2024 年 8 月 26 日
株式会社日立製作所
国立研究開発法人産業技術総合研究所

日立と産総研が共同開発した新たな墨塗署名技術が ISO/IEC に採用

公的文書等のプライバシー保護と真正性を両立し、安全なデータ活用社会に貢献

株式会社日立製作所(執行役社長兼 CEO：小島 啓二/以下、日立)と国立研究開発法人産業技術総合研究所(理事長：石村 和彦/以下、産総研)が共同開発した墨塗署名技術(以下、墨塗署名)の 2 つの方式が、国際標準化機構(ISO)/国際電気標準会議(IEC) の第一合同技術委員会 (JTC 1)での最終承認を経て、このたび ISO/IEC 23264-2 として採用されました。これらの方式は、文書を部分的に開示する際に、その文書が改ざんされていないこと(真正性)を保証します。

墨塗署名は、文書の部分開示の手続きをデジタル技術で実現しつつ、不正な修正や改ざんを検出可能にする技術です。今回新たに採用された 2 方式により、公的文書の部分開示がさらに効率化されるとともに、医薬品、金融などの商品開発において、データ利活用の利便性を損なわずに匿名化処理(プライバシー保護)の正当性を保証することが可能となり、安全なデータ活用社会の実現への貢献が期待されます。

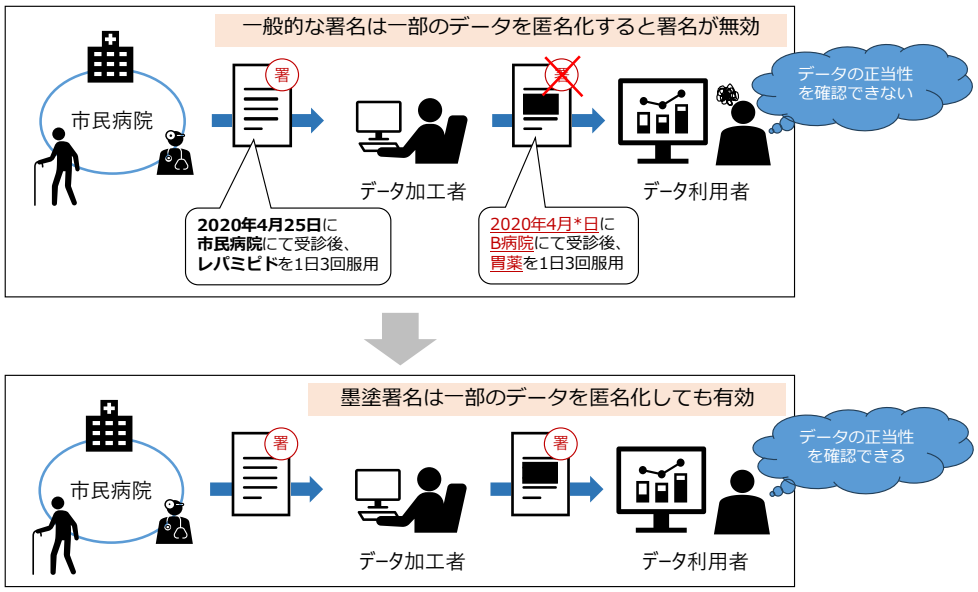

図 1 医療データへの墨塗署名の活用事例

（医薬品開発において、既存商品の利用者データを活用する際に、データに含まれる個人情報などを匿名化処理する事例）

■標準化の背景

近年、デジタル技術の普及により、従来印刷物主体だった各種手続きが電子的手続きに置き換わり、データの修正や改ざんを検出し、データの真正性を保証する電子署名技術がますます重要となっています。

現在の公的文書の管理では、プライバシーなどへの配慮を目的として公開前に文書の一部を削除する、いわゆる「墨塗り」と呼ばれる処置が施されることがあります。しかし、従来の電子署名技術は、墨塗り自体を文書の改ざんと判断してしまうため、墨塗りされた文書の真正性を保証することが困難でした。

こうした中、用途が広がってきた電子署名技術の応用の一環として、ISO/IEC JTC 1[*1]は、文書の編集が可能な暗号技術(redaction of authentic data)の規格 ISO/IEC 23264 の策定を実施しています。この標準化を推進するため、日立と産総研は約 20 年前から、文書の墨塗りをデジタル方式で実現する電子署名技術(墨塗署名)の研究開発を先行的に進めてきました。この共同開発の成果として、国際標準規格 ISO/IEC 23264-2 に 2 つの墨塗署名技術の方式(MHI06, MIMSYTI05)が採用されました。

■標準化された技術の特徴

墨塗署名では、文書の生成時に墨塗り可能なデータブロックをあらかじめ設定し、開示前に各データブロックの開示/非開示を設定できます。また、文書の生成時に付与された署名により、部分的に非開示となった文書を検証し、正当な編集のみが行われた文書であることを確認できます。さらに、今回 ISO/IEC 23264-2 に採用された複数の墨塗署名の方式には、それぞれ異なる付加的なセキュリティの性質があり、日立と産総研が共同開発した MHI06 と MIMSYTI05 は、いずれも複数回の文書編集が可能という性質を持ち、開示範囲を複数の階層に分けて制御するという特徴を持ちます。

MHI06 は、あらかじめ指定された範囲で複数の署名付き文書やデータを統合する「統合可能性(Mergeability)」および墨塗りされた箇所の情報を秘匿する性質「墨塗箇所検出不可能性(Undetectability of redactions)」を備えています。プライバシー保護の状況やデータの提供先に応じて、開示する署名付きデータの範囲を動的かつ効率的に変更する用途に適した方式です。

MIMSYTI05 は、任意の署名方式を用いて墨塗署名の機能を付加することを可能にします。RSA 署名[*2]や ECDSA[*3]だけでなく、量子計算機でも解読できない署名方式とも組み合わせることが可能です。さらに、墨塗りが行われたかどうかを検出できるので、墨塗りの有無によって文書を振り分けるといった用途に適した方式です。

■今後の展開

当初、墨塗署名は公的文書の保護を目的として開発されたデジタル技術でしたが、今後はそれだけに留まらず、部分的に開示されたデータの原本性の検証など、幅広い応用が見込まれます。例えば、匿名化技術と組み合わせることで、プライバシー保護とデータの真正性保証を両立する技術として広く活用が期待されます。日立と産総研は、これからも墨塗署名をはじめとする暗号技術の研究開発や製品・サービス化に取り組み、安全なデジタル社会の実現に貢献していきます。

*1ISO/IEC JTC 1: 国際標準化機構 (ISO: International Organization for Standardization)、国際電気標準会議 (IEC: International Electrotechnical Commission) の第一合同技術委員会 (JTC 1: Joint Technical Committee 1)

*2 RSA 署名: 素因数分解の困難性を安全性の根拠とする電子署名方式

*3 ECDSA(Elliptic Curve Digital Signature Algorithm): 楕円曲線上の離散対数問題の困難性を安全性の根拠とする電子

署名方式

■日立製作所について

日立は、データとテクノロジーでサステナブルな社会を実現する社会イノベーション事業を推進しています。お客さまの DX を支援する「デジタルシステム&サービス」、エネルギーや鉄道で脱炭素社会の実現に貢献する「グリーンエナジー&モビリティ」、幅広い産業でプロダクトをデジタルでつなぎソリューションを提供する「コネクティブインダストリーズ」という 3 セクターの事業体制のもと、IT や OT(制御・運用技術)、プロダクトを活用する Lumada ソリューションを通じてお客さまや社会の課題を解決します。デジタル、グリーン、イノベーションを原動力に、お客さまとの協創で成長をめざします。3 セクターの 2023 年度(2024 年 3 月期)売上収益は 8 兆 5,643 億円、2024 年 3 月末時点で連結子会社は 573 社、全世界で約 27 万人の従業員を擁しています。詳しくは、日立のウェブサイト(https://www.hitachi.co.jp/)をご覧ください。

■国立研究開発法人産業技術総合研究所について

国立研究開発法人産業技術総合研究所は、国内に 12 か所の研究拠点を持ち、約 2,300 名の研究者を擁する国立の研究開発法人です。経済および社会の発展に資する科学技術の研究開発を行う日本最大級の公的研究機関であり、「社会課題解決」と「産業競争力強化」をミッションとしています。そのための体制として産総研のコア技術を束ね、その総合力を発揮する「5 領域 2 総合センター」があり、イノベーションを巡る環境の変化やそれらを踏まえて策定された国家戦略等に基づき、ナショナルイノベーションシステムの中核的、先駆的な立場で研究開発を行っています。

詳しくは、産総研のウェブサイト(https://www.aist.go.jp/)をご覧ください。

■お問い合わせ先

株式会社日立製作所　研究開発グループ
お問い合わせフォーム：　https://www8.hitachi.co.jp/inquiry/hqrd/news/jp/form.jsp

国立研究開発法人産業技術総合研究所　サイバーフィジカルセキュリティ研究センター
お問い合わせページ：　https://www.cpsec.aist.go.jp/contact/

以上