2004－ＤＰＳ－117　(4)
2004－CSEC－　24　(4)
2004／3／4

サーバ型電子署名システムの提案

小栗　伸幸[†]　塚田　千佳子[†]　関野　公彦[†]
[†]（株）NTT ドコモ　〒239-8536　神奈川県横須賀市光の丘 3-5

あらまし　公的個人認証サービスの開始によって，電子署名の普及が見込まれる．また，SSL 機能の搭載など，携帯電話における PKI 技術の適用が注目される．本稿では，携帯電話における機能制約を考慮した上で，携帯電話の SSL 機能を有効活用し，サーバと連携することによって電子署名を生成するサーバ型電子署名システムを提案する．

Server-aided digital signature system

Nobuyuki Oguri[†], Chikako Tukada[†], Kimihiko Sekino[†]
[†]NTT DoCoMo, Inc.　3-5, Hikarinooka, Yokosuka, Kanagawa, 239-8536 Japan

Abstracts　With the introduction of JPKI service, growth of digital signature is expected. Also, with the availability of mobile phones with SSL functionality, focus will be on PKI technology. In this paper, with the limitation of functionality of mobile phones, we propose server-aided digital signature system that generate digital signature by using SSL function of a mobile phone, and cooperative server.

１　はじめに

電子署名法の施行[1]，公的個人認証サービスの開始[2]に伴い，電子署名を用いて電子申請が可能となった．今後，行政を中心とした PKI の普及に伴い，一般にも PKI が浸透し，電子申請および電子契約等においても，電子署名が用いられることが見込まれる．

一方，携帯電話において SSL 機能が実装されるなど，PKI 技術の適用が注目される．今後，携帯電話における PKI 技術も，PKI の一般への普及およびモバイルECの発展により，電子署名等へ拡がることが期待される．

以下，本稿では，電子署名生成に関して，携帯電話の機能制限という課題を考慮した，サーバ型電子署名システムを提案する．

２　本研究の目的と前提

２－１　目的

電子申請において利用される電子署名の形式としては，XML 署名[3]が一般的である．XML 署名は，W3C および IETF において標準化された，署名対象，署名アルゴリズム，

署名値および証明書などを XML 形式で表現する電子署名形式である．今後，電子申請での利用を契機に，他サービスへの拡がりが見込める電子署名形式と考えられる．従って，本稿では，次節で述べる前提を考慮しつつ，携帯電話を用いて XML 署名を生成可能とするシステムを提案する．

２－２　本検討における前提

携帯電話は，小型軽量化および低消費電力が求められるため，処理機能に制限がある．また，携帯電話において SSL 機能が実装され始めていることを考慮し，以下に前提を置く．

前提１

携帯電話においては cHTML 形式，HDML 形式等の文書を処理できるが，汎用的な XML 形式の文書を処理できない．

前提２

携帯電話において SSL クライアント認証機能を搭載しており，鍵管理および署名値生成が可能である．

３　関連技術

前記前提に基づくと，携帯電話単独での XML 署名生成は行えない．そのため，サーバが補助することによって電子署名を生成するシステム（サーバ型電子署名システム）が必要になる．従来のサーバ型電子署名システムとして，サーバにおいて鍵・証明書管理を行い，ユーザに代行して電子署名を生成する Server-Supported Signature[4]があげられる．このモデルでは，ユーザからの依頼に基づきサーバで管理する鍵 SK_S を用いて電子署名を生成する．従って，ユーザの電子署名とするには，サーバが生成する電子署名とユーザの紐付けが課題となる．このため，通常の署名対象 M に加え，ユーザ識別子 ID とユーザが管理するハッシュ鎖を用いて生成するランダム値 h_i を署名対象として，電子署名 $SIG_{SK_S}(M, ID, h_i)$ を生成する．さらに，サーバによる ID および h_i の不正利用等による電子署名の偽造を防ぐために，サーバが生成した電子署名をユーザが検証し，正当ならば，ユーザが管理するハッシュ鎖を用いて，$hash(h_{i-1}) = h_i$ を満たすランダム値 h_{i-1} を生成・付与することで，$SIG_{SK_S}(M, ID, h_i), h_{i-1}$ とし，ユーザの電子署名とする方法が提案されている（図１）．

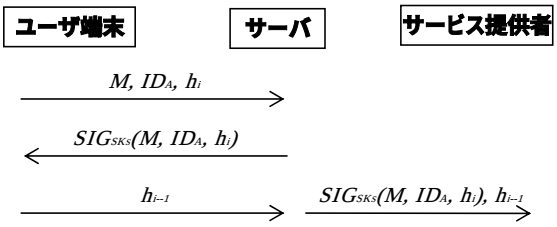

図1. Server-Supported Signarute**のフロー概要**

一方，SecureWare[5]において，XML 分離署名として，サーバ側で署名対象の生成，ハッシュ値の生成を行い，ユーザ端末において署名値生成を行うことで，電子署名を生成する方法が提案されている．

４　提案モデル

４－１　設計思想

SecureWare において提案されている XML 分離署名を基本概念として，携帯電話に適用するモデルを提案することとする．

2 章で述べた前提１を考慮して，携帯電話おいて処理できない汎用的な XML 形式の文書を，処理できる cHTML 形式に変換して携帯電話に提供することとする．このために，携帯電話の機能を補助する文書変換サーバを

設けることによって，サービス提供者から得たXML形式の文書を，cHTML形式の文書に変換した後，携帯電話に提供することを可能にする．これによって，汎用的なXML形式の文書処理ができない携帯電話であっても，記載内容の確認が可能となる．

また，前提２を考慮して，SSLクライアント認証機能を有効活用し，携帯電話において，鍵管理および署名値生成を行うこととする．これによって，サーバに署名鍵を預ける必要がなくなり，携帯電話において，ユーザが管理する署名鍵によって署名値の生成が可能となる．

４－２　モデル概要

提案モデルにおいては，携帯電話および文書変換サーバが連携することによって，XML署名を生成する．以下，XML署名生成のフロー（図２）を，文書変換サーバの処理に基づき３つのステップに分けて解説する．

ステップ１　テンプレート取得・提供

１．携帯電話から文書変換サーバを経由して，サービス提供者にテンプレートを要求する．

２．　サービス提供者は，XMLテンプレートを，文書変換サーバに送信する．

３．　文書変換サーバは，事前にサービス提供者と共有しているXSLファイルと，サービス提供者から得たXMLテ

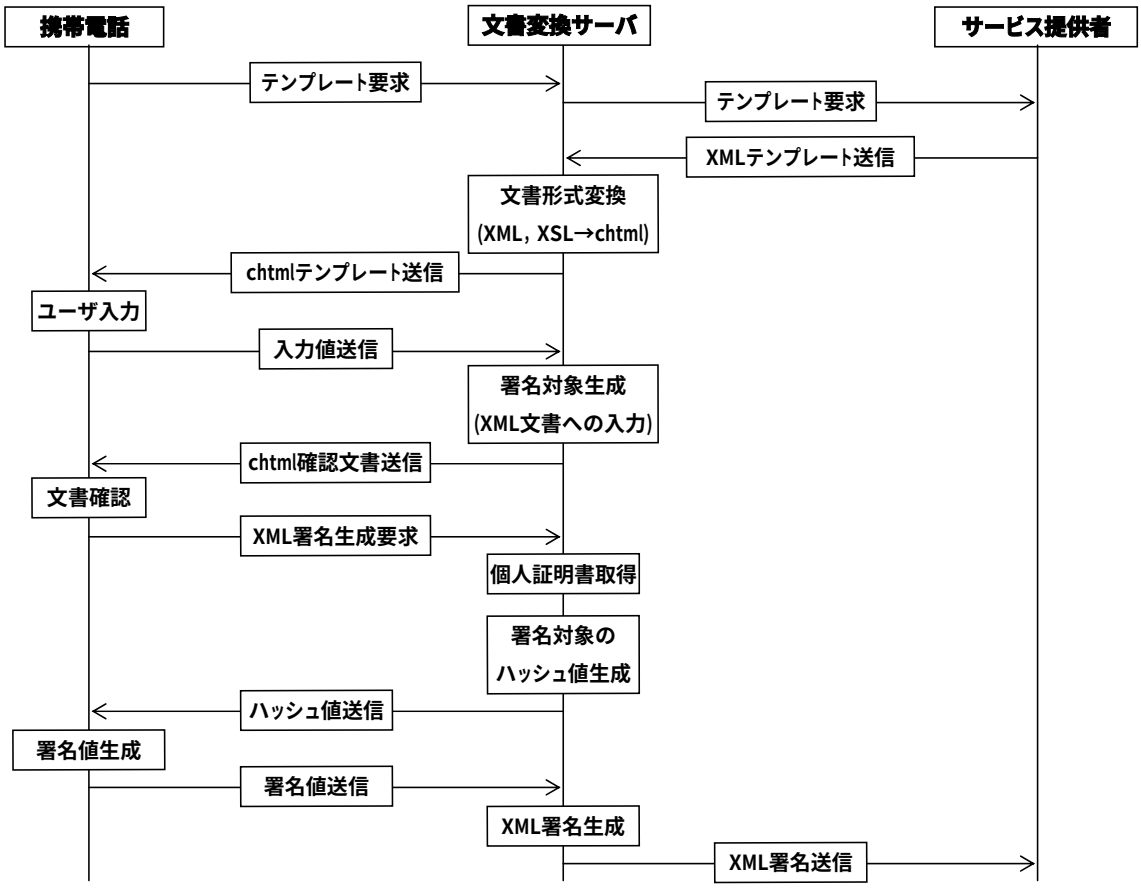

図2．XML署名生成フローの例

ンプレートから，cHTML テンプレートを生成し，携帯電話に送信する．

ステップ２ 署名対象生成

４．文書変換サーバから得た cHTML テンプレートに，ユーザは名前等の情報を入力することで，携帯電話から文書変換サーバに，入力値を送信する．

５．文書変換サーバは, XML テンプレートの所定箇所に，携帯電話から得た入力値を入力し，電子署名の対象文書（署名対象）を生成する．

６．文書変換サーバは，署名対象を３における処理と同様に形式変換し，携帯電話に対して cHTML 確認文書として送信する．

ステップ３ XML 署名生成

７．ユーザは携帯電話が受信した cHTML 確認文書を確認後，文書変換サーバに対して，XML 署名生成要求を行う．

８．文書変換サーバは, XML 署名生成要求を行ったユーザの個人証明書を取得する．また, XML 署名要求された署名対象のハッシュ値を生成し，携帯電話に送信する．

９．携帯電話は, ユーザの PIN 入力等により，管理する署名鍵および受信したハッシュ値を用いて，署名値を生成し，文書変換サーバに送信する．

１０．文書変換サーバは，７において生成した署名対象，１０において取得した証明書，１１において生成したハッシュ値，１２において受信した署名値を用いて，XML 署名を生成し，サービス提供者に送信する．

５　提案モデルの考察

５－１　電子署名の要件

電子署名には次の 2 つの要件が求められる．

（１）本人性

署名者の本人性を確認できる情報であること．

（２）完全性

署名対象が改変されていないことを確認できる情報であること．

本稿において，本人と鍵の結びつきを保証できることで，本人性を満たしていることとし，また，サーバにおける文書の入れ替えも署名対象の改変とする．

５－２　要件の充足性

電子署名の要件に対する充足性を，3 章で述べた従来モデルおよび提案モデルにおいて考察する．

本人性

従来モデルは，通常の署名対象に加え，ユーザの ID とユーザが管理するハッシュ鎖を用いたランダム値を署名対象とすることで，ユーザと電子署名の紐付けを行い，ユーザの本人性を保証できるモデルとなっている．従って，特殊なロジックを埋め込んだ署名形式となり，検証者は通常の電子署名の検証に加え，ハッシュ鎖によるランダム値の検証が必要となる．また, CA によるサーバに対する公開鍵証明書発行に加え，ユーザに対するハッシュ鎖証明書発行も必要となる．

一方，提案モデルは，ユーザ自身が管理する携帯電話において，鍵管理を行うため，ユーザの意思に基づく署名値生成が実現され，これにより一般的な署名形式によって，署名

者の本人性を保証できるモデルとなっている．従って，検証者は通常の電子署名検証のみで検証可能であり，CA による証明書発行は，ユーザに対する公開鍵証明書発行で良い．

完全性

従来モデルは，ユーザ端末において署名対象を処理できる前提で検討されている．そのため，サーバが生成した電子署名を，ユーザ端末において確認後，サービス提供者に送信するモデルとなっている．これによって，サーバによる文書の改変を防ぐことが可能となっている．

提案モデルは，ユーザ端末を携帯電話に限定しており，携帯電話において署名対象となる文書形式を処理できない前提としている．このため，ユーザ端末単体で行われる XML 署名生成（図 3）と異なり，サーバにおいて XML 署名対象を形式変換した cHTML 文書，XML 署名対象から生成したハッシュ値が，ユーザ端末である携帯電話に提供される（図４）．従って，サーバが提供する cHTML 文書およびハッシュ値の正当性を保証することが課題となる．

また，従来モデルも，ユーザ端末を携帯電話とした場合，提案モデルと同様に署名対象をユーザ端末において直接処理することができないと考えられ，サーバによる形式変換が必要になると考えられる．従って，サーバが提供する文書の正当性を保証することが課題になると考えられる．

上記に述べたように，提案モデルは，従来モデルに比べて，本人性の保証を容易に実現可能とした．また，提案モデルにおいても，従来モデルにおいても完全性を保証する方式の検討が必要となる（表１）．

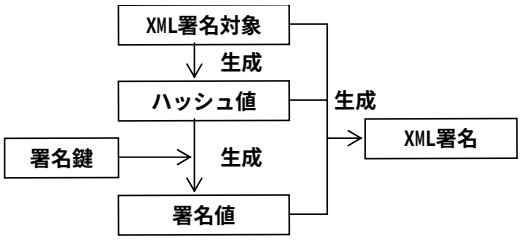

図3．ユーザ端末単体の場合

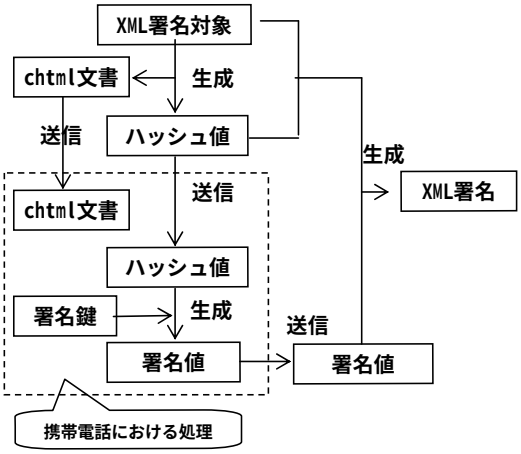

図4．提案モデルの場合

表１．モデル比較

	本人性	完全性
従来モデル	△*1	—*2
提案モデル	○	△*3

*1)特殊なロジックを埋め込む必要がある．

*2)ユーザ端末で文書処理が可能であることを前提に検討されている．ユーザ端末を携帯電話にした場合，提案モデルと同様の課題が生じると考えられる．

*3)文書変換サーバより携帯電話に提供される chtml 文書，ハッシュ値の正当性を保証する必要がある．

６　まとめ

携帯電話の機能を補助する文書変換サーバを設けることにより，携帯電話において文書確認を行い，携帯電話を用いて電子署名の生成を行うサーバ型電子署名システムを提案し

た．これによって，電子申請等において適用される XML 署名を，携帯電話において cHTML 文書等によりユーザの意思確認をした上で，汎用的な XML 形式の文書を処理できない携帯電話を用いて生成可能となった．提案システムにおいて課題となる完全性に関しては, [6]において検討する. また, 今後は, プロトタイプシステムを構築し，定量的な評価を行う予定である．

参考文献

[1] “電子署名及び認証業務に関する法律”, http://www.meti.go.jp/policy/netsecurity/digitalsign-law.htm

[2] “公的個人認証サービス”, http://www.jpki.go.jp/

[3] D. Eastlake, J. Reagle, and D.Solo, “XML-Signature Syntax and Processing”, RFC3075, March 2001.

[4] N. Asokan, G. Tsudik, and M.Waidner, “Server - Supported Signatures”, *Journal of Computer Security,* vol.5, no.1, 1997.

[5] 日本電気株式会社, “SecureWare”, http://www.sw.nec.co.jp/middle/SecureWare/

[6] 塚田，小栗，関野, “サーバ型電子署名システムにおける真正性保証方式”，第 24 回コンピュータセキュリティ研究会, 2004 年 3 月.