購入者-販売者電子透かしプロトコルへの仲介者の導入

窪田 峻† 満保 雅浩†† 岡本 栄司†††

† 株式会社ラック
102-0093 東京都千代田区
平河町 2-16-1
平河町森タワー
shun.kubota@lac.co.jp

†† 金沢大学理工研究域
920-1192 石川県金沢市
角間町

††† 筑波大学システム情報系
305-8573 茨城県つくば市
天王台 1-1-1
okamoto@risk.tsukuba.ac.jp

あらまし 購入者-販売者電子透かしプロトコルは，コンテンツホルダである販売者と購入者の直接取引において，双方の権利を保護する技術である．しかし，現実のデジタルコンテンツビジネスでは，購入者と販売者の間にコンテンツホルダではない機関が存在する．本論文では，購入者と販売者の中間に仲介者が存在する購入者-仲介者-販売者電子透かしプロトコルを提案し，従来プロトコルと同程度の安全性を維持しながら，購入者負担の少ない匿名性を達成することを示す．

Incorporating Middleman into Buyer-Seller Watermarking Protocol

Shun Kubota† Masahiro Mambo†† Eiji Okamoto†††

†LAC Co., Ltd. 2-16-1 Hirakawa-cho, Chiyoda-ku, Tokyo, 102-0093, JAPAN
††Institute of Science and Engineering, Kanazawa University
Kakuma-cho, Kanazawa-shi, Ishikawa, 920-1192, JAPAN
†††Institute of Information Sciences and Electronics, University of Tsukuba
1-1-1, Ten-nodai, Tsukuba-shi, Ibaraki, 305-8573, JAPAN

Abstract Buyer-Seller Watermarking Protocol can protect not only the seller's rights but also the buyer's rights in direct transaction. In actual digital contents business, there exist third parties between the buyer and the seller, and transactions are often made indirectly. In this paper, we propose a new protocol called Buyer-Middleman-Seller Watermarking Protocol, which incorporates middleman between buyer and seller. Our protocol can achieve high security level similar to the existing protocols and buyer's anonymity with lower computational cost for buyers.

1 はじめに

通信技術や情報処理技術の進展により，デジタルコンテンツの複製や配布が容易になった．一方で，静止画像や動画，音楽などのコンテンツを不正に複製し，配布する著作権侵害行為が大きな社会問題となっており，著作権を電子的に保護するための技術が必要とされている．

電子透かし方式は，コンテンツに対して透かしと呼ばれるデータを埋め込み，主に不正者の特定に利用する技術である．しかしながら，販売者が購入者に配布した透かし入りコンテンツと同じものを所有しているため，販売者が自分でコピーコンテンツの配布を行い，購入者を不当に告訴することが可能である．Memon-Wong のプロトコル [6] に代表される購入者-販売者電子透かしプロトコルは，電子透かしの埋め込み

処理を含む購入の手続きを規定し，流出した著作権侵害コンテンツの責任の所在を明確にする．これまでに，販売者が購入者の個人情報を得られない匿名化方式 [5] などが提案されているが，対象となるビジネスモデルは販売者と購入者の直接取引に限られている．

一方，現実のデジタルコンテンツビジネスでは，購入者と販売者の中間にコンテンツホルダではない機関が存在し，情報を集約している場合がありえる．例えば，日本国内の携帯電話向けコンテンツ市場では，携帯電話通信事業者が購入者情報を管理し，購入者からの料金回収を代行することで，販売者の負担を軽減している [9, 10]．そこで購入者-販売者電子透かしプロトコルにおいても，信頼できる第三者機関を購入者と販売者の中間に置くことで，購入者と販売者の負担を軽減できると考えた．

本論文 [11] では，購入者と販売者の中間に信頼できる仲介者が存在するモデル（仲介者モデル）を導入した，購入者-仲介者-販売者電子透かしプロトコルを提案する．具体的には，既存の購入者負担の少ないプロトコル [8] に仲介者モデルを導入し，購入者-仲介者-販売者電子透かしプロトコルを構成する．そして，既存のさまざまな方式と同程度の高い安全性を維持しながら，購入者負担の少ない匿名性を達成することを示す．

2 予備知識

2.1 電子透かし方式

購入者-販売者電子透かしプロトコルで広く使われている電子透かし方式として，Cox らの拡散スペクトラム電子透かし方式 [3] が存在する．この方式は電子透かしの多重埋め込みが可能であり，また，多くの電子的処理や購入者間の結託攻撃に耐性があることが分かっている．コンテンツ X に対して透かし W を埋め込む演算を以下のように定義する．ここで，$\oslash$ は透かし埋め込みを表す演算子，X^W は透かし入りコンテンツである．

$$X^W = X \oslash W \tag{1}$$

2.2 電子暗号方式

購入者-販売者電子透かしプロトコルで利用されている電子暗号方式として，Paillier 暗号方式 [7] と，カメレオン暗号方式 [1] が存在する．Paillier 暗号方式 [7] は非対称暗号方式のひとつであり，2 つの暗号文に対する演算性質の準同型性をもつ．a と b を平文，$\Gamma_{pk}(\cdot)$ を公開鍵 pk による暗号化関数とする．このとき，平文上の二項演算子 $\circ_M$ と暗号文上の二項演算子 $\bullet_C$ に対して以下の性質が成り立つとき，その暗号方式は準同型性を有すると定義される．

$$\Gamma_{pk}(a \circ_M b) = \Gamma_{pk}(a) \bullet_C \Gamma_{pk}(b) \tag{2}$$

Adelsbach らのカメレオン暗号方式 [1] は，電子透かし方式と組み合わせて使用するものである．この暗号方式は，復号鍵が暗号化鍵とわずかに異なっており，これらの鍵による演算の差分が透かしとして残る性質をもつ．暗号化鍵はマスタテーブル MT，復号鍵はユーザーテーブル UT，差分はフィンガープリントテーブル FT と呼ばれる．マスタテーブル MT はランダムな実数ベクトルであり，フィンガープリントテーブル FT は利用する電子透かし方式に応じて計算される実数ベクトルである．

カメレオン暗号方式は，4 つのサブプロトコルから構成される．それらは，準備フェーズ，暗号化フェーズ，復号フェーズ，特定フェーズである．本論文では処理の入出力のみを示し，具体的な処理内容は Poh-Martion の文献 [8] に基づくものとする．

準備フェーズ　鍵生成と透かし生成を行うフェーズである．入力は，コンテンツのメタ情報 INF_X とユーザー数 N である．出力は，1 個のマスタテーブル MT とそれに対応する N 個のユーザーテーブル $UT^{(1)}, ..., UT^{(N)}$，N 個の透かし $W^{(1)}, ..., W^{(N)}$ である．

暗号化フェーズ　コンテンツの暗号化を行うフェーズである．入力は，コンテンツ X，マスタテーブル MT，セッションキー K_r である．出力は，暗号化コンテンツ $\Upsilon_{MT,K_r}(X)$ である．

復号フェーズ　コンテンツの復号を行うフェーズである．入力は，暗号化コンテンツ $\Upsilon_{MT,K_r}(X)$，

ユーザーテーブル $UT^{(i)}$，セッションキー K_r である．出力は，透かし入りコンテンツ $X^{W^{(i)}}$ である．

特定フェーズ　準備フェーズで生成した透かしとコピーコンテンツから抽出した透かしを照合するフェーズである．入力は，透かし $W^{(1)}$, ..., $W^{(N)}$ と透かし $\hat{W}^{(i)}$ $(1 \leq i \leq N)$ である．出力は，値 b $(0 \leq i \leq N)$ である．ここで，$W^{(1)}, ..., W^{(N)}$ は準備フェーズで生成した透かしである．また，$\hat{W}^{(i)}$ は，透かし入りコンテンツ $X^{W^{(i)}}$ のコピーコンテンツ $\hat{X}^{W^{(i)}}$ から抽出した透かしである．b は値が $1 \leq i \leq N$ のとき，$\hat{W}^{(b)}$ を $W^{(b)}$ と特定成功，値が 0 のとき特定失敗を表す．

2.3　購入者-販売者電子透かしプロトコル

2.3.1　プロトコルの参加者

購入者-販売者電子透かしプロトコルには，主に 5 種類の参加者が存在する．

購入者　デジタルコンテンツを購入する．

販売者　デジタルコンテンツの所有者（コンテンツホルダ）であり，コンテンツを販売する．

認証局　公開鍵暗号基盤 (PKI) に基づき，公開鍵を証明する．プロトコルによっては購入者情報の管理機能や，鍵生成機能を持つこともある．

透かし認証局　透かしの生成と認証を行なう．

調停者　告訴を調停する．

ここで，認証局，透かし認証局，調停者はそれぞれ信頼できる第三者機関であると仮定する．

2.3.2　プロトコルの構成

購入者-販売者電子透かしプロトコルは，主に 4 つのサブプロトコルから構成される．

準備プロトコル　購入者と販売者が取引の準備を行う．たとえば，購入者と販売者がそれぞれ公開鍵-秘密鍵の組を生成し，認証局に各自の公開鍵を登録する処理が含まれる．

透かし埋め込みプロトコル　購入者と販売者が通信を行い，コンテンツの注文から透かし入りコンテンツの受領までの処理を行う．このプロトコルには透かしの埋め込み処理が存在し，また，多くの場合，透かしの生成処理も含まれる．

特定プロトコル　販売者が自身の著作権侵害コンテンツを発見したときに，告訴の証拠を準備する．このプロトコルには透かしの抽出処理が含まれる．

告訴プロトコル　調停者が販売者による購入者の特定を検証し，購入者が有罪であるか無罪であるか判断する．

2.3.3　安全性要求

購入者-販売者電子透かしプロトコルが満たさなければならない安全性（基本性質）として，以下の 3 つを定義する．

追跡可能性　正当な販売者は，透かし入りコンテンツからコンテンツの不正な複製・配布を行った購入者を正確に追跡・特定できる．

購入者安全性　正当な購入者は，悪意ある販売者や他の購入者から著作権侵害の罪を着せられることはない．

販売者安全性　コンテンツの不正な複製・配布を行った購入者は，自身の著作権侵害を否定することができない．

さらに，プロトコルをより安全なものにする性質として，以下の 4 つの安全性（追加性質）を定義する．

匿名性　購入者は販売者に対して匿名でコンテンツを購入できる．この性質は購入者がコンテンツの不正な複製・配布を行い，告訴プロトコルで個人情報が明らかにされるまで保たれる．また，異なる 2 つの透かし入りコンテンツが与えられたとき，同じ購入者がそれらを購入したか誰も判別することができない性質も含む．

参加者間結託問題の解決　悪意ある購入者が第三者機関と結託を行っても，販売者安全性を破ることができない．なおかつ，悪意ある販売者が第三者機関と結託を行っても，購入者安全性を破ることができない．

告訴問題の解決　告訴プロトコルにおいて，購入者が自身の個人情報や秘密鍵を明かす必要はない．

非束縛問題の解決　販売者が著作権侵害コンテンツから透かしを抽出した後，別の高価なコンテンツに埋め直して告訴を行ったとしても，埋め直したコンテンツに対する告訴は成立しない．

2.3.4　従来プロトコル

Memon-Wong のプロトコル [6] は，安全性の基本性質を満たす購入者-販売者電子透かしプロトコルとして，最初に広く知られるようになったものである．このプロトコルは，Paillier 暗号方式 [7] の準同型性を戦略として用いる．まず，購入者は自身の公開鍵を透かし認証局に送信し，自身の公開鍵で暗号化された透かしを発行してもらう．次に，購入者は暗号化された透かしと自分の公開鍵を販売者に送信する．そして，販売者は購入者の公開鍵でコンテンツを暗号化し，暗号文上で透かしの埋め込みを行って購入者に返す．これにより，購入者だけが自身の秘密鍵で復号を行い，目的の透かし入りコンテンツを得ることができる．

Memon-Wong のプロトコル [6] 以降も，さまざまな購入者-販売者電子透かしプロトコルが提案されてきた．Lei らのプロトコル [5] は，匿名性を満たす購入者-販売者電子透かしプロトコルとして，最初に広く知られるようになったものである．Deng-Preneel のプロトコル [4] は，参加者間結託問題の解決を達成する安全性の高いプロトコルとしてよく知られている．Poh-Martin のプロトコル [8] は，計算量の高い準同型暗号方式を使わないプロトコルとしてよく知られている．本論文では各プロトコルの詳細を割愛するが，いずれも購入者と販売者が直接取引するビジネスモデルを対象としたものである．

2.4　デジタルコンテンツビジネス

図 1 は，財団法人デジタルコンテンツ協会の示した電子書籍におけるビジネスモデル [12] を表している．このビジネスモデルは，権利者，ユーザーの 2 人の参加者と，マーケットプレイス，決済プラットフォームの 2 種類のプラットフォームで構成される．マーケットプレイスは，権利者の保有するコンテンツを一か所に収集し，

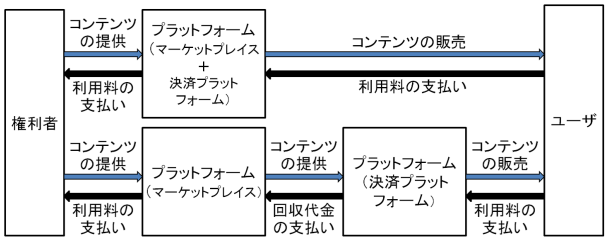

図 1: 電子書籍のビジネスモデル

ユーザーに提供するものである．また，決済プラットフォームは，権利者に代わってユーザーからコンテンツ利用料を徴収するものである．電子書籍におけるビジネスモデルでは，マーケットと決済の両方の機能がひとつのプラットフォームにまとめられる場合と，それぞれが独立したプラットフォームで存在する場合が存在する．

ここで，消費者は購入者に，また，権利者とマーケットプレイスは販売者に置き換えることができる．すなわち，マーケットと決済の両方の機能をひとつのプラットフォームにまとめるビジネスモデルは，従来の購入者-販売者電子透かしプロトコルのように，購入者と販売者が直接取引を行うものである．しかし，マーケットプラットフォームと決済プラットフォームが独立して存在するビジネスモデルでは，決済プラットフォームがコンテンツホルダではないために，従来プロトコルとは異なる手続きを考える必要がある．

マーケットプラットフォームと決済プラットフォームが独立して存在するビジネスモデルの例として，国内の携帯電話通信事業者が提供する料金回収代行サービス [9, 10] が存在する．このサービスは，購入者から携帯電話の月額料金とともにコンテンツの利用料を回収し，利用料を販売者に支払うものである．このとき，料金回収を行う携帯電話通信事業者はコンテンツホルダではないため，独立した決済プラットフォームの役割を果たす．したがって，携帯電話通信事業者の料金回収代行サービスはコンテンツの形式にかかわらず，マーケットプラットフォームと決済プラットフォームが独立して存在するビジネスモデルに当てはまると考えられる．

3 仲介者モデルとその導入手法

3.1 仲介者モデルの定義

マーケットプラットフォームと決済プラットフォームが独立して存在するビジネスモデルとして，仲介者モデルを定義する．仲介者は購入者と販売者の中間に存在し，デジタルコンテンツの売買の仲介を行う参加者である．また，仲介者はコンテンツの商品情報やメタデータを保有するが，元コンテンツを保有しないとする．仲介者モデルにおける購入手続きは以下の手順で実行される．

(1) 購入者は，仲介者に対してコンテンツを注文する．
(2) 仲介者は，購入者の注文を処理と販売者へのコンテンツ発注を行う．
(3) 販売者は，仲介者の提供する通信経路を用いる方法，または仲介者を中継する方法で購入者にコンテンツを送信する．
(4) 購入者は，仲介者に対してコンテンツの利用料を支払う．
(5) 仲介者は，販売者に購入者から回収した利用料を支払う．

3.2 プロトコル概要

本論文では，Poh-Martin の購入者-販売者電子透かしプロトコル [8] に仲介者モデルを導入し，購入者-仲介者-販売者電子透かしプロトコルを構成する．具体的には，透かしの埋め込みとコンテンツの暗号化にカメレオン暗号方式を用い，販売者の負担を軽減する．そして，公開鍵の証明と透かしの生成を仲介者が行い，Poh-Martin のプロトコルでは達成されていなかった匿名性を，購入者の負担を抑えて実現する．

提案する購入者-仲介者-販売者電子透かしプロトコルの参加者は 4 人であり，それらは購入者 B，販売者 S，仲介者 M，調停者 A である．各参加者は電子署名鍵 sk_i と検証鍵 pk_i（i は参加者のイニシャル）を所持しているとする．また，仲介者 M と調停者 A は信頼できる第三者機関であることを仮定する．

3.3 プロトコル詳細

3.3.1 準備プロトコル

購入者は以下の手順で取引準備を行う．

(1) 購入者 B は，電子署名 $S_{B1} = \mathrm{Sign}_{sk_B}(pk_B, \mathrm{ID}_B)$ を生成し，pk_B，ID_B, S_{B1} を仲介者 M に送信する．
(2) 仲介者 M は，電子署名 S_{B1} の正当性を検証する．正当であれば，電子証明 $Cert_M(pk_B)$ を生成し，購入者 B に送信する．その後，pk_B，ID_B，S_{B1} を購入者データベースに登録する．

販売者は以下の手順で取引準備を行う．

(1) 販売者 S は公開鍵暗号方式の鍵の組（pk^*, sk^*）を生成する．そして，電子署名 $S_{S1} = \mathrm{Sign}_{sk_S}(\mathrm{ID}_S, \mathrm{INF}_X, pk^*, pk_s)$ を生成し，ID_S，INF_X，pk^*，pk_s，S_{S1} を仲介者 M に送信する．
(2) 仲介者 M は，電子署名 S_{S1} の正当性を検証する．正当であれば，コンテンツのメタ情報 INF_X と事前に設定した購入者数 N を入力として，カメレオン暗号方式の準備フェーズを実行する．次に，電子署名 $S_{M1} = \mathrm{Sign}_{sk_M}(MT)$ と電子証明 $\mathrm{Cert}_M(pk^*, pk_S)$ を生成する．そして，MT，S_{M1}，$\mathrm{Cert}_M(pk^*, pk_S)$ を販売者 S に送信する．最後に，ID_S，INF_X，pk^*，pk_s，S_{S1} を販売者データベースに登録する．
(3) 販売者 S は，電子署名 S_{M1} の正当性を検証する．正当であれば，証明された検証鍵 pk_S，公開鍵 pk^* を購入者が利用できるようにする．

3.3.2 透かし埋め込みプロトコル

透かし埋め込みプロトコルは以下の手順で進められる．本論文では，販売者が仲介者を中継する方法で購入者にコンテンツを送信する場合を示す．処理を図示したものを，図 2 に示す．

(1) 購入者 B は，仲介者 M に対してコンテンツ X の注文をリクエストする．

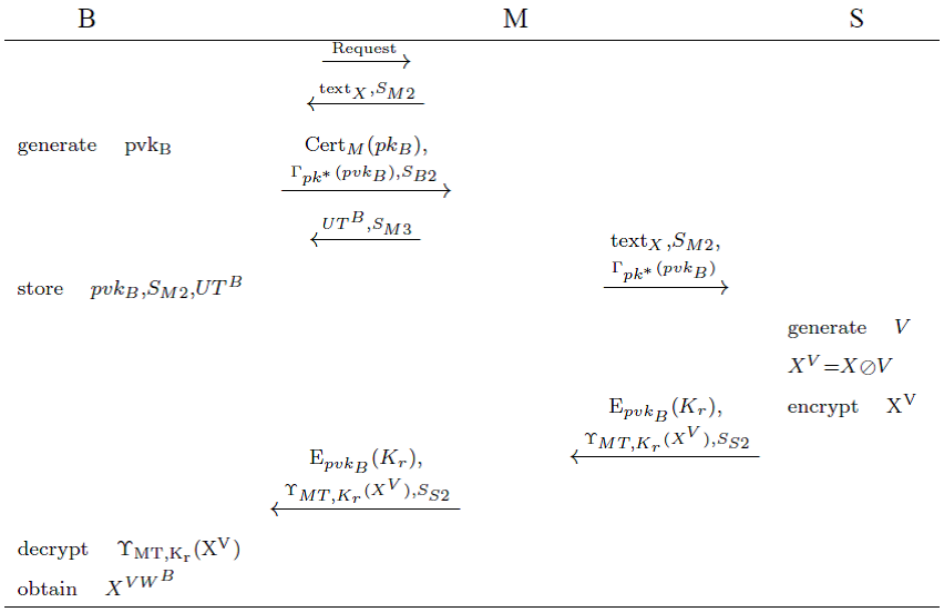

図 2: 透かし埋め込みプロトコル

(2) 仲介者 M は，コンテンツ X の注文同意書 text_X と電子署名 $S_{M2} = \text{Sign}_{sk_M}(\text{text}_X)$ を生成する．そして，text_X，S_{M2} を購入者 B に送信する．

(3) 購入者 B は，電子署名 S_{M2} の正当性を検証する．正当であれば，ランダムに正当な共通鍵 pvk_B を生成する．続いて，販売者の公開鍵 pk^* を得て，暗号文 $\Gamma_{pk^*}(pvk_B)$ と電子署名 $S_{B2} = \text{Sign}_{sk_B}(\text{text}_X, \Gamma_{pk^*}(pvk_B))$ を生成する．そして，$\text{Cert}_M(pk_B)$，$\Gamma_{pk^*}(pvk_B)$，S_{B2} を仲介者 M に送信する．

(4) 仲介者 M は，電子署名 S_{B2} の正当性を検証する．正当であれば，電子署名 $S_{M3} = \text{Sign}_{sk_M}(UT^B)$ $(1 \leq B \leq N)$ を生成する．そして，UT^B，S_{M3} を購入者 B に送信する．

(5) 購入者 B は，電子署名 S_{M3} の正当性を検証する．正当であれば，pvk_B，S_{M2}，UT^B を一時的に記憶する．

(6) 仲介者 M は，text_X，S_{M2}，$\Gamma_{pk^*}(pvk_B)$ を販売者 S に送信する．そして，ID_B，text_X，S_{B2}, W^B $(1 \leq B \leq N)$ を課金データベースに登録する．

(7) 販売者 S は，電子署名 S_{M2} の正当性を検証する．正当であれば，暗号文 $\Gamma_{pk^*}(pvk_B)$ を復号し，共通鍵 pvk_B を得る．次に，検証用透かし V を生成し，これをコンテンツ X に埋め込み，X^V を得る．続いて，疑似乱数生成器を用いてセッションキー K_r を生成し，カメレオン暗号方式の暗号化フェーズにより暗号文 $\Upsilon_{MT,K_r}(X^V)$ を得る．さらに，暗号文 $\text{E}_{pvk_B}(K_r)$，電子署名 $S_{S2} = \text{Sign}_{sk_S}(\text{E}_{pvk_B}(K_r), \Upsilon_{MT,K_r}(X^V), S_{M2})$ を生成する．そして，$\text{E}_{pvk_B}(K_r)$，$\Upsilon_{MT,K_r}(X^V)$，S_{S2} を仲介者 M に送信する．最後に，V，K_r，text_X，S_{M2}，S_{S2} を取引データベースに登録する．

(8) 仲介者 M は，$\text{E}_{pvk_B}(K_r)$，$\Upsilon_{MT,K_r}(X^V)$，S_{S2} を購入者 B に送信する．

(9) 購入者 B は，電子署名 S_{S2} の正当性を検証する．次に，暗号文 $\text{E}_{pvk_B}(K_r)$ を復号し，疑似乱数 K_r を得る．そして，カメレオン暗号方式の復号フェーズを実行し，透かし入りコンテンツ X^{VW^B} を得る．

3.3.3 特定プロトコル

販売者 S は，コンテンツ X のコピーコンテンツ X' を発見したとする．まず，販売者 S は X' から検索用透かしを抽出する．このとき抽出された検索用透かしを V' とする．次に，取引データベースを検索し，V' と最も類似度の高い透かし V をもつ取引を見つける．そして，

X^V と $\Upsilon_{MT,K_r}(X^V)$ を計算する．最後に，X'，X^V，$\Upsilon_{MT,K_r}(X^V)$，K_r，text_X，S_{M2} を調停者 A に送信し，告訴を行う．

3.3.4 告訴プロトコル

特定プロトコルに続いて，調停者 A は以下の処理を行う．

(1) 調停者 A は電子署名 S_{M2}，S_{S2} の正当性を検証する．正当であれば，コンテンツ X' から追跡用透かしを抽出する．ここで，抽出された透かしを W' とする．続いて，仲介者 M に W' を送信し，カメレオン暗号方式の特定フェーズの実行を要求する．

(2) 仲介者 M は特定フェーズを実行する．特定に成功した場合，出力値に対応する W^B を持つ ID_B と S_{B2} を調停者 A に返す．

(3) 調停者 A は電子署名 S_{B2} の正当性を検証する．正当であれば，ID_B をもつ購入者がコンテンツ X' の出所であると判断し，これを罪に問う．

4 提案プロトコルの評価

4.1 提案プロトコルの安全性

購入者-仲介者-販売者電子透かしプロトコルと従来の購入者-販売者電子透かしプロトコルの安全性を比較した結果を表 1 に示す．チェックのある項目は，その性質が達成されていることを表す．提案プロトコルは販売者が購入者に関して得られる情報が，ランダムに生成された共通鍵 pvk_B だけであるため，匿名性を満たす．また，告訴プロトコルにおいて購入者の参加を必要としないため，告訴問題の解決を達成する．さらに，電子署名 S_{M2}，S_{S2} がコンテンツ X と取引を束縛しているため，非束縛問題の解決を達成する．しかし，購入者安全性と販売者安全性が仲介者の信頼性に依存するため，参加者間結託問題を解決していない．したがって，すべての性質を満たす Deng-Preneel のプロトコル [4] には及ばないが，他のプロトコルと同等かそれ以上の安全性を達成することができる．

表 1: 安全性の比較評価

	[6]	[5]	[4]	[8]	提案方式
基本性質	√	√	√	√	√
匿名性		√	√		√
参加者間結託問題の解決			√		
告訴問題の解決		√	√	√	√
非束縛問題の解決		√	√	√	√

表 2: 購入者負担

	匿名性	公開鍵再証明	再生成アイテム
[6]	なし	不要	不要
[5]	あり	必要	公開暗号方式鍵，電子署名方式鍵
[4]	あり	不要	公開暗号方式鍵，透かし
[8]	なし	不要	不要
提案方式	あり	不要	共通鍵

4.2 提案プロトコルの効率

4.2.1 購入者負担

取引後に購入者が別のコンテンツを購入するとき、匿名性を保つために発生する購入者の負担を表 2 に示す．提案プロトコルは，取引ごとに購入者が第三者機関に公開鍵の証明を受ける必要がない．また，取引ごとに購入者が再生成しなければならないアイテムはひとつの共通暗号鍵のみである．したがって，提案プロトコルは購入者の匿名性を達成するための負担が最も少ない．

4.2.2 販売者負担

販売者負担を評価する基準として，コンテンツの暗号化計算量や暗号化コンテンツのサイズに着目する．これらの評価結果を表 3 に示す．ここで，n はコンテンツサイズ，m は公開鍵暗号方式で使用する素数積，Z はカメレオン暗号方式で使用する拡大パラメータを表す．カメレオン暗号方式の計算量，暗号文サイズの計算結果は Poh-Martin の文献 [8] に基づくものである．

Poh-Martin は，各係数が 16 ビットの長さを持つ 10000 要素（$n = 10000$）のコンテンツに対して，十分な品質を保つことのできる値として $|Z| = 16$，$|m| = 1024$ を与えている．この

表 3: コンテンツ暗号化方法とその負担量

	[6, 5, 4]	[8], 提案方式
暗号化方式	Paillier 暗号方式 [7]	カメレオン 暗号方式 [1]
暗号化計算量	$O(\|n\|\|m\|^2)$	$O(\|n\|\|Z\|)$
暗号文サイズ	$n \cdot \|m\|$	$n \cdot \|Z\|$

条件下では，Paillier 暗号方式 [7] を用いた場合，$n \cdot |m| = 10000 \cdot 1024$ ビット，すなわち約 1.3 メガバイトとなる．一方，カメレオン暗号方式 [1] を用いた場合，$n \cdot |Z| = 10000 \cdot 16$ ビット，すなわち約 20 キロバイトとなる．したがって，提案プロトコルならびに Poh-Martin のプロトコル [8] は，Paillier 暗号方式を利用するプロトコル [6, 5, 4] よりも，コンテンツの暗号化と暗号化コンテンツの転送にかかる負担を小さくすることができる．

5 結論

本論文では，購入者-販売者電子透かしプロトコルに対して，購入者と販売者の間に仲介者を取り入れたモデルを導入した．具体的には，Poh-Martin のプロトコル [8] の戦略に仲介者モデルを導入して購入者-仲介者-販売者電子透かしプロトコルを構成した．そして，この提案プロトコルが従来プロトコルと同程度の安全性を達成することを示し，効率における提案プロトコルの優位性を述べた．提案プロトコルは購入者の負担が少ないという Poh-Martin のプロトコルの優位性を保ちつつ，Poh-Martin のプロトコルが満たしていない匿名性を満たすという利点も有する．

今後の課題として，理想機能・現実機能パラダイム [2] による安全性の証明，購入者が携帯電話端末を用いる環境を想定した実装が挙げられる．

参考文献

[1] A. Adelsbach, U. Huber, and A.-R. Sadeghi, “Fingercasting–Joint Fingerprinting and Decryption of Broadcast Messages,” ACISP’06, LNCS, vol. 4058, pp. 136–147, 2006.

[2] R. Canetti, “Universally composable security: A new paradigm for cryptographic protocols,” FOCS ’01, pp. 136–145, 2001.

[3] I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, “Secure spread spectrum watermarking for multimedia,” IEEE Transactions on Image Processing, vol. 6, no. 12, pp. 1673–1687, 1997.

[4] M. Deng and B. Preneel, “Attacks On Two Buyer-Seller Watermarking Protocols And An Improvement For Revocable Anonymity,” ISECS ’08, pp. 923–929, 2008.

[5] C.-L. Lei, P.-L. Yu, P.-L. Tsai, and M.-H. Chan, “An efficient and anonymous buyer-seller watermarking protocol,” IEEE Transactions on Image Processing, vol. 13, no. 12, pp. 1618–1626, 2004.

[6] N. Memon and P. W. Wong, “A buyer-seller watermarking protocol,” IEEE Transactions on Image Processing, vol. 10, no. 4, pp. 643–649, 2001.

[7] P. Paillier, “Public-Key Cryptosystems Based on Composite Degree Residuosity Classes,” EUROCRYPT ’99, LNCS, vol. 1592, pp. 223–238, 1999.

[8] G. S. Poh and K. M. Martin, “An Efficient Buyer-Seller Watermarking Protocol Based on Chameleon Encryption,” IWDW ’08,LNCS, vol. 5450, pp. 433–447, 2009.

[9] KDDI 株式会社, “ＫＤＤＩが提供するプラットフォームタイプサービス,” ユビキタスネット社会におけるプラットフォーム機能のあり方に関する研究会, 総務省, 2005.

[10] 株式会社 NTT ドコモ, “i モード情報料回収代行サービスについて,” 決済に関するワーキング・グループ（第 5 回）, 金融審議会金融分科会第二部会, 2008.

[11] 窪田 峻 “購入者-販売者電子透かしプロトコルへの仲介者の導入効果に関する研究,” 筑波大学大学院システム情報工学研究科平成 23 年度修士論文, 2012.

[12] 財団法人デジタルコンテンツ協会, “デジタルコンテンツの市場環境変化に関する調査研究報告書,” 平成 22 年度デジタルコンテンツの保護・活用に関する調査研究等補助事業, 2011.

表記	
ID_*	識別子
$text_*$	購入同意書
INF_*	商品情報ならびにメタデータ
(pk_*, sk_*)	公開鍵と秘密鍵の対
pvk_*	共通鍵
$\mathrm{Sign}_{sk_*}(\cdot)$	電子署名
$\mathrm{Cert}_*(\cdot)$	電子証明書
$\mathrm{E}_{pvk_*}(\cdot)$	共通鍵暗号方式の暗号化
$\Gamma_{pk_*}(\cdot)$	公開鍵暗号方式の暗号化
$\Upsilon_{MT,K_r}(\cdot)$	カメレオン暗号方式の暗号化