宿題提出期限日(11/27)に、最もアクセスが集中している。

5. おわりに

Java ゼミナールのための Time Stamp システムを開発し、宿題の提出時間の改ざんを防ぐことに成功した。

今後の課題として、検証の際にまとめて検証できるようにプログラムを変更することなどが挙げられる。

参考文献

[1] 宇根，他，デジタルタイムスタンプ技術の現状と課題，金融研究第 19 巻別冊第 1 号，pp. 105-154，2000.