M-4

電子企業印を共有できる電子署名サーバー

日本アイ・ビー・エム株式会社 ソフトウェア開発研究所

岡本 康介、鈴木 美幸

Keywords: PKI, Security, 電子署名、公開鍵証明書, 電子政府

アブストラクト:.

インターネットにおける通信の安全性の確保や確実な本人確認を行うための仕組みとしてPKI(Public Key Infrastructure ： 公開鍵基盤)導入を検討する企業が増加しつつあり、『電子認証による電子署名』は電子商取引き、電子申請を行う上で非常に重要な位置を占めている。しかしながら、現在のところ電子認証（公開鍵暗号方式でいう秘密鍵＝電子企業印と本論では呼ぶ）を安全に共有できる仕組みは提案されていない。

本論文では、電子認証を安全に共有できる仕組みを提案する。この仕組みにより電子企業印が安全に企業内で共有できるようになった。また、CSPレベルでの実装によりアプリケーションからも電子鍵の共有が可能になった。

背景

2001年4月の電子署名法（電子署名及び認証業務に関する法律）の施行とあいまってインターネットにおける通信の安全性の確保や確実な本人確認を行うための仕組みとしてPKI (Public Key Infrastructure:公開鍵インフラストラクチャ) 導入を検討する企業が増加しつつある。また、インターネットを通じて行政サービスを提供する『電子政府・自治体プロジェクト』が本格的に動き始めている[1]。政府が2001年1月に発表した『e-Japan戦略』では、2003年度までに行政機関への申請・届出等のすべての手続きをインターネットで行う電子申請の構築を計画している。電子申請では、申請書に入力したデータをXML化し、さらに電子署名をすることになる。また、行政機関への申請に必要な手数料については、銀行のインターネットバンキングからマルチペイメントネットワーク（金融機関と収納機関の相互接続システム）を経由して電子署名した文書により支払えるようになる。このような動きのなかで『PKIによる電子署名』は文書の受け手が署名された文書が改ざんされておらず署名した本人のものであること（本人性）を電子的に完全に保証する唯一の手段であり電子商取引き、電子申請を行う上で非常に重要な位置を占めている。

企業印（秘密鍵）共有の要件

現在、図１は政府認証基盤（GPKI）であり、法務省商業登記認証局が企業に対して電子認証（公開鍵暗号方式でいう秘密鍵）を発行して企業間/政府間の相互認証基盤を構築しようとしている。また、国土交通省の電子入札のためには帝国データバンクが電子認証を発行している。法務省商業登記認証局や帝国データバンクの電子認証は、企業を代表する電子認証で契約書への署名や電子入札等において企業を代表して使われる電子認証であり、まさしく電子の企業印＝電子企業印と呼ぶべきものである。

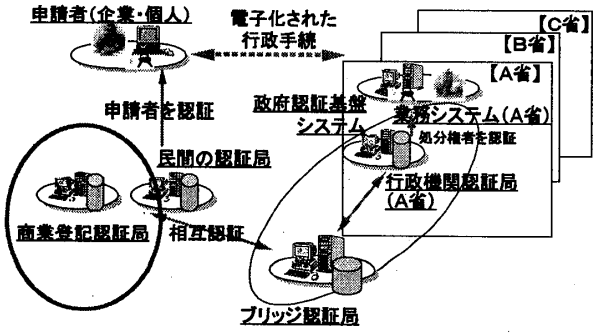

図1. 政府認証基盤と商業登記認証局

この電子企業印の使用にあたっては企業内で安全かつ便利な形で共有される必要がある。つまり、

－ 盗まれたことがすぐにわかる（コピーの場合は物理的には残っているのでわかりにくい）

－ 誰が使用したかわかる

－ 便利に使える

といった要件が必要となってくる。

既存の方法とその問題点

現在、電子企業印を作成するための秘密鍵の保管/使用する手段としては、PKCS12 形式、Java KeyStore 形式のファイルで保管する、IC カードやタンパ装置と呼ばれる鍵を閉じ込めるためハードウェアにいれて保管する方法が一般的である。しかしながら秘密鍵は元来共有すべきものではないので、鍵の共有を考えた場合、次のような問題点がある。

ファイル

１．ファイルコピーによる共有

- 不正コピーを制限できない
- 不正使用を検出できない

ハードウェア

２．タンパ装置、セキュリティ・チップ

- 不正コピーはできないが、逆にコピーできないため、デバイス自体の共有が必要
- タンパ装置を装着した単一のマシンに企業印を使用する複数アプリケーションを導入が必要。

３．IC カードの共用

- 不正使用を検出できない
- 利便性が悪い

企業印共有の概念図

上述の問題点を解決するために企業印を共有できる電子署名サーバーを考案した。これにより、

- 鍵使用権限のある要求者のみ署名作成可能
- 使用履歴の記録による監査性の確保

を実現できる。

図 2 に、電子署名サーバーが企業印を共有する様子を示す。図の矢印 1-6 はそれぞれの動作を示す。

１．商業登記認証局から証明書を取得し、署名サーバーへインストールする

２．申請者 A は電子申請のための Web ページへアクセスし申請書に入力する

３．申請プログラムは申請者 A 鍵＋証明書を使って SSL 相互認証で認証サーバーへ

４．認証サーバーで識別と認証に成功したら署名サーバーへ

5．署名サーバーは電子署名を作成して申請プログラムへ
6．申請プログラムは電子署名付きの申請書を業務システムへ送信する

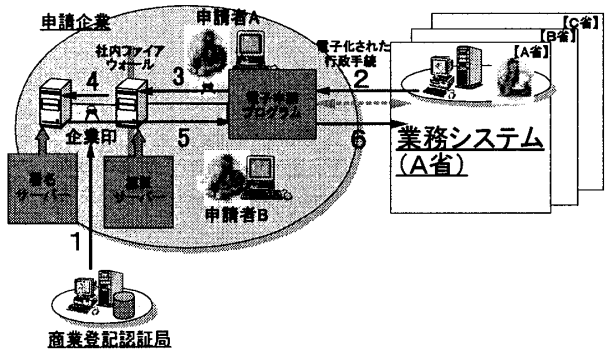

図2. 署名サーバーによる企業印共有の概念図

実装方式

署名サーバーの実装においては、Java[2]や Windows[3]の各プラットフォームで規定されている暗号サービスプロバイダ(CSP: Cryptographic Service Provider)としてクライアント側を実装した。既存のアプリケーションの多くはプラットフォームごとの CSP を介して暗号サービスを利用するように実装されている。図 3 のように、標準的に提供されている秘密鍵をファイルとして扱う CSP のほかに、IC カード用の CSP では署名対象データを IC カードに送って署名値を計算するようになっている。

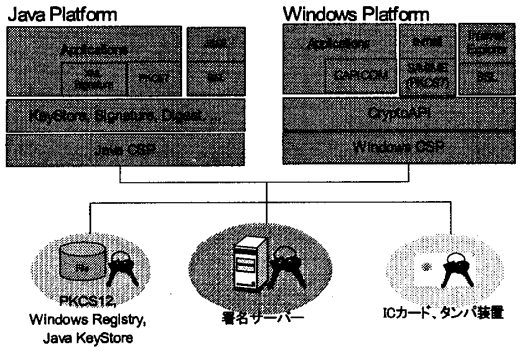

図3. Java、Windowsの暗号サービスプロバイダ

図 4 に示す通り、クライアントとサーバー間は HTTP, HTTPS などを使ってデータをやり取りする。クライアントは署名対象となるデータを、ネットワークを介してサーバーへ送り込む。サーバーは受け取ったデータを単純なビット列とみなして署名値を計算し、クライアントへ返す。

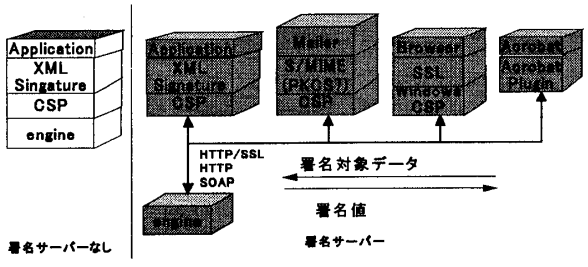

図4. CSPと暗号エンジン間で分けた実装

署名値を受け取ったクライアントは上位のレイヤで規定される署名形式としてデータを組み上げる。秘密鍵は署名サーバーに閉じ込められており、鍵自体が送受信されることはない。

また、今回の実装では署名サーバーへのアクセスを制限する認証サービスとして Policy Director を使っている。これは開発期間の短縮という目的以外に、Policy Director 関連製品群を組み合わせることで柔軟なユーザー認証を提供できるからである。電子企業印へのアクセス制御を行うためには、アクセス要求者の識別だけでなく、時刻や要求を行う場所なども考慮に入れる場合が想定される。

効果

CSP としてクライアントを実装し、暗号エンジンをサーバー側に置くことにより、

- 署名サーバー用 CSP をプラグインするだけで、既存アプリケーションの枠組みで適用可能となった
- 任意のデータ (XML, PKCS7, S/MIME, SSL など)に適用可能であり可能性がひろがった
- **Acrobat Plugin** を開発することで **Acrobat** も対応可能である。

アクセス制御を Policy Director に任せることにより、

- Policy Director 提供の認証方式に適用可能で、
- 関連製品群の一つである Privacy Manager による動的なユーザー権限の変更が可能

である

サーバー側で鍵使用履歴を保存することにより、

- 不正使用の防止、
- 監査性

を達成できた。

まとめ

本署名サーバーにより、安全な形で電子企業印の共有の仕組みは実現でき、人のみならずアプリケーションとも電子署名の共有ができるようになった。これにより、電子政府プロジェクトへの参画を通して電子企業印の共有の仕組みのないことによる利便性の悪さが解決できた。この署名サーバーにより **2003** 年からの政府電子調達の本格的な運用に伴った企業内での電子認証の共有の必要性の高まりに対して対応できるようになった。

また、いままでは **XML** 署名プロキシという形で企業署名付き **XML** メッセージ作成を行う方式の提案はあったが、本稿で述べた署名サーバーは **CSP** を介して企業印を共有することを目的としており、共有という観点において初めての実装であると考える。

謝辞

日本アイ・ビー・エム株式会社 ソフトウェア開発研究所の本署名サーバーを開発テーマとして推薦、選定していただいた方々、開発を支援していただいた方々に心より感謝します。

参考文献

[1] 総務省行政管理局 政府認証基盤 http://www.gpki.go.jp/
[2] "Java(TM) Security", http://java.sun.com/security/, Sun Microsystems, Inc.
[3] "Microsoft Platform SDK: Cryptographic Service Providers", http://msdn.microsoft.com/library/en-us/security/Security/cryptographic_service_providers_start_page.asp, Microsoft Corporation.