Vol.2017-DPS-170 No.6
Vol.2017-CSEC-76 No.6
2017/3/2

Man In The Browser 攻撃対策を実現する 人間・銀行サーバ間のセキュア通信プロトコル（その 2）

土屋貴史[†1]　神農泰圭[†1]　藤田真浩[†2]
高橋健太[†3]　尾形わかは[†4]　西垣正勝[†2]

概要 : Man In The Browser 攻撃（MITB 攻撃）は，ブラウザのマルウェア感染が原因であるため，SSL のような機械（ブラウザ）と機械（銀行サーバ）間のセキュア通信では対策不可能である．著者らは CSEC69 において，人間・銀行サーバ間でセキュア通信を実現するチャレンジ&レスポンス方式のプロトコルを提案し，CAPTCHA を応用することでプロトコルが実現可能であることを示した．本稿では，MITB 攻撃と CAPTCHA を定式化し，提案プロトコルに対する安全性証明を行う．タグベース暗号の安全性をベースに CAPTCHA の安全性を定義した上で，(1,N)-OW-CAPTCHA-CCA を満足する CAPTCHA を用いた提案プロトコルが攻撃モデルに対し安全であることを証明する．

Secure Communications Protocol Between Humans and a Bank Server to Prevent Man In The Browser Attack (part 2)

TAKASHI TSUCHIYA[†1]　YASUYOSHI JINNO[†1]　MASAHIRO FUJITA[†2]
KENTA TAKAHASHI[†3]　WAKAHA OGATA[†4]　MASAKATSU NISHIGAKI[†2]

Abstract: Man-in-the-Browser (MITB) attacks are caused by malware that infects a web browser; hence, conventional secure communication channels between a machine (web browser) and a machine (bank server) such as SSL cannot prevent the attacks. In CSEC69, the authors proposed a challenge and response protocol that achieves secure communication channels between a machine (bank server) and a human (end user).The authors also showed that the protocol is feasible by applying CAPTCHA technology. In this paper, we formulate MITB attacks and CAPTCHA and provide the security proof of the protocol. We define the security for CAPTCHA based on the security for tag-based-encryption and provide the proof that the protocol is safe against information falsification MITB attack if the CAPTCHA has (1,N)-OW-CAPTCHA-CCA security.

1. はじめに

1.1 背景

近年，インターネットバンキングにおける不正送金の被害が急増している[1]．不正送金には種々の攻撃が存在するが，その中でも特に Man In The Browser 攻撃（MITB 攻撃）が注目を集めている．MITB 攻撃は，PC に感染したマルウェアがブラウザの操作を乗っ取ることで，認証情報の盗取や不正送金を行う攻撃である．

現在，多くのインターネットバンキングは，ブラウザと銀行サーバ間でエンド・エンドのセキュア通信（TLS，SSL 通信）を行うことで，不正送金を対策している[2][3]．しかし，MITB 攻撃は「マルウェアが PC（ブラウザ）の操作を乗っ取る」攻撃であるため PC（ブラウザ）・銀行サーバ間のセキュア通信では対策できない．したがって，現状の対策に加えて，MITB 攻撃対策をインターネットバンキングへ導入することが急務となっている．

筆者らは CSEC69 において，人間（ユーザ）とコンピュータ（銀行サーバ）の間に直にセキュア通信チャネルを構築するというアイデアに基づく MITB 攻撃対策の一例として，「マルウェアが盗聴できない通信チャネル」を利用したチャレンジ&レスポンス方式のセキュア通信プロトコルを提案した[4]．提案プロトコルの安全性検討を行い，「マルウェアが盗聴できない通信チャネル」が実現できるのであれば提案プロトコルにおいてユーザ・銀行サーバ間のセキュア通信が可能であることを表層的に示した．また，「マルウェアが盗聴できない通信チャネル」の一実装方法として，人間の持つ高度な認知能力を利用した CAPTCHA を応用することを提案した．CAPTCHA を利用した「マルウェアが盗聴できない通信チャネル」を CAPTCHA チャネルと呼ぶ．

1.2 本論文の貢献

本稿では，CAPTCHA チャネルを用いて提案プロトコルを構成した場合の安全性証明を行う．

まず，CAPTCHA を定式化し，その安全性を定義する．

†1 静岡大学大学院総合科学技術研究科
Graduate School of Integrated Science and Technology, Shizuoka University
†2 静岡大学創造科学技術大学院
Graduate School of Science and Technology, Shizuoka University
†3 株式会社日立製作所研究開発グループセキュリティ研究部
Hitachi, Ltd, R&D Group, Security Research Dept.
†4 東京工業大学工学院
School of Engineering, Tokyo Institute of Technology

次に提案プロトコルに対する安全性を定義し，提案プロトコルの安全性をCAPTCHAの安全性に帰着させることによって証明する．その結果，(1,N)-OW-CAPTCHA-CCA 安全を満足するCAPTCHAチャネルを用いて実装される提案プロトコルは，取引内容改ざん型MITB攻撃に対し安全であることが証明された．

1.3 本論文の構成

1 章では，本研究の背景と貢献について述べた．2 章では，提案プロトコルについて説明する．3 章では，CAPTCHAの定式化と安全性定義を行う．4 章では，提案プロトコルの安全性を定義する．5 章で提案プロトコルの安全性証明を行い，6 章でまとめと今後の課題について述べる．

2. 提案プロトコル

本章ではMITB攻撃と，著者らがCSEC69 で提案したセキュア通信プロトコル[4]について説明する．

2.1 インターネットバンキングの送金プロトコル

本稿で想定するインターネットバンキングにおける送金プロトコルについて述べる．ここでは簡単のため，仕組みを単純化して説明している．

2.1.1 エンティティ

インターネットバンキングにおける送金プロトコルの構成要素（エンティティ）は以下の通りである．

銀行サーバ：インターネットバンキングサービスを提供する金融機関のサーバである．本稿では，銀行サーバは安全性が確保されているものとする（たとえば，サーバ内のデータが漏洩したり，サーバ内の処理が改ざんされたりすることはない）．銀行サーバはコンピュータであるため，高い計算機能力（および記憶能力）を有する．

ユーザ：インターネットバンキングサービスを利用する顧客である．送金処理を実行する際には，金融機関が提供する送金プロトコルに従って PC の操作を行う．ヒューマンエラーは起こさない（想定されていない操作は行わない）ものとする．ユーザは人間であるため，低い計算機能力（および記憶能力）しか有さない．

PC：キーボード，ディスプレイを備えており，インターネットを介して銀行サーバに接続されている．PC にはブラウザがインストールされており，ユーザはブラウザを利用してインターネットバンキングの操作を行う．PC（実際には，ブラウザ）はコンピュータ（実際には，コンピュータ上のソフトウェア）であるため，高い計算機能力（および記憶能力）を有する．

2.2 MITB 攻撃の分類

MITB攻撃は，PC に感染したマルウェアがブラウザの操作を乗っ取ることで，認証情報の盗取や不正送金を行う攻撃である．MITB 攻撃は取引内容改ざん型と ID 盗取型に大別される[5]．取引内容改ざん型MITB攻撃について以下に示す．

2.2.1 取引内容改ざん型 MITB 攻撃

取引内容改ざん型は，ユーザが PC（ブラウザ）に入力した取引情報を，PC に潜むマルウェアが改ざんする攻撃である．一般的な送金プロトコルに対する取引内容改ざん型MITB攻撃の手順（図 1）を以下に示す．

Step 1. ユーザは送金情報Xを PC へ入力する．
Step 2. PC（ブラウザ）に潜むマルウェアは送金情報Xを$X'(\neq X)$ へ改ざんし銀行サーバへ送信する．
Step 3. 銀行サーバは送金内容の確認を行うために，確認情報$Y(=X')$ を PC へ送信する．
Step 4. PC は$Y(=X')$ を受け取る．PC に潜むマルウェアはY を$Y'(=X)$ へ改ざんしたうえでユーザへ表示する．
Step 5. ユーザは$Y'(=X)$ を読み，「Y'が確かに自分の入力した送金情報Xと一致している」ことが確認できた場合に，送金を確定する．Step 4 で$Y(=X')$ が$Y'(=X)$ に改ざんされているため，ユーザは「送金情報は一致している」と判断することに注意されたい．
Step 6. ユーザは，送金確定を指示するために TRUE を PC へ入力する．
Step 7. PC はユーザが入力した TRUE を銀行サーバへ送信する．
Step 8. 銀行サーバは TRUE を受信した時点で，X'に関する送金を実行する．

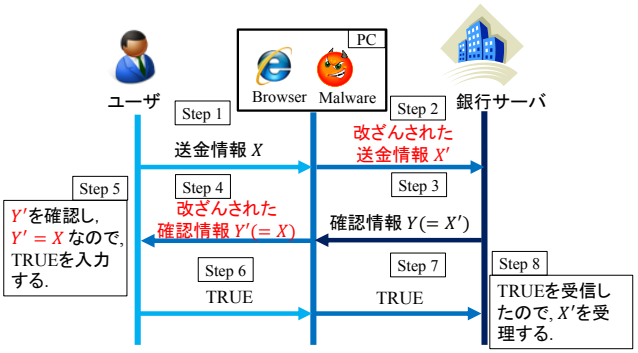

図 1 取引内容改ざん型 MITB 攻撃

2.3 提案プロトコル

著者らがCSEC69 で提案したセキュア通信プロトコル[4]について説明する．

2.3.1 マルウェアが盗聴できない通信チャネル

提案プロトコルでは，「マルウェアが盗聴できない通信チャネル」を利用することを前提とする．この通信チャネルの定義は下記のとおりである．

[定義] サーバからユーザへの通信チャネルが存在し，時

刻 T においてサーバがユーザへそのチャネルを用いてデータ$\alpha_1,\alpha_2,\ldots,\alpha_m$を一度に送信したとする．このときチャネルに流れたデータを$\{\alpha_1,\alpha_2,\ldots,\alpha_m\}_T$と表記した際，

(i) マルウェア（機械）は$\{\alpha_1,\alpha_2,\ldots,\alpha_m\}_T$から$\alpha_i(1\leqq i\leqq n)$を求めることができない．

(ii) マルウェア（機械）は$\alpha_i(1\leqq i\leqq n)$を知っていたとしても，$\{\alpha_1,\alpha_2,\ldots,\alpha_m\}_T$のどの部分が$\alpha_i$を表しているかはわからない．

(iii) ユーザは$\{\alpha_1,\alpha_2,\ldots,\alpha_m\}_T$から任意の$\alpha_i(1\leqq i\leqq n)$を求めることができる．

という条件を満たす時，そのチャネルを「マルウェアが盗聴できない通信チャネル」と呼ぶ．

ここで，上記の定義はマルウェアの読取り能力に関する制約を意味しており，マルウェアも「マルウェアが盗聴できない通信チャネル」を使ってユーザ（人間）に任意のデータを送信すること自体は可能である．すなわち，サーバからユーザに送信されたデータ$\alpha_1,\alpha_2,\ldots,\alpha_m$の値をマルウェアが知ることができた場合には，そのマルウェアは時刻 T’（≠T）において，正しいデータ（$\{\alpha_1,\alpha_2,\ldots,\alpha_m\}_T$），一部を偽の値に改ざんしたデータ（たとえば$\{\beta_1,\alpha_2,\ldots,\alpha_m\}_T$），完全な偽データ（$\{\beta_1,\beta_2,\ldots,\beta_n\}_T$）などを捏造し，ユーザに送信することができる．一方で，定義(ii)より，サーバからユーザに送信された$\{\alpha_1,\alpha_2,\ldots,\alpha_m\}_T$に対しては，マルウェアはその中に含まれるデータを部分的に改ざんすることはできない．すなわち，α_1の値を知っているマルウェアが$\{\alpha_1,\alpha_2,\ldots,\alpha_m\}_T$を入手したとしても，そのマルウェアは$\{\alpha_1,\alpha_2,\ldots,\alpha_m\}_T$を例えば$\{\beta_1,\alpha_2,\ldots,\alpha_m\}_T$に改ざんすることはできない．

2.3.2 提案プロトコルの手順

提案プロトコルの手順を以下に示すとともに図 3 に図示する．Step4 および Step5 で$\{Y,\ R\}_T$と表記されている箇所は「マルウェアが盗聴できない通信チャネル」を用いてYとRが送信されていることを意味する．

Step 1. ユーザは送金情報 X を PC へ入力する．
Step 2. PC はX を銀行サーバへ送信する．
Step 3. 銀行サーバは乱数R を生成し，$\{Y,\ R\}_T$ を生成する．ここで，$Y=X$である．
Step 4. 銀行サーバは$\{Y,\ R\}_T$ を PC へ送信する．
Step 5. PC は$\{Y,\ R\}_T$ を受信し，ユーザに表示する．
Step 6. ユーザは$\{Y,\ R\}_T$ から Y と R を得る．
Step 7. $Y=X$ の場合，ユーザは送金を実行するために$Q=R$ を PC へ入力する．$Y\neq X$の場合，ユーザは送金を中止するために$Q=0$ を PC へ入力する．
Step 8. PC はQ を銀行サーバへ送信する．
Step 9. 銀行サーバはQ を受信する．$Q=R$ のとき，送金を受理する．$Q\neq R$ あるいは$Q=0$ のとき，送金を中止する．

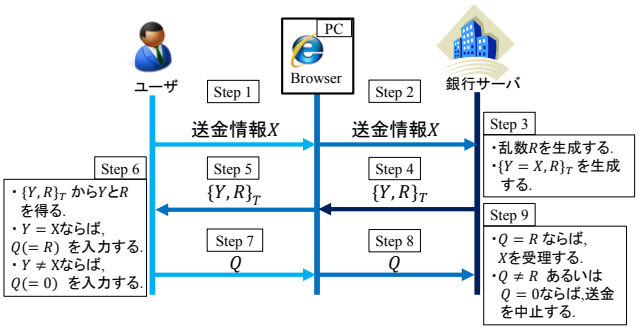

図 2 提案プロトコル

3. CAPTCHA チャネルの定式化

提案プロトコルの実現には「マルウェアが盗聴できない通信チャネル」の実装が必要である．このようなチャネルを実現する一手法として，人間の持つ高度な認知能力に基づく CAPTCHA が利用できると考えられる．CAPTCHA を利用した「マルウェアが盗聴できない通信チャネル」を CAPTCHA チャネルと呼称する．本章では CAPTCHA チャネルを構成し得る CAPTCHA に関する定式化を行う．まず，タグベース暗号の定義と安全性について概説したのち，これをもとに CAPTCHA を定式化し，その安全性を定義する．

3.1 タグベース暗号

本節ではタグベース暗号[6]について概説する．

3.1.1 タグベース暗号アルゴリズム

タグベース暗号は 3 つのアルゴリズム（$TBE.Gen$, $TBE.Enc$, $TBE.Dec$）からなり，$TBE.Gen$は1^k（kはセキュリティパラメータ）を入力とし，秘密鍵sk，公開鍵pkを出力するアルゴリズム，$TBE.Enc$はpk，タグt，平文mを入力として暗号文cを出力するアルゴリズム，$TBE.Dec$はsk, t, cを入力としてmあるいは⊥（復号不可）を出力するアルゴリズムである．

3.1.2 タグベース暗号の安全性定義

タグベース暗号の安全性の定義としては，一方向性，識別不可能性，頑強性がそれぞれ定式化されている．本稿では一方向性のみ説明する．

● タグ選択平文攻撃に対する一方向性（OW-TBE-CPA）

タグ選択平文攻撃とは，攻撃者が任意の平文に対応する暗号文を入手できる条件下で，挑戦者から提示された暗号文（ただし，暗号文のタグは攻撃者が指定できる）の平文を攻撃者が求める攻撃である．

攻撃者Aに対する挑戦者Bを設定し，AとBの間で実行される次のようなゲーム（OW-TBE-CPA ゲーム）を構成する．

1. Bは，$TBE.Gen$に1^kを入力し秘密鍵sk，公開鍵pkのペアを出力し，Aにpkを入力する．
2. Aはチャレンジタグt^*を出力し，Bに渡す．
3. Bは平文mを平文空間から一様に選択し，$c^*\leftarrow$

$TBE.Enc(pk, t^*, m)$ を計算し，c^*をAに返す．

4. Aは$\hat{m}$を出力する．$\hat{m} = m$のときAの勝ちとする．

上記の OW-TBE-CPA ゲームに対する攻撃者Aのアドバンテージを

$$Adv_A^{OW-TBE-CPA}(k) = Pr[\hat{m} = m]$$

と定義し，いかなる多項式時間アルゴリズムAに対しても $Adv_A^{OW-TBE-CPA}(k) < \varepsilon(k)$ が成立するとき，そのタグベース暗号アルゴリズムは OW-TBE-CPA 安全であるという．

- タグ選択暗号文攻撃に対する一方向性（OW-TBE-CCA）

タグ選択暗号文攻撃とは，攻撃者が任意の暗号文（ただし，チャレンジタグt^*を入力として生成された暗号文を除く）に対応する平文を入手できる条件下で，挑戦者から提示された暗号文（ただし，暗号文のタグは攻撃者が指定できる）の平文を攻撃者が求める攻撃である．

攻撃者Aに対する挑戦者Bを設定し，AとBの間で実行される次のようなゲーム（OW-TBE-CPA ゲーム）を構成する．

1. Bは，$TBE.Gen$に1^kを入力し秘密鍵sk，公開鍵 pkのペアを出力し，Aにpkを入力する．
2. Aはチャレンジタグt^*を出力し，Bに渡す．
3. Bは平文mを平文空間から一様に選択し，$c^* \leftarrow TBE.Enc(pk, t^*, m)$ を計算し，c^*をAに返す．
4. Aは$\hat{m}$を出力する．$\hat{m} = m$のときAの勝ちとする．

上記ゲームにおいて，Aは任意のタイミングで復号オラクルを利用することができる．復号オラクルは$TBE.Dec$アルゴリズムと等価だが，$t = t^*$が入力された際には⊥（復号不可）を返すという制限がある．

上記の OW-TBE-CCA ゲームに対する攻撃者Aのアドバンテージを

$$Adv_A^{OW-TBE-CCA}(k) = Pr[\hat{m} = m]$$

と定義し，いかなる多項式時間アルゴリズムAに対しても $Adv_A^{OW-TBE-CCA}(k) < \varepsilon(k)$ が成立するとき，そのタグベース暗号アルゴリズムは OW-TBE-CCA 安全であるという．

3.2 タグベース CAPTCHA

CAPTCHA は機械と人を判別するチューリングテストである[7]．著者らが知る限り，CAPTCHA の安全性を暗号学的に定式化した例は見当たらない．本節では 3.1 節で見たタグベース暗号の安全性の定義をもとに，タグベース CAPTCHA を定式化し，その安全性を定義する．

3.2.1 タグベース CAPTCHA アルゴリズム

タグベース CAPTCHA は 2 つのアルゴリズム（C_Enc, C_Dec）から構成される．C_Enc は，タグtと平文mを入力として CAPTCHA 型暗号文cを出力するアルゴリズム，C_Decはtとcを入力としてmあるいは⊥（復号不可）を出力するアルゴリズムである．ここでcは，AI 困難[8]な問題であり，現在効率的なアルゴリズムは見つかっておらず，人間にしか実行できないものと仮定する．

理解を促すためにあえて文字判読型 CAPTCHA を例に用いて説明する[a]と，図 3 は，C_Encにタグt=bity，平文m =logyro を入力した場合の CAPTCHA 型暗号文cの一例である．図 3 の CAPTCHA 型暗号文とタグ bity の入力に対し，C_Decは平文 logyro を出力する．図 3 の CAPTCHA 型暗号文が bity 以外のタグとともにC_Decに入力された場合は，C_Decの出力は⊥（復号不可）となる．

図 3 文字判読型 CAPTCHA

3.2.2 タグベース CAPTCHA の安全性

タグベース CAPTCHA の安全性の定義として，タグ選択平文攻撃に対する一方向性（OW-CAPTCHA-CPA）と，タグ選択暗号文攻撃に対する一方向性（OW-CAPTCHA-CCA）を定義する．

- タグ選択平文攻撃に対する一方向性

タグベース CAPTCHA のタグ選択平文攻撃に対する一方向性を定義する（OW-CAPTCHA-CPA）．タグ選択平文攻撃とは，攻撃者が任意の平文に対応する CAPTCHA 型暗号文を入手できる条件下で，挑戦者から提示された CAPTCHA 型暗号文（ただし，CAPTCHA 型暗号文のタグは攻撃者が指定できる）の平文を攻撃者が求める攻撃である．

定義 1

攻撃者Aに対する挑戦者Bを設定し，AとBの間で実行される次のようなゲーム（OW-CAPTCHA-CPA）を構成する

1. Aはチャレンジタグt^*を出力し，Bに渡す．
2. Bはmを平文空間から一様に選択し，$c^* \leftarrow C_Enc(t^*, m)$を計算し，$c^*$を$A$に返す．
3. Aは$\hat{m}$を出力する．$\hat{m} = m$のときAの勝ちとする．

上記の OW-CAPTCHA-CPA ゲームに対する攻撃者Aのアドバンテージを

$$Adv_A^{OW-CAPTCHA-CPA} = \Pr[\hat{m} = m]$$

と定義し，いかなるアルゴリズムAに対しても $Adv_A^{OW-CAPTCHA-CPA} < \varepsilon$ が成立するとき，その CAPTCHA アルゴリズムは OW-CAPTCHA-CPA 安全であるという．

更に復号オラクルへのクエリ回数が q（OW-CAPTCHA-CPA において復号オラクルは利用できな

a 文字判読型 CAPTCHA は，既にマルウェアによる解析が報告されている[9]ため、AI 困難な問題には当たるとは言えず、C_EncとC_Decの例としては実際には不適である．

いため$q = \varphi$である），リソース[b]がNに制限される任意のアルゴリズムAに対して，そのアドバンテージが無視できるとき，そのCAPTCHAアルゴリズムは(q,N)-OW-CAPTCHA-CPA安全であるという．

- タグ選択暗号文攻撃に対する一方向性

タグベースCAPTCHAのタグ選択暗号文攻撃に対する一方向性（OW-CAPTCHA-CCA）を定義する．タグ選択暗号文攻撃とは，攻撃者が任意のCAPTCHA型暗号文（ただし，チャレンジタグt^*を入力として生成されたCAPTCHA型暗号文を除く）に対応する平文を入手できる条件下で，挑戦者から提示されたCAPTCHA型暗号文（ただし，暗号文のタグは攻撃者が指定できる）の平文を攻撃者が求める攻撃である．

定義 2

攻撃者Aに対する挑戦者Bを設定し，AとBの間で実行される次のようなゲーム（OW-CAPTCHA-CCAゲーム）を構成する

1. Aはチャレンジタグt^*を出力し，Bに渡す．
2. Bはmを一様に選択し，$c^* \leftarrow C_Enc(t^*, m)$を計算し，$c^*$を$A$に返す．
3. Aは$\hat{m}$を出力する．$\hat{m} = m$のときAの勝ちである．

上記ゲームにおいて，Aは任意のタイミングで復号オラクルを利用することができる．復号オラクルはC_Decアルゴリズムと等価だが，$t = t^*$が入力された際には⊥（復号不可）を返すという制限がある．

上記のOW-CAPTCHA-CCAゲームに対する攻撃者Aのアドバンテージを

$$Adv_A^{OW-CAPTCHA-CCA} = \Pr[\hat{m} = m]$$

と定義し，いかなるアルゴリズムAに対しても$Adv_A^{OW-CAPTCHA-CCA} < \varepsilon$が成立するとき，そのCAPTCHAアルゴリズムはOW-CAPTCHA-CCA安全であるという．

更に復号オラクルへのクエリ回数がq，リソースがNに制限される任意のアルゴリズムAに対して，そのアドバンテージが無視できるとき，そのCAPTCHAアルゴリズムは(q,N)-OW-CAPTCHA-CCA安全であるという．

4. 提案プロトコルの安全性定義

本章では，2.1節で説明した取引内容改ざん型MITB攻撃に対する提案プロトコルの安全性を定義する．

4.1 受動的攻撃に対する安全性

受動的攻撃（IMP-PA）に対する提案プロトコルの安全性を定義する．

定義 3

受動的攻撃（IMP-PA）に対する提案プロトコルの安全性は，攻撃者A，証明者P（ユーザ），検証者V（銀行サーバ）間の以下のIMP-PAゲームによって定義される．

学習フェーズ：Aは，P，V間での正規のプロトコルの実行を監視し続けることによって，その通信系列πを入手する．

実行フェーズ：A，V間でプロトコルを実行する．

1. Aは偽の送金情報X'をVへ送る．
2. VはRを一様に選択し，$c(= C_Enc(X', R))$をAへ送る．
3. Aが$Q = R$をVへ送ることができたなら，Aの勝ちである．

上記のIMP-PAゲームに対する攻撃者Aのアドバンテージを

$$Adv_A^{IMP-PA} = \Pr[Q = R]$$

と定義し，いかなるアルゴリズムAに対してもアドバンテージが無視できるとき，提案プロトコルは受動的攻撃に安全（IMP-PA安全）であるという．

4.2 能動的攻撃に対する安全性

能動的攻撃（IMP-AA）に対する提案プロトコルの安全性を定義する．

定義 4

能動的攻撃（IMP-AA）に対する安全性は，攻撃者Aと証明者P（ユーザ）と検証者V（銀行サーバ）間の以下のIMP-AAゲームによって定義される．

学習フェーズ：Aは，P，V間での正規のプロトコルの実行を監視し続けることによって，その通信系列πを入手する．

実行フェーズ：P，A，V間でプロトコルを実行する．

1. Pが送金情報XをAへ送る．
2. Aは送金情報Xを$X'(\neq X)$に変更してVへ送る．
3. VはRを一様に選択し，$c(= C_Enc(X', R))$をAへ送る．
4. Aは任意のc'をPへ送ることができる．
5. Pは$R' \leftarrow C_Dec(X, c')$を計算する．タグ$X$で正しく復号できた場合（確認情報が送金情報$X$に一致した場合）には$Q = R'$を$A$へ送る．復号不可⊥の場合（確認情報が送金情報$X$に一致しない場合）には$Q = 0$を$A$へ送る．
6. Aが$Q' = R$をVへ送ることができたなら，Aの勝ちである．

上記のIMP-AAゲームに対する攻撃者Aのアドバンテージを

$$Adv_A^{IMP-AA} = \Pr[Q' = R]$$

と定義し，いかなるアルゴリズムAに対してもアドバンテージが無視できるとき，提案プロトコルは能動的攻撃に安全（IMP-AA安全）であるという．

b ここで「リソース」とは，計算時間や回路サイズ，学習データサイズなど，効率性に関する任意の指標を含む．

定義 5

定義 3 と定義 4 を同時に満たすとき提案プロトコルは取引内容改ざん型 MITB 攻撃に安全であるという．

5. 提案プロトコルの安全性証明

5.1 IMP-PA 安全であることの証明

OW-CAPTCHA-CPA 安全な CAPTCHA を利用する提案プロトコルは IMP-PA 安全であることを証明する．

定理 1

CAPTCHA が OW-CAPTCHA-CPA 安全ならば，その CAPTCHA を用いる提案プロトコルは IMP-PA 安全である．

定理 1 の証明

以下の(1)を証明する．

(1) 提案プロトコルに対し IMP-PA ゲームに無視できない確率で勝利するアルゴリズムAが存在するならば，OW-CAPTCHA-CPA 安全な CAPTCHA に対し OW-CAPTCHA-CPA ゲームに無視できない確率で勝利するアルゴリズムBが存在する．

Aを利用してBを構成する（図 3）．①BはAからのクエリに対して$\pi(=(m_B, t_B, c_B(=C_Enc(t_B, m_B))))$を送る．ここで$m_B, t_B, c_B$は$B$が任意に生成したものである．②$A$は送金情報$X$を$B$へ出力する．③$B$は$X$をチャレンジタグ$t^*$として IMP-PA ゲームの挑戦者に送る．④挑戦者はmを一様に選択し，$c^* \leftarrow C_Enc(t^*, m)$を計算し，⑤$B$へ入力する．$B$はこれを$A$へ入力する．⑥$A$は Q を出力する．⑦$B$は$\hat{m}(=Q)$を挑戦者に返答する．

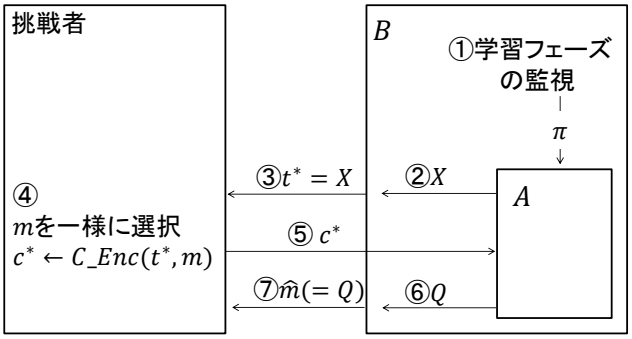

図 4 定理 1 の証明

ここで, Aは IMP-PA ゲームに無視できない確率で成功するアルゴリズムであるため$Q = m$ を無視できない確率で出力する．BはAからの出力Q を $\hat{m}$ としてそのまま出力するため，Aが無視できない確率で$Q = m$を出力するとき，Bは$\hat{m} = m$ を出力でき，無視できない確率で OW-CAPTCHA-CPA ゲームに勝利することができる．

したがって，定義 1 と定義 3 より

$$Adv_A^{IMP-PA} = Adv_B^{OW-CAPTCHA-CPA} < \varepsilon$$

となる．

以上より定理 1 が証明された．

5.2 IMP-AA 安全であることの証明

OW-CAPTCHA-CCA 安全な CAPTCHA を利用するプロトコルは IMP-AA 安全であることを証明する．

定理 2

CAPTCHA が OW-CAPTCHA-CCA 安全ならば，その CAPTCHA を用いる提案プロトコルは IMP-AA 安全である．

定理 2 の証明

以下の(2)を証明する．

(2) 提案プロトコルに対し IMP-AA ゲームに無視できない確率で勝利するアルゴリズムAが存在するならば，OW-CAPTCHA-CCA 安全な CAPTCHA に対し OW-CAPTCHA-CCA ゲームに無視できない確率で勝利するアルゴリズムBが存在する．

Aを利用してBを構成する（図 4）．①BはAからのクエリに対して$\pi(=(m_B, t_B, c_B(=C_Enc(t_B, m_B))))$を送る．ここで$m_B, t_B, c_B$は$B$が任意に生成したものである．②$B$は送金情報$X$を$A$に入力する．③$A$は送金情報$X'(=X)$を出力する．④$B$は$X'$をチャレンジタグ$t^*$として IMP-AA ゲームの挑戦者に送る．⑤挑戦者はmを一様に選択し，$c^* \leftarrow C_Enc(t^*, m)$を計算し，⑥それを$B$に入力する．$B$は$c^*$を$A$に入力する．⑦$A$は$c'$を出力する．⑧$B$は$X$と$c'$を復号オラクルへ送信する．⑨$X \neq t^*$であるため復号オラクルは機能し，$C_Dec(X, c')$を実行した結果（$m'$あるいは⊥）を$B$に送る．⑩$B$は復号オラクルから$m'$を受け取った場合，$Q = m'$ をAに入力する．復号オラクルから⊥を受け取った場合，$Q = 0$ をAに入力する．⑪AはQ'を出力するため，⑫B は$\hat{m}(=Q')$を挑戦者に返答する．

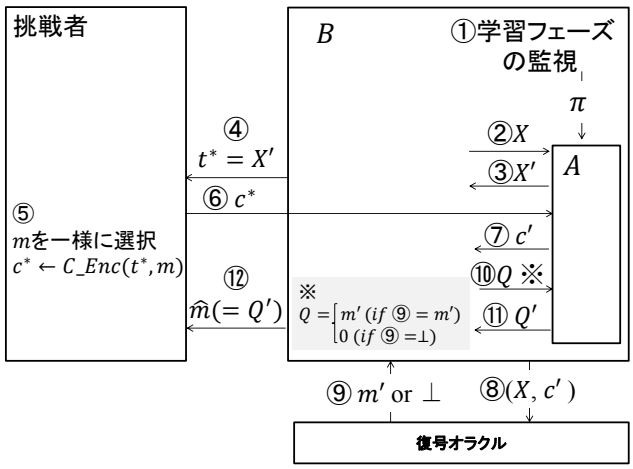

図 5 定理 2 の証明

ここで，Aは IMP-AA ゲームに無視できない確率で成功するアルゴリズムであるため$Q' = m$ を無視できない確率で出力する．BはAからの出力Q' を $\hat{m}$ としてそのまま出力するため, Aが無視できない確率で$Q' = m$ を出力するとき，

B は $\hat{m} = m$ を出力でき，無視できない確率で OW-CAPTCHA-CPA ゲームに勝利することができる．

したがって，定義 2 と定義 4 より

$$Adv_A^{IMP-\mathrm{AA}} = Adv_B^{OW-CAPTCHA-CCA} < \varepsilon$$

となる．

以上より定理 2 が証明された．

更に，定理 2 の証明（図 5）を見ると，Bは復号オラクルに対しクエリを一度しか行っていない．したがって，(1,N)-OW-CAPTCHA-CCA 安全な CAPTCHA を用いる提案プロトコルは IMP-AA 安全であるといえる．

提案プロトコルに対する取引内容改ざん型 MITB 攻撃に関し，受動的攻撃（IMP-PA）と能動的攻撃（IMP-AA）に対する提案プロトコルの安全性を，それぞれ，タグベース CAPTCHA の OW-CAPTCHA-CPA 安全性と (1,N)-OW-CAPTCHA-CCA 安全性に帰着できた．(1,N)-OW-CAPTCHA-CCA 安全は OW-CAPTCHA-CPA 安全を包含するため，(1,N)-OW-CAPTCHA-CCA 安全を満足するタグベース CAPTCHA を用いて CAPTCHA チャネルを構成したならば，提案プロトコルは取引内容改ざん型 MITB 攻撃に対し安全である．

以上より，CAPTCHA チャネルを実現する一手法としては(1,N)-OW-CAPTCHA-CCA 安全な CAPTCHA が利用できることが示された．

6. おわりに

本稿では人間（ユーザ）とコンピュータ（銀行サーバ）間のセキュア通信を実現することで MITB 攻撃への対策を試み，その第一歩として，人間・銀行サーバ間でセキュア通信を実現するチャレンジ＆レスポンス方式のプロトコルを提案した．CAPTCHA を応用することで提案プロトコルが実装可能であることを示した．また，タグベース暗号をもとに CAPTCHA を定式化し，(1,N)-OW-CAPTCHA-CCA を満たす CAPTCHA を用いた提案プロトコルが取引内容改ざん型 MITB 攻撃に対し安全であることを証明した．

提案プロトコルの実現には CAPTCHA チャネルの構成のために(1,N)-OW-CAPTCHA-CCA 安全な CAPTCHA が必要であり，これについては今後検討を行っていく必要がある．

参考文献

[1] “平成 26 年上半期のサイバー空間をめぐる脅威の情勢について”.http://www.npa.go.jp/kanbou/cybersecurity/H26_kami_jousei.pdf (参照 2017-02-03).
[2] “三菱東京 UFJ 銀行，当行のセキュリティ対策”. http://direct.bk.mufg.jp/secure/toukou.html (参照 2016-02-04).
[3] “三井住友銀行，三井住友銀行での取り組み”. http://www.smbc.co.jp/kojin/security/school/web/program.html (参照 2016-02-04).
[4] 土屋 貴史.他.”Man In The Browser 攻撃対策を実現する人間・銀行サーバ間のセキュア通信プロトコル”.CSEC.2015, vol.2015-CSEC-69,no.22.
[5] 鈴木 雅貴，中山 靖司，古原 和邦,”インターネット・バンキングに対する Man-in-the-Browser 攻撃への対策「取引認証」の安全性評価”.金融研究.2013,vol.32,no.3, pp.51-76.
[6] David Galindo.” A Separation Between Selective and Full-Identity Security Notions for Identity-Based Encryption”. ICCSA 2006, 2006,vol.3982,pp.318-326.
[7] “The Official CAPTCHA Site”.http://www.captcha.net/ (参照 2017-02-03).
[8] Luis Von Ahn, Manuel Blum, Nicholas J. Hopper, et al.” CAPTCHA: using hard AI problems for security”. EUROCRYPT 03,2003,vol.2656,pp.294-311.
[9] J.Yan, A.S.E.Ahmad, ” Breaking Visual CAPTCHAs with Naïve Pattern Recognition Algorithms”. 2007 Computer Security Applications Conference, pp.279-291.