1F-2

# セキュアストレージシステムの開発(2)
## - デジタル署名有効期限延長方式の提案 -

鴨志田 昭輝　　宮崎 一哉　　中川路 哲男
三菱電機(株) 情報技術総合研究所

## 1. はじめに

近年の企業内や官公庁における急速な情報化に伴い、公文書、カルテ、課金情報、技術文書、顧客情報といった高度なセキュリティを要するデジタルデータについても、急速に電子化が進められている。このようなニーズにこたえるために、著者らはデジタルデータを安全に長期間保存するセキュアストレージシステムの開発を行っている。セキュアストレージシステムのコンセプト、安全要件およびそれを実現する技術については、文献[1]にて詳しく述べる。本稿では、高度なセキュリティを要するデジタルデータを長期間保存する技術、特にデジタル署名の有効期限延長方式について述べる。そして、セキュアストレージシステムにおける信頼モデルを定義し、それに適合する効率のよいデジタル署名有効期限延長方式を提案する。

## 2. デジタルデータの長期保存技術

高度なセキュリティを要するデジタルデータを長期間にわたり保存する場合に発生すると考えられる問題点を以下に挙げる。

1. データに付加されたデジタル署名が、有効期限切れのため失効する(有効性が失われる)
2. 保存されている暗号化データの秘匿性が、時間の経過に伴って失われる
3. 保存されているデータを閲覧するための環境が、時間の経過に伴って失われる
4. 不慮の事態に備えてのバックアップ情報から、情報が漏洩する

本稿では、主に問題点 1. を解決する手段について論じる。問題点 2. を解決する手段としては、適切なタイミングで、保存されている暗号化データをより強い暗号方式、あるいはよりサイズの大きい暗号鍵を用いて再度暗号化する等が考えられる。問題点 3. を解決する手段としては、XML を用いてデータを保存することにより、将来予想される閲覧プログラムの更新に備える等が考えられる。問題点 4. を解決する手段としては、データを暗号化してバックアップする等が考えられるが、鍵管理の問題など解決すべき課題は多い。

## 3. デジタル署名の有効期限延長

デジタル署名を長期間保存する場合、保存されているデジタル署名の有効性が時間の経過に伴って失われてしまうという問題がある。文献[2]では、デジタル署名にタイムスタンプを付加する(延長されたデジタル署名に現在時刻を結合し、第三者機関の署名を付加する)ことにより、デジタル署名の有効期限を延長する方式が提案されている。このようなデジタル署名有効期限延長方式の原理を図 1に示す。

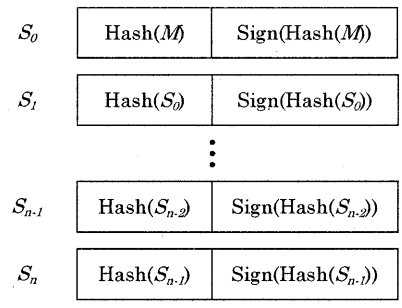


**図 1 デジタル署名の有効期限延長方式の原理**

上記のような方式では、保存しているデジタル署名が有効である期間内のある時点で、信頼できる機関のデジタル署名を付加するといった処理が行われる。しかし、延長されたデジタル署名にも有効期限があるた

---

Development of Secure Storage System (2)
- How to extend validity of digital signature -
Akiteru Kamoshida, Kazuya Miyazaki, Tetsuo Nakakawaji
Information Technology R & D Center,
Mitsubishi Electric Corporation

め、長期間保存する場合には何度も有効期限の延長を行う必要がある。延長署名を検証する場合、最新の延長署名 $S_n$ の有効性を検証するだけでなく、オリジナル署名 $S_0$ および延長署名 $S_1$～$S_n$ のすべての整合性を検証する必要があるため、検証に手間がかかり、データ量も大きくなるという欠点がある。

## 4. セキュアストレージシステムの信頼モデル

セキュアストレージシステムにおけるデジタル署名の有効期限延長に関わるコンポーネントの構成を図 2 に示す。

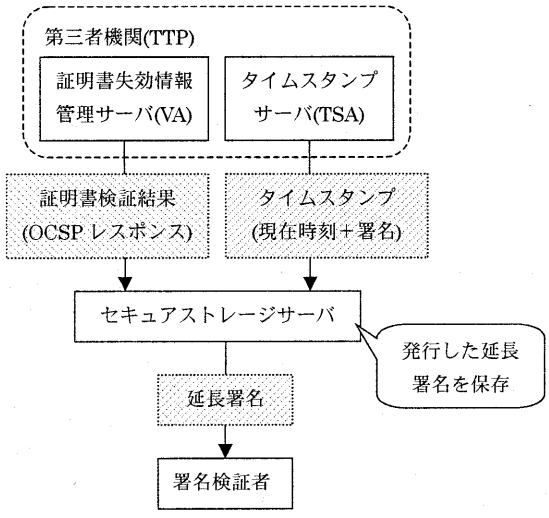


図 2 セキュアストレージシステムの構成

セキュアストレージシステムにおける各エンティティの信頼モデルは以下のように定義される。

1. 署名検証者は、第三者機関(Trusted Third Party)を常に信頼する
2. 署名検証者は、通常はセキュアストレージを信頼する
3. 裁判などより高度な証拠能力が必要なケースでは、セキュアストレージは不正をしていないことを立証できる証拠(タイムスタンプ等)を提出する(署名検証者はセキュアストレージを信用しない)

## 5. 提案するデジタル署名有効期限延長方式

上記のような信頼モデルにおいては、図 3ような方式を適用することにより、検証に要する手間とデータ量を削減することができる。

1. 署名延長時、セキュアストレージは最新の延長署名延長 $S_{n-1}$ のハッシュにオリジナル署名 $S_0$ のハッシュを連結したものに第三者機関の署名(タイムスタンプ)を付加し、延長署名 $S_n$ を発行する
2. 通常(セキュアストレージが十分信頼できるケース)の検証時には、最新の延長署名 $S_n$ の有効性と、最新の延長署名 $S_n$ およびオリジナル署名 $S_0$ の整合性を検証する
3. より高度な証拠能力が必要な場合の検証時には、最新の延長署名 $S_n$ の有効性だけでなく、オリジナル署名 $S_0$ および延長署名 $S_1$～$S_n$ のすべての整合性を検証する

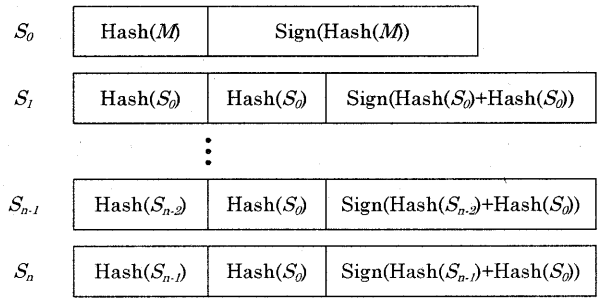


図 3 提案方式の原理

提案方式により、通常の検証に要する手間とデータ量を削減することができる。より高度な証拠能力が必要な場合の検証には、従来通りの手間とデータ量が必要となる。

## 6. まとめ

セキュアストレージシステムにおける信頼モデルを定義し、それに適合するデジタル署名有効期限延長方式を提案した。これにより、検証に要する手間とデータ量を軽減することができる。

## 参考文献

[1] 宮崎 一哉, 鴨志田 昭輝, 中川路 哲男, "セキュアストレージシステムの開発(1)," 第 61 回情報処理学会全国大会講演論文集, 1F-1, Sep. 2000

[2] J. Ross, D. Pinkas, N. Pope, "Electric Signature Formats for long term electronic signature," IETF S/MIME-WG Internet Draft, Jul. 2000