2005－CSEC－29（9）
2005／5／19

時刻認証子による時刻配信システムの実網上での評価

久保寺　範和*　　島　成佳*　　石崎　健太郎†

E-mail: n-kubotera@bp.jp.nec.com, shima@ap.jp.nec.com, ishizaki-kxb@necst.nec.co.jp

* 日本電気株式会社
システム基盤ソフトウェア開発本部
〒108-8557　東京都港区芝浦 2-11-5

† NEC システムテクノロジー株式会社
〒731-3168　広島市安佐南区伴南 1-40-1

概要：標準時配信局（TA：Time Authority）は、タイムスタンプ局（TSA：Time-Stamping Authority）の内部時計の改ざんを検出するため、時刻監査を行っている。しかし、現在の時刻監査では監査結果を再検証する仕組みがないため、後日監査結果を証明することは難しい。そこで「時刻認証子による時刻証明方式」において、TSA が TA から監視を受けることにより、再検証を可能とする方式を提案した。だが、実網上では TA と TSA の間のネットワーク遅延、時刻誤差があるため、監視が失敗する場合が考えられる。本論文では、インターネット上で時刻認証子による時刻配信システムを構築し、実網上での監視間隔の理想値を求める。監視間隔が理想値に設定された場合、時刻認証子による時刻配信は時刻改ざんの検出に有効なことが明らかとなった。

An Evaluation of Systems of Time Distribution using Time Evidence on The Internet

Norikazu KUBOTERA*, Shigeyoshi SHIMA*, Kentaro Ishizaki †

E-mail: n-kubotera@bp.jp.nec.com, shima@ap.jp.nec.com, ishizaki-kxb@necst.nec.co.jp

* NEC Corporation,
System Platform Software Development Division
2-11-5 Shibaura, Minato-ku, Tokyo, 108-8557, Japan

† NEC System Technologies, Ltd.
1-40-1 Tomominami, Asamimami-ku, Hiroshima-si,
Hiroshima, 731-3168, Japan

Abstract：Time Authority (TA) audits a local clock of Time-Stamping Authority (TSA) in order to detect tampering of time. It is difficult to verify audit logs of local time after audit of local time of TSA. Then we propose a method of detecting time tampering by checking TSA by TA. The method is described as “A Method of Time Certification using Time Evidence”. Because there is the network delay and the time offset between TA and TSA in the internet, the check may fail. In this paper, we construct a time distribution system using Time Evidence on the internet, and we get an ideal interval between checks. We know that it is available to detect tampering of time by using Time Evidence if the interval between checks are set as ideal values.

1. はじめに

近年、ネットワーク上で電子商取引や各種行政手続等が行われるようになっており、使用する電子データの存在性、完全性を確保することが重要となっている。電子データの存在性と完全性は、信頼できる第三者機関であるタイムスタンプ局（TSA：Time-Stamping Authority）が電子データのハッシュ値にタイムスタンプ[1]を付与する

ことで、保証できる。

TSA や企業内のタイムサーバ、システム、ネットワーク機器等の時刻の正確性を証明する第三者機関として標準時配信局（TA：Time Authority）がある。TA は、信頼できる正確な時刻を保持しており、TSA 等へ時刻配信を行い、NTP（Network Time Protocol）[2]を利用して時刻の監査を行っている。TA は、TSA の内部時計に対する時刻監査の中で、時刻精度を確認し、監査結果を監査ログとして記録する。監査ログは、後日監査の再検証する際に、存在性・完全性を確保しなければならない。しかし、現状監査ログの存在性・完全性を確保する方法はない。そのため、監査当時に TSA 内の時計が正確な時刻であったか検証するのは困難である。

再検証が難しいという課題に対しては、TA および TSA で、時刻の証拠である時刻認証子を生成する方式を示した[3][4]。時刻認証子による時刻の検証方式は、TA から TSA に対して監視を実施することにより再検証を可能とする。

監視の間隔は短くすることで、時刻を改ざんできる範囲を小さくできる。しかし、TA と TSA 間のネットワーク遅延や時刻誤差により、正しく監査できない場合がある。本論文では、TA と TSA をインターネットに接続し、ネットワーク遅延や時刻誤差から監視の間隔の最適な値を求める。さらに、求めた最適値が、時刻改ざんの防止に有効な値であることを示す。

2. 配信時刻証明方式の概要と特徴

2.1 時刻認証子概要

TA および TSA で生成される時刻認証子は以下を満たす。

(1) 生成された時刻認証子の改ざん検出を可能とする。

(2) 時刻認証子を予測して事前に生成するのは困難である。

(3) 時刻認証子の配信経路の特定を可能とする。

(1)の改ざん検出を可能とするには、信頼できる第三者機関である TA から監視を受ける必要がある。

2.2 時刻認証子の生成方法とフォーマット

TA および TSA の時刻認証子の生成モデルを図 1 に示す。ただし、生成モデルは以前の論文と同様である。図 1 では、TA、TSA の時刻認証子の生成タイミングを示しており、時間が矢印の方向に過去から未来へ流れている。TA および TSA では、時刻の流れを示す矢印上に横線にて、時刻認証子が生成されたことを示す。

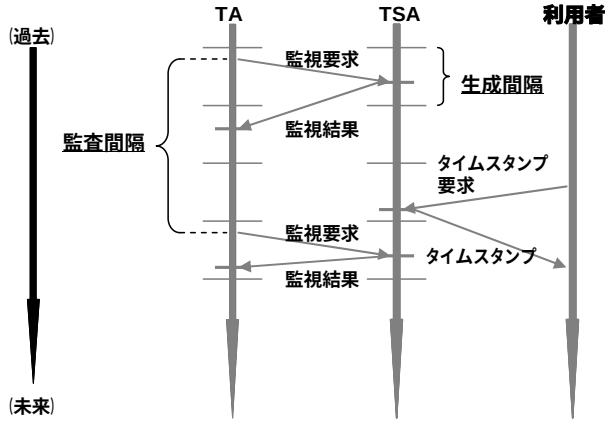

図 1：時刻認証子生成図

時刻認証子の生成タイミングは、①一定時間ごと、②TSA が TA からの監視要求を受けたとき、③TA が TSA から監視結果を受けたとき、④TSA が利用者からタイムスタンプ要求を受けたときの 4 種類である。各時刻認証子は、TA、TSA にて、それぞれで直前に生成された時刻認証子のハッシュ値を基に生成されているため、改ざんが困

難である。また監視の際、TA の時刻認証子を TSA に送付し、TA の時刻認証子のハッシュ値を基に TSA の時刻認証子を生成する。

本論文で算出する「監視間隔」とは、TA から監視を実施する間隔のことである。また、監視間隔は一定時間ごとの時刻認証子の生成される間隔（以下「生成間隔」とする）に依存する。

時刻認証子に格納されるデータは、主に以下がある。

- 時刻認証子を生成した機関（TA または TSA）を示す情報（例：IP アドレス）
- 時刻認証子を配信した機関（TA）を示す情報（例：IP アドレス）
- ランダム値（事前予測を防止するため）
- ハッシュ値（時刻認証子の完全性を検証するための情報）

3. 生成・監視間隔の算出方法

3.1 生成・監査間隔の計算式

時刻認証子の適正な監視間隔および生成間隔を算出するために TA と TSA をインターネットを介して接続した。インターネットには、10Mbps の通信速度の回線で接続した。回線は TA、TSA 以外の通信装置と共用で使用しており、実使用と同等の環境で実験を行った。

TA は、TSA が不正な時刻認証子を生成するのを防止するために監視を行う。TSA 内で生成される時刻認証子は、ハッシュ値によりリンクされているため改ざんは困難であるが、監視間隔が長くなった場合、ハッシュ値が衝突する可能性が高くなるため監視間隔は短いほうが望ましい。

監視間隔を生成間隔の 2 倍にした場合（図 2）、TA からの監視(te_s_1)と監視(te_s_4)の間に生成される時刻認証子は 2 個(te_s_2 と te_s_3)になる。

te_s_1 と te_s_4 は、TA の時刻認証子を元に生成され、TA にて保存されているため、TSA 内で改ざんを行った場合、検出を可能とする。te_s_2, te_s_3 はそれぞれ、改ざんの検出が可能な te_s_1, te_s_4 とハッシュ値によりリンクされているため、ハッシュの衝突可能性を低減している。

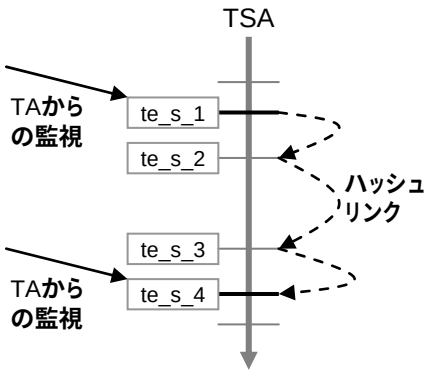

図 2：監視間隔算出図

監視間隔を生成間隔の 2 倍以下にした場合、TSA で生成される一定時間ごとの全ての時刻認証子は、監視要求を受けたときの時刻認証子とリンクするため、改ざんはより困難となる。監視間隔を生成間隔の 2 倍以上にした場合、監視要求を受けたときに生成される時刻認証子と直接リンクしない時刻認証子が生成されるため、ハッシュ値の衝突発生の危険性が高まる。よって、生成間隔は監視間隔の 2 倍以下が望ましい。

TSA が監視結果を意図的に遅らせることで、TSA は結果を遅らせた分の時刻を改ざんすることが可能となる。したがって、監査要求を送信してから監視結果を受信するまでの時間は、生成間隔より短くてはならない（図 3）。

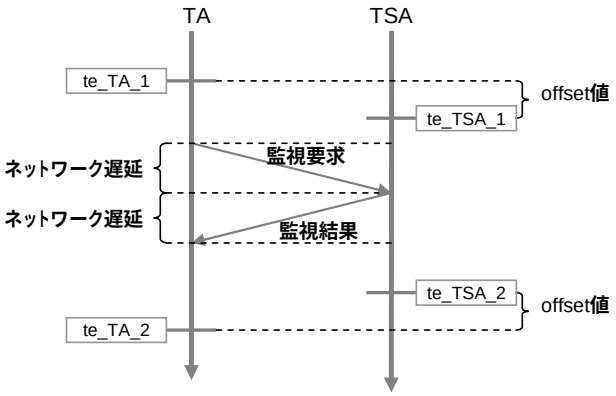

図 3：生成間隔算出図

te_TA_1, te_TA_2 は TA で、te_TSA_1, te_TSA_2 は TSA で、それぞれ一定時間ごとに生成される時刻認証子を示している。監視に要する時間はインターネットを介したネットワーク遅延の 2 倍以上かかり、時刻誤差（以下 offset 値と記述する。[2]参照）を考慮した場合、以下の計算式を得る。

$0 < T_a \leqq 2T_g$

$T_g \geqq 2(T_o + T_d)$

T_a：TA～TSA 間の監視間隔
T_g：時刻認証の生成間隔
T_o：TA～TSA 間の offset 値の絶対値
T_d：TA～TSA 間のネットワーク遅延

3.2　測定値と生成・監査間隔の最適値

実際に計測した、offset 値、ネットワーク遅延を以下に示す。計測データは、NTPv4 を使用して約 1 週間かけて収集したものである。

●offset 値
最大　19.014 ミリ秒
最小　-11.708 ミリ秒
平均　0.113265 ミリ秒

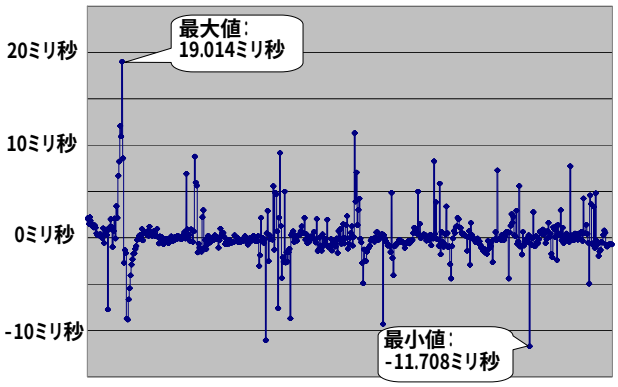

図 4：offset 値

●インターネットを介したネットワーク遅延
最大値：79.071 ミリ秒
平均値：22.02011 ミリ秒

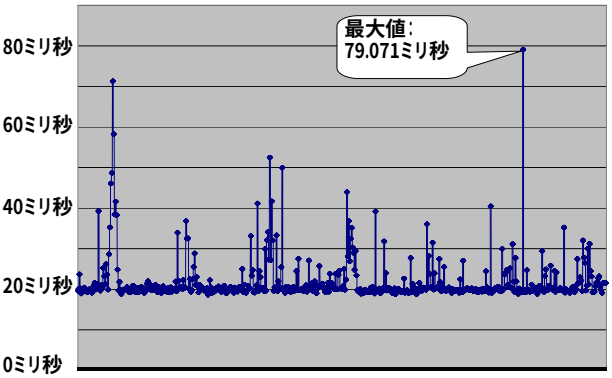

図 5：インターネットを介したネットワーク遅延

また、2 (T_o + T_d) の値は以下のようになった。
最大：181.558 ミリ秒
平均：46.5722 ミリ秒

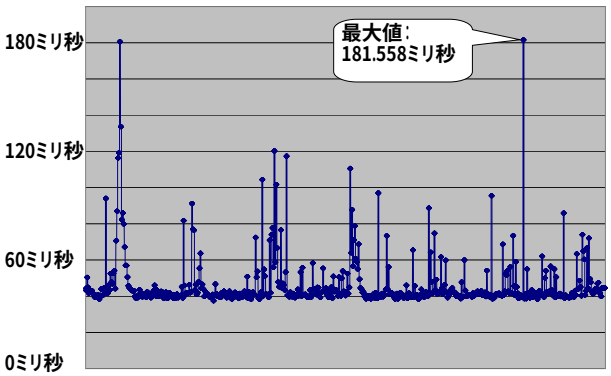

図 6：2 (T_o + T_d) の値

1 週間で取得した offset 値、ネットワーク遅延のサンプル数は 9477 個であった。取得したサンプルに対し、以下の生成間隔に設定した場合の監視の成功率を示す。

①生成間隔　182 ミリ秒
　全体サンプル数：9477
　監視成功数：9477
　監視成功率：100%

生成間隔を 182 ミリ秒以上に設定した場合、監視は全て成功する。時刻認証子による時刻配信を実施する際には、事前にネットワーク遅延、offset 値を調査し、監視成功率 100%となる値の設定を推奨する。また、時刻認証子配信に専用線を使用できない場合、想定外のネットワーク遅延、offset 値が発生する場合が考えられるので、生成間隔を大きめに設定したほうがよい。

②生成間隔　181 ミリ秒
　全体サンプル数：9477
　監視成功数：9460
　監視成功率：99.82061%

生成間隔を 181 ミリ秒以下に設定した場合、監視が失敗するケースが発生する。監視が成功するまで、時刻認証子の非改ざん性を保証できない。

④生成間隔　37 ミリ秒以下（参考）
　全体サンプル数：9477
　監視成功数：0
　監視成功率：0%

生成間隔を 37 ミリ秒以下に設定した場合、監視はまったく成功しない。

4. 本方式の考察

本論文では、インターネットを使用した場合の、時刻認証子の監視間隔、生成間隔の理想値を求めた。よって、TA が TSA の時刻の正当性をミリ秒のオーダーで検証することを可能とし、TSA 管理者による時刻改ざんの不正行為の検出・防止を可能とする。今回、実際のインターネット上で計測した値から、時刻認証子の生成間隔は 182 ミリ秒以上を理想的な値とした。したがって、TSA 管理者は、時刻認証子を改ざんした場合でも 182 ミリ秒以内の改ざんしかできない。現在、1 秒未満の精度を必要とするアプリケーションは見当たらないため、この生成間隔で時刻認証子を生成するのは有効である。また、今後ミリ秒単位の精度を必要とするアプリケーションが普及した場合でも、有効と思われる。

生成間隔を 182 ミリ秒に設定した場合でも、offset 値、ネットワーク遅延によっては、監視が成功しない可能性がある。監視が失敗した場合、次回以降監視が成功すれば、TSA の時刻認証子の非改ざん性を保証できる。

時刻認証子の生成と監視間隔を共に 1 秒にしたとき、TSA で生成された時刻認証子のデータ量は 1 週間で 135.5M バイトであった。また、1 週間分の時刻認証子の正当性検証には、約 6.6 秒の時間がかかった（実行環境：ペンティアム 4

3.2GHz、メモリ　1.0Gbyte)。生成間隔、監視間隔を共に 200 ミリ秒にした場合、1 年間で生成される時刻認証子のデータ量は、約 33G バイトと予想される。また、1 年間に生成される時刻認証子の検証に要する時間は、約 28 分程度と予想される。したがって、実際に TA が TSA 内の時刻認証子を検証する場合、十分実用可能な時間で検証が完了する。

5. おわりに

時刻認証子による時刻配信システムに関して、「時刻認証子による時刻証明方式」[3]では、時刻認証子の基本方式を提案した。また「時刻認証子よる配信時刻証明方式」[4]では、時刻認証子による時刻配信システムの実装のため、時刻認証子のパラメータの改良を行った。本報告では、時刻認証子を実網上で評価した結果、時刻認証子による時刻配信方式を用いたシステムは、時刻改ざんの検出に実使用環境で有効なことが明らかになった。

6. 謝辞

本評価を実施するにあたり、実験環境の提供をいただいた、株式会社アット東京様(http://www.attokyo.co.jp)に深く感謝いたします。

参考文献

[1] C. Adams, C. Cain, D. Pinkas, R. Zuccherato, “Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)”, RFC3161, August 2001

[2] David L. Mills, “Network Time Protocol (Version 3) Specification, Implementation and Analysis”, RFC 1305, March 1992

[3]島成佳，小松文子，時刻認証子による時刻証明方式，コンピュータセキュリティ研究会 2003

[4]久保寺範和，島成佳，石崎健太郎，小松文子，時刻認証子による配信時刻証明方式，コンピュータセキュリティ研究会 2004