M-066

電子文書の訂正・流通を考慮した部分完全性保証技術の提案

Proposal on Partial Integrity Assurance Technology that Considers Correction and Distribution for Electronic Documents

吉岡 孝司†　　武仲 正彦†
Takashi Yoshioka　Masahiko Takenaka

1. はじめに

近年、ＩＴの進展に伴い、電子文書保管時の課題を解決する原本性保証システムの開発が急速に進んでいる。しかしながら現状システムのほとんどは、確定された最終形態の文書を原本として安全に管理する、いわゆる原本の所在が明確である文書を対象としており、複数のエンティティ間を追加・訂正されながら転々流通していく文書の原本性確保については特に考慮されていない。本稿では、上記環境下における電子文書訂正に関する要件を明確にし、その解決策を示す。更に、解決策のひとつとして「部分完全性保証システム」とその手法について提案する。

2. 電子文書訂正の問題点

電子文書の訂正を従来の電子保存環境（原本性保証システム等）で実現する際の問題点を以下に示す。

問題1.　訂正箇所を特定できない、同時に、訂正箇所以外は改変がないことを確認できない
問題2.　訂正箇所はいつ、誰が訂正したのか確認できない
問題3.　訂正してもよい箇所かどうか確認できない
問題4.　一部の情報を隠した状態で第三者に提示する場合、秘匿箇所以外が不変であることを示すためには、前版の本文を提示する必要がある。つまり、秘匿内容を明示しなくてはならない
問題5.　複数枚に分かれた派生文書の同時性・関連性が確認できない

以上のような問題があるため、従来環境では訂正済み電子文書の完全性を保証することは困難であった。これらの問題解決のためには、従来紙が持っていた訂正事象に対する原本性の確保を第三者的に証明可能な形式で実現する必要がある。

3. 電子文書訂正の要件

電子文書訂正に求められる要件を、紙媒体の原本性から考察する。紙媒体は、以下の要件を満たしているために、原本性を保証していた。

- **部分特定性の保証**
  訂正箇所の特定とそれ以外の不変保証。例えば、訂正箇所の文字を二重線で抹消し、余白に訂正文字を記入していた。それ以外の不変は一目瞭然である。
- **部分本人性の保証**
  訂正者を特定保証。例えば、訂正文字の上に訂正者本人の訂正印を押印していた。ただし、訂正時期については、経年劣化（紙質・黄ばみ等）により予測できたが、正確な日時までは特定できなかった。
- **部分管理性の保証**
  訂正事象の正しさとその検証性保証。例えば、記載方法や訂正可能範囲・条件等は事前に規定されており、これらをもとに当該文書が正しく作成・訂正されているかを管理可能である。
- **部分秘匿性の保証**
  一部情報の秘匿とそれ以外の不変保証。例えば、申込書のような文書では、カーボン紙を用いることで秘匿内容を複写しないようにしていた。
- **部分同時性の保証**
  複数枚に分かれた派生文書の同時性・関連性保証。例えば、原紙から複写されたカーボン紙は作成者本人によって書かれたこと（本人による筆跡同一性の確保）を保証していた。

紙媒体では、訂正文書に対して以上のような５つの要件を満たすことで、原本性を保証していた。電子文書訂正を行うためには、これらの要件を解決する必要がある。

4. 要件の解決策

4.1　部分特定性の保証

訂正箇所の特定とそれ以外の不変を保証するために、文書中の一要素[1]単位（または、一文字単位）に毎回異なる任意情報を付加し、ハッシュ関数等の一方向性関数を用いてダイジェスト情報を生成する。更にそれらをまとめた情報に対して署名を付与し、「部分識別情報」として本文と一緒に原本保管装置に格納する。この部分識別情報は、訂正事象毎に原本同様版数管理を行い、前版との比較を行うことで部分訂正箇所を特定可能とする。「部分識別情報」を用いることで、問題１が解決される。

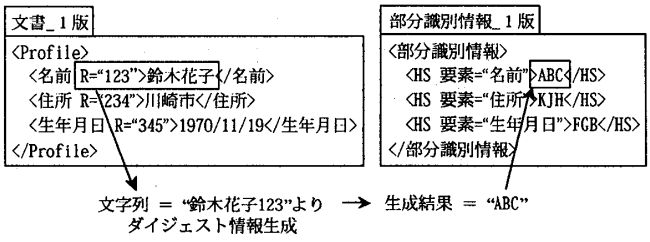

図１：部分特定性を考慮した部分識別情報の生成例

図１は部分特定性を考慮した部分識別情報の生成例である。「文書_１版」の各要素に含まれる属性“R”は、任意情報を表している。この任意情報の付加については後述する。

4.2　部分本人性の保証

訂正日、訂正者を特定するために、いつ、誰が、どの箇所に対して、どのような操作を行ったか、訂正理由等をまとめた情報を訂正事象毎に「部分訂正情報」として生成し、本文と一緒に原本保管装置に格納する。当該情報も部分識

†（株）富士通研究所

[1] この場合、例えば、ＸＭＬのような構造化文書を想定

別情報同様、訂正事象毎に版数管理を行う。同時に当該情報にはタイムスタンプ・訂正者の署名を施すことで、訂正日時・訂正者を特定することが可能となる。「部分訂正情報」を用いることで、問題２が解決される。

4.3 部分管理性の保証

部分訂正が正しく行われたことを作成前後で確認・検証できるよう文書毎に訂正者や訂正可能・不可範囲等の情報をまとめた「訂正ポリシ情報」を事前設定し、当該情報を用いることで、電子文書訂正に関する管理を可能とする。「訂正ポリシ情報」を用いることで、問題３が解決される。

4.4 部分秘匿性の保証

一部情報の秘匿とそれ以外の不変を保証するために、４.１節の方法で生成した「部分識別情報」を用いる。図２は部分秘匿性を考慮した部分識別情報の生成例である。

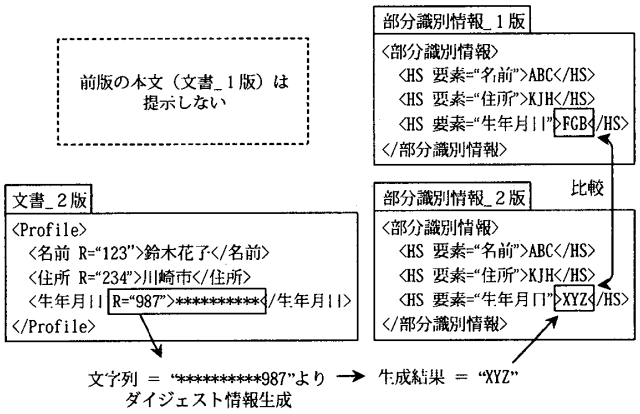

図２：部分秘匿性を考慮した部分識別情報生成例

このような生成・管理方法によれば、「部分識別情報_１版」と「部分識別情報_２版」を比較することで、生年月日を秘匿したまま、名前と住所は変更がないことを証明できる。よって、「文書_２版」＋「部分識別情報_１版」＋「部分識別情報_２版」を公開することで、前版の本文「文書_１版」の提示を回避したまま第三者証明を行うことが可能となる。よって、問題４が解決される。なお、本方式と同様の概念は、電子文書の墨塗り方式として[１]で提案されている。[１]では本方式の任意情報として乱数が用いられている。

4.5 部分同時性の保証

複数枚に分かれた派生文書の同時性・関連性を保証するために、４.１節の方法で生成した「部分識別情報」を用いる。ここで、毎回異なる任意情報として時刻関連情報（ｔ）を採用する。具体的には、前版からの訂正箇所のみ新しいｔを用いて新たな部分識別情報を生成し、訂正箇所以外は前版の部分識別情報をコピーする。これにより、訂正文書はオリジナル文書の派生文書であることを証明でき、かつ、同一人物が同じ内容を記載しても毎回異なる部分識別情報が生成されるため、紙ベースで実現されている「筆跡が同一」であることが証明可能となる。よって、問題５が解決される。また、ｔを採用する場合、ｔ＝“年月日時分秒”のように予測可能な形式で構成される可能性があり、４.４節で示したような一部情報の秘匿を行った場合、前版の部分識別情報から秘匿内容が容易に推測される脅威が発生する。より安全性を高めるため、部分識別情報の生成は、以下のアルゴリズムによって算出する。

日時（時刻）tにk番目の要素が書き換わったことを$E_{t,k}$と表現すると、
この時のk番目の要素の部分識別情報$H_{t,k}$は、

$$H_{t,k} = h(E_{t,k}, f(t))$$

と表現できる。
f：任意関数、h：ハッシュ関数等の一方向性関数

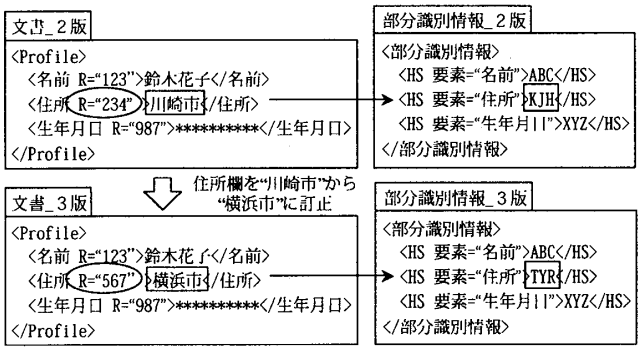

図３：部分同時性を考慮した部分識別情報生成例

5. システム構成

４章で示した電子文書訂正を行うための要件の解決策をもとに、部分完全性保証システムのプロトタイプを試作した。部分完全性保証システムの構成図を図４に示す。

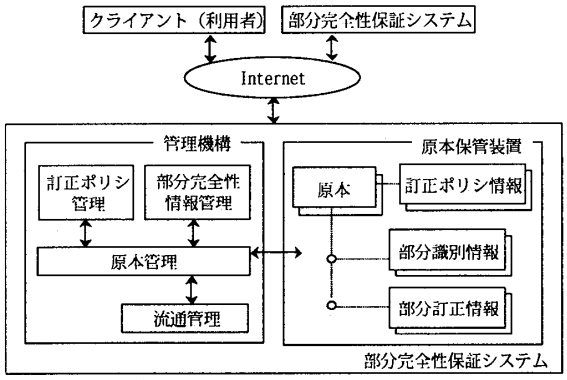

図 ４：部分完全性保証システムの構成

6. まとめ

本稿では、従来技術、および、その単純な組み合わせでは不可能であった以下の要件を満足する部分完全性保証技術を提案した。

- ✓ 電子文書の訂正箇所の特定、ならびに、訂正箇所以外は変更されていないことを特定することが可能
- ✓ 複数のエンティティ間で訂正済み電子文書を転々流通させ、かつ、各エンティティにおいて訂正・追加等を行う場合、各時点において電子文書の完全性・原本性を保証（第三者証明）することが可能
- ✓ 全ての版数の電子文書を取り出さなくても、一部の情報が隠された状態や、一部の版のみを用いた第三者証明や流通を行うことが可能

参考文献

[１] 宮崎他、「電子文書墨塗り問題」、2003-CSEC-22