改ざん困難なエビデンスを用いた文書管理方法

池田 大地[1,a)]　森田 光[1]

概要：組織では，後から事実を検証するために，事業内容を文書化することが行われる．しかし，森友学園問題では，役所で文書が改ざんされた疑いがあり，その検証に困難をきわめた．文書の改ざん防止の為には，文書の責任者と文書の関連性などのエビデンスを記録に留め，検証可能にする必要がある．
本稿ではエビデンスを作成し，公開する方法を提案する．第 3 者がエビデンスの検証を行うことで，文書の正当性を確認できる．また，文書の検証は調停者が行うので，必要な文書データを公開することで改ざん困難な文書管理方法を提案する．

キーワード：CBC モード，CMAC

A management scheme by using document evidences

Daichi Ikeda[1,a)]　Hikaru Morita[1]

Abstract:
Organizations keep the document their business description to later verify the facts. However, in the Moritomo Gakuen problem, there was a suspicion that the document was falsified at the government office, and it was difficult to verify it. For the prevention of falsification of documents, it is necessary to record evidences such as the relationship between the person responsible for the document and the document so that it can be verified.
In this paper, the authors propose a method to create and publish evidence. A third party can verify the evidence by legitimate evidence. In addition, since the arbitrator verifies the document, the authors propose a management method that makes it hard to falsified by showing necessary document data.

Keywords: CBC Mode, CMAC

1. はじめに

組織では，後から事業を検証するために，事業内容を文書化する．正確に文書化することで，文書の信頼性が保たれ，組織が正しい事業を行なっていることを示すことができる．不正が起こった場合でも，文書をもとに検証することで，原因が判明する．また，正確に検証ができれば，文書の偽造を事前に防止することができる．

しかし，森友学園問題をはじめとした，公的機関による決定事項に関する文書の改ざん疑惑などがある [1]．また，かんぽ生命保険の不正販売問題で，顧客に無断で契約書類を偽造するなどといった問題がある [2]．

文書の不正が起こる要因として不正をする機会が存在している．不正を起こす要因として正当化，動機，機会があり，この 3 つの要因があると不正が起こる．公的機関では文書を保存する上で保存期間を設定する必要がある．その期間を満了した後に，文書の内容を精査する [3]．しかし一年未満に設定した場合，精査せずに文書を破棄することができる．その結果，不正を行う機会があったため，不正が起きる要因になった．

文書の改ざん防止の為には，文書の責任者と文書の関連性などのエビデンスを記録に留め，検証可能にする必要がある．強固な管理方法を実現することで不正の機会を事前に防ぐためである．本稿ではエビデンスを作成し，公開す

[1] 神奈川大学大学院
Graduate School of Kanagawa University
[a)] r201970069wk@jindai.jp

る方法を提案する．第 3 者がエビデンスの検証を行うことで，文書の正当性を確認できる．また，文書の検証は調停者が行うので，必要な文書データを公開することで改ざん困難な文書管理方法を提案する．

本論文の構成は以下の通りである．第 2 節では，提案方法と定義を示す．第 3 節では，システムを示す．第 4 節では考察を示す．第 5 節でまとめる．

2. 提案方法

本提案では，文書の一部データをエビデンスとして作成し，文書を作成する権限がない第 3 者に公開する．第 3 者によるエビデンスの検証により，改ざん困難な文書にすることを目的とする．

担当者がエビデンスを作成したとき，対応した識別子を取得する．この識別子によって公開されたエビデンスの中身を閲覧することができ，文書の存在が明らかになる．エビデンス内に簡易な事業内容や署名があり，第 3 者はその内容を検証できる．そこで不備がある場合，調停者に開示請求を行い，文書の必要データを取得する．エビデンスを用いた検証で改ざんを検出することができ，署名により担当者を判別することで改ざん困難な文書を実現できる．

上記の機能を実現するため，エビデンス，文書，署名の定義を用いることにする．また，エビデンスの公開と文書の検証では電子掲示板 (BBS) を用いる．

2.1 エビデンス

2.1.1 記号の定義

- メタデータ; mt
- 担当者 ID; BID
- 署名; Sig
- ハッシュ値; $h(m)$
- 文書 ID; DID=$h(BID, Sig, h(m), mt)$
- 文書; m

ここで，mt は文書の内容をもとに簡易な内容を示したデータである．mt を確認することで該当する m の一部内容を確認することができる．BID は事業を行っていく上で，関わった担当者 ID に相当する．Sig は m を作成した担当者がデジタル署名により生成した署名に相当する．$h(m)$ は m をもとに生成したハッシュ値に相当する．m と関係性を持たせるため格納する必要がある．DID は $BID, h(m), Sig, mt$ のデータをハッシュ化した識別子に相当する．

2.1.2 エビデンスの定義

エビデンス E_{pub} は次のように定義する：

$$E_{pub} = (DID, BID, Sig, h(m), mt)$$

この E_{pub} は基本的に公開する．E_{pub} によって第 3 者は m に関する一部データを閲覧することができる．

2.2 文書

2.2.1 記号の定義

- 事業内容; t

ここで，t は事業内容に相当する．原則 t のデータは非公開である．

2.2.2 文書の定義

文書 m は次のように定義する：

$$m = (DID, BID, t,)$$

m は基本的に非公開であるため，第 3 者は m が正当に管理されているか判断できない．そこで E_{pub} で生成された DID を m に格納する．DID は E_{pub} が生成された場合，担当者が取得する．DID が m に格納されることによって，担当者が E_{pub} を公開した証明になり，正当な手順で m を生成している証明になる．また，担当者は DID を第 3 者に公開するので，E_{pub} により，m は非公開でも正当に作成されているか判断できる．

2.3 署名

ここでは，エビデンスの署名方法を示す．エビデンスを作成する上で，文書に署名を付与することで誰が関わったか判明する．また，その署名に信頼性があれば，不正が行われる可能性が低くなる．本稿ではデジタル署名**?**, block 使用する．以下、関連する記号を定義する:

記号の定義

- 公開鍵; Vk
- 秘密鍵; Sk

担当者が Sk で DID に署名する.

$$Sk(DID) = Sig$$

対応する Vk での署名の確認

$$Vk(Sig, DID)$$

Sig を生成する上で，担当者は自身の Sk を用いて DID に対しての Sig を生成し，E_{pub} に付与する．この時，担当者は Vk を公開することで第 3 者も Sig の検証ができるため，E_{pub} の正当性を判別できる．

2.4 エビデンスの掲載

E_{pub} を第 3 者に公開するため，電子掲示板 (BBS) を用いる．担当者は BBS に E_{pub} と Vk を掲載する．Vk は E_{pub} 内にある Sig を検証するために保管する．E_{pub} の識別子である DID は掲載後，担当者に送る．担当者は DID を m に格納することで E_{pub} を作成した証明になる．

2.5 エビデンスの公開

第 3 者が E_{pub} を閲覧するには DID を BBS に送り，該当

した E_{pub} を取得する．そのため，担当者は第 3 者に DID を公開する必要がある．公開された DID を用いて E_{pub} を取得する．また BBS 内に Vk も格納されていることから，第 3 者は Vk をもとに Sig を検証することができる．

2.6 文書の検証

m を検証する上で，信頼性のある調停者が m の検証を行う．担当者は不正の疑惑がある m を調停者に送る．調停者はハッシュ関数を用いて m のハッシュ値を求める．その後，BBS の E_{pub} 内の $h(m)$ を取得し，2 つの値の検証を行う．値が同じだった場合は BBS に掲載された後も，m は変更されていなかったことを示す．もし，値が異なっていた場合，BBS に掲載された後に m が変更されたことを示すため，その担当者が改ざんした可能性があることを示す．

3. システム図

第 2 節で定義した提案方法を用いてシステム構成を定義する．システムとしてエビデンスの管理方法と文書の検証方法を定義する．

3.1 エビデンスの管理方法

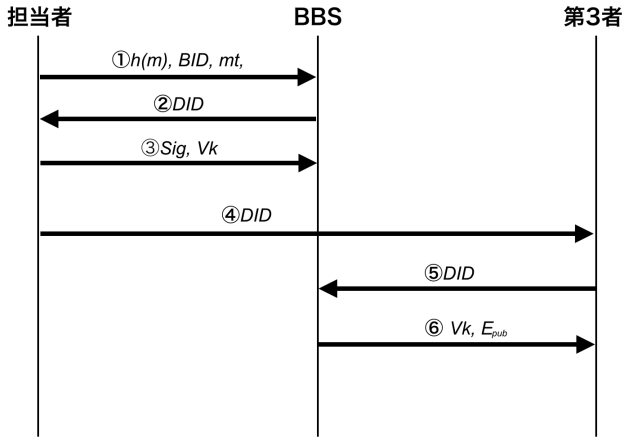

図 1 管理方法

(1) 担当者は m を作成した後に，BBS に $h(m), BID, mt$ を送る．
(2) BBS 内で E_{pub} が作成され，DID を担当者に送る．
(3) 担当者は Sig, Vk を BBS に送る．Sig の検証を行い，正しければ E_{pub} に格納する．
(4) 担当者は DID を第 3 者に公開する．
(5) 第 3 者は DID を用いて BBS 内の E_{pub} と Vk を要求する．
(6) 取得した E_{pub} 内の Sig を検証する．

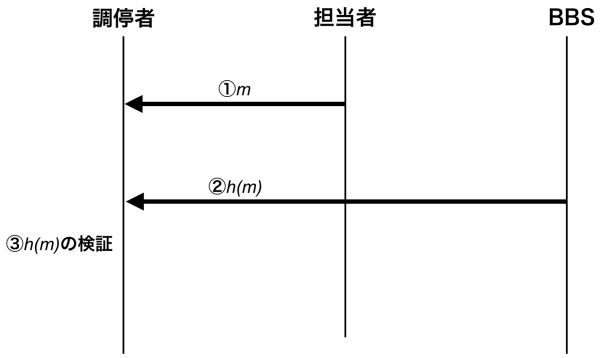

図 2 検証方法

3.2 文書の検証方法

(1) 調停者は不正の疑いがある担当者から m を取得し，m のハッシュ値を求める．
(2) 公開されている E_{pub} から，$h(m)$ を取得する．
(3) 調停者は，$h(m)$ の検証を行う．
(4) 調停者は開示請求を受けた文書の必要部分 m' を第 3 者に公開する．

3.3 文書の開示請求

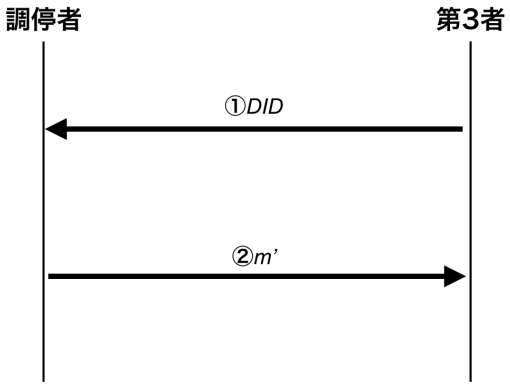

図 3 検証方法

(1) 第 3 者は DID を用いて調停者に開示請求を行う．
(2) 調停者は開示請求を受けた文書の必要部分 m' を第 3 者に公開する．

4. 考察

4.1 必要データのみを復号

本稿では，エビデンスとハッシュ値を用いた文書の検証方法を提案した．文書のハッシュ値を検証することで文書が改ざんされたか明らかになる．ここで，第 3 者が調停者に検証した文書を開示請求する場合がある．この段階では文書は作成途中であり，機密情報が漏洩する恐れがあるため，必要な情報のみ公開することが妥当である．しかし，この判断は調停者では不十分である．

このことから，担当者が調停者に文書を送る前に判断す

る必要がある．担当者は文書を暗号化し，調停者が復号する時，必要データのみを閲覧可能にする．必要データ以外は復号不可にすればいい．

本稿では，CBC モード [4], [5] と CMAC[4] による必要データのみを復号を一考察として提案する．

4.1.1 CBC モードによる暗号化

暗号ブロック連鎖 (CBC) モードでは，各平文は一つ前の暗号文ブロックとの XOR をとってから暗号化される．ただし，最初のブロックにはフィードバックするデータがないため，初期値 (IV) を設定する．図 4 で CBC モードを用いた文書の暗号化を示す．

- 文書; m
- 初期値; IV=c_0
- 暗号文; $c_i = E_k(m_i \oplus c_{i-1})$

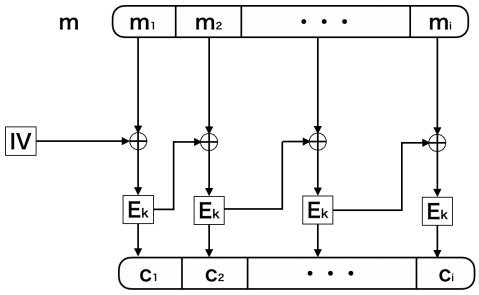

図 4　CBC モードによる暗号化

担当者は m を i ビット長に分割し，暗号化を行う．分割したデータごとに暗号文が生成されるため，一部データを閲覧不可能にすることができる．閲覧不可能にしたい平文に該当する暗号文を調停者に提供しなければ復号することはできない．

4.1.2 CBC モードによる復号

CBC モードによる復号の際は，暗号化の逆の手順を踏む．最初の暗号文ブロックは普通に復号され，その結果はフィードバックレジスタに格納される．次のブロックが復号された後に，その結果はフィードバックレジスタの内容と XOR される．図 5 で CBC モードを用いた文書の復号を示す．

- 暗号文; c
- 共通鍵による暗号化; Ek
- 初期値; IV
- 文書; $m_i = c_{i-1} \oplus D_k(c_i)$

調停者が復号する際，担当者から受け取った c を使用する．ここで閲覧不可能にする場合，調停者は一部の暗号文を担当者から受け取っていないことになる．m_1 のデータを閲覧不可能にする場合，c_1 が所持していないことになる．その結果，m_2 を復号する際は c_2 の他に c_1 が必要なので m_2 も閲覧不可能になる．しかし，m_3 からは復号するデータ

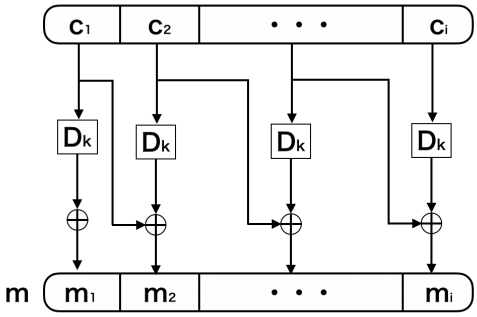

図 5　CBC モードによる復号

がそれっているので，閲覧は可能である．このことから，自己同期化があるといえる．

4.1.3 CMAC による認証子

CMAC は暗号化モードである CBC モードをベースにして作られたメッセージ認証コードである CBC-MAC の改良版です．CMAC では鍵が一つですみ，メッセージ長はブロック長 n の整数倍である必要がなく，任意長のメッセージを扱うことができる．CMAC は文書を分割して暗号化する際，途中の暗号文は出力しない．最後の文書を暗号化し，その出力を認証子とする．

- 暗号文; c
- 共通鍵による復号; Dk
- 初期値; IV
- 文書; m
- L=$E_k(0^n)$
- 認証子; $Tag = E_k(c_{i-1} \oplus m_i \oplus (L \cdot u))$

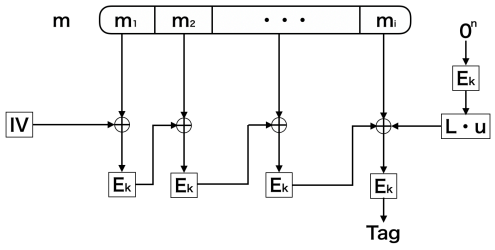

図 6　CMAC に認証子の付与

本稿では，CBC モード暗号を使用した上で最後の暗号文 c_n に CMAC で Tag をつける．調停者は共通鍵を用いて Tag の検証を行う．Tag の値が正しい場合，暗号文の復号を行う．

5. まとめ

本稿で，改ざん困難な文書管理方法を提案した．文書 ID を用いた署名方式により担当者のなりすましを防ぎ，エビデンスの公開により文書の改ざん対策になることを示した．また，必要データのみの文書開示機能も一考察として提案した．これらの機能を用いることで改ざん困難な文書

管理方法を実現した.

参考文献

[1] 安藤武,”「森友」問題、政局より真相解明を”, 日経ビジネス 2018 年 4 月
[2] 武田安恵, ”かんぽ、社内に不適切販売の温床”, 日経ビジネス 2019 年 7 月
[3] 内閣官房, ”内閣官房行政文書管理規則” 2018 年 4 月
[4] IPUSIRON,”暗号技術のすべて”, 翔泳社 2017 年 9 月
[5] ブルース・シュナイアー, ”暗号技術大全” , 厚徳社,2005 年 2 月