大学における私的電子公証サービス

場田, 隼也
九州大学理学部物理学科情報理学コース

伊東, 栄典
九州大学情報基盤研究開発センター : 准教授 : 情報学

中國, 真教
九州大学情報基盤研究開発センター : 准教授 : 情報学

出版情報：電子情報通信学会2009総合大会. BS-11-4, 2009-03. 電子情報通信学会
バージョン：
権利関係：

大学における私的電子公証サービス

Private Electronic Notary Service in University

場田隼也 [1] 伊東栄典 [2] 中國真教 [2]
Toshiya Bata Eisuke Ito Masanori Nakakuni

九州大学 理学部 物理学科 情報理学コース [1]
Informatics Course, Department of Physics, Faculty of Science, Kyushu University
九州大学 情報基盤研究開発センター [2]
Research Institute for Information Technology, Kyushu University

1 はじめに

近年，様々なコンテンツがインターネット上で公開されている。大学においても，論文の電子ファイルを機関リポジトリなどで公開している。コンテンツをインターネット上で公開することにより，コンテンツの流通が活発化し，かつコンテンツの閲覧が容易化する反面，途中でコンテンツの一部が欠落したり改竄される可能性が高くなる。コンテンツ作成者に無断で書き換えられることは作成者や閲覧者にとって不利益となる。例えば，論文の内容が事実に反した内容へと書き換えられていれば，作成者および大学の信用を損なう。従って，作成したコンテンツの公開では，作成者や発行元，コンテンツの内容についての信頼性を保証する仕組みが必要である。

我々は大学のような機関が所有・公開するコンテンツの信頼性向上の仕組みとして，私的電子公証サービス (PENS) を提案する。本論文では，PENS の提案と大学における PENS の利用例について述べる。

2 PKI によるコンテンツの信頼性検証

コンテンツの信頼性を検証する有力な方法として，公開鍵基盤 (PKI: Public Key Infrastructure) [1] を用いたものがある。

サーバには，サーバの秘密鍵で暗号化されたコンテンツがある。コンテンツをダウンロードした後，復号する際に必要となるサーバの公開鍵は，もしかしたら悪意を持った者による偽の公開鍵かもしれない。そこで閲覧者も信頼している認証局 (CA:Certificate Authority) によって，サーバの公開鍵が本物であることを証明してもらうというものだ。まず，認証局の秘密鍵でサーバの公開鍵と所有者情報を暗号化し，署名を作成する。この署名を閲覧者が認証局の公開鍵で復号化することで，サーバの公開鍵を手に入れることができ，その公開鍵が本物であることが分かるという仕組みである。

PKI を用いた方法は，署名によりコンテンツの改竄を防ぐことができ，不特定多数を相手にしても 鍵の管理が楽であるという利点を持っている。しかし，公的な認証局を用いると導入時にコストを要し，私的な認証局を設けても自己署名証明書を配布することが難しいという大きな欠点を持っている。また，閲覧者がコンテンツを開く度に署名の有無を確認することは大変煩わしい。そのため，誰もが容易にコンテンツの信頼性を検証できるような仕組みを安価で実現する必要性がある。

3 PENS システム

3.1 ハッシュ値を用いたコンテンツの信頼性検証

誰もが容易にコンテンツの信頼性を検証できる仕組みとして，ハッシュ値を用いたコンテンツの信頼性を検証する方法を提案する。これは，改竄などがされていない中身が一致する 2 つのコンテンツであればそれぞれハッシュ値は必ず一致するという事実を用いた方法である。2 つのハッシュ値を比較して，データの同一性を検証する方法は従来から存在するが，この方法を閲覧者が容易に使用できるようなシステム [2][3] の構築を検討した。我々は，このシステムを PENS(Private Electrical Notary Service: 私的電子公証サービス) と名付けた。

権限を与えられた登録者は，利用者認証を経て，コンテンツをアップロードする。サーバはコンテンツのハッシュ値を生成し，コンテンツのメタデータ (作成者，作成日，タイトル等) を PENS のデータベースに登録する。その過程を図 1 に示す。データベースでは，登録されたハッシュ値とメタデータを公開する。信頼性を検証したい閲覧者は，定められた手順に従って，入手したコンテンツのハッシュ値とデータベースに登録されたハッシュ値の両者を比較・照合する。照合できればコンテンツの作成者に関する情報が得られ，照合できなければ第三者によって改竄された可能性があることを知ることができる。その過程を図 2 に示す。

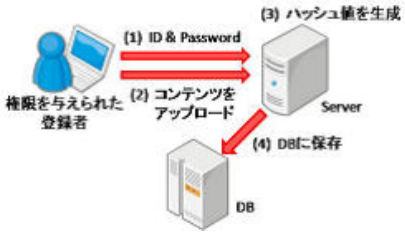

図 1 コンテンツの登録

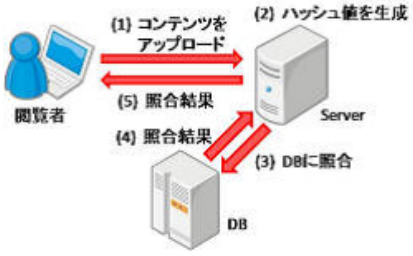

図 2 コンテンツの信頼性検証

3.2 PENS Network

コンテンツの信頼性を検証するために，ある PENS サーバで照合する。サーバに一致するものがなければ，次にどの機関の PENS サーバにアクセスすればよいかを閲覧者自身が判断するのは困難である。コンテンツの作成者やその所属が不明であれば，照合を試みる PENS サーバを選ぶことはできない。

そこで，PENS Network を提案する。これは機関ごとに設けられた PENS サーバを結んで PENS Network を構築し，それぞれの PENS サーバで照合していくというものである。その概念図を図 3 に示す。

Network の構成方法については，メッシュ構造やハブ構造，木構造などがある。PENS Network においては，木構造を用いる。木構造であれば，PENS サーバの数がどれほど多くなったとしても，他の構造より処理速度を速くすることができると考えるからである。

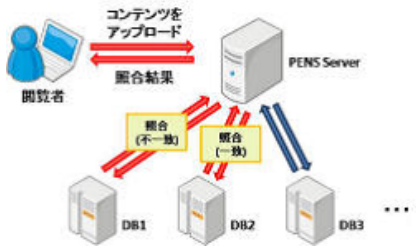

図 3　PENS Network の概念図

4　PENS システムの試作

ここでは試作した PENS システムについて述べる。PENS システムの開発環境を表 1 に示す。

表 1　PENS システム開発環境

ハードウェア	
CPU	AMD Athlon 64 Processor 3500+
memory	512MB
HDD	400GB
ソフトウェア	
OS	FreeBSD6.2
ウェブサーバ	Apache2.2.4
データベース	SQLite3
開発言語	Ruby on Rails2.0.2, Ruby1.8.6
ハッシュ関数	SHA-1(Secure Hash Algorithm 1)

コンテンツの登録者は，ウェブブラウザで PENS サーバにアクセスする。その際，所属組織によって提供される認証サーバと連携し，利用者認証を行う。筆者の所属する九州大学では LDAP サーバでの認証サービスを行っているため，今回の試作システムでは LDAP サーバとの連携による認証を行うこととした。登録するコンテンツを PENS サーバにアップロードすると，PENS サーバ側でハッシュ値生成を行い，そのハッシュ値とメタデータを DB に登録する。

PENS の試作システムでは，ハッシュ値を生成するハッシュ関数として SHA-1(Secure Hash Algorithm 1)[4] を用いた。これはコンテンツの長さが 2^{64}bit，つまり 2EB 未満において使用可能で，ハッシュ値が 160bit の固定長で出力される。

信頼性の検証を行う閲覧者は，ウェブブラウザで PENS サーバにアクセスする。検証を行いたいコンテンツを PENS サーバにアップロードすると，PENS サーバ側でハッシュ値を生成し，そのハッシュ値が一致するコンテンツがあるかを DB で照合する。一致するものがあればコンテンツのメタデータを，一致するものがなければないことを返す。これをウェブブラウザに表示させる。

5　おわりに

本論文では，自らが作成したコンテンツを公開する場合に，作成者・発信者の信用を損なわない仕組みについて検討した。そのための枠組みを提案し，PENS と名付けた。コンテンツのハッシュ値を利用してコンテンツの信頼性を検証する仕組みである。コンテンツの改竄を防ぐことはできないが，コンテンツの作成者と改竄の有無を検証することができる。

PENS で用いたハッシュ関数 SHA-1 は衝突耐性突破が見つかっている。より衝突の可能性が低い SHA-256(Secure Hash Algorithm 256) の導入を検討したい。

今後，PENS Network の構造を具体的に検討し，実現に向けて進めていきたい。

参考文献

[1] K Park, S Lim, K Park: ”Computationally efficient PKI-based single sign-on protocol, PKASSO for mobile devices”, IEEE Transactions on Computers 57 (6), pp. 821-834 (2008)

[2] M. Nakakuni, E. Ito, Y. Kasahara, S. Inoue and H. Dozono: ”Construction and Use Examples of Private Electronic Notary Service in Educational Institutions”, WSEAS TRANSACTIONS on Advances in Engineering Education, Issue.10 Volume.5, pp.676-686 (2008)

[3] M. Nakakuni, E. Ito, Y. Kasahara, and H. Dozono: ”Private Electronic Notary Service in Universities and Its Utilization in Education”, Proceedings of the 4th WSEAS/IASME Int. Conf. on EDUCATIONAL TECHNOLOGIES (EDUTE’08), pp.170-175 (2008)

[4] T Grembowski, R Lien, K Gaj, N Nguyen, P Bellows, J Flidr, T Lehman, B Schott: ”Comparative Analysis of the Hardware Implementations of Hash Functions SHA-1 and SHA-512”, Lecture notes in computer science, pp.75-89 (2002)