1F-1

セキュアストレージシステムの開発(1)
- 電子データの長期保存における原本保証、秘匿、公証技術 -

宮崎 一哉　　鴨志田 昭輝　　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。本稿では、セキュアストレージシステムのコンセプト、安全性要件およびそれを実現する技術について述べる。

2. セキュアストレージシステム

セキュアストレージシステムは、日常の業務で定常的に利用する文書のリポジトリではなく、主に法制度からの理由により長期間保存することが要請される文書を保管するシステムである。文書管理システムやワークフローシステム等のバックエンド、あるいは、従来の紙やマイクロフィルムの倉庫サービスの電子版、いわばデジタル倉庫サービスを実現するためのシステムとして位置づけられる(図1)。このようなシステムには操作性や信頼性も要求されるが、本稿では特に安全性に関して述べることとする。

3. 安全性要件

我々は、セキュアストレージで実現すべきデジタルデータ保存における安全性要件を、以下のように定義した。

1. 保存したデジタルデータが原本として正しく管理され、改竄等の脅威から守られていること
2. 情報が不正に流出しないこと
3. デジタルデータの特定時刻における存在、預け入れや削除等の事象を第三者に証明できること

上記のような安全性要件を満たすため、我々は以下のようなセキュリティ機能をセキュアストレージシステムで実現した。

1. 原本性保証機能
2. 秘匿機能
3. 公証機能

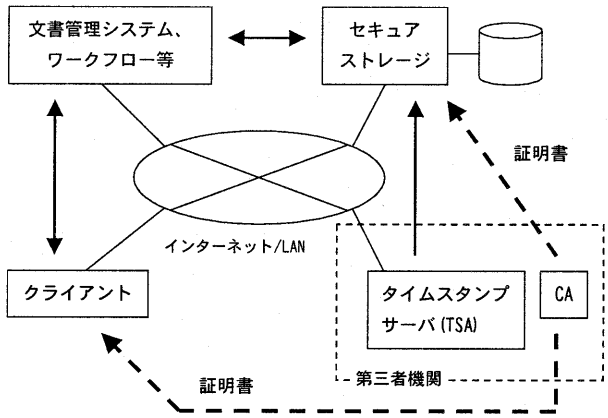

図 1 システム構成例

4. 原本性保証技術

保存したデジタルデータは、セキュアストレージ上で原本として正しく管理され、改竄等の脅威から守られている必要がある。文献[2]では、“原本性を確保する”とは、“電子文書について、紙文書と比較した場合の保存・管理上の問題点が解決された状態にあるようにしておくこと”と定義したうえで、原本性を確保するために充足すべき要件を以下のように定義している。

1. 完全性の確保 … デジタルデータの原本が確定的なものとして作成され、改竄への対策が十分なされ

Development of Secure Storage System (1)
- Certification of Originality, Provision of Confidentiality and Notary Service -
Kazuya Miyazaki, Akiteru Kamoshida, Tetsuo Nakakawaji
Information Technology R & D Center,
Mitsubishi Electric Corporation

ている

2. 機密性の確保 … デジタルデータへのアクセスが適切に制御され、情報漏洩の防止措置が十分なされている
3. 見読性の確保 … デジタルデータの内容が必要な機材を用いて直ちに表示できるように措置されている

上記要件をセキュアストレージシステムで満たすべき要件とし、これらを満たすために以下のようなセキュリティ機能を実現した。

1. PKI ベースのユーザ認証およびアクセス制御
2. 保存データおよび通信路の暗号化
3. 保存データへのアクセス履歴の記録
4. 保存データへのデジタル署名の付加

なお、見読性については、必要な機材の配置など運用面で十分カバーが可能と思われるため、本稿の記述範囲外とした。

5. 秘匿技術

扱われるデータは、情報の漏洩を防ぐための措置が十分に図られている必要がある。セキュアストレージでは、PKI に基づいた通信路上のデータおよび保存データの暗号化を実現した。保存データの暗号化については、以下の 2 つのケースを想定している。

1. セキュアストレージに対して内容を秘匿する場合 … 利用者がデータを暗号化し、セキュアストレージに保存する
2. セキュアストレージに対して内容を秘匿しない場合 … セキュアストレージがデータを暗号化し、保存する

また、保存データへのアクセス制御を適切に行うことによっても、情報の漏洩を防止している。

6. 公証技術

重要なデータを預ける場合、預け入れた事実などを第三者に証明することができる必要がある。また、保存データのコピーが、サーバ上の原本と一致するかどうかについても、第三者に証明することができる必要がある。

セキュアストレージシステムでは、アクセスした事象や原本との一致を証明するために、電子証書を発行する。定義した電子証書は、以下の通りである。

1. 保管証明 … データをセキュアストレージに預け入れたときに発行される。データを預け入れた事象および預け入れたデータの内容を証明する。
2. 削除証明 … データをセキュアストレージから削除したときに発行される。データを削除した事象および削除したデータの内容を証明する。
3. 原本証明 … データをセキュアストレージより取得したときに発行される。データを取得した事象および取得したデータがセキュアストレージ上の原本と相違ないことを証明する。

電子証書は、上記の事象の宣言やデータの内容に対して施したセキュアストレージサービスを提供する主体によるデジタル署名と、信頼できる第三者機関が発行する特定時刻にデータが存在したことを証明するためのタイムスタンプで構成される。

7. まとめ

高度なセキュリティを要するデジタルデータを保管するシステムにおける安全性要件を整理し、セキュアストレージシステムのコンセプトを提案し、安全性要件を満たすため技術について検討した。

本提案では、特殊な耐タンパハードウェアを利用せず、PKI に立脚した暗号ソフトウェアの技術による解決を想定している。この場合、文書の長期保存を考えると、デジタル証明書の有効性の限界に起因する問題を避けて通ることができない。これらの問題点やそれを解決する技術については、文献[1]にて詳しく述べる。

参考文献

[1] 鴨志田 昭輝, 宮崎 一哉, 中川路 哲男, “セキュアストレージシステムの開発(2),” 第 61 回情報処理学会全国大会講演論文集, 1F-2, Sep. 2000

[2] 総務庁, “インターネットによる行政手続きの実現のために,” Mar. 2000