M_037

携帯電話を利用した電子印鑑システムの作成実験

An experiment on a digital stamp using a mobile phone

星 耕平† 野口 健一郎‡
Kohei Hoshi Kenichiro Noguchi

1．まえがき

現在、多くの電子文書がやり取りされるにつれ、セキュリティの向上が必要になってきている。そのための技術の一つであるデジタル署名の信頼性を高めるためには、署名のための個人鍵の管理性の向上が重要である。そこで、携帯電話に個人鍵を格納し、携帯電話を電子印鑑として機能させるシステムを作成する事で、デジタル署名の安全性の向上を試みた。PC に格納された被署名文書に対して、PC から携帯電話に署名用のダイジェスト値などを送信し、署名計算を実行させる。結果の署名値は PC へ返信される。

なお、署名規格として XML 署名規格[1]を利用した。また、PC と携帯電話間の通信には赤外線通信を用いた。

2. システムの概要

PC で電子文書を読み込み、ダイジェスト値などを生成し、携帯電話へ送信する。携帯電話で、受信したダイジェスト値に対して携帯電話に格納された個人鍵を用いて署名計算を行う。計算結果の署名値と公開鍵を携帯電話から PC に送信し、PC で署名文書を作成する。(図 2 を参照)

3. 研究課題

(1) 携帯電話(電子印鑑)と PC との処理分担
(2) 携帯電話上での署名計算の実装
(3) 安全性の確保

4. 携帯電話(電子印鑑)と PC との処理分担

4.1 全体の流れ

処理の全体的な流れを図 2 に示した。

①XML 文書を PC で読み込み、XML 署名規格に従い、ダイジェスト値と確認データの生成まで行う。
②そのダイジェスト値と確認データを赤外線で携帯電話へ送信する。
③携帯電話上に確認データを表示し、署名者が署名する文書を確認し、携帯電話内に格納された個人鍵を用いて署名計算を行う。
④ 赤外線で署名値と公開鍵を PC へ送り返す。
⑤PC は受け取った 2 つのデータを元に、署名処理を完了させる。

なお、署名アルゴリズムには RSAwithSHA1 を用いた。

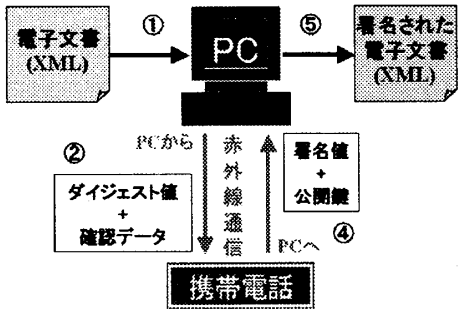

図 2 システム全体の流れ

4.2 PC 上での処理

携帯電話での処理前後で、PC の処理が分かれる。

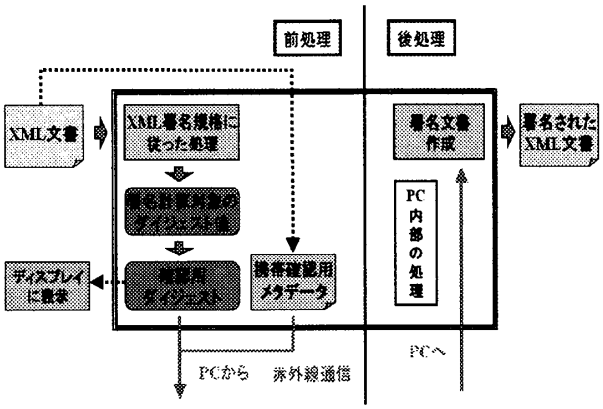

図 3 PC 上での処理

（1）前処理 （図 3 左側）
①入力した XML 文書からメタデータを読み込む。
②入力した XML 文書全体から、XML 署名規格に従って、ダイジェスト値の生成まで行う。
③そのダイジェスト値から、確認用ダイジェストを生成して表示する。
④「ダイジェスト値」、「メタデータ」、「確認用ダイジェスト」の 3 つを赤外線で携帯電話に送信する。

（2）後処理 （図 3 右側）
⑤携帯電話から受信した公開鍵と署名値を元に、署名文書の作成を完了し、出力する。

4.3 携帯電話上での処理

携帯電話上での処理を図 4 に示す。

† 神奈川大学理学部情報科学科（現在 東横システム株式会社）
‡ 神奈川大学理学部情報科学科

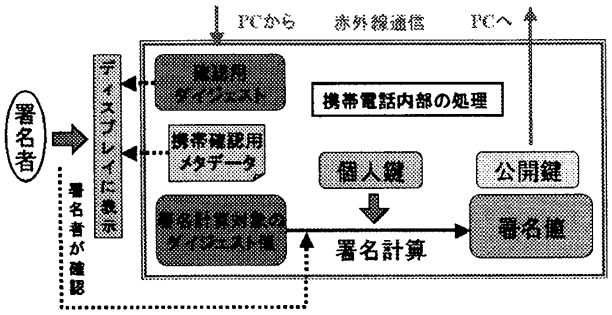

図4　携帯電話上での処理

①PC から受信した確認用ダイジェストとメタデータを表示し、署名者が文書を確認する。
②受信したダイジェスト値で署名計算をする。
③署名値と公開鍵を PC へ送信する。

5. 携帯電話上での署名計算の実装

携帯電話向けの Java 実行環境である J2ME の CLDC (Connected Limited Device Configuration)では、巨大な整数を扱うクラスが提供されていない。そこで、巨大な整数を扱うクラスはすでに当研究室で開発済みのものを利用した。署名計算に必要な「べき乗の剰余(modPow)」の高速化も行っている。

6. 安全性の確保

6.1 メタデータ

署名する XML 文書の内容を確認する為、入力する XML 文書にメタデータ格納用の要素を作り、その内容を携帯電話のディスプレイに表示して、確認出来るようにした。XML 文書の概要を図 5 に示す。

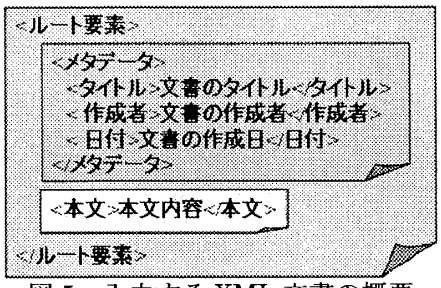

図5　入力する XML 文書の概要

7.2 確認用ダイジェスト

署名者が、「自分が署名しようとしている文書が正しいものかどうか」を確認する為に、確認用ダイジェストを生成して、確認できるようにした。
①署名対象となるダイジェスト値(160bit)から MD5 で 128bit のダイジェスト値を生成する。
②それを BASE64 で符号化し、確認用ダイジェストを生成する。
③これを PC のディスプレイに表示する。
④更に、PC から携帯電話に送信し、携帯電話のディスプレイにも表示する。
⑤署名者はこの両方を見比べて、署名する文書が正しいかを確認し、署名する。

①②の変換（図 6 に示す）で、10 進数で 50 桁程度あったダイジェストを 24 文字程度まで減らす事が出来た。

図6　確認ダイジェストへの変換

7. 評価

7.1 性能

携帯電話での署名計算の実行結果を表 2 に示す。

表2　実行結果

測定環境：NEC 製　FOMA N901iS

署名計算時間	約 2 分
RSA の個人鍵	50 桁(10 進数)

今回使用した個人鍵の長さは、160bit のダイジェスト値を署名計算するのに必要最低限の値を使用しているが、安全性を考慮すればより大きい値を使用する必要がある。更に、現在の構成でさえ署名計算に 2 分を要しており、アルゴリズムの高速化とハードウェアの性能向上が望まれる。

7.2 安全性

今回は、文書の確認用にメタデータと確認用ダイジェストを利用したが、確認用ダイジェストは PC 上で生成したものを携帯電話へ送信している。しかし、より安全な方法としては、ダイジェスト値のみを携帯電話に送信し、携帯電話上で表示する確認用ダイジェストの生成は、携帯電話上ですべきだと思われる。

8. 今後の課題

(1)DSA 暗号の実装
(2)携帯電話上での確認用ダイジェストの生成

謝辞

PC での赤外線通信機能の実装に、さかきけい氏作成の「OBEX ライブラリ」[4]を利用させて頂きました。

参考文献

[1] World Wide Web Consortium: XML-Signature Syntax and Processing, W3C Recommendation, 12 February 2002.
(http://www.w3.org/TR/xmldsig-core/)
[2] 丸山宏：XML と Web サービスのセキュリティ —XML デジタル署名と暗号化、共立出版、2004 年.
[3] 神戸博之・高坂一城：J2ME プログラミングガイド—505i (DoJa - 3.0)対応版、IDG ジャパン、2003 年.
[4] さかきけい：Java と Windows で赤外線 OBEX 通信をする試み、KEI SAKAKI's PAGE：
http://godwood.allnet.ne.jp/vioret/j2seobex.html