関数型暗号とブロックチェーンの組合せによる秘匿分散記録システムの試作

柴田陽一[1] 小関義博[1] 川合豊[1] 大松史生[1] 高橋剛[2] 重森猛[2]

概要：ブロックチェーンを活用しているシステムは，耐障害性，耐改ざん性，低コストが期待される．一方で参加している全ノードで同じ台帳を共有するため，機微な情報を扱う用途には採用が躊躇われるという課題がある．そこで，我々は関数型暗号によりブロックチェーンに記録される情報を暗号化，秘匿情報を不正なアクセスから保護する仕組みを秘匿分散記録システムとして考案した．電子母子手帳システムを題材に秘匿分散記録システムのプロトタイプを開発し，秘匿情報の閲覧に対するアクセス制御が有効に機能することを確認した．

Secure distributed recording system based on functional encryption and blockchain

YOICHI SHIBATA[1] YOSHIHIRO KOSEKI[1]
YUTAKA KAWAI[1] FUMIO OMATSU[1]
GO TAKAHASHI[2] TAKERU SHIGEMORI[2]

1. はじめに

ブロックチェーンは Bitcoin に代表される仮想通貨を支える分散型台帳技術として注目を集め，昨今では，金融分野に限らず，様々な分野でブロックチェーンを活用した実証実験等が行われている．

例えば，東京海上日動と NTT データは，保険証券へのブロックチェーン技術適用に向けて実証実験を行い，その結果を報告している[1]．また，エナリスは，ブロックチェーン技術を活用した電力取引サービス等の商用化に向けた検討及び実証実験を行っている[2][3].

ブロックチェーンを活用したシステムは，以下のメリットが期待できる．

- 複数ノードでの情報共有により，耐障害性を得られる．
- 電子署名をベースとしたチェーンにより，改ざん困難なデータ構造となっている．
- 中央集権的にシステムを統括する管理者が不要であるため，低コストで運用できる．

一方，ブロックチェーンは参加している全ノードで同じ台帳を共有するため，機微な情報を扱う用途には採用が躊躇われるという課題がある．

そこで，我々は関数型暗号によりブロックチェーンに記録される情報を暗号化，秘匿情報を不正なアクセスから保護する仕組みを秘匿分散記録システムとして考案した．

更に，電子母子手帳システムを題材としてプロトタイプを試作し，秘匿分散記録システムの有効性を検証した．

検証の結果，利用者からのアクセスに対する制御ができており，関数型暗号による遅延の影響もなく，秘匿分散記録システムとして有効に機能していることを確認した．

2. ブロックチェーン

ブロックチェーンでは，取引記録を束ねたブロックを電子署名で時系列に連ねてチェーンを構築する．構築されたチェーンは，参加している全ノードで共有され，各ノードによってチェーンの妥当性が検証される．そのため，ブロックチェーンを活用したシステムは，以下のメリットが期待できる．

- 複数ノードでの情報共有により，耐障害性を得られる．
- 電子署名をベースとしたチェーンにより，改ざん困難なデータ構造となっている．
- 中央集権的にシステムを統括する管理者が不要であるため，低コストで運用できる．

一方，ブロックチェーンを活用したシステムにおいて，個人情報や企業機密のような秘匿情報を扱う場合には注意が必要である．ブロックチェーンに記録された情報は参加しているノードで共有されているため，情報の所有者による管理が届かない状態にある．そのため，情報の所有者の意図しないところで，秘匿情報への不正なアクセスが行われる可能性がある．

そこで，我々は次章で説明する関数型暗号を用いてブロックチェーンに記録される情報を暗号化し，情報の所有者による管理が届かない状態であっても，秘匿情報を不正なアクセスから保護する仕組みを考案した．

1 三菱電機株式会社 情報技術総合研究所 情報セキュリティ技術部
Mitsubishi Electric Corporation
2 （株）ハウインターナショナル
HAW International Inc.

3. 関数型暗号

本章では，秘匿分散記録システムで用いる関数型暗号について説明する．

本稿では，関数型暗号として，2010 年に岡本，高島が提案した方式[4]を用いている．関数型暗号においては，属性(例：所属部=経理部，役職=部長)と述語 (例：所属部=総務部 AND 役職=課長)の関係が真の場合のみ復号が可能となる．属性は型と値を「=」で結んだ表現とする．関数型暗号の方式は，暗号文側に述語を設定する CP(Ciphertext-Policy)型と，ユーザ秘密鍵側に述語を設定する KP(Key-Policy)型，暗号文とユーザ秘密鍵の双方に述語を設定できる UP(Unified-Policy)型の 3 種類の方式が存在する．CP 型はファイル共有，KP 型はコンテンツ配信への応用例が多い．秘匿分散記録システムにおいては，CP 型の関数型暗号を用いることにする．

4. 関数型暗号とブロックチェーンの組合せによる秘匿分散記録システム

我々はブロックチェーンに記録する情報を関数型暗号で暗号化することにより，秘匿情報を不正なアクセスから保護する仕組みを秘匿分散記録システムとして考案した．

秘匿分散記録システムでは，ブロックチェーンを活用したシステムにおける課題である秘匿情報の管理を，関数型暗号が持つアクセス制御機能により解決する．具体的には，ブロックチェーンに記録する秘匿情報を関数型暗号で暗号化し，復号可能な人を該当の秘匿情報にアクセスが認められた人に限定する．ブロックチェーンに記録された秘匿情報は参加しているノードで共有され，情報の所有者の手からは離れるが，秘匿情報を復号して情報にアクセスできる人はアクセス可能な人に限定されているため，情報の所有者が意図しないアクセスからは保護されていることになる（図 1 参照）．

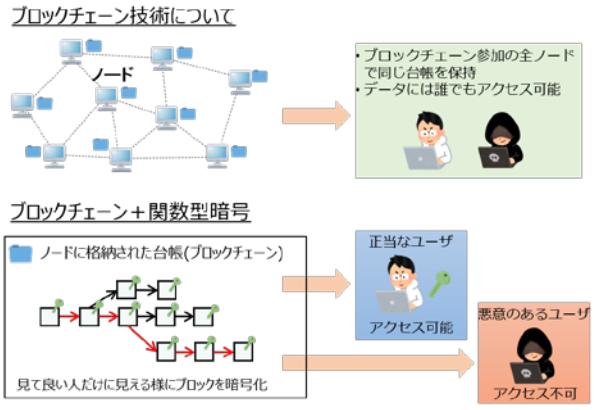

図 1　関数型暗号による秘匿情報の保護

5. 電子母子手帳を題材にしたプロトタイプシステム

我々は，秘匿分散記録システムの有効性を検証するため，具体的なアプリケーションを想定したプロトタイプを開発した．本章では，開発したプロトタイプシステムについて説明する．

5.1 アプリケーション

プロトタイプを実装する上でのアプリケーションには，予防接種情報を主とした母子手帳の電子化を選択した．その理由は以下の通りである．

- 母子手帳の紛失などにより，過去に接種した予防接種の情報が確認できなくなるなどの問題が発生しており，母子手帳の電子化による問題解決のニーズがある．実際に母子手帳の電子化は様々な自治体で行われている[5][6].
- 母子手帳は自治体ごとに管理しているため，電子化に要するシステムの構築及び運用コストの削減が求められる．ブロックチェーンをシステムの基盤として活用することによりコストの削減が期待できる．
- 予防接種の情報はプライバシー情報であり，閲覧可能な人を限定することが求められる．関数型暗号によりプライバシー情報の閲覧が可能な人を限定することが可能である．

5.2 シナリオ

プロトタイプ開発において，予防接種情報に関連する電子母子手帳の利用シナリオを検討した．検討した利用シナリオは以下の通りである．

- 登場人物

接種者：予防接種の対象者.
接種者の親：予防接種の対象者の親.
医者：予防接種を行う医者.
自治体：接種者が居住する自治体.
製薬メーカー：予防接種ワクチンを製造したメーカー.
データ分析企業：予防接種ワクチンの効果や副作用などを分析する企業.

- ユースケース

ケース１：予防接種実施時に，医者が接種者の予防接種情報をシステムに記録する.
ケース２：接種者または接種者の親が接種者の予防接種の情報をシステムから確認する.
ケース３：自治体が予防接種の接種率や未接種者の把握のためにシステムから情報を収集する.
ケース４：製薬メーカーが自社で製造したワクチンの効果や副作用などを調査するためにシステムから情報を取得する.
ケース５：データ分析企業が予防接種による効果や副作用などを分析するためにシステムから情報を収集する.

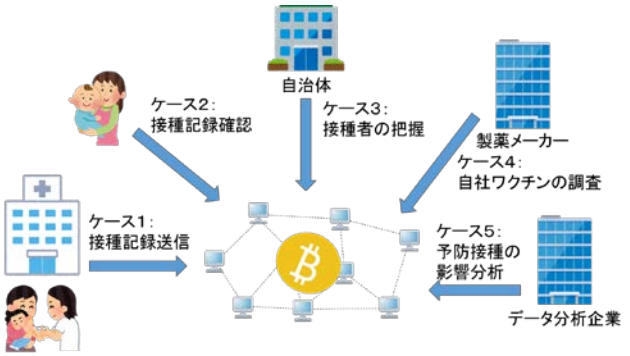

図 2　プロトタイプのユースケース

5.3　プロトタイプシステムの構成

5.2 節のシナリオを実現するシステムをプロトタイプとして構築した．構築したプロトタイプシステムは以下の構成となっている．

システムの基盤となるブロックチェーンは，実際のブロックチェーンの動作をクラウド上で模倣する形で構築した．利用者はスマートフォン及びパソコンからクラウドにアクセスすることでシステムを利用する（図 3 参照）．

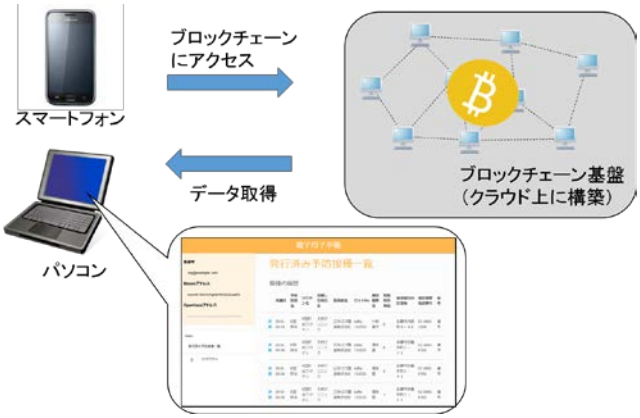

図 3　プロトタイプシステムの構成

各ユースケースでの利用方法は以下の通りである．

ケース１：病院のパソコンまたはスマートフォンからシステムにアクセスし，図 4 の画面から 接種情報を入力する．

図 4　予防接種情報入力画面

ケース２：接種者または接種者の親が自身のパソコンまたはスマートフォンからシステムにアクセスし，図 5 の画面から接種情報を確認する．

図 5　予防接種情報の閲覧

ケース３：自治体のパソコンからシステムにアクセスし，図 6 の画面から接種者の記録を確認する．

図 6　自治体による接種情報の確認

ケース４：製薬メーカーのパソコンからシステムにアクセスし，図 7 の画面から自社で製造したワクチンの接種情報を確認する．

図 7　製薬メーカーによる接種情報の確認

ケース５：データ分析企業のパソコンからシステムにアクセスし，図 8 の画面から接種情報を確認する．

図 8　分析企業による接種情報の確認

6. 考察

本章では開発したプロトタイプシステムについて考察する．

- 秘匿分散記録システムの有効性

プロトタイプシステムにおいては，製薬メーカーとデータ分析企業からの接種情報の閲覧に対して，関数型暗号によるアクセス制御が有効に機能している．製薬メーカーは自社が製造したワクチンの情報のみが閲覧可能であり，データ分析企業は接種者の個人情報を閲覧できない．

- 関数型暗号による影響

本プロトタイプシステムでは，接種情報の記録時と閲覧時に関数型暗号による暗号化・復号を行う．暗号化・復号の処理により若干の遅延が生じる可能性があるが，通信やその他の遅延と比較して十分に小さな遅延に収まると考えられる．実際にプロトタイプシステムで動作を確認した限りにおいても利用者の操作に支障が出るような遅延は確認されなかった．

- 関数型暗号の鍵管理

今回のプロトタイプシステムでは，関数型暗号によるアクセス制御が有効に機能することの確認に重点を置いていたため，関数型暗号の鍵を管理する仕組みまでは実装していない． 実際にシステムを運用する上では，鍵の生成や失効を行う仕組みを実装する必要がある．

7. おわりに

本稿では，秘匿分散記録システムについて説明した．秘匿分散記録システムは，関数型暗号によりブロックチェーンに記録される情報を暗号化，秘匿情報を不正なアクセスから保護する仕組みである．電子母子手帳システムを題材に秘匿分散記録システムのプロトタイプを開発し，秘匿情報の閲覧に対するアクセス制御が有効に機能することを確認した．

参考文献

[1]　東京海上日動火災保険株式会社，株式会社 NTT データ:“保険証券へのブロックチェーン技術適用に関する実証実験の完了”，http://www.tokiomarine-nichido.co.jp/company/release/170424_01.html (参照 2018-04-17).

[2]　株式会社エナリス:“ブロックチェーン技術を活用した電力取引サービス等の商用化に向けた検討を開始”，https://www.eneres.co.jp/news/release/20170531.html(参照 2018-04-17).

[3]　株式会社エナリス:“ブロックチェーンを活用したスマートシステムによる，「高齢者の見守りサービス」，福島県浪江町で実証試験を開始”，https://www.eneres.co.jp/news/release/20180116.html (参照 2018-04-17).

[4]　Tatsuaki Okamoto,Katsuyuki Takashima " Fully Secure Functional Encryption with General Relations from the Decisional Linear Assumption," CRYPTO 2010, volume 6223 of LNCS, pp.191-208 2010.8

[5]　“マイ ME-BYO カルテと連携する電子母子手帳アプリ（「母子モ」）”，http://www.pref.kanagawa.jp/docs/mv4/cnt/f532715/p1061642.html(参照 2018-05-07).

[6]　“電子親子手帳サービスを配信しています”，https://www.city.ichihara.chiba.jp/kosodate/kodosatesien/kosodatesiensisetu/neuvolacenter/sukusuku.html(参照 2018-05-07)