2007 年 6 月 8 日
株式会社日立製作所

電子署名付与後に真正性を維持しながら秘匿すべき情報を削除できる「表計算ソフト向け墨塗り署名ツール」の試作品を開発

日立製作所 システム開発研究所(所長：前田 章／以下、日立)は、このたび、表計算ソフトで作成した電子文書に対して、電子署名(*1)を付与してデータの真正性(*2)を証明するとともに、付与後も改ざんとみなされずに秘匿すべき情報の削除(墨塗り)ができる電子署名ツール「表計算ソフト向け墨塗り署名ツール」の試作品を開発しました。

本試作品は、「墨塗り署名技術」(*3)を活用し、表計算シートのセル(マス目)ごとに、墨塗りすることができます。また、墨塗りを行っても改ざんとはみなされず、墨塗り前に付与した電子署名を用いて、データの真正性を証明することが可能です。

これにより、官公庁や企業において、表計算ソフトで作成した電子データを開示する際、個人情報や企業情報などの秘匿すべき情報を、改ざんとはみなされずに確実に削除し、かつ、墨塗り箇所以外の部分が電子署名後に変更されていないことを証明することが可能となります。

近年、法整備に伴う文書の電子化の進展や、官公庁・企業の内部統制の徹底、説明責任重視の背景から、電子文書の真正性を証明する必要性が高まっています。一方、電子文書の開示にあたっては、個人情報保護や機密情報管理のため、秘匿すべき情報を確実に削除することが必要です。現在、電子文書の真正性を証明するための電子署名ツールや秘匿すべき情報を確実に削除する墨塗りツールはあるものの、従来の電子署名技術では、たとえ適切な削除であっても改ざんとみなされてしまうため、秘匿すべき部分のみを墨塗りし、その他の部分の非改ざんを証明しつつ開示することはできませんでした。

このような背景から、日立は 2003 年に早稲田大学の岩村充教授などと共同で、電子署名を付与した電子文書に墨塗りを行っても改ざんとみなされずに、墨塗り以外の変更がされていないことを、墨塗り前に付与した電子署名を用いて検証することができる電子署名技術「墨塗り署名技術」を開発しました。その後、スキャンデータなどの画像データや XML ファイルに対応した試作品などを開発してきました。

日立は、官公庁や企業などにおいて、表計算ソフトが申請書や報告書作成など幅広い用途に使用されていることに着目し、今回、新たに表計算ソフトに、墨塗り署名技術を適用した試作品を開発しました。表計算ソフトに墨塗り署名技術を適用するにあたり、表計算ソフトが内部的に管理するセル情報のデータ形式を解析することで、墨塗りしたセルと墨塗り署名時に埋め込む識別情報などとの紐付けが可能となり、実現できました。

本試作品は、墨塗り署名技術を利用することで、表計算シートの真正性を証明するだけでなく、秘匿すべきセルを墨塗りできます。墨塗りを行う際、単に黒く表示するだけではなく、セルの情報を削除し、元のデータを復元できない特殊な情報を埋め込むため、秘匿すべき情報を確実に削除でき、情報漏えい事故を防止することが可能です。さらに、文書全体の情報から一度に電子署

名を生成するのではなく、まず、墨塗りによるデータ変更の影響をなくすため、セルごとに処理を行い、その結果得られた情報から電子署名を生成するため、墨塗り後に、墨塗り箇所以外のセルが変更されていないことを証明することも可能です。

今回、世の中に広く普及している表計算ソフトに墨塗り署名技術を適用したことにより、情報漏えい防止の観点から、適切な範囲の開示が求められる行政文書や企業の報告書、監査資料、内部統制文書などの作成に、誰でも手軽に墨塗り署名技術を利用することが可能になります。各種資料に墨塗り署名をすることで、真正性を証明しつつ、秘匿すべき情報を確実に削除して情報漏えいを防ぐとともに、適切な範囲のみを開示することが可能となり、説明責任の履行と機密情報管理を両立でき、業務効率向上にもつながります。

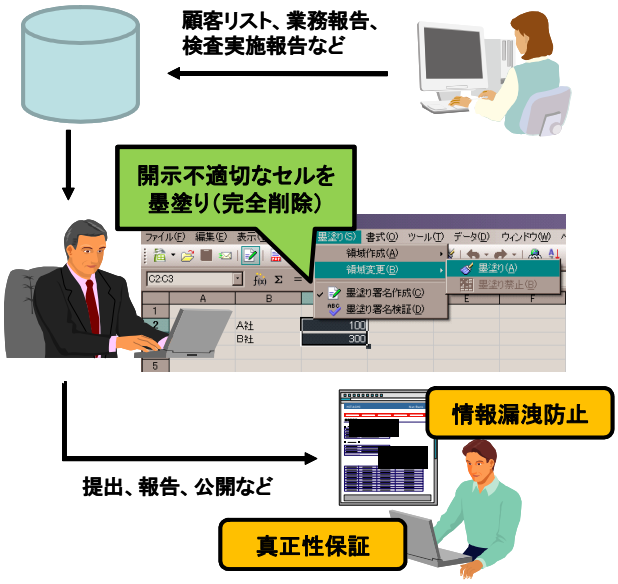

図 1. 表計算ソフト向け墨塗り署名ツールの利用イメージ

本試作品を実現した技術の特徴は以下の通りです。

(1) 表計算シートの真正性を保証する電子署名機能

本ツールでは、表計算シートの真正性を保証するため、墨塗り署名技術を利用した電子署名を付与します。

電子署名を作成する際、まず、セルごとに乱数を付与します。この乱数を用いて各セルにハッシュ関数(*4)でハッシュ値(*5)を生成し、それぞれのハッシュ値から表計算シート全体の要約値を生成します。これを公開鍵暗号方式(*6)の秘密鍵で暗号化することで、電子署名を生成します。なお、ここでセルごとに付与した乱数は、表計算シートに埋め込まれ、一緒に保存や送付がなされます。

電子署名を検証する際は、表計算シートに埋め込まれた乱数を用い、電子署名付与時と同様に生成した表計算シート全体の要約値と、電子署名を公開鍵で復号した元の要約値とを比較することで、文書の改ざんなどを検知することができます(図 2)。

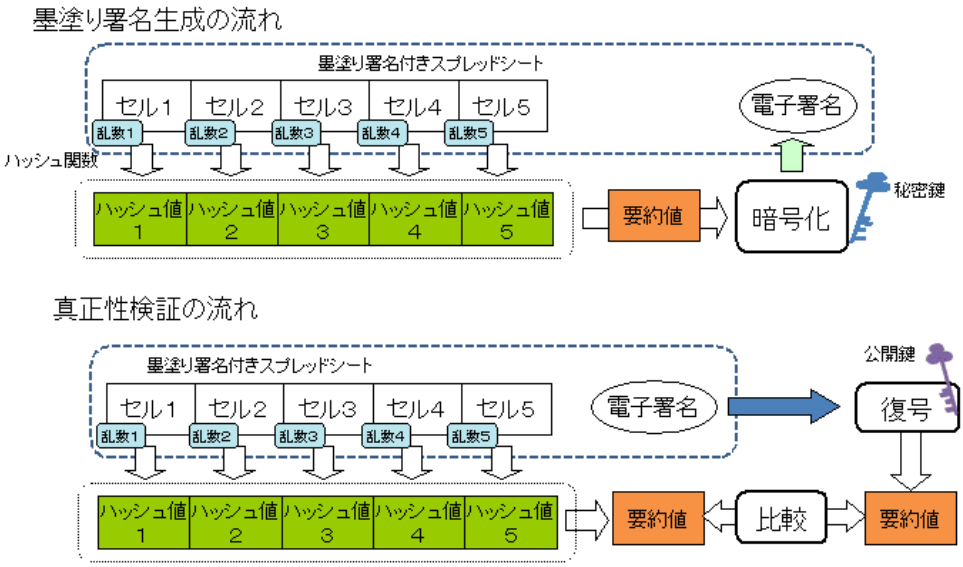

図 2. 墨塗り署名生成と真正性検証の流れ

(2) 表計算シートからの情報漏えいを防止する墨塗り機能と真正性を確認する検証機能

表計算シート中に、秘匿すべき情報が含まれたセルがある場合、本試作品にて電子署名を付与後、当該セルを墨塗りできるとともに、その際も改ざんとはみなされずに、墨塗り以外の変更がないことを証明することが可能です。

墨塗りは、署名作成時に乱数を設定したセルごとに行います。これは、墨塗りしたセルを単に黒く表示するのとは異なり、墨塗りしたセルの内容と乱数を削除し、削除したデータの替わりのハッシュ値を表計算シートに埋め込み保存します。なお、ハッシュ値からは元のデータを復元できないため、情報漏えいを防止できます(図 3)。

署名を検証する際は、墨塗りされたセルは埋め込まれているハッシュ値を用い、それ以外は、表計算シートに埋め込まれた乱数を使用し、ハッシュ値を生成します。そして、それらのハッシュ値から生成した表計算シート全体の要約値と、電子署名を公開鍵で復号した要約値とを比較することで、墨塗りしても改ざんはとみなされず、墨塗り前に付与した電子署名を用いて、表計算シート全体の真正性を証明することが可能です(図 4)。

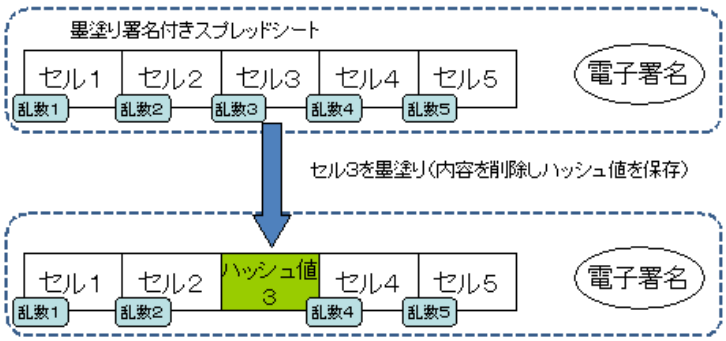

図 3. 墨塗りの流れ

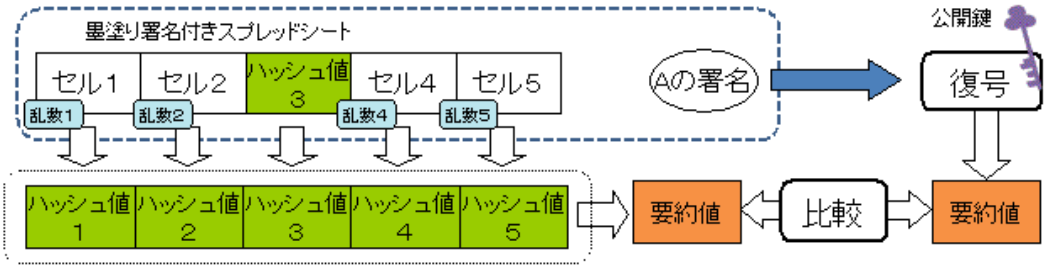

図 4. 墨塗り後の検証の流れ

なお、本成果は、2007 年 5 月 29 日に東京都小金井市で開催された電子情報通信学会の第 1 回マルチメディア情報ハイディング研究会においてデモ展示を行いました。

■注釈

(*1) 電子署名：文書作成者のなりすましや電子文書の改ざんを防ぐための技術。

(*2) 真正性：誰が作ったのか、また、作られてから改ざんされていないかの証明。

(*3) 墨塗り署名技術：日立製作所が、早稲田大学 岩村充教授、横浜国立大学 松本勉教授、東京電機大学 佐々木良一教授、電気通信大学 吉浦裕教授、東京大学 今井秀樹教授（当時）と共同で開発した電子署名技術。従来の電子署名技術では、たとえ適切な削除であっても改ざんとみなされてしまうのに対し、墨塗り署名技術では、秘匿すべき部分だけを墨塗りし、その他の部分の非改ざんを証明しつつ開示することが可能。

(*4) ハッシュ関数：任意長の入力データから短い固定長(例：160-bit，256-bit など)のデータを出力する関数。出力値から元の入力データを逆算することや、同じ出力値を与える２つの異なる入力データを一組見つけることが事実上不可能といった性質をもつ。

(*5) ハッシュ値：ハッシュ関数の出力値。

(*6) 公開鍵暗号方式：暗号化方式の一種。暗号化に使う鍵と、復号に使う鍵が異なることが特徴。秘匿性保持目的で利用する場合、暗号化は、公開鍵と呼ばれる誰もが知りうる鍵を使って行い、復号は、それと対になる秘密鍵と呼ばれる特定のユーザのみが知る鍵を使用して行う。真正性保証目的で利用する場合(電子署名として利用する場合)は、特定ユーザのみが知る秘密鍵を使ってメッセージ(またはそのハッシュ値)を暗号化し、署名を得る。この署名を検証する際は、秘密鍵と対になる公開鍵を使用して署名を復号し、署名とともに送られてきたメッセージ(またはそのハッシュ値)と比較を行う。

■照会先

株式会社日立製作所 システム開発研究所 企画室［担当：森］
〒215-0013 神奈川県川崎市麻生区王禅寺 1099 番地
電話 044-959-0325(ダイヤルイン)

以上