社団法人 情報処理学会 研究報告
IPSJ SIG Technical Report

2004－CSEC－25 (10)
2004／5／21

様相論理による公平性の定義および認証プロトコルの安全性検証

今本 健二 * 櫻井 幸一 †

概要 様相論理に基づいた検証法であるSVOロジックを用いて公平性を定義し，公平交換プロトコルの安全性を検証する．本論文では公平交換プロトコルとして配達証明付き電子メールに着目し，Schneierらが提案したプロトコルを検証し，公平性を実現するために必要となる仮定を明確にする．

キーワード 認証プロトコル，公平性，安全性検証

Definition of Fairness and Verification of Authentication Protocol By Modal Logic

Kenji IMAMOTO * Kouichi SAKURAI †

Abstract— We define fairness by SVO logic based on modal logic, and verify the security of a fair exchange protocol. In this paper, we focus on certified mail protocol. We verify the fairness of the protocol proposed by Schneier et al. [4], and clarify assumptions needed to achieve defined fairness.

1 はじめに

情報関連技術の発達，インターネットなどの通信インフラの普及に伴い，遠隔地にいる相手との電子商取引が活況となっている．このような遠隔地にいる相手との公平な契約に関わる問題のひとつとしてメール配達証明問題がある [1]．これはメールの送信者が，相手がメールを受け取ったかどうかを第三者に証明したい状況を考えた際に起こる問題である．すなわち，送信者がメールを送ったことを第三者に対してレシートによって証明できるようにし，同時に受信者もそのメールを確実に受け取るアプリケーションを考える．

このとき求められる最も重要な性質は，“受信者がメールを受け取ったにも関わらず送信者はレシートを受け取ることができない（メールを送ったのに，受信者がメールを受け取ったことを証明できない）”，または“受信者がメールを受け取っていないにも関わらず送信者はレシートを受け取る（メールを送ってないのに，受信者がメールを受け取ったことになってしまう）”ということが起こらないという性質である．このような性質は公平性と呼ばれ，電子商取引において極めて重要な性質の1つとなっている．

この性質が満たされていない電子商取引システムの場合，購買者が代金を払ったにも関わらず商品を受け取ることができない，もしくは商品を受け取ったにもかかわらず代金を払わない，といった不公平な状況に陥る可能性がある．

これまでに様々な認証プロトコルが提案されてきたが，そのうちのいくつかは後に攻撃法が見つかっている．そこで，プロトコルを設計した際にはその方式が安全であるかどうか，どのような性質が実現できるのかを検証することが必要となる．本論文では公平交換プロトコルに対し，様相論理に基づいた

* 九州大学大学院システム情報科学府 〒812-8581 福岡市東区箱崎 6-10-1, Graduate School of Information Science and Electrical Engineering, Kyushu University, 6-10-1 Hakozaki, Higashi-ku, Fukuoka City, Japan: imamoto@itslab.csce.kyushu-u.ac.jp
† 九州大学大学院システム情報科学研究院 〒812-8581 福岡市東区箱崎 6-10-1, Faculty of Information Science and Electrical Engineering, Kyushu University, 6-10-1 Hakozaki, Higashi-ku, Fukuoka City, Japan: sakurai@csce.kyushu-u.ac.jp

形式的検証法であるSVOロジック[2, 3]を用いてプロトコルの安全性検証を行い，求められる性質を提案方式が実現していることを示す．

ただし，従来のSVOロジックを用いた検証では公平性が定義されていないため，公平性の概念をSVOロジックで新たに定義し，公平交換プロトコルの検証を行った．

本論文は以下の手順で説明を行う．2章では，SVOロジックで用いられる表記法や公理，また実現すべき要求として公平性を新たに定義する．3章ではSchneierらが提案した配達証明付き電子メールプロトコル[4]の公平性を検証する．4章では，3章で得られた検証結果を元に，公平性を実現するために必要となる仮定について考察する．

2 様相論理に基づいたプロトコルの安全性検証

本章では，提案方式に対し，様相論理に基づいた形式的検証法の一つであるSVOロジック[2, 3]を用いて安全性の検証を行う．SVOロジックは認証プロトコルの検証に用いられるツールであり，特にDiffie-Hellman鍵交換を用いた秘密共有プロトコルの検証に適したロジックである．

SVOロジックでは，最初にプロトコルを実行する際の前提（既知共有鍵やPKIの利用など），プロトコルを実行することによって各参加者が得るメッセージ，およびそのメッセージから各参加者が確信できる事象を仮定し，これらの仮定よりプロトコルが要求を実現していることを検証する．ロジックを用いて検証することにより，その認証プロトコルが必要とする仮定，実現可能な要求を確認できる．

本章では，SVOロジックで用いられている表記法や規則，公理を説明する．その後，公平交換プロトコルにおいて満たすべき性質を定義する．

2.1 表記法

ここでは，[2, 3]に基づき以下のような表記法を導入する．P, Qは参加者，X, Yは事象やメッセージを意味する．

P ***believes*** X ： PはXが真であると信じる．

P ***received*** X ： PはXを含むメッセージを受け取った．

P ***said*** X ： PはXを含むメッセージを過去に送った．

P ***says*** X ： Pは現在のプロトコル開始後にXを送った．

P ***has*** X ： 以下の条件のうち1つ以上が成立している．

- プロトコル開始時から，PはXを所有している，
- PはXを受け取った，
- XはPによって新しく生成された．

P ***controls*** X ： PはXをコントロールしている．

$fresh(X)$ ： Xは現在のプロトコル実行以前に送信されたメッセージ内に含まれていなかった．

$P \overset{k}{\longleftrightarrow} Q$ ： PとQは通信のために共有鍵kを用いる．kはP，Q，もしくはPやQに信頼された参加者以外の存在に知られていない．

$PK_\delta(P, k)$ ： kは，Pのセッション鍵生成の際の公開要素である．

$PK_\psi(P, k)$ ： kは，Pの公開暗号化鍵である．

$PK_\sigma(P, k)$ ： kは，Pの公開署名検証鍵である．

$SV(X, K, Y)$ ： 署名付きメッセージXを与えられたとき，鍵Kを署名検証鍵として利用し，Yを対応する秘密鍵で署名されたメッセージであることを検証する．

$\{M\}_k$ ： メッセージMに対して鍵kを用いた暗号化．暗号化されたメッセージの内容は正しい鍵を持っている参加者のみ読み出しや検証が可能である．

$[M]_k$ ： メッセージMに対して鍵kを用いた署名．

$\langle X \rangle_{*P}$ ： PはメッセージXを知らない（例：$\{X\}_k$ where P does not know k）．

$P \overset{k-}{\longleftrightarrow} Q$ ： "$P \overset{k}{\longleftrightarrow} Q \wedge P$ *has* k"と等しい．

2.2 規則

SVOロジックでは，以下の2つの推論規則がある．

Modus Ponens ： φかつ$\varphi \rightarrow \psi$ならば，ψが推論される

Necessitation ： $\vdash \varphi$ならば，$\vdash P$ *believes* φが推論される

ここで，"$\Gamma \vdash \varphi$"は，上記の規則を用いることにより，φがΓから導くことが可能であることを意味する．"$\vdash \varphi$"は定理である（すなわち，仮定なしで公理のみから推測可能）．

2.3 公理

ここでは，SVOロジックで用いられる公理を導入する．Fは効率的な1対1関数であり，Pが計算可能な関数である．

Belief Axioms

1. $(P\ believes\ \varphi \wedge P\ believes\ (\varphi \rightarrow \psi))$
   $\rightarrow P\ believes\ \psi$
2. $P\ believes\ \varphi \rightarrow P\ believes\ (P\ believes\ \varphi)$

Source Association Axiom

3. $(P \overset{k}{\longleftrightarrow} Q \wedge R\ received\ \{X\ from\ Q\}_k)$
   $\rightarrow (Q\ said\ X \wedge Q\ has\ X)$
4. $(PK_\sigma(Q,k) \wedge R\ received\ X \wedge SV(X,k,Y))$
   $\rightarrow\ Q\ said\ Y$

Key Agreement Axiom

5. $(PK_\delta(P,k_P) \wedge PK_\delta(Q,k_Q)) \rightarrow P \overset{F_0(k_P,k_Q)}{\longleftrightarrow} Q$

   $F_0(k,k')$は，共有鍵を計算するためkとk^{-1}（もしくはk'とk^{-1}）を結びつける関数であり，暗黙的にDiffie-Hellman鍵交換を表している．

6. $\varphi \equiv \varphi[F0(K,K')/F0(K',K)]$

Receiving Axioms

7. $P\ received\ [X]_k \rightarrow P\ received\ X$
8. $P\ received\ (X_1,\cdots,X_n)$
   $\rightarrow P\ received\ X_i,\ for\ i=1,\cdots,n$
9. $(P\ received\ \{X\}_{k^+} \wedge P\ has\ k^-)$
   $\rightarrow P\ received\ X$

   このとき，k^+ and k^-はそれぞれ暗号化鍵，復号化鍵である（共通鍵暗号では$k^+ = k^- = k$）．

Posession Axioms

10. $P\ received\ X \rightarrow P\ has\ X$
11. $P\ has\ (X_1,\cdots,X_n)$
    $\rightarrow P\ has\ X_i,\ for\ i=1,\cdots,n$
12. $(P\ has\ X_1 \wedge\cdots\wedge P\ has\ X_n)$
    $\rightarrow P\ has\ F(X_1,\cdots,X_n)$

Comprehension Axiom

13. $P\ believes\ (P\ has\ F(X))$
    $\rightarrow P\ believes\ (P\ has\ X)$

Saying Axioms

14. $P\ said\ (X_1,\cdots,X_n)$
    $\rightarrow P\ said\ X_i \wedge P\ has\ X_i,\ for\ i=1,\cdots,n$
15. $P\ says\ (X_1,\cdots,X_n)$
    $\rightarrow (P\ said\ (X_1,\cdots,X_n) \wedge P\ says\ X_i),$
    $for\ i=1,\cdots,n.$

Freshness Axioms

16. $fresh(X_i) \rightarrow fresh(X_1,\cdots,X_n),$
    $for\ i=1,\cdots,n.$
17. $fresh(X_1,\cdots,X_n) \rightarrow fresh\ F(X_1,\cdots,X_n)$

Jurisdiction and Nonce-Verification Axioms

18. $(P\ controls\ \varphi \wedge P\ says\ \varphi) \rightarrow \varphi$
19. $(fresh(X) \wedge P\ said\ X) \rightarrow P\ says\ X$

Symmetric Goodness Axiom

20. $P \overset{k}{\longleftrightarrow} Q \equiv Q \overset{k}{\longleftrightarrow} P$

2.4 実現すべき要求

[2, 3]では，鍵交換プロトコルが実現すべき一般的な要求（認証，鍵確認，鍵のフレッシュネスなど）を定義している．また，[5]では非拒否性を導入している．しかし，前述した通り，公平な交換を実現する場合は公平性（両方のユーザが望んでいる結果を得る，またはどちらのユーザも得ることができない）を満たすことが最も重要である．そこで，以下では公平交換プロトコルにおける公平性をSVOロジックの表記法を用いて表す．

- **公平性**：参加者PがメッセージMを参加者Qへ送信し，QはPへメッセージM'を送信するとする．このとき，片方の参加者がメッセージを得た場合，必ずもう片方の参加者もメッセージを入手できる．これは以下のように表すことができる．

$$\text{“}P\ received\ M' \equiv Q\ received\ M\text{”}$$

上記の表記式のうち，参加者Pをメール送信者，参加者Qをメール受信者，Mをメール，M'をレシートとすることによって，配達証明付き電子メールへ適用できる．すなわち，上記式により，受信者がメッセージを入手した場合には必ず送信者はレシートが入手でき，受信者がメッセージを入手した場合には必ず送信者はレシートを入手できることが表現できる．配達証明付き電子メールにおけるレシートとは「メッセージMを受信者が確かに受信した」ことを検証者Jに証明するためのものである．よって，配達証明付き電子メールへ上記公平性を適用すると，“$J\ believes\ (Q\ received\ M) \equiv Q\ received\ M$”となる．

3 プロトコルの公平性検証

本章では，Schneier らが提案した公開掲示板を用いたプロトコル [4] を検証する．

本章では，メールを送信する存在を**送信者** (A)，A がメールを送信する相手を**受信者** (B) と呼ぶことにする．また，A と B の公平な交換を補助する**仲介者** (C：公開掲示板，もしくは信頼できる第三者機関) を利用する．また，交換の仲裁を行う存在を**検証者** (J) と呼ぶ．

3.1 Schneier らのプロトコル [4]

Schneier らの方式における仮定は以下の通りである．

B は自身の署名鍵を所有しており，A はプロトコル開始前から B の署名検証鍵を知っている．ここで，PB を B の署名検証鍵，SB を B の署名鍵として表す．

また，公開掲示板の性質は以下の通りである．

- 掲示板は公開されており，誰でも書き込み，閲覧できる
- 掲示板上で行われた取引は保存される

受信者がメールを受け取ったことは，掲示板が公開，保存している情報によって証明される（掲示板に公開されている正しい書き込みをレシートとする）．

具体的な手順は以下の通りである．

(1) 送信者 A はランダムにセッション鍵 K を生成し，メッセージ M を暗号化する．そして，B に $A, \{M\}_K$ を送信する．

(2) 受信者 B は S，$\{M\}_K$ に電子署名を付加し，$[S, \{M\}_K]_{SB}$ を A に送信する．

(3) A は 受信した $[S, \{M\}_K]_{SB}$ の署名を検証し，正しいことを確認する．正しければ，セッション鍵 K と $\{M\}_K$ を掲示板 C に送信し，公開する．

(4) B は C よりセッション鍵 K を手に入れ，メッセージ M を復号化する．

送信者は，受信者がメッセージ M を受け取ったことを，メッセージと署名値，および掲示板の公開記録を示すことにより証明する．

3.1.1 検証

ここでは [4] における公開鍵所有の前提や掲示板の持つ性質，プロトコルでの通信のやり取りから，どのような仮定が存在するか確認する．その後，それらの仮定に対して公理や規則を用いることによって，2 章で導入した公平性が実現できるかどうかを検証する．

仮定

以下では，Schneier らの方式における仮定を示す．

Schneier らの方式では受信者の署名が必要である．そのため，以下の式が仮定される．このとき，P1 は B が公開署名検証鍵を所有しており，プロトコル参加者はその公開鍵が確かにそのユーザのものであることを信じていることを示す．P2 は B がそれに対応した秘密鍵を所有していることを意味する．

P1. A, B *and* J *believe* $PK_\sigma(B, PB)$

P2. B *has* SB

また，プロトコルより，以下のように仮定される．P3 は，B がプロトコルの最初のメッセージを受信しない限り，A はプロトコルの 2 番目の通信を受信できないことを示している．P4 は，A が受信したプロトコルの 2 番目の通信が正しく署名されたものでない限り，C は 3 番目の通信を受信・公開できないことを示している．

P3. A *received* $[A, \{M\}_K]_{SB}$
$\rightarrow$ B *received* $(A, \{M\}_K)$

P4. C *said* $(K, \{M\}_K)$
$\rightarrow$ A *says* $(A, \{M\}_K)$
$\wedge$ A *received* $[A, \{M\}_K]_{SB}$
$\wedge SV([A, \{M\}_K]_{SB}, PB, (A, \{M\}_K))$

プロトコルの最後の通信で，A は C へメッセージ $(K, \{M\}_K)$ を送る．掲示板の性質により，掲示板へ送信されたメッセージは全て公開し，全参加者が閲覧できるため，以下の式が仮定される．

P5. C *said* $(K, \{M\}_K)$
$\rightarrow$ J *believes* C *said* $(K, \{M\}_K)$

P6. J *believes* C *said* $(K, \{M\}_K)$
$\rightarrow$ J *believes* B *received* $(K, \{M\}_K)$

署名，および公開記録 $(K, \{M\}_K)$ を検証者へ示すことにより，AがBへメッセージ M ($\{M\}_K$ を K で復号化した値) を送信したことをJへ証明できる．すなわち，セッション鍵，暗号文が公開されている場合に限り，BはMを入手でき，かつAはBのメール受信を証明できるルールであるため，以下のことが仮定される．

P7. J *believes* B *received* $(K, \{M\}_K)$
$\wedge$ J *received* $[A, \{M\}_K]_{SB}$
$\equiv J$ *believes* B *received* M

公平性を実現するため，Aがセッション鍵 K を掲示板に公開した場合，およびその場合に限り，Bはメッセージ M を得ることができるという仮定が必要である．すなわち，Bはその他の方法では鍵を得ることができず，掲示板が送信した内容はBへ届くことを意味する．よって，以下のことを仮定する．

P8. B *received* $M \equiv C$ *said* $(K, \{M\}_K)$

また，掲示板の情報公開に関する仮定として，Jは掲示板が送信したメッセージは全参加者に届くと信じる．さらに，AはBより署名を受信した後，Bのメール受信を検証してもらうため，Jに対して $[A, \{M\}_K]_{SB}$ を送信する．よって，以下のことが仮定される．

P9. A *received* $[A, \{M\}_K]_{SB}$
$\rightarrow J$ *received* $[A, \{M\}_K]_{SB}$

誘導

Schneierらの方式の参加者が得るbeliefを導き，実現可能な性質を解析する．ここでは，2章で定義した公平性を満たしていることを誘導する．

最初に，Bがメッセージを受信した場合，JはBの受信を検証できることを示す（すなわち，以下の式を誘導："B *received* $M \rightarrow J$ *believes* B *received* M"）．

(1) C *said* $(K, \{M\}_K)$

by (B *received* M) の仮定，P8，Belief Axioms

(2) J *believes* C *said* $(K, \{M\}_K)$

by (1)，P5，Belief Axioms

(3) J *believes* B *received* $(K, \{M\}_K)$

by (2)，P6，Belief Axioms

(4) A *received* $[A, \{M\}_K]_{SB}$

by (1)，P4，Belief Axioms

(5) J *received* $[A, \{M\}_K]_{SB}$

by (4)，P9，Belief Axioms

(6) J *believes* B *received* M

by (3)，(5)，P7，Belief Axioms

上記の誘導式のうち，(6) により，本方式は与式を満たしていることが分かる．

次に，JがBのメッセージ受信を検証できる場合，Bは必ずメッセージを受信できることを示す（すなわち，以下の式を誘導："J *believes* B *received* $M \rightarrow B$ *received* M"）．

(1) C *said* $(K, \{M\}_K)$

by (J *believes* B *received* M) の仮定，P7，Belief Axioms

(2) B *received* M

by (1)，P8，Belief Axioms

上記の誘導式のうち，(3) により，本方式は与式を満たしていることが分かる．

以上の検証より，"B *received* $M \equiv J$ *believes* B *received* M" が誘導されるため，公平性が実現できることが確認できた．

4 検証結果の解析

4.1 仮定の持つ意味

3章では，様相論理に基づいたプロトコルの解析手法の一つであるSVOロジックを用い，Schneierらプロトコル [4] の解析を行った．ここでは特に，公平交換プロトコルが満たすべき要求として，2章で提案した公平性について検証し，プロトコルがこの要求を満たしていることを確認した．

この要求を満たすためには様々な仮定が必要となった．検証の結果，必要となった仮定を前提ごとに分類すると以下のようになる．

公開鍵所有の前提	P1, P2
プロトコル	P3, P4
掲示板の性質	P5, P6
検証者によるメール受信検証	P7
セッション鍵の入手法	P8
検証情報の入手法	P9

公開鍵所有の前提に関しては，公開鍵認証基盤 (PKI) の存在を仮定することにより満たすことができる．プロトコルに関する仮定は，決められた以外の手続き

を行わないと前提を置けば実現できる．また，検証者によるメール受信検証に関しては，検証者が決められたルールに則って受信の有無を検証するとすれば，このことも仮定できる．メール受信を証明するためには，送信者は検証者に対して署名情報を送る必要がある．そのため，送信者が署名情報を入手した場合は検証者に対してその情報を検証者に送ると仮定できる（この手続きは，プロトコルの一部と考えることも出来る）．

P5では，掲示板が情報を公開した場合，検証者は掲示板により情報公開されたことを信じることを仮定している．また，P6では掲示板が情報を公開した場合，受信者はその情報を受信できることを仮定している．

しかし，掲示板が公開した情報は，攻撃者によって改ざん・横取りされた場合，もしくは攻撃者が掲示板になりすまして情報を公開した振りをした場合，このことは成り立たない．

よって，このことを仮定するためには，掲示板から各参加者へ送信した情報は通信途中で消失しないこと，および掲示板から送信した情報を受信した参加者はその情報が掲示板から送信された情報であることを確認できることが必要である．

また，セッション鍵の入手について仮定したP8についても考察する．この仮定では，掲示板がセッション鍵を公開しない限り受信者はメッセージを復号化できず，掲示板がセッション鍵を公開すれば受信者はメッセージを復号化できることを意味する．

このことは，送信者から掲示板へ送られる2番目の通信が受信者に横取りされた場合には成り立たない．同様に，受信した情報を掲示板が公開せず，受信者に漏洩した場合にも成り立たない．

以上のことを防止するためには，送信者から掲示板への通信情報を受信者が横取りできない仮定，もしくは横取りしたとしても，その情報からメッセージを復号化できない仮定が必要である．また，掲示板は受信した情報を必ず全て公開する仮定が必要となる．

4.2 仮定を実現するための手法

以上の考察をまとめると，Schneierらの方式において公平性を実現するためには以下のような性質が必要となる．

- 掲示板から受信者・検証者への送信情報は必ず届く
- 受信者はプロトコル3番目の通信情報を横取りしてメッセージを復号化できない
- 掲示板になりすますことはできない
- 掲示板は受信した情報を全て公開する

上記のうち，2番目の性質については公開鍵暗号化を用いることにより解決できる（例えば，送信者は掲示板へ3番目の通信を送る場合，掲示板の公開鍵で暗号化して送信し，掲示板はその情報を復号化して公開）．また，3番目の性質については電子署名を用いることにより解決できる（例えば，掲示板は情報を公開する際，自身の署名を付加して公開）．

1番目は通信路に関する性質であり，暗号学的手法では解決困難と考えられるため，物理層での対策が必要となる可能性がある．また，4番目は掲示板に対する信頼に関する性質であり，複数機関による掲示板の運用・管理・検証による解決法が考えられる．

5 おわりに

本論文では，様相論理に基づいたプロトコル検証法の一つであるSVOロジックを用いて公平交換プロトコルを検証するため，新たに公平性の定義を行い，配達証明付き電子メールプロトコルである[4]を検証した．その結果，公平性を実現できることを示せたが，公平性を実現するためには通信路の仮定や掲示板の振る舞いに対する仮定が必要であることが確認できた．また，その対策についても考察した．

参考文献

[1] D. Molnar, "Signing Electronic Contracts," 2001.

[2] P. Syverson and P. C. van Oorschot, "A Unified Cryptographic Protocol Logic," NRL CHAOS Report, 1996.

[3] P. Syverson and I. Cervesato, "The Logic of Authentication Protocols," FOSAD'00, LNCS2171, pp.63–137, 2001.

[4] B. Schneier and J. Riordan, "A Certified E-Mail Protocol," 13th Annual Computer Security Applications Conference, ACM Press, 1998.

[5] J. Zhou, "Non-repudiation in Electronic Commerce," Computer Security Series, Artech House, 2001.