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

「モノの電子署名」の複数物体への拡張
Extension of “Signature for Objects” to Multiple Objects

浅野 泰輝 * 林 リウヤ * † 林田 淳一郎 * † 松田 隆宏 †
Taiki Asano Ryuya Hayashi Junichiro Hayata Takahiro Matsuda

山田 翔太 † 勝又 秀一 † 坂井 祐介 † 照屋 唯紀 †
Shota Yamada Shuichi Katsumata Yusuke Sakai Tadanori Teruya

シュルツ ヤコブ † アッタラパドゥン ナッタポン † 花岡 悟一郎 †
Jacob Schuldt Nuttapong Attrapadung Goichiro Hanaoka

松浦 幹太 * 松本 勉 † ‡
Kanta Matsuura Tsutomu Matsumoto

キーワード 電子署名，サプライチェーン

あらまし

近年の偽造品や海賊版製品の取引の増加に伴い，取引の正当性を検証可能にする技術の必要性が高まっており，その１つとして電子署名がある．しかしながら，従来の電子署名方式では，電子データではない物体そのものに対しての署名作成はできない．そこで，[1] により，物体の加工や電子データへの変換といった物理的な操作を取り扱うことが可能な枠組みを定式化することで，任意の物体を対象とした「モノの電子署名」が提唱された．

しかし，[1] は一物体のみに対して加工，変換を施すことを想定しているため，本稿ではこの枠組みを複数物体においても動作するよう拡張し，より実システムに近い形での署名方式を与える．特に，サプライチェーンの各ステップにおいて物体の生成，加工，組み合わせのいずれかが可能であるという状況のもとで，各物体に対してそれがどのような変遷をたどってきたかを保証する署名を付与できるモデルを導入する．さらに，その安全性定義，および Append-Only 署名と集約署名を用いた一般的構成を提案し，簡単な概念実証も行う．

参考文献

[1] 林 リウヤ ほか, “モノの電子署名：物体に署名するための一検討, Signature for Objects: Formalization, Security Definition, and Provably Secure Constructions, ”2021 年 コンピュータセキュリティシンポジウム (CSS2021) 予稿集, pp.740-747, 2021

* 東京大学生産技術研究所, 東京都目黒区駒場 4-6-1, Institute of Industrial Science, the University of Tokyo, 4-6-1 Komaba, Meguro-ku, Tokyo 153-8505 Japan
† 産業技術総合研究所, 東京都江東区青海 2-3-26, National Institute of Advanced Industrial Science and Technology, 2-3-26 Aomi, Koto-ku, Tokyo 135-0064 Japan
‡ 横浜国立大学大学院環境情報研究院, 神奈川県横浜市保土ケ谷区常盤台 79-7, Faculty of Environment and Information Sciences, Yokohama National University, 79-7 Tokiwadai, Hodogaya-ku, Yokohama 240-8501 Japan