D-038

サーバー型放送で利用するメタデータのデジタル署名方式

XML Signature for Metadata on Broadcasting System Based on Home Servers

西本 友成[†] **馬場 秋継**[†] **石川 清彦**[†] **中村 晴幸**[†] **栗岡 辰弥**[†]*
Yusei Nishimoto[†], Akitsugu Baba[†], Kiyohiko Ishikawa[†], Haruyuki Nakamura[†] and Tatsuya Kurioka[†]*

1．まえがき

サーバー型放送は、番組やシーンの関連情報であるメタデータを利用することで、重要なシーンのみを視聴するダイジェスト視聴や、シーン単位のコンテンツ検索など多様な視聴機能を提供する。このメタデータを利用した新しい放送サービスに関する検討結果を既に報告した[1]。メタデータを用いてコンテンツを編集・再構成して視聴することが容易になるため、放送事業者の意図しないコンテンツ利用が行われる恐れがある。メタデータ利用におけるコンテンツの著作権保護を実現するためには、メタデータの改ざんを防止し、メタデータの制作者を証明できる必要がある。

本稿では、メタデータの制作環境と検討課題について述べ、課題解決のためのデジタル署名方式を提案する。さらに、試作した検証実験システムで本デジタル署名方式を検証した結果について報告する。

2．メタデータの制作環境と検討課題

サーバー型放送のメタデータは、XML(eXtensible Markup Language)で記述され、以下の４種類に大別できる。

1)コンテンツ記述メタデータ
　タイトルやジャンルなどの一般的なコンテンツ情報を記述
2)インスタンス記述メタデータ
　チャンネル名などのコンテンツの送出過程の情報を記述
3)セグメンテーションメタデータ
　番組内のシーンなどのセグメント情報や、そのセグメントをまとめたセグメントグループ情報を記述
4)視聴者メタデータ
　ブックマークなどの視聴者によって作成されるメタデータを記述

放送事業者が 1)～3)すべてのメタデータを制作し放送・通信により配信するだけでなく、複数の制作者が連携してメタデータを制作することが想定されている。例えば、コンテンツ著作者がコンテンツ記述メタデータとセグメンテーションメタデータ、放送・通信事業者がインスタンスメタデータ、視聴者が視聴者メタデータを制作して、一つのメタデータを作成する。

そのため、複数の制作者が連携したメタデータ制作環境に適用できるメタデータのためのデジタル署名技術を開発する必要ある。また、すでに規格化されているメタデータの記述スキーム[2][3]の変更を最小限に抑えなければならない。

3．メタデータのためのデジタル署名方式

XML 文書の改ざんを防止し、文書の制作者を証明できる技術として、XML 署名技術がある。今回、XML 署名技術をベースとしたメタデータのためのデジタル署名方式を開発した。

図 1 に、本デジタル署名方式の概要を示す。コンテンツ著作者はコンテンツ記述メタデータとセグメンテーションメタデータを制作して署名し、放送・通信事業者はインスタンス記述メタデータを追加して署名する。さらに、視聴者が視聴者メタデータを追加して署名する。

この署名に、XML 署名技術を適用すると、放送・通信事業者がインスタンス記述メタデータを追加した時点で、改ざんとみなされてしまう。そのため、各の制作者は、署名後に追加されるメタデータを考慮しておく必要がある。そこで、署名対象を XPath(XML Path Language)でフィルタリングして署名する方式とした。表 1 に、フィルタリング方法を示す。各の制作者が制作するメタデータの種類を整理し、XML 署名の Refernce 要素で指定するフィルタを定義した。

図 2 に、本デジタル署名方式を用いて制作したメタデータインスタンスを示す。各の制作者の署名値はメタデータ文書の最後に列挙することとした。規格化されている記述スキームは、署名値のみの追加となり、変更を最小限に抑えることができた。

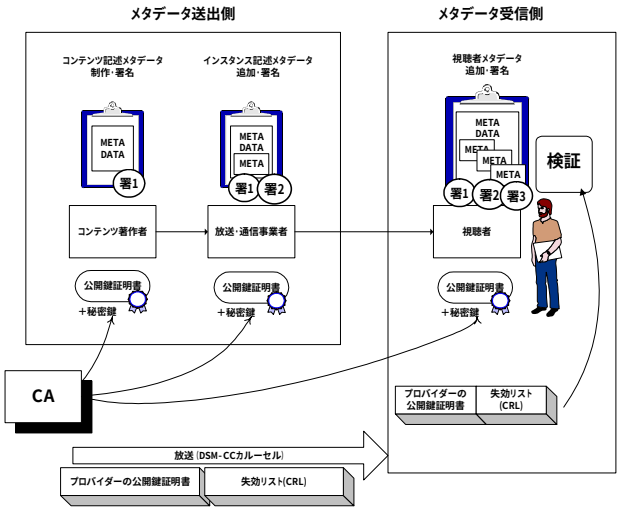

図１　メタデータのためのデジタル署名方式

†NHK 放送技術研究所
＊現在、NHK 営業局受信技術センター(受信計画)
†NHK Science and Technical Research Labs.
＊Currently with NHK Audience Services Department, Engineering & Services Center for Reception (Planning)

表 1　デジタル署名におけるフィルタリング方法

メタデータ制作者の種別	フィルタリング方法	指定手段
コンテンツ記述メタデータと セグメンテーションメタデータの制作者	次のタグ以外を対象とする ・ProgramLocationTable ・ServiceInformationTable ・他で作成された SegmentInformation SegmentGroupInformation	Xpath
インスタンス記述メタデータの制作者	次のタグを対象とする ・ProgramLocationTable ・ServiceInformationTable	Xpath
視聴者メタデータの制作者	追加したタグを対象とする ・SegmentInformation ・SegmentGroupInformation	Xpath

4．検証実験

4.1 検証実験システム

メタデータの署名検証を行う受信機を Pentium4 3.0GHz、メモリ 512MB の PC で試作した。デジタル署名用の公開鍵証明書と秘密鍵の暗号アルゴリズムは RSA とした。安全性を確保するために、その秘密鍵と公開鍵証明書を、IC カード内(CAS カード)に納めて配布する構成とした。また、公開鍵証明書の失効確認は、放送経由で受信機に事前に蓄積した失効リストを用いた。

4.2 デジタル署名の検証処理

本方式の受信機への負荷を把握するために、デジタル署名付きメタデータの読み込み時間を評価した。図 3 に評価結果を示す。メタデータのデジタル署名をコンテンツ著作者と放送・通信事業者の 2 者とし、その 2 者によって制作される一つのメタデータのサイズの合計を 13kB とした。

評価した結果、デジタル署名付きメタデータを一つ読み込むのに、4.8 秒必要であることが分かった。コンテンツの提示まで考慮すると、さらに暗号化コンテンツを復号するためのライセンス設定処理が必要である。そのため、メタデータを読み込んでからコンテンツを提示するまで、6 秒程度必要になる。この時間はできるだけ短くすることが要求される。メタデータを受信機に入力する時に予め署名検証して蓄積する手法をとれば、この時間を 1、2 秒程度に抑えることができる。

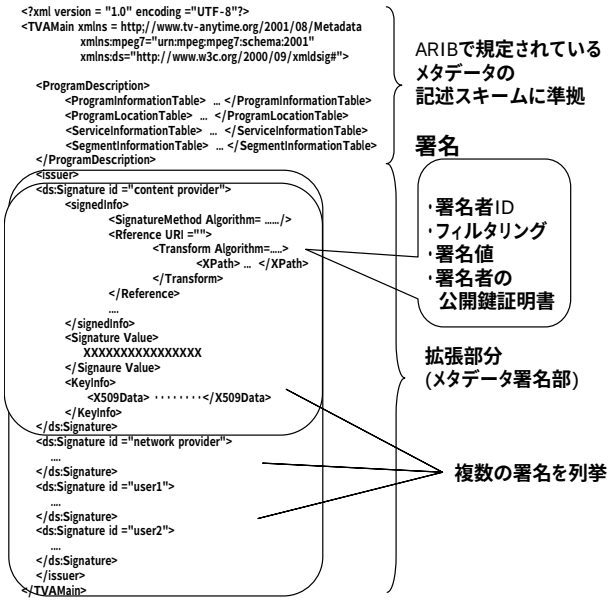

図 2　デジタル署名付きメタデータインスタンス

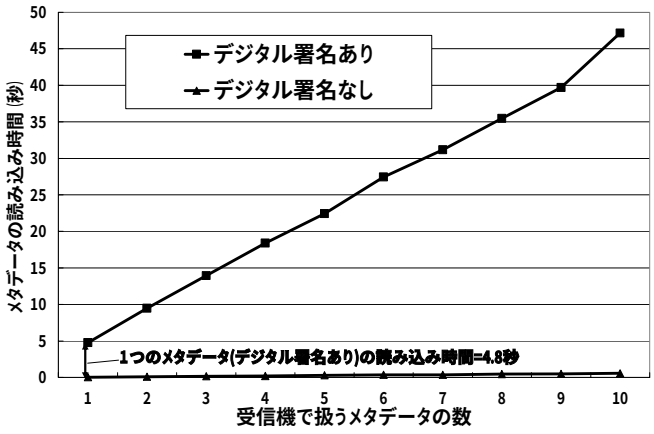

図 3　メタデータの署名検証に必要な時間

5．まとめ

規格化されているメタデータの記述スキームの変更を最小限に抑えながら、複数の制作者が連携してメタデータ制作できる、サーバー型放送のためのデジタル署名方式を提案し、その実現性を確認した。

【参考文献】
[1]馬場、西本、南、栗岡:“メタデータを利用したサーバー型放送の一検討”映情学年大、1-5(2002)
[2]電波産業会:“サーバー型放送における符号化、伝送方式、伝送及び蓄積制御方式”標準規格、ARIB STD-B38 (2003)
[3]TV-AnytimeForum:“Metadata”、SP003v13(2003)