

複合的証明情報提供サービス

Multiple events certification services

宮崎 一哉†

Kazuya Miyazaki

の信頼性が問題となる。

1. はじめに

偽装、偽造に関わる昨今の事件を反映して、安全・安心に対する国民の意識はますます高まっている。一方、ICT (Information & Communication Technology: 情報通信技術) による社会基盤が整備され、利活用が進みつつある中においても、不正や過失によるデータの容易な改竄が大きな社会不安を招くことが危惧されている。このような背景のもと、安全・安心に関わる行為が正当になされたか、正しく管理されたか等を第三者によって証明する仕組みに対する要求が高まっている。

タイムスタンプサービス[1]はそのような要求に応える社会基盤としての仕組みの一つである。タイムスタンプサービスは、電子データの存在時刻及び非改竄性を第三者として証明する。総務省が2004年11月5日に発表した「タイムビジネスに係る指針(ネットワークの安心な利用と電子データの安全な長期保存のために)」においてタイムスタンプサービス(時刻認証業務)を定義しており(http://www.soumu.go.jp/s-news/2004/041105_3.html)、それに呼応して、財団法人日本データ通信協会が2005年2月に「タイムビジネス信頼・安心認定制度」(<http://www.dekko.or.jp/tb/tbtop.html>)を創設、既に数社が認定を受け、商用サービスを提供するに至っている。

また、システムの基本的なデータとして様々な場面で使われる“位置”と“時刻”の情報を、GPS衛星による位置情報と気象衛星から定期的に送信される雲の画像をもとに生成する証明情報により第三者の立場で証明する位置時間証明情報サービス“COCO-DATES[2]”もある。

前者のタイムスタンプサービスは、デジタルデータと時刻を、後者のCOCO-DATESは位置と時刻、更には証明情報の発行を要求した端末の識別情報を複合させ、その関連性を証明するものである。本稿では、このような複合させた情報の関連性を証明するための基本的な仕組みを提案し、その適用例について考察を加える。

2. 複合的証明の条件

複合的証明とは、ある事象に関連して計測あるいは認識した結果を複合的に証明することである。例えば、タイムスタンプサービスでは、クライアント端末で電子文書のハッシュ値を計算(広い意味で認識処理と捉える)、サーバに送付し、サーバにおいてシステム時計で計測した時刻情報とを結合し、その関連性を証明するために結合データに改竄検知コードを付与する。また、COCO-DATESでは、クライアント端末でGPSにより位置情報を計測し、サーバ側では位置情報にクライアント端末ID(認識結果と捉える)と時刻情報を組み合わせ、改竄検知コードを付与する。このとき、特にクライアント端末における計測/認識結果

†三菱電機(株), Mitsubishi Electric Corporation

対象	入力データ	処理装置	結果
電子文書	電子文書データ	ハッシュ計算モジュール	文書のハッシュ値
時刻	クロック信号	システム時計	時刻情報
位置	複数のGPS衛星からの信号	GPS端末装置	位置情報
顔(個人)	顔画像	顔認識装置	個人ID

3. システム構成

証明情報の提供を要求するクライアント端末と、証明情報を提供するサーバはインターネット等のネットワークで結合されているものとする。クライアントとサーバの構成を図1に示す。

クライアント及びサーバは、それぞれ複合計測/認識機能を持つ。これは、複数の対象を計測あるいは認識した結果を結合し、それに対して改竄検知コードを付与する機能である。

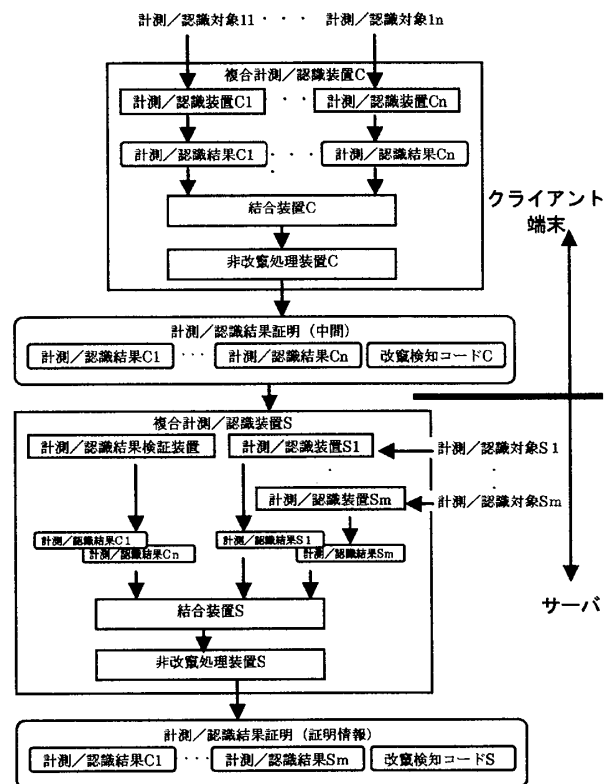


図1 システム構成

4 システムの動作

位置と時刻に加え、操作者個人の本人性を複合的に証明する場合を例に取り、システム動作を説明する。

(1) クライアント端末の処理

計測／認識装置 C 1 に GPS アンテナが、計測／認識装置 C 2 として顔認識装置が割り当てられているとする。計測／認識装置 C 1 (GPS アンテナ) によりクライアント端末の位置情報を含む情報を計測／認識結果 C 1 として得る。ここに、結果の正当性を証明する正当性保証情報 (偽造防止用のエビデンス) を含んでも良い。

計測／認識装置 C 2 (顔認識装置) により、計測／認識装置 C 2 の入力装置 (カメラ) から得た顔画像を照合用の登録データと照合するなどして、認識処理を行い、照合結果として個人に割り当てられた ID などを含む情報を計測／認識結果 C 2 として得る。同様に、結果の正当性を証明する正当性保証情報を含んでも良い。

結合装置 C で、計測／認識結果 C 1 と計測／認識結果 C 2 を結合し、結合データを得る。次に非改竄処理装置で、結合データに対して改竄検知コードを生成し、結合データと改竄検知コードを結合して計測／認識結果証明 (中間) を得る。改竄検知コードの生成方法としては、(電子署名法で定義されるような) 電子署名、HMAC などを利用する。

(2) 転送処理

得られた計測／認識結果証明 (中間) をクライアント端末からサーバにネットワークを利用して転送する。転送にはネットワークを利用しない方法 (記憶媒体を用いる方法、USB、その他のデータ転送手段を用いる方法など) を利用してもかまわない。

(3) サーバの処理

サーバでクライアント端末から転送されたデータを受け取ると、受け取ったデータを計測／認識結果検証装置で検証する。検証内容は、改竄検知コード C の検証による結合データ C の非改竄性で、改竄検知コード C の生成方法に応じた方法により検証する。検証内容として、計測／認識結果自体の正当性検証を含めても良い。この場合、計測／認識結果自体に含まれる正当性保証情報 (偽造防止用エビデンス) や、サーバが持つ正当性保証情報あるいは方法により検証することになる。

検証に成功すると、サーバ側では複合計測／認識装置 S の計測／認識装置 S 1 (システム時計) により、現在時刻を計測／認識結果 S 1 として得る。そして、クライアント端末から送付された計測／認識結果 C 1、計測／認識結果 C 2、サーバ側で生成した計測／認識結果 2 1 を結合装置 S で結合し、結合データ S を得る。最後に非改竄処理装置 S で、結合データ S に対して改竄検知コード S を生成し、結合データ S と改竄検知コード S を結合して最終的な計測／認識結果証明 (証明情報) を得る。

得られた計測／認識結果証明をサーバからクライアント端末に送り返しても良い。

5. 考察

クライアント端末が計測／認識結果証明 (中間) に改竄検知コード C を添付することにより、クライアント端末以外による計測／認識結果の改竄は検知可能 (改竄がないことを証明可能) となる。クライアント端末が計測／認識結

果証明 C を生成することにより、クライアント端末が計測／認識結果を保証する。クライアント端末が信頼できれば、通信路上での改竄の余地はなくなり、計測／認識結果証明 (中間) の計測／認識結果が信頼できることとなる。

またクライアント端末から送付された計測／認識結果証明 (中間) をサーバが計測／認識結果検証装置により検証を行うことにより、クライアント端末から送付された計測／認識結果の内容が第三者により改竄されているか否かを検知できる。この場合、計測／認識結果自体に含まれる正当性保証情報や、サーバが持つ正当性保証情報あるいは方法により検証すると、クライアント端末が生成した計測／認識結果自体の正当性を検証できる。このようにクライアント端末とサーバで2段階の認証 (検証) を行なうことにより、証明内容をより信頼性高いものとできる。

また、クライアント端末での認証 (検証) に失敗した場合はサーバ側にデータを送付しないようにすることにより、認証 (検証) に成功するデータのみを送付でき、無駄なトラフィックを低減できるという効果も得られる。

サーバが計測／認識結果証明に改竄検知コード S を添付することにより、サーバ以外による計測／認識結果の改竄は検知可能 (改竄がないことを証明可能) となる。サーバは信頼のおける第三者機関であると想定すると、計測／認識結果証明の内容が信頼できることとなる。

この技術により、従来の証明内容が、時刻、位置、機器 (ID) に限られていたものが、本人であることなどを更に組み合わせて証明することができるようになる。

安全性を高めるためには、複合計測／認識装置 C を耐タンパな装置として実現することが考えられる。これにより内部の処理やデータを改竄不能とでき、つまりクライアント端末操作者による故意の改竄を防止することができ、クライアント端末による計測／認識結果の信頼性が高まる。またそれに伴い、その計測／認識結果に基づいてサーバにより生成される計測／認識結果証明の信頼性も高まる。

6. おわりに

複合的証明情報提供サービスにより、従来実現されていた電子データの存在時刻と非改竄性、位置と時刻と端末 ID など関連性の証明情報だけでなく、顔認証との組み合わせにより、更に本人であることとの関連性 (いつ、誰が、どこで、何を、など) をも証明できる可能性がある。ただし、偽造のできない安全な証明情報を提供するためには、端末の耐タンパ化や正当性保証情報 (偽造防止用エビデンス) による対策が鍵となる。特に後者は計測／認識対象により変わってくる場所であるが、現在、顔認証に基づく本人認証証明を可能とする仕組みを検討している。今後、これらの検討を深め、安全な複合的証明情報提供サービスの実現を目指す。

参考文献

- [1] RFC3161, "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)", 2001
- [2] 宮崎他、「位置時刻情報証明サービス COCODATES」、システム/制御/情報、第 50 巻 第 4 号、システム制御情報学会、2005