SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

データに対する匿名加工を考慮したデジタル署名の検討
A Study on Digital Signature Considering Data Anonymization

肥後　春菜 * 一色　寿幸 * 森　健吾 * 田宮　寛人 † 土田　光 *
Haruna Higo Toshiyuki Isshiki Kengo Mori Hiroto Tamiya Hikaru Tsuchida

キーワード 匿名化，墨塗署名，カメレオンハッシュ

あらまし

個人情報保護法の改正 [3] や次世代医療基盤法 [4] の施行により，匿名加工されたデータの第三者提供によるデータ利活用が活発になると考えられる．データの真正性を保証する技術としてデジタル署名が知られているが，加工されたデータの第三者提供を行う場合，デジタル署名を用いても真正性の検証に失敗することが知られている．また，データに対して真に正しい加工を行ったかという加工処理の正当性についても，デジタル署名では検証することができない．

加工されたデータの第三者提供における，データの真正性や加工処理の正当性を保証する技術として，墨塗署名を用いた方式 [2, 5] が提案されている．しかし，先行研究では署名生成時にデータに対する加工方法をあらかじめ指定する必要がある．このため，データに対する加工の柔軟性が失われ，所望のデータ加工を行えない場合があった．

本稿では，匿名加工されたデータに対するカメレオンハッシュベースの墨塗署名 [1] の適用を検討する．検討する方式では，データの真正性を保証しつつ，対象となるデータに対して任意の加工を施すことができる．

参考文献

[1] G. Ateniese, D. H. Chou, B. de Medeiros, and G. Tsudik. Sanitizable signatures. In *ESORICS*, Vol. 3679 of *Lecture Notes in Computer Science*, pp. 159–177. Springer, 2005.

[2] 藤原, 佐藤. 匿名化の正当性を検証可能な墨塗り匿名化方式の提案. 2019 年暗号と情報セキュリティシンポジウム (SCIS2019). IEICE, 2019.

[3] 個人情報の保護に関する法律及び行政手続における特定の個人を認識するための番号の利用等に関する法律の一部を改正する法律, 2015. (2021 年 12 月 8 日　確認).

[4] 医療分野の研究開発に資するための匿名加工医療情報に関する法律 — e-gov 法令検索, 2017. (2021 年 12 月 8 日　確認).

[5] 冨樫, 山本, 佐藤, 吉野. 匿名化の正当性を検証可能な匿名化署名方式の提案. コンピュータセキュリティシンポジウム 2021 (CSS2021). CSEC 研究会, 2021.

* NEC, 〒 211-8666 神奈川県川崎市中原区下沼部 1753, NEC Corporation, 1753 Shimonumabe, Nakahara-ku, Kawasaki-shi, Kanagawa, 211–8666 Japan. {h-higo-aj,toshiyuki-isshiki,ke-mori.bx,h_tsuchida}@nec.com
† 本成果は NEC 在籍時のものである．