社団法人 情報処理学会　研究報告
IPSJ SIG Technical Report

2004－ＤＰＳ－117　(5)
2004－CSEC－　24　(5)
2004／3／4

電子署名システムにおける真正性保証方式

塚田　千佳子†，　関野　公彦†，　小栗　伸幸†

†（株）NTT ドコモ　〒239-8536　神奈川県横須賀市光の丘 3-5

近年の e コマースの普及に伴い,セキュリティ確保の為,電子署名が普及し始めている.しかしながら,既存の電子署名技術は,携帯電話端末など機能的に制限があるものでは利用が難しい.ここでいう機能的な制限とは，携帯電話の機能が,今後普及の見込める XML 署名の汎用的な環境をサポートしていない,という事である.この問題を解決するためにサーバ型電子署名方式が提案された.これは，文書変換サーバによって XML 文書を携帯電話に適したフォーマットへ変換し,署名付与を代行するものである.この方式で新たに課題となるのが，元の文書と，文書変換サーバによって変換され携帯電話に提供される文書が同じ内容であること，またハッシュ値が元となる XML 文書から正しく生成できているか，についての保証である.本稿では,このような場合の脅威分析・必要条件抽出を行った後,第三者機関に変換前後の文書を委託し,文書の真正性を保証するモデルの提案をする.

Genuineness Guarantee Method at Server-aided Digital Signature System

Chikako Tsukada†, Kimihiko Sekino†, Nobuyuki Oguri†

†NTT DoCoMo, Inc.　3-5, Hikarinooka, Yokosuka, Kanagawa, 239-8536 Japan

With the growth of e-commerce, to insure security, use of digital signature is becoming popular. Still, there are some difficulties in using digital signature on small terminals such as mobile phones because XML which is common form of digital signature is not supported on these terminals. For this reason, server-aided digital signature system which transforms XML into HTML, which can be used by mobile phones, was proposed. In this paper, we discuss threats for the system, and then propose a guarantee method to overcome these threats.

1 はじめに

現在,オンラインショッピングや電子申請等,電子文書のやり取りにより契約を締結する電子商取引が普及しつつある.ここで,電子文書のセキュリティを確保する技術として,電子署名があげられる.そのうちのひとつである XML 署名を行うには,XML 文書が扱えることが必須であるが, 現状,携帯電話端末では XML 文書を扱うことができないのが一般的である.このような携帯電話端末での XML 文書の扱いや電子署名に対する機能制限を補完するために提案されたのがサーバ型電子署名方式である [1].サーバ型電子署名方式は,XML 文書をサポートしていない携帯電話端末用に,文書変換を施し,cHTML 文書等に変換する事によって,機能制限のある携帯電話端末での文書表示を可能とする技術である. ここで文書の形式変換を行った際,問題となるのが変換前後の文書の対応及び電子署名の対象文書とハッシュ値の対応である.このような文書変換機能を有しているシステムで,電子署名に対する脆弱性が懸念される.本稿では,この問題点に着目し,セキュリティ脅威となる項目についての分析を行った後,真正性を保証する対策の提案を行う.

2 サーバ型電子署名システムの概要

2－1 概要

[1]で提案されているサーバ型電子署名システムは,XML 環境をサポートしない電子署名端末（携帯電話端末等）の機能制限を文書変換サーバが補うことにより, XML 署名等の電子署名生成を実現するものである.このシステムにおいて,文書変換サーバは,次の文書処理を行う.

・文書変換：署名要求元から発行された XML 文書およびその XML 文書にユーザ入力値を加えた XML 文書を電子署名端末対応形式（cHTML 等）に変換し,電子署名端末に提供する.
・ハッシュ値作成：XML 文書にユーザ入力値を加えた文書のハッシュ値を作成し,電子署名端末に提供する.

また, 電子署名端末は次の文書処理を行う.

・署名値作成：文書変換サーバから提供されたハッシュ値に,管理している鍵を用いて署名演算し, 文書変換サーバに提供する.

本稿において, 上記サーバ型電子署名システムを対象として,真正性保証について検討する.

2－2 問題点

一般的な署名者･検証者からなる二者間の電子署名システムにおいて,電子署名が保証するのは,署名対象文書の完全性,署名者の本人性の確認である. つまり,文書真正性を保証するには, 本人性, 完全性がいかに保証されるかを検討する必要がある.ここで本稿の対象となるサーバ型電子署名システムでの署名対象文書の真正性を保証するには「形式変換が正しく対応付けられて改変されることなく変換されているか」「電子署名の対象文書とハッシュ値が正しく対応付けられて改変されることなく作成されているか」を保証する事が必要である.

3 脅威分析と課題

２－２で述べたように,サーバ型電子署名システムでは,文書変換サーバを加えた三者のモデルになることより,完全性の保証が課題として考えられる. 従って, 文書変換サーバの信頼レベルに基づき, トラストモデルを分類し, 各モデルにおいて,完全性およびユーザの事後否認に関して, 脅威を分析する. トラストモデルは以下の三点とする.

Ⅰ　サーバが信頼できる場合

この場合，文書変換サーバは,あらゆる文書変換において trust であり,誤りはない.

Ⅱ　サーバが改ざんを行うが正直な場合

この場合,文書変換サーバはエラーを起こすが,エラーを申告する悪意のない正直なモデルである.

Ⅲ　文書変換に改ざんの悪意がある場合

この場合,文書変換サーバが悪意を持って文書変換を行う.

なお,全ての場合において,携帯電話端末の特性から,ユーザによる改ざんは困難であると仮定し,ユーザは以下の否認行為を行うものとする.

①　署名した行為を否認

ユーザが,自分の管理している秘密鍵によって署名値を生成していないと主張すること.

②　署名した文書を否認

ユーザが,署名値を提供した文書でないと主張すること.すなわち，サーバによって文書が改ざんされたとのクレームを起こすこと.ここでの改ざんは以下を含む.

・署名対象文書とハッシュ値の対応が取れていない.
・署名対象文書と署名端末での確認画面の対応が取れていない.

Ⅰ　サーバが信頼できる場合

ここで考えられる脅威は,ユーザの事後否認のみである.

①署名した行為を否認

署名値の作成が出来るのは秘密鍵をユーザが保持し,かつ PIN の入力など本人の意思が介在する場合のみである.よって否認できないという事が言える.

②署名した文書を否認

サーバにおける文書の改ざんはあり得ないモデルであるため,ユーザには，常に正当な文書が提供されることとなる.従って，否認の防止は可能である.

以上よりこのモデルではユーザによる否認防止が可能であり，課題となるのは,脅威を防ぐことではなく，どのようにサーバに完全な trust を与えるのかということである.

Ⅱ　サーバが改ざんを行うが正直な場合

サーバがエラー処理等の改ざん行為を行った場合，サーバが正直に申告するため，エラーによる改ざんについては検知できる.ユーザの事後否認については，次のように考えられる.

①署名した行為を否認

Ⅰの場合と同様に否認できない.

②署名した文書を否認

サーバにおける文書の改ざん（エラー処理等）が生じた場合，サーバが honest に申告するためモデルであるため,サーバ責として否認される.また，サーバが正常な状態でのユーザ否認についてはサーバの honest より保証できる.

以上の事をまとめると,ユーザの署名した行為否認については保証できるが,変換時の文書改ざんによる署名文書の否認に対しては課題が生じる.サーバにエラーが生じた場合，サーバ責となる健全なモデルと考えられるが,言い換えれば,ユーザの否認が成立するモデルとなっていることになる.一方，サーバにエラーが生じなかった場合，サーバの honest が第三者によって証明されていなければならない.第三者に証明されない場合,サーバにエラーが生じなかったにも関わらず,ユーザがサーバのエラーを主張することで，サーバ責，ユーザ責が不明確になる.従って，次の「文書変換サーバに改ざんの悪意がある場合の脅威」と同じレベル

で検討しなくてはならない.

Ⅲ文書変換サーバに改ざんの悪意がある場合

サーバの改ざんについてはあらゆる文書変換においての改ざんが疑われる.ユーザの事後否認に関しては次のように考えられる.

① 署名した行為を否認

Ⅰの場合と同様に否認できない.

② 署名した文書を否認

サーバにおいて改ざんの疑いがあるモデルの為,文書変換サーバから提供される文書の信頼性がない. よって, 文書変換サーバによって改ざん行われた場合のユーザ否認について, 文書変換サーバが改ざんを否定することで, サーバ責・ユーザ責が不明確となる. また, 改ざんが行われていない場合のユーザが否認について, 文書変換サーバによる改ざんの可能性を否定できないため, サーバ責・ユーザ責が不明確となる.

以上のことより,ユーザの署名した行為否認については保証できるが, サーバの悪意ある改ざんが生じることで, ユーザ否認において, ユーザ・サーバのどちらに責があるのか特定できない場合が出てくる.従って, どちらの責かを明確にするために, サーバの改ざんを検知する必要がある. サーバによる改ざんとして, 具体的には以下が考えられる.

署名要求元が送信した XML 文書が文書変換サーバにて悪意ある文書に置き換えられた上変換され, 悪意ある HTML 文書がユーザに送信される. または, 文書変換サーバで受信した XML 文書が置き換えられなかったとしても, 悪意ある文書変換によって署名要求元が意図しない HTML 文書に変換され, 間違った HTML 文書がユーザに送信される. さらに, 文書変換処理が正しく行われたとしても, 文書変換サーバ内にある他の HTML 文書と置き変えられてユーザに送信される.

よって,次章において, これら脅威を防ぐための必要な条件を分析した後,このような場合の保証の方法を提案し,対策案として示す.

4 完全性要件分析

前章より, 完全性保証の為には以下の脅威がある事が分かった.

1、署名対象文書等の改ざん

2、文書変換サーバの不当な文書処理

3、偽文書の送信

これら脅威を防ぐ為に以下の三点が必要となる.

表1, 脅威と保証の為の条件

脅威	脅威防衛の為の必要条件
署名対象文書等の改ざん	いつ誰が何を使ったのかの明確化
文書変換サーバの不当な文書処理	文書変換サーバにおける文書処理の保証
偽文書の送信	変換前後の文書の紐付け

①「いつ,どのエンティティが何を使ったかを明確にしているか」

署名対象文書等の改ざんのためには, どのエンティティがどのタイミングで何を行ったのかという保証すれば良い. そのために,「いつ」,「誰が」,「何を」送付したのかという証明が求められる. 実際,このような保証は従来の技術で証明できるものである.具体的には,タイムスタンプ,電子署名によって存在証明, 文書保管, 内容証明を実現出来る. これにより「いつ」「だれが」「何を」を証明する事ができる[2][3] .

②「文書変換サーバにおける文書処理は本当に正しいのか」

文書変換サーバの不当な文書処理を防ぐ為には, 文書変換サーバにおける文書処理の保証

を行う．署名対象文書は,文書変換サーバで文書処理を施され,クライアントの電子署名端末上に表示される.文書変換処理を施す事で,署名要求元が意図した通りの文書が端末上に提供されていないかもしれない.この文書処理機能を保証する仕組みが必要となる.

③「署名要求元が提供した文書と,電子署名端末に提供された文書の紐付けの正しいか」

偽文書を送信してない事を示すためには,変換前後の文書の紐付けの保証を行えば良い.サーバ型電子署名システムにおいては署名対象文書と変換後の文書が生成される為，これが必ず１：１に対応している必要がある.このような文書の紐付けについては,文書に署名を施す,文書に固有の ID を付ける,トランザクションに ID を付けるなどを行い,その ID に基づき,同一トランザクションで送受信された文書管理の解決法が考えられる.

以上の条件をまとめ,第三者機関による保証方式を提案する.

表 2，対策案

必要条件	対策案
①	TSA、原本保証、長期保存等の技術で対応可能
②	第三者機関による保証方式の提案
③	文書への署名・IDの付与で対応可能
以上の対策案をまとめ，第三者機関での保証方式を提案する	

5 システム提案

5－1 方針

前章で述べた要件のうち既存技術によって,文書単体の保証はできるが，文書を紐付けて,文書処理が正当に行われたことの保証まではできない．従って，既存技術では保証しきれない要件も満たす文書真正性の保証システムを提案する.ここでは,信頼できる第三者機関によって,変換前後の文書を保管する事によりどのプレイヤーにより，いつ，何が提出されたかを保証し,第三者機関から変換機能を文書変換サーバへ提供する事により,文書変換機能の保証を行い,さらに変換前後文書の対応を署名・ID 等を文書に付与することにより保証を行う機能を設けることとした.

5－2 概要説明

提案モデルでは,トランザクション毎に文書をくくり付け第三者機関に文書を保管する.又,文書変換サーバにおける変換機能は,第三者機関から保証・提供されたものを使用することにより,変換の保証を取るものとする.文書変換の正当性を保証する方法は次の通りである.

文書変換を行う際,署名要求元は署名対象である XML 文書を第三者機関に署名を付けて登録する.XML 文書を受信した文書変換サーバは,先ほどの XML 文書及び XSL ファイルを使用し cHTML 文書を作成し署名端末に送信する.ここで使用された XSL ファイルを文書変換サーバが第三者機関に登録する.cHTML 文書を受け取った署名端末は,その cHTML 文書を第三者機関に登録する.３つの文書を受け取った第三者機はそれらを紐付けて保管する.

検証を行う際は,保管されている XML，XSL，cHTML 文書のセットに対して,第三者機関にある変換機能を使用して再変換を施す.具体的には,取得した XML,XSL ファイルに対し文書変換を行った後,保管していた cHTML 文書と結果を突合する.突合結果が同じならば文書の変換の真正性は保証され,結果が違った場合は改ざんが検知される.

又，ハッシュ値生成の正当性の保証についても，電子署名端末からの入力値と署名要求文書 XML を用いることで，上記と同様の方法により保証する.

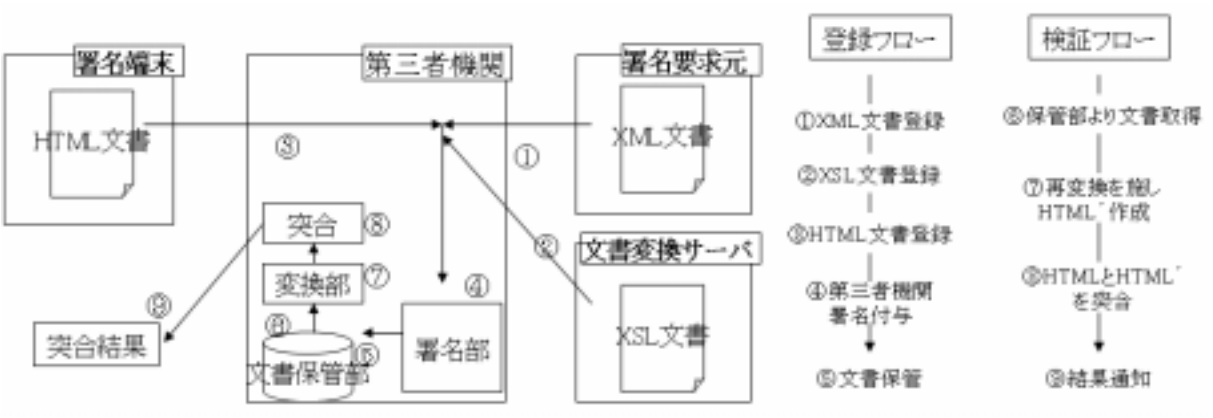

図１，処理フロー

6 まとめ

本稿ではサーバ型電子署名システムにおいて文書変換サーバの信頼度レベル毎に分類して,各レベルにおける脅威の分析を行い,対策案を提案した.具体的な対策として,信頼できる第三者機関を用いることで,サーバ型電子署名システムにおいて,真正性を保証する方式を提案した.

参考文献

[1] 小栗伸幸,関野公彦,塚田千佳子,“サーバ型電子署名システムの提案”,第 24 回コンピュータセキュリティ研究会,2004 年 3 月

[2]電子商取引推進協議会認証・公証ワーキンググループ,“電子署名文書中間保存に関する中間報告”,平成 13 年 3 月

[3]宮崎邦彦,吉浦裕,岩村充,松本勉,佐々木良一,“第三者機関への依存度に基づく長期利用向け電子署名技術評価手法の提案”,情報処理学会論文誌 ジャーナル Vol.44 No.08, 平成 15 年 6 月