

大規模タイムスタンプサービスシステムの構築事例

佐藤雅之[†]

三菱電機株式会社 情報技術総合研究所[†]

1. はじめに

タイムスタンプサービスは、電子申請、電子調達における申請内容や入札内容の原本性確保および入札時刻の証明や、電子債券市場(確定日付の IT 化)などで使用され、3 年～10 年、あるいはそれ以上の長期に渡って提供し続けるサービスである。なお、タイムスタンプ(TimeStampToken)は、信頼における時刻と文書などのデジタル情報に対し、変更、改ざんがあったかどうかを検知できる情報であり、デジタル情報に時刻情報を付与し、電子署名として発行する¹⁾。

本稿では、ユーザ業務に基づき、大規模ユーザへのタイムスタンプ発行を行う大規模タイムスタンプサービスの構築事例を報告する。

2. RFC3161 タイムスタンププロトコル

タイムスタンプサービスの発行において、使われるプロトコルは、RFC3161 に規定されるタイムスタンププロトコルである。RFC3161 によるタイムスタンプの発行手順は、図 1 に示す通り。

1. 利用者は、TSA(Time Stamping Authority)と呼ばれるタイムスタンプ局にタイムスタンプの発行要求であるリクエストを送る。
2. TSA は、利用者にレスポンスとしてタイムスタンプを送る。

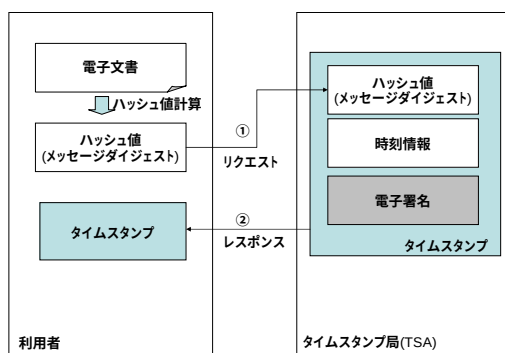


図1. タイムスタンプ(TimestampToken)の発行²⁾

A construction example of a large-scale time stamp service system.

Masayuki SATO

Information Technology R&D Center, Mitsubishi Electric Corporation.

3. 大規模タイムスタンプサービス構築における課題

タイムスタンプサービスは、長期に渡ったサービス提供を行うため、利用するユーザ数も拡大することが見込まれる。このため、タイムスタンプサービスの提供者は、スケーラビリティに考慮したシステム構築を行う必要がある。すなわち、システム設計フェーズにおいて、ユーザ数に応じたシステム性能を求めることが必要となる。

今回は、次の手順により、大規模タイムスタンプサービスを構築した。

1. システム要件、ユーザ業務を元に、システムモデルを設計する。
2. ユーザ業務モデルから、システムのトラフィックモデルを構築し、システムの物理設計を行う。

4. システムモデルの導出

システム要件とユーザ業務モデルに基づいて、システムモデルを導出する。

[システム要件]

- ・ 大規模タイムスタンプサービス提供者は、最大ユーザ数 x [人]に対してサービスを行う。
- ・ リクエストおよびレスポンスの大きさは、高々1KBである。
- ・ ユーザを個々に認証し、利用に応じて、課金を行う。

[ユーザ業務モデル]

- ・ ユーザは、エンドユーザにサービスを提供する。その時間は、毎日、数分～数十分である。ユーザは、エンドユーザにサービスを提供した後に、電子文書を作成し、タイムスタンプを添付するため、リクエストを行う。
- ・ ユーザはリクエストから、8[sec]程度、結果を待つことができる。
- ・ タイムスタンプの検証は、数年に1度行われる。
- ・ 各ユーザは、独立にサービスを提供する。

課金認証のシステム要件より、本システムは、RFC3161 プロトコルによるリクエストの前に、プロキシサーバを配置することにより、ユーザ認証を行うものとした。タイムスタンプサービスの提供者は、これにより、ユーザ認証の都度、ユーザに対し課金を行う。

以上のシステム要件、ユーザ業務モデルから、次のように、機能分割を行ったシステムモデルを設計した。

- ・ タイムスタンプサーバ…RFC3161 におけるタイムスタンプ生成を行う。
- ・ プロキシサーバ…リバースプロキシ。認証サーバにユーザ認証要求を送る。
- ・ 認証サーバ…ユーザ認証を行う。

タイムスタンプシステムモデルを図2に示す。

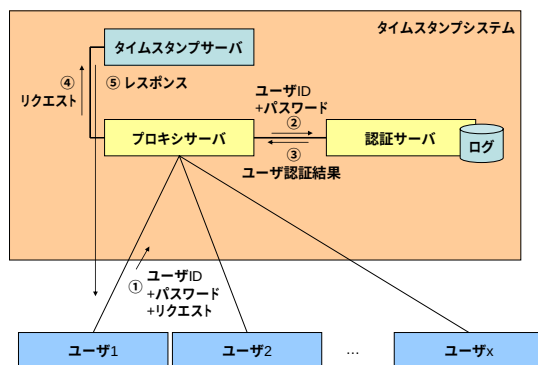


図2. タイムスタンプサービスシステムモデル

- ① ユーザは、ユーザ ID およびパスワードおよび、リクエストをプロキシサーバに送る。
- ② プロキシサーバは、ユーザ ID とパスワードを認証サーバに送る。
- ③ 認証サーバは、ユーザ ID とパスワードにより、ユーザを認証し、記録をログに残す。認証サーバは、結果をプロキシサーバに返す。
- ④ プロキシサーバは、認証結果を受けて、タイムスタンプ要求のリクエストをタイムスタンプサーバに送る。
- ⑤ タイムスタンプサーバは、リクエストから、タイムスタンプを作成し、ユーザに返す。
- ⑥ 認証サーバログから、ユーザに対して課金を行う。

5. ユーザ数に対応したシステム性能

以上のシステム要件およびユーザ業務モデルに、次の仮定を導入した。

- ・ 本システムは、ピーク時に x [人]のユーザ中、 y [%]のユーザが同時にアクセスを行う。

タイムスタンプサービスは、サービス提供の過程で、 y の値の精度を上げるものとした。

以上から、ピーク時のトラフィックを、次のように求めた。

[ピーク時のアクセス数]= $x \times y / 100$ [件]

[ピーク時のトラフィック]= $= x \times y / 100 \times 1 / 8 \times 1$ [KB]= $x \times y / 800$ [KB/sec]

すなわち、 $x \times y / 800$ [KB/sec]を処理する性能をシステムに持たせる。この特性を図3に示す。

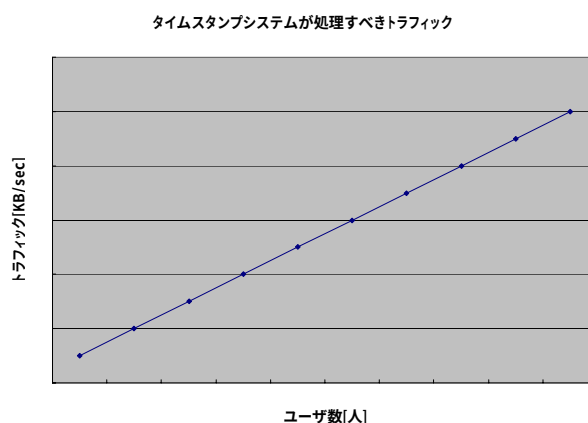


図3. タイムスタンプシステムが処理するトラフィック

タイムスタンプサービスの提供者は、図3に示す特性を元に、物理設計を行う。これにより、タイムスタンプサービスの提供者は、長期のサービスに対応し、スケーラビリティを持つ大規模タイムスタンプサービスを構築することができた。

6. おわりに

ユーザモデルを構築し、大規模タイムスタンプシステムを構築する事例について報告した。タイムスタンプサービスの提供者は、実際に、大規模タイムスタンプシステムを構築し、サービスを開始している。今後は、ユーザモデルの精度を向上させ、より大規模なタイムスタンプサービスに発展させる予定である。

[参考文献]

1. NIC タイムビジネス協議会 用語集
2. IPA タイムスタンプ技術に関する調査報告書,2004.4
3. NIC タイムビジネス協議会 タイムビジネス利用に関する国内動向調査報告書,2004.5